IGEL OS

- Partner Solutions (see page 3)
- IGEL OS Articles (see page 19)
- IGEL OS Reference Manual (see page 1211)
- IGEL UD Pocket Manual (see page 2112)
- IGEL OS Creator (see page 2119)
- IGEL OS Creator for Windows (OSCW) (see page 2198)
- IGEL OS Release Notes (see page 2282)
- IGEL OS SCCM Add-On (see page 3459)

Partner Solutions

- Crossmatch / Digital Persona (see page 4)
- Diktamen Compatibility (see page 5)
- Imprivata OneSign Compatibility with IGEL OS (see page 6)
- Jabra Handsets / Headsets Compatibility with IGEL OS (see page 7)
- Nuance Compatibility (see page 9)
- Olympus Compatibility with IGEL OS (see page 10)
- Poly Headsets Compatibility with IGEL OS (see page 11)
- EPOS / Sennheiser Compatibility with IGEL OS (see page 12)
- Signotec Compatibility (see page 14)
- StepOver Signature Pads Compatibility (see page 15)
- Wacom Compatibility (see page 16)
- deviceTrust Support on IGEL OS Endpoints (see page 17)
- Philips Speech (see page 18)

A dongle must be used if delivered with a device (e.g. with a headset, etc.).

Crossmatch / Digital Persona

Users can authenticate to a Citrix server using a Crossmatch / DigitalPersona fingerprint reader. For this purpose, the associated server software must be integrated into the server.

The following Crossmatch / Digital Persona fingerprint readers are supported (for Citrix only):

- U.are.U 4500
- Eikon Touch 510
- Eikon Touch 710

→ To use the fingerprint readers in Citrix sessions, enable the **Crossmatch DigitalPersona fingerprint channel**; see Device Support (see page 1261).

Diktamen Compatibility

As of IGEL OS 10, the following devices with Diktamen dictation solutions are supported:

Dictation devices	**Vendor ID**	**Product ID**
Grundig SonicMic EU	0x15d8	0x0025
Grundig SonicMic US	0x15d8	0x0026
Grundig SonicMic US	0x15d8	0x002A
Grundig Cordex	0x15d8	0x0020
Philips 32xx, 35xx, 37xx	0x0911	0x0c1c
Philips 52xx	0x0911	0x149a
Philips 6264	0x0911	0x1878
Philips 6274	0x0911	0x2512
Olympus DR 2000	0x07b4	0x0216
Olympus DR 2100	0x07b4	0x0253
Foot pedals	**Vendor ID**	**Product ID**
VEC	0x05f3	0x00ff
Philips, old version	0x0911	0x184c
Philips	0x0911	0x1844
Infinity	0x0e0f	0x0003
Grundig	0x15d8	0x0024
Olympus	0x07b4	0x0218
DictaPhone	0x04b4	0x0100

Imprivata OneSign Compatibility with IGEL OS

The following endpoint devices are officially supported as of Imprivata OneSign Embedded. Also, we recommend checking the Supported Components Guide by Imprivata.

IGEL Partner Devices

- Supported devices with IGEL OS 11.03.500 or later. (*Hardware* > *Supported Devices* > *Devices Supported by IGEL OS11*)
  To convert endpoint devices to IGEL OS permanently, use the IGEL OS Creator (OSC) (see page 2120).
  To run IGEL OS as a live system without any permanent changes to the device, use UD Pocket (see page 2112).

IGEL Devices

IGEL Device	IGEL OS	Imprivata Ready	Citrix Receiver Support	VMware Horizon Support
UD2 LX	11.03.500 or later	✓	✓	✓
UD3 LX	11.03.500 or later	✓	✓	✓
UD6 LX	11.03.500 or later	✓	✓	✓
UD7 LX	11.03.500 or later	✓	✓	✓
UD9 LX	11.03.500 or later	✓	✓	✓
UD9 LX Touch	11.03.500 or later	✓	✓	✓

Jabra Handsets / Headsets Compatibility with IGEL OS

IGEL OS integrates remote call control (RCC) for Jabra headsets. The Jabra RCC is intended to control the state of radio connection in Bluetooth headsets.

To save battery power, the connection must be closed after every call.

A dongle must be used if delivered with a device (e.g. with a headset, etc.).

Jabra Devices Tested by IGEL

IGEL OS supports the following Jabra handsets and headsets (verified with Citrix and enabled Unified Communications Settings for Citrix Sessions in IGEL OS (see page 1281)):

Jabra model	IGEL OS 11.05.100 and higher
Jabra Engage 50	✓
Jabra Engage 65	✓
Jabra Engage 75	✓
Jabra Evolve 30 II	✓
Jabra Evolve 30 II	✓
Jabra Evolve2-40 USB-A (verified with Microsoft Teams optimization only; based on test results from the field)	✓
Jabra Evolve 40 - USB-C	✓
Jabra Evolve 40	✓
Jabra Evolve 65	✓
Jabra Evolve2 65	✓
Jabra Evolve 75	✓
Jabra Evolve2 85 (verified with Microsoft Teams optimization only; based on test results from the field)	✓
Jabra Handset 450	✓
Jabra Pro 9470	✓

For more information on the configuration of Jabra headsets, see Jabra (see page 2003) and How to Deploy a Jabra Xpress Package (see page 1052).

Nuance Compatibility

IGEL OS 11.01.100 or higher contains Nuance Citrix Client Audio Extension.

Nuance Citrix Client Audio Extension configures audio redirection on a Linux device in a Citrix environment to provide optimal support for speech recognition.

For further information, see the Readme for IGEL by Nuance.

Olympus Compatibility with IGEL OS

IGEL OS 11.08.330 and higher supports the following Olympus / OM SYSTEM dictation devices:

Device	Supported Protocols	
	RDP	Citrix
RS27H	✓	✓
RS27	✓	✓
RS27N	✓	✓
OM SYSTEM RS28N (earlier known as RS28H)	✓	✓
RS28	✓	✓
RS28N	✓	✓
OM SYSTEM RS31N (earlier known as RS31H)	✓	✓
RS31	✓	✓
RS32	✓	✓
DS9500	✓	✓
OM SYSTEM DS9100 (earlier known as DS9000)	✓	✓
RM4000P	✓	✓
RM4010P	✓	✓
RM4015P	✓	✓
RM4100N	✓	✓
RM4100S	✓	✓
RM4110N	✓	✓
RM4110S	✓	✓

Poly Headsets Compatibility with IGEL OS

IGEL OS supports the following Poly (former Plantronics) headsets (verified with Citrix and enabled HDX RealTime Media Engine (see page 1281)):

- Blackwire 5210
- Savi 8220
- Savi 8245 Office
- Voyager 5200 UC
- Voyager 5200 UC B5200 (Bluetooth)

The following headsets are End of Life (EOL) since December 31, 2023:

- Blackwire 325 (wired)
- C320 (wired)
- Voyager 6200 UC
- Voyager 8200 UC
- Voyager Focus UC B825

EOL devices are not qualified with current IGEL OS software releases.

A dongle must be used if delivered with a device (e.g. with a headset, etc).

EPOS / Sennheiser Compatibility with IGEL OS

The following EPOS/Sennheiser headsets are supported (verified with Citrix and enabled HDX RealTime Media Engine (see page 1281)):

With IGEL OS 11.04.200 or higher, EPOS Connect is integrated. For more information, see EPOS Connect (see page 2007).

A dongle must be used if delivered with a device (e.g. with a headset, etc).

Tested by IGEL

- EPOS/Sennheiser DW Pro USB
- EPOS/Sennheiser MB Pro
- EPOS/Sennheiser MB 660
- EPOS/Sennheiser SC 45
- EPOS/Sennheiser SC 70
- EPOS/Sennheiser SC 160
- EPOS/Sennheiser SC 260
- EPOS/Sennheiser SC 630

Tested by EPOS / Sennheiser

Wired Headsets

- Culture Series:
  - SC 30 USB ML
  - SC 60 USB ML
- Culture Plus Series:
  - SC 40 USB MS BLACK
  - SC 70 USB MS BLACK
- Culture Plus Mobile Series:
  - SC 45 USB MS
  - SC 75 USB MS
- Circle Series:
  - SC 230 USB MS II
  - SC 260 USB MS II
  - SC 230 with USB-ED CC 01 MS
  - SC 260 with USB-ED CC 01 MS
- Century Series:
  - SC 630 USB ML
  - SC 660 USB ML
  - SC 630 with USB-ED CC 01 MS

- SC 660 with USB-ED CC 01 MS

Wireless Headsets

- Bluetooth headsets:
  - MB Pro 1 UC ML
  - MB Pro 2 UC ML
  - Presence UC ML
  - MB 660 UC MS
- DECT headsets:
  - DW Office ML
  - DW Pro 1 ML
  - DW Pro 2 ML
  - SD Office ML
  - SD Pro 1 ML
  - SD Pro 2 ML
  - D 10 USB ML

Speakerphones

- SP 10 ML
- SP 20 ML
- SP 220 MS

Solution Based on Experience from the Field
The below solution has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.
The following EPOS audio devices need this configuration to work in Citrix or VMware Horizon with Skype for Business:

- `DW Pro 1 / DW Pro 2 = DIP 4 Autolink ON = pick up softphone = connect`
- `SDW 5035 / 5065 = DIP 5 = Oben = Audio Quality Best`
- `SDW 5035 / 5065 = DIP 2 = Unten = Autolink ON`

`DIP` means DIP switch which is integrated in the base station (hardware).

Signotec Compatibility

The following Signotec devices are supported:

Signotec Device	IGEL Firmware from	Citrix Receiver Support	RDP Support	VMware Horizon (RDP) Support
Signotec LCD Signature Pad Alpha	IGEL Linux 5.08.x	✓	✓	✓
Signotec LCD Signature Pad Gamma	IGEL Linux 5.09.x	✓	✓	✓
Signotec LCD Signature Pad Sigma	IGEL Linux 5.08.x	✓	✓	✓
Signotec LCD Signature Pad Omega	IGEL Linux 5.08.x	✓	✓	✓

StepOver Signature Pads Compatibility

As of IGEL OS 11.02.100, the StepOver TCP Client supports the applications eSignatureOffice, SimpleSigner, and StepOver APIs with the following devices:

duraSign pads:

- duraSign Pad Brilliance
- duraSign Pad 10.0

naturaSign pads:

- Standard 1 (FW 1.x)
- Standard 2
- Standard 2.5
- Classic
- Biometric
- Mobile
- Flawless
- Comfort
- ColourPad

The legacy models +Pad and BlueMobile are not supported.

Learn more in the how-to document "Using a StepOver Signature Pad (see page 1058)".

Wacom Compatibility

IGEL OS 11 supports the following Wacom devices (for Citrix only):

- DTU-1141B
- STU-500
- STU-520
- STU-530
- STU-300
- STU-430

deviceTrust Support on IGEL OS Endpoints

The deviceTrust client, which first comes with IGEL OS 10, adds context awareness to an endpoint. Access to a remote session can be granted or denied, depending on the device's location, network connection, hardware, or according to other criteria. For further information, see:

- https://www.igel.com/ready/showcase-products/devicetrust/[1]
- https://devicetrust.com/technology-platform/igel/
- https://docs.devicetrust.com/docs/20.2/installation/installation-client-igel/

To enable deviceTrust:

- For Citrix sessions: See Device Support (see page 1261)
- For RDP sessions: See Device Support
- For AVD sessions: Go to **System > Registry** and activate the following registry key:

Parameter	deviceTRUST
Registry	`sessions.wvd<inst>.plugins.devicetrust`
Value	enabled / disabled

- For Amazon WorkSpaces: Go to **System > Registry** and activate the following registry key:

Parameter	deviceTRUST
Registry	`awsc.plugins.devicetrust`
Value	enabled / disabled

- For VMware Horizon (as of IGEL OS 11.08.230): Go to **System > Registry** and activate the following registry key:

Parameter	deviceTRUST virtual channel
Registry	`vmware.view.vcdevicetrust.enable`
Value	enabled / disabled

1. https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.igel.com%2Fready%2Fshowcase-products%2Fdevicetrust%2F&data=04%7C01%7Cloew%40igel.com%7C17f55dbdebb343b3204208d8f0423240%7C3f04441122ea4ba182dfd85e25879b4f%7C0%7C0%7C637523514995310251%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=0%2FZ0VHPstSTCXMIDmv33CtvM1yUD%2BQ0l9oDkT0UIlpA%3D&reserved=0

Philips Speech

The following dictation and accessory devices have been tested with IGEL OS by Philips Speech.

Device Category	Device Type	Officially tested by IGEL
SpeechAir	PSP1100 PSP2100	
Digital PocketMemo 4	DPM8000 DPM8200 DPM8500	✔
SpeechOne	PSM6000	
SpeechMike Premium Air	SMP4000 SMP4010	
SpeechMike Premium Touch	SMP3810 SMP3800 SMP3710 SMP3700	
SpeechMike Premium	LFH3610 LFH3600 LFH3520 LFH3510 LFH3500	✔
SpeechMike 3	LFH3310 LFH3300 LFH3220 LFH3210 LFH3200	✔
Foot Control	ACC2330 ACC2320 ACC2310 LFH2330 LFH2320 LFH2310	✔
AirBridge	ACC4100	

IGEL OS Articles

- Overview: First Steps with IGEL OS 11 (see page 20)
- Update and Upgrade (see page 23)
- BIOS Tools (see page 327)
- Citrix (see page 389)
- RDP (see page 449)
- VMware Horizon (see page 466)
- Evidian (see page 481)
- IBM iAccess (see page 486)
- Imprivata (see page 505)
- Microsoft Azure Virtual Desktop (AVD) (see page 508)
- SSH (see page 535)
- Using Amazon WorkSpaces via the HP Anyware PCoIP Client (see page 539)
- Login Enterprise Configuration (see page 548)
- Nutanix (see page 561)
- Browser (see page 565)
- System (see page 588)
- Network (see page 607)
- Security (see page 665)
- Certificates (see page 744)
- Smartcard (see page 781)
- Desktop and Display (see page 821)
- Customizing (see page 851)
- Devices (see page 980)
- Printer (see page 1120)
- UD Pocket (see page 1133)
- Miscellaneous (see page 1151)

Overview: First Steps with IGEL OS 11

The following article provides a short overview of how to get started with an IGEL device or a third-party device that you want to convert to IGEL OS. The steps are generally the same, but in the case of a third-party device you will need to use the IGEL OS Creator.

IGEL Device	3d-Party Device
Step 1: Download and install the UMS • IGEL Download Server[2] • Instruction: *Universal Management Suite > IGEL UMS Reference Manual > UMS Installation and Update > IGEL UMS Installation* • Video: UMS installation on a Windows Server[3] • Video: UMS installation on a Linux operating system[4] **Step 2: Activate your IGEL OS 11** **with the Setup Assistant (free evaluation license)**: • Instruction: Setup Assistant for IGEL OS (see page 2101), section "Register for Demo License". See also *IGEL Subscription & More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Getting a Demo License*. • Video: Acquire a Demo License Including Workspace Edition and Enterprise Management Pack[5] **via UMS (purchased license)**: • *IGEL Subscription & More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploy licenses using automatic or manual license deployment method*. • Video: Register an endpoint in the UMS and assign a license to it[6] **Step 3: Configure your device** **with the UMS**:	**Step 1: Download and install the UMS** • IGEL Download Server[9] • Instruction: *Universal Management Suite > IGEL UMS Reference Manual > UMS Installation and Update > IGEL UMS Installation* • Video: UMS installation on a Windows Server[10] • Video: UMS installation on a Linux operating system[11] **Step 2: Download IGEL OS 11** • IGEL Download Server[12], section **OS 11 > OS Creator** **Step 3: Convert your device to IGEL OS 11** • IGEL OS Creator Manual (see page 2120) • Video: Converting an x86-Endpoint Using the IGEL OS Creator[13] **Step 4: Activate your IGEL OS 11** **with the Setup Assistant (free evaluation license)**: • Instruction: Setup Assistant for IGEL OS (see page 2101), section "Register for Demo License". See also *IGEL Subscription & More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Getting a Demo License*. • Video: Acquire a Demo License Including Workspace Edition and Enterprise Management Pack[14] **via UMS (purchased license)**:

2. https://www.igel.com/software-downloads/workspace-edition/
3. https://www.youtube.com/watch?v=3YJnFiE7y5w
4. https://www.youtube.com/watch?v=p52CxtB_0ok
5. https://www.youtube.com/watch?v=j31c8dzBMAg
6. https://www.youtube.com/watch?v=01N-9b3P4wo
9. https://www.igel.com/software-downloads/workspace-edition/
10. https://www.youtube.com/watch?v=3YJnFiE7y5w
11. https://www.youtube.com/watch?v=p52CxtB_0ok
12. https://www.igel.com/software-downloads/workspace-edition/
13. https://www.youtube.com/watch?v=xVqcX6QTZ5g
14. https://www.youtube.com/watch?v=j31c8dzBMAg

IGEL Device	3d-Party Device

• Create a profile* with the required settings and assign it to the device**.
  • **IGEL Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS > Using Profiles > Creating Profiles in the IGEL UMS*
  • ***IGEL Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS > Using Profiles > How to Allocate IGEL UMS Profiles*
 	
See also *IGEL Universal Management Suite > UMS Articles > Profiles in IGEL UMS.*
 	
• Video: Configure an endpoint in the UMS using profiles[7]
 	
without the UMS:
 	
• Use the IGEL Setup on the device, e.g. to configure User Interface (see page 1844) and Sessions (see page 1243).
• Video: Configuring an Endpoint with IGEL OS 11[8]
	• *IGEL Subscription & More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploy licenses using automatic or manual license deployment method.*
	• Video: Register an endpoint in the UMS and assign a license to it[15]
	
	Step 5: Configure your device with the UMS:
	
	• Create a profile with the required settings and assign it to the device.
	  • **IGEL Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS > Using Profiles > Creating Profiles in the IGEL UMS*
	  • ***IGEL Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS > Using Profiles > How to Allocate IGEL UMS Profiles*
	
	See also *IGEL Universal Management Suite > UMS Articles > Profiles in IGEL UMS.*
	
	• Video: Configure an endpoint in the UMS using profiles[16]
	
	without the UMS:
	
	• Use the IGEL Setup on the device, e.g. to configure User Interface (see page 1844) and Sessions (see page 1243).
	• Video: Configuring an Endpoint with IGEL OS 11[17]

7. https://www.youtube.com/watch?v=Sc38mRv5Z1s
8. https://www.youtube.com/watch?v=6WfLVgYBTHg
15. https://www.youtube.com/watch?v=01N-9b3P4wo
16. https://www.youtube.com/watch?v=Sc38mRv5Z1s
17. https://www.youtube.com/watch?v=6WfLVgYBTHg

Update and Upgrade

- Upgrade and Downgrade Limit on IGEL OS 11.10.410 or Higher (see page 24)
- Upgrading (Migration) from IGEL OS 11 to IGEL OS 12 (see page 25)
- Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61)
- Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update (see page 64)
- Upgrading from IGEL OS 10 to IGEL OS 11 (see page 129)
- Buddy Update (see page 303)
- Firmware Update (see page 310)
- Updating IGEL OS Using a USB Storage Device (see page 314)
- Updating the Firmware using the Linux Console (see page 315)
- Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318)
- Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG (see page 321)
- Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher (see page 323)
- IGEL OS Automatic Update Service for Device Evaluation (see page 325)

Upgrade and Downgrade Limit on IGEL OS 11.10.410 or Higher

> ⚠ The shim bootloader signature used in IGEL OS 12.6.1 PR1 or lower and in OS 11 releases lower than 11.10.410 could potentially be revoked.
> If the older shim bootloader signature is revoked and Secure Boot is enabled, the device may become unbootable.
> Upgrade and downgrade limits are introduced to prevent unbootable systems and ensure a consistent user experience.
> Verify boot compatibility before upgrading or downgrading.

Upgrade Limit

Starting from IGEL OS 11.10.410, IGEL OS 11 devices can no longer be upgraded (migrated) to IGEL OS 12 versions lower than 12.7.0. This restriction applies to IGEL UD Pocket[18] devices and endpoints with Secure Boot enabled (see Verifying that Secure Boot is Enabled[19]).

In such cases, migration attempts to versions prior to 12.7.0 will be refused to maintain system integrity and boot security.

Downgrade Limit

Starting from IGEL OS 11.10.410, the IGEL OS 11 can no longer be downgraded to versions lower than 11.10.410. This restriction applies to IGEL UD Pocket[20] devices and endpoints with Secure Boot enabled (see Verifying that Secure Boot is Enabled[21]).

In such cases, downgrade attempts to versions prior to 11.10.410 will be refused to maintain system integrity and boot security.

18. https://kb.igel.com/hardware/current/ud-pocket-powered-by-igel-ud-pocket-products
19. https://kb.igel.com/security-safety/current/verifying-that-secure-boot-is-enabled
20. https://kb.igel.com/hardware/current/ud-pocket-powered-by-igel-ud-pocket-products
21. https://kb.igel.com/security-safety/current/verifying-that-secure-boot-is-enabled

Upgrading (Migration) from IGEL OS 11 to IGEL OS 12

This document describes upgrading endpoint devices from IGEL OS 11 to IGEL OS 12 via the Universal Management Suite (UMS).

The IGEL UMS serves as the standard update server for device upgrades. However upgrades can be performed using other methods, such as migration through the Distributed Peer Update Server. This approach is useful when upgrading a large number of devices simultaneously, as it reduces bandwidth consumption and accelerates update delivery, especially across geographically distributed networks. For details, see How to Upgrade Devices from IGEL OS 11 to OS 12 Using Distributed Peer Update .

Please test the upgrade on one or more representative devices before you upgrade all devices. For this purpose, perform the upgrade described under Manual Upgrade (see page 37) on the test devices.

It is highly recommended that IGEL OS 11.10.210 or higher be used to perform inline migration to IGEL OS 12.
The benefits are:

- Added notifications on progress, error, and download completed
- Added command to perform a certificate check via UMS (to ensure that the device is ready to migrate to OS 12)
- Latest minor improvements

License Required

For migration to IGEL OS 12, an active Workspace Edition or Workspace Edition Evaluation license is required.
An IGEL OS Starter License is not valid for migrating devices to IGEL OS 12.

Action Required if Devices Are Managed via ICG and UMS 12.02.130

If some of the devices you want to upgrade are managed via the IGEL Cloud Gateway (ICG) and you are using UMS 12.02.130, please follow the instructions under Errors after OS12 Upgrade of an OS11 Device which Is Managed via ICG (see page 58).

IGEL Community Video

See also the IGEL Community video How to update IGEL OS 11 to IGEL OS 12[22]

Synopsis

The procedure is as follows:

22. https://www.youtube.com/watch?v=nJOLrvsyM0I

1. Get IGEL OS 12 from the App Portal (see page 27)
2. Create new Profiles for IGEL OS 12 (see page 33)
3. Manual Upgrade (see page 37) - test the upgrade on one or more typical devices
4. Unattended Upgrade (see page 47) - automated mass upgrade

Devices That Can Be Upgraded to IGEL OS 12

For hardware requirements, see Devices Supported by IGEL OS 12 .

IGEL OS 11.09.260 provides a hardware check to determine whether the endpoint device's hardware is suitable for IGEL OS 12.

It is possible to upgrade devices with 2 GB. For this purpose, you must set the registry parameter **system.upgrade_igelos.ignore_memory_requirement** to **enabled**.
Please note that an upgrade of devices that do not meet the minimal requirements for IGEL OS 12, which is the case for devices with less than 4 GB, is at your own risk. There is no official support from IGEL.

Required UMS Version

For upgrading devices from IGEL OS 11 to IGEL OS 12, the Universal Management Suite (UMS) version 12.02.120 or later is required.

For upgrading devices from IGEL OS 11 to IGEL OS 12 via the ICG, the Universal Management Suite (UMS) version 12.02.130 or later is required.

Required IGEL OS 11 Version

Use IGEL OS 11.10.210 or later as a starting point, as many upgrade-related issues have been fixed with that version; for details, see New Features 11.10.210 (see page 2365) , section "Firmware update" and Resolved Issues 11.10.210 (see page 2375), section "Firmware update". For instructions on updating to a higher version of IGEL OS 11, see Firmware Update (see page 310) .

Required IGEL OS 12 Verison

Upgrade Limitation

Starting from IGEL OS 11.10.410, IGEL OS 11 devices can no longer be upgraded to IGEL OS 12 versions lower than 12.7.0, due to an older shim bootloader signature used in IGEL OS 12.6.1 PR1 or earlier. For details, see Upgrade and Downgrade Limit on IGEL OS 11.10.410 or Higher (see page 24) .

Recommendation: Use IGEL OS 12.7.1 or Higher for Unattended Upgrade

If you are planning to use the unattended upgrade (see page 47) method, IGEL OS 12.7.1 or later is the recommended target version.
With lower versions of IGEL OS 12, a manual reboot is required to finish the upgrade.

Important! Consider This Before Upgrading!

Features (e.g. Clients)

IGEL OS 12 does not have the complete feature set of IGEL OS 11. Make sure that the current version of the IGEL OS 12 base system combined with the available apps meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions Not Supported

Custom Partitions are not supported by IGEL OS 12. If a device has a Custom Partition, the system check will deny the upgrade.
However, you can force the upgrade by setting the registry parameter **system.upgrade_igelos.delete_custom_partition** to **enabled**. The Custom Partition will then be deleted during the upgrade.

No Downgrade to IGEL OS 11

A downgrade from IGEL OS12 to IGEL OS11 is not possible. Please test IGEL OS12 thoroughly before upgrading.

IGEL OS 12 Profiles Must Be Created

There is no conversion of UMS profiles for IGEL OS 11 to UMS profiles for IGEL OS 12. Therefore, you must create appropriate IGEL OS 12 profiles before the upgrade. This is necessary to ensure that your device settings will be preserved.

Battery Power

If the device is running on battery, the charge status must be at least 50%.

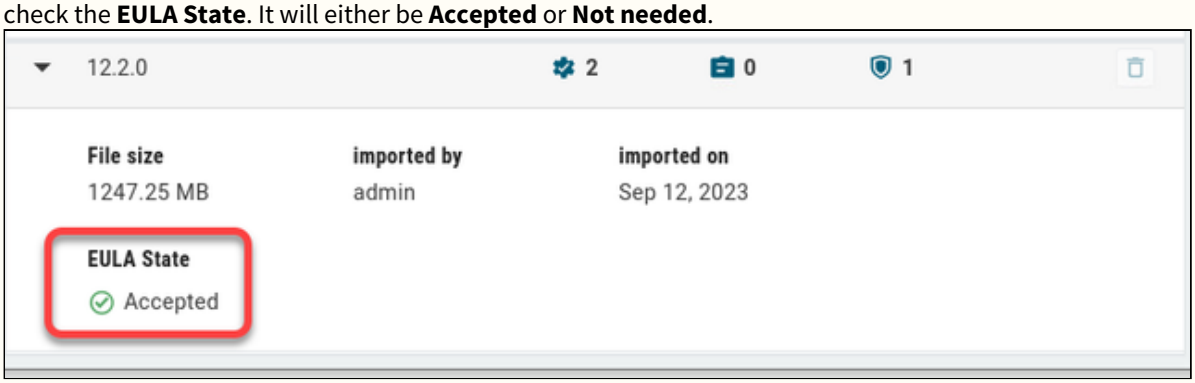
Connection to UMS 12 without VPN

The device must be connected to a UMS 12.02.120 or higher without the use of a VPN.

Getting IGEL OS 12 from the App Portal

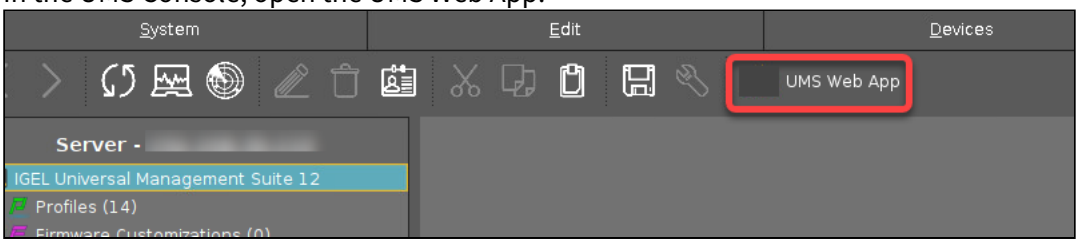
If the target version of IGEL OS 12 has already been imported into your UMS, you must ensure that the EULA has been accepted.

→ In your UMS Web App, go to **Apps > IGEL OS Base System**, find the version you want to upgrade to, and check the **EULA State**. It will either be **Accepted** or **Not needed**.

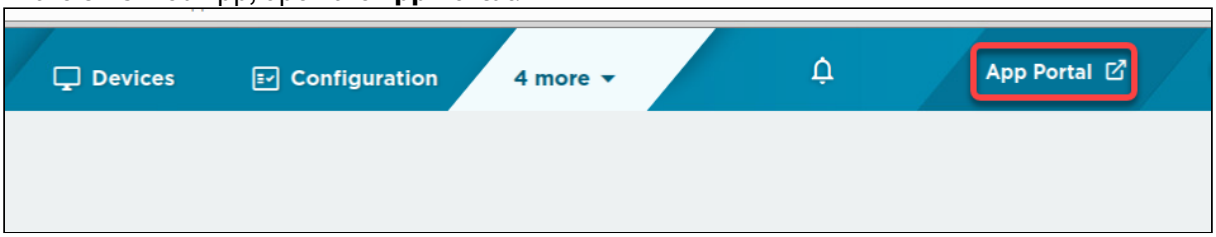


If the **EULA State** is **Accepted**, everything is in order. If it is **Not needed**, the upgrade process will be aborted. To circumvent this, see Workaround: What to Do If the EULA State is "Not Needed" (see page 56).

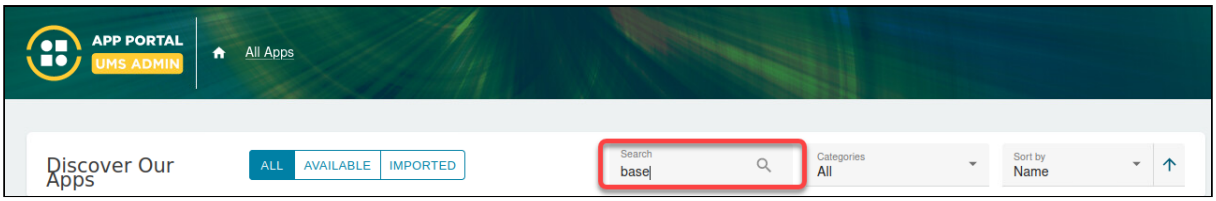
1. In the UMS Console, open the UMS Web App.

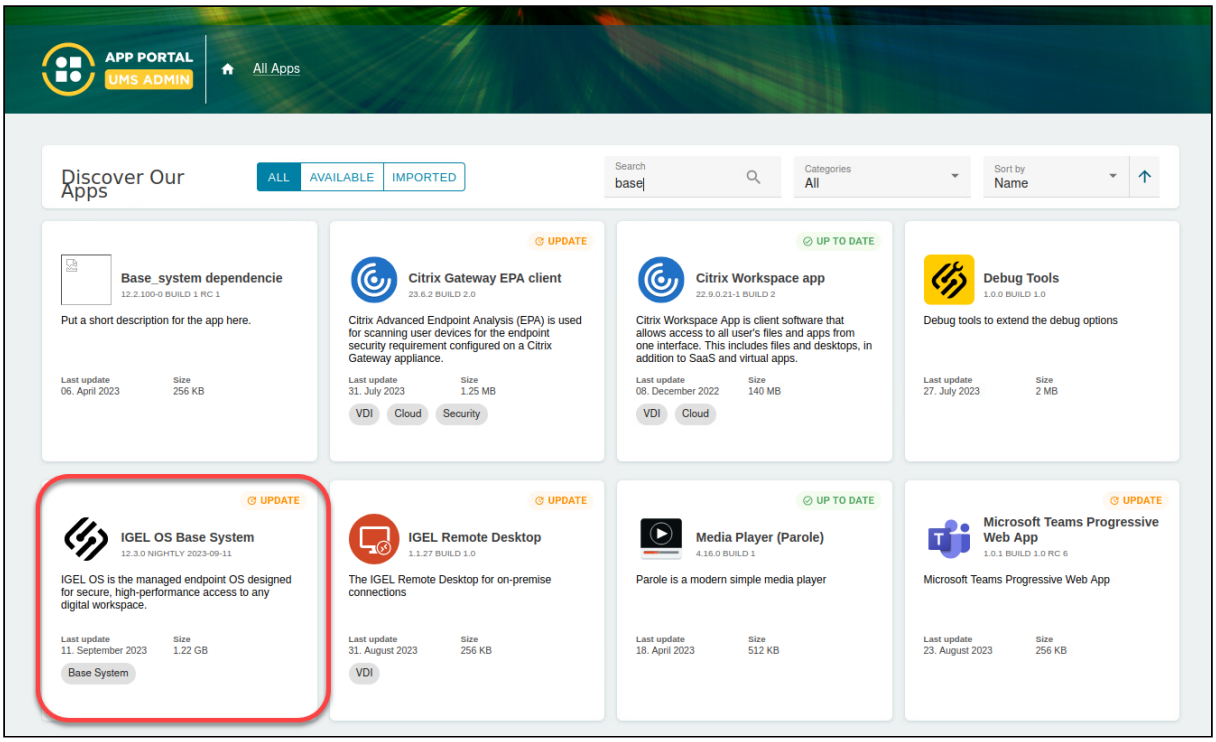


2. In the UMS Web App, open the **App Portal**.



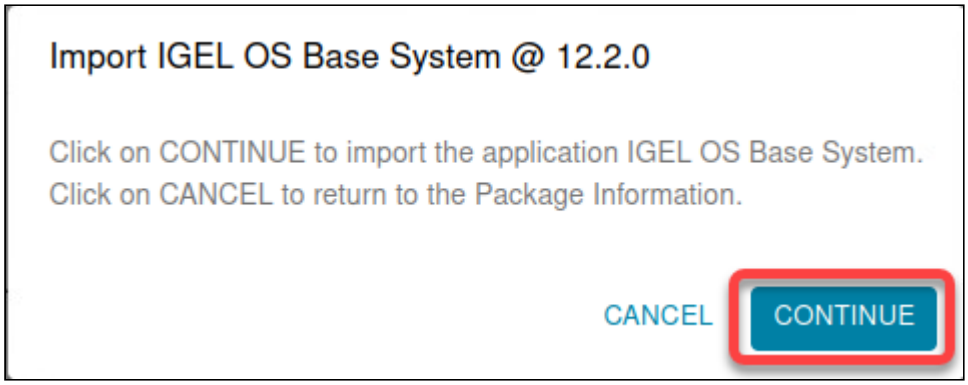
3. In the App Portal, search for"base" and then select **IGEL OS Base System**.





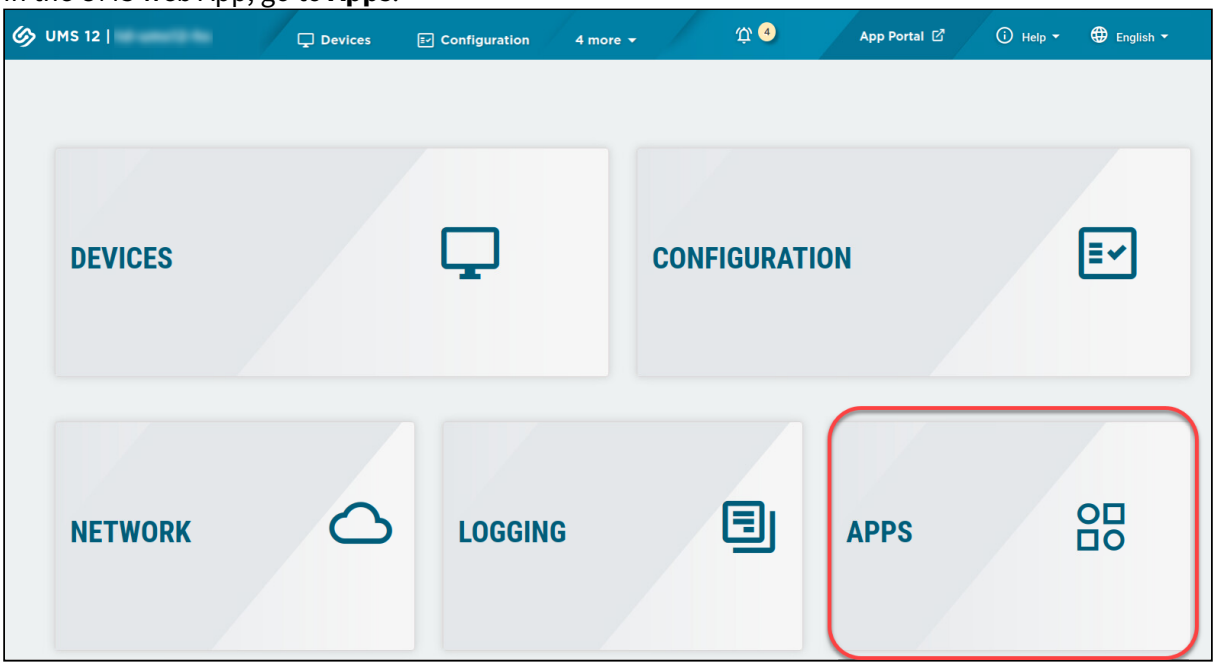
4. Choose the appropriate version, click **IMPORT** and confirm the dialogs.

APP PORTAL
UMS ADMIN
All Apps › IGEL OS Base System
UP TO DATE
IGEL OS Base System
Versions
12.2.0
IMPORT
DESCRIPTION
HISTORY
IGEL OS 12
IGEL OS 12 is the latest version of IGEL's managed endpoint OS designed for secure,
workspace.

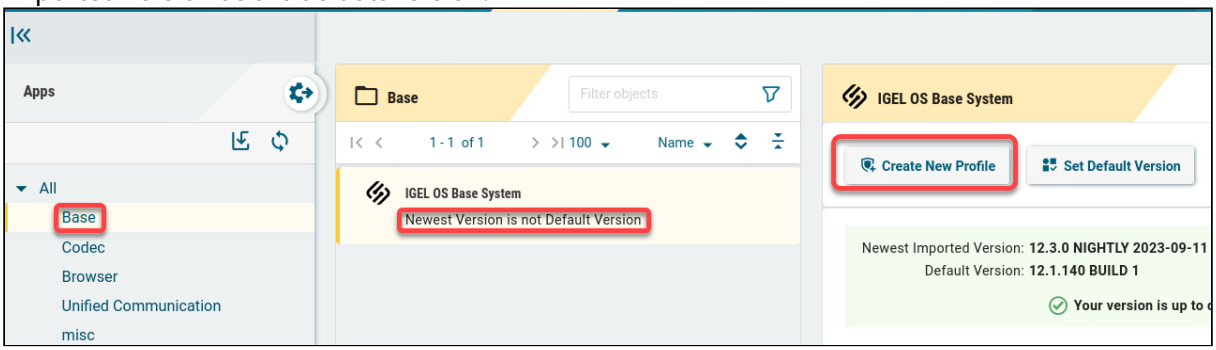

Import IGEL OS Base System @ 12.2.0
Click on CONTINUE to import the application IGEL OS Base System.
Click on CANCEL to return to the Package Information.
CANCEL
CONTINUE

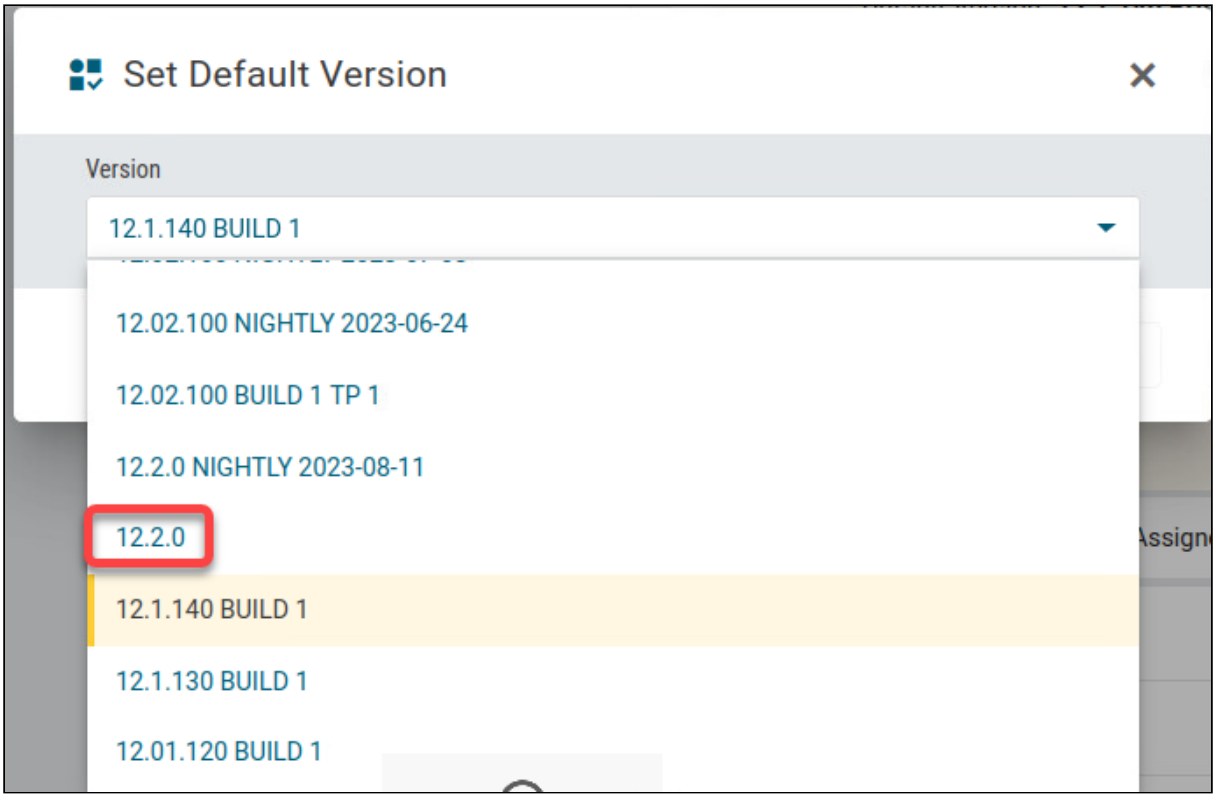
The IGEL OS Base System app is imported into your UMS and will be available for your devices.

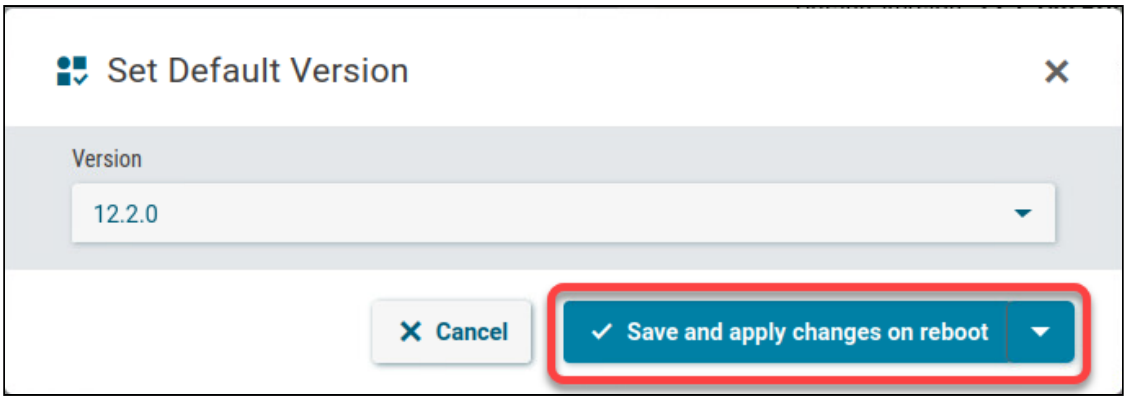
5. In the UMS web App, go to **Apps**.



6. In the **Apps** list, select **Base**. If **Newest Version is not Default Version** is displayed, set the newly imported version as the default version.







Creating new Profiles for IGEL OS 12

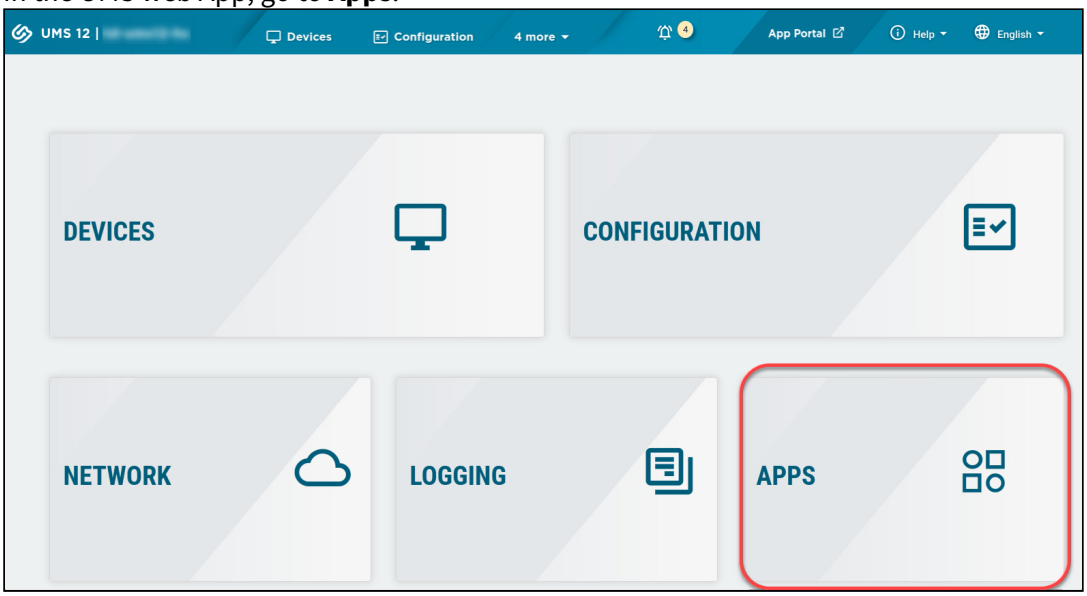
All the device settings that have been made via profiles must be defined again with IGEL OS 12 profiles. This is because OS 11 profiles cannot be assigned to OS 12 devices.

For those settings that refer to a session, like Citrix, RDP, or the Chromium browser, the IGEL OS 12 profile will trigger the installation of the appropriate app.

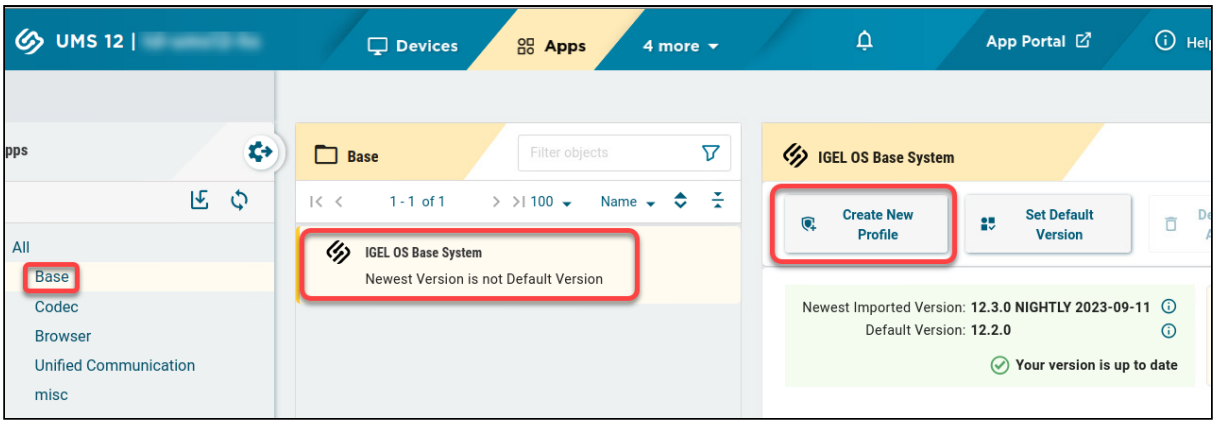
In the following, we create a profile for basic settings and a profile for the Chromium browser. The basic settings profile will configure the base system app, while the Chromium browser will configure the Chromium browser app.

Example Profile: Basic Settings

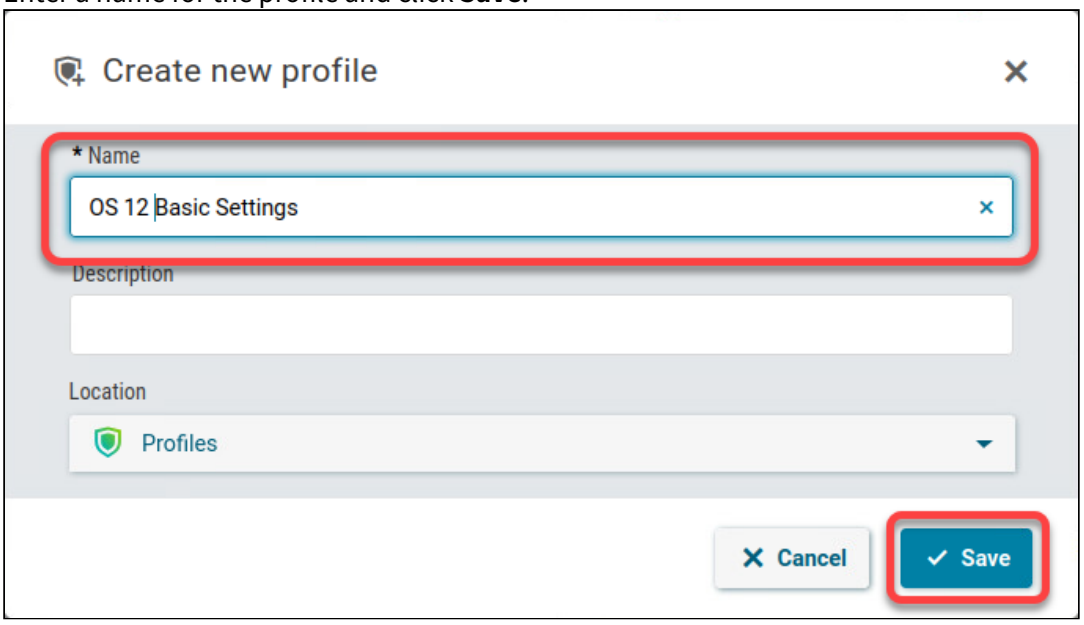
1. In the UMS web App, go to **Apps**.



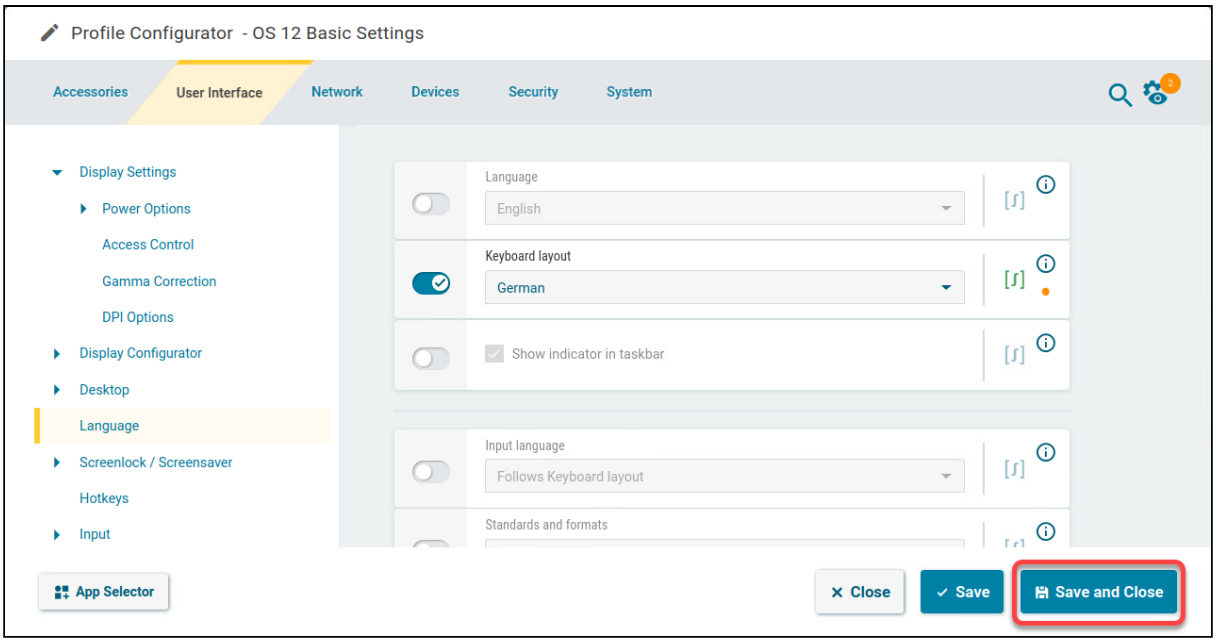
2. Select the **IGEL OS Base System** and then click **Create new profile**.



3. Enter a name for the profile and click **Save**.

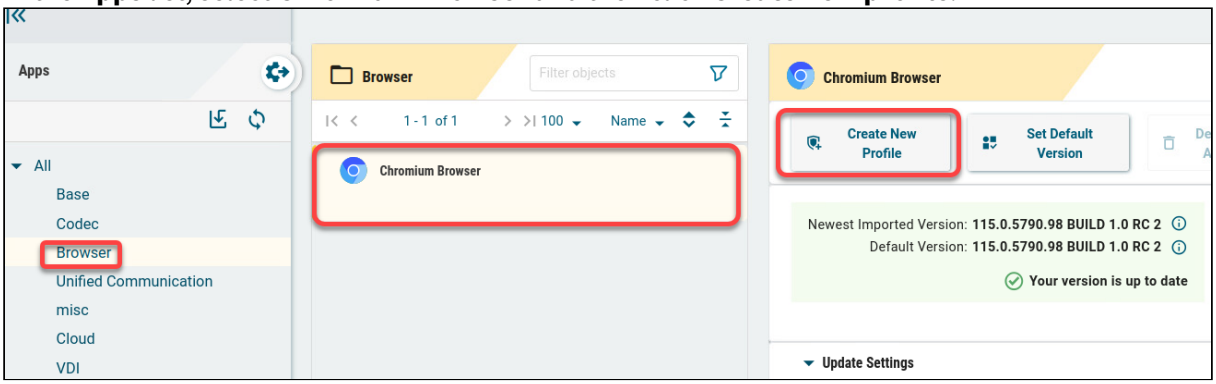


4. Edit the settings according to your needs and then click **Save and close**.

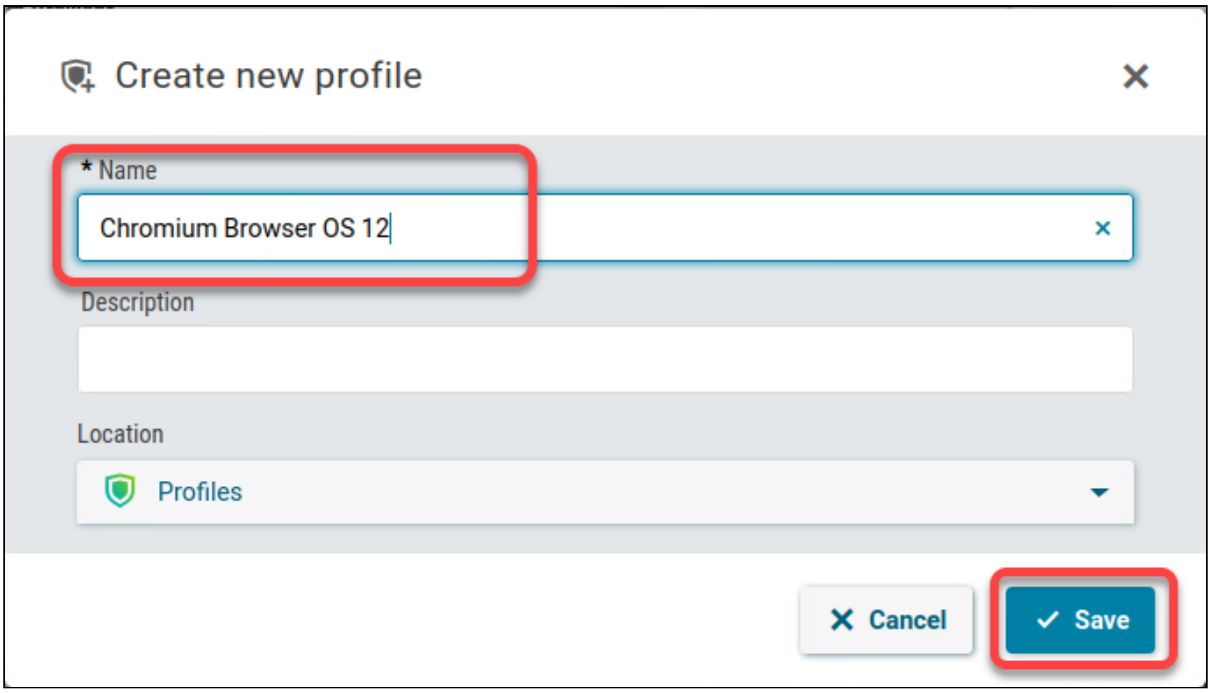


Example Profile: Chromium Browser

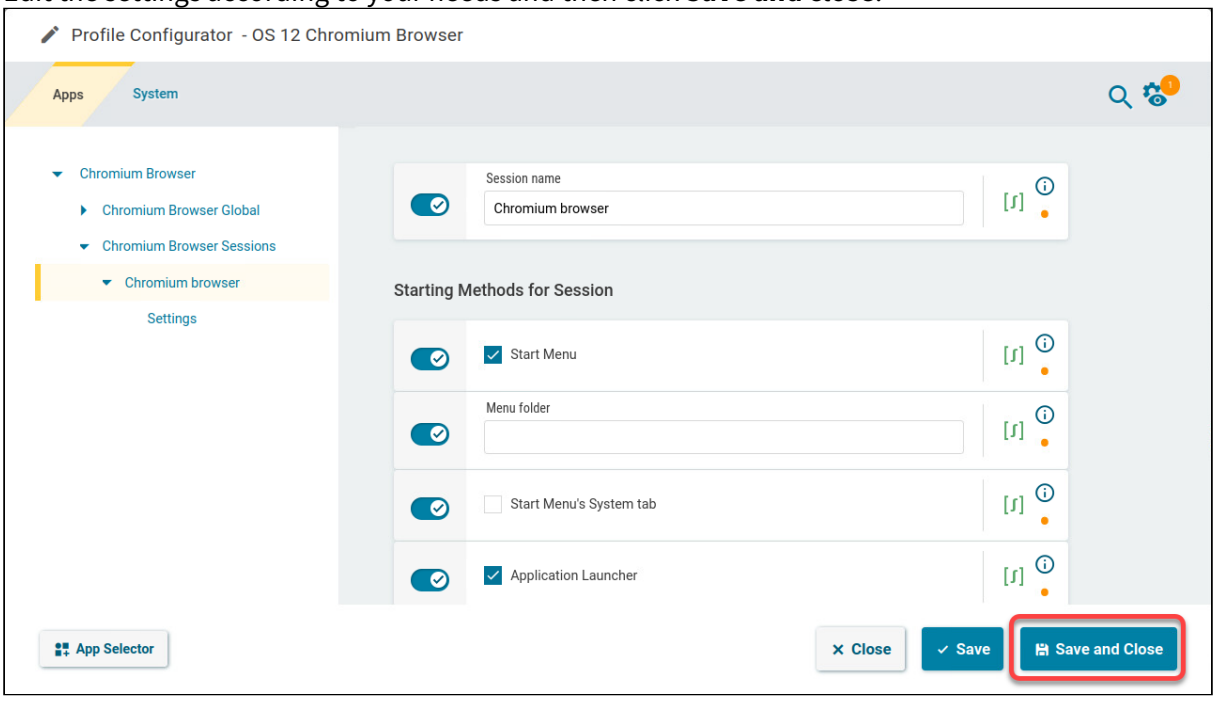
1. If the **Chromium Browser** app is not available in your UMS, import it. The process is the same as that for the Base System, see Getting IGEL OS 12 from the App Portal (see page 27).
2. In the **Apps** list, select **Chromium Browser** and then click **Create new profile**.



3. Enter a name for the profile and click **Save**.



4. Edit the settings according to your needs and then click **Save and close**.

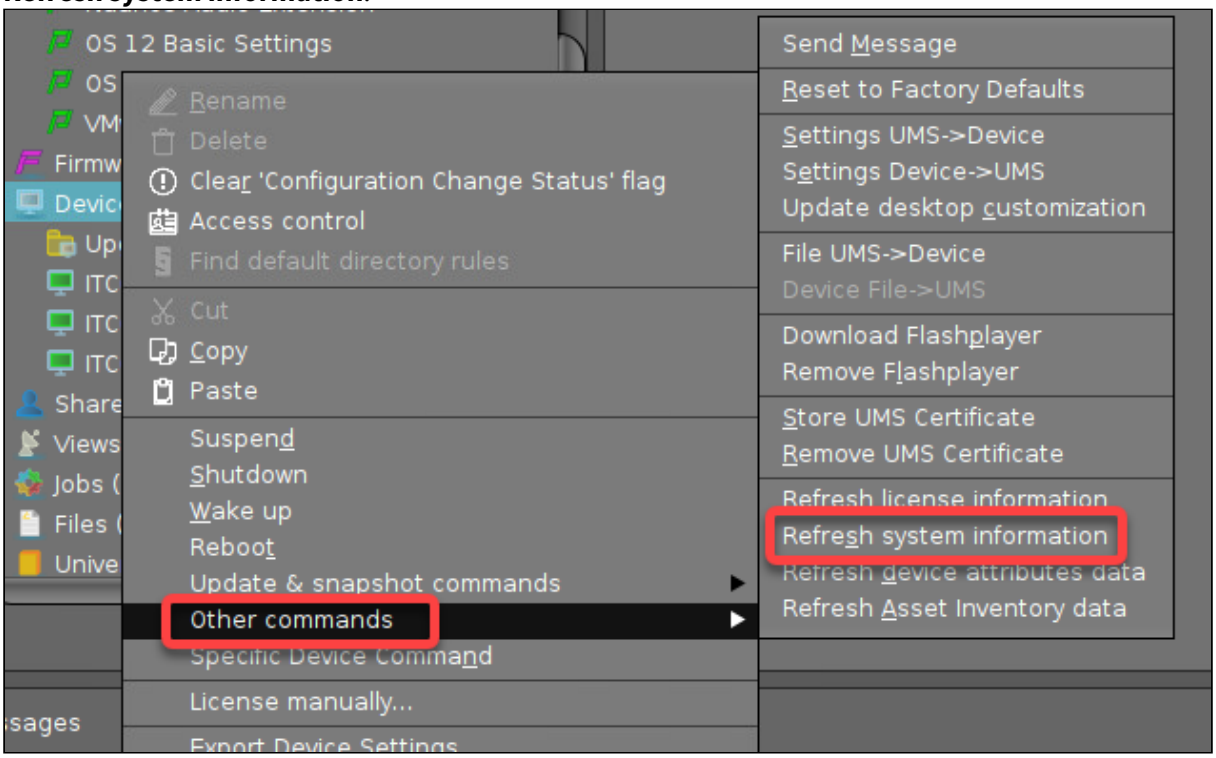


Manual Upgrade

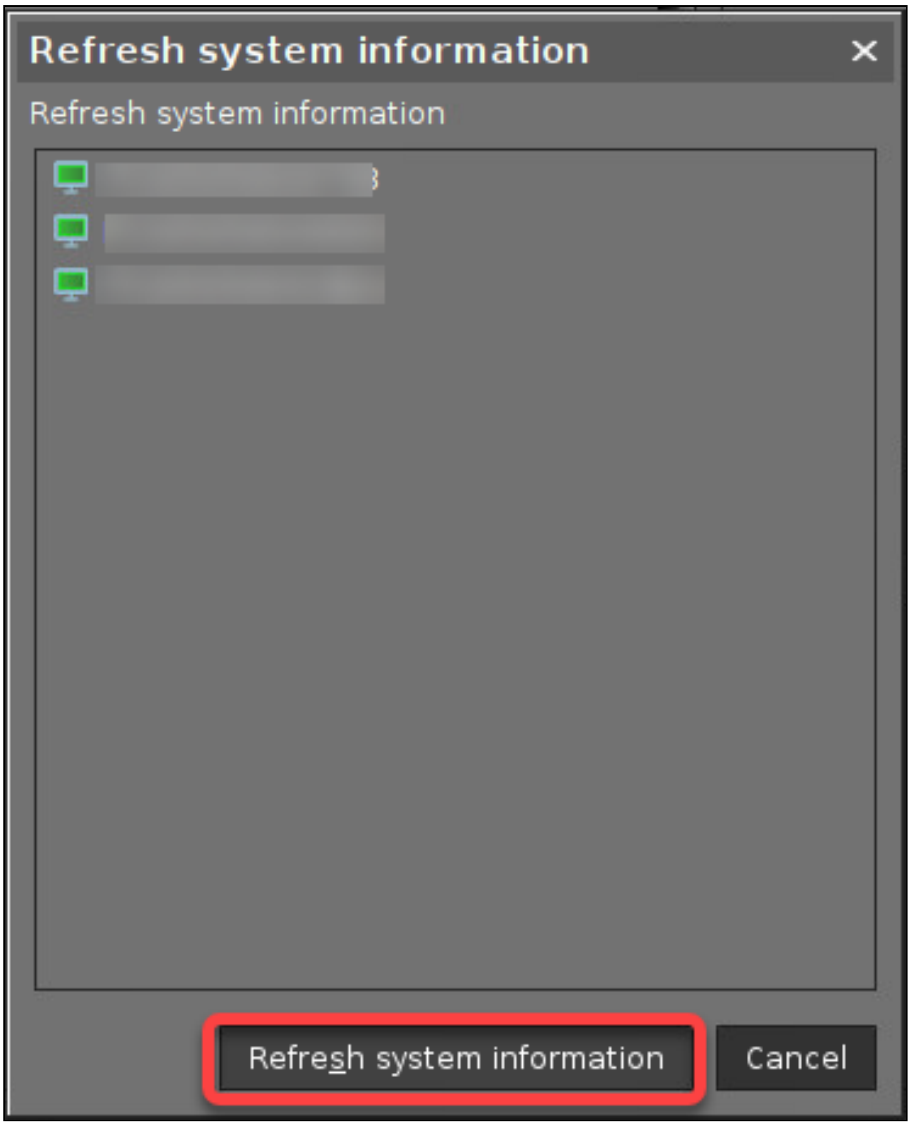
Checking for Upgradeability

In this step, we will determine if the upgradeability check on the devices has been passed. This is especially recommended when you are testing the upgrade.

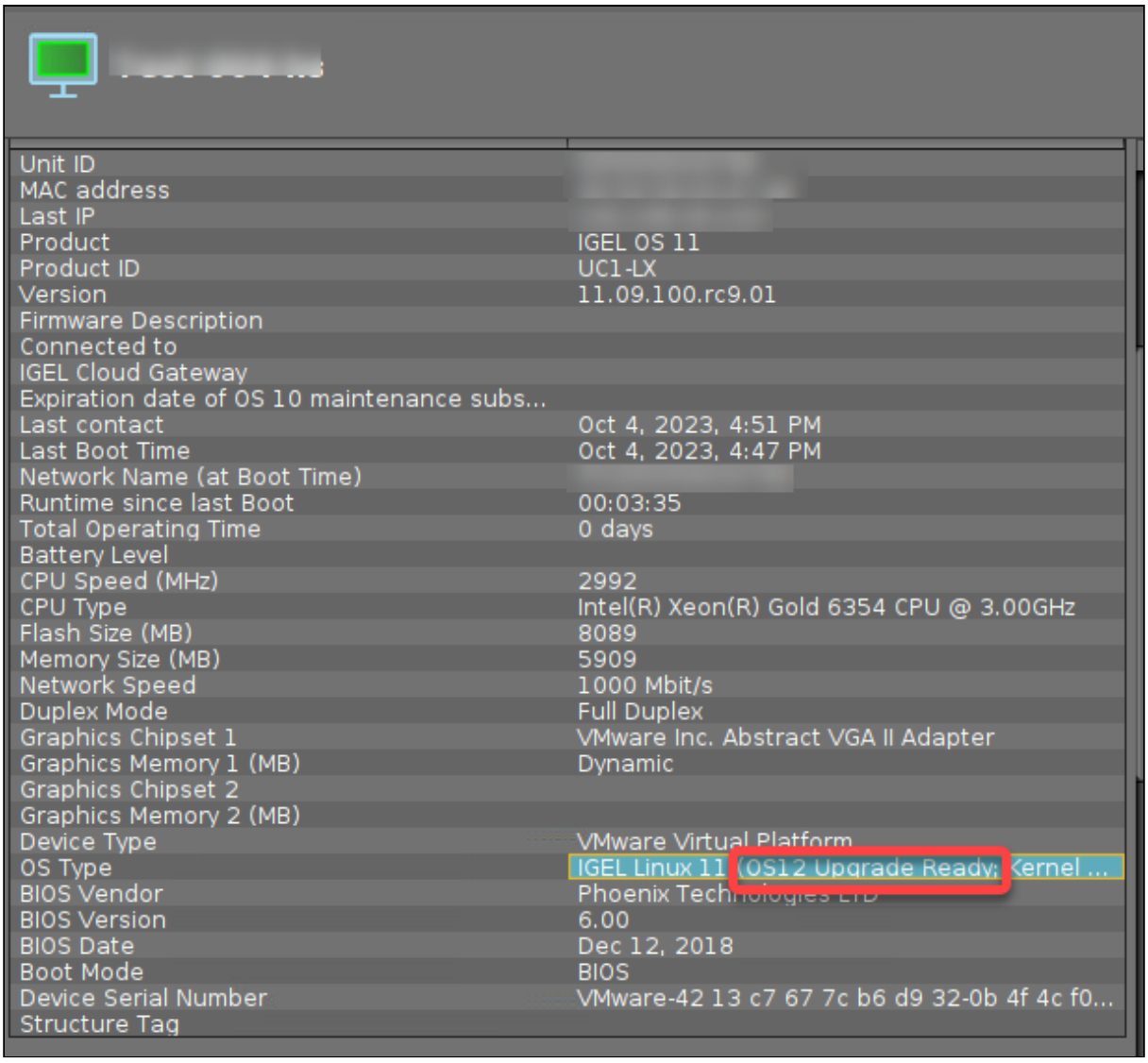
1. In the UMS Console, go to **Devices**, open the context menu, and then select **Other commands > Refresh system information**.



2. Click **Refresh system information**.



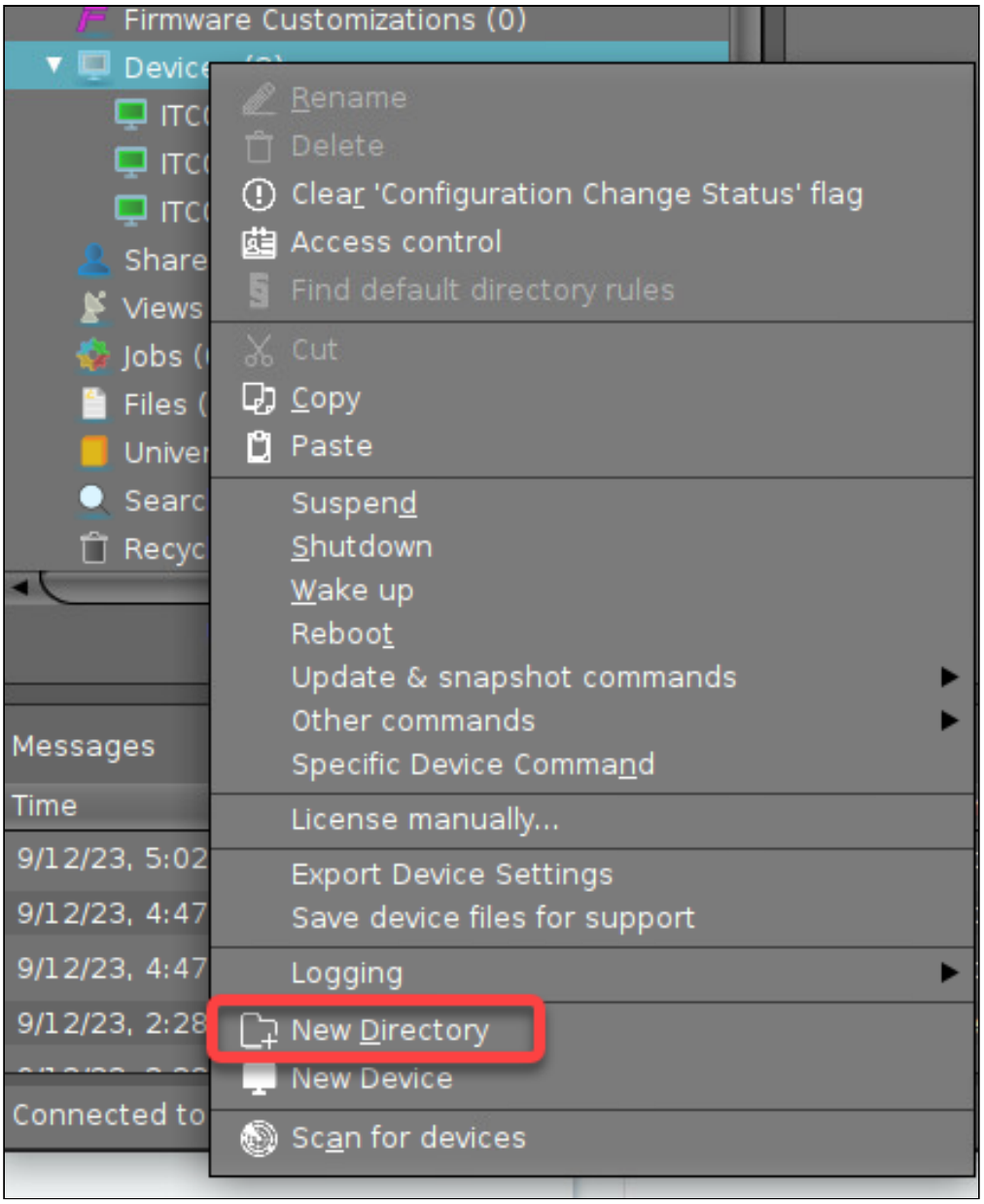
3. Select a device, look up the **Advanced System Information** section, and check if the value of **OS Type** contains the text **OS 12 Upgrade Ready**.

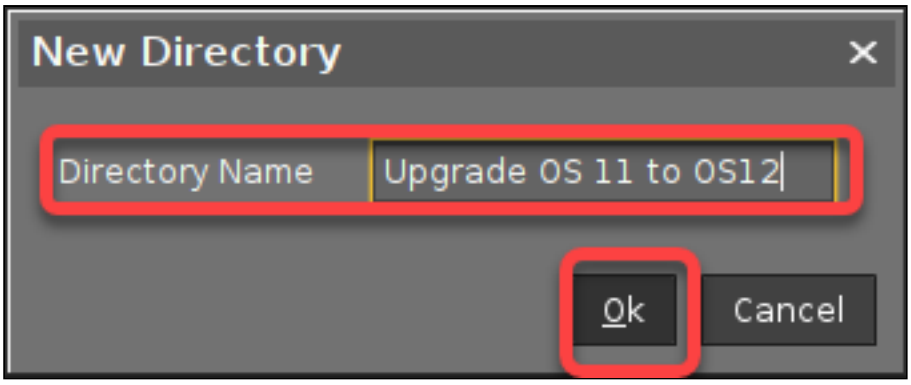


If this is the case, you can continue with the next step.

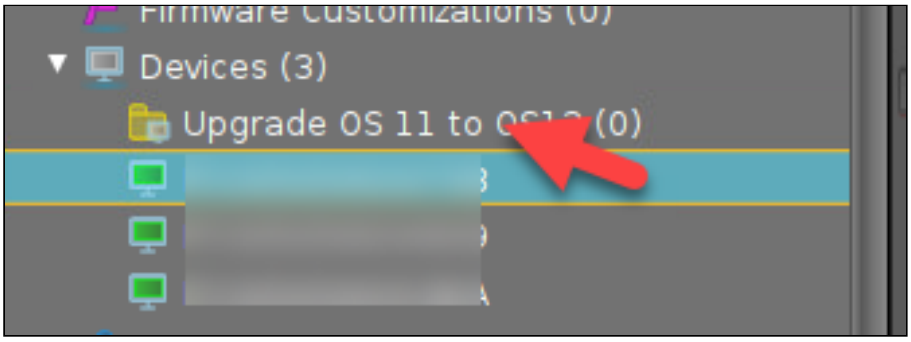
Assigning the IGEL OS 12 Profiles to the Device via a Directory

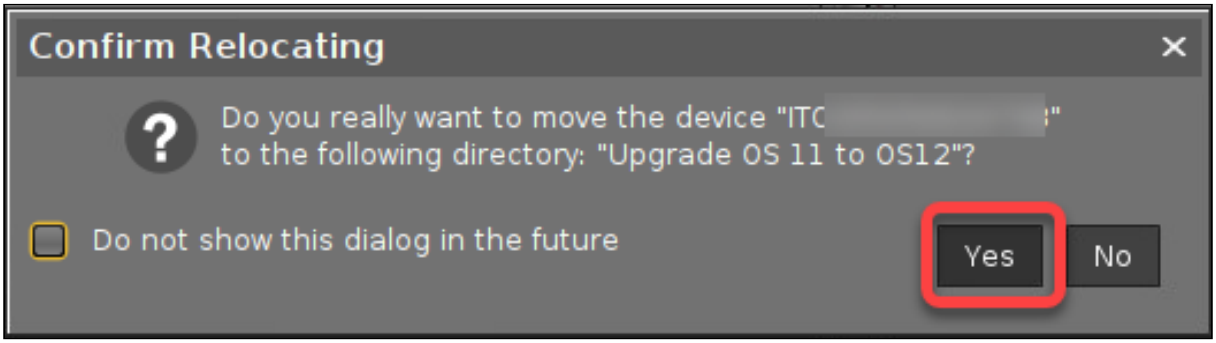
1. Create a directory for the device/devices you want to upgrade.

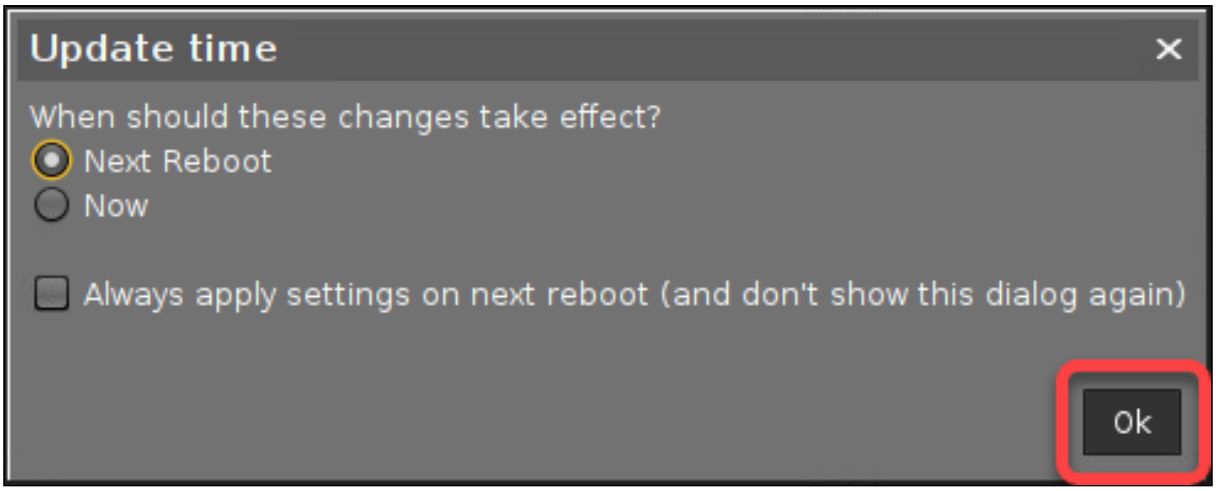

Firmware Customizations (0)
Rename
Delete
Clear 'Configuration Change Status' flag
Access control
Find default directory rules
Cut
Copy
Paste
Suspend
Shutdown
Wake up
Reboot
Update & snapshot commands
Other commands
Specific Device Command
License manually...
Export Device Settings
Save device files for support
Logging
New Directory
New Device
Scan for devices
Messages
Time
9/12/23, 5:02
9/12/23, 4:47
9/12/23, 4:47
9/12/23, 2:28
Connected to



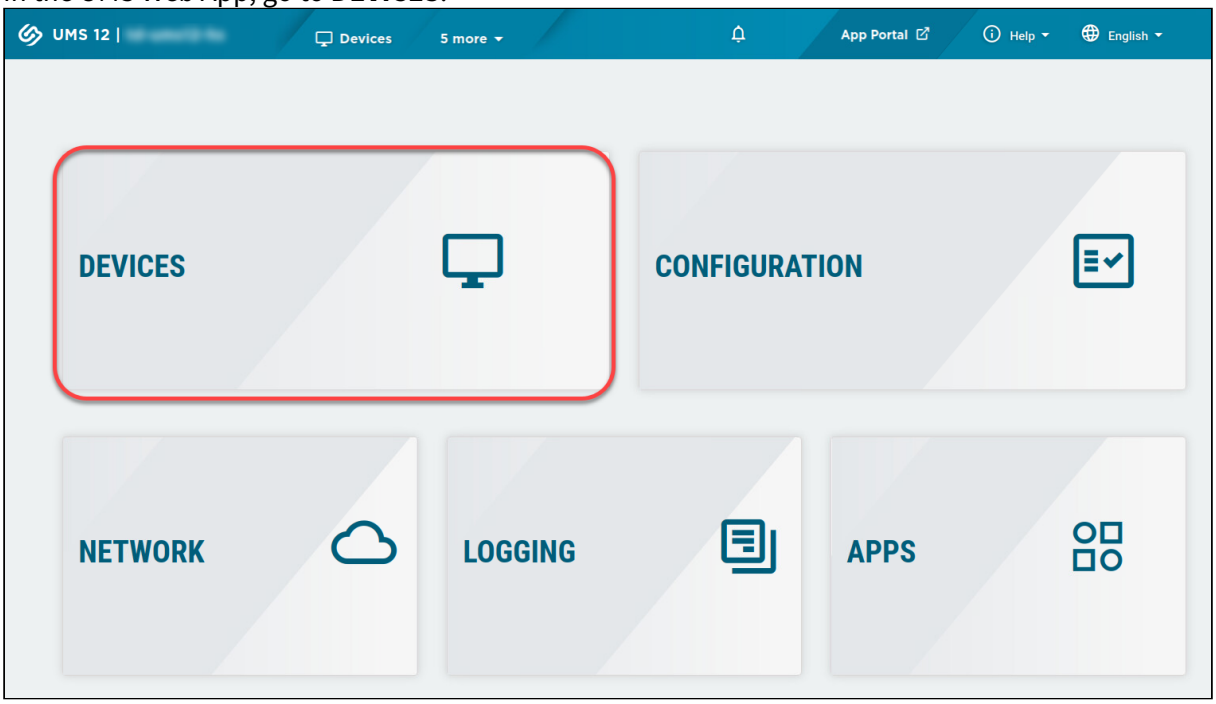
2. Put the test devices into it.



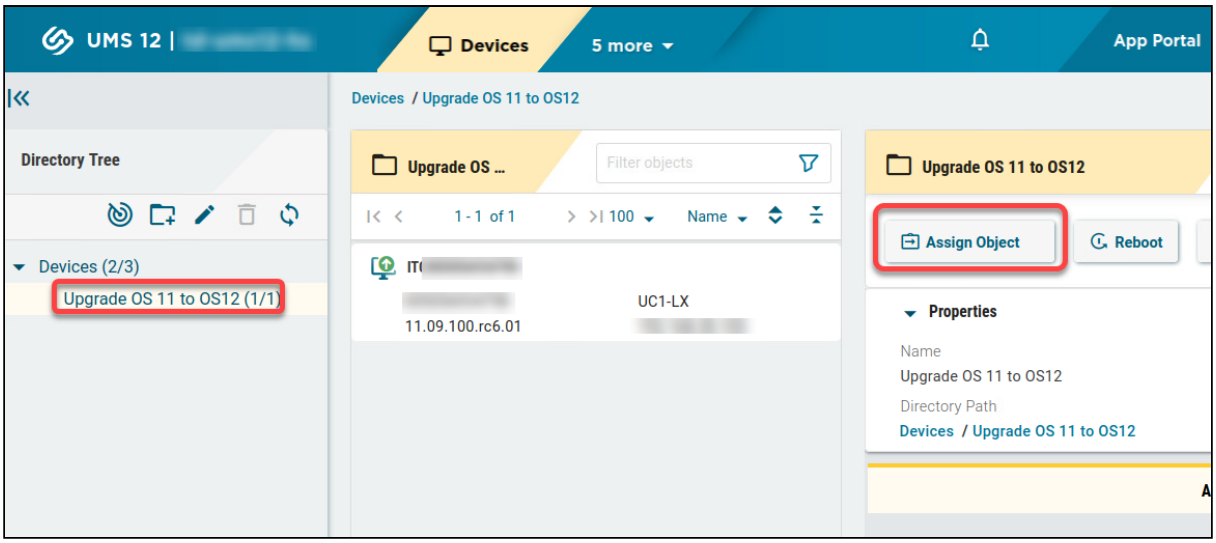




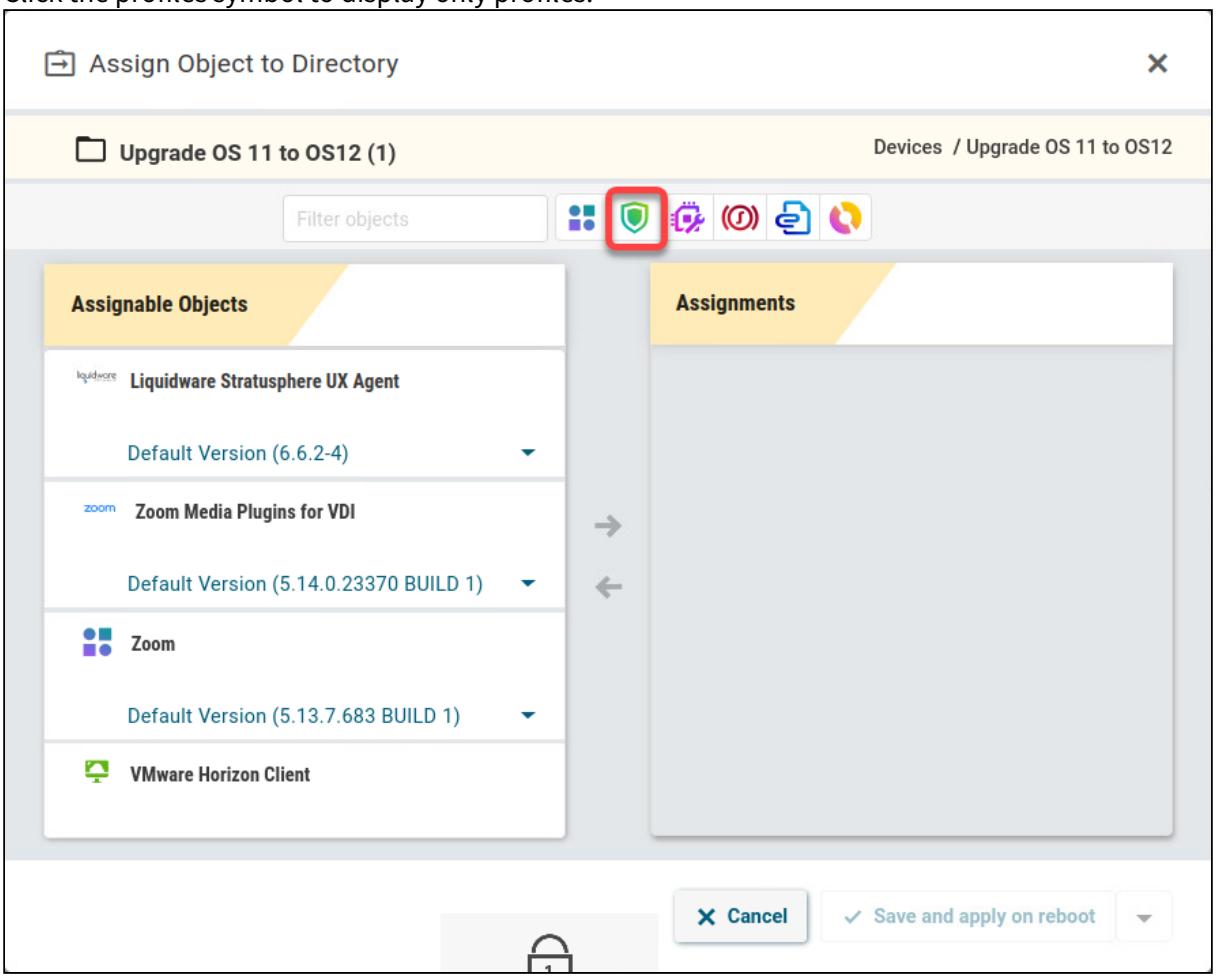
3. In the UMS Web App, go to **DEVICES**.



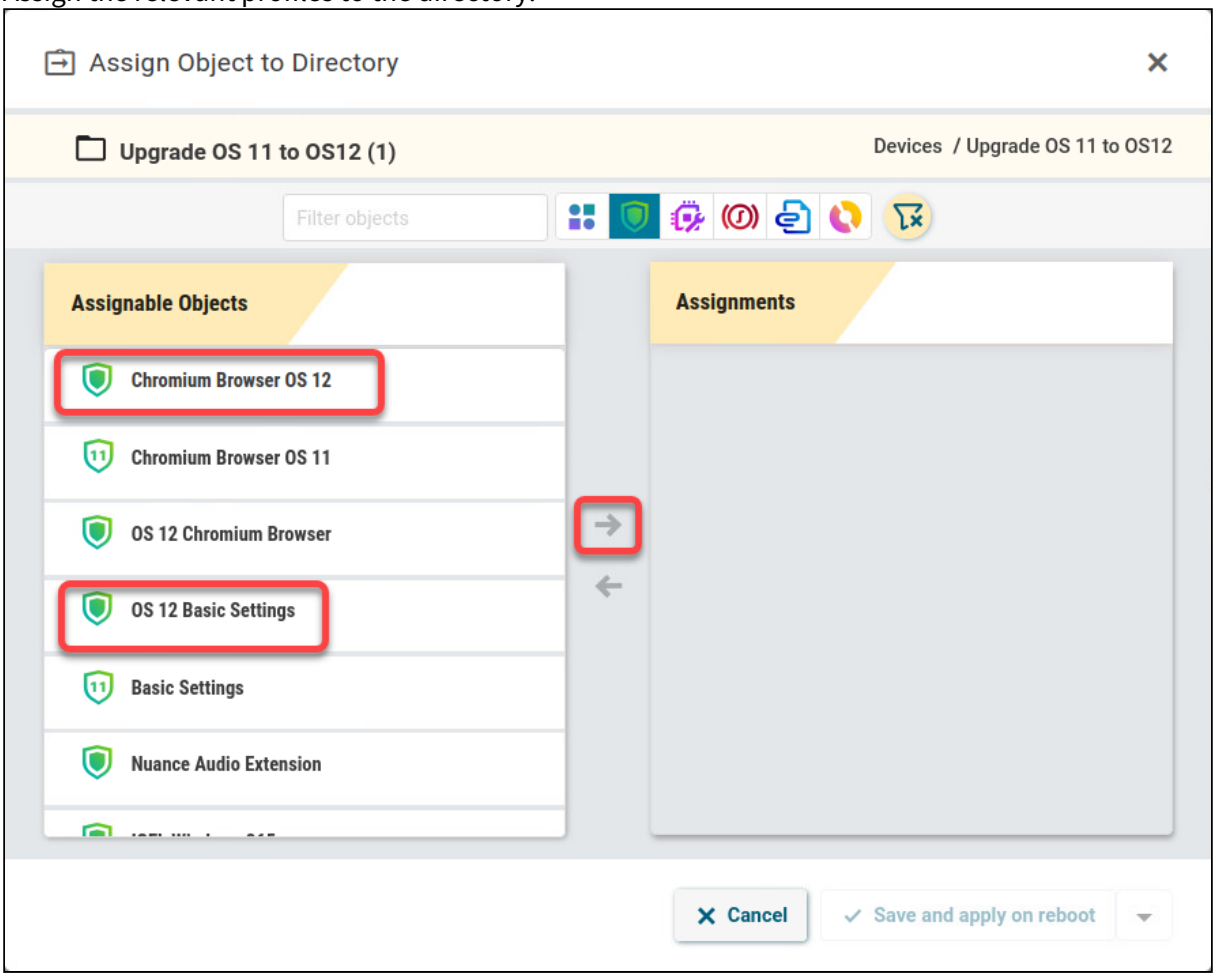
4. Select the directory you have created beforehand and click **Assign object**.

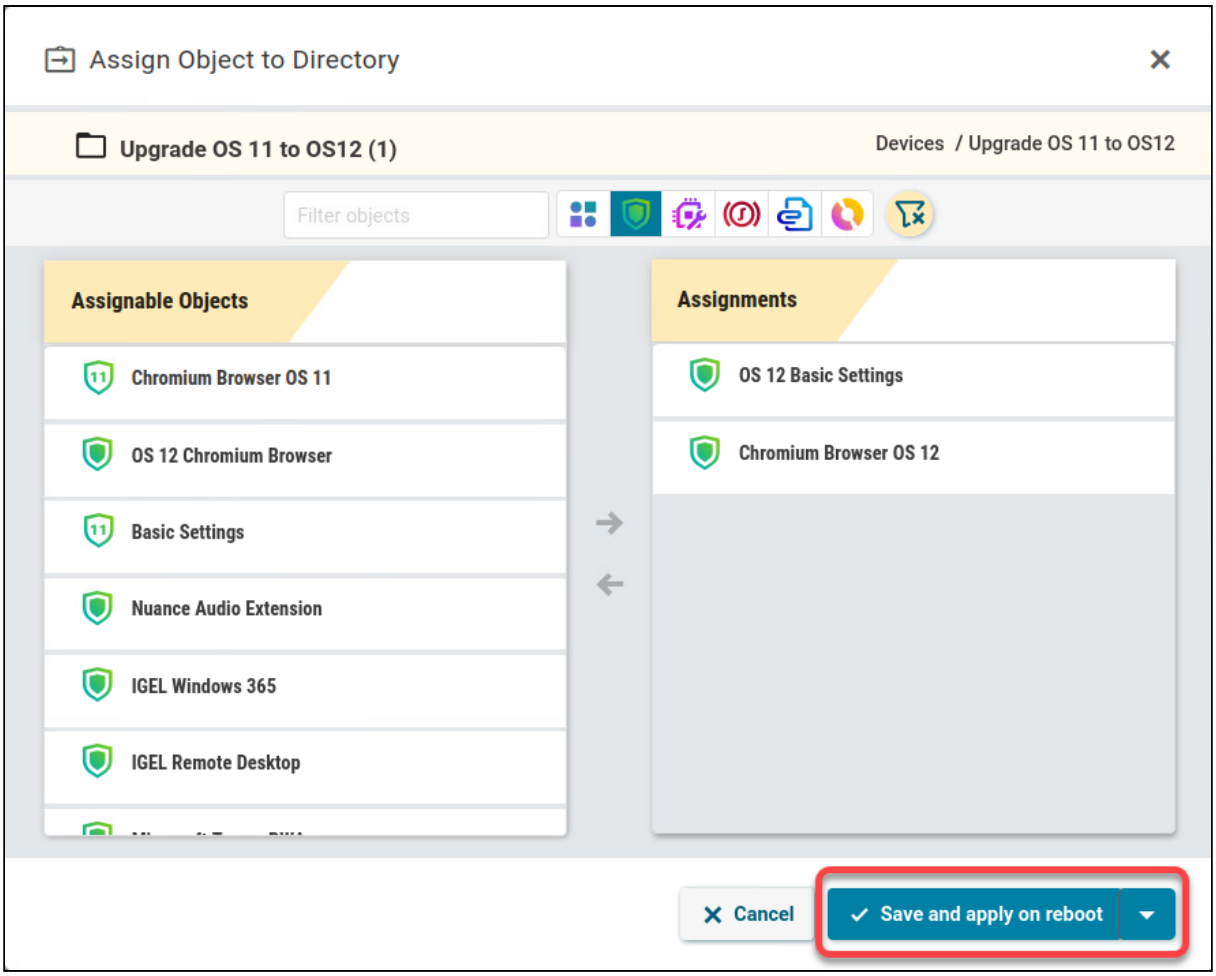


5. Click the profiles symbol to display only profiles.



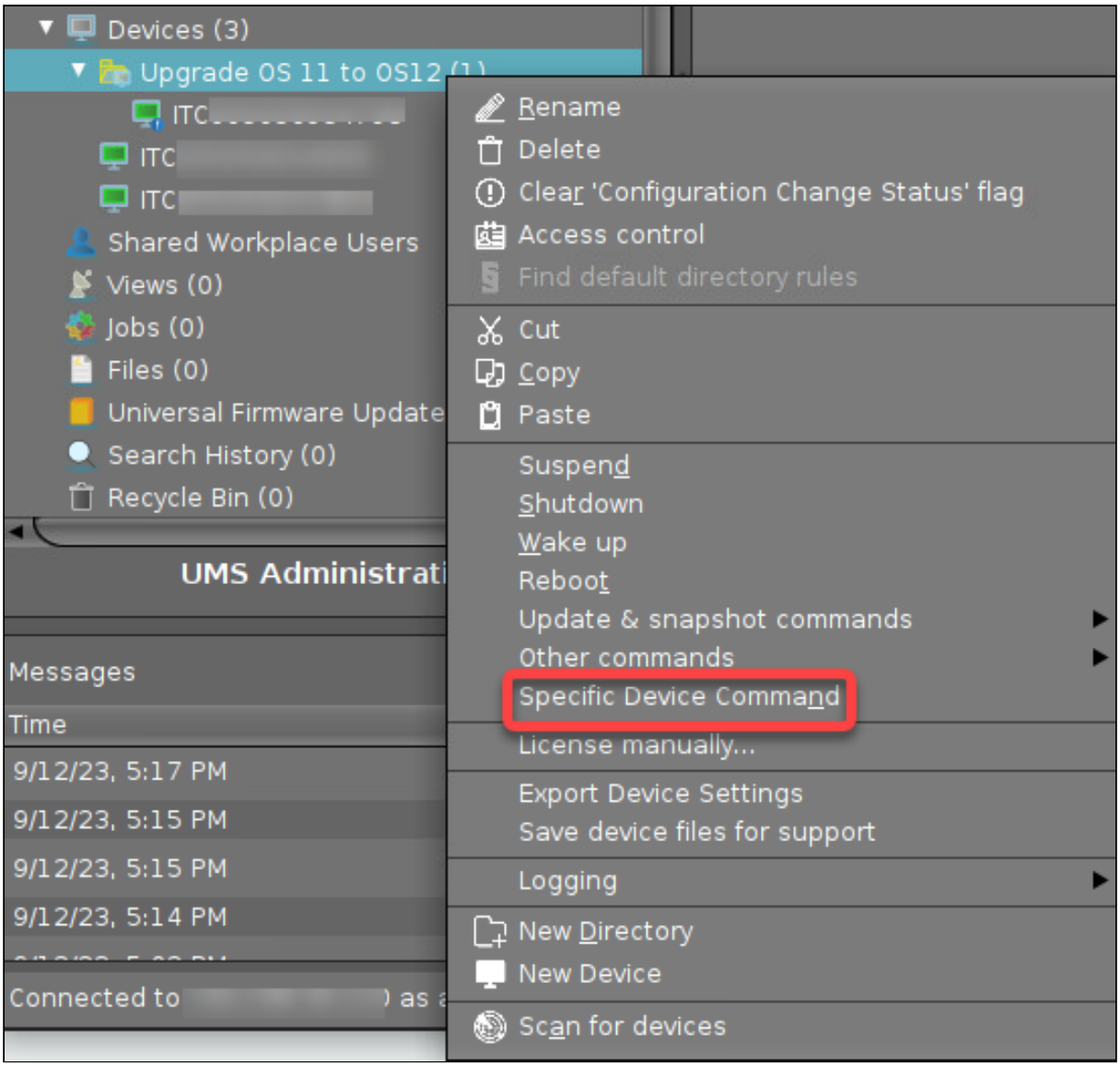
6. Assign the relevant profiles to the directory.



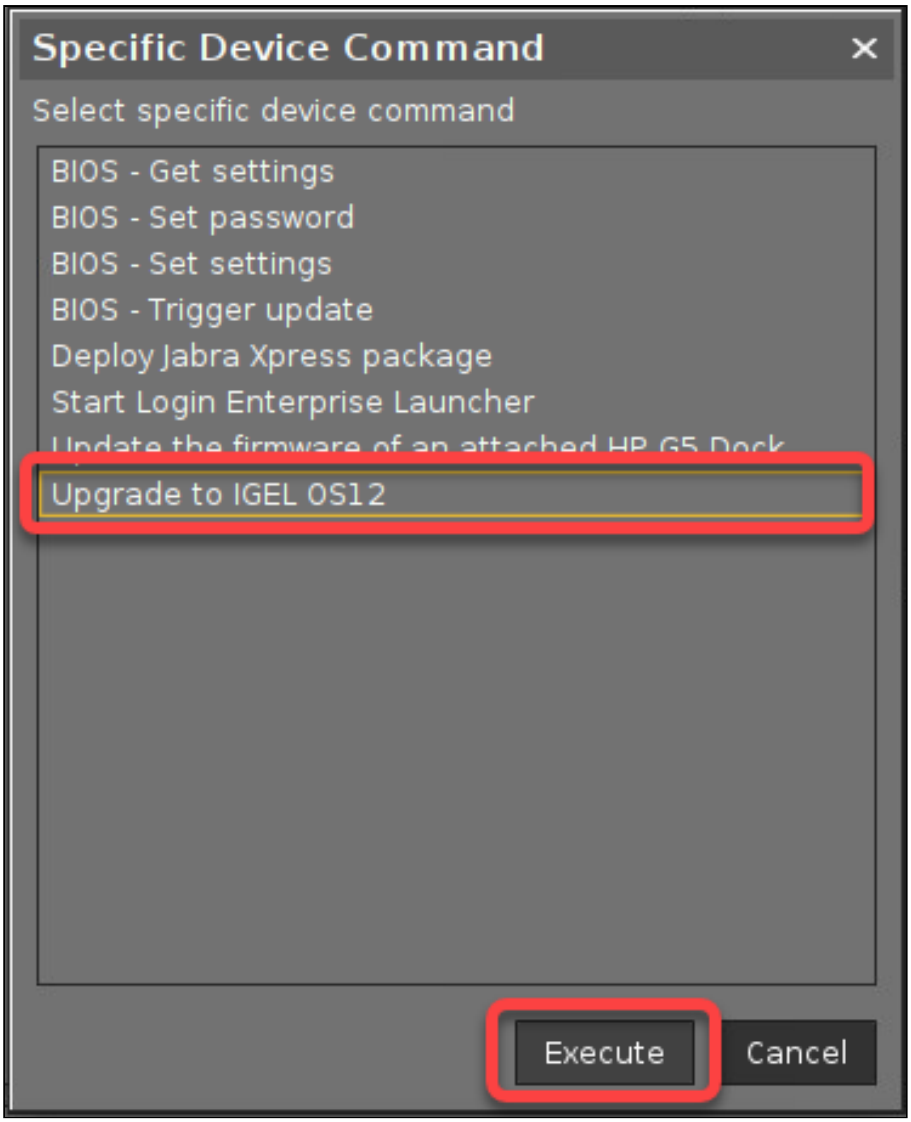


Starting the Upgrade

1. In the UMS Console, open the context menu on our upgrade directory and select **Specific Device Command**.



2. Select **Upgrade to IGEL OS 12** and click **Execute**.



After a few reboots, the upgrade is complete, including the newly installed apps. No user interaction is necessary because all dialogs that are displayed during the update process have a timeout.

Unattended Upgrade

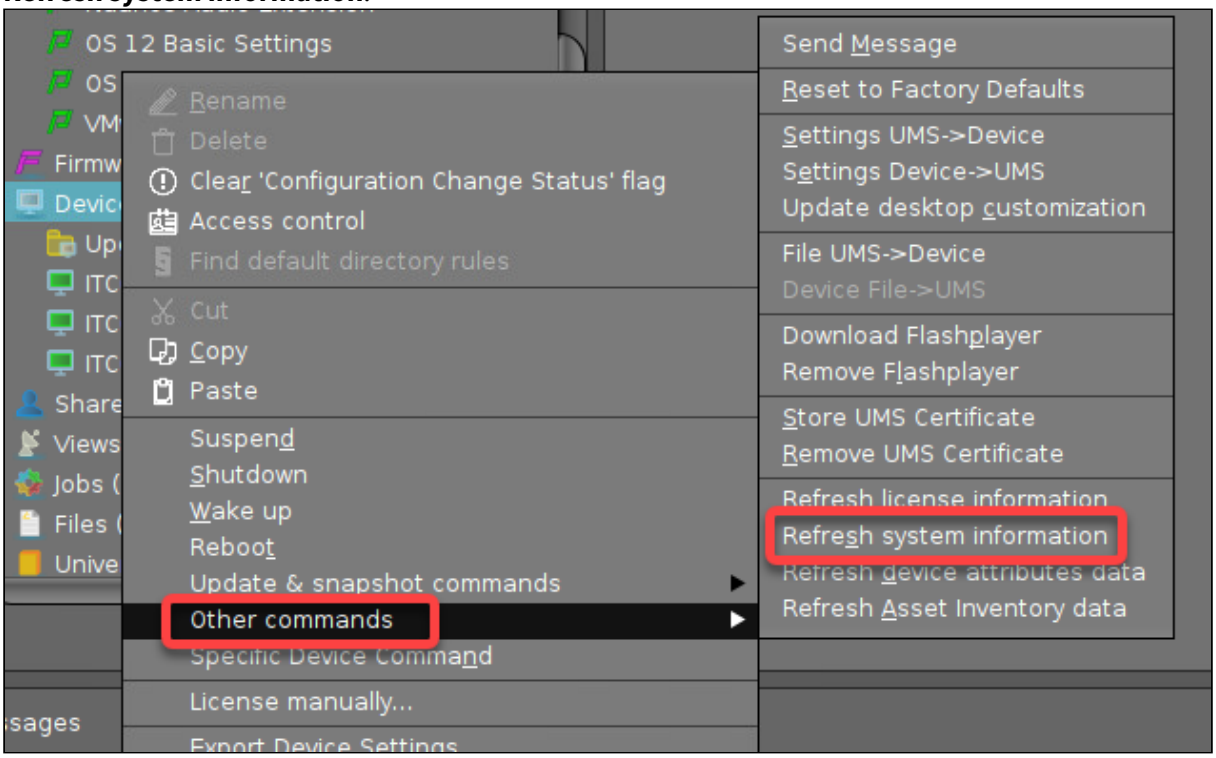
To upgrade your devices without disrupting your users, you can use the automation facilities of the UMS to upgrade your devices overnight or over the weekend, for instance.

We will create a search that covers all devices on which the upgradeability test has been passed. Afterward, we create a scheduled job that issues the upgrade command to all these devices.

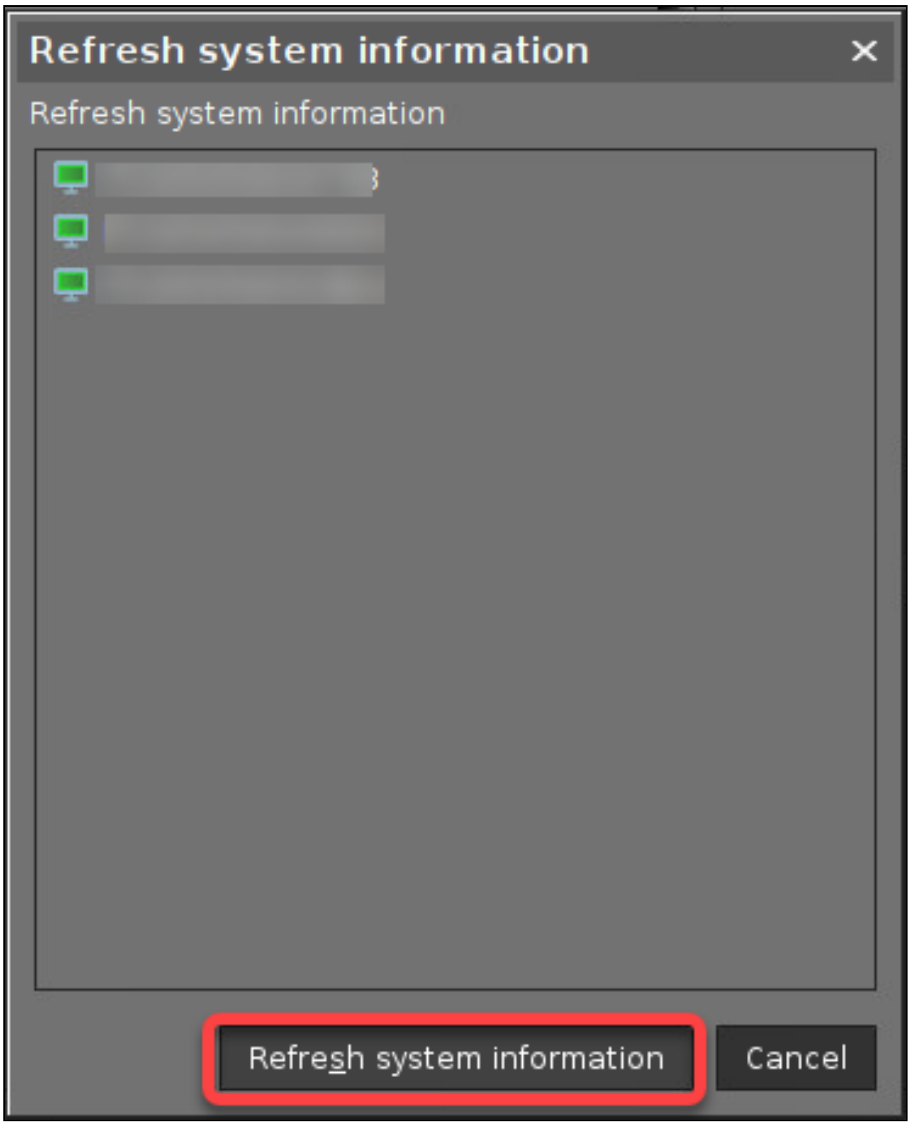
Refreshing the System Information

To make sure that all upgradeable devices present their status to the UMS, we refresh the system information manually.

1. In the UMS Console, go to **Devices**, open the context menu and then select **Other commands > Refresh system information**.

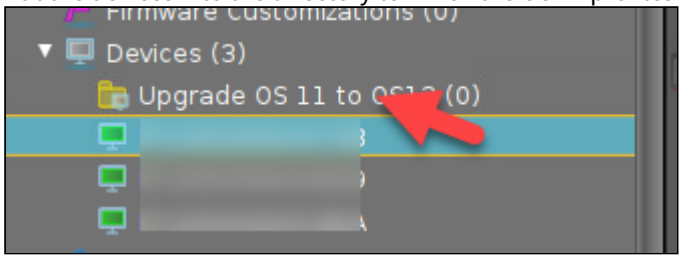


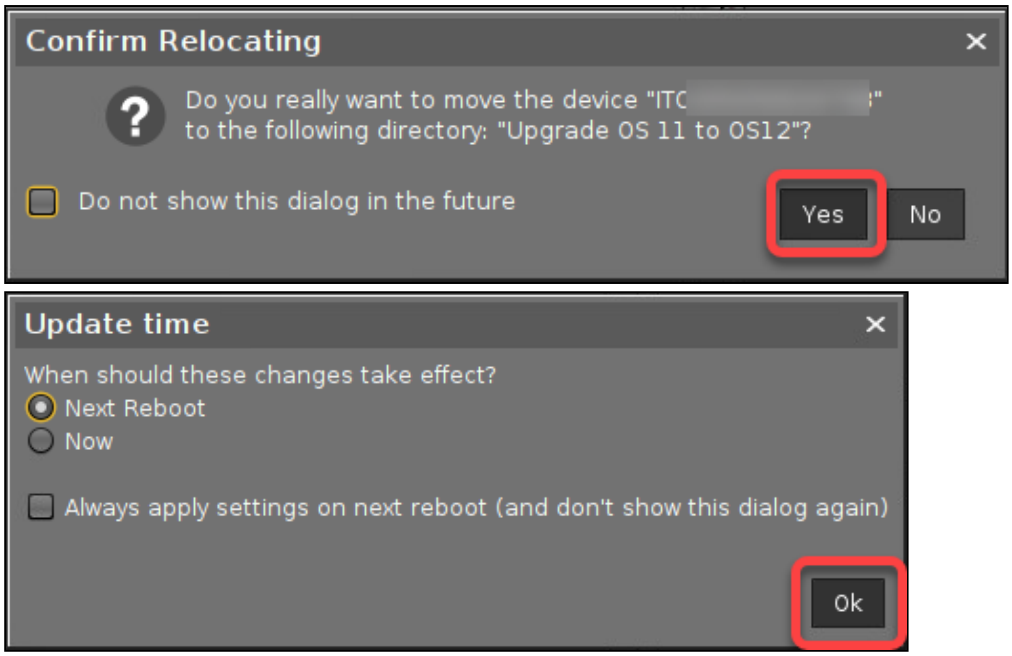
2. Click **Refresh system information**.



Assigning the IGEL OS 12 Profiles to the Device via Directory

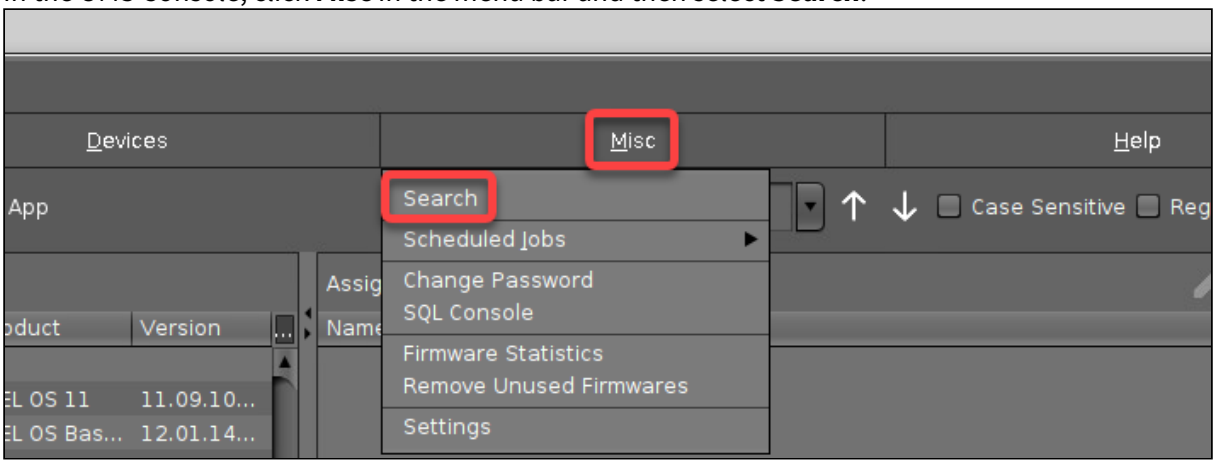
Put the devices into the directory to which the OS 12 profiles have been assigned.



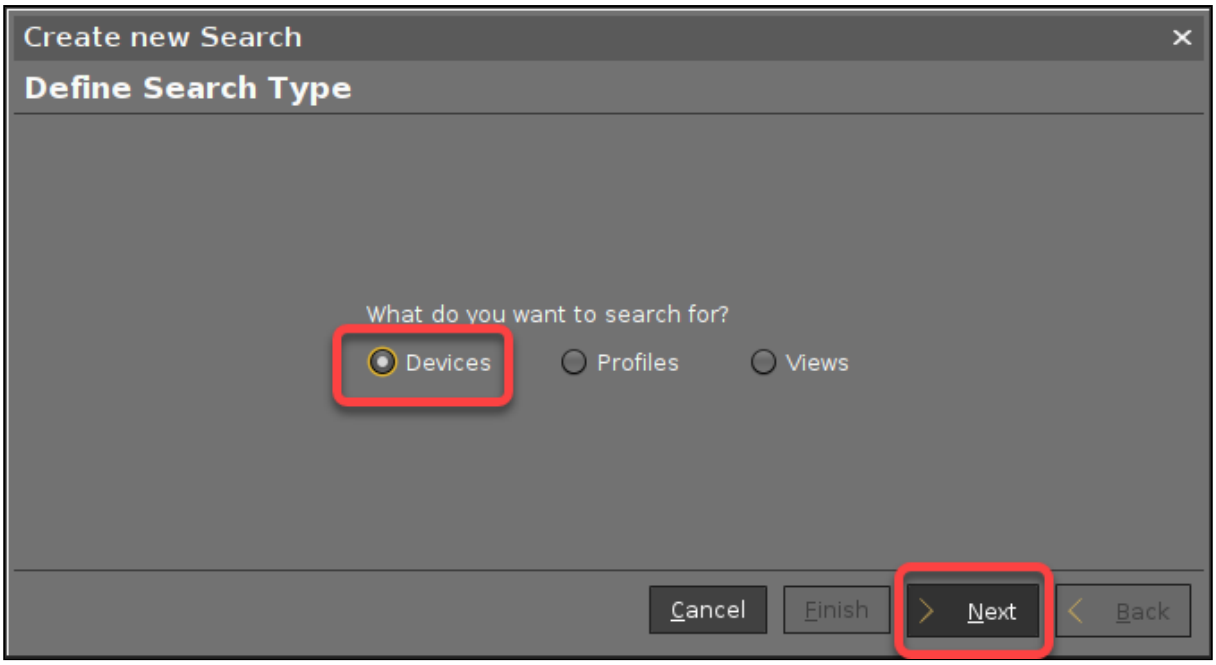


Creating the Search

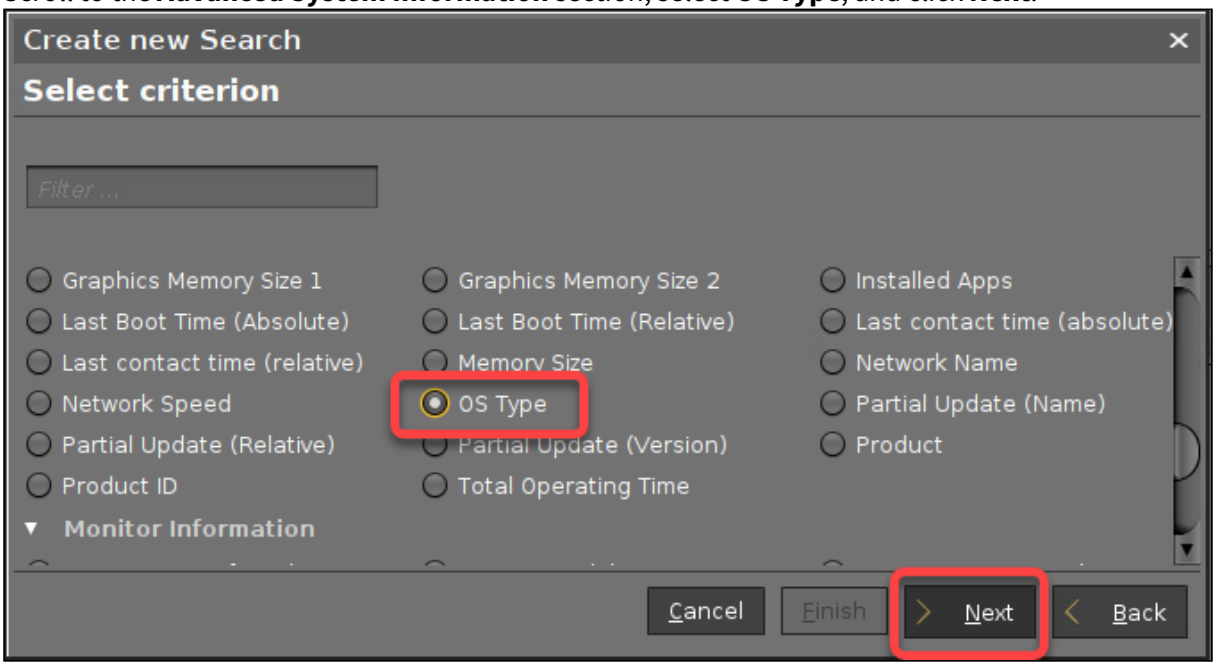
1. In the UMS Console, click **Misc** in the menu bar and then select **Search**.



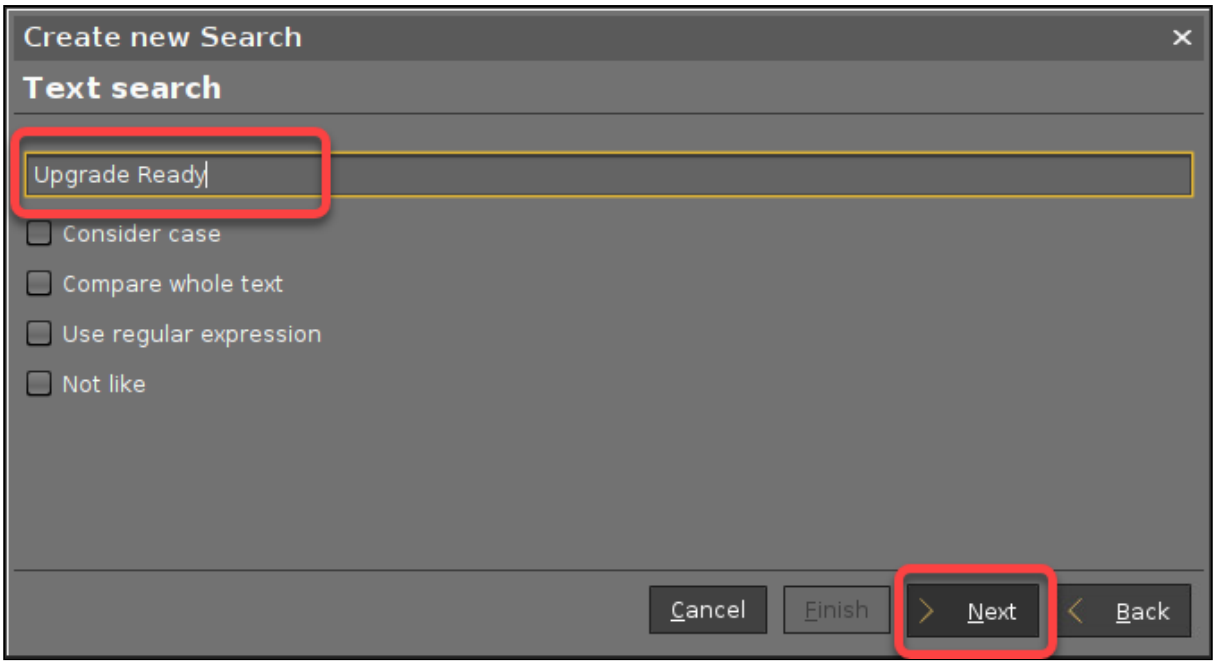
2. Make sure that **Devices** is selected and click **Next**.



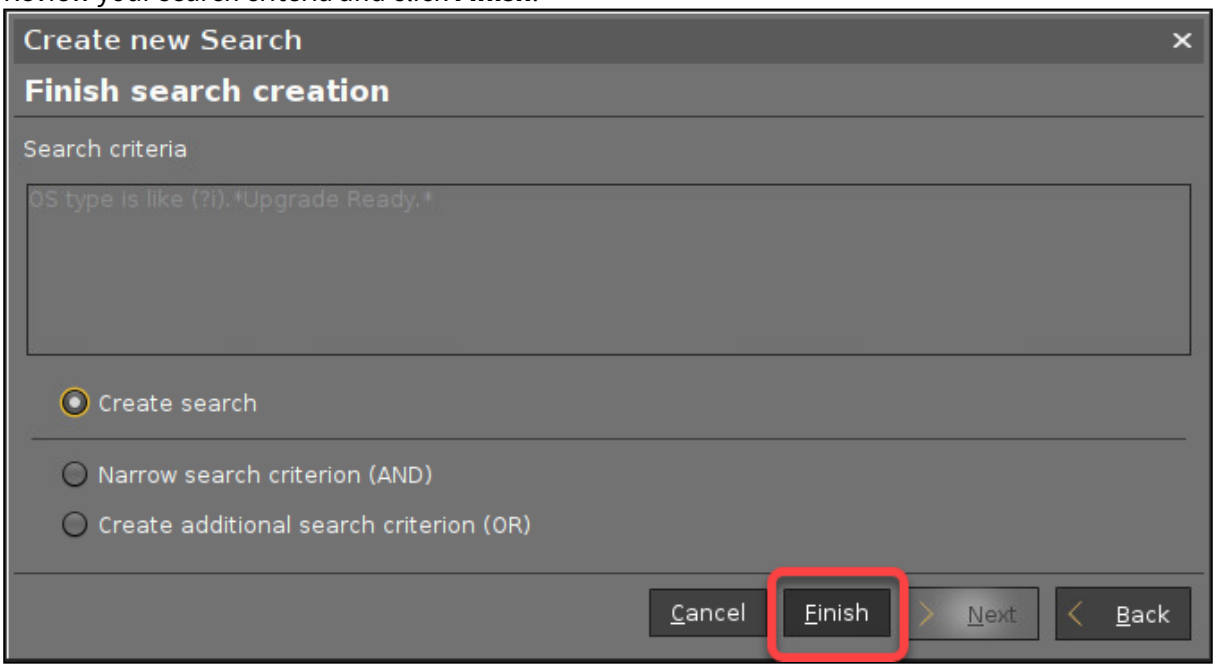
3. Scroll to the **Advanced System Information** section, select **OS Type**, and click **Next**.



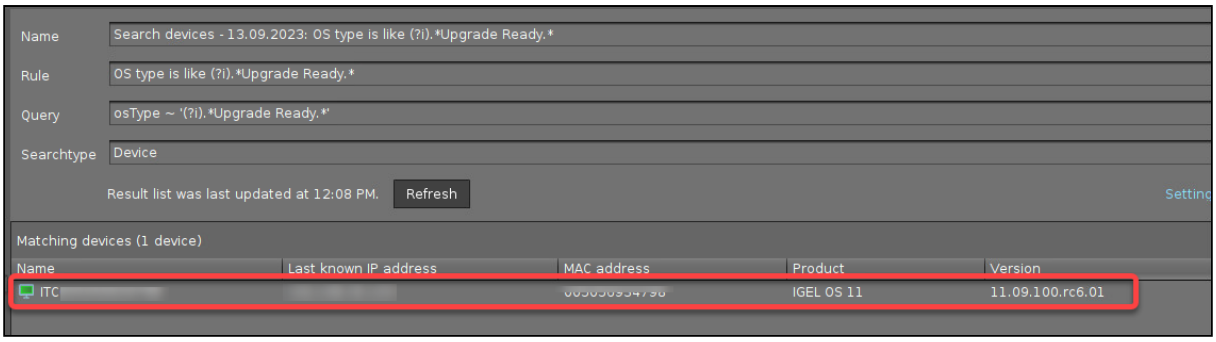
4. As the search text, enter "Upgrade Ready" and click **Next**.



5. Review your search criteria and click **Finish**.

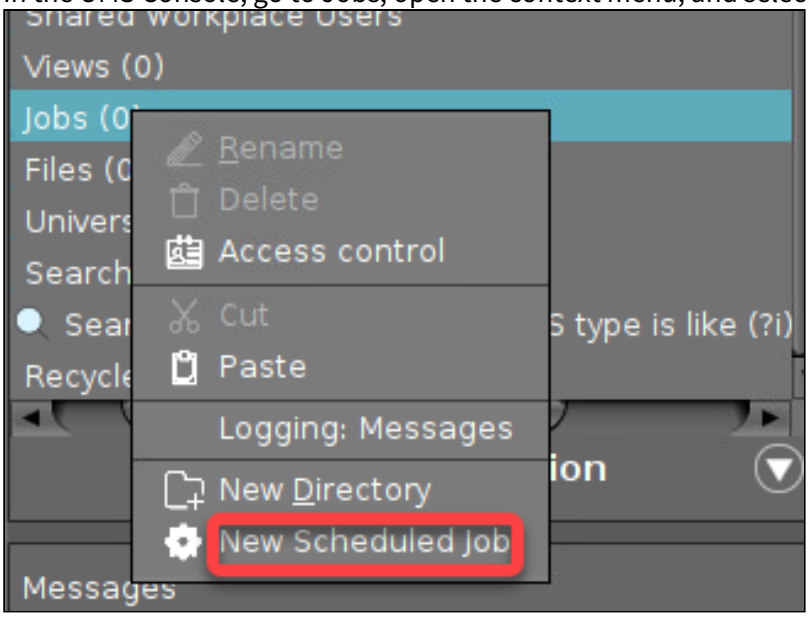


6. The devices that are considered upgradeable are displayed.

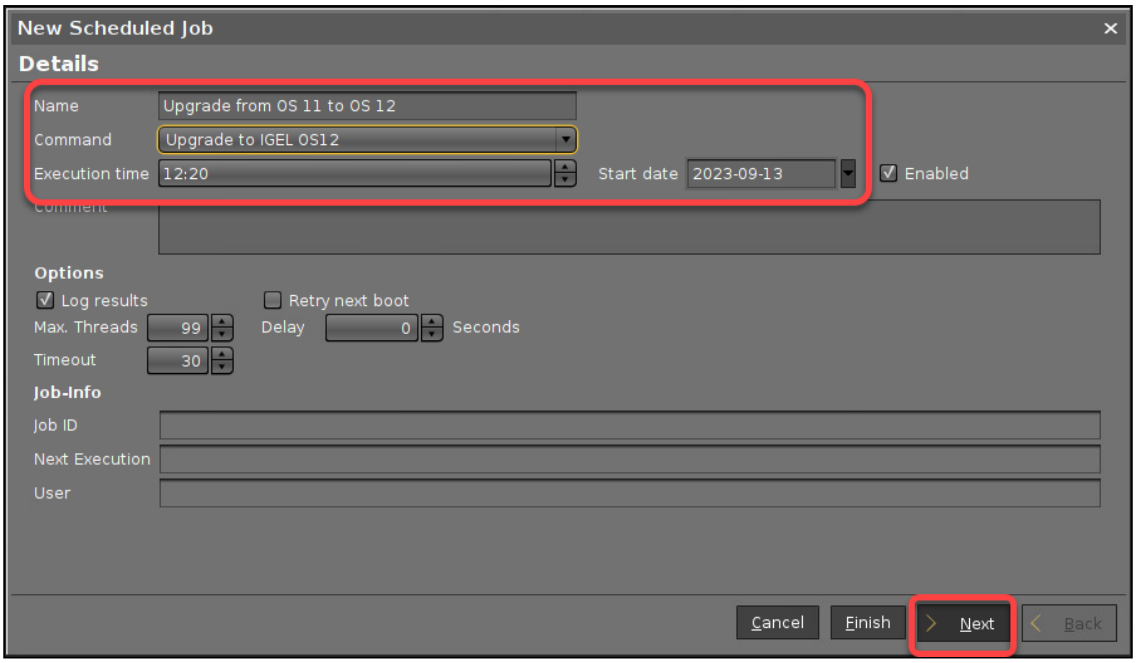


Creating the Scheduled Job

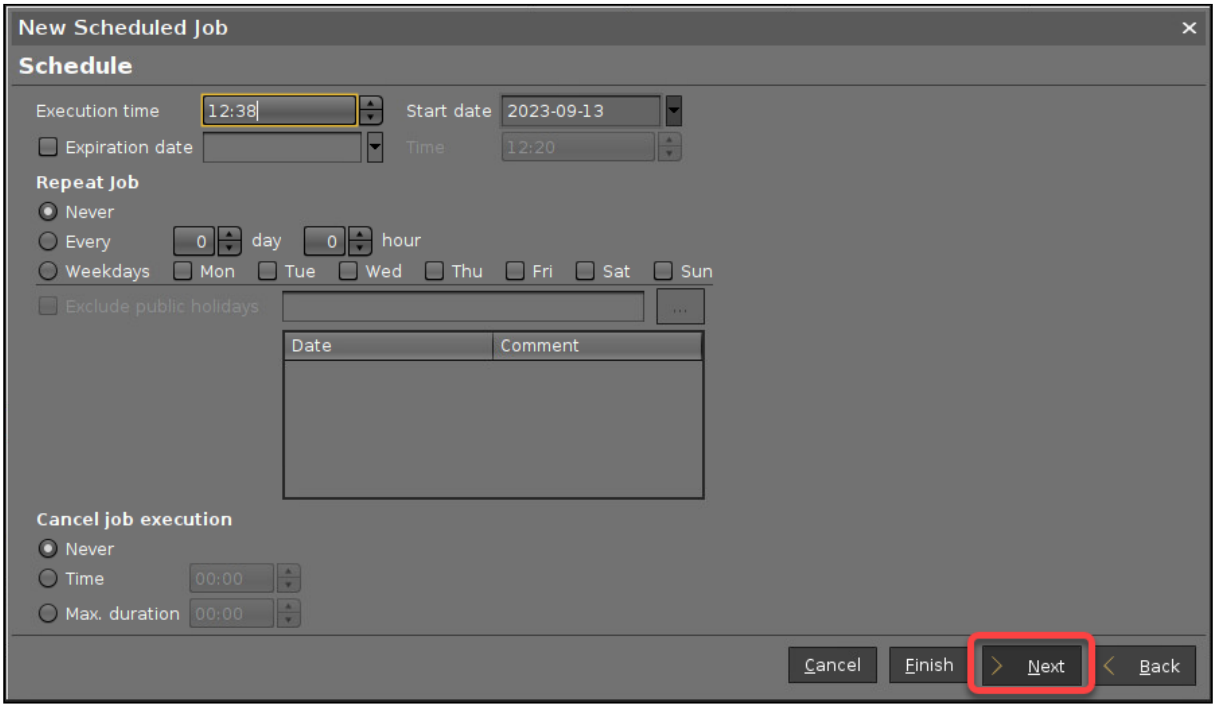
1. In the UMS Console, go to Jobs, open the context menu, and select **New Scheduled Job**.



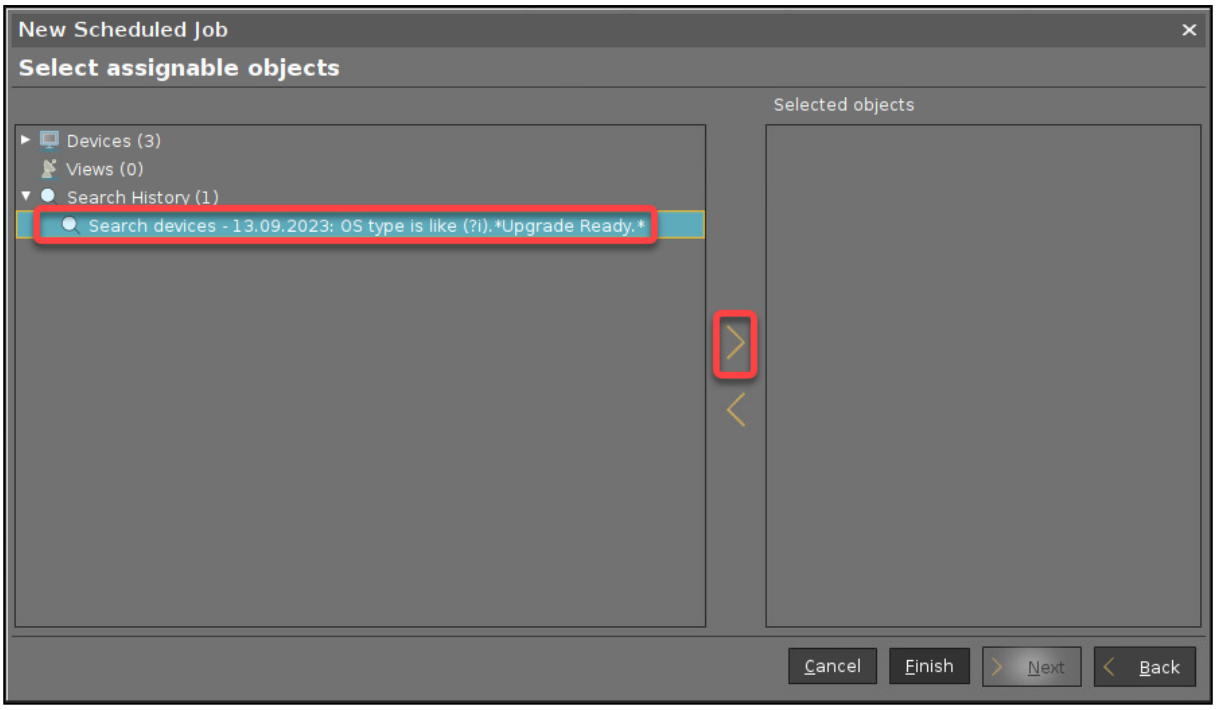
2. Enter the following data and then click **Next**:
   - **Name**: An appropriate name for the job
   - **Command**: **Select Upgrade to IGEL OS 12**.
   - **Execution time**: The time at which the job is to be executed
   - **Start date**: The date on which the job is to be executed

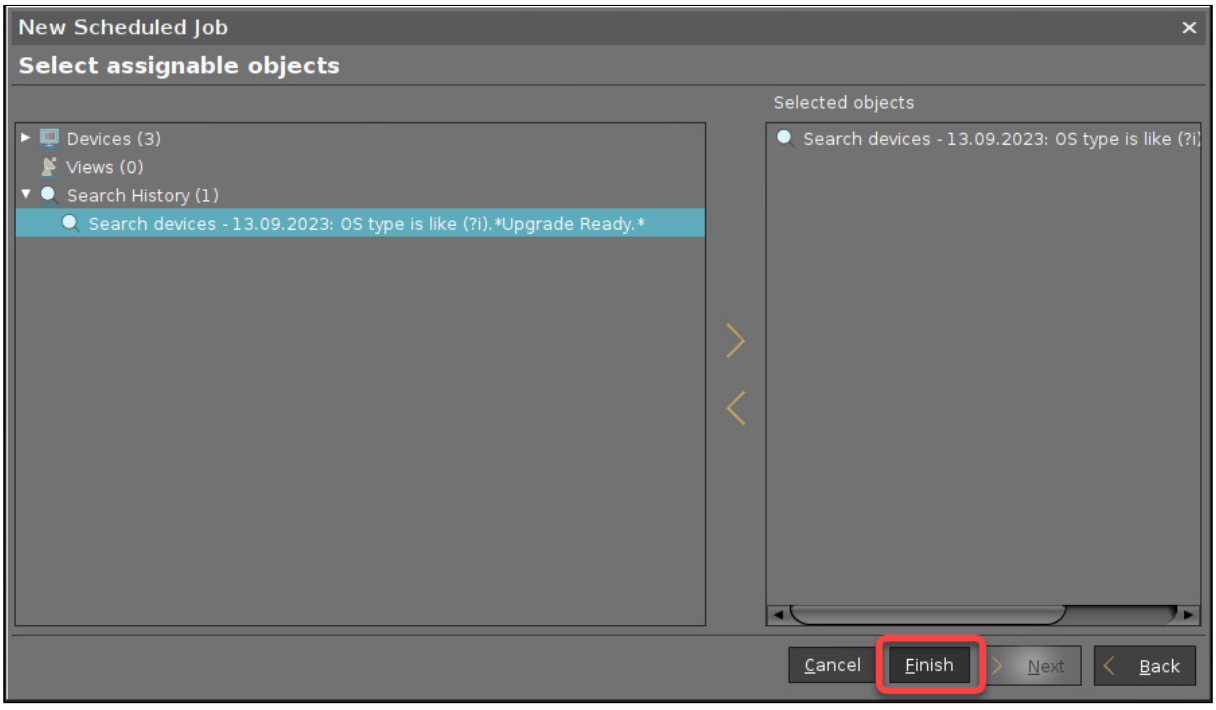


3. Review the data and click **Next**.

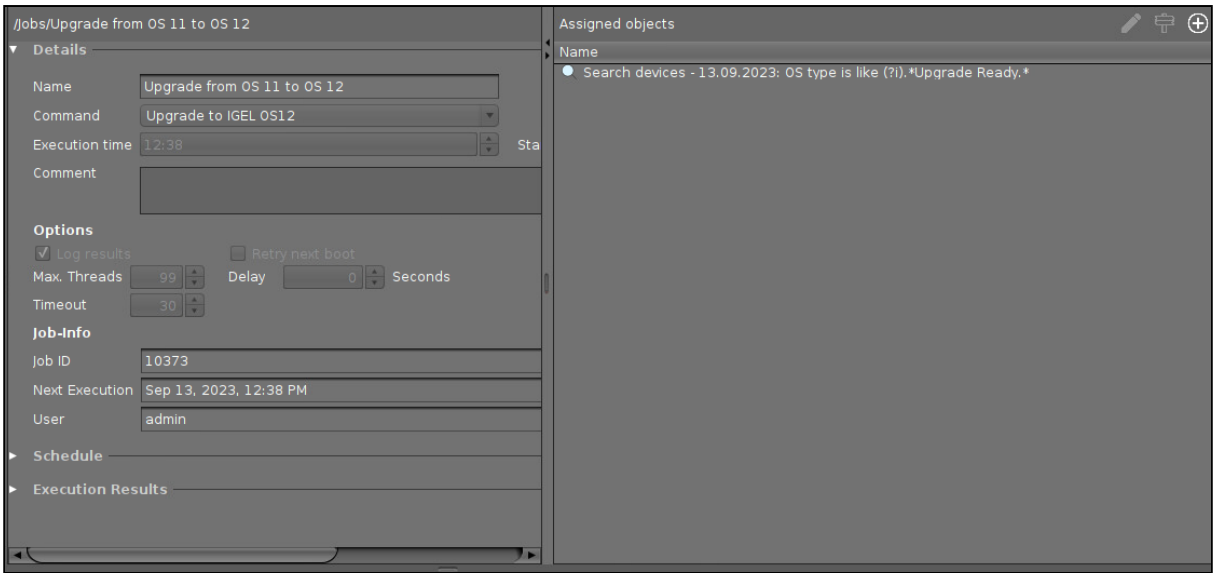


4. Assign the search we have created before to this job and click **Finish**.





The scheduled job is displayed. It will be executed at the defined time and date.



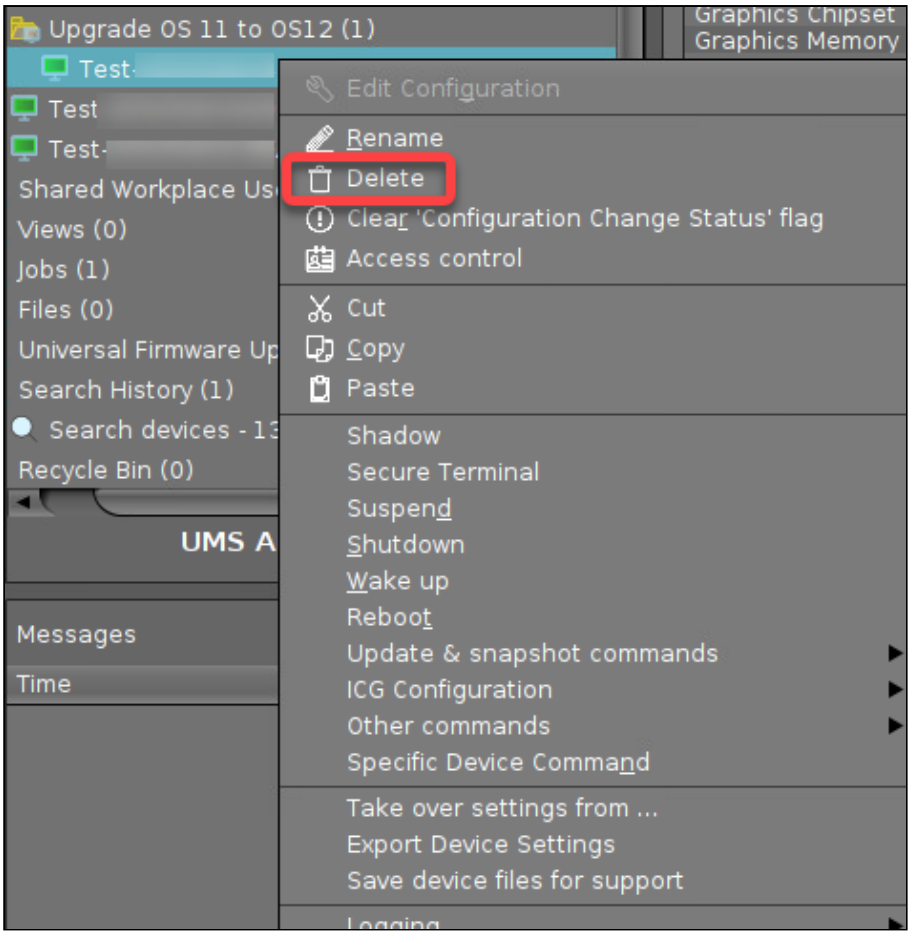
When the job is executed, the devices are upgraded, which includes the installation of the configured apps. No user interaction is necessary because all dialogs that are displayed during the update process have a timeout.

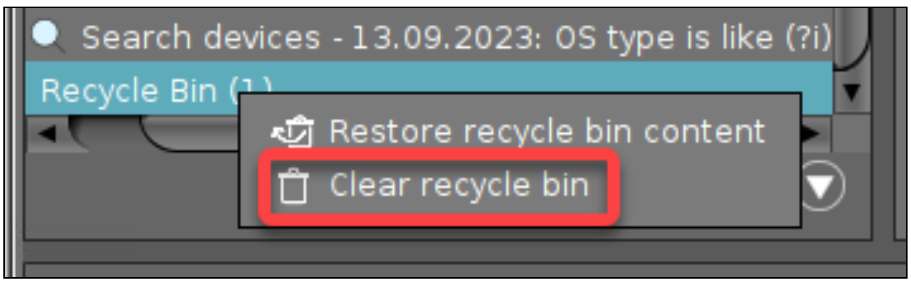
Workaround: What to Do If the EULA State is "Not Needed"

When the **EULA State** of your target version of IGEL OS 12 is **Not needed**, you must ensure that it gets changed to **Accepted**.

To achieve this, proceed as follows:

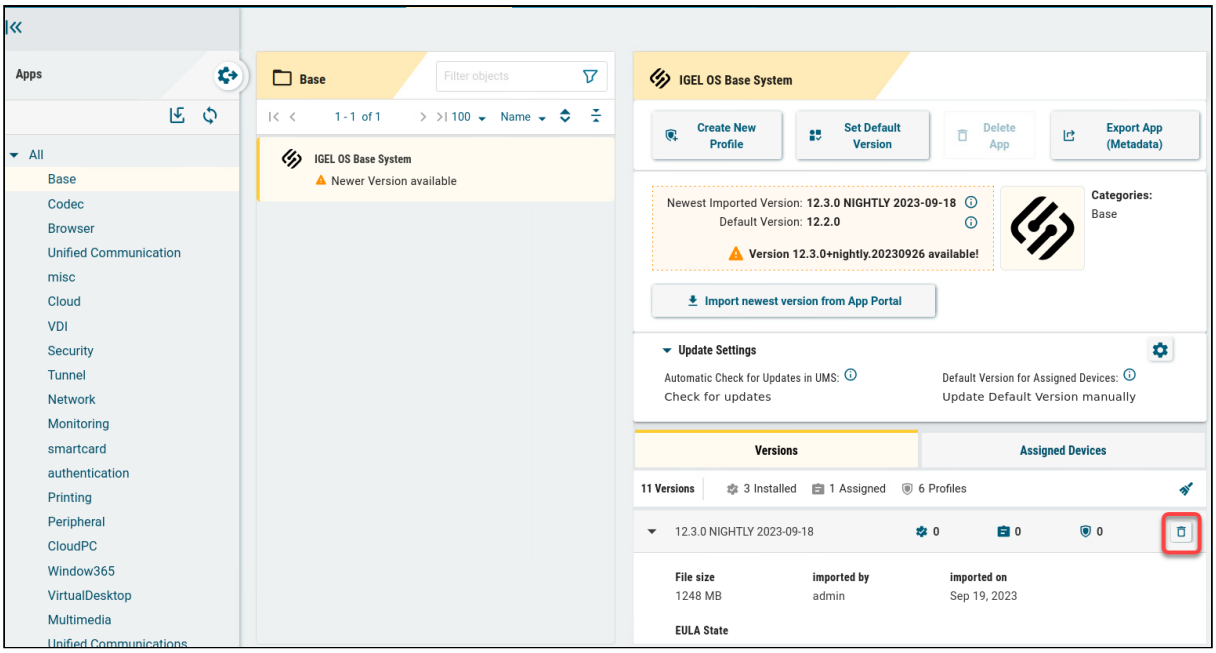
1. Find the device that has imported the IGEL OS 12 version in question and delete it from the UMS. Do not forget to clear the recycle bin afterward.





As an alternative to deleting the device, you can change the version of the IGEL OS 12 Base System for all devices in the UMS; this includes all profiles that configure the Base System.

2. In the UMS web app, go to **Apps > Base** and delete the Base System version in question.



Now you can start with Getting IGEL OS 12 from the App Portal. (see page 27)

Errors after OS12 Upgrade of an OS11 Device which Is Managed via ICG

Environment

- IGEL UMS 12.02.130
- IGEL ICG 12.xx

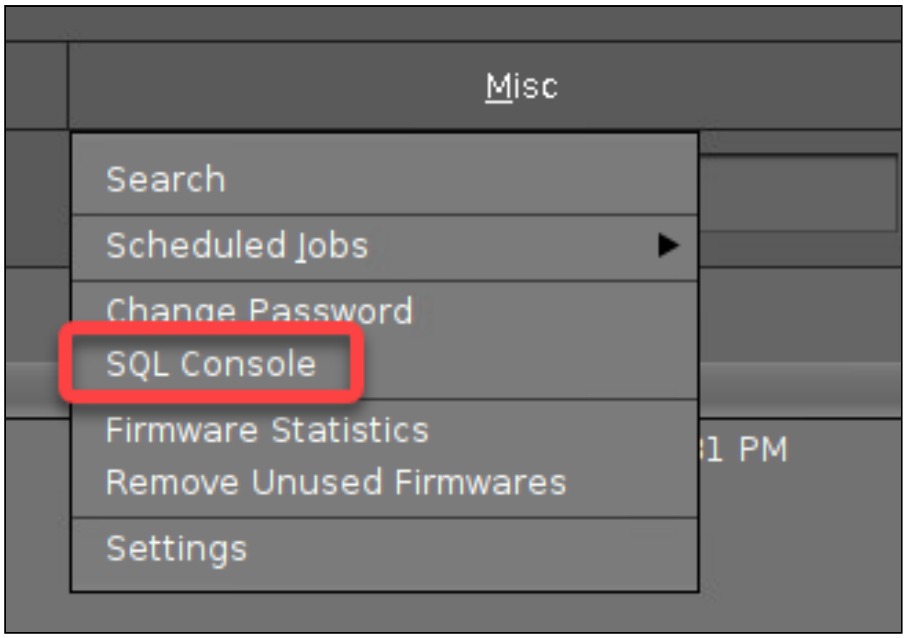
Symptom

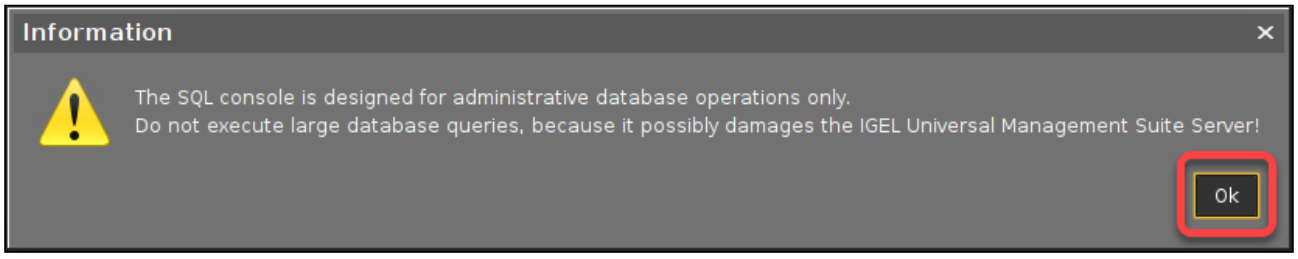
An OS11 device that is managed via ICG is not fully manageable after the upgrade to OS12. It is not possible to send commands or configurations to the device.

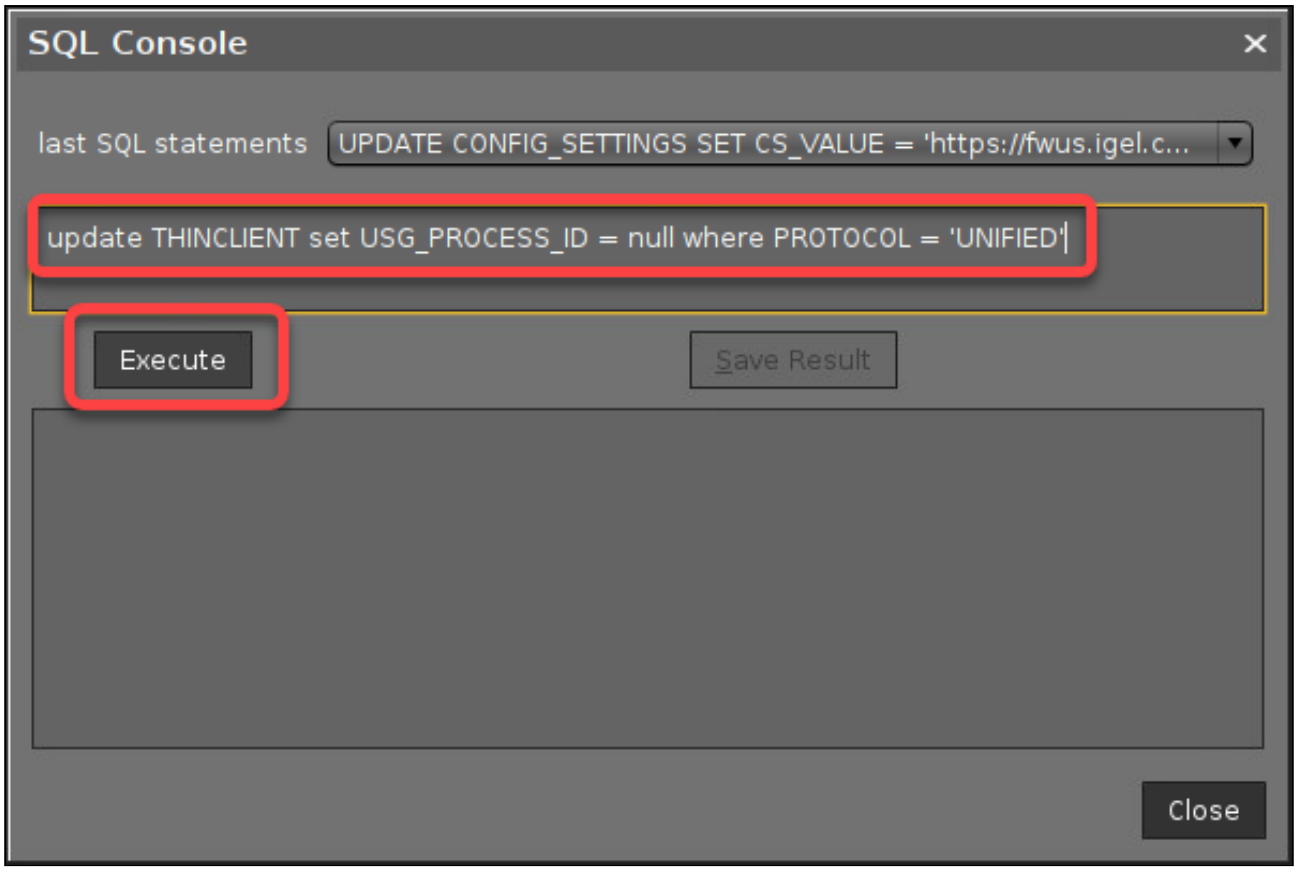
Solution

→ On your UMS Console, open the SQL console and execute the following statement:

```
update THINCLIENT set USG_PROCESS_ID = null where PROTOCOL = 'UNIFIED'
```


Misc
Search
Scheduled Jobs
Change Password
SQL Console
Firmware Statistics
Remove Unused Firmwares
Settings
1 PM


Information
The SQL console is designed for administrative database operations only.
Do not execute large database queries, because it possibly damages the IGEL Universal Management Suite Server!
Ok



Afterward, the device will be fully manageable.

Troubleshooting

If the device has encountered errors, it collects them in its journal and makes them available to the UMS.

You can use the UMS to collect the error files and prepare them for sending them to the IGEL Support Team.

For instructions, see (12.04.120) Save Device Files for Support in the IGEL UMS .

Adapting IGEL OS 11.04 or Higher for Devices with Small Storage

Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher
- UMS 6.05 or higher (recommended)
- Endpoint device that is supported by IGEL OS 11.04.100 or higher but the free storage is lesser than required by the full feature set

Overview

For IGEL OS 11.04.100 or higher with the full feature set, a minimum of 2 GB storage is required. If your device has less free storage than required, e.g. because of large custom partitions, you can reduce the feature set so that the firmware fits on your device's storage.

Perform these two steps:

1. Determining Which Features to Deactivate (see page 61)
2. Reducing the feature set by one of the following methods:
    - Using a UMS Profile (see page 61)
    - Using the Preconfigured Reduced INF File (see page 62)
    - Customizing the INF File (see page 63)

Determining Which Features to Deactivate

→ Determine the storage requirements of the individual IGEL OS features using one of these methods:

- Go to https://kb.igel.com/release-notes/current/release-notes , select the "Notes for Release" of your firmware version, then select "Component Versions...", and go to the "Services" section. The "Reduced Firmware" column indicates for each feature whether it is included in the preconfigured reduced feature set or not.
- Open the `readme[version].txt` in your update source directory and search for "Reduced Firmware".

Reducing the Feature Set

Using a UMS Profile

> **Buddy Update Server**
>
> When you download a firmware that has been reduced with the UMS (or the device's Setup) on a buddy update server, the buddy server itself will have the full feature set anyway. Hence, all devices that are used as update servers must have sufficient free storage.

1. Choose an appropriate profile that is assigned to all relevant devices, or create a new profile. For further information, see (12.06.100-en) Creating Profiles in the IGEL UMS .
2. Go to **System > Firmware Customization > Features** and deactivate all features that are not needed.

Using the Preconfigured Reduced INF File

> **Reduced Feature Set Cannot Be Changed by Setup/UMS**
>
> When you have reduced the firmware using this method, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

> **Buddy Update Server**
>
> When you have downloaded a reduced firmware on a buddy update server, also the buddy server itself has the reduced feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.

Replace the `lxos.inf` file as follows:

1. Go to the directory that contains the source files for the firmware update. If you use the WebDav capability of the UMS, this is `<UMS installation directory>\rmguiserver\webapps\ums_filetransfer\<firmware version>`; example: `C:\Program Files\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\IGEL_OS_11-11.04.100`
2. Delete `lxos.inf`

   > It is safe to delete `lxos.inf` because there is a backup file named `lxos-full.inf`

3. Copy `lxos-reduced.inf` to `lxos.inf`
4. Start the firmware update as usual.

Customizing the INF File

> **Reduced Feature Set Cannot Be Changed by Setup/UMS**
>
> When you have reduced the firmware using this method, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

> **Buddy Update Server**
>
> When you have downloaded a reduced firmware on a buddy update server, also the buddy server itself has the reduced feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.

To customize the INF file:

1. Open `lxos.inf`
2. In the `[INFO]` section, add the following line:
   `custom="true"`
3. Delete the `[PART]` section of every partition you want to exclude, but do this ONLY IF the section has both of the following entries:
   `dispensable="true"`
   `type="squashfs-auto"`
4. Save `lxos.inf` and start the firmware update as usual.

Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update

This document describes how to upgrade UDC3 or UD Pocket devices from IGEL OS 10.06 to IGEL OS 11 via the Universal Firmware Update feature of the UMS (Universal Management Suite).

Since a new licensing model has been introduced with IGEL OS 11, a license from an IGEL Workspace Edition Product Pack must be available for each device. If you have valid maintenance for your devices, you can convert your existing UDC3 or UD Pocket Product Packs to Workspace Edition (WE) Product Packs; see *Licenses & More* > *IGEL License Portal (ILP)* > *The IGEL License Portal (ILP) - User Guide* > *Converting UDC3 or UD Pocket Licenses for Upgrading to IGEL OS 11*.

Read all the following chapters in the order given and follow the instructions.

1. Devices That Can Be Upgraded to IGEL OS 11 1 (see page 65)
2. Important! Consider This Before Upgrading (see page 79)
3. Getting the UMS Ready (see page 81)
4. Deploying the Licenses 3 (see page 82)
5. Creating the Universal Firmware Update (see page 83)
6. Creating an Upgrade Profile (see page 96)
7. Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices (see page 108)
8. Testing the Upgrade 1 (see page 113)
9. Unassigning the Upgrade Profile and the Universal Firmware Update (see page 116)
10. If Applicable: Restoring Custom Partition and Custom Applications (see page 118)
11. Upgrading All Devices (see page 119)

Devices That Can Be Upgraded to IGEL OS 11

In this section, you find the general hardware requirements for IGEL OS 11 and a list of third-party devices officially supported by IGEL OS 11.

> Partner Solutions for Peripherical Devices
>
> For further supported hardware from IGEL partners, e.g. headsets, see *IGEL OS Base System > Partner Solutions*.

Core Requirements

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

  RAM size higher than 2 GB is recommended if you use any of the following:
  - Unified Communications optimizations (uses a client-side media engine)
  - High-resolution graphics output
  - More than two monitors

  With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Storage: Depends on the release version of IGEL OS 11. The details are listed below:
  - Up to IGEL OS 11.03: 2 GB minimum; ≥ 4 GB recommended
  - From IGEL OS 11.04 to IGEL OS 11.07: If the full feature set is applied, at least 2.4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher .
  - From IGEL OS 11.08 onwards: If the full feature set is applied, at least 4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher.
- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

Devices Supported by OSC and UD Pocket with IGEL OS 11

> The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the minimum requirements will not function with IGEL OS: Any x86-64 hardware endpoint device that meets the IGEL-stated minimum hardware requirements for IGEL OS (for example, the processor speed and RAM) can be expected to work adequately with IGEL OS and should be considered a candidate for repurposing from another OS. With an IGEL OS subscription or active maintenance, customers can expect IGEL to make any

necessary “best effort” to support, regardless of whether the endpoints in question are specifically listed within the IGEL Knowledge Base or elsewhere (e.g. on the IGEL Ready Showcase at https://www.igel.com/ready/showcase-categories/endpoints/).
For any devices not listed here or on the IGEL Ready showcase, you can contact your hardware vendor and request those devices to be added to the IGEL Ready program.
Integrated drivers and supported peripherals are listed in the Third-Party Hardware Database[23]. For more solutions compatible with IGEL OS, see *IGEL OS Base System > Partner Solutions*.

HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[24] to get information on which device models are available with pre-installed IGEL OS.

For some of the devices listed here, Flash memory must be extended to ≥ 2 GB. For these devices, an appropriate note is added.

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft’s 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see *Security & Safety > UEFI Secure Boot Enabling Guides > Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot*.

[Fn] keys may not work on some supported and listed laptop/notebook models.

ADS-Tec

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DVG-VMT9010	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

23. https://www.igel.com/linux-3rd-party-hardware-database/
24. https://www.igel.com/technology-partners/

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DVG-VMT9012	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9015	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9112	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

Advantech

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L*	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L*	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrial PC/ Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

Dell / Wyse

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Notes
5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100	
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100	
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140	
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100	
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100	
Latitude 5510	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100	Wake-on-LAN functionality is not supported.
Optiplex 3000	Thin Client	4 GB	32 GB	Intel Celeron N5105	11.08.200	

Dynabook

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Portegé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portegé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

Elo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

Fujitsu

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100		
HP t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	Intel AC9260	
HP t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100		

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100		
HP t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100		
HP t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100		
HP t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	Intel AC9260 Realtek RTL8852AE	This model is not supported with HP USB-C Essential G5 Dock
HP t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	Intel AC9260 Realtek RTL8852AE	
HP mt46	Mobile Thin Client	8 GB	32 GB	AMD Ryzen 3 PRO 4450U	11.07.100		Excluding support for WWAN and Wake-on-LAN (both features are planned)
HP Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	Realtek RTL8852BE	

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.08.330) Excluding support for Wake-on-LAN (feature is planned) Excluding support for built-in fingerprint sensor
				AMD Ryzen 5 5625U	11.08.330		
HP t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	Realtek RTL8852AE	
HP Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	Realtek RTL8852CE (Supported as of 11.09.150)	
HP Pro mt440 G3	Mobile Thin Client	8 GB	128 GB	Intel Celeron 7305	11.08.440	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.09.260)
HP Elite t755	Thin Client	8 GB	128 GB	AMD Ryzen Embedded V2546	11.09.260	Realtek RTL8852CE	This model offers no USB-C docking support

HP Docking Stations

Name	Supported from IGEL OS Version	Notes
HP USB-C Docking Station G5	11.08.230	
HP USB-C G5 Essential Dock	11.08.290	Not supported with HP t640

Intel

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

Lenovo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	Intel AC9260	11.04.100	
		8 GB	128 GB	AMD A4-9120e	QCA6174 802.11ac	11.04.100	
ThinkCentre M75n	Desktop PC	8 GB	256 GB	AMD Ryzen 3 Pro 3300U	Intel AC9260	11.05.100	
ThinkCentre M70q Gen1	Desktop PC	16 GB	256 GB	Intel i5-10500t	Comet Lake PCH CNVi WiFi, Intel	11.05.100	
ThinkCentre M70q Gen 3	Desktop PC	16 GB	256 GB	Intel Core i5-12500T	Intel AX201	11.08.240	
ThinkCentre M75q Gen 2	Desktop PC	4 GB	128 GB	AMD Ryzen 3 Pro 5350GE	Intel AX200	11.08.240	
K14 AMD Gen 1	Laptop/ Notebook	8 GB	256 GB	AMD Ryzen 5 PRO 5650U	Mediatek MT7921	11.08.240	

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkPad L14 AMD Gen 1	Laptop/ Notebook	64 GB	1 TB	AMD Ryzen 7 Pro 4750U	Wi-Fi 6 AX200, Intel	11.05.100	
14w	Laptop/ Notebook	4 GB	64 GB	AMD A6-9220C	QCA6174 802.11ac	11.05.100	
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360
ThinkCentre Neo50q Gen 4	Thin Client	8 GB	256 GB	Intel Core i3-1215U	Wi-Fi 6 RTL8852BE	11.08.240	
		4 GB	256 GB	Intel Celeron 7305	Wi-Fi 6 AX201		
K14 Intel Gen 1	Laptop/ Notebook	16 GB	256 GB	Intel Core i5-1135G7	Intel AX210 WiFi / BT combo	11.08.290	
ThinkPad L14 Intel Gen 3	Laptop/ Notebook	16 GB	512 GB	Intel Core i5-1235U	Intel Wi-Fi 6 AX201 2x2 AX vPro	11.08.330	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360
ThinkEdge SE10	Thin Client	8 GB	1 TB	Intel Atom x6425RE	MediaTek MT7921LEN	11.08.360	
			256 GB	Intel Atom x6214RE	Intel AX210	11.08.360	

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkPad L14 AMD Gen 4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L15 AMD Gen4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L14 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L15 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L13 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX201	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN
ThinkPad L13 AMD Gen 4	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 3 PRO 7330U	AMD RZ616	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN

Lenovo Docking Stations

Name	Supported from IGEL OS Version
ThinkPad USB-C Hybrid Dock	11.07.100
IOBOX	11.07.100
Universal USB-C Dock	11.08.440

Lenovo USB-C to Ethernet Adapter

Name	Supported from IGEL OS Version	Supported with
USB-C to Ethernet Adapter	11.09.260	• ThinkPad L13 Intel Gen4 • ThinkPad L14 AMD Gen4

LG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CK550**	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
24CK560**	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
38CK950	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
38CK900	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
34CN650	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CR670	All in One	4 GB	16 GB	Intel Celeron N5105	11.09.110
34CR650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210
27CQ650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210

LG Docking Stations

Name	Supported from IGEL OS Version
LG USB Multi Port Hub	11.09.100

OnLogic

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/ Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

Onyx Healthcare

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

Pepperl+Fuchs

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
BTC12N	Industrial Box Thin Client	4 GB	32 GB	Intel Apollo Lake N4200	11.09.100

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
BTC14N	Industrial Box Thin Client	4 GB	32 GB	AMD Ryzen Embedded V1202B	11.09.100

Rein Medical

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

Secunet

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

USB Memory Sticks That Can Be Used as UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133

Transcend

Name
Powered by IGEL UD Pocket
Powered by IGEL UD Pocket 2

Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

⚠ Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

ℹ For some features, more than 2 GB RAM is required. Example: if you use dual monitor environments, a virtual machine must have at least 8 GB RAM.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

- Delock Adapter DP 1.2 to DVI does not work.

** When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher

Check List

✅ The devices you want to upgrade meet the hardware requirements for IGEL OS 11.

Next Step

>> Important! Consider This Before Upgrading (see page 79)

Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

Existing partitions: Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

No Downgrade

You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

Features (e.g. Clients)

IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions

The contents of Custom Partitions will be deleted by the upgrade. Make sure that the Custom Partition is restored after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a Custom Partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device.

Custom Commands

The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

Power Supply

Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

Network

All devices must be connected to a LAN or WLAN. LAN is the recommended option. The device will not be upgraded if OpenVPN, OpenConnect, mobile broadband, or genucard is configured. To be sure, check if the following parameters are deactivated resp. no session is configured:

- **Network > VPN Open VPN** (registry: `sessions.openvpn%`)
- **Network > VPN > OpenConnect VPN** (registry: `sessions.openconnect%`)
- **Network > Mobile Broadband**, checkbox **Enable Mobile Broadband** (registry: `network.interfaces.mobile_broadband.enabled`)
- **Network > VPN > genucard** (registry: `network.interfaces.genucard_vpn_connector.autostart_enabled`)

When you have changed the settings, restart the device to enable the upgrade.

Check List

- The limitations and conditions are understood and do not constitute a problem.

Next Step

>> Getting the UMS Ready (see page 81)

Getting the UMS Ready

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instrucitons, see *Knowledge Base Archive > IGEL Universal Management Suite PDF > Updating a UMS Installation.*
2. Make sure that your devices are registered with the UMS. For more information, see the chapter *Knowledge Base Archive > IGEL Universal Management Suite PDF > Registering Devices on the UMS Server.*

Check List

- Your Universal Management Suite (UMS) version is 6.01.130 or higher.
- All devices that will be upgraded are registered in the UMS.

Next Step

>> Deploying the Licenses 3 (see page 82)

Deploying the Licenses

Checking If the Required Licenses Are Available

→ Ensure that you have the following licenses:

- A valid license from an IGEL Workspace Edition (WE) Product Pack for each device.
- Depending on the features you want to use, you might need IGEL Enterprise Management (EMP) licenses in addition. For further information, see *IGEL Subscription and More > IGEL Software License Overview*.

Deploying the Licenses

→ Choose one of the following methods:

- If you want to deploy a license quickly on a single device: See *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS without UMS*; start from step 5.
- If you have a smaller or medium number of devices and want to control exactly which device should get a license: See *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Manual License Deployment for IGEL OS.*
- If you have a medium or greater number of devices, and you are planning to add new devices/licenses regularly: See *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Set up Automatic License Deployment (ALD) with ALD Token*.
- If you have a medium or greater number of devices, and you are planning to add new devices/licenses frequently (licensing can be managed completely in the IGEL License Portal): See *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD)*.

Check List

✅ The licenses have been purchased.

✅ License deployment is set up.

Next Step

>> Creating the Universal Firmware Update (see page 83)

Creating the Universal Firmware Update

In this step, we will create a Universal Firmware Update that will be used for testing the upgrade and for rolling out the upgrade on all relevant machines.

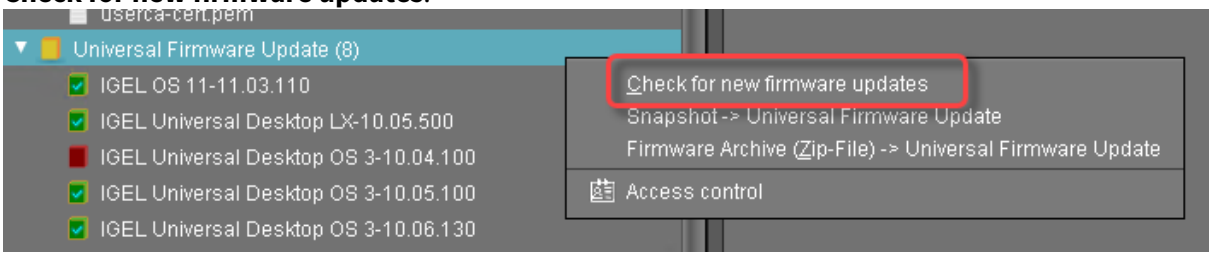
> If you use the *Knowledge Base Archive* > *IGEL Universal Management Suite PDF* > *High Availability Extension*, note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

Choose the procedure that suits your needs:

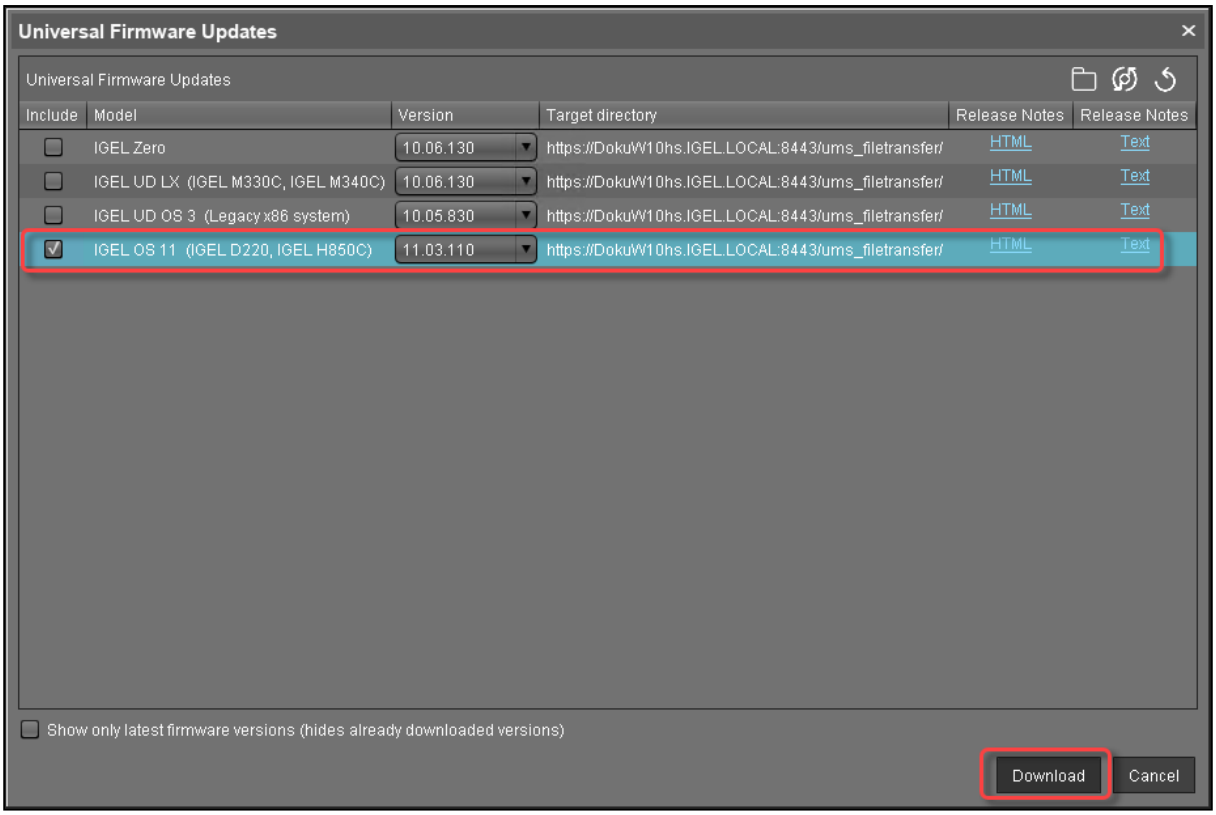
- Configuring the Universal Firmware Update with Files Hosted by the UMS (see page 83)
- Configuring the Universal Firmware Update with Files Hosted by FTP Server (Required for ICG)

Configuring the Universal Firmware Update with Files Hosted by the UMS

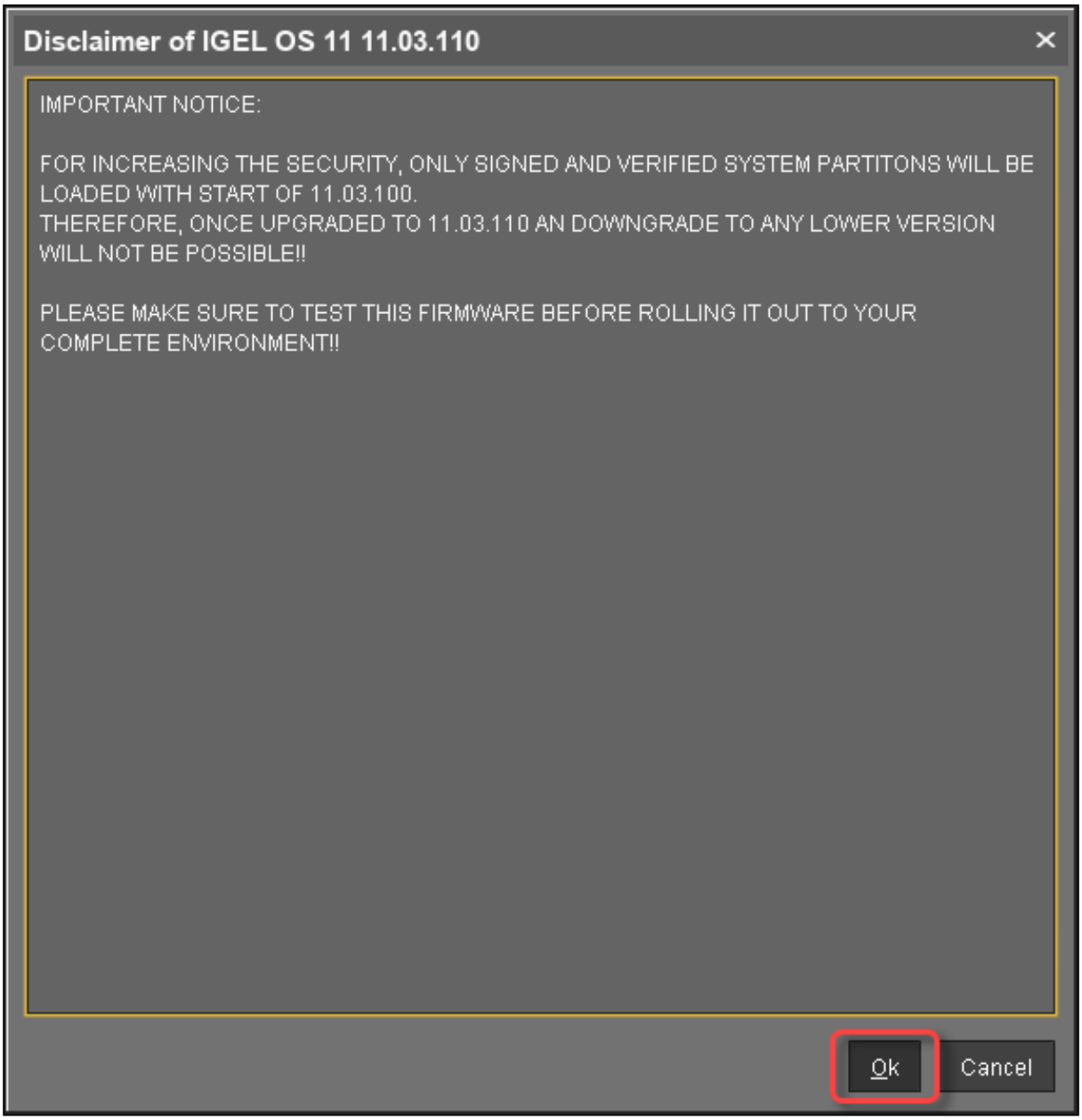
1. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



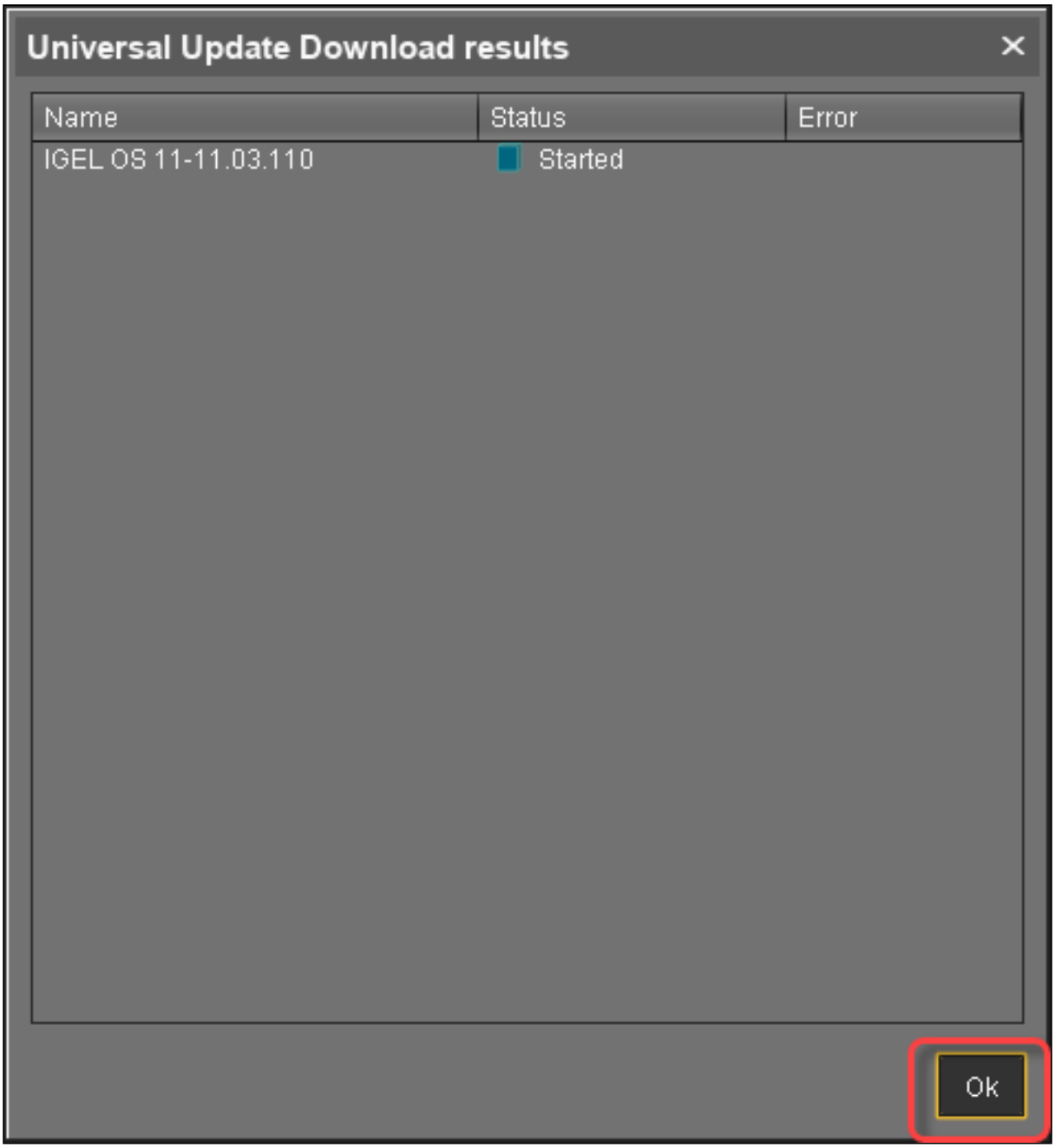
2. Select the entry for the IGEL OS 11 firmware and then select **Download**. (In the example, IGEL OS 11.03.110 is used.)



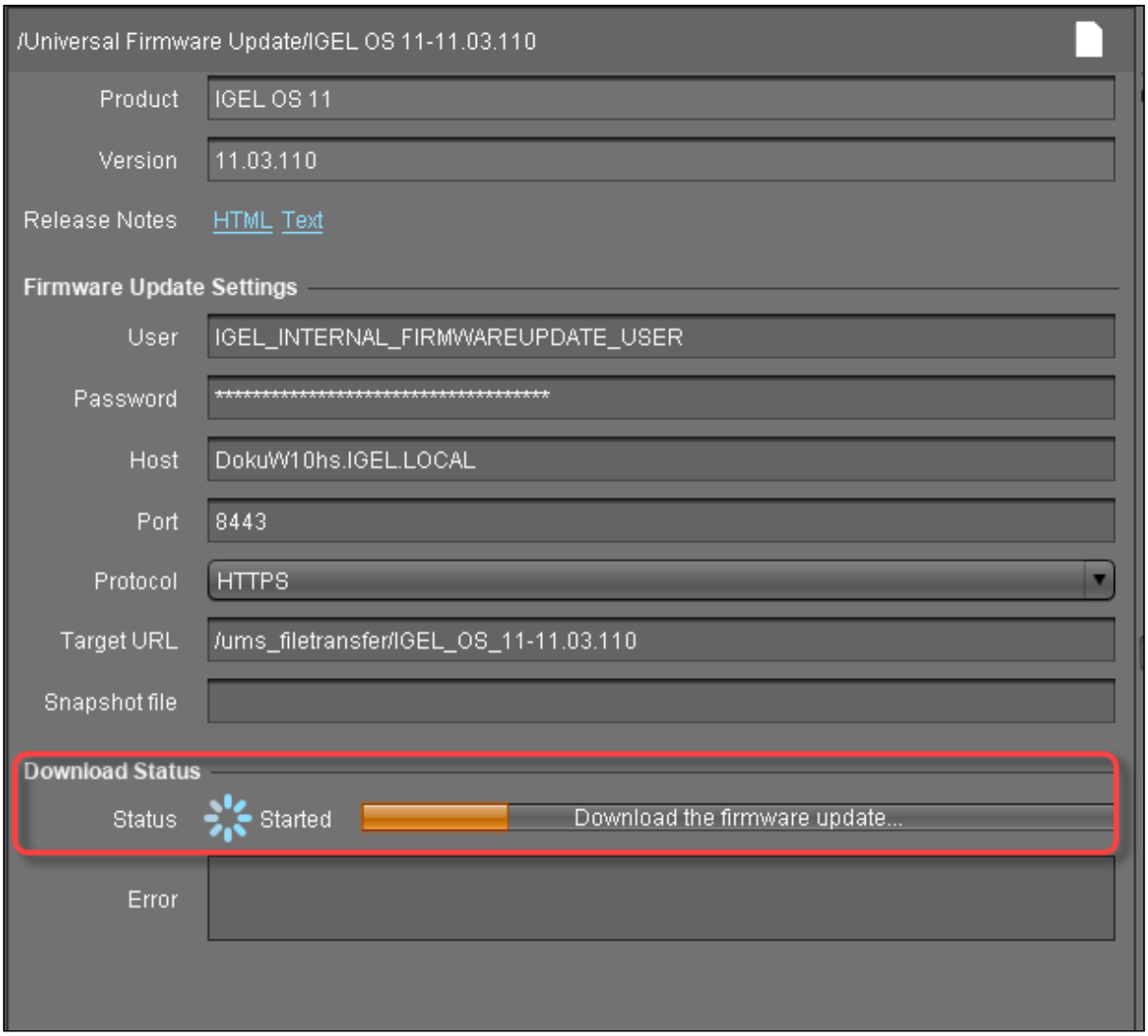
3. Read and confirm the disclaimer. (IGEL OS 11.03.100 or higher only)



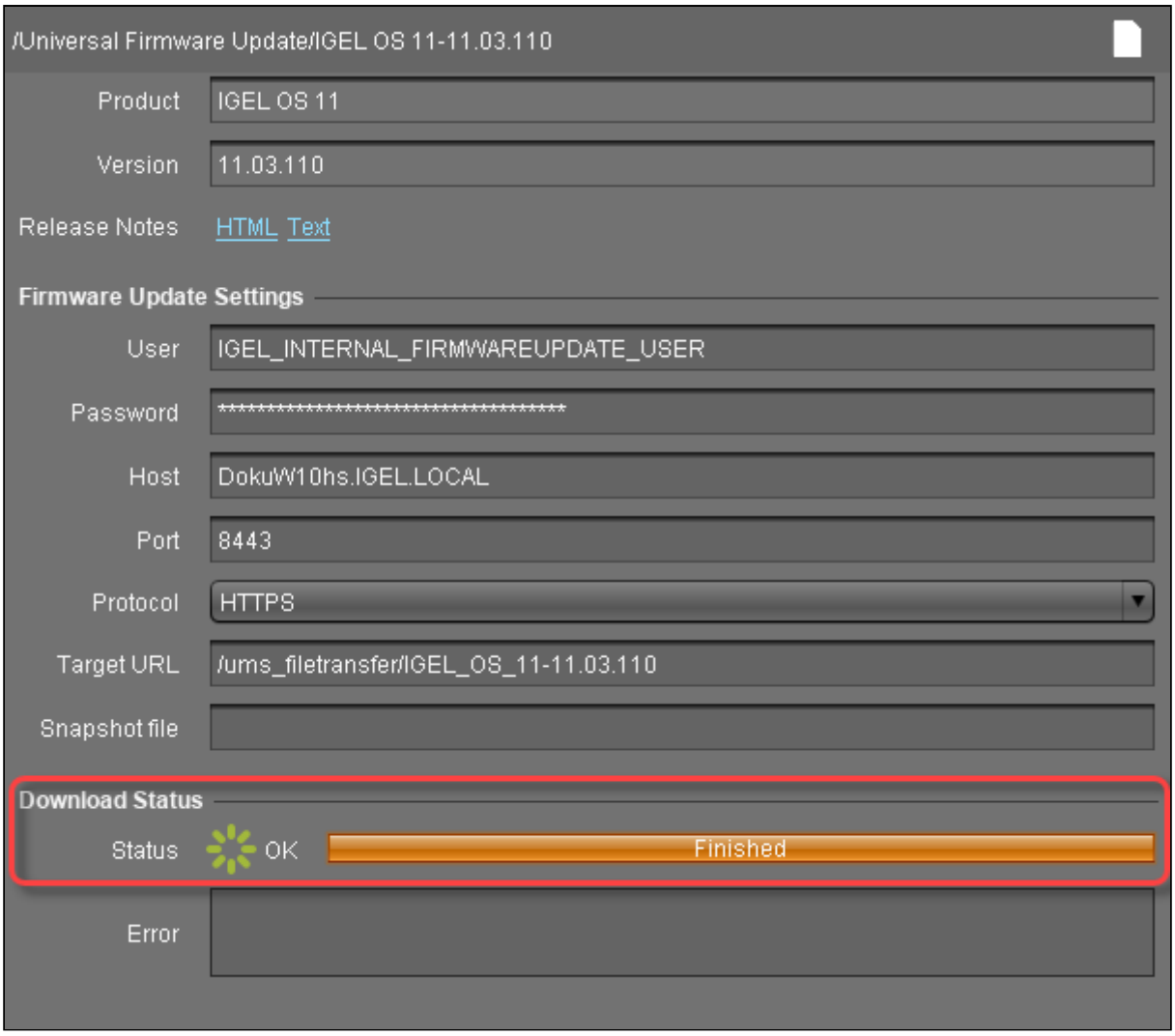
4. Confirm the status message.



In the main window, you can monitor the download process.



When the status is **Finished**, your Universal Firmware Update is ready for use.

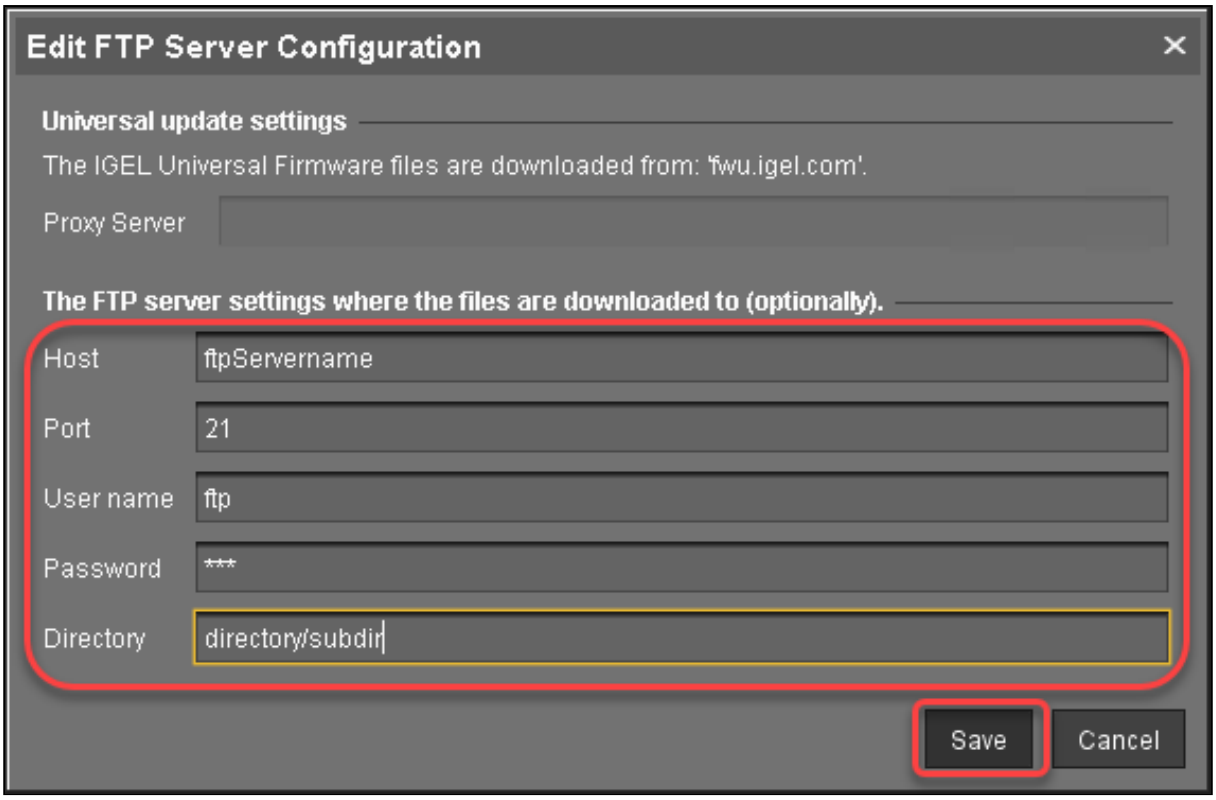


Configuring the Universal Firmware Update with Files Hosted by FTP Server (Required for ICG)

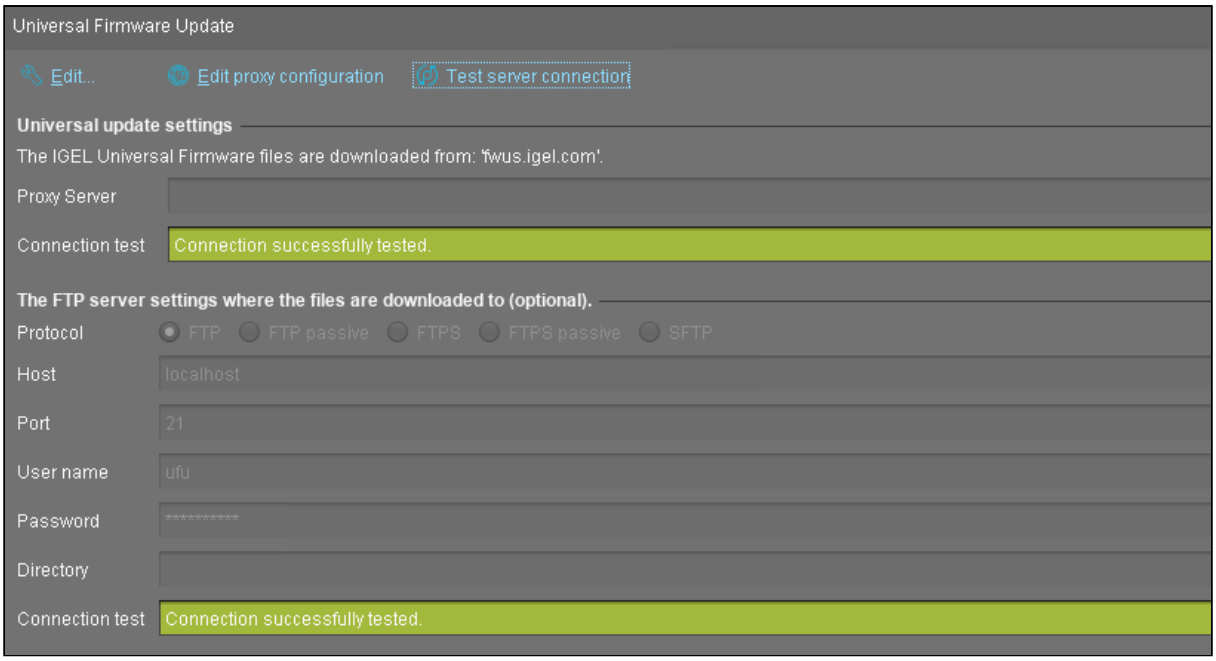
You can use an FTP server instead of the UMS to host the firmware files. If you are using IGEL Cloud Gateway (ICG), an FTP server is required.

To configure an FTP server as update source:

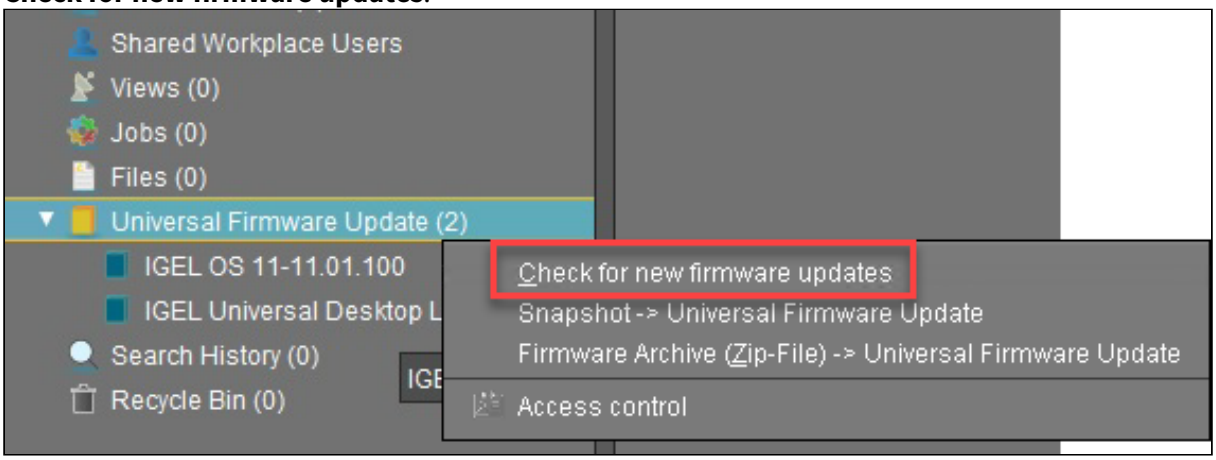
1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click **Edit**.
2. Enter the data required for accessing the FTP server and click **Save**.



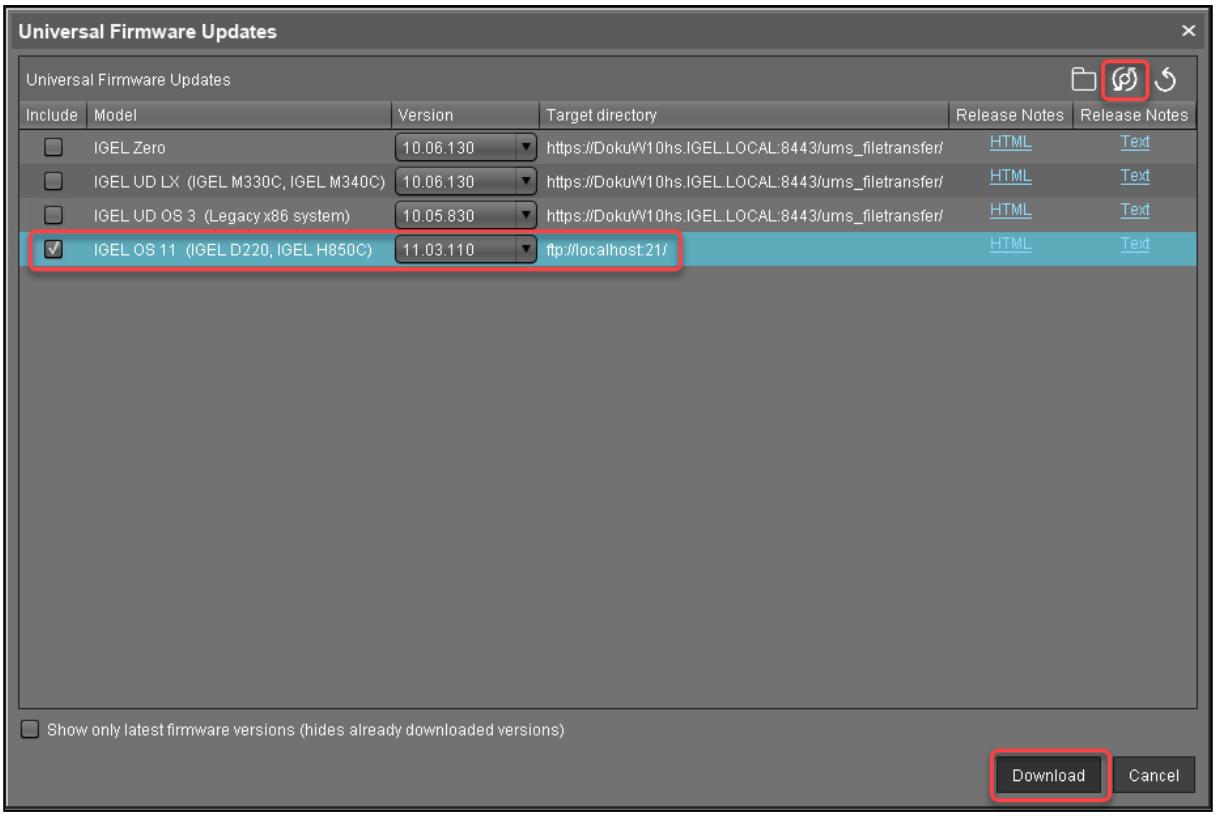
3. Click **Test server connection** to test your settings.
   If everything went well, a success message is shown both for the IGEL download server and for the FTP server:



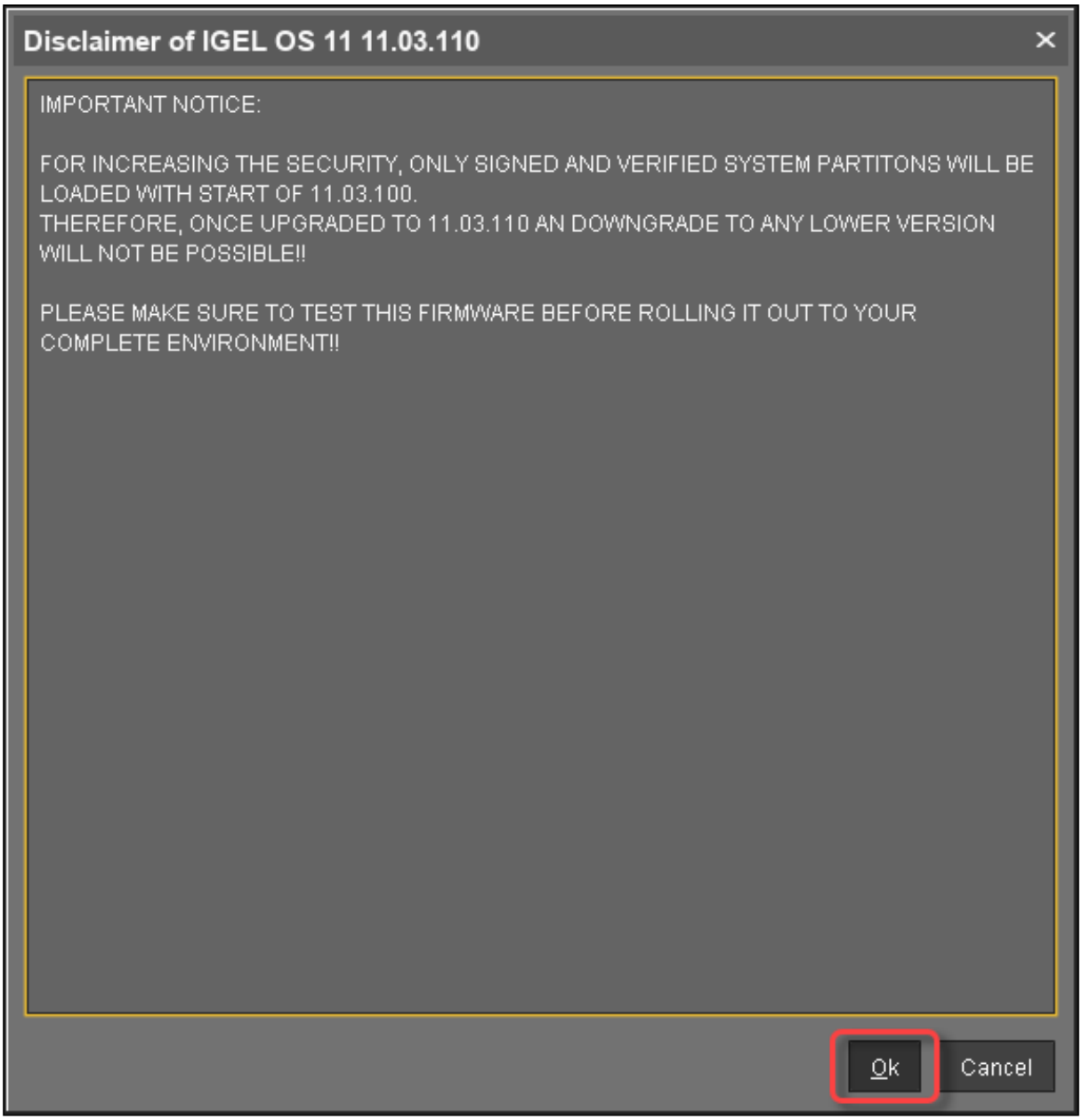
4. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



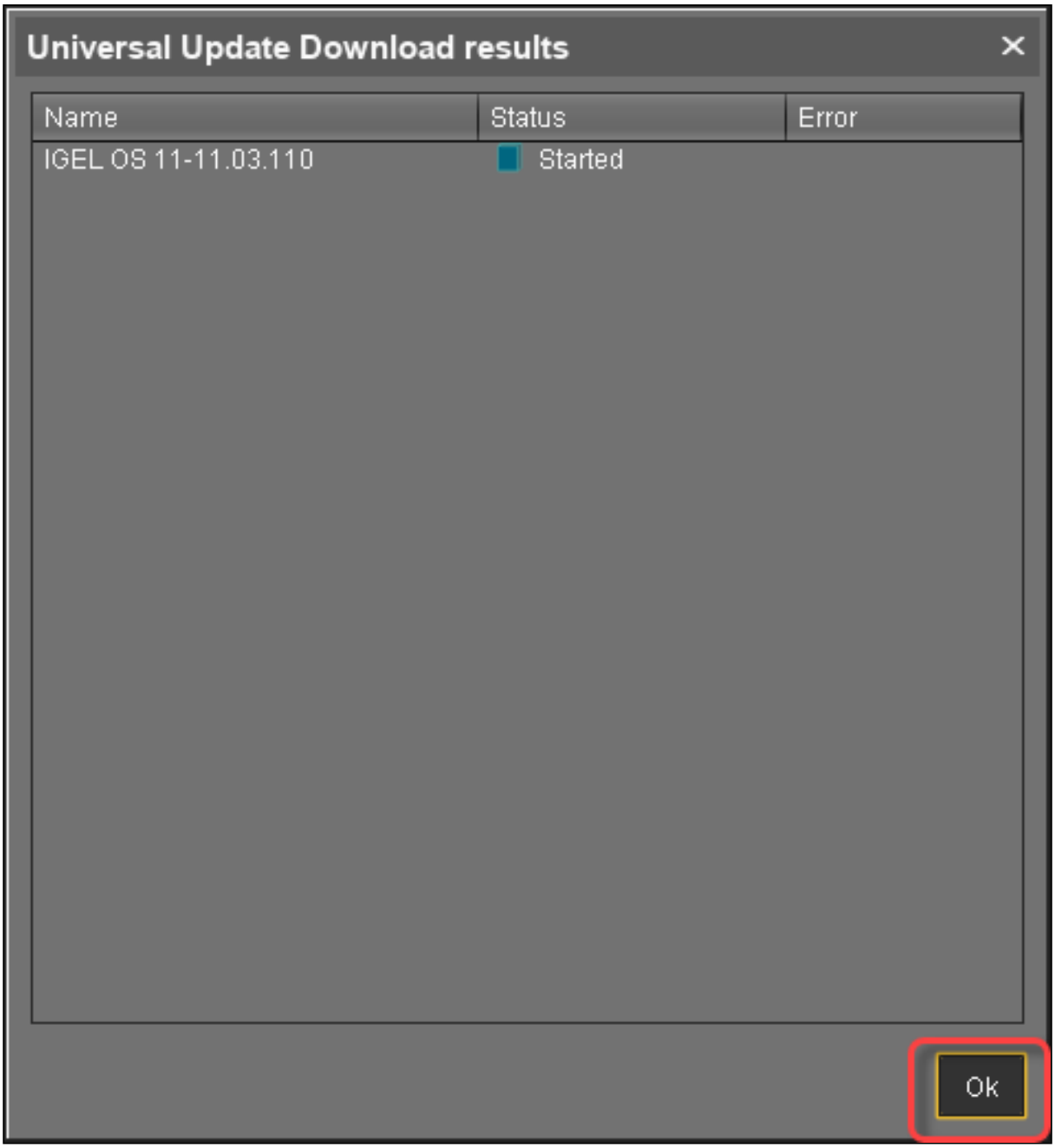
5. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and then select **Download**.



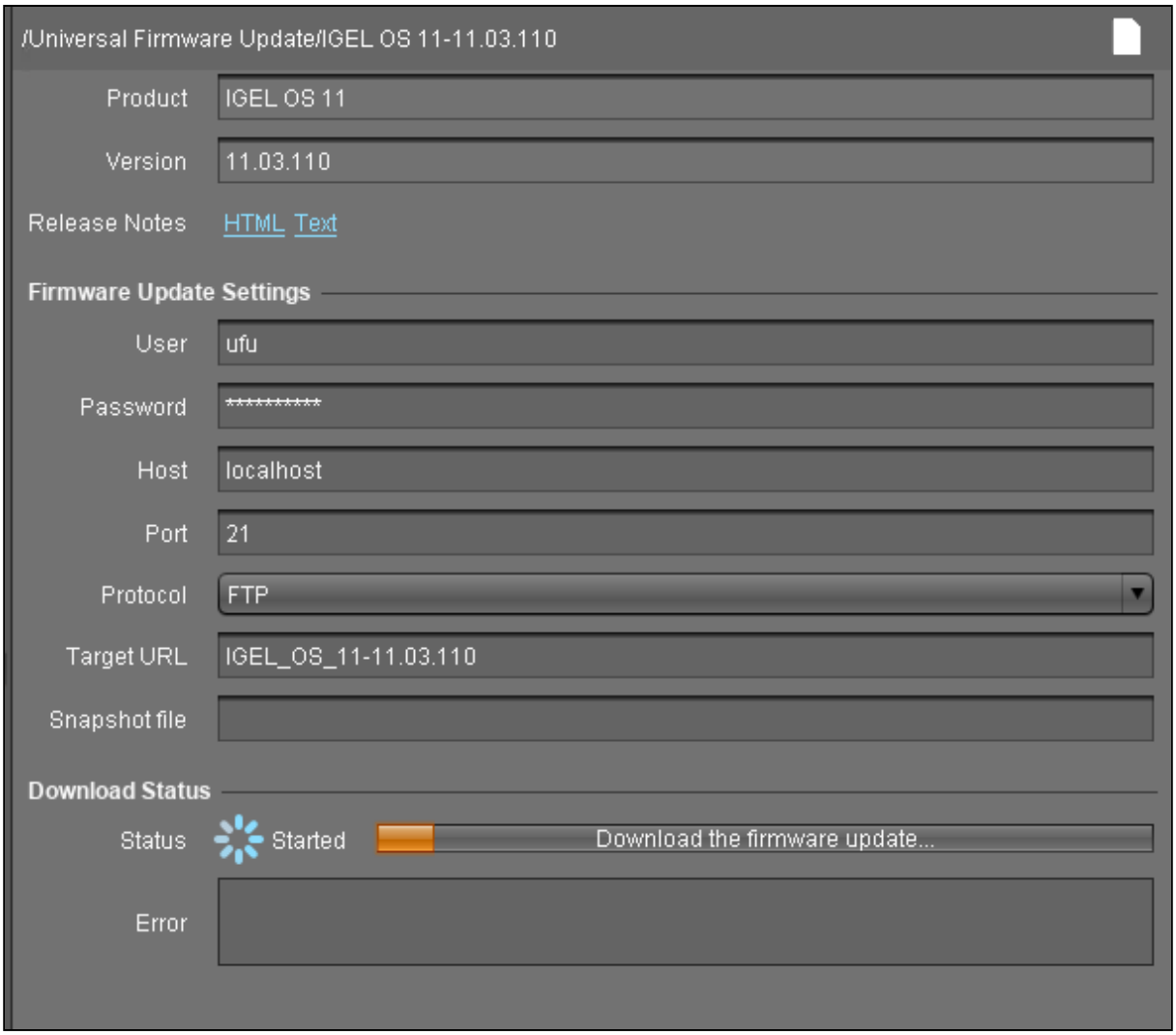
6. Read and confirm the disclaimer. (IGEL OS 11.03.100 or higher only)



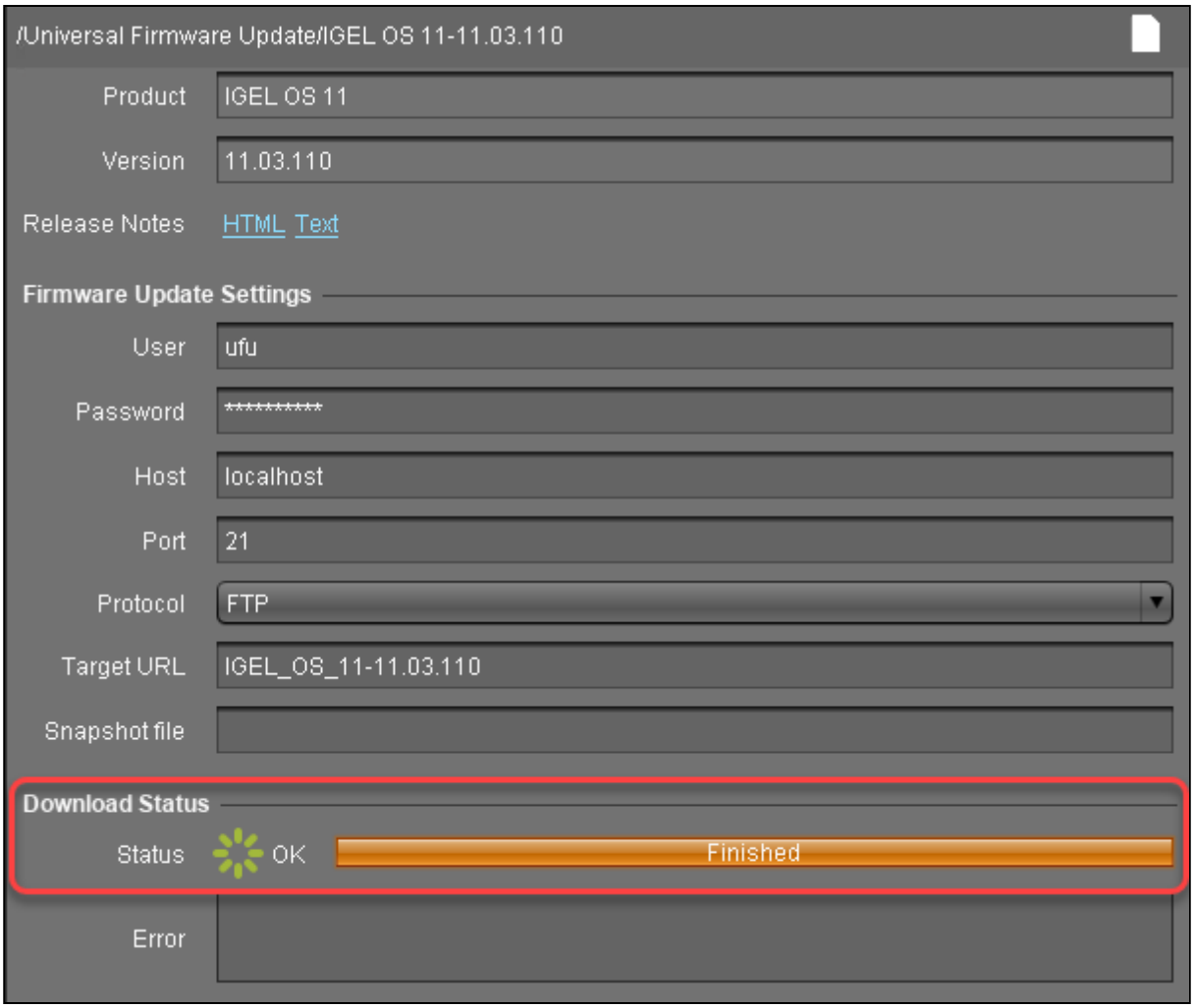
7. Confirm the status message.



The firmware is transferred to the FTP server. In the main window, you can monitor the download process.



When the status is **Finished**, your Universal Firmware Update is ready for use.



Check List

The Universal Firmware Update has been created successfully.

Next Step

>> Creating an Upgrade Profile (see page 96)

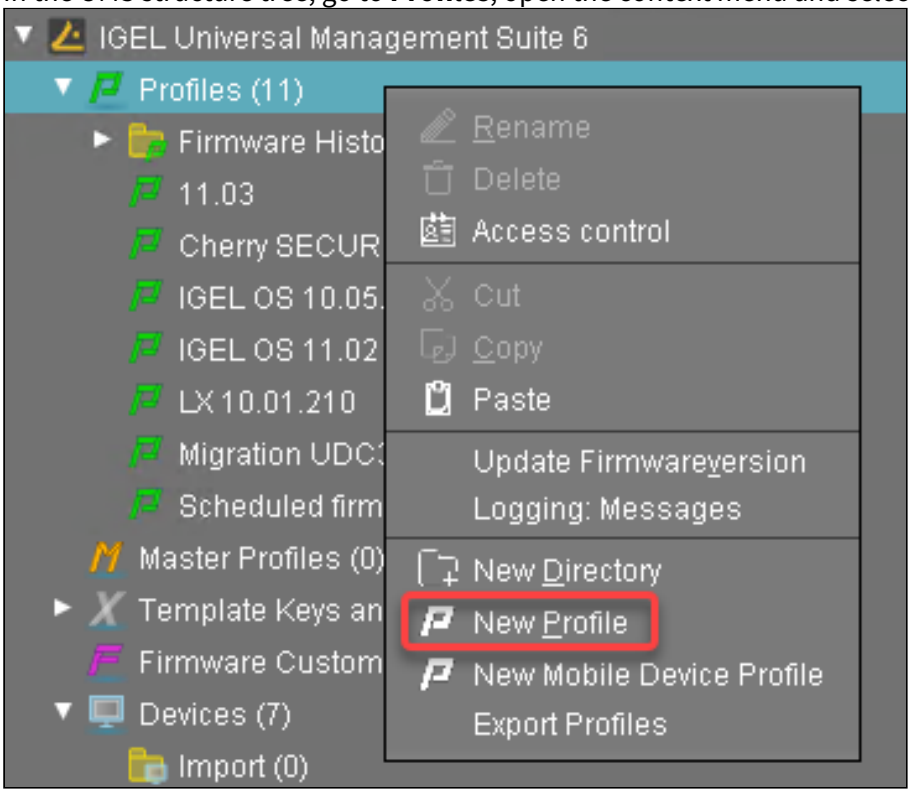
Creating an Upgrade Profile

The upgrade profile varies, depending on whether the devices are in the same network as the UMS or connected via ICG. Choose the appropriate procedure:

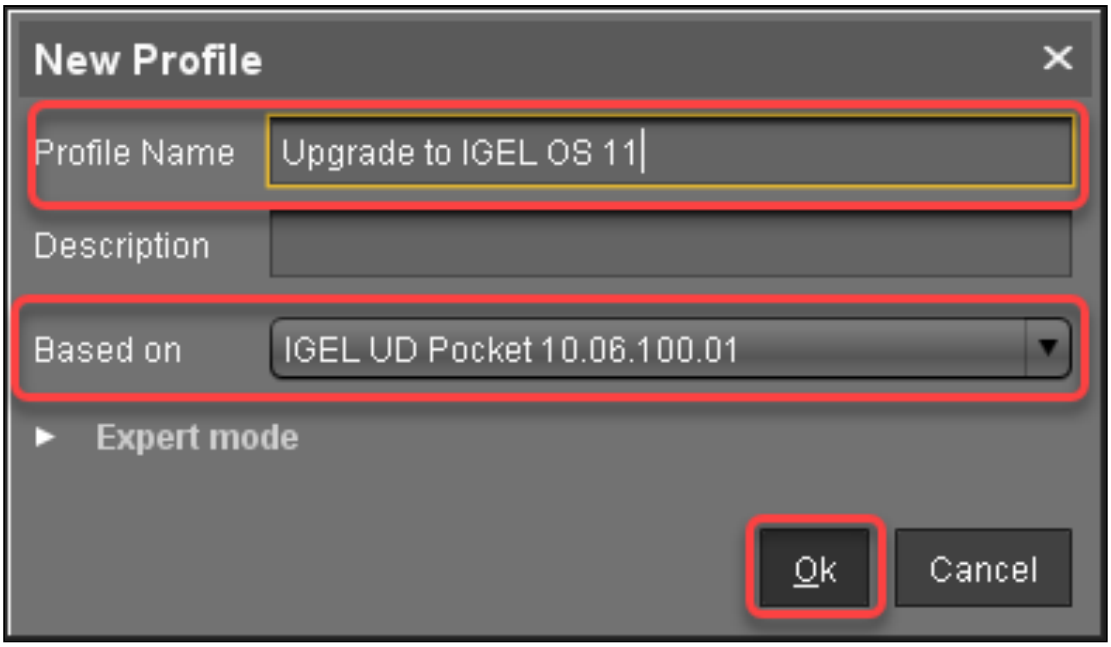
- For Devices that Are in the UMS Network (see page 96)
- For Devices that Are Connected via ICG (see page 101)

For Devices That Are in the UMS Network

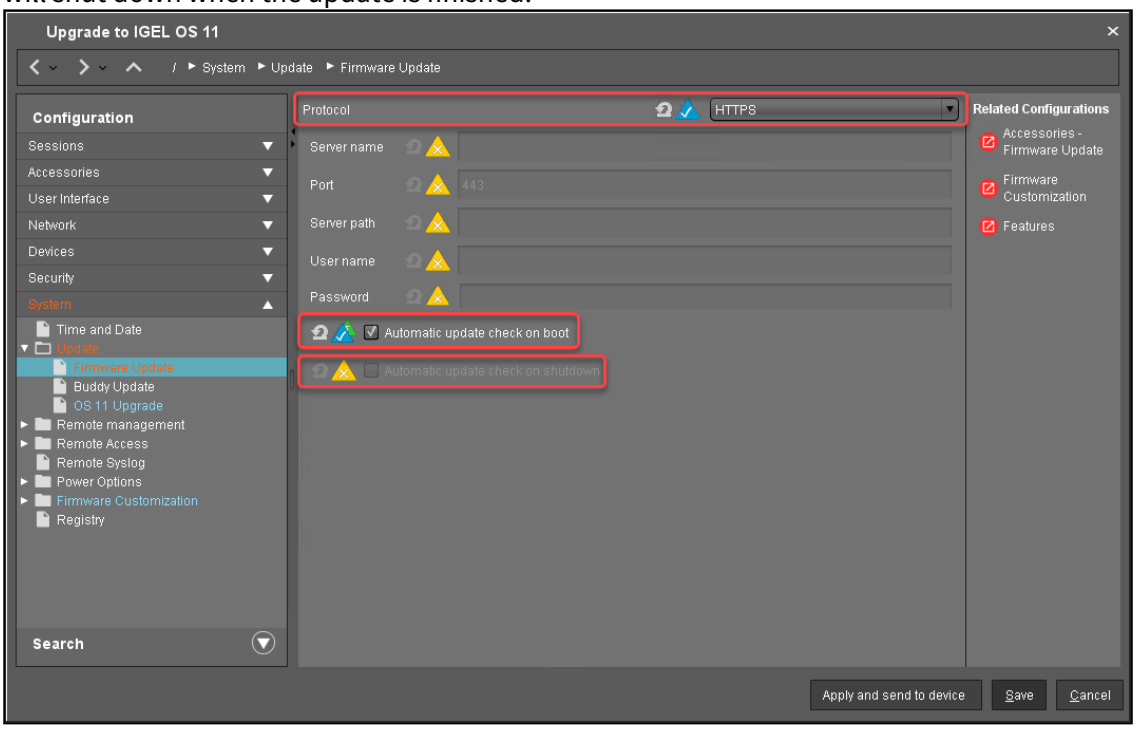
1. In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.



2. Enter the following data:
   - **Profile Name**: Name for the profile, e. g. "Upgrade to IGEL OS 11".
   - **Description**: Optional description for the profile.
   - **Based on**: Firmware version for the profile; select the current firmware of your devices, that is, "IGEL UD Pocket 10.06.100".
3. Click **Ok**.

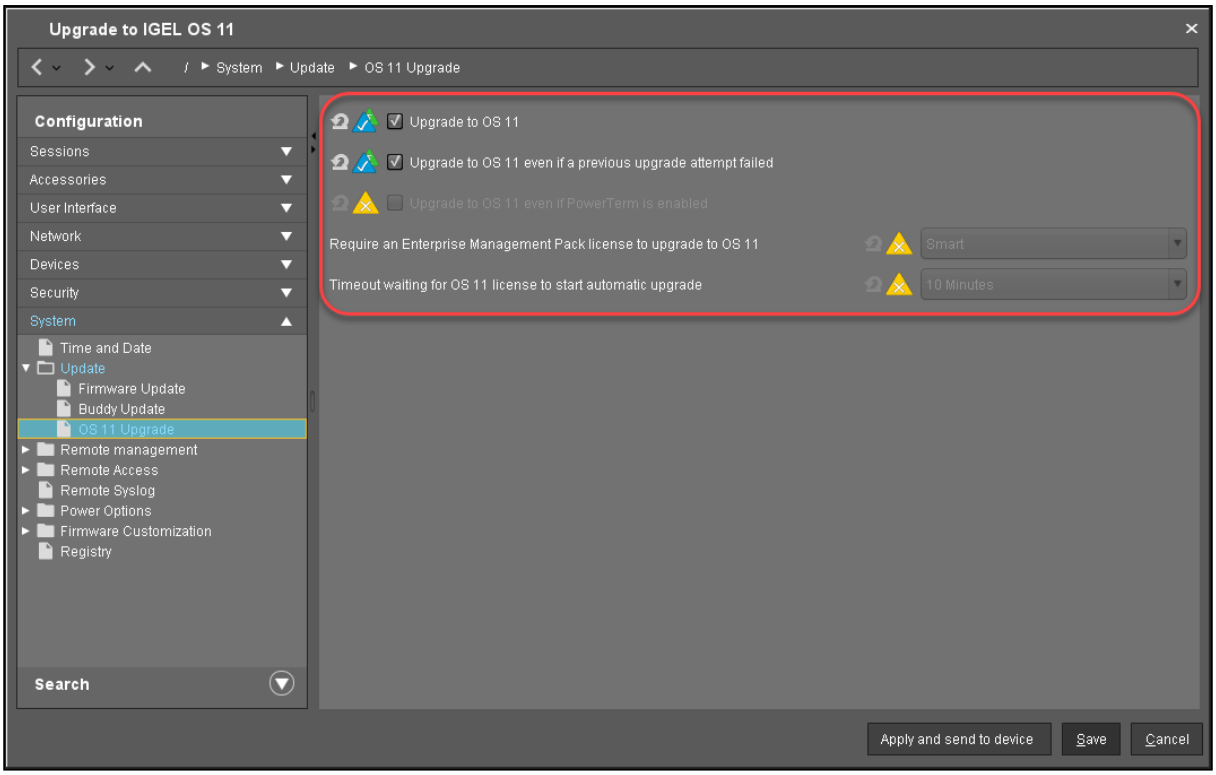


4. Go to **System > Update > Firmware Update** and change the settings as follows:
   - Select "HTTPS" as the **Protocol**.
   - Activate **Automatic update check on boot**.
   - Ensure that **Automatic update check on shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.

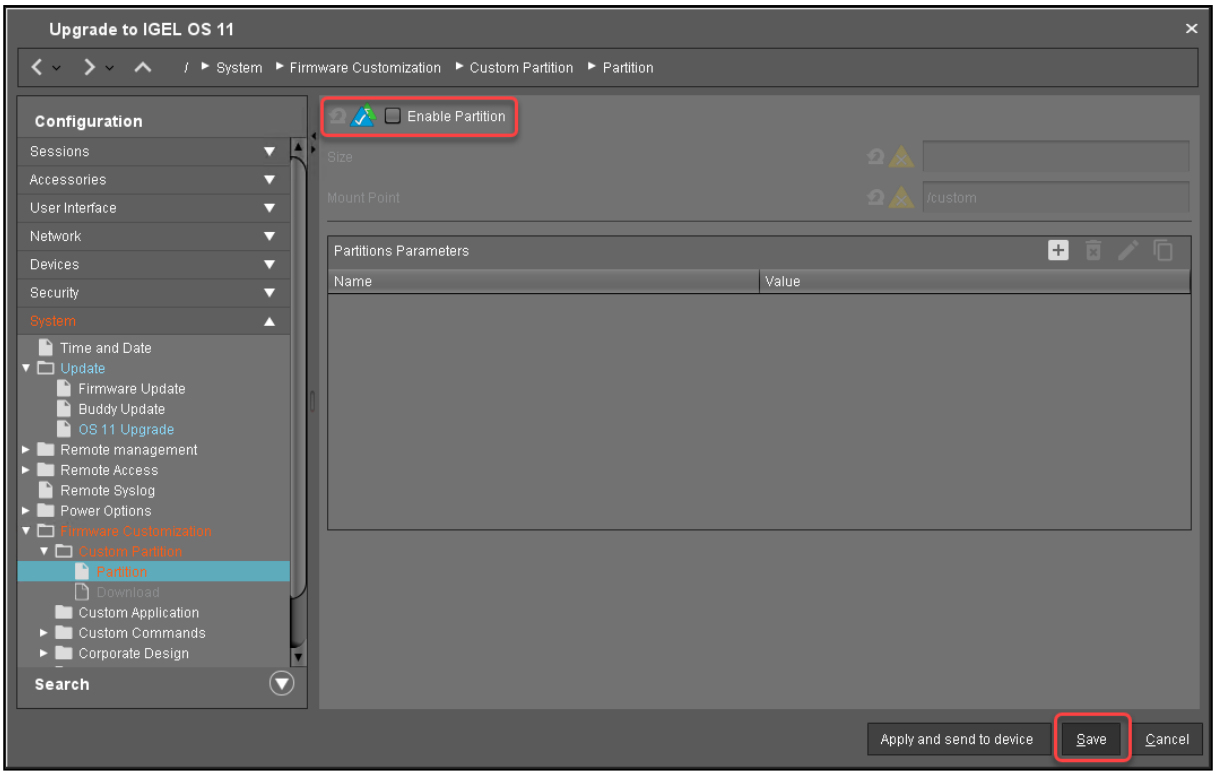


5. Go to **System > Update > Firmware Update > OS 11 Upgrade**.
6. Activate **Upgrade to OS 11**.

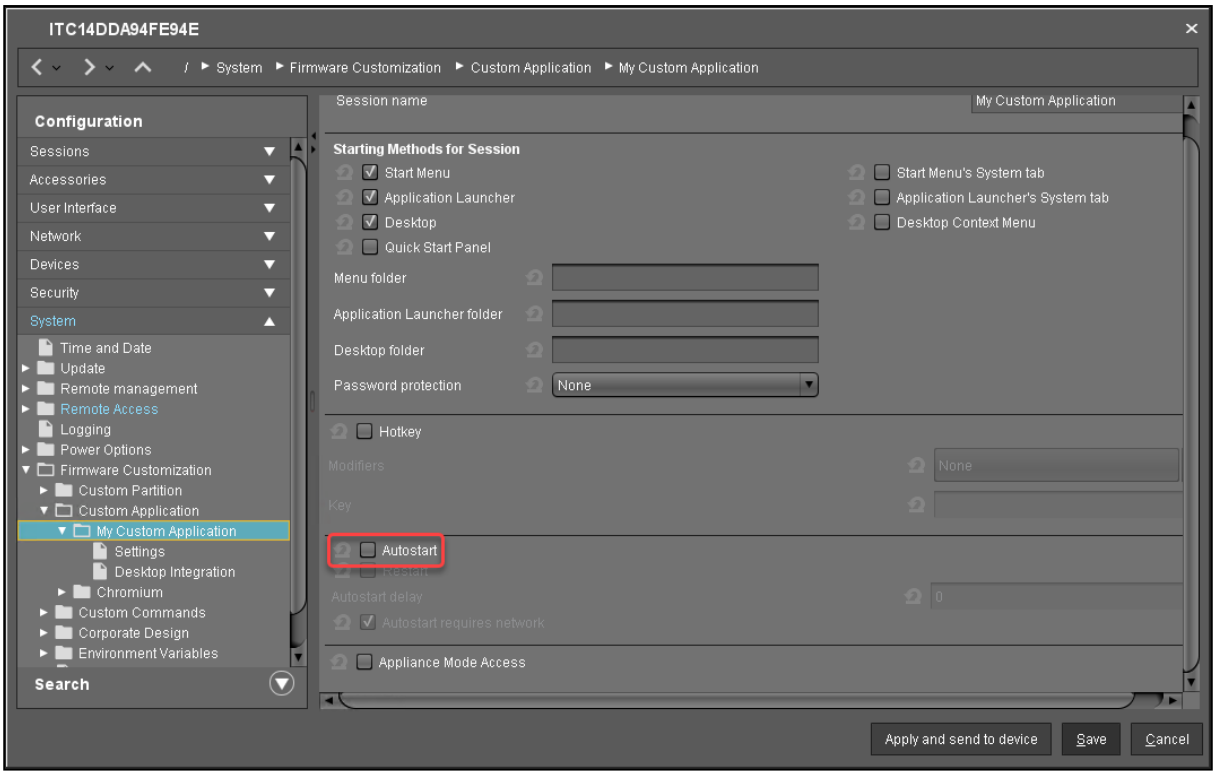
7. Make the following settings according to your needs:
    - If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. With this setting, the device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
    - If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though IGEL OS 11 does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
    - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
        - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When **Smart** is selected, and one of these features is activated, the upgrade is performed only if the device succeeded in fetching a license from an Enterprise Management Pack.
        - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if this license has been fetched, select **Always**.
        - If you want the device to upgrade to IGEL OS 11 without fetching a license from an Enterprise Management Pack, disregarding the features, select **Never**.
8. Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario. This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.



9. If you have a Custom Partition, go to **Firmware Customization > Custom Partition > Partition** and deactivate **Enable Partition**.



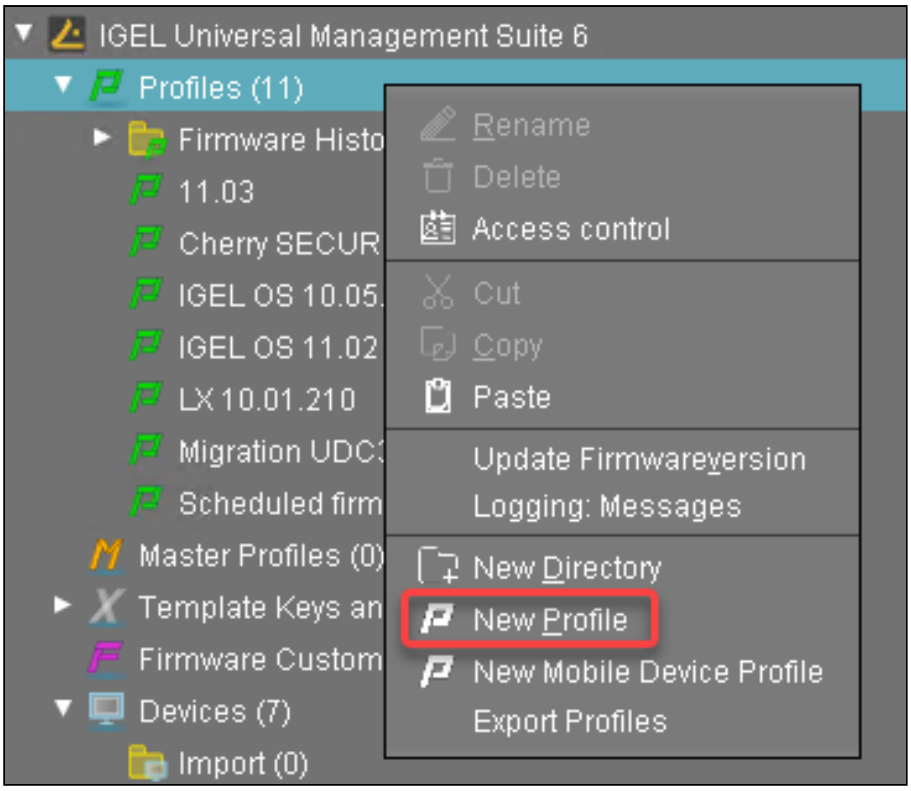
10. If you have custom applications, go to **Firmware Customization > Custom Application** and, for each custom application, deactivate **Autostart**. This is to prevent the custom application from interfering with the device's system before it can be tested properly.



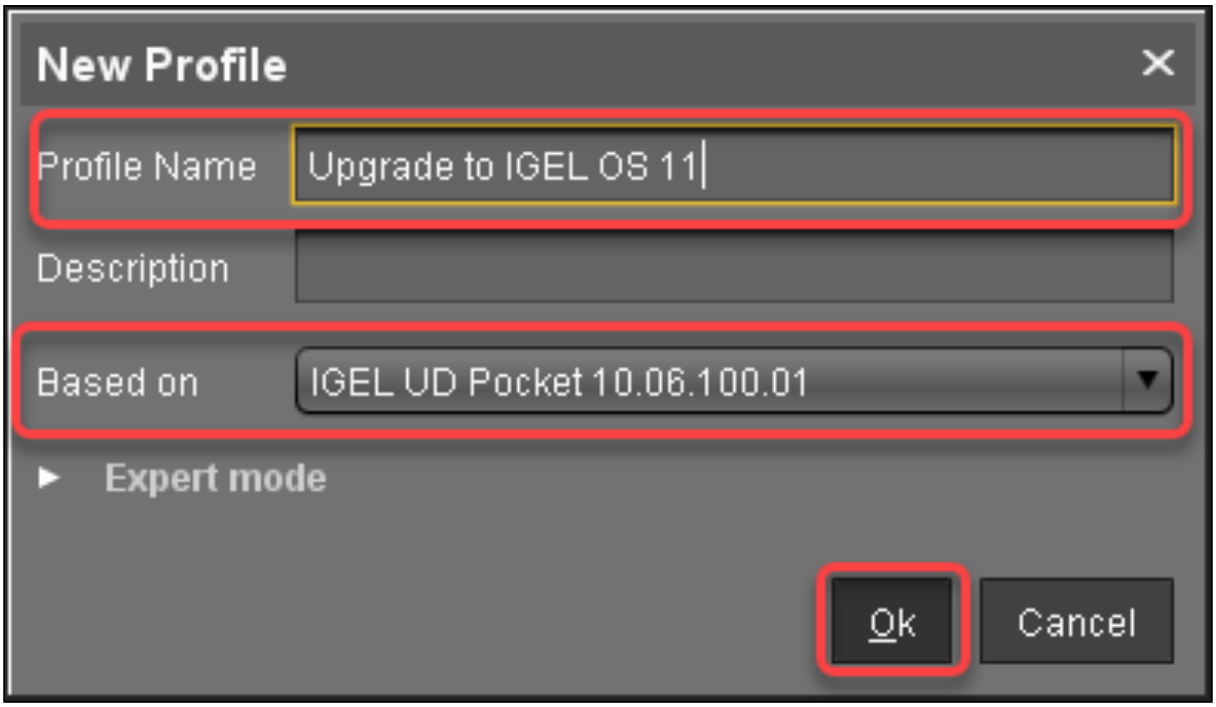
11. Click **Save**.

For Devices That Are Connected via ICG

1. In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.

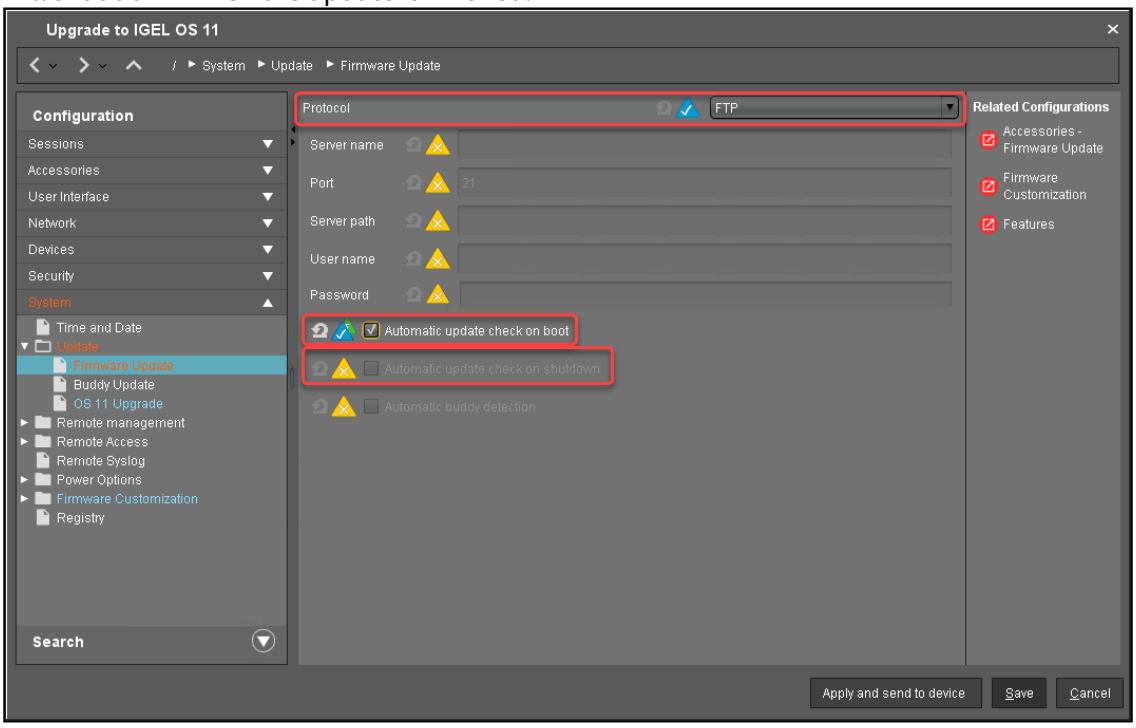


2. Enter the following data:
    - **Profile Name**: Name for the profile, e. g. "Upgrade to IGEL OS 11".
    - **Description**: Optional description for the profile.
    - **Based on**: Firmware version for the profile; select the current firmware of your devices, that is, "IGEL UD Pocket 10.06.100".
3. Click **Ok**.



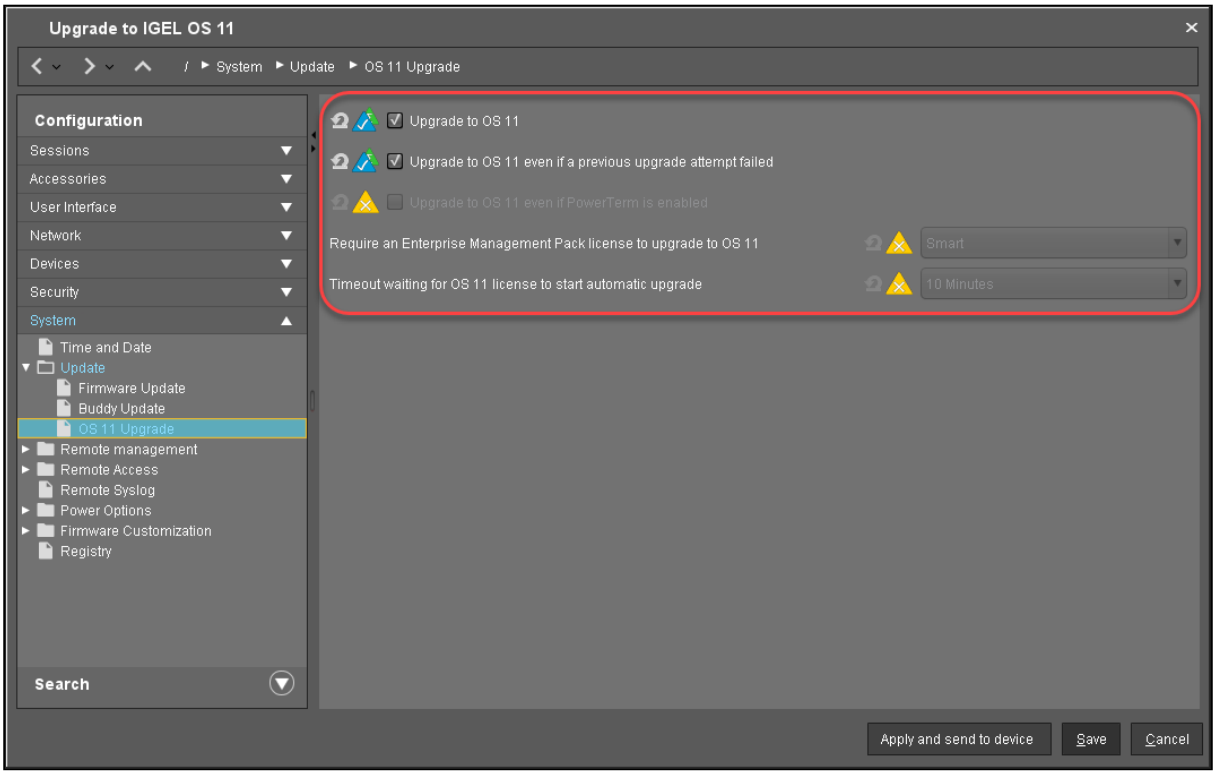
4. Go to **System > Update > Firmware Update** and change the settings as follows:
    - Select "FTP" as Protocol.
    - Activate **Automatic update check on boot**.

- Ensure that **Automatic update check on shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.

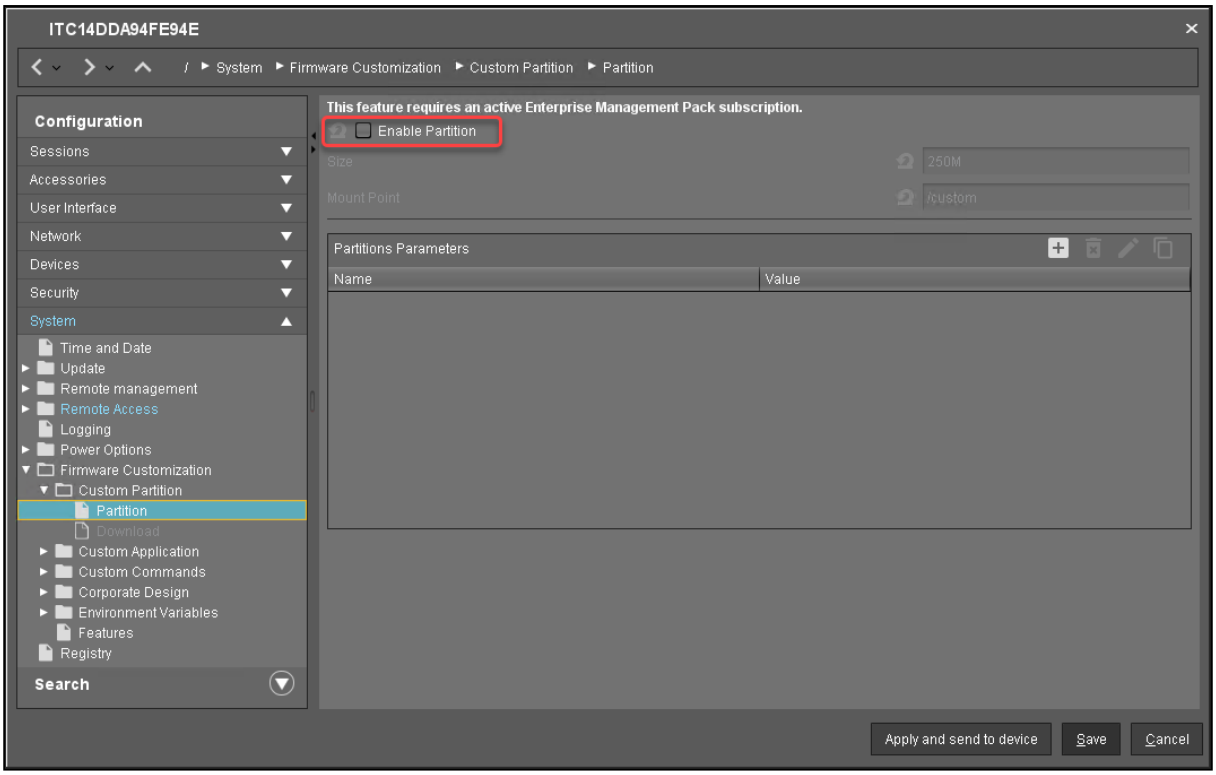


5. Go to **System > Update > Firmware Update > OS 11 Upgrade**.
6. Activate **Upgrade to OS 11**.
7. Make the following settings according to your needs:
   - If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. With this setting, the device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
   - If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though IGEL OS 11 does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
   - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
     - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When **Smart** is selected, and one of these features is activated, the upgrade is performed only if the device succeeded in fetching a license from an Enterprise Management Pack.
     - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if this license has been fetched, select **Always**.
     - If you want the device to upgrade to IGEL OS 11 without fetching a license from an Enterprise Management Pack, disregarding the features, select **Never**.
8. Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario. This setting prevents the device from

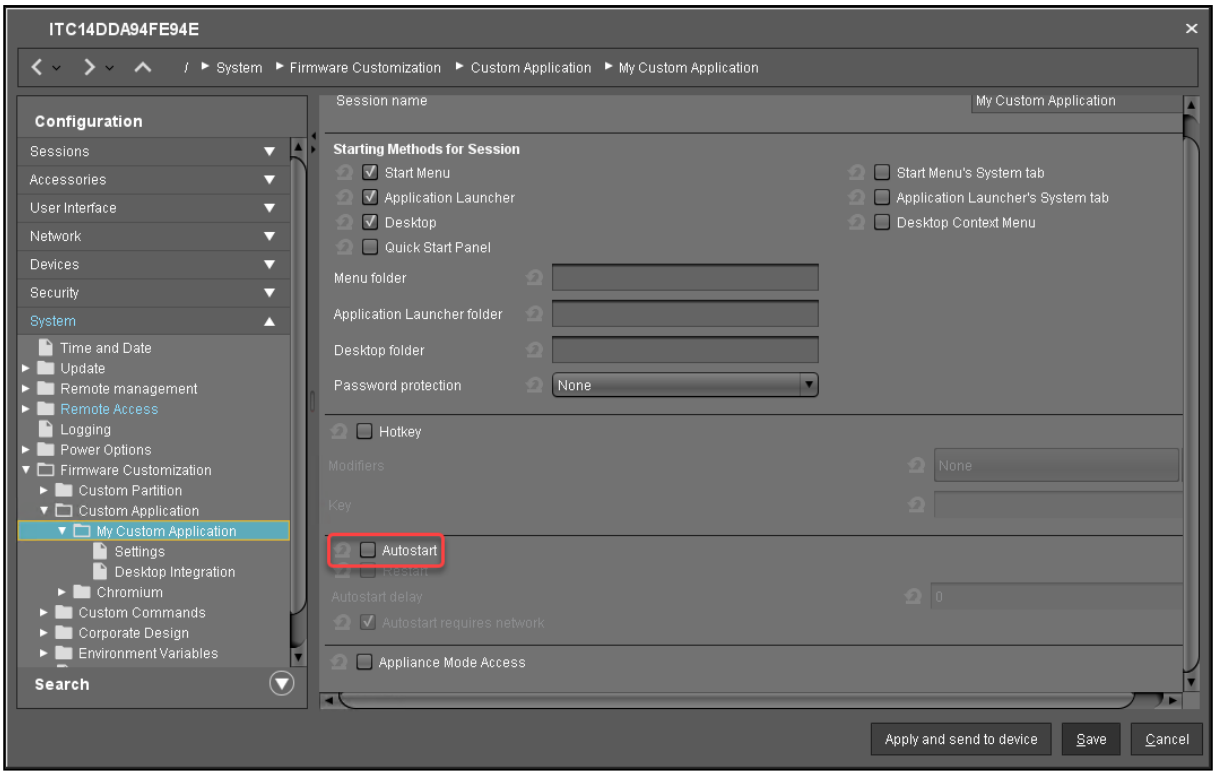
starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.



9. If you have a Custom Partition, go to **Firmware Customization > Custom Partition > Partition** and deactivate **Enable Partition**.



10. If you have custom applications, go to **Firmware Customization > Custom Application** and, for each custom application, deactivate **Autostart**. This is to prevent the custom application from interfering with the device's system before it can be tested properly.



11. Click **Save**.

Check List

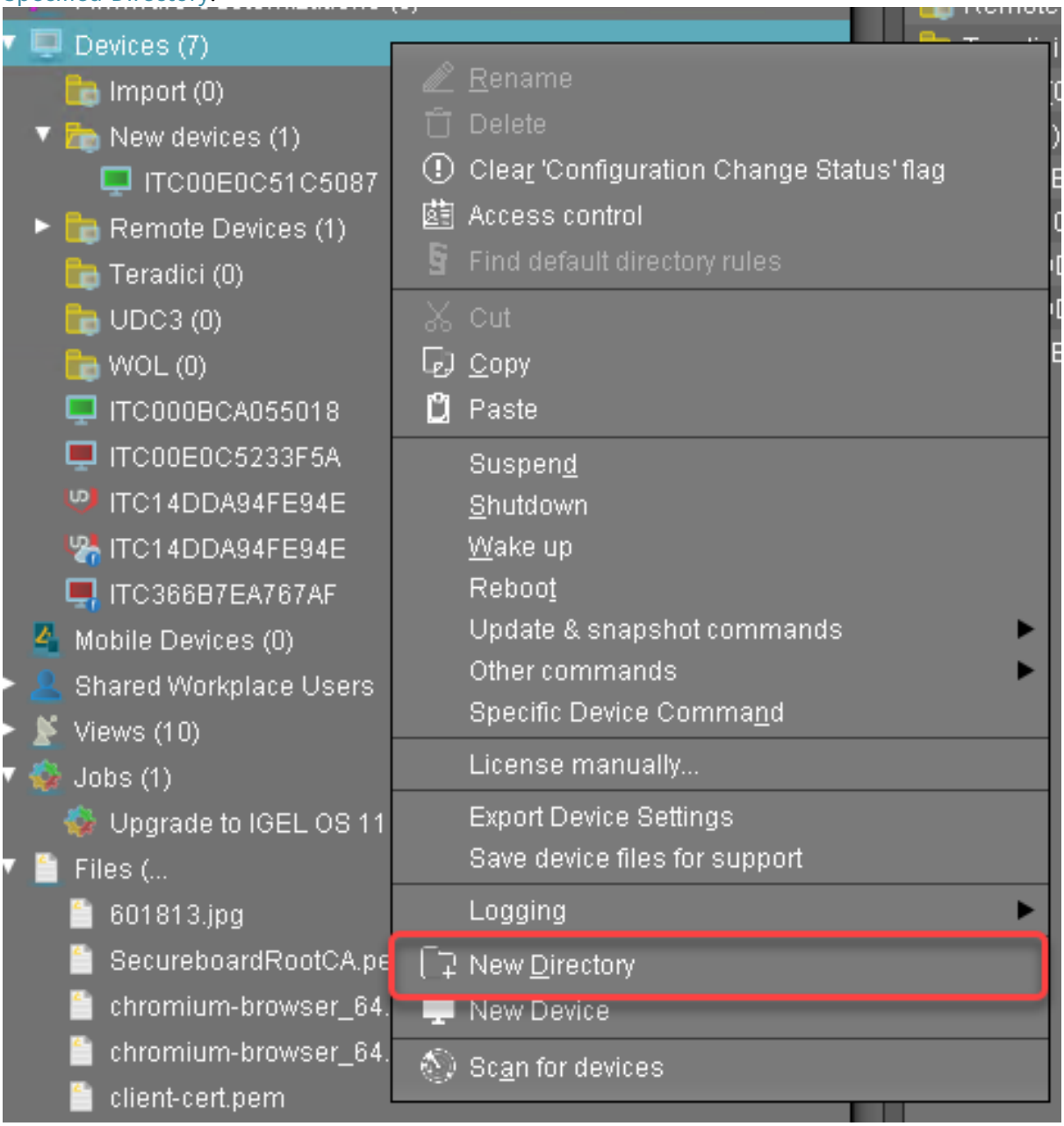
The upgrade profile is configured properly for your needs.

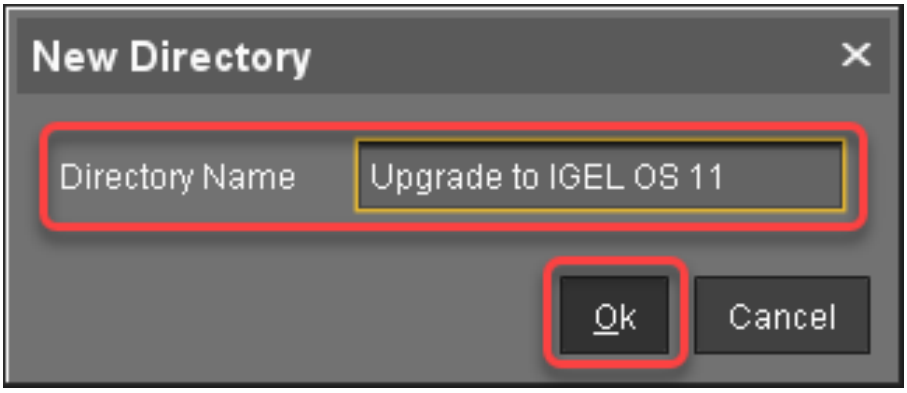
Next Step

>> Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices (see page 108)

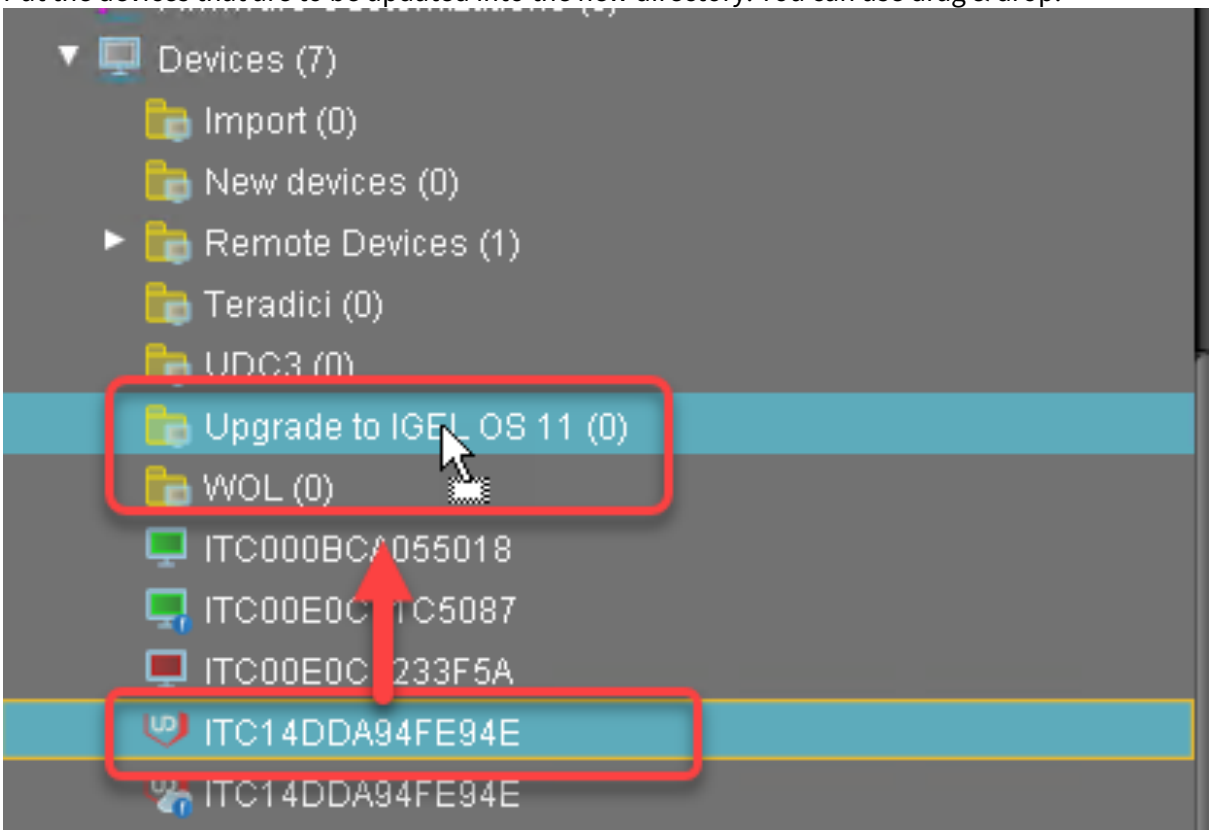
Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices

1. If you have not already created a directory as a distribution condition while setting up Automatic License Deployment (ALD): In the **Devices** node of the UMS structure tree, create a directory and name it "Upgrade to IGEL OS 11", for instance. For more information about distribution conditions, see https://kb.igel.com/en/igel-subscription-and-more/current/how-to-configure-the-distribution-conditions-of-li#HowtoConfiguretheDistributionConditionsofLicenses-DistributingLicensestoDevicesinaSpecifiedDirectoryDistributing-Licenses-to-Devices-in-a-Specified-Directory.

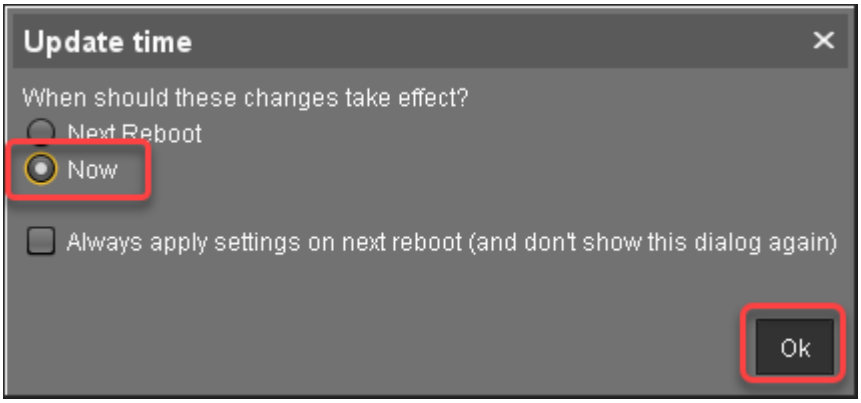




2. Put the devices that are to be updated into the new directory. You can use drag & drop.

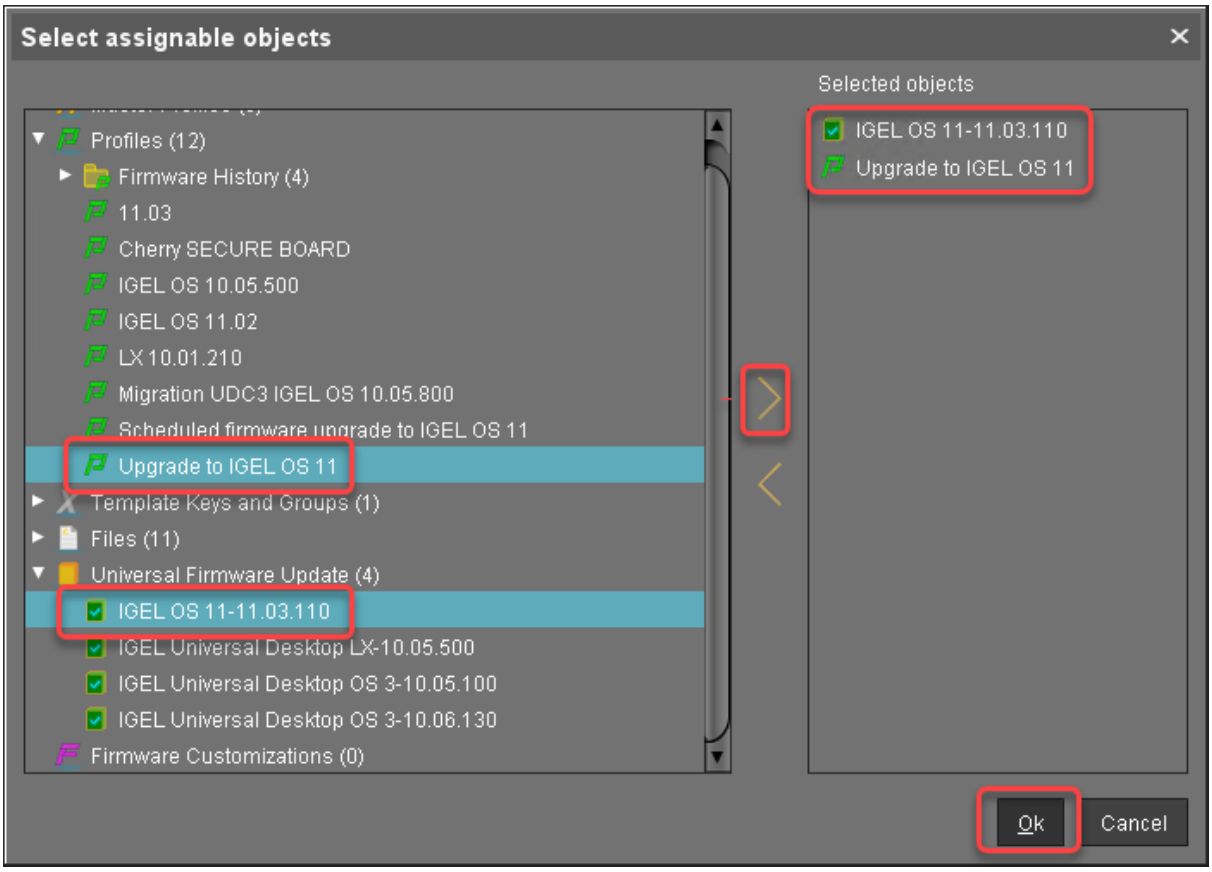


3. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change is communicated immediately to the device.

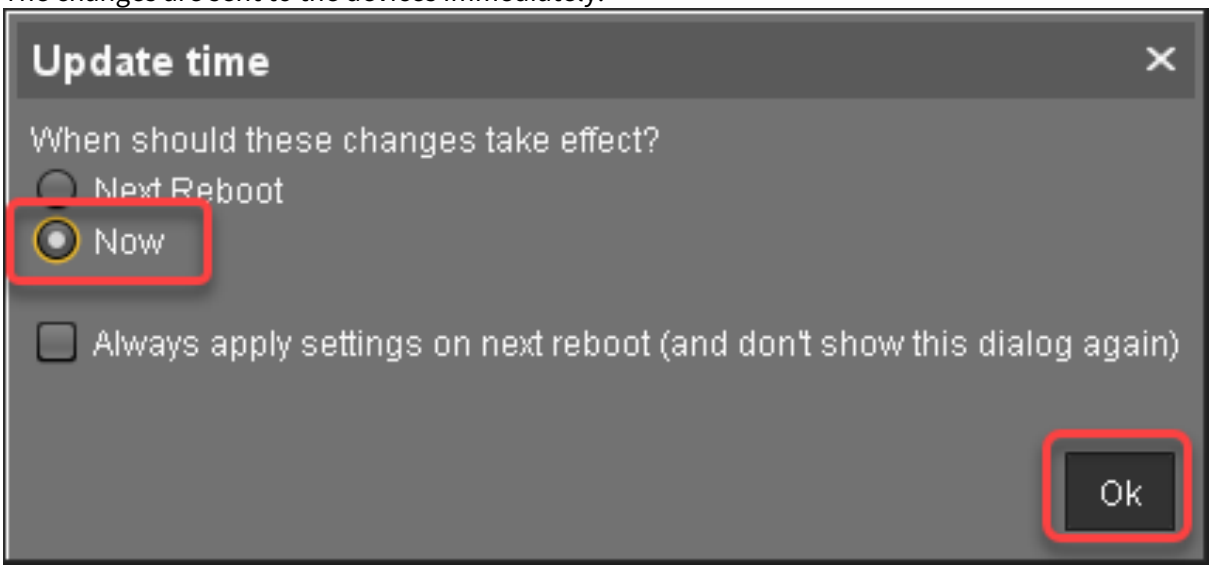


4. Select the directory and in the **Assigned objects** area, click .

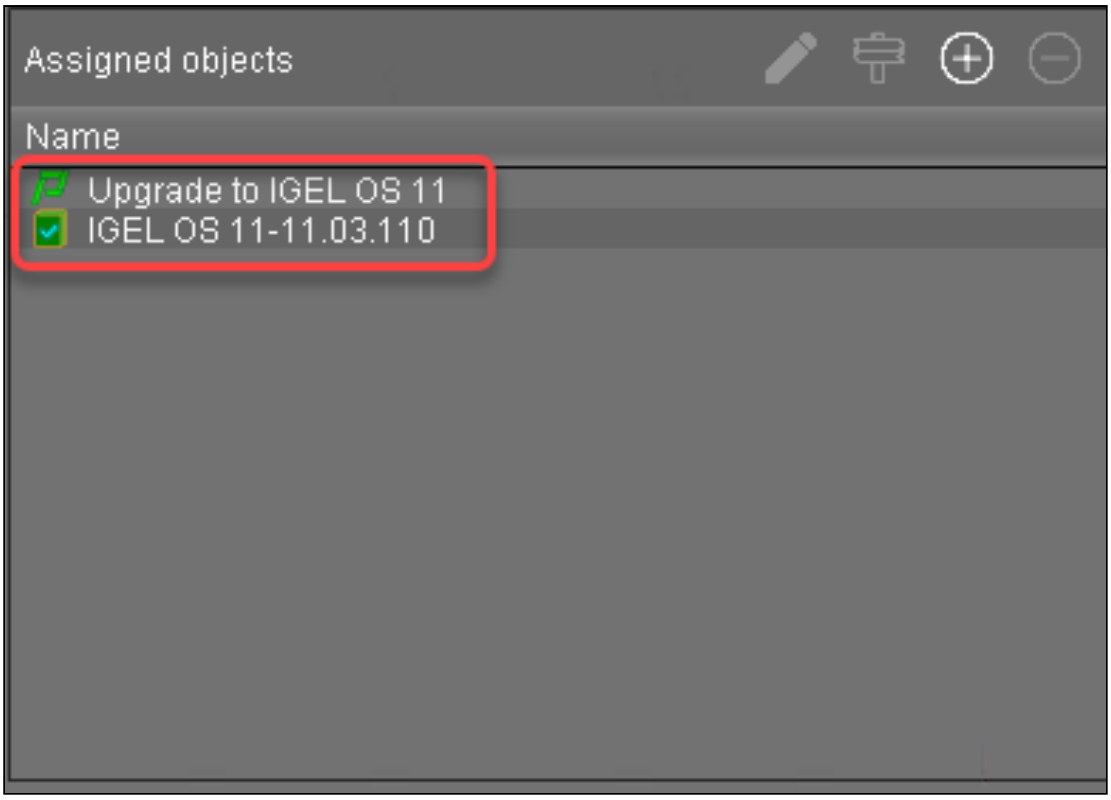
5. Assign the upgrade profile and the Universal Firmware Update for IGEL OS 11.03 to the directory and click **Ok**.



6. In the **Update time** dialog, select **Now** and click **Ok**.
   The changes are sent to the devices immediately.



In the **Assigned objects** area, the profile and the Universal Firmware Update are shown:



If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see Configuring the Distribution Conditions[25], section "Distributing Licenses to Devices in a Specified Directory".

Check List

The test devices are in a directory to which the upgrade profile and the Universal Firmware Update are assigned.

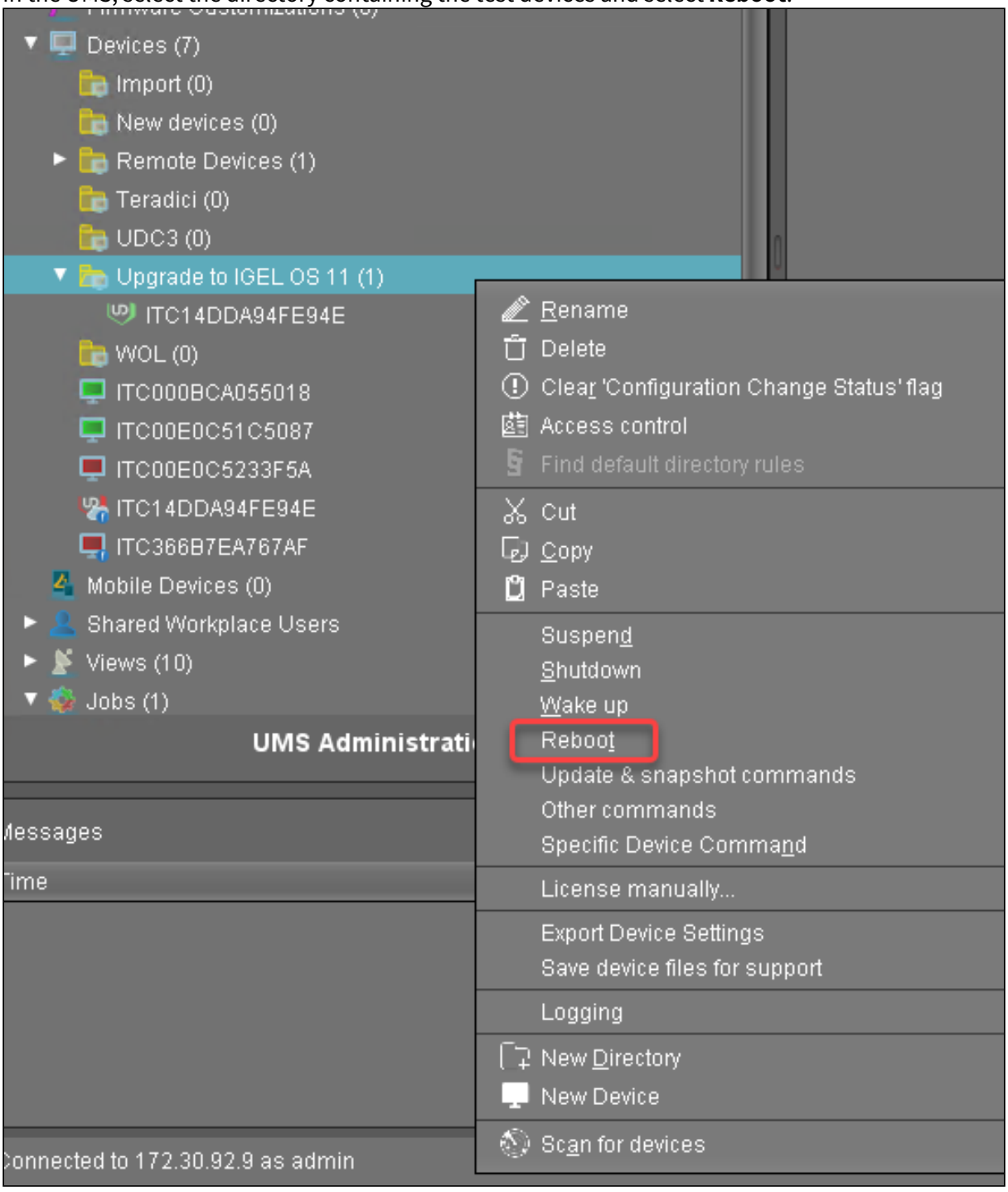
Next Step

>> Testing the Upgrade 1 (see page 113)

25. https://kb.igel.com/en/igel-subscription-and-more/current/how-to-configure-the-distribution-conditions-of-li

Testing the Upgrade

1. In the UMS, select the directory containing the test devices and select **Reboot**.



2. In the **Reboot devices** dialog, click **Reboot**.

   If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Creating an Upgrade Profile (see page 96), step 8.
   The parameter **Automatic update check on boot** makes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.
   The upgrade is completed.
3. Check whether all features and functions of your test devices are working as expected.

Check List

- All features and functions of your test devices are working as expected.

Next Step

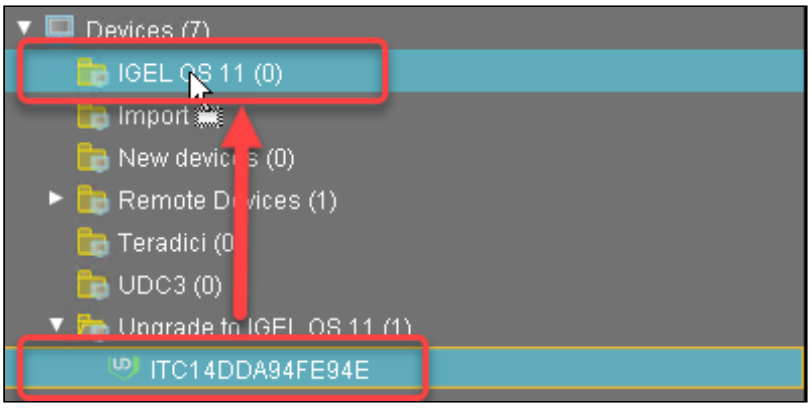
>> Unassigning the Upgrade Profile and the Universal Firmware Update (see page 116)

Unassigning the Upgrade Profile and the Universal Firmware Update

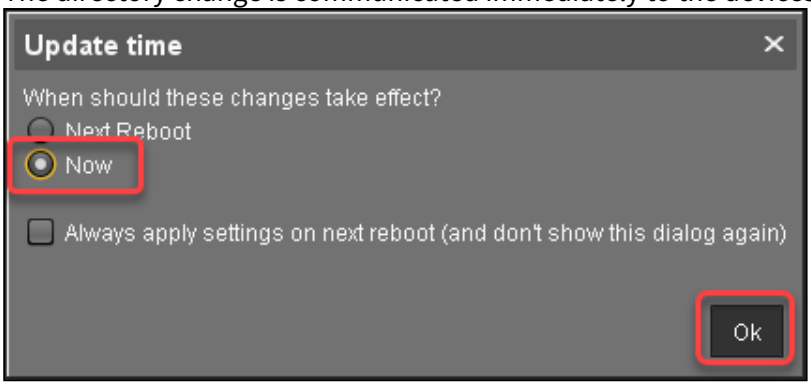
The upgrade profile and the Universal Firmware Update should be unassigned from the devices after they have been upgraded to IGEL OS 11 successfully.

To unassign upgrade profile and the Universal Firmware Update:

1. Move the devices to a different folder.



2. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change is communicated immediately to the devices.



   If a device had a Custom Partition before, it will be downloaded by the device and activated again.

Check List

If a device had a Custom Partition before:

- The Custom Partition has been downloaded by the device and activated.

Next Step

If some devices have a Custom Partition:

>> If Applicable: Restoring Custom Partition and Custom Application (see page 118)

If no device has a Custom Partition:

>> Upgrading All Devices (see page 119)

If Applicable: Restoring Custom Partition and Custom Applications

If a device had a custom partition before the upgrade, it has been downloaded and activated again after the upgrade profile has been unassigned; see Unassigning the Upgrade Profile and the Universal Firmware Update (see page 116). It cannot be ruled out that custom commands and the applications and drivers of a Custom Partition disturb your device's system. Therefore, it is very important to check the Custom Partition, the custom applications, and the device's basic functionality.

1. Test the Custom Partition and the custom applications. If errors should occur, modify the Custom Partition and the custom applications accordingly.
2. Check if all other functions are still working properly.

Check List

- The Custom Partition and the custom applications are enabled and can be used.
- All other functions are working properly.

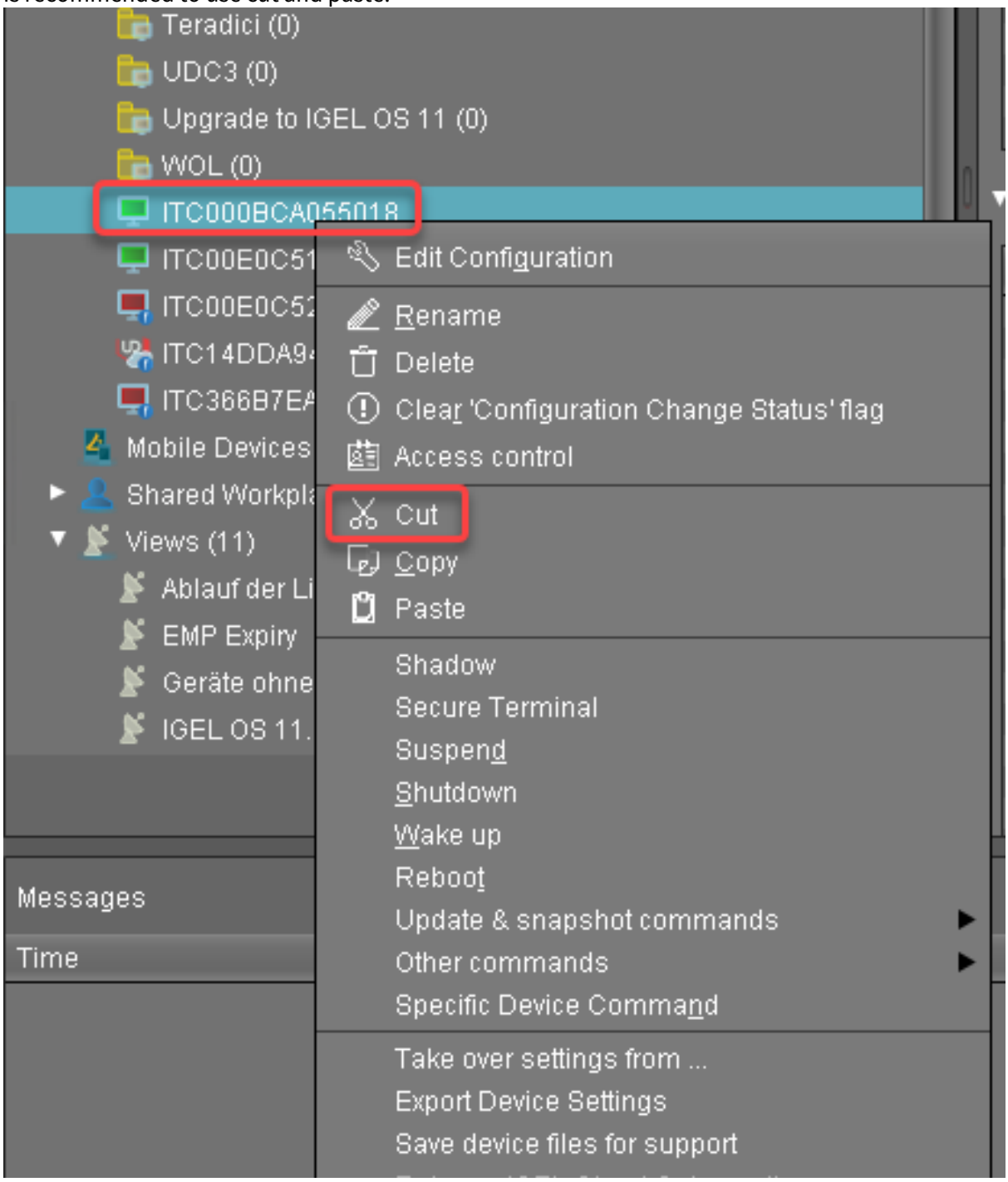
Next Step

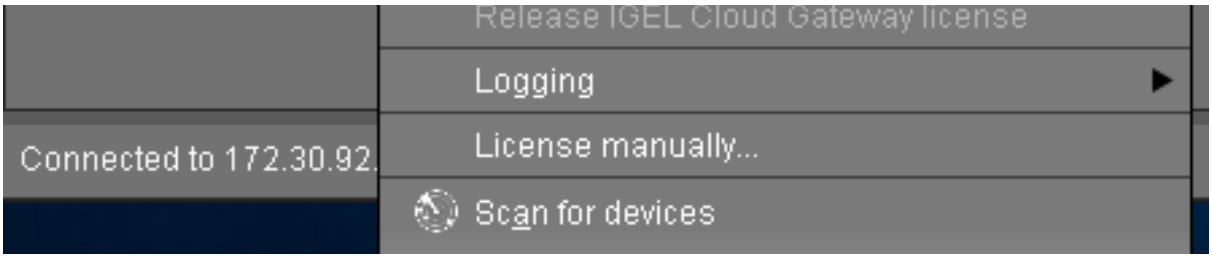
>> Upgrading All Devices (see page 119)

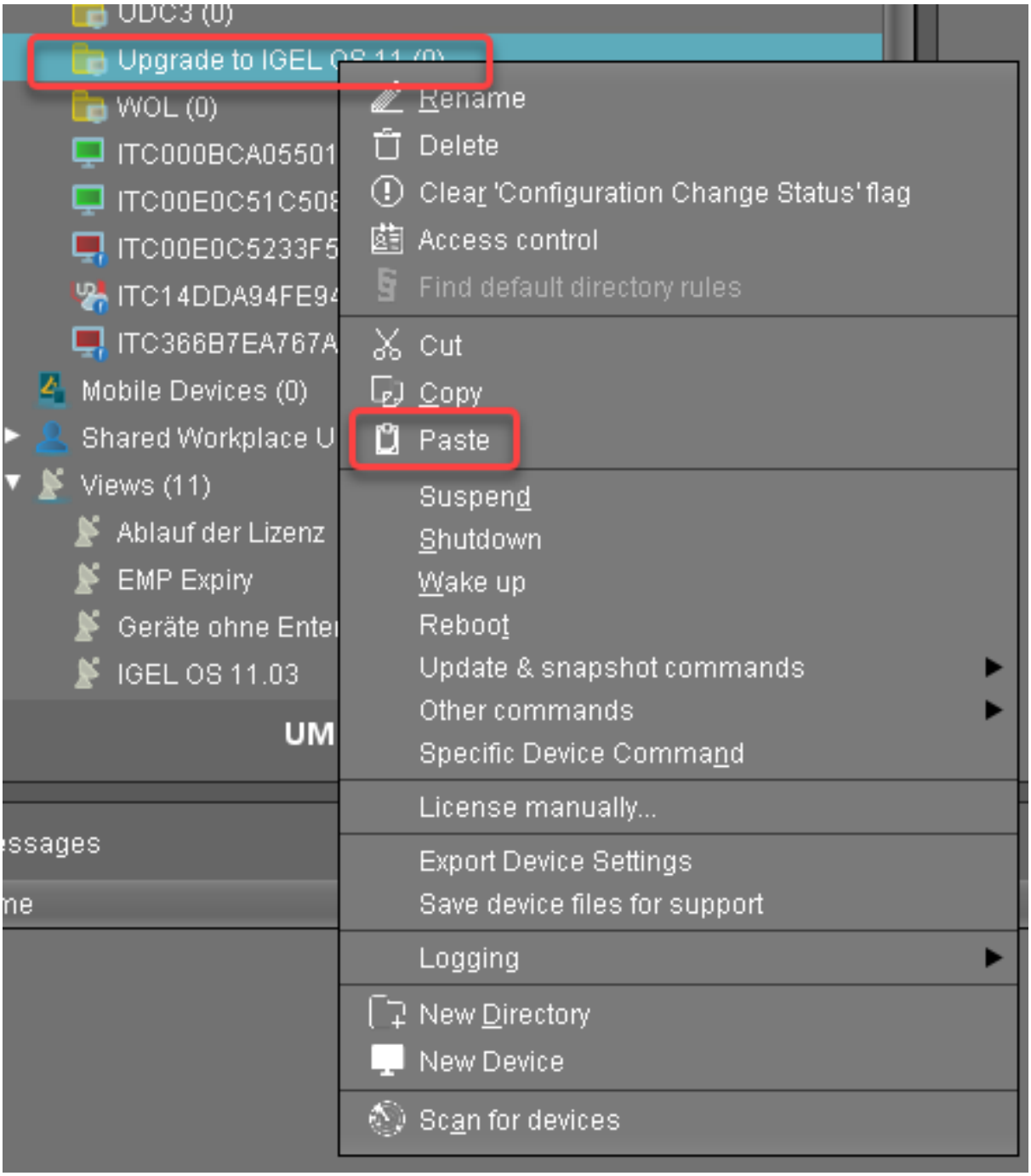
Upgrading All Devices

Assigning the Upgrade Profile and the Universal Firmware Update to the Devices

1. Put the devices that are to be upgraded into the directory you have created for the test devices. It is recommended to use cut and paste.

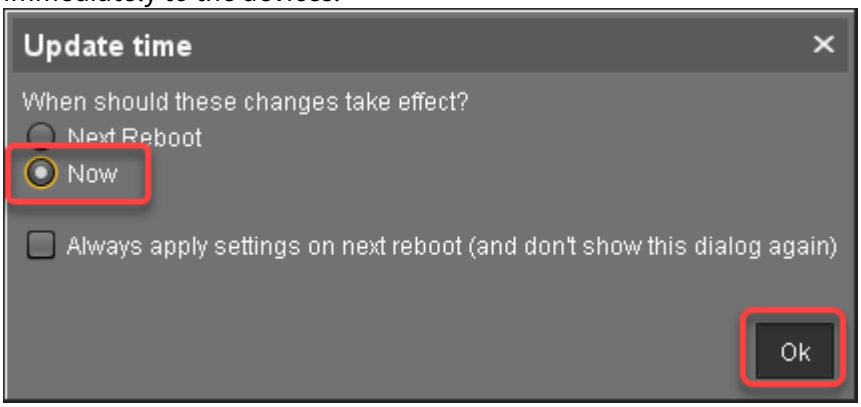



Release IGEL Cloud Gateway license
Logging
Connected to 172.30.92.
License manually...
Scan for devices

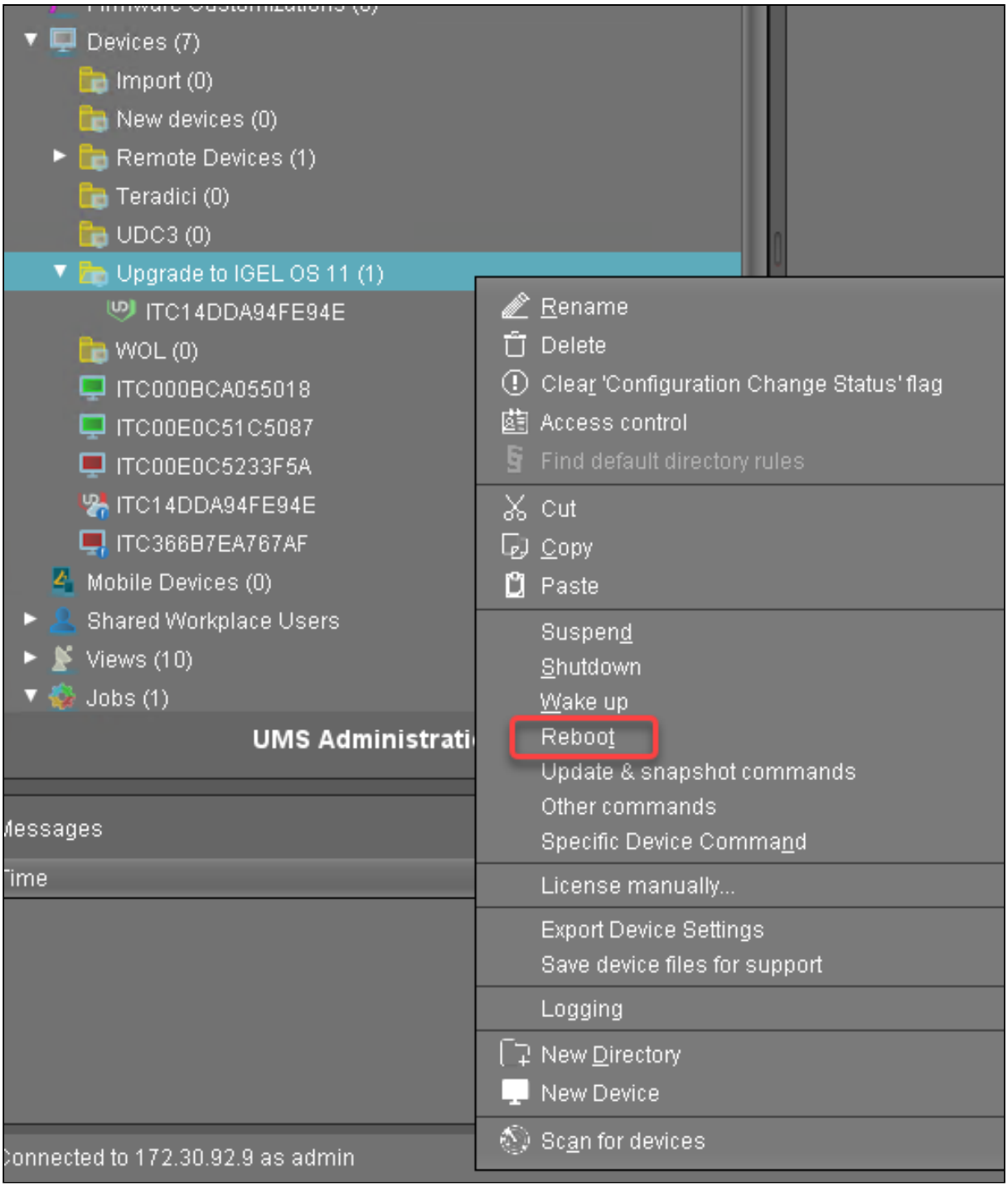


2. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change, the upgrade profile and the Universal Firmware Update are communicated

immediately to the devices.



3. In the UMS, select the directory with the devices and select **Reboot**.

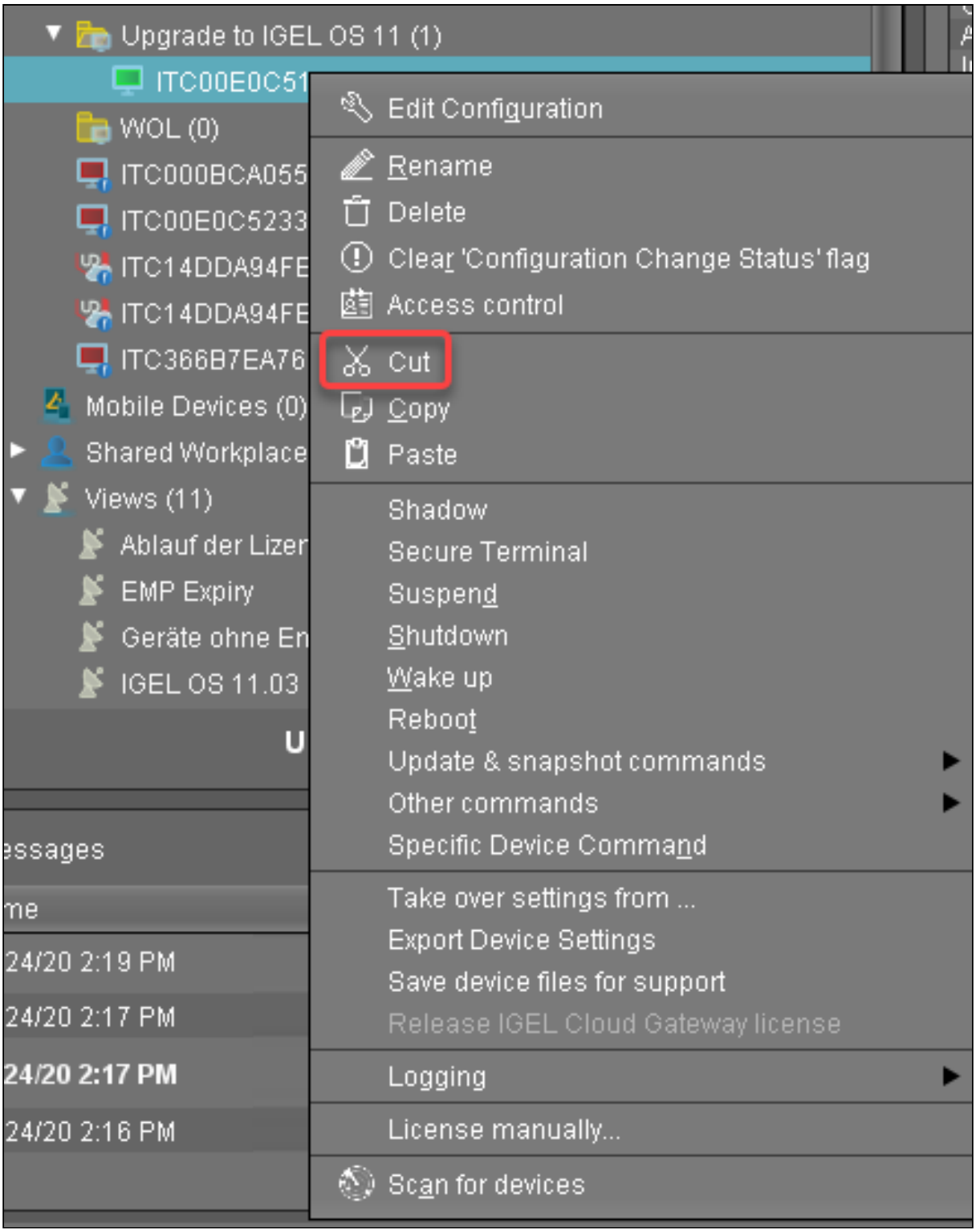


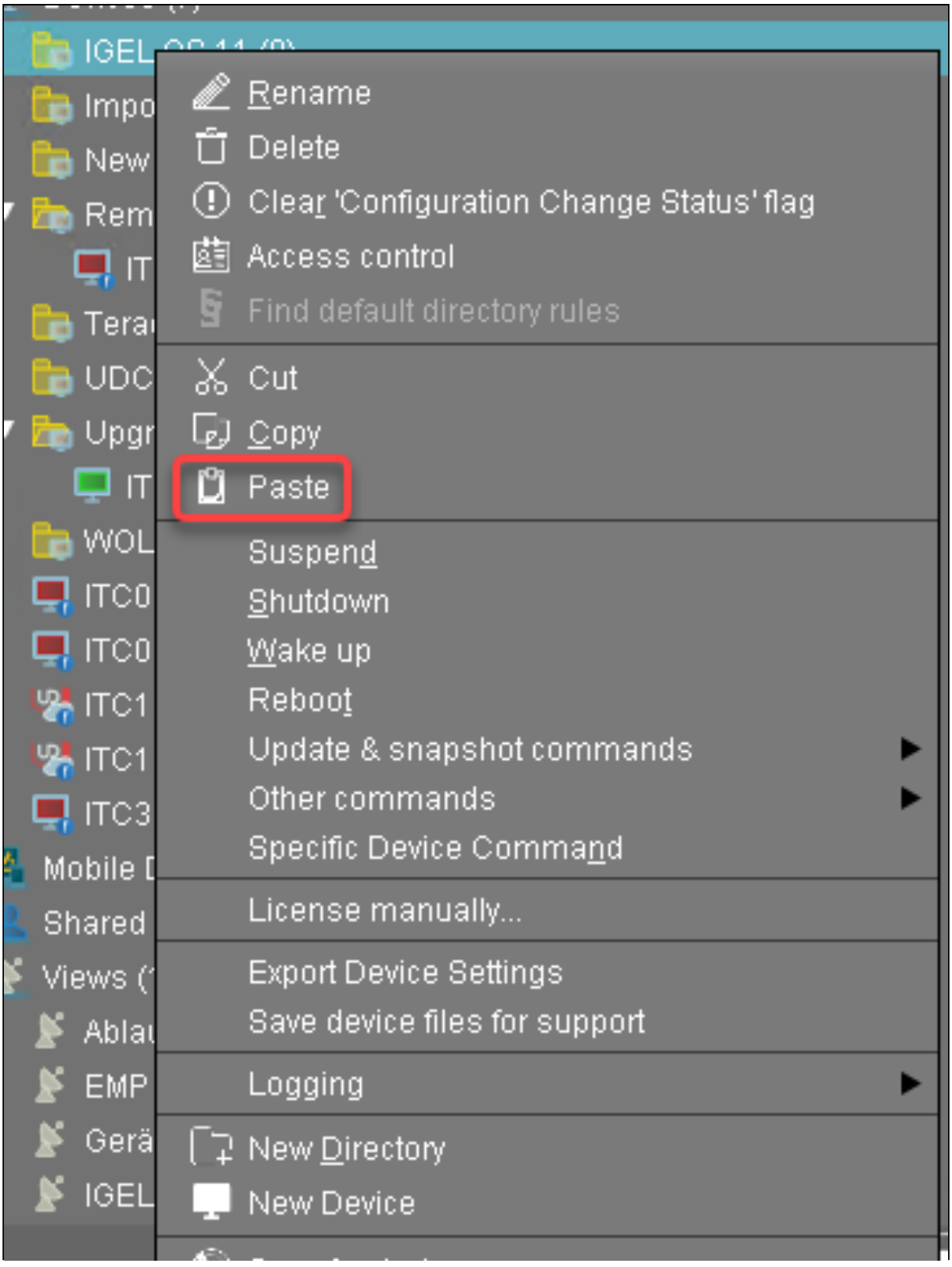
4. In the **Reboot devices** dialog, click **Reboot**.

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period a device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Creating an Upgrade Profile (see page 96), step 8.
The parameter **Automatic update check on boot** makes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

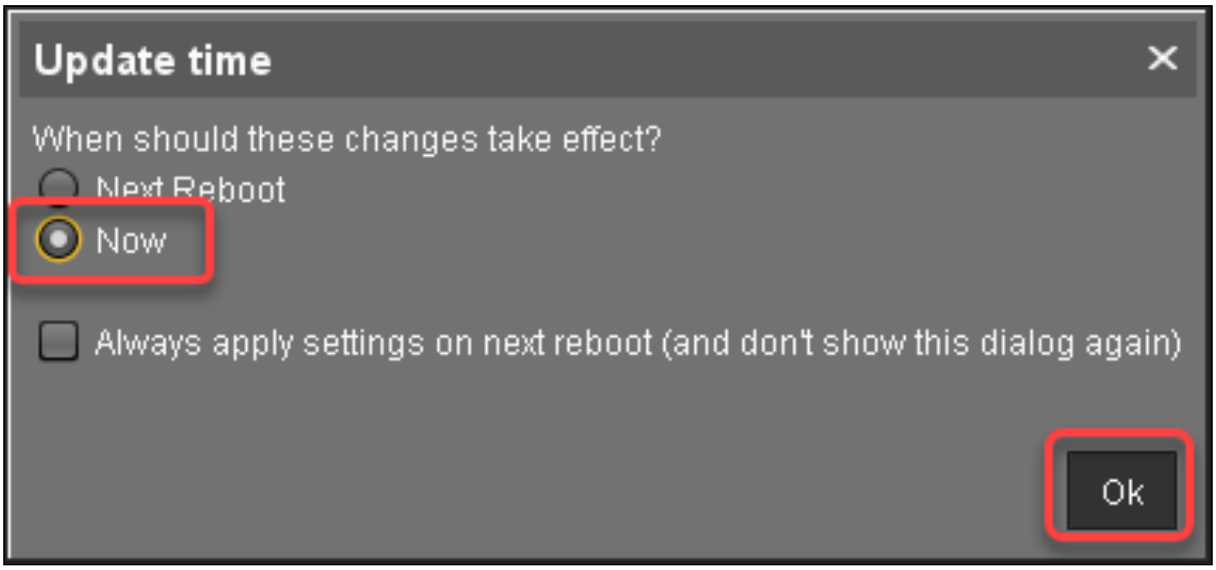
Unassigning the Upgrade Profile and the Universal Firmware Update

1. To unassign the upgrade profile and the Universal Firmware Update, move the devices to a different folder.


Upgrade to IGEL OS 11 (1)
ITC00E0C51
WOL (0)
ITC000BCA055
ITC00E0C5233
ITC14DDA94FE
ITC14DDA94FE
ITC366B7EA76
Mobile Devices (0)
Shared Workplace
Views (11)
Ablauf der Lizer
EMP Expiry
Geräte ohne En
IGEL OS 11.03
Edit Configuration
Rename
Delete
Clear 'Configuration Change Status' flag
Access control
Cut
Copy
Paste
Shadow
Secure Terminal
Suspend
Shutdown
Wake up
Reboot
Update & snapshot commands
Other commands
Specific Device Command
Take over settings from ...
Export Device Settings
Save device files for support
Release IGEL Cloud Gateway license
Logging
License manually...
Scan for devices


Rename
Delete
Clear 'Configuration Change Status' flag
Access control
Find default directory rules
Cut
Copy
Paste
Suspend
Shutdown
Wake up
Reboot
Update & snapshot commands
Other commands
Specific Device Command
License manually...
Export Device Settings
Save device files for support
Logging
New Directory
New Device

2. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change is communicated immediately to the device.



   If a device had a Custom Partition before the upgrade, it has been downloaded and activated again after the upgrade profile has been unassigned.
3. If applicable, restore the required custom applications; see If Applicable: Restoring Custom Partition and Custom Applications (see page 118).

Update Can be Canceled After Timeout

An ongoing update can be canceled by the user if the “network online” status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

Check List

- All devices have been upgraded to IGEL OS 11.
- All required functionality is available, including custom applications.

Upgrading from IGEL OS 10 to IGEL OS 11

- Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11 (see page 130)
- Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11 (see page 228)

Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11

This document describes how to upgrade any number of devices (UDC3) from IGEL OS 10 to IGEL OS 11.

IGEL OS 10.05.800 or higher is required for upgrading to IGEL OS 11. If you have an older version of IGEL OS 10, you need to update to version 10.05.800 or a higher version first.

Since a new licensing model has been introduced with IGEL OS 11, a license from an IGEL Workspace Edition Product Pack must be available for each device. If you have a valid maintenance for your devices, you can convert your existing UDC3 or UD Pocket Product Packs to Workspace Edition (WE) Product Packs; see How to Convert UDC3 or UD Pocket Licenses for Upgrading to IGEL OS 11[26].

The following methods of mass deployment are described here:

- Zero-Touch Deployment Using Universal Firmware Update 1 (see page 131): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using Universal Firmware Update. This method can be started immediately or as a scheduled job (wake up or reboot).
- Zero-Touch Deployment Using Buddy Update (see page 175): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using two devices as update buddies. This method can be started immediately or as a scheduled job (wake up or reboot).
- Zero-Touch Deployment Using a Scheduled Job[27]: Upgrade devices that are already running IGEL OS 10.05.800 (or higher) using a specific scheduled job.

26. https://kb.igel.com/knowledge-base-archive/current/archive-igel-licensing
27. https://kb.igel.com/en/igel-os/11.10.270/mass-deployment-using-a-scheduled-job

Zero-Touch Deployment Using Universal Firmware Update

This method is the most convenient way to upgrade from IGEL OS 10 to IGEL OS 11. The method uses the Universal Firmware Update feature of the UMS (Universal Management Suite) and a profile.

Read all the following chapters carefully and follow the instructions.

- Devices That Can Be Upgraded to IGEL OS 11 (see page 132)
- Important! Consider This Before Upgrading (see page 146)
- Preparing the Upgrade (see page 147)
- Testing the Upgrade (see page 152)
- Checking the Requirements (see page 157)
- Creating the Universal Firmware Updates (see page 158)
- Creating a Profile (see page 164)
- Deploying the Licenses (see page 169)
- Putting It All Together (see page 170)
- Executing the Upgrade (see page 173)

Devices That Can Be Upgraded to IGEL OS 11

Partner Solutions for Peripherical Devices
For further supported hardware from IGEL partners, e.g. headsets, see Peripherals Supported by IGEL OS 12.[28]

Core Requirements

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

  RAM size higher than 2 GB is recommended if you use any of the following:
  - Unified Communications optimizations (uses a client-side media engine)
  - High-resolution graphics output
  - More than two monitors

  With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Storage: Depends on the release version of IGEL OS 11. The details are listed below:
  - Up to IGEL OS 11.03: 2 GB minimum; ≥ 4 GB recommended
  - From IGEL OS 11.04 to IGEL OS 11.07: If the full feature set is applied, at least 2.4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher[29].
  - From IGEL OS 11.08 onwards: If the full feature set is applied, at least 4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher[30].
- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

Devices Supported by OSC and UD Pocket with IGEL OS 11

The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the minimum requirements will not function with IGEL OS: Any x86-64 hardware endpoint device that meets the IGEL-stated minimum hardware requirements for IGEL OS (for example, the processor speed and RAM) can be expected to work adequately with IGEL OS and should be considered a candidate for repurposing from

28. https://kb.igel.com/hardware/current/peripherals-supported-by-igel-os-12
29. https://kb.igel.com/en/igel-os/11.10.250/error-not-enough-space-on-local-drive-when-updatin
30. https://kb.igel.com/en/igel-os/11.10/error-not-enough-space-on-local-drive-when-updatin

another OS. With an IGEL OS subscription or active maintenance, customers can expect IGEL to make any necessary “best effort” to support, regardless of whether the endpoints in question are specifically listed within the IGEL Knowledge Base or elsewhere (e.g. on the IGEL Ready Showcase at https://www.igel.com/ready/showcase-categories/endpoints/).
For any devices not listed here or on the IGEL Ready showcase, you can contact your hardware vendor and request those devices to be added to the IGEL Ready program.
Integrated drivers and supported peripherals are listed in the Third-Party Hardware Database[31]. For more solutions compatible with IGEL OS, see Peripherals Supported by IGEL OS 12[32].

HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[33] to get information on which device models are available with pre-installed IGEL OS.

For some of the devices listed here, Flash memory must be extended to ≥ 2 GB. For these devices, an appropriate note is added.

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft’s 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see *Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot*.[34]

[Fn] keys may not work on some supported and listed laptop/notebook models.

ADS-Tec

31. https://www.igel.com/linux-3rd-party-hardware-database/
32. https://kb.igel.com/hardware/current/peripherals-supported-by-igel-os-12
33. https://www.igel.com/technology-partners/
34. https://kb.igel.com/security-safety/current/secured-core-pcs-microsoft-3rd-party-uefi-certific

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DVG-VMT9010	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9012	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9015	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9112	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

Advantech

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L*	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L*	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrial PC/ Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

Dell / Wyse

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Notes
5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100	
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100	
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140	
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100	
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100	
Latitude 5510	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100	Wake-on-LAN functionality is not supported.
Optiplex 3000	Thin Client	4 GB	32 GB	Intel Celeron N5105	11.08.200	

Dynabook

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Portegé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portegé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

Elo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

Fujitsu

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100		
HP t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	Intel AC9260	
HP t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100		
HP t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100		
HP t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100		

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100		
HP t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	Intel AC9260 Realtek RTL8852AE	This model is not supported with HP USB-C Essential G5 Dock
HP t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	Intel AC9260 Realtek RTL8852AE	
HP mt46	Mobile Thin Client	8 GB	32 GB	AMD Ryzen 3 PRO 4450U	11.07.100		Excluding support for WWAN and Wake-on-LAN (both features are planned)
HP Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	Realtek RTL8852BE	
HP Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.08.330) Excluding support for Wake-on-LAN (feature is planned) Excluding support for built-in fingerprint sensor
				AMD Ryzen 5 5625U	11.08.330		
HP t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	Realtek RTL8852AE	

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	Realtek RTL8852CE (Supported as of 11.09.150)	
HP Pro mt440 G3	Mobile Thin Client	8 GB	128 GB	Intel Celeron 7305	11.08.440	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.09.260)
HP Elite t755	Thin Client	8 GB	128 GB	AMD Ryzen Embedded V2546	11.09.260	Realtek RTL8852CE	This model offers no USB-C docking support

HP Docking Stations

Name	Supported from IGEL OS Version	Notes
HP USB-C Docking Station G5	11.08.230	
HP USB-C G5 Essential Dock	11.08.290	Not supported with HP t640

Intel

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

Lenovo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	Intel AC9260	11.04.100	
		8 GB	128 GB	AMD A4-9120e	QCA6174 802.11ac	11.04.100	
ThinkCentre M75n	Desktop PC	8 GB	256 GB	AMD Ryzen 3 Pro 3300U	Intel AC9260	11.05.100	
ThinkCentre M70q Gen1	Desktop PC	16 GB	256 GB	Intel i5-10500t	Comet Lake PCH CNVi WiFi, Intel	11.05.100	
ThinkCentre M70q Gen 3	Desktop PC	16 GB	256 GB	Intel Core i5-12500T	Intel AX201	11.08.240	
ThinkCentre M75q Gen 2	Desktop PC	4 GB	128 GB	AMD Ryzen 3 Pro 5350GE	Intel AX200	11.08.240	
K14 AMD Gen 1	Laptop/ Notebook	8 GB	256 GB	AMD Ryzen 5 PRO 5650U	Mediatek MT7921	11.08.240	
ThinkPad L14 AMD Gen 1	Laptop/ Notebook	64 GB	1 TB	AMD Ryzen 7 Pro 4750U	Wi-Fi 6 AX200, Intel	11.05.100	
14w	Laptop/ Notebook	4 GB	64 GB	AMD A6-9220C	QCA6174 802.11ac	11.05.100	
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkCentre Neo50q Gen 4	Thin Client	8 GB	256 GB	Intel Core i3-1215U	Wi-Fi 6 RTL8852BE	11.08.240	
		4 GB	256 GB	Intel Celeron 7305	Wi-Fi 6 AX201		
K14 Intel Gen 1	Laptop/ Notebook	16 GB	256 GB	Intel Core i5-1135G7	Intel AX210 WiFi / BT combo	11.08.290	
ThinkPad L14 Intel Gen 3	Laptop/ Notebook	16 GB	512 GB	Intel Core i5-1235U	Intel Wi-Fi 6 AX201 2x2 AX vPro	11.08.330	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360
ThinkEdge SE10	Thin Client	8 GB	1 TB	Intel Atom x6425RE	MediaTek MT7921LEN	11.08.360	
			256 GB	Intel Atom x6214RE	Intel AX210	11.08.360	
ThinkPad L14 AMD Gen 4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L15 AMD Gen4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L14 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L15 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkPad L13 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX201	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN
ThinkPad L13 AMD Gen 4	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 3 PRO 7330U	AMD RZ616	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN

Lenovo Docking Stations

Name	Supported from IGEL OS Version
ThinkPad USB-C Hybrid Dock	11.07.100
IOBOX	11.07.100
Universal USB-C Dock	11.08.440

Lenovo USB-C to Ethernet Adapter

Name	Supported from IGEL OS Version	Supported with
USB-C to Ethernet Adapter	11.09.260	• ThinkPad L13 Intel Gen4 • ThinkPad L14 AMD Gen4

LG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CK550**	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CK560**	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
38CK950	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
38CK900	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
34CN650	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360
24CR670	All in One	4 GB	16 GB	Intel Celeron N5105	11.09.110
34CR650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210
27CQ650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210

LG Docking Stations

Name	Supported from IGEL OS Version
LG USB Multi Port Hub	11.09.100

OnLogic

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/ Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

Onyx Healthcare

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

Pepperl+Fuchs

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
BTC12N	Industrial Box Thin Client	4 GB	32 GB	Intel Apollo Lake N4200	11.09.100
BTC14N	Industrial Box Thin Client	4 GB	32 GB	AMD Ryzen Embedded V1202B	11.09.100

Rein Medical

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

Secunet

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

USB Memory Sticks That Can Be Used as UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133

Transcend

Name
Powered by IGEL UD Pocket[35]
Powered by IGEL UD Pocket 2[36]

Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

35. https://kb.igel.com/hardware/current/ud-pocket-powered-by-igel-ud-pocket
36. https://kb.igel.com/hardware/current/ud-pocket-2-powered-by-igel-ud-pocket-2

Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

For some features, more than 2 GB RAM is required. Example: if you use dual monitor environments, a virtual machine must have at least 8 GB RAM.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

- Delock Adapter DP 1.2 to DVI does not work.

** When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider Important! Consider This Before Upgrading[37].

37. https://kb.igel.com/en/igel-os/11.10.250/important-consider-this-before-upgrading

Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

Existing partitions: Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

No Downgrade
You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

Features (e.g. Clients)
IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions
The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

Custom Commands
The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

Power Supply
Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

Network
All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard or mobile broadband.

When you have considered everything that is relevant, continue with Preparing the Upgrade (see page 147).

Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

To prepare the upgrade, perform the following steps:

1. Preparing the UMS (see page 148)
2. Adjusting the Setup (see page 149)
3. Deploying a License (see page 150)
4. Configuring the Update Source (see page 151)

Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see *Universal Management Suite > UMS Reference Manual > UMS Installation and Update > IGEL UMS Update*.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter *Universal Management Suite > UMS Reference Manual > Registering IGEL OS Devices on the UMS Server.*

When the UMS is ready, continue with Adjusting the Setup (see page 149).

Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Firmware Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
    - Activate **Upgrade to OS 11**.

> When **Upgrade to OS 11** is activated, the device checks for a Workspace Edition license and stops checking for a legacy UDC3 or UD Pocket license. Therefore, in the UMS, it is displayed as an unlicensed device until a Workspace Edition license has been deployed.

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
    - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
    - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see Zero-Touch Deployment Using Universal Firmware Update (see page 131), Zero-Touch Deployment Using Buddy Update (see page 175) and Mass Deployment Using a Scheduled Job (see page 283)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

3. Click **Apply**.

When the Setup is adjusted, continue with Deploying a License (see page 150).

Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality; see

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality
- If one of the following features is used, one Enterprise Management Pack license is required:
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

→ Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see https://kb.igel.com/en/igel-subscription-and-more/current/manual-license-deployment-for-igel-os.
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, seehttps://kb.igel.com/en/igel-subscription-and-more/current/setting-up-automatic-license-deployment-ald.
- Download three demo licenses from https://www.igel.com/download/ .

When the device has a license, continue with Configuring the Update Source[38].

38. https://kb.igel.com/en/igel-subscription-and-more/current/deploying-the-license-on-the-device

Configuring the Update Source

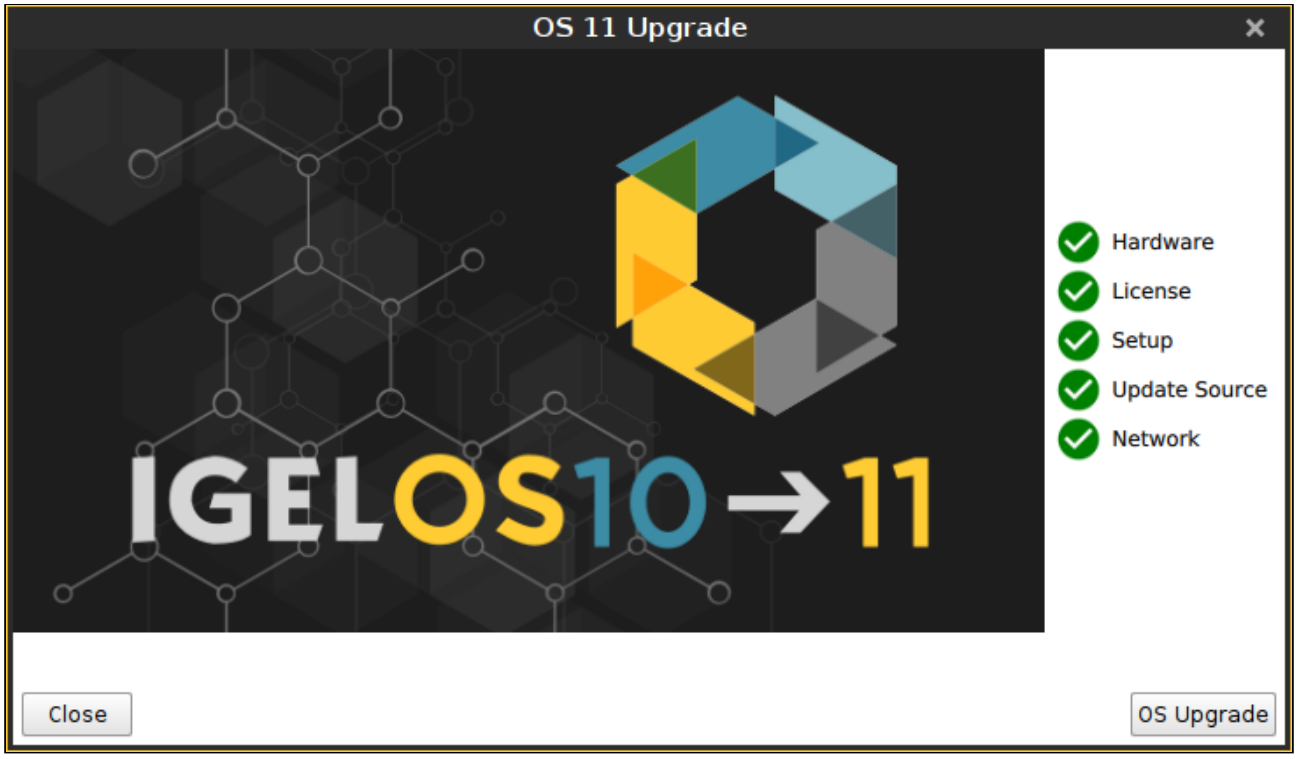
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update Settings for IGEL OS (see page 2056) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue withTesting the Upgrade (see page 152).

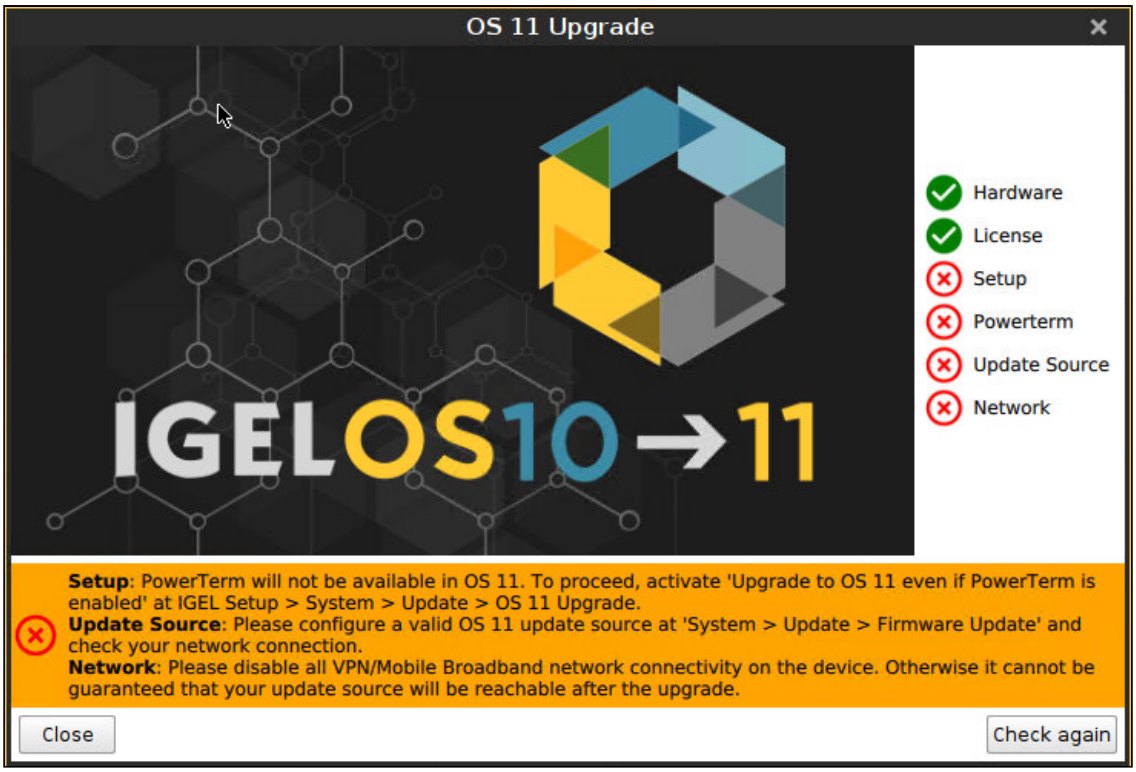
Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

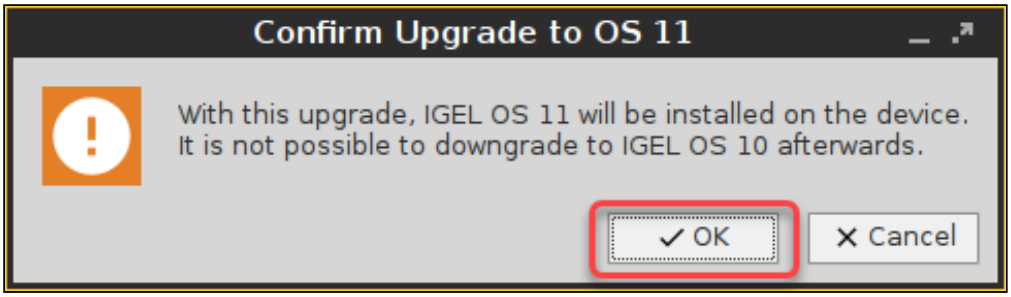


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:
   - If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
   - If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**, and you can start the upgrade.

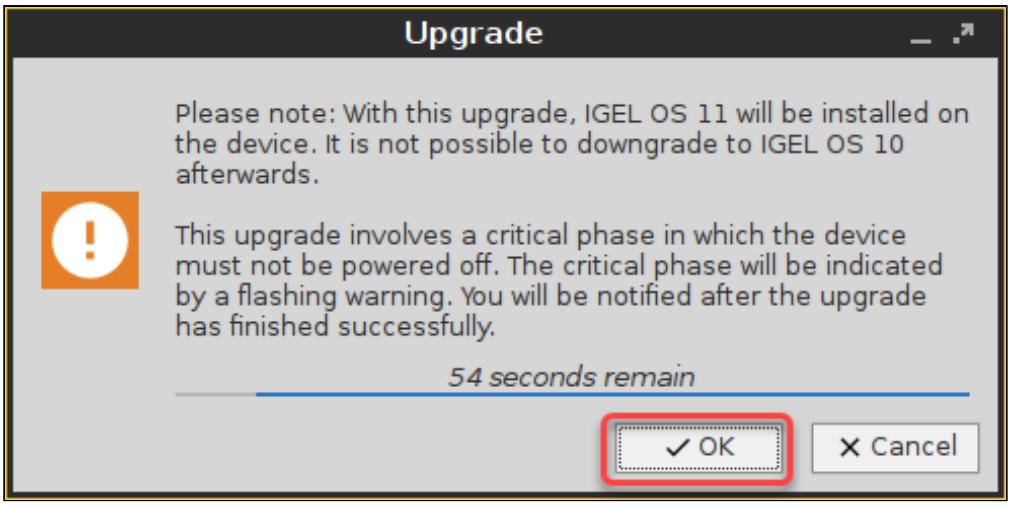


When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



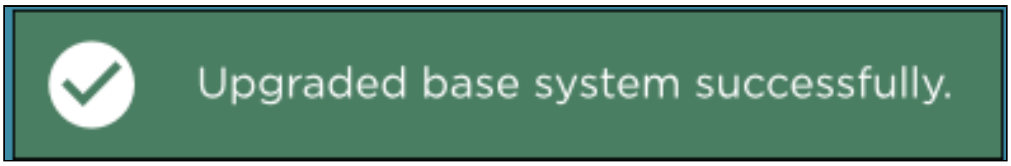
A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



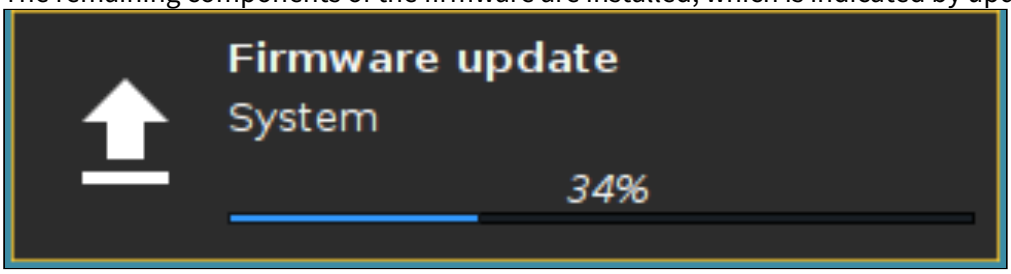
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window shows the progress.

During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.

When the base system is upgraded successfully, a message is shown.



The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:

After a few seconds the device reboots into IGEL OS 11.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 157).

Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The appropriate IGEL OS 10 firmware version (10.05.700 or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate IGEL OS 10 firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with Creating the Universal Firmware Updates (see page 158).

Creating the Universal Firmware Updates

For detailed information, see the chapter *Universal Management Suite > UMS Reference Manual > Universal Firmware Update in the IGEL UMS*.

If you use the *Universal Management Suite > UMS Extensions > IGEL UMS High Availability (HA)*, note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

1. Create a Universal Firmware Update for IGEL OS 10.05.800 (or higher).
2. After you have created the Universal Firmware Update for IGEL OS 10.05.800 (or higher), create a Universal Firmware Update for IGEL OS 11.

The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see Executing the Upgrade (see page 173).

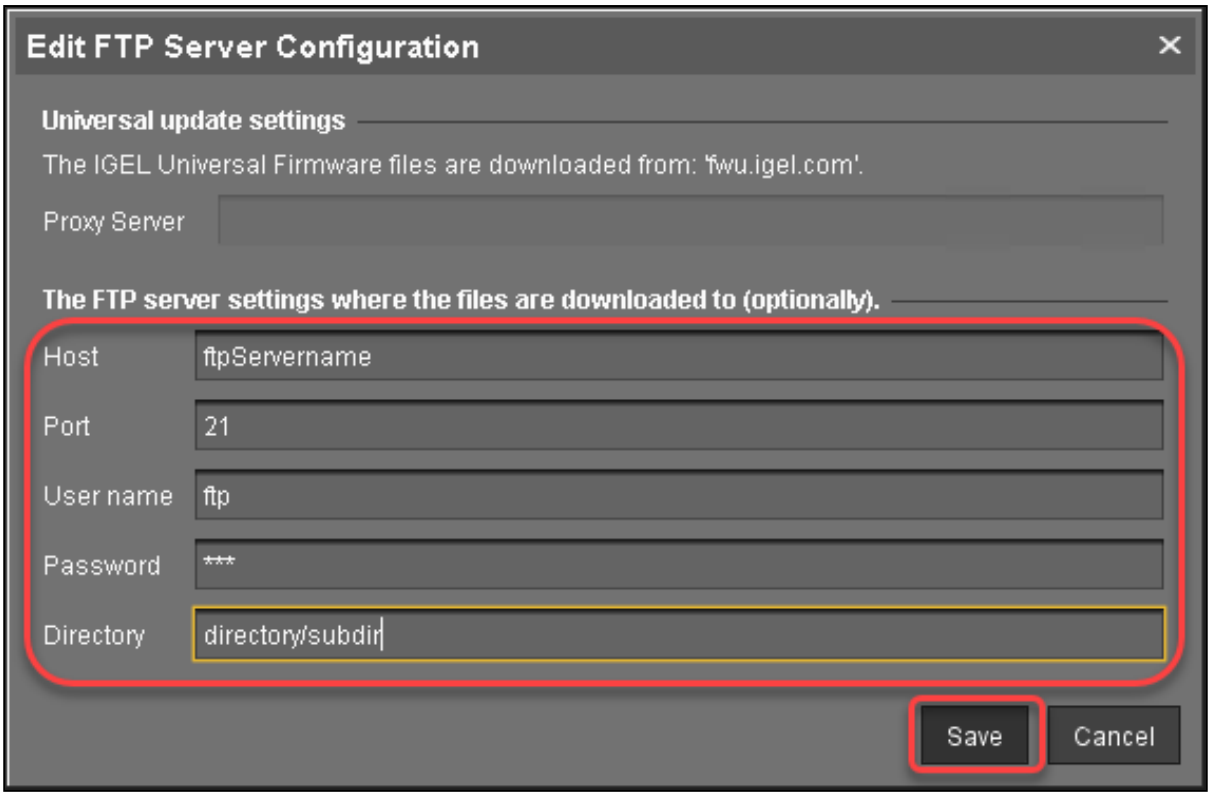
Configuring the Universal Firmware Update for ICG

If you are using IGEL Cloud Gateway (ICG), an FTP server that is accessible to all devices must be configured as an update source.

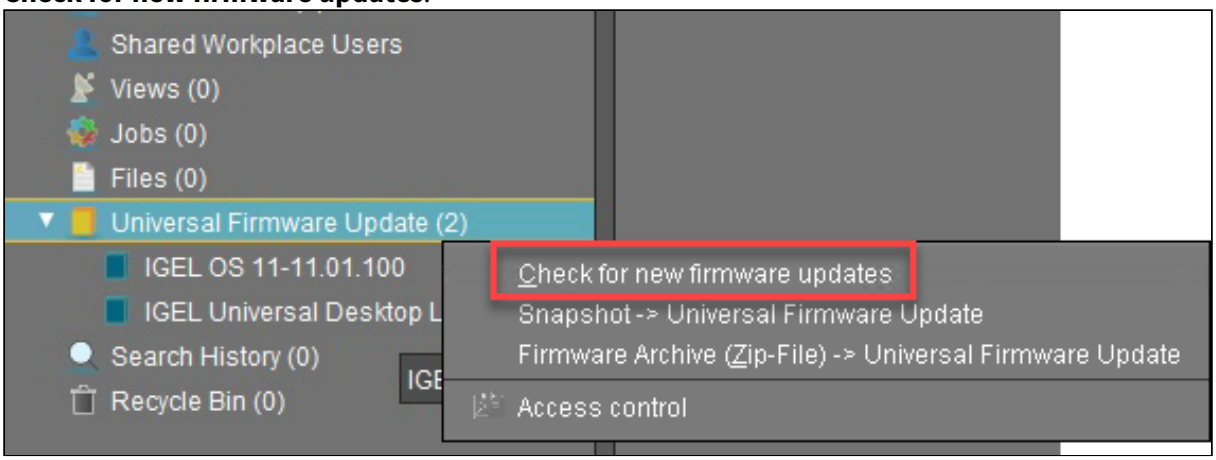
To configure an FTP server as update source:

1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click

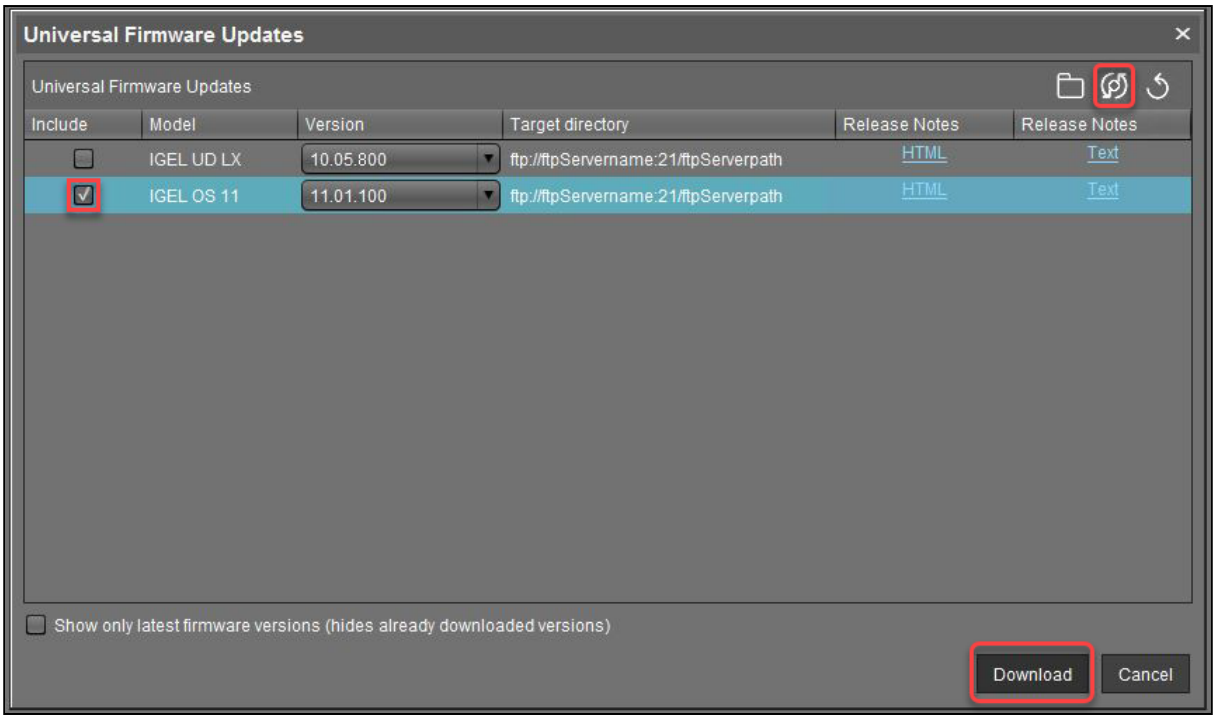
2. Enter the data required for accessing the FTP server and click **Save**.



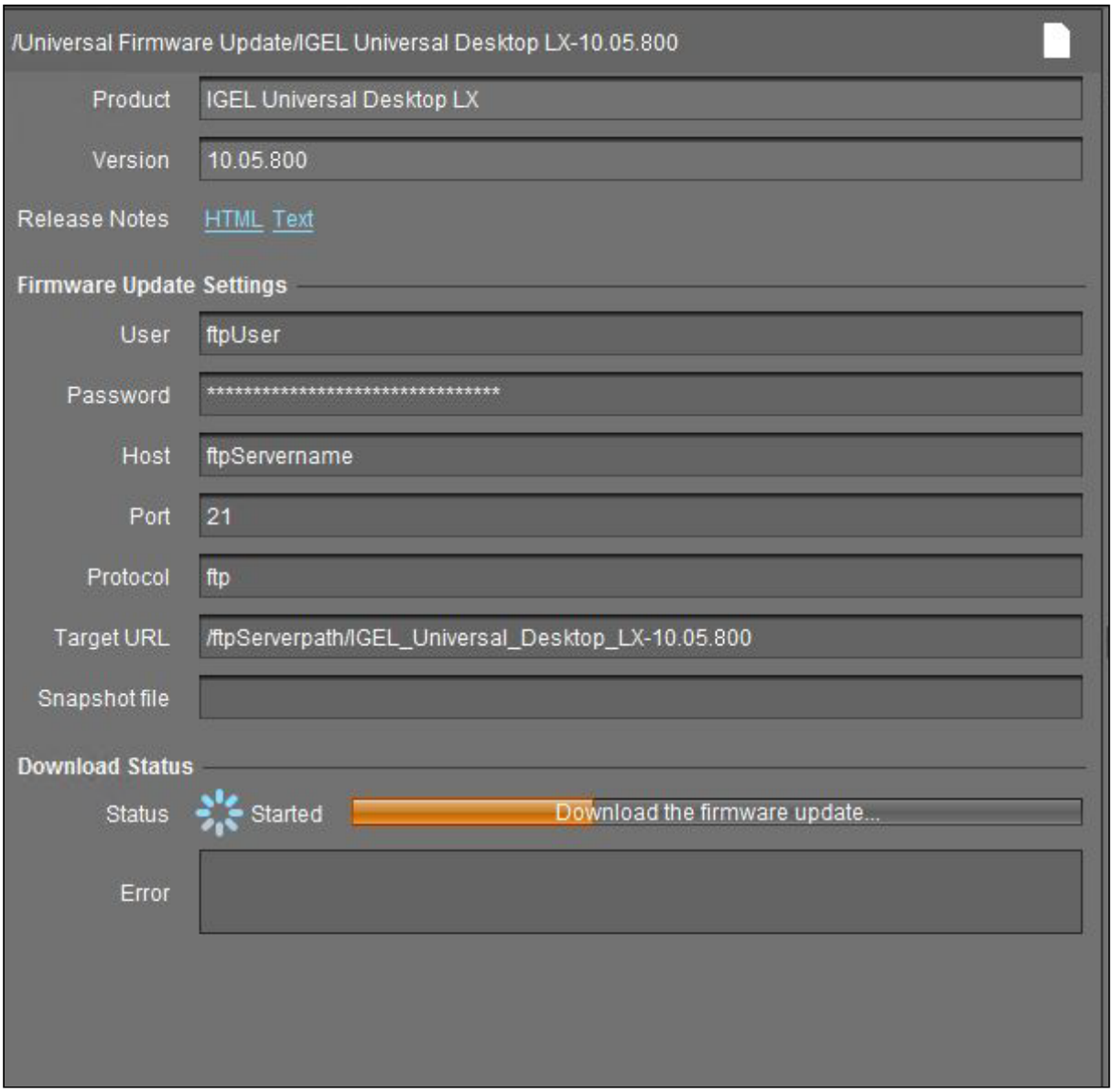
3. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



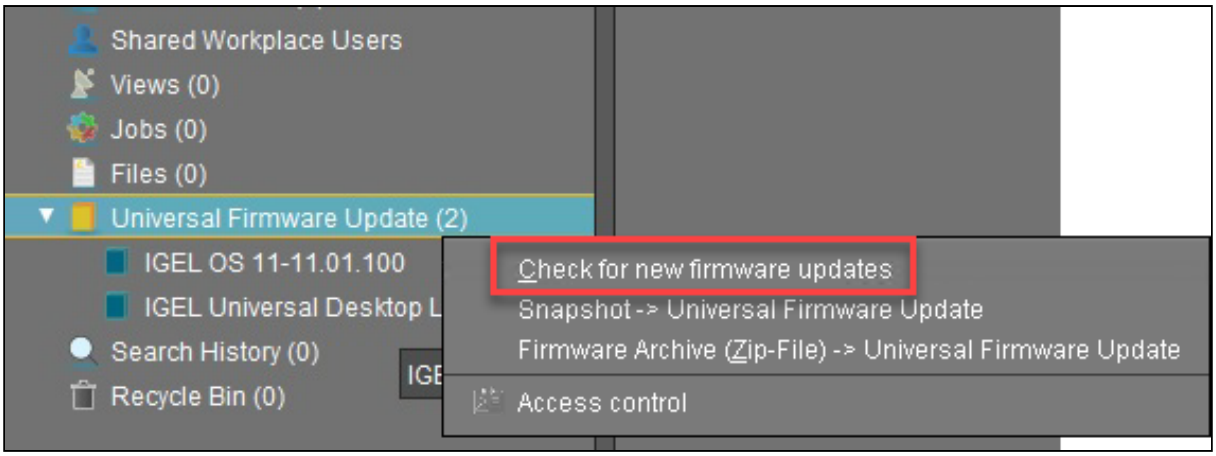
4. Select the entry for the IGEL OS 10.05.800 (or higher) firmware, click to select the FTP server selected in step 2 and then select **Download**.



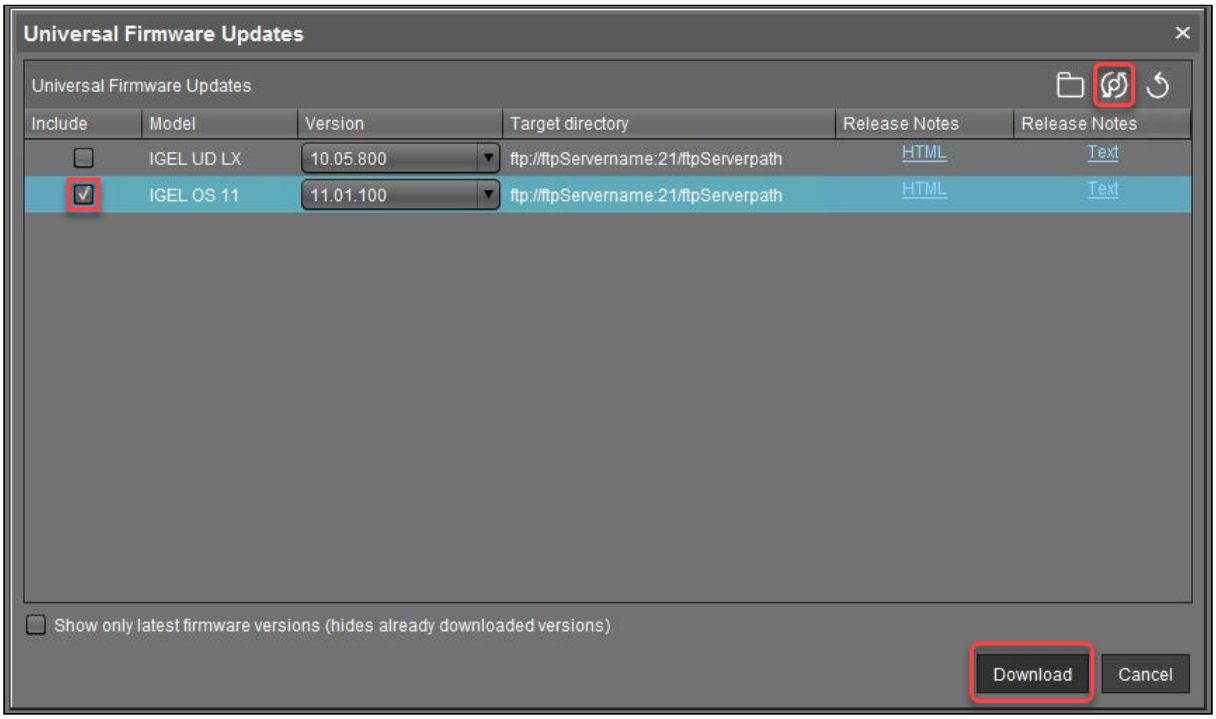
5. The firmware is transferred to the FTP server.



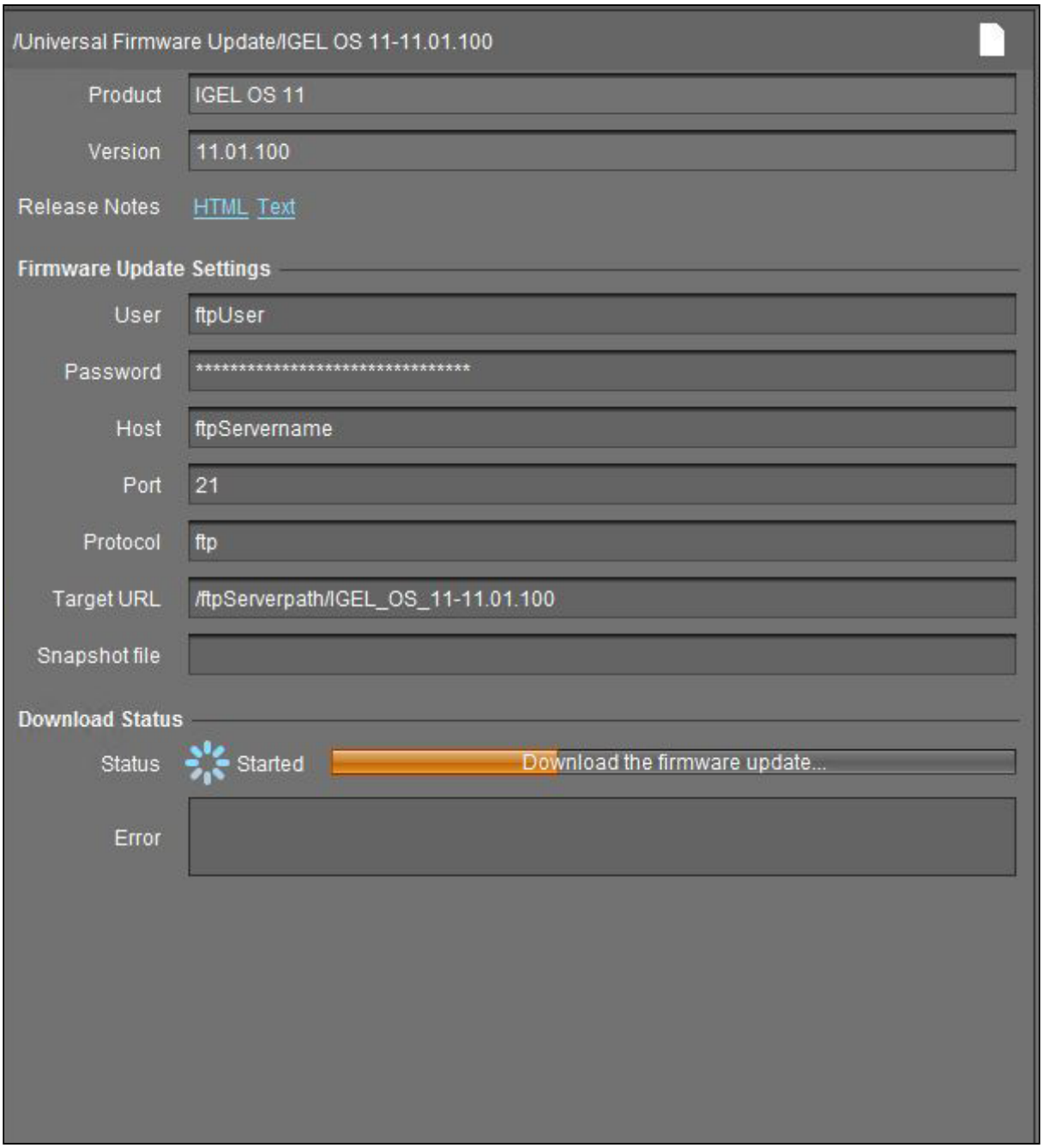
6. Under **Server - [UMS address] > Universal Firmware Update**, in the context menu, select **Check for new firmware updates** again.



7. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and select **Download**.



8. The firmware is transferred to the FTP server.

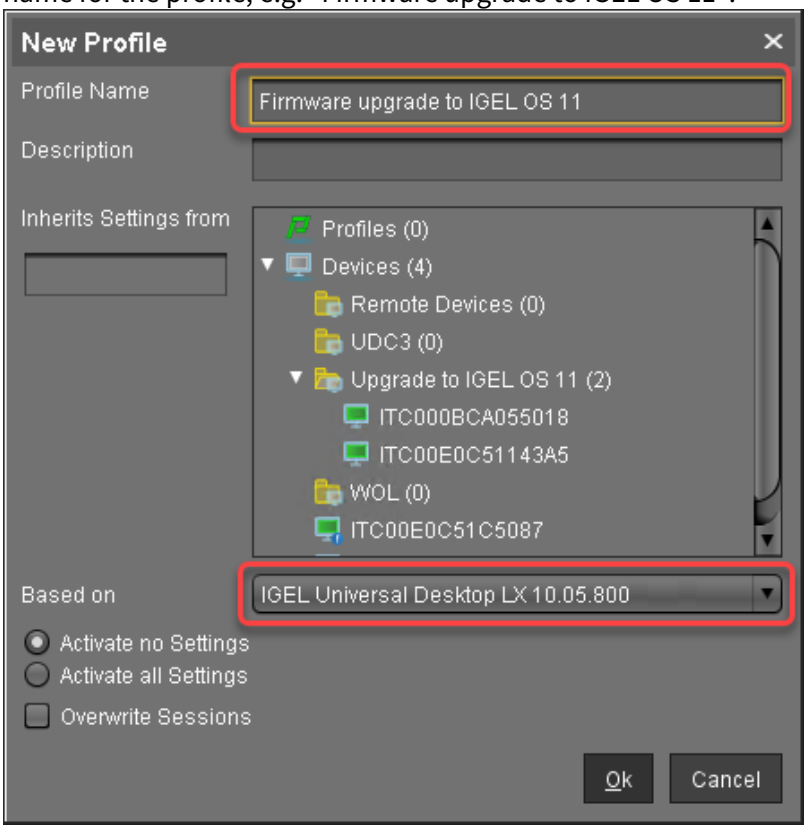


The devices can download the firmware from the FTP server,

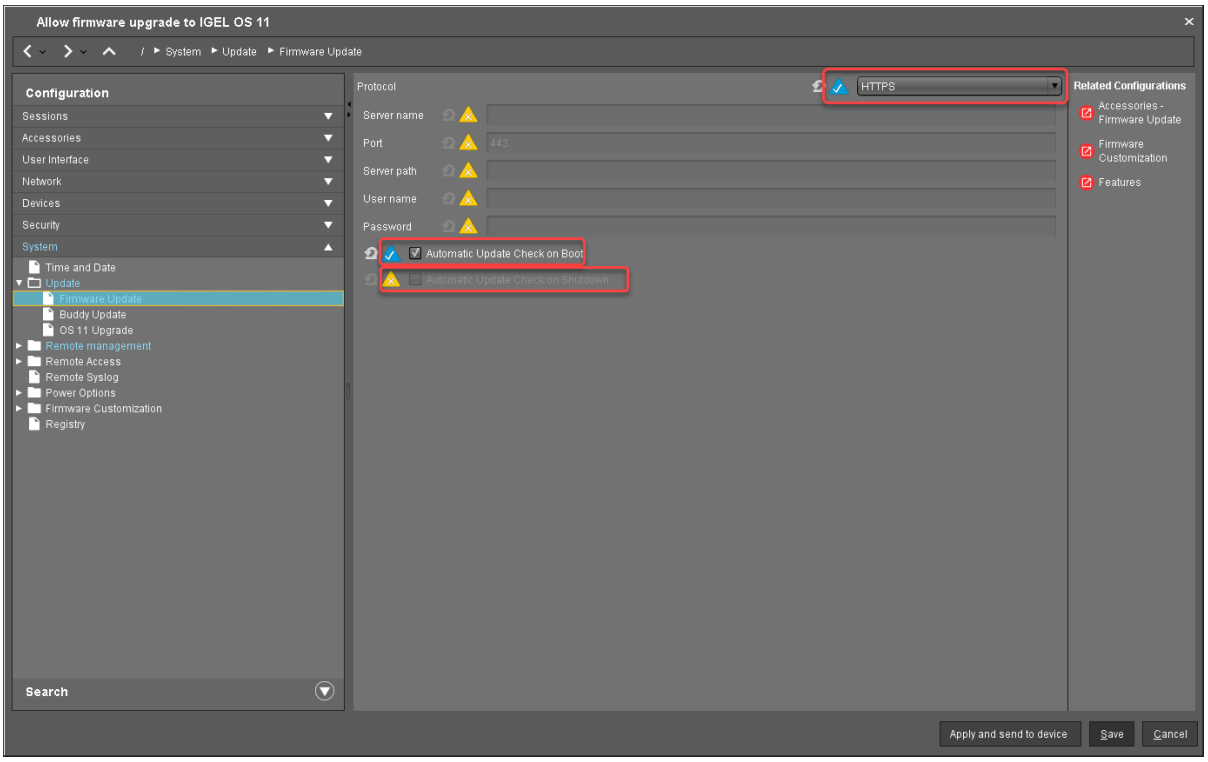
When the Universal Firmware Update is ready, continue with Creating a Profile (see page 164).

Creating a Profile

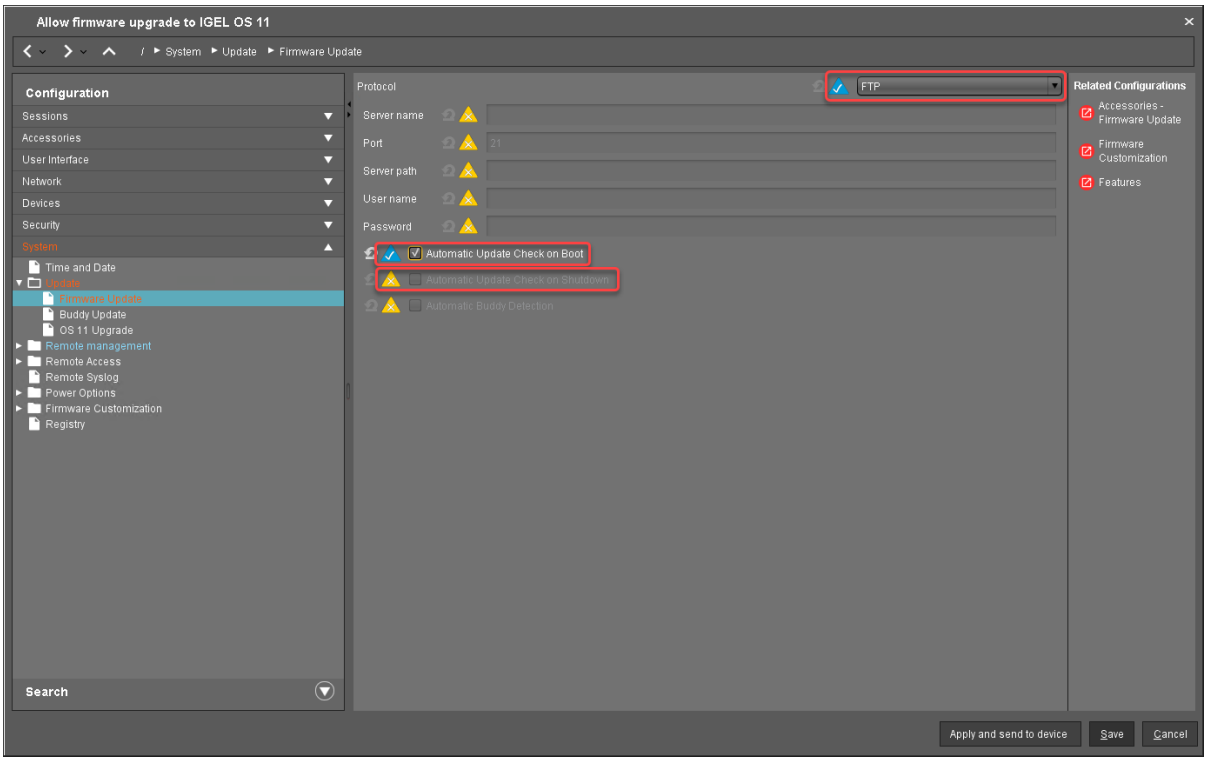
1. Create a profile that is based on the IGEL OS 10 firmware (10.08.800 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".



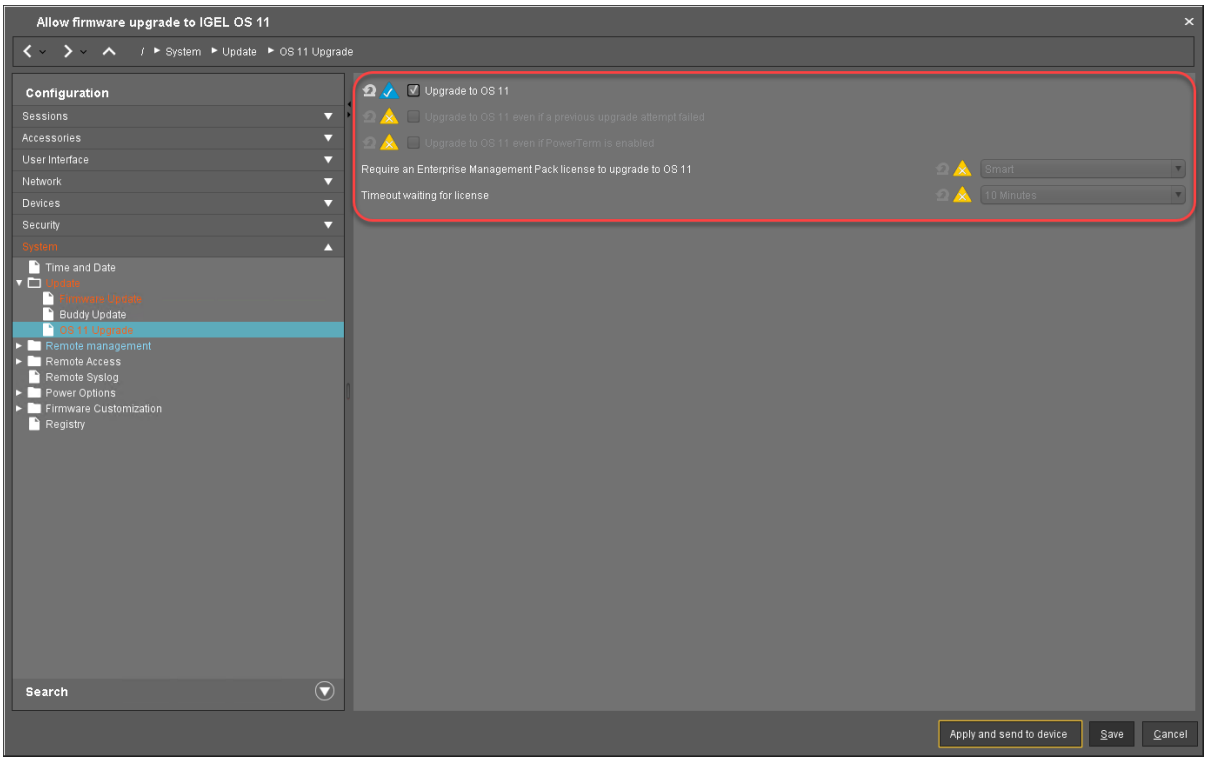
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:
    - If the UMS and the devices are in one and the same network and no IGEL Cloud Gateway (ICG) is used:
        - Select "HTTPS" as **Protocol**.
        - Activate **Automatic Update Check on Boot**.
        - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



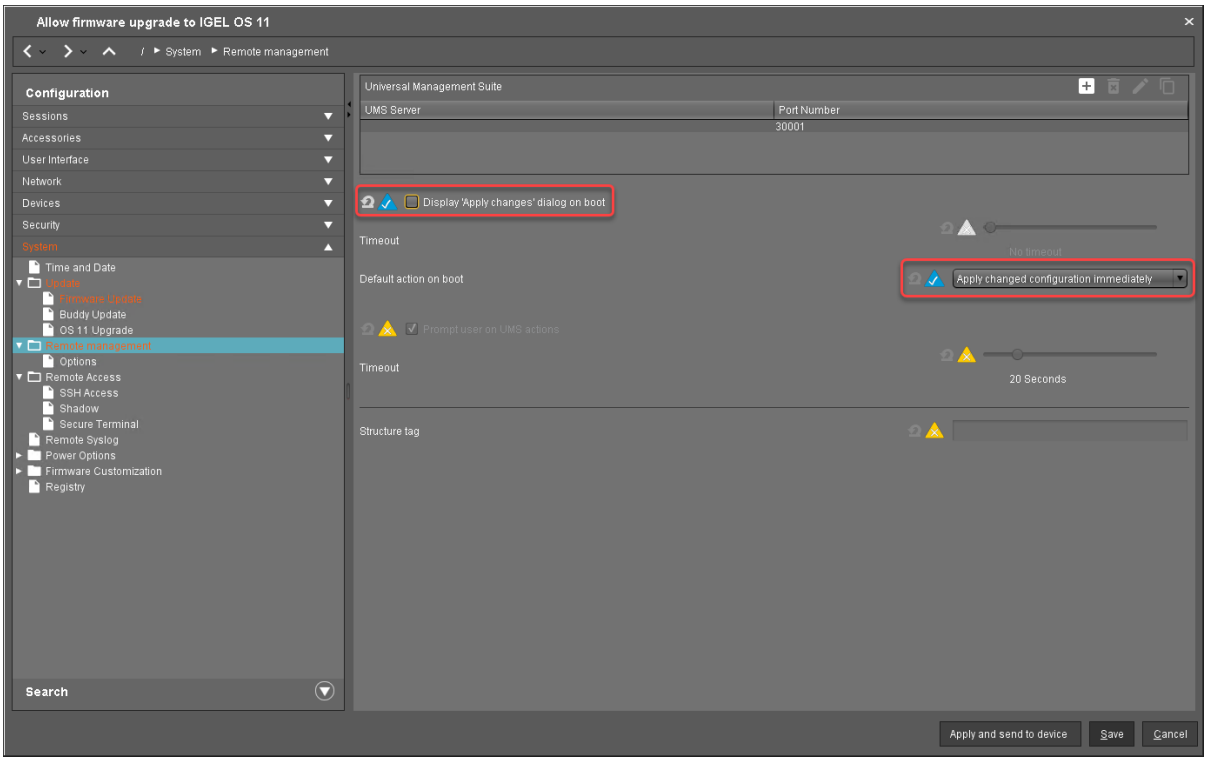
- If IGEL Cloud Gateway (ICG) is used:
  - Select "FTP" as **Protocol**.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details of the settings, see Adjusting the Setup (see page 149)):
    - Activate **Upgrade to OS 11**.
    - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
    - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
    - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
    - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 169).

Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

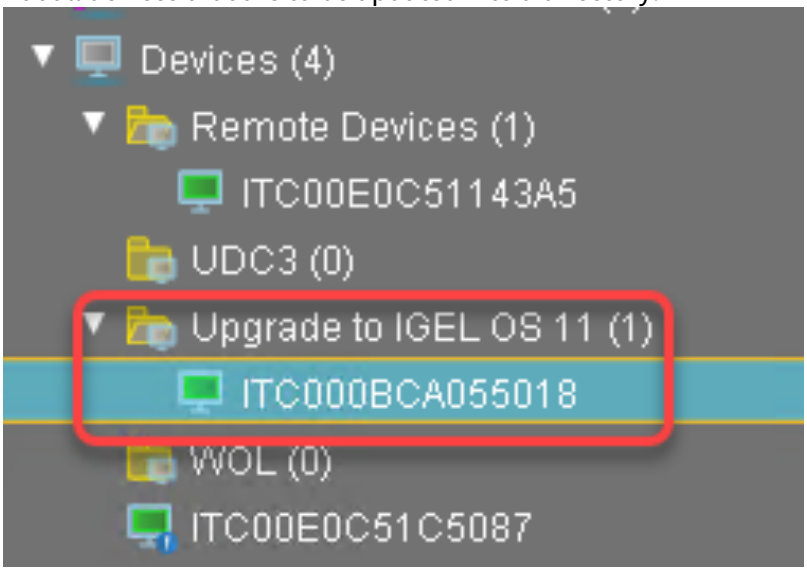
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see https://kb.igel.com/en/igel-subscription-and-more/current/setting-up-automatic-license-deployment-ald.
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see https://kb.igel.com/en/igel-subscription-and-more/current/manual-license-deployment-for-igel-os.

When the license deployment is set up, continue with Putting It All Together[39].

39. https://kb.igel.com/en/igel-os/11.10.250/putting-it-all-together-1

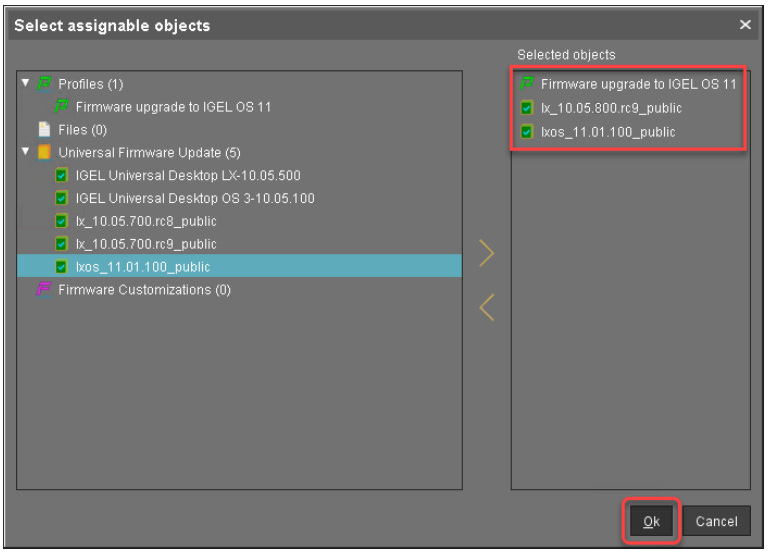
Putting It All Together

1. Put all devices that are to be updated into a directory.

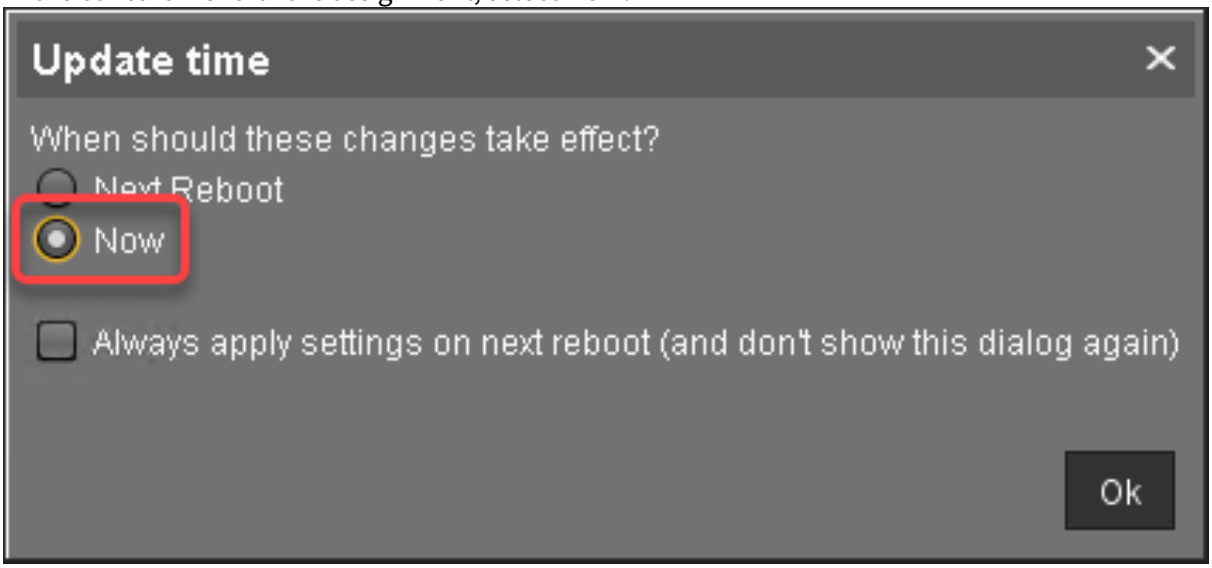


2. Select the directory and in the **Assigned objects** area, click ⊕

3. Assign the profile (see Creating a Profile (see page 164)) and the two Universal Firmware Updates (see Creating the Universal Firmware Updates (see page 158)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.



In the **Assigned objects** area, the profile and the Universal Firmware Updates are shown:

5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see *IGEL Subscription and*

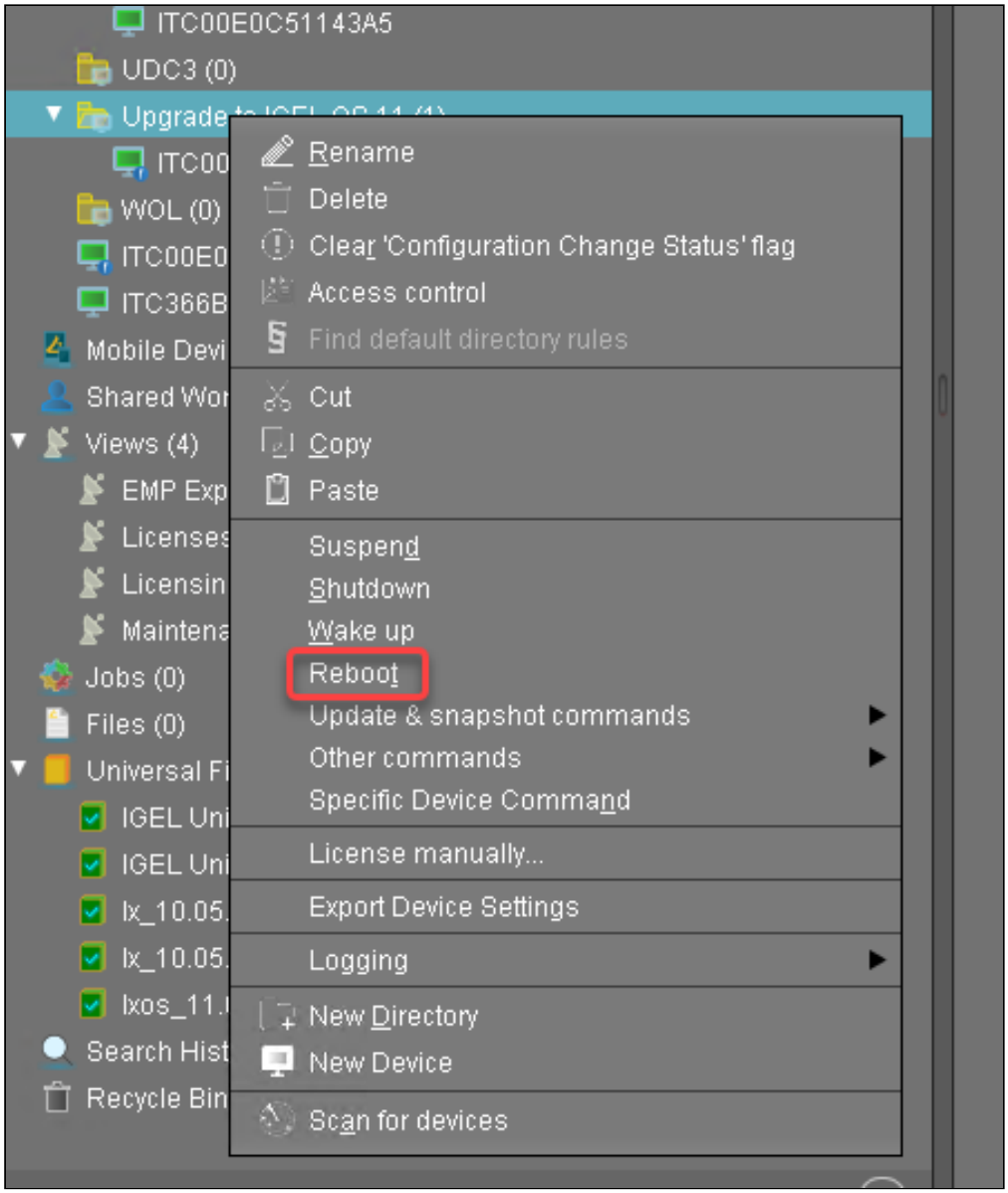
More > IGEL Licensing > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) with ALD Token > How to Configure the Distribution Conditions of Licenses, section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with Executing the Upgrade (see page 173).

Executing the Upgrade

1. In the UMS, select the directory containing all devices that are to be upgraded and reboot them.

> Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices. For more information, see *Universal Management Suite > UMS Reference Manual > Jobs - Sending Automated Commands to Devices in the IGEL UMS*.



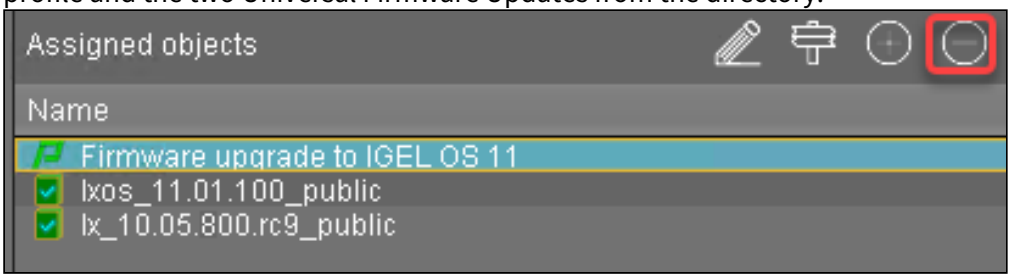
On reboot or wake up, the devices update to the appropriate IGEL OS 10 firmware (10.05.800 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Adjusting the setup (see page 149).
The parameter **Automatic update check on boot** causes the devices look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

Update Can Be Canceled After Timeout
An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

2. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile and the two Universal Firmware Updates from the directory.



The upgrade is completed.

Zero-Touch Deployment Using Buddy Update

This method uses the buddy update feature of IGEL OS. One or more devices that are configured as an update buddy access the main server and download the firmware. The other devices are configured to download their firmware from an update buddy.

Read all the following chapters carefully and follow the instructions.

- Devices That Can Be Upgraded to IGEL OS 11 (see page 176)
- Important! Consider This Before Upgrading (see page 190)
- Preparing the Upgrade (see page 192)
- Testing the Upgrade (see page 197)
- Checking the Requirements (see page 202)
- Configuring Two Update Buddies (see page 203)
- Creating a Profile (see page 204)
- Deploying the Licenses (see page 206)
- Putting It All Together (see page 207)
- Executing the Upgrade (see page 208)

Devices That Can Be Upgraded to IGEL OS 11

Partner Solutions for Peripherical Devices
For further supported hardware from IGEL partners, e.g. headsets, see Partner Solutions (see page 3).

Core Requirements

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

RAM size higher than 2 GB is recommended if you use any of the following:
- Unified Communications optimizations (uses a client-side media engine)
- High-resolution graphics output
- More than two monitors

With devices that have 2 GB RAM and shared video memory, a maximum of 512 MB may be used as video memory.

- Storage: Depends on the release version of IGEL OS 11. The details are listed below:
  - Up to IGEL OS 11.03: 2 GB minimum; ≥ 4 GB recommended
  - From IGEL OS 11.04 to IGEL OS 11.07: If the full feature set is applied, at least 2.4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318).
  - From IGEL OS 11.08 onwards: If the full feature set is applied, at least 4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318).
- No VIA graphic adapter; VIA graphics support is discontinued in IGEL OS.
- Legacy Bios and EFI/UEFI are supported.

Devices Supported by OSC and UD Pocket with IGEL OS 11

The following list only includes those devices that are **tested by IGEL** (with each major release of IGEL OS). By no means it implies that the devices which are not included in this list but meet the minimum requirements will not function with IGEL OS: Any x86-64 hardware endpoint device that meets the IGEL-stated minimum hardware requirements for IGEL OS (for example, the processor speed and RAM) can be expected to work adequately with IGEL OS and should be considered a candidate for repurposing from another OS. With an IGEL OS subscription or active maintenance, customers can expect IGEL to make any necessary “best effort” to support, regardless of whether the endpoints in question are specifically listed within the IGEL Knowledge Base or elsewhere (e.g. on the IGEL Ready Showcase at https://www.igel.com/ready/showcase-categories/endpoints/).
For any devices not listed here or on the IGEL Ready showcase, you can contact your hardware vendor and request those devices to be added to the IGEL Ready program.

Integrated drivers and supported peripherals are listed in the Third-Party Hardware Database[40]. For more solutions compatible with IGEL OS, see Partner Solutions (see page 3).

HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[41] to get information on which device models are available with pre-installed IGEL OS.

For some of the devices listed here, Flash memory must be extended to ≥ 2 GB. For these devices, an appropriate note is added.

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft's 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see *Security & Safety > UEFI Secure Boot Enabling Guides > Secured-Core PCs: Microsoft 3d-Party UEFI Certificate for Secure Boot*.

[Fn] keys may not work on some supported and listed laptop/notebook models.

ADS-Tec

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DVG-VMT9010	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9012	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

40. https://www.igel.com/linux-3rd-party-hardware-database/
41. https://www.igel.com/technology-partners/

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DVG-VMT9015	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9112	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

Advantech

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L* (see page 189)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 189)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
DLT-V6210	Industrial PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrial PC/ Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

Dell / Wyse

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Notes
5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100	
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100	
5020	Thin Client	2 GB	8 GB	AMD G-Series SoC	11.02.140	
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100	
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100	
Latitude 5510	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100	Wake-on-LAN functionality is not supported.
Optiplex 3000	Thin Client	4 GB	32 GB	Intel Celeron N5105	11.08.200	

Dynabook

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Portegé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portegé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

Elo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
i2 Touch (15 and 22 inches)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

Fujitsu

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Q957	Desktop PC	8 GB	500 GB	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

HP

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100		
HP t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	Intel AC9260	
HP t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100		
HP t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100		
HP t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100		

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100		
HP t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	Intel AC9260 Realtek RTL8852AE	This model is not supported with HP USB-C Essential G5 Dock
HP t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	Intel AC9260 Realtek RTL8852AE	
HP mt46	Mobile Thin Client	8 GB	32 GB	AMD Ryzen 3 PRO 4450U	11.07.100		Excluding support for WWAN and Wake-on-LAN (both features are planned)
HP Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	Realtek RTL8852BE	
HP Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.08.330) Excluding support for Wake-on-LAN (feature is planned) Excluding support for built-in fingerprint sensor
				AMD Ryzen 5 5625U	11.08.330		
HP t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	Realtek RTL8852AE	

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Wi-Fi Chip	Notes
HP Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	Realtek RTL8852CE (Supported as of 11.09.150)	
HP Pro mt440 G3	Mobile Thin Client	8 GB	128 GB	Intel Celeron 7305	11.08.440	Realtek RTL8852BE	Support for WWAN Intel XMM 7560 (as of 11.09.260)
HP Elite t755	Thin Client	8 GB	128 GB	AMD Ryzen Embedded V2546	11.09.260	Realtek RTL8852CE	This model offers no USB-C docking support

HP Docking Stations

Name	Supported from IGEL OS Version	Notes
HP USB-C Docking Station G5	11.08.230	
HP USB-C G5 Essential Dock	11.08.290	Not supported with HP t640

Intel

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
NUC 5i5MYHE	Desktop PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

Lenovo

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkCentre M625q	Desktop PC	4 GB	32 GB	AMD E2-9000e	Intel AC9260	11.04.100	
		8 GB	128 GB	AMD A4-9120e	QCA6174 802.11ac	11.04.100	
ThinkCentre M75n	Desktop PC	8 GB	256 GB	AMD Ryzen 3 Pro 3300U	Intel AC9260	11.05.100	
ThinkCentre M70q Gen1	Desktop PC	16 GB	256 GB	Intel i5-10500t	Comet Lake PCH CNVi WiFi, Intel	11.05.100	
ThinkCentre M70q Gen 3	Desktop PC	16 GB	256 GB	Intel Core i5-12500T	Intel AX201	11.08.240	
ThinkCentre M75q Gen 2	Desktop PC	4 GB	128 GB	AMD Ryzen 3 Pro 5350GE	Intel AX200	11.08.240	
K14 AMD Gen 1	Laptop/ Notebook	8 GB	256 GB	AMD Ryzen 5 PRO 5650U	Mediatek MT7921	11.08.240	
ThinkPad L14 AMD Gen 1	Laptop/ Notebook	64 GB	1 TB	AMD Ryzen 7 Pro 4750U	Wi-Fi 6 AX200, Intel	11.05.100	
14w	Laptop/ Notebook	4 GB	64 GB	AMD A6-9220C	QCA6174 802.11ac	11.05.100	
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkCentre Neo50q Gen 4	Thin Client	8 GB	256 GB	Intel Core i3-1215U	Wi-Fi 6 RTL8852BE	11.08.240	
		4 GB	256 GB	Intel Celeron 7305	Wi-Fi 6 AX201		
K14 Intel Gen 1	Laptop/ Notebook	16 GB	256 GB	Intel Core i5-1135G7	Intel AX210 WiFi / BT combo	11.08.290	
ThinkPad L14 Intel Gen 3	Laptop/ Notebook	16 GB	512 GB	Intel Core i5-1235U	Intel Wi-Fi 6 AX201 2x2 AX vPro	11.08.330	Quectel EM05-G 4G CAT4 LTE support as of 11.08.360
ThinkEdge SE10	Thin Client	8 GB	1 TB	Intel Atom x6425RE	MediaTek MT7921LEN	11.08.360	
			256 GB	Intel Atom x6214RE	Intel AX210	11.08.360	
ThinkPad L14 AMD Gen 4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L15 AMD Gen4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L14 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L15 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Notes
ThinkPad L13 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX201	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN
ThinkPad L13 AMD Gen 4	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 3 PRO 7330U	AMD RZ616	11.09.210	Quectel EM05-G 4G CAT4 No integrated LAN

Lenovo Docking Stations

Name	Supported from IGEL OS Version
ThinkPad USB-C Hybrid Dock	11.07.100
IOBOX	11.07.100
Universal USB-C Dock	11.08.440

Lenovo USB-C to Ethernet Adapter

Name	Supported from IGEL OS Version	Supported with
USB-C to Ethernet Adapter	11.09.260	• ThinkPad L13 Intel Gen4 • ThinkPad L14 AMD Gen4

LG

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CK550** (see page 189)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
24CK560** (see page 189)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
38CK950	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
38CK900	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
34CN650	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360
24CR670	All in One	4 GB	16 GB	Intel Celeron N5105	11.09.110
34CR650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210
27CQ650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210

LG Docking Stations

Name	Supported from IGEL OS Version
LG USB Multi Port Hub	11.09.100

OnLogic

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
CL210G-10	Industrial PC/ Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

Onyx Healthcare

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

Pepperl+Fuchs

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
BTC12N	Industrial Box Thin Client	4 GB	32 GB	Intel Apollo Lake N4200	11.09.100
BTC14N	Industrial Box Thin Client	4 GB	32 GB	AMD Ryzen Embedded V1202B	11.09.100

Rein Medical

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

Secunet

Name	Device Category	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

USB Memory Sticks That Can Be Used as UD Pocket Hardware

DIGITTRADE

Name	Storage	Supported from IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133

Transcend

Name
Powered by IGEL UD Pocket
Powered by IGEL UD Pocket 2

Officially Supported Virtual Environments

- Tested with Ubuntu (64-bit) and default settings

⚠ Note that the use of a UD Pocket within a virtual machine is **not** supported by IGEL.

For some features, more than 2 GB RAM is required. Example: if you use dual monitor environments, a virtual machine must have at least 8 GB RAM.

Name	Memory (RAM)	Storage	Type	Supported from IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

*Delock Adapter DP 1.2 to DVI does not work.

** When using an additional 4k screen with this device, please edit the BIOS settings as follows:

1. Go to the **Chipset** screen.
2. Set **Integrated Graphics** to “Force”.
3. Set **UMA Frame Buffer Size** to “256M” or higher

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider Important! Consider This Before Upgrading 3 (see page 190).

Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

No Downgrade
You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

Features (e.g. Clients)
IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions
The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

Custom Commands
The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

Network
All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband.

Hardware Support
Make sure that your devices support IGEL OS 11; please refer to *Hardware* > *Supported Devices* > *Devices Supported by IGEL OS 11*. This document describes upgrading methods for IGEL UD and IGEL IZ devices. Upgrading methods for IGEL UDC3 and UD Pocket are described under Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11 (see page 130).

License
- A valid license from an IGEL Workspace Edition (WE) Product Pack must be available for each device. For general information, see *IGEL Subscription and More* > *_Hide from Viewport* > *IGEL Software License Overview*. For deploying licenses, see *IGEL Subscription*

and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) or *Manual License Deployment for IGEL OS.*

- IZ devices are not allowed to upgrade to IGEL OS 11. Please contact your IGEL sales representative for a UD Upgrade License which allows you to upgrade your IZ devices.

UMS Version
UMS version 6.01.130 or higher is required for upgrading from IGEL OS 10 to IGEL OS 11.

When you have considered everything that is relevant, continue with Preparing the Upgrade (see page 192).

Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

To prepare the upgrade, perform the following steps:

1. Preparing the UMS (see page 193)
2. Adjusting the Setup 3
3. Deploying a License 1 (see page 195)
4. Configuring the Update Source 1

Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see *Universal Management Suite > UMS Reference Manual > UMS Installation and Update > IGEL UMS Update*.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter *Universal Management Suite > UMS Reference Manual > Registering IGEL OS Devices on the UMS Server.*

When the UMS is ready, continue with Adjusting the Setup[42].

42. https://kb.igel.com/en/igel-os/11.10.270/adjusting-the-setup-2

Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Firmware Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
    - Activate **Upgrade to OS 11**.

> When **Upgrade to OS 11** is activated, the device checks for a Workspace Edition license and stops checking for a legacy UDC3 or UD Pocket license. Therefore, in the UMS, it is displayed as an unlicensed device until a Workspace Edition license has been deployed.

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
    - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
    - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see Zero-Touch Deployment Using Universal Firmware Update (see page 131), Zero-Touch Deployment Using Buddy Update (see page 175) and Mass Deployment Using a Scheduled Job (see page 283)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

3. Click **Apply**.

When the Setup is adjusted, continue with Deploying a License (see page 195).

Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality
- If one of the following features is used, one Enterprise Management Pack license is required:
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

→ Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see https://kb.igel.com/en/igel-subscription-and-more/current/manual-license-deployment-for-igel-os.
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see https://kb.igel.com/en/igel-subscription-and-more/current/setting-up-automatic-license-deployment-ald.
- Download three demo licenses from https://www.igel.com/download/ .

When the device has a license, continue with Configuring the Update Source[43].

43. https://kb.igel.com/en/igel-os/11.10.250/configuring-the-update-source-2

Configuring the Update Source

1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update Settings for IGEL OS (see page 2056) chapter in the IGEL OS Manual.
2. Click **Ok**.

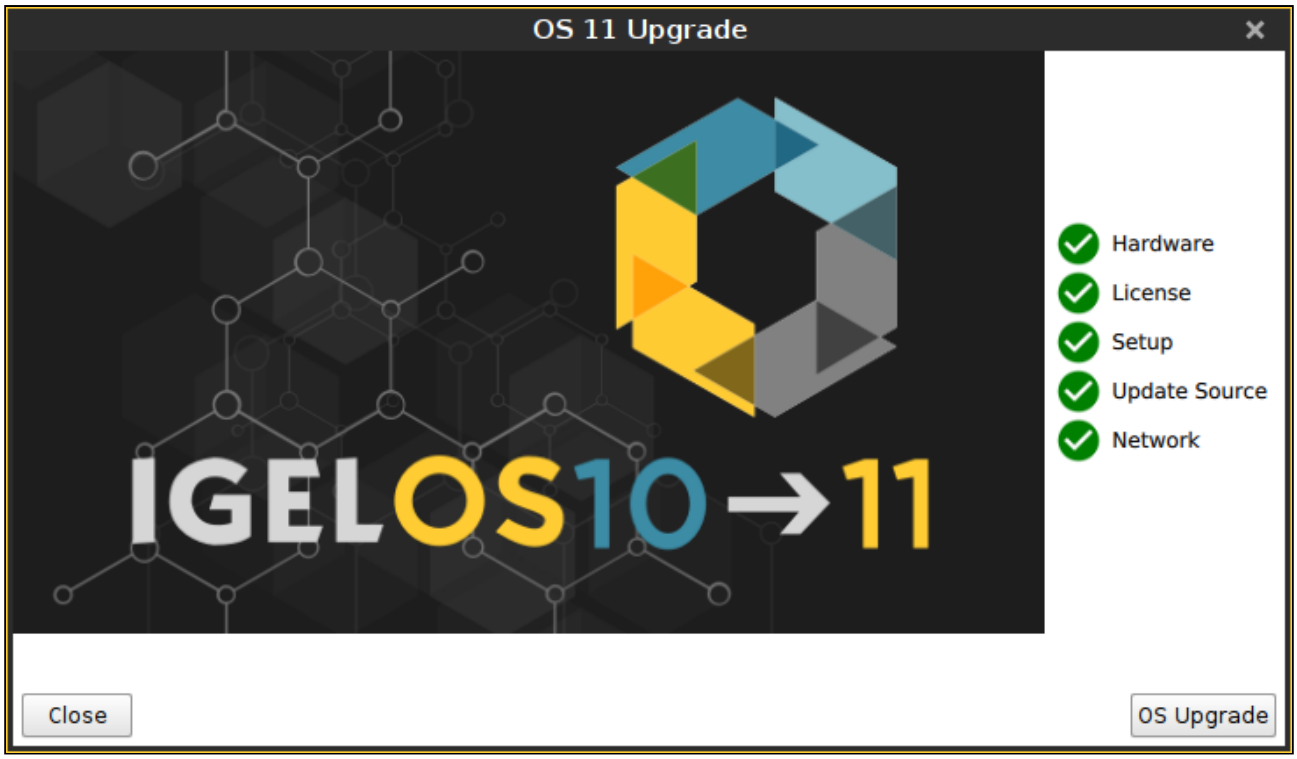
When the correct update source is configured, continue withTesting the Upgrade (see page 197).

Testing the Upgrade

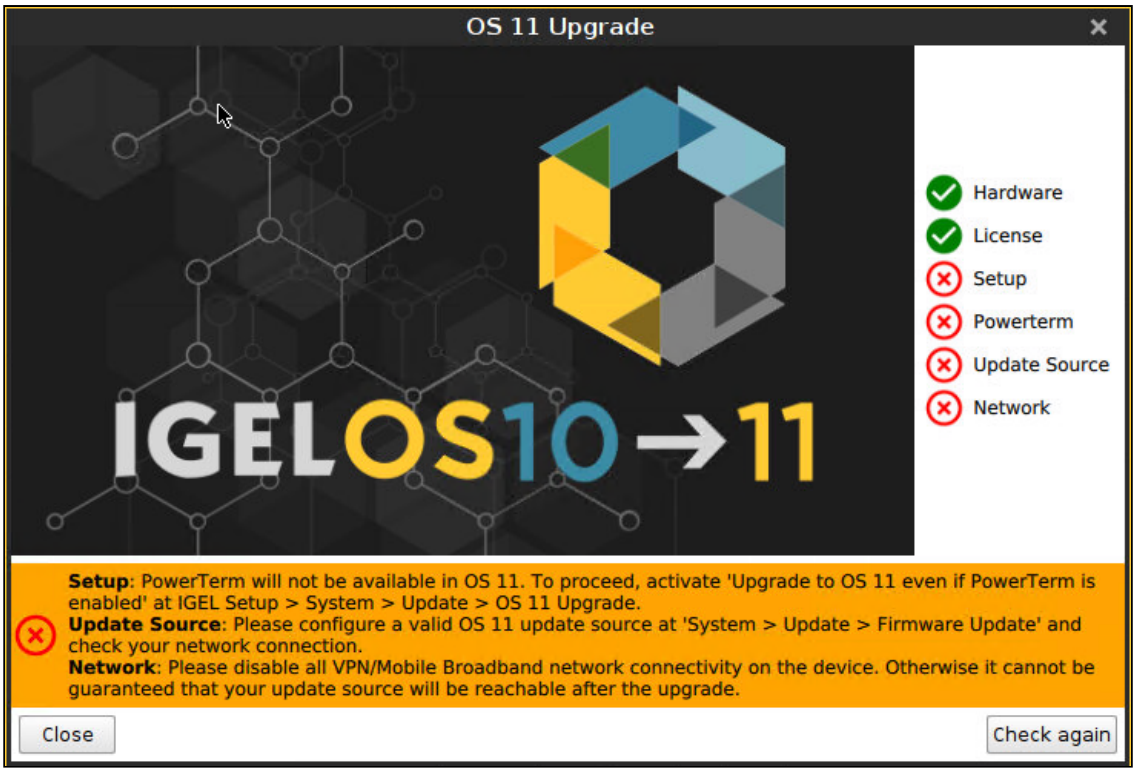
When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements 1.

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

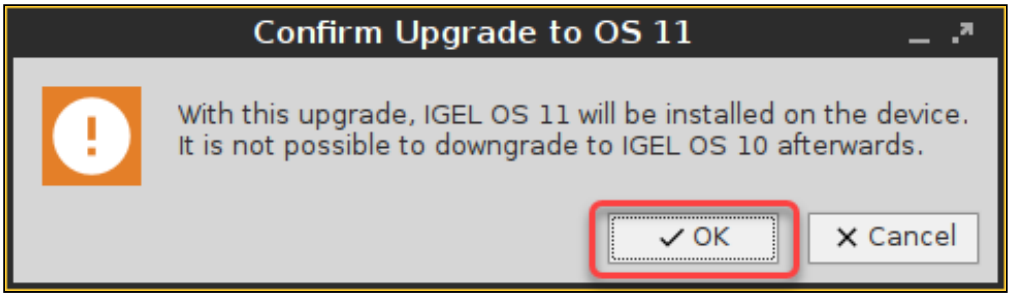


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:
   - If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
   - If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**, and you can start the upgrade.

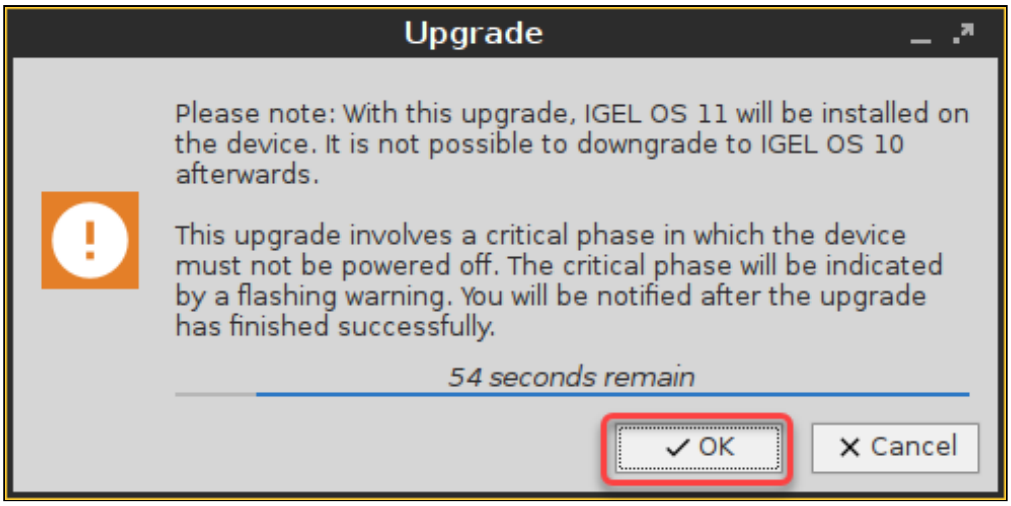


When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



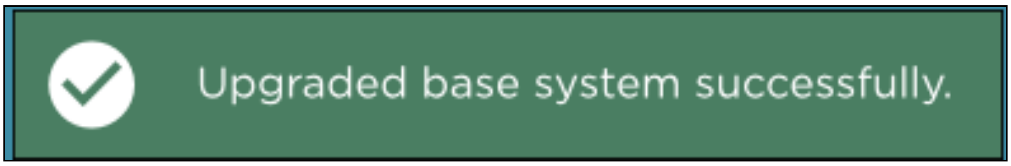
A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



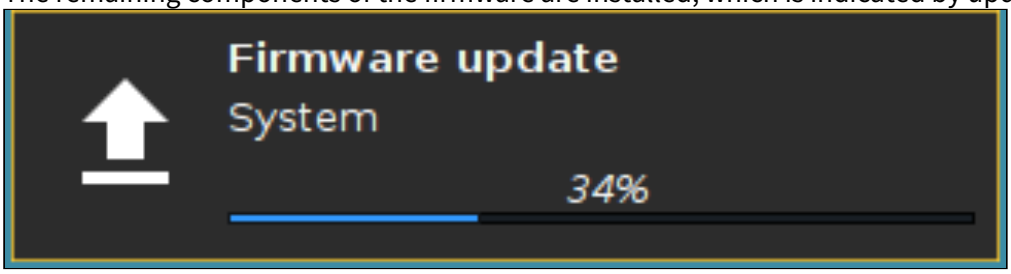
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window shows the progress.

During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.

When the base system is upgraded successfully, a message is shown.



The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:

After a few seconds the device reboots into IGEL OS 11.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements 1.

Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The appropriate IGEL OS 10 firmware version (10.05.700 or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate IGEL OS 10 firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with Configuring Two Update Buddies (see page 203).

Configuring Two Update Buddies

For setting up buddy updates, see the how-to Buddy Update (see page 303).

Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

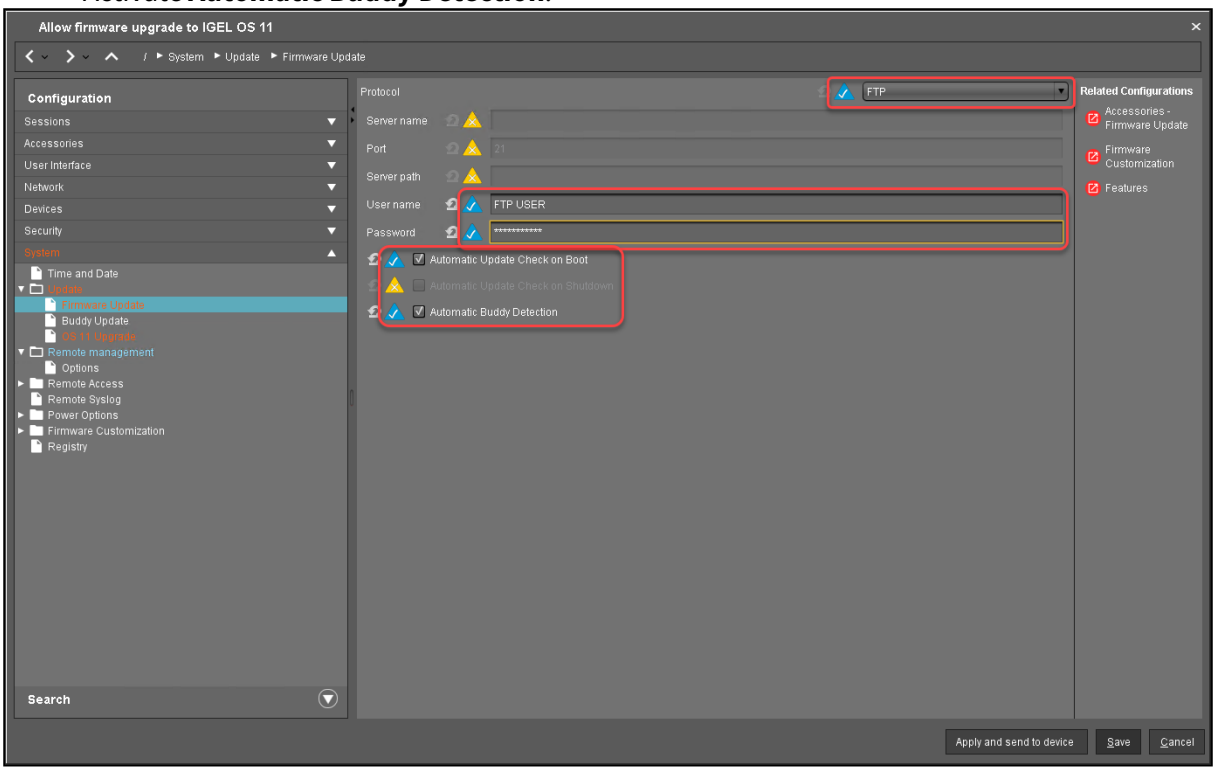
1. Update one device to the appropriate IGEL OS 10 firmware (10.05.800 or higher) and configure it as an update buddy.
2. Upgrade another device to IGEL OS 11 and configure it as an update buddy. Make sure that the IGEL OS 11 update buddy has the same **User Name** and **Password** in **System > Update > Buddy Update** as the IGEL OS 10 update buddy.

When the update buddies are configured, continue with How to Create a Profile for the Zero-Touch Buddy Update[44].

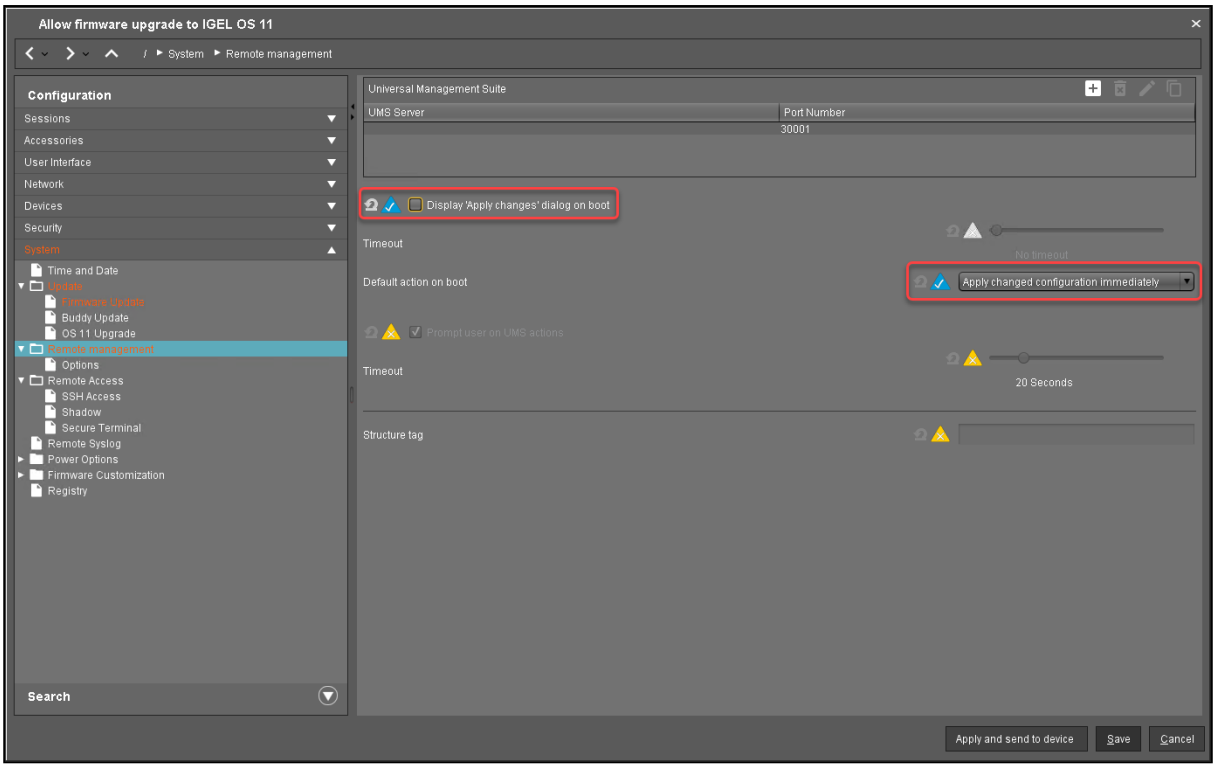
44. https://kb.igel.com/en/igel-os/11.10.250/creating-a-profile-2

Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 version (10.05.800 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings as follows:
    - Select "FTP" as **Protocol**.
    - Enter **User Name** and **Password** according to the update buddy server.
    - Activate **Automatic Update Check on Boot**.
    - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the upgrade to OS 10.05.800 is finished.
    - Activate **Automatic Buddy Detection**.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details, see Adjusting the Setup (see page 194)):
    - Activate **Upgrade to OS 11**.
    - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
    - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
    - Set **Timeout waiting for OS 11 license to start automatic upgrade** to **10 Minutes**.
4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile es created, continue with Deploying the Licenses (see page 206).

Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*

When the license deployment is set up, continue with Putting It All Together 2.

Putting It All Together

1. Assign the profile to all devices that are to be upgraded. This can be done by assigning the profile to the directory that contains these devices.

> Do not assign the profile to the update buddies.

2. In the context menu of the assignment, select **Now**.
3. For Automatic license deployment, a condition can be set to the directory. For more information, see *IGEL Subscription and More > IGEL Licensing > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) with ALD Token > How to Configure the Distribution Conditions of Licenses* section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with Executing the Upgrade (see page 208).

Executing the Upgrade

1. In the UMS, select all devices that are to be upgraded and reboot them.

> Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices; for more information, see (12.05.100-en) Jobs - Sending Automated Commands to Devices in the IGEL UMS .

On reboot or wake up, the devices choose the IGEL OS 10 buddy. They ignore the IGEL OS 11 buddy at this stage because this version is not known to them yet. The devices update to the appropriate IGEL OS 10 version (10.05.800 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).
If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Adjusting the Setup 3 (see page 194).
The parameters **Automatic update check on boot** and **Automatic buddy detection** cause the devices to look for a new firmware and wait for an IGEL OS 11 update buddy to reply. When an IGEL OS 11 update buddy is found, the devices start the upgrade process.

Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

2. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile.

The upgrade is completed.

Mass Deployment Using a Scheduled Job

This scenario is appropriate if you already have a working environment with IGEL OS 10.05.800 (or higher) and want to update all devices to IGEL OS 11 at a defined time.

Read all the following chapters carefully and follow the instructions.

1. Checking the Requirements (see page 210)
2. Creating a Profile (see page 211)
3. Deploying the Licenses (see page 215)
4. Assigning the Profile (see page 216)
5. Creating the Scheduled Job (see page 218)

Checking the Requirements

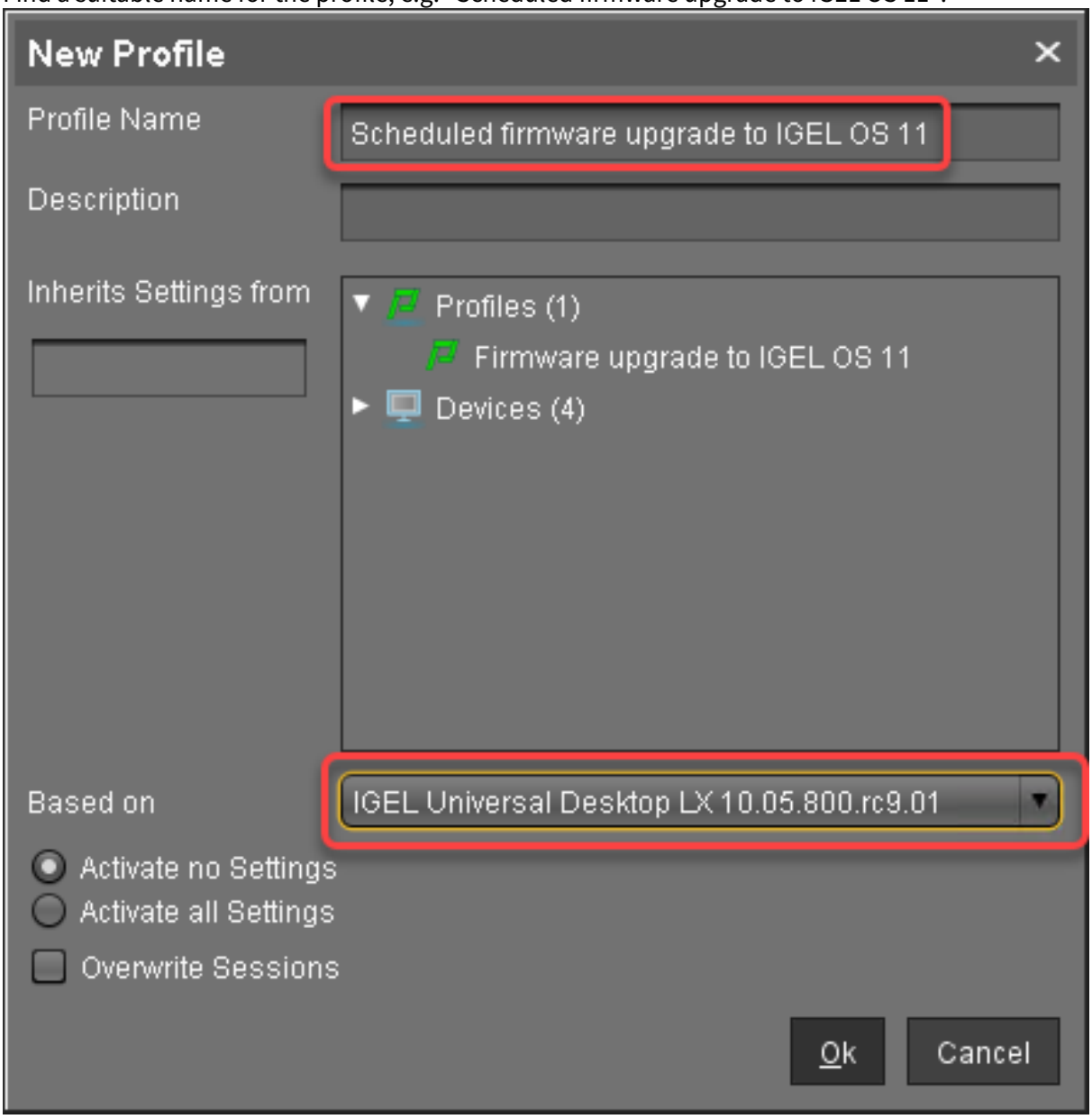
The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The appropriate IGEL OS 10 firmware version (10.05.700 or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate IGEL OS 10 firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with Creating a Profile (see page 211).

Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.800 or higher). Find a suitable name for the profile, e.g. "Scheduled firmware upgrade to IGEL OS 11".



2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:

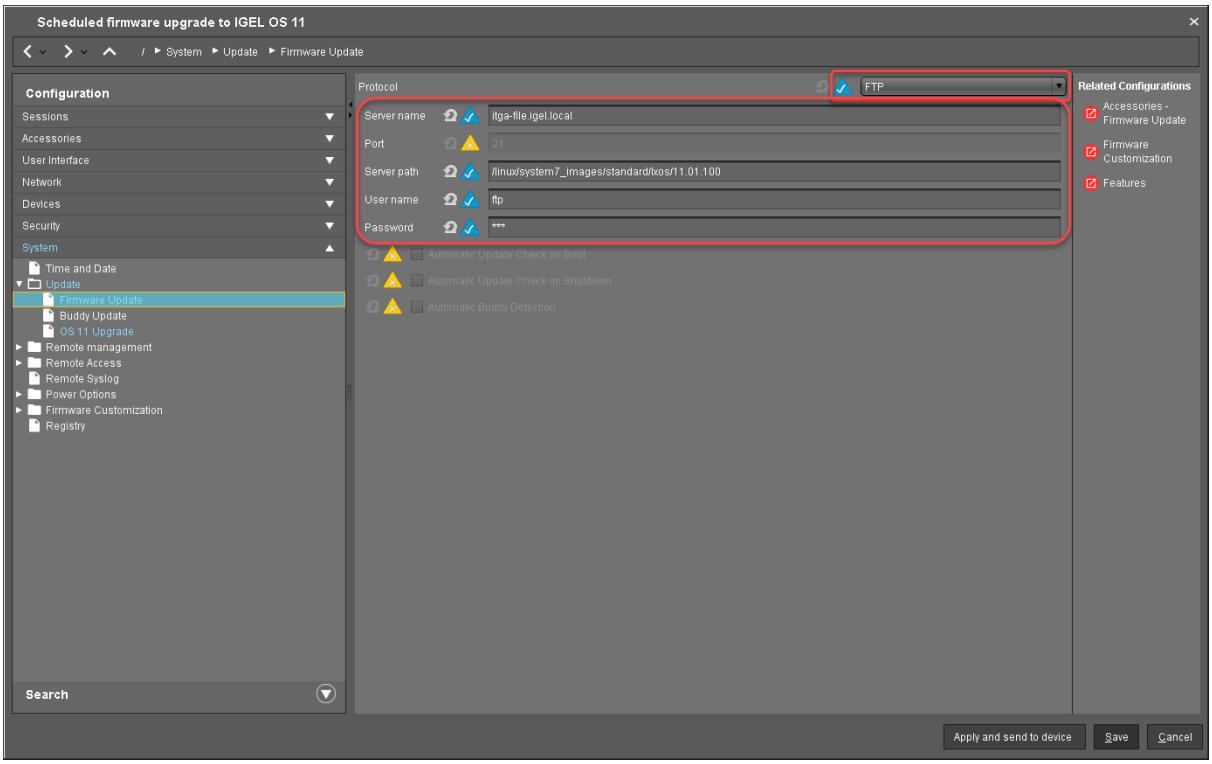
> If you use Universal Firmware Update (see page 244) for OS 11, you do not need to configure the settings described in this step.

- Select an update source for IGEL OS 11. For further information, see Firmware Update Settings for IGEL OS (see page 2056).

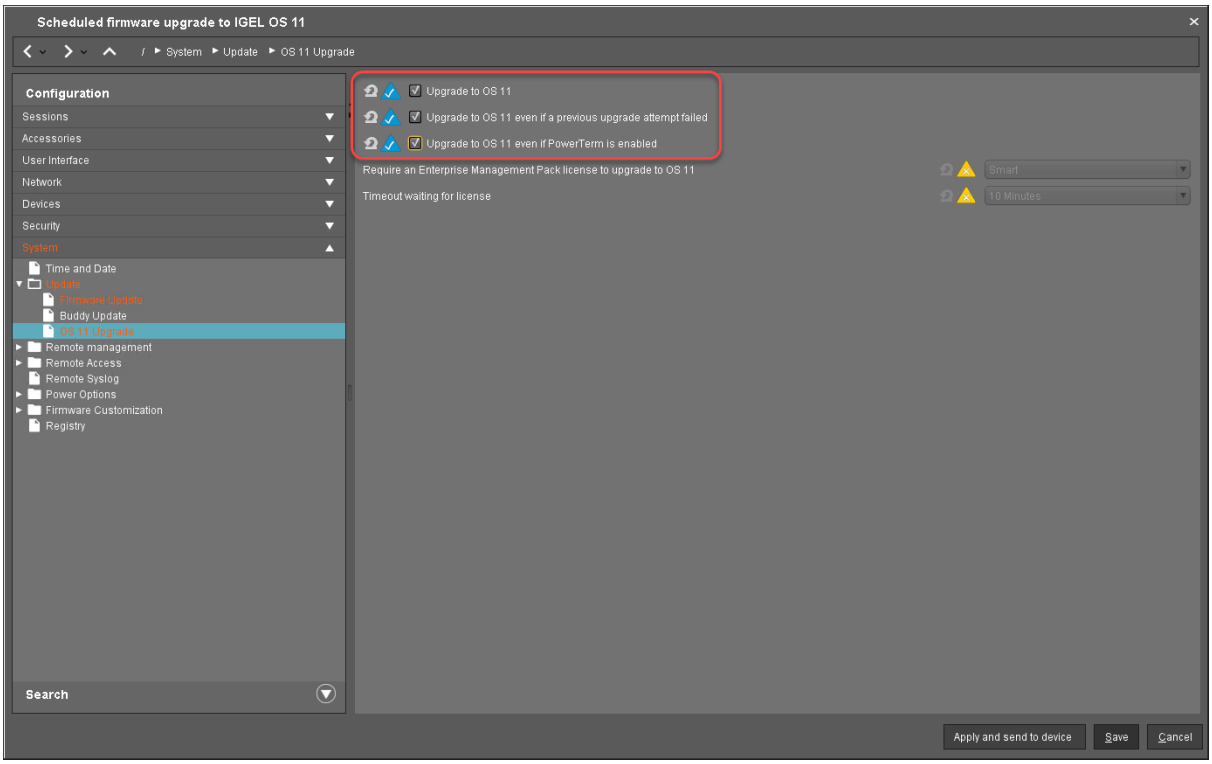
  If you use **FILE** as the protocol (local file or network drive), the device will show an error message and go through an additional reboot. Apart from that, the upgrade will work normally.

- Ensure that **Automatic Update Check on Boot** and **Automatic Update Check on Shutdown** are deactivated.

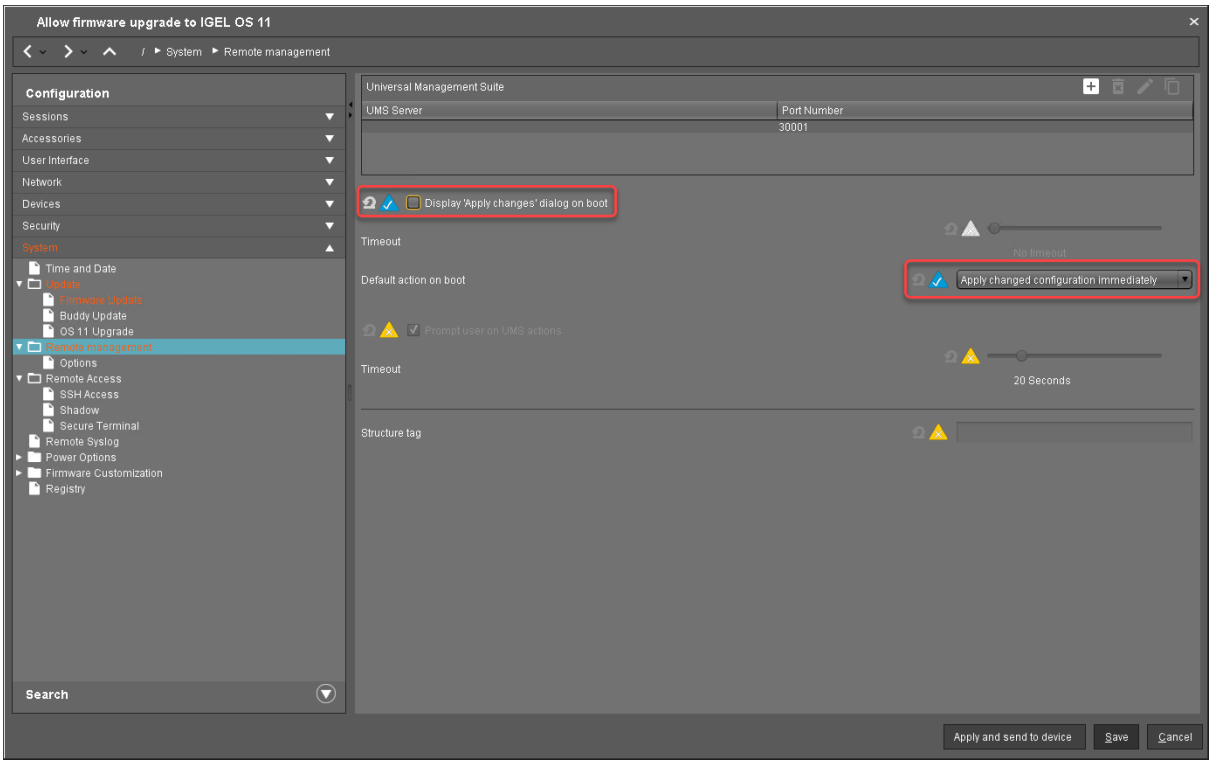
  In the following screenshot, FTP is used as an example. The other protocols can be used as well.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:
   - Activate **Upgrade to OS 11**.
   - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
   - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
   - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
   - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 169).

Deploying the Licenses

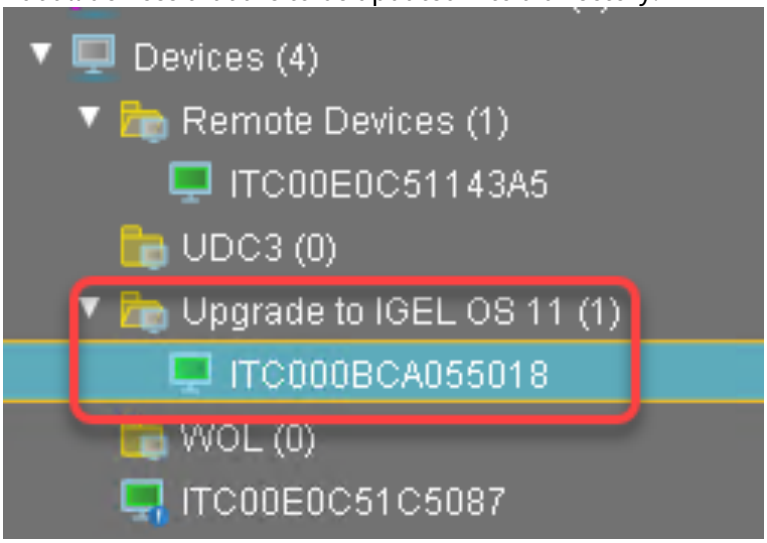
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*

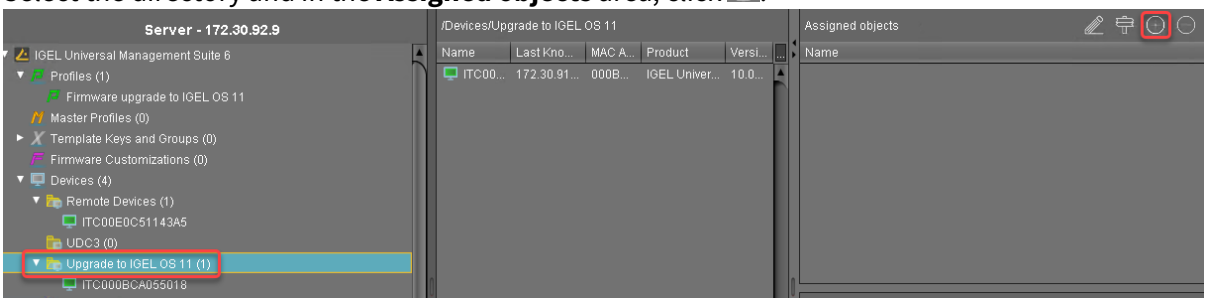
When the license deployment is set up, continue with Assigning the Profile 2.

Assigning the Profile

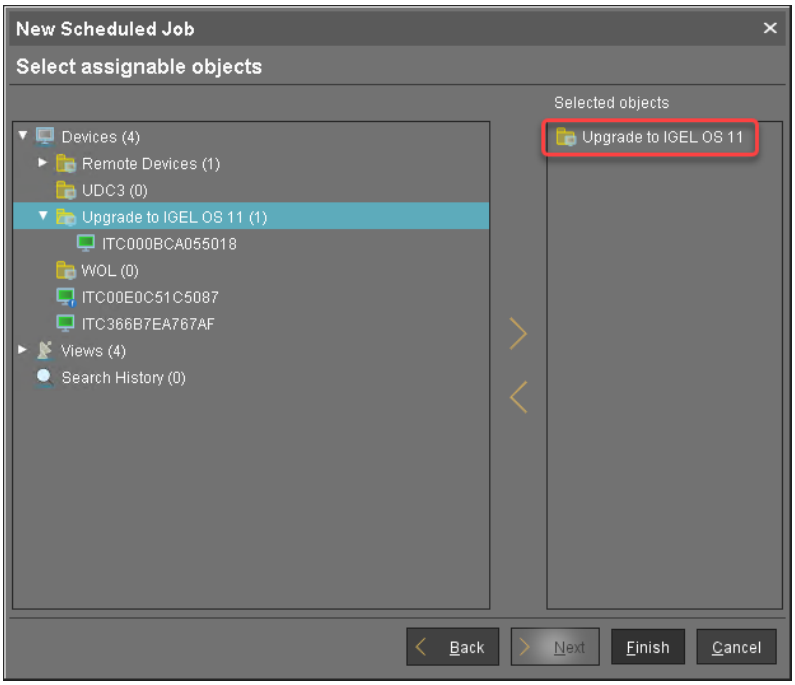
1. Put all devices that are to be updated into a directory.



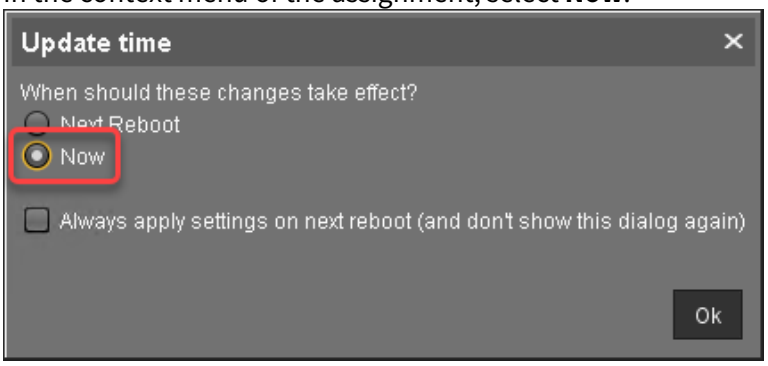
2. Select the directory and in the **Assigned objects** area, click .



3. Assign the profile (see Creating a Profile) to the directory and click **Ok**.



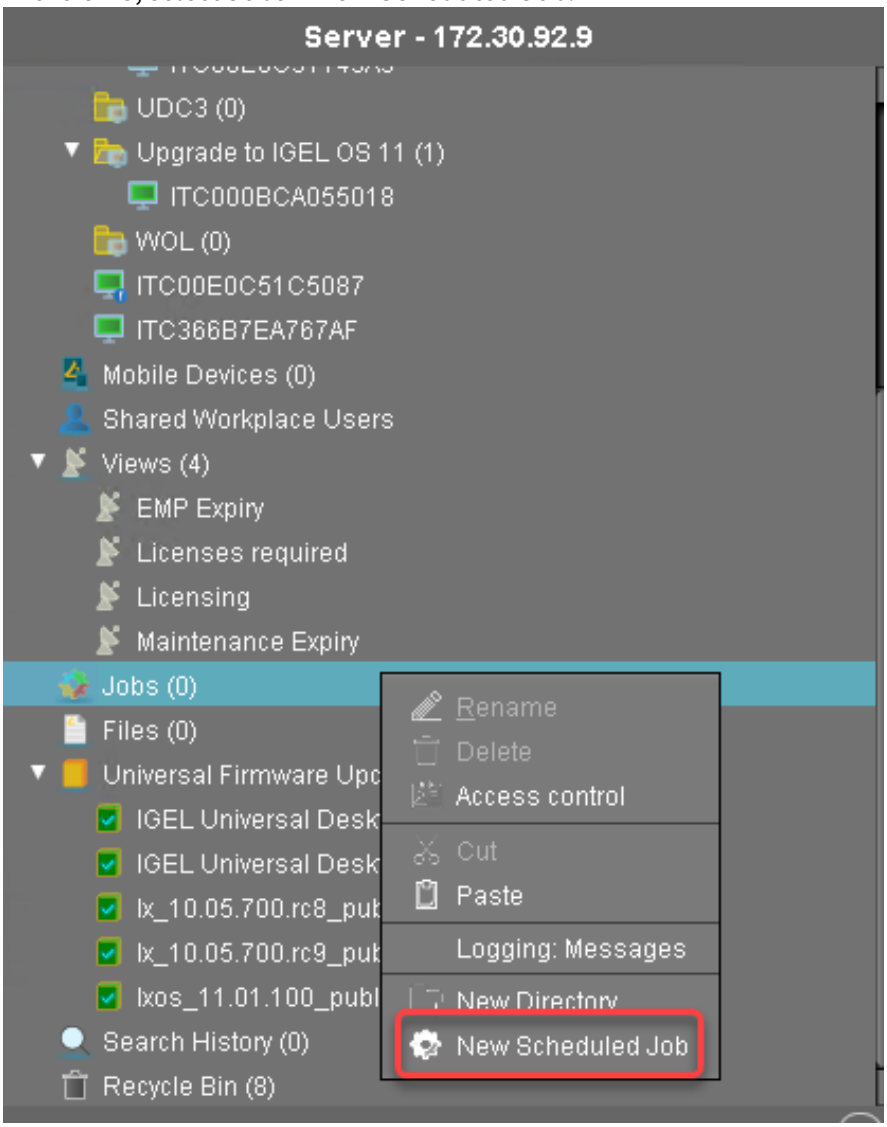
4. In the context menu of the assignment, select **Now**.



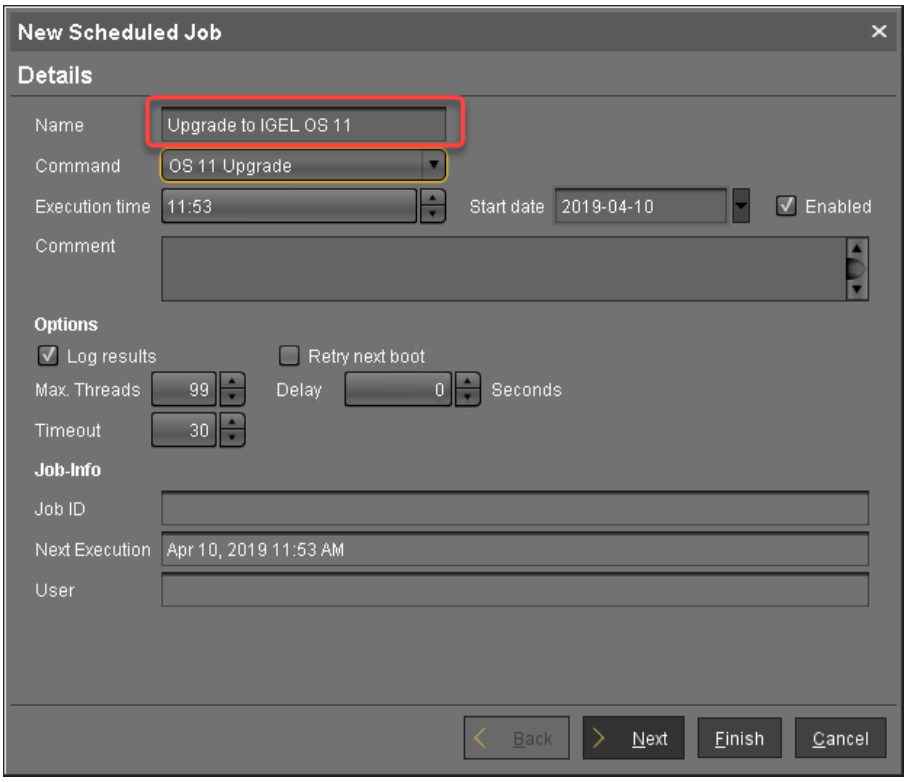
When the profile is assigned, continue with Creating the Scheduled Job (see page 218).

Creating the Scheduled Job

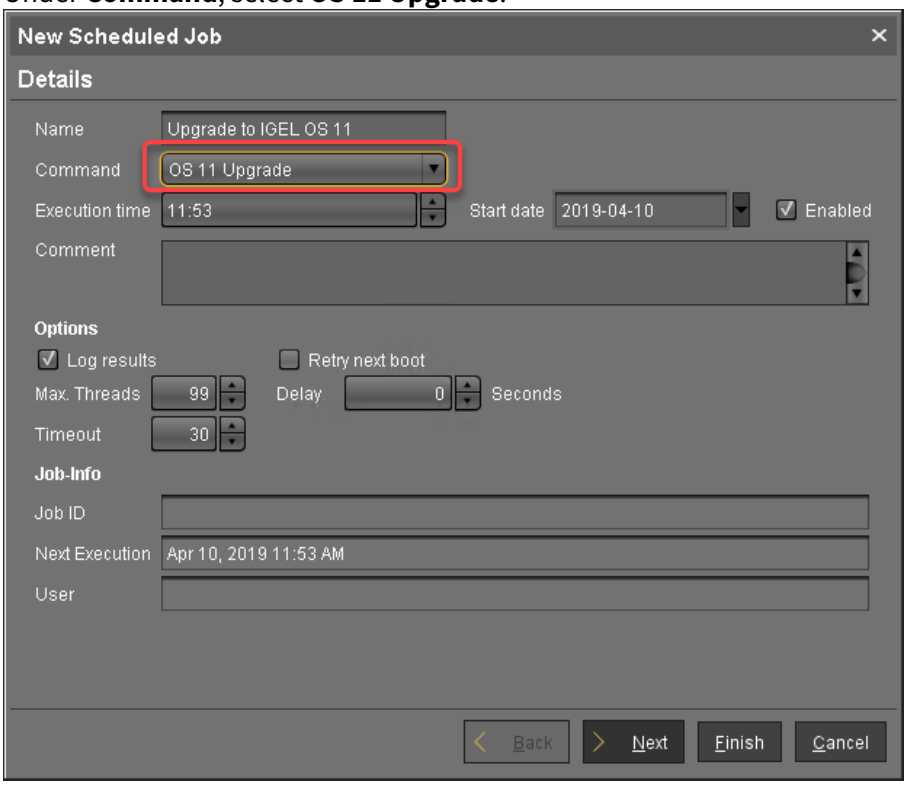
1. In the UMS, select **Jobs > New Scheduled Job**.



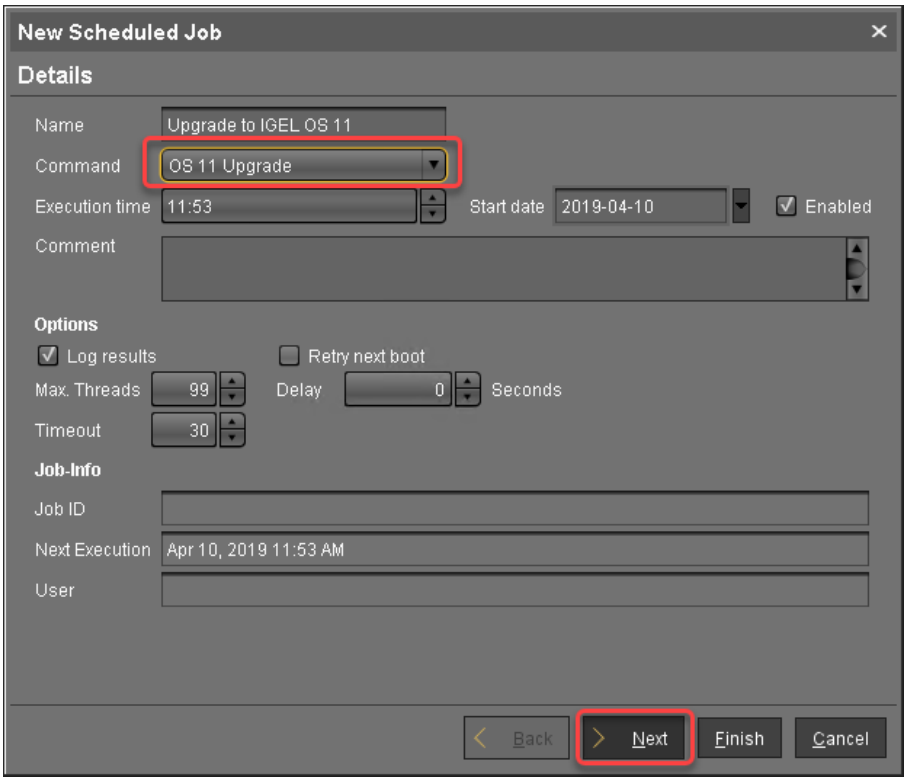
2. Under **Name**, enter a suitable name for the job, e. g. "Upgrade to IGEL OS 11".



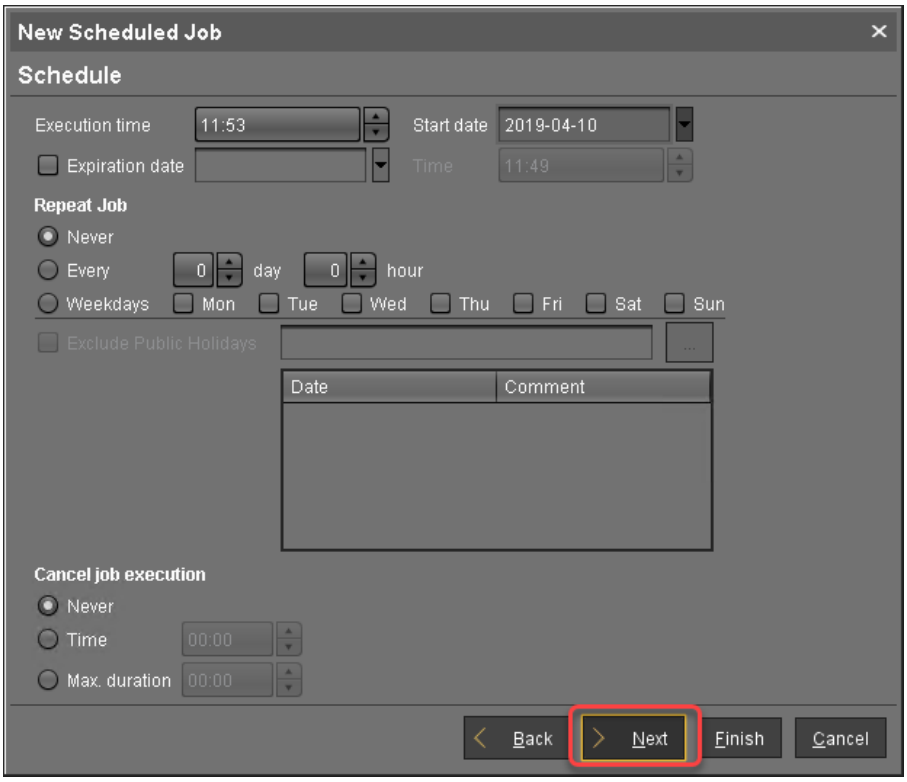
3. Under **Command**, select **OS 11 Upgrade**.



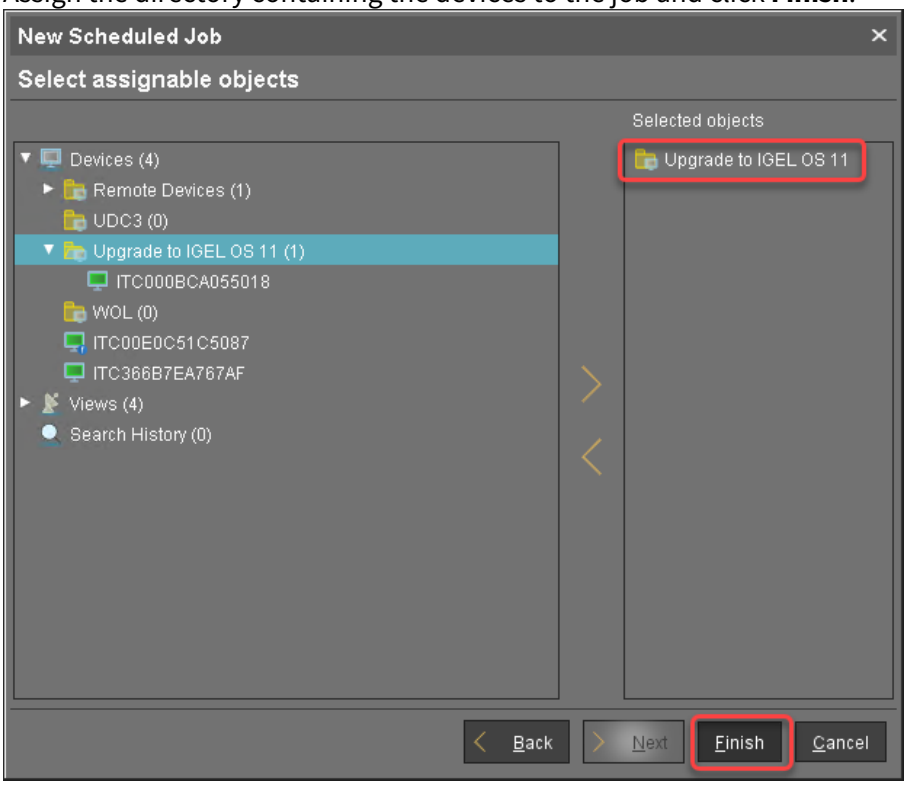
4. Under **Execution time** and **Start date**, set the time at which the upgrade should be executed, and click **Next**.



5. Review the execution time and click **Next**.



6. Assign the directory containing the devices to the job and click **Finish**.



Update Can Be Canceled After Timeout
An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

The upgrade is completed.

Troubleshooting

This section describes possible error cases and solutions.

- Regaining a Usable System (see page 224)
- Getting Error Messages (see page 225)
- Starting an New Upgrade Attempt (see page 226)
- Starting Another Upgrade Attempt after 5 Retries (see page 227)

Regaining a Usable System

Here you can find typical upgrade failures and the appropriate methods to regain a usable system.

Device Has Upgraded to Igel OS 11, but Does Not Boot Any More

To get a working IGEL OS 11 system:

→ Use the IGEL OS Creator to recover the IGEL OS 11 system. For more information, see the IGEL OS Creator Manual (see page 2119).

IGEL OS 10 Rescue System Fails to Update Missing Partitions

If a severe error has occurred during the upgrade process, the device boots into a minimal IGEL OS 10 (10.05.800 or higher) rescue system. If unattended, the device tries to download and update the missing partitions and reboots on failure.

To regain a full IGEL OS 10 system, you have two possibilities:

→ In the rescue system, start the Setup, go to **System > Update > Firmware Update** and set a valid update source for the appropriate IGEL OS 10 firmware (10.05.800 or higher).

Or:

→ Configure a UMS profile that contains a valid update source for the appropriate IGEL OS 10 firmware (10.05.800 or higher) under **System > Update > Firmware Update** and assign it to the device.

Getting Error Messages

→ Open the OS 11 Upgrade Tool (default path: click System and then **Upgrade to OS 11**).

The OS 11 Upgrade Tool shows the error messages. The most important message is prefixed with **Retries**; see the example below:

→ For more information, review the main migration log under `/wfs/migration.log`

You can use the system log viewer to review the migration log (see the chapter System Log Viewer (see page 1750) in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see the chapter Save TC Files for Support support).

Starting an New Upgrade Attempt

If you want the device to start multiple upgrade attempts (and the device is not already configured to do so):

1. In the UMS profile or in the Setup, go to **System > Update > OS 11 Upgrade** and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. Reboot the device.

Starting Another Upgrade Attempt after 5 Retries

When the **Upgrade to OS 11 even if a previous upgrade attempt failed** option is set and the upgrade has failed each time, the system will stop trying after 5 attempts.

To reset the retry counter:

1. In the Setup or the UMS profile, go to **System > Update > OS 11 Upgrade** and deactivate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. When the setting is effective on the devices, go to **System > Update > OS 11 Upgrade** again and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**..
   The retry counter is reset, and the devices will try upgrading another 5 times, if necessary.

Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11

This document describes how to upgrade any number of IGEL Universal Desktop devices (UD) from IGEL OS 10 to IGEL OS 11.

IGEL OS 10.05.700 or higher is required for upgrading to IGEL OS 11. If you have an older version of IGEL OS 10, you need to update to version 10.05.700 or a higher version first.

The following methods of mass deployment are described here:

- Zero-Touch Deployment Using Universal Firmware Update (see page 229): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using Universal Firmware Update. This method can be started immediately or as a scheduled job (wake up or reboot).
- Zero-Touch Deployment Using Buddy Update (see page 262): Mass upgrade from any version of IGEL OS 10 to IGEL OS 11 in one step using two devices as update buddies. This method can be started immediately or as a scheduled job (wake up or reboot).
- Mass Deployment Using a Scheduled Job (see page 283): Upgrade devices that are already running IGEL OS 10.05.700 (or higher) using a specific scheduled job.

Zero-Touch Deployment Using Universal Firmware Update

This method is the most convenient way to upgrade from IGEL OS 10 to IGEL OS 11. The method uses the Universal Firmware Update feature of the UMS (Universal Management Suite) and a profile.

Read all the following chapters carefully and follow the instructions.

- IGEL Devices That Can Be Upgraded to IGEL OS 11 (see page 230)
- Important! Consider This Before Upgrading from OS 10 to IGEL OS 11 (see page 232)
- Preparing the Upgrade (see page 233)
- Testing the Upgrade to OS 11 in Zero-Touch Deployment (see page 238)
- Checking the Requirements (see page 243)
- Creating the Universal Firmware Updates (see page 244)
- Creating a Profile (see page 250)
- Deploying the Licenses (see page 255)
- Putting It All Together (see page 256)
- Executing the Upgrade (see page 259)

IGEL Devices That Can Be Upgraded to IGEL OS 11

Core Requirements for IGEL OS 11

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB
  RAM size higher than 2 GB is recommended if you use any of the following:
  - Unified Communications optimizations (uses a client-side media engine)
  - High-resolution graphics output
    For details on the supported graphics-related characteristics of IGEL devices, see Graphics on IGEL Devices or, for older devices, Graphics on Legacy IGEL Devices .
  - More than two monitors
- Storage: 2 GB minimum; ≥ 4 GB recommended
  Storage Requirements for IGEL OS 11.04 or Higher
  IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD2****	D220	40	Yes	2 GB	4 GB	Yes
UD2*	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51 / 52***	Yes	2 or 4 GB	8 GB	Yes
UD3*	M340C	50	Yes	2 GB	4 GB	Yes
UD3*	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5*	H830C	50	Yes	2 GB	4 GB	Yes
UD6*	H830C	51	Yes	2 GB	4 GB	Yes
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7**	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD9*	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

*IGEL UD3-LX 50 and UD5-LX 50 are supported up to IGEL OS 11.05, incl. private builds.

IGEL UD9-LX 40 / 41 (Touch) devices are supported up to IGEL OS 11.07.910.
IGEL UD2-LX 50 devices are supported up to IGEL OS 11.09.160.
IGEL UD3-LX 51 devices are supported up to IGEL OS 11.09.160.
IGEL UD6-LX 51 devices are supported up to IGEL OS 11.09.160.

** As of December 2019, IGEL UD7 model H850C is equipped with the (en) AMD Secure Processor ; for further information, see (en) UD7 Model H850C .

*** IGEL UD2-LX 52 is supported with IGEL OS 11.06.140 and later.

**** UD2-LX 40 (model D220) is supported up to IGEL OS 11.08.200. For an overview of the end-of-sales (EOS) and end-of-maintenance (EOM) dates for IGEL devices, see Legacy IGEL OS Hardware Support .

IGEL Zero

Note on IZ Devices

The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also https://www.igel.com/os11migration/ .

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider Important! Consider This Before Upgrading 1 (see page 232).

Important! Consider This Before Upgrading from OS 10 to IGEL OS 11

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

Existing partitions: Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

No Downgrade
You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

Features (e.g. Clients)
IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions
The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

Custom Commands
The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

Power Supply
Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

Network
All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard or mobile broadband.

When you have considered everything that is relevant, continue with Preparing the Upgrade (see page 233).

Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

First of all, you should check thoroughly if IGEL OS 11 has all features required for your purposes.

→ Continue with Preparing the UMS (see page 234).

.

Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see *Universal Management Suite > UMS Reference Manual > UMS Installation and Update > IGEL UMS Update*.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter *Universal Management Suite > UMS Reference Manual > Registering IGEL OS Devices on the UMS Server.*

When the UMS is prepared, continue with Adjusting the Setup (see page 235).

Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
    - Activate **Upgrade to OS 11**.
    - If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
    - If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
    - Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
        - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
        - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
        - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
    - Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see Zero-Touch Deployment Using Universal Firmware Update (see page 229), Zero-Touch Deployment Using Buddy Update (see page 262) and Mass Deployment Using a Scheduled Job (see page 283)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.
3. Click **Apply**.
4. Continue with Deploying a License 2.

Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality
- If one of the following features is used, one Enterprise Management Pack license is required:
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

→ Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Download three demo licenses from

  https://www.igel.com/download/

When the device has a license, continue with Configuring the Update Source 3.

Configuring the Update Source

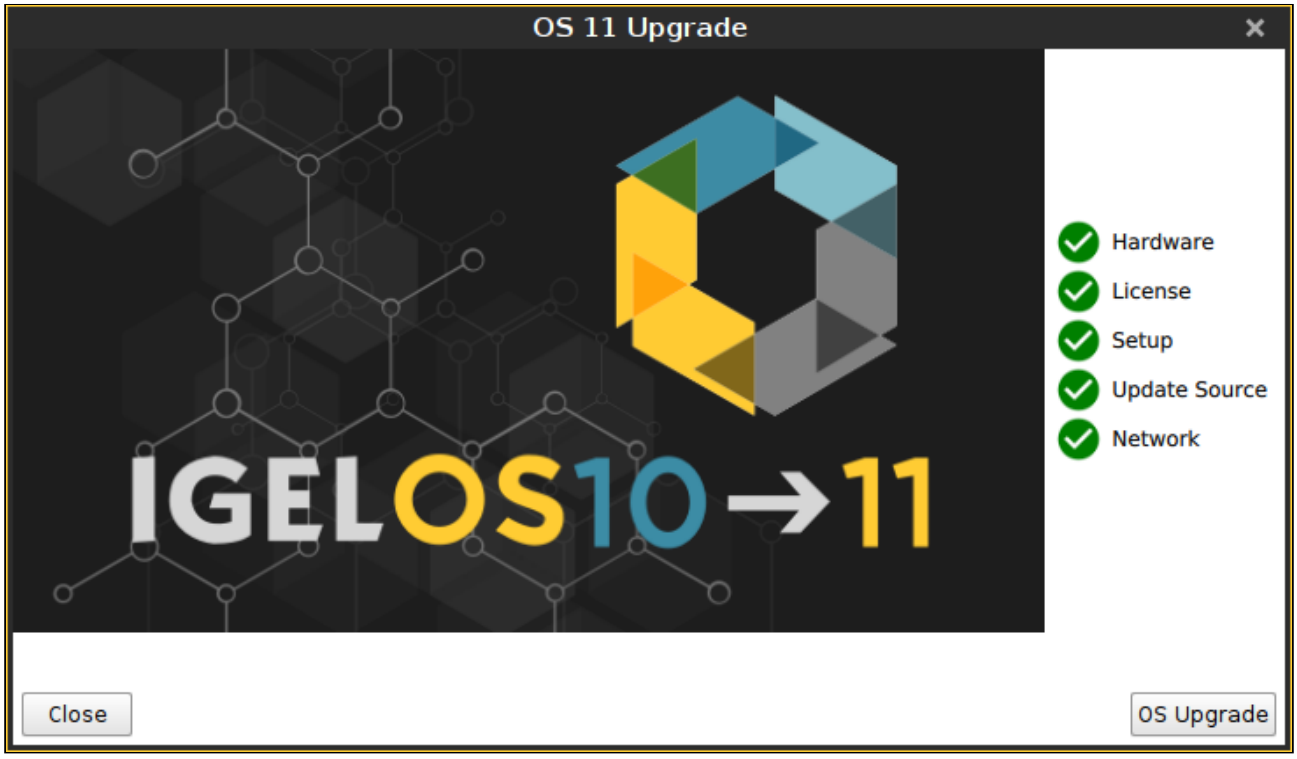
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update Settings for IGEL OS (see page 2056) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade to OS 11 in Zero-Touch Deployment (see page 238).

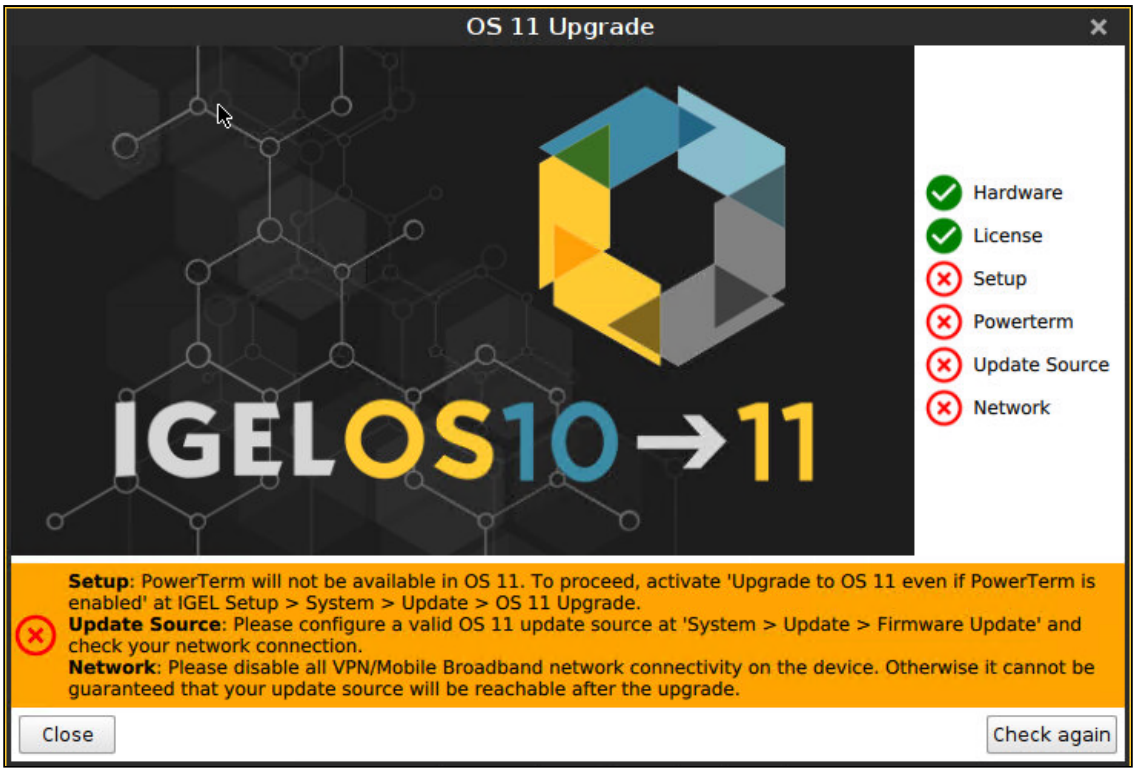
Testing the Upgrade to OS 11 in Zero-Touch Deployment

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

> You can change the starting the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

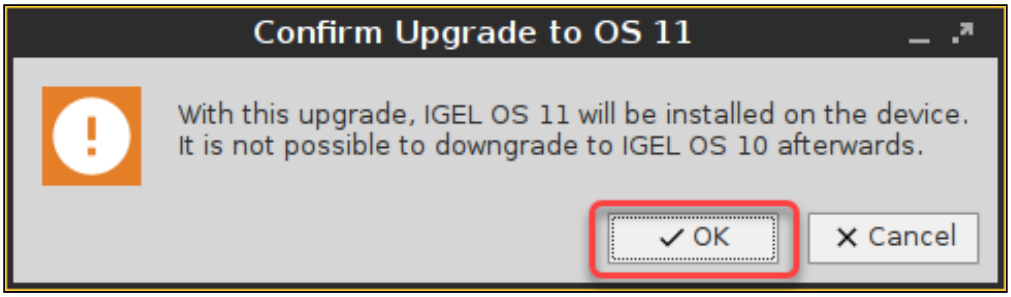


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:
   - If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
   - If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**, and you can start the upgrade.

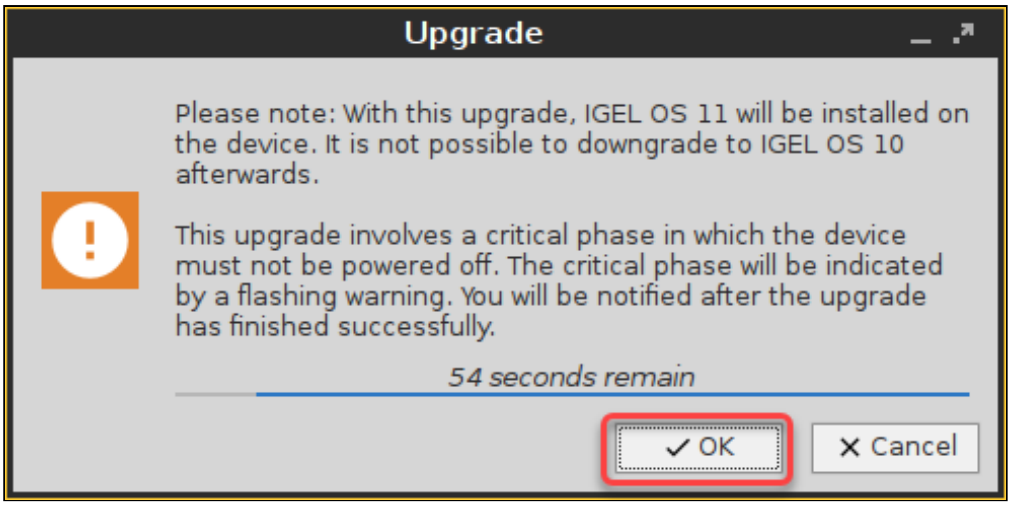


When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



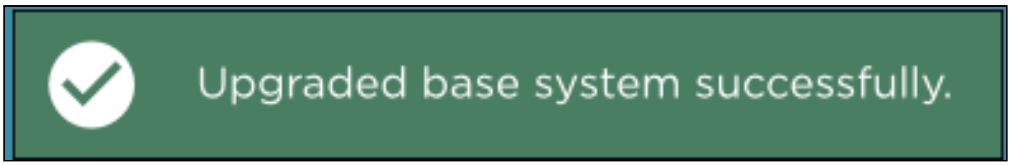
A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



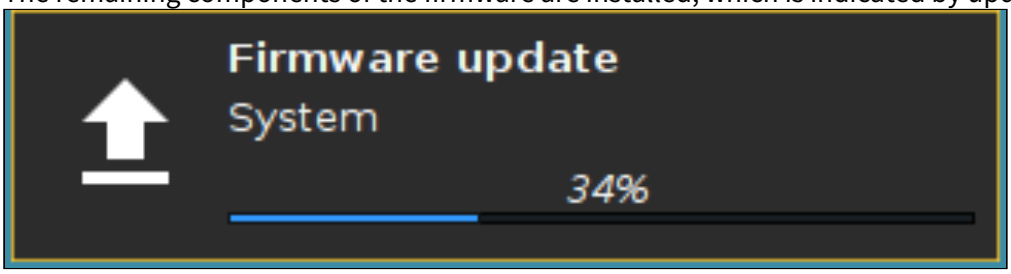
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window shows the progress.

During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.

When the base system is upgraded successfully, a message is shown.



The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:

After a few seconds the device reboots into IGEL OS 11.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 243).

Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The firmware IGEL OS 10.05.800 (or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all the requirements are met, continue with Creating the Universal Firmware Updates (see page 244).

Creating the Universal Firmware Updates

For detailed information, see the chapter (12.05.100-en) Universal Firmware Update in the IGEL UMS in the UMS Manual.

If you use the (12.06.100-en) IGEL UMS High Availability (HA), note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

1. Create a Universal Firmware Update for the appropriate IGEL OS 10 firmware (10.05.700 or higher).
2. After you have created the Universal Firmware Update for IGEL OS 10, create a Universal Firmware Update for IGEL OS 11.

The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see Executing the Upgrade (see page 259).

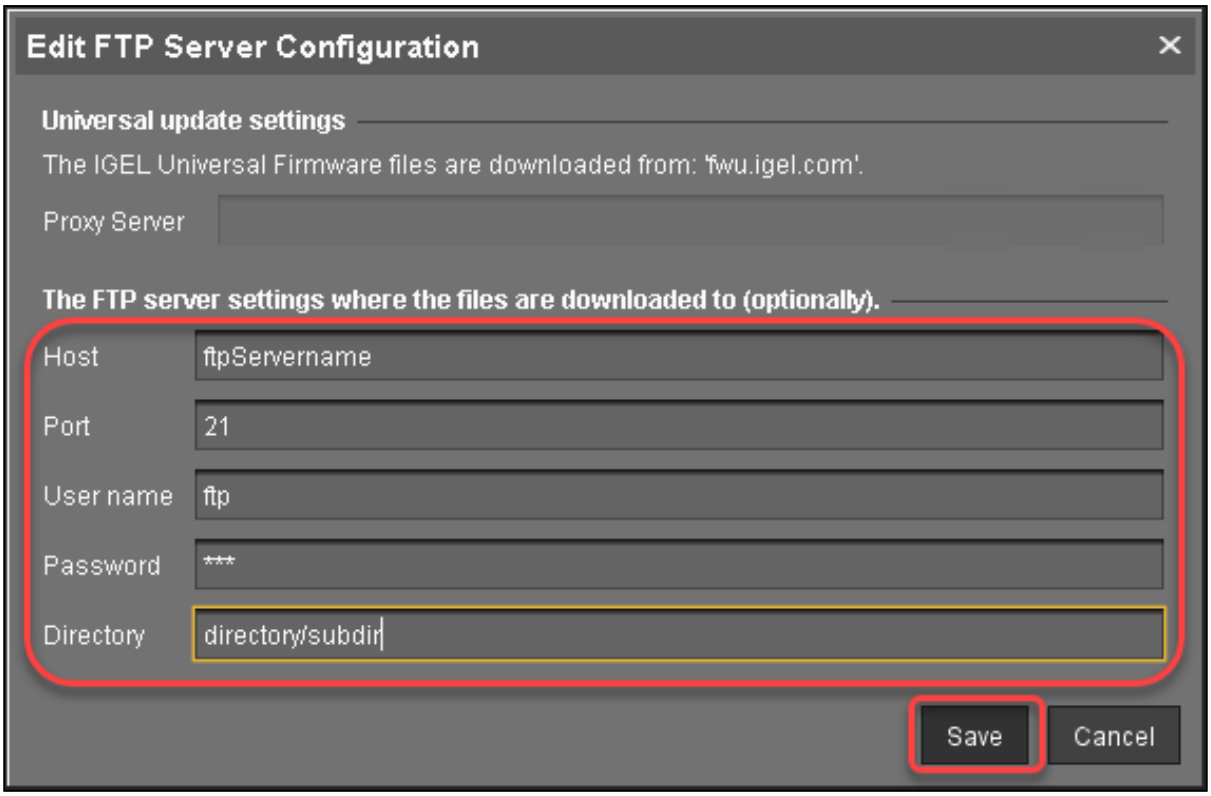
Configuring the Universal Firmware Update for ICG

If you are using IGEL Cloud Gateway (ICG), an FTP server that is accessible to all devices must be configured as the update source.

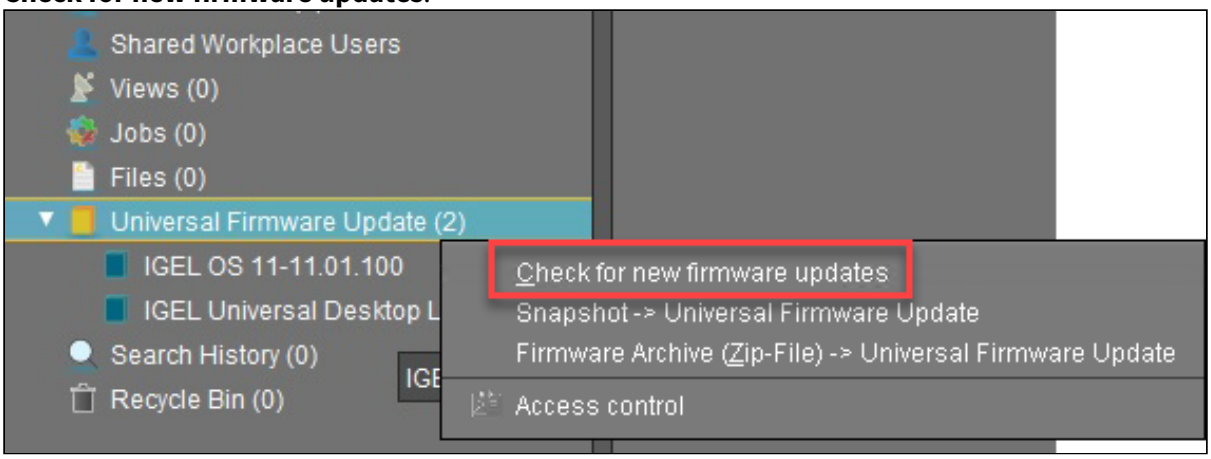
To configure an FTP server as update source:

1. In the UMS, go to **UMS Administration > Universal Firmware Update** and click

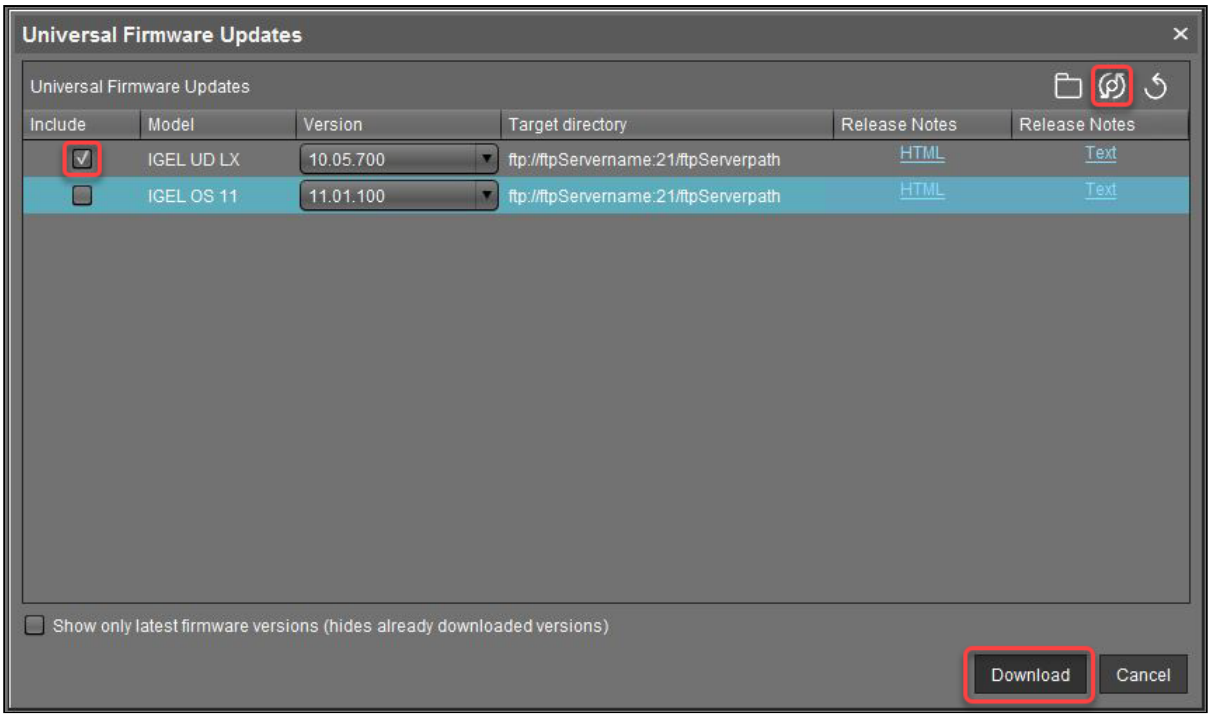
2. Enter the data required for accessing the FTP server and click **Save**.



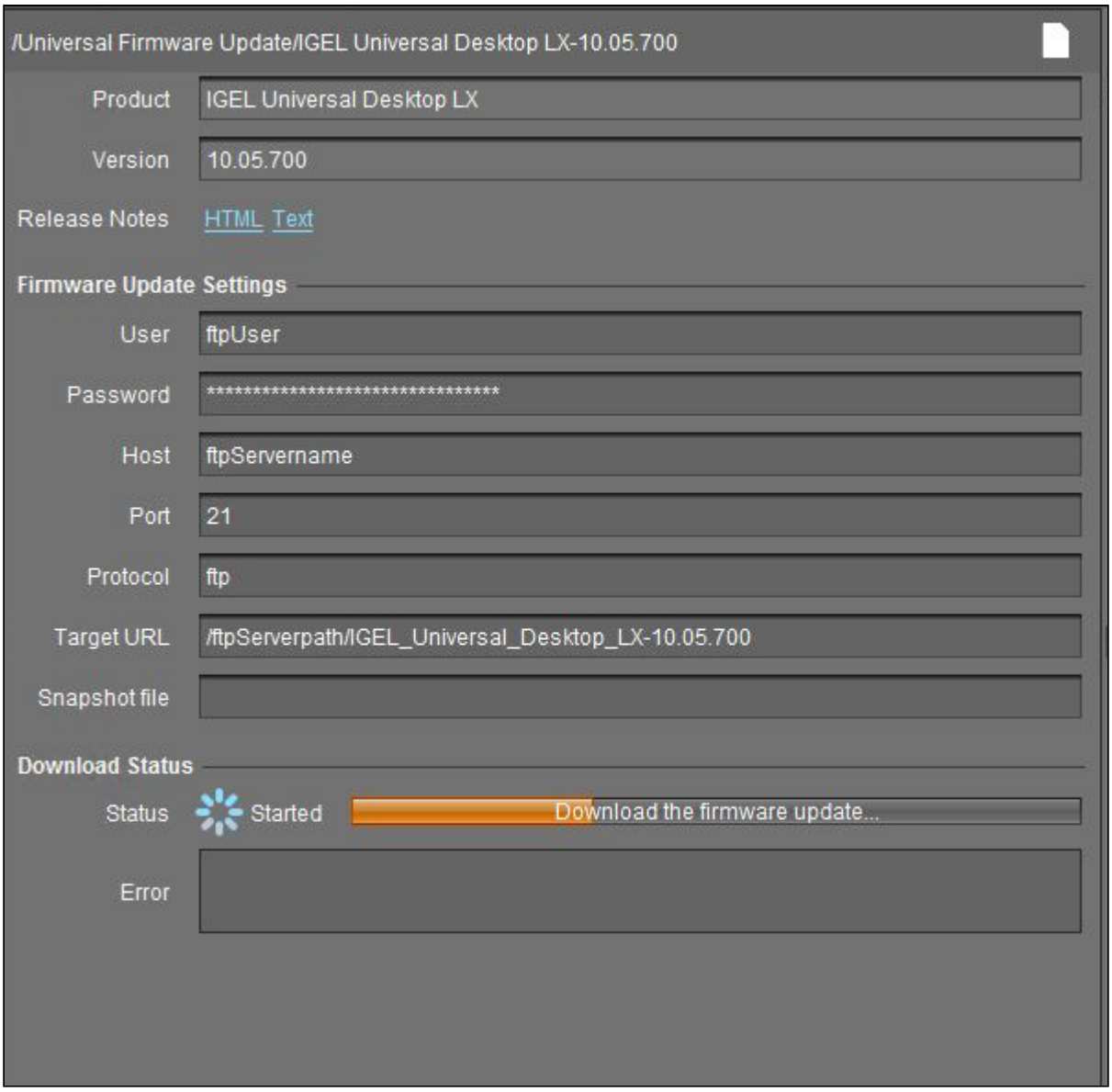
3. Go to **Server - [UMS address] > Universal Firmware Update** and in the context menu, select **Check for new firmware updates**.



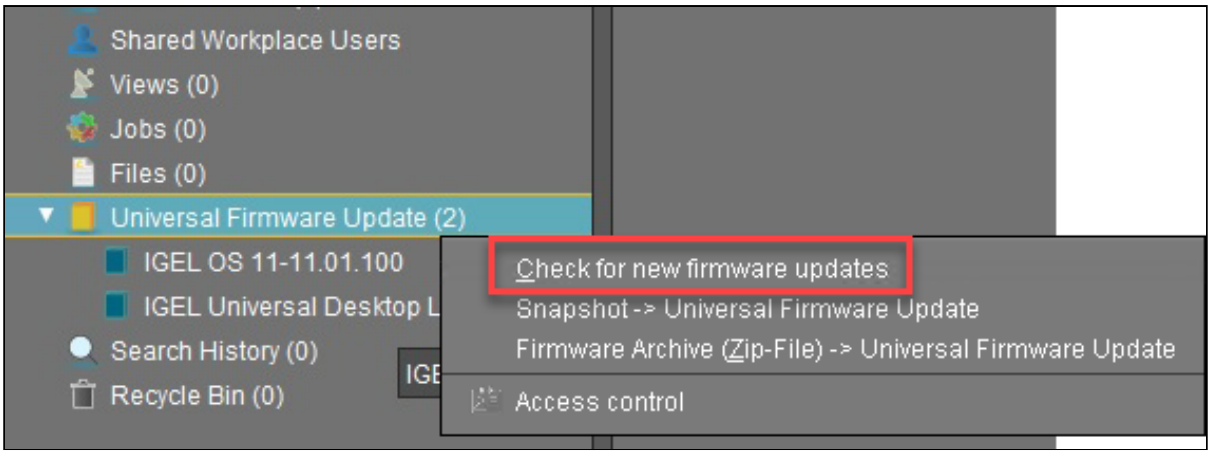
4. Select the entry for the appropriate IGEL OS firmware, click to select the FTP server selected in step 2 and select **Download**.



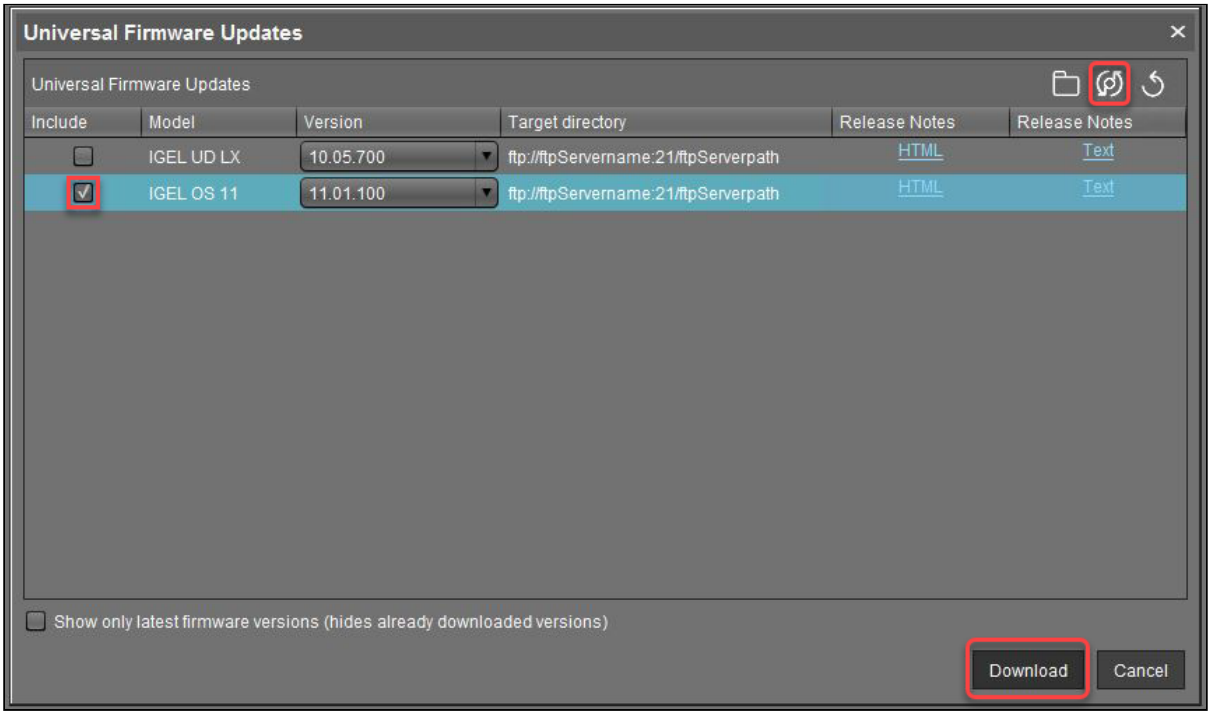
5. The firmware is transferred to the FTP server.



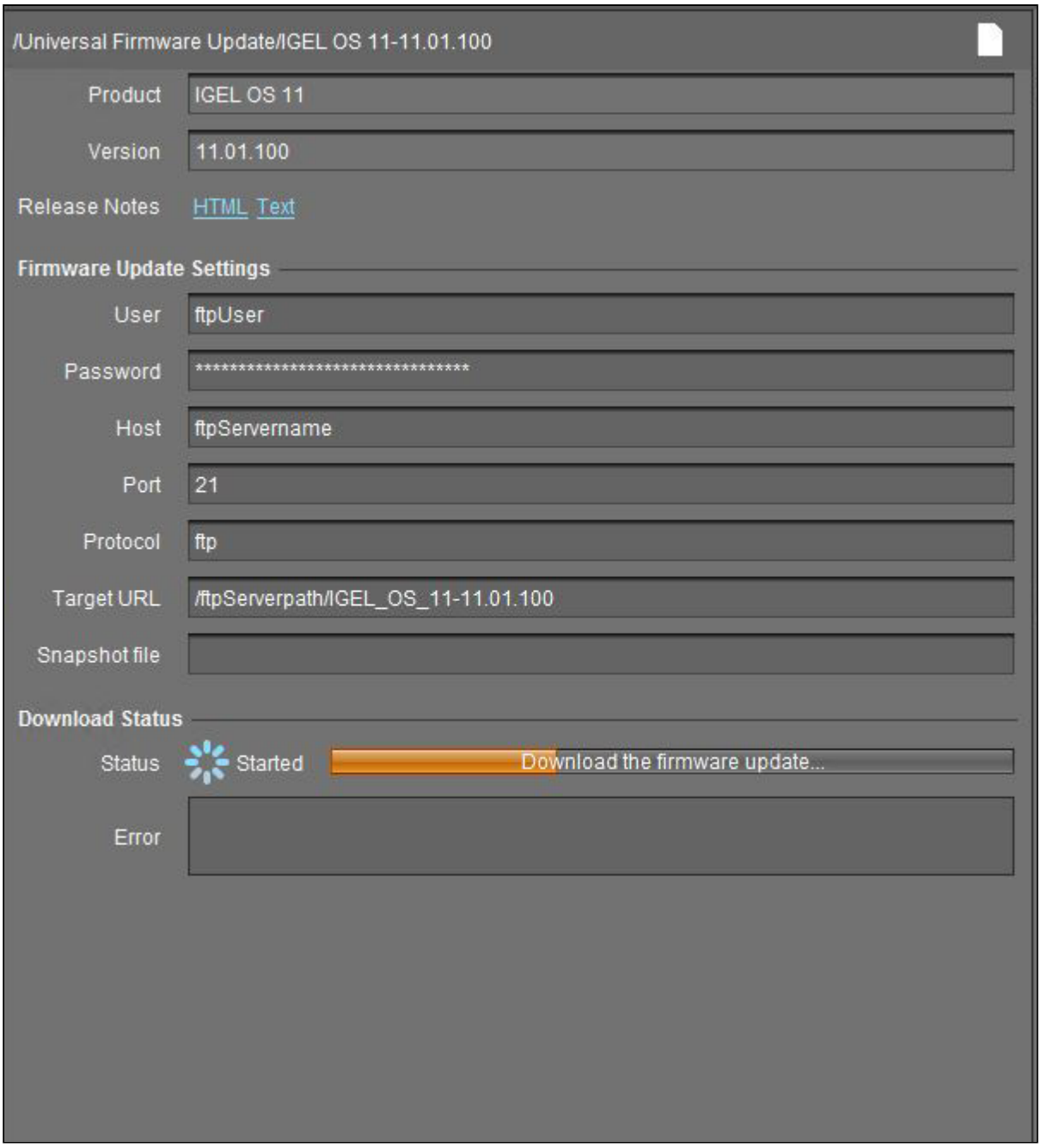
6. Under **Server - [UMS address] > Universal Firmware Update**, in the context menu, select **Check for new firmware updates** again.



7. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and select **Download**.



8. The firmware is transferred to the FTP server.

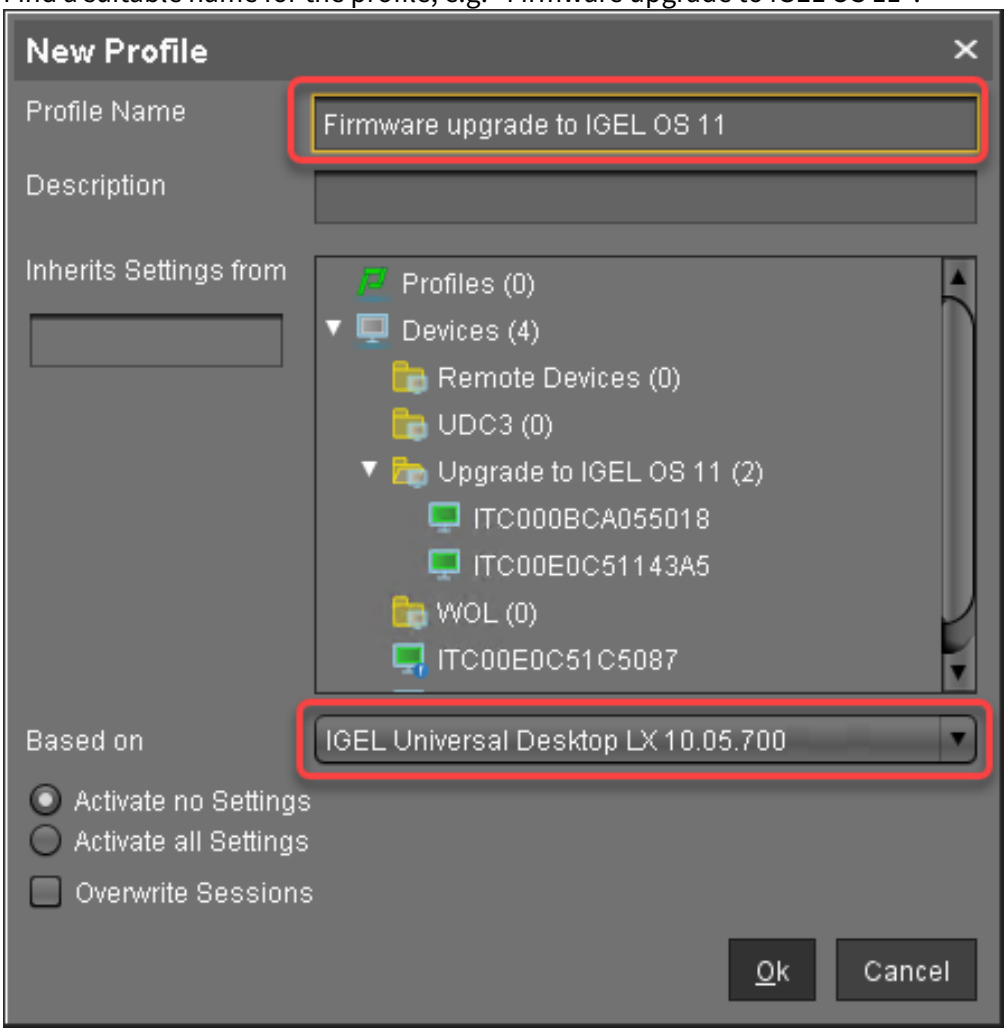


The devices can download the firmware from the FTP server.

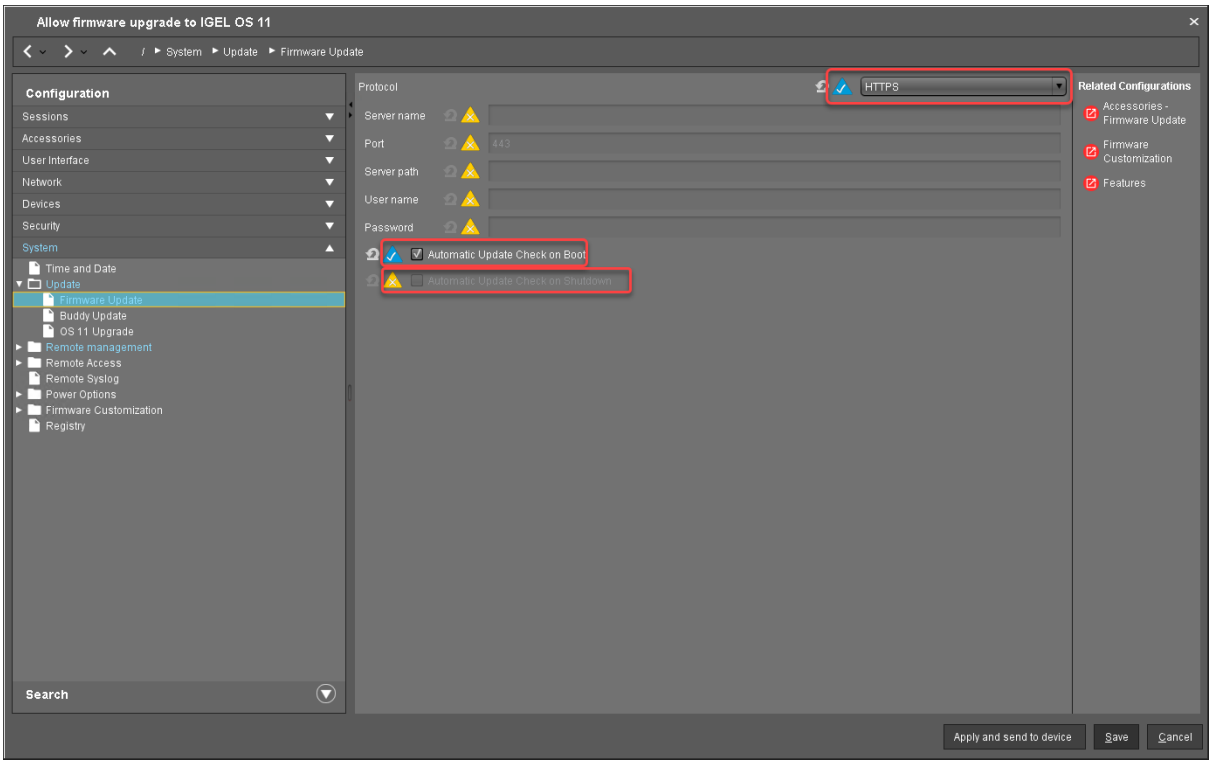
When the Universal Firmware Update is ready, continue with Creating a Profile 1 (see page 250).

Creating a Profile

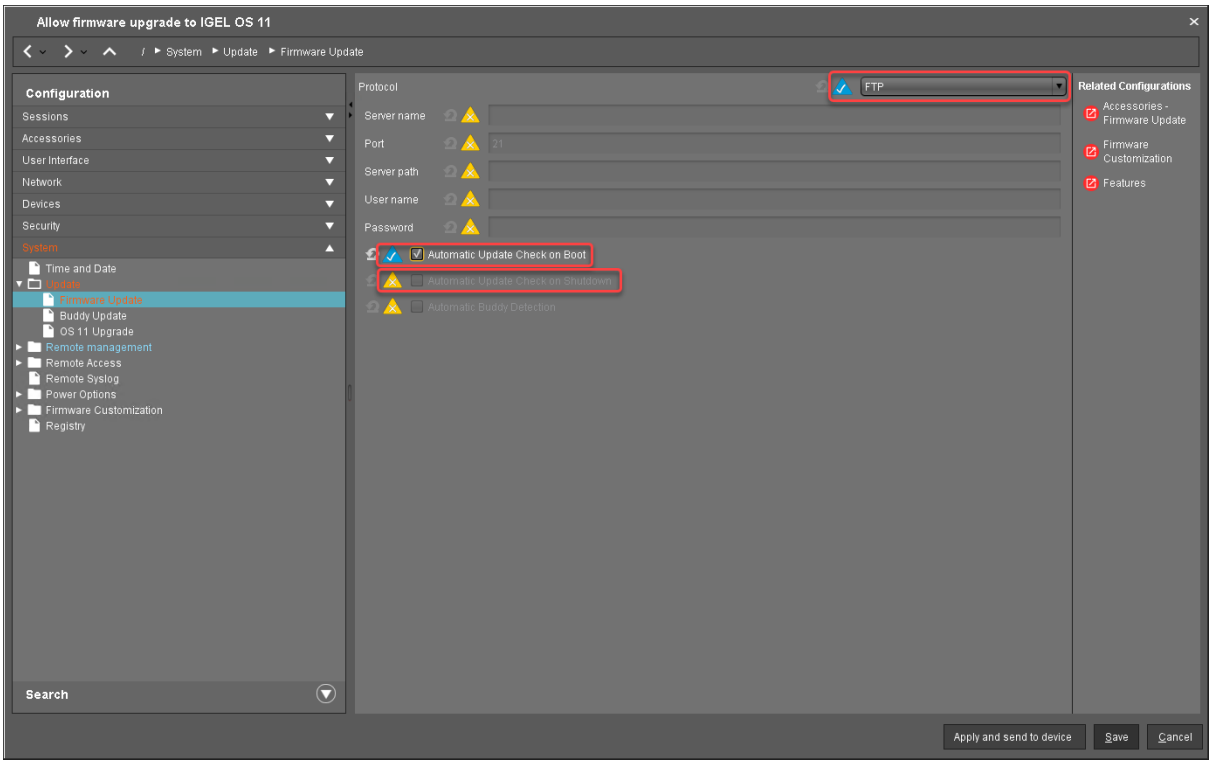
1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".



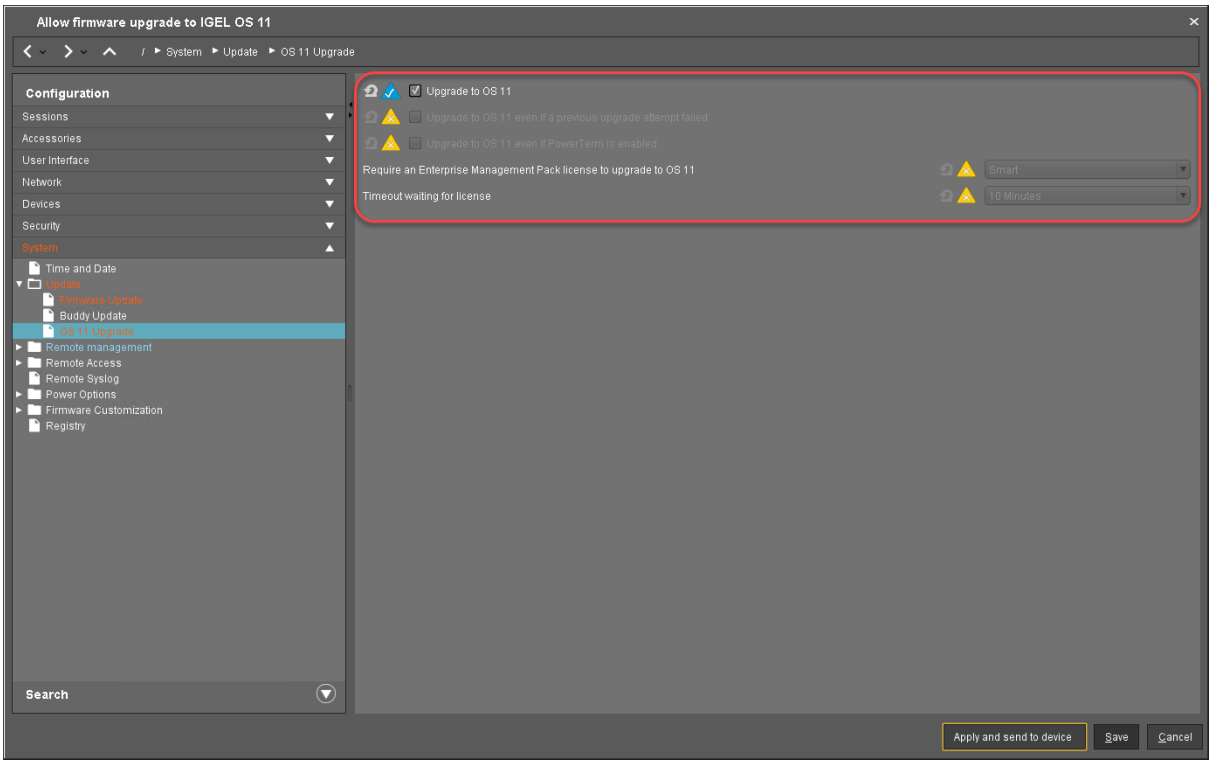
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:
   - If the UMS and the devices are in one and the same network, and no IGEL Cloud Gateway (ICG) is used:
     - Select "HTTPS" as **Protocol**.
     - Activate **Automatic Update Check on Boot**.
     - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



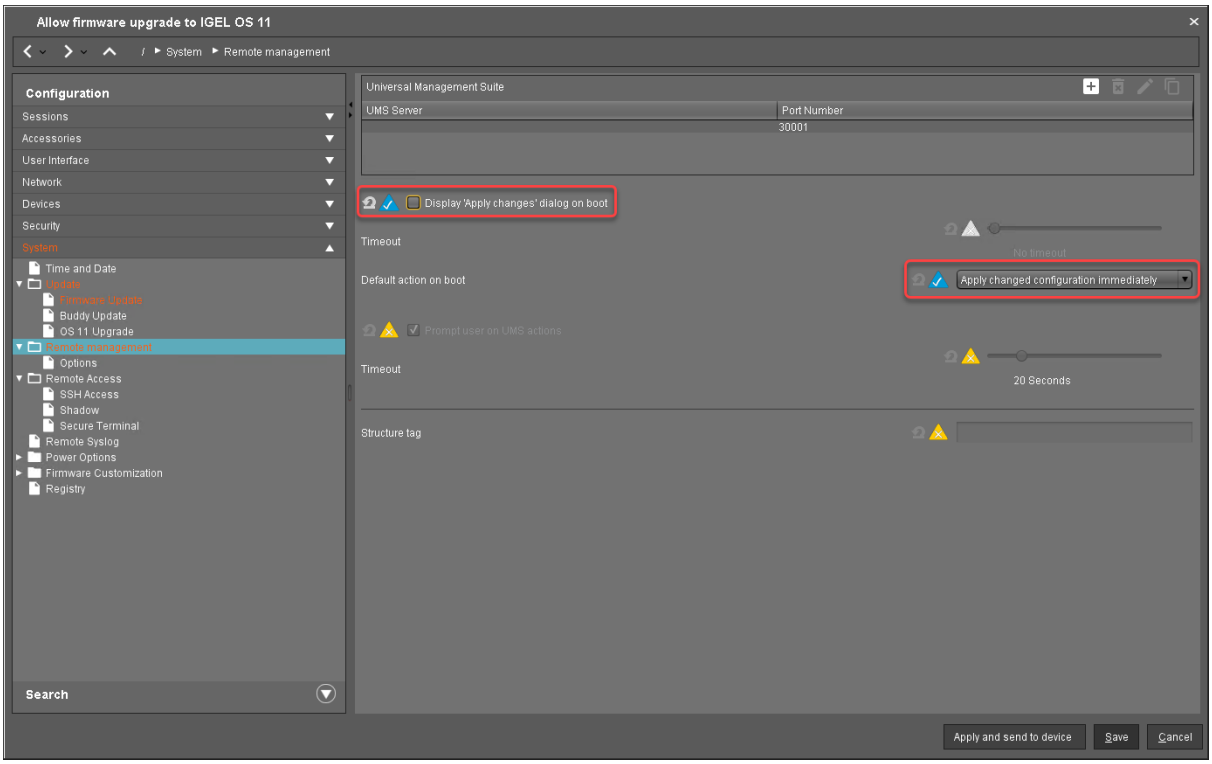
- If IGEL Cloud Gateway (ICG) is used:
  - Select "FTP" as **Protocol**.
  - Activate **Automatic Update Check on Boot**.
  - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:
    - Activate **Upgrade to OS 11**.
    - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
    - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
    - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
    - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile es created, continue with Deploying the Licenses (see page 255).

Deploying the Licenses

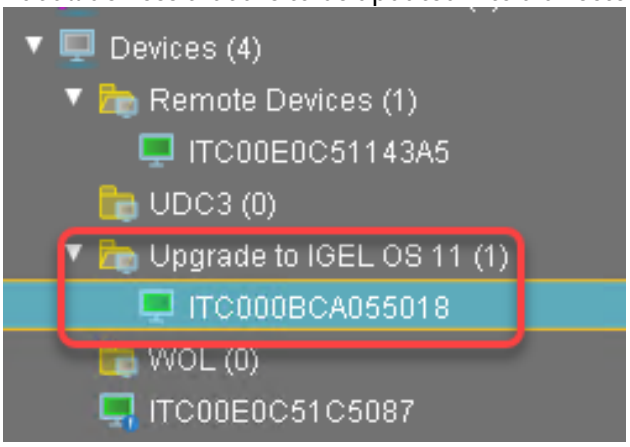
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*

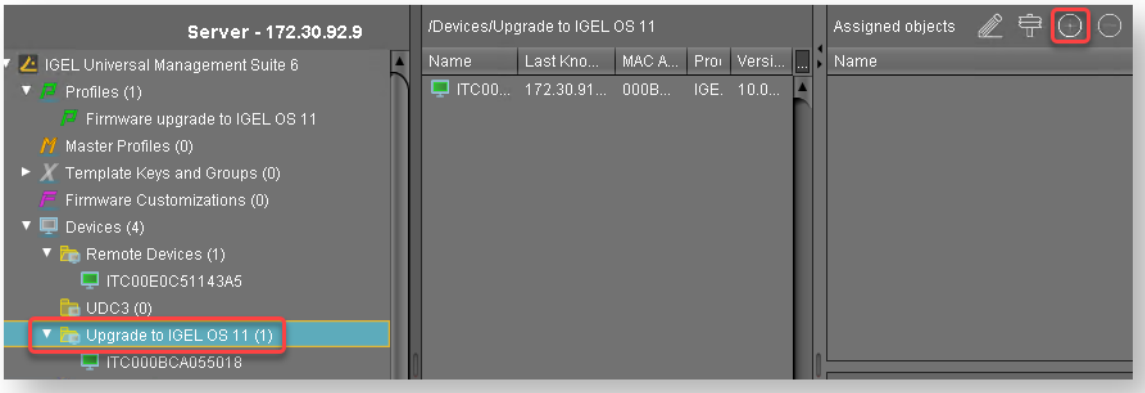
When the license deployment is setup up, continue with Putting It All Together (see page 256).

Putting It All Together

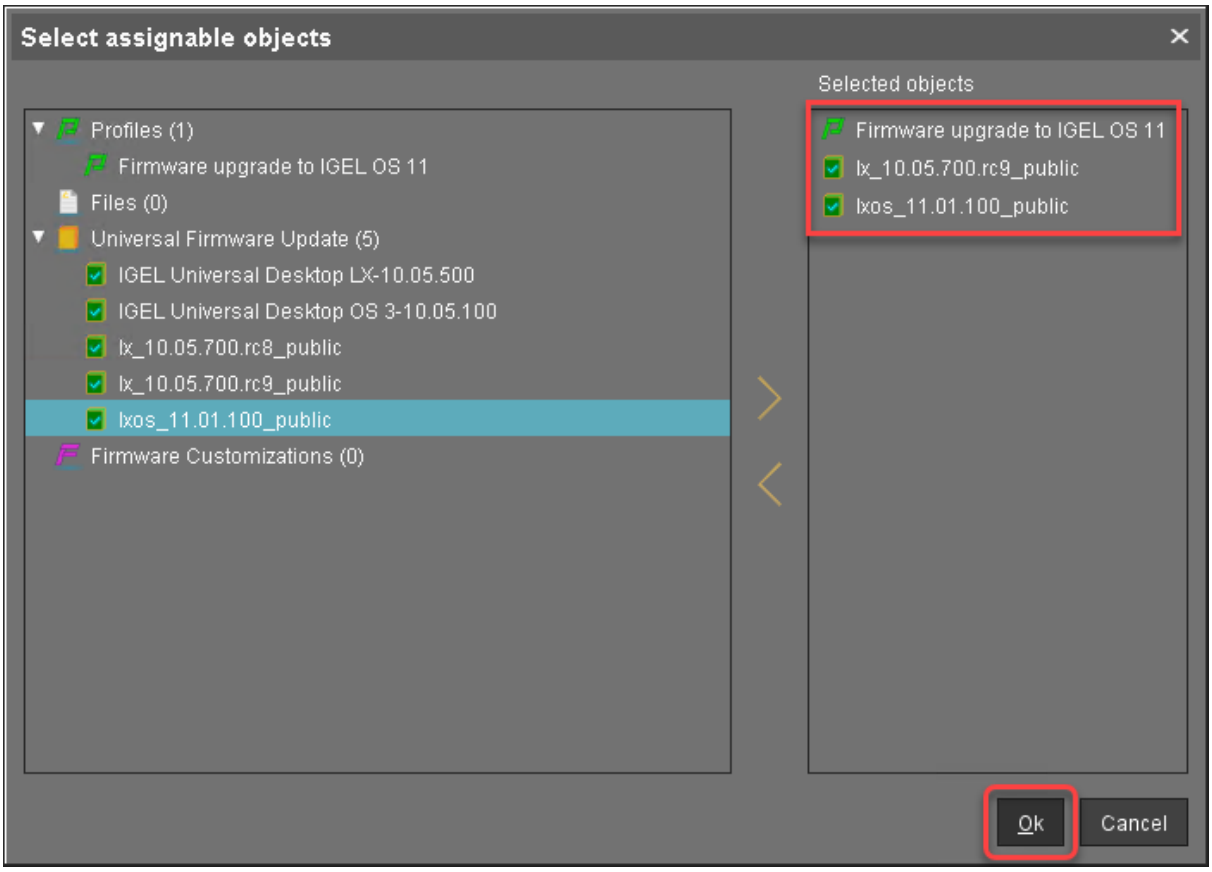
1. Put all devices that are to be updated into a directory.



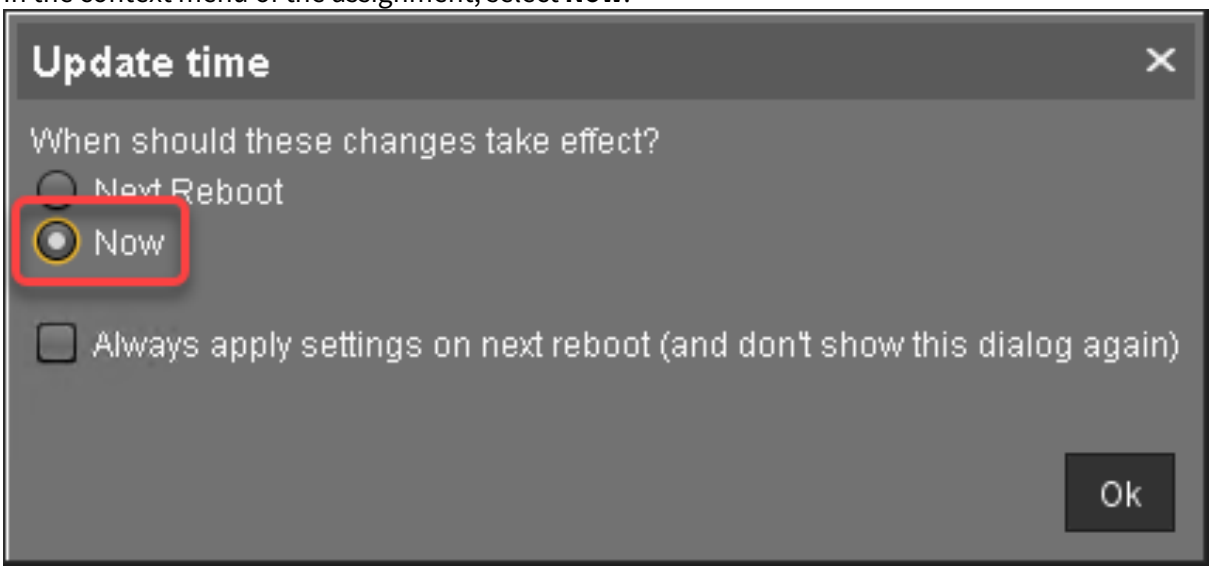
2. Select the directory and in the **Assigned objects** area, click .



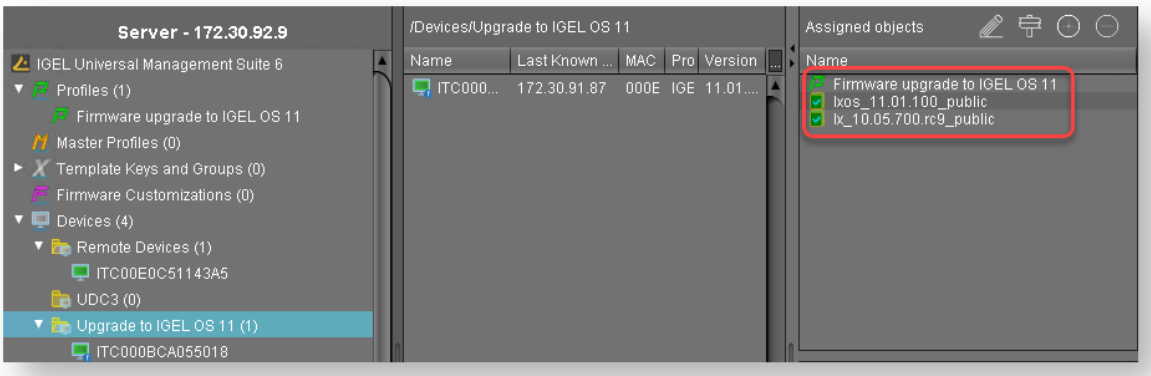
3. Assign the profile (see Creating a Profile 1 (see page 250)) and the two Universal Firmware Updates (see Creating the Universal Firmware Updates (see page 244)) to the directory and click **Ok**.



4. In the context menu of the assignment, select **Now**.



In the **Assigned objects** area, the profile and the Universal Firmware Updates are shown:



5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see *IGEL Subscription and More > IGEL Licensing > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) with ALD Token > How to Configure the Distribution Conditions of Licenses* section "Distributing Licenses to Devices in a Specified Directory".

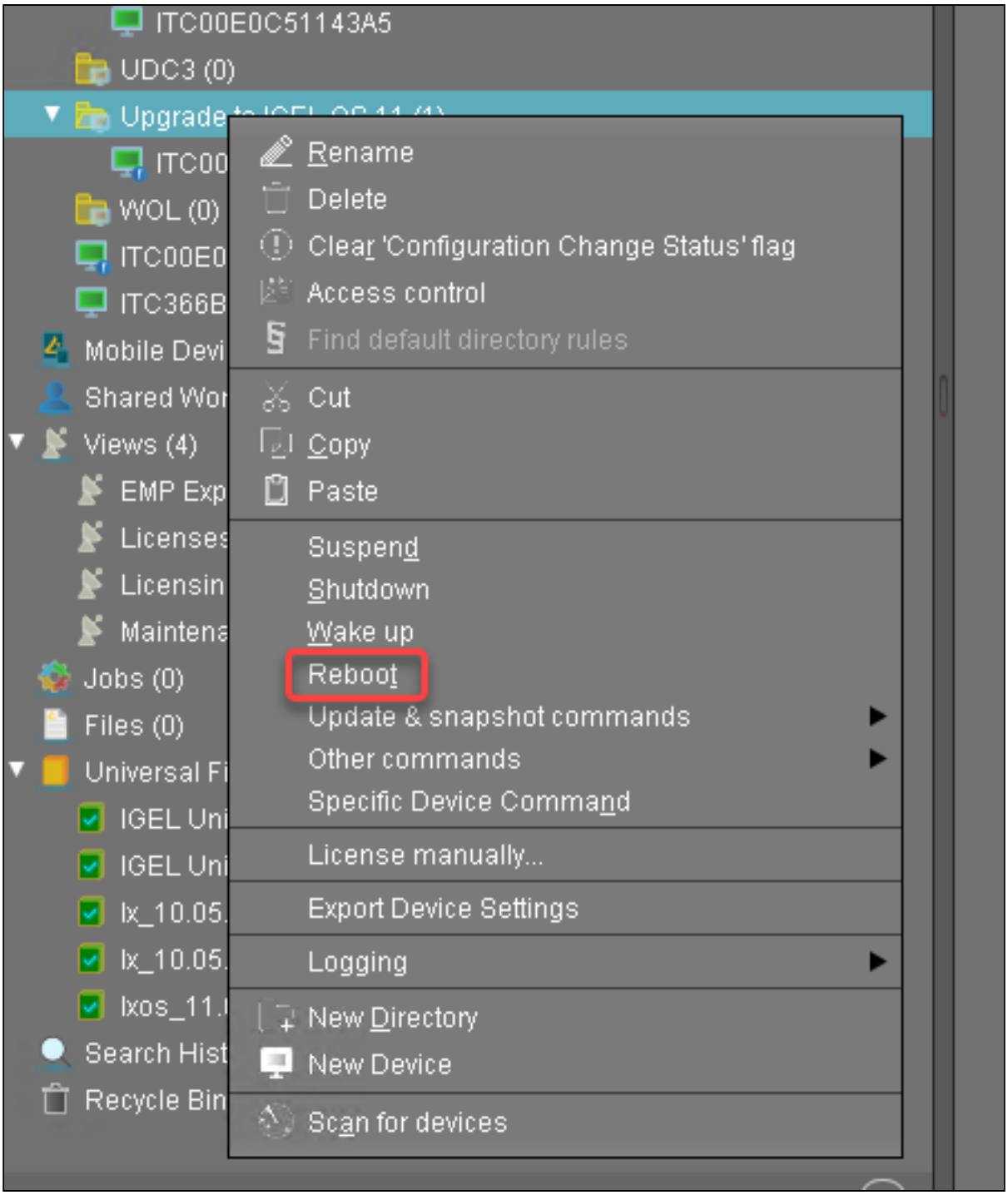
When everything is in place, continue with Executing the Upgrade (see page 259).

Executing the Upgrade

1. In the UMS, select the directory containing all devices that are to be upgraded and reboot them.

   Alternatively, you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices. For more information, see Jobs[45].

45. https://wiki.test.toolchain.igel.kreuzwerker.net/endpointmgmt-5.08/en/jobs-910606.html



On reboot or wake up, the devices update to the appropriate IGEL OS firmware version (10.05.700 or higher). With this version, the **Upgrade to OS 11** parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).

If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Adjusting the Setup (see page 235).
The parameter **Automatic update check on boot** causes the devices to look for new firmware again. Although two Universal Firmware Updates are assigned to the devices, the UMS offers the IGEL OS 11 firmware, because the ID of the IGEL OS 11 firmware is higher than the ID of the IGEL OS 10 firmware.

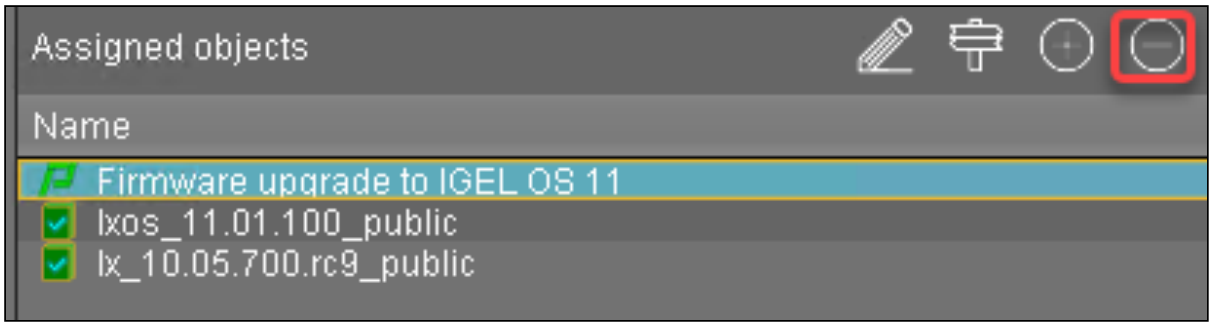
2.

Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

3. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile and the two Universal Firmware Updates from the directory.



The upgrade is completed.

Zero-Touch Deployment Using Buddy Update

This method uses the buddy update feature of IGEL OS. One or more devices that are configured as an update buddy access the main server and download the firmware. The other devices are configured to download their firmware from an update buddy.

Read all the following chapters carefully and follow the instructions.

- IGEL Devices That Can Be Upgraded to IGEL OS 11 (see page 263)
- Important! Consider This Before Upgrading (see page 265)
- Preparing the Upgrade (see page 266)
- Testing the Upgrade (see page 271)
- Checking the Requirements of the Buddy Update (see page 276)
- Configuring Two Update Buddies (see page 277)
- Creating a Profile (see page 278)
- Deploying the Licenses (see page 280)
- Putting It All Together (see page 281)
- Executing the Upgrade (see page 282)

IGEL Devices That Can Be Upgraded to IGEL OS 11

Core Requirements for IGEL OS 11

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

> RAM size higher than 2 GB is recommended if you use any of the following:
> - Unified Communications optimizations (uses a client-side media engine)
> - High-resolution graphics output
>
> For details on the supported graphics-related characteristics of IGEL devices, see Graphics on IGEL Devices or, for older devices,https://kb.igel.com/knowledge-base-archive/current/eol-eos-eom-archive.
> - More than two monitors

- Storage: 2 GB minimum; ≥ 4 GB recommended

> **Storage Requirements for IGEL OS 11.04 or Higher**
> IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD2****	D220	40	Yes	2 GB	4 GB	Yes
UD2*	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51 / 52***	Yes	2 or 4 GB	8 GB	Yes
UD3*	M340C	50	Yes	2 GB	4 GB	Yes
UD3*	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5*	H830C	50	Yes	2 GB	4 GB	Yes
UD6*	H830C	51	Yes	2 GB	4 GB	Yes

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7**	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9*	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

- IGEL UD3-LX 50 and UD5-LX 50 are supported up to IGEL OS 11.05, incl. private builds.

IGEL UD9-LX 40 / 41 (Touch) devices are supported up to IGEL OS 11.07.910.
IGEL UD2-LX 50 devices are supported up to IGEL OS 11.09.160.
IGEL UD3-LX 51 devices are supported up to IGEL OS 11.09.160.
IGEL UD6-LX 51 devices are supported up to IGEL OS 11.09.160.

** As of December 2019, IGEL UD7 model H850C is equipped with the (en) AMD Secure Processor ; for further information, see (en) UD7 Model H850C .

*** IGEL UD2-LX 52 is supported with IGEL OS 11.06.140 and later.

**** UD2-LX 40 (model D220) is supported up to IGEL OS 11.08.200. For an overview of the end-of-sales (EOS) and end-of-maintenance (EOM) dates for IGEL devices, see https://kb.igel.com/knowledge-base-archive/current/hardware-legacy-igel-devices.

IGEL Zero

Note on IZ Devices
The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also https://www.igel.com/os11migration/ .

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

When you have confirmed that your devices can be upgraded to IGEL OS 11, make sure to consider Important! Consider This Before Upgrading (see page 265).

Important! Consider This Before Upgrading

To make sure that your upgrade can be successful, check the following warnings and notes; a warning symbol indicates that irreversible damage can be done to your devices.

Existing partitions: Any existing partition on the target drive of your device will be deleted. The installer will repartition the target device. The overall size of the newly created partitions will be calculated based on the available disk space. The minimum disk usage is 2 GB, the maximum is 16 GB.

No Downgrade
You cannot restore your IGEL OS 10 system once you have migrated to IGEL OS 11. The device storage is overwritten completely with a new partitioning scheme.

Features (e.g. Clients)
IGEL OS 11 does not have the complete feature set of IGEL OS 10. Make sure that the current version of IGEL OS 11 meets your requirements. For details, refer to the appropriate release notes.

Custom Partitions
The contents of custom partitions will be deleted by the upgrade. Make sure to back up the contents and restore them after the upgrade has finished. Besides becoming dysfunctional after the upgrade, applications and kernel drivers in a custom partition might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. We recommend that you disable custom partitions when upgrading; you can enable them once the upgrade has been successfully completed.

Custom Commands
The persistence of custom commands cannot be guaranteed. Besides becoming dysfunctional after the upgrade, custom commands might corrupt the upgrade. For this reason, make sure to first test the upgrade on a characteristic device. In general, custom commands must be adapted for IGEL OS 11. We recommend that you disable custom commands when upgrading; you can enable them once the upgrade has been successfully completed.

Power Supply
Ensure that the device is not running on battery power, i.e. it must be connected to a power supply during the complete upgrade process.

Network
All devices must be connected to a WLAN or LAN. LAN is the recommended option. The device will not be upgraded if connected to OpenVPN, OpenConnect, genucard or mobile broadband.

When you have considered everything that is relevant, continue with Preparing the Upgrade (see page 266).

Preparing the Upgrade

This section describes the required preparations and tests before any productive devices can be updated. The testing should be done with at least one device that is characteristic of your environment. This device should have every custom partition and every custom command that may possibly exist in any of your devices.

To prepare the upgrade, perform the following steps:

- Preparing the UMS (see page 267)
- Adjusting the Setup (see page 268)
- Deploying a License (see page 269)
- Configuring the Update Source (see page 270)

Preparing the UMS

To upgrade your devices to IGEL OS 11, you need the appropriate version of the UMS. Also, the devices must be registered with the UMS to receive their licenses.

1. If you have not already done so, update your UMS to version 6.01.130 or higher. For instructions, see *Universal Management Suite > UMS Reference Manual > UMS Installation and Update > IGEL UMS Update*.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter *Universal Management Suite > UMS Reference Manual > Registering IGEL OS Devices on the UMS Server.*

When the UMS is ready, continue with Adjusting the Setup (see page 268).

Adjusting the Setup

Depending on the features that are in use now or will be used in the future, a specific set of parameters must be set in the device's Setup.

1. In the Setup, go to **System > Firmware Update > OS 11 Upgrade**.
2. Make your settings as appropriate:
    - Activate **Upgrade to OS 11**.

> When **Upgrade to OS 11** is activated, the device checks for a Workspace Edition license and stops checking for a legacy UDC3 or UD Pocket license. Therefore, in the UMS, it is displayed as an unlicensed device until a Workspace Edition license has been deployed.

- If you want the device to retry the upgrade immediately after a failed attempt, activate **Upgrade to OS 11 even if a previous upgrade attempt failed**. The device will retry the upgrade 5 times. When the 5th attempt has failed, a message will be shown in the upgrade tool window.
- If your device has a PowerTerm license, and you want to upgrade to IGEL OS 11 even though it does not support PowerTerm, you must activate **Upgrade to OS 11 even if PowerTerm is enabled**.
- Under **Require an Enterprise Management Pack license to upgrade to OS 11**, select the appropriate option:
    - If you are using IGEL Cloud Gateway (ICG) or Shared Workplace (SWP) or a Custom Partition and want to make sure that the upgrade is performed only if these features can be used furthermore, select **Smart**. When this option is selected, and any of these features is activated, the upgrade is performed only if the device could fetch a license from an Enterprise Management Pack.
    - If you want to force the device to fetch a license from an Enterprise Management Pack and make sure that the upgrade is performed only if the license could be fetched, select **Always**.
    - If you want the device to upgrade to IGEL OS 11 without fetching an Enterprise Management Pack, disregarding the features that might be activated, select **Never**.
- Under **Timeout waiting for OS 11 license to start automatic upgrade**, set the time period the device will wait for a license in a mass deployment scenario (see Zero-Touch Deployment Using Universal Firmware Update (see page 131), Zero-Touch Deployment Using Buddy Update (see page 175) and Mass Deployment Using a Scheduled Job (see page 283)). This setting prevents the device from starting the upgrade at an inappropriate time as a result of the license just being deployed. This way, the setting prevents unwanted interruptions at work. For a mass deployment scenario, the default value **10 Minutes** is recommended.

3. Click **Apply**.

When the Setup is adjusted, continue with Deploying a License (see page 269).

Deploying a License

To upgrade from IGEL OS 10 to IGEL OS 11, you need an appropriate license. Depending on your requirements, one or more of these licenses will be needed for each device:

- One Workspace Edition license for basic functionality
- If one of the following features is used, one Enterprise Management Pack license is required:
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - if IGEL OS 11.03.100 or lower is the target version; in IGEL OS 11.03.500 or higher, the Custom Partition feature is included in the Workspace Edition.

Proceed as follows:

→ Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*
- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Download three demo licenses from https://www.igel.com/download/ .

When the device has a license, continue with Configuring the Update Source (see page 270).

Configuring the Update Source

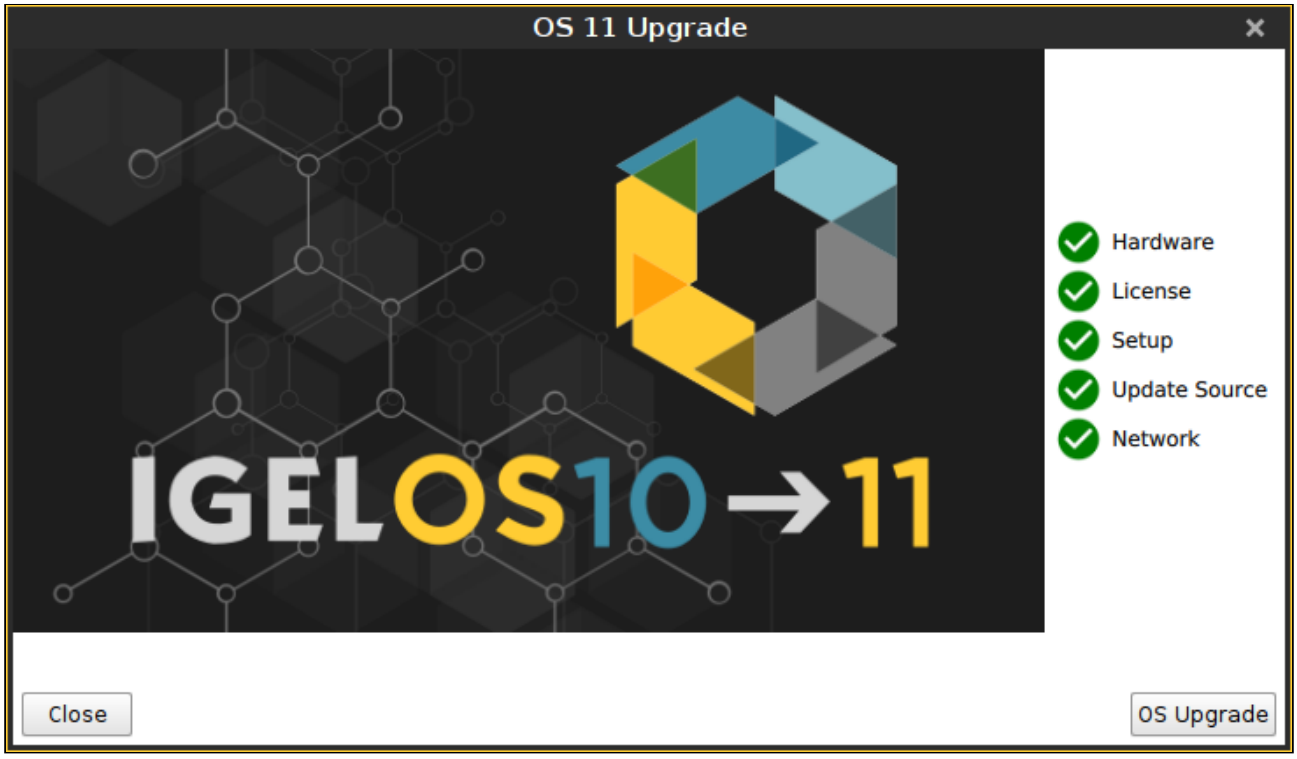
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update Settings for IGEL OS (see page 2056) chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade (see page 271).

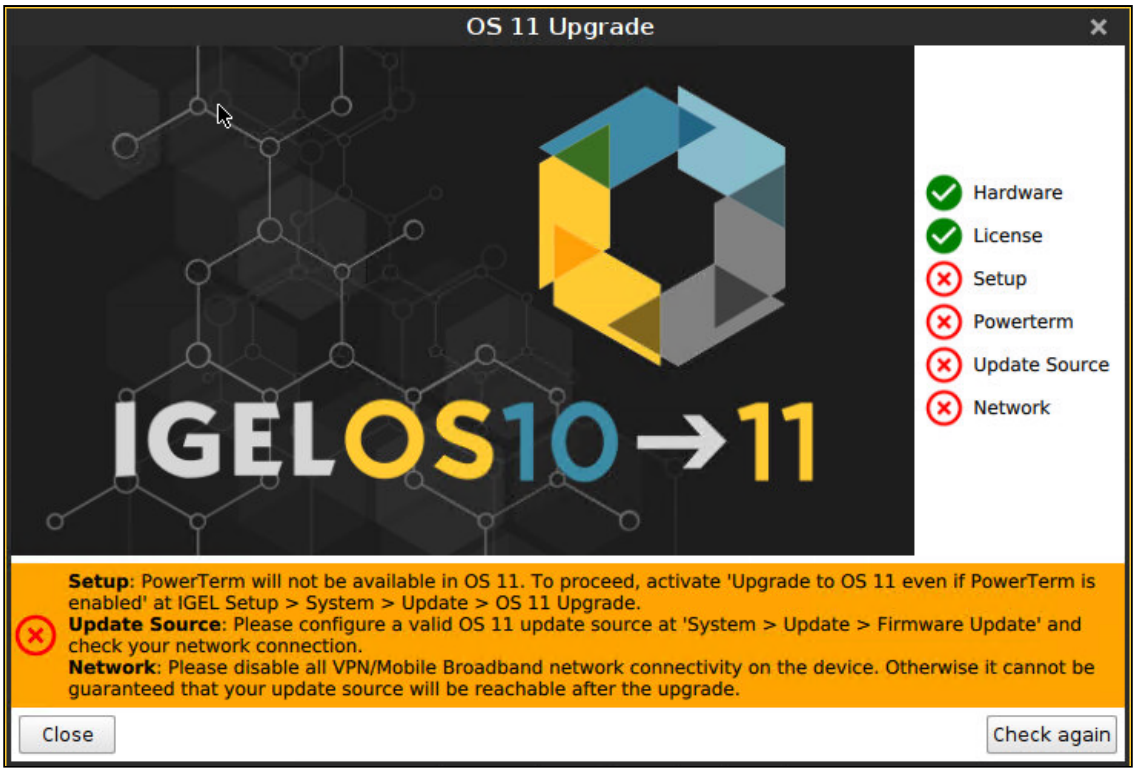
Testing the Upgrade

1. Click System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

You can change the starting the starting methods for the OS 11 Upgrade Tool in the Setup under **Accessories > OS11 Upgrade**.

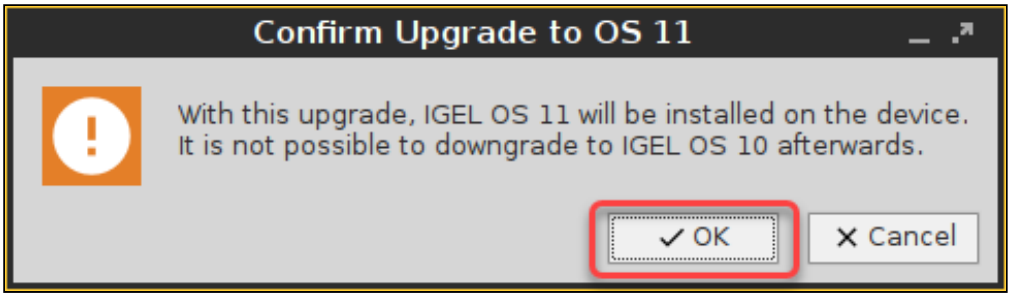


2. Check the output of the OS 11 Upgrade Tool and continue appropriately:
   - If each requirement has an icon, click **OS Upgrade** to start the upgrade process.
   - If one or more requirements have an icon, check the messages and resolve the issues. Afterwards, click **Check again**. If all requirements are met, the button changes to **OS Upgrade**, and you can start the upgrade.

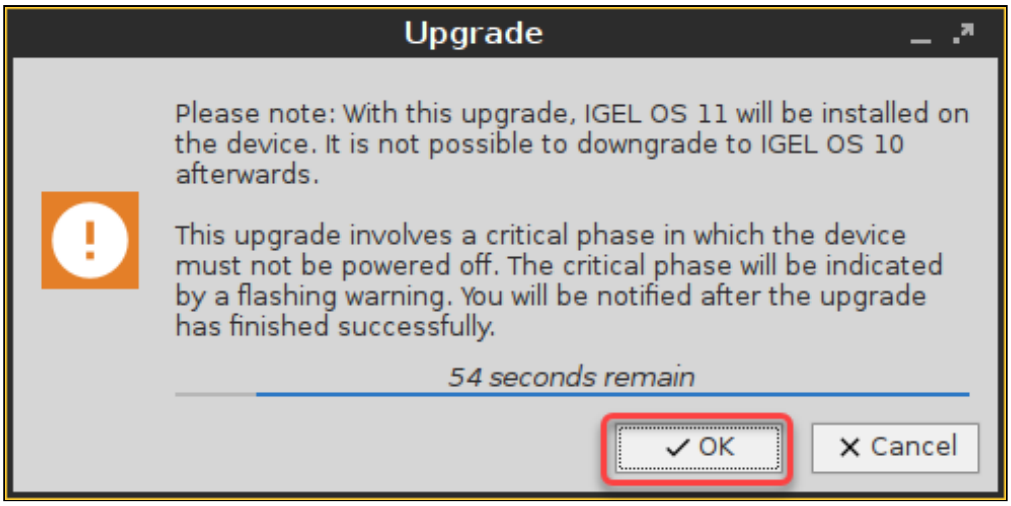


When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



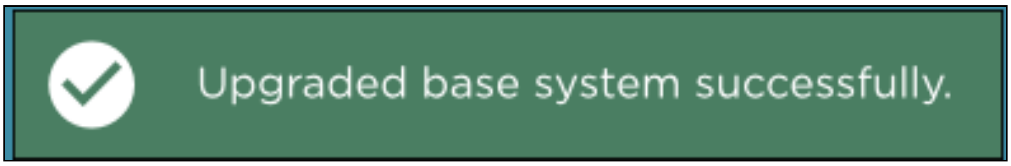
A warning dialog with a timeout is shown. If you click **Cancel** before the timeout expires, the upgrade is canceled. If you click **OK** or just wait for the timeout to expire, the upgrade is started



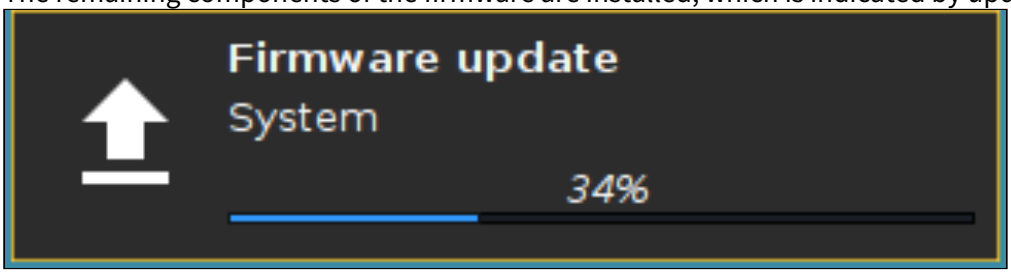
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window shows the progress.

During the critical phase, the device must not be powered off. At this stage in the progress, an additional warning is shown.

When the base system is upgraded successfully, a message is shown.



The remaining components of the firmware are installed, which is indicated by update messages.



When the installation is completed, the **Upgrade** window looks like this:

After a few seconds the device reboots into IGEL OS 11.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements 5.

Checking the Requirements of the Buddy Update

The following requirements must be met:

- The upgrade has been tested with characteristic devices; see Testing the Upgrade[46].
- UMS 6.01.130 or higher is available.
- The firmware IGEL OS 10.05.700 or 10.05.800 is known to the UMS. For this purpose, a device with OS 10.05.700 or 10.05.800 must be registered in the UMS. This is already the case if you tested the upgrade (see Testing the Upgrade[47]) with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with OS 10.05.700 or 10.05.800 now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

46. https://kb.igel.com/en/igel-os/11.10.250/testing-the-upgrade-1
47. https://kb.igel.com/en/igel-os/11.10.250/testing-the-upgrade-1

Configuring Two Update Buddies

For setting up buddy updates, see the How-To Buddy Update (see page 303).

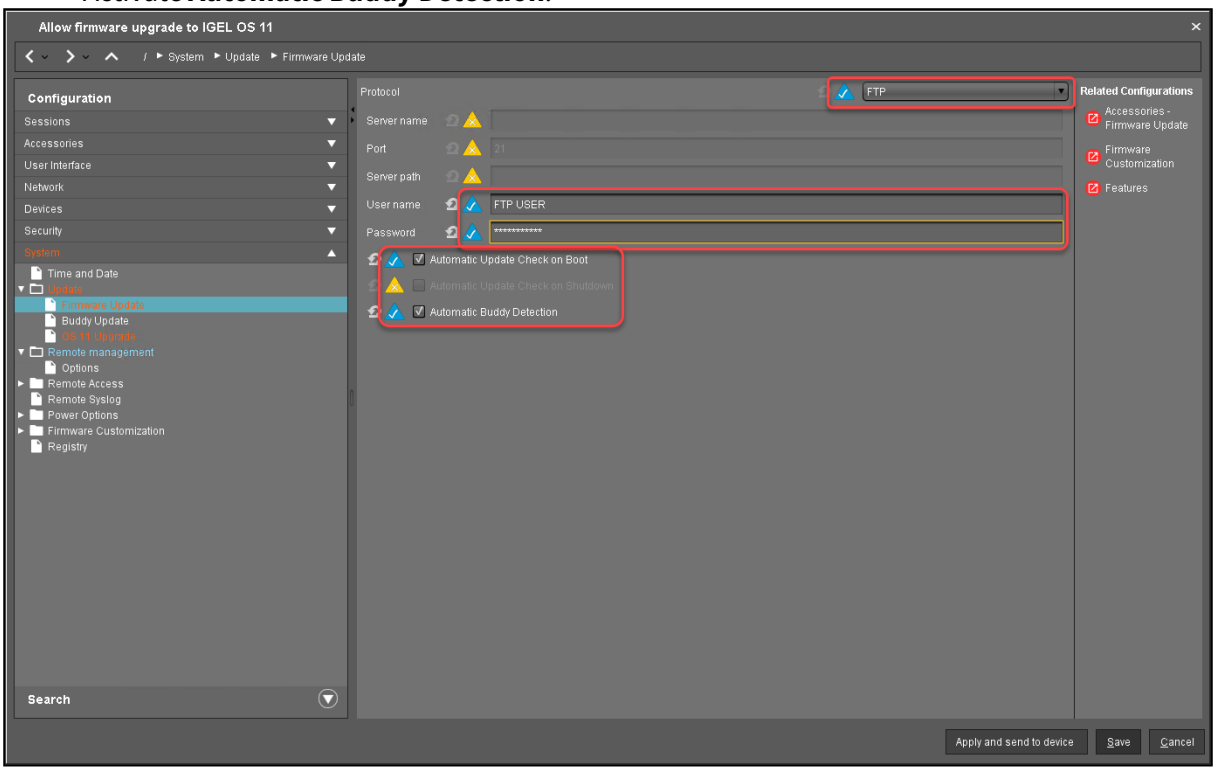
Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

1. Update one device to the appropriate IGEL OS 10 firmware (10.05.700 or higher) and configure it as an update buddy.
2. Upgrade another device to IGEL OS 11 and configure it as an update buddy. Make sure that the IGEL OS 11 update buddy has the same **User Name** and **Password** in **System > Update > Buddy Update** as the IGEL OS 10 update buddy.

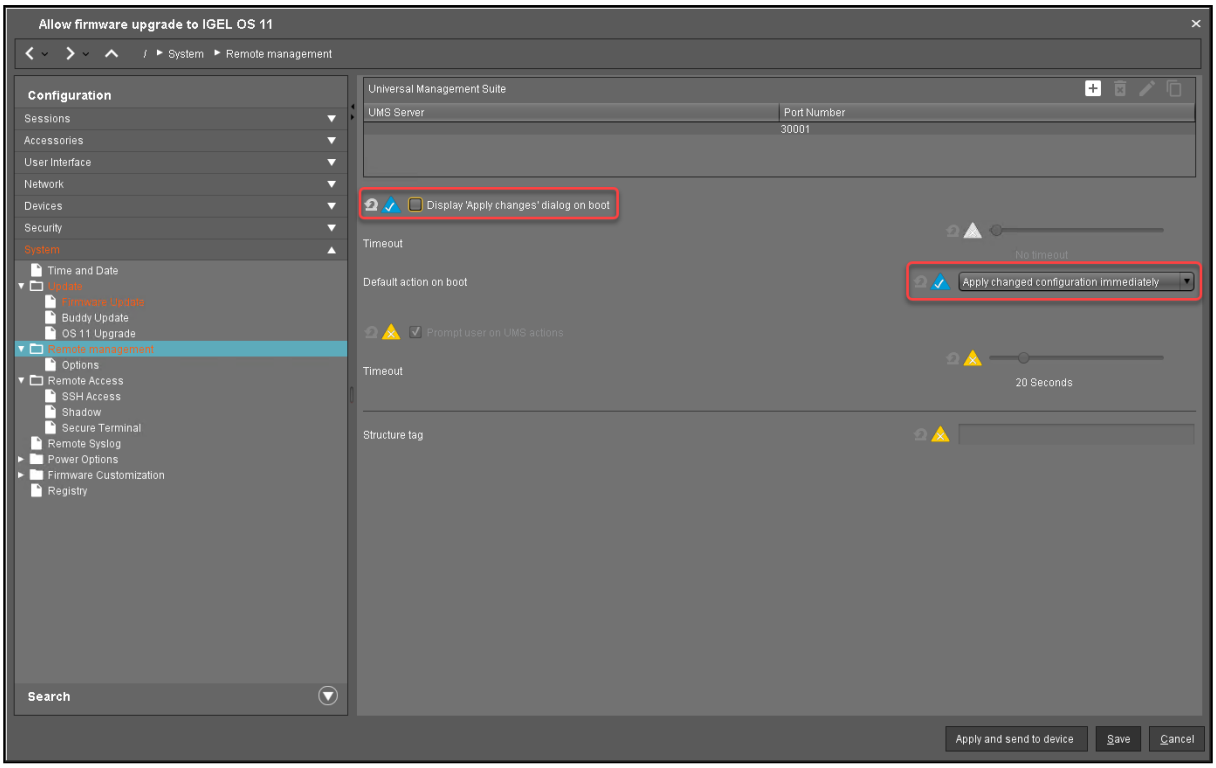
When the update buddies are configured, continue with Creating a Profile (see page 278).

Creating a Profile

1. Create a profile which is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Firmware upgrade to IGEL OS 11".
2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings as follows:
    - Select "FTP" as **Protocol**.
    - Enter **User Name** and **Password** according the update buddy server.
    - Activate **Automatic Update Check on Boot**.
    - Ensure that **Automatic Update Check on Shutdown** is deactivated. Otherwise, the device will shut down when the update is finished.
    - Activate **Automatic Buddy Detection**.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test:
    - Activate **Upgrade to OS 11**.
    - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
    - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
    - Set **Timeout waiting for OS 11 license to start automatic upgrade** to **10 Minutes**.
4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 280).

Deploying the Licenses

Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*

When the license deployment is set up, continue with Putting It All Together (see page 281).

Putting It All Together

1. Assign the profile to all devices that are to be upgraded. This can be done by assigning the profile to the directory that contains these devices.

   Do not assign the profile to the update buddies.

2. In the context menu of the assignment, select **Now**.
3. For Automatic license deployment, a condition can be set to the directory. For more information, see Configuring the Distribution Conditions, section Distributing Licenses to Devices in a Specified Directory[48].

When everything is in place, continue with Executing the Upgrade (see page 282).

48. https://kb.igel.com/en/igel-subscription-and-more/current/how-to-configure-the-distribution-conditions-of-li#HowtoConfiguretheDistributionConditionsofLicenses-DistributingLicensestoDevicesinaSpecifiedDirectoryDistributing-Licenses-to-Devices-in-a-Specified-Directory

Executing the Upgrade

1. In the UMS, select all devices that are to be upgraded and reboot them.

> Alternatively you can create a scheduled job for reboot or wake up and assign it to the devices or the directory containing these devices; for more information, see Jobs[49].

On reboot or wake up, the devices choose the IGEL OS 10 buddy. They ignore the IGEL OS 11 buddy at this stage because this version is not known to them yet. The devices update to the appropriate version of IGEL OS 10 (10.05.700 or higher). With this version, the Upgrade to OS 11 parameter is recognized by the devices; also, the devices request IGEL OS 11 licenses from the UMS (Workspace Edition and, if required, Enterprise Management Pack).
If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period the device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Adjusting the Setup (see page 235).
The parameters **Automatic update check on boot** and **Automatic buddy detection** cause the devices to look for a new firmware and wait for an IGEL OS 11 update buddy to reply. When an IGEL OS 11 update buddy is found, the devices start the upgrade process.

2.

> **Update Can Be Canceled After Timeout**
> An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:
> - Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
> - A feature has been activated, e.g. VPN OpenConnect.
>
> *A Custom Partition has been activated or changed.

3. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile.

The upgrade is complete.

49. https://wiki.test.toolchain.igel.kreuzwerker.net/endpointmgmt-5.08/en/jobs-910606.html

Mass Deployment Using a Scheduled Job

This scenario is appropriate if you already have a working environment with IGEL OS 10.05.700 (or higher) and want to update all devices to IGEL OS 11 at a defined time.

Read all the following chapters carefully and follow the instructions.

- Checking the Requirements (see page 284)
- Creating a Profile (see page 285)
- Deploying the Licenses (see page 289)
- Assigning the Profile (see page 290)
- Creating the Scheduled Job (see page 292)

Checking the Requirements

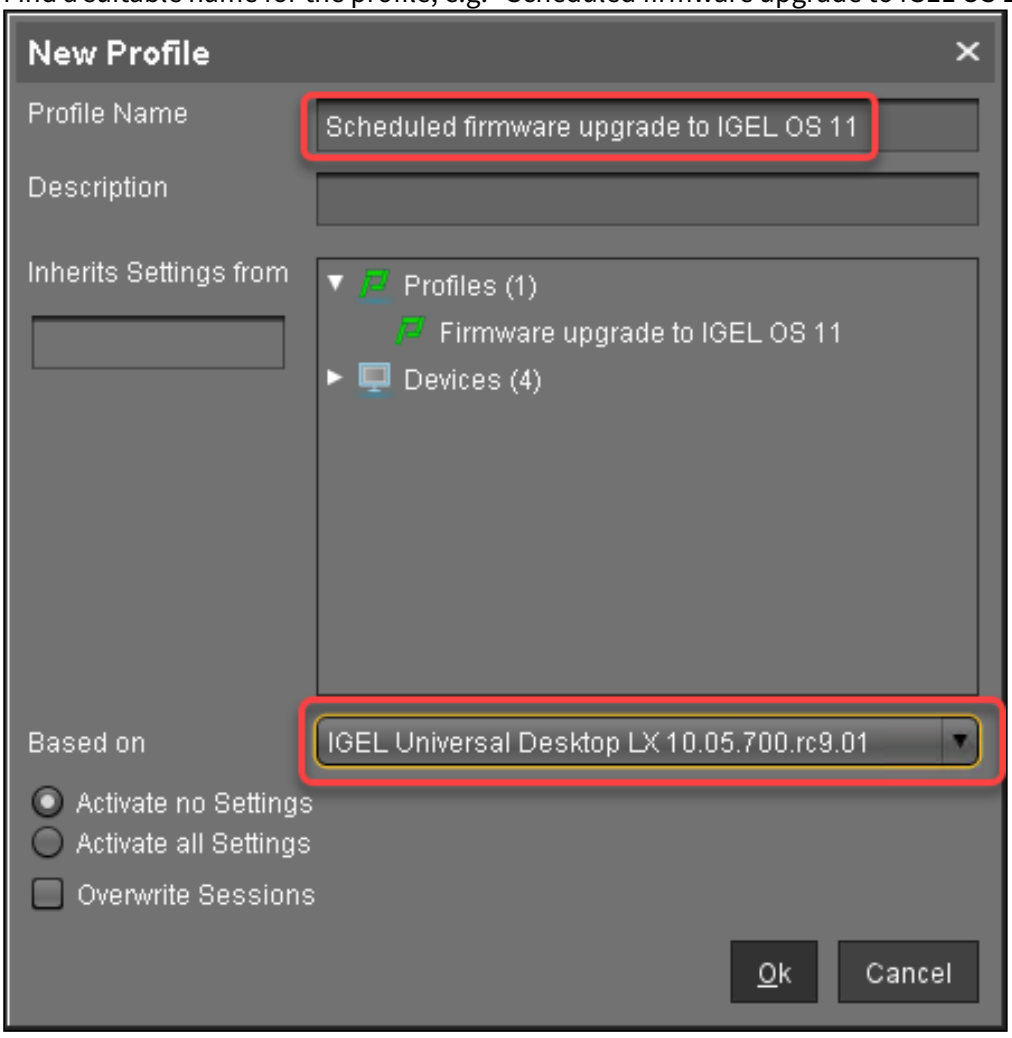
The following requirements must be met:

- The upgrade has been tested with characteristic devices.
- UMS 6.01.130 or higher is available.
- The firmware IGEL OS 10.05.800 (or higher) is known to the UMS. For this purpose, a device with this firmware version must be registered in the UMS. This is already the case if you tested the upgrade with the same UMS with which you are about to do the mass upgrade. If not, you must register a device with the appropriate firmware version now.
- All devices are connected to a regular LAN (not OpenVPN, OpenConnect, genucard, NCP VPN or mobile broadband).
- All devices are in a safe environment where the upgrade process cannot be disrupted, e.g. by powering off the devices.

When all requirements are met, continue with Creating a Profile (see page 285).

Creating a Profile

1. Create a profile that is based on the appropriate IGEL OS 10 firmware version (10.05.700 or higher). Find a suitable name for the profile, e.g. "Scheduled firmware upgrade to IGEL OS 11".



2. In the profile's configuration dialog, go to **System > Update > Firmware Update** and change the settings according to your environment:

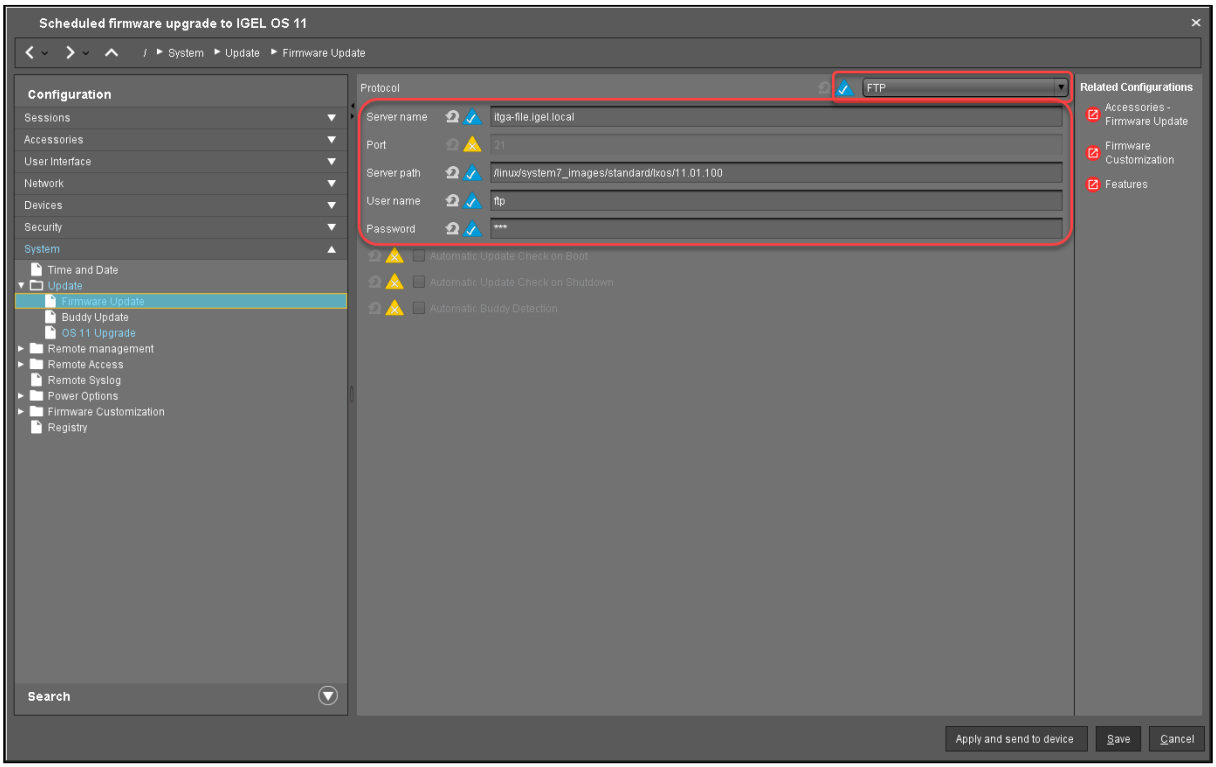
   If you use Universal Firmware Update (see page 244) for OS 11, you do not need to configure the settings described in this step.

   - Select an update source for IGEL OS 11. For further information, see Firmware Update (see page 2056).

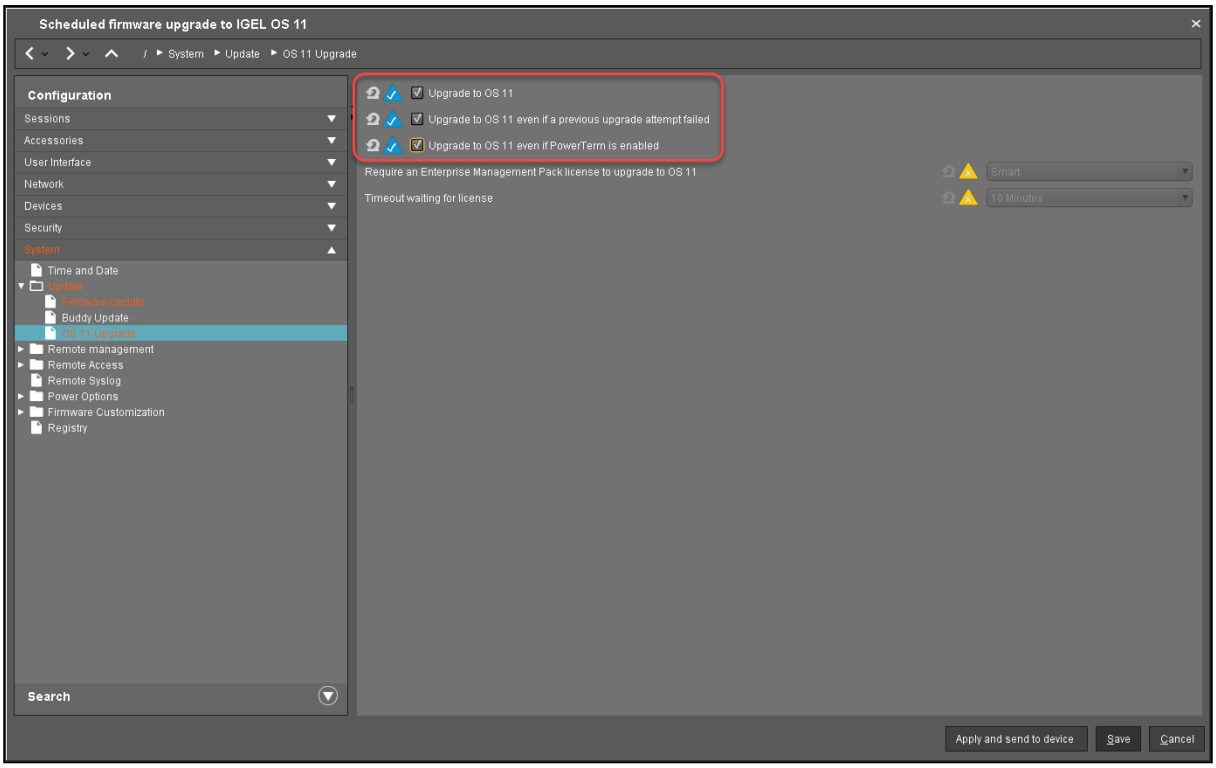
     If you use **FILE** as the protocol (local file or network drive), the device will show an error message and go through an additional reboot. Apart from that, the upgrade will work normally.

- Ensure that **Automatic Update Check on Boot** and **Automatic Update Check on Shutdown** are deactivated.

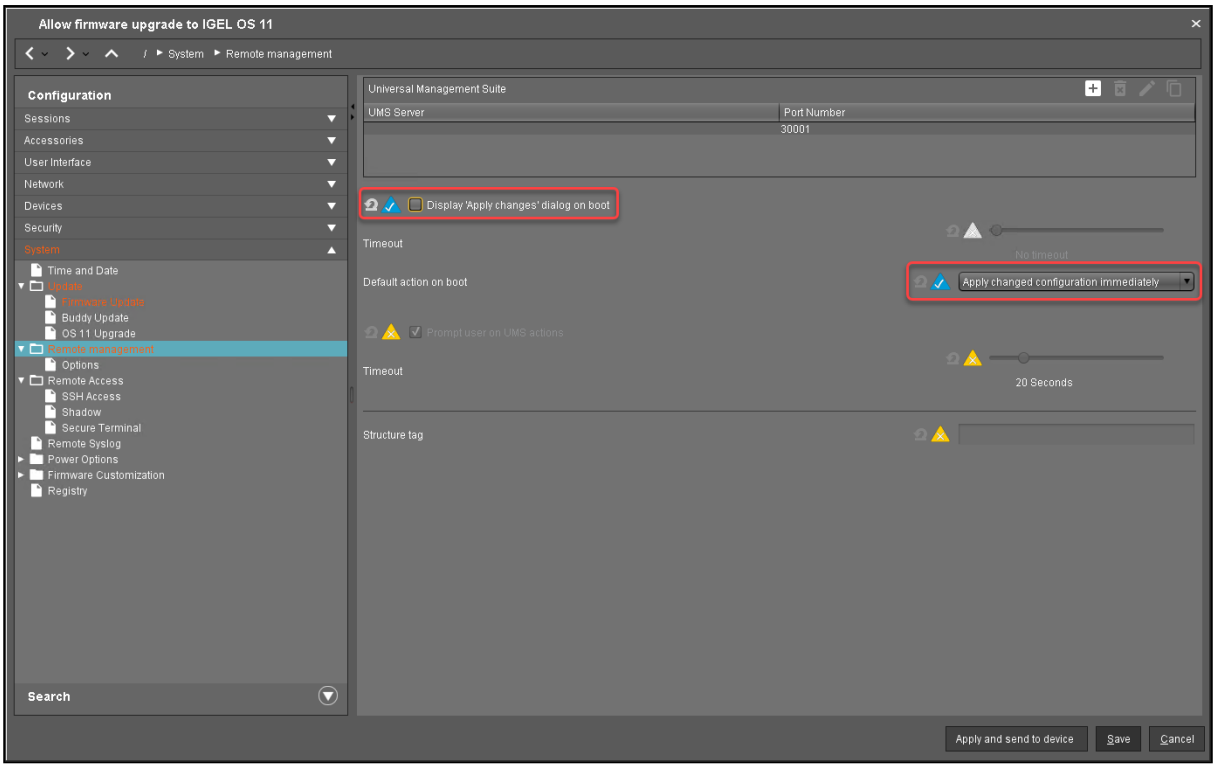
  In the following screenshot, FTP is used as an example. The other protocols can be used as well.



3. Go to **System > Update > OS 11 Upgrade** and change the following settings according to your successful upgrade test (for details of the settings, see Adjusting the Setup (see page 235)):
   - Activate **Upgrade to OS 11**.
   - Set **Upgrade to OS 11 even if PowerTerm is enabled** according to your needs.
   - Set **Upgrade to OS 11 even if a previous upgrade attempt failed** according to your needs.
   - Set **Require an Enterprise Management Pack license to upgrade to OS 11** according to your needs.
   - Ensure that the **Timeout waiting for OS 11 license to start automatic upgrade** is set to **10 Minutes**.



4. Go to **System > Remote Management** and change the settings as follows:
    - Deactivate **Display 'Apply changes' dialog on boot**.
    - Set **Default action on boot** to **Apply changed configuration immediately**.



5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 289).

Deploying the Licenses

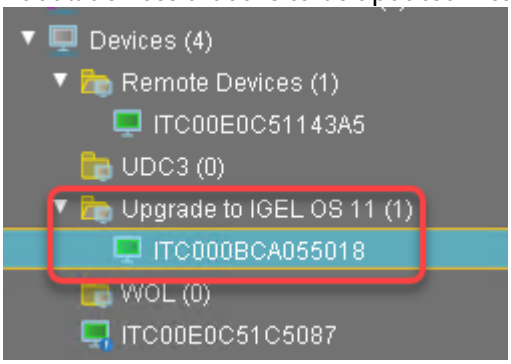
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD).*
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Manual License Deployment for IGEL OS.*

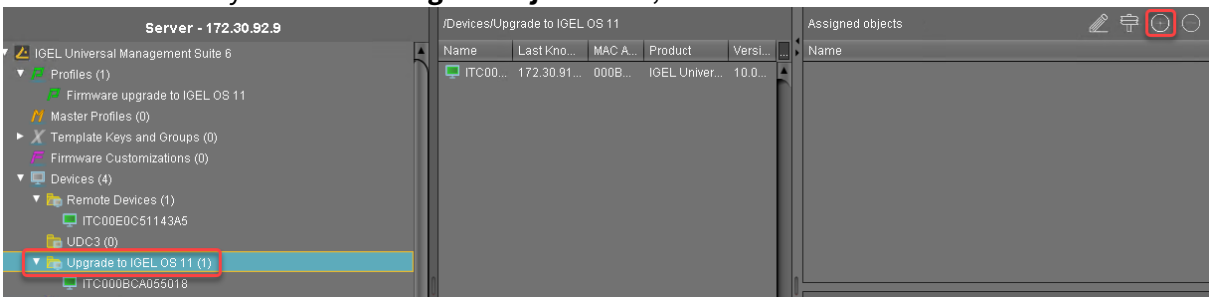
When the license deployment is set up, continue with Assigning the Profile (see page 290).

Assigning the Profile

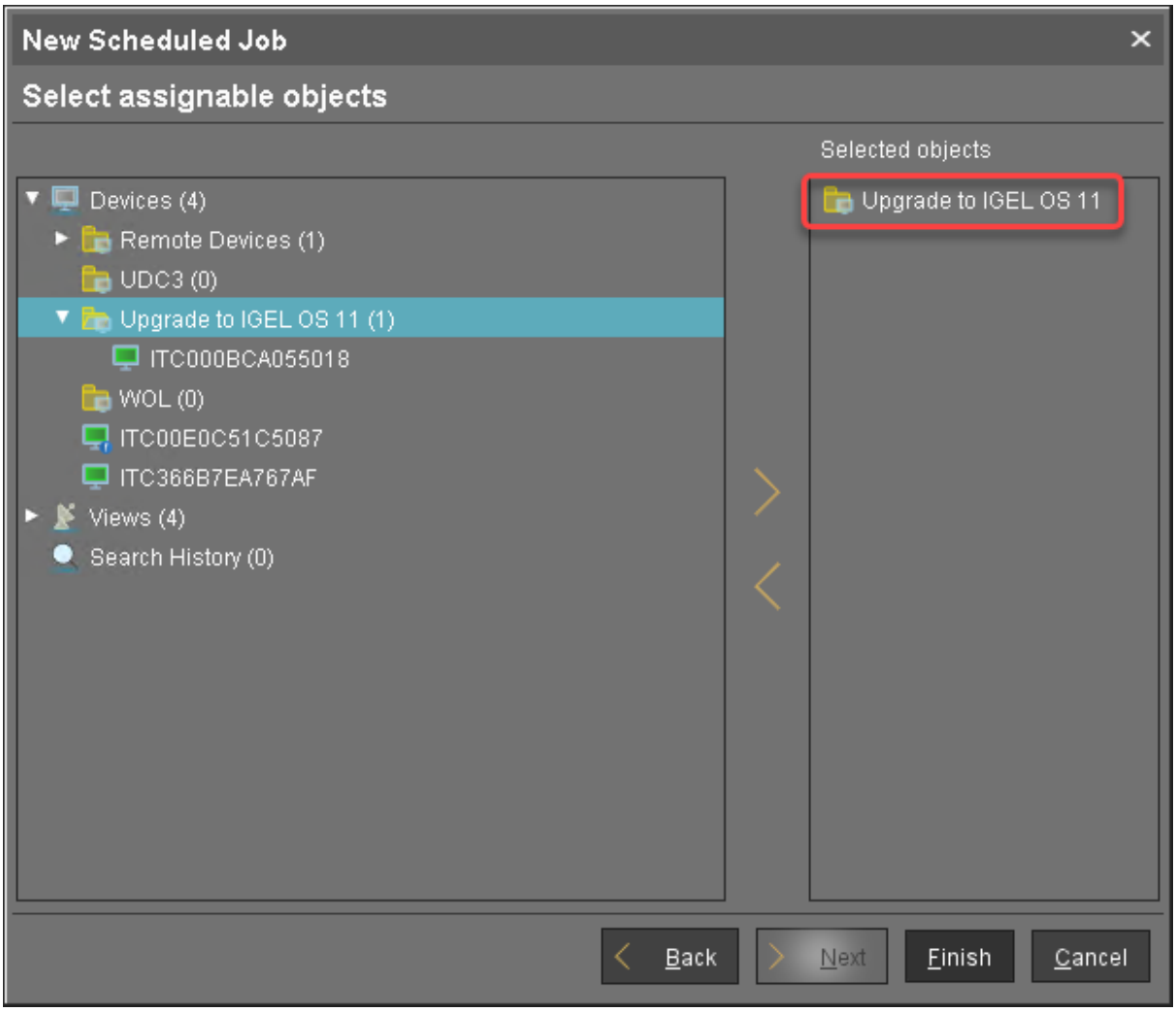
1. Put all devices that are to be updated into a directory.



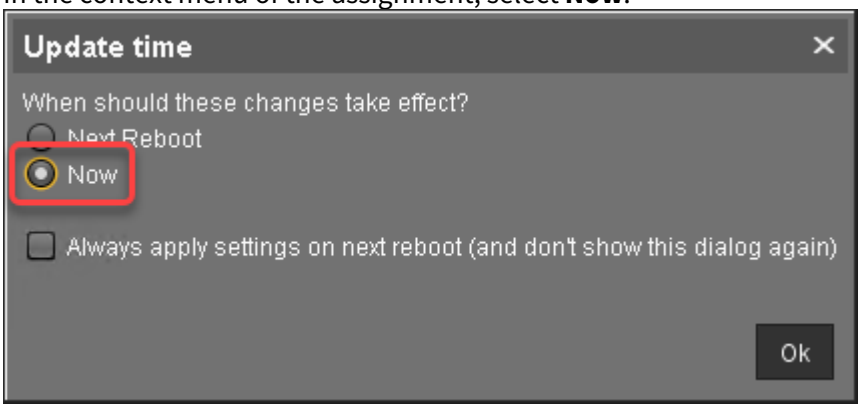
2. Select the directory and in the **Assigned objects** area, click .



3. Assign the profile (see Creating a Profile (see page 285)) to the directory and click **Ok**.



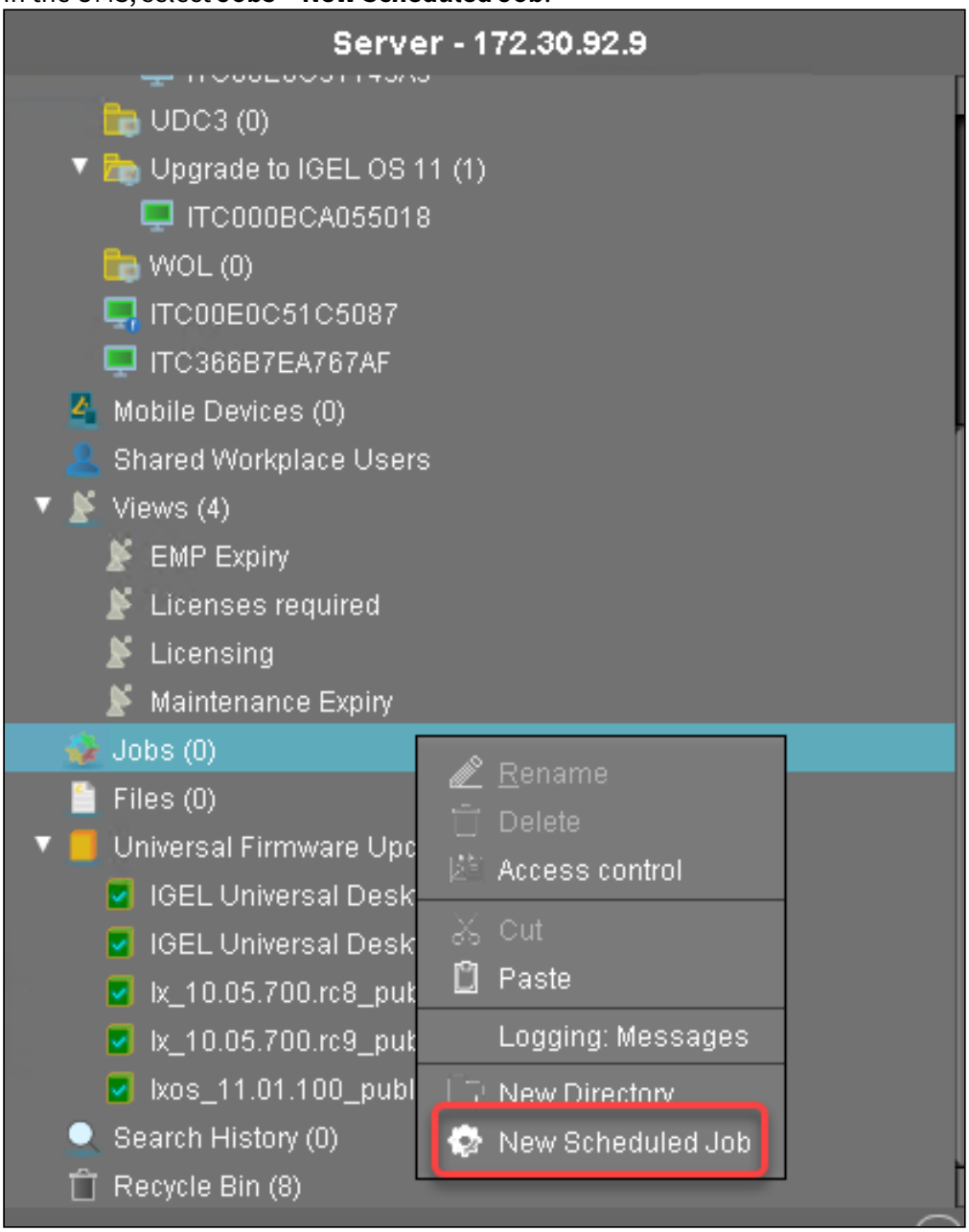
4. In the context menu of the assignment, select **Now**.



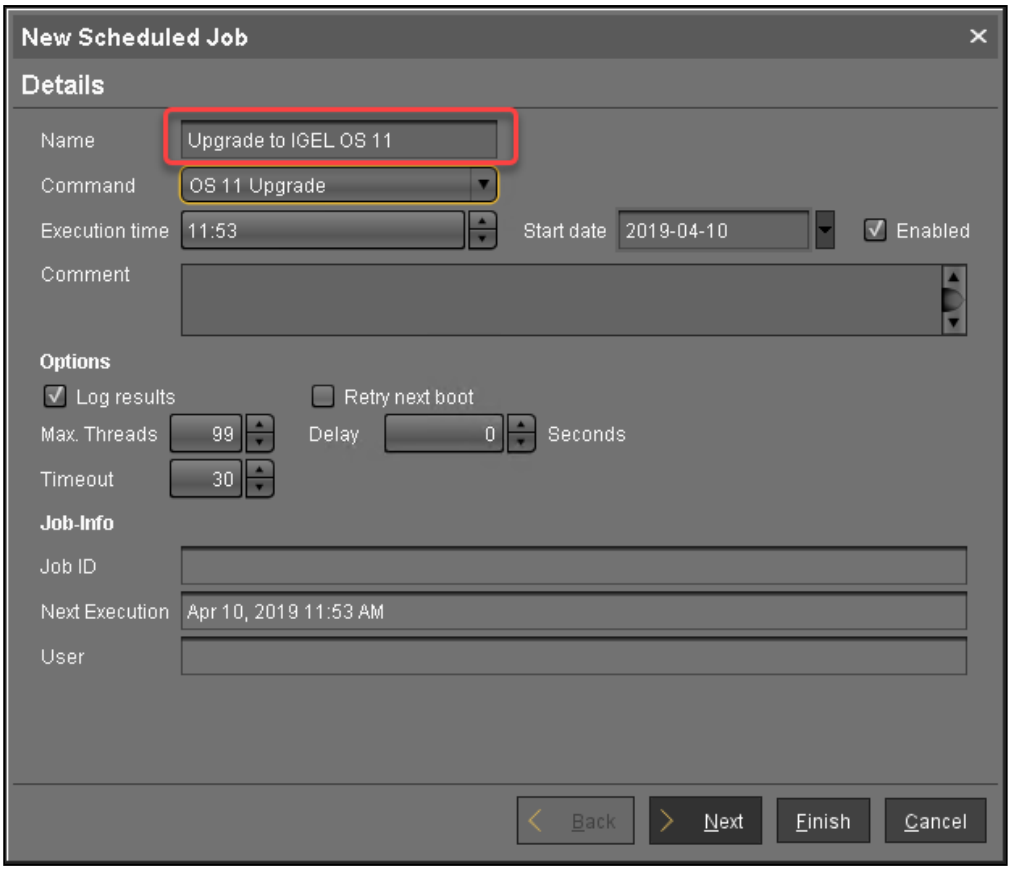
When the profile is assigned, continue with Creating the Scheduled Job (see page 292).

Creating the Scheduled Job

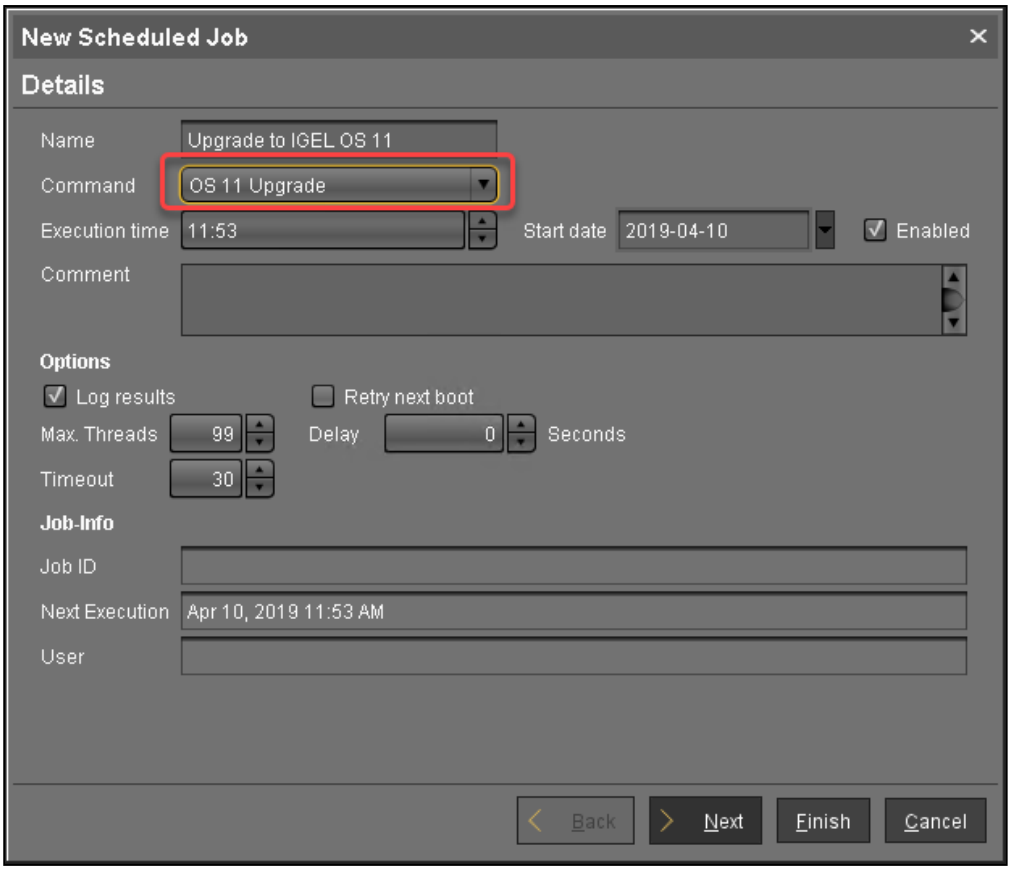
1. In the UMS, select **Jobs > New Scheduled Job**.



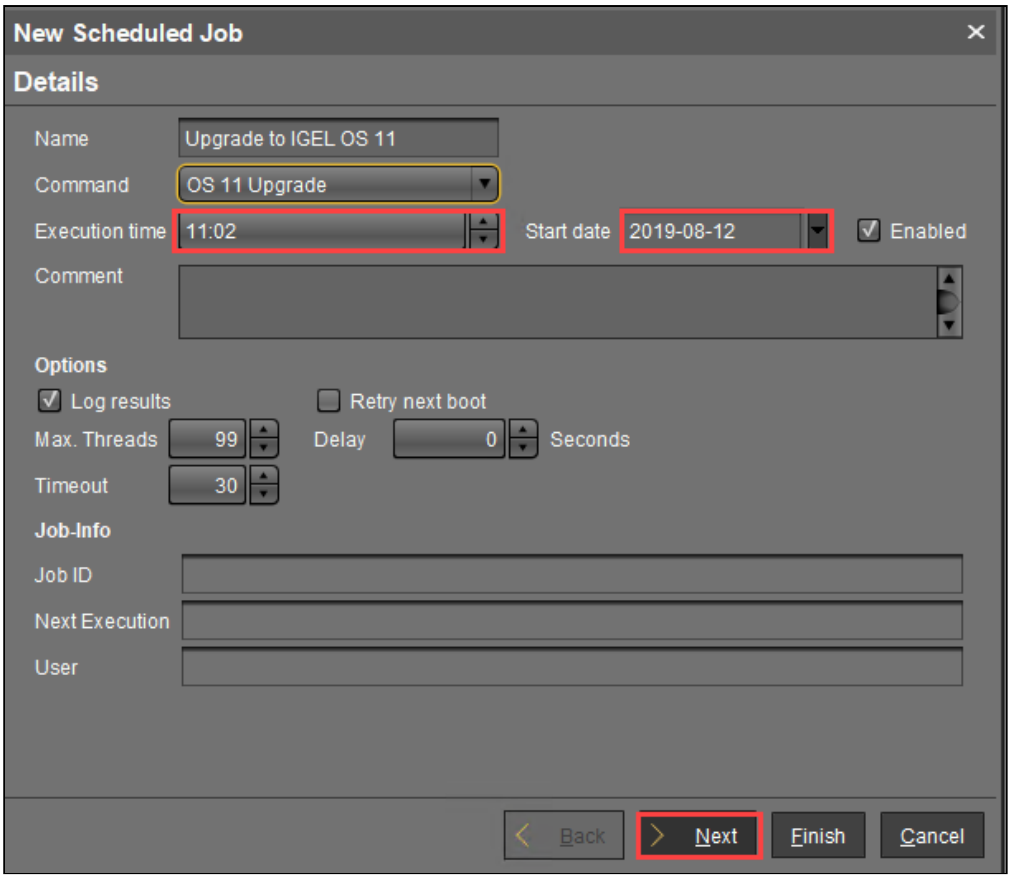
2. Under **Name**, enter a suitable name for the job, e. g. "Upgrade to IGEL OS 11".



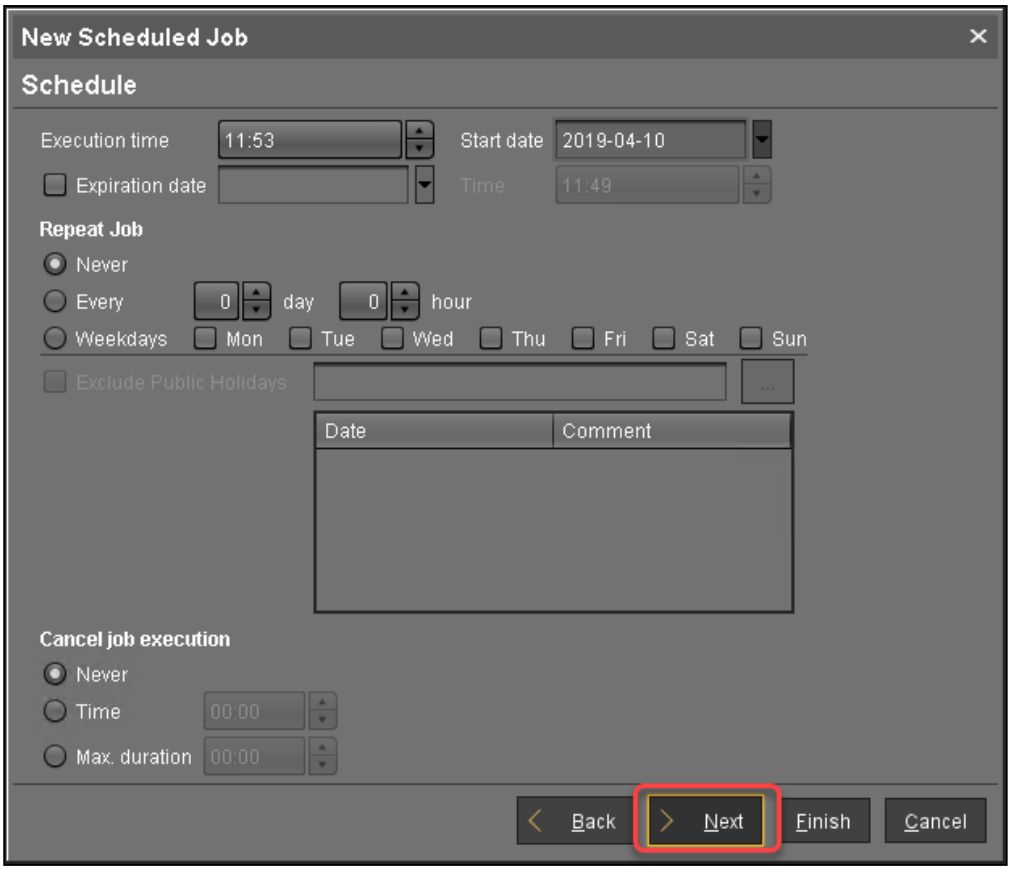
3. Under **Command**, select **OS 11 Upgrade**.



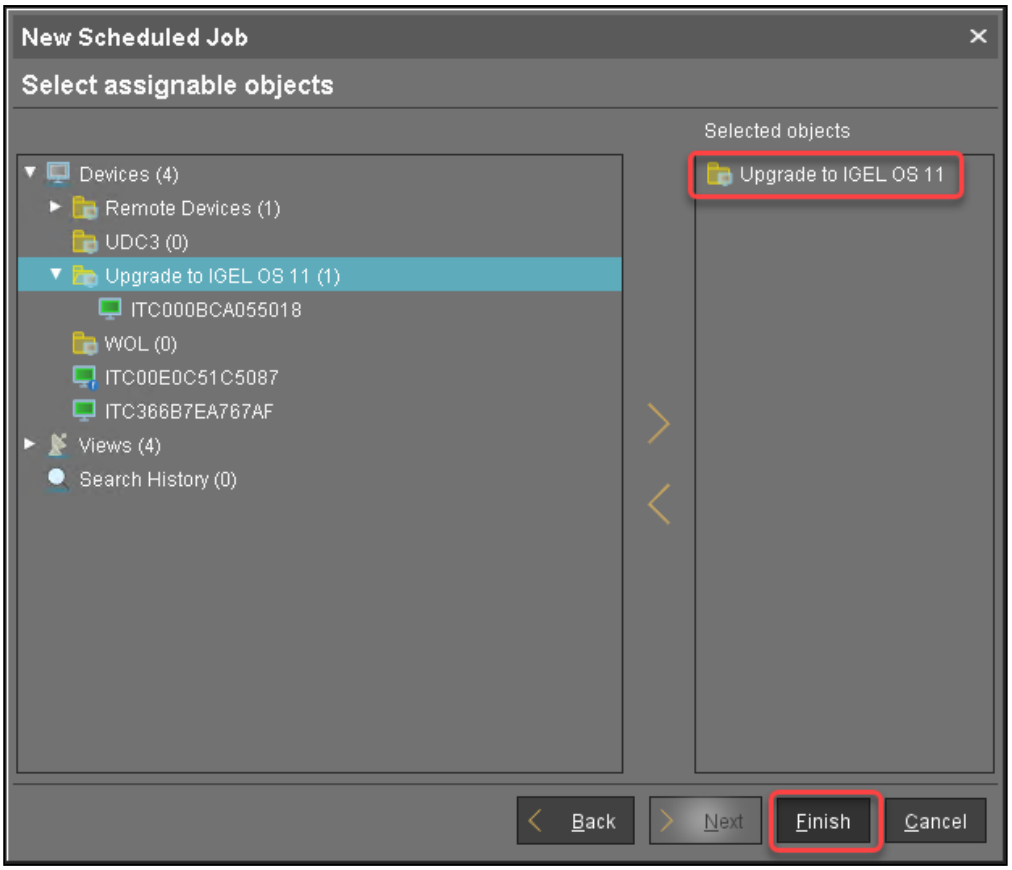
4. Under **Execution time** and **Start date**, set the time at which the upgrade should be executed, and click **Next**.



5. Review the execution time and click **Next**.



6. Assign the directory containing the devices to the job and click **Finish**.



Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

Troubleshooting

This section describes possible error cases and solutions.

- Regaining a Usable System (see page 299)
- Getting Error Messages (see page 300)
- Starting a New Upgrade Attempt (see page 301)
- Starting Another Upgrade Attempt after 5 Retries (see page 302)

Regaining a Usable System

Here you can find typical upgrade failures and the appropriate methods to regain a usable system.

Device Has Upgraded to Igel OS 11, but Does Not Boot Any More

To get a working IGEL OS 11 system:

→ Use the IGEL OS Creator to recover the IGEL OS 11 system. For more information, see the IGEL OS Creator Manual (see page 2119).

IGEL OS 10 Rescue System Fails to Update Missing Partitions

If a severe error has occurred during the upgrade process, the device boots into a minimal 10.05.700 (or higher) rescue system. If unattended, the device tries to download and update the missing partitions and reboots on failure.

To regain a full IGEL OS 10 system, you have two possibilities:

→ In the rescue system, start the Setup, go to **System > Update > Firmware Update** and set a valid update source for the appropriate IGEL OS 10 firmware version (10.05.700 or higher).

Or:

→ Configure a UMS profile that contains a valid update source for the appropriate IGEL OS 10 firmware version (10.05.700 or higher) under **System > Update > Firmware Update** and assign it to the device.

Getting Error Messages

→ Open the OS 11 Upgrade Tool (default path: click System and then **Upgrade to OS 11**).

The OS 11 Upgrade Tool shows the error messages. The most important message is prefixed with **Retries**; see the example below:

→ For more information, review the main migration log under `/wfs/migration.log`

You can use the system log viewer to review the migration log (see the chapter System Log Viewer (see page 1750) in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see *Universal Management Suite > UMS Reference Manual > Save Device Files for Support*).

Starting a New Upgrade Attempt

If you want the device to start multiple upgrade attempts (and the device is not already configured to do so):

1. In the UMS profile or in the Setup, go to **System > Update > OS 11 Upgrade** and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. Reboot the device.

Starting Another Upgrade Attempt after 5 Retries

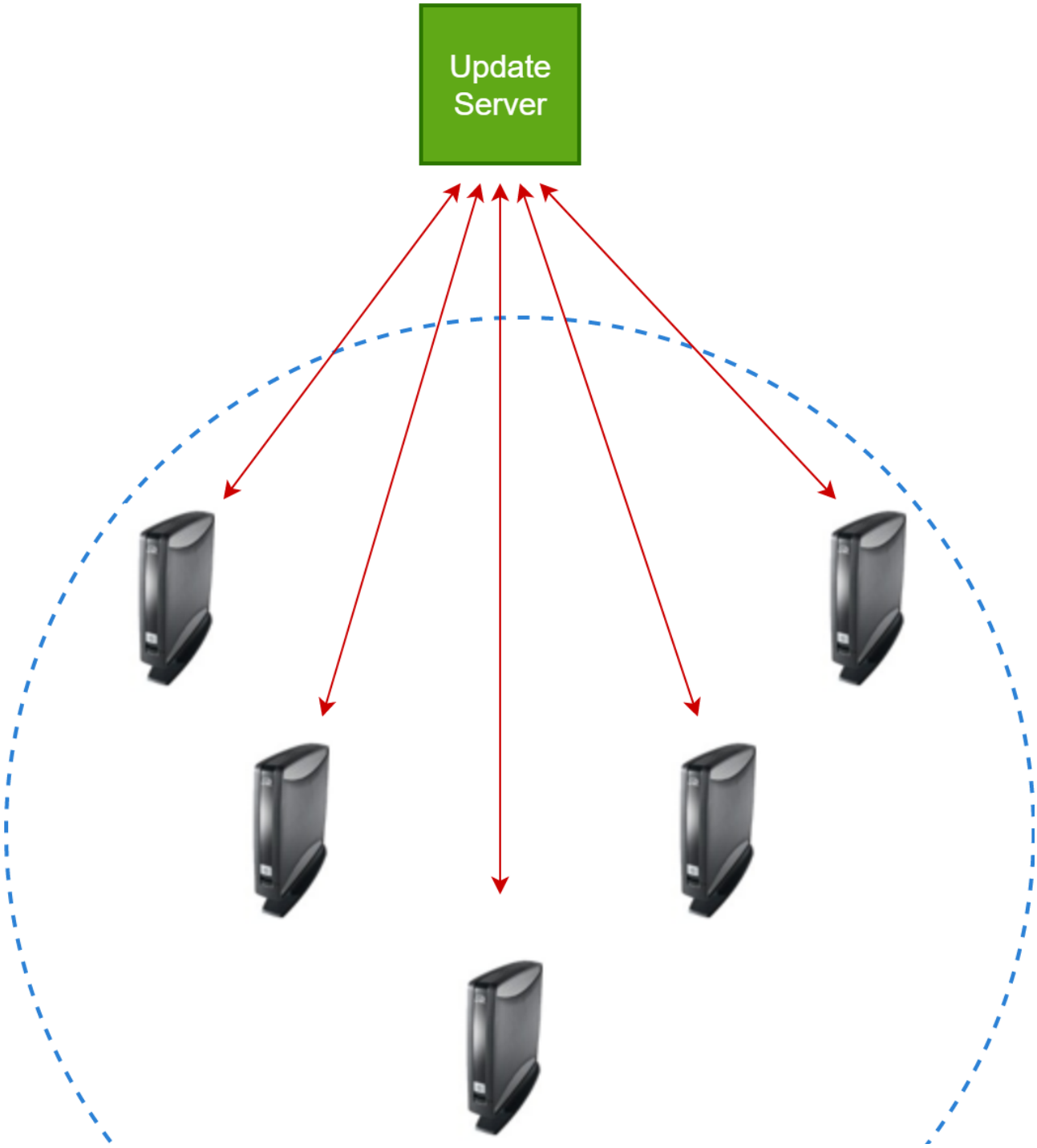
When the **Upgrade to OS 11 even if a previous upgrade attempt failed** option is set and the upgrade has failed each time, the system will stop trying after 5 attempts.

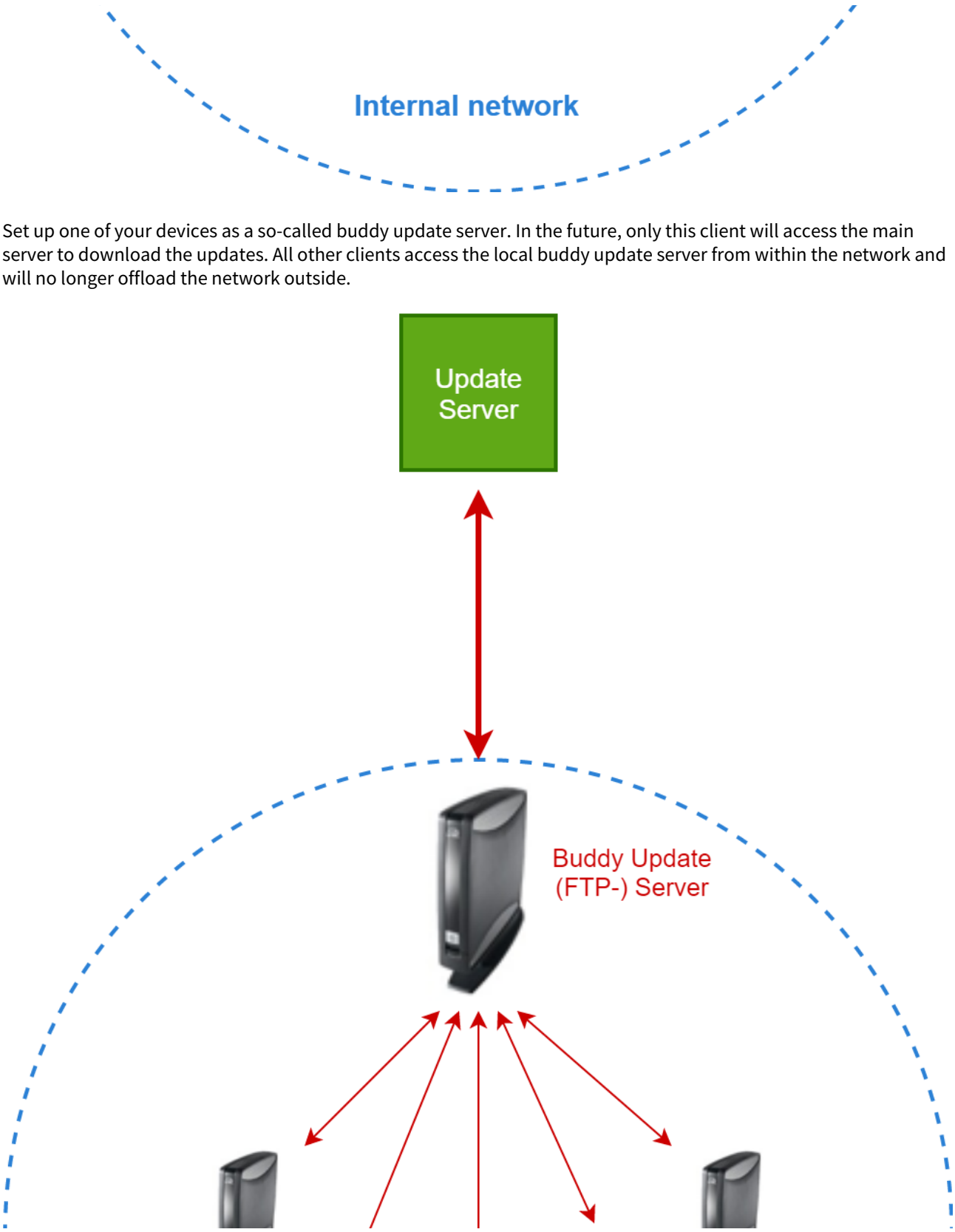
To reset the retry counter:

1. In the Setup or the UMS profile, go to **System > Update > OS 11 Upgrade** and deactivate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. When the setting is effective on the devices, go to **System > Update > OS 11 Upgrade** again and activate **Upgrade to OS 11 even if a previous upgrade attempt failed**..
   The retry counter is reset, and the devices will try upgrading another 5 times, if necessary.

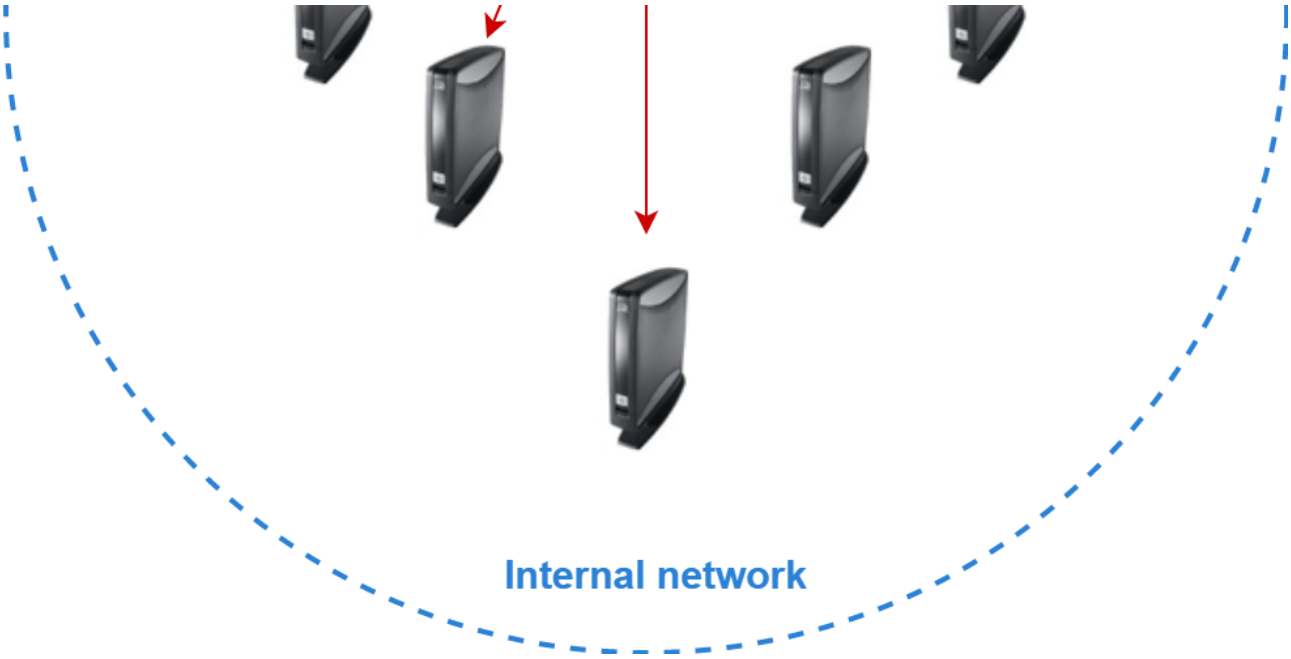
Buddy Update

A certain number of devices that are running IGEL OS in your company regularly need to be updated. If every device accesses the main update server individually, maybe even over a great geographical distance, the update could take quite a long time and might overload the entire connection.





Set up one of your devices as a so-called buddy update server. In the future, only this client will access the main server to download the updates. All other clients access the local buddy update server from within the network and will no longer offload the network outside.



The buddy update server is always an FTP server.

For the configuration details, see:

- Configuring the Buddy Update Server (see page 306)
- Configuring the Buddy Update Client (see page 308)

TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=IVUlFtOT5uE

Configuring the Buddy Update Server

> **No Downgrade from IGEL OS 11.03**
>
> It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

Basic Configuration

1. In the Setup, go to **System > Update > Buddy Update**.
2. Activate **Enable Update Server**.
3. Enter the credentials **User Name** and **Password**.
4. Specify the maximum number of **Concurrent Logins** allowed.
5. Click **Save** to confirm the changes.
6. Perform a complete firmware update on the server.
7. Reboot the server.

> Whenever a buddy update server has received a firmware update, it needs to be rebooted before it can distribute the new firmware to other devices.

Configuration for Different Firmware Versions

This feature is available for the following versions of IGEL OS:

- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

If you have an environment which requires two or more different firmware versions running simultaneously, you can use the buddy update method to provide each buddy update client device with the appropriate firmware version. A typical use case might be two groups of employees, of which one requires an older version of the browser, or an older version of the Citrix receiver, whereas the other group should get the newest version of IGEL OS. This is achieved by dividing both the clients and the servers into groups. To each group, a specific firmware version is assigned by first installing that version on the group's update servers. As an example, you can assign group 1 to IGEL OS 10.07.100, and group 2 to IGEL OS 10.08.100.

In the following description, the local Setup is used for simplicity reasons; however, in a productive environment, it is recommended to use profiles. For further information, see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*.

To assign a server to a group:

1. Configure the server as described above (under Basic Configuration), using the firmware that is to be assigned to this group.
2. In the Setup, go to **Registry > update > ftp > buddy_group_id**.
3. In the field **Buddy Group ID**, set the appropriate group id. Unsigned integers are allowed.
4. Click **Ok**.
5. Reboot the device.
   The device will provide the firmware update for the group it is assigned to.

For client configuration, see Configuring the Buddy Update Client (see page 308), "Configuration for Different Firmware Versions".

Configuring the Buddy Update Client

Basic Configuration

1. In the Setup, go to **System > Update > Firmware Update**.
2. Set the following parameters:
   Server Name: IP address of the buddy update server
   Port: 21 (default with FTP protocol)
   Server Path: -
   User Name: User name of the buddy update server
   Password: Password of the buddy update server

   > Ensure that all servers in the network use the same credentials. For security reasons, you have to enter them in the upper mask, even if you did not specify a server.

3. Activate **Automatic Update Check** if you want the client to check automatically during the boot process whether new updates are available on the server.
4. Activate **Automatic Buddy Detection** if you want the client to look for a buddy update server on its own.
   This is useful if you work with more than one buddy update server and do not wish to determine a specific one.
   In this case, you do not need to define the **Server Name**, **Port** and **Server Path**. If you enter a server name anyway, the system treats this server as a fall-back. Thus, you can be sure that the system accesses at least this one server if it cannot find any others.
5. Click **Ok**.
6. Continue with further configuration changes or reboot the device.

Configuration for Different Firmware Versions

The feature is available for the following versions of IGEL OS:

- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

This feature is described under Configuring the Buddy Update Server (see page 306), "Configuration for Different Firmware Versions".

In the following description, the local Setup is used for simplicity reasons; however, in a productive environment, it is recommended to use profiles. For further information, see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*.

To assign a client to a group:

1. In the Setup, go to **Registry > update > ftp > buddy_group_id**.
2. In the field **Buddy Group ID**, set the id of the group to which the desired firmware is assigned.
3. Click **Ok**.
4. Reboot the device.
   The device will use the firmware update for the group it is assigned to.

Balancing the Server Load

This feature is available for the following versions of IGEL OS:

- IGEL OS 10: 10.06.100 or higher
- IGEL OS 11: 11.02.100 or higher

It is possible to balance the load between several buddy update servers. If **System > Update > Firmware Update > Automatic Buddy Detection** is activated, the clients send a broadcast in their network to determine which buddy servers are available. Each server that responds within a fixed timeout is added to a list whose maximum length can be defined. When the list is complete, either because its maximum length is reached or because the timeout has expired, the client selects a random server from the list. This way, the load of the buddy servers is distributed evenly.

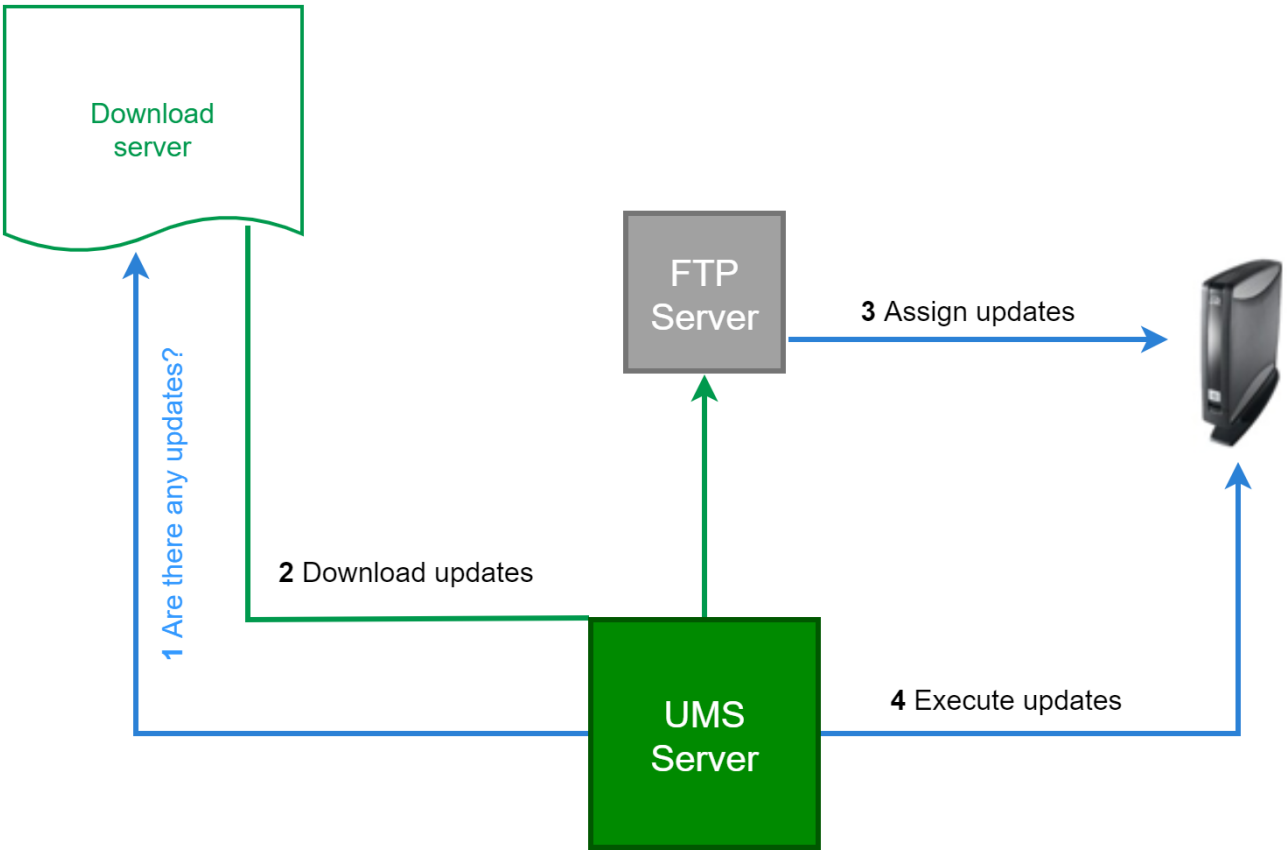
To configure a client for balancing the server load:

1. In the Setup, go to **Registry > update > ftp > buddy_server_candidates**.
2. In the field **Buddy Update Server Candidates**, enter the maximum number of servers the client should collect. If the number is 1, the server that responds first is selected.
3. Click **Ok**.
4. Reboot the device.

Firmware Update

Here we show you the best practice of downloading a firmware update from our download server and distributing it to various devices in your company:

1. Check our download server[50] to see whether there are new updates which are relevant for your applications.
2. Download the relevant update files.
3. Install an update directory for them on the UMS server or on your FTP server.
4. Assign this update directory to your devices.
5. Start the update process manually or via a Scheduled Job (see page 313).



- Downloading Updates and Storing them on an FTP Server (see page 311)
- Executing an Update Process (see page 313)

50. https://www.igel.com/software-downloads/

Downloading Updates and Storing them on an FTP Server

You can save the update files either directly on the UMS server or you can put them on your captive FTP server. If you have many devices to be updated, you should work with the FTP server because it makes it easier to distribute large amounts of data in the local network.

No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

Important Notes on Downgrading from IGEL OS 11.06 or Higher

- If you have encrypted your IGEL OS 11.06 device, downgrading to IGEL OS 11.05 or lower will imply data loss on the following partitions, due to different partition schemes:
  - Browsing history of the browsers Firefox and Chromium
  - Custom Partitions
- The device settings and the UMS connection are preserved.
- The device encryption password must be entered by the user.

Preparation

1. Click **Universal Firmware Update** in the UMS Administration area of *UMS c*onsole.
2. Click **Edit...** .
3. Enter your FTP server under **Host**, to save the update files in this location.
4. Add further details like storage path and access data for the server.
5. Save your settings and click **Test Server Connection**.

Downloading updates

1. Right-click **Universal Firmware Update** on the UMS console tree.
2. Choose **Check for new firmware updates** from the context menu.
   A window opens with a list of all updates associated with the firmware versions registered in the UMS database.
3. Choose a **Version** in the drop-down-list.
4. Click **Information** to see the release notes of each update.
5. Activate the check box **Include** for downloading a certain update.
6. Click **Download** to start the process.
   The update will be added to the tree and the current processing status will be shown.
   The unpacked firmware files are finally in the target directory on the FTP server.

Assigning updates to the thin clients

Assign the downloaded update by dragging and dropping to your device directory. Now, if you click this directory you can see the firmware update in the right window under **Assigned objects**. The devices will now know where to find the firmware update in the event of an update command.

Executing an Update Process

1. Create one or more new **Views** to distinguish which thin clients will get the new update.
2. Create a new **Job**, called "firmware update" for example.
3. Specify on the **Schedule** tab when you want the update to be performed.

   > The **Repeat job** option should not be activated for **Update**, **Update on boot** or **Update on shutdown** commands.

4. Add one or more **Views** on the **Assignment tab**.
5. Save the job.

The update process will be performed according to the schedule specified in the job.

Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

Updating IGEL OS Using a USB Storage Device

You can use a USB storage device to update IGEL OS locally. This method is particularly suitable if only one device or only a few devices are to be updated and it would not be worth installing an FTP or HTTP server purely for the update.

To update the device's firmware without having access to the local setup, follow Updating the Firmware using the Linux Console (see page 315).

To update IGEL OS using a USB storage device, proceed as follows:

1. Download the update file (.zip) for your device from the IGEL download server[51].
2. Unpack the update files and save them to a USB storage device.

   > You can find the officially supported file systems under Storage Hotplug (see page 1969).

3. Open the IGEL Setup on the device and select **Devices > Storage Devices > Storage Hotplug**.
4. Set **Client Drive Mapping** to **Static**.
5. Enable **Private drive letter for each storage drive**.
6. Set **Number of drives** to at least 1.
7. **Apply** the changes so that they are effective for the device.

   > You can find more information under Storage Hotplug (see page 1969).

8. Connect the USB storage device to the device and wait until the device has been detected.
9. Go to **System > Update > Firmware Update**.
10. Set **Protocol** to **FILE**.
11. Start the file chooser (**Server path**) and navigate to `/userhome/media/label of the USB storage device` / `lxos.inf` and click **Open**.

    > Do NOT use spaces in the USB device name.

12. Click **Update firmware** and confirm the warning message.
    The device will reboot while updating the firmware. Do not remove the USB device until the update has finished.

> Make sure you do not boot from the USB storage device. You might need to change the boot order in the BIOS/UEFI.

51. https://www.igel.com/software-downloads/workspace-edition/

Updating the Firmware using the Linux Console

Issue

You have to update the device's firmware without *IGEL Universal Management Suite* or local *IGEL Setup* application.

Solution

The device's firmware update can also be carried out directly on the Linux console itself without IGEL Setup:

1. Restart the device.
2. Press [ESC]key during booting to bring up the boot menu.
3. Select **Verbose Boot** from the boot menu.
4. When instructed, switch to the console by pressing [CTRL-ALT-F11] or [CTRL-ALT-F12].
5. Press [RETURN]key to log in.
   You may have to enter your password.

Carry out the update. The exact procedure varies according to the protocol which is to be used, that is, FILE, HTTP, or FTP; see the instructions below. You can check whether the correct parameter values have been passed using the `get` command, e.g. `get update.protocol`

HTTP

1. If necessary, set up a static IP address (DHCP is active by default)
   `setparam network.interfaces.ethernet.device0.usedhcp false`
   `setparam network.interfaces.ethernet.device0.manual true`
   `setparam network.interfaces.ethernet.device0.ipaddr`
   `setparam network.interfaces.ethernet.device0.netmask`
2. Configure the update server
   `setparam update.protocol http`
   `setparam update.http.server`
   `setparam update.http.port`

   > The default UMS port is `9080`

   `setparam update.http.path`
   `setparam update.http.user`
   `setcryptparam update.http.crypt_password`

3. Start the update process in the `/` directory using the command `update`

FTP

1. If necessary, set up a static IP address (DHCP is active by default)
   `setparam network.interfaces.ethernet.device0.usedhcp false`
   `setparam network.interfaces.ethernet.device0.manual true`
   `setparam network.interfaces.ethernet.device0.ipaddr`
   `setparam network.interfaces.ethernet.device0.netmask`
2. Configure the update server
   `setparam update.protocol ftp`
   `setparam update.ftp.server`
   `setparam update.ftp.port`

   > The default port is `21`

   `setparam update.ftp.path`
   `setparam update.ftp.user`
   `setcryptparam update.ftp.crypt_password`
3. Start the update process in the `/` directory using the command `update`

FILE

> Requirement: The unpacked update files are available in the root directory of a USB storage device.

1. Configure at least one hotplug USB device:
   `setparam devices.hotplug.usb-storage.numdevices 1`
2. Apply your changes:
   `kill_postsetupd`
3. Connect the USB storage device to the device.
4. Wait for the USB storage device to be mounted automatically.
5. Determine the mount point:
   `ls /media/`
6. Configure the update parameters:
   `setparam update.protocol file`
   `setparam update.file.path /media/<name of USB storage device>`

7. Start the update process in the `/` directory using the command `update`

Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher

Symptom

You have tried to update a device to IGEL OS 11.08 or higher, but the update fails with the error message "Not enough space on local drive".

Problem

IGEL OS 11.08 or higher requires more than 4 GB storage; your device has less storage than required.

Environment

This article is valid for the following environment:

- IGEL OS 11.08 or higher
- UMS 6.05 or higher (recommended)
- Endpoint device that is supported by IGEL OS 11.08 or higher but has a storage size of 4 GB or lower, that is, lesser than the storage size required by the full feature set

Solution

The recommended storage size for IGEL OS 11.08 or higher is over 4 GB. However, you can update an endpoint device with less storage than required by a regular IGEL OS installation. This can be done by reducing the feature set. A modified INF file (`lxos-reduced.inf`) in the update source defines a reduced feature set that makes the firmware fit into your endpoint device's storage.

As an alternative to the preconfigured INF file, you can customize the INF file yourself to define your own reduced feature set.

Reduced Feature Set Cannot Be Changed by Setup/UMS

When you have reduced the firmware as described below, you cannot reactivate features via the Setup resp. the UMS configuration dialog. To recover the complete feature set, you must copy `lxos-full.inf` to `lxos.inf` and then start the firmware update.

Buddy Update

When you have downloaded a reduced firmware on a buddy update server by mistake, the buddy server itself has the reduced feature set. To recover the complete feature set on the buddy server, you must copy `lxos-full.inf` to `lxos.inf` in the update source and then update the buddy update server again.

Using the Preconfigured INF File

→ To find out which features are included in the reduced feature set, open the `readme[version].txt` in your update source directory and search for "Reduced Firmware". The table shows the features, the storage size they require, and whether they are included in the reduced feature set.

Replace the `lxos.inf` file as follows:

1. Go to the directory that contains the source files for the firmware update. If you use the WebDav capability of the UMS, this is `<UMS installation directory>\rmguiserver\webapps\ums_filetransfer\<firmware version>`; example: `C:\Program Files\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\IGEL_OS_11-11.08.110`
2. Delete `lxos.inf`

It is safe to delete `lxos.inf` because there is a backup file named `lxos-full.inf`

3. Copy `lxos-reduced.inf` to `lxos.inf`
4. Start the firmware update as usual.

Customizing the INF File

→ To get a list of all features and their storage requirement, go to IGEL OS Release Notes (see page 2282), look up your version of IGEL OS, go to "Component Versions [your version]", and find the "Services" section.

To customize the INF file:

1. Open `lxos.inf`
2. In the [INFO] section, add the following line: `custom="true"`
3. Delete the `[PART]` section of every partition you want to exclude, but do this ONLY IF the section has both of the following entries:
   `dispensable="true"`
   `type="squashfs-auto"`

4. Save `lxos.inf` and start the firmware update as usual.

Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG

Possible Problem

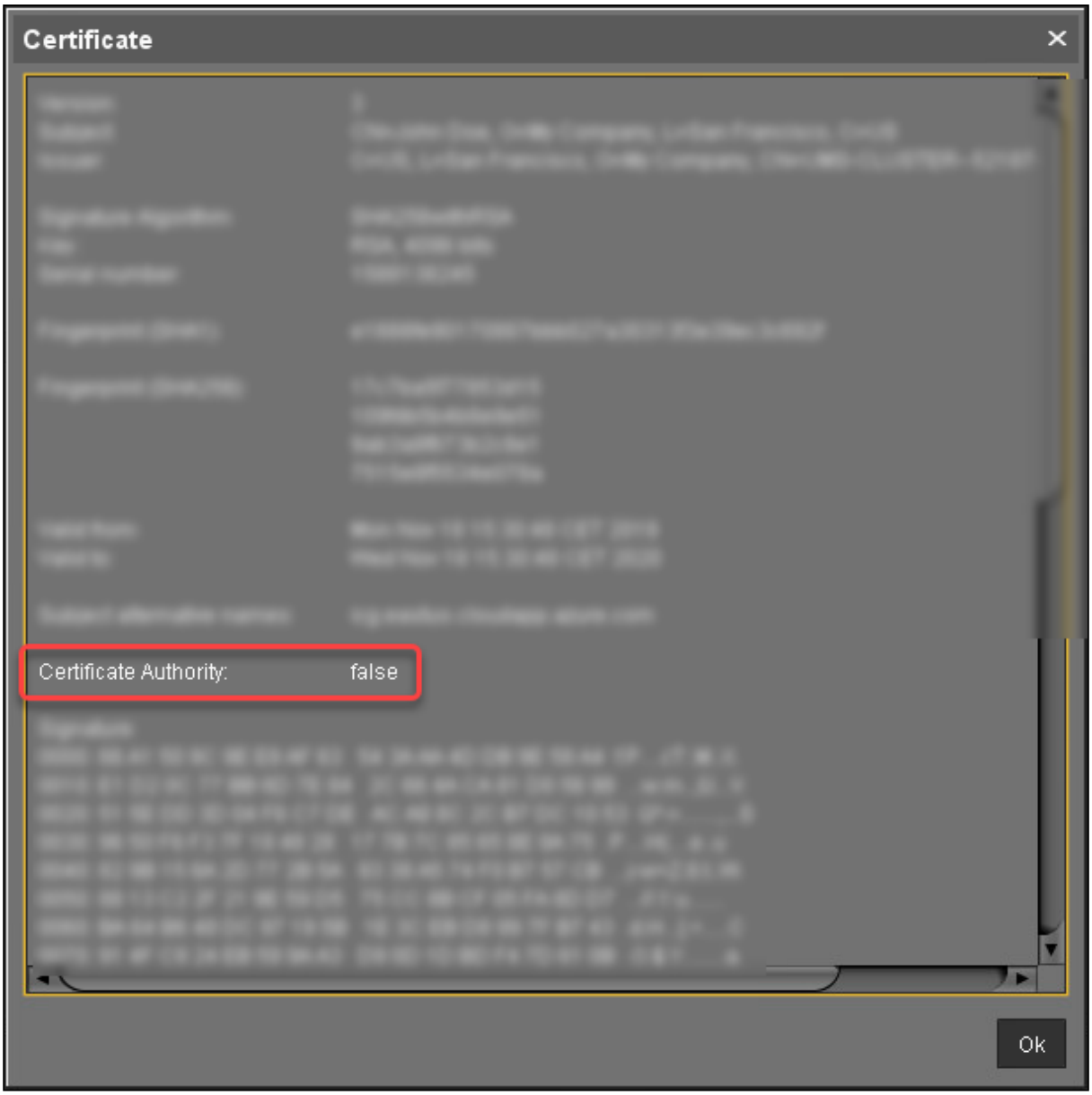
If you update to IGEL OS 11.04 or higher, devices might fail to connect to the ICG afterward because the CA root certificate does not have the CA flag (i.e. X509v3 BasicConstraint extension "is_ca" is set to "false"). This is the case when the certificate has been created with UMS 5.07 or UMS 5.08.

Environment

- UMS 5.07 or higher (update to UMS 6.06 or higher will be required if not already present)
- ICG with older root certificates that have been created with UMS 5.07 or UMS 5.08

Diagnosis

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway Configuration** (UMS 5.07 to UMS 6.05) or **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** (UMS 6.06 or higher) and select your ICG root certificate.
2. Click to review the content of the certificate.
3. If **Certificate Authority:** is **false**, find further instructions under Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG#Solution (see page 321).



Solution

1. Request IGEL OS 11.04.221DER from the IGEL Support team.
2. Update your devices to IGEL OS 11.04.221DER.
3. Update your UMS to version 6.06.100, if you have not already done so.
4. Exchange the root certificate for the ICG connection; see How to Exchange the Root Certificate for ICG[52].
5. Update your devices to IGEL OS 11.04.240 or higher.

52. https://kb.igel.com/en/igel-cloud-gateway/current/how-to-exchange-the-root-certificate-for-icg

Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher

Symptom

After an update to IGEL OS 11.04 or higher, the device fails to connect to the UMS via ICG. The log journal shows a message similar to this:

```
igelrm_agent[9824]: [2020/11/11 17:56:16:0140] ERR: SSL error: invalid CA certificate (preverify_ok=0;err=24;depth=1)
```

Environment

- UMS 5.07 or higher
- ICG with older root certificates that have been created with UMS 5.07 or UMS 5.08
- Devices that have just been updated to IGEL OS 11.04 or higher

Problem/Possible Cause

CA root certificates for ICG that have been created with UMS 5.07 or UMS 5.08 are not accepted by IGEL OS 11.04. This is because version 1.1 of the OpenSSL library does not accept certificates as CA certificates if they do not have the CA flag (i.e. X509v3 BasicConstraint extension "is_ca" is set to "false"). As a consequence, IGEL OS 11.04 or higher refuses to use such a certificate.

Diagnosis

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway Configuration** (UMS 5.07 to UMS 6.05) or **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** (UMS 6.06 or higher) and select your ICG root certificate.
2. Click to review the content of the certificate.

3. If **Certificate Authority:** is **false**, find further instructions under Solution (see page 324).

Solution

1. ReInstall the ICG using an appropriate root certificate. For details, see the following articles:
   - Providing the Certificates (see page 323)
   - Installing the IGEL Cloud Gateway (see page 323)
2. Register the devices again. For details, see Connecting the Devices (see page 323).

IGEL OS Automatic Update Service for Device Evaluation

Overview

The automatic update service checks for available firmware updates periodically; if a firmware update is available, the user is prompted to start the update. The firmware is provided by IGEL via a download server that is known by the automatic update service. Alternatively, you can use a download server of your own.

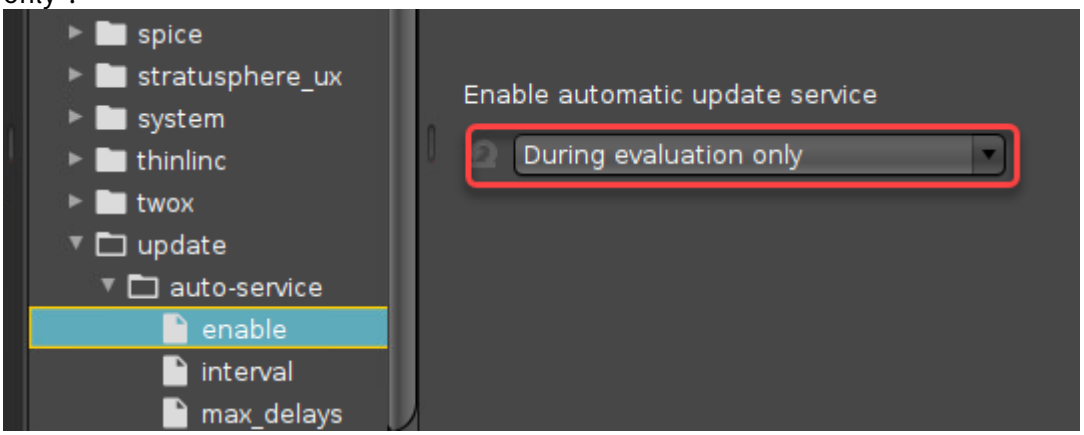
The automatic update service is only available for devices with an evaluation license; when the device receives a Workspace Edition license, the service is deactivated.

Environment

- Endpoint device with IGEL OS 11.06.100 or higher

Configuring the Automatic Update Service

1. In the UMS configuration dialog or the local Setup, go to **System > Registry > update > auto-service > enable** and ensure that **Enable automatic update service** is set to "During evaluation only".



2. Set the following parameters according to your requirements:
   - **interval**: Time interval in hours in which the device should check for firmware updates during runtime. When the value is 0, the device only checks on boot.
   - **max_delays**: Maximal times the user can postpone an update. Example: When this value is set to 9, the user can postpone the update 9 times before the update will be forced. When the value is 0, the update will be forced immediately.
   - **randomized_delay**: Delay time that is added to the interval to avoid an excessive amount of requests to the server at the same time.
   - **server**: If you want to use an update server of your own, enter its address here. If the field is empty, the public update server provided by IGEL will be used.
   - **user_dialog_timeout**: Timeout in seconds before the user dialog is closed and the update is started. When set to 0, the dialog remains open until the user closes it.

- **version**: The target version to which the device should be updated. If the field is left empty, the current version will be used. Example: "11.05.133"

3. Click **Apply** or **Ok** to confirm your settings.

BIOS Tools

- BIOS Update for Devices Supported by LVFS (see page 328)
- BIOS Tools for Supported HP Devices (see page 349)

BIOS Update for Devices Supported by LVFS

BIOS Updates at Your Own Risk
IGEL is offering and supporting the LVFS BIOS Update mechanism - BIOS updates are performed at your own risk!

Legacy BIOS Not Supported

The LVFS BIOS update mechanism works only with EFI/UEFI, not with legacy BIOS.

The LVFS BIOS update mechanism is functional even with Secure Boot enabled and when a BIOS password is set.

If the BIOS of your devices is distributed via the Linux Vendor Firmware Service (LVFS), you can update, downgrade, or reinstall it using the IGEL Universal Management Suite (UMS).

As the procedure for reinstalling and downgrading the BIOS are analogous to the update procedure, we will use the term "update" in the following instructions.

Supported Devices

For a list of supported devices, see https://fwupd.org/lvfs/devices/

Requirements

- UMS 6.01 or higher
- Device supports LVFS, for example, supported Lenovo devices.
- The device has IGEL OS 11.08.100 or higher; it is recommended to use IGEL OS 11.08.230 due to significant improvements in our implementation.
- If the device has IGEL OS 11.08.290 or higher, the BIOS Tools feature must be installed explicitly. Instructions are provided under **Configuring the BIOS Update**, step 3.

Getting the BIOS Update File from LVFS

→ Look up the latest update file from https://fwupd.org/lvfs/devices/ and download it. If you want to use the UMS for file distribution, store it in a location that is reachable from the machine on which your UMS Server is running.

Installing the BIOS Tools Feature (IGEL OS 11.08.290 or Higher)

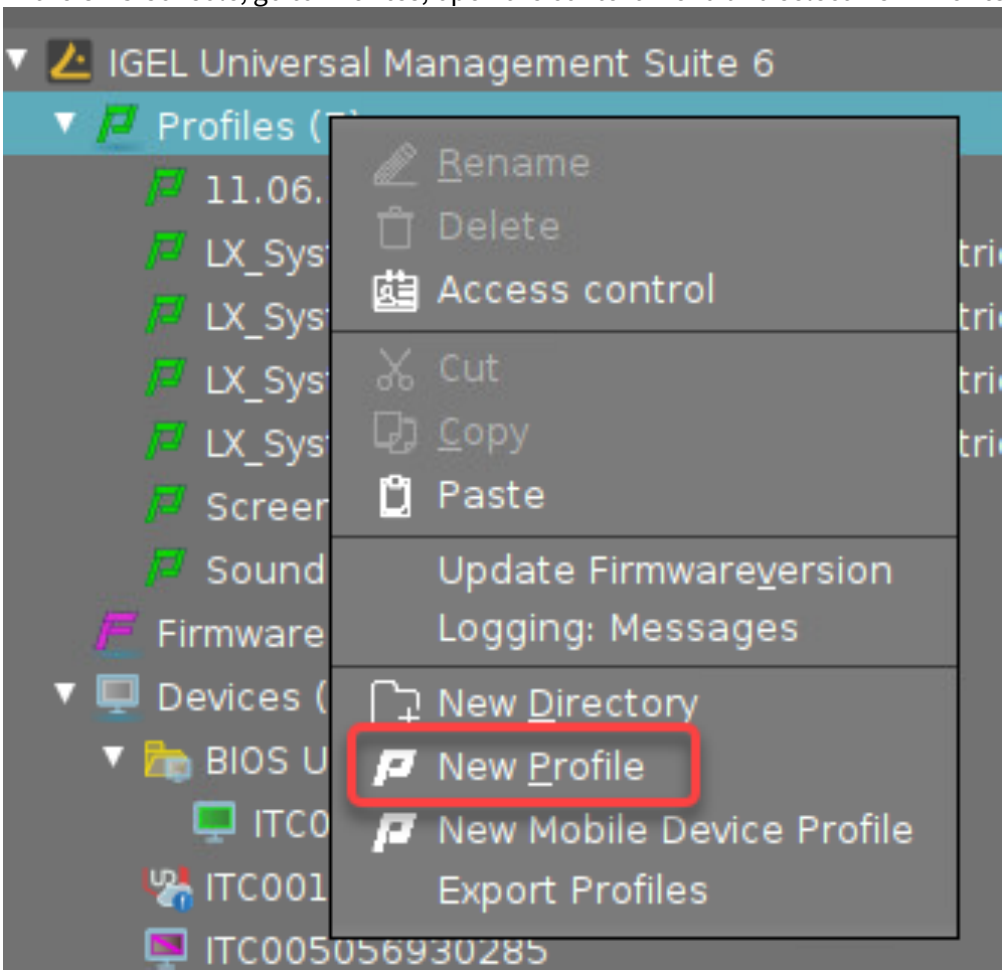
With IGEL OS 11.08.290 or higher, the BIOS Tools feature must be installed first.

1. In the local Setup or, preferably, in a profile, go to

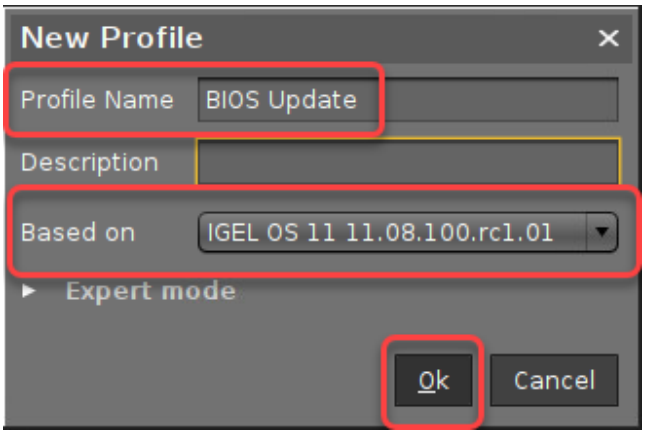
Configuring the BIOS Update

We will create a profile to make the settings available for all relevant devices.

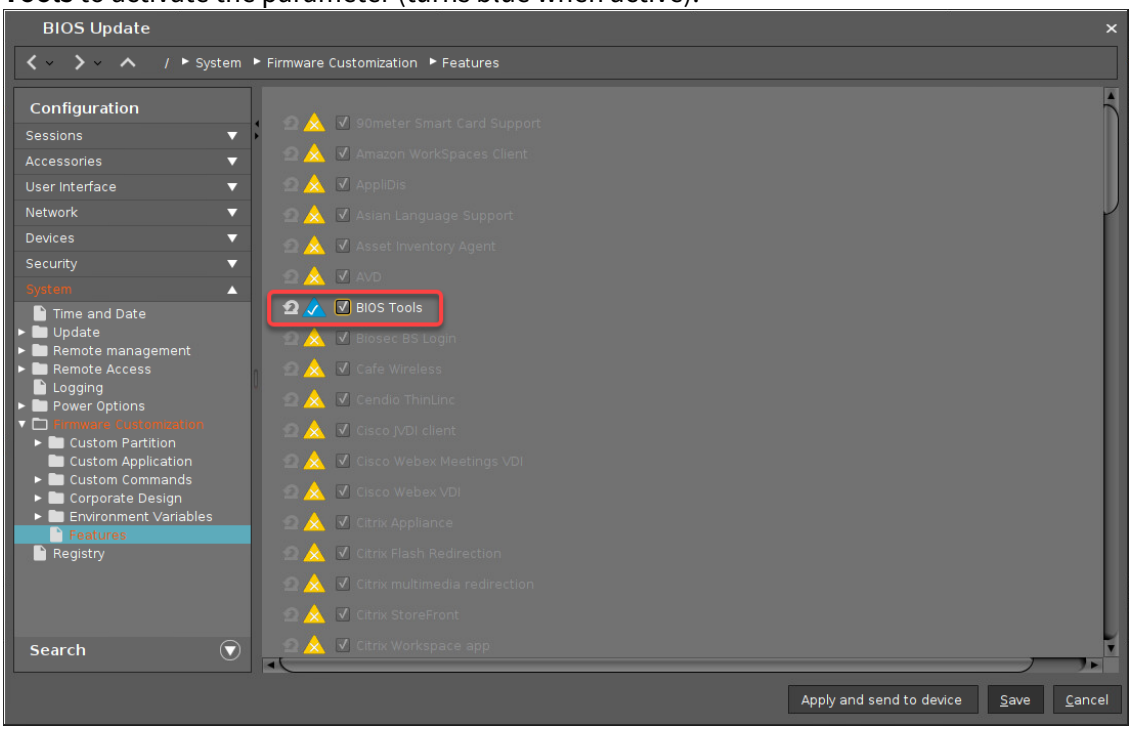
1. In the UMS Console, go to **Profiles**, open the context menu and select **New Profile**.



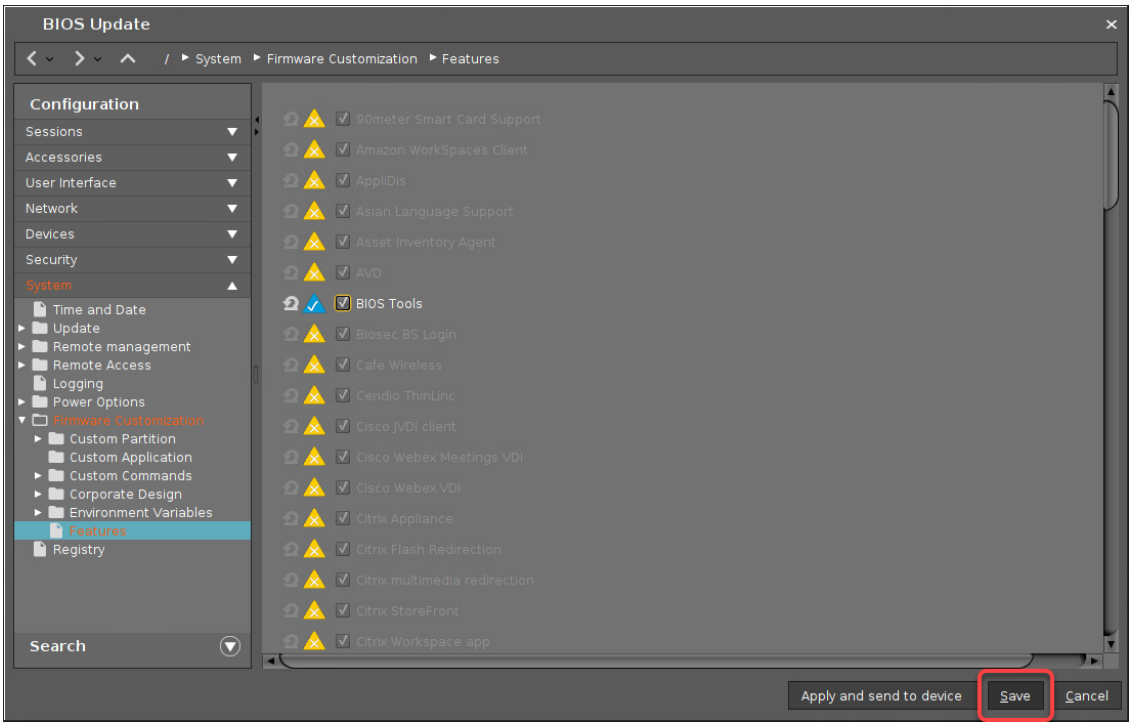
2. Provide the following data and then click **Ok**.
   - **Profile Name**: Display name of the profile
   - **Based on**: Select the IGEL OS version of the devices; must be IGEL OS 11.08 or higher



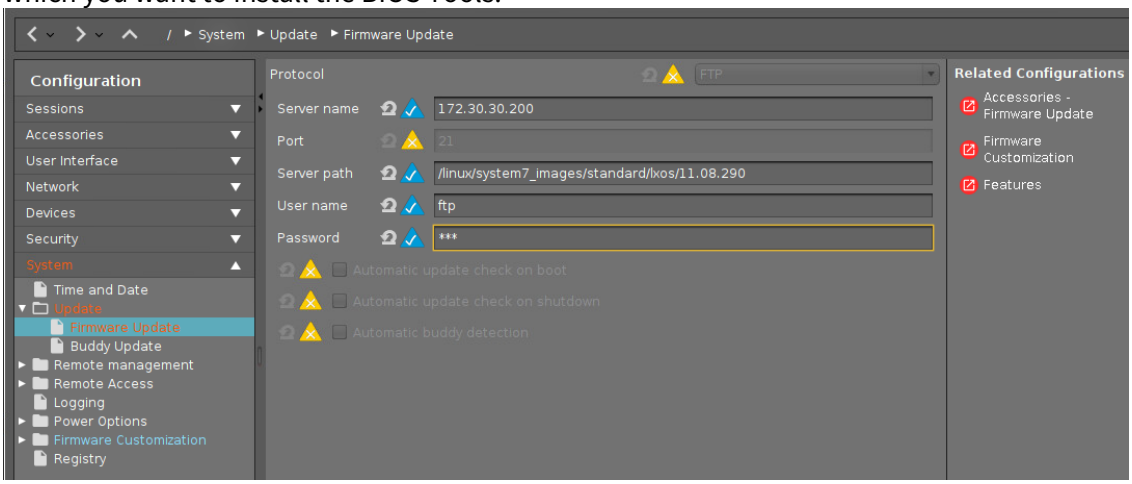
3. If your devices have IGEL OS 11.08.290 or higher, you must install the BIOS Tools feature first. Perform the following steps:
   a. Go to **System > Firmware Customization > Features** and click the yellow icon beside **BIOS Tools** to activate the parameter (turns blue when active).



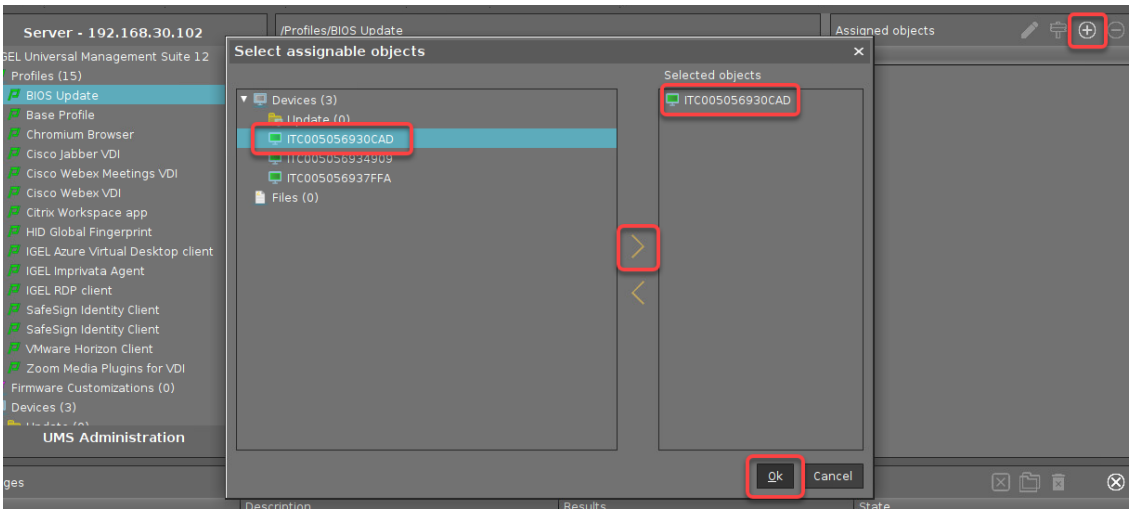
   b. Click **Save**.



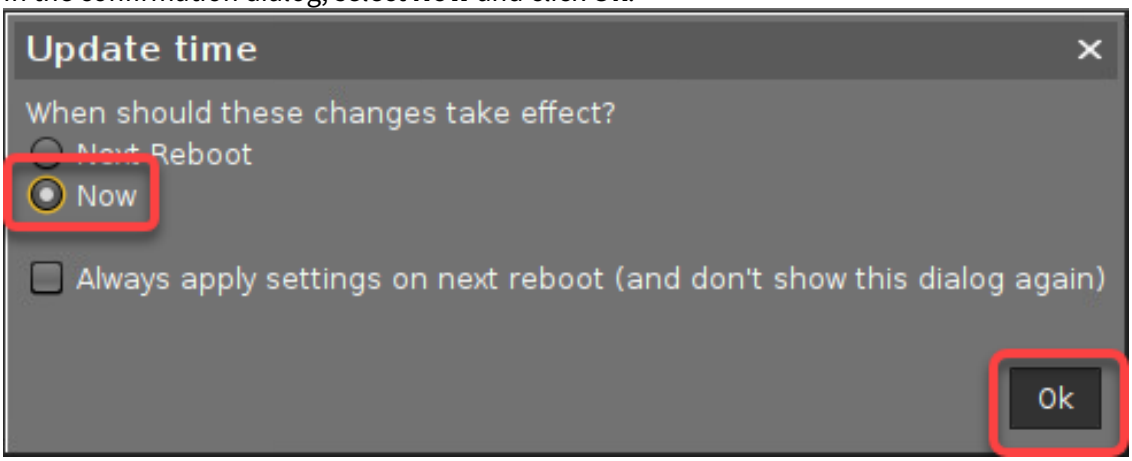
c. Check if the settings under **System > Update > Firmware Update** are valid for all devices on which you want to install the BIOS Tools.



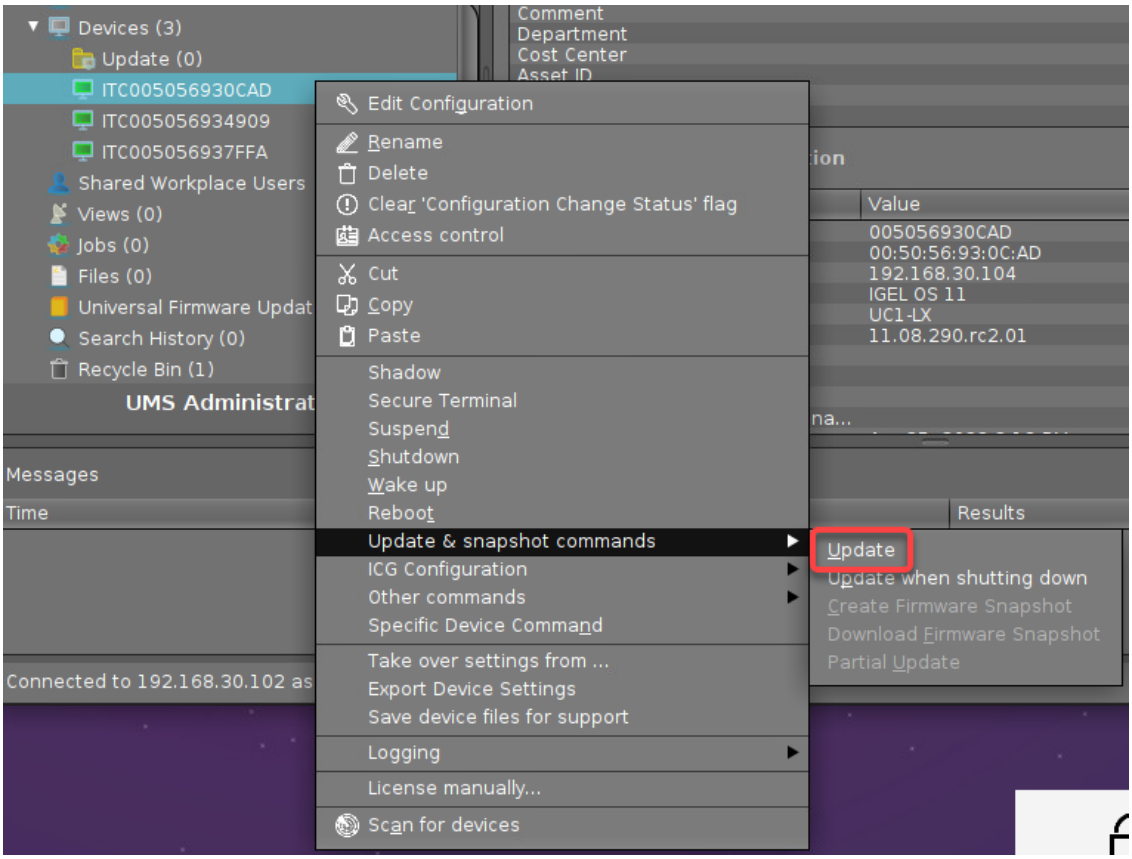
d. Assign the profile to the devices.



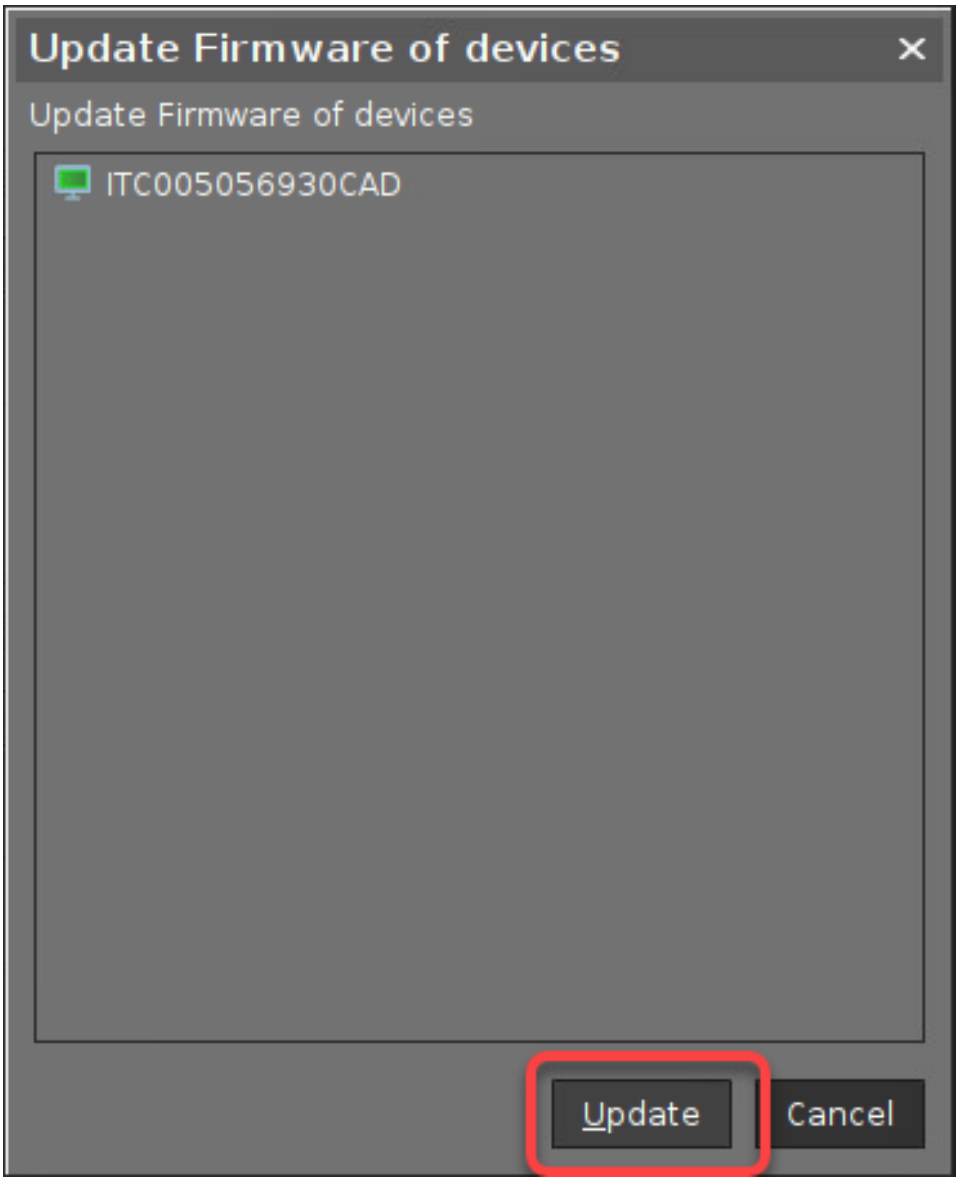
e. In the confirmation dialog, select **Now** and click **Ok**.



f. Select the relevant devices, open the context menu, and select **Update**.

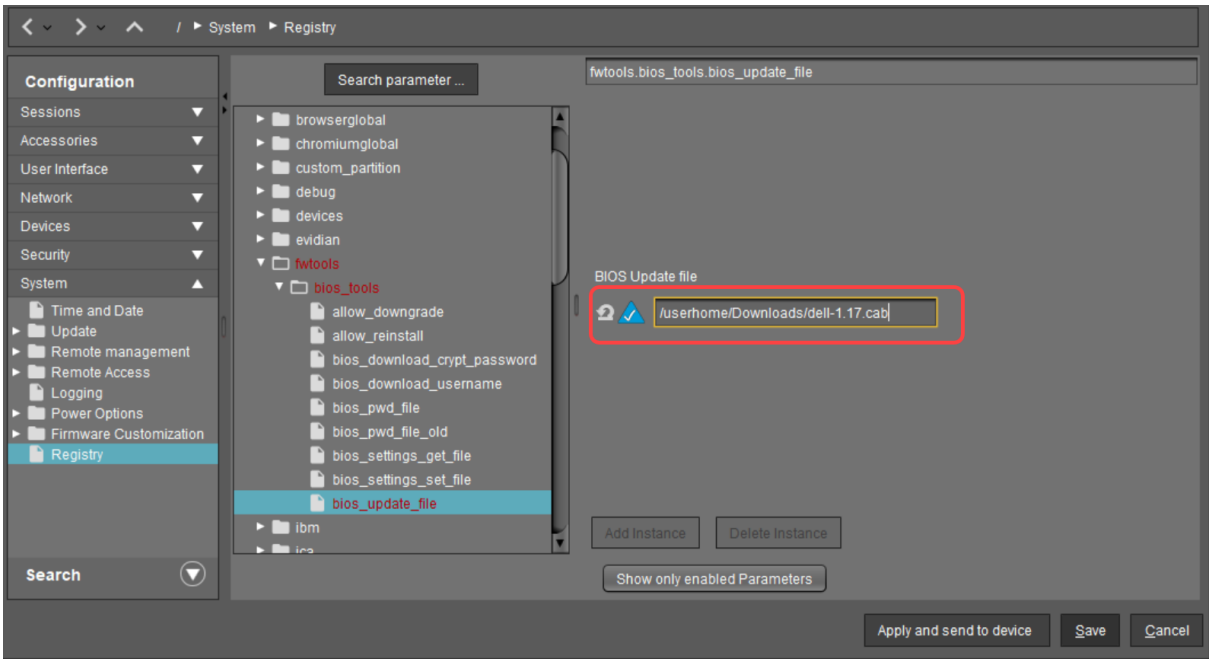


g. Confirm the update.

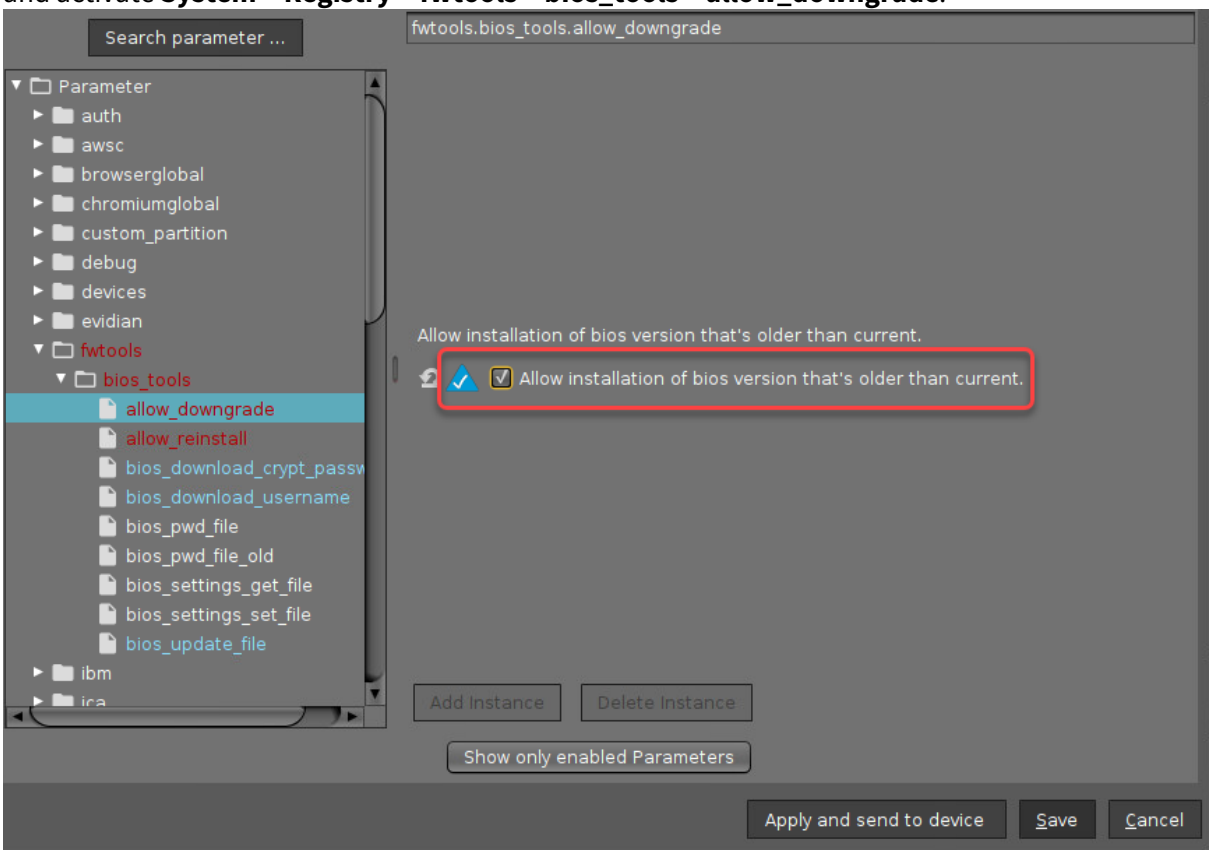


The devices will download and install the BIOS Tools feature.

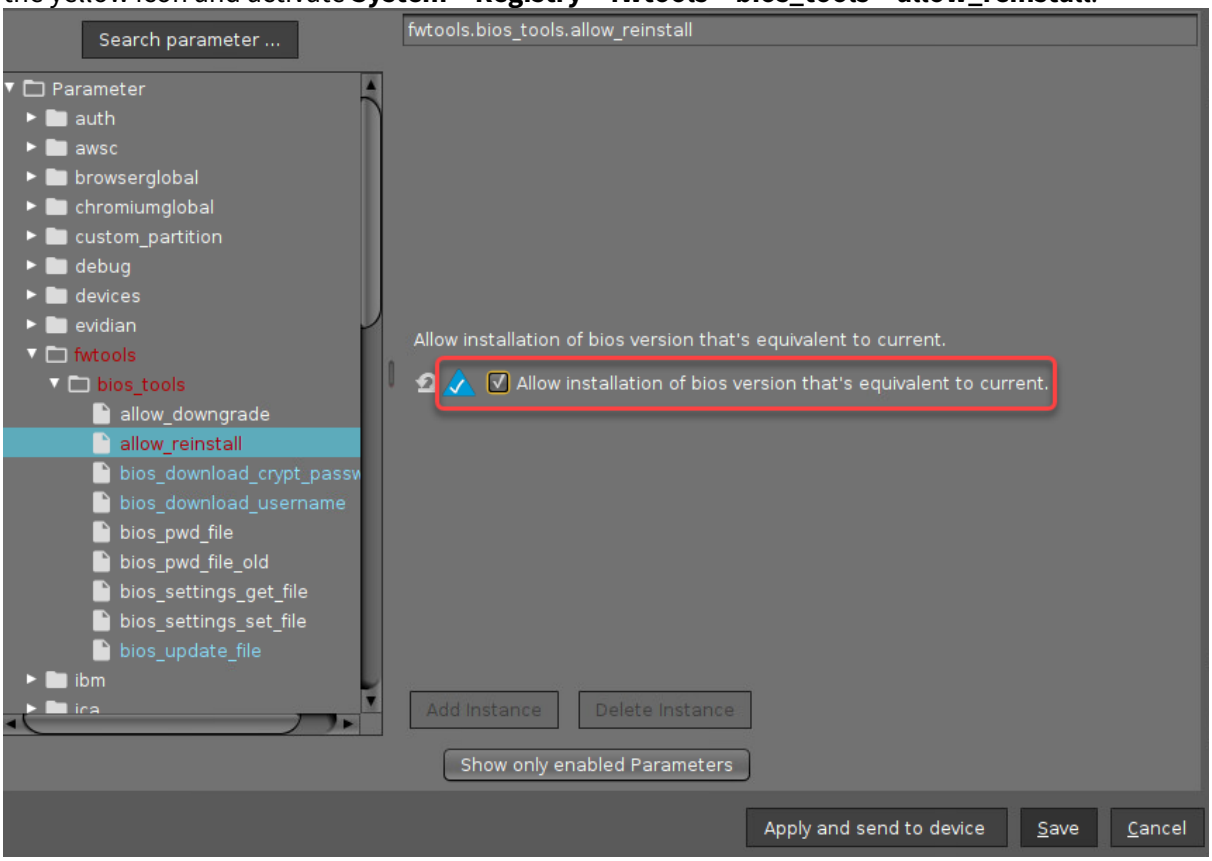
4. Go to **System > Registry > fwtools > bios_tools > bios_update_file**, click the yellow icon to activate the parameter (turns blue when active), and enter the path or the URL of the update file.



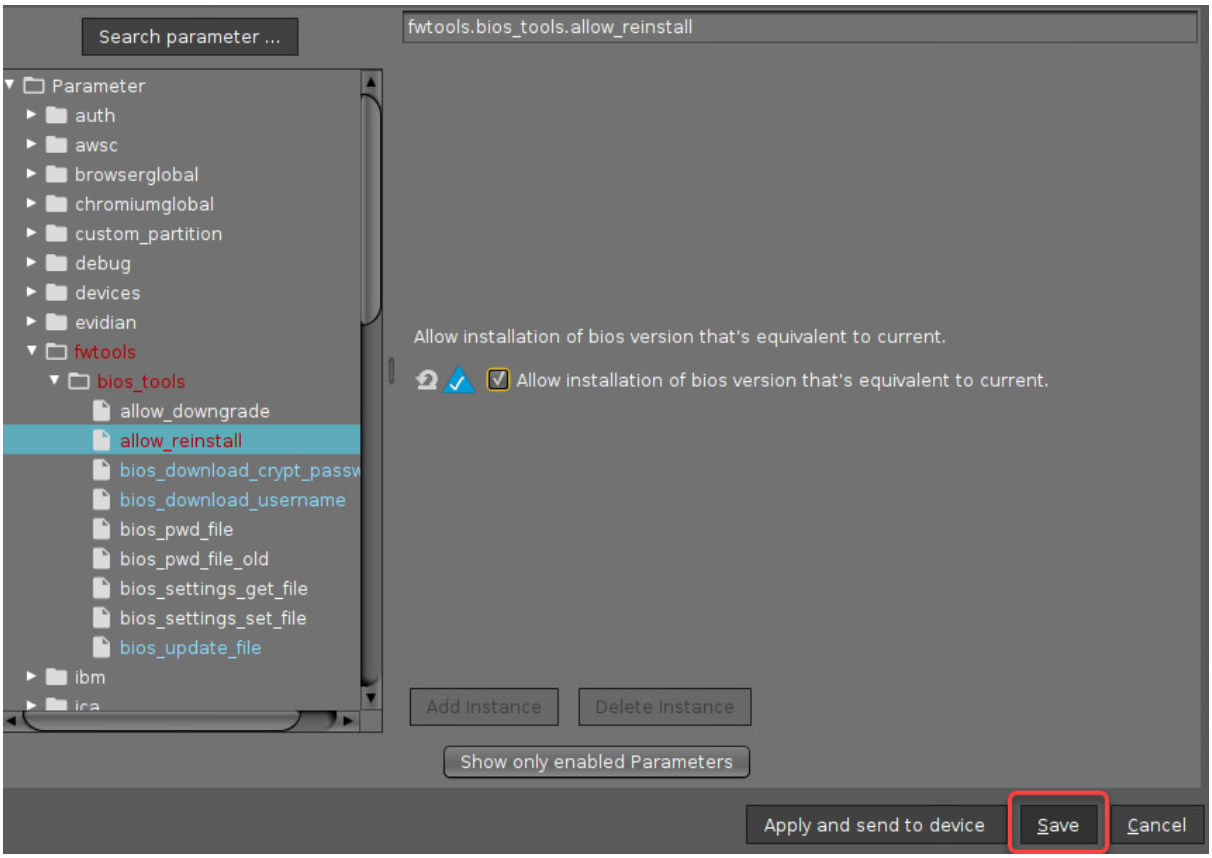
5. If you want to downgrade the BIOS, i.e. replace the BIOS with a lower version: Click the yellow icon and activate **System > Registry > fwtools > bios_tools > allow_downgrade**.



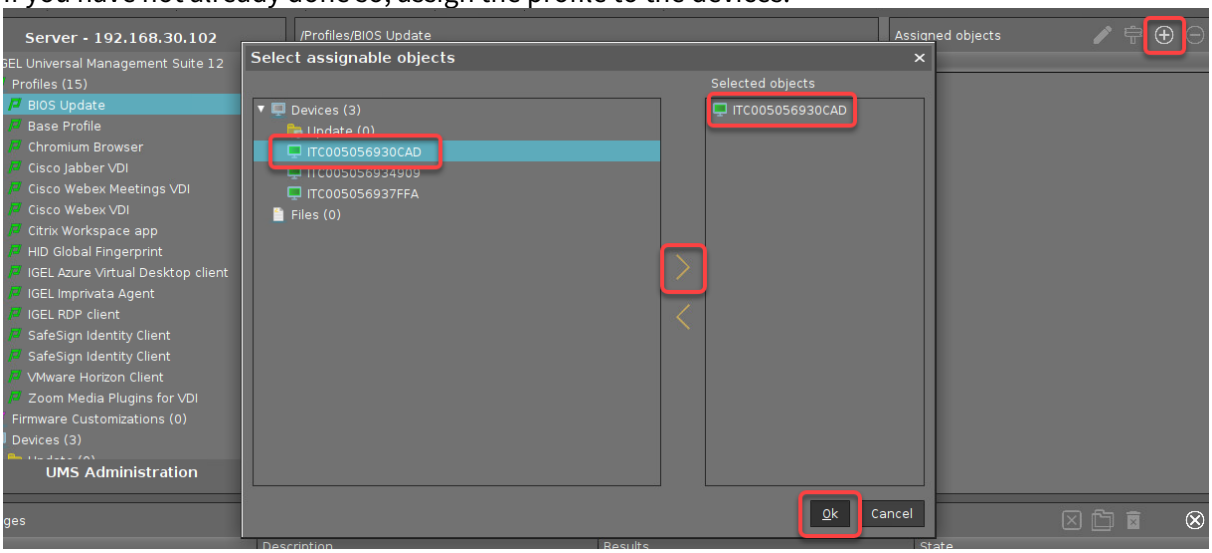
6. If you want to reinstall the BIOS, i.e. replace the BIOS with a fresh BIOS of the same version: Click the yellow icon and activate **System > Registry > fwtools > bios_tools > allow_reinstall**.



7. Click **Save** to write the profile.



8. If you have not already done so, assign the profile to the devices.

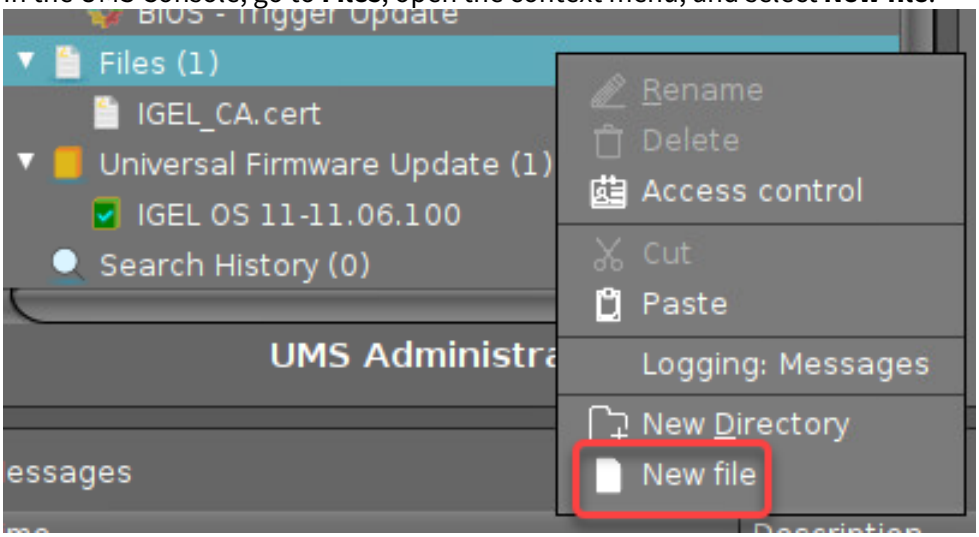


Providing the BIOS Update File

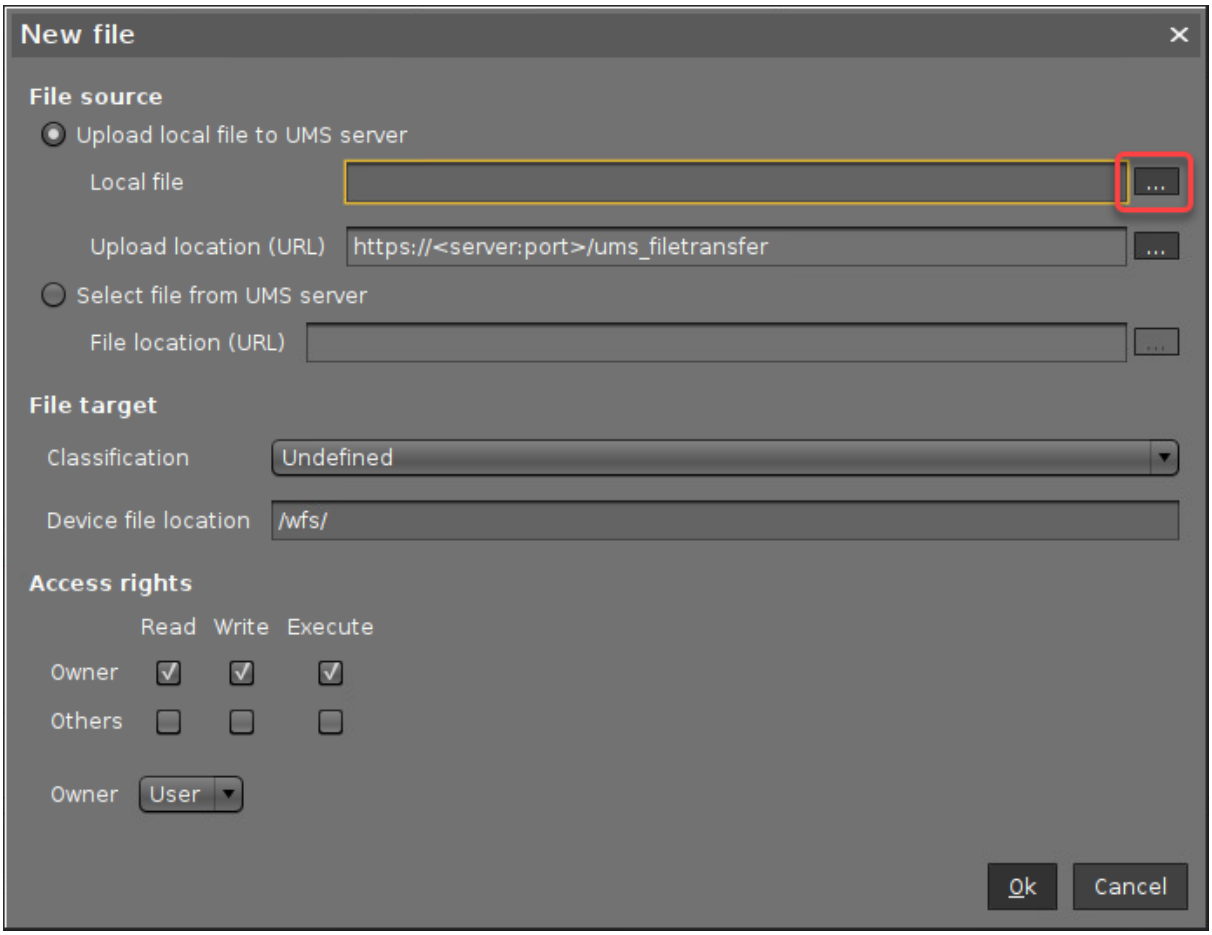
Local Source

To transfer the BIOS update file to the device, we will use the UMS file transfer functionality.

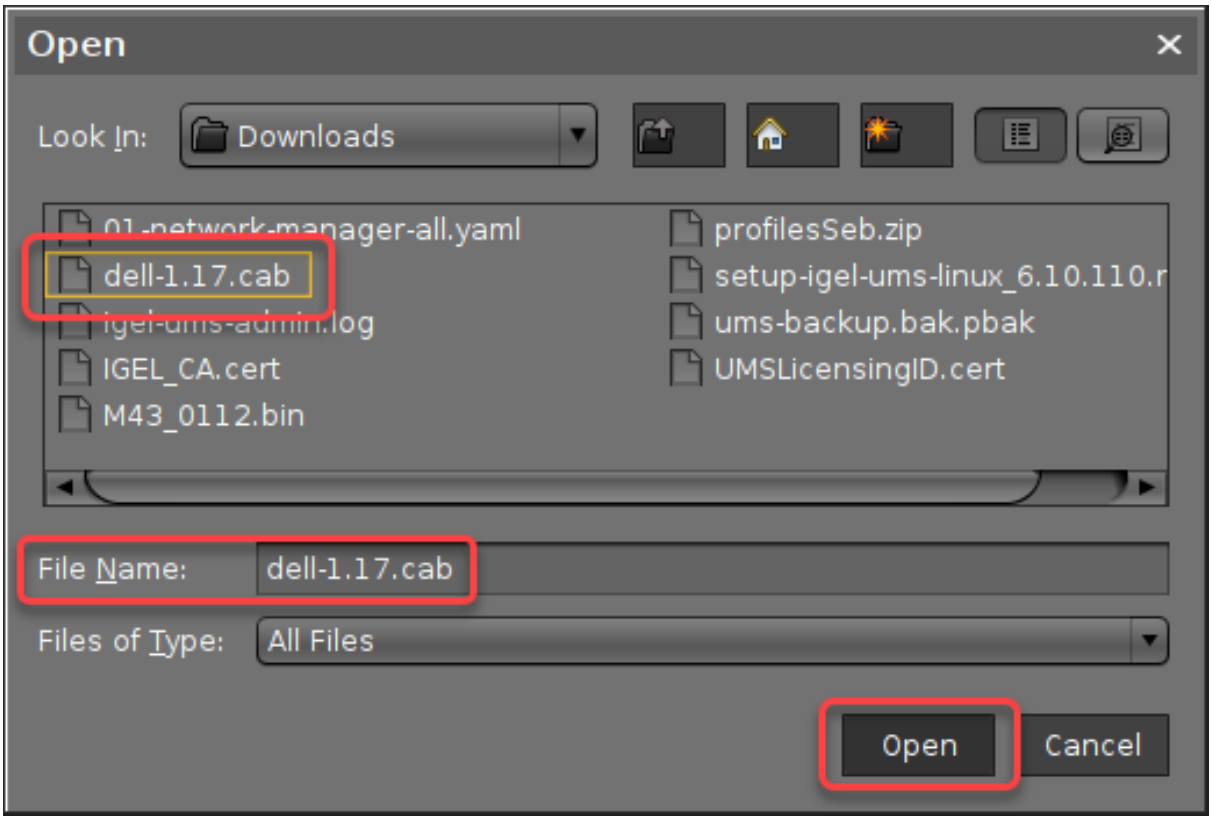
1. In the UMS Console, go to **Files**, open the context menu, and select **New file**.



2. Click the file chooser button.

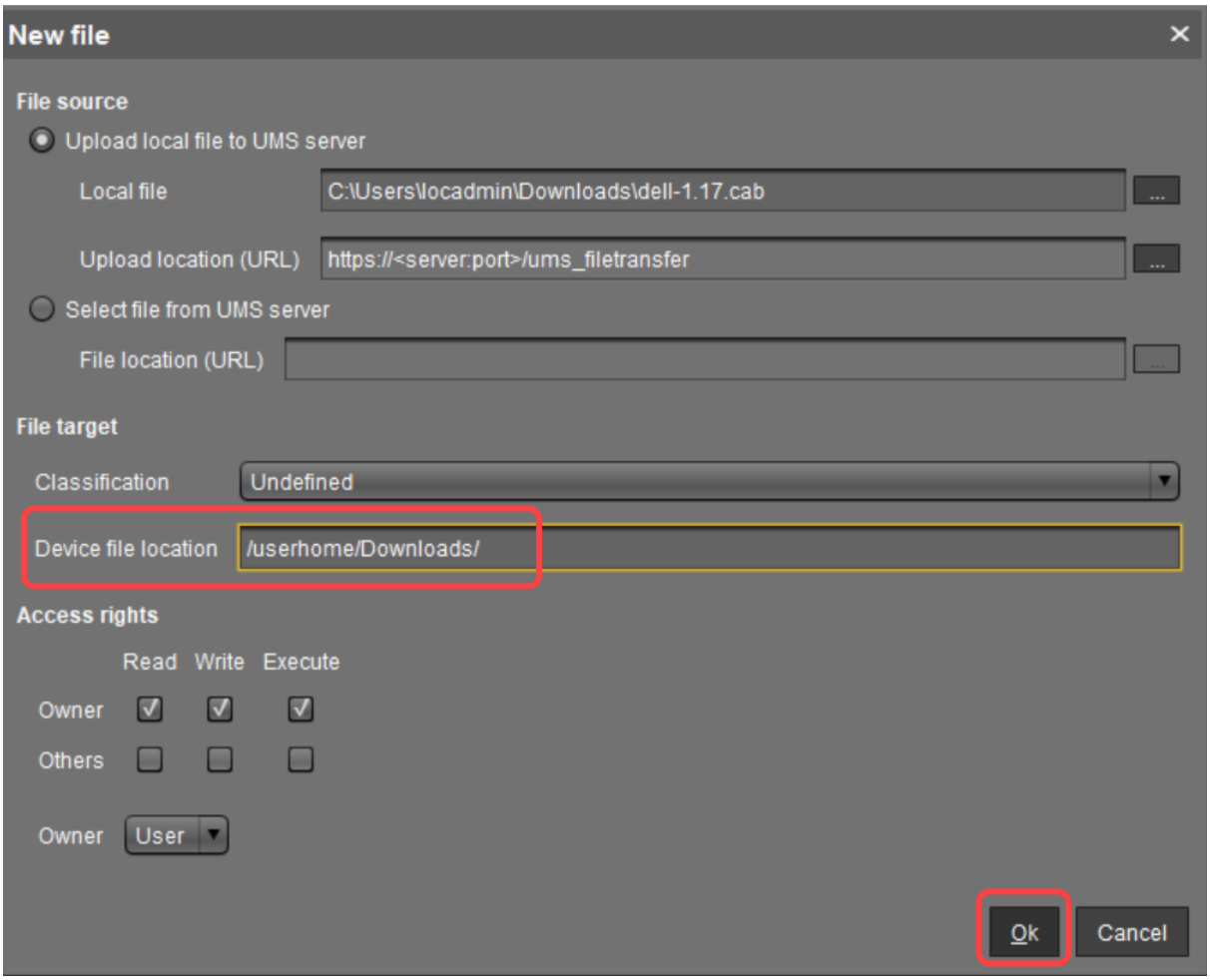


3. Find the BIOS update file in your file system, select it and click **Ok**.



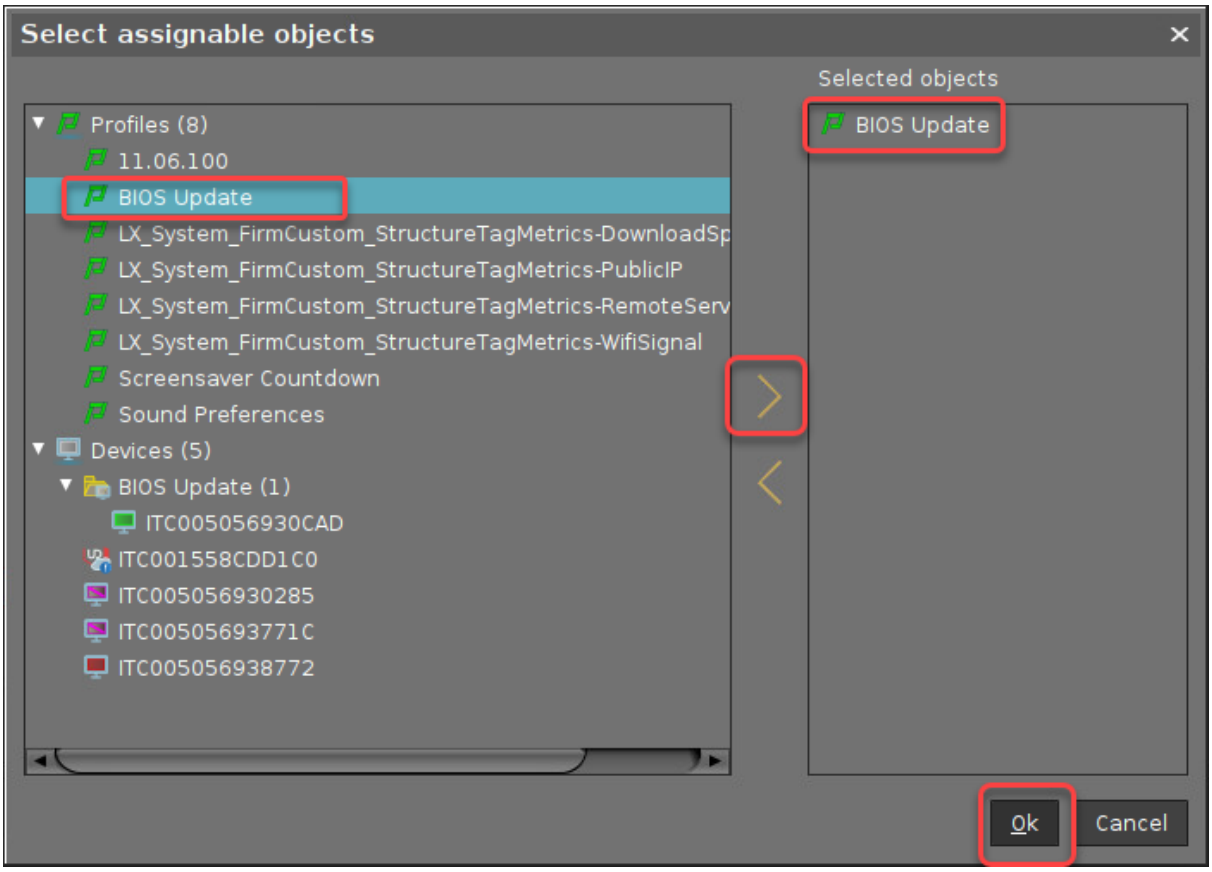
4. In the field **Device file location**, define the local path in which the file will be stored on the device, e.g. `/userhome/Downloads/`. Afterward, click **Ok**.

   ⚠ It is recommended NOT to use `/wfs/` to store the BIOS update file.



5. Click the ⊕ icon to open the assignment dialog.

6. Assign the file to your devices by assigning it to the profile we have created beforehand.

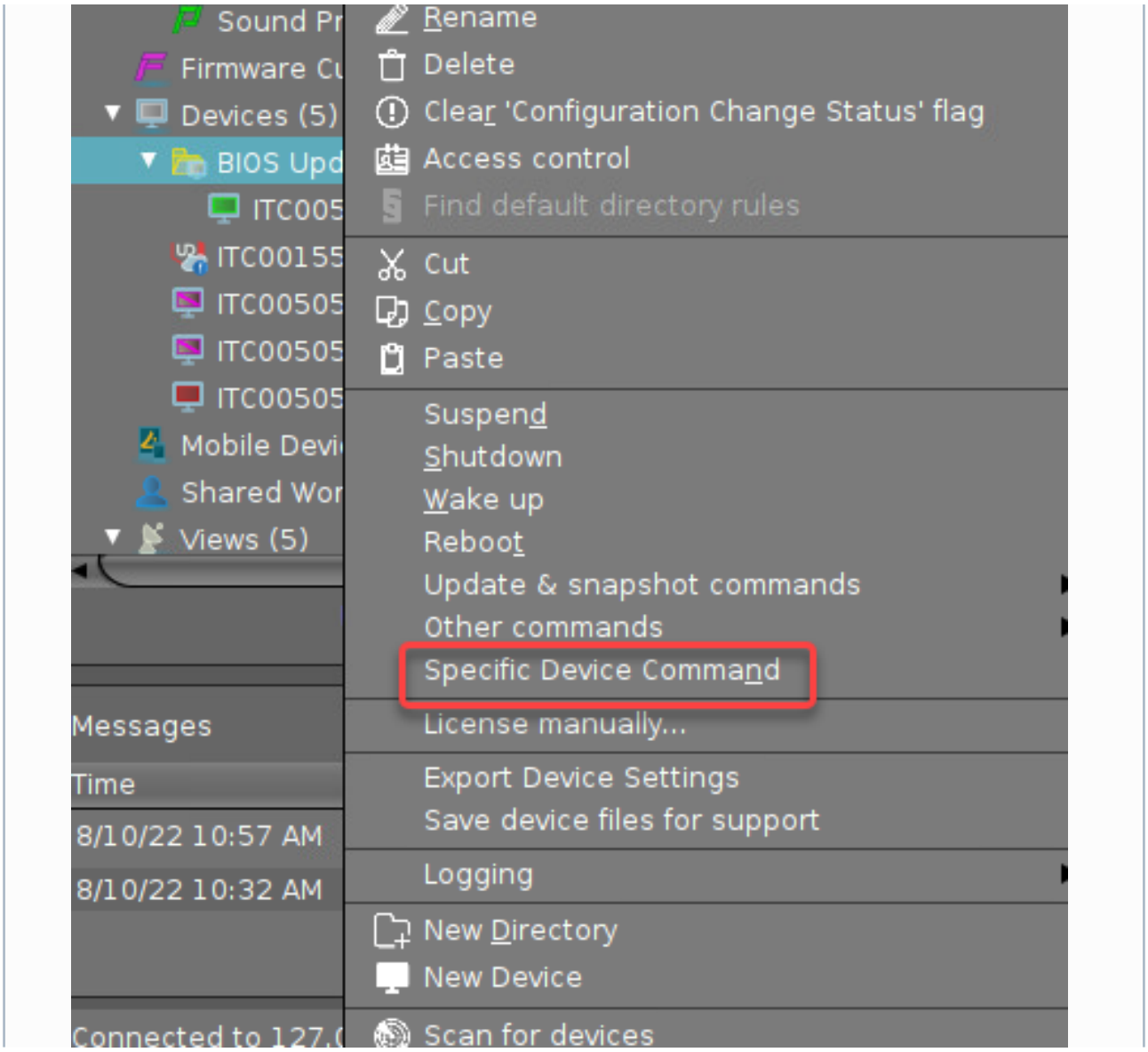


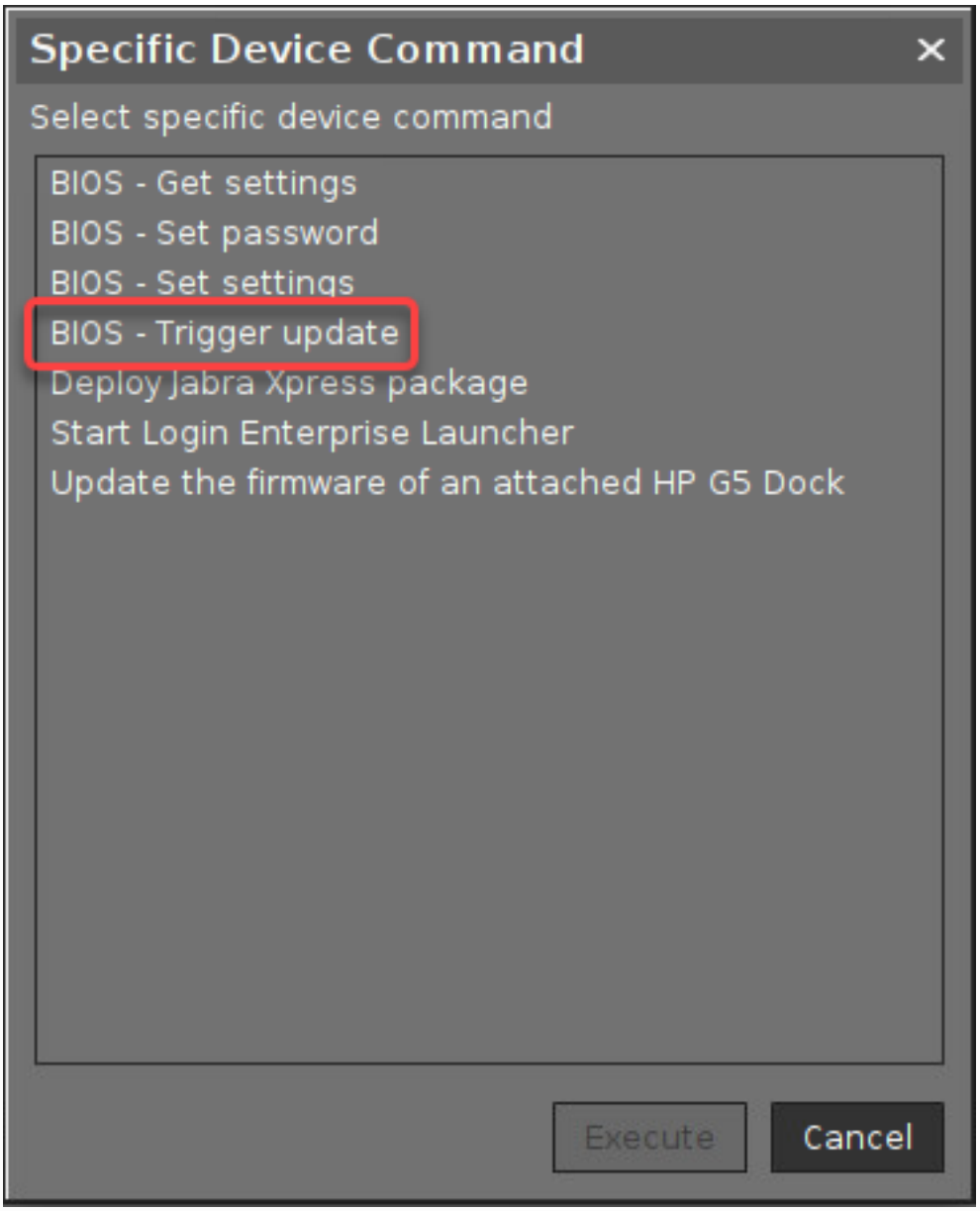
Remote Source

▶ Transfer the file to an HTTP server; ensure that the URL provided under **System > Registry > fwtools > bios_tools > bios_update_file** is matched.

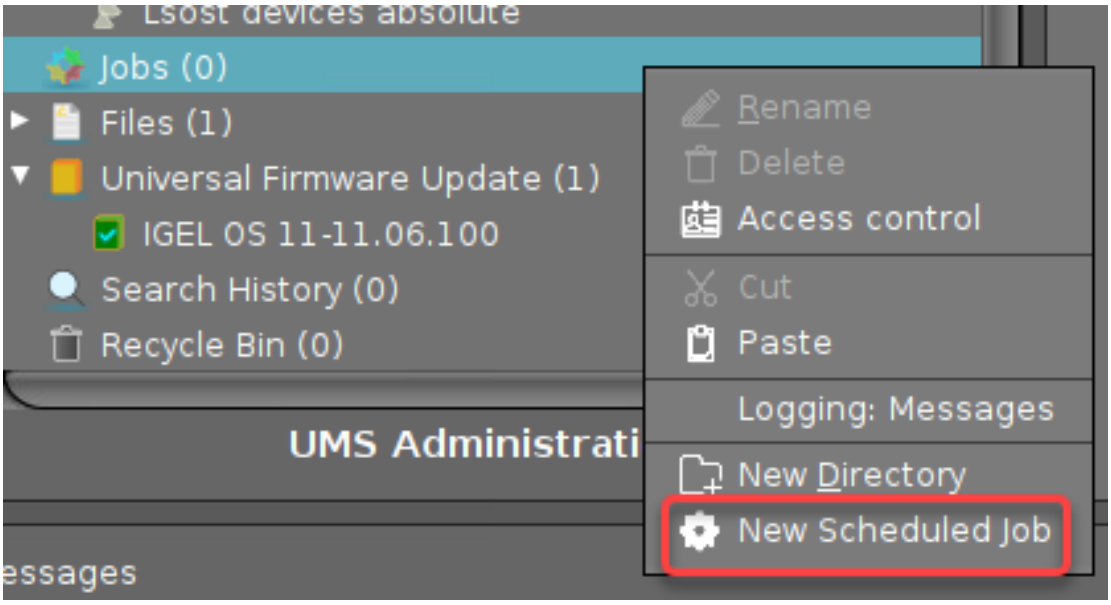
Triggering the BIOS Update

In the following instruction, we will use a scheduled job to trigger the BIOS update.
Alternatively, you can trigger the BIOS update manually. For this purpose, select **Specific Device Command** from the context menu of the device or the corresponding directory and then select **BIOS - Trigger update**:

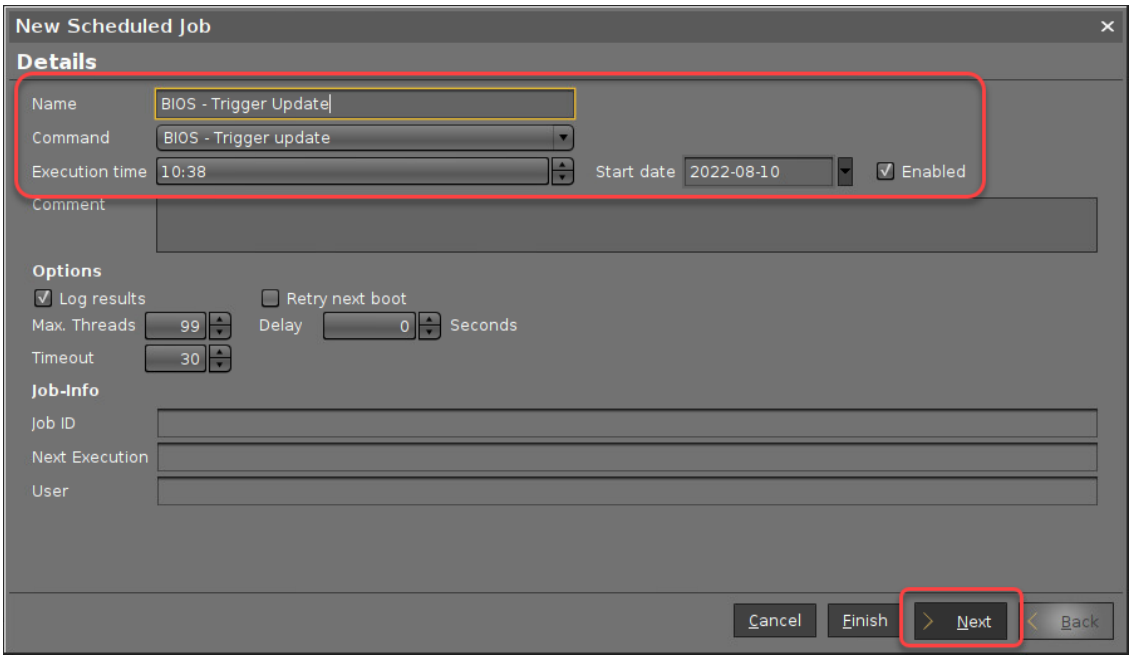

Sound Pr
Firmware Cu
Devices (5)
BIOS Upd
ITC005
ITC00155
ITC00505
ITC00505
ITC00505
Mobile Devi
Shared Wor
Views (5)
Messages
Time
8/10/22 10:57 AM
8/10/22 10:32 AM
Connected to 127.(
Rename
Delete
Clear 'Configuration Change Status' flag
Access control
Find default directory rules
Cut
Copy
Paste
Suspend
Shutdown
Wake up
Reboot
Update & snapshot commands
Other commands
Specific Device Command
License manually...
Export Device Settings
Save device files for support
Logging
New Directory
New Device
Scan for devices



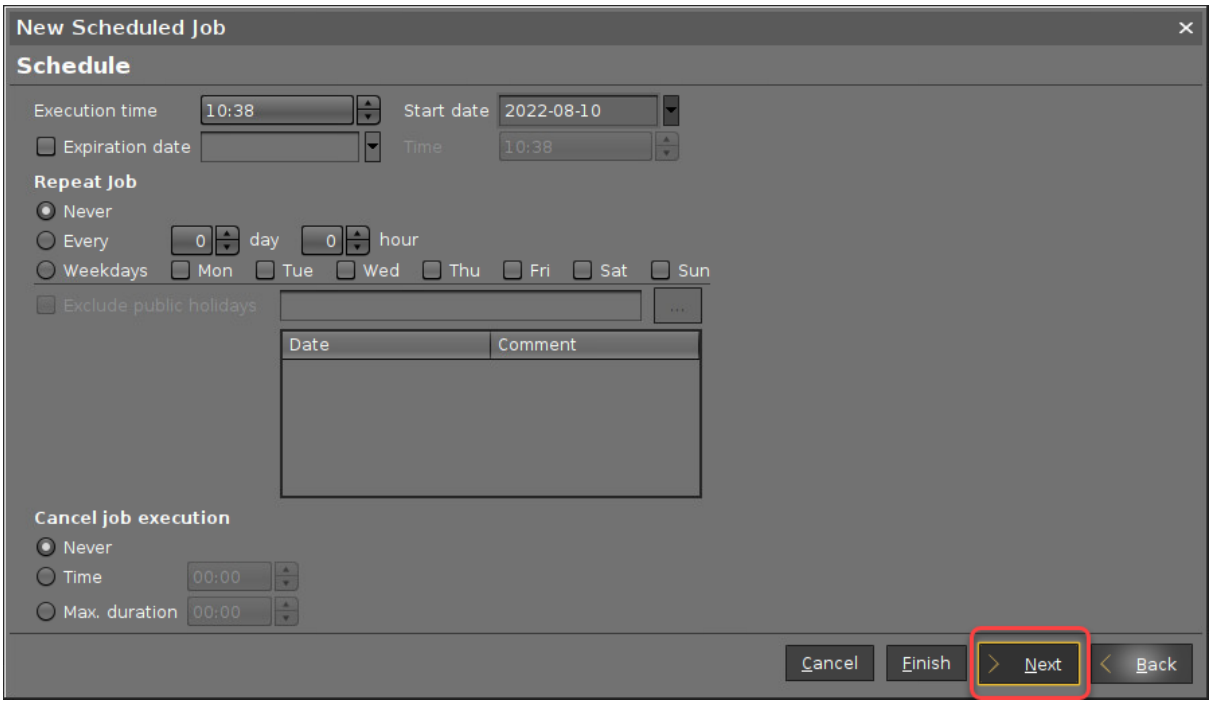
1. In the UMS Console, go to **Jobs**, open the context menu and select **New Scheduled Job**.



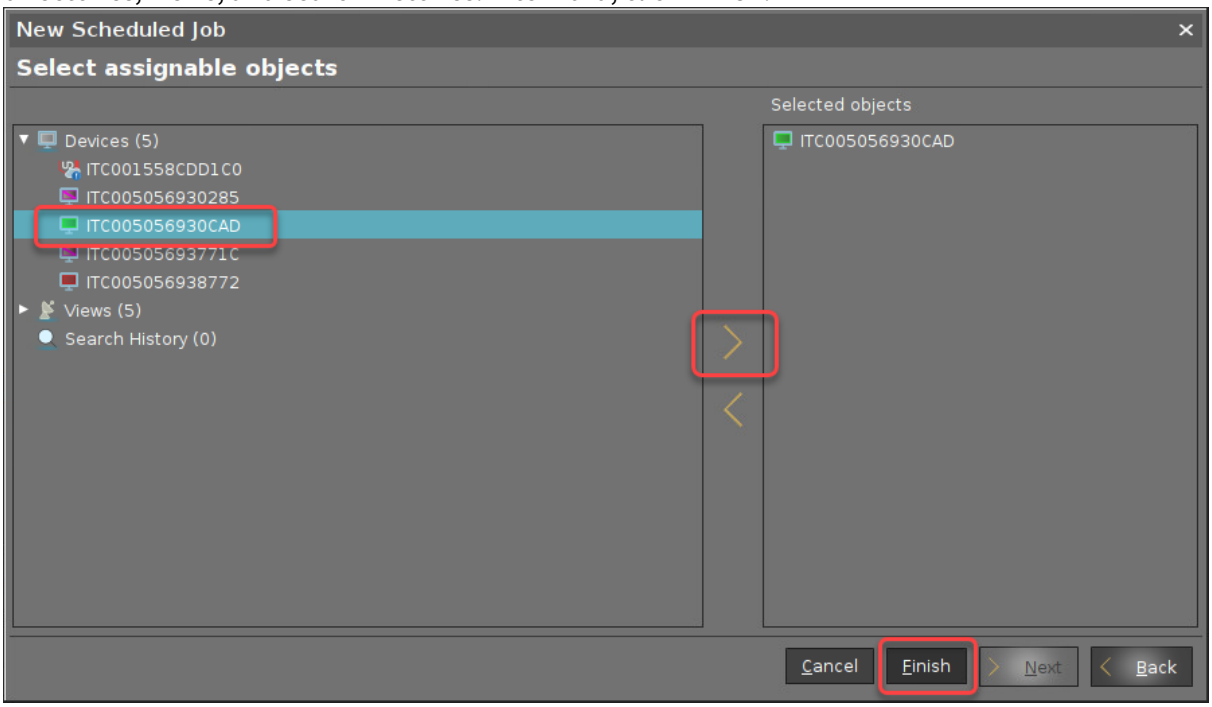
2. Provide the following data and then click **Next**.
   - **Name**: Display name for the job
   - **Command**: Select **BIOS - Trigger update**.
   - **Execution time**: Time at which the BIOS should be updated
   - **Start date**: Date at which the BIOS should be updated
   - **Enabled**: Ensure that this is activated



3. Make sure that **Repeat Job** is set to **Never** and click **Next**.



4. Select the devices on which the BIOS update should be performed. You can select single devices, directories, views, and search histories. Afterward, click **Finish**.



When the job is executed, a dialog informs the user that a reboot is required. The user can choose between two options:

- Perform the reboot and update right away
- Postpone the update to the next reboot

Using the Command Line Tool (bios-tools)

For testing the BIOS update on a single device, you can use the command line tool as an alternative to a scheduled job from the UMS.

As a prerequisite, the steps described under **Getting the BIOS Update File from LVFS, Configuring the BIOS Update**, and **Providing the BIOS Update File** must be completed. As an alternative, you can also use a USB storage device (see Storage Hotplug[53]) or an NFS network drive (see NFS[54]).

When the command has been executed, a dialog informs you that a reboot is required. You can choose between two options:
- Perform the reboot and update right away
- Postpone the update to the next reboot

Usage

```
bios-tools [OPTIONS] COMMAND [ARGS]...
```

Options

Option / Contrary Option	Comment
`--debug / --no-debug`	Provide extensive information (verbose mode)
`--help`	Show the help text and exit

Commands

Command	Argument (Short / Long Form)	Comment
`update`		Handle BIOS update
	`-e --enable`	Enable BIOS update. Will be triggered after reboot.
	`-d --disable`	Disable BIOS update
	`-s --show`	Show if BIOS update is enabled or not
	`--help`	Show the help text and exit

53. https://kb.igel.com/en/igel-os/11.10.250/storage-hotplug
54. https://kb.igel.com/en/igel-os/11.10.250/nfs

Example

The following command performs a BIOS update and displays extensive information:

```
update --debug -e
```

BIOS Tools for Supported HP Devices

With the BIOS tools, you can manage and update the BIOS of specific Hewlett-Packard (HP) devices using the IGEL Universal Management Suite (UMS).

We will use profiles and specific device commands to handle any number of devices simultaneously.

BIOS Updates at Your Own Risk
IGEL is offering and supporting the BIOS Update mechanism - BIOS updates are performed at your own risk!

The BIOS update mechanism is functional even with Secure Boot enabled and when a BIOS password is set.

Supported Devices

BIOS tools are only supported for the models listed here.

From OS version 11.10.150:

- HP Pro mt440 G3
- HP Elite mt645 G7
- HP Elite mt645

From OS version 11.08.330:

- HP t540
- HP t640

From OS version 11.09.150:

- HP t430
- HP Pro t550
- HP Elite t655
- HP t740

From OS version 11.09.260:

- HP Elite t755

Requirements

- UMS 6.10 or higher
- Supported devices with IGEL OS 11.08.330 or higher

The IGEL OS needs to be installed directly on the device. BIOS tools are not supported if the IGEL OS boots from a UD Pocket.

- A Windows machine for creating the password file

Setting up the File Source

Since not only updating the BIOS but also its configuration is done using files, we need to set up a file source that is reachable by all devices.

The creation of the files is described in the relevant sections. The procedures described here are the same for all files in question, that is:

- BIOS update file
- BIOS settings file
- BIOS password file

Security Note

If you use password files, make sure that the password file is not accessible longer than necessary.

Using an External Source (HTTP/HTTPS)

If you want to deploy the BIOS update file, the BIOS settings file, and the password file from an external source, you can set up an HTTP/HTTPS server.

You can secure the file access using a username and password. The devices can be configured to provide a username and password; see If the External File Source Has Password Protection (see page 358).

Using a Local Storage Device (USB)

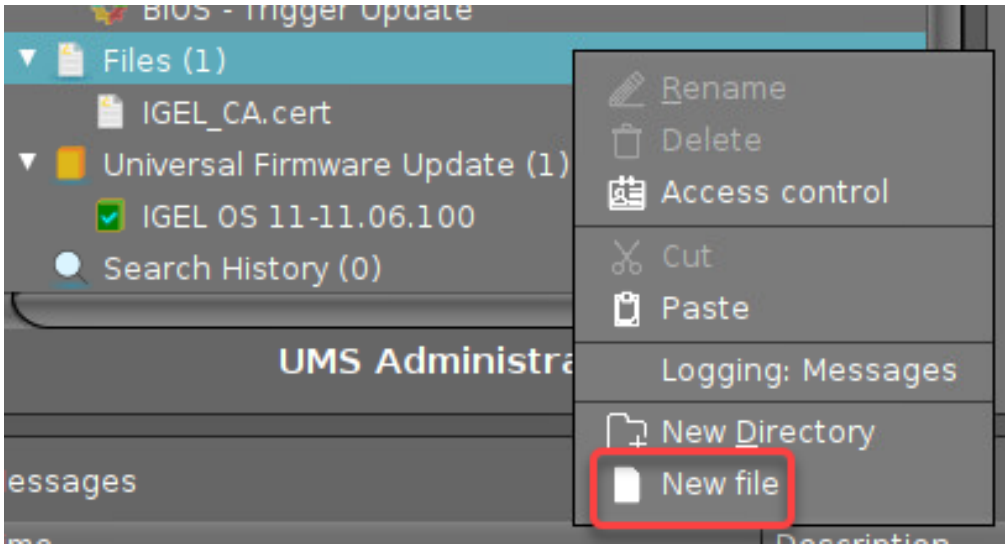
For more information on how to use a storage device with IGEL OS, see Storage Hotplug (see page 1969).

Using UMS File Transfer

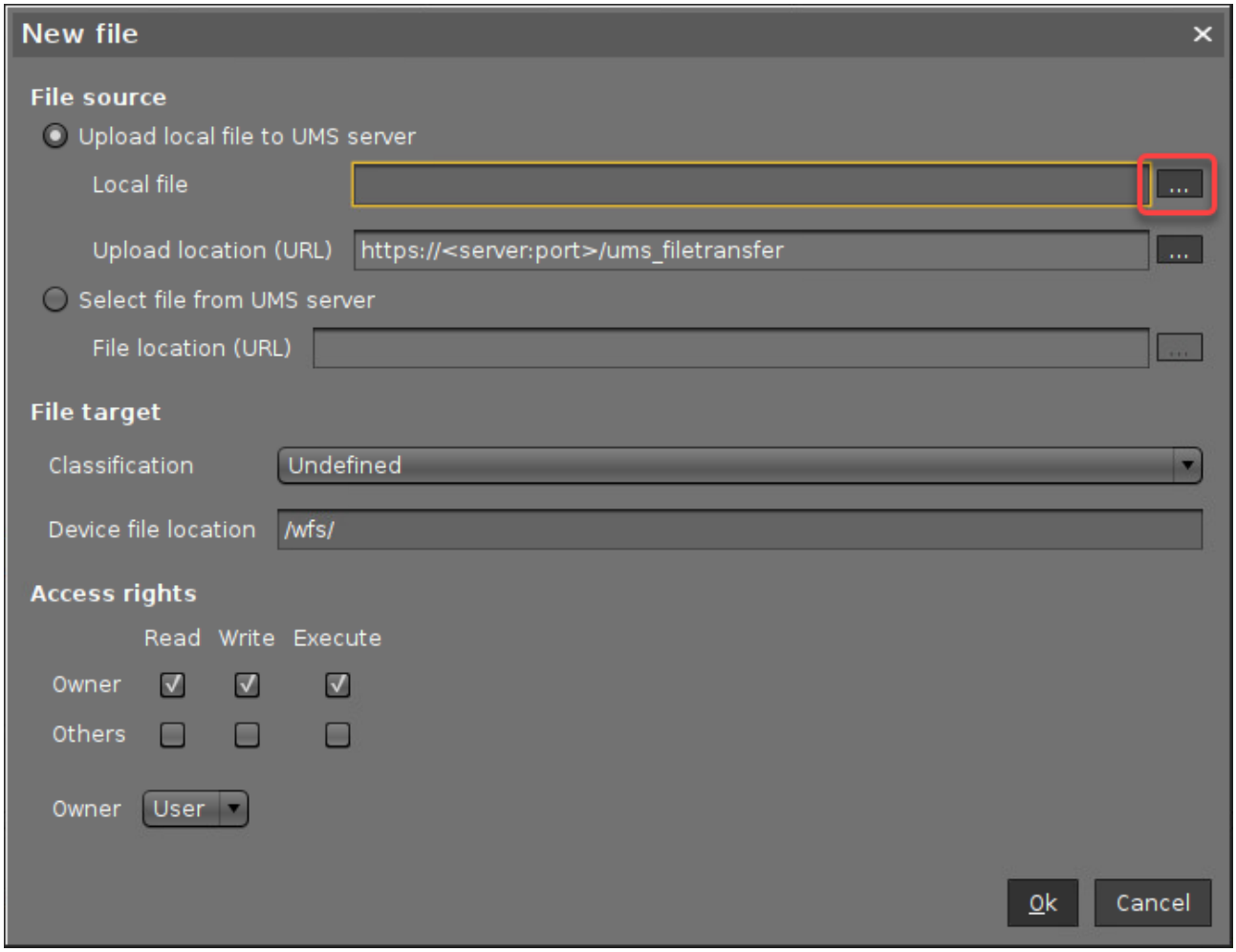
The following example shows how to use the UMS file transfer facility for file deployment. In this example, a BIOS update file is provided; the procedure is the same for settings and password files.

1. Create a profile as described in Enabling the BIOS Tool (see page 354). You will use this profile to assign the file to the devices.

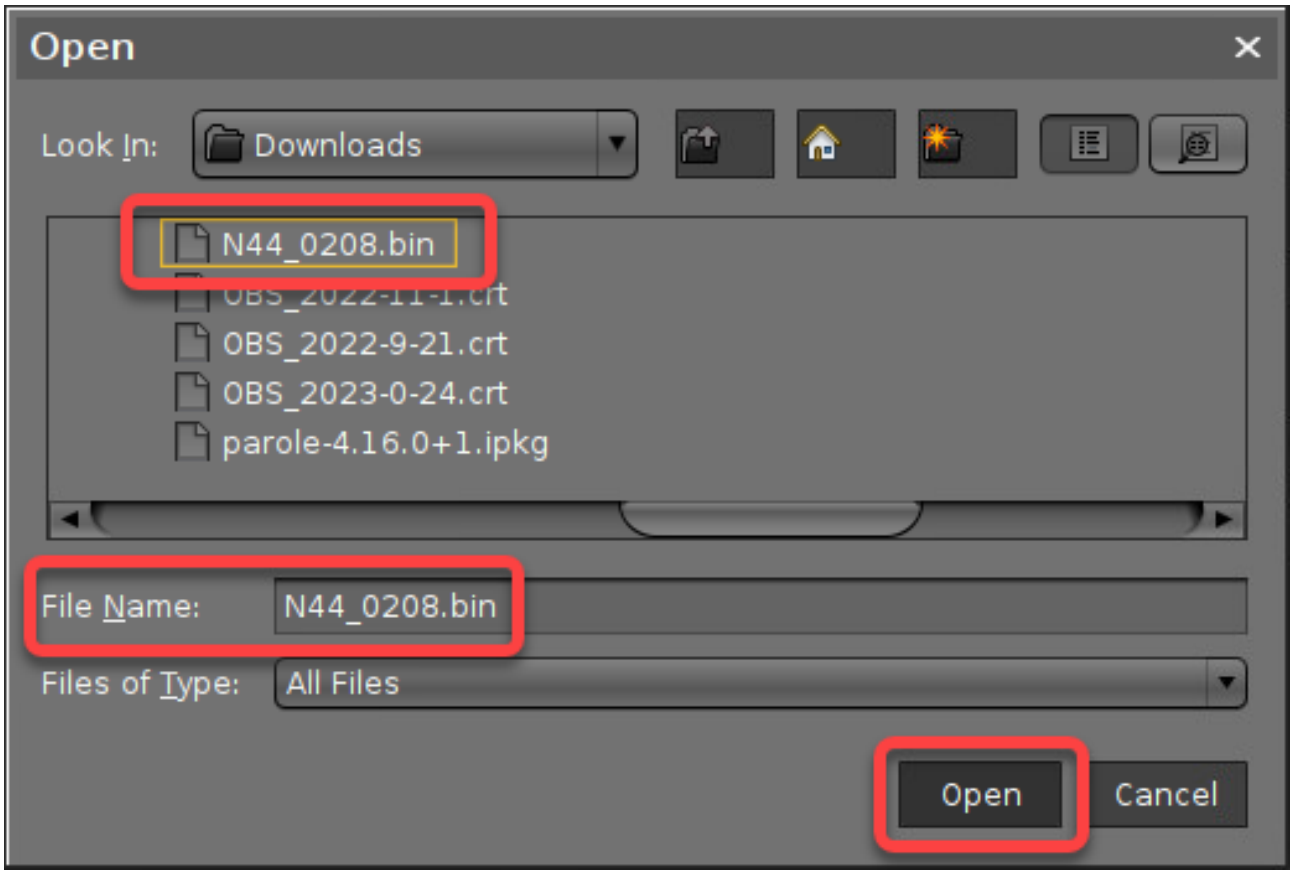
2. In the UMS Console, go to **Files**, open the context menu, and select **New file**.



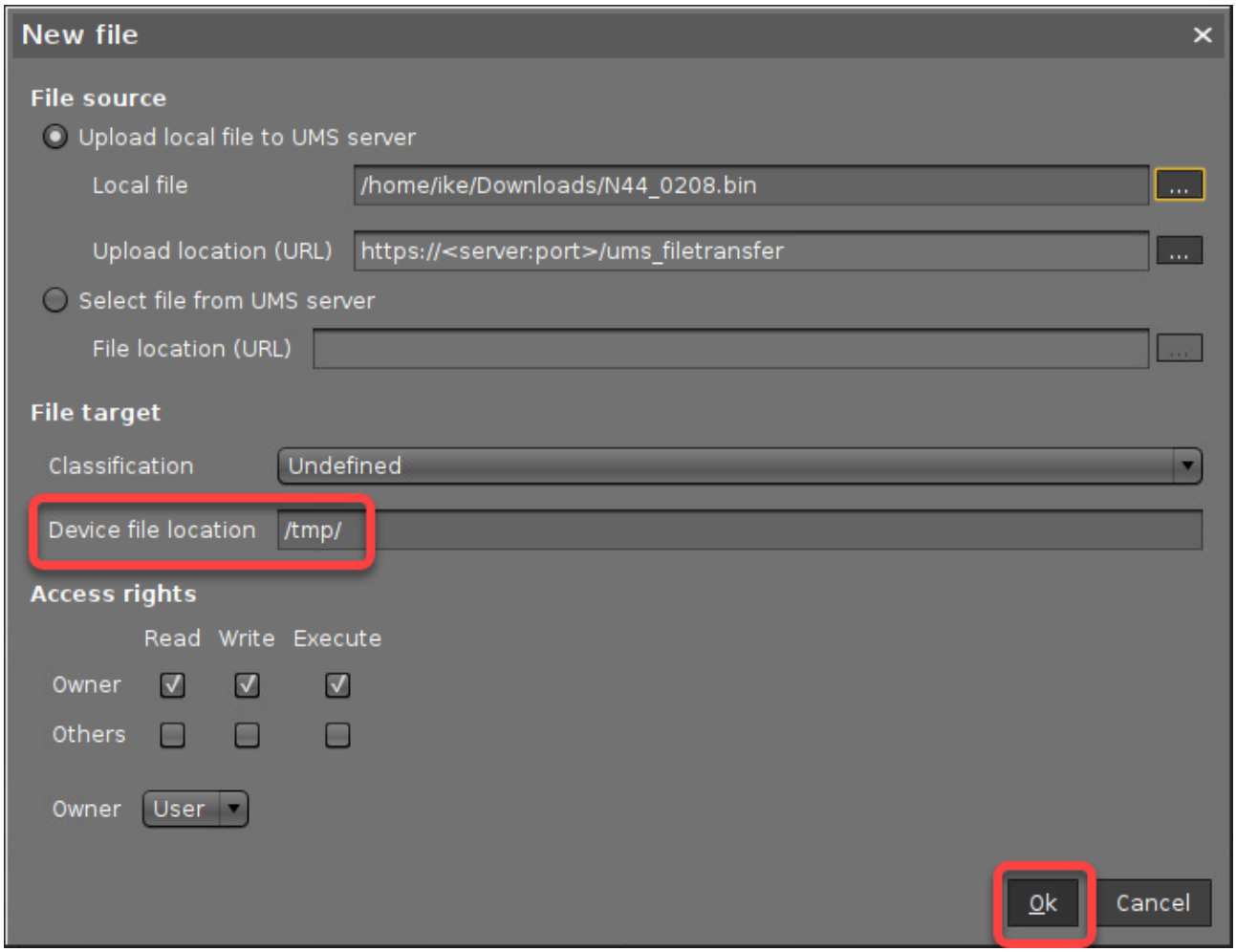
3. Click the file chooser button.



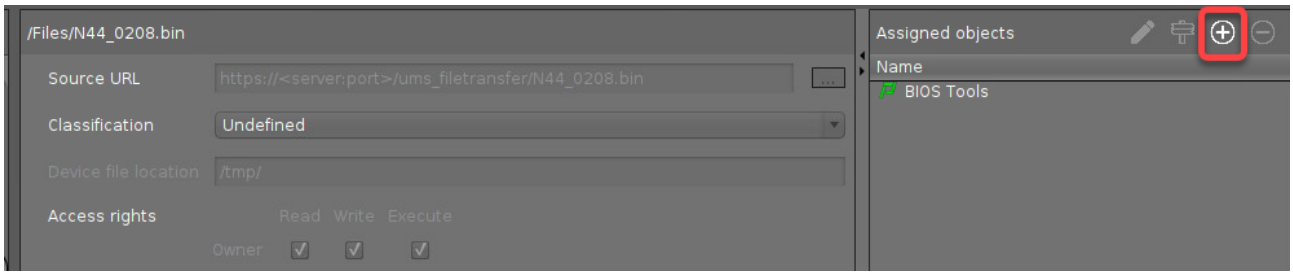
4. Find the BIOS update file in your file system, select it, and click **Open**.

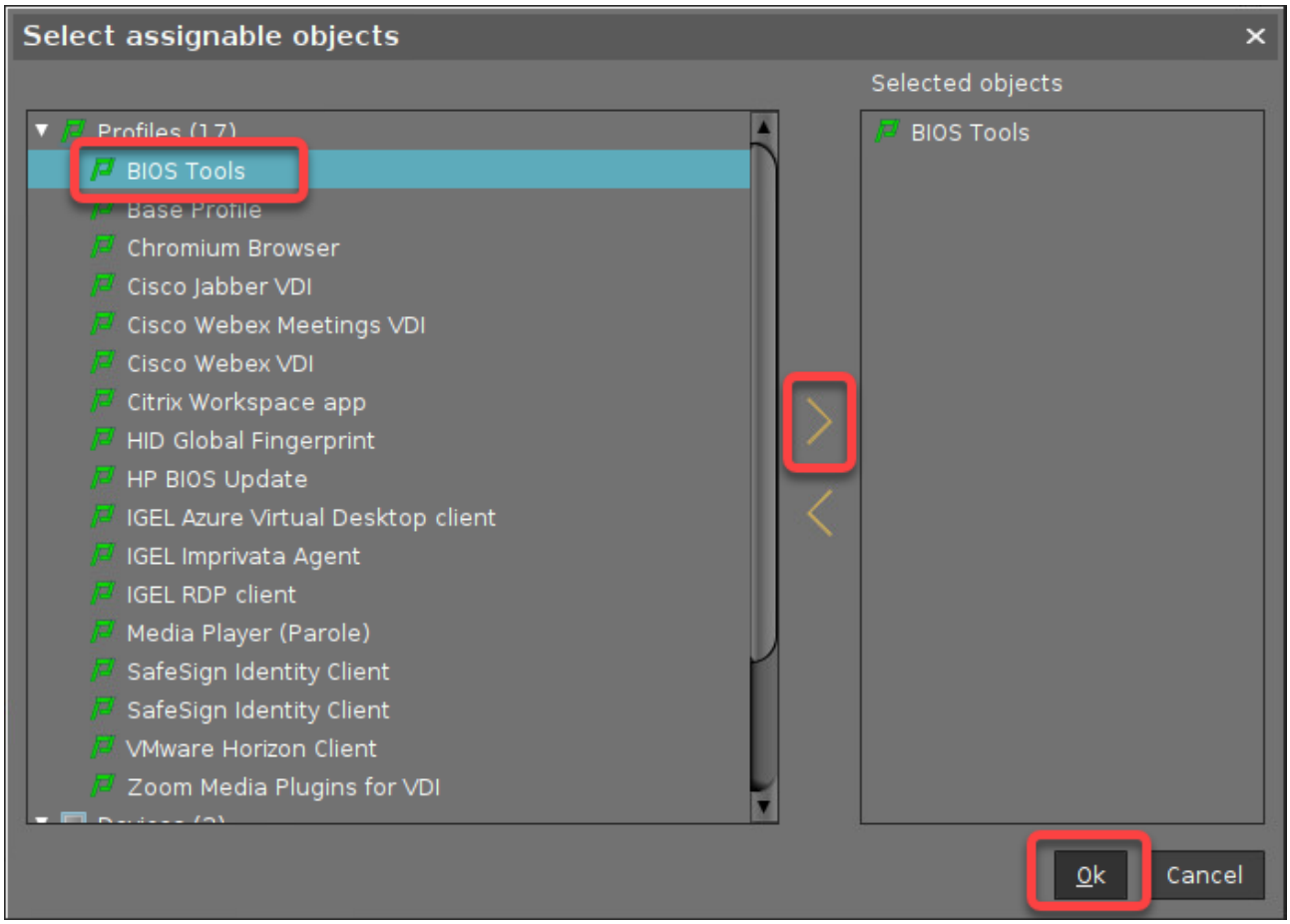


5. In the field **Device file location**, define the local path in which the file will be stored on the device, e.g. `/tmp/`. Afterward, click **Ok**.



6. Assign the file to your devices by assigning it to the profile we have created beforehand.





Configuring the Devices

This section describes the necessary preparations for each use case.

First of all, the BIOS Tool feature must be enabled and installed.

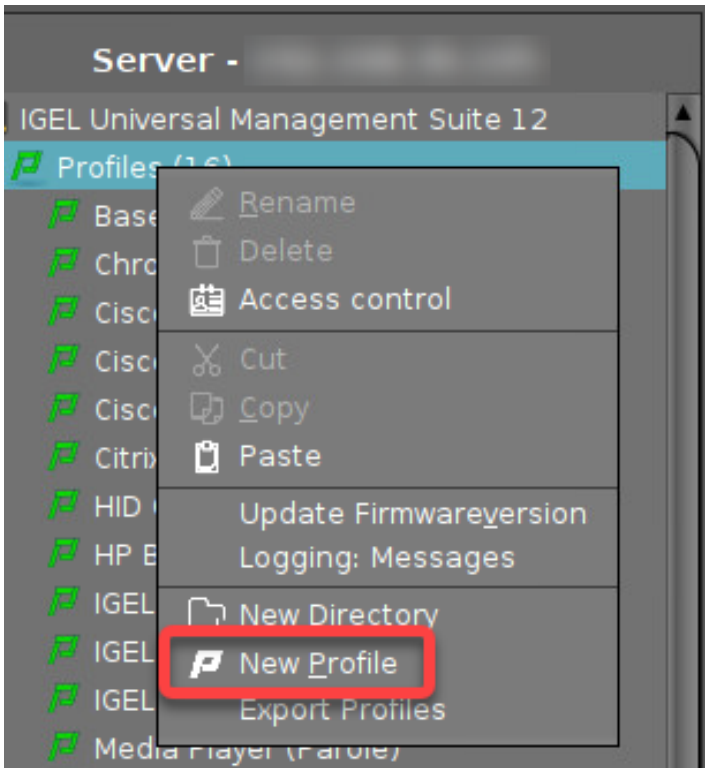
Then, depending on the use case, specific parameters must be set and files must be created.

The following registry parameters are currently not relevant to the procedures described here:

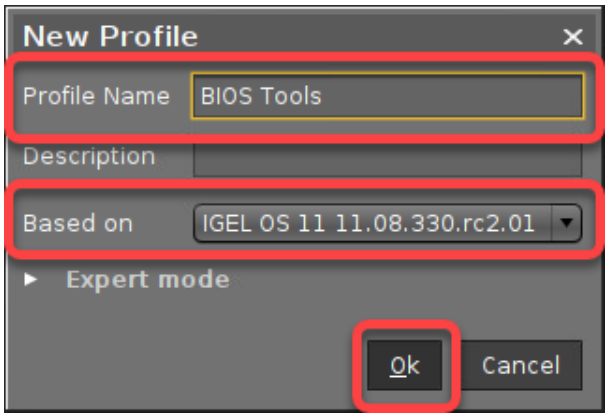
- `fwtools.bios_tools.allow_downgrade`
- `fwtools.bios_tools.allow_only_trusted`
- `fwtools.bios_tools.allow_reinstall`

Enabling the BIOS Tool

1. In the UMS Console, go to **Profiles**, open the context menu, and select **New Profile**.

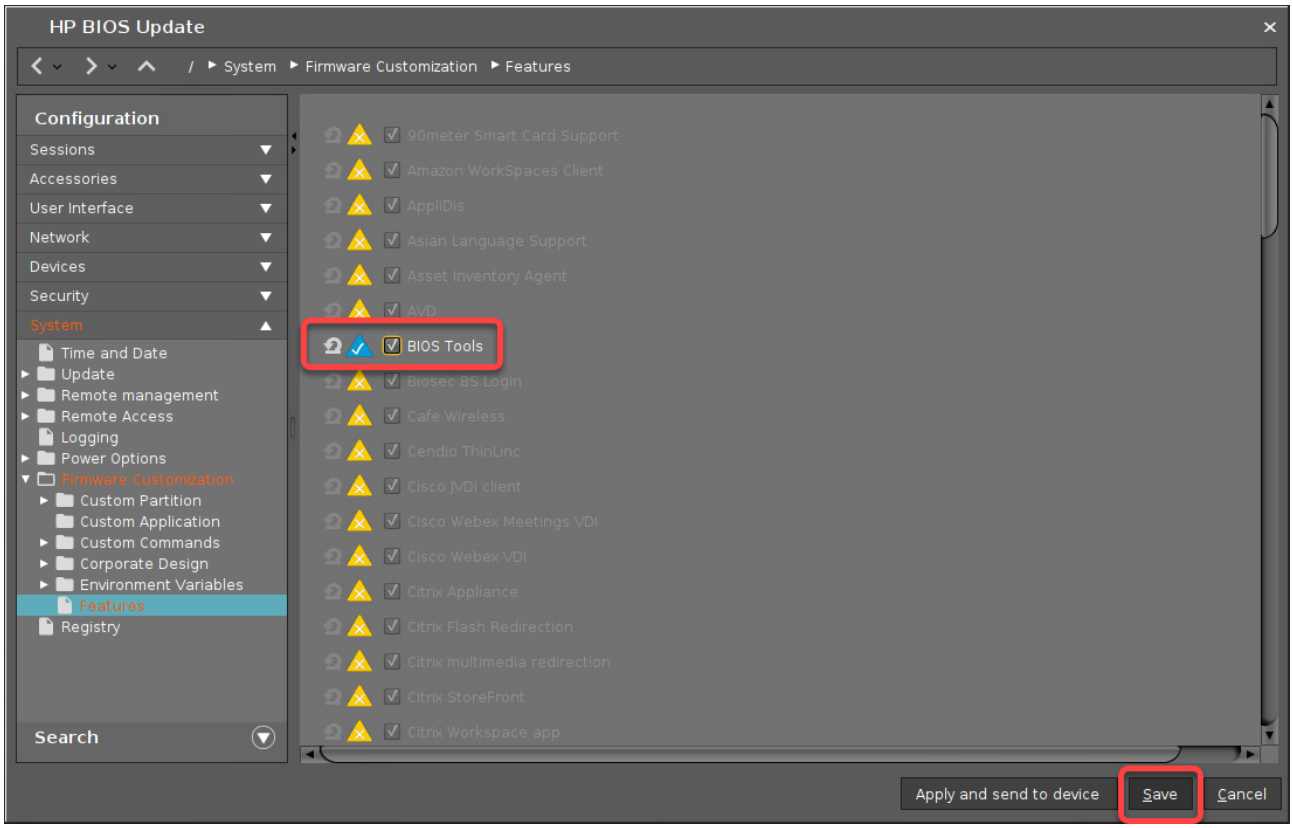


2. Provide the following data and then click **Ok**.
    - **Profile Name**: Display name of the profile
    - **Based on:** Select the IGEL OS version of the devices; must be IGEL OS 11.08.330 or higher.

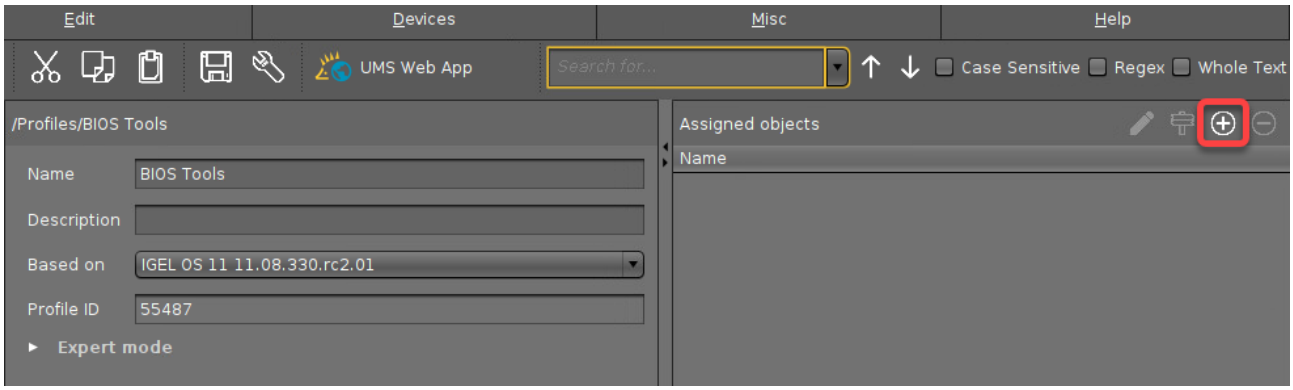


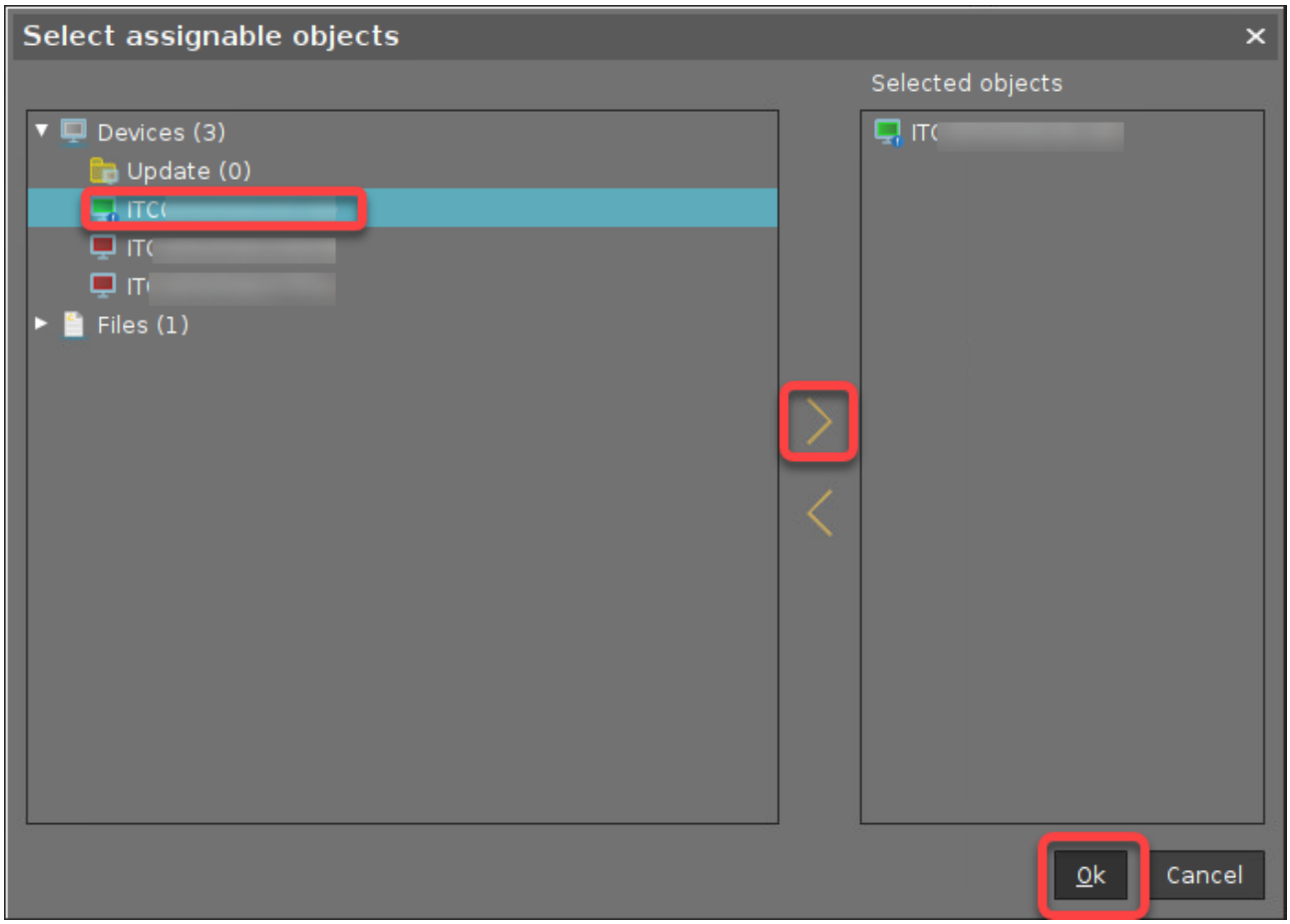
3. Make sure that the settings under **System > Update > Firmware Update** are valid since the device will use this source for installing the BIOS Tools.

4. Go to **System > Firmware Customization > Features**, find **BIOS Tools**, click the yellow icon next to the parameter (turns blue when active), enable it, and save the profile.

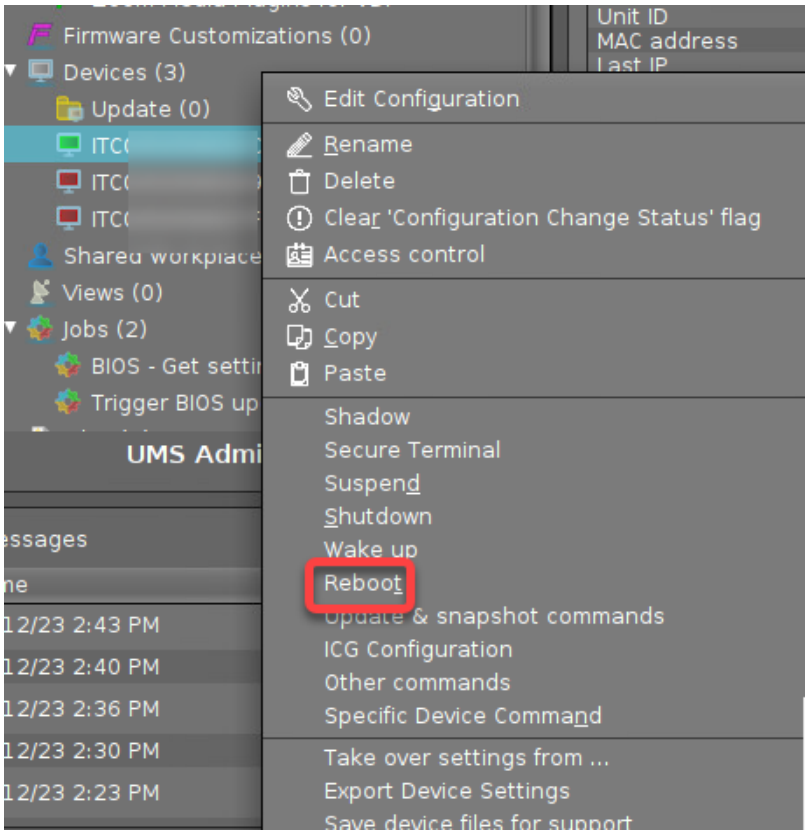


5. Assign the profile to the devices in question.





6. Reboot the device.

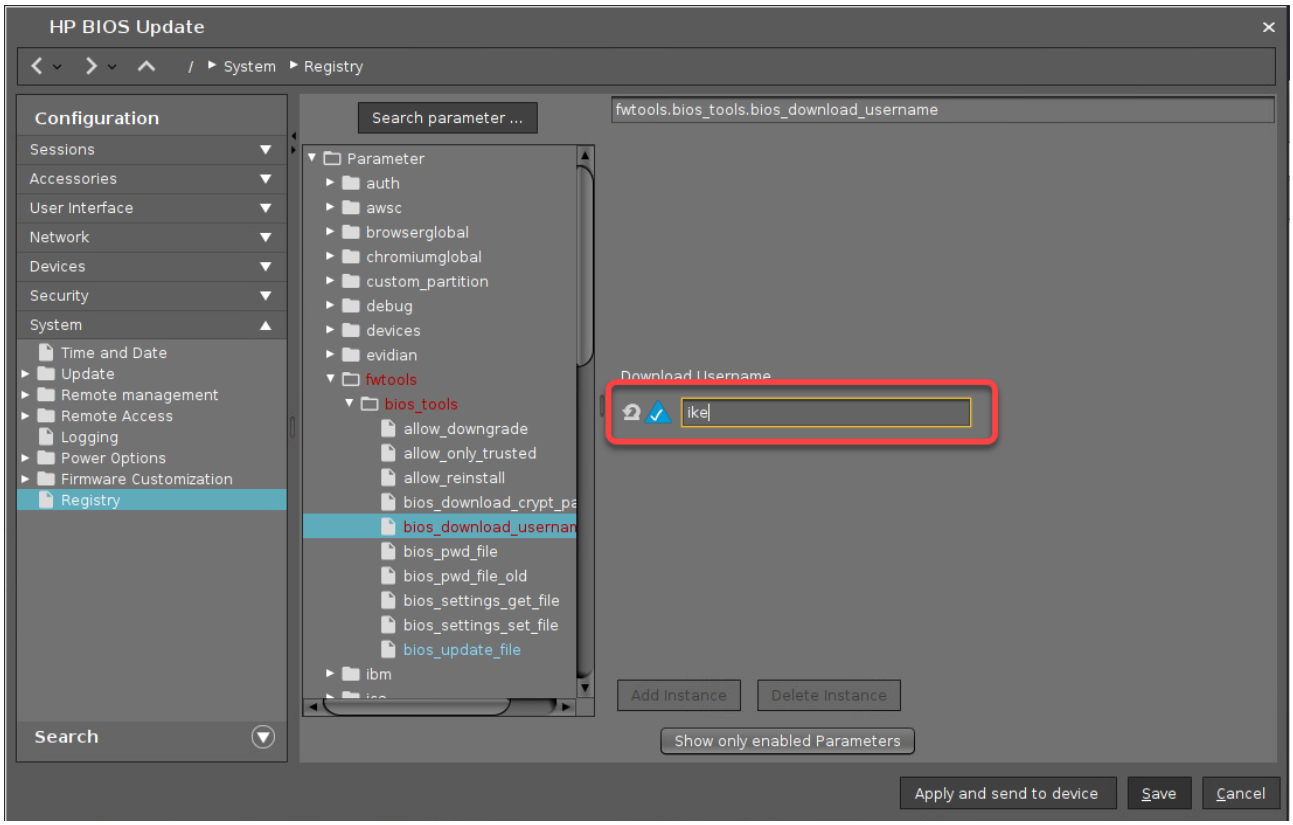


After the reboot, the BIOS Tools are available.

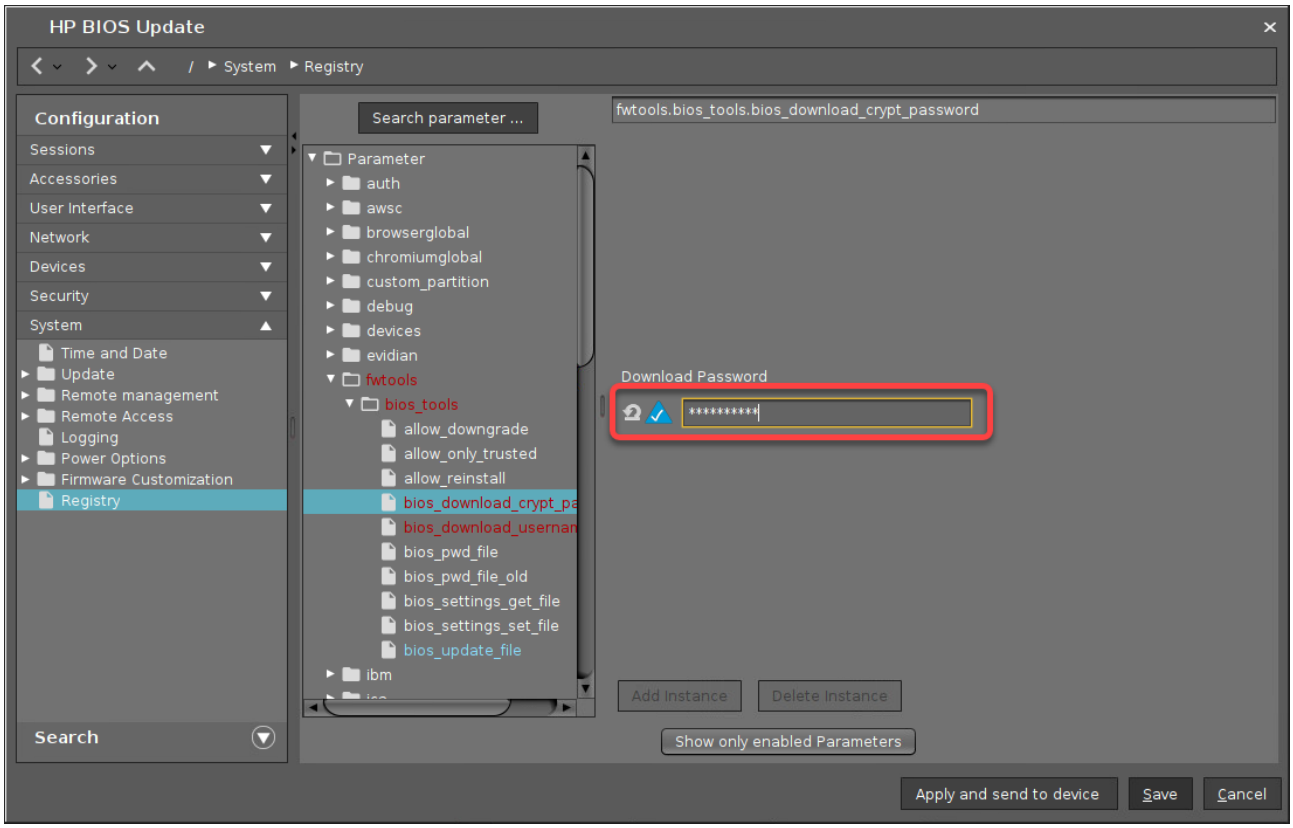
If the External File Source Has Password Protection

If your external source for the BIOS update file, the BIOS settings file, or the BIOS password file has password protection, edit the configuration as follows:

1. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_download_username**, click the yellow icon to activate the parameter (turns blue when active), and enter the username.



2. Go to **System > Registry > fwtools > bios_tools > bios_download_crypt_password**, click the yellow icon to activate the parameter (turns blue when active), and enter the password.



If Your BIOS is Password-Protected: Provide BIOS Password File to Make Changes

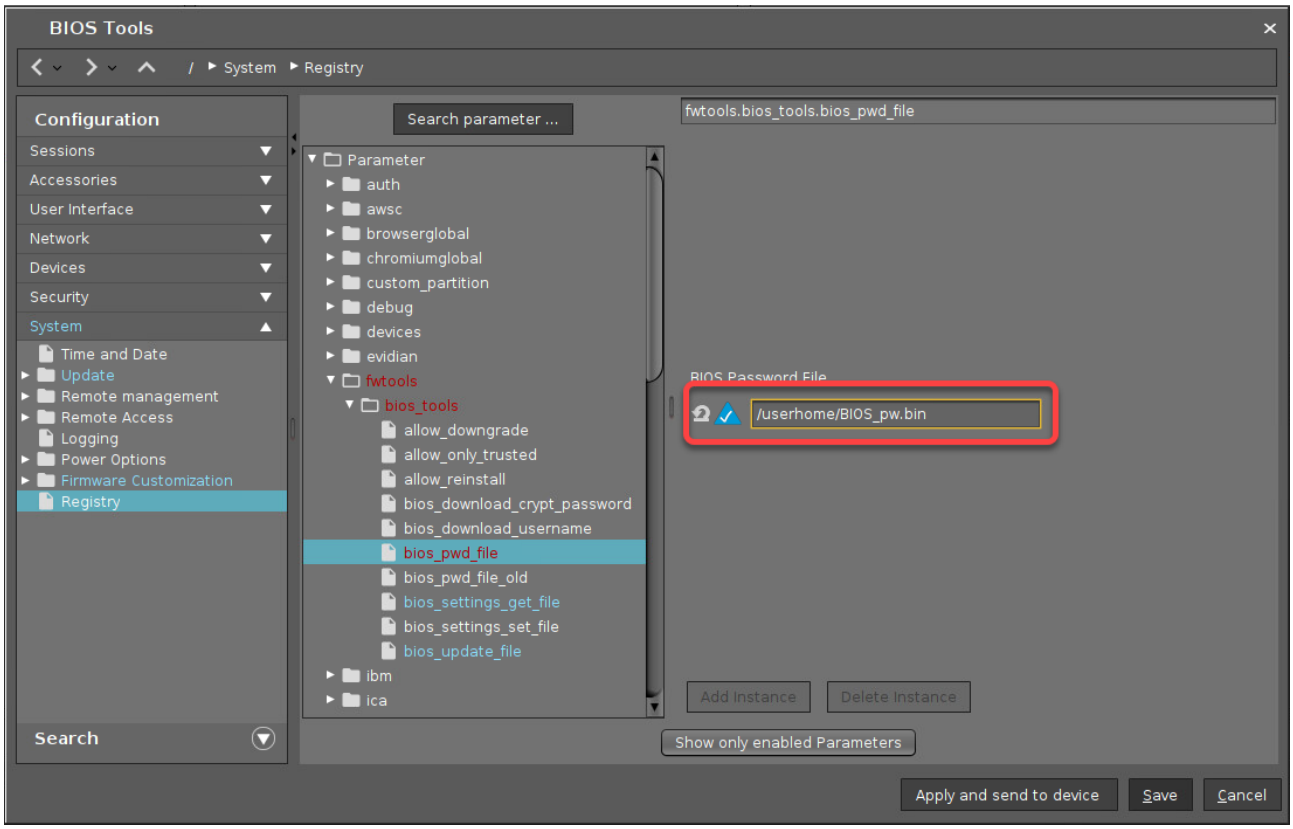
If your BIOS is protected by a password, a valid password file must be provided in order to allow any kind of changes to the BIOS. For this purpose, you must create a password file and make it available to the device.

As a precondition, you must of course know the BIOS password of your devices.

1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

2. Create a password file with the known password and make it available as described under Setting up the File Source (see page 350).

3. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_pwd_file** , click the yellow icon to activate the parameter (turns blue when active), and enter the local or remote file path.



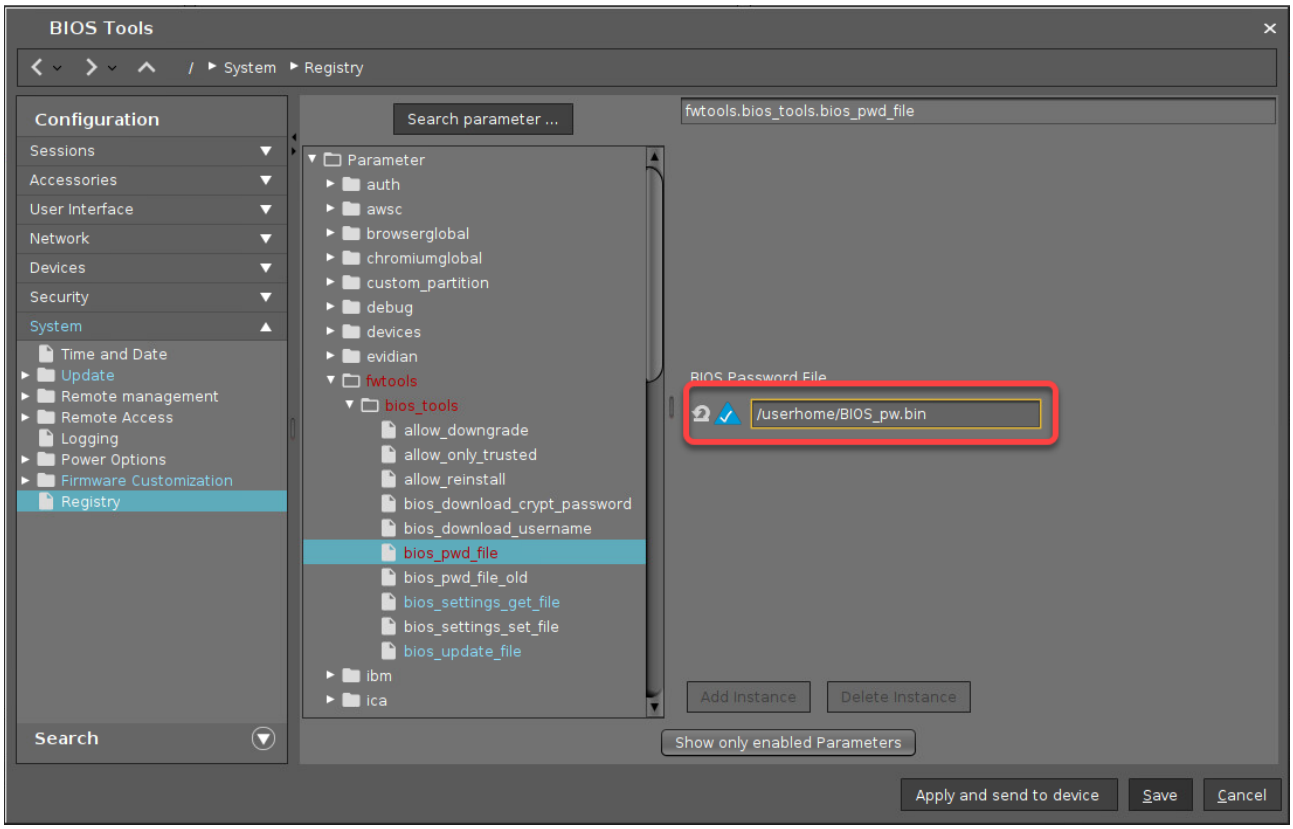
Set a BIOS Password to Protect Your BIOS

If your BIOS is not protected by a password yet and you want to secure it with a BIOS password, proceed as follows:

1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

2. Create a password file with the new password and make it available as described under Setting up the File Source (see page 350).

3. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_pwd_file** , click the yellow icon to activate the parameter (turns blue when active), and enter the local or remote file path.



4. Save your settings. Afterward, you can continue with Setting a BIOS Password.

Change the BIOS Password

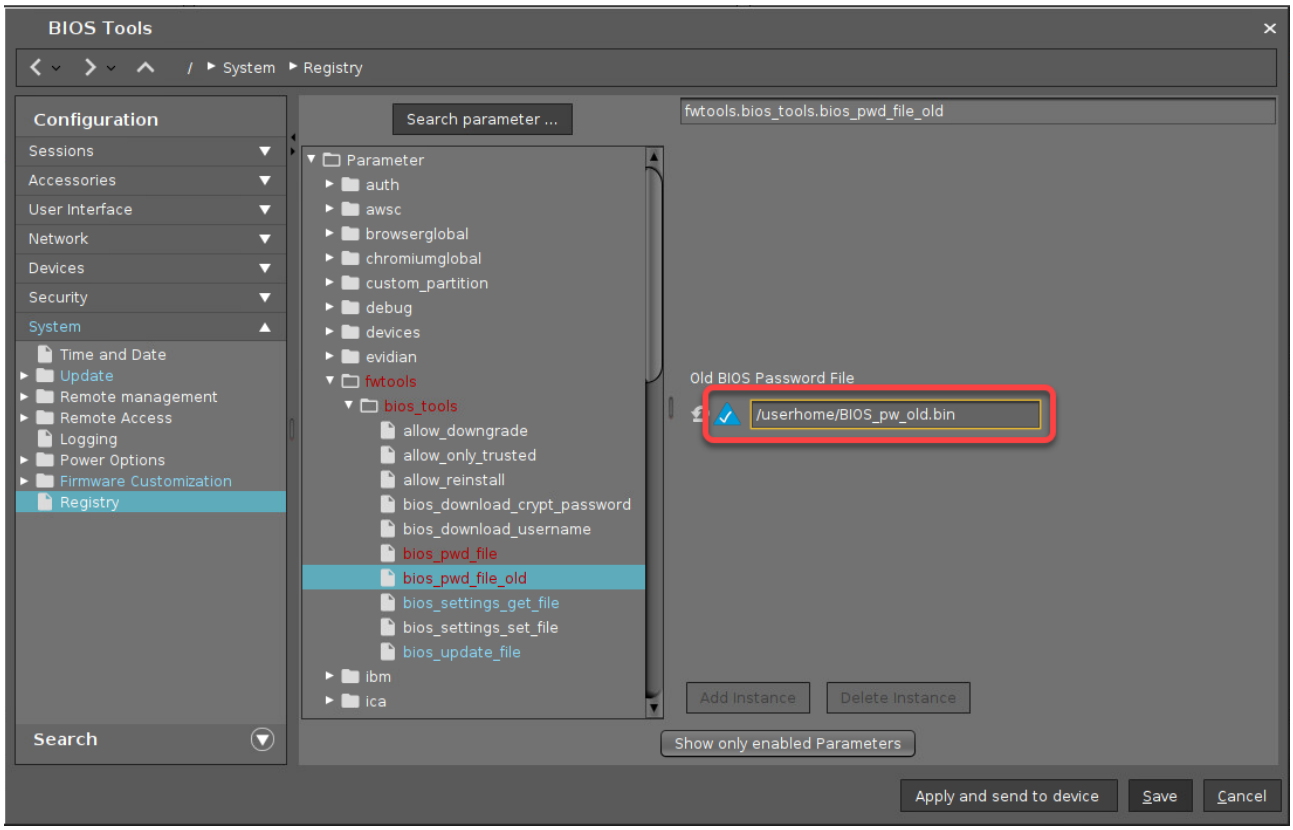
If your devices already have a BIOS password and you want to change it, proceed as follows:

1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

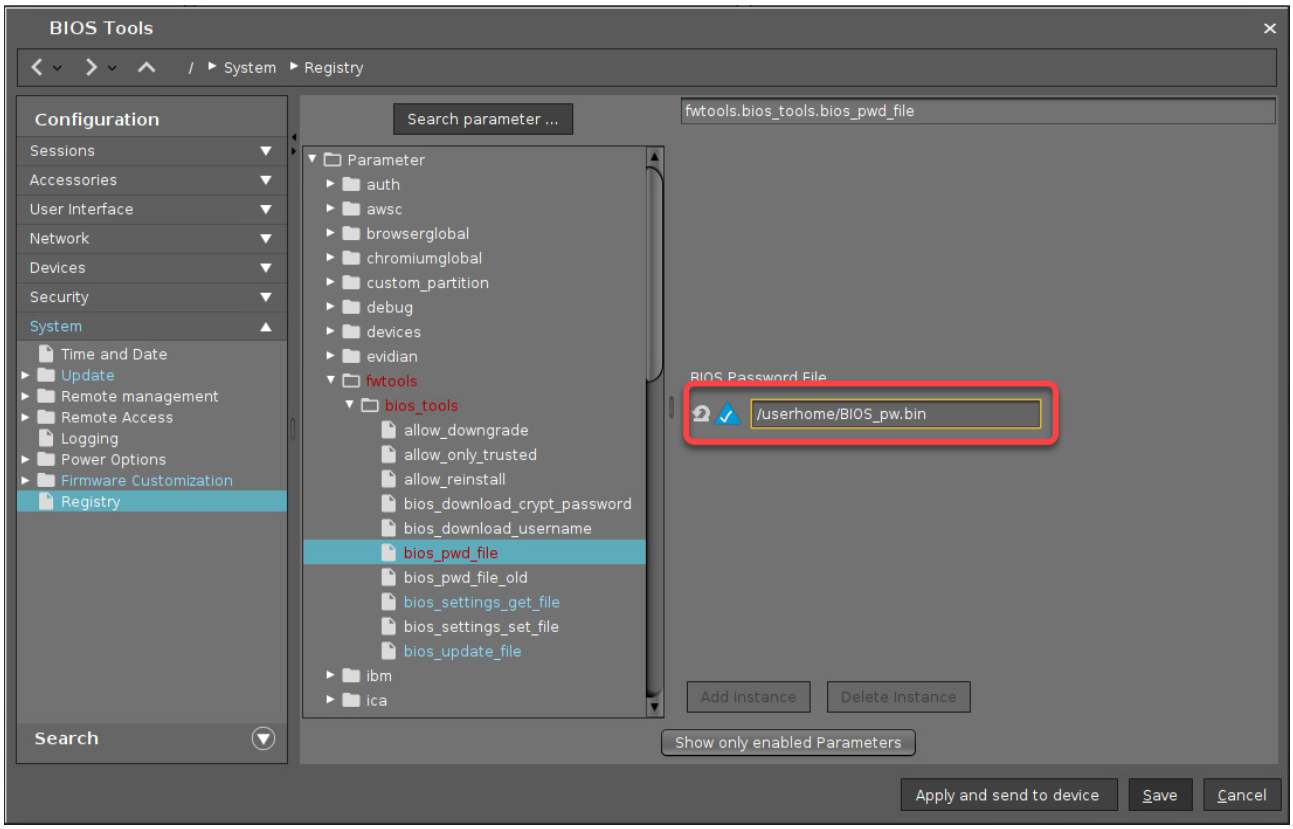
2. Create a password file with the current password and make it available as described under Setting up the File Source (see page 350).

3. Create a password file with the new password and make it available as described under Setting up the File Source (see page 350).

4. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_pwd_file_old**, click the yellow icon to activate the parameter (turns blue when active), and enter the local or remote file path of the password file with the current password.



5. Go to **System > Registry > fwtools > bios_tools > bios_pwd_file**, click the yellow icon to activate the parameter (turns blue when active), and enter the local or remote file path of the password file with the new password.



6. Save your settings. Afterward, you can continue with Changing the BIOS Password (see page 383).

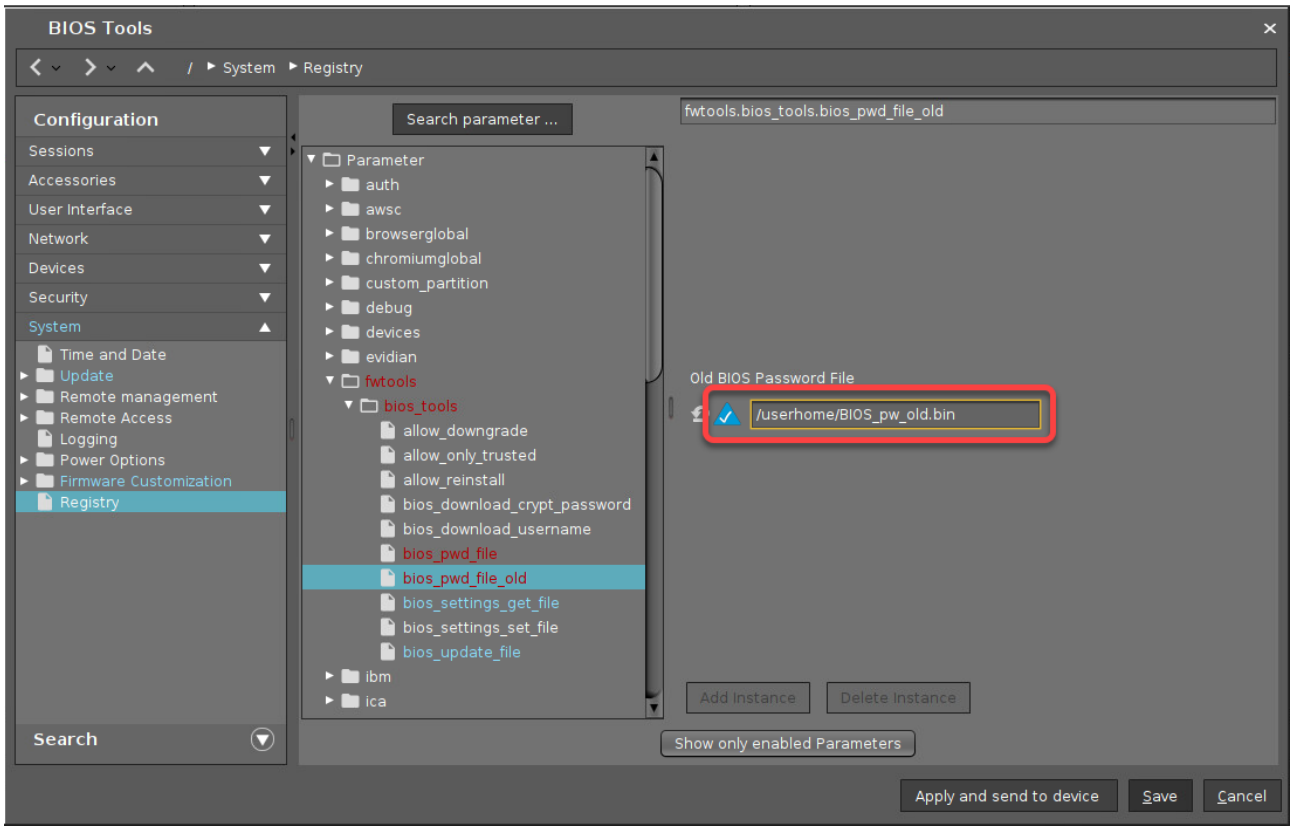
Reset the BIOS Password (Remove Password Protection)

If your devices have a BIOS password and you want to reset it so that the BIOS will be accessible without a password, proceed as follows:

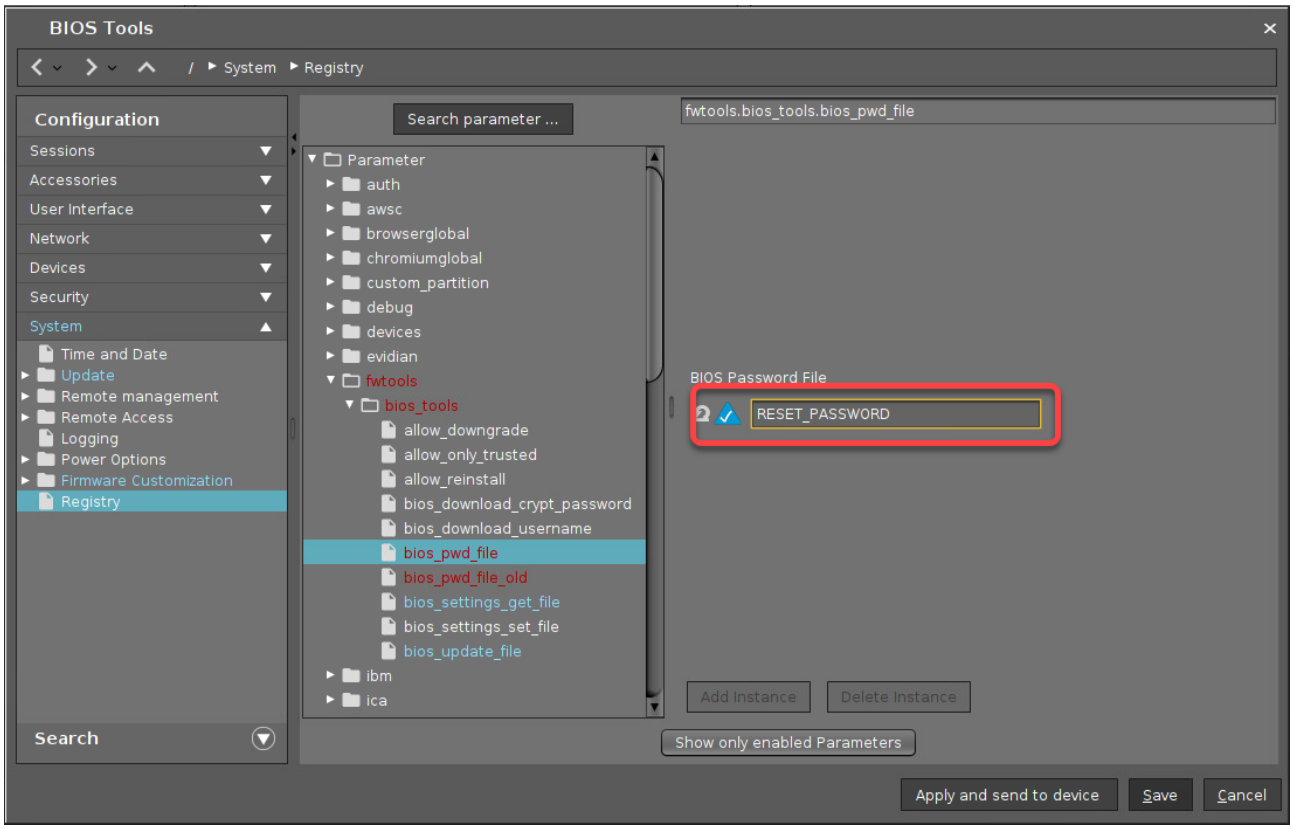
1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

2. Create a password file with the old password and make it available as described under Setting up the File Source (see page 350).

3. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_pwd_file_old** , click the yellow icon to activate the parameter (turns blue when active), and enter the local or remote file path of the password file with the current password.



4. Go to **System > Registry > fwtools > bios_tools > bios_pwd_file**, click the yellow icon to activate the parameter (turns blue when active), and enter `RESET_PASSWORD`

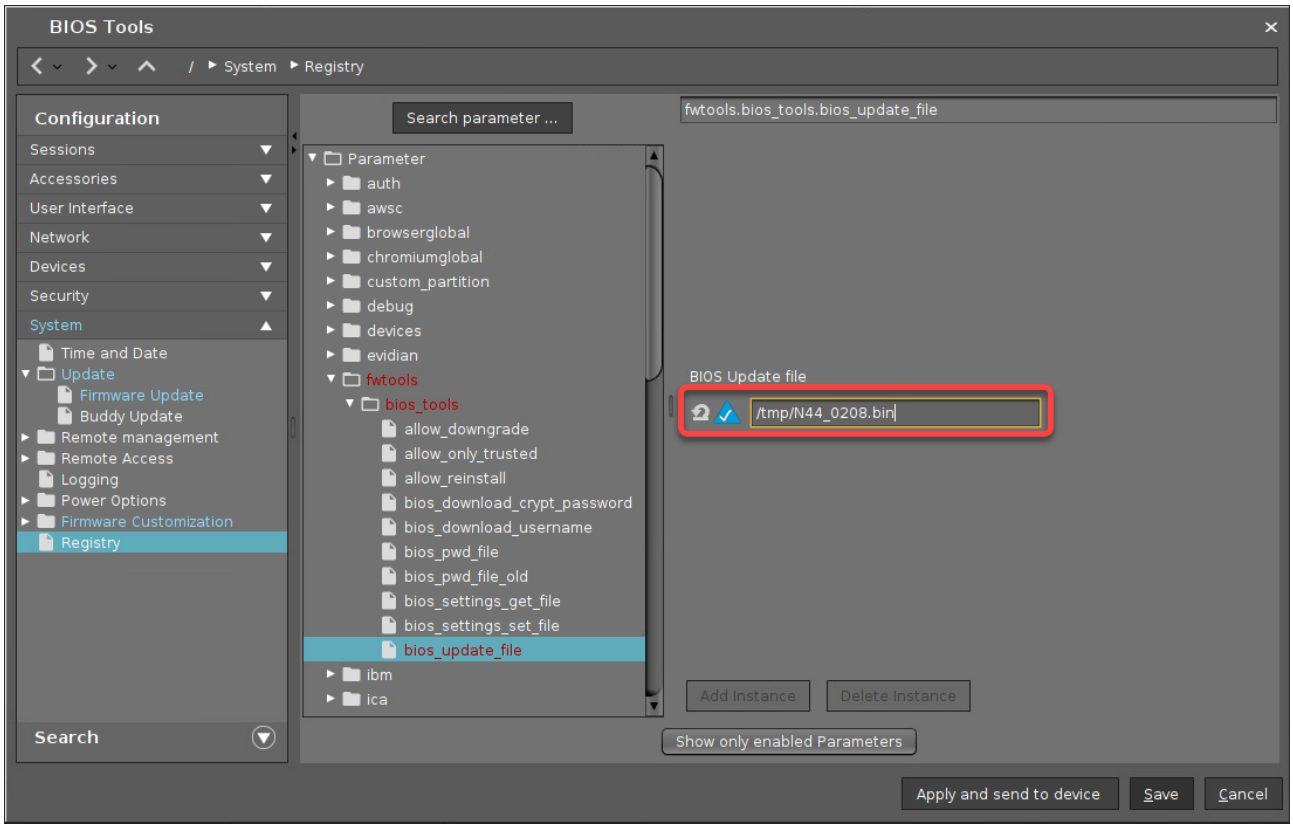


5. Save your settings. Afterward, you can continue with Resetting the BIOS Password (Removing Password Protection).

BIOS Update

> ⚠ You can replace the current BIOS with a higher version, but not with the same version. Therefore, restoring the original BIOS that had been installed on the device before is not possible.
> Moreover, it is not possible to downgrade the BIOS.

1. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_update_file** , click the yellow icon (turns blue when active), and enter the local path or URL to the BIOS update file.



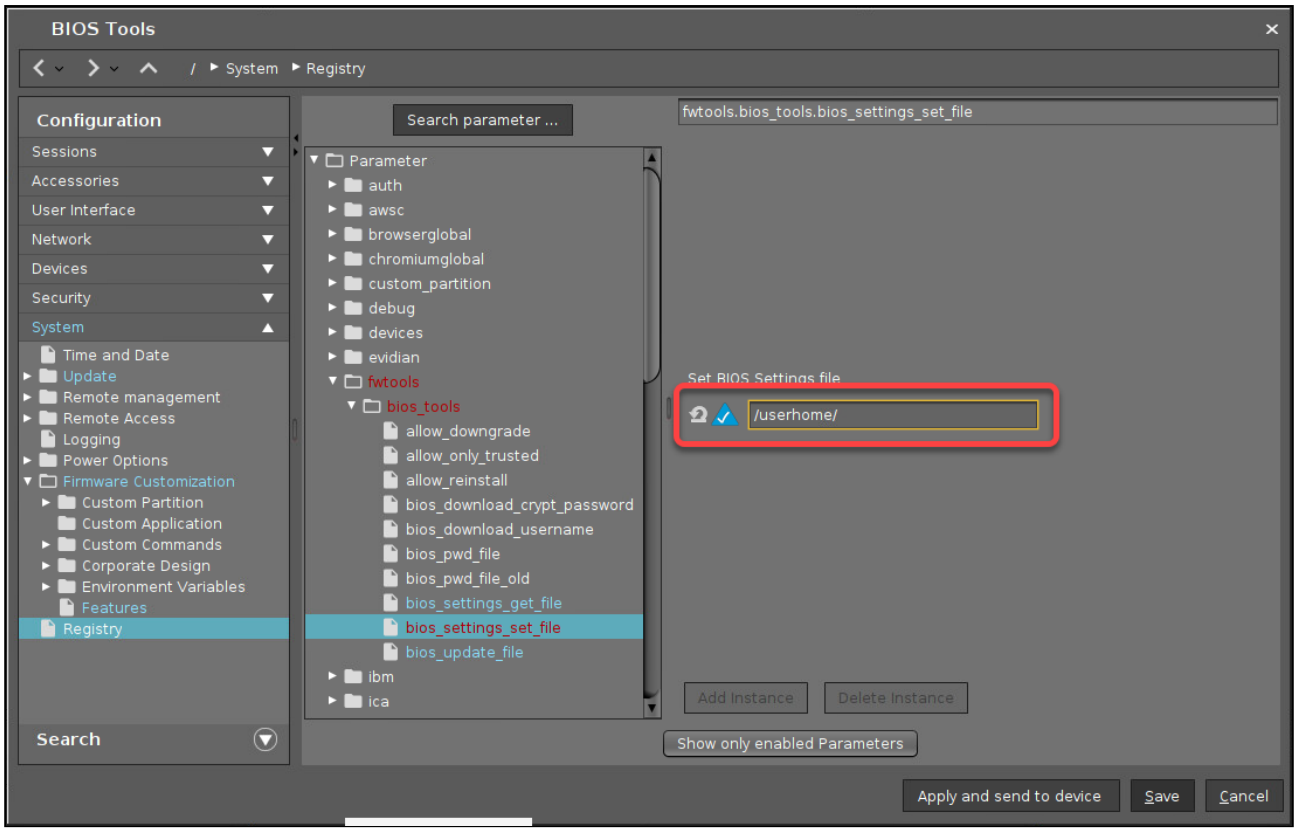
2. Save your settings. Afterward, you can continue with Updating the BIOS (see page 368).

Change the BIOS Settings

In this section, we will first define a local directory path in which the BIOS Tools facility will store the current settings as a file when it has extracted them from the device's BIOS. Then, we will define a local directory path in which the edited settings file will be stored so the BIOS tools facility can apply it to the device's BIOS.

1. In the BIOS Tools configuration profile, go to **System > Registry > fwtools > bios_tools > bios_settings_get_file** , click the yellow icon (turns blue when active), and enter the path on the device where the BIOS update file will be saved.

2. Go to **System > Registry > fwtools > bios_tools > bios_settings_set_file** , click the yellow icon (turns blue when active), and enter the directory path on the device where the settings file will be saved. The filename will be `bios_settings<unit_id>` ; example: `bios*settings*005056784DBA`



3. Save your settings. Afterward, you can continue with Changing the BIOS Settings (see page 370).

Updating the BIOS

Getting the BIOS Update File from HP

1. Open https://support.hp.com/, select your device, click **Software, Drivers and Firmware**, and follow the steps.

2. Download the file (example: `sp126570.exe`) and unzip it.

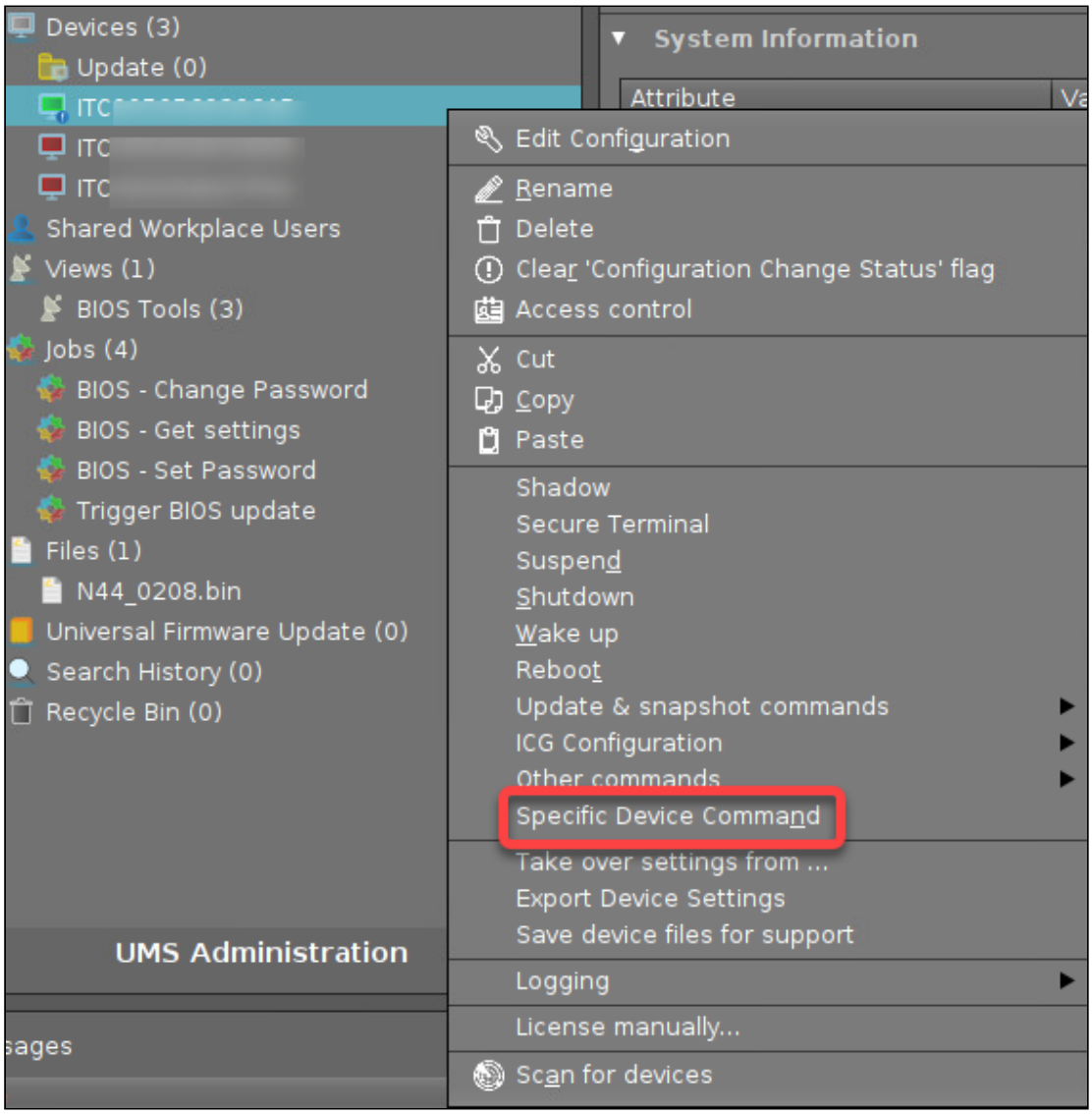
3. In the directories created by unzipping, look for a file with the ending `.bin`, for instance, `M44_0103.bin`, and store it in a location that is reachable from your UMS machine.

Making the BIOS Update File Available

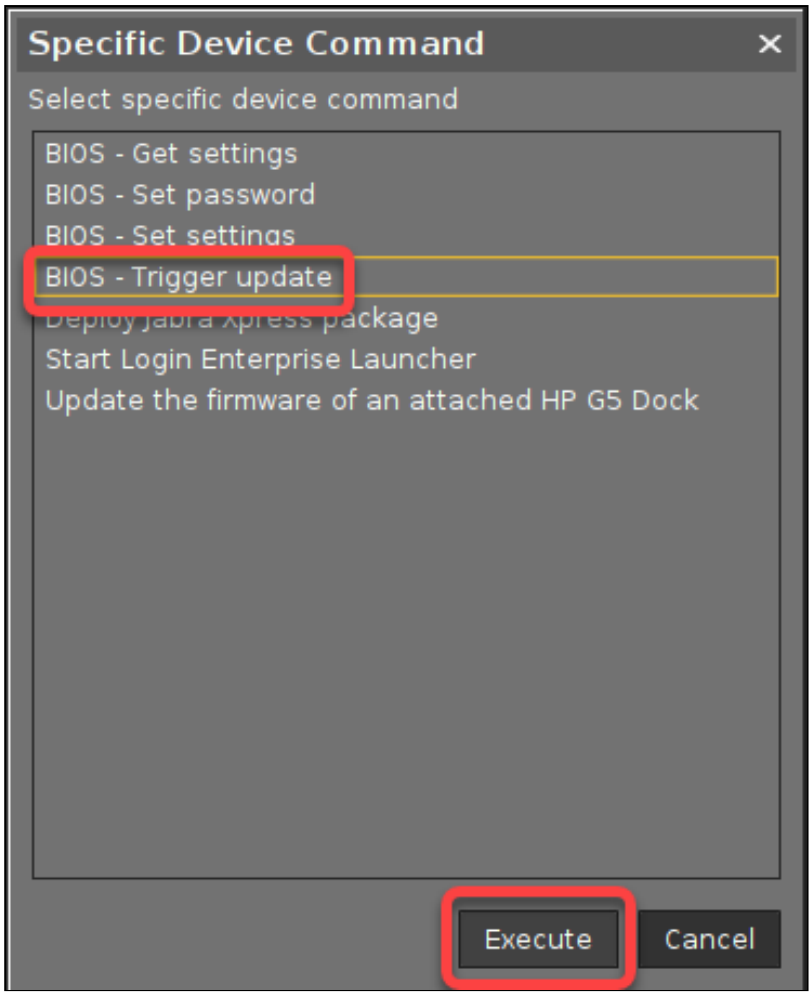
→ Make the BIOS update available to your devices; see Setting up the File Source (see page 350).

Triggering the BIOS Update

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.



2. Select **BIOS - Trigger update** and click **Execute**.

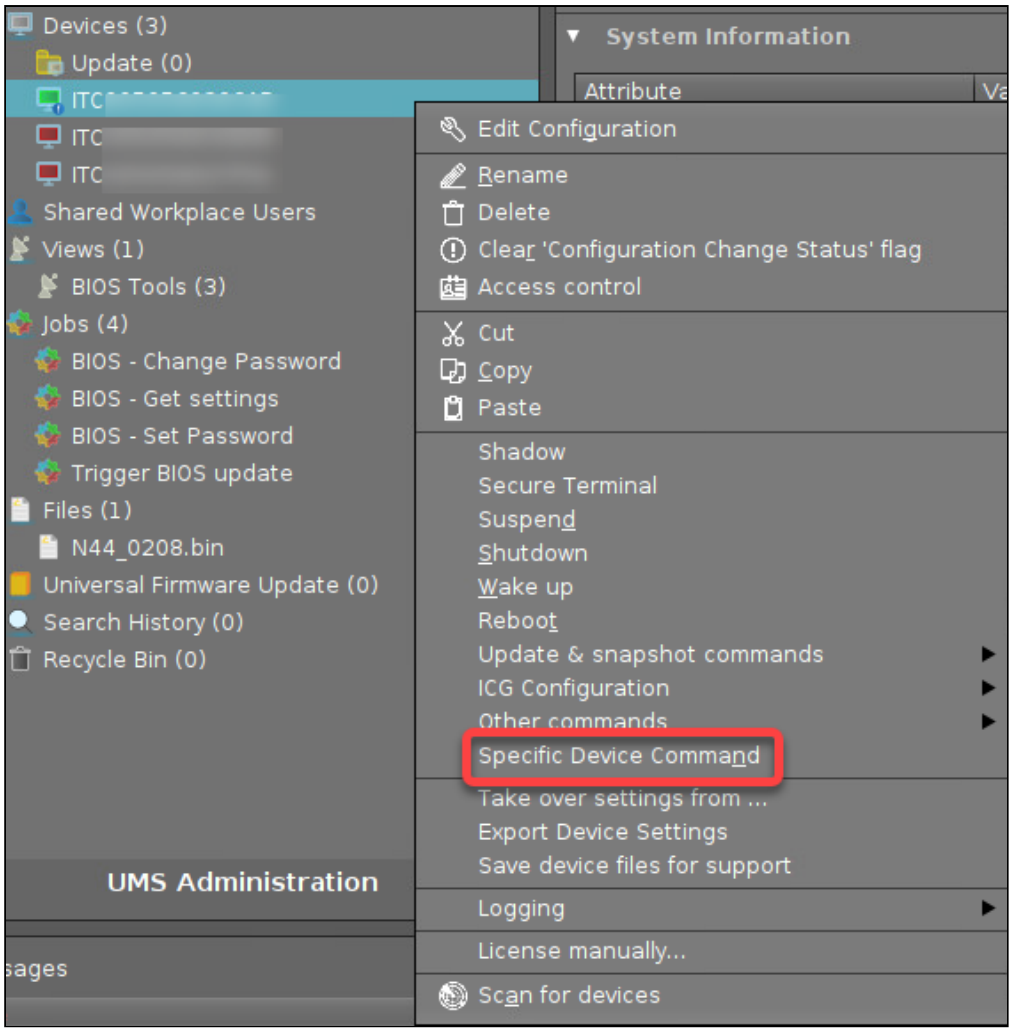


Changing the BIOS Settings

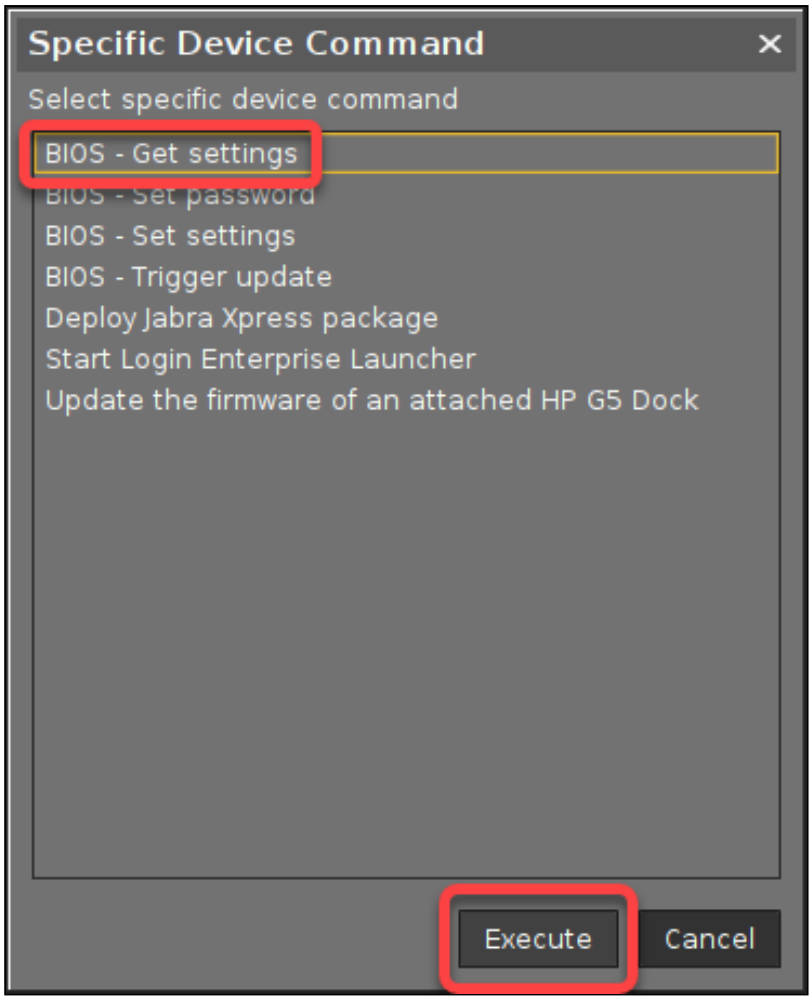
To change the BIOS configuration, you must first retrieve the BIOS settings from the device, then edit them, and finally deploy the edited settings to the device.

Getting the BIOS Settings

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

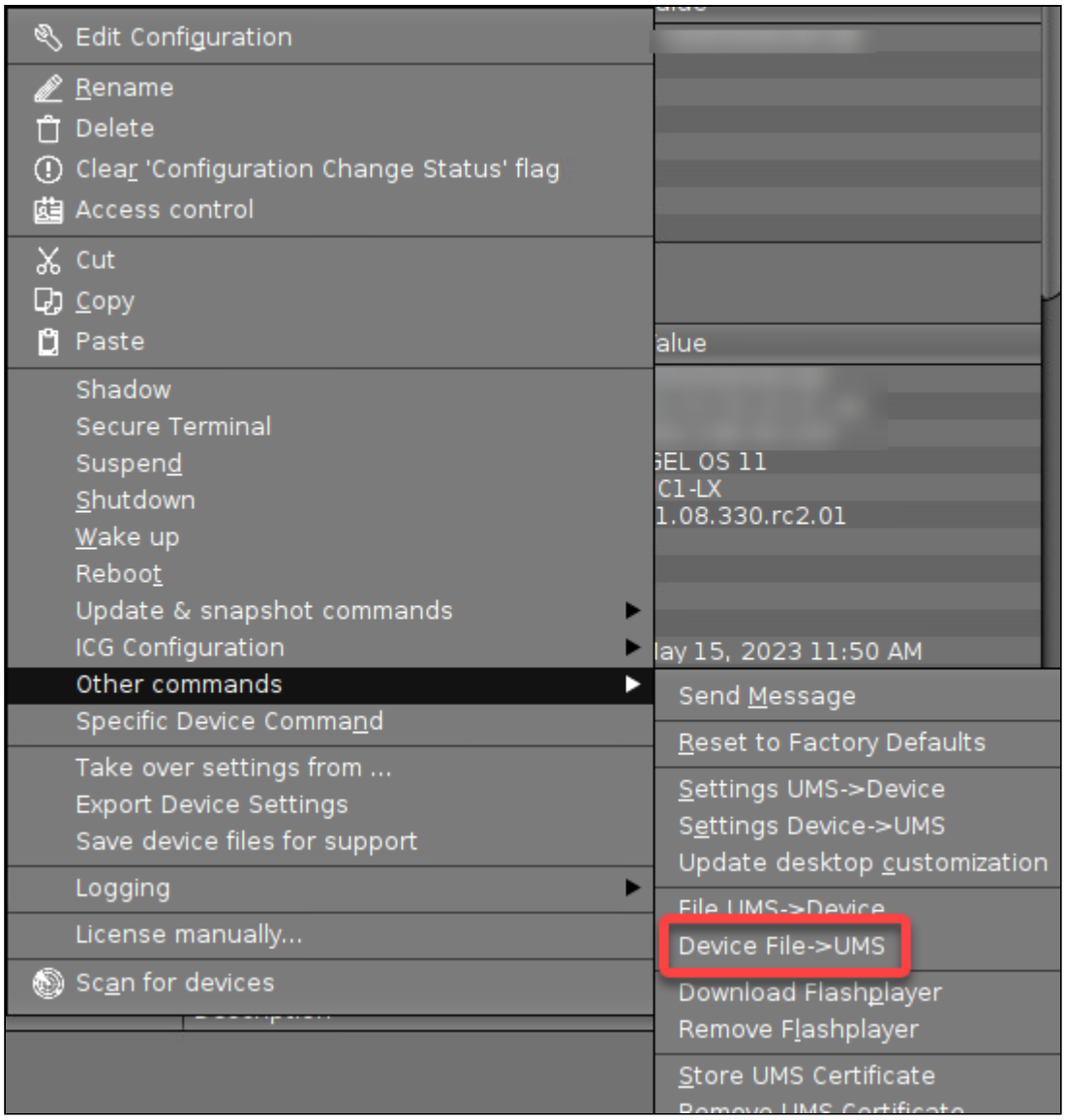


2. Select **BIOS - Get settings** and click **Execute**.

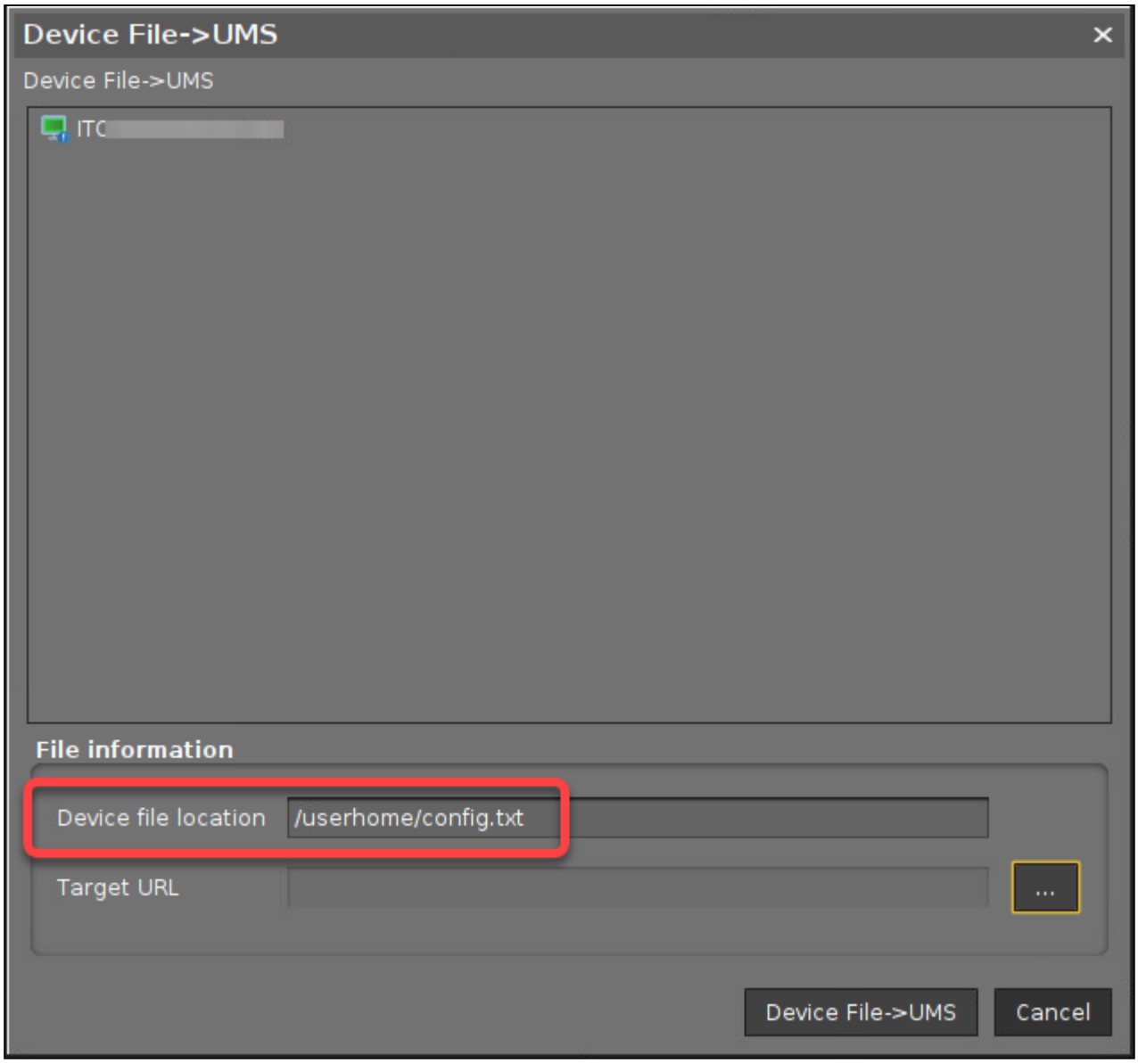


Editing the BIOS Settings File

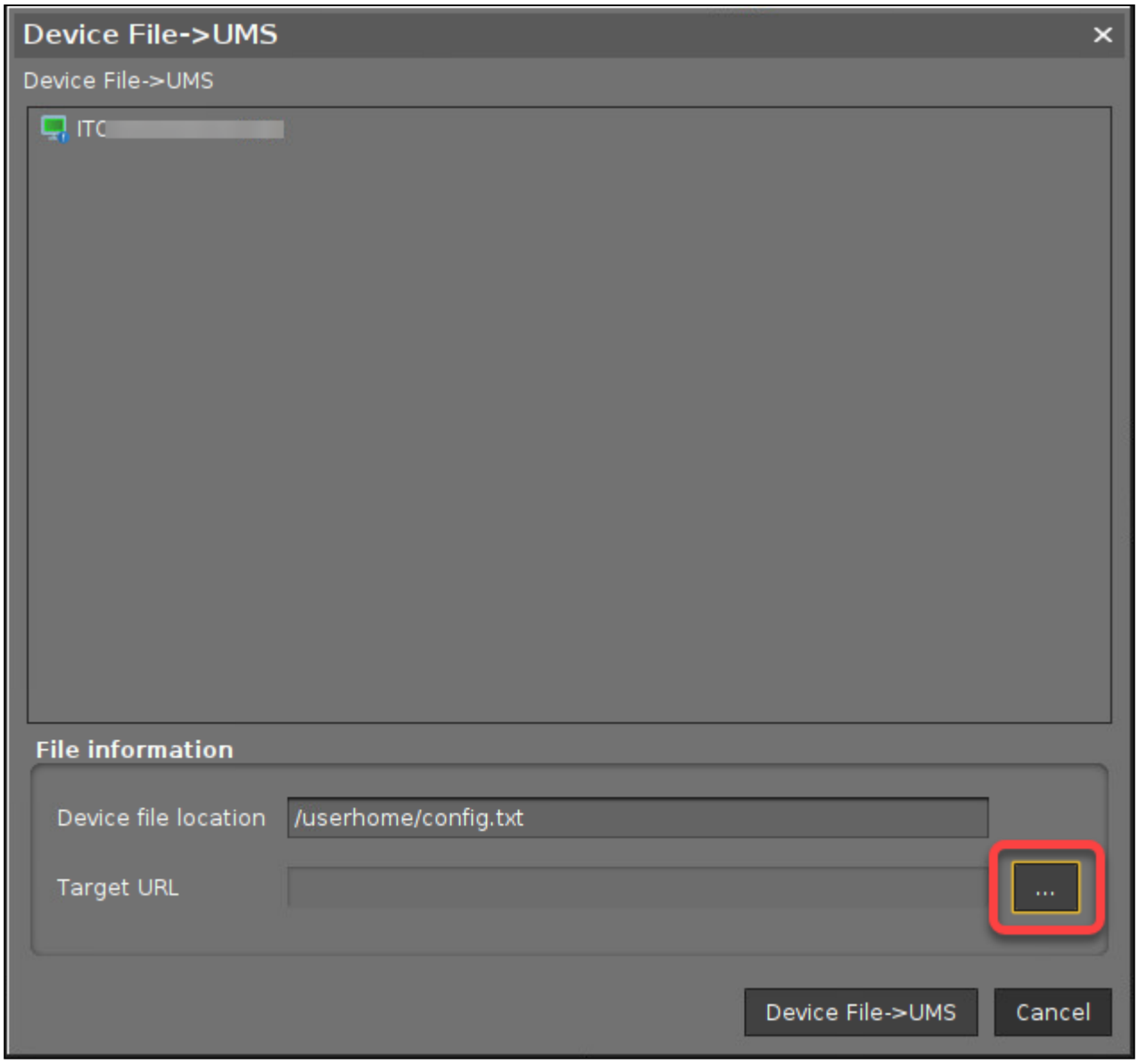
1. Look up your device in the UMS structure tree, open the context menu, and select **Other commands > Device File -> UMS**.



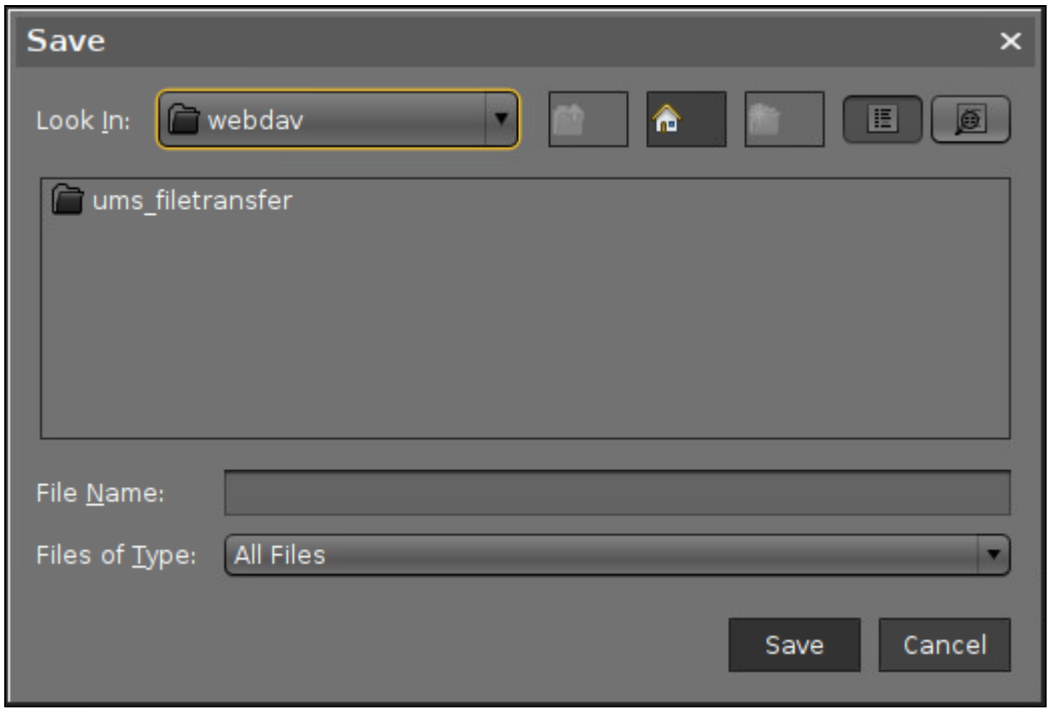
2. Under **Device file location**, provide the local path to which the settings file has been stored; this location has been specified in the step Change the BIOS Settings (see page 367).



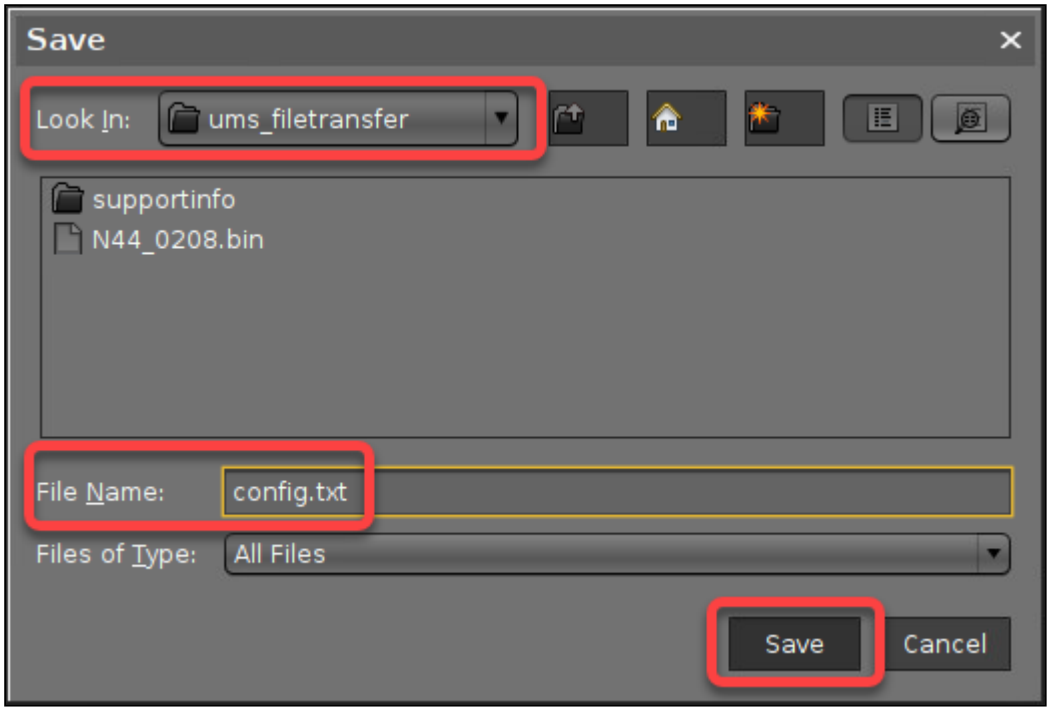
3. Define the path on the UMS machine under which the settings file should be stored so you can retrieve and edit it.



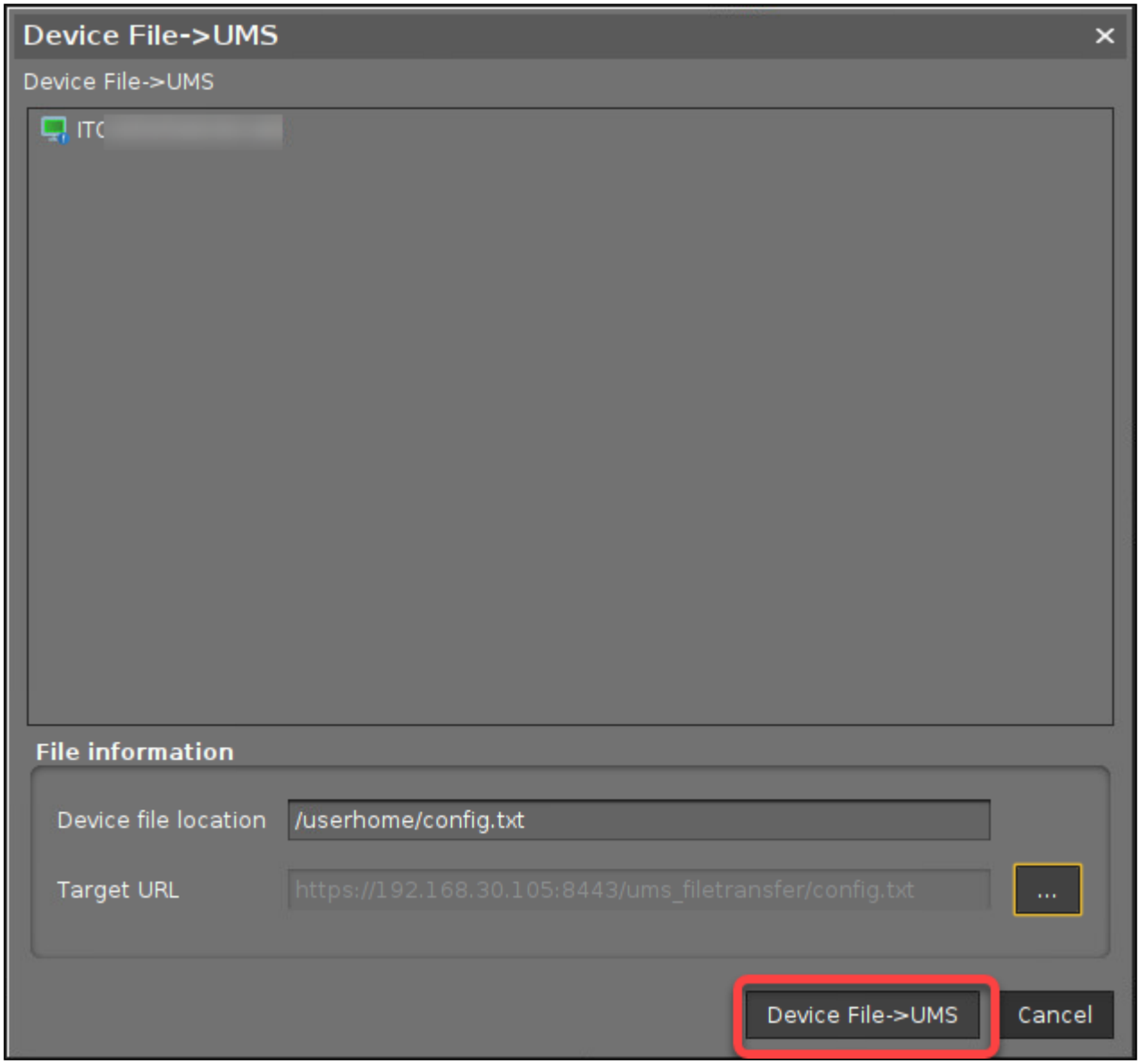
A file chooser opens.



4. Set the following parameters and click **Save**.
   - **Look in**: File path on the UMS machine under which the settings file should be stored, e.g. **ums_filetransfer**.
   - **File Name**: The file name under which the settings file should be stored.



5. Click **Device File -> UMS** to transfer the file from the device to the UMS machine.



6. Download and install the HP BIOS Configuration Utility. For information on the download source and the use of the utility, see https://ftp.ext.hp.com/pub/caps-softpaq/cmit/whitepapers/BIOS_Configuration_Utility_User_Guide.pdf.
7. Edit the configuration file as desired.

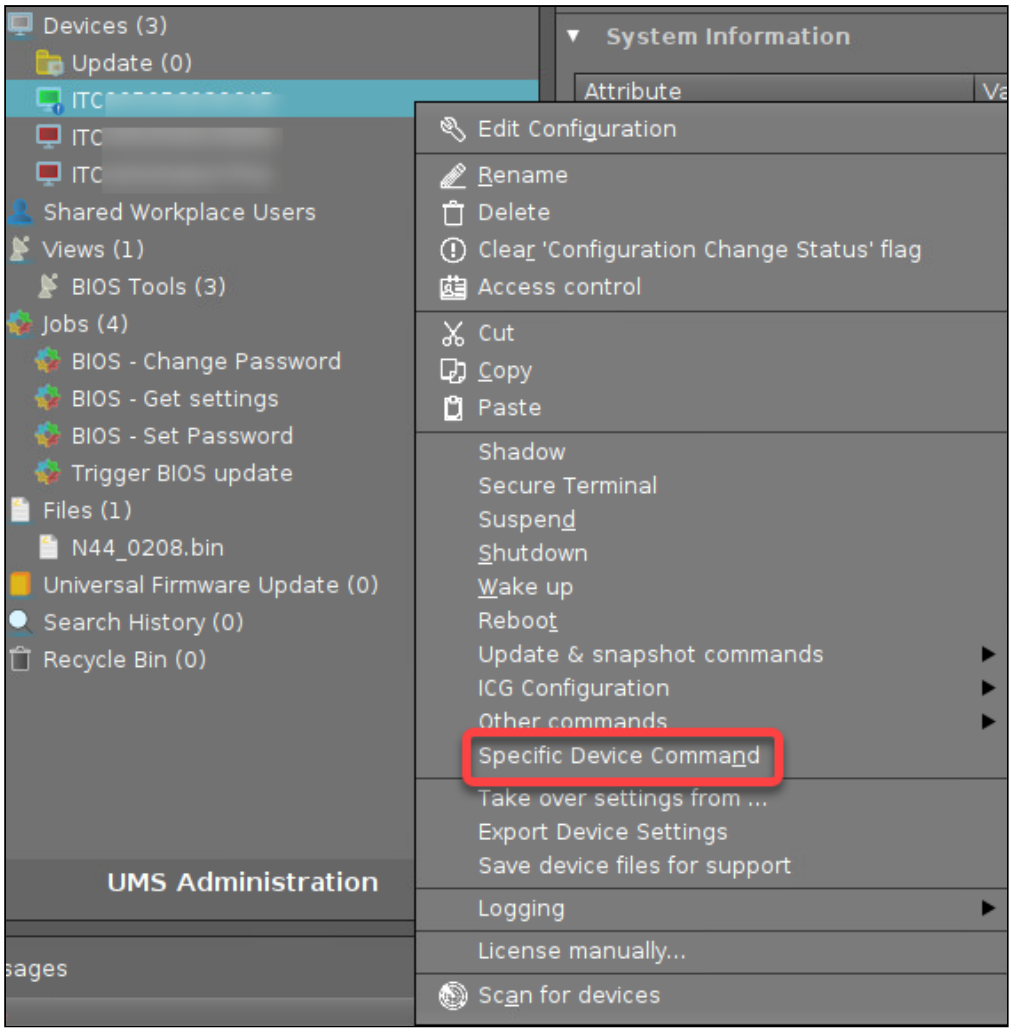
Make sure that the BIOS settings file is formatted properly and that the REPSET format is respected. For further information, see https://ftp.ext.hp.com/pub/caps-softpaq/cmit/whitepapers/BIOS_Configuration_Utility_User_Guide.pdf

It is sufficient to specify only those BIOS settings you want to change so that your edited file contains snippets instead of all possible settings.

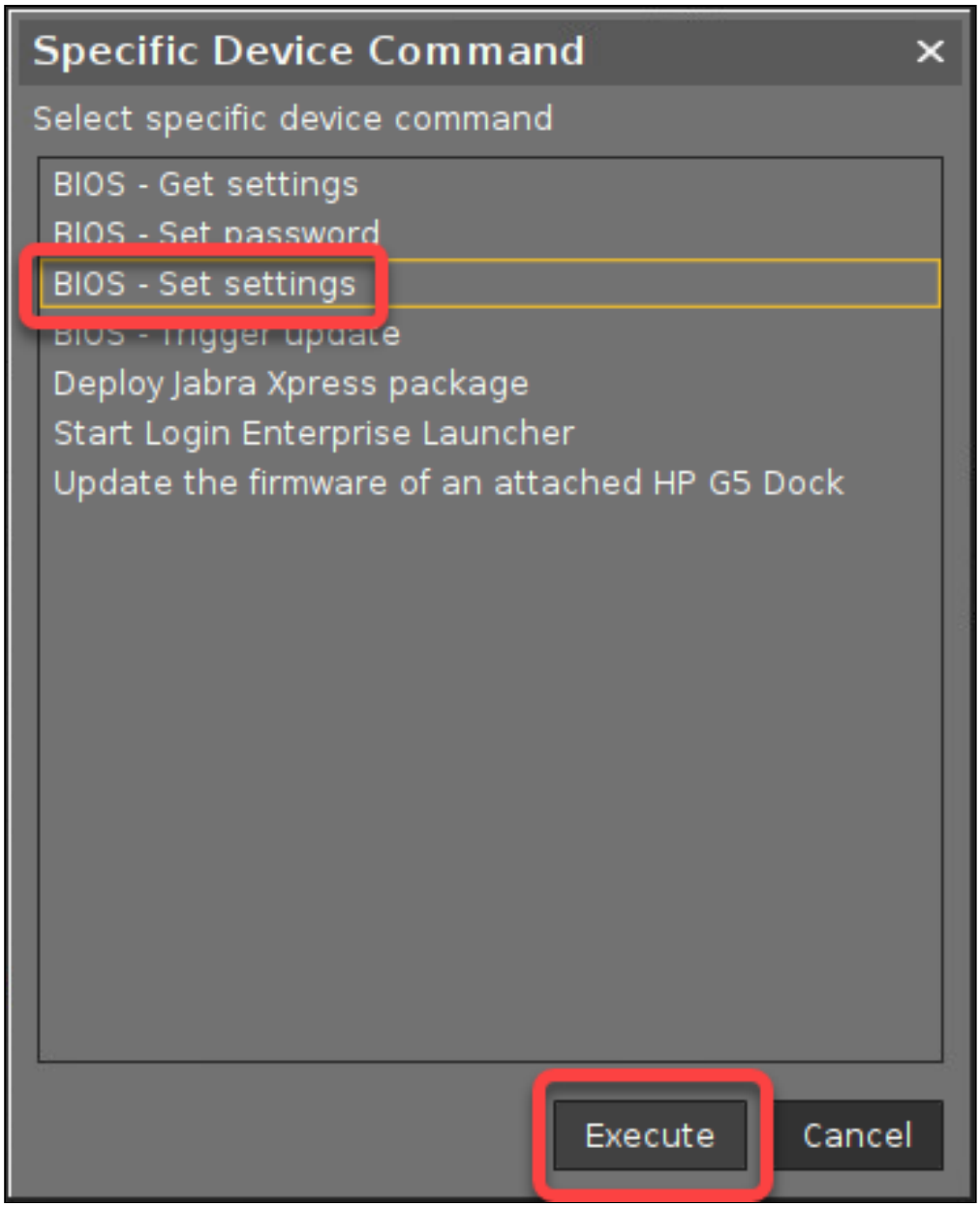
8. Save the settings file, e.g. as `config.txt`. Make the edited file available as described under Setting up the File Source (see page 350).

Deploying the Changed Settings on the Device

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

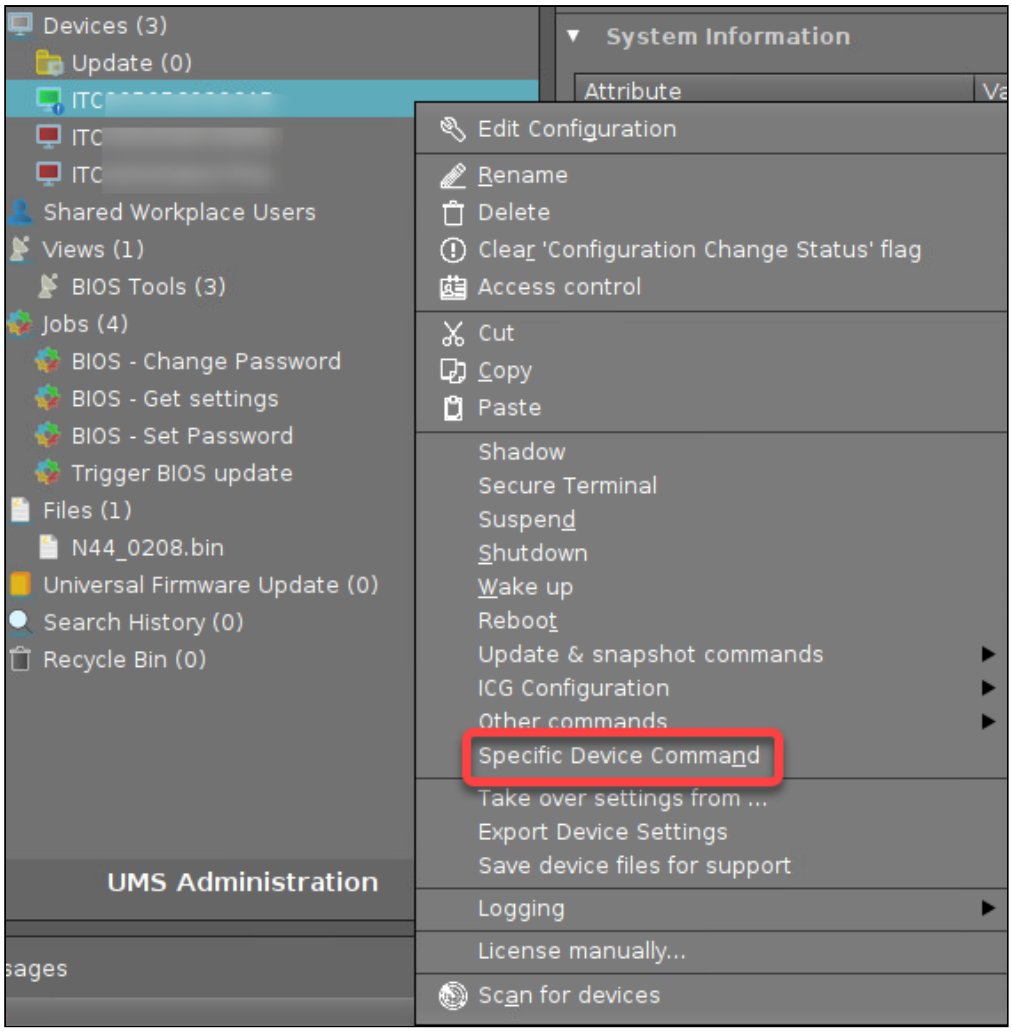


2. Select **BIOS - Set settings** and click **Execute**.

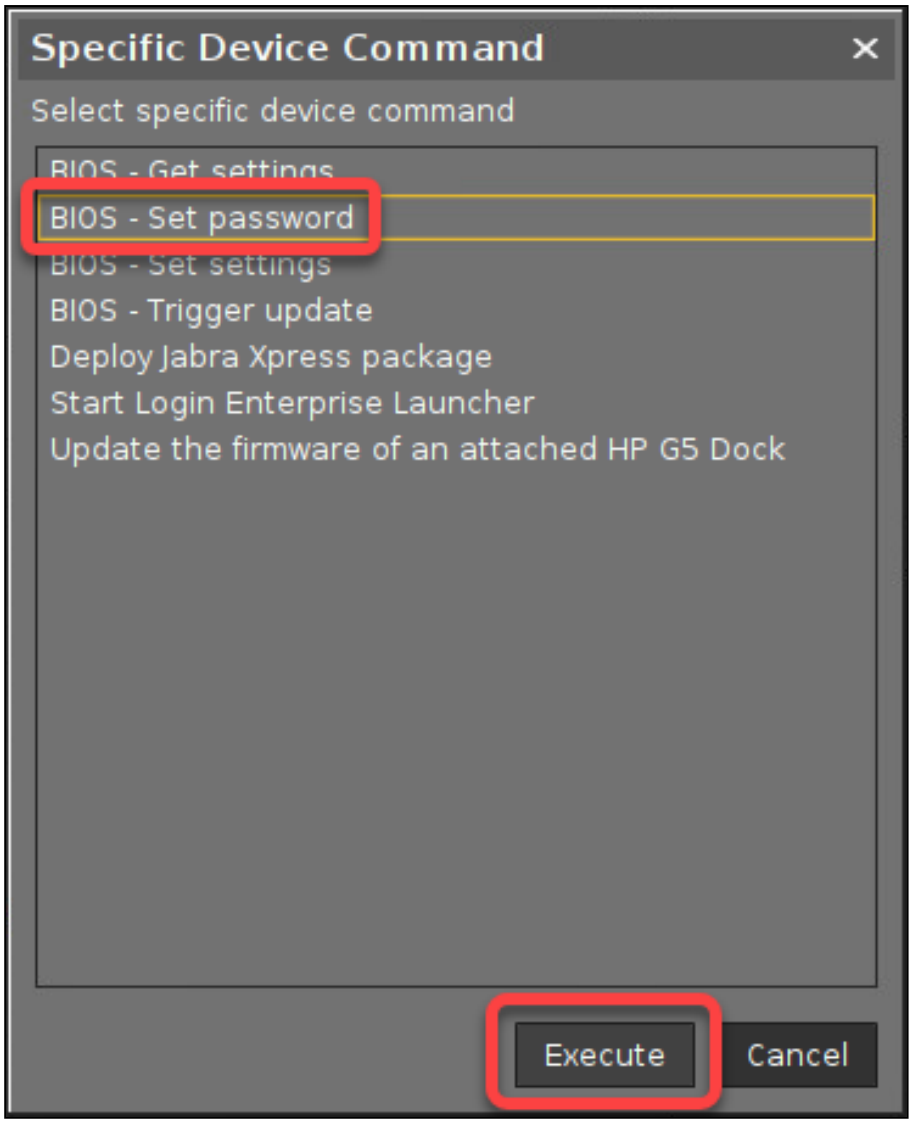


Resetting the BIOS Settings to Default

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

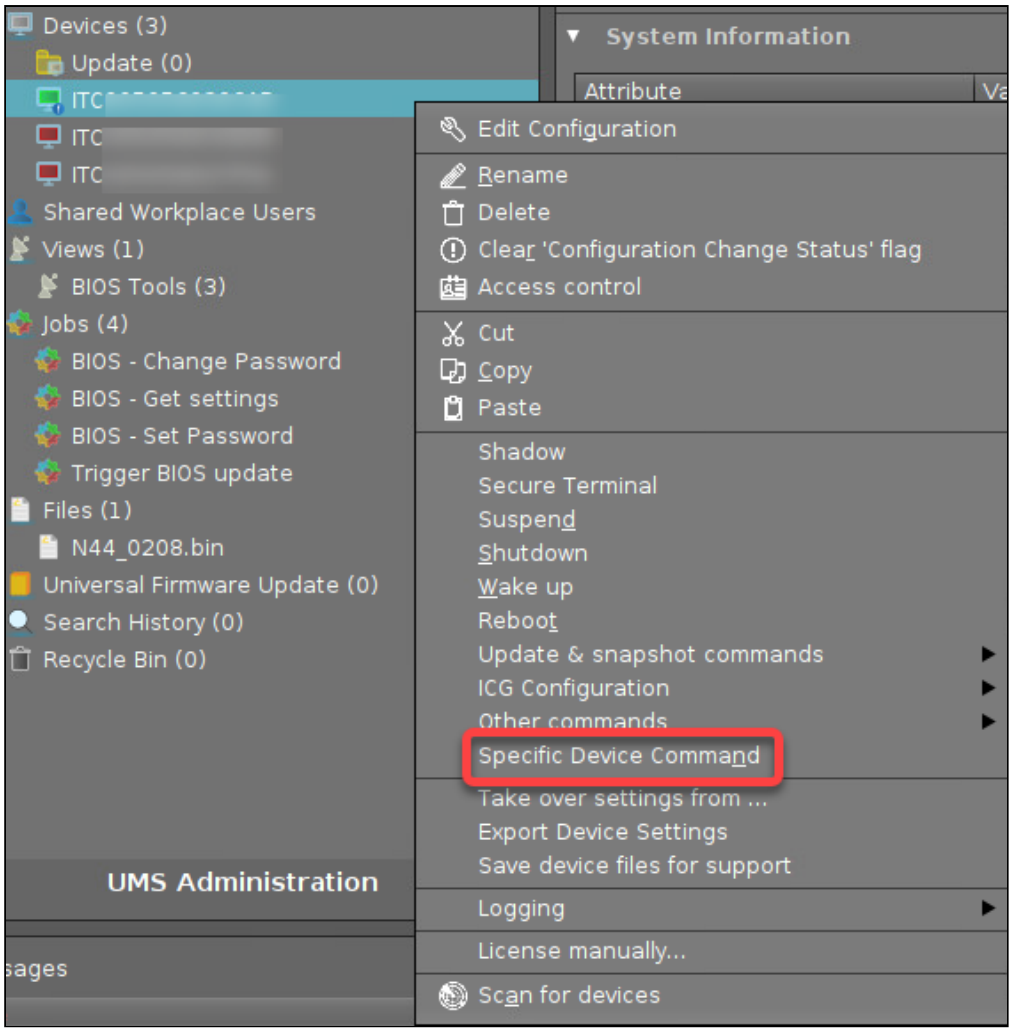


2. Select **BIOS - Set password** and click **Execute**.

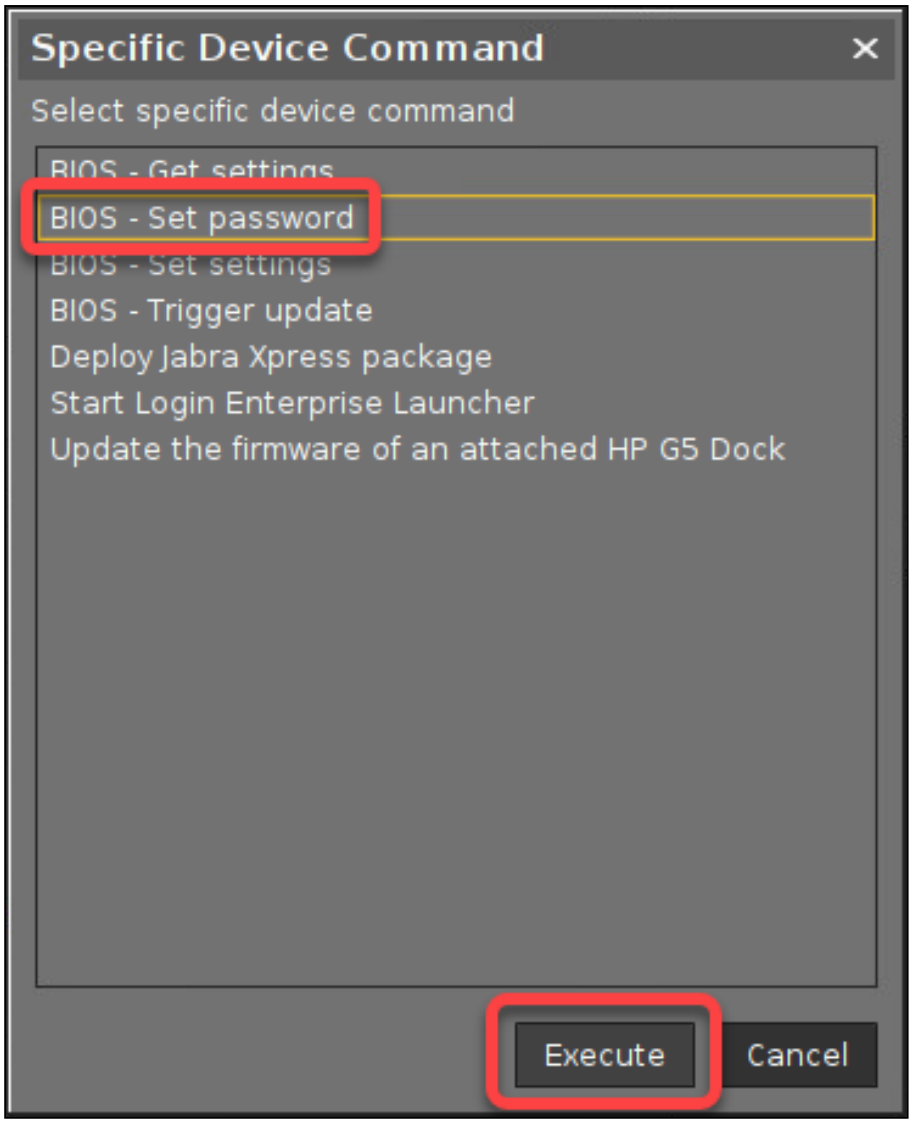


Setting a BIOS Password

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

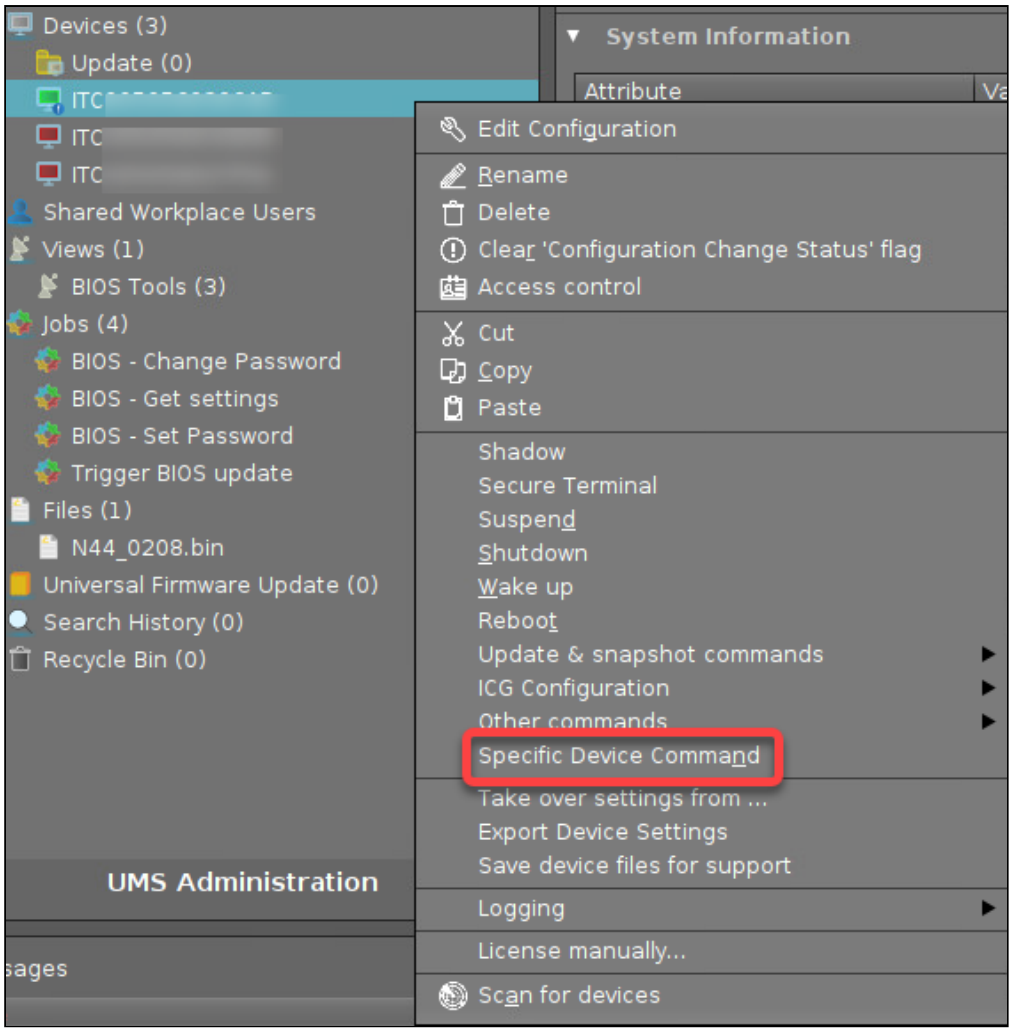


2. Select **BIOS - Set password** and click **Execute**.

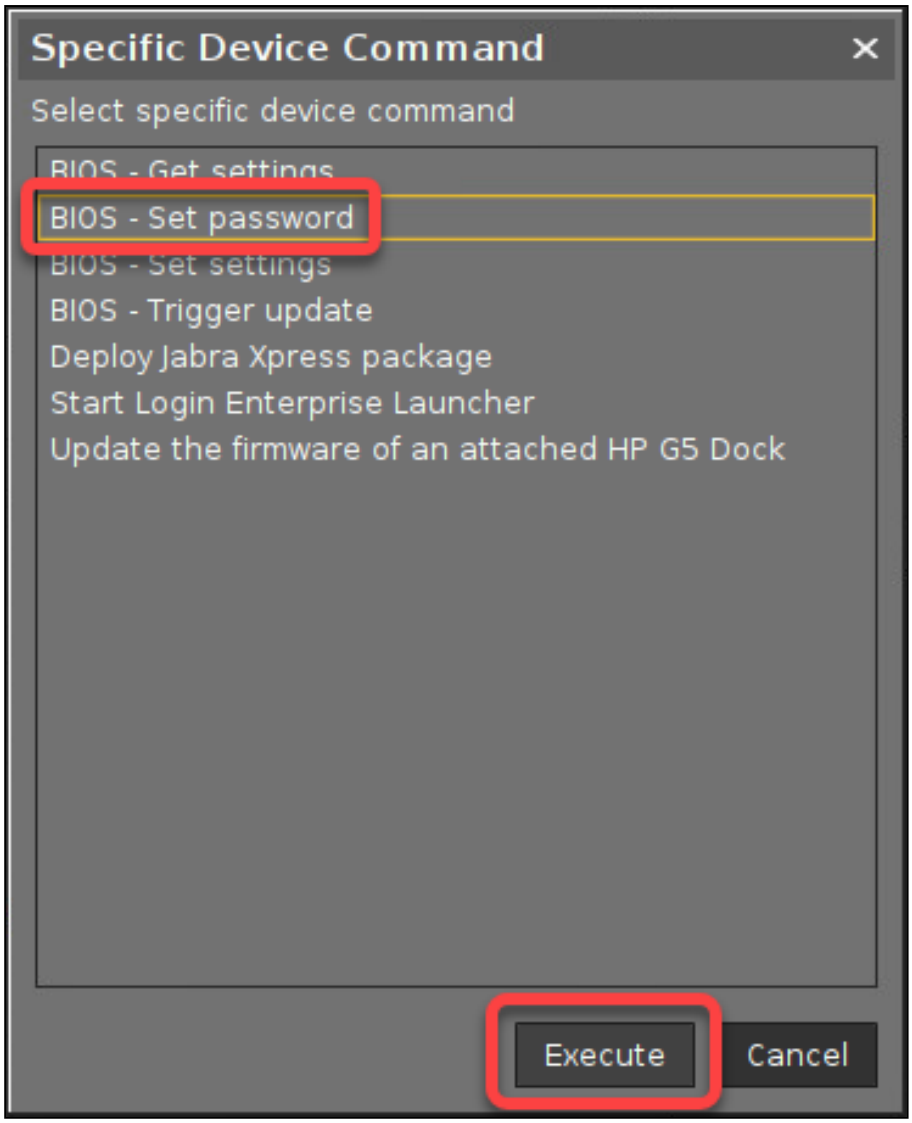


Changing the BIOS Password

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

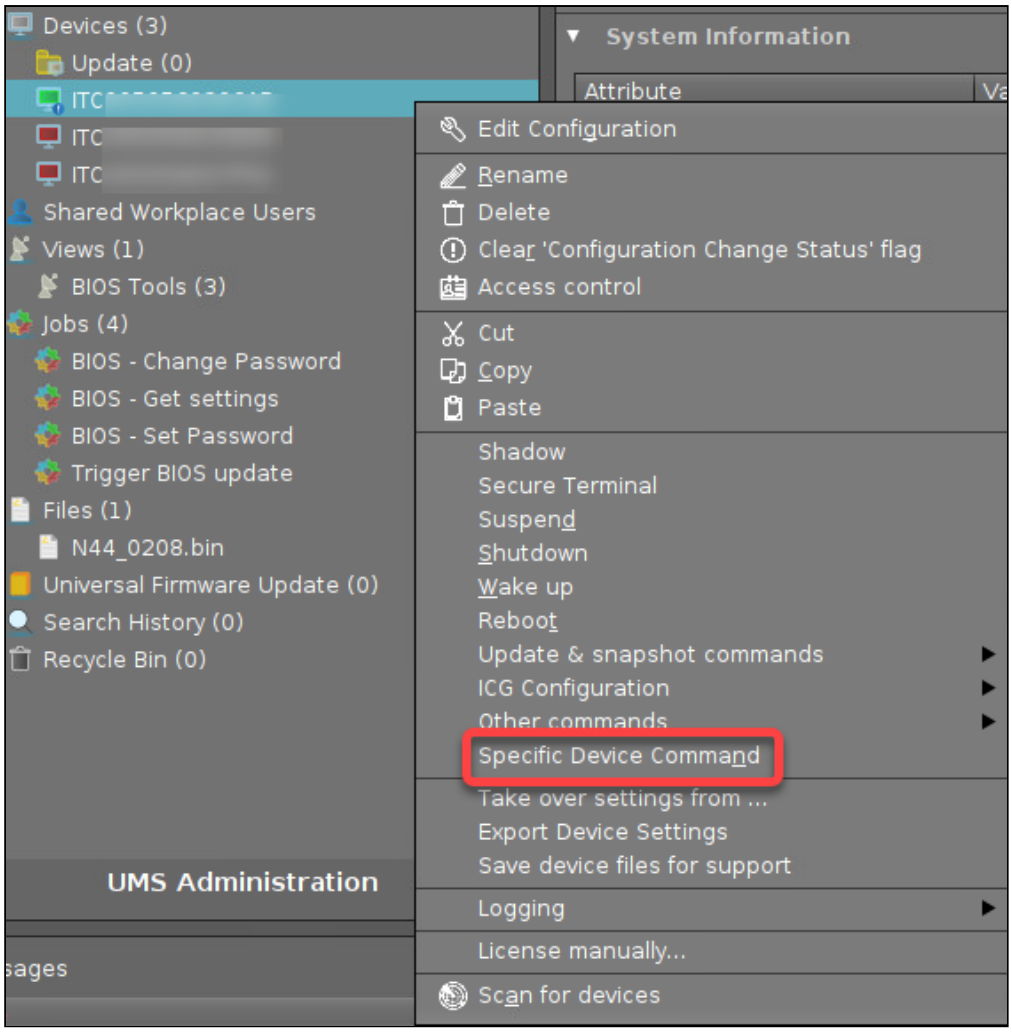


2. Select **BIOS - Set password** and click **Execute**.

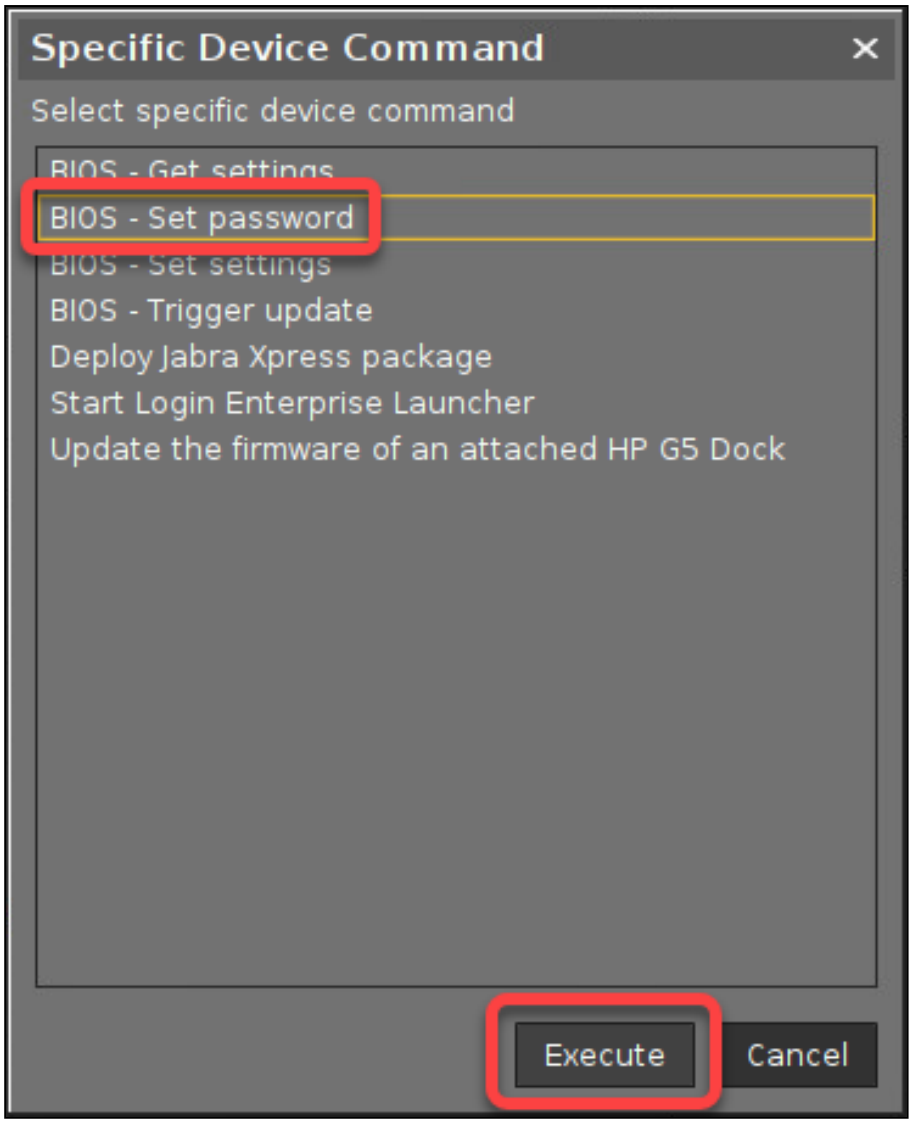


Resetting the BIOS Password (Removing Password Protection)

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.



2. Select **BIOS - Set password** and click **Execute**.



Command Line Interface (CLI) for the BIOS Tools

For testing the BIOS update on a single device, you can use the command line tool as an alternative to a scheduled job from the UMS.

As a prerequisite, the steps described under Setting up the File Source (see page 350) and Configuring the Devices (see page 354) must be completed.

When the command has been executed, a dialog informs you that a reboot is required. You can choose between two options:

- Perform the reboot and update right away
- Postpone the update to the next reboot

Usage

```
bios-tools [OPTIONS] COMMAND [ARGS]...
```

Options

Option	Description
`--debug / --no-debug`	
`--info / --no-info`	
`--test / --no-test`	
`--help`	Show this message and exit

Commands

Command	Argument	Description
`password`		Set BIOS password
`settings`		Handle BIOS settings
	`-c, --configure`	Configure BIOS settings with a configuration file
	`-g, --get`	Get current BIOS settings
	`--help`	Show this message and exit
`update`		Handle BIOS update
	`-e, --enable`	Enable BIOS update. The update will be triggered after a reboot.
	`-d, --disable`	Disable BIOS update
	`-s, --show`	Show if BIOS update is enabled or not
	`--help`	Show this message and exit

Citrix

- Performance (see page 390)
- Mouse (see page 395)
- How to Configure Citrix Native USB Redirection (see page 402)
- Citrix Fabulatech Scanner Redirection in IGEL OS (see page 404)
- How to Map USB Storage Media into Citrix Sessions (see page 406)
- How to Auto-Hide Toolbar in Appliance Mode (see page 408)
- How to Create a Seamless, Transparent User Experience with Appliance Mode (see page 409)
- How to Connect to a Citrix Farm (see page 410)
- How to Create a Self-Service Setup for the User with Quick Settings (see page 416)
- Troubleshooting: Login Failed because of the Expired AD Password (see page 418)
- How to Configure Auto Logon for Citrix Virtual Desktops (see page 420)
- Force Citrix Logout Using Hotkey (see page 424)
- Citrix: Freeze at Logout (see page 425)
- Warning Message: [Citrix Store] Could Not Connect to the Citrix Server (see page 426)
- How to Set Up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec (see page 428)
- Troubleshooting: Highly Secured XenServer has Problems with LD_BIND_NOW Workaround (see page 429)
- Troubleshooting: Workaround for Citrix Receiver X Error (see page 430)
- Troubleshooting: Citrix HTML5 Receiver Issue (see page 431)
- How to Configure Macbook Keyboard Layout inside Citrix Session (see page 432)
- How to Use Lync / Skype for Business with Citrix HDX RealTime Optimization Pack (see page 433)
- Citrix Advanced Endpoint Analysis (EPA) Client on IGEL OS (see page 434)
- Citrix Netscaler Gateway Client (NSGClient) for Netscaler VPN Connections (see page 435)
- Troubleshooting: Unexpected Keyboard Layout in a Citrix Session (see page 440)
- How to Use Font Smoothing (ClearType) in Citrix Sessions (see page 443)
- Citrix Feature Matrix (see page 445)

Performance

- Troubleshooting: Poor Performance with Black Blocks and Stripes in Citrix Sessions (see page 391)
- Troubleshooting: Poor Performance with Citrix XenDesktop 7.6 Deep Compression (see page 392)
- Troubleshooting: Citrix Receiver - Grey Blocks in Excel 2013 (see page 393)
- Troubleshooting: Bar Code Scanning is Slow via Citrix (see page 394)

Troubleshooting: Poor Performance with Black Blocks and Stripes in Citrix Sessions

Symptom

In the Citrix session, you sometimes experience a problem with black blocks, frames, or stripes.

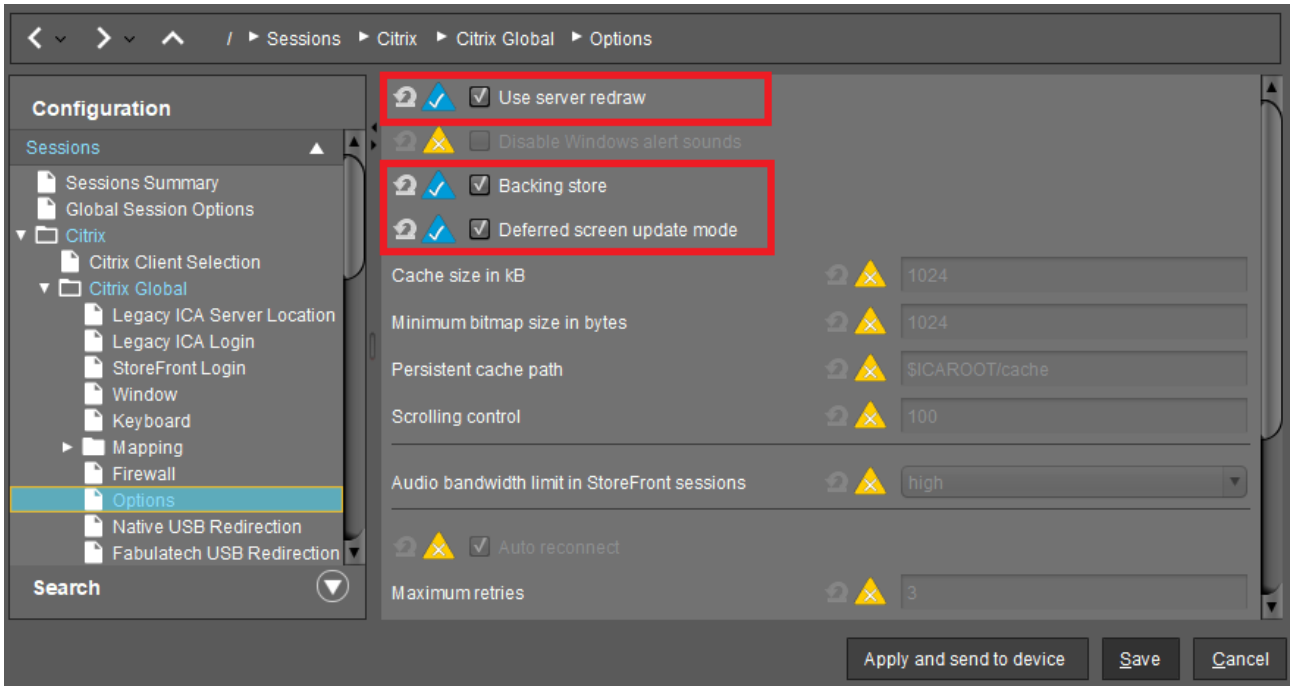
Problem

Poor performance is often connected with the delayed or slow refreshing of the screen content.

Solution

->In the IGEL Setup or the configuration dialog in the UMS, activate one of the following parameters or all of them under **Sessions > Citrix > Citrix Global > Options**:

- **Use server redraw**
- **Backing store**
- **Deferred screen update mode**



See also Options for an IGEL OS Citrix Session (see page 1264) in the manual chapter for Citrix.

If this doesn't work, see also Black Box Next to the Mouse Cursor (see page 401).

Troubleshooting: Poor Performance with Citrix XenDesktop 7.6 Deep Compression

Symptom

When using XenDesktop 7.6 on Windows Server 2008R2 with Citrix Receiver 13.0.4, 13.1.4 or 13.2.1 with H.264 Deep Compression Codec, dragged Windows lag and the performance is generally poor.

Problem

Server and/or client do not have enough computing power for the H.264 Deep Compression Codec.

Solution

Enable the legacy graphics mode on the XenDesktop 7.6 server via a policy.

Troubleshooting: Citrix Receiver - Grey Blocks in Excel 2013

Symptom

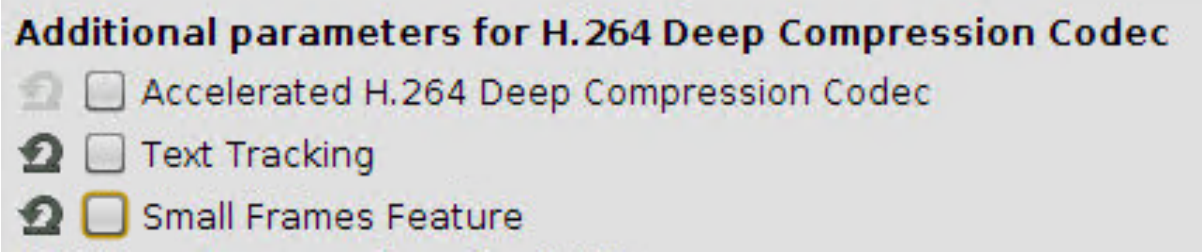
When using Microsoft Excel 2013 on XenDesktop 7.6 with Citrix Receiver 13.1.3, 13.1.4 or 13.2, grey blocks appear especially if you mark multiple cells.

Problem

Codec parameters may not be optimal for this use case.

Solution

1. In IGEL Setup, go to **Sessions > Citrix > Citrix Global > Codec**.
2. Disable **Text Tracking**.
3. Disable **Small Frames Feature**.



Troubleshooting: Bar Code Scanning is Slow via Citrix

Solution Based on Experience from the Field
This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Issue

Bar code scanning is slow via Citrix.

Environment

- Firmware version: any
- UMS version: any

Description

USB attached bar code scanner is very slow via Citrix.

Solution

In order to pass the Bar Code scanner through correctly, you want it to be a HID so it passes through as a HID instead of using Native USB Redirection. A quick way to determine that would be to open a terminal in IGEL OS and simply scan something. If it populates data in the terminal, then it is configured as HID. Also, check the configuration guide for the particular scanner that you are using. The config guide is simply a bunch of barcodes that the device can scan. Once a code is scanned, the device beeps twice, and that changes the config on the scanner. On some devices, there is a setting for Alternate OS Linux/MACOS. The default setting for the scanner usually doesn't enable this. Once the setting was set, everything scanned very fast and that same speed was shown in Citrix.

Mouse

- How to Change the Middle Mouse Button Function for Citrix Session and Local Firefox Browser (see page 396)
- How to Connect a SpaceMouse with a Citrix Session (see page 397)
- Troubleshooting: Solve SpaceMouse USB Reset Problem (see page 399)
- Troubleshooting: Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session (see page 400)
- Troubleshooting: Black Box Next to the Mouse Cursor (see page 401)

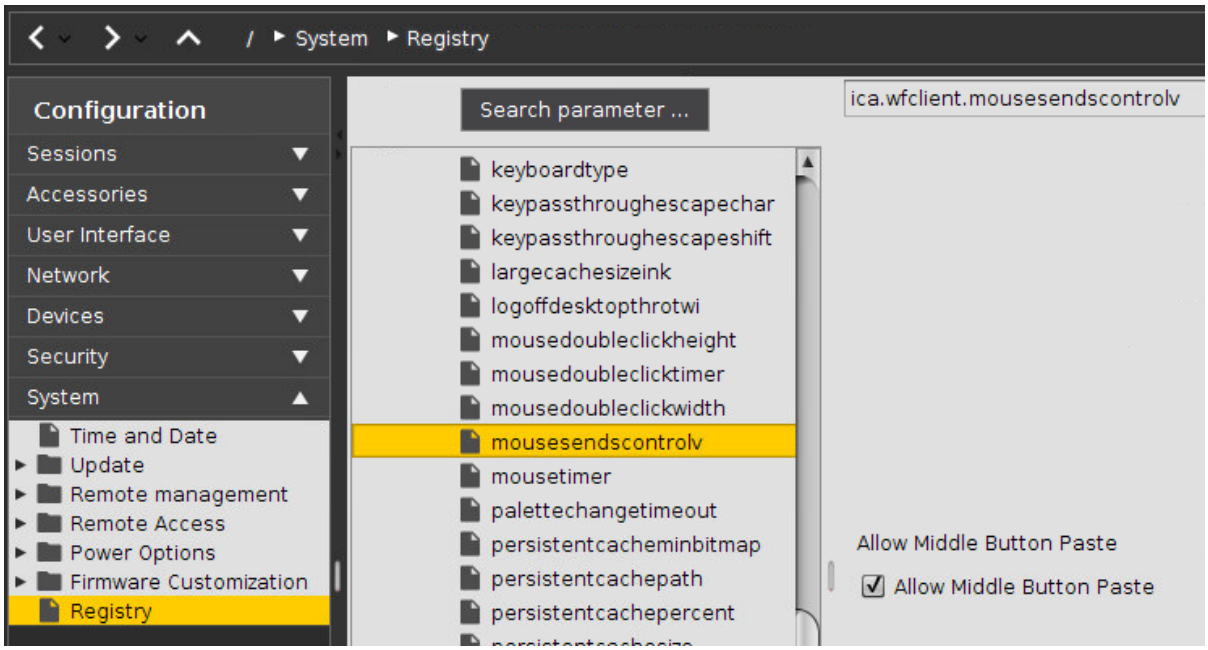
How to Change the Middle Mouse Button Function for Citrix Session and Local Firefox Browser

Middle mouse button cannot be used for smooth scrolling within applications like *Excel* or *Internet Explorer* within a Citrix session or with the local *Firefox b*rowser.

Menu Path: Configuration > System > Registry

The default function of the middle mouse button is *copy and paste*.

->Open IGEL **Registry** in local client setup or UMS.



->For Citrix sessions change:

- **System > Registry > ica.wfclient.mousesendscontrolv**

->For local Firefox browser change:

- **System > Registry > browserglobal.app.middlemouse_contentloadurl**
- **System > Registry > browserglobal.app.middlemouse_paste**

The changes will take effect after rebooting the thin client.

More information on the Firefox parameters can be found at
http://kb.mozillazine.org/Middlemouse.contentLoadURL
http://kb.mozillazine.org/Middlemouse.paste

How to Connect a SpaceMouse with a Citrix Session

This article describes how to use a 3Dconnexion SpaceMouse in a Citrix session.

Always use a SpaceMouse only as an additional, i.e. second, mouse.

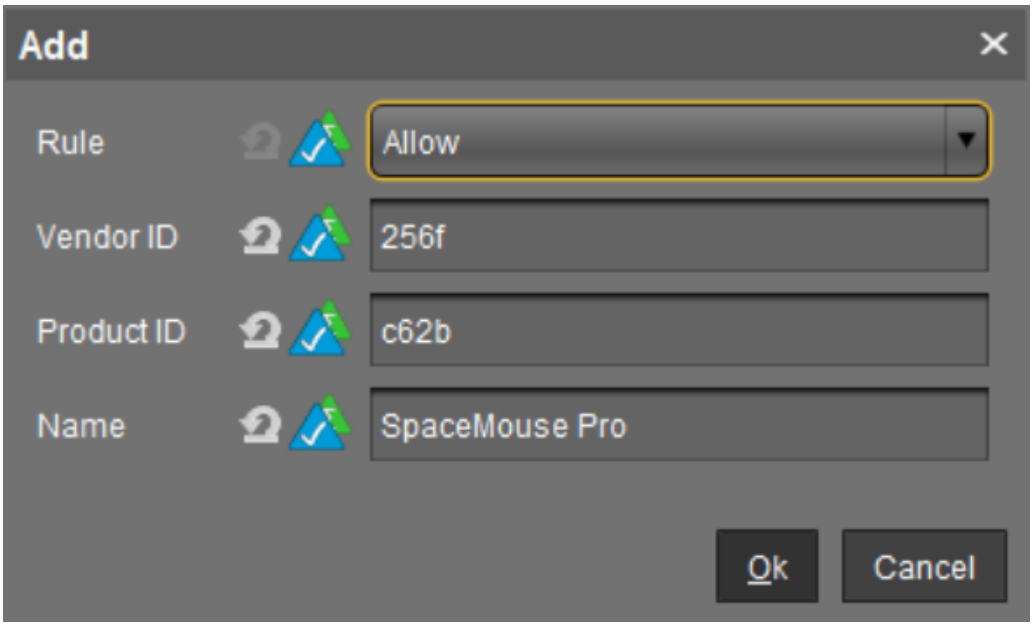
From **version 10.06.100** or **11.02.100** on, the SpaceMouse does not interfere anymore with the local mouse pointer because of a registry key which is enabled by default.
This registry parameter ignores the SpaceMouse for the IGEL graphical user interface:

IGEL Setup	**System > Registry**
Parameter	Deactivates 3Dconnexion/Logitech SpaceMouse products as a standard mouse
Registry Key	`userinterface.mouse.spacemouse.x11_ignore`
Value	enabled/disabled
Info	"enabled" means that the SpaceMouse is passed through to the session and ignored by the local GUI. "disabled" means that the SpaceMouse is also used for the local GUI.

To configure the SpaceMouse for Citrix sessions:

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Activate the checkbox **Native USB Redirection**.
3. Set the **Default rule** to **Deny**.
4. Add a device exception rule as in the following screenshot with the **Vendor ID** and **Product ID** of your specific SpaceMouse:
   SpaceMouse products included (VID, PID, Vendor, Product)

   - 0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT
   - 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman
   - 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic
   - 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000
   - 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse
   - 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse
   - 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse
   - 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse
   - 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks
   - 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse
   - 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro
   - 0x256F; *; 3Dconnexion; SpaceMouse



5. Save the settings.

Now, the SpaceMouse is ready for use.

To achieve that the mouse behaves as usual in CAD programs, change the configuration as follows:

1. Go to **IGEL Setup > System > Registry > ica.wfclient.mousesendscontrolv**.
2. Set the parameter to **disable**.

If the SpaceMouse does not function properly after the previous Citrix session, the USB reset of the SpaceMouse must additionally be configured. Follow the instructions in Troubleshooting: Solve SpaceMouse USB Reset Problem (see page 399).

Troubleshooting: Solve SpaceMouse USB Reset Problem

Environment

Valid for IGEL hardware H850C, H830C, and M340C

Problem

After a previous Citrix session, the SpaceMouse does not function properly (e.g. after the end of the Citrix session, the reset of the SpaceMouse does not take place; as a result, the display of the SpaceMouse always remains bright).

Solution

Use a power cycle command to automatically turn all USB devices off and on again:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Commands > Post Session**.
2. Under **Session type**, select **Citrix**.
3. Under **Post session command**, enter the following command: `/etc/igel/usb-power-reset/igel-usb-power-ctl -p cycle`

   > You do not need root permissions for this action.

As a result of the configured USB power cycle, after the end of the Citrix session, the display of the SpaceMouse should become dark for about 1 second and then bright again.

See also How to Connect a SpaceMouse with a Citrix Session (see page 397).

Troubleshooting: Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session

Solution Based on Experience from the Field
This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Issue

Wireless Mouse Keyboard Set Logitech k520 freezes in Citrix XenDesktop session.

Environment

- IGEL OS 11
- UMS 6.01 and higher

Description

If the Wireless Mouse Keyboard's infrared signal is disturbed, it freezes.

Solution

This particular device uses infrared dongle. BT devices should work fine as a workaround and we suggest using those. Citrix discourages the use of the IR dongles.

Troubleshooting: Black Box Next to the Mouse Cursor

Symptom

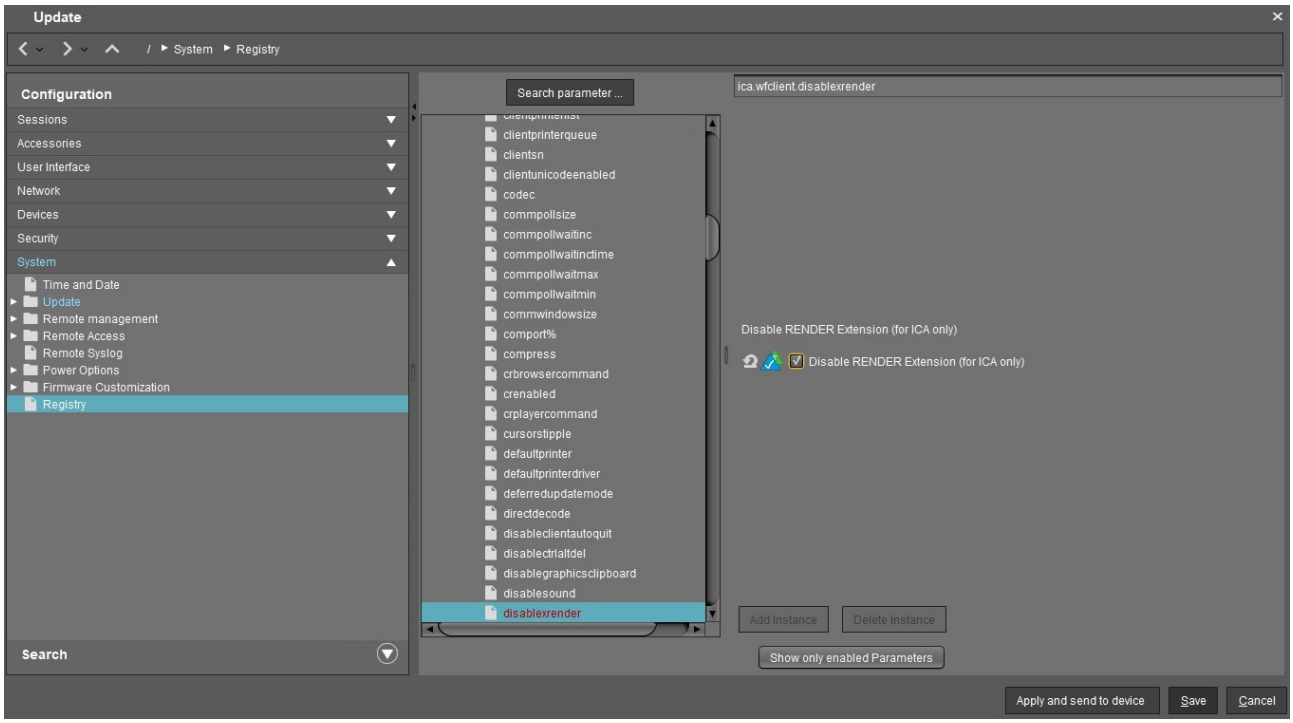
With certain programs (Adobe Reader, Visual Studio, ...) a black box is always displayed next to the cursor in XenDesktop VMs.

Problem

This only happens when a connection is made to an IGEL device and disappears when a Windows device is connected. The box is only visible directly on the client (not via VNC).
The problem occurs on the UD7 as well as on Intel NUCs.

Solution

->In the IGEL Setup disable the parameter **Disable RENDER Extension (for ICA only)** under **System > Registry > ica.wfclient.disablexrender:**



See also at Citrix: https://support.citrix.com/article/CTX212013

How to Configure Citrix Native USB Redirection

Native USB Redirection redirects most popular USB devices to the Citrix session. To use this feature, you must have at least **XenDesktop 7.6** installed. In addition, the guidelines for USB redirection must be defined. More information can be found on the following pages

- Citrix Generic USB Redirection Configuration Guide[55]
- Generic USB redirection and client drive considerations[56]

The following types of USB device are **not** supported by default for use in a **Citrix Virtual Apps** and **Desktops** session:

- Bluetooth dongles
- Integrated NICs
- USB hubs

The following types of device are supported directly in a **Citrix Virtual Apps** and **Desktops** session, and so do not use USB support:

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

In addition to the server policies, the USB redirection must also be activated at the client:

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Enable **Native USB Redirection**.
3. Set the **Default rule** to **Deny** or **Allow**:
   - **Allow**: All devices that are allowed by default are redirected.
   - **Deny**: No device is redirected.

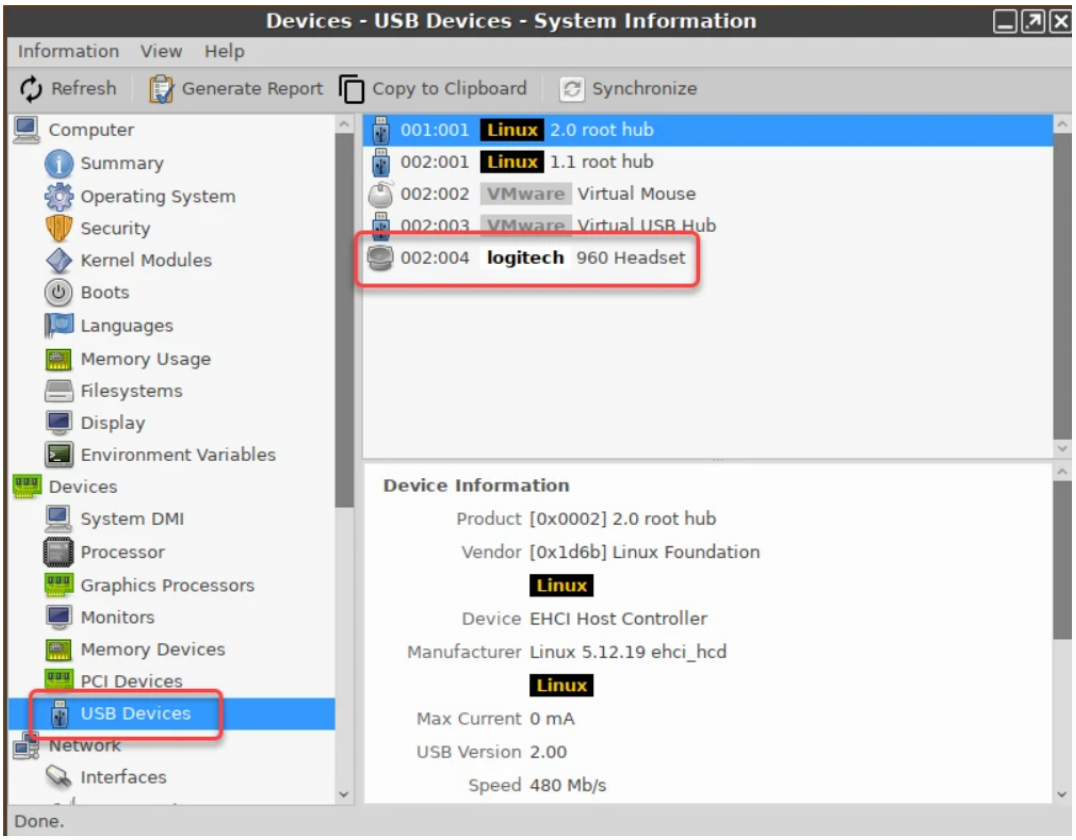
Tip
To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

4. To customize the USB redirection, you can create classes or device rules to redirect e.g. Bloomberg keyboards or 3D Spacemouse.

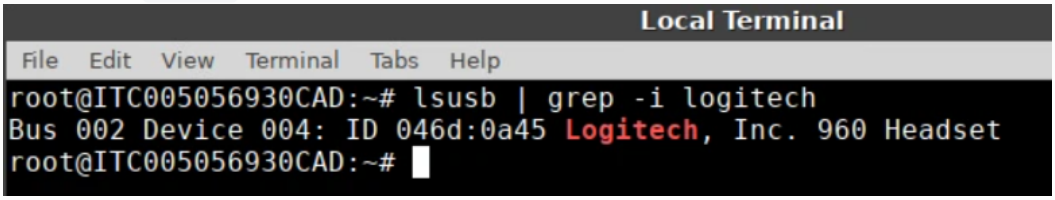
Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:

55. https://support.citrix.com/article/CTX137939
56. https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/general-content-redirection/usb.html



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.
Example for `lsusb`:



For a device exception rule, use the SpaceMouse Guide (see page 397).
For more information about USB redirection rules, see Native USB Redirection for Citrix Sessions in IGEL OS (see page 1267) and the documentation of the respective Citrix Workspace app.

Citrix Fabulatech Scanner Redirection in IGEL OS

The following article details how you can activate Fabulatech scanner redirection for Citrix sessions.

> Note that Fabulatech Scanner for Remote Desktop must also be installed on the backend server. For more information and a free trial version, see https://www.scanner-for-remote-desktop.com/.

How to Enable Fabulatech Scanner Redirection for Citrix

1. In the IGEL Setup, go to **System > Firmware Customization > Features** and make sure that **Scanner support /SANE (Limited support - functionality "as is", see product documentation for details)** is activated.

   - If the option is already activated, continue with step 2.
   - If the option has not been activated before, the software component must be downloaded first. For this purpose, make sure that the source of the current firmware is set correctly:
     - If you are using Universal Firmware Update, make sure that the device is assigned to the current firmware. For details, see Universal Firmware Update and Assigning updates.
     - If you are not using Universal Firmware Update, make sure that **System > Update > Firmware Update** is set to the source of the current firmware. For details, see Firmware Update Settings for IGEL OS (see page 2056).
   - After clicking **OK** to confirm your changes, you must reboot the system.
2. In the IGEL Setup, go to **Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**.

3. Check **Fabulatech Scanner for Remote Desktop**.

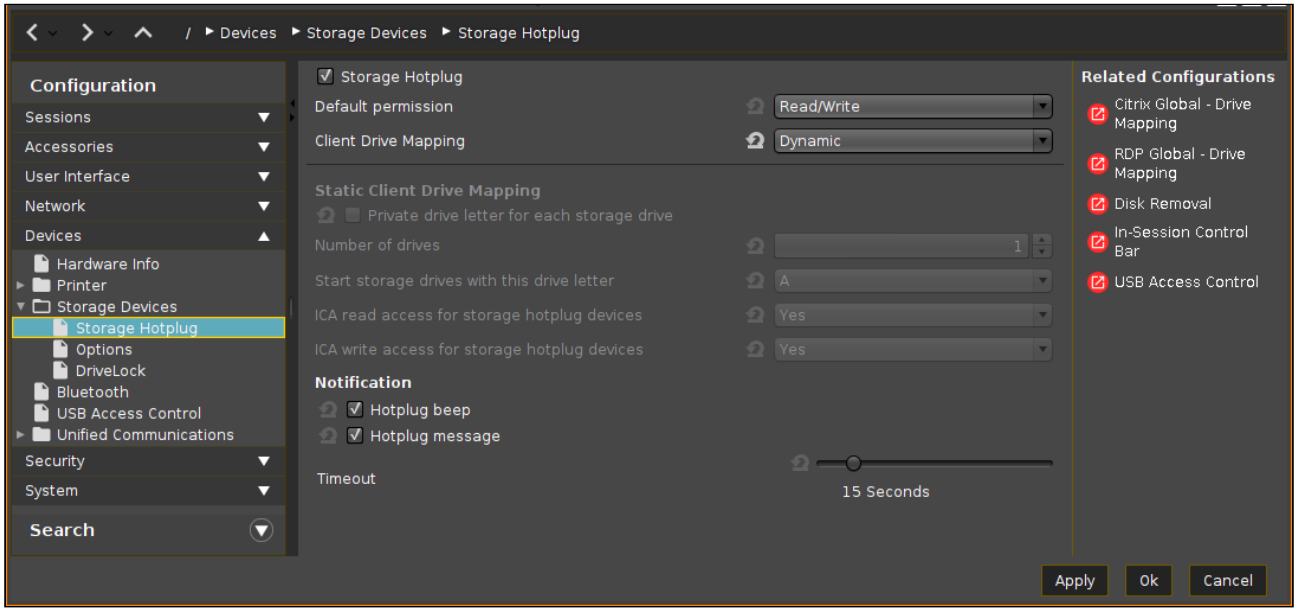
4. Click **Apply** or **Ok** to confirm the settings.

How to Map USB Storage Media into Citrix Sessions

How to configure USB storage mapping so that users can access USB storage media attached to the IGEL OS device within Citrix sessions?

The mapping of USB storage devices is possible for "USB mass storage class" devices. The storage of smartphones and digital cameras is usually accessed via the MTP protocol. Mobile device access via MTP is available with IGEL Linux 10.04.100 or higher; for more information see the how-to Using Mobile Device Access (see page 1076).

Basic Configuration of the Client



Within the IGEL Setup or a UMS profile, you basically need to configure these parameters:

->Activate **Devices > Storage Devices > Storage Hotplug > Client drive mapping > Dynamic**. This option activates dynamic client drive mapping. It automatically recognizes new storage media as they are connected to the endpoint device. The endpoint device beeps and shows a notification while it mounts the new device. The storage devices automatically become usable on the endpoint and in Citrix ICA Sessions.

Mounted devices need to be unmounted before they are removed to ensure data integrity. This can be done via the Disk Utility (see page 1799), the Disk Removal (see page 1803) tool, or a tray icon.

Additional Parameters to Check

->The following parameters are set by default, thus storage mapping will work, but maybe for some reason you have changed these and need to adjust them to allow the storage mapping:

Sessions > Citrix > Citrix Global > Mapping > Drive Mapping > Drive mapping (set checkmark)

Sessions > Citrix > Citrix Global > Native USB Redirection > Native USB redirection (remove checkmark)

Sessions > Citrix > Citrix Global > Fabulatech USB Redirection > Fabulatech USB redirection (remove checkmark)

Devices > USB access control > Enable (remove checkmark)

Sessions > RDP > RDP Sessions > [session name] > USB Redirection > Enable Native USB Redirection (set to **Global setting**)

Sessions > RDP > RDP Sessions > [session name] > Mapping > Enable Drive Mapping (set to **Global setting**)

Assigning a Drive Letter within the Session (Optional)

->In case you not only want to see the drive in the session as e.g. "A on IGEL-123456789", but want to address the drive with a real drive letter within the session, you may run one of these commands:

```
subst T: \\tsclient\t
```

or

```
net use T: \\tsclient\t
```

In this example, "T on IGEL-123456789" is assigned to drive letter T: within the session. You may also assign the mapped drive to another drive letter than is used in its name.

Configuration on the Server Side

On the server side, e.g. with Windows Server 2008R2, a user in the group "Users" with access to the terminal server will have the mapping default. This is true for a newly installed server. But the mapping can be prevented by changing the policies:

> **Do not allow drive redirection** specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format [driveletter] on [computername]. You can use this setting to override this behavior." Source: https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx

How to Auto-Hide Toolbar in Appliance Mode

Environment

IGEL Linux v5.x or newer

Problem

In the appliance mode, the toolbar at the top of the screen is permanently displayed.

You want to configure the toolbar to hide automatically after it loses the focus of the mouse pointer.

Solution

1. In IGEL Setup, go to **System > Registry > userinterface.igel_toolbar.show_always_in_appliance_mode**.
2. Disable **Show toolbar always in appliance mode**.
3. Click **Ok** to save the changes.

For the changes to take effect, you need to restart active appliance mode sessions.

How to Create a Seamless, Transparent User Experience with Appliance Mode

With appliance mode, you can confine a device to a specific session. In appliance mode, the device itself fades in the background, and the session is presented to the user in the most straighforward way. The user will not have to deal with a Linux desktop, multiple login procedures, switching between windows, or device configuration.

Use the appliance mode to allow access only to one specific session. On device startup, the user is directed immediately to the login screen of the virtual desktop.

The appliance mode can be applied to the following session types:

- VMware Horizon
- Citrix Self-Service (for published desktops only, not for published applications)
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- XDMCP for this display

To configure a session that runs in appliance mode:

1. Open the setup and go to **Sessions > Appliance mode**.
2. Choose the session type of the desired session using the drop-down menu **Appliance mode**.
3. Configure your appliance mode session as appropriate.

For further information, see the manual chapter Appliance Mode (see page 1413).

How to Connect to a Citrix Farm

By connecting a Citrix farm, your data and applications are kept centrally on a Citrix farm. Applications must now be delivered instantly to users anywhere on any device.

There are several ways of connecting to a Citrix farm and starting sessions. We describe three best practice variants below:

- Citrix StoreFront (see page 411): Integrates published applications into the IGEL GUI.
- Citrix Self-Service (see page 412): Users will be directed to a web interface where they will find pre-defined published applications and they will be able to add more published applications the server provides.
- Appliance Mode (see page 415): Shows only the web interface of the farm and hides the IGEL GUI completely.

Citrix StoreFront

Prerequisites:

- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates in IGEL OS (see page 764))

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix StoreFront > Server**.
3. Click the **ADD** icon in the **Server location** window.
   The **ADD** mask opens.
4. Enter the names or IP addresses of the services sites.
5. Confirm with **OK**.
6. Click **Citrix StoreFront > Desktop Integration**.
7. Enter "Citrix Storefront" under **Login Session Name**.
8. Choose **Desktop** as the starting method.
9. Click **OK** to save the changes.
   Setup closes.
10. Doubleclick the Citrix icon on the desktop.
    The login window opens.
11. Enter the credentials of a user in the login window.
    The published applications of the Citrix farm will appear on the desktop.
12. Doubleclick an application icon on the desktop to start the program.

Citrix Self-Service

Prerequisites:

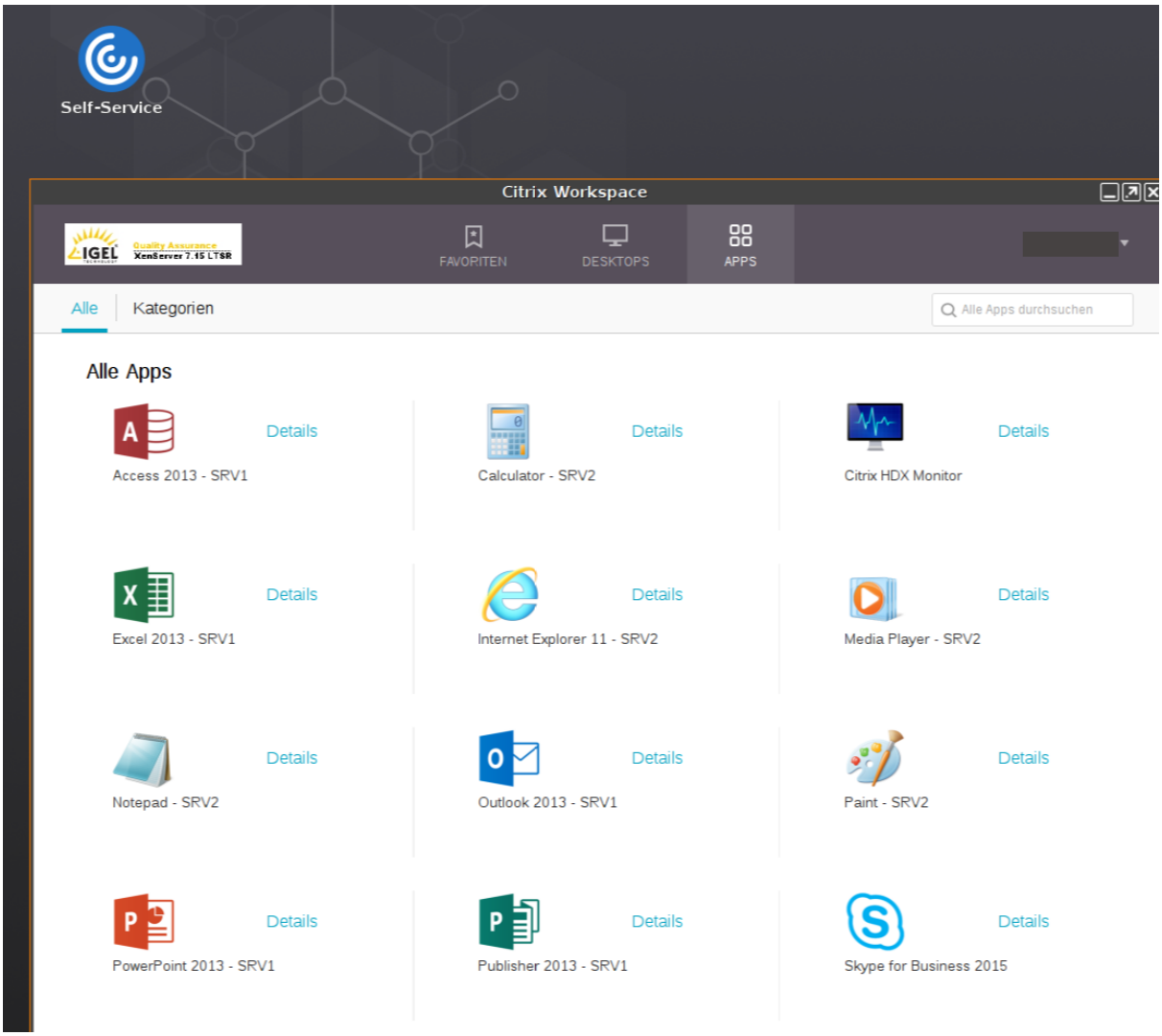
- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates in IGEL OS (see page 764))

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix Self-Service > Server**.
3. Enter the **Server**, the **Path to Store** and the **Store name** of the services sites.
4. Confirm with **OK**.
5. Click **Citrix Self-Service > Desktop Integration**.
6. Enter "Citrix Self-Service" under **Login Session Name**.
7. Choose **Desktop** as the starting method.
8. Click **OK** to save the changes.
   Setup closes.
9. Doubleclick the Citrix icon on the desktop.
   The login window opens.
10. Enter the credentials of a user in the login window.
    The published application icons of the Citrix farm will appear in the Self-Service UI.
11. Doubleclick an application icon to start the program.

Using Citrix Self-Service

1. Start **Citrix Self-Service** e.g. with desktop icon.
2. Log on to the server.
3. Add published applications to the list (**+**-button on the left).
4. Click a published application to start.
5. Use the search bar to find a published application.
6. Use the user's menu to change preferences, server etc.



- Configure Full-Screen Mode (see page 414)

Configure Full-Screen Mode

Use following parameter in your Custom Command script to activate the full-screen mode for *Citrix Self-Service*:

-> `$ICADIR/storebrowse -c FullscreenMode=[0/1/2]`

With following options:

- `0` = The window is not displayed full-screen
- `1` = The window is displayed full-screen
- `2` = The window is displayed maximized and undecorated, which does not mask the desktop environment's taskbar

Appliance Mode

Connecting Citrix via Selfservice:

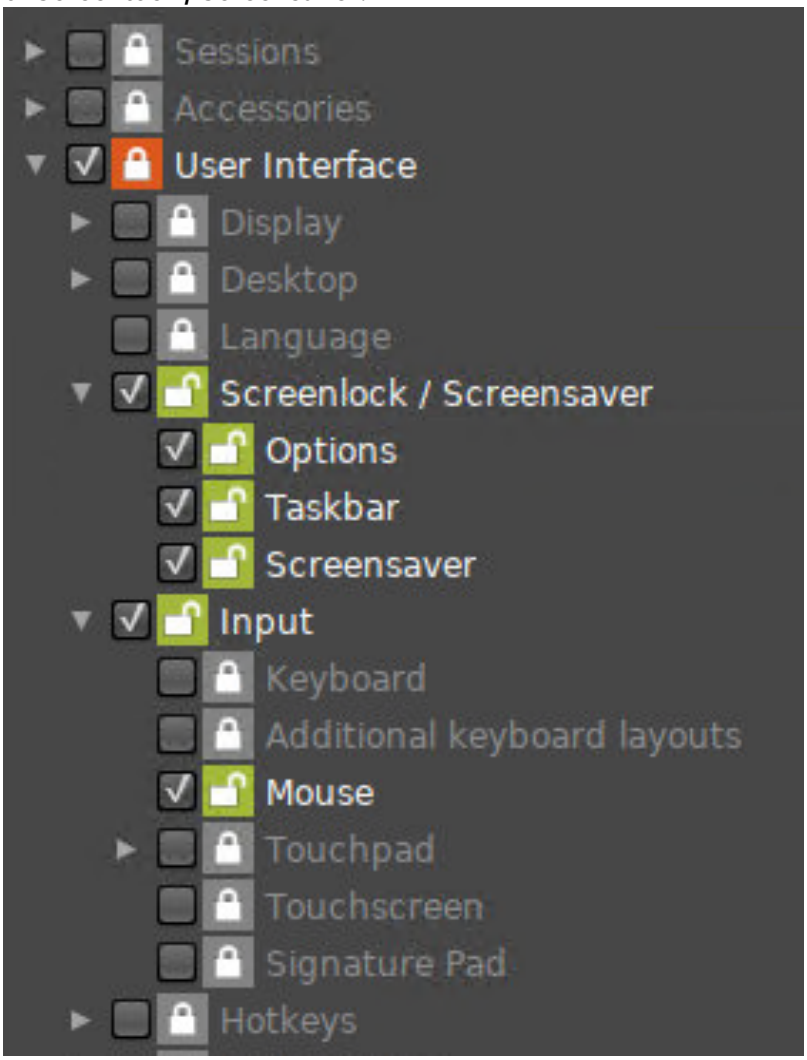
1. Click **Sessions > Appliance Mode** in the configuration tree of the IGEL setup.
2. Select **Citrix Self-Service** under **Appliance mode**.
3. Enter the **URL** of the delivery server.
4. Click **OK** to save the changes and close setup.
5. Follow the instructions on the screen.

How to Create a Self-Service Setup for the User with Quick Settings

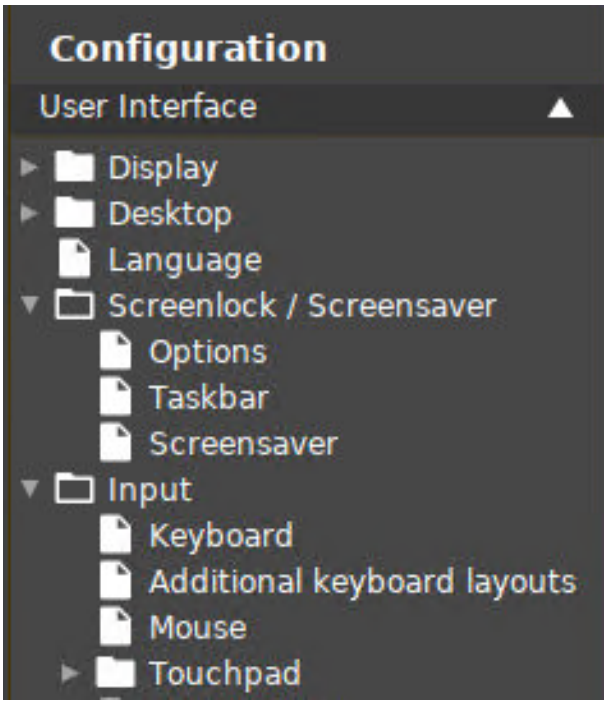
Usually, the user should not have full access to the thin client's setup. However, it may prove useful to enable users to quickly change certain settings by themselves, without even needing a password. Typical examples are settings for keyboard, mouse, or screen. This can be done using the **Quick Settings**.

Here is how to select setup pages for quick setup:

1. Open the setup and go to **Accessories** > **Quick Settings** > **Setup User Permissions**.
2. Select the setup pages to which the user should have access, e. g. **User Interface > Input > Mouse**, or **Screenlock / Screensaver**.



3. Click **Apply** or **Ok**.
   When the user starts **Quick Settings**, the previously selected options are presented.



Quick settings set permissions for setup screens. If you want to set permissions for individual parameters, you can use UMS profiles. For more information, see Profiles in the IGEL UMS[57].

57. https://kb.igel.com/en/universal-management-suite/12.04.120/profiles-in-the-igel-ums

Troubleshooting: Login Failed because of the Expired AD Password

Problem

When you try to log in to a native **Citrix Storefront** session, you get the error message "Login Failed!" because your Active Directory password expired.
You are unable to change your password, because the local login does not provide an option for that.

> Before you follow these instructions, check that the ports are open, maybe you can fix the problem by that:
>
> - Login to Client -> Port: 88
> - Change password -> Port: 464
>
> Here you find an overview of ports of the domain controller: Required Ports to Communicate with Domain Controller[58]

Solution

Enable **Active Directory/Kerberos** authentication for the **Storefront** session. The next time you try to log in to IGEL OS, you will be prompted to change your expired password.

Changing an Expired Active Directory Password

> When using sessions with passthrough authentication, it is essential that you lock your device's screen when leaving it unattended.

Enabling Active Directory/Kerberos Authentication for Storefront Sessions

1. In IGEL setup, go to **Security > Login > Active Directory/Kerberos**.
2. Enable **Login to Active Directory domain**.
3. Go to **Security > Active Directory/Kerberos**.
4. Activate **Enable**.
5. Fill in the **Default domain (fully qualified domain name)**.
6. Go to **Sessions > Citrix > Citrix Storefront > Login**.
7. Enable **Use passthrough authentication**.
8. Click **Apply** or **Ok**.

> Please note that the client must now be locked locally and no longer in the session to prevent another person from entering the session via the passthrough without specifying the password.

58. https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS

Enabling Screenlock

1. In the IGEL setup go to **User Interface > Screenlock / Screensaver**.
2. Enable **Use hotkey**.
3. Under **Modifiers** select `Win`.
4. Under **Hotkey** enter "L".
5. Got to **User Interface > Screenlock / Screensaver > Options**.
6. Enable **User password**.

So the "Win + L" hotkey locks the IGEL client instead of the session desktop.

The AD password must be entered to activate the IGEL clients.

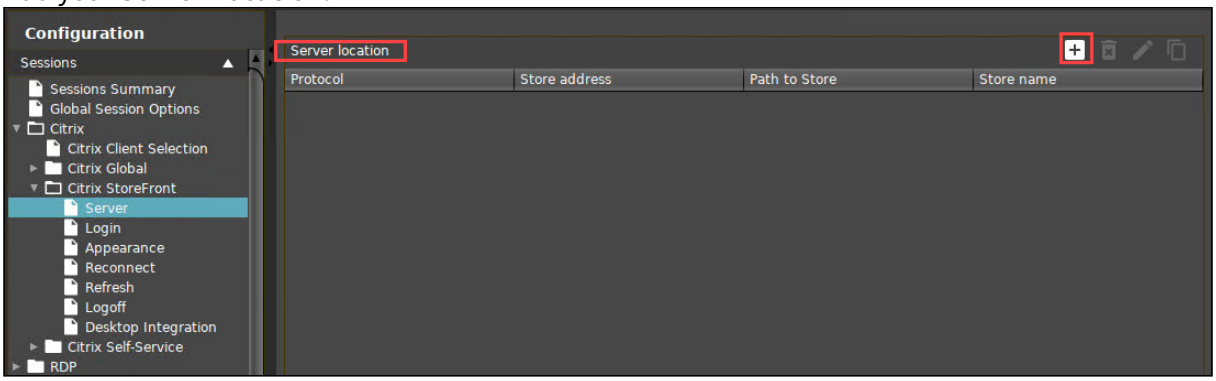
How to Configure Auto Logon for Citrix Virtual Desktops

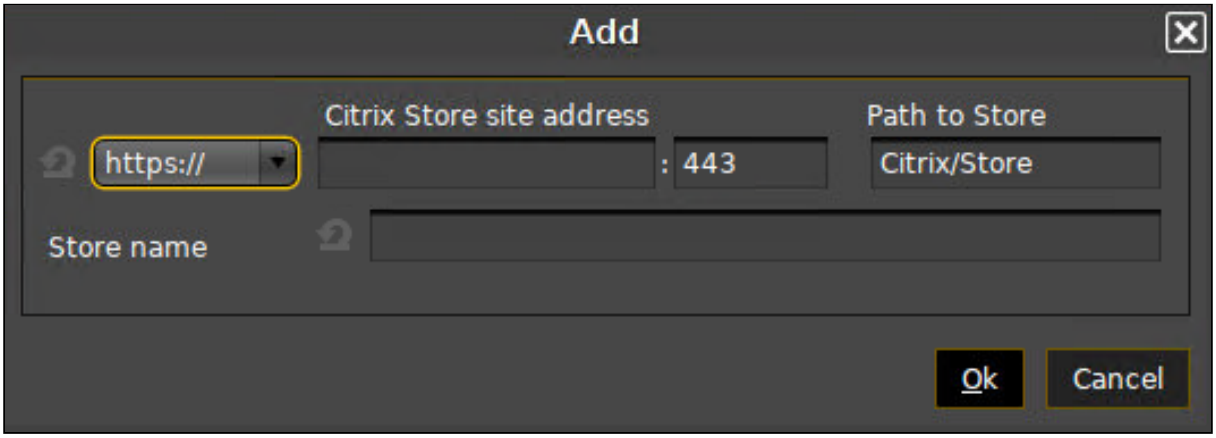
This how-to describes how to configure Auto Logon for Citrix Virtual Desktops.

Steps

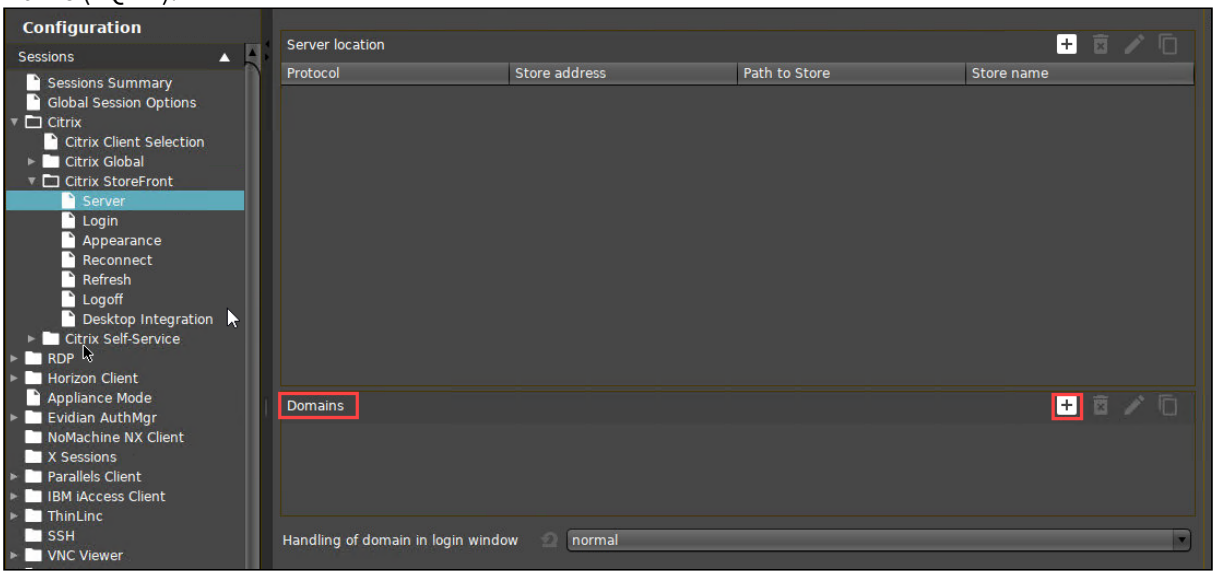
1. In IGEL Setup, go to **Sessions > Citrix > Citrix StoreFront > Server**.

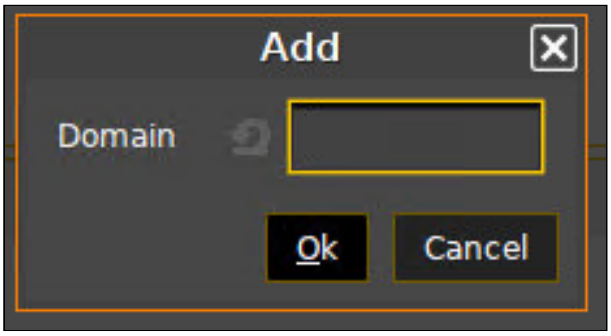
2. Add your **Server Location**.



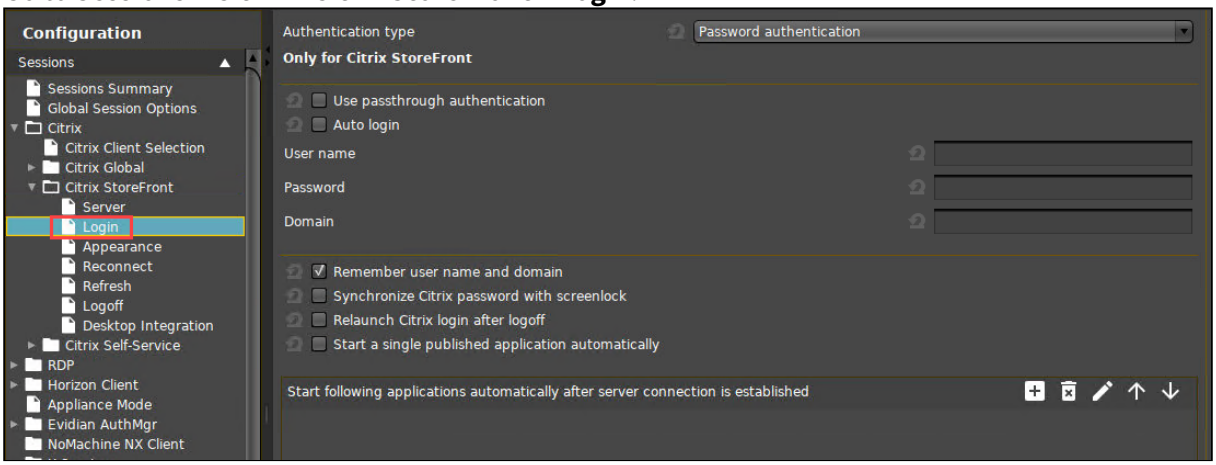


3. Add your Active Directory domain to **Domains**, making sure that you use its Fully Qualified Domain Name (FQDN).

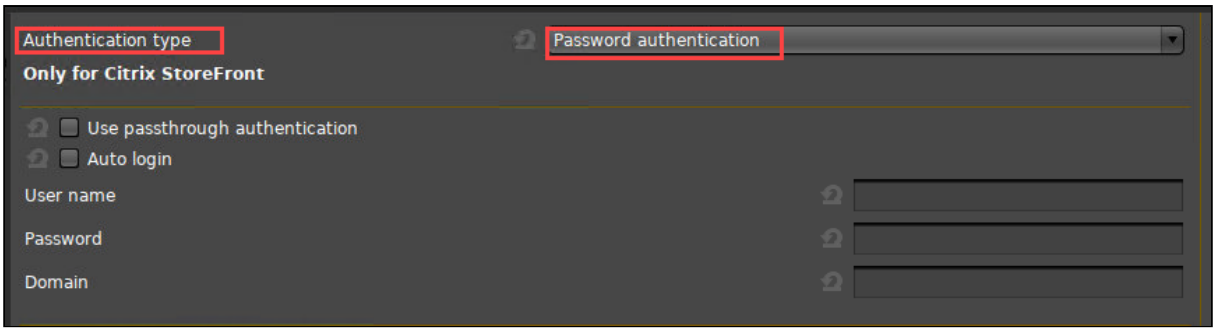




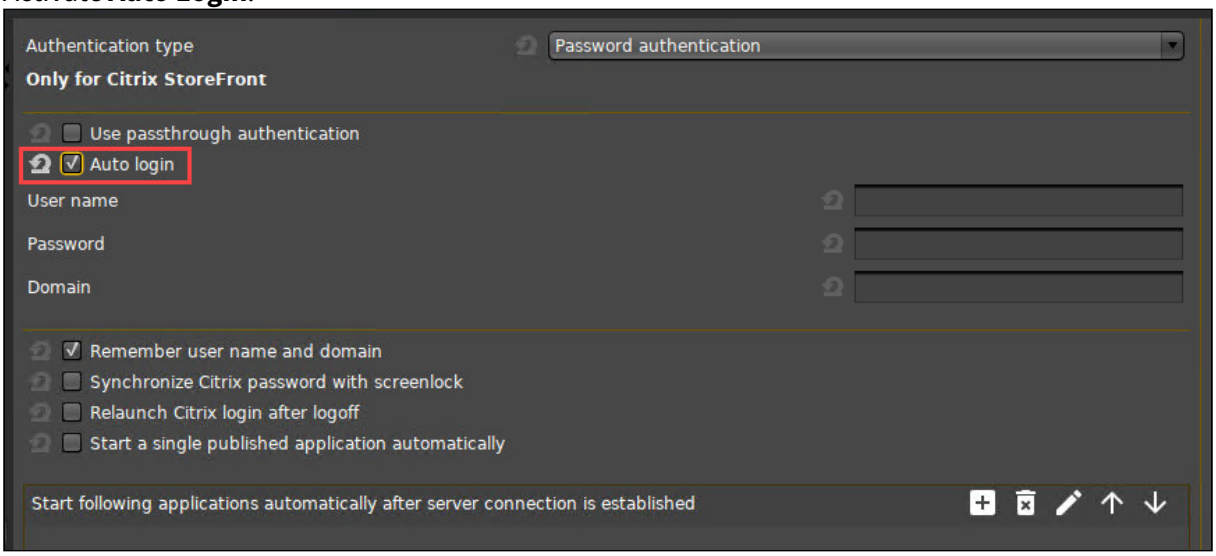
4. Go to **Sessions > Citrix > Citrix StoreFront > Login**.



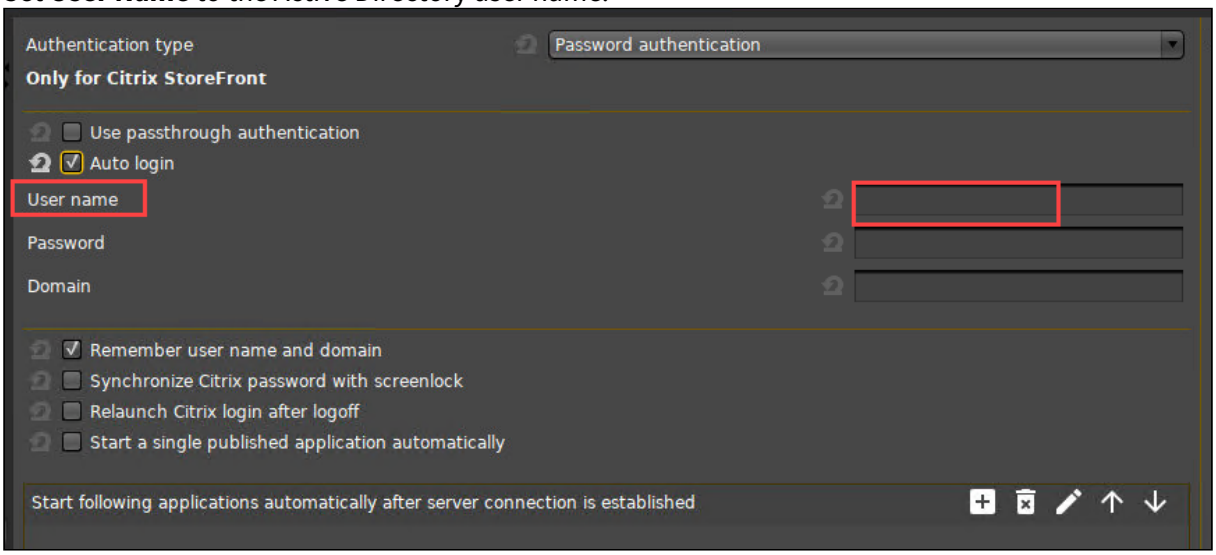
5. Set **Authentication type** to **Password authentication**.



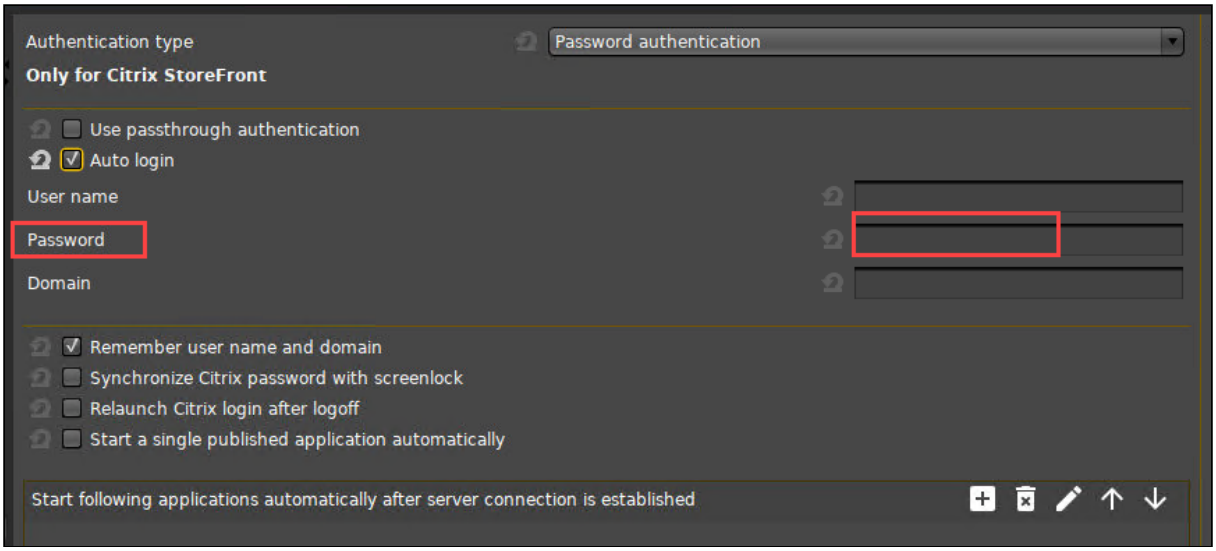
6. Activate **Auto Login**.



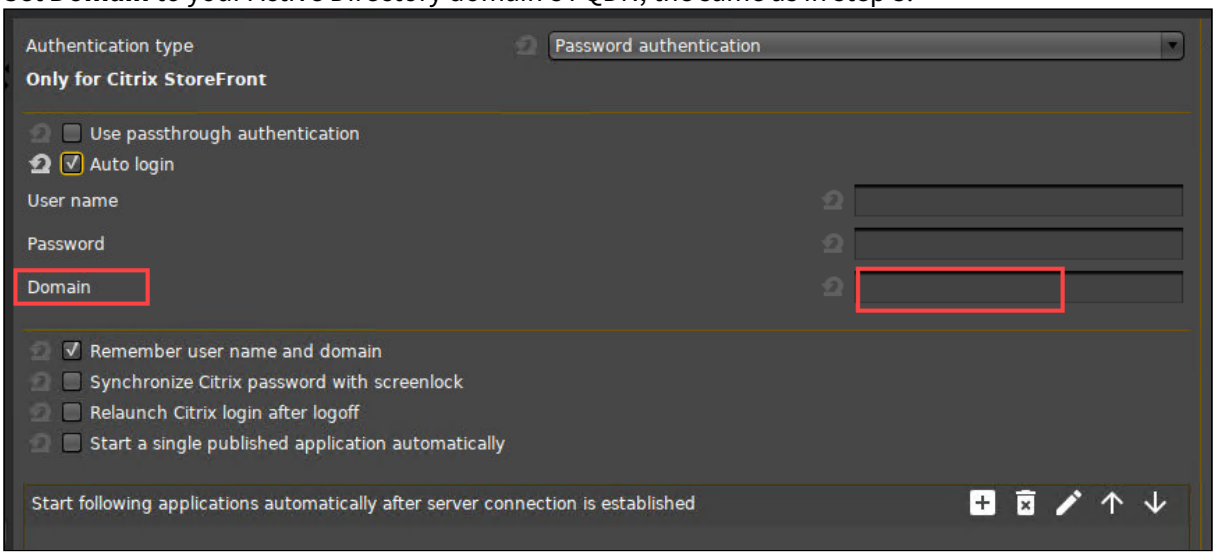
7. Set **User Name** to the Active Directory user name.



8. Set the **Password**.



9. Set **Domain** to your Active Directory domain's FQDN, the same as in step 3.



Force Citrix Logout Using Hotkey

You will find the instructions under Citrix: Freeze at Logout (see page 425).

This page is due for deletion. Please check the above link and use it in the future.

Citrix: Freeze at Logout

Symptom

A user tries to log out from a Citrix session but the session does not respond.

Example: Once you connect to a Citrix session, everything works. After having reconnected and disconnected several times, you log out. The window freezes while the logout screen is shown.

Solution

▶ Try to use another Citrix Receiver version: **Sessions > Citrix > Citrix Client Selection > Citrix client version**.

OR

▶ Troubleshoot the issue with your Citrix infrastructure to discover why the session is not closing when the `wfica` process makes the call for disconnection.

Workaround

As a less recommended alternative, you can configure a hotkey to force a logout in such situations. Note, however, that this workaround can cause issues with hung sessions on the Citrix servers.

To configure a logout hotkey:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Application**.
2. Click ⊞ to create a new **Custom Application** and name it e.g. "Kill Citrix Sessions".
3. Disable all **Starting Methods** for this session.
4. Enable **Hotkey**.
5. Choose e.g. `Ctrl|Alt` as **Modifiers** and define `C` (for "Citrix) as **Key**.
6. Go to **System > Firmware Customization > Custom Application > Kill Citrix Sessions > Settings**.
7. Enter an **Icon name**.
8. Enter `/tmp/kill_citrix` as **Command**.
9. Go to **System > Firmware Customization > Custom Commands > Desktop**.
10. In the field **Desktop initialization** enter following command in one line:
    ```
    echo -e "#! /bin/bash\n\nps -eo comm,pid | grep ^wfica | while read c p tail; do echo \$p; done | xargs -r kill -TERM" >/tmp/kill_citrix; chmod 755 /tmp/kill_citrix
    ```
11. Click **Apply** and reboot the device.

To configure the hotkey for a group of devices, you can alternatively create a profile or use this one: profile_KillCitrixSessionsViaHotkey.xml (see page 425).

Here you can learn how to import a profile: Importing a Profile and Firmware (see page 425).

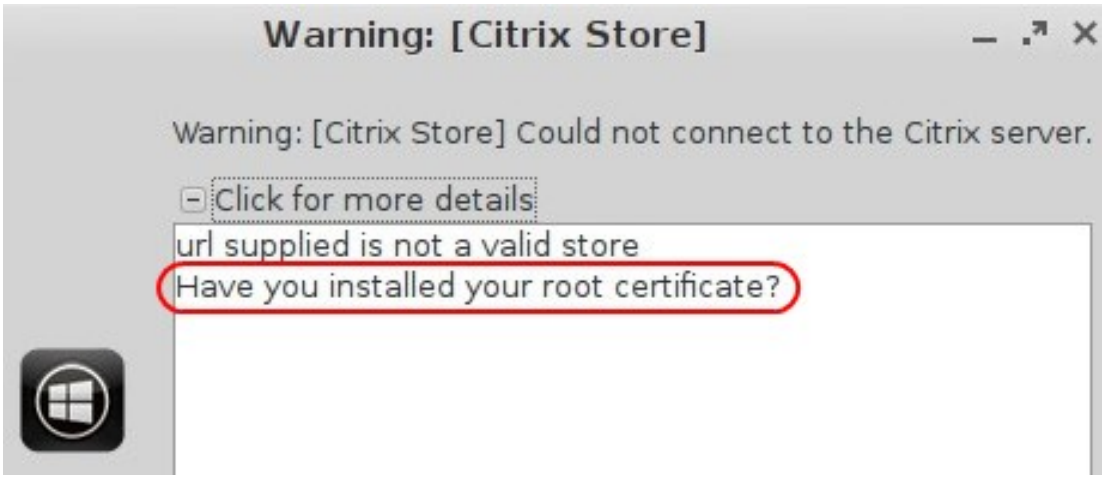
Warning Message: [Citrix Store] Could Not Connect to the Citrix Server

Environment

- You are using Citrix Receiver 13.0.x or newer.
- You have a session of the type Citrix StoreFront configured.

Symptom

- When establishing the connection, a warning message appears:
  `Warning: [Citrix Store] Could not connect to the Citrix server.`



or

Problem

Citrix Receiver 13.0.x or newer on Linux only supports connections via HTTPS, and you have to make sure the device has a valid root certificate of the Certificate Authority (CA) available. If the root certificate is missing, the connection will fail.

Solution

Install an appropriate root certificate on the device to allow HTTPS connections to your Citrix Server.

For information on how to distribute the certificate, see Deploying Trusted Root Certificates in IGEL OS (see page 764).

How to Set Up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec

This document describes how to activate a hardware-accelerated H.264 deep compression codec for Citrix sessions.

Prerequisites

- Licensed IGEL Multimedia Codec Pack
- IGEL UD device offering hardware video acceleration, see the FAQ Hardware Video Acceleration on IGEL OS (see page 1180).
- Citrix XenApp / XenDesktop server with active H.264 display mode
  See http://support.citrix.com/article/CTX200370 to learn how to determine the display mode.

Activating the Codec

1. In Setup, go to **System > Firmware Customization > Features**.
2. Enable **Hardware Video Acceleration**.
3. Go to **Sessions > Citrix > Citrix Client Selection.**
4. Select the **Citrix Client Version**.
5. Go to **Sessions > Citrix > Citrix Global > Codec**.
6. Set **Graphical Codec** to **H.264 Deep Compression Codec**.
7. Enable **Accelerated H.264 Deep Compression Codec**.

Known issues on VIA-based IGEL devices UD3-LX 40/41/42 and UD10-LX:

- Hardware-accelerated HDX only works with 256 MB video memory or more. Video memory must be adjusted in the system BIOS. The default is 128 MB.
- Seamless window mode is not supported.
- Desktop sessions spanning 2 monitors are not supported.
- Desktop sessions on rotated screens may flicker (depending on the screen resolution).

If you use the **Citrix Receiver 13.5** or older in combination with a **Citrix Server 7.15**, the **Always Lossless** option for the **Visual Quality** policy will not work under Linux.
With IGEL Linux version 10.05.100 the **Build to Lossless** option for the **Visual Quality** policy will work on the condition that you are using **Citrix Receiver 13.6** or younger and the **Use Video Codec** policy is set to **For actively changing regions**.

Troubleshooting: Highly Secured XenServer has Problems with LD_BIND_NOW Workaround

Problem

You want to launch multiple desktop sessions with RTME and H.264 acceleration, but it doesn't work.

Solution

1. In **IGEL Setup**, go to **System > Registry > ica > workaround-dual-rtme** (Search parameter: **ica.workaround-dual-rtme**)
2. Enable **Activate workaround for dual RTME sessions and H264 acceleration**.
3. Click **Apply** or **Ok** to save the changes.

> This registry key should not be used if "Enable Secure ICA" is active for the specific delivery group. You have to decide if you want to use the registry key or to reduce security.

Troubleshooting: Workaround for Citrix Receiver X Error

Problem

When starting Citrix XenApp you get the following Citrix Receiver errors on your IGEL OS devices:

```
The X Request 55.0 caused error: "9: BadDrawable (invalid Pixmap or Window parameter)"
```

```
The X Request 60.0 caused error: "13: BadGC (invalid GC parameter)".
```

Environment

- Citrix XenApp 7.15
- Citrix Receiver e.g. 13.2, 13.3, 13.7, 13.8

Solution

Two parameters have to be activated in IGEL Setup:

1. Go to **System > Registry > ica > forceignorexerrors**.
2. Activate **Suppress X error message boxes**.
3. Go to **System > Registry > ica > wfclient > ignorexerrors**.
4. Activate **IgnoreXErrors** and pass the parameters: `55.0/9, 60.0/13`

See also the corresponding entry in the Citrix forum[59].

59. https://discussions.citrix.com/topic/393872-possible-workaround-citrix-receiver-x-error-on-linux-thin-clients/

Troubleshooting: Citrix HTML5 Receiver Issue

Affected Versions

- IGEL OS 10.05.100 or higher
- IGEL OS 11.01.100 or higher

Issue

Due to the abolition of plugin technology in Firefox 60+, the Workspace app installed under Linux is no longer automatically recognized.

Solution

1. If your device has IGEL OS 10.05, update to IGEL OS 10.06; if applicable, you can also upgrade to IGEL OS 11.02. If your device has IGEL OS 11.01, update to IGEL OS 11.02.
   IGEL OS 10.06 and IGEL OS 11.02 have been adapted for a workaround that requires server-side modifications.
2. Change the server-side settings according to the instructions under https://support.citrix.com/article/CTX237727.

How to Configure Macbook Keyboard Layout inside Citrix Session

To get the Macbook keyboard layout working correctly inside Citrix sessions, proceed as follows:

1. Under **Sessions > Citrix > Citrix Global > Keyboard > Keyboard mapping file**, select "Linux".
2. Under **User Interface > Input > Keyboard > Keyboard type**, select "Macbook".
   All other keyboard layout settings can be left unchanged, i.e. as set by default.

In order to type special characters like € and #, use the right-hand Alt/Option key, not the left-hand key.

How to Use Lync / Skype for Business with Citrix HDX RealTime Optimization Pack

Issue

You want to use Microsoft Lync or Skype for Business via a Citrix session with IGEL OS devices.

Solution

IGEL OS comes with Citrix HDX RealTime Media Engine (RTME) preinstalled: Setup **> Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**. See also HDX Multimedia Settings for an IGEL OS Citrix Session (see page 1276).

- IGEL OS 11.04.100 or higher contains RTME 2.9 (activated by default).
- IGEL OS 11.02.100 or higher contains RTME 2.8 (activated by default).
- IGEL OS 11.01.100 contains RTME 2.7 (disabled by default).
- IGEL OS 10.06.100 contains RTME 2.8 (disabled by default).
- IGEL OS 10.05.500 contains RTME 2.6 (disabled by default).
- IGEL OS 10.05.100 contains RTME 2.6 (disabled by default).

For further information, see Citrix HDX RealTime Optimization Pack[60].

60. https://docs.citrix.com/en-us/hdx-optimization/

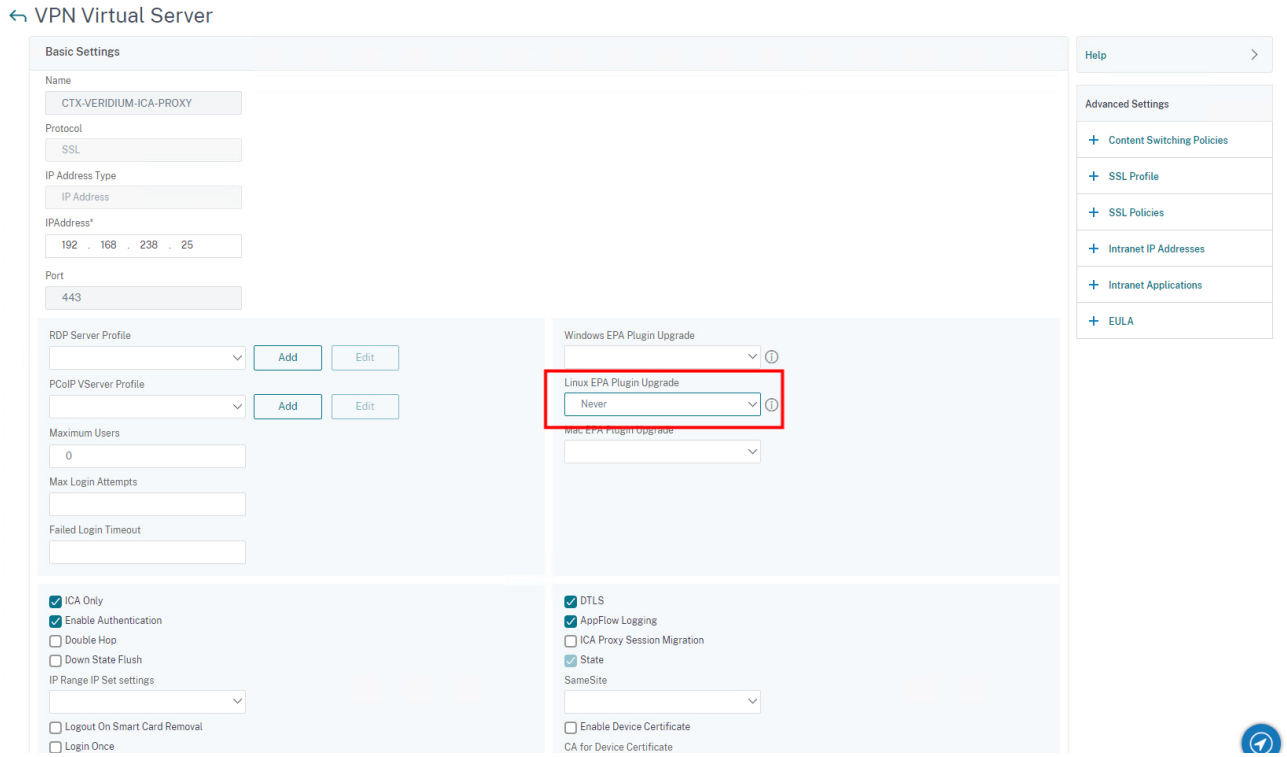
Citrix Advanced Endpoint Analysis (EPA) Client on IGEL OS

This article is valid for IGEL OS 11.08.290 or higher.

As of version 11.08.290, the Citrix Advanced Endpoint Analysis (EPA) client has been integrated into IGEL OS. On the client side, no configuration is necessary. When the Netscaler URL is opened in the device's browser (Chromium or Firefox), the NSEPA checks configured in Netscaler are performed automatically.

As dynamic updates are not possible in IGEL OS, due to the read-only system, you must disable the automatic update in Netscaler.

->In Netscaler, set **Linux EPA Plugin Upgrade** to **Never**.



Citrix Netscaler Gateway Client (NSGClient) for Netscaler VPN Connections

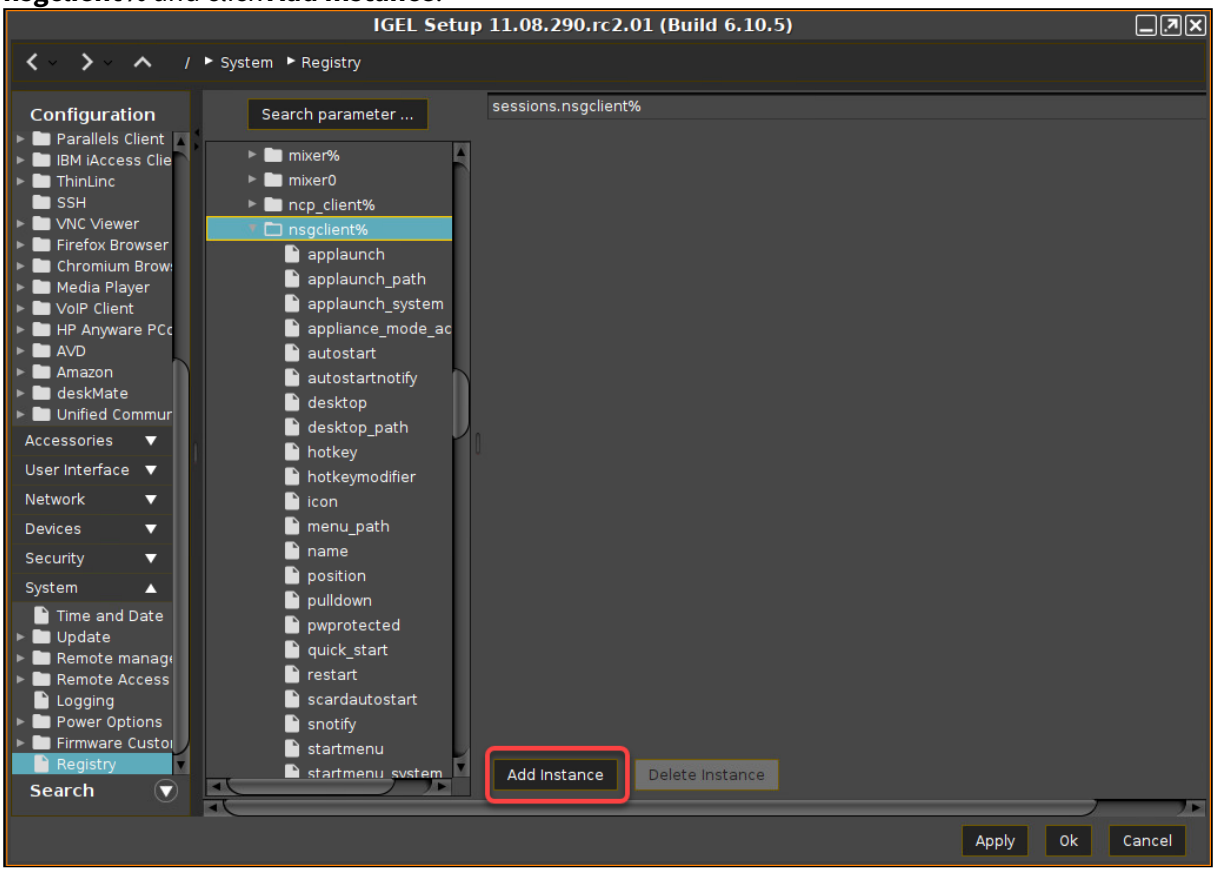
This article is valid for IGEL OS 11.08.290 or higher.

As of version 11.08.290, the Citrix Netscaler Gateway Client (NSGClient) for Netscaler VPN Connections has been integrated into IGEL OS. On the client side, no configuration is necessary. When the Netscaler URL is opened in the device's browser (Chromium or Firefox), the Citrix Netscaler Gateway Client is configured automatically.

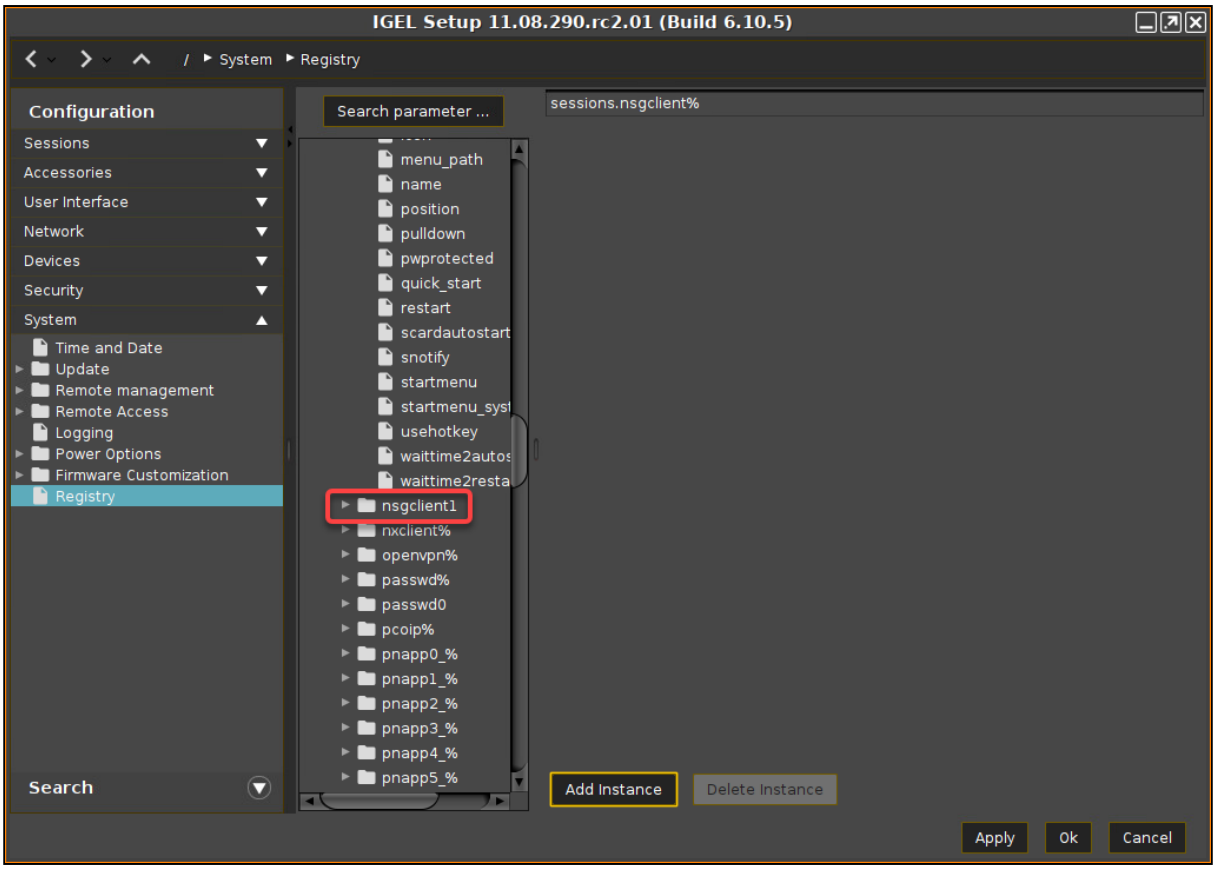
Additionally, a starter icon can be configured.

Configuring a Starter Icon on the Desktop

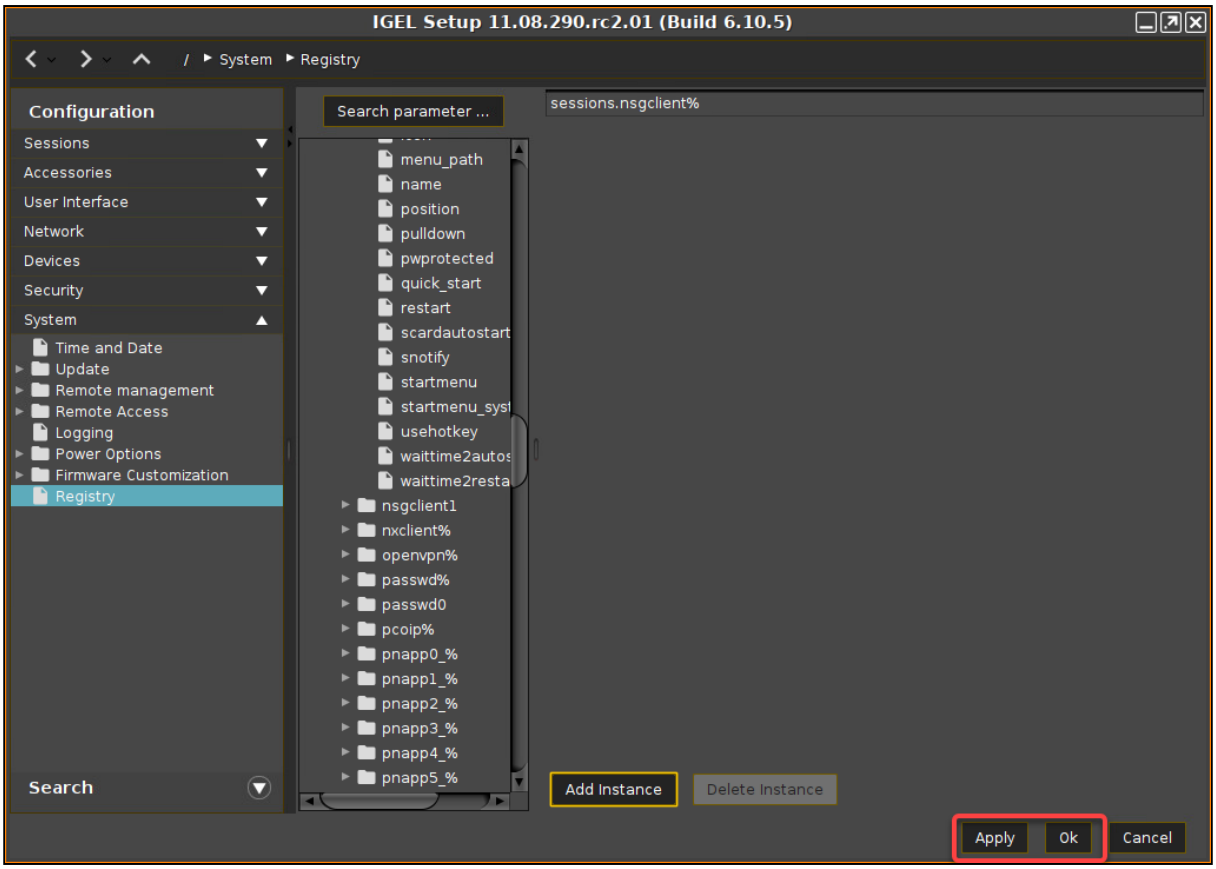
1. In the UMS Profile Configurator or the local IGEL Setup, go to **System > Registry > sessions > nsgclient%** and click **Add Instance**.



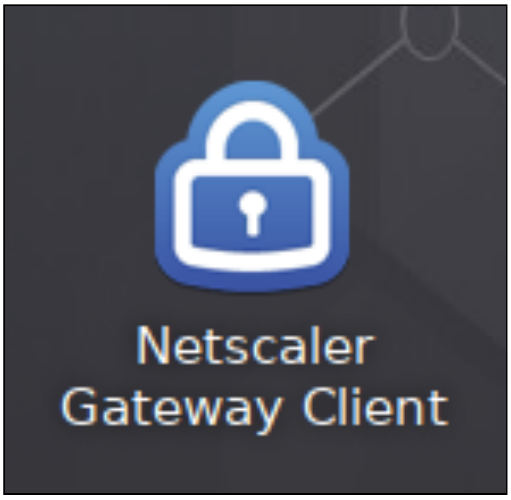
The instance **nsgclient1** is created.



2. Click **Apply** or **Ok** to save your changes.

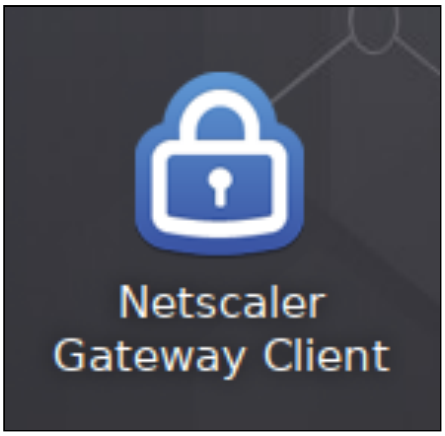


An starter icon is created on the device's desktop.



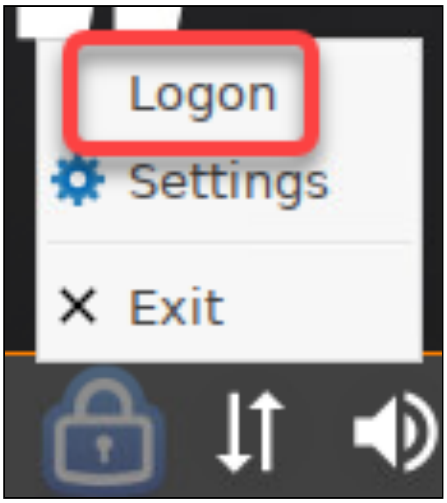
Starting the Netscaler Gateway Client with the Starter Icon

1. Click on the starter icon of the Netscaler Gateway Client.

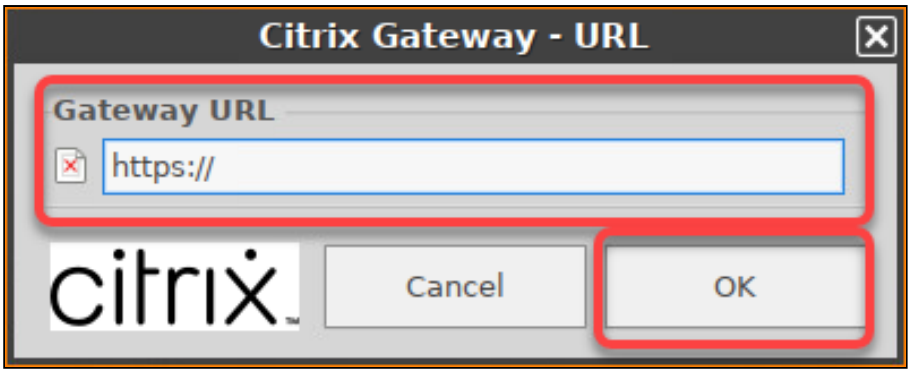


An icon is created in the system tray.

2. Click on the system tray icon and select **Logon**.



3. Enter the **Gateway URL** and click **OK** to start the connection.


Citrix Gateway - URL
Gateway URL
https://
citrix
Cancel
OK

Troubleshooting: Unexpected Keyboard Layout in a Citrix Session

Problem

When a Citrix session has started, the keyboard layout changes in an unexpected way. On the local system, the keyboard layout may still be as expected.

The problem has been reported for the following keyboard layouts:

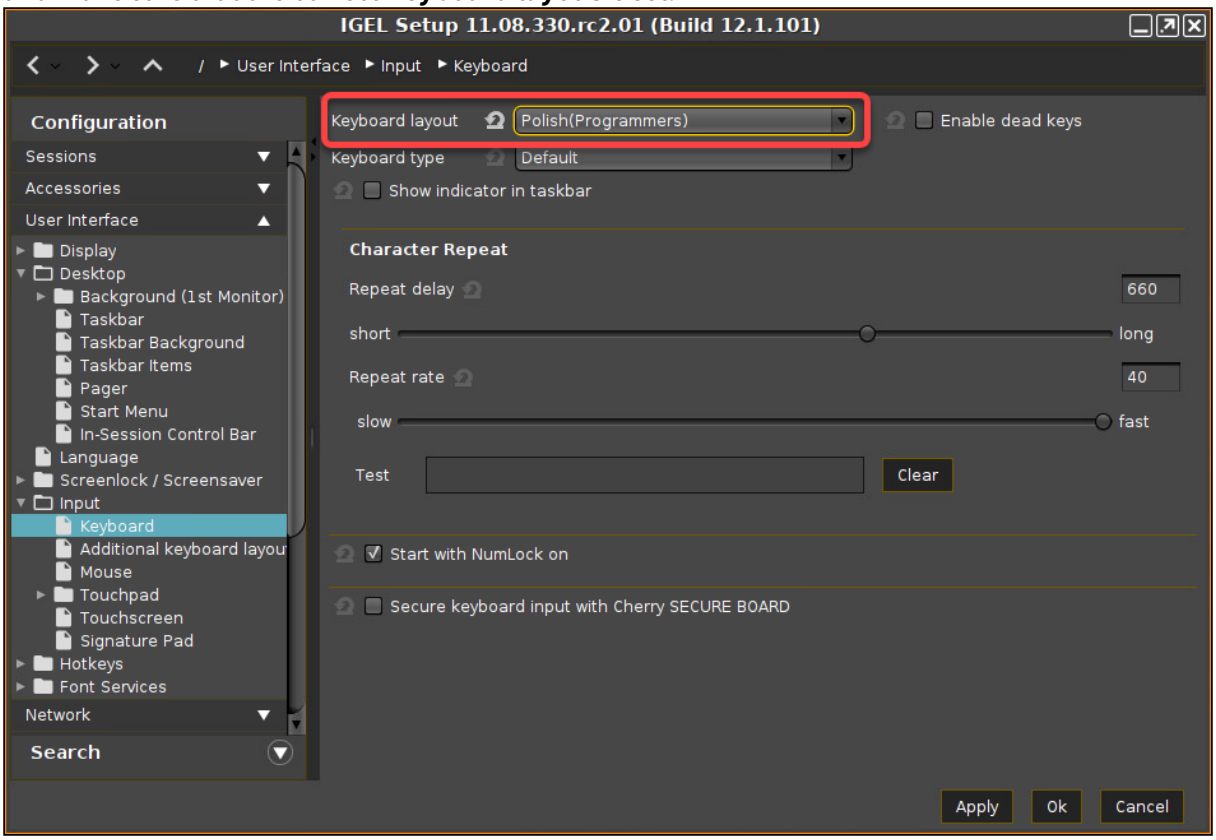
- **English(International)** with dead keys enabled
- **Polish (Programmers)**

Environment

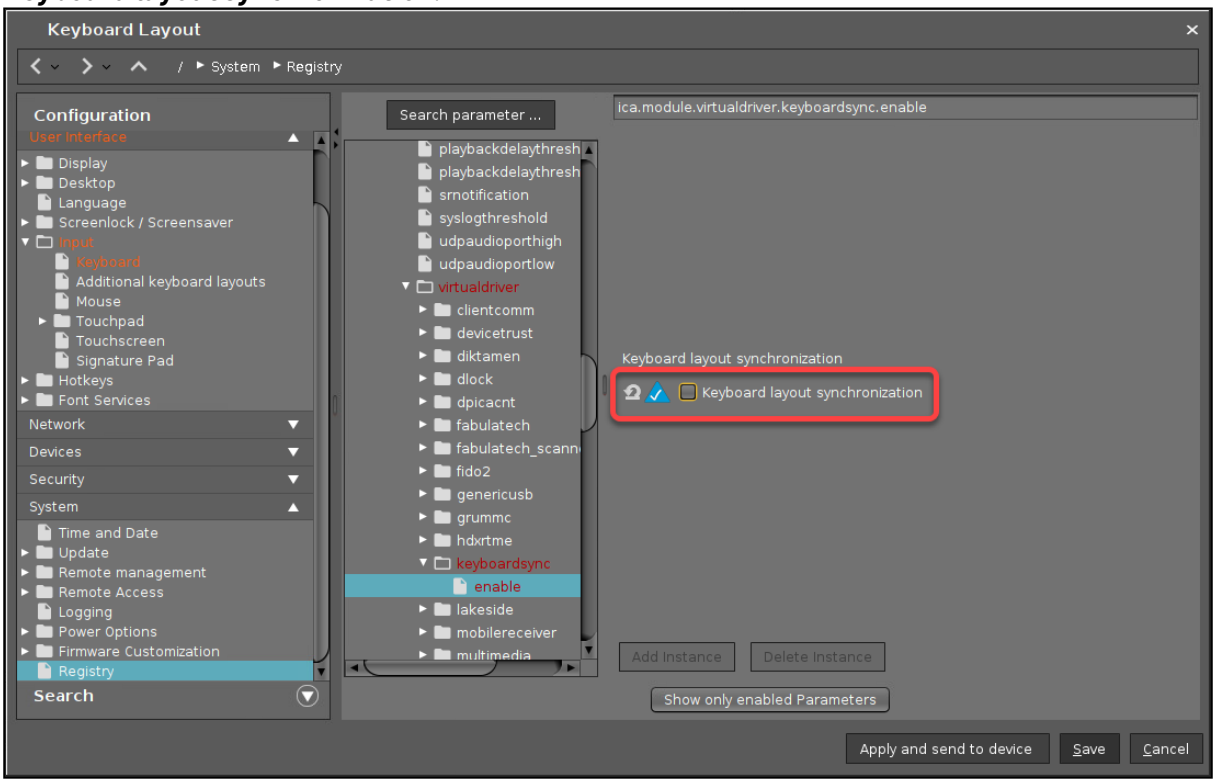
- Devices with IGEL OS 11.07.110 or higher (all IGEL OS versions that contain Citrix Workspace App 2203 or higher)

Solution

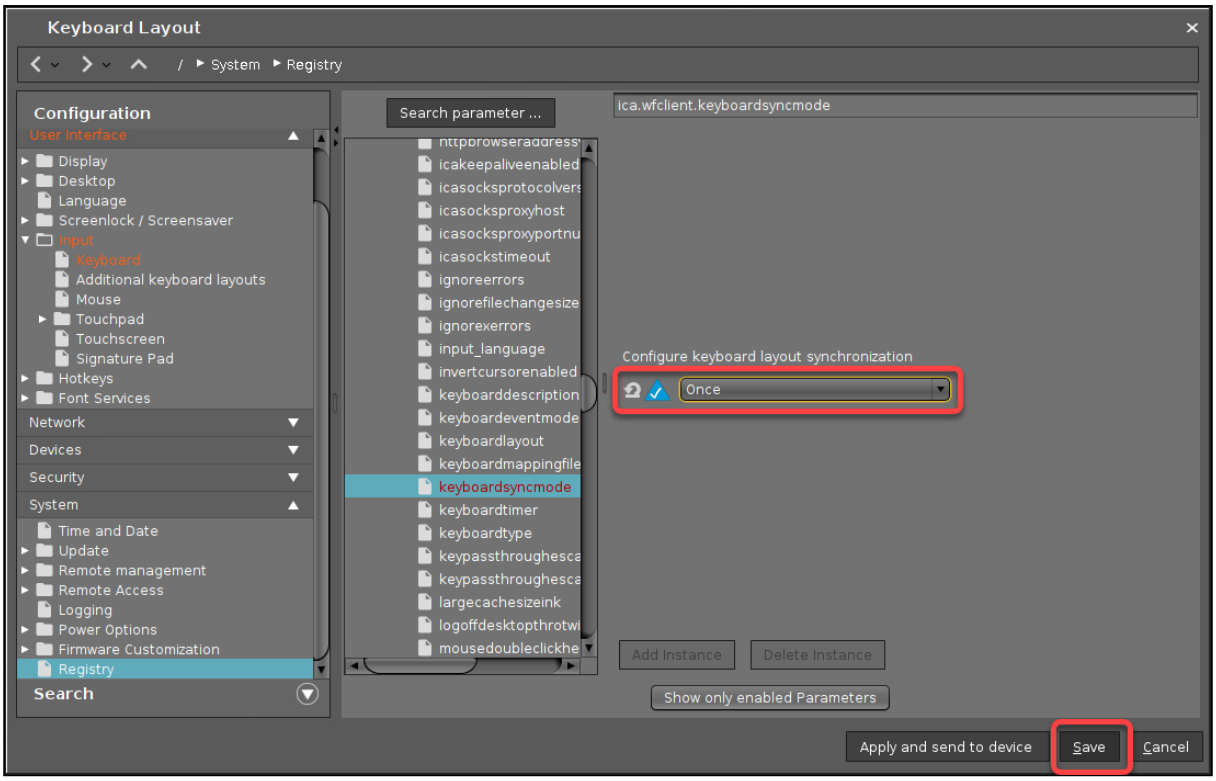
1. Open the UMS configuration dialog or the local Setup, go to **User Interface > Input > Keyboard**, and make sure that the correct **Keyboard layout** is set.



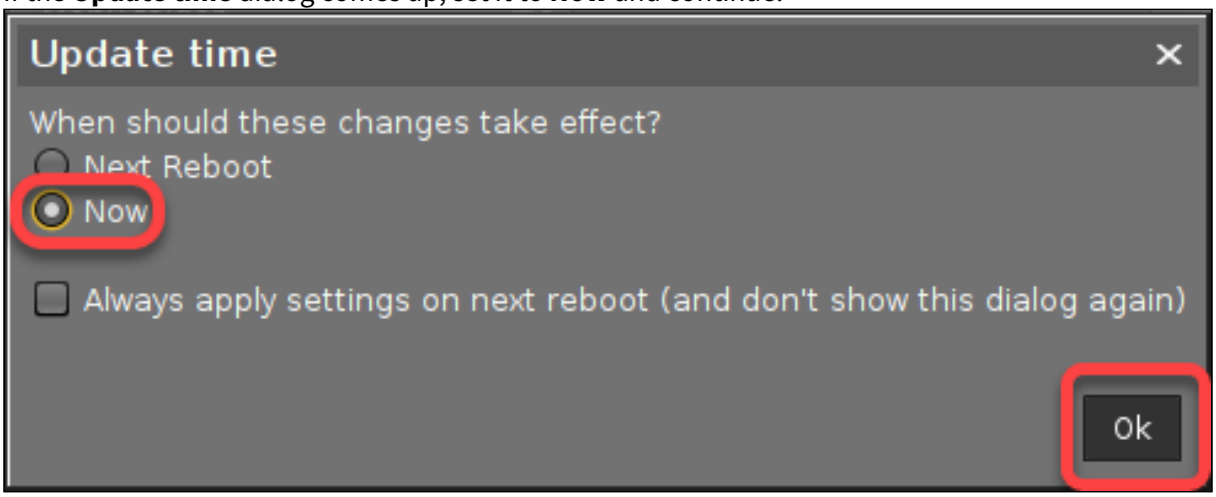
2. Go to **System > Registry > ica > module > virtualdriver > keyboardsync > enable** and disable **Keyboard layout synchronization**.



3. Go to **System > Registry > ica > wfclient> keyboardsyncmode**, set **Configure keyboard layout synchronization** to **Once**, and then confirm your settings with **Save**.



4. If the **Update time** dialog comes up, set it to **Now** and continue.



When the user logs in to the Citrix session, the keyboard layout should be correct.

How to Use Font Smoothing (ClearType) in Citrix Sessions

Symptom

- You have set **Font Smoothing** to *ClearType* in **IGEL Setup > Sessions > Citrix > Citrix Global > Window > Font smoothing (Off / Standard / ClearType)**
- *ClearType* does not work for *Citrix PNAgent* / *Webinterface* sessions.

Problem

ClearType is not supported in *PNAgent / Webinterface* sessions because *Citrix Receiver* uses *Windows* settings which are not present on the Linux client.

Solution

All *Citrix Receivers* up to version 12.x do not use `wfclient.ini` to configure **Font Smoothing**. To force *Webinterface*, *PNAgent/XenApp* to enable **Font Smoothing** proceed as follows:

PNAgent / XenApp:

1. On the *Citrix* server open `C:\inetpub\wwwroot\citrix\pnagent\config\default.ica`.
2. Go to section **Application**.
3. Add new line `FontSmoothingType=3`.
4. Save and close the file.

Webinterface:

1. On the *Citrix* server open `C:\inetpub\wwwroot\citrix\xenapp\config\default.ica`.
2. Go to section **Application**.
3. Add new line `FontSmoothingType=3`.
4. Save and close the file.

> If you installed the *Webinterface* site to a different location, please change the path accordingly.

FontSmoothingType parameter options:

- `0` = No smoothing
- `1` = No smoothing

- `2` = Standard smoothing
- `3` = *ClearType* (horizontal sub-pixel) smoothing (default)

> **Legal Note**
>
> IGEL's Terms & Conditions[61] apply.

61. https://www.igel.com/terms-conditions/

Citrix Feature Matrix

According to the details provided by the vendor, the following Citrix Client features are supported with Citrix Workspace App 2009:

> For details on the Citrix Clients that are built into your version of IGEL OS, see IGEL OS Release Notes (see page 2282) > Notes for Release [your version] > Component Versions [your version].
> See also the original document at https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-workspace-app-feature-matrix.pdf.

Category	Feature	Supported
Citrix Workspace	Citrix Virtual Apps	yes
	Citrix Virtual Desktops	yes
	Citrix Content Collaboration (Citrix Files)	no
	Citrix Access Control Service	no
	Citrix Workspace Browser	no
	SaaS/Webapps with SSO	yes
	Citrix Mobile Apps	no
	Intelligent Workspace features	no
Endpoint Management	Auto configure using DNS for Email Discovery	no
	Centralized Management Settings	yes
	App Store Updates / Citrix Auto updates	no
UI	Desktop Viewer/Toolbar	yes
	Multi-tasking	yes
	Follow Me Sessions (Workspace Control)	yes
HDX Host Core	Adaptive transport	yes
	SDWAN support	yes
	Session reliability	yes
	Auto-client Reconnect	yes
	Bi-directional Content redirection	no
	URL redirection	yes
	File open in Citrix Workspace app	yes

Category	Feature	Supported
	Browser content redirection	yes
	Multiport ICA	yes
HDX IO / Devices / Printing	Local Printing	yes
	Generic USB Redirection	yes
	Client drive mapping / File Transfer****	yes
HDX Integration	Local App Access	no
	Multi-touch	no
	Mobility Pack	no
	HDX Insight	yes
	HDX Insight with NSAP VC	yes
	EUEM Experience Matrix	yes
	Session Sharing	yes
HDX Multi-media	Audio Playback	yes
	Bi-directional Audio (VoIP)	yes
	Web-cam redirection	yes
	Video playback	yes
	Flash redirection	yes
	Microsoft Teams Optimization	yes
	Skype for business Optimization pack	yes
	Cisco Jabber Unified Communications Optimization	yes
	Windows Multimedia redirection	yes
	UDP Audio	yes (not with NSG)
Security	TLS 1.2	yes
	TLS 1.0/1.1	yes
	DTLS 1.0	yes
	DTLS 1.2	no
	SHA2 Cert	yes

Category	Feature	Supported
	Smart Access	yes
	Remote Access via Citrix Gateway	yes
	Workspace for Web Access	yes
	IPV6	yes
HDX Graphics	H.264-enhanced SuperCodec	yes
	Client hardware acceleration	yes
	3DPro Graphics	yes
	External Monitor Support	yes
	Desktop Composition redirection	no
	True Multi Monitor	yes
	Location Based Services (Location available via API-description)	no
Authentication	Federated Authentication (SAML/Microsoft Entra ID)	yes
	NetScaler Full VPN	yes
	RSA Soft Token	no
	Challenge Response SMS (Radius)	no
	User Cert Auth via NetScaler Gateway (via Browser Only)	no
	Smart Card (CAC,PIV Etc.)	yes
	Proximity/Contactless Card	yes
	Credential insertion (E.g.. Fast Connect, Storebrowse)	yes
	Pass Through Authentication	no
	Save credentials *(on prem and only SF)	no
	NetScaler nFactor Authentication	yes
	Netscaler Native OTP	yes
	Biometric Authentication (Touch ID, Face ID..)	no
	Single Sign-On to Citrix Files App	no
	Single Sign on to Citrix Mobile apps	no

Category	Feature	Supported
	Anonymous Store Access	yes
Keyboard Enhancements	Dynamic Keyboard Layout Synchronization with Windows VDA Note: Dynamic keyboard layout sync for non-Windows receivers requires enablement of the Unicode Keyboard Layout Mapping feature on the Windows VDA.	yes
	Unicode Keyboard Layout Mapping with Windows VDA	yes
	Client IME Enhancements with Windows VDA	no
	Language Bar Show/Hide with Windows VDA Applications	no
	Option Key mapping for server-side IME input mode on Windows VDA	no
	Dynamic Keyboard Layout Synchronization with Linux VDA	yes
	Client IME Enhancements with Linux VDA	no
	Language Bar support for Linux VDA Applications	yes

RDP

- How to Map USB Storage Media into RDP Sessions (see page 450)
- FAQ: What Is the String for Token-Based Load Balancing? (see page 452)
- How to Enable RDP Fabulatech Scanner Redirection (see page 453)
- How to Configure RDP RemoteApp Parameter Settings (see page 455)
- How to Enhance RDP Performance (see page 457)
- Troubleshooting: RDP Session playing Sound: Error RDPSND_NEGOTIATE (see page 458)
- Troubleshooting: Crackling and Audio Dropouts in RDP Sessions (see page 459)
- Troubleshooting: Login Failed Because of Expired AD Password (see page 461)
- Troubleshooting: User Has to Provide Credentials Twice for RDP Logon (see page 463)
- Bad Sound Quality of Flash/HTML Videos in RDP Session (see page 465)

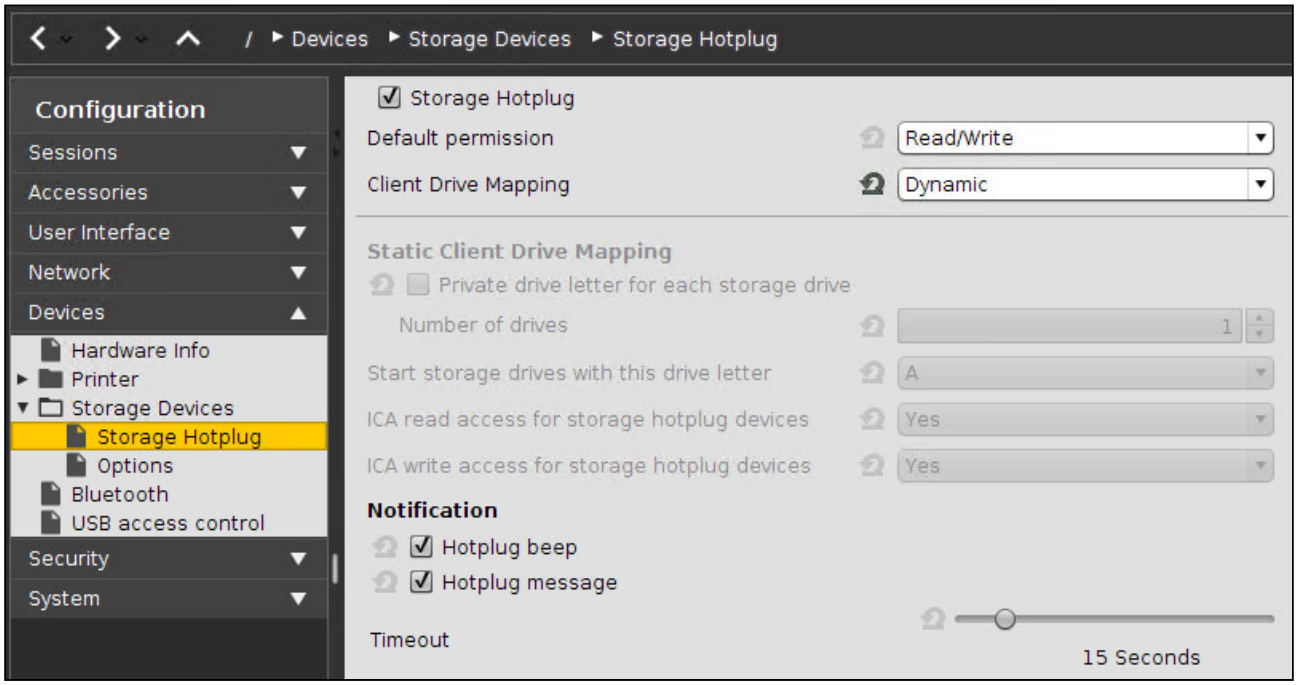
How to Map USB Storage Media into RDP Sessions

How to configure USB Storage mapping so that users can access USB storage media attached to the IGEL LX Client within RDP sessions?

Solution:

The mapping of USB storage devices is possible for "usb mass storage class" devices. The storage of smartphones and digital cameras is usually accessed via the MTP protocol. Mobile device access via MTP is available with IGEL Linux 10.04.100 or higher; for more information see the how-to Using Mobile Device Access (see page 1076).

Basic Configuration of the Client



Within the IGEL Setup or an UMS profile you basically need to configure these parameters:

->Activate **Devices > Storage Devices > Storage Hotplug > Client drive mapping > Dynamic**. This option activates dynamic client drive mapping. It automatically recognizes new storage media as they are connected to the thin client. The thin client beeps and shows a notification while it mounts the new device. The storage devices automatically become usable on the thin client and in Citrix ICA Sessions.

Mounted devices need to be unmounted before they are removed to ensure data integrity. This can be done via the **Disk Utility**, the new **Safely Remove Hardware** Tool or a tray icon.

Additional Parameters to Check

->The following parameters are set by default, thus storage mapping will work, but maybe for some reason you have changed these and need to adjust them to allow the storage mapping:

Sessions > RDP > RDP Global > Mapping > Drive Mapping > Enable Drive mapping (set checkmark)

Sessions > RDP > RDP Global > Native USB Redirection > Enable Native USB redirection (remove checkmark)

Sessions > RDP > RDP Global > Fabulatech USB Redirection > Enable Fabulatech USB redirection (remove checkmark)

Devices > USB access control > Enable (remove checkmark)

Sessions > RDP > RDP Sessions > [session name] > USB Redirection > Enable Native USB Redirection (global setting)

Sessions > RDP > RDP Sessions > [session name] > Mapping > Enable Drive Mapping (global setting)

Assigning a Drive Letter within the Session (Optional)

->In case you not only want to see the drive in the session as e.g. "A on IGEL-123456789", but want to address the drive with a real drive letter within the session, you may run one of these commands:

```
subst T: \\tsclient\t
```

or

```
net use T: \\tsclient\t
```

In this example "T on IGEL-123456789" is assigned to drive letter T: within the session. You may also assign the mapped drive to another drive letter than is used in its name.

Configuration on the Server Side

On the server side, e.g. with Windows Server 2008R2, a user in the group "Users" with access to the terminal server will have the mapping default. This is true for a newly installed server. But the mapping can be prevented by changing the policies:

Do not allow drive redirection Specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format [driveletter] on [computername]. You can use this setting to override this behavior." Source: https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx

FAQ: What Is the String for Token-Based Load Balancing?

Environment

A token-based mechanism is used as a load balancing method. This document does not apply to other load balancing methods.

Question

What string should be entered in **Sessions > RDP > RDP Sessions > [Session name] > Options** to make token-based load balancing work?

Answer

IGEL OS 10.05.700 or Higher, IGEL OS 11.01.110 or Higher

->Under **Sessions > RDP > RDP Sessions > [Session name] > Options > Collection**, simply enter the name of your RDS collection. The collection name has been defined by the server administrator.

IGEL OS 10.01 to 10.05.500, 11.01.100

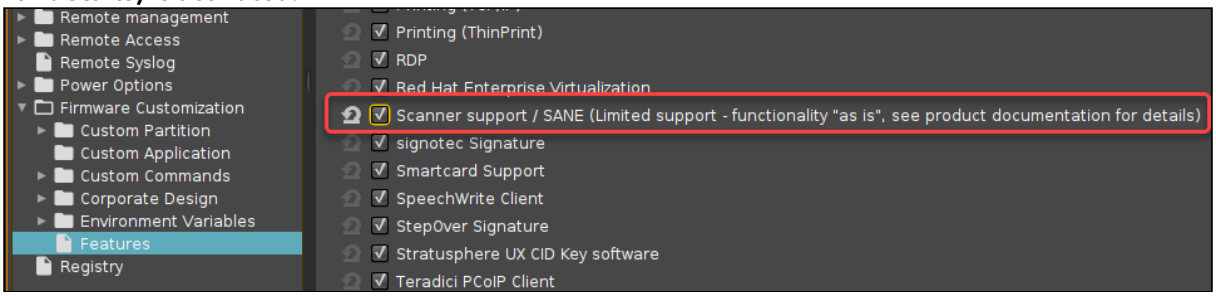
->Under **Sessions > RDP > RDP Sessions > [Session name] > Options > Load balancing routing token**, enter tsv:// MS Terminal (see page 452) `Services Plugin.1.[collection name]`, where

- tsv://MS Terminal (see page 452) `Services Plugin.1.` is the routing token and
- `[collection name]` is the name of the RDS collection, defined by the server administrator.

How to Enable RDP Fabulatech Scanner Redirection

Enabling Fabulatech Scanner Redirection

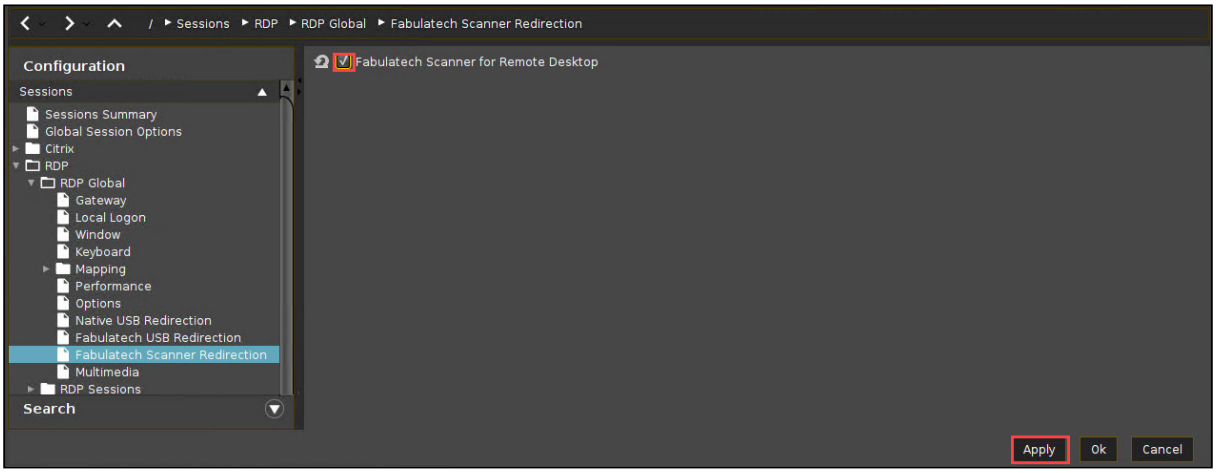
1. In the IGEL Setup, go to **System > Firmware Customization > Features** and make sure that **Scanner support /SANE (Limited support - functionality "as is", see product documentation for details)** is activated.



   - If the option is already activated, continue with step 2.
   - If the option has not been activated before, the software component must be downloaded first. For this purpose, make sure that the source of the current firmware is set correctly:
     - If you are using Universal Firmware Update, make sure that the device is assigned to the current firmware. For details, see Universal Firmware Update[62] and Assigning updates[63].
     - If you are not using Universal Firmware Update, make sure that **System > Update > Firmware Update** is set to the source of the current firmware. For details, see Firmware Update Settings for IGEL OS (see page 2056).
   - After clicking **OK** to confirm your changes, you must reboot the system.
2. In the IGEL Setup, go to **Sessions > RDP > RDP Global > Fabulatech Scanner Redirection.**

62. https://kb.igel.com/en/universal-management-suite/current/universal-firmware-update-1
63. https://kb.igel.com/en/universal-management-suite/current/how-to-assign-firmware-updates-to-devices-in-the-i?utm_source=ai_search&ai_search=true

3. Check **Fabulatech Scanner for Remote Desktop.**



4. Click **Apply** or **Ok** to confirm the settings.

How to Configure RDP RemoteApp Parameter Settings

Symptom

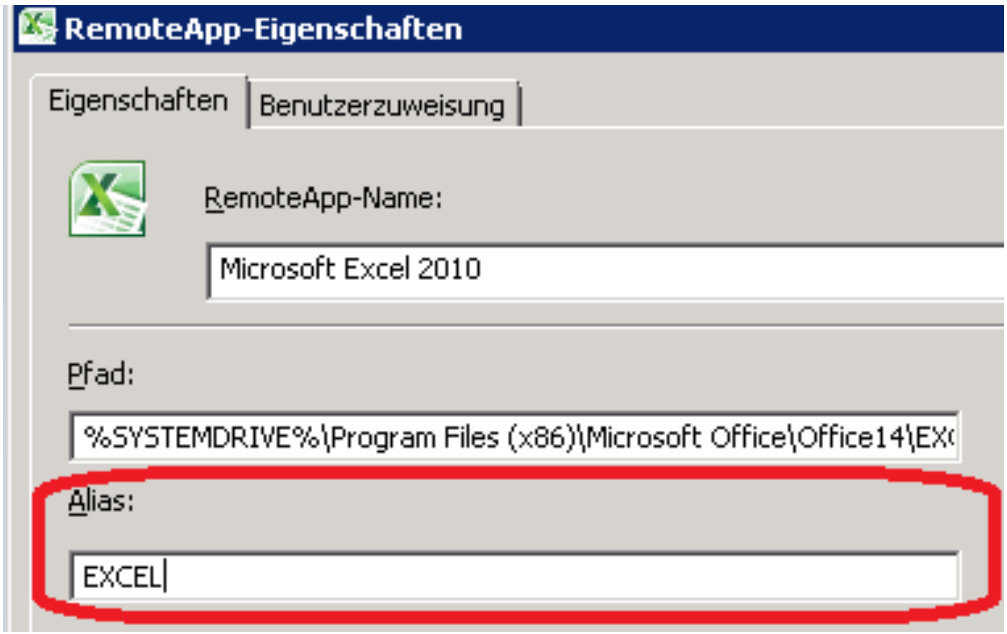
RemoteApp is not starting or closes immediately after login.

Problem

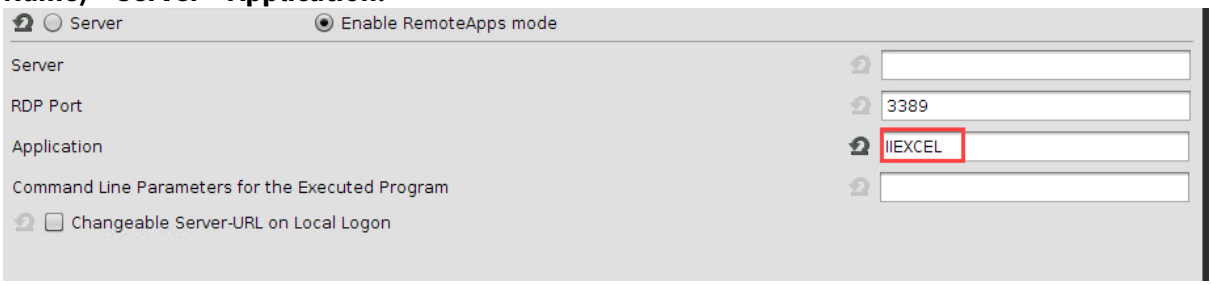
Missing or incomplete session settings on server or device

Solution

1. Set an ALIAS for the RemoteApp with the **RemoteApp Management Console** on the Terminalserver.



2. Use that ALIAS value in the device's setting in **Setup > Sessions > RDP > RDP Sessions > (Session Name) > Server > Application.**



Add two pipe-characters (||) at the beginning of the ALIAS value.

How to Enhance RDP Performance

Symptom

RDP users have performance issues (bad user experience).

For example:

- Mouse is lagging
- Screen is building up very slow
- Session uses high bandwidth
- Several other performance issues

Problem

There are many different causes that can result in bad performance.

Solution

The following settings can be used as a single option and also in combination.

Basics

- The color depth should be the same on the server, the device, and in the session (best: 32 bit).
- In the BIOS, set the VGA shared memory to 64 MB or more.

Optimizations for a LAN Environment

- Under **Sessions > RDP > RDP Global > Performance**, edit the settings as follows:
  - Disable **Compression**. (Increases performance, generates about 30% more traffic)
  - If RemoteFX 8 is available, activate **Enable RemoteFX**.
  - If RemoteFX 8 is available, set **RemoteFX codec mode** to "Optimized for LAN".
- If Windows Server 2012 R2 or lower or Windows 8.1 or lower is used: Under **Sessions > RDP > RDP Global > Multimedia**, activate **Enable Video Redirection**.

Optimization for a WAN Environment

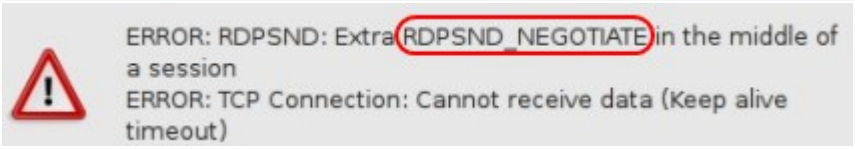
- Under **Sessions > RDP > RDP Global > Performance**, edit the settings as follows:
  - Enable **Compression**. (Generates about 30% less traffic, consumes more local resources)
  - If RemoteFX 8 is available, activate **Enable RemoteFX**.
  - If RemoteFX 8 is available, set **RemoteFX codec mode** to "Optimized for WAN".

Troubleshooting: RDP Session playing Sound: Error RDPSND_NEGOTIATE

Symptom

If the user plays some sound within the RDP session the connection terminates on some devices with error message:

```
ERROR: RDPSND: Extra RDPSND_NEGOTIATE in the middle of a session
ERROR: TCP Connection: Cannot receive data (Keep alive timeout)
```



Problem

This may happen if during data transmission the connection fails.

Solution

Try a different sound driver for RDP session:

1. Go to **System > Registry > rdp.winconnect.sound-driver**
2. Choose **OSS** or **ALSA**

Troubleshooting: Crackling and Audio Dropouts in RDP Sessions

Symptom

The user experience with RDP sessions is disturbed by crackling noises and glitches.

Environment

- Device with a sound card that has a small buffer, e. g. IGEL UD3 (M340C)
- Required for the solution: IGEL OS 11.03.500 or higher

Problem

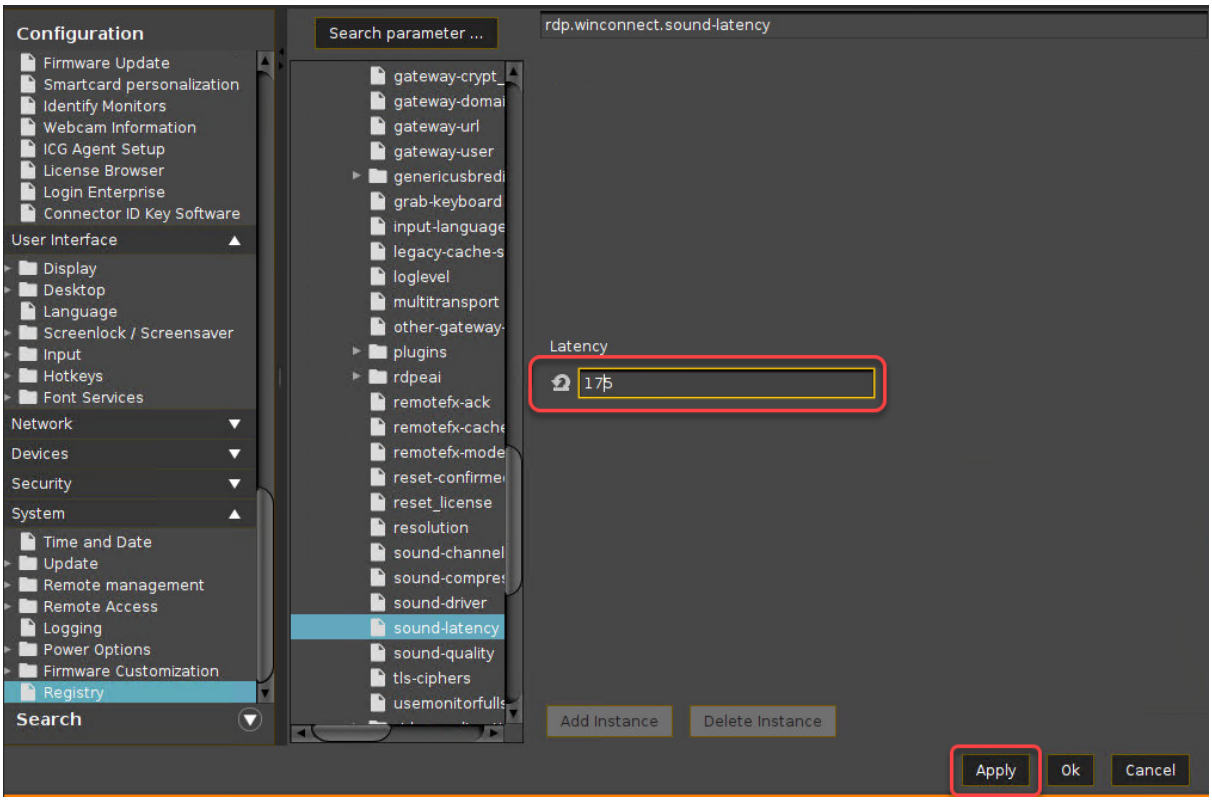
The crackling noises, or audio glitches, result from buffer underruns. This occurs when new audio data are not delivered fast enough and the sound card buffer has no more audio data left to play. Thus, it is not possible to bridge the replay gap. This is more likely to happen with sound cards that have a relatively small buffer.

Solution

To enable the device to bridge bigger gaps, buffer capacity must be added. This can be done by increasing the buffer of the RDP client, which implies increasing the latency. However, high latency can lead to a problem with interactive applications, such as calls or video conferences. Thus, the latency should be increased in small steps.

To increase the latency of the RDP client:

1. Open the Setup and go to **System > Registry > rdp > winconnect > sound-latency** (registry key: `rdp.winconnect.sound-latency`).
2. Increase the **Latency** by about 50 milliseconds (recommended) and click **Apply**.



3. Restart the RDP session and test the audio playback.
4. If the audio quality is good, click **Ok** to close the Setup. If there are still crackling noises, repeat steps 2 and 3 until the audio quality is acceptable.

Troubleshooting: Login Failed Because of Expired AD Password

Issue

When you try to log in to a **RDP** session, you get the error message "Login Failed!" because your Active Directory password expired.
You are unable to change your password because the local logon does not provide an option for that.

Before following these instructions, check the ports:

- Login to Client -> Port 88
- Change password -> Port 464

Here you find an overview of ports of the Domain Controller: Required Ports to Communicate with Domain Controller[64]

Solution

Enable **Active Directory/Kerberos** authentication for the **RDP** session. The next time you try to log in to IGEL OS, you will be prompted to change your expired password.

Changing an Expired Active Directory Password

When using sessions with passthrough authentication, it is essential that you lock your device's screen when leaving it unattended.

Enabling Active Directory/Kerberos Authentication for RDP Sessions

1. In IGEL setup, go to **Security > Logon > Active Directory/Kerberos**.
2. Enable **Login to Active Directory Domain**.
3. Go to **Security > Active Directory/Kerberos**.
4. Activate **enable**.
5. Fill in the **Default Domain (Fully Qualified Domain Name)**.
6. Go to **Sessions > RDP > RDP sessions > [RDP session] > Logon.**
7. Enable **Use passthrough authentication for this session**.
8. Click **Appy** or **Ok**.

Please note that the client must now be locked locally and no longer in the session to prevent another person from entering the session via the passthrough without specifying the password.

64. https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS

Enabling Screen Lock

1. In the IGEL setup go to **User Interface > Screenlock / Screensaver**.
2. Enable **Use Hotkey**.
3. Under **Modifiers** select `Win`.
4. Under **Hotkey** enter "l".
5. Got to **User Interface > Screenlock / Screensaver > Options**.
6. Enable **User Password**.

So the "Win + L" hotkey locks the IGEL client instead of the session desktop.

The AD password must be entered to activate the IGEL clients.

Troubleshooting: User Has to Provide Credentials Twice for RDP Logon

Issue

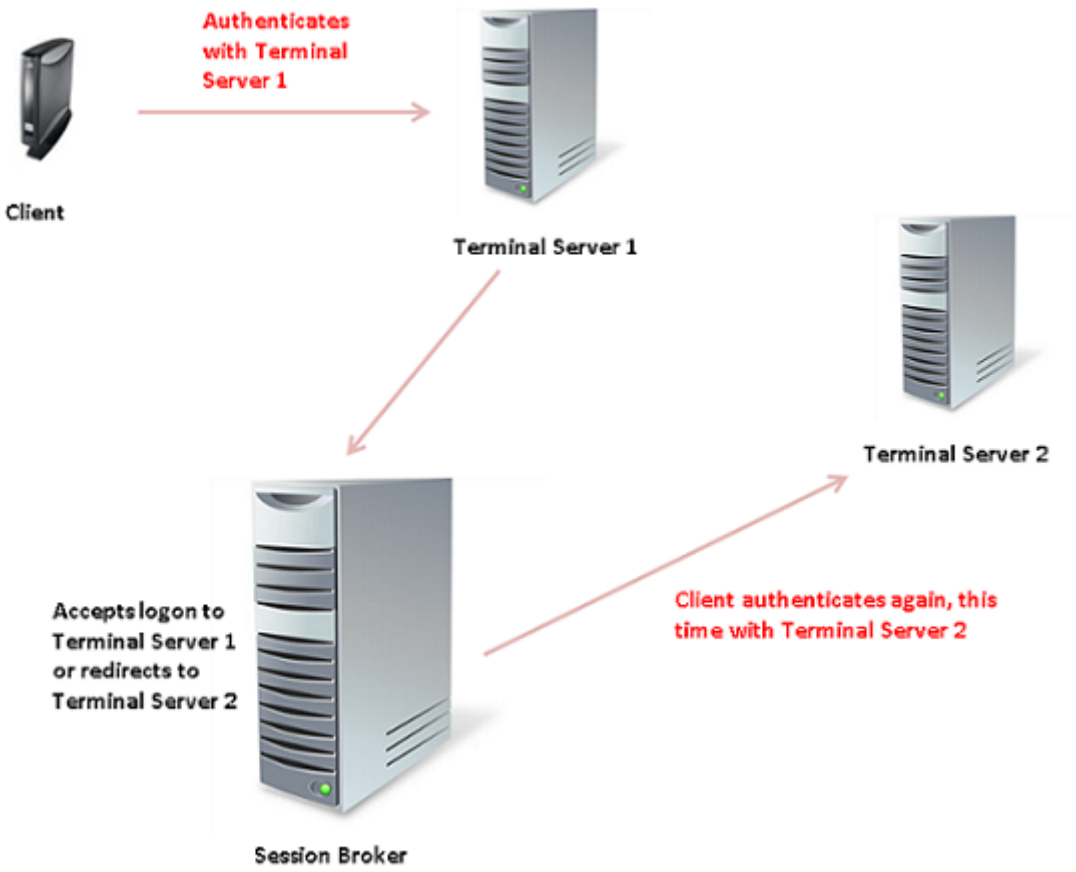
When you connect to a Windows terminal server, you are asked to provide your credentials twice.

Cause

This behavior is caused by the way RDS load balancing works. The crucial point to understand is that the terminal server does not communicate with the session broker directly.

Instead, the scenario is the following:

1. The client connects to terminal server 1 and authenticates with terminal server 1. This is the first time the user is asked for their credentials.
2. Since we have a load balancing setup, terminal server 1 will talk to the session broker and ask if the client can use terminal server 1 or if it should be redirected to a different terminal server.
3. If redirection occurs, the client will also have to authenticate with the terminal server the client was redirected to (terminal server 2 in the figure below). This is the second time the user is asked for their credentials.



Solution

The issue can be resolved by activating Kerberos/Active Directory authentication. For further information, see Active Directory/Kerberos[65].

65. https://kb.igel.com/en/igel-os/11.10.270/active-directory-kerberos

Bad Sound Quality of Flash/HTML Videos in RDP Session

Symptom

Flash or HTML5 browser video playing within RDP session has bad (choppy) sound quality.

Problem

The Flash/video implementation within Google Chrome or Chromium browser seems to cause the problem. Apparantly Chrome tries to sync video and audio signal and this does not work via RDP.

Solution

Use a different browser such as Mozilla Firefox or Microsoft Internet Explorer within the RDP session to play the video.

VMware Horizon

- How to Set up VMware Blast Sessions (see page 467)
- How to Use NLA (Network Layer Authentication) for Logon with Horizon Client Sessions (see page 468)
- Workaround for Hotkeys in Horizon Sessions (see page 469)
- Troubleshooting: Multimedia Acceleration with VMware Horizon View in VESA Mode (see page 470)
- Horizon Feature Matrix (see page 471)
- Troubleshooting the Horizon Client (see page 478)
- Troubleshooting: VMware Horizon Authentication Issues (Certificate Revocation List) (see page 479)

How to Set up VMware Blast Sessions

Prerequisites

- Device offering hardware video acceleration, see the FAQ Hardware Video Acceleration on IGEL OS (see page 1180).
- VMware Horizon 7 Server
  For further information about the server configuration, refer to VMware's documents at http://pubs.vmware.com/horizon-7-view/index.jsp

Activating VMware Blast

1. In Setup, go to **System > Firmware Customization > Features**.
2. Enable **Hardware Video Acceleration**.
3. Go to **Sessions > Horizon Client > Horizon Client Global > Server Options**.
4. Set **Preferenced desktop protocol** to **VMware Blast**.
5. Click **Apply** or **Ok**.

How to Use NLA (Network Layer Authentication) for Logon with Horizon Client Sessions

Starting a session, even just presenting a logon screen, has quite an impact on resources. Each time a user tries to logon, processes are started on the remote machine, no matter whether the user's credentials are valid or not. You can save resources and prevent Denial of Service (DoS) attacks by using Network Layer Authentication (NLA). NLA checks whether a user is the right person before any logon processes is started.

For more information about NLA, see https://technet.microsoft.com/en-us/magazine/hh750380.aspx.

NLA for *Horizon Client* Sessions is available from *IGEL* Linux version 5.08.100 upwards.

To use NLA for a *Horizon Client* session:

1. Open the setup and go to **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**.
2. Activate **Network Level Authentication**.

Workaround for Hotkeys in Horizon Sessions

Issue

You want to switch from the VMware Horizon session to the IGEL desktop with the key combination [Ctrl] + [Windows] + [D]. While the key combination [Ctrl] + [Windows] + [D] can be realized with IGEL OS 11.01.100 or lower (Horizon Client 4.x), this is not possible for IGEL OS 11.01.110 or higher (Horizon Client 5.x).

Solution

1. Press [Ctrl] + [Alt] and release the keys.
   The focus is switched from the VMware Horizon session to the local system.
2. Use [Ctrl] + [Windows] + [D] to switch to the IGEL desktop.
3. To switch the focus back to the VMware Horizon session, click into the VMWare Horizon session window.

Troubleshooting: Multimedia Acceleration with VMware Horizon View in VESA Mode

Symptom

You did install IGEL Universal Desktop OS 2 on not fully supported hardware using IGEL Universal Desktop Converter 2. Multimedia acceleration is not working within a VMware Horizon View session.

Problem

The graphics chip of your hardware is not supported and as a fallback the VESA mode is used.

Solution

There is no other solution to the problem than using fully supported hardware. Information on supported hardware can be found in the UDC2 manual.[66]

You can also access IGEL's 3rd party hardware support database[67] to find fully supported graphic chips.

66. http://edocs.igel.com/index.htm#11873.htm
67. https://www.igel.com/linux-3rd-party-hardware-database/

Horizon Feature Matrix

According to the details provided by the vendor, the following Horizon Client features are supported with Horizon Client 5.4:

For details on the Horizon Clients that are built into your version of IGEL OS, see IGEL OS Release Notes (see page 2282) > Notes for Release [your version] > Component Versions [your version].
See also the original document at https://kb.vmware.com/s/article/80386.

Category	Feature	Supported
Client Appearance and Workflow	Customer branding	no
	Kiosk mode	yes
	English localization	yes
	Language localization	yes
Broker Connectivity	XML-API version	15
	SSL	yes
	SSL certificate verification	yes
	Disclaimer dialog	yes
	Security Server compatibility	yes
	UAG compatibility	yes
	Multi-broker/Multi-site redirection - DaaS	yes
	Client info	yes
	Phonehome	yes
Broker Authentication	Password authentication	yes
	Password change	yes
	Certificate authentication	no
	RSA authentication	yes
	Radius	yes
	Integrated RSA SecurID token generator	no
	Single Sign On	yes
	Log in as current user	no
	Nested log in as current user	no

Category	Feature	Supported
	Biometric authentication	no
	Unauthentication access	yes
Smartcard	x.509 certificate authentication (Smart Card)	yes
	CAC support	no
	.Net support	yes
	PIV support	yes
	Java support	no
	Purebred derived credentials	no
Desktop Operations	Reset	only supported with VDI
	Restart	only supported with VDI
	Log off	yes
Session Management (Blast Extreme & PCoIP)	Switch desktops	yes
	Multiple Connections	yes
	App Launch on Multiple end points	yes
	Auto-Retry	yes
	Auto-Retry 5+ minutes	yes
	Fullscreen mode	yes
	Fullscreen toolbar	yes
	Windowed mode	yes
	Time Zone Synchronization	yes
	Jumplist integration (Windows 7-Windows 10)	no
Client Customization	Command Line Options	yes
	URI Schema	yes
	Preference File	yes
	Non Interactive Mode	yes
	GPO-based customization	no

Category	Feature	Supported
Protocols supported	Blast Extreme	yes
	H.264 - HW decode	yes
	H.265 - HW decode	no
	Blast Codec	yes
	JPEG / PNG	yes
	Switch Encoder	yes
	BENIT	yes
	Blast Extreme Adaptive Transportation	yes
	RDP 8.x, 10.x	yes
	PCoIP	yes
Protocol Enhancements	RDP-VC Bridge	yes
	Session Enhancement SDK	yes
Monitors / Displays	Dynamic Display Resizing	yes
	Multiple Monitor Support	yes
	External Monitor Support	yes
	Display Pivot	yes
	Multiple Aspect Ratio support	yes
	Number of displays supported	4
	Maximum Resolution	3840x2160
	Video out	yes
	High DPI scaling	only supported with VDI
	DPI Sync	yes
	Exclusive Mode	no
	Multiple Monitor Selection	yes
Input Device (Keyboard / Mouse)	Relative mouse	yes
	External Mouse Support	yes
	Local buffer text input box	no
	Keyboard Mapping	yes

Category	Feature	Supported
	Unicode Keyboard Support	no
	International Keyboard Support	yes
	Input Method local/remote switching	no
	IME Sync	yes
Clipboard Services	Clipboard Text	yes
	Clipboard Graphics	no
	Clipboard memory size configuration	yes
	Drag and Drop text	no
	Drag and Drop images	no
Client Caching	View Agent to Client-side caching	yes
Connection Management	Blast network recovery	yes
	IPv6 translation with UAG	no
	IPv6 only network support	no
	PCoIP IP roaming	yes
High-Level Device Redirection	Serial (COM) Port Redirection	yes
	Client Drive Redirection/File Transfer	yes
	Scanner (TWAIN/WIA) Redirection	yes
	x.509 Certificate (Smart Card)	yes
	Gyro Sensor Redirection	no
Real-Time Audio-Video	Analog in (input)	yes
	Real-Time Audio-Video	yes
	Multiple webcams	no

Category	Feature	Supported
USB Redirection	Generic USB / HID	yes
	Policy: ConnectUSBOnInsert	only supported with VDI
	Policy: ConnectUSBOnStartup	only supported with VDI
	Connect/Disconnect UI	yes
	USB device filtering (client side)	yes
	Isochronous Device Support	only supported with VDI
	Split device support	yes
	Bloomberg Keyboard compatibility	only supported with VDI
	Smartphone sync	only supported with VDI
	USB 3.0	yes
	USB Redirection USB storage devices	yes
Unified Communications	Cisco UC Jabber	only supported with VDI
	Avaya UC One-X Desktop	only supported with VDI
	Mitel UCA	no
	Microsoft Lync 2013	no
	Skype for business	yes
	Microsoft Teams RTAV	yes
Multimedia Support	Multimedia Redirection (MMR)	yes
	Flash URL Redirection (Unicast/Multicast)	only supported with VDI
	Flash Redirection	no
	HTML5 Redirection	yes
	Directshow Redirection	no
Graphics	vDGA	only supported with VDI
	vSGA	only supported with VDI
	NVIDIA GRID VGPU	yes
	Intel vDGA	only supported with VDI
	AMD vGPU	only supported with VDI

Category	Feature	Supported
Mobile Support	Client-side soft keyboard	no
	Client-side soft touchpad	no
	Full Screen Trackpad	no
	Gesture Support	no
	Multi-touch Redirection	no
	Presentation Mode	no
	Unity Touch	no
Printing	Printer Redirection	yes
	VMware Integrated Printing	yes
	Location Based Printing	yes
	Native Driver Support	yes
Security	FIPS-140-2 Mode Support	yes
	Imprivata Integration	no
	Opswat agent	yes
	Opswat on-demand agent	no
	TLS 1.1	yes
	TLS 1.2	yes
Session Collaboration	Session Collaboration	yes
	Read-only Collaboration	yes
Update	Update notifications	no
	App Store update	no

Category	Feature	Supported
Other	Smart Policies	yes
	File Type Association	no
	URL content redirection	yes
	Browser content redirection	no
	Remember credentials	no
	Access to Linux Desktop - Blast Protocol Only	only supported with VDI
	Audio Playback	yes
	Seamless Window	yes
	Launching multiple client instances using URI	yes
	Parameter pass-through to RDSH apps	yes
	Performance Tracker	only supported with VDI
	Shortcuts from server	no
	Pre-install shortcuts from server	no
	Workspace ONE mode	yes

Troubleshooting the Horizon Client

> **Solution Based on Experience from the Field**
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Symptom

There are some issues with the performance of the Horizon client.

Environment

- IGEL OS 10 or higher

Problem

You don't know how to collect the log files and send them to the IGEL Support team.

Solution

1. In the Setup, go to **System > Registry > sessions > vdmcient% > options > debug** and activate **Save debug information** (registry parameter: `sessions.vdm_client%.options.debug`).
2. Go to **System > Registry > vmware > USB > log** and set **Set VMware Horizon USB debug level** to "debug" (registry parameter: `vmware.view.usb.log`).
3. Go to **System > Registry > vmwarevdmapp > debug** and activate **Save debug informations** (registry parameter: `vmwarevdmapp.debug`).

   The log files are created in the `/tmp` directory and can be found using the following patterns:

   `/tmp/vvdm*`

   `/tmp/vmware-*`
4. Change to `/tmp` and put the log files into a compressed tar file: `tar -czf vmware-logs.tar.gz [logfiles]`
5. In the structure tree of the UMS Console, go to the device and select **Device File->UMS** the context menu.
6. Under **Devices file location**, enter "/tmp/vmware-logs.tar.gz".
7. Under **Target URL**, select the location on the UMS Server where the file is to be stored.
8. Click **Device->UMS**.

Troubleshooting: VMware Horizon Authentication Issues (Certificate Revocation List)

Newer versions of VMware Horizon Client for Linux attempt to download a Certificate Revocation List (CRL) for any certificates used to connect to a VMware Horizon environment. Sometimes, this can cause a problem on lower-powered devices or on devices that do not have access to a CRL address.

The following article explains how to disable the CRL download if you have problems with authentication for VMware Horizon sessions in IGEL OS.

Problem

You face the following issues:

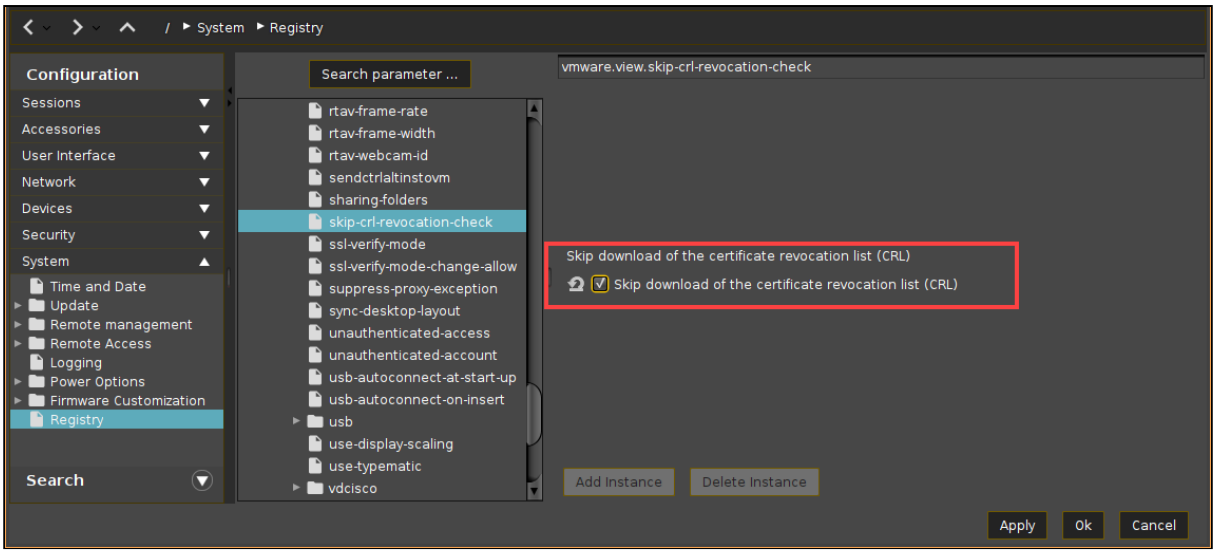
- The VMware Horizon Client "hangs" during authentication.
  OR
- The VMware Horizon Client takes a long time to authenticate (in some cases, over 1 minute).
  OR
- You are using a certificate issued by the domain's CA (certificate authority) and get the following error message:
  "`Failed to connect to the connection server. The server provided an invalid certificate. Unsupported URI in CRL distribution points extension, only http/https are supported.`"

Solution

These issues usually occur due to the default setting for CRL download for the VMware Client for Linux. If you experience the above issues, it is recommended to disable downloading of the CRL.

To disable the download of the CRL, proceed as follows:

1. In IGEL Setup or in the configuration dialog in the UMS, go to **System > Registry**.
2. Enable the registry key `vmware.view.skip-crl-revocation-check`, i.e. **Skip download of the certificate revocation list (CRL)**.



3. Apply the settings. If you have created a profile, assign the profile to the required devices.
4. Reboot the devices and test the connection again.

Evidian

- How to Authenticate with Evidian Authentication Manager (see page 482)

How to Authenticate with Evidian Authentication Manager

You can connect to Citrix, RDP and VMware Horizon roaming sessions using RFID badges with Evidian Authentication Manager (AuthMgr). Custom commands are supported as well.

Prerequisites

- IGEL Universal Desktop Linux 5.06.100 or newer on the device.
- An installed and running Evidian SSO Controller, version 10.0 or higher
- When using HTTPS (IGEL Linux 5.07.100 or newer), the User Access Server's CA root certificate saved locally on the device.
- The device and the server(s) have to be part of the same Active Directory domain.
- A supported RFID reader (e.g. *OMNIKEY 5022 CL, OMNIKEY 5421)*, connected to the device.
- RFID badges that are already enrolled.

Configuring an Evidian Authentication Manager Session

1. In IGEL Setup, go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions**.
2. Add a new session.
3. Go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Connection**.
4. Choose the **Protocol** used for the user access service (e.g. HTTP).
5. Enter the IP address or DNS name used for the user access service under **Server**.
6. Choose the **Port** for the user access service (e.g. 9764).
7. Under **Path to service**, enter the path for the user access service (e.g. `/soap`).
8. Under **CA certificate**, enter the path to the CA certificate, including its name, or path of the certification authority (e.g. `/wfs/ca-certs/ca.crt`). The certificate is required for HTTPS connections.
9. Enter the secret for the **Roaming session secret**.
10. When using HTTPS, select **CA certificate** as the user access server's CA root certificate on the device.
11. Under **Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Options**, select the desired **Session type**.
    This will make Evidian Authentication Manager use the first configured session of its type, e.g. RDP. Make sure that a session is configured.

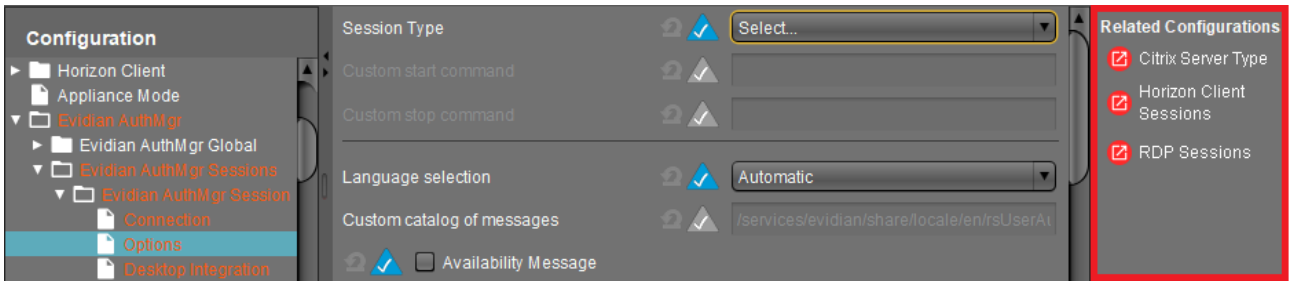
    > If you choose the user-defined session type, you need to supply the custom commands; see Custom Commands (see page 484). For further options, see Options of Evidian AuthMgr Sessions (see page 1440) in the IGEL OS Reference Manual.

12. Start the new session by clicking on its icon in the **Start Menu**. Alternatively, reboot the device. In the default autostart setting the Evidian Authentication Manager for your session will start automatically and wait for an RFID badge to be placed on the reader.

> You can only start a single instance of an Evidian Authentication Manager session.

Configuring Citrix/RDP/VMware Horizon Sessions

->Configure the session that you want to use with Evidian Authentication Manager as the first session of its kind. The shortcuts to the session settings are provided in the Setup section **Related Configurations**:



Using a Custom Configuration File

Instead of using the settings provided by IGEL Setup, you can enable a custom configuration file under **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name]** > **Options > Use configuration file**. Then all the other session settings will be ignored. You find a commented template for the configuration file at `/etc/rsUserAuth/rsUserAuth.ini`.

Logging in with Evidian Authentication Manager

1. Place your RFID badge on the RFID reader (or tap the reader with it if you configured **Tapping Mode**)
2. Your Citrix/RDP/VMware Horizon session will open if an active roaming session for your user already exists. If it does not, you will be presented with a password prompt for the user's Active Directory password.
3. Remove your RFID badge (or tap the reader again) to disconnect from the session.

Custom Commands

The following simple shell scripts illustrate how to write custom commands that receive username and domain as parameters from *Evidian Authentication Manager.*

In order to use them

1. Save the scripts in `/wfs/.`
2. Make them executable with `chmod a+x [filename].`
3. Enter their full path (e.g. `/wfs/start.sh`) in **Sessions > Evidian > [Session name] > Options.**

Start Script

```
#!/bin/sh
# Sample start script
if [ $# -eq 3 ] ; then
   # Start "session"
   gtkmessage -t "Evidian Authentifcation Manager Login" -m "Login as user '$1' with domain '$3'."
else
   exit 1
fi
exit 0
```

Stop Script

```
#!/bin/sh
# Sample stop script
# Close running "session"
pkill gtkmessage
gtkmessage -t "Evidian Authentication Manager Logout" -s 5 -S -m "Logout user '$1'."
exit 0
```

Debugging and Troubleshooting

Debugging

1. Enable **Debug mode** in **Sessions > Evidian > [Session Name] > Options** in **Setup** and set the level of detail.
2. Kill the *Evidian Authentication Manager* process (see Further Troubleshooting).
3. Start the desired Evidian session from the **Start Menu**.
4. Watch the output with `tail -F /var/log/user/rsuserauth[Session Number].debug` in **Local Terminal.** Alternatively, add the file to **System Log Viewer.**

   > The session number starts with 0, not 1. To watch the output of the first configured session, use thus `tail -F /var/log/user/rsuserauth0.debug`

Further Troubleshooting

1. Open **Local Terminal**
2. Enter `ps fax | grep rsuserauth | grep -v grep` to look for *Evidian Authentication Manager* processes.
3. Use the **Evidian AuthMgr Restart** session to restart all Evidian sessions if neccesary
   OR kill unwanted processes by entering `kill [process ID]` in the terminal, start desired processes via the Evidian entries in the **Start Menu**.

IBM iAccess

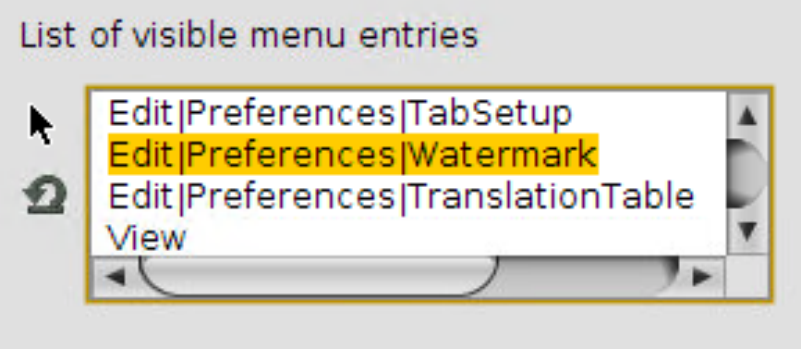
- How to Edit the List of Visible Menu Entries for IBM iAccess (see page 487)
- How to Configure Key Mapping for IBM iAccess Client (see page 489)

How to Edit the List of Visible Menu Entries for IBM iAccess

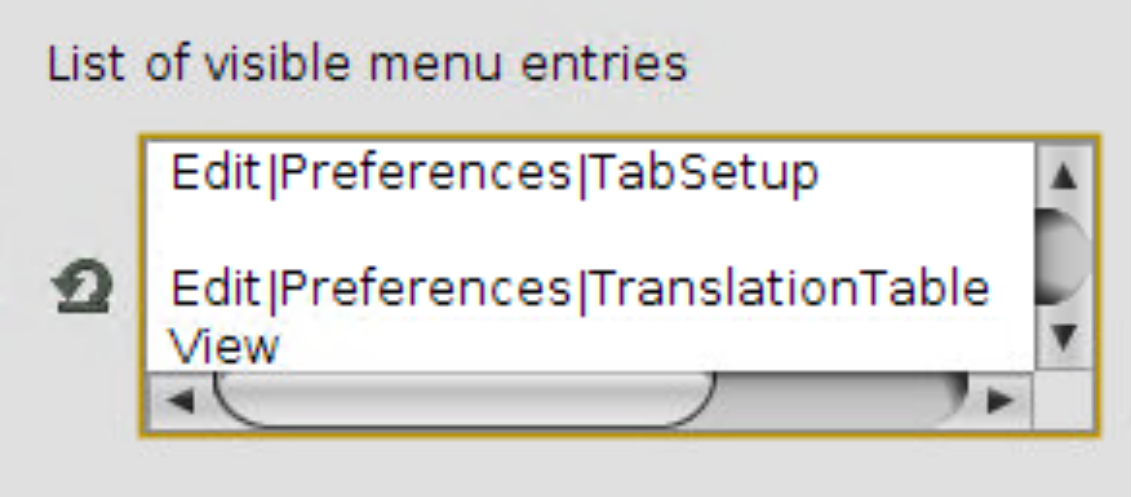
You can simplify the menu of an IBM iAccess client session by removing items from the menu tree. You also can restore the original menu.

Removing Menu Items

1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: `sessions.iaccess[NUMBER].options.deletemenus`). [NUMBER] is the instance number of the session you want to configure; 0, for instance, stands for the first session, 1 for the the second session, etc.
2. In the **List of visible menu entries**, using the mouse, mark the line with the entry you want to delete:



3. Press the backspace [←] or delete [Del] key.
   The menu item is deleted:



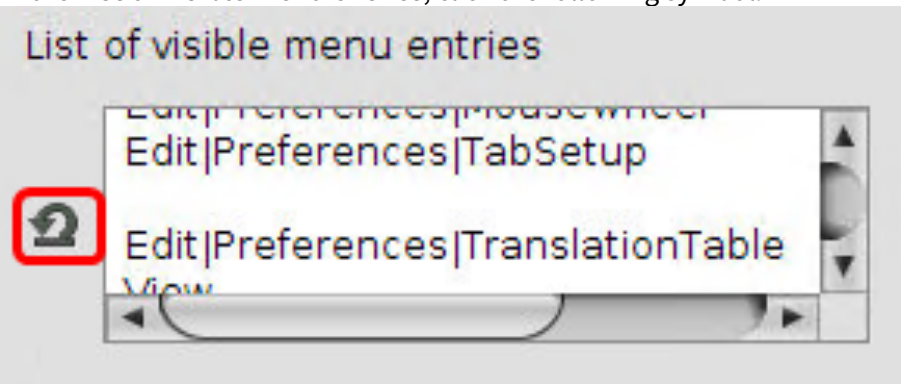
> If you delete a menu item that has subitems, the subitems will be invisible, too.

4. To remove further menu items, repeat steps 2 and 3.

5. Click **Apply** or **Ok**.
6. Start or restart the IBM iAccess client to check your changes.

Restoring the Original Menu

1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: `sessions.iaccess[NUMBER].options.deletemenus`). [NUMBER] is the instance number of the session whose menu you want to restore; 0, for instance, stands for the first session, 1 for the the second session, etc.
2. In the **List of visible menu entries**, click the following symbol:



   The original menu is restored.
3. Click **Apply** or **Ok**.

How to Configure Key Mapping for IBM iAccess Client

Problem

When you change the key mapping in the IBM iAccess client, the changes are not retained when the client is restarted.

Applying the changes via IGEL Setup is not possible.

Environment/Prerequisites

- IGEL OS 10.05.100 or higher
- UMS 5.09.110 or higher
- IBM iAccess Client session is set up

Solution

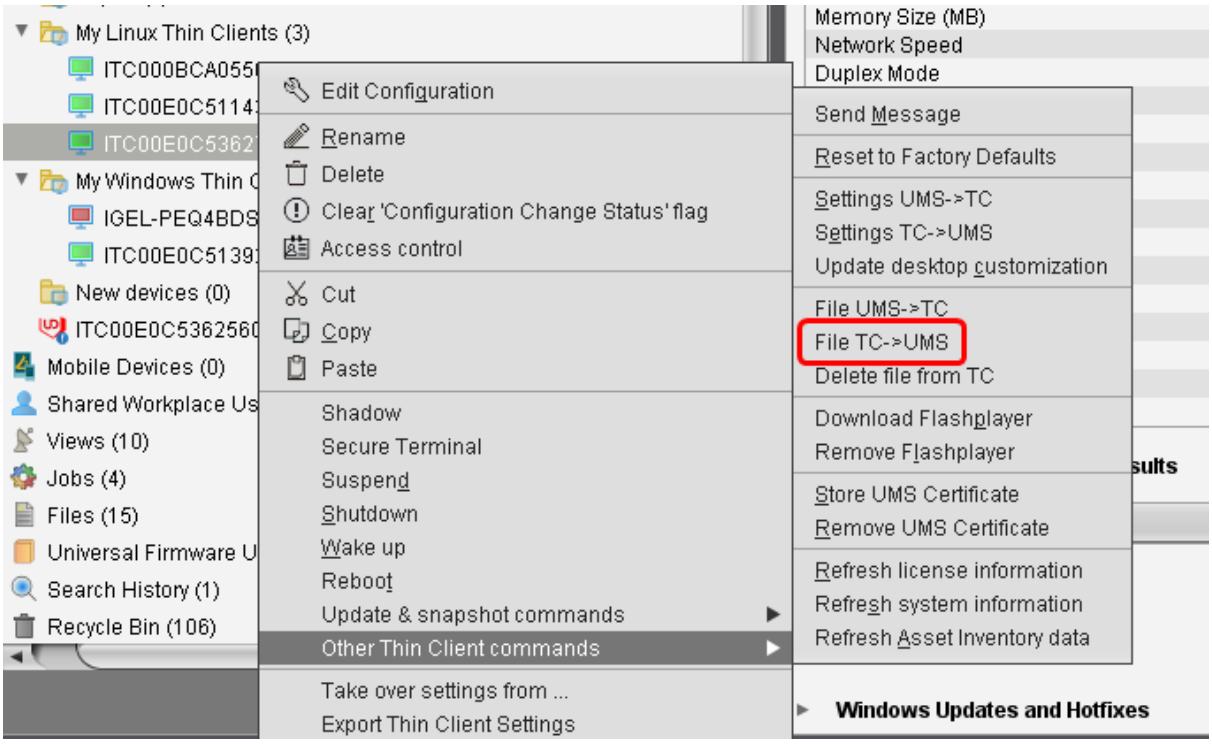
Save the settings made in the IBM iAccess client in a file and distribute that file via the UMS.

Editing the Key Mappings

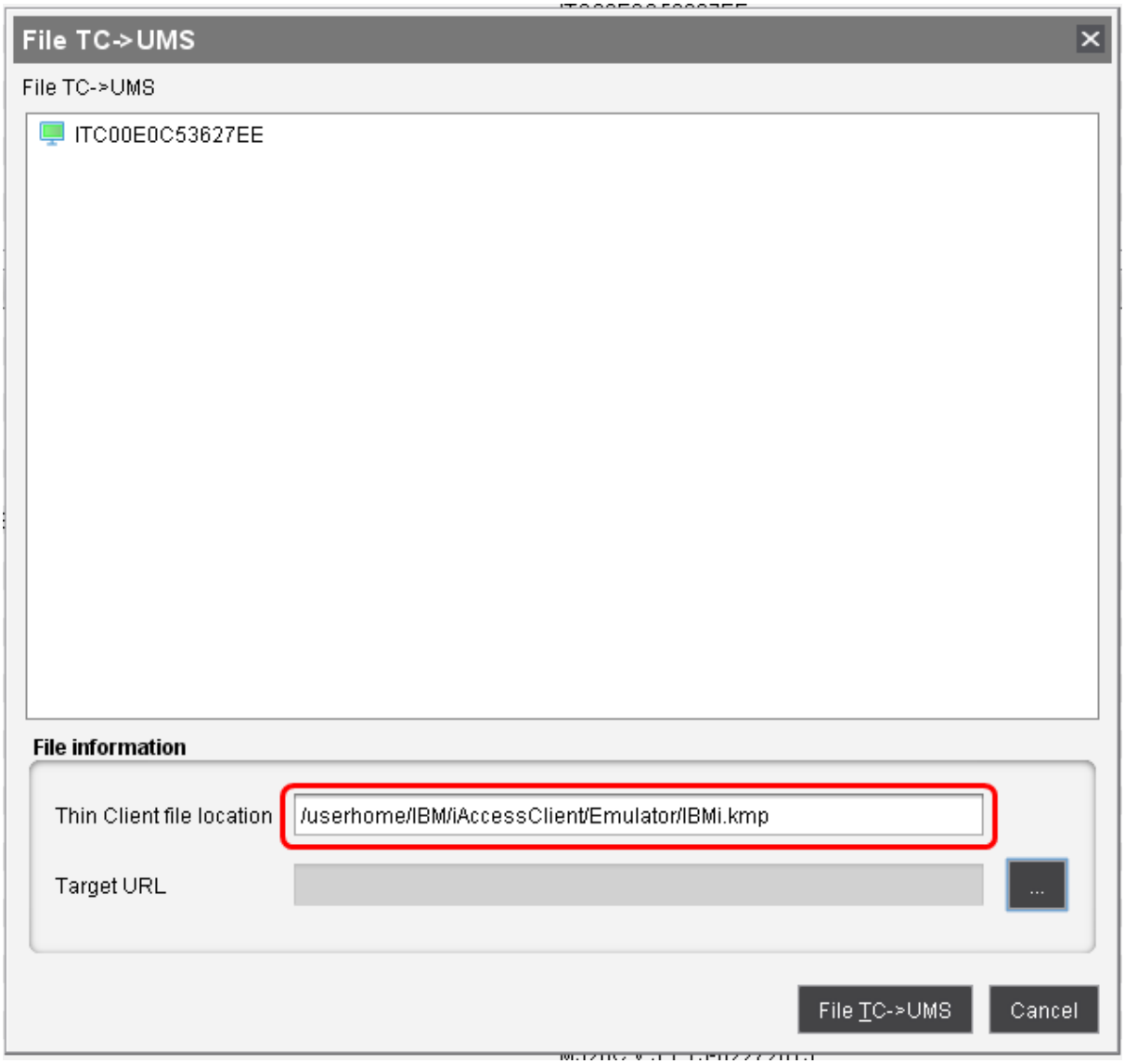
1. Open the IBM iAccess session and log on to your remote environment.
2. In the IBM iAccess client, go to **Edit > Preferences > Keyboard**.
3. On the **Key Assignment** tab, create the desired key bindings.
4. When you are finished creating key bindings, click **Save as...**.
5. In the save dialog, choose **File** and edit the file path as follows: `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp`
6. Click **OK**.
   The IBM iAccess client will recognize the file `IBMi.kmp` as the default key.

Importing the Configuration File to the UMS

1. Open the UMS.
2. In the navigation tree, find the thin client with the `IBMi.kmp` file and select **Other Thin Client commands > File TC->UMS** in the context menu.

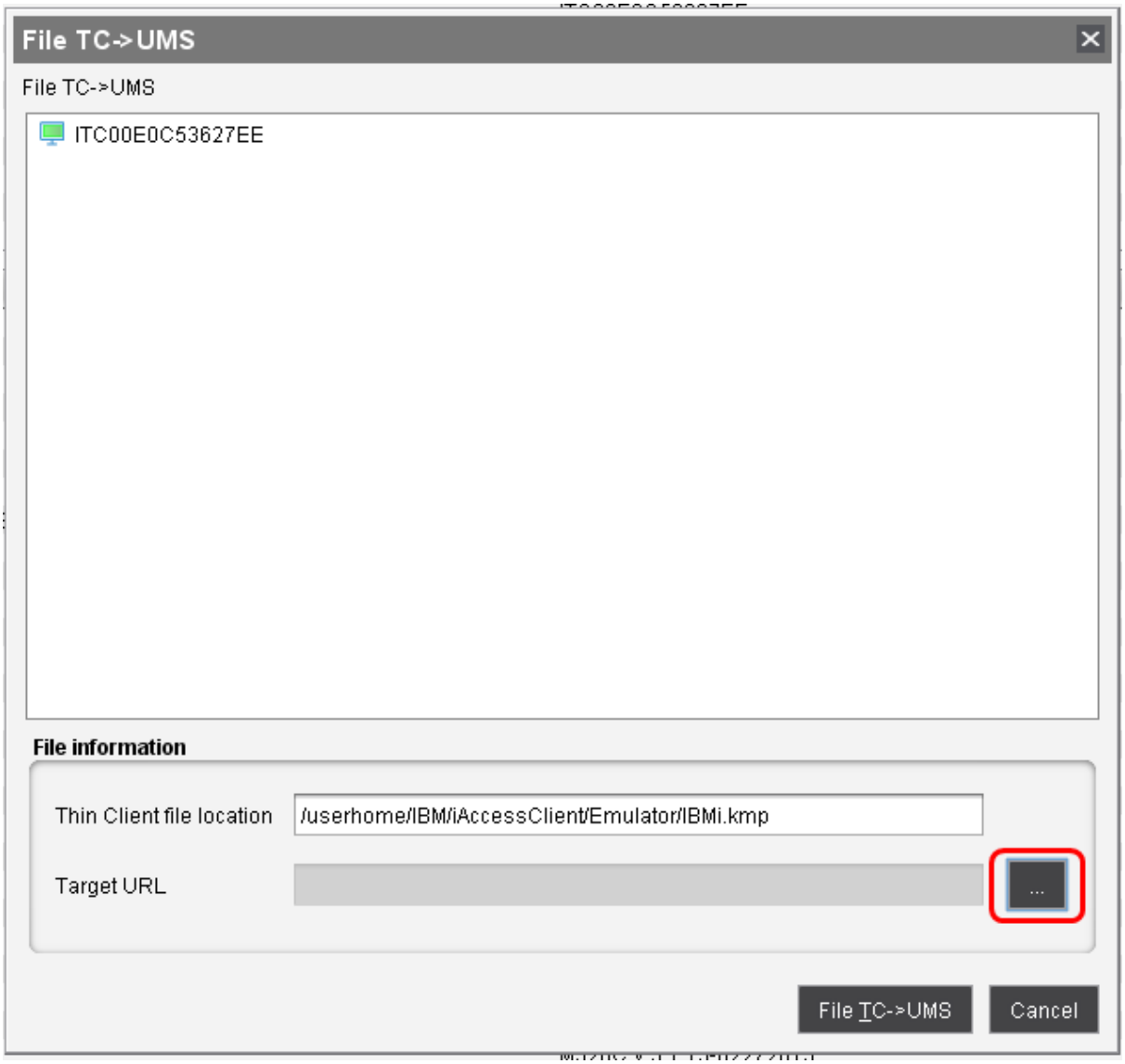


3. Under **Thin Client file location**, enter `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp`

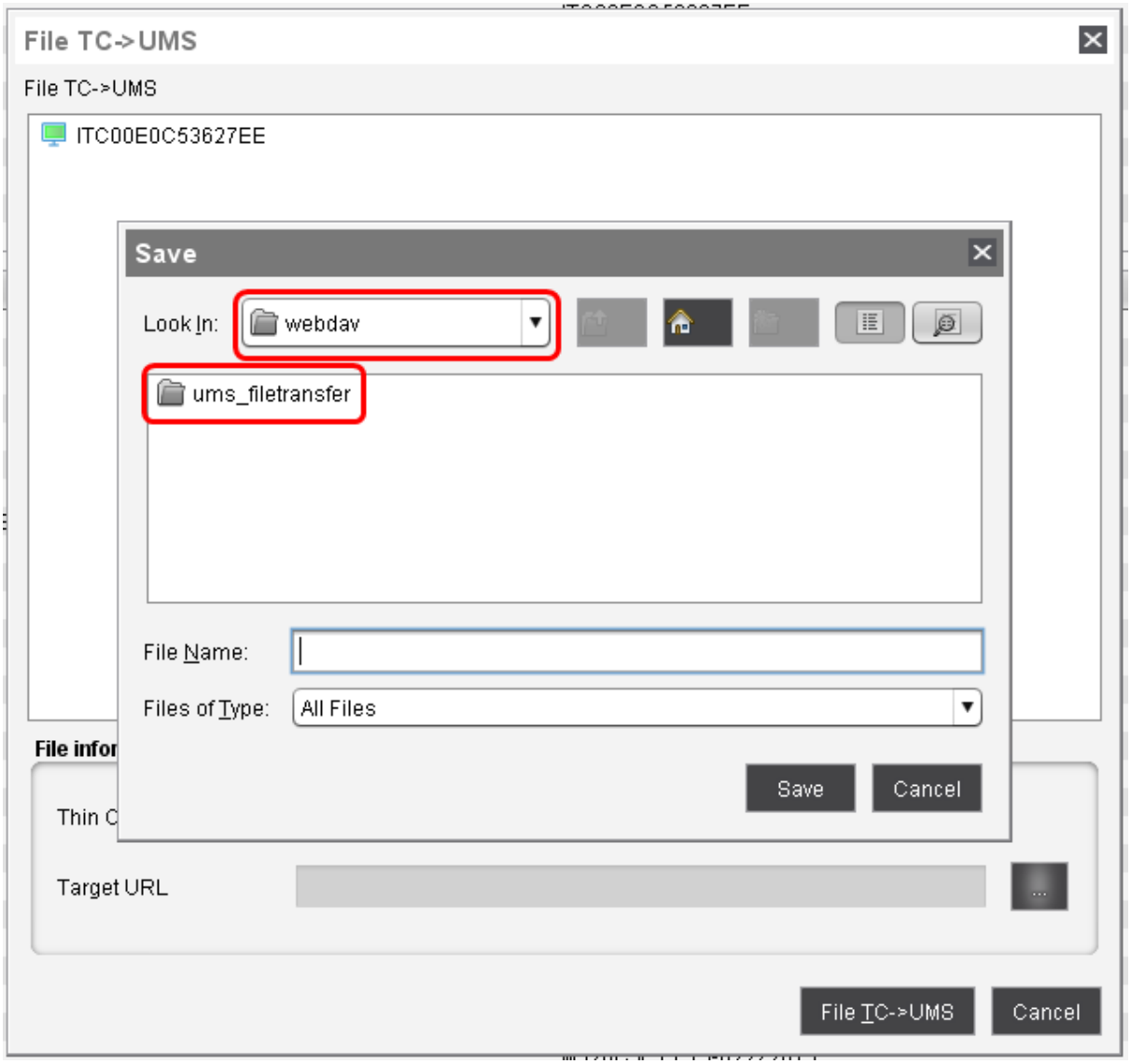


4. Click

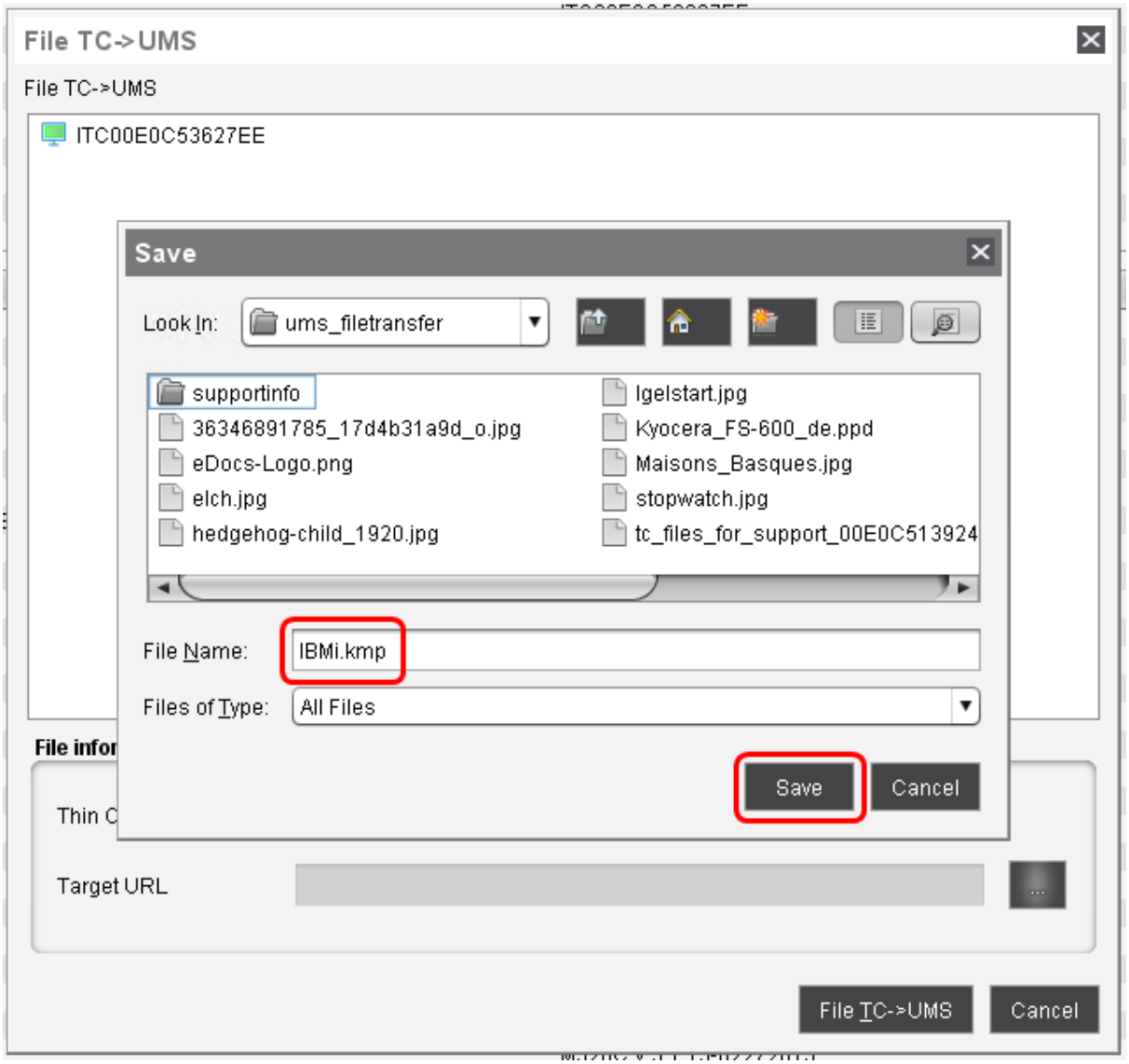
to open the **Save** dialog.



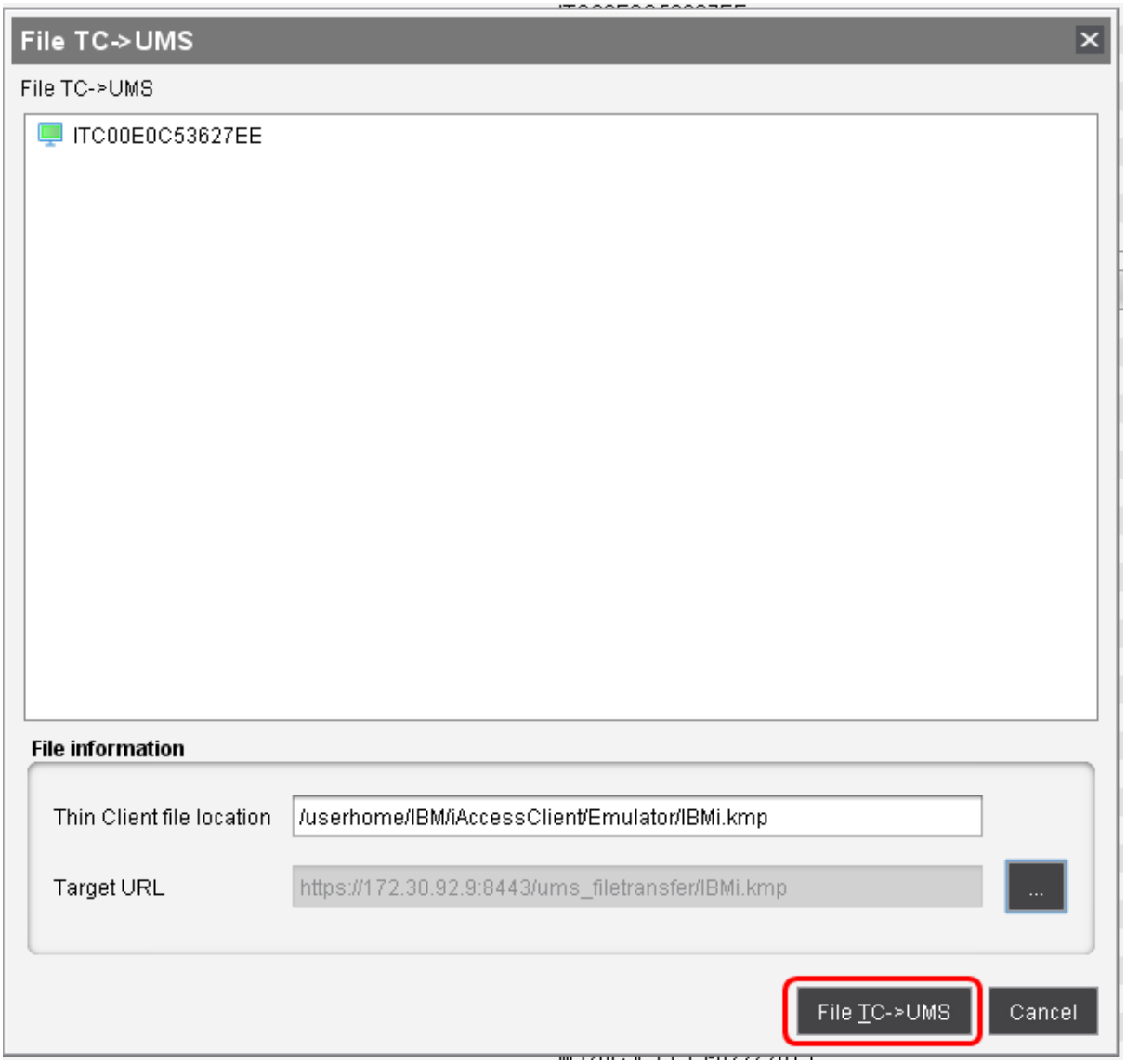
5. Choose a file location within the `ums_filetransfer` folder.



6. Under **File Name**, enter `IBMi.kmp` and click **Save**.



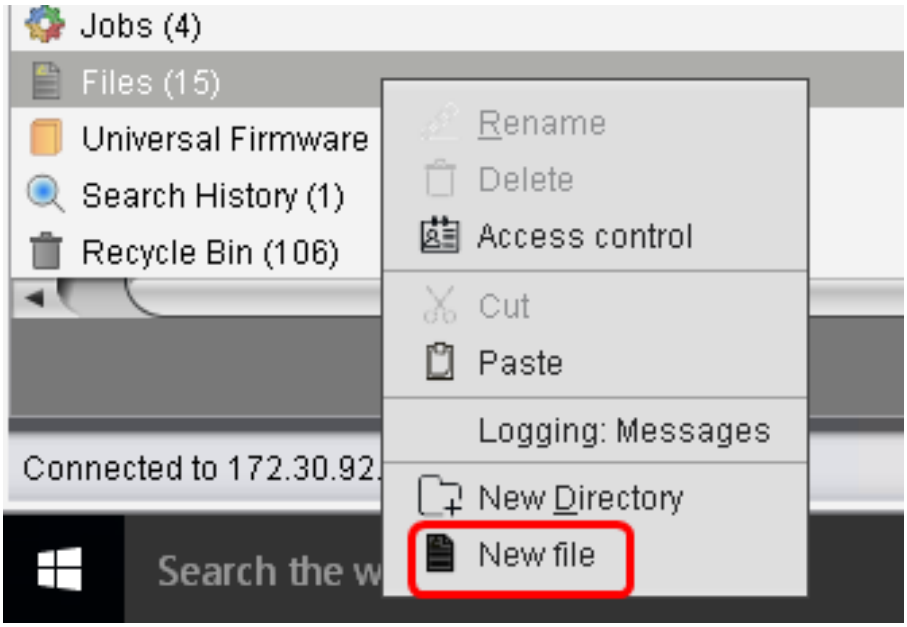
7. Click **TC->UMS**.



The file is stored within the UMS. Next, we will make it available as an object.

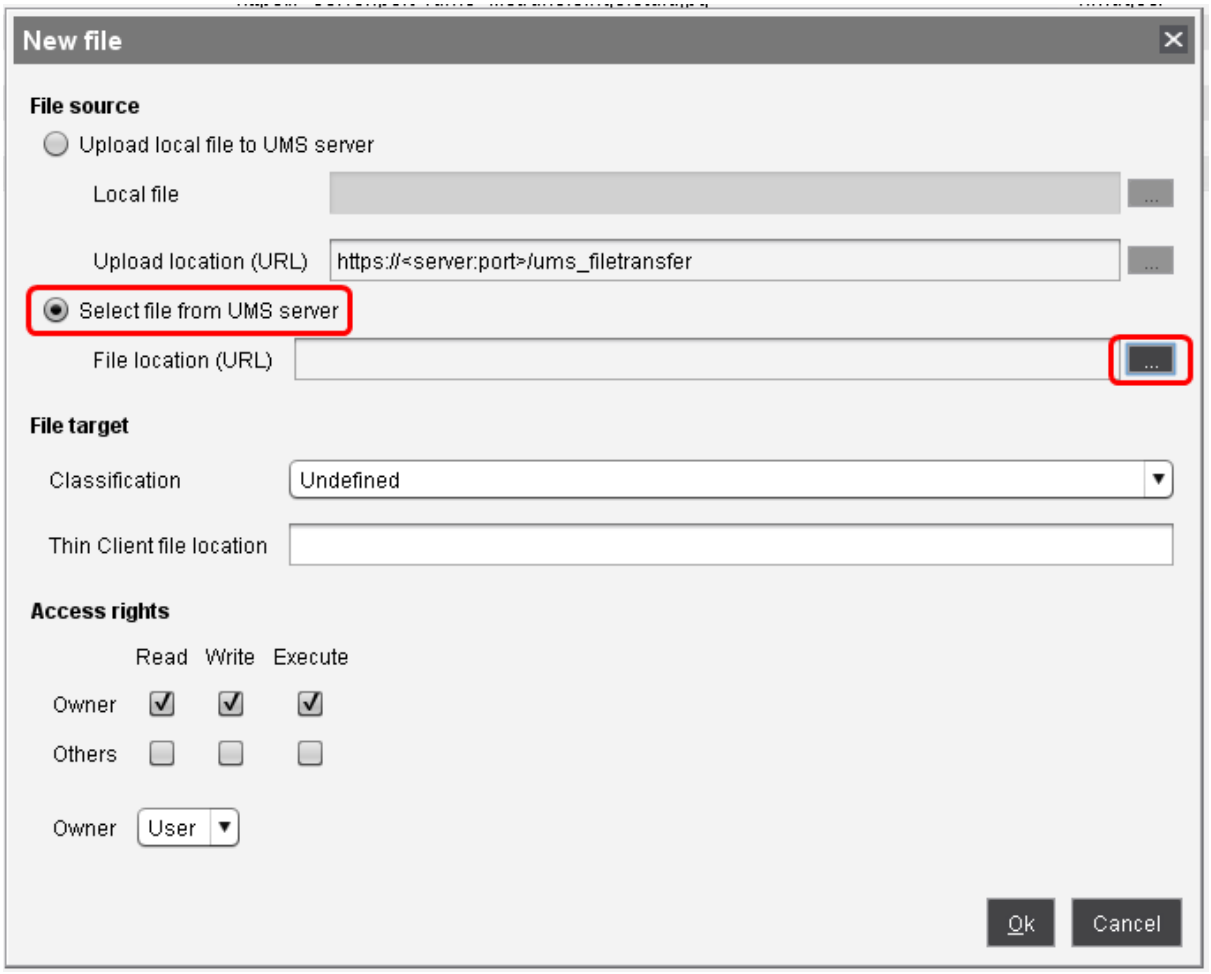
Creating the File Object in the UMS

1. In the navigation tree, go to **Files**, open the context menu and choose **New file**.

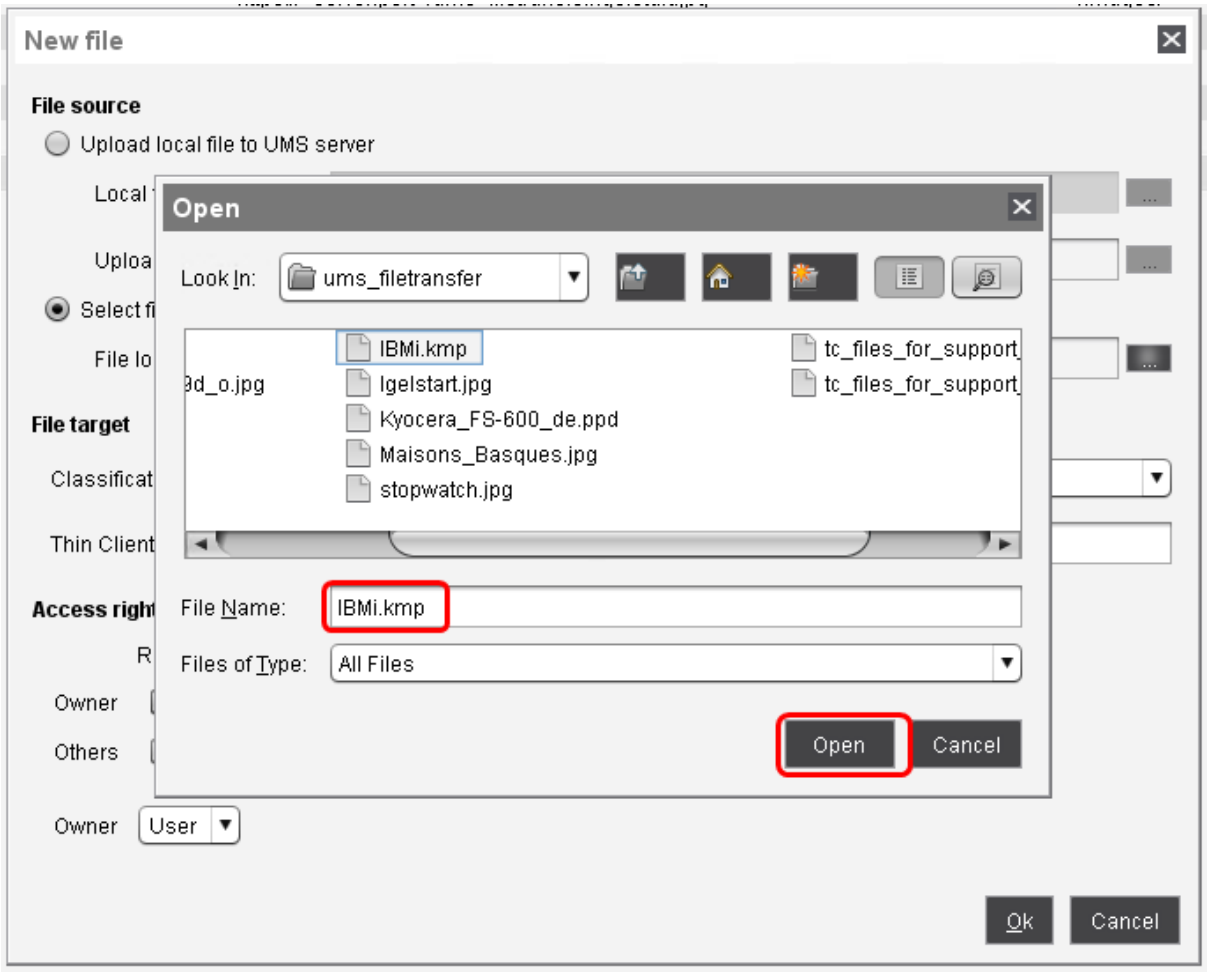


2. In the **New file** dialog, choose **Select file from UMS server** and click

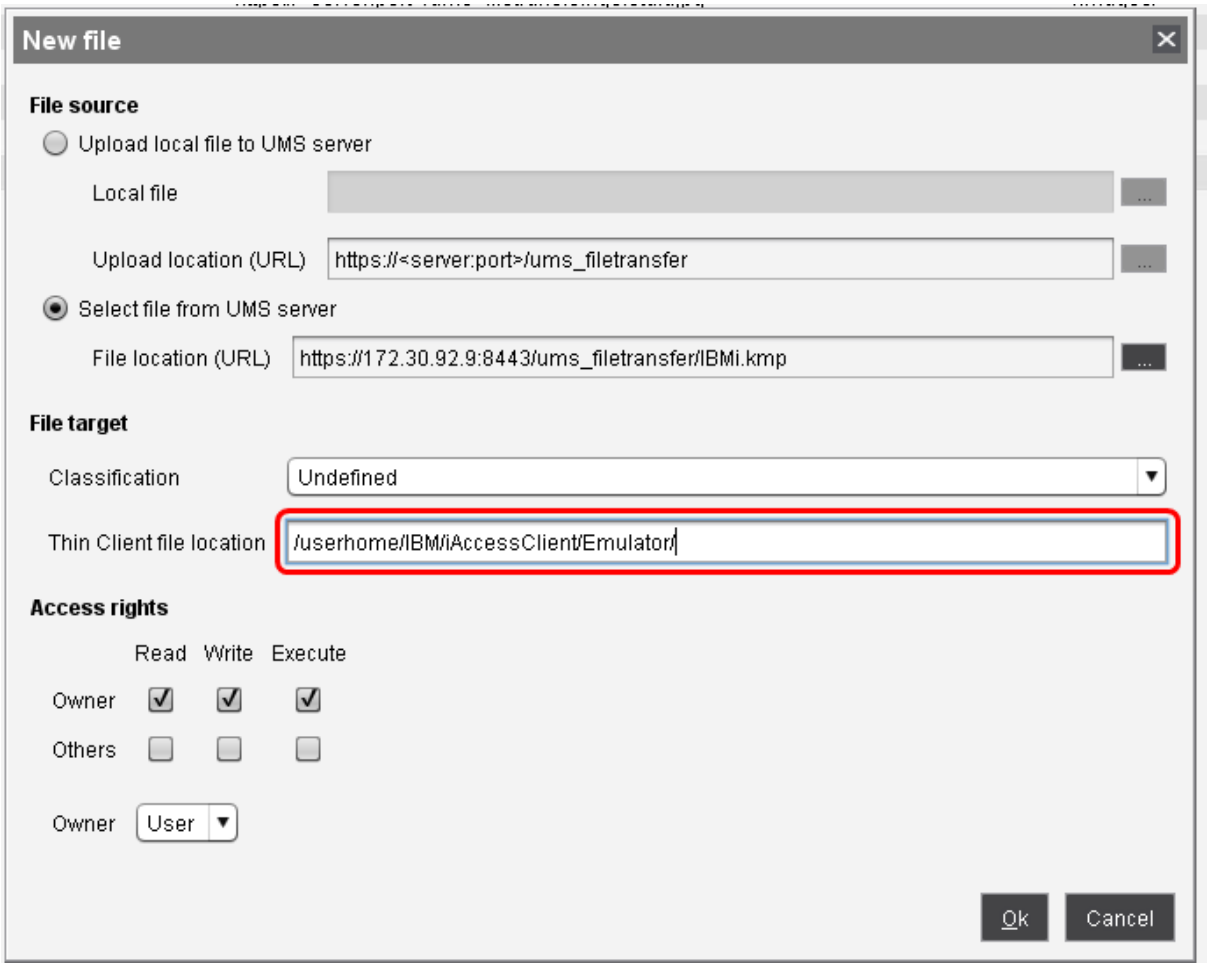
to open the file dialog.



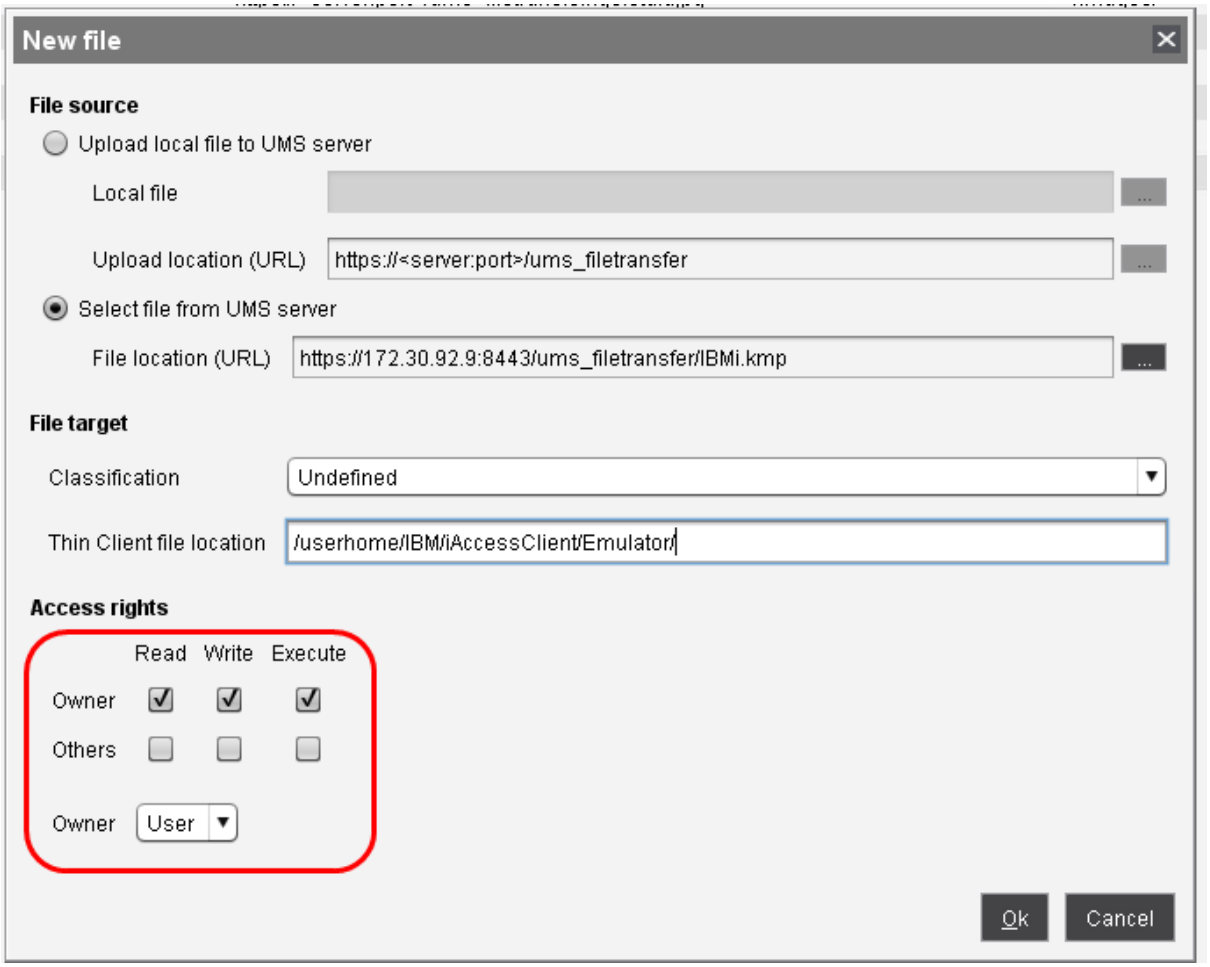
3. In the file dialog, find the file `IBMi.kmp` you created previously, and click **Open**.



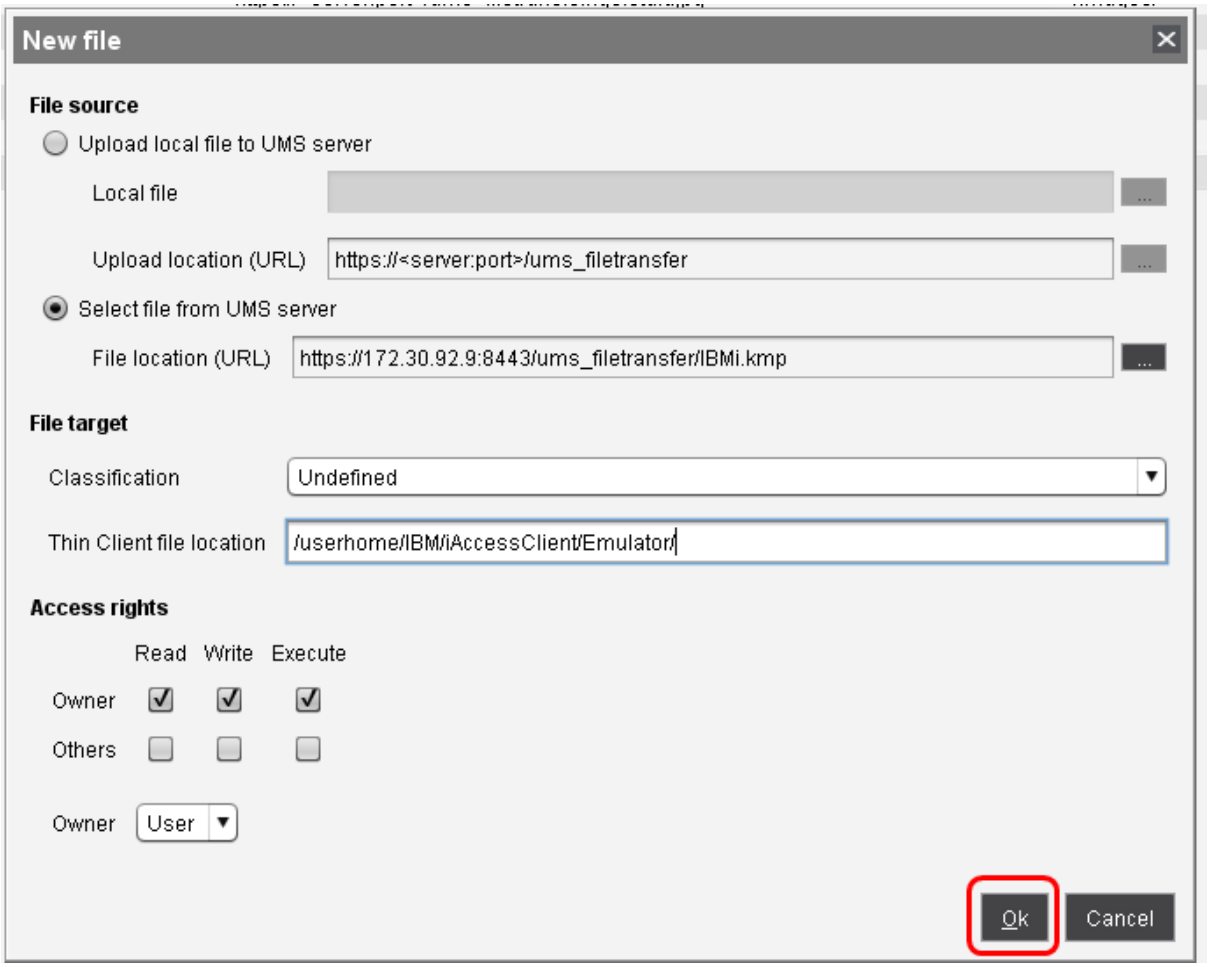
4. Back in the **New file** dialog, enter the **Thin Client file location** as follows: `/userhome/IBM/iAccessClient/Emulator/`



5. Ensure that the **Access rights** and **Owner** are set as follows:
    - **Owner** rights: **Read**, **Write**, **Execute**
    - **Owner**: "User"


New file
File source
Upload local file to UMS server
Local file
Upload location (URL)
https://<server:port>/ums_filetransfer
Select file from UMS server
File location (URL)
https://172.30.92.9:8443/ums_filetransfer/IBMi.kmp
File target
Classification
Undefined
Thin Client file location
/userhome/IBM/iAccessClient/Emulator/
Access rights
Read
Write
Execute
Owner
Others
Owner
User
Ok
Cancel

6. Click **Ok**.

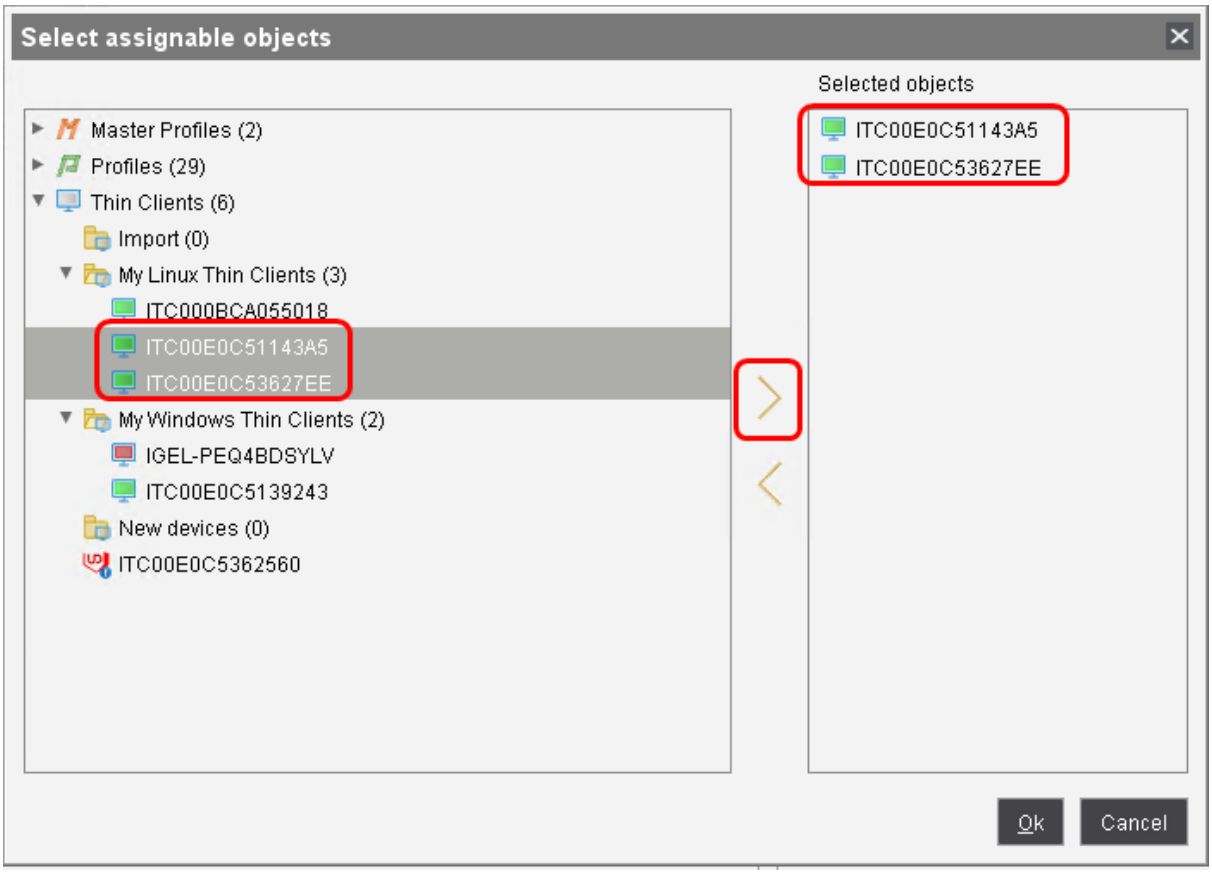


The file object "IBMi.kmp" is created.

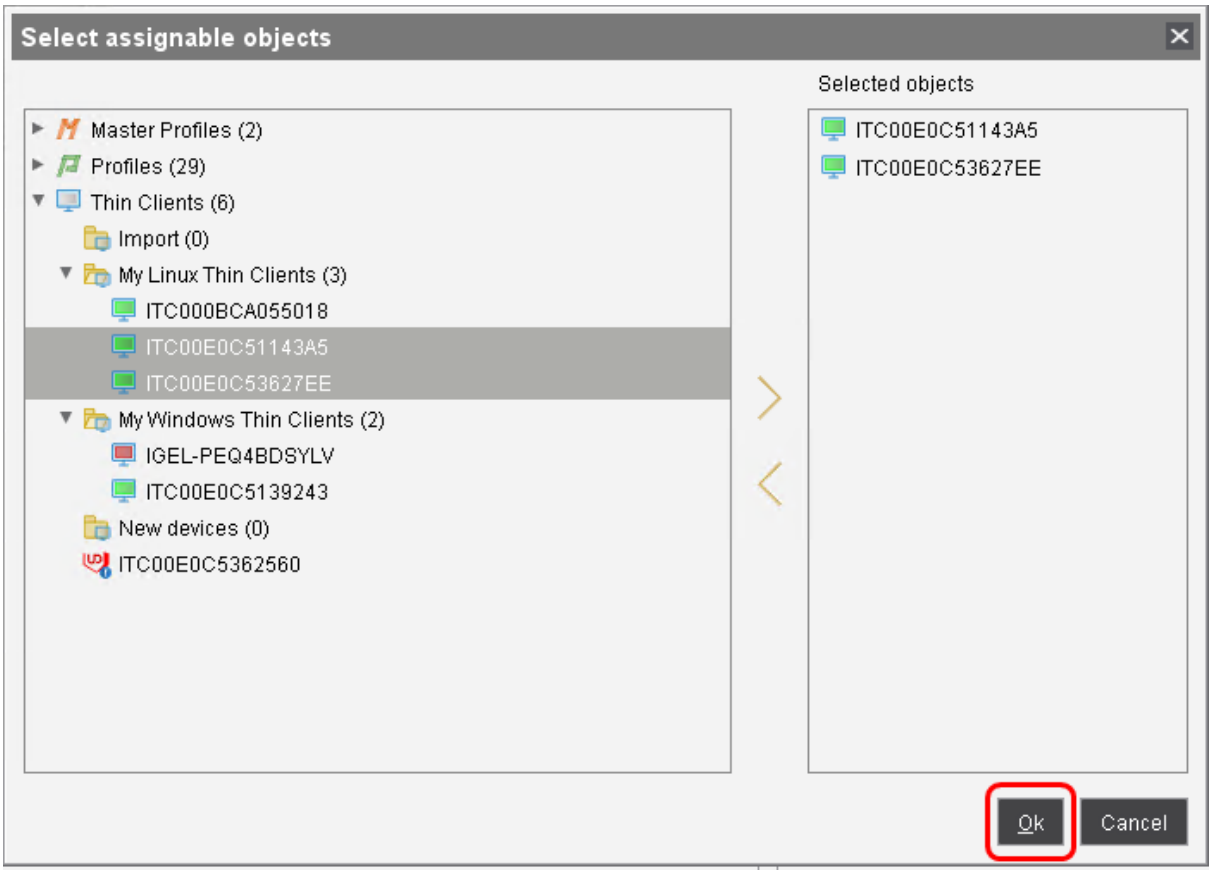
Assigning the File Object to Thin Clients

1. In the navigation tree, select the file object "IBMi.kmp" and click

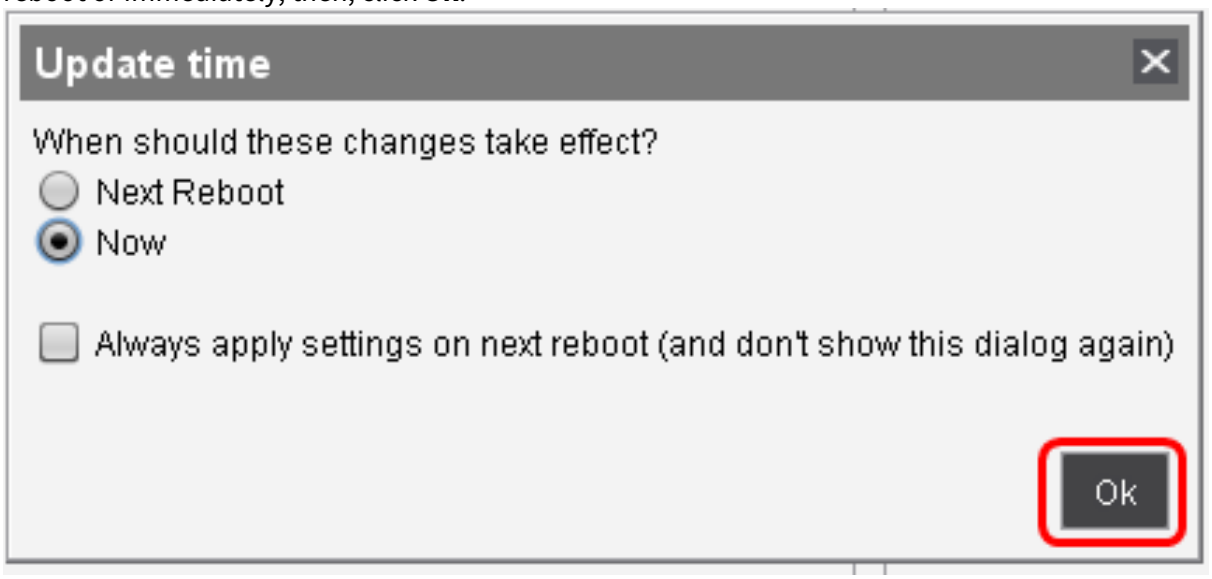
   in the **Assigned objects** area (upper right).
2. In the **Select assignable objects** dialog, select the thin clients to which you want to assign the new key mapping and add them to the **Selected objects** area.


Select assignable objects
Selected objects
Master Profiles (2)
Profiles (29)
Thin Clients (6)
Import (0)
My Linux Thin Clients (3)
ITC000BCA055018
ITC00E0C51143A5
ITC00E0C53627EE
My Windows Thin Clients (2)
IGEL-PEQ4BDSYLV
ITC00E0C5139243
New devices (0)
ITC00E0C5362560
ITC00E0C51143A5
ITC00E0C53627EE
Ok
Cancel

3. Click **Ok**.



4. In the **Update time** dialog, choose whether the file should be assigned to the thin clients at next reboot or immediately; then, click **Ok**.



The file is transferred to the thin clients.

Imprivata

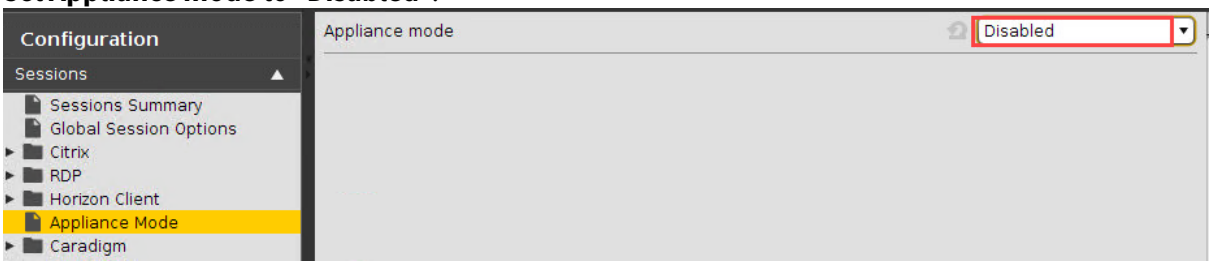
- How to Clear the Imprivata Data Partition (see page 506)
- Imprivata: Session Customization (see page 507)

How to Clear the Imprivata Data Partition

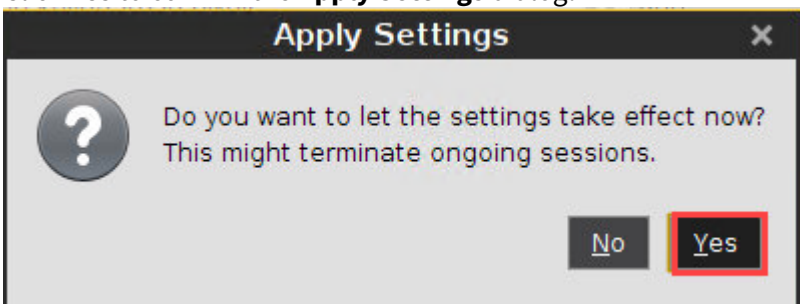
The function that explicitly clears the Imprivata data partition has been removed. However, you can simply emulate this feature by disabling and re-enabling the Imprivata appliance mode.

If you already have a valid appliance running and want to delete the Imprivata data partition, take the following steps:

1. In the IGEL Setup, go to **Sessions > Appliance Mode.**
2. Set **Appliance mode** to "**Disabled**".



3. Click **Ok** to save the setting.
4. Click **Yes** to confirm the **Apply Settings** dialog**.**



   Normal desktop mode is active. The Imprivata data partition is void now.
5. In the IGEL Setup, go to **Sessions > Appliance Mode.**
6. Set **Appliance Mode** to "**Imprivata**".
7. In the **Set the URL to the Server** field, enter the new server address.

8. Click **Ok** and confirm the **Apply Settings** dialog.
   Now you have a fresh Imprivata appliance mode without any outdated data.

Imprivata: Session Customization

You can make the same settings in the **IMPRIVATA_RDP** (**IGEL Setup > RDP > RDP Sessions > Imprivata_RDP**) and **IMPRIVATA_VMware** (**IGEL Setup > Horizon Client > Horizon Client Sessions > IMPRIVATA_VMware**) sessions as in the standard sessions (see the description for RDP Session (see page 1339) and Horizon Client Session (see page 1399)).

> **IMPRIVATA_RDP** and **IMPRIVATA_VMware** will be shown in the IGEL Setup when **Imprivata** is selected under **Setup > Sessions > Appliance Mode**, see Imprivata (see page 1419).

However, the changes under the following subsections will be ignored:

Imprivata_VMware Session

- **Connection Settings**

> You can also ignore the VMware protocol selected by the Imprivata appliance by activating the registry key **imprivata.ignore_horizon_protocol** under **System > Registry**. Instead, the local selection under **Horizon Client > Horizon Client Global > Server Options > Preferred desktop protocol** will be used.

Imprivata_RDP Session

- **Server**
- **Logon**

Microsoft Azure Virtual Desktop (AVD)

This IGEL release is a build of IGEL OS which includes the AVD client as a configurable method for connecting to Azure Virtual Desktops.

- Feature Matrix: AVD (RDP3) for IGEL OS 11 (see page 509)
- How to Connect IGEL OS to Azure Virtual Desktop (see page 513)
- Importance of Keeping IGEL OS Firmware Up-to-Date for Microsoft AVD and Windows 365 CloudPC (see page 517)
- Microsoft Teams Feature Comparison for IGEL OS (see page 531)
- Authentication Issue with Microsoft Azure Virtual Desktop on IGEL OS (see page 533)

Feature Matrix: AVD (RDP3) for IGEL OS 11

The following matrix shows a selection of features and their state of implementation.

Feature	Linux RD Core SDK by Microsoft	IGEL OS RDP3 Client	Notes
AzureAD authentication	not applicable	yes	
Azure Resource Manager v2 Feed support	yes	yes	
Folder redirection	yes	yes	Folder redirection is bound to the /media folder, so that locally mounted storage devices, including USB sticks, will be forwarded to the remote session.
Dynamic folder redirection	no	no	User may select specific drives/folders to redirect at run time.
Smartcard redirection	no	no	Smartcard redirection is implemented but not working. The problem exists in the RD Core SDK.
Clipboard redirection (text and images)	yes	yes	
Clipboard redirection (files)	no	no	
Microphone redirection	yes	yes	
Speaker redirection	yes	yes	
Webcam redirection	not applicable	yes	Fabulatech webcam redirection (see page 1660) is implemented.

Feature	Linux RD Core SDK by Microsoft	IGEL OS RDP3 Client	Notes
Printer redirection	yes	yes	ezeep cloud printing (see page 1676) is implemented. It is directly related to the ThinPrint configuration. CUPS printer redirection (see page 1675) is implemented.
USB redirection	not applicable	yes	Fabulatech USB redirection (see page 1660) is implemented.
Scanner redirection	not applicable	yes	Fabulatech scanner redirection (see page 1660) is implemented.
Mouse input	yes	yes	
Keyboard input (scancodes)	yes	yes	
Keyboard input (Unicode)	yes	yes	
Keyboard input mapping of dead/special keys	not applicable	yes	
Teams conferencing redirection	yes	yes	The “Annotations” feature is currently not available.
Zoom conferencing redirection	not applicable	yes	Zoom redirection (see page 1677) cannot be activated globally, but only for a specific session.
Multitouch redirection	no	no	No multitouch API present in the Linux RD Core SDK by Microsoft.
AVC Codec support (hardware acceleration)	yes	work in progress	

Feature	Linux RD Core SDK by Microsoft	IGEL OS RDP3 Client	Notes
Dynamic display change	yes	yes	
Monitor DPI sync	yes	yes	
Monitor Layout Sync (multimon)	yes	yes	
Restrict full-screen sessions to single display	not applicable	yes	
On-premises services	not applicable	work in progress	
RemoteApps	yes	limited	Current user interface for RemoteApps control is to be further improved.
Seamless apps	work in progress	no	
Session auto reconnect	yes	yes	
Proxy support	yes	yes	
Local hostname in a session	yes	yes	
Launch a single resource session/ application	not applicable	yes	A resource is launched if only one resource is returned.
Dynamic virtual channel support	yes	work in progress	
UDP network support	work in progress	no	

Feature	Linux RD Core SDK by Microsoft	IGEL OS RDP3 Client	Notes
User-definable hotkeys	not applicable	yes	Session chooser, session switcher, minimize to taskbar
Realtime user experience indicator	work in progress	no	
Configurable AVD Resource Feed	yes	yes	

How to Connect IGEL OS to Azure Virtual Desktop

Quick Start Guide

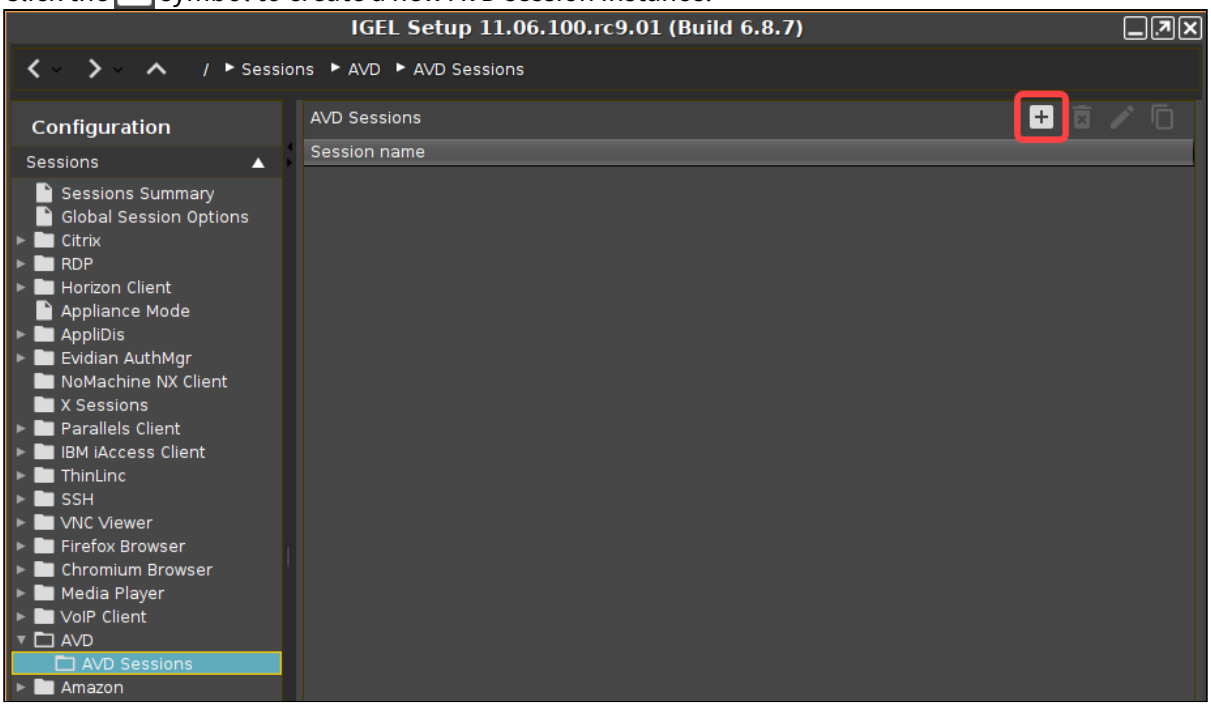
This section describes how to set up an Azure Virtual Desktop (AVD) session (formerly Windows Virtual Desktop, WVD) with IGEL's AVD client based on Microsoft's RD Core SDK for Linux which can be used to connect to an AVD deployment.

Requirements

- Device with IGEL OS 11.03.261 or higher; download the latest version at igel.com/avd[68]
- Azure Virtual Desktop deployment

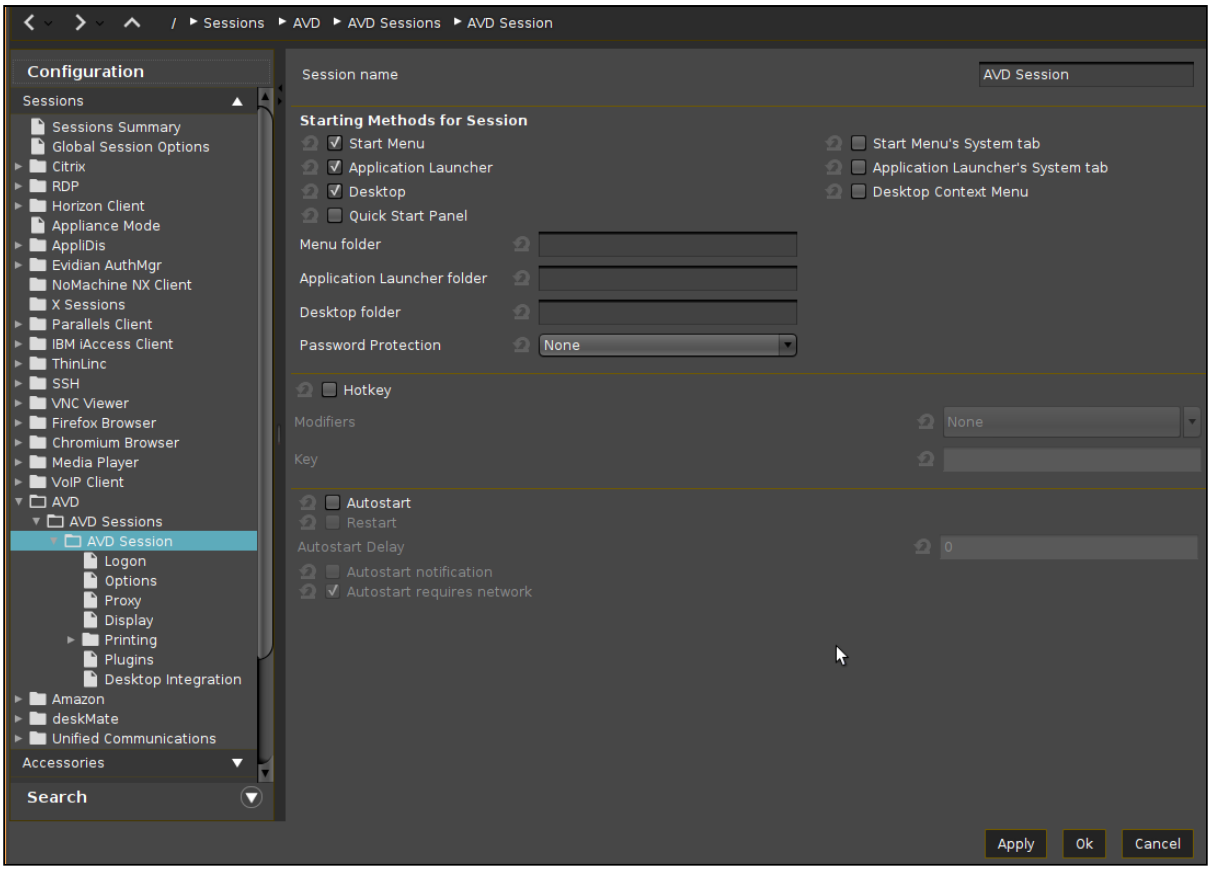
Instructions

1. Open the Setup or the configuration dialog in the UMS and go to **Sessions > AVD > AVD Sessions**.
2. Click the + symbol to create a new AVD session instance.

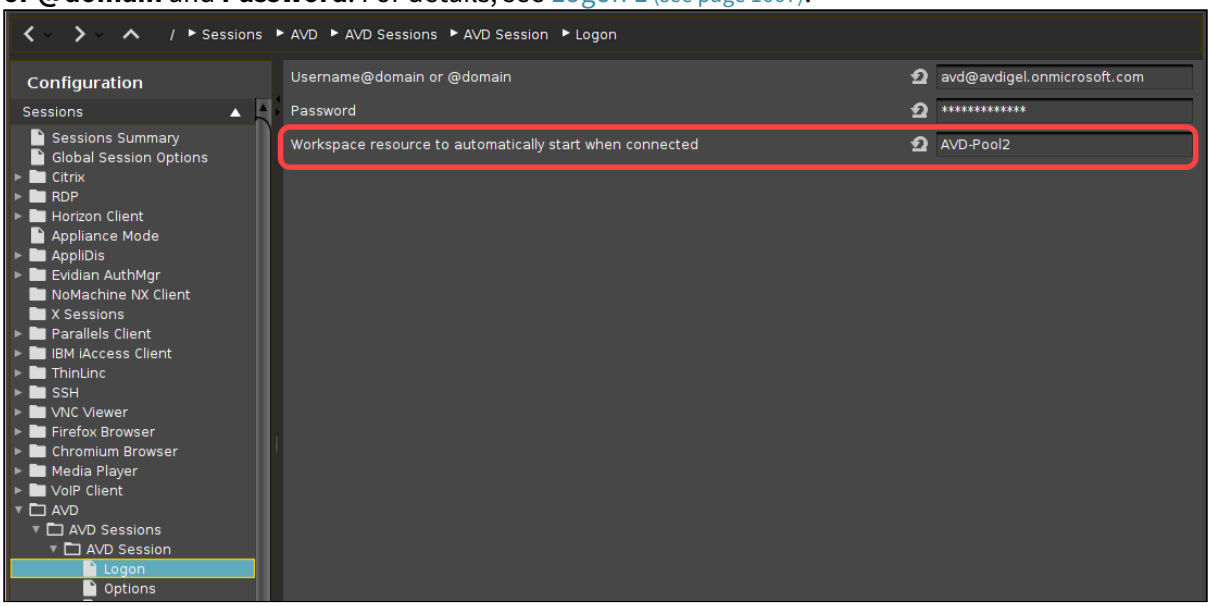


3. Enter a **Session name** and configure the starting methods according to your needs.

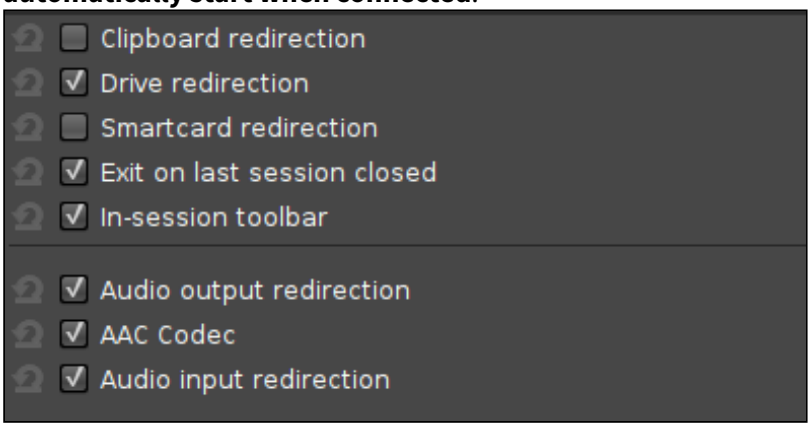
68. https://www.igel.com/igel-solution-family/windows-virtual-desktop/



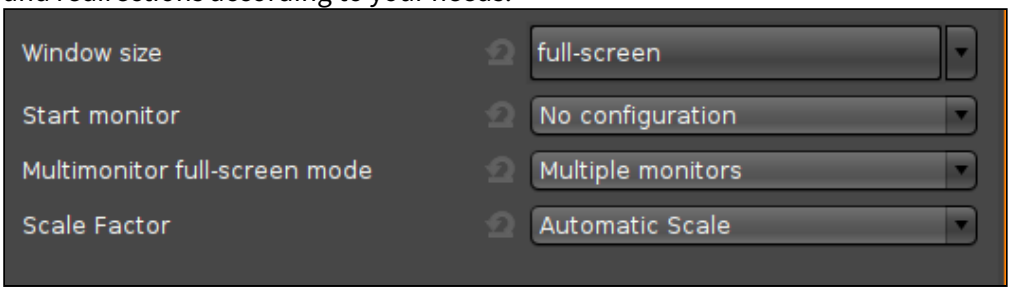
4. If the login is to be started automatically on session startup, go to **Sessions > AVD > AVD Sessions > [Session name] > Logon** and enter your credentials under **Username@domain or @domain** and **Password**. For details, see Logon 1 (see page 1667).



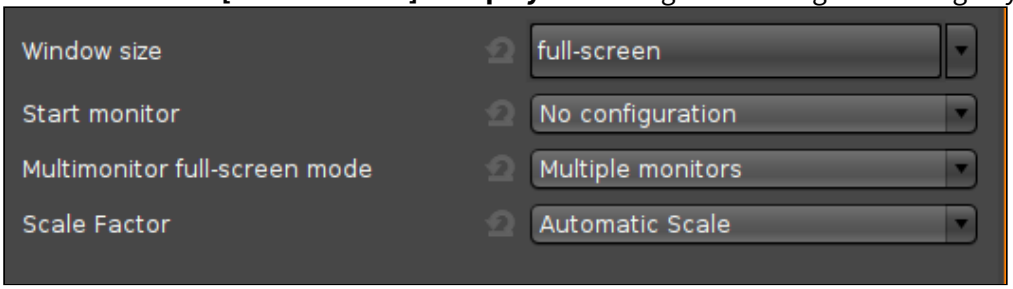
5. If a specific resource is to be started automatically, enter its name under **Workspace resource to automatically start when connected**.



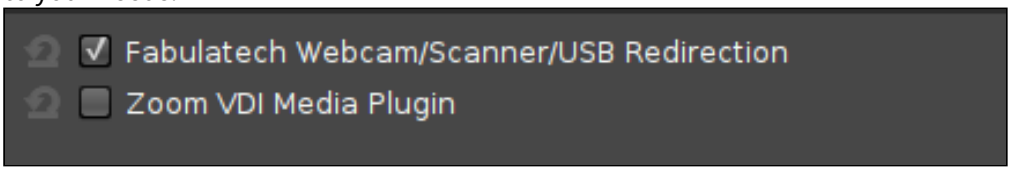
6. Go to **Sessions > AVD > AVD Sessions > [Session name] > Options** and enable or disable features and redirections according to your needs.



7. If you do not want to run the AVD client on all available screens in fullscreen, go to **Sessions > AVD > AVD Sessions > [Session name] > Display** and change the settings according to your needs.



8. Go to **Sessions > AVD > AVD Sessions > [Session name] > Plugins** and enable features according to your needs.



9. Click **Apply** or **OK**.
   The AVD session is configured and can be started with the starting methods you have configured in step 3.

If you want to configure further AVD sessions, start again from step 2.

See also the reference manual chapter AVD Session (see page 1664).

Importance of Keeping IGEL OS Firmware Up-to-Date for Microsoft AVD and Windows 365 CloudPC

If you are running the Microsoft Azure Virtual Desktop (AVD) client on an IGEL OS-powered endpoint (PC, laptop, or client), it is important to ensure that the client version is up-to-date.

Why Is It Important to Keep Your Igel OS Firmware Updated?

If the client version is not up-to-date, changes on the Microsoft AVD's server-side could lead to functionality issues. The latest IGEL OS firmware version is, in most cases, the current official build. To find the latest version, see **https://www.igel.com/software-downloads/workspace-edition/ >** click **OS 11** to expand the relevant section.

However, an IGEL OS private build may be released to adapt for server-side changes that have been introduced between IGEL OS releases. This way, we maintain existing functionality and support new features/functionality. Therefore, please refer to www.igel.com/avd[69] for the latest Microsoft AVD / Windows 365 CloudPC specific IGEL OS releases.

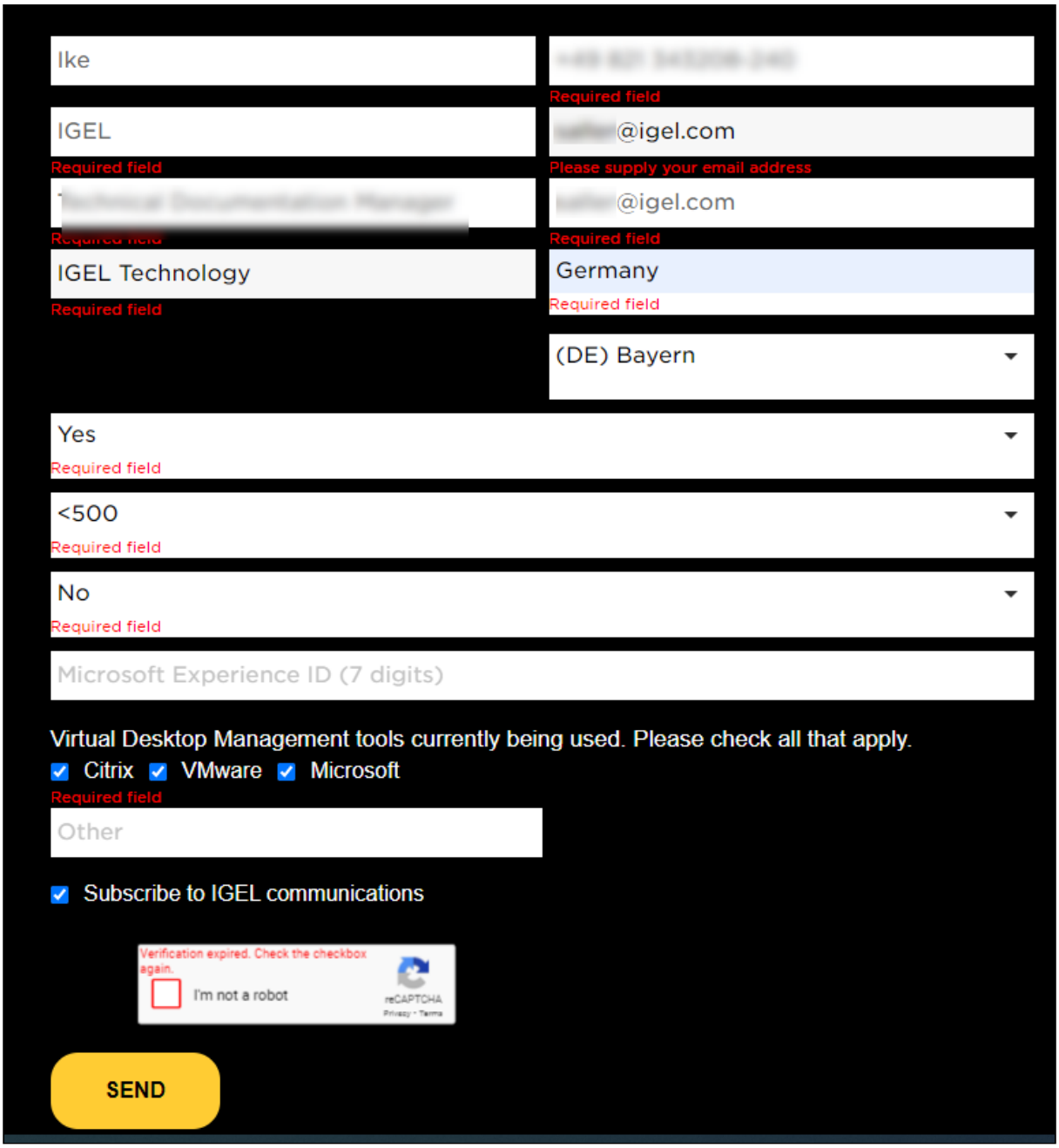
IGEL Environment

- Endpoints with IGEL OS 11
- IGEL AVD client is used for Azure Virtual Desktop (AVD) and Windows 365 CloudPC by Microsoft
- Universal Management Suite (UMS) 6.08 or higher

How to Check for the Latest IGEL OS Firmware Version

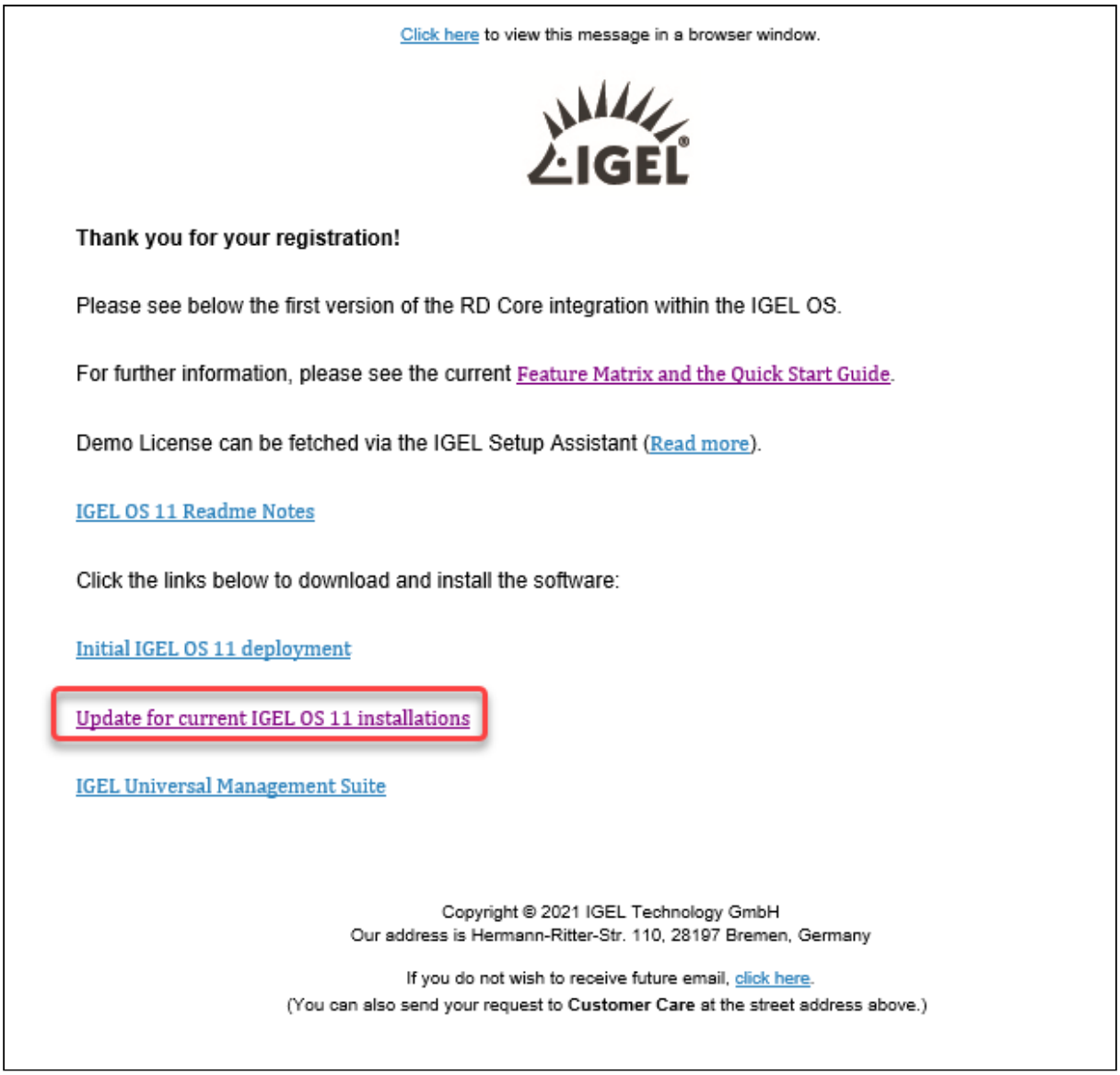
1. Open the web browser and go to www.igel.com/avd[70].
2. Fill in the form to register for AVD client access and submit it.

69. http://www.igel.com/avd
70. http://www.igel.com/avd



After a few minutes, you will receive a confirmation mail from IGEL.

3. In the confirmation mail, click **Update for current IGEL OS 11 installations**.



The IGEL OS firmware with the latest AVD client is downloaded (official or private build).

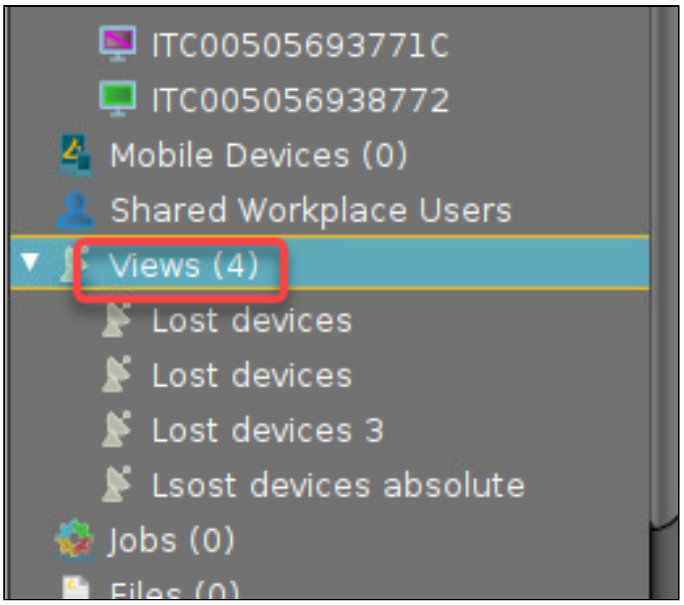
4. Note the version number that can be derived from the file name.

   Example: When the file name is `lxos_11.06.100_public.zip`, the version is 11.06.100.

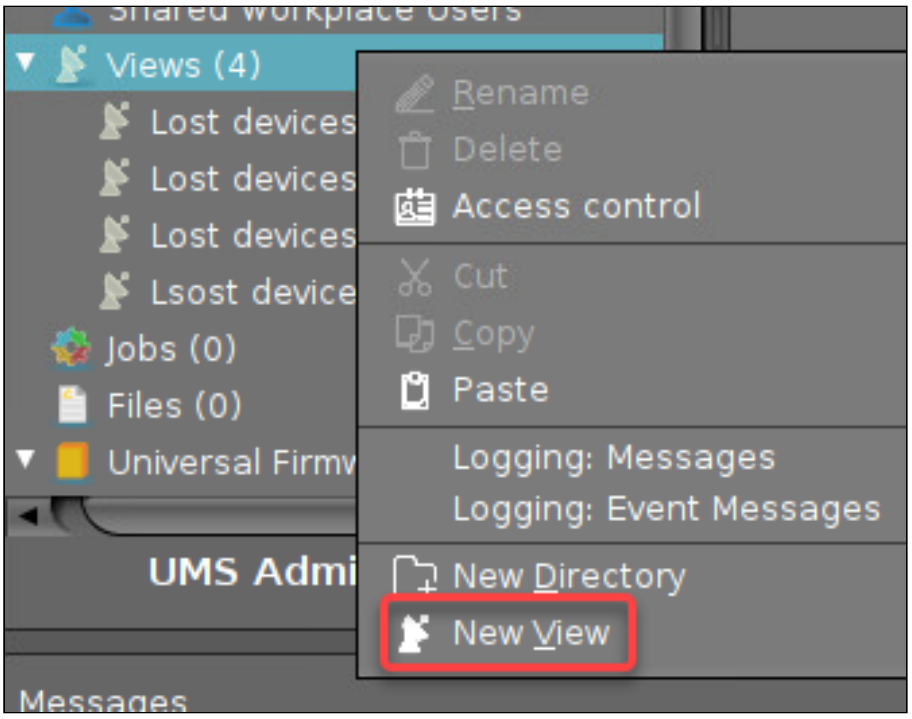
How to Check If the IGEL OS Version Is Out-of-Date

We will create a view to find out which endpoint devices are running a firmware version lower than the one with the latest AVD client.

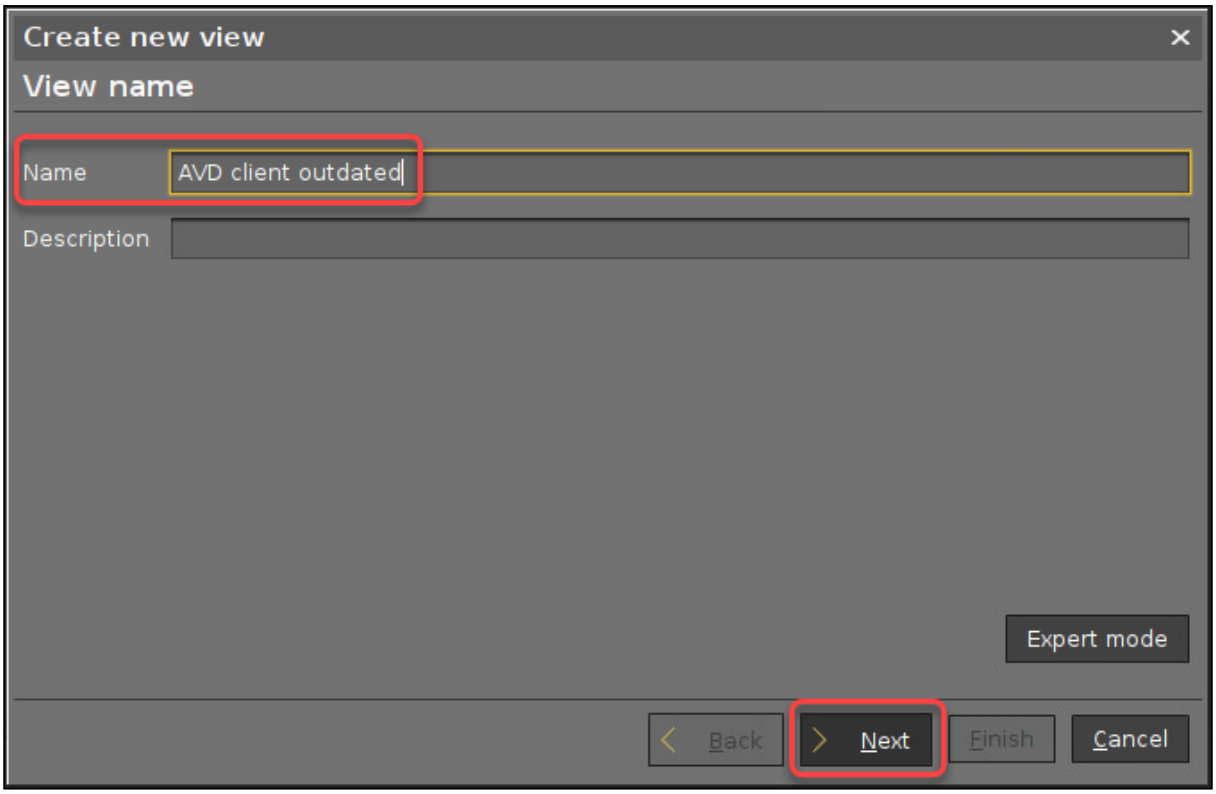
1. Open the UMS console and in the structure tree, go to **Views**.



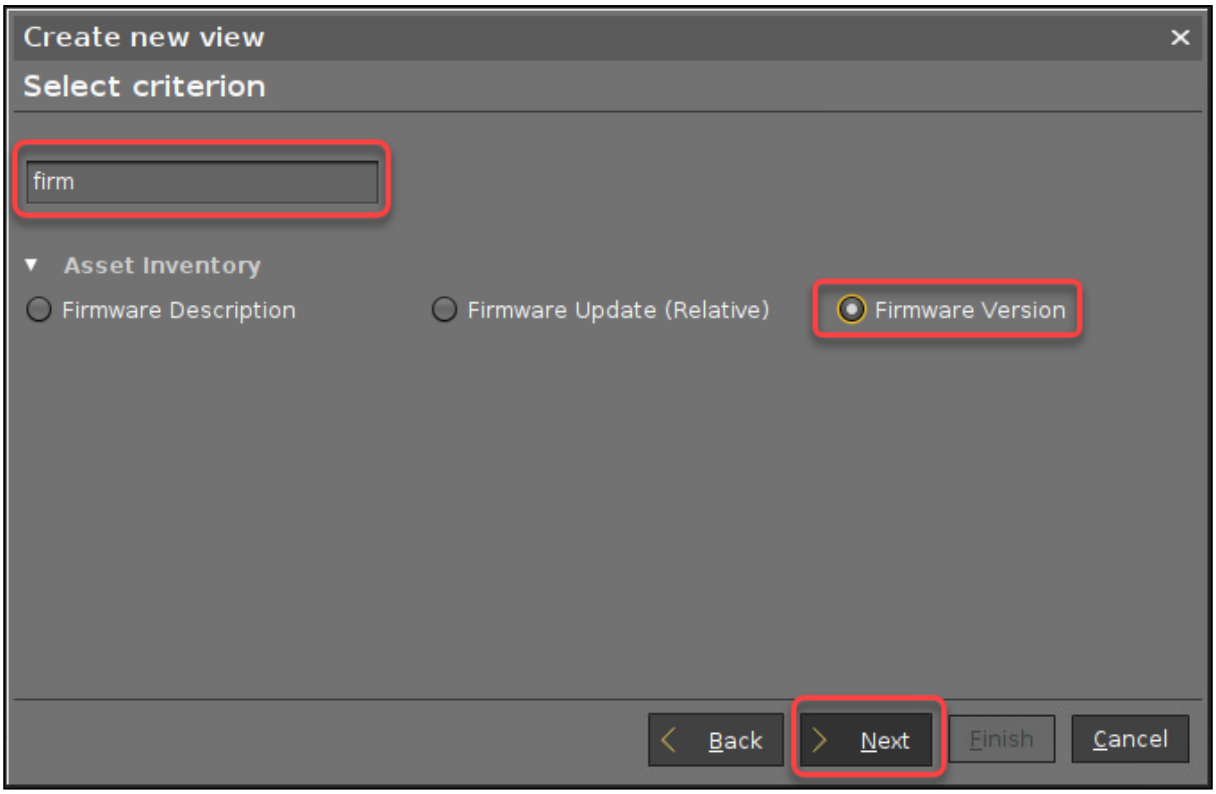
2. Select **New View**.



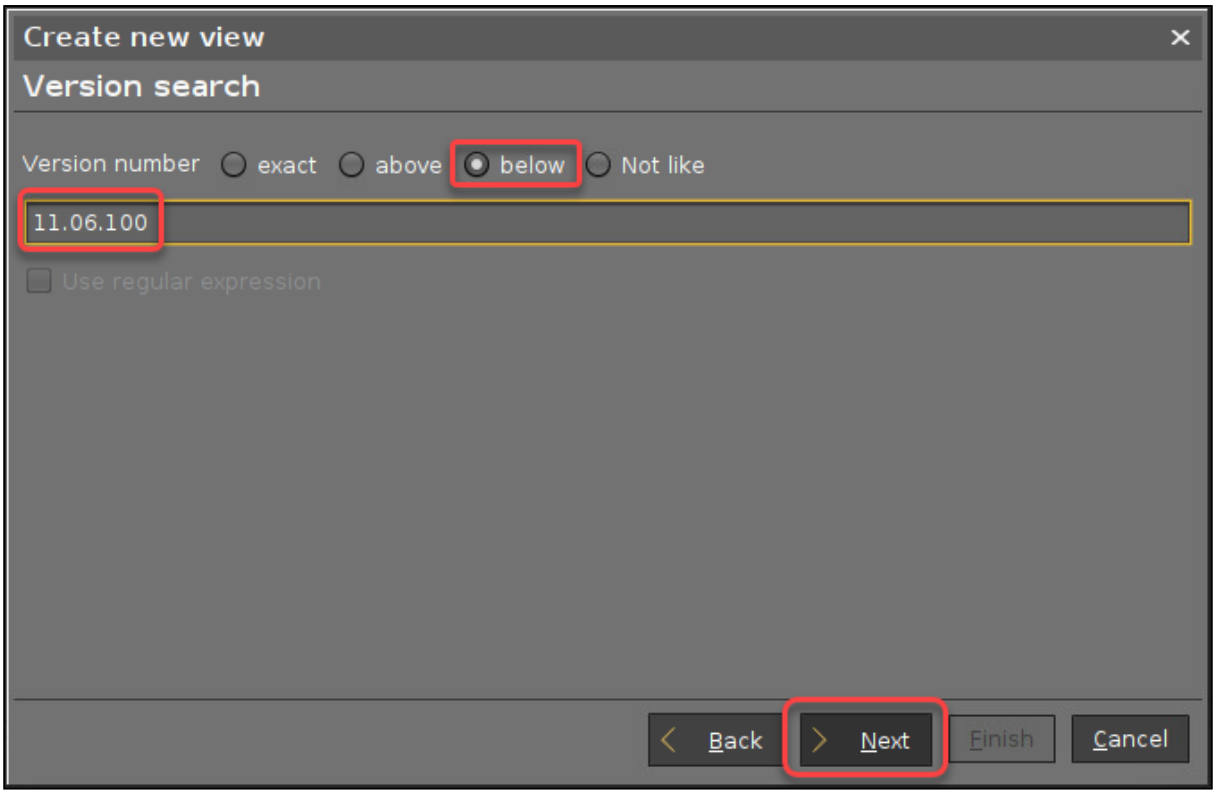
3. Enter an appropriate **Name** and click **Next**.



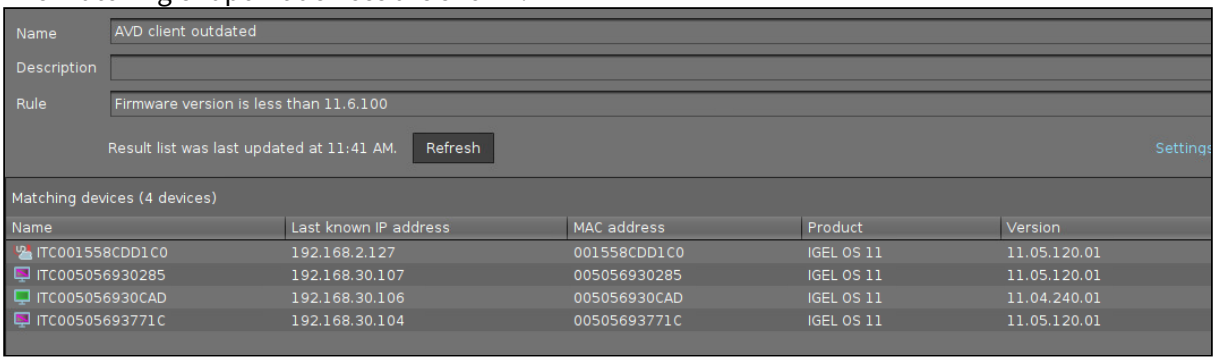
4. In the search field, enter "firm", select **Firmware version,** and click **Next**.



5. Select **below**, enter the version number of the firmware you have downloaded beforehand, and click **Next**.



6. Click **Finish**.
   The matching endpoint devices are shown.

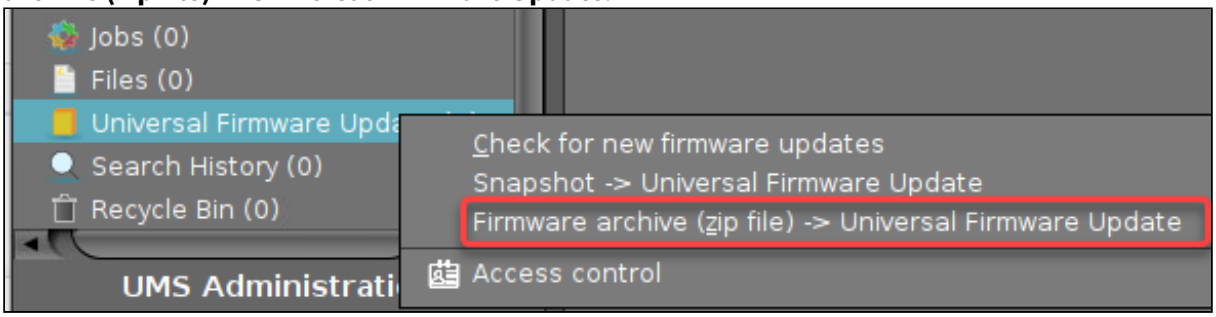


How to Update IGEL OS Endpoint Devices to the Latest Firmware Version

In the following instructions, we will use the Universal Firmware Update feature of the UMS. For alternative methods, see Firmware Update (see page 310), Buddy Update (see page 303), Updating IGEL OS Using a USB Storage Device (see page 314), and Updating the Firmware using the Linux Console (see page 315).

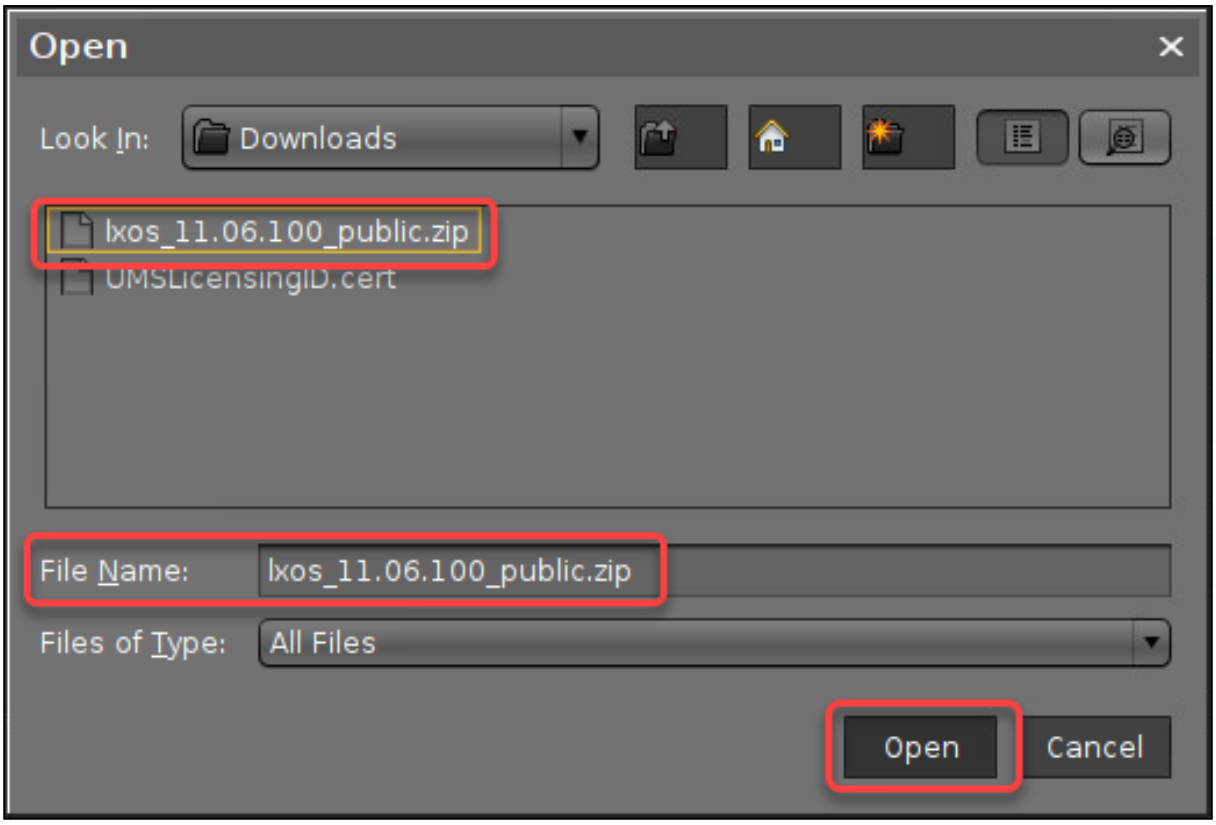
1. Make sure that the firmware file (in our example: `lxos_11.06.100_public.zip`) can be accessed from the machine that hosts the UMS Console (via local file or network drive).

2. In the structure tree of the UMS Console, go to **Universal Firmware Update** and select **Firmware archive (zip file) -> Universal Firmware Update**.

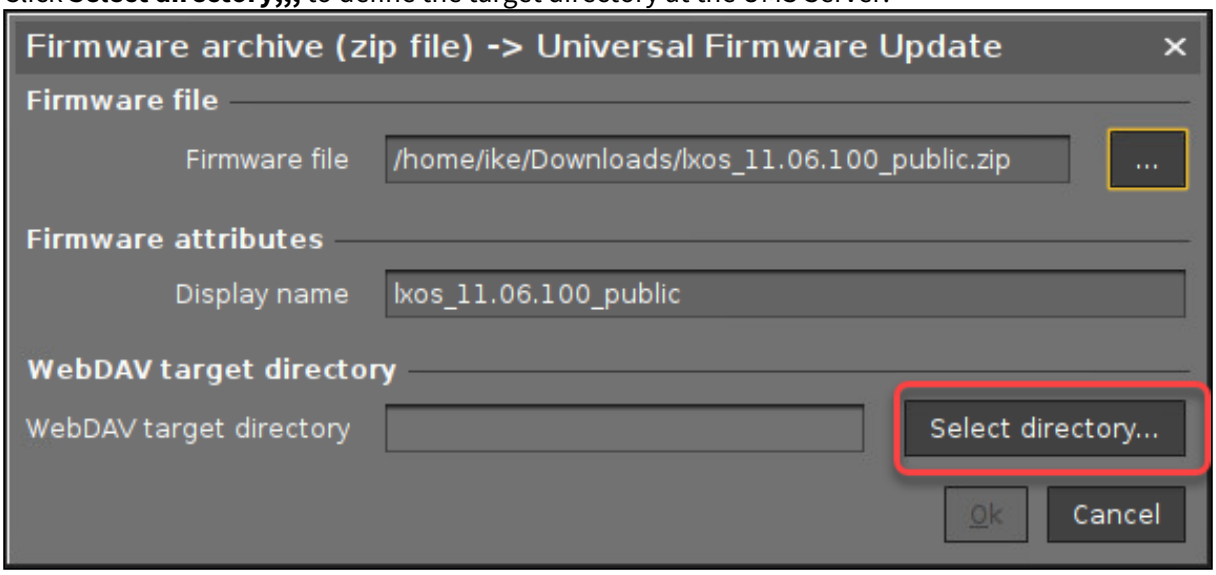


3. Make sure that **Firmware archive (zip file) -> Universal Firmware Update** is selected and click **Next**.

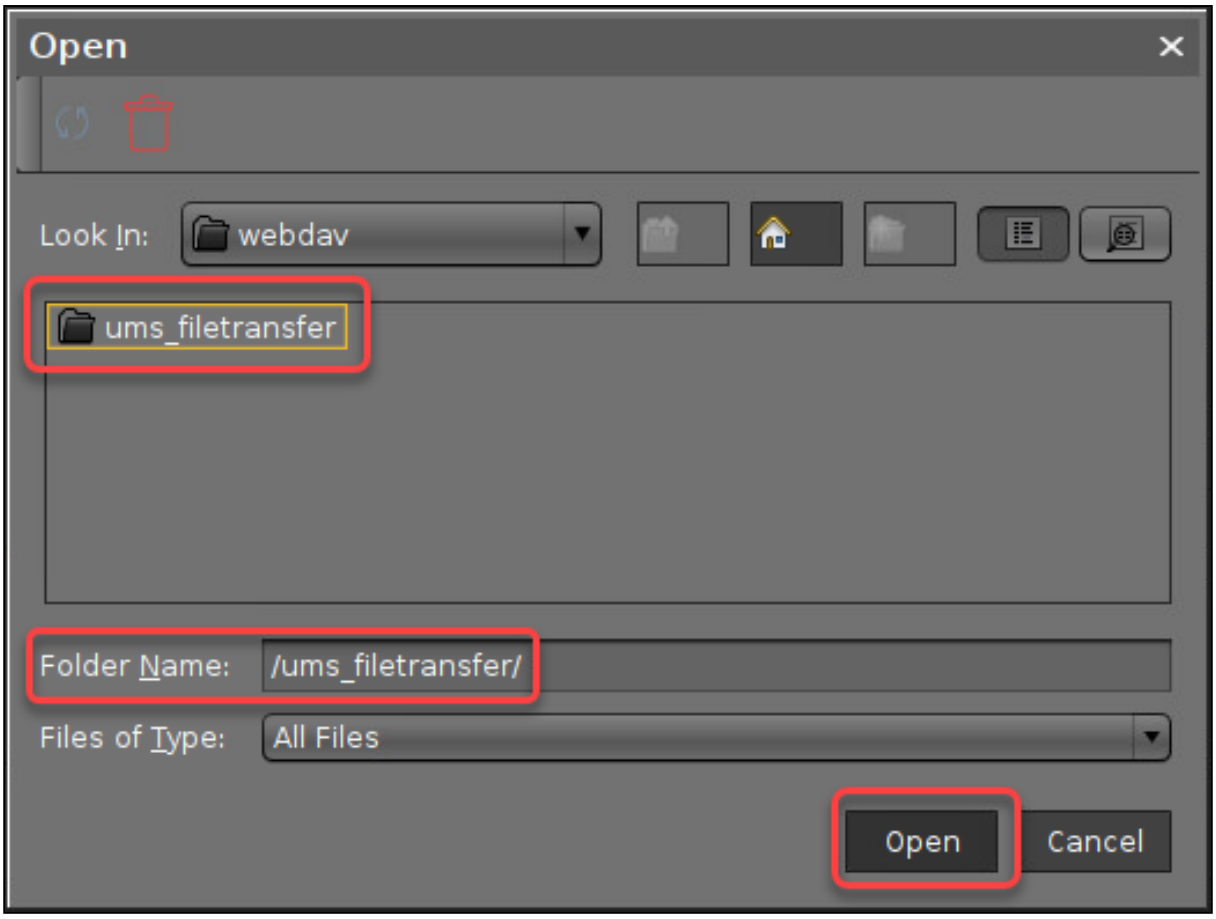
4. Click the file chooser icon, find the firmware file and click **Open**.



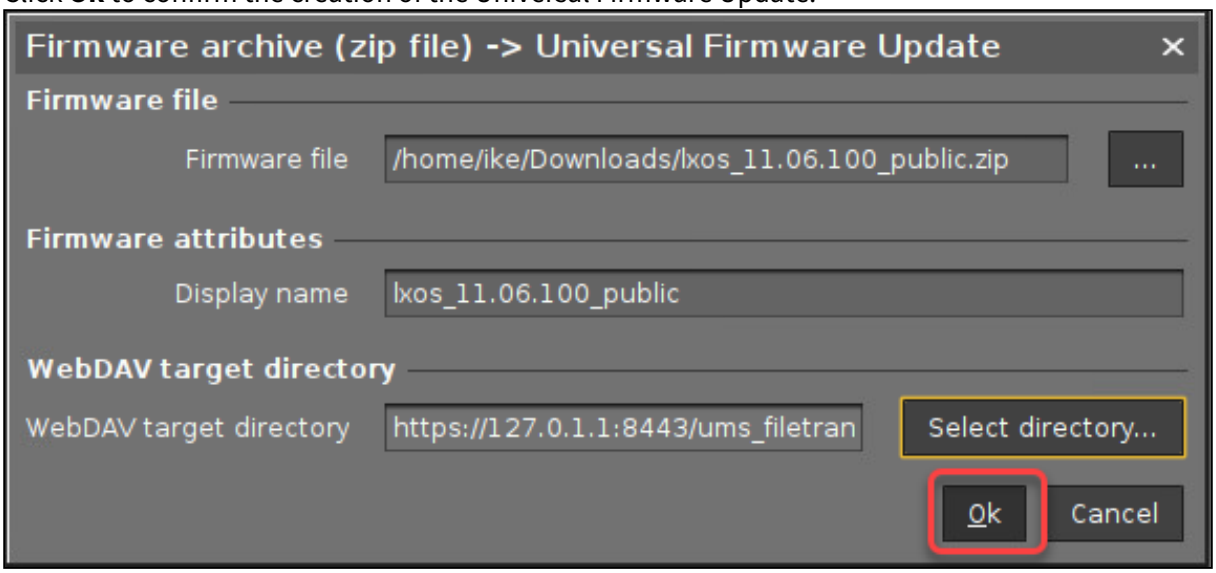
5. Click **Select directory,,,** to define the target directory at the UMS Server.



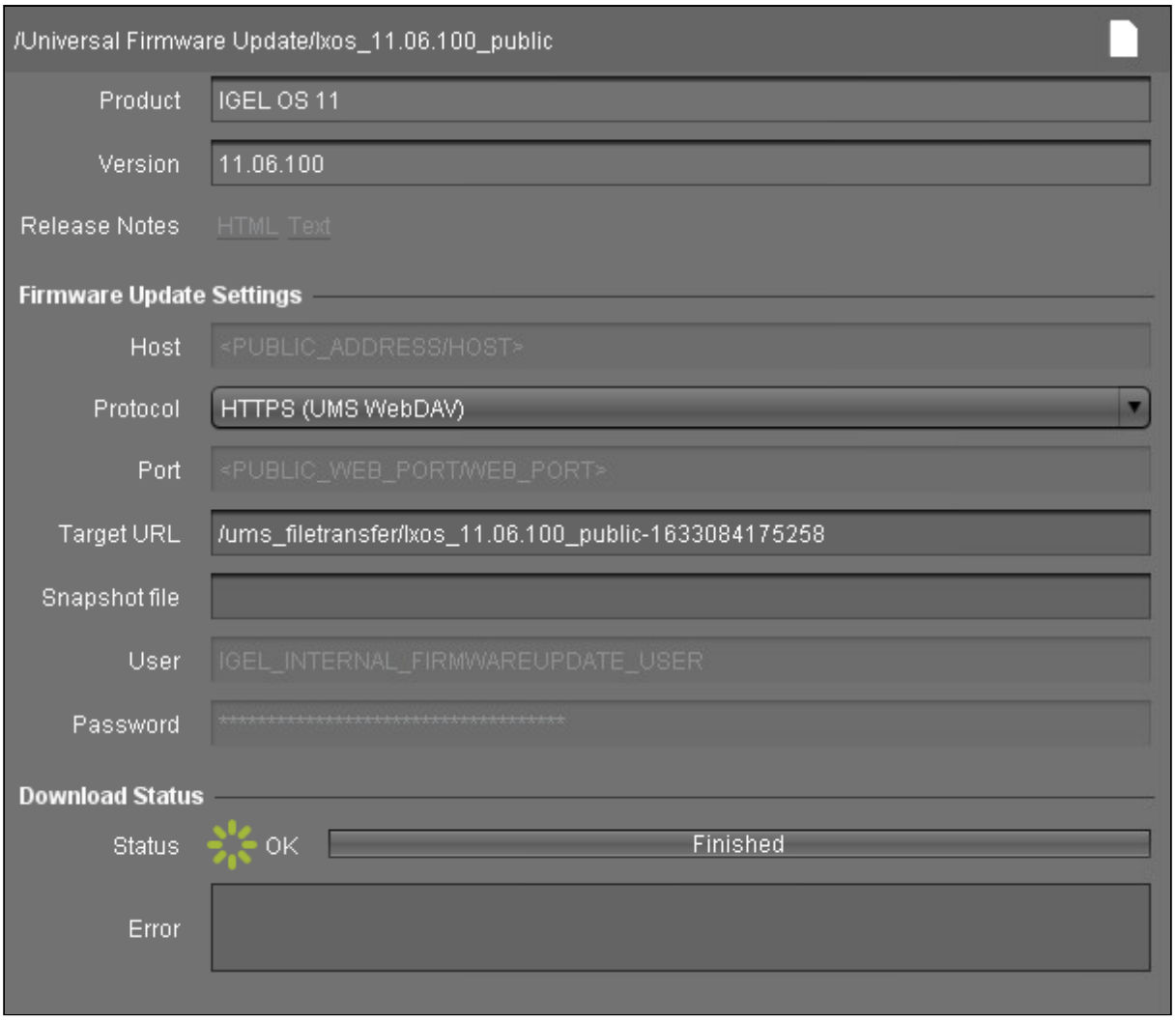
6. Select the directory, typically `ums_filetransfer`, and click **Open**.



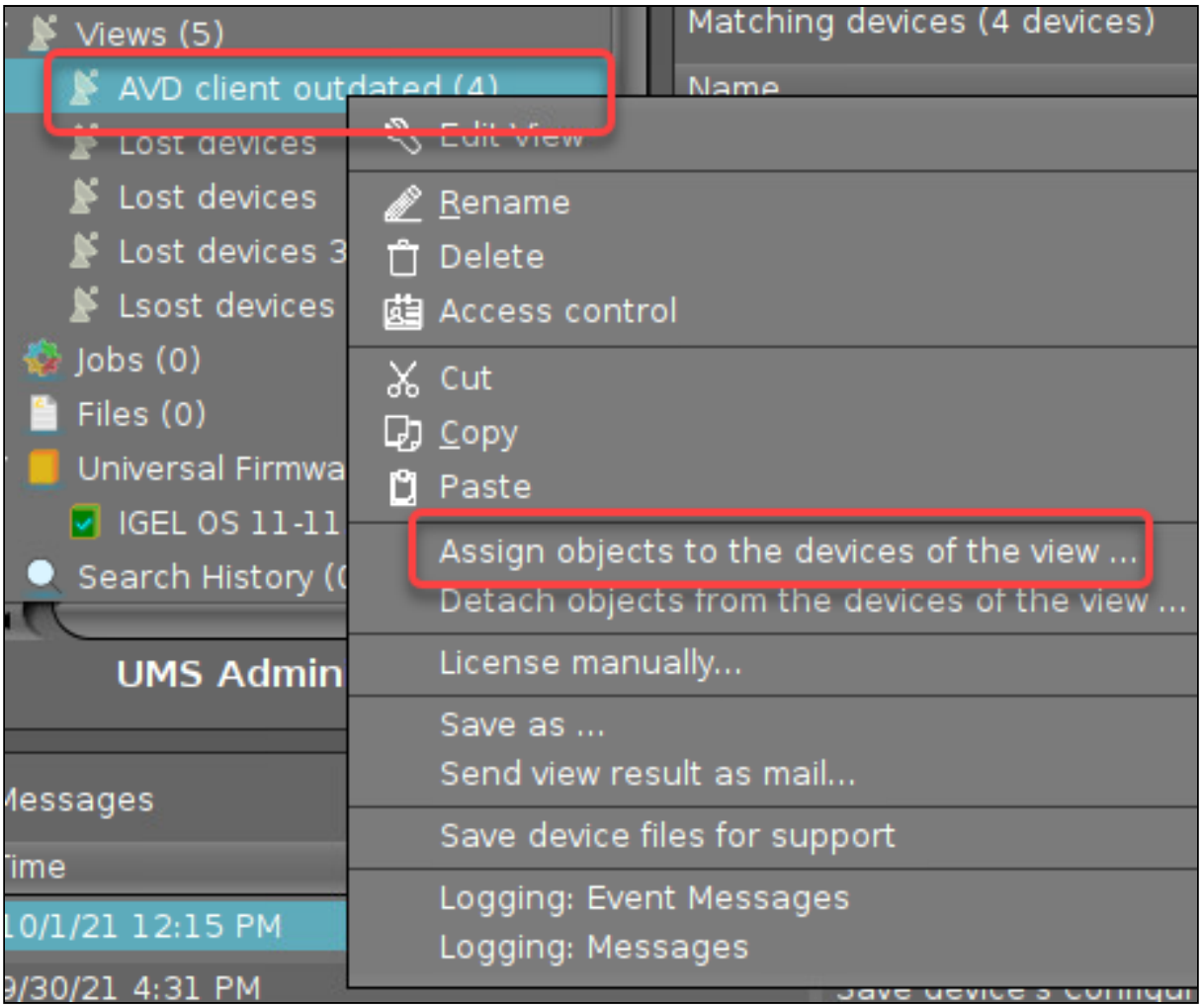
7. Click **Ok** to confirm the creation of the Universal Firmware Update.



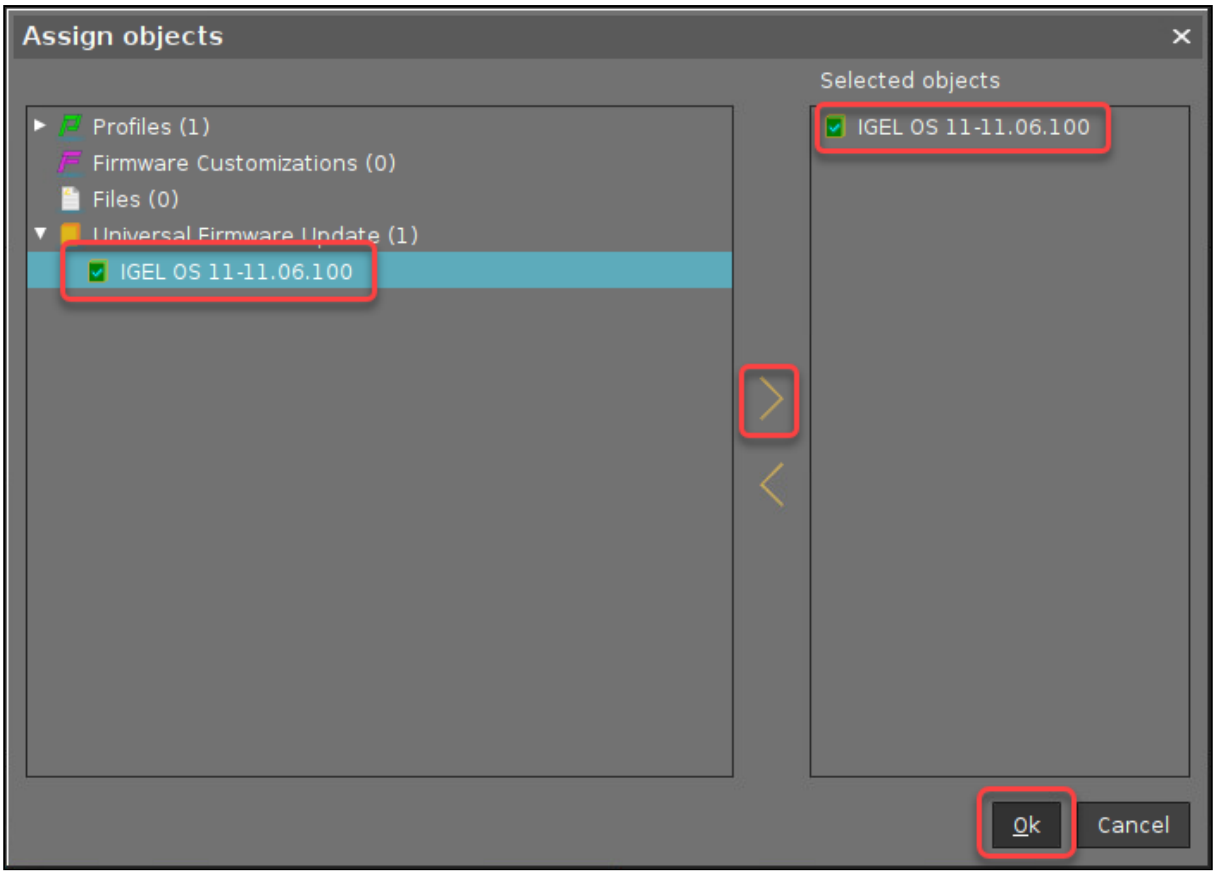
If everything went well, the new Universal Firmware Update is displayed.



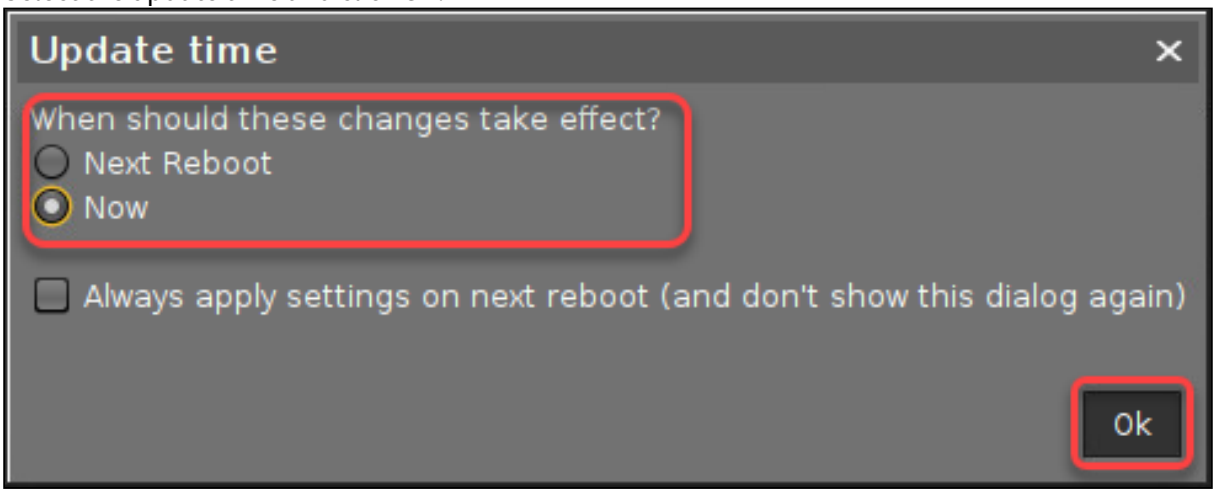
8. Go to the view you have created beforehand, open the context menu, and select **Assign objects to the devices of the view...**.



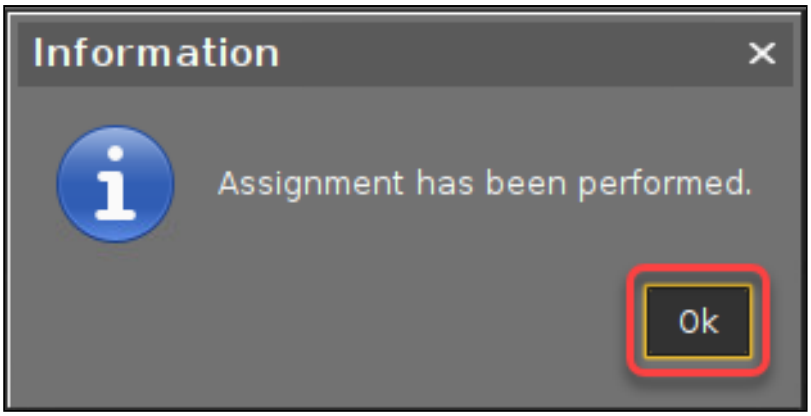
9. Select the Universal Firmware Update and click **Ok**.



10. Select the update time and click **Ok**.



11. Confirm the message window.



On the next reboot, the endpoint devices will update their firmware.

Whether you are implementing classic VDI, virtual apps, DaaS, or in this case AVD, it is always a good practice to make sure you are running the very latest version of IGEL OS to take advantage of the latest features.

Microsoft Teams Feature Comparison for IGEL OS

> **Rolling Release Info: OS 11.07.110**
>
> The information provided here is valid with IGEL OS 11.07.110 and higher.

> The information presented here reflects the state on May 12, 2022.
> The information was mostly obtained from https://support.microsoft.com/en-us/office/teams-features-by-platform-debe7ff4-7db4-4138-b7d0-fcc276f392d3

Feature	IGEL OS AVD / Windows 365	IGEL OS Citrix	Windows 10 AVD / Windows 365	Windows 10 Native	Comments
Audio Calls					
One-to-One Call	yes	yes	yes	yes	
Group Call (3+ users)	yes	yes	yes	yes	
Video Calls					
One-to-One Call	yes	yes	yes	yes	
Group Call (3+ users)*	yes	yes*	yes	yes	* Random minor issues with the video feeds of users connected to media-optimized Teams sessions. Resizing the Teams application window and/or turning webcams on/off often solves the problems.
Gallery View	yes	yes	yes	yes	
Large Gallery View	yes	yes	yes	not applicable	
Together Mode	yes	yes	yes	yes	

Feature	IGEL OS AVD / Windows 365	IGEL OS Citrix	Windows 10 AVD / Windows 365	Windows 10 Native	Comments
Desktop Sharing	yes	yes*	yes	yes	* Presenter's webcam feed not available while sharing desktop; presenter must also restart webcam after stopping desktop share.
Presentation Point Sharing (PowerPoint)	yes	yes	yes	yes	
Application Sharing (Non-PowerPoint)	yes*	yes*	yes*	yes*	* OneDrive and SharePoint are the available applications.
User Remote Control	yes	yes	yes	no	
Chat Functions	no	no	no	yes	
Whiteboard Display	no	no	no	yes	
Whiteboard Sharing	yes	yes	yes	no	Full Teams client does not offer a white whiteboard sharing
Document Whiteboard Sharing	yes	yes	yes	yes	Full Teams client offers to share a scanned document or document camera
Background Blur	yes	yes	yes	yes	
Background Virtual	no	no	no	yes	
Device Button Support	no	no	no	yes	Pressing the mute button on the headset is reflected in the Teams mute (button) functionality

Authentication Issue with Microsoft Azure Virtual Desktop on IGEL OS

The IGEL Azure Virtual Desktop client recently underwent critical client-side changes related to the Microsoft's RD Client for Linux SDK to leverage a newly optimized Azure backend for the Azure Virtual Desktop service.

Microsoft updated the RD Client SDK on Nov 29, 2022 which is when they committed their Kestrel code. (commit 89f7e52).

⚠ To avoid being impacted by this upcoming change, please **upgrade to IGEL OS 11.08.330 or newer before August 15** to avoid any impact from the Azure environment changes going into production.

If you want to update your IGEL OS, see Firmware Update Settings for IGEL OS (see page 2056).

Overview

IGEL OS Version	Release Date	Kestrel
11.08.230	13. December 2022	**No**
11.08.290	30. March 2023	**Yes**

IGEL OS 11.08.330 has other enhancements that make it the better choice for those upgrading.

⚠ Microsoft and IGEL recommend that the AVD client be kept as current as possible and that customers upgrade to make sure that compatibilities with new features and guarantee continued support.

For usage of Private Builds:

The first version of IGEL AVD client that we would consider safe would be **1.1.12**.

ℹ Check the corresponding release notes or open a terminal and enter: `/services/avd/bin/igelrdp3 -v` for a direct check.
The Version of the IGEL AVD client is also included in the release notes for private builds. They can be found in `readme.<version>.txt` under the **Component Versions** section. See IGEL OS Release Notes (see page 2282)

What Happens If You Don't Update To the Latest IGEL OS Version?

Users who continue using older versions of the IGEL Azure Virtual Desktop client may experience frequent session disconnections once Microsoft rolls out the backend changes into production.

ℹ If you want to learn more about the technical details regarding the change, please see A Heavy Lift: Bringing Kestrel + YARP to Azure App Services (microsoft.com)[71].”

71. https://devblogs.microsoft.com/dotnet/bringing-kestrel-and-yarp-to-azure-app-services/

If you have any problems regarding the Update, please contact the support via the IGEL Customer Portal[72].

72. https://cosmos.igel.com/csm

SSH

- How to Enable Weaker Algorithms in the Built-in OpenSSH Server (see page 536)
- How to Enable Weaker Algorithms in the SSH Client (see page 537)
- SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100 (see page 538)

How to Enable Weaker Algorithms in the Built-in OpenSSH Server

Problem

You are trying to connect to the built-in OpenSSH server of IGEL OS with an SSH client which does not support the strong algorithms of the server.

Solution

To enable weaker encryption algorithms, proceed as follows:

1. In Setup, go to **System > Registry > network > ssh_server**.
2. Change the settings according to your requirements:
    - **disable_weak_encryption:** Disable this option to enable weaker encryption.
    - **disable_weak_hostkey_algos:** Disable this option to enable weaker host key algorithms.
    - **disable_weak_kexalgorithms:** Disable this option to enable weaker key exchange algorithms.
    - **disable_weak_macs:** Disable this option to enable weaker MACs.
    - **minimal_encryption_level:** The minimal level of encryption

How to Enable Weaker Algorithms in the SSH Client

Environment

IGEL Linux 10.04.100 or higher

Problem

You are trying to connect to an SSH server which does not support the strong algorithms enabled by default in the SSH client.

Solution

To enable weaker encryption algorithms, proceed as follows:

1. In Setup, go to **System > Registry > network > ssh_client**.
2. Change the settings according to your requirements:
    - **disable_weak_encryption**: Disable this option to enable weaker encryption.
    - **disable_weak_hostkey_algos**: Disable this option to enable weaker host key algorithms.
    - **disable_weak_kexalgorithms**: Disable this option to enable weaker key exchange algorithms.
    - **disable_weak_macs**: Disable this option to enable weaker MACs.
    - **minimal_encryption_level**: The minimal level of encryption

SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100

As of IGEL Linux 10.04.100, certain older, less secure algorithms are deprecated in both the SSH client and server.

The following table shows the algorithms enabled by default as of IGEL Linux version 10.04.100.

Key exchange algorithms	• curve25519-sha256@libssh.org • ecdh-sha2-nistp521 • ecdh-sha2-nistp384 • ecdh-sha2-nistp256 • diffie-hellman-group-exchange-sha256
Message authentication codes (MACs)	• hmac-sha2-512-etm@openssh.com • hmac-sha2-256-etm@openssh.com • umac-128-etm@openssh.com • hmac-sha2-512 • hmac-sha2-256 • umac-128@openssh.com
Host keys	• ssh-ed25519-cert-v01@openssh.com • ssh-rsa-cert-v01@openssh.com • ssh-ed25519 • ssh-rsa • ecdsa-sha2-nistp521-cert-v01@openssh.com • ecdsa-sha2-nistp384-cert-v01@openssh.com • ecdsa-sha2-nistp256-cert-v01@openssh.com • ecdsa-sha2-nistp521 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp256

If you need to enable weaker algorithms, see Enable Weaker Algorithms in the SSH client (see page 537) and/or How to Enable Weaker Algorithms in the Built-in OpenSSH Server (see page 536).

Using Amazon WorkSpaces via the HP Anyware PCoIP Client

You can configure an Amazon WorkSpaces session under **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces Session**, see Amazon WorkSpaces (see page 1681).

Alternatively, you can use Amazon WorkSpaces via HP Anyware PCoIP (see page 1651). This is described in the following articles.

- Connecting Your IGEL OS Device to Amazon WorkSpaces with the HP Anyware PCoIP Client (see page 540)
- How to Configure Your HP Anyware Client for Amazon WorkSpaces in IGEL OS (see page 544)
- Broker Types for Connecting to Amazon WorkSpaces with the HP Anyware Client on IGEL OS (see page 546)
- How Can I Use H.264 Acceleration in an HP Anyware PCoIP Session? (see page 547)

Connecting Your IGEL OS Device to Amazon WorkSpaces with the HP Anyware PCoIP Client

You can use the HP Anyware PCoIP client to connect your IGEL OS device to Amazon WorkSpaces. The HP Anyware PCoIP client is an alternative to the Amazon WorkSpaces client (see page 1681).

Set Up the Device Connection

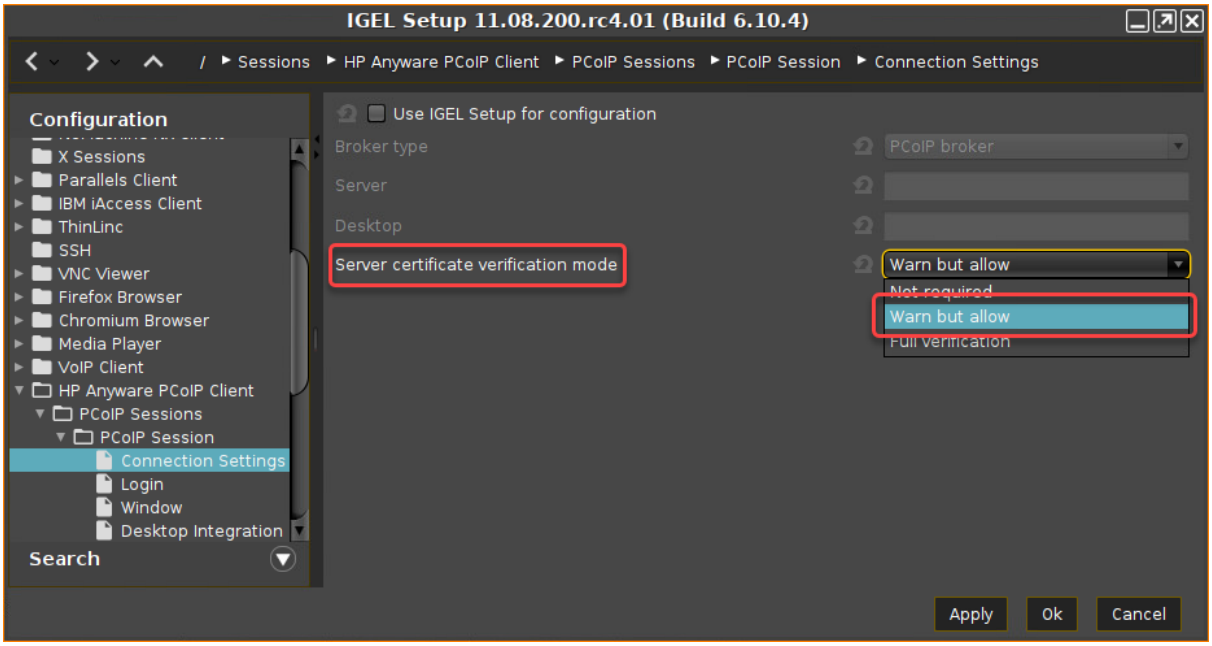
Before you connect the device to Amazon WorkSpaces for the first time, you might need to change some settings. Your Amazon WorkSpaces administrator can provide you with additional setup instructions that are required for your particular environment.

Session Connection

To set the session connection:

1. In the IGEL Setup, go to **Sessions > HP Anyware PCoIP Client > PCoIP Sessions**.
2. Click

   to create a new session.
3. Go to **Connection Settings**.
4. Set **Server certificate verification mode** to "Warn but allow".

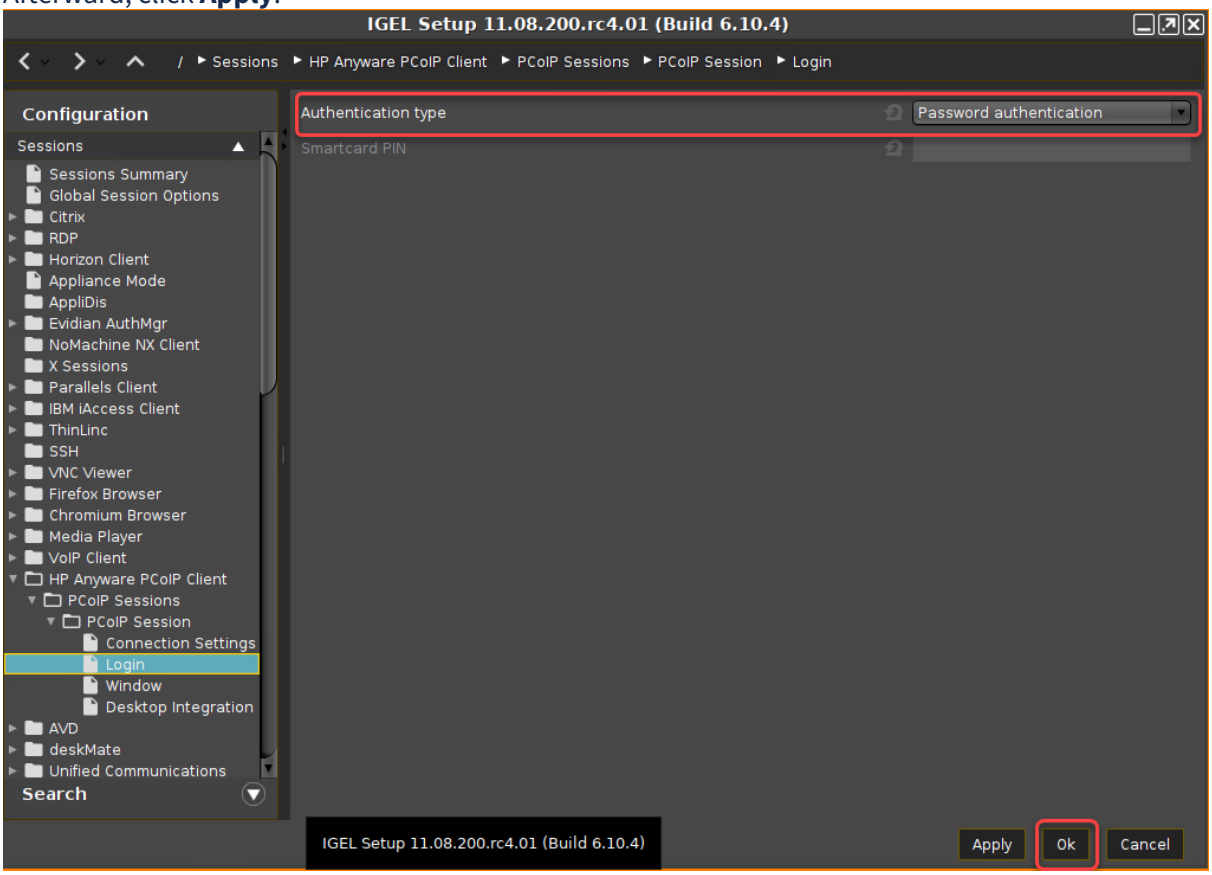


If you do not enable **Use IGEL Setup for configuration**, you have to enter the host address or code in the HP Anyware client login window. See the screenshot under "Connecting to Amazon WorkSpaces".

If you activate **Use IGEL Setup for configuration**, see How to Configure Your HP Anyware Client for Amazon WorkSpaces in IGEL OS (see page 544).

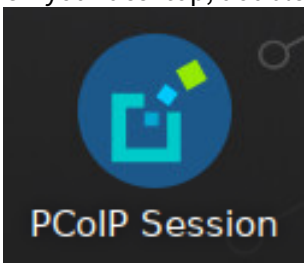
For more information about the connection with the **Broker type** "PCoIP broker" or "Hardhost", see Broker Types for Connecting to Amazon WorkSpaces with the HP Anyware Client on IGEL OS (see page 546).

5. Go to **Login** and make sure that **Authentication type** is set to "Password authentication". Afterward, click **Apply**.



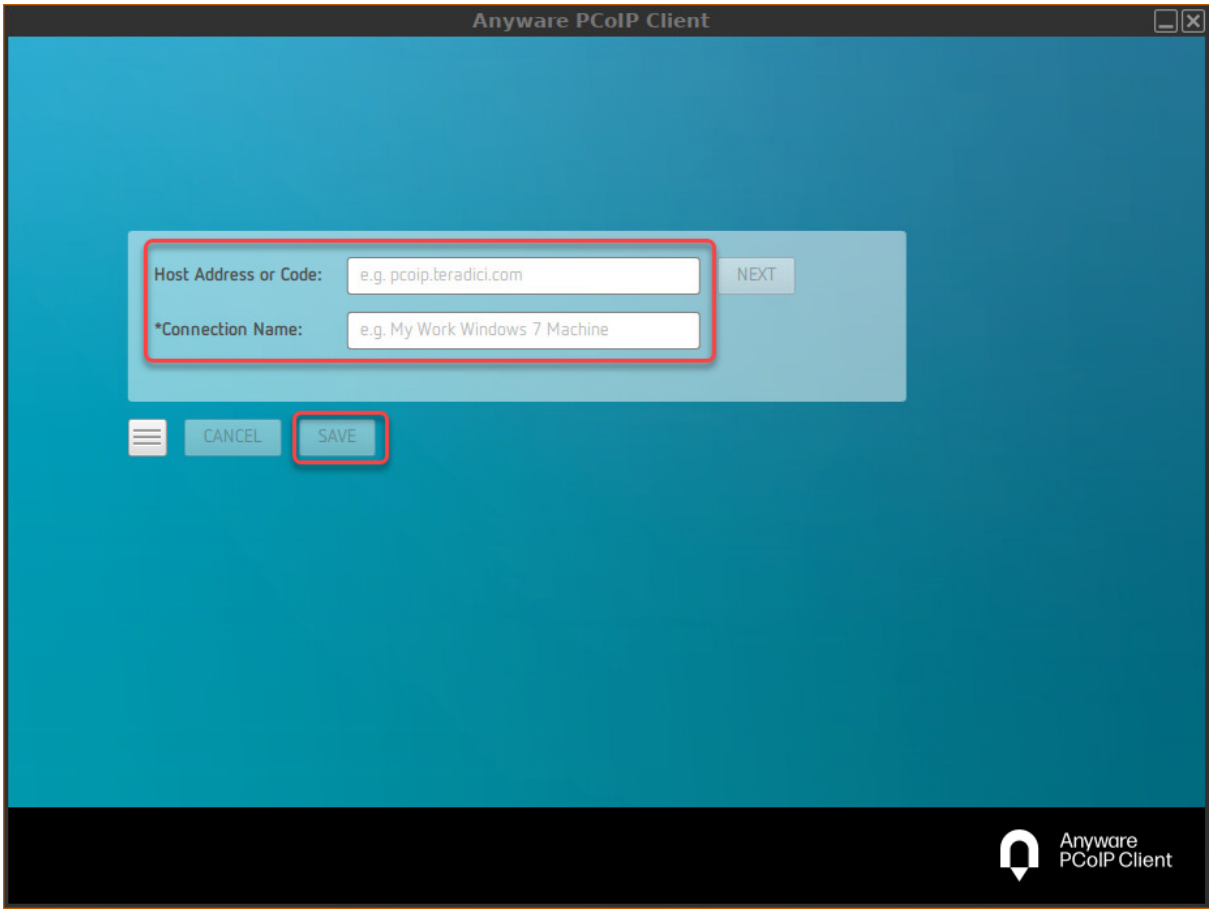
Connecting to Amazon WorkSpaces

1. On your desktop, double-click on the icon of the PCoIP session.



The **Anyware PCoIP Client** dialog opens.

2. Enter the **Host Address or Code** that has been sent to you in the welcome e-mail from Amazon WorkSpaces.
3. Enter the **Connection Name** and click **SAVE**.



4. Enter your Amazon WorkSpaces credentials.
5. Enter the **Multi-Factor Authentication (MFA) Token**.

> Multi-factor authentication is a proof of user identity that combines two different components (factors) that are independent of one another.

> If you do not use multi-factor authentication, you still need to enter something in the MFA field, even when it is just a number or "1234".
> Otherwise, no connection to Amazon WorkSpaces can be established.

6. Click **Ok**.
   The Amazon WorkSpaces desktop is shown.

See also our video description on youtube:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
https://www.youtube.com/watch?v=NDQxTEKLPZE

How to Configure Your HP Anyware Client for Amazon WorkSpaces in IGEL OS

Configuring the Connection in the IGEL Setup

If you want to use the IGEL Setup for the configuration, proceed as follows:

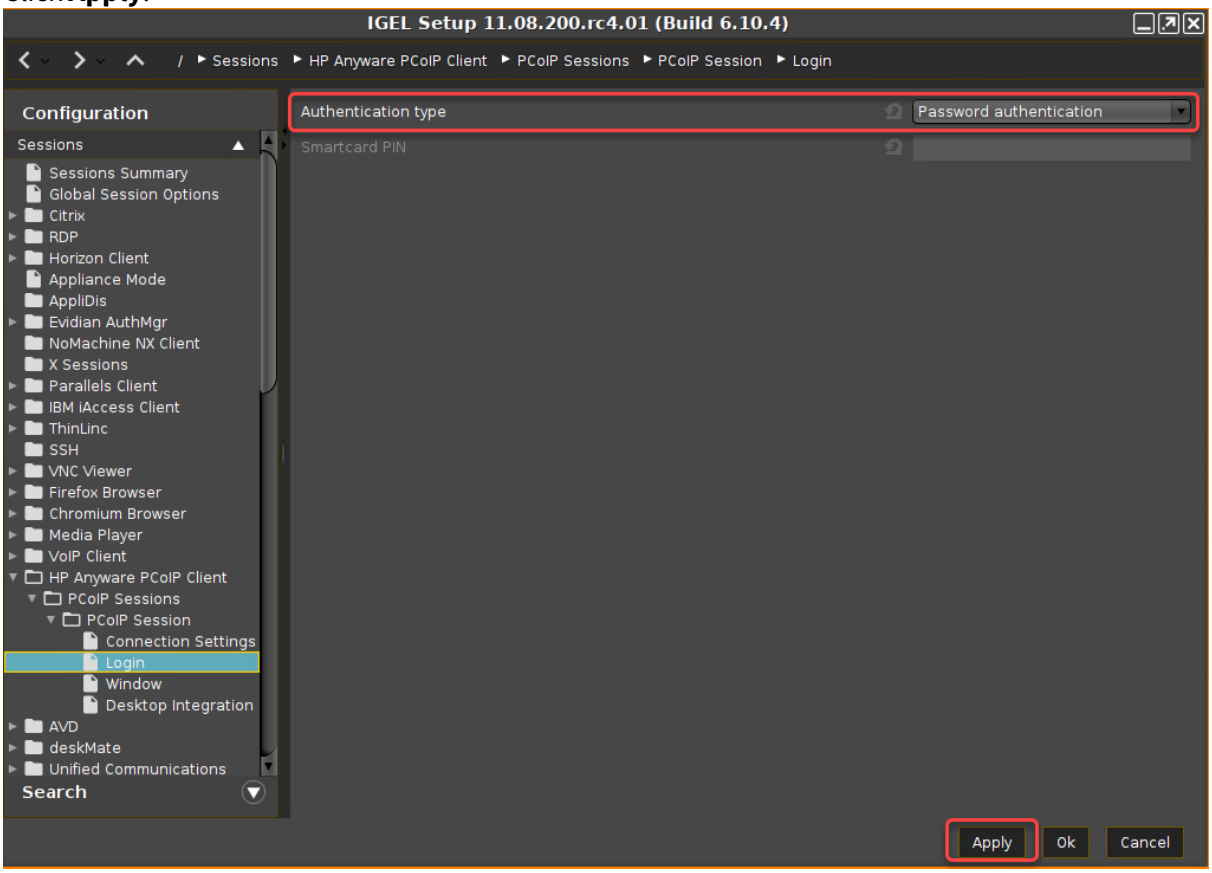
1. Enable **Use IGEL Setup for Configuration**.
2. Select the **Broker type** you want to connect to Amazon WorkSpace.
    a. Broker type: **Direct hardhost**
        - Enter the Registration Code for Amazon Workspaces as **Server**.
        - Set **Server certificate verification mode** to "Warn but allow".

    b. Broker type: **PCoIP broker**
        - Enter the server from the PCoIP broker as **Server**.
        - Set **Server certificate verification mode** to "Warn but allow".

> For more information about the broker types, see Broker Types for Connecting to Amazon WorkSpaces with the HP Anyware Client on IGEL OS (see page 546).

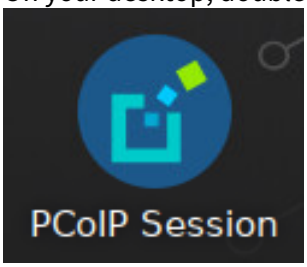
3. Click **Apply**.
4. Go to **Login** and set **Authentication type** to "Password authentication".

5. Click **Apply**.



Connecting to Amazon WorkSpaces

1. On your desktop, double-click on the icon for your PCoIP session.



2. The HP Anyware PCoIP Client mask takes over the information you entered in the IGEL Setup.
3. Click **SAVE**.
4. Now enter your Amazon WorkSpace credentials.
   For the rest of the procedure, see aws.amazon.com[73].

73. https://aws.amazon.com/de/?nc2=h_lg

Broker Types for Connecting to Amazon WorkSpaces with the HP Anyware Client on IGEL OS

You can choose between two broker types for connecting to Amazon WorkSpaces with the HP Anyware Client on IGEL OS.

PCoIP Broker

PCoIP broker is a resource manager that dynamically assigns host PCs to zero clients based on the identity of the user established from the zero client. Connection brokers are also used to allocate a pool of hosts to a group of zero clients in a PCoIP deployment. If the zero clients are configured to always connect to the same host (i.e., a static one-to-one pairing), then a connection broker is not required.

Direct Hardhost

A direct hardhost is a direct connection between a zero client and a remote workstation containing a PCoIP Remote Workstation Card. You can specify a host's DNS name or IP address, or you can configure clients to use the Service Location Protocol (SLP) to discover a host. You can also configure clients to automatically reconnect to a host when a session is lost.

How Can I Use H.264 Acceleration in an HP Anyware PCoIP Session?

Question

How must I configure the client and the server to get H.264 acceleration in an HP Anyware PCoIP Session?

Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher

  > With IGEL OS 11.08.200, the client was renamed from "Teradici PCoIP" to "HP Anyware PCoIP".

- UMS 6.04 or higher
- HP Anyware PCoIP Graphics Agent for Windows 20.04

Answer

Server-side

1. Open the Group Policy Editor (`gpedit.msc`).
2. Go to **Local Computer Policy > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults**.
3. Edit the settings as follows:
   - Set **Configure PCoIP image quality levels** to "Enabled".
   - Set **Configure PCoIP image quality levels > YUV chroma subsampling** to "4:2:0".
   - Set **Enable PCoIP Ultra GPU optimization** to "Enabled".

Client-side

1. Open the Setup or the UMS configuration dialog.
2. Go to **System > Registry > pcoip > codec_h264** and activate **H.264 codec** (registry parameter: `pcoip.codec_h264`).
3. Save your settings.

Login Enterprise Configuration

With Login Enterprise Launcher (former Login PI), you can test changes that affect the performance of desktop and application logins, as well as the current processing of both applications and specific tasks inside of a given application before you implement them on real devices.

- How to Login Enterprise Launcher in IGEL OS (see page 549)
- How to Get the Secret for Login Enterprise Launcher (see page 554)
- How to Use the Login Enterprise Launcher within a VMware Horizon Session (see page 557)

How to Login Enterprise Launcher in IGEL OS

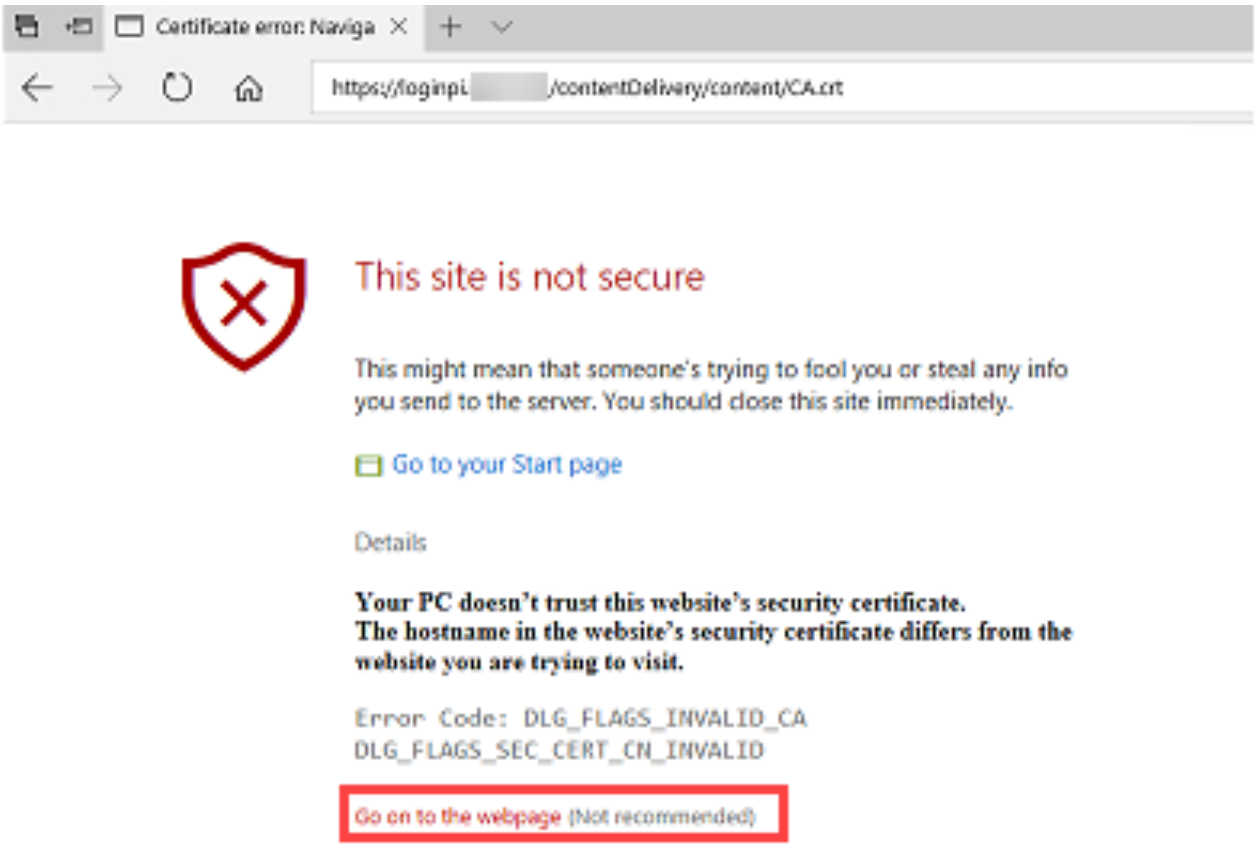
Requirements

- IGEL OS 11.03.100 or higher

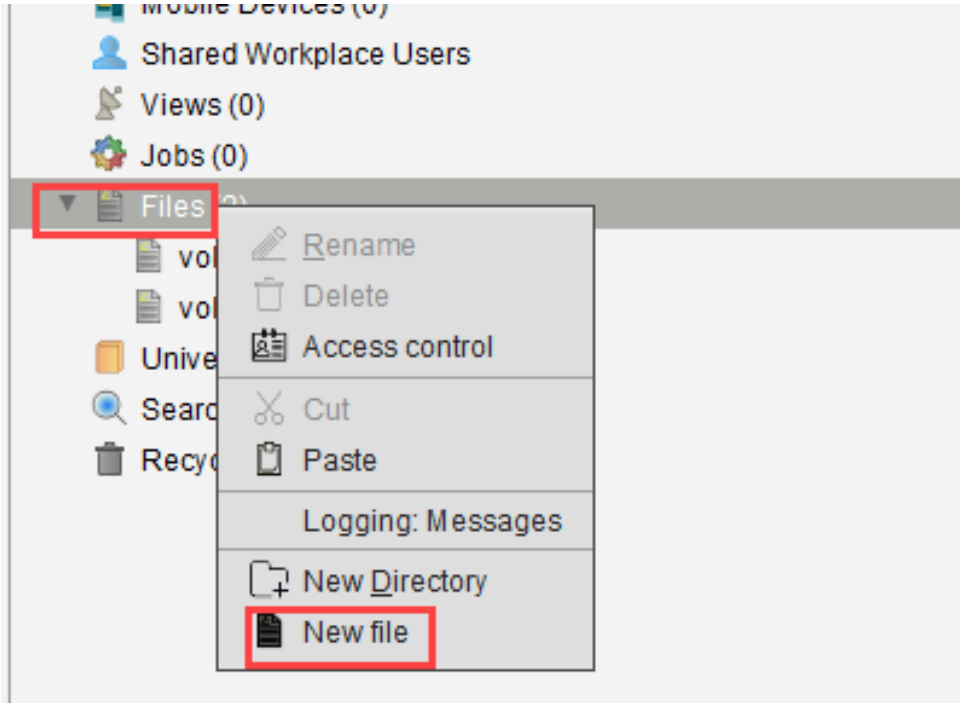
Uploading the SSL Certificate

In order to use Login Enterprise Launcher (former Login PI), you need first to download the SSL certificate from your Login Enterprise server: `https://yourServerURL/contentDelivery/content/CA.crt`. Click **Go on to the webpage**. Download the certificate.

> You have to rename the file name from `CA.crt` to `LoginPI.crt`.

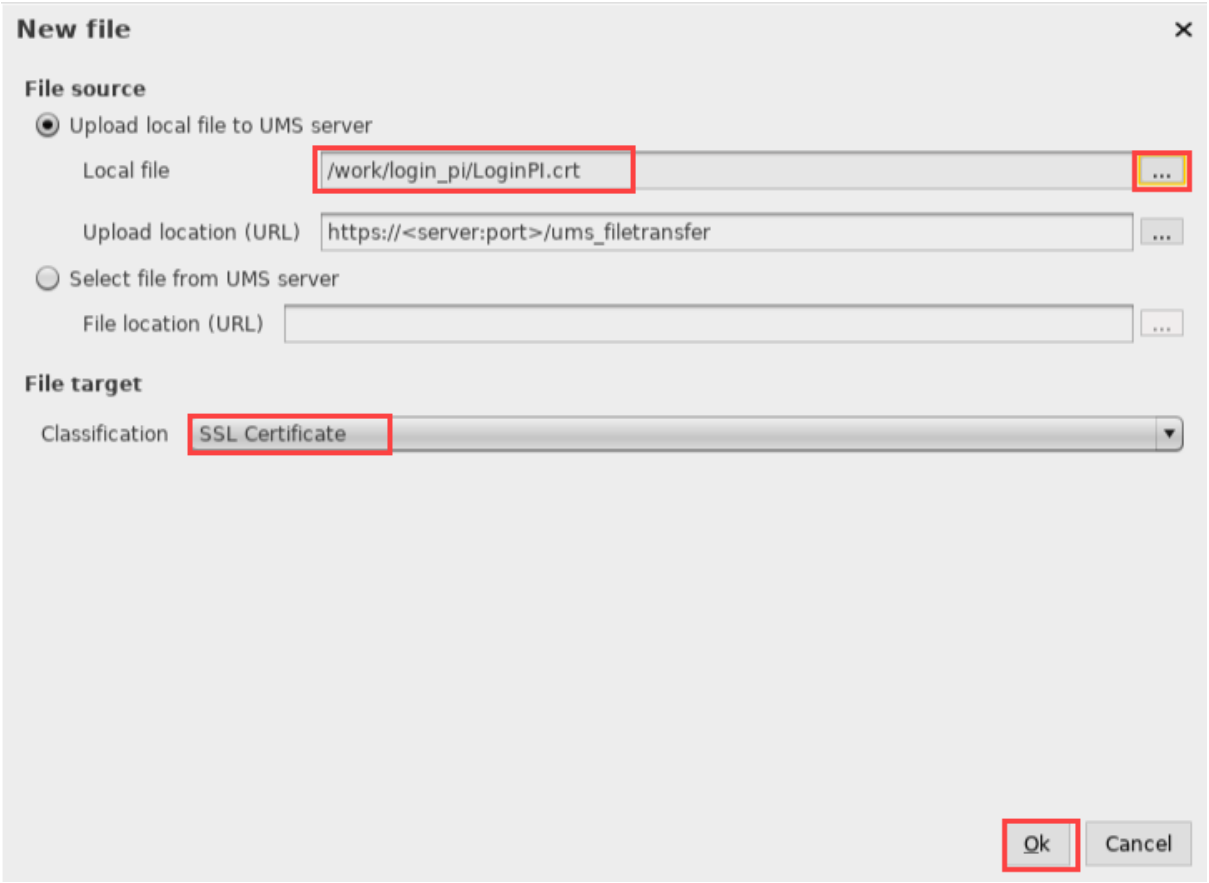


1. Open the **UMS Console**.
2. Select **New File** in the **Files** context menu.



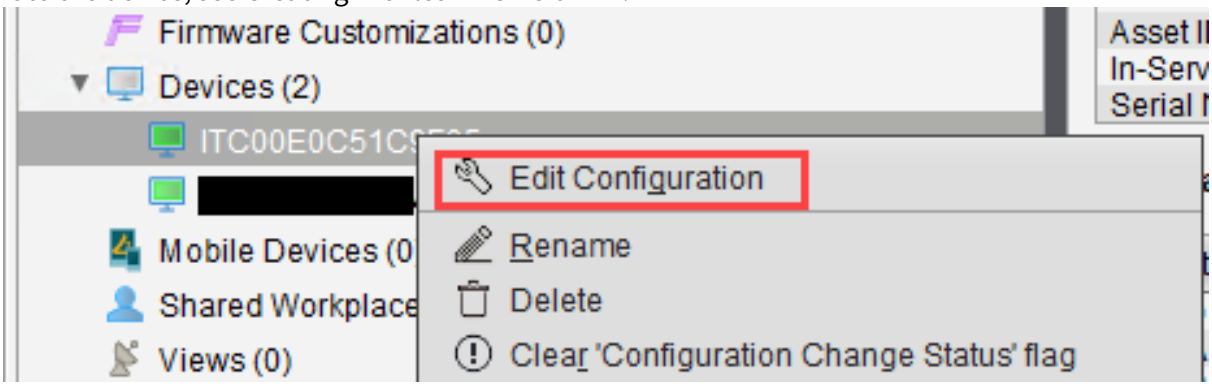
   The window **New file** opens.
3. Select the **Local file** under **Upload local file to UMS server**.

4. Choose **SSL Certificate** under **Classification** and click **Ok**.



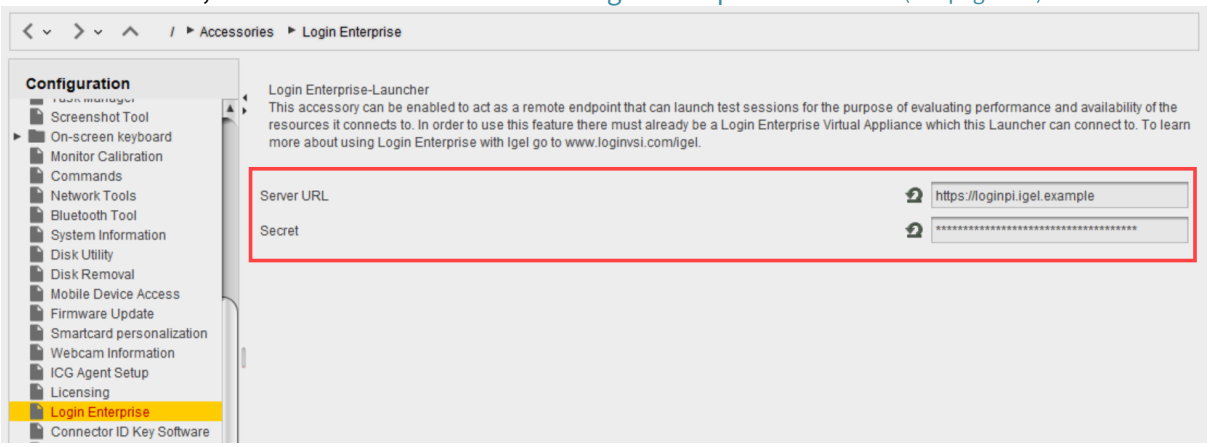
Configuration of Login Enterprise Launcher

1. Under **Devices** in the UMS structure tree, choose the device and click **Edit Configuration** in its context menu. Or you can create a new profile with the required settings under **Profiles** and assign it to the device, see Creating Profiles im UMS 6 PDF.



2. Go to **Accessories > Login Enterprise**.
3. Enter the **Server URL** of your Login Enterprise server.

4. Enter the **Secret**, see How to Get the Secret for Login Enterprise Launcher (see page 554).



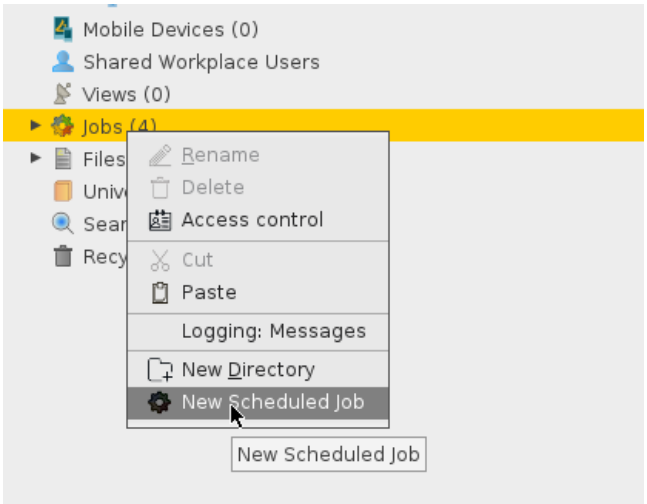
5. Save the settings.

> If you want to use the Login Enterprise Launcher within a VMware session, see How to Use the Login Enterprise Launcher within a VMware Horizon Session (see page 557).

Starting the Login Enterprise Launcher from the UMS

After the Login Enterprise server has been set up, you can create a job in the UMS for the automatic start of your Login Enterprise Launcher at a defined time.

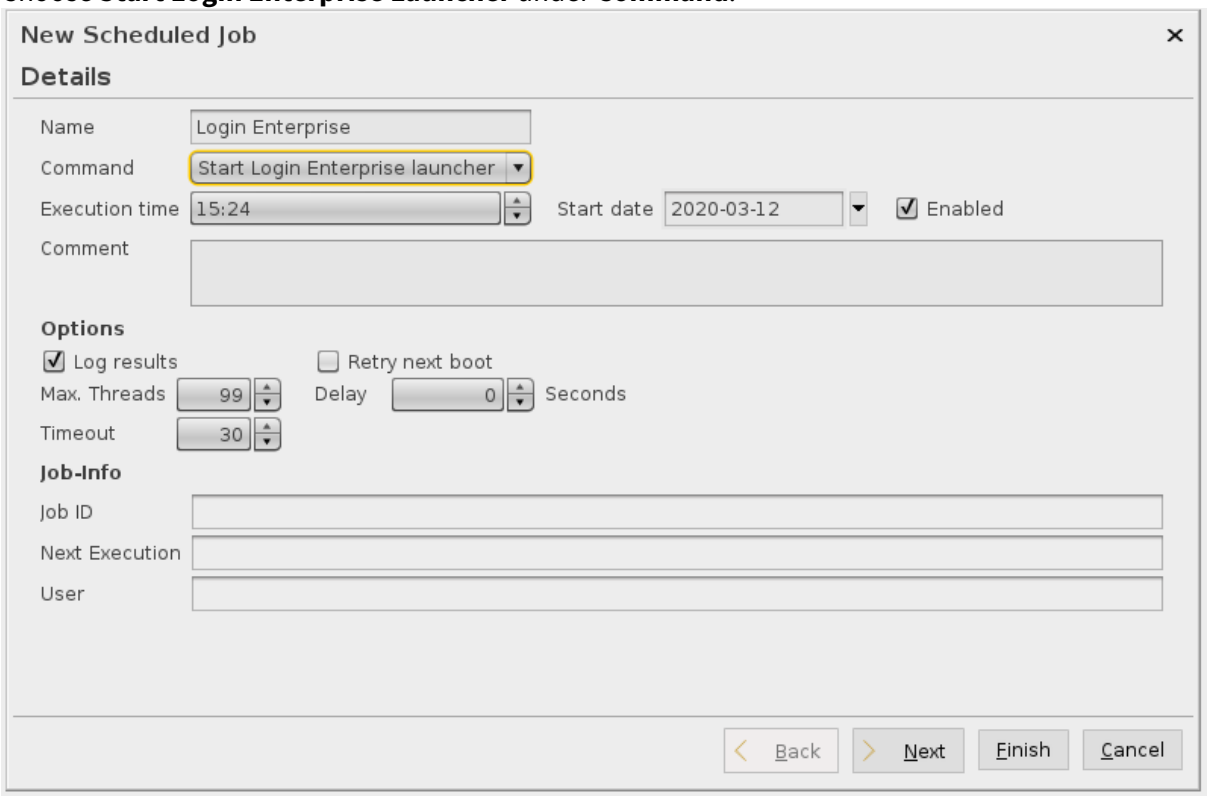
1. Select **Jobs** in the UMS structure tree and choose **New Scheduled Job** in the context menu.



The **New Scheduled Job** window opens.

2. Under **Name**, enter the name for the job, e.g. "Login Enterprise".

3. Choose **Start Login Enterprise Launcher** under **Command**.



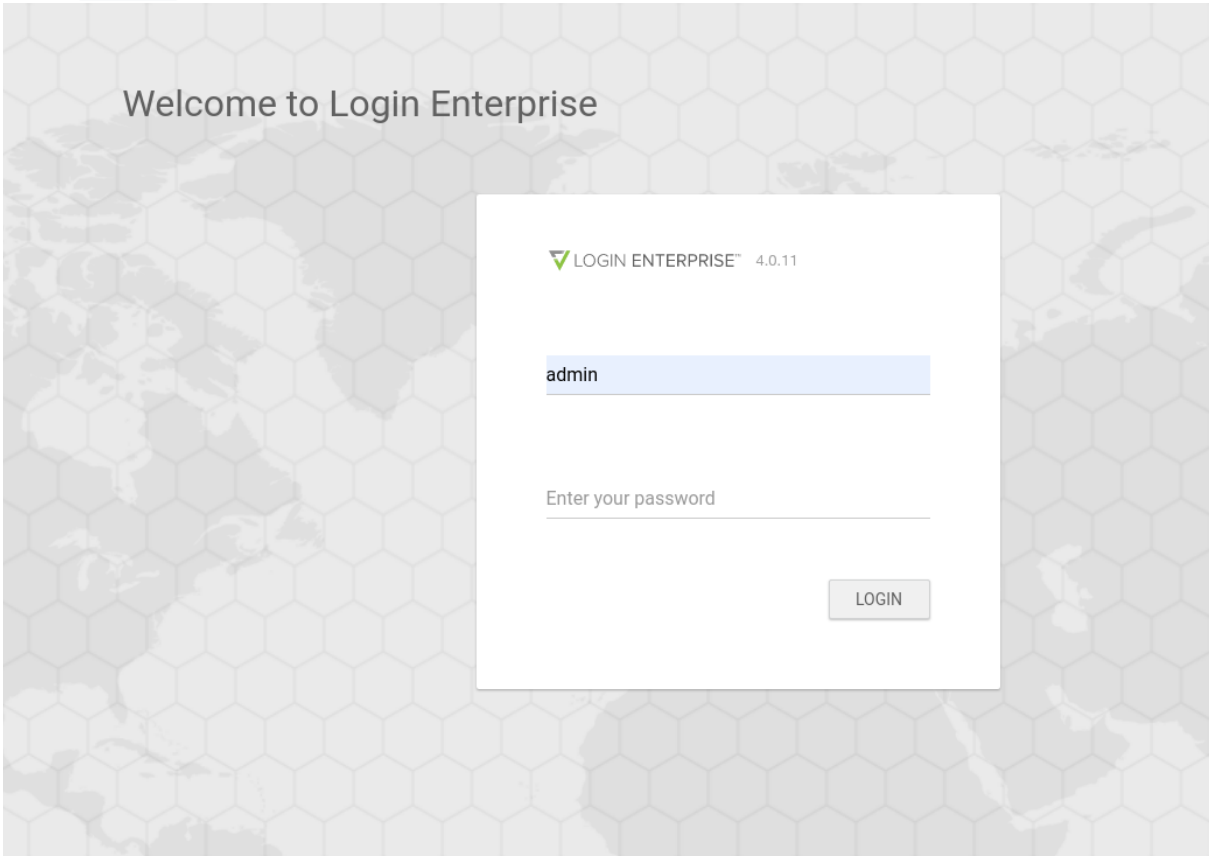
4. Select the **Execution time** and **Start date**.
5. Click **Next** and assign the devices.
6. Click **Finish** to save the job.

To learn more about using Login Enterprise with IGEL, see https://www.loginvsi.com/igel/.

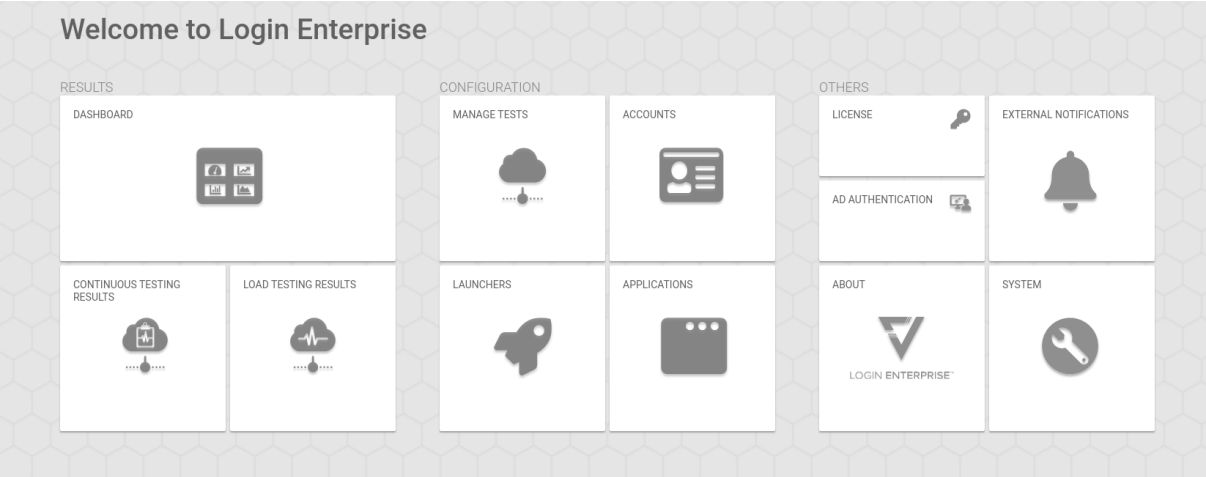
How to Get the Secret for Login Enterprise Launcher

This how-to explains how to get a **Secret** to configure Login Enterprise Launcher (see page 549).

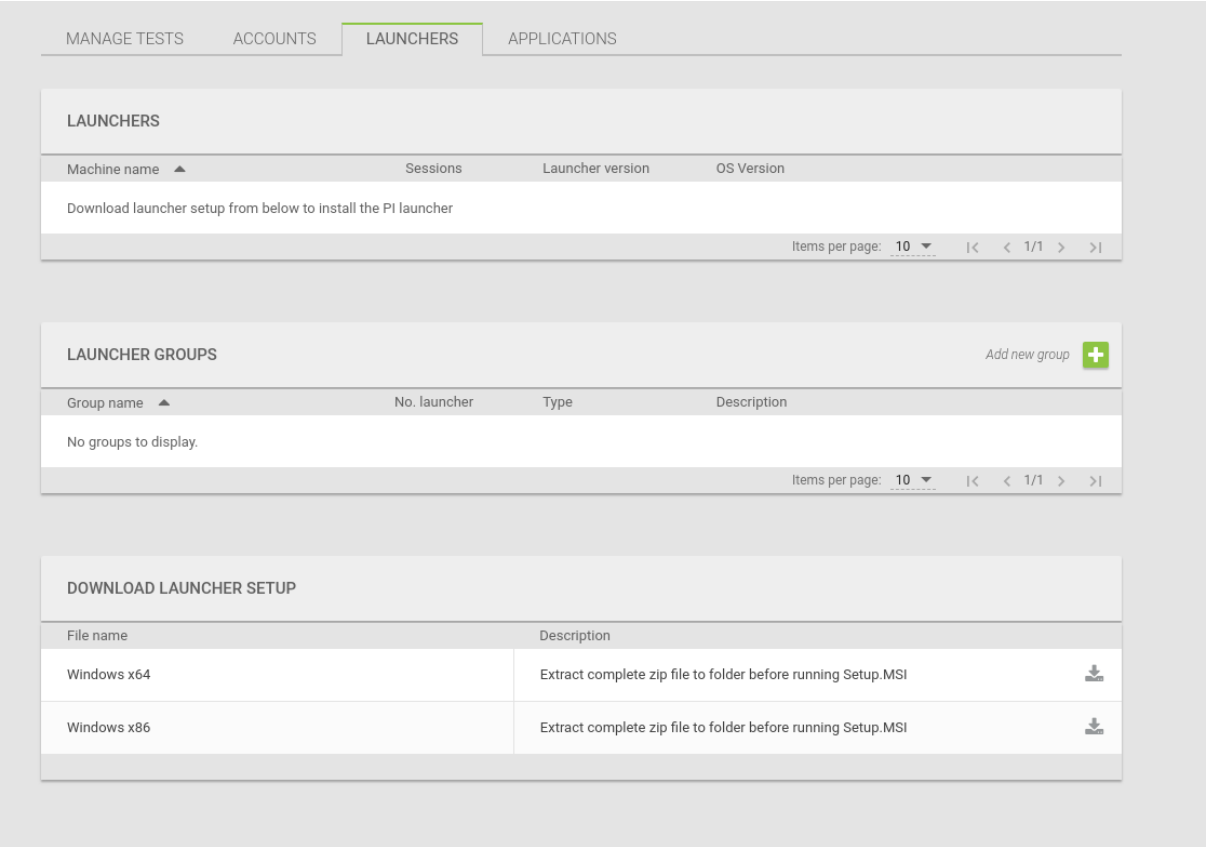
1. Go to `https://yourServerURL`.
   Enter `admin` as a username and password and click **LOGIN**.



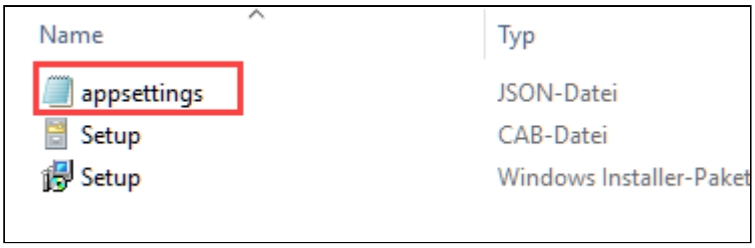
2. Go to **Launchers**.



3. Download a required `.zip` file under **Download Launcher Setup** and unpack it.



4. Open the `appsettings.json` file in the editor.



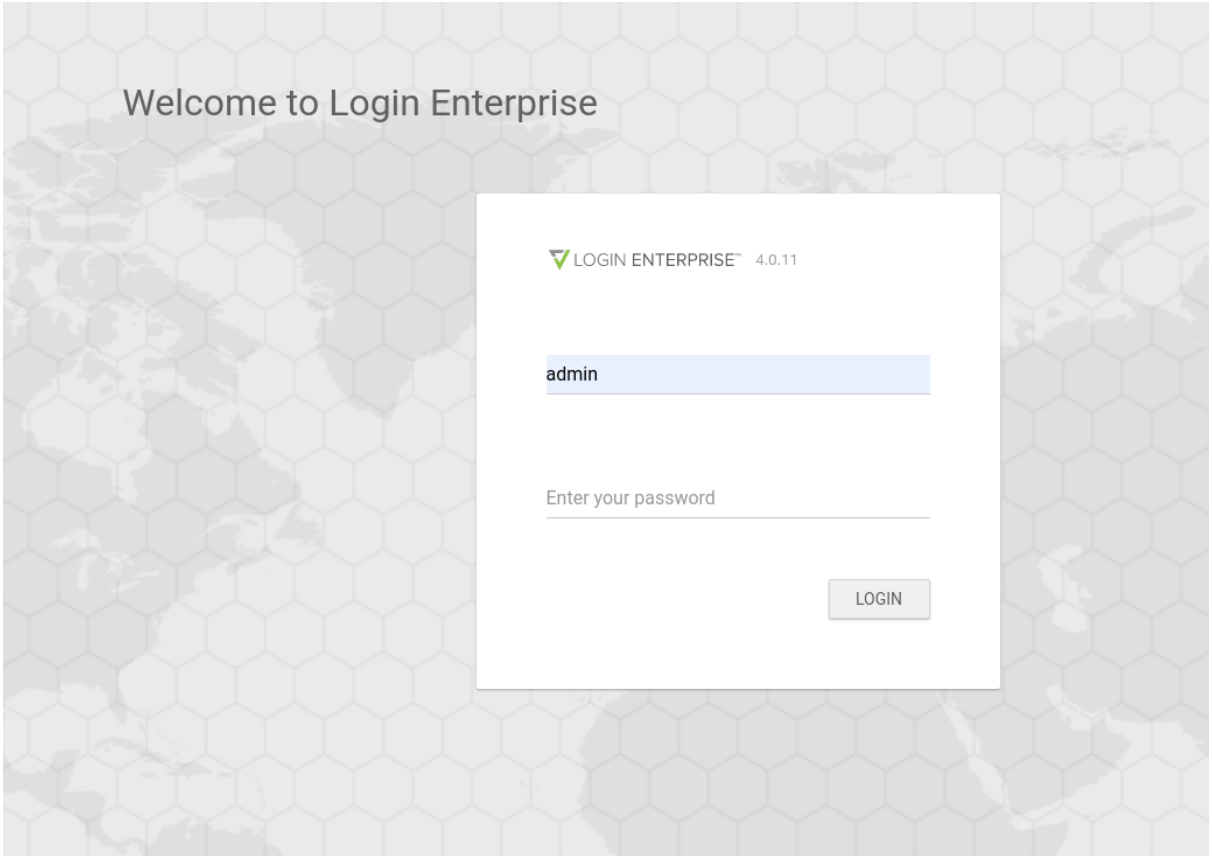
Here you find the **Secret** for your Login Enterprise Launcher.

Use the **Secret** without the quotation marks "".

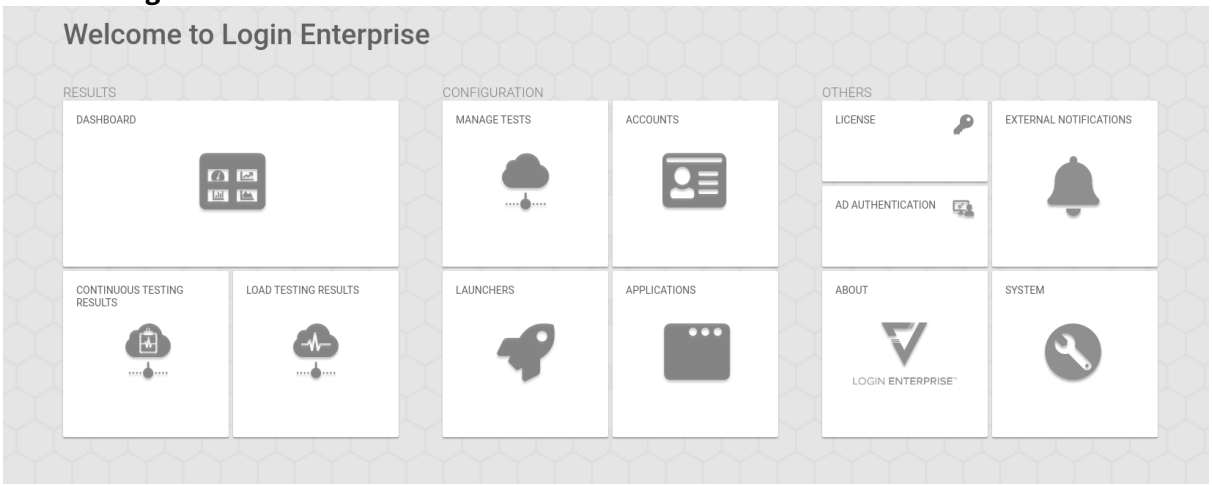
How to Use the Login Enterprise Launcher within a VMware Horizon Session

If you want to use the Login Enterprise Launcher within a VMware Horizon Session on your IGEL OS device, note the following:

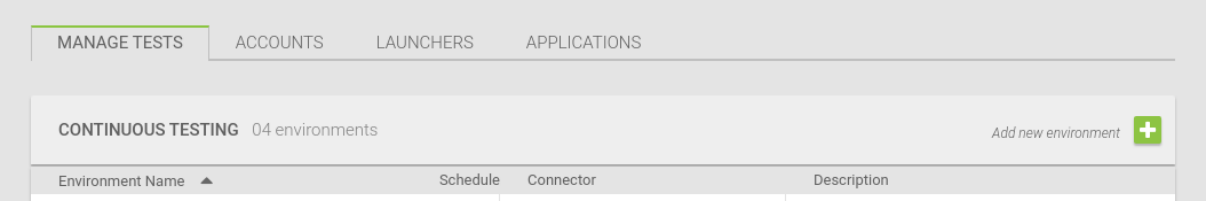
1. Go to `https://yourServerURL` and log in.



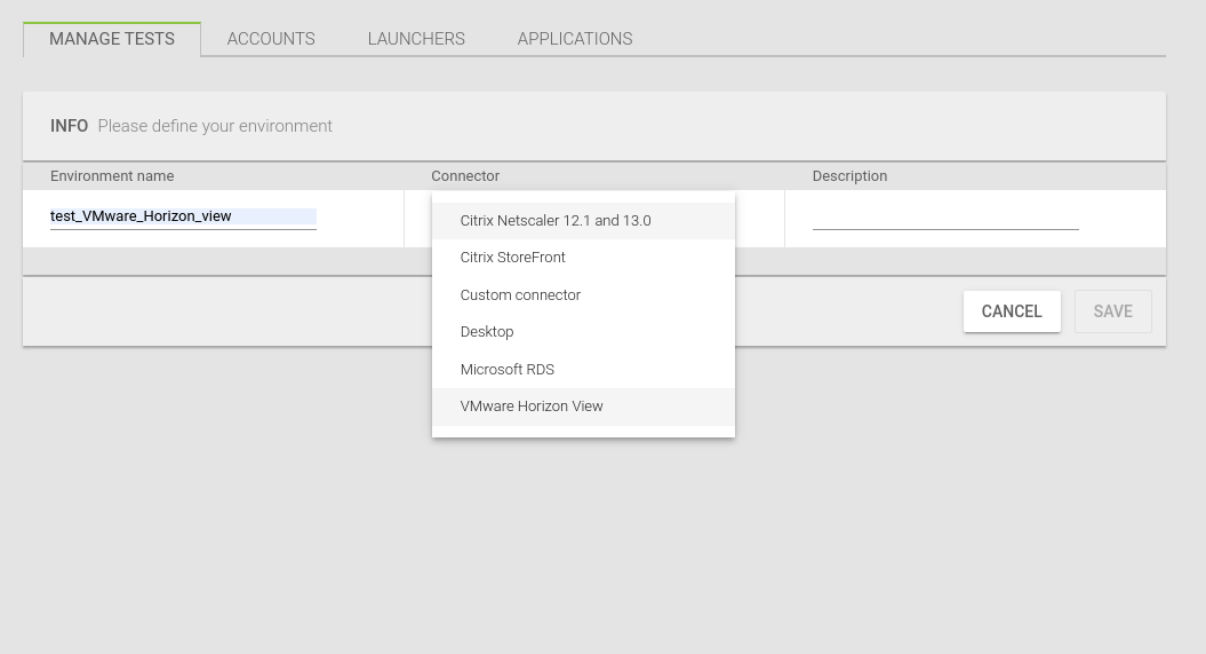
2. Go to **Manage Tests**.



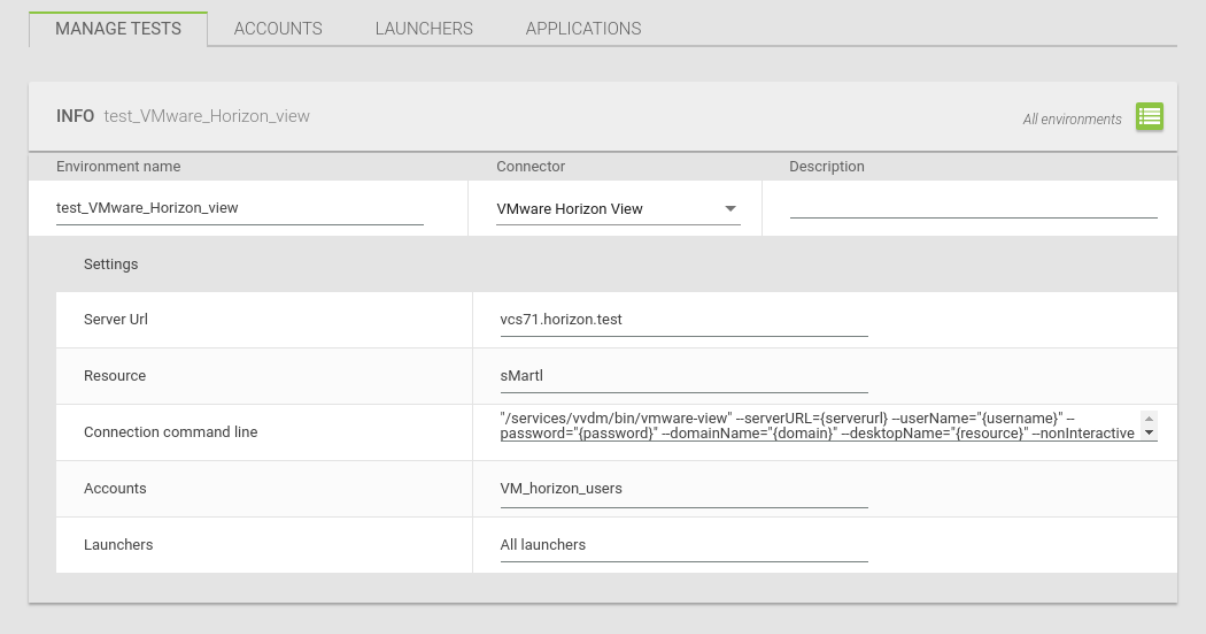
3. Click **Add new environment**.



4. Enter an **Environment name**.
5. Select **VMware Horizon View** under **Connector**.

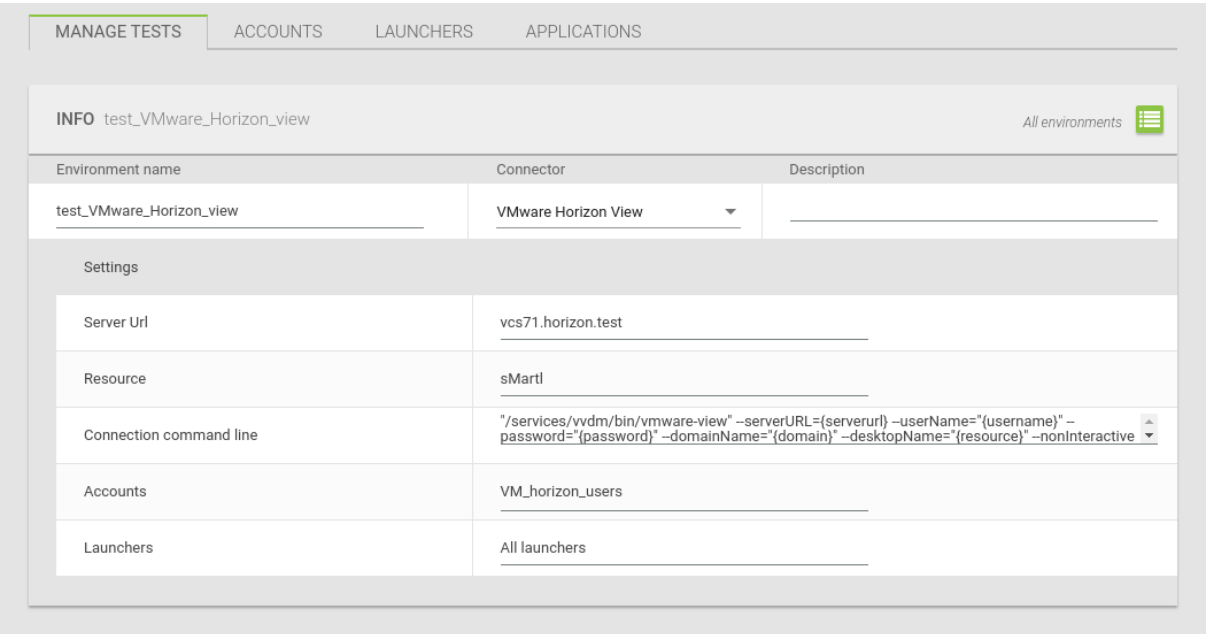


6. Enter the **Server URL** and the **Resource**.



7. Copy the following:

   "/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" --password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive and paste it under **Connection command line**.



This is important if you use the Login Enterprise Launcher for IGEL OS devices!

For more information on the configuration, see http://www.loginvsi.com.

Nutanix

Nutanix enables IT teams to build and operate high-performance multi-cloud architectures. The enterprise cloud OS software combines private, public, and distributed cloud operating environments and provides centralized control to manage IT infrastructures and applications of all sizes.

Nutanix solutions are 100 % software-based and leverage the industry's most popular hyper-converged infrastructure (HCI) technology.

> ### Hyper-converged infrastructure (HCI)
>
> Hyper-convergent infrastructures are a further development of convergent infrastructures in which hardware and software are also bundled.

They provide a complete infrastructure stack that combines computing, virtualization, storage, networking, and security to run any application of any size.

The Software runs across multiple cloud environments to harmonize IT operations and proved smooth mobility for all applications. For more information, see nutanix.com[74].

Frame on Nutanix

Frame is the easiest way to run virtual apps and desktops on your choice of infrastructure.

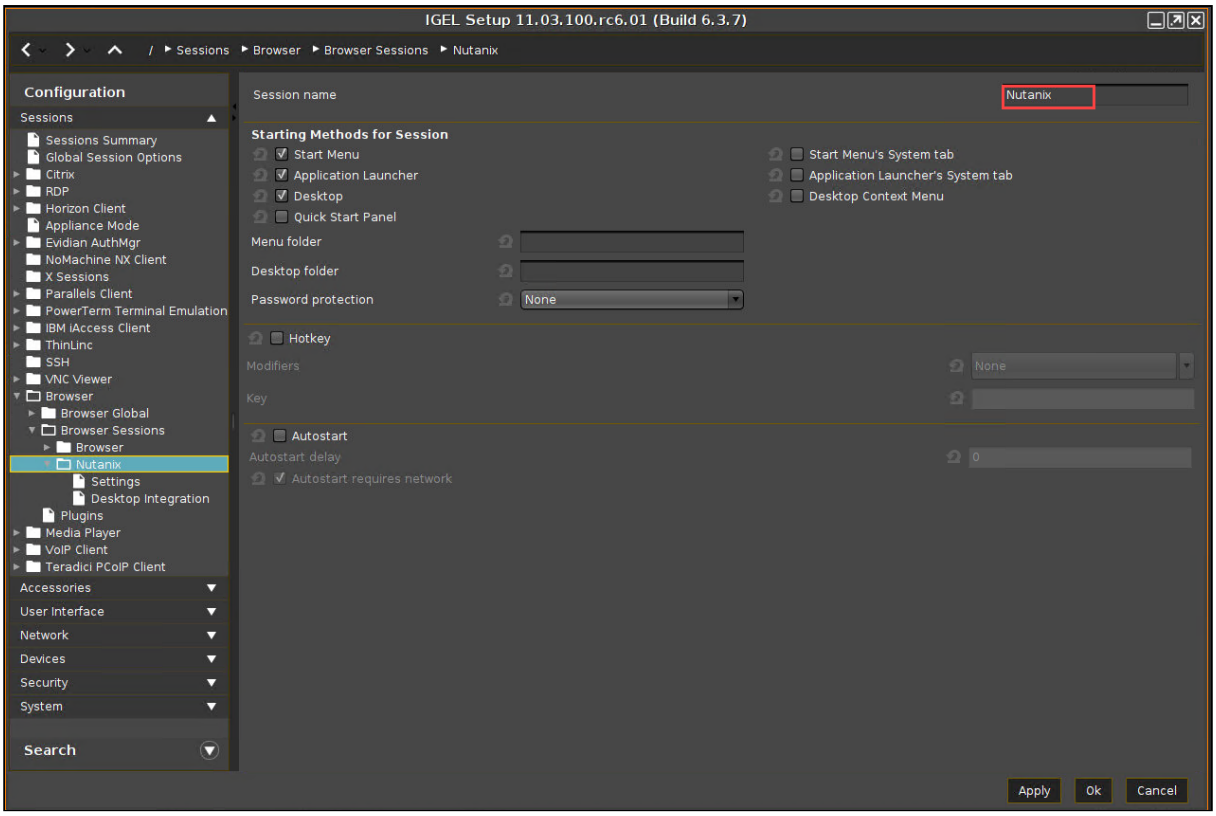
It's a new option to use Frame Desktop-as-a-Service (DaaS) with apps, desktops, and user data hosted on your Nutanix (AHV) infrastructure.

You have to create a browser profile and put in the address of your frame broker.

Setting Up Frame Connection

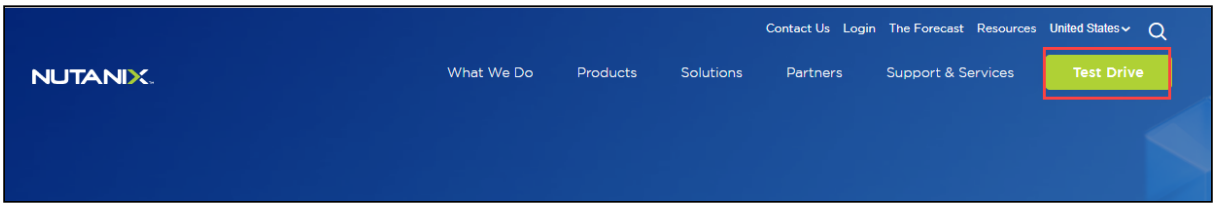
1. In the IGEL Setup, go to **Sessions > Firefox Browser > Firefox Browser Sessions**.
2. Click + to add a browser session.
   For more information about the setup, see Firefox Browser Session (see page 1589).

74. https://www.nutanix.com/en



Running the Nutanix Test Drive on IGEL

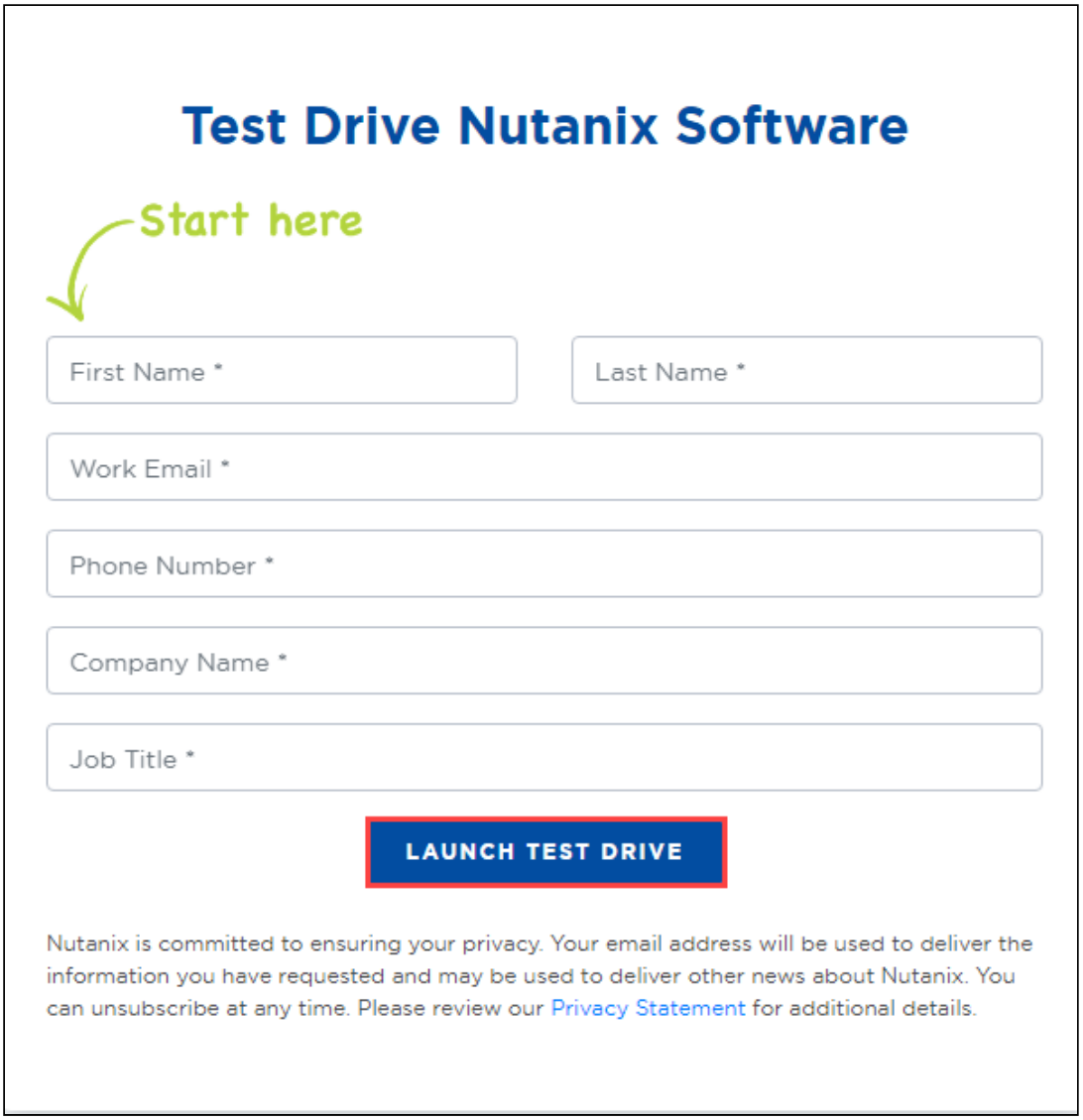
1. Open the Firefox browser.
2. Enter https://www.nutanix.com[75].
3. Click **Test Drive.**



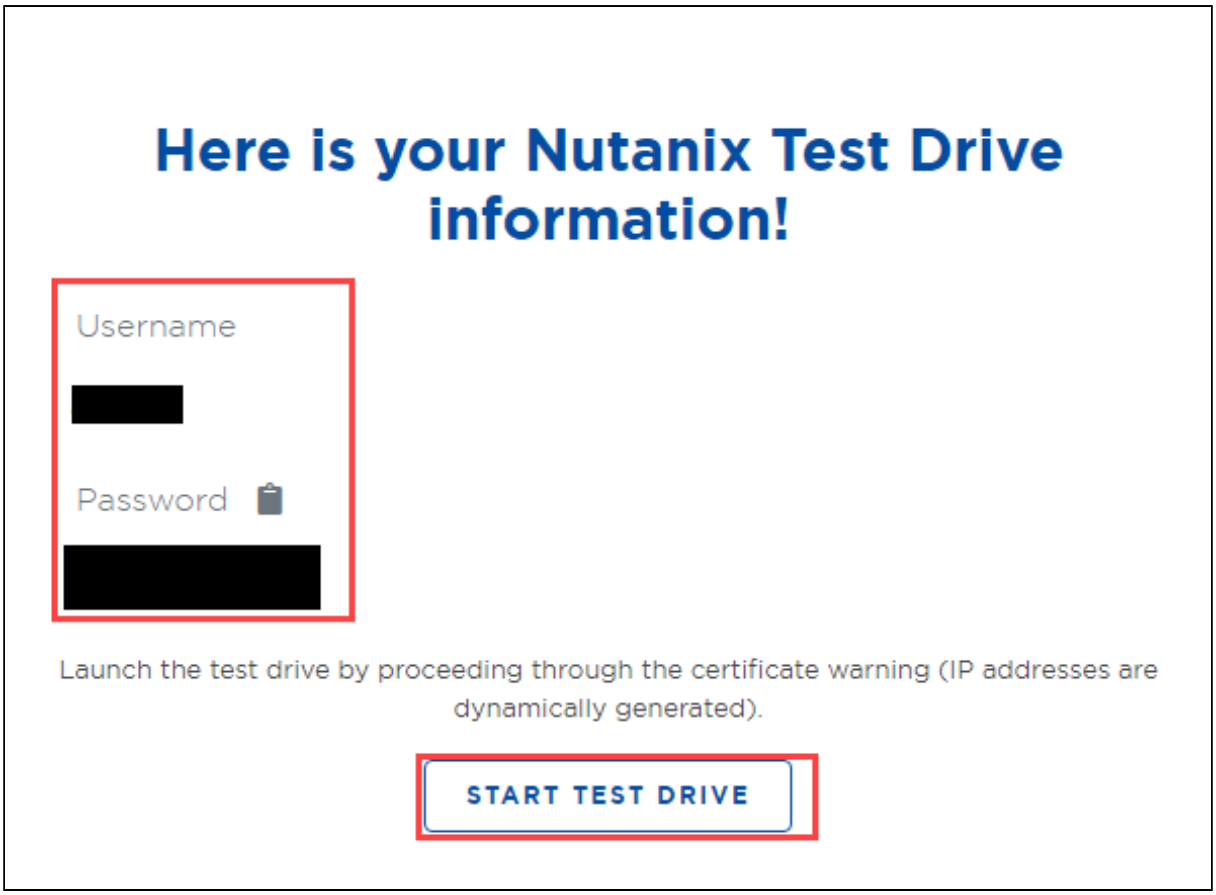
4. Enter the required data.

75. https://www.nutanix.com/en

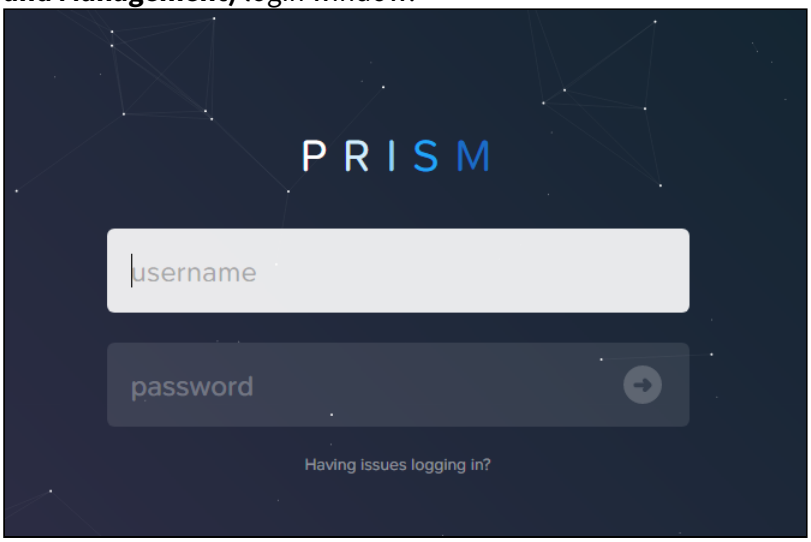
5. Click **Launch Test Drive.**



6. Your **Nutanix Test Drive information** is shown.
7. Click **Start Test Drive.**



8. Enter your credentials in the **PRISM (Planning tool for Resource Integration, Synchronization and Management)** login window.



For the next steps, follow the instructions of Nutanix.

Browser

- How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices? (see page 566)
- How to Define Multiple Start Pages for Your Browser (see page 569)
- Touchscreen: Multitouch/Gesture Support for Firefox (see page 570)
- How to Set Advanced User Preferences for the Browser (see page 571)
- How to Use the Firefox Browser in Kiosk Mode (see page 573)
- Troubleshooting: SSL/TLS Error with Firefox in Appliance Mode (see page 581)
- Troubleshooting: Browser Cannot Download Files (see page 582)
- Troubleshooting: Some PDFs are not opened by Firefox (see page 583)
- Can I Install Firefox Extensions? (see page 585)
- Troubleshooting: Cannot Download Outlook E-mail Attachments (see page 586)
- Troubleshooting: Cannot Log in to MS Teams in Chromium Browser (see page 587)

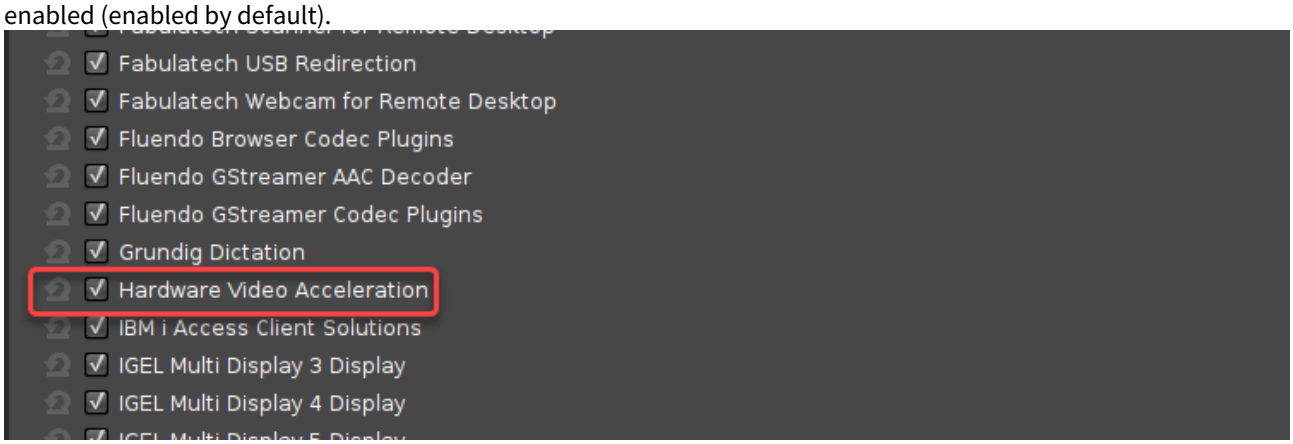
How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices?

IGEL OS allows you to play videos from YouTube or other Internet resources with hardware acceleration, provided the videos are encoded with H.264. Due to license restrictions, either Chromium or Firefox can use H.264 hardware acceleration, but not both of them.

This article provides detailed information on how to configure H.264 hardware acceleration for Chromium or Firefox.

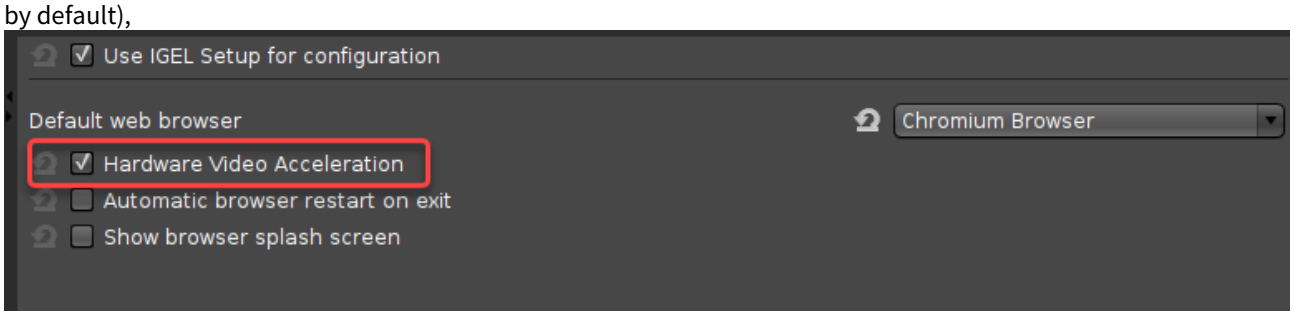
Checking Whether Hardware Video Acceleration Is Enabled Globally

->Make sure that **System > Firmware Customization > Features >** parameter **Hardware Video Acceleration** is enabled (enabled by default).



Checking Whether Hardware Video Acceleration Is Enabled for Chromium

->If you want to use hardware video acceleration with the Chromium browser, make sure that **Sessions > Chromium Browser > Chromium Browser Global >** parameter **Hardware Video Acceleration** is enabled (enabled by default),



Does the Default Browser Setting Matter?

If Chromium and Firefox both have the number of sessions configured, the default browser matters. Example: If Firefox and Chromium both have three sessions, and Firefox is set as the default browser, Firefox will get H.264 hardware acceleration.

Exception: If browser content redirection is activated, Chromium will always get H.264 hardware acceleration; see **Browser Content Redirection for Citrix Sessions**.

The Browser with the Higher Number of Configured Sessions Gets Hardware Video Acceleration

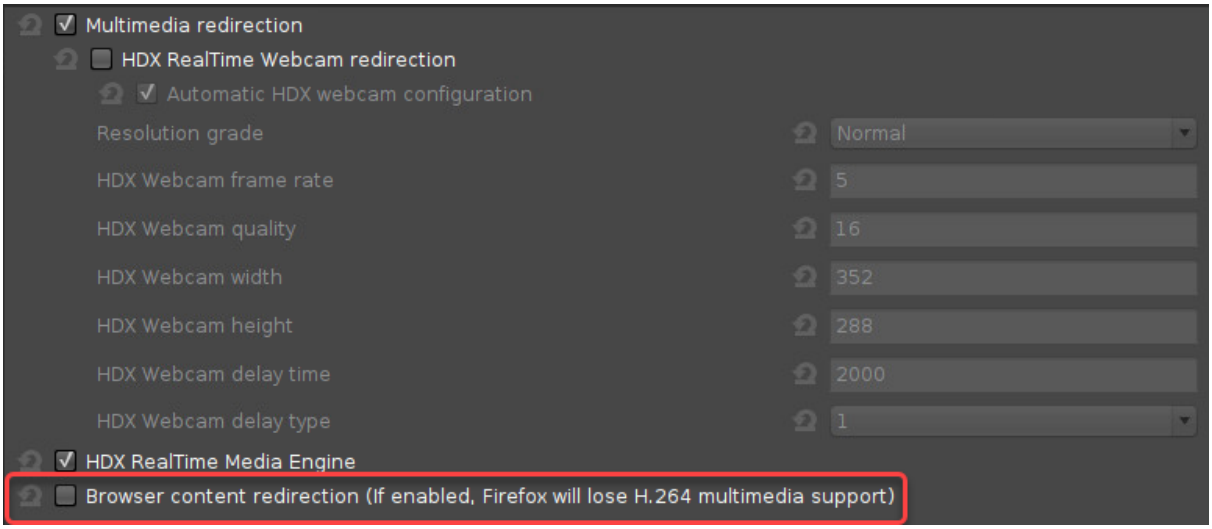
The browser that has more sessions configured is the one that gets H.264 hardware acceleration. Example: If two sessions are configured for Chromium and three sessions are configured for Firefox, Firefox will get H.264 hardware video acceleration.

Exception: If browser content redirection is activated, Chromium will always get H.264 hardware acceleration; see **Browser Content Redirection for Citrix Sessions**.

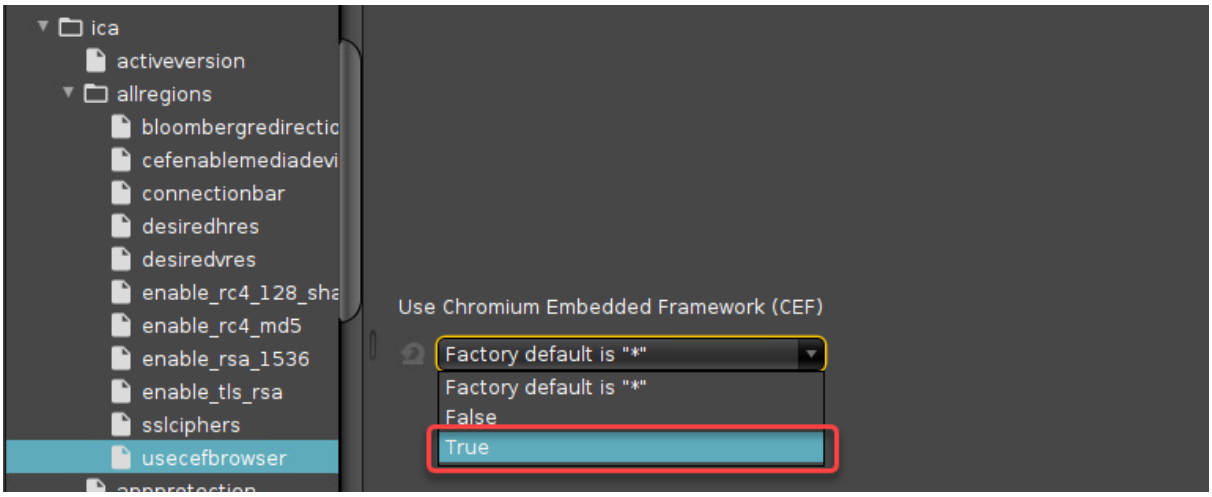
Browser Content Redirection for Citrix Sessions Forces Hardware Video Acceleration for Chromium

The Chromium browser always gets H.264 hardware acceleration, regardless of the number of configured sessions, if all of these conditions are met:

- **Sessions > Citrix > Citrix Global > HDX Multimedia** > parameter **Browser content redirection** is activated.



- **System > Registry > ica > allregions > usecefbrowser > Use Chromium Embedded Framework (CEF)** is set to "True".



Setting Chromium to Select the H.264 Video Stream

Generally, the default setting, which allows the Chromium browser to choose the video stream automatically, is recommended. Alternatively, you can set the Chromium browser to prefer the H.264 video stream even if hardware video acceleration is not enabled, or not prefer the H.264 video stream, disregarding the availability of hardware video acceleration.

->Go to **System > Registry > force_264** and set **Force H.264** according to your needs:

- "Auto": The Chromium browser prefers the H.264 video stream if hardware video acceleration is enabled.
- "Enabled": The Chromium browser always prefers the H.264 video stream, regardless of whether hardware video acceleration is enabled or not.
- "Disabled": The Chromium browser never prefers the H.264 video stream.

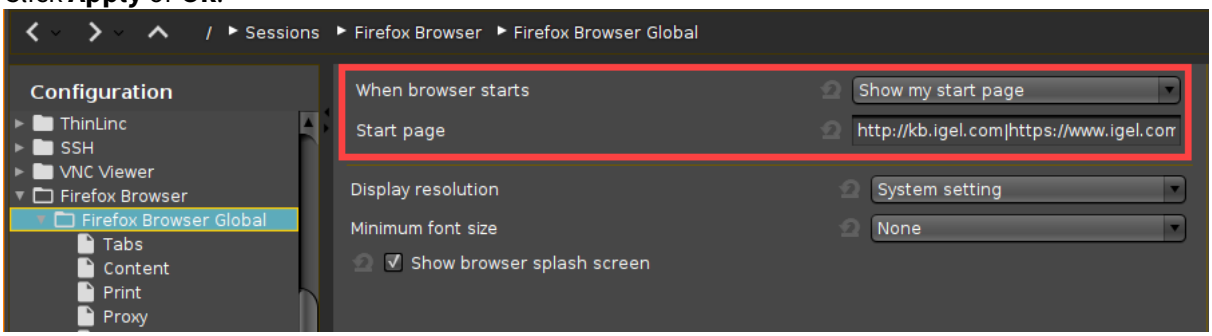
How to Define Multiple Start Pages for Your Browser

In some cases, a fixed set of start pages displayed in separate tabs may prove useful. For instance, if the browser is working in kiosk mode, reusing a set of tabs from an earlier session is not an option.

Here is how to define multiple start pages to be opened at browser startup.

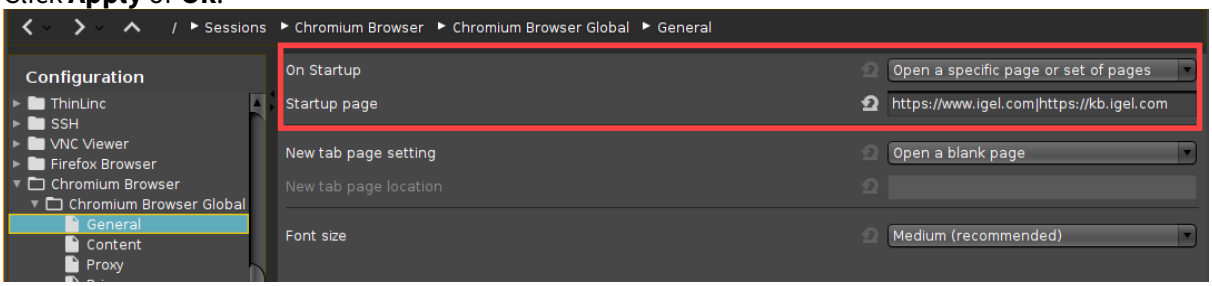
Firefox

1. Open the IGEL Setup and go to **Sessions > Firefox Browser > Firefox Browser Global**.
2. Set **When browser starts** to **Show my start page**.
3. Set **Start page** to the URLs that the browser should open at startup. Use "|" as a separator.
4. Click **Apply** or **Ok**.



Chromium

1. Open the IGEL Setup and go to **Sessions > Chromium Browser > Chromium Browser Global > General**.
2. Set **On Startup** to **Open a specific page or set of pages**.
3. Set **Startup page** to the URLs that the browser should open at startup. Use "|" as a separator.
4. Click **Apply** or **Ok**.

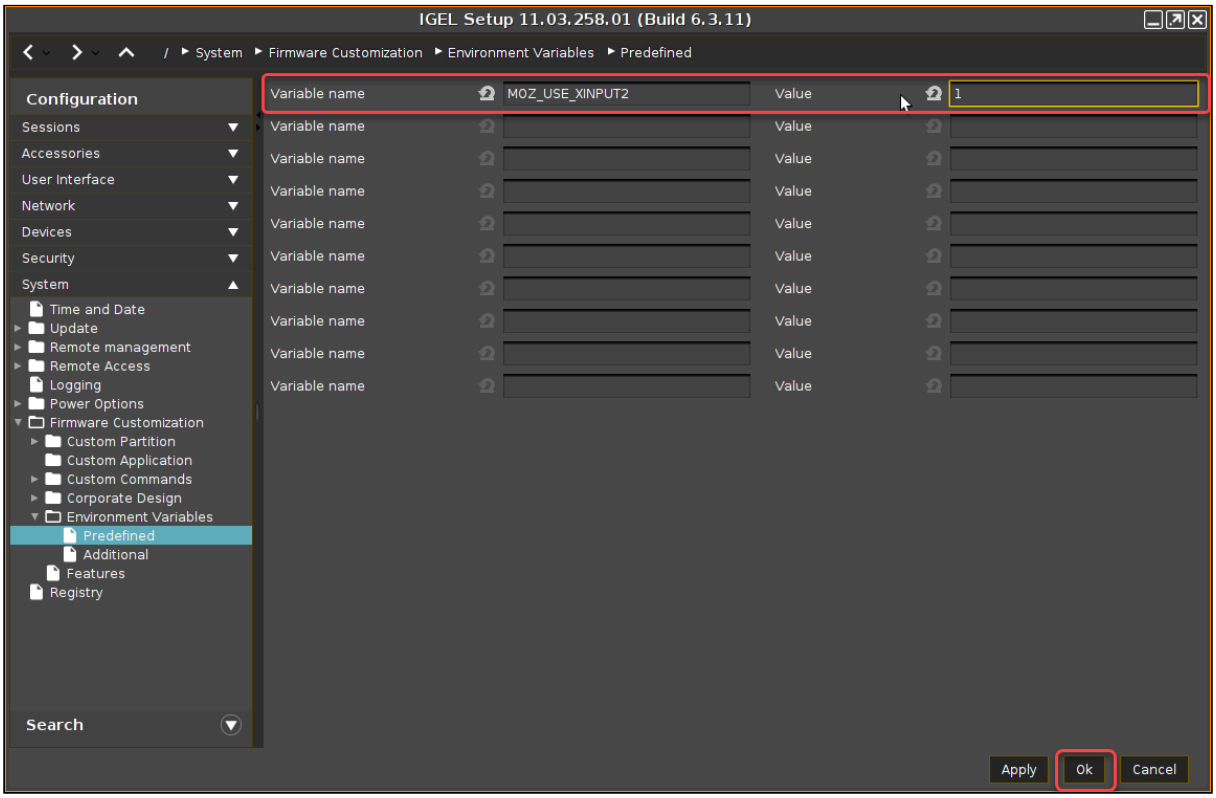


Touchscreen: Multitouch/Gesture Support for Firefox

You can use multitouch/gestures in the Firefox browser that is built into IGEL OS 10 and IGEL OS 11. This is done by adding an environment variable.

To enable multitouch:

1. Open the local Setup or the UMS configuration dialog and go to **System > Firmware Customization > Environment Variables > Predefined**.
2. In the first free **Variable name** field, enter `MOZ_USE_XINPUT2.`
3. In the corresponding **Value** field, enter `1.`
4. Click **Ok**.



5. Reboot the device.
6. To check if multitouch is working, open the Firefox browser and go to https://www.paulirish.com/demo/multi.

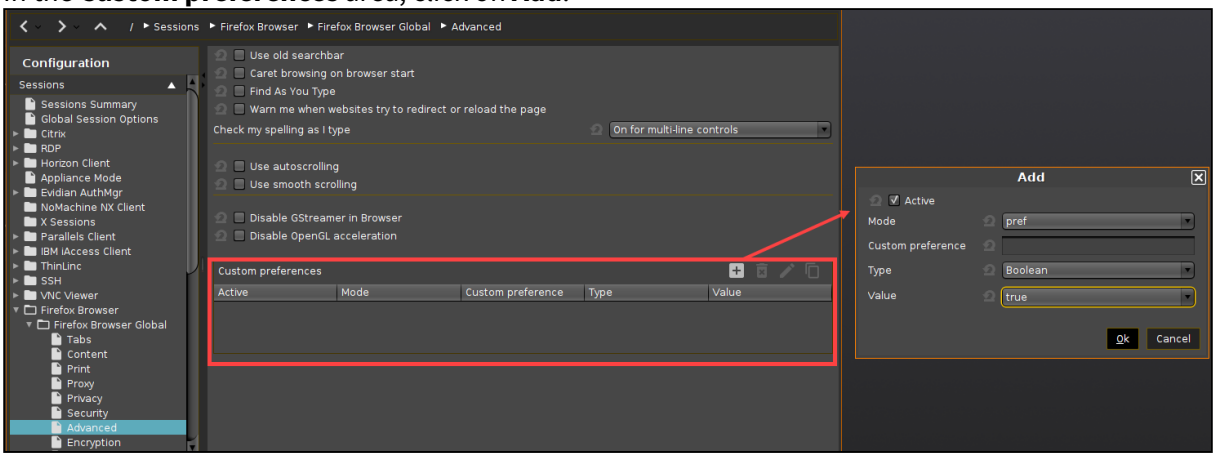
How to Set Advanced User Preferences for the Browser

The Mozilla Firefox browser included in IGEL OS offers a vast array of configuration options. They range from the sorting order of bookmarks over encryption algorithms to fixing quirks in web applications that are important to you. In total, they are too many to present them as individual items in IGEL Setup. However, as of IGEL Linux version 5.09.100, IGEL Setup lets you set any browser user preference in a generic way.

Changes to the advanced Firefox browser settings can impair its stability, security, and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in IGEL *Setup*.

You will find information regarding the configuration parameters for Firefox in the MozillaZine Knowledge Base under Firefox About:config entries[76].

1. In Setup, go to **Sessions > Firefox Browser > Firefox Browser Global > Advanced**.
2. In the **Custom preferences** area, click on **Add**.



3. Using the **Active** option, specify whether the configuration parameter is to be active.
4. Specify the **Mode** of the configuration parameter - for many cases **pref** will do.
5. Under **Custom preference**, give the name of the configuration parameter. Example:
   `ui.textSelectBackground`
6. Specify the **Type** of the configuration parameter.
   Possible values:
   - **String**: The value is a string of characters.
   - **Integer**: The value is a whole number.
   - **Boolean**: The value is a Boolean value, i.e. `true` or `false`.
7. Specify the **Value** of the configuration parameter. The possible entries depend on the **Type** selected.
8. Click **Ok**.
   The configuration parameter will take effect the next time that the browser is launched.

76. http://kb.mozillazine.org/About:config_entries

For more details on browser configuration, refer to the section Firefox Browser Global[77] in the IGEL OS reference manual.

77. https://kb.igel.com/en/igel-os/11.10.270/firefox-browser-global-settings-in-igel-os

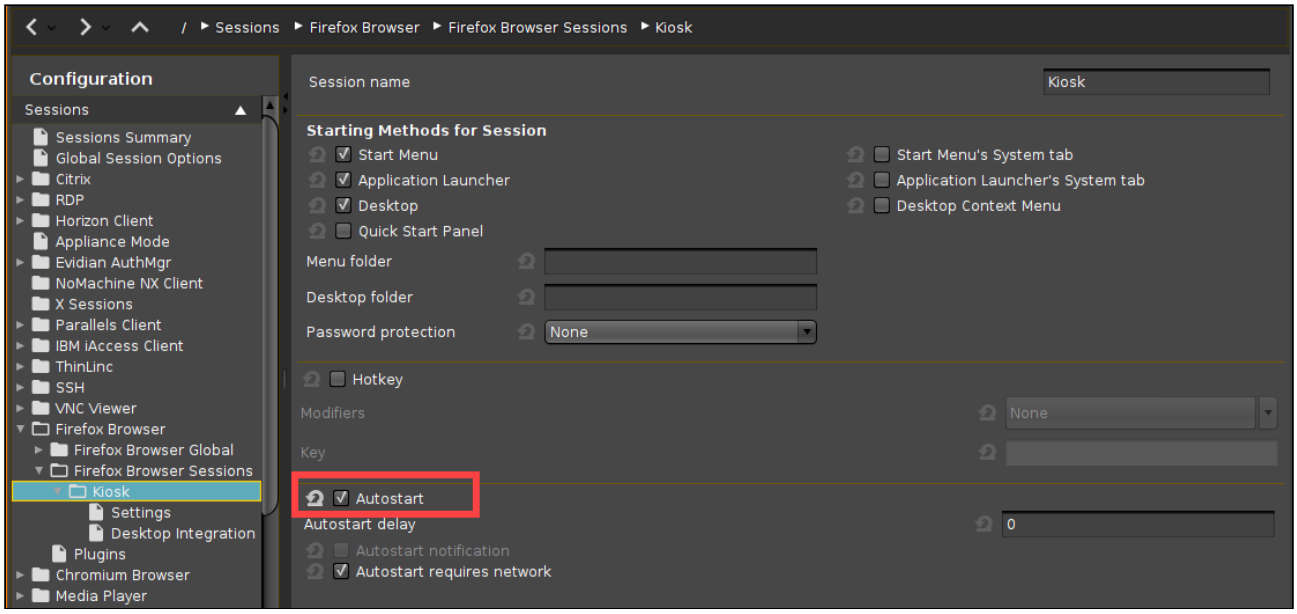
How to Use the Firefox Browser in Kiosk Mode

Browser kiosk mode is an option when you are operating any kind of public terminal with anonymous access, e.g.:

- Educational service in a museum
- Service terminals or ticket vending machines for public transport
- Entry portal for a corporate intranet

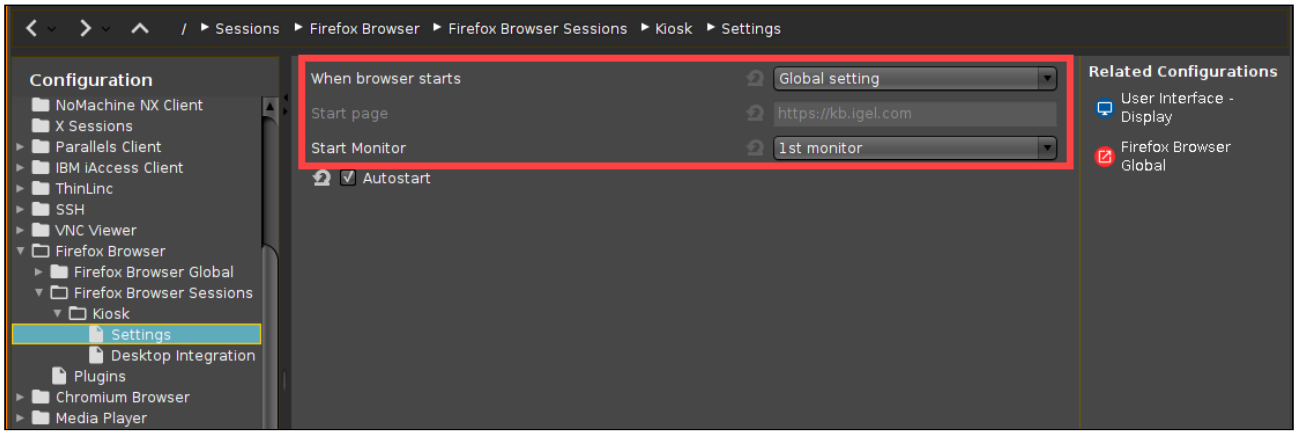
Albeit configuring an IGEL OS device for browser kiosk mode may seem quite extensive, you have the possibility to define your own flavor of kiosk mode. Consider the following settings.

Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name]



->Activate **Autostart**.

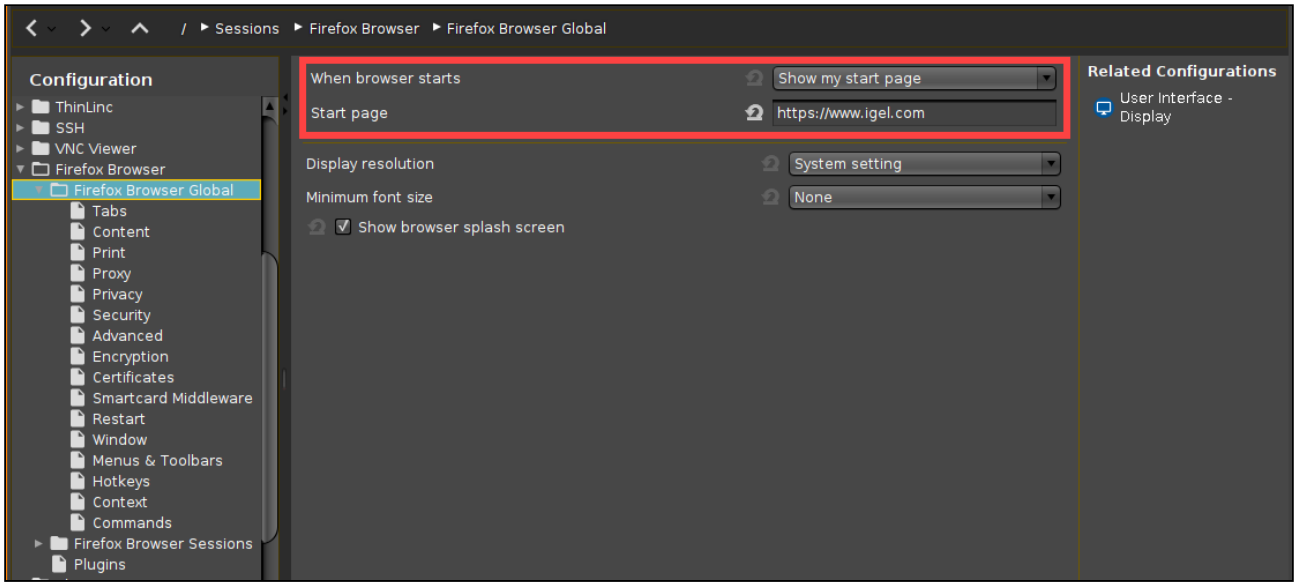
Settings under Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings



->Set **When browser starts** to **Global setting**.

->If necessary, select the correct **Start Monitor**.

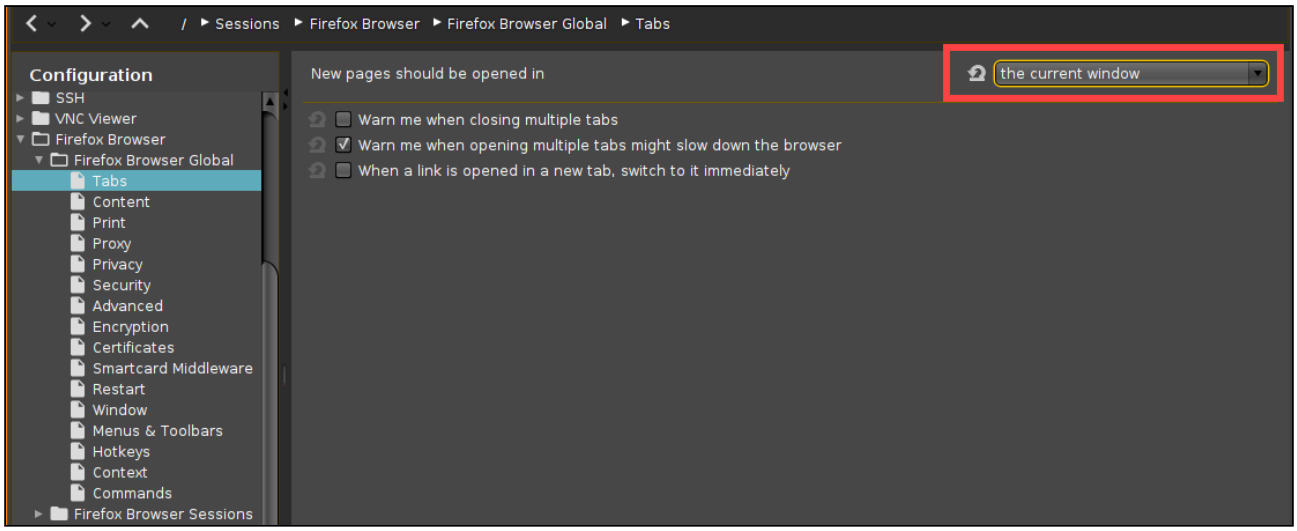
Settings under Sessions > Firefox Browser > Firefox Browser Global



->Set **When browser starts** to **Show my start page**.

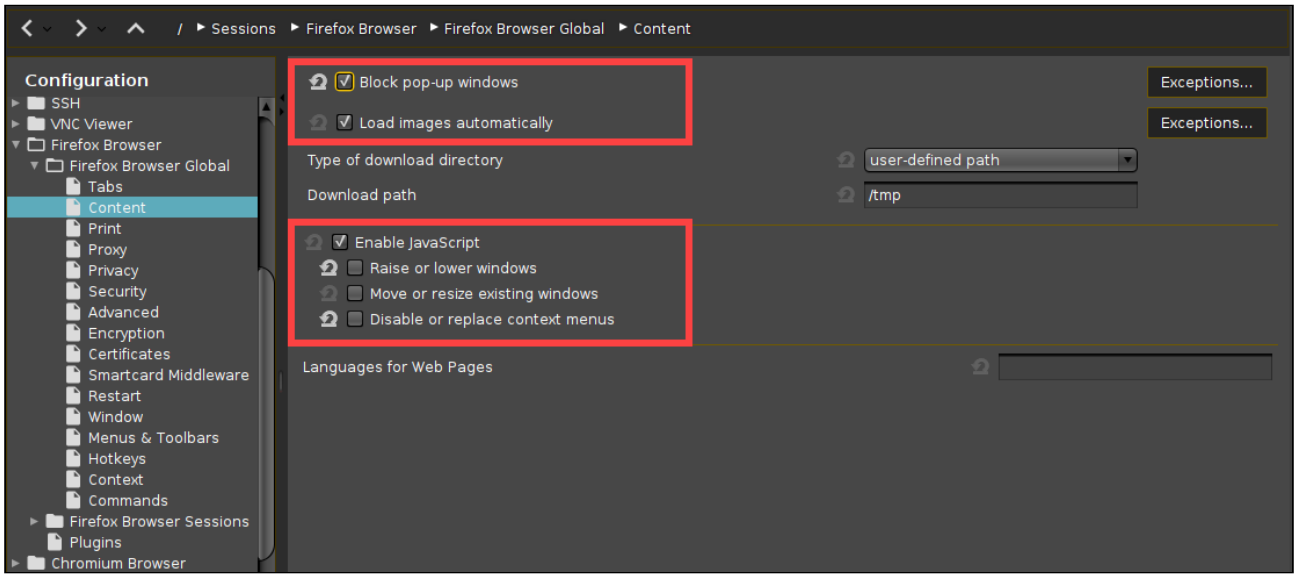
->Set **Start Page** to the desired start page.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Tabs



->Set **New pages should be opened in** to **the current window** or to **a new tab**.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Content

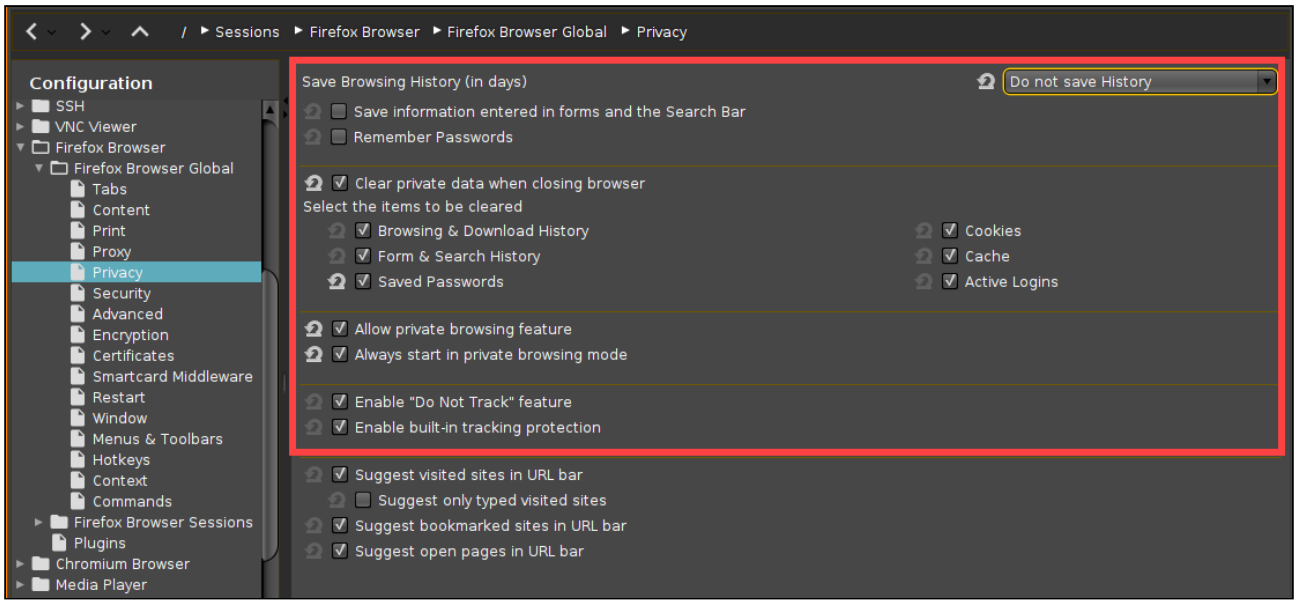


->If applicable, activate **Block pop-up windows**.

->Activate **Load images automatically**.

->If required, activate **Enable JavaScript** and adapt the actions permitted for JavaScript according to your needs.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Privacy



->Set **Save Browsing History (in days)** to **Do not save History**.

->Deactivate **Save information entered in forms and the Search bar**.

->Deactivate **Remember Passwords**.

->Activate **Clear private data when closing browser**.

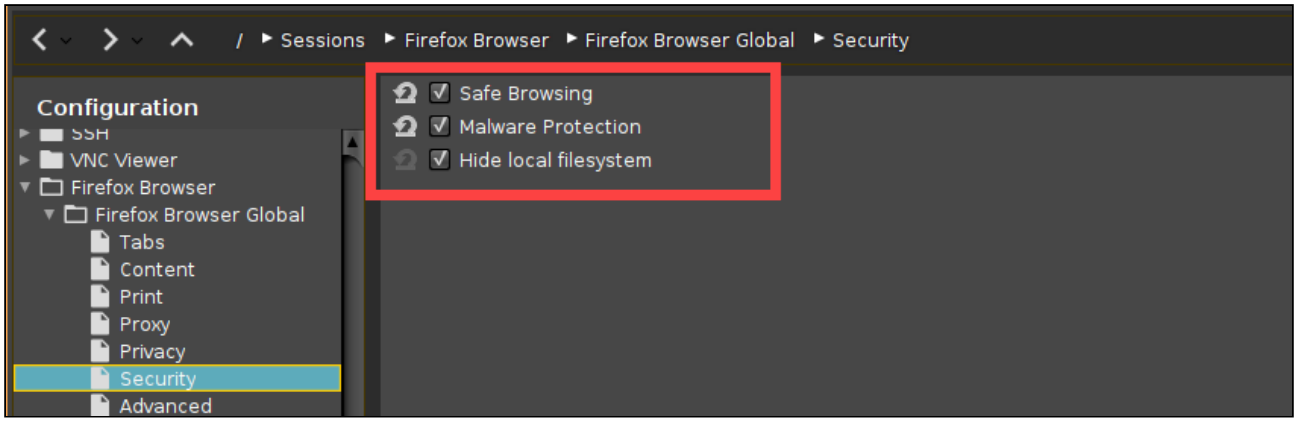
->Activate all items in the area **Select the items to be cleared**.

->If you want to suppress any tracking of the user's activities, activate **Allow private browsing feature** and **Always start in private browsing mode**.

->If applicable, activate **Enable "Do Not Track" feature**.

->To make the browser block domains and websites which are known for tracking users, activate **Enable built-in tracking protection**.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Security

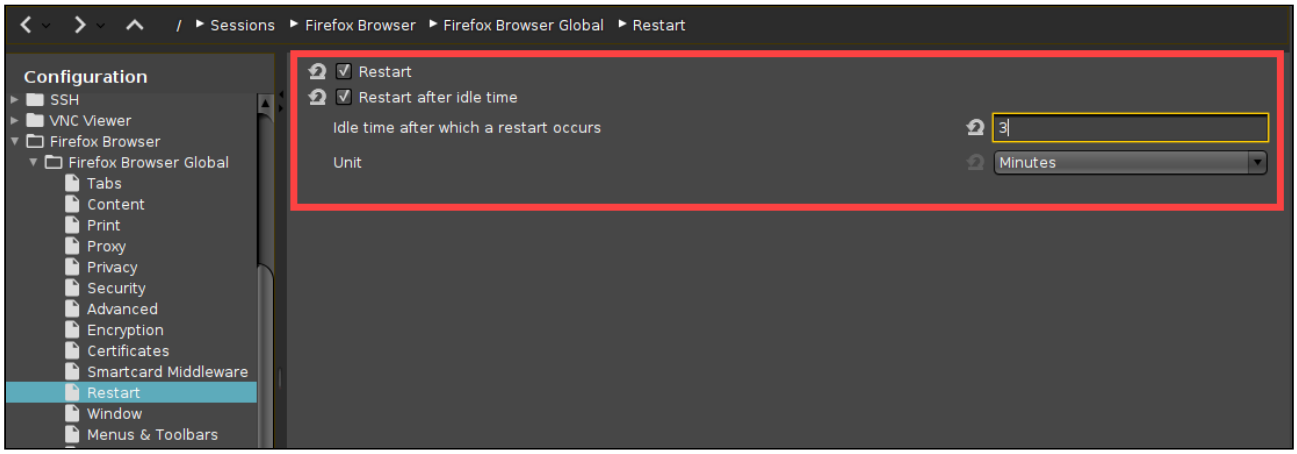


->To enable phishing protection, activate **Safe Browsing**.

->To enable protection against malicious downloads, activate **Malware Protection**.

->Activate **Hide local filesystem**.

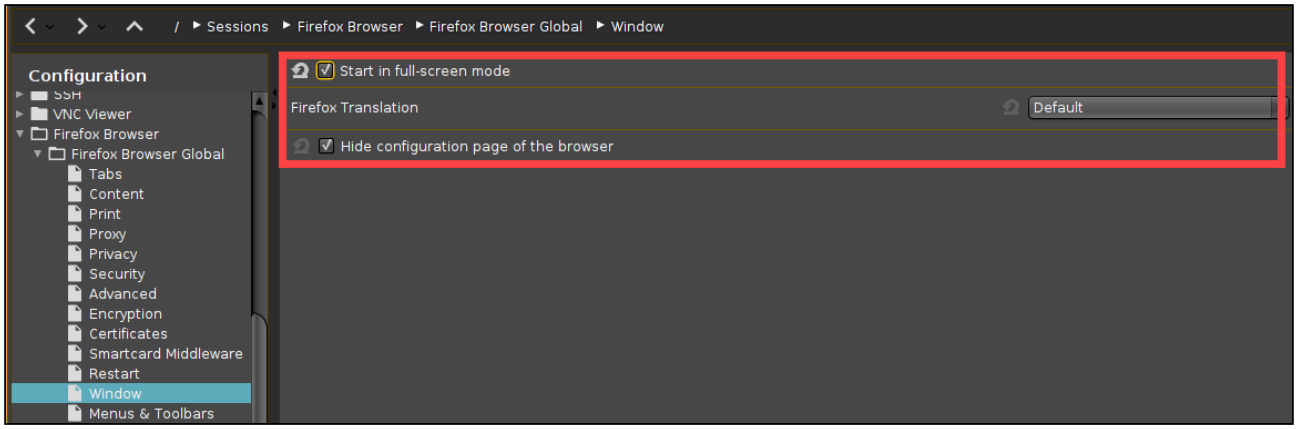
Settings under Sessions > Firefox Browser > Firefox Browser Global > Restart



->Activate **Restart**. The browser will restart automatically if a user closes the browser window.

->If you want the browser to restart automatically after some idle time, activate **Restart after idle time** and specify **Idle time after which a restart occurs** in minutes or seconds.

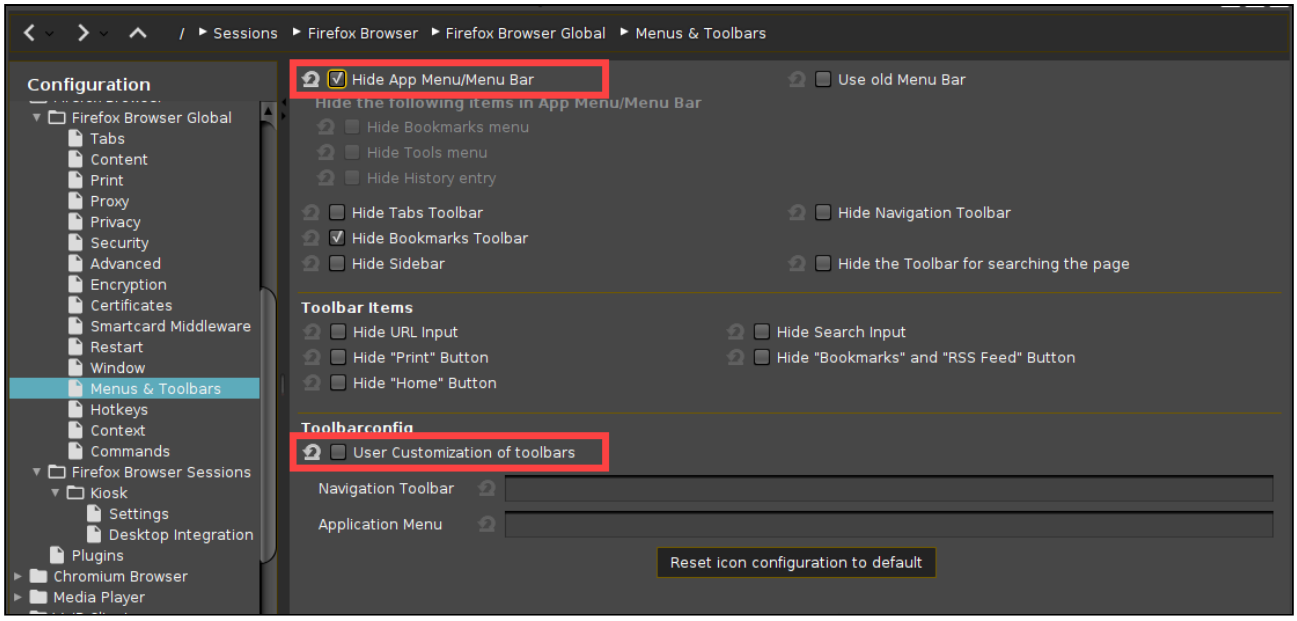
Settings under Sessions > Firefox Browser > Firefox Browser Global > Window



->If the browser shall run in full-screen mode, activate **Start in full-screen mode**.

->Activate **Hide configuration page of the browser**.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars

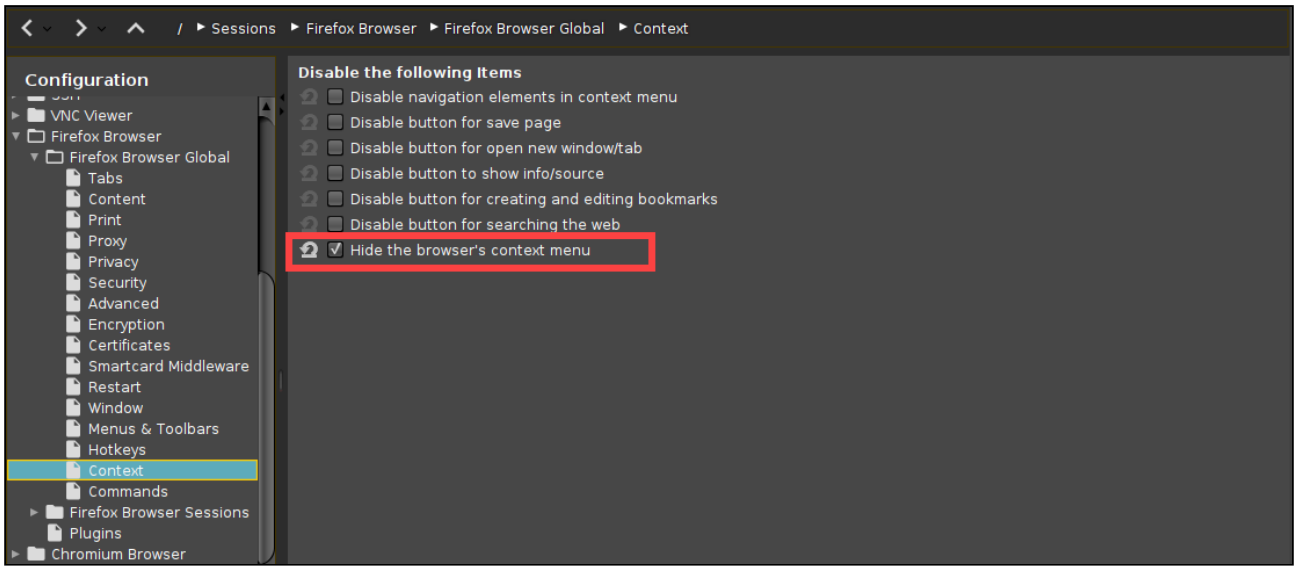


->Activate **Hide App Menu/Menu Bar**.

->Select which menus and toolbars are to be hidden. In the kiosk mode, all menus, toolbars, and the address bar are commonly hidden.

->Deactivate **User Customization of toolbars**.

Settings under Sessions > Firefox Browser > Firefox Browser Global > Context



->Activate **Hide the browser's context menu**.

Disabling Access to Developer Tools

To disable access to the developer tools, add the following custom preference.

For general instructions on adding custom preferences, see How To Set Advanced User Preferences for the Browser (see page 571).

Mode	`pref`
Custom preference	`devtools.toolbox.host`
Type	`String`
Value	(leave the value field empty)

Disabling Crash Reports

To disable crash reports, add the following three custom preferences.

For general instructions on adding custom preferences, see How To Set Advanced User Preferences for the Browser (see page 571).

Mode	`pref`
Custom preference	`datareporting.policy.dataSubmission`

Type	`Boolean`
Value	`false`
Mode	`pref`
Custom preference	`datareporting.healthreport.upload`
Type	`Boolean`
Value	`false`
Mode	`pref`
Custom preference	`toolkit.telemetry`
Type	`Boolean`
Value	`false`

Troubleshooting: SSL/TLS Error with Firefox in Appliance Mode

Symptom

Firefox on IGEL Linux 5.07.100 warns of an SSL/TLS error in appliance mode that does not occur in normal window mode. The error code is ssl_error_unsupported_version. This does not happen on IGEL Linux 5.06.x.

Problem

You cannot connect to the affected HTTPS service.

Solution

As a workaround you can instruct Firefox to ignore issues with SSL/TLS versions:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Commands > Base Commands**
2. Enter the following command into the **After Session Configuration** input field:
   `echo "clearPref(\"security.tls.version.min\");" >> /services/fbrw/firefox/firefox.cfg`

There is also an IGEL Linux private build that addresses this issue.

Troubleshooting: Browser Cannot Download Files

Symptom

You are trying to view or download a file with the browser, but you get error messages instead.

Problem

The browser has no permissions for the file path you have selected for download. This is because the Firefox browser is being guarded by AppArmor for security reasons.

Solution

Check whether one of the following possibilities for downloading files is applicable/available:

- Storage hotplug device (USB flash drive) which is mounted to `/media/[device name]` or `/userhome/media/[device name]`
  For hotplug storage configuration, see Storage Hotplug (see page 1969).
- Network drive which is mounted to `/mnt/[folder name]`
- Folder `/userhome` in the local file system; not persistent

Troubleshooting: Some PDFs are not opened by Firefox

Symptom

When opening some PDFs from the Internet, the Mozilla Firefox browser opens a new window or tab, but fails to display the PDF contents.

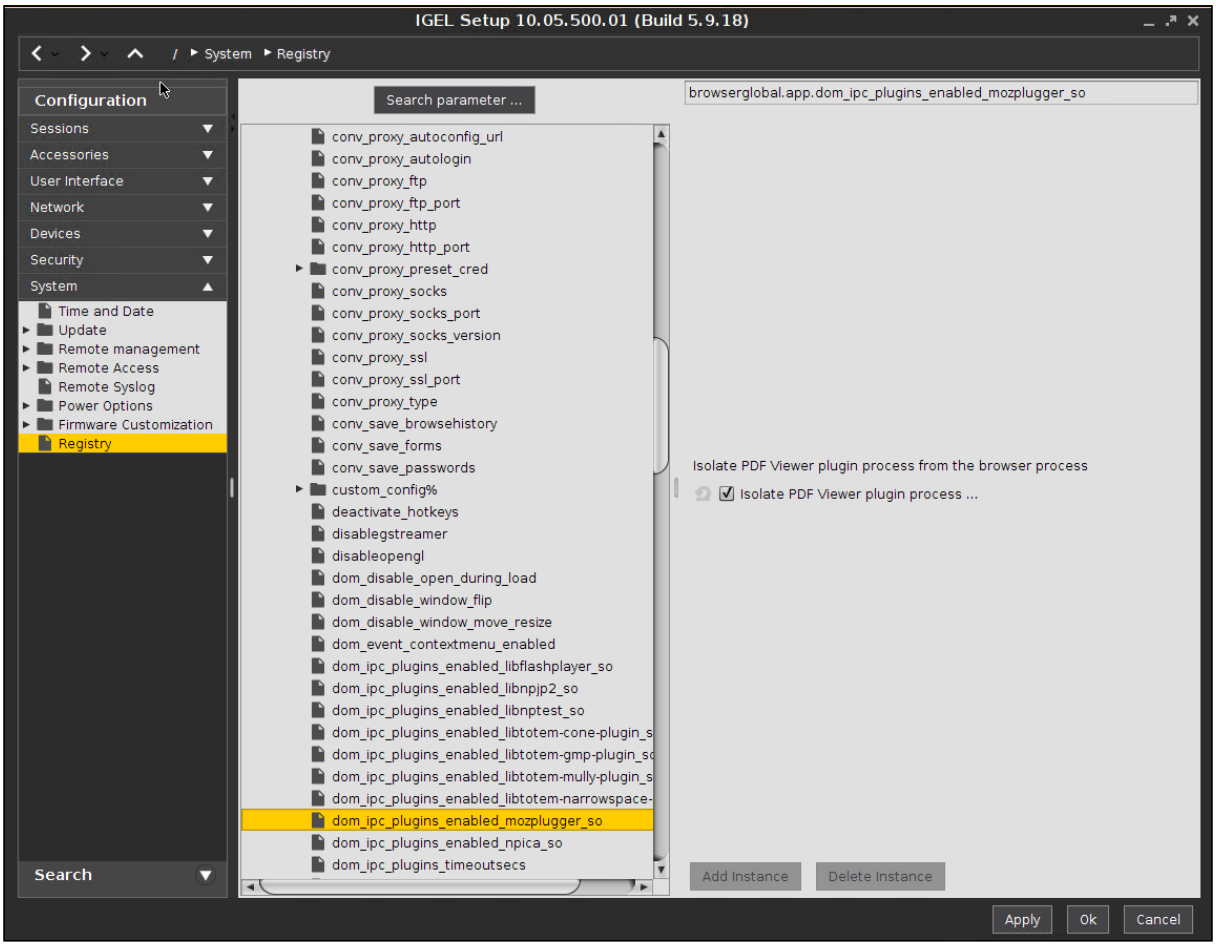
Problem

This can be due to a malfunction of the mozplugger Firefox component.

Solution

Disable mozplugger. Firefox will download the PDF document and open it with a local application (*IGEL Linux* 5.07.100 or newer):

1. Go to **System > Registry** in *IGEL Setup*.
2. Use **Search Parameter ...** to find the parameter `browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so`.
3. Check **Completely disable mozplugger**.
4. Confirm the setting with **Apply** or **OK**.
5. Restart Firefox.


IGEL Setup 10.05.500.01 (Build 5.9.18)
/ System Registry
Configuration
Sessions
Accessories
User Interface
Network
Devices
Security
System
Time and Date
Update
Remote management
Remote Access
Remote Syslog
Power Options
Firmware Customization
Registry
Search
Search parameter ...
conv_proxy_autoconfig_url
conv_proxy_autologin
conv_proxy_ftp
conv_proxy_ftp_port
conv_proxy_http
conv_proxy_http_port
conv_proxy_preset_cred
conv_proxy_socks
conv_proxy_socks_port
conv_proxy_socks_version
conv_proxy_ssl
conv_proxy_ssl_port
conv_proxy_type
conv_save_browsehistory
conv_save_forms
conv_save_passwords
custom_config%
deactivate_hotkeys
disablegstreamer
disableopengl
dom_disable_open_during_load
dom_disable_window_flip
dom_disable_window_move_resize
dom_event_contextmenu_enabled
dom_ipc_plugins_enabled_libflashplayer_so
dom_ipc_plugins_enabled_libnpjp2_so
dom_ipc_plugins_enabled_libnptest_so
dom_ipc_plugins_enabled_libtotem-cone-plugin_s
dom_ipc_plugins_enabled_libtotem-gmp-plugin_s
dom_ipc_plugins_enabled_libtotem-mully-plugin_s
dom_ipc_plugins_enabled_libtotem-narrowspace-
dom_ipc_plugins_enabled_mozplugger_so
dom_ipc_plugins_enabled_npica_so
dom_ipc_plugins_timeoutsecs
browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so
Isolate PDF Viewer plugin process from the browser process
Isolate PDF Viewer plugin process ...
Add Instance
Delete Instance
Apply
Ok
Cancel

Can I Install Firefox Extensions?

Question

Can Firefox extensions be installed?

Answer

The installation of Firefox extensions is not possible. This applies to any version of both IGEL Linux v5.x and IGEL OS.

Troubleshooting: Cannot Download Outlook E-mail Attachments

Problem

When trying to download an attachment from e-mails in Outlook in Chromium Browser, Chromium only downloads a file named with a uid.

Solution

Deactivate the dialog for accepting downloads by disabling the following registry key:

Parameter	**Enable IGEL Download Dialog**
Path	**System > Registry**
Registry	`chromiumglobal.app.enable_download_dialog`
Value	**enabled** (default) / **disabled**

Troubleshooting: Cannot Log in to MS Teams in Chromium Browser

Problem

When you try to sign in to Microsoft Teams in Chromium Browser, the site loops continuously, and you can't sign in.

For more information, see https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-sign-in/sign-in-loop#resolution.

Solution

For Microsoft Teams to work in Chromium Browser, it is required to allow the use of cookies. You can allow the use of all third party cookies in Chromium Browser by disabling the **Block third party cookies** parameter under **Sessions > Chromium Browser > Chromium Browser Global > Privacy**.

You can also configure cookie exceptions while keeping third party cookies blocked through adding a custom policy:

1. Go to **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Policies**.
2. Click + **Add** to create a policy.
3. For **Policy name**, enter: `CookiesAllowedForUrls`
4. In the **Policy value** field enter the following list of URLs: `[[*.]microsoft.com; [*.]microsoftonline.com; [*.]teams.skype.com; [*.]teams.microsoft.com; [*.]sfbassets.com; [*.]skypeforbusiness.com]`
5. Save the changes.

System

- Which Features of IGEL OS Will Be Affected If the UMS Is Down? (see page 589)
- Solving Issues with Signed Partitions (see page 590)
- Fabulatech Redirection Server Component (see page 598)
- How to Show the Boot Mode of IGEL OS (see page 599)
- Error: "Unknown filesystem..." (see page 600)
- Troubleshooting: Custom Boot Commands Are Still Active after Factory Reset (see page 601)
- How to Disable IGEL OS Features to Reduce Firmware Size (see page 602)
- How to Reset a Device with Unknown Administrator Password (see page 604)
- How Can I Install IGEL OS 11 on a Virtual Machine? (see page 606)

Which Features of IGEL OS Will Be Affected If the UMS Is Down?

Overview

In general, IGEL OS works independently of the Unified Management Suite (UMS). This includes, for instance, all remote desktop clients like Citrix, RDP, or VMware Horizon, and browsers.

Any configuration changes that are made via the UMS are stored on the device and thus remain stable when the UMS is down.

However, the Shared Workplace (SWP) feature and administration functions are affected by a UMS outage.

The following sections list the details.

Productivity Features That Are Affected If the UMS Is Down

- Login via Shared Workplace (SWP); see SWP in Archive > UMS PDF

Administration Functions That Are Affected If the UMS Is Down

- Configuration changes
- License Management
- Secure Shadowing
- Secure Terminal
- Universal Firmware Update
- Firmware Customizations
- Transfer of files to the device, including Custom Partitions
- Remote commands, such as Wake-on-LAN or restart

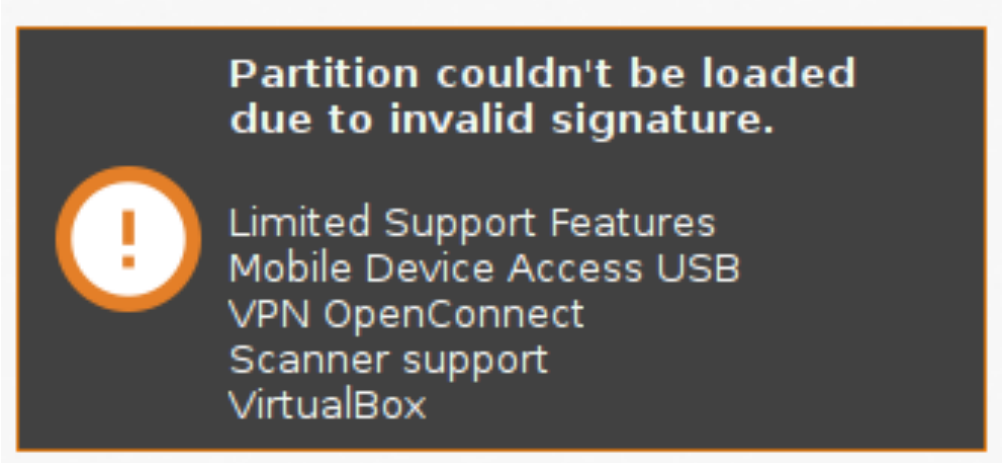
Solving Issues with Signed Partitions

- Error: "Partition couldn't be loaded due to invalid signature" (see page 591)
- Error: Device Plays a Beep Code Instead of Booting (see page 592)
- Error: "The new firmware is not signed. Update not allowed." (see page 595)
- Error: "Invalid signature - Failed to read from partition" (see page 597)

Error: "Partition couldn't be loaded due to invalid signature"

Symptom

During operation, a system message like this appears:



Environment

- IGEL OS 11.03 or higher

Problem

A system partition has been invalidated, which prevents system components from being loaded.

Solution

1. Ensure that a valid update source is configured under **System > Update > Firmware Update** and the correct firmware is stored on the server. (For detailed information, see Firmware Update (see page 2056).) If the local Setup is not accessible, use the UMS.
2. Reboot the device.
   The device fetches the valid partition from the update source.

Error: Device Plays a Beep Code Instead of Booting

Symptom

The boot process fails, and a beep code is played. Two beep codes are possible:

- 3 short and 1 long beep, repeated 2 times (whole sequence repeats up to 1 minute)
- Long beep is played for 1,1 seconds, then 2,9 seconds pause (repeats up to 1 minute)

Environment

- IGEL OS 11.03 or higher

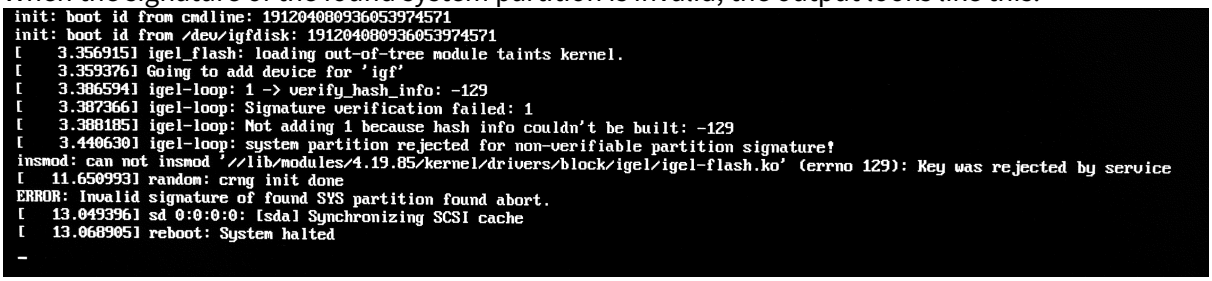
Problem

- 3 short and 1 long beep, repeated 2 times (whole sequence repeats up to 1 minute): The signature of the found system partition is invalid.
- Long beep is played for 1,1 seconds, then 2,9 seconds pause (repeats up to 1 minute): After up to 120 tries, no suitable system partition has been found at all.

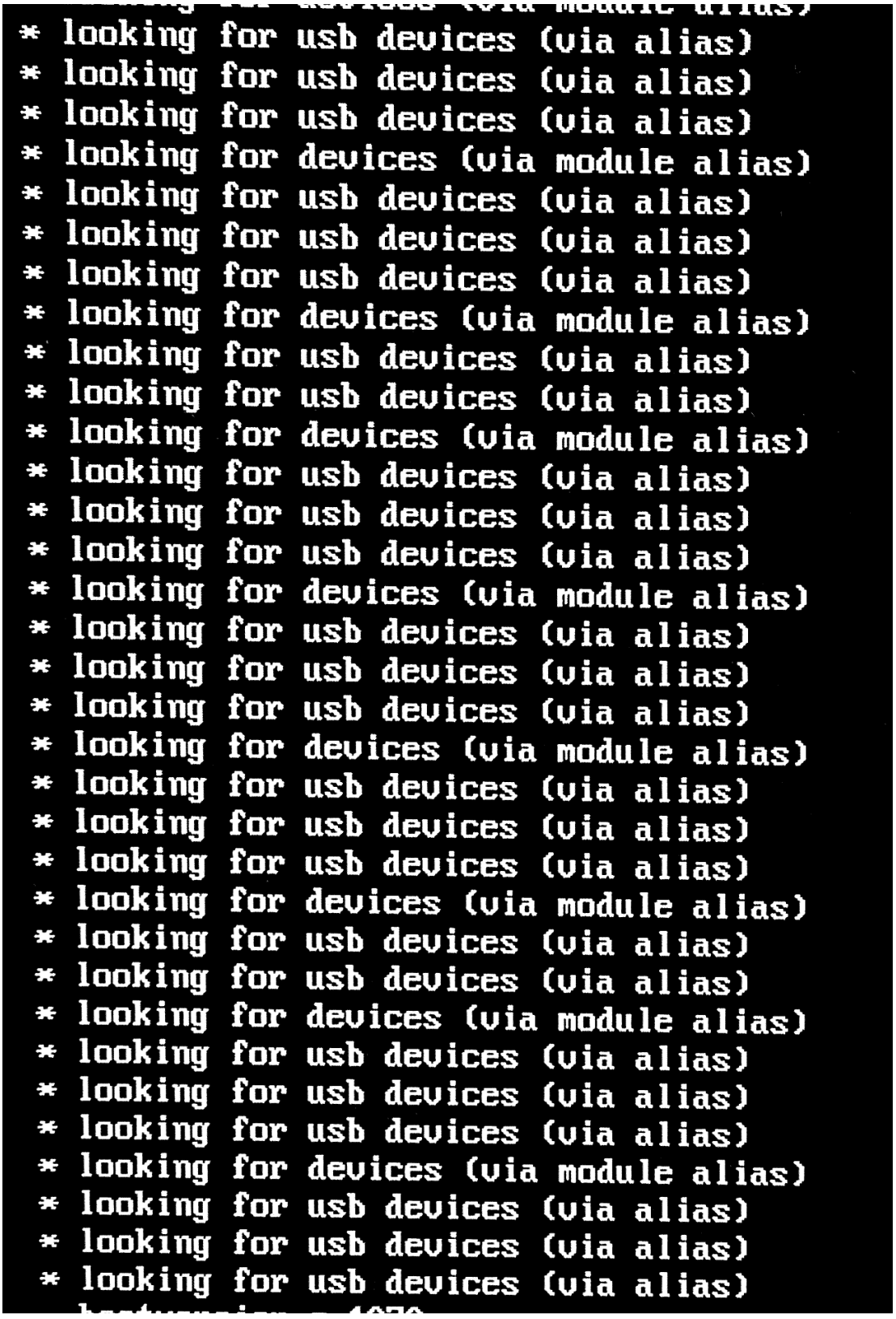
Diagnosis

To obtain further details:

1. Reboot the device and press [ESC] repeatedly.
2. Select **Verbose Boot**.
   When the signature of the found system partition is invalid, the output looks like this:



   When no suitable system partition has been found at all, the output looks like this:


* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for devices (via module alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)
* looking for usb devices (via alias)

Solution

→ Install IGEL OS anew on the device with IGEL OS Creator (OSC). For instructions, see the Installation (see page 2125) chapter of the IGEL OS Creator Manual (see page 2120).

Preserve Your Settings

To prevent the device's settings from being deleted, ensure that **Migrate Old Settings** is activated in the installation settings; see Installation Procedure (see page 2137).

Data That Will Be Lost

When IGEL OS is installed anew, the following data will be lost:

- All data on the writable partition `/wfs`
- All data that has been stored in a Custom Partition since its deployment; Custom Partitions will be reset to their original state.

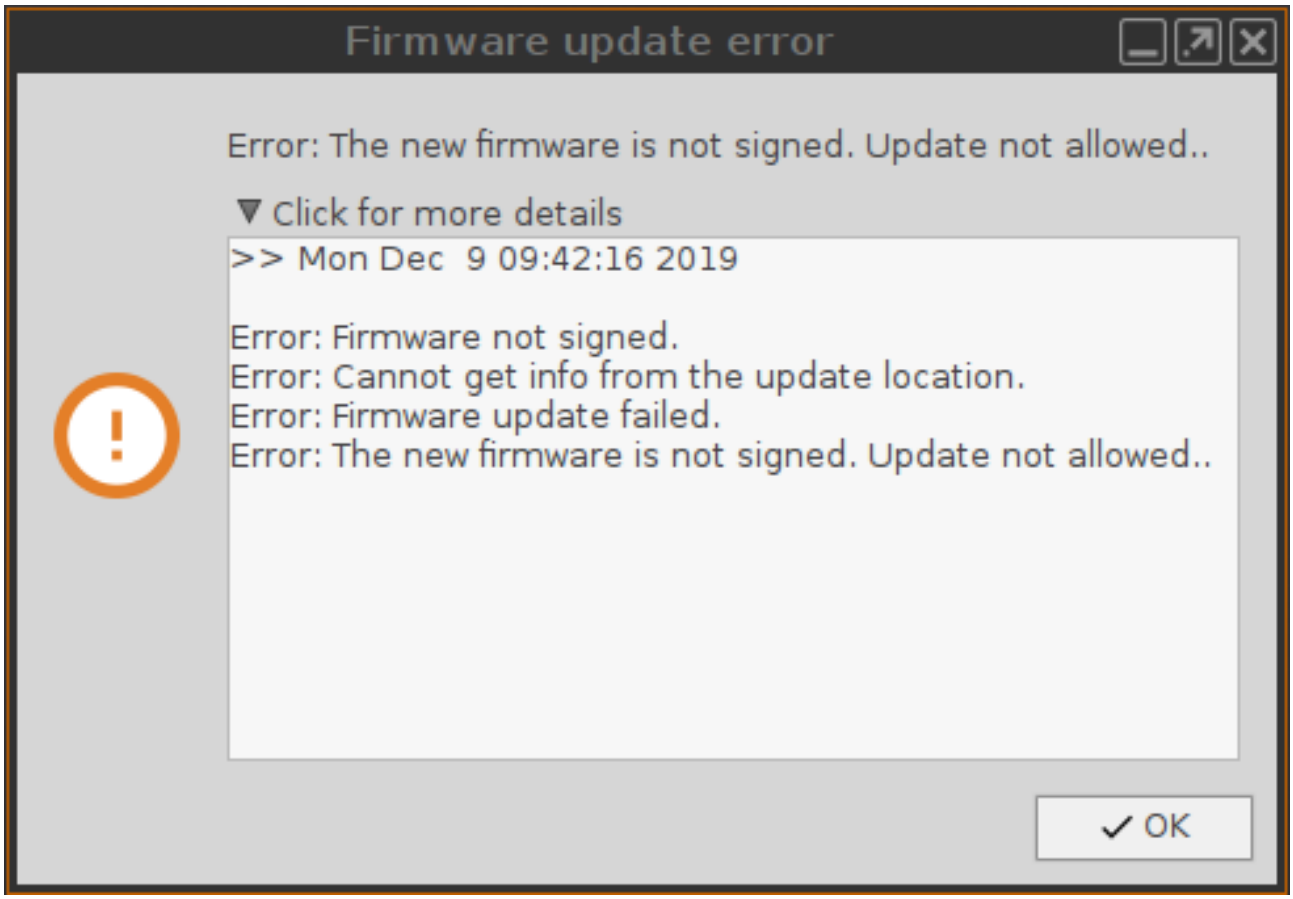
Preservation of Licenses

When IGEL OS is installed anew, any licenses stored on the device are preserved, provided that the relevant partition is valid.

Error: "The new firmware is not signed. Update not allowed."

Symptom

During the update process, the following error messages are shown:



Environment

- IGEL OS 11.03 or higher

Problem

The system expects signed system partitions, but the partitions of the update source are not signed. This will occur when you have tried to downgrade from IGEL OS 11.03 or higher to an older version of IGEL OS 11.

Solution

->If you want to downgrade from IGEL OS 11.03 to IGEL OS 11.02, e. g. because you need certain older client versions, set the update source to IGEL OS 11.02.200.

IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 which has signed partitions; this version can only be obtained from the IGEL Support Team.

Error: "Invalid signature - Failed to read from partition"

Symptom

During operation, a system message like this appears:

Environment

- IGEL OS 11.03 or higher

Problem

A system partition has been invalidated, which prevents system components from being loaded.

Solution

1. Ensure that a valid update source is configured under **System > Update > Firmware Update** and the correct firmware is stored on the server. (For detailed information, see Firmware Update (see page 2056).) If the local Setup is not accessible, use the UMS.
2. Reboot the device.
   The device fetches the valid partition from the update source.

Fabulatech Redirection Server Component

For Fabulatech USB Redirection and Scanner Redirection, a special Fabulatech server component must be installed on the Citrix, Horizon, AVD, Amazon, RDP or HP Anyware PCoIP server (USB for Remote Desktop IGEL Edition).

You can find more detailed information on the function and download the component at the Fabulatech partner site[78].

Current versions:

- USB Redirection: https://www.fabulatech.com/usb-for-remote-desktop-download.html#tab_usbrdp-lin-linux-current
- Scanner Redirection: https://www.usb-over-network.com/partners/igel/scanner-for-remote-desktop-download.html

You can find more information on Fabulatech Redirections in IGEL OS in the following articles:

- Citrix: Fabulatech USB Redirection for Citrix in IGEL OS (see page 1271) and Fabulatech Scanner Redirection (see page 1275)
- RDP: Fabulatech USB Redirection for RDP in IGEL OS (see page 1333) and Fabulatech Scanner Redirection (see page 1275)
- Horizon: Fabulatech USB Redirection for Horizon in IGEL OS (see page 1378) and Fabulatech Scanner Redirection 2 (see page 1386)
- AVD: Fabulatech Redirection for AVD in IGEL OS (see page 1660)

78. http://www.usb-over-network.com/partners/igel/

How to Show the Boot Mode of IGEL OS

To check the boot mode of IGEL OS, proceed as follows:

1. Open the IGEL start menu.
2. Click the i-icon.
   The **About** dialog opens.
3. Find the parameter **Boot Mode** under the **Hardware** section.
   Example: BIOS

Error: "Unknown filesystem..."

Symptom

The boot process is aborted at an early stage; the error message is "Unknown filesystem. Couldn't find valid IGEL partition..."

Environment

- IGEL OS (any version)

Problem

One or more system partitions could not be found or are not valid.

Solution

→ Install IGEL OS anew on the device with IGEL OS Creator (OSC). For instructions, see the Installation (see page 2125) chapter of the IGEL OS Creator Manual (see page 2120).

> **Preserve Your Settings**
>
> To prevent the device's settings from being deleted, ensure that **Migrate Old Settings** is activated in the installation settings; see Installation Procedure (see page 2137).

> **Data That Will Be Lost**
>
> When IGEL OS is installed anew, the following data will be lost:
>
> - All data on the writable partition `/wfs`
> - All data that has been stored in a Custom Partition since its deployment; Custom Partitions will be reset to their original state.

> **Licenses Will Be Lost**
>
> In this scenario, the licenses stored on the device will be lost. However, the licenses are cached in the UMS, so that they will be restored when the device registers with the UMS.

Troubleshooting: Custom Boot Commands Are Still Active after Factory Reset

Symptom

You have reset your device to factory defaults, but the custom boot commands are still active.

Problem

After a factory reset, the following settings will still be available:

- `boot_id`
- `uptime_total`
- `product`
- `force_Legacy`
- The bootreg entry `Splash` will be set to `1`

Solution

You can delete these settings manually with the following command:

1. Open a local terminal and log in as root.
2. Enter the following command to delete the settings:
   `bootreg delete /dev/igfdisk boot_cmd`

For further information about custom boot commands, see Custom Boot Command (see page 1226).

How to Disable IGEL OS Features to Reduce Firmware Size

You want to update your IGEL OS firmware to a higher release version, but the firmware update requires more disk space. Updating devices with less disk space than required leads to an error: `Not enough space on local drive`.

Problem

The size of the new firmware

- with all enabled software features included
- with the NVIDIA graphics driver
- with the Firefox profile partition
- possibly with a custom partition
- possibly with custom wallpaper and bootsplash

exceeds the device's disk space (e.g. 2 GB).

Solution

Disable firmware features not needed for the productive operation to reduce the size of the firmware:

1. In IGEL Setup, go to **System > Firmware Customization > Features**.
2. Disable features not needed in your environment.
3. Save your settings with **Apply** or **OK**.
4. Reboot the device.
5. Update the device.

> Use profiles in order to deactivate features on a group of devices. For details on profiles, see Profile (see page 602).

> **Alternative Method for Reducing the Feature Set as of IGEL OS 11.04**
> If you update to IGEL OS 11.04 or higher, you can alternatively use the method described under Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318). The advantage of this method in comparison to disabling features via the IGEL Setup is that you won't have to disable the deactivated features once again in case you reset the endpoint device to factory defaults (see Reset to Factory Defaults (see page 1225)).

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=KmcCcdoGbNM

How to Reset a Device with Unknown Administrator Password

Symptom

An administrator password has been set on IGEL OS (via **Setup > Security > Password > Administrator**) but it has been lost.

Problem

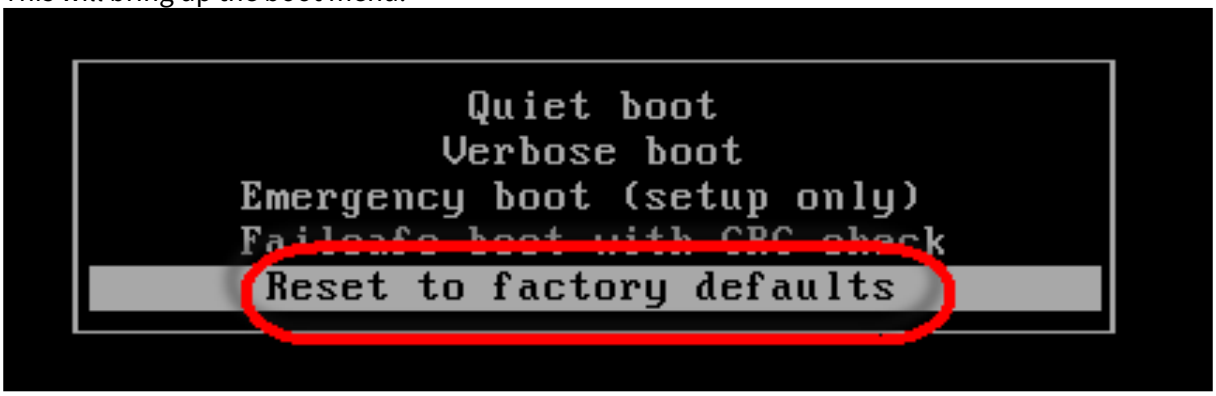
The local setup is not accessible without the password. Also, resetting the device to factory defaults seems impossible.

Solution

- Change the administrator password using IGEL UMS via **Setup > Security > Password > Administrator**
  or
- Reset the device using IGEL UMS via **Devices > Other commands > Reset to Factory Defaults** in the UMS menu.
  or
- Reset the thin client locally using a reset to defaults key provided by IGEL (as described below):

You can reset IGEL OS devices to factory defaults through the boot menu as described here, but the best practice is to reset devices using the OSC as descried in IGEL OS Creator Manual[79].

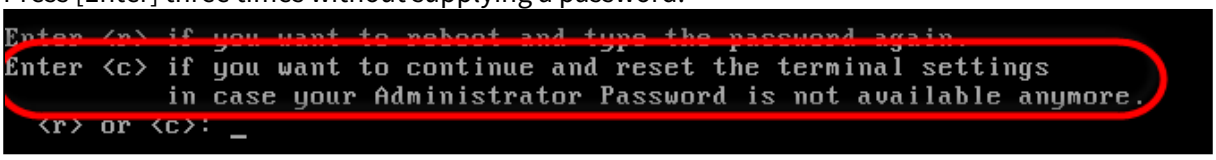
1. Press the [ESC] key repeatedly in rapid succession while the device is booting.
   This will bring up the boot menu.



2. Choose **Reset to factory defaults** and press [Enter].
   The following will be displayed:

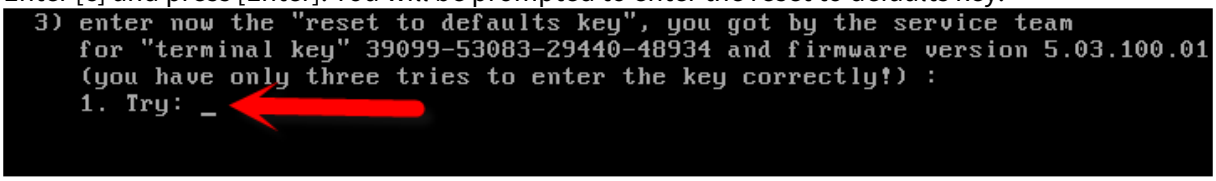
79. https://kb.igel.com/en/igel-os/11.10.270/igel-os-creator-manual

3. Press [Enter] three times without supplying a password.



4. Enter [c] and press [Enter].
   The software will then display a terminal key. Make a note of it, as you need it for requesting the reset to defaults key from IGEL.
5. Request a reset to defaults key from IGEL. Write an email to license@igel.com[80] containing
   - your terminal key
   - your email address as registered with IGEL support
   - your company address
   - your phone number

   IGEL will send you the reset to defaults key.
6. In the current session, enter [e] and press [Enter] to shut down the device.
7. On receiving the reset to defaults key, repeat steps 1 to 3 to boot the device with the same terminal key.
8. Enter [c] and press [Enter]. You will be prompted to enter the reset to defaults key.



9. Enter the reset to defaults key. Enter `yes` and press [Enter] to confirm resetting the client. All local thin client settings will be lost.

Should you enter the wrong key or mistype the key you will have to resume from step 1.

80. mailto:license@igel.com

How Can I Install IGEL OS 11 on a Virtual Machine?

You can install IGEL OS 11 on a virtual machine. Simply install the ISO file as usual.

The requirements for the virtual machines on which IGEL OS 11 has been tested successfully are described in the following.

VMWare Workstation

- Guest tools: Open Virtual Machine Tools (open-vm-tools)
- Size: 2,5 GB

Oracle VirtualBox

- Guest tools: VirtualBox Guest Additions
- Size: 2 GB

Microsoft Hyper-V

- Guest tools: none required, driver already integrated in the kernel
- Size: 2 GB

Network

- How to Configure Wi-Fi Network Roaming (see page 608)
- How to Change the SMB Protocol Version (see page 610)
- How to Make a Telnet Connection from IGEL Linux (see page 611)
- How to Configure Dynamic DNS Updates via DDNS (see page 612)
- How to Improve WiFi Connectivity (see page 614)
- Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates (see page 618)
- How to Prevent Permanent Storage of Wireless Network Keys (see page 622)
- Extended Logging With Syslog, Tcpdump and Netlog (see page 623)
- How to Run the OpenVPN Client with a Preconfigured Configuration File (see page 637)
- How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden (see page 639)
- How to Configure Open VPN Sessions (see page 641)
- How to Connect to a Wi-Fi Network with Hidden SSID (see page 653)
- How Can I Configure OpenVPN with an .ovpn or .conf File for IGEL OS Devices? (see page 654)
- Multiple Users with Individual VPNs Sharing One Endpoint (see page 660)
- IPv6 Settings (see page 661)

How to Configure Wi-Fi Network Roaming

Issue

Different wireless network instances have been configured for a mobile device. The device should switch over to the strongest network automatically.

Solution

Parameters to configure Wi-Fi roaming options can be found in the IGEL registry (**Setup > System > Registry**). These settings should be changed by experts only.

- Parameters for better control of Wi-Fi roaming capabilities with access points that share the same SSID:
  network.interfaces.wirelesslan.device0.lock_initial
  Default: `false`
  If `true`, the device will stick to the access point it is connected to even if candidates with better signal quality are present.
  Setting this parameter to `true` is a last resort for problems that are caused by too much roaming.

  network.interfaces.wirelesslan.device0.bgscan.module
  Default: `default` (Perserving the unpachted NM's behaviour)
  Possible values:
  `default`: No background scanning is done.
  `simple`: The Wi-Fi module tries to scan for a potentially better signal in the background.

  bgscan.module `simple` provides following options:
  network.interfaces.wirelesslan.device0.bgscan.simple.signal_strength (default: `-45 dBm`)
  This defines a threshold that determines which of the following two parameters shall be effective:

  network.interfaces.wirelesslan.device0.bgscan.simple.short_interval (default: `30 s`)
  Interval between background scans (in seconds) if the actual signal level of the currently connected access point is worse than signal_strength.

  network.interfaces.wirelesslan.device0.bgscan.simple.long_interval (default: `300 s`)
  Interval between background scans (in seconds) if the actual signal level of the currently connected access point is better than signal_strength.

If parameter **lock_initial** is `true`, it is recommended to set **bgscan.module** to `none`.

- Parameters to control Wi-Fi roaming between Wi-Fi networks with different SSIDs:
  network.interfaces.wirelesslan.device0.mssid_check_interval (default: `10 s`)
  The interval in seconds between checking if automatic roaming might be neccessary. This includes detecting that a connection has been lost and a new one should be established.

  network.interfaces.wirelesslan.device0.mssid_quality_threshold (default: `20`)
  If the current connection's quality percentage is below this value, scanning will be performed to find a potentially better network.

  network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold (default: `40`)
  A candidate for automatic roaming is only considered if its quality percentage is this much better than the current connection's quality.

  network.interfaces.wirelesslan.device0.mssid_previously_used_threshold (default: `55`)
  During boot: If the previously used SSID's quality percentage is above this threshold, it is preferred.

  network.interfaces.wirelesslan.device0.mssid_user_selection (default: `false`)
  If `true`, the user can initiate roaming to a network via the Wi-Fi tray icon's context menu (must be enabled).

  If automatic roaming shall not interfere with the user's choice, the following values are appropriate:
  network.interfaces.wirelesslan.device0.mssid_quality_threshold = `0`
  network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold = `101`
  network.interfaces.wirelesslan.device0.mssid_previously_used_threshold = `0`

How to Change the SMB Protocol Version

Depending on which Windows (Samba) server you are using, you will need a specific SMB protocol version.

> Due to security reasons, Microsoft recommends to disable SMB version 1.0 support on Windows ,so you need to switch to at least version 2.0 to be further able to access systems with disabled SMBV1.

IGEL Linux *version 10.04.100* and higher offer several SMB protocol versions.

To change the version setting:

1. In the IGEL Setup go to **System > Registry**.
2. Go to parameter `network.smbmount.smb_version`.
3. Select the apropriate **SMB protocol version**.
   Possible options:
   - 1.0
   - 2.0
   - 2.1
   - 3.0
4. Click **Save** or **Apply and send to thin client**.
   The windows shares are configurable at **IGEL Setup > Network > Network Drives > Windows Drive**.

How to Make a Telnet Connection from IGEL Linux

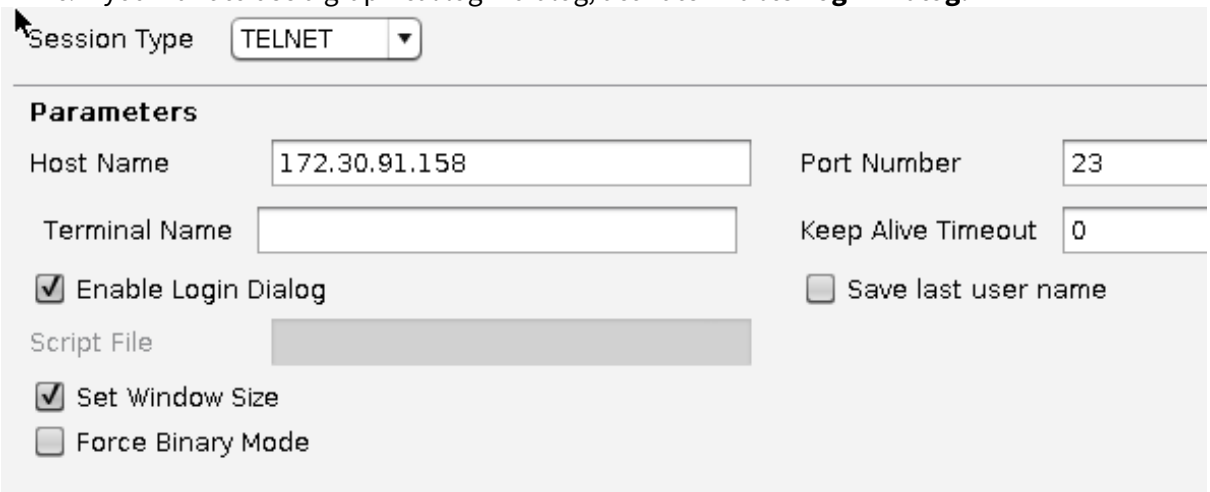
Issue

You want to connect to a Telnet service and can't find a Telnet command on the device.

Solution

Using Ericom Powerterm (Requires the Ericom Powerterm Firmware Feature):

1. In Setup, go to **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions**.
2. Create a new session.
3. Edit the session.
4. Under **Connection**, make the following settings:
    a. Select **TELNET** as **Session Type.**
    b. Enter an IP adress or a name in **Host Name.**
    c. If you want to use a graphical login dialog, activate **Enable Login Dialog.**



5. Under **Desktop Integration** enter a **Session Name** and enable the desired **Starting Methods for the Session.**
6. Click **Apply** to save your settings or **OK** to save and exit.
7. Start the new session and enter your username and password.

How to Configure Dynamic DNS Updates via DDNS

Issue

You want to register a device's IP address with your DNS server.

You are not using DHCP.

Solution

Use the DDNS tools contained in *IGEL Linux*, which can be configured by Setup.

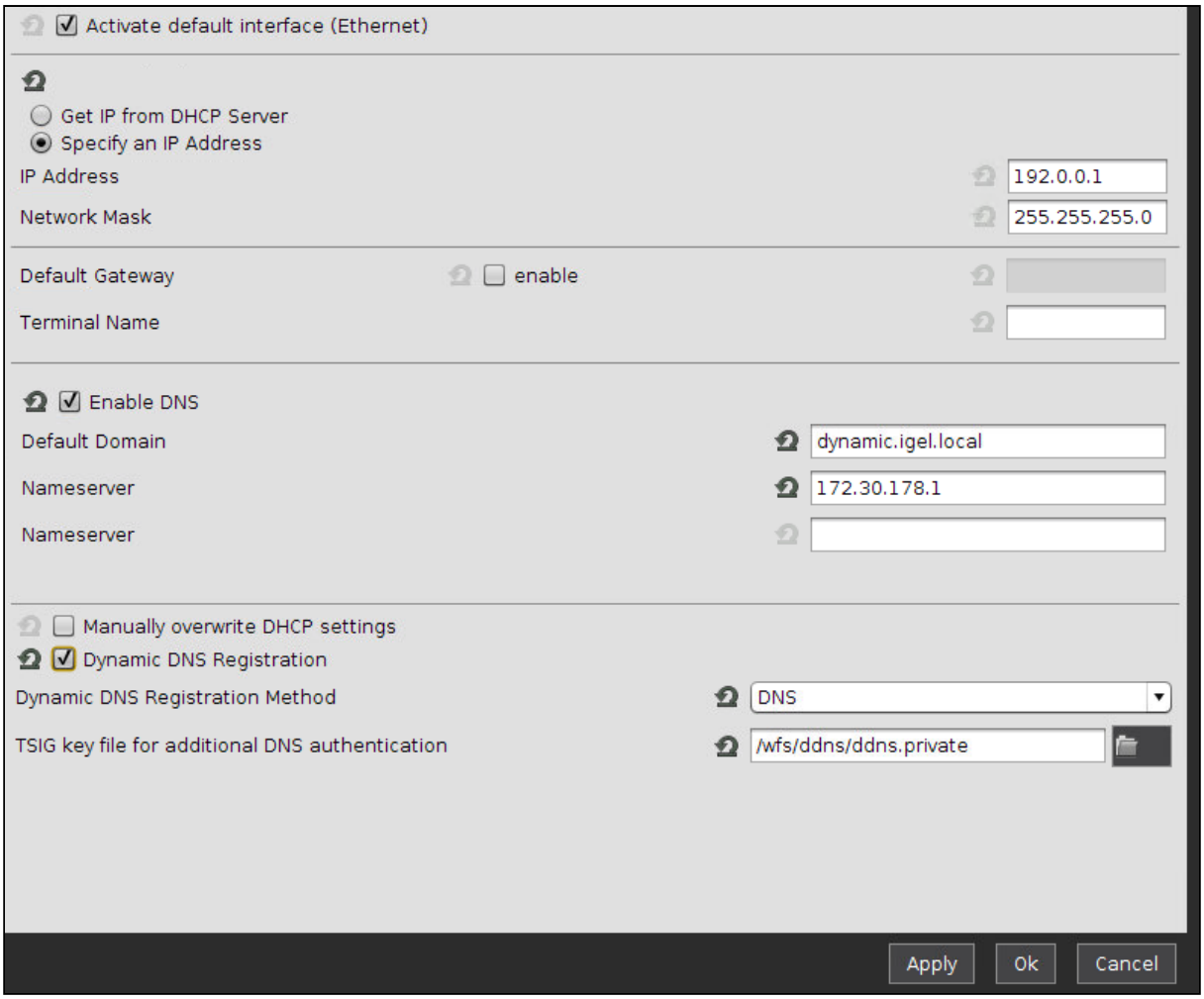
> This only works for BIND9 or other nameservers supporting TSIG, not for Microsoft Active Directory servers.

Distribute your nameserver's shared TSIG key with the UMS:

1. Create a **New File**.
2. Set the **Device Storage Path** to `/wfs/ddns`.
3. Enable **Read** permission for the **Owner** and disable all other permissions.
4. Set the **Owner** to **Root**.

Set up Dynamic DNS Registration:

1. Go to **Network > LAN Interfaces** in *Setup*.
2. Enable **Specify an IP Address.**
3. Enter an **IP Address** and **Network Mask**.
4. Enter a **Terminal Name**.
5. Check **Enable DNS**.
6. Enter a **Default Domain**.
7. Enter at least one **Nameserver** IP address.
8. Enable **Dynamic DNS Registration**.
9. Select **DNS** as **Dynamic DNS Registration Method**.
10. If the nameserver expects a TSIG key: Select the **TSIG key file.**
    Otherwise, leave the input field blank.
11. Click **Apply** or **OK** to confirm your settings.


Activate default interface (Ethernet)
Get IP from DHCP Server
Specify an IP Address
IP Address
192.0.0.1
Network Mask
255.255.255.0
Default Gateway
enable
Terminal Name
Enable DNS
Default Domain
dynamic.igel.local
Nameserver
172.30.178.1
Nameserver
Manually overwrite DHCP settings
Dynamic DNS Registration
Dynamic DNS Registration Method
DNS
TSIG key file for additional DNS authentication
/wfs/ddns/ddns.private
Apply
Ok
Cancel

How to Improve WiFi Connectivity

Problem

Your WiFi connection is unstable, or weak, or both.

Environment

- UDC with IGEL Linux v5??? or IGEL OS??? or higher???
- UD Pocket IGEL Linux v5??? or IGEL OS??? or higher???

Possible Causes and Solutions

There are many circumstances and parameters which influence the quality of a device's WiFi connection. To find a suitable solution to your problem, check out the following collection of possible causes and suggested solutions, workarounds and hints for debugging.

Several Access Points (APs) Are Using the Same Channel

If more than one Access Points visible to the thin client are using the same WiFi channel, interference issues may arise.

->Reconfigure the Access Point (AP) in question to use different channels.

Roaming within One Network (Same SSID)

When the device is configured to roam within its network, it tries to make sure that it is using the strongest/nearest Access Point (AP) within its network. Dependent on the given situation, it might be feasible to disable or to optimize roaming.

See also How to Configure Wi-Fi Network Roaming (see page 608).

Avoid Roaming

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > lock_initial** (Registry key: `network.interfaces.wirelesslan.device0.lock_initial`) and activate **Avoid roaming within the same network**.

> If roaming is deactivated, **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module** should be set to **none**.

Select the Access Point with the Best Signal

With the following setting, the thin client selects the Access Point that emits the best signal when the device starts up.

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bssid** (Registry key: `network.interfaces.wirelesslan.device0.bssid`) and enter `bestsignal` in the **BSSID** field.

Automatic Roaming

Automatic roaming is feasible if the device is moved around frequently, and several Access Points are available.

In the following example, the device is configured to start scanning for another Access Point 10 seconds after the signal of the current Access Point has dropped below -78 db, while a routine scan is executed every 60 seconds, :

1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module`) and select **simple**.
2. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > long_interval** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.long_interval`) to 60.
3. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > short_interval** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.short_interval`) to 10.
4. Set **System > Registry > network > interfaces > wirelesslan > device0 > bgscan > module > simple > signal_strength** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.signal_strength`) to -78.

40 MHz Bandwidth in the 2.4 GHz Band

With some Access Points, it may be feasible to disable the 40 MHz bandwidth in the 2.4 GHz band.

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > driver > cfg80211 > cfg80211_disable_40mhz_24ghz** (Registry key: `network.interfaces.wirelesslan.device0.driver.cfg80211.cfg80211_disable_40mhz_24ghz`) and deactivate **Disable 40 MHz channel bandwidth in 2.4 GHz band**.

High Throughput Option

In some environments, the high throughput functionality built into the driver may not produce optimal results. You can disable this functionality and check if the connection has improved.

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > driver > disable_ht** (Registry key: `network.interfaces.wirelesslan.device0.driver.disable_ht`) and deactivate **Disable HT**.

2.4 GHz Band Only

In some environments, it might be better to use only the 2.4 GHz band.

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > band** (Registry key: `network.interfaces.wirelesslan.device0.band`) and select **2.4 GHz**.

If one or more alternative WiFi networks (SSIDs) are configured, do the following for each alternative SSID:

->In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > alt_ssid[number] > band** (Registry key: `network.interfaces.wirelesslan.device0.alt_ssid[number].band`) and select **2.4 GHz**.

Frame Aggregation

It might be helpful to disable the frame aggregation feature of IEEE 802.11n.

->Disable frame aggregation on your Access Point (AP).

> On your Access Point, this feature may have a different name.
> Also note that IGEL cannot give a guarantee that the Access Point will function properly after the suggested configuration changes.

WiFi Driver Scans And Selects Access Point

By default, the WPA supplicant initiates scanning and the selection of an Access Point. You can change this behavior and assign this task to the driver.

1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > wpa > ap_scan** (Registry key: `network.interfaces.wirelesslan.device0.wpa.ap_scan`) and select **WLAN driver initiates scanning and AP selection**.
2. Restart the thin client.

Whitelist of BSSIDs

You can restrict the number of Access Points to be scanned by creating a whitelist. This whitelist contains only the BSSIDs of those Access Points that the device should scan.

In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > bssid_whitelist** (Registry key: `network.interfaces.wirelesslan.device0.bssid_whitelist`) and enter the BSSIDs of those Access Points that should be scanned, separated by whitespaces.

Debugging

If none of the methods described above work, you can create a log file and send it to the IGEL Support Team.

1. In the Setup, go to **System > Registry > network > interfaces > wirelesslan > device0 > wpa > debug** (Registry key: `network.interfaces.wirelesslan.deviceo.wpa.debug`) and select **very verbose**.
2. Restart the thin client.

3. Send the file `/tmp/wpa_debug.all` to the IGEL Support Team.

Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates

This document describes how to use UMS to configure Wi-Fi connections on IGEL OS with WPA Enterprise / WPA2 Enterprise and TLS client certificates.

There are two options for supplying client certificates and keys to devices:

Via SCEP (NDES)

SCEP allows the automatic provisioning of client certificates via an SCEP server and a certification authority (CA).

Learn how to configure it, using How-To Certificate Enrollment and Renewal with SCEP (NDES) (see page 745).

Via Files Served from UMS

You need:

- a client certificate in PEM (base64) format
- a client private key (needs to be passphrase-protected) in PEM (base64) format

Alternatively,

- a PKCS#12 file containing both client certificate and private key (needs to be passphrase-protected).

> In both cases, SCEP and files from UMS, the device needs to have a working Ethernet or Wi-Fi connection to the SCEP server or the UMS first, so that it can fetch the necessary certificates before it can connect to the target Wi-Fi.

- How to Deploy Client Certificates and Keys (see page 619)
- How to Configure the Network Interface (see page 620)

How to Deploy Client Certificates and Keys

To deploy client certificates and keys via UMS, follow these steps for the client certificate and client private key files (or the PKCS#12 files containing both):

1. In the **UMS Console** navigation tree, right-click **Files** and select **New file** from the context menu. The **New file** dialog opens.
2. Under **File source**, use the file chooser to choose the file as the **Local file**.
3. Under **File target**, leave the classification as **Undefined**.
4. Set the **Thin Client file location** to `/wfs/wpa-tls/`
5. Under **Access rights**, set check **Read** and **Write** for the **Owner** and none for **Others**.
6. Set the **Owner** to **Root**.
7. Click **OK** to upload the file.
8. Drag the file icon onto a thin client or thin client directory in order to assign the file.

How to Configure the Network Interface

This describes how to configure the Wi-Fi interface.

> In both cases, SCEP and files from UMS, the device needs to have a working Ethernet or Wi-Fi connection to the SCEP server or the UMS first, so that it can fetch the necessary certificates before it can connect to the target Wi-Fi.

Using SCEP (NDES)

1. In Setup go to **Network > LAN Interfaces > Wireless**.
2. Check **Activate Wireless Interface**.
3. Go to **Default WiFi-network**.
4. Select **Enable WPA Encryption**.
5. Enter the **Wireless Network Name (SSID)**.
6. Select **WPA Enterprise** or **WPA2 Enterprise** according to your preferences.
7. Set **EAP Type** to **TLS**
   or set **EAP Type** to **PEAP** and **Auth Method** to **TLS**.

   > IGEL OS supports both EAP-TLS and PEAP-EAP-TLS. Choose one that is supported by your infrastructure.

8. Leave **Validate Server Certificate** enabled.
9. Enter the path to a **CA Root Certificate** if you use a CA other than those supported by IGEL OS (see page 764).
10. Check **Manage Certificates with SCEP (NDES)**.
11. Click **Save**.

Using Certificate and Key Files

1. In Setup go to **Network > LAN Interfaces > Wireless**.
2. Check **Activate Wireless Interface**.
3. Go to **Default Wi-Fi network**.
4. Select **Enable WPA Encryption**.
5. Enter the **Wireless Network Name (SSID)**.
6. Select **WPA Enterprise** or **WPA2 Enterprise** according to your preferences.
7. Set **EAP Type** to **TLS**
   or set **EAP Type** to **PEAP** and **Auth Method** to **TLS**

   > IGEL OS supports both EAP-TLS and PEAP-EAP-TLS. Choose one that is supported by your infrastructure.

8. Leave **Validate Server Certificate** enabled. Enter the path to a **CA Root Certificate** if you use a CA other than those supported by IGEL OS (see page 764).
9. Enter the path to the **Client Certificate** file in PEM (base64) format, e.g. `/wfs/wpa-tls/client.crt`.
   Leave this field blank if you use a PKCS#12 file containing both certificate and private key.
10. Enter the path to the **Private Key** file in PEM (base64) format.
    If you use a PKCS#12 file containing both certificate and private key, enter its path here.
11. Specify the **Identity** to be used if your key/certificate contains more than one entry.
12. Enter the **Private Key Password**.
13. Click **Save**.

How to Prevent Permanent Storage of Wireless Network Keys

This document describes how to prevent users from storing wireless network keys/passwords for **Wireless Manager** on the endpoint device.

1. In Setup, go to **System > Registry**.
2. Go to the `network.applet.wireless.allow_storing_credentials` parameter.
3. Uncheck **Allow permanently storing credentials**, which is checked by default.
4. Click **Apply**.

This will affect the **Wireless Manager** dialogs for wireless networks with the network authentication methods in their variants requiring passwords:

- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

In particular, users will not have check boxes labeled **Permanently store identity and password** or **Permanently store network key** available.

Extended Logging With Syslog, Tcpdump and Netlog

The IGEL OS **Registry** offers a number of extended logging options that can help customers, Support and PreSales debug system and network issues.

For instructions on how to send log files to the IGEL support team via the UMS, see Sending Device Log Files to IGEL Support (see page 1152).

- Debuglog Partition (see page 624)
- Syslog (see page 626)
- Tcpdump (see page 627)
- Netlog (see page 630)

Debuglog Partition

Logfiles can get very large quite fast. This is why they are stored in a separate partition. It is mounted at `/debuglog`.

Enabling and Configuring the Debuglog Partition

The partition is enabled and configured in the **Registry**:

	IGEL Setup > System > Registry		
	> Enable debuglog partition	debug.tools.log_partition.enabled	enabled / disabled
	Enables the debuglog partition.		

	IGEL Setup > System > Registry		
	> Size of debuglog partition in MiB	debug.tools.log_partition_size	50 ... 500 / 100

Resizing the debuglog partition will delete its contents!

Debuglog Partition Contents

Depending on which logging options you enable (see the following topics), you may find the following files in the debuglog partition:

- Syslog
  - `messages` (the current syslog)
  - `messages[1-9].gz` (compressed and rotated syslog)
- Ethtool
  - `netlog-ethtool-[device].log`
- Ping
  - `netlog-host-[0-9]-ping.log` (ping log)
  - `netlog-host-[0-9]-ping[n].log.gz` (compressed and rotated ping log)
- Ifconfig
  - `netlog-ifconfig-[device].log`
- Netstat
  - `netlog-netstat.log` (netstat log)

    - `netlog-netstat[n].log.gz` (compressed and rotated netstat log)
- Socket Status
    - `netlog-socket_status.log` (socket status log)
    - `netlog-socket_status[n].log.gz` (compressed and rotated socket status log)
- Tcpdump
    - `tcpdump[0-3]_capture_current[n]` (tcpdump capture)
    - `tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (compressed and rotated tcpdump captures)
- Tcpdump triggered by an error
    - `ERROR_[timestamp]/tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (compressed and preserved tcpdump captures)

Syslog

It is possible to send all syslog messages that are written to `/var/log/message` (IGEL Linux *version 5.10.250 and versions 5.11.x*) or to the systemd journal (IGEL Linux *version 10.01.100*) to the debuglog partition as well. The logfile will be rotated and compressed as needed. This preserves the log if the thin client crashes, and logs from several previous boots.

Configure it in the **Registry**:

IGEL Setup > System > Registry		
> Enable syslog log to debuglog partition	debug.tools.syslog0.enabled	true/ false
IGEL Setup > System > Registry		
> Number of Rotate Files	debug.tools.syslog0.num_rotate_files	2 ... 9
Number of files to be kept while rotating.		
IGEL Setup > System > Registry		
> Logfile rotate size in MiB	debug.tools.syslog0.rotate_size	2, 4 , 8, 16
Rotate when the size of the compressed file reaches this size in MiB.		

Tcpdump

Tcpdump will help you debug network issues by capturing packets from up to 4 individual network interfaces.

> Using the Netlog (see page 630) facility, it is possible to copy capture files to a subdirectory, triggered by an error in another log, so the captures before and after the error will be preserved for your analysis.

> You can use Wireshark on an external system for analyzing capture files.

Find out more about Tcpdump from its homepage[81].

IGEL Setup > Registry		
> Resolve addresses/ports to names	`debug.tools.tcpdump[0-3].address_resolution`	enabled / disabled
IGEL Setup > Registry		
> Compression Method	`debug.tools.tcpdump[0-3].compression`	lzop, gzip, bzip2, xz
The compression method affects file size as well as system performance while compressing. The default lzop methiod is relatively light on the CPU.		
IGEL Setup > Registry		
> Interface for tcpdump logging	`debug.tools.tcpdump[0-3].interface`	user editable string / eth0
Note: Names `eth0`, `eth1`, `wlan0`, etc. are treated as symbolic names and will internally be replaced by the correct PNINs automatically. For details on PNINs, see LAN Interfaces (see page 1899).		
IGEL Setup > Registry		
> Number of Rotate Files	`debug.tools.tcpdump[0-3].num_rotate_files`	3 ... 10
Number of files to be kept while rotating.		
IGEL Setup > Registry		

81. http://www.tcpdump.org

> Only Log Package Headers	`debug.tools.tcpdump[0-3].only_headers`	enabled / disabled
IGEL Setup > Registry		
> Enable promisc tcpdump logging	`debug.tools.tcpdump[0-3].promisc`	enabled / disabled
Enable promiscuous mode on the network interface to also capture packets not intended for this host.		
IGEL Setup > Registry		
> Logfile rotate size in MiB	`debug.tools.tcpdump[0-3].rotate_size`	10, 15 ,20 ,25 ,30 , 40
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup > Registry		
> Logfile rotate time in s	`debug.tools.tcpdump[0-3].rotate_time`	0 / user editable integer
Time in seconds after which the logfile is rotated and compressed. If set to 0 no time-based rotation happens.		
IGEL Setup > Registry		
> Additional Parameters for tcpdump	`debug.tools.tcpdump[0-3].tcpdump_additional_parameters`	user editable string
Use with care.		
IGEL Setup > Registry		
> Enable tcpdump	`debug.tools.tcpdump[0-3].tcpdump_enabled`	enabled / disabled
IGEL Setup > Registry		
> tcpdump filter expression	`debug.tools.tcpdump[0-3].tcpdump_filter`	user editable string

Tcpdump filter expression. For the expression syntax, see the pcap-filter(7)[82] manpage.

82. http://www.tcpdump.org/manpages/pcap-filter.7.html

Netlog

The netlog facility combines the following network diagnosis tools:

- `ethtool`
- `ifconfig`
- `netstat`
- `ping`
- `ss` (socket status)

It can also trigger `tcpdump`.

IGEL Setup > Registry		
> Enable netlog logging	debug.tools.netlog.enabled	enabled / disabled
IGEL Setup > Registry		
> period between netlog logs in s	debug.tools.netlog.period	1, 5, 10, 20, 30, 60, 120
Ping logging is not affected by this and uses its own timing.		

- Ethtool (see page 631)
- Ifconfig (see page 632)
- Netstat (see page 633)
- Ping (see page 634)
- Socket Status (ss) (see page 636)

Ethtool

Ethtool is the standard Linux utility for getting diagnostic information about wired Ethernet devices and their drivers.

IGEL Setup > Registry		
> Disable ethtool logging	debug.tools.netlog.ethtool.disabled	true / <u>false</u>
By default Ethtool logging is included in Netlog logging. However, you can disable it here.		
IGEL Setup > Registry		
> Log only if ethtool output changes	debug.tools.netlog.ethtool.log_on_changes_only	<u>true</u> / false
Log only if ethtool output changes (on bootup there will always be at least one log entry)		
IGEL Setup > Registry		
> Number of Rotate Files	debug.tools.netlog.ethtool.num_rotate_files	<u>2</u> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines)		
IGEL Setup > Registry		
> Logfile rotate size in MiB	debug.tools.netlog.ethtool.rotate_size	<u>2</u>, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		

Ifconfig

Ifconfig

Apart from configuring network devices, ifconfig also gives diagnostic information such as RX bytes, TX bytes and dropped packets.

IGEL Setup >		
> Disable ifconfig logging	debug.tools.netlog.ifconfig.disabled	true / <u>false</u>
By default Ifconfig logging is included in Netlog logging. However, you can disable it here.		
IGEL Setup >		
> Log only if ifconfig output changes	debug.tools.netlog.ifconfig.log_on_changes_only	no,<u>error_counter</u>,all
• **no**: log on every netlog run • **error_counter**: log only if an error counter or the address changes • **all**: log on every change of ifconfig output		
IGEL Setup >		
> Number of Rotate files	debug.tools.netlog.ifconfig.num_rotate_files	<u>2</u> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.ifconfig.rotate_size	<u>2</u>, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup >		
> Trigger tcpdump log	debug.tools.netlog.ifconfig.trigger_tcpdump_save	true / <u>false</u>
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.		

Netstat

Netstat displays a variety of network statistics for the local machine.

> Disable netstat logging	debug.tools.netlog.netstat.disabled	true / false
By default `netstat -s` logging is included in Netlog logging. However, you can disable it here.		
> Number of Rotate files	debug.tools.netlog.netstat.num_rotate_files	2 ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
>Logfile rotate size in MiB	debug.tools.netlog.netstat.rotate_size	2, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		
>Log only if triggered	debug.tools.netlog.netstat.trigger_log	net_error_changes, net_changes, ifconfig_changes, ethtool_changes, no_trigger

- **net_error_changes**: log if ethtool output changes or ifconfig error counter or address changes
- **net_changes**: log if ethtool or ifconfig output changes
- **ifconfig_changes**: log if ifconfig output changes
- **ethtool_changes**: log if ethtool output changes
- **no_trigger**: log on every netlog run

Ping

IGEL Setup >		
> Enable ping check	debug.tools.netlog.ping_host[0-9].enabled	true / false
IGEL Setup >		
> Log only if ping fails	debug.tools.netlog.ping_host[0-9].log_only_on_error	true / false
Log only if any one of the configures pings [0-9 fails.]		
IGEL Setup >		
> Number of Rotate Files	debug.tools.netlog.ping_host[0-9].num_rotate_files	2 ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.ping_host0.rotate_size	2 ... 4
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup >		
> Trigger tcpdump save	debug.tools.netlog.ping_host0.trigger_tcpdump_save	2 ... 4
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.		
IGEL Setup >		
> Ping target	debug.tools.netlog.ping_host0.ping_target	user-editable string
Target IP/hostname to ping (if none is given ping will be considered as disabled!)		
IGEL Setup >		
> Time between pings	debug.tools.netlog.ping_host0.ping_time	1, 5, 10, 30, 60, 120
Time between pings in seconds.		
IGEL Setup >		

> Type of ping	debug.tools.netlog.ping_host0.type	icmp, http request, https request
• **icmp**: use normal `ping` command • **http request**: send an http request (fails if no `HTTP/*.* * OK` answer is received) • **https request**: send an https request (fails if no `CONNECTED` is returned by openssl)		

Socket Status (ss)

Socket Status (ss)

IGEL Setup >		
> Disable socket status Logging	debug.tools.netlog.socket_status.disabled	true / <u>false</u>
By default socket_status logging is included in Netlog logging. However, you can disable it here.		
IGEL Setup >		
> Number of Rotate Files	debug.tools.netlog.socket_status.num_rotate_files	true / <u>false</u>
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines)		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.socket_status.rotate_size	true / <u>false</u>
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup >		
> Log only if triggered	debug.tools.netlog.socket_status.trigger_log	<u>ping_errors</u>, no_trigger
• **ping_errors**: log only if ping test fails • **no_trigger**: log on every netlog run		

How to Run the OpenVPN Client with a Preconfigured Configuration File

> **Solution Based on Experience from the Field**
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

This article describes a basic solution for getting the built-in OpenVPN client running with a preconfigured configuration file. This is an alternative to using the Setup for configuration.

Environment

This article is valid for the following environment:

- IGEL OS 10 or higher
- OpenVPN server

Setting up an OpenVPN Connection with a Preconfigured Configuration File

1. In the UMS Console, open the context menu on **Files** and select **New File**.
2. Select your `.ovpn` file in the file system.
3. In the **File target** section, under **Devices file location**, enter "/wfs/".
4. Click **Ok**.
   The file is uploaded to the UMS.
5. Assign the file object to your device by clicking the "+" symbol in the **Assigned objects** area (upper right).
6. Create a profile with a suitable name, e. g. "OpenVPN Connection".
7. In the profile, go to **System > Firmware Customization > Custom Commands > Network**.
8. In the **Final network command** field, enter the following code, replacing `example.ovpn` with the correct filename:

```
while :; do if [ -z $(pgrep openvpn) ]; then echo "openvpn is not running";
openvpn --config /wfs/example.ovpn --auth-user-pass <(echo -e $(zenity --forms
--text="Enter your VPN credentials" --add-entry=Username --add-
password=Password --title=OpenVPN) | sed 's/|/\n/'); else echo "openvpn is
running"; fi; sleep 1; done &
```

9. Click **Save** to save the profile.
10. Assign the profile to your device by clicking the "+" symbol in the **Assigned objects** area.
11. Reboot the device.
    After reboot, you should see a login window for OpenVPN.
12. Enter your OpenVPN credentials.
    If the login was successful, a **Network connecting** popup appears briefly. No other indicator is

shown. You can disconnect only by rebooting the device.
If the login has failed, the login window reappears.

Removing the OpenVPN Connection

->To remove the OpenVPN connection from the settings, unassign the profile from the device and reboot it.

How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden

Problem

The taskbar or system tray has been disabled for some reason (**User Interface > Desktop** > **Taskbar** / **Taskbar Items**; also **User Interface > Screenlock /Screensaver > Taskbar**). As a result, a systray icon for the Wireless Manager (see page 1910) can't be accessed anymore, and the user can't manage wireless networks.

⚠ Notice that also the Wi-Fi switch will be inaccessible if you disable the taskbar or system tray, see Switch for the Wi-Fi Connection (see page 1912). See also "Enable Wi-Fi automatic switch" under Wireless (see page 1907).

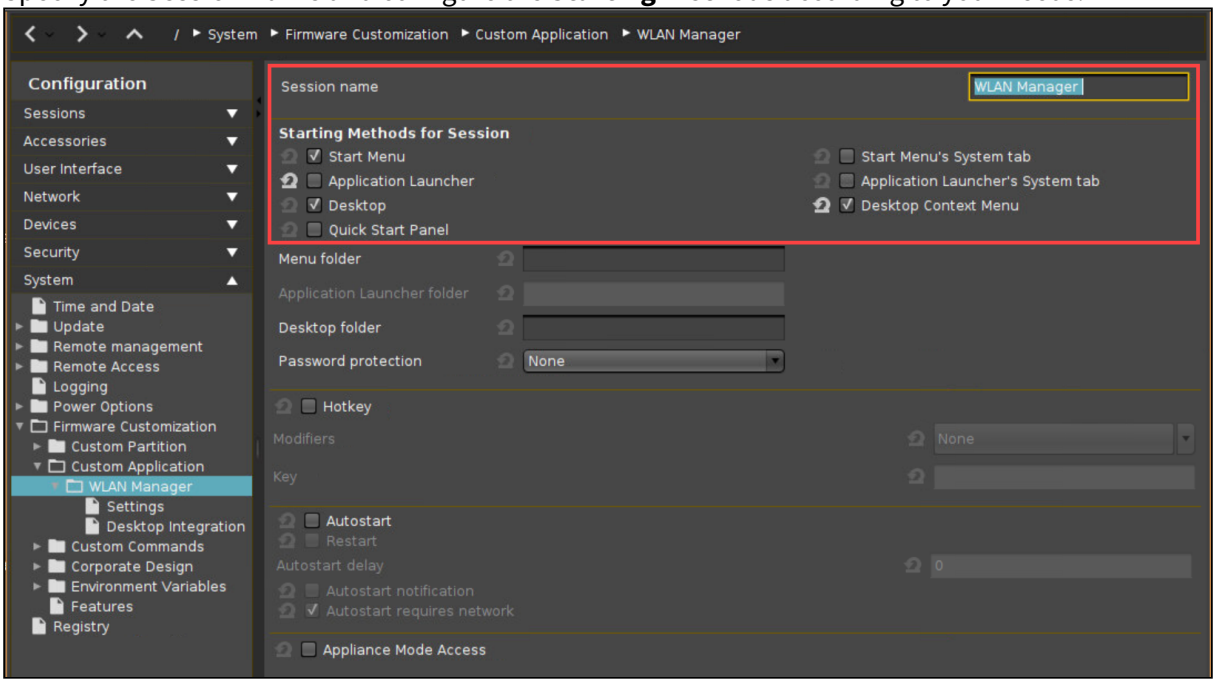
Environment

- IGEL OS 10.06 or higher

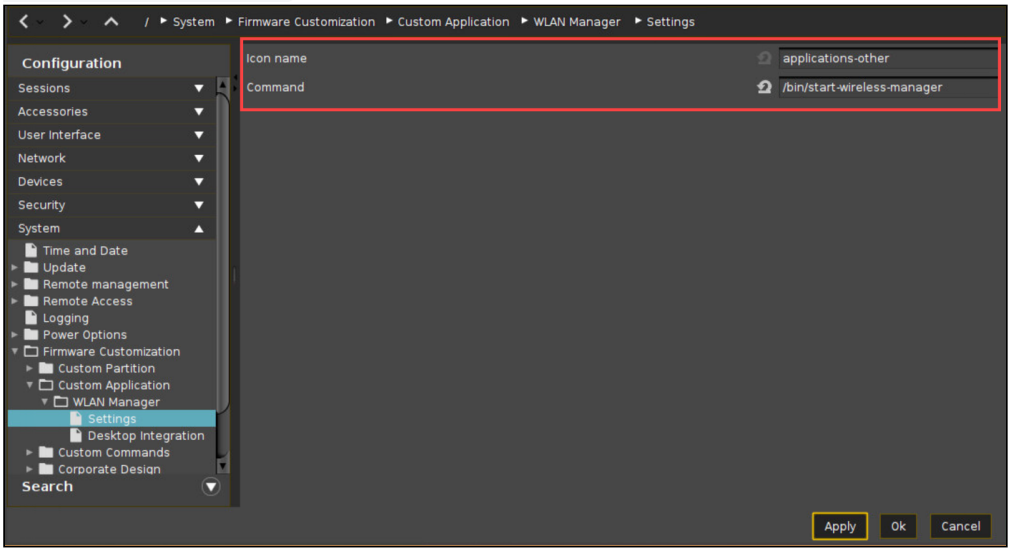
Solution

You can configure the Wireless Manager as a custom application and define the way it can be launched.

1. Go to **Network > LAN Interfaces > Wireless** and check that the wireless interface and the Wireless Manager are enabled.
2. Go to **System > Firmware Customization > Custom Application** and click ＋.
3. Specify the **Session name** and configure the **Starting methods** according to your needs.



4. Under **Settings**, specify the **Icon name** and enter the following **Command**: `/bin/start-wireless-manager`



5. Click **Apply** or **OK**.
   The Wireless Manager can now be launched via the configured starting methods.

How to Configure Open VPN Sessions

This document describes how to configure the *OpenVPN* Client on *IGEL Linux*.

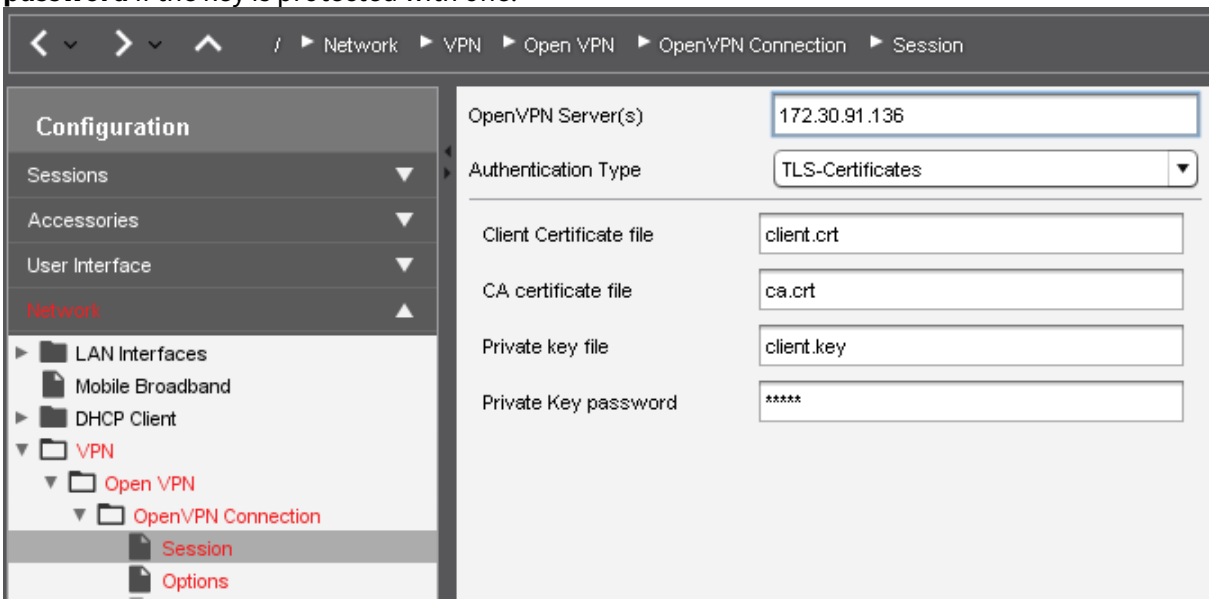
Prerequisites

- A configured and running *OpenVPN* 2.x server
- Information about the *OpenVPN* server configuration (e.g. authentication method)
- A thin client with *IGEL Linux* 10.01.100 or newer
- The certificate and private key files for the client, along with the root certificate of the CA that signed the client and server certificates.
- Optionally, a Smartcard or eToken supported by *IGEL Linux*.
  To learn how to distribute keys and certificates to the thin clients, refer to the How-To document "Securely Distributing Keys and Certificates (see page 652)".

- Authenticating with TLS Certificates (see page 642)
- Authenticating with Name/Password (see page 643)
- Authenticating with Name/Password with TLS Certificates (see page 644)
- Authenticating with Static Key (see page 645)
- Options and TLS Options (see page 646)
- DNS and Routing Options (see page 647)
- Proxy (see page 648)
- How to Check the VPN Connection (see page 649)
- How to Start Automatically the VPN During Boot (see page 650)
- Further Information about OpenVPN (see page 651)
- Securely Distributing Keys and Certificates for OpenVPN (see page 652)

Authenticating with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **TLS-Certificates** as the **Authentication Type.**
4. Select the client certificate as the **Client Certificate file**.
5. Select the root certficate of the CA as the **Certificate Authority (CA) file** .
6. Select the client's private key as the **Private Key file**. Enter the passphrase in **Private Key password** if the key is protected with one.

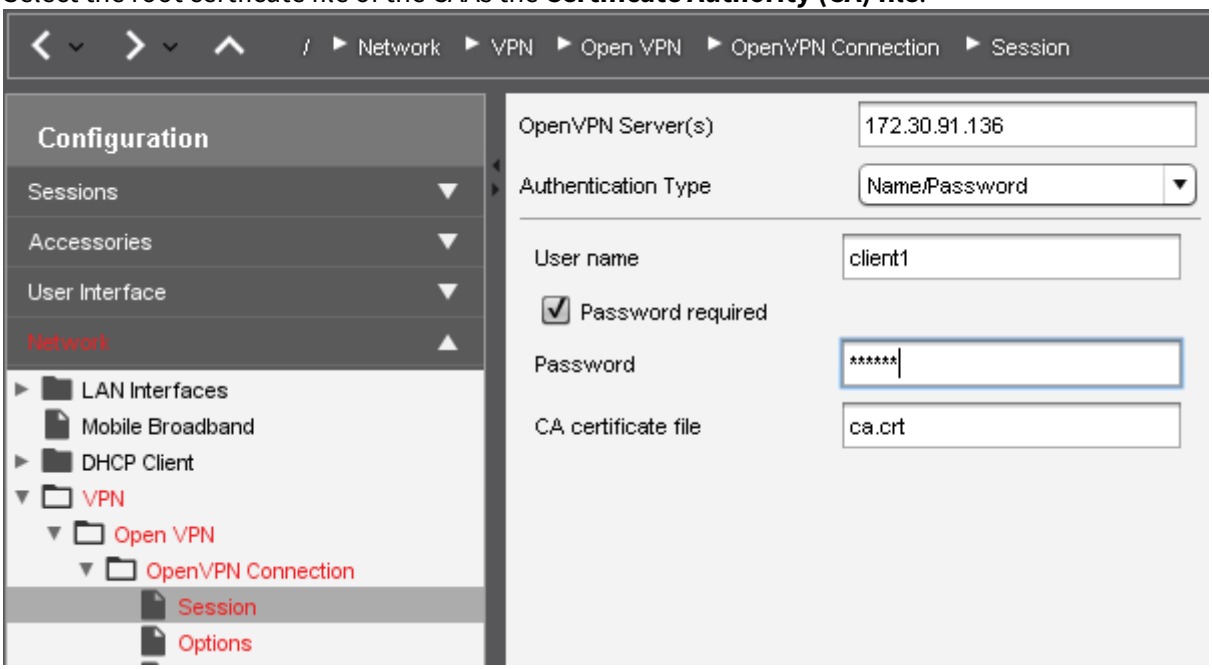


7. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

> If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

Authenticating with Name/Password

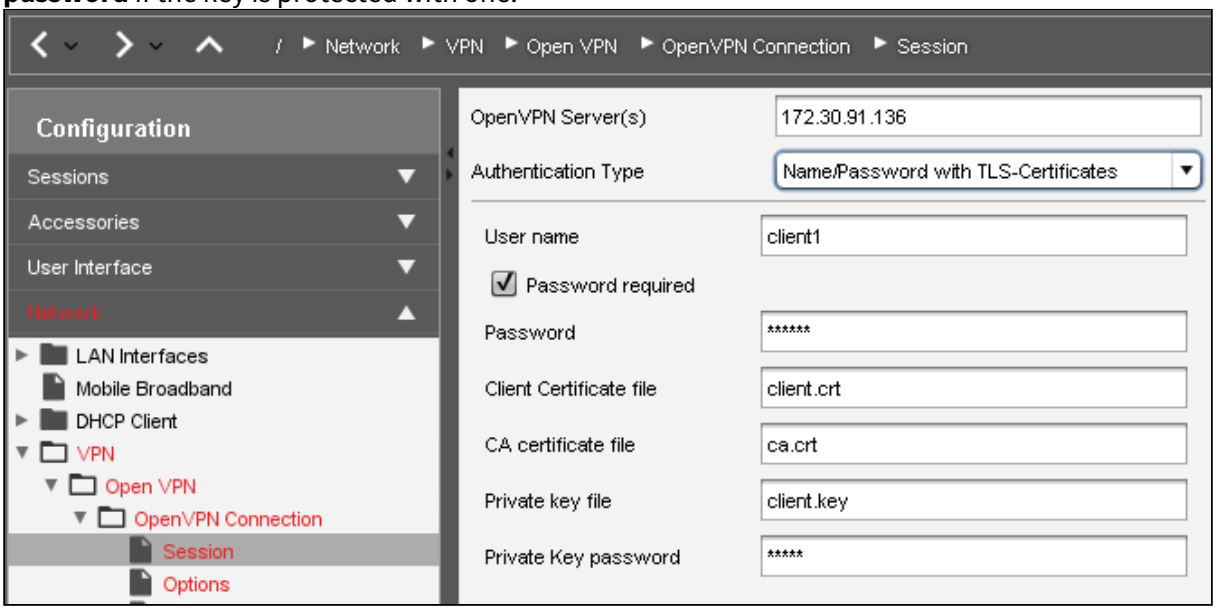
1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password** as the **Authentication Type.**
4. Enter the **Username.** If you leave this field blank the user will be prompted for the Username when connecting.
5. Check **Password required.**
6. Enter the **Password.** If you leave this field blank the user will be prompted for the password when connecting.
7. Select the root certficate file of the CAAs the **Certificate Authority (CA) file**.



8. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

Authenticating with Name/Password with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password with TLS-Certificates** as the **Authentication Type**.
4. Enter the **Username.** If you leave this field blank the user will be prompted for the username when connecting.
5. Check **Password required.**
6. Enter the **Password.** If you leave this field blank the user will be prompted for the password when connecting.
7. Select the client certificate as the **Client Certificate file**.
8. Select the root certficate of the CA as the **Certificate Authority (CA) file**.
9. Select the client's private key as the **Private Keyfile**. Enter the passphrase in **Private Key password** if the key is protected with one.

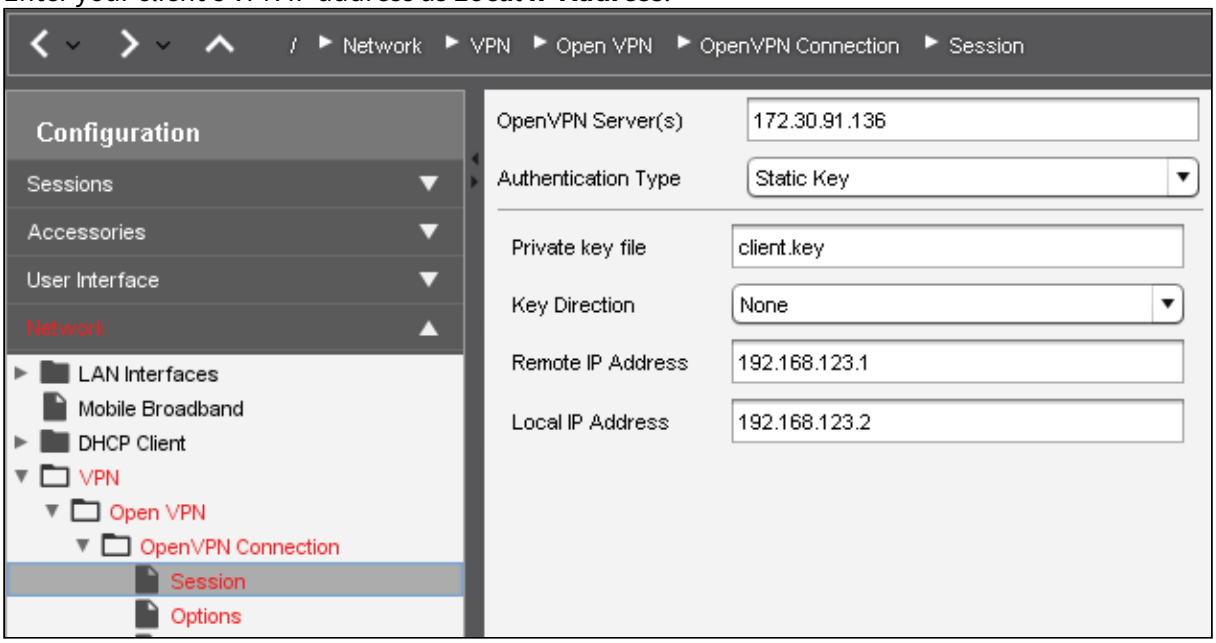


10. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

> If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

Authenticating with Static Key

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Static Key** as the **Authentication Type**.
4. Select the static key file as the **Private Key**.
5. Select **None** as the **Key Direction**.
6. Enter the server's VPN IP address as **Remote IP Address**.
7. Enter your client's VPN IP address as **Local IP Address**.



8. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

Options and TLS Options

Options

Under **Network > VPN > OpenVPN > [Session Name] > Options**, you can set various options for the OpenVPN client. Usually, you can leave the default settings as they are. If the server uses compression, enable **Use LZO data compression**.

If establishing a tunnel fails, try again with **Use LZO data compression** enabled.

The **--comp-lzo** option is considered deprecated from OpenVPN v2.4 and should not be used any more. For more information, see https://community.openvpn.net/openvpn/wiki/DeprecatedOptions#Option:--comp-lzoStatus:Pendingremoval.

When using a proxy, set **Protocol used for communication to the host** to **tcp-client**.

TLS Options

Under **Network > VPN > OpenVPN > [Session Name] > TLS-Options**, you can set various TLS-related options. In particular, you can configure whether the **remote peer certificate** will be verified.
For details about these settings, refer to How to Configure Open VPN Sessions (see page 641) or OpenVPN (see page 1930).

DNS and Routing Options

By default, OpenVPN automatically uses the server's settings for DNS and routing.

If you want to change these settings, go to **Network > VPN > Open VPN > [Session Name] > IPv4**. Here you can:

- Deactivate **Automatic DNS**
- Add **Extra nameserver(s)**
- Add **Extra search domains**
- Deactivate **Automatic Routes**
- Deactivate **VPN is the default route**

Additionally, you can enable three custom routes in **Network > VPN > Open VPN > [Session Name] > Route [0,1,2].** For each enabled route you can configure:

- whether it is a **Network Route** or a **Host Route**
- **Network/Host IP**
- **Network Mask** (for Network Route only)
- Optional: **Gateway**
- Optional: **Metric** (a quality rating used for routing decisions, 0 being the best)

Proxy

If you wish to configure a proxy for your VPN connection, go to **Network > VPN > OpenVPN > [Session Name] > Proxy.** Here you can configure:

- **Proxy Type**: **SOCKS** or **HTTP**, by default this is set to **None**
- **Proxy Address** and **Proxy Port**
- **Retry indefinitely when errors occur**

If you select the **HTTP** proxy type you can configure:

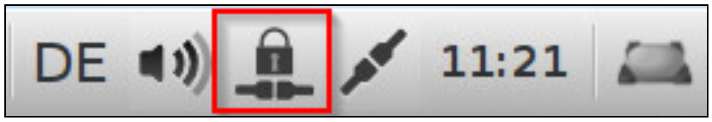
- **Proxy Username**
- **Proxy Password**

> When using a proxy, set **Options > Protocol used for communication to the host** to **tcp-client**.

> When experiencing issues with OpenVPN, read the messages in `/var/log/messages`, e.g. using the **System Log Viewer**.

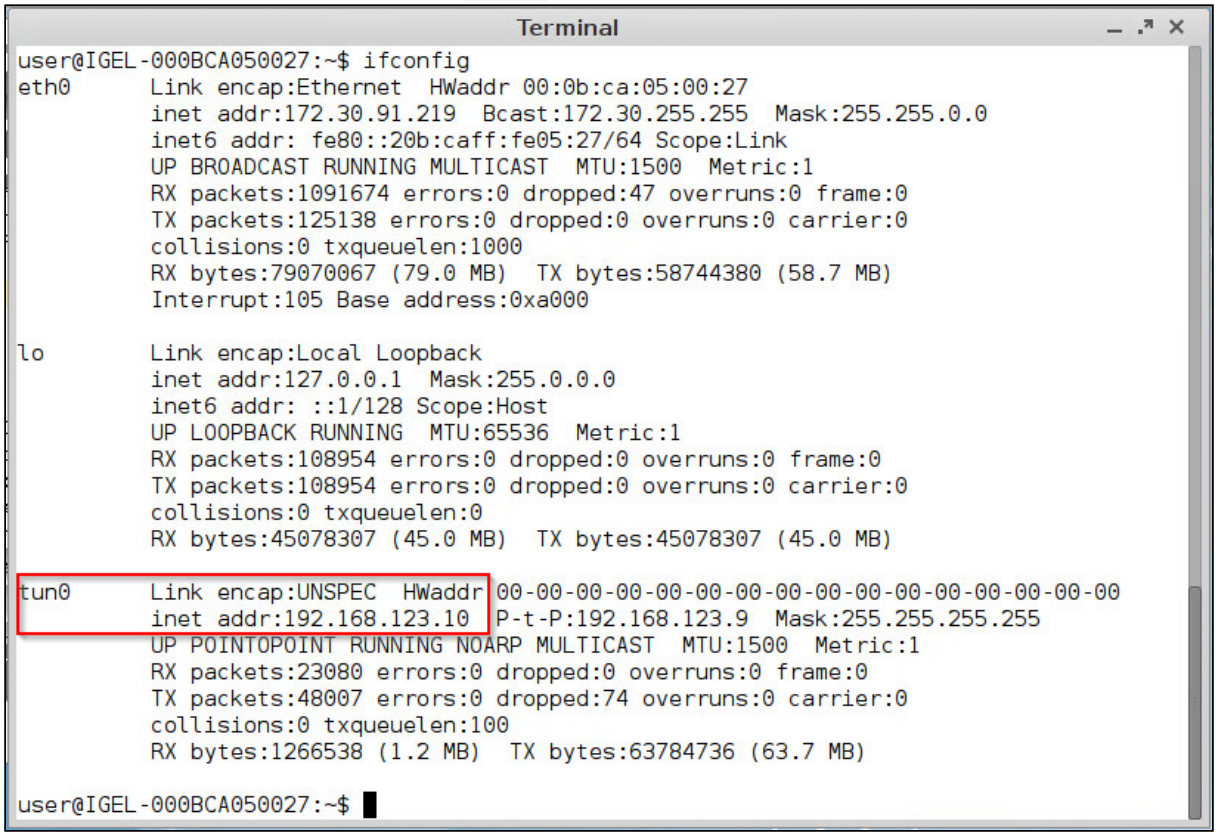
How to Check the VPN Connection

As soon as a VPN connection is established, a lock icon with connected plugs is shown in the panel:



However, this only serves as an indicator. To be sure that the VPN connection really exists:

1. Open a **Local Terminal.**
2. Run the command `ifconfig.`
3. Check whether the output contains a `tun` device with an IP address from the private network.



4. Additionally, check whether you can ping the VPN server's private IP address.

How to Start Automatically the VPN During Boot

If you want to update the firmware via the VPN, you need to enable **Autostart During Boot**. Enabling Autostart of the control application in **Network > VPN > OpenVPN > [session name]** is not adequate!

1. Go to **Network > VPN > OpenVPN.**
2. Check **Enable Autostart During Boot.**
3. Select one of the configured sessions.
4. Click **Set Auto.**
   The session will be marked in the **Auto** column**.**
   Click **Set Auto** again to dectivate autostarting the session.

   The system will prompt you for key pass phrases or the eToken/smartcard PIN if necessary.

Further Information about OpenVPN

Further information about *OpenVPN* can be found in

- the OpenVPN how-to[83] and
- the OpenVPN manual page[84]

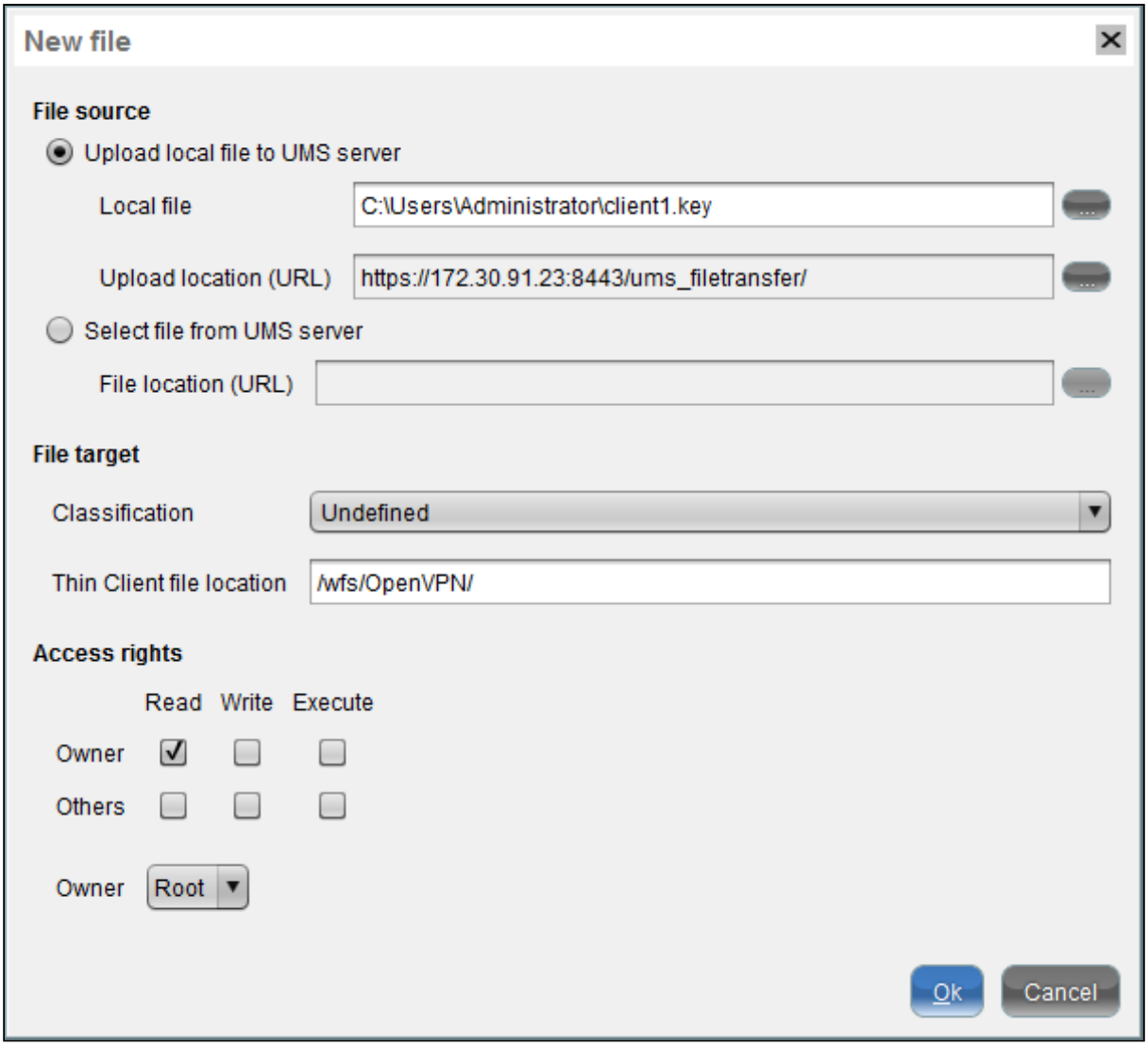
maintained by the *OpenVPN* project.

83. https://openvpn.net/index.php/open-source/documentation/howto.html
84. https://openvpn.net/community-resources/reference-manual-for-openvpn-2-0/

Securely Distributing Keys and Certificates for OpenVPN

Use the file distribution mechanism in the *Universal Management Suite (UMS)* to securely distribute keys and certificates to the thin clients:

1. Select **Undefined** as the **Classification.**
2. Enter `/wfs/OpenVPN/` as **the thin client file location.**
3. Enable the **Read** permission for the **Owner** exclusively, and uncheck all remaining permissions.
4. Select **Root** as the **Owner.**



How to Connect to a Wi-Fi Network with Hidden SSID

Symptom

The device does not connect to a wireless network with hidden SSID.

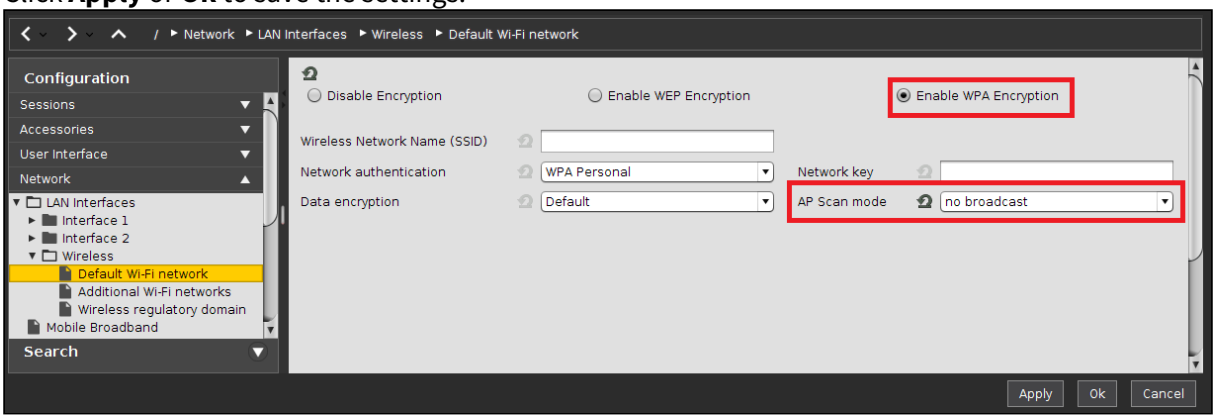
Problem

An option in the device's network configuration is missing.

Solution

If you need to configure a hidden access point, proceed as follows:

1. Start IGEL Setup or open the device configuration dialog in the UMS.
2. Go to **Network > LAN Interfaces > Wireless > Default Wi-Fi network** (or **Additional Wi-Fi networks** depending on your configuration).
3. Choose **Enable WPA Encryption**.
4. Set parameter **AP Scan mode** to "**no broadcast**".
5. Click **Apply** or **Ok** to save the settings.



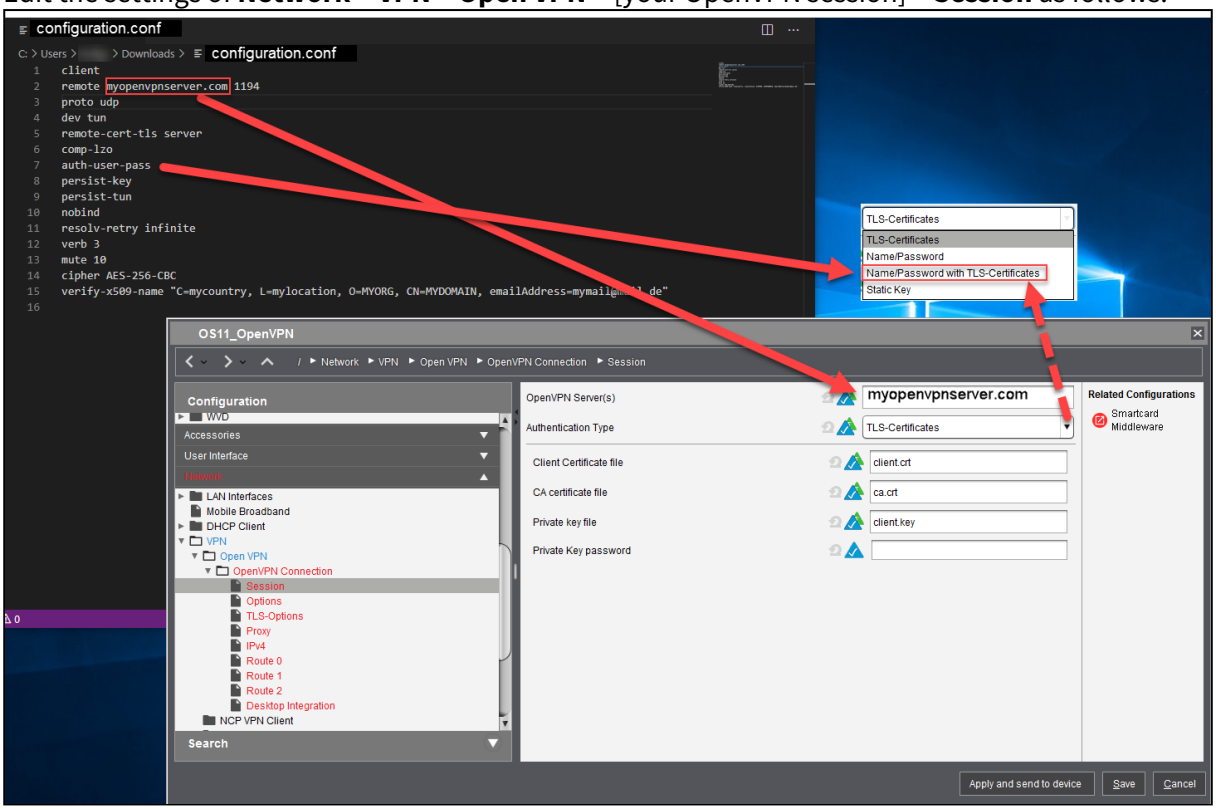
How Can I Configure OpenVPN with an .ovpn or .conf File for IGEL OS Devices?

You can use the `.ovpn` or the `.conf` file from your firewall to configure OpenVPN for your IGEL OS device.

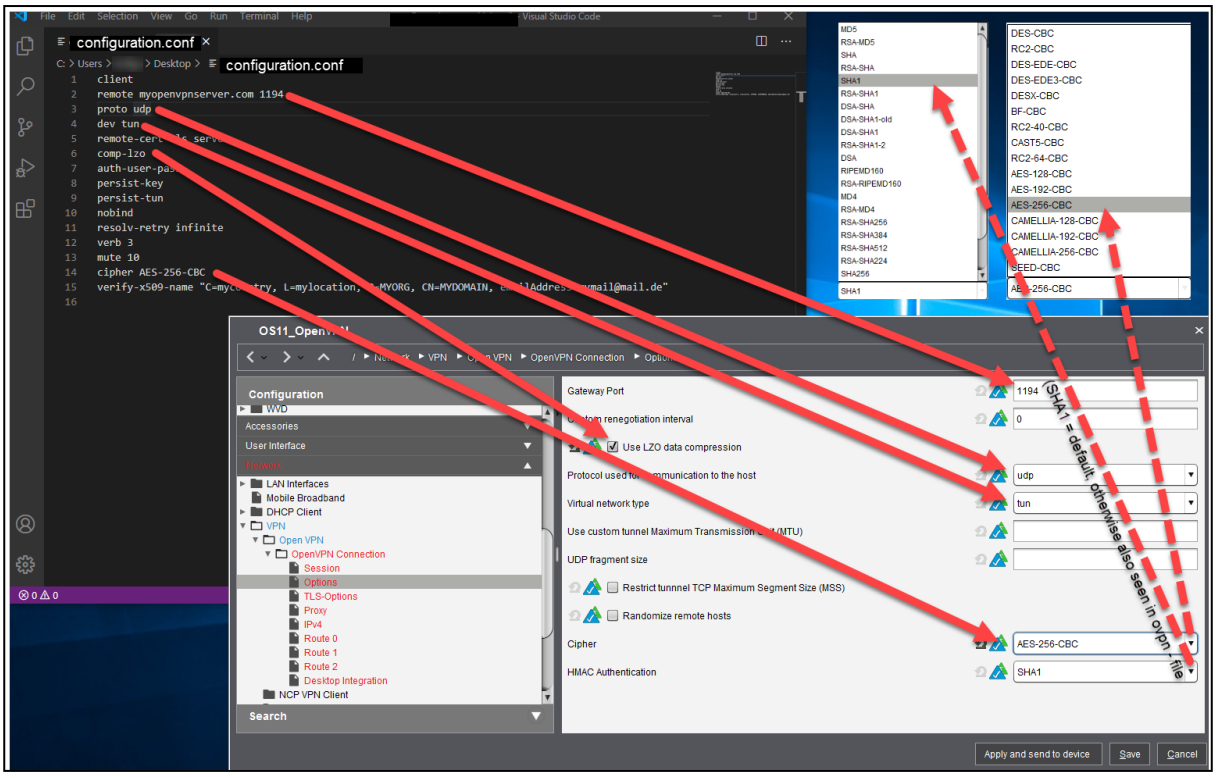
> **Solution Based on Experience from the Field**
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Creating a Profile

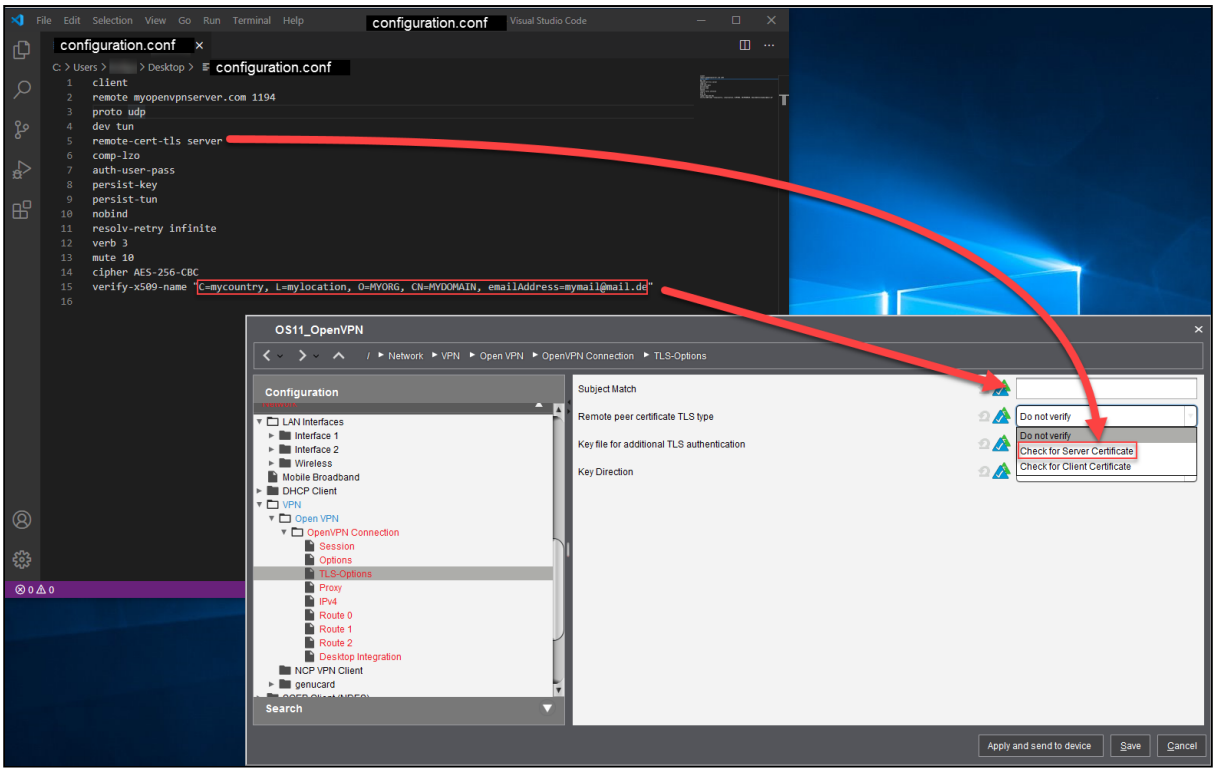
1. Open the `.ovpn` or the `.conf` file in “Microsoft Visual Studio Code” (freeware) or any other editor that can save files in UTF-8 and uses LF (not CR-LF) for a newline.
2. In the UMS, create a profile with an appropriate name, e.g. "OS11_OpenVPN".
3. Go to **Network > VPN > Open VPN** and click + to create an OpenVPN session.
4. Edit the settings of **Network > VPN > Open VPN >** [your OpenVPN session] **> Session** as follows:



5. Go to **Network > VPN > Open VPN >** [your OpenVPN session] **> Options** and edit the settings as follows:



6. Go to **Network > VPN > Open VPN >** [your OpenVPN session] **> TLS Options** and edit the settings as follows:



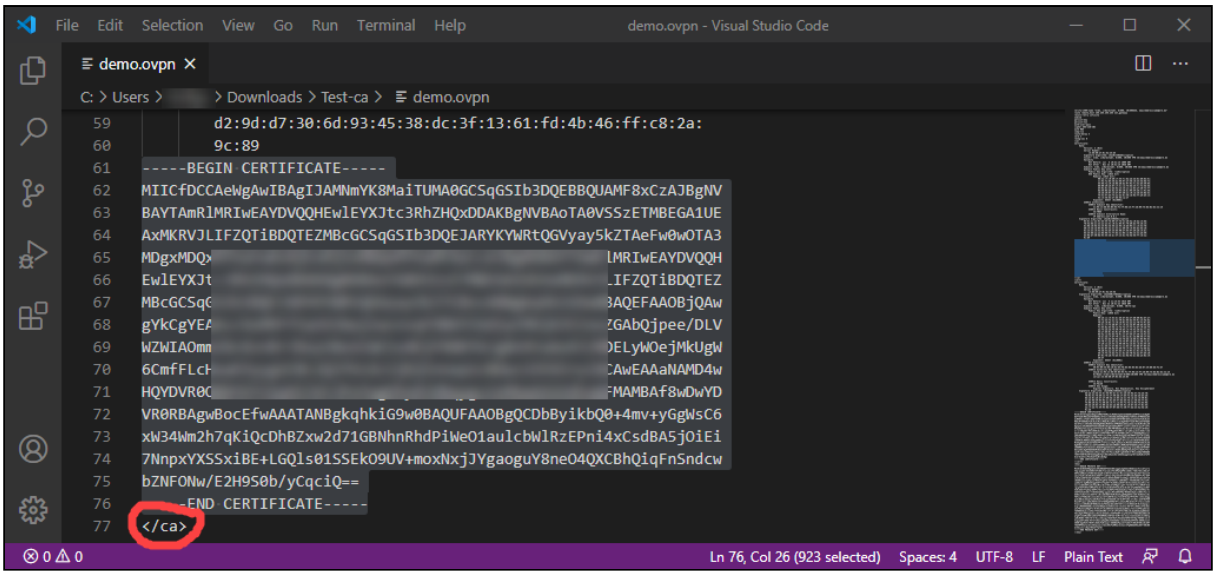
Creating the Certificate/Key Files

If you already have the following files, you can skip this section and jump to Transferring the Files to the UMS (see page 658):

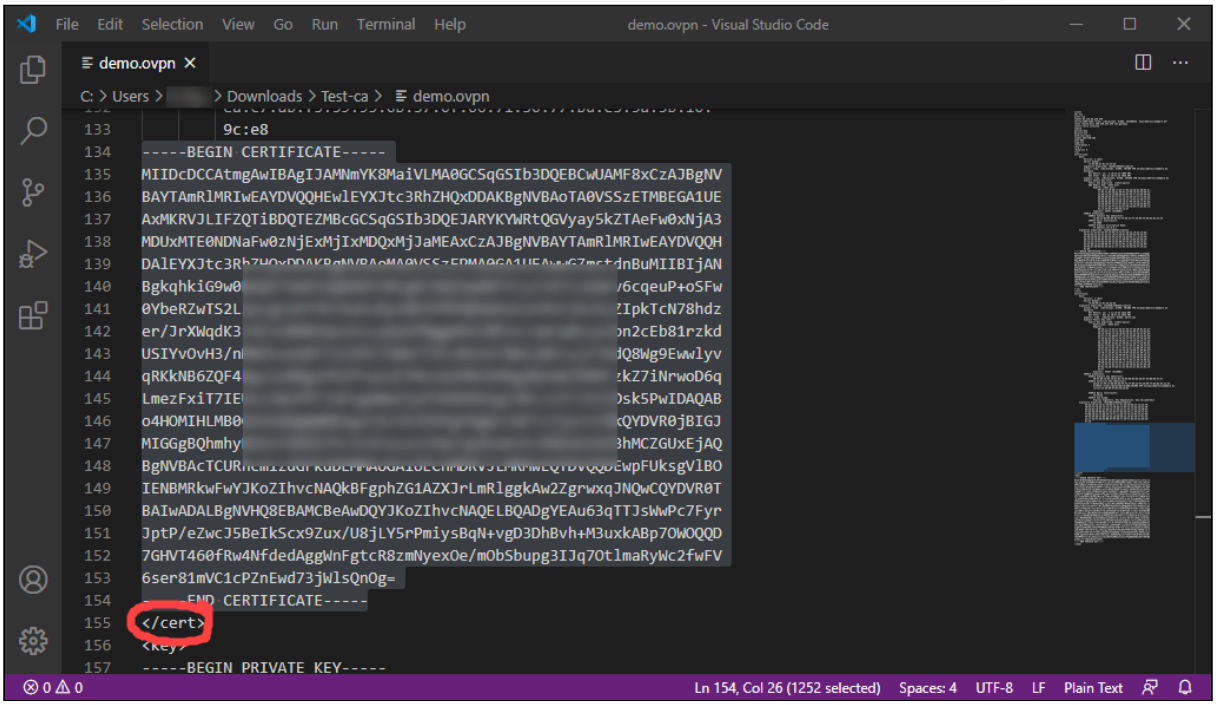
- `ca.crt`
- `client.crt`
- `client.key`

If the certificates and the key are embedded in your `.ovpn` file, extract the certificates and key as follows:

1. Open the `.ovpn` file in your editor (must be able to save as UTF-8 and use LF, not CR-LF, for a newline).
2. Go to the section tagged as `<ca> ... </ca>` and copy the marked certificate, including `----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----`.

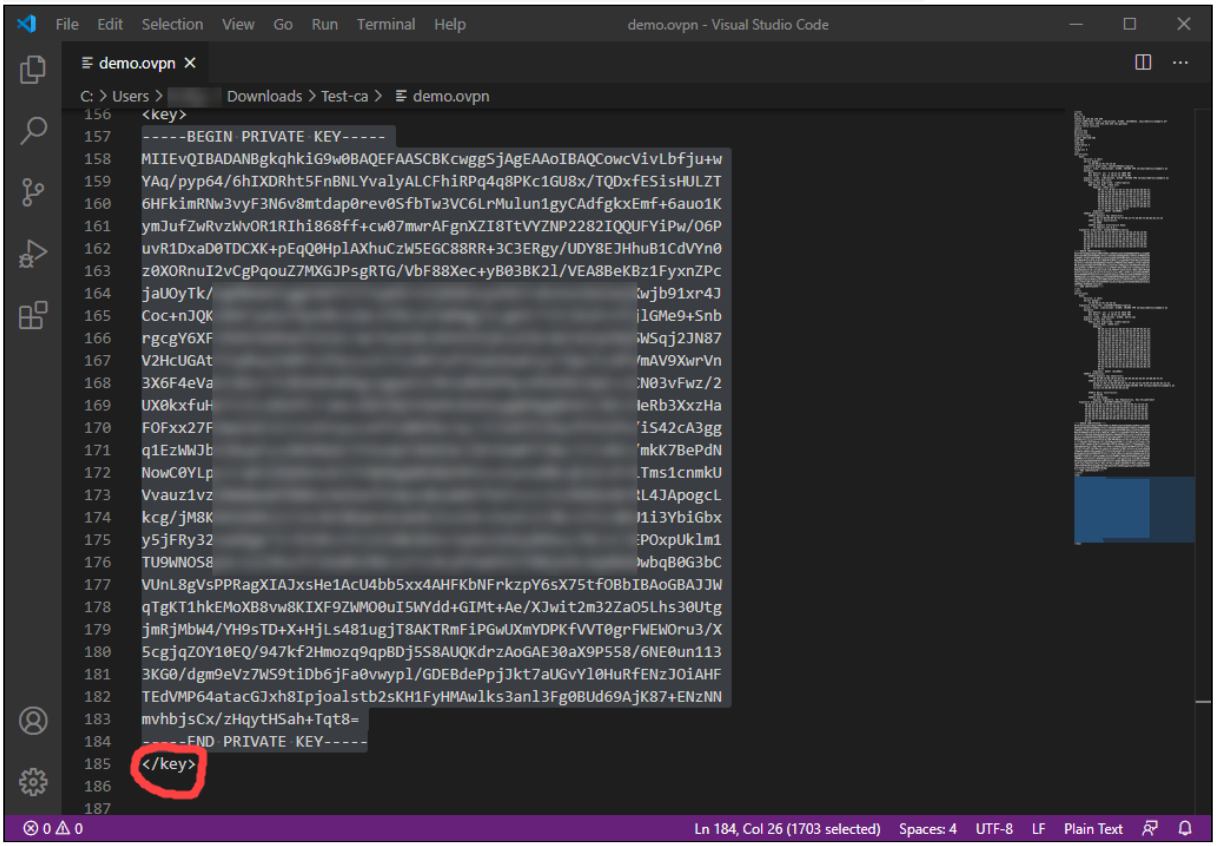


3. Paste the text to the editor and save it to a file named `ca.crt` (file type "All files").
4. Go to the section tagged as `<cert> ... </cert>` and copy the marked certificate, including `----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----`.



5. Paste the text to the editor and save it to a file named `client.crt` (file type "All files").

6. Go to the section tagged as `<key> ... </key>` and copy the marked key, including `-----BEGIN PRIVATE KEY-----` and `-----END PRIVATE KEY-----`.



7. Paste the text to the editor and save it to a file named `client.key` (file type "All files").

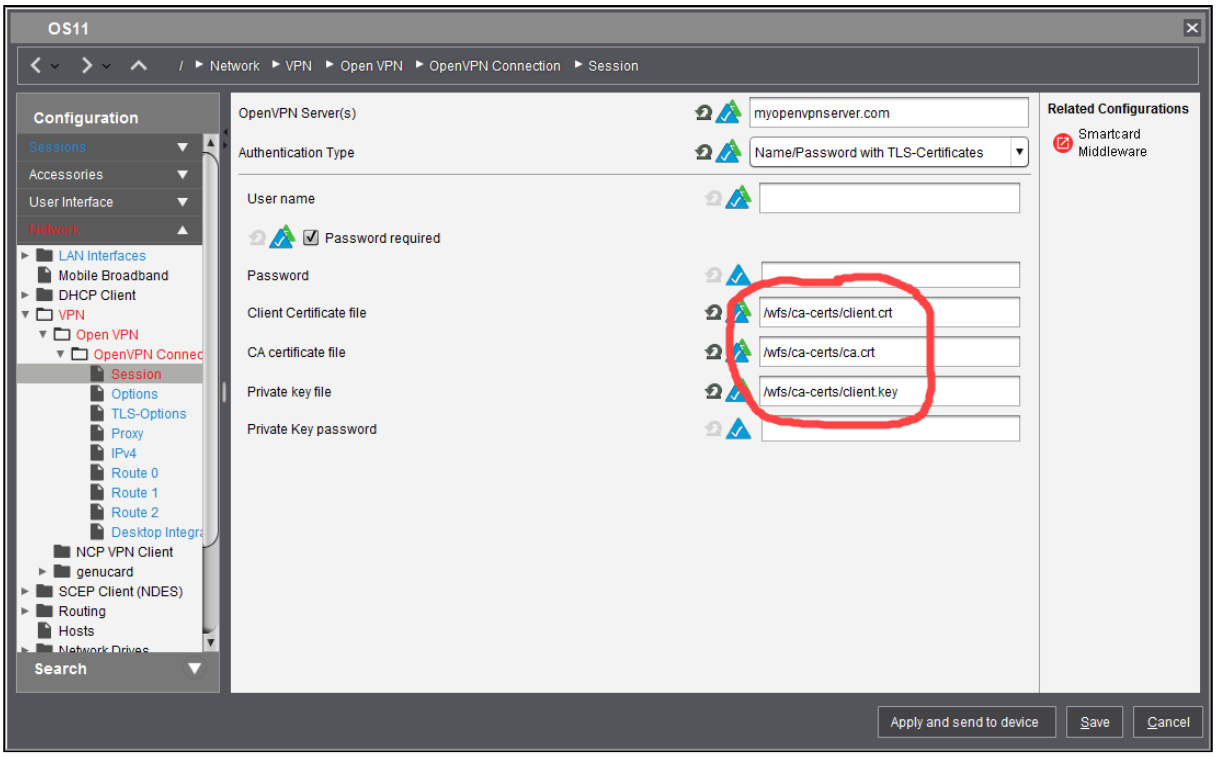
Transferring the Files to the UMS

1. In the UMS, go to **Files > [context menu] > New file** and create a file object for each certificate/key file; set **Classification** to "Common Certificate (all purpose)".
2. Assign the file objects to the endpoint devices on which you want to use the OpenVPN connection.

For detailed information on how to create file objects in the UMS and transfer them to devices, see *Universal Management Suite > UMS Reference Manual > Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices*.

Adjust the Profile

1. In the UMS, open the profile you have created for your OpenVPN connection and go to **Network > VPN > Open VPN >** [your OpenVPN connection] **> Session**.
2. Edit the file locations as follows:



3. Apply the profile to the endpoint devices on which you want to use the OpenVPN connection.

Multiple Users with Individual VPNs Sharing One Endpoint

> **Solution Based on Experience from the Field**
>
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

The trick is that we have to get all the users' OpenVPN config files (`.ovpn`) named `as <username>.ovpn` and placed under `/wfs`

We then have this script /wfs/openvpn/connect.sh

#!/bin/bash

1. Requirements:
2. - all users' ovpn config file needs to be in /wfs/`

1. Initialise variables
   answer=-1
   declare -a profiles=($(cd /wfs ; ls *ovpn | sed -e 's/\.ovpn//' | tr '\n' ' '))
   count=${#profiles[@]}

1. Loop until a valid profile index is selected
   until [$answer -ge 0 -a $answer -lt ${count}]; do
   clear
   for((i=0;i<${count};i++)); do
   echo "${i}: ${profiles[${i}]}"
   done;
   read -p "Select the number corresponding to your account: " answer
   done

1. export variable vpnuser in case a child process needs it (probably overkill)
   export vpnuser=${profiles[${answer}]}

1. Provide a name server only if one is not already installed
   grep -q 192.168.1.222 /etc/resolv.conf || echo "nameserver 192.168.1.222" >> /etc/resolv.conf

1. Start the openvpn client
   openvpn --config /wfs/${vpnuser}.ovpn --daemon

(The nameserver bit is required. It needs to be an internal DNS server, not sure how you'd generalize this)

Next we have a custom application with "Command" as:

pkexec /usr/bin/xfce4-terminal -T VPN --geometry=90x40-0+0 -x /wfs/openvpn/connect.sh

IPv6 Settings

IGEL Linux version 5.07.100 or newer and IGEL *Linux version 10.01.100* or newer offer new options for configuring network interfaces for IPv6.

Application Scenario

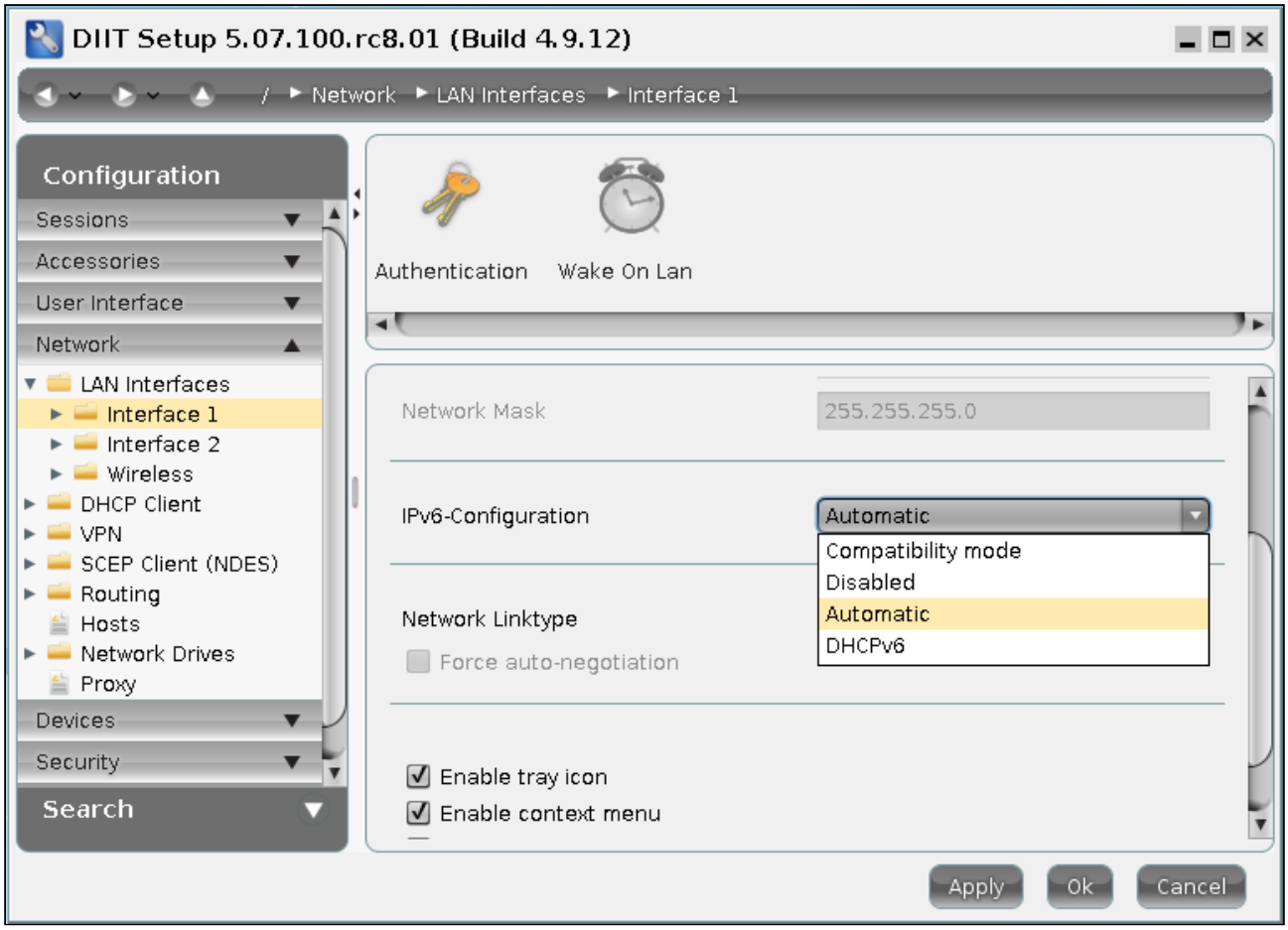
IGEL devices cannot so far communicate with the UMS via IPv6. Therefore, the major application scenario for IPv6 is as follows:

- Devices still receive their IPv4 configuration and potentially *IGEL*-specific DHCP options from a DHCPv4 server.
- Most of the settings are received from the *UMS* via IPv4.
- Only the default options are requested from the DHCPv6 server. These are as follows:
  - IPv6 address
  - nameservers
  - DNS search list.
- Regarding DNS, only IPv6 nameserver addresses should be delivered (in router advertisements or DHCPv6 options). The resolver should be able to use these for retrieving AAAA records and also A records if necessary.
- Clients and servers use IPv6 if they are prepared to do so.
  Examples:
  - An NTP server (**System > Time and date > NTP time server**) can be specified as an IPv6 address or as a name for which the DNS has only an AAAA record available.
  - Similarly, in a web browser session, IPv6 will be used when the DNS has AAAA records available for servers.

- Available IPv6-Configurations (see page 662)
- Timeouts in Automatic Configuration (see page 664)

Available IPv6-Configurations

IPv6 support is configured by network interface in **Network > LAN Interfaces:**



The following configurations are available:

Value	Effect
Compatibilty mode	Equivalent to former versions of IGEL Linux: NetworkManager ignores the device, but the kernel performs some basic configuration. In particular, it assigns an IPv6 link local address to the device.
Disabled	IPv6 is disabled completely.
Automatic	The device tries to perform an IPv6 stateless or stateful autoconfiguration based on router advertisements. Depending on the router advertisements, this involves DHCPv6 (see RFC 4861).

DHCPv6	This option is supported by NetworkManager. It can be used when a DHCPv6 server is available but no router advertisements. Routing has to be configured by other means. In most cases **Automatic** will be preferable.

In all cases IPv4 is configured in the usual way.

Timeouts in Automatic Configuration

If **Automatic** is selected, there is a configurable timeout for the dual stack mode. This is the time that the system waits after the first of the stacks IPv4 or IPv6 has completed its configuration for the other stack to complete its own configuration. After this time has elapsed, it runs the scripts that depend on the network being up. The default timeout value is 15 seconds.

The timeout can be configured with the following parameters in **System > Registry:**

Parameter	Device
`network.interfaces.ethernet.device0.dual_stack_timeout`	First ethernet device
`network.interfaces.ethernet.device1.dual_stack_timeout`	Second ethernet device
`network.interfaces.wirelesslan.device0.dual_stack_timeout`	Wireless LAN device

Use the **Search parameter ...** function with the string `dual_stack` to find these parameters quickly.

Security

- Securing IGEL OS Endpoints (see page 666)
- Secure Shell (SSH) Access to IGEL OS with Keys (see page 711)
- Secure Terminal (Telnet with TLS/SSL) (see page 717)
- Secure Shadowing (VNC with TLS/SSL) (see page 718)
- Cherry eGK Channel Substitution (see page 722)
- Single Sign-on for the Browser Proxy (see page 724)
- Enforcing User Authentication at the Device (see page 727)
- Limiting the Number of Permitted Login Attempts (see page 731)
- How to Deploy Device Encryption (see page 732)
- Security: Timeout for Secure Shadowing and Secure Terminal (see page 736)
- Mitigate Terrapin Vulnerability through Registry Parameter in IGEL OS (see page 738)
- Configuring IGEL OS11 NTLM Passthrough Authentication (see page 739)

Securing IGEL OS Endpoints

This document describes settings for IGEL OS that will increase security.

It applies to the following types of devices:

- IGEL UD devices
- Devices which are temporarily converted by UD Pocket
- Devices which are permanently converted by IGEL OS Creator (OSC)

- Security Introduction (see page 667)
- Setting Passwords (see page 668)
- How to Keep the System Up-To-Date (see page 675)
- Disabling Access to Components (see page 682)
- Minimizing the Attack Surface (see page 687)
- Configuring Remote Access and Management (see page 699)
- Wi-Fi and Bluetooth (see page 707)
- Using IGEL UD Pocket for BYOD Devices (see page 710)

Security Introduction

This document describes various settings to make IGEL OS more secure. In general, the more of these settings you apply, the better device security will be. However, it is up to you to strike a balance between security and enabling your users to do their work. Some settings may even be inappropriate for your use case, e.g. if you use Bluetooth peripherals, it does not make sense to disable Bluetooth.

In order to configure multiple devices, put the relevant settings into a Universal Management Suite (UMS) master profile, which you can assign to any number of devices. For more information, see Master Profiles under Archive > UMS PDF.

Setting Passwords

You can restrict access to various system components by setting passwords.

- Setting Local Passwords (see page 669)
- Password-Protecting Sessions and Accessories (see page 670)
- Using Screenlock (see page 671)
- Do Not Save Session Passwords (see page 672)
- Setting a UEFI Password (see page 673)
- Using Two-Factor Authentication (2FA) (see page 674)

Setting Local Passwords

Rationale

Passwords protect the system against local changes. They restrict access to the Local Terminal, Setup, and to the rescue shells on the virtual consoles. The administrator password is also needed to reset the system to factory defaults.

These passwords are saved in a way (salted and hashed) that prevents them from being recovered from the local storage.

By default, no passwords are set on IGEL OS. Set at least an administrator password:

Instructions

1. In IGEL Setup go to **Security > Password**.
2. In the **Administrator** area, check **Use Password**.
3. Enter a password twice when prompted.
4. Optional: If you want to grant unprivileged user access to IGEL Setup check **Use Password** in the **Setup user** area and enter a password twice when prompted.
5. Click **Apply**.

For configuration of the **User Account for Remote Access**, see Using Secure SSH Settings (see page 705).

Find further information in the IGEL OS manual under Password - Restrict Access to IGEL OS Components (see page 2017).

Password-Protecting Sessions and Accessories

Rationale

Sessions can be used to access corporate resources, while the accessories in IGEL OS can be used to make changes to the local system. If you do not want to disable certain sessions or accessories completely, you can set passwords to restrict access to them.

Instructions

By default, sessions do not have passwords set. In IGEL Setup, you can set a password on the **Desktop Integration** page of a session or accessory.

To enable password protection:

1. In the Setup, go to the relevant **Desktop Integration** page. The path has the following pattern: **Sessions > [session type] > [session name] > Desktop Integration**.
   For accessories, go to **Accessories > [accessory name]**.
2. Set **Password Protection** to
   - **Administrator** to require the Administrator password, or
   - **User** to require the User password, or
   - **Setup User** to require the Setup User password.
3. Click **Apply**.

Using Screenlock

Rationale

Leaving a screen unlocked enables attackers to access the system with the logged-in user's privileges. Manual or automatic locking the screen with a password prevents such access.

Instructions for Enabling Manual Locking

By default, there is no way for the user to manually lock the screen. To enable manual locking, follow these steps:

1. In the Setup, go to **User Interface > Screenlock / Screensaver**.
2. Do one or both of the following:
   - Activate the **Quick start panel** starting method to give the user a button for locking the screen manually.
   - Activate **Use hotkey** and set a combination of keys that lets the user lock the screen manually, e.g. [Ctrl+Shift+L].
3. Click **Apply**.

Instructions for Automatic Locking

By default, the screensaver is started automatically after 5 minutes, but the screen is not locked with a password. To enable locking, follow these instructions:

1. Go to **User Interface > User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.
3. Set the **Timeout**, i.e. the number of minutes of user inactivity before the screensaver starts automatically.
4. As a password, select **User password** (see Setting Local Passwords (see page 668)) or a separate **Screenlock password** (and set one).
5. If applicable, activate **Allow administrator password** to allow the administrator to unlock the screen.
6. Click **Apply**.

Do Not Save Session Passwords

Rationale

Passwords for sessions should not be stored on the endpoint device.

Instructions

->When configuring a session, on the login page, leave the **Password** field empty. The user will then be prompted interactively for the password.

->Wherever possible use Two-Factor Authentication (2FA) (see page 674).

Setting a UEFI Password

Rationale

In the UEFI settings you can modify very fundamental system properties, e.g. disable booting from USB. Access to these settings should be protected by a password.

Instructions for IGEL Devices

→ If UEFI is not enabled, see the instructions under UEFI Secure Boot Enabling Guides[85].

By default no UEFI password is set on IGEL UD devices. To set a password, do the following:

1. Hold down the [Del] key ([F2] key for UD2) while booting.
   The UEFI menu opens.
2. Using the arrow and return keys, go to **SCU**.
   The **Setup Utility** opens.
3. Using the arrow and return keys, go to **Security**.
4. Use the arrow keys to select **Set Supervisor Password**.
5. Hit [Return].
6. Enter the desired UEFI password and hit [Return]
7. Enter the same UEFI password again and hit [Return] twice.
8. Hit [F10] in order to save and exit.
9. Confirm **Exit Saving Changes?** by hitting [Return].
   The system boots, and the UEFI settings are now password-protected.

Instructions for 3rd-Party Devices Converted with OS Creator (OSC)

→ Refer to the instructions of your BIOS/UEFI vendor.

Alternatively, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing [Del], [F1], or [F2] during booting.

85. https://kb.igel.com/security-safety/current/uefi-secure-boot-enabling-guides

Using Two-Factor Authentication (2FA)

Rationale

Two-factor authentication (2FA) combines two different factors to prove the user's identity, often a hardware device such as smartcard or smart token and a password or PIN. This improves protection against impostors, as they would have to gain both possession of the hardware device and knowledge of the password or PIN.

Instructions

Use two-factor authentication with a smartcard or smart token where possible. IGEL OS supports this for the following sessions:

- Smartcard authentication for sessions (see page 791)
  - Citrix Storefront (see page 795)
  - RDP Sessions (see page 797)
  - Horizon Sessions (see page 798)
  - Web browser (see page 799)
- (Kerberos) Passthrough Authentication (see page 1173)

How to Keep the System Up-To-Date

Rationale

Software updates fix newly discovered vulnerabilities in IGEL OS and applications. This means that keeping up with updates is one of the most important measures in securing IGEL OS systems.

To start and configure updates, you can use IGEL Setup and/or the Universal Firmware Update feature of the Universal Management Suite (UMS).

The instructions described on this page use the Universal Firmware Update feature of the UMS. For defining a scheduled job, see the section "As a Job" in *Universal Management Suite* > *UMS Reference Manual* > *Devices* > *Managing Devices* > *Assigning Updates*; for configuring the update on a device, see Firmware Update Settings for IGEL OS (see page 2056).

Instructions

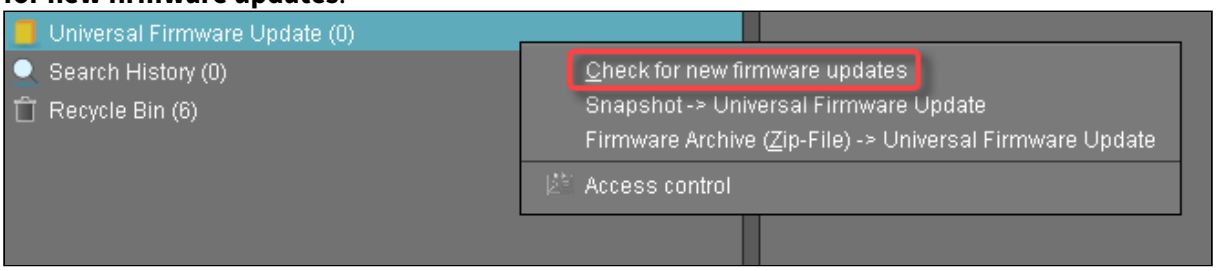
→ To get new ISNs and ISN updates delivered to your inbox, subscribe to the Security Announcements Mailing List. Go to http://igel.com and find the "Subscribe for Updates" form at the bottom of the page. This will initially subscribe you to all mailings from IGEL, but by using the unsubscribe link at the bottom of a mail, you can select which communications you wish to receive and which not.

The upgrade procedure consists of the following steps:

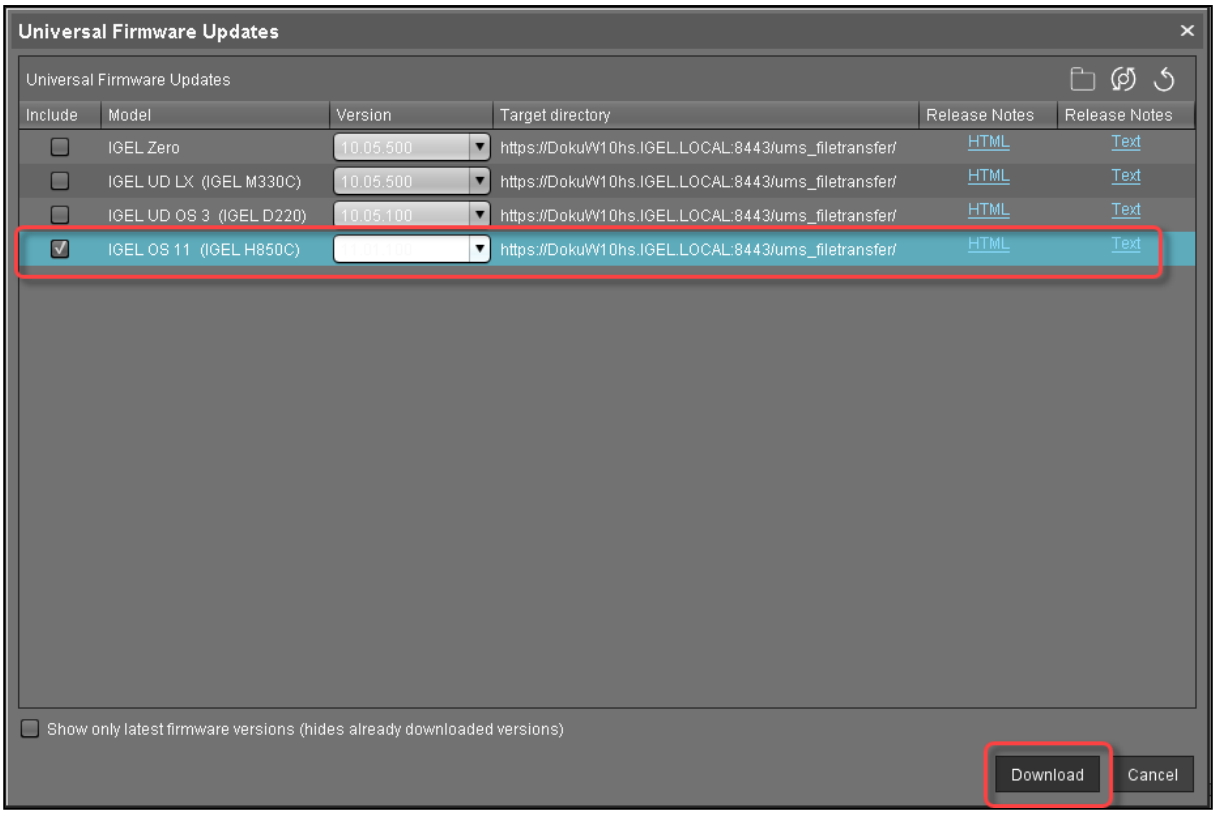
- Getting the update from the IGEL download server
- Testing the update on one or a few devices
- Rolling out the update on all devices

Getting the Update from the IGEL Download Server

1. In the UMS Console, go to **Universal Firmware Update**, open the context menu, and select **Check for new firmware updates**.

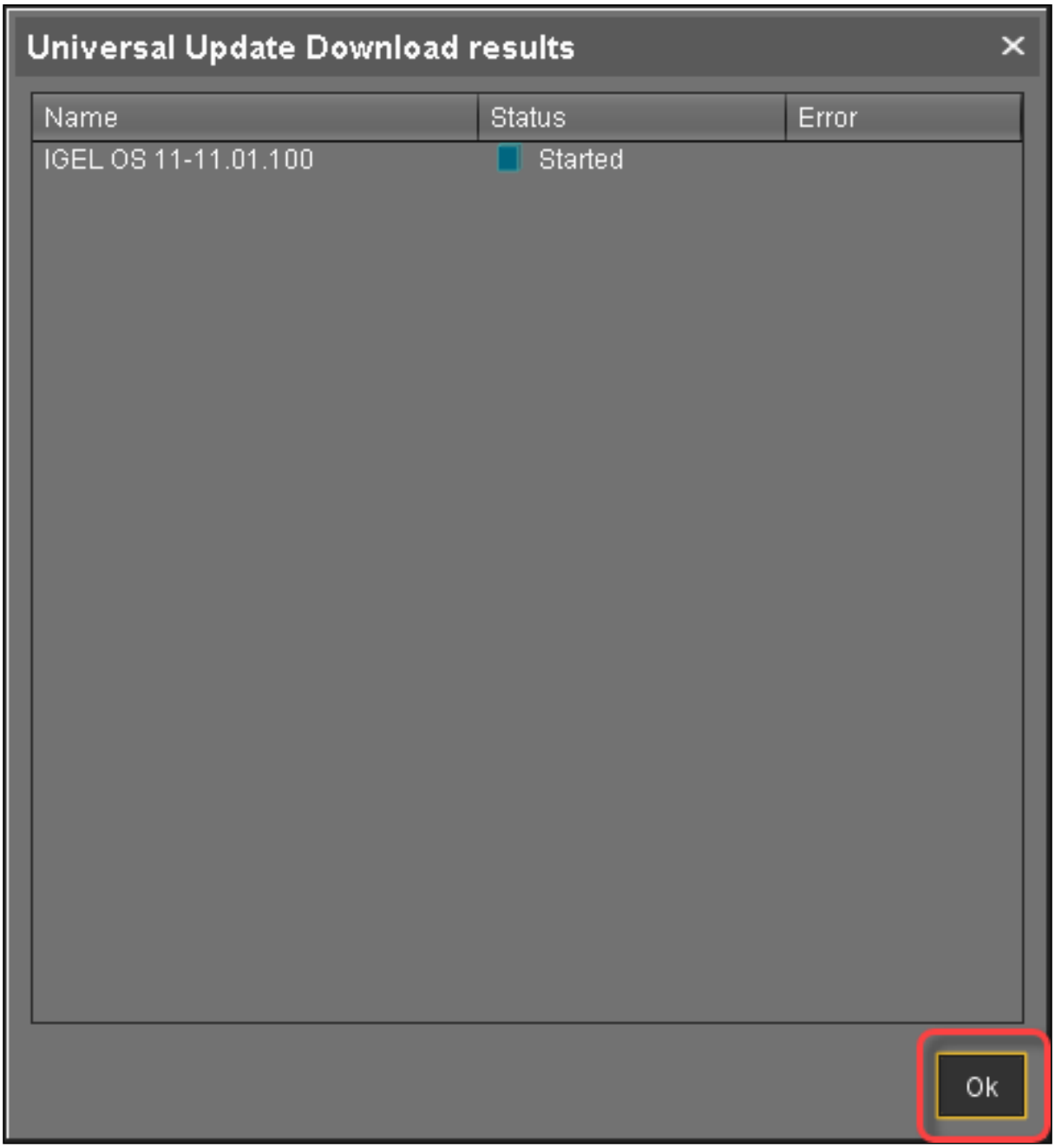


2. Activate the firmware you want to download and click **Download**.

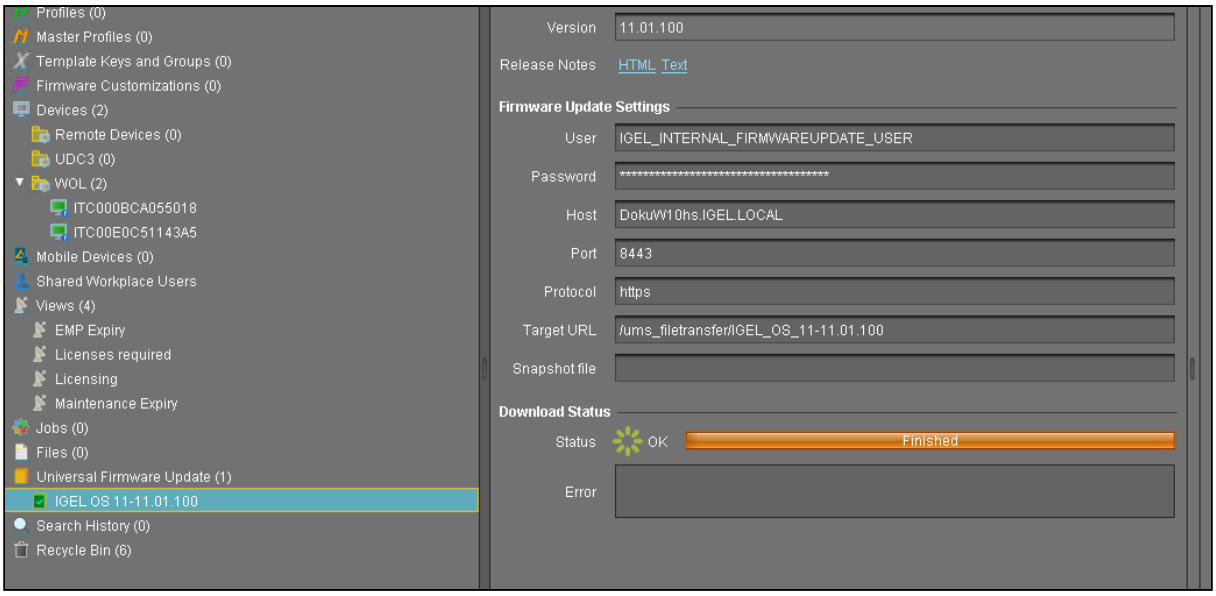


The current status of the firmware download is shown.

3. Click **Ok**.

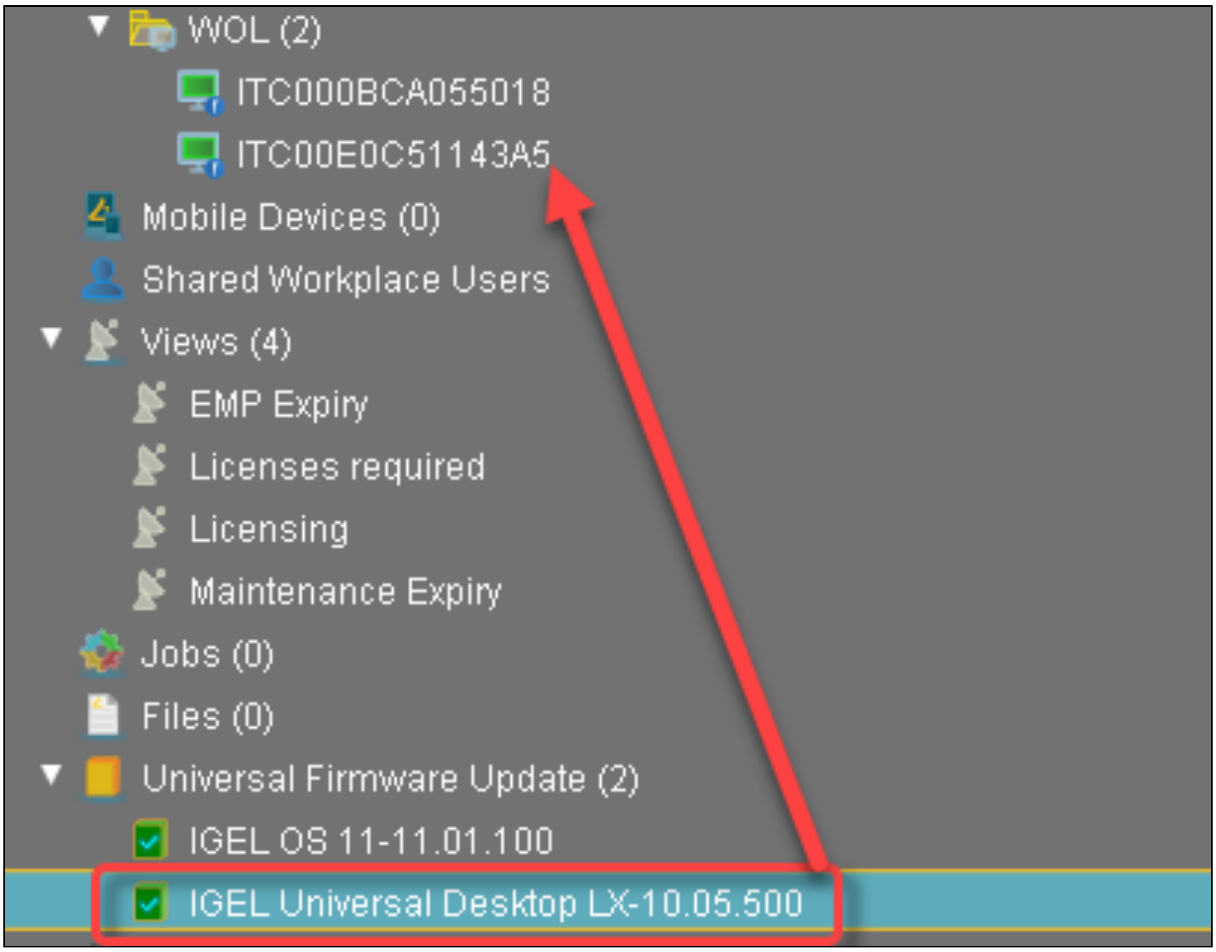


4. When the download has succeeded, the firmware is registered and stored in the UMS.

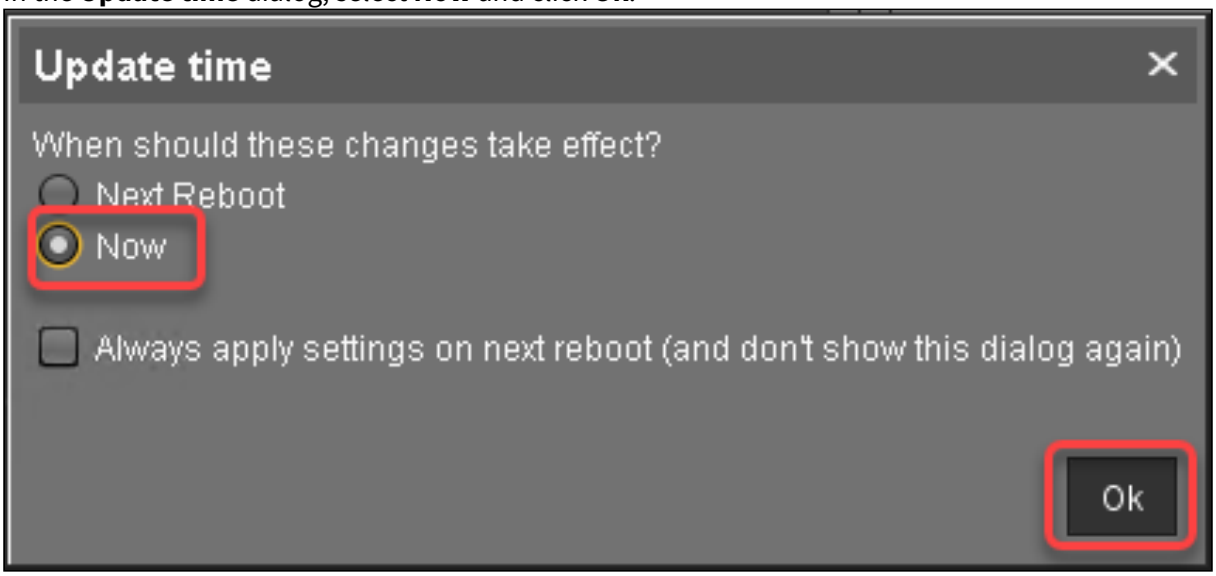


Testing the Update on One or a Few Devices

1. In the UMS Console, go to **Universal Firmware Update**, select the desired firmware and drag and drop it on the test device or on the folder containing the test devices.



2. In the **Update time** dialog, select **Now** and click **Ok**.



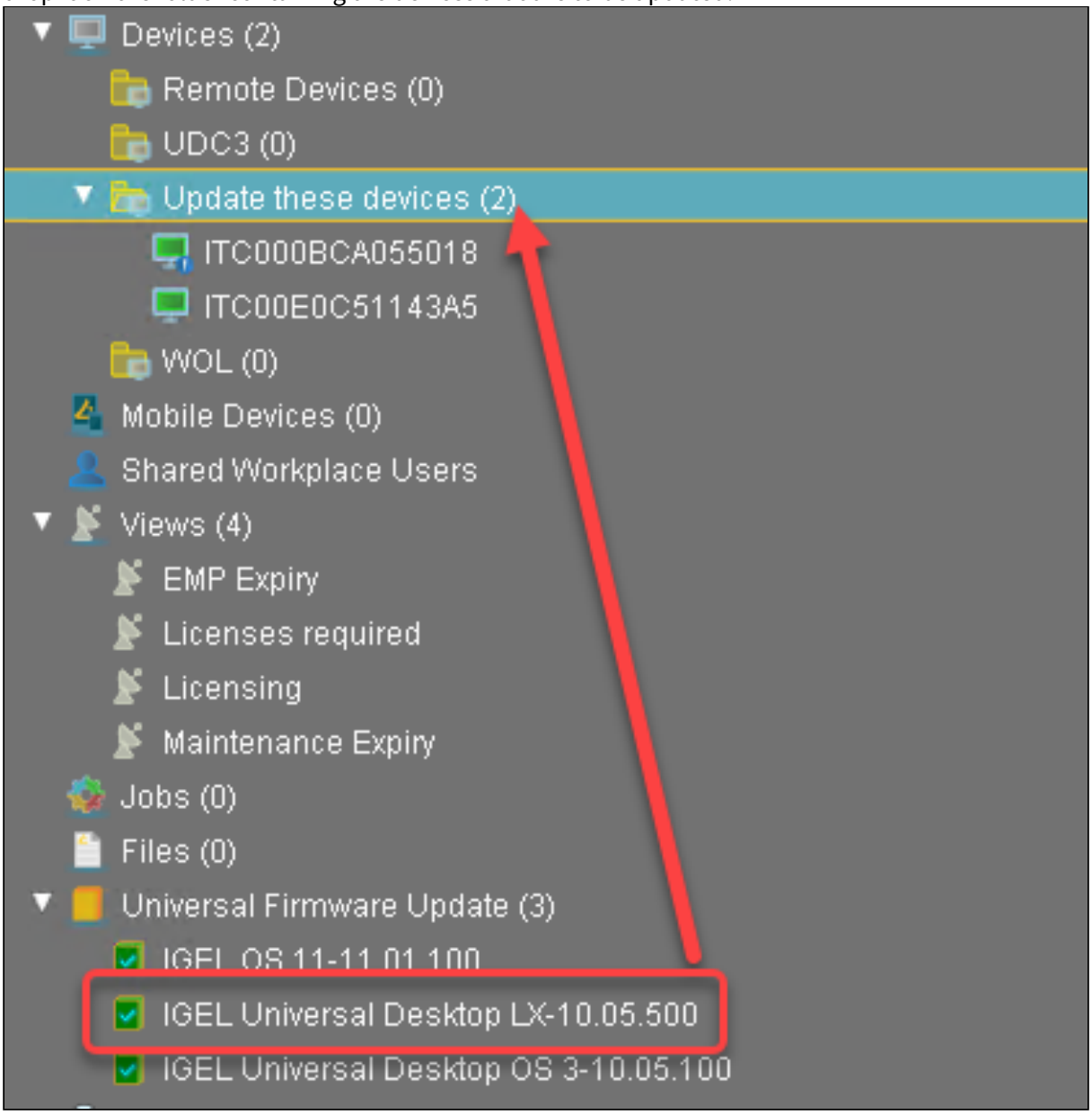
The firmware is updated on the devices; during the update process, the devices reboot.

Rolling out the Update on All Devices

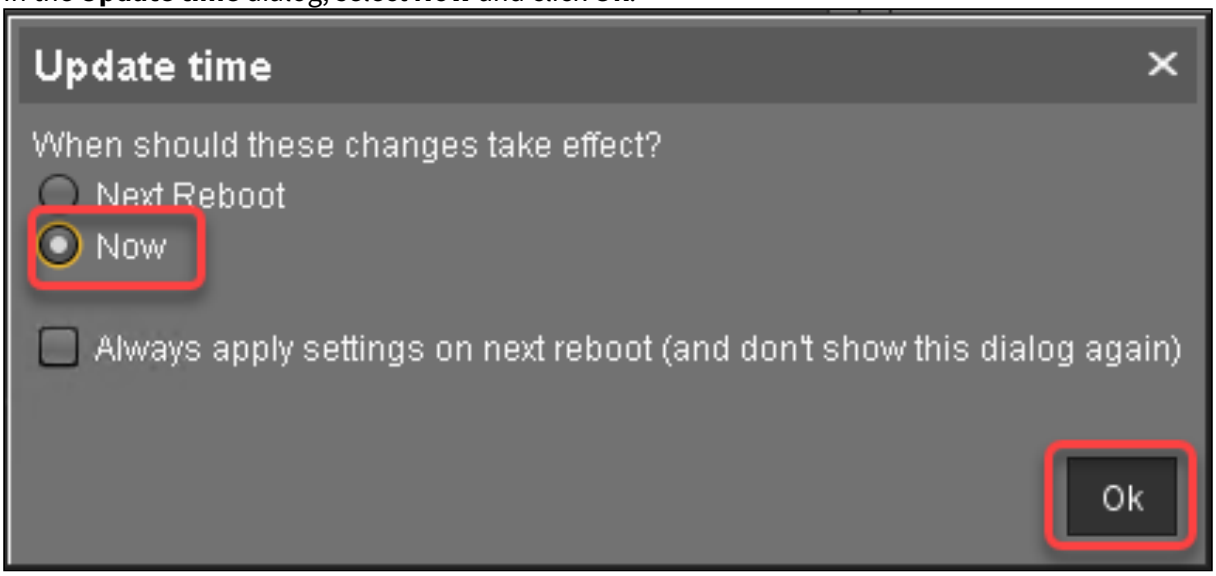
You can either start the update immediately or use a scheduled job to start it at a defined time.

To start the update immediately:

1. In the UMS Console, go to **Universal Firmware Update**, select the desired firmware and drag and drop it on the folder containing the devices that are to be updated.



2. In the **Update time** dialog, select **Now** and click **Ok**.



The firmware is updated on the devices; during the update process, the devices reboot.

Disabling Access to Components

You can hide IGEL OS components from the user that could be used to make changes to the system.

- Disabling Local Terminal Access (see page 683)
- Disabling Virtual Console Access (see page 684)
- Using Appliance Mode (see page 685)
- Hiding Unused Accessories (see page 686)

Disabling Local Terminal Access

The **Local Terminal** accessory allows the user to execute commands or make changes to the system. By default, the local terminal is disabled, that is, no local terminal session is configured. To enhance security, you should do one of the following:

- Leave the local terminal disabled
- If a local terminal session is configured, but not needed, disable it.
- If a local terminal session is needed, password-protect it.

Instructions

To remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Alternatively, you can password-protect the terminals.

To password-protect the local terminal:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Password-Protecting Sessions and Accessories (see page 670).

Disabling Virtual Console Access

Rationale

The virtual consoles `tty11` and `tty12` give the user access to a shell. Disabling these makes it more diffcult to execute commands or make changes to the system.

Instructions

By default, the user can access the virtual consoles with the [Ctrl]+[Alt]+[F11] and [Ctrl]+[Alt]+[F12] keyboard commands. To disable access, do the following:

1. In IGEL Setup go to **User Interface > Display > Access Control**
2. Activate **Disable Console switching** (Default: Console switching enabled)
3. Click **Apply**.

Using Appliance Mode

Rationale

By default, IGEL OS users are not presented with a full-screen remote session, but have access to the desktop and to the start menu. On the contrary, in the appliance mode, a single predefined session is presented full-screen to the user. As access to other applications is prevented, this reduces the system's potential exposure to attack.

Instructions

The appliance mode is available for the following session types:

- VMware Horizon (see page 1415)
- Appliance Mode Browser (see page 1416)
- Citrix Self-Service (see page 1417)
- RHEV/Spice (see page 1418)
- Imprivata (see page 1419)
- RDP MultiPoint Server (see page 1422)
- XDMCP for This Display (see page 1423)

To enable the appliance mode for a session, proceed as follows:

1. In IGEL Setup, go to **Sessions > Appliance Mode**.
2. Pick the session and configure it according to the manual chapter Appliance Mode (see page 1413).

You can combine most of the appliance mode sessions with Two-factor Authentication (see page 674) for increased security.

Hiding Unused Accessories

Rationale

Accessories can be used to make changes to the system. Restricting access to these accessories helps to keep the system secure.

Instructions

To hide individual accessories (both in the start menu and the Application Launcher):

1. In IGEL Setup go to **Accessories > [accessory name]**.
2. Disable all **Starting Methods for Session**.
3. Click **Apply**.

To password-protect an accessory:

->Follow the instructions under Password-Protecting Sessions and Accessories (see page 670).

To hide the complete **System** icon of the start menu:

1. In IGEL Setup go to **User Interface > Desktop > Start Menu**.
2. Deactivate **System tab**.
3. Click **Apply**.

To hide the complete Application Launcher's **System** icon:

1. In IGEL Setup go to **Accessories > Application Launcher > Application Launcher Configuration**.
2. Activate **Hide system page**.
3. Click **Apply**.

Minimizing the Attack Surface

Removing unused features and disabling unneeded network services reduces the parts of the system that can be attacked.

- Removing the Local Web Browser (see page 688)
- Configuring the Browser (Kiosk Mode) (see page 689)
- Disabling Java in the Browser (see page 691)
- Disabling the PC/SC Daemon (see page 692)
- Disabling X Server TCP Connections (see page 693)
- Removing Unused Features (see page 694)
- Disabling Storage Hotplug (see page 695)
- Using USB Device Control (see page 696)
- Disabling USB Boot (see page 697)
- Leveraging AppArmor (see page 698)

Removing the Local Web Browser

Rationale

The local web browser may expose vulnerabilities to the internet and can be an entry point for malware. If the browser is not needed, it is safer to remove it.

Do not remove the local web browser if you use Citrix StoreFront sessions.

Instructions

By default, IGEL OS has a local web browser (Firefox and Chromium) installed, even if no web browser session is configured. To remove the browser:

1. In the IGEL Setup, go to **System > Firmware Customization > Features**.
2. Uncheck the **Local Browser (Firefox)** and **Local browser (Chromium)** feature.
3. Click **Apply**.
4. Reboot the device.

Configuring the Browser (Kiosk Mode)

Rationale

If you want to offer a local web browser, there are some settings that improve its security. Additionally, these settings add up to a kiosk mode, hiding the rest of IGEL OS from the user.

Instructions

By default, the web browser makes all of its features and menus available. To achieve a restricted 'kiosk' mode, follow these instructions.

Firefox

1. In the IGEL Setup under **Sessions > Firefox Browser > Firefox Browser Global > Security**, activate the following options:
    - **Safe Browsing**
    - **Malware Protection**
    - **Hide local filesystem**
2. Under **Sessions > Firefox Browser > Firefox Browser Global > Content**, activate **Block pop-up windows**, if required.
3. Under **Sessions > Firefox Browser > Firefox Browser Global > Privacy**, activate the following options:
    - **Clear private data when closing browser** and all options in the area **Select the items to be cleared**
    - **Allow private browsing feature**
    - **Always start in private browsing mode**
    - **Enable "Do Not Track" feature** and **Enable built-in tracking protection**, if necessary
4. Under **Sessions > Firefox Browser > Firefox Browser Global > Restart**, activate **Restart**.
5. Under **Sessions > Firefox Browser > Firefox Browser Global > Window**, activate the following options:
    - **Start in full-screen mode**
    - **Hide configuration page of the browser**
6. Under **Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars**, activate **Hide App Menu/Menu Bar**.
7. Under **Sessions > Firefox Browser > Firefox Browser Global > Context**, activate **Hide the browser's context menu**.
8. Under **Sessions > Firefox Browser > Firefox Browser Sessions > [session name] > Settings**, activate **Autostart**.
9. Click **Apply**.
10. Reboot the device.

For additional information, see also How to Use the Firefox Browser in Kiosk Mode (see page 573).

Chromium

1. In the IGEL Setup under **Sessions > Chromium Browser > Chromium Browser Global > Security**, activate **Safe browsing** and disable **File access**.
2. Under **Sessions > Chromium Browser > Chromium Browser Global**, activate **Automatic browser restart on exit**.
3. Under **Sessions > Chromium Browser > Chromium Browser Global > Content**, activate **Block pop-ups and redirects**, if required.
4. Under **Sessions > Chromium Browser > Chromium Browser Global > Privacy**, activate the following options:
    - **Clear browsing data** and all options in the area **Select the items to be cleared**
    - "Forced" for the setting **Allow incognito mode**
    - **Enable "Do Not Track" feature**, if necessary
5. Under **Sessions > Chromium Browser > Chromium Browser Global > Window**, activate **Enable kiosk mode**.
6. Under **Sessions > Chromium Browser > Chromium Sessions > [session name]**, activate **Autostart**.
7. Click **Apply**.
8. Reboot the device.

Disabling Java in the Browser

Java Applets and Java Web Start may constitute a potential security threat and are now regarded as deprecated. As of IGEL OS version 10.06.100, they are no longer included in IGEL OS. The registry keys under **System > Registry > java > deployment** are obsolete.

Disabling the PC/SC Daemon

Rationale

Unless you are running smartcard readers that use it, you can disable the PC/SC daemon. Running fewer daemons reduces the attack surface.

Instructions

To deactivate the PC/SC daemon:

1. In the IGEL Setup go to **Security > Smartcard > Services**.
2. Deactivate **Activate PC/SC Daemon**.
3. Click **Apply**.

Disabling X Server TCP Connections

Rationale

The X graphics server in IGEL OS has network functionality that could allow others to see your screen and read keyboard input. Leave it disabled to keep your data confidential.

Instructions

By default the network functionality of the X server is disabled. To disable it again at a later time, do the following:

1. In IGEL Setup go to **User Interface > Display > Access Control**
2. Make sure that **Access Control** is activated.
3. Make sure that **Disable TCP connections** is activated.
4. Click **Apply**.

Removing Unused Features

Rationale

Reducing the amount of software running on a system reduces its attack surface. Therefore a basic security measure for IGEL OS 11 is to remove all unused features.

Instructions

To disable a feature:

1. In the IGEL Setup, go to **System > Firmware Customization > Features**.
2. Deactivate all the features that you do not intend to use.
3. If you do not use local printers on the endpoint device that you want to share with others, activate:
   - **Printing (Internet Printing Protocol CUPS)**
   - **Printing (Line Printer LPD)**
   - **Printing (TCP/IP)**
   - **Printing (ThinPrint)**

   Do not remove the **Custom Partition** feature if you have a custom partition that contains software or data for which you have no backup copy. After disabling the feature and a reboot the contents of the custom partition will be lost.

   Do not remove **Fluendo Gstreamer Codec Plugins** or **Hardware Video Acceleration** if you use sessions that make use of these features.
4. Click **Apply**.
5. Reboot the device.

Alternative Method for Reducing the Feature Set as of IGEL OS 11.04
If you update to IGEL OS 11.04 or higher, you can alternatively use the method described under Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher[86]. The advantage of this method in comparison to disabling features via the IGEL Setup is that you won't have to disable the deactivated features once again in case you reset the endpoint device to factory defaults (see Reset to Factory Defaults (see page 1225)).

86. https://kb.igel.com/en/igel-os/11.10.270/error-not-enough-space-on-local-drive-when-updatin

Disabling Storage Hotplug

Rationale

Removable USB media can be used to steal data or to execute unauthorized software or even malware on the device.

Instructions

Storage hotplug is disabled by default. Should you want to disable it again at any later point, follow these instructions:

1. In IGEL Setup go to **Devices > Storage Devices > Storage Hotplug**.
2. Deactivate **Storage Hotplug**.
3. Click **Apply**.
   Storage devices are no longer automatically mounted when they are plugged in.

Using USB Device Control

Rationale

USB devices such as pen drives, wireless controllers, or printers can be used to steal data or to execute unauthorized software or even malware. Deactivating as many USB device classes as possible increases security.

Instructions

To enable and configure USB access control:

1. In IGEL Setup, go to **Devices > USB Access Control**.
2. Check **Enable**.

> ⚠ The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.
> It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.
> Note that the USB access control is completely separate than USB redirection for remote sessions, see When to Use USB Redirection (see page 1093).
> Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

3. Set **Default rule** to **Deny**.
   In combination with the preconfigured rule that allows Human Interface Devices (HID), no USB devices apart from e.g. mouse and keyboard are allowed.
4. Configure further rules as needed. For instructions, see How to Configure USB Access Control (see page 1097).
5. Click **Apply**.
6. Reboot the device.

Disabling USB Boot

Rationale

Disabling USB ´boot prevents booting another operating system, which could be used to manipulate or (even accidentally) overwrite IGEL OS on mass storage.

Instructions for IGEL Devices

USB boot is disabled in the factory settings on IGEL UD LX devices. If it has been enabled and you want to disable it again, follow the instructions given here:

1. Hold down the [Del] key ([F2] key for UD2) while the system is booting.
   The UEFI menu opens.
2. Use the arrow and return keys to go to **SCU**.
3. Enter the UEFI password if one is set.
   The **Setup Utility** opens.
4. Go to **Boot**.
5. Set **USB Boot** to **Disabled**.
6. Press [F10].
7. Confirm **Exit Saving Changes?**
   The device boots.

> Additionally, set a UEFI Password (see page 673) so the boot settings cannot be changed back.

Instructions for 3rd-Party Devices Converted with OSC

->Refer to the instructions of your BIOS/UEFI vendor.

> Alternatively, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing [Del], [F1], or [F2] during booting.

Leveraging AppArmor

AppArmor controls which privileges should be granted to an application that is running on the system. This way even vulnerabilities that are yet unknown can be mitigated.

The following applications are guarded by AppArmor:

- Firefox browser
- Cups print server
- Evince pdf viewer

The following system programs are guarded by AppArmor:

- tcpdump
- haveged
- dhclient

By default, AppArmor is enabled. They registry key is `system.security.apparmor`

Configuring Remote Access and Management

Remote management via UMS and remote access are powerful features of IGEL OS. Select secure settings and disable what you do not use.

- Tying Endpoints to Your UMS instance (see page 700)
- Disabling Shadowing (see page 701)
- Using Secure VNC Settings (see page 702)
- Disabling SSH Access (see page 703)
- Disabling X11 Forwarding (see page 704)
- Using Secure SSH Settings (see page 705)
- Disabling Secure Terminal (see page 706)

Tying Endpoints to Your UMS instance

Rationale

Devices that have remote management enabled but are not yet tied to a UMS instance can be taken over by an attacker's UMS. Make sure to register all IGEL devices on your network.

Instructions

By default, remote management is enabled on IGEL OS devices. Use automatic registration to catch all devices in your corporate network:

1. Assign the DNS entry `igelrmserver` to the UMS host. For further instructions, see Archive > UMS 6 PDF > Registering Devices Automatically on the IGEL UMS.
2. In the UMS console go to **UMS Administration > Global Configuration > Device Network Settings.**
3. Activate **Enable automatic registration (without mac address import)**
   Now all new IGEL devices, UD Pockets and devices converted with OSC that are booting up in the network will automatically register with your UMS instance.
4. Optionally, put newly registered devices into a quarantine directory automatically with UMS (See Archive > UMS 6 PDF > Default Directory Rules)
5. Optionally, assign a Master Profile (see Archive > UMS 6 PDF > Master Profile) to this directory, thereby enforcing secure settings, e.g. a local administrator password.

> Alternatively you can disable remote management in the local IGEL Setup under **System > Remote management**. Of course this means losing one of the most powerful features of IGEL OS. However, this may be an option for particular devices.

Disabling Shadowing

Rationale

Shadowing is made possible by a VNC server on IGEL OS, which is a network service. Reducing the number of running network services reduces the system's attack surface.

Instructions

By default, Shadowing is not active on IGEL OS. However, if you want to disable it at any time, follow these steps:

1. In the IGEL Setup go to **System > Remote Access > Shadow**
2. Deactivate **Allow Remote Shadowing**.
3. Click **Apply**.

Using Secure VNC Settings

Rationale

If you intend to use shadowing on IGEL OS, there are a number of options that can make it more secure.

Instructions

By default, Shadowing does not use encrypted network transport or a password. To activate these security features, do the following:

1. In IGEL Setup go to **System > Remote Access > Shadow**.
2. Make as many of the following settings as possible for your use case. Each setting improves security, and often also privacy:
   - Enable **Secure Mode.**
   - Enable **Use Password** and set a strong password (not needed in **Secure Mode**). The maximum length for this password is 8 characters.
   - Enable **Prompt User to allow Remote Session.**
   - Enable **Allow User to disconnect Remote Shadowing.**
   - Disable **Allow Input from Remote.**
3. Click **Apply**.

> Secure mode for shadowing can be enabled globally in **UMS under UMS Administration > Global Configuration > Remote Access**. There you can also enable the logging of users who have used secure mode shadowing .

Disabling SSH Access

Rationale

The SSH server on IGEL OS is a network service. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as SSH by design enables a remote user to execute commands on the system.

Instructions

By default, the SSH server is running on IGEL OS. To deactivate it, follow these steps:

1. In IGEL Setup go to **System > Remote Access > SSH Access**.
2. Deactivate **Enable**.
3. Click **Apply**.

Disabling X11 Forwarding

When X11 forwarding is disabled, graphic applications cannot be run over SSH. By default, X11 forwarding is disabled.

> If X11 forwarding is disabled, it is not possible to launch the IGEL Setup from an SSH session.

To ensure that X11 forwarding is disabled:

1. In the Setup, go to **System > Remote Access > SSH Access** and make sure that **Permit X11 forwarding** is deactivated.
2. Click **Apply** or **Ok**.

Using Secure SSH Settings

Rationale

If you intend to allow SSH connections to IGEL OS, there are a number of options that can make these more secure.

Instructions

To secure the SSH settings of your devices, make as many of the following settings as possible for your use case

1. In IGEL Setup go to **System > Remote Access > SSH**.
2. Deactivate **Permit empty passwords**.
3. Deactivate **Permit administrator login**.
4. Deny **User access** for `user`, who can execute any command with regular user privileges.
5. Allow **User access** for `ruser`, whose access is restricted by the list **Applications access for remote user 'ruser'**.
6. Where needed, edit the list **Applications access for remote user 'ruser'**. It defines the commands that `ruser` can run from remote. By default, a local shell (`localshell`) and IGEL Setup (`/config/sessions/setup0`) are allowed.
7. Click **Apply**.
8. Go to **Security > Password**, under **User Account for Remote Access** activate **Use Password** and set a password
9. Click **Apply**.

Disabling Secure Terminal

Rationale

The secure terminal server on IGEL OS is a network service, providing a TLS/SSL-encrypted Telnet session. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as the secure terminal by design enables a remote user to execute commands on the system.

Instructions

By default, the secure terminal is not active. Should you want to deactivate it at any time, do the following:

1. In IGEL Setup go to **System > Remote Access > Secure Terminal**
2. Deactivate **Secure Terminal**.
3. Click **Apply**.

> Secure Terminal can be enabled globally in the UMS under **UMS Administration > Global Configuration > Remote Access**. There you can also enable the logging of users of the secure terminal.

Wi-Fi and Bluetooth

Rogue or unencrypted Wi-Fi access points can put your data at risk, as can Bluetooth devices. If your device has Wi-Fi and Bluetooth, make sure to configure them securely or disable them.

- Restricting Wi-Fi Access (see page 708)
- Disabling Bluetooth (see page 709)

Restricting Wi-Fi Access

Rationale

Using an unencrypted Wi-Fi network or falling for a rogue access point puts your users' data at risk. Enable strong encryption and restrict Wi-Fi access to a default network and optionally employ a whitelist of additional networks in order to prevent this.

Instructions

By default, Wi-Fi is not activated on IGEL OS. To activate it and preconfigure one or more allowed networks, follow these instructions:

1. In IGEL Setup go to **Network > LAN Interface > Wireless**.
2. Activate **Activate Wireless Interface**.
3. Do not activate **Enable wireless manager**, as this would give the user free choice of Wi-Fi networks.
4. Click **Apply**.
5. Go to **Network > LAN Interface > Wireless > Default Wi-Fi network**.
6. Check **Enable WPA Encryption**.
7. Enter the **Wireless network name (SSID)**.
8. Make authentication and encryption settings, see Default Wi-Fi Network in IGEL OS[87] in the IGEL OS Manual.
9. Click **Apply**.
10. If needed, add further networks under **Network > LAN Interface > Wireless > Additional Wi-Fi networks**.

87. https://kb.igel.com/en/igel-os/11.10.270/default-wi-fi-network-in-igel-os

Disabling Bluetooth

Rationale

If your device has a Bluetooth interface it may be used to access data. Disabling the interface reduces the risk of data theft.

Instructions

By default Bluetooth is deactivated on IGEL OS. Should you want to disable it at any time, do the following:

1. In the IGEL Setup go to **Devices > Bluetooth**.
2. Decativate **Bluetooth**.
3. Click **Apply**.

Using IGEL UD Pocket for BYOD Devices

The following document explains how you can ensure corporate security in a "bring your own device" (BYOD) model simply by using IGEL UD Pocket.

Rationale

Letting users access company resources with their own devices and software poses a security risk: These systems may have insecure configurations or even contain malware. In addition, company data should not be saved on users' private devices.

Instructions

->Use the IGEL UD Pocket. This ensures the use of secure and trusted software. As the UD Pocket does not access the device's mass storage, company data and private data will remain separated.

For details on the IGEL UD Pocket and on how to select it during the boot procedure, see IGEL UD Pocket Manual (see page 2112).

Secure Shell (SSH) Access to IGEL OS with Keys

IGEL OS has a built-in OpenSSH server that can be activated and configured via the Setup application. It lets you connect securely to the device over the network in order to issue commands or transfer files. While authentication can be done with a username-password combination, using a private-public key pair can increase convenience and/or security. This document describes how to generate and distribute the keys required.

- Generating the SSH Key Pair (see page 712)
- Distributing the Public Key with UMS (see page 714)
- Configuring SSH Access on the Device (see page 716)

Generating the SSH Key Pair

Prerequisites

- Linux/Unix operating system, typically on the administrator's workstation
- *OpenSSH* client software installed

Introduction

The following procedure will generate two keys:

- **Public key**: This key is distributed to all machines the administrator wants to connect to. It can be made public.
- **Private key**: This key stays on the administrator's machine and has to be kept secret.

  For the confidentiality of the encrypted connection to devices, it is essential to keep the private key secret.

  An easily understandable explanation of private and public keys can be found in a blog post by the programmer Blake Smith[88].

Generating the Key Pair

1. Open a terminal session on your workstation as the user who is going to make the SSH connections to the devices.
2. Issue the following command:
   `ssh-keygen`
3. When prompted for the location to store the key pair in, you can:
   - Hit return, which will accept the default file name `~/.ssh/id_rsa`

   Using the default name may overwrite existing SSH key pairs!

   - Enter an absolute file path and key file name of your choice `.`
4. When prompted for a passphrase, you can
   - Enter a passphrase (twice)

   A passphrase protects the private key file in case it gets into the hands of an attacker. On the other hand, it may be inconvenient to enter the passphrase for every connection.

   - Hit return in order to use no passphrase.

88. http://blakesmith.me/2010/02/08/understanding-public-key-private-key-concepts.html

This increases convenience because you will be able to log in without entering the passphrase. However, it weakens security: The private key file will be unprotected if it gets into the hands of an attacker.

Two files have been generated (default names):

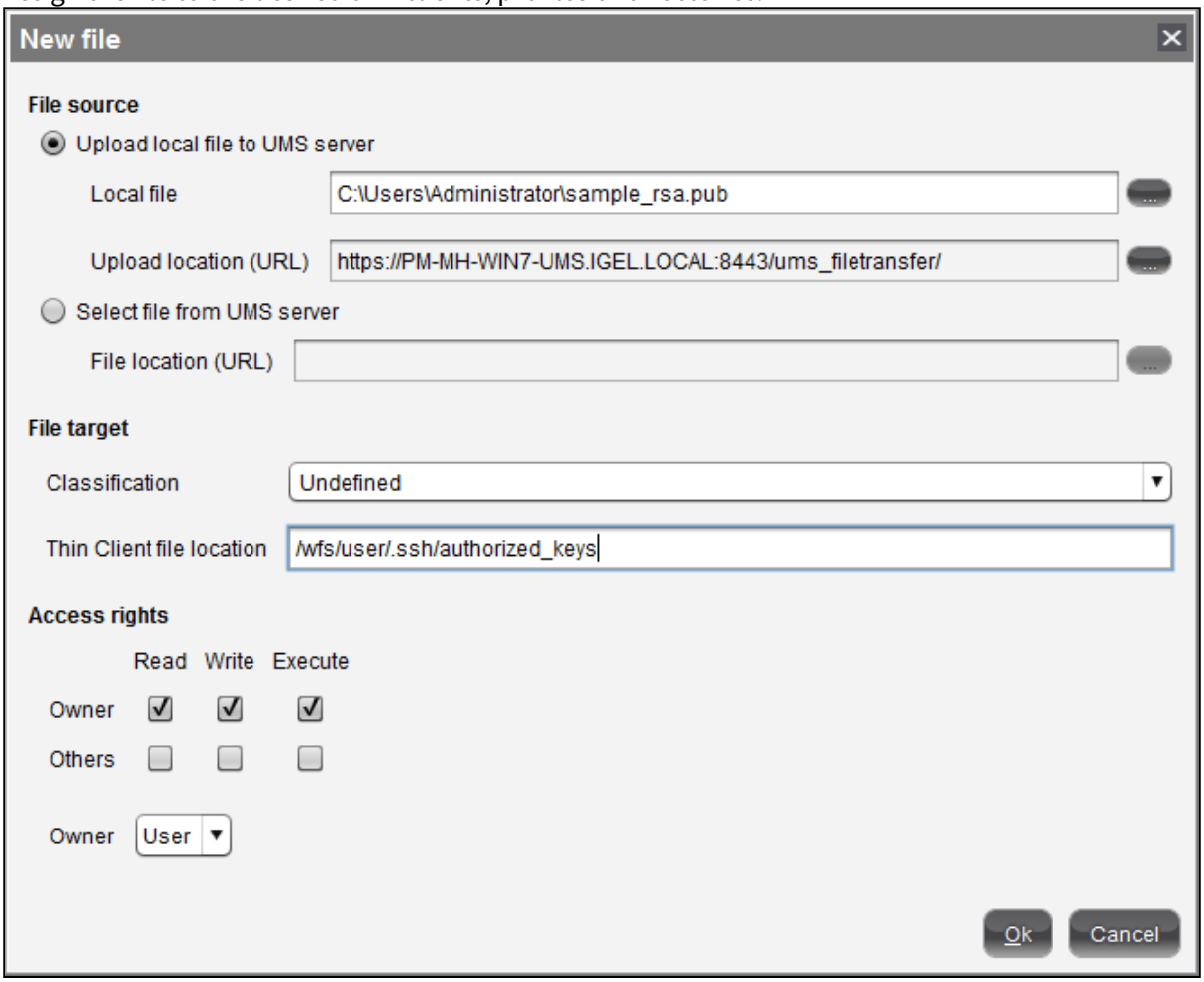
- `id_rsa` - the private key file
- `id_rsa.pub` - the public key file

Distributing the Public Key with UMS

1. In *UMS Console*, right-click on **Files** in the navigation tree.
2. Select **New File.**
3. Upload the public key file (`*.pub`) as a **Local File**.

> Make sure that you do not upload the private key file by mistake.

4. Set the **Classification** to **Undefined.**
5. Specify the **Thin Client file location** as `/wfs/user/.ssh/authorized_keys`
6. Leave the **Access rights** as **Read, Write, Execute.**
7. Leave the **Owner** as **User.**
8. Assign the file to the desired thin clients, profiles or directories.



If you wish to authorize more keys for SSH connections to thin clients, prepare an `authorized_keys` file containing all the public keys. Simply append them using a text editor.

Configuring SSH Access on the Device

1. Go to **System > Remote Access > SSH Access** in the IGEL Setup or a profile.
2. Check **Enable.**
3. Optionally, if `user` has an empty password, check **Permit empty passwords.**
4. Set **Deny** to **No** in the **User access** entry for **user**.

   > This configuration gives the remote user full shell access as if they were the local user on the client.

   Now you can connect to the device from the administrator's machine with the following command:

   ```
   ssh user@[client name or IP address]
   ```

   Depending on whether you set a passphrase for the key, you may have to enter it or not.

Secure Terminal (Telnet with TLS/SSL)

IGEL Linux version 5.11.100 or newer and IGEL Linux version 10.01.100 or newer allow terminal access via UMS with transport encryption. In analogy to secure shadowing (see page 718), network traffic is encrypted with TLS/SSL. Secure terminal connections can only be initiated from the UMS whose certficate is stored on the device.

For details about setting up a secure terminal connection, see UMS manual *Universal Management Suite > Universal Management Suite (UMS) > UMS Reference Manual > Devices > Secure Terminal (Secure Shell)*.

Secure Terminal is the best way to create a remote access from the UMS (on Linux or Windows installed) to Linux devices, without installing an additional terminal software. Because the UMS includes the software.

Secure Shadowing (VNC with TLS/SSL)

The **Secure Shadowing** function improves security when remotely maintaining a device via VNC at a number of locations:

- **Encryption**: The connection between the shadowing computer and the shadowed device is encrypted.
  This is independent of the VNC viewer used.
- **Integrity**: Only devices in the UMS database can be shadowed.
- **Authorization**: Only authorized persons (UMS administrators with adequate authorizations) can shadow devices.
  Direct shadowing without logging on to the UMS is not possible.
- **Limiting**: Only the VNC viewer program configured in the UMS (internal or external VNC viewer) can be used for shadowing.
  Direct shadowing of a device by another device is likewise not permitted.

In addition,*IGEL Management Interface (IMI) > IMI Manual* in Version 2 or newer provides an API for Secure Shadowing.

- **Logging**: Connections established via secure shadowing are recorded in the UMS server log.
  In addition to the connection data, the associated user data (shadowing UMS administrator, optional) can be recorded in the log too.

Of course, this is only relevant to devices that meet the requirements for secure shadowing and have enabled the corresponding option. Other devices can be "freely" shadowed in a familiar manner and, if necessary, secured by requesting a password. If you would like to allow secure shadowing only, you can specify this in the UMS Console under **UMS Administration > Global Configuration > Remote Access**[89].

- Basic Principles and Requirements (see page 719)
- Shadow Devices Securely (see page 720)
- VNC Logging (see page 721)

89. https://kb.igel.com/en/igel-os/11.10.270/remote-access

Basic Principles and Requirements

The **Secure Shadowing** option can be enabled if the following requirements are met:

- IGEL Linux as of version 5.03.190 and 10.01.100 or IGEL Windows Embedded Standard 7 from version 3.09.100
- IGEL Universal Management Suite from version 4.07.100 onwards
- The device is registered on the UMS Server
- The device can communicate with the UMS Console and UMS Server (see below)

Basic Technical Principles

Unlike with "normal" shadowing, the connection between the VNC viewer and the VNC server (on the device) is not established directly during secure shadowing. Instead, it runs via two proxies – one for the UMS Console and one for the VNC server on the device. These proxies communicate via a TLS/SSL-encrypted channel, while the local communication, e.g. between the VNC viewer application and the UMS proxy, takes place in the conventional unencrypted manner. As a result, a secure connection can also be established with external VNC programs that do not support TLS/SSL connections.

The two proxies (UMS Console and device) communicate with TLS/SSL encryption via the same port as the "normal" VNC connection: 5900. As a result, no special rules for firewalls need to be configured in order to perform secure shadowing.

If secure shadowing is active for a device under **Setup > System > Remote Access > Shadow > Secure mode**), the device generates a certificate in accordance with the *X.509* standard and transfers it to the UMS Server when the system is next started. The UMS Server checks subsequent requests for a secure VNC connection using the certificate. The certificate in PEM format can be found in the `/wfs/client-certs/tc_ca.crt` directory on the device. The validity of the certificate can be checked on the (Linux) client using the command: `x11vnc -sslCertInfo /wfs/client-certs/tc_ca.crt`

If a UMS administrator calls up the **Shadowing** function in the UMS Console for the device, the console receives a signed request from the UMS Server which is then passed on to the device to be shadowed. This in turn passes on the request to the UMS Server which checks the validity of the request using the original certificate. If this check is successful, the console reports that the channel for the connection between the proxies can be established. The UMS proxy on the console connects to the server proxy on the device, and the server proxy, in turn, establishes on the device the connection to its VNC server.

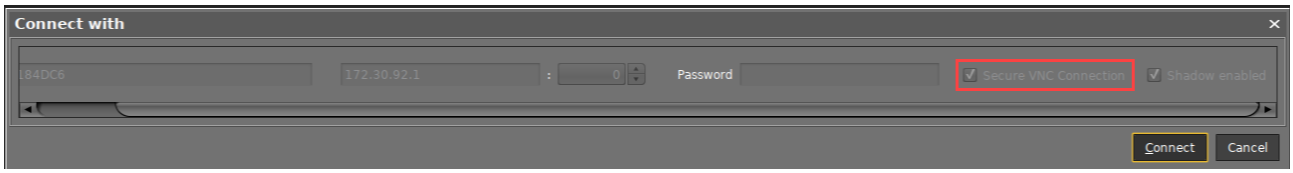
Only when these connections have been established, the console calls up the VNC viewer which then connects to the console proxy. The VNC client and VNC server are now connected via the two proxies which transfer data with TLS/SSL encryption.

Secure shadowing can be enforced independently of the device configuration for all devices that support this function: **UMS Administration > Global Configuration > Remote Access > Enable secure VNC globally**.

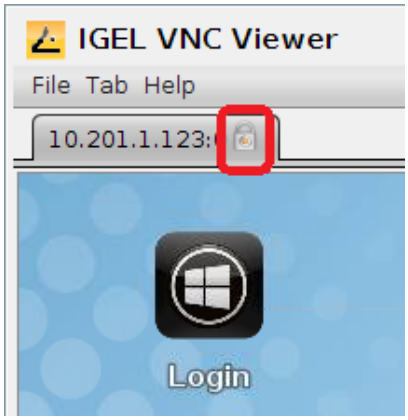
Shadow Devices Securely

In order to shadow a device securely (with encryption), the administrator must log on to the server via the UMS console. When doing so, it is irrelevant whether a purely local UMS administrator account is used or the user was adopted via an Active Directory for example. As always, however, the UMS administrator must have the permission to shadow the object, see Object-Related Access Rights under **Archive > UMS 6 PDF**.

The device to be shadowed is called up in the structure tree and, as usual, can be executed via **Shadow** in the context menu. The connection window, however, differs from the dialog for normal VNC shadowing. The IP and port of the client to be shadowed cannot be changed, and a password for the connection is not requested – this is superfluous after logging on to the console beforehand.



When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:



VNC Logging

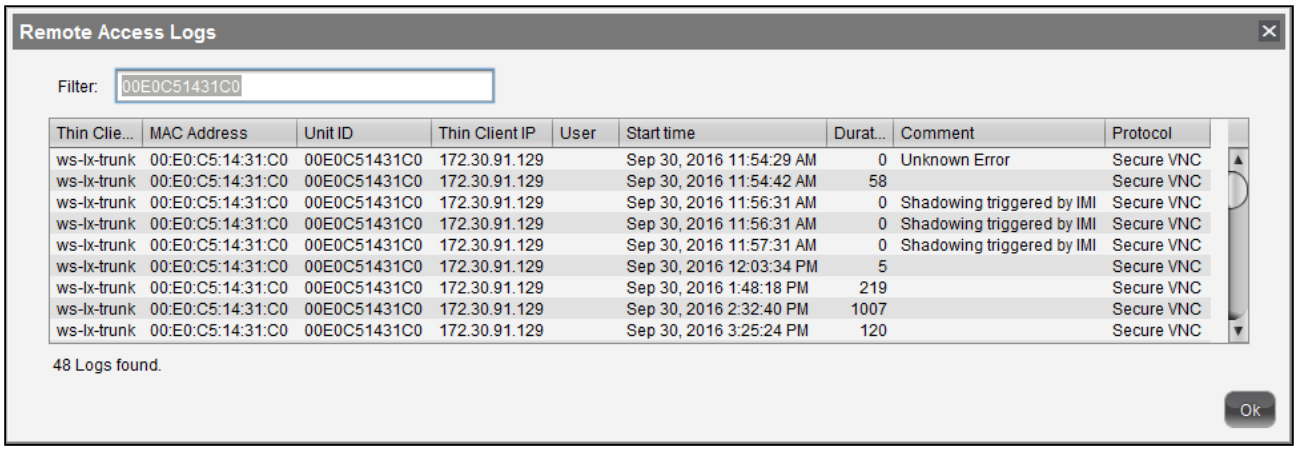
Connections via secure shadowing are always logged in the UMS. Via **UMS Administration > Global Configuration > Remote Access > Secure VNC**, you can configure whether the user name of the person shadowing is to be recorded in the log:

Log user for secure VNC

☑ The user name is included in the log.

☐ The user name is not included in the log. (default)

The VNC log can be called up via the **context menu** of a device or folder (for several devices, **Logging > Logging: Secure Access Logs**). The name, MAC address and IP address of the shadowed device, the time and duration of the procedure and, if configured accordingly, the user name of the shadowing UMS administrator are logged.



→ To sort the list (e.g. according to user names), click on the relevant column header or filter the content shown by making entries in the **Filter** field.

Cherry eGK Channel Substitution

As of firmware version 10.05.100, the Cherry eGK Channel is no longer available. In the Igel Universal Desktop Firmware, Linux V5, the VirtualChannel for Cherry eGK devices is still included parallel to the Cherry USB2LAN Proxy. If you want to continue using the G87-1504/ST-1503 as before, with firmware version 10.05.100 and higher you have to activate the proxy. All settings are automatically applied and run through the connector in the network.

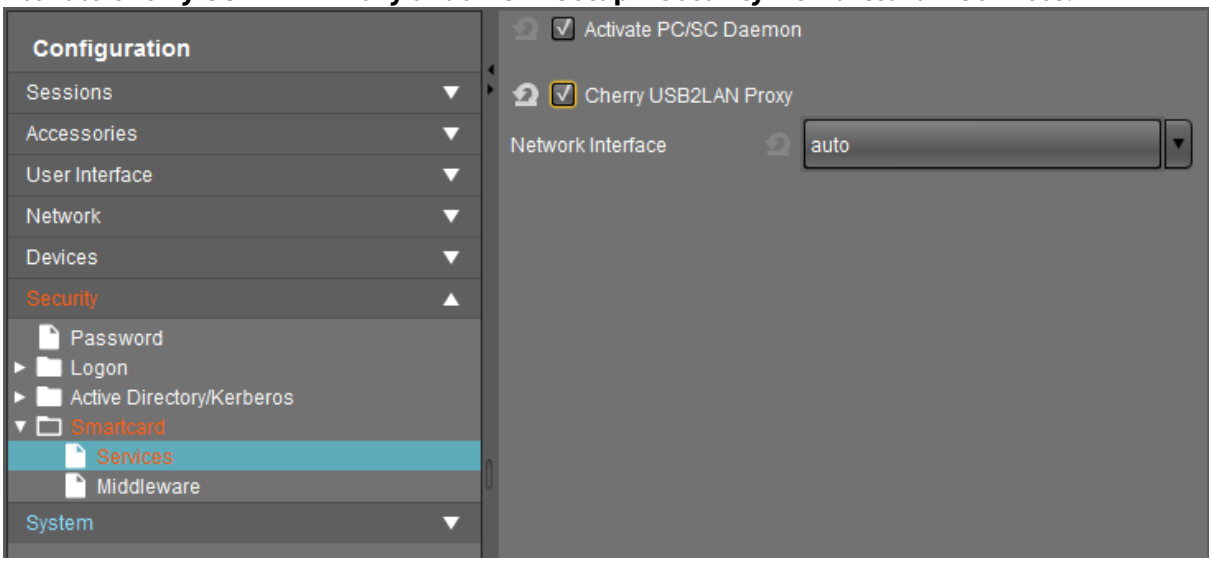
Using the G87-1504/ST-1503 with firmware version 10.05.100 and higher:

- Activate the proxy - this can also be done from the backend.

- Cherry USB2LAN Proxy (Under Smartcard) (see screenshot)
- IGEL device, valid for Cherry devices G87-1505, G87-1504/ST-1503 to USB

For IGEL Lx v5 and OS10:

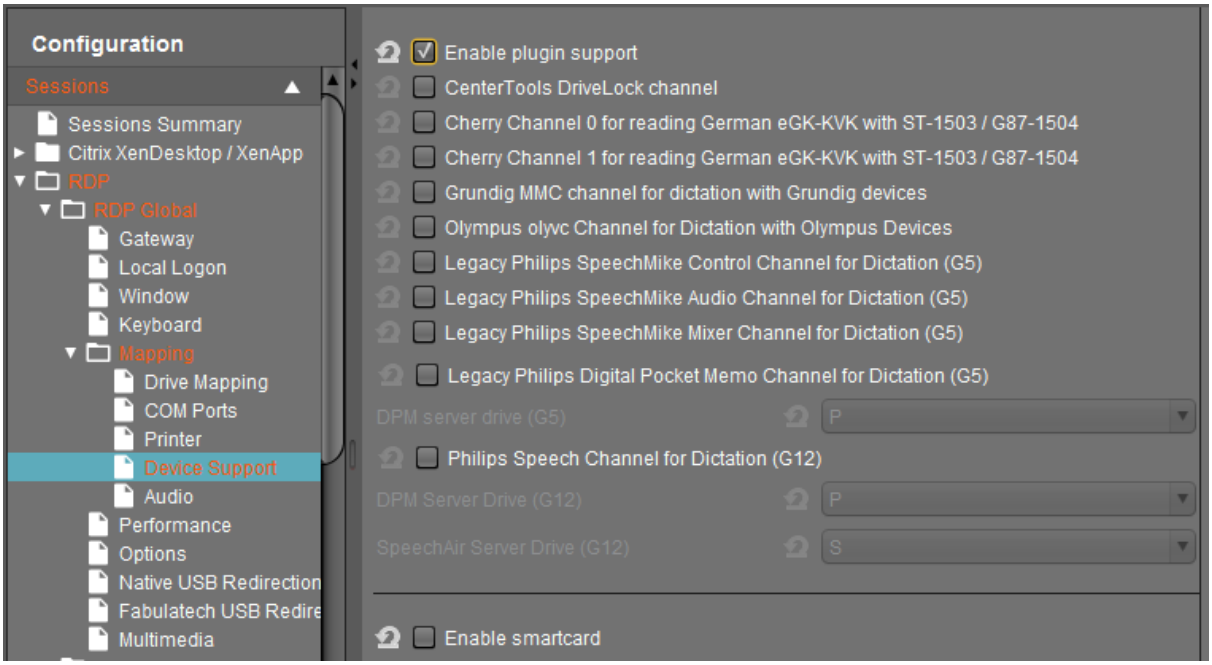
- Activate **Cherry USB2LAN Proxy** under **IGEL Setup > Security > Smartcard > Services**.



For IGEL Lx v5:

- Disable **Cherry Channel 0** and **Cherry Channel 1** under **IGEL Setup > Sessions > RDP > RDP Global > Mapping > Device Support**.

- Do not activate smartcard.



Install the Cherry eGK KVK software on the server. See https://www.cherry.de/files/software/Cherry-eGK-KVK_Software_33.zip

Install the Cherry Linux software on the device.

- In the CT-API configuration the G87-1504/ST-1503 can be configured as network device.
- Link to Doku Client Server Integration: https://www.cherry.de/files/manual/64410063-01_USBLANProxyClientServerUndCitrix.pdf
- Link to the software architecture documentation:: https://www.cherry.de/files/manual/Cherry-eGK-KVK_Sofware-Architektur_Windows-20130927-v04.pdf

The VirtualChannel was replaced due to the following difficulties and the future application of the telematics infrastructure (see also gematik anforderung lan)

- Independent of Citrix version (no need to check compatibility anymore)
- Independent of the server version (2008, 2012...), if the connection runs via RDP

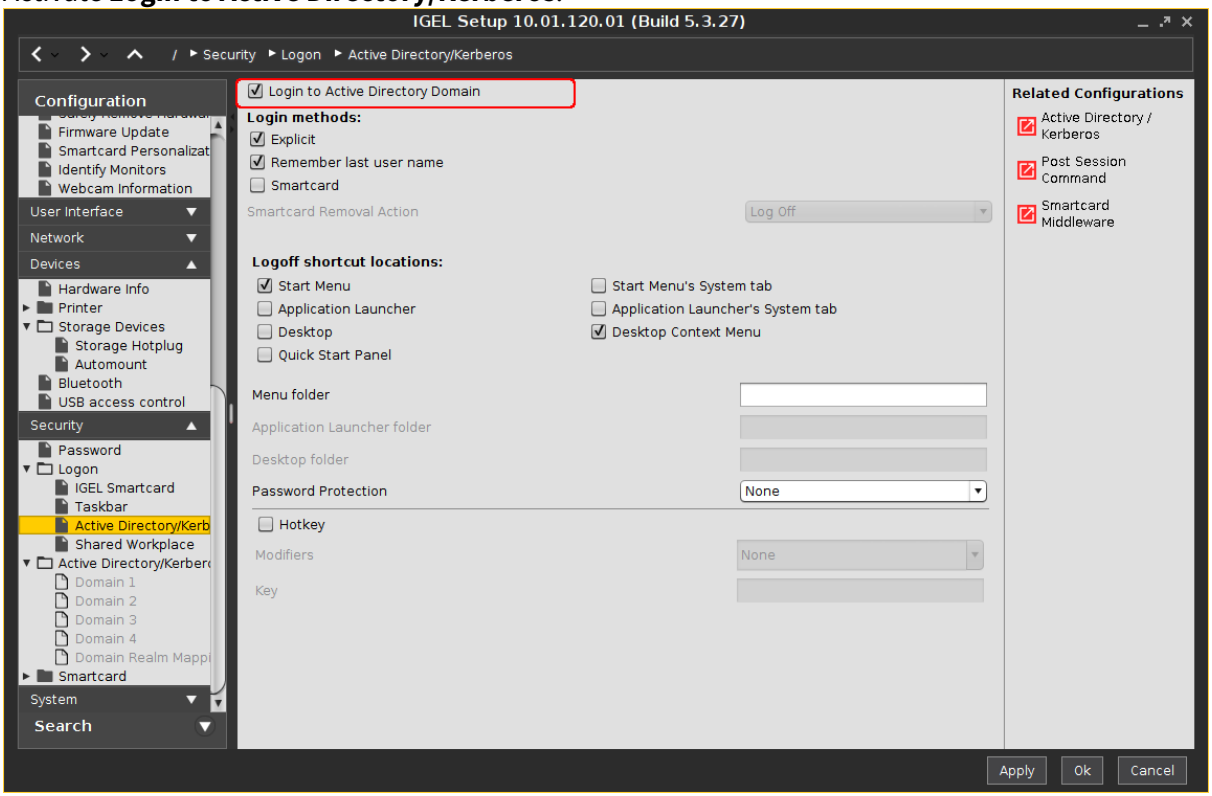
Single Sign-on for the Browser Proxy

Using a proxy to handle a browser's internet traffic provides additional security and control. However, if the proxy is password-authenticated, the user has to enter their credentials, which adds some inconvenience.

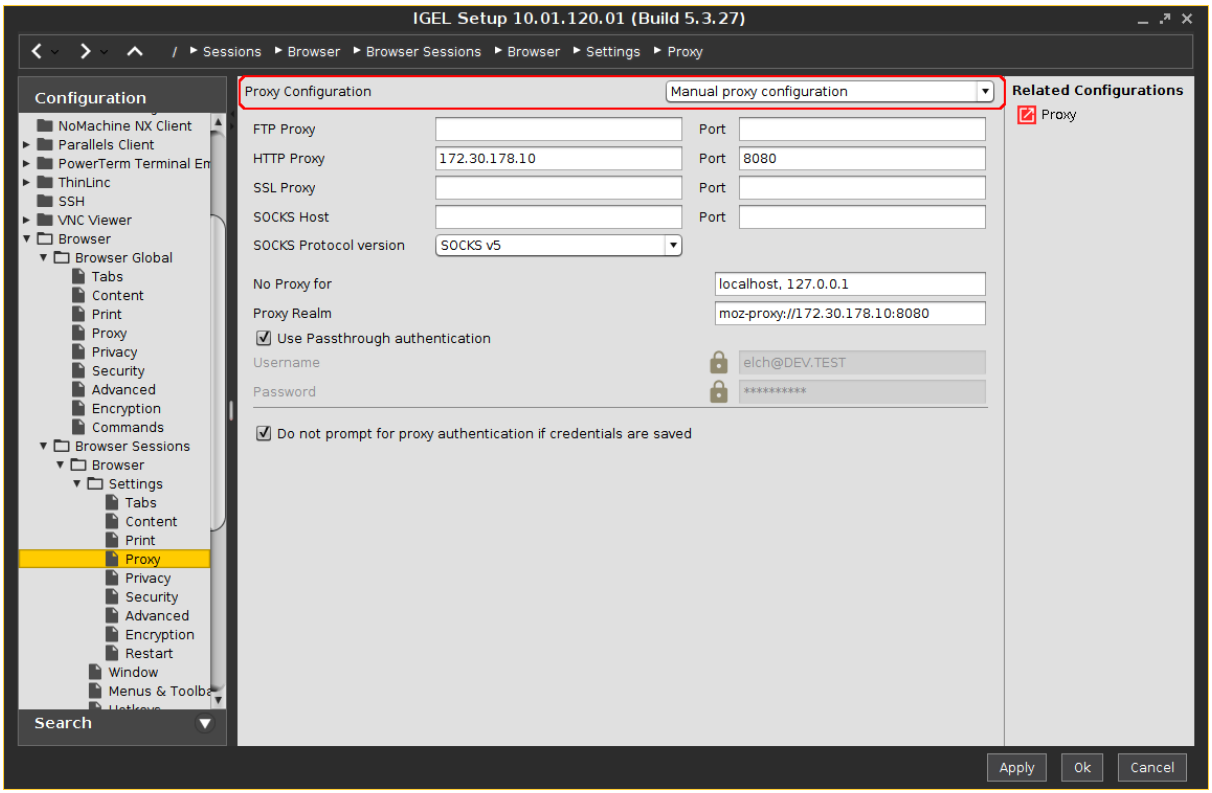
With IGEL Linux *version 5.08* or newer and IGEL Linux *version 10.01.100* or newer, you can avoid this inconvenience by using the passthrough feature. As a prerequisite, user logon must be carried out via Kerberos.

To enable single sign-on for the browser proxy:

1. Open the Setup and go to **Security > Logon > Active Directory/Kerberos**.
2. Activate **Login to Active Directory/Kerberos**.

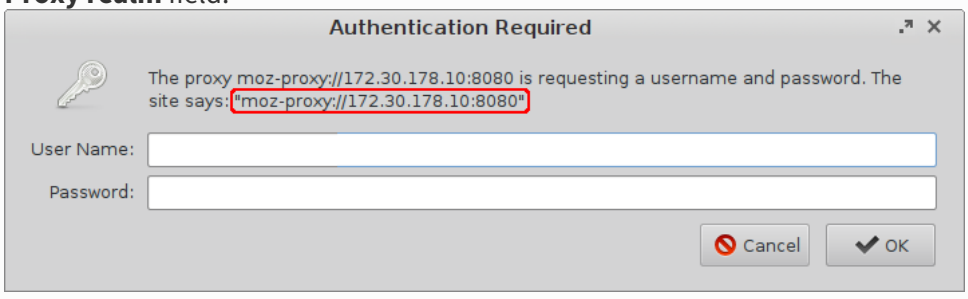


3. Go to **Sessions > Browser > Browser Sessions >** [name of the browser session] **> Settings > Proxy**.
4. In the **Proxy Configuration** choice, select **Manual proxy configuration**.



5. For an HTTP proxy, define the following settings:
   - **HTTP proxy**: IP address or hostname of the proxy to be used
   - **Port**: Port of the proxy for HTTP
   - **No proxy for**: IP addresses or hostnames of servers that can be accesses directly
   - **Proxy realm**: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

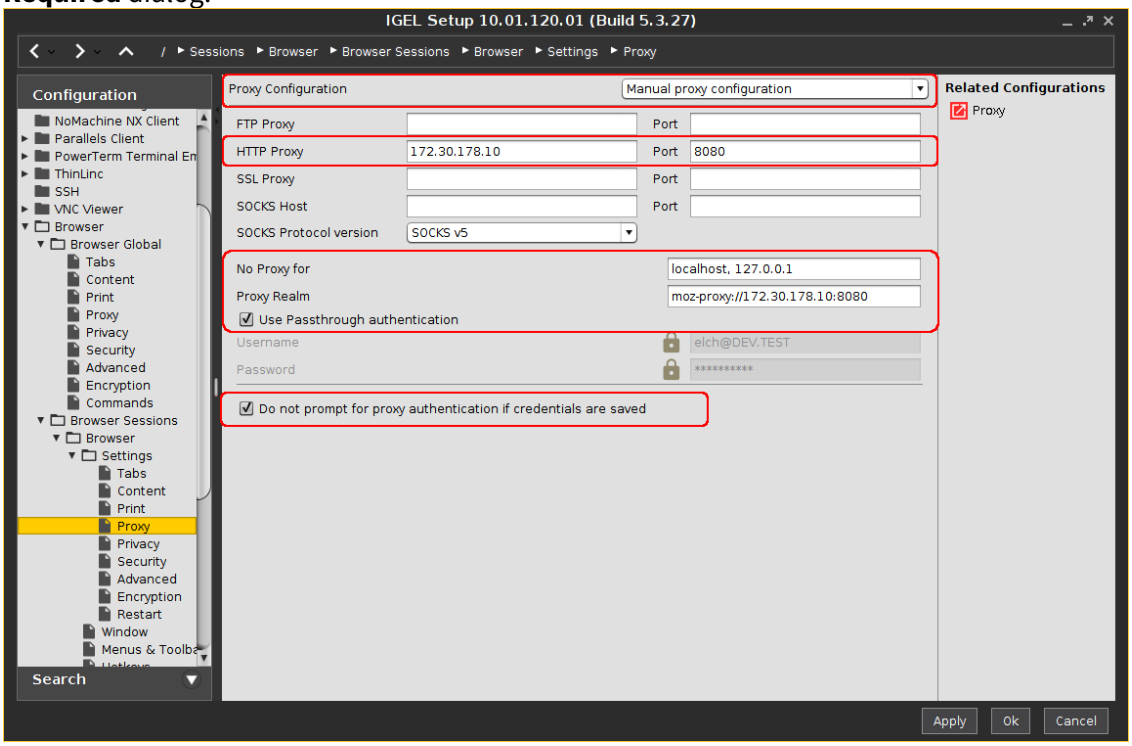
The **Proxy realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy]:[Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:



In the

example above, the value for the **Proxy realm** field is as follows: `moz-proxy://172.30.178.10:8080`

- **Use passthrough authentication**: Must be enabled to allow single sign-on for the browser proxy.
- **Do not prompt for proxy authentication if credentials are saved**: Must be enabled to enable seamless single sign on for the browser proxy; suppresses the **Authentication Required** dialog.



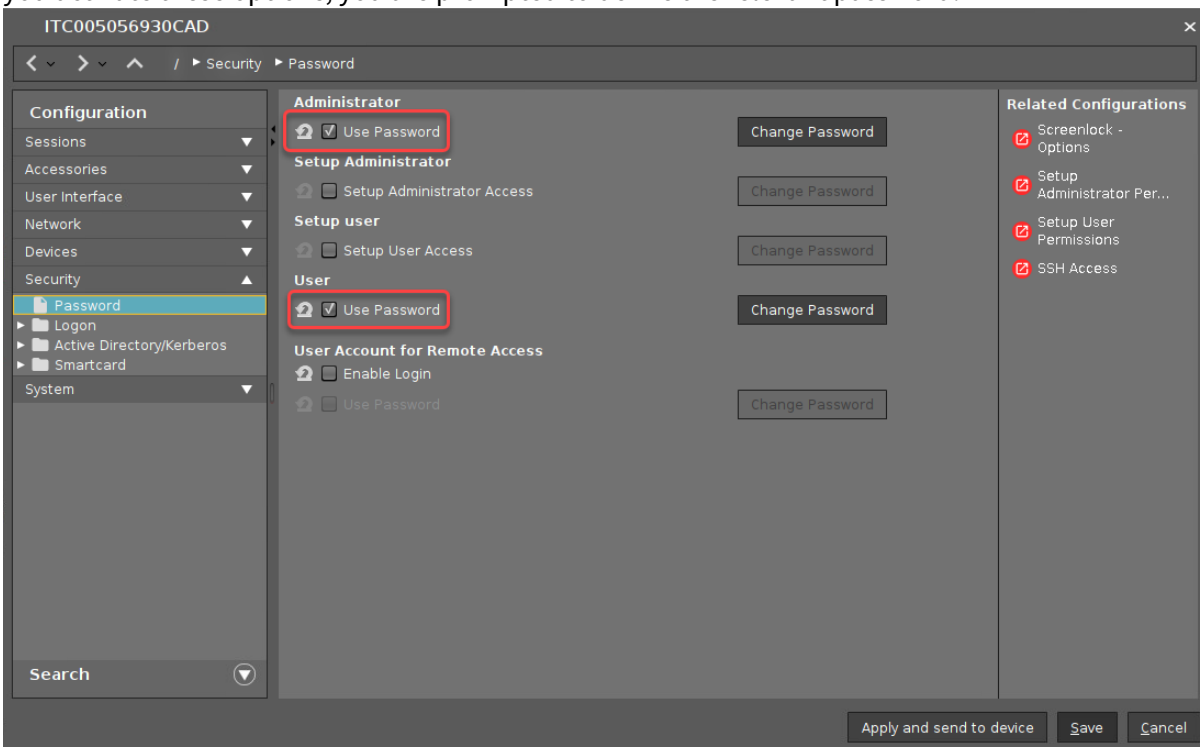
The next time the user logs in to the device, the browser proxy is ready to use.

Enforcing User Authentication at the Device

You can configure your device to require authentication by the user on each system start. This is possible both for the local user and for an Active Directory (AD) user.

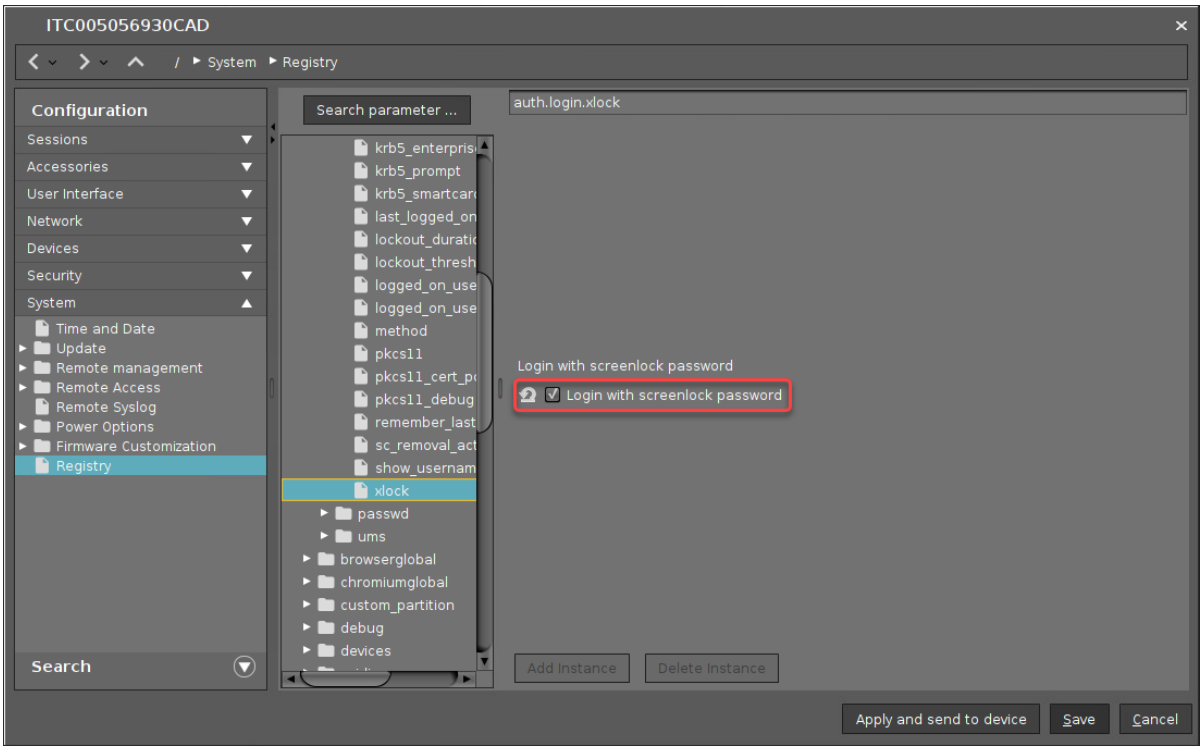
The following instructions describe the configuration for the local user. If you are using Active Directory, see Active Directory/Kerberos[90] in the IGEL OS Reference Manual (see page 1211).

1. Open the configuration dialog (UMS) or the local Setup.
2. Go to **Security > Password** and activate **Use Password** for the **Administrator** and the **User**. When you activate these options, you are prompted to define the relevant password.

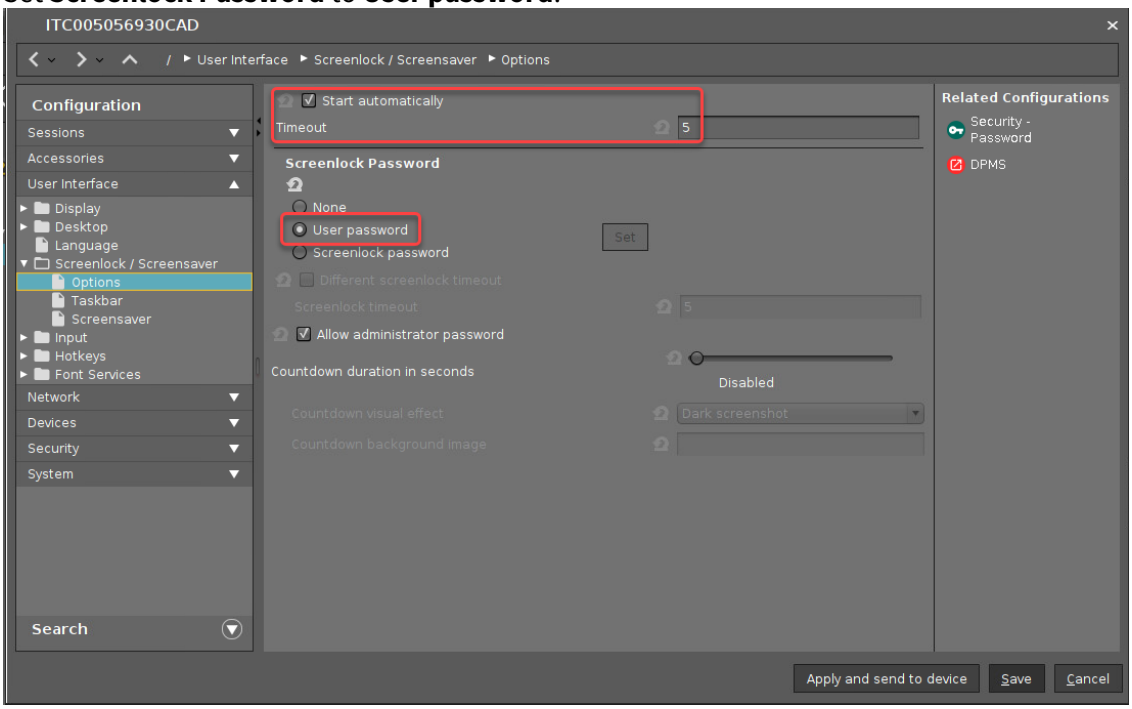


3. Go to **System > Registry > auth > login > lock** and activate **Login with screenlock password**.

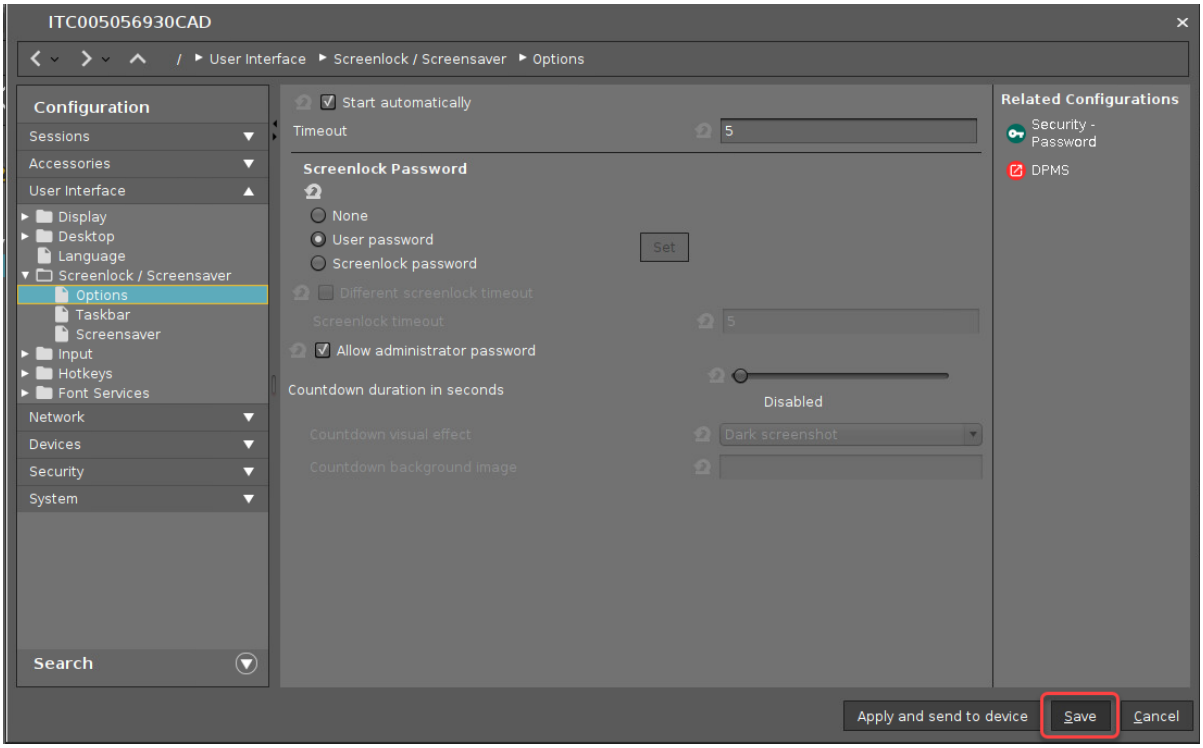
90. https://kb.igel.com/en/igel-os/11.10.270/active-directory-kerberos



4. If you want a screen lock after a defined time of inactivity, go to **User Interface > Screenlock / Screensaver > Options** and edit the settings as follows:
    - Activate **Start automatically**.
    - Set **Timeout** to the desired time of inactivity (in minutes).
    - Set **Screenlock Password** to **User password**.



5. Click **Save**.



6. To check if it works, reboot the device and. After reboot, the GUI should look like this:

local user
Password
local user
DE
11:38

Limiting the Number of Permitted Login Attempts

Symptom

Users can attempt logging in as often and as fast as they want at the screen unlock prompt and local login prompts (e.g. for Kerberos, Shared Workplace, IGEL Smartcard).

Problem

This leaves the system and remote sessions vulnerable to brute force login attacks.

Solution

In IGEL OS *10.03.100* and newer, the number of login attempts is limited to 5 within 30 seconds.

These values can be changed in the system registry:

1. In Setup, go to **System > Registry**
2. Go to the `auth.login.lockout_threshold` parameter to set the maximum number of login attempts within the specified interval.
3. Go to the `auth.login.lockout_duration` parameter to set the interval in seconds.
4. Click **Apply** or **Ok**.

How to Deploy Device Encryption

Overview

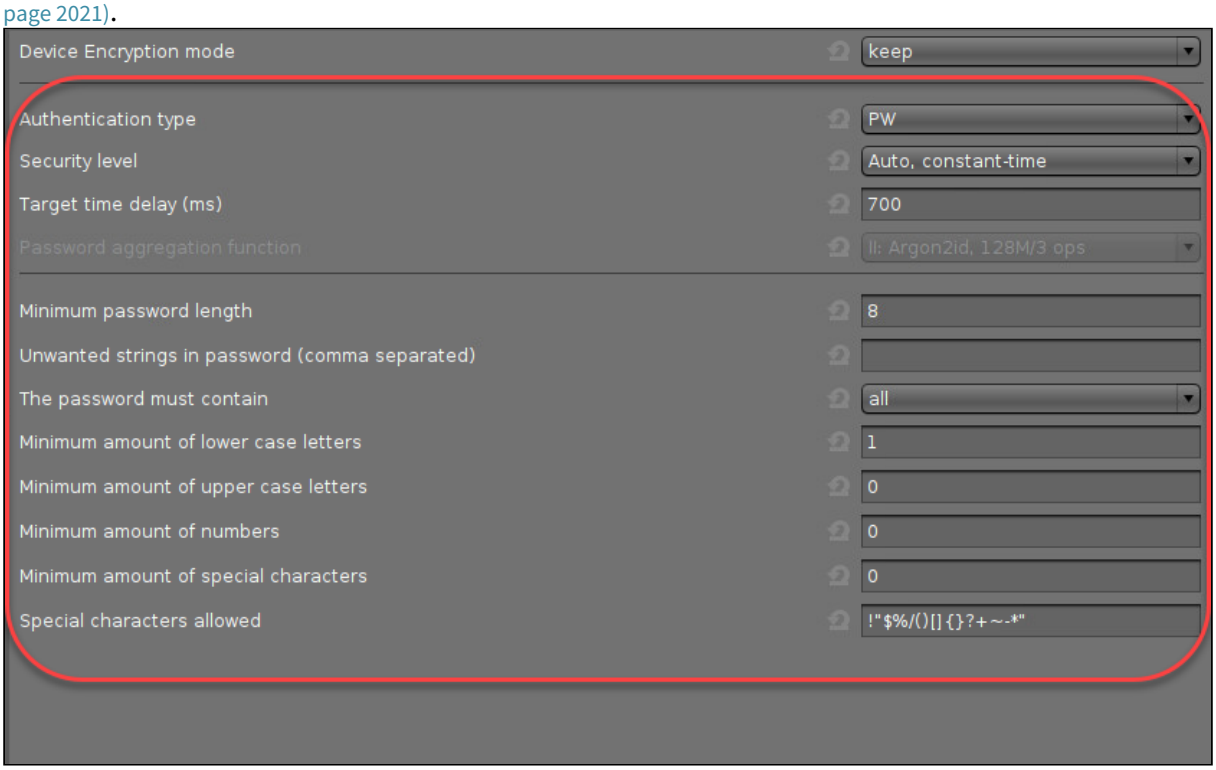
IGEL OS 11.06 or higher offers strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

Important Notes on Downgrading

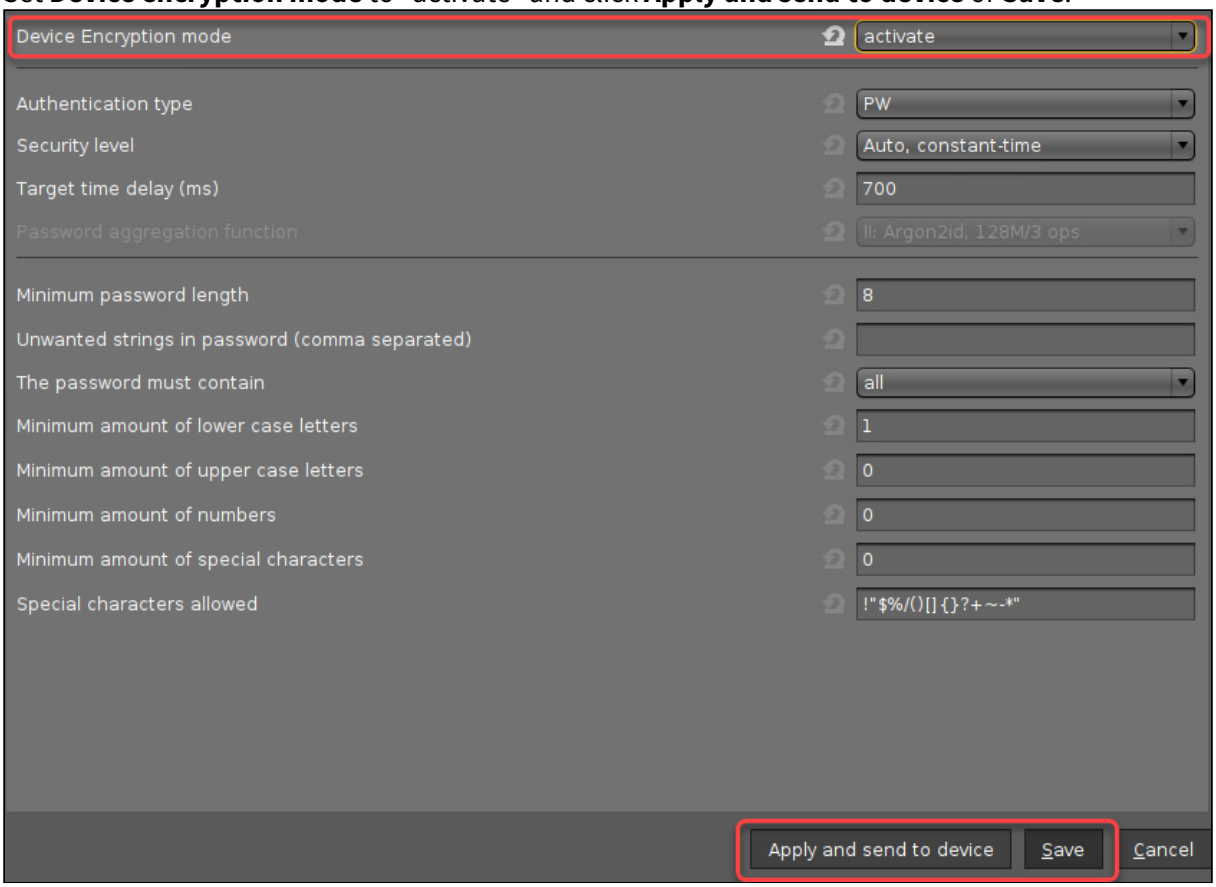
- If you have encrypted your IGEL OS 11.06 device, downgrading to IGEL OS 11.05 or lower will imply data loss on the following partitions, due to different partition schemes:
  - Browsing history of the browsers Firefox and Chromium
  - Custom Partitions
- The device settings and the UMS connection are preserved.
- The device encryption password must be entered by the user.

Instructions

1. In the UMS configuration dialog or the local Setup, go to **Security > Device Encryption**.
2. Set the parameters to meet your requirements. For details, see Device Encryption for IGEL OS (see page 2021).

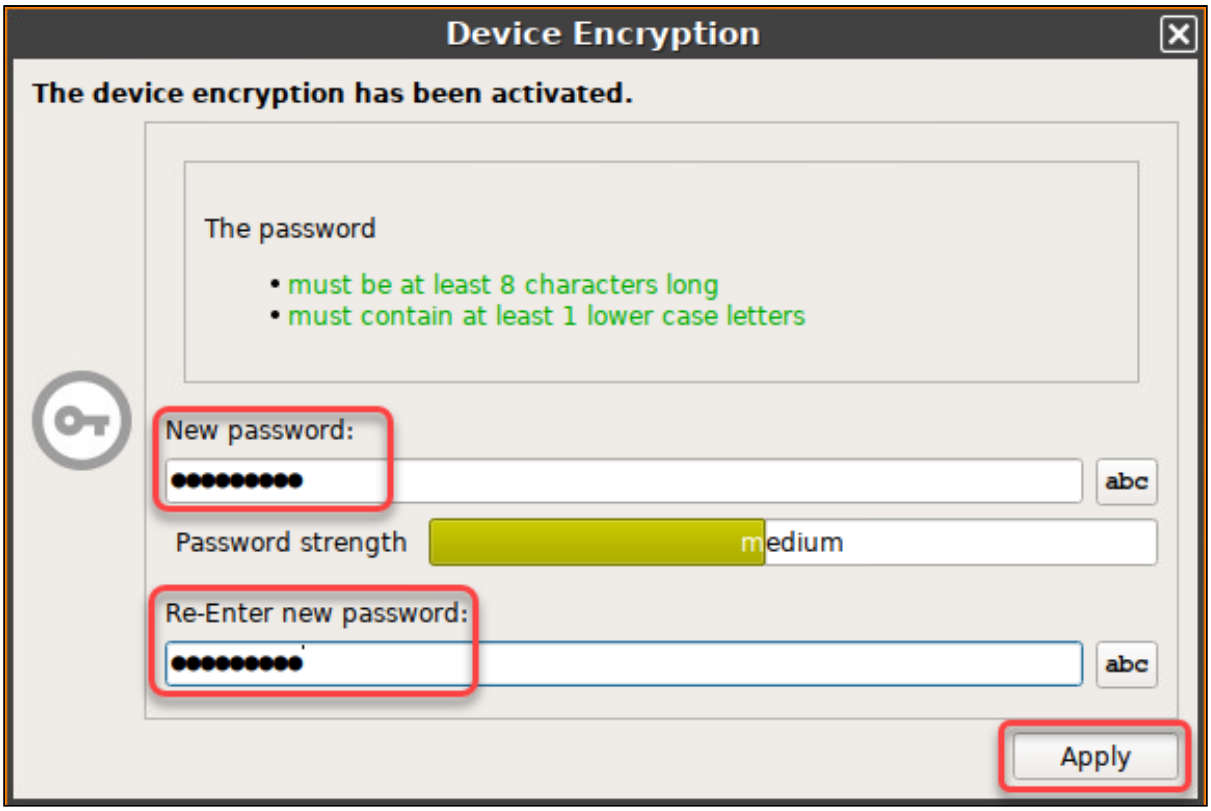


3. Set **Device encryption mode** to "activate" and click **Apply and send to device** or **Save**.



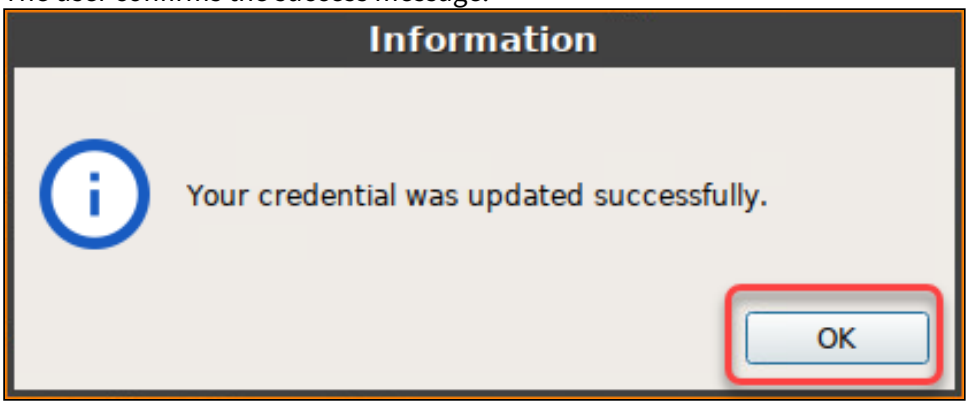
When the settings have been sent to the device, a password dialog is presented to the user.

4. The user enters an encryption password that meets the requirements and clicks **Apply**.



Several partitions are re-encrypted. This might take up to 60 seconds, depending on your hardware capabilities and the size of your Custom Partition.

5. The user confirms the success message.



6. On system start, the user must enter the device encryption password.

Device encryption is active
Press ENTER to log in.
Enter password
de_DE

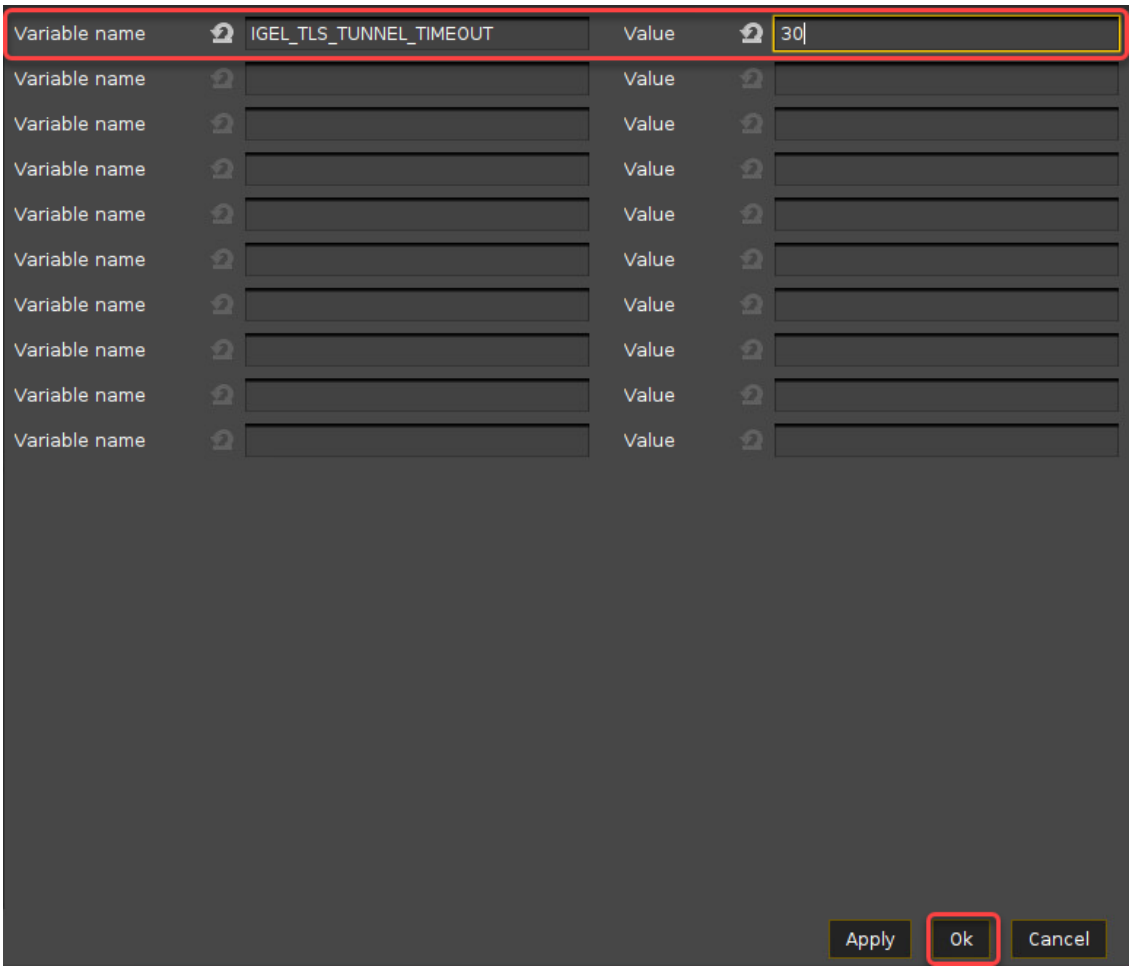
Security: Timeout for Secure Shadowing and Secure Terminal

Overview

To avoid a denial of service attack by blocking port 30022, which is used for secure shadowing (secure VNC) and secure terminal connections, a timeout can be configured. This timeout limits the establishing process for connections to port 30022. The duration is 180 seconds by default and can be changed via an environment variable.

Configuring the Timeout

1. Open the UMS configuration dialog or the local Setup and go to **System > Firmware Customization > Environment Variables > Predefined**.
2. Enter the following data and then click **Ok**:
    - **Variable name**: `IGEL_TLS_TUNNEL_TIMEOUT`
    - **Value**: Timeout in seconds. The range is 0 to180. When the value is set to 0, there will be no timeout.



Some services are restarted on the device. Afterward, the timeout is set.

Mitigate Terrapin Vulnerability through Registry Parameter in IGEL OS

To mitigate ISN 2023-39: SSH Terrapin Vulnerability (see page 738), you can enable a registry parameter that will disable weak MACs and Chipers to prevent terrapin attacks. For more information on terrapin attacks and the related CVE-2023-48795, see https://terrapin-attack.com/ and https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-48795.

> If you use OpenSSH 9.6p1 both on the client and server there is no need to use this registry parameter. IGEL OS versions 11.09.210 or higher use the latest OpenSSH 9.6p1. when you use this version or newer on the peer, they will automatically use the new "strict KEX" protocol extension.

To enable Terrapin mitigation through the registry parameter:

1. In IGEL Setup, go to **System > Registry > network > ssh_server > enable_terrapin_mitigation**.
2. Enable the parameter.
3. Click **Apply** or **OK** to save the change.

The following options vulnerable to Terrapin attack are disabled:

- the ChaCha20-Poly1305 cipher
- all -cbc ciphers
- all -ctr ciphers
- all -etm@openssh.com macs

> If you want to deactivate SSH completely, follow the instructions in Disabling SSH Access (see page 703).

Configuring IGEL OS11 NTLM Passthrough Authentication

Overview

This document describes, in exemplary fashion, the following Single Sign-On (SSO) scenario: The user logs on to Microsoft Active Directory/Kerberos via a smartcard that is connected to an IGEL OS endpoint device. Later on, the Firefox browser or the Zoom VDI client connects to a remote site via a proxy. This proxy offers NTML authentication as the only authentication method.

Because NTLM requires a password, and the non-interactive logon via smartcard does not provide a password, a replacement password has to be acquired. Both the Kerberos system of Active Directory and the endpoint device must be configured appropriately; Kerberos must send supplemental NTLM credentials encapsulated in a Kerberos service ticket, and the endpoint device must acquire and decrypt an appropriate service ticket at logon.

Environment

- Endpoint devices with IGEL OS 11.06 or higher
- IGEL Universal Management Suite (UMS) 6.08 or higher
- Smartcard reader
- Microsoft Active Directory
- Proxy with NTML authentication

Applications that Can Use the NTLM

- Firefox browser
- Zoom VDI client

Instructions

Creating a User Account in Active Directory

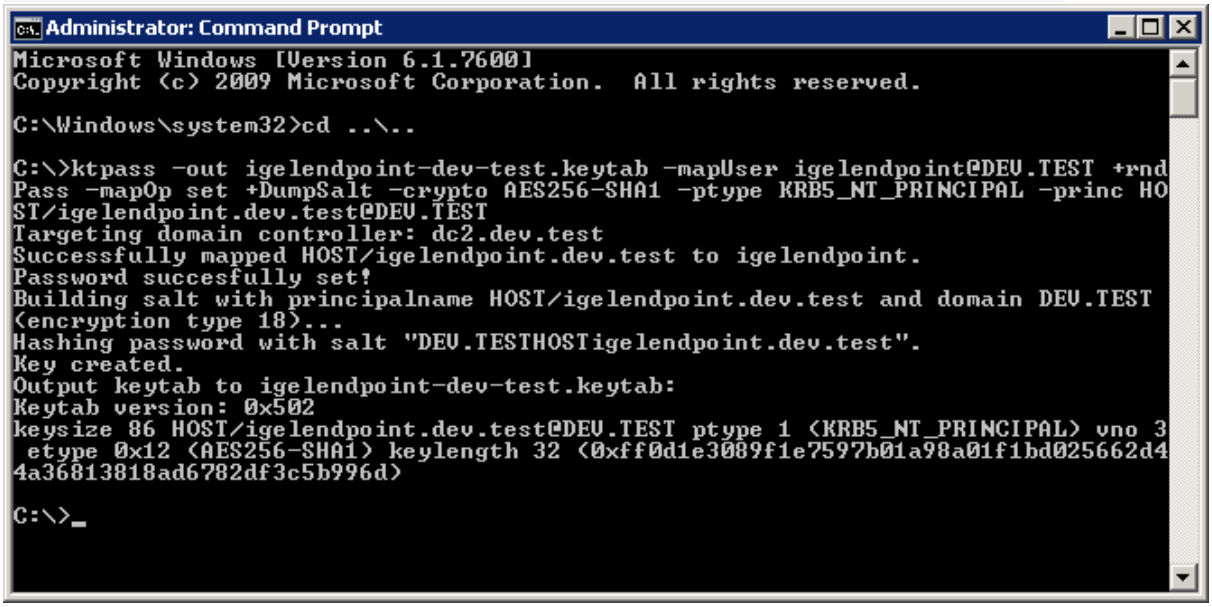
1. Create an Active Directory user account with a random logon name, e.g. "igelendpoint".
2. Set the following options for this account;
    - "Password never expires"
    - "This account supports Kerberos AES 256 bit encryption."

Mapping the Service Principal Name (SPN) and Creating a Keytab

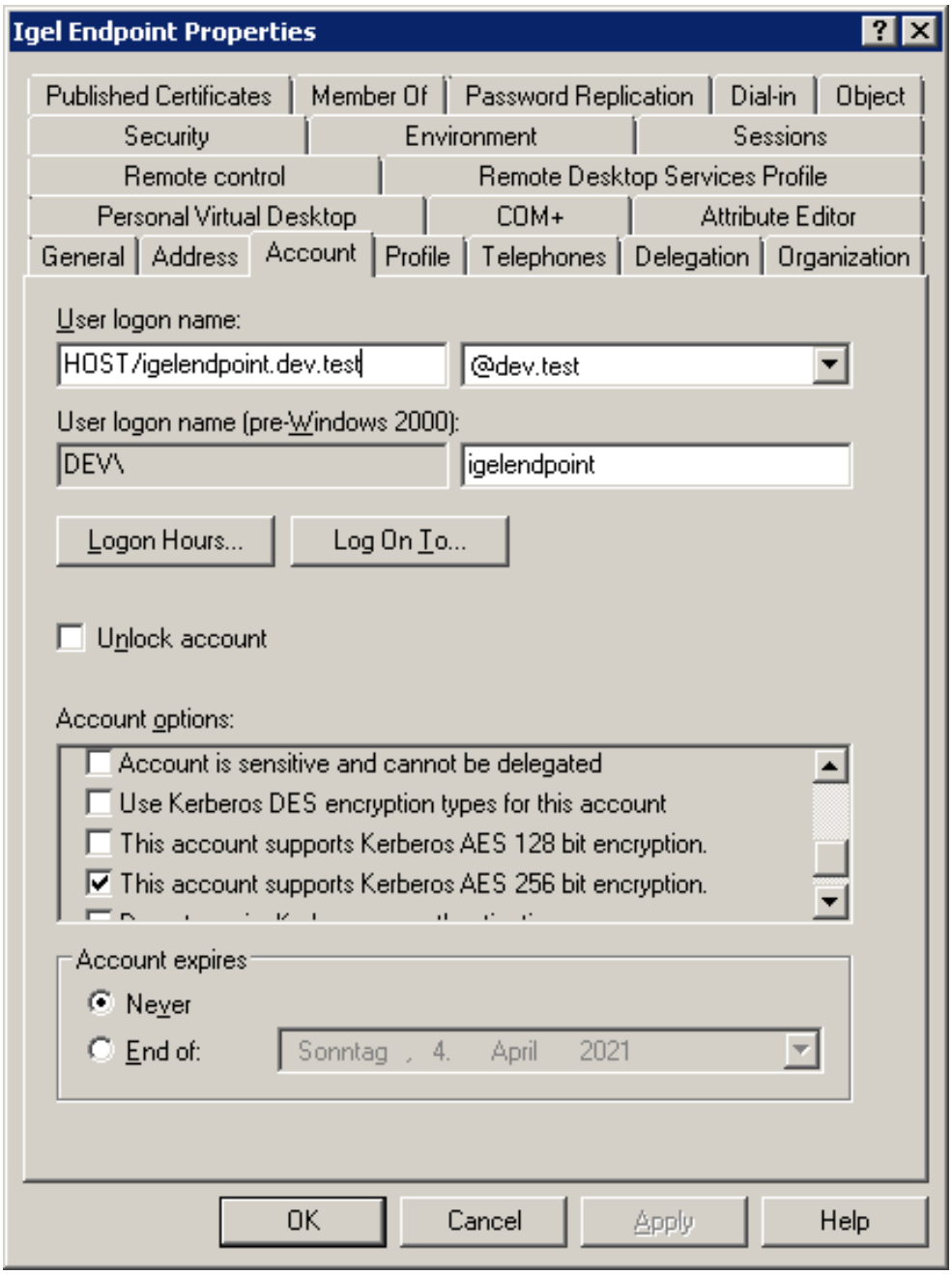
With the following procedure, you map the Service Principal Name `Host/igelendpoint.dev.test` to the user `igelendpoint@DEV.TEST`, set the password for the user `igelendpoint` to a randomized string, and export a keytab with an AES256-SHA1 key:

1. Open the command-line shell (`cmd.exe`) as Administrator.
2. Enter the following command:
   `ktpass –out igelendpoint-dev-test.keytab -mapUser` igelendpoint@DEV.TEST

```
 +rndPass -mapOp set +DumpSalt -crypto AES256-SHA1 -ptype
KRB5_NT_PRINCIPAL -princ HOST/igelendpoint.dev.test@DEV.TEST
```



3. Check the properties of your new AD user; the **User logon name** should have changed to the SPN name:



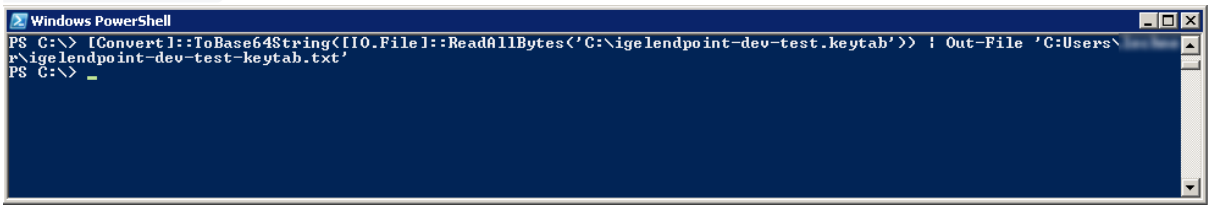
Encoding the Keytab in Base64

To transfer the binary key tab file to the UMS, you must encode it in Base64.

With the following procedure, you encode the binary keytab file `igelendpoint-dev-test.keytab` to `igelendpoint-dev-test-keytab.txt` with Windows PowerShell:

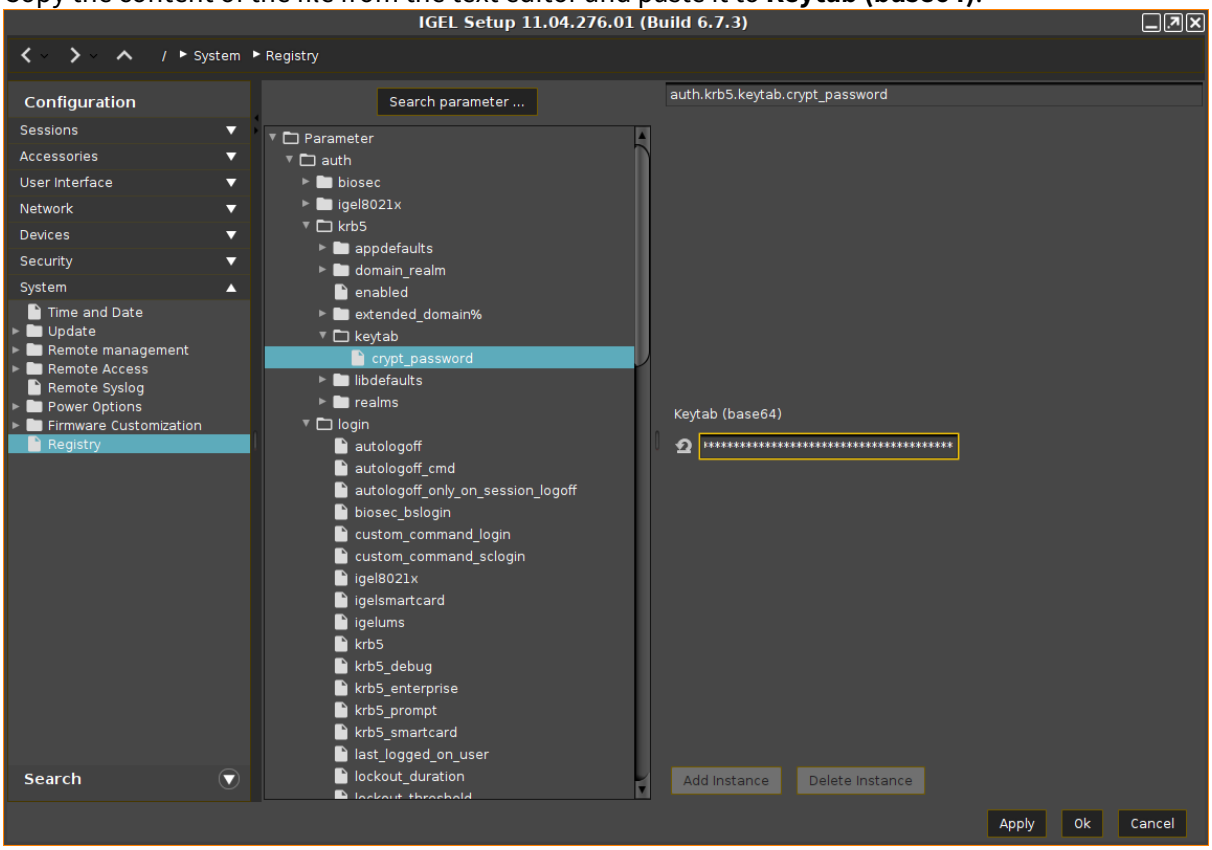
1. Open Windows PowerShell.

2. Enter the following command:
   `[Convert]::ToBase64String([IO.File]::ReadAllBytes('C:\igelendpoint-dev-test.keytab')) | Out-File 'C:\igelendpoint-dev-test-keytab.txt')`

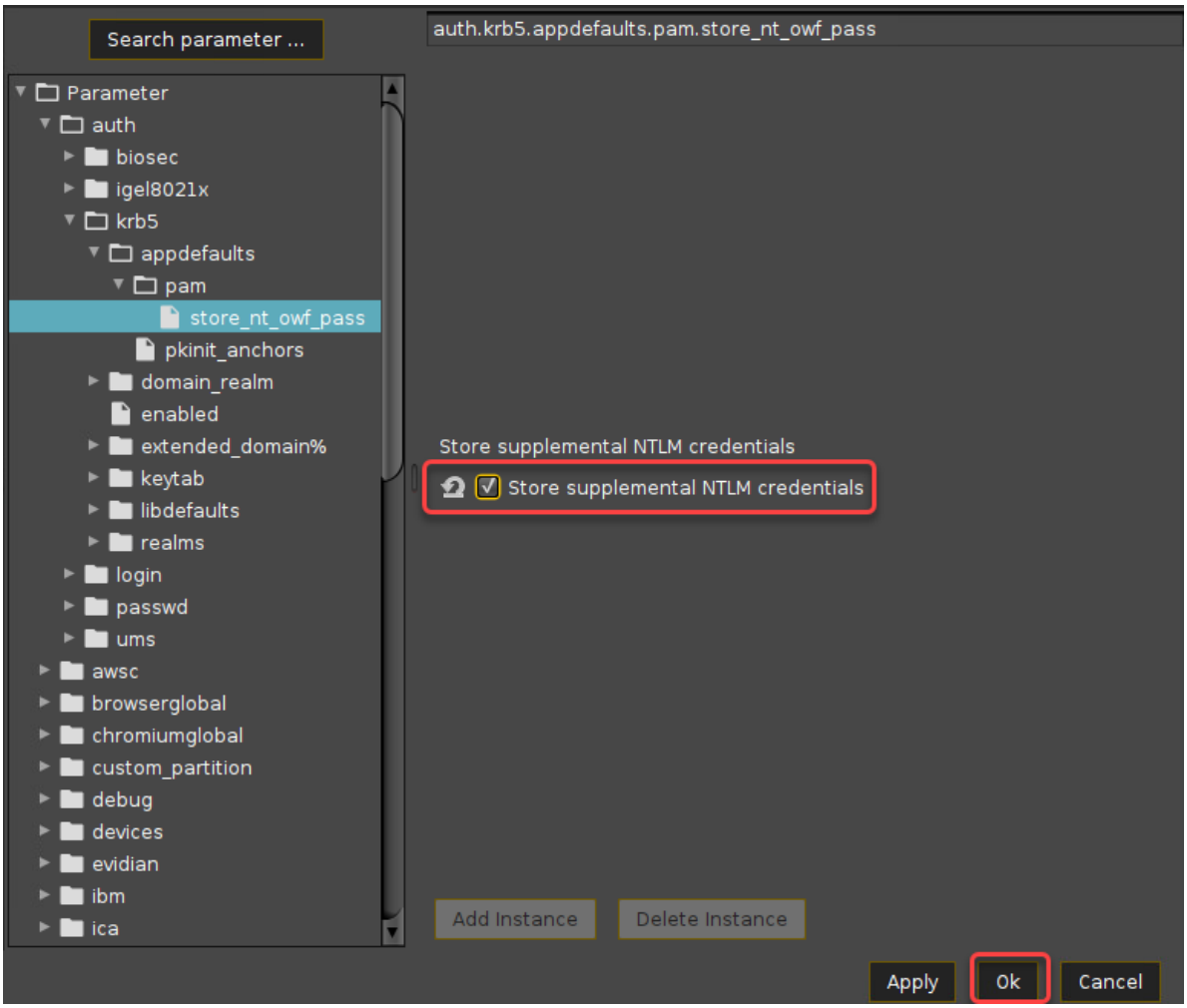


Transferring the keytab to the UMS

1. Open the UMS configuration dialog or the local Setup of your device and go to **System > Registry > auth > krb5 > keytab > crypt_password**.
2. Open the Base64 encoded keytab file (in our example: `igelendpoint-dev-test-keytab.txt`) with a text editor.
3. Copy the content of the file from the text editor and paste it to **Keytab (base64)**.



4. Go to **System > Registry > auth > krb5 > appdefaults > pam > store_nt_owf_pass** and enable **Store supplemental NTLM credentials**. and click **Ok**



5. Check if the NTLM passthrough authentication works as expected.

Certificates

- Certificate Enrollment and Renewal with SCEP (NDES) (see page 745)
- Deploying Trusted Root Certificates in IGEL OS (see page 764)
- Which CA Certificates Are Contained in IGEL OS? (see page 768)

Certificate Enrollment and Renewal with SCEP (NDES)

SCEP is a protocol for certificate management that supports the secure issuance of certificates to network devices.

Requirements

⚠ Applying Microsoft patch KB5014754[91] to your NDES server may break requests for certificates from clients using SCEP clients for authentication. This includes IGEL OS devices.
Currently, there is no official workaround or patch from Microsoft.

- SCEP server
  The following SCEP server implementations can be used with IGEL OS:
  - Windows 2008 Server with the Network Device Enrollment Service (NDES) role
  - Windows 2012 Server
  - Windows 2016 Server

  For information on how to deploy the NDES, see the Microsoft documentation[92].
- Connection between the SCEP server and the certification authority (CA).

This document explains the enrollment of certificates with SCEP.

- Client Enrollment Details (see page 746)
- Technical Background (see page 748)
- Configuration of the SCEP Client (see page 750)
- Files Involved (see page 759)
- Troubleshooting (see page 760)

91. https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16
92. https://learn.microsoft.com/en-us/archive/technet-wiki/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes

Client Enrollment Details

This section describes the actual certificate enrollment in detail. The process described here corresponds to step 7 to 10 in the overall process (see page 748).

The enrollment request and the response from the CA that contains the req

1. The client requests the CA's public certificate from the SCEP server.
2. The SCEP server sends the CA's public certificate to the client.
3. The client checks the CA's public certificate against the relevant fingerprint. The fingerprint has been provided by the administrator via a UMS profile; see Defining the Certification Authority (see page 755).
4. The client sends an enrollment request to the SCEP server. This enrollment request is an HTTP GET request that contains the following:

Signed data PKCS7	Enveloped data PKCS7	Certificate Signing Request (PKCS 10)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
Recipient and related encrypted data encryption key; the recipient is the CA.		
Encrypted data: (encrypted with a randomly generated key that is encrypted with the recipient's public key)	Version	
Requested subject name		
Public key of client		
Challenge password		
Requested extensions		
Signature algorithm		
Digital signature		
Client certificate		
Digital signature		

5. If the request was successful, the HTTP response from the SCEP server includes the following data:

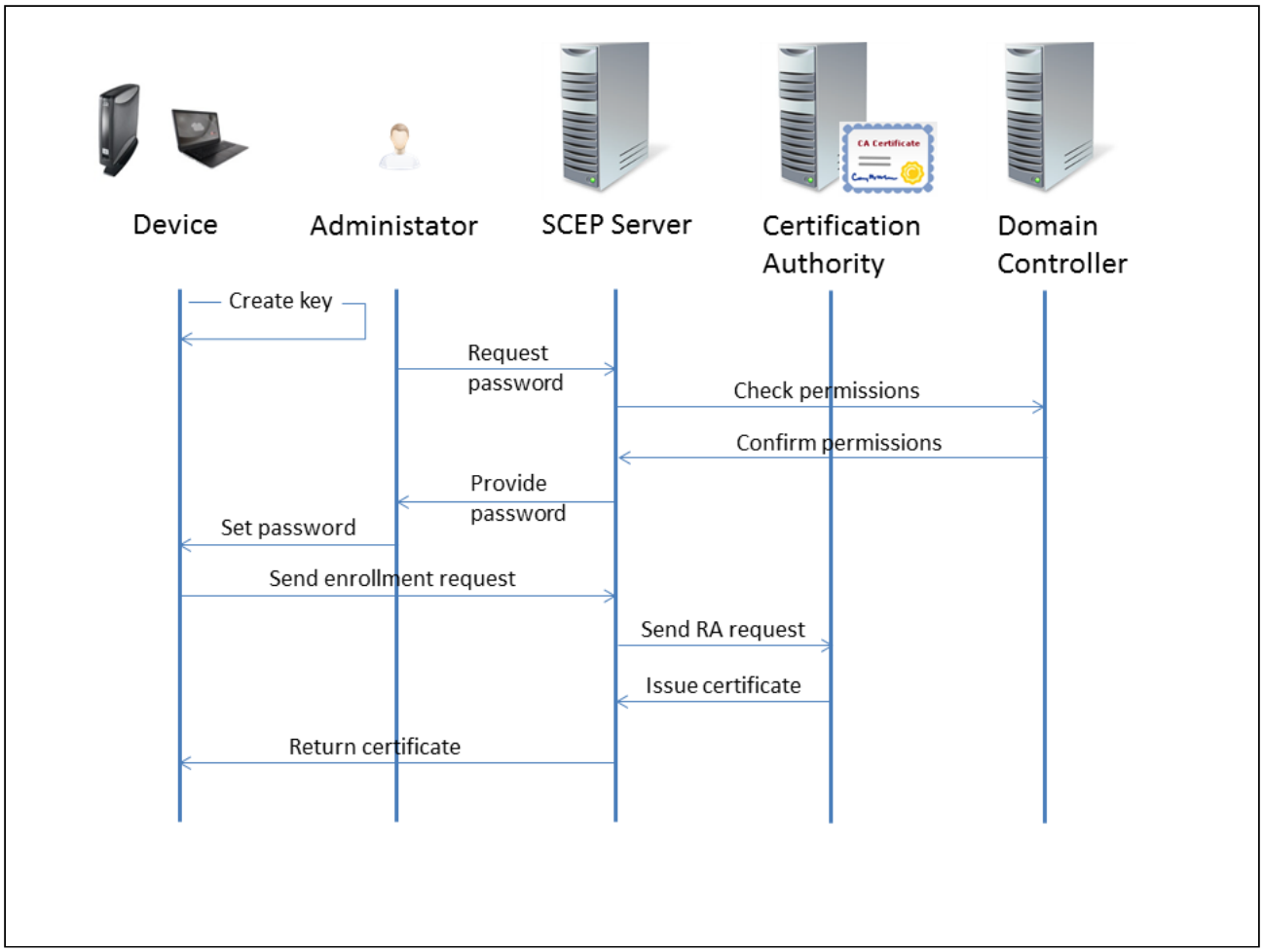
Signed data PKCS7	Enveloped data PKCS7	Degenerate Certificates (only PKCS7)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
List of recipients		
Encrypted data:	Version	
Issued X.509 certificate		
CA certificate		
Digital signature		

Technical Background

The Simple Certificate Enrollment Protocol (SCEP) defines a way of automatically enrolling certificates for the authentication of network devices or VPNs. The client uses HTTP requests to fetch root certificates, to send certificate requests, and to fetch client certificates from the server.

For an in-depth description, see the Microsoft documentation[93].

Here is a typical certificate enrollment process:



1. The device creates an RSA public-private key pair.
2. The administrator requests a challenge password from the SCEP service (e. g. NDES).

> The challenge password is only required for the first enrollment request. For certificate renewal, the current certificate is used for authentication.

93. https://learn.microsoft.com/en-us/archive/technet-wiki/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes

3. The SCEP server asks the domain controller if the administrator holds the required permissions for the configured certificate templates.
4. The domain controller confirms that the administrator holds the required permissions.
5. The SCEP server creates a challenge password and hands it over to the administrator.

> Typically, the challenge password expires after a defined time. With the NDES that is included in Windows 2008 Server, the default expiry time is 60 minutes.

6. The administrator provides the device with the challenge password, the CA identifier, and the fingerprint of the CA certificate.
7. The device sends the enrollment request to the SCEP server, using the challenge password to authenticate with the SCEP server. This action is triggered by the administrator.
8. The SCEP server signs the enrollment request with its enrollment agent certificate and sends it to the CA.
9. The CA issues the desired certificate and returns it to the SCEP server.
10. The SCEP server returns the certificate to the device.

Configuration of the SCEP Client

The configuration of the SCEP client on the IGEL OS device is carried out as follows:

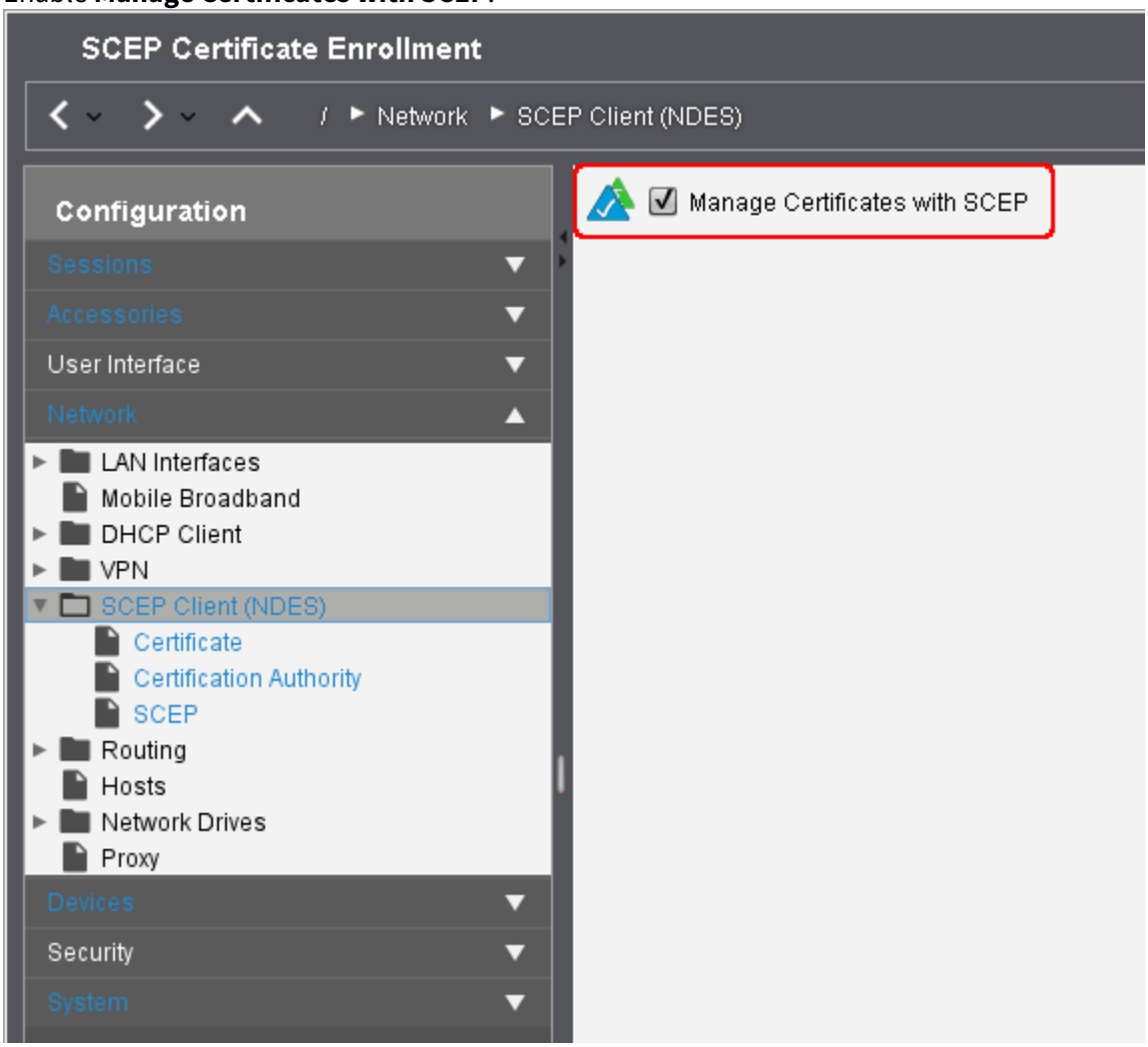
- Creating a Profile in the UMS (see page 751)
- Activating the SCEP Client (see page 752)
- Entering the Data for the Certificate Signing Request (CSR) (see page 753)
- Defining the Certification Authority (CA) (see page 755)
- Providing the SCEP Server Data (see page 756)
- Applying the Profile to the Devices (see page 757)

Creating a Profile in the UMS

1. In the UMS structure tree, go to **Profiles**, open the context menu and select **New Profile**.
2. Enter an appropriate **Profile Name**.
3. In the **Based on** menu, select the firmware version that is installed on the devices in question.
4. Click **OK**.
   The configuration dialog opens. The configuration dialog corresponds to the IGEL Setup available on the devices to which the profile is assigned.

Activating the SCEP Client

1. Go to **Network > SCEP Client (NDES)**.
2. Enable **Manage Certificates with SCEP**.



Entering the Data for the Certificate Signing Request (CSR)

→ Go to **Network > SCEP Client (NDES) > Certificate** and enter the following data:

Type of CommonName/SubjectAltName: The characteristic for linking the certificate to the device.

- IP address: The IP address of the device.
- DNS name: The DNS name of the device.
- IP address (auto): The IP address of the device (inserted automatically).
- DNS name (auto): The DNS name of the device (inserted automatically).
- Email address: An email address.
- DNS name as UPN (auto)

If the client automatically obtains its network name, **DNS Name (auto)** is a good type for the client certificate.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**:

CommonName/SubjectAltName: Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**:

CommonName/SubjectAltName Suffix: Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- "none": No suffix will be added.
- "dot + DNS domain (auto)": The system's current DNS domain name separated with a dot will be added. Example: `.igel.local`
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
  - `%D` is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: `@%D` will be changed into `@igel.de` if the system's current DNS domain name is `igel.de`.
  - %% will be replaced by %. Example: `A%%B` will be changed into `A%B`.
  - Other combinations with % are currently discarded. Example: `A%BC` will be changed into `AC`.

If you have to specify the suffix manually, make sure you enter the separator.

Organizational unit: Stipulated by the certification authority.

Organization: A freely definable designation for the organization to which the client belongs.

Locality: Details regarding the device's locality. Example: "Augsburg".

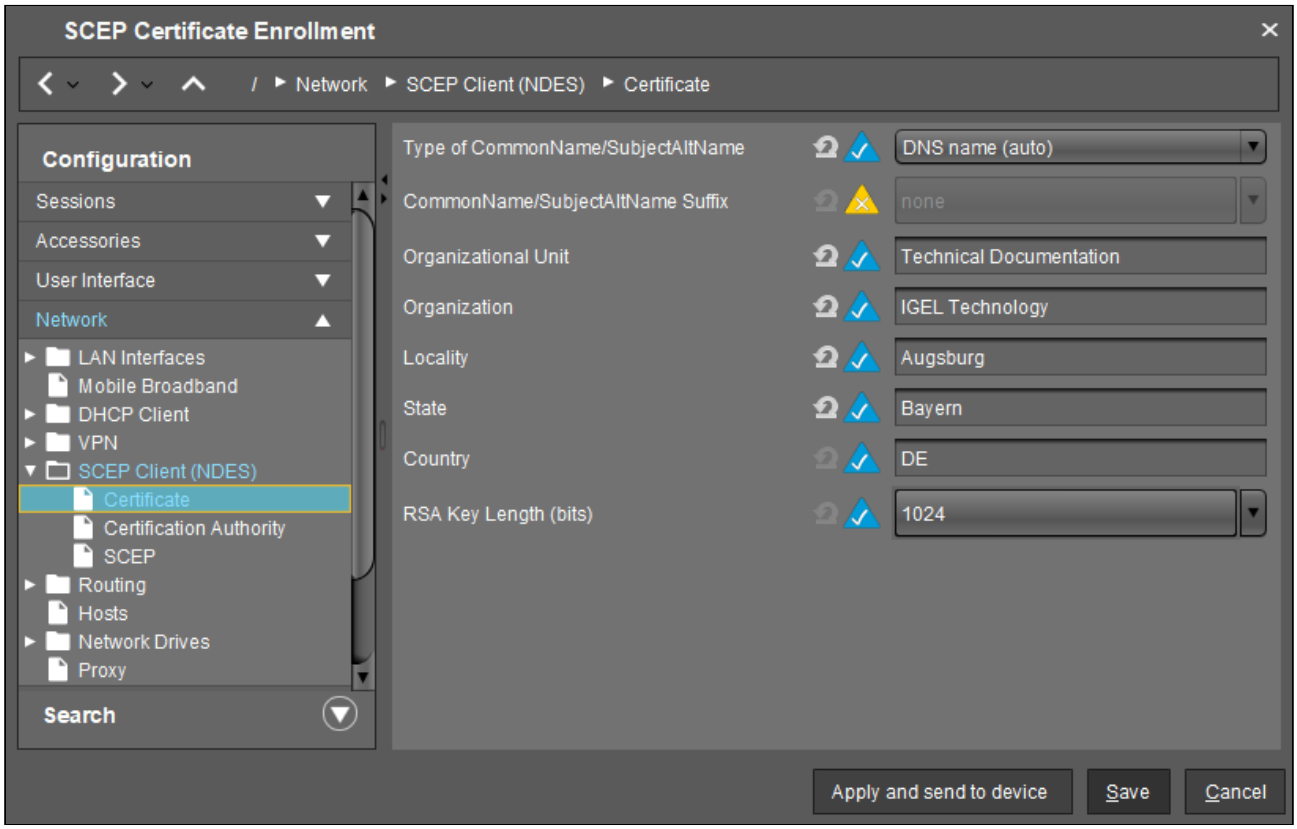
State: Details regarding the device's locality. Example: "Bayern".

Country: Two-digit ISO 3166-1 country code. Example: "DE".

RSA key length (bits): Select a key length (one suited to the certification authority) for the certificate that is to be issued.
Possible values:

- "1024"
- "2048"
- "4096"

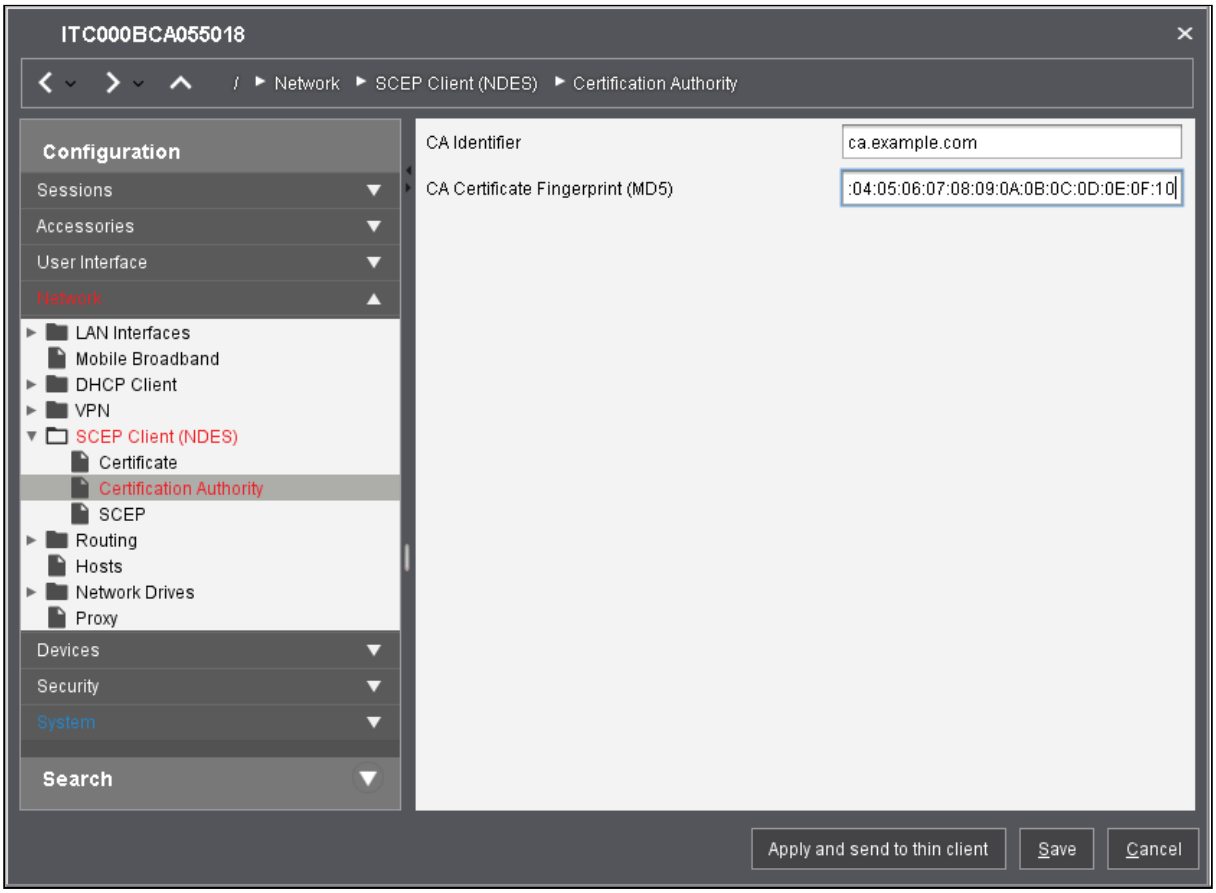
The RSA key length specified here must not be lower than the minimum key length configured on the server.



Defining the Certification Authority (CA)

1. Go to **Network > SCEP Client (NDES) > Certification Authority**.
2. Enter the details for the certification authority (CA):
   - **CA Identifier**: FQDN (fully qualified domain name) of the CA
   - **CA Certificate Fingerprint (MD5)**: Fingerprint of the CA certificate in the form `01:02:03:04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10`

> You can get the fingerprint from your NDES server: `https://<NDES Servername>/certsrv/mscep_admin`



If the CA certificate fingerprint is specified, the client will use it to check the integrity of the CA certificate it receives from the SCEP server.

Providing the SCEP Server Data

1. Go to **Network > SCEP Client (NDES) > SCEP**.
2. Enter the following data:
   - **SCEP server URL**: URL by which the SCEP client communicates with the SCEP server.

   > HTTPS is not supported; however, all security critical data that are transferred between the SCEP client and other components are encrypted.

   - **Proxy server for SCEP requests** (optional): IP address or host name of the proxy server that is used for the communication between the device and the SCEP server. If a web application firewall is used instead of a proxy, its IP address or host name of the proxy server must be entered here.
   - **Challenge password**: Password that the SCEP client must present to the SCEP server in its request (CSR).

   > On a Microsoft NDES server, you can retrieve the password by default under `https:///certsrv/mscep_admin`.

   > By default, the password on a Microsoft NDES server is valid for 1 hour and can be used only once. In order to use the password on numerous devices, additional settings must be made on the NDES server. For information, see the section "Password and Password Cache" on https://social.technet.microsoft.com[94].

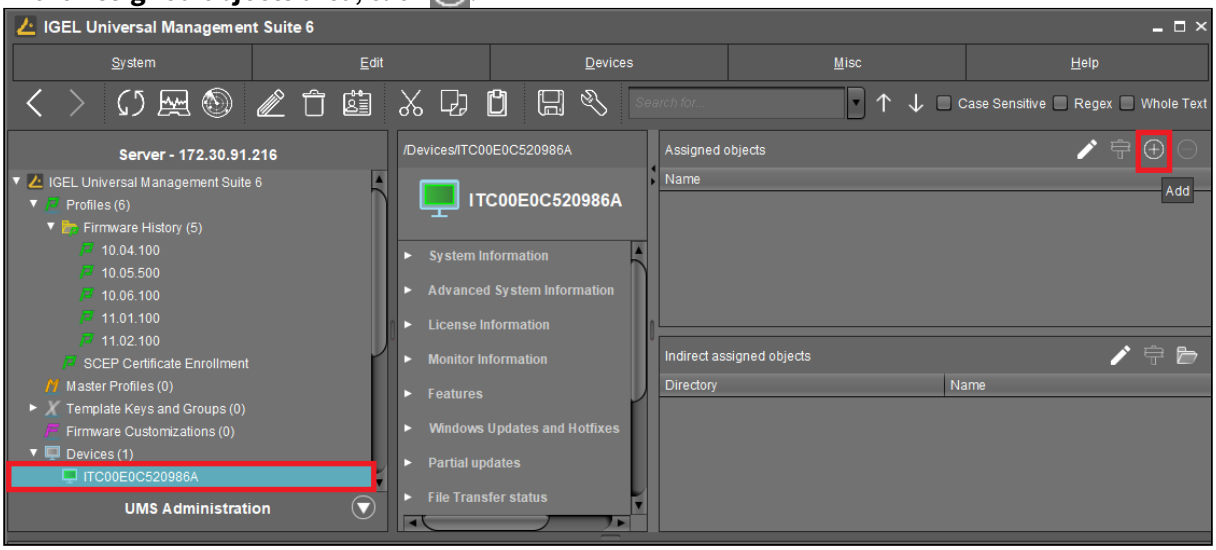
   - **Certificate renewal period (days)**: Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)
   - **Certificate expiry check interval (days)**: Specifies how often the certificate is checked against its expiry date. (Default: 1)

3. Save the settings.

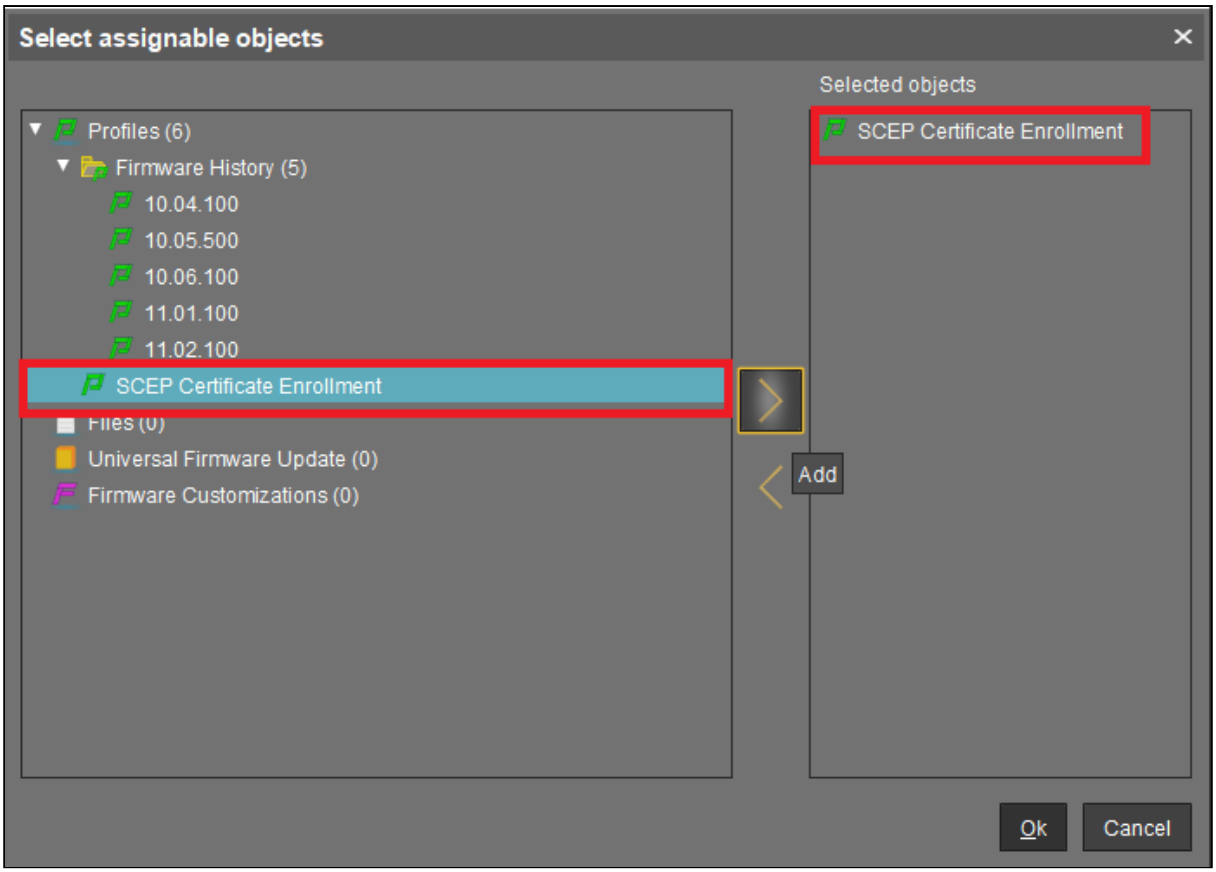
94. https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx

Applying the Profile to the Devices

1. In the UMS structure tree under **Devices**, select the devices you want to assign the profile to.
2. In the **Assigned objects** area, click .



3. In the **Select assignable objects** dialog, select the relevant profile and click to assign it.



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.
   The device performs the actions as described in Client Enrollment Details (see page 746).

Files Involved

All files involved are stored in the directory `/wfs/scep_certificates/cert0`. The following fixed file names are used:

`cacert.pem`	CA certificate
`racert_enc.pem`	RA certificate used for encryption (optional)
`racert_sig.pem`	RA certificate used for signature (optional)
`client.csr`	Certificate signing request
`client.cert`	Client certificate
`client.key`	Private key of client certificate

Troubleshooting

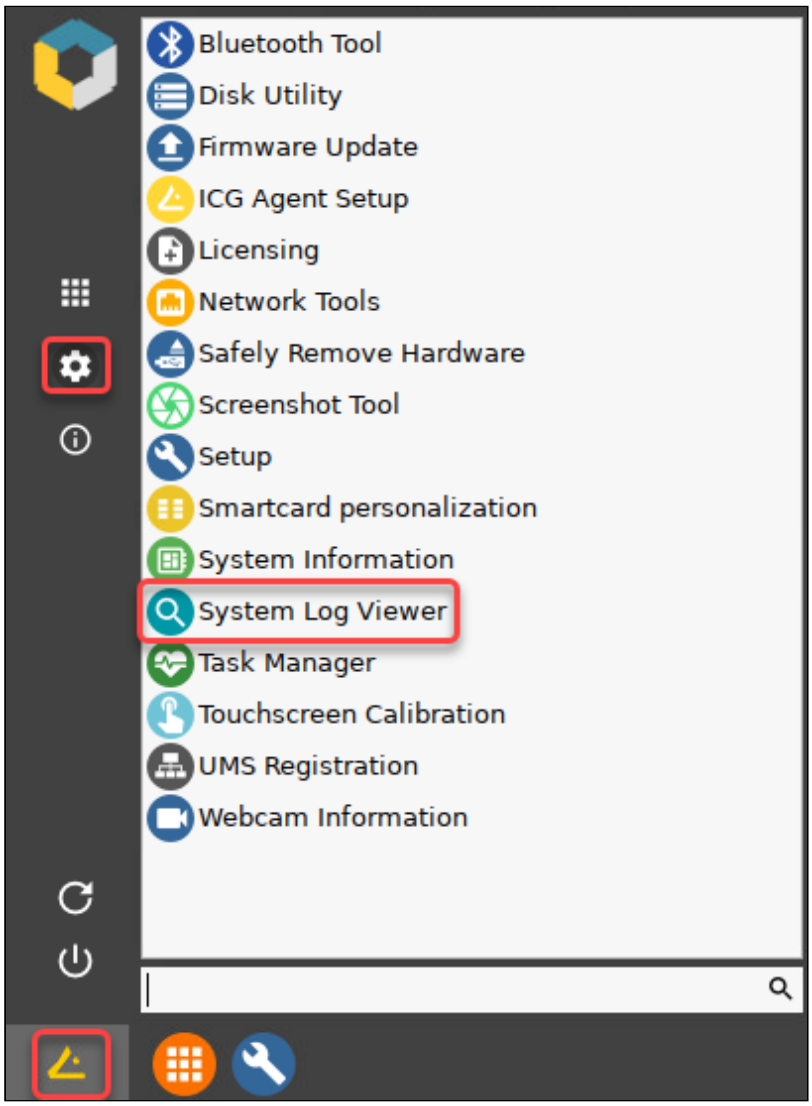
- Diagnostics (see page 761)

Diagnostics

Preliminary: Tools

System Log Viewer

→ In the start menu, select the system icon and then **System Log Viewer**.



For more information on starting, using, and configuring the system log viewer, see the System Log Viewer (see page 1750) chapter of the IGEL OS Manual (see page 1211).

Local Terminal

→ Start the local terminal, if available.

If a local terminal session has not been set up on your device, proceed as follows:

1. Open the Setup and go to **Accessories > Terminals**.
2. Click ⊞ to create a local terminal session.
3. Click **Ok** to save the setting and exit the Setup.

For more information on starting and using the local terminal, see the Terminals (see page 1708) chapter of the IGEL OS Manual (see page 1211).

Checking the Current Status of the Client Certificate Enrollment

->In the local terminal, enter the command `cert_show_status`

The status for each certificate relating to SCEP is shown:

- CA certificate
- RA encryption certificate
- RA signature certificate
- Client certificate

Reviewing Log Messages

1. Open the system log viewer and select `/tmp/journal.log`
2. Press [Ctrl] + [F] and enter `cert_agent` to search for relevant messages.

Alternatively, you can open a local terminal and enter `journalctl | grep cert_agent`

Reviewing the Certificates and Certificate Requests in the File System

1. Open a local terminal and login as `user`.
2. Enter `ls /wfs/scep-certificates/cert0/`

Deleting a Certificate Request

1. Open a local terminal and login as `root`.
2. Enter `rm -rf /wfs/scep-certificates/cert0/`
   The directory that includes the certificate request, received certificates (if existing), and the device's own private client key, is deleted. This can be useful for debugging purposes, and if SCEP is no longer used.

Checking the CA

1. Open a local terminal and login as `root`.
2. Enter `scep_getca 0`

Generating an SCEP Request Manually

1. Open a local terminal and login as `root`.
2. Enter `scep_mkrequest 0`

Enrolling a Certificate Manually

1. Open a local terminal and login as `root`.
2. Enter `scep_enroll 0`

Testing Certificate Renewal

1. Open a local terminal and login as `root`.
2. Generate an SCEP request and append "new" to the key file name: `scep_mkrequest 0 “new”`
   An SCEP request is issued. In the directory `/wfs/scep-certificates/cert0/`, the key file `clientnew.key` is created.
3. Renew the certificate: `scep_renew 0`
4. Overwrite the old certificate with the new one: `mv /wfs/scep-certificates/cert0/clientnew.cert /wfs/scep-certificates/cert0/client.cert`
5. Overwrite the old key with the new one: `mv /wfs/scep-certificates/cert0/clientnew.key /wfs/scep-certificates/cert0/client.key`

Deploying Trusted Root Certificates in IGEL OS

IGEL OS comes with a number of trusted root certificates from certain Certificate Authorities (CA) pre-installed. For a complete list of pre-installed root certificates, see Which CA Certificates Are Contained in IGEL OS? (see page 768)

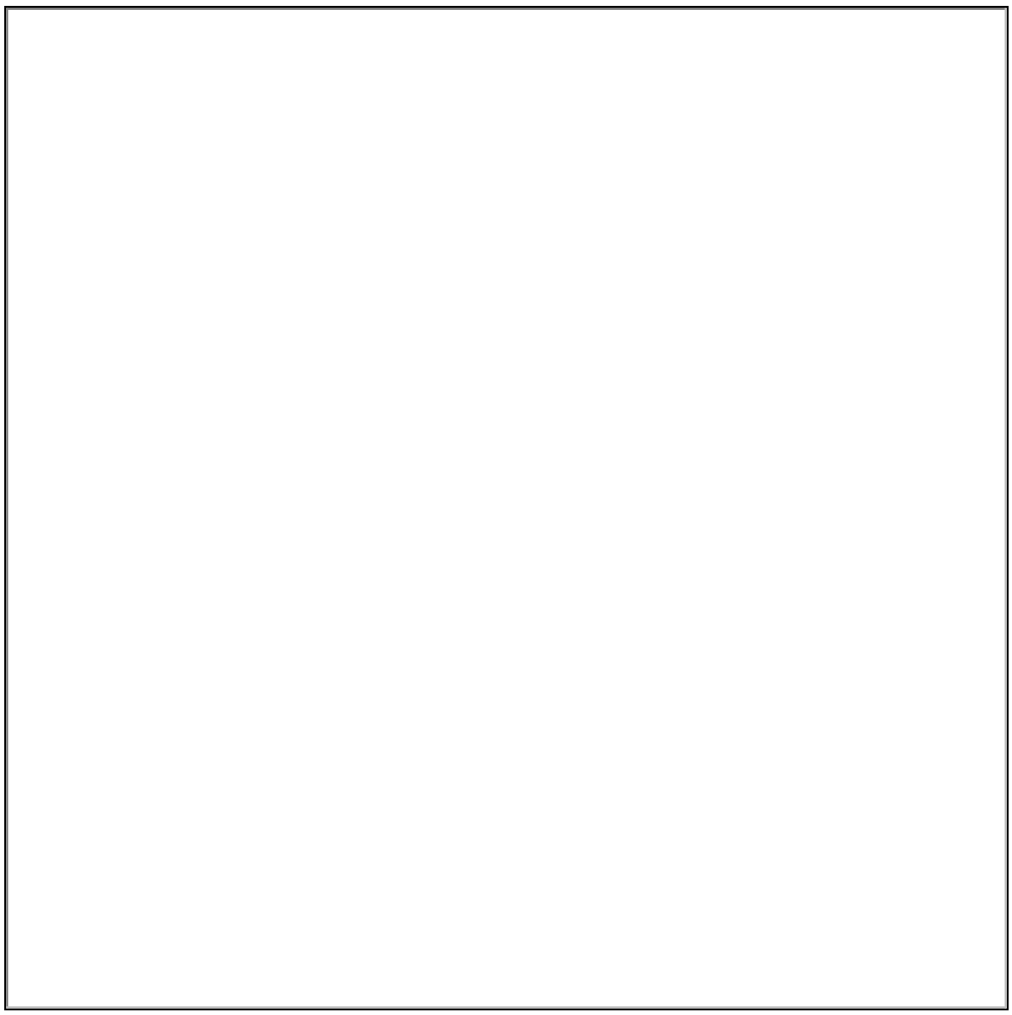
Certificates signed with these root certificates can be used for server authentication and encryption in ICA, RDP, Horizon, and browser sessions. You can also verify the origin of Java applications.

Nevertheless, the root certificate you need might be missing. This document explains how to load and distribute it.

Requirements

The certificates must be available in the Base64 file format encoded with the file extension `.pem`, `.crt` or `.cer`.

To check the file format, open the certificate with a text editor. It should look like this:



Solution

Deploying Certificates via the UMS

We recommend using IGEL Universal Management Suite (UMS) when you need to deploy certificates, especially if you have to do this for multiple endpoint devices.

You can load certificates in the UMS Console via **Files > New file**: simply select your certificate file under **Local file**, select the suitable **Classification** of the certificate, and assign the certificate file to the required devices; see Files - *Universal Management Suite > UMS Reference Manual > Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices*.

We advise you to use the following file transfer types for distributing the certificates via the UMS:

Type	To be used for
Undefined	All-purpose class, you need to set the owner and access permissions manually.
Web Browser Certificate	Server authentication/encryption of HTTPS websites in browsers
SSL Certificate	Server authentication/encryption in ICA, RDP, or Horizon sessions Authentication via Active Directory (AD)
Java Certificate	Authentication/encryption for Java applications
IBM iAccess Certificate	Server authentication/encryption for IBM iAccess sessions
Common Certificate (all-purpose)	Multiple applications needing a certificate, e.g. if you want to launch an ICA session in a browser or if you want to secure a Java session on a secure website.

With these file transfer types, you will not need to reboot after installing.

Providing Certificates Manually

If you want to install certificates manually, see Installing Certificates Manually in IGEL OS (see page 766).

Installing Certificates Manually in IGEL OS

A certificate you require is not pre-installed in IGEL OS and, for some reason, you do not want to use the IGEL Universal Management Suite (UMS) for certificate deployment, see Deploying Trusted Root Certificates in IGEL OS (see page 764). In this case, you can install certificates manually. A USB flash drive can be used for the manual import of certificates.

Importing SSL Certificates (ICA, RDP, Horizon)

If a CA certificate is missing for RDP, ICA, or VMware Horizon, you can copy it from a USB storage device to the endpoint device:

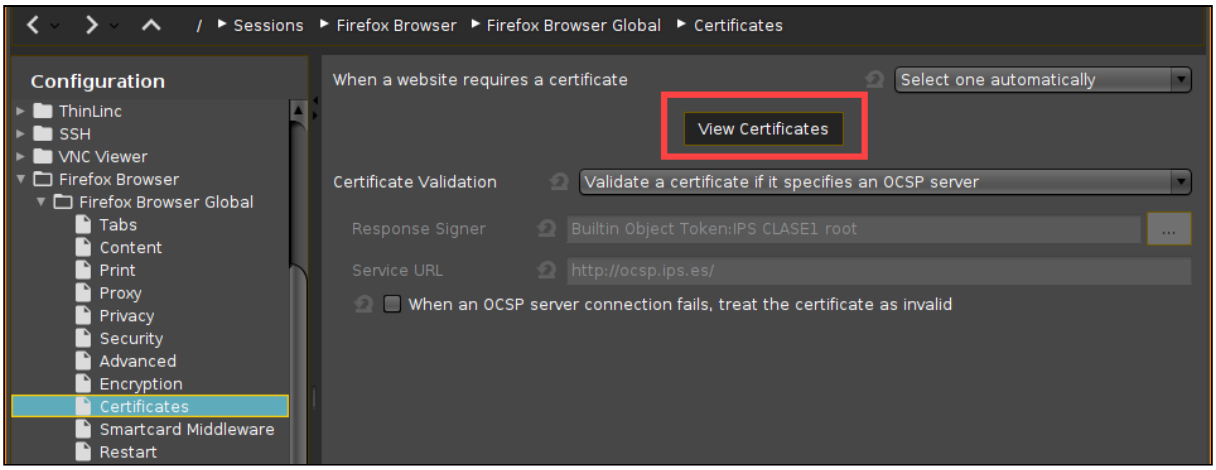
1. Connect your USB storage device to the endpoint.
2. Launch a Local Terminals (see page 1708) session or press [CTRL]+[ALT]+[F11] to log in as **ROOT** on the Linux console of the endpoint.
3. Create a directory for certificates:
   `mkdir /wfs/ca-certs`
4. Change to the directory:
   `cd /wfs/ca-certs`
5. Get the name of your USB storage device:
   `ls /userhome/media`
6. Copy the certificate to the endpoint:
   `cp /userhome/media// /wfs/ca-certs`
7. Check whether the certificate was transferred:
   `ls -al /wfs/ca-certs`
8. End the terminal session or press [CTRL]+[ALT]+[F1] to exit the console.

The certificates you have saved will be available when you boot up the endpoint next time.

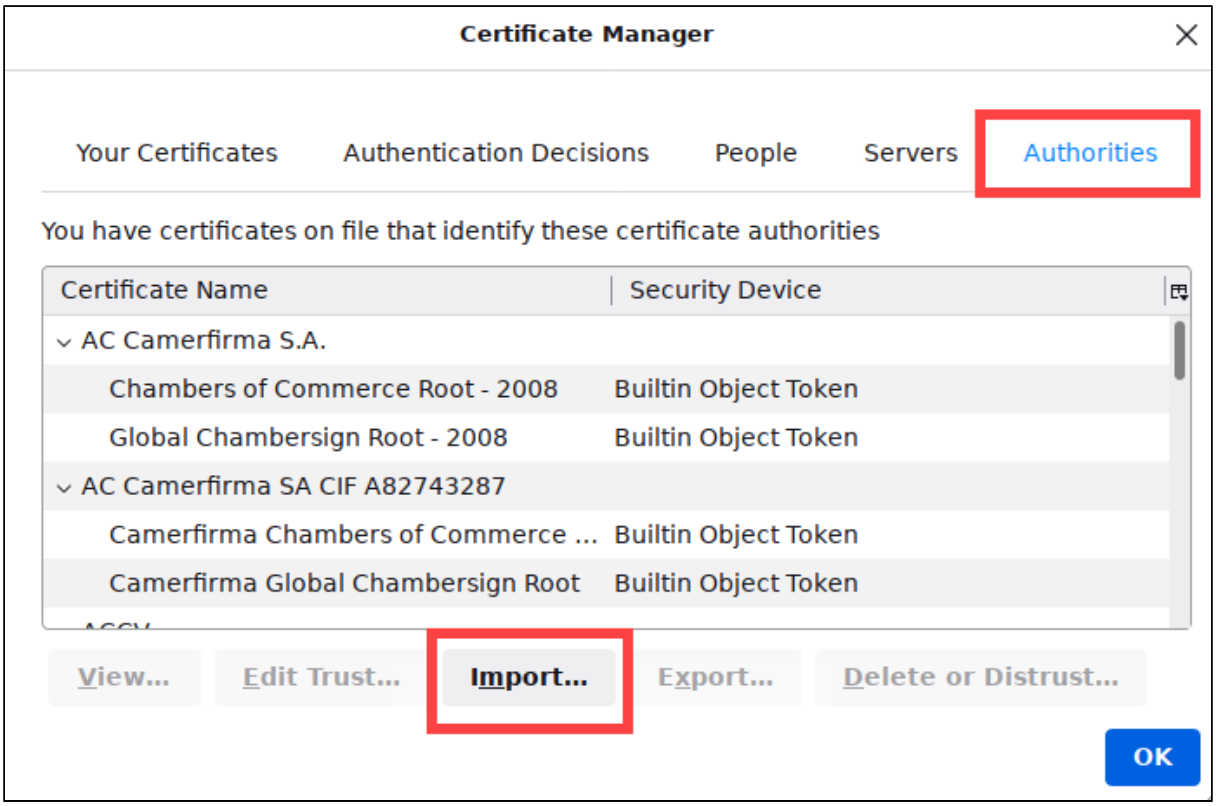
Installing Web Browser Certificates

Use the **Firefox Certificate Manager** in order to manually install web browser certificates:

1. Open the IGEL Setup.
2. Click **Sessions > Firefox Browser > Firefox Browser Global > Certificates > View Certificates** to open the **Firefox Certificate Manager**.



3. In the **Authorities** tab, click **Import...** to import a new certificate from a directory or a USB flash drive.



Manually installed certificates will be saved permanently without any further configuration.

Which CA Certificates Are Contained in IGEL OS?

The following CA certificates are contained in IGEL OS 11.08.330:

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	`ACCVRAIZ1.crt`
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	`AC_RAIZ_FNMT-RCM.crt`
AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Dec 20 09:37:33 2043 GMT	`AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt`
ANF Secure Server Root CA	Aug 30 10:00:38 2039 GMT	`ANF_Secure_Server_Root_CA.crt`
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	`Actalis_Authentication_Root_CA.crt`
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	`AffirmTrust_Commercial.crt`
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	`AffirmTrust_Networking.crt`
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	`AffirmTrust_Premium.crt`
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	`AffirmTrust_Premium_ECC.crt`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`Amazon_Root_CA_1.crt`
Amazon Root CA 2	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Amazon Root CA 3	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_3.crt`
Amazon Root CA 4	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_4.crt`
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	`Atos_TrustedRoot_2011.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	May 5 15:22:07 2036 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068_2.crt`
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`Baltimore_CyberTrust_Root.crt`
Buypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	`Buypass_Class_2_Root_CA.crt`
Buypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	`Buypass_Class_3_Root_CA.crt`
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	`CA_Disig_Root_R2.crt`
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	`CFCA_EV_ROOT.crt`
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	`COMODO_Certification_Authority.crt`
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_ECC_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_RSA_Certification_Authority.crt`
Certainly Root E1	Apr 1 00:00:00 2046 GMT	`Certainly_Root_E1.crt`
Certainly Root R1	Apr 1 00:00:00 2046 GMT	`Certainly_Root_R1.crt`
Certigna	Jun 29 15:13:05 2027 GMT	`Certigna.crt`
Certigna Root CA	Oct 1 08:32:27 2033 GMT	`Certigna_Root_CA.crt`
Certum EC-384 CA	Mar 26 07:24:54 2043 GMT	`Certum_EC-384_CA.crt`
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	`Certum_Trusted_Network_CA.crt`
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	`Certum_Trusted_Network_CA_2.crt`
Certum Trusted Root CA	Mar 16 12:10:13 2043 GMT	`Certum_Trusted_Root_CA.crt`
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_AAA_Services_root.crt`
D-TRUST BR Root CA 1 2020	Feb 11 09:44:59 2035 GMT	`D-TRUST_BR_Root_CA_1_2020.crt`
D-TRUST EV Root CA 1 2020	Feb 11 09:59:59 2035 GMT	`D-TRUST_EV_Root_CA_1_2020.crt`
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	`D-TRUST_Root_Class_3_CA_2_2009.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	`D-TRUST_Root_Class_3_CA_2_EV_2009.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCertGlobalRootCA.pem)`
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Assured_ID_Root_CA.crt`
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G2.crt`
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G3.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Global_Root_CA.crt`
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G2.crt`
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G3.crt`
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_High_Assurance_EV_Root_CA.crt`
DigiCert TLS ECC P384 Root G5	Jan 14 23:59:59 2046 GMT	`DigiCert_TLS_ECC_P384_Root_G5.crt`
DigiCert TLS RSA4096 Root G5	Jan 14 23:59:59 2046 GMT	`DigiCert_TLS_RSA4096_Root_G5.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	`DigiCert_Trusted_Root_G4.crt`
E-Tugra Global Root CA ECC v3	Mar 12 09:46:58 2045 GMT	`E-Tugra_Global_Root_CA_ECC_v3.crt`
E-Tugra Global Root CA RSA v3	Mar 12 09:07:17 2045 GMT	`E-Tugra_Global_Root_CA_RSA_v3.crt`
Entrust.net[95] Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	`Entrust.net_Premium_2048_Secure_Server_CA.crt`
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	`Entrust_Root_Certification_Authority.crt`
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	`Entrust_Root_Certification_Authority_-_EC1.crt`
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	`Entrust_Root_Certification_Authority_-_G2.crt`
Entrust Root Certification Authority - G4	Dec 27 11:41:16 2037 GMT	`Entrust_Root_Certification_Authority_-_G4.crt`
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	`GDCA_TrustAUTH_R5_ROOT.crt`
GLOBALTRUST 2020	Jun 10 00:00:00 2040 GMT	`GLOBALTRUST_2020.crt`
GTS Root R1	Jun 22 00:00:00 2036 GMT	`GTS_Root_R1.crt`

95. http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
GTS Root R2	Jun 22 00:00:00 2036 GMT	`GTS_Root_R2.crt`
GTS Root R3	Jun 22 00:00:00 2036 GMT	`GTS_Root_R3.crt`
GTS Root R4	Jun 22 00:00:00 2036 GMT	`GTS_Root_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R5.crt`
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	`GlobalSign_Root_CA.crt`
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.crt`
GlobalSign	Dec 10 00:00:00 2034 GMT	`GlobalSign_Root_CA_-_R6.crt`
GlobalSign Root E46	Mar 20 00:00:00 2046 GMT	`GlobalSign_Root_E46.crt`
GlobalSign Root R46	Mar 20 00:00:00 2046 GMT	`GlobalSign_Root_R46.crt`
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	`Go_Daddy_Class_2_CA.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Go_Daddy_Root_Certificate_Authority_-_G2.crt`
HARICA TLS ECC Root CA 2021	Feb 13 11:01:09 2045 GMT	`HARICA_TLS_ECC_Root_CA_2021.crt`
HARICA TLS RSA Root CA 2021	Feb 13 10:55:37 2045 GMT	`HARICA_TLS_RSA_Root_CA_2021.crt`
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	`Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt`
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt`
HiPKI Root CA - G1	Dec 31 15:59:59 2037 GMT	`HiPKI_Root_CA_-_G1.crt`
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	`Hongkong_Post_Root_CA_1.crt`
Hongkong Post Root CA 3	Jun 3 02:29:46 2042 GMT	`Hongkong_Post_Root_CA_3.crt`
ISRG Root X1	Jun 4 11:04:38 2035 GMT	`ISRG_Root_X1.crt`
ISRG Root X2	Sep 17 16:00:00 2040 GMT	`ISRG_Root_X2.crt`
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	`IdenTrust_Commercial_Root_CA_1.crt`
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	`IdenTrust_Public_Sector_Root_CA_1.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	`Imprivata.crt`
Izenpe.com[96]	Dec 13 08:27:25 2037 GMT	`Izenpe.com`[97]`.crt`
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	`Microsec_e-Szigno_Root_CA_2009.crt`
Microsoft ECC Root Certificate Authority 2017	Jul 18 23:16:04 2042 GMT	`Microsoft_ECC_Root_Certificate_Authority_2017.crt`
Microsoft RSA Root Certificate Authority 2017	Jul 18 23:00:23 2042 GMT	`Microsoft_RSA_Root_Certificate_Authority_2017.crt`
NAVER Global Root Certification Authority	Aug 18 23:59:59 2037 GMT	`NAVER_Global_Root_Certification_Authority.crt`
NetLock Arany (Class Gold) Főtanúsítvány	Dec 6 15:08:21 2028 GMT	`NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt`
OISTE WISeKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	`OISTE_WISeKey_Global_Root_GB_CA.crt`
OISTE WISeKey Global Root GC CA	May 9 09:58:33 2042 GMT	`OISTE_WISeKey_Global_Root_GC_CA.crt`
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	`QuoVadis_Root_CA_1_G3.crt`
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	`QuoVadis_Root_CA_2.crt`

96. http://Izenpe.com
97. http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	`QuoVadis_Root_CA_2_G3.crt`
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	`QuoVadis_Root_CA_3.crt`
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	`QuoVadis_Root_CA_3_G3.crt`
SSL.com[98] EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	`SSL.com_EV_Root_Certification_Authority_ECC.crt`
SSL.com[99] EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	`SSL.com_EV_Root_Certification_Authority_RSA_R2.crt`
SSL.com[100] Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	`SSL.com_Root_Certification_Authority_ECC.crt`
SSL.com[101] Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	`SSL.com_Root_Certification_Authority_RSA.crt`
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	`SZAFIR_ROOT_CA2.crt`
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	`SecureSign_RootCA11.crt`
SecureTrust CA	Dec 31 19:40:55 2029 GMT	`SecureTrust_CA.crt`
Secure Global CA	Dec 31 19:52:06 2029 GMT	`Secure_Global_CA.crt`

98. http://SSL.com
99. http://SSL.com
100. http://SSL.com
101. http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
Security Communication ECC RootCA1	Jan 18 05:15:28 2038 GMT	`Security_Communication_ECC_RootCA1.crt`
Security Communication RootCA2	May 29 05:00:39 2029 GMT	`Security_Communication_RootCA2.crt`
Security Communication RootCA3	Jan 18 06:17:16 2038 GMT	`Security_Communication_RootCA3.crt`
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	`Security_Communication_Root_CA.crt`
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	`Starfield_Class_2_CA.crt`
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Root_Certificate_Authority_-_G2.crt`
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Services_Root_Certificate_Authority_-_G2.crt`
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	`SwissSign_Gold_CA_-_G2.crt`
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	`SwissSign_Silver_CA_-_G2.crt`
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_2.crt`
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_3.crt`
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	`TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	`TWCA_Global_Root_CA.crt`
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	`TWCA_Root_Certification_Authority.crt`
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	`TeliaSonera_Root_CA_v1.crt`
Telia Root CA v2	Nov 29 11:55:54 2043 GMT	`Telia_Root_CA_v2.crt`
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	`TrustCor_ECA-1.crt`
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	`TrustCor_RootCert_CA-1.crt`
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	`TrustCor_RootCert_CA-2.crt`
Trustwave Global Certification Authority	Aug 23 19:34:12 2042 GMT	`Trustwave_Global_Certification_Authority.crt`
Trustwave Global ECC P256 Certification Authority	Aug 23 19:35:10 2042 GMT	`Trustwave_Global_ECC_P256_Certification_Authority.crt`
Trustwave Global ECC P384 Certification Authority	Aug 23 19:36:43 2042 GMT	`Trustwave_Global_ECC_P384_Certification_Authority.crt`
TunTrust Root CA	Apr 26 08:57:56 2044 GMT	`TunTrust_Root_CA.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	`UCA_Extended_Validation_Root.crt`
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	`UCA_Global_G2_Root.crt`
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_ECC_Certification_Authority.crt`
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_RSA_Certification_Authority.crt`
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	`XRamp_Global_CA_Root.crt`
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	`certSIGN_ROOT_CA.crt`
certSIGN ROOT CA G2	Feb 6 09:27:35 2042 GMT	`certSIGN_Root_CA_G2.crt`
e-Szigno Root CA 2017	Aug 22 12:07:06 2042 GMT	`e-Szigno_Root_CA_2017.crt`
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	`ePKI_Root_Certification_Authority.crt`
emSign ECC Root CA - C3	Feb 18 18:30:00 2043 GMT	`emSign_ECC_Root_CA_-_C3.crt`
emSign ECC Root CA - G3	Feb 18 18:30:00 2043 GMT	`emSign_ECC_Root_CA_-_G3.crt`
emSign Root CA - C1	Feb 18 18:30:00 2043 GMT	`emSign_Root_CA_-_C1.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
emSign Root CA - G1	Feb 18 18:30:00 2043 GMT	`emSign_Root_CA_-_G1.crt`
vTrus ECC Root CA	Jul 31 07:26:44 2043 GMT	`vTrus_ECC_Root_CA.crt`
vTrus Root CA	Jul 31 07:24:05 2043 GMT	`vTrus_Root_CA.crt`

Smartcard

- Authentication with IGEL Smartcard (see page 782)
- Smartcard Authentication in IGEL OS (see page 791)

Authentication with IGEL Smartcard

Smartcards make the user experience more convenient by providing a single device that supports multiple authentication products across the enterprise. The user only has to remember a single PIN that unlocks the smart card to access the network.

Prerequisites

Before using the IGEL smartcard, the relevant profiles and session information need to be written to the smartcard.

We describe a best practice way of how to proceed. The names of folders and profiles are only examples and can be changed individually.

It is useful to use following folders and profiles on the Universal Management Suite (UMS):

Folder	Profile	Purpose
Smartcard Creation		Folder for devices which will be used for smartcard creation.
	Smartcard Key	This profile will apply the defined company key to the devices. This key will be written while creating the IGEL smartcard.
Smartcard Operation		Folder for devices whose authentication process will work only via IGEL smartcard.
	Smartcard Login	This profile will apply the company key to the devices and will activate the login with IGEL smartcard.

->Create two folders under **Profiles** in the Universal Management Suite (UMS), e.g. "Smartcard Operation" and "Smartcard Creation".

->Create the profile "Smartcard Login" for "Smartcard Operation".

->Create the profile "Smartcard Key" for "Smartcard Creation".

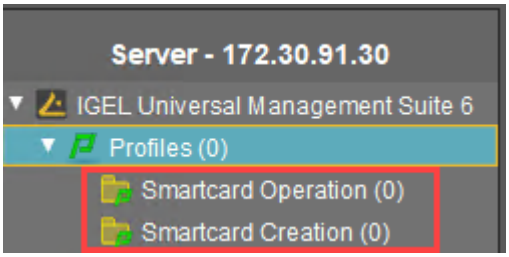
_____

- Creating IGEL Smartcard Folders (see page 783)
- Folder "Smartcard Operation" (see page 784)
- Folder "Smartcard Creation" (see page 785)
- Writing the IGEL Smartcard (see page 786)
- Smartcard Readers Supported by IGEL Smartcards (see page 790)

Creating IGEL Smartcard Folders

First, add two new profile folders for creating profiles and assigning them to devices:

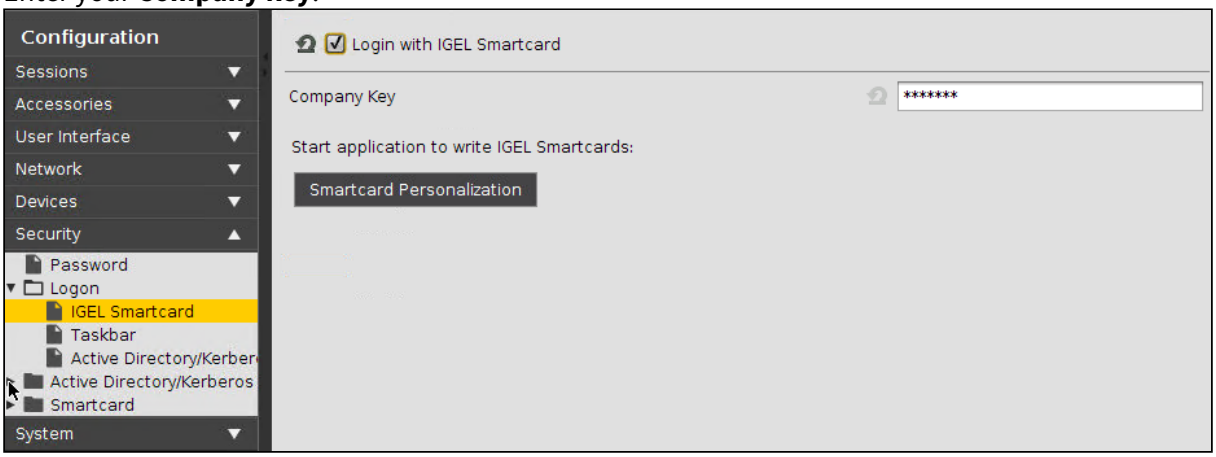
- "Smartcard Operation";
- "Smartcard Creation".



Folder "Smartcard Operation"

In this folder, you create a new profile "Smartcard Login":

1. Right-click the folder "Smartcard Operation".
2. Choose **New Profile**.
3. Enter a **Profile Name**, e.g. "Smartcard Login".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enable **Login with IGEL smartcard**.
6. Enter your **Company key**.



Later on, this profile will be applied to all devices where the authentication process shall work only with a smartcard.
This way, the device will receive:

- the company key and
- the information that the authentication is only possible with the smartcard.

The company key is a private key shared between devices and smartcards. It should be chosen similarly to a good password. If the smartcard does not hold the same company key as the device, authentication will not be possible. Remember this company key because you will need later to write exactly the same key to the smartcard.

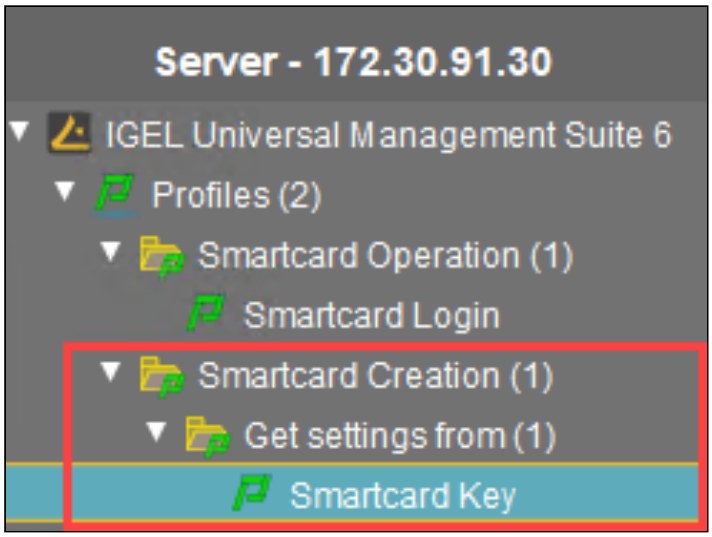
Folder "Smartcard Creation"

In this folder, you create a new profile "Smartcard Key":

1. Right-click the folder "Smartcard Creation".
2. Choose **New Profile**.
3. Enter a profile name, e.g. "Smartcard Key".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enter the same **Company key** as in the profile "Smartcard Login".

Another additional folder is useful:

->Create the subfolder "Get settings from" under "Smartcard Creation".
In this folder, you create the profile with the session information you want to write to the smartcard.



You need this additional folder because the assignment of active profiles from the UMS to the IGEL smartcard can cause problems (firmware version < 5.06.100). Later on, you will copy the folder locally to your device.

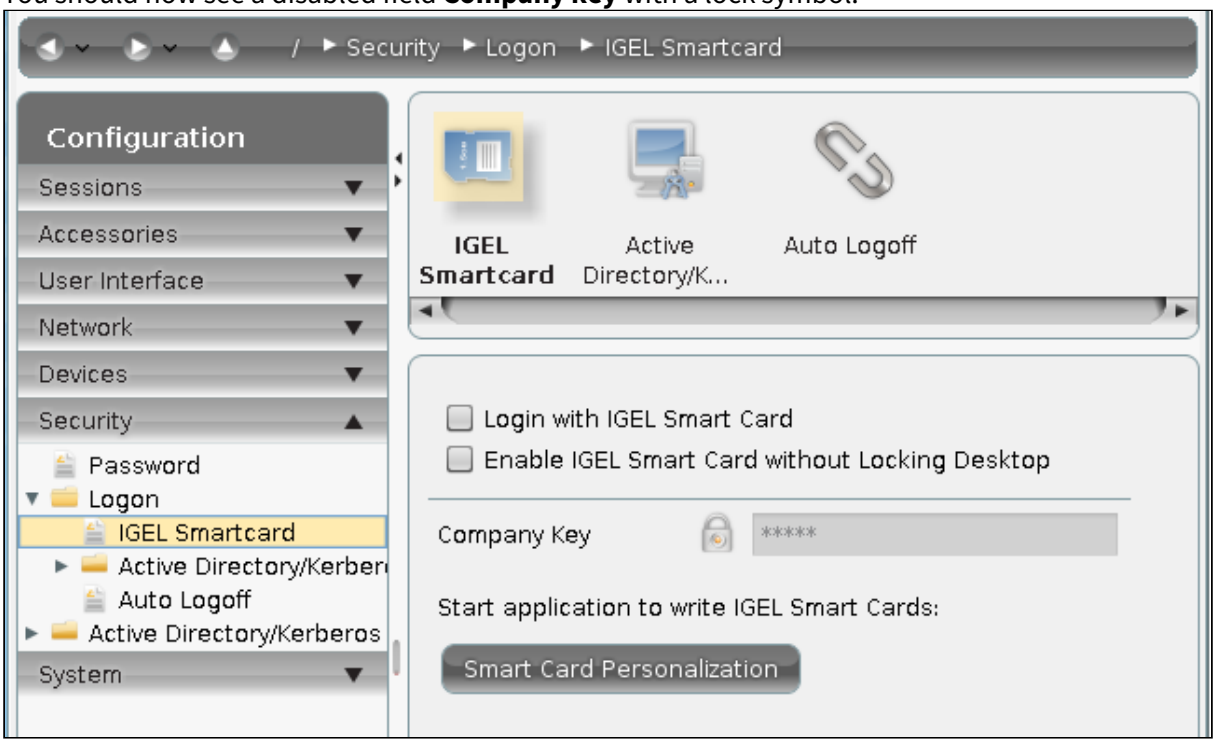
Writing the IGEL Smartcard

Assigning the Profile "Smartcard Creation" to the Device

1. Prepare one device which has a smartcard reader/writer.
2. Integrate this device in the UMS and put it into the folder "Smartcard Creation".
   Now the device automatically receives the company key from the profile. It will be used when writing the smartcard.

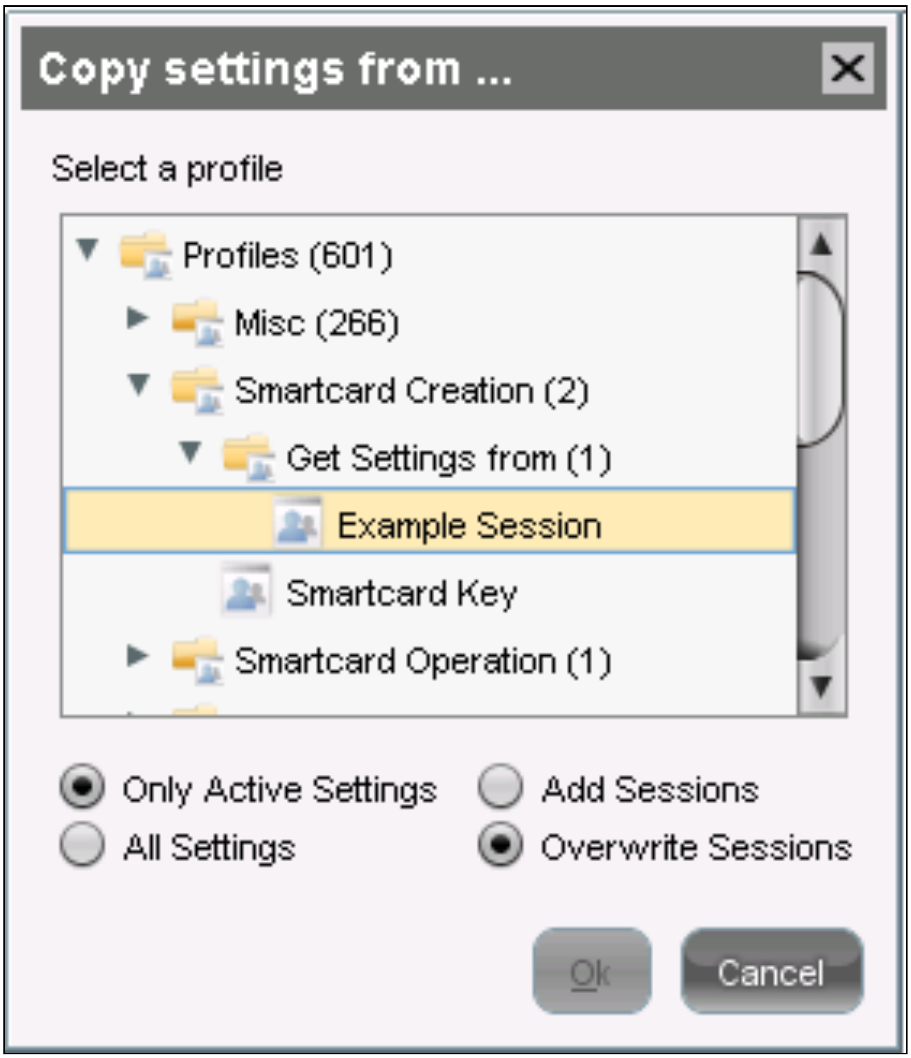
Ensuring That the Profile Assignment Was Successful

1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.
   You should now see a disabled field **Company key** with a lock symbol.



Writing the Profiles to the Smartcard

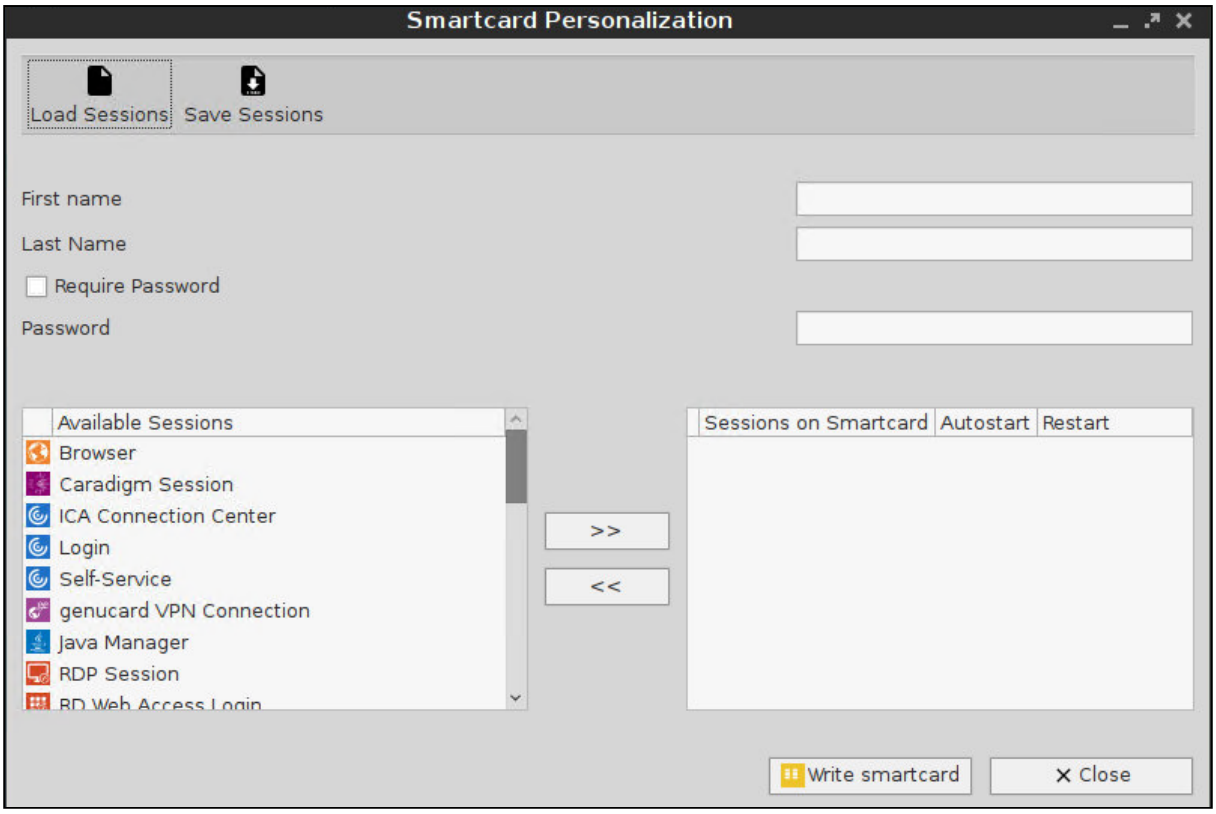
1. Open the folder "Smartcard Creation" in the UMS.
2. Right-click your device.
3. Choose **Take over settings from...** to copy the profile settings to the device.
   The dialog **Copy settings from...** opens.
4. Choose your profile from the folder "Smartcard Creation" > "Get settings from".
5. Enable **Overwrite Sessions**.



6. Click **OK** to copy the profile with the settings and the company key to the device.

Writing the Smartcard

1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.
3. Click **Smartcard personalization**.
   The **Smartcard personalization** dialog opens.



4. Enter the **First name** and the **Last name** of the smartcard holder that should appear at the login prompt.
5. Activate **Require password** and specify the **Password** if a password has to be required for the smartcard login.
6. Select the local sessions you want to write to the smartcard.

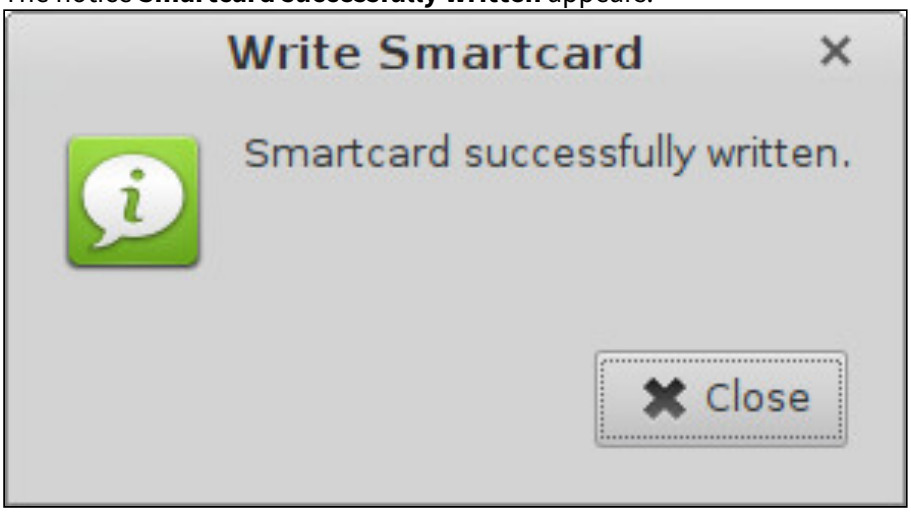
   Use the arrow buttons to add a session to the smartcard session list.

7. Activate **Autostart** for a session in the smartcard list if it should be automatically started at login. Check **Restart** if desired.

   The configuration of the sessions can be saved and reloaded at a later time.

8. Click **Write smartcard** to start the writing process with the defined settings.
9. Confirm the security question with **Yes**.

The notice **Smartcard successfully written** appears.



Testing the New IGEL Smartcard

1. Go to the UMS.
2. Register a new device in the UMS and put it in the folder "Smartcard Operation".
   The device gets the company key and the profile information that authentication is only possible with the IGEL smartcard.
3. Restart the device.
   The **Insert Smartcard...** dialog opens.
4. Insert the IGEL smartcard into your device and verify the selected configuration.

Smartcard Readers Supported by IGEL Smartcards

IGEL smartcards are supported by the following third-party smartcard readers:

- OMNIKEY CardMan 3111
- OMNIKEY CardMan 3x21
- OMNIKEY CardMan 3621
- OMNIKEY CardMan 6121
- OMNIKEY CardMan 3821
- USB CCID Smart Card Reader
- USB CCID Smart Card Reader Keyboard
- Fujitsu Siemens Computers SmartCard-Reader USB 2A
- Fujitsu Siemens Computers SmartCard-Reader Keyboard USB 2A
- Fujitsu Siemens Computers SmartCard-Reader USB 2C
- Cherry SmartBoard XX44
- OMNIKEY CardMan 5121
- OMNIKEY CardMan 5x21
- HID Global OMNIKEY 3x21 Smart Card Reader
- Cherry KC 1000 SC
- Cherry KC 1000 SC/DI
- Cherry KC 1000 SC Z
- Cherry KC 1000 SC/DI Z
- Cherry SmartTerminal XX44 v2
- Cherry SmartTerminal XX44
- OMNIKEY CardMan
- CCID SC Reader
- Cherry SC Reader.

Smartcard Authentication in IGEL OS

The following article provides an overview of how you can configure smartcard authentication in IGEL OS for various sessions like RDP, VMware Horizon, etc. as well as explains how you can set up Active Directory login with a smartcard and local login with a smartcard certificate.

If you use IGEL smartcards, see also Authentication with IGEL Smartcard (see page 782).

Certificate Authentication

The smartcards discussed here can hold digital certificates (x.509) and corresponding private keys. The private key cannot be read from the card, but it can be used by the card itself for signing and decryption of data.

This enables the use of what is known as two-factor authentication: the user not only possesses the smartcard, he or she can also prove the knowledge of the smartcard PIN by signing data using the private key stored on the smartcard.

If you want to use Active Directory (AD), the certificate chain used by the key distribution center (domain controller) must be available on the device. To deploy certificate files, register them in the UMS (set **Classification** to "SSL Certificate") and assign to the devices, see *Universal Management Suite > UMS Reference Manual > Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices*.

Smartcard Readers

Smartcards are accessed via smartcard readers, using either a contact or contactless interface. The IGEL Third Party Database[102] lists the readers supported in IGEL OS.

PC/SC Resource Manager

The PC/SC Resource Manager is a common Application Programming Interface (API) that is available on Windows and Linux operating systems. It provides a standardized way for applications to handle smartcards and readers.

The PC/SC Resource Manager is active by default in IGEL OS and can be controlled in the IGEL Setup via the **Activate PC/SC daemon** parameter under **Security > Smartcard > Services**.

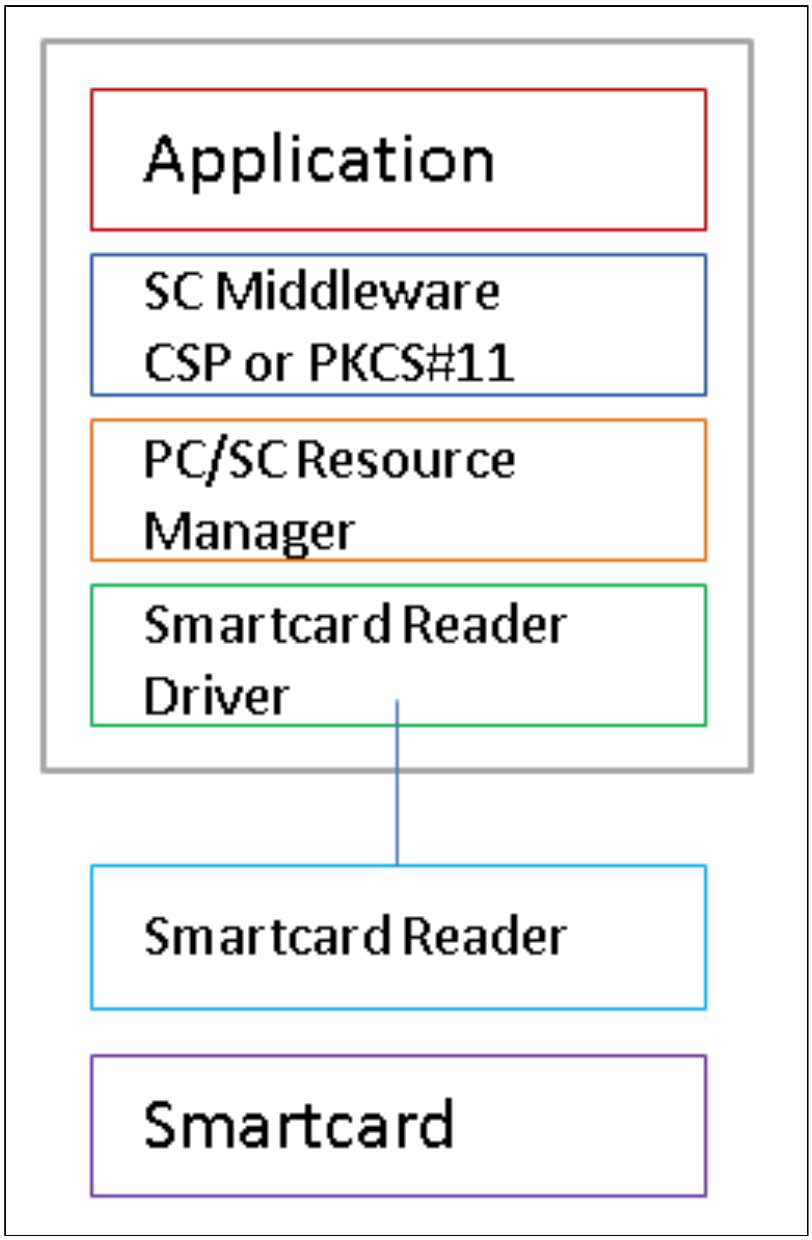
Smartcard Middleware

In order to provide a generalized interface to different types of smartcard hardware, there is an additional software layer called smartcard middleware.

There are different types of middleware:

	Windows	Linux
CSP, Cryptographic Service Provider	✓	
PKCS#11, Public-Key Cryptographic Standards	✓	✓

102. https://www.igel.com/linux-3rd-party-hardware-database/



Some of the smartcard authentication methods require smartcard middleware to be installed on the endpoint device. The following modules are available:

- Gemalto SafeNet
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- SecMaker Net iD Enterprise (formerly called "SecMaker Net iD")
- SecMaker Net iD Client (the next generation of SecMaker Net iD Enterprise, see http://docs.secmaker.com/net-id-client/latest/index.html)
- Coolkey

- OpenSC
- 90meter

> Licensed Feature
>
> This feature requires an add-on license; see *IGEL Subscription and More > Hide from Viewport IGEL Software License Overview > Add-On Licenses*. Please contact your IGEL reseller.

For information on how to use a custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 922).

- Active Directory Logon with Smartcard (see page 794)
- Citrix StoreFront (see page 795)
- RDP Sessions (see page 797)
- Horizon Sessions (see page 798)
- Smartcard Authentication in Browser (see page 799)
- Local Login with Smartcard Certificate (see page 800)

Active Directory Logon with Smartcard

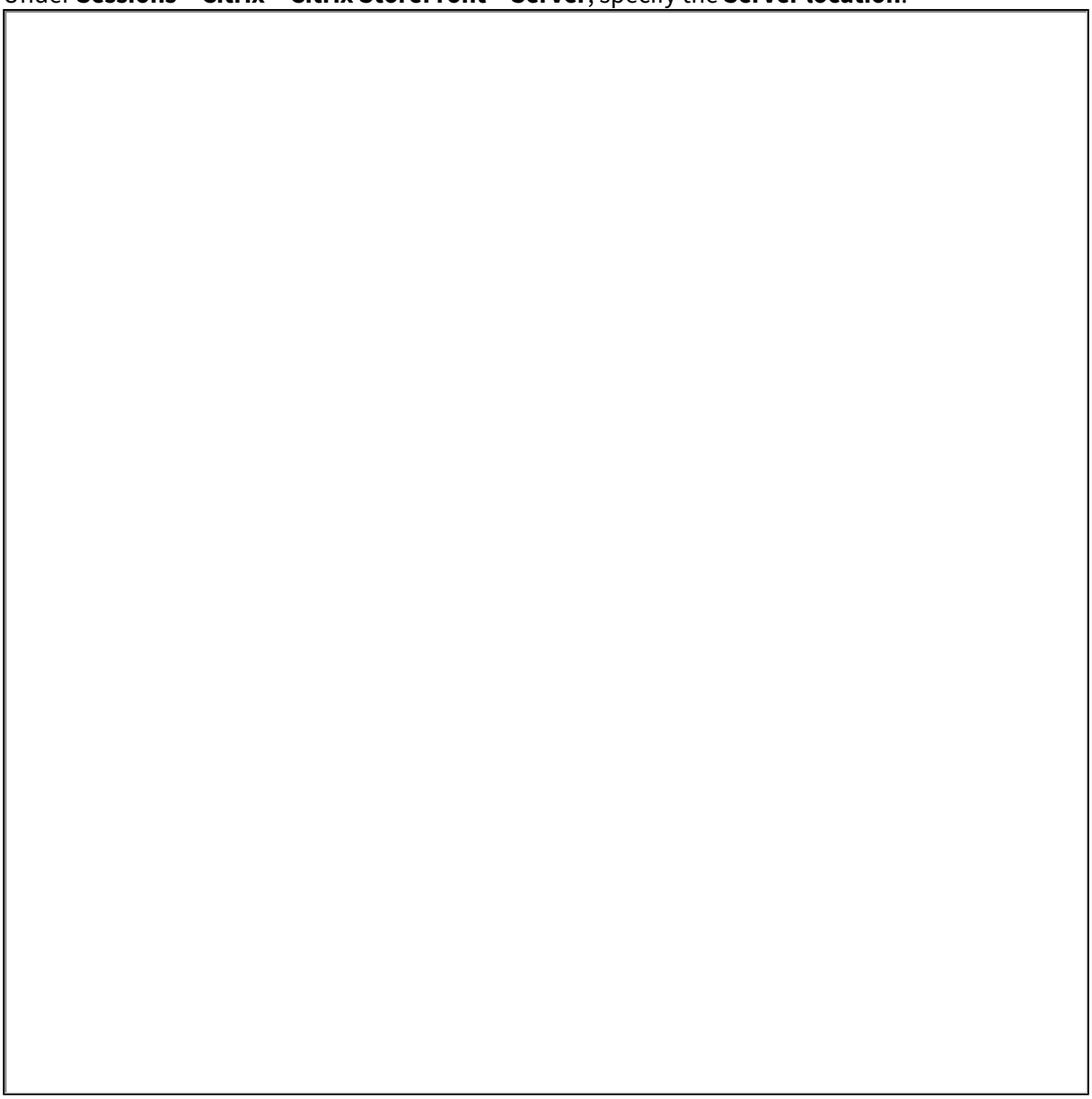
See the how-to Passthrough Authentication (see page 1165).

Citrix StoreFront

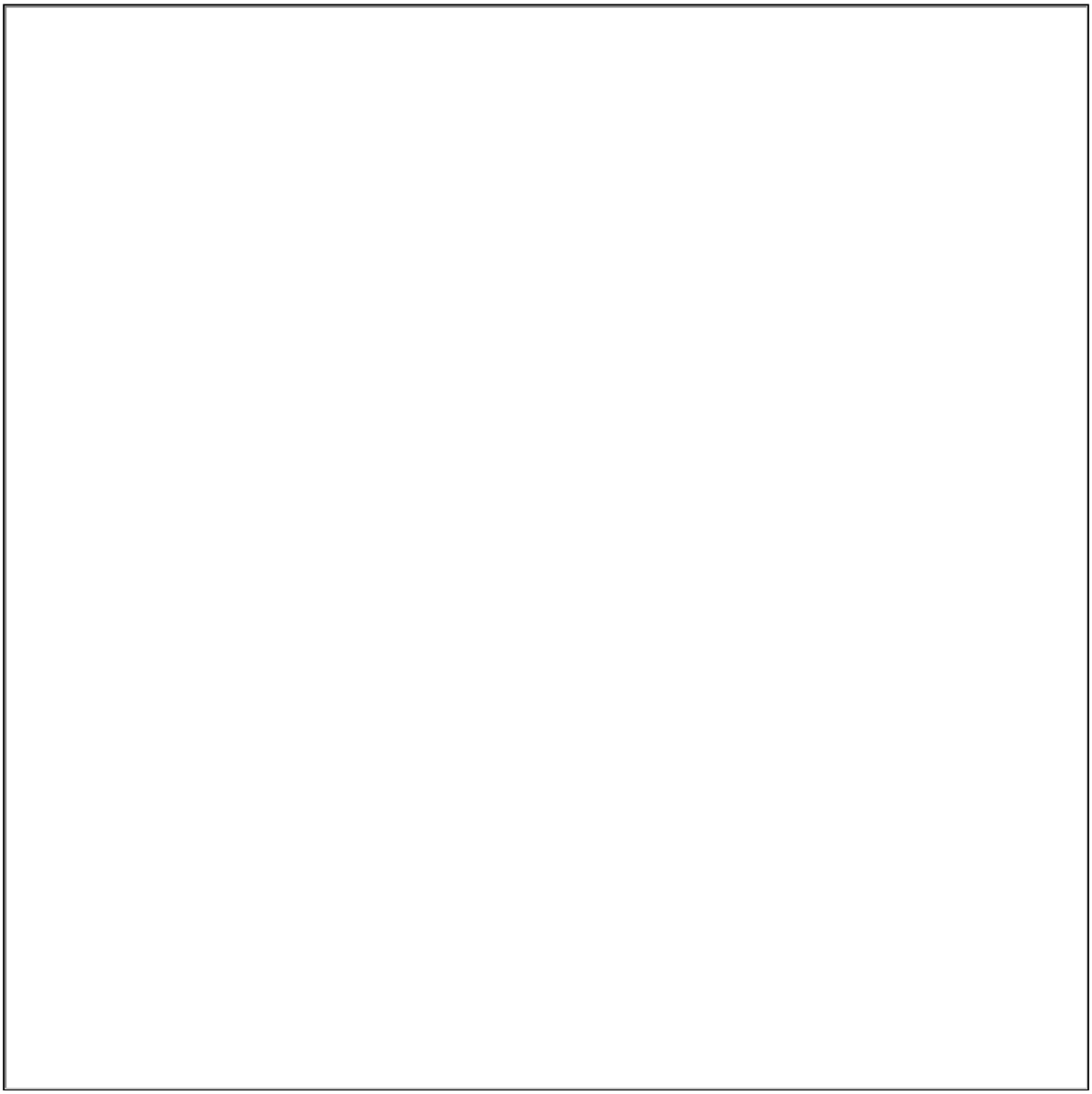
The following article describes how you can configure smartcard authentication in IGEL OS for Citrix StoreFront.

Note that the root certificate of the web server certificate used by the StoreFront server has to be known as the trusted root certificate on the endpoint device – see Deploying Trusted Root Certificates in IGEL OS (see page 764), certificate type **SSL Certificate**.

1. Under **Sessions > Citrix > Citrix StoreFront > Server**, specify the **Server location**.



2. Under **Sessions > Citrix > Citrix StoreFront > Login > Authentication type**, choose **Smartcard authentication**.



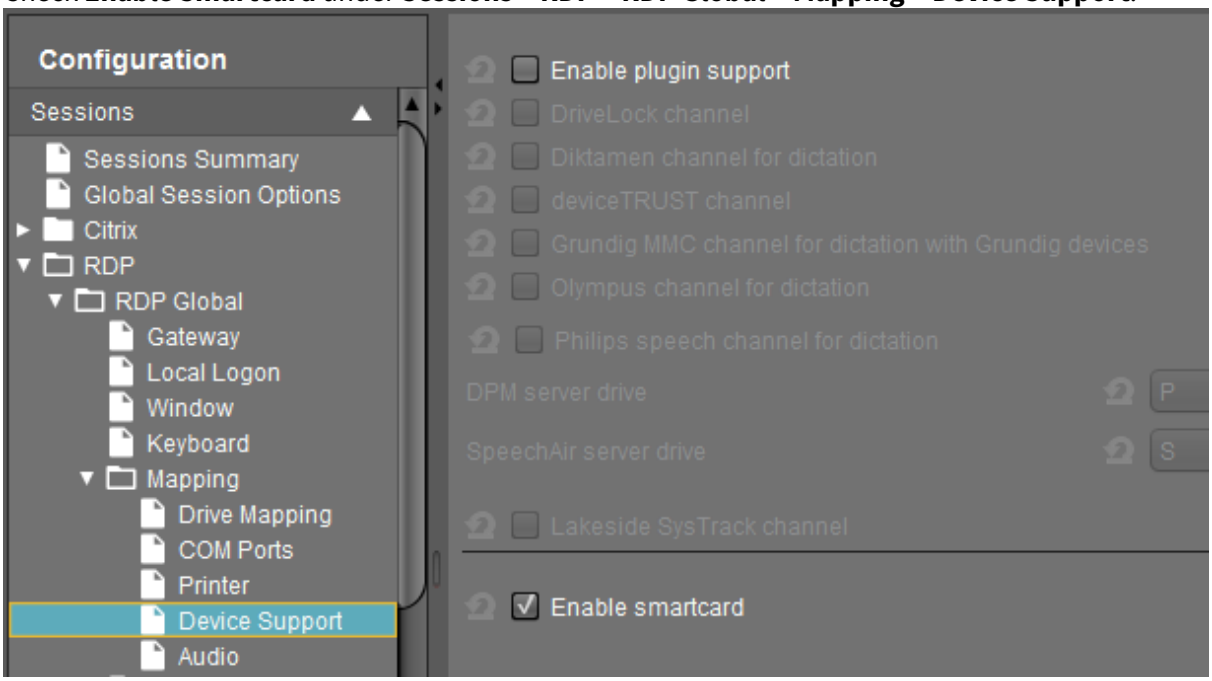
When used in combination with Active Directory Logon (see page 2034), the enabled **Use passthrough authentication** activates single sign-on with a smartcard.

3. Select the appropriate PKCS#11 module for the smartcard under **Security > Smartcard > Middleware** or specify there your own PKCS#11 library, see Middleware for Smartcards in IGEL OS (see page 2027).

RDP Sessions

In this scenario, the smartcard middleware has to be installed on the server side.

1. Enable **Activate PC/SC Daemon** under **Security > Smartcard > Services**.
2. Check **Enable Smartcard** under **Sessions > RDP > RDP Global > Mapping > Device Support**.



Horizon Sessions

In this scenario, the smartcard middleware has to be installed on the virtual desktops as well as configured on the endpoint device side.

The View Connection Server has to be configured on the endpoint device side.

> The View Connection Server has to be configured to accept connections via SSL/TLS secured https URLs. The root certificate of the certificate used for this service has to be known as the trusted root certificate on the thin client (see the how-to Deploying Trusted Root Certificates in IGEL OS (see page 764), certificate type **SSL Certificate**).

1. Select the appropriate PKCS#11 module for the smartcard under **Sessions > Horizon Client > Horizon Client Global > Smartcard**, see Smartcard Middleware Settings for VMware Horizon Sessions in IGEL OS (see page 1391).

   For details on the custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 922).
2. Configure the **Server URL** under **Sessions > Horizon Client > Horizon Client Sessions > [session name] > Connection settings**.

   > Start the URL with `https://`

Smartcard Authentication in Browser

It is possible to authenticate using a smartcard at websites, e. g. *Citrix Web Interface* or *StoreFront*.

When connecting via an SSL/TLS secured https URL, the root certificate of the web server certificate has to be known as the **Trusted Root Certificate** on the endpoint device; see Deploying Trusted Root Certificates in IGEL OS (see page 764), certificate types **Web Browser Certificate** and (!) **SSL Certificate**.

->Select the appropriate PKCS#11 module (security device) for the smartcard under **Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware** or/and under **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**.

- Gemalto SafeNet
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- SecMaker Net iD Enterprise (formerly called "SecMaker Net iD")
- SecMaker Net iD Client (the next generation of SecMaker Net iD Enterprise, see http://docs.secmaker.com/net-id-client/latest/index.html)
- Coolkey
- OpenSC
- 90meter

Licensed Feature

This feature requires an add-on license; see *IGEL Subscription and More > Hide from Viewport IGEL Software License Overview > Add-On Licenses*. Please contact your IGEL reseller.

For details on the custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 922).

Local Login with Smartcard Certificate

Overview

This is a method for local login at the endpoint device with a smartcard holding a certificate.

It can be used in two ways:

- As a standalone authentification method; see Standalone Authentification Method (see page 801)
- In combination with AD/Kerberos; see Combination with the "AD/Kerberos with Smartcard" Method (see page 811) (see also Passthrough Authentication (see page 1165)). The AD/Kerberos login is tried first. If this has been successful, the login is successful. If not, login with the smartcard certificate is performed as a fallback.

For the login with a smartcard certificate, the pam_pkcs11 module is used. For reference, see https://github.com/OpenSC/pam_pkcs11.

- Standalone Authentification Method (see page 801)
- Combination with the "AD/Kerberos with Smartcard" Method (see page 811)

Standalone Authentification Method

Prerequisites

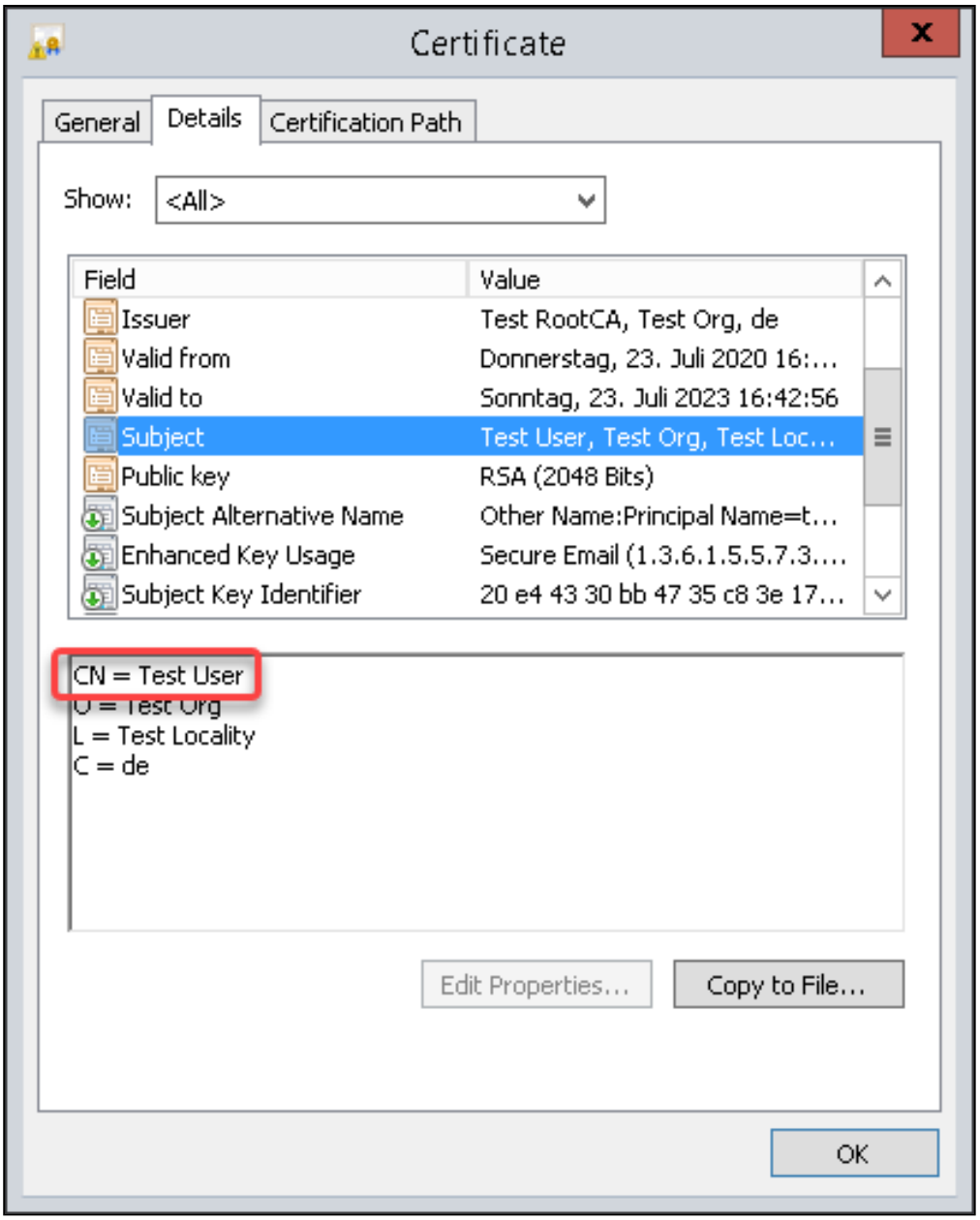
The following files are required:

- Root certificate and intermediate CA certificates, as applicable
- File `cn_map` which contains mappings of common names to UPN names for each smartcard certificate

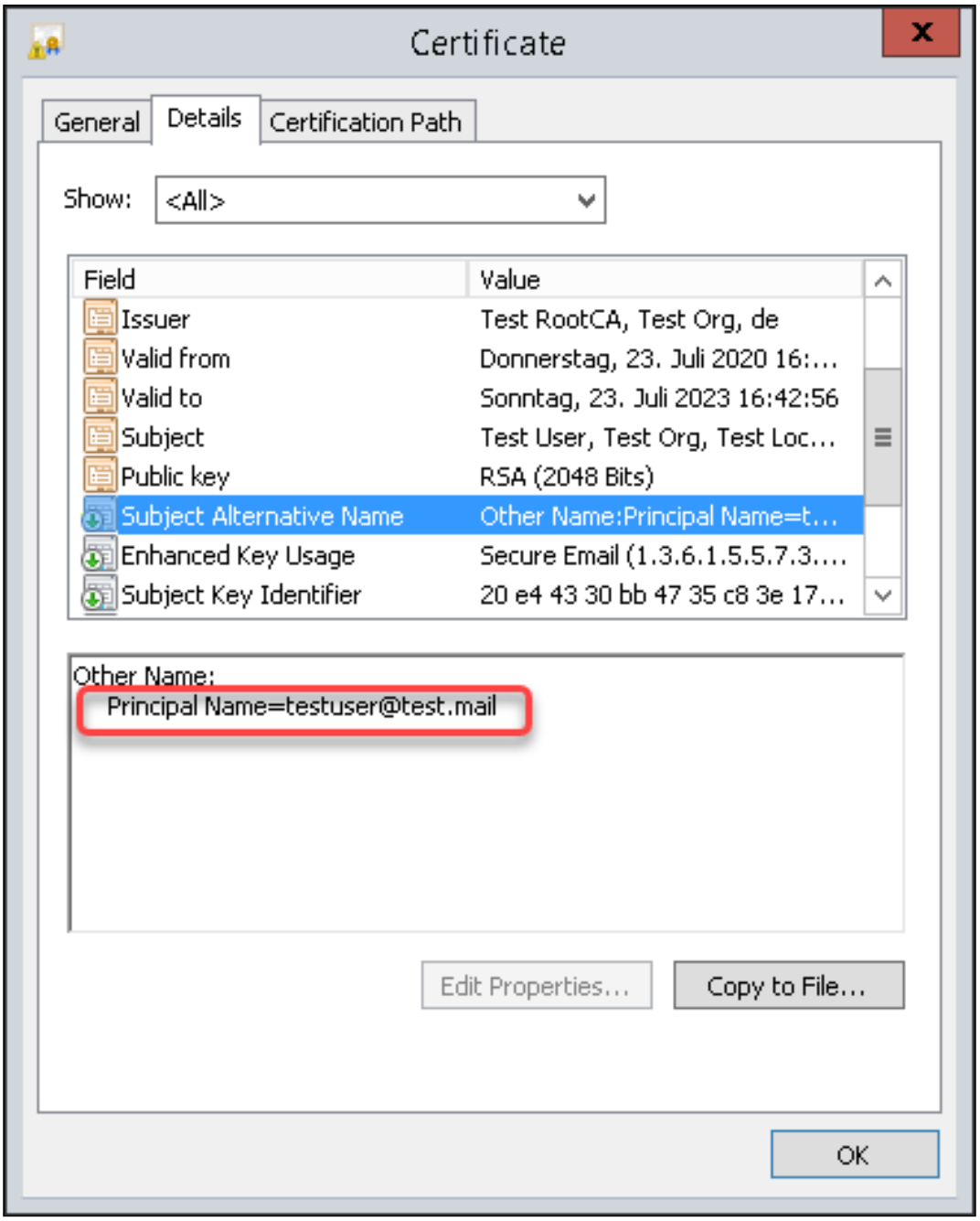
Creating the cn_map File

→ Create a file named `cn_map` in which each line is in the format `<common name> -> <logon name>` where

- `<common name>` is the common name part of the certificate's subject
  Example from a client certificate:



- `<logon name>` is the UPN name of the SubjectAltName extension of the certificate. The UPN name is dependent on whether Enterprise Kerberos names are enabled or disabled (the setting is described under Configuring the Devices (see page 809)):
  - When Enterprise Kerberos names are enabled, the user domain may differ from the default domain. In the following example, the user's domain is `test.mail`, while the default domain is `MY.DOMAIN`: `testuser@test.mail@MY.DOMAIN`
    Example from a client certificate:



- When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example: `testuser@MY.DOMAIN`

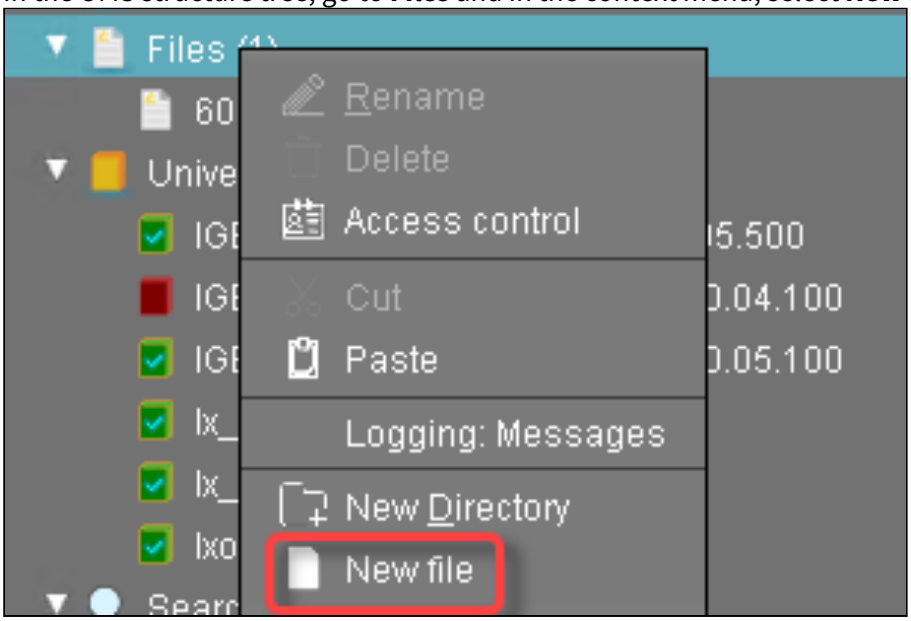
Example line: `Test User -> testuser@test.mail@MY.DOMAIN`

Transferring the cn_map File to the Devices

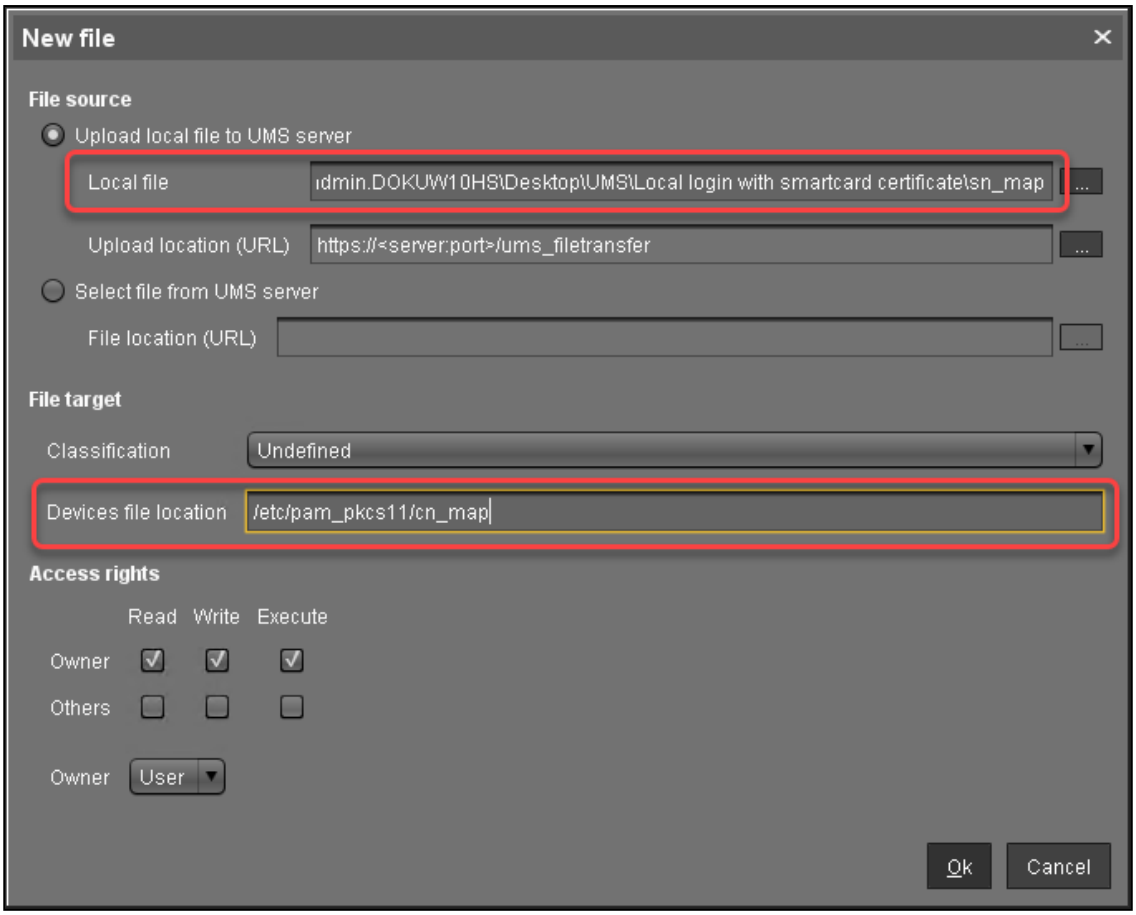
The `cn_map` file must be located in the directory `/etc/pam_pkcs11/cn_map`. This can be achieved via UMS file transfer.

To transfer the `cn_map` file to the devices:

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.

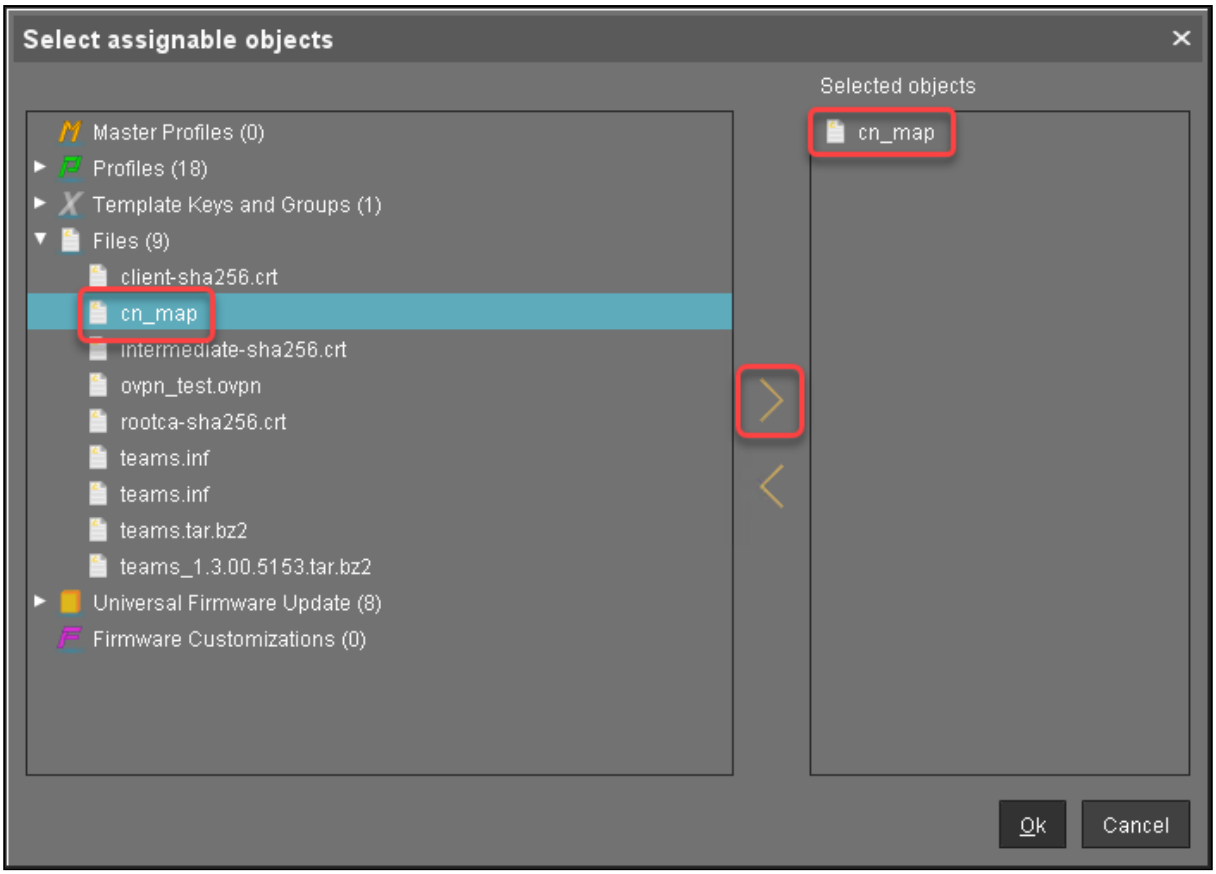


2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of the certificate. Use the file chooser by clicking ...
   - **Device file location**: `/etc/pam_pkcs11/cn_map`



3. Click **Ok**.
   The file object is created in the UMS.
4. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see Profiles in the IGEL UMS[103]).
5. In the **Assigned objects** area, click .
6. Under **Files**, select the file object using the button:

103. https://kb.igel.com/en/universal-management-suite/current/profiles-in-the-igel-ums



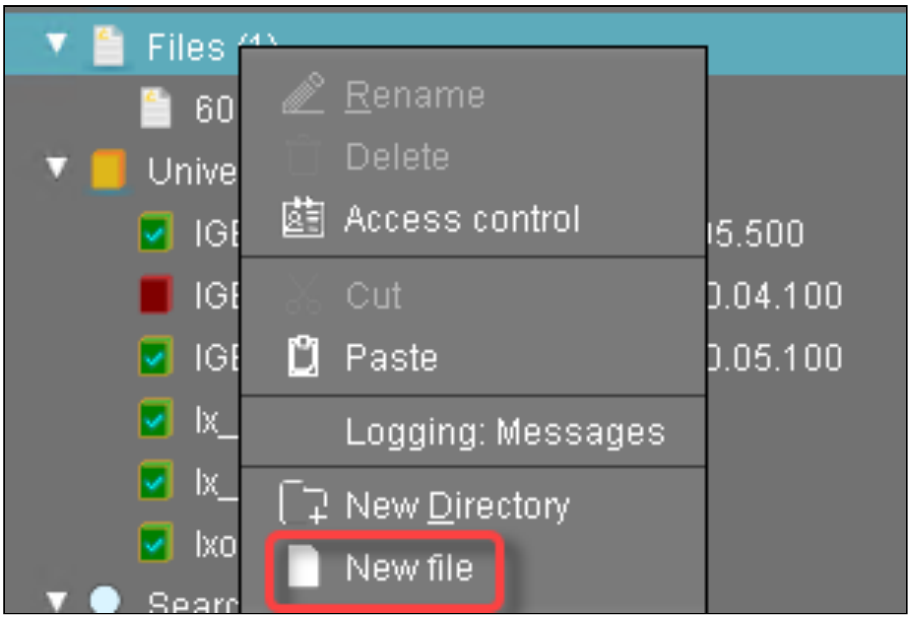
7. Click **Ok.**
8. In the **Update time** dialog, select **Now** and click **Ok**.
   The `cn_map` file is transferred to the endpoint device.

Transferring the Certificate Files to the Devices

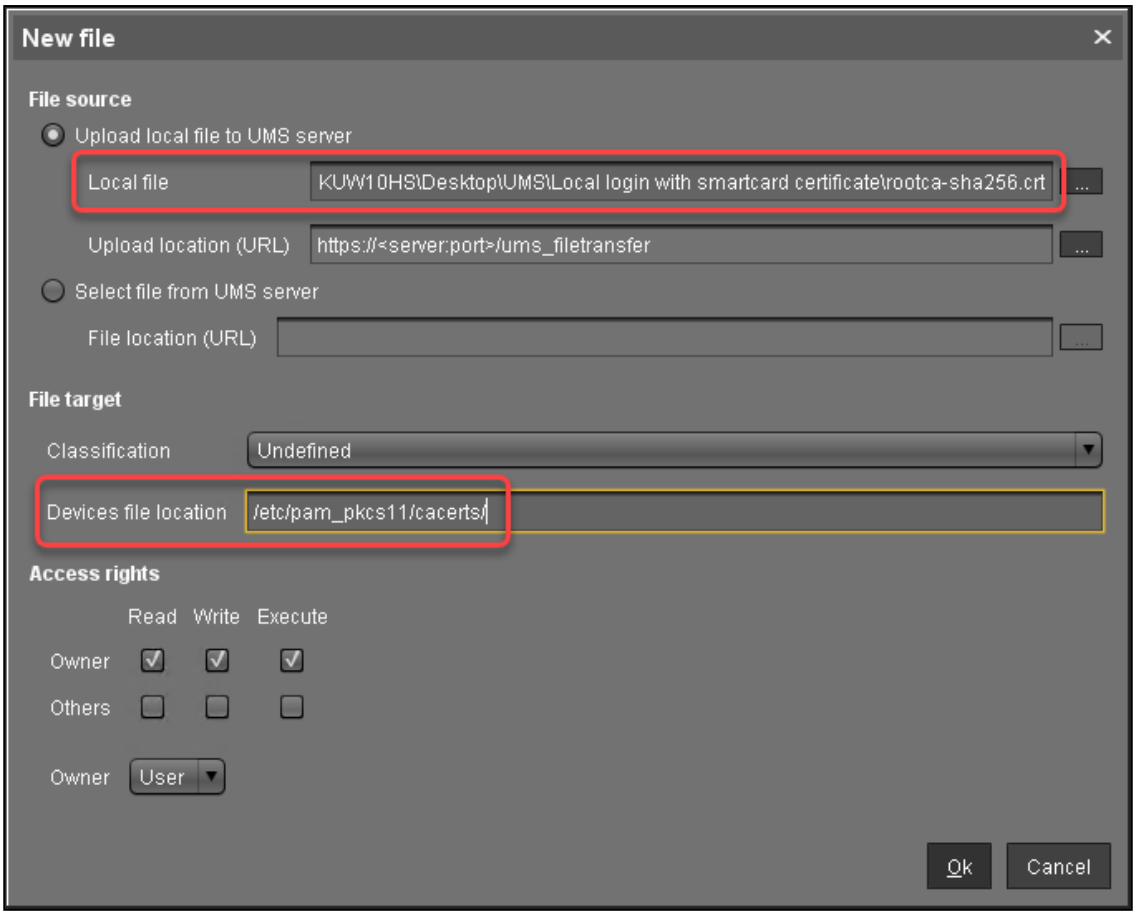
Registering the Certificate Files as File Objects

To transfer the certificate files to the devices, perform the following steps for each certificate file:

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of the certificate. Use the file chooser by clicking ....
   - **Device file location**: `/etc/pam_pkcs11/cacerts /`

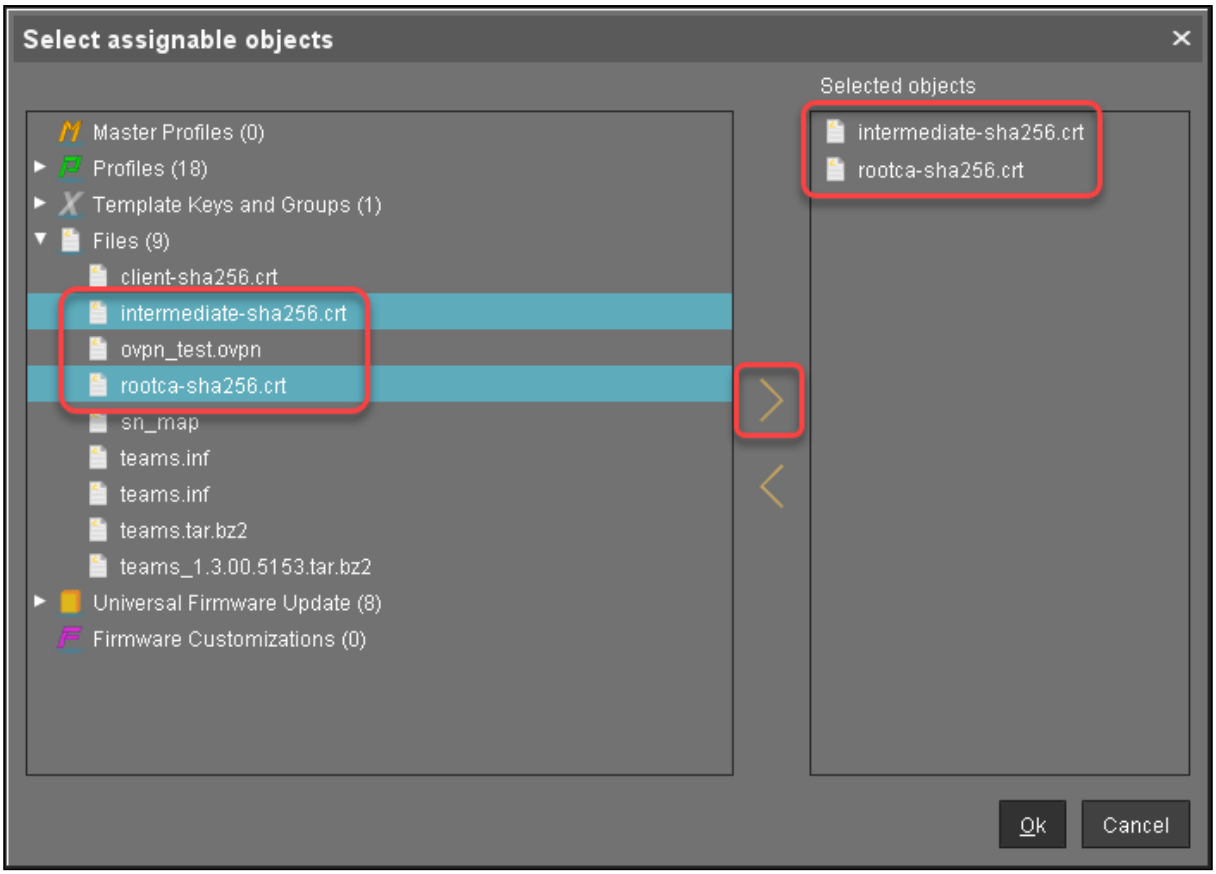


3. Click **Ok**.
   The file object is created in the UMS.

Assign the Certificate Files to the Devices

1. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see Profiles in the IGEL UMS[104]).
2. In the **Assigned objects** area, click ⊕.
3. Under **Files**, select the required file objects using the > button:

104. https://kb.igel.com/en/universal-management-suite/current/profiles-in-the-igel-ums



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.
   The certificates are transferred to the endpoint device.

Configuring the Devices

To enable local login with a smartcard certificate, you must configure the devices appropriately. For mass deployment, it is recommended to use a profile.

1. Go to **Security > Smartcard > Middleware** and select the middleware to be used.
2. Go to **System > Registry > auth > login > pkcs11** (registry key: `auth.login.pkcs11`) and activate **Login with smartcard certificate**.
3. Go to **System > Registry > auth > login > pkcs11_cert_policy** (registry key: `auth.login.pkcs11_cert_policy`) and enter the methods for certificate verification that are to be used. For further information, see the documentation in https://github.com/OpenSC/pam_pkcs11.
4. If Kerberos enterprise names are used, go to **System > Registry > auth > login > krb5_enterprise** and activate **Allow enterprise names**.

Debugging

→ If you need to debug the smartcard certificate login, go to **System > Registry > auth > login > pkcs11_debug** (registry key: `auth.login.pkcs11_debug`) and activate **Enable debugging of smartcard certificate login**.
Logging messages will be available via syslog.

Combination with the "AD/Kerberos with Smartcard" Method

Prerequisites

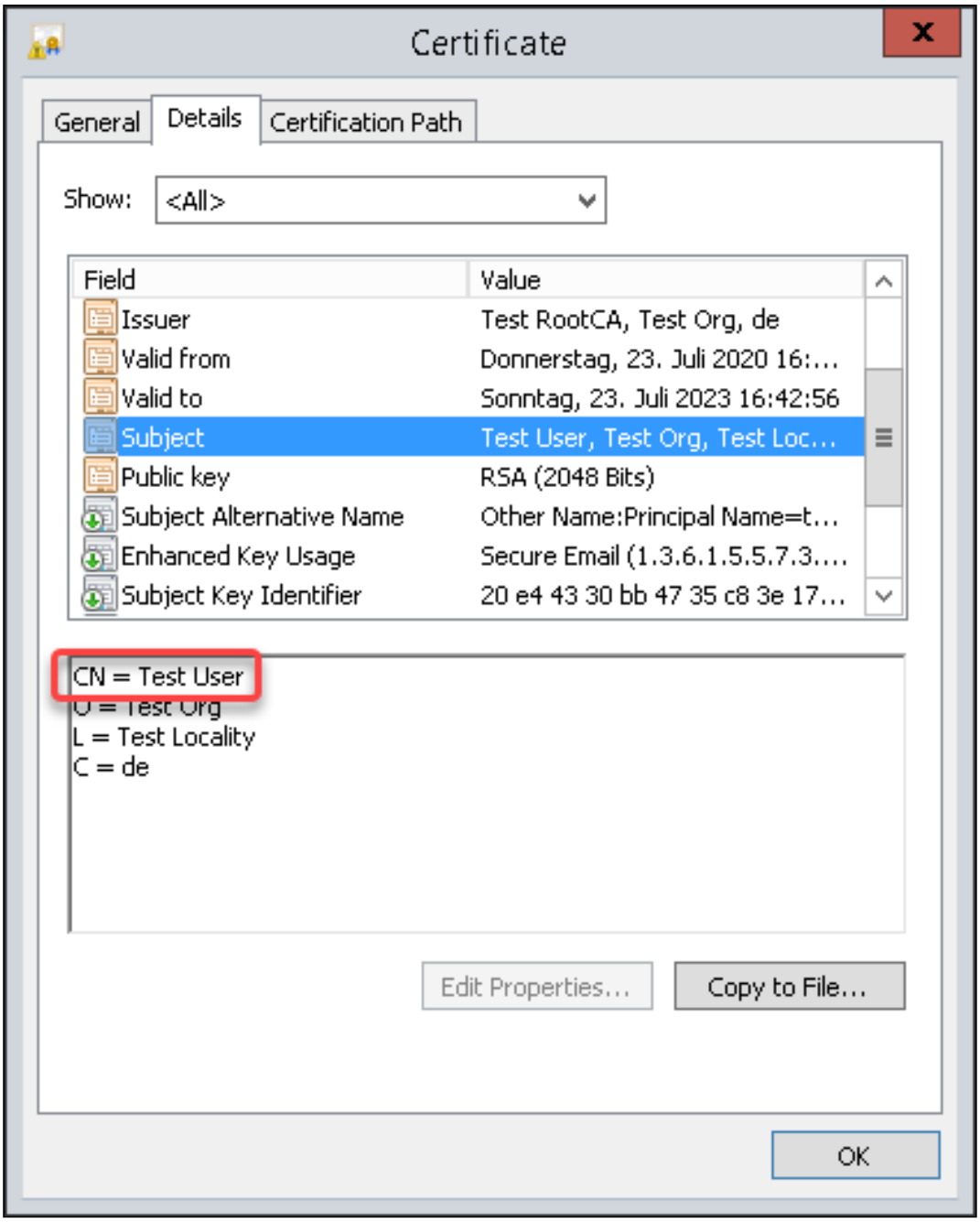
The following files are required:

- Root certificate and intermediate CA certificates, as applicable
- File `cn_map` which contains mappings of common names to UPN names for each smartcard certificate

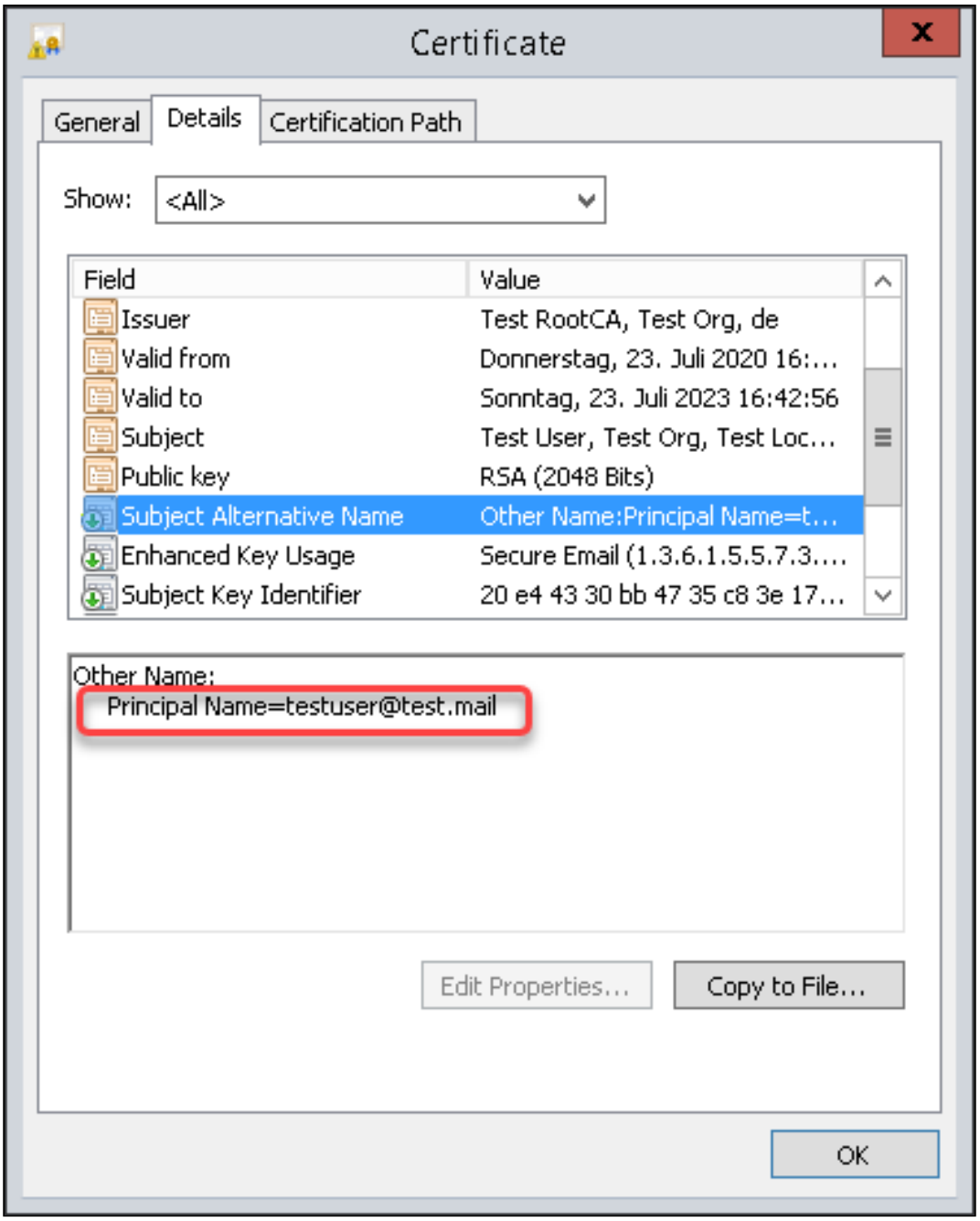
Creating the cn_map File

→ Create a file named `cn_map` in which each line is in the format `<common name> -> <logon name>` where

- `<common name>` is the common name part of the certificate's subject
  Example from a client certificate:



- `<logon name>` is the UPN name of the SubjectAltName extension of the certificate. The UPN name is dependent on whether Enterprise Kerberos names are enabled or disabled (the setting is described under Configuring the Devices (see page 819)):
  - When Enterprise Kerberos names are enabled, the user domain may differ from the default domain. In the following example, the user's domain is `test.mail`, while the default domain is `MY.DOMAIN`: `testuser@test.mail@MY.DOMAIN`
    Example from a client certificate:



- When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example: `testuser@MY.DOMAIN`

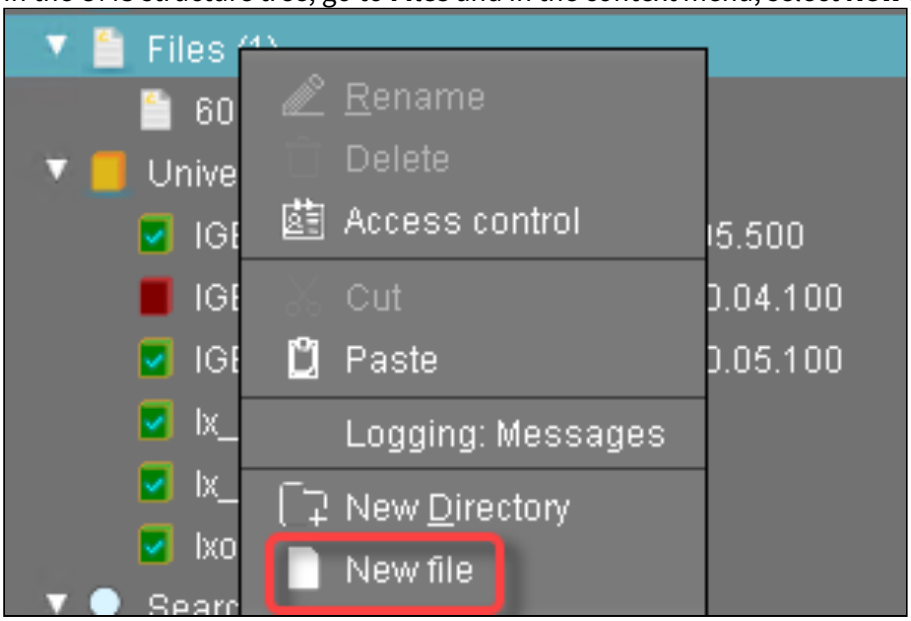
Example line: `Test User -> testuser@test.mail@MY.DOMAIN`

Transferring the cn_map File to the Devices

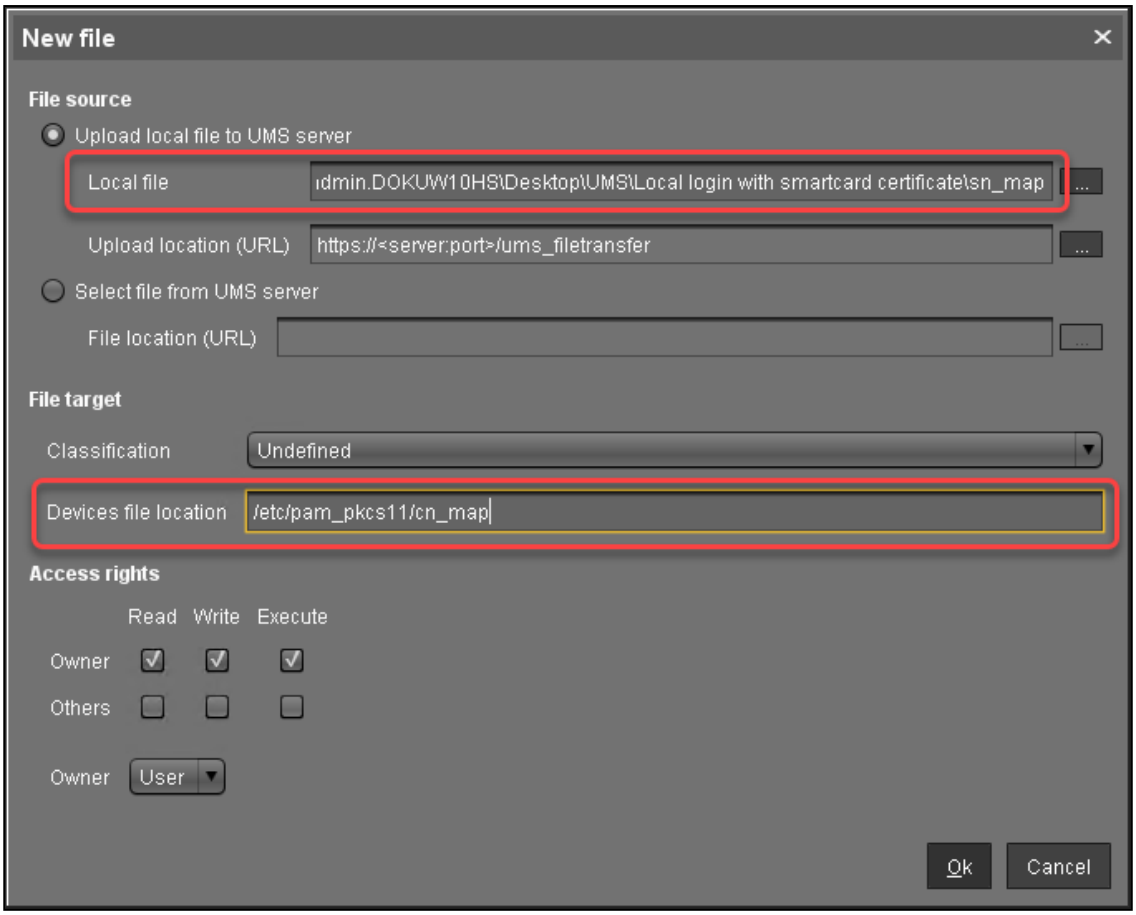
The `cn_map` file must be located in the directory `/etc/pam_pkcs11/cn_map`. This can be achieved via UMS file transfer.

To transfer the `cn_map` file to the devices:

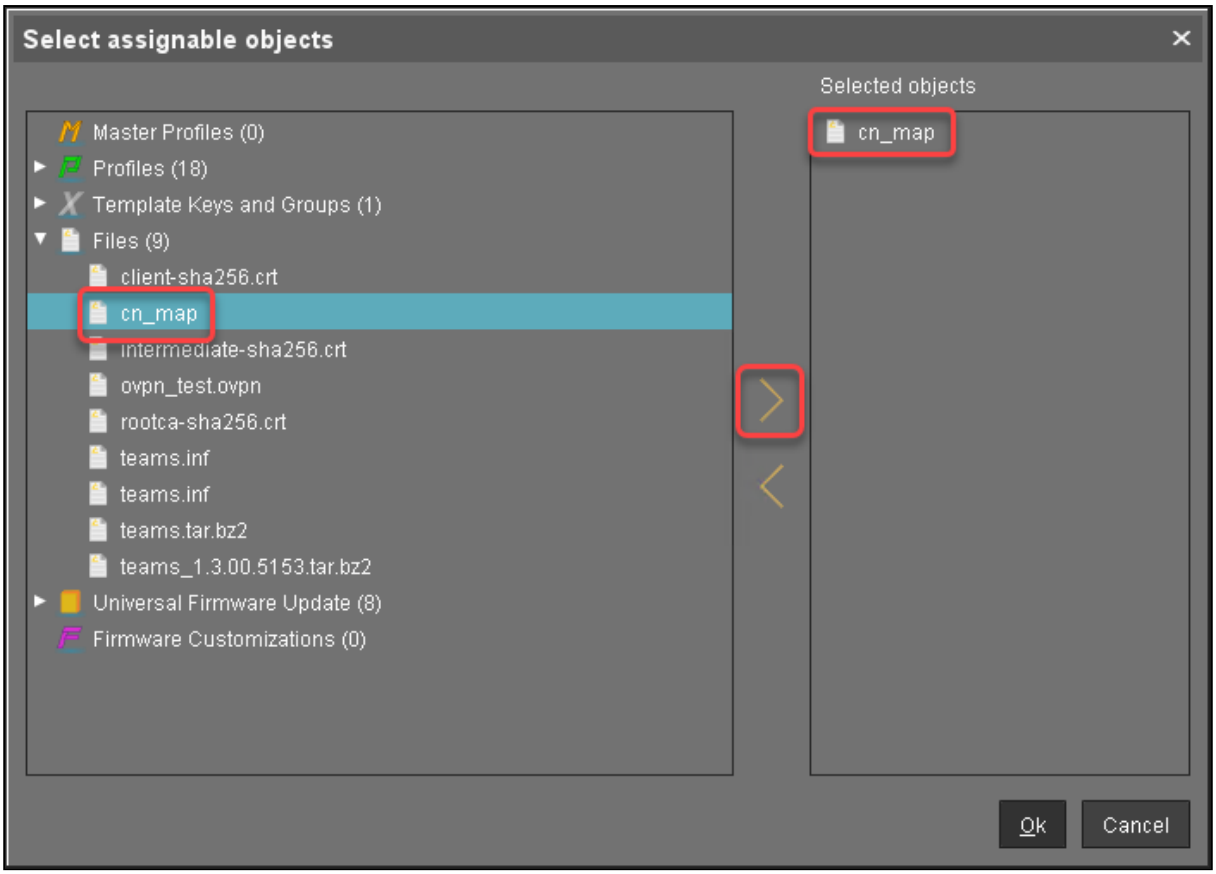
1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of the certificate. Use the file chooser by clicking ...
   - **Device file location**: `/etc/pam_pkcs11/cn_map`



3. Click **Ok**.
   The file object is created in the UMS.
4. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see (12.06.100-en) Profiles in the IGEL UMS).
5. In the **Assigned objects** area, click .
6. Under **Files**, select the file object using the button:



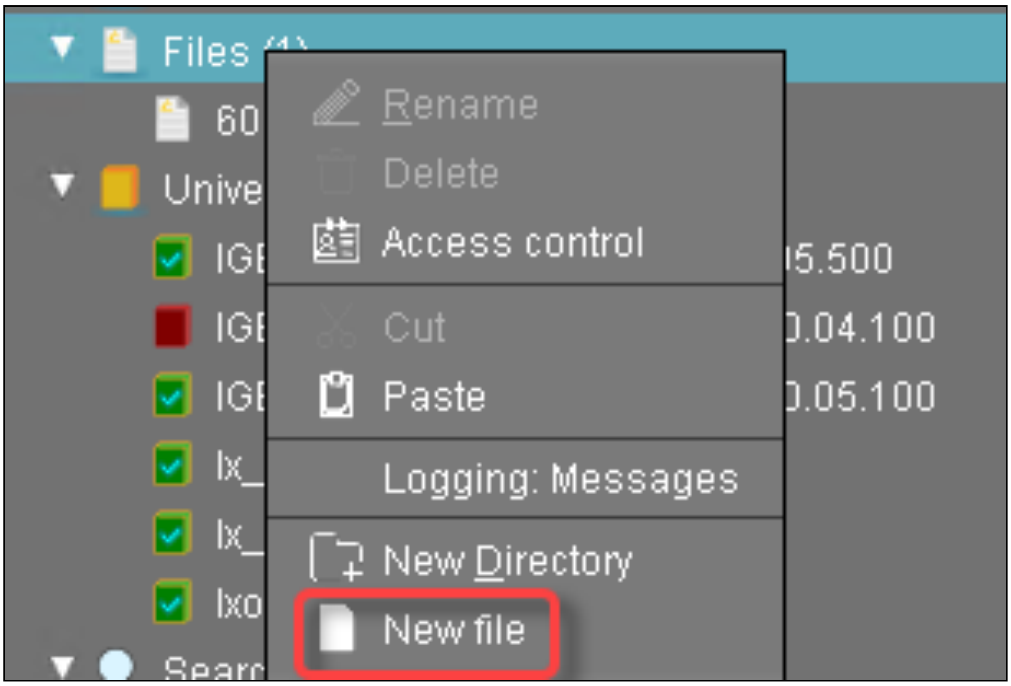
7. Click **Ok**.
8. In the **Update time** dialog, select **Now** and click **Ok**.
   The `cn_map` file is transferred to the endpoint device.

Transferring the Certificate Files to the Devices

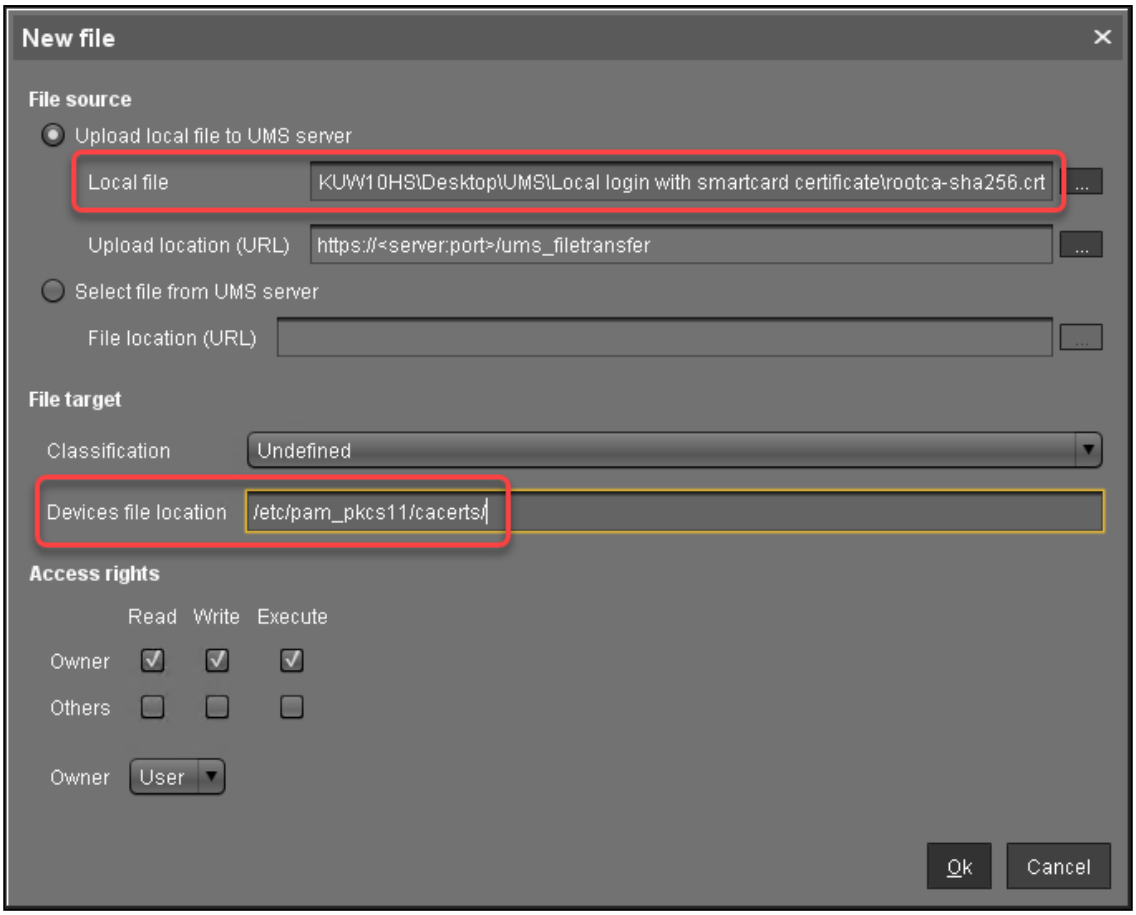
Registering the Certificate Files as File Objects

To transfer the certificate files to the devices, perform the following steps for each certificate file:

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



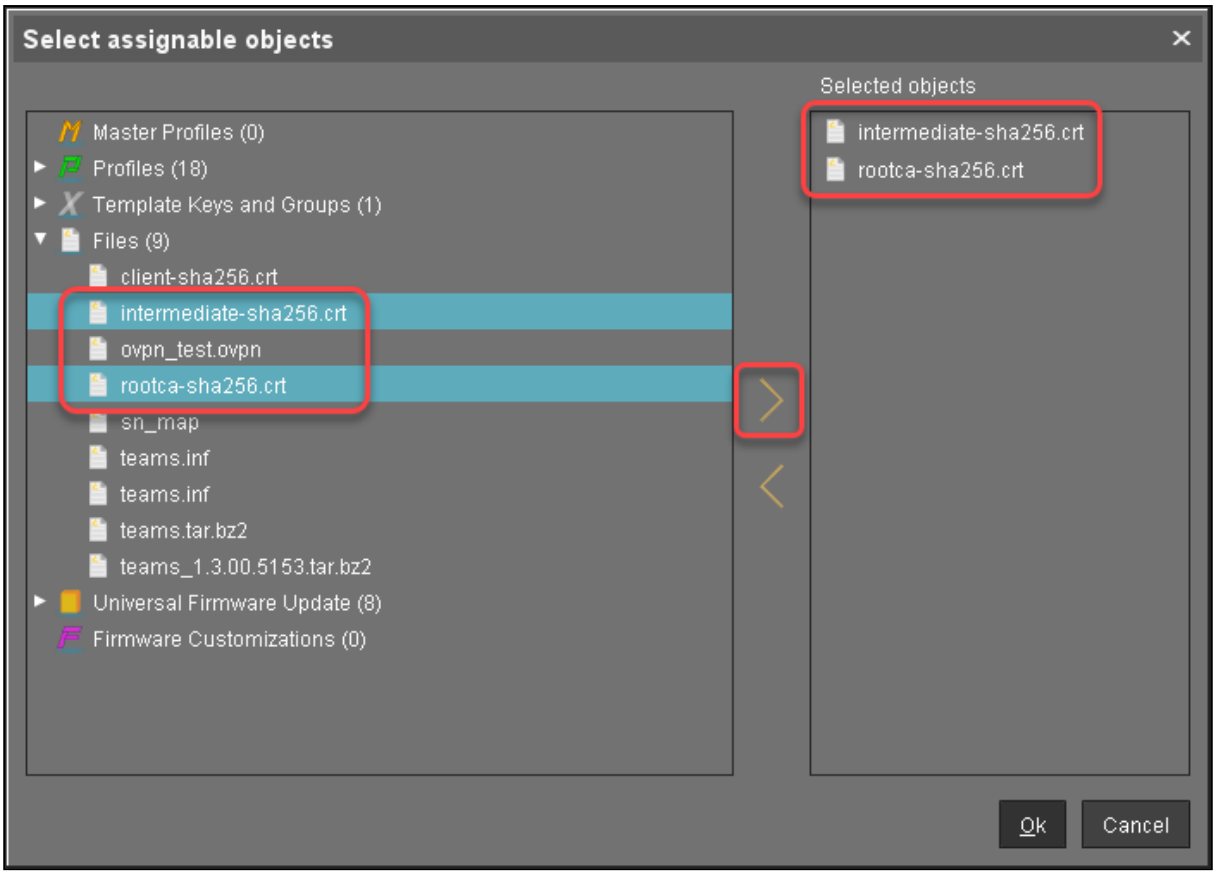
2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of the certificate. Use the file chooser by clicking ... .
   - **Device file location**: `/etc/pam_pkcs11/cacerts` `/`



3. Click **Ok**.
   The file object is created in the UMS.

Assign the Certificate Files to the Devices

1. In the UMS structure tree, select the endpoints for which you want to configure the local login with a smartcard certificate. For mass deployment, it is recommended to use a directory containing the endpoint devices or a profile (see (12.06.100-en) Profiles in the IGEL UMS).
2. In the **Assigned objects** area, click ⊕.
3. Under **Files**, select the required file objects using the button:



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.
   The certificates are transferred to the endpoint device.

Configuring the Devices

To enable local login with a smartcard certificate, you must configure the devices appropriately. For mass deployment, it is recommended to use a profile.

1. Go to **Security > Smartcard > Middleware** and select the middleware to be used.
2. Go to **Security > Active Directory/Kerberos**, activate **Enable**, and set **Default domain (fully qualified domain name)**. For details, see Active Directory/Kerberos (see page 2014) .
3. Go to **System > Registry > auth > login > pkcs11** (registry key: `auth.login.pkcs11`) and activate **Login with smartcard certificate**.
4. Go to **System > Registry > auth > login > pkcs11_cert_policy** (registry key: `auth.login.pkcs11_cert_policy`) and enter the methods for certificate verification that are to be used. For further information, see the documentation in https://github.com/OpenSC/pam_pkcs11.

5. If Kerberos enterprise names are used, go to **System > Registry > auth > login > krb5_enterprise** and activate **Allow enterprise names**.

Debugging

→ If you need to debug the smartcard certificate login, go to **System > Registry > auth > login > pkcs11_debug** (registry key: `auth.login.pkcs11_debug`) and activate **Enable debugging of smartcard certificate login**.
Logging messages will be available via syslog.

Desktop and Display

- Troubleshooting: Display Configurations Change with Downgrade of IGEL OS 11 (see page 822)
- Display Switch (see page 823)
- Screen Issues When Redocking Notebook (see page 827)
- Bluelight Filter for Nighttime Display (see page 828)
- Showing and Hiding the On-Screen Software Keyboard Automatically (see page 833)
- Screen Flickers on Intel Devices, Error Log Shows " [drm] *ERROR* CPU pipe C FIFO underrun" (see page 834)
- Multimonitor (see page 835)
- Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar (see page 847)
- Display Configuration for Shared Workplace (SWP) (see page 849)
- Using an External NVIDIA Graphics Card (see page 850)

Troubleshooting: Display Configurations Change with Downgrade of IGEL OS 11

You see an unwanted change in the display configurations when you are using multiple external displays and you downgrade your IGEL OS to 11.10.100 or later. After the upgrade, the configuration goes back to the original display config.

Environment

- Downgrading from IGEL OS 11.10.110 or later to IGEL OS 11.10.100 or later
- Hardware: Multiple external displays

Problem

With the 6.6.x kernel there was a bigger change in the connector enumeration handling of the i915 driver which causes the display connectors to switch after the downgrade. There is a default setting implemented that reverses the order back to the original, but for some hardware a manual reset is needed.

Solution

Use the registry key to change the connector order of intel GPUs. As newer kernels changed the order this can be used to revert it to the former state:

1. In the IGEL Setup, go to **System > Registry > x.drivers.intel.reverse_connector_enumeration**.
2. Set the **Reverse the connector enumeration** parameter to **Yes**.

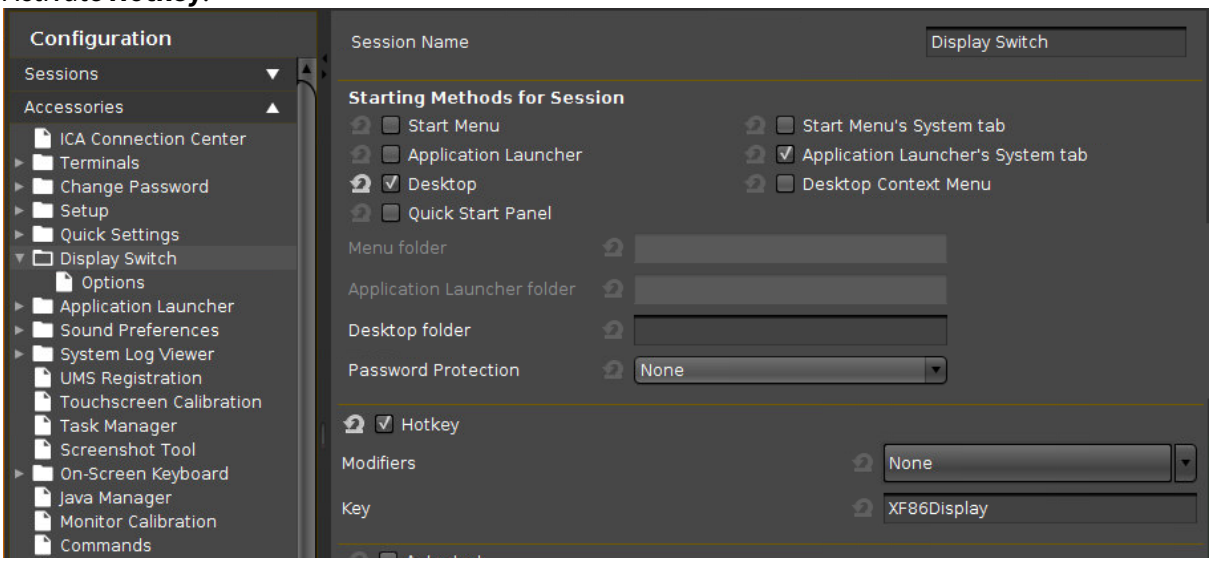
Display Switch

If you are using a notebook with IGEL UDC2, UDC3, or UD Pocket, you might want to connect an additional monitor. If you are using an IGEL thin client (UD series), you might want to use two monitors. Any thinkable display mode, like clone mode/mirroring or extended mode, is possible. Moreover, you can change between the display modes quickly.

Configure a Starter for the Display Switch

There are many ways to start the display switch. The following example shows how to define a hotkey typical for a notebook.

1. Open the Setup and go to **Accessories > Display Switch**.
2. Activate **Hotkey**.



By default, [Fn]+[F7] (`XF86Display`) is defined as the hotkey for starting the display switch. You can change the hotkey by selecting or entering different keys in **Modifiers** and **Key**.

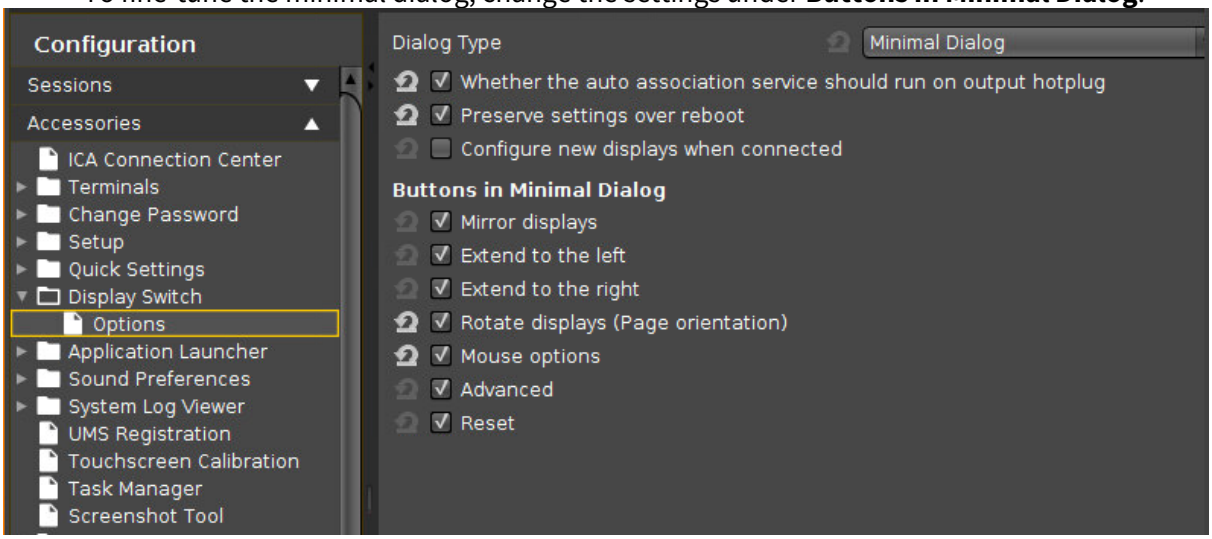
> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard` . Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

3. Press **Apply** or **Ok**.

Configure the Display Switch

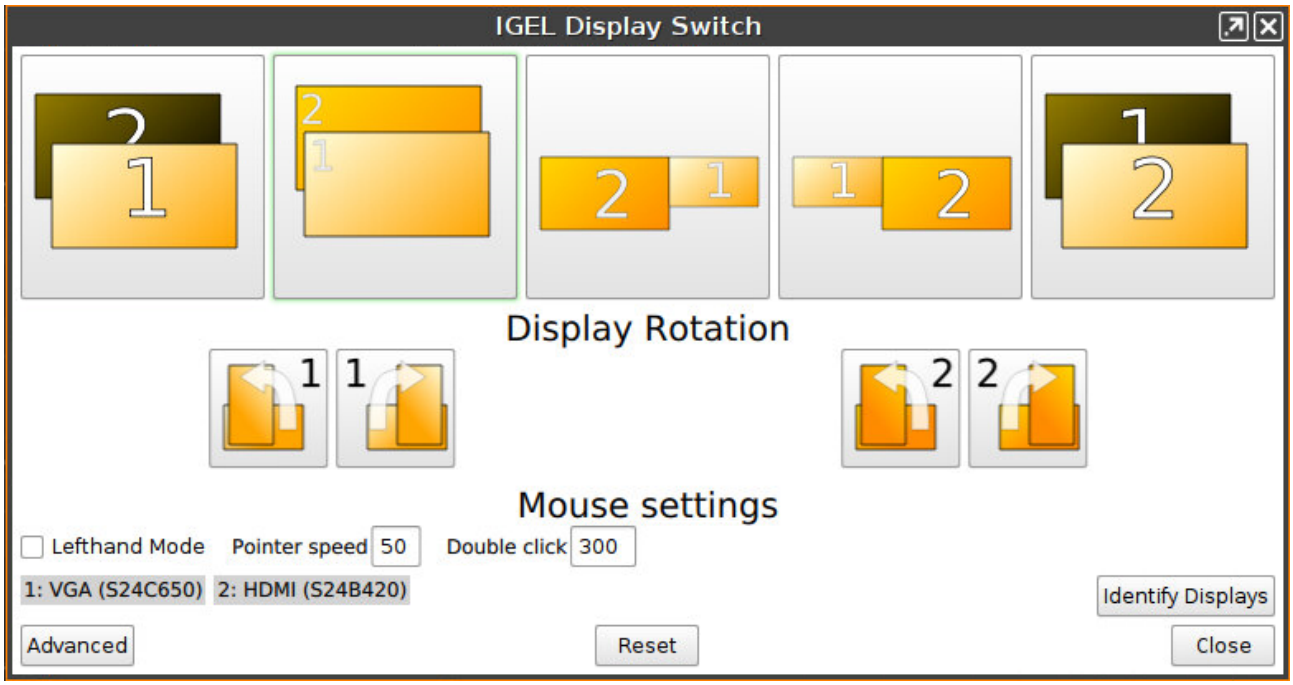
1. Open the Setup and go to **Accessories > Display Switch > Options**.
2. Consider the following settings:

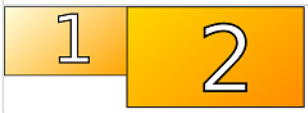
- **Dialog Type**: In most cases, you can leave it at **Minimal Dialog**. The user can always switch to the advanced dialog, provided that **Advanced** in the **Minimal Dialog** area is activated.
- **Smart display configuration**: Activate this option, if you want to save all your display configurations.
- **Preserve settings over reboot**: Activate this if the settings made by the display switch are to remain unchanged after reboot.
- **Configure new displays when connected**: Activate this if you want the display switch to start automatically as soon as a new monitor is connected.
- To fine-tune the minimal dialog, change the settings under **Buttons in Minimal Dialog**.

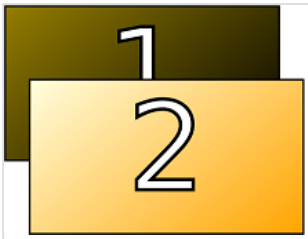
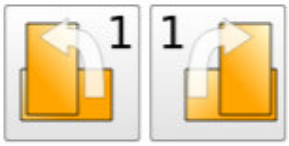


Use the Display Switch

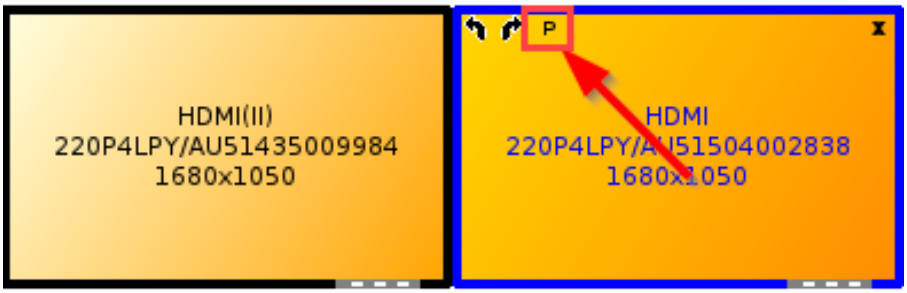
The minimal dialog will look similar to this; details depend on your specific setup:



Button	Function
	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the right.
	Extends the display area to the screen on the left

	Uses only display 2.
	Rotates the selected display to the left or to the right.

For more information, see the manual chapter Using Display Switch (see page 1737).



The **P** marks the primary Display**.**

Screen Issues When Redocking Notebook

Environment

UDC-converted notebooks running IGEL Linux *5* and above.

Issue

When you take a notebook off the dock, e. g. to move to meeting rooms or other locations, and redock the notebook, the screen resolution ends up wrong, sometimes with a black screen and other similar screen issues.

Solution

1. In Setup, go to **Accessories > Display Switch > Options**.
2. Enable **Configure new Displays when connected**.
   The display switch will start when the notebook is redocked.
3. Use the display switch to configure the display appropriately. For further information, see the Tips & Tricks article Display Switch (see page 823).
4. Click **Ok** to save the settings.

Legal Note

IGEL's Terms & Conditions[105] apply.

105. https://www.igel.com/terms-conditions/

Bluelight Filter for Nighttime Display

You can configure a blue light filter in your IGEL OS device to reduce your display's percentage of blue light display for nighttime use.

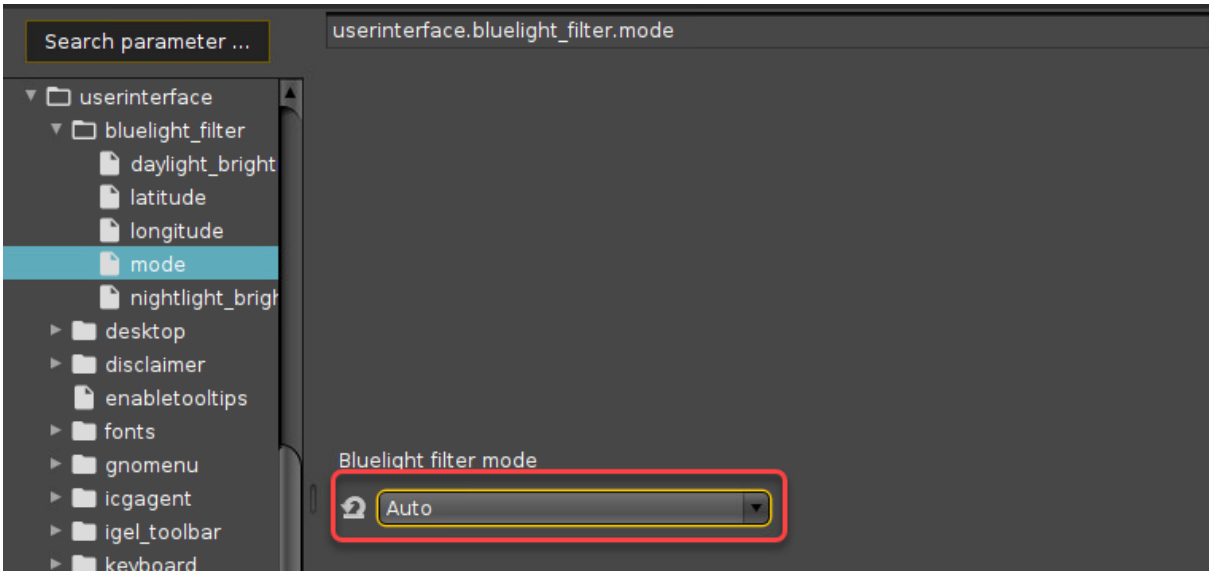
By default, the blue light filter is disabled.

Automatic Retrieval of the Geodata (Recommended)

When you select automatic mode, IGEL OS will collect the geo-coordinates for your device to determine the right time zone. For this purpose, Geoclue is used. Geoclue utilizes a variety of location sources, e.g. the Mozilla Location Service. For more information about Geoclue, see https://gitlab.freedesktop.org/geoclue/geoclue/-/wikis/home. For more information about the Mozilla Location Service, see https://wiki.mozilla.org/CloudServices/Location.

Based on this data, it will switch the display to daylight brightness at sunrise time and switch it to nighttime brightness at sunset time.

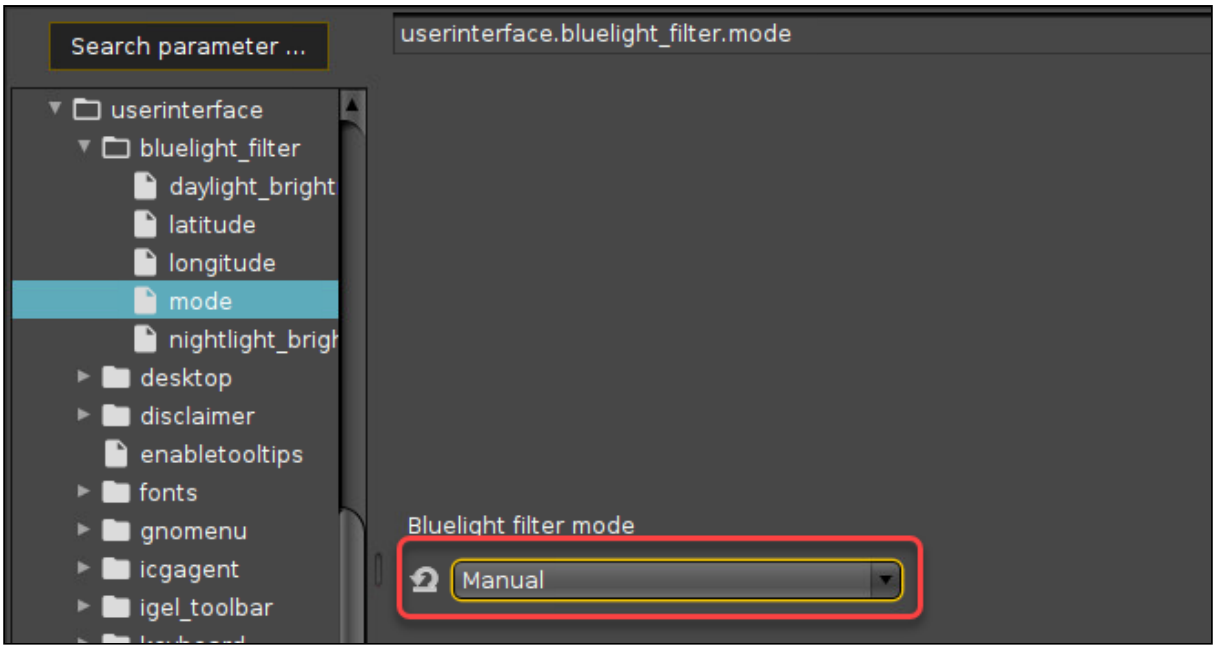
1. Open the configuration dialog and set **System > Registry > userinterface > bluelight_filter > mode** to **Auto**.



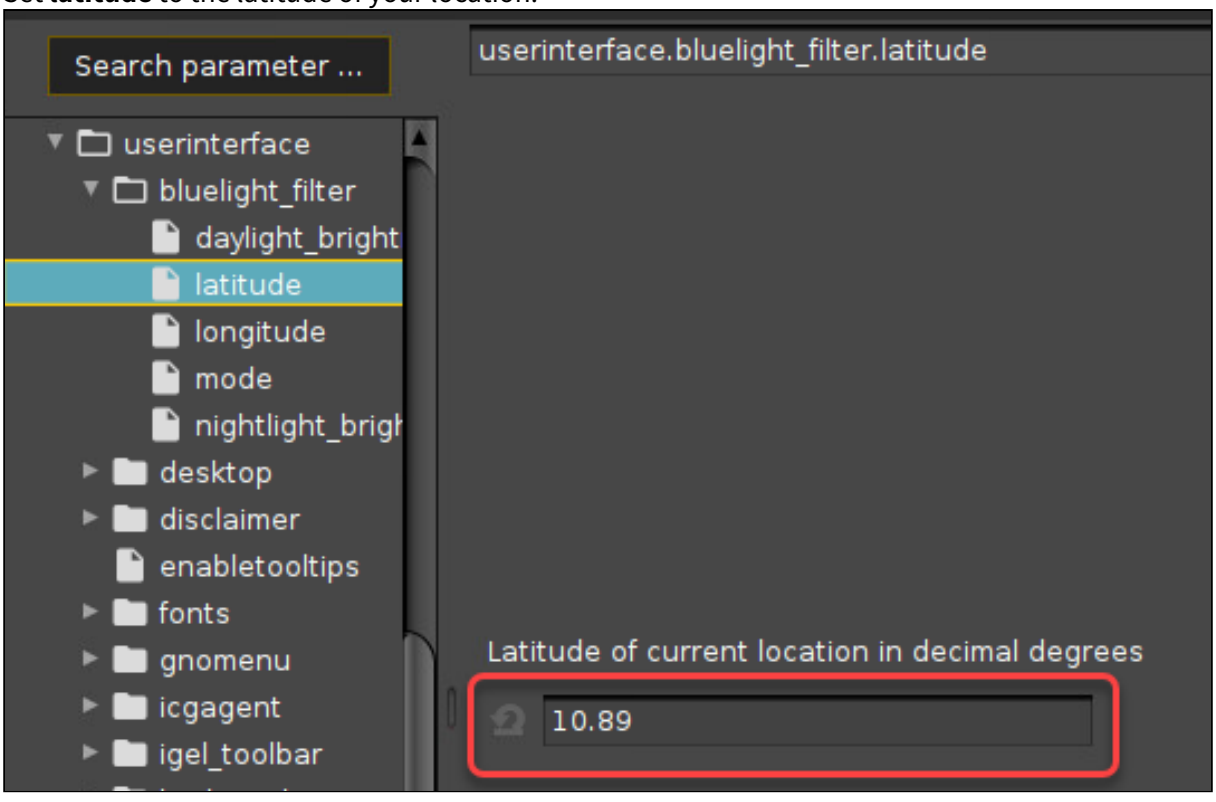
2. Continue with configuring the **Daylight and Nightlight Brightness** below.

Setting the Geodata Manually

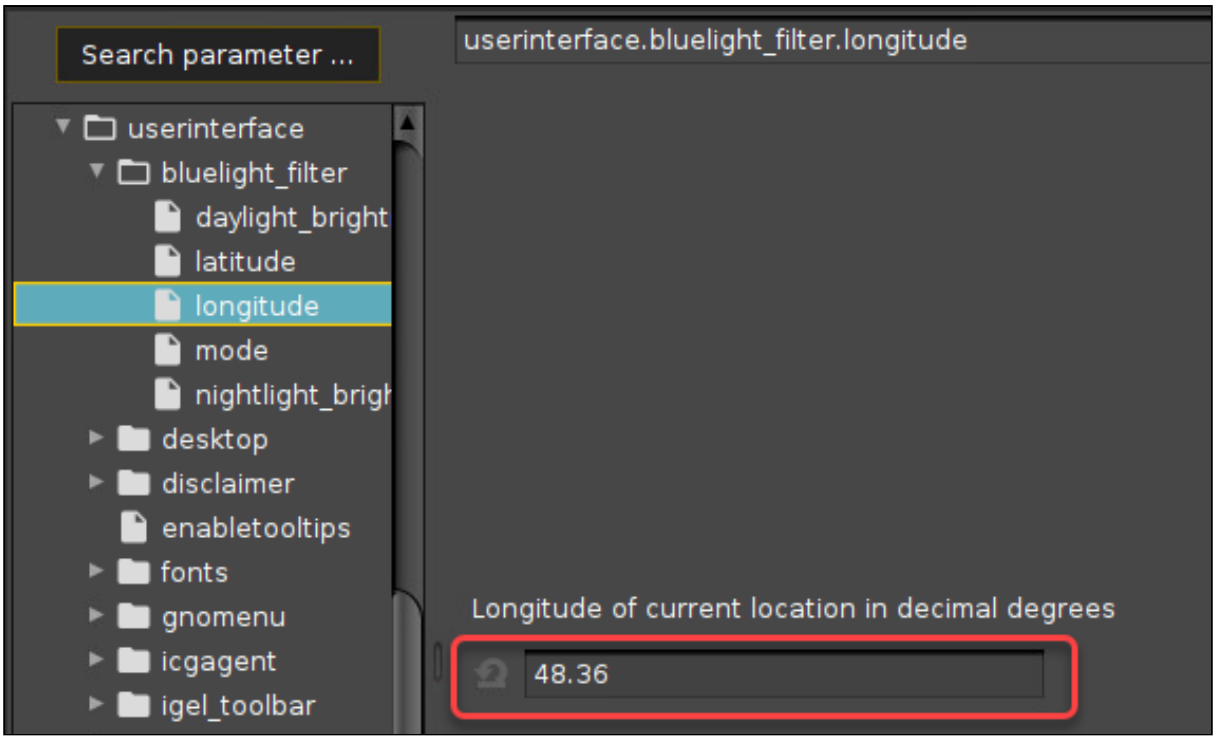
1. Open the configuration dialog and set **System > Registry > userinterface > bluelight_filter > mode** to **Manual**.



2. Set **latitude** to the latitude of your location.



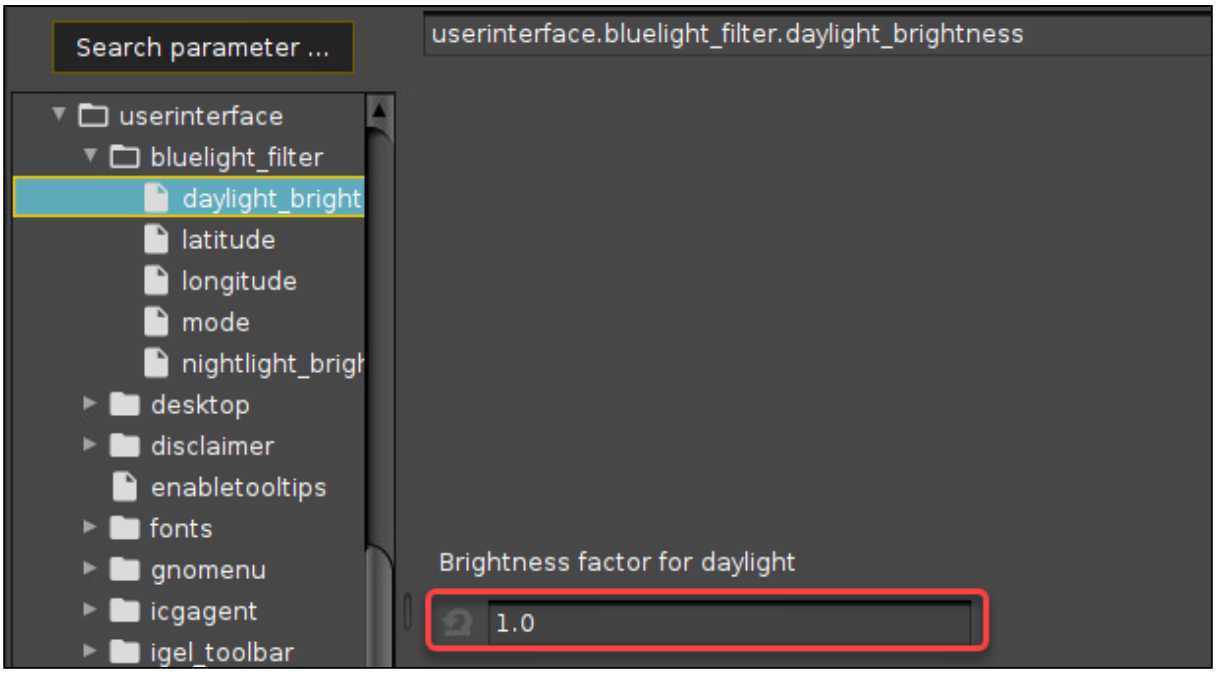
3. Set **longitude** to the longitude of your location.



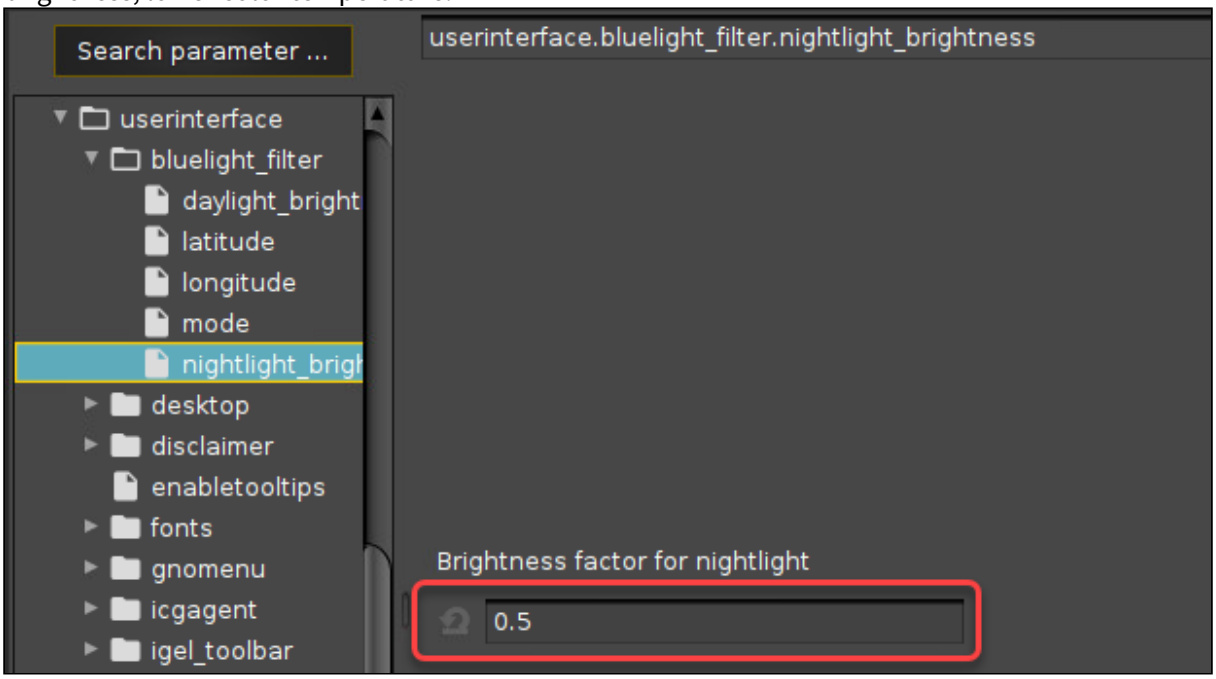
4. Continue with configuring the Daylight and Nightlight Brightness.

Daylight and Nightlight Brightness

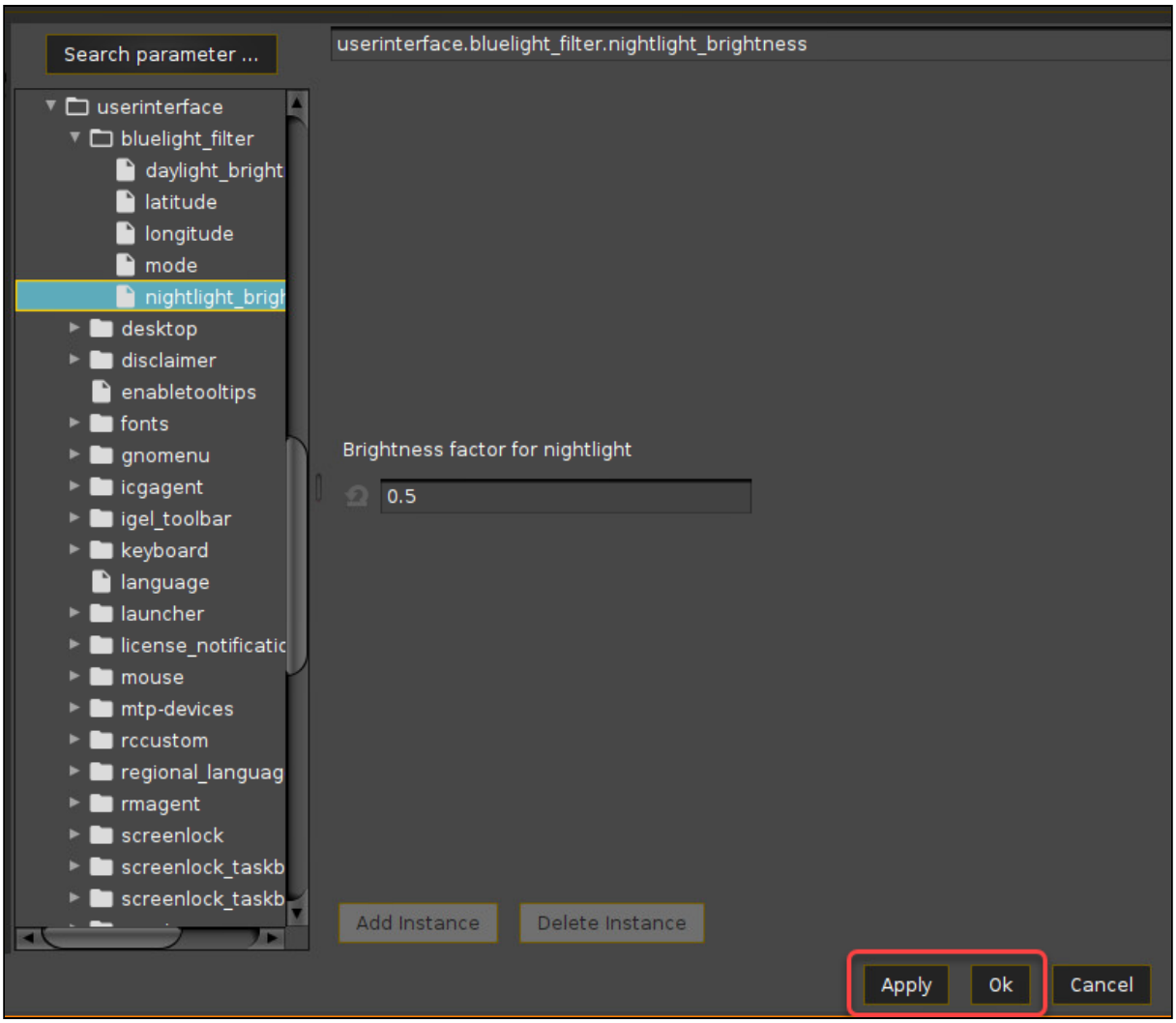
1. Go to **daylight brightness** and set the value according to your needs. Example: 1.0 = full brightness, high color temperature



2. Go to **nightlight brightness** and set the value according to your needs. Example: 0.5 = 50% brightness, lower color temperature.



3. Click **Apply** or **Ok** to save your changes.


Search parameter ...
userinterface.bluelight_filter.nightlight_brightness
userinterface
bluelight_filter
daylight_bright
latitude
longitude
mode
nightlight_brigh
desktop
disclaimer
enabletooltips
fonts
gnomenu
icgagent
igel_toolbar
keyboard
language
launcher
license_notificatic
mouse
mtp-devices
rccustom
regional_languag
rmagent
screenlock
screenlock_taskb
screenlock_taskb
Brightness factor for nightlight
0.5
Add Instance
Delete Instance
Apply
Ok
Cancel

Showing and Hiding the On-Screen Software Keyboard Automatically

You can configure the on-screen software keyboard to appear or disappear automatically when an input box is selected or deselected (e. g. Firefox or screenlock).

Showing Automatically

With the following setting, a software keyboard will be shown automatically when an input box is focused.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autoshow** (parameter: `userinterface.softkeyboard.autoshow`).
2. Enable **Automatically show on-screen keyboard when text field is selected**.

Hiding Automatically

With the following setting, the software keyboard will be hidden automatically when an input box is not focused anymore.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autohide** (parameter: `userinterface.softkeyboard.autohide`)
2. Enable **Automatically hide on-screen keyboard when text field is deselected**.

If there are any problems, e. g. the keyboard does not hide automatically, you have to disable **Automatically hide on-screen keyboard when text field is deselected** and make sure that the following Setup parameters have been enabled:

- **Accessories > On-Screen Keyboard > Autostart**
- **Accessories > On-Screen Keyboard > Restart**

Screen Flickers on Intel Devices, Error Log Shows " [drm] *ERROR* CPU pipe C FIFO underrun"

Environment

- Intel devices with IGEL OS 11.08.200

Issue

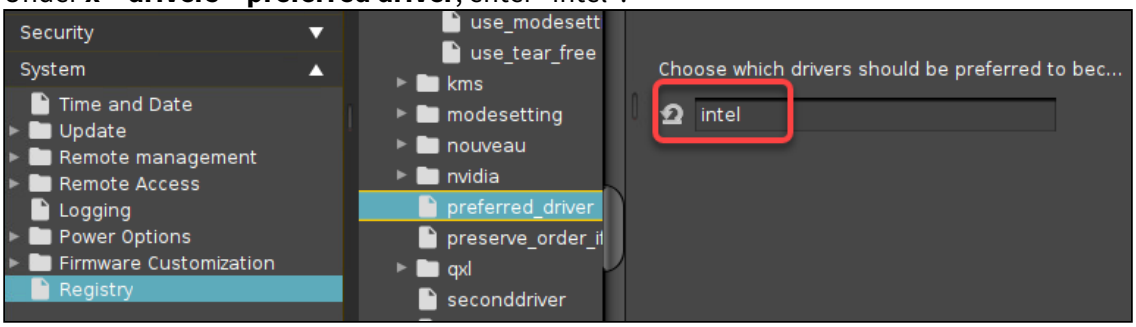
On Intel devices, the screen flickers. The error logs contain lines like the following (example):

```
Nov 09 14:21:58 M-TC-12883 kernel: i915 0000:00:02.0: [drm] *ERROR* CPU pipe C FIFO underrun
```

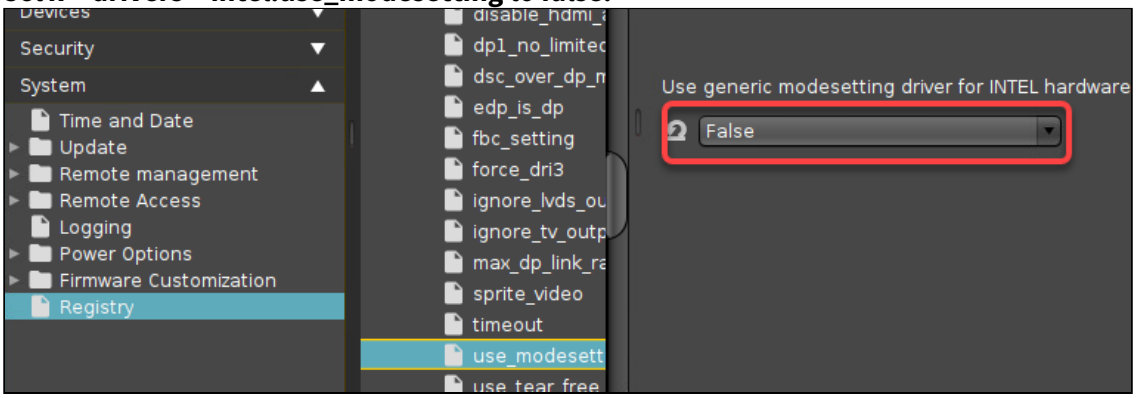
Solutions

Use one of the following methods to resolve the issue:

- In the UMS Configuration Dialog or the local Setup of the affected devices, go to **System > Registry** and make the following changes:
  - Under **x > drivers > preferred driver**, enter "intel".



  - Set **x > drivers > intel.use_modesetting** to **false.**



- Downgrade your devices to a version lower than 11.08.200.

Multimonitor

Working with two or more screens is becoming increasingly popular in professional working environments.

You can find out how to configure several screens and an extended desktop with the IGEL setup here.

There are different screen configuration options:

- Automatic Configuration (see page 836)
- Manual Configuration (see page 838)
- Additional Settings (see page 840)
- Auto Switch Monitor Configuration for Laptops (see page 845)

If you work with IGEL Universal Desktop or supported UDC2 hardware, multimonitor support is guaranteed.

Difficulties may arise if you work with UDC2 hardware and your hardware is not fully supported by IGEL.

> Multimonitor configuration for unsupported hardware only works if native graphic driver support functions properly. You must ensure that the native driver really does work because the fallback VESA driver does not allow multimonitor configuration. Click **About** in the **Application Launcher** to determine which graphic chipset you work with. If VESA is listed there, the native driver will not work and multimonitor configuration will not be possible.

->See the Linux 3rd party hardware database[106] for supported graphic cards.

106. https://www.igel.com/linux-3rd-party-hardware-database/

Automatic Configuration

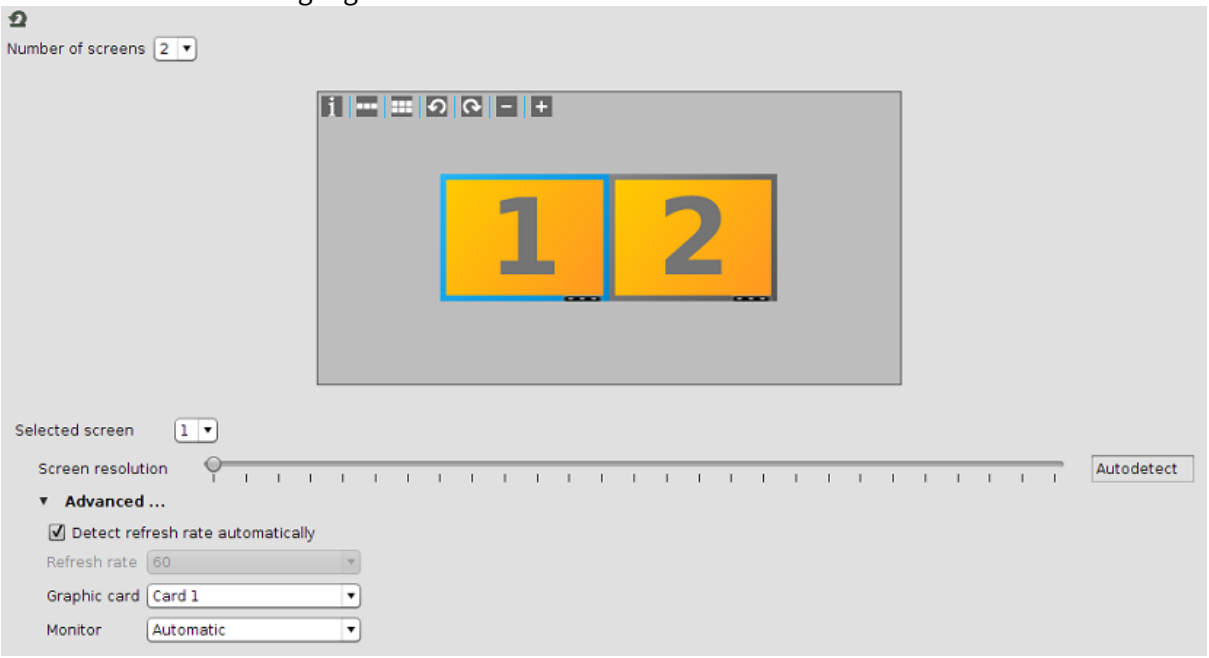
The firmware recognizes the native graphic driver and will apply the screens automatically by default.

Define two or more monitors:

1. Go to **User Interface > Display** in the structure tree.
2. Select **2** (or more) under **Number of screens**.

> The number of monitors that you can select depends on your hardware. Using the Universal Management Suite (UMS), you can choose up to 8 monitors.

3. Choose the screen under **Selected screen** or by clicking it with a mouse.
   The selected screen is highlighted with a blue frame:



4. Set **Screen Resolution** to **Autodetect** (default setting).
   The operating system reads out the EDID (Extended Display Identification Data) of the monitors through DDC (Display Data Channel). With these data, the correct resolution for the monitors can be recognized and set.

> If the **Autodetect** resolution is not available check **Monitor probing (DDC)** under **User Interface > Display > Options**. The **Monitor probing (DDC)** must be enabled (default setting).

> With more than 2 monitors, the screen resolution has to be specified for each screen manually.

5. Enable **Detect refresh rate automatically** (default setting) under **Advanced**.

6. Set **Monitor** to **Automatic**.
   The selected screen is automatically assigned to the graphic connector (monitor).
7. Drag and drop the rectangles to position the screens.

   > Screen 1 is always the primary screen where the taskbar is situated.

8. Click **Apply** or **OK** to save the settings.

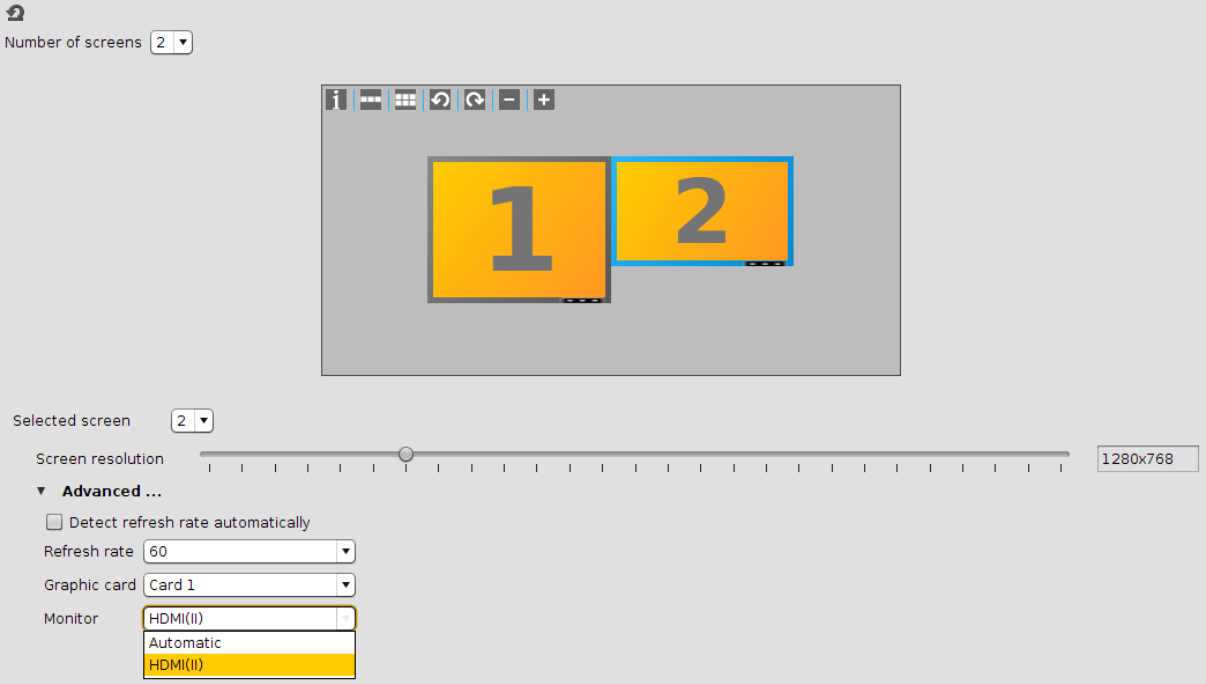
Manual Configuration

During automatic configuration, the following problems can sometimes arise:

- One of the screens remains black.
- There is the same display on all screens.

In this case, you can set the screens manually:

1. Go to **User Interface > Display** in the structure tree.



2. Select a screen number under **Selected screen**.
3. Specify the resolution manually under **Screen resolution**.

> The standard resolution setting is **Autodetect**.

> From IGEL Linux Version 10.03.100, you have the option of defining your own resolutions via the registry (`x.xserver0.custom_resolution`). In order for the values set there to take effect, the resolution must be set to **Autodetect** (the slider at the far left). The following parameters apply to the entry in the registry:
>
> - `WxH` : W = width, H = height (example: 1920x1080)
> - `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

4. Select for all screens the respective connector under **Monitor**. The manual configuration can take effect only if you assign the monitor connector to all screens.

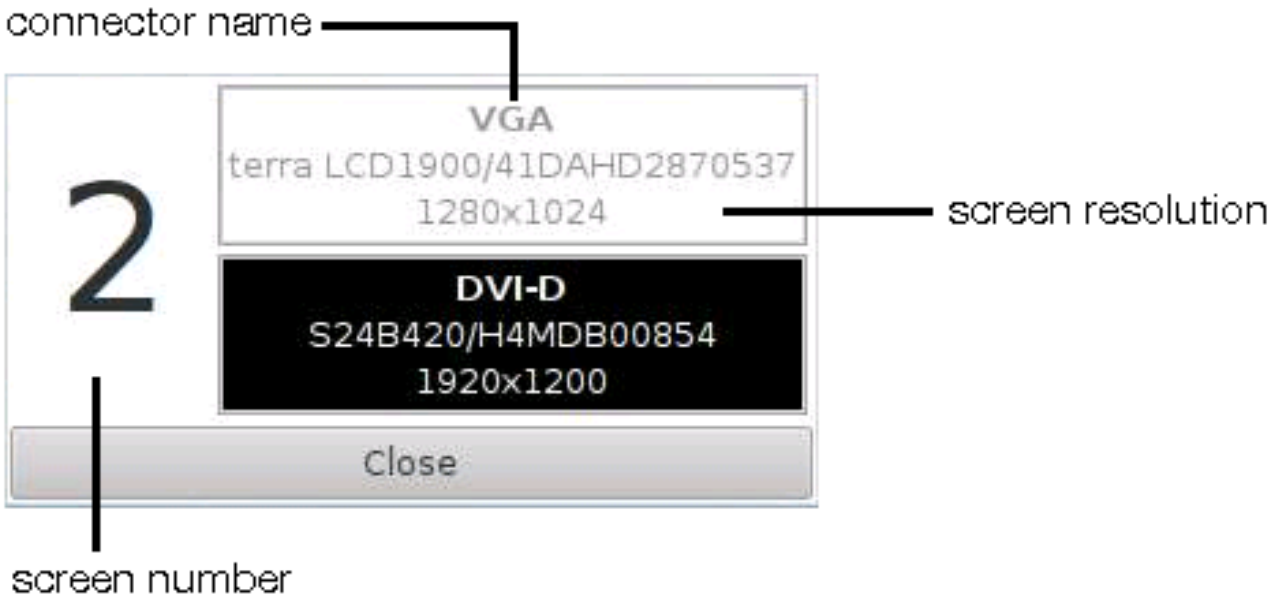
   > If you adjust the settings directly in IGEL Setup, only the connected monitors will be available in the selection list. If you want to configure the screens using the UMS profile, all possible connectors will be shown in the selection list and you will not know which one is relevant for your device.

Tip:

->Click in your client setup to obtain information about the connector names, screen resolutions and screen numbers.

> This configuration cannot be accessed from the UMS.

The black field belongs to the screen number on the left side:



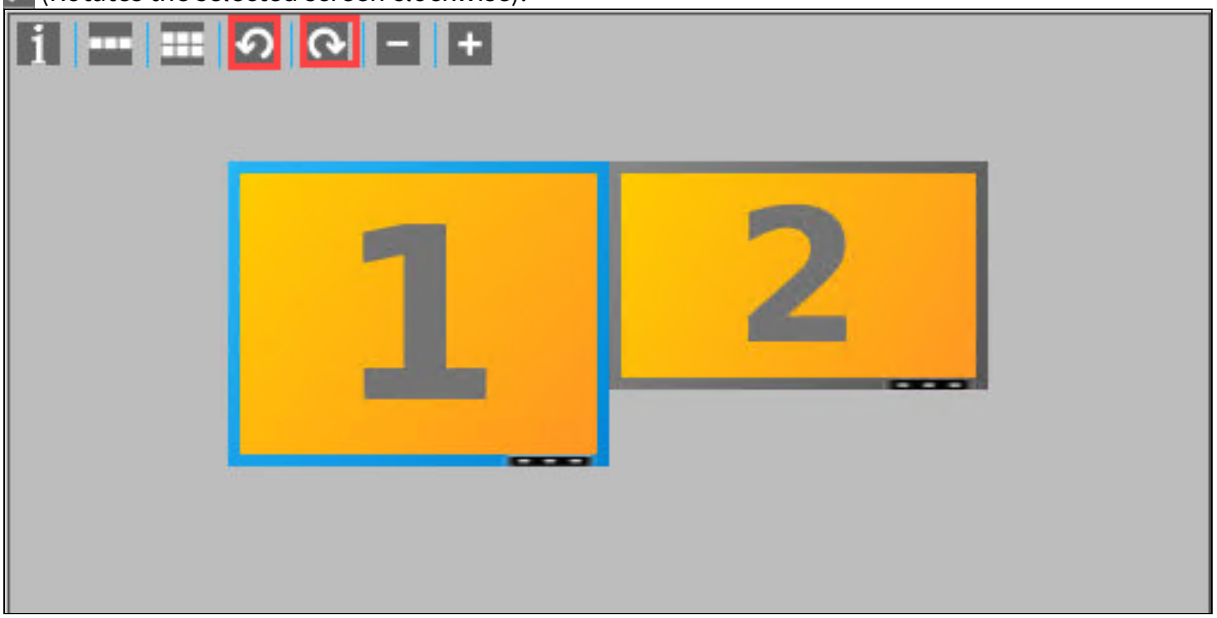
Additional Settings

A number of useful tips are provided below:

- Rotating a Screen (Pivot) (see page 841)
- Setting Different Backgrounds (see page 842)
- Useful Window Settings (see page 843)

Rotating a Screen (Pivot)

1. Click on a monitor field.
2. Select **(Rotates the selected screen counterclockwise)** or (Rotates the selected screen clockwise).



Two screens with autodetected resolutions are automatically aligned to the top.

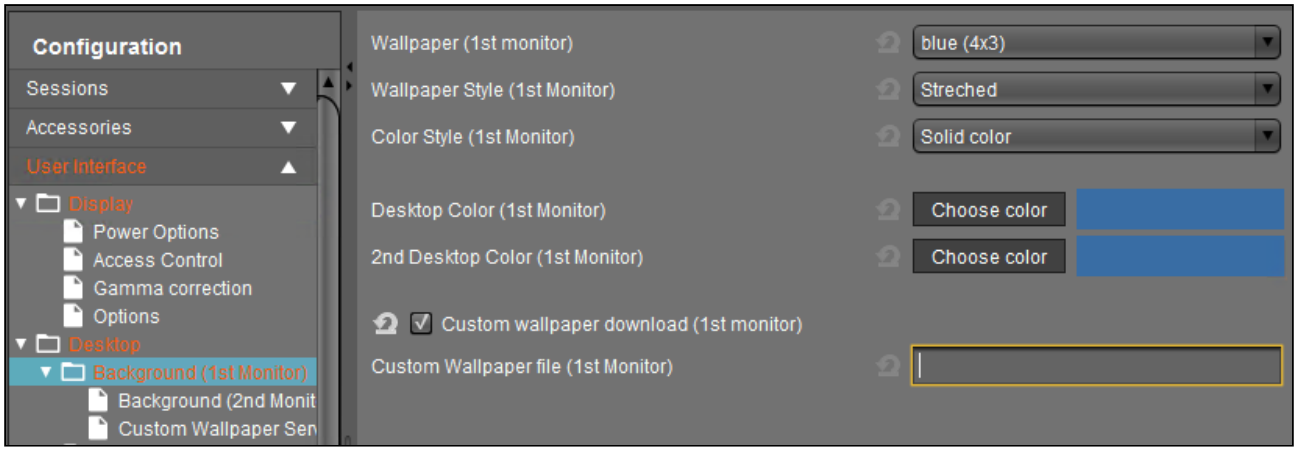
->Alignment: If you enter the correct resolution, you can see the real size of the screens and you will be able to align them the way you want.

The individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap.

Setting Different Backgrounds

You can easily set different backgrounds for your screens.

->Click **User Interface > Desktop > Background** in the structure tree of the setup.
There is a configuration page for each screen.



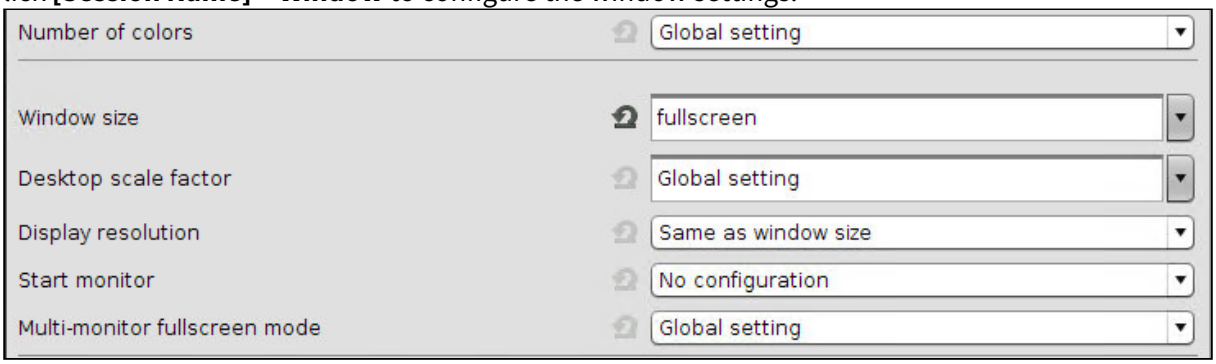
->Select the wallpaper and define the style.

> You may also upload your own **Custom Wallpaper**, e.g. a background with your corporate design. See Creating Your Own Wallpaper (see page 943).

Useful Window Settings

Setting the Start Monitor or Full-screen Mode:

1. Click the name of your session under **Sessions** in the IGEL Setup, e.g. **RDP > RDP Sessions**.
2. lick **[Session Name] > Window** to configure the window settings.



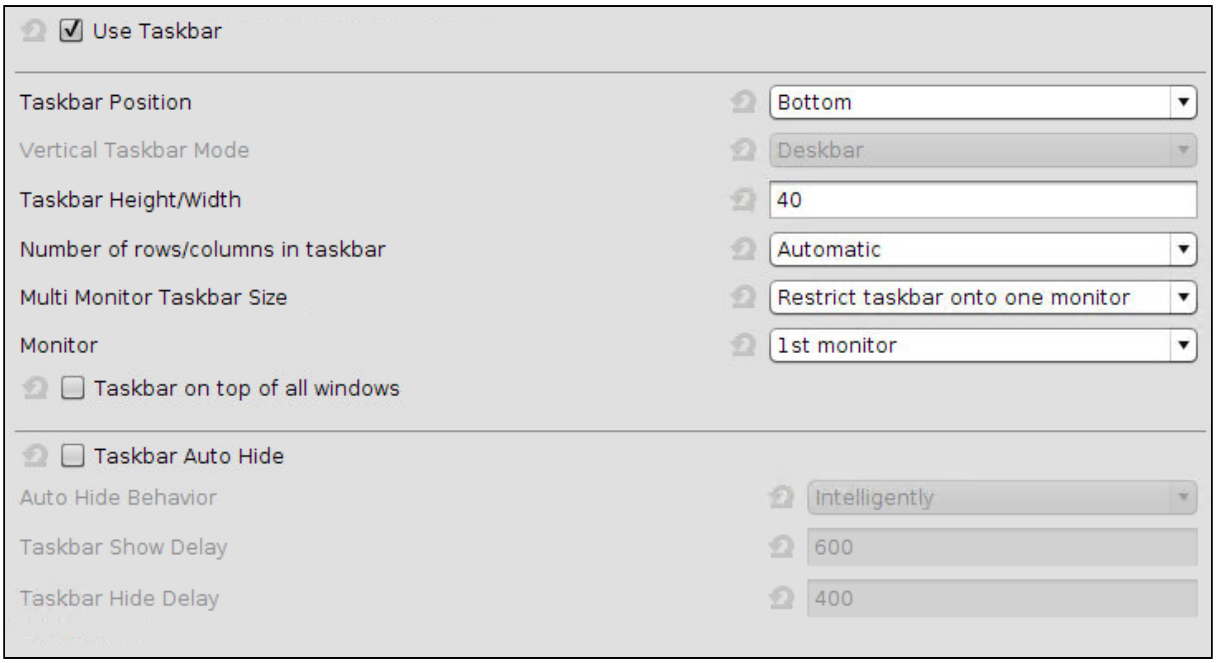
For the function "**2nd monitor** as **Start monitor**" the **Window size** has to be set to **full-screen**.

Setting the Multimonitor Full-screen Mode

1. Click **Window** in the global folder of your session, e.g. **RDP > RDP Global > Window**.
2. Configure the window settings.

Defining the Taskbar

1. Click **User Interface > Desktop > Taskbar**.
2. Define the **Taskbar** settings.

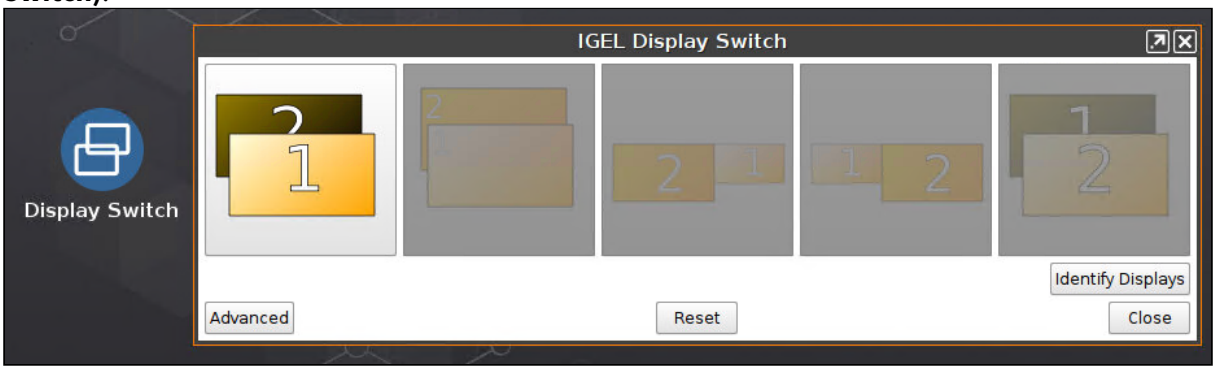


If you want to expand the taskbar onto all monitors, you have to ensure that the screens are aligned to the bottom. Otherwise, you will see only half of the taskbar on one monitor.

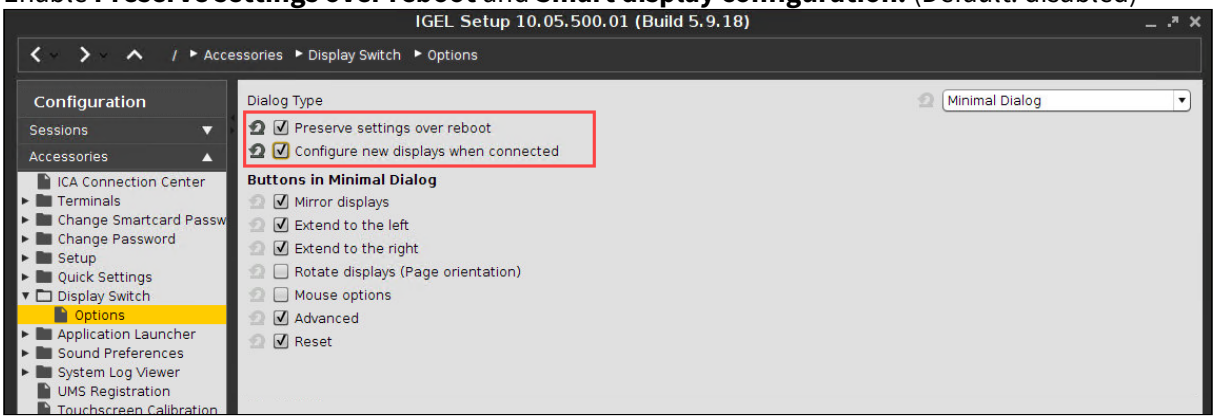
Auto Switch Monitor Configuration for Laptops

This ist one example of how to configure auto switch monitor for Laptops.

1. Connect the device and close/open lid.
2. Open the **Display Switch** utility (which has already been activated under **Accessories > Display Switch)**.



3. In the advanced mode, you can drag & drop the displays for your intended configuration.
   The display will snap adjacent to others.
4. If a display should not be used, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
5. To show the same content on multiple displays, one display should be dragged onto an other active screen.
   The interface will show **Mirrors**. The mirroring monitor will be displayed on the lower right.
6. Press **Apply** to save the setting.
7. Press **Yes** on the **Keep configuration** dialog so that the current settings will be saved to persistent storage and associated with the profile.
   You can configure advanced functionality (e. g. panning, scaling and resolutions) in drop-down boxes (hidden in a drawer on the right side)
   - Klick the **>** button on the right edge.
8. Go in IGEL Setup under **Accessories > Display Switch > Options.**
9. Enable **Preserve settings over reboot** and **Smart display configuration.** (Default: disabled)



10. The IGEL Display Switch utility is now used for NVIDIA graphic devices as well.

Configuration of the display setting for Notebook lid handling

You can configure the lid handling of a notebook so that the notebook goes into standby mode by closing the lid, regardless of whether the notebook is plugged in or not.

Settings of the Standby Mode

If you want your notebook to go into standby mode by closing the lid, while your notebook is plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > ac**.
2. Set **Lid close action while plugged in** to **Suspend**.(Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting.

If you want your notebook to go into standby mode by closing the lid, while your notebook isn't plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > battery**.
2. Set **Lid close action while not plugged in** to **Suspend**.(Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting.

If you want that the notebook **turn off display** after closing the lid, it makes sense to set the following setting to switch off the notebook internally:

1. Go under **IGEL Setup** to **System > Registry > sessions > user_display0 > options > lid_events.**
2. Enable **React on lid open and close event.**
3. Click **Apply** or **Ok** to save the setting.

Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar

Running a session in full-screen mode gives you the advantage that the complete real estate of your monitor is at the disposal of that session. However, you might still want to eject a hotplug drive, or to minimize or end the current session. The solution provided by IGEL Linux is called **in-session control bar**.

Activating the in-session control bar:

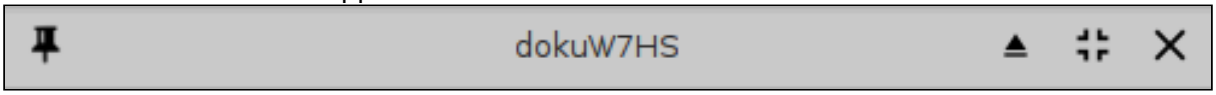
1. Open the Setup and go to **User Interface > Desktop > In-Session Control Bar**.
2. Activate **Use in-session control bar in all supported sessions** if you want to have an in-session control bar in all session types for which it is supported. If you want to have an in-session control bar only in sessions of certain types, activate the appropriate options, e.g. **Control bar for RDP sessions**.

3. In the **Start Monitor** choice, select the display on which you want the in-session control bar to appear. If unsure, leave it at **Automatic**.

4. Click **Apply** or **Ok**.

Using the in-session control bar:

1. Move the mouse to the upper edge of the desktop.
   The in-session control bar appears.



2. To perform the desired action, click the appropriate icon:
    - To eject a USB device, click .
    - To minimize the session view, click .
    - To end the session, click .
    - To make the in-session control bar visible permanently, click .

Display Configuration for Shared Workplace (SWP)

As of IGEL Universal Desktop Linux version 4.14.100 and version 5.06.100, Shared Workplace allows user specific screen resolutions and configurations. Resolution, layout, refresh rate, rotation, number of screens, monitor connectors (DVI, VGA, ...) can be set per user, but color depth cannot.

There are technical limitations to user-specific settings: For VIA graphics drivers/hardware, the maximum desktop size is set in the `Screen` section of the X `confi` guration file. The name and location of the X configuration file depends on the firmware version:

- IGEL Linux *version 10*: `/config/Xserver/xorg.conf-0`
- IGEL Linux *version 5*: `/config/Xserver/xorg.conf-0` or `/etc/X11/xorg.conf` (this is a symbolic link that points to `/config/Xserver/xorg.conf-0`)

  In the `Screen` section of the above-mentioned configuration file, you can find a line such as `Virtual 1920 1200` . The size defined here cannot be changed dynamically; it is a hard limit for the overall desktop size.

Best practice

It is recommended to set the initial desktop configuration to the maximum number of screens and the resolutions to A `utodetect` . This way the user specific resolutions will not be restricted.

Debugging

If the total framebuffer size of the user specific resolutions exceeds the limits of the `Virtual [width] [height]` setting from `/config/Xserver/xorg.conf-0` (or `/etc/X11/xorg.conf`), the user specific resolutions cannot be activated and the screen configurations are not changed dynamically.

There is no warning dialog or anything else to alert the user to this restriction. But you can find related log messages via `journalctl` or in `/var/log/messages` :

```
XRANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XRANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

Using an External NVIDIA Graphics Card

Goal

You want to use an external NVIDIA graphics card for your endpoint device and need to connect it with all graphics outputs.

Environment

- IGEL OS 11.04.100 or higher

Solution

1. In the IGEL Setup, go to **System > Registry**.
2. Set the registry key **x.drivers.preferred_driver** to `nvidia`.
3. Enable the registry key **x.drivers.nvidia.use_modeset**. This registry key should be used if you want to use PRIME.
4. Restart the device manually, e.g. by pressing the power switch.
5. Under **User Interface > Display**, orient and position your monitors.
6. For fine-tuning, use the **Display Switch** function, which can be enabled under **Accessories > Display Switch**. See Using Display Switch (see page 1737) and Display Switch 1 (see page 1730).

Then the onboard graphics ports as well as the ports of the NVIDIA card can be used, which is the recommended mode since everything is rendered on the NVIDIA GPU.

Customizing

- Custom Partition Tutorial (see page 852)
- Using a Custom PKCS#11 Library (see page 922)
- Adding an Icon for Browsing Removable Storage (see page 924)
- Adding an Icon for the Image Viewer (see page 926)
- Creating a Timed Command (Cron Replacement) (see page 928)
- Customizing IGEL OS Desktop (see page 930)
- How to Change the Font Color of the Desktop Icons (see page 954)
- How to Set Up a Countdown to Prevent an Undesired Screen Lock In IGEL OS (see page 957)
- Keyboard Shortcuts for Managing Windows (see page 964)
- Make Frequent User Actions Easier by Defining Hotkeys (see page 965)
- Shutdown/Suspend Devices Automatically at the End of a Session (see page 967)
- Suspend to RAM - Wake Up by USB Mouse (see page 968)
- Taking Screenshots on IGEL Linux (see page 969)
- Setting the Device's System Time (see page 971)
- Updating Timezone Information (Daylight Saving Time, DST) (see page 972)
- Adding or Changing a MIME Type Handler (see page 975)
- Regional Settings in Sessions (see page 979)

Custom Partition Tutorial

The Custom Partition mechanism solves the task of supplying additional software or other files to IGEL OS while still being able to update the system in the regular way.

This tutorial describes creating content for a Custom Partition for IGEL OS 11.01.100 or newer. In the examples, IGEL OS 11.03.500 is used. You may also find it useful for updating existing Custom Partitions in order to make them work on IGEL OS 11.01.100 or newer, as some details have changed.

The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

If you want to build a Custom Partition and give it to third parties, make sure you have redistribution permission for the software. This is usually the case for Open Source / Free Software, but not for proprietary software. Read the license agreements and respect them.

This tutorial contains the following sections:

- A First Simple Custom Partition (see page 853)
- Packaging the Custom Partition (see page 864)
- A Real-World CP: Chromium (see page 884)
- Zoom as a Custom Partition (see page 899)

A First Simple Custom Partition

As a first step, this tutorial will guide you through creating a simple Custom Partition. It will open a message window greeting the user, which can be run by clicking a desktop icon. You will learn about some basic mechanisms of Custom Partitions in this section.

Read all the following chapters in the order given and follow the instructions.

1. Development Environment (see page 854)
2. Activating the Custom Partition Functionality (see page 855)
3. "Hello World" Program (see page 856)
4. Creating the Custom Application (see page 859)
5. Using a Partition Parameter (see page 862)

Development Environment

For this first simple Custom Partition, you only need `root` access to a device with IGEL OS version 11.01.100 or higher.

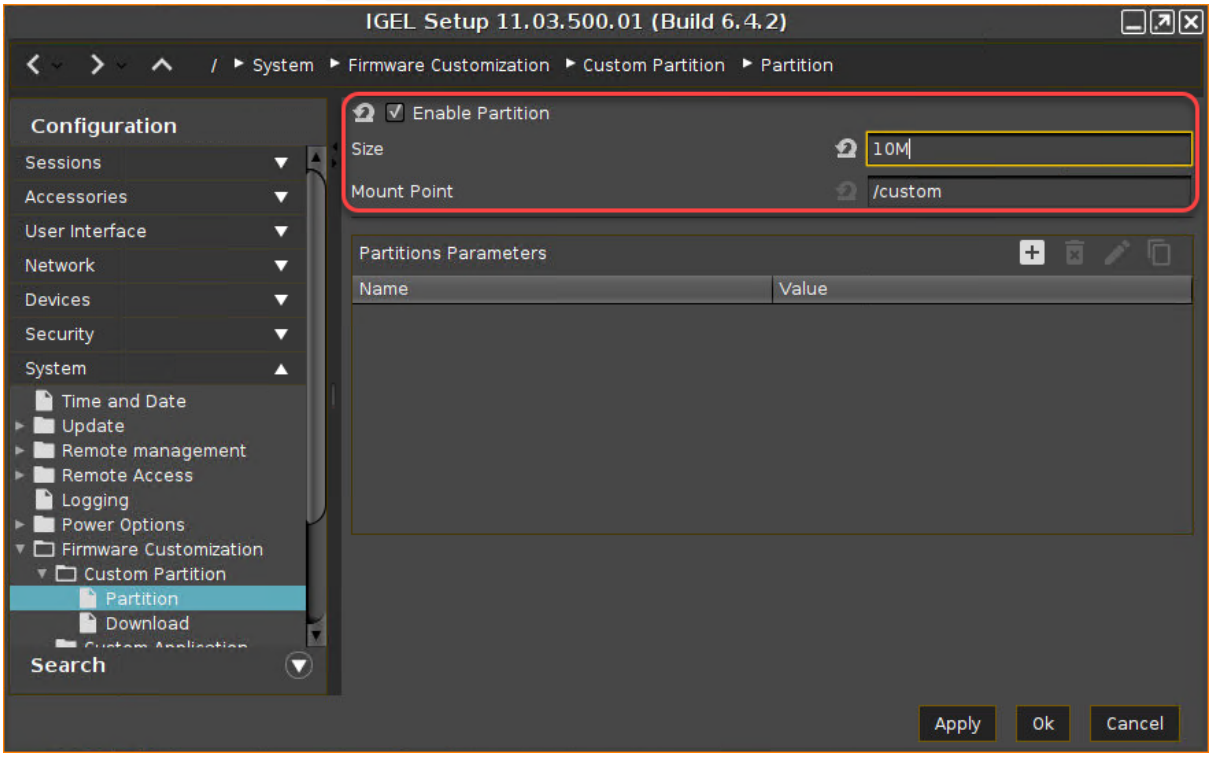
Next Step

>> Activating the Custom Partition Functionality (see page 855)

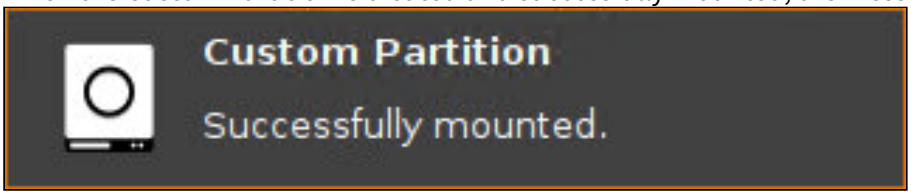
Activating the Custom Partition Functionality

First, you must activate the Custom Partition functionality. It is deactivated by default.

1. Open the Setup and go to **System > Firmware Customization > Custom Partition > Partition**.
2. Check **Enable Partition**.
3. Set the **Size** to "10M" Megabyte).
4. Leave the **Mount Point** at `/custom`



5. Click **Apply**.
   The Custom Partition is created on the device's mass storage, which is indicated by a message.
   When the Custom Partition is created and successfully mounted, the message reads:



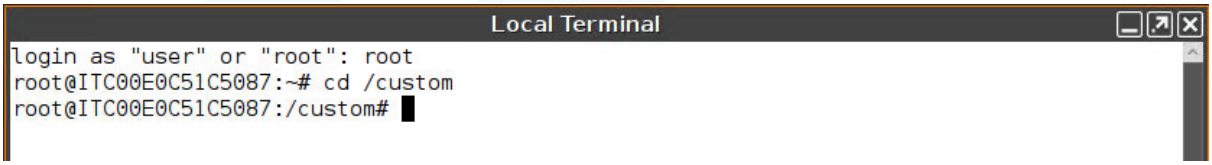
Next Step

>> "Hello World" Program (see page 856)

"Hello World" Program

Your first Custom Partition will contain a simple shell script that displays the message "Hello, world!" with the help of the `gtkmessage` utility.

1. Open the local terminal on your device and log in as `root`. If the local terminal has not been configured yet, see Local Terminals (see page 1708).
2. Change into the `/custom` directory: `cd /custom`



3. Make a `hello` directory for your Custom Partition contents: `mkdir hello`

```
root@ITC00E0C51C5087:/custom# mkdir hello
```

4. Change into the `hello` directory: `cd hello/`

```
root@ITC00E0C51C5087:/custom# cd hello/
```

5. Open a new plaintext file using the GNU nano editor: `nano hello.sh`

```
root@ITC00E0C51C5087:/custom/hello# nano hello.sh
```

> The colors used by default for syntax highlighting in nano may be inconvenient for reading. You can change the colors with the following command: `sed -i "s#color cyan#color blue#; s#color brightyellow#color red#" /usr/share/nano/sh.nanorc`
> Also, you can use the vi editor as an alternative; the commands for exiting and saving a file will be different then.

6. Put this content into the file:

```
#!/bin/bash
```

gtkmessage -m "Hello, World!" -t "Hello" -o "Close"

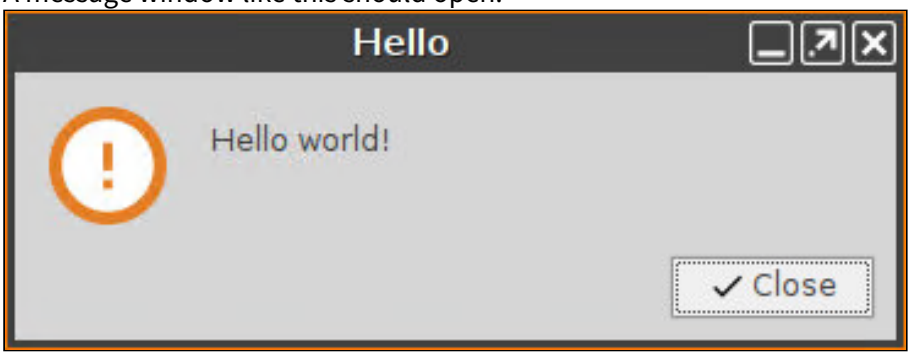
7. Save the file by pressing [Ctrl]+[o], [Return].
8. Exit the GNU nano editor by pressing [Ctrl]+[x].
9. Make the file executable: `chmod a+x hello.sh`

   ```
   root@ITC00E0C51C5087:/custom/hello# chmod a+x hello.sh
   ```

10. Run the shell script from the command line to test it: `./hello.sh`

    ```
    root@ITC00E0C51C5087:/custom/hello# ./hello.sh
    ```

    A message window like this should open:



You can close it with the **Close** button.

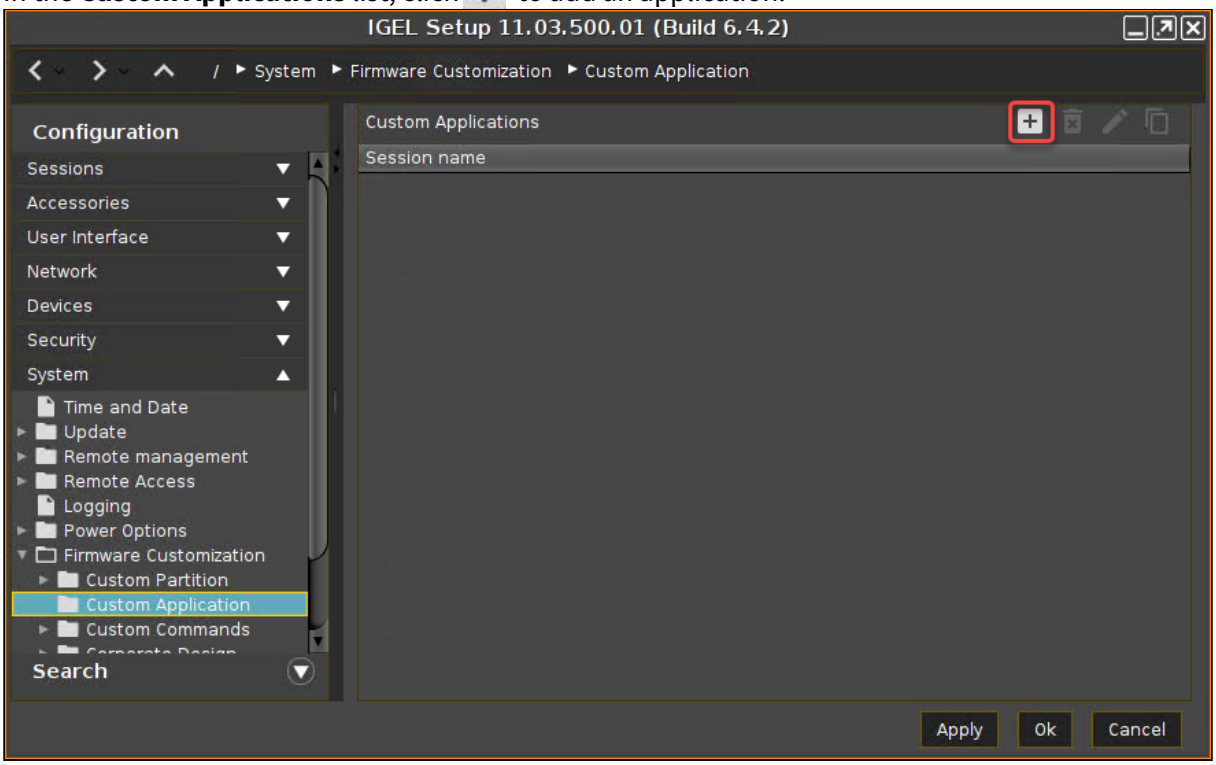
Next Step

>> Creating the Custom Application (see page 859)

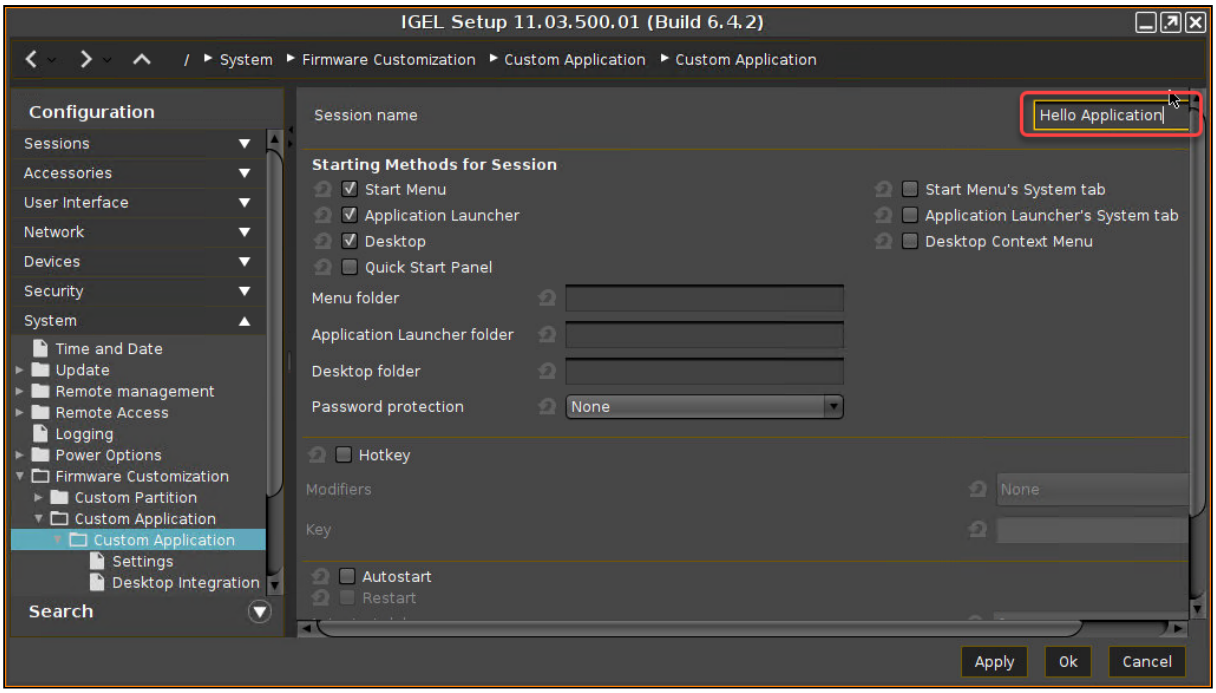
Creating the Custom Application

In the previous step, you have created a little application and executed it from the command line. Now make it more convenient for end-users: Create a custom application and place an icon on the desktop that users can click.

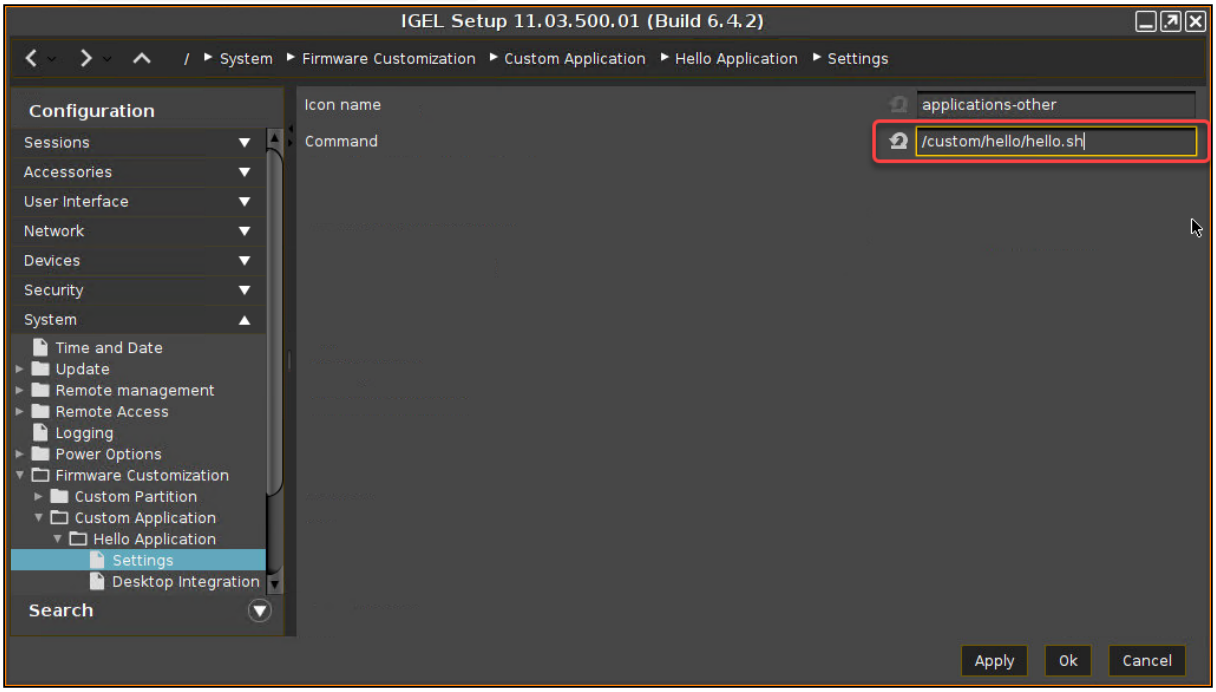
1. In the Setup, go to **System > Firmware Customization > Custom Application**.
2. In the **Custom Applications** list, click + to add an application.



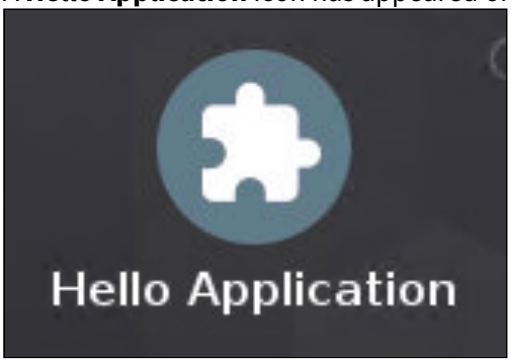
   The **Desktop Integration** page opens.
3. Enter `Hello Application` as the **Session name**.



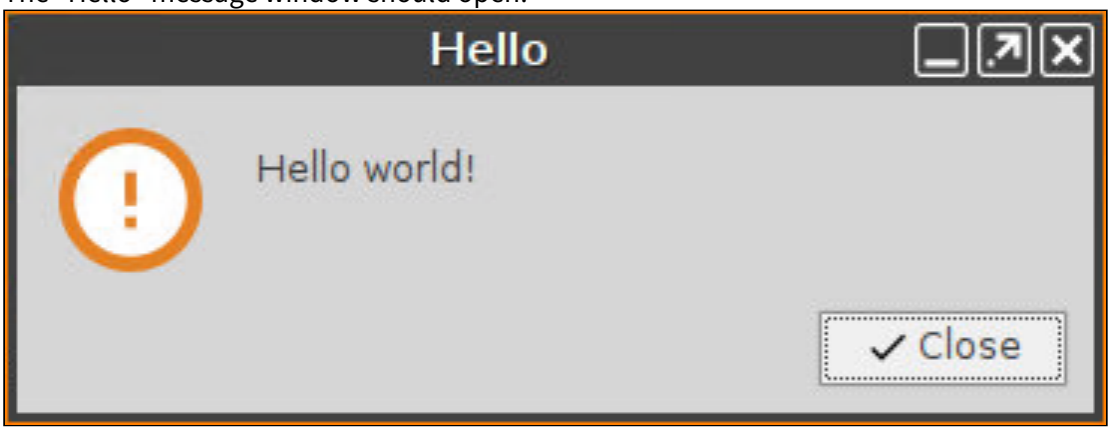
4. Click **Apply**.
5. Go to **Settings**.
6. Enter `/custom/hello/hello.sh` as the **Command**.



7. Click **OK**.
   A **Hello Application** icon has appeared on the desktop.



8. Double-click the icon.
   The "Hello" message window should open.



Next Step

>> Using a Partition Parameter (see page 862)

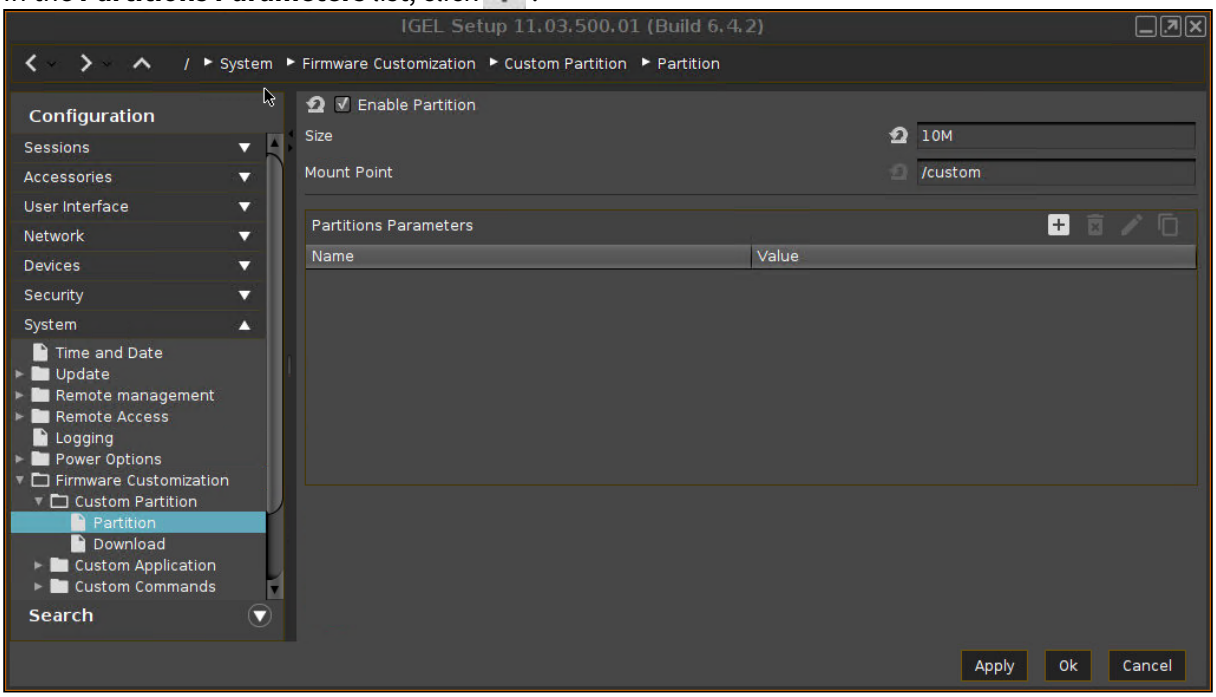
Using a Partition Parameter

When you roll out the same Custom Partition contents to many devices, you may still want the application to use different data or options on some of the devices. Partition parameters allow you to do this.

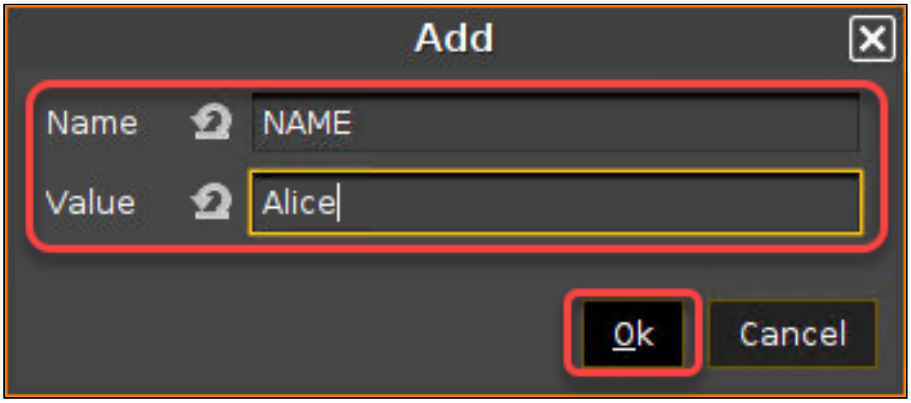
This is how you add a partition parameter to our "Hello World" program.

Setting a Partition Parameter in the Setup

1. Go to **System > Firmware Customization > Custom Partition > Partition**.
2. In the **Partitions Parameters** list, click + .



3. In the dialog that opens, enter `NAME` as the **Name** and `Alice` as the **Value**. Click **OK**.



4. Click **Apply**.

Getting the Value of a Partition Parameter

This is the command line for getting or setting a Partition Parameter's value:

```
customparam [get|set] PARAMETER_NAME [PARAMETER_VALUE]
```

1. Change the `hello.sh` script to use this command to get the parameter value:
   `#!/bin/bash`
   gtkmessage -m "Hello $(customparam get NAME)!" -t "Hello" -o "Close"
2. Click the **Hello Application** desktop icon.
   You should see the following:

Packaging the Custom Partition

In the previous section, you developed Custom Partition contents locally on a device. Now, package it in order to deploy it to many devices via the Universal Management Suite (UMS).

Read all the following chapters in the order given and follow the instructions.

1. Development Environment (see page 865)
2. Compressing the Custom Partition Contents (see page 866)
3. Writing the *.inf Metadata File (see page 867)
4. Uploading the Files to the UMS 1 (see page 868)
5. Creating a Profile for the Custom Partition (see page 875)
6. Assigning the Profile 1 (see page 881)

When you have built this Custom Partition successfully, you can continue with a real-world partition. The following Custom Partitions are described in our tutorial:

- Chromium
- Zoom (see page 899)

Development Environment

For this section, you need:

- a system with IGEL OS 11.01.100 or newer
- Universal Management Suite (UMS) 6.01.100 or newer

Next Step

>> Compressing the Custom Partition Contents (see page 866)

Compressing the Custom Partition Contents

The contents of a Custom Partition are packaged as a compressed `tar` file. Create it on the Linux command line, e.g. on a device that is running IGEL OS:

1. In the local terminal, become `root` and change to the `/custom` directory: `cd /custom`
   ```
   root@ITC00E0C51C5087:~# cd /custom
   ```
2. Compress the contents of the `hello/` directory into an archive file named `hello.tar.bz2` :
   `tar cjvf hello.tar.bz2 hello/`
   ```
   root@ITC00E0C51C5087:/custom# tar cjvf hello.tar.bz2 hello/
   ```

   The result is a `hello.tar.bz2` file, sitting side-by-side with the `hello/` directory. You will upload it to UMS later.

Next Step

>> Writing the *.inf Metadata File 2 (see page 867)

Writing the *.inf Metadata File

In addition to the compressed archive that you created in the previous step, a plain text file with essential information for the endpoint device is necessary. In this, step you will create the `hello.inf` file.

---

1. Change to the directory that contains the compressed contents of our Custom Partition (`hello.tar.bz2`): `cd /custom/`
   ```
   root@ITC00E0C51C5087:/custom# cd /custom/
   ```
2. Create a new file named `hello.inf` and put the following into it:
   ```
   [INFO]
   [PART]
   file="hello.tar.bz2"
   version="1.0_igel1"
   size="10M"
   name="hello"
   minfw="11.01.100"
   ```
   The individual entries and their meaning are:
   `[INFO]` Mandatory string
   `[PART]` Mandatory string
   `file` The filename of the `*.tar.bz2` archive
   `version` The version of the contents, consisting of the vendor version (let's say this is "hello 1.0") and the IGEL package version (the first package we produced of the software), joined with an underscore.
   `size` Size of the decompressed contents
   `name` Name of this content, used for naming the subdirectory within the custom partition and for keeping track of installed contents
   `minfw` Minimum firmware version required for these contents
3. Save the file.

Next Step

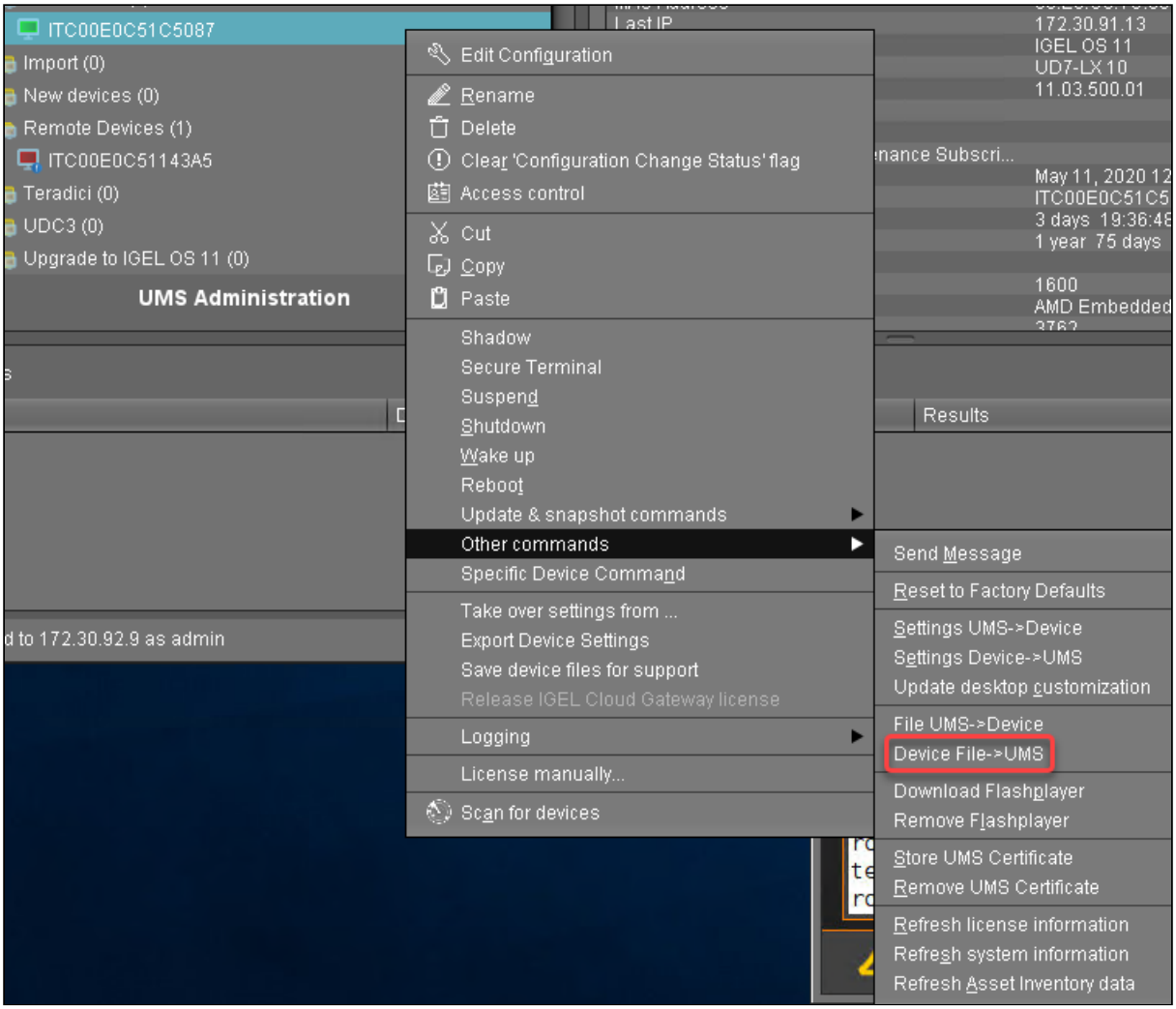
>> Uploading the Files to the UMS (see page 868)

Uploading the Files to the UMS

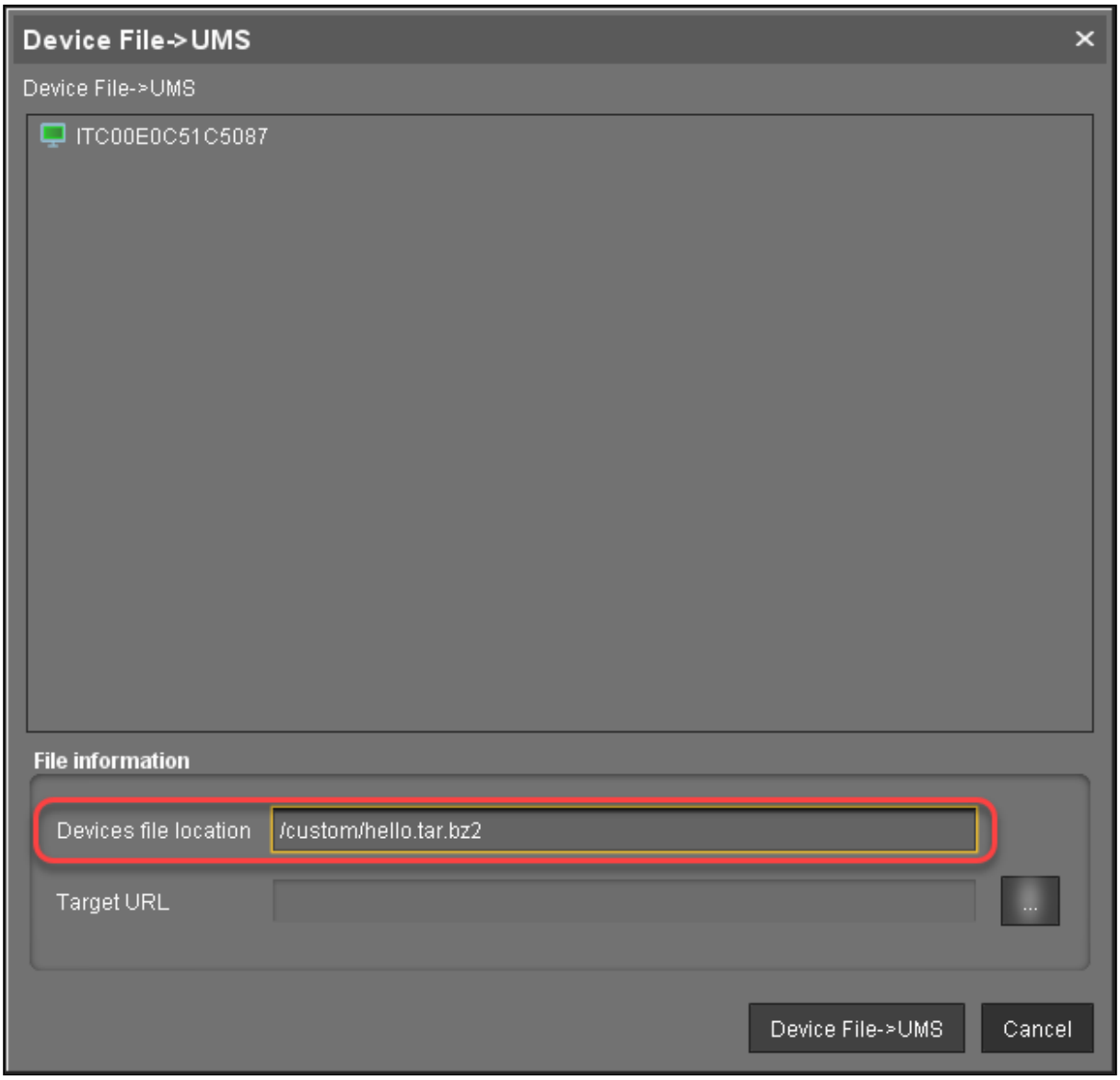
In this step, you upload the compressed `hello.tar.bz2` archive and the `hello.inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

Transferring the Files to the UMS

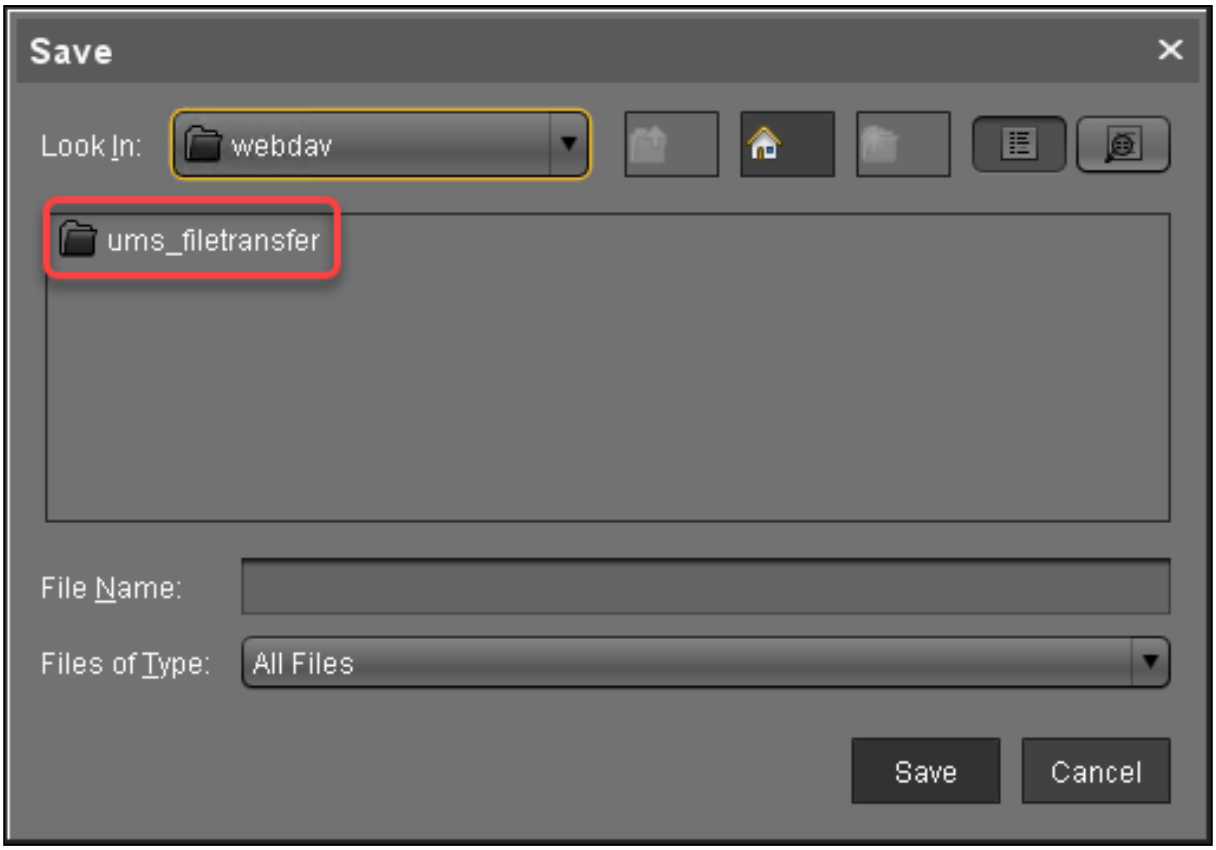
1. In the structure tree of the UMS Console, go to the device on which you have created the files and select **Other commands > Device File->UMS**.



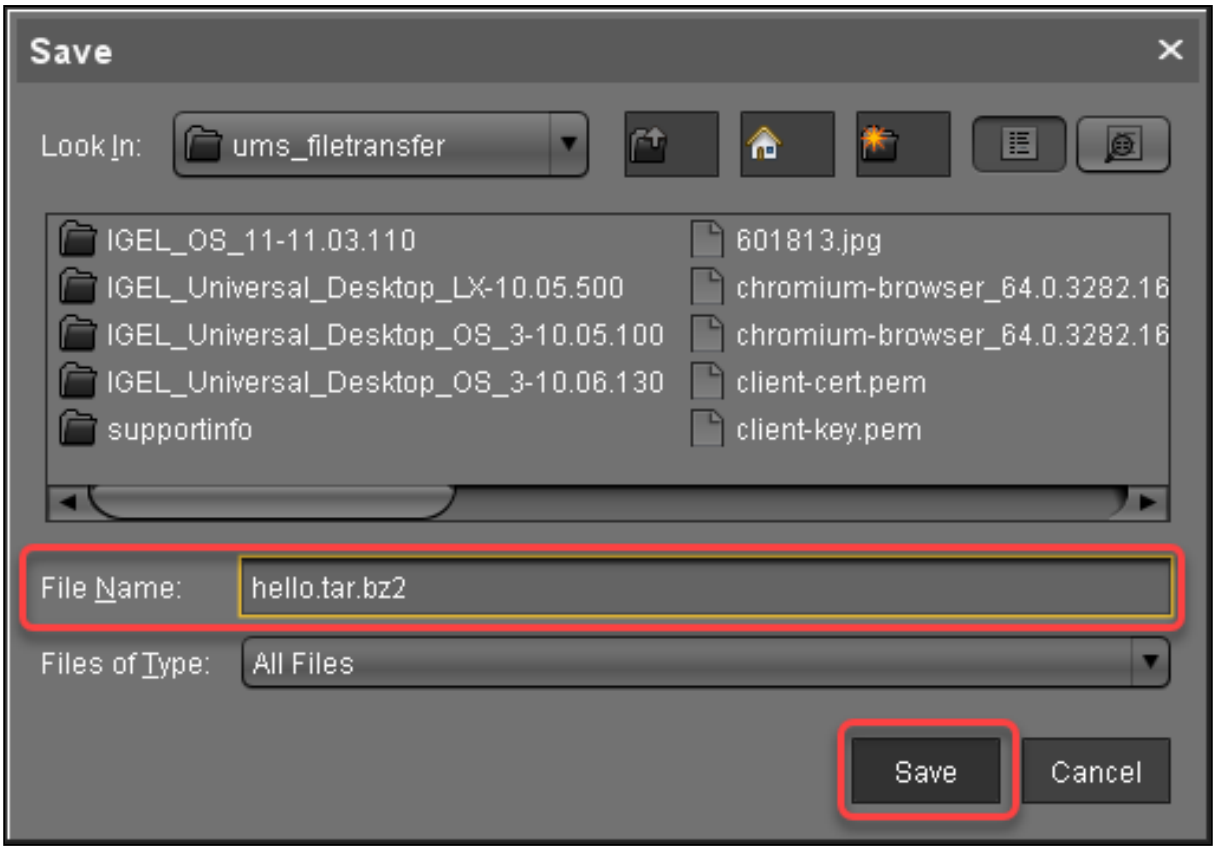
2. In the **Device File->UMS** dialog, under **Device file location**, enter the complete path and file name of the bz2 archive: "/custom/hello.tar.bz2"



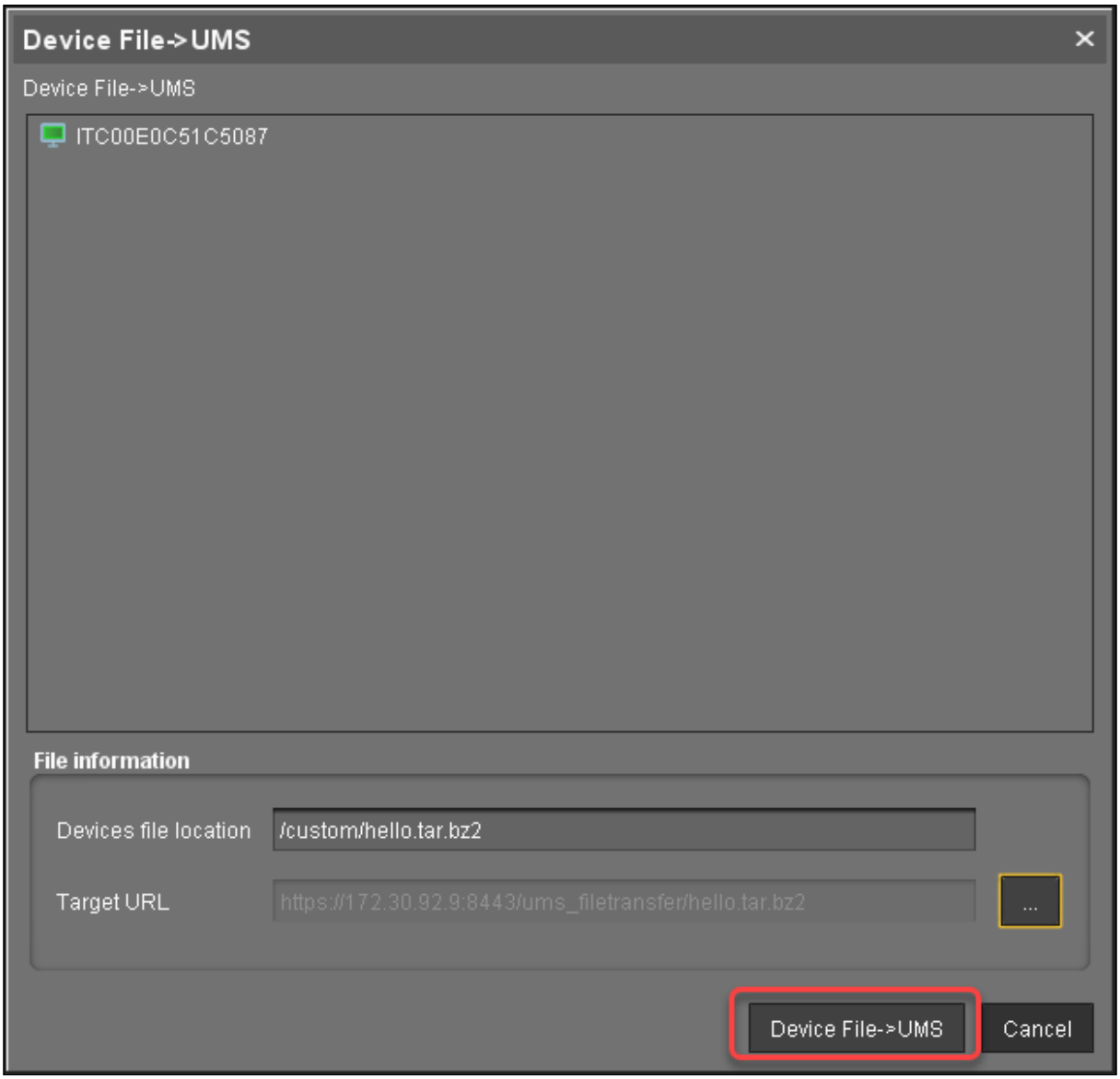
3. Click ... next to the **Target URL** to define the file path on the UMS Server.
4. In the **Save** dialog, select **ums_filetransfer** as the directory.



5. Enter "hello.tar.bz2" as the **File Name** and click **Save**.



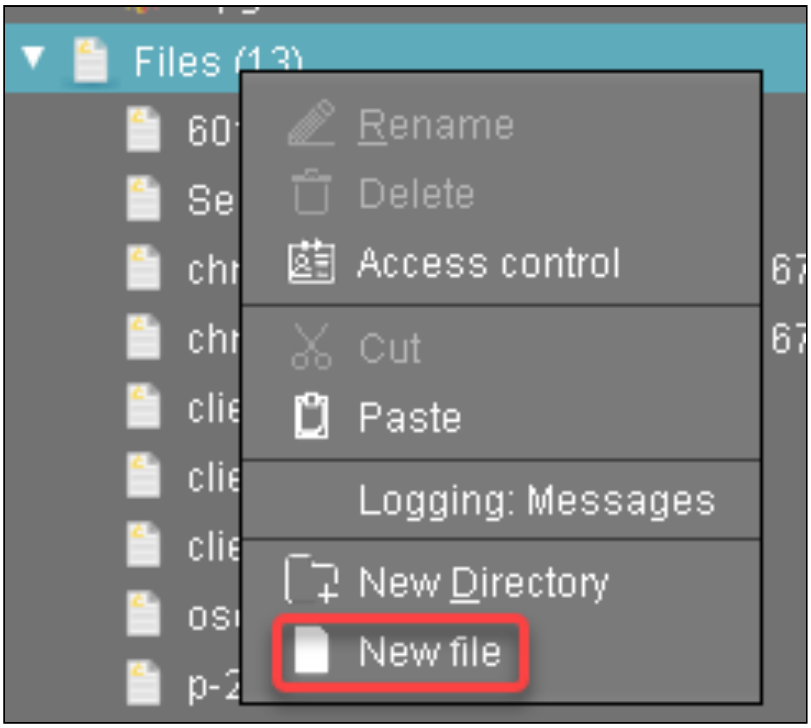
6. Back in the **Device File->UMS** dialog, click **Device File->UMS**.



7. Repeat steps 1 to 6 for the metadata file `hello.inf`.

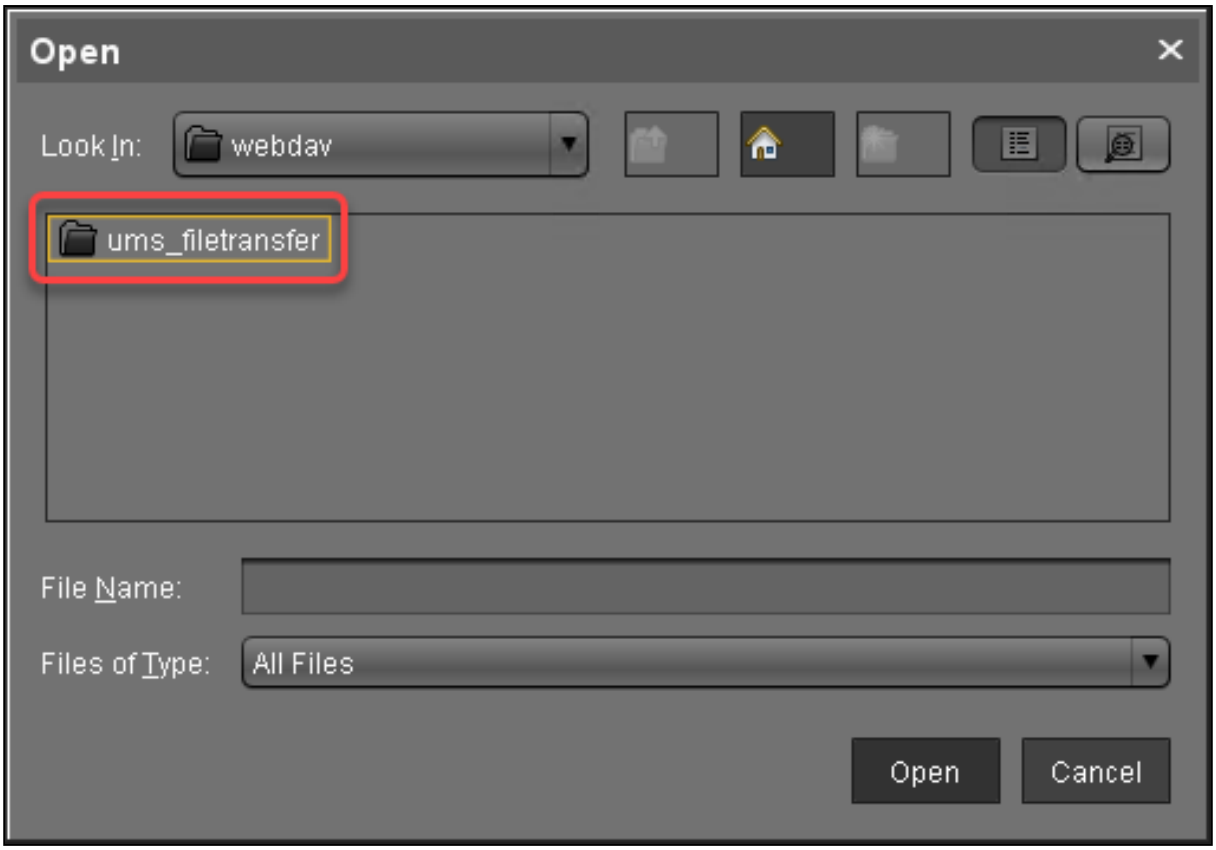
Creating File Objects

1. In the UMS Console, right-click the **Files** folder in the structure tree and select **New File** from the context menu.



The **New file** dialog opens.

2. Activate **Select from UMS server** and click ... next to this option to open the file chooser.
3. Select **ums_filetransfer**.



4. Select "hello.tar.bz2" and click **Open**.
5. Back in the **New file** dialog, click **Ok**.
6. Repeat steps 1 to 4 for the metadata file `hello.inf`.

Next Step

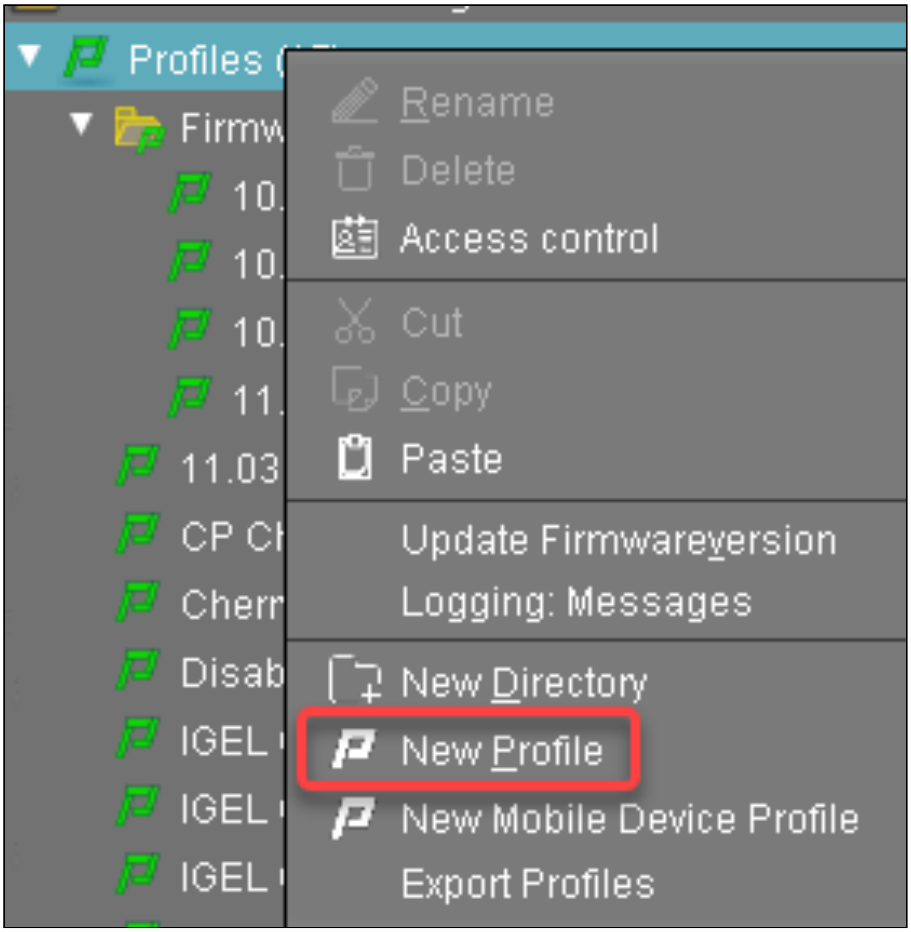
>> Creating a Profile for the Custom Partition (see page 875)

Creating a Profile for the Custom Partition

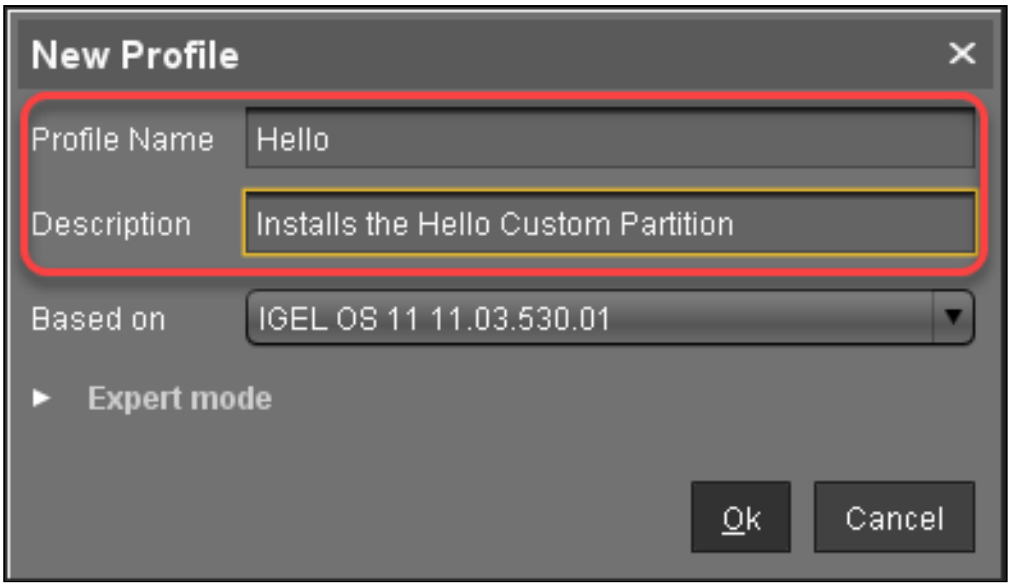
After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, we will create a profile.

Activating the Custom Partition

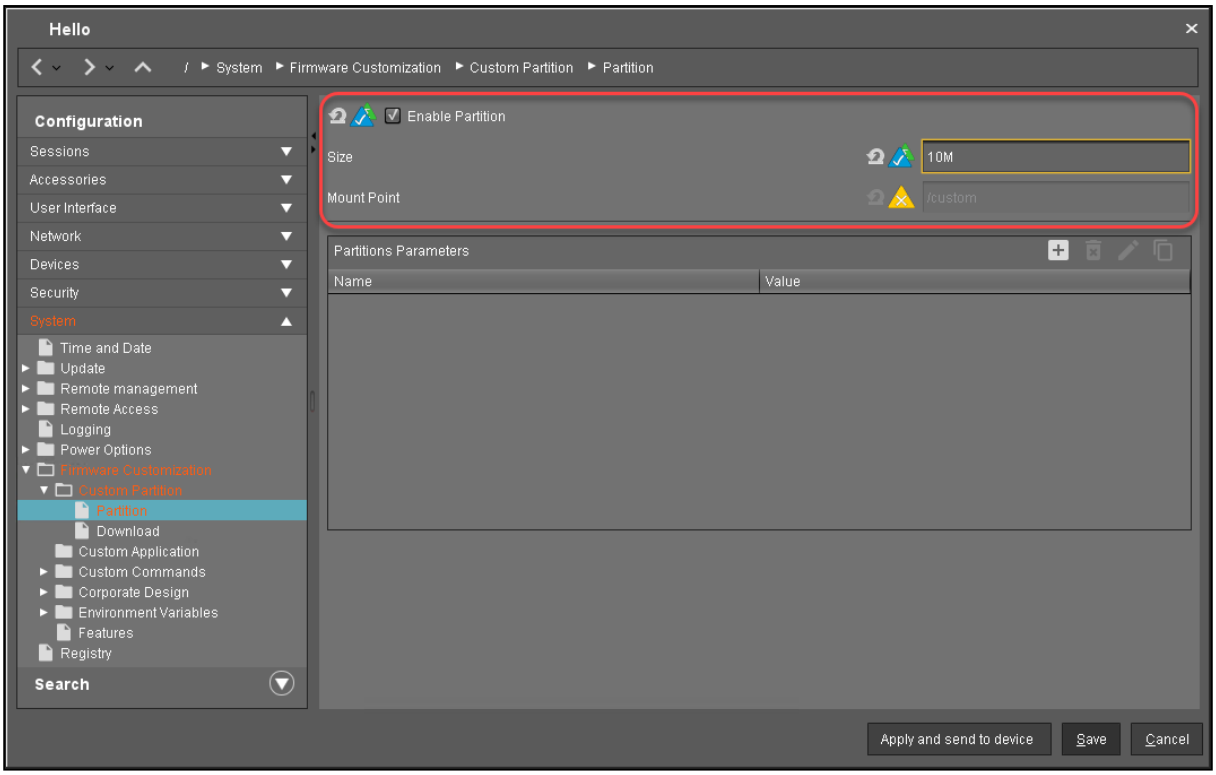
1. In the structure tree of the UMS Console, right-click the **Profiles** folder and select **New Profile** from the context menu.



2. In the **New Profile** dialog, enter "Hello" as the **Profile Name** and something like "Installs the Hello Custom Partition" as the **Description**. You can leave the remaining fields.



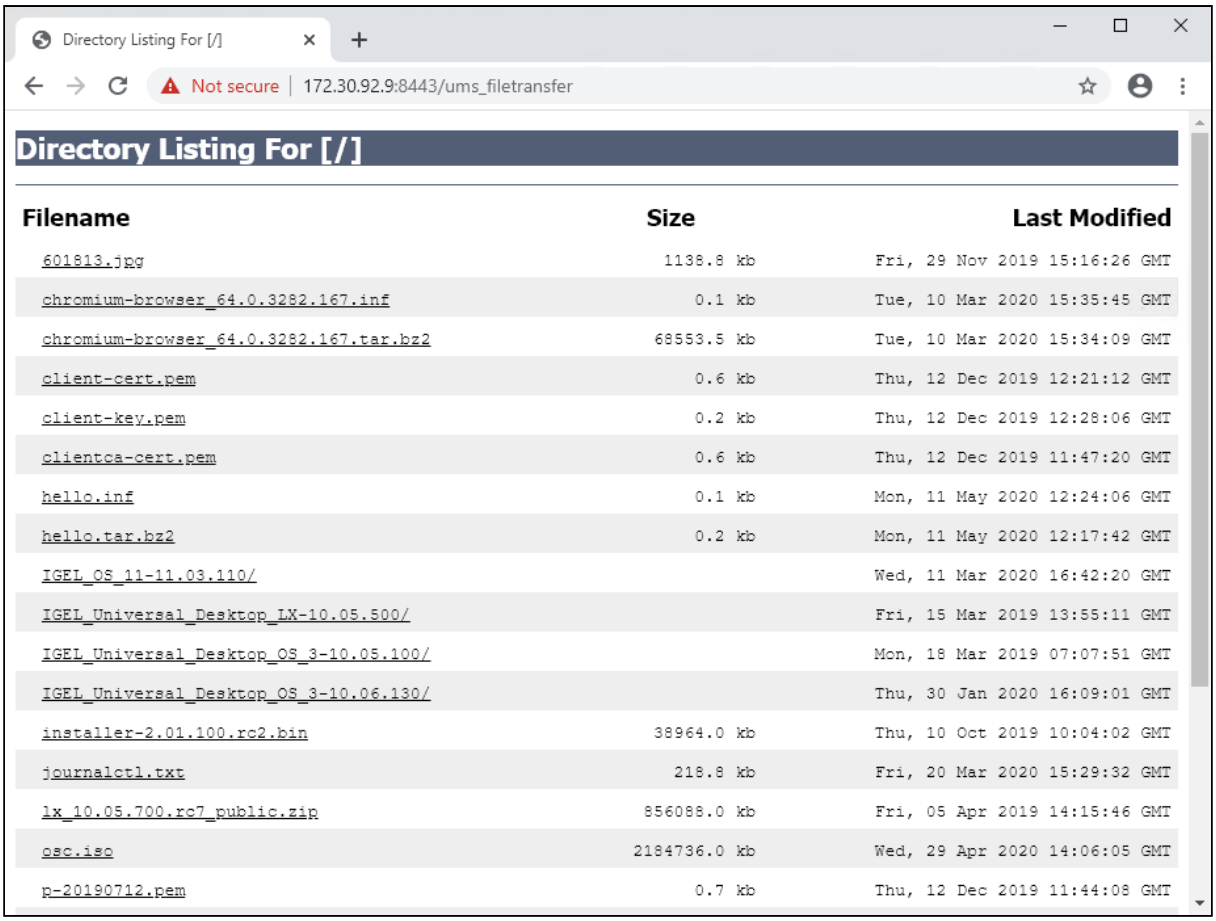
3. Click **OK**.
   The configuration dialog opens, where you will make the settings for this profile.
4. Go to **System > Firmware Customization > Custom Partition > Partition**.
5. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue.
6. Check **Enable Partition**.
7. Unlock the **Size** setting by clicking the orange triangle so that it turns blue, and enter "10M".
8. Leave the **Mount Point** at "/custom".



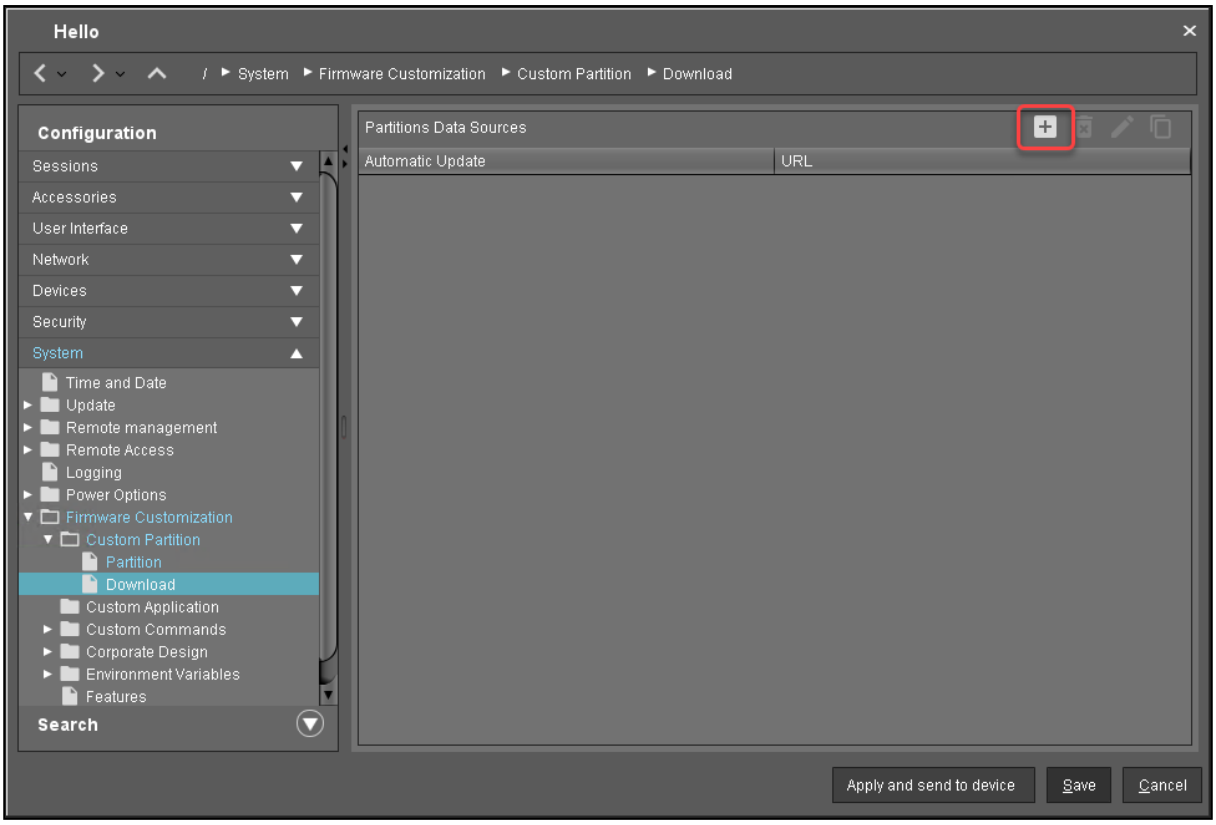
Setting the Download Source

For this step, you need to determine the HTTPS download address for the `hello.inf` file first.

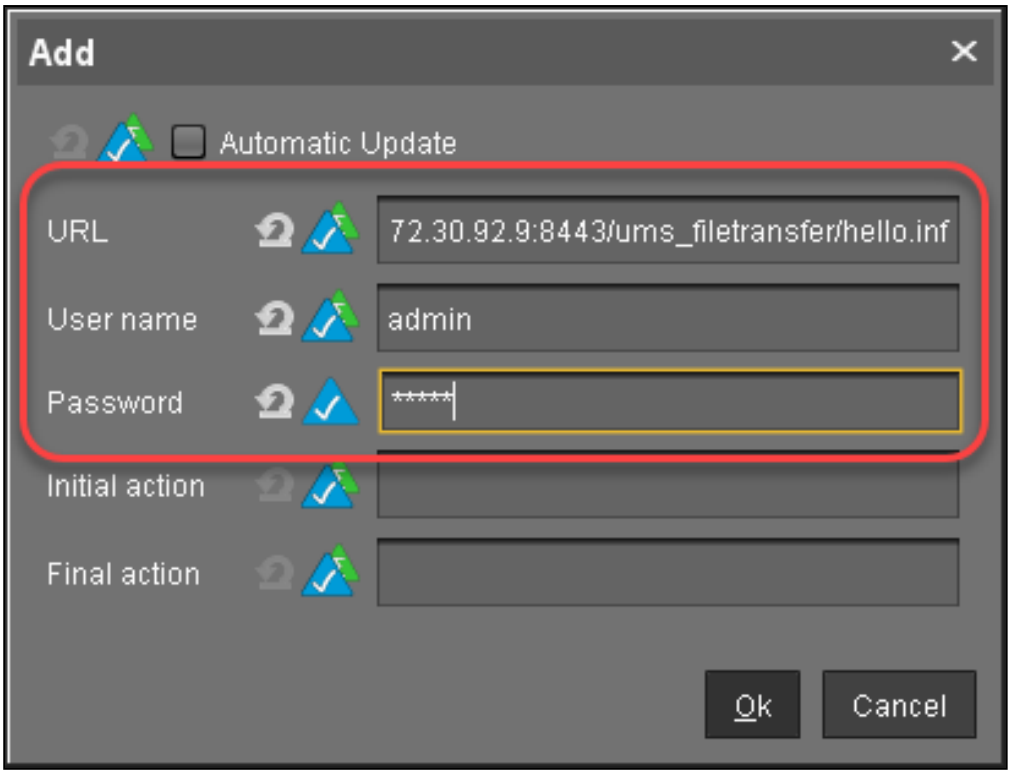
1. To find out the IP address of your UMS, go to **System > Remote Management** in the configuration dialog. You will find the IP address of the UMS Server your device is registered with.
2. Open a web browser and visit the following URL:
   `https://[IP or name of your UMS host]:8443/ums_filetransfer`
3. When prompted, authenticate with your UMS username and password.
   You will see a directory listing of the files that can be downloaded from the UMS.



4. Right-click the `hello.inf` entry and select **Copy link address** (or the like, depending on your browser).
5. In the profile's settings, go to **System > Firmware Customization > Custom Partition > Download**.
6. Next to **Partitions Data Sources**, click [+].



7. The **Add** dialog opens.
8. Paste the URL you copied from the browser into **URL**.
9. Enter the **User name** and **Password** so that the device has access to your UMS.
   You can ignore the **Initial action** and **Final action** fields for the time being



10. Click **OK**.

Creating a Custom Application

->Add a custom application to the profile by following the steps in Creating the Custom Application (see page 859).

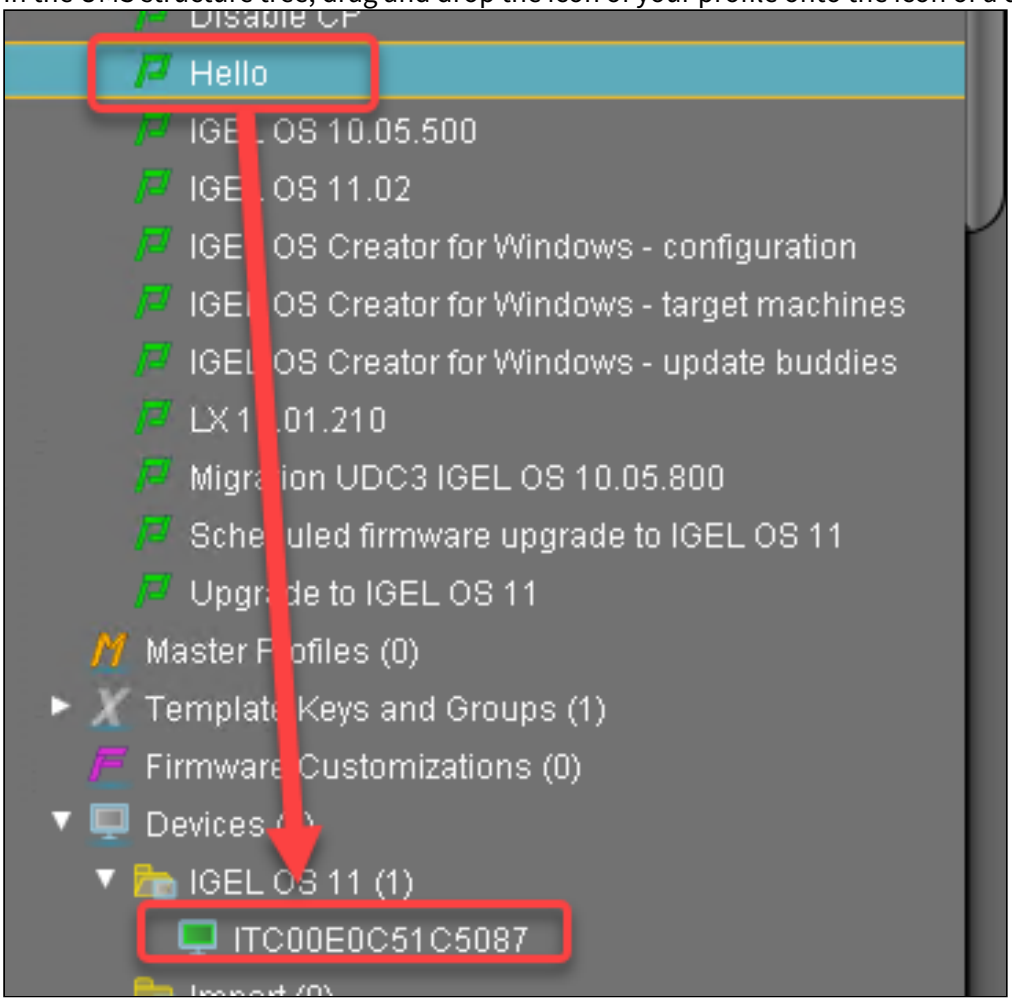
Next Step

>> Assigning the Profile (see page 881)

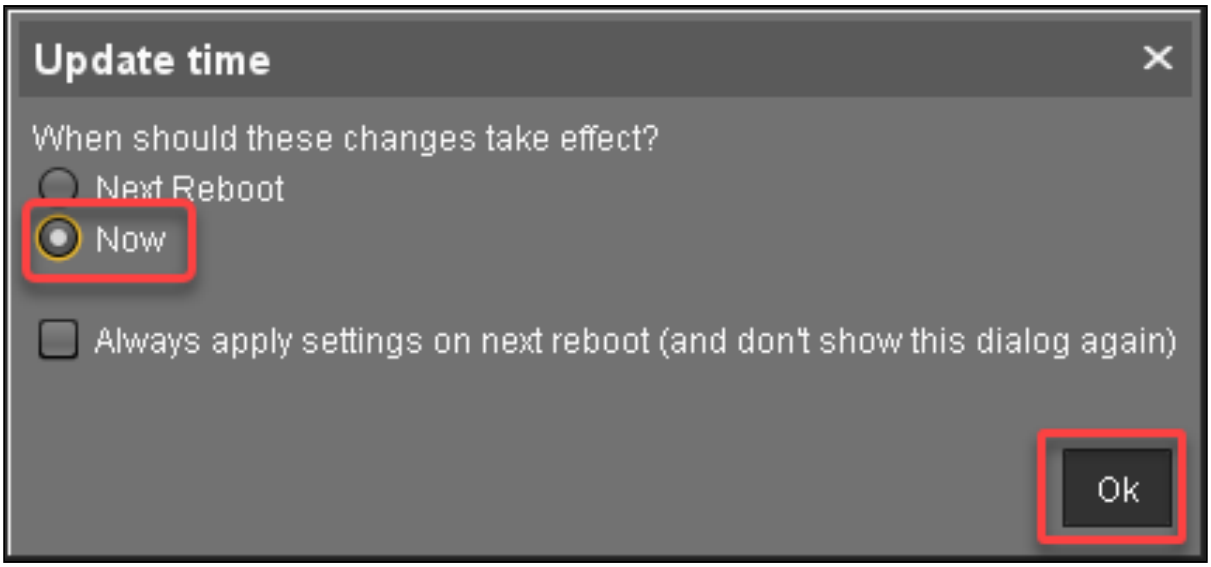
Assigning the Profile

eNow that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

1. In the UMS structure tree, drag and drop the icon of your profile onto the icon of a device.

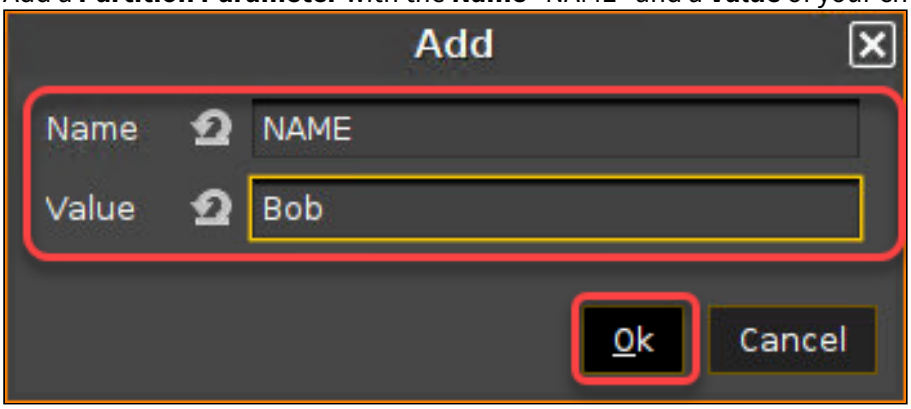


   The **Update time** dialog opens.
2. Select **Now** and click **Ok**.



The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition and uncompresses them.
The **Hello Application** icon appears on the desktop.

3. In the device's local Setup, go to **System > Firmware Customization > Custom Partition > Partition**.
4. Add a **Partition Parameter** with the **Name** "NAME" and a **Value** of your choice.



5. Back in the Setup, click **Ok**.
6. Click the icon to test the application.
It should open, displaying a text containing the name of your choice.

Hello
Hello Bob!
Close

A Real-World CP: Chromium

The previous example was simplified, but it taught you a lot of the IGEL Custom Partition fundamentals. Now build on top of these and try your hand at a real-world CP: the Chromium web browser - the Open Source sibling of Google Chrome, a complex application with a variety of features.

> As you will be working with original Ubuntu packages, actual version numbers (or packages) may differ from this tutorial, as Ubuntu frequently update their packages. The method for building the CP, however, remains the same.

- Development Environment (see page 885)
- Getting the Ubuntu Package (see page 886)
- Unpacking the Ubuntu Package (see page 887)
- Creating a Larger CP (see page 888)
- Setting Up Library Paths via Script (see page 889)
- The First Run (see page 891)
- Obtaining Libatomic (see page 892)
- Installing Libatomic (see page 893)
- Another Test Run (see page 894)
- Providing Libffmpeg (see page 895)
- Chromium Starts Successfully (see page 896)
- Packaging the Custom Application (see page 897)
- Advanced (see page 898)

Development Environment

For this section you need

- a system with IGEL OS *version 10.03.100* or newer,
- a Windows or Linux workstation with Universal Management Suite (UMS) in *version 5.07.100* or newer,
- a Debian or Ubuntu Linux workstation for unpacking the `*.deb` package (can be the same as the Linux workstation hosting UMS),
- a method to exchange files between the thin client and the workstation.
  While a USB pen or disk drive would do the trick, it is more convenient to have either a
  - Windows fileshare or
  - an NFS export

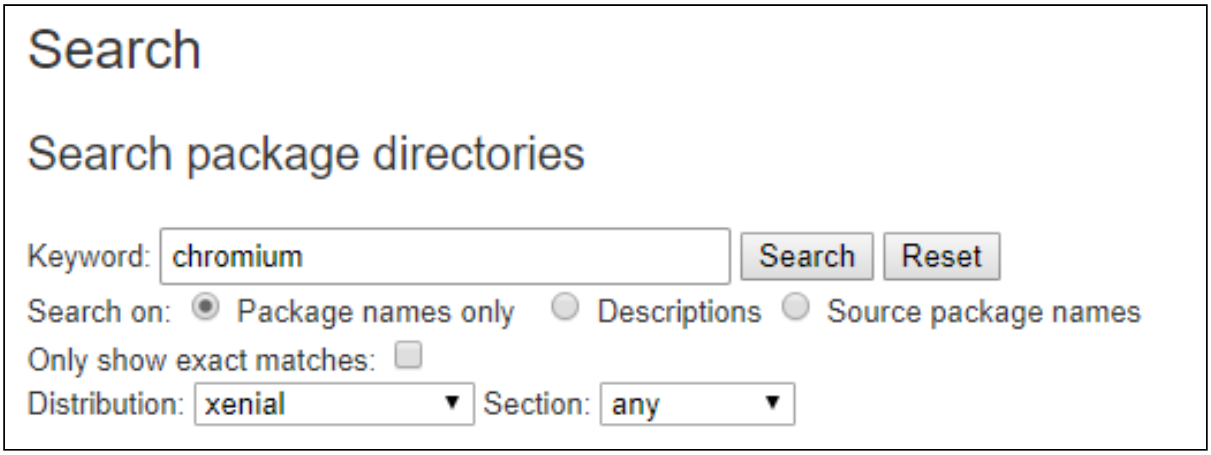
  that you can access both from the thin client and the workstation in order to exchange files.
  Learn how to mount network drives in the IGEL OS Manual. (see page 1923)

Getting the Ubuntu Package

As the Chromium web browser is Free Software it can be found in the package repositories of Linux distributions. To build Custom Partitions, use the software packages from exactly that Ubuntu version on which your version of IGEL OS is based. From IGEL OS 10.04 up to IGEL OS 11.03, this is Ubuntu 16.04 (Xenial Xerus). You need packages for the `amd64` (also known as `x86_64`) architecture.

This is how to find the right package and download it to your Linux workstation:

1. In a web browser, go to `https://packages.ubuntu.com`
2. Use the **Search package directories** form to search
   a. Set **Keyword** to `chromium`
   b. Set **Distribution** to `xenial`
   c. Click **Search**.



3. On the results page, click the **chromium-browser** package to go to its details page.
4. At the bottom of the details page, click the **amd64** link to download the package to a local directory on your Linux workstation.

Unpacking the Ubuntu Package

Extract the Ubuntu package on your Debian/Ubuntu Linux workstation in order to access its files:

1. Open a terminal emulator.
2. Change to the directory where you saved the Ubuntu package.
3. Create a directory to extract the files to:
   ```
   mkdir chromium-browser
   ```
4. Extract the package to the new directory:
   ```
   dpkg -x *.deb chromium-browser/
   ```
5. Run the following command to see how much space the package contents need in total (in MB):
   ```
   du -cms chromium-browser/*
   ```
   The total is 255 MB (your package may differ slightly). To be on the safe side let's memorize that we need approximately 400 MB of space for the CP contents.

Creating a Larger CP

Create a larger Custom Partiton so we can put all the Chromium package files into it.

1. On the thin client, make sure that you have closed all **Local Terminal** windows.
2. In UMS Console, navigate to your target thin client.
3. In **Assigned Objects**, remove the **Hello CP** profile from this thin client.
4. When prompted **When should these changes take effect?** select **Now**.
   The existing Custom Partition is deleted.
5. Right-click the thin client and select **Edit Configuration**.
6. In Setup go to **System > Firmware Customization > Custom Partition > Partition**.
7. Check **Enable Partition**.
8. Set the **Size** to `400M` (Megabyte) to be on the safe side.
9. Leave the **Mount Point** at `/custom`
10. Click **Save**.
    The new Custom Partition is created.
11. On the thin client, open a **Local Terminal** and log in as `root`
12. Change into the Custom Partition: `cd /custom`
13. Check the size of the Custom partition: `df -h ./`
    It should be roughly 400M - if it is still roughly 10M, close **Local Terminal** and use **Setup** to first disable and then re-create the Custom Partition again.
14. Copy the complete `chromium-browser/` directory with all its contents from the Debian/Ubuntu machine into the Custom Partition on the thin client.

Setting Up Library Paths via Script

With the whole package contents in place, you need to make sure that Chromium will be able to find its libraries and other needed files. There is a pre-fabricated script for this.

1. Log into **Local Terminal** as `root`.
2. Change into the `/custom/chromium-browser` directory.
3. Enter the command `ls -l`.
4. You will see that instead of a single script as in the previous example there are the `etc/` and `usr/` directories. They include many libraries and other files that Chromium will need to run. However, it expects these directories not within the `/custom/chromium-browser/` directory, but in the filesystem root, where system directories such as `/usr` are located. The Initialization Script for the Custom Partition will fix this by setting up symbolic links, so that for example `/custom/chromium-browser/usr/lib/library.so` will appear to be in `/usr/lib/library.so`, where Chromium expects it.
5. Use the GNU nano editor to create the file `custompart-chromium-browser` and put the following contents into it - alternatively, edit the file elsewhere and copy it into `/custom/chromium-browser/`:

```
#!/bin/sh
ACTION="custompart-chromium-browser_${1}"
# mount point path
MP=$(get custom_partition.mountpoint)
# custom partition path
CP="${MP}/chromium-browser"
# output to systemlog with ID amd tag
LOGGER="logger -it ${ACTION}"
echo "Starting" | $LOGGER
case "$1" in
init)
    # Initial permissions
    chown -R root:root "${CP}" | $LOGGER
    chmod 755 "${MP}" | $LOGGER
    # Linking files and folders on proper path
    find "${CP}" | while read LINE
    do
        DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
        if [ ! -z "${DEST}" -a ! -e "${DEST}" ]; then
            # Remove the last slash, if it is a dir
            [ -d $LINE ] && DEST=$(echo "${DEST}" | sed -e "s/\/$//g") |
$LOGGER
            if [ ! -z "${DEST}" ]; then
                ln -sv "${LINE}" "${DEST}" | $LOGGER
```

```
            fi
        fi
    done
    ldconfig
;;
stop)
    killall -q -SIGTERM chromium-browser
    sleep 1
    killall -q -SIGKILL chromium-browser
;;
esac
echo "Finished" | $LOGGER
exit 0
```

Use this as a script template for your Custom Partitions, replacing all instances of `chromium-browser` with the directory name of your CP.

6. Make the script executable with the following command:
   `chmod a+x custompart-chromium-browser`
7. Run the script:
   `./custompart-chromium-browser init`
   It should run and finish without any errors.
   The library paths are set up now.

The First Run

Now that the paths for the complete Chromium package contents have been set up, try running the program for the first time:

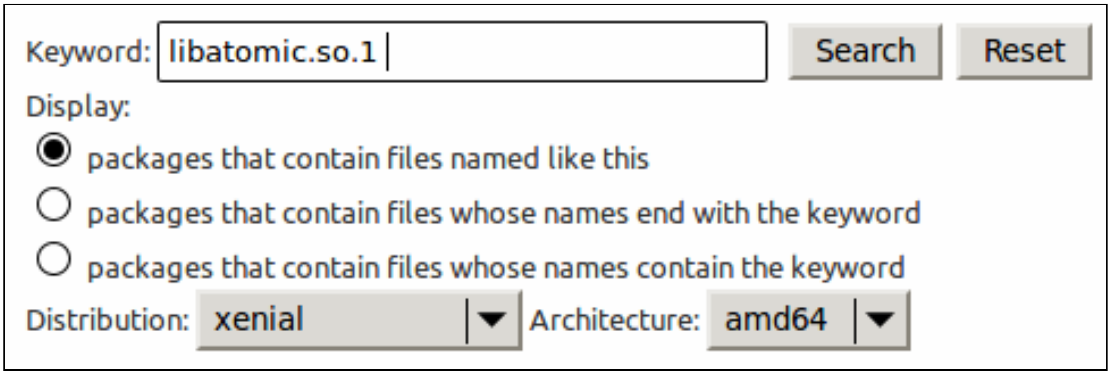
1. Log into **Local Terminal** as `root`.
2. Change into the `/custom/chromium-browser/` directory.
3. The `usr/bin/` and `usr/lib/` directories are good candidates for Chromium's main executable. Try to run the following command:
   `./usr/lib/chromium-browser/chromium-browser`

   You will see the following error message:
   `/usr/lib/chromium-browser/chromium-browser: error while loading shared libraries:`
   `libatomic.so.1: cannot open shared object file: No such file or directory`
   This tells you that the program tries to load the shared library `libatomic.so.1`, but can't find it.
   You will need to obtain `libatomic.so.1` and install it.

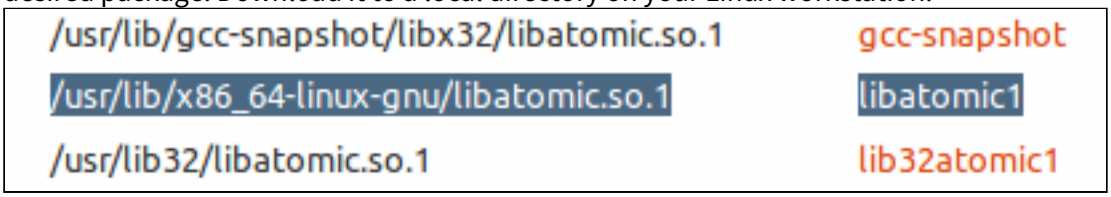
Obtaining Libatomic

The source for Libatomic will be Ubuntu Package Search again:

1. In a web browser, go to `https://packages.ubuntu.com`
2. This time use the **Search the contents of packages** form to search.
   a. Set **Keyword** to `libatomic.so.1`
   b. Select **packages that contain files named like this**.
   c. Set **Distribution** to `xenial`
   d. Set **Architecture** to `amd64`
   e. Click **Search**.



3. This time the results page lists a lot of packages. But with the background knowledge that IGEL OS libraries are located in `/usr/lib/x86_64-linux-gnu/` you will find that **libatomic1** is the desired package. Download it to a local directory on your Linux workstation.



Installing Libatomic

This step installs Libatomic and sets up a symbolic link so the Chromium will find it.

1. Extract the package contents with this command:
   `dpkg -x libatomic*.deb libatomic`
2. Change into the extracted contents:
   `cd libatomic1/usr/lib/x86_64-linux-gnu/`
3. List its contents in long form: `ls -l`

   ```
   lrwxrwxrwx 1 huber huber    18 Nov  3  2016 libatomic.so.1 -> libatomic.so.1.1.0
   -rw-r--r-- 1 huber huber 26760 Nov  3  2016 libatomic.so.1.1.0
   ```

   This shows you that the library file is actually named `libatomic.so.1.1.0` and that `libatomic.so.1` is a symbolic link to it. We will recreate the link on the thin client later.
4. Transfer the `libatomic.so.1.1.0` file to the thin client and place it in:
   `/custom/chromium-browser/usr/lib/chromium-browser/`
5. Change into the directory:
   `cd /custom/chromium-browser/usr/lib/chromium-browser/`
6. Create the symbolic link:
   `ln -s libatomic.so.1.1.0 libatomic.so.1`
   Now Libatomic is set up to be used by Chromium.

Another Test Run

Test whether Chromium now has everything it needs to run.

1. Change into the Custom Partition directory on the thin client:
   `cd /custom/chromium-browser`
2. Run Chromium:
   `./usr/lib/chromium-browser/chromium-browser`
3. You will see this error message:
   `/usr/lib/chromium-browser/chromium-browser: error while loading shared libraries:`
   libffmpeg.so: cannot open shared object file: No such file or directory

   It seems Libatomic is no longer a problem, but now Chromium needs a further library:
   `libffmpeg.so`

Providing Libffmpeg

To obtain Libffmpeg, repeat the process for obtaining Libatomic (see page 892). Hint: The Ubuntu package is named `chromium-codecs-ffmpeg`. It contains the file `libffmpeg.so`, which you need to transfer to the thin client. Place it in `/custom/chromium-browser/usr/lib/chromium-browser/.`

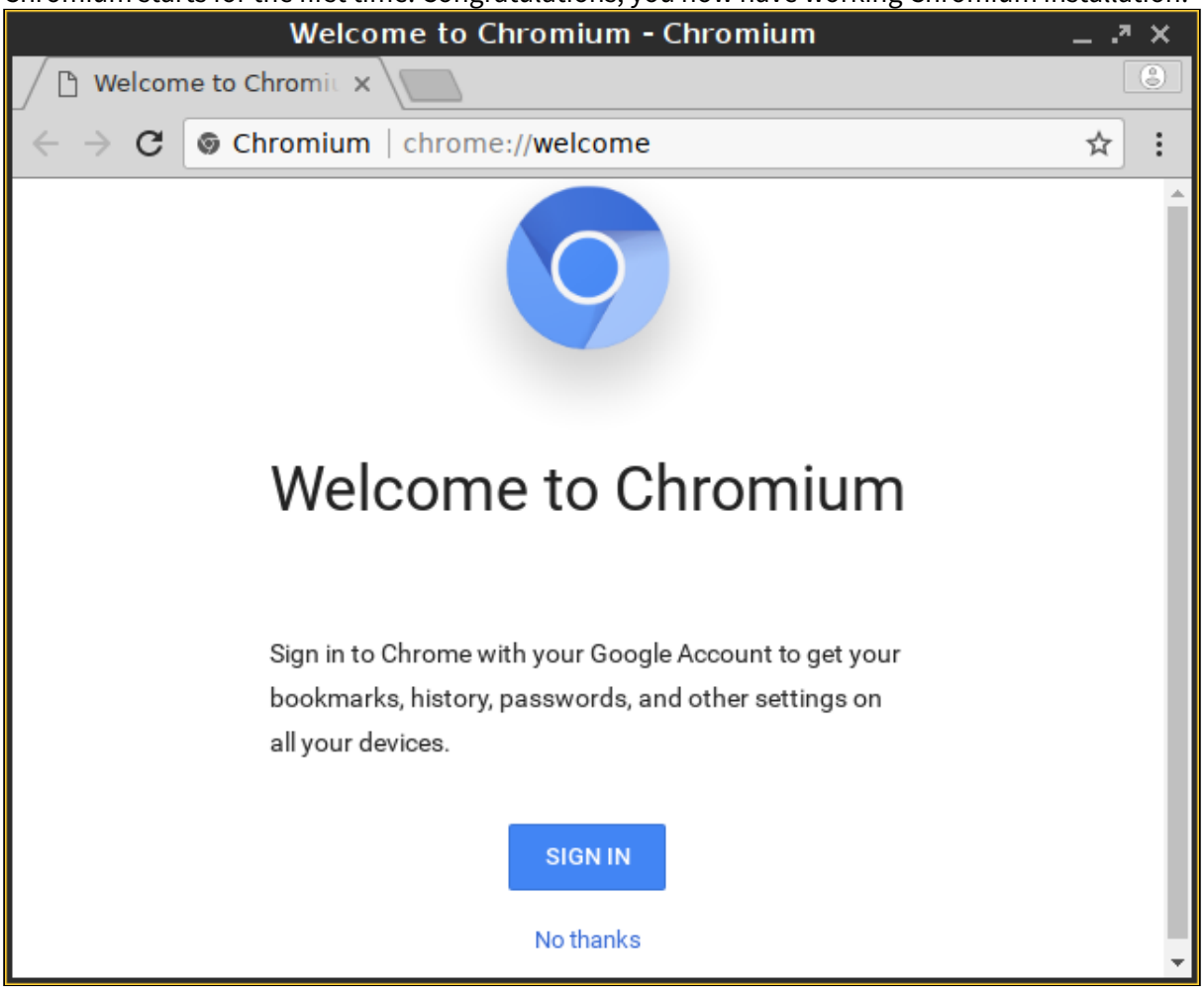
This is a procedure that you need to repeat until you have supplied all required libraries:

- Run the application from the commandline.
- Scan the error message for needed libraries.
- Obtain and install the required libraries.
- Run the application from the commandline.
- ...

Chromium Starts Successfully

Now you are ready to give running Chromium another try. It does not like to be started by `root`, because it is much safer to run it as the non-privileged `user`.

1. Log into **Local Terminal** as `user`.
2. Change into the `/custom/chromium-browser` directory.
3. Enter the following command:
   `./usr/lib/chromium-browser/chromium-browser`
   Chromium starts for the first time. Congratulations, you now have working Chromium installation.



The next step will package the Custom Partition so it can be deployed to any number of thin clients from UMS:

Packaging the Custom Application

Now that the hardest part of creating the Custom Partition is done, package the CP for UMS. You are already familiar with most of the steps from earlier in this tutorial.

1. Compress the CP Contents (see page 866) into `chromium-browser.tar.bz2`
2. Upload the compressed file to UMS as a new **File**.
3. Write the *.inf Metadata File (see page 867) with `400M` as **size**.
4. Upload the *.inf Metadata File to UMS as a new **File**.
5. Create a Profile for the CP (see page 875) with the **Initializing Action** set to:
   `/custom/chromium-browser/custompart-chromium-browser init`
   and the **Finalizing Action** set to:
   `/custom/chromium-browser/custompart-chromium-browser stop`
6. Create a Custom Application (see page 859) with the **Command** set to:
   `/custom/chromium-browser/usr/lib/chromium-browser/chromium-browser`
7. Assign the CP to a new thin client in order to test everything.

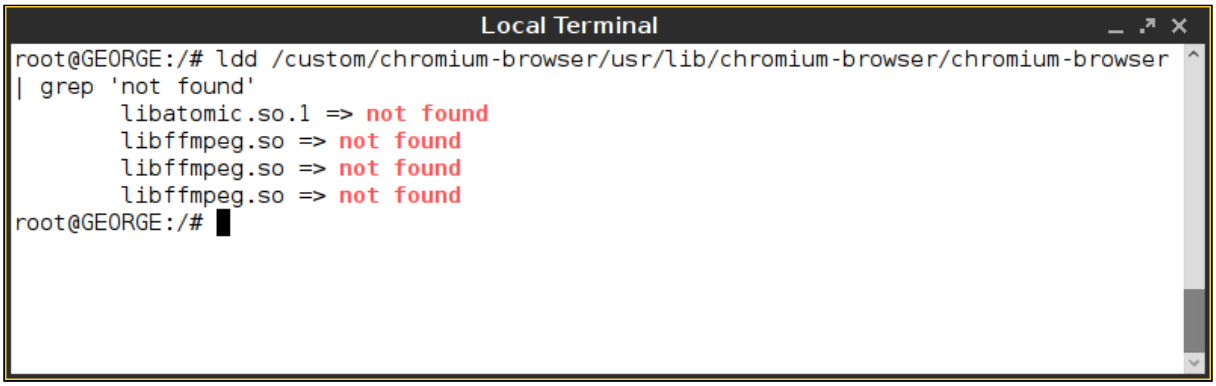
Advanced

Here are some advanced topics for you to try after you have completed this tutorial.

Using ldd to Find Required Libraries

Using the `ldd` command is another way of determining the libraries that a binary requires.

1. Log into **Local Terminal** as `root`.
2. Find out which file the main binary of the Custom Partition is. It is usually found in `bin/`, `usr/bin/` or `usr/lib/` and is named similar to the application name.
3. Run the following command:
   `ldd /custom/[name]/[binary] | grep 'not found'`
   This command line contains a filter, so that it will only show you those libraries that could not be found.



Auto-updating Custom Partitions

The Custom Partition mechanism in IGEL OS can update the Custom Partition contents automatically when a newer version is available on UMS. To activate it, follow these steps:

1. In Setup, go to **System > Firmware Customization > Custom Partitition > Download**.
2. Open the CP entry in the **Partitions Data Sources** list.
3. Enable **Automatic Update**.
4. Click **OK**.
5. Click **Apply** or **Save** in the Setup window.
6. On UMS, increase the `version` property in the `*.inf` metadata file.
   When booting, the thin client checks whether there is a higher version of the Custom Partition available on UMS. If so, the new CP version will be downloaded automatically.

Zoom as a Custom Partition

Now that you have learned the IGEL Custom Partition fundamentals, build on top of these and try your hand at a real-world Custom Partition: Zoom.

Read all the following chapters in the order given and follow the instructions.

1. Development Environment (see page 900)
2. Getting the Packages (see page 901)
3. Unpacking the Packages (see page 902)
4. Creating the Initialization Script (see page 903)
5. Compressing the Custom Partition Contents (see page 906)
6. Writing the *.inf Metadata File (see page 907)
7. Uploading the Files to the UMS (see page 908)
8. Creating a Profile for the Custom Partition (see page 911)
9. Assigning the Profile and Testing the Application (see page 920)

Development Environment

For this section, you need

- a system with IGEL OS 11.01.100 or newer,
- Universal Management Suite (UMS) 6.01.100 or newer,
- a Debian or Ubuntu workstation for unpacking the `*.deb` package (can be the same as the Linux workstation hosting the UMS. Ideally, the machine is running Ubuntu 18.04 LTS.
- a method to exchange files between the endpoint device and the workstation.
  While a USB memory stick or disk drive would do the trick, it is more convenient to have either a
  - Windows fileshare or
  - an NFS export

  that you can access both from the endpoint device and the workstation in order to exchange files.
  Learn how to mount network drives in the IGEL OS Manual. (see page 1923)

Next Step

>> Getting the Packages (see page 901)

Getting the Packages

Get the required packages for Ubuntu. Apart from the Zoom package, you need the package `libxcb-xtest0[version].deb` (contains the shared libraries `libxcb-test.so.0` and `libxcb-test.so.0.0.0` which are required by the Zoom package).

1. Open https://zoom.us/download?os=linux in a browser and select the following:
   - **Linux Type**: "Ubuntu"
   - **OS Architecture**: "64 bit"
   - **Version**: "16.04+"
2. Download the Ubuntu/Debian package `zoom_amd64.deb`

   Version 5.0.399860.0429 has been tested by IGEL. Newer versions should work, too.

3. Change to the download directory on your workstation (typically `/home/[username]/Downloads`).
4. Download `libxcb-xtest0[version].deb` with the following command:
   `apt download libxcb-xtest0`

Next Step

>> Unpacking the Packages (see page 902)

Unpacking the Packages

In this step, you extract the Ubuntu packages on your Linux workstation in order to access their files:

1. Open a terminal.
2. Change to the directory where you saved the packages.
3. Create a directory to extract the files to:
   ```
   mkdir zoom
   ```
4. Extract the packages to the new directory:
   ```
   dpkg -x zoom*.deb zoom/
   ```
   ```
   dpkg -x libx*.deb zoom/
   ```
5. Run the following command to see how much space the package contents need in total (in MB):
   ```
   du -cms zoom/*
   ```
   The total is 151 MB (your package may differ slightly). To be on the safe side, let's memorize that we need approximately 500 MB of storage space for the Custom Partition contents.

Next Step

>> Creating the Initialization Script (see page 903)

Creating the Initialization Script

In this step, you will create an initialization script that enables the application to work inside a Custom Partition. In a regular installation, the files of the Zoom application would be located in `/usr`, `/opt` and so on, whereas in the Custom Partition, they are located under `/custom/zoom/usr`, `/custom/zoom/opt` and so on. The initialization script will fix this by creating symbolic links so that for example `/custom/zoom/usr/lib/library.so` will appear to be in `/usr/lib/library.so`, where Zoom expects it.

1. On your workstation, go to the directory where the `zoom` directory is located.
2. Open your text editor of choice and enter the following script:

```
#!/bin/sh

ACTION="custompart-zoom_${1}"

# mount point path
MP=$(get custom_partition.mountpoint)

# custom partition path
CP="${MP}/zoom"

# wfs for persistent login and history
WFS="/wfs/user/.zoom/data"

# .zoom directory
ZOOM="/userhome/.zoom/"

# output to systemlog with ID amd tag
LOGGER="logger -it ${ACTION}"

echo "Starting" | $LOGGER

case "$1" in
init)
        # Linking files and folders on proper path
    find ${CP} | while read LINE
        do
                DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
                if [ ! -z "${DEST}" -a ! -e "${DEST}" ]; then
                        # Remove the last slash, if it is a dir
                        [ -d $LINE ] && DEST=$(echo "${DEST}" | sed -e "s/\/$//
g") | $LOGGER
                        if [ ! -z "${DEST}" ]; then
                                ln -sv "${LINE}" "${DEST}" | $LOGGER
                        fi
                fi
        done
```

```
    # Linking /userhome/.zoom/data to /wfs/user/.zoom/data for some basic
persistency
    mkdir -p ${WFS}
    chown -R user:users ${WFS}
    mkdir -p ${ZOOM}/data
    chown -R user:users ${ZOOM}/data
        mkdir -p ${ZOOM}/data/VirtualBkgnd_Custom
        chown -R user:users ${ZOOM}/data/VirtualBkgnd_Custom
        mkdir -p ${ZOOM}/data/VirtualBkgnd_Default
        chown -R user:users ${ZOOM}/data/VirtualBkgnd_Default

    ln -sv ${WFS}/zoomus.db ${ZOOM}/data/zoomus.db | $LOGGER
    ln -sv ${WFS}/zoommeeting.db ${ZOOM}/data/zoommeeting.db | $LOGGER
    ln -sv ${WFS}/VirtualBkgnd_Custom ${ZOOM}/data/ | $LOGGER
    ln -sv ${WFS}/VirtualBkgnd_Default ${ZOOM}/data/ | $LOGGER

        chown user:users /wfs/user/.zoom
        ln -sv /wfs/user/.zoom/zoomus.conf /userhome/.config/zoomus.conf |
$LOGGER

        # remove all com.zoom.ipc* files from /wfs/user/.zoom/data - might
cause issues when updating zoom
        rm ${WFS}/com.zoom.ipc*

    # add /opt/zoom to ld_library
    echo "${CP}/opt/zoom" > /etc/ld.so.conf.d/zoom.conf
    ldconfig

    ${MP}/zoom_postinst | $LOGGER

;;
stop)
    # unlink linked files
    find ${CP} | while read LINE
        do
                DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
        unlink $DEST | $LOGGER
    done

    # remove zoom.conf because it is not needed anymore
    rm /etc/ld.so.conf.d/zoom.conf


;;
esac

echo "Finished" | $LOGGER

exit 0
```

> The code line `echo "${CP}/opt/zoom" > /etc/ld.so.conf.d/zoom.conf` tells the Zoom application via the configuration file `zoom.conf` to search for libraries in `/custom/opt/zoom`. This is expected by the Zoom application.

3. Save the file as `custompart-zoom`

Next Step

>> Compressing the Custom Partition Contents 2 (see page 906)

Compressing the Custom Partition Contents

To make the unpackaged software package usable in a Custom Partition, make the application files executable and put them into a compressed `tar` file.

1. On your Linux workstation, open a terminal and change to the directory that contains the `zoom/` directory with the application files and the initialization script `custompart-zoom`.
2. Make the files in `zoom/` and the initialization script executable:
   `chmod -R +x zoom`
   `chmod +x custompart-zoom`
3. Compress the `zoom/` directory and the initialization script into an archive file named `zoom_[version].tar.bz2` (in our example: `zoom_5.0.399860.0429.tar.bz2`):
   `tar cjvf zoom_5.0.399860.0429.tar.bz2 zoom custompart-zoom`

Next Step

>> Writing the *.inf Metadata File 1 (see page 907)

Writing the *.inf Metadata File

In addition to the compressed archive that you created in the previous step, a plain text file with essential information for the endpoint device is necessary. In this, step you will create the `zoom.inf` file.

1. Change to the directory that contains the compressed contents of our Custom Partition.
2. Create a new file named `zoom.inf` and put the following into it:

```
[INFO]
[PART]
file="zoom_5.0.399860.0429.tar.bz2"
version="5.0.399860.0429_igel1"
size="500M"
name="zoom"
minfw="11.01.100"
```

> For an explanation of the settings, see the corresponding page in the section about building a simple Custom Partition: Writing the *.inf Metadata File (see page 867).

Next Step

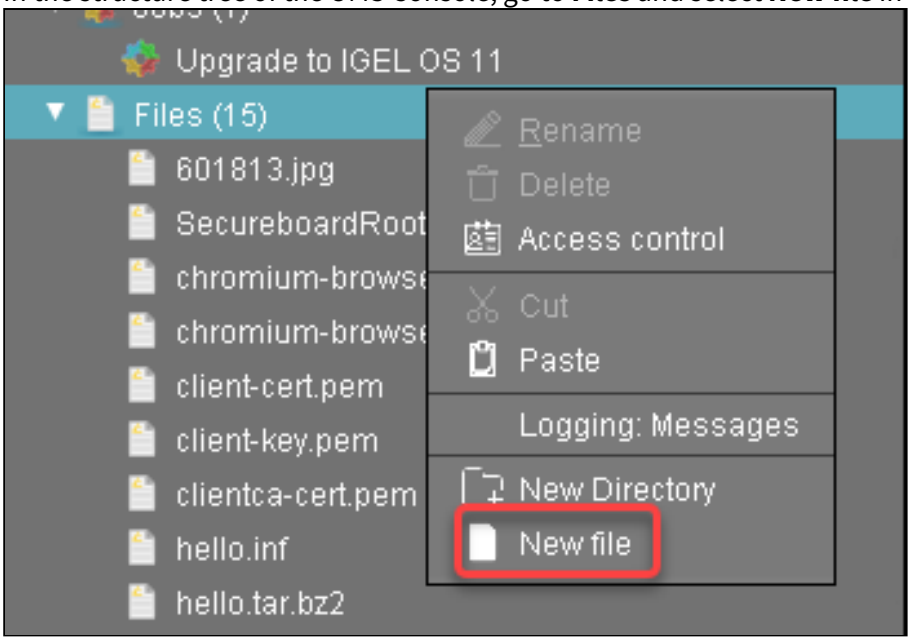
>> Uploading the Files to the UMS 2 (see page 908)

Uploading the Files to the UMS

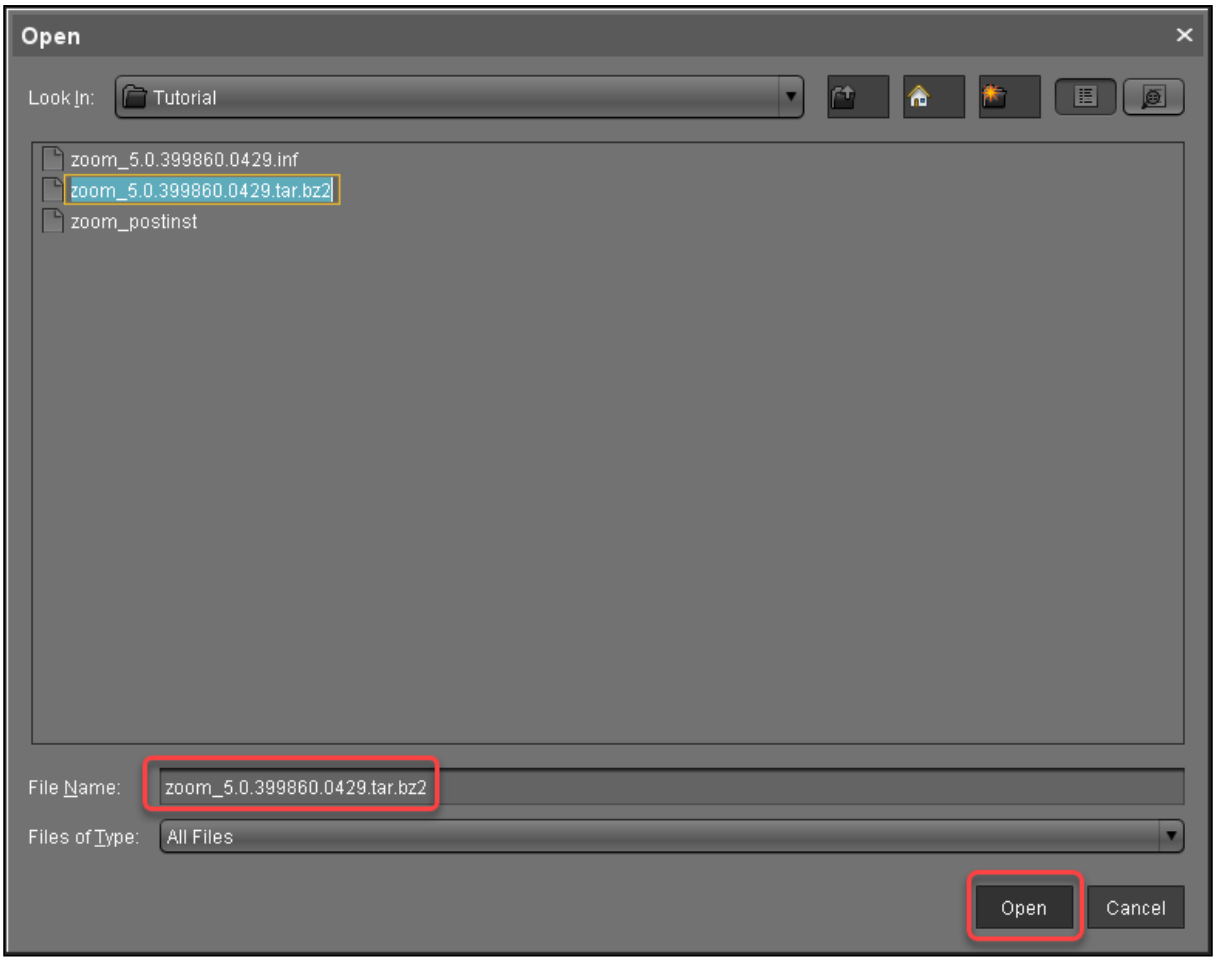
In this step, you upload the compressed `zoom_[version].tar.bz2` archive and the `zoom_[version].inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

Transferring the Files to the UMS

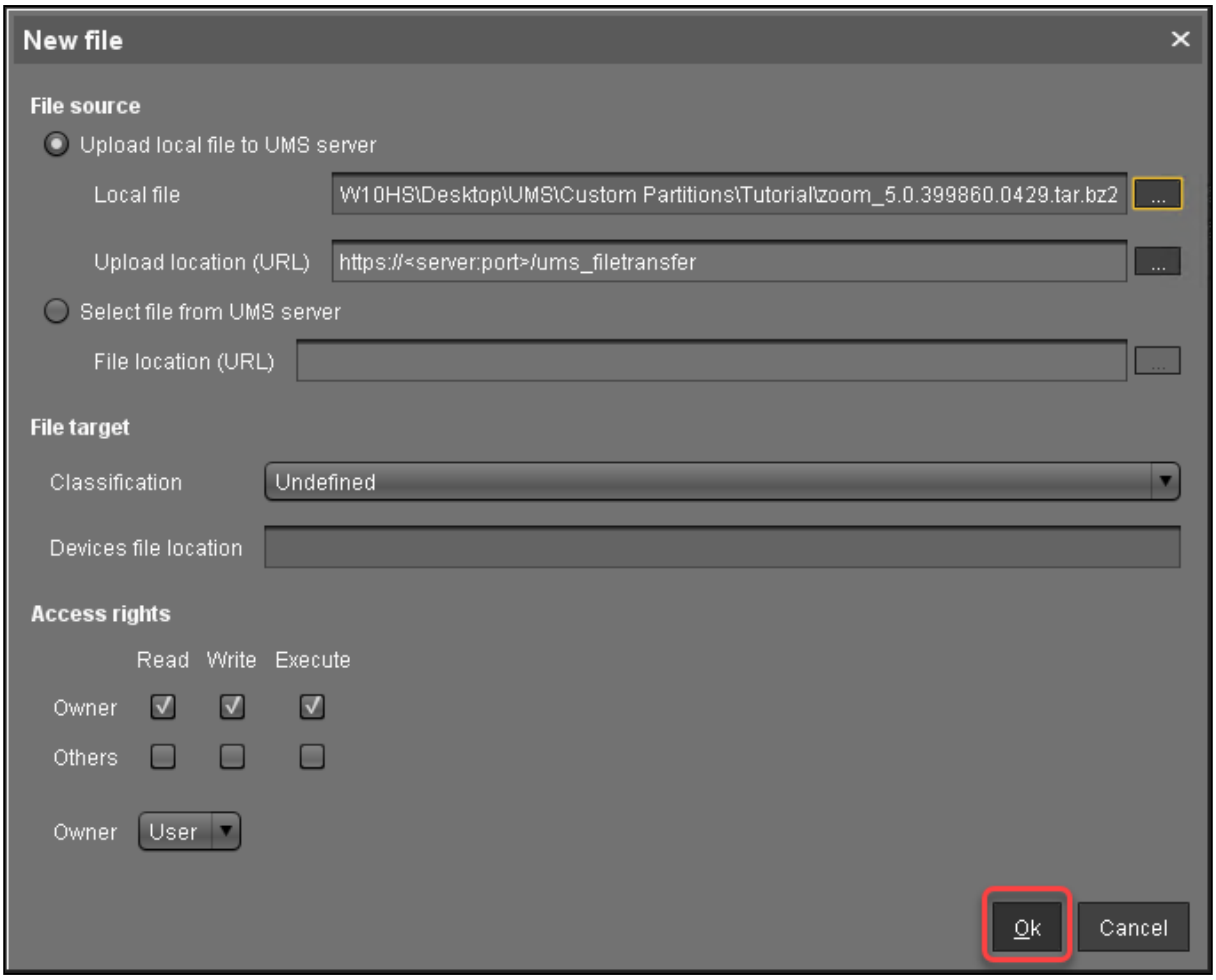
1. Make sure that the Zoom files can be accessed from the machine that hosts the UMS Console.
2. In the structure tree of the UMS Console, go to **Files** and select **New file** in the context menu.



3. Click ... next to the **Local file** field, select `zoom_[version].tar.bz2` on your local machine, and click **Open**.



4. Click ... next to the **Target URL** to define the file path on the UMS Server.
5. Review the file name at **Local file** and click **Ok**.



6. Repeat steps 1 to 5 for `zoom_[version].inf`

Next Step

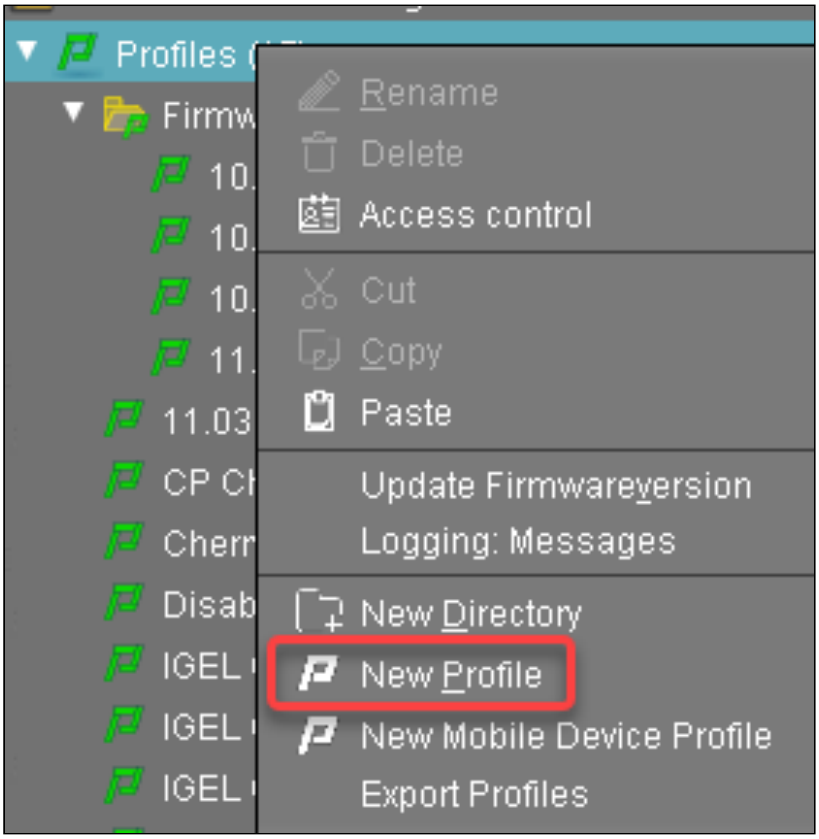
>> Creating a Profile for the Custom Partition (see page 911)

Creating a Profile for the Custom Partition

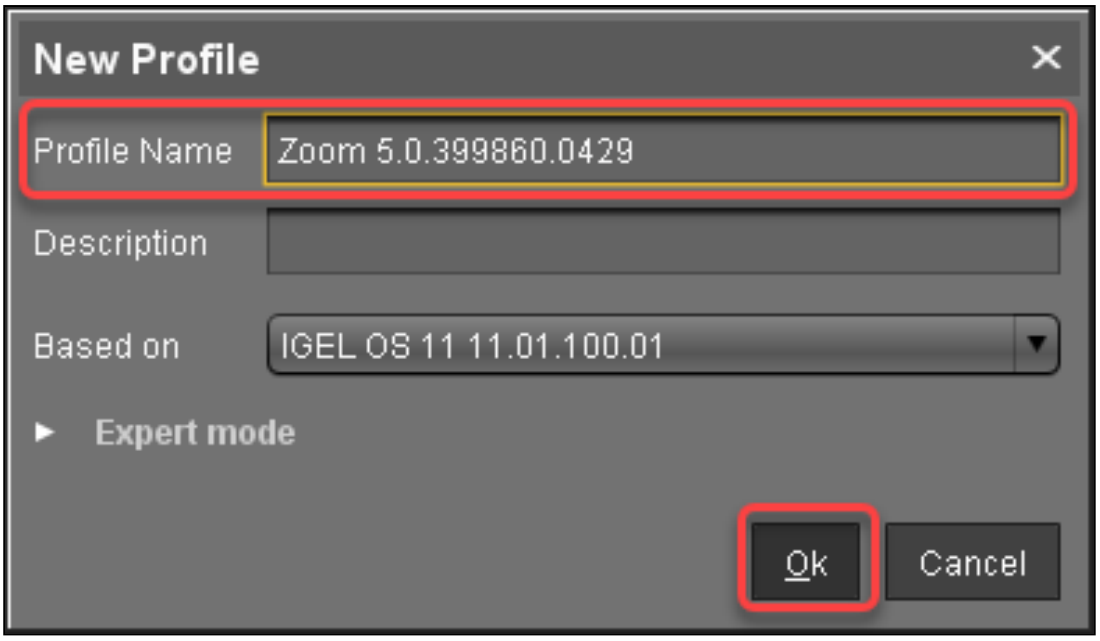
After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, you create a profile.

Activating the Custom Partition

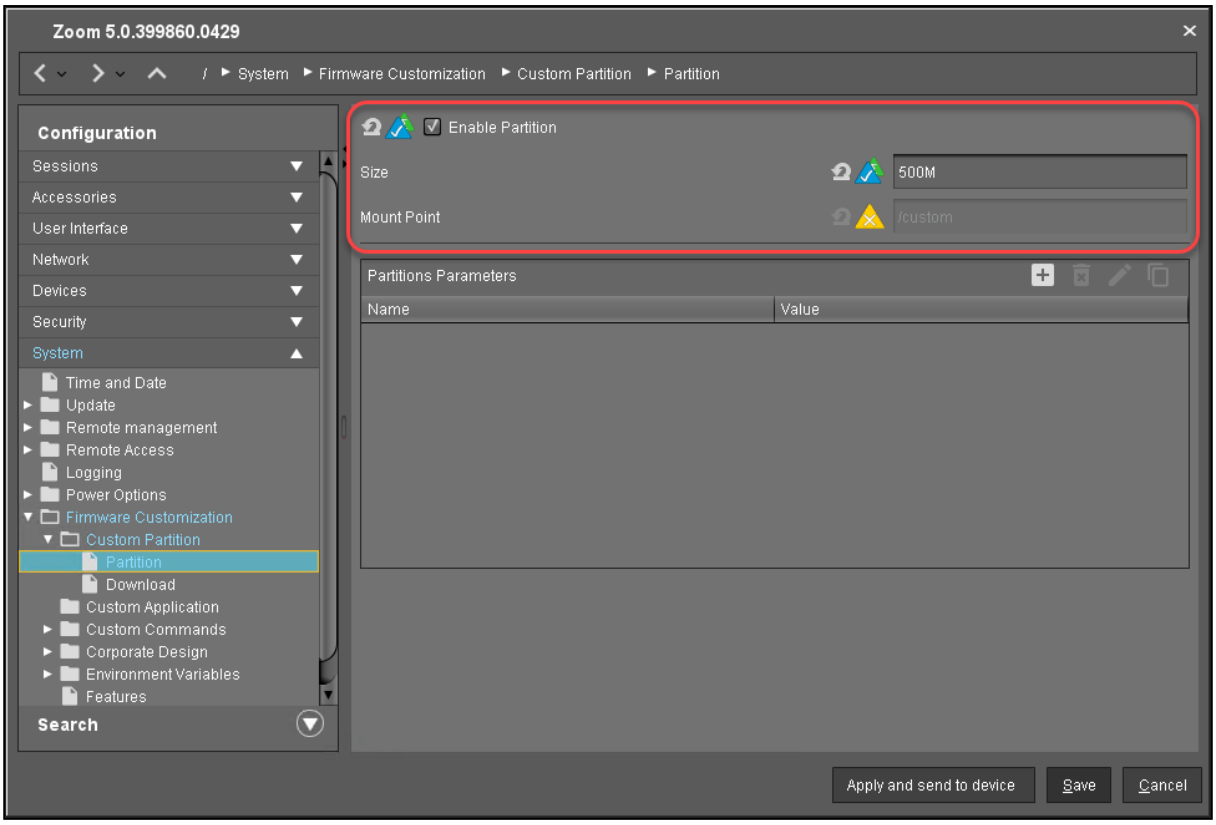
1. In the structure tree of the UMS Console, right-click the **Profiles** folder and select **New Profile** from the context menu.



2. In the **New Profile** dialog, enter a **Profile Name**, e. g. "Zoom" followed by the version name, and click **Ok**.



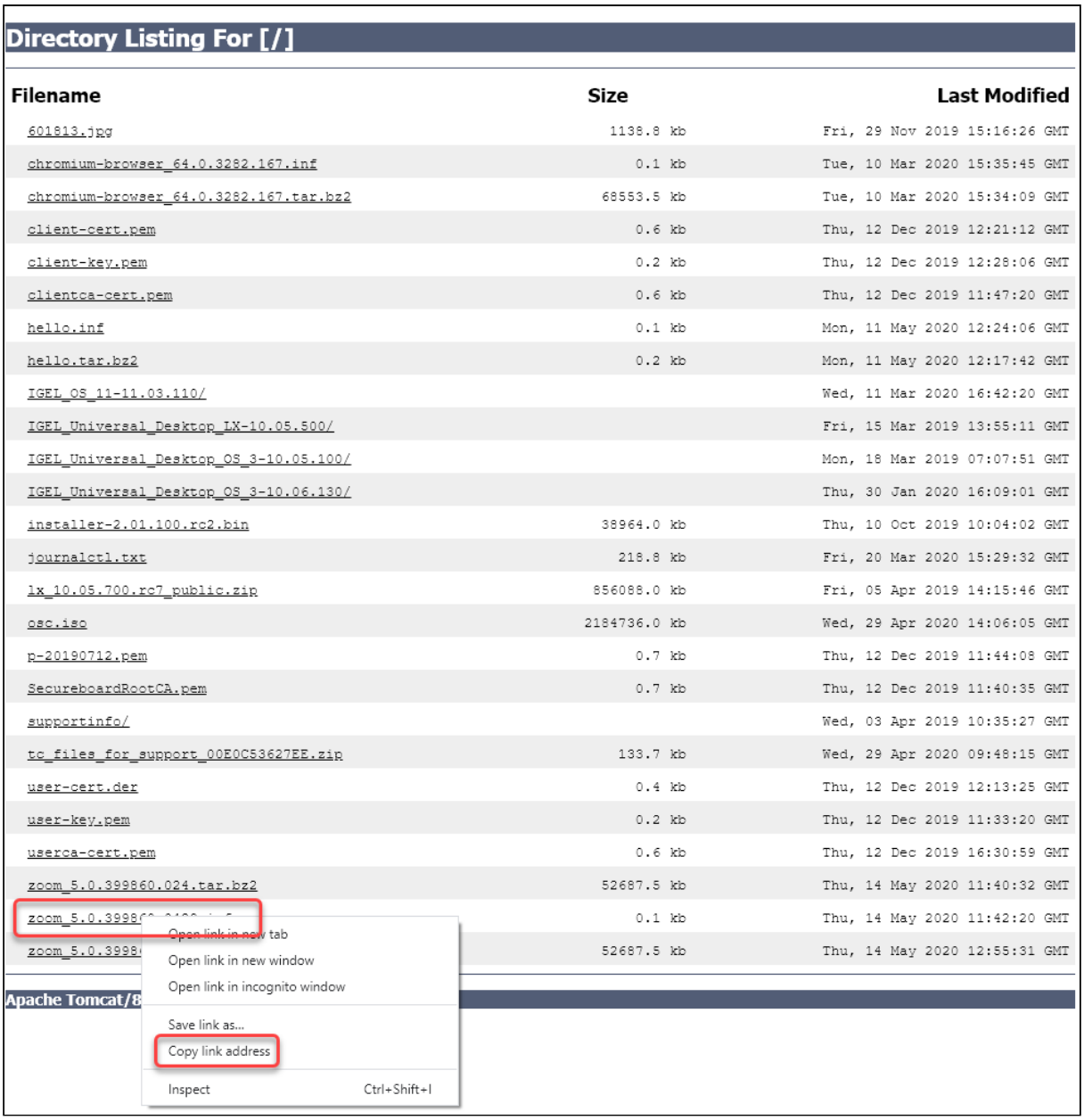
3. Go to **System > Firmware Customization > Custom Partition > Partition**.
4. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue.
5. Check **Enable Partition**.
6. Unlock the **Size** setting by clicking the orange triangle so that it turns blue, and enter "500M".
7. Leave the **Mount Point** at "/custom".



Setting the Download Source

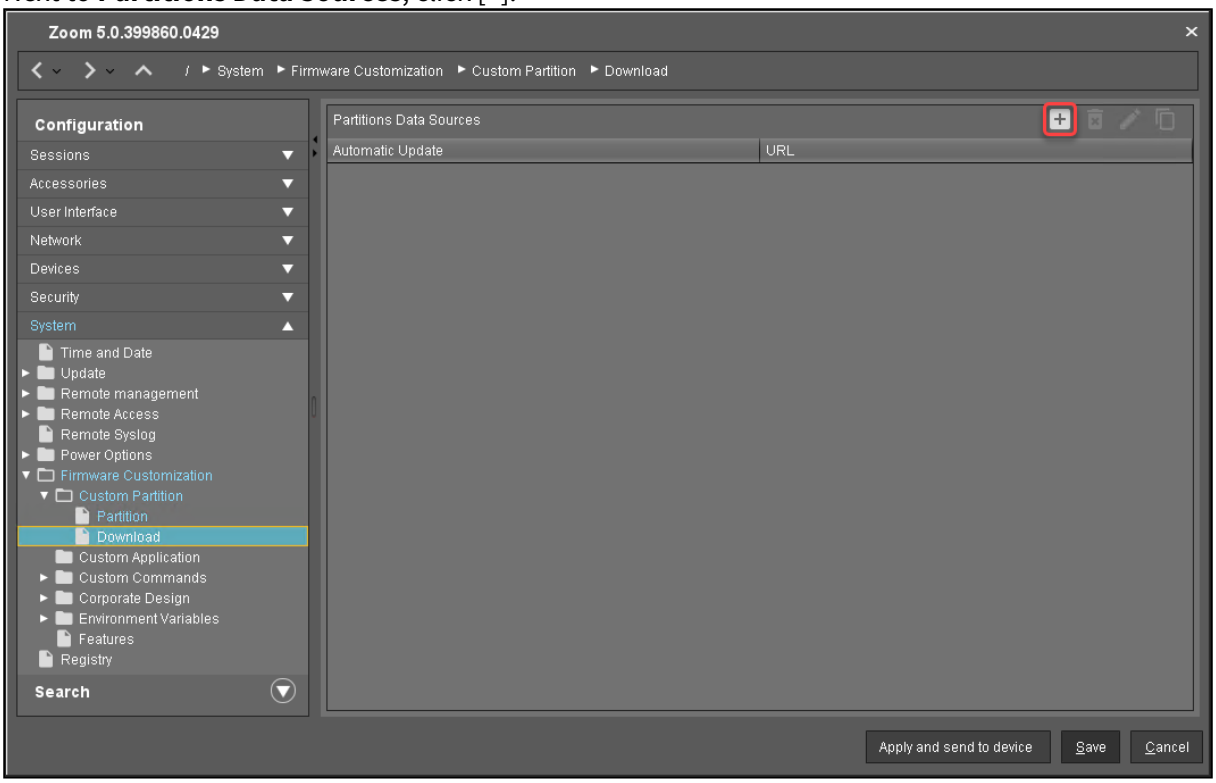
For this step, you need to determine the HTTPS download address for the `zoom.inf` file first.

1. To find out the IP address of your UMS, go to **System > Remote Management** in the configuration dialog. You will find the UMS Server your device is registered with and its IP address.
2. Open a web browser and visit the following URL:
   `https://[IP or name of your UMS host]:8443/ums_filetransfer`
3. When prompted, authenticate with your UMS username and password.
   You will see a directory listing of the files that can be downloaded from the UMS.
4. Right-click the **zoom_[version].inf** entry and select **Copy link address** (or the like, depending on your browser).



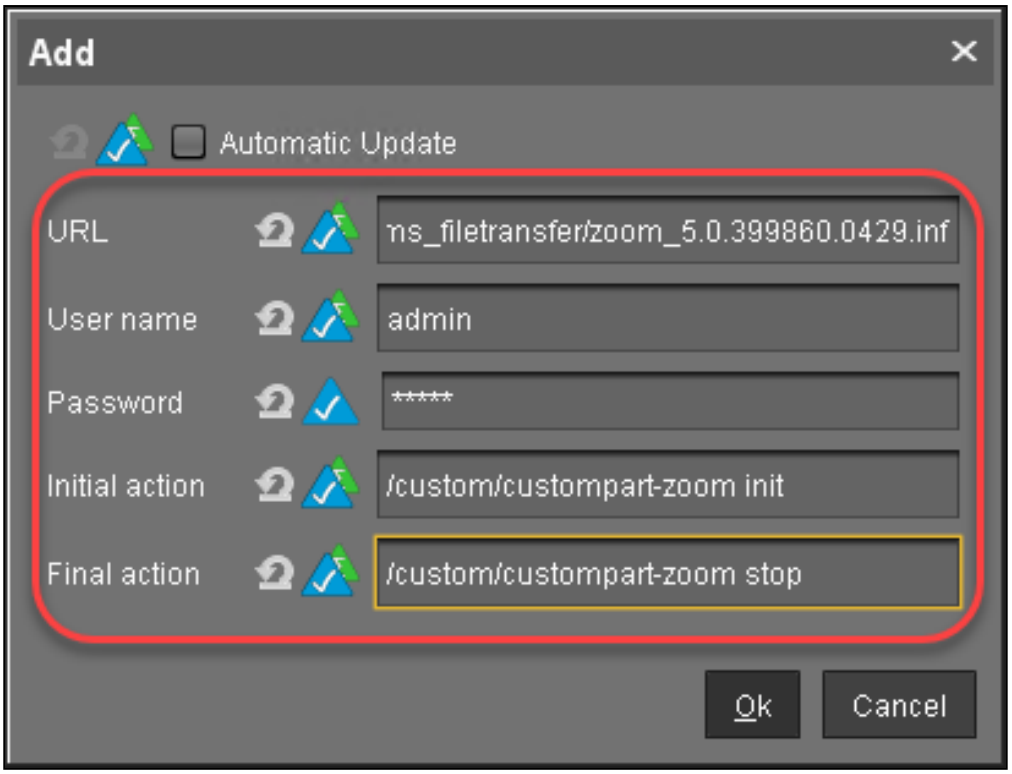
5. Back in the profile, go to **System > Firmware Customization > Custom Partition > Download**.

6. Next to **Partitions Data Sources**, click [+].



The **Add** dialog opens.

7. Edit the settings as follows:
    - **URL**: Paste the URL you copied from the browser.
    - **User name**: Username for accessing the UMS
    - **Password**: Password for the username
    - **Initial action**: Enter "/custom/custompart-zoom init".
    - **Final action**: Enter "/custom/custompart-zoom stop".

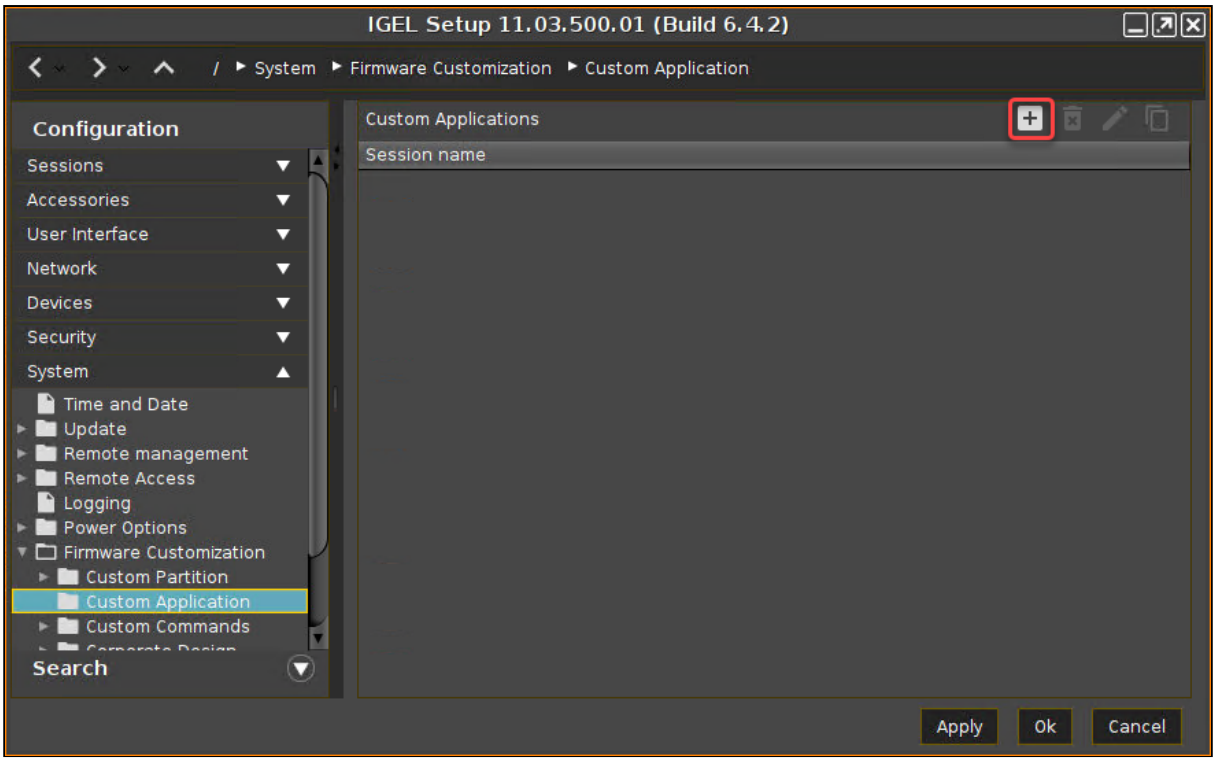


8. Click **OK**.

Configuring the Custom Application

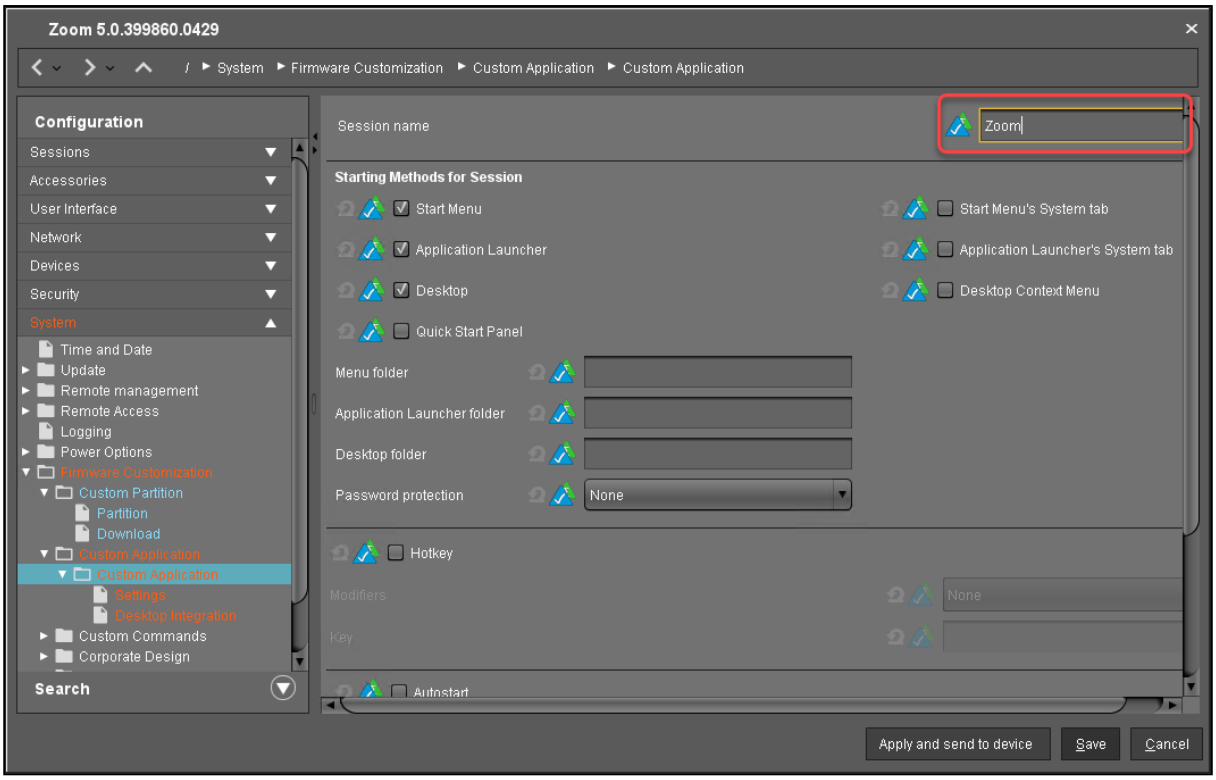
To create a convenient starting method for the user, create a custom application that includes a starter icon on the desktop.

1. Go to **System > Firmware Customization > Custom Application**.
2. In the **Custom Applications** list, click + to add an application.

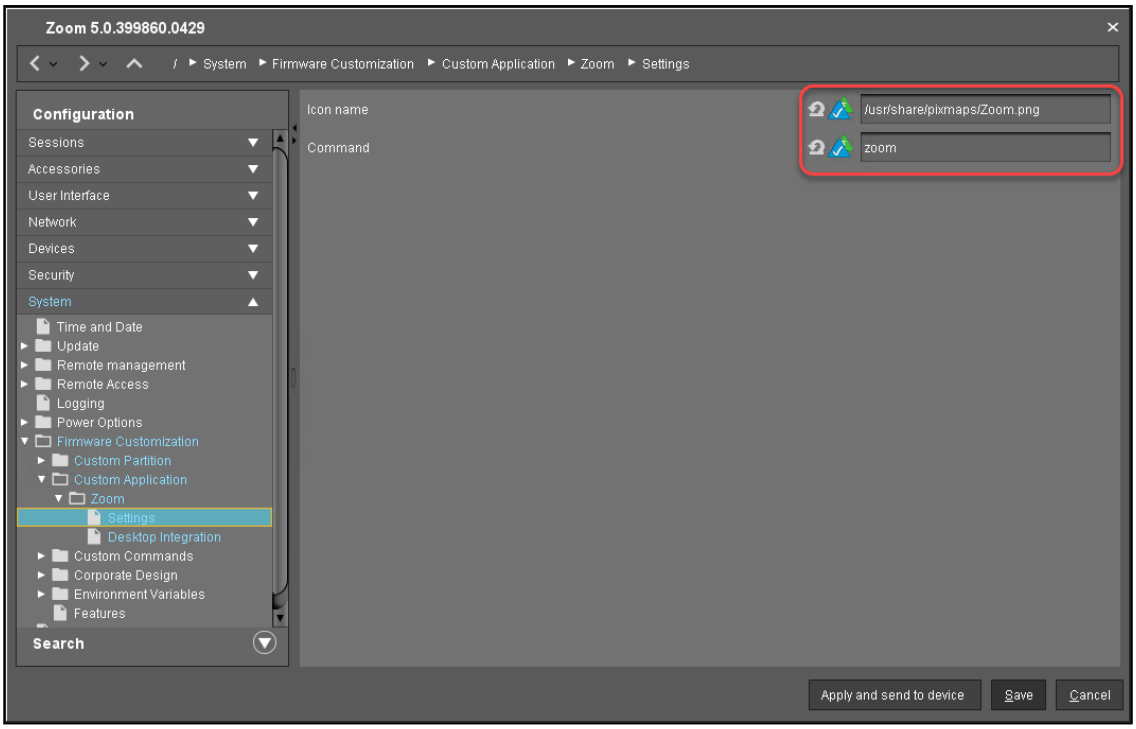


The **Desktop Integration** page opens.

3. Enter "Zoom" as the **Session name**.



4. Go to **Settings**.
5. Edit the settings as follows:
    - **Icon name**: Enter "/usr/share/pixmaps/Zoom.png".
    - **Command**: Enter "zoom".



6. Click **Save**.

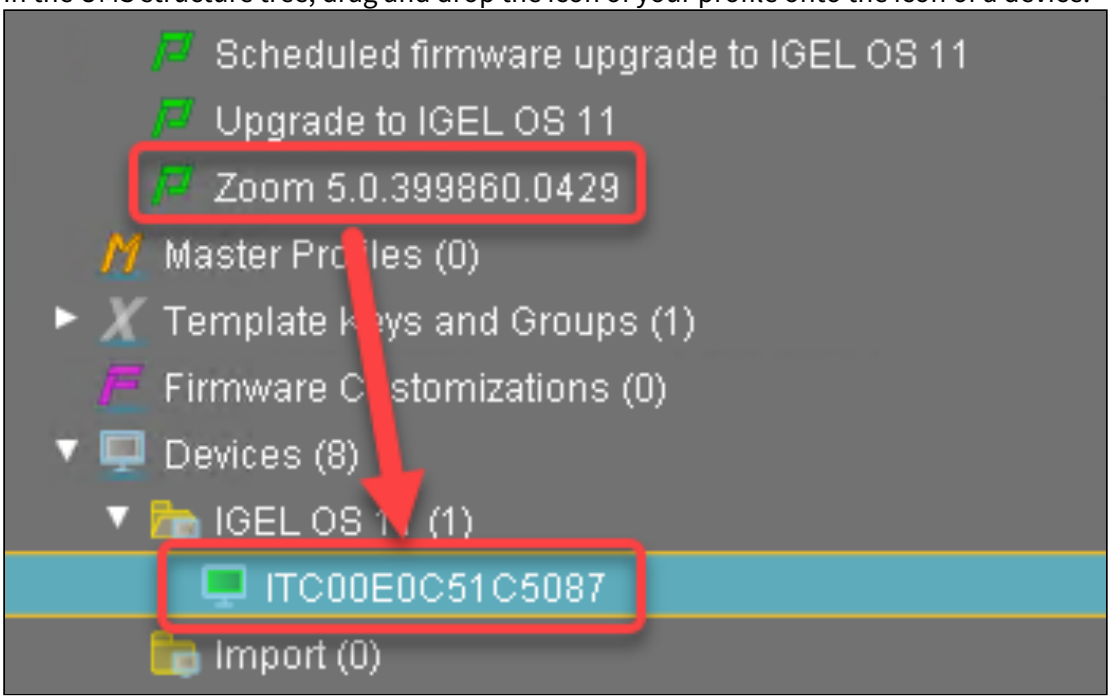
Next Step

>> Assigning the Profile and Testing the Application (see page 920)

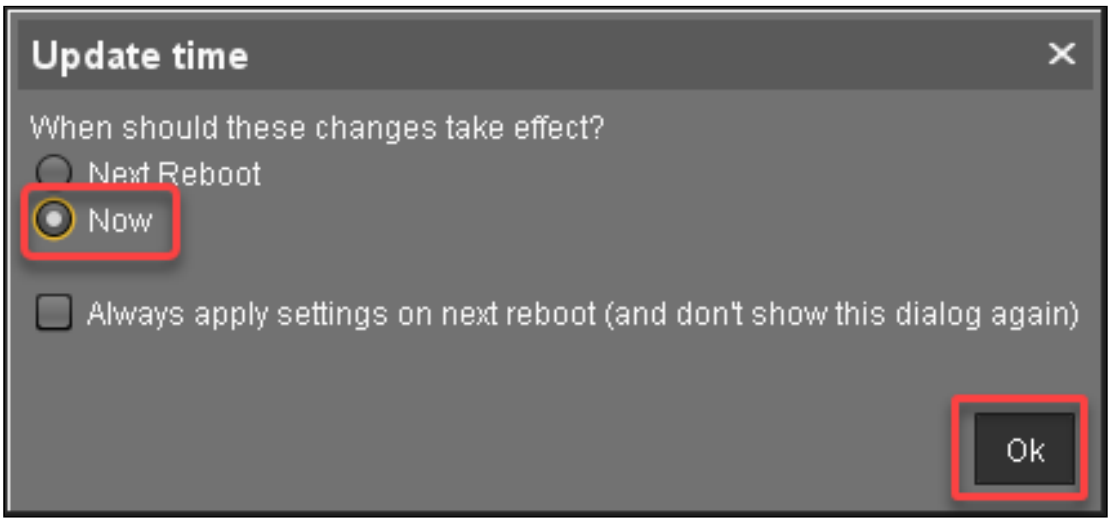
Assigning the Profile and Testing the Application

Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

1. In the UMS structure tree, drag and drop the icon of your profile onto the icon of a device.



   The **Update time** dialog opens.
2. Select **Now** and click **Ok**.



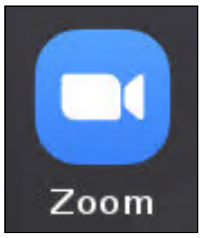
The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition, and uncompresses them.

Update Can Be Canceled After Timeout

An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

On the desktop of the endpoint device, the Zoom icon should appear:



3. Click on the Zoom icon to test the Zoom application.

Using a Custom PKCS#11 Library

Issue

You want to use your own PKCS#11 library.

Problem

In the Setup, you cannot find how to activate a custom PKCS#11 library.

Solution

> In case of the installation of a custom PKCS#11 library, the file(s) must be placed on the endpoint device either via *Universal Management Suite > Universal Management Suite (UMS) > UMS Articles > IGEL UMS Communication Ports > UMS and Devices: File Transfer* or Custom Partition Tutorial (see page 852).
> The use of the `/wfs` folder is NOT recommended because of its space limit.

Using with Kerberos and/or Citrix StoreFront Logon

To use a custom PKCS#11 library with Kerberos and/or Citrix StoreFront Logon:

- In Setup, go to **Security > Smartcard > Middleware**.
- Select **Custom PKCS#11 module**.
- Under **Path to the library**, enter the path to your PKCS#11 library. Example: `/usr/lib/pkcs11/[name of the library].so`

Using with VMware Horizon

To use a custom PKCS#11 library with VMware Horizon:

- In Setup, go to **System > Registry**.
- Enable the registry key `vmware.view.pkcs11.use_custom`.
- Set the registry key `vmware.view.pkcs11.custom_path` to the path to your PKCS#11 library. Example: `/usr/lib/pkcs11/[name of the library].so`

Using with Firefox Browser

To use a custom PKCS#11 library with the Firefox browser:

- In Setup, go to **System > Registry**.
- Enable the registry key `browserglobal.security_device.custom.enable`.
- Set the registry key `browserglobal.security_device.custom.device_name` to the name of your PKCS#11 library.

- Set the registry key `browserglobal.security_device.custom.lib_path` to the path to your PKCS#11 library. Example: `/usr/lib/pkcs11/[name of the library].so`

Using with Chromium Browser

To use a custom PKCS#11 library with the Chromium browser:

- In Setup, go to **Sessions > Chromium Browser > Chromium Browser Global > Smartcard middleware**.
- Enable **Use a custom security device**.
- Under **Name of the security device**, enter an arbitrary name for the library.
- Under **Path to the library**, enter the path to your PKCS#11 library. Example: `/usr/lib/pkcs11/[name of the library].so`

Adding an Icon for Browsing Removable Storage

Symptom

There is no obvious way of viewing files from removable media locally on the thin client.

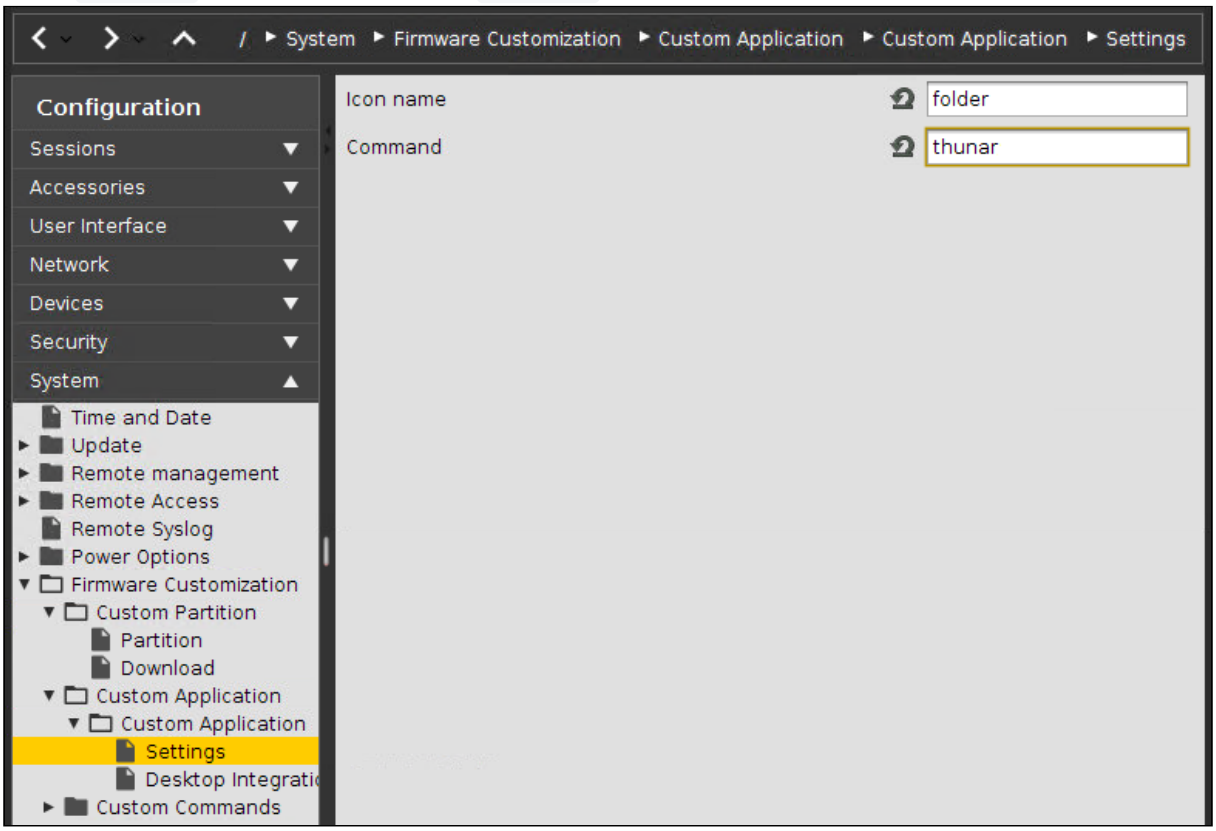
Problem

You want to view files from removable media locally on the thin client.

Solution

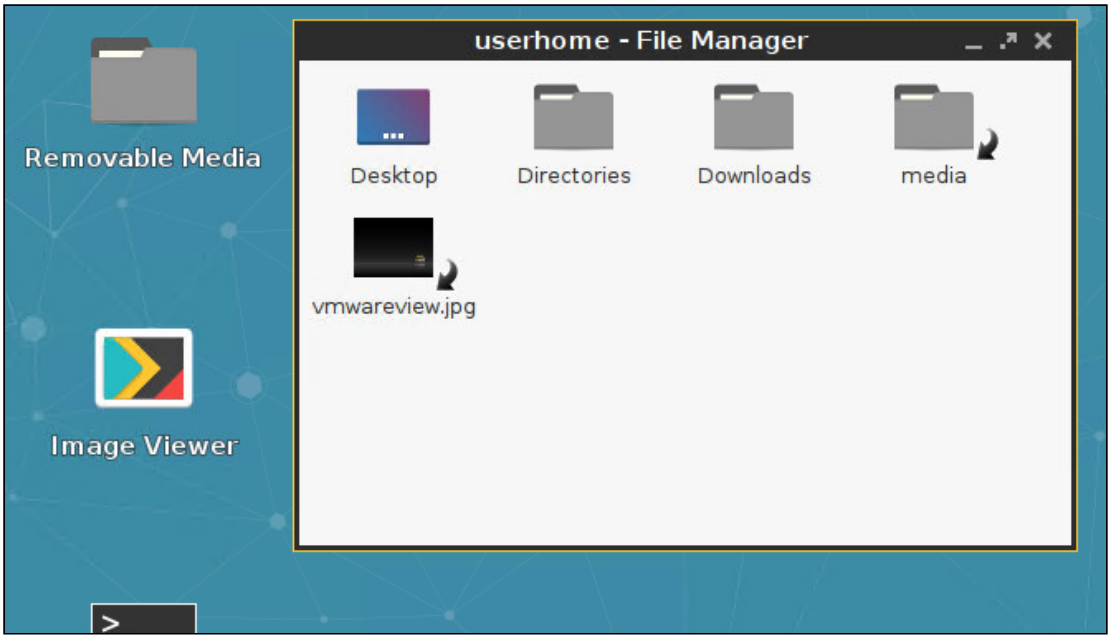
Create a custom application that opens the contents of removable media in the **File Manager**.

1. Go to **System > Firmware Customization > Custom Application** in **Setup**.
2. Click the star symbol to create a new **Custom Application**.
3. Enter a name, e.g. *Removable Media*, and choose desktop integration options for the application.
4. Enter `folder` as the **Icon name** and `thunar` as the **Command** in the **Settings** dialog:



5. Save the settings.

6. Insert a removable medium such as a USB stick into the thin client.



7. Click the new **Removable Media** icon. This opens **File Manager** and lets you browse the contents. Clicking a file will open it in the application configured by the MIME type handler (as of IGEL LINUX 5.06.100, Adding or Changing a MIME Type Handler (see page 975)).

Adding an Icon for the Image Viewer

Symptom

You want to view images locally on the thin client.

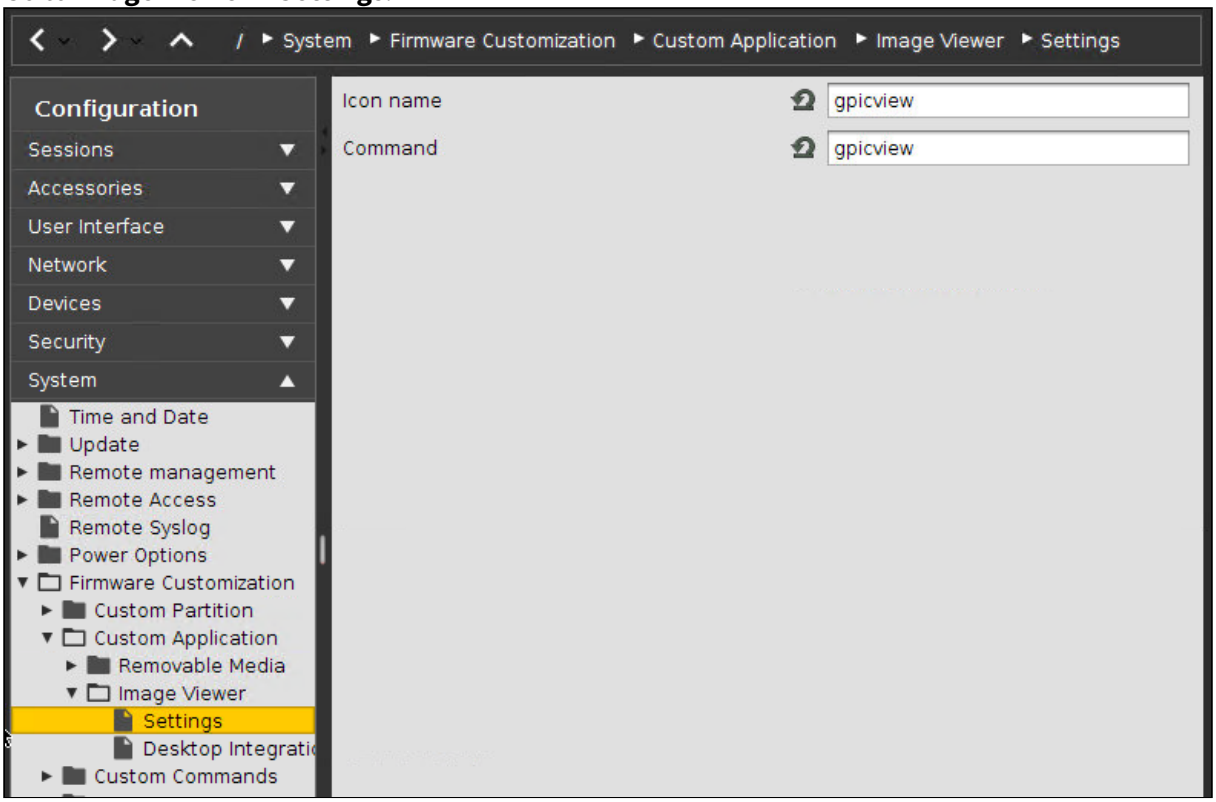
Problem

The image viewer contained in *IGEL Linux* as from version 5.06.100 on has no desktop icon or menu entry.

Solution

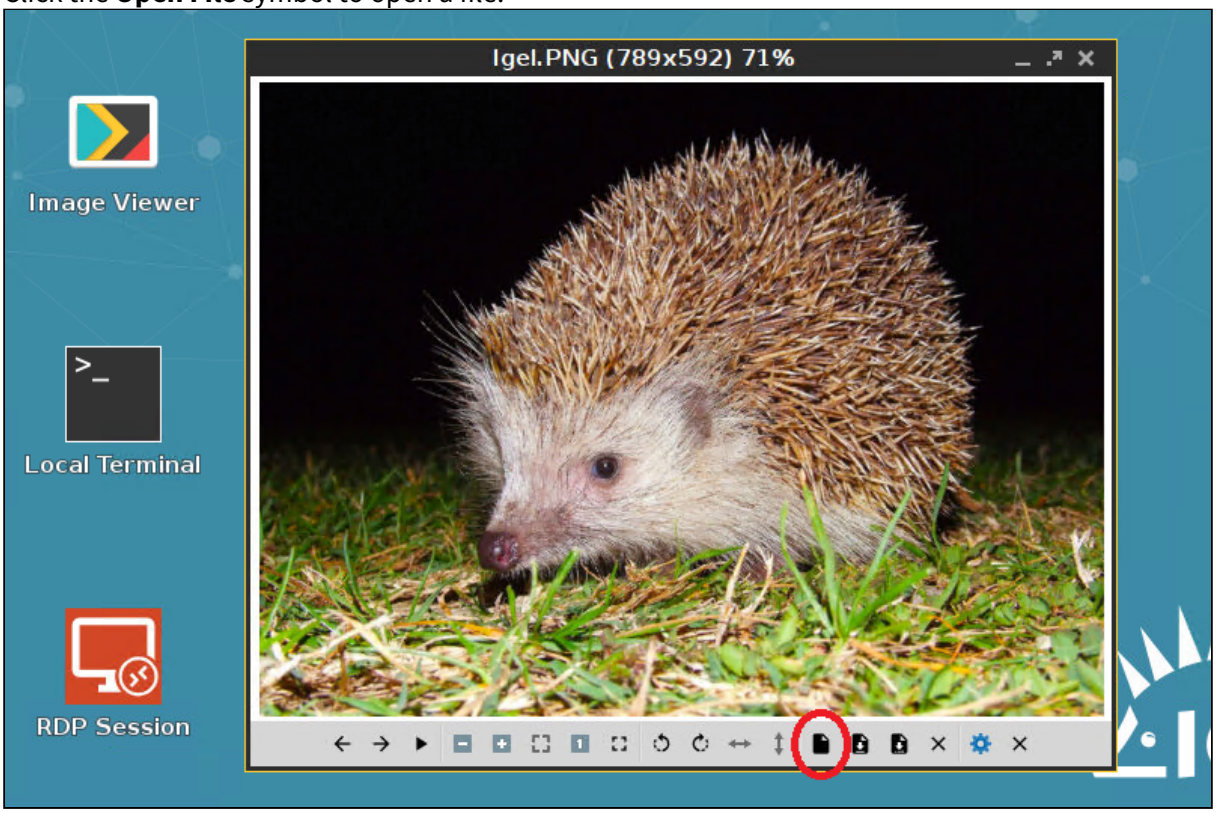
Create a custom application that opens the Image Viewer.

1. Go to **System > Firmware Customization > Custom Application** in Setup.
2. Click + to create a new **Custom Application**.
3. Enter a name, e.g. *Image Viewer*, and choose desktop integration options for the application.
4. Go to **Image Viewer > Settings**:



5. Enter `gpicview` as both the **Icon name** and the **Command** in the **Settings** dialog.
6. Save the settings.

7. Click the newly created icon for **Image Viewer**.
8. The **Image Viewer** opens.
9. Click the **Open File** symbol to open a file.



Creating a Timed Command (Cron Replacement)

You can define one or more commands which are executed at a defined time. The configuration is similar to that of a `cron` job. The implementation in IGEL OS uses `systemd` to execute the command.

To define a timed command:

1. In the Setup, go to **System > Registry > system > cron > cronjob%**
2. Activate **enable_cron**.
3. If you want to define paths to executables in addition to the existing path environment variable, add them under **path**, separated by ":".
4. Click **Add Instance**.
   The instance "cronjob1" is created, which will be renamed to "cronjob0" when the device has restarted.
5. Set the parameters for your timed command according to your needs:
   - **command**: Command to be executed. Example for testing purposes: `gtkmessage -m "Here is your cron replacement"`
   - **day_of_month**: Day of the month
     Possible values:
     - "1" ... "31": The command is executed on the defined day. To select a list of days for execution, enter a comma-separated list, e.g. "1,8". To enter a range of days, use a hyphen, e.g. "1-3".
     - "*": The command is executed every day of the month.
   - **day_of_week**: Day of a week
     Possible values;
     - "1" ... "7": The command is executed on the defined day. "0" and "7" both mean Sunday. To select a list of days for execution, enter a comma-separated list, e.g. "1,3". To enter a range of days, use a hyphen, e.g. "1-3".
     - "*": The command is executed every day of the week.
   - **hour**
     Possible values:
     - "0" ... "23": The command is executed in the defined hour. Example: "15" means 3 p.m, plus the minutes defined under **minute**. To select a list of hours for execution, enter a comma-separated list, e.g. "9,17". To enter a range of hours, use a hyphen, e.g. "9-17".
     - "*": The command is executed every hour.
   - **minute**
     Possible values:
     - "0" ... "59": The command is executed in the defined minute. To select a list of minutes for execution, enter a comma-separated list, e.g. "15,45". To enter a range of minutes, use a hyphen, e.g. "5-10".
     - "*": The command is executed every minute.
   - **month**
     Possible values:
     - "1" ... "12"; The command is executed in the defined month. To select a list of months for execution, enter a comma-separated list, e.g. "1,4". To enter a range of months, use a

hyphen, e.g. "1-3".
- "*": The command is executed every month.

- **user**: The user under which the command is executed
  Possible options:
  - "root"
  - "user"
- **year**: Year in 4-digit format. Example: "2019". To select a list of years for execution, enter a comma-separated list, e.g. "2019,2020". To enter a range of years, use a hyphen, e.g. "2019-2021". If the command is to be executed each year, enter "*".

6. Click **Apply** or **Ok**.
7. Restart the device.
   After the device has restarted, the command will be executed as configured.

Customizing IGEL OS Desktop

You want to give your IGEL OS desktops a more individual look and feel. This document shows how to customize your IGEL OS desktops using the Universal Management Suite (UMS). There are two ways to do it:

- via a firmware customization;
- via a profile.

> With a firmware customization function, you can change your desktop design much easier and quicker than with a profile.
> For an example, see Creating Your Own Wallpaper via Firmware Customization (see page 944). See also Firmware Customization (see page 2068) and *Universal Management Suite > Universal Management Suite (UMS) > UMS Reference Manual > Firmware Customizations in the IGEL UMS > Create Firmware Customization* in the UMS Reference Manual.

For information on customizing IGEL OS desktops via a profile, see:

- How to Create a Custom Bootsplash for IGEL OS Devices via the UMS (see page 931)
- Assigning Your Own Company Logos (see page 936)
- Creating Your Own Screensaver (see page 938)
- Creating Your Own Wallpaper (see page 943)
- Creating Your Own Taskbar (see page 947)
- Customizing Desktop Icons (see page 948)
- Introduction (see page 950)

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=qFQttefMlX8

How to Create a Custom Bootsplash for IGEL OS Devices via the UMS

This document shows how you can create a custom bootsplash for your endpoint devices using the Universal Management Suite (UMS). There are two ways to do it:

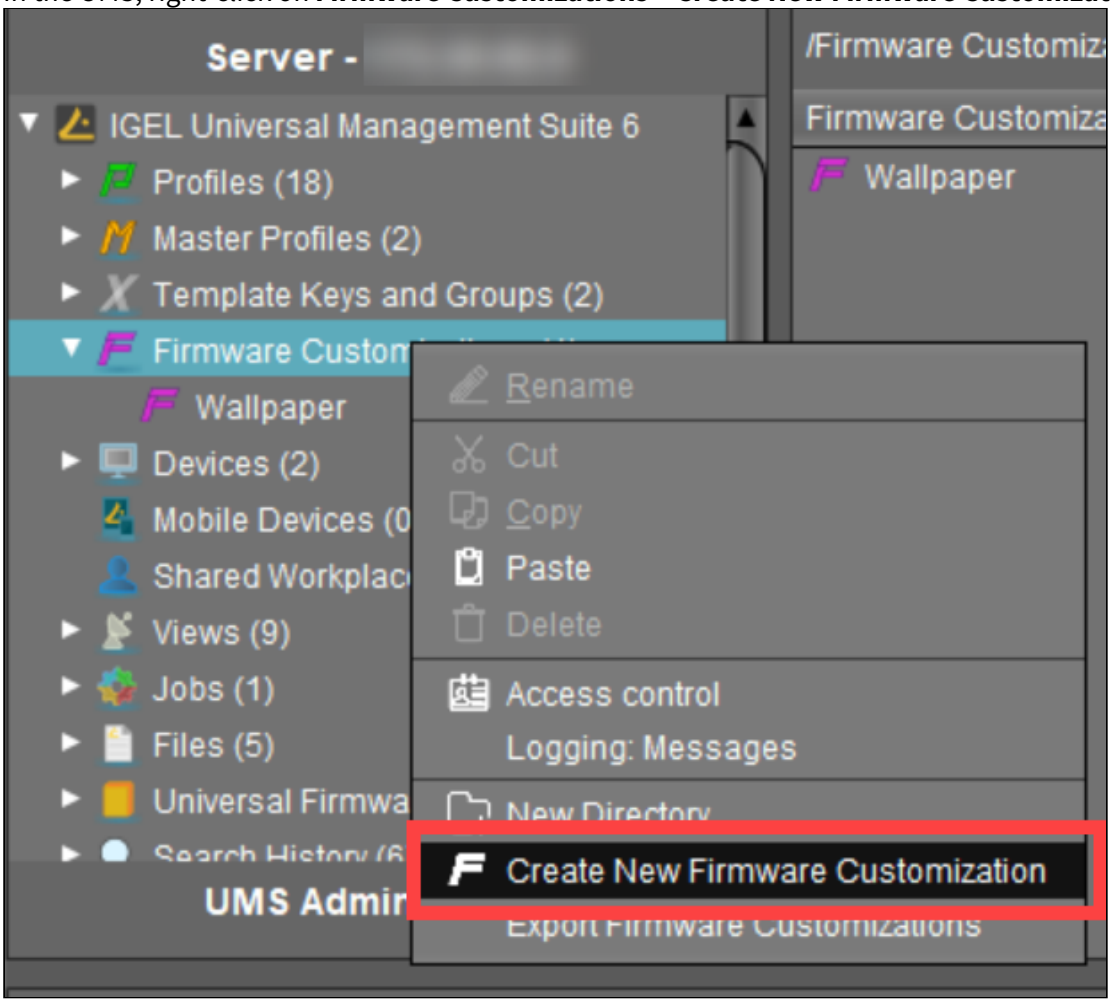
- via a firmware customization (recommended as it is easier and quicker)
- via a profile

> ⚠ If the image file or any setting of an existing custom bootsplash is changed, the bootsplash code has to be rebuilt. You can trigger this from the UMS via **Jobs > New Scheduled Job** with the command **Update desktop customization** or via **Devices > [context menu] > Other commands > Update desktop customization**.

How to Create a Custom Bootsplash via a Firmware Customization

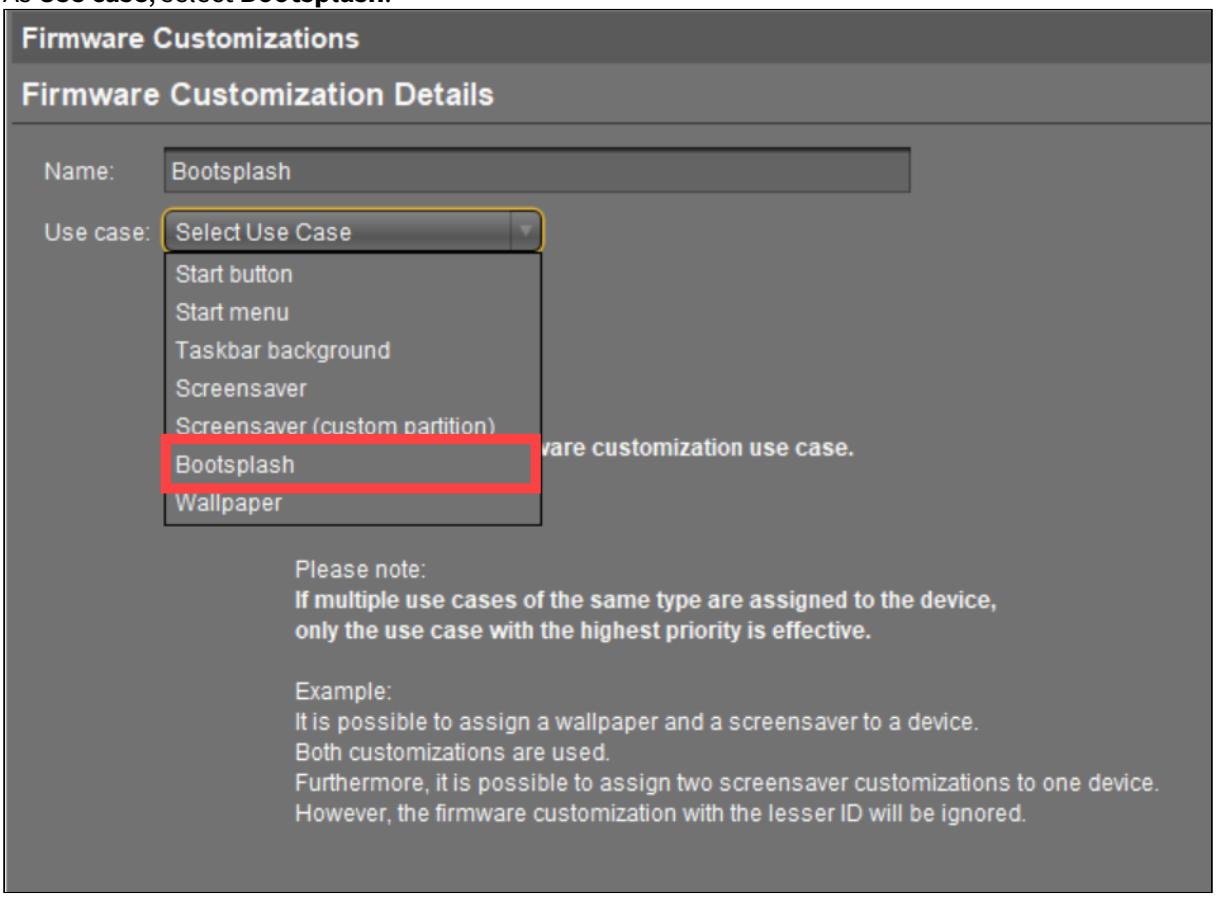
This is how you can create your own bootsplash using a firmware customization function in the UMS:

1. In the UMS, right-click on **Firmware Customizations > Create New Firmware Customization**.



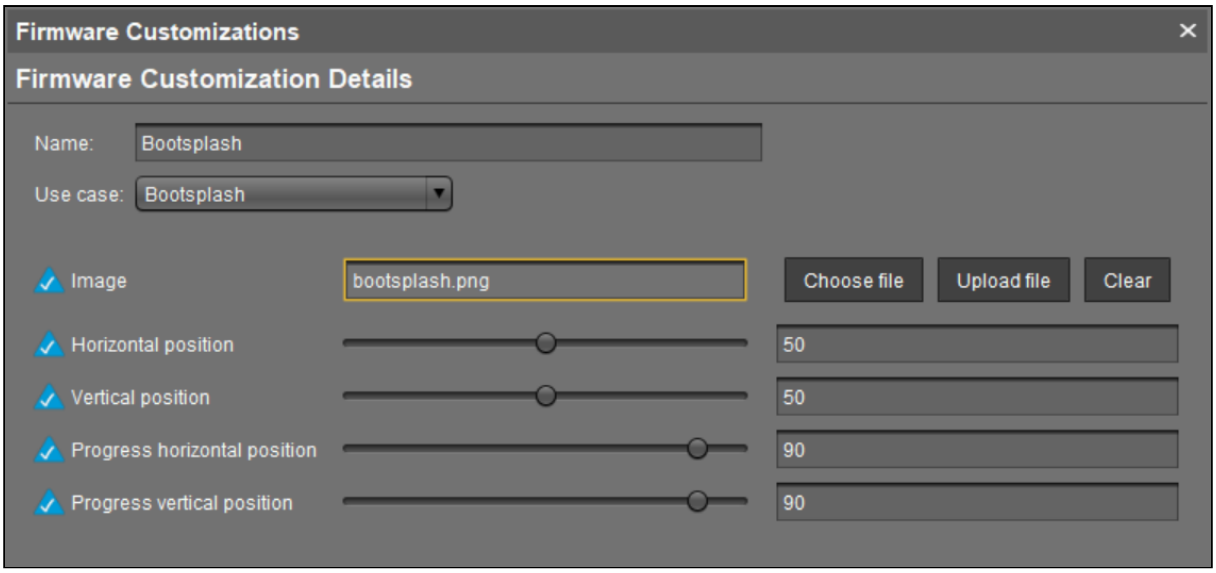
The **Firmware Customization Details** dialog opens.

2. Enter a **Name** for your bootsplash customization.
3. As **Use case**, select **Bootsplash**.



4. Select the image file for your bootsplash:
   - Click **Choose file** if you have already uploaded a file to the UMS Server.
   - Click **Upload file** if you want to upload a new file.

- The file name must not contain any blank spaces or special characters such as %, §, umlauts, etc.
- The following file types are supported: JPG, JPEG, BMP, and PNG.
- The optimum size of the picture is 800 x 600 pixels.



5. Define the position of your bootsplash.
6. Click **Next** to assign this new firmware customization to a device or a device directory.
   Or assign it later per drag & drop or via **Assigned objects**.
7. Click **Finish** to save your new firmware customization.

How to Create a Custom Bootsplash via a Profile

This is how you can create your own bootsplash using a profile in the UMS:

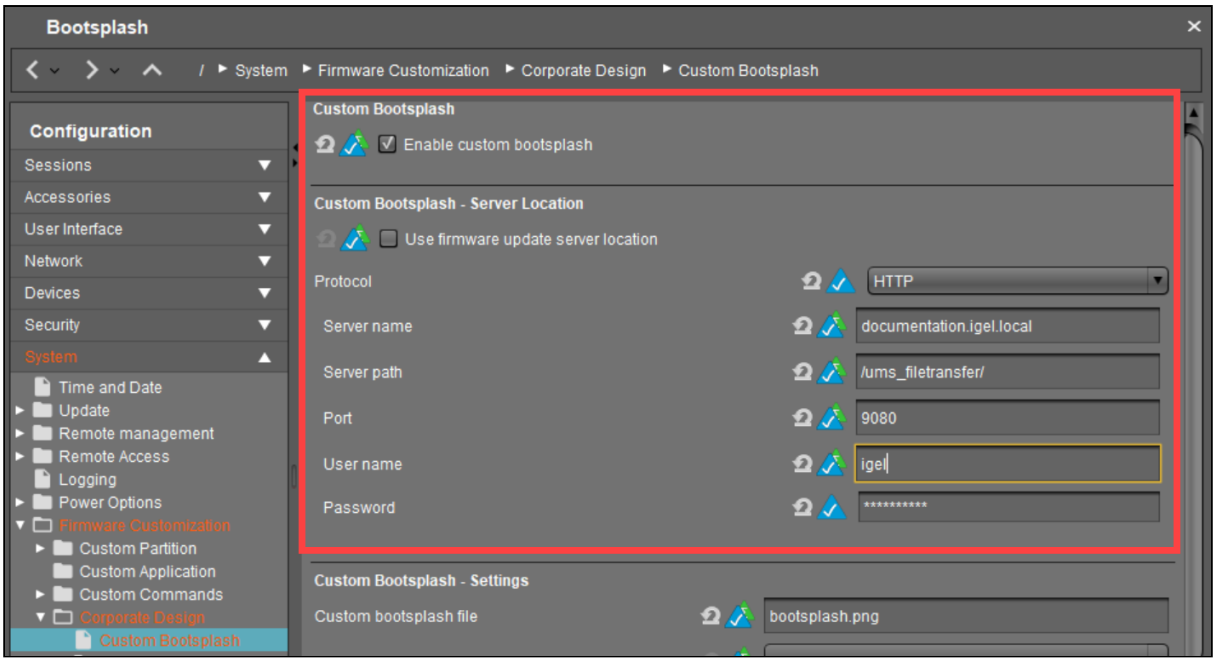
1. Upload your bootsplash image to the UMS Server; see Uploading a Picture (see page 951).

   - The file name must not contain any blank spaces or special characters such as %, §, umlauts, etc.
   - The following file types can be used: JPG, JPEG, BMP, PNG, SVG, GIF, and TIFF.
   - The optimum size of the picture is 800 x 600 pixels.

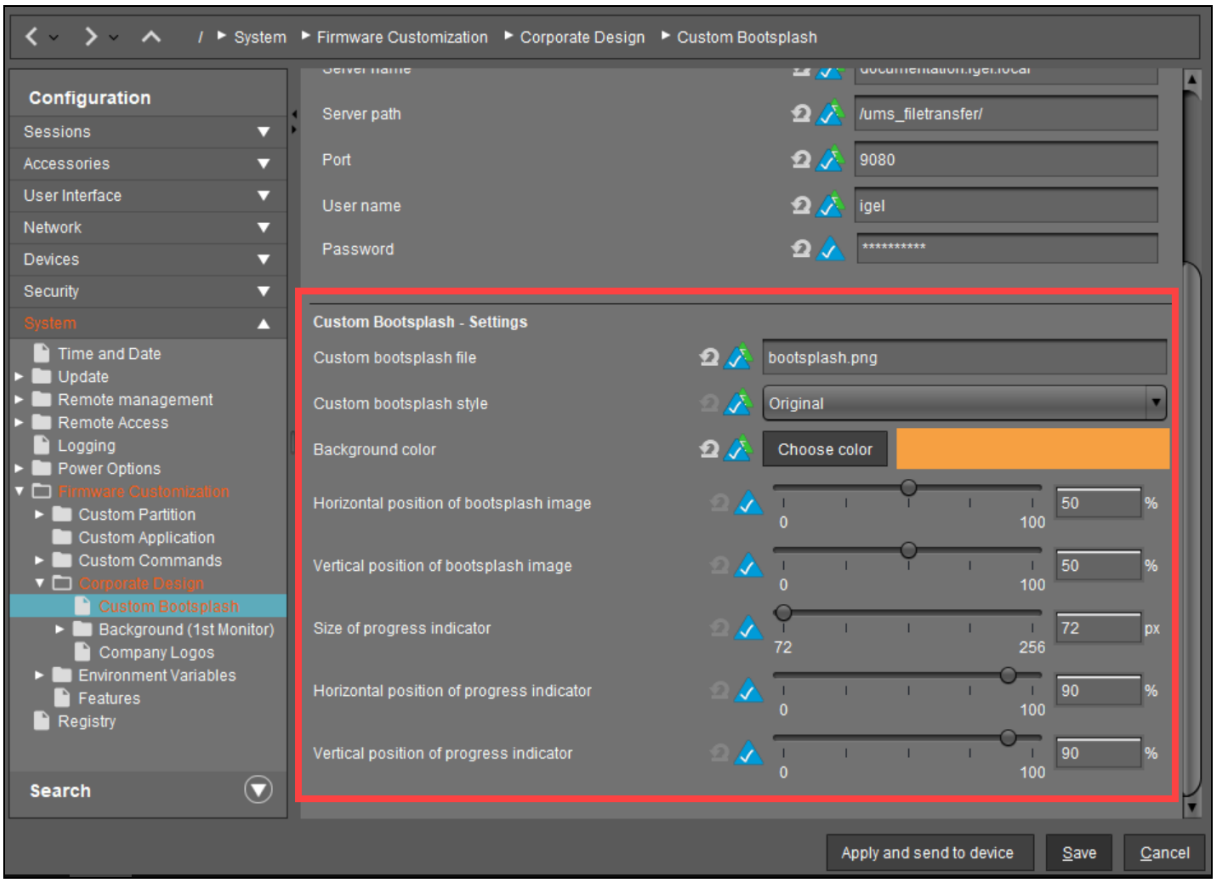
2. Create a new profile named **Bootsplash**; see Creating a Profile (see page 952).
3. In the profile configuration window, go to **System > Firmware Customization > Corporate Design > Custom Bootsplash** to create your own bootsplash.
4. Activate **Enable custom bootsplash**.
5. Choose **HTTP** as **Protocol**.
6. Under **Server name**, enter the name or the IP address of your UMS Server.
7. Enter the path of your boot logo directory as **Server path**.
8. Specify your HTTP server port under **Port**.

The default UMS HTTP server port is 9080. For more information on UMS ports, see *Universal Management Suite > Universal Management Suite (UMS) > IGEL UMS Communication Ports.*

9. Enter your UMS administrator **User name** and **Password**.



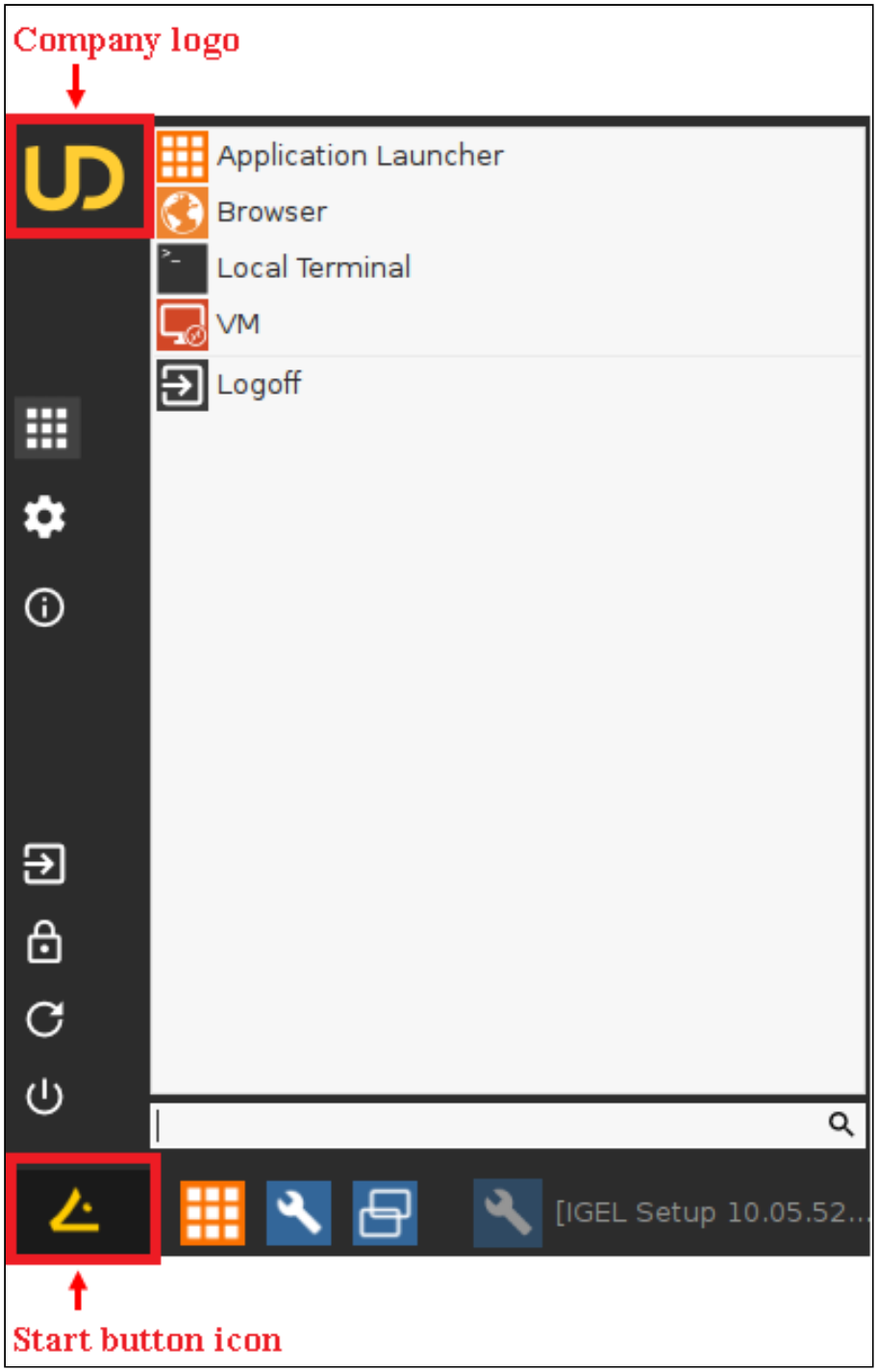
10. Enter the name of your bootsplash image under **Custom bootsplash file**.
11. Define **Custom bootsplash style** and **Background color**.
12. Define **vertical** and **horizontal position** for the bootsplash image and progress indicator. The scale goes from 0 (left) to 100 (right); 50 means "centered".



13. **Save** the settings.
14. Assign your bootsplash image to the created profile.
15. Assign the profile to your devices per drag & drop or by adding them under **Assigned objects**. For more information on the profile assignment, see *Universal Management Suite > Universal Management Suite (UMS) > UMS Reference Manual > Profiles in the IGEL UMS > Using Profiles > How to allocate IGEL UMS Profiles*.

Assigning Your Own Company Logos

You can set your own images for the **start button** and the **company logo in the start menu**.



The **Start button icon** is customizable in IGEL Linux 5.08.100 and newer.

To see a start menu with a company logo, you first have to set the **Start Menu Type** on **Advanced** under **User Interface > Desktop > Start Menu**.
If you set the **Start Menu Type** on **Auto** and the device has a clock frequency of 1 GHz, the system will choose the advanced type.

To assign your own icons via UMS:

1. Upload your logos to the UMS server. For details, see Uploading a Picture (see page 951).
2. Create a new profile. For details, see Creating a Profile (see page 952).
   The profile configuration window opens.
3. Go to **System > Firmware Customization > Corporate Design > Company Logos > Start Menu.**
4. Enter the file name and the full path of the image under **Start button icon**.
5. Enter the file name and the full path of the image under **Company logo in start menu**.
6. Click **Save** or **Apply and send to Thin Client** to save the settings.
7. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

An alternative to this is the chapter *Universal Management Suite > Universal Management Suite (UMS) > UMS Reference Manual > Firmware Customizations > Create Firmware Customization* in the UMS manual. Here you will find further configuration options for adapting the UMS to your requirements.

Creating Your Own Screensaver

This section describes how to configure an autostart screensaver with your own picture using the UMS.

Proceed as you did for the wallpaper:

1. Upload your logo to the UMS server. For details, see Uploading a Picture (see page 951).

   > The size of the picture is irrelevant because it will be reduced automatically to 200 x 150 pixels.

2. Create a new Profile named **Screensaver**. For details, see Creating a Profile (see page 952).
3. Configure the profile settings.
   There are four areas where you have to make settings in the screensaver profile:

   - Setting a Delay Time for Booting (see page 939)
   - Setting a Timeout for Autostart (see page 940)
   - Assigning the Custom Logo (see page 941)
   - Assigning the Custom Clock (see page 942)

4. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

Setting a Delay Time for Booting

Configure **Autostart** in the screensaver profile under **User Interface > Screenlock / Screensaver**.

1. Enter a **Session name**, for example **Screensaver**.
2. Enable **Autostart**.
3. Enter the number of seconds of **Delay**.

> This setting tells the system that it must launch the autostart of this session with a certain delay during booting.

Setting a Timeout for Autostart

1. Click **User Interface > Screenlock / Screensaver > Options**.
2. Enable **Start automatically**.
3. Enter a number of minutes for **Timeout**.

> With this setting, you decide how long the system has to wait before starting the screensaver after the last input.

Assigning the Custom Logo

1. Go to **System > Firmware Customization > Corporate Design > Company Logos**.
2. Activate **Enable image display**.
3. Enter the **Image file/directory** you have defined under **Thin Client file location**. See Uploading a Picture (see page 951).

   > If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **display time** for the images can be configured.

4. Activate **One image per monitor** if you use more than one monitor and if you want to show different pictures on each screen.
5. Under **Image duration** specify the time in seconds that you want to wait before the image is to be changed.
6. Under **Image display mode** you can choose between the following different image actions:
   - **Small-sized hopping**: Small pictures are shown in changing positions.
   - **Medium-sized hopping**: Bigger pictures are shown in changing positions.
   - **Full-screen center cut out**: The pictures will be shown in full-screen mode. They may possibly be cut at the border.
   - **Full-screen letterbox**: The pictures are shown in full size as large as possible according to the screen.

Assigning the Custom Clock

You can also configure a digital screensaver clock independently of the screen display.

1. Click **User Interface > Screenlock / Screensaver > Screensaver**.
2. Select the **Clock display monitor** where you want to display the clock.
3. Activate **Show seconds** if you want to see the digital time display, including seconds.
4. Define the **size**, **position** and **color** settings of your screensaver clock.

Creating Your Own Wallpaper

There are two ways how to create an own wallpaper:

- Via a Firmware Customization (see page 944)
- Via a Profile (see page 945)

With a Firmware Customization, setting up your own wallpaper is much easier than with a profile.

Creating Your Own Wallpaper via Firmware Customization

This is how you can create your own wallpaper using a firmware customization function in the UMS:

1. In the UMS, right-click on **Firmware Customizations > Create New Firmware Customization**. The **Firmware Customization Details** dialog opens.
2. Enter a **Name** for your wallpaper customization.
3. As **Use Case**, select **Wallpaper**.
4. Select the image file for each monitor:
   - Click **Choose file** if you have already uploaded a file in the UMS.
   - Click **Upload file** if you want to upload a new file.

   > The file name must not contain any special characters such as %, §, umlauts, etc.

5. Select your image file and click **Open**.
6. Check the image file location and click **OK**.
7. Optionally, click **Next** to directly apply this new firmware customization to a device or folder of devices.
8. Click **Finish** to save your new firmware customization.

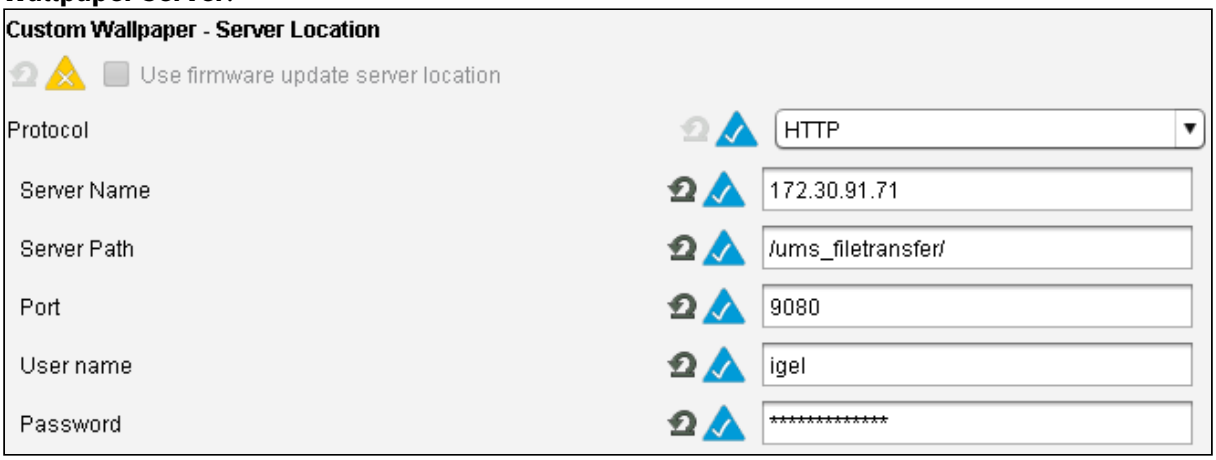
Creating Your Own Wallpaper via a Profile

You have already uploaded your wallpaper picture; see Uploading a Picture (see page 951).

1. Create a profile and name it, for example, **Wallpaper**; see Creating a Profile (see page 952).
   The **Profile Configuration** window opens.
2. Set the wallpaper server location; see below "Setting the Wallpaper Server Location".
3. Configure the background of the client desktop; see below "Configuring the Background".

Setting the Wallpaper Server Location

1. Click **System > Firmware Customization > Corporate Design > Background > Custom Wallpaper Server**.



2. Choose **HTTP** as **Protocol**.
3. Enter the **Server name** of your UMS Server.
4. Enter the path of your wallpaper directory as **Server path**.
5. The standard **Port** should be 9080.
6. Set your UMS administrator **User name** and **Password**.
7. Click **Save** to save the settings.

Configuring the Background

1. Open the profile.
2. Click **System > Firmware Customization > Corporate Design > Background (1st Monitor)**.
3. Activate **Custom wallpaper download**.
4. Enter under **Custom wallpaper file** the name of the picture you want to define as your background image.

> If you use more than one monitor, you have to assign the background image to each one of them manually.

5. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

Checking the Results

1. Choose the device in the UMS structure tree under **Devices**.
2. Go to **User Interface > Desktop > Background**.
   You will see that the wallpaper has already been assigned by the profile; you cannot set it manually any more.
   Alternatively, you can shadow your thin client and you will see the new wallpaper.

This way, you can automatically assign background images to your devices. It is very easy to maintain them because the only thing you have to do if you want to choose another image is to change it in the profile.

Creating Your Own Taskbar

You can apply your own design to a taskbar. To customize the taskbar on multiple devices, use the IGEL UMS and proceed as follows:

1. Upload the desired image to the UMS server, see Uploading a Picture (see page 951).
2. Create a new profile, seeCreating a Profile (see page 952).
3. Assign the image to the profile by dragging and dropping it or by adding it under **Assigned objects**.
4. In the profile configuration window, go to **User Interface > Desktop > Taskbar Background**.
5. Select **Background image** under **Background style**.

6. Enter the full path of the desired image under **Background image path**.
7. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

Customizing Desktop Icons

> You can only customize the desktop icon of a session. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.

Prerequisites

You can use the following graphic formats and resolutions for a custom desktop icon:

- PNG - common resolutions are 128x128, 96x96, 64x64, 48x48, 32x32, 24x24, 22x22, 16x16, but others are also accepted and scaled accordingly.

> We recommend at least a resolution of 64x64.

- SVG - no resolutions because SVG contains freely scalable vector graphics.

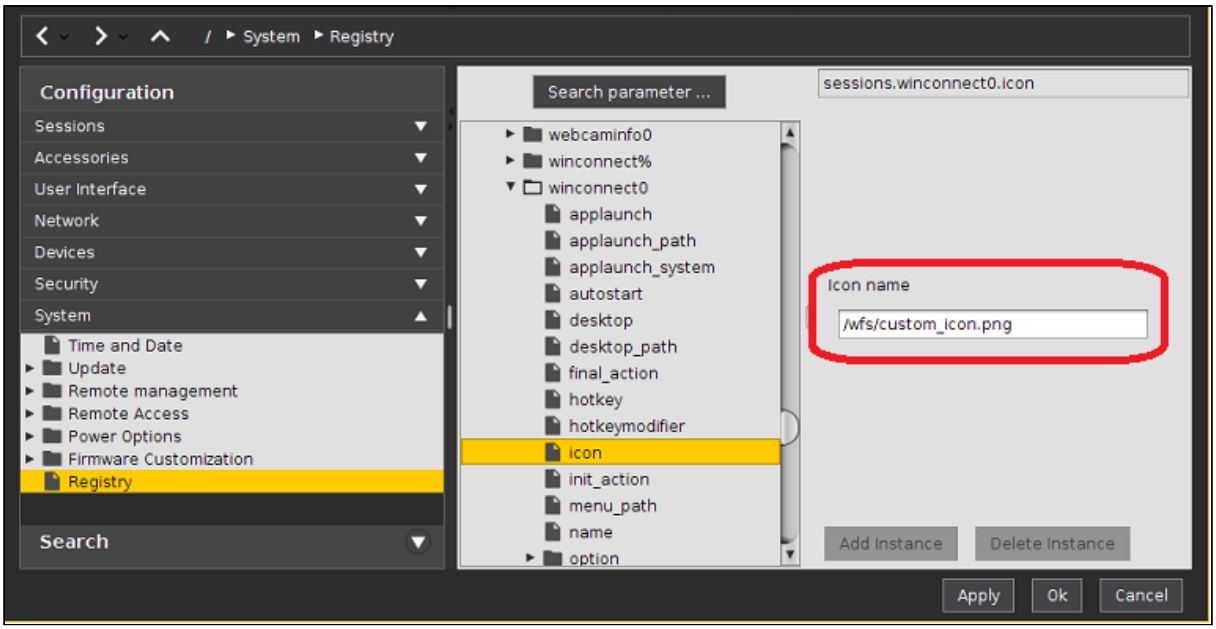
> Even though other formats like BMP or JPEG are supported, only PNG and SVG are recommended because these formats support transparency.

To customize the desktop icon of a session, proceed as follows:

1. In the Setup, go to **System > Registry**.
2. In the Registry, navigate to **sessions.[session name].icon**.

   > For technical reasons, some registry keys do not match the session's name. For example, RDP sessions are found under the key `winconnect[0-...]`.

3. Enter under **Icon name** the absolute path to your custom icon as shown in the sample picture below.



4. Click **Ok** to save the changes.

Introduction

If you want to roll out your complete corporate design changes and apply them to multiple devices, you can create one single profile for all settings.

Before defining special profiles, you must take the following steps:

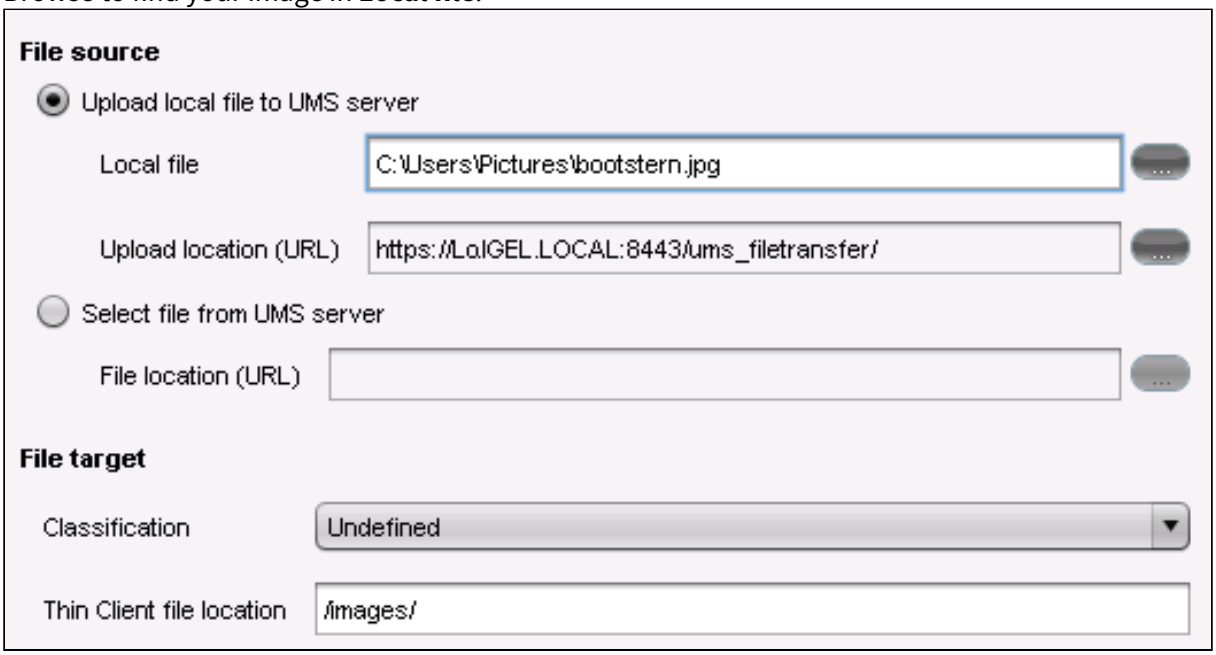
- Uploading a Picture (see page 951)
- Creating a Profile (see page 952)

Uploading a Picture

Upload your image files to the UMS server, then assign them to the relevant profile and also to your devices. You can choose between the following formats for your pictures : **BMP, JPG, GIF, TIF, PNG** and **SVG**. Ensure that the name of your image file has no blanks, otherwise the file will not be accepted. **25 MB** of free storage space are available for your pictures.

Upload your files:

1. Click **New file** on the context menu of the **Files** directory in the tree.
2. Browse to find your image in **Local file**.



3. Browse to select a picture directory in **Upload location (URL)**.
   Since UMS version 5 you can use as upload location only /ums-filetransfer/ and its subdirectories.
4. Enter a **Thin Client file location** directory for the target device.
   If you enter a directory which does not yet exist, it will be created automatically. If you do not enter a specific directory, the image will be put in the root directory.
5. Click **OK**.
   Your image will be listed in the list of **Files**.
6. Assign the image to your devices by dragging and dropping them or by adding them under **Assigned objects**.

> If you put more than one image in the **Thin Client file location** directory, all images will be alternately shown by the screensaver (see page 938), one after the other.

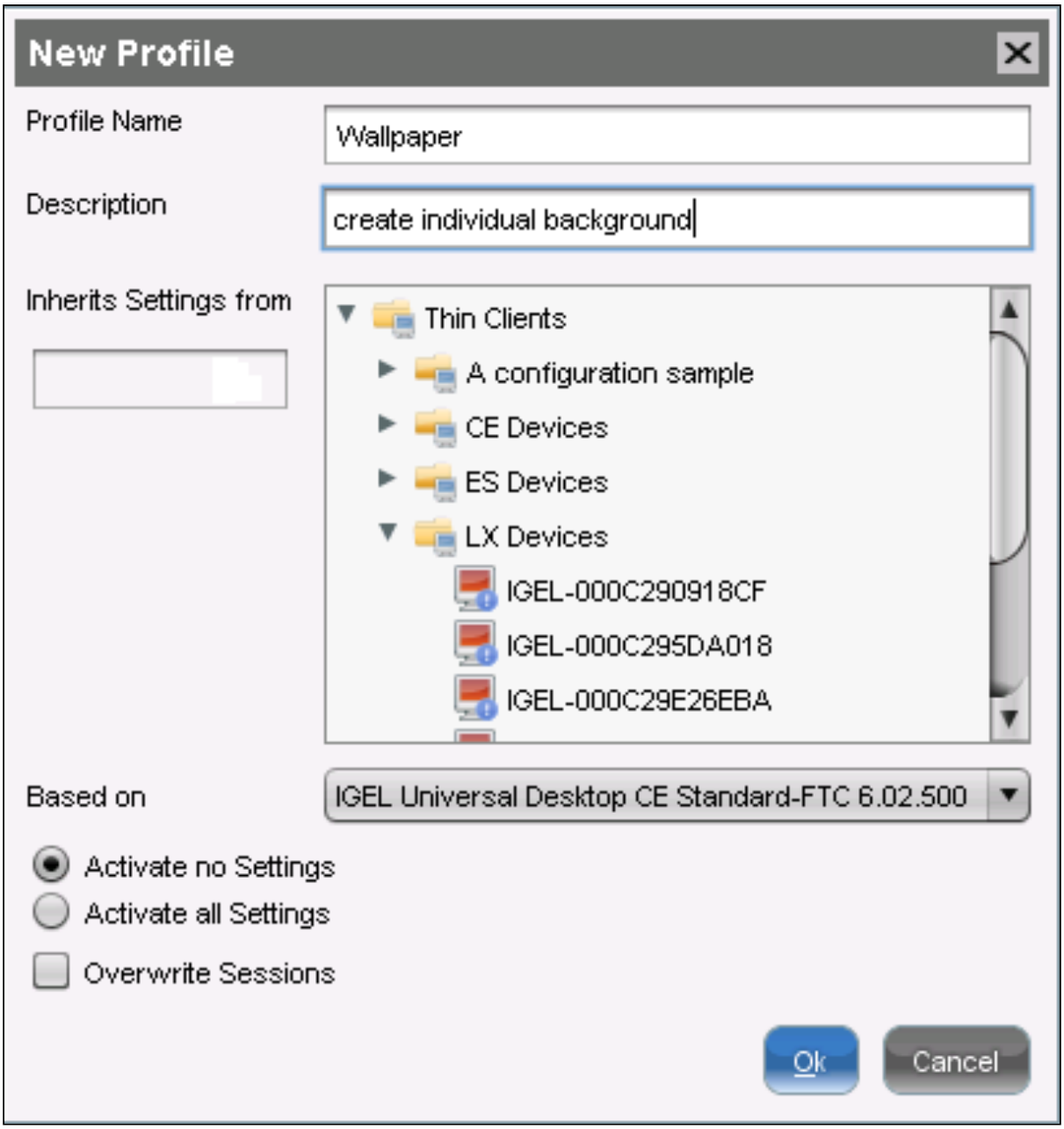
Creating a Profile

You have already Uploading a Picture (see page 951).

As you work with the UMS, to manage several clients, you need to create a profile to assign the new settings to your clients.

Create a **Profile** to assign your settings to the clients:

1. Click **New profile** in the context menu of the **Profiles** directory in the tree.
2. Enter a **Profile Name**.
3. Enter a **Description** and choose the firmware of your thin client under **Based on**.


New Profile
Profile Name
Wallpaper
Description
create individual background
Inherits Settings from
Thin Clients
A configuration sample
CE Devices
ES Devices
LX Devices
IGEL-000C290918CF
IGEL-000C295DA018
IGEL-000C29E26EBA
Based on
IGEL Universal Desktop CE Standard-FTC 6.02.500
Activate no Settings
Activate all Settings
Overwrite Sessions
Ok
Cancel

4. Click **OK**.

How to Change the Font Color of the Desktop Icons

Overview

You want to alter the font color of the desktop icons.

Environment

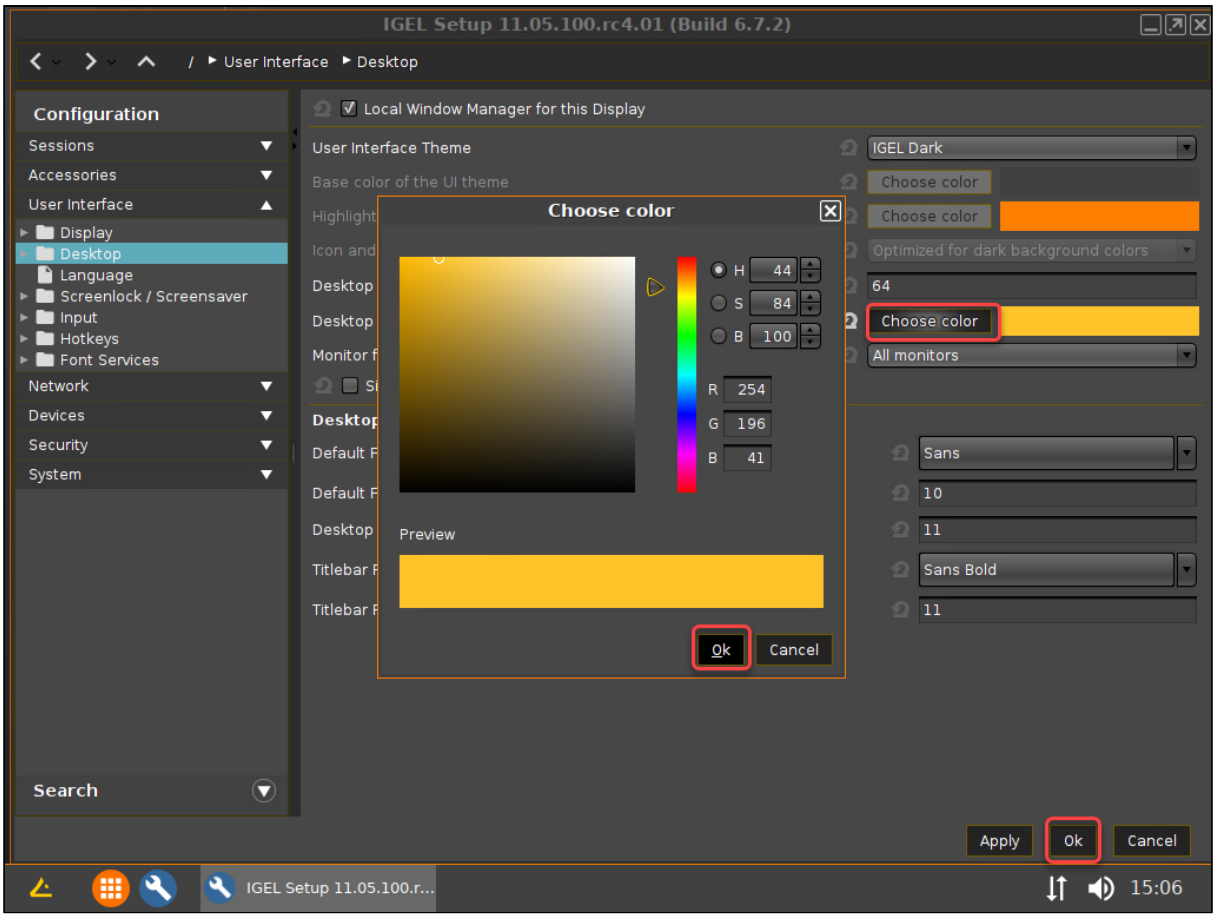
- IGEL OS 11.05.100 or higher

Instructions

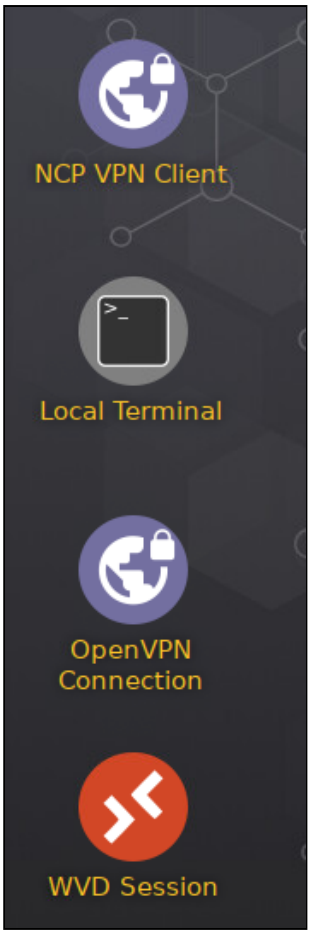
1. In the Setup, go to **User Interface > Desktop**.

   > As an alternative, you can enter the hexadecimal RGB hex value in **System > Registry > windowmanager > defaulttheme > desktop_iconfont_color** (registry key: `windowmanager.defaulttheme.desktop_iconfont_color`). Example: `#FEC429`

2. Beside **Desktop icon font color**, click **Choose color** and select the desired color using the color picker. Confirm your change with **Ok**.



The font color of the desktop icons is changed.


NCP VPN Client
Local Terminal
OpenVPN Connection
WVD Session

How to Set Up a Countdown to Prevent an Undesired Screen Lock In IGEL OS

In some situations, a screen lock that comes without a warning can cause disruption. Typically, this is the case when a user who is logged in to a remote session does not interact with the device for some time, which results in the screen lock kicking in. To circumvent this problem, you can set a visible countdown that is started before the screen is locked, so the user can react in time.

> Review the timeouts in the power settings of your device to ensure that the display won't turn black before the countdown is started; see System Power Options in IGEL OS (see page 2063) and Screen (see page 2066).

The configuration is described in the following sections:

- **Defining the Countdown's Behavior**
- **Defining the Countdown's Appearance**

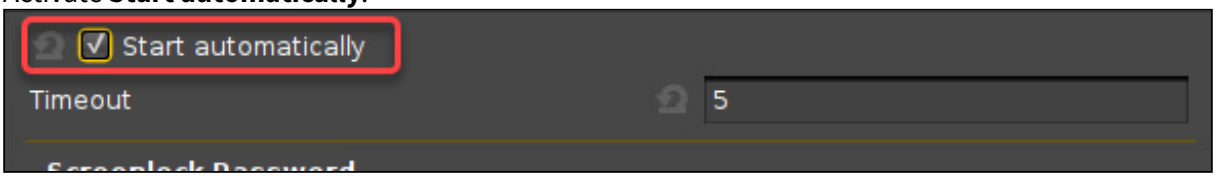
For special purposes, like closing a remote session to prevent it from running unattended, you can configure an additional set of commands. It consists of a command that determines whether the countdown should be started (typically, check whether the remote session is running) and a command that will be executed when the countdown reaches 0 (typically, close the remote session). The configuration is described in the following section:

- Configuring a Conditional Countdown and Command (see page 961)

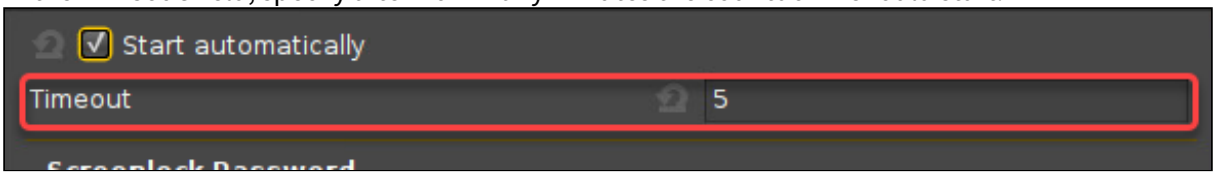
Defining the Countdown's Behavior

For a description of all options, see Options 20 (see page 1849).

1. In the Setup or UMS configuration dialog, go to **User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.



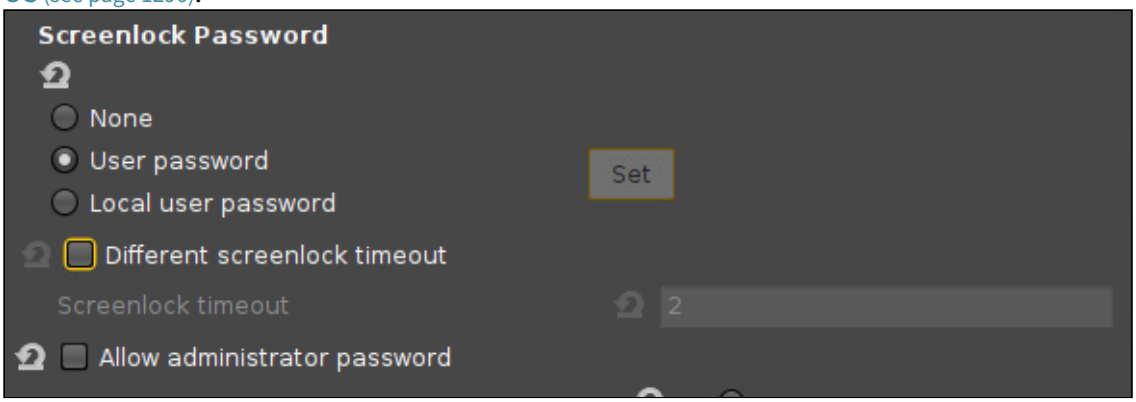
3. In the **Timeout** field, specify after how many minutes the countdown should start.



4. Select the password to be used to unlock the screen:
   - **None**: The user can unlock the screen without a password. Please note that the countdown will not be started when this option is selected!
   - **User password**: The user must enter the user password to unlock the screen. If you are using Microsoft Active Directory (AD) resp. Kerberos for authentication, which is highly recommended, the user's AD/Kerberos password will be used here. For details, see Active

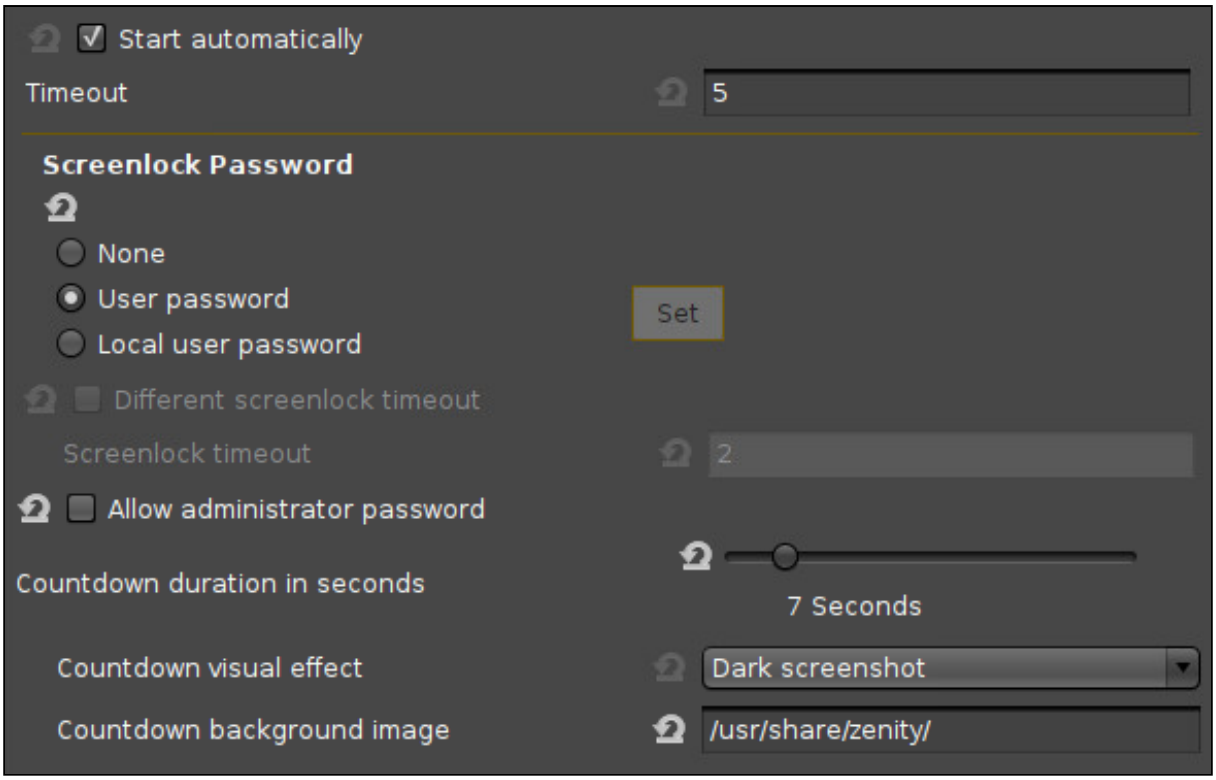
Directory/Kerberos 1 (see page 2014). If you are not using AD/Kerberos, the user password is configured in **Security > Password** under **User**. Please note that the password should not, at any rate, be set via a UMS profile, otherwise all affected devices would have the same password!

- **Local user password**: The user must enter a special screen lock password to unlock the screen; click **Set** to define this password. Please note that the password should not, at any rate, be set via a UMS profile, otherwise all affected devices would have the same password! This password is also used for **Security > Logon > Local User > Login with local user password**; see Local User (see page 2039).
  If the user is logged in via Active Directory (AD[107]), the AD credentials are used instead of this password to unlock the screen.
  If you are using Citrix Storefront, this password can be synchronized with the Citrix session password by enabling **Synchronize Citrix password with screen lock** under **Sessions > Citrix > Citrix StoreFront > Login**; see also Login Settings for Citrix StoreFront in IGEL OS (see page 1296).



5. Set the **Countdown duration in seconds**. The range is from 1 to 60.
   Configuration example:

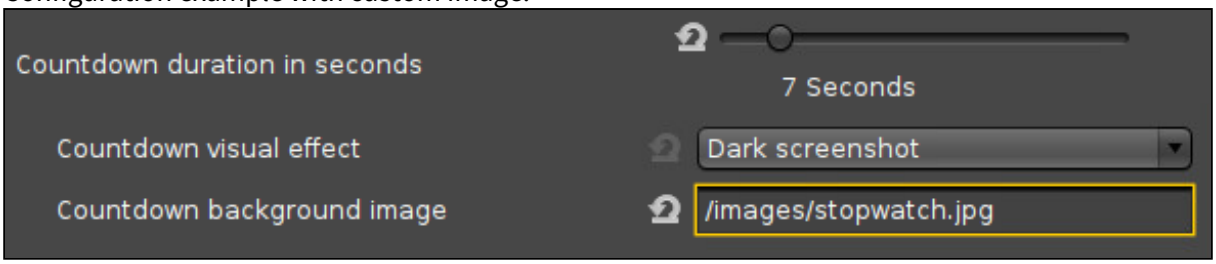
107. https://kb.igel.com/en/igel-os/11.10/active-directory-kerberos



6. Apply the settings to your devices or to your profile.

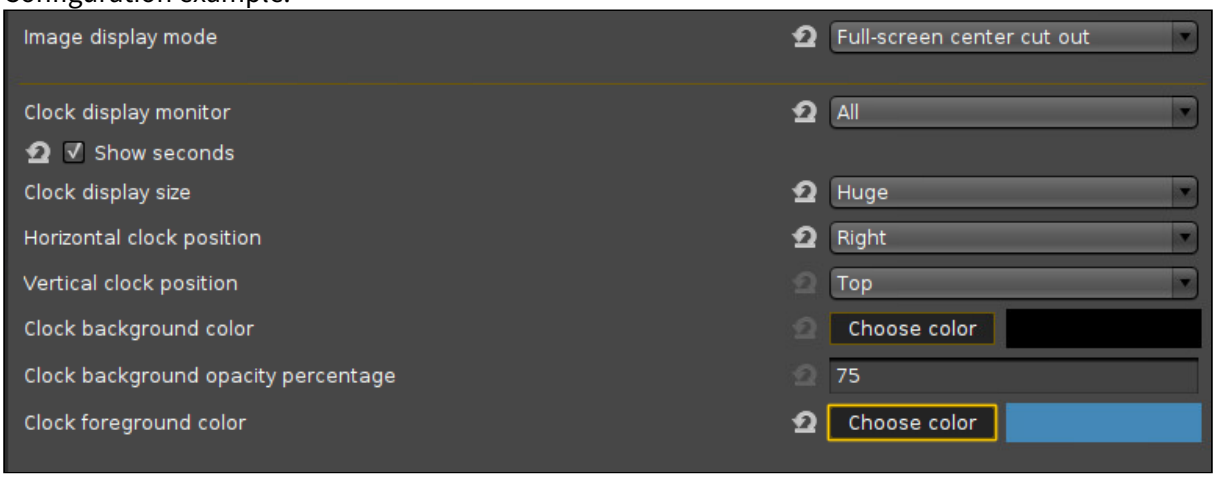
Defining the Countdown's Appearance

1. In the Setup, go to **User Interface > Screenlock / Screensaver > Options**.
2. If you want the current desktop as a background image during the countdown, select the visual effect:
   - **Dark screenshot**: The desktop screenshot is darkened.
   - **Gray screenshot**: The desktop screenshot is grayed out.
3. If you want a custom image as a background image during the countdown, enter a valid path and file name. Example: `/images/`. If the image is not already residing on your device, you can upload it using the UMS; see Uploading a Picture (see page 951).
   Configuration example with custom image:



4. Go to **User Interface > Screenlock / Screensaver > Screensaver**.
5. Customize the countdown's appearance using the following parameters; these parameters define the appearance of both the screensaver's clock and the countdown. For further information, see Screensaver (see page 1852).
   - **Image display mode**: Position and scaling for the background image
   - **Clock display monitor**: Select the monitor(s) on which the countdown is to be shown.
   - **Show seconds**: Define whether the seconds should be displayed on the clock.
   - **Clock display size**: Size of the countdown digits
   - **Horizontal clock position**: Horizontal position of the countdown digits
   - **Vertical clock position**: Vertical position of the countdown digits
   - **Clock background color**: Color of the countdown background area. The countdown background area is a rectangle with rounded corners.
   - **Clock background opacity percentage**: Set the opacity for the clock's background area (defined by **Clock background color**),
   - **Clock foreground color**: Color of the countdown digits

   Configuration example:



6. Apply the settings to your devices or to your profile.
   Here is an example of the countdown with a custom image:

Configuring a Conditional Countdown and Command

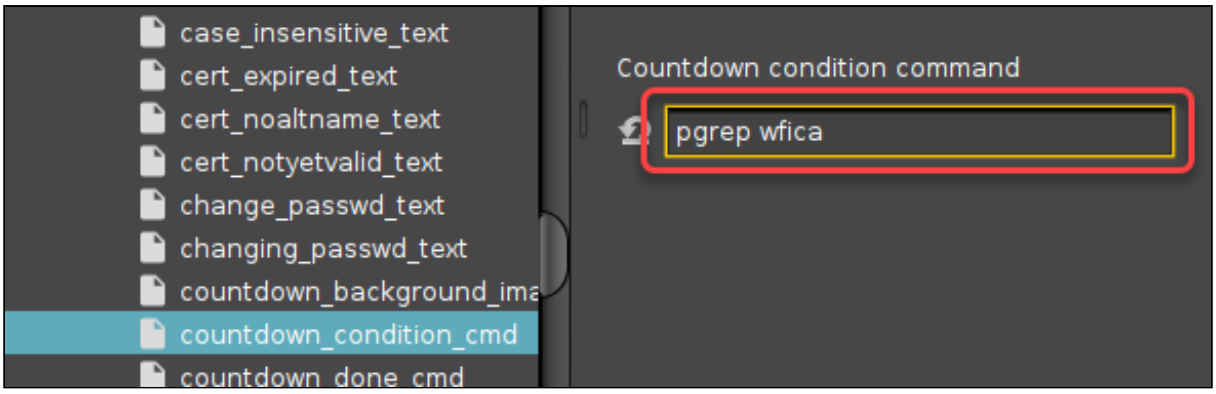
In our example, a Citrix session is running (e.g. in appliance mode), and the endpoint device has been idle for a while. After the timeout, the system checks whether a Citrix session is running; this is to prevent the session from running unattended. The Citrix session is detected, so the countdown kicks in. The user does not interact with the device, so the countdown is not stopped. When the countdown has reached 0, the system kills the Citrix client; the user is logged off.

In the following, we will first specify the command that determines whether the countdown should be started. Then, we will specify the command that is executed when the countdown has reached 0.

Command That Determines the Condition under Which the Countdown Should Be Started

⚠ This command only makes sense in combination with a command that is to be executed after the countdown is done; see Command to Be Executed after the Countdown (see page 962).

1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown_condition_cmd** (`sessions.xlock0.options.countdown_condition_cmd`).
2. Enter the command in the field **Countdown condition command**. The user that issues the commands is `user` . If no command is defined here, the countdown will be started. Examples: `pgrep wfica` (returns 0 if a Citrix session is present), `pgrep igelrdp2`

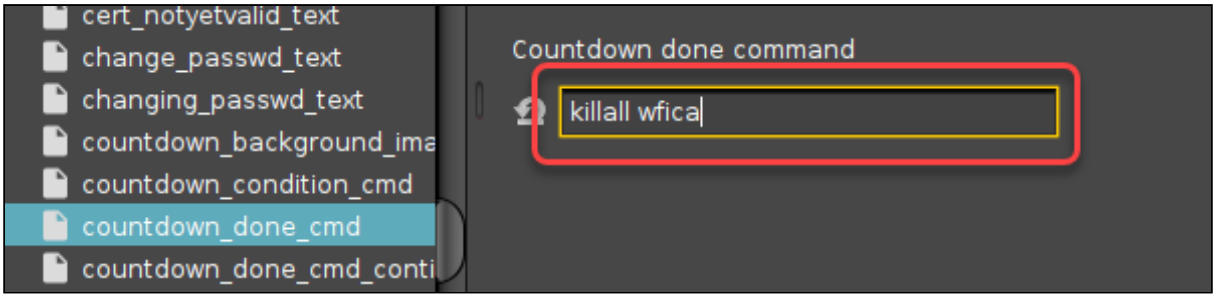


3. Click **Apply** or **Ok**.
   If the command returns 0, the countdown is started. When the countdown has reached 0, the command specified with **System > Registry > sessions > xlock0 > options > countdown_done_cmd** is executed (see Command to Be Executed after the Countdown (see page 962)).
   If the command returns a non-zero value, the countdown is not started. A command that is configured for execution after the countdown will therefore not be executed. The screen lock or screensaver will be started.

Command to Be Executed after the Countdown

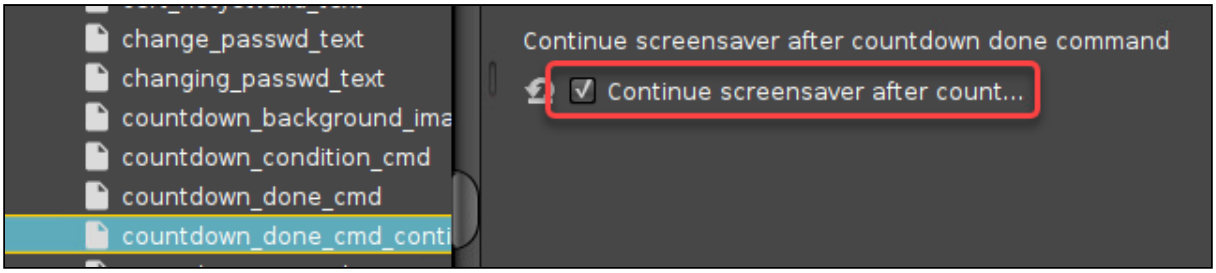
1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown_done_cmd** (`sessions.xlock0.options.countdown_done_cmd`).
2. Enter the command in the field **Countdown done command**. The user that issues the commands is `user` . Examples: `killall wfica` (terminates the Citrix ICA client), `logoff`

   > The command is executed synchronously before the countdown goes away. If the command doesn't terminate quickly, it must be sent to the background by appending " `&` ".



3. (Optional) If you want to enforce the start of the screensaver after the **Countdown done command** has been executed, open the registry key **sessions > xlock0 > options > countdown_done_cmd_continue** (`sessions.xlock0.options.countdown_done_cmd_continue`) and enable **Continue screensaver after countdown done command**.

Some applications stop the screensaver when they get restarted, so this does not always have the desired effect.



4. Click **Apply** or **Ok**.

Keyboard Shortcuts for Managing Windows

Switching back and forth between open application windows by using keyboard shortcuts is a common way of managing windows.

If you work in a fullscreen environment, you also need a way to switch to the desktop.

With IGEL Linux OS *version 10.03.500*, the device desktop was added to the window cycle of the window manager.

Use the following default shortcuts to switch from application windows to the desktop:

Task	Default Shortcut
Switch between active windows using Task Switcher	Ctrl + Alt + Tab
Switch between active windows using Task Switcher (backwards)	Ctrl+Alt+Shift+Tab
Switch focus to next window	Ctrl + Esc
Switch focus to next window (2)	Ctrl + Alt + UpArrow
Switch focus to next window (reverse order)	Ctrl + Alt + DownArrow

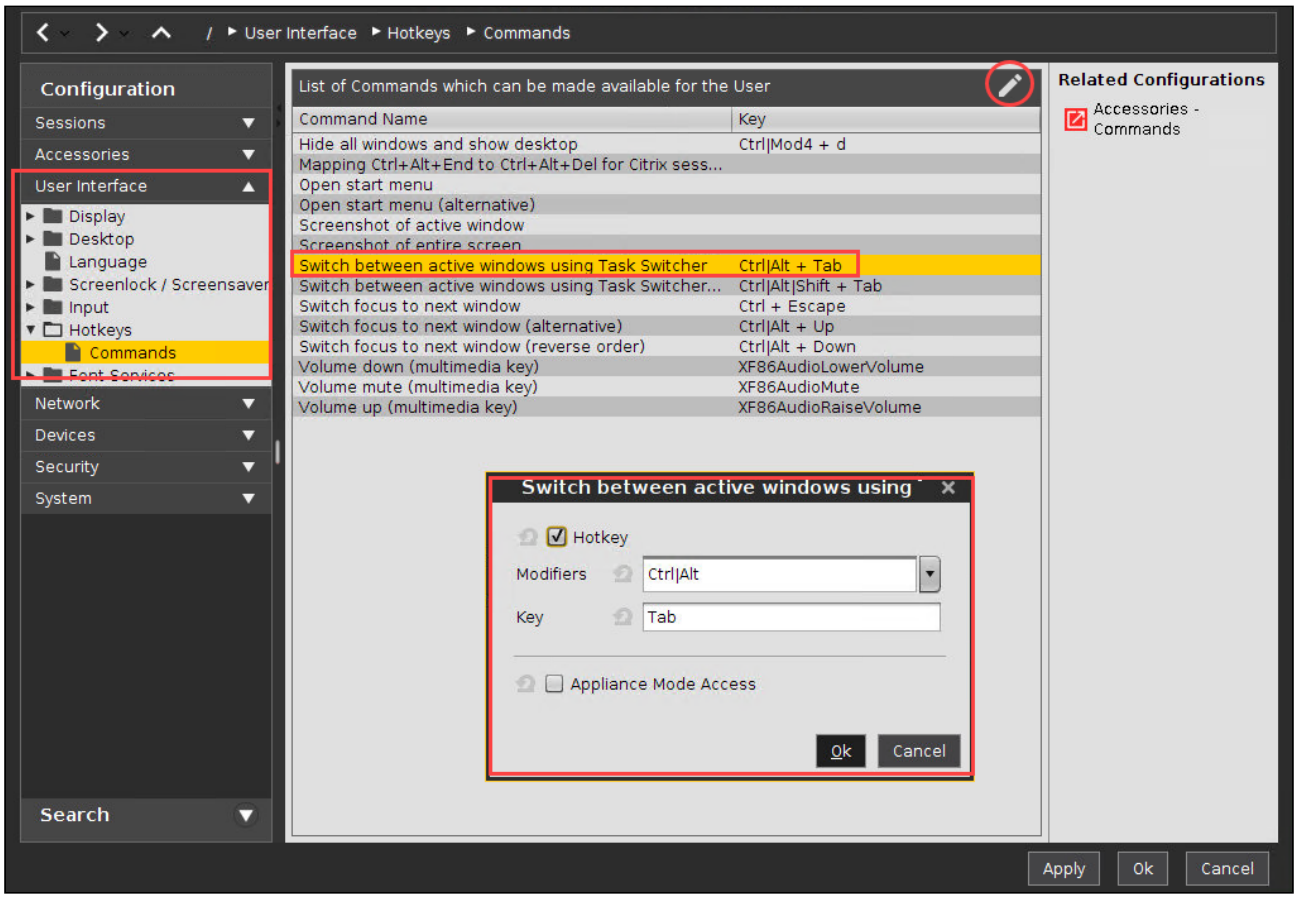
Go to IGEL Setup > User Interface > Hotkeys > Commands (see page 1587) to change these shortcut combinations.

Switching to the desktop minimizes all windows. Switching back to a window right after that restores all windows.

Make Frequent User Actions Easier by Defining Hotkeys

For common actions, such as switching between different windows, or lock the screen, you can use a hotkey. Some hotkeys are preconfigured, but you can activate, deactivate, and modify them.

The following example shows how to find out or modify the hotkey for switching between windows:

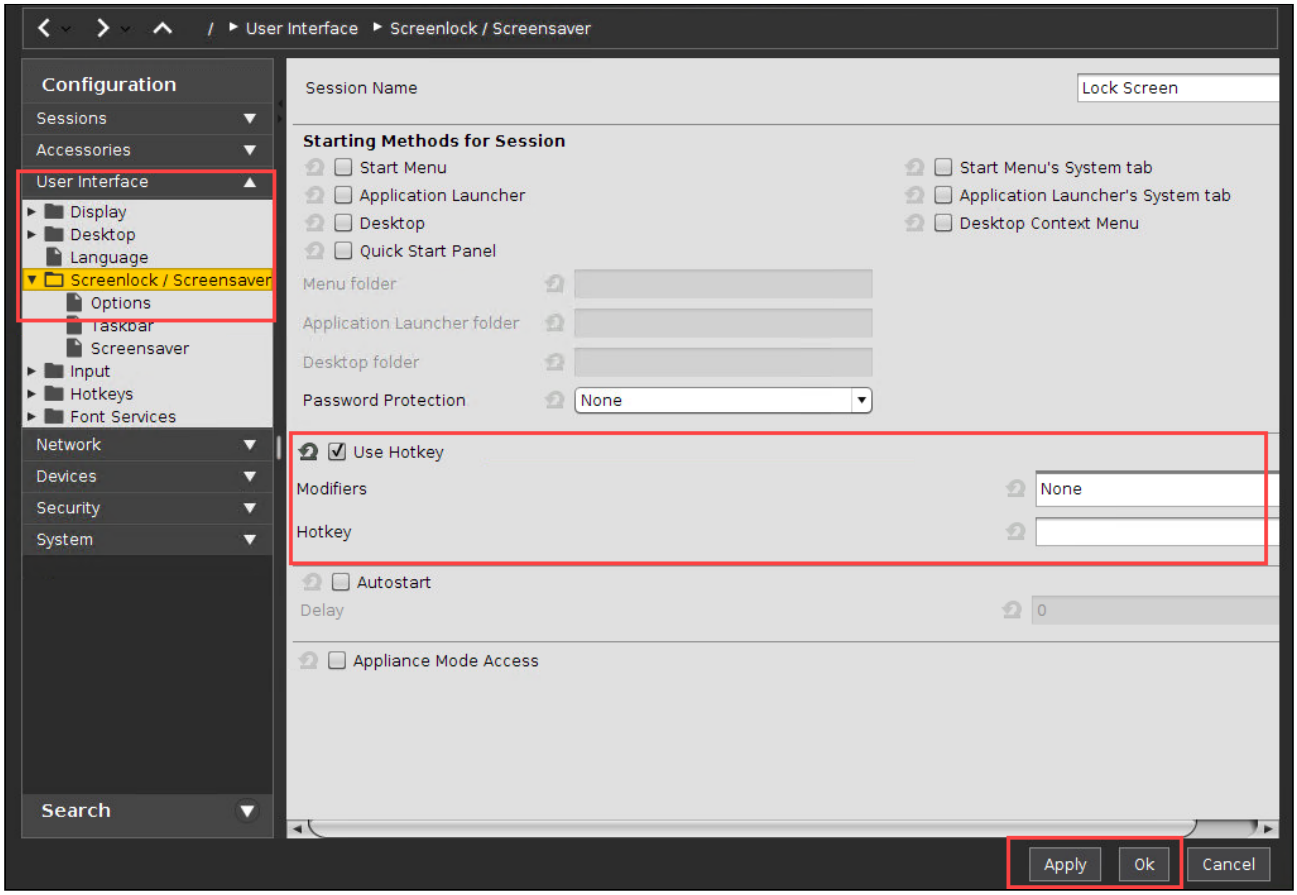


1. Open the setup and go to **User Interface > Hotkeys > Commands**.
2. Select **Switch between active windows using Task Switcher**.
3. Click on **Modify**.
   A dialog window is opened.
4. Enable **Hotkey**, if not already enabled.
5. Select a modifier key or a combination of modifier keys under **Modifiers**.
6. Enter a **Key**.

> If you want to enter a key that has no visible character assigned, e. g. the [Tab] key, open a terminal, logon as user and enter `xev -event keyboard`. Press the key designated for the hotkey. The text in brackets starting with `keysym` will contain the desired string for the **Key** field; example: `Tab` in `(keysym 0xff09, Tab)`

7. Click on **Ok**.
8. Click on **Apply** or **Ok**.
   The hotkey is ready for use.

The following example shows how to define a hotkey to lock the screen:



1. Open the setup and go to **User Interface > Screenlock/Screensaver**.
2. Enable **Hotkey**.
3. Select a modifier key or a combination of modifier keys under **Modifiers**.
4. Enter a **Key**.
5. Click on **Apply** or **Ok**.
   The hotkey is ready for use.

Shutdown/Suspend Devices Automatically at the End of a Session

Issue

You may want to shut down, suspend, restart or log off from the device automatically after ending a session.

Solution

You can define an "after-logoff-action" dependent on a session type. This action is performed after ending the last instance of the defined session type.

Proceed as follows:

1. In the device's local Setup (or its UMS configuration or profile), navigate to **System > Firmware Customization > Custom Commands** > **Post Session**.
2. Choose a **Session type**.
3. Choose a **Post-session command**.
4. Save the changes with **Apply** or **OK**.

If the last instance of the chosen session type is ended, the post-session command will be processed.

See also IGEL OS manual: Post Session Custom Commands in IGEL OS (see page 2081)

The post-session command **Shutdown/suspend** will perform the default action defined under **System > Power Options > Shutdown > Default action**. Please check this parameter before using the command.

The post-session command **Logoff** is futile unless you define a login method under **Security > Logon** (Smartcard, Active Directory/Kerberos, or IGEL Shared Workplace). The **Logoff** command also cannot be used with an appliance – in this case, only **Shutdown/suspend** or **Reboot** commands are working.

When using auto-logoff commands with an appliance, make sure to define the corresponding session type – e.g. **Horizon View** when using the *VMware Horizon View* appliance.

Suspend to RAM - Wake Up by USB Mouse

You can wake up your device by mouse click or key press.

> The wake-up functionality strongly depends on the hardware and BIOS version in use. We recommend testing this function before using it. With devices converted by UDC3/OS Creator (OSC) or UD Pocket, it only works when the hardware is fully supported.

Setting System Suspend as the Default Action

1. In Setup, go to **System > Power Options > Shutdown.**
2. Activate **Allow system suspend.**
3. Under **Default action**, select "Suspend".
4. Save the setting by clicking **Apply** or **Ok**.
   From now on, the system will be suspended to RAM whenever it is shut down.

To use the wake-up functionality, the following steps must be performed:

Configuring the BIOS for PS/2 Mouse and Keyboard

1. Open the BIOS of your device and check if the power management section has parameters named "PS/2 Wake up from S3" or similar.
2. If present, set the parameters to enabled.
3. Save the BIOS configuration and continue booting.

Configuring the BIOS for USB Mouse and Keyboard

1. Open the BIOS of your device and check if the power management section has parameters named "USB Wake Up from S3" or similar.
2. If present, set the parameters to enabled.
3. Save the BIOS configuration and continue booting.

Enabling the Wake-Up Functionality

1. In the IGEL Setup, activate **System > Registry > system > acpi_wakeup > enabled > Wakeup from S3 by USB devices**.
2. Click **Apply** or **Ok.**

To check if the wake-up functionality works, click > , wait a few minutes, and try to wake up the device using a mouse click or a key press.

Taking Screenshots on IGEL Linux

Issue

For support or documentation purposes, the user wants to take a screenshot in IGEL Linux without accessing the client via VNC.

Solution

On IGEL Linux 5.08.100 and newer or IGEL Linux 10.01.100 and newer, use the pre-installed Screenshot Tool (see page 1769).

On earlier versions:

1. Download the tool Rapid Screenshot[108].

   > The default download location of local Firefox is `/tmp/`.

2. Open a **Local Terminal** and log in as root.
3. Copy the downloaded `.jar` file from the `/tmp/` directory to `/wfs/screenshot.jar`:
   `cp /tmp/ /wfs/screenshot.jar`
   It is important to copy the file to `/wfs` because otherwise the file would be flushed with a reboot.
4. Open IGEL setup and create a new **custom application**:
   System > Firmware Customization > Custom Application
5. Set **Command** to `java -jar /wfs/screenshot.jar` in **Settings**.
6. Click the new icon on the desktop to run the **custom application**.

To distribute this application to several thin clients use the file transfer option in IGEL UMS and set up a profile with the custom application configuration.

1. HOW TO USE *Easy Screenshot Maker*:
   a. Start the application.
   b. Make a screenshot.
   c. Save the file for example as `test.png`.
2. HOW TO USE *Rapid Screenshot*:
   a. Start the application.
   b. Click **Save in** to configure the path to store screenshots.
   c. Click button **Click**.
   The screenshot will be saved automatically as `.jpg`.

108. https://sourceforge.net/projects/screenshot/?source=directory

Please note the licenses for both screenshot capture tools mentioned on the websites of these specific tools!

Setting the Device's System Time

Issue

The thin client's system time is not correct.

Solution

1. Open the thin client's configuration either locally or in UMS.
2. Go to **System > Time and Date**
3. Choose your **Continent/Area** (e.g. America).
4. Choose your **Location** (e.g. New York).
5. Set time and date
    a. either manually by clicking **Set time and date**
    b. or automatically by configuring an **NTP Time Server**.
6. Click **OK** or **Apply** to save your settings.

> Note: If choosing **General** as **Time Zone Area** you have to set your GMT time zone (**Location**) following the POSIX standard (as usual in Linux) - which means you have to invert the offset of your common UTC time zone! (See tool tip for **Location** as well.) Therefore it is preferable to set the system's time zone by choosing the corresponding area and location instead of defining the GMT offset.

Example for America/New York: In POSIX standard **GMT+5** is the time zone **5 hours west** of Greenwich and corresponds to **UTC-5**

Legal Note

IGEL's Terms & Conditions[109] apply.

109. https://www.igel.com/terms-conditions/

Updating Timezone Information (Daylight Saving Time, DST)

Symptom

The device is showing an incorrect time of day for your location, although you have set the correct time zone.

Problem

The time zone or the regulation for Daylight Saving Time (DST) for your location has changed.

Solution

->Update the time zone information files via IGEL Universal Management Suite (UMS).

Retrieving Current Time Zone Information Files

On Windows

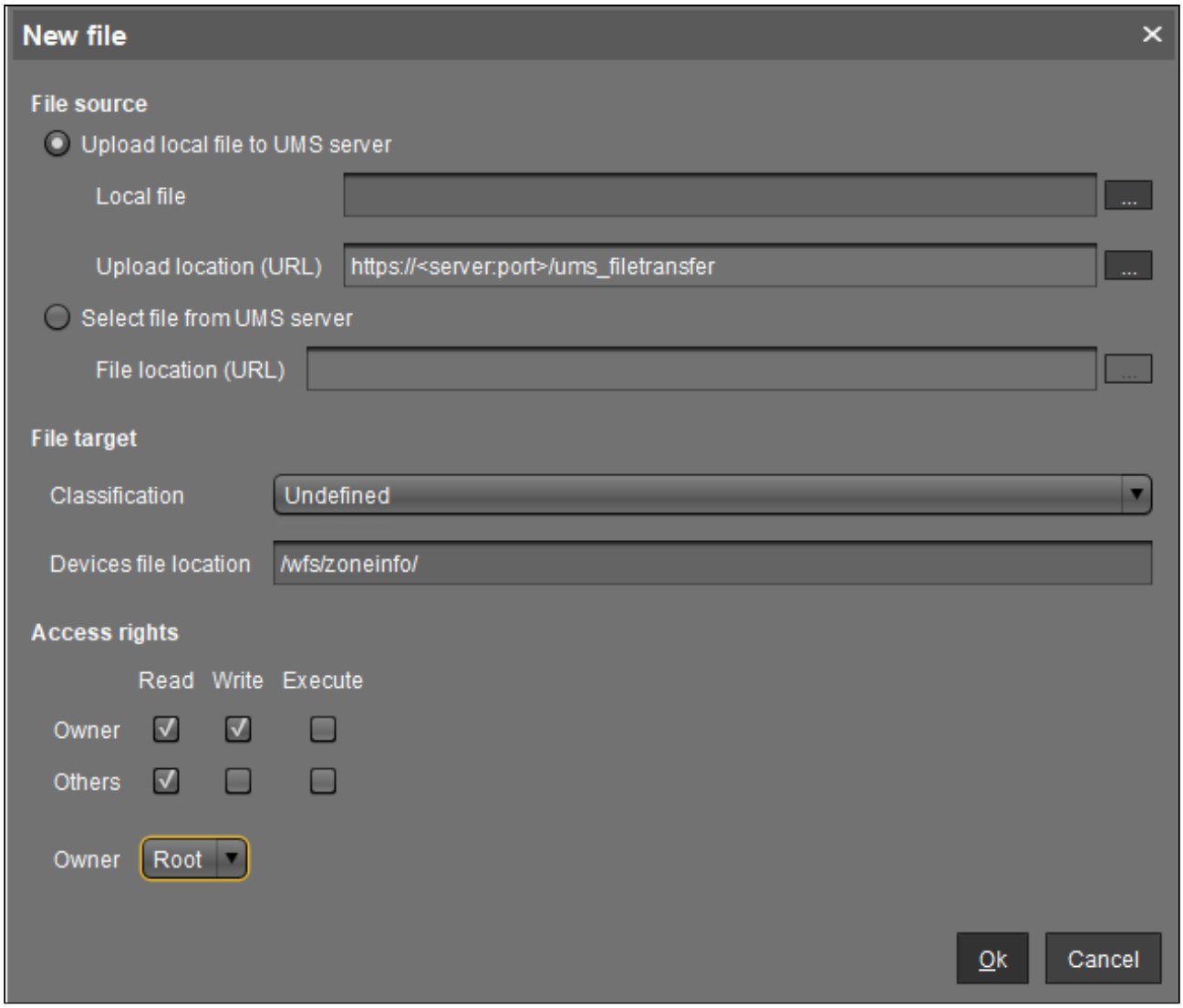
- Use your web browser to download the following package files:
  - http://packages.ubuntu.com/xenial-updates/all/tzdata/download for IGEL Linux version 10.x
- Extract the package contents using the program 7-Zip (freely available from http://www.7-zip.org).
- Find the file for your location in the extracted directory in `usr/share/zoneinfo/`, e.g. `usr/share/zoneinfo/Africa/Casablanca` for Morocco.

On Linux

- Update your system time zone information with these commands: `sudo apt-get update` `sudo apt-get install tzdata`
- Find the file for your location in the system directory `/usr/share/zoneinfo/`, e.g. `/usr/share/zoneinfo/Africa/Casablanca` for Morocco.

Distributing the Files from IGEL Universal Management Suite

- Select **System > New > New File** from the UMS Console menu bar or go to **Files** in the tree structure and select **New File** from the context menu.
- Select the time zone file for your location under **Local File**.
- Select **Undefined** under **Classification**.
- Specify `/wfs/zoneinfo/` as the **Devices file location**.
- Set the **Access rights** to Read and Write for the Owner, and to Read for Others.
- Select Root as the **Owner**.
- Click **OK** to confirm the settings.



On a device, you can verify the transfer and activation of the new time zone information files:

- In the **Local Terminal**, enter `grep 'timezone_config' /var/log/messages`

> On IGEL Linux version 10.x, use: `journalctl | grep 'timezone_config'`

- The output should look like the following:
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/Africa/Casablanca`
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/posix/Africa/Casablanca`

`Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/Casablanca`

Adding or Changing a MIME Type Handler

Symptom

Files or protocols are opened with the wrong application.

Problem

The MIME type handler for the file type or the protocol is missing or misconfigured.

Solution

Change the MIME type handler or add a new one.

MIME type handlers are defined by `*.desktop` files in the `/usr/share/applications.mime/` directory.

To add a new `*.desktop` file, use the following sample and edit it according to your needs:

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Type=Application
Name=Browser//A name for the MIME type handler
Categories=Application
Exec=/usr/bin/firefox %u//The binary to execute on opening an associated file
MimeType=x-scheme-handler/http;x-scheme-handler/https;text/html;application/
xhtml+xml;//A list of MIME types separated by semicolon
Terminal=false
StartupNotify=false
NoDisplay=true
```

You can find out more about `*.desktop` files in a specification at freedesktop.org (see page 975).

These are the default handlers on IGEL Linux:Images (opened via gpicview)

- image/bmp;
- image/gif;
- image/jpeg;
- image/jpg;
- image/png;
- image/x-bmp;
- image/x-pcx;

- image/x-tga;
- image/x-portable-pixmap;
- image/x-portable-bitmap;
- image/x-targa;
- image/x-portable-greymap;
- application/pcx;
- image/svg+xml;
- image/svg-xml;

Videos and Music (opened via `/services/mplr/bin/mediaplayer`)

Note that `/services/mplr/bin/mediaplayer` calls either `/config/sessions/mediaplayer0` if existent or `totem` if this is not the case

- application/mxf;
- application/ogg;
- application/ram;
- application/sdp;
- application/smil;
- application/smil+xml;
- application/vnd.ms-wpl;
- application/vnd.rn-realmedia;
- application/x-extension-m4a;
- application/x-extension-mp4;
- application/x-flac;
- application/x-flash-video;
- application/x-matroska;
- application/x-netshow-channel;
- application/x-ogg;
- application/x-quicktime-media-link;
- application/x-quicktimeplayer;
- application/x-shorten;
- application/x-smil;
- application/xspf+xml;
- audio/3gpp;
- audio/ac3;
- audio/AMR;
- audio/AMR-WB;
- audio/basic;
- audio/midi;
- audio/mp4;
- audio/mpeg;
- audio/mpegurl;
- audio/ogg;
- audio/prs.sid;
- audio/vnd.rn-realaudio;

- audio/x-ape;
- audio/x-flac;
- audio/x-gsm;
- audio/x-it;
- audio/x-m4a;
- audio/x-matroska;
- audio/x-mod;
- audio/x-mp3;
- audio/x-mpeg;
- audio/x-mpegurl;
- audio/x-ms-asf;
- audio/x-ms-asx;
- audio/x-ms-wax;
- audio/x-ms-wma;
- audio/x-musepack;
- audio/x-pn-aiff;
- audio/x-pn-au;
- audio/x-pn-realaudio;
- audio/x-pn-realaudio-plugin;
- audio/x-pn-wav;
- audio/x-pn-windows-acm;
- audio/x-realaudio;
- audio/x-real-audio;
- audio/x-sbc;
- audio/x-scpls;
- audio/x-speex;
- audio/x-tta;
- audio/x-wav;
- audio/x-wavpack;
- audio/x-vorbis;
- audio/x-vorbis+ogg;
- audio/x-xm;
- image/vnd.rn-realpix;
- image/x-pict;
- misc/ultravox;
- text/google-video-pointer;
- text/x-google-video-pointer;
- video/3gpp;
- video/dv;
- video/fli;
- video/flv;
- video/mp4;
- video/mp4v-es;
- video/mpeg;
- video/msvideo;
- video/ogg;

- video/quicktime;
- video/vivo;
- video/vnd.divx;
- video/vnd.rn-realvideo;
- video/vnd.vivo;
- video/x-anim;
- video/x-avi;
- video/x-flc;
- video/x-fli;
- video/x-flic;
- video/x-flv;
- video/x-m4v;
- video/x-matroska;
- video/x-mpeg;
- video/x-ms-asf;
- video/x-ms-asx;
- video/x-msvideo;
- video/x-ms-wm;
- video/x-ms-wmv;
- video/x-ms-wmx;
- video/x-ms-wvx;
- video/x-nsv;
- video/x-ogm+ogg;
- video/x-theora+ogg;
- video/x-totem-stream;
- x-content/video-dvd;
- x-content/video-vcd;
- x-content/video-svcd;

Documents (opened via `/usr/bin/evince`)

- application/pdf;
- image/tiff

Web (opened via `/usr/bin/firefox -remote`)

- x-scheme-handler/http;
- x-scheme-handler/https;
- text/html;
- application/xhtml+xml;

Regional Settings in Sessions

>Symptom

If you set a certain keyboard language it has no effect on the regional settings.

Problem

In the *IGEL* setup there are several input fields for regional settings. You would like to understand which setting has what effect in the sessions.

Solution

Defining general regional settings:

->Go to **IGEL Setup > User Interface > Language**.

- **Language**: Select one of the languages offered for the graphical user interface.
- **Keyboard Layout**: Select the country-specific assignment of keys, e.g. English(US).
- **Input Language**: Set the language you are going to write in, e.g. English(Australia).
- **Standards and Formats**: Select country-specific formats, e.g. for date and time or currency.

Defining session-specific regional settings:

->Go to the settings of your session, e.g. Citrix: **IGEL Setup > Sessions > Citrix > Citrix Global > Keyboard**.

> The default settings are those you defined under **User Interface > Language**.

->Specify **Keyboard Layout** and **Input Language** for your Citrix Session.

Devices

- Monitor (see page 981)
- Using a Cherry SECURE BOARD (see page 1001)
- Webcam Redirection and Optimization in IGEL OS (see page 1034)
- Webcam Information (see page 1046)
- Bluetooth Tool (see page 1048)
- How to Deploy a Jabra Xpress Package (see page 1052)
- Connecting Signature Pads (see page 1056)
- Using a Kofax / Wacom Signature Pad (see page 1057)
- Using a StepOver Signature Pad (see page 1058)
- eGK/KVK - Card Reader (see page 1064)
- Using Mobile Device Access (see page 1076)
- Swapping Function of Mouse Buttons (e.g. When Using an Evoluent Mouse) (see page 1085)
- Using Natural Scrolling (Reverse Scrolling Direction) on IGEL OS Devices (see page 1087)
- Connecting a Serial Barcode Scanner (see page 1089)
- Using DriveLock with IGEL Devices (see page 1091)
- Restricting the Mounting of Hotplug Storage Devices on IGEL Linux (see page 1092)
- When to Use USB Redirection (see page 1093)
- How to Configure USB Access Control (see page 1097)
- Issues with USB IDs in USB Devices Rules (see page 1100)
- How Can I Fix Touchpad Issues? (see page 1102)
- How Do I Configure a Fujitsu PalmSecure Vein Scanner with IGEL OS? (see page 1105)
- Virtual Background for Unified Communication Apps in IGEL OS (see page 1110)

Monitor

- Touchscreen Calibration (see page 982)
- Touchscreen in Multimonitor Environment (see page 995)
- USB-Powered ASUS Monitor and IGEL OS 11 (see page 996)
- Solving Hotplugging Issues with DisplayPort Monitors (see page 997)
- No Sound When Using a DisplayPort Monitor (see page 998)
- Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters (see page 1000)

Touchscreen Calibration

For setting up a touchscreen, you have to enable the touchscreen function and select a specific touchscreen driver.

> The initial configuration should take place with a mouse and keyboard connected to ensure that you can open the setup and navigate within it.

To set up a touchscreen:

1. In IGEL Setup, go to **User Interface > Input > Touchscreen**.
2. Activate **Enable touchscreen**.
3. Select your touchscreen driver under **Touchscreen type**.

Depending on the selected driver, you have different configuration options. For further information, click the appropriate link:

- EvTouch (USB) (see page 983)
- eGalax (see page 987)
- Elo Multitouch (USB) (see page 989)
- Elo Singletouch (USB) (see page 991)
- TSHARC (USB) (see page 993)

EvTouch (USB)

Supported Devices

Supported touch monitors and touchscreen controllers:

Vendor	Product	Name
0x16FD	0x5453	Reakin, TS2005F USB TouchController
0x7374	0x0001	
0x04E7	0x0020	Elo TouchSystems, Touchscreen Interface (2700)
0x1870	0x0001	Nexio Co., Ltd, iNexio Touchscreen controller
0x10F0	0x2002	Nexio Co., Ltd, iNexio Touchscreen controller
0x0664	0x0306	ET&T Technology Co., Ltd., Groovy Technology Corp. GTouch Touch Screen
0x0664	0x0309	ET&T Technology Co., Ltd. Groovy Technology Corp. GTouch Touch Screen
0x14C8	0x0003	Zytronic, Unknown device
0x1AC7	0x0001	
0x0F92	0x0001	
0x08F2	0x00F4	Gotop Information Inc., Unknown device
0x08F2	0x00CE	Gotop Information Inc., Unknown device
0x08F2	0x007F	Gotop Information Inc., Super Q2 Tablet
0x0DFC	0x0001	GeneralTouch Technology Co., Ltd, Touchscreen
0x1391	0x1000	IdealTEK, Inc., URTC-1000
0x6615	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x595A	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x0AFA	0x03E8	
0x0637	0x0001	
0x1234	0x5678	Brain Actuated Technologies, Unknown device
0x16E3	0xF9E9	
0x0403	0xF9E9	Future Technology Devices International, Ltd, Unknown device
0x0596	0x0001	MicroTouch Systems, Inc., Touchscreen
0x134C	0x0004	PanJit International Inc., Touch Panel Controller

Vendor	Product	Name
0x134C	0x0003	PanJit International Inc., Touch Panel Controller
0x134C	0x0002	PanJit International Inc., Touch Panel Controller
0x134C	0x0001	PanJit International Inc., Touch Panel Controller
0x1234	0x0002	Brain Actuated Technologies, Unknown device
0x1234	0x0001	Brain Actuated Technologies Unknown device
0x0EEF	0x0002	D-WAV Scientific Co., Ltd, Touchscreen Controller(Professional)
0x0EEF	0x0001	D-WAV Scientific Co., Ltd, eGalax TouchScreen
0x0123	0x0001	
0x3823	0x0002	
0x3823	0x0001	

Setup Parameters

- **Touchscreen type**

  More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

- **Swap X and Y values**
  More

IGEL Setup > User Interface > Input > Touchscreen		
> Swap X and Y values	userinterface.touchscreen.swapxy	enabled / disabled

- **Set driver specific defaults** for resetting calibration values.

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.
   More

IGEL Setup > User Interface > Touchscreen		
> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / disabled

3. Set **Touchscreen type** to **EvTouch (USB)**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

4. Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.
   This will call the *xinput_calibrator* calibration tool which is located at `/usr/bin/xinput_calibrator`. The calibration parameter will be saved in IGEL setup.

Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / disabled

2. Set under **Right button timeout** the time after which right-click is generated.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: 1000 msec

Multimonitor

Multimonitor configuration is not supported.

eGalax

Supported Devices

EETI eGalax eMPIA USB touchscreens.

Setup Parameters

- **Touchscreen type**
  More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.
   More

IGEL Setup > User Interface > Touchscreen		
> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / disabled

3. Set **Touchscreen type** to **eGalax**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

4. Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.
   This will call the proprietary EETI calibration tool, which is located at `/usr/bin/eCalib`. The calibration parameter will be saved in `/wfs/egtouch.d`.

Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / disabled

2. Set under **Right button timeout** the time after which right-click is generated.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: 1000 msec

Multimonitor

Multimonitor configuration is not supported.

Elo Multitouch (USB)

Supported Devices

IntelliTouch Plus/iTouch Plus 2515-07(non HID), 2521 (HID), 2515-00(HID) PCAP 2 touch, 4 touch and 10 touch controllers.

Setup Parameters

- **Touchscreen type**

More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.
   More

IGEL Setup > User Interface > Touchscreen		
> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / disabled

3. Set **Touchscreen type** to **Elo Multitouch (USB)**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

4. Reboot the device or click in IGEL Setup **Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.
   This will call the proprietary ELO Multitouch calibration tool which is located at `/etc/opt/`

`elo-mt-usb/elova`. The calibration parameter will be saved in `/wfs/elo-usb.d/MT-USBConfigData`.

Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / disabled

2. Set under **Right button timeout** the time after which right-click is generated.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: 1000 msec

Multimonitor

Multiple ELO Multitouch (USB) touchscreens on a single IGEL device are supported. Calibration of the second ELO Multitouch USB touchscreen can be done via command line by using: `/etc/opt/elo-mt-usb/elova --videoscreen=2` where 2 is the second ELO Multitouch touchscreen connected to the IGEL device.

To view a list of video and USB touchscreen devices available for calibration, use the command: `/etc/opt/elo-mt-usb/elova --viewdevices`.

Elo Singletouch (USB)

Supported Devices

Elo Smartset USB Controllers:

- IntelliTouch(R) 2701, 2700, 2600, 2500U
- CarrollTouch(R) 4500U, 4000U
- Accutouch(R) 2216, 3000U, 2218
- Surface Capacitive 5020, 5010, 5000
- Accoustic Pulse Recognition(APR) Smartset 7010
- Other Elo Smartset USB controllers

Setup Parameters

Touchscreen type

More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Set **Touchscreen already calibrated** to 'false'.
   More

IGEL Setup > User Interface > Touchscreen		
> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / disabled

3. Set **Touchscreen type** to **Elo Singletouch (USB)**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

4. Reboot the device or click in IGEL Setup **Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.
   This will call the proprietary ELO Singletouch calibration tool which is located at `/etc/opt/elo-usb/elova`. The calibration parameter will be saved in `/wfs/elo-usb.d/USBConfigData`.

Hold-to-Right-Click Feature

The feature is not supported.

Multimonitor

Multiple ELO Singletouch USB touchscreens on a single IGEL device are supported. Calibration of the second ELO Singletouch USB touchscreen can be done via command line by using: `/etc/opt/elo-usb/elova --videoscreen=2` where 2 is the second ELO Singletouch USB touchscreen connected to the IGEL device.

> To view a list of video and USB touchscreen devices available for calibration, use the command: `/etc/opt/elo-usb/elova --viewdevices`.

TSHARC (USB)

Supported Devices

Hampshire TSHARC USB touchscreens.

Setup Parameters

- **Touchscreen type**
  More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

Calibration / Reset

Calibrating the touchscreen:

1. Go to **IGEL Setup > User Interface > Input > Touchscreen**.
2. Disable **Touchscreen already calibrated**.
   More

IGEL Setup > User Interface > Touchscreen		
> Touchscreen already calibrated	userinterface.touchscreen.calibrated	enabled / disabled

3. Set **Touchscreen type** to **TSharc**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Touchscreen type	userinterface.touchscreen.driver	

4. Reboot the device or click **IGEL Setup > Accessories > Touchscreen Calibration** to use the IGEL touchscreen calibration tool.

This will call the proprietary Hampshire calibration tool, which is located at `/usr/bin/tscal`.
The calibration parameter will be saved in `/wfs/tsharc.d`.

Hold-to-Right-Click Feature

To activate the feature:

1. Enable the option **Emulate right button** under **User Interface > Input > Touchscreen**.
   More

IGEL Setup > User Interface > Input > Touchscreen		
> Emulate right button	userinterface.touchscreen.emulatethirdbutton	enabled / disabled

2. Set under **Right button timeout** the time after which right-click is generated.
   More

IGEL Setup > User interface > Input > Touchscreen		
> Right button timeout	userinterface.touchscreen.emulatethirdbuttontimeout	Default: 1000 msec

Multimonitor

Multimonitor configuration is not supported.

Touchscreen in Multimonitor Environment

Symptom

You are using a touchscreen in a multimonitor environment. In this case, it can happen that the touchscreen coordinate matrix expands over both monitors, with the result that the monitor interprets the touch point in a wrong way.

Problem

You touch the touchscreen in its center and the cursor moves between the two screens.

Solution

To avoid the unrequested expansion of the touchscreen matrix you have to select the correct touchscreen connection type in the setup:

1. Click **User Interface > Input > Touchscreen** in the IGEL setup.
2. Select the correct connection type under **Multi Monitor** > **Touchscreen Monitor**.

USB-Powered ASUS Monitor and IGEL OS 11

> Solution Based on Experience from the Field
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Issue

USB-powered monitor

Environment

- IGEL OS 11 (11.03.100)
- UMS 6.01 and higher

Description

Recommendation for a USB-powered monitor

Solution

In the following link, you can find the USB-powered ASUS monitor that works plug and play with IGEL OS https://www.asus.com/us/Monitors/MB168B/.

Solving Hotplugging Issues with DisplayPort Monitors

Symptom

On IGEL Linux, in a dual view configuration, the following problem occurs: If a monitor connected via DisplayPort is only switched on after booting the device, it will remain black.

Problem

The DisplayPort standard allows for a powered-off monitor to be undetectable by the graphics card.

Solution

The following checks whether a monitor contained in the configuration is missing (i.e. powered off) and makes it usable as soon as it appears (i.e. is powered on):

1. If you are using IGEL Linux 5, make sure you are running version 5.10.410 or newer.
   If you are using IGEL Linux 10 you do not need to upgrade.
2. In Setup, go to **System > Registry > Parameter >**
   `session.user_display%.options.enhanced_hotplug`
3. Make sure the parameter is set to `true` (default).

> There is another setting you can use if you do not want IGEL Linux to change the display settings every time a DisplayPort monitor is switched on/off:
>
> - Go to **System > Registry > Parameter >**
>   s `essions.user_display%.options.disable_hotplug`
> - Set it to **DP_Disconnect_Only**.

No Sound When Using a DisplayPort Monitor

Symptom

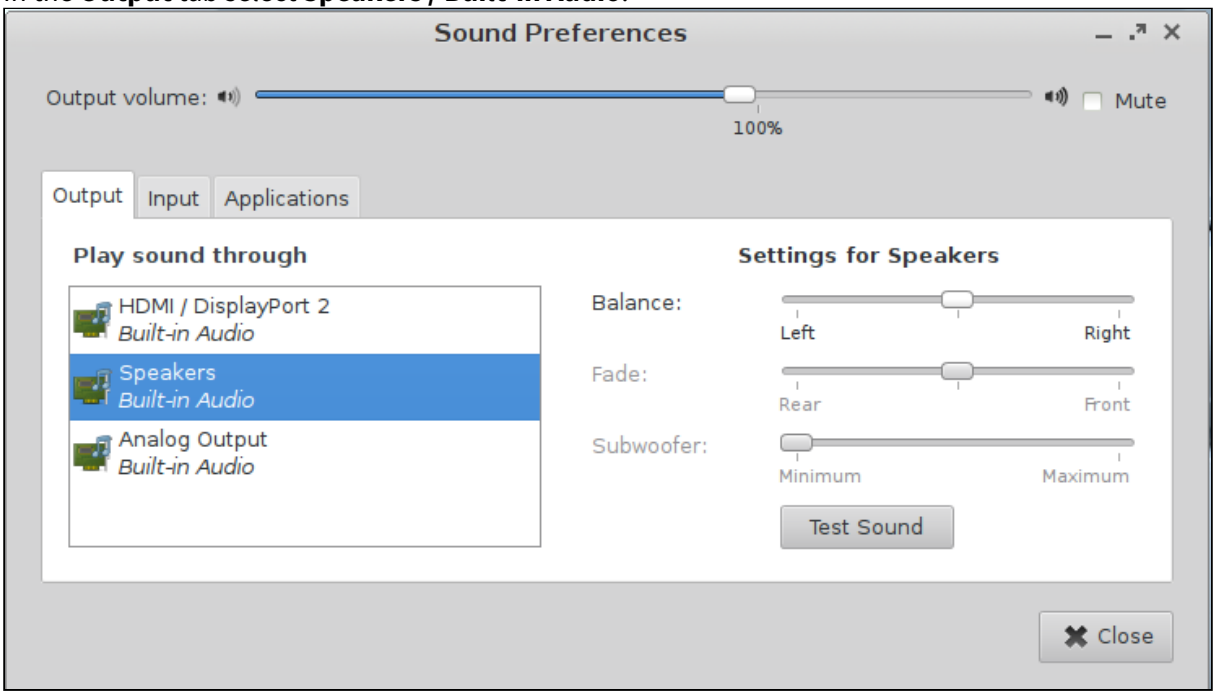
You do not hear any sound from your *IGEL UD5* or *UD6* device. You are using a monitor connected via DisplayPort.

Problem

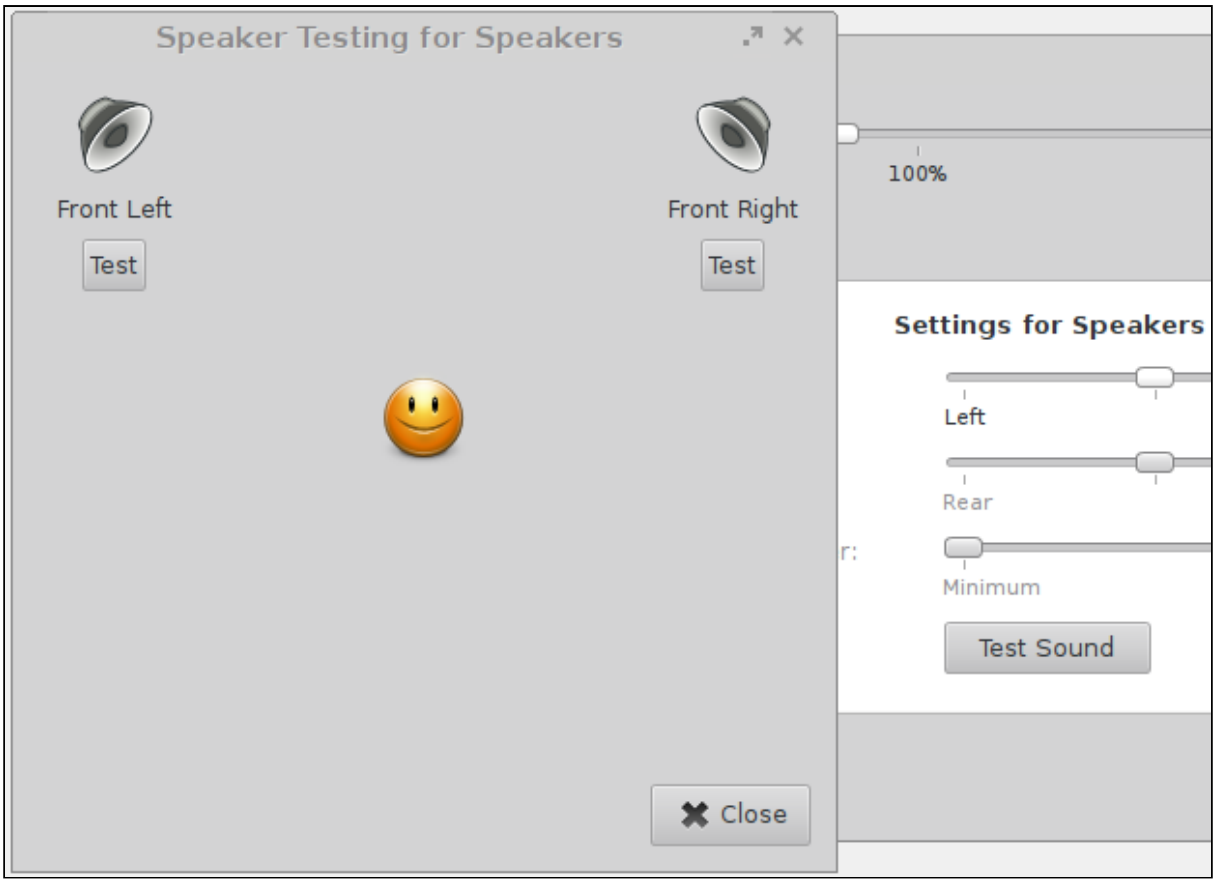
Some DisplayPort monitors misleadingly report support for display audio although they do not have loudspeakers. Therefore *IGEL Linux* will try to play back audio via the monitor.

Solution

1. Right-click on the loudspeaker icon in the panel and open **Sound Preferences**.
2. In the **Output** tab select **Speakers / Built-in Audio**.



3. Click **Test Sound** to test the new setting. Check if you hear a voice saying "Front Left" and "Front Right" on the device speakers.


Speaker Testing for Speakers
Front Left
Test
Front Right
Test
Close
100%
Settings for Speakers
Left
Rear
Minimum
Test Sound

Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters

Problem

When three DVI monitors are connected to a UD7 thin client over passive DisplayPort adapters, only one or two monitors are detected.

Solution

> This solution is only persistent if energy saving is switched off.

1. Open the thin client's Setup.
2. Go to **System > Registry > x > xserver0 > force_reconfig** (Registry key: `x.xserver0.force_reconfig`) and set the value to **never**.
3. Click **Ok** to save the setting and close the Setup.
4. Restart the device.
   All three monitors should be detected.

Using a Cherry SECURE BOARD

Overview

Cherry SECURE BOARD 1.0 provides a secure keyboard input mode which safeguards against hardware keylogging and "Bad USB" attacks.

The following security features are available when an IGEL OS 11 device is connected to a Cherry SECURE BOARD 1.0 in secure mode:

- Your IGEL OS 11 devices will accept keyboard input only from a personalized Cherry SECURE BOARD with secure mode enabled.
- The keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection.
- Optionally, the keyboard can be configured so that it will only accept endpoints that have the right certificates.

For further details on the Cherry SECURE BOARD, see https://www.cherry-world.com/cherry-secure-board-1-0.html.

Prerequisites

- Devices with IGEL OS 11.03 or higher
- UMS 6.01 or higher

Getting the Cherry SECURE BOARD to Work in Secure Mode

To set up a number of Cherry SECURE BOARD keyboards, you must first configure one endpoint that will be used for personalizing the keyboards. The personalization process implies deploying the appropriate certificates to every Cherry SECURE BOARD keyboard that will be used in secure mode.

In addition, the endpoints that are to be connected to the Cherry SECURE BOARD keyboards must be provisioned with the appropriate certificates.

To set up and use Cherry SECURE BOARD keyboards, perform the following steps:

1. Getting the Certificates (see page 1002)
2. Setting Up the Personalization Machine (see page 1022)
3. Personalizing the Cherry SECURE BOARD (see page 1024)
4. Setting Up the Endpoints (see page 1028)

If you want to put a Cherry SECURE BOARD keyboard into its original state, see Resetting the Cherry SECURE BOARD to Its Original State (see page 1033).

Getting the Certificates

Secure mode requires a set of certificates being present both on the endpoint and the keyboard. First, all required certificates are transferred to the endpoint. Then, the endpoint installs a user certificate and the corresponding key on the keyboard; optionally, the client root CA certificate is also installed. This installation of certificates is referred to as personalization.

Downloading the Device Certificates

->Download all certificates from https://github.com/secureboard10/secureboard-ca:

- Device root CA certificate: `SecureboardRootCA.pem`
- Device intermediate CA certificates: `p-20190712.pem`, `p-20191030` etc.

Creating the Custom Certificates

According to "CHERRY SECUREBOARD 1.0, Software Developer's Guide", chapter 9.5, all certificate and key pairs that are sent to the keyboard must meet the following requirements:

- X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys
- Size: Maximum of 572 bytes resp. 475 bytes in DER format

->Create the following custom certificates:

An example how-to for OpenSSL can be found in "CHERRY SECUREBOARD 1.0, Software Developer's Guide", chapter 9.5; see Cherry_Secureboard_0.4[110].
Also, the SECURE BOARD 1.0 Quick Installation Package contains a ready-made shell script that creates example certificates. Download the package from Cherry Secure Board 1.0[111], unzip the file, and use `Cherry Secureboard 1.0 cert-package V1.0/secureboard_linx/create_certs.sh` (Linux) or `Cherry Secureboard 1.0 cert-package V1.0/secureboard_windows/create_certs.bat` (Windows).

110. https://www.cherry.de/en-gb
111. https://www.cherry.de/en-gb/product/secure-board-1-0

Certificate	Required/Optional	Requirements	Encoding/Extension	Max. File Size*	File Name	Remarks
User root CA certificate	required	not specified	PEM	not specified	not specified	If this certificate is also used as the client root CA certificate for mutual authentication, it must meet the requirements for certificates that are sent to the keyboard: X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys; max. 475 bytes
Intermediate CA certificates	optional (according to the certificate chain that is to be used)	not specified	PEM	not specified	not specified	
User certificate (keyboard)	required	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	DER (binary)	572 bytes	`user-cert.der`	
Corresponding user key (keyboard)	required	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM (without a passphrase)	not specified	`user-key.pem`	
Client root CA certificate (keyboard)	optional; for mutual authentication** (see page 1004)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM	475 bytes	not specified	Can be identical with the user root CA certificate

Certificate	Required/Optional	Requirements	Encoding/Extension	Max. File Size*	File Name	Remarks
Client certificate (endpoint)	optional; for mutual authentication** (see page 1004)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM	475 bytes	`client-cert.pem`	
Client key (endpoint)	optional; for mutual authentication** (see page 1004)	X509 Version 3 using ECDSA over NIST curve prime256v1 with corresponding keys	PEM (without a passphrase)	not specified	`client-key.pem`	

* The relevant value is the file size that the certificate has when it is stored in binary format.

** When these certificates are installed, the keyboard can verify if the endpoint is authentic. Without the optional certificates, only the verification of the keyboard's authenticity by the endpoint will be carried out.

Provisioning the Personalization Machine

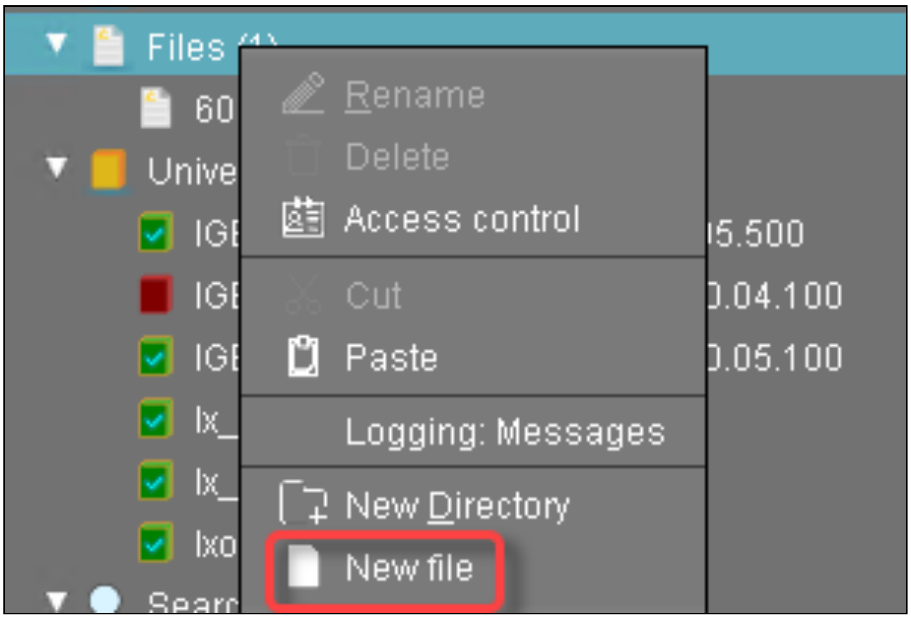
The following instructions describe how to transfer the required certificates to the personalization machine. The personalization machine will deploy the certificates to the keyboard. The UMS will be used for this purpose.

First, a file object is created for each certificate or key file so that the files can be handled by the UMS.

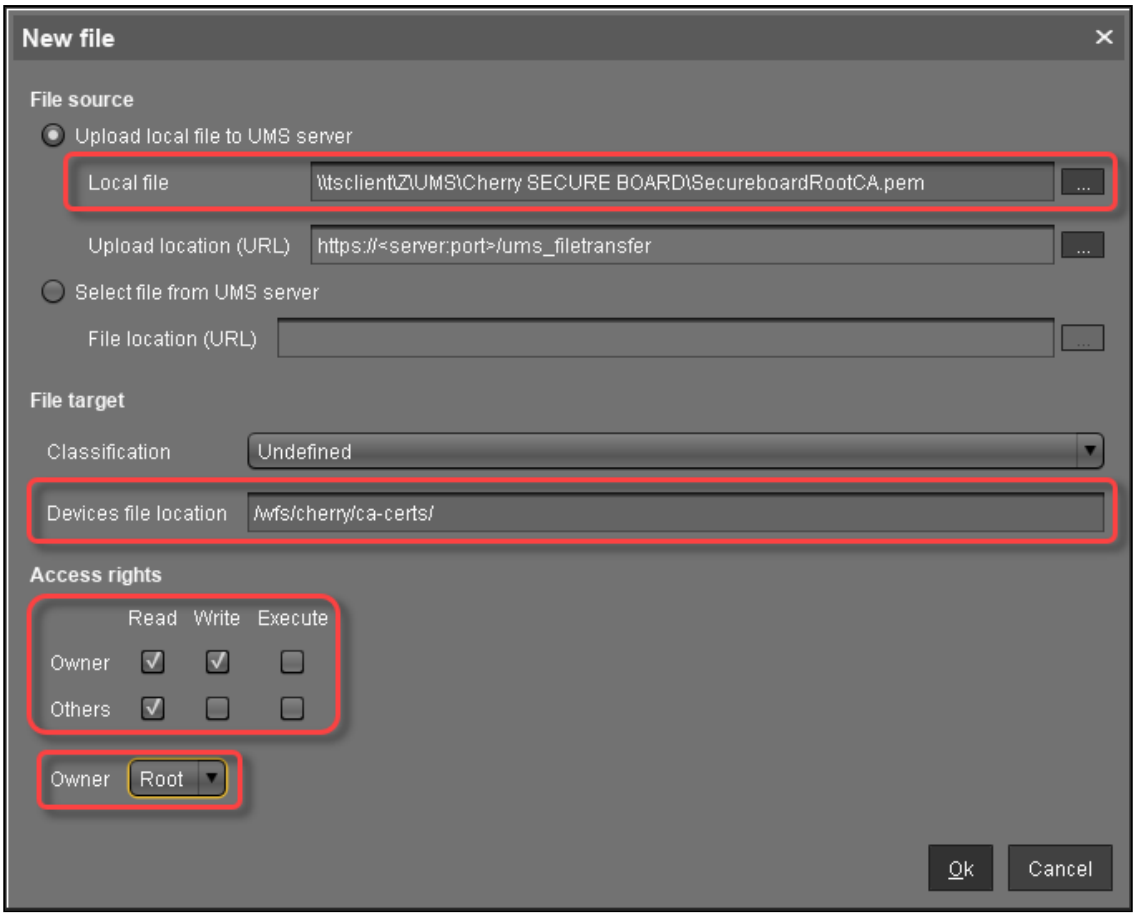
Second, the file objects are assigned to the personalization machine, which results in the files being transferred to that machine.

Creating the File Object for the Device Root CA Certificate

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



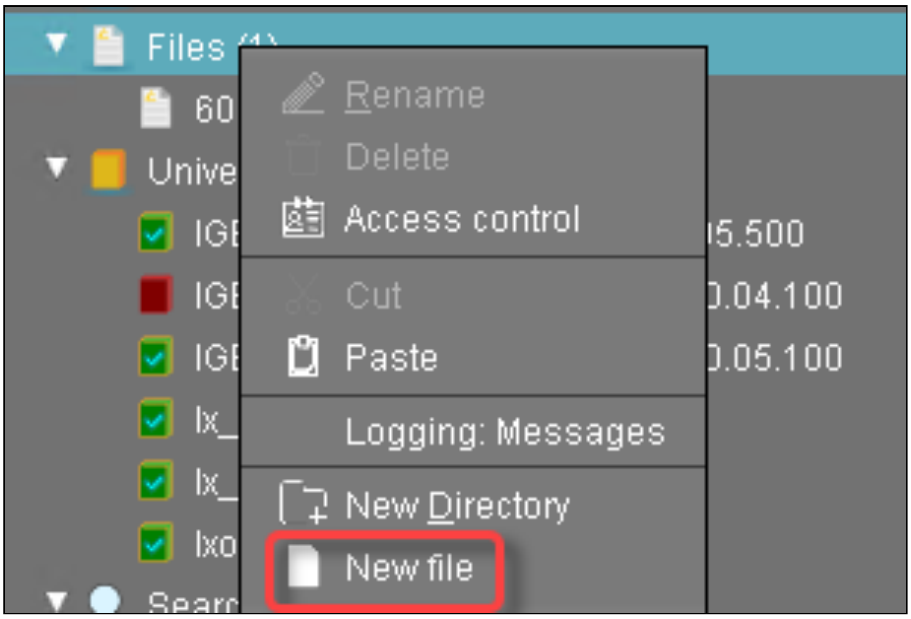
2. In the **New file** dialog, configure the settings as follows:
3. **Local file**: Local file path of `SecureboardRootCA.pem`. Use the file chooser by clicking ....
   - **Device file location**: `/wfs/cherry/ca-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read
   - **Owner**: Root



4. Click **Ok**.
   In the UMS, the file object **SecureBoardRootCA.pem** is created.

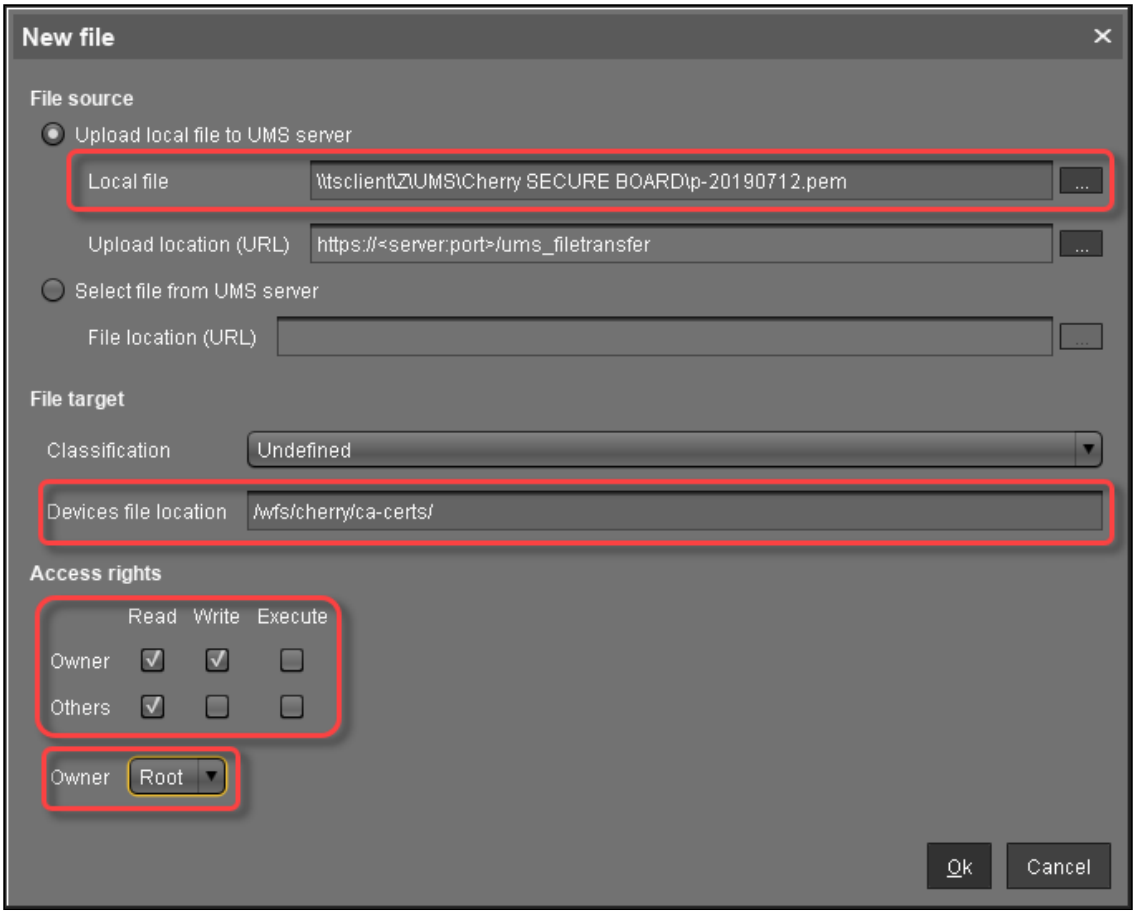
Creating the File Object for the Device Intermediate CA Certificate

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
3. **Local file**: Local file path of `p-20190712.pem`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/ca-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read

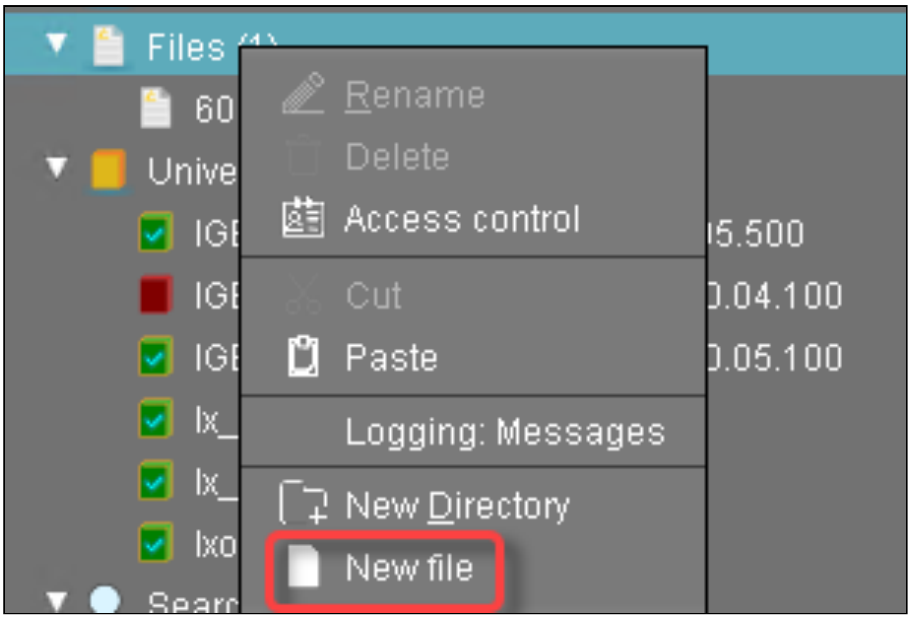
- **Owner**: Root



4. Click **Ok**.
   In the UMS, the file object **p-20190712.pem** is created.

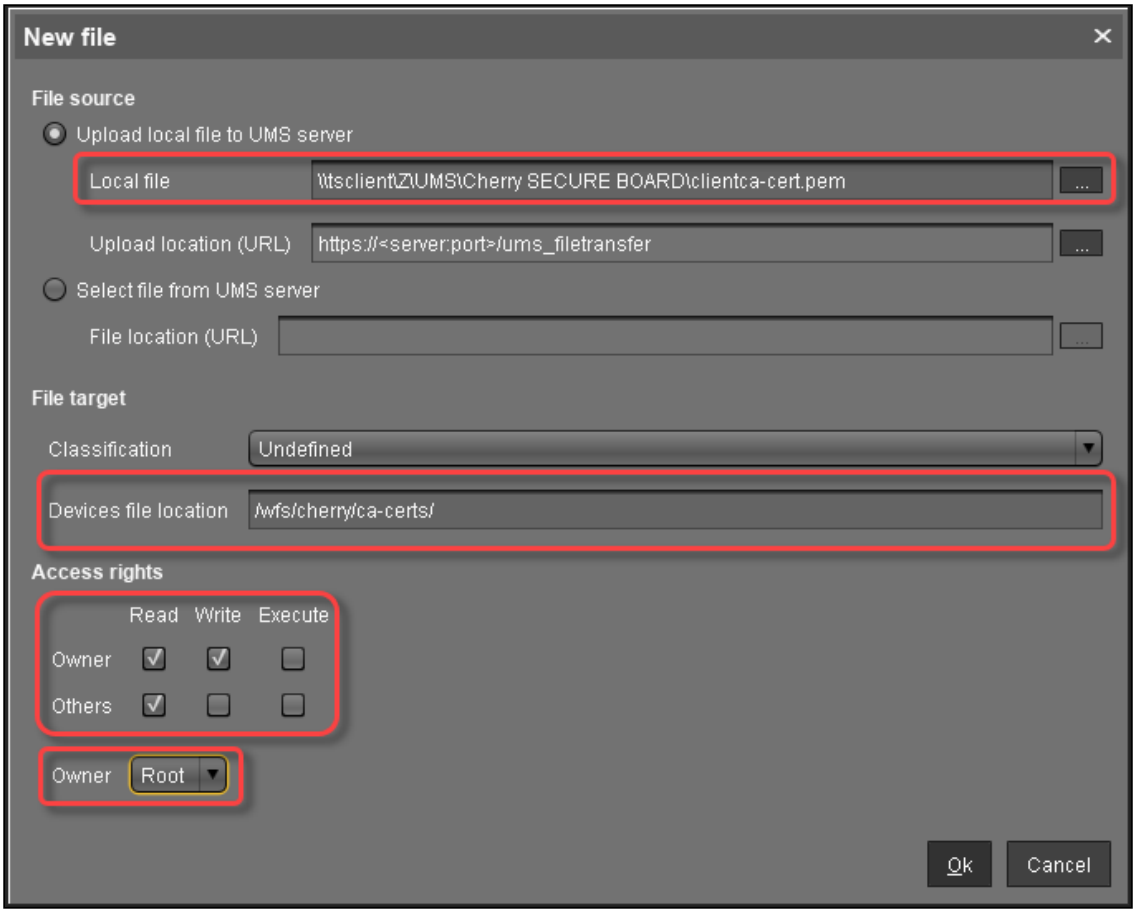
Creating the File Object for the Device Client CA Certificate (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of `clientca-cert.pem`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/ca-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read

- **Owner**: Root

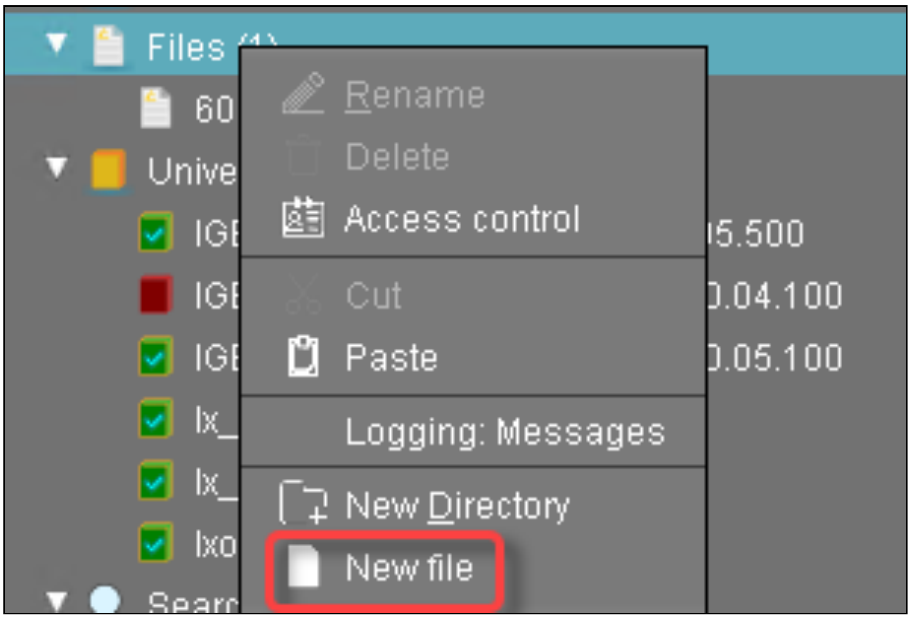


3. Click **Ok**.
   In the UMS, the file object **clientca-cert.pem** is created.

Creating the File Object for the User Certificate (Keyboard)

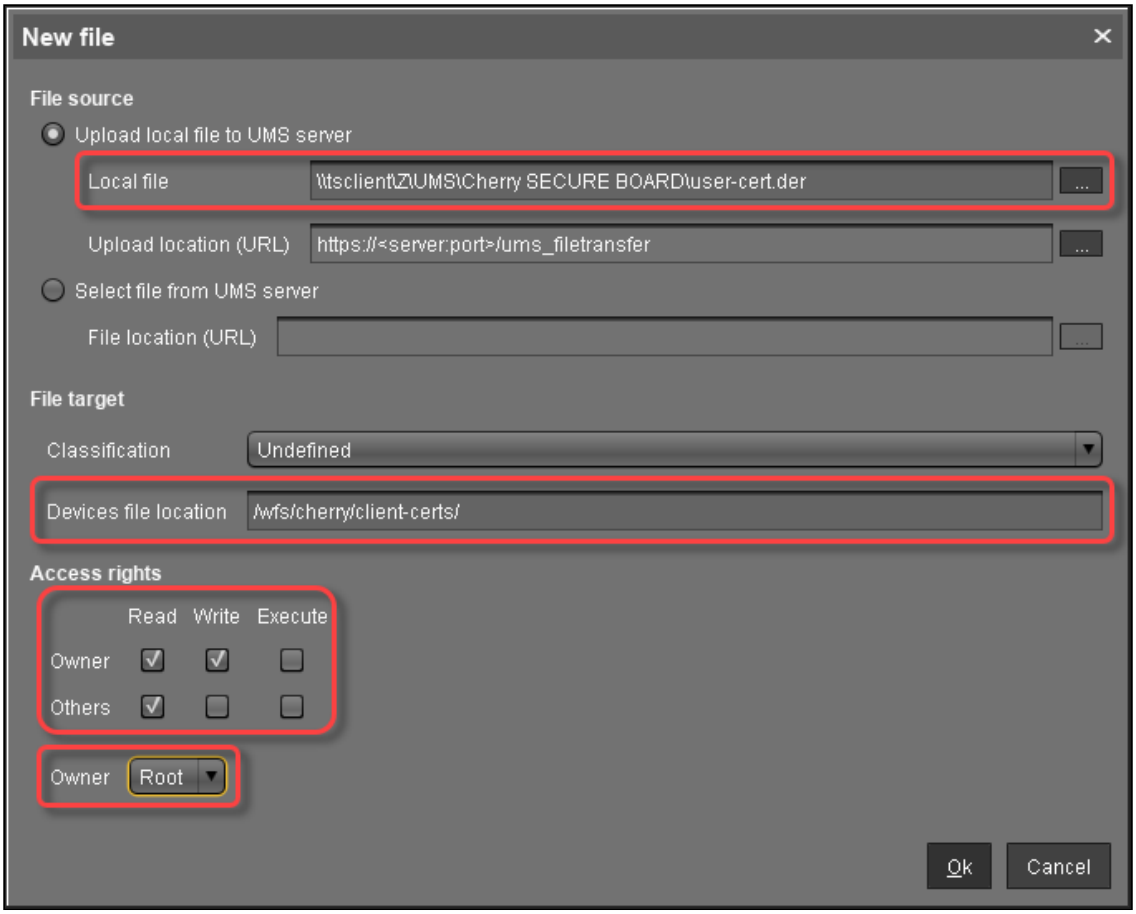
To transfer the certificate file `user-cert.der` to the directory `/wfs/cherry/client-certs/` on the personalization machine, proceed as follows:

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of `user-cert.der`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/client-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read

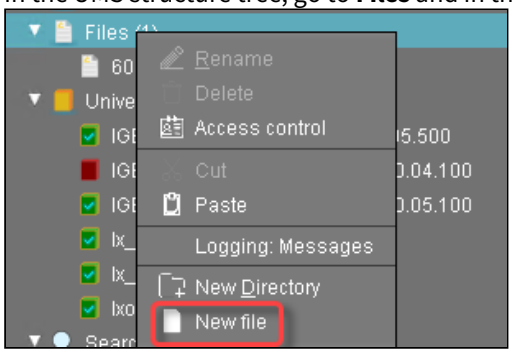
- **Owner**: Root



3. Click **Ok**.
   In the UMS, the file object **user-cert.der** is created.

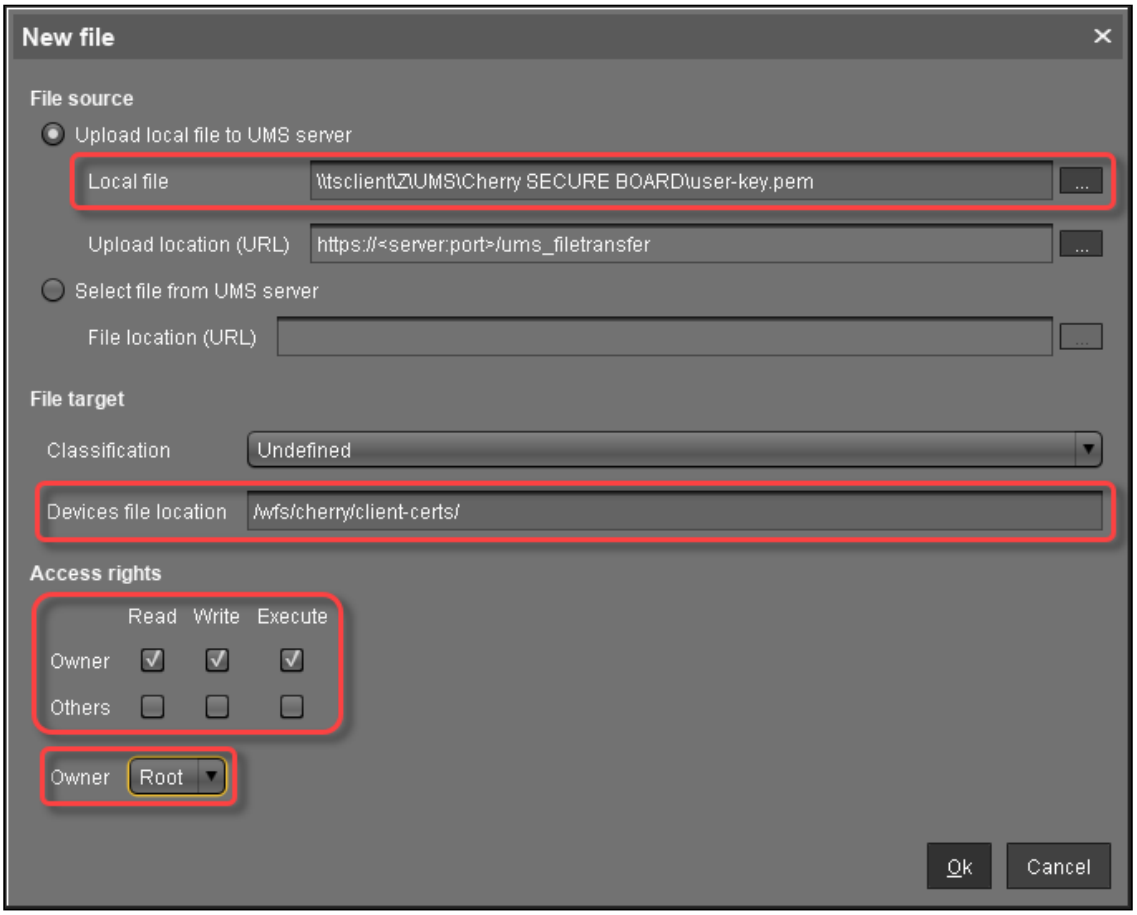
Creating the File Object for the User Key (Keyboard)

In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



1. In the **New file** dialog, configure the settings as follows:
2. **Local file**: Local file path of `user-key.pem`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/client-certs/`

- **Access rights - Owner**: Read, Write
- **Access rights - Others**: -
- **Owner**: Root



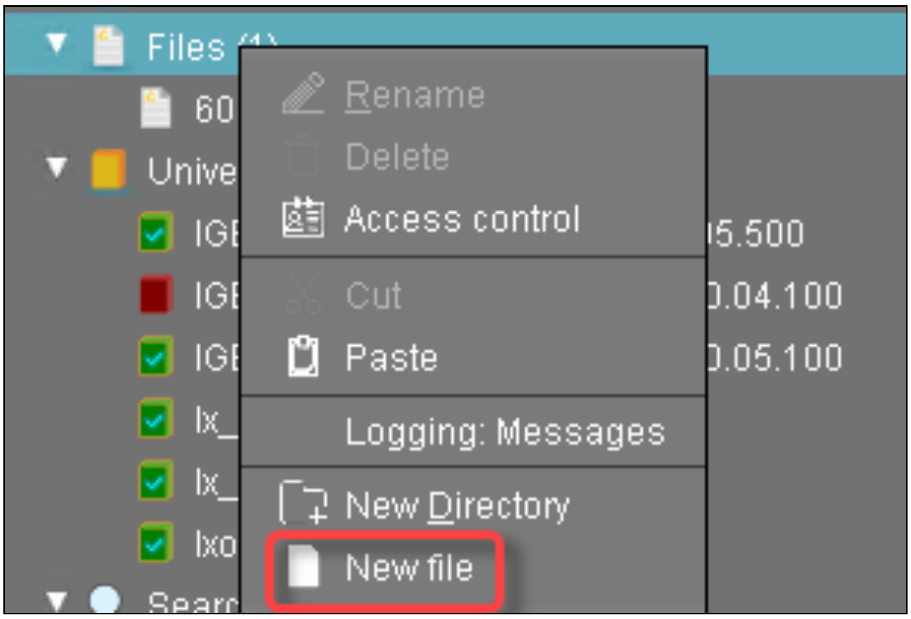
3. Click **Ok**.
   In the UMS, the file object **user-key.pem** is created.

Provisioning the Endpoints for Using the SECURE BOARD

The following instructions describe how to transfer the required certificates to the endpoints which will be connected to the SECURE BOARD in secure mode.

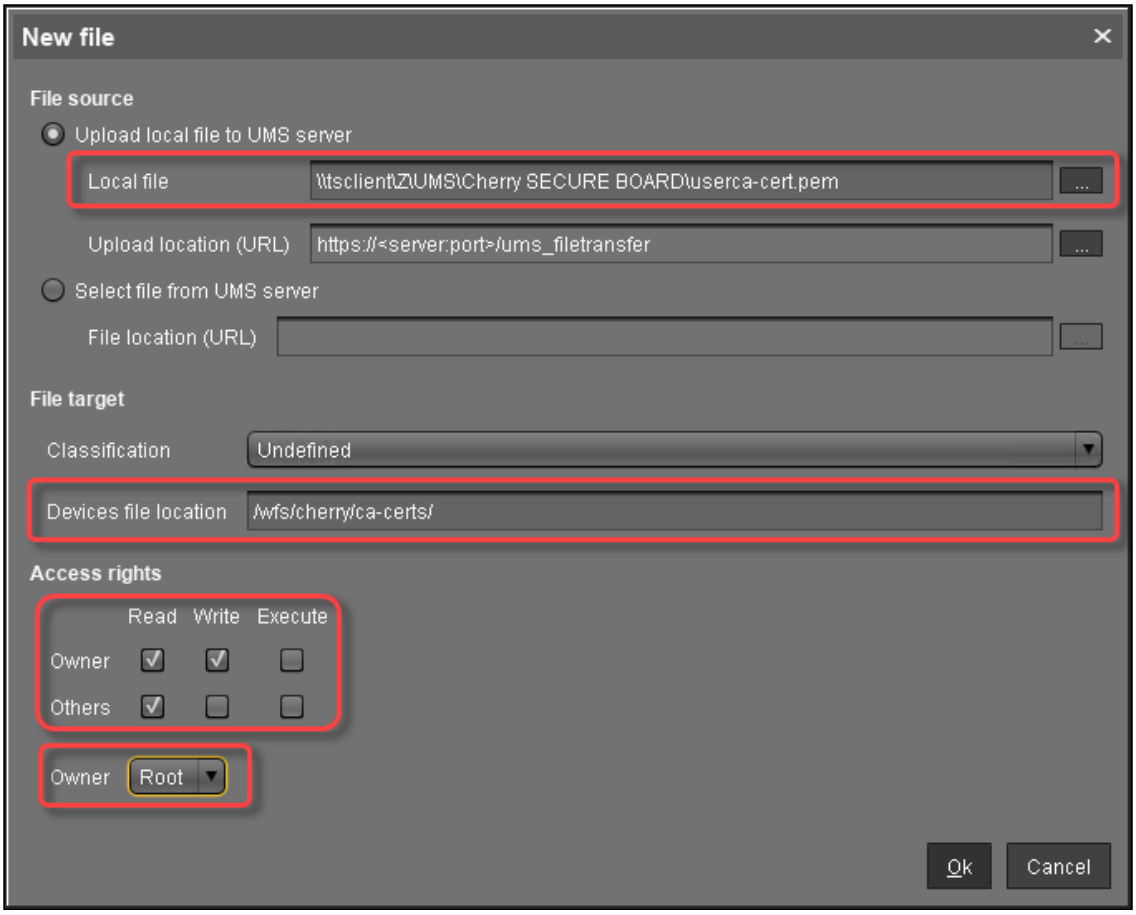
Creating the File Object for the User Root CA Certificate

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
    - **Local file**: Local file path of the certificate file. Use the file chooser by clicking ... .
    - **Device file location**: `/wfs/cherry/ca-certs/`
    - **Access rights - Owner**: Read, Write
    - **Access rights - Others**: Read

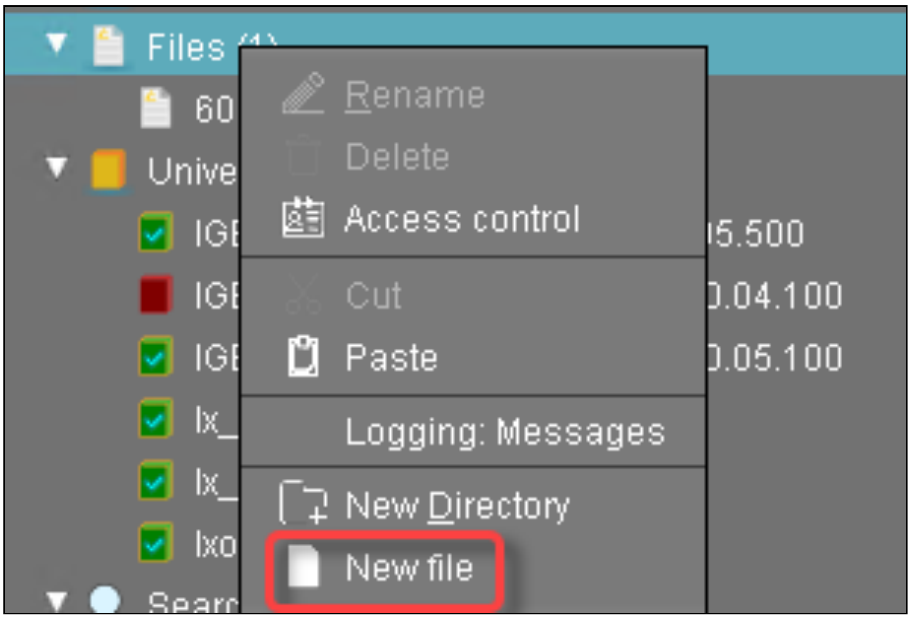
- **Owner**: Root



3. Click **Ok**.
   In the UMS, the file object is created. The name of the file object is derived from the file name.

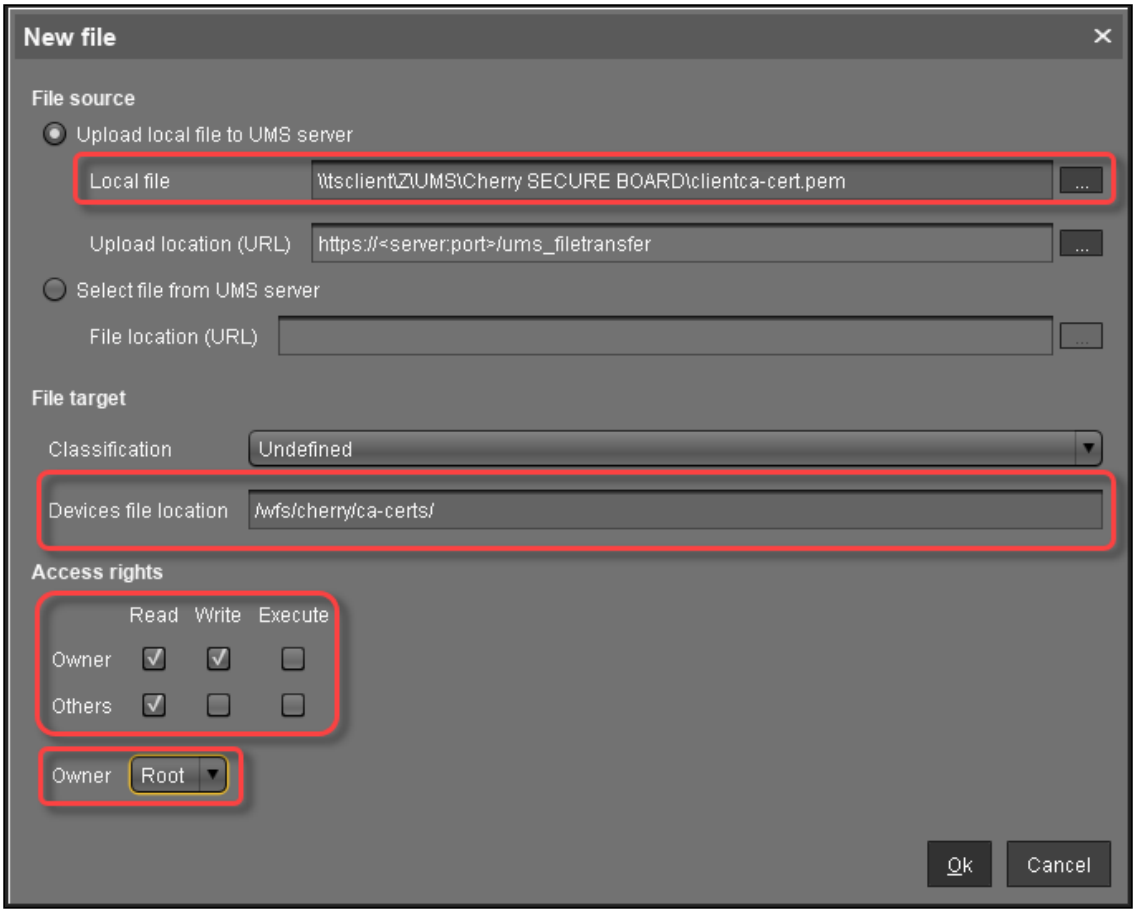
Creating the File Object for the Client Root CA Certificate (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of the certificate file. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/ca-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read

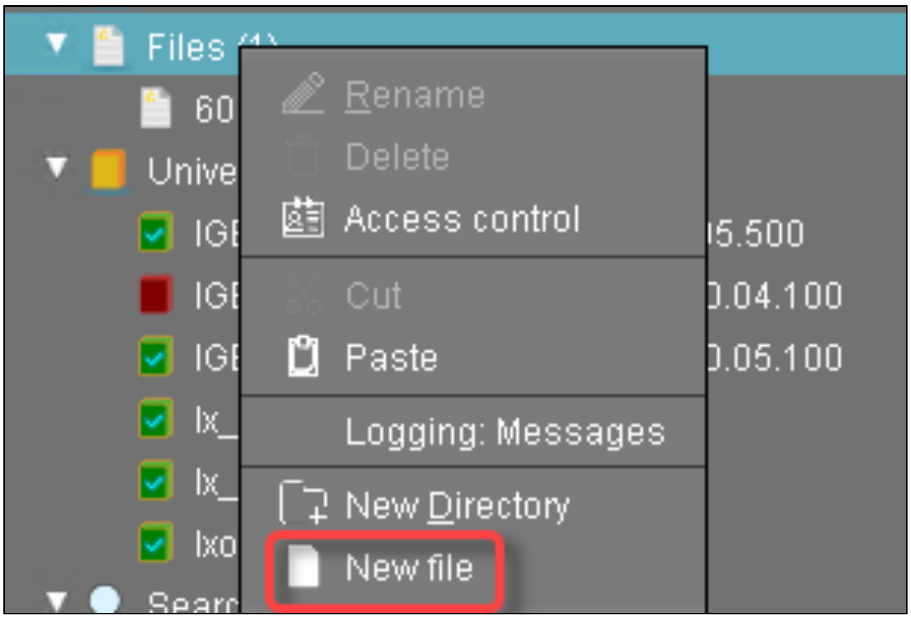
- **Owner**: Root



3. Click **Ok**.
   In the UMS, the file object is created. The name of the file object is derived from the file name.

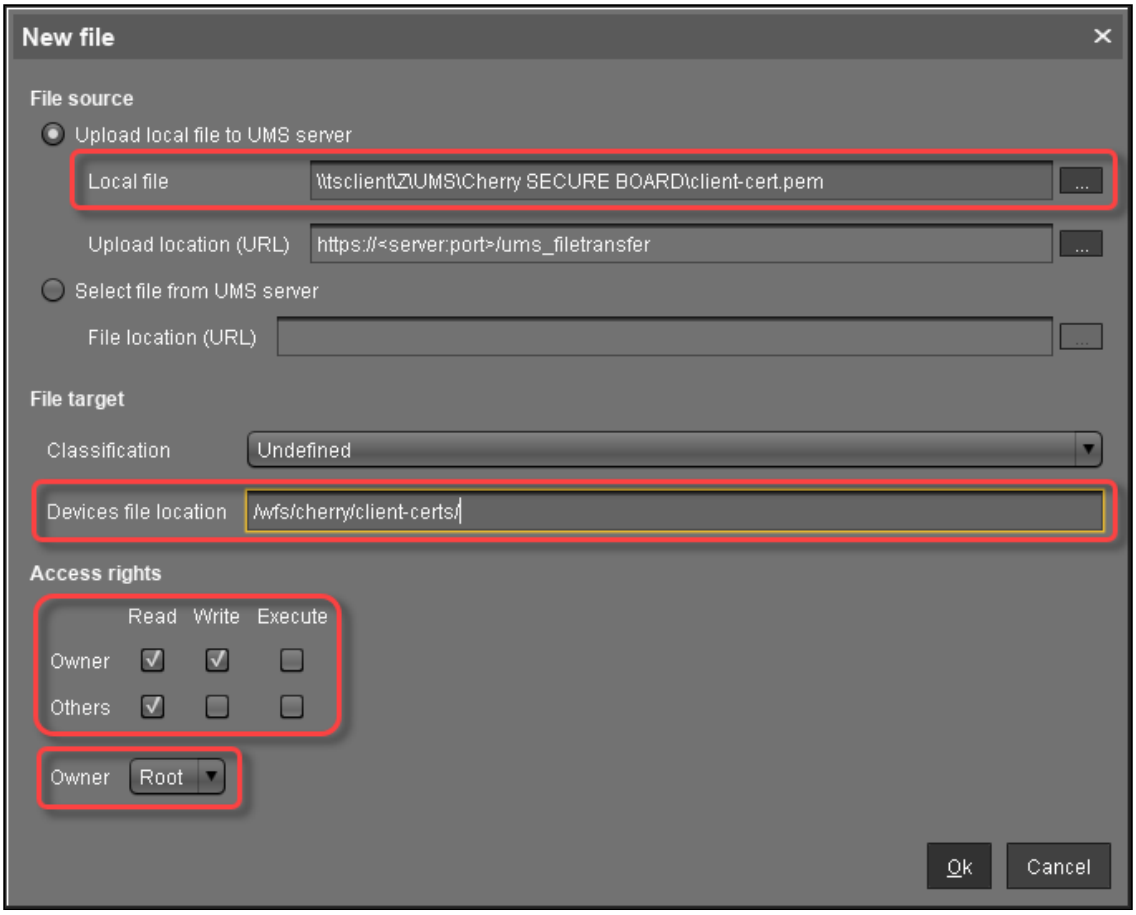
Creating the File Object for the Client Certificate (Endpoint) (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
3. **Local file**: Local file path of `client-cert.pem`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/client-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: Read

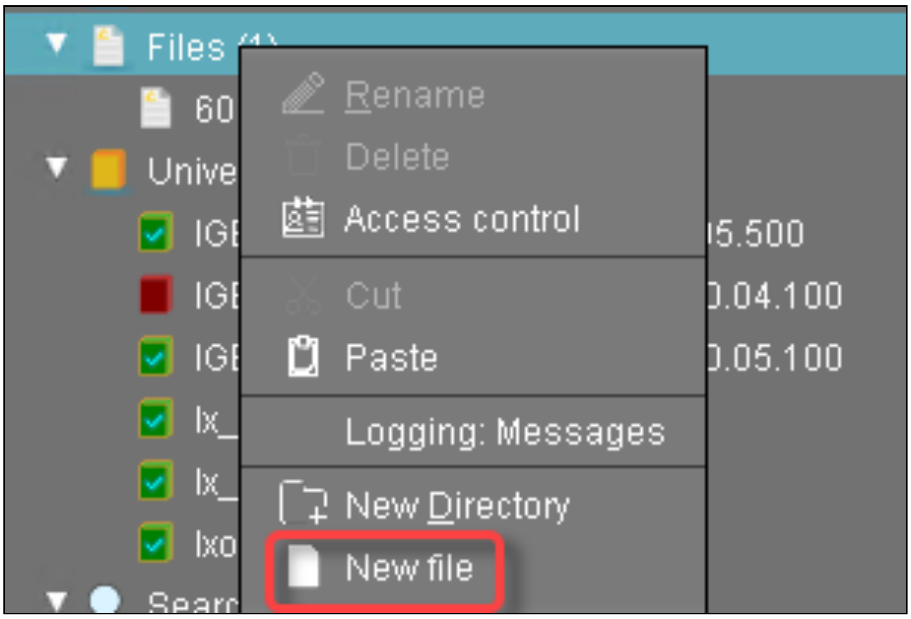
- **Owner**: Root



4. Click **Ok**.
   In the UMS, the file object is created. The name of the file object is derived from the file name.

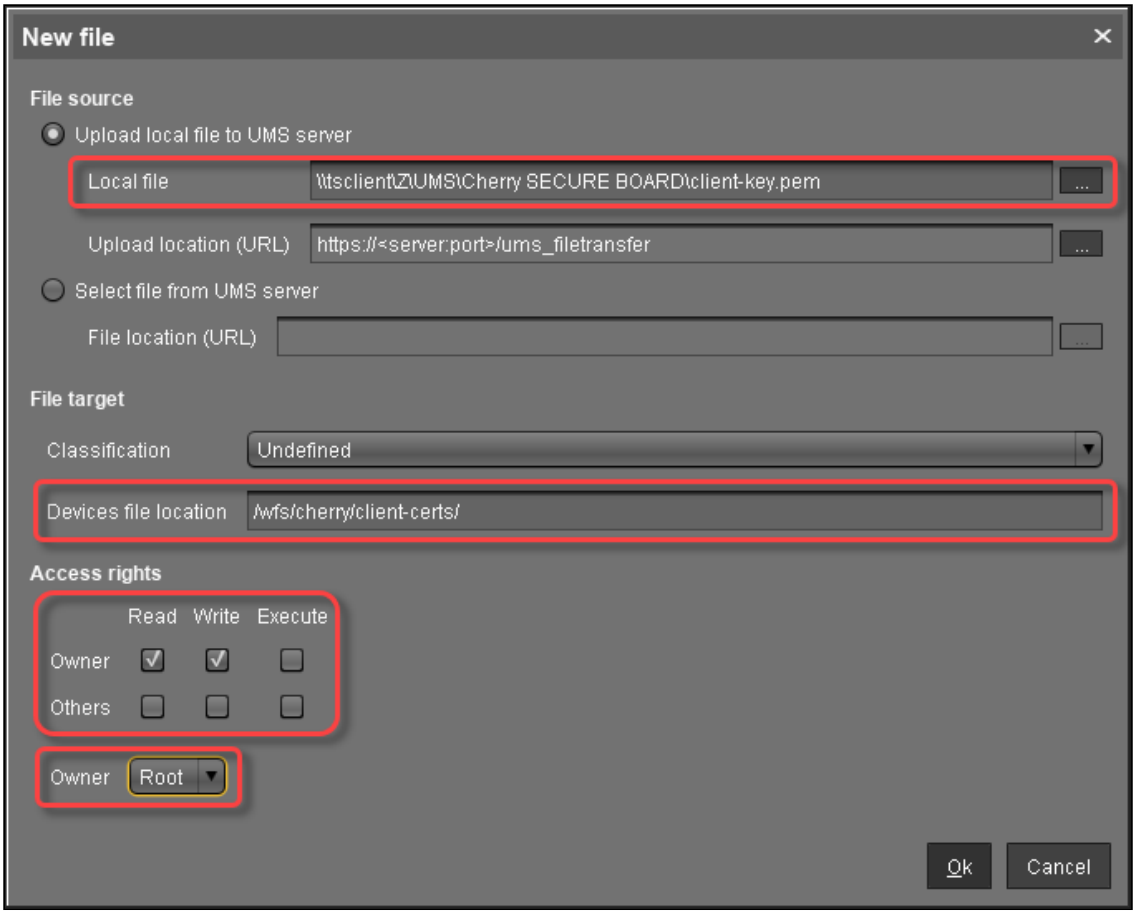
Creating the File Object for the Client Key (Endpoint) (Optional)

1. In the UMS structure tree, go to **Files** and in the context menu, select **New file**.



2. In the **New file** dialog, configure the settings as follows:
   - **Local file**: Local file path of `client-key.pem`. Use the file chooser by clicking ... .
   - **Device file location**: `/wfs/cherry/client-certs/`
   - **Access rights - Owner**: Read, Write
   - **Access rights - Others**: -

- **Owner**: Root



3. Click **Ok**.
   In the UMS, the file object is created. The name of the file object is derived from the file name.

Setting Up the Personalization Machine

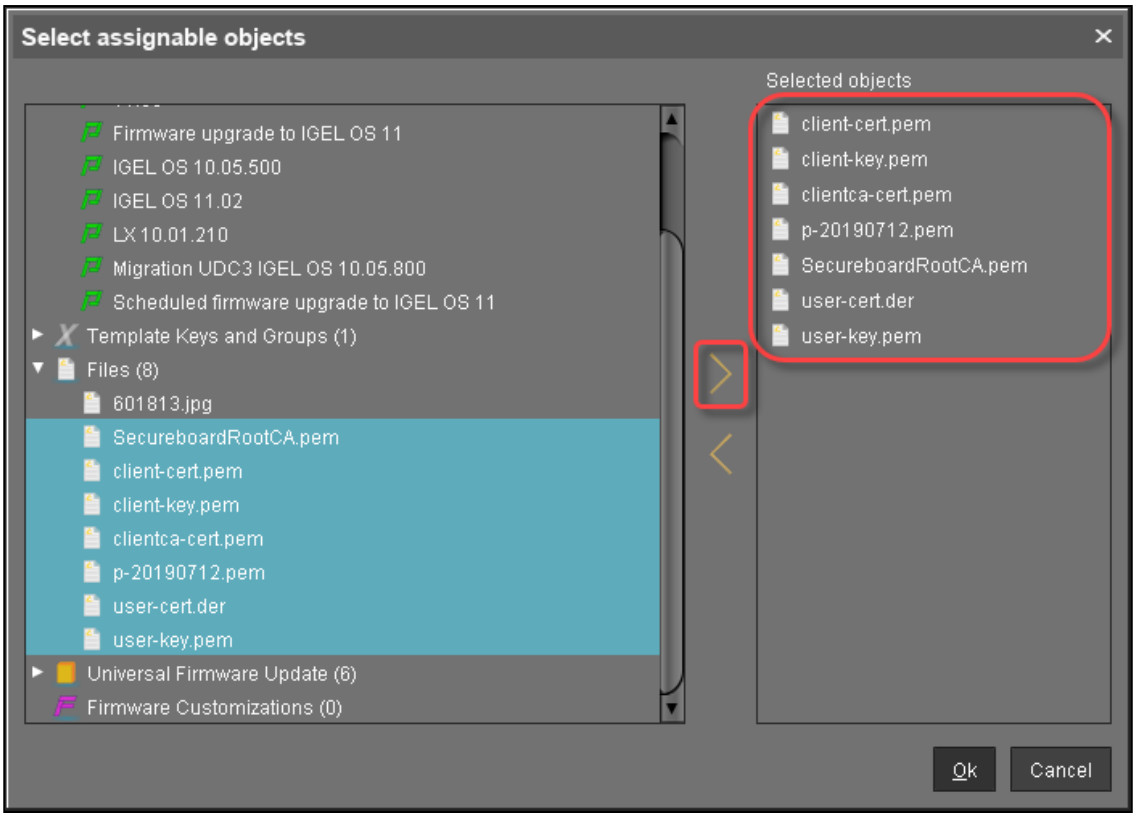
Setting Up the Local Terminal

If a local terminal session has already been configured on the designated personalization machine, you can skip this step.

1. Open the device's Setup and go to **Accessories >Terminals**.
2. Select .
3. Click **Ok**.
   On the desktop and in the Application Starter, a starter for the terminal session is created.

Assigning the File Objects to the Personalization Machine

1. In the UMS structure tree, select the endpoint that will act as the personalization machine.
2. In the **Assigned objects** area, click .
3. Under **Files**, select the file objects using the button:
   - **SecureboardRootCA.pem**
   - Device intermediate CA certificates; here: **p-20190712.pem**
   - **user-cert.der**
   - **user-key.pem**
   - **client-cert.pem** (optional)
   - **client-key.pem** (optional)
   - Device client CA certificate; here: **clientca-cert.pem** (optional)

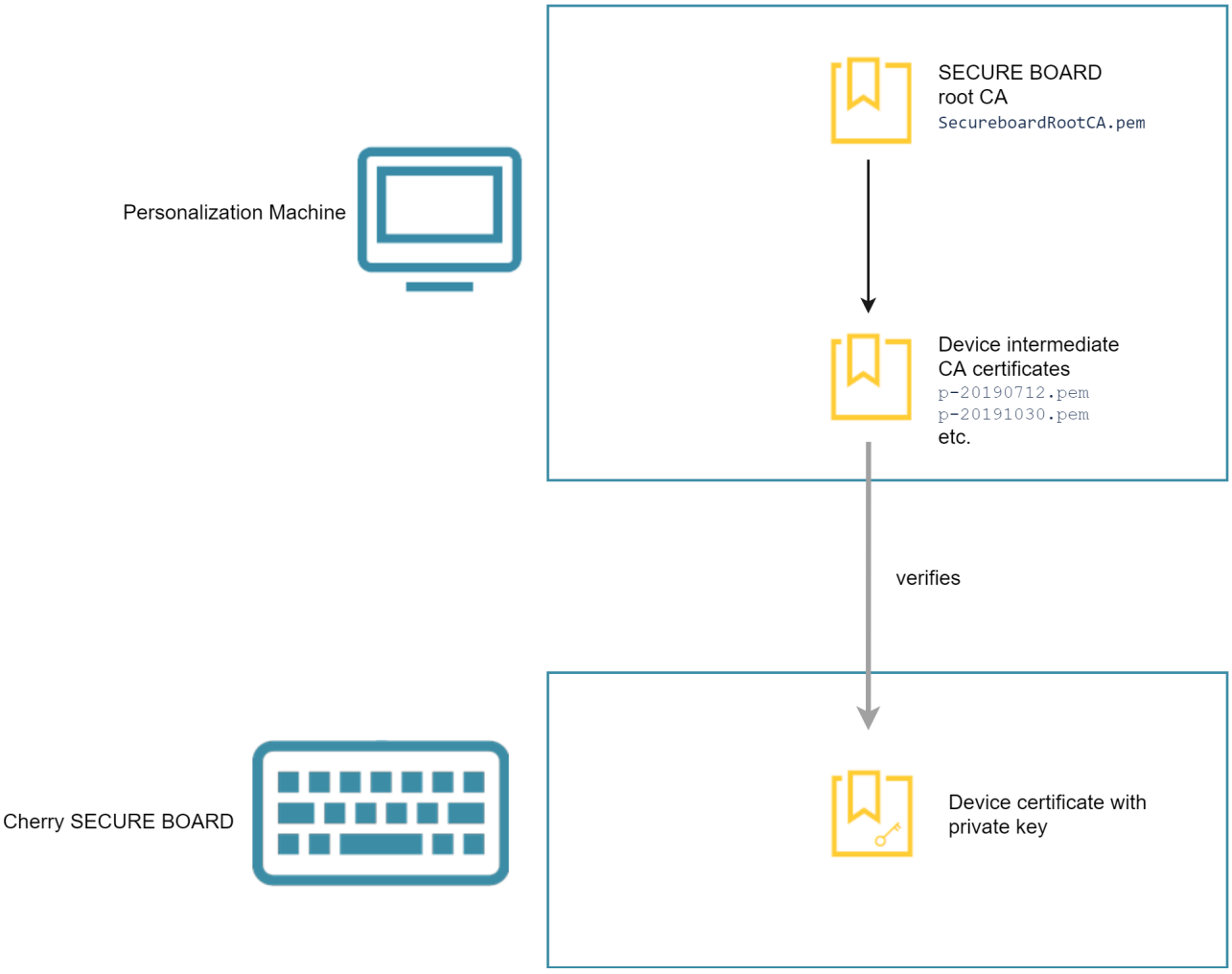


4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.
   The certificate and key files are transferred to the personalization machine. The personalization machine is ready for operation.

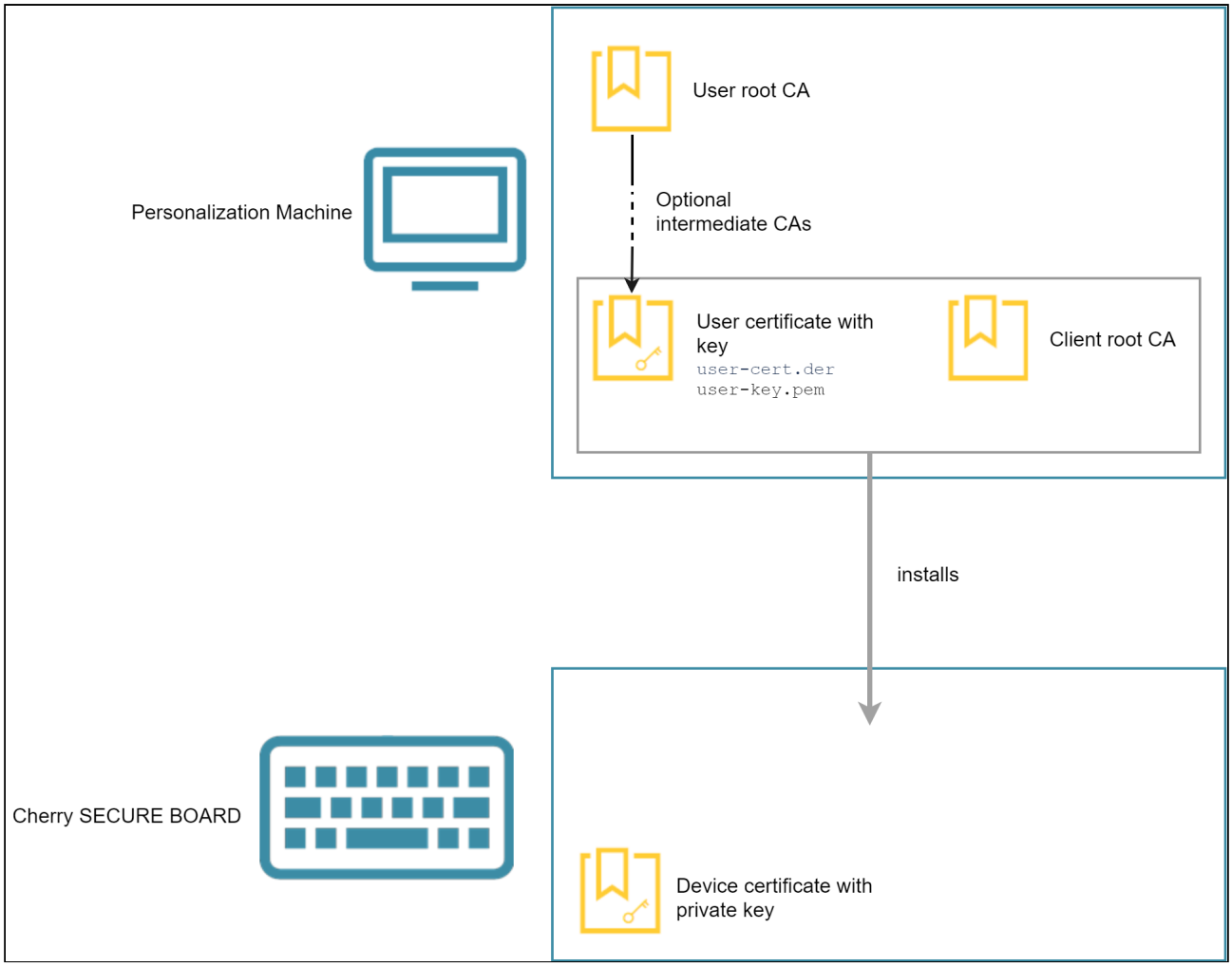
Personalizing the Cherry SECURE BOARD

Overview

Personalization Machine Verifies if the Keyboard Is a Genuine Cherry SECURE BOARD



Personalization Machine Installs the Certificates on the Keyboard

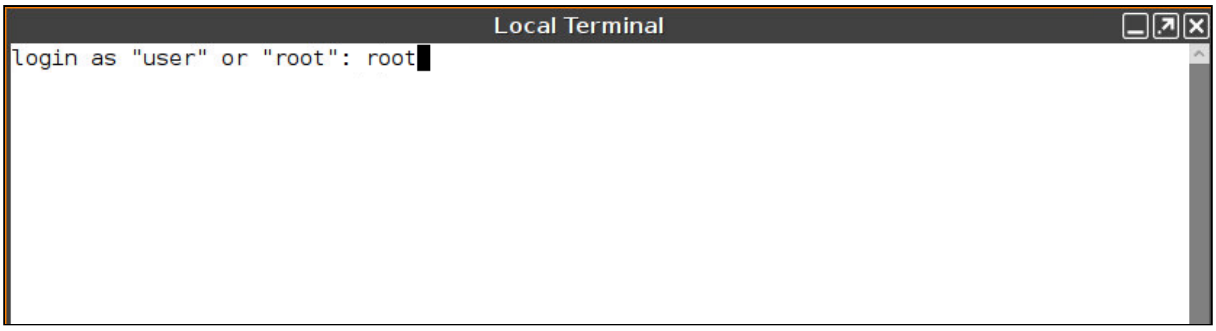


Prerequisites

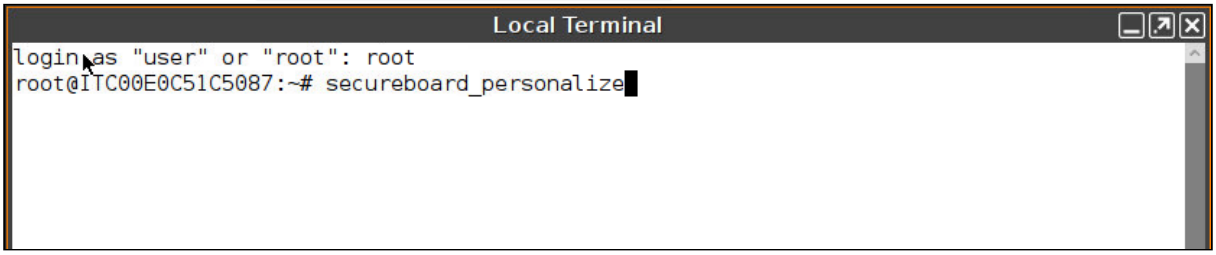
- The machine has been prepared as described under Setting Up the Personalization Machine (see page 1022).
- The Cherry SECURE BOARD keyboards are in factory state or have been reset (see Resetting the Cherry SECURE BOARD to Its Original State (see page 1033)).

Instructions

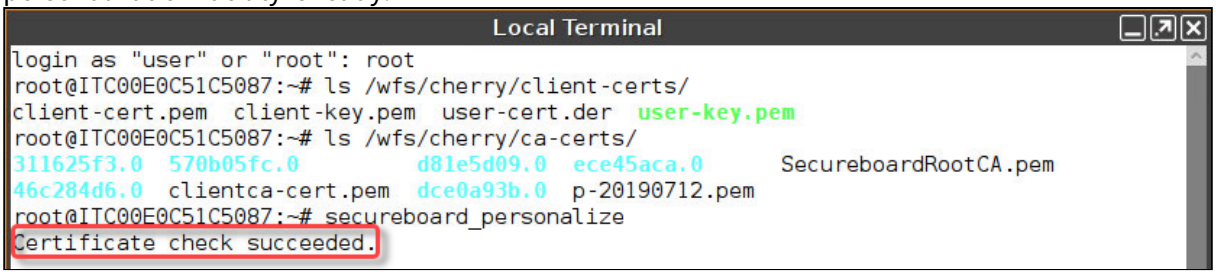
1. Start the local terminal and log in as `root`.



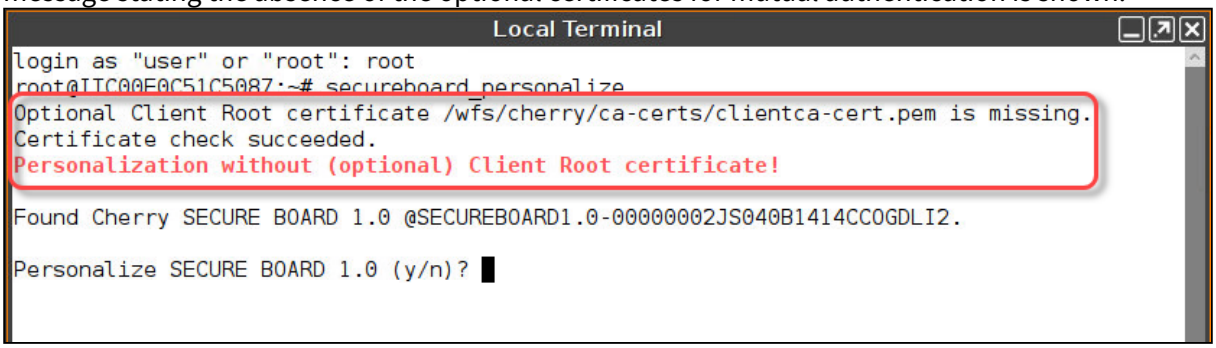
2. Enter the command `secureboard_personalize`



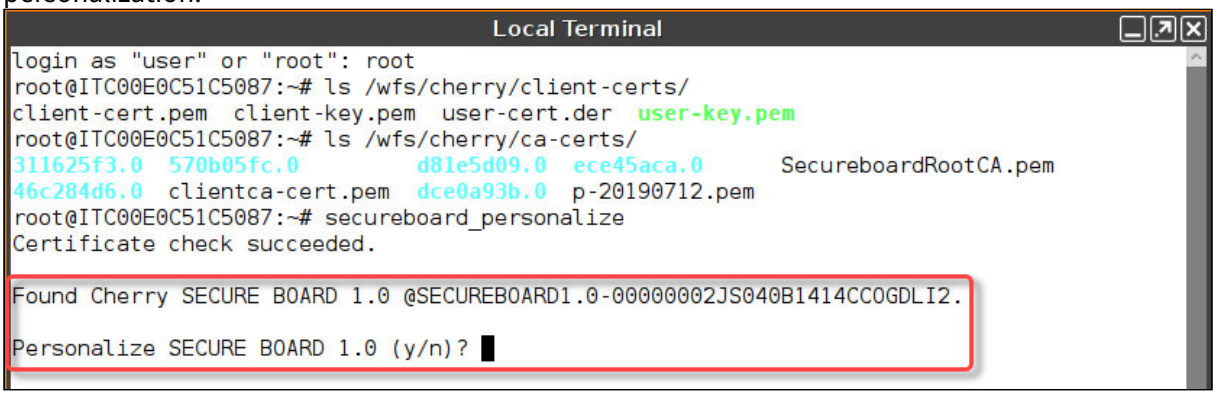
If all required certificates and the optional certificates for mutual authentication are present, the personalization facility is ready.



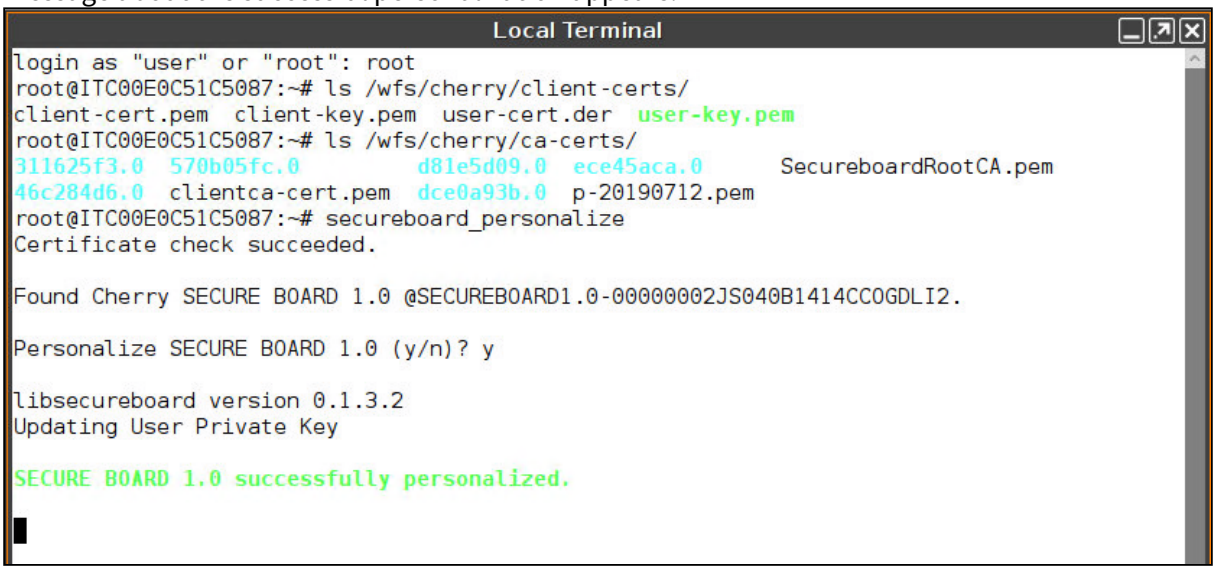
In case only the required certificates are present, the personalization facility is ready, but a message stating the absence of the optional certificates for mutual authentication is shown:



3. Plug in a Cherry SECURE BOARD.
   A message confirms that the keyboard has been detected; you are prompted to start the personalization.



4. Enter `y` to start the personalization process.
   During the personalization process, a few messages are shown. If everything has gone well, a message about the successful personalization appears.

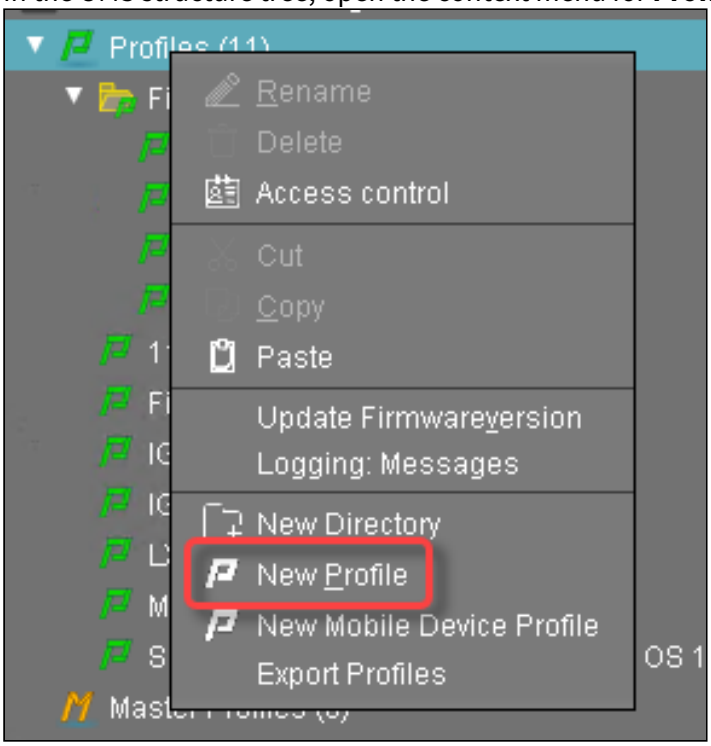


5. Unplug the personalized Cherry SECURE BOARD and proceed with the next Cherry SECURE BOARD.

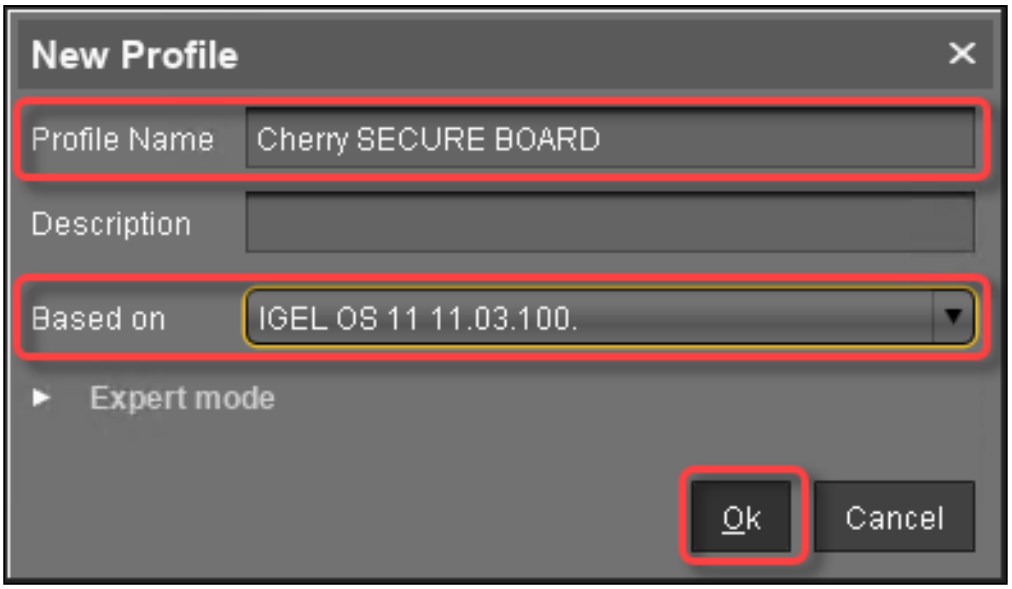
Setting Up the Endpoints

Creating a Profile for the Endpoints

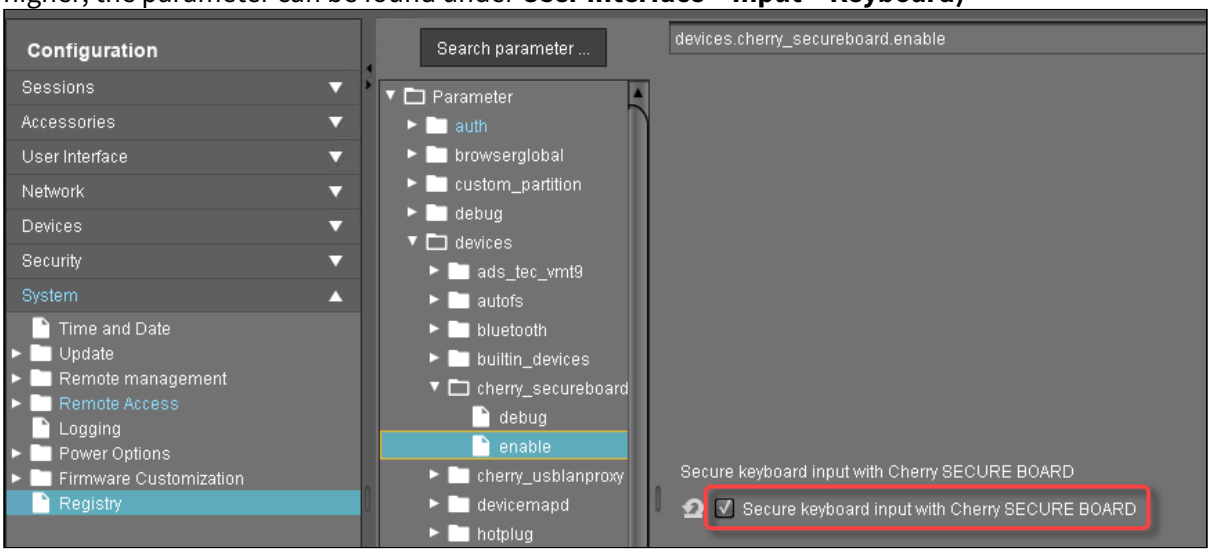
1. In the UMS structure tree, open the context menu for **Profiles** and select **New Profile**.



2. In the **New Profile** dialog, enter the required data and click **Ok**:
   - **Profile Name**: Name for the profile
   - **Based on**: Select the version of IGEL OS that is installed on your devices (IGEL OS 11.03.100 or higher).

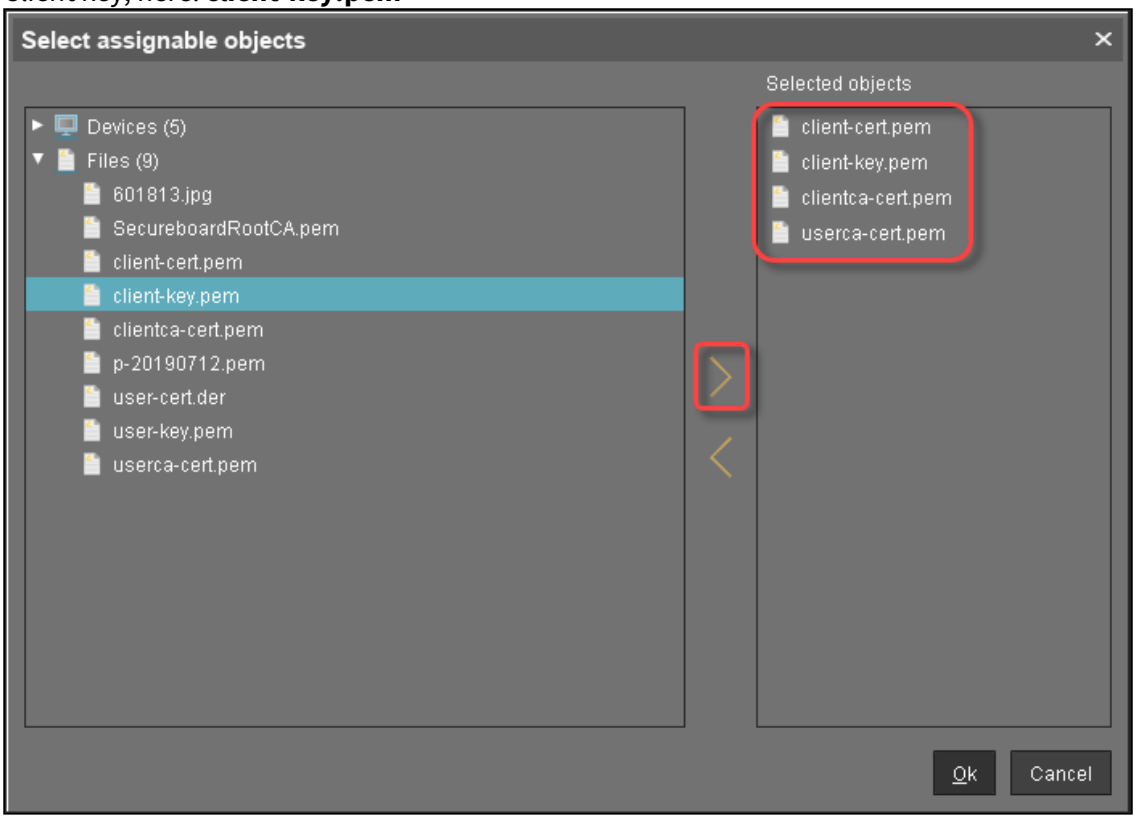


3. In the configuration dialog of the profile, go to **System > Registry > devices > cherry_secureboard > enable** and activate **Secure keyboard input with Cherry SECURE BOARD** (registry key: `devices.cherry_secureboard.enable`). (From UMS 6.03.130 or higher, the parameter can be found under **User Interface > Input > Keyboard)**



4. Click **Ok** to save and close the profile.
5. Make sure that the profile is selected in the UMS structure tree.
6. In the **Assigned objects** area, click .
7. Under **Files**, select the file objects using the button:
   - User root CA certificate; here: **userca-cert.pem**
   - Client root CA certificate; here: **clientca-cert.pem** (optional)
   - Client certificate; here: **client-cert.pem**

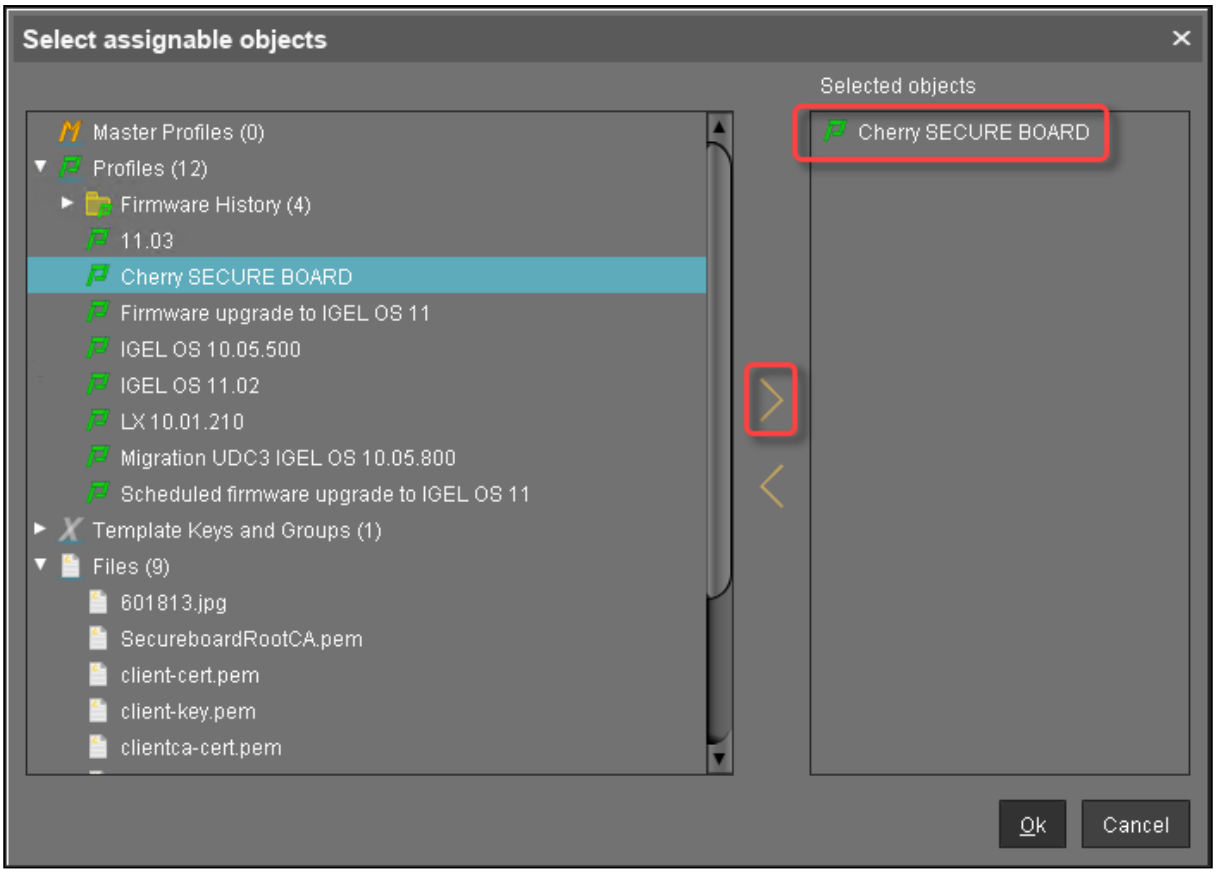
- Client key; here: **client-key.pem**



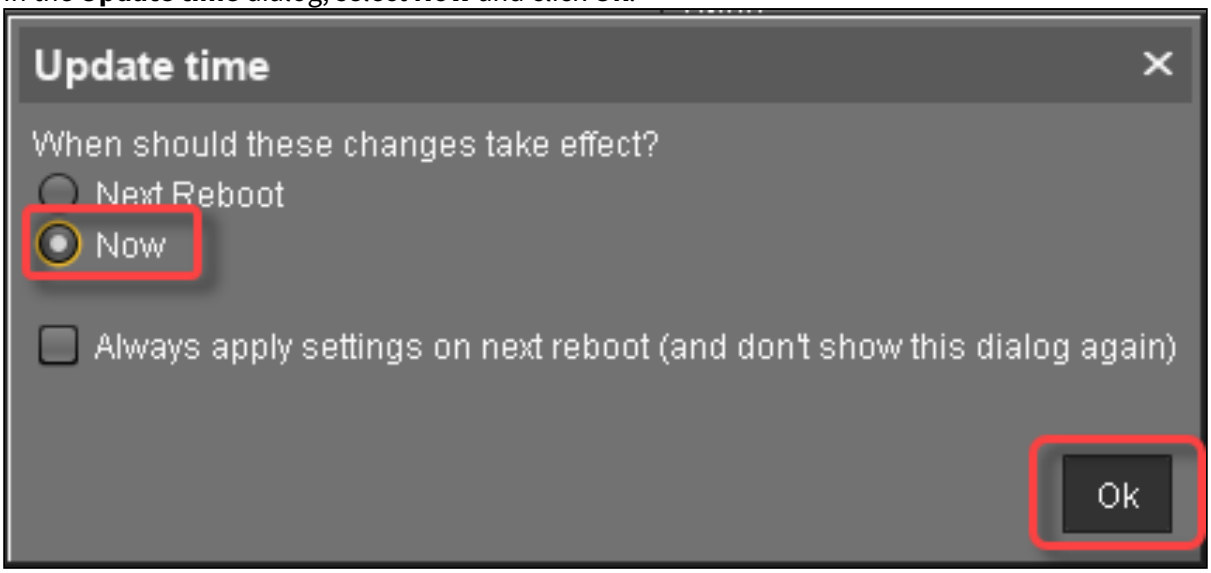
8. Click **Ok**.
9. In the **Update time** dialog, select **Now** and click **Ok**.
   The certificate and key files are assigned to the profile.

Assigning the Profile to the Endpoints

1. In the UMS structure tree, select the devices that are to be connected to the Cherry SECURE Board keyboards.
2. In the **Assigned objects** area, click .
3. Under **Profiles**, select the appropriate profile using the button.



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.

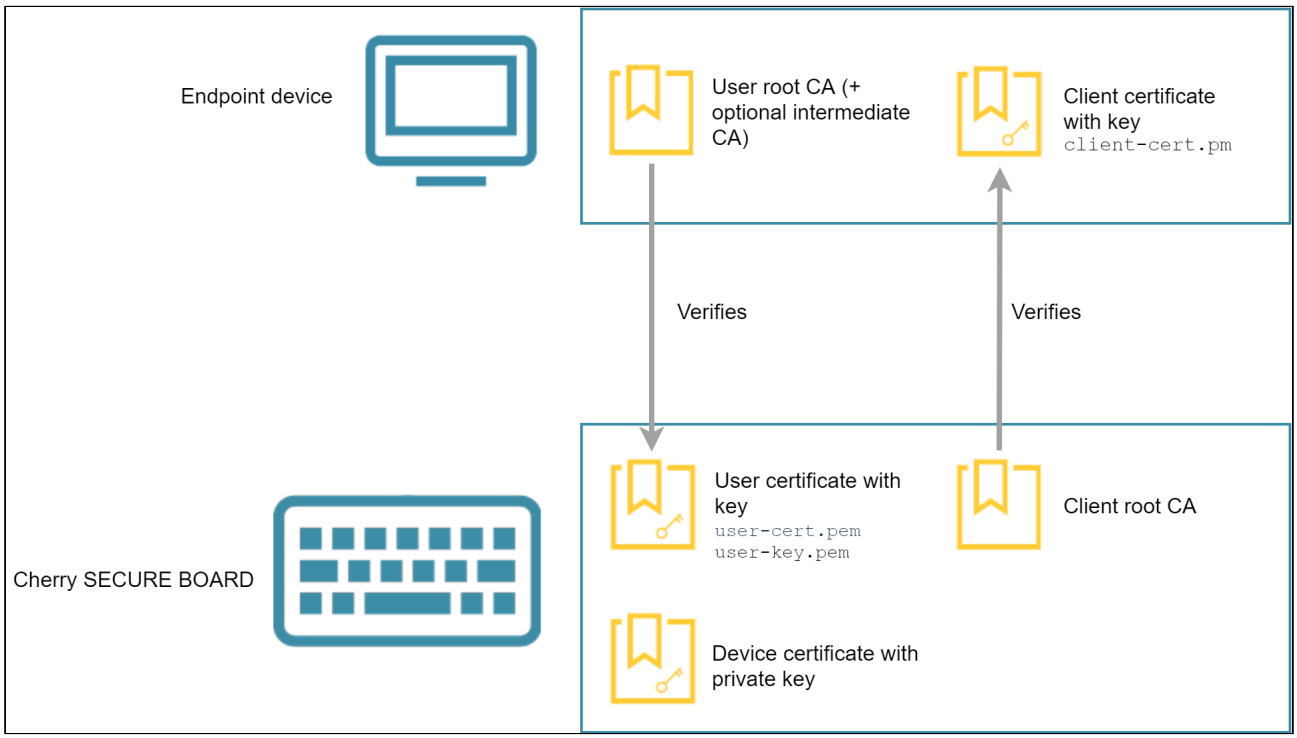


The settings and certificate and key files are transferred to the endpoints. The endpoints are ready for connecting to the Cherry SECURE BOARD keyboards.

Operation

The endpoint verifies if the Cherry SECURE BOARD has the right certificates. When the optional client certificates have been installed, too, the Cherry SECURE BOARD verifies if the endpoint has the right certificates. When everything went well, the endpoint and the Cherry SECURE BOARD work in secure mode.

On the keyboard side, the secure mode is indicated by the red light next to the lock symbol. On the endpoint side, the secure mode is indicated by an icon on the system tray.



Resetting the Cherry SECURE BOARD to Its Original State

To reset the Cherry SECURE BOARD to its factory settings:

1. Disconnect the keyboard from the endpoint.
2. Hold the keys [D], [J] and [RGUI] (right Windows key) and, at the same time, connect the keyboard to the endpoint.
   When the reset has been successful, all LEDs flash for about 1 second. After that, the keyboard starts normally, and the certificate store is emptied. The keyboard can be personalized again.

Webcam Redirection and Optimization in IGEL OS

This article provides an overview and best-practice recommendations for the use of webcams in IGEL OS within remote sessions such as Citrix, VMware Horizon, and RDP.

Overview

In general, webcam support in IGEL OS can be divided into three categories:

Unoptimized	The raw data from the webcam is sent over the network via USB redirection. The raw data from the webcam is highly affected by network latency between the client and the server and takes up a lot of bandwidth, requires the correct drivers on the server-side, increases the server's CPU and RAM load. Example: **Native USB Redirection** for RDP sessions
Optimization type 1	In this case, the video and audio data is compressed on the client side. This optimization type makes the webcam stream far more efficient and reliable, although the data stream must still pass via the VDI server in addition to the cloud servers of the particular communication software (Teams, Zoom, etc.). Examples: **HDX RealTime Webcam redirection** for Citrix sessions, **Real Time Audio Video (RTAV)** for VMware Horizon sessions
Optimization type 2	In this case, the video and audio data is also compressed on the client side. However, unlike type 1, this optimization type offloads the data stream from the VDI server and sends it *directly* to Teams/Zoom/etc. in the cloud, i.e. "single-hop". This allows for the best performance and also removes the server load, but relies on the correct optimization pack being present on the client and is specific to each communication suite. It may also require a more complex network configuration because the endpoint has to be able to communicate directly with the communication cloud server and not only the VDI server. Examples: **Microsoft Teams optimization** and **Zoom Media plugin** for Citrix sessions

⚠ In the case of optimization type 1 or type 2, it is important to ensure that the agent/component on the server side is installed and is compatible with the client-side version. For details on the latter, see the "Component Versions" section of the IGEL OS release notes (see page 2282).

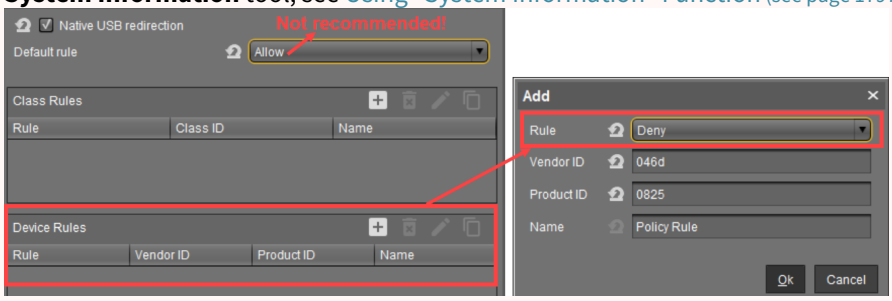
General Recommendations

For optimal performance of webcams in IGEL OS, the correct optimization pack has to be enabled for the specific application, e.g. **Microsoft Teams optimization**, **Zoom VDI Media plugin**, **Cisco Webex VDI**, etc. However, optimization packs are not available for all session types.

USB Redirection

If no optimization pack exists for your session type or the optimization pack available does not function correctly, you can try to use USB redirection – either the **Native USB Redirection** or the less frequently used **Fabulatech USB Redirection** (not both together), – but ONLY as a LAST RESORT, when no other solution is possible.
In general, where USB redirection is available as an option inside the VDI session options, it should be disabled for the webcam devices.

- Set **Default rule** to **Deny**
- OR, if the **Default rule** is **Allow** (NOT recommended), go to **Device Rules** and add **Deny** rules for the specific Vendor ID and Product ID of the webcam.
  How to Find Out Vendor and Product IDs
  To get Vendor/Product IDs, use the command `lsusb` in the terminal. You can also use the **System Information** tool, see Using "System Information" Function (see page 1797).



This is necessary because USB redirection will block the webcam from being correctly optimized (if optimization is possible).

Do not forget to check and adjust settings and policies on the server side. Otherwise, your webcam may not work, even if all settings in the IGEL OS are configured correctly.

Always check the IGEL OS release notes (see page 2282) for specific remarks, especially in the case of private builds (*IGEL Subscription and More > General Product Information > Software Release Overview > Versioning Scheme for IGEL OS 11 to IGEL OS 12.01)*. Always try to use the latest firmware, see IGEL download server[112].

In certain cases, some of the settings described later on in this article may not be visible even though you have selected the correct firmware version for the profile in the UMS. In this case, update the UMS to the latest version.

112. https://www.igel.com/software-downloads/workspace-edition/

Citrix

Option 1: Unified Communications (Best Choice)

Microsoft Teams Optimization	Path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions > Microsoft Teams optimization** (see page 1281) (enabled by default) • Available as of IGEL OS version 11.04.100. • Depends on the version of Citrix Workspace App used. For best results, the latest version should be preferred. For the Citrix Workspace App versions included, see IGEL OS release notes (see page 2282). For server-side requirements for Microsoft Teams optimization, see Microsoft Teams installation[113]. To troubleshoot Microsoft Teams optimization in Citrix, see: • Troubleshooting HDX Optimization for Microsoft Teams[114] • Peripherals in Microsoft Teams[115]
Zoom VDI Media Plugin	Path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions > Zoom VDI Media Plugin** (see page 1281) • Available as of IGEL OS version 11.04.100 • For the Zoom VDI Media Plugin versions included, see IGEL OS release notes (see page 2282). • As of IGEL OS 11.06, you can change the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection**. For more information about Zoom Media Plugin, including server-side requirements, see Getting started with VDI[116].

113. https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-teams-installation
114. https://support.citrix.com/article/CTX253754
115. https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#peripherals-in-microsoft-teams
116. https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI

Cisco Webex Meetings VDI / Cisco Webex VDI	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco > Cisco Webex Meetings VDI** or **Cisco Webex VDI** (see page 1281) • Available as of IGEL OS version 11.04.100 • For the Cisco Webex Meetings VDI / Cisco Webex VDI versions included, see IGEL OS release notes (see page 2282). • As of IGEL OS 11.06, you can change the Cisco Webex Meetings VDI client version under **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection**. For more information about Cisco Webex products for VDI, including supported environments, see: • Cisco Webex Meetings Virtual Desktop Software[117] • Overview of Webex App for VDI[118]
Cisco JVDI Client	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco > Cisco JVDI client** (see page 1281) • For the Cisco JVDI client versions included, see IGEL OS release notes (see page 2282). For more information about Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0[119].
Skype for Business	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business > HDX RealTime Media Engine** (see page 1281) (enabled by default) • Skype for Business webcam redirection relies on the **Citrix HDX Realtime Media Engine** (client-side counterpart to the Lync Optimization Pack). • This setting is the same as **Sessions > Citrix > Citrix Global > HDX Multimedia > HDX RealTime Media Engine**. **IMPORTANT:** Skype for Business Online will be retired by Microsoft on July 31, 2021[120]. After this, it will no longer be available, and Microsoft Teams must be used instead.

117. https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software
118. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html
119. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html
120. https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833

Option 2: HDX RealTime Webcam Redirection (Should Only Be Used If Optimization Packs under Option 1 Are Not Applicable)

For other VDI programs which require the use of a webcam (e.g. the browser), HDX RealTime Webcam redirection (see page 1276) can be used. This option enables the compression of audio and video on the client side, which is redirected to an HDX virtual webcam on the server side. It also allows for the resolution of the webcam to be defined manually.

> ⚠ Only One Option at a Time for a Particular Device
>
> - **HDX RealTime Webcam redirection** and **HDX RealTime Media Engine (Skype for Business)** should not be enabled at the same time.
> - If you use HDX or an application-specific optimization pack (e.g. **Zoom VDI Media plugin**), **Native USB Redirection / Fabulatech USB Redirection** should be disabled.

Settings on the Server Side	Settings on the Client Side
The following policy settings must be enabled: • Multimedia conferencing (enabled by default) • Windows Media Redirection (enabled by default) For details, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/webcam-compression.html.	1. Go to **Sessions > Citrix > Citrix Global > HDX Multimedia**. 2. Enable **Multimedia redirection** (enabled by default). 3. Enable **HDX RealTime Webcam redirection**. 4. Configure the webcam resolution, 352 x 288 by default, and other settings if required. ⚠ Certain webcam models may only support specific resolutions. 5. If the USB redirection is enabled (not recommended), use **Device Rules** to forbid the forwarding of the webcam via USB redirection. See the section above (see page 1035).

Dependencies

- **HDX RealTime Webcam Redirection** is supported for 32-bit applications on the server side (limitation of Citrix Receiver/Workspace App for Linux). Deploy a 32-bit browser to verify the webcam redirection online, e.g. www.webcamtests.com[121]. See also https://support.citrix.com/article/CTX223199.

  Webcam redirection for 64-bit apps is supported as of CWA 2203; for the configuration, see https://virtualbrat.com/2023/02/23/citrix-hdx-webcam-redirection-for-64-bit-applications-how-to-guide/.

121. http://www.webcamtests.com

Before that, it was not in general availability phase, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#webcams.

- Webcam redirection generally works with or without **HDX RealTime Media Engine (RTME)**. However, to avoid conflicts and for the better performance of webcam redirection, disabling **RTME** (enabled by default) is highly recommended.
- Webcam usage is limited to one application. For instance, when Skype is running with a webcam and GoToMeeting is started, you have to exit Skype to use the webcam with GoToMeeting.

Supported Video Conferencing Applications

- Adobe Connect
- Cisco Webex and Webex for Teams (Give preference to the optimization pack for Cisco Webex Meetings / Teams VDI instead, see above (see page 1036))
- GoToMeeting
- Google Hangouts and Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015, 2016, and 2019 (Give preference to the optimization pack for Skype for Business instead, see above (see page 1036))
- Microsoft Lync 2010 and 2013
- Microsoft Skype 7 or higher
- Media Foundation-based video applications on Windows 8.x or higher and Windows Server 2012 R2 and higher

HDX RealTime Webcam Redirection is NOT supported for Microsoft Teams. Use **Microsoft Teams optimization** instead, see above (see page 1036).

Does Webcam Audio Work but Video Doesn't?

->Try to increase the graphics memory in the BIOS to 512 MB.

For more detailed information about HDX RealTime Webcam, see:

- https://support.citrix.com/article/CTX132764
- https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#webcams

VMware Horizon

Option 1 (Best Choice)

Microsoft Teams Optimization	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions > Microsoft Teams optimization** (see page 1393) (enabled by default) • Available as of IGEL OS version 11.06.100 For more information about Microsoft Teams, see Microsoft Teams Optimization with VMware Horizon[122] and Configuring Media Optimization for Microsoft Teams[123].
Zoom VDI Media Plugin	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions > Zoom VDI Media Plugin** (see page 1393) • For the Zoom VDI Media Plugin versions included, see IGEL OS release notes (see page 2282). • As of IGEL OS 11.06, you can change the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection**. ⚠ Zoom Media Plugin will NOT function if you enable **HTML5 multimedia redirection** (**Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**, enabled by default). For more information about Zoom VDI Media Plugin, including server-side requirements, see Getting started with VDI[124].

122. https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon
123. https://docs.vmware.com/en/VMware-Horizon/2106/horizon-remote-desktop-features/GUID-F68FA7BB-B08F-4EFF-9BB1-1F9FC71F8214.html
124. https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI

Cisco Webex Meetings VDI / Cisco Webex VDI	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco > Cisco Webex Meetings VDI** or **Cisco Webex VDI** (see page 1393) • For the Cisco Webex Meetings VDI / Cisco Webex VDI versions included, see IGEL OS release notes (see page 2282). • As of IGEL OS 11.06, you can change the Cisco Webex Meetings VDI client version under **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection**. For more information about Cisco Webex products for VDI, including supported environments, see: • Cisco Webex Meetings Virtual Desktop Software[125] • Overview of Webex App for VDI[126]
Cisco JVDI Client	Path: **Sessions > Horizon Client > Horizon Client Global> Unified Communications > Cisco > Cisco JVDI client** (see page 1393) • For the Cisco JVDI client versions included, see IGEL OS release notes (see page 2282). For more information about Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0[127].
Skype for Business	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business > Virtualization Pack Skype for Business** (see page 1393) (enabled by default) **IMPORTANT:** Skype for Business Online will be retired by Microsoft on July 31, 2021[128]. After this, it will no longer be available, and Microsoft Teams must be used instead.

Option 2: Real-Time Audio-Video (RTAV)

Real-time Audio-Video (RTAV) is the optimization pack for audio and video calls inside VMware Horizon sessions. RTAV compresses audio and video on the client side and sends it to the Horizon server, where a VMware Virtual Webcam instance is created.

125. https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software
126. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html
127. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html
128. https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833

Like for Citrix sessions, USB redirection should be disabled if RTAV is to be used.

->Enable **Sessions > Horizon Client > Horizon Client Global > Multimedia > Real Time Audio Video (RTAV)** (see page 1389).

RTAV is only available when connecting via PCoIP or VMware Blast.

Note that only one webcam will be redirected (limitation of Horizon client for Linux). If multiple webcams are available on the client, the preferred webcam can be defined in the IGEL Setup under **System > Registry > vmware.view.rtav-webcam-id**. For details, see Select a Preferred Webcam or Microphone on a Linux Client System[129].

For more information about RTAV, see Configuring Real-Time Audio-Video[130].

Microsoft Teams

Microsoft Teams can be used with RTAV in "Fallback Mode". This configuration is not an optimal solution as the data makes multiple hops between the Horizon client, server, and Microsoft Teams server. For more information, see Configuring Microsoft Teams with Real-Time Audio-Video[131].
Microsoft Teams media optimization (single-hop or "Optimized Mode") in Horizon sessions is currently only supported with the Horizon client for Windows 10 in conjunction with Horizon 8 (2006). For more information, see Microsoft Teams Optimization with VMware Horizon[132].

RDP

There is currently no optimization available for webcam redirection in RDP sessions. It may be possible to redirect webcams via USB redirection, e.g. **Native USB Redirection**. However, each webcam has to be individually tested for if it functions with this method. It often depends on the webcam itself and its Windows driver whether they can cope with the higher latencies that occur with USB redirections compared to the real USB bus.

In some situations, webcams may not be redirected correctly due to network latency, bandwidth limitations, or the lack of compatible drivers on the server.

Unoptimized Webcam Support

- Note that because USB redirection is not designed for redirecting video devices, the bandwidth usage and server CPU load may increase significantly.

129. https://docs.vmware.com/en/VMware-Horizon-Client-for-Linux/2111/horizon-client-linux-installation/GUID-C8C17975-AA1E-4378-A305-00E02FF93201.html
130. https://docs.vmware.com/en/VMware-Horizon/2111/horizon-remote-desktop-features/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html
131. https://docs.vmware.com/en/VMware-Horizon/2006/horizon-remote-desktop-features/GUID-E64B3E85-BA1E-4FB7-9DB4-FF9B7B7A892C.html
132. https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon

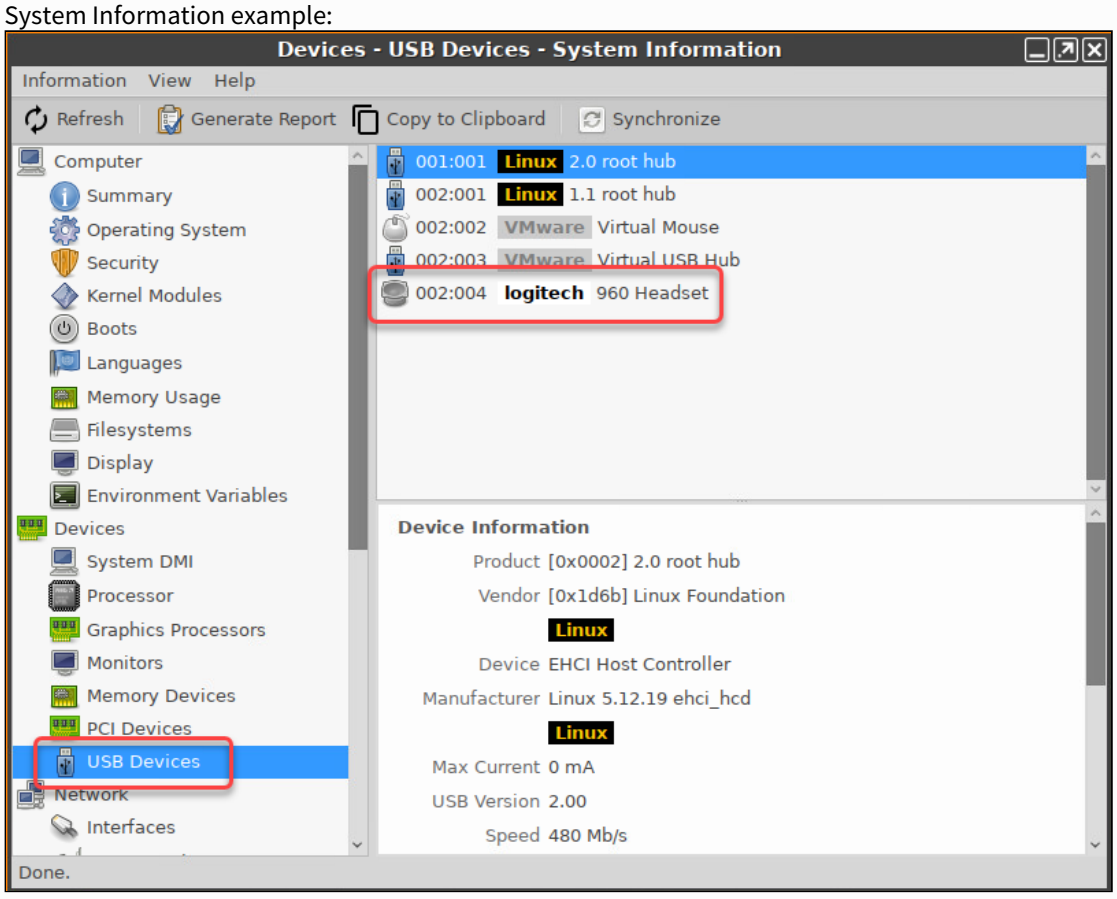
- For this reason, it is recommended to use webcams that output directly H.264 or H.265 streams, and not MJPEG, in order to reduce the data volume.

Native USB Redirection

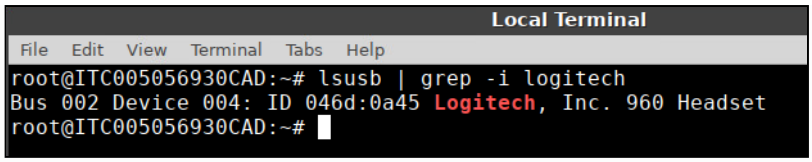
1. Enable **Sessions > RDP > RDP Global > Native USB Redirection > Enable native USB redirection**.
2. Set the **Default rule** to **Deny**.
3. Under **Device Rules**, add the specific **Vendor ID** and **Product ID** of the device to be redirected.

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.
Example for `lsusb`:



On RDS servers, the following may be helpful:
->Disable the setting **Do not allow supported Plug and Play device redirection** under **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**.

For Microphone (e.g. Headset)

->Enable **Sessions > RDP > RDP Global > Mapping > Audio > Audio recording**.

Custom Partition as a Local Alternative

You can also use Custom Partitions (see page 852) for Microsoft Teams or Zoom, e.g. in order to save backend resources, which may be a good choice in slow RDP backends. The Custom Partition is locally installed but is easy to access in the remote session.

- For details, see Zoom as a Custom Partition (see page 899).
- Contact the IGEL Support Team to get support for the deployment of Custom Partitions.

For how to open up the webcam in Windows 10, see Open the Camera in Windows 10[133].

For a video overview on using webcams and other USB devices in remote sessions, see:

English

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=PYCU1AEfS-g&feature=youtu.be

German

133. https://support.microsoft.com/en-us/windows/open-the-camera-in-windows-10-8da044ed-c4a8-2fb4-da51-232362e4126d#:~:text=To%20open%20up%20your%20webcam,Let%20apps%20use%20my%20camera.

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=caNhFib5cuA&feature=youtu.be

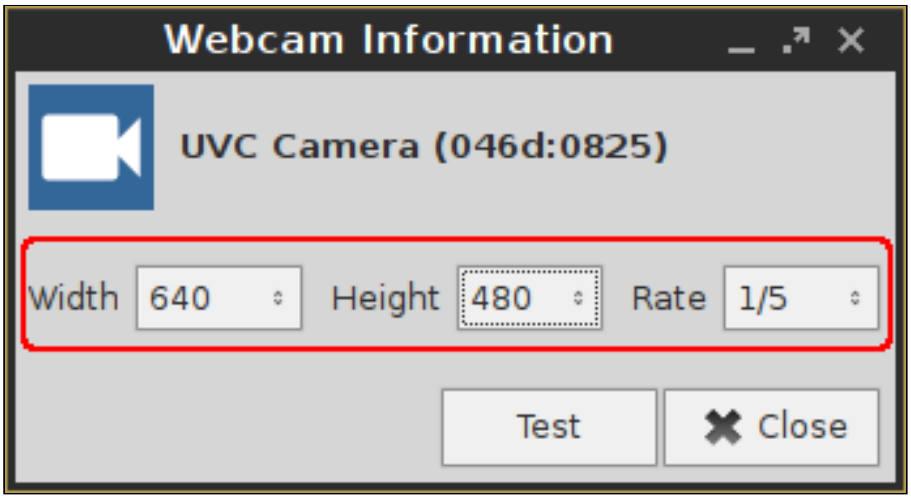
Webcam Information

If you are running a device with *IGEL Linux* version *5.3.100* or higher, you can configure and test a webcam using a built-in tool. This tool is called **Webcam Information**.

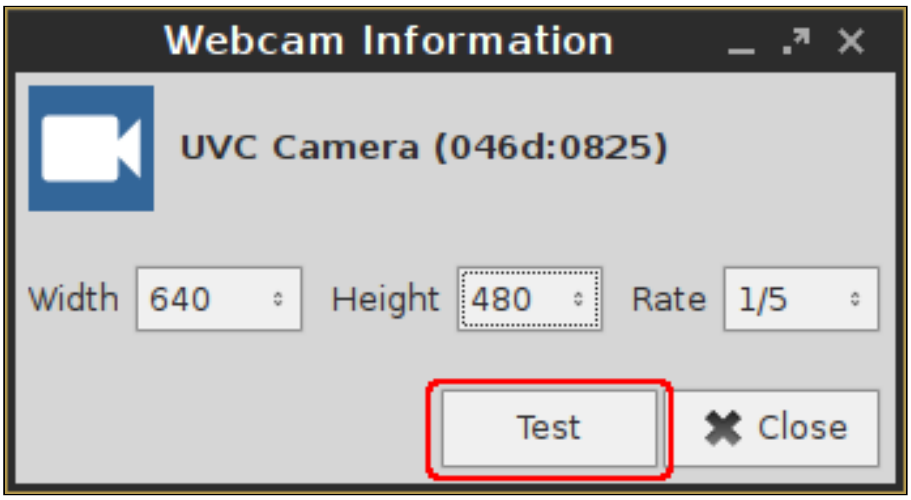
->To configure a starter for **Webcam Information**, open the IGEL Setup and go to **Accessories > Webcam Information**.

To determine and change the width, height, and frame rate of your webcam:

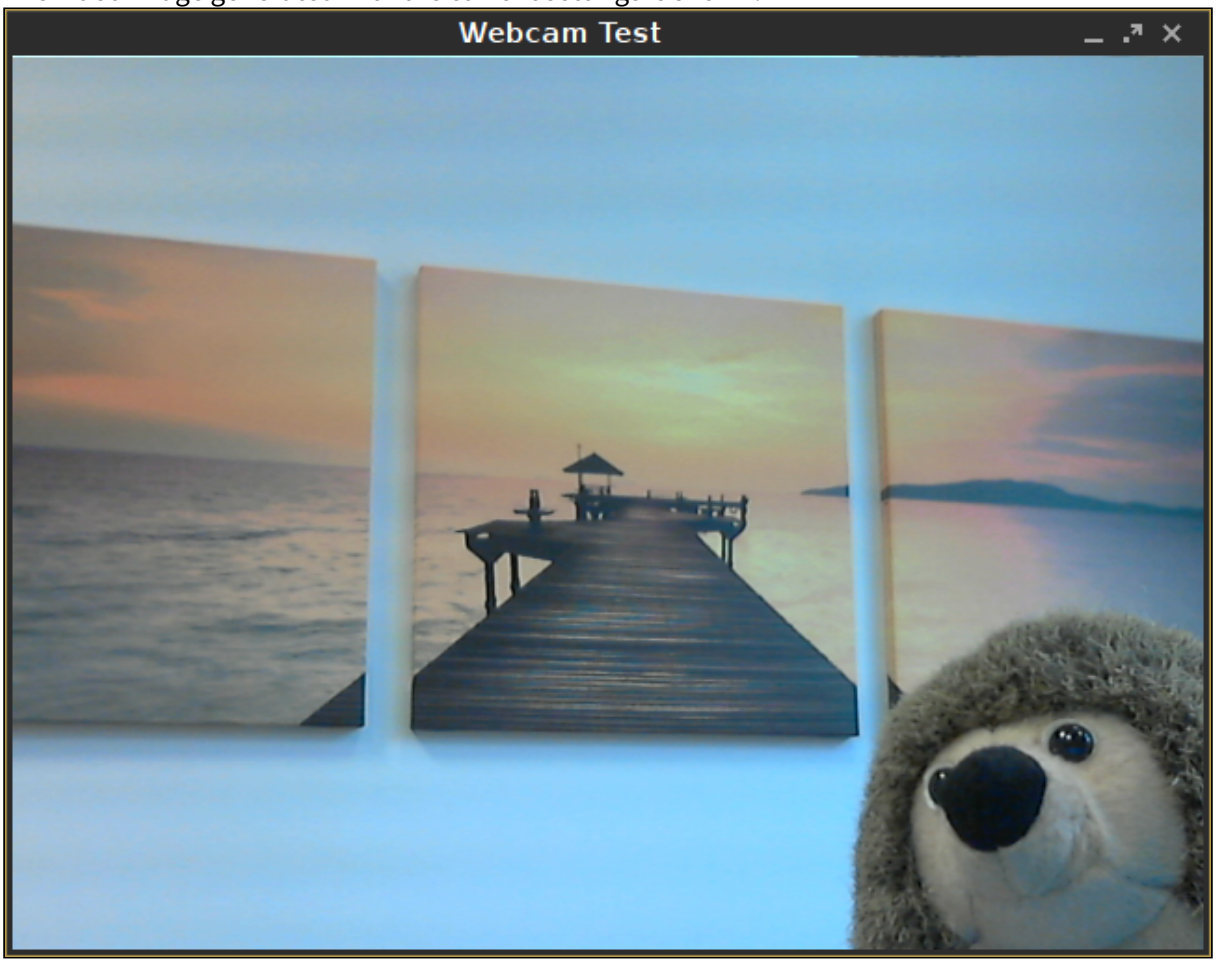
1. Start the **Webcam Information** tool.
   The following values are shown:
   - **Width**: Width of the image in pixels
   - **Height**: Height of the image in pixels
   - **Rate**: Frame rate in fps (frames per second). Example: **1/30** means 30 single images per second.



2. Click on on one of the fields to change the value. In doing so, the supported values are shown.
3. Click **Test**.



The video image generated with the current settings is shown.



To check if the webcam is working in a session (e.g. via Citrix HDX webcam redirection), open a browser in the session and go to https://www.onlinemictest.com/webcam-test/.

Bluetooth Tool

You can connect or disconnect Bluetooth devices conveniently using the Bluetooth tool. The Bluetooth tool supports the following pairing methods:

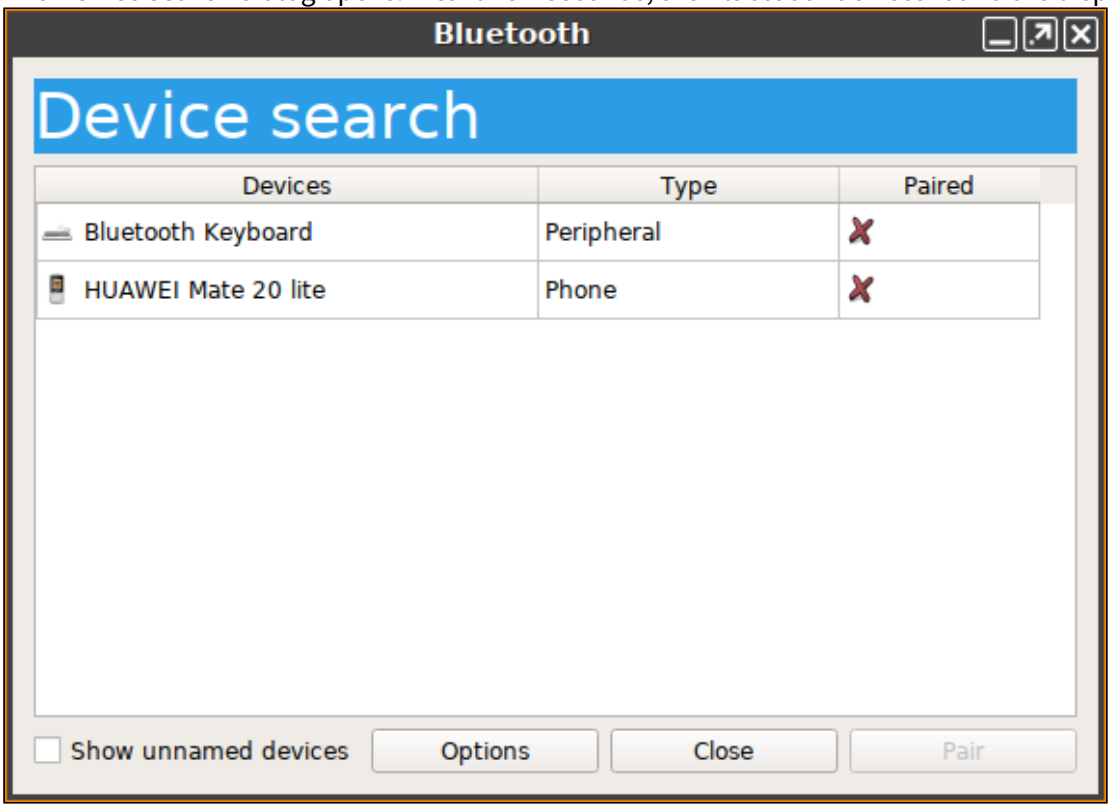
- **Automatic PIN selection**: Pairing with automatic PIN allocation
- **0000**, **1111**, **1234**: Pairing with a fixed PIN (for most headsets, mice, or GPS devices)
- **Custom PIN**: Pairing with a fixed PIN entered by the user.
  For further information, refer to the manual chapters Using Bluetooth Tool (see page 1791) and Bluetooth Tool (see page 1788).

In the following example, we will connect a Bluetooth keyboard with **Automatic PIN selection**:

1. Make sure that the following preconditions are met:
   - The options **Devices > Bluetooth > Bluetooth** and **Tray Icon** are enabled in the IGEL Setup.
   - The Bluetooth device is ready.

   > If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

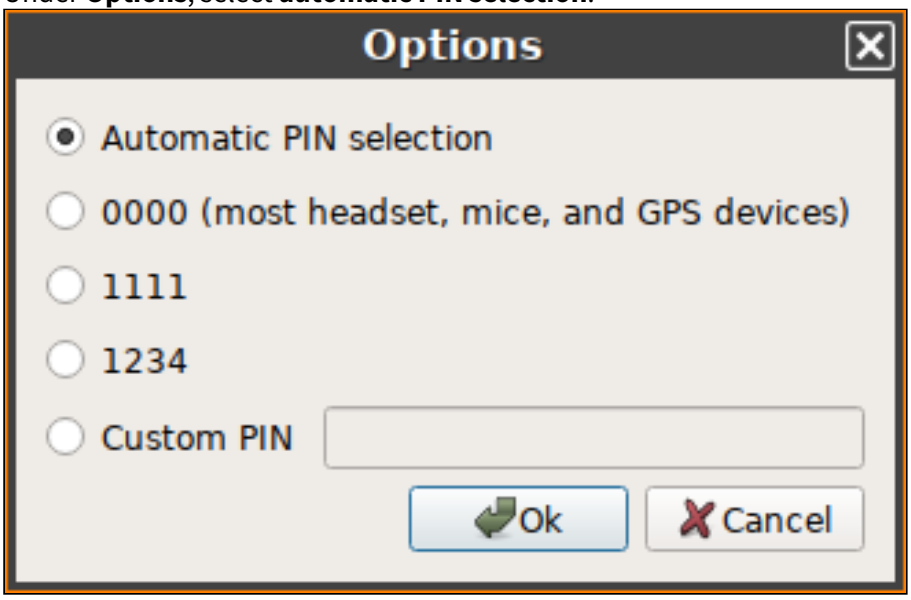
2. Launch the **Bluetooth Tool** from the IGEL menu via **System > Bluetooth Tool** or another launch option, if available.
   The **Device search** dialog opens. After a few seconds, the Bluetooth devices found are displayed.



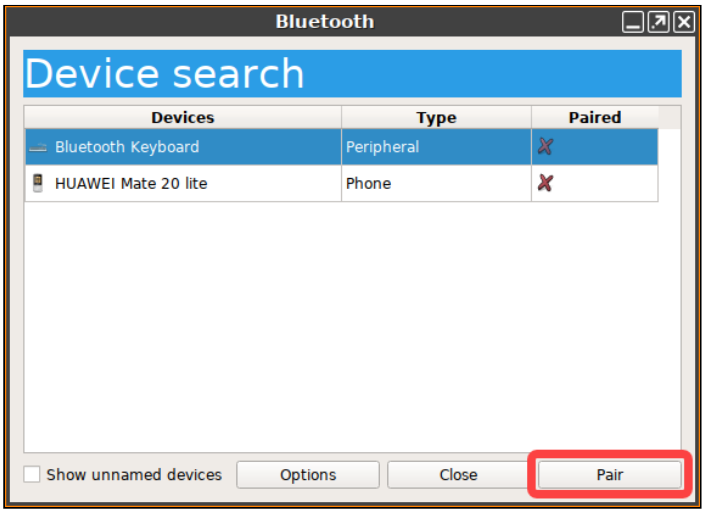
> **Tip**

If no devices are found, turn the Bluetooth device off and on again or press the Bluetooth pairing button, in our case **Connect** on the back side of the keyboard.

3. Highlight the desired Bluetooth device.
4. Under **Options**, select **automatic PIN selection**.



5. Click on **Pair**.



A PIN to be entered will be shown.

Tip

If no PIN is displayed, click the **Pair** button again.

6. Enter the PIN into your Bluetooth device.
   If everything went well, the status of the connection will be shown.

7. Close the dialog.

   Your Bluetooth device is ready for use. By right-clicking the icon in the system tray, you can start the Bluetooth tool again, e.g. to pair another Bluetooth device or to unpair a device.

How to Deploy a Jabra Xpress Package

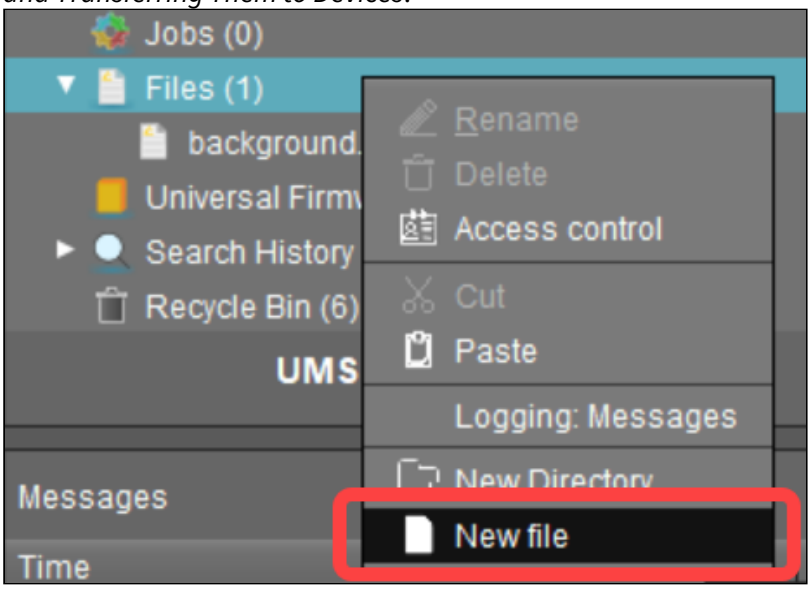
Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing settings, firmware updates, etc. for Jabra devices. For more information, see https://www.jabra.com/supportpages/jabra-xpress#/.

Deployment of a Jabra Xpress package involves the following steps:

1. Making the package available for download over the FTP(S) or HTTP(S) protocol (see page 1052)
2. Configuring the source URL in the IGEL Setup (see page 1052)
3. Triggering the deployment process in the UMS (see page 1053)

Making the Jabra Xpress Package Available for Download

1. Create a package on the Jabra Xpress portal and download it.
2. Place the ZIP archive onto your FTP(S) or HTTP(S) server.
   If you want to use the UMS as a source location, register the ZIP archive in the UMS under **Files > [context menu] > New file**. For details on how to register a file in the UMS, see *Universal Management Suite (UMS) > UMS Reference Manual > Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices*.

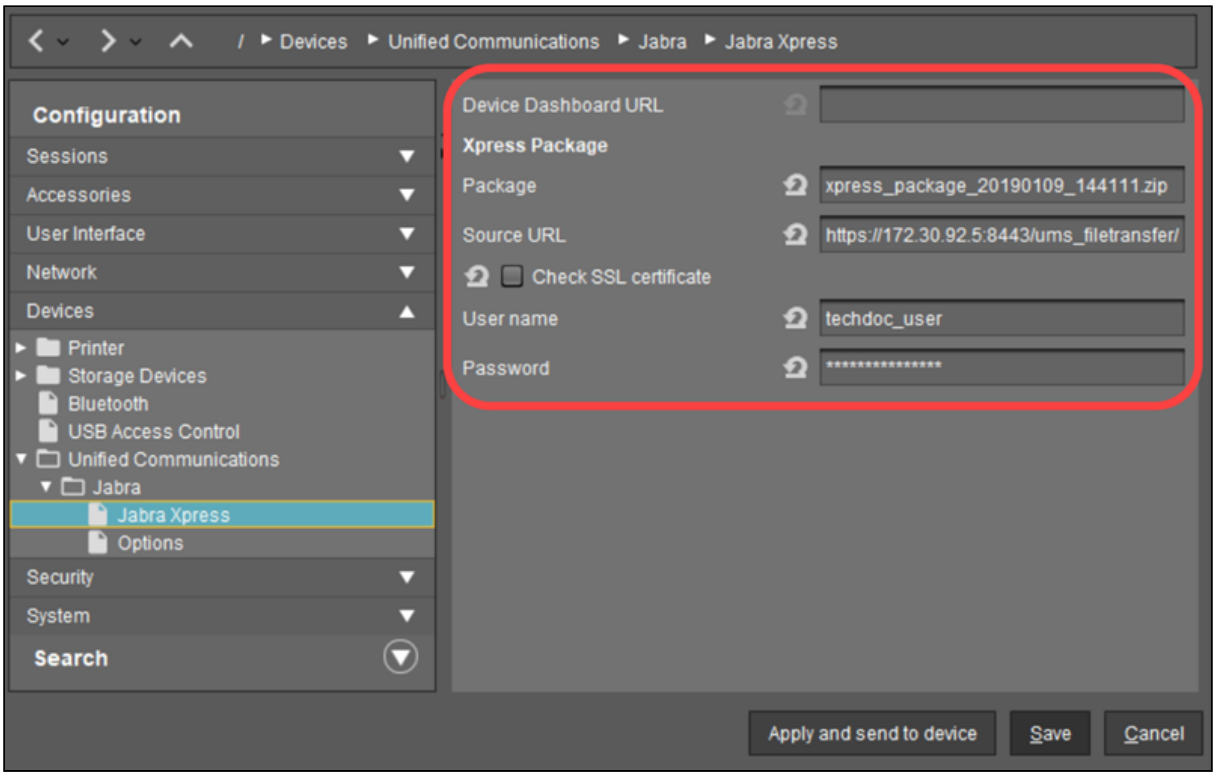


Configuring the Source URL

Now you have to configure the download location:

1. In the IGEL Setup or in the configuration dialog in the UMS, go to **Devices > Unified Communications > Jabra > Jabra Xpress**.
2. Under **Device Dashboard URL**, you can optionally specify the URL of the dashboard server of the Jabra device.

3. Under **Package**, enter the file name of the Jabra Xpress package.
   Example: `xpress_package_20190109_144111.zip`.
4. Under **Source URL**, specify the URL to the directory containing the Xpress package.
   Example: `https://172.30.92.5:8443/ums_filetransfer/` if you use the UMS as the source location.
5. Disable **Check SSL certificate** if your HTTPS or FTPS server uses a self-signed certificate.
6. Under **User name**, specify the user name for accessing the Xpress package that resides under the **Source URL**.
7. Under **Password**, specify the password for accessing the Xpress package that resides under the **Source URL**.

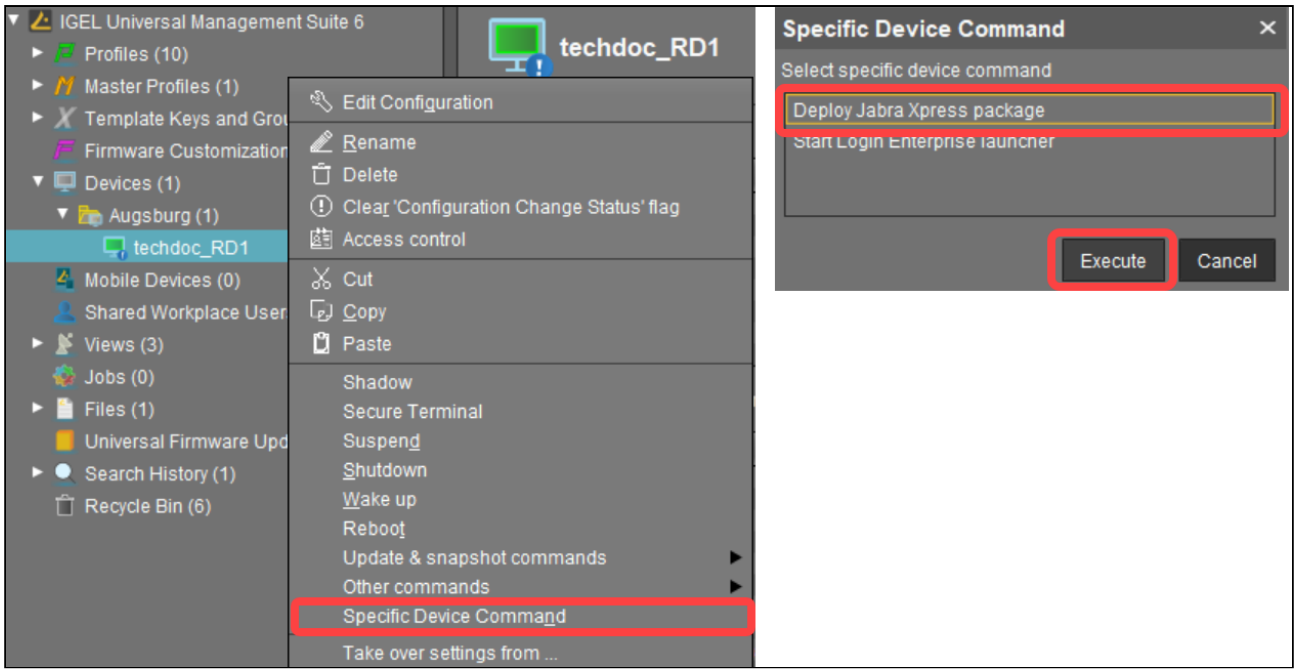


8. Save the settings.

Triggering the Deployment Process

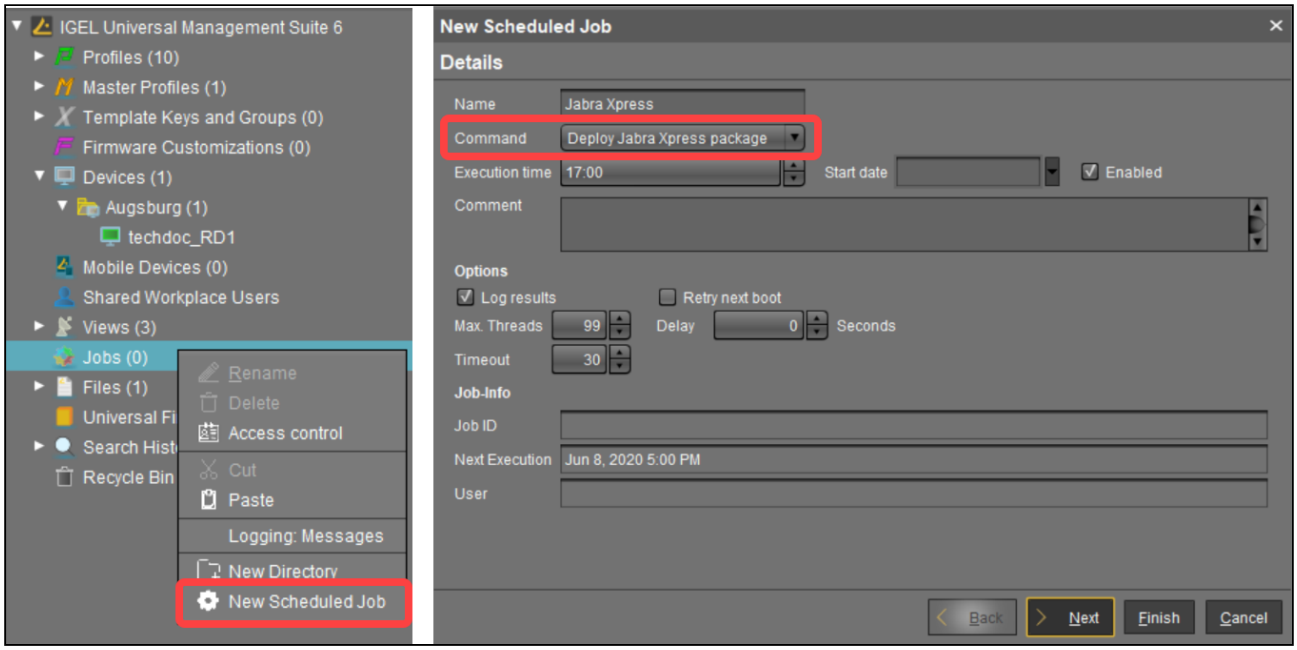
Finally, you have to trigger the deployment process. There are two possibilities:

->In the UMS, go to **Devices >** [context menu of the device] **> Specific Device Command** and select **Deploy Jabra Xpress Package**.



OR

->In the UMS, go to **Jobs > New Scheduled Job** and select **Deploy Jabra Xpress package** as **Command**. Assign the job to the necessary devices, see Assignment .



Note that it is not possible to reverse the deployment process, e.g. to remove an Xpress package from the Jabra device. If you require the previous settings, you have to configure and deploy a new Jabra Xpress package with the old headset firmware and configuration.

See also Jabra Xpress (see page 2004) in the IGEL OS reference manual.

Connecting Signature Pads

You can connect signature pads from the following manufacturers:

- StepOver;
- signotec.

->To enable them, go to Setup **> User Interface > Input > Signature Pad**.

->To configure a serial connection in order to be able to use USB signature pads from these manufacturers, proceed as follows:

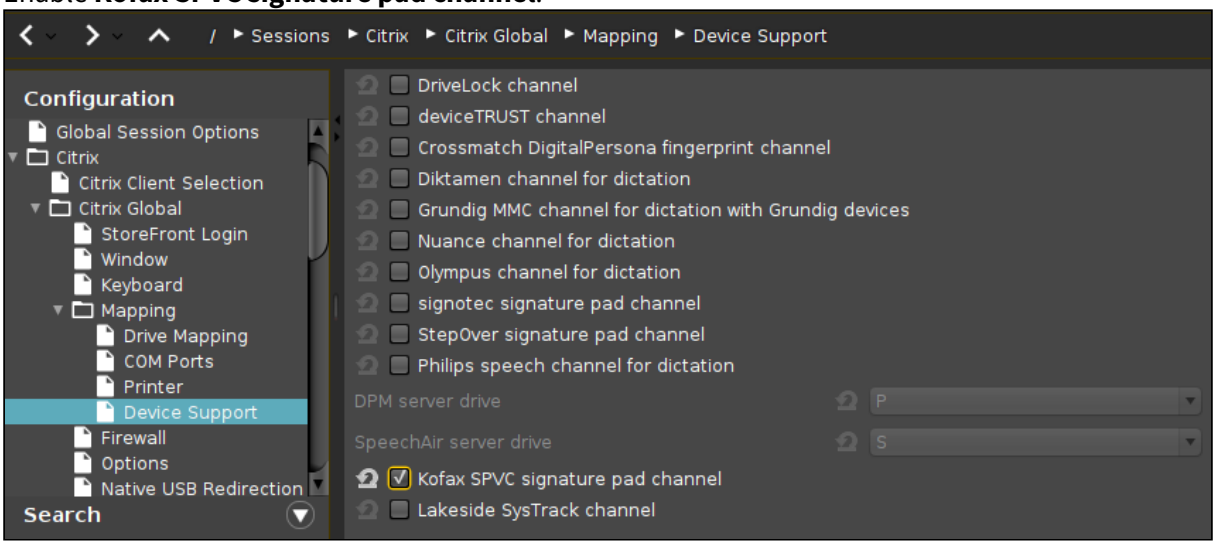
1. Enable **COM port mapping** under:
   - Setup **> Sessions > Citrix > Citrix Global > Mapping > COM Ports** for Citrix sessions;
   - Setup **> Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP sessions.
2. Click on **Add** .
3. Click **Detect Devices...** .
4. Select your device.
   Your signature pad can now be used.

Using a Kofax / Wacom Signature Pad

You can use a Kofax / Wacom signature pad in Citrix sessions using the Kofax SPVC signature pad channel. The Virtual Serial Sign Pad method is no longer supported.

On the Device

1. Connect the signature pad to one of the device's USB ports.
2. Go to **Sessions > Citrix > Citrix Global > Mapping > Device Support**.
3. Enable **Kofax SPVC signature pad channel**.



On the VDI Server (Windows)

->Install the required software from Kofax / Wacom.
The driver contained in this software will listen for signature pads on a virtual channel. Applications such as SignDoc will be able to use the signature pad.

Using a StepOver Signature Pad

You can use a StepOver signature pad in Citrix and RDP sessions. There are two different means to achieve this:

- With StepOver TCP Client (see page 1059)
- With StepOver Signature Pad Channel (see page 1063)

Only one of the methods can be used at a given time. Which of the two you need is determined by your applications on the server side.

See also StepOver Signature Pads Compatibility (see page 15).

With StepOver TCP Client

On the Device

->Connect the signature pad to one of the device's USB ports.

->Go to **User Interface > Input > Signature Pad** in IGEL Setup.

->Enable **StepOver TCP Client**.

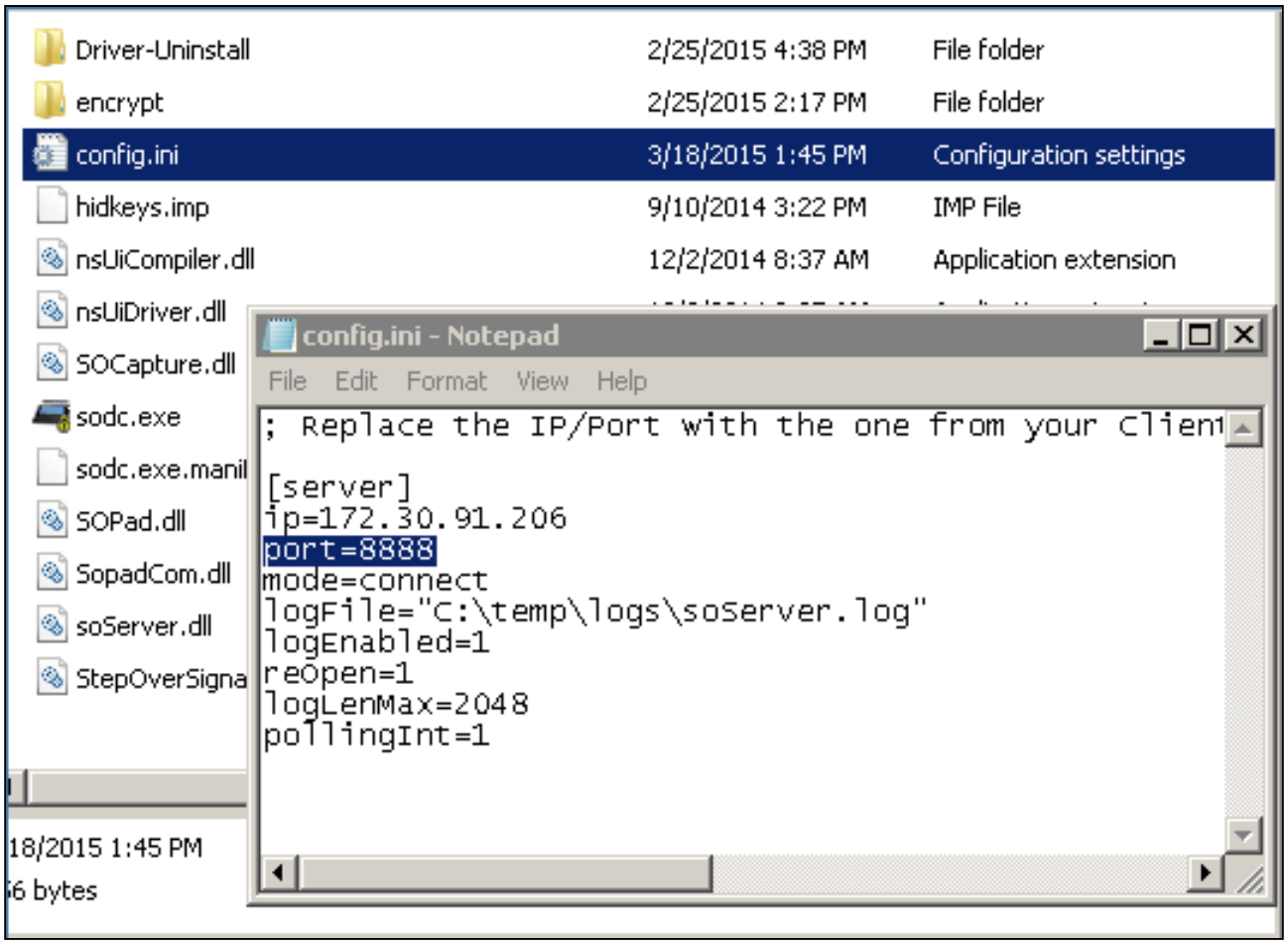
->Modify **Listening TCP Port** if needed. (Default: 8888)

You can check whether the **StepOver TCP Client** is running on the device by entering the following in a local terminal: `ps waux | grep sotcp`. The result should contain an `sotcp` process.

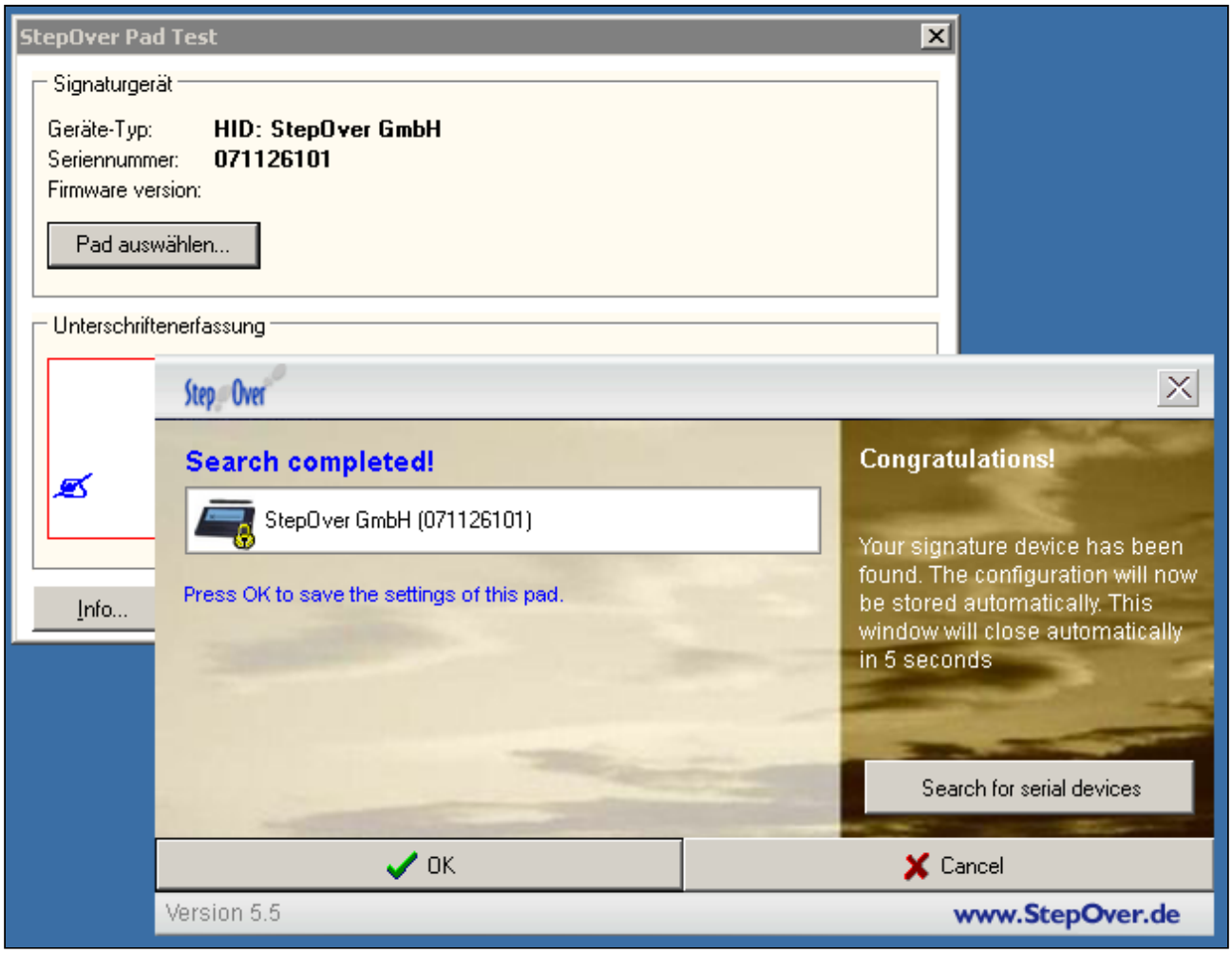
On the VDI Server (Windows)

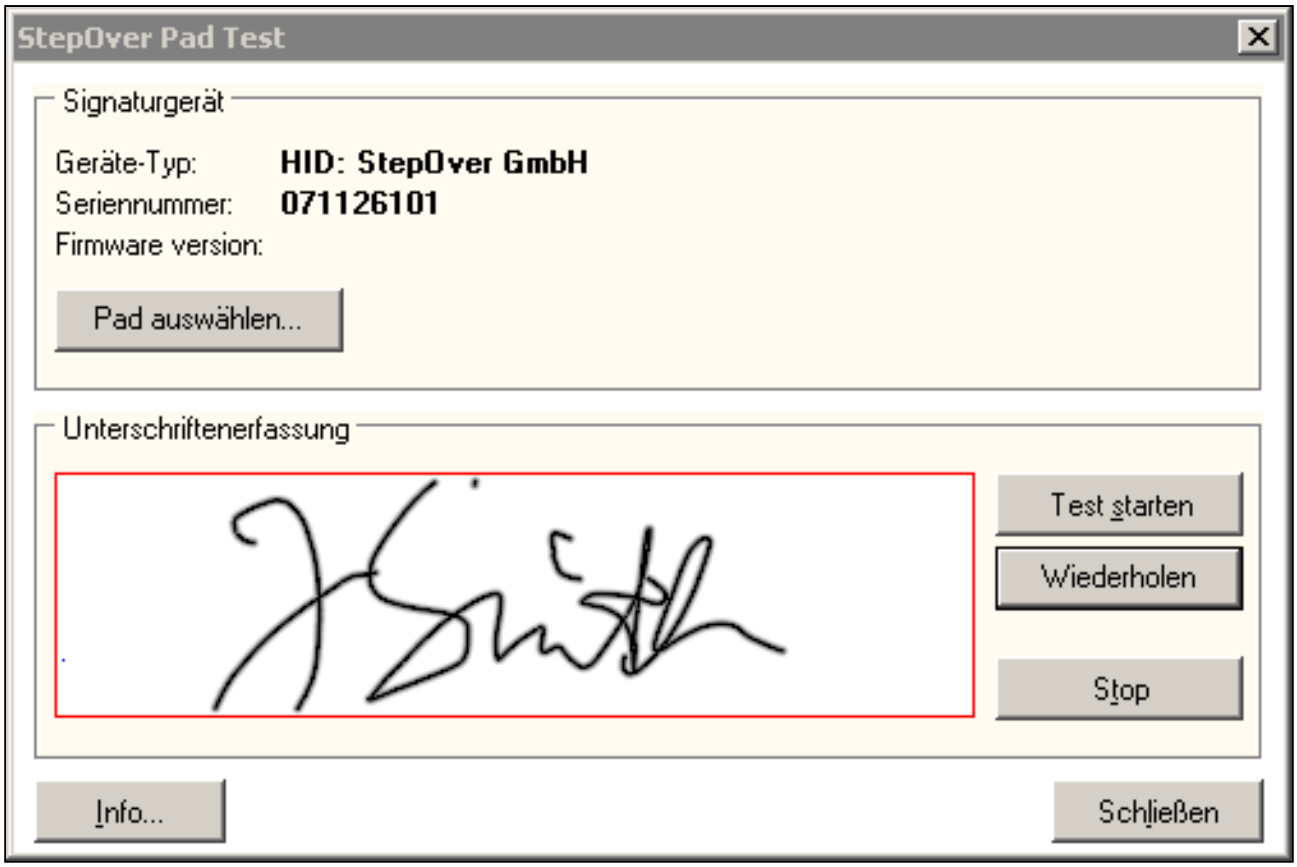
->Locate the `sodc.exe` program on the server. It is the part of StepOver eSignature Office and can be found in `[Your Program Files Directory]\StepOver\eSignatureOffice [version]\driver\`.

->If you are using a non-standard TCP port, change it in the `config.ini` file located in the same directory.



->Execute `sodc.exe`. The **StepOver Pad Test** window will open. Use its buttons to search and select your signature pad and try writing into the provided field.


StepOver Pad Test
Signaturgerät
Geräte-Typ: HID: StepOver GmbH
Seriennummer: 071126101
Firmware version:
Pad auswählen...
Unterschriftenerfassung
Info...
Step Over
Search completed!
StepOver GmbH (071126101)
Press OK to save the settings of this pad.
Congratulations!
Your signature device has been found. The configuration will now be stored automatically. This window will close automatically in 5 seconds
Search for serial devices
OK
Cancel
Version 5.5
www.StepOver.de



The status LED of the pad will turn to green when the connection is successful. The signature pad is now ready to be used with enabled applications such as StepOver eSignature Office.

With StepOver Signature Pad Channel

StepOver signature pad channel is applicable to Citrix sessions only. It activates StepOver Citrix Client and enables the redirection via Citrix virtual channel.

On the Device

->In the IGEL Setup, go to **Sessions > Citrix > Citrix Global > Mapping > Device Support**.

->Enable **StepOver signature pad channel** and save the changes.

On the Server

->During the installation of the StepOver software, select the option "Citrix".

eGK/KVK - Card Reader

IGEL OS devices support the reading of German electronic health cards (eGK), health insurance cards (KVK) and the German card for allied health professions (HBA) by a variety of readers connected via RDP or ICA. Configuration and functionality vary according to the reader type.

The following tested solutions are available:

Reader	Port	Client/server connection
Cherry G80-1502	Serial	COM port mapping
Cherry ST-2052	USB	Smartcard mapping
Cherry ST-1506	USB	USB RNDIS. IGEL OS endpoint acts as a NAT router.
Cherry ST-1503 and Cherry G87-1504	USB	Cherry Virtual Channel (IGEL Linux v5 only)
SICCT via LAN provided by the Cherry USB2LAN proxy (IGEL Linux *version 5.12.100* and IGEL Linux *version 10.03.100* onwards)		
ORGA 910/920 M	USB	COM port mapping
ORGA 6041 L eGK eHealth-BCS	USB	COM port mapping
SCM Microsystems eHealth200	USB	Smartcard mapping
SCM Microsystems eHealth500	USB	COM port mapping
celectronic CARD STAR /medic2	Serial	COM port mapping
celectronic CARD STAR /memo3	USB	COM port mapping

- Cherry G80-1502 at the Serial Port (see page 1065)
- Cherry ST-2052 (see page 1066)
- Cherry ST-1503 und G87-1504 (USB) (see page 1067)
- Using Cherry eHealth Card Terminal ST-1506 in USB RNDIS Mode with IGEL OS (see page 1068)
- Orga 910/920 M (see page 1072)
- Orga 6041 L eGK eHealth-BC S (see page 1073)
- celectronic CARD STAR / medic2 (see page 1074)
- celectronic CARD STAR/ memo3 (see page 1075)

Cherry G80-1502 at the Serial Port

Connecting the keyboard

☑ Connect the keyboard to both the PS/2 port and the serial port of the thin client.

> Firmware version 1.19 of the keyboard must be present and the keyboard must be in mode S1. Refer to https://www.cherry.de/service/downloads#21892.

Functionality	
Software:	Cherry eHealth eGK/KVK software
Device/server connection:	COM port mapping

Configuring the device

In IGEL Setup, add the COM port device to which the keyboard is connected:

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports**
2. Click .
3. Select a **COM port device** (COM1, COM2,...).

Configuring the server

1. Install the eGK-KVK software by *Cherry*.
   See also https://cherry.saas.contentserv.com/admin/ImageServer.php?ID=4602ea123940@iko249&rand=14ce2d7bb343451d398e569529511890&lang=1&force=true&download=1
2. Start the program CT-API configuration.
3. Select the appropriate port number for the G80-1502.

Cherry ST-2052

Functionality	
USB ID:	046a:003e
Software:	Cherry eHealth eGK/KVK software
Device/server connection:	Smartcard (PC/SC) mapping

Configuring the device

->Select **Activate PC/SC Daemon** in Setup under **Security > Smartcard > Services**:

Configuring the server

1. Install the eGK-KVK software by *Cherry*.
   See also http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf
2. Start the program *CT-API configuration*.
3. Select port number 1 for the ST-2052.

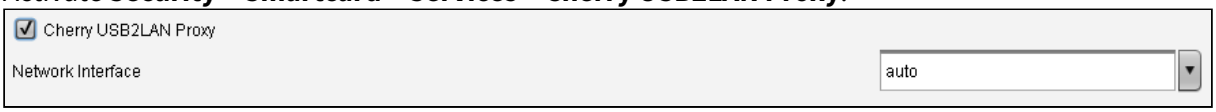
Cherry ST-1503 und G87-1504 (USB)

Functionality	
USB ID:	046a:0080 for ST-1503 046a:0081 for G87-1504
Software:	Cherry eHealth eGK/KVK software
Client/server connection:	SICCT via LAN provided by the Cherry USB2LAN proxy

Cherry USB2LAN proxy: Makes Cherry electronic health card devices available in the network via SICCT. The communication between card reader and server takes place independently of the VDI connections.

Configuring the Thin Client for Using the Cherry USB2LAN Proxy

1. Activate **Security > Smartcard > Services > Cherry USB2LAN Proxy**:



Configuring the Server for the Cherry USB2LAN Proxy

1. Install the eGK-KVK software by Cherry.
2. Configuration according to chapter 6 in http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf.

Using Cherry eHealth Card Terminal ST-1506 in USB RNDIS Mode with IGEL OS

If you, for example, do not have a free network socket, you can operate your Cherry eHealth Card Terminal ST-1506 via an endpoint in USB RNDIS (Remote Network Driver Interface Specification) mode. In this case, IGEL OS endpoint acts as a NAT router. The card terminal will use the network interface of your IGEL OS device.

For more information on ST-1506, see:

- CHERRY eHealth Terminal ST-1506 Administrators Manual (German only): https://cherry.saas.contentserv.com/admin/ImageServer.php?ID=c9d5ca123973@iko249&rand=7fd8bfbaf76d6640e20fb48013ada6fe&lang=1&force=true&download=1
- CHERRY ST-1506 USB-LAN Proxy User Guide (German only): https://cherry.saas.contentserv.com/admin/ImageServer.php?ID=fa222a123000@iko249&rand=ecdbe080457ef3f85ef67ef99515bbf2&lang=32&force=true&download=1
- USB-Modus (RNDIS) Configuration Manual (German only): https://cherry.saas.contentserv.com/admin/ImageServer.php?ID=b95fba122999@iko249&rand=4184538cb599fac797ec81076c31e366&lang=1&force=true&download=1
- For further downloads, see: https://www.cherry.de/service/downloads#15239

Requirements

- IGEL OS 11.08.100 or higher
- Cherry ST-1506 must have a static IP configuration

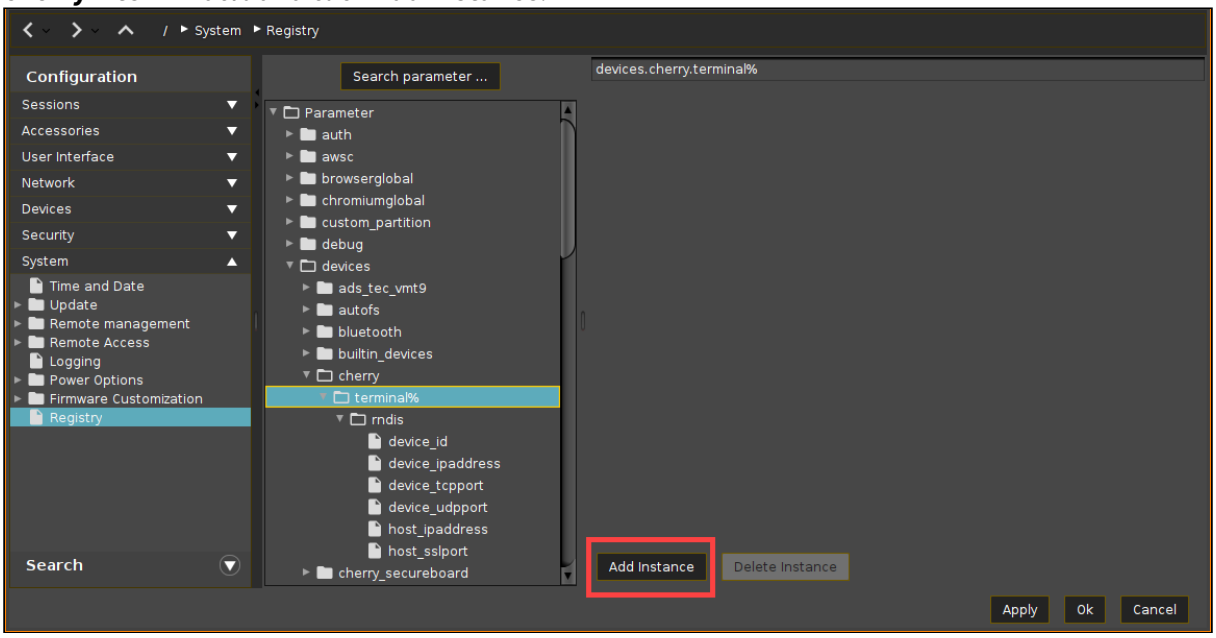
Configuration on Your Cherry ST-1506

1. Connect your card terminal to the IGEL OS device.
2. In the **Menu > Admin Menu**, enter your admin PIN.
3. Go to **Connection > USB Ethernet**.
4. Activate **RNDIS**.
5. Disable **DHCP**.
6. Configure a static **IP address**.
7. As **Gateway**, specify the Host IP address which you configure on your IGEL OS device with the registry key `devices.cherry.terminal%.rndis.host_ipaddress` (Default: 192.168.42.1). See the instructions below.
8. Save the settings.

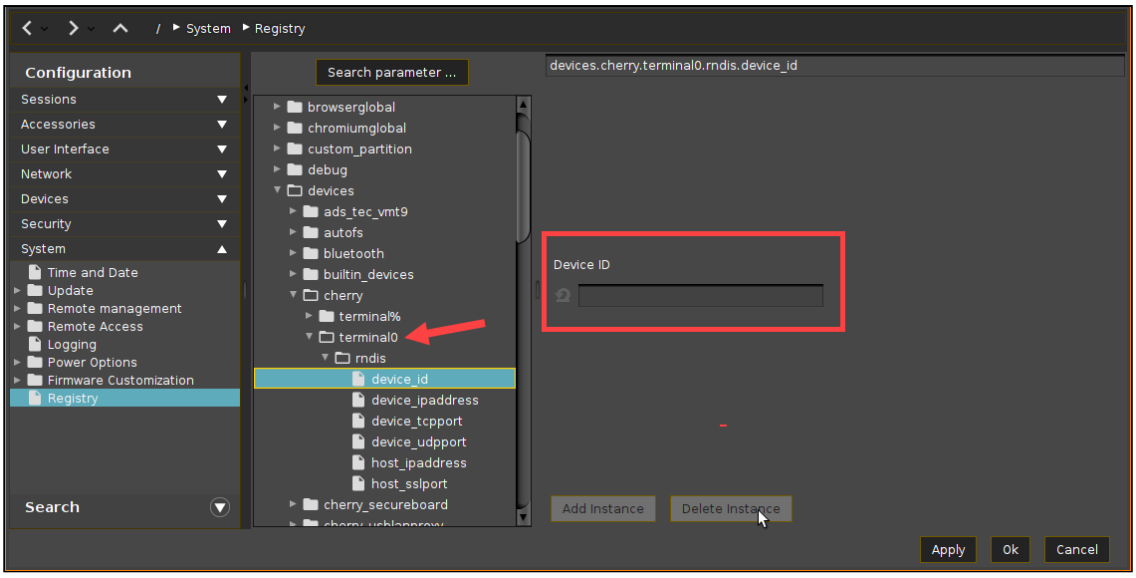
Configuration on Your IGEL OS Device

Per each card terminal, one instance of the template `devices.cherry.terminal%` must be created and configured. By default, none is configured and so the feature is essentially disabled. To add and configure an instance, proceed as follows:

1. In the IGEL Setup or the configuration dialog in the UMS, go to **System > Registry > devices > cherry > terminal%** and click **Add Instance**.



   For the added instance, configure the following:
2. For distinguishing purposes if multiple ST-1506 devices are connected, configure the registry key `devices.cherry.terminal%.rndis.device_id`. It may be left empty if only one card terminal shall be supported.
   Here, you specify:
   - a MAC address of the card terminal (To find it out, you can use, for example, the command `ifconfig` in the Local Terminals (see page 1708) or view it directly on the ST-1506 in the admin menu)
     OR
   - the value of the udev property `ID_NET_NAME_PATH` (To find it out, you can use, for example, the command `udevadm info --export-db| less`)



3. Configure the **Device IP address**:

Parameter	Device IP address
Registry	`devices.cherry.terminal%.rndis.device_ipaddress`
Type	string
Value	192.168.42.42 (Default)
Note	Here, you specify a static IP you have configured on your ST-1506 via the admin menu. • You can leave the default value unchanged if you use it also on your ST-1506. • If you have multiple ST-1506 devices connected, you must configure a different IP for each card terminal.

4. Configure the **Host IP address**:

Parameter	Host IP address
Registry	`devices.cherry.terminal%.rndis.host_ipaddress`
Type	string
Value	192.168.42.1 (Default)
Note	This is the IP address which you must specify as **Gateway** on your ST-1506 via the admin menu.

5. If required, configure the following registry keys:

Parameter	Device TCP port

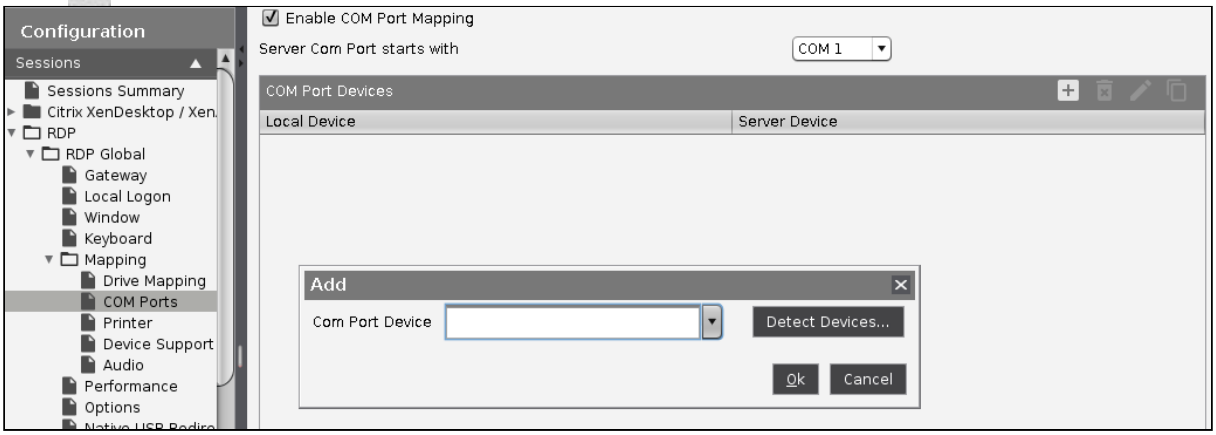
Registry	`devices.cherry.terminal%.rndis.device_tcpport`
Type	string
Value	4742 (Default)
Note	This port on the host will be passed through to the same port on the device. • If you have multiple ST-1506 devices connected, you must configure a different port for each card terminal.
Parameter	Passed through device UDP port
Registry	`devices.cherry.terminal%.rndis.device_udpport`
Type	string
Value	4742 (Default)
Note	This port on the host will be passed through to the same port on the device. • If you have multiple ST-1506 devices connected, you must configure a different port for each card terminal.
Parameter	Host SSL port
Registry	`devices.cherry.terminal%.rndis.host_sslport`
Type	string
Value	empty (Default)
Note	This port on the host will be forwarded to the device's port 443. Configure this registry key if you are using a web browser for the remote management of your ST-1506 devices. • If you have multiple ST-1506 devices connected, you must configure a different port for each added instance.

Orga 910/920 M

Functionality	
USB ID:	0780:1202
Software:	CT-API by Orga
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP
2. Select **Enable Com Port Mapping**:
3. Click + .



4. Select USB COM 1 as a new COM port device (`/dev/ttyUSB0`).

Configuring the server

1. Download the appropriate driver for *Orga 910/920 M* from the download page: http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx[134]
2. Install the driver.

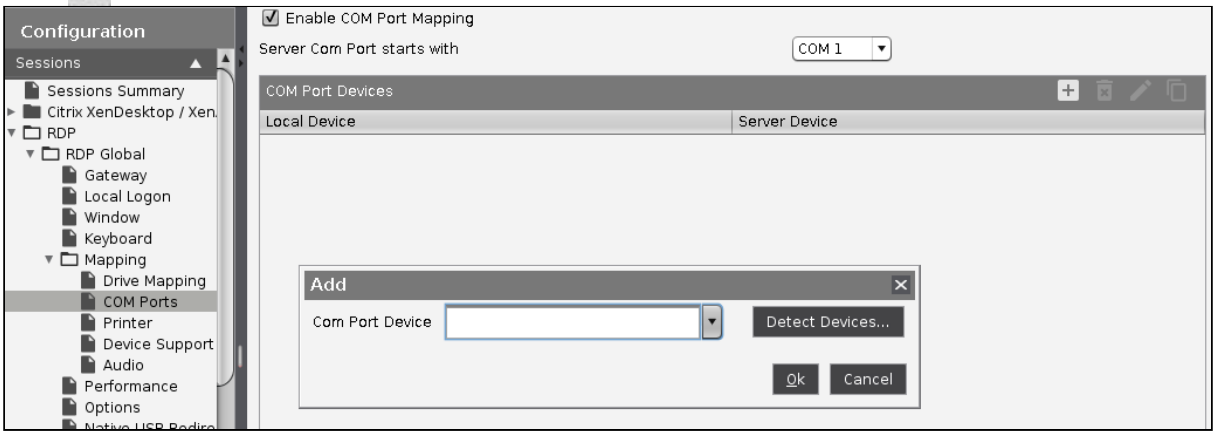
134. https://ingenico.de/healthcare/downloads

Orga 6041 L eGK eHealth-BC S

Functionality	
USB ID:	0780:1302
Software:	CT-API by Orga
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click + .



4. Select USB COM 1 as a new COM port device (`/dev/ttyUSB0`).

Configuring the server

1. Download the appropriate driver for *Orga 6041 L eGK eHealth-BC S* from the download page: http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx[135]
2. Install the driver.

135. https://ingenico.de/healthcare/downloads

celectronic CARD STAR / medic2

Connecting the reader

->Connect the reader to the COM port of the thin client.

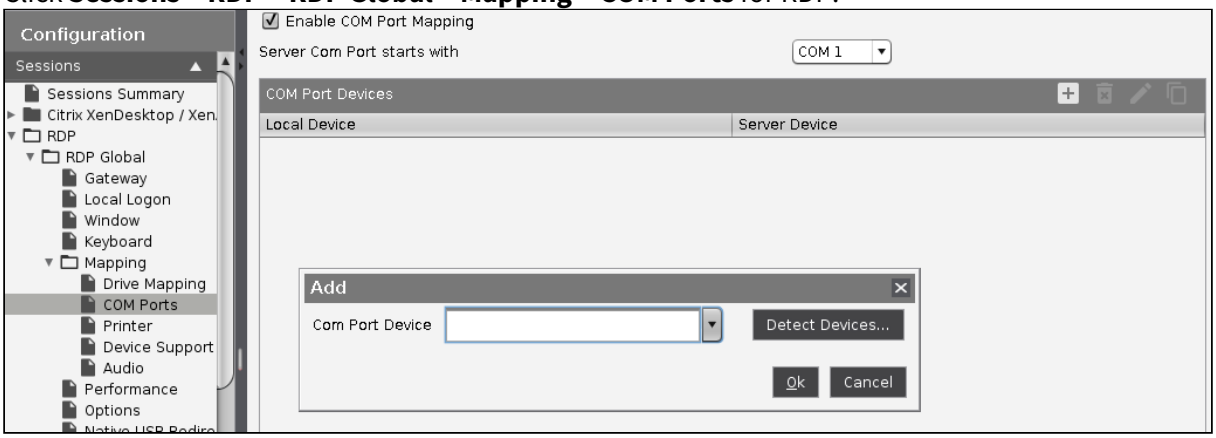
> The reader must be set to host/PC serial interface.

Functionality	
Software:	CT-API by celectronic
Device/server connection:	COM port mapping

Configuring the device

In IGEL Setup, add the COM port device to which the keyboard is connected:

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.



2. Click .
3. Select a **COM port device** (COM1, COM2,...).

Configuring the server

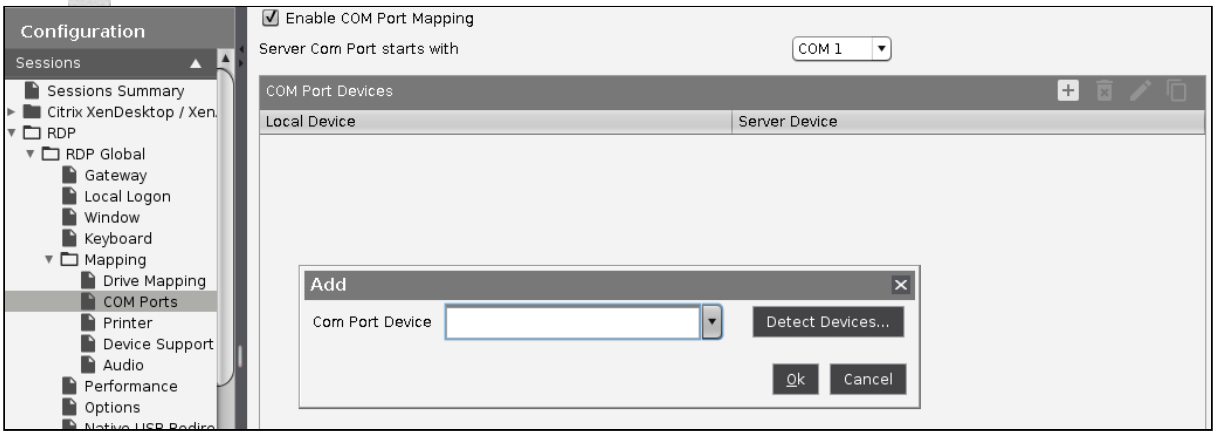
1. Download the appropriate driver for *celectronic CARD STAR /medic2* from the download page: https://www.ccv.eu/de/
2. Install the driver.

celectronic CARD STAR/ memo3

Functionality	
USB ID:	152a:8180
Software:	CT-API by celectronic
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click + .



4. Select USB COM 1 as a new COM port device (`/dev/ttyUSB0`).

Configuring the server

1. Download the appropriate driver for *celectronic CARD STAR memo3* from the download page: https://www.ccv.eu/[136]
2. Install the driver.

136. https://www.ccv.eu/de/

Using Mobile Device Access

You can access your mobile device file structure via USB, e.g. to make it available in a session.

Feature with limited support! The mobile device access feature comes with “limited support”. This feature is offered 'as is' without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The following device types can be used:

- Smartphones with Android (via MTP / PTP) or iOS
- Tablets with Android via MTP / PTP) or iOS
- Digital cameras

The functionality may differ according to the specific device and operating system version.

Environment

- IGEL Universal Desktop (UD) with IGEL OS10.04.100 or higher

  IZ devices are not supported!

- IGEL Universal Desktop Converter 3 (UDC3) with IGEL Linux 10.04.100 or higher
- UD Pocket with IGEL Linux 10.04.100 or higher
- To configure the feature via UMS, UMS version 5.08.110 is required.

- Enabling Mobile Device Access (see page 1077)
- Disabling Mobile Device Access (see page 1078)
- Mapping a Mobile Device for a Session (see page 1079)
- Connecting Your Mobile Device (see page 1080)
- Accessing the Mobile Device USB Window from a Session (see page 1081)
- Viewing the Files and Directories Locally (see page 1082)
- Safely Removing the Mobile Device (see page 1084)

Enabling Mobile Device Access

1. Ensure that the settings under **System > Update > Firmware Update** are correct. The **Server Path** must point to the firmware version that is currently installed. This is required because the software package for mobile device access must be downloaded in order to deploy the feature.
2. Go to **System > Firmware Customization > Features** and activate **Mobile Device Access USB**.
3. Confirm the warning dialog with **Ok**.
4. Click **Ok** in the main window.
5. Reboot the device.
   On reboot, the device downloads and installs the software package for the mobile device access feature.
6. If mobile device access should be available permanently, make sure that **Autostart** is activated under **Accessories > Mobile Device Access**. The other start options are described in the manual under Mobile Device Access (see page 1806).

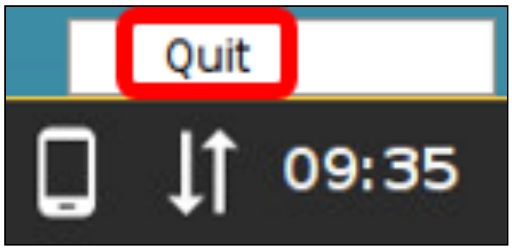
> If you want to use mobile device access in appliance mode, you must enable autostart or configure a hotkey. Autostart is recommended.

7. Configure the start options for mobile device access according to your requirements.
8. If you have activated **Autostart** as the only start option, restart the device.
   When the mobile device access is activated, the smartphone symbol is shown in the task bar. For appliance mode sessions, the in-session control bar is available; see Accessing the Mobile Device USB Window from a Session (see page 1081).

Disabling Mobile Device Access

Disabling Mobile Device Access

->In the context menu of the tray icon, click **Quit**.



Mapping a Mobile Device for a Session

There are two alternative options to map a mobile device to a drive in a session:

- Automatic Drive Mapping
- Manual Mapping to a Specific Drive

Automatic Drive Mapping

You can use dynamic client drive mapping to have a drive automatically mapped to your mobile device. The directories and files on your mobile device will be accessible under this drive.

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage hotplug**.
2. Set **Client drive mapping** to "**Dynamic**".
3. Click **OK**.

You can access the directories and files on your mobile device like with a regular hotplug storage device.

For further information, see the manual chapter Storage Hotplug (see page 1969).

Manual Mapping to a Specific Drive

You can specifiy a drive letter under which the directories and files on your mobile device will be accessible.

1. If the session will run in fullscreen mode, open the IGEL Setup, go to **User Interface > Desktop** and activate **In-Session Control Bar**.
2. If the session will run in fullscreen mode or appliance mode, ensure that **Autostart** under **Accessories > Mobile Device Access** is enabled. See here also Enabling Mobile Device Access (see page 1077).
3. Go to the **Drive Mapping** page for your session type. Example: With RDP sessions, the setup path is **Sessions > RDP > RDP Global > Mapping > Drive Mapping**.
4. Activate **Enable drive mapping**.
5. Click + **Add** to bring up the mapping window.
6. Click **Enabled** to enable the drive connection.
7. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.
8. Enter `/media` as the **Local Drive Path**.
9. Click **OK**.

You can access the directories and files on your mobile device like with a regular hotplug storage device.

Connecting Your Mobile Device

1. If mobile device access is not started already, use one of the start options configured under **Accessories > Mobile Devices Access**.
2. Connect your mobile device with your thin client.
3. Allow file transfer on your phone, e. g. **Transfer Files** (Android smartphones) or **Trust The Computer** (Apple iPhone).
   The directories of your mobile device are mounted.
   You can view the contents; see Viewing the Files and Directories Locally (see page 1082).
   You can remove the mobile device securely; see Safely Removing the Mobile Device (see page 1084).

Accessing the Mobile Device USB Window from a Session

Non-Fullscreen Session

->Click to open the **Mobile Device Access USB** window.
The **Mobile Device Access USB** window appears.
You can view the directories and files on your mobile device or safely remove the device; see Safely Removing the Mobile Device (see page 1084).

Fullscreen Session

In a session that is running in fullscreen mode or appliance in a fullscreen session, you can use the in-session control bar to open the **Mobile Device Access USB** window.

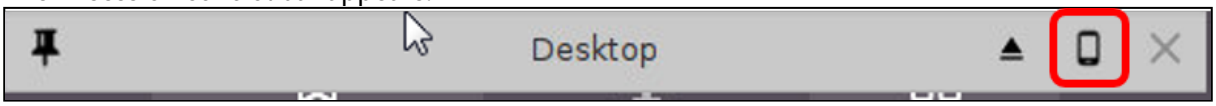
1. Move the mouse pointer to the upper edge of the screen.
   The in-session control bar appears.

2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

Appliance Mode Session

In a session that is running in appliance mode, you can use the in-session control bar to open the **Mobile Device Access USB** window.

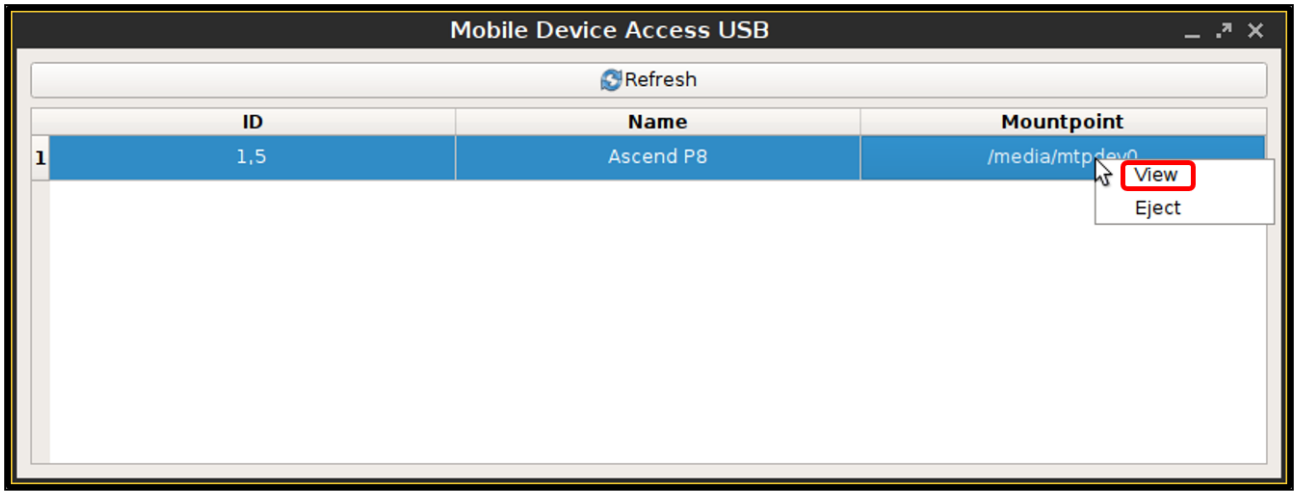
1. Move the mouse pointer to the upper edge of the screen.
   The in-session control bar appears.



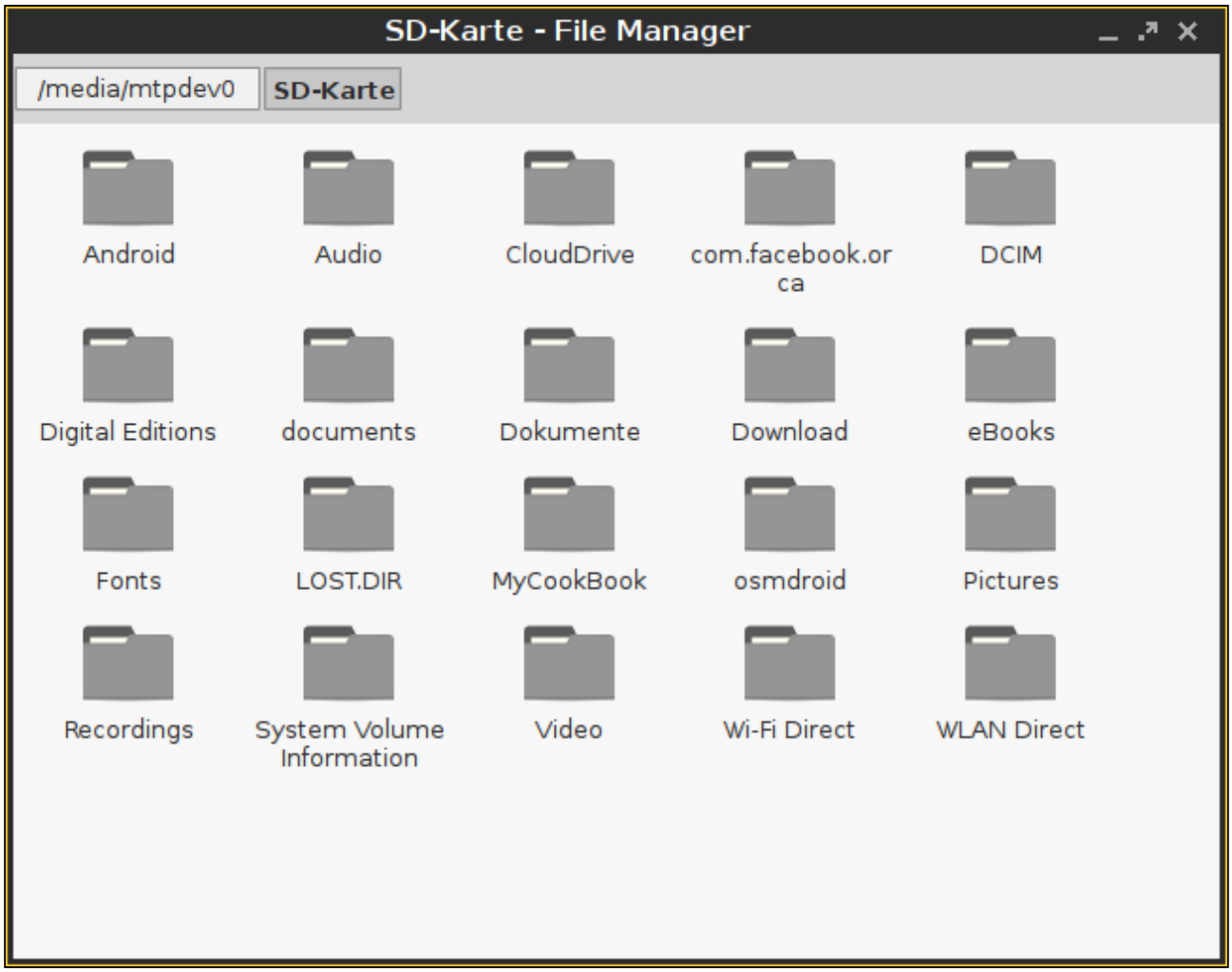
2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

Viewing the Files and Directories Locally

->Select **View** in the context menu.

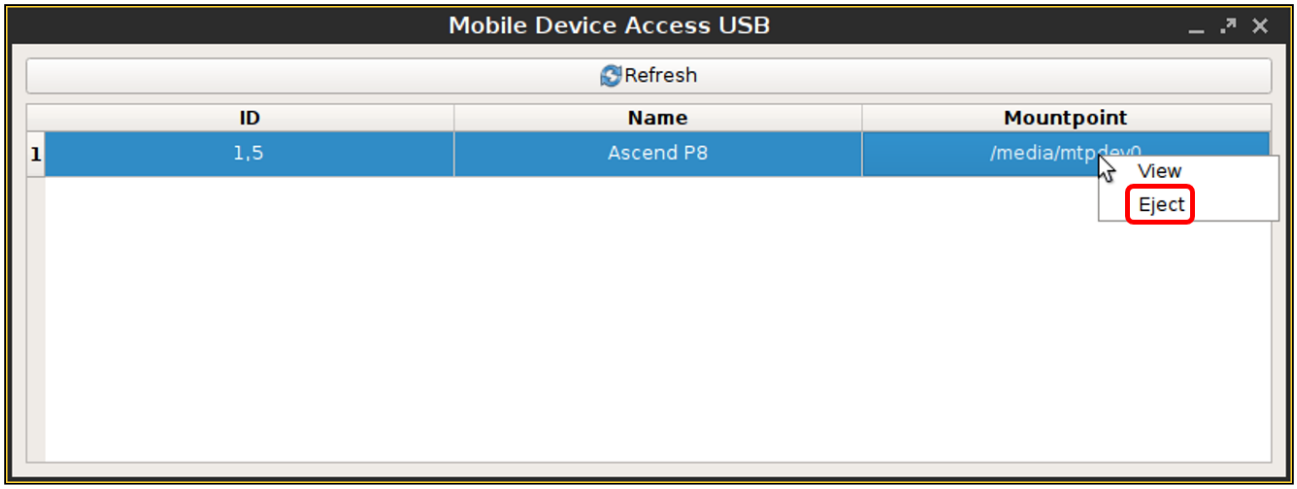


The directories on your smartphone are displayed. Access is read-only, i. e. you can only view the directories and files.


SD-Karte - File Manager
/media/mtpdev0
SD-Karte
Android
Audio
CloudDrive
com.facebook.orca
DCIM
Digital Editions
documents
Dokumente
Download
eBooks
Fonts
LOST.DIR
MyCookBook
osmdroid
Pictures
Recordings
System Volume Information
Video
Wi-Fi Direct
WLAN Direct

Safely Removing the Mobile Device

->Click **Eject** in the context menu for the device in question.



Swapping Function of Mouse Buttons (e.g. When Using an Evoluent Mouse)

The assignment of mouse buttons for *Evoluent Mouse* 3 changed between firmware versions 5.04.130 and 5.05.100.

Problem

Users have become used to the assignment as it was up to 5.04.130, so you want to reproduce the same assignment in 5.05.100.0.

Solution

A. To manually analyze the assignment and determine how it needs to be adjusted:

1. Open a local terminal.
2. Find the mouse ID: `xinput list`
   The output should look something like this: `⎡ Virtual core pointer id=2[master pointer (3)] ⎜- Virtual core XTEST pointer id=4[slave pointer (2)] ⎜- Logitech USB Optical Mouse id=10[slave pointer (2)] - Virtual core keyboard id=3[master keyboard (2)] - Virtual core XTEST keyboard id=5[slave keyboard (3)] - Power Button id=6[slave keyboard (3)] - Video Bus id=7[slave keyboard (3)] - Power Button id=8[slave keyboard (3)] - Sleep Button id=9[slave keyboard (3)] - Logitech USB Keyboard id=11[slave keyboard (3)] - Logitech USB Keyboard id=12[slave keyboard (3)]`
3. Find your mouse and its ID in the output (here: Logitech USB Optical Mouse, id=10).
4. Check the number of buttons in the button map: `xinput get-button-map [ID]` (where ID is the ID of your mouse device).
5. Now check which button number is set for the buttons in question: `xev`
   A test window will appear.
6. Click into the window using the buttons that you want to swap. Look for the button numbers in the terminal output: `ButtonPress event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25542794, (114,113), root:(2884,634), state 0x10, button 1, same_screen YES ButtonRelease event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25542898, (114,113), root:(2884,634), state 0x110, button 1, same_screen YES ButtonPress event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25543218, (114,113), root:(2884,634), state 0x10, button 3, same_screen YES`

`ButtonRelease event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25543330, (114,113), root:(2884,634), state 0x410, button 3, same_screen YES`

In the above example the buttons number 1 and 3 were used.

B. To change the assigment of the mouse buttons on the local thin client:

1. Set a new button map for the mouse in **Setup > System > Firmware Customization > Custom Commands > Desktop Commands > Final**.
2. Swap the buttons in the map. To swap e.g. the buttons 1 and 3, change the setting from `xinput set-button-map [ID] 1 2 3 4 5 6 7` to `xinput set-button-map [ID] 3 2 1 4 5 6 7`

C. To automatically change the assignment using a UMS profile:

As the ID of the mouse may be different on each client, you cannot use the command as shown in B2 but need to use a script that will automatically map the correct input device.

1. Run the following command in a local terminal: `xinput --list`
2. Make a note of the complete name of the mouse.
3. Create a profile in **Setup > System > Firmware Customization > Custom Commands > Desktop Commands > Final** with a custom command: `MouseID=$(xinput --list --id-only 'NAME OF MOUSE') xinput set-button-map $MouseID 3 2 1 4 5 6 7`
4. Replace NAME OF MOUSE with the name of the mouse as determined in step C1.

Using Natural Scrolling (Reverse Scrolling Direction) on IGEL OS Devices

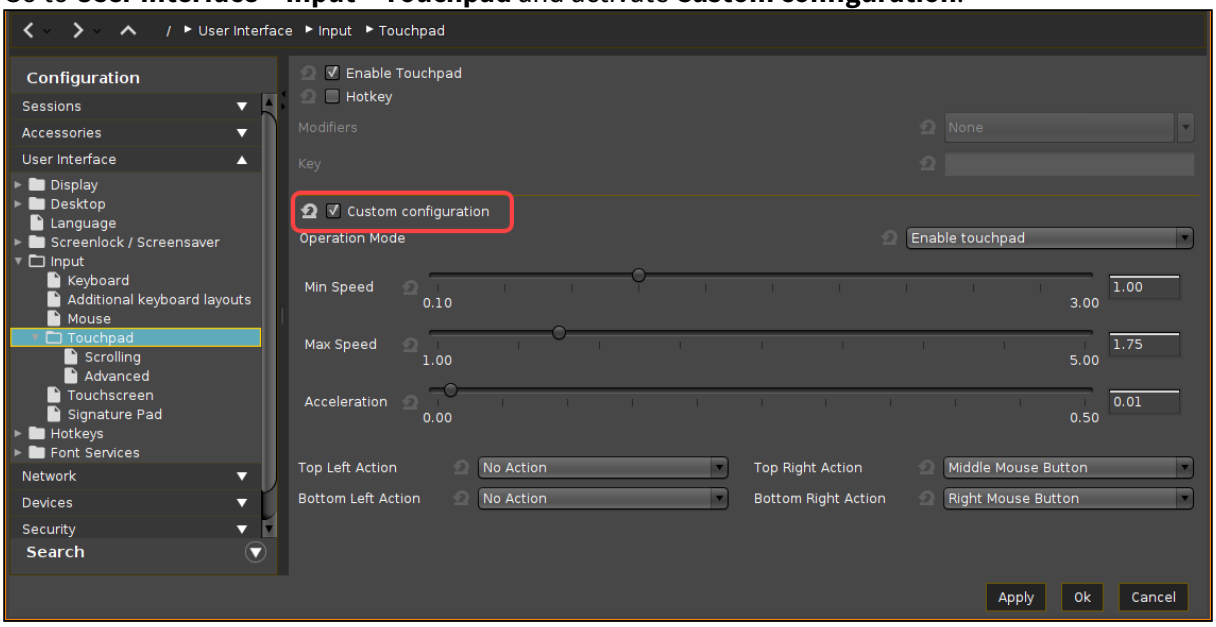
On IGEL OS devices, you are using a touchpad instead of a mouse and you want to reverse the scrolling direction to have natural scrolling – with the screen content moving synchronously to the fingers' movement on the touchpad.

Problem

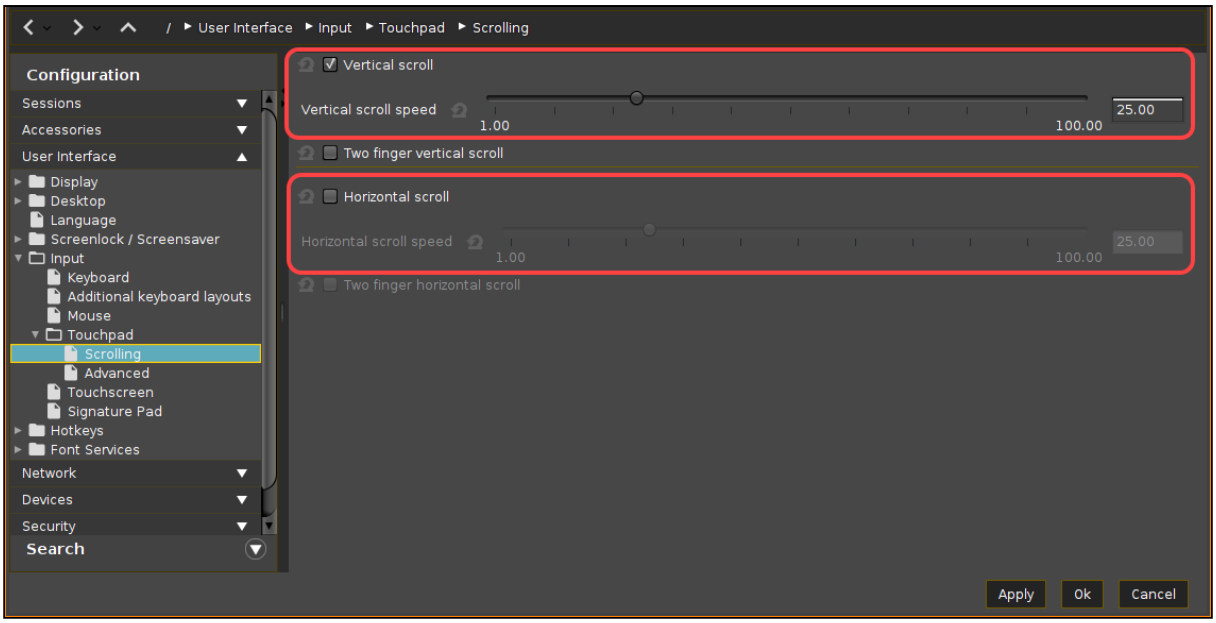
There is no "reverse scrolling" parameter in IGEL Setup.

Solution

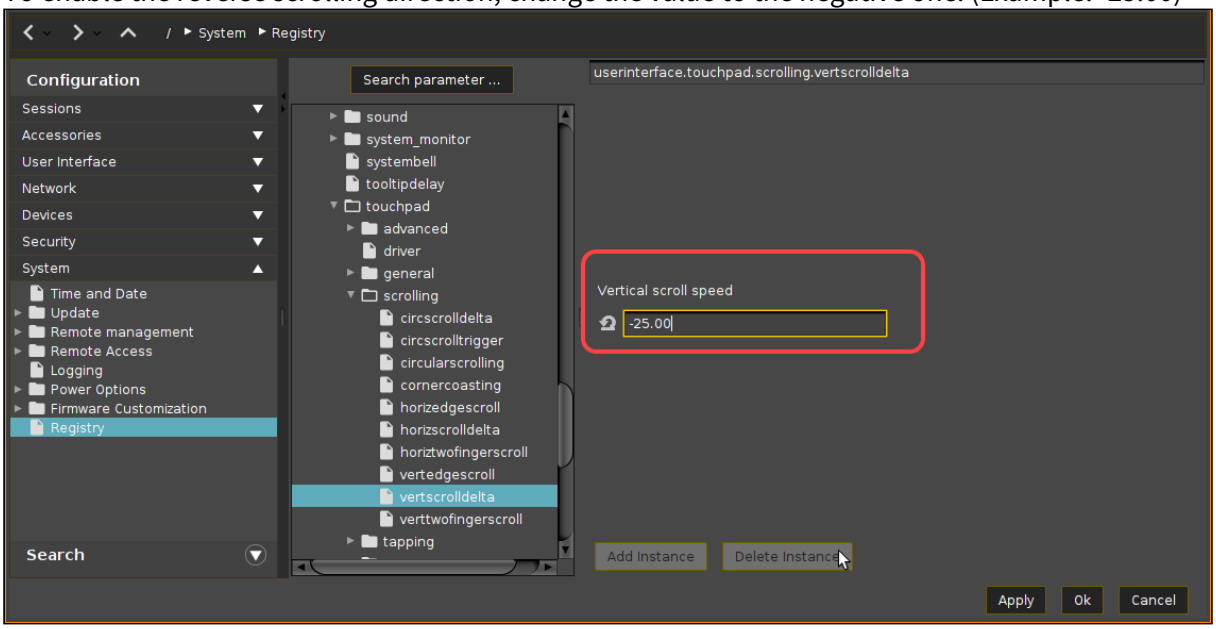
1. Open the device's configuration either locally or in the UMS.
2. Go to **User Interface > Input > Touchpad** and activate **Custom configuration**.



3. Under **Scrolling**, specify the **Vertical scroll speed** and, if required and supported, **Horizontal scroll speed**. (Default: 25.00)



4. Go to **System > Registry > userinterface > touchpad > scrolling > vertscrolldelta** and/or **horizscrolldelta**.
5. To enable the reverse scrolling direction, change the value to the negative one. (Example: -25.00)



If you want to enable the normal scrolling direction again, simply change the value back to the positive one.

6. Save the settings and restart the device.

Connecting a Serial Barcode Scanner

Connecting Barcode Scanner via COM Port

1. Determine to which COM port of the device the barcode reader is physically connected.
2. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach** and enable the relevant key, according to the COM port in use:
   - COM1 (`/dev/ttyS0`): **devices.serial.inputattach.com0.enabled**
   - COM2 (`/dev/ttyS1`): **devices.serial.inputattach.com1.enabled**
   - COM3, COM4 ...: Add a new instance by clicking **devices.serial.inputattach.com% > Add Instance** and define the port appropriately, e.g. `/dev/ttyS2` for COM3.
3. If the device's baud differs from 9600 (default), enter the correct baud under **devices.serial.inputattach.com0.baud**.

   With most barcode readers, you can change the baud by scanning a specific bar code.

4. In the Setup, click **Apply** or **Ok** to submit the new settings. To make absolutely sure that the new settings are effective, you can reboot the device.
5. Check if the barcode scanner is working.

Connecting Barcode Scanner via USB

If the barcode scanner is connected over USB, the challenge is to identify the device which is assigned to it. Depending on your specific device and environment, your mileage may vary. Start with the Connecting a Serial Barcode Scanner#simple procedure. If you are lucky, this will do it. If not, continue with the Connecting a Serial Barcode Scanner#extended procedure.

Simple Procedure

1. Connect the barcode to a USB port. This will trigger an event which will be logged and reported by dmesg.
2. Open a terminal on your endpoint device. For further information on the device's terminal, see Local Terminals (see page 1708).
3. To find the right device file, enter `dmesg | grep tty` in the terminal.

   If you are lucky, the relevant device file is listed. Its name is either `ttyUSB<NUM>` or `ttyACM<NUM>` . Example: `ttyUSB0`

   If the relevant device file is not listed, try the Connecting a Serial Barcode Scanner#extended procedure below.
4. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach**.
5. Set the **devices.serial.inputattach.com0.port** to the device file you have found. Example: If the device file is `ttyUSB0` , enter `/dev/ttyUSB0`

6. Activate **devices.serial.inputattach.com0.enabled**.
7. If the device's baud differs from 9600 (default), enter the correct baud under **devices.serial.inputattach.com0.baud**.

   With most barcode readers, you can change the baud by scanning a specific bar code.

8. Click **Apply** or **Ok** to submit the new settings. To make absolutely sure that the new settings are effective, you can reboot the endpoint device.
9. Check if the barcode scanner is working.

Extended Procedure: Device File Was Not Found on the First Go

If the device file could not be found using the simple procedure, try loading the device driver manually. As the explicit loading of the driver must be executed with every system start, a custom command must be added.

1. In the terminal, enter the following commands, one after the other:
   `modprobe cdc-acm`
   `dmesg | grep tty`
   The relevant device file is listed. Its name is either `ttyUSB<NUM>` or `ttyACM<NUM>`.
   Example: `ttyACM0`
2. Open the IGEL Setup, go to **System > Registry > devices > serial > inputattach**.
3. Set the **devices.serial.inputattach.com0.port** to the device file you have found. Example: If the device file is `ttyUSB0`, enter `/dev/ttyACM0`
4. Activate **devices.serial.inputattach.com0.enabled**.
5. If the device's baud differs from 9600 (default), enter the correct rate under **devices.serial.inputattach.com0.baud**.

   With most barcode readers, you can change the baud by scanning a specific barcode.

6. Go to **System > Firmware Customization > Custom Commands > Base** and under **Initialization**, enter `modprobe cdc-acm`
7. Click **Apply** or **Ok** to submit the new settings. Reboot the device.
8. Check if the barcode scanner is working.

Using DriveLock with IGEL Devices

Issue

DriveLock allows the system administrator to control access to removable devices within Citrix or RDP sessions. This is possible for USB devices; as of IGEL OS version 10.04.100, SATA devices are also supported.

Problem

How to integrate DriveLock solution with IGEL OS devices?

Solution

After configuring the Citrix or RDP server according to the original documentation, you have to activate the DriveLock virtual channel in the Setup.
See the original DriveLock documentation.

Using DriveLock with RDP:

1. In **Devices > Storage Devices > Storage Hotplug**, change the settings as follows:
    - Deactivate **Enable dynamic client drive mapping**.
    - Set **Number of storage hotplug devices** to 1 or higher.
    - Activate **Private drive letter for each storage drive**.
2. In **Sessions > RDP > RDP Global > Mapping > Drive Mapping**, change the settings as follows:
    - Activate **Enable Drive Mapping**.
3. In **Sessions > RDP > RDP Global > Mapping > Device Support**, change the settings as follows:
    - Activate **DriveLock channel**.

Using DriveLock with Citrix:

1. In **Devices > Storage Devices > Storage Hotplug**, change the settings as follows:
    - Deactivate **Enable dynamic client drive mapping**.
    - Set **Number of storage hotplug devices** to 1 or higher.
    - Activate **Private drive letter for each storage drive**.
2. In **Sessions > Citrix > Citrix Global > Mapping > Drive Mapping**, change the settings as follows:
    - Enable **Activate Drive Mapping**.
3. In **Sessions > Citrix > Citrix Global > Mapping > Device Support**, change the settings as follows:
    - Activate **DriveLock channel**.

Restricting the Mounting of Hotplug Storage Devices on IGEL Linux

Goal:

You want to restrict the mounting of hotplug storage devices.

Solution:

As of *IGEL Linux version 5.10.100*, the following registry keys let you disable the mounting of hotplug storage devices based on the device class (floppy, optical, harddisk, flash, other).

- `devices.hotplug.enable_floppy`
- `devices.hotplug.enable_optical`
- `devices.hotplug.enable_harddisk`
- `devices.hotplug.enable_flash`
- `devices.hotplug.enable_other`

These are all of type **bool**. Their default value is **true**. If true, mounting volumes on floppies, optical media, harddisks, flash memory devices, and others is enabled respectively.

> Even if the above settings allow mounting hotplug storage devices, the following settings may still restrict it:
> - **Devices > USB access control**
> - **Devices > Storage Devices > Storage Hotplug**

In order to disable mounting of a device class system-wide:

1. In setup, go to **System > Registry**.
2. In the **Parameter** tree, open **Devices** > **hotplug**.
3. To disable the mounting of a device class, uncheck its **Enable hotplug [...]** parameter.

When to Use USB Redirection

Document Purpose

In general, USB redirection is not needed for standard functionality such as audio, video, HID input, etc. However, in some special circumstances, a device may need to be redirected into a VDI session for full functionality, or if it requires a specific driver to function.

For webcams, seeWebcam Redirection and Optimization in IGEL OS (see page 1034).

Use USB redirection ONLY WHEN ABSOLUTELY REQUIRED.

In this document, we will define the best practices for using USB redirection in a VDI environment and go through the process with an example.

The example described here is for VMware Horizon, but it is similar for Citrix, RDS, and most other VDI technologies as well.

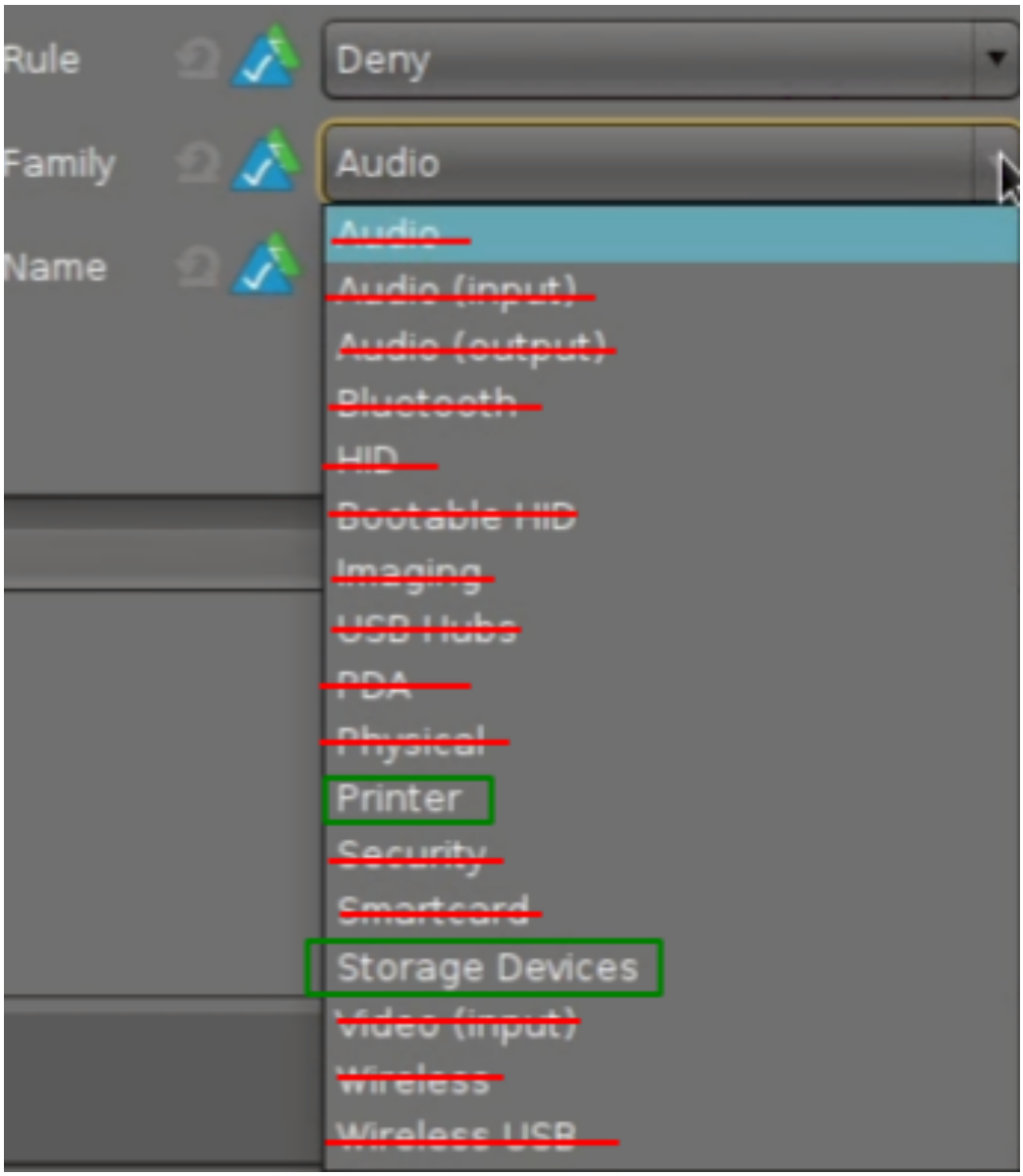
Best Practices for USB Redirection

Below are some general rules that, if followed, will provide the best performance and reliability when using USB redirection.

- ALWAYS set the default rule to "Deny".
- DO use VID and PID to redirect devices whenever possible. This is the best way to make sure that a device is redirected and that the USB virtual channels are not flooded with excess redirection.
- Enable USB redirection for the minimal amount of devices required to support user workflows
- As a rule, the USB classes below should NEVER be redirected. Instead, redirect individual devices in these classes using **Device Rules**.

Audio	**Audio (input)**	**Audio (output)**	**Bluetooth**
HID	**Bootable HID**	**Imaging**	**USB Hubs**
PDA	**Physical**	**Security**	**Smart Card**
Video (input)	**Wireless**	**Wireless USB**	

- The following classes may be redirected in specific circumstances:
  - **Printers**
    - Only if CUPS configurations or a third party does not fill this requirement
  - **Storage**
    - Only if mass storage options do not meet the requirements for user workflows or software compatibility



Rules are meant to be broken, right? If redirecting these classes is the only way things work, take a deeper look and see if there is a better way. If there is no obvious better way, then test thoroughly before moving into production.

Example: Redirecting a Nuance Powermic (Dictaphone)

Below we will run through the basic process of redirecting a single device into a Horizon VDI session from an IGEL device.

Some devices, including the Nuance Powermic, require custom split rules in Horizon, which will not be covered in this article. The splitting can be done with Horizon Group Policy on the VM, or as additional settings on IGEL. Please contact your vendor for their best practice for the devices.

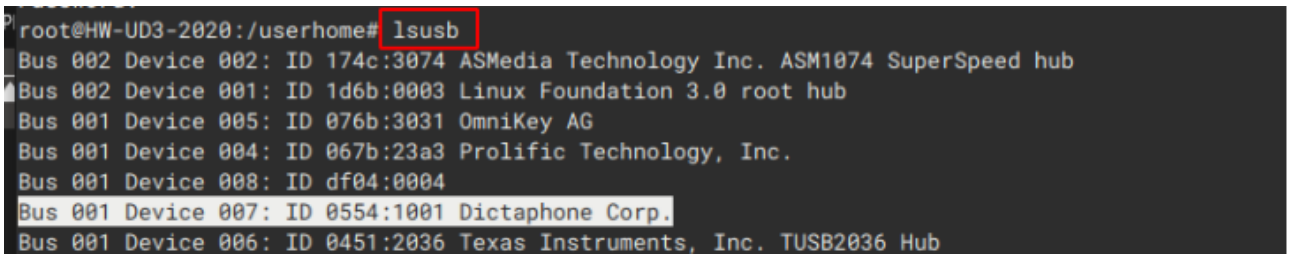
Prerequisites

1. Make sure that **Devices > USB Access Control** is disabled on IGEL OS devices, or make sure there are no USB access control rules restricting access to the USB device. More information about IGEL USB access can be found under USB Access Control (see page 2010).
2. USB redirection policies for Horizon/Citrix/RDS must be configured to allow redirection to happen.
3. The VDI image must have compatible drivers installed for the devices being redirected into the session.

Getting Device Information from IGEL

The first step that needs to be done is to identify the device's vendor ID and product ID which will be used to create our redirection rule.

1. Plug in the USB device to your endpoint device.
2. Connect to the IGEL OS device using SSH or **IGEL Secure Terminal**.
3. Log in as **user** with the user password set by the IGEL profile.
4. Type `su` to switch to the root account and provide the root password when prompted.
5. Run `lsusb` to display a list of devices and locate the device.
6. Note the **ID numbers** separated by a colon ":"
   a. In the Dictaphone example, this is `0554` and `1001`.
   b. The first number is the vendor ID (VID) and the second is the product ID (PID).



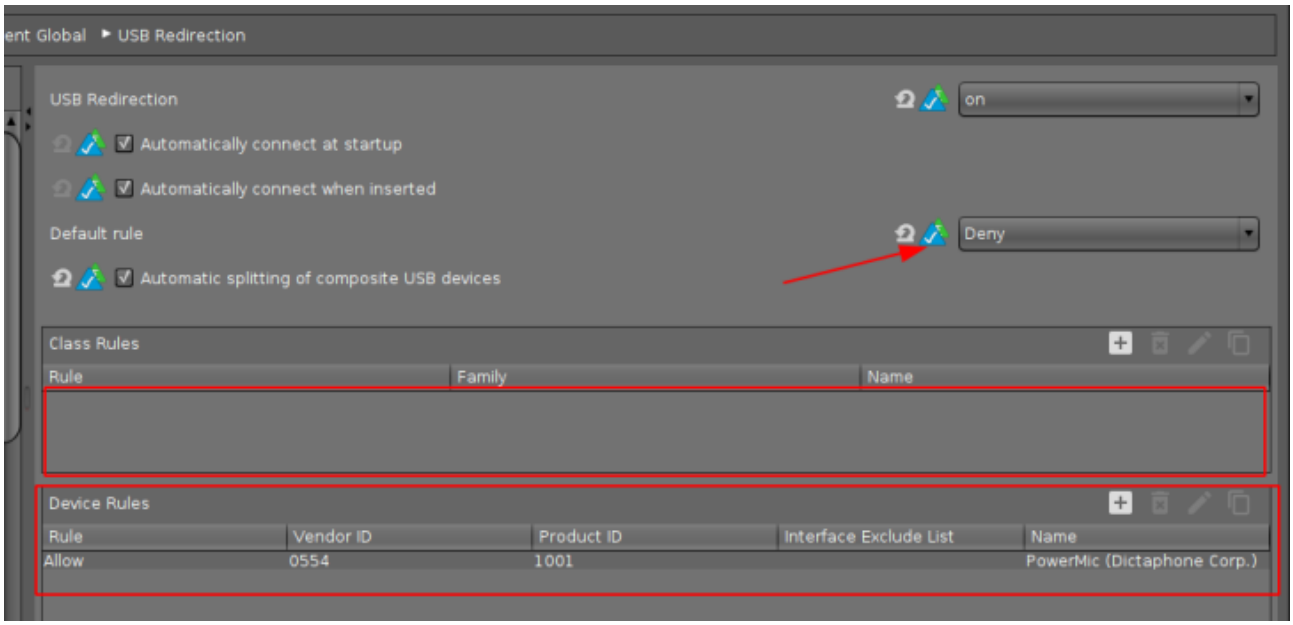
If the device cannot be easily identified by name, then disconnect the device and run `lsusb` again to see which one disappeared.

Configuring the IGEL Profile

1. Create a new profile in the UMS called "USB Redirection".
2. Go to the **USB Redirection** page for your session.
3. Set **USB Redirection** to "on" and set the **Default rule** to "Deny".
4. Make sure that both **Automatically connect at startup** and **Automatically connect when inserted** are both **enabled**.
5. Clear out any existing **Class Rules** that may have previously existed (if using an existing profile).
6. Add a **Device Rule** using the **Vendor ID** and **Product ID** collected in the previous section, and set it to "Allow".

   To make it easy, set the name of the rule to match the device name.

7. Apply the new profile to the device, and reboot for safe measures.
   The device should now be reflected in the Windows Device manager in the VDI session. If so, then the redirection rule is correct and working as expected.



If the device shows up as **unknown**, then, most likely, a driver will need to be installed in the OS to support the device.

How to Configure USB Access Control

You can allow and prohibit the use of USB devices on your endpoint device. Specific rules for individual devices or device classes are possible.

> The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.
> It is recommended to make settings for **USB Access Control** as the last step in the device configuration.
> Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.
> Note that the USB access control is completely separate than USB redirection for remote sessions, see When to Use USB Redirection (see page 1093).
> Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

Enable USB Access Control

1. Open the Setup and go to **Devices > USB Access Control**.
2. Enable the option **Enable**.
3. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.
4. Create one or more rules for classes of devices or individual devices.

Create a Class Rule

1. To create a new rule, click + in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Class ID**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Mass Storage**.
4. Under **Name**, give a name for the rule.
5. Click **OK**.
6. Save the changes.
   The rule is active.

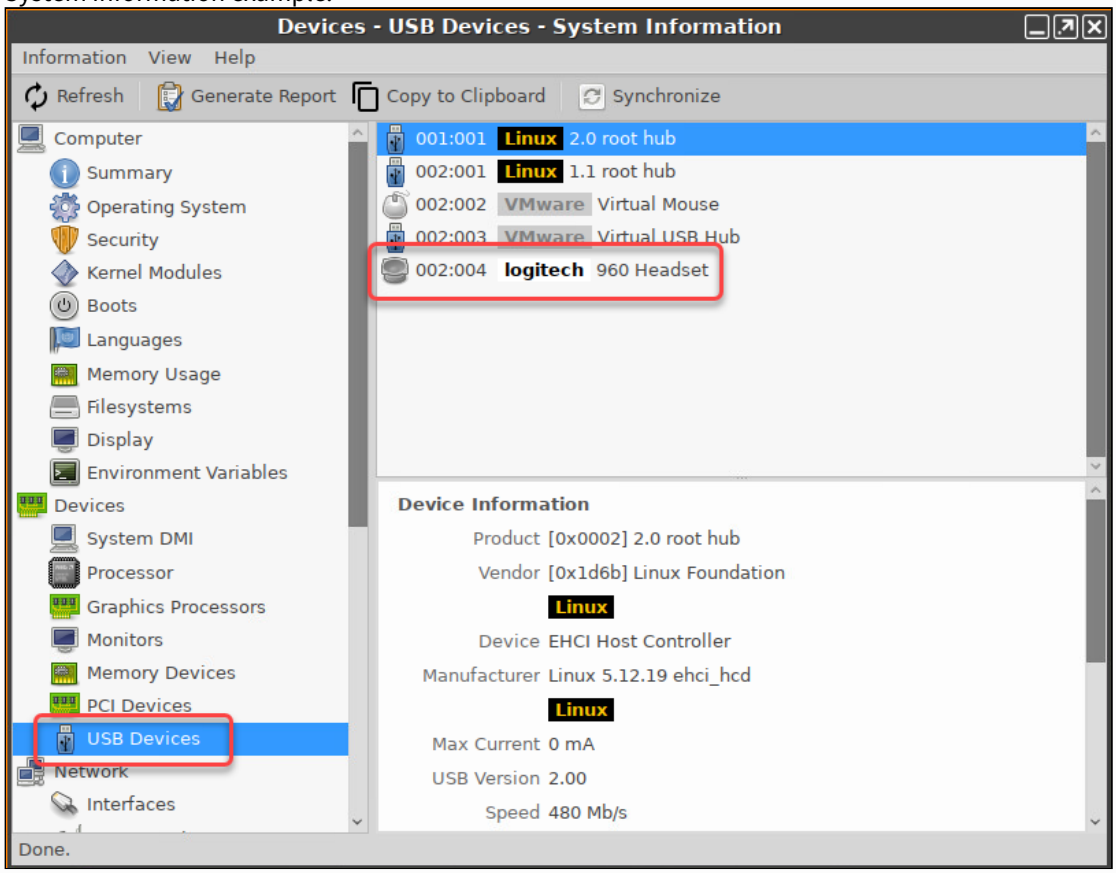
Create a Device Rule

> When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **UUID** must be given.

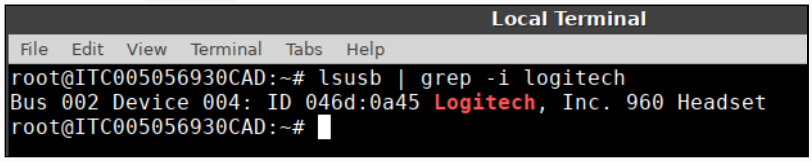
1. To create a new rule, click + in the **Device Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.
Example for `lsusb`:



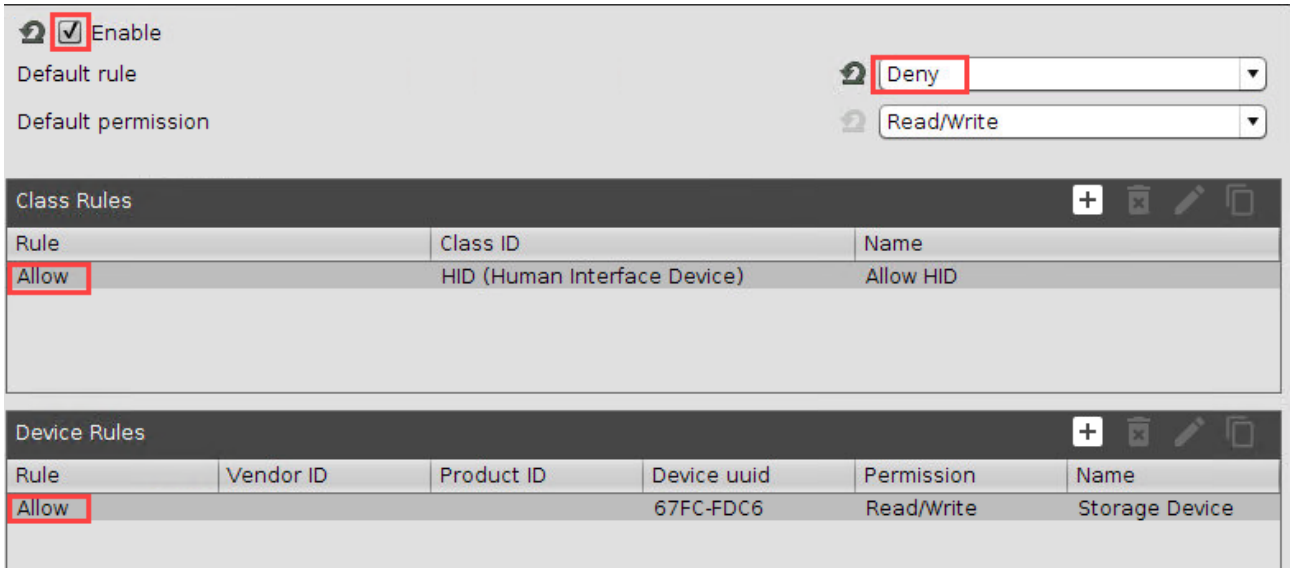
5. Give the **Device UUID** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.
   Possible values:
   - Global setting: The default setting for hotplug storage devices is used; see **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.
   - Read only

- Read/Write

7. Under **Name**, give a name for the rule.
8. Click **OK**.
9. Save the changes.
   The rule is active.

Example

- The set rule prohibits the use of USB devices on the device.
- A class rule allows the use of all entry devices (HID = Human Interface Devices).
- A device rule allows the use of the USB storage device with the UUID 67FC-FDC6.
- The use of all other USB devices, for example, storage devices or printers, is prohibited.



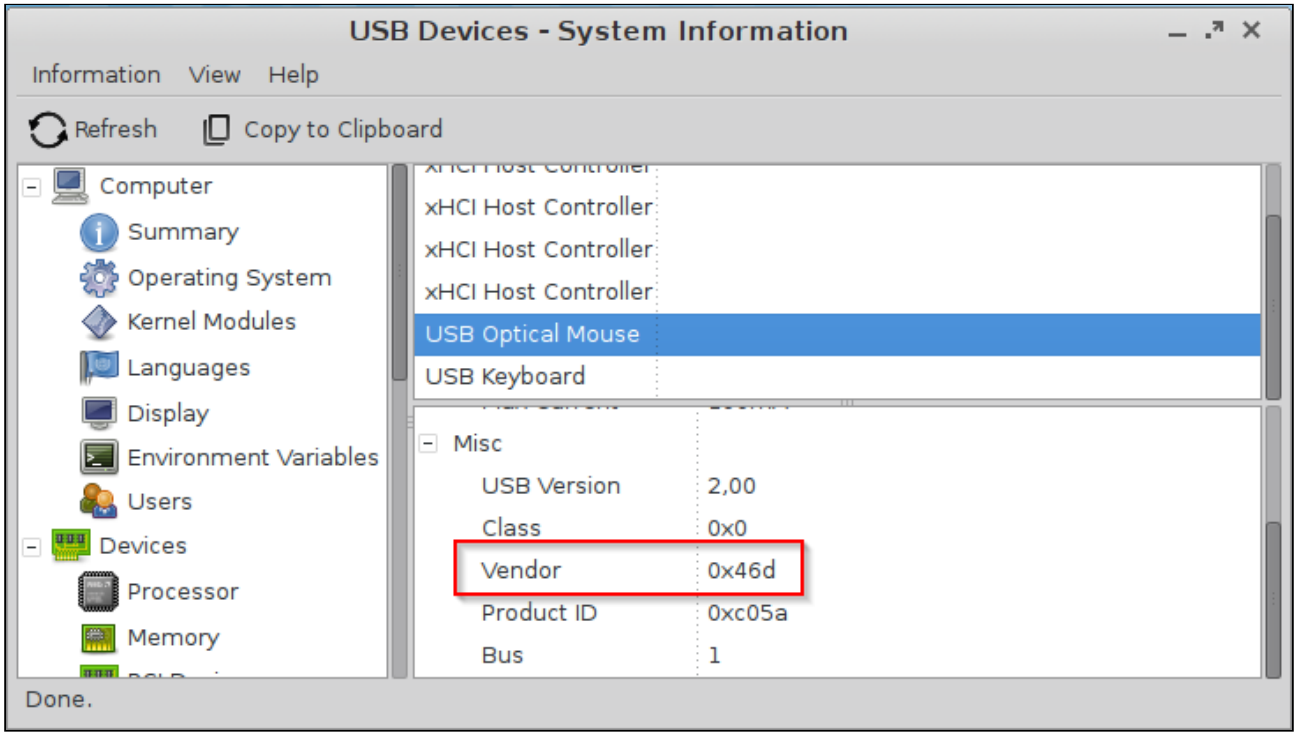
Issues with USB IDs in USB Devices Rules

Symptom

USB Device Rules you configured do not take effect.

Problem

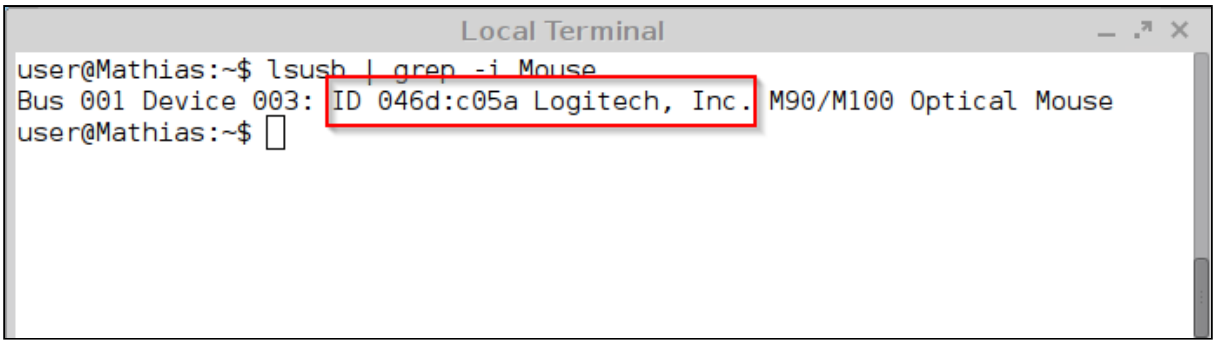
The System Information (see page 1794) tool in IGEL OS up to version 11.04.100 omits leading zeros in USB vendor and product IDs. These are shown only three hexadecimal digits long.



Solution

If you see three-digit USB IDs in **System Information**, use the `lsusb` command:

1. Open **Local Terminal**.
2. Enter the `lsusb` command.
3. Look for the device in question, possibly using `grep` to search in the `lsusb` output:
   `lsusb | grep -i [search term]`



4. Use the four-digit IDs that `lsusb` reports.

How Can I Fix Touchpad Issues?

Overview

On some notebooks, the touchpad does not work properly with IGEL OS. Some of these issues can be solved by adding or modifying parameters for the device driver. For usability, the parameter modifications are accessible via the Registry of the IGEL Setup.

If your changes do not seem to be effective after you confirmed them, reboot the device.

Issues and Solutions

Issues with the i2c-i801 Driver

The Registry parameter: `system.module_params.i2c_i801.blacklist` defines whether the i2c-i801 driver is to be blacklisted. The driver is blacklisted by default because it might cause system freezes. If the driver is blacklisted, some functions are not available.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > i2c_i801 > blacklist**. and select the desired option:
   - "Default": The decision of whether the i2c-i801 driver is blacklisted or not may change dependent on the hardware you are using.
   - "Yes": The i2c-i801 driver is blacklisted.
   - "No": The i2c-i801 driver is not blacklisted.
2. Click **Apply** or **Ok**.

Touchpad Is a Synaptics Intertouch Device

If your notebook has a Synaptics Intertouch touchpad, the Registry parameter `system.module_params.psmouse.synaptics_intertouch` should be enabled.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >synaptics_intertouch** and activate **Set this if touchpad is a synaptics intertouch device**.
2. Click **Apply** or **Ok**.

Touchpad Needs the A4tech Workaround

If your touchpad needs the A4tech workaround, enable it with the Registry parameter `system.module_params.psmouse.a4tech_workaround`. If you are unsure whether you need the A4tech workaround, ask your hardware vendor.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >a4tech_workaround** and activate **Set this if touchpad needs the a4tech workaround**.

2. Click **Apply** or **Ok**.

Changing the Compat Protocol

A solution for touchpad issues might lie in changing the communication protocol; this is done with the Registry parameter `system.module_params.psmouse.protocol`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >protocol** and select the desired option:
   - "Default": The system will detect the protocol automatically.
   - "PS/2"
   - "ImPS/2"
   - "ImExPS/2"
2. Click **Apply** or **Ok**.

Changing the Resolution

You can change the resolution for your touchpad via the Registry parameter `system.module_params.psmouse.resolution`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >resolution**, parameter **Resolution in dpi (0 means use default)**, and enter the desired resolution in dpi as an integer.
2. Click **Apply** or **Ok**.

Changing the Report Rate / Polling Rate

You can change the report rate resp. polling rate for your touchpad via the Registry parameter `system.module_params.psmouse.rate`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >rate**, parameter **Report rate in reports per second (0 means use default)**, and enter the desired report rate as an integer.
2. Click **Apply** or **Ok**.

Reset the Touchpad after a Defined Number of Lost Packages

You can force a reset of the touchpad after a defined number of data packages has been lost; the Registry parameter is `system.module_params.psmouse.resetafter`.

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >resetafter**, parameter **Reset device after so many packages (0 means never)**, and enter the desired number of packages as an integer.
2. Click **Apply** or **Ok**.

Forcing a Resync after a Defined Idle Time

1. In the Setup or the UMS configuration dialog, go to **System > Registry > system > module_params > psmouse >resync_time**, parameter **Mouse idle time before forcing resync in seconds (0 means never)**, and enter the desired number of seconds as an integer.
2. Click **Apply** or **Ok**.

How Do I Configure a Fujitsu PalmSecure Vein Scanner with IGEL OS?

You can use the Fujitsu PalmSecure Vein Scanner with IGEL OS endpoint devices to achieve highly secure authentication for remote sessions.

The following session types are supported:

- Microsoft RDP
- Citrix StoreFront
- VMware Horizon

To configure the Fujitsu PalmSecure Vein Scanner, you must first configure the middleware and then enable the passthrough authentication for your session.

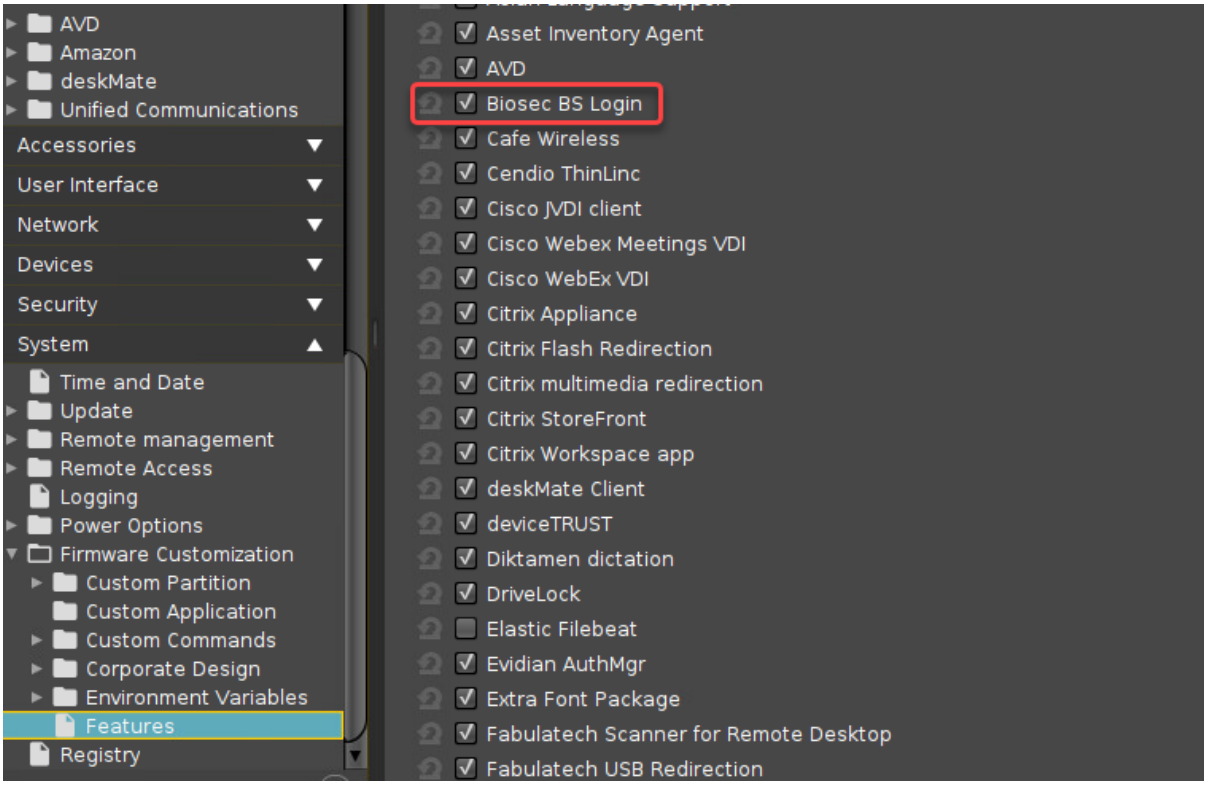
Environment

- IGEL OS 11.03.100 or higher

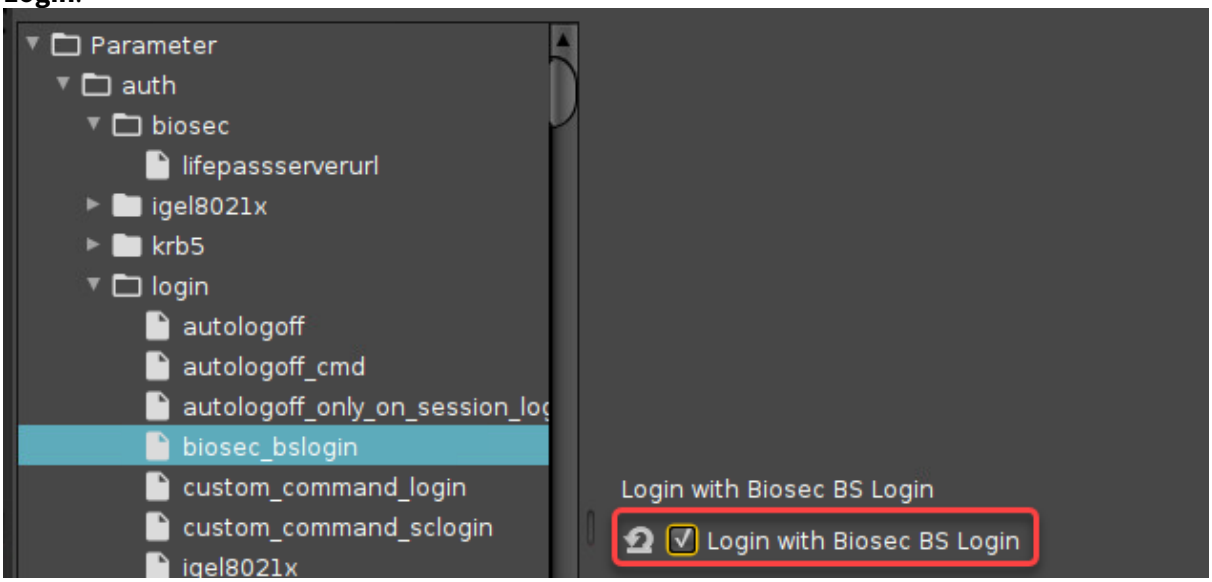
Configuring the BioSec Middleware

1. Open the local Setup of your device or the configuration dialog of the IGEL Universal Management Suite (UMS).
2. Go to **System > Firmware Customization > Features** and make sure that **Biosec BS Login** is enabled.

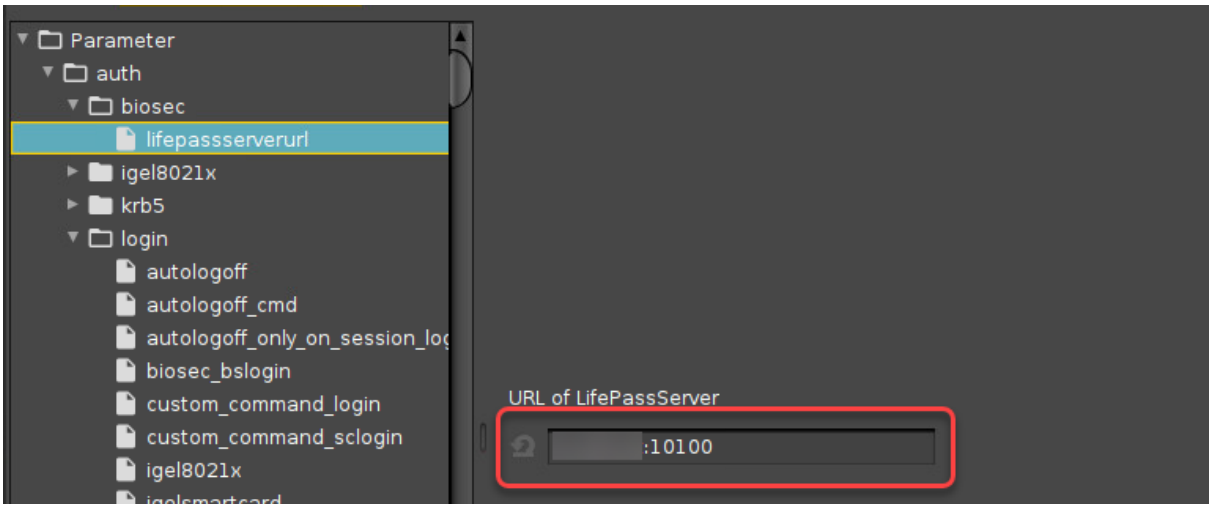
   If **Biosec BS Login** had been disabled beforehand, the firmware module must be downloaded first. Proceed as follows:
   - Make sure that the settings under **System > Update > Firmware Update** are correct; for details, see Firmware Update Settings for IGEL OS (see page 2056). If you are using Universal Firmware Update, the settings should be correct.
   - Save your changes.
   - Reboot the device.
     The firmware module for BioSec login is downloaded on reboot.



3. Go to **System > Registry > auth > login > biosec_bslogin** and activate **Login with Biosec BS Login**.



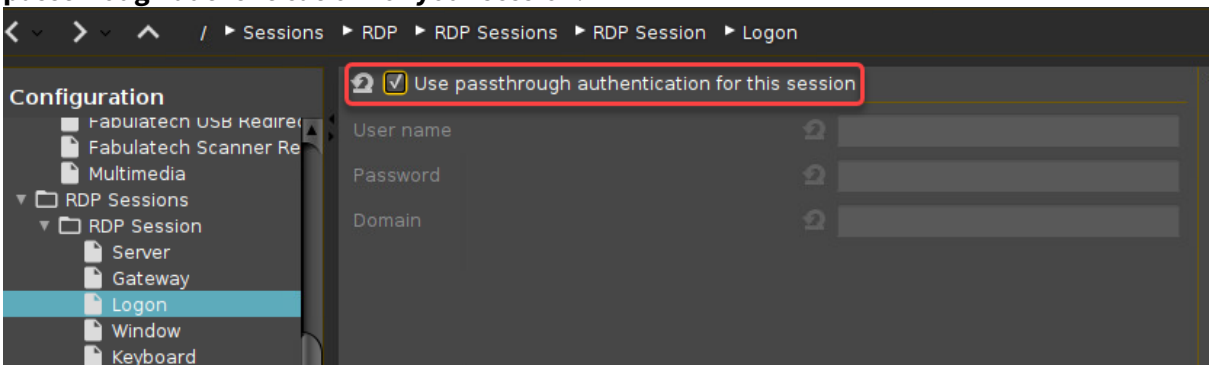
4. Go to **System > Registry > auth > biosec > lifepassserverurl** and enter the URL of the LifePass server.



Enabling Passthrough

For RDP Sessions

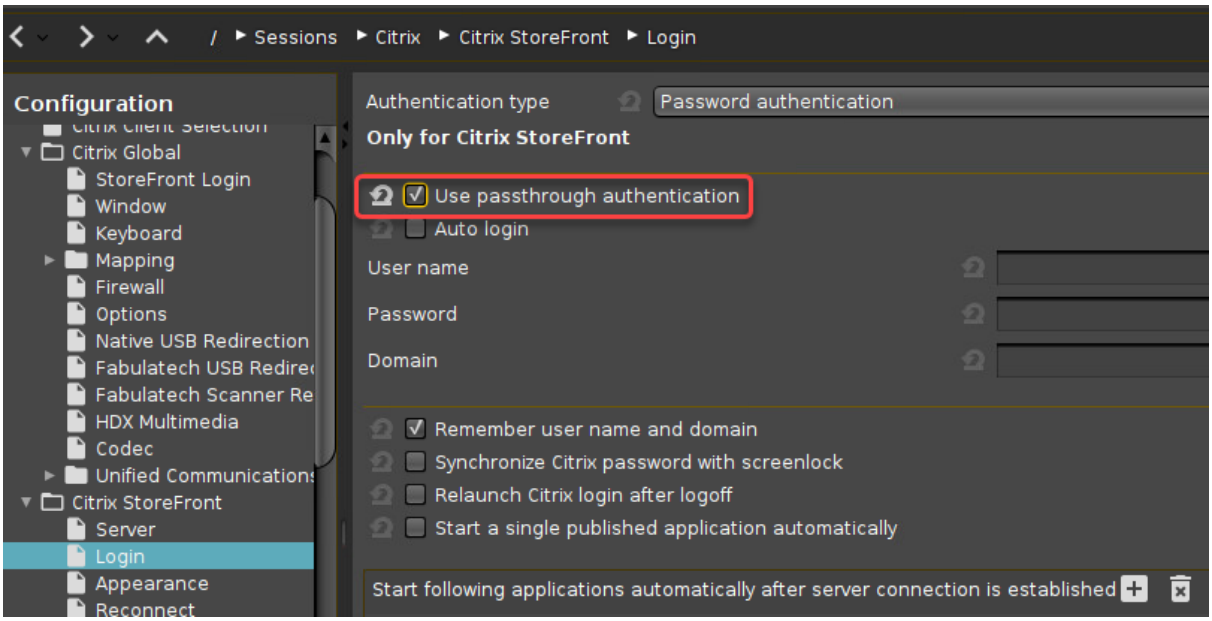
1. Go to **Sessions > RDP > RDP Sessions > [name of your RDP session] > Login** and enable **Use passthrough authentication for your session**.



2. Save your changes.

For Citrix StoreFront Sessions

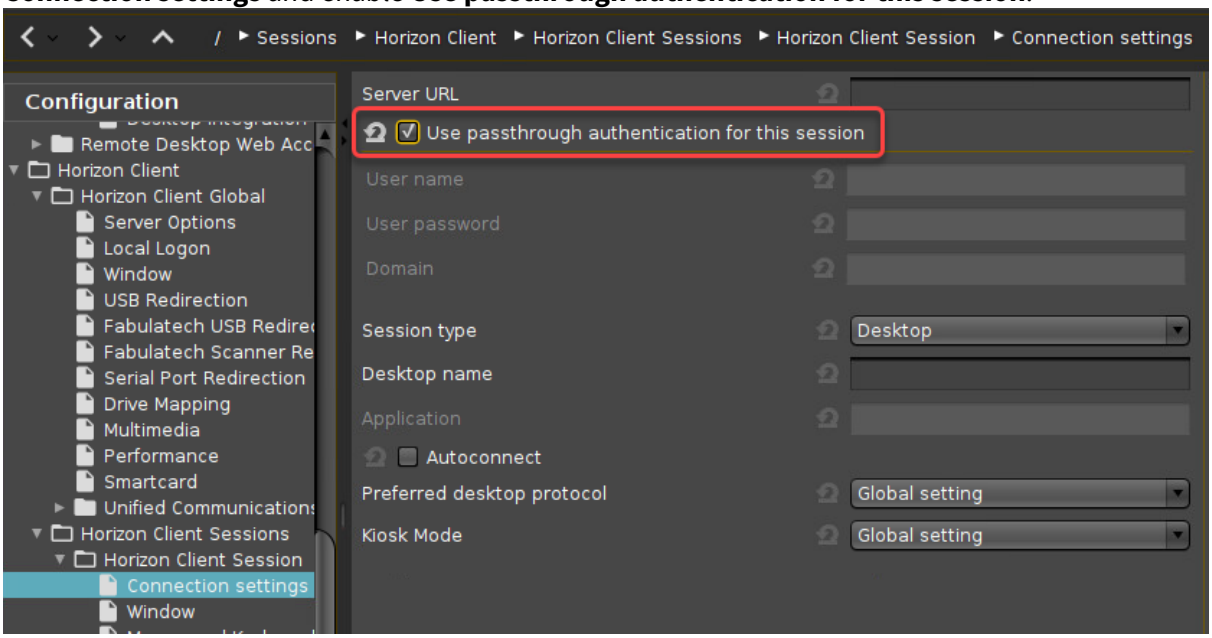
1. Go to **Sessions > Citrix > Citrix StoreFront > Login** and enable **Use passthrough authentication**.



2. Save your changes.

For VMWare Horizon Sessions

1. Go to **Sessions > Horizon Client > Horizon Client Sessions > [name of your Horizon session] > Connection settings** and enable **Use passthrough authentication for this session**.



2. Save your changes.

Virtual Background for Unified Communication Apps in IGEL OS

Most modern Unified Communication solutions are able to hide the background behind the person that sits in front of the webcam. Typically, the background is blurred out, or replaced with an image or a video.

For those Unified Communication apps that do not support this feature, at least not in a VDI context, IGEL OS provides a universal virtual background that can be used by any Unified Communication solution. This is achieved by creating a virtual webcam; within this virtual webcam, the virtual background is mixed with the video input from the real webcam. The video stream from the virtual webcam is then fed to the Unified Communication client.

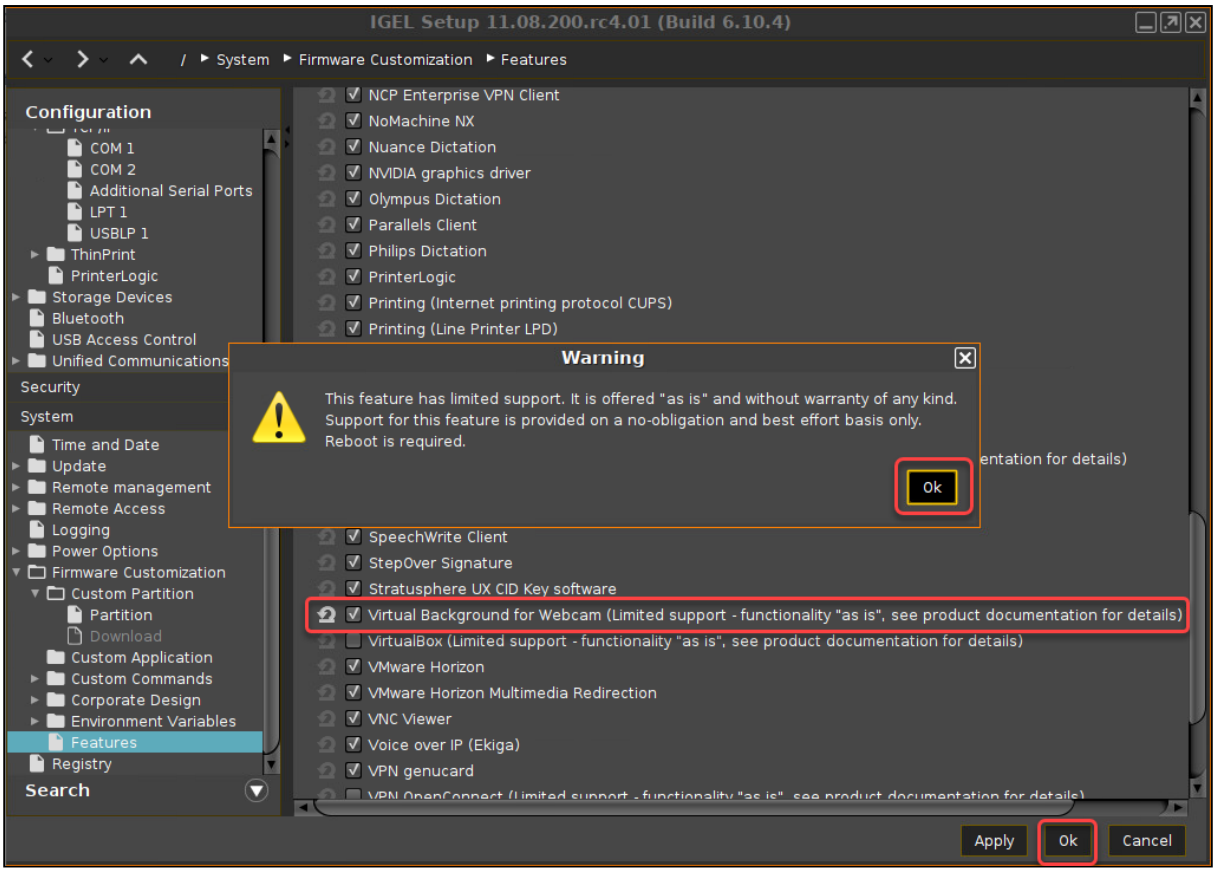
> **Feature with Limited Support**
>
> This feature has limited support; for more information, please refer to What is the Meaning of "Features with Limited Support"?

Minimum Hardware Requirements

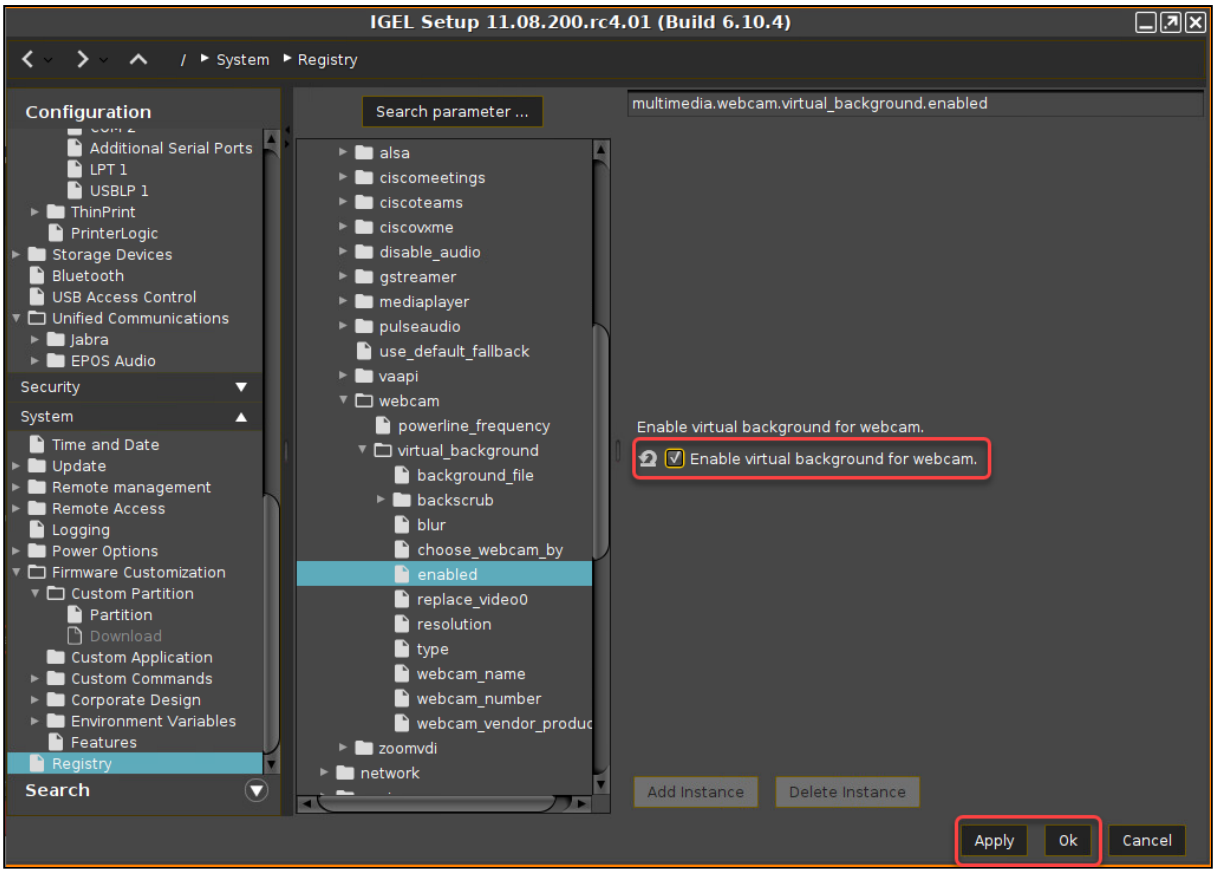
- 4 GB RAM
- Quad Core CPU with 1.5 GHz or higher

Enabling the Virtual Background Feature

1. In the UMS configuration dialog or the local Setup, go to **System > Firmware Customization > Features**.
2. Activate **Virtual Background for Webcam (Limited support - functionality "as is", see product documentation for details)**, confirm the warning, and click **Ok**.



3. Reboot the endpoint device.
4. Go to **System > Registry > multimedia > webcam > virtual_background > enabled** and activate **Enable virtual background for webcam** and click **Ok** or, if you want to change further settings, click **Apply**.



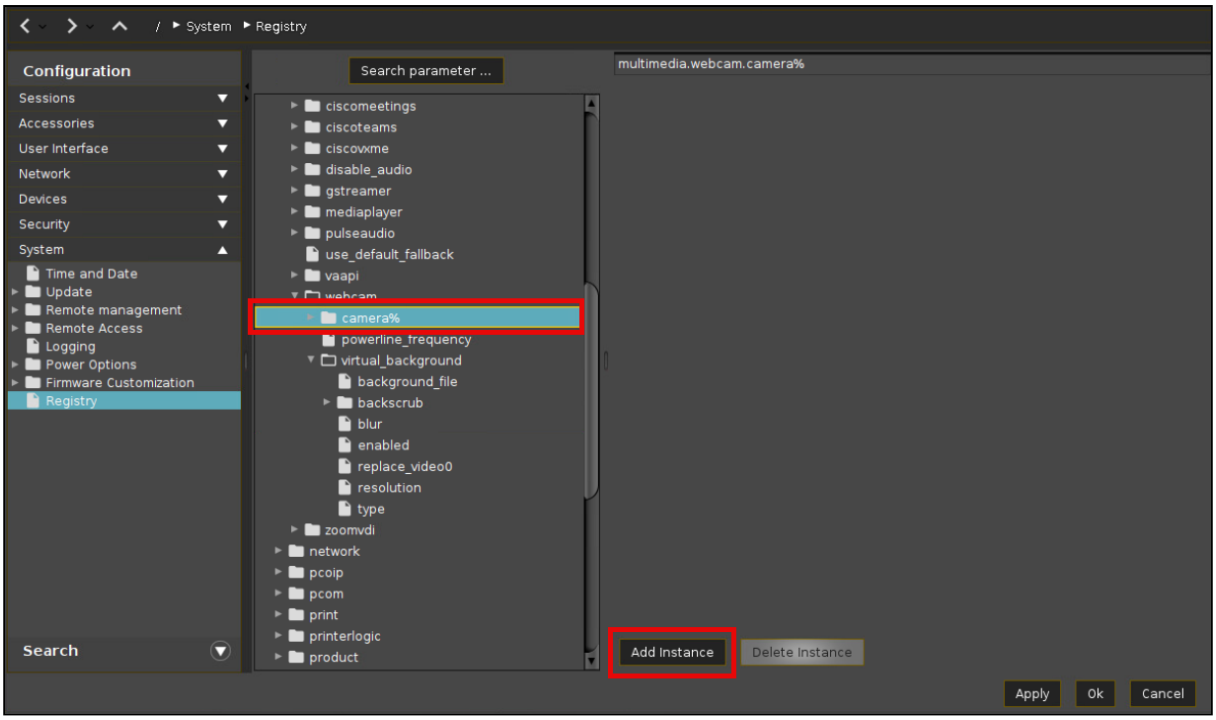
The virtual background provided by the virtual webcam can be used with the default settings.

Selecting the Webcam to Provide Input to the Virtual Webcam

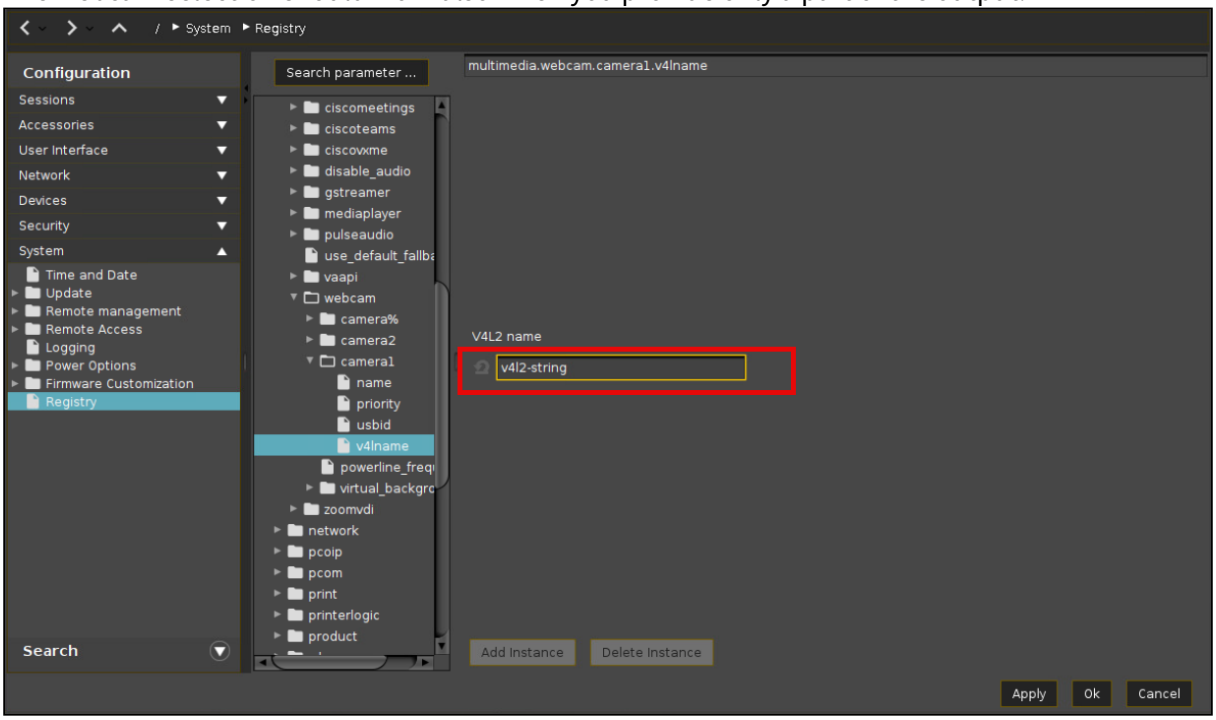
As of IGEL OS 11.10.250, the configuration of webcam priority has been changed. V4L name is used for identifying the webcam. If only one webcam is present, no configuration is needed. In case multiple webcams are present, the first initialized webcam will be used if the priority is not set.

If you use several webcams and need to configure their priority, proceed as follows:

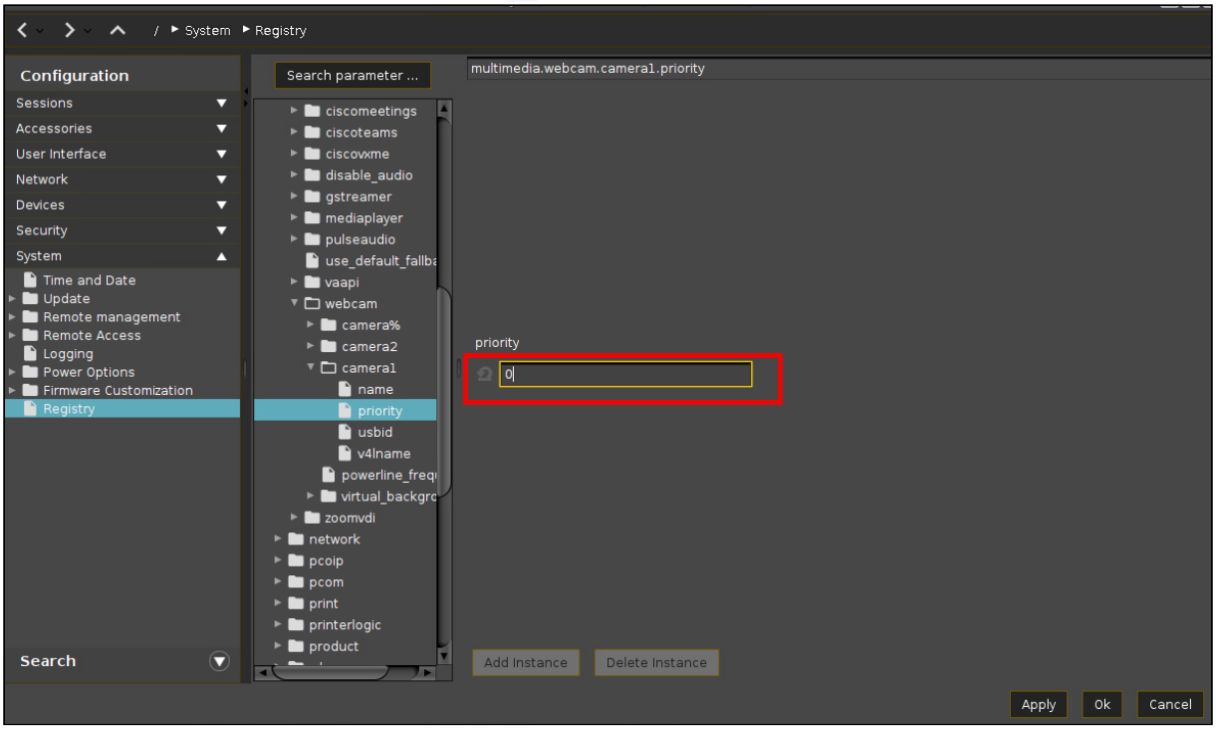
1. Go to **System > Registry > multimedia > webcam > camera%** and click **Add Instance** to add the required number of instances, e.g. two instances if two webcams are used.



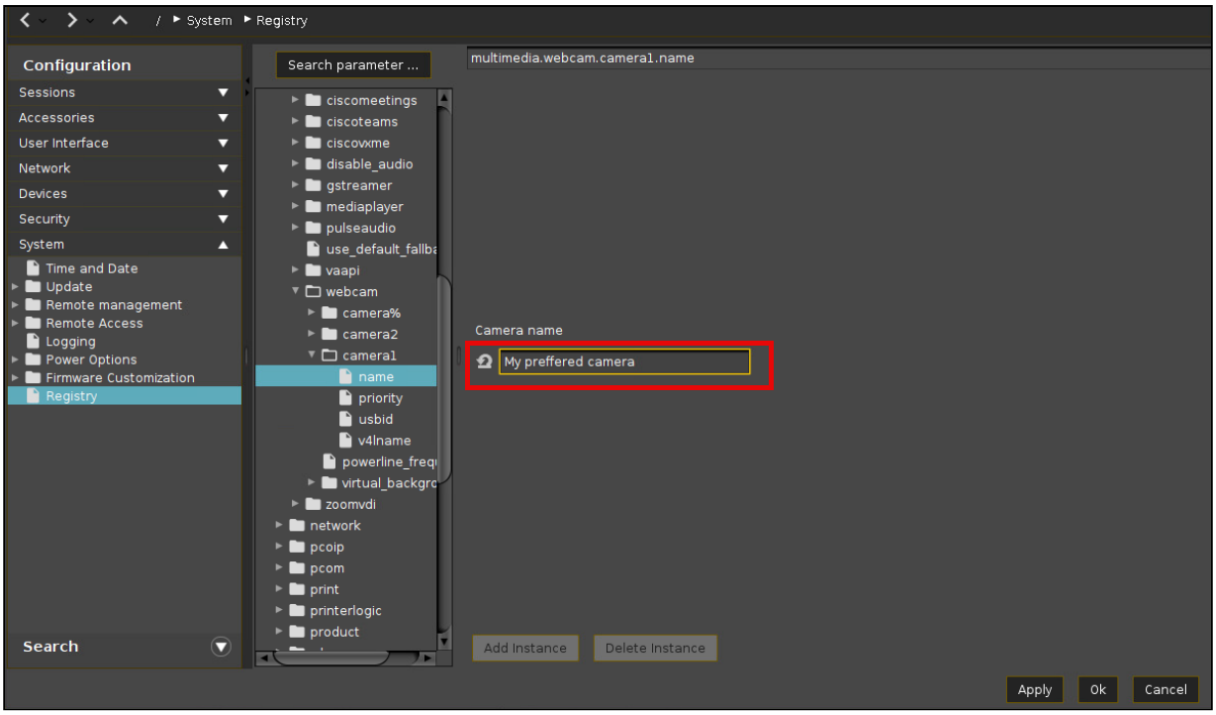
2. Select the created instance and set **System > Registry > multimedia > webcam > [camera instance] > v4lname** to the name of the desired webcam. To get the V4L2 webcam name, you can use the command `v4l2-ctl --list-devices`.
   The webcam selection should work also when you provide only a part of the output.



3. Under **System > Registry > multimedia > webcam > [camera instance] > priority**, set the priority, e.g. `0,1,2`.
   Note that lower number means higher priority, i.e. if available, the webcam with priority `0` will be used first, then the webcam with priority `1`, etc.



4. Set **System > Registry > multimedia > webcam > [camera instance] > name** to the desired display name for the camera.

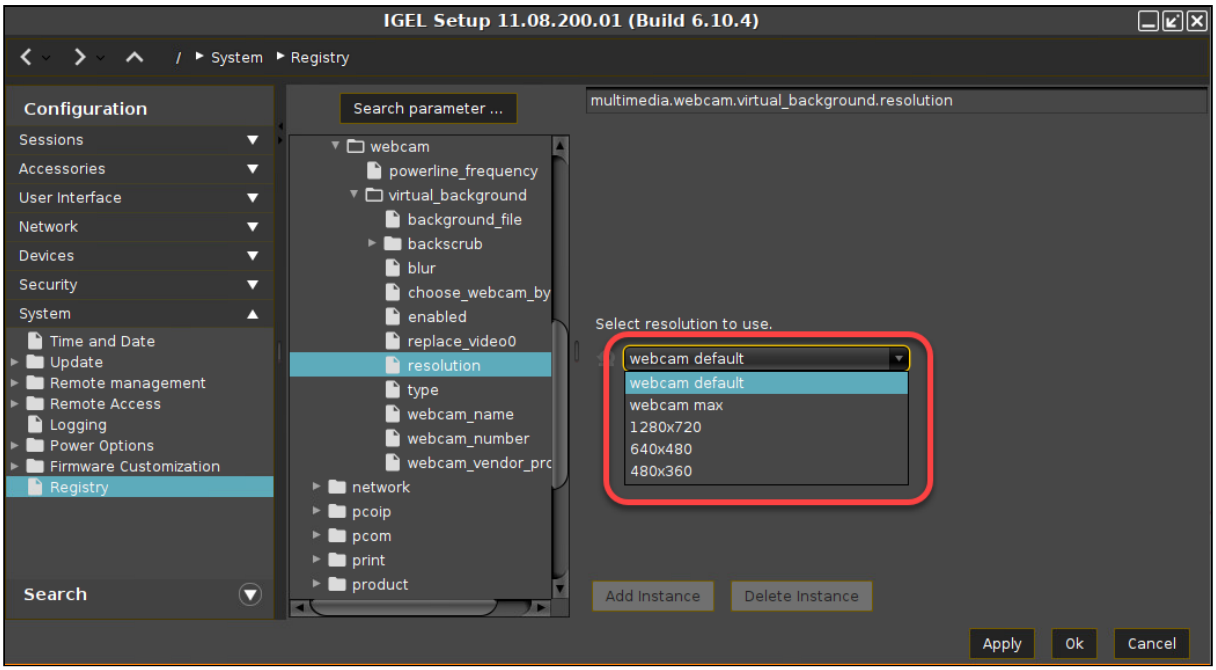


5. Repeat these actions for all added camera instances.
6. Click **Apply** or **OK** to save the settings.

Selecting the Resolution of the Webcam

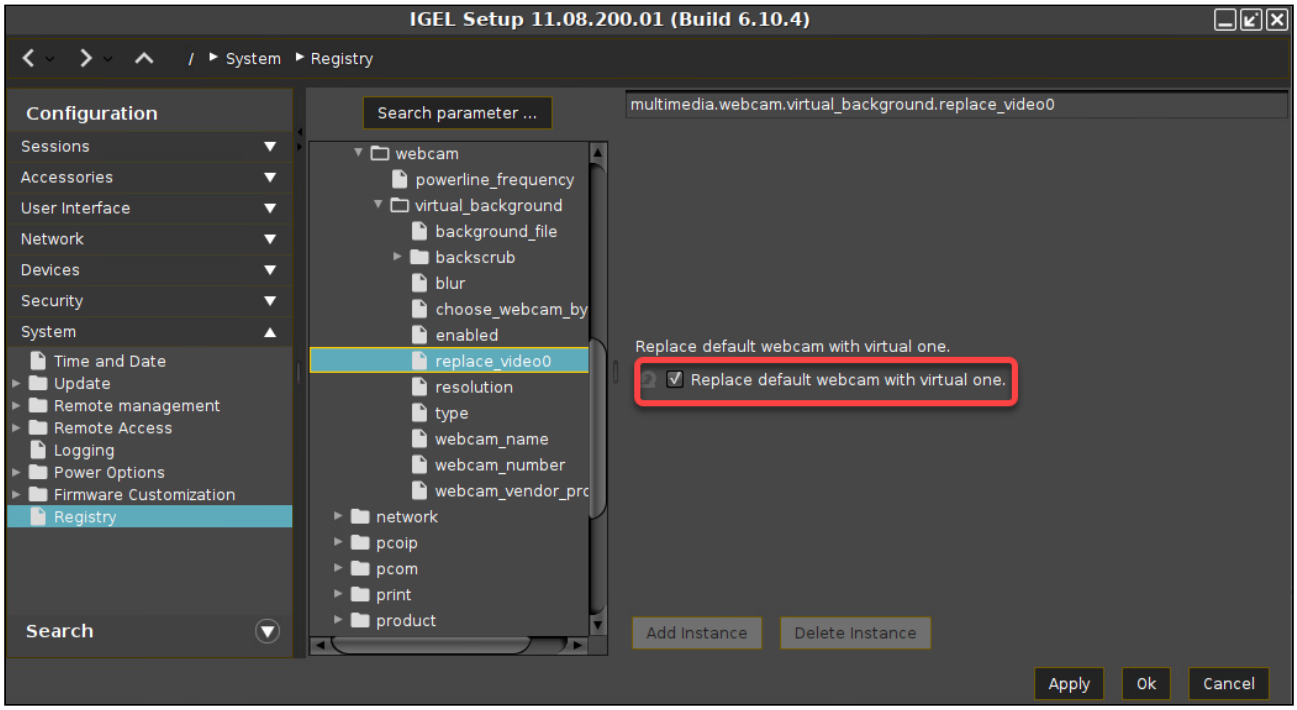
→ Go to **System > Registry > multimedia > webcam > virtual_background > resolution** and choose from the possible options:

- **webcam default**: The default resolution of the webcam.
- **webcam max**: The maximum resolution of the webcam.
- **1920x1080**
- **1280x720**
- **640x480**
- **480x360**
- **424x240**
- **320x240**
- **320x180**



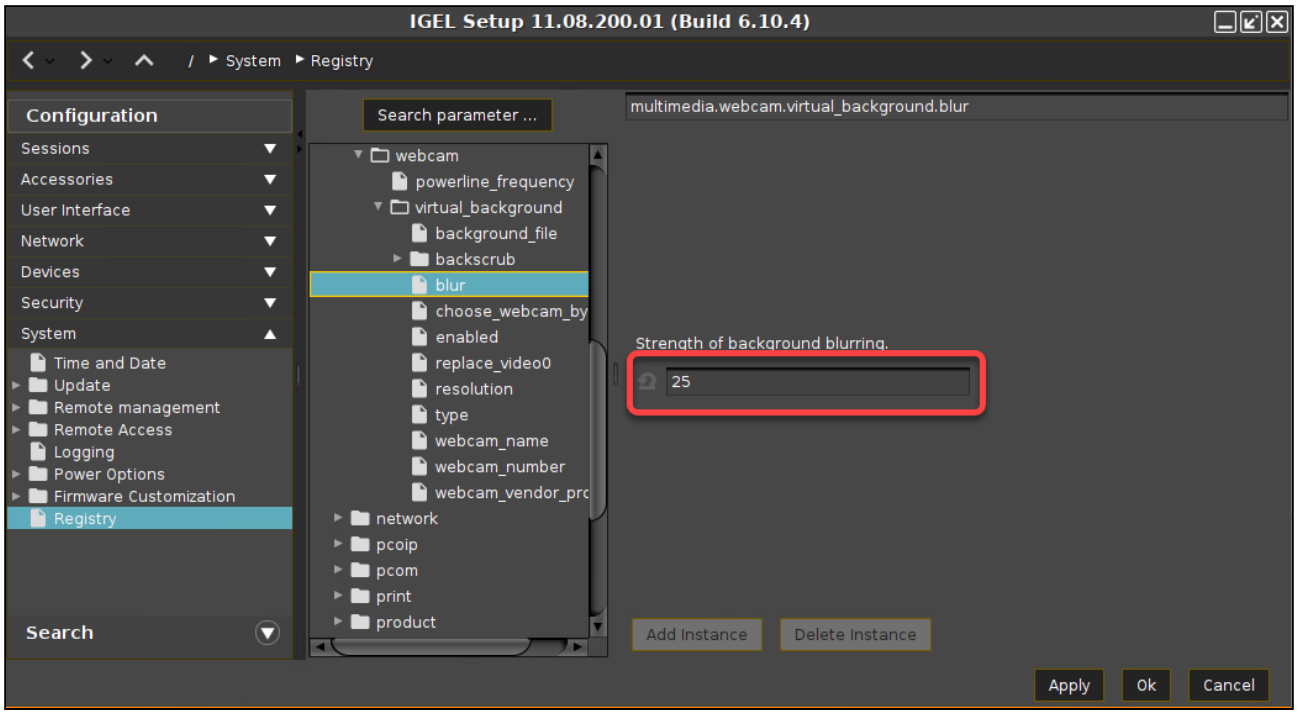
Setting the Virtual Webcam as Default Webcam

→ Go to **System > Registry > multimedia > webcam > virtual_background > replace_video0** and make sure that **Replace default webcam with virtual one** is activated.



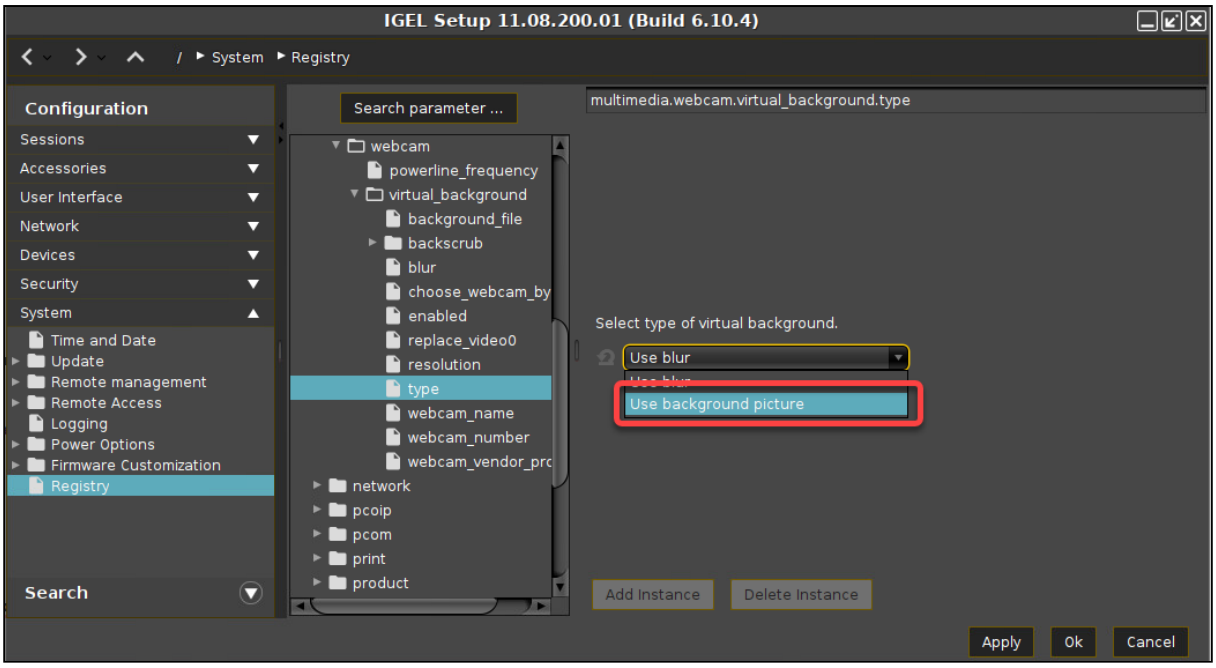
Setting the Strength of Background Blurring

→ Go to **System > Registry > multimedia > webcam > virtual_background > blur** and set the value of **Strength of background blurring** according to your needs.
Range: 1 (minimal blurring) ... 100 (maximal blurring)

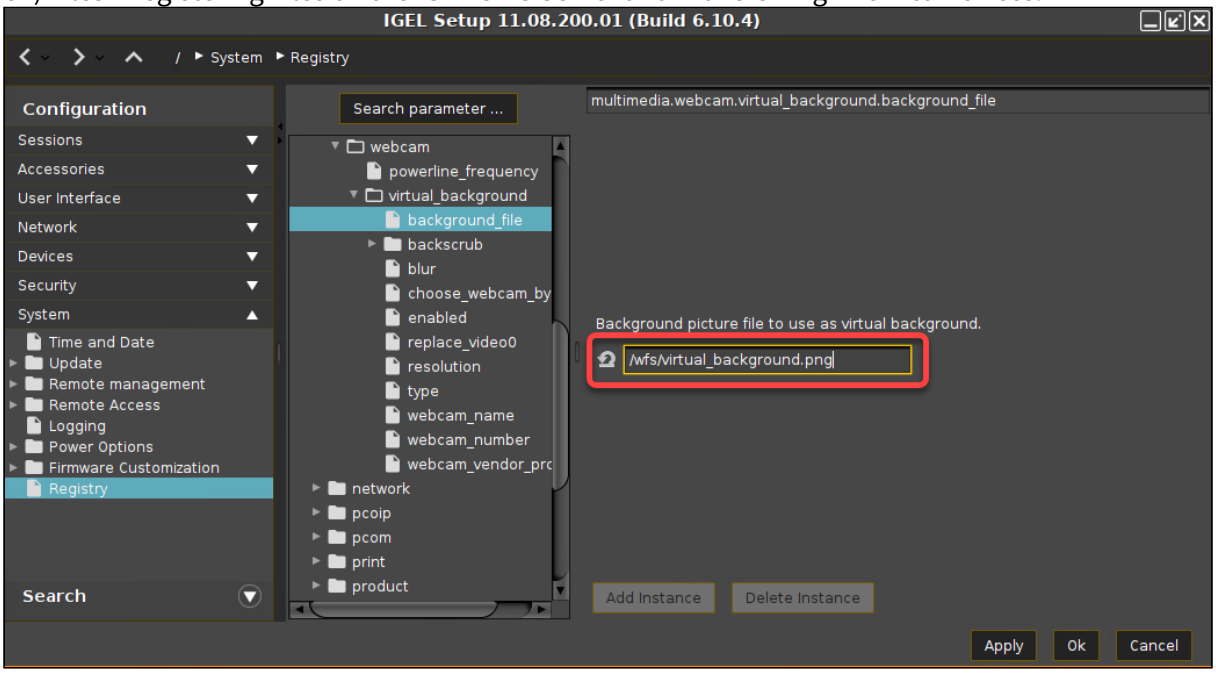


Using an Image as Virtual Background Instead of Blurring the Background

1. Go to **System > Registry > multimedia > webcam > virtual_background > type** and set **Select type of virtual background** to **Use background picture**.



2. Go to **System > Registry > multimedia > webcam > virtual_background > background_file** and enter the path to the background image file under **Background picture file to use as virtual background**. For instructions on how to transfer the file to your endpoint device, see (12.07.100-en) Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices.

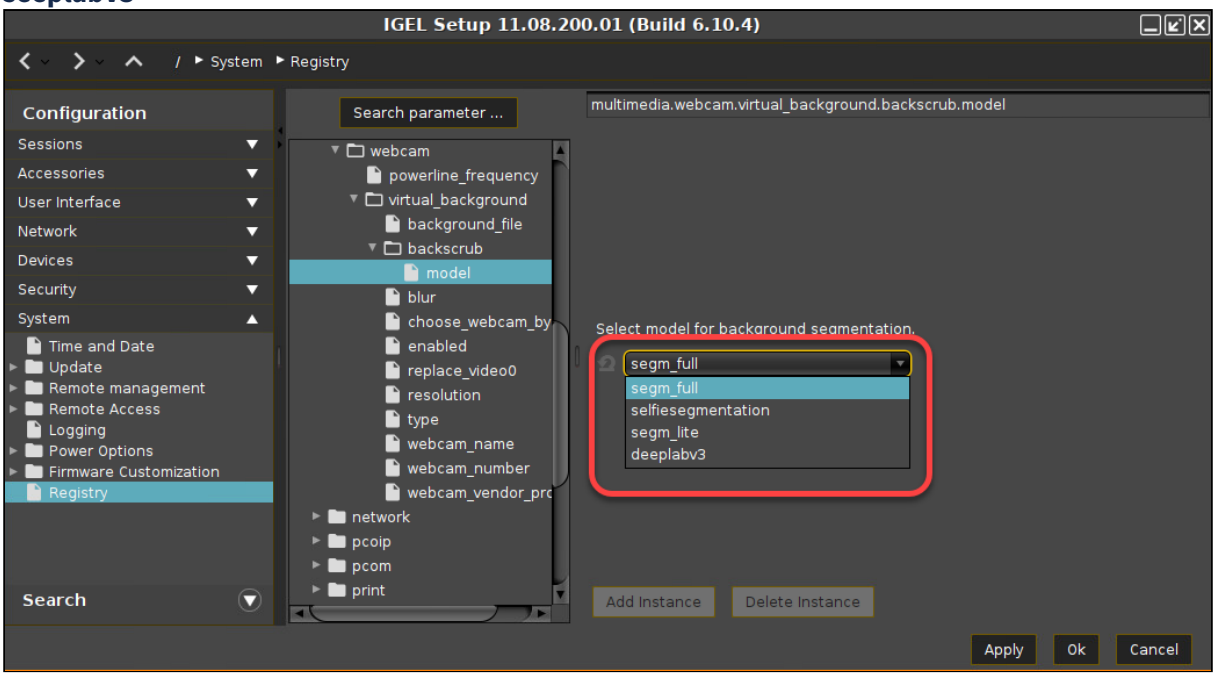


Selecting the Model for Background Segmentation

You can select the method of discerning the foreground, i.e. the person, from the background.

→ Go to **System > Registry > multimedia > webcam > virtual_background > backscrub > model** and choose from the possible options:

- **segm_fill**
- **selfiesegmentation**
- **segm_lite**
- **seeplabv3**



Printer

- How to Map a Local Printer to a Citrix or RDP Session on IGEL OS (see page 1121)
- Print Server Configuration (see page 1127)
- Installing a Custom CUPS Driver (see page 1130)
- Dynamic Selection of the Default Printer on IGEL OS (see page 1131)

How to Map a Local Printer to a Citrix or RDP Session on IGEL OS

This article explains how to map a standard USB laser or ink-jet printer into a Citrix or Remote Desktop (RDP) session on IGEL OS.

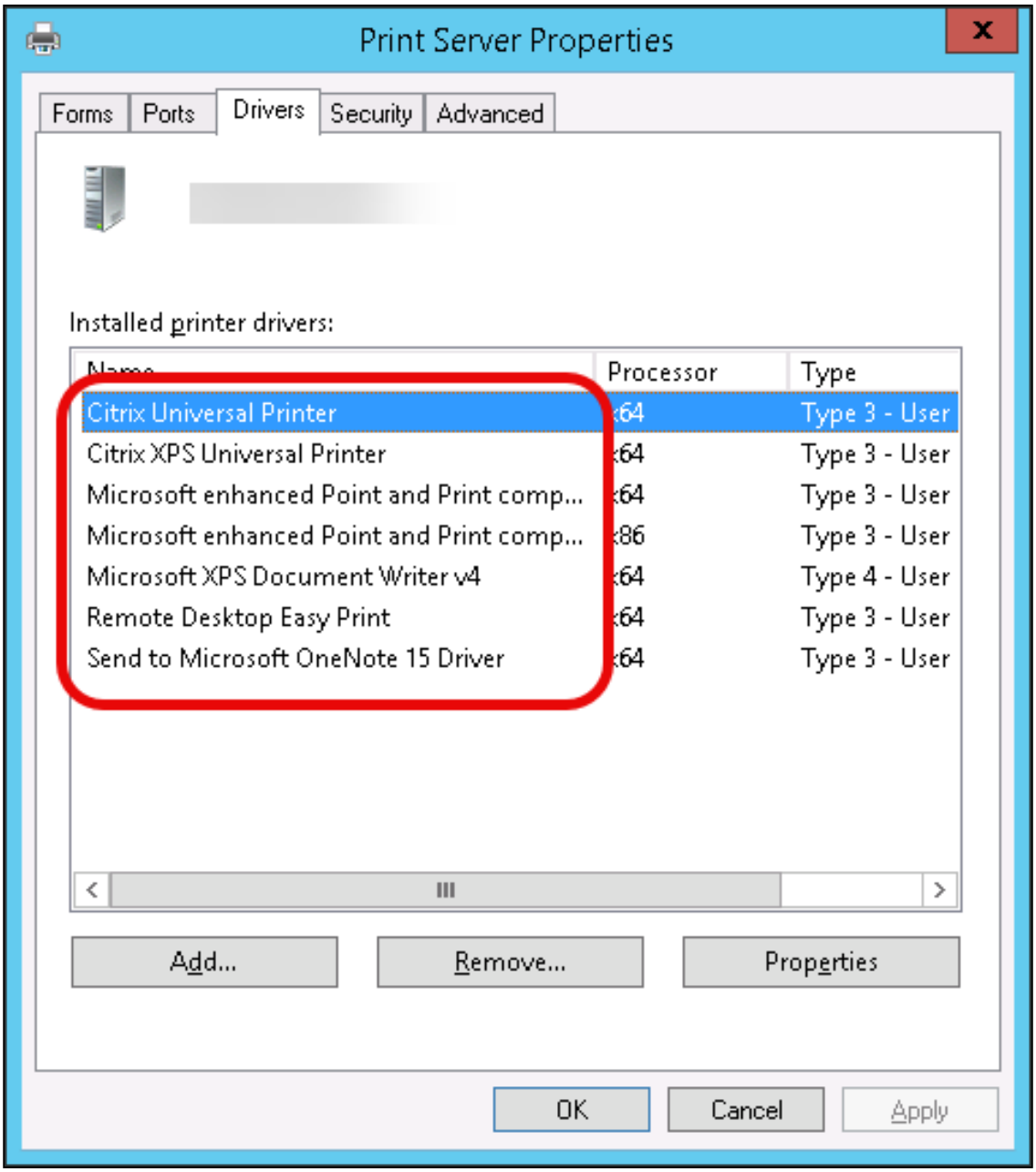
> This method may not work with specialty printers (i.e. label printers, or heat printers). If this does not work for your printer, you may need to use USB redirection.

Prerequisites

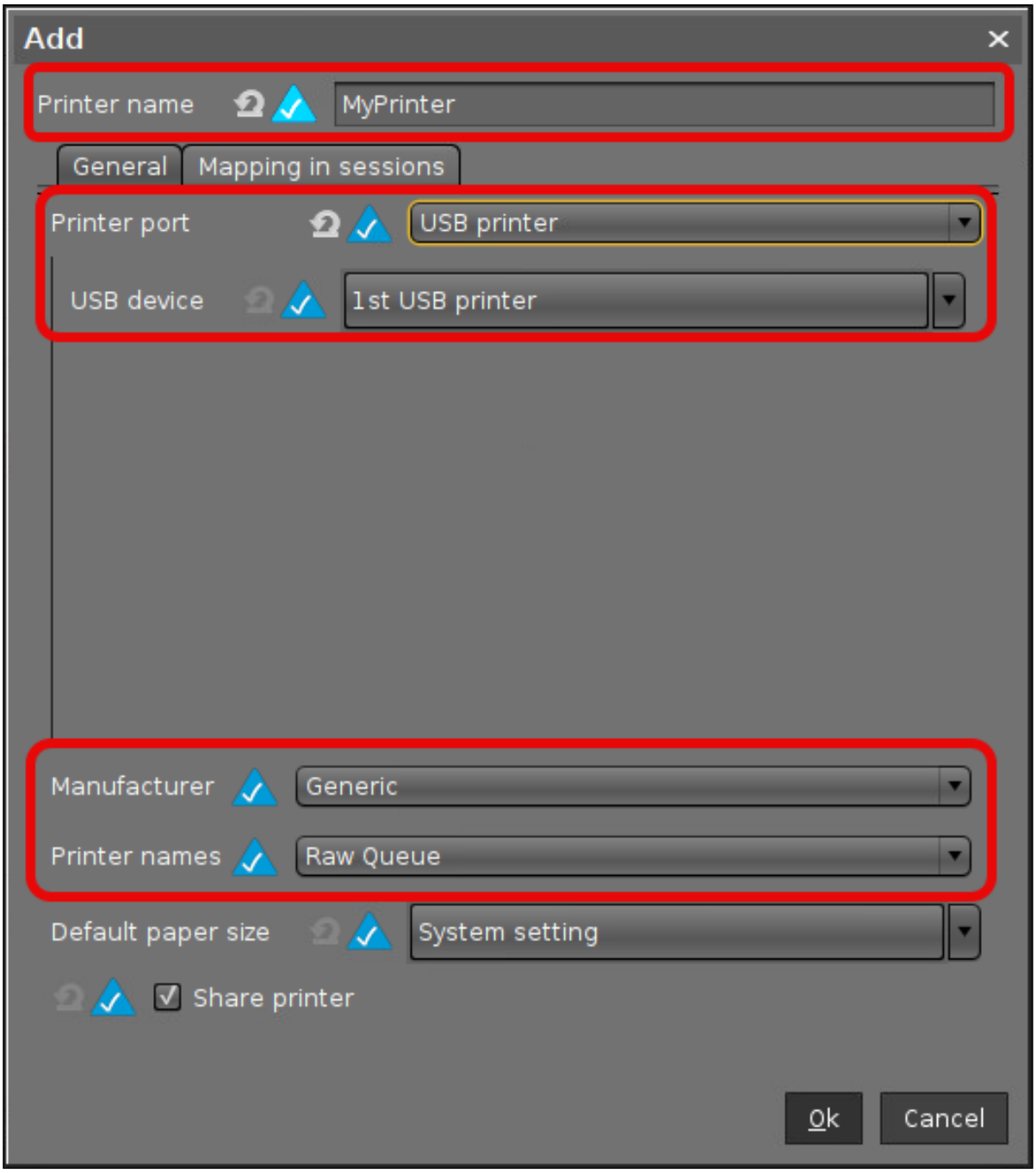
- Citrix: Install the HP Color LaserJet 2800 Series PS driver on the server side to redirect the local printer to Citrix sessions; see https://support.citrix.com/article/CTX140208.

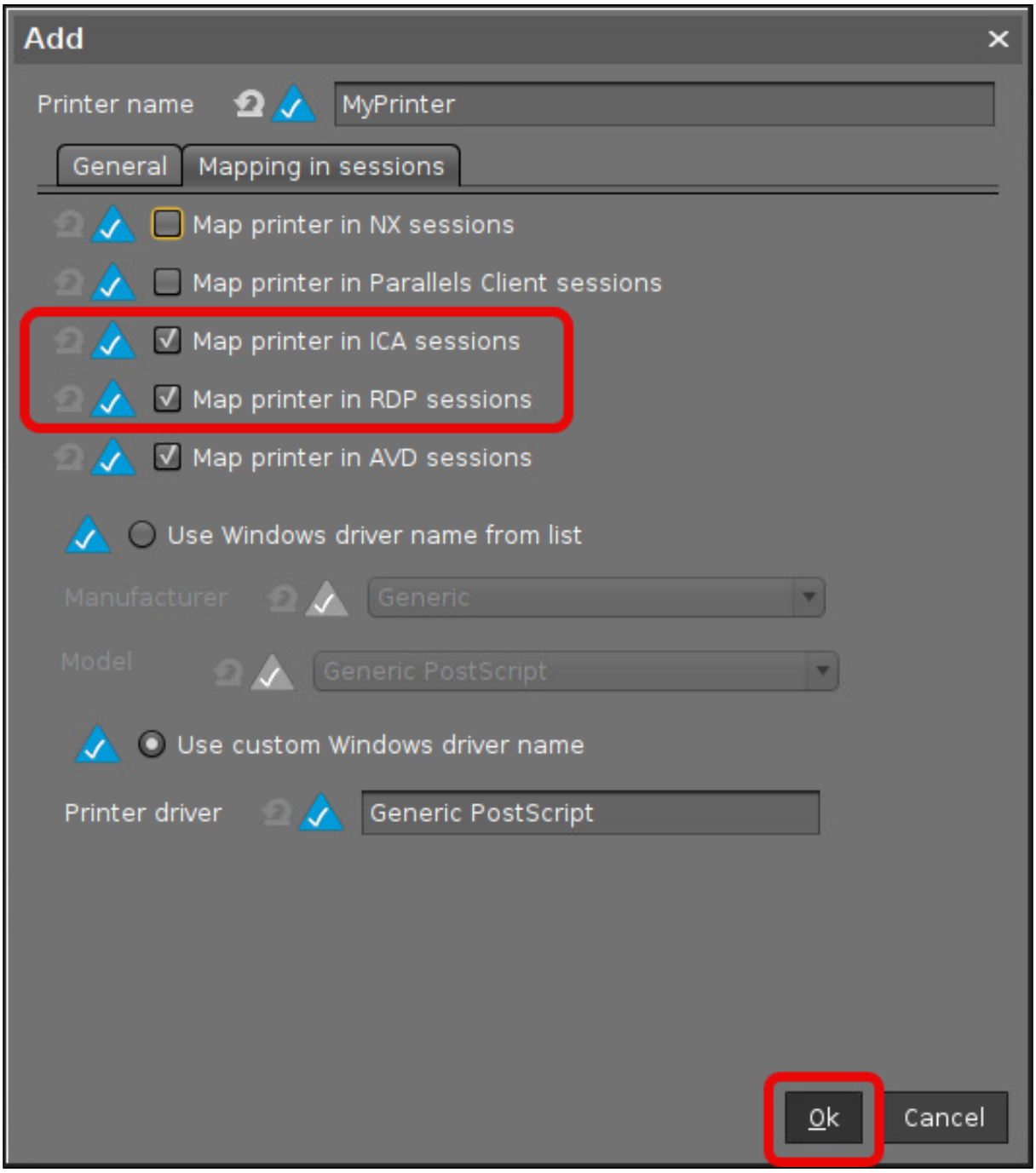
Configuring a Printer for Raw Redirection

1. Go to **Devices > Printer > CUPS > Printers**.
2. Create a new printer and define a **Printer Name**.
3. Select the **Printer Port** your printer is connected to.
4. Set **Manufacturer** to **Generic**.
5. Set **Printer names** to **Raw Queue**.
6. Switch to the tab **Mapping in sessions**.
7. Enable **Map Printer in ICA Sessions** (for Citrix sessions) or **Map Printer in RDP Sessions**.
8. Enable **Use Custom Windows Driver Name**.
9. Enter one of the following into the **Printer driver** field:
    - If you want to use the Citrix universal print driver, enter "Citrix Universal Printer".
    - If you want to use a different printer driver, open your remote Windows system and get the exact name of the driver from the **Print Server Properties** dialog:

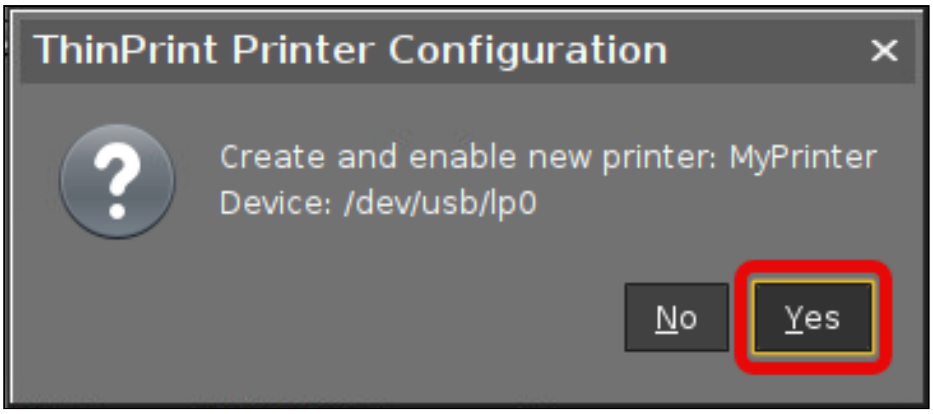


10. Review the settings in the tabs **General** and **Mapping in sessions** and then click **Ok**.


Add
Printer name
MyPrinter
General
Mapping in sessions
Printer port
USB printer
USB device
1st USB printer
Manufacturer
Generic
Printer names
Raw Queue
Default paper size
System setting
Share printer
Ok
Cancel



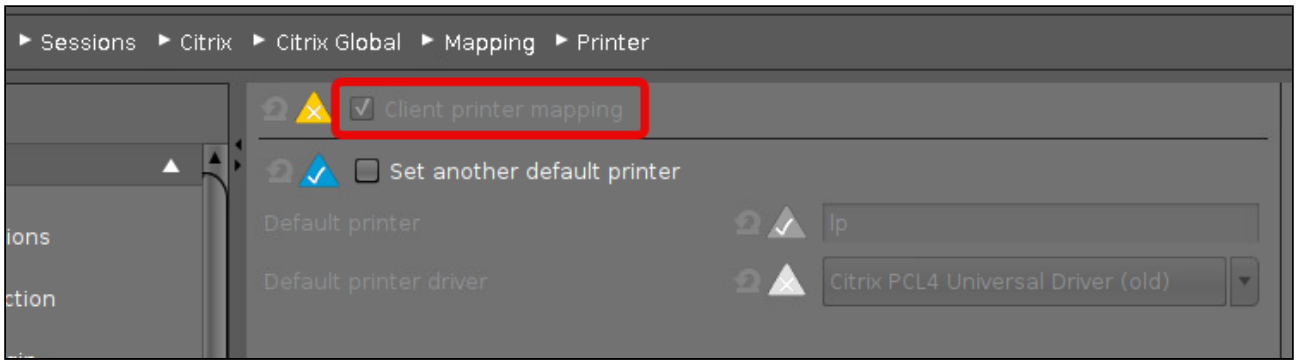
11. Confirm the creation of the new printer.



Configuring the Session at the Client

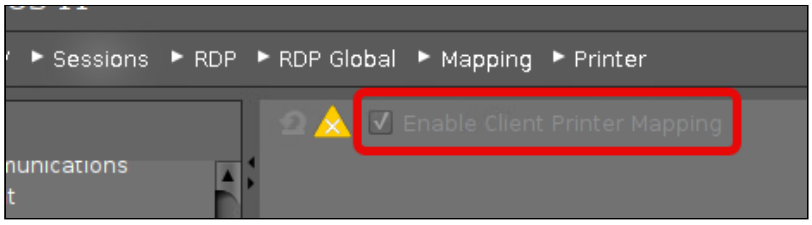
Citrix

->Go to **Sessions > Citrix > Citrix Global > Mapping > Printer** and ensure that **Client printer mapping** is enabled.



RDP

->Go to **Sessions > RDP > RDP Global > Mapping > Printer** and ensure that **Enable Client Printer Mapping** is enabled.



Installing the Printer Driver on the Server Side (If Not Already Present)

The following step is only required if the printer driver is not already on the server.

->Start the ICA or RDP session as administrator and install the printer driver with the redirected port named "TS00x/ClientPort".

Related Information

- Printers - Configure CUPS Printers in IGEL OS (see page 1976), section "Map printer in ICA sessions"
- Printers - Configure CUPS Printers in IGEL OS (see page 1976), section "Map printer in RDP sessions"

Print Server Configuration

Prerequisites

- IGEL OS version 10 or higher
- Printer with the integrated PCL/PS controller.

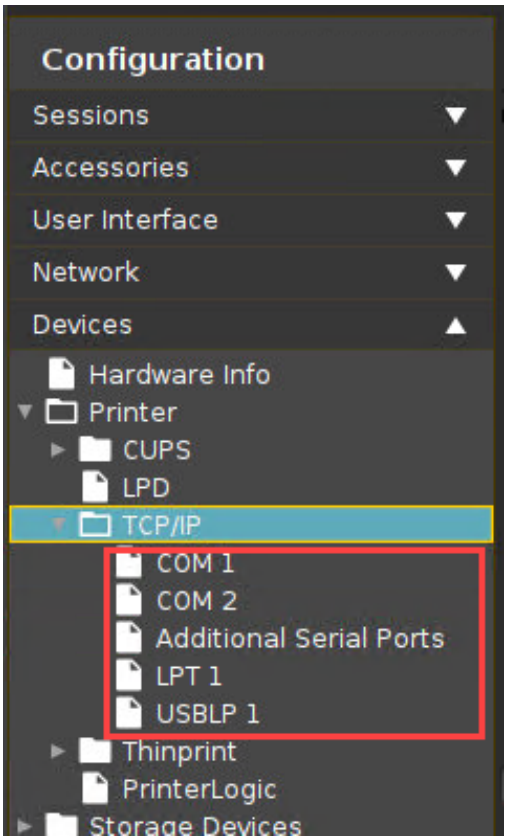
Recommendation

Assign a fixed IP address to the IGEL device or reserve one for it via DHCP.

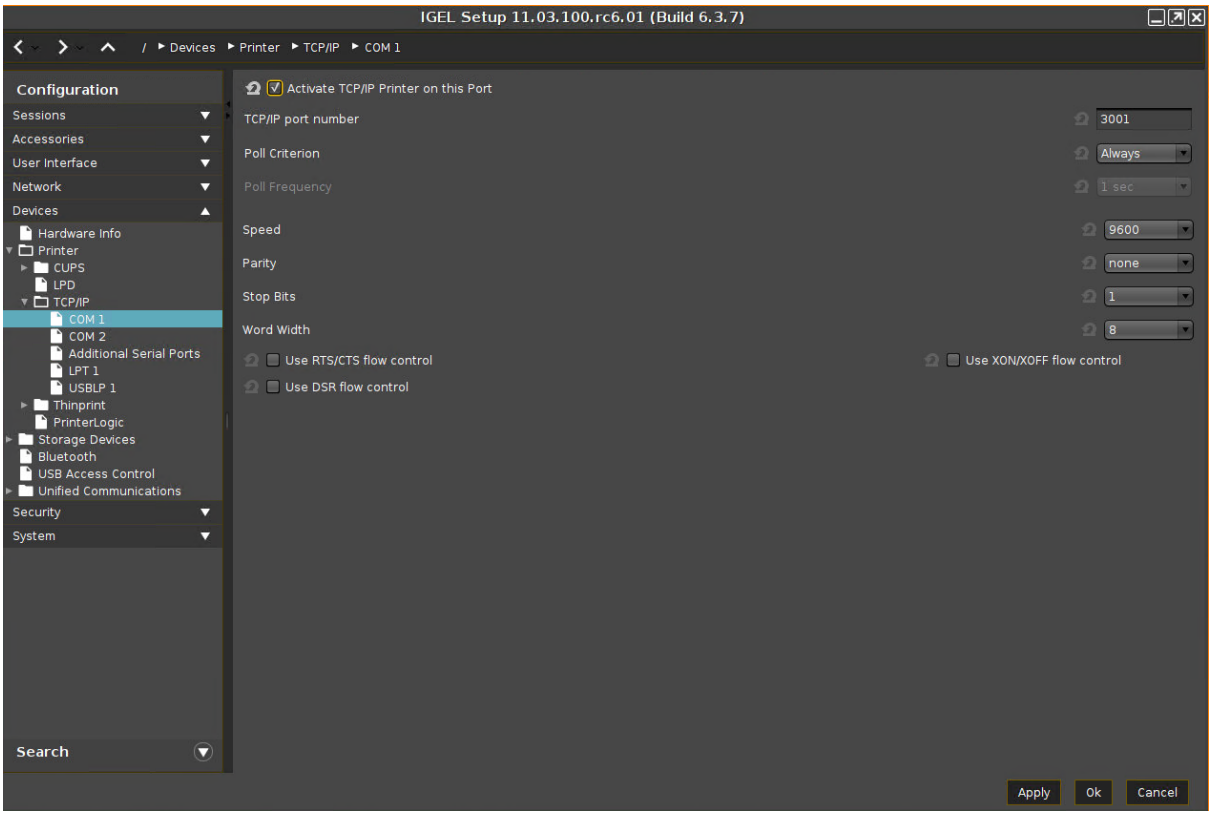
Instructions

To use the IGEL device as a print server for locally connected printers, follow the steps below:

1. In the IGEL Setup, go to **Devices > Printer > TCP/IP**.
2. Select the port to which the printer is connected.
    - COM 1
    - COM 2
    - Additional Serial Ports
    - LPT 1
    - USBLP 1



3. Enable **Activate TCP/IP Printer on this Port.**
   Enter the **TCP/IP port number** on which the print server service is listening. (Windows default: 9100)
   Poll Criterion and **Poll Frequency** must only be adjusted if required by the environment.
4. Click **Apply** or **Ok** to save the settings.



The printer can be installed and used by other systems like a regular network printer.

Installing a Custom CUPS Driver

Environment

IGEL Linux v5 and higher.

Issue

Your printer is not included in the CUPS default configuration.

Solution

You can install a custom driver from your manufacturer.

Copying the PPD Driver File to the Device

->Copy the driver file (PPD file) to the folder `/wfs` using the UMS file transfer mechanism, see *Universal Management Suite (UMS) > UMS Reference Manual > Files - Registering Files on the IGEL UMS Server and Transferring Them to Device*.

Adding a New CUPS Driver

Now that you have copied the driver file to the device, you have to add a new printer and set the PPD file as the driver definition. To do so, proceed as follows:

> For a detailed description of the CUPS configuration options, see CUPS (see page 1975).

1. In Setup, go to **Devices > Printer > CUPS > Printer**.
2. Click + to get to **Add** dialogue.
3. Define the following settings:
   - **Printer name:** Name of the printer.
   - **Printer port:** Port to which the printer is connected. Depending on which type you select, you will have to provide additional information, e.g. server and port in the case of **TCP Printer Port**.
   - **Manufacturer:** Choose **Custom,** which will bring up the **Driver definition** field.
   - **Driver definition:** Enter the absolute path to the PPD file.
4. Click **Ok** to save the settings.
5. Restart your device.

Dynamic Selection of the Default Printer on IGEL OS

If your users change their workplace often, e.g. in a mobile workplace scenario, they might often face the problem that the local printer is not the one that is set as the default printer.

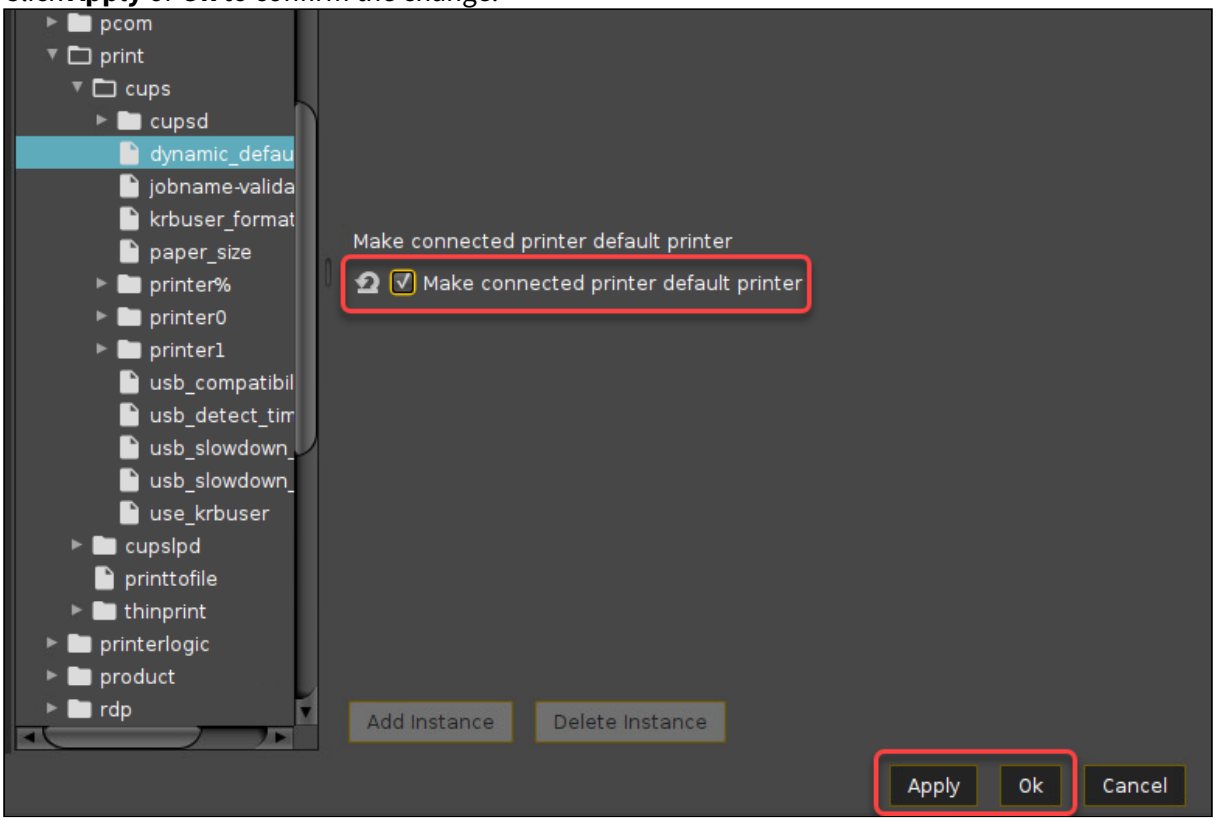
To save your users from dealing with default printer selection, you can configure IGEL OS to automatically set the currently connected printer as the default printer. This feature works with USB printers.

Environment

- Endpoint devices with IGEL OS 11.08.200 or higher
- The connectable USB printers are configured on the endpoint devices; for instructions, see Printers - Configure CUPS Printers in IGEL OS (see page 1976)
- Endpoint Management: UMS 6.10 or higher

Enabling Dynamic Setting of the Default Printer

1. In the local Setup or the UMS configuration dialog, go to **System > Registry > print > cups > dynamic_default** and enable **Make connected printer default printer**.
2. Click **Apply** or **Ok** to confirm the change.



Limitations / Alternative Methods of Selecting the Default Printer

The method of automatically selecting the currently connected printer as the default printer is feasible if only one printer is connected at a time. However, if the user plugs in the preferred printer while another printer is already connected, the preferred printer will no longer be selected as the default printer as soon as another printer is disconnected and then reconnected. Also, the default printer selection may change on a reboot of the endpoint device.

Thus, if two or more printers are connected to the endpoint device at the same time, you should consider one of the following methods of default printer selection.

USB Printer Class

The printer is assigned by matching patterns. This method is recommended if the endpoint device is to be configured completely with the UMS, preferably with a profile.

1. Open the relevant printer under **Devices > Printer > CUPS > Printers**.
2. Edit the printer settings as described under Settings to Be Configured for Each Printer Port Type (see page 1980), section 'Printer Port: "USB class printer"'.
3. Under **Devices > Printer > CUPS > Printers**, set the appropriate printer to **Default**.

USB ID of the Printer

The printer is assigned by its USB ID. This method requires access to the local Setup or remote access by shadowing; see Shadowing VNC (see page 718).

1. Open the relevant printer under **Devices > Printer > CUPS > Printers**.
2. Click **Detect devices...**
3. Select the entry with the prefix **(BY USBID)** and click **Ok**.

4. Under **Devices > Printer > CUPS > Printers**, set the appropriate printer to **Default**.

UD Pocket

- Creating IGEL OS Live USB Sticks for Single-device Use (see page 1134)
- Running IGEL OS from UD Pocket on a Dell WYSE ZX0D (aka 7010) Device (see page 1141)
- Running UD Pocket on an Acer Chromebook C910 (see page 1142)
- UD Pocket Seems to Break Microsoft Surface (see page 1143)
- How to Boot from the UD Pocket on Mac mini, MacBook Air 2018, MacBook Pro (see page 1146)
- How to Reflash Your IGEL UD Pocket (see page 1147)

Creating IGEL OS Live USB Sticks for Single-device Use

Solutions from the Field

This article provides solutions that have not been approved by the IGEL Research and Development department. Following the instructions given here is at your own risk.

You can use the IGEL OS Creator (OSC) to create an IGEL OS live USB stick for single-device use. The functionality of this live USB stick is similar to an IGEL UD Pocket. The main difference lies in the assignment of licenses: a UD Pocket license is assigned to a unit ID that is hard-wired into the UD Pocket itself, while the license for the solution presented here is bound to the very first device that boots from this USB stick.

For the procedure described here, a video is available:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=3M9beTl8JX0

See also this external article: https://virtualbrat.com/2020/03/19/igel-ud-pockets-for-everyone/

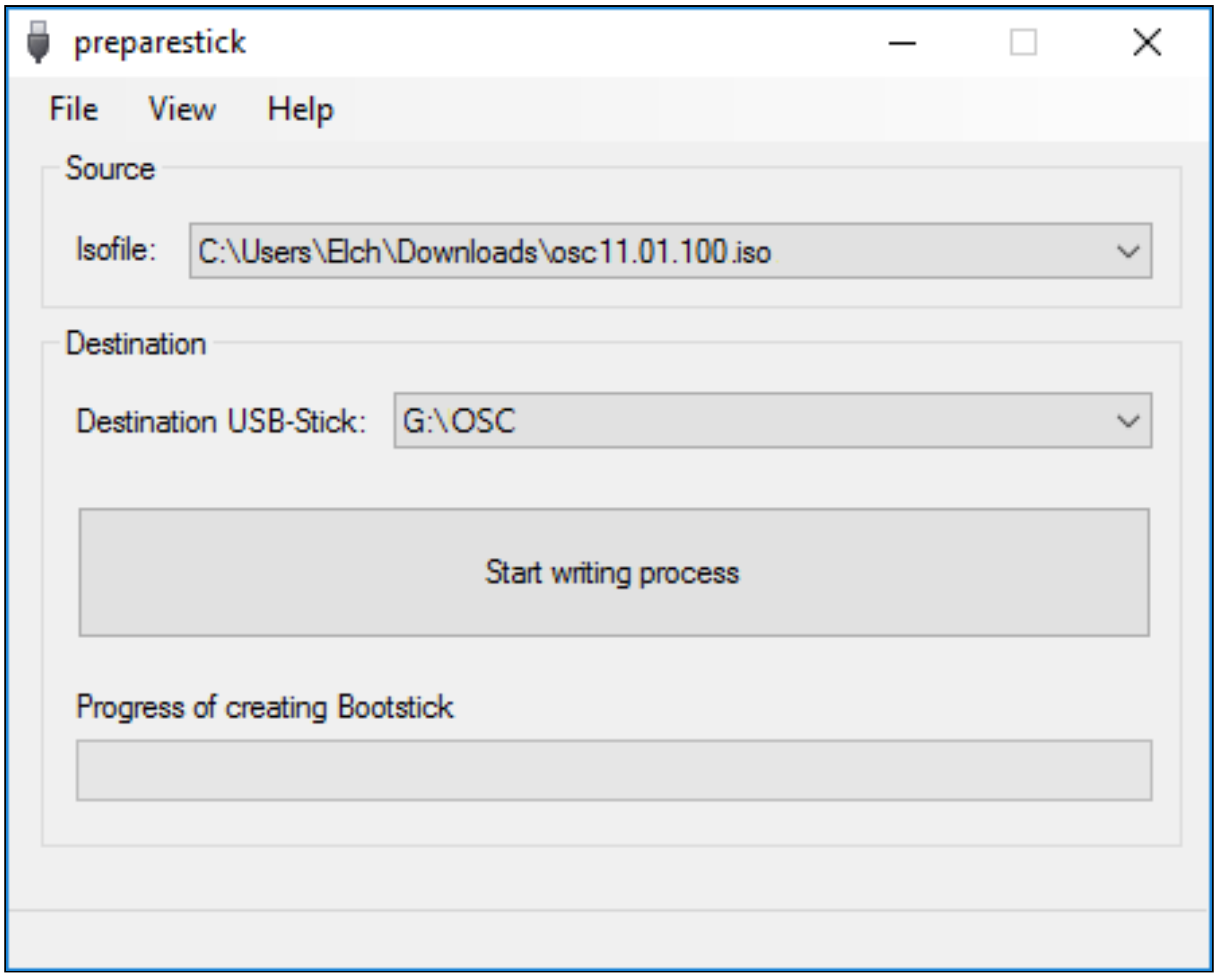
Requirements

- PC with Windows 10 or Linux
- 2 USB sticks with 4 GB or more without any important data (will be overwritten)

Creating the IGEL OS Creator Stick under Windows

1. Download the ZIP archive for OSC from https://www.igel.com/download/ (latest public release) or from https://www.igel.com/igel-solution-family/windows-virtual-desktop/ (latest release with WVD support).
2. Unzip the contents into a local directory.
3. Connect a USB memory stick with at least 4 GB capacity to the computer.
4. Double-click the `preparestick.exe` file from the unzipped directory.

   If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.



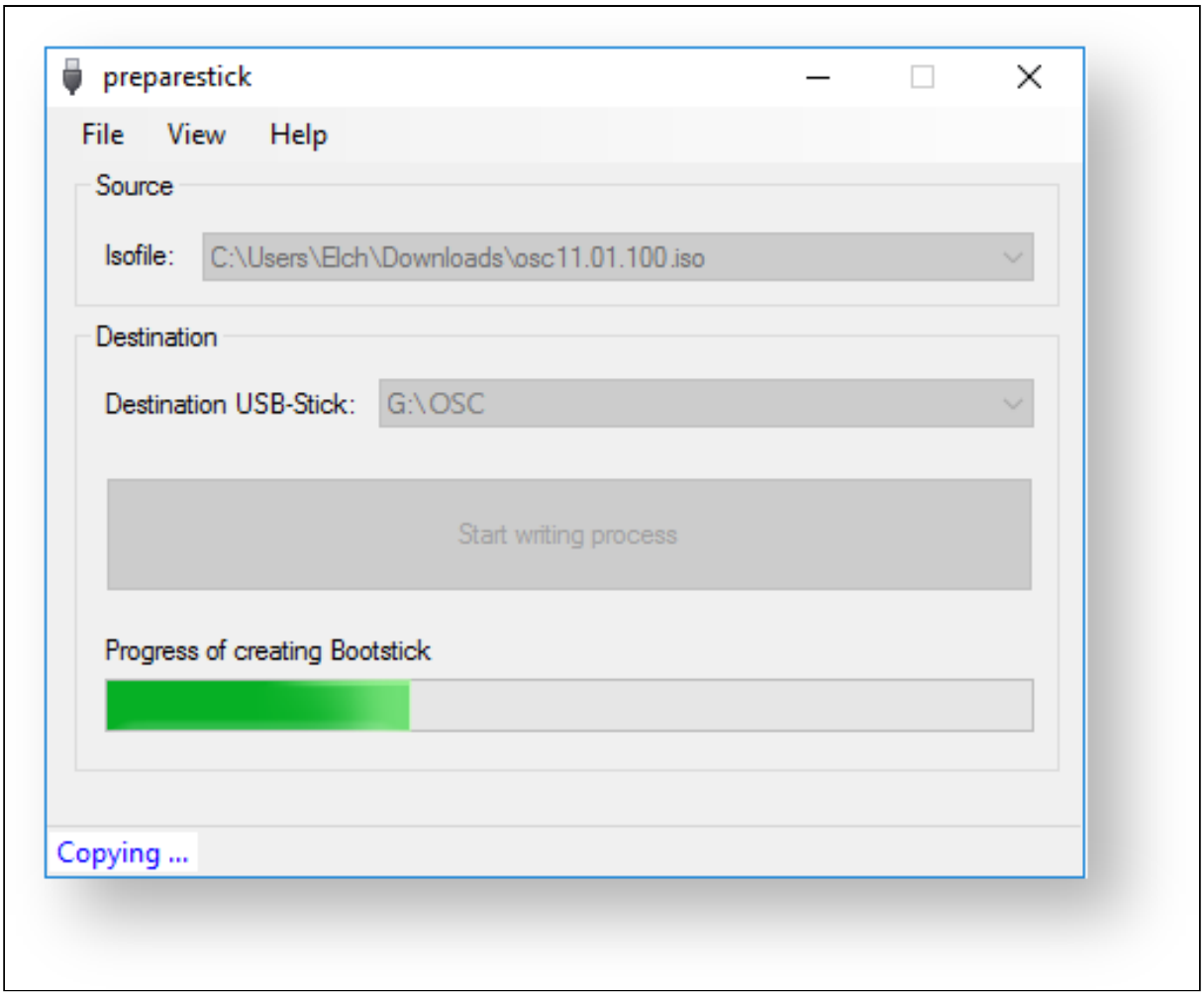
The dropdown-menu **Isofile** shows the ISO files contained in the unzipped directory.

5. Unter **Isofile**, select the appropriate ISO file, e. g. `osc11.01.100.iso`
6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.

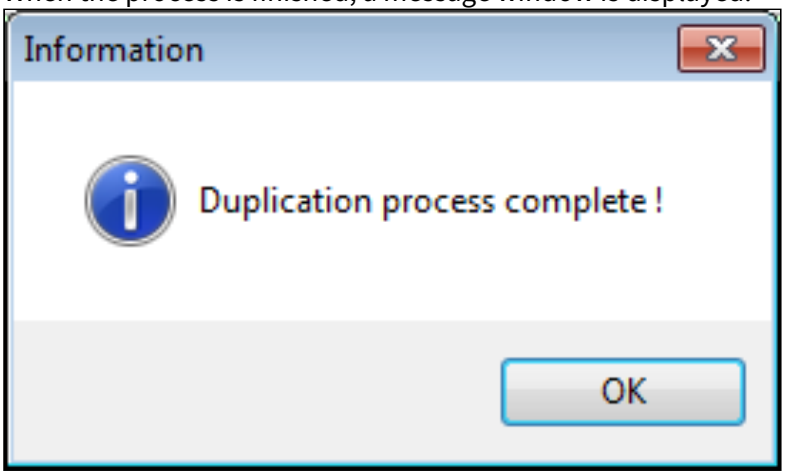
   It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.

   Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List.**

7. Click on **Start writing process**.
   In the program window, the progress of the process is shown.



When the process is finished, a message window is displayed.



8. Close the message window and the program.
9. After about 3 seconds, remove the USB memory stick.

> If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

Creating the IGEL OS Creator Stick under Linux

1. Download the ZIP archive for OSC from https://www.igel.com/download/ (latest public release) or from https://www.igel.com/igel-solution-family/windows-virtual-desktop/ (latest release with WVD support).
2. Unzip the contents into a local directory.
3. From this directory, you will need the ISO file (e. g. `osc11.01.100.iso`) to create a bootable medium.
4. Connect a USB memory stick with at least 4 GB capacity to the computer.

   > All existing data on the USB memory stick will be destroyed.

5. Open a terminal emulator and enter the command `dmesg` to determine the device name of the USB memory stick.
   Example output:

   ```
   [...]
   [19514.742229] scsi 3:0:0:0: Direct-Access JetFlash Transcend 8GB 1100 PQ: 0 ANSI: 6
   [19514.742805] sd 3:0:0:0: Attached scsi generic sg1 type 0
   [19514.744688] sd 3:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/7.35 GiB)
   [19514.745370] sd 3:0:0:0: [sdb] Write Protect is off
   [19514.745376] sd 3:0:0:0: [sdb] Mode Sense: 43 (0) 00 00 00
   [19514.746040] sd 3:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
   [19514.752438] sdb: sdb1
   ```

   In this example, the device name searched for is `/dev/sdb`.

   > Ensure that you have determined the correct device name. Use of the `dd` command in the next step can destroy your operating system if you use the wrong device name.

6. The following command writes the installation data to the USB memory stick:
   `dd if=osc11.01.100.iso of=/dev/sdX bs=1M oflag=direct`
   Replace `sdX` with the device name of the USB memory stick that you have determined.
   When the `dd` command has terminated, you can see the terminal emulator input prompt again.
7. Wait for about 3 seconds after the `dd` command has terminated, and remove the USB memory stick.

   If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

   The USB memory stick for OSC installation is ready for use.

Adjusting the Boot Settings

OSC works on systems with BIOS and UEFI.

To use your PC for creating the USB live stick, it must support booting from USB storage media. This may already be enabled, or you may have to enable it yourself.

IGEL OS 11 supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS.

If IGEL OS fails to boot in UEFI mode, try it in legacy/BIOS mode. IGEL OS will then be installed in legacy/BIOS mode.

For older devices or if you haven't been able to boot the installer at all, use the legacy installer.

The required key presses for this may vary from vendor to vendor. However, here are some hints:

->While the device is booting, try pressing [F12] (in general), [F10] (Intel devices) or [F9] (Hewlett-Packard devices) in order to access a list of boot devices and select UD Pocket.

->If the above does not work, access the BIOS settings via pressing [Del], [F1] or [F2] during boot and activate booting from USB storage media and/or change the boot order.

->See the BIOS/UEFI documentation for your system for details of how to boot from USB storage media.

Creating the IGEL OS Live USB Stick

1. Connect the IGEL OS Creator stick to your PC.
2. Connect the second USB stick to your PC and switch it on.

3. Make sure to boot from the IGEL OS Creator stick.
4. Select **Standard Installation + Recovery** from the boot menu.
5. **Please choose your language**: Select the language for the installation process.
6. Accept the **EULA** by clicking **I agree**.
   The installation program **IGEL OS Creator** starts.
7. Under **Target drive**, select the second USB stick. This USB stick will become the IGEL OS live USB stick.

   Make sure you select the right target device! Otherwise, data on your PC may be damaged.

8. Click **Install firmware**.
   The installation program will set up IGEL OS 11 on the target drive. If you see the **IGEL OS Creator build finished successfully** message, the installation is complete.
9. Detach any external network adapters from the device.
   In this way, you ensure that the unit ID for the device (MAC address) is derived from the built-in network adapter. The unit ID will be saved on the device persistently, regardless of any external network adapter that may be used in the future. This is important for licensing.
10. Click on **Reboot** at the bottom of the installation window.
11. Remove the IGEL OS Creator.
12. Close the message window.
    The system will shut down and then boot IGEL OS 11 from the newly created IGEL OS live USB stick.

Solutions from the Field

This article provides solutions that have not been approved by the IGEL Research and Development department. Following the instructions given here is at your own risk.

Running IGEL OS from UD Pocket on a Dell WYSE ZX0D (aka 7010) Device

Here you can learn which settings you have to make on the Dell WYSE ZXoD (aka 7010) to be able to start the device with a UD pocket.

1. Boot up the Dell device.
2. In the BIOS go to the **Advanced** tab.
3. Enable **Boot From USB**.
4. Change to the **Boot** tab.
5. Change the boot priority to make **USB HDD** the default by moving it to the top.
6. Save the settings
7. Put in the UD Pocket

See this video:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=C0NWdjVE1RI

Running UD Pocket on an Acer Chromebook C910

You can use the IGEL UD Pocket with the Acer Chromebook C910. This requires installation of a BIOS extension which enables the device to boot into an alternative operating system.

> The procedures described here have been tested with the Acer Chromebook C910; the procedures may differ for other Chromebook types.

For further information, refer to MrChromebox.tech[137].

Enabling Your Device to Boot from UD Pocket

1. Ensure that you have a WiFi connection; this is required for downloading the SeaBIOS extension.
2. Boot into recovery mode by pressing [ESC] + (Refresh) + (Power) simultaneously.
   The recovery mode screen is shown, which states that the OS is broken.
3. Press [Ctrl] + [D] to enter developer mode.
   The developer mode screen is shown, confirming that OS verification is off.
4. Open a root-capable shell by pressing [Ctrl] + [Alt] + (F2).
5. Login as `chronos`; no password is required unless one has been set.
6. Change to /tmp: `cd /tmp`.
7. Download the ChromeOS firmware utility script: `curl -LO https://mrchromebox.tech/firmware-util.sh`
8. Start the script with root permissions: `sudo bash firmware-util.sh`
9. Enter `1` to select the first option.
10. Enter `y` to confirm.
    The RW_Legacy firmware is downloaded to your device.
11. When the download has completed, press [Enter].
12. Enter `r` to reboot.
    The device reboots into developer mode.
13. To boot from UD Pocket, press [Ctrl] + [L].

Booting from UD Pocket

1. Ensure that the device is in developer mode. This should be the case if the device has been configured according to the procedures described above, and if since then no changes were made that have affected the developer mode.
2. Press [Ctrl] + [L] to boot from UD Pocket.

137. https://mrchromebox.tech

UD Pocket Seems to Break Microsoft Surface

Please note that this device is not officially supported. Therefore, we can not offer any guarantee or support for the procedures described in this article.

Tested Environment

The following information describes the exact environment on which the issue and the troubleshooting method have been tested. However, the method will probably work on similar versions.

- Microsoft Surface Book 1
- Windows 10 build 1903 4/25/2019 18362.267
- IGEL UD Pocket with IGEL OS 11.02.100

Issue

After having booted successfully into UD Pocket once, the Microsoft Surface notebook is not able to boot into Windows anymore.

Solution

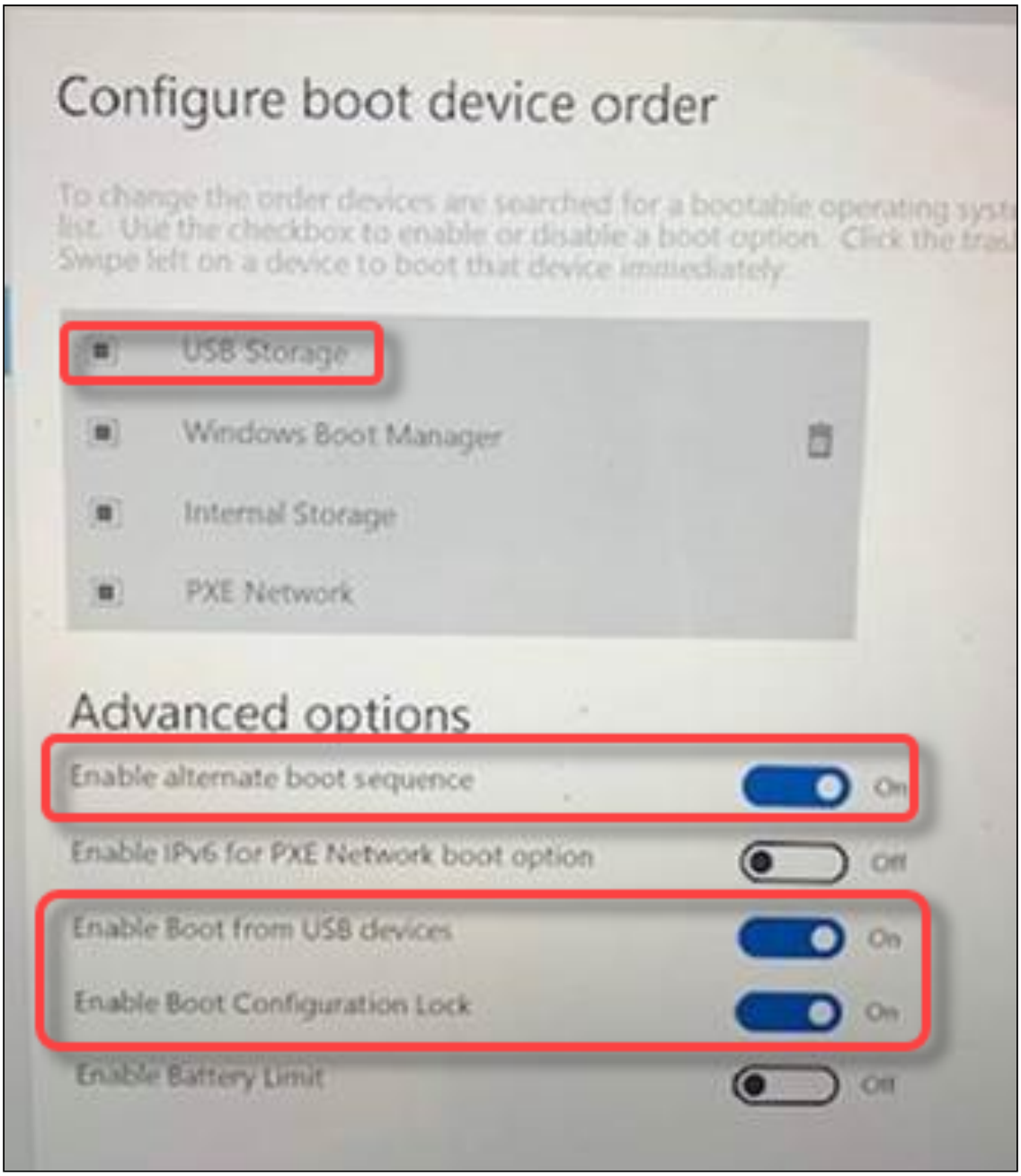
With the following procedures, you can set your Microsoft Surface to boot from USB storage permanently or, alternatively, on-demand.

For detailed information, see How do I use the BIOS/UEFI?[138] by Microsoft.

Enabling Boot from USB Storage Permanently

1. Ensure that your Microsoft Surface has shut down.
2. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
3. When the Surface logo appears, release the volume + (up) button.
   The UEFI menu is displayed.
4. Under **Configure boot device order**, move **USB Storage** to the top using drag & drop.
5. Under **Advanced options**, change the settings as follows:
   - **Enable alternate boot sequence**: **On**
   - **Enable Boot from USB devices**: **On**
   - **Enable Boot Configuration Lock**: **On**
     Your UEFI settings should look like this:

138. https://support.microsoft.com/en-ae/help/4023532/surface-how-do-i-use-the-bios-uefi



6. Exit the UEFI settings.
7. Insert the UD Pocket into the USB port of your Microsoft Surface.
8. Reboot your Microsoft Surface.
   Your Microsoft Surface boots from your UD Pocket.

Booting from USB Storage On-Demand

1. Ensure that your Microsoft Surface has shut down.
2. Insert the UD Pocket into the USB port of your Microsoft Surface.

3. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
4. When spinning dots appear beneath the Surface logo, release the volume + (up) button. Your Microsoft Surface boots from your UD Pocket.

How to Boot from the UD Pocket on Mac mini, MacBook Air 2018, MacBook Pro

> **Solution Based on Experience from the Field**
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Environment

- Mac devices with an Apple T2 Security Chip, e.g. Mac mini, MacBook Pro, MacBook Air 2018, iMac Pro

Problem

The secure boot implemented with the Apple T2 Security Chip does not allow to boot Linux on the above-mentioned devices. For details, see the German overview https://www.computerbase.de/2018-11/apple-t2-linux-installation-umgehung/. Therefore, some configuration changes on these devices are required to boot from the UD Pocket.

Solution

Via the recovery menu, it is possible to disable the secure boot option. To do this, proceed as follows:

1. To get into the macOS recovery menu, press and hold the command key [⌘] + [R] during the boot process as soon as the Apple logo appears.
2. Under **Utilities**, select the **Startup Security Utility**.
3. Use an administrator account to deactivate the secure boot option under **Secure Boot > No Security**.

For more information about the Startup Security Utility on Mac devices, see https://support.apple.com/en-us/HT208198.

How to Reflash Your IGEL UD Pocket

Because of misconfiguration, an incorrectly performed update, or some other reason, you may sometimes need to re-image your IGEL UD Pocket. The procedure is generally the same as IGEL OS Creator (OSC) installation procedure. The difference is that you must select your UD Pocket as a target device, and not your PC, during the installation.

Requirements

- PC with 2 free USB ports
- 1 USB stick with 4 GB or more without important data (will be overwritten)
- IGEL UD Pocket

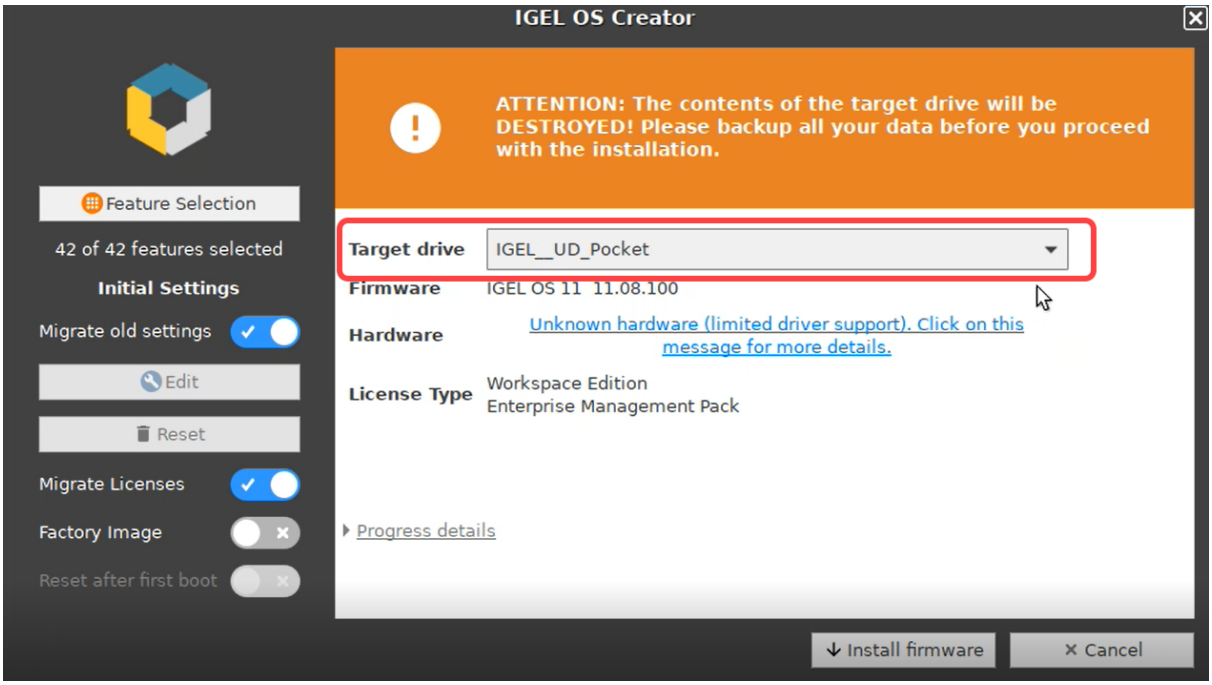
Re-Image IGEL UD Pocket

1. First of all, you must create an IGEL OS Creator stick. For the instructions, see:
   - Create USB installation medium (Windows) (see page 2127)
   - Create USB installation medium (Linux) (see page 2130)
2. If not already enabled, activate booting from USB storage media on your PC, see Boot Settings (see page 2133).
3. Connect the created IGEL OS Creator stick to the PC.
4. Connect the IGEL UD Pocket to the PC.
5. Switch the PC on and make sure to boot from the IGEL OS Creator stick.
6. Select **Standard Installation + Recovery** from the boot menu.

7. Select the language for the installation process.

8. Under **Target drive**, select your UD Pocket.

> Make sure you **select the right target device! Otherwise, data on your PC will be deleted!** Installing IGEL OS via OSC destroys all data on the device selected under **Target drive**. Therefore, be careful not to accidentally select your PC's hard drive!



9. If your UD Pocket is still functional and has no errors, leave the option **Migrate old settings** activated to migrate the previous settings.

   Disable **Migrate old settings** if your UD Pocket has some misconfiguration problems or is not bootable anymore.

10. Make sure **Migrate Licenses** is activated if you want to keep the existing licenses.

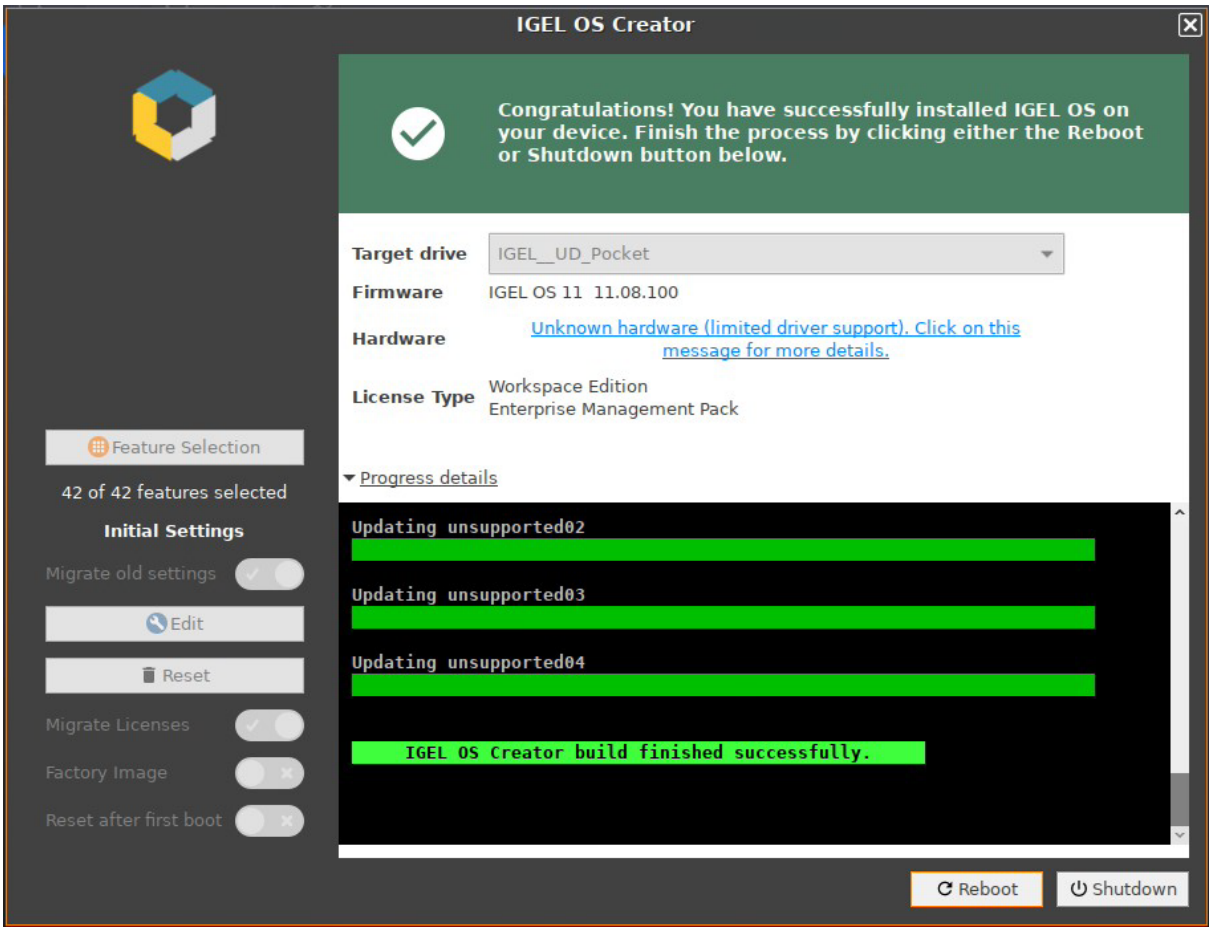
11. Optional settings:
    - **Force legacy installation** (only available if the PC has booted in UEFI mode)
    - **Force MS-DOS Partitioning** (only available if the PC has booted in UEFI mode)
    - **Feature Selection**
    - **Edit / Reset**
      For details on these options, see Installation Procedure (see page 2137).

12. Click **Install firmware**.
    The installation program will set up IGEL OS 11 on the UD Pocket.

13. Accept the EULA by clicking **I agree**.

14. Confirm the warning dialog.

15. If you see the message **IGEL OS Creator build finished successfully**, the installation is complete.



16. Click on **Reboot** at the bottom of the installation window.

17. Remove the IGEL OS Creator stick.

18. Close the message window.
    The system will shut down and then boot IGEL OS 11 from your re-imaged UD Pocket.

Miscellaneous

- Sending Device Log Files to IGEL Support (see page 1152)
- Exporting the Local Configuration of the IGEL OS Device (see page 1161)
- Which Unified Communication Solutions Does IGEL OS Support? (see page 1163)
- Passthrough Authentication (see page 1165)
- Hardware Video Acceleration on IGEL OS (see page 1180)
- Running Commands before or after a Session (see page 1183)
- Copy Sessions in Setup or UMS (see page 1185)
- IZ1 and UD2-MM Usage of RAM (see page 1186)
- Using Symantec Ghost to Deploy IGEL OS (see page 1187)
- Starting UMS Console Crashes NX Session (see page 1189)
- Accessing IGEL Setup within Appliance Mode (see page 1190)
- Application Is Terminated with Message "Low memory! Killing process ..." (see page 1191)
- An Application Window Cannot Be Repositioned (see page 1192)
- Updating IGEL UMD: Error "not compatible with System5" (see page 1194)
- IGEL Endpoint Partners: Ensuring Image Integrity with a Checksum (see page 1195)
- Will My Session Be Closed When My IGEL OS Endpoint Device Enters Suspend Mode? (see page 1196)
- Microsoft Remote Desktop Client: Comparison of IGEL OS with Other Vendors (see page 1198)
- IGEL OS Third Party Integrations (see page 1207)
- How Do I Get My Fn Keys to Work? (see page 1209)
- Invalid Session Names (see page 1210)

Sending Device Log Files to IGEL Support

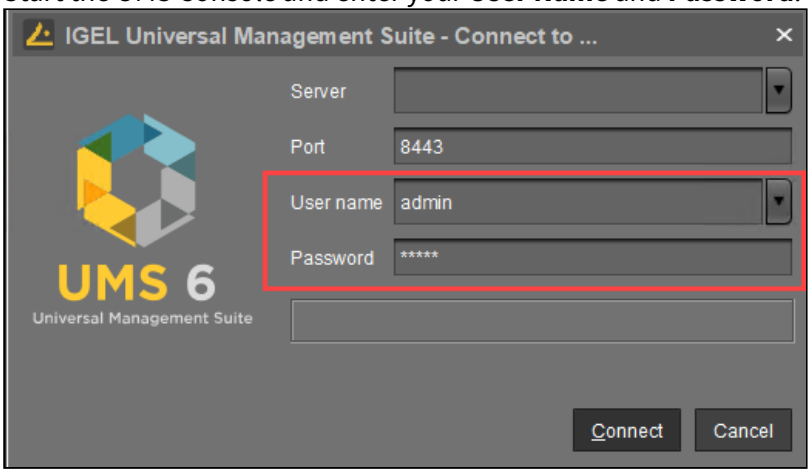
When the IGEL support team asks you to provide your device's log files, follow the instructions below.

There are two possibilities to send log files to the support team, one that uses the IGEL Universal Management Suite (UMS) and one that works locally with a USB memory stick:

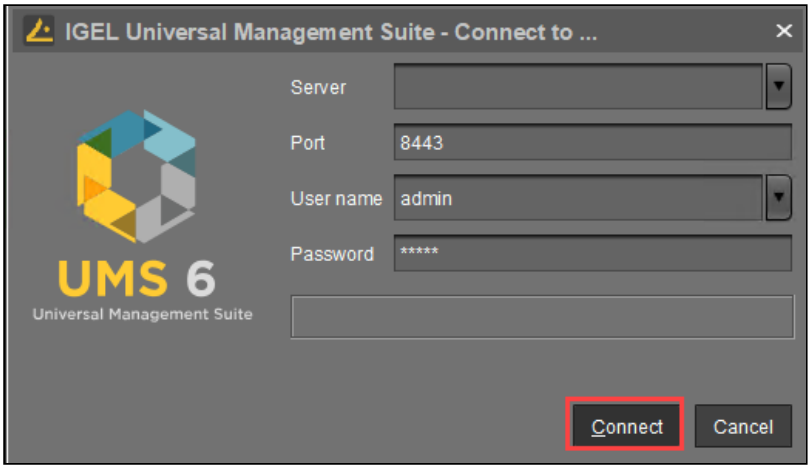
- With UMS (see page 1152)
- Without UMS (see page 1158)

With UMS

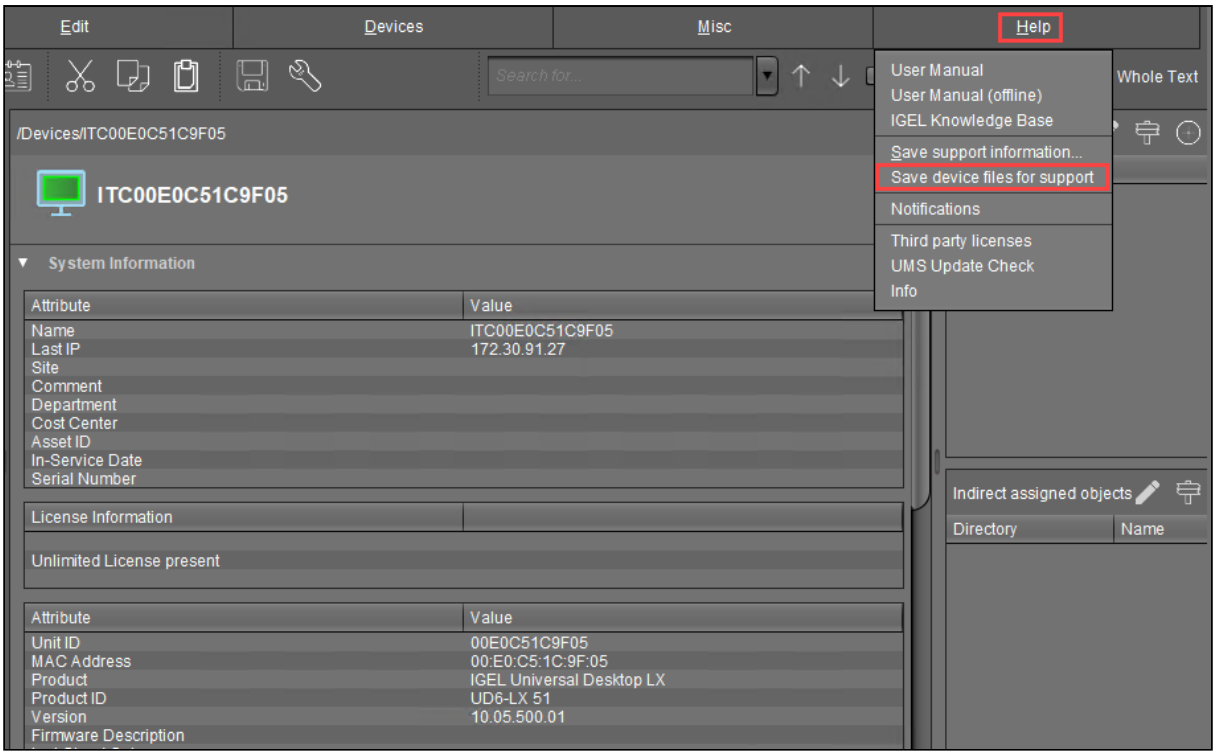
1. Start the UMS Console and enter your **User Name** and **Password**.



2. Click **Connect**.

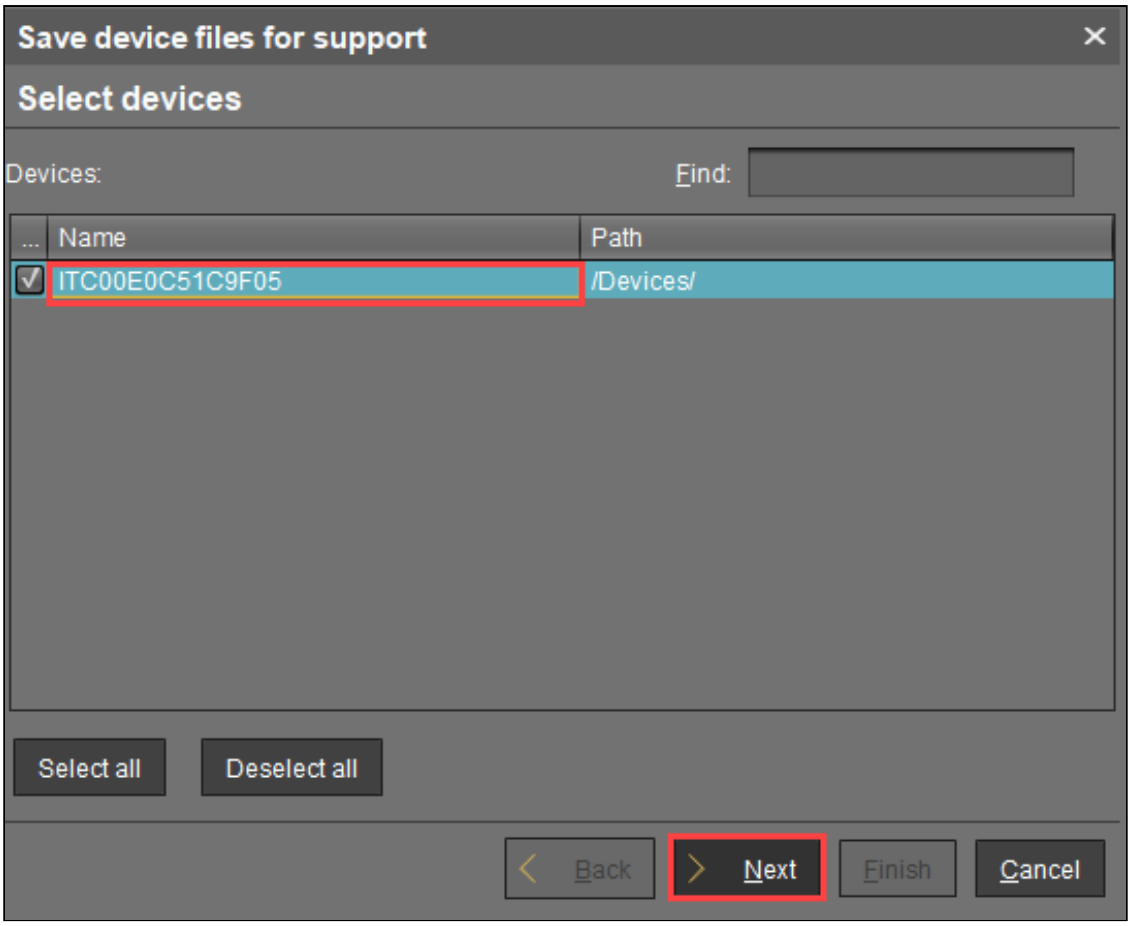


   The UMS Console window opens.
3. Open the **Help** submenu and select **Save device files for support**.



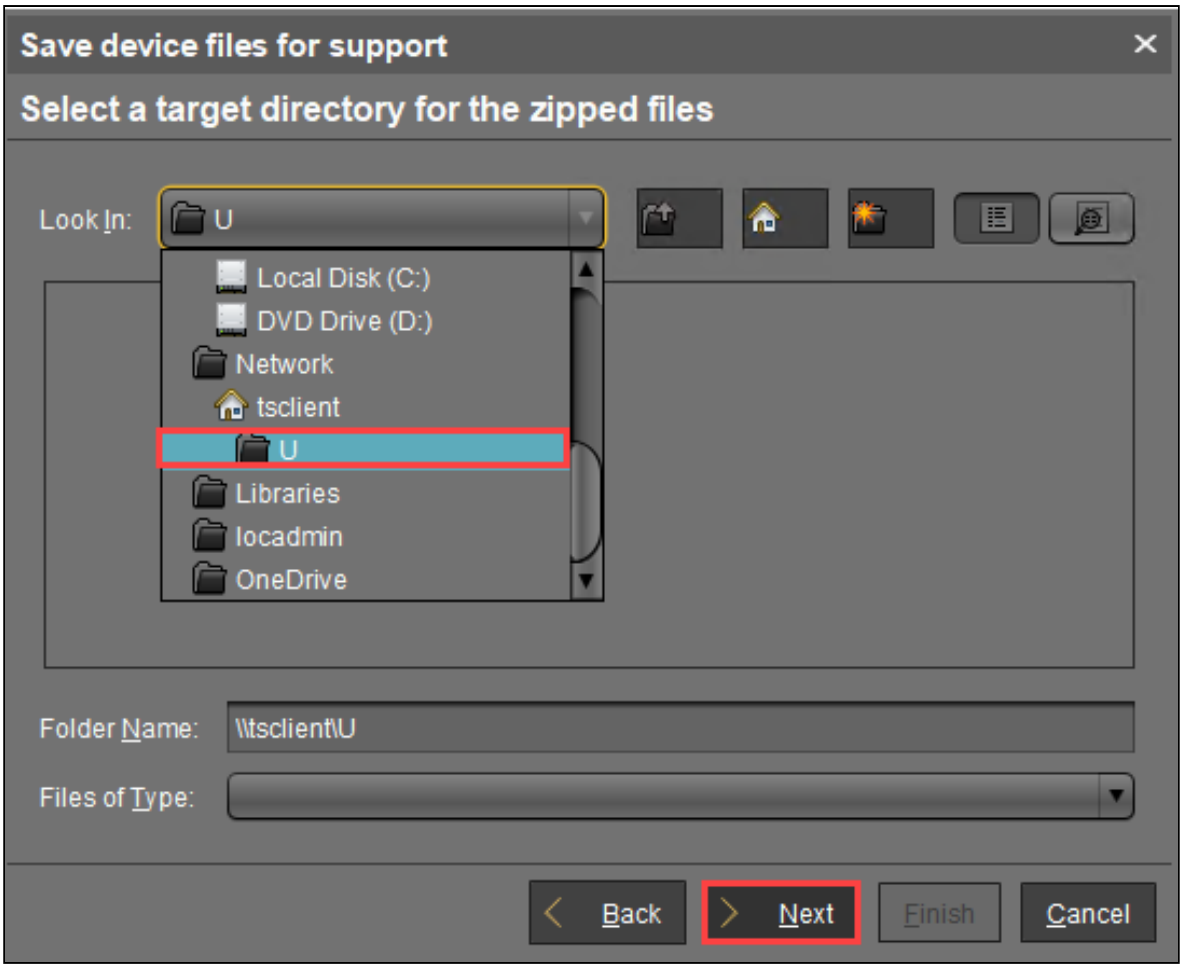
The dialog **Save device files for support** opens.

4. Select the device in question and click **Next**.

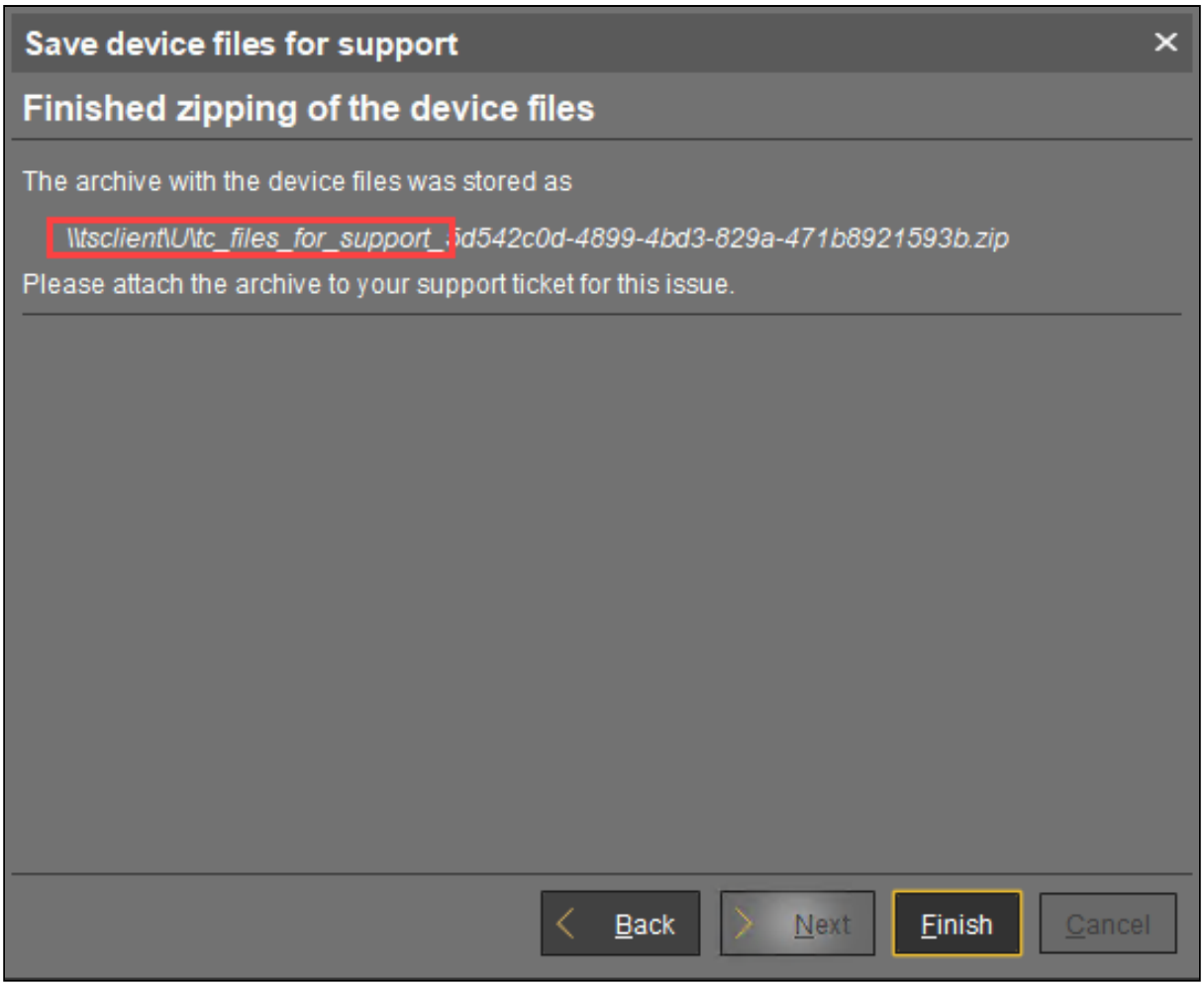


The dialog **Select a target directory for the zipped files** opens.

5. Select a directory suitable for saving the zipped log files, and click **Next**.



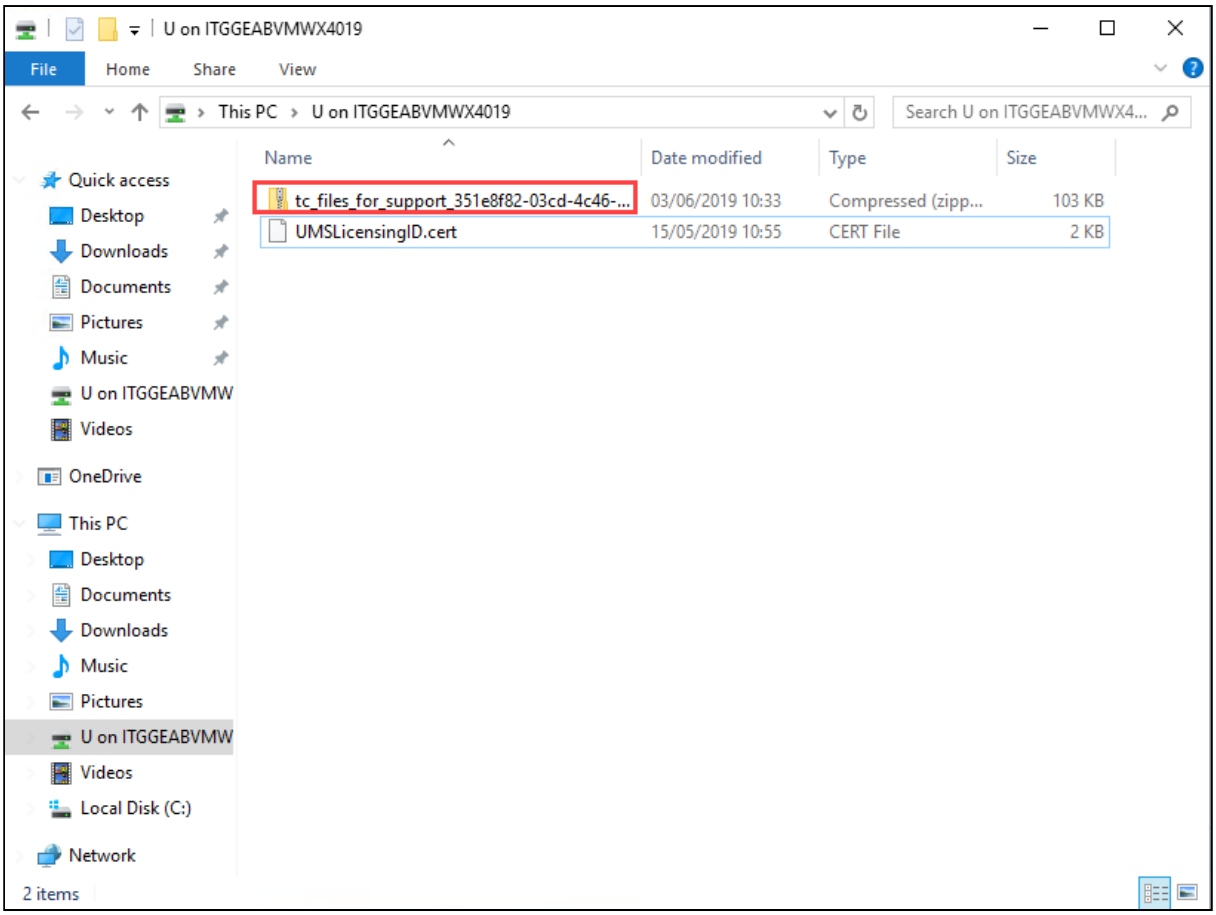
A confirmation dialog shows the path and file name under which the log files are stored. Depending on your system, you can copy the path using [Ctrl] + [C] and paste it into the File Explorer's address bar.



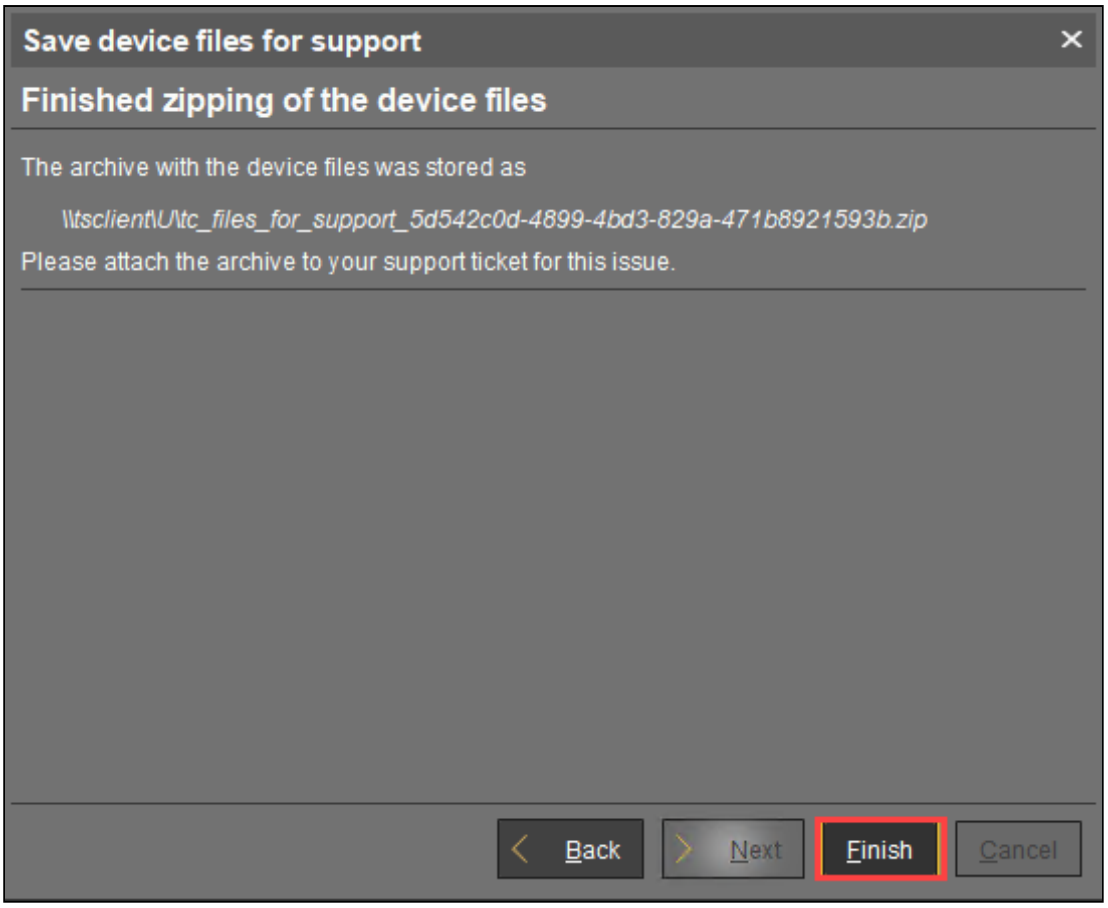
Depending on your network, hardware, and the amount and size of the log files, the collection and the upload of the files might take up to a few minutes.
In the case of failure, try the following:

- If you are using UMS 6.10.110 or higher: Go to **UMS Administration > Global Configuration > Device Network Settings** and change the parameter **Timeout for the device support file upload action (seconds)** to a higher value. The maximum is 9000 seconds.
- Check if port 8443 is open for TCP connections.
- If everything should fail, try the method described under Without UMS (see page 1158).

6. Open your system's File Explorer, go to the path portion of the file location.



7. Send the ZIP file to the IGEL support team.
8. Close the confirmation dialog by clicking **Finish**.



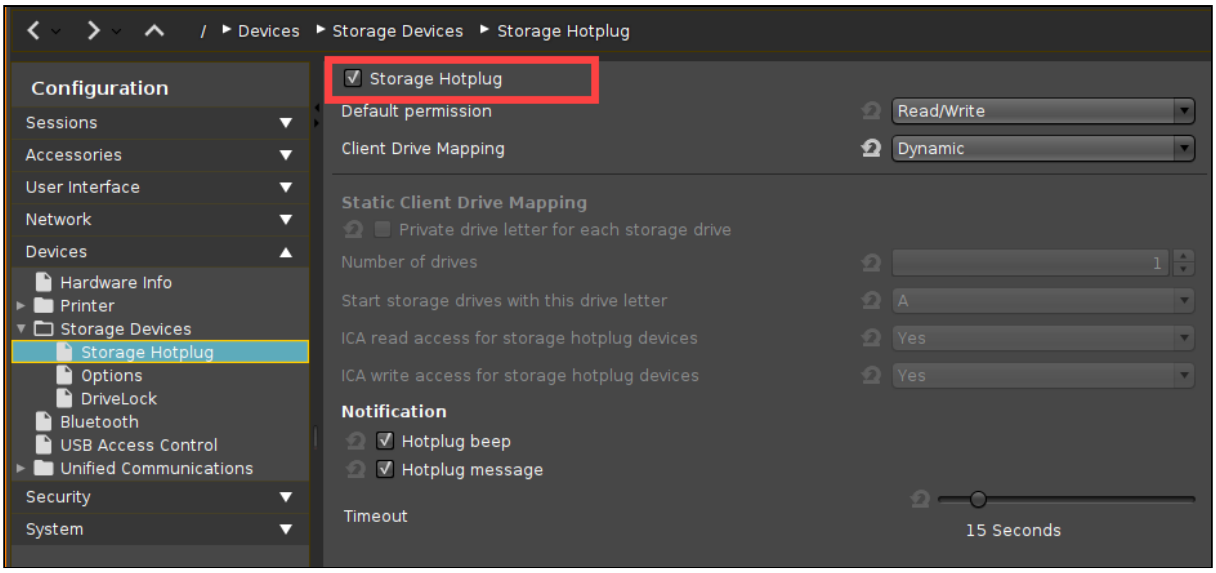
The above procedure collects only those logs that have been written since the last system start. To allow persistent logs, you can configure a dedicated partition for debug logs. For more information, also on adding additional logs, see Extended Logging With Syslog, Tcpdump and Netlog (see page 623).

Without UMS

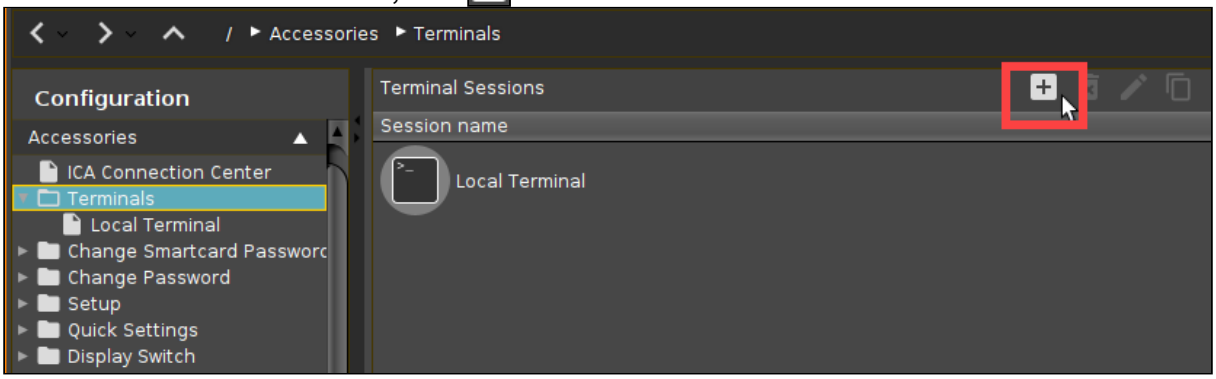
When the UMS is not accessible or there is an issue with network connectivity, you can still extract system logs from a device and send them to support. You will need a USB stick, preferably formatted to NTFS format, to transfer the logs to.

Setting Up the Device

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage Hotplug**.

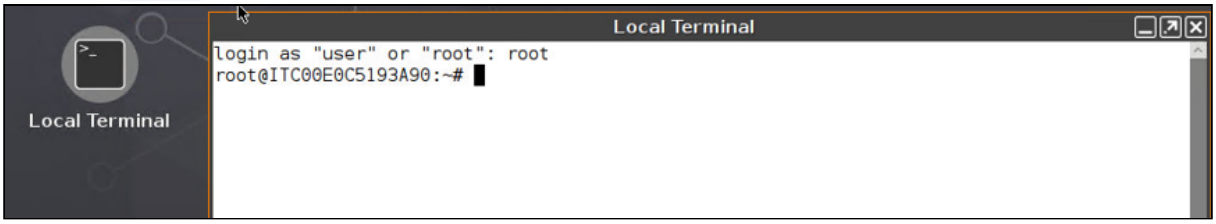


2. Under **Accessories > Terminals**, click + to create a terminal session.



Identifying the USB Stick

1. Plug the USB stick into the IGEL OS device and start the terminal session.
2. Log in as `root` (by default, no password).



3. Enter the following commands:

```
cd /userhome/media
ls -l
```

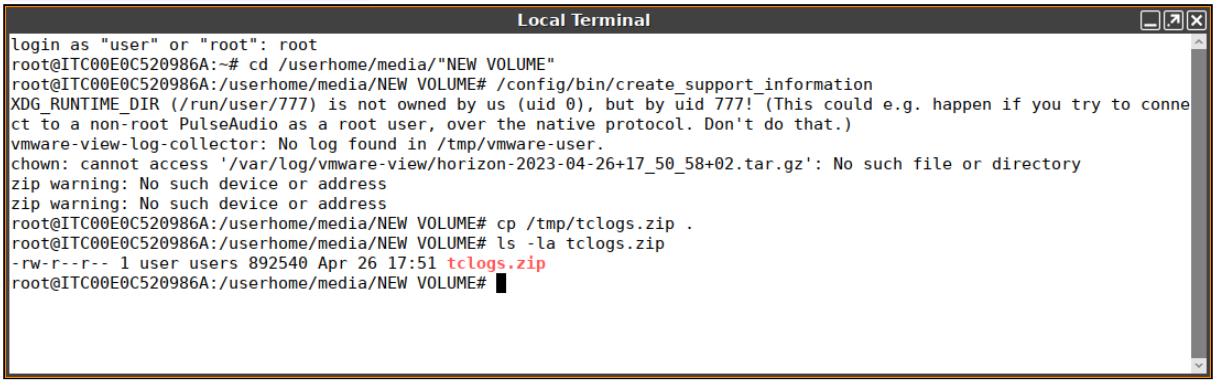
4. Note the name of the USB stick:

Writing the Log File

1. In the terminal, run the command `cd /userhome/media/[Name of your USB stick]`

> After `/media/`, you can press the tab key for autocompletion.
>
> **IMPORTANT**: If there are spaces in the device name, use quotation marks "". Example: `cd /userhome/media/"NEW VOLUME"`
>
> If there are no spaces in the device name, quotation marks are not required.

2. Run the command `/config/bin/create_support_information`
   This will generate the file `tclogs.zip` in the `/tmp` folder.
3. Copy `tclogs.zip` onto your USB stick using the following command. The dot at the end means the current folder:
   `cp /tmp/tclogs.zip .`



4. Safely eject the USB stick from the IGEL OS device.
   You can now examine this log file yourself or send it to IGEL support for analysis.

Exporting the Local Configuration of the IGEL OS Device

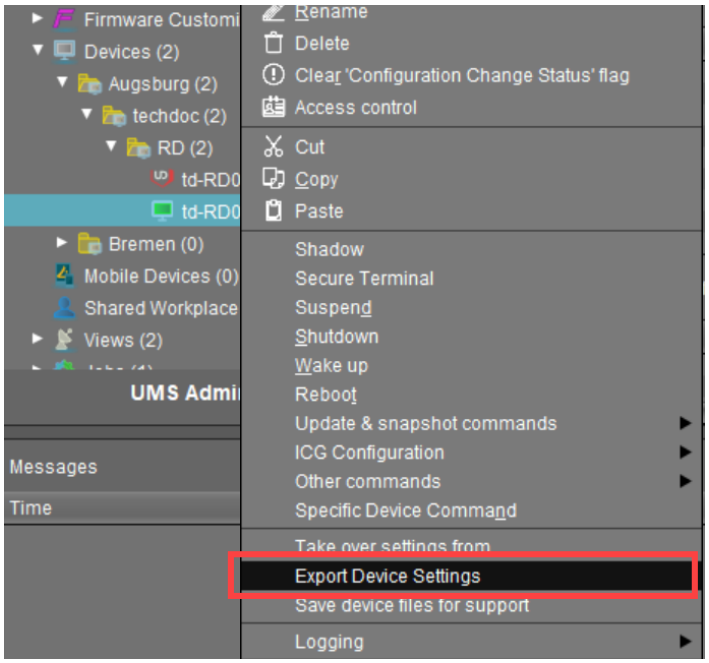
If you need to read out the current local configuration of a device (e.g. during a specific support case), you can copy the two local files `setup.ini` and `group.ini` either locally or via IGEL Universal Management Suite (UMS).

Option 1: Via UMS Console > Help > Save device files for support

You can transfer the `setup.ini` and `group.ini` files together with the device's log files as described in the section "With UMS" under Sending Device Log Files to IGEL Support (see page 1152).

Option 2: Via UMS Console > [device's context menu] > Export Device Settings

Alternatively, you can export the effective settings that affect the device (i.e. the interaction of local settings and all profiles) as an XML file: **UMS Console > [device's context menu] > Export Device Settings**.
The IGEL Support can import this file into the UMS as a profile and view the effective settings directly in the UMS Console.



Option 3: Via UMS Console > [device's context menu] > Other commands > Device File->UMS

You can also transmit the `setup.ini` and `group.ini` files from the device to the UMS via **UMS Console > [device's context menu] > Other commands > Device File->UMS**, see Transferring a File to the IGEL UMS Server[139].

139. https://kb.igel.com/en/universal-management-suite/current/how-to-transfer-a-file-to-the-igel-ums-server

Option 4: Via copying to a USB storage device

You can also save the files locally on a FAT32-formatted USB stick:

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage Hotplug**.
   If you use static client drive mapping, make sure that the **Number of drives** is greater than zero.
   See Storage Hotplug (see page 1969).

2. Create a terminal session under **Accessories > Terminals**.

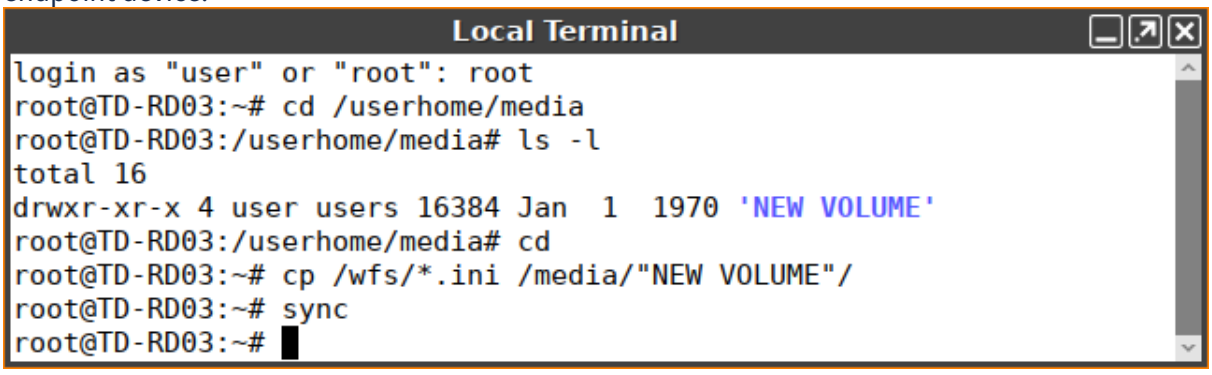
3. Connect your USB stick.

4. Open the terminal and log in as `root`.

   > To find out the name of the USB stick, you can use the commands:
   > `cd /userhome/media`
   > `ls -l`
   > If there are spaces in the device name, you'll have to include it later in the quotation marks "".
   > If there are no spaces in the device name, quotation marks will not be required.

5. Type `cp /wfs/*.ini /media/[name of USB storage device]/` and press [Return] to copy all `.ini` files from your endpoint device, incl. `setup.ini` and `group.ini`, to the USB stick.

6. Type `sync` and press [Return]. Wait a few seconds before safely ejecting the USB stick from the endpoint device.



Which Unified Communication Solutions Does IGEL OS Support?

This article provides an overview of the Unified Communication software and hardware solutions that are supported by IGEL OS.

Unified Communication Hardware Supported by IGEL OS

- Jabra Handsets / Headsets (see page 7)
- Poly Headsets (see page 11)
- EPOS / Sennheiser (see page 12)

Virtual Desktop Optimizations in IGEL OS

The virtual desktop optimizations provide the endpoint device with a media engine and redirect the audio and video streams so that they are exchanged directly between the endpoint devices. This results in higher performance and a lower server load.

Virtual Desktop Optimizations for Citrix Sessions

IGEL OS supports the following virtual desktop optimizations for Citrix sessions:

- Skype for Business
- Cisco Jabber (JVDI Client)
- Cisco Webex Meetings VDI and Cisco Webex VDI
- Microsoft Teams optimization
- Zoom VDI Media Plugin

For the configuration, see Unified Communications Settings for Citrix Sessions in IGEL OS (see page 1281).

Virtual Desktop Optimizations for Horizon Sessions

IGEL OS supports the following virtual desktop optimizations for VMware Horizon sessions:

- Skype for Business
- Cisco Jabber (JVDI Client)
- Cisco Webex Meetings VDI and Cisco Webex VDI
- Microsoft Teams optimization
- Zoom VDI Media Plugin

For the configuration, see Unified Communications Settings for VMware Horizon Sessions in IGEL OS (see page 1393).

Local Installation on the Endpoint Device with a Custom Partition

In contrast to the virtual desktop optimizations, where the Unified Communication apps are installed on the VDI server, this approach involves installing the apps on the endpoint device. This is achieved by using the Custom Partition mechanism of IGEL OS.

For building a Custom Partition by yourself, see the Custom Partition Tutorial (see page 852).

You can acquire any of the following Custom Partitions free of cost; just ask your IGEL contact person:

- Zoom (see also Zoom as a Custom Partition (see page 899))
- TeamViewer

Passthrough Authentication

Passthrough authentication is a convenient single sign-on method. With this function, an IGEL user logs in once and gains access to all sessions without having to explicitly authenticate themselves again for each of them.

This document explains what basic settings are necessary for passthrough authentication and where you can enable the single sign-on method in the relevant sessions.

- Introduction (see page 1166)
- Basic configuration (see page 1168)
- Session Configuration (see page 1175)

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=JxGOEGAb3LI

Introduction

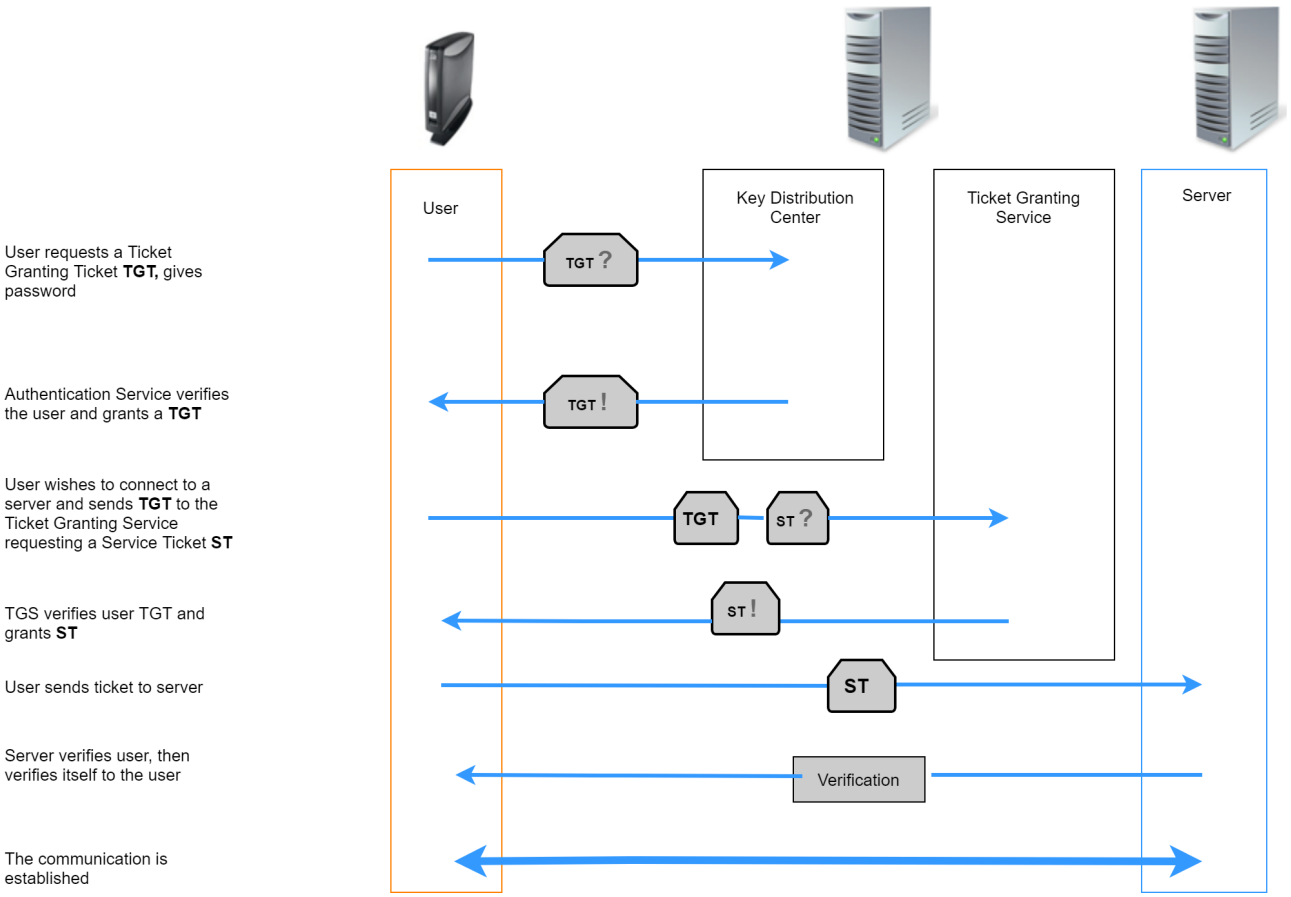
Two methods of single sign-on for a session are available:

Kerberos Passthrough	Real Kerberos authentication with clients that support Kerberos. Within a session, you can access network resources, e.g. file servers, without having to authenticate yourself again; this works automatically via Kerberos.
Passthrough	Uses cached credentials (user name and password) from local log-on for authentication. For access to network resources within sessions, you have to enter your credentials again.

Kerberos is an authentication service. It operates with user, service and computer entities which are known as **principals**. These principals all belong to a **realm**, an administrative unit. Each principal has a unique **principal name** within the realm. To provide the authentication system, a service known as **key distribution center** is used.

As an example, Microsoft Windows Domains form a realm. The Windows Domain name is the realm name (in upper case letters), e.g. `EXAMPLE.COM`. A user principal would be for example `user@EXAMPLE.COM`. The domain controllers take on the role of the key distribution centers.

When logging in, a user obtains a **ticket granting ticket** from the key distribution center. This ticket expires after a certain time (usually 1 day). When the user starts an ICA session for example, the client can obtain a so-called **service ticket** from the key distribution center with the aid of the ticket granting ticket. With this service ticket, authentication for the ICA server is accomplished.



To enable passthrough authentication you have to make certain settings:

1. Modify certain basic settings which are necessary to fulfill the conditions for Kerberos passthrough authentication. (see page 1168)
2. Enable passthrough authentication in the relevant session. (see page 1175)

Basic configuration

Your client configuration must fulfill certain conditions before you can enable passthrough authentication.

- Set the time correctly on all involved hosts and clients. (see page 1169)
- Configure the domain. (see page 1170)
- Activate login to the Active Directory domain. (see page 1172)

When activating the **Smartcard** login method, some additional configuration may be necessary (see page 1173).

Time

The time must be set correctly on all involved hosts and clients.

The best practice procedure is as follows:

1. Activate **Use NTP Time Server** under **System > Time and Date** in the setup.
2. Specify the **NTP Time Server**.

> A Windows domain controller can be used for this, if applicable.

Domains/Realms

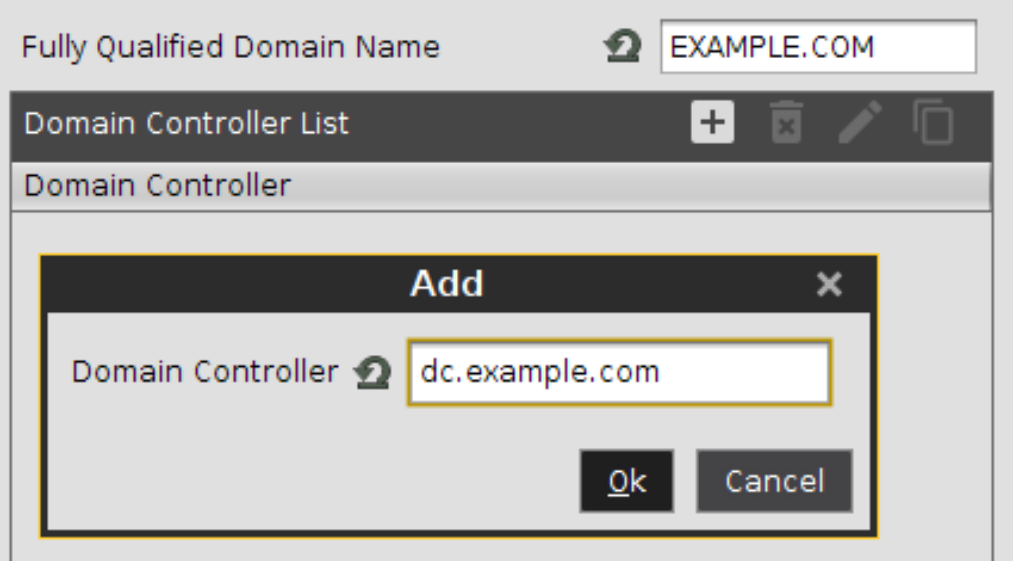
To configure the domain(s) proceed as follows:

1. Click **Security > Active Directory/Kerberos**.
2. Activate **enable** to enable Kerberos.
3. Enter the fully qualified domain name under **Default Domain**, e.g. `EXAMPLE.COM` (upper case letters).
4. Enable **DNS Lookup for Domain Controller** and **DNS Lookup for Domain**.

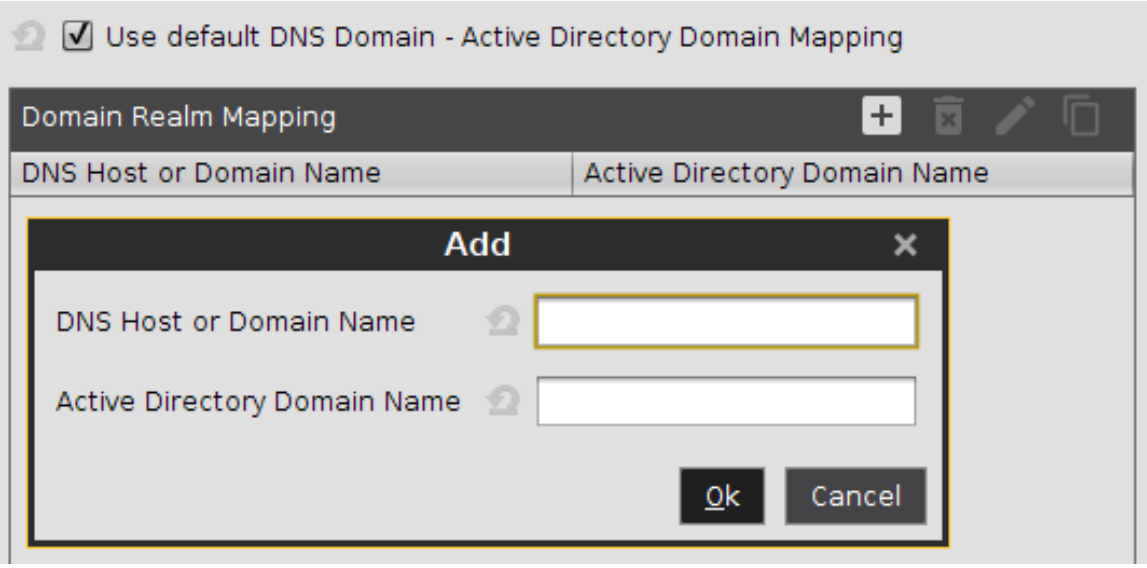
> These settings are sufficient for the domain setup when the DNS servers, e.g. the domain integrated MS DNS servers, are aware of the Active Directory.

Otherwise you may configure up to 4 domains/realms:

1. Click **Security > Active Directory/Kerberos > Domain1...4**.
2. Enter the **fully qualified domain name** , e.g. `EXAMPLE.COM` (upper case letters).
3. Specify at least one Windows domain controller (Kerberos key distribution center) in the **Domain Controller List**.
   It can be a DNS name or an IP address.



4. Click **Security > Active Directory/Kerberos > Domain Realm Mapping** to define the mapping between Active Directory domain names and DNS names.
5. Activate **Use default DNS Domain - Active Directory Domain Mapping**.



If both names match, i.e. if a host in the domain `EXAMPLE.COM` has the DNS name `host.example.com`, nothing needs to be done here and the default setting is sufficient. Otherwise an appropriate entry in the **Domain Realm Mapping** list has to be created.

Login

1. Click **Security > Logon > Active Directory/Kerberos**.
2. Activate **Login to Active Directory Domain**.
3. Choose one or more of the following login options:
    - **Explicit**: A login dialog is presented to the user.
    - **Remember last user name**: The login dialog will be prepopulated with the last user name that logged in. This option can be checked for convenience if **Explicit Login** is selected.
    - **Smartcard**: Login with smartcard and related smartcard PIN.
4. Underneath **Logout Shortcut Locations**, specify where a log-out button will appear.

Smartcard

For using the **Smartcard** login method, some additional configuration is necessary:

1. Under **Security > Logon > Active Directory/Kerberos**, activate **Smartcard**.
2. Under **Smartcard removal action**, define what should happen when the smartcard is removed:
   - **Log out**: Performs a disconnect or log out of running sessions, removes all user related data from the device and prepares the device for the next user login.
   - **Lock device**: Locks the screen during sessions. Only the user who is already logged in can unlock the device with his smartcard and PIN. Additionally, select **User password** under **User Interface > Screenlock / Screensaver > Options**, to make the setting effective.
3. Choose an appropriate PKCS#11 module under **Security > Smartcard > Middleware**.

   The smartcards for this login must be supported by a PKCS#11 module which can access the certificates on the smartcard.

Kerberos login with a smartcard involves certificates. The root certificate of the certificate used by the key distribution center (domain controller) must therefore be available on the device. Either the root certificate is one of the public trusted certificate authorities or it must be deployed to the device, see Deploying Trusted Root Certificates in IGEL OS (see page 764).

When using Windows 2000 or Windows Server 2003-based domain controllers in combination with smartcard login, the parameter `auth.krb5.realms.pkinit.pkinit_win2k` has to be activated in the registry. This enables the use of an earlier protocol version of `PKINIT preauthentication`.

Kerberos Ports

The following Kerberos ports are relevant for Linux environments:

	UDP Port	TCP Port
Getting tickets including the initial TGT	88	88
Changing password from UNIX/Linux		749

Session Configuration

For single sign-on with sessions, two methods are available:

- **Kerberos Passthrough**: Uses real Kerberos authentication with clients that support Kerberos.
- **Passthrough**: Uses cached user name and password from local logon for authentication.

> Currently, real Kerberos authentication is only available in Citrix sessions.

In the following sections, you can find how to activate passthrough authentication in sessions that support it:

- Citrix StoreFront/Web Interface (see page 1176)
- RDP (see page 1177)
- Horizon Client (see page 1178)
- Parallels Client (see page 1179)

Citrix StoreFront/Web Interface

1. Go to **Sessions > Citrix > Citrix Global > StoreFront Login**.
2. Select the **Authentication type**:
    - **Password authentication**: To enable passthrough, this option must be selected, and **Use Passthrough authentication** must be activated.
    - **Kerberos passthrough authentication**
    - **Smartcard authentication (StoreFront only, not Web Interface)**: Authentication via smartcard will only work with StoreFront, not with Web Interface.
    - **Citrix authentication mechanism (instead of IGEL), Smartcard disabled**
    - **Citrix authentication mechanism (instead of IGEL), Smartcard enabled**

See also StoreFront Login (see page 1249).

RDP

For RDP sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > RDP > RDP Sessions > [session name] > Logon**.
2. Enable **Use passthrough authentication for this session**.

Horizon Client

For Horizon sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > Horizon Client > Horizon Client Sessions > [session name] > Connection settings**.
2. Enable **Use passthrough authentication for this session**.

Parallels Client

For Parallels Client sessions, passthrough is supported. Kerberos passthrough is not yet supported.

1. Go to **Sessions > Parallels Client > Parallels Client Sessions > [session name] > Connection**.
2. Enable **Use system credentials** to use the passthrough authentication.

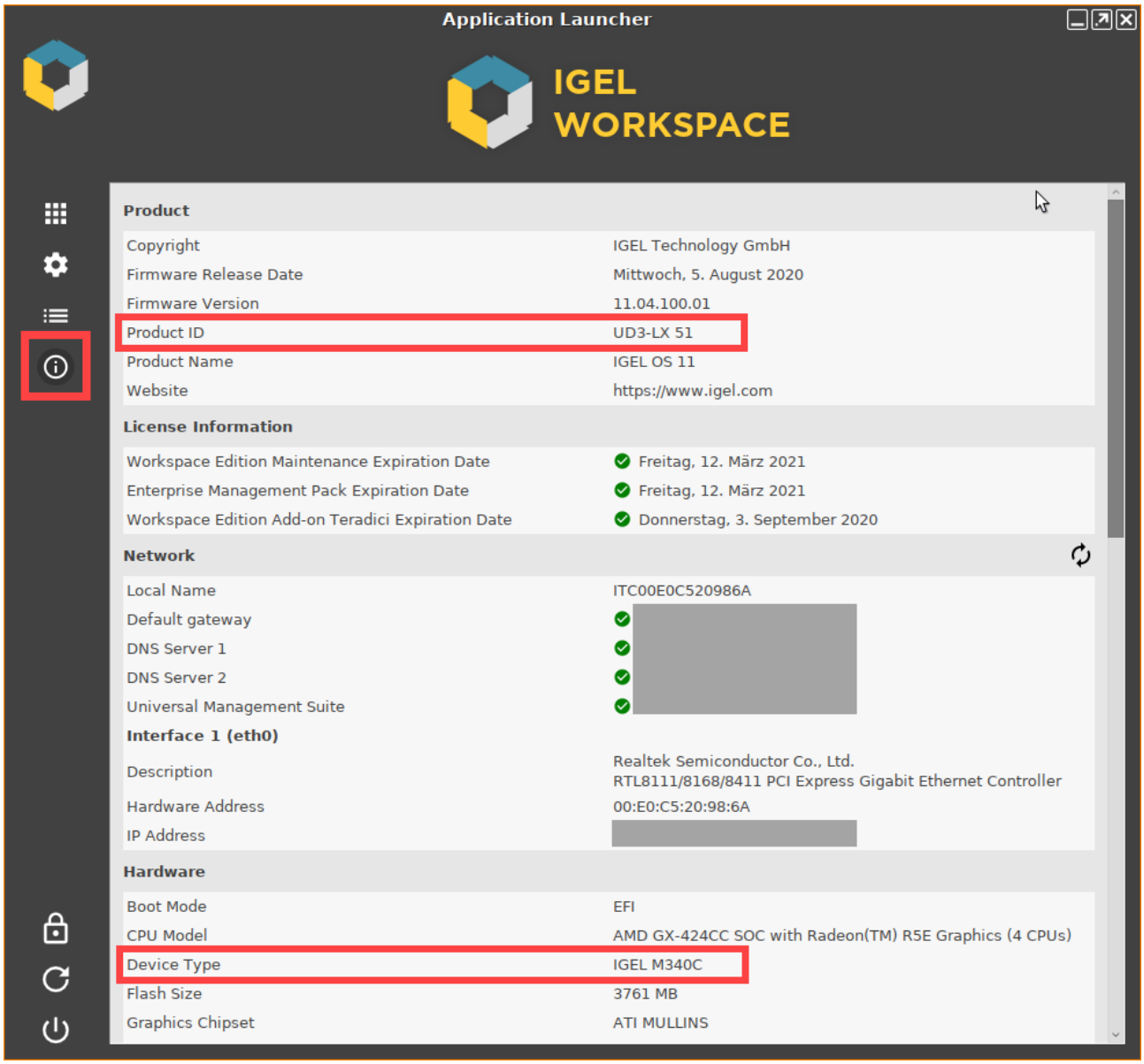
Hardware Video Acceleration on IGEL OS

Question

Does my hardware running IGEL OS offer video acceleration?

Answer

Open **Application Launcher > About** to look up your product ID and device type:



In version 5.07.100 and newer and version 10.01.100 and newer, IGEL OS offers hardware video acceleration for

- Media Player
- Citrix Multimedia Redirection
- RDP Multimedia Redirection (TSMF and EVOR)
- VMware Horizon Multimedia Redirection

on selected devices. This allows playing back HD video with a maximum of 20% CPU usage.

> The Multimedia Codec Pack (MMCP) is required for this feature if your IGEL OS version is lower than 11.01.100.

Hardware video acceleration is supported on the following IGEL devices:

Product ID	Device Type	Chipset	IGEL Linux >= v5.07.100	IGEL Linux >= v5.09.100	IGEL OS 10	IGEL OS 11
IZ2-HDX/RFX/ HORIZON 40* (see page 1182)	IGEL D220	Intel Bay Trail	✓	✓	✓	✓* (see page 1182)
IZ3-HDX/RFX/ HORIZON 41, 42	IGEL M330C	VIA VX900	✓			
IZ3-HDX/RFX/ HORIZON 50* (see page 1182)	IGEL M340C	ATI Mullins		✓	✓	✓* (see page 1182)
IZ3-HDX/RFX/ HORIZON 51* (see page 1182)	IGEL M340C	ATI Mullins			✓	✓* (see page 1182)
UD2-LX 40	IGEL D220	Intel Bay Trail	✓	✓	✓	✓
UD2-LX 50, 51	IGEL M250C	Intel HD Graphics				✓
UD3-LX 40	IGEL M320C	VIA VX900	✓	✓		
UD3-LX 41, 42	IGEL M330C	VIA VX900	✓	✓		
UD3-LX 50	IGEL M340C	ATI Mullins		✓	✓	✓
UD3-LX 51	IGEL M340C	ATI Mullins			✓	✓
UD3-LX 60	IGEL M350C	AMD Radeon Vega 3 Graphics				✓

Product ID	Device Type	Chipset	IGEL Linux >= v5.07.100	IGEL Linux >= v5.09.100	IGEL OS 10	IGEL OS 11
UD5-LX 40	IGEL H820C	Intel Sandy Bridge	✓	✓	✓	
UD5-LX 50	IGEL H830C (Dualcore CPU Model)	Intel Bay Trail	✓	✓	✓	✓
UD6-LX 51	IGEL H830C (Quadcore CPU Model)	Intel Bay Trail	✓	✓	✓	✓
UD7-LX 10	IGEL H850C	AMD Radeon Graphics			✓	✓
UD7-LX 11	IGEL H850C	AMD Radeon Graphics				✓
UD7-LX 20	IGEL H860C	AMD Radeon Vega 8 Graphics				✓
UD9-LX 40, UD9-LX 41 Touch	IGEL UD9 BT	Intel Bay Trail		✓	✓	✓
UD10-LX	IGEL UD10 TC236	VIA VX900	✓	✓		

On 3rd-party hardware with UDC3, IGEL OS Creator (OSC), and UD Pocket, hardware video acceleration depends on the graphics chipset of the device.

Codecs

The following codecs are supported:

- MPEG-2 (simple and main profiles)
- H.264 (baseline, main and high profiles)
- WVC1/WMV3 (simple, main and advanced profiles)
- MPEG-4 (DivX/Xvid): only on VIA VX900 and ATI Mullins

* To upgrade your IZ device to IGEL OS 11, please contact your IGEL sales representative. See also https://www.igel.com/tradeup/ and The IGEL OS 11 Migration Plan[140].

140. https://kb.igel.com/knowledge-base-archive/current/archive-igel-licensing

Running Commands before or after a Session

Symptom

You want to run shell commands before a specific session is started or after it has terminated.

Problem

You need hooks which will call your shell commands.

Solution

As of IGEL *Universal Desktop Linux 5.06.100* there is a generic mechanism for calling shell commands before and after a session. It works with Citrix ICA, RDP and VNC Viewer sessions.

This feature is accessible only through the **Registry**.

Open **Setup** at **System > Registry**. Use either the Registry tree or the **Search parameter ...** function to locate the following Registry keys:

for VNCviewer:

`sessions.vncviewer*.init_action`

`sessions.vncviewer*.final_action`

for RDP:

`sessions.winconnect*.init_action`

`sessions.winconnect*.final_action`

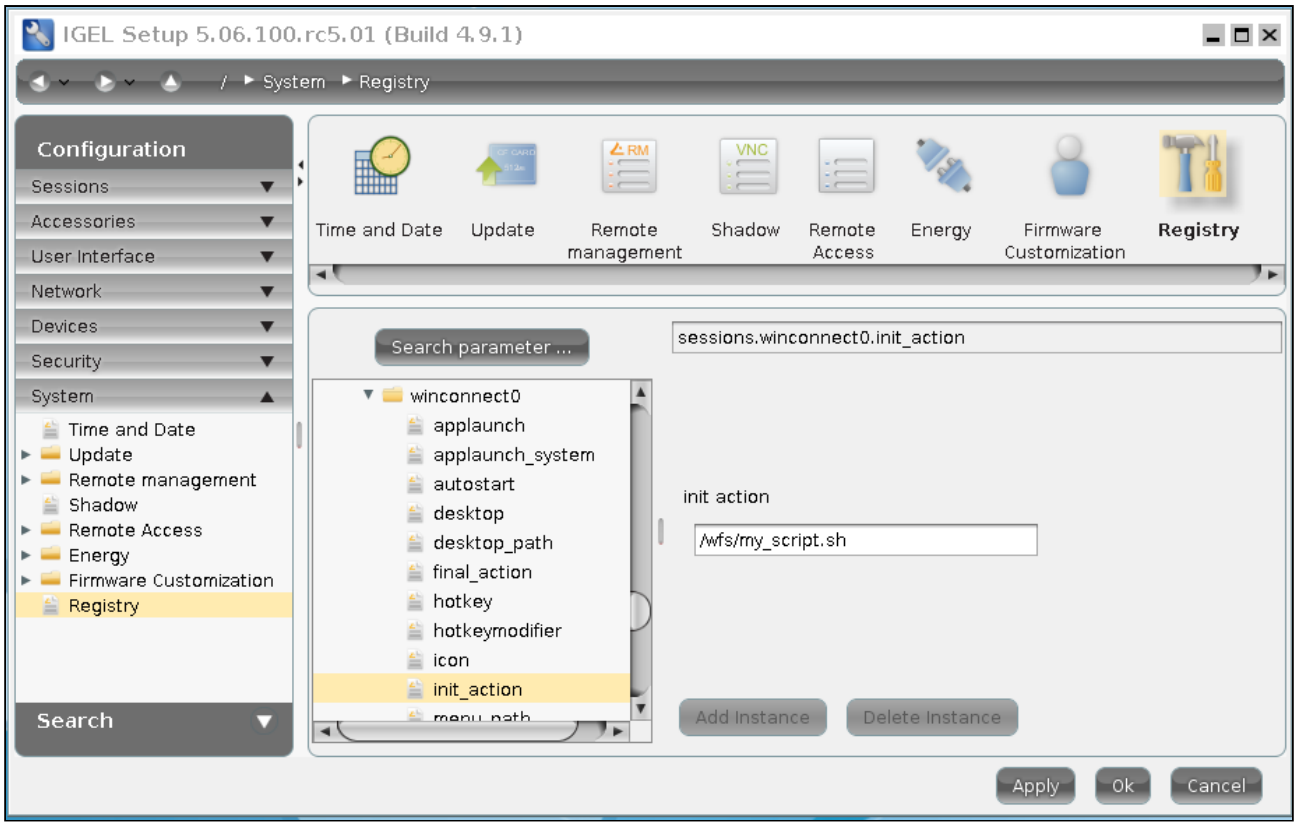
for Citrix/ICA:

`sessions.ica*.init_action`

`sessions.ica*.final_action`

(where * is the related session number, e.g. 0,1,2,3,...)

The `init_action` is executed before the session is started. The `final_action` is executed after the session has been terminated. Enter shell commands or the path to a custom script or executable:



The Registry keys for newly created sessions only appear after a restart of **Setup**.

Your `init_action` scripts or executables have to return before the session will start. Alternatively, background your command by adding `'&'` to the end of the commandline.

Copy Sessions in Setup or UMS

Sometimes you want to create a session that differs from another only in a few details. *IGEL* Linux *version 5.10.100* or newer and UMS *version 5.02.100* or newer let you copy complete sessions. Once the session is copied, you can easily adapt the required settings.

Copying is available in the **Sessions** section of *IGEL* Setup (and occasionally in some other sections) as well as in the **Edit Configuration** function in UMS.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. Click .
   A copy of the session will be created within the same folder.

IZ1 and UD2-MM Usage of RAM

How is RAM used by processes in UD2-MM and IZ1 (also known as ARM or SoC devices)?

A total of 1024 MB main memory is divided as follows:

- ~128 MB is used for graphics
- ~362 MB is used for internal processes such as communication between DSP and ARM processor
- ~534 MB is available for user processes

Using Symantec Ghost to Deploy IGEL OS

> Solution Based on Experience from the Field
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Topic of discussion/Issue

Using Symantec Ghost to Deploy IGEL OS

Firmware version

OS10 and OS11 (11.02.100)

UMS version

6.01

Description

This is in lieu of SCCM and our Deployment Appliance

Solution

We are deploying and capturing our IGEL base installation to/from a virtual machine using:

vSphere Client 6.0, version 11 VM:

- 8 GB RAM
- 4 CPUs (1 socket, 4 cores)
- Video: 1 display, 4 MB memory
- SCSI Controller Type: LSI Logic SAS
- CD/DVD Drive 1: IGEL_UDC_10.05.500.ISO
- CD/DVD Drive 2: Symantec WinPE
- HDD: SCSI, Thick Provision Lazy Zeroed, 20 GB
- Network Adapter: VMXNET 3
- Boot Options/Firmware: EFI

Boot to CD/DVD drive 1 and navigate through the UDC installation options:

- UDC Installation
- Language: English
- EULA: I Agree
- Force Legacy Installation: Not selected
- Force MS-DOS partitioning during installation: Selected

- Migrate old settings: Not selected
- Install Firmware
- Shutdown (do NOT reboot)

Boot to CD/DVD drive 2:

- Boot to WinPE
- Capture HDD image using Ghost command: `ghost64.exe -sure -clone,mode=create,src=1,dst=s:\igel\igel 10.05.500-YYYYMMDD_HHMMSS-0.gho -ial -ibg -nolilo`
  - `-ial` = Forces a sector-by-sector copy of Linux partitions. Other paritions are copied normally.
  - `-ibg` = Ignore Ghost Boot partition.
  - `-nolilo` = Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -NOLILO switch, you can restart your computer from a storage device after a clone and then `run/sbin/lilo` or GRUB install script as the root user to reinstall the boot loader.

To deploy to a physical client:

- Boot to WinPE
- Execute Diskpart:
  - select Disk 0
  - clean
  - exit
- Deploy HDD image using Ghost command: `ghost64.exe -sure -clone,mode=restore,dst=1,src=s:\igel\igel 10.05.500-20190510_185741-0.gho -ial -ibg -nolilo`
  - `-ial` = Forces a story-by-sector copy of Linux partitions. Other partitions are copied normally.
  - `-ibg` = Ignore Ghost Boot partition.
  - `-nolilo` = Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -NOLILO switch, you can restart your computer from a storage device after a clone and then run `/sbin/lilo` or the GRUB install script as the root user to reinstall the boot loader.
  - `-szee` = Forces Norton Ghost to keep the sizes of all destination partitions the same as in the source partition (no resizing).

  We don't do any image prep other than the `diskpart clean` command.

Starting UMS Console Crashes NX Session

Symptom:

When you are connected to an Ubuntu host via NX, starting UMS console on the Ubuntu host crashes the NX session.

Solution:

1. Become **Root** on the Ubuntu host.
2. Open the configuration file `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in a text editor.
3. Add the line `vmparam -Dsun.java2d.xrender=false` to the file.
4. Save the file.
5. Become a regular user.
6. Start UMS Console.

Accessing IGEL Setup within Appliance Mode

Symptom

When using the appliance mode, IGEL Setup is not accessible directly.

Problem

Within the appliance mode, all other local applications are hidden; the system's hotkey [Ctrl+Alt+s] does not work either.

Solution

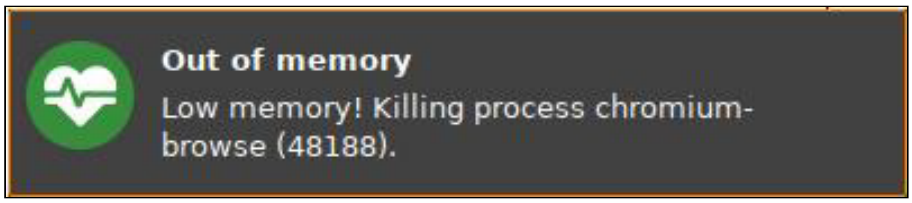
To start the IGEL Setup within the appliance mode, press hotkey [Ctrl+Alt+F2].

Application Is Terminated with Message "Low memory! Killing process ..."

Symptom

A local application or session is killed, and a message that reads **Low memory! Killing process [...]** is shown.

Example:



Environment

- IGEL OS 11.04 or higher

Problem

The system is running out of memory. As a countermeasure, the system has terminated the application.

Solution

->Close other applications that are not needed and restart the application.

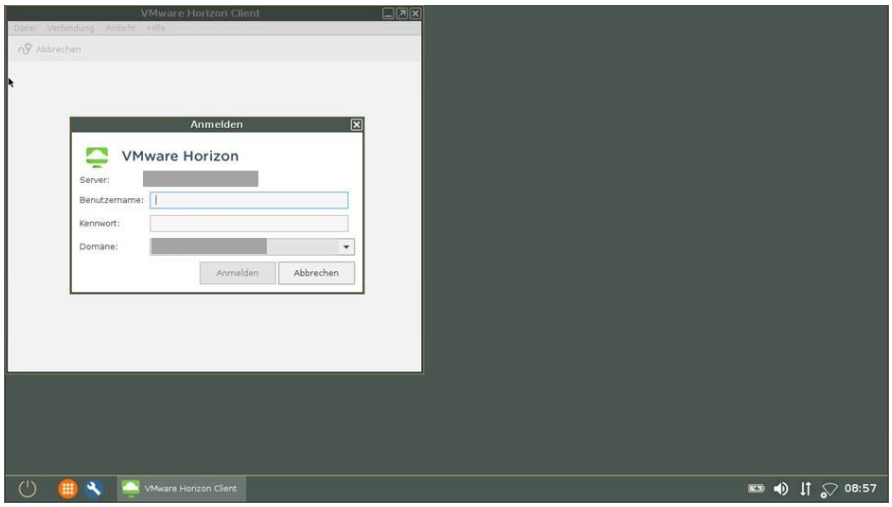
->If the terminated application is Chromium or Firefox, restart it and try using fewer open tabs.

->If the issue occurs often, consider extending the memory size of the devices.

An Application Window Cannot Be Repositioned

Symptom

Some application windows, e.g. VMware Horizon windows, are placed at startup in the upper left corner instead of being displayed in the middle. In case of frameless applications, the window cannot then be moved and may conceal the icons.



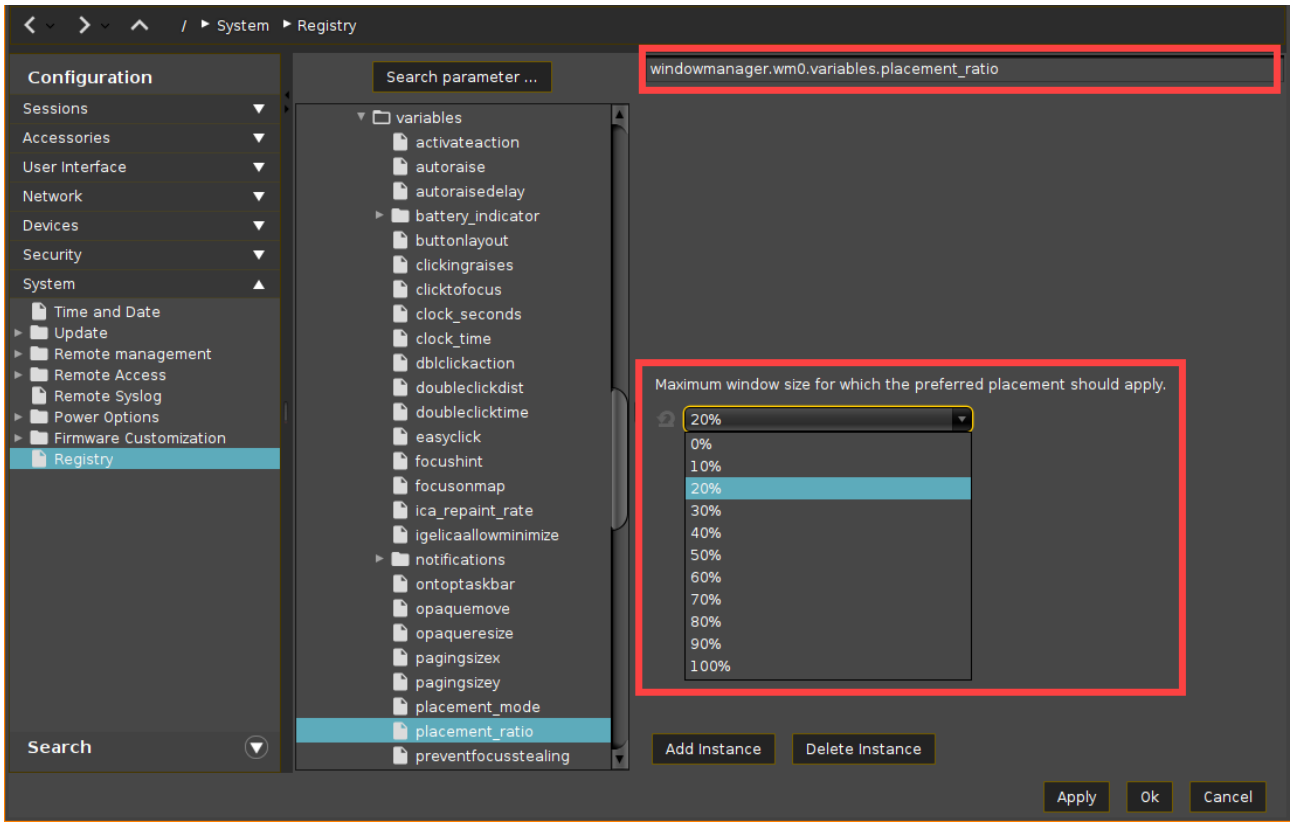
Problem

Either the screen is too small or the selected resolution is too low.

Solution

1. Go to **System > Registry**.
2. Select the registry key `windowmanager.wm0.variables.placement_ratio`.
3. Specify a higher percentage value under **Maximum window size for which the preferred placement should apply**. This entry refers to the total work area.

> The preferred placement is defined with the registry key `windowmanager.wm0.variables.placement_mode`.



Example

Session: VMware Horizon Client
Screen resolution: 1366x768
Value for **Maximum window size for which the preferred placement should apply**: at least 40%

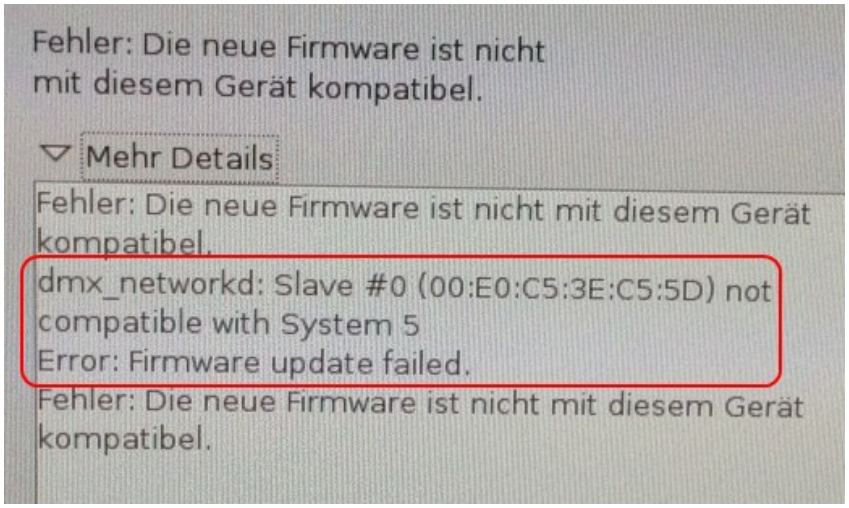
Updating IGEL UMD: Error "not compatible with System5"

Symptom

Universal Multi Display firmware (IGEL UMD) can't be updated to version 4.13.100.

Error Message:

```
Firmware not compatible.
dmx_networkd: Slave #0 (MAC) not compatible with System5
```



Solution

Delete file `/tmp/NOT_SYS_5_COMPATIBLE` from UMD master client and update again without rebooting.

IGEL Endpoint Partners: Ensuring Image Integrity with a Checksum

Overview

To ensure the integrity of your master image, it is recommended to create checksums and compare them between the original image and the images derived from it. This article describes how to create checksums for IGEL OS images that have been created using the IGEL OS Creator (OSC).

Requirements

- IGEL OS Creator (OSC) with IGEL OS 11.05.120 or higher

Instructions

For IGEL OS images that have been created with IGEL OSC Creator (OSC), partition 4 of the main device must be checked with the checksum method.

In the following example, the main device is `/dev/sda`:

1. Open a terminal on the device that contains the image. For more information, see Local Terminals (see page 1708).
2. In the terminal, enter `sha512sum /dev/sda4`
   The result should look like this:
   `7d5a25fac1756ef81ac78398d49db197904f60a0cf6594eac92071a5f6a8d6d4562fd3c8dc127cf22f89f6894000ca94918703c7143bfb11f1dd2ec052eaa52d /dev/sda4`
3. Repeat this process for all IGEL OS image copies you want to check and compare their checksums. If the checksums are identical, the images can be deployed.

Will My Session Be Closed When My IGEL OS Endpoint Device Enters Suspend Mode?

This article will teach you how to configure your IGEL OS device so that your session is not interrupted when your device goes into suspend mode.

Session Disconnection on Suspend

When an IGEL OS endpoint device goes into suspend mode (S3), remote sessions like Citrix, Microsoft Windows RDP, or VMware Horizon, for instance, will be disconnected.

IGEL Environment

- Endpoint device with IGEL OS 11
- Remote session, e.g. Citrix, Microsoft Windows RDP, or VMware Horizon

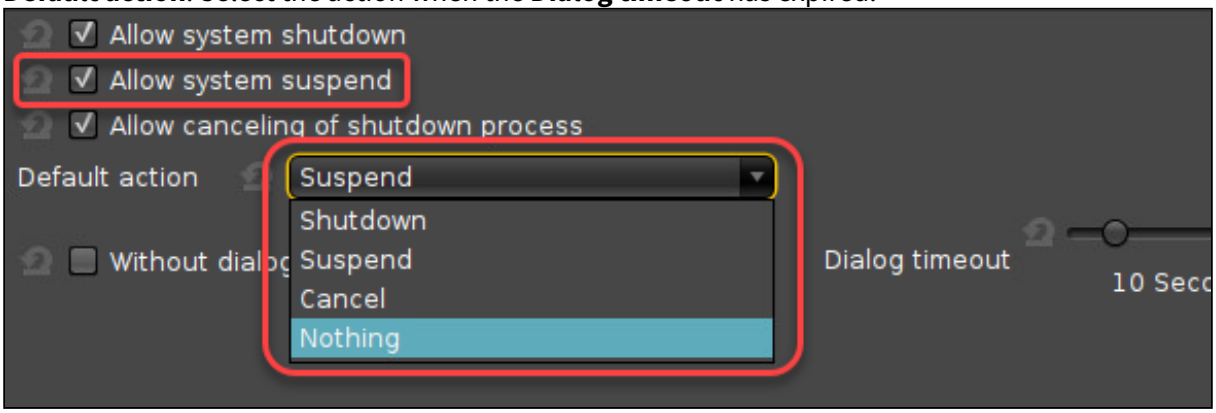
Avoiding Possible Issues

Modern server-based or cloud-based systems provide remote session resume features on the server side. Check out the relevant documentation for your system.

Configuring Suspend Mode

->To allow or disallow suspend mode, go to **System > Power Options > Shutdown** and set the following parameters according to your needs:

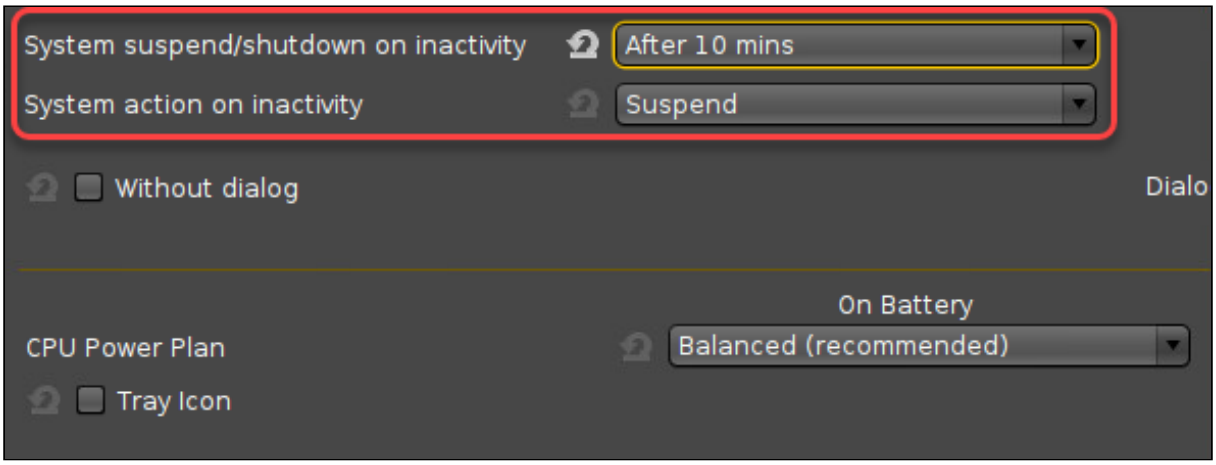
- **Allow system suspend**
- **Default action**: Select the action when the **Dialog timeout** has expired.



->To configure suspend or shutdown on inactivity, go to **System > Power Options > System** and set the following parameters according to your needs:

- **System suspend/shutdown on inactivity**: Set the timeout after which the system shuts down or enters suspend mode.

- **System action on inactivity**: Define whether the system should enter suspend mode or shut down after the timeout.



Microsoft Remote Desktop Client: Comparison of IGEL OS with Other Vendors

Rolling Release Info: OS 11.08.330

The information provided here is valid with IGEL OS 11.08.330 and higher.

The information provided here reflects the state on May 13, 2022.
The information was mostly obtained from the following sources:
Microsoft:

- https://support.microsoft.com/en-us/office/teams-features-by-platform-debe7ff4-7db4-4138-b7d0-fcc276f392d3
- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-features
- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-app-compare

Citrix:

- https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html
- https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/citrix-workspace-app-feature-matrix.pdf

VMware:

- https://kb.vmware.com/s/article/86475
- https://kb.vmware.com/s/article/80386?lang=en_US

The following table shows the features currently available in Microsoft Remote Desktop Client, including IGEL OS which is built with the Microsoft RD Core for Linux.

Feature	Windows 10		Microsoft Store Client	Android	iOS	macOS	Web	IGEL OS			Comments
	RDP	AVD / W365	Native	Native				AVD / W365	Citrix	VMware	
Common											
Remote Desktop sessions	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	The desktop of a remote computer is presented in a full-screen or windowed mode

Integrated RemoteApp sessions	yes	yes	no	no	no	yes	no	no	yes	no	Individual remote apps are integrated into the local desktop as if they are running locally
Immersive RemoteApp sessions	no	no	yes	yes	yes	no	yes	yes (no taskbar)	no	yes	Individual remote apps are presented in a window or maximized to a full screen
Multiple monitors	16 monitor limit	16 monitor limit	no	no	no	16 monitor limit	no	16 monitor limit	8 monitor limit	8 monitor limit	Allows the user to run a remote desktop or remote apps on all local monitors
Dynamic resolution	yes	yes	yes	no	no	yes	yes	yes	yes	yes	The resolution and orientation of local monitors are dynamically reflected in the remote session. If the client is running in windowed mode, the remote desktop is resized dynamically to the size of the client window.
Smart sizing	yes	yes	yes	no	no	yes	no	yes	yes	yes	The remote desktop in windowed mode is dynamically scaled to the window's size
Localization	no	yes	yes	English only	yes	yes	yes	English only	yes	no	The client user interface is available in multiple languages
Multi-factor authentication	no	yes	yes	yes	yes	yes	yes	yes	yes*	yes	Supports multi-factor authentication for remote connections

Prioritized datastreams	no	no	no	no	no	no	no	no	yes	no	Admins can configure the priority for certain data streams
* Targeting Citrix Storefront directly, smartcards and federated authentication (SAML/AzureAD) are supported. Using Citrix ADC, multiple MFA-Providers and methods are supported.											
Input Redirection											
Keyboard	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	
Mouse	yes	yes	yes	yes	yes*	yes	yes	yes	yes	yes	
Touchscreen	yes	yes	yes	yes	yes	no	yes (except IE)	no	yes	no	
Pen	yes	yes	no	yes (as touch)	yes (as touch)	no	no	no	yes**	no	
* View the list of supported input devices for the Remote Desktop iOS client: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-ios#supported-input-devices ** Depending on the pen											
Port Redirection											
COM Port	yes	yes	no	no	no	no	no	no	yes	yes	
USB	yes	yes	no	no	no	no	no	yes*	yes	yes	*Fabulatech USB Redirection
Other Redirections (devices, etc.)											
Cameras	yes	yes	no	no	yes	yes	no	yes*	yes	yes	*Fabulatech Webcam Redirection
Enhanced Camera Redirection	no	no	no	no	no	no	no	no	yes	no	Allows configuration of camera parameters to be used within the remote session

Clipboard	yes	yes	yes	Text	Text, images	yes	Text	yes	yes	yes	
Local drive/ storage	yes	yes	no	yes	yes	yes	no	yes	yes	yes	
Location	yes	yes	no	no	no	no	no	no	no	no	
Microphones	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	
Multi-audio	no	no	no	no	no	no	no	no	yes	no	Allows the redirection of multiple local audio devices into VDI
Printers	yes	yes	no	no	no	yes (CUPS)	PDF Print	yes (CUPS only)	yes (CUPS)	yes	
Scanners	yes	yes	no	no	no	no	no	yes*	yes*	yes	*Fabulatech Scanner Optimization
Smartcards	yes	yes	no	no	no	yes (Windows logon not supported)	no	no	yes	yes	
Speakers	yes	yes	yes	yes	yes	yes	yes (except IE)	yes	yes	yes	
Browser Content	no	yes*	no	no	no	no	no	no	yes	no	Allows execution of e.g. browser-based multimedia content on the client device to reduce load and traffic within the datacenter *Multimedia redirection for AVD (preview)

GPU acceleration	no	yes [2]	no	no	no	no	no	no	yes [1]	yes	Allows running graphics-heavy applications running in virtualized environments utilizing the server's GPU and lossless compression for e.g. CAD applications [1] Citrix HDX 3D Pro requires Citrix Virtual Apps and Desktops Platinum License [2] GPU-optimized AVD host (pool) with GPU-accelerated app rendering, GPU-accelerated frame encoding, or fullscreen video encoding
Additional Features (UI / UX / Security)											
Screen pinning	no	no	no	no	no	no	no	no	yes	no	Save complete display layout on Storefront servers (also supports Geo load balancing)
Keyboard layout synchronization	yes	yes	no	no	no	no	no	yes	yes	yes	The keyboard layout within the VDI is set according to the client's keyboard
Keylogging protection	no	no	no	no	no	no	no	no	yes	yes	A keylogger on the client only sees encrypted keystrokes

Screenshot prevention	no	no	no	no	no	no	no	no	yes	yes	Screenshots created on the endpoint will only show blank content when capturing a VDI screen.
UC Optimization											
Feature	**Windows 10**	**Windows 10**	**Microsoft Store Client**	**Android**	**iOS**	**macOS**		**IGEL OS**			**Comments**
	RDP	**AVD / W365**	**Native**	**Native**		**Web client**	**Native**	**AVD / W365**	**Citrix**	**VMware**	
MS Teams	no	yes	no	no	no	no	no	yes	yes	yes	Media optimizations for Microsoft Teams to provide high-quality calls and screen-sharing. Learn more at Use Microsoft Teams on Azure Virtual Desktop.[141]
Cisco Jabber	no	no	no	no	no	no	no	no	yes	no	Optimization enables the physical client to directly communicate and offload webcam and audio from the server to the client completely transparent to the user

141. https://docs.microsoft.com/en-us/azure/virtual-desktop/teams-on-avd

Cisco Webex Meetings / Teams	no	no	no	no	no	no	no	no	yes	yes	The Cisco Webex media engine redirects audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter
Skype for Business	no	no	no	no	no	no	no	no	yes	yes	Signaling information is sent via a virtual channel to the client's RealTime media engine. That allows RealTime media to be executed directly on the user's device.
Zoom	no	yes	no	no	no	no	no	yes	yes	yes	The Zoom plugin on the client will offload video encoding and decoding and communication directly to the Zoom cloud

Avaya IX Workplace	no	yes [1]	no	no	no	no	no	yes [1] [2]	yes [1]	yes [1]	VDI optimization for customers using Avaya UC Client within their environment. Control information gets exchanged via the remote desktop protocol (ICA or Blast). Calls take place via SIP directly, surpassing the VDI. [1] Avaya IX Workplace for IGEL OS is not generally available because of the Avaya distribution policy/ license agreement. The customer needs to get in contact with Avaya support to receive custom partition files and support [2] Not approved. Needs to be verified/tested.
Estos ProCall	no	no	no	no	no	no	no	no	yes [1] [2]	no	[1] Audio datastream (UDP Opus or G.711a) between the ProCall Client (WebRTC Stack) and the UC Media Server is routed through the Citrix Server(s) and transferred via Citrix HDX-Audio to the endpoint. [2] Not officially tested/ verified by IGEL

WebRTC (in general)	no	yes [2]	no	no	no	no	no	no	yes [1]	yes [2]	Optimize WebRTC to offload webcam and audio to the client [1] Using Citrix BCR feature [2] Part of Teams optimization (based on WebRTC). Needs to be verified.

IGEL OS Third Party Integrations

Rolling Release Info: OS 11.07.110

The information provided here is valid with IGEL OS 11.07.110 and higher.

The following table shows the 3rd party features included in IGEL OS that are currently supported with the listed VDI connections.

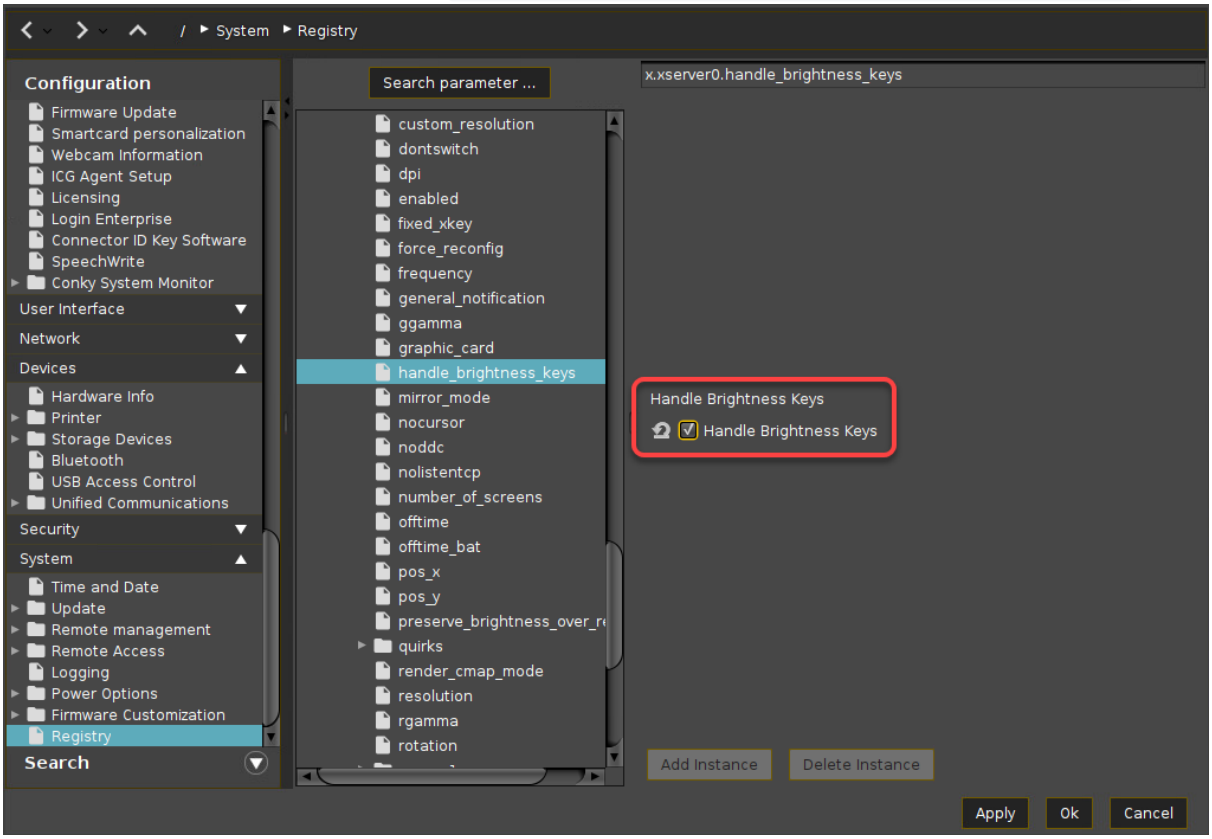
Feature	IGEL OS AVD / W365	IGEL OS Citrix	IGEL OS VMware	IGEL OS RDP	Comments
Cisco JVDI Client	no	yes	yes	no	
Cisco WebEx Meetings VDI	no	yes	yes	no	
Cisco WebEx VDI	no	yes	yes	no	
Zoom VDI Media Plugin	yes	yes	yes	no	
Microsoft Teams Optimization	yes	yes	yes	no	
Fabulatech USB Redirection	yes	yes	yes	yes	
Fabulatech Camera Redirection	yes	yes	no	no	
Fabulatech Scanner Redirection	yes	yes	yes	yes	
deviceTRUST (see page 17)	yes*	yes	yes*	no	* Will be available soon
DriveLock	no	yes	no	yes	
Diktamen (see page 5)	no	yes	partially*	yes	* Dictation supported, but no virtual channel initiated
Grundig dictation	no	yes	partially*	yes	* Dictation supported, but no virtual channel initiated
Nuance dictation (see page 9)	no	yes	partially*	no	* Dictation supported, but no virtual channel initiated

Feature	IGEL OS AVD / W365	IGEL OS Citrix	IGEL OS VMware	IGEL OS RDP	Comments
Olympus dictation (see page 10)	no	yes	partially *	yes	* Dictation supported, but no virtual channel initiated
Philips dictation (see page 18)	no	yes	partially *	yes	* Dictation supported, but no virtual channel initiated
SpeechWrite	no	yes	partially *	no	* Dictation supported, but no virtual channel initiated
Signotec signature (see page 14)	no	yes	yes*	yes	* Using VMware HID Optimization
StepOver signature (see page 15)	no	yes	yes*	yes	* Using VMware HID Optimization
Kofax signature (Wacom) (see page 16)	no	yes	yes*	yes	* Using VMware HID Optimization
Lakeside SysTrack	yes	yes	yes	yes	Using client virtual channels
PrinterLogic	no	yes	no	yes	
ThinPrint	yes*	yes	yes	yes	* Using ezeep (see page 1676) for Azure
Tricerat	yes*	no	no	no	* Using Tricerat custom partition for IGEL

How Do I Get My Fn Keys to Work?

Brightness Key

1. In the Profile Configurator or local Setup, enable **System > Registry > x > xserver0 > handle_brightness_keys**. (Registry `key: x.xserver0.handle_brightness_keys`)



2. Confirm your changes with **Ok** or **Apply**.

Invalid Session Names

Symptom

A session on the thin client does not start or the session name is not displayed correctly.

Problem

The problem may be caused by an invalid name of the session. The session's name must not contain the following characters: `\ / : * ? “ < > | [ ] { } ( )`

Solution

Rename the session without using prohibited characters.

IGEL OS Reference Manual

- What Is New in 11.10.410? (see page 1212)
- IGEL Workspace Edition (see page 1213)
- Bluetooth Assistant (see page 1217)
- Boot Procedure (see page 1218)
- The IGEL OS Desktop (see page 1228)
- Setup (see page 1237)
- Sessions (see page 1243)
- Accessories (see page 1703)
- User Interface (see page 1844)
- Network (see page 1898)
- Devices (see page 1967)
- Security (see page 2013)
- System (see page 2041)
- Setup Assistant for IGEL OS (see page 2101)

What Is New in 11.10.410?

The release notes for the latest release of IGEL OS 11.10.410 can be found on our download server at www.igel.com/software-downloads/workspace-edition/[142] as well as in the Knowledge Base under IGEL OS Release Notes (see page 2282).

142. https://www.igel.com/software-downloads/workspace-edition/

IGEL Workspace Edition

IGEL devices comprise the latest hardware and an embedded operating system based on IGEL Linux.

The firmware included with every IGEL Workspace product is multifunctional and contains a wide range of protocols allowing access to server-based services.

Management software: Universal Management Suite

For optimum management of your IGEL devices, the IGEL Universal Management Suite (UMS) is available on our download page[143].

> With the IGEL Universal Management Suite, you can configure devices in the same way as in the devices' local setup.

- Supported Formats and Codecs (see page 1214)
- IGEL Devices Supported by IGEL OS 11 (see page 1215)

143. https://www.igel.com/software-downloads/igel-universal-management-suite/

Supported Formats and Codecs

As supplied, IGEL OS 11 supports the following multimedia formats and codecs:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC
- Multimedia Codec Pack (MMCP); enabled by the Workspace Edition, see *IGEL Subscription and More > IGEL Subscription and More > _Hide from Viewport > IGEL Software License Overview*
  The MMCP includes the following codecs:

Supported Formats	Supported Codecs
AVI	MP3
MPEG	AAC
ASF (restricted under Linux)	WMA stereo
WMA	WMV 7/8/9
WMV (restricted under Linux)	MPEG 1/2
MP3	MPEG4
OGG	H.264

AC3 is not licensed.

IGEL Devices Supported by IGEL OS 11

Core Requirements for IGEL OS 11

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

RAM size higher than 2 GB is recommended if you use any of the following:
- Unified Communications optimizations (uses a client-side media engine)
- High-resolution graphics output
  For details on the supported graphics-related characteristics of IGEL devices, see Graphics on IGEL Devices[144]. For older devices, see https://kb.igel.com/knowledge-base-archive/current/eol-eos-eom-archive.
- More than two monitors

- Storage: 2 GB minimum; ≥ 4 GB recommended

Storage Requirements for IGEL OS 11.04 or Higher
IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD2****	D220	40	Yes	2 GB	4 GB	Yes
UD2*	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51 / 52***	Yes	2 or 4 GB	8 GB	Yes
UD3*	M340C	50	Yes	2 GB	4 GB	Yes
UD3*	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5*	H830C	50	Yes	2 GB	4 GB	Yes

144. https://kb.igel.com/hardware/current/graphics-on-igel-devices

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD6*	H830C	51	Yes	2 GB	4 GB	Yes
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7**	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9*	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

*IGEL UD3-LX 50 and UD5-LX 50 are supported up to IGEL OS 11.05, incl. private builds.
IGEL UD9-LX 40 / 41 (Touch) devices are supported up to IGEL OS 11.07.910.
IGEL UD2-LX 50 devices are supported up to IGEL OS 11.09.160.
IGEL UD3-LX 51 devices are supported up to IGEL OS 11.09.160.
IGEL UD6-LX 51 devices are supported up to IGEL OS 11.09.160.

** As of December 2019, IGEL UD7 model H850C is equipped with the (en) AMD Secure Processor ; for further information, see (en) UD7 Model H850C .

*** IGEL UD2-LX 52 is supported with IGEL OS 11.06.140 and later.

**** UD2-LX 40 (model D220) is supported up to IGEL OS 11.08.200. For an overview of the end-of-sales (EOS) and end-of-maintenance (EOM) dates for IGEL devices, see https://kb.igel.com/knowledge-base-archive/current/archive-list-of-legacy-igel-devices.

IGEL Zero

Note on IZ Devices
The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also https://www.igel.com/os11migration/ .

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

Bluetooth Assistant

A Bluetooth Assistant starts before the actual Setup Assistant. This tests whether a USB mouse and/or a USB keyboard are available. If not, it searches for unconnected Bluetooth devices and helps you connect them.

The assistant starts with a window in which a timeout expires for a few seconds. During this time you can still cancel the wizard.

On the following setup pages you can make settings related to Bluetooth:

Bluetooth Tool:

Path: Accessories > Bluetooth Tool (see page 1788)

Here you define the start options for the **Bluetooth Tool** session.

USB Access Control:

Path: Devices > USB Access Control (see page 2010)

If you have USB access control enabled, you should make sure that you explicitly allow the connection to your Bluetooth devices via a class rule or device rule.

Bluetooth

Path: Devices > Bluetooth (see page 2009)

Bluetooth must be activated here so that you can work with Bluetooth devices.

If you activate **Tray Icon**, you can start the Bluetooth tool via an icon in the system bar.

If you want to disable the Bluetooth Assistant in general, put the file `.igel_skip_bt-autopairing` in the directory `/wfs/user/`
The assistant will be skipped.

For more information about enabling Bluetooth services, see Bluetooth (see page 2009).

Boot Procedure

The quick installation procedure is complete.

→ Restart the system in order to start the boot procedure.

- Network Integration (see page 1219)
- Boot Menu (see page 1220)
- X-Server (see page 1227)

Network Integration

Once the kernel has been loaded, the network can be configured.

There are three possible ways of integrating the terminal into the network environment.

Depending on the terminal settings, choose between

- **DHCP**,
- **BOOTP**,
- **manually configured IP address**.

> The network interface can be stopped and restarted on the Linux Console (accessible via [Ctrl]+[Alt]+[F11]) with this command: `/etc/init.d/network stop` `/etc/init.d/network start`

Boot Menu

During the boot procedure, a boot menu is available on request. Via this menu, you can access system parameters or reset the device to the factory defaults if the device is configured incorrectly or you experience problems when booting.

→ During the boot procedure, press the [Esc] key repeatedly in rapid succession in the second stage loader when the "loading kernel" message is shown on the screen.
A menu with four boot options as well as an option for resetting the device to the default factory settings will appear:

- **Quiet boot**: Normal start (default)
- **Verbose boot**: Start with system messages and an interactive root shell
- **Emergency boot (setup only)**: Setup only
- **Failsafe boot with CRC check**: Start with an integrity check of the operating system
- **Reset to factory defaults**: Reset the client to factory defaults
- **Custom boot command**: Boot with configurable command line options

Quiet Boot

Quiet boot is the default boot mode. In this mode, all kernel messages are disabled and the graphical user interface is started.

Verbose Boot

Unlike in **Quiet boot** mode, the boot messages are shown in **Verbose boot** mode. The boot procedure also pauses before the graphics system and the user session start.

This gives you an opportunity to open a root shell and interactively execute debugging commands (such as `ifconfig` etc.).

> Use the root shell only if you have adequate knowledge of Linux or if you are instructed to do so by the IGEL Helpdesk and are given appropriate guidance. Incorrect use can destroy the operating system.

Proceed as follows:

1. Select **Verbose boot** from the boot menu.
2. Wait until the boot messages stop at `Reached target IGEL Network Online`.
3. Open a virtual console with the key combination [Ctrl]+ [Alt]+ [F11]or [Ctrl]+ [Alt]+ [F12].
4. Log in by pressing [Return]and enter the root password if necessary.
5. Go through the desired individual commands.
6. Now enter the following command to continue the normal boot procedure:
   `systemctl default`
   The graphical user session will start.

Emergency Boot

During an **Emergency Boot**, the device is started without network drivers and with a resolution of 640 x 480 - 60 Hz. The setup is then opened directly.

This option is useful if, for example, you have selected an excessively high screen resolution or a wrong mouse type and these settings can no longer be changed in the normal setup.

→ Close the setup window to shut down the system or restart it.
Unlike with a reset, the setup will open with the actual settings.

Failsafe Boot - CRC Check

During a **Failsafe boot**, a check of the file system is carried out first. The device then starts in **Verbose mode**.

This option is helpful if you no longer have a bootable system after a firmware update. The **Failsafe boot** checks where the problem is. If need be, an old version will be booted and you will need to repeat the firmware update.

Reset to Factory Defaults

You can reset IGEL OS devices to factory defaults through the boot menu, but the best practice is to reset devices using the OSC as descried in IGEL OS Creator Manual[145].
You can also reset your device to factory defaults in the UMS Console under **Devices > Other commands > Reset to Factory Defaults**, see Devices section in Menu Bar of the IGEL UMS Console[146].

If you select **Reset to factory defaults**, all personal settings on the device (including your password and the sessions you have configured) will be lost.

A warning message will appear on the screen before the procedure is carried out. If the device is protected by an administrator password, you will be prompted to enter this password.

Do You Know the Password?

1. Confirm the warning message.
2. Enter the password. You have three attempts.

Do You Not Know the Password?

1. Confirm the warning message.
2. When you are prompted to enter the password, press the Enter key three times.
3. Press [c].
   The Terminal Key will appear.
4. Contact us using license@igel.com[147].
5. Enter the Terminal Key that is shown, the firmware version, and your contact details.
   IGEL will send you a so-called Reset to Factory Defaults Key that is specific for your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.
   See also How to Reset a Device with Unknown Administrator Password[148] .

145. https://kb.igel.com/en/igel-os/11.10.270/igel-os-creator-manual
146. https://kb.igel.com/en/universal-management-suite/current/menu-bar-of-the-igel-ums-console
147. mailto:license@igel.com
148. https://kb.igel.com/en/igel-os/11.10.270/how-to-reset-a-device-with-unknown-administrator-p

Custom Boot Command

If you select **Custom boot command**, preconfigured options will be placed on the kernel command line. This allows you for example to investigate and rectify problems with specific hardware components.

The Custom boot command is merely a temporary solution – it is not an everyday booting method. It must therefore be selected manually in the boot menu.

To configure the options for the Custom boot command, proceed as follows:

1. Open a **local terminal** and log in as `root`.
2. Enter the following command to bring up the current options:
   `bootreg get /dev/igfdisk boot_cmd`
3. Save your desired options with the following command:
   `bootreg set /dev/igfdisk boot_cmd "<Your Options>"`
4. Check the options that you have entered:
   `bootreg get /dev/igfdisk boot_cmd`

If you would like to delete options for the Custom boot command, leave an empty string of characters in their place: `bootreg set /dev/igfdisk boot_cmd ""`

X-Server

The final step in the boot procedure involves starting the **X-Server** and the local **windowmanager**.

The IGEL OS Desktop

You can operate the device via the taskbar and the IGEL menu.

The following items can be found in the taskbar at the bottom of the screen:

1	Opens the *IGEL* menu.
2	**Quick Start Panel**
	Application Launcher: Opens a dialog window with start symbols for sessions.
	Setup: Opens the *IGEL* setup.
	Symbol for sessions: Launches a session.
3	**Window bar**
	Allows you to switch between open windows.

4	**System tray**
	CPU power plan: Changes the power saving settings.
	Volume control
	Allows you to remove a USB stick safely
	Local network connection
	09:14 Time / date

The *IGEL* menu offers the following areas and functions:

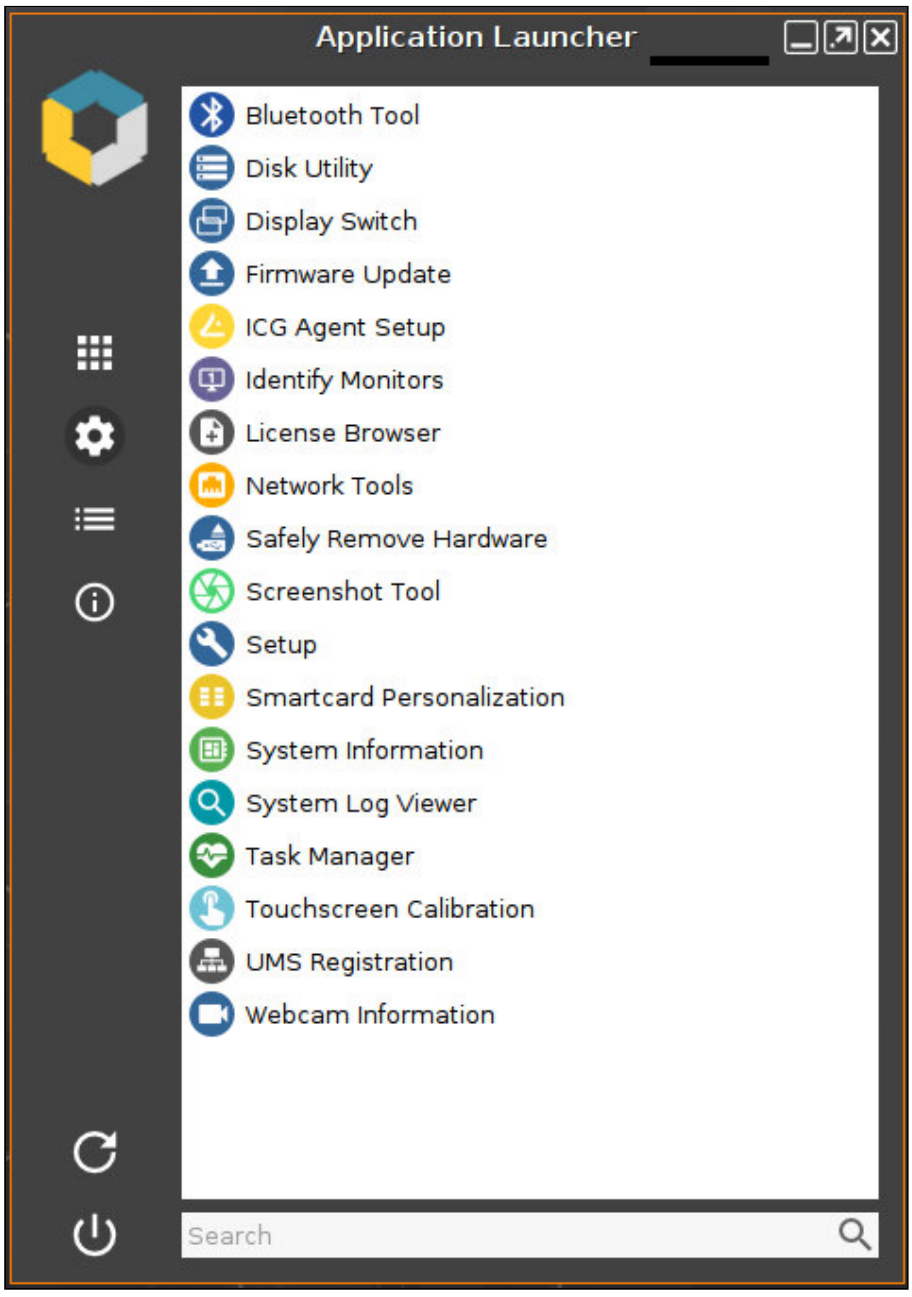
- **Sessions**: Allows you to launch sessions
- **System**: Allows you to launch system programs
- **About**: Shows all relevant system information
- **Search window**: Allows you to find sessions and functions in the start menu
- Allows you to shut down the device
- Allows you to restart the device

- Application Launcher (see page 1230)
- Sessions (see page 1232)
- System (see page 1233)
- License (see page 1234)
- About Window (see page 1235)
- Restart and Shutdown (see page 1236)

Application Launcher

To launch the **Application Launcher**, proceed as follows:

→ Click on in the Quick Start Panel or in the start menu.



The sub-areas of the Launcher provide access to:

	Listing of the Sessions (see page 1232) that have been set up
	Listing of the most important System (see page 1233)
	License (see page 1234) for the components used
	The About Window (see page 1235) with information about the system
	Restart
	Shut down
	Search field for fast access to the components

You will find information regarding the configuration under Application Launcher (see page 1740).

Sessions

All sessions created are shown in a list of applications if they are enabled for the main session page.

→ To open an application, double-click on it or click on **Run**.
Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu.
Applications can also be launched automatically and a key combination (hotkey) can be defined.
It is also possible, to build a file structure for the sessions in the application launcher. Therefor, in the setup page **Desktop Integration** of the relevant application you have to define a folder in the application launcher.

> The available options for launching a session can be defined under **Desktop Integration** in the session configuration.

System

Under **System** , you can execute various tools including the firmware updating tool with the pre-set update information.

The following tools are available:

- **Identify Monitors**: Shows the screen's number and manufacturer details.
- **Screenshot Tool**: Takes photos of the screen content.
- **Bluetooth Tool**: Starts the Bluetooth tool.
- **Firmware Update**: Carries out the update with the settings made during the setup.
- **Savely Remove Hardware**: Removes external storage devices without a risk of losing data.
- **Disk Utility**: Shows information regarding connected USB drives.
- **Network Tools**: Provides detailed information on the network connection and offers a number of problem analysis tools such as ping or traceroute.
- **Setup**: Launches the IGEL Setup.
- **System Information**: Shows information regarding hardware, the network and connected devices.
- **System Log Viewer**: Shows system log files "live" and allows you to add your own logs.
- **Task Manager**: Manages all processes.
- **Touchscreen Calibration**: Allows a connected touchscreen monitor to be calibrated.
- **UMS Registration**: Logs the device on to a UMS server (access data for the server are required).
- **Webcam Information**: Shows data relating to a connected webcam and allows the camera to be tested.

License

Under **License** , you will find information on the provision of a copy of source code, e.g. under GPL (General Public License).

About Window

In the **About** window, accessible via the icon, you will find the following data:

- **Product**: Information regarding the installed firmware
  - Copyright
  - Firmware Release Date
  - Firmware Version
  - Product ID
  - Product Name
  - Website
- **License Information**: Expiration dates of available licenses
- **Network**: Computer name, hardware address, and IP address of the device
  - Local Name
  - Default Gateway (only with valid network connection)
  - DNS Server (only with valid network connection)
  - Universal Management Suite
- **Interface** [number name]:
  - Description
  - Hardware Address
  - IP Address

If the network status changes, the details will automatically be updated. To force an update, click on .

- **Hardware**:
  - Boot Mode
  - CPU Model
  - Device Type
  - Flash Size
  - Graphic Chipset
  - Memory Size
  - Total Operating Time
  - Unit ID (equal to MAC address (UD, UDC) or serial number (UD Pocket))
- **Licensed Features**: List with all firmware features for which a license is available

You can copy individual entries via the context menu (right mouse button).

Restart and Shutdown

Within the **Application Launcher** you will find two buttons for **rebooting** or **shutting down** the device. Both actions can be disabled for the user and will then be available to the administrator only.

You can change the default action when shutting down the device using the button on the screen or the on/off button on the device itself in the setup under **System > Power Options > Shutdown**.

Setup

With the help of the setup, you can change the system configuration and session settings.

> Any changes you have made in the UMS take precedence and may no longer be able to be changed. A lock symbol before a setting indicates that it cannot be changed.

_____

- Starting the Setup (see page 1238)
- End the Setup (see page 1239)
- Setup Areas (see page 1240)
- Quick Setup (see page 1241)
- Setup Search (see page 1242)

Starting the Setup

You can open the setup in the following ways:

- Double-click in the **Application Launcher**
- or click on **Run**.
- Double-click on the desktop (if available based on the settings).
- Select **Setup** in the desktop context menu (if available based on the settings).
- Select **System >** **Setup** in the start menu.
- Click on in the Quick Start Panel.
- Launch the setup using the keyboard command [Ctrl]+[Alt]+[s], or in the Appliance Mode using [Ctrl]+[Alt]+[F2].

You can configure how the setup can be launched under **Accessories**. The options described above as well as combinations thereof are available.

End the Setup

In order to end the setup again, you have the following options:

→ Click on **Apply** if you have finished configuring a setup area and would like to save your settings without closing the setup program.

→ Click on **Cancel** if you have not made any changes and would like to abort the setup.

→ Click on **OK** to save your changes and exit the setup.

Setup Areas

The setup application comprises the following main areas:

- **Sessions**: Allows you to configure application sessions such as ICA, RDP, PowerTerm, browser and others
- **Accessories:** Allows you to configure various local tools - setup pages for the local shell (*Terminal*), sound mixer, screen keyboard (for touchscreen monitors), options for the **Application Launcher** and the setup application itself.
- **User Interface:** Allows you to configure display settings, entry devices, hotkey commands etc.
- **Network:** Allows you to configure all network settings for LAN/WLAN interfaces and the dial-up connections
- **Devices:** Allows you to configure various devices
- **Security:** Allows you to set the administrator/user passwords and user authorizations etc.
- **System:** Allows you to set various basic system parameters including the date and time, information regarding the firmware update, remote management etc.

→ Click on one of the areas to open up the relevant sub-structure.

The tree structure allows you to switch between the setup options.

Three navigation buttons are available. The buttons allow you to move back and forth between the setup pages you have visited or reach the next level up within the structure.

You will find a more detailed description of the individual setup options elsewhere. This is merely a brief overview.

Quick Setup

As administrator, you prepare the setup for the user. If you want to give the user the option of defining their own settings in certain areas of the setup, you can prepare a quick setup. A quick setup is a slimmed down version of the setup. It only displays areas the user is allowed to change.

To create a quick setup session, proceed as follows:

1. Enable the password for the administrator in IGEL Setup under **Security >** *IGEL OS Base System > IGEL OS Base System > Security Configuration in IGEL OS 12 > Password*

> If users are to be allowed to edit parts of the setup only with a password, enable the password for the setup user too.

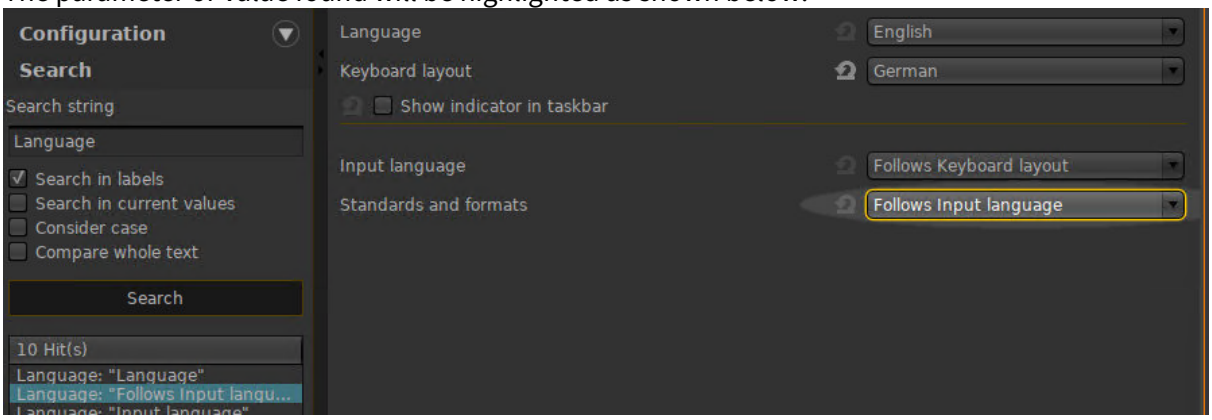
2. Under **Accessories >** Quick Settings (see page 1726), define the name and options for calling up the quick setup.
3. Under **Accessories > Quick Settings >** Setup User Permissions (see page 1729) enable those areas to which the user is to have access.

> You can set up a hotkey to start quick setup in appliance mode. Instructions for setting up the hotkey can be found under Quick Settings (see page 1726).

Setup Search

The **Search** function enables you to find parameter fields or parameter values within the setup.

1. To start a **search**, click on the button below the tree structure.
2. Enter the text to be searched for and the search details.
3. Select one of the hits.
4. Click on **Show result** and you will be taken to the relevant setup page.
   The parameter or value found will be highlighted as shown below.



Sessions

Menu path: **Sessions > Sessions Summary**

In this area, you will find an overview of all available sessions.

Add: Adds a session from the selection of available session types.

Filter: Filters sessions shown in the list according to the string of characters entered.

- Copy Session (see page 1244)
- Global Session Options (see page 1245)
- Citrix (see page 1246)
- RDP Global (see page 1310)
- RDP Session (see page 1339)
- Remote Desktop Web Access (see page 1354)
- Horizon Client Global (see page 1368)
- Horizon Client Session (see page 1399)
- Appliance Mode (see page 1413)
- AppliDis (see page 1424)
- Evidian AuthMgr (see page 1433)
- NoMachine NX Client (see page 1445)
- X Sessions (see page 1466)
- Parallels Client Global (see page 1474)
- Parallels Client Session (see page 1480)
- PowerTerm Selection in IGEL OS (see page 1493)
- PowerTerm Session (see page 1494)
- IBM iAccess Client (see page 1498)
- ThinLinc Global (see page 1521)
- ThinLinc Session (see page 1528)
- SSH Session (see page 1542)
- VNC Viewer Sessions (see page 1550)
- Firefox Browser Global Settings in IGEL OS (see page 1560)
- Firefox Browser Session (see page 1589)
- Chromium Browser Global Session in IGEL OS (see page 1597)
- Chromium Sessions (see page 1616)
- Media Player Global (see page 1623)
- Media Player Session (see page 1628)
- VoIP Client (see page 1636)
- PCoIP Sessions with the HP Anyware Client in IGEL OS (see page 1651)
- AVD Global (see page 1658)
- AVD Session in IGEL OS (see page 1664)
- Amazon WorkSpaces (see page 1681)
- deskMate Session (see page 1691)
- Unified Communications (see page 1700)

Copy Session

You can copy a session in the setup. The copy of the session has all the properties of the original session and is located in the same folder as the original session.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. In the **[Session Type] Sessions** area, click . Alternative: Open the context menu of the session by right-click and select **Copy**.
   A copy of the session will be created.

Global Session Options

Menu path: **Setup > Sessions > Global Session Options**

- **Network notification on session start**: If when launching sessions no network is available, a notification will be shown.
  - ☑ Network notification is enabled (default)
  - ☐ Network notification is disabled
- **Notification delay**: Time in seconds after which the notification is shown. (default: 15)
  Possible values:
  - 1 ... 120 seconds
- **Delay session start at boot time to apply new UMS settings**: If new settings were made in the UMS, the device may receive them during the boot procedure.
  - ☑ The session start will be delayed until the settings have been transferred or the time limit has been exceeded.

- **Timeout**: Delay in seconds. (default: 10)
  Possible values:
  - 1 ... 120 seconds

Citrix

Menu path: **Setup > Sessions > Citrix**

- Citrix Client Selection in IGEL OS (see page 1247)
- Citrix Global (see page 1248)
- Citrix Self-Service (see page 1287)
- Citrix StoreFront (see page 1294)

Citrix Client Selection in IGEL OS

When configuring Citrix sessions in IGEL OS, you can specify which version of Citrix Workspace App will be used for all StoreFront connections.

Menu path: **Sessions > Citrix > Citrix Client Selection**

Citrix client version

Selects the Citrix client version to be used for Citrix sessions.

For the included Citrix client versions, see the "Component Versions" section in the IGEL OS Release Notes (see page 2282).

⚠ When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

ℹ After changing the **Citrix client version**, check the settings under:

- **Citrix > Citrix StoreFront > Server**
- **Citrix > Citrix StoreFront > Login**

Citrix Global

Menu path: **Sessions > Citrix > Citrix Global**

This section describes global Citrix settings which apply for all Citrix sessions. Most of these settings can be either carried over or overwritten in the individual sessions.

> Please note that a number of configuration options depend on the version of the Citrix Receiver selected.

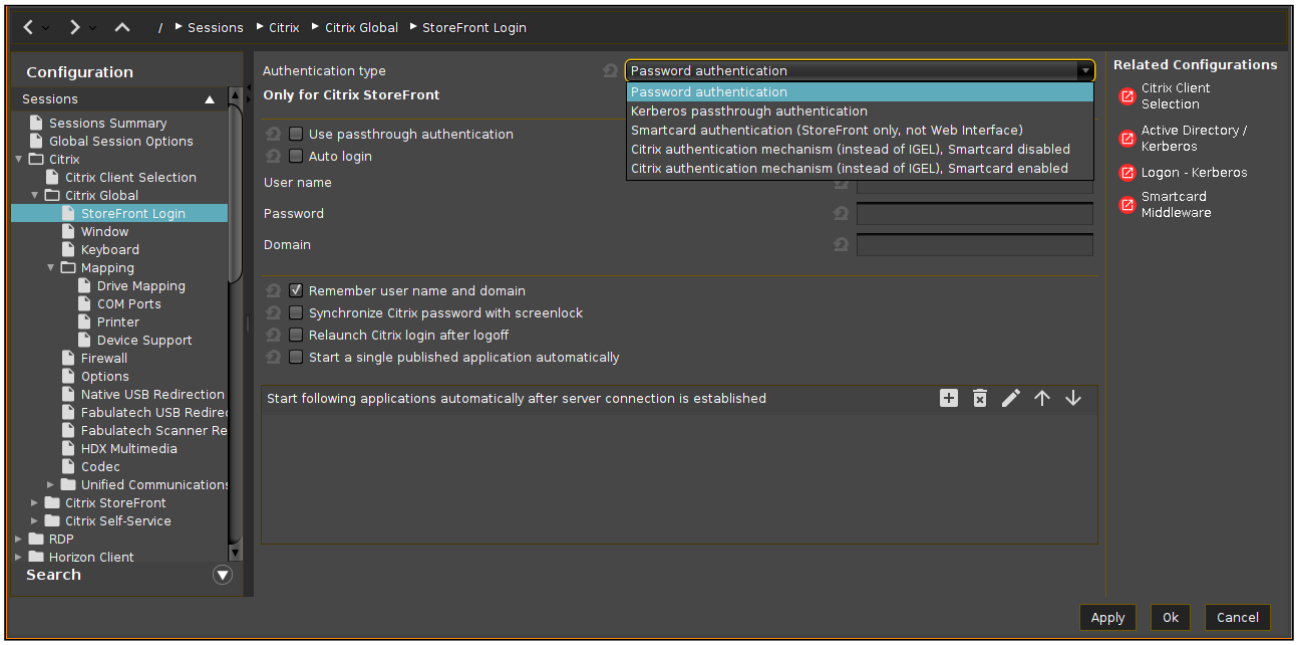
If there are problems with the logging in to a Citrix Storefront session because of the expired password, see Troubleshooting: Login Failed because of the Expired AD Password (see page 418).

- StoreFront Login (see page 1249)
- Window (see page 1252)
- Citrix Global - Keyboard (see page 1254)
- Mapping (see page 1255)
- Firewall (see page 1263)
- Options for an IGEL OS Citrix Session (see page 1264)
- Native USB Redirection for Citrix Sessions in IGEL OS (see page 1267)
- Fabulatech USB Redirection for Citrix in IGEL OS (see page 1271)
- Fabulatech Scanner Redirection (see page 1275)
- HDX Multimedia Settings for an IGEL OS Citrix Session (see page 1276)
- Codec (see page 1279)
- Unified Communications Settings for Citrix Sessions in IGEL OS (see page 1281)

StoreFront Login

In this area, you can globally configure login options for Citrix sessions in IGEL OS. For individual sessions, login options can be defined under **Sessions > Citrix > Citrix StoreFront > Login**.

Menu path: **Sessions > Citrix > Citrix Global > StoreFront Login**



Authentication type

Depending on the Citrix client version, the following types are available:

- **Password authentication**: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- **Kerberos passthrough authentication**: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device, see Active Directory/Kerberos[149].
- **Smartcard authentication (StoreFront only, not Web Interface)**: Authentication via smartcard will only work with StoreFront, not with Web Interface. For configuration details, see Citrix StoreFront (see page 795).
- **Citrix authentication mechanism (instead of IGEL), Smartcard disabled**: Recommended for cloud environments and Citrix NetScaler.
- **Citrix authentication mechanism (instead of IGEL), Smartcard enabled**: Recommended for cloud environments and Citrix NetScaler.

If you have set an authentication type with smartcard, select the type of card on the Smartcard (see page 2024) page. You may find it also helpful to read the how-to Smartcard Authentication in IGEL OS (see page 791).

149. https://kb.igel.com/en/igel-os/11.10.270/active-directory-kerberos

Depending on the selected authentication type, the following options are available:

Use passthrough authentication

- Cached login data are used for listing and starting applications. For more information, see Passthrough Authentication (see page 1165).
- No passthrough authentication. (Default)

Auto login

- Uses the login data preset on this page when connecting to the server.
- Do not log in automatically. (Default)

User name

Can only be filled in with password authentication.

Password

Can only be filled in with password authentication.

> ⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Can only be filled in with password authentication.

Remember username and domain

- Saves the user name and domain from the last login. (Default)
- The user name and domain will not be saved.

Synchronize Citrix password with screenlock

- Synchronizes the screenlock password (see page 1849) with that of the Citrix application. You can use this option if you want, for example, to use the user's AD password to unlock the screen.
- No synchronization (Default)

Relaunch Citrix login after logoff

- Automatically shows the login dialog again after logging out.
- Does not start the login procedure again. (Default)

Start a single published application automatically

This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

- ☑ The published application is started when the user has logged in.
- ☐ The published application is not started on login. (Default)

Start following applications automatically after server connection is established

A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the **Add** dialog, give the name of the application.

> Application names are case-sensitive.
> You can also enter part of the name followed by an asterisk (*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

> After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

> **App Protection Feature for the Citrix Workspace App**
> To strengthen the security of your Citrix environment, you can use the app protection feature in IGEL OS 11.08.200 or higher. It provides anti-keylogging and anti-screen-capturing functionalities. For more information on this feature and the required server-side settings, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/secure/app-protection.html .
> To activate the feature on IGEL OS, go to **System > Registry** and enable the Citrix App Protection registry key: `ica.appprotection`
> The feature is supported for Citrix Workspace app version 22.07 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 1247).

Window

Menu path: **Sessions > Citrix > Citrix Global > Window**

Under **Window**, you can configure the following settings:

Multimonitor full-screen mode

Possible options:

- Restrict full-screen session to one monitor
- Expand full-screen session across all monitors
- Expand the session over a self-selected number of monitors

Select this setting if you do not want to span the session across all monitors, but only across a certain number of monitors. Under **Monitor selection**, specify the relevant monitors.

StoreFront start monitor: This setting is available if you selected **Restrict full-screen session to one monitor** for **Multimonitor full-screen mode**.

Monitor selection: This setting is available if you selected **Expand the session over a self-selected number of monitors** for **Multimonitor full-screen mode**.

Example

Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert `2,3,4` or `2,4`.

Embed systray icons into window manager taskbar: Specifies if an application icon is shown in the local taskbar.

- On
- Off

Citrix connection bar

Possible options:

- Off
- On
- Factory default is "*": The Citrix connection bar is enabled or disabled by the server.

Control bar for Citrix sessions

The in-session control bar is present in Citrix sessions. For details, see In-Session Control Bar (see page 1872).

Screen Pinning

You can run multiple Citrix desktop sessions simultaneously on different monitors. In this section, you assign one or more monitors to each session.

If a desktop session is not assigned to monitors, the default settings in the general section of this Setup page apply to it.

⚠ This feature works only with desktop sessions; published applications cannot be controlled.

→ For each Citrix desktop session, click + to configure a corresponding monitor setup. The following parameters must be set:

Citrix session name: Name of the desktop session as displayed in the browser, desktop, or Self-Service. The session name is provided by the server. The wildcards "*" (any number of any characters) and "?" (any single character) can be used.

> **Example**
> With three desktop sessions that are named "Desktop2019", "DesktopW10", and "DesktopD10", you can assign settings like so, for instance:
> "Desktop*": The settings are assigned to all three desktops.
> "Desktop?10": The settings are assigned to "DesktopW10" and "DesktopD10".
> "DesktopW10": The settings are assigned to "DesktopW10".

Multimonitor full-screen mode: Defines how the desktop sessions are distributed over the monitors. For the arrangement of the monitors and their numbering, go to **User Interface > Display** (see Display Settings in IGEL OS (see page 1889)).

Possible options:

- Restrict full-screen session to one monitor: The desktop session is displayed on the monitor that is selected under **Desktop session start monitor**.
- Expand full-screen session across all monitors: The desktop session uses all monitors.
- Expand the session over a self-selected number of monitors: The monitors can be selected with **Monitor selection**.

Desktop session start monitor: The desktop session is displayed on the selected monitor.

Monitor selection: Selects one or several monitors on which this desktop session is to be displayed. This setting is available if you selected **Expand the session over a self-selected number of monitors**.

> **Example**
> Sample configuration: If you have 4 monitors and want to expand your session across monitor 2, 3, and 4 you have to insert `2,3,4` or `2,4`.

Citrix Global - Keyboard

Menu path: **Setup > Sessions > Citrix > Citrix Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In *Windows* for example, the key combination [Alt]+[F4] closes the current window. This key combination works in ICA sessions too. All key combinations with [Alt] which are not used by the *X Window Manager* function in the familiar way during an ICA session.

The following settings can be configured:

- **Keyboard layout**
  - default: The local keyboard setting will be used in ICA too.
  - Other Countries
- **Input language**:
  - default: The local keyboard setting will be used in ICA too.
  - Other Countries
- **Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions**
  - ☑ The user can use the combination [Ctrl]+[Alt]+[End]to change the password instead of [Ctrl] +[Alt]+[Del]when the corresponding prompt message appears.
  - ☐ No mapping (default)

- **Keyboard mapping file**: You can choose between two alternatives.
  - generic: Sends language-independent scancodes from the keyboard to the computer.
  - Linux: Sends language-specific scancodes.

  The key alternatives are restricted to [Ctrl]+[Shift]+[Key] by default. However, you can change the settings by clicking on the Hotkey Modifier drop-down field and/or hotkey symbol for the relevant key combination.
  - Possible keys: [F1] – [F12] , [Plus], [Minus], [Tab]
  - Possible modifiers: [Shift], [Ctrl], [Alt], [Alt]+[Ctrl], [Alt]+[Shift], [Ctrl]+[Shift]
  - **Toggle SpeedScreen**: Key combination for switching *SpeedScreen* (client reacts immediately to keyboard inputs or mouse clicks) on and off alternately.

Mapping

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in ICA sessions.

_____

- Drive Mapping (Citrix) (see page 1256)
- COM Ports (see page 1258)
- Printer (see page 1260)
- Device Support (see page 1261)

Drive Mapping (Citrix)

Menu path: **Setup > Sessions > Citrix > Citrix Global> Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to you during *ICA* sessions on *Citrix* servers.

In this area, you can specify which drives and paths are mapped during the logon. This applies for all *ICA* sessions.

- **Drive mapping**:
  ☑ *Citrix* servers can access the device's local drives. (default)

To manage the **Drive Mapping** list, proceed as follows:

→ Click on + to create a new entry.

→ Click on to remove the selected entry.

→ Click on to edit the selected entry.

→ Click on to copy the selected entry.

Local (USB) devices which are to be used for drive mapping purposes must first be set up as storage devices. For more information, see Storage Hotplug (see page 1969).

Before you unplug a hotplug storage device from the device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see In-Session Control Bar (see page 1872).
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Add Drive Mapping

- **Enable**:
  ☑ The drive will be made available in the session.
- **Drive to map**: DOS-style drive letters on the Citrix Server.

If the drive letter you have selected is no longer available on the Citrix server, the specified directory or local drive will be given the next free letter during the logon.

- **Local drive path**: Unix path name of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field.

- **Read access**
  Possible options:
  - yes
  - no
  - ask user: The read access right is queried when each ICA session is accessed for the first time.
- **Write access**
  Possible options:
  - yes
  - no
  - ask user: The write access right is queried when each ICA session is accessed for the first time.

COM Ports

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > COM Ports**

- **COM port mapping**
  Enables the mapping of serial devices connected to the device to the serial interfaces of the Citrix server. (Default)

If you would like to use signature pads, you must enable them beforehand under **User Interface > Input >** Signature Pad (see page 1883).

To manage the list of **COM port devices**, proceed as follows:

→ Click + to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Add

- **COM port device**: Allows you to select from all serial and USB interfaces on the device.
  Possible values:
  - "COM 1"
  - "COM 2"
  - "COM 3"
  - "COM 4"
  - "USB COM 1": For UD3-LX60 devices (mainboard: *Hardware > Hardware > UD3 > M350C > Disassembly Guide of UD3 M350C > Manual of UD3 M350C*), this port must be used instead of "COM 1".
  - "USB COM 2"
  - "USB COM 3"
  - "USB COM 4"
- **Detect Devices...**: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:
  - (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion.
    Example: `/dev/ttyUSB0`
  - (BY PORT) [device designation]: According to USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`

- (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`
- (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: `/dev/ttyVST0`

If your device has an additional multiport PCI card, more than 2 connections may be available.

Printer

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

- **Client printer mapping**: With this function, the locally connected device printer is made available for your ICA sessions, provided that it was not disabled on the server side.
- **Set another default printer**:
  - ☑ Allows you to specify a default printer for the client which differs from the one defined in the printer setup.
  - ☐ Do not set another default printer. (default)
- **Default printer**: Print queues used on the device to specify the default printer for the session. `lp` is the locally configured default printer.
- **Default printer driver:** Windows driver name for the printer which is automatically set up. Enter one of the universal drivers or your own driver name here.
  Possible values:
  - Citrix PCL4 universal driver (old)
  - Citrix Universal Printer
  - Citrix XPS Universal Printer
  - User entry

See also https://support.citrix.com/article/CTX140208.

The printers must be set up on the **Devices > Printers > CUPS > Printer** page and must be enabled there for mapping in ICA sessions, see ICA sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.

Device Support

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Device Support**

In this area, you can enable virtual ICA channels for communicating with various devices connected to the device.

The devices supported are listed in the IGEL Third Party Hardware Database[150].

DriveLock channel: The virtual DriveLock channel is implemented on the device. The channel must also be installed on the Citrix server.
DriveLock can read hardware data from local USB devices and transfer these data to the Citrix server with the help of the Virtual ICA Channel Extension. From IGEL Linux *Version 10.03.500*, this is also possible with SATA devices. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account.

Important information regarding DriveLock can be found in the FAQ Using DriveLock with IGEL Devices (see page 1091).

- ☑ A virtual channel for DriveLock is enabled.
- ☐ No virtual channel for DriveLock is enabled. (Default)

deviceTRUST channel

- ☑ A virtual channel for deviceTRUST is enabled.
- ☐ No virtual channel for deviceTRUST is enabled. (Default)

Crossmatch DigitalPersona fingerprint channel

- ☑ A virtual channel for Crossmatch DigitalPersona is enabled.
- ☐ No virtual channel for Crossmatch DigitalPersona is enabled. (Default)

Diktamen Channel for Dictation

- ☑ A virtual channel for Diktamen is enabled.
- ☐ No virtual channel for Diktamen is enabled. (Default)

Grundig MMC-Kanal for dictation with Grundig devices

- ☑ A virtual channel for communication with Grundig devices is enabled.
- ☐ No virtual channel for communication with Grundig devices is enabled. (Default)

Nuance channel for dictation: Virtual audio channel for dictation devices. Dictation microphones from Grundig, Philips and Olympus are supported.

> This channel is only responsible for audio transmission. The channel for dictation device operating elements is manufacturer-specific and must be enabled separately.

- ☑ The Nuance audio channel is enabled.
- ☐ The Nuance audio channel is not enabled. (Default)

150. https://www.igel.com/linux-3rd-party-hardware-database/

Olympus Channel for dictation

- ☑ A virtual channel for communication with Olympus devices is enabled.
- ☐ No virtual channel for communication with Olympus devices is enabled. (Default)

signotec signature pad channel

- ☑ A virtual channel for communication with signotec signature pads is enabled.
- ☐ No virtual channel for communication with signotec signature pads is enabled. (Default)

StepOver signature pad channel

- ☑ A virtual channel for communication with StepOver signature pads is enabled.
- ☐ No virtual channel for communication with StepOver signature pads is enabled. (Default)

Philips speech channel for dictation

- ☑ A virtual channel for communication with Philips dictation devices is enabled.
- ☐ No virtual channel for communication with Philips dictation devices is enabled. (Default)

DPM server drive: Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

> The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Storage Hotplug (see page 1969) and Drive mapping (see page 1256).

SpeechAir server drive: Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server. (Default: S)

> The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Storage Hotplug (see page 1969) and Drive mapping (see page 1256).

Kofax SPVC signature pad channel

- ☑ The Kofax SPVC signature pad channel is enabled.
- ☐ The Kofax SPVC signature pad channel is not enabled. (Default)

Lakeside SysTrack channel

- ☑ The Lakeside SysTrack channel is enabled.
- ☐ The Lakeside SysTrack channel is not enabled. (Default)

Firewall

Menu path: **Setup > Sessions > Citrix > Citrix Global > Firewall**

In this area, you can configure the following firewall settings:

Alternative address

- ☑ Allows you to use a proxy or Secure Gateway server as an alternative address for connections via a firewall.
- ☐ Do not use an alternative address (default)

SOCKS / Secure Proxy

Proxy type

- None (Direct Connection)
- SOCKS: A proxy that uses the SOCKS protocol
- Secure (HTTPS): An HTTP proxy with TLS/SSL encryption.

Proxy server: Name or IP address of the proxy server

Proxy port: TCP port of the proxy server (default: 1080)

Secure Gateway (Relay Mode)

Secure gateway address: If you would like to use a Citrix Secure Gateway in relay mode, you must give the full DNS name – the IP address is not sufficient in this case.

Port: TCP port of the gateway (default: 443)

Options for an IGEL OS Citrix Session

In this area, you can optimize the general behavior and performance for Citrix sessions in IGEL OS.

Menu path: **Sessions > Citrix > Citrix Global > Options**

Use server redraw

- ☑ The Citrix server is responsible for refreshing the screen content.
- ☐ Do not use server redraw.*

Disable Windows alert sounds

- ☑ Switches off the Windows warning sounds.
- ☐ The warning sounds remain enabled.*

Backing store

- ☑ The X Server temporarily stores hidden window content.
- ☐ Window content is not stored.*

Deferred screen update mode

- ☑ Enables delayed updates from the local video buffer on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.
- ☐ No delayed update.*

Cache size in kB

Default: 1024

Minimum bitmap size in bytes

The minimum size of the bitmap files that are to be stored in the cache. (Default: 1024)

Persistent cache path

The directory where the files are to be stored locally. (Default: $ICAROOT/cache)

Do not make the cache too big; otherwise, you run the risk of the device having too little storage space for its own system and other applications. You may have no alternative but to equip your device with additional RAM.

Scrolling control

Depending on the speed of your network or the response time of your server, there may be a delay between you letting go of the mouse button on a scroll bar and the scrolling actually stopping (e.g. when using Excel). Changing this value may help. (Default: 100)

Audio bandwidth limit in StoreFront sessions

- **High***
- **Medium**
- **Low**

Higher quality requires more network and computing resources.

Auto reconnect

- Automatically attempt to reconnect if the connection is terminated. *
- Do not attempt to reconnect.

Maximum retries

Default: 3

Delay in seconds before reconnecting

Default: 30

Allow Kerberos passthrough authentication in StoreFront sessions

- Kerberos passthrough authentication is allowed.*
- Kerberos passthrough authentication is not allowed.

This point concerns Citrix XenApp in Version 6.5 and older.

CGP address

- **Use server address**
- **Text input**
- **disabled***

Multistream sessions

- Support multistream ICA.
- Do not support multistream ICA.*

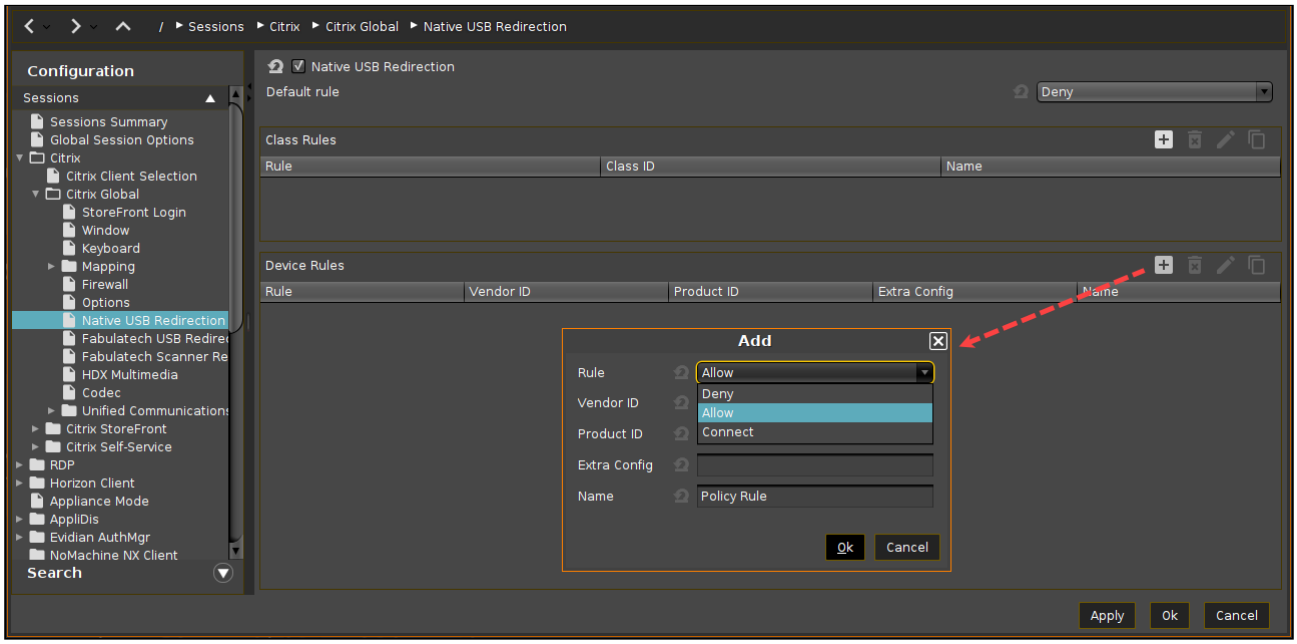
* IGEL OS system default

Native USB Redirection for Citrix Sessions in IGEL OS

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under USB Access Control (see page 2010). See also How to Configure Citrix Native USB Redirection (see page 402).

An overview and best-practice recommendations for the use of webcams can be found under Webcam Redirection and Optimization in IGEL OS (see page 1034).

Menu path: **Sessions > Citrix > Citrix Global > Native USB Redirection**



Native USB redirection

- ☑ Native USB redirection is enabled globally.
- ☐ Native USB redirection is disabled. (Default)

Enable either **native USB redirection** or **Fabulatech USB redirection**, but not both together.

Disable USB redirection if you use DriveLock. Further information can be found under Using DriveLock with IGEL Devices (see page 1091).

Default rule

This rule will apply if no special rule was configured for a class or a device.

- **Deny** (Default)
- **Allow**

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

→ Click to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Add class rule:

Rule:

- **Deny**: No automatic redirect of a device
- **Allow**: Automatic redirect of a device only after a session starts
- **Connect**: Automatic redirect of a device when a session starts

In the case of **Connect** or **Allow**, the device is automatically redirected when it is unplugged and plugged in during a session, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb .

Class ID: Selection list

Sub-class ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add device rule:

Rule:

- **Deny**: No automatic redirect of a device
- **Allow**: Automatic redirect of a device only after a session starts
- **Connect**: Automatic redirect of a device when a session starts

In the case of **Connect** or **Allow**, the device is automatically redirected when it is unplugged and plugged in during a session, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb .

If you have problems with device redirection after the update to Citrix Workspace App 22.07 or higher, try to change the rule to **Connect**.

Composite USB Redirection
In IGEL OS 11.08.200 and higher, you can configure composite USB redirection which is needed for multifunctional devices that use different interfaces. Examples of such composite USB devices are dictation microphones or Bloomberg keyboards which comprise a keyboard, fingerprint reader, an audio device, USB hub, etc.

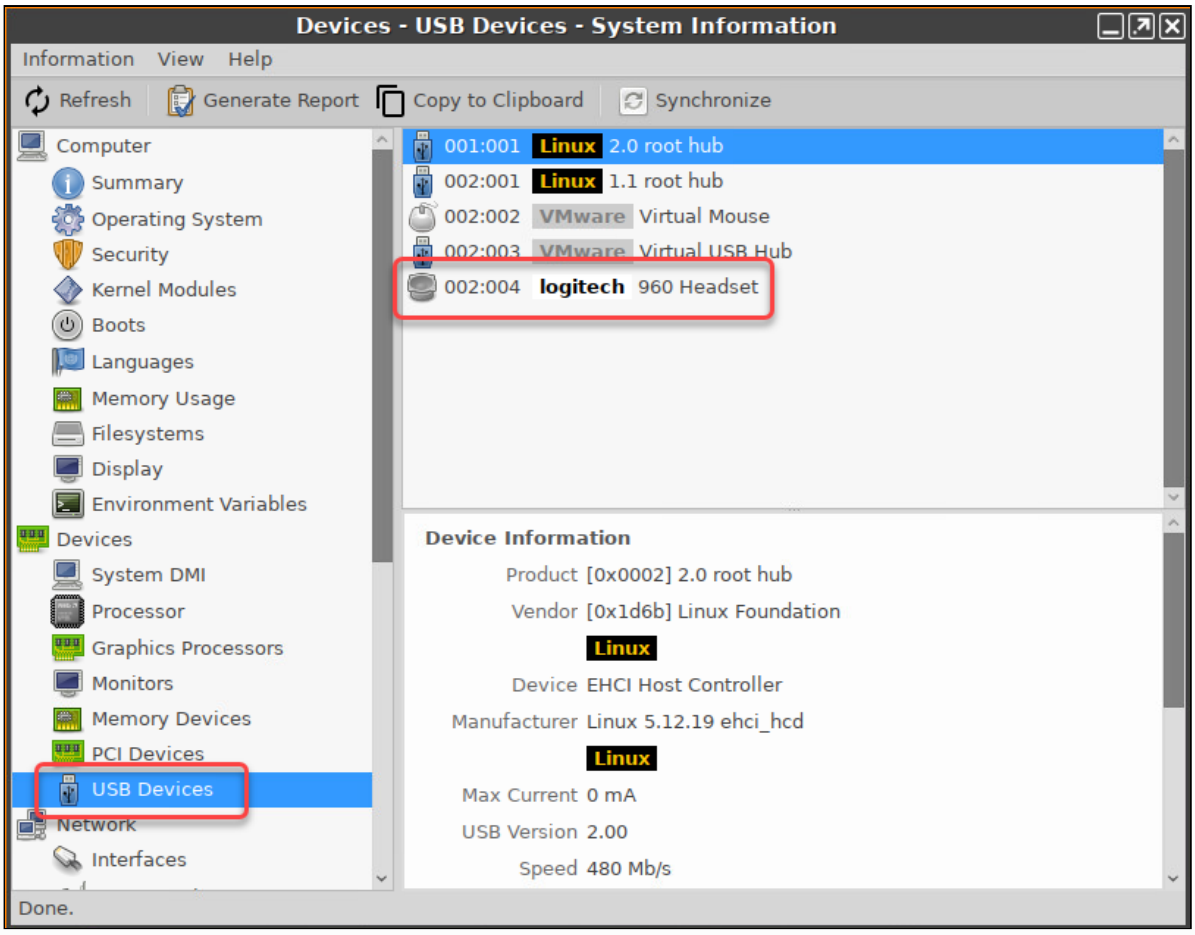
To redirect the entire composite device to the session, only **Vendor ID** (`vid`) and **Product ID** (`pid`) must be added.
If you need to split the composite device and redirect only the child interfaces that use a generic USB channel, you must also add filter parameters `split` and `intf` under **Extra Config**. For more information on composite USB redirection and sample device rules, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb .

Vendor ID: Hexadecimal manufacturer number

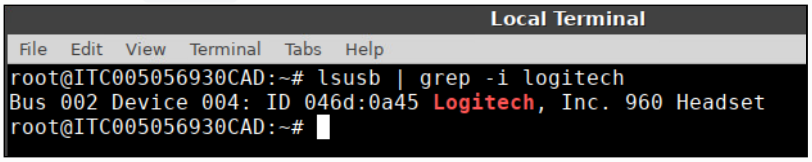
Product ID: Hexadecimal device number

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.
Example for `lsusb`:



Extra Config: Allows to add `split` and `intf` parameters to split the **composite USB device**.
Example:
`CONNECT: vid=047F pid=C039 split=1 intf=03` # Allow HID device and connect automatically.

Name: Free text entry

Fabulatech USB Redirection for Citrix in IGEL OS

Redirection for USB devices can be allowed or denied during an RDP session using rules and sub-rules for specific devices or device classes. The use of rules is described in detail under USB Access Control (see page 2010).

Important Notes

- For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see http://www.usb-over-network.com/partners/igel/. For details on the configuration, see https://www.usb-over-network.com/partners/igel/usb-for-remote-desktop-docs.html. Please note that licenses must be purchased from Fabulatech to enable this functionality.
- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech USB Redirection**

Fabulatech USB Redirection

- ☑ Fabulatech USB Redirection is enabled for all Citrix sessions.
- ☐ Fabulatech USB redirection is disabled. (Default)

Default rule

This rule will apply if no special rule was configured for a class or a device.
Possible options:

- **Deny** (Default)
- **Allow**

Tip
To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

→ Click to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Class rule properties:

Rule:

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- Deny: Devices that have the properties defined here are not redirected.

Class ID: Device class

Subclass ID: Subclass relating to the specified device class

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts.
- ☐ The USB device is no longer shown immediately after the system is booted. (Default)

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- ☑ The USB device may be removed from the system (endpoint device).
- ☐ The USB device may not be removed. (Default)

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated.
- ☐ The device will be reset after the connection with the session has been terminated. (Default)

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- **Allow** (Default)
- **Deny**

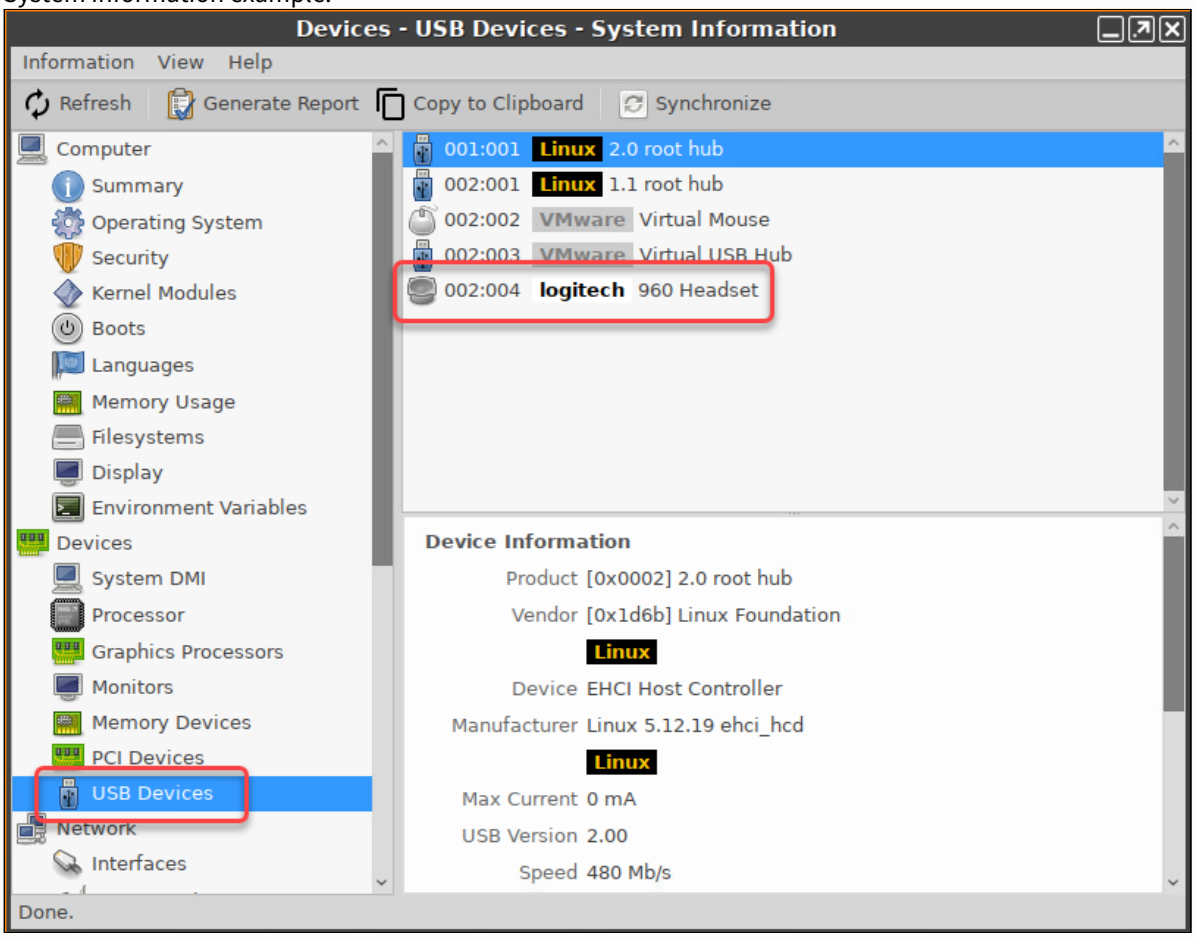
Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

Getting USB Device Information

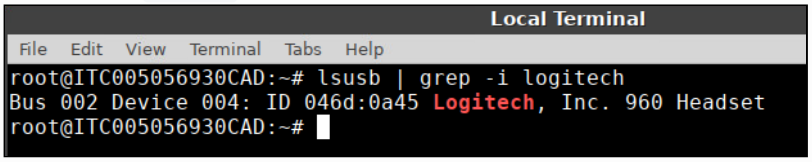
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name: Free text entry

Override serial: Serial number that will appear in the session.

Override name: Device name that will appear in the session.

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts. (Default)
- ☐ The USB device is no longer shown immediately after the system is booted.

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- ☑ The USB device may be removed from the system (endpoint device). (Default)
- ☐ The USB device may not be removed.

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated. (Default)
- ☐ The device will be reset after the connection with the session has been terminated.

Fabulatech Scanner Redirection

Menu path: **Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during a Citrix session.

Fabulatech Scanner for Remote Desktop

- ☑ Fabulatech Scanner for Remote Desktop is enabled.

For more information, see Citrix Fabulatech Scanner Redirection in IGEL OS (see page 404) .

HDX Multimedia Settings for an IGEL OS Citrix Session

You can configure HDX multimedia redirection for Citrix sessions in IGEL OS to improve the playback of audio and video content during the session.

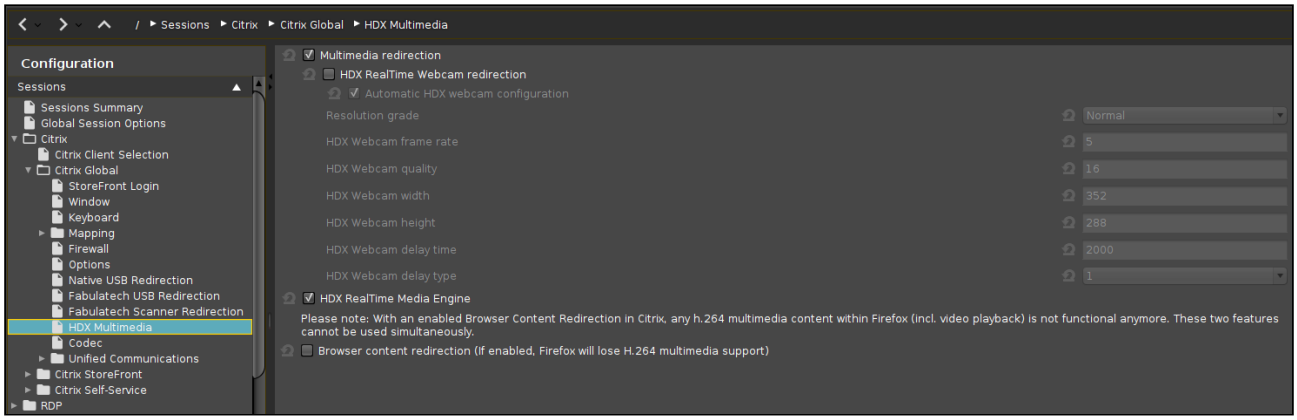
Hardware acceleration for multimedia playback is available on specific devices. For further information, see Hardware Video Acceleration on IGEL OS (see page 1180).

See also an overview and best-practice recommendations for the use of webcams under Webcam Redirection and Optimization in IGEL OS (see page 1034).

⚠ When you use Citrix through Chromium, HDX redirection only works if Chromium uses the same Gstreamer version as Citrix. By default, Chromium uses a different Gstreamer version, so you need to align the versions used by configuring the following registry keys under **System > Registry**:

- Set **multimedia.gstreamer.version** to **1.x**
- Set **sessions.chromium%.gstreamer_version** to **1.0**

Menu path: **Sessions > Citrix > Citrix Global > HDX Multimedia**



Multimedia redirection

- ☑ Multimedia data are sent to the device and decoded there.*
- ☐ Multimedia data are decoded on the server.

HDX RealTime Webcam redirection

- ☑ Redirection is enabled.
- ☐ Redirection is disabled.*

Automatic HDX webcam configuration

- ☑ The endpoint device detects the characteristics of the webcam and derives 6 different quality levels from these characteristics. The user can choose a quality level with the **Resolution grade** parameter.*
- ☐ The webcam must be configured manually using **HDX Webcam frame rate** and the subsequent parameters. For information on how to determine the capabilities of the webcam, see Using Webcam Information (see page 1824).

Resolution grade

Possible options:

- **Very low**
- **Low**
- **Normal***
- **High**
- **Very high**
- **Best**: The highest resolution that is possible while maintaining a fluent video replay

HDX Webcam frame rate

The frame rate that is requested from the webcam. (Default: 5)

HDX Webcam quality

The image quality requested from the webcam. Range: 1-63. (Default: 16)

HDX Webcam width

The image width requested from the webcam. (Default: 352)

HDX Webcam height

The image height requested from the webcam. (Default: 288)

HDX Webcam delay time

Time to wait before the webcam is opened, in milliseconds. (Default: 2000)

HDX Webcam delay type

Possible options:

- **0**: No delay
- **1***: If the time interval since the last closing of the webcam is less than the defined delay time (**HDX Webcam delay time**), the delay length is the remaining time.
- **2**: The delay time is as defined by **HDX Webcam delay time**.

HDX RealTime Media Engine

- ☑ The HDX RealTime Media Engine is enabled and significantly improves the performance of Lync / Skype for Business.*
- ☐ The HDX RealTime Media Engine is not used.

Browser content redirection (If enabled, Firefox will lose H.264 multimedia support)

Please note: With an enabled **Browser content redirection** in Citrix, any H.264 multimedia content within Firefox (incl. video playback) is not functional anymore. These two features cannot be used simultaneously.

- [x] The browser content is redirected from the server to the device, e.g. to reduce the load on the server. This setting has an effect on the hardware video acceleration with Chromium or Firefox; see How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices? (see page 566)
- [ ] Browser content redirection is disabled.*

*IGEL OS system default

Codec

Menu path: **Setup > Sessions > Citrix > Citrix Global > Codec**

- **Graphical codec**: Decoding method for the transferred screen content
  - Automatic: Automatically selects the appropriate codec according to the performance of the hardware.
  - H.264 Deep Compression Codec:
    - High image quality is possible, with lower network load
    - Without available hardware acceleration it is very CPU intensive.

    > At the Citrix Server following policies must be set:
    > - **Use video codec for compression** must be enabled.
    > - **For the entire screen**: Text tracking should be enabled if bandwidth is not a problem to increase readability in Office applications
    > - **For actively changing regions**: Citrix Receiver 13.6+ required, otherwise JPEG fallback will be loaded
    > - **Use video codec when preferred**: If **For actively changing regions** is selected by Citrix, a Citrix receiver 13.6+ must be activated, otherwise JPEG fallback is loaded.

  - JPEG:
    - High image quality possible, with high network load
    - Moderate CPU load

Additional parameters for H.264 Deep Compression Codec

These parameters are relevant if **Automatic** or **H.264 Deep Compression Codec** is selected.

- **Accelerated H.264 Deep Compression Codec**
  - ☑ Enables hardware-accelerated decoding with H.264, which reduces CPU load.
  - ☐ Uses the software implementation of H.264 and results in a greater CPU load. (default)

  For more information, read the How to Set Up Citrix Sessions with Hardware-Accelerated H.264 Deep Compression Codec (see page 428) How-To.

Following options are available in combination with H.264 Deep Compression Codec:

- **Text tracking**:
  - ☑ Loss-free depiction of texts (default)
    Text is displayed sharper, especially if "Visual Quality" is set to Low/Medium. Recommended for office applications, but requires a higher available bandwidth. With bad connection and EDT over UDP it can lead to missing text parts.
- **Small frames feature**:
  - ☑ Pixel-perfect depiction of lines etc. (default)
    This feature allows efficient processing when only a small part of the screen changes over time (for example, when a cursor flashes on an otherwise stable background).

Additional parameters for JPEG

These parameters are relevant if **JPEG** is selected.

- **JPEG direct-to-screen decoding**
  - ☑ Decodes image tiles directly without using a bitmap cache.
  - ☐ No JPEG direct-to-screen decoding (default)
- **JPEG batch decoding**
  - ☑ Enables batch processing and delayed XSync. (default)

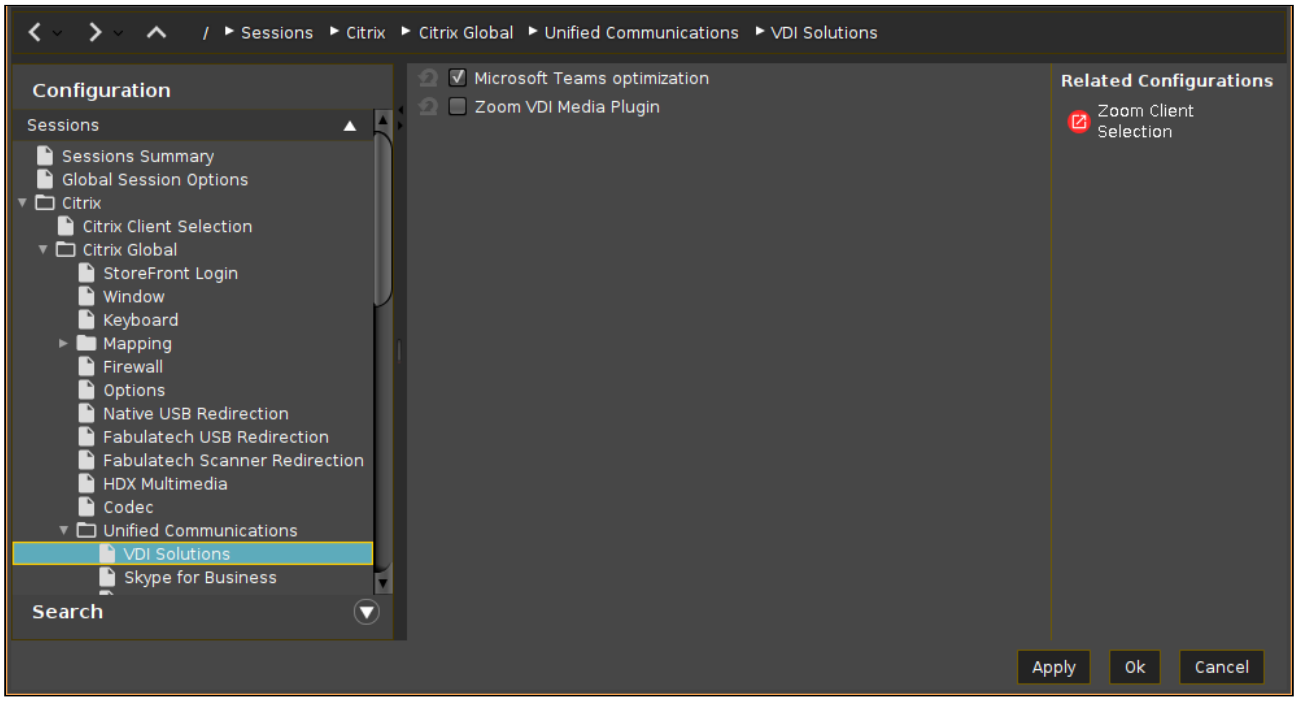
Unified Communications Settings for Citrix Sessions in IGEL OS

This article shows you how to use the Citrix session-related unified communications settings in IGEL OS. It is necessary to set some additional parameters in IGEL OS to leverage the Citrix-related multimedia enhancements. These parameters and their functions are explained below.

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications**

VDI Solutions

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**



Microsoft Teams optimization

Server and Network Requirements
Microsoft Teams optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.
For more information, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html.

- [x] The audio and video streams for Microsoft Teams are redirected to the endpoint devices. Audio and video data are not processed by the server.*
- [ ] The audio and video streams for Microsoft Teams are not redirected.

Dynamic e911 Support

IGEL OS 11.08.200 and higher supports dynamic emergency calling with MS Teams for Citrix sessions. When Microsoft Calling Plans, Operator Connect, and Direct Routing are used, the feature allows you to configure and route emergency calls like 999, 911, etc. and to notify security staff. The notification is provided based on the current location of the Citrix Workspace app running on the endpoint device. For more information on dynamic emergency calling in Citrix and the required server-side settings, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-phone-system.
To enable dynamic emergency calling in IGEL OS, go to **System > Registry** and activate the following registry key: `ica.emergencycalling`
The feature is supported for Citrix Workspace app version 21.12 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 1247).

Zoom VDI Media Plugin

Server and Network Requirements
Zoom optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.
For more information, see https://support.zoom.us/hc/en-us/articles/201362163-Mass-Installation-and-Configuration-for-Windows.

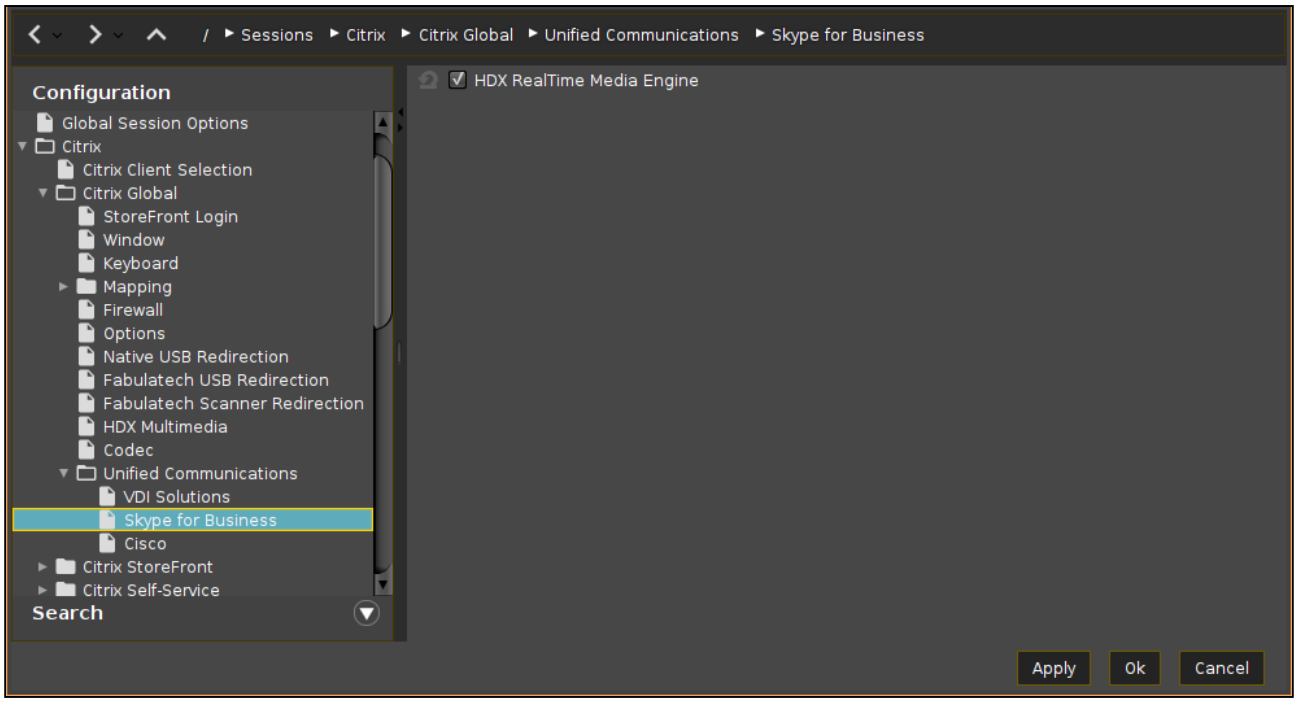
- [x] The audio and video streams for Zoom are redirected to the endpoint devices. Audio and video data are not processed by the server.
- [ ] The audio and video streams for Zoom are not redirected.*

The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article VDI backwards compatibility[151].
You can select the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection > Zoom client version**.

Skype for Business

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**

151. https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility



Server and Network Requirements
Skype for Business optimization requires additional configuration on the Citrix VDI Desktop image, as well as some additional network configurations.
For more information, see https://docs.citrix.com/en-us/hdx-optimization/current-release.html.

The HDX RealTime Media Engine is required for using Skype for Business in a Citrix session.

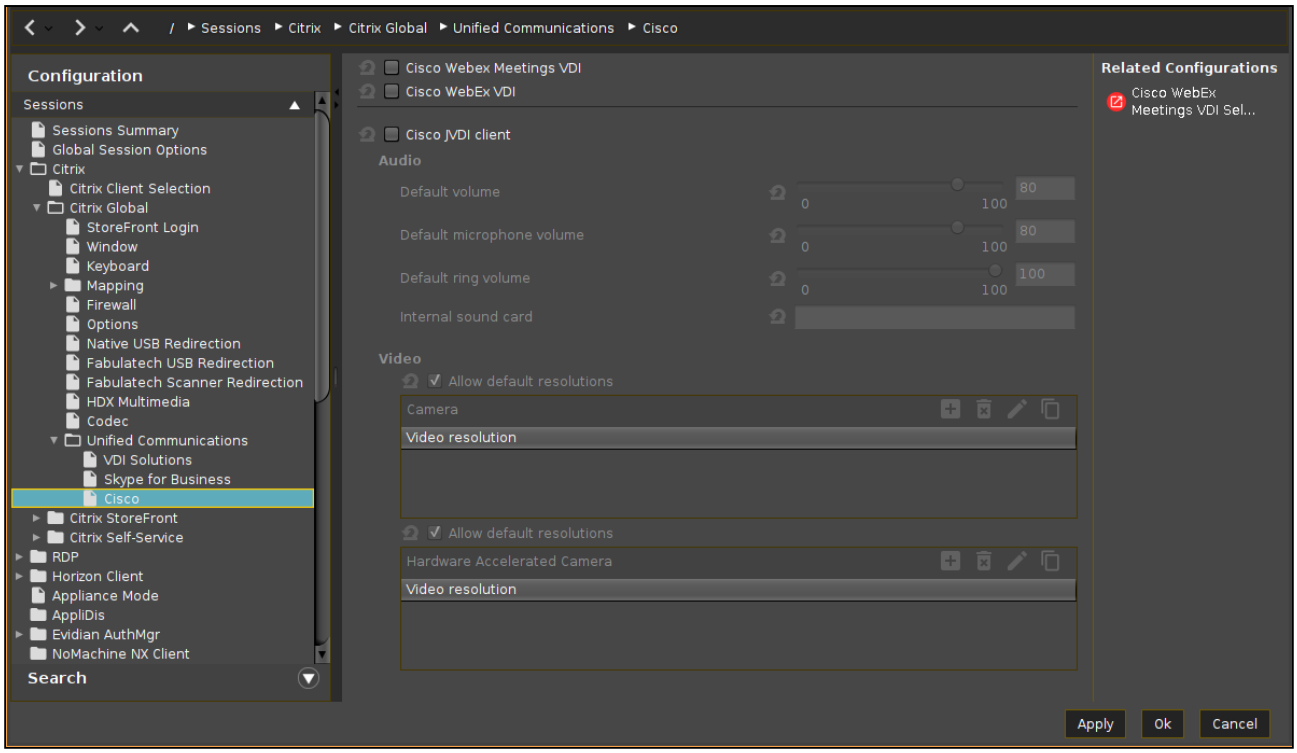
HDX RealTime Media Engine

- ☑ The HDX RealTime Media Engine is active.*
- ☐ The HDX RealTime Media Engine is not active.

Cisco

Menu path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco**

Here you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.



Cisco Webex Meetings VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly between the endpoint devices and Webex Meetings cloud, without going through the hosted virtual desktop in the datacenter.

> ⚠ The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see Webex Meetings VDI Release Notes[152].
> To select the version of the Cisco Webex Meetings plugin:
>
> 1. In the UMS configuration dialog or the local Setup, go to **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection > Cisco Webex Meetings client version**.
>   (If you do not see the corresponding version in the UMS configuration dialog, but it is listed in the release notes, please update the firmware your profile is based on.)
> 2. Select the desired version and click **Apply** or **Ok**.

For further information, see the Cisco documentation for Webex Meetings:

- General information: https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software
- Administration guide: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8.html[153]

152. https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5

- Installation: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8/webex_m_wvdi-software-installation.html

- [x] The Cisco Webex Meetings VDI solution is enabled.
- [ ] The Cisco Webex Meetings VDI solution is disabled. (Default)

Cisco Webex VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter.

For further information, see the Cisco documentation for Webex VDI:

- General information: https://www.cisco.com/c/dam/en_us/solutions/collaboration/docs/cisco-webex-teams-solution-overview.pdf
- Overview about the supported versions: https://help.webex.com/en-us/ntp1us7/Webex-VDI-Release-Notes#Cisco_Reference.dita_13d9aace-b6f9-41dc-a6e0-9f7a48834060
- Administration guide: Administration - Webex App | Installation and Automatic Upgrade[154]
- Installation: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide.pdf

- [x] The Cisco Webex VDI solution is enabled.
- [ ] The Cisco Webex VDI solution is disabled. (Default)

Cisco JVDI Client

For the vendor documentation for the Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0[155].

- [x] The Cisco JVDI Client is enabled.
- [ ] The Cisco JVDI Client is disabled. (Default)

> If you do not see the option **Cisco JVDI Client**, check if the **Cisco JVDI Client** is enabled under **System > Firmware Customization > Features**. Reboot the device if required.
> If you have reduced the IGEL OS feature set before and cannot activate **Cisco JVDI Client**, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

Audio

153. https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fcollaboration%2Fwebex_vdi%2Fadmin%2Fwebex_b_admin-cisco-wmvdi-40-8.html&data=04%7C01%7Cfeeney%40igel.com%7Cbbb4ae6a9db34ec84a0b08d88cee6ac9%7C3f04441122ea4ba182dfd85e25879b4f%7C0%7C0%7C637414302911303723%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=NrHywiQaoFcqcl5f%2FCRgK2BJw7%2BFfWirNQNj4MYTz0s%3D&reserved=0
154. https://help.webex.com/en-US/article/nw5p67g/Webex-App-%7C-Installation-and-Automatic-Upgrade
155. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html

Default volume

Headphone volume control. (Default: 80%)

Default microphone volume

Microphone volume control. (Default: 80%)

Default ring volume

Ringtone volume control. (Default 100%)

Internal sound card

Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see Sound Preferences (see page 1744)

Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

Allow default resolutions (for cameras without hardware resolution)

- ☑ The default resolutions of the camera are used. (Default)
- ☐ A user-defined set of resolutions is used. You can add a resolution by clicking ⊞ in the **Camera** area and selecting the desired resolution.

Allow default resolutions (for cameras with hardware resolution)

- ☑ The default resolutions of the camera are used. (Default)
- ☐ A user-defined set of resolutions is used. You can add a resolution by clicking ⊞ in the **Hardware Accelerated Camera** area and selecting the desired resolution.

Related Topics

Webcam Redirection and Optimization in IGEL OS (see page 1034)

Which Unified Communication Solutions Does IGEL OS Support? (see page 1163)

Citrix Self-Service

Menu path: **Sessions > Citrix > Citrix Self-Service**

The Citrix Self-Service interface allows access to Citrix Virtual Desktops and Apps via Self-Service UI.

- Server (see page 1288)
- Options (see page 1290)
- Desktop Integration (see page 1291)

Server

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server**

To manage the list, proceed as follows:

->Click on to create a new entry.

->Click on to remove the selected entry.

->Click on to edit the selected entry.

->Click on to copy the selected entry.

Server: Web Interface

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))
- **Path to config.xml file:** (default: Citrix/PNAgent/config.xml)
- **Store Name**: Name for the store

Server: StoreFront

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))
- **Path to the store** (default: Citrix/Store)
- **Store Name**: Name for the store

Server: StoreFront Legacy Mode

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))

- **Path to the config.xml file** (default: Citrix/Store/PNAgent/config.xml)
- **Store Name**: Name for the store

Options

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server > Options**

- **Display mode**: Display type for the Self-Service user interface
  Possible values:
  - Window
  - Full screen

  > In full screen mode, the IGEL desktop will not be available.

- **Multi user**
  ☑ The user data on the client will be deleted after logging off or terminating Self-Service. (default)
- **Reconnect after logon**:
  ☑ The Self-Service user interface reconnects automatically to applications and desktops after being launched.
  ☐ The Self-Service user interface does not reconnect automatically.
- **Reconnect to apps after starting an application**:
  ☑ The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
  ☐ The Self-Service user interface will not attempt to reconnect. (default)

Desktop Integration

Self-Service session: Name for the Self-Service session. (Default: Self-Service)

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

> ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

> ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Citrix StoreFront

Menu path: **Sessions > Citrix > Citrix StoreFront**

Most of the settings were already configured under Citrix Global.

- Server of Citrix StoreFront (see page 1295)
- Login Settings for Citrix StoreFront in IGEL OS (see page 1296)
- Appearance (see page 1299)
- Reconnect with Citrix StoreFront (see page 1301)
- Refresh with Citrix StoreFront (see page 1303)
- Logoff (see page 1305)
- Desktop Integration (see page 1307)

Server of Citrix StoreFront

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront** > **Server**

- **Server location:** You can set up up to 5 Citrix master browsers per domain. If the first browser is not available, the second will be queried and so on. Please note that multiple farms can be searched. You can therefore specify addresses for a number of server farms.
- To manage the list, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
  - Click on to copy the selected entry.

Add

- **Protocol**:
  - https://
- **Citrix Store site address**: Server name or IP address of the server
- **Port**: Network port on which the service is available (default: 443)
- **Path to Store**: (default: Citrix/Store)
- **Store name**: Name of the Citrix store

Domains

- To manage the list of **domains**, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
  - Click on to copy the selected entry.

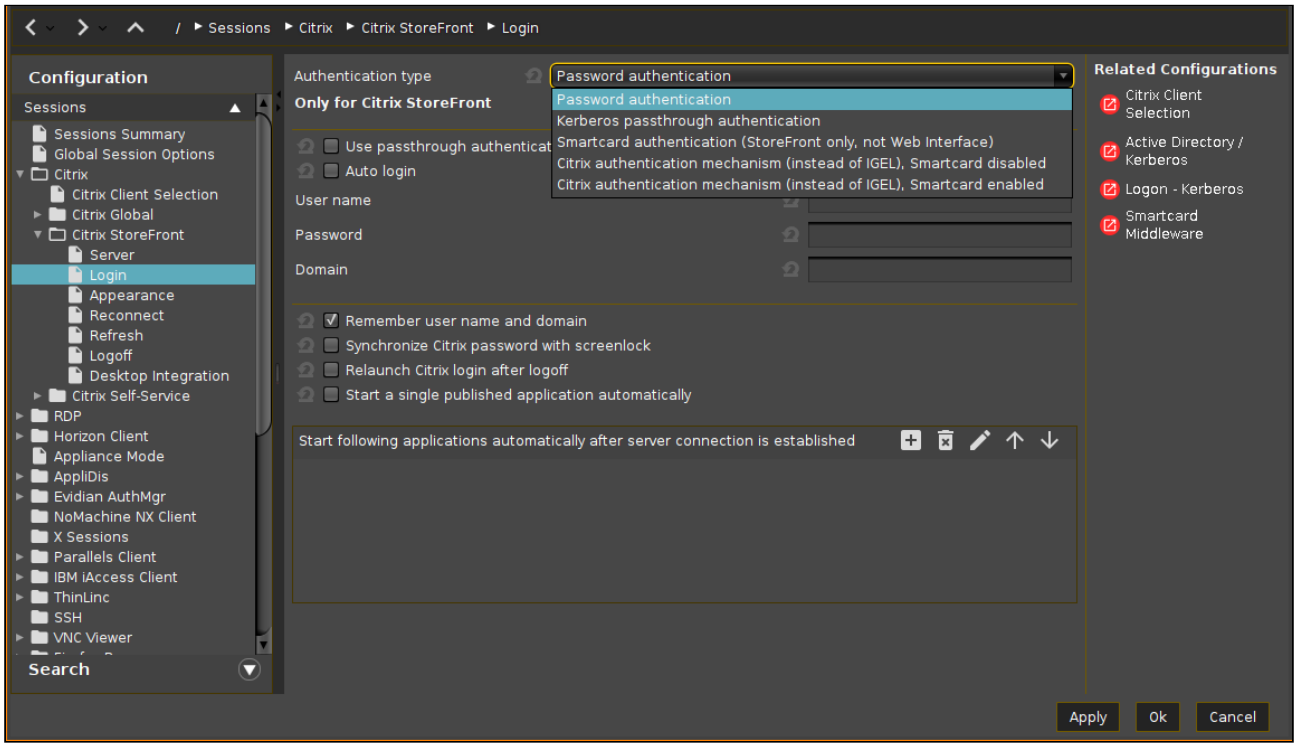
Handling of domain in login window:

- normal
- locked
- hidden

Login Settings for Citrix StoreFront in IGEL OS

In the **Login** area, you can define session-specific login options. Login options for Citrix sessions can also be configured in IGEL OS globally under **Citrix > Citrix Global > StoreFront Login**.

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**



Authentication type

Depending on the Citrix client version, the following types are available:

- **Password authentication**: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- **Kerberos passthrough authentication**: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device, see Active Directory/Kerberos (see page 2014).
- **Smartcard authentication (StoreFront only, not Web Interface)**: Authentication via smartcard will only work with StoreFront, not with Web Interface. For configuration details, see Citrix StoreFront (see page 795).
- **Citrix authentication mechanism (instead of IGEL), Smartcard disabled**: Recommended for cloud environments and Citrix NetScaler.
- **Citrix authentication mechanism (instead of IGEL), Smartcard enabled**: Recommended for cloud environments and Citrix NetScaler.

If you have set an authentication type with smartcard, select the type of card on the Smartcard (see page 2024) page. You may find it also helpful to read the how-to Smartcard Authentication in IGEL OS (see page 791).

Depending on the selected authentication type, the following options are available:

Use passthrough authentication

- Cached login data are used for listing and starting applications. For more information, see Passthrough Authentication (see page 1165).
- No passthrough authentication. (Default)

Auto login

- Uses the login data preset on this page when connecting to the server.
- Do not log in automatically. (Default)

User name

Can only be filled in with password authentication.

Password

Can only be filled in with password authentication.

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Can only be filled in with password authentication.

Remember username and domain

- Saves the user name and domain from the last login. (Default)
- The user name and domain will not be saved.

Synchronize Citrix password with screenlock

- Synchronizes the screenlock password (see page 1849) with that of the Citrix application. You can use this option if you want, for example, to use the user's AD password to unlock the screen.
- No synchronization (Default)

Relaunch Citrix login after logoff

- ☑ Automatically shows the login dialog again after logging out.
- ☐ Does not start the login procedure again. (Default)

Start a single published application automatically

This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.

- ☑ The published application is started when the user has logged in.
- ☐ The published application is not started on login. (Default)

Start following applications automatically after server connection is established

A list of applications to be started in the session.

To edit the list, proceed as follows:

- Click on to create a new entry. In the **Add** dialog, give the name of the application.

> Application names are case-sensitive.
> You can also enter part of the name followed by an asterisk (*).

- Click on to remove the selected entry.
- Click on to move the entry upwards.
- Click on to move the entry downwards.

> After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

> **App Protection Feature for the Citrix Workspace App**
> To strengthen the security of your Citrix environment, you can use the app protection feature in IGEL OS 11.08.200 or higher. It provides anti-keylogging and anti-screen-capturing functionalities. For more information on this feature and the required server-side settings, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/secure/app-protection.html .
> To activate the feature on IGEL OS, go to **System > Registry** and enable the Citrix App Protection registry key: `ica.appprotection`
> The feature is supported for Citrix Workspace app version 22.07 and higher; for how to change the version, see Citrix Client Selection in IGEL OS (see page 1247).

Appearance

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Appearance**

- **Show applications in the start menu**
  - ☑ Applications will appear in the start menu (default)
  - ☐ Applications will not appear in the start menu
- **Show in the start menu**
  - All: All Citrix applications will be shown in the start menu.
  - Follow server settings
- **Resize icons for the start menu**
  - ☑ The size of icons for the start menu will automatically be adjusted. (default)

> Automatic scaling can prolong the logon procedure.

- **Apply display filter to start menu entries**
  - ☑ Only the applications selected in the display filter will be shown in the start menu.
  - ☐ Do not use display filter (default)
- **Show applications in the Application Launcher**
  - ☑ Applications will be shown in the Application Launcher. (default)

- **Apply display filter to Application Launcher entries**
  - ☑ Only the applications selected in the display filter will be shown in the Application Launcher.
  - ☐ Do not use display filter (default)

- **Show applications on desktop**
  - ☑ The applications will be shown on the desktop. (default)

- **Keep folder structure on desktop**
  - ☑ The Citrix sessions are shown in their directory structure on the desktop.
  - ☐ The directory structure is not shown. (default)
- **Show desktop shortcuts**
  - All: All Citrix applications will be shown in the Desktop Launcher.
  - Follow server settings

- **Apply display filter to desktop icons**
  - ☑ Desktop icons are created only for the applications selected in the display filter (see below). (default)

- **Display filter: Show only the following applications**. In the **Add** dialog, enter the name of the application that is to be shown on the desktop.
  To manage the list, proceed as follows:
  - Click on to create a new entry.
  - Click on to remove the selected entry.
  - Click on to edit the selected entry.
- **Enable following applications in quick start panel**: In the **Add** dialog, enter the name of the application that is to be shown in the quick start panel.

Reconnect with Citrix StoreFront

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Reconnect**

- **Automatic reconnection at logon**
  - ☑ Connection will take place when logging on.
  - ☐ Do not reconnect (default)
- **Connect to**
  Possible values:
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Automatic reconnection from menu/desktop**
  - ☑ Reconnect
  - ☐ Do not reconnect (default)

- **Connect to**
  Possible values
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Reconnect session name**: Session name (default: Reconnect)

Starting Methods for Sessions

- **Start menu**: If this option is enabled, the session can be launched from the start menu.
- **Application Launcher**: If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop**: If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel**: If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system icon**: If this option is enabled, the session can be launched with the start menu's system icon.
- **Application Launcher's system icon**: If this option is enabled, the session can be launched with the Application Launcher's system icon.
- **Desktop context menu**: If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

- **Password protection**: Specifies which password will be requested when launching the session. Possible values:
  - **None**: No password is requested when launching the session.
  - **Administrator**: The administrator password is requested when launching the session.
  - **User**: The user password is requested when launching the session.
  - **Setup user**: The setup user's password is requested when launching the session.
- **Hotkey**:
  - The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers**: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:
  - (No modifier) = `None`
  - = `Shift`
  - [Ctrl] = `Ctrl`
  - = `Super_L`
  - [Alt] = `Alt`

  Key combinations are formed as follows with `|`:
  - Ctrl + = `Ctrl|Super_L`
- **Key**: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Refresh with Citrix StoreFront

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Refresh**

Refresh Session Name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.

Desktop

- The session can be launched with a program launcher on the desktop.

Quick start panel

- The session can be launched with the quick start panel

Start menu's system tab

- The session can be launched with the start menu's system tab.

Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

Desktop context menu

- The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

- The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Logoff

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Logoff**

- **Logoff session name:** Session name (default: Logoff)

Starting Methods for Session

- **Session name**: Name for the session

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

- **Start menu**:
  - ☑ The session can be started with the start menu. (Default)
  - ☐ The session cannot be found in the start menu.
- **Application Launcher**:
  - ☑ The session can be started with the Application Launcher. (Default)
  - ☐ The session cannot be found in the Application Launcher.
- **Desktop**:
  - ☑ The session can be started with a program starter on the desktop. (Default)
  - ☐ The session does not have a program starter on the desktop.
- **Quick start panel**:
  - ☑ The session can be started with the quick start panel.
  - ☐ The session cannot be found in the quick start panel. (Default)
- **Start menu's system icon**:
  - ☑ The session can be started with the start menu's system icon.
  - ☐ The session cannot be found in the start menu's system icon. (Default)
- **Application Launcher's system icon**:
  - ☑ The session can be started with the Application Launcher's system icon.
  - ☐ The session cannot be found in the Application Launcher's system icon. (Default)
- **Desktop context menu**:
  - ☑ The session can be started with the desktop context menu.
  - ☐ The session cannot be found in the desktop context menu. (Default)

- **Menu folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection**: Specifies which password will be requested when launching the session. Possible values:
  - None: No password is requested when launching the session.
  - **Administrator**: The administrator password is requested when launching the session.
  - **User**: The user password is requested when launching the session.
  - **Setup user**: The setup user's password is requested when launching the session.

- **Hotkey**: A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers**: One or two modifiers for the hotkey:
  - `None`
  - = `Shift`
  - [Ctrl] = `Ctrl`
  - = `Super_L`
  - [Alt] = `Alt`

  Modifiers can be combined by using the pipe character `|`:
  - [Ctrl]+ = `Ctrl|Super_L`
- **Key**: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the character string for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Desktop Integration

Menu path: **Sessions > Citrix > Citrix StoreFront> Desktop Integration**

Login session name: Session name.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

- The session can be launched from the start menu.

Application Launcher

- The session can be launched with the Application Launcher.

Desktop

- The session can be launched with a program launcher on the desktop.

Quick start panel

- The session can be launched with the quick start panel

Start menu's system tab

- The session can be launched with the start menu's system tab.

Application Launcher's system tab

- The session can be launched with the Application Launcher's system tab.

Desktop context menu

- The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

- ☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.
- ☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

- ☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.
- ☐ The session is started automatically, even when no network is available.

RDP Global

Menu path: **Setup > Sessions > RDP > RDP Global**

This section describes the procedure for configuring the global RDP settings. This configuration applies for all RDP sessions.

> The protocol version cannot be configured manually. The version used by the server is automatically recognized and used.

_____

- RDP Global Gateway (see page 1311)
- RDP Global Local Logon (see page 1313)
- Window (see page 1314)
- Keyboard (see page 1316)
- RDP Global Mapping (see page 1317)
- Performance (see page 1325)
- Options (see page 1329)
- Native USB Redirection (see page 1330)
- Fabulatech USB Redirection for RDP in IGEL OS (see page 1333)
- Fabulatech Scanner Redirection (see page 1337)
- Multimedia (see page 1338)

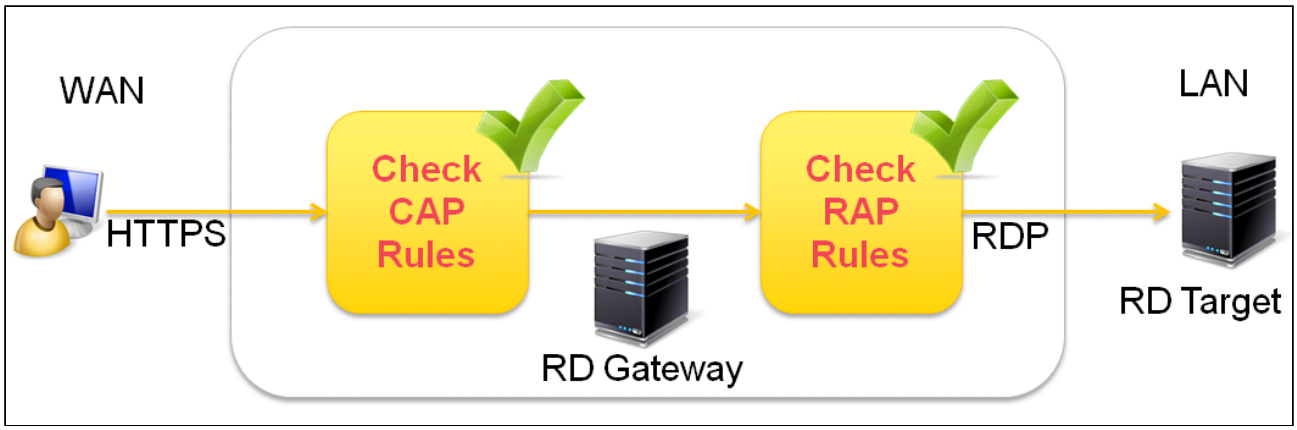
RDP Global Gateway

Menu path: **Setup > Sessions > RDP > RDP Global > Gateway**

Via *Microsoft Remote Desktop Gateway*, you can access remote *Windows* systems.

The gateway translates between the internal *Remote Desktop Protocol* (RDP) and the external HTTPS connection.

Access to the Remote Desktop environment is provided via the browser. The browser establishes a secure connection to the gateway. From here, the connection query is forwarded to the target system. In the process, pre-defined *Connection Access Policies* and *Resource Access Policies* (CAP and RAP) for access control are evaluated.



Enable gateway support:

☑ Gateway support is enabled and you can configure the following settings:

☐ Gateway support is disabled. (default)

- **Gateway address**

  RD gateway requires *Microsoft Windows Server 2008R2* or *Server 2012* with various restrictions for each server version.

  The following Windows Server editions can preferably be used as gateway servers:
  Server 2008R2 Standard (restricted to 250 RD Gateway connections)
  Server 2008R2 Enterprise
  Server 2008R2 Datacenter
  Server 2012 Standard
  Server 2012 Datacenter
  Server 2012 Essential (restricted to the RD Gateway role)
  Server 2012R2 Standard
  Server 2012R2 Essential (restricted to the RD Gateway role)

  RD Gateway is not supported in the IGEL RDP Legacy Mode.

- **Use other logon data for RD gateway**

☑ Uses custom data that can be defined below rather than the session access data.
☐ Uses the session access data. (default)

- **Gateway user name**: User name when logging on to the gateway
- **Gateway password**: Password when logging on to the gateway
- **Gateway domain**: Domain in which the gateway is located

RDP Global Local Logon

Menu path: **Setup > Sessions > RDP > RDP Global > Local Logon**

In this area, you can prepopulate user data. As a result, you can avoid users possibly having to log in a number of times.

> You can also use **Local logon** to freely select the server in the logon window of an RDP session.

- **Use local login window**
  ☑ The RDP login window is used on the terminal side to set the user name and domain when a connection to the terminal server is established for the first time. (default)

You can configure the following presets:

- **Preset login information**
  ☑ The login window is prepopulated with the user name and domain. (default)
- **Type**: Here, you can prepopulate the user name and domain in the logon window.
  Possible values:
  - Set user/domain from last login
  - Set user/domain from session setup
- **Show domain**
  ☑ Shows the domain entry in the logon window. (default)
- **Set client name to user name**
  ☑ The name of the client for the RDP connection will be set to the user name. This setting may help to resolve reconnection problems during load balancing. (default)
- **Relaunch mode**
  ☑ The RDP login window is displayed in restart mode and cannot be closed.
  ☐ The RDP window will not be displayed in restart mode. (default)
- **Enable network authentication**
  ☑ Enables network authentication via NTLM. Smartcards are not supported here. (default)
- **Domains**: Allows you to add domains which are to be available. If you enter a number of domains, these will be shown in the **Domains** drop-down area in the login module.

To manage the list of domains, proceed as follows:

→ Click + to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Window

Menu path: **Sessions > RDP > RDP Global > Window**

In this area, you can configure the window for RDP sessions.

You can change the following settings:

Number of Colors: Specifies the color depth.
Possible values:

- 256
- Thousands
- Millions

Window size: Specifies the width and height of the window.

- Full-screen: The session is shown on the full screen. The device's taskbar is not visible.
- Work area: The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Desktop scale factor: Specifies the desktop scaling in percent. Select a value from the selection list or enter a percentage value manually.

> Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

Possible values:

- Automatic: The resolution set under **User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
- Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%

> Set the **Desktop scale factor** to a fixed value of 100% to allow server-side desktop scaling take effect. All values other than 100% overwrite the server-side setting.

Enable Display Control

☑ The window size can be changed during the session. (Default)

> If the window size is to be changed during the session, at least Windows 8.1 or Windows Server 2012 R2 must be running on the server.

> It is not possible to change the window size during the session if **Window size** is set to **full-screen** or **workarea**.

Control Bar for RDP-Sessions

☑ A control bar for minimizing and closing a full-screen session will be shown.

☐ No control bar will be shown. (Default)

If the symbol bar is enabled, a session will be shown on one monitor only, even if **Multimonitor fullscreen mode** is set to **Expand full-screen session across all monitors**.

Multimonitor full-screen mode - If more than one monitor is connected to the terminal:

- Restrict full-screen session to one monitor
- Display full-screen session on all monitors
- Expand full-screen session across all monitors

Keyboard

Menu path: **Setup > Sessions > RDP > RDP Global > Keyboard**

Configure how the keyboard reacts within RDP sessions. The following options are available:

- **Enable clipboard**
  ☑ You can use the clipboard. (default)
- **Input language**: Here, you can determine which language is used for auto-correction in the RDP session. This is independent of the keyboard layout. The "Default" setting corresponds to the system setting. (default: Default).
- **Override local window manager keyboard shortcuts**
  ☑ All keyboard entries, including those which would otherwise be processed by the local window manager, will be sent straight to the Windows server.
  ☐ The keyboard shortcuts of the local window manager will not be overridden. (default)

RDP Global Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping**

In this area, you can make available locally connected devices such as printers or USB storage devices in RDP sessions.

- Drive Mapping (see page 1318)
- COM Ports (see page 1319)
- Printers Mapping (see page 1321)
- Device Support (see page 1322)
- Audio (see page 1324)

Drive Mapping

Menu path: **Sessions > RDP > RDP Global > Mapping > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

Enable Drive Mapping

☑ Drive mapping is enabled. (Default)

Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See Storage Hotplug (see page 1969).

Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on ⏏ in the task bar. The taskbar is not available in a fullscreen session.
- Click on ⏏ in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see In-Session Control Bar (see page 1872).
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

Drive Mapping: List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click ➕ **Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated floppy drive).

COM Ports

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Serial Connections**

As with locally connected mass storage devices, you can also map the device's local serial connections (COM ports) during an RDP session:

Enable COM port mapping:

☑ COM port mapping is enabled. (default)

Server COM Port starts with: Specifies the lowest device number that is used on the server for mapping. Possible values:

- COM 1 to COM 6. (default: COM1)

COM Port Devices: List with mapped local serial devices.
Click + to add a serial device.

- **COM Port Device**:
  Possible values:
  "COM 1"
  "COM 2"
  "COM 3"
  "COM 4"
  "USB COM 1": For UD3-LX60 devices (mainboard: M350C), this port must be used instead of "COM 1".
  "USB COM 2"
  "USB COM 3"
  "USB COM 4"

Detect Devices...: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:

(GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion. Example: `/dev/ttyUSB0`

(BY PORT) [device designation]: According to the USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`

(BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`

(Virtual) [device designation]: Virtual device; used for signature pads for example. Example: `/dev/ttyVST0`

ℹ If your device has an additional multiport PCI card, more than 2 connections may be available.

If you would like to use signature pads, you must enable them beforehand under **User Interface > Input >** Signature Pad (see page 1883).

Printers Mapping

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Printers**

In this area, you can configure printer mapping.

Enable Client Printer Mapping

☑ The locally connected device printer is made available for your RDP sessions, provided that it was not disabled on the server-side. (default)

The printers must be set up on the **Devices > Printer > CUPS >** Printers - Configure CUPS Printers in IGEL OS (see page 1976) page and must be enabled there for mapping in RDP sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.

Device Support

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Device Support**

In this area, you can enable virtual RDP channels for communicating with various devices connected to the device.

The devices supported are listed in the IGEL Third Party Hardware Database[156].

- **Enable plugin support**
  ☑ Communication between connected devices and the relevant server applications is enabled. The individual channels must also be enabled.
  ☐ Communication between connected devices and server applications is not enabled. (Default)

When using *DriveLock*, ensure that the use of USB devices is not universally restricted; see **Devices >** USB Access Control[157].

- **DriveLock channel**: The virtual DriveLock channel is implemented on the device. The channel must also be installed on the RDP server.
  DriveLock can read hardware data from local USB devices and transfer these data to the server with the help of the virtual RDP channel extension. From IGEL Linux *Version 10.03.500* this is also possible with SATA devices. When using whitelists, rules based on the hardware properties of the connected drive (e.g. manufacturer details, model and serial number) are taken into account. Important information regarding DriveLock can be found in the Using DriveLock with IGEL Devices[158] FAQ.
  ☑ A virtual channel for DriveLock is enabled.
  ☐ No virtual channel for DriveLock is enabled. (Default)
- **Diktamen channel for dictation**
  ☑ A virtual channel for Diktamen is enabled.
  ☐ No virtual channel for Diktamen is enabled. (Default)
- **deviceTRUST channel**
  ☑ A virtual channel for deviceTRUST is enabled..
  ☐ No virtual channel for deviceTRUST is enabled. (Default)
- **Grundig MMC channel for dictation with Grundig devices**
  ☑ A virtual channel for communication with Grundig devices is enabled.
  ☐ No virtual channel for communication with Grundig devices is enabled. (Default)
- **Olympus channel for dictation**
  ☑ A virtual channel for communication with Olympus dictation devices is enabled.
  ☐ No virtual channel for communication with Olympus dictation devices is enabled. (Default)
- **Philips speech channel for dictation**
  ☑ A virtual channel for communication with Philips dictation devices is enabled.
  ☐ No virtual channel for communication with Philips dictation devices is enabled. (Default)
- **DPM server drive**: Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

156. https://www.igel.com/linux-3rd-party-hardware-database/
157. https://kb.igel.com/en/igel-os/11.10.270/usb-access-control
158. https://kb.igel.com/en/igel-os/11.10.270/using-drivelock-with-igel-devices

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Hotplug storage device[159] and Drive mapping[160].

- **SpeechAir server drive**: Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server (default: S)

The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter. Further information can be found under Hotplug storage device[161] and Drive mapping[162].

- **Lakeside SysTrack channel**
  ☑ The Lakeside SysTrack channel is enabled.
  ☐ The Lakeside SysTrack channel is not enabled. (Default)
- **Enable smartcard**
  ☑ The device's smartcard reader will appear within the RDP session. Applications can access the reader and the smartcards it contains. (Default)
  ☐ The device's smartcard reader will not appear within the RDP session.

159. https://kb.igel.com/en/igel-os/11.10.270/restricting-the-mounting-of-hotplug-storage-device
160. https://kb.igel.com/en/igel-os/11.10.250/drive-mapping
161. https://kb.igel.com/en/igel-os/11.10.270/restricting-the-mounting-of-hotplug-storage-device
162. https://kb.igel.com/en/igel-os/11.10.250/drive-mapping

Audio

Menu path: **Setup > Sessions > RDP > RDP Global > Mapping > Audio**

In this area, you can configure the settings for local audio transmission.

- **Enable client audio**
  Possible values:
  - On: Audio will be transmitted.
  - Off: No audio will be transmitted.
- **Audio quality mode**
  Possible values:
  - Automatic
  - High: High audio quality is favored.
  - Medium: Medium audio quality is favored.
  - Dynamic
- **Audio compression**
  Possible values:
  - Automatic
  - On: Compressed audio data will be accepted.
  - Off: Compressed audio data will not be accepted.
- **Audio recording**
  ☑ The microphone will be diverted to the session.
  ☐ The microphone will not be diverted to the session. (Default)

Performance

Menu path: **Setup > Sessions > RDP > RDP Global > Performance**

In this area, you can configure settings in order to improve the performance of the RDP session.

Enable RemoteFX

☑ Remote FX is enabled. (Default)

RemoteFX codec mode

Possible options:

- Use server setting
- Optimized for LAN
- Optimized for WAN
- Legacy mode

Hardware accelerated codecs AVC420/AVC444 (H.264)

Possible options:

- Automatic: H.264 is activated automatically if supported by the device's hardware.
- On: H.264 is activated, regardless of hardware support.

> For testing purposes only; this option can lead to display flaws.

- Off: H.264 is deactivated.

→ You can disable graphics functions which are not absolutely necessary.

Graphics settings that you can disable in order to improve performance:

Disable wallpaper

☑ Desktop background is disabled.

☐ Desktop background is enabled. (Default)

Don't show contents of window while dragging

☑ Window content will be hidden.

☐ Window content will be shown. (Default)

Disable menu and window animation

☑ Menu and window animation is disabled.

☐ Menu and window animation is enabled. (Default)

Disable themes

☑ Themes are disabled.

☐ Themes are enabled. (Default)

Disable cursor shadow

☑ Cursor shadow is disabled.

☐ Cursor shadow is enabled. (Default)

Disable cursor settings

☑ Cursor settings are disabled. No "unnecessary" mouse movements will be sent.

☐ Cursor settings are enabled. (Default)

Enable font smoothing

☑ Font smoothing is enabled.

☐ Font smoothing is disabled. (Default)

Compression

> In low-bandwidth environments, you should use **compression** in order to reduce network traffic. Note that the use of compression reduces the burden on the network but does use CPU power.

☑ Data are compressed.

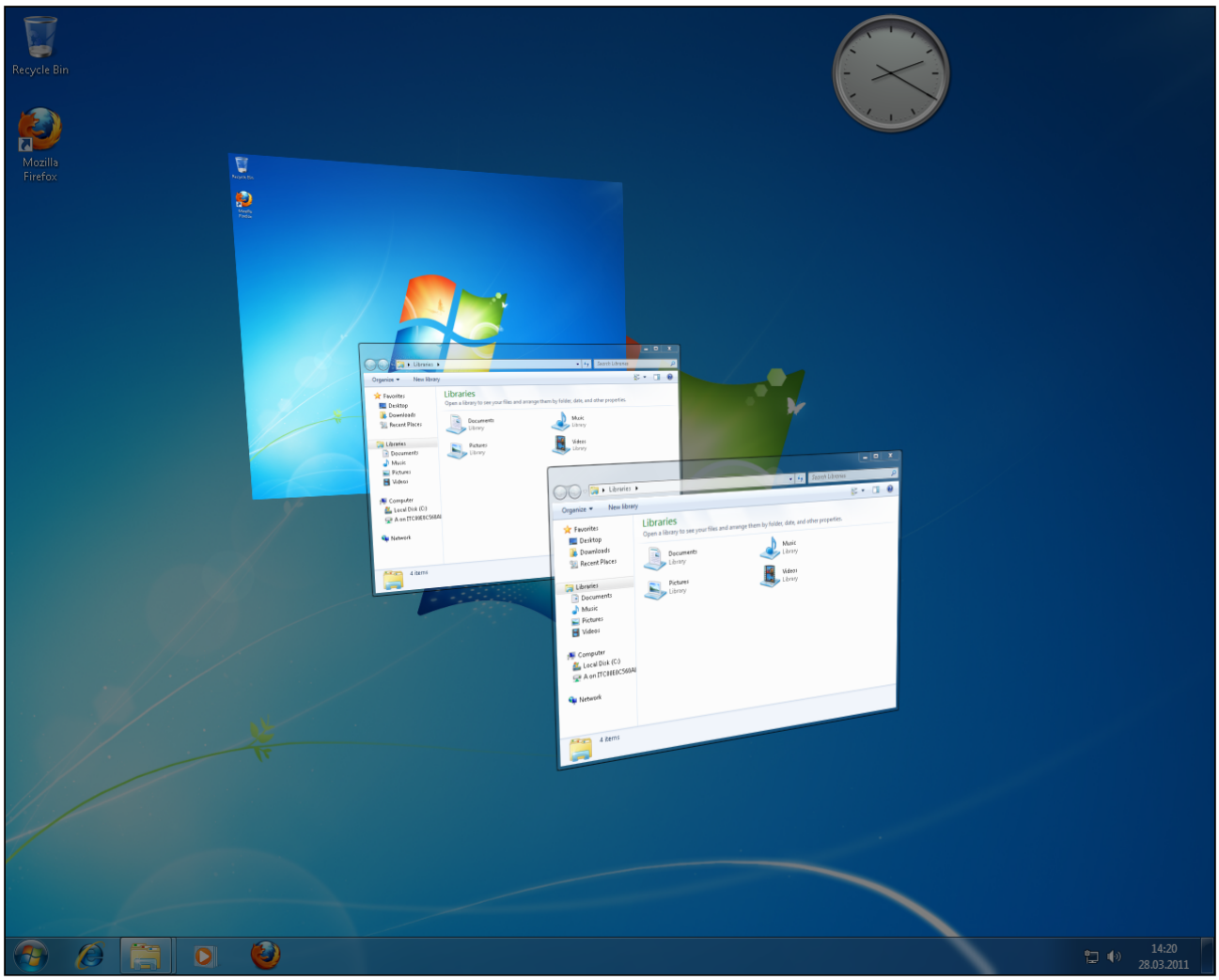
☐ Data flow is not compressed. (Default)

RemoteFX Support

Menu path: **Setup > Sessions > RDP > RDP Global > Performance > RemoteFX Support**

With the Service Pack 1 for *Windows Server 2008 R2*, local system functions such as *Windows Aero* or 3D display can be made available in RDP sessions too.

In order to do this, the RemoteFX extension for RDP must be enabled. You can configure the relevant settings under **RDP Global > Performance** or in the corresponding session settings.



Globally enabling Remote FX is not recommended as conventional RDP sessions may also be affected by this. With RemoteFX, all graphics effects available under Performance are enabled. This may slow down the session as a result. It is better to enable the function only for individual sessions which establish a connection to appropriately equipped servers.

Further information on Remote FX and the server-related requirements is available from Microsoft at https://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx[163].

In the IGEL Registry, you can configure the number of frames sent by the server without confirmation under the key `rdp.winconnect.remotefx-ack`. The default value is 1. A value of 2 or 3 can lead to improved performance in networks with high latency.

163. http://technet.microsoft.com/en-us/library/dd736539(ws.10).aspx

Options

Menu path: **Setup > Sessions > RDP > RDP Global > Options**

In this area, you can configure the following settings:

- **Inverted cursor color**
  Possible values:
  - Black
  - White
  - Dotted

  > You can also configure your own values `custom:,`. The colors must be given in the ARGB8888 format, e.g. 0xFF000000.

- **Reset license**
  ☑ The Microsoft llicense will be removed from the device. The device must then be restarted.
  ☐ The license will not be removed. (default)
- **Reset confirmed server certificates**
  ☑ All confirmed server certificated will be deleted from the client.
  ☐ The certificates will not be deleted. (default)
- **Client name**: Client name for terminal service identification.
  Possible values:
  - Special client name: Specify a special client name in the next field.
  - MAC address: Use the MAC address of the computer as the client name
  - Computer name: Use the name of the computer
- **Custom client name**: If you have opted for a special client name, you can enter the name here. If the field remains empty, the MAC address of the client will be used automatically.
- **Verify server certificate**
  ☑ The server certificate will be verified if the connection is TLS-encrypted. (default)

Native USB Redirection

Menu path: **Sessions > RDP > RDP Global > Native USB Redirection**

USB devices can be permitted or prohibited during an RDP session on the basis of default rules. Sub-rules for specific devices or device classes are also possible. The use of rules is described under USB Access Control (see page 2010).

> Enable either **Native** or **Fabulatech USB Redirection** – not both together. For details on **Fabulatech USB Redirection**, see Fabulatech USB Redirection for RDP in IGEL OS (see page 1333).

> Disable USB redirection if you use DriveLock. Further information can be found under Using DriveLock with IGEL Devices (see page 1091).

Enable native USB redirection

☑ Native USB redirection is enabled and you can define default rules below.

☐ Native USB redirection is not enabled. (Default)

Default rule
Possible values:

- Deny
- Allow

> **Tip**
>
> To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

→ Click + to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Add a class rule:

Rule:

- Deny
- Allow

Class ID: Selection list

Subclass ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add a device rule:

Rule:

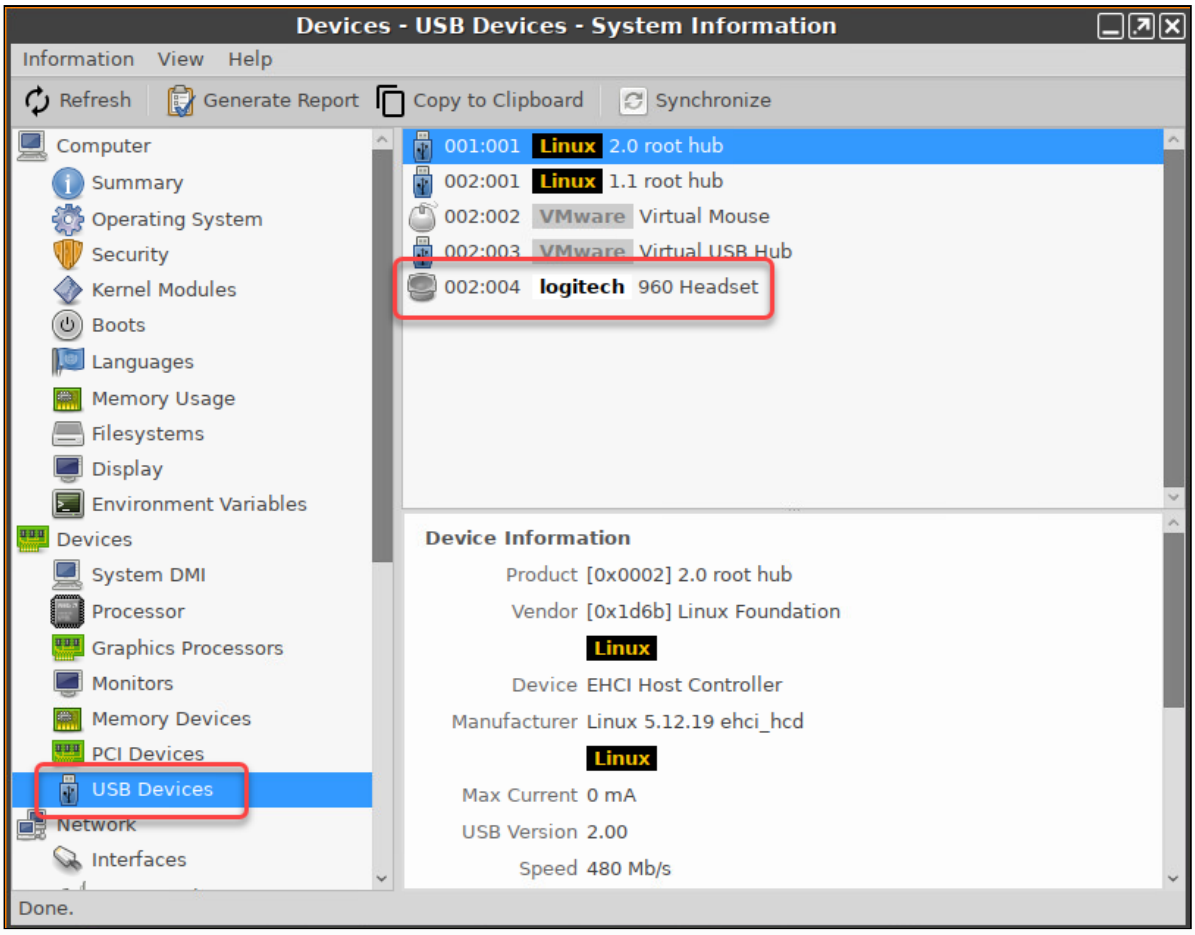
- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

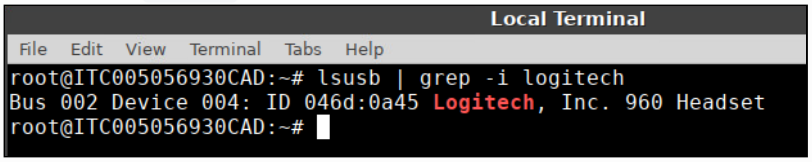
Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name: Free text entry

See also an overview and best-practice recommendations for the use of webcams under Webcam Redirection and Optimization in IGEL OS (see page 1034).

Fabulatech USB Redirection for RDP in IGEL OS

Redirection for USB devices can be allowed or denied during an RDP session using rules and sub-rules for specific devices or device classes. The use of rules is described in detail under USB Access Control (see page 2010).

Important Notes

- For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see http://www.usb-over-network.com/partners/igel/. For details on the configuration, see https://www.usb-over-network.com/partners/igel/usb-for-remote-desktop-docs.html. Please note that licenses must be purchased from Fabulatech to enable this functionality.
- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

Menu path: **Sessions > RDP > RDP Global > Fabulatech USB Redirection**

Fabulatech USB Redirection

☑ Fabulatech USB redirection is enabled for all RDP sessions.

☐ Fabulatech USB redirection is disabled. (Default)

Default rule

This rule will apply if no special rule was configured for a class or a device.
Possible options:

- **Deny** (Default)
- **Allow**

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

→ Click to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

Class rule properties:

Rule:

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB redirection.
- Deny: Devices that have the properties defined here are not redirected.

Class ID: Device class

Subclass ID: Subclass relating to the specified device class

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts.

☐ The USB device is no longer shown immediately after the system is booted. (Default)

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device).

☐ The USB device may not be removed. (Default)

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated.

☐ The device will be reset after the connection with the session has been terminated. (Default)

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- **Allow** (Default)
- **Deny**

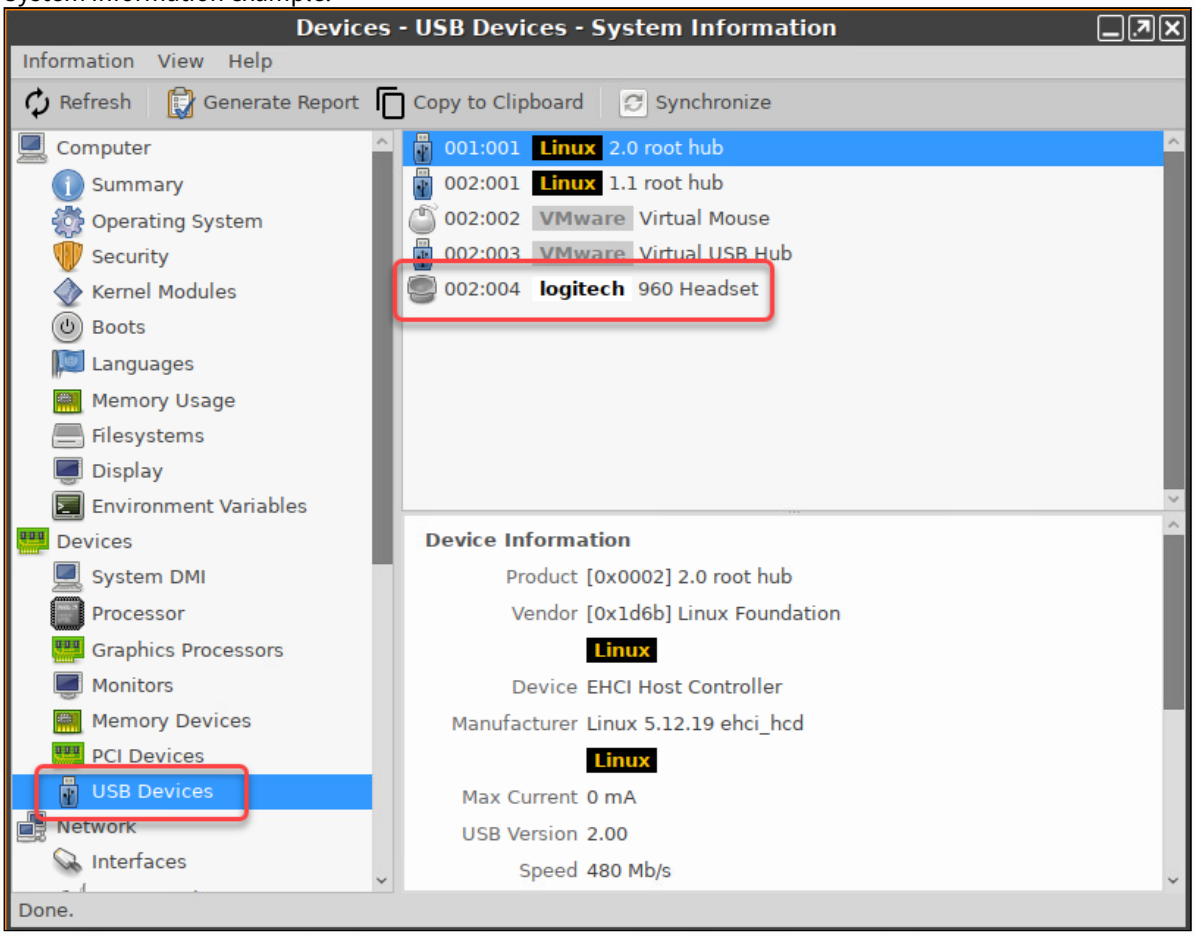
Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

Getting USB Device Information

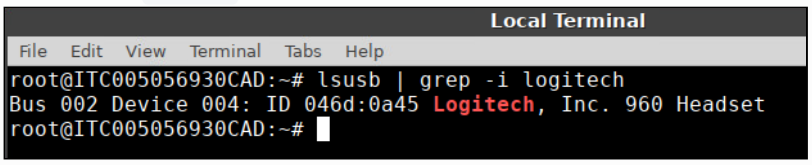
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts. (Default)

☐ The USB device is no longer shown immediately after the system is booted.

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device). (Default)

☐ The USB device may not be removed.

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated. (Default)

☐ The device will be reset after the connection with the session has been terminated.

Fabulatech Scanner Redirection

Menu path: **Sessions > RDP > RDP Global > Fabulatech Scanner Redirection**

Redirection for a Fabulatech scanner can be allowed during an RDP session.

Fabulatech Scanner for Remote Desktop

☑ Fabulatech Scanner for Remote Desktop is enabled.

For more information, see How to Enable RDP Fabulatech Scanner Redirection (see page 453).

Multimedia

Menu path: **Setup > Sessions > RDP > RDP Global > Multimedia**

In this area, you can enable video redirection in order to allow optimized video playback in remote sessions.

- **Video redirection**
  ☑ Use video redirection. The device renders the video data.
  ☐ Do not use video redirection. (default)
  From *IGEL Linux 5.06.100*, hardware acceleration for multimedia playback is available on certain devices. You will find more detailed information in the FAQ Hardware Video Acceleration on IGEL OS[164].

164. https://kb.igel.com/en/igel-os/11.10.270/hardware-video-acceleration-on-igel-os

RDP Session

Menu path: **Sessions > RDP > RDP Sessions**

You can set up your own RDP sessions here.

The following configuration pages offer you detailed setup options for the RDP session:

- Server (see page 1340)
- Gateway (see page 1341)
- RDP Session Logon (see page 1342)
- Window (see page 1343)
- Keyboard (see page 1345)
- Mapping (see page 1346)
- Performance (see page 1347)
- Options (see page 1348)
- USB Redirection (see page 1349)
- Multimedia (see page 1350)
- Desktop Integration (see page 1351)

Server

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Server**

In this area, you can change the information regarding the server connection.

→ Choose between **Server** and **RemoteApps mode**.

Server

Server: Name or IP address of the server.

RDP port: The RDP TCP/IP port which is used for the connection. (Default: 3389)

Collection: The name of the Remote Desktop Services (RDS) collection to connect to.

> Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is `tsv://MS Terminal Services Plugin.1.RDS collection name`. For more information, see https://kb.igel.com/en/igel-os/11.10.270/faq-what-is-the-string-for-token-based-load-balanc

Application: Start application for the terminal server session.

Command line parameter for the executed program: Command line parameter with which you would like to call up your own application in the RemoteAPP mode.

Changeable server URL on local login

☑ The server can be entered freely when the user logs in locally. Local login must be enabled in order to do this.

☐ The terminal server's login window will be shown. When using local login, the device's login window will be shown. (Default)

> If the **Passthrough Authentication** option is enabled, the session with the local login data for the terminal user, e.g. from the domain login, is used. However, this setting will be overridden by the **Local Login** global parameter. You should not therefore use both options at the same time.

Enable RemoteApp Mode

Like the published applications of a Citrix server, MS Windows Server 2008 offers the option of passing on RemoteApps to the device.

Detailed instructions regarding server configuration can also be found on the Microsoft website: TS RemoteApp Step-by-Step Guide[165].

On the client side, only a few parameters need to be configured after enabling the RemoteApp mode.

> Please note that the name of the application to be launched must be preceded by two pipe characters (||), e.g. `||Excel`.

165. https://technet.microsoft.com/en-us/library/cc730673(v=ws.10).aspx

Gateway

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Gateway**

Here, you can specify custom gateway details for your RDP session.

Enable gateway support

- Global setting: The settings from **RDP Global > Gateway** will be carried over.
- Session setting: Here, you can configure custom settings. The entry options correspond to those under RDP Global Gateway (see page 1311).
- Off: No gateway support

Gateway address

> RD Gateway requires Microsoft Windows Server 2008R2 or Server 2012 with various restrictions for each server version.

The following Windows Server editions can preferably be used as gateway servers:
Server 2012 Standard
Server 2012 Datacenter
Server 2012 Essential (restricted to the RD Gateway role)
Server 2012R2 Standard
Server 2012R2 Essential (restricted to the RD Gateway role)
Server 2016
Server 2019

> RD Gateway is not supported in the IGEL RDP Legacy Mode.

Use other credentials for RD Gateway authentication:

☑ Uses custom data that can be defined below rather than the session access data.

- **Gateway user name**
- **Gateway password**
- **Gateway domain**

RDP Session Logon

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Logon**

Here, you can specify session-specific settings for login.

Use passthrough authentication for this session

☑ This option can be used if the local device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.

☐ The login data are not passed on. (Default)

User name: Name of the user

Password: Password of the user

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain: Windows domain

Window

Menu path: **Setup > Sessions> RDP > RDP-Sessions > [Session Name] > Window**

Here, you can specify the settings for the RDP session window.

- **Number of colours**
  Possible values:
  - Global setting
  - 256
  - Thousands
  - Millions
- **Window size**
  Possible values:
  - Global setting
  - Fullscreen: The session is shown on the full screen. The thin client's taskbar is not visible.
  - Workarea: The session is shown on the full screen, minus the area needed by the thin client's taskbar.
  - Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.
- **Desktop scale factor**: Specifies the desktop scaling in percent. This function is available from IGEL Linux *Version 10.02*.

  > Desktop scaling is supported from Windows Server 2012 or higher and from Windows 8.1 or higher.

  Possible values:
  - Global setting (default)
  - Automatic: The resolution set under **Setup > User Interface > Display > Options > Monitor-DPI** will be used for the RDP session.
  - Numeric details: The display will be magnified by the factor given here. Value range: 100% - 500%
- **Display resolution**
  Possible values:
  - Same as window size
  - Value selection: The session runs on the server side with the screen resolution selected here. The session will be shown on the thin client in the screen resolution set with the **Window size** parameter. If the screen resolution on the server side is smaller than the **Window size**, the display will be magnified accordingly and anti-aliasing may be used. Example: Applications that only work or work optimally with a specific screen resolution.
- **Start monitor**: Specifies the monitor on which the session is to start.
  - No configuration
  - Selects a specific monitor
- **Multi-monitor fullscreen mode**: This setting is relevant if more than one monitor is connected to the terminal:
  - Global setting

- Restrict fullscreen session to one monitor.
- Display fullscreen session on all monitors.
- Expand fullscreen session across all monitors.

Keyboard

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Keyboard**

Here, you can specify session-specific keyboard settings.

- **Keyboard map**
  Possible values:
  - Automatic
  - Country name
- **Override local window manager keyboard shortcuts**
  Possible values:
  - Global setting
  - On
  - Off

Mapping

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Mapping**

- **Enable COM port mapping**
  - Global setting:
  - On
  - Off
- **Enable drive mapping**
  - Global setting from **RDP Global > Mapping > Drive Mapping**
  - On
  - Off
- **Enable printer mapping**
  - Global setting from **RDP Global > Mapping > Printers**
  - On
  - Off
- **Enable plugin support**
  - Global setting from **RDP Global > Mapping > Drive Support**
  - Off
- **Enable client audio**
  - Global setting from **RDP Global > Mapping > Audio**
  - On
  - Off
- **Audio quality mode**
  - Global setting from **RDP Global > Mapping > Audio**
  - Automatic
  - High: High audio quality is favored.
  - Medium: Medium audio quality is favored.
  - Dynamic
- **Audio compression**
  - Global setting from **RDP Global > Mapping > Audio**
  - Automatic
  - On
  - Off
- **Audio capture**
  - Global setting from **RDP Global > Mapping > Audio**
  - On
  - Off
- **Enable clipboard**
  - Global setting from **RDP Global > Keyboard**
  - On
  - Off

Performance

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Performance**

- **Enable RemoteFX**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Hardware accelerated codecs AVC420/AVC444 (H.264)**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Disable wallpaper**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Do not show contents of window while dragging**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Disable menu and window animation**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Disable themes**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Disable cursor shadow**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Disable cursor settings**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Enable font smoothing**
  - Global setting from **RDP Global > Performance**
  - On
  - Off
- **Compression**
  - Global setting from **RDP Global > Performance**
  - On
  - Off

Options

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Options**

Here, you can specify the name and symbol for the RDP client.

- **Client name**: Specifies the name that is sent to the terminal server for identification purposes. Possible values:
  - Global setting: The setting from **RDP Global > Options** will be carried over.
  - Custom client name: The name given under **Custom client name** will be used as the client name.
  - MAC address: The MAC address of the computer will be used as the client name.
  - Host name: The name of the device specified under **Setup > Network > LAN Interfaces > Terminal name** will be used as the client name. See LAN Interfaces (see page 1899).
- **Custom client name**: Custom client name; if the field is empty, the MAC address will be used.
- **Collection**: The name of the Remote Desktop Services (RDS) collection to connect to.

  > Instead of the collection name, it is also possible to specify under **Collection** the token that directs the RDP client to a specific RDS collection. The token format is `tsv://MS Terminal Services Plugin.1.RDS collection name`. For more information, see FAQ: What Is the String for Token-Based Load Balancing? (see page 452).

- **Icon name**: File name of the icon without file extension. (Default: rdp)

USB Redirection

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > USB Redirection**

Native USB redirection

- Global setting: The settings from **RDP Global > Native USB Redirection** will be carried over.
- On: Native USB redirection is enabled.
- Off: Native USB redirection is disabled.

Further information regarding the global settings can be found under Native USB Redirection (see page 1330).

Multimedia

Menu path: **Setup > Sessions > RDP > RDP Sessions > [Session Name] > Multimedia**

- **Enalbe video redirection**
  - Global setting: The setting from **RDP Global > Multimedia** will be used.
  - On: Video redirection is enabled.
  - Off: Video redirection is disabled.

  Further information regarding the global settings can be found under Multimedia[166].

166. https://kb.igel.com/en/igel-os/11.10.250/multimedia-2

Desktop Integration

Menu path: **Sessions > RDP > RDP Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Remote Desktop Web Access

Menu path: **Sessions > RDP > Remote Desktop Web Access**

With Web Access for Remote Desktop (Web Access for RD), users can access RemoteApp and a Remote Desktop connection via the start menu on a computer or via a web browser.

RemoteApps and Remote Desktop connections therefore provide a modified view of RemoteApp programs and virtual desktops for users.

More information on Web access for Remote Desktop can be found under Microsoft Technet - Web Access for RDP[167].

The settings for launching the session are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

167. http://technet.microsoft.com/en-us/library/cc731923.aspx

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Desktop Integration (see page 1357)
- Authentication (see page 1360)
- Logoff (see page 1361)
- Server (see page 1363)
- Appearance of the Remote Desktop Web Access in IGEL OS (see page 1367)

Desktop Integration

Menu path: **RDP > Remote Desktop Web Access > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Authentication

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Authentication**

You can change login settings on the server and select applications that are launched automatically after logging in.

> The login settings on the server are only effective if **Sessions > RDP > Remote Desktop Web Access > Server > Server configuration** is set to **Predefined configuration**. Further information can be found under Server (see page 1363).

Authentication mode: Specifies how the user authenticates themselves on the server.
Possible values:

- "Passthrough authentication": This option can be used if the local endpoint device login takes place via Kerberos or Shared Workspace. The login data saved temporarily when logging in to the device will be used for the user name and password.
- "Auto logon": The login data in **Username**, **Password**, and **Domain** will be used to log in.
- "User logon": The user enters the data in a login window.

Username: User name when logging in to the server

Password: Password when logging in to the server

Domain: Domain in which the user name and password are valid

Save username and domain from the last login
Possible options:

- "Yes": The username and domain from the last login will be saved.
- "No": The username and domain from the last login will not be saved.
- "Legacy": It will be checked whether **Sessions > RDP > RDP Global > Local Logon > Preset login information** is enabled. If it is enabled, the saved data of **Local Logon** will be used also for RD Web Access.

To select an application for automatic launching, proceed as follows:

1. Click + in the **Start following applications automatically after server connection is established** area.
2. In the **Add** dialog, enter the name of the application. (Example: `Word 2013`)

   > You can also enter part of the name followed by an asterisk (`*`). If you enter e.g. `Word*`, all available versions of *Microsoft Word* as well as *Microsoft WordPad* will be opened.

3. Click on **Ok**.
   After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

Logoff

Menu path: **Setup > RDP > Remote Desktop Web Access > Logoff**

Here, you can specify how you would like to log off from the application.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Server

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

In this area, you can specify the server configuration.

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux endpoint device in the *Firefox* browser. See Via Browser (see page 1366).

Server configuration
Possible values:

- "Predefined configuration": You can define several server connections with the same user access data. The user must enter their access data and the domain in the login window. See Predefined Configuration (see page 1364).
- "Ask user": The connection is preconfigured on the server side. The user only needs to enter their corporate e-mail address. See Ask User (see page 1365).

Server location: These settings are needed if **Server configuration** is set to "Predefined configuration".

Protocol
Possible values:

- "http://"
- "https://"

RD Web Access Server: Name of the Web Access server

Path to web portal (Default: /rdweb/feed/webfeed.aspx)

Enable gateway support
Possible values:

- "Global settings"
- "Session settings"
- "Off"

Gateway address: If you would like to carry over the session settings, you must also specify the gateway address.

Domains: Domain of the Web Access server

- Predefined Configuration (see page 1364)
- Ask User (see page 1365)
- Via Browser (see page 1366)

Predefined Configuration

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

To predefine settings, proceed as follows:

1. Go to **Sessions > RDP > Remote Desktop Web Access > Server**.
2. Under **Server configuration**, select **Predefined configuration**.
3. Create a new session. See the Server (see page 1363) section regarding the session settings.
4. Select a login option under **Remote Desktop Web Access > Authentication**.
   If you have selected **Predefined configuration**, the **Passthrough authentication** mode will be available for logging in in addition to the normal user authentication process.
5. Under Desktop Integration (see page 1357) and Logoff (see page 1361), you can specify how you would like to log in and off.

   > You must make a setting for the login icon because this is not preconfigured and you will not otherwise have access to the Web Access logon.

The applications can be provided in the Application Launcher, in the start menu, in the quick start panel, or on the desktop. Under Appearance of the Remote Desktop Web Access in IGEL OS[168], you can choose from the list of available applications for display on the desktop or in the quick start panel.

168. https://kb.igel.com/en/igel-os/11.10.270/appearance-of-the-remote-desktop-web-access-in-ige

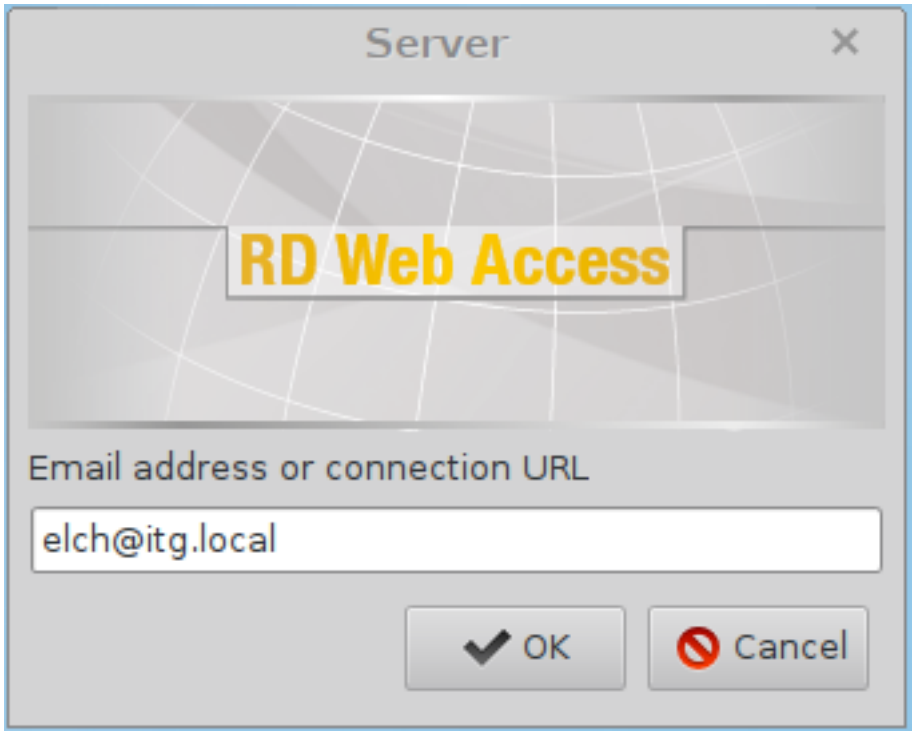
Ask User

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Server**

With this logon method, the network connections connected with the user name on the server side must be preconfigured and it must be possible to query them via DNS.

To configure access via **Ask user**, proceed as follows:

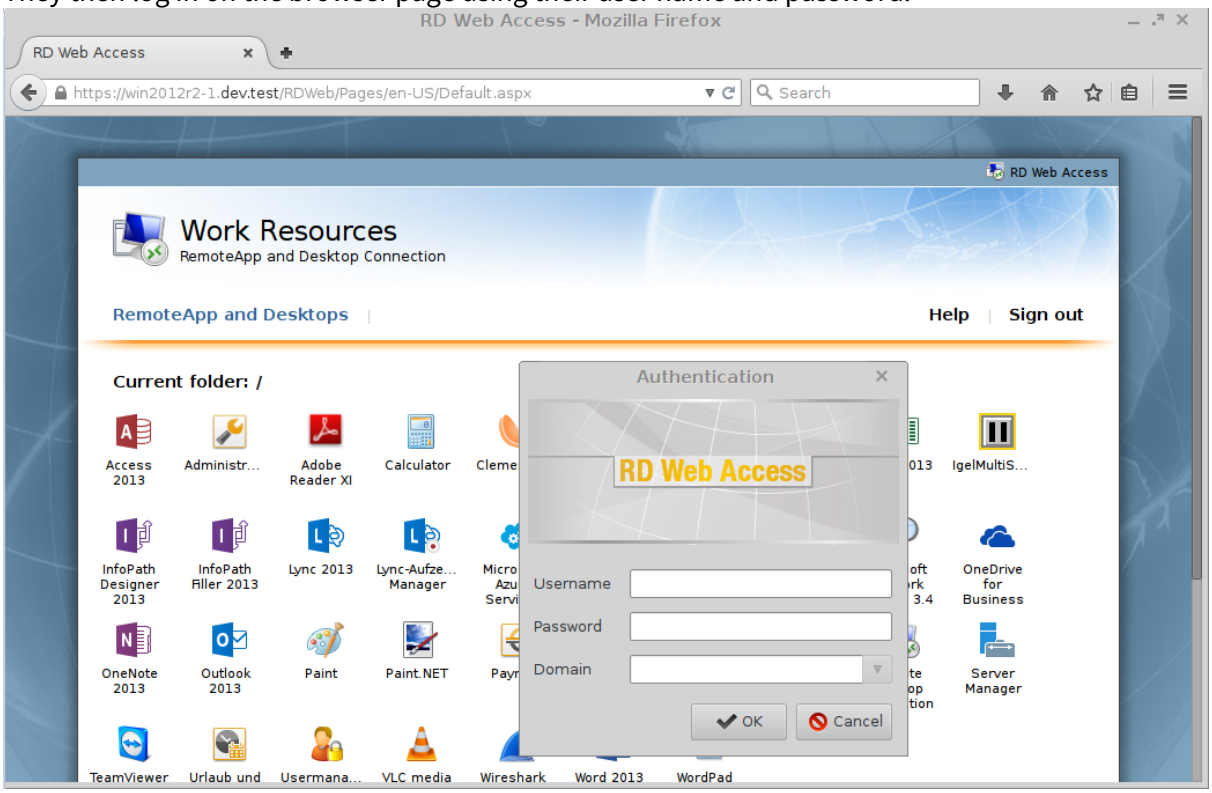
->Select **Ask user** under **RD Web Access > Server > Server configuration** menu.
The user is given a login window in which they enter their e-mail address consisting of `@`:



Via Browser

The Web Access page for *Windows Server 2012* and *Windows Server 2012 R2* can also be used on a Linux thin client in the *Firefox* browser.

- The user only needs the corresponding URL which is entered in the address bar.
- They then log in on the browser page using their user name and password.



If the user clicks one of the applications offered by Web Access, the thin client will open a logon mask and then a *Remote Desktop* session for the application chosen.

Appearance of the Remote Desktop Web Access in IGEL OS

Menu path: **Setup > Sessions > RDP > Remote Desktop Web Access > Appearance**

In this area, you can decide where you would like to display Remote Desktop Web Access applications.

Show applications in start menu

The applications are shown in the start menu. (Default)

Apply display filter to start menu entries

☑ Only the applications listed in the display filter will be shown in the start menu.

☐ All applications will be shown in the start menu. (Default)

Show applications in Application Launcher

☑ The applications are shown in Application Launcher. (Default)

Apply display filter to Application Launcher entries

☑ Only the applications listed in the display filter will be shown in the Application Launcher.

☐ All applications will be shown in the Application Launcher. (Default)

Show applications on desktop

☑ The applications will be shown on the desktop. (Default)

Apply display filter to desktop icons

☑ Only the applications listed in the display filter will be shown on the desktop.

☐ All applications will be shown on the desktop. (Default)

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Display filter: Show only the following applications

→ Via + , you can add applications to the display filter and determine display options for this selected group.

Enable following applications in Quick Start Panel

→ Via + , you can specify applications which will be added to the quick start panel.

Horizon Client Global

Menu path: **Sessions > Horizon Client > Horizon Client Global**

In this area, you can define the global settings for Horizon Client sessions.

The following setting is carried over from the global settings for RDP sessions if "RDP" is selected as a **preferred desktop protocol**, see Server Options for Horizon Sessions in IGEL OS (see page 1369) and Connection Settings (see page 1402):

- **Number of colors**; see Window (see page 1314)

- Server Options for Horizon Sessions in IGEL OS (see page 1369)
- Local Logon Options for Horizon Client in IGEL OS (see page 1371)
- Window (see page 1373)
- USB Redirection (see page 1374)
- Fabulatech USB Redirection for Horizon in IGEL OS (see page 1378)
- Fabulatech Scanner Redirection (see page 1386)
- Serial Port Redirection (see page 1387)
- Drive Mapping (see page 1388)
- Multimedia (see page 1389)
- Horizon Client Global Performance (see page 1390)
- Smartcard Middleware Settings for VMware Horizon Sessions in IGEL OS (see page 1391)
- Unified Communications Settings for VMware Horizon Sessions in IGEL OS (see page 1393)

Server Options for Horizon Sessions in IGEL OS

In this area, you can specify the settings for the connection between the server and the VMware Horizon Client that is built into IGEL OS.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Server Options**

Preferred desktop protocol

The selected option is preferred by the client when negotiating the connection protocol. If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- **Server setting**: The client does not provide the server details of a preferred connection protocol. The connection protocol preferred by the server is used.*
- **RDP**: The client tells the server that it prefers RDP as the connection protocol.
- **PCoIP**: The client tells the server that it prefers PCoIP as the connection protocol.
- **VMware Blast**: The client tells the server that it prefers VMware Blast as the connection protocol.

Hardware video acceleration can be used for VMware Blast. Information regarding hardware video acceleration on IGEL devices can be found under Hardware Video Acceleration on IGEL OS (see page 1180). If no hardware video acceleration is available, rendering will take place via software, without acceleration.

High Color Accuracy Mode

Enables H.264 encoding with High Color Accuracy in VMware Blast Sessions. The Horizon Client uses high color accuracy only if the agent supports it. On mobile devices that are running on battery, this feature might reduce battery life and performance.

☑ High color accuracy is allowed.

☐ High color accuracy is not allowed.*

Kiosk mode

☑ Horizon client sessions are held in kiosk mode.

As an alternative, you can also use the Appliance Mode (see page 1413).

☐ Horizon client sessions are held in normal mode.*

Server certificate verification mode

Specifies what will happen if server certificate verification fails.

Possible values:

- **Reject if verification fails**
- **Warn if verification fails***

See also Deploying Trusted Root Certificates in IGEL OS (see page 764).

- **Allow unverifiable connections**

Action to take in case there are running applications from previous sessions

Specifies the start behavior of an **application**-type session if applications from a previous session are still running. The session type is defined under **Sessions > Horizon Client > Horizon Client Session > [Session Name] > Connection Settings > Session Type**.

Possible values:

- **Ask to reconnect to open applications**: When the session starts, the user is asked whether they want to re-establish the connection. If the connection is reestablished, the applications running will be available. The applications will have the same status as when the connection was terminated.*
- **Reconnect automatically to open applications**: The connection will be re-established automatically. The application running will be available. The application will have the same status as when the connection was terminated.
- **Do not ask to reconnect and do not reconnect**: The connection will not be re-established.

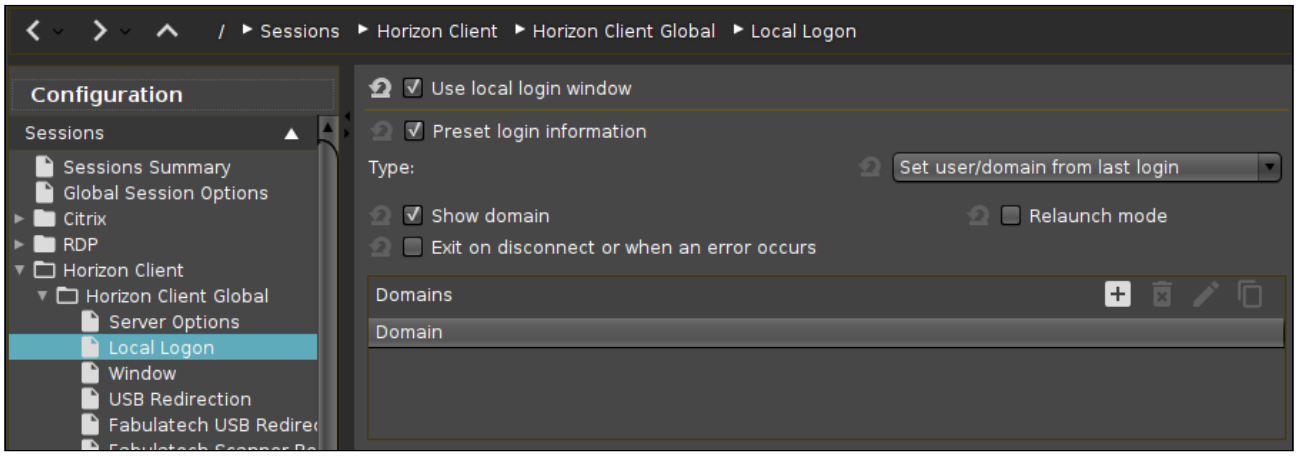
*IGEL OS system default

Local Logon Options for Horizon Client in IGEL OS

Using **Local Logon** settings, described in this article, you can prepopulate user data for VMware Horizon sessions. As a result, you can avoid users possibly having to log in a number of times.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Local Logon**

Local Logon Configuration for VMware Horizon



Use local login window

☑ The local login window of the endpoint device will be used to log in to the server. If you use the local login window, you can prepopulate login information.

☐ The local login window will not be used.*

Preset login information

☑ Login information will appear automatically in the login window. With **Type**, you can specify the source of the login information.*

Type

- **Set user/domain from last login**: The login information from the last session will appear automatically in the login window.*
- **Set user/domain from session setup**: Session-specific login information will appear automatically in the login window. The session-specific login information is described under Connection Settings (see page 1402).

Show domain

☑ The domain will be shown in the login window.*

Relaunch mode

☑ The login window is shown in relaunch mode and cannot be closed.

☐ The login window is not shown in relaunch mode.*

Exit on disconnect or when an error occurs

☑ The session will be ended completely when the connection is terminated.

☐ The connection overview will be shown when the connection is terminated.*

Domain

This is how you can work with the domain list:

->Click to add a new domain.

->Click to remove the selected domain.

->Click to edit the selected domain.

->Click to copy the selected domain.

Further settings options can be found under **Security >** **Active Directory / Kerberos** (see page 2014) and **Security > Logon >** **Active Directory / Kerberos** (see page 2034).

*IGEL OS system default

Window

Menu path: **Sessions > Horizon Client > Horizon Client Global > Window**

Window size: Specifies the width and height of the window.

Possible options:

- "Full-screen": The session is shown on the full screen. The device's taskbar is not visible.
- "Work area": The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Multimonitor full-screen mode - If more than one monitor is connected to the terminal:

- "Restrict full-screen session to one monitor"
- "Display full-screen session on all monitors"
- "Expand full-screen session across all monitors": The same as "Display full-screen session on all monitors"

USB Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > USB Redirection**

In this area, you can enable and configure USB redirection for specific devices. A USB composite device can be split into its components (interfaces). Example: USB dictation device that is split into the components loudspeaker, microphone, storage device/drive, and control buttons.

Ensure that the power supplied by the USB connection is adequate for the device.

If USB redirection is enabled, drive mapping should be disabled; see Drive Mapping (see page 1388). Otherwise, USB redirection can cause a storage device to be removed from the drive mapping. This is the case if the **Automatically connect when inserted** option is enabled.

You can change the following settings:

USB Redirection

- On
- Off

Automatically connect at startup

☑ USB devices that were inserted before the start of the session are available in the session. (default)

Automatically connect when inserted

☑ USB devices that are inserted during the session are available in the session. (default)

Default rule: This rule will apply if no special rule was configured for a class or a device.

- Allow
- Deny

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Automatic splitting of composite USB devices

☑ A USB composite device will automatically be split into its individual components (interfaces). The class rules will be applied to these individual devices.

☐ The device will not be split into its components.

Creating a Class Rule

1. To create a new rule, click + in the **Class Rules** area.
2. Choose a **Rule**. The rule specifies whether the use of the device class defined here is allowed or prohibited.
3. Under **Family**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Smartcard**, **Storage Devices**.
4. Under **Name**, give a name for the rule.

5. Click on **Ok**.
6. Click on **Apply** or **Ok**.
   The rule is active.

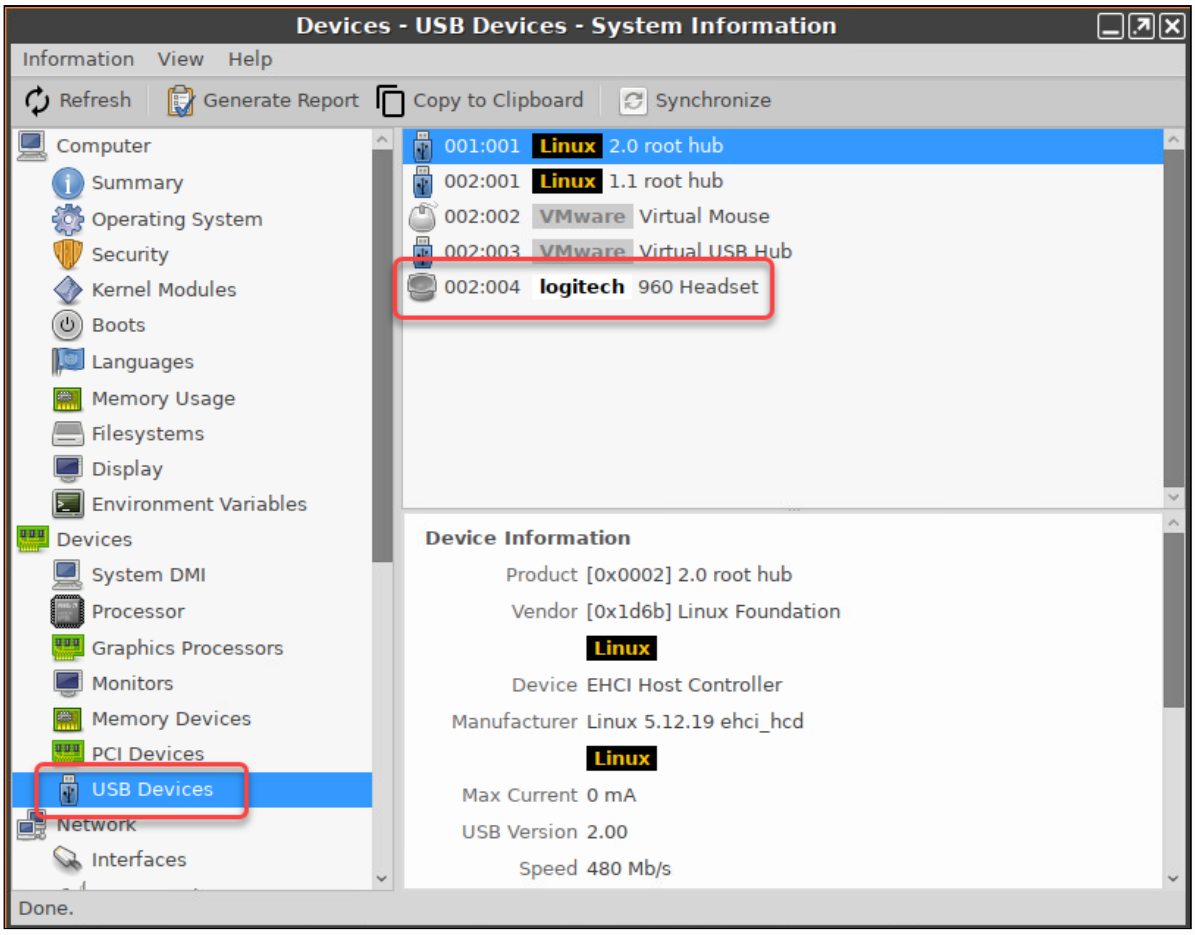
Creating a Device Rule

When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** must be given.

1. To create a new rule, click + in the **Device Rules** area.
2. Choose a **Rule**. The following rules are available:
   - Deny: The device will not be redirected via USB redirection.
   - Allow: The device will be redirected via USB redirection.
   - Split: A USB composite device will automatically be split into its individual components (interfaces).
   - No auto-split: A USB composite device will not be split.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value. The product ID can contain asterisks '*', each asterisk representing one hexadecimal digit. If the field is left empty, any product ID is matched.

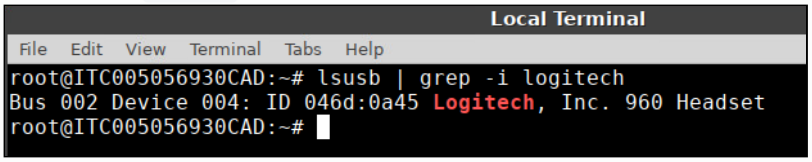
Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



5. Only for USB composite devices: Under **Interface Exclude List**, enter a list of interfaces that are to be excluded from USB redirection. The individual interfaces are separated by spaces. Example: "0 1".
6. Under **Name**, give a name for the rule.
7. Click on **Ok**.
8. Click on **Apply** or **Ok**.
   The rule is active.

See also an overview and best-practice recommendations for the use of webcams under Webcam Redirection and Optimization in IGEL OS (see page 1034).

Troubleshooting Topaz USB Not Passed through to Horizon on IGEL OS

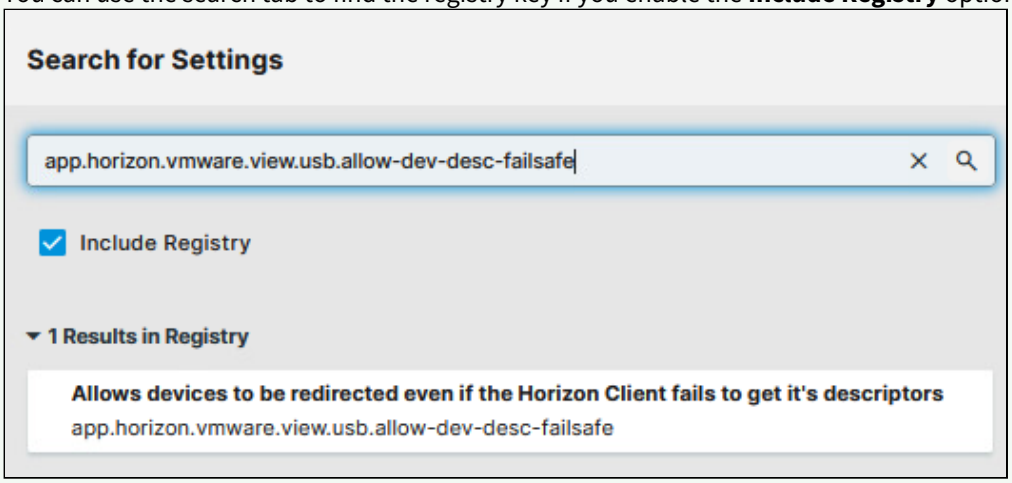
Problem

The Topaz USB device is not passing through to the Horizon VDI environment running on IGEL OS 11.

Solution

1. Enable the following setting in the system registry:
   `app.horizon.vmware.view.usb.allow-dev-desc-failsafe`

You can use the search tab to find the registry key if you enable the **Include Registry** option.



2. Apply the setting to the device.

3. Restart the session or restart the IGEL OS.

Fabulatech USB Redirection for Horizon in IGEL OS

The Fabulatech redirection of webcams and scanners as well as the common Fabulatech USB redirection can be enabled or disabled. The Fabulatech USB redirection can be controlled based on class rules and device rules. The use of rules is described in detail under USB Access Control (see page 2010).

Important Notes

- For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see http://www.usb-over-network.com/partners/igel/. For details on the configuration, see https://www.usb-over-network.com/partners/igel/usb-for-remote-desktop-docs.html. Please note that licenses must be purchased from Fabulatech to enable this functionality.
- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech USB Redirection**

Fabulatech USB Redirection

☑ Fabulatech USB Redirection is used.

☐ Fabulatech USB Redirection is not used.*

Default rule

This rule will apply if no special rule was configured for a class or a device.
Possible options:

- Deny*
- Allow

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

Create a new entry.

Remove the selected entry.

Edit the selected entry.

Copy the selected entry.

The class rule properties are described in the following.

Rule

Possible options:

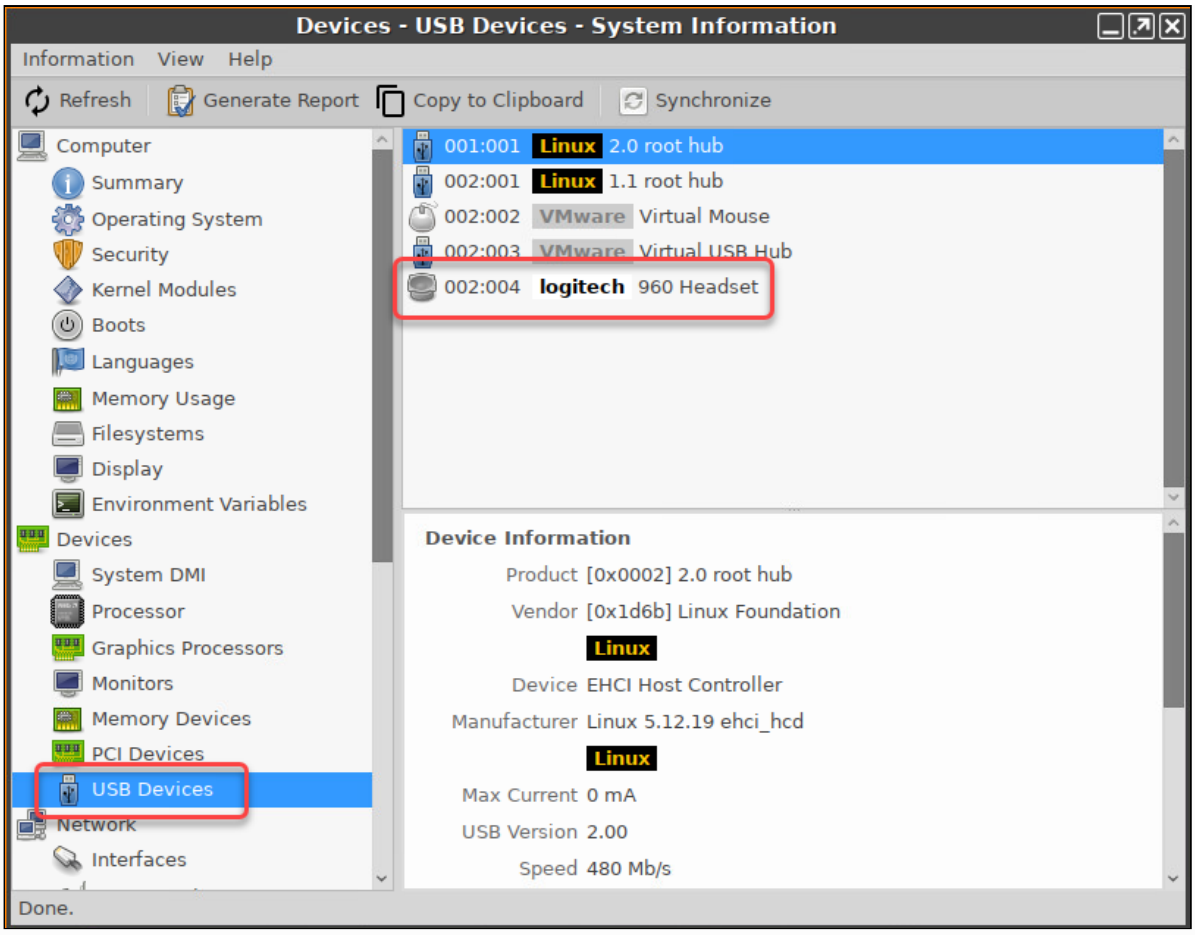
- Deny: Devices that have the properties defined here are not redirected.
- Allow: Devices that have the properties defined here are redirected by the **Fabulatech USB Redirection**.*

Class ID

Device class

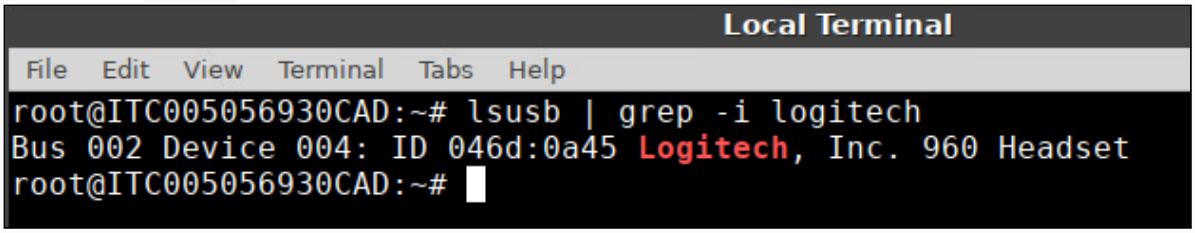
Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



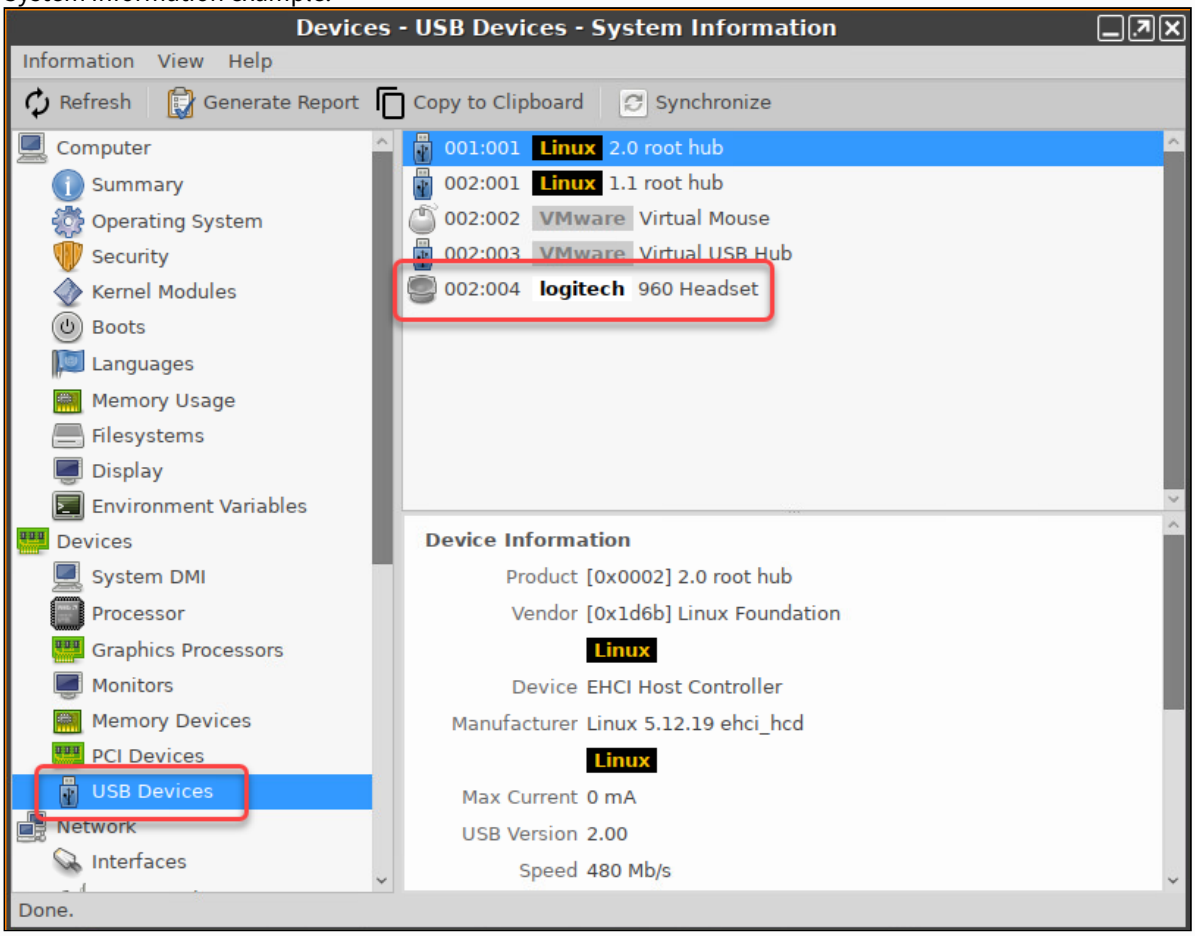
Subclass ID

Subclass relating to the specified device class

Getting USB Device Information

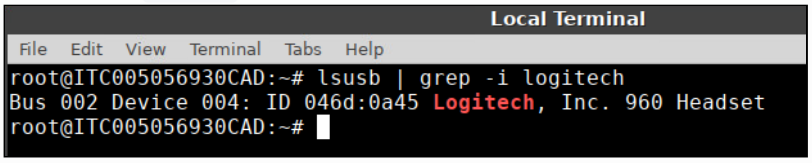
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name

Free text entry

Override serial

Serial number that will appear in the session

Override name

Device name that will appear in the session

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts.

☐ The USB device is no longer shown immediately after the system is booted.*

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device).

☐ The USB device may not be removed.*

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated.

☐ The device will be reset after the connection with the session has been terminated.*

Device Rules

A device rule applies to a specific device that is identified by its serial number.

The device rule settings are described in the following.

Rule

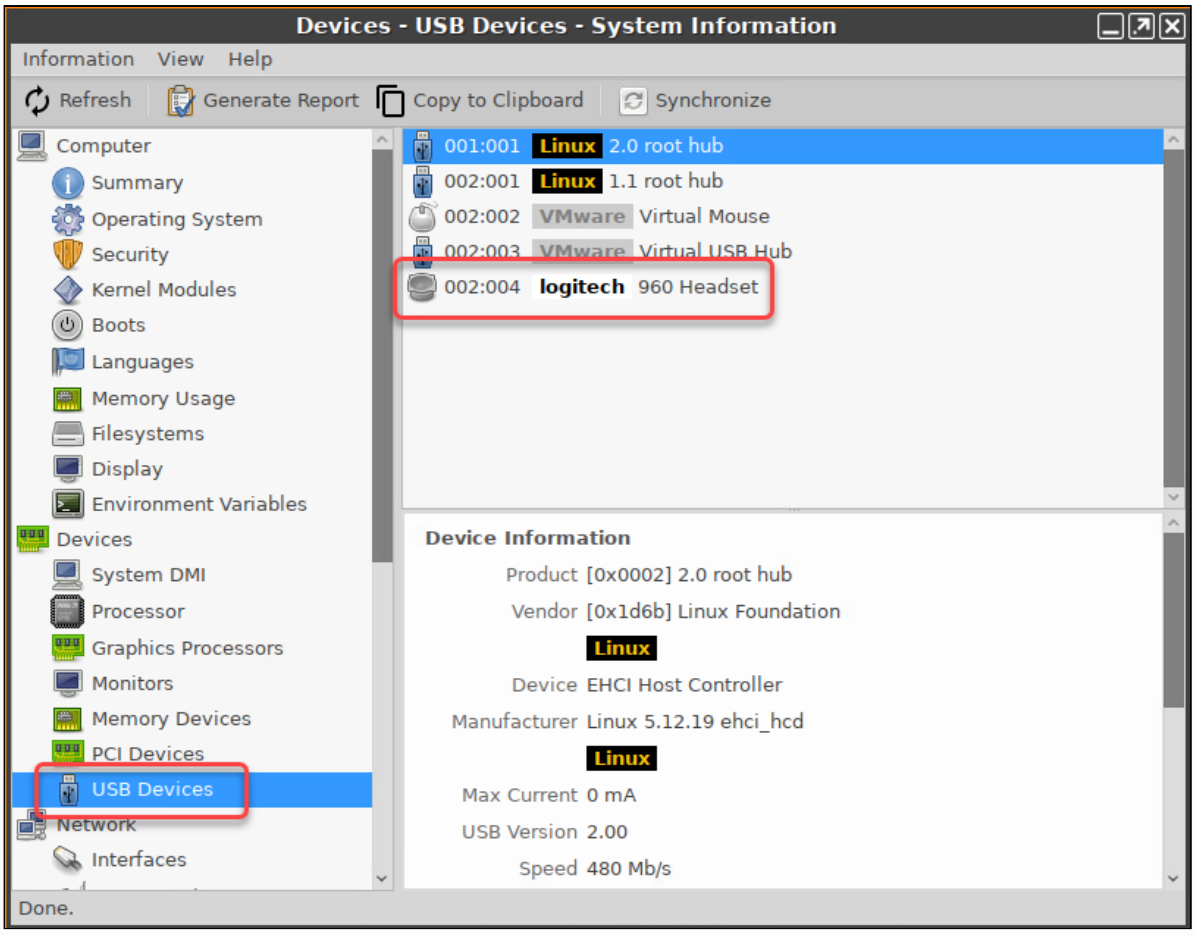
Possible options:

- Deny: The device will not be redirected via Fabulatech USB Redirection.
- Allow: The device will be redirected via Fabulatech USB Redirection.*

Vendor ID

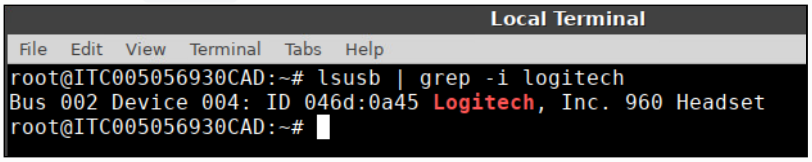
Hexadecimal manufacturer number

> Getting USB Device Information
>
> To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
> System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



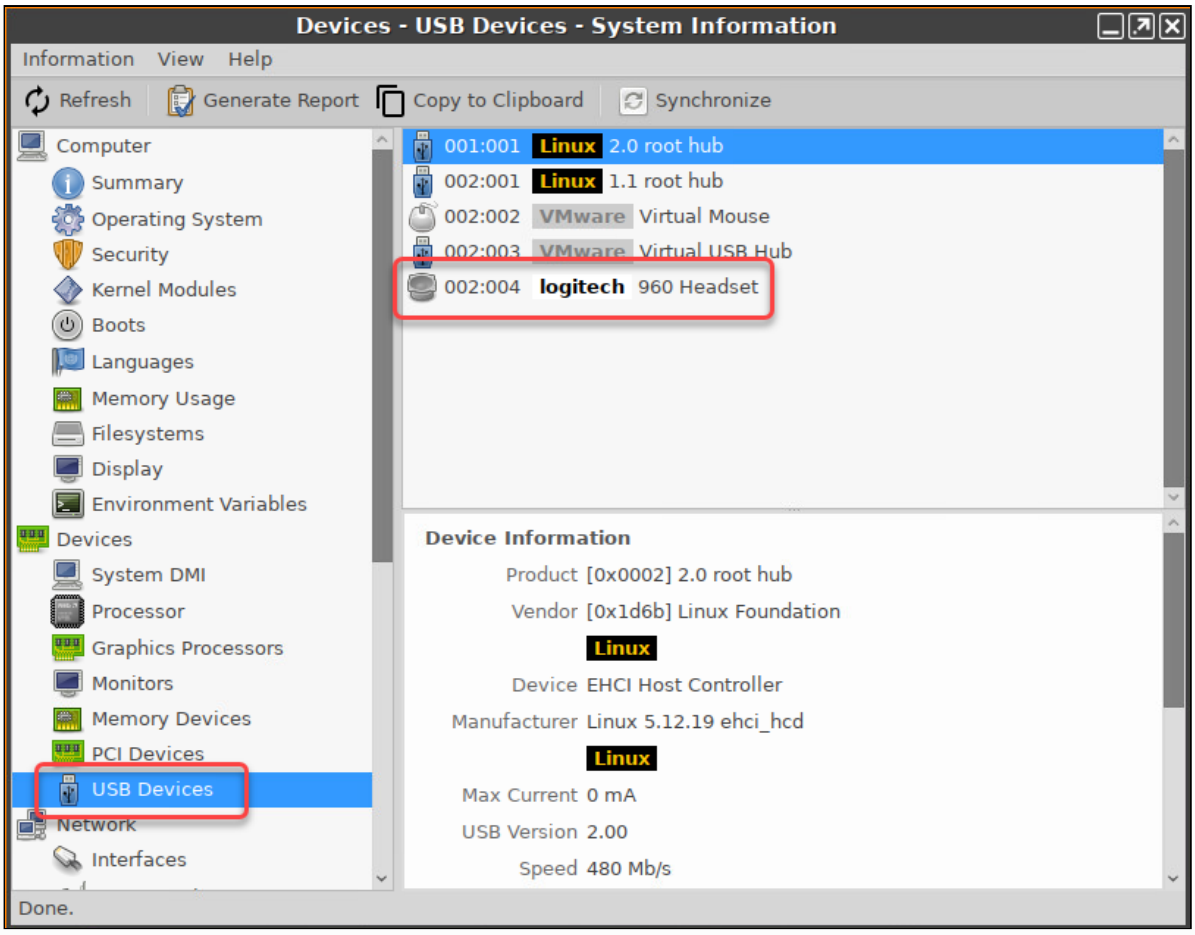
Product ID

Hexadecimal device number

Getting USB Device Information

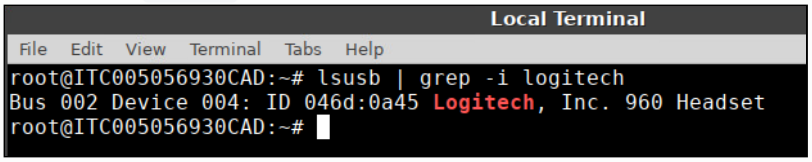
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name

Free text entry

Override serial

Serial number that will appear in the session.

Override name

Device name that will appear in the session.

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts.*

☐ The USB device is no longer shown immediately after the system is booted.

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device).*

☐ The USB device may not be removed.

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated.*

☐ The device will be reset after the connection with the session has been terminated.

*IGEL OS system default

Fabulatech Scanner Redirection

Menu path: **Sessions > Horizon Client > Horizon Client Global > Fabulatech Scanner Redirection**

You can enable or disable Fabulatech scanner redirection.

Fabulatech Scanner for Remote Desktop

☑ Fabulatech scanner redirection is enabled.

Serial Port Redirection

Serial Port Redirection

With the serial port redirection feature, youcan redirect locally connected serial (/dev/ttyS) ports, such as built-in RS232 ports or USB-to-Serial adapters, to their RDS-hosted desktops.

☑ Serial Port Redirection is enabled.

☐ Serial Port Redirection is disabled. (Default)

Drive Mapping

Menüpfad: **Horizon Client > Horizon Client Global > Drive Mapping**

Through drive mapping, connected mass storage devices can be made available in the session. Specify which folders or drives are mapped during the login.

Enable Drive Mapping

☑ Drive mapping is enabled. (Default)

Local (USB) devices which are to be used for drive mapping purposes must first be set up as devices. See Storage Hotplug (see page 1969).

Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on ⏏ in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see In-Session Control Bar (see page 1872).
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

- **Drive Mapping**: List of mapped drives.

To set up drive mapping, proceed as follows:

1. Click ➕ **Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Select a **Drive to map** from the list under which the local device or the folder is to be mapped.

If the drive letter you have selected is no longer available on the server, the specified directory or local drive will be given the next free letter during the login.

4. Give the **Local Drive Path** of the local directory to which the mapping is to refer.

If you map a locally connected device, use the pre-defined path names available in the drop-down field. The directories in question are those on which the devices are mounted by default during the boot procedure (e.g. `/autofs/floppy` for an integrated floppy drive).

Multimedia

Menu path: **Sessions > Horizon Client > Horizon Client Global > Multimedia**

You can change the following multimedia settings:

VMware Multimedia Redirection
Possible values:

- Off: The server renders the multimedia data and sends the individual images to the client.
- On: The client renders the multimedia data supplied by the server.

Real Time Audio Video (RTAV): Specifies the redirection of video data from the client USB webcam.
Possible values:

- Off: The client does not forward the webcam data as video data.

> With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled.
> For an overview and best-practice recommendations for the use of webcams, see Webcam Redirection and Optimization in IGEL OS (see page 1034).

- On: The client forwards the webcam data as video data.

Horizon Client Global Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Global > Performance**

In this area, you can optimize the performance of *Horizon Client* sessions.

You can change the following settings:

PCoIP client-side image cache size: Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred.
Possible values:

- 50 MB
- 100 MB
- 150 MB
- 200 MB
- 250 MB
- 300 MB

Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

Lakeside SysTrack

☑ The Lakeside SysTrack is enabled.

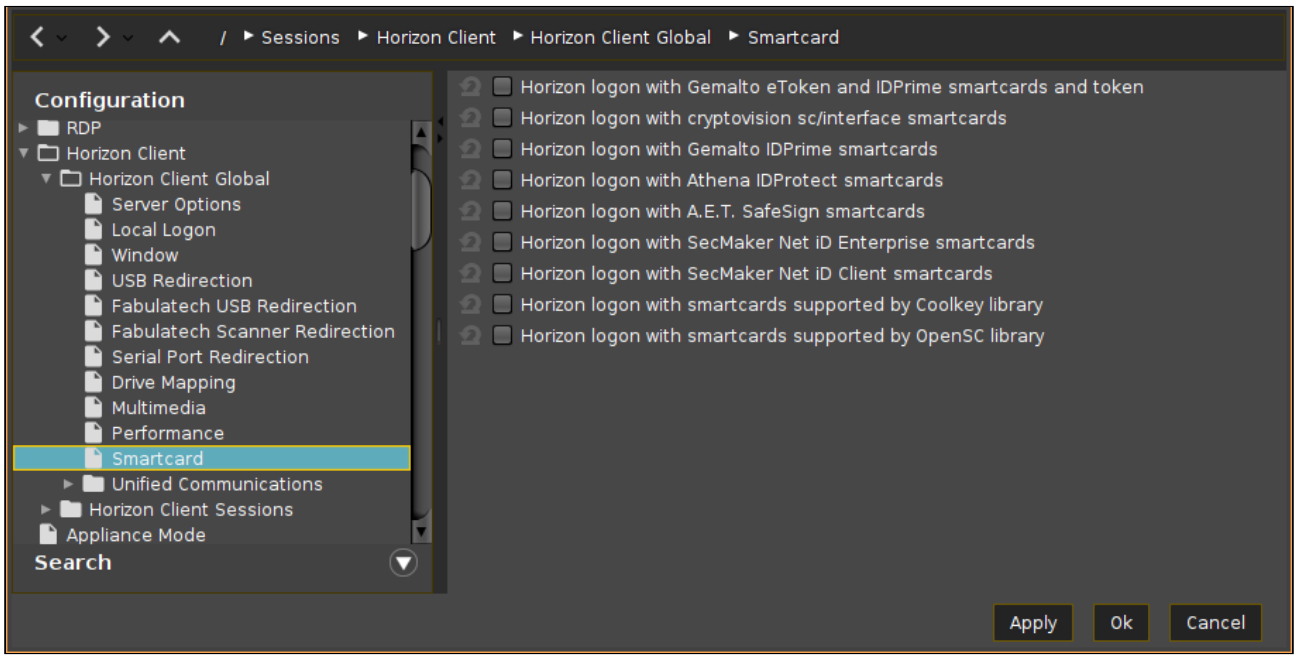
☐ The Lakeside SysTrack is not enabled. (Default)

Smartcard Middleware Settings for VMware Horizon Sessions in IGEL OS

When configuring login with a smartcard, you have to define smartcard middleware to be used. In this area of the IGEL Setup, you select the middleware (PKCS#11 module) which matches your card or your token. If you want to use your own PKCS#11 library with VMware Horizon, see Using a Custom PKCS#11 Library (see page 922).

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS (see page 791).

Menu path: **Sessions > Horizon Client > Horizon Client Global > Smartcard**



Horizon logon with Gemalto eToken and IDPrime smartcards and token

☑ The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is used.

☐ The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and tokens is not used.*

Horizon logon with cryptovision sc/interface smartcards

☑ The middleware for cryptovision sc/interface smartcards is used.

☐ The middleware for cryptovision sc/interface smartcards is not used.*

Horizon logon with Gemalto IDPrime smartcards

> Activate this Gemalto middleware if you want to use Gemalto common criteria devices in unlinked mode.

☑ The middleware for Gemalto IDPrime smartcards is used.

☐ The middleware for Gemalto IDPrime smartcards is not used.*

Horizon logon with Athena IDProtect smartcards

☑ The middleware for Athena IDProtect smartcards is used.

☐ The middleware for Athena IDProtect smartcards is not used.*

Horizon logon with A.E.T. SafeSign smartcards

☑ The middleware for A.E.T. SafeSign Smartcards is used.

☐ The middleware for A.E.T. SafeSign Smartcards is not used.*

Horizon logon with SecMaker Net iD Enterprise smartcards

☑ The SecMaker Net iD Enterprise middleware, formerly known as "SecMaker Net iD", is used.

☐ The SecMaker Net iD Enterprise middleware is not used.*

Horizon logon with SecMaker Net iD Client smartcards

☑ The SecMaker Net iD Client middleware is used. SecMaker Net iD Client is the next generation of Net iD Enterprise, see http://docs.secmaker.com/net-id-client/latest/index.html.

☐ The SecMaker Net iD Client middleware is not used.*

Horizon logon with smartcards supported by Coolkey library

☑ The Coolkey middleware is used.

☐ The Coolkey middleware is not used.*

Horizon logon with smartcards supported by OpenSC library

☑ The OpenSC middleware is used.

☐ The OpenSC middleware is not used.*

Horizon logon with smartcards supported by 90meter library

> This feature requires an add-on license; see *IGEL Subscription and More* > *IGEL Software License Overview* > *Add-on Licenses*. Please contact your IGEL reseller.

☑ The 90meter middleware is used.

☐ The 90meter middleware is not used.*

* IGEL OS system default

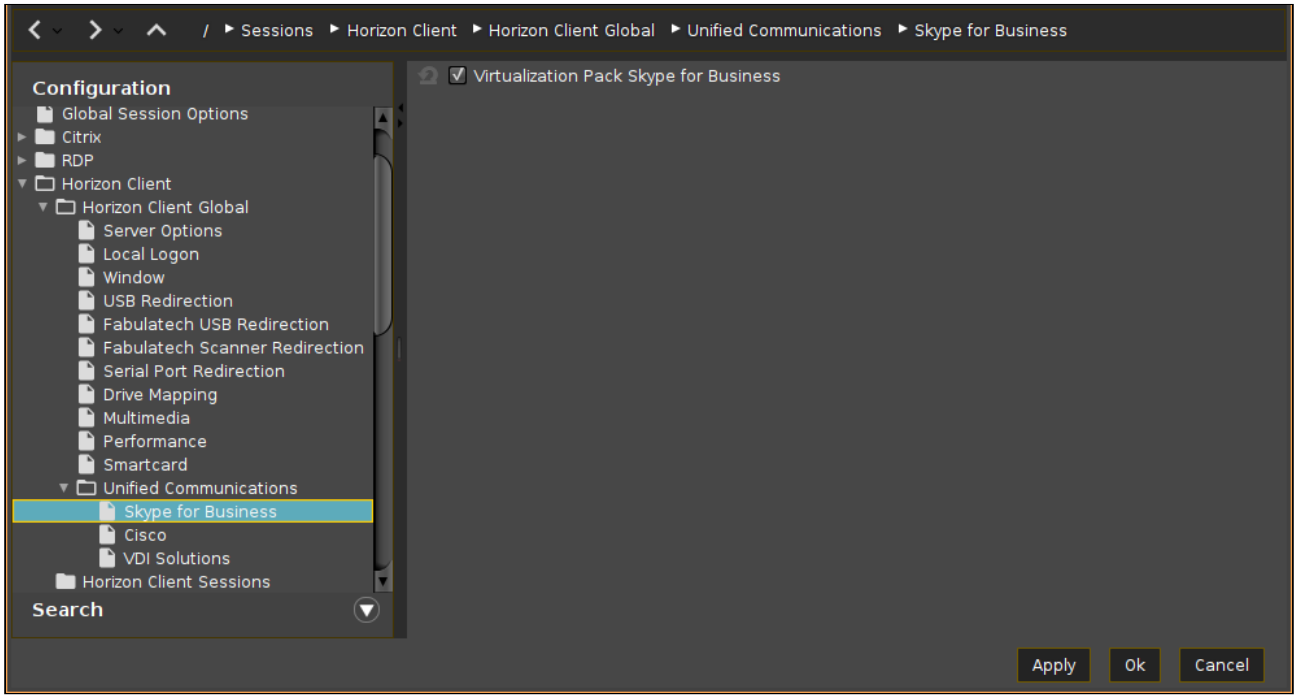
Unified Communications Settings for VMware Horizon Sessions in IGEL OS

This article shows you how to use the IGEL OS unified communications settings for VMware Horizon sessions. It is necessary to set some additional parameters in IGEL OS to leverage the VMware Horizon-related multimedia enhancements. These parameters and their functions are explained below.

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications**

Skype for Business

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**



Server and Network Requirements
Skype for Business optimization requires additional configuration on the server side. For more information, see the VMware article Configuring VMware Virtualization Pack for Skype for Business[169].

Virtualization Pack Skype for Business

☑ The Virtualization Pack Skype for Business is active.*

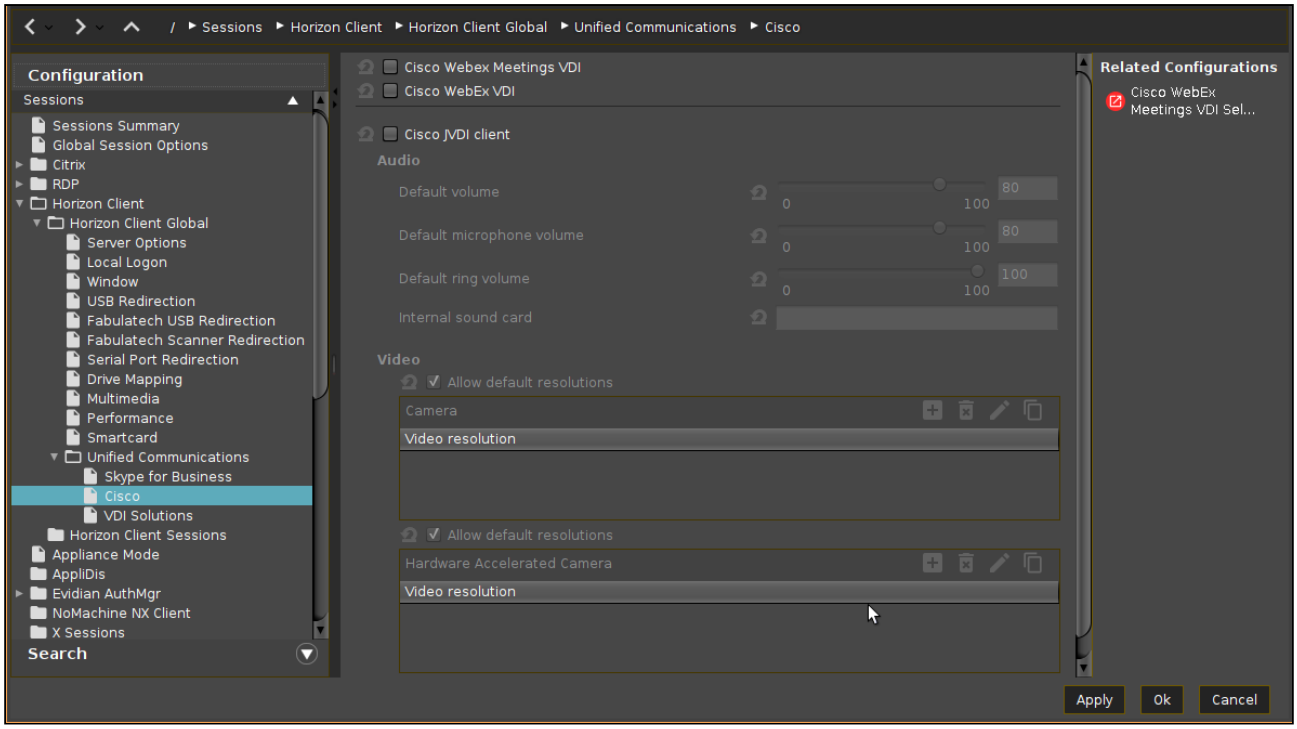
☐ The Virtualization Pack Skype for Business is not active.

Cisco

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco**

169. https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-remote-desktop-features/GUID-ABE8ACEE-02DE-4F1C-99D8-6B589E1762E9.html

Here you can activate or deactivate the virtual desktop optimization for Cisco Webex and define settings for the Cisco JVDI client.



Cisco Webex Meetings VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly between the endpoint devices and Webex Meetings cloud, without going through the hosted virtual desktop in the datacenter.

The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see Webex Meetings VDI Release Notes[170].
To select the version of the Cisco Webex Meetings plugin:

1. In the UMS configuration dialog or the local Setup, go to **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection > Cisco Webex Meetings client version**.
   (If you do not see the corresponding version in the UMS configuration dialog, but it is listed in the release notes, please update the firmware your profile is based on.)
2. Select the desired version and click **Apply** or **Ok**.

For further information, see the Cisco documentation for Webex Meetings:

- General information: https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software

170. https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5

- Administration guide: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8.html[171]
- Installation: https://www.cisco.com/c/en/us/td/docs/collaboration/webex_vdi/admin/webex_b_admin-cisco-wmvdi-40-8/webex_m_wvdi-software-installation.html

☑ The Cisco Webex Meetings VDI solution is enabled.

☐ The Cisco Webex Meetings VDI solution is disabled.*

Cisco Webex VDI

This virtual desktop optimization contains a media engine and redirects the audio and video streams so that they are exchanged directly, without going through the hosted virtual desktop in the datacenter.

For further information, see the Cisco documentation for Webex VDI:

- General information: https://www.cisco.com/c/dam/en_us/solutions/collaboration/docs/cisco-webex-teams-solution-overview.pdf
- Overview about the supported versions: https://help.webex.com/en-us/ntp1us7/Webex-VDI-Release-Notes#Cisco_Reference.dita_13d9aace-b6f9-41dc-a6e0-9f7a48834060
- Administration guide: Administration - Webex App | Installation and Automatic Upgrade[172]
- Installation: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide.pdf

☑ The Cisco Webex VDI solution is enabled.

☐ The Cisco Webex VDI solution is disabled.*

Cisco JVDI Client

For the vendor documentation for the Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0[173].

☑ The Cisco JVDI Client is enabled.

☐ The Cisco JVDI Client is disabled.*

If you do not see the option **Cisco JVDI Client**, check if the **Cisco JVDI Client** is enabled under **System > Firmware Customization > Features**. Reboot the device if required.
If you have reduced the IGEL OS feature set before and cannot activate **Cisco JVDI Client**, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

171. https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cisco.com%2Fc%2Fen%2Fus%2Ftd%2Fdocs%2Fcollaboration%2Fwebex_vdi%2Fadmin%2Fwebex_b_admin-cisco-wmvdi-40-8.html&data=04%7C01%7Cfeeney%40igel.com%7Cbbb4ae6a9db34ec84a0b08d88cee6ac9%7C3f04441122ea4ba182dfd85e25879b4f%7C0%7C0%7C637414302911303723%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=NrHywiQaoFcqcl5f%2FCRgK2BJw7%2BFfWirNQNj4MYTz0s%3D&reserved=0
172. https://help.webex.com/en-US/article/nw5p67g/Webex-App-%7C-Installation-and-Automatic-Upgrade
173. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html

Audio

Default volume

Headphone volume control. (Default: 80%)

Default microphone volume

Microphone volume control. (Default: 80%)

Default ring volume

Ringtone volume control. (Default 100%)

Internal sound card

Here you have the possibility to define a sound card. If you leave the field empty, the default sound card of the system is used.

For further information, see Sound Preferences (see page 1744).

Video

You can set the Cisco JVDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

Allow default resolutions (for cameras without hardware resolution)

☑ The default resolutions of the camera are used.*

☐ A user-defined set of resolutions is used. You can add a resolution by clicking + in the **Camera** area and selecting the desired resolution.

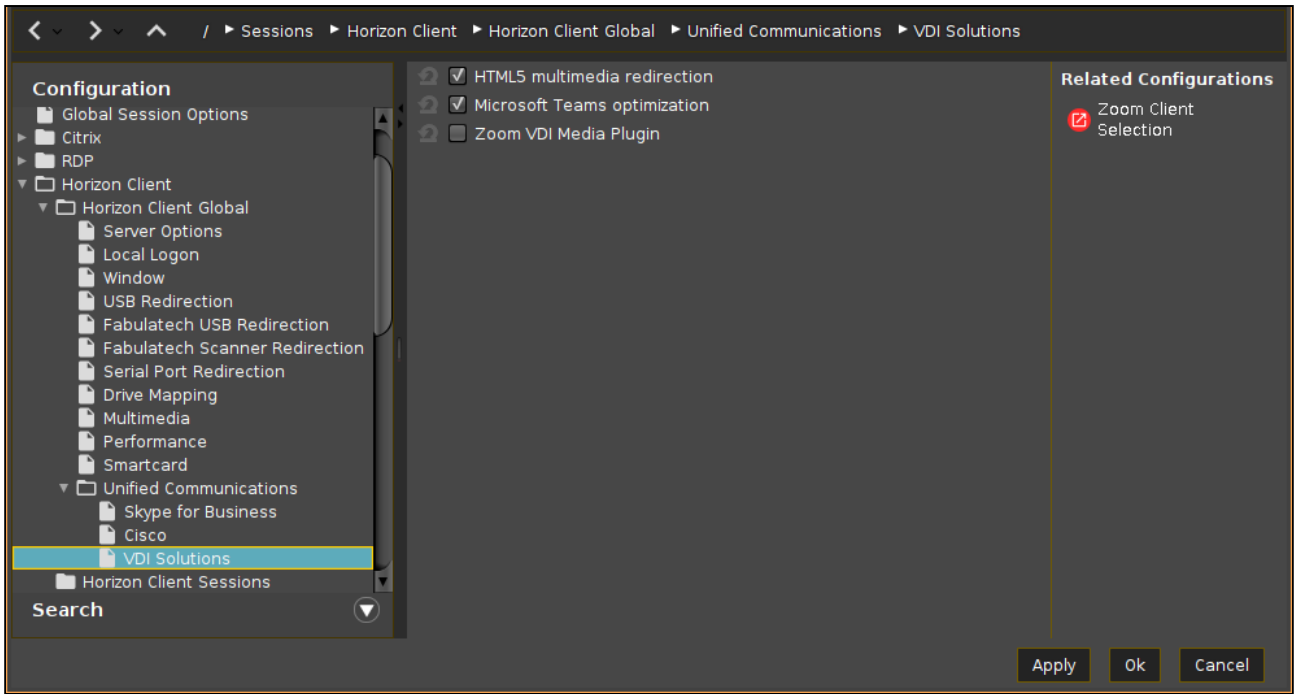
Allow default resolutions (for cameras with hardware resolution)

☑ The default resolutions of the camera are used.*

☐ A user-defined set of resolutions is used. You can add a resolution by clicking + in the **Hardware Accelerated Camera** area and selecting the desired resolution.

VDI Solutions

Menu path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions**



HTML5 multimedia redirection

> **Server and Browser Requirements**
> HTML5 multimedia redirection requires additional configuration on the server side. For more information, see the VMware article Configuring HTML5 Multimedia Redirection[174].

☑ HTML5 multimedia content is redirected from a remote desktop to the endpoint devices.*

☐ HTML5 multimedia content is not redirected.

Microsoft Teams optimization

> **Server and Network Requirements**
> Microsoft Teams optimization requires additional configuration on the server side. For more information, see the VMware articles Microsoft Teams Optimization with VMware Horizon[175] and Configuring Media Optimization for Microsoft Teams[176].

☑ The audio and video streams for Microsoft Teams are redirected to the endpoint devices. Audio and video data are not processed by the server.*

☐ The audio and video streams for Microsoft Teams are not redirected.

174. https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-remote-desktop-features/GUID-6A68ECA4-6B9C-43C5-B437-D39B71005BAD.html
175. https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon
176. https://docs.vmware.com/en/VMware-Horizon/2106/horizon-remote-desktop-features/GUID-F68FA7BB-B08F-4EFF-9BB1-1F9FC71F8214.html

Zoom VDI Media Plugin

Server and Network Requirements
Zoom optimization requires additional configuration on the server side. For more information, see the Zoom articles Getting started with VDI[177] and Mass deployment with preconfigured settings for Windows[178].

☑ The audio and video streams for Zoom are redirected to the endpoint devices. Audio and video data are not processed by the server.

☐ The audio and video streams for Zoom are not redirected.*

The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article VDI backwards compatibility[179].
You can select the Zoom VDI Media Plugin version under **Sessions > Unified Communications > Zoom Client Selection > Zoom client version**.

Related Topics

Webcam Redirection and Optimization in IGEL OS (see page 1034)

Which Unified Communication Solutions Does IGEL OS Support? (see page 1163)

*IGEL OS system default

177. https://support.zoom.us/hc/en-us/articles/360031096531-Erste-Schritte-mit-VDI
178. https://support.zoom.us/hc/en-us/articles/201362163-Mass-Installation-and-Configuration-for-Windows
179. https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility

Horizon Client Session

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name]**

You can configure one or more Horizon Client sessions.

The settings for launching the session are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Connection Settings (see page 1402)
- Window (see page 1403)
- Horizon Client Sessions Mouse and Keyboard (see page 1404)
- Mapping (see page 1405)
- Performance (see page 1406)
- Options (see page 1407)
- Horizon Client Sessions Multimedia (see page 1408)
- Proxy (see page 1409)
- Desktop Integration (see page 1410)

Connection Settings

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings**

In this area, you can specify the settings for the connection between the *Horizon Client* and the server.

- **Server URL**: URL of the *VMware Horizon* server
- **Use passthrough authentication for this session**
  ☑ The user name and password are temporarily saved and used for authentication purposes in this session.
  ☐ Passthrough authentication is not used. (default)
- **User name**: User name when logging on to the *VMware Horizon* server
- **User password**: Password when logging on to the *VMware Horizon* server
- **Domain**: Domain when logging on to the *VMware Horizon* server
- **Session type**: Specifies whether the session contains a desktop or an individual application.
  Possible values:
  - Desktop: The session contains a desktop.
  - Application: The session contains an individual application.
- **Desktop name**: Specifies a name for the desktop. This option is available if **Session Type** is set to “Desktop”.
- **Application**: Application that is launched during the session. This option is available if **Session Type** is set to “Application”.
- **Autoconnect**
  ☑ When the session starts, the connection to the desktop or application will automatically be established. For this to be possible, the name of the desktop or application must be defined.
  ☐ When the session starts, the overview will be shown. (default)
- **Preferred desktop protocol**: The selected option is preferred by the client when negotiating the connection protocol.
  Possible values:
  - Global setting
  - Server setting
  - RDP
  - PCoIP
  - VMWare Blast
- **Enable kiosk mode**
  - Global setting
  - On
  - Off

  Further settings options can be found under AD/Kerberos Configuration (see page 2014).

Window

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Window**

In this area, you can change the way in which the session is displayed.

Window size: Specifies the width and height of the window.
Possible values:

- Global setting: The window size is carried over from the global settings for Horizon Client sessions, see Window (see page 1373).
- Fullscreen: The session is shown on the full screen.
- User selection
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Number of colors: Specifies the color depth.

- Global setting: The color depth is carried over from the global settings for RDP sessions, see Window (see page 1314).
- 256
- Thousands
- Millions

Start monitor: Specifies the monitor on which the session is shown.

Horizon Client Sessions Mouse and Keyboard

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mouse and Keyboard**

In this area, you can define the settings for the mouse and keyboard.

Disable Mouse Motion Events

☑ The mouse pointer will only be shown locally on the thin client. If the user moves the mouse over a session item, no reaction of the item will be shown.

Further settings options can be found in the user interface setup area under Language Settings for IGEL OS 11 (see page 1845) as well as Keyboard (see page 1874) and Additional Keyboard Layouts (see page 1875).

Mapping

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Mapping**

In this area, you can specify the data transmission between the thin client and *Horizon Client* session.

> These settings only apply to RDP-based sessions.
> ->Check whether **Sessions > Horizon Client Sessions > Horizon Client Session > Connection Settings > Preferred Connection Protocol** selection is set to "RDP".

- **Enable Client Audio**
  - Global setting
  - On - enhanced
  - On - secure
  - Off
- **Enable Clipboard**
  - Global setting
  - On
  - Off
- **Enable Printer Mapping**
  - Global setting
  - On
  - Off
- **Enabling COM Port Mapping**
  - Global setting
  - On
  - Off
- **Enable Drive Mapping**
  - Global setting
  - On
  - Off
- **Enable USB Redirection**
  - Global setting
  - Off

  Further settings options can be found in the RDP Global setup area under Drive Mapping (see page 1388), COM Ports (see page 1258), Printers Mapping (see page 1321), Audio (see page 1324), Keyboard (see page 1874) and in the Devices area under Printer (see page 1974).

Performance

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Performance**

In this area, you can save system resources by disabling certain visual functions of the user interface.

- **Disable wallpaper**:
  - On: No desktop background image is shown.
- **Do not show contents of window while dragging**:
  - On: The content of a window will not be shown while the window is being moved.
- **Disable menu and window animation**:
  - On: Transitions for menus and windows will not be animated.
- **Disable themes**:
  - On: No optional desktop theme can be used.
  - Off: An optional desktop theme can be used.
- **Disable cursor shadow**:
  - On: The mouse pointer will be shown without a shadow.
  - Off: The mouse pointer will be shown with a shadow.
- **Disable cursor settings**
  - On: The mouse pointer settings cannot be changed.
  - Off: The mouse pointer settings can be changed.
- **Enable font smoothing**:
  - Global setting: The setting under Sessions > Horizon Client > Horizon Client Global will be used.
  - On: Edges will be smoothed when text is displayed.
  - Off: Edges will not be smoothed when text is displayed.

  Further settings options can be found in the Horizon Global setup area under Horizon Client Global Performance (see page 1390) and in the RDP Global area under Performance (see page 1325).

Options

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Options**

In this area, you can change the following settings:

- **Working directory**: Directory that is used after logging on
- **Compression**:
  - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
  - On: The data flow between the client and server will be compressed.
  - Off: The data flow will not be compressed.
- **Enforce TLS-encrypted connections**:
  - Global setting: The setting from **Setup > Sessions > Horizon Client > Horizon Client Global** will be carried over.
  - On: Encryption of the connection with TLS will be forced.
  - Off: Encryption will not be forced.
- **Network level authentication**:
  - On: The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.

> If network level authentication is enabled, the local logon window is used. This also applies if the **Use local logon window** option under **Setup > Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

  - Off: Conventional authentication
- Further settings options can be found in the RDP Global setup area under Options (see page 1329), Performance (see page 1325) and in the Horizon Global area under Local Logon Options for Horizon Client in IGEL OS (see page 1371).

Horizon Client Sessions Multimedia

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Multimedia**

You can change the following multimedia setting:

- **Enable VMware multimedia redirection**
  Possible values:
  - Global setting: The setting under **Sessions > Horizon Client > Horizon Client Global** will be used.
  - off: The server renders the multimedia data and sends the individual images to the client.

Proxy

Menu path: **Setup > Sessions > Horizon Client > Horizon Client Sessions > [Session Name] > Proxy**

In this area, you can configure the use of a proxy for the connection between the client and server.

You can change the following settings:

Direct connection to the Internet

☑ No proxy will be used.

Manual proxy configuration

☑ A proxy will be used. The configuration must be specified in the following fields.

- **HTTP proxy**: URL of the proxy for HTTP
- **Port**: Port of the proxy for HTTP
- **SSL proxy**: URL of the proxy for SSL
- **Port**: Port of the proxy for SSL
- **SOCKS host**: URL of the proxy for SOCKS
- **Port**: Port of the proxy for SOCKS
- **SOCKS protocol version**: Version of the SOCKS protocol used. Possible values:
  SOCKS v4
  SOCKS v5 (Default)
- **No proxy for**: List of URLs for which no proxy is to be used (separated by commas).
- **System-wide proxy configuration**:

☑ The proxy configured under **Setup > Network > Proxy** will be used.

You will find further settings options in the Setup under Proxy (see page 1928).

Desktop Integration

Menu path: **Sessions > Horizon Client > Horizon Client Sessions > [Session name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Appliance Mode

Menu path: **Sessions > Appliance Mode**

In the appliance mode, only one specific session is accessible. You can activate the appliance mode for one of the following session types (if available on your system):

- VMware Horizon (see page 1415)
- Appliance Mode Browser (see page 1416)
- Citrix Self-Service (see page 1417)
- RHEV/Spice (see page 1418)
- Imprivata (see page 1419)
- RDP MultiPoint Server (see page 1422)
- XDMCP for This Display (see page 1423)

The system hotkey [Ctrl]+[Alt]+[s] for launching the setup application does not work in the appliance mode. Use [Ctrl]+[Alt]+[F2] instead.

You can set up a hotkey to start quick setup in appliance mode.

By default, access to other applications is not possible in appliance mode. However, these applications can be made available by activating **Appliance Mode Access** at the corresponding **Desktop Integration** page:

- ICA Connection Center (see page 1704)
- Task Manager (see page 1762)
- Application Launcher (see page 1740)
- Firmware Update (see page 1809)
- Quick Settings (see page 1726)
- Sound Preferences (see page 1744)
- Disk Utility (see page 1799)
- Commands (see page 1780)
- Webcam Information 1 (see page 1821)
- Touchscreen Calibration 1 (see page 1758)
- Screen Lock/Saver (see page 1846)
- Monitor Calibration (see page 1777)
- Network Tools (see page 1783)
- Screenshot Tool (see page 1769)
- System Information (see page 1794)
- Bluetooth Tool 1 (see page 1788)
- Display Switch[180]
- Identify Monitors (see page 1817)
- System Log Viewer (see page 1750)
- Local Terminal (see page 1708)
- SSH Session (see page 1542)
- Custom Application (see page 2073)

180. https://kb.igel.com/en/igel-os/11.10.250/display-switch-1

- Mobile Device Access (see page 1806)
- Open VPN (see page 1941)
- OpenConnect VPN (see page 1948)
- genucard (see page 1951)

Additionally, the in-session control bar can be used in an appliance mode session. With the in-session control bar, the user can eject a USB drive, start the wireless manager, start the Mobile Device Access USB tool and end the session. For further information, see In-Session Control Bar (see page 1872).

VMware Horizon

Menu path: **Sessions > Appliance Mode > VMware Horizon**

Server URL
URL of the VMware Horizon server.

User name
User name when logging on to the VMware Horizon server.

User password
Password when logging on to the VMware Horizon server.

> ⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain
Domain when logging on to the VMware Horizon server.

Desktop name
Desktop that is to be launched automatically.

Autoconnect

☑ The desktop given in **Desktop name** is launched automatically.

Network level authentication

- on: The user will authenticate themselves on the network level (network layer authentication) in order to establish an RDP connection.
- off: Conventional authentication.

> ℹ If network level authentication is enabled, the local login window is used. This also applies if the **Use local login window** option under **Sessions > Horizon Client > Horizon Client Global > Local Logon** is disabled.

Appliance Mode Browser

Menu path: **Sessions > Appliance Mode > Browser**

When this appliance mode is active, the Firefox browser is started to establish a connection with a session, e.g. a Citrix XenDesktop session. With a Citrix session, the browser is restarted after the session has been closed.

> If your session requires an on-screen keyboard, you can jump to the relevant configuration page via the link **On-screen keyboard** on the right-hand side. See also On-Screen Keyboard (see page 1773).

Web URL: URL for the session

Citrix Self-Service

Menu path: **Sessions > Appliance Mode > Citrix Self-Service**

> At least Citrix Receiver Version 13 is required.

Self-Service delivery server URL: Server address including the `https://` prefix.

> In the appliance mode, only one server can be used for Self-Service.

Multi User (StoreFront servers only)

☑ The user data on the client will be deleted after logging off or terminating Self-Service.

Reconnect after logon

☑ The Self-Service GUI reconnects automatically after being launched.

Reconnect to apps after starting an application

☑ The Self-Service GUI will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.

RHEV/Spice

Menu path: **Sessions > Appliance Mode > RHEV/Spice**

Connection Broker: URL of the Connection Broker.

Imprivata

Imprivata offers digital security solutions for healthcare organizations. For more information, see imprivata.com[181].

Menu path: **Sessions > Appliance Mode > Imprivata**

Set the URL to the server

URL address of the single sign-on server.

Path to the appliance

Path to the application on the single sign-on server. (Default: `sso/servlet/getembeddedloader?arch=amd64`)

Enable component's logging

☑ Log files will be generated. You will need them if support is required in the future.

Redirection of smartcards

☑ A smartcard will be redirected into a session.

PIE application launcher for Citrix

☑ Enables the grid theme for organizing Citrix apps.

The following setting is active if **Enable component's logging** is enabled:

Component's logging verbosity

Specifies the level of detail for the log files.
Possible options:

- "debug": Detailed information on the flow through the system.
- "info": Runtime events (startup/shutdown).
- "warning": Events that may lead to unexpected behavior.
- "error": Other errors or unexpected conditions.
- "critical": Events that may break the workflow.

Path to certificate

Absolute path to the certificate your Imprivata Appliance or Certification Authority issued. (Default: `/wfs/ca-certs/ssoCA.cer`)

181. https://www.imprivata.com/

IMPORTANT NOTE
If you rename the certificate or decide to store it in a different place, you have to adjust the path accordingly under **Sessions > Appliance Mode > Imprivata > Path to Certificate**.
Best practice is to change it directly through the profile which also issued the firmware update.

Fast User Switching

FUS user

The username for the preconfigured session.
Possible options:

- Hostname: The hostname of the endpoint device will be used as a username.
- MAC address: The MAC address of the device will be used as a username.
- Serial of the board: The serial number of the device will be used as a username.
- Free text entry

FUS user's domain

The domain the user belongs to.

FUS user's password

The password of the user running the preconfigured session.

Citrix Store URL

URL of the StoreFront website or of XenApp Services.

FUS resource

The resource, like the Desktop or Application, that is assigned to the username.

Single Application Kiosk

The Imprivata PIE agent will be signaled that the FUS resource is an application.

More on FUS at: https://www.imprivata.com/resources/datasheets/fast-user-switching-imprivata-onesign

Enable on-screen keyboard

☑ If a touchscreen is used, the on-screen keyboard is enabled.

The following settings are active if **Enable on-screen keyboard** is activated:

x coordinate of on-screen keyboard

Specifies the X position of the on-screen keyboard in pixels. (Default: 2)

y coordinate of on-screen keyboard

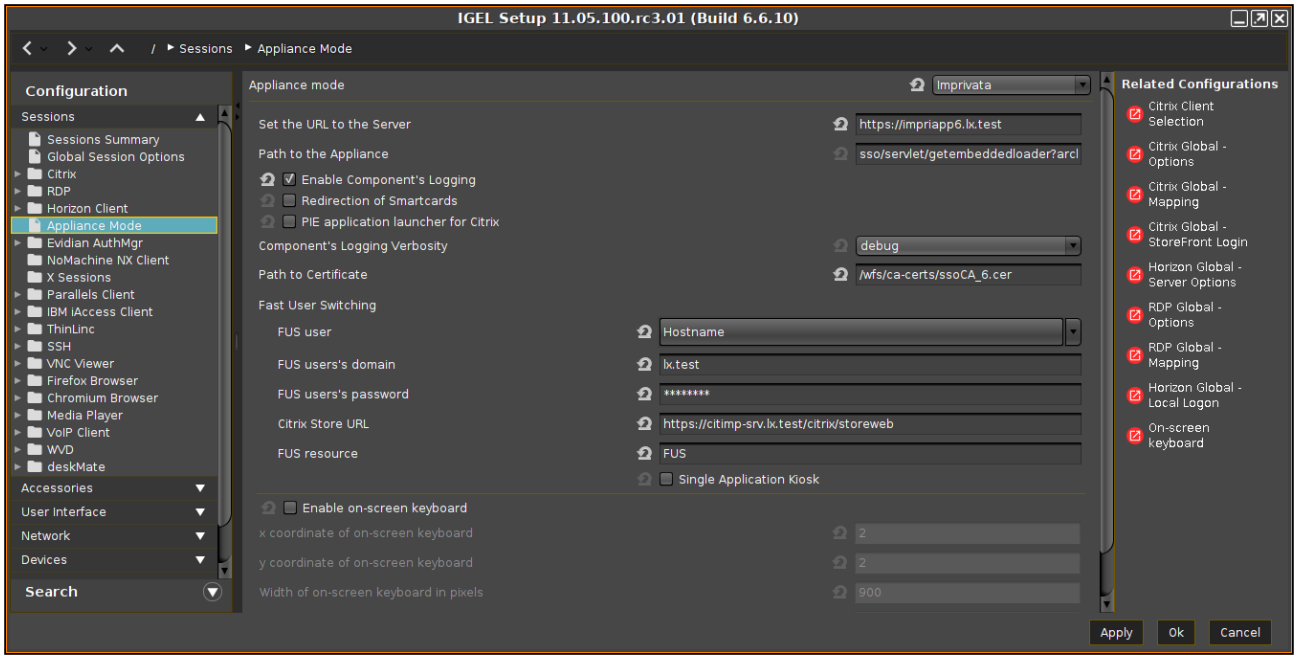
Specifies the Y position of the on-screen keyboard in pixels. (Default: 2)

Width of on-screen keyboard in pixels

It is recommended that you specify either the width or the height. (Default: 900)

Height of on-screen keyboard in pixels

It is recommended that you specify either the width or the height. (Default: 0)



If you need to modify and adjust the sessions, see Imprivata: Session Customization (see page 507).

Imprivata automatically creates a data partition, i.e. storage location for internal data.
If you are asked by your support to delete the data partition or you want to delete it for other reasons, see How to Clear the Imprivata Data Partition (see page 506).

Useful Registry Keys

- If you need to set a default AD domain for PIE agent, go to **System > Registry > imprivata.default_domain** and specify the NetBIOS name of your AD domain.
- If you need to ignore the VMware protocol selected by the Imprivata appliance, activate **System > Registry > imprivata.ignore_horizon_protocol**. In this case, the local selection under **Horizon Client > Horizon Client Global > Server Options > Preferred desktop protocol** will be used.
- To avoid focus theft from other windows, activate **System > Registry > imprivata.avoid_focus_ownership**.

RDP MultiPoint Server

Menu path: **Sessions > Appliance Mode > RDP MultiPoint Server**

Connect to server as soon as it is found: If you always have to connect to the same server, you can preset the connection here by giving the DNS name of your RDP MultiPoint Server.
Otherwise, the device will find one or more RDP MultiPoint Servers automatically as soon as you launch the session. For this to be possible, the servers must be in the same network as the device and obtain their IP address from the same DHCP server as the device.

XDMCP for This Display

Menu path: **Sessions > Appliance Mode > XDMCP for this display**

If this session type is selected, the device acts as an XDMCP client.

Connection type: The type of the connection.
Possible values:

- "Indirect via localhost": At startup, the device generates a list of found XDMCP hosts. The user can select a host. (Default)
- "Indirect": At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of the server**. The user can select a host.
- "Direct": The login mask of the host specified under **Name or IP of the server** is displayed.
- "Broadcast": The device starts a broadcast request. The login mask of that XDMCP host is displayed which is the first to respond to the broadcast request.

Name or IP of server: The name or IP of the XDMCP server.

Enable hotkeys for XDMCP Display: Defines whether hotkeys are managed by the device or the host.

☑ Hotkeys are managed by the device. When the user enters a shortcut key that is defined as a hotkey on the device, it starts the appropriate action. The input is not forwarded to the server. (Default)

☐ Hotkeys are not managed by the device. Almost all keyboard shortcuts are forwarded to the server. The hotkey [Ctrl + Alt + s] for opening the IGEL Setup can still be used, provided that this hotkey is activated under **Accessories > Setup**.

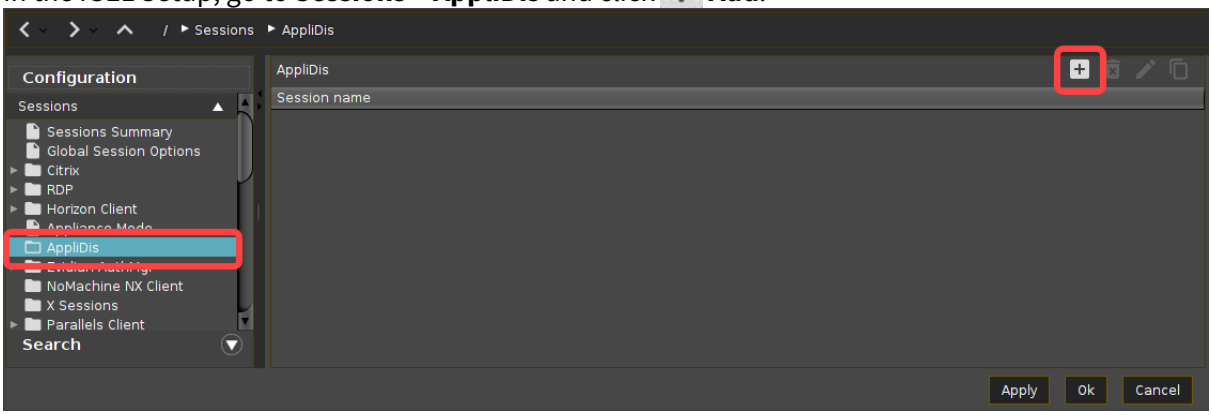
AppliDis

In IGEL OS, you can use the AppliDis client. AppliDis Fusion is a virtualization solution which combines the virtualization of desktops and applications in a single console. For more information, see https://www.systancia.com/en/systancia-workplace/.

Menu path: **Sessions > AppliDis**

To create an AppliDis session, proceed as follows:

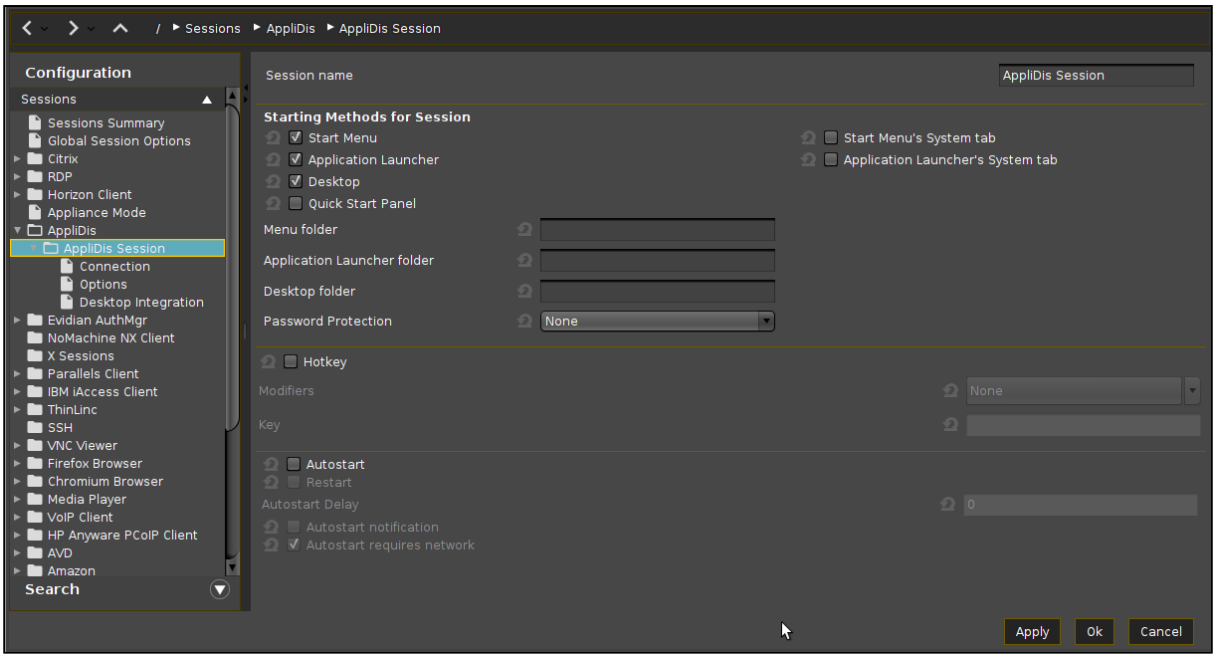
1. In the IGEL Setup, go to **Sessions > AppliDis** and click **Add**.



For the added session, you can perform the following actions:

- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

2. In the following area or under **Desktop Integration**, configure the **session name** and **starting methods** for this session.



3. Configure other settings according to your needs.
4. Click **Apply** or **Ok** to save the settings.

- Connection Settings for the AppliDis Client in IGEL OS (see page 1426)
- Options for the AppliDis Client in IGEL OS (see page 1427)
- Desktop Integration (see page 1430)

Connection Settings for the AppliDis Client in IGEL OS

In IGEL OS, you can add an AppliDis session; for how to add a session, see AppliDis (see page 1424). In the **Connection** area, you can provide details of the **server URL** and **connect type** for logging in. If you use AppliDis SLB Linux in the connector mode, the name of the application that uses the connector can be specified here.

Menu path: **Sessions > AppliDis > Connection**

Server URL

Address of the AppliDis server or the administration server

HTTP/HTTPS service port

Protocol for communication with the AppliDis server

Possible options:

- http
- https

Connect type

Possible options:

- Last option used
- TS desktop
- Virtual desktop
- Session maker
- VDI desktop

Forces the VDI desktop

Name of the desktop to be started, e.g. `Win10Test`, `TD-RD Desktop`. This feature is active if "VDI desktop" is selected under **Connect type**.

AppliDis SLB connector mode

Name of the application which the connector uses if AppliDis SLB Linux is to be used in the connector mode.

Options for the AppliDis Client in IGEL OS

In IGEL OS, you can add an AppliDis session; for how to add a session, see AppliDis (see page 1424). In the **Options** area, you can define the language, credentials, access path, and further settings for the AppliDis client.

Menu path: **Sessions > AppliDis > Options**

Language

Language for the AppliDis client

Possible options:

- English (Default)
- French

How the password is sent to the RDP Client

The method for sending the password configured below to the RDP Client

Possible options:

- cmdline (Default)
- prompt

Working directory

Complete path of the work directory for the application on the server

User name

User name when logging in to the server

Password

Password when logging in to the server

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain

Domain when logging in to the server

Full path to cert

Path to the certificate with file name

Timeout

Maximum time in minutes that the system waits for a response from the server. (Default: 30)

AppliDisXML access path

Path for XML communication with the AppliDis administration server. (Example: `/AppliDisXML/AppliDisServer.asp`)

Lock connection type

☑ The connection type is locked. (Default)

☐ The connection type is not locked.

Hide “Close” tab

☑ The “Close” tab is hidden. (Default)

☐ The “Close” tab is not hidden.

Close AppliDis client at end of session

☑ The client is closed when the session ends. (Default)

☐ The client is not closed.

Force insecure mode

☑ Insecure mode is forced.

☐ Insecure mode is not forced. (Default)

Enable debug mode

☑ Debug mode is enabled.

☐ Debug mode is disabled. (Default)

Activate SSL mode

☑ SSL mode is enabled.

☐ SSL mode is disabled. (Default)

Remember user

☑ AppliDis remembers the user name. (Default)

☐ AppliDis does not remember the user name.

Discard credentials

☑ The credentials are not saved. (Default)

☐ The credentials are saved.

Hide “Filter” tab

☑ The “Filter” tab is not shown.

☐ The “Filter” tab is shown. (Default)

Hide “Service” tab

☑ The “Service” tab is not shown.

☐ The “Service” tab is shown. (Default)

Hide “Server” tab

☑ The “Server” tab is not shown.

☐ The “Server” tab is shown. (Default)

SLB graphic mode disabled?

☑ A window for selecting the desktop is not shown. (Default)

☐ A window is shown where the user can choose which desktop he wants to be connected to.

Desktop Integration

In IGEL OS, you can add an AppliDis session; for how to add a session, see AppliDis (see page 1424). In the **Desktop Integration** area, you can define the session name and how the session should be started.

Menu path: **Sessions > AppliDis > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Evidian AuthMgr

Menu path: **Sessions > Evidian AuthMgr**

The procedure for configuring your Evidian AuthMgr session is described below.

- Evidian AuthMgr Global (see page 1434)
- Evidian AuthMgr Session (see page 1438)

Evidian AuthMgr Global

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global**

Here, you can configure the global settings for Evidian AuthMgr sessions.

- Restart for Evidian AuthMgr Global (see page 1435)
- Options (see page 1437)

Restart for Evidian AuthMgr Global

Here, you can define the desktop integration for restarting Evidian AuthMgr.

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Restart**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Options

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Global > Options**

Options

Language selection: Language selection of catalog messages.
Possible values:

- Global setting (Default)
- English (UK)
- English (US)
- German
- French
- Danish
- Custom

Custom catalog of messages: Choose here the file for the custom catalog of messages. (Default: `/services/evidian/share/locale/en/rsUserAuth.cat`)

Data Partition

Evidian AuthMgr Data Partition

☑ The data partition is activated so that additional data can be stored persistently.

☐ The data partition is deactivated. (Default)

Size: Size of the Evidian AuthMgr data partition in MB. (Default: 10)

Evidian AuthMgr Session

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions**

Here, you can set up your own Evidian AuthMgr session.

- Connection (see page 1439)
- Options of Evidian AuthMgr Sessions (see page 1440)
- Desktop Integration (see page 1442)

Connection

Menu path: **Setup > Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Connection**

In this area, you can specify the settings for the connection between Evidian AuthMgr and the server.

Protocol: Protocol that is used for user access.
Possible values:

- "HTTP" (Default)
- "HTTPS"

Server: IP address or DNS name that is used for user access.

Port: Port that is used for user access.
Possible values:

- "9764 (HTTP)" (Default)
- "9765 (HTTPS)"
- "Custom"

Custom port: If you selected "Custom" above, you can enter a port of your own here.

Path to service: Service path that is used for user access. (Default: /soap)

CA certificate: Path to the CA certificate with file name. The certificate is needed for HTTPS connections. (Example: `/wfs/ca-certs/ca.crt`)

- Download the Certificate for Evidain from the EAM in **base64 encoded x509 CER** format,
- Convert it to crt by the following command: **openssl x509 -inform PEM -in YOUR_CERT.cer -out YOUR_CRT.crt**
- Eventually **move YOUR_CRT.crt** to the endpoint

Roaming session secret: Password for the roaming session.

Fallback User Access Services

Click on the logo to specify up to four alternative connections. These will be used if the primary authentication server is not available. The alternative servers will be queried in sequence.

Options of Evidian AuthMgr Sessions

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Options**

Specify further options for your Evidian AuthMgr session.

Session type
Possible values:

- Citrix ICA
- RDP
- VMware Horizon
- RDWEB
- Custom

If you have selected the user-defined session type, you can enter your own start and stop commands here:

Custom start command: Command that is executed when the card is inserted. (Example: `/wfs/start.bash`)

Custom stop command: Command that is executed when the card is removed. (Example: `/wfs/stopp.bash`)

Language selection: Language selection of catalog messages.
Possible values:

- Automatic (Default)
- English (UK)
- English (US)
- German
- French
- Custom

Custom catalog of messages: Choose here the file for the custom catalog of messages. (Default: `/services/evidian/share/locale/en/rsUserAuth.cat`)

Availability message

☑ A message is shown when the authentication tool is available.

☐ A message is not shown when the authentication tool is available.

Tapping mode

☑ The operating mode can be changed by briefly tapping the card on the reader. Each tap triggers an action.

☐ The operating mode cannot be changed by tapping the card on the reader.

Delay for dynamic tapping: Tapping delay in seconds.

Allow password authentication

☑ Password is required for the authentication.

☐ Password is not required for the authentication.

Allow password forgotten

☑ Resetting the password is allowed.

☐ Resetting the password is not allowed.

Default domain name for password authentication: Domain name used by default for password authentication.

Debug mode

☑ Debug mode is activated, and all outputs are switched to the default error output.

☐ Debug mode is deactivated.

Level for trace: Specifies the trace level. The level of detail of the log messages decreases as you move down through the selection list.
Possible values:

- none
- low
- medium
- high
- details

Use configuration file

☑ Instead of the preconfigured session, a custom configuration file is used. All other session settings are ignored.

☐ A custom configuration file is not used.

Path: Path to the configuration file with file name. (Example: `/etc/rsUserAuth/rsUserAuth.ini`)

UPN format

☑ The UPN (User Principal Name) format for credentials is allowed.

☐ The UPN format cannot be used.

No trivial PIN code

☑ A trivial PIN, i.e. consisting of three or more consecutive numbers or identical digits, is not allowed.

☐ A PIN can consist of three or more consecutive numbers or identical digits. (Example: `2345`, `1111`)

4-eye authentication

☑ 4-eye authentication is enabled. For details, see https://www.evidian.com/products/enterprise-sso/4eyes-authentication/.

☐ 4-eye authentication is disabled.

Ignore smartcard removal on this reader: You can ignore the removal of the smartcard/RFID badge on the reader which you specify here via the reader's name or its product ID. The use of wildcards is possible. Example: `*3x21*`

Desktop Integration

Menu path: **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

NoMachine NX Client

Menu path: **Sessions > NoMachine NX Client > [Session Name]**

You can configure one or more NoMachine NX sessions.

Further information regarding configuration can be found in the original documentation provided by NoMachine: http://www.nomachine.com/documents.

The settings for launching the session are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Server (see page 1448)
- Unix Desktop (see page 1449)
- Unix Display (see page 1451)
- Windows Desktop (see page 1452)
- Windows Display (see page 1453)
- VNC Desktop (see page 1455)
- VNC Display (see page 1456)
- Shadow Display (see page 1457)
- Logon (see page 1459)
- Advanced (see page 1460)
- NoMachine NX Client Services (see page 1462)
- Desktop Integration (see page 1463)

Server

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Server**

Here, you can specify the connection data for the *NoMachine NX session*.

- **Host**: Host name or IP address of the *NoMachine NX* server.
- **Port**: Port for connecting with the *NoMachine NX* server (default: 22).
- **Connection service**: Protocol for connecting to the *NoMachine NX* server.
  Possible values:
  - SSH
  - NX
- **Session**: Session type
  Possible values:
  - Unix: The session will run under Unix/Linux on the server side. X11 serves as the transmission protocol.
  - Windows: The session will run under Windows on the server side. RDP serves as the transmission protocol.
  - VNC: The session will be transmitted with VNC (Virtual Network Computing) via RFP (Remote Framebuffer Protocol). On the server side, the session can run on any operating system. A VNC server is required on the server.
  - Shadow: Protocol version for older VNC servers
- **Use following DSA key**: DSA key which is to be used instead of the default key when logging on to the server. If no key is entered here, i.e. the field is empty, the thin client's default key will be used.
  The default key is saved under `/wfs/nxkeys/server.id_dsa.key`.

Unix Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Desktop**

Here, you can specify which window manager or display manager is to be launched on the server when the user logs on with the *NoMachine NX* client. The window manager must be available on the server.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Unix".

- **Desktop**
  Possible values:
  - KDE: KDE will be launched. (Default)
  - Gnome: Gnome will be launched.
  - CDE: CDE will be launched.
  - XDM: The display manager XDM will be launched.
  - Custom: A custom window manager will be used.

Settings options if "Desktop" is set to "XDM":

- **Login**: These options are available if **Desktop** is set to “XDM”.
  - **Let the NX server decide**: The configuration of the *NoMachine NX* server will be used for logon purposes.
  - **Query an X desktop manager**: The *NoMachine NX* client will connect to the X desktop manager of the computer defined under **Host**. The set **Port** will be used for this connection (default: 177).
  - **Broadcast XDM request**: The *NoMachine NX* client will send a request for available XDM servers in the subnet via the set **Port** (default: 177). The *NoMachine NX* client will use the first XDM server that responds to the request.
  - **Get a list of available X desktop managers**: The *NoMachine NX* client will send a request to the computer defined under **Host** via the set **Port** (default: 177). This computer will reply with a list of available XDM servers. This option is relevant to older versions of the *NoMachine NX* server.

Settings options if "Desktop" is set to "Custom":

Application

- **Run console**: The terminal set by default will be launched. Example: Xfce terminal
- **Run default X client script on server**: The script for the default desktop environment set by default will be launched. Example: `/home/user/startxfce.sh`
- **Run the following command**: Start command for the desired application or the desired window manager. Example: `startxfce`

Options

- **Floating window**: The session will be shown in a separate window. This option makes particularly efficient use of bandwidth.
- **Use X agent encoding**
  ☑ The data traffic will be decoded by the NX agent rather than in the X protocol. (default)
  ☐ The data traffic will remain in the X protocol and will be tunneled and compressed by the NX proxy.
- **Use taint of X replies**
  ☑ Trivial sources of X roundtrips will be suppressed by generating the response on the side of the X client. This option is relevant to older versions of the *NoMachine NX* server. (default)
- **New virtual desktop**: The session will take place on a new virtual desktop on the server side.

Unix Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Unix Display**

Here, you can define the properties for image transmission from the NoMachine NX server to the NoMachine NX client.

> The image transmission properties can also be defined on the server side. If a server-side setting competes with a client-side setting, the server-side setting will be effective.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Server > Session** is set to "Unix".

Display: Size of the display area that is used for the session.
Possible values:

- "640x480"
- "800x600"
- "1024x768"
- "Available area": The entire display area is used for the session. The taskbar is not visible.
- "Fullscreen": The session will be shown in full-screen mode, i. e. stretched across the entire screen.
- "Custom": The **Width** and **Height** can be freely defined.
- "Multimonitor fullscreen": The session will be shown in full-screen mode on all available monitors, i.e. stretched across the entire screen of each monitor.

Width: Width of the display area for the session. (Default: 800)

Height: Height of the display area for the session. (Default: 600)

Use custom settings

☑ The image transmission properties can be changed on the client side.

☐ The image transmission properties are specified on the server side only. (Default)

Use both JPEG and RGB compression: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

Use JPEG and RGB compression, and use custom JPEG quality: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

Only use JPEG compression: Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.

Use JPEG compression and custom JPEG quality: Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.

Only use RGB compression: Only RGB compression (loss-free) will be used.

Use plain X bitmaps: The images will be transmitted as bitmaps without compression.

JPEG quality: If **Use JPEG and RGB compression, and use custom JPEG quality** or **Use JPEG compression and cusom JPEG quality** is enabled, the quality of images in JPEG format can be defined. (Default: 6)

Windows Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Desktop**

Here, you can specify which *Windows* terminal server (or remote desktop service) is used, how the user logs on and whether the entire desktop or an individual application is launched.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

- **Windows terminal server**: Host name or IP address of the *Windows* server on which the desktop or the application runs
- **Windows terminal server domain**: Domain in which the *Windows* terminal server is located
- **Use the NX user's credentials**: When the session starts, the logon information under **Setup > NoMachine NX Client Sessions > [Session Name] > Logon** will be used. (default)
- **Use following credentials**: When the session starts, the logon information under **Username** and **Password** will be used.
    - **Username**: User name for starting the session
    - **Password**: Password for starting the session
- **Start Windows login screen**: When starting the session, the user must enter their logon information.
- **Run desktop**: When starting the session, the *Windows* desktop is shown (default)
- **Run application**: When starting the session, the *Windows* application given in the text field is launched.

Windows Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Windows Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Windows".

Display: Size of the display area that is used for the session
Possible values:

- 640x480
- 800x600
- 1024x768
- Available area:
- Full screen: The session will be shown in full-screen mode, i. e. stretched across the entire screen. (Default)
- Custom: The **width** and **height** can be freely defined.
- Multi-monitor full screen:

Width: Width of the display area for the session (default: 800)

Height: Height of the display area for the session (default: 600)

Colors
Possible values:

- 256
- 32K
- 64K
- 16M

Use custom settings

☑ The image transmission properties can be changed on the client side.

☐ The image transmission properties are specified on the server side only. (default)

- **Use JPEG and RGB compression**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and define JPEG quality**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression**: Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality**: Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression**: Only RGB compression (loss-free) will be used.
- **Use plain X bitmaps**: The images will be transmitted as bitmaps without compression.
- **JPEG quality**: If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).

Enable RDP image cache

☑ The cache is enabled. This increases the amount of memory needed. However, the speed of the session may be increased. (default)

VNC Desktop

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Desktop**

Here, you can specify the VNC server as well as the password for the VNC session.

> These settings are only relevant up to NoMachine NX Server Version 3.5.

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

- **VNC server**: Name or IP address of the server
- **:** Number of the display.
- **Password**: Password for the VNC session

VNC Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > VNC Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "VNC".

> These settings are only relevant up to NoMachine NX Server Version 3.5.

Display: Size of the display area that is used for the session
Possible values:

- 640x480
- 800x600
- 1024x768
- Available area
- Fullscreen: The session will be shown in full-screen mode, i. e. stretched across the entire screen. (Default)
- Custom: The **width** and **height** can be freely defined.
- Multimonitor Fullscreen
- **Width**: Width of the display area for the session (default: 800)

Height: Height of the display area for the session (default: 600)

Use custom settings

☑ The image transmission properties can be changed on the client side.

☐ The image transmission properties are specified on the server side only. (default)

- **Use both JPEG and RGB compression**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG and RGB compression, and use custom JPEG quality**: JPEG compression (results in losses) as well as RGB compression (loss-free) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use JPEG compression**: Only JPEG compression (results in losses) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
- **Use JPEG compression and custom JPEG quality**: Only JPEG compression (results in losses) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
- **Only use RGB compression**: Only RGB compression (loss-free) will be used.
- **Use plain X bitmaps**: The images will be transmitted as bitmaps without compression.
- **JPEG quality**: If **Use JPEG and RGB compression and define JPEG quality** or **Use JPEG compression and define JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).

Shadow Display

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Shadow Display**

This area is active if the parameter **Setup > Sessions > NoMachine NX Client > [Session Name] > Session** is set to "Shadow".

These settings are only relevant up to NoMachine NX Version 3.5.

- **Display**: Size of the display area that is used for the session
  Possible values:
  - 640x480
  - 800x600
  - 1024x768
  - Available area:
  - Fullscreen: The session will be shown in fullscreen mode, i. e. stretched across the entire screen.v (Default)
  - Custom: The **width** and **height** can be freely defined.
  - Multi-monitor full screen:
- **Width**: Width of the display area for the session (Default: 800)
- **Height**: Height of the display area for the session (Default: 600)
- **Enable custom settings**
  ☑ The image transmission properties can be changed on the client side.
  ☐ The image transmission properties are specified on the server side only. (default)
  - **Use both JPEG and RGB compression**: JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
  - **Use JPEG and RGB compression, and use custom JPEG quality**: JPEG compression (lossy) as well as RGB compression (lossless) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
  - **Only use JPEG compression**: Only JPEG compression (lossy) will be used. The level of JPEG compression will be adjusted dynamically depending on the compressibility.
  - **Use JPEG compression and custom JPEG quality**: Only JPEG compression (lossy) will be used. The level of JPEG compression is specified by the parameter **JPEG quality**.
  - **Only use RGB compression**: Only RGB compression (lossless) will be used.
  - **Use plain X images**: The images will be transmitted as bitmaps without compression.
  - **JPEG quality**: If **Use JPEG and RGB compression and use custom JPEG quality** or **Use JPEG compression and custom JPEG quality** is enabled, the quality of images in JPEG format can be defined (default: 6).
- **Enable render extension**
  ☑ The "Render" or "XRender" protocol extension is enabled. This allows a transparency effect where windows overlap on the screen. (default)
- **Disable the backing store**
  ☑ The cache is disabled. This reduces the amount of memory needed. However, the speed of the session may be reduced.
  ☐ The cache is enabled. (default)

- **Disable the composite extension**
  ☑ The "Composite" protocol extension is disabled. Transparency effects where windows overlap on the screen are not possible.
  ☐ The "Composite" protocol extension is enabled. (default)
- **Disable the shared memory extension**
  ☑ The shared memory extension is disabled.
  ☐ The shared memory extension is enabled. (default)
- **Disable emulation of shared pixmaps**
  ☑ The emulation of shared images (shared pixmaps) is disabled.
  ☐ The emulation of shared images (shared pixmaps) is enabled. (default)

Logon

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Logon**

Here, you can specify the logon information for starting the session.

- **Login method**
  Possible values:
  - Password: The user logs on with a logon and password.
  - Private key: The logon takes place with a private key.
- **Login**: User name when logging on to the server
- **Password**: Password when logging on to the server

> ⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Advanced

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Advanced**

Here, you can change advanced settings.

- **Link speed**
  Possible values:
  - Modem
  - ISDN
  - ADSL
  - WAN
  - LAN (Default)
- **Disable ZLIB stream compression**
  Possible values:
  ☑ The data traffic between the client and server will not be compressed.

  > Switching off compression can be helpful if the data traffic is compressed on another level, e.g. by VPN software.

  ☐ The data traffic between the client and server will be compressed. (default)
- **Enable SSL encryption on all traffic**
  ☑ Connections with NX, SSH and UDP will be encrypted. (default)
  ☐ Connections with NX and SSH will be encrypted, connections with UDP will remain unencrypted.
- **Connect through a HTTP proxy**
  ☑ The connection between the client and server will be routed via an HTTP proxy.
  ☐ The connection between the client and server will be direct. (default)
- **Host**: Host name or IP address of the HTTP proxy
- **Port**: Port of the HTTP proxy (default: 8080)
- **Username**: User name when logging on to the HTTP proxy

  > This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Password**: Password when logging on to the HTTP proxy

  > This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Remember my password**

  > This setting is only relevant up to NoMachine NX Server Version 3.5.

  ☑ The password will be saved.
  ☐ The password will not be saved and must therefore be entered again for each session. (default)
- **Disable deferred screen updates**: Delayed screen refreshing ("lazy encoding") compensates for bottlenecks in data transmission. If a bottleneck occurs, refresh procedures requiring large

amounts of bandwidth are delayed in favor of interactivity. There are two levels of delayed screen refreshing. With Level 1, refresh actions which are not displayed directly ("offscreen") are dismissed. With Level 2, refresh actions which are displayed directly ("onscreen") are dismissed.

> This setting is only relevant up to NoMachine NX Server Version 3.5.

☑ Bottlenecks in data transmission are not compensated for through delayed screen refreshing.
☐ If the connection speed is set to "WAN", Level 1 delayed screen refreshing will be used. If the connection speed is set to "MODEM, "ISDN" or "ADSL", Level 2 delayed screen refreshing will be used. (default)

- **Disk cache**: Size of the persistent memory for caching images (default: 64 MB)

  > This setting is only relevant up to NoMachine NX Server Version 3.5.

- **Memory cache**: Size of the volatile memory for caching images (default: 16 MB)

  > This setting is only relevant up to NoMachine NX Server Version 3.5.

NoMachine NX Client Services

Here, you can enable or disable services for printers and audio playback on your thin client.

Menu path: **Setup > Sessions > NoMachine NX Client > [Session Name] > Services**

- **Enable multimedia support**
  You will find further information regarding audio playback on the *Nomachine NX* client in the NoMachine Knowledge Base[182].
  ☑ Audio output is forwarded to the media player via *esound*.
  ☐ A dedicated channel is used for audio output. (default)
- **Enable CUPS printing**
  ☑ Printing via the thin client is enabled. (default)
  ☐ Printing via the thin client is disabled.
- **Port**: Port via which CUPS can be configured with a browser (default: 631)
- **Public printer**
  ☑ The printer connected to the thin client is shared via the network. A server-side configuration is required for this purpose.
  ☐ The printer is not shared. (default)

182. https://www.nomachine.com/?q=AR03D00355

Desktop Integration

Menu path: **Sessions > NoMachine NX Client > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the NoMachine NX session.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

X Sessions

Menu path: **Sessions > X Sessions > [Session Name]**

You can configure one or more X sessions.

The settings for launching the session are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Server (see page 1469)
- Desktop Integration (see page 1471)

Server

Menu path: **Setup > Sessions > X Sessions > [session name] > Server**

Connection type: Connection type for the XDMCP session

Possible options:

- Indirect via localhost: At startup, the thin client generates a list of found XDMCP hosts. The user can select a host.
- Indirect: At startup, a list of XDMCP hosts is displayed. This list is generated by the server specified under **Name or IP of server**. The user can select a host.
- Direct: The login mask of the host specified under **Name or IP of server** is displayed
- Broadcast: The thin client starts a broadcast request. The login mask of that XDMCP host is displayed which responds first.
- Local display: The command specified under **Command to be displayed** is run.

Name or IP of server: Hostname or IP address of the XDMCP server

Command to be displayed: Command to be executed. The display is set in the DISPLAY environment variable.

Access control

☑ Access to this display from other computers will be controlled.

Terminate after one session

☑ The session is terminated when the user has logged out from the remote server.

Use quit hotkey

☑ The session can be terminated with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- [Ctrl] = `Ctrl`
- = `Super_L`
- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

Ctrl + = `Ctrl|Super_L`

Quit hotkey: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Use fullscreen

☑ The XDCMP session is displayed in fullscreen mode.

Use fullscreen restricted to workarea

☑ The thin client's local taskbar is visible.

Window size: Window size for the XDMCP session. Default: 640x480

Color depth: Color depth for the XDMCP session.

Possible options:

- Same as display: The system settings for the thin client is used.
- 256 colors
- 65535 colors
- True Color (24)
- True Color (32)

Color allocation policy

Possible options:

- Default
- Mono
- Gray
- Color

Start monitor: Selects the monitor on which the XDMCP session ist displayed.

Possible options:

- No configuration: The monitor is selected according to already existing windows and to the current position the mouse pointer.
- 1st monitor
- 2nd monitor
- Fullscreen on all monitors

Desktop Integration

You can configure one or more X sessions.

The settings for launching the session are described below.

Menu path: **Sessions > X Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Parallels Client Global

Menu path: **Sessions > Parallels Client > Parallels Client Global**

In this area, you can configure global settings for all Parallels Client sessions.

- Keyboard (see page 1475)
- USB Redirection (see page 1476)

Keyboard

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > Keyboard**

In this area, you can select the keyboard layout for Parallels Client sessions.

Keyboard layout
Possible values:

- System presets as well as all available input schemes.

USB Redirection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Global > USB Redirection**

In this area, you can configure USB Redirection for Parallels Client sessions.

USB Redirection

☑ USB redirection is enabled.

☐ USB redirection is disabled. (Default)

Automatically redirect all USB devices: Defines whether the **Device Rules** will be ignored and all USB devices redirected.

☑ All USB devices will be redirected.

☐ USB devices will be redirected according to the **Device Rules**. (Default)

Device Rules

In this area, you can define device rules for USB redirection.

Defining new rules:

Click + to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

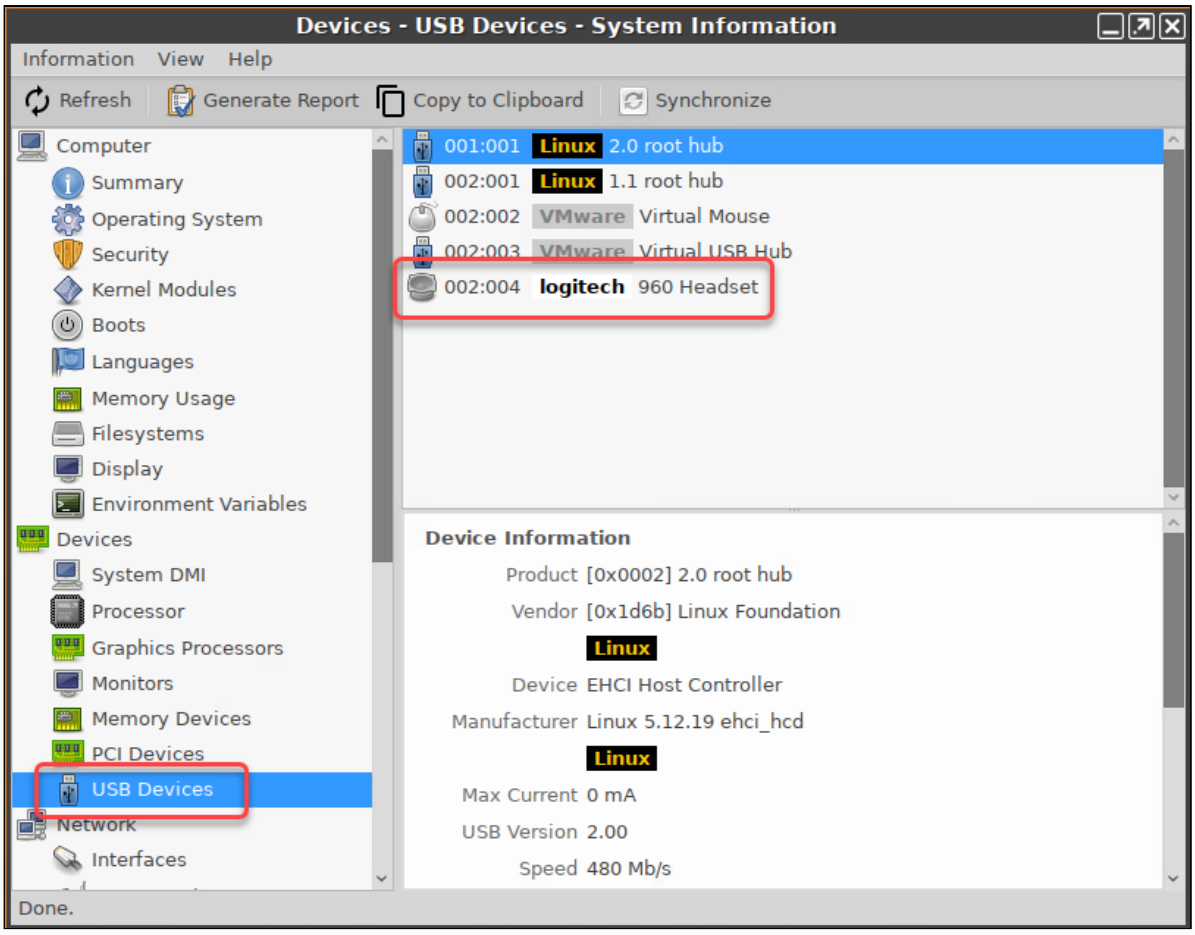
Rule
Possible values:

- "Deny" (Default)
- "Allow"

Vendor ID: Hexadecimal manufacturer number.

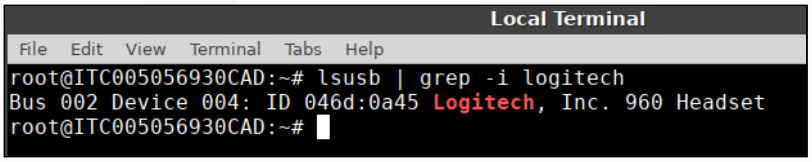
Product ID: Hexadecimal device number.

> Getting USB Device Information
>
> To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
> System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name: Free text entry.

PTP/MTP redirection

☑ PTP/MTP redirection is enabled.

☐ PTP/MTP redirection is disabled. (Default)

Automatically redirect all PTP/MTP devices: Defines whether the **Device Rules** will be ignored and all PTP/MTP devices redirected.

☑ All PTP/MTP devices will be redirected.

☐ PTP/MTP devices will be redirected according to the **Device Rules**. (Default)

Device Rules

In this area, you can define device rules for PTP/MTP redirection.

Defining new rules:

Click + to get to the **Add** dialog.

In the **Add** dialog, you can define the following settings:

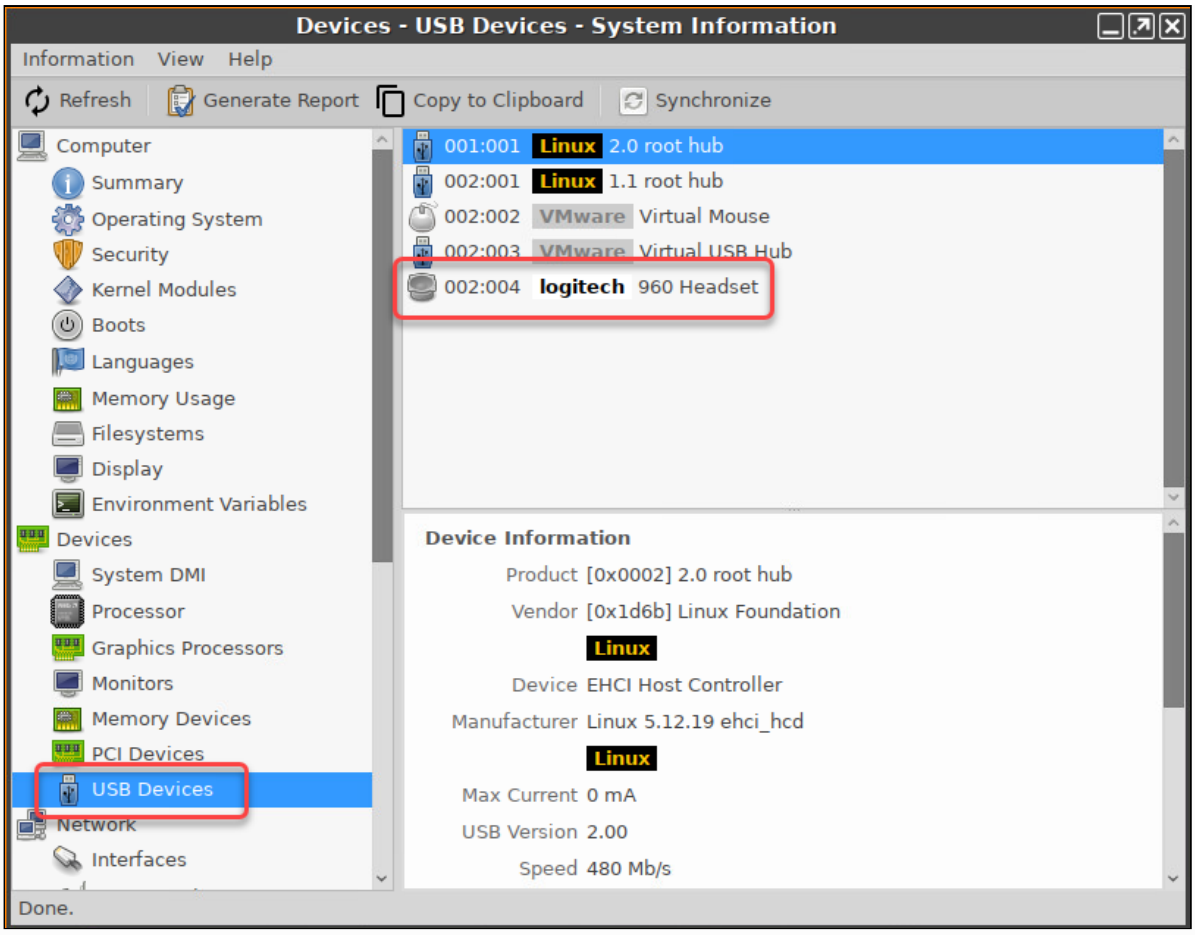
Rule
Possible values:

- "Deny" (Default)
- "Allow"

Vendor ID: Hexadecimal manufacturer number.

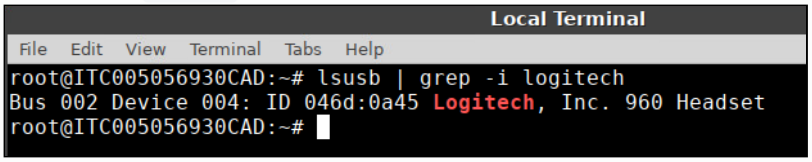
Product ID: Hexadecimal device number.

> Getting USB Device Information
>
> To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).
> System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Name: Free text entry.

Parallels Client Session

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name]**

You can configure one or more Parallels Client sessions.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Connection (see page 1483)
- Display (see page 1485)
- Local Resources (see page 1486)
- Experience (see page 1487)
- Network (see page 1488)
- Advanced Settings of the Parallels Client Sessions (see page 1489)
- Desktop Integration (see page 1490)

Connection

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Connection**

In this area, you can specify the settings for the connection between the Parallels Client and the server.

Application Server

Primary Server: Name or IP address of the primary application server.

Secondary Server: Name or IP address of the secondary application server. The secondary application server is used if the primary application server cannot be contacted.

Connection Mode
Possible values:

- "Gateway Mode": This mode is suitable if the Parallels Client does not have access to a physical server and no special demands as regards security apply. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80. The RDP sessions runs in a tunnel within this connection. (Default)
- "Direct Mode": This mode is suitable if the Parallels Client has direct access to a physical server. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 80 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server. This mode is the most efficient because the connection to the gateway is temporary and the data traffic is correspondingly low.
- "Gateway SSL Mode": This mode is suitable if the Parallels Client does not have access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443. The RDP sessions runs in a tunnel within this connection.
- "Direct SSL Mode": This mode is suitable if the Parallels Client has direct access to a physical server and there are high demands as regards security. The Parallels Client establishes a connection to the Parallels SecureClientGateway via port 443 in order to negotiate connection data for the RDP session with the application server. The Parallels Client then terminates the connection to the gateway and establishes the session with the application server.

Port: Port for communication with the application server. (Default: 80)

Logon

Use system credentials

☑ The system-wide logon data will be used for logging on to the application server (single sign-on). This option can be used if the local device logon takes place via Kerberos. The logon data saved temporarily when logging on to the device will be used for the user name and password.

☐ The logon data given under **User name**, **Password**, and **Domain** will be used when logging on to the application server. (Default)

User: User name when logging on to the application server.

Password: Password when logging on to the application server.

> ⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Domain: Domain when logging on to the application server.

Enable support for FIPS 140-2 compliance

☑ The support for FIPS 140-2 standard is enabled.

☐ The support for FIPS 140-2 standard is disabled. (Default)

Display

Display color depth: Number of colors displayed

Possible values:

- 8 bit
- 15 bit
- 16 bit
- 24 bit
- 32 bit (Default)

Graphics acceleration: Type of graphics acceleration. Higher graphics acceleration means better graphics quality, but requires more CPU power.
Possible options:

- "None": No acceleration
- "Basic": Basic acceleration
- "RemoteFX": Microsoft RemoteFX will be used.
- "RemoteFX Adaptive": RemoteFX Adaptive and H.264 codecs will be used. (Default)
- "AVC Adaptive": H.264/AVC will be used.

> If "RemoteFX" or "RemoteFX Adaptive" is enabled, the color depth will automatically be set internally to 32 bit, regardless of the value set under **Display color depth**.

Use all monitors for desktop session (if applicable)

☑ All monitors will be used for the desktop session.

☐ The primary monitor will be used for the desktop session. (Default)

Use only primary monitor for published applications
Published applications run on the server, the input and output data is exchanged between the client and the application server.

☑ Published applications will only be shown on the primary monitor.

☐ Published applications will only be shown on all available monitors. (Default)

Span desktop across all monitors

☑ The desktop will be shown across all available monitors.

☐ The desktop will only be shown on the primary monitor. (Default)

Local Resources

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Local Resources**

Remote audio playback
Possible values:

- "Bring to this computer": The device plays back the audio data supplied by the application server. (Default)
- "Do not play": The device does not play back the audio data supplied by the application server.
- "Leave at remote computer": The audio data will be played back on the application server.

Remote audio recording
Possible values:

- "Record from this computer": The audio input (microphone) is redirected to the application server.
- "Do not record": The audio input (microphone) is not redirected to the application server.

Apply Windows key combinations for desktops only
Possible values:

- "On the local computer": Windows-specific hotkeys are used for the local desktop only.
- "On the remote computer": Windows-specific hotkeys are used for the application server only.
- "In full-screen mode only": Windows-specific hotkeys are used for remote applications in full-screen mode only.

Local devices

Connect local serial ports

☑ The device's serial interfaces can be used in the Parallels Client session.

☐ The serial interfaces cannot be used in the Parallels Client session. (Default)

Connect local smartcards

☑ The device's card reader can be used in the Parallels Client session.

☐ The card reader cannot be used in the Parallels Client session. (Default)

Connect local drives

☑ The drives connected to the device can be used in the Parallels Client session.

☐ The drives cannot be used in the Parallels Client session. (Default)

Connect local printers

☑ The printer connected to the device can be used in the Parallels Client session.

☐ The printer cannot be used in the Parallels Client session. (Default)

Connect clipboard

☑ The clipboard of the Parallels Client session can be used. (Default)

☐ The clipboard of the Parallels Client session cannot be used.

Experience

Menu path: **Setup > Parallels Client > Parallels Client Sessions > Parallels Client Session > Experience**

You can enable or disable the features for the graphical display according to the bandwidth of the network connection. The features can also be activated or deactivated individually.

Connection speed: Activates the features for the graphical display depending on the bandwidth of the network connection to provide the optimal performance.
Possible options:

- "Modem 56 Kbps": The features **Themes** and **Bitmap caching** will be enabled.
- "Low speed broadband (256 Kbps-2 Mbps)": The features **Themes** and **Bitmap caching** will be enabled.
- "Satellite (2 Mbps-16 Mbps with high latency)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "High speed broadband (2 Mbps-16 Mbps)": The features **Menu and window animation**, **Desktop composition**, **Themes**, and **Bitmap caching** will be enabled.
- "WAN (10 Mbps or higher with high latency)": All features below will be enabled.
- "LAN (10 Mbps or higher)": All features below will be enabled.
- "Detect connection quality automatically": The automatically detected quality of the network connection determines which of the features below should be used for the optimal user experience. The individual feature selection is not possible.

Desktop background

☑ The desktop background image for the session will be shown.

Font smoothing

☑ Edges will be smoothed when text is displayed.

Menu and window animation

☑ Transitions for menus and windows will be animated.

Desktop composition

☑ Visual effects can be used for the desktop. For details on desktop composition, see e.g. https://docs.microsoft.com/en-us/windows/win32/dwm/dwm-overview.

Show contents of window while dragging

☑ The window content will be shown when a window is moved.

Themes

☑ The design of the desktop can be modified.

Bitmap caching

☑ Bitmap resources, e.g. icons or images, are cached locally. This allows reducing the amount of data sent, and, thus improves the performance.

Network

Menu path: **Setup > Parallels Client > Parallels Client Sessions > [Session Name] > Network**

Here, you can configure a proxy for communication between the Parallels Client and application server.

Use proxy server

☑ A proxy is used for communication between the Parallels Client and the application server.

☐ A direct network connection is used for communication between the Parallels Client and the application server. (default)

Proxy type: Type or protocol of the proxy used
Possible values:

- SOCKS 4
- SOCKS 4A
- SOCKS 5
- HTTP 1.1

Proxy host: URL of the proxy

Proxy port: Port of the proxy (default: 8080)

Use proxy credentials: If a proxy demands a logon, this option must be enabled and the logon data must be entered under **Proxy user** and **Proxy password**.

☑ The logon data in **Proxy user** and **Proxy password** will be sent to the proxy.

Proxy user: User name when logging on to the proxy

Proxy password: Password when logging on to the proxy. The password is relevant if either the “SOCKS 5” or “HTTP 1.1” protocol is selected as the proxy type.

Advanced Settings of the Parallels Client Sessions

Menu path: **Setup > Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Advanced**

Redirect URLs to client

☑ URLs will be opened on the client.

☐ URLs will be opened on the application server. (Default)

Redirect MAIL to client

☑ E-mails will be opened on the client.

☐ E-mails will be opened on the application server. (Default)

Compression

☑ The data flow between the Parallels Client and the application server will be compressed. (Default)

> Compression reduces network traffic but requires more CPU power.

☐ The data flow between the Parallels Client and the application server will not be compressed.

Use pre-windows 2000 login format

☑ Legacy login format (pre-Windows 2000) can be used. (Default)

☐ Legacy login format (pre-Windows 2000) cannot be used.

Network level authentication

☑ Network level authentication (NLA) is activated for the Parallels Client session. The client has to authenticate before connecting to the server. (Default)
For more information about NLA, see https://technet.microsoft.com/en-us/magazine/hh750380.aspx.

☐ Network level authentication is disabled.

Override computer name: The name entered here will override the name of the application server shown at the top of the session window.

Desktop Integration

In this area, you can configure desktop integration for the Parallels Client session.

Menu path: **Sessions > Parallels Client > Parallels Client Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

PowerTerm Selection in IGEL OS

IGEL OS integrates the Ericom PowerTerm terminal emulator solution, which allows you to easily access your legacy applications.

For more information on Ericom PowerTerm, see e.g. https://www.ericom.com/powerterm/embedded-thin-clients/.

Under **PowerTerm Selection**, you can choose the required version of the PowerTerm terminal emulator in order to ensure the best possible compatibility with your terminal applications.

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Selection**

Licensed Feature

This feature requires an add-on license. Please contact your IGEL reseller.

PowerTerm version

Selects the version of the PowerTerm terminal emulator.

For the included PowerTerm versions, see the "Component Versions" section in the IGEL OS release notes (see page 2282).

When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

PowerTerm Session

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Session**

You can configure one or more sessions for PowerTerm terminal emulation.

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

The configuration dialogs were designed to look as similar as possible to the setup pages described in the original documentation from ERICOM Software Ltd.

You will find detailed information on configuring the PowerTerm software in the PowerTerm Interconnect Manual on the Ericom website[183].

183. http://www.ericom.com/help.asp?cat=support

Desktop Integration

Menu path: **Sessions > PowerTerm Terminal Emulation > PowerTerm Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

IBM iAccess Client

IBM iAccess Client is an emulation of the IBM-5250 terminal in Java and supports numerous encodings.

Menu path: **Sessions > IBM iAccess Client**

->Add a session in order to be able to use the IBM iAccess Client.

->Under the **Connection** point under **Destination address**, give at least the DNS name or the IP address of a server. The client can also retrieve further logon information interactively.

->Under **Help > Information Center** in the IBM iAccess Client menu, you can read the help provided by the manufacturer in your browser.

IBM iAccess certificates for server authentication and encryption can be distributed as files using the Universal Management Suite (UMS).

- iAccess Global (see page 1499)
- IBM iAccess Session (see page 1502)

iAccess Global

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global**

Here you can define global settings for the emulation.

- Tab Setup (see page 1500)
- Font (see page 1501)

Tab Setup

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Tab Setup**

Open new sessions in a new tab

☑ The new session will be opended in a new tab. (Default)

☐ A new session will be opened in a new window.

Always display the tab bar

☑ The tab bar will always be displayed.

☐ The tab bar will not be displayed. (Default)

Switch to new tab when created

☑ Switches to new tab. (Default)

☐ Remains in current tab.

Send a warning when closing multiple tabs

☑ Sends warning. (Default)

☐ Multiple tabs are closed without warning.

Do not start tabbed sessions until the tab is selected

☑ Applies.

☐ Does not apply. (Default)

New Tab Action

- Disable and hide
- Run the same (Default)
- Run other...

Tab Placement

- Top (Default)
- Bottom
- Left
- Right

Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Global > Font**

Font File or Dirctory: Enter the path to your font file or font directory.

IBM iAccess Session

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [Session Name]**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Connection (see page 1505)
- Screen (see page 1508)
- Preferences (see page 1513)

Connection

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection**

Destination Address: Name or IP of the server

Destination Port: Server port (Default value: "default")

> If you leave **Destination Address** set to the string value "default" (default value) while **Use TLS/SSL** is enabled, port 229 is used. Without **Use TLS/SSL** enabled, port 23 is used. However, you are free to enter a custom port number.

Use TLS/SSL

☑ TLS/SSL is used.

☐ TLS/SSL is not used. (Standard)

Server Authentication: Defines if the client validates the authenticity of the server when connecting.

> To perform server authentication, the endpoint device must have the CA certificate that is associated with the server certificate. For instructions on how to deploy the certificate on the device, see Deploying Trusted Root Certificates in IGEL OS (see page 764).

☑ The client requires the server to authenticate itself. (Default)

☐ The client connects to the server without server authentication.

Workstation ID: Name of the client that is presented to the server. This name must be unique. For more information, go to **Help > Information Center** in your iAccess client.

Screen Size

Possible values:

- 24x80
- 27x132

Host Code Page

Possible values:

- 1140 United States Euro (Default)
- 1141 Germany Euro
- 1141 Austria Euro
- 1142 Denmark Euro
- ...

Enable Unicode Data Stream

☑ Unicode Data Stream is enabled.

☐ Unicode Data Stream is disabled. (Default)

Enable DBCS in Unicode Fields

☑ DBCS is enabled in unicode fields.

☐ DBCS is disabled in unicode fields. (Default)

Auto-Connect

☑ Automatically connect to the server on client startup. (Default)

Auto-Reconnect

☑ Automatically make a reconnect attempt if the server connection is lost. (Default)

- Advanced (see page 1507)

Advanced

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Connection > Advanced**

Connection Timeout (seconds) (Default: 0)

Inactivity Timeout (minutes) (Default: 0)

Keep-Alive

☑ Keep-Alive is enabled.

☐ Keep-Alive is disabled. (Default)

Enable ENPTUI

☑ ENPTUI is enabled. (Default)

Password Prompting

Possible values:

- Use default user name to prompt once for each system: The credentials preconfigured in the fields **User ID** and **Password (optional)** are used.
- Prompt for user name and password every time (Default)
- Use Kerberos authentication: The credentials from the Active Directory login are used; only available if the user has logged in to the thin client via Active Directory. For more information, see Active Directory/Kerberos in IGEL OS (see page 2034).

User ID: The user ID to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".

Password (optional): The password to be used when **Password Prompting** is set to "Use default user name to prompt once for each system".

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Bypass sign-on:

☑ The logon to the system is bypassed. (Default)

Screen

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen**

Cursor Shape

Possible Values:

- Underline (Default)
- Block

_____

- Font (see page 1509)
- IBM IAccess Session Cursor (see page 1510)
- Rule Line (see page 1511)
- IBM iAccess Session Color in IGEL OS (see page 1512)

Font

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Font**

Fixed Font

☑ Use a fixed font.

☐ Use no fixed font. (Default)

Fixed Font Size

Possible values:

- 8
- 10 (Default)
- 12
- 14
- ...
- 58

Font Scaling

☑ Font is scaled. (Default)

Antialiasing

☑ Antialiasing is activated.

☐ Antialiasing is diabled. (Default)

Font Name

Possible values:

- IBM3270 (Default)
- Monospaced
- Courier 10 Pitch
- DejaVu Sans Mono
- Liberation Mono
- Lucida Sans Typewriter
- Numbus Mono L
- PComm Session
- Ubuntu Mono

Font Style

Possible values:

- Plain (Default)
- Bold
- Italic

IBM IAccess Session Cursor

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Cursor**

Cursor Shape

Possible values:

- Underline (Default)
- Block

Cursor Pointer

Possible values

- Default (Default)
- Crosshair

Allow blinking cursor

☑ Blinking cursor is allowed.

☐ Blinking cursor is diabled. (Default)

Show blinking text with

Possible values:

- Blinking Text
- Host Color (Default)
- Mapped color

Blink Color: Select a color in which the cursor should blink.

Blink Color Background: Select a background color.

Rule Line

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Rule Line**

Rule Line

☑ Rule line is activated.

☐ Rule line is disabled. (Default)

Follow Cursor

☑ The follow cursor effect is enabled.

☐ The follow cursor effect is disabled. (Default)

Style

Possible values:

- Crosshair (Default)
- Vertical
- Horizontal

IBM iAccess Session Color in IGEL OS

Menu path: **Sessions > IBM iAccess Client > IBM iAccess Session > [session name] > Screen > Color**

Field Color: Choose respective colors.

OIA Color: Select a suitable color for the respective indicators.

- Status Indicators
- Information Indicators
- Attention Indicators
- Error Indicators
- OIA Background

Other

- **Screen Background**: Choose a color.

> This color overrides all Field Color Background colors which are set to black.

- **Highlight active field**

☑ Active field is highlighted.

☐ Active field is not highlighted. (Default)

- **Active field**: Choose a color
- **Active Field Background**: Choose a color
- **Crosshair Ruler Color**: Choose a color
- **Column Separator**: Choose a color

Preferences

Menüpfad: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences**

Start window maximized

☑ The windows starts in maximal size.

☐ The windows does not start in maximal size. (Default)

Automatic Resize

☑ Automatic window resizing is enabled. (Default)

☐ Automatic window resizing is disabled.

Show Border

☑ The session screen is framed by a border.

☐ No additional border is added. (Default)

Graphical OIA

☑ The Graphical OIA (Graphical Operator Information Area) is displayed. (Default)

☐ The Graphical OIA (Graphical Operator Information Area) is hidden.

Textual OIA

☑ The Textual OIA (Textual Operator Information Area) is displayed.

☐ The Textual OIA (Textual Operator Information Area) is hidden. (Default)

Keypad

☑ The Keypad is displayed.

☐ The Keypad is hidden. (Default)

Toolbar

☑ The toolbar is displayed. (Default)

☐ The toolbar is hidden.

Toolbar Text

☑ Textual items are added to the toolbar icons.

☐ No textual items are added to the toolbar icons. (Default)

Status Bar

☑ The status bar is displayed. (Default)

☐ The status bar is hidden.

Macro Manager

☑ The Macro Manager toolbar is displayed.

☐ The Macro Mananger toolbar is hidden. (Default)

Right Mouse Button Popup Keypad

☑ Right-clicking will bring up the the Popup Keypad.

☐ Right-clicking will bring up the default menu. (Default)

Scratch Pad

☑ The Scratch Pad (integrated basic text editor) is displayed.

☐ The Scratch Pad (integrated basic text editor) is hidden. (Default)

'Save' in Scratch Pad

☑ The **Save** button in the Scratch Pad is active.

☐ The **Save** button in the Scratch Pad is inactive. (Default)

Quick Connect

☑ The Quick Connect toolbar is displayed.

☐ The Quick Connect toolbar is hidden. (Default)

Search Text

☑ The Search Text area is displayed.

☐ The Search Text area is hidden. (Default)

Screen History

☑ The Screen History area is displayed.

☐ The Screen History area is hidden. (Default)

History Screen Type Simple (Text)

☑ The History Screen will be displayed black and white.

☐ The History Screen will have the default terminal (green screen) look and feel. (Default)

Menu Bar

☑ The main menu bar is displayed. (Default)

☐ The main menu bar is hidden.

_____

- Window (see page 1515)
- Preferences Start Options (see page 1516)
- Language (see page 1517)
- Keyboard (see page 1518)
- Popup Keypad (see page 1519)
- Toolbar (see page 1520)

Window

Here you can define how the iAccess client application window is positioned and sized by default on start. If you leave the fields empty, the window will be positioned and sized automatically.

Menu path: **Sessions > IBM iAccess Client > [session name] > Preferences > Window**

Width: Width of the window

Height: Height of the window

Horizontal offset: Horizontal offset of the window

Vertical offset: Vertical offset of the window

Preferences Start Options

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Start Options**

Session ID

Possible values:

- Automatic (Default)
- [Various alphabetic values]

Language

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Language**

Emulation Language

Possible values:

- Default: The language of the IGEL User Interface (**User Interface** > **Language**) will be used.
- [Various languages]

Keyboard

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Keyboard**

Keyboard Remapping File: Enter the file name (Default: IBMi.kmp)

The directory `/userhome/IBM/iAccesClient/Emulator` is used by default.

Popup Keypad

Menu path: **Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Popup Keyboard**

Popup Keypad File: Enter the file name.

The directory `/userhome/IBM/iAccesClient/Emulator` is used by default.

Toolbar

Menu path: Sessions > IBM iAccess Client > iAccess Sessions > [session name] > Preferences > Toolbar

Toolbar File: Enter the file name.

The directory `/userhome/IBM/iAccesClient/Emulator` is used by default.

ThinLinc Global

In this area, you can change the global settings for ThinLinc sessions.

Menu path: **Sessions > ThinLinc > ThinLinc Global**

- Server (see page 1522)
- Window (see page 1523)
- Options (see page 1524)
- Optimization (see page 1526)
- VNC Optimization (see page 1527)

Server

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Server**

You can specify the port for communication between the client and server and allow remote monitoring of the client through shadowing.

- **SSH port**
  Possible values:
  - Default SSH (22): Port 22 is used. (Default)
  - HTTP (80): Port 80 is used.
  - Custom: Under **Custom port number**, you can enter an alternative port number.
- **Custom port number**: Alternative port number
- **Allow shadowing**
  ☑ The session can be remote monitored by shadowing via VNC.
  ☐ The session cannot be remote monitored by shadowing. (default)

Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Window**

In this area, you can define the window settings for ThinLinc sessions.

Screen size
Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor": The entire display area of the current monitor is used for the ThinLinc session. (Default)
- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

Custom screen width: Width of the display area for the session in pixels.

Custom screen height: Height of the display area for the session in pixels.

Full-screen mode

☑ The entire display area is used for the ThinLinc session. (Default)

Full-screen all monitor

☑ The entire display area of all monitors is used for the ThinLinc session. (Default)

Control bar for ThinLinc sessions

☑ If the ThinLinc session takes place in full-screen mode, an in-session control bar will be shown. You can minimize or close the session with the control bar. Further information can be found under In-Session Control Bar (see page 1872).

☐ The in-session control bar will not be shown. (Default)

Options

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Options**

You can change various settings and enable local directories.

Enable sound

☑ Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.

☐ Audio output will not be forwarded to the device. (Default)

Redirect serial port

☑ The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.

☐ The serial port data will not be forwarded to the server. (Default)

Enable printer

☑ The local printer can be used in the ThinLinc session. (Default)

☐ The local printer cannot be used in the ThinLinc session.

Enable smartcard readers

☑ The server has access to the device's local smartcard reader.

☐ The server does not have access to the local smartcard reader. (Default)

Enable drive access

☑ The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.

☐ The server does not have access to local directories. (Default)

Exported Paths and Permissions

To edit the list, proceed as follows:

- Click on + to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

To select a local directory for server-side access, proceed as follows:

1. Click on +.
2. In the **Path** field, enter the local directory path. Example: `/userhome`
3. Select the **Permission** that the server is to have for the directory.
   - Read only: The server has read rights for the directory but no write rights.
   - Read/write: The server has read and write rights for the directory.

- Disabled: The server has no read rights and no write rights for the directory.

> If you set a directory to “Disabled”, ensure that it is not a sub-directory of a directory for which the server has read or write rights.

4. Click on **Ok**.

Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Enable custom compression level**
  ☑ You can specify how much the data transmitted between the client and server are compressed.
  ☐ The default value will be used for the compression level. (default)
- **Compression level**: Allows you to select the compression level; 9 is the highest compression (default: 8)
- **Enable JPEG compression**: If this option is enabled, graphical data will be compressed using the JPEG procedure.
  ☑ Graphical data will be compressed in accordance with the JPEG procedure. (default)

> A higher JPEG compression level saves bandwidth but reduces the image quality.

- **JPEG quality**: Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)
- **SSH compression**
  ☑ The data will be compressed using SSH compression.
  ☐ The data will not be compressed using SSH compression. (default)

VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Global > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

VNC autoselect

☑ The preferred coding and color depth will be specified automatically. (Default)

☐ The **Preferred coding** and **Color depth** can be specified by the user.

Preferred encoding: Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.
Possible values:

- "Tight": Suitable for slow networks too. (Default)
- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

Color depth: Allows you to select the color resolution.
Possible values:

- "Full (all colors)": The maximum value set on the server is used. (Default)
- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"

ThinLinc Session

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name]**

->Click on + **Add** to create a ThinLinc session.

In this area, you can configure desktop integration for the ThinLinc session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Server (see page 1531)
- Login (see page 1532)
- ThinLinc Sessions Window (see page 1534)
- Options (see page 1535)
- ThinLinc Sessions Optimization (see page 1536)
- VNC Optimization (see page 1537)
- User Interface (see page 1538)
- Desktop Integration (see page 1539)

Server

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**

Server: Name or IP address of the ThinLinc server

User: User name for the connection to the ThinLinc server

Password: Password for the connection to the ThinLinc server

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Use global SSH port settings

☑ The port set under **Sessions > ThinLinc > ThinLinc Global > Server** will be used. (Default)

☐ The port set in **SSH port** or **Custom port number** will be used.

SSH port
Possible values:

- Default SSH (22): Port 22 is used. (Default)
- HTTP (80): Port 80 is used.
- Custom: Under **Custom port number**, you can enter an alternative port number.

Custom port number: Alternative port number

Login

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Login**

Method of authentication: A method used for the authentication.
Possible values:

- "Password" (Default)
- "Public key"
- "Smartcard"
- "Kerberos"

User: The user credentials are taken from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User**.

Password: A password specified under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > Password** is used for the authentication. (Available if **Password** is selected as **Method of authentication**).

> If modified here (under **Login**), **User** and **Password** will automatically be changed under **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server**.

The following settings can be configured if **Smartcard** is used as a **Method of authentication**.

Smartcard only

Use certificate subject as name for login

☑ The certificate subject will be used as login name. (Default)

☐ The user credentials from **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Server > User** will be used as login name.

Connect the client automatically if a smartcard is found

☑ The client will be connected automatically if a smartcard is detected (available if **Use subject of smartcard as name for login** is enabled). (Default)

☐ The client will not be connected automatically by the smartcard detection.

Disconnect the client automatically when the smartcard is removed

☑ The client will be disconnected automatically if the smartcard is removed. (Default)

☐ The client will not be disconnected at the smartcard removal.

Allow transmission of the smartcard's passphrase for logging in

☑ The transmission of the smartcard's passphrase for logging in is allowed.

☐ The transmission of the smartcard's passphrase for logging in is not allowed. (Default)

> The transmission of the smartcard's passphrase is not recommended by Cendio.

Smartcard filter: The smartcard filter must be specified in the format described under "SMARTCARD_FILTER_n" in https://www.cendio.com/resources/docs/tag/clientconf.html.

ThinLinc Sessions Window

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Window**

In this area, you can define the window settings for the specific ThinLinc session.

> You can enable the in-session control bar for ThinLinc sessions only in the global settings, see Window (see page 1523).

Use global screen settings

☑ The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Window** will be used. (Default)

☐ The settings for this session are defined here.

Screen size
Possible values:

- "800x600"
- "1024x768"
- "1280x1024"
- "1600x1200"
- "Current monitor": The entire display area of the current monitor is used for the ThinLinc session. (Default)
- "All monitors": The display area of all monitors is used for the ThinLinc session.
- "Work area (maximized)": The display area of the current monitor minus the height of the taskbar is used for the ThinLinc session.
- "Custom size": The display area specified with **Custom screen width** and **Custom screen height** is used for the ThinLinc session.

Custom screen width: Width of the display area for the session in pixels.

Custom screen height: Height of the display area for the session in pixels.

Full-screen mode

☑ The entire display area is used for the ThinLinc session. (Default)

Full-screen all monitor

☑ The entire display area of all monitors is used for the ThinLinc session. (Default)

Options

You can change various settings and enable local directories.

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Options**

Use global shadowing settings

☑ The option **Setup > Sessions > ThinLinc > ThinLinc Global > Server > Enable Shadowing** will be used.

☐ The global setting **Enable shadowing** will not be used for this session.

Enable shadowing

☑ The session can be monitored remotely by shadowing via VNC.

☐ The session cannot be remotely monitored by shadowing. (Default)

Use global resourse settings

☑ The settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Options** will be used. (Default)

☐ The settings for this session are defined here.

Enable sound

☑ Audio output will be forwarded from the server to the device. The audio data can then be played back via the built-in loudspeaker or the headset.

☐ Audio output will not be forwarded to the device. (Default)

Enable serial port

☑ The serial port data will be forwarded from the device to the server. The serial port can be used in the ThinLinc session.

☐ The serial port data will not be forwarded to the server. (Default)

Enable printer

☑ The local printer can be used in the ThinLinc session. (Default)

☐ The local printer cannot be used in the ThinLinc session.

Enable smartcard readers

☑ The server has access to the device's local smartcard reader.

☐ The server does not have access to the local smartcard reader. (Default)

Enable drive access

☑ The server has access to local directories. These directories can be selected in the **Exported Paths and Permissions** area.

☐ The server does not have access to local directories. (Default)

Options popup key: Key to be used for opening the options menu during the session. (Default: F8)

ThinLinc Sessions Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Optimization**

You can select a suitable compression procedure in order to optimize the transmission speed between the client and server.

- **Use global compression level**
  ☑ The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use custom compression level** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Compression level** selection will be used. (default)
  ☐ The specific settings for this session will be used.
- **Enable custom compression level**
  ☑ You can specify how much the data transmitted between the client and server are compressed.
  ☐ The default value will be used for the compression level. (default)
- **Compression level**: Allows you to select the compression level; 9 is the highest compression (default: 8)
- **Use global JPEG quality settings**
  ☑ The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > Use JPEG compression** option and **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > JPEG Quality** selection will be used. (default)
  ☐ The specific settings for this session are defined here.
- **Enable JPEG compression**

  > A higher JPEG compression level saves bandwidth but reduces the image quality.

  ☑ Graphical data will be compressed in accordance with the JPEG procedure. (default)
- **JPEG quality**: Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 7)
- **Use global SSH connection settings**
  ☑ The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > Optimization > SSH Compression** option will be used. (default)
  ☐ The specific setting for this session will be used.
- **SSH compression**
  ☑ The data will be compressed using SSH compression.
  ☐ The data will not be compressed using SSH compression. (default)

VNC Optimization

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > VNC Optimization**

You can change VNC protocol settings in order to optimize transmission.

Use global VNC settings

☑ The global settings under **Setup > Sessions > ThinLinc > ThinLinc Global > VNC optimization** will be used. (Default)

☐ The specific settings for this session are defined here.

VNC auto select

☑ The **Preferred encoding** and **Color level** will be specified automatically. (Default)

☐ The **Preferred encoding** and **Color level** can be specified by the user.

Preferred encoding: Specifies how the data to be transmitted are to be coded. The coding is negotiated between the client and server.
Possible values:

- "Tight": Suitable for slow networks too. (Default)
- "ZRLE": Compatible with RealVNC.
- "Hextile": Recommended for fast networks.
- "Raw": No compression.

Color level: Allows you to select the color resolution.
Possible values:

- "Full (all colors)": The maximum value set on the server is used. (Default)
- "Medium (256 colors)"
- "Low (64 colors)"
- "Very low (8 colors)"

User Interface

Menu path: **Setup > Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > User Interface**

You can change the fields and settings options of the logon window as well as the **ThinLinc Client Options** dialog.

Lock server name

☑ The server name given under **Setup > Sessions > ThinLinc Sessions > Server** will be used and it will not be possible to change it in the logon window. (default)

Hide options button

☑ The **Options** button will not appear in the logon window. The **ThinLinc Client Options** dialog therefore cannot be opened. (default)

Advanced mode

☑ The fields that can be opened under **Advanced** will appear when starting the session.

☐ The fields that can be opened under **Advanced** will not appear when starting the session. (default)

Lock ThinLinc options tab

☑ The settings in the **Options** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

Lock Local Devices options tab

☑ The settings in the **Local Devices** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

Lock ThinLinc Screen tab

☑ The settings in the **Screen** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

Lock ThinLinc Optimization tab

☑ The settings in the **Optimization** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

Lock Security tab

☑ The settings in the **Security** tab of the **ThinLinc Client Options** dialog cannot be changed. (default)

Debug level: Specifies how detailed the debugging information is to be. 1 is the lowest level (default), 5 is the highest.

Desktop Integration

Menu path: **Sessions > ThinLinc > ThinLinc Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the ThinLinc session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

SSH Session

Menu path: **Sessions > SSH > [Session Name]**

You can launch applications on a remote computer via SSH (Secure Shell). The display is usually on the terminal; X11 connections too can be routed via SSH.

->Click on + **Add** to create an SSH session.

In the following area, you can configure desktop integration for the SSH session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- SSH Command (see page 1545)
- Options (see page 1546)
- Desktop Integration (see page 1547)

SSH Command

Menu path: **Sessions > SSH > [Session Name] > Command**

Remote user name: User name under which the application runs on the remote computer If you do not give a name, you will be asked when the session starts.

Remote host: Host name or IP address of the remote computer.

Command line: Command which is to be executed on the remote computer immediately after logging in.

Options

Menu path: **Sessions > SSH > [Session Name] > Options**

As of IGEL OS 11.04.100, SSHv1 is no longer supported. Migrate to SSHv2 if you have not yet done so.

Here, you can change the following settings:

Enable X11 connection forwarding

☑ X11 applications on the remote computer that are launched via the SSH session will be shown on your device. (Default)

☐ No X11 programs can be launched on the remote computer via the SSH session.

Enable compression

☑ The data will be compressed for transmission.

Port: SSH port. (Default: 22)

Desktop Integration

Menu path: **Sessions > SSH > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the SSH session.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

VNC Viewer Sessions

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name]**

With the VNC viewer, you can access the graphical user interface of a remote computer.

->Click on + to create a VNC viewer session.

The settings for starting the session are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- VNC Viewer Connection (see page 1553)
- VNC Viewer Compression (see page 1554)
- Input (see page 1555)
- VNC Viewer Misc (see page 1556)
- Desktop Integration (see page 1557)

VNC Viewer Connection

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Connection**

- **Name or IP address of VNC server**: Host name or IP address of the VNC server
- **Password**: User password for logging on to the VNC server, if necessary

⚠ Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

VNC Viewer Compression

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Compression**

- **Compression level (default = 2)**: Allows you to select the compression level; 9 is the highest compression (default: 2)
- **JPEG quality level**: Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (default: 8)

Input

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Input**

Here, you can change the settings for keyboard input for the VNC session.

- **View only**
  ☑ Mouse and keyboard inputs are not forwarded to the remote computer. You can only observe the remote computer.
  ☐ Mouse and keyboard inputs are forwarded to the remote computer. You can remote control the remote computer. (default)
- **Pass system keys directly to the server (full-screen)**
  ☑ You can use system key combinations in the VNC session, e.g. [Alt] + [Tab]. (default)
  ☐ System key combinations cannot be used in the VNC session.
- **Menu key**: Key which brings up the menu.
  Possible options (default: F8):
  - [F2] ... [F12]
  - [Pause]
  - [Print]
  - [Scroll lock]
  - [Esc]
  - [Ins]
  - [Del]
  - [Home]
  - [Page up]
  - [Page down]

VNC Viewer Misc

Menu path: **Setup > Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Misc**

Shared mode

☑ When starting a session, other users' sessions with the same server are not terminated. The sessions run alongside each other with equal status.

☐ If another user has a VNC session with the same server, the other user's session will be terminated when the session is started. (default)

Fullscreen mode

☑ The session will be shown in full-screen mode. The taskbar is not visible.

☐ The taskbar is visible. (default)

Color level: Number of possible colors
Possible values:

- Default: The highest available color depth will be used. (Default)
- Very low (8 colors)
- Low (64 colors)
- Medium (256 colors)

Desktop Integration

Menu path: **Sessions > VNC Viewer > VNC Viewer Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Firefox Browser Global Settings in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global**

In this area, you can define the start page, display resolution, and font size for the browser.

You can change the following settings:

When browser starts: Specifies what pages are shown when the browser is launched.

- Start with a blank page
- Show my start page (default)
- Resume previous session: All tabs from the last session are reopened.

Start page: Specifies the URL of the start page. You can specify the number of start pages by separating the URLs of the start pages with a vertical dash "|".

Default web browser: Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront.
Possible options:

- "Firefox Browser"
- "Chromium Browser"

Display resolution: Specifies the display resolution for the browser in DPI. Typical values are **72** for medium screens and **96** for large screens.
Possible values:

- System setting (Default)
- (Various discreet values)

Minimum font size: Specifies the minimum size of the fonts displayed on websites. The formats of the websites are overwritten in the process.
Possible values:

- None: The fonts can be as small as you like. (default)
- (Various discreet values)

Show browser splash screen

☑ While the browser is starting, a Firefox logo will be shown in the middle of the screen. (default)

☐ No Firefox logo will be shown.

For information on the kiosk mode, see How to Use the Firefox Browser in Kiosk Mode (see page 573).

> Please note: With an enabled **Browser content redirection** under **Sessions > Citrix > Citrix Global > HDX Multimedia**, any H.264 multimedia content within Firefox (incl. video playback) is not functional anymore. These two features cannot be used simultaneously. See HDX Multimedia Settings for an IGEL OS Citrix Session (see page 1276).

- Firefox Browser Global Tabs in IGEL OS (see page 1562)
- Firefox Browser Global Content in IGEL OS (see page 1563)
- Firefox Browser Global Print in IGEL OS (see page 1565)
- Firefox Browser Global Proxy (see page 1566)
- Firefox Browser Global Privacy in IGEL OS (see page 1569)

- Security (see page 1571)
- Advanced (see page 1572)
- Firefox Browser Global Encryption (see page 1575)
- Certificates in the Firefox Browser in IGEL OS (see page 1576)
- Smartcard Middleware for Firefox Browser in IGEL OS (see page 1577)
- Restart (see page 1579)
- Window (see page 1580)
- Menus & Toolbars (see page 1581)
- Firefox Browser Global Hotkeys in IGEL OS (see page 1585)
- Firefox Browser Global Context in IGEL OS (see page 1586)
- Firefox Browser Global Commands (see page 1587)

Firefox Browser Global Tabs in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Tabs**

In this area, you can define settings for the browser tabs.

New pages should be opened in: Specifies how links to new pages are to be opened.

Possible values:

- Current window: The page will open in the current window, even if the link defines a new window as the target.
- New window: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new window. (default)
- New tab: If the link does not define a target, the page will open in the current window. If the link defines a new window as the target, the page will open in a new tab.

Warn me when closing multiple tabs

☑ A warning will be shown as soon as you attempt to close a browser window with a number of tabs.

☐ No warning will be shown if you close a number of browser windows. (default)

Warn me when opening multiple tabs might slow down the browser

☑ A warning will be shown if a very large number of tabs are loaded simultaneously. (default)

☐ No warning will be shown if a very large number of tabs are loaded simultaneously.

When a link is opened in a new tab, switch to it immediately

☑ When a new tab is opened via a link, the focus will switch to the new tab.

☐ When a new tab is opened via a link, the focus will not change. (default)

Firefox Browser Global Content in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Content**

In this area, you can change settings regarding popups, JavaScript, downloads and the browser display.

Block pop-up windows

☑ The automatic opening of popup windows by websites will be blocked. With **Exceptions...**, you can allow popups to be opened automatically for specific websites.

☐ The automatic opening of popup windows will not be blocked. (default)

To add an exception for the automatic opening of popups, proceed as follows:

1. Click on **Exceptions...**.
2. Click on ＋.
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Click on **Ok**.

Load images automatically

☑ Websites will be loaded fully including all images. (default)

☐ Images in websites will not be loaded; placeholders will be shown instead of the images. As a result of this, websites can be loaded more quickly, but the layout is impaired. With **Exceptions...** you can allow or prevent automatic loading for specific websites.

To add an exception for the automatic loading of images, proceed as follows:

1. Click on **Exceptions...**.
2. Click on ＋.
3. In the **Website** field, give the URL of the website for which the exception is to apply.
4. Using the **Status** drop-down menu, specify whether the automatic loading of images is to be allowed or prevented for the given website.
5. Click on **Ok**.

Type of download directory
Specifies the directory in which a downloaded file is saved.

- User directory: The file is saved locally on the thin client desktop.
- Custom path: You can specify whether the downloaded file is to be opened with an application or saved locally. (default)

Download path
Local directory in which the downloaded file is saved if **Type of download directory** is set to **Custom path**. (default: `/tmp`)

Enable JavaScript

☑ JavaScript code will be executed on websites. (default)

☐ JavaScript code will not be executed.

Raise or lower windows

☑ A website can place windows in the background or foreground via JavaScript. (default)

☐ Websites cannot place windows in the background or foreground via JavaScript.

Move or resize existing windows

☑ A website can move windows or change the window size via JavaScript.

☐ Websites cannot move windows or change the window size via JavaScript. (default)

Disable or replace context menus

☑ A website can define a custom context menu via JavaScript; the browser's own context menu will be suppressed in the process.

☐ Websites cannot define a custom context menu.

Languages for web pages
One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With `de, en, fr, it`, the website will be shown in German, if available, otherwise in English, etc.

Firefox Browser Global Print in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Print**

In this area, you can set the default paper size for the printer.

Use system settings for default paper size

☑ The globally set paper size will be used when printing websites. (Default)

☐ You can set the paper size via **Default paper size**.

Default paper size: Preset paper size when printing websites.
Possible values:

- Letter
- Legal
- Executive
- A5
- A4 (Default)
- A3

Firefox Browser Global Proxy

In this area, you can change the proxy configuration.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Proxy**

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** pull-down menu, select the type of proxy configuration.
   The following proxy configurations are available:
   - Direct connection to the Internet (Default)
   - Manual proxy configuration
   - Automatic proxy configuration
   - System-wide proxy configuration
   - Auto-detect proxy settings for this network
2. Enter the necessary configuration data for the selected proxy configuration.

Direct Connection to the Internet

With this proxy configuration, no proxy is used.

Manual Proxy Configuration

The configuration data must be specified in the following fields.

FTP proxy: URL of the proxy for FTP

Port: Port of the proxy for FTP

HTTP proxy: URL of the proxy for HTTP

Port: Port of the proxy for HTTP

SSL proxy: URL of the proxy for SSL

Port: Port of the proxy for SSL

SOCKS host: URL of the proxy for SOCKS

Port: Port of the proxy for SOCKS

SOCKS protocol version: Version of the SOCKS protocol used (default: SOCKS v5)

No proxy for: List of URLs for which no proxy is to be used (default: `localhost, 127.0.0.1`)

Proxy realm: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

> The **Proxy realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy]:[Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:

In the example above, the value for the **Proxy realm** field is as follows: `moz-proxy://172.30.178.10:8080`

Use passthrough authentication: This option can be used if the local thin client logon takes place via Kerberos.

☑ The logon information saved temporarily when logging on to the thin client will be carried over when logging on to the proxy.

User name: User name with which the browser authenticates itself for the proxy.

Password: Password with which the browser authenticates itself for the proxy.

Do not prompt for proxy authentication if credentials are saved

☑ If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Automatic Proxy Configuration

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

URL: URL of the proxy configuration file

Do not prompt for proxy authentication if credentials are saved

☑ If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

System-Wide Proxy Configuration

With this proxy configuration, the proxy configured under **Setup > Network > Proxy** will be used.

Do not prompt for proxy authentication if credentials are saved

☑ If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Auto-Detect Proxy Settings for This Network

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.

Do not prompt for proxy authentication if credentials are saved

☑ If logon data are already saved in the browser, the user will not be asked for a user name and password. (default)

This option should not be enabled in multiuser environments. If this option is enabled in a multiuser environment, a user can use the logon data of a previous user.

Firefox Browser Global Privacy in IGEL OS

In this area, you can configure settings relevant to data protection.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Privacy**

Save browsing history (in days): Specifies how long your browsing history will be stored. If you select **Do not store history**, all browsing history data will be lost when the browser restarts. (default: 9)

All browsing history data stored before the period specified here will be lost.

Save information entered in forms and the search bar

☑ Entries in forms and search bars will be retained after the browser restarts.

☐ Entries in forms and search bars will be retained only for the duration of the session. (default)

Remember passwords

☑ Passwords entered will be retained after the browser restarts.

☐ Passwords entered will be retained only for the duration of the session. (default)

Clear private data when closing browser

☑ Data entered will be deleted when the browser is closed. What data are deleted is specified in the following options.

☐ Data entered will not be deleted when the browser is closed. (default)

Select the Items to Be Cleared

The options in this area are effective if **Clear private data when closing browser** is enabled.

Browsing & download history

☑ Addresses (URLs) of visited websites and the list of downloads will be deleted when the browser is closed. (default)

Form & search history

☑ Entries in the search window and in website forms will be deleted when the browser is closed. (default)

Saved passwords

☑ Passwords entered will be deleted when the browser is closed.

☐ Passwords entered will be retained after the browser restarts. (default)

Cookies

☑ Cookies will be deleted when the browser is closed. (default)

Cache

☑ The cache for temporarily saving websites will be emptied when the browser is closed. (default)

Active logins

☑ Ongoing sessions on websites will be terminated when the browser is closed and will need to be restarted after the browser restarts. (default)

☐ Ongoing sessions on websites will be retained after the browser restarts.

Allow private browsing feature

☑ You can open one or more private windows in the browser. All data from private windows will be deleted after the browser is closed.

☐ Private windows cannot be opened. (default)

Always start in private browsing mode

☑ The browser will start in private mode. All data will be deleted after the browser is closed.

☐ The browser will start in default mode. (default)

Enable "Do Not Track" feature

☑ The browser will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded. (default)

The browser will use the `DNT` ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when `DNT` is set to 1.

Enable built-in tracking protection

☑ The browser will block specific domains and websites that use tracking. The browser has an internal list for selecting the domains and websites to be blocked. (default)

If tracking protection is enabled, a shield symbol will be shown at the left-hand edge of the address bar.

Suggest visited sites in URL bar

☑ Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history. (default)

Suggest only typed visited sites

☑ The suggestions will be based only on the websites that were typed directly into the address bar. Websites that were visited via bookmarks or links in other websites will not be used for the suggestions.

☐ Websites that were visited via bookmarks or links in other websites will also be used for the suggestions. (default)

Suggest bookmarked sites in URL bar

☑ Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on bookmarks. (default)

Suggest open tabs in URL bar

☑ Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously opened tabs. (default)

Security

In this area, you can define settings for preventing phishing and malware.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Security**

Safe browsing

☑ The browser will check each address entered as to whether it can be found in the black list of fraudulent websites which use phishing. If this is the case, you will be given a warning.

☐ The browser will not check whether an address is on the black list of fraudulent websites.

Malware protection

☑ The browser will check before a file is downloaded whether the relevant website can be found in the black list of fraudulent websites which provide malware for downloading. If this is the case, you will be given a warning.

☐ The browser will not check whether an address is on the black list of fraudulent websites which provide malware for downloading.

Hide local filesystem

☑ The local file system will not be shown in the dialogs for saving data. The user cannot change the location for saving files.

☐ The local file system will be shown in the dialogs for saving data.

Advanced

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Advanced**

In this area, you can change various settings as well as add or change custom configuration parameters.

You can change the following settings:

Use old search bar

☑ The logo of the search engine currently set will be shown in the search window.

☐ The search engine currently set will not be shown in the search window, and search suggestions will be shown in the drop-down menu. (default)

Caret browsing on browser start

☑ Caret browsing is enabled when the browser starts. If caret browsing is enabled, you can navigate with the keyboard in websites without using the mouse. With the insertion mark, you can copy text to the clipboard.

> You can enable or disable caret browsing at any time by pressing [F7]. To prevent caret browsing being disabled, you will also need to enable the **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys > Disable hotkeys for caret browsing** option.

☐ Caret browsing is not enabled when the browser starts. (default)

Find as you type

☑ Search suggestions that match the characters typed will be shown while you type.

☐ No search suggestions will be shown while you type. (default)

Warn me when websites try to redirect or reload the page

☑ A message window will be shown as soon as a website tries to get the browser to load another website or reload the current page.

☐ No message window will be shown if a website tries to load another website or reload the current page. (default)

Check my spelling as I type
Possible options:

- "Off": Your spelling will not be checked while you type.
- "On for text fields": Your spelling will be checked if you are typing in text fields with multiple lines. (default)
- "On for text fields and lines": Your spelling will be checked if you are typing in text fields with one line or multiple lines.

Use autoscrolling

☑ You can launch automatic page scrolling by clicking on the middle mouse button to place a scroll symbol in the text and then positioning the mouse pointer above or below the anchor.

☐ Autoscrolling is disabled. (default)

Use smooth scrolling

☑ You can browse through a page using the [Page Up/Down] keys smoothly as with scrolling.

☐ When you press the [Page Up/Down] keys, the display will jump immediately. (default)

Disable GStreamer in Browser

☑ GStreamer will not be used to play back videos. This may be a good idea if you experience problems when playing back videos.

> We recommend that you disable this option if there is no multimedia codec pack installed on your thin client and you wish to view videos on HTML5 websites.

☐ GStreamer will be used to play back videos.

Disable OpenGL acceleration

☑ Hardware acceleration with OpenGL will not be used. This may be a good idea if you experience problems with OpenGL applications.

To add a custom preference, proceed as follows:

> Changes to the advanced Firefox browser settings can impair its stability, security and speed. IGEL Support is not responsible for problems caused by changing the browser configuration, even if the browser configuration was changed in the IGEL setup.

> Custom preferences can also be changed in the browser via `about:config`. To do this, the **Firefox Browser > Firefox Browser Global > Window > Hide configuration page of the browser** option must be disabled.

Custom Preferences

In this area, you can add custom preferences.

→ Click + to get to the **Add** dialogue.

In the **Add** dialogue, you can define the following settings:

Active: Defines whether the preference is active.

☑ The preference is active. (Default)

☐ The preference is not active.

Mode: The mode of the preference.
Possible values:

- "pref": You can change the value in the browser via `about:config`. When the browser restarts, this change will be lost and the value set here will be used. (Default)
- "defaultPref": You can change the value in the browser via `about:config`. When the browser restarts, this change will remain.
- "lockPref": You cannot change the value in the browser via `about:config`.

- "clearPref": You cannot change the value in the browser via `about:config` and the value will not be shown via `about:config.`

Custom preference: The name of the custom preference. Example: `ui.textSelectBackground`

Type: The type of the custom preference.
Possible values:

- "String": The value is a string of characters.
- "Integer": The value is a whole number.
- "Boolean": The value is a Boolean value, i.e. `true` or `false`. (Default)

Value: The value of the custom preference. The possible entries depend on the **Type** selected.

→ Click **Ok** to add the custom preference.
The custom preference will take effect the next time that the browser is launched.

You will find information regarding custom preferences in Firefox in the MozillaZine Knowledge Base under Firefox About:config entries[184].

184. http://kb.mozillazine.org/About:config_entries

Firefox Browser Global Encryption

In this area, you can define the settings for encryption methods.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Encryption**

Minimum required encryption protocol: This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.
Possible options:

- SSL3 (Default)
- TLS 1.0
- TLS 1.1
- TLS 1.2

Maximum supported encryption protocol: This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.
Possible options:

- SSL3
- TLS 1.0
- TLS 1.1
- TLS 1.2 (Default)

Certificates in the Firefox Browser in IGEL OS

In this area, you can define the settings for certificate validation.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Certificates**

When a website requests a certificate: Specifies how the browser behaves if a website requests a security certificate.
Possible values:

- Select one automatically: The browser selects a certificate automatically. (Default)
- Ask me every time: A dialog window requesting the certificate will be displayed.

View certificates: If you click on this button, the certificates saved in the browser's **Certificate Manager** will be displayed.

Certificate validation: Specifies the validation of certificates using OCSP (Online Certificate Status Protocol).

- Do not use OCSP for certificate validation: The certificate will not be validated using OCSP.
- Validate a certificate if it specifies an OCSP server: The certificate will be validated with the OCSP server specified in the certificate. If no OCSP server is specified, no certificate validation will take place. (Default)
- Validate all certificates with the following OCSP server: All certificates will be validated with the OCSP server specified under the **Service URL**, irrespective of which OCSP server is specified in the certificate.

Response signer: Signer of the response from the OCSP server

Service URL: URL of the OCSP server

When an OCSP server connection fails, treat the certificate as invalid:

☑ If, owing to a failed connection to the OCSP server, no validation can take place, the certificate will be treated as invalid. In this case, the browser will show the “This connection is not trusted” error message.

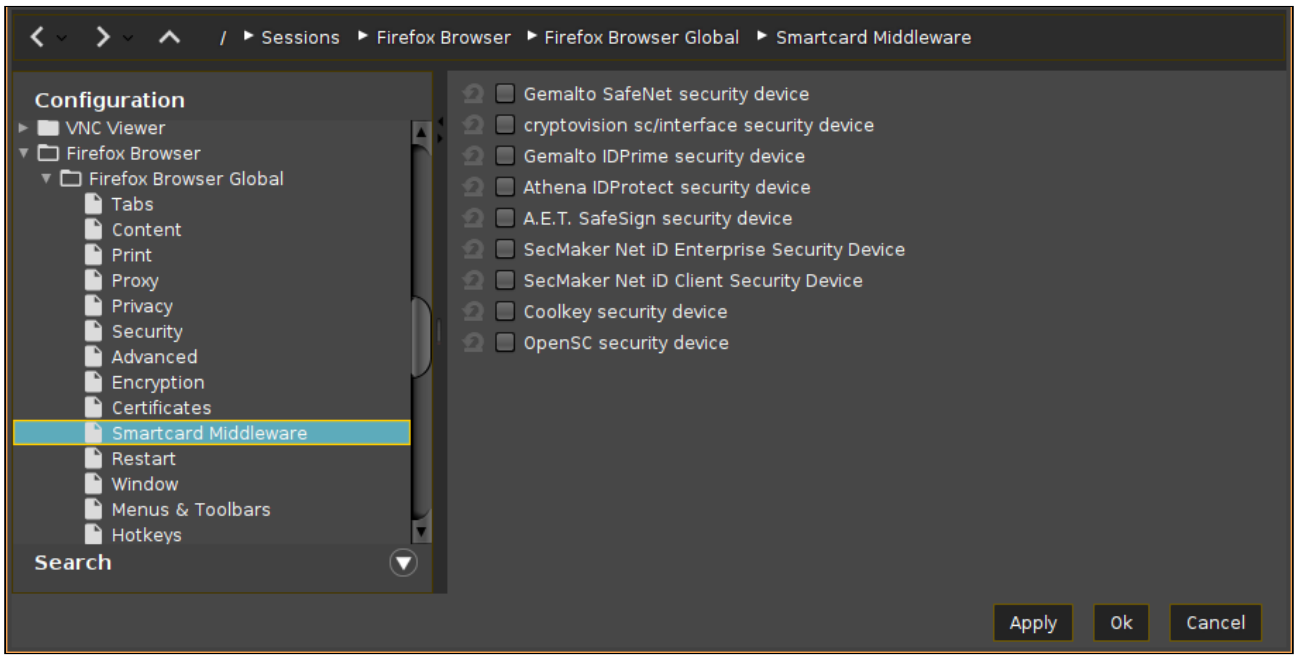
☐ The certificate will not be deemed invalid if no check can take place because there is no connection to the OSCP server. (default)

Smartcard Middleware for Firefox Browser in IGEL OS

In this area of the IGEL Setup, you can activate or deactivate smartcard middleware (PKCS#11 module) that is to be used for encryption. If you want to use your own PKCS#11 library with the Firefox browser, see Using a Custom PKCS#11 Library (see page 922).

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS (see page 791).

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware**



Gemalto SafeNet security device

☑ Gemalto/SafeNet eToken will be used for encryption.

☐ Gemalto/SafeNet eToken will not be used for encryption.*

cryptovision sc/interface security device

☑ cryptovision sc/interface will be used for encryption.

☐ cryptovision sc/interface will not be used for encryption.*

Gemalto IDPrime security device

☑ Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.

☐ Gemalto IDPrime will not be used for encryption.*

Athena IDProtect security device

☑ Athena IDProtect will be used for encryption.

☐ Athena IDProtect will not be used for encryption.*

A.E.T. SafeSign security device

☑ A.E.T. SafeSign will be used for encryption.

☐ A.E.T. SafeSign will not be used for encryption.*

Pointsharp Net iD Enterprise security device

☑ Pointsharp Net iD Enterprise, formerly known as "Pointsharp Net iD", will be used for encryption.

☐ Pointsharp Net iD Enterprise will not be used for encryption.*

Pointsharp Net iD Client security device

☑ Pointsharp Net iD Client will be used for encryption. For more on Pointsharp Net iD Client, see https://docs.pointsharp.com/net-id-client/latest/index.html

☐ Pointsharp Net iD Client will not be used for encryption.*

Coolkey security device

☑ Coolkey will be used for encryption.

☐ Coolkey will be not used for encryption.*

OpenSC security device

☑ OpenSC will be used for encryption.

☐ OpenSC will not be used for encryption.*

90meter security device

Licensed Feature

This feature requires an add-on license. Please contact your IGEL reseller.

☑ 90meter will be used for encryption.

☐ 90meter will not be used for encryption.*

* IGEL OS system default

Restart

In this area, you can specify whether the browser automatically starts and whether it is automatically restarted after being closed and after what delay time.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Restart**

Restart

☑ The browser automatically restarts if it was closed.

☐ The browser does not automatically restart if it was closed. (default)

Restart after idle time

☑ If no action on the part of the user has occurred after the idle time has elapsed, the browser will automatically be restarted.

☐ There will be no automatic restart after a specific idle time has elapsed. (default)

Idle time after which a restart occurs: Time interval after which the browser is automatically restarted if in the meantime no action on the part of the user has occurred. (default: 5)
The time unit can be selected under **Unit**.

Unit: Time interval for the idling time
Possible options:

- Minutes (Default)
- Seconds

Window

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Window**

In this area, you can define the window settings for a browser session.

Start in full-screen mode

☑ The browser will start in fullscreen mode.

☐ The browser will start in a standard window. (default)

Firefox translation: Language of the user interface
Possible values:

- System setting: The language set under **User Interface > Language > Language** will be used for the browser. (Default)
- English
- German
- French
- Dutch
- Spanish
- Italian

Hide configuration page of the browser

☑ The browser configuration page (`about:config`) is locked. As a result, the user cannot change the configuration. (Default)

☐ The browser configuration page (`about:config`) can be used.

Menus & Toolbars

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Menus & Toolbars**

In this area, you can change the browser's menus and toolbars.

Hide app menu/menu bar

☑ The button for opening the browser menu will not be shown.

☐ The button for opening the browser menu will be shown. (default)

Use old menu bar

☑ The browser menu will be shown in the menu bar as in earlier browser versions.

☐ The browser menu can be opened via a button. (default)

Hide the Following Items in App Menu/Menu Bar

Hide bookmarks menu

☑ The bookmarks menu will not be shown in the menu bar.

☐ The bookmarks menu will be shown in the menu bar. (default)

Hide tools menu

☑ The "Tools" menu will not be shown.

☐ The "Tools" menu will be shown. (default)

Hide history entry

☑ The button for showing the browser history will not be shown.

☐ The button for showing the browser history will be shown. (default)

Hide tabs toolbar

☑ The tabs will not be shown in the menu bar. The user cannot switch between a number of tabs.

☐ The tabs will be shown in the menu bar. (default)

Hide bookmarks toolbar

☑ The bookmarks toolbar will not be shown. (default)

☐ The bookmarks toolbar will be shown.

Hide sidebar

☑ The sidebar will not be shown.

☐ The sidebar will be shown. The bookmarks can be shown in the sidebar. (default)

Hide navigation toolbar

☑ The navigation bar will not be shown.

☐ The navigation bar will be shown. (default)

Hide the toolbar for searching the page

☑ The search bar will not be shown.

☐ The search bar will be shown. (default)

Toolbar Items

Hide URL input

☑ Only search terms can be entered in the entry field; URLs cannot be entered manually.

☐ Both search terms and URLs can be entered in the entry field. (default)

Hide "Print" button

☑ The button for printing websites will not be shown.

☐ The button for printing websites will be shown. (default)

Hide "Home" button

☑ The Home button will not be shown.

☐ The Home button will be shown. (default)

Hide "Search" input

☑ The search field will not be shown.

☐ The search field will be shown. (default)

Hide “Bookmarks” and “RSS Feed” button

☑ The button for displaying bookmarks and RSS feeds will not be shown.

☐ The button for displaying bookmarks and RSS feeds will be shown. (default)

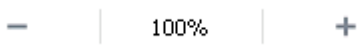
Toolbarconfig

User customization of toolbars

☑ The user can customize the toolbars. (default)

☐ The user cannot customize the toolbars.

Navigation toolbar: Specifies which symbols are shown in the navigation toolbar. The symbols are given as follows; multiple symbols should be separated by commas “,”:

loop-button	
zoom-controls	
edit-controls	

history-panelmenu	
privatebrowsing-button	
save-page-button	
find-button	
open-file-button	
developer-button	
sidebar-button	
feed-button	
print-button	
characterencoding-button	
social-share-button	
panic-button	

web-apps-button	
new-window-button	
fullscreen-button	
tabview-button	
downloads-button	

Application menu: Specifies which symbols are shown in the application menu. Multiple symbols should be separated by commas “,”.

Firefox Browser Global Hotkeys in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Hotkeys**

In this area, you can disable Firefox hotkeys.

Disable hotkey Quit/Close

☑ The hotkey for terminating/closing the browser is disabled.

☐ The hotkey for terminating/closing the browser is enabled. (default)

Disable hotkey for print dialog

☑ The hotkey for opening the print dialog is disabled.

☐ The hotkey for opening the print dialog is enabled. (default)

Disable hotkey for save page

☑ The hotkey for saving a website is disabled.

☐ The hotkey for saving a website is enabled. (default)

Disable hotkeys for opening new window/tab

☑ The hotkey for opening a new window or tab is disabled.

☐ The hotkey for opening a new window or tab is enabled. (default)

Disable hotkeys for opening a new webpage/location and download window

☑ The hotkey for opening a new website/location and the download window is disabled.

☐ The hotkey for opening a new website/location and the download window is enabled. (default)

Disable hotkeys to show history and page info

☑ The hotkey for showing the history and page information is disabled.

☐ The hotkey for showing the history and page information is enabled. (default)

Disable hotkeys for creating bookmarks

☑ The hotkey for creating a bookmark is disabled.

☐ The hotkey for creating a bookmark is enabled. (default)

Disable hotkeys for opening help pages

☑ The hotkey for displaying help is disabled.

☐ The hotkey for displaying help is enabled. (default)

Disable hotkeys for caret browsing

☑ The hotkey for starting caret browsing is disabled.

☐ The hotkey for starting caret browsing is enabled. (default)

Firefox Browser Global Context in IGEL OS

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Context**

In this area, you can disable various items in the browser context menu.

Disable navigation elements in context menu

☑ The navigation elements will not be shown in the context menu.

☐ The navigation elements will be shown in the context menu. (default)

Disable button for save page

☑ The button for saving a page will not be shown in the context menu.

☐ The button for saving a page will be shown in the context menu. (default)

Disable button for open new window/tab

☑ The button for opening a new window/tab will not be shown in the context menu.

☐ The button for opening a new window/tab will be shown in the context menu. (default)

Disable button for show info/source

☑ The button for showing page information/page source text will not be shown in the context menu.

☐ The button for showing page information/page source text will be shown in the context menu. (default)

Disable button for creating and editing bookmarks

☑ The button for creating and editing bookmarks will not be shown in the context menu.

☐ The button for creating and editing bookmarks will be shown in the context menu. (default)

Disable button for searching the web

☑ The button for searching the web will not be shown in the context menu.

☐ The button for searching the web will be shown in the context menu. (default)

Hide the browser's context menu

☑ The context menu will not be shown.

☐ The context menu will be shown. (default)

Firefox Browser Global Commands

In this area, you can define start options for browser commands.

Menu path: **Sessions > Firefox Browser > Firefox Browser Global > Commands**

The following commands are available:

Restart Browser

To open the dialogue for defining start options, proceed as follows:

1. Select the command. Example: **Restart Browser**
2. Click **Modify...**

The following start options are available:

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Firefox Browser Session

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name]**

In this area, you can configure desktop integration for the browser session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Settings (see page 1592)
- Desktop Integration (see page 1593)
- Plugins (see page 1596)

Settings

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

When browser starts: Specifies what pages are shown when the browser is launched.
Possible options:

- "Global setting" (Default)
- "Start with a blank page"
- "Show my home page"
- "Resume previous session": All tabs from the last session are reopened.

Start page: Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **When browser starts.**

Start monitor: Specifies the monitor on which the browser is launched. (Default: 1st monitor)

Autostart

☑ The browser is automatically launched when the system starts.

Desktop Integration

Menu path: **Sessions > Firefox Browser > Firefox Browser Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Firefox browser session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Plugins

Menu path: **Sessions > Firefox Browser > Plugins**

To obtain an overview of the plugins available in the browser, proceed as follows:

->Click on the **About:Plugins** button.
The browser will start with the `about:plugins` page. The plugins available in the browser will be shown.

Chromium Browser Global Session in IGEL OS

IGEL OS has a built-in Chromium browser. On this Setup page, you can set the default browser for IGEL OS, enable or disable hardware video acceleration and change the startup behavior of the Chromium browser.

The settings will be valid for all Chromium browser sessions.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global**

Use IGEL Setup for configuration

☑ The settings made in the IGEL Setup or the UMS configuration dialog will be effective.

☐ The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

Default web browser

Defines which browser will be chosen by the system, e.g. for opening Citrix Storefront.
Possible options:

- **Firefox Browser***
- **Chromium Browser**

Hardware Video Acceleration

☑ Hardware video acceleration is enabled for the Chromium browser.*
Please see How Can I Use H.264 Hardware Acceleration for Chromium or Firefox Browsers on IGEL OS Endpoint Devices? (see page 566)

☐ Hardware video acceleration is disabled for the Chromium browser.

Automatic browser restart on exit

☑ Chromium is restarted when the user closes it.

☐ Chromium is not restarted on exit.*

Show browser splash screen

☑ The Chromium splash screen is shown at the start.

☐ Chromium starts without a splash screen.*

- General Settings (see page 1599)
- Content (see page 1600)
- Proxy (see page 1601)
- Privacy (see page 1603)
- Security (see page 1605)
- Encryption Settings for the Chromium Browser in IGEL OS (see page 1606)

- Menus & Toolbars for the Chromium Browser Global in IGEL OS (see page 1607)
- Window (see page 1608)
- Custom Setup (see page 1609)
- Smartcard Middleware for Chromium Browser in IGEL OS (see page 1613)

*IGEL OS system default

General Settings

In this area, you can change the following settings for Chromium Browser Global

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > General**

On startup: Specifies what pages are shown when Chromium is launched.
Possible options:

- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

Startup page: Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Open a specific page or set of pages" is chosen under **On startup.**

New tab page setting: Specifies the page that is shown when a new tab is opened.
Possible options:

- "Open a blank page"
- "Open a specific page": The page defined under **New tab page location** is shown.

New tab page location: Specifies the page that is shown when the user opens a new tab. This is effective only if **New tab page setting** is set to "Open a specific page".

Font size: Specifies the font size for web content.
Possible options:

- "Very small"
- "Small"
- "Medium (recommended)"
- "Large"
- "Very large"

Content

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Content**

Block pop-ups and redirects

☑ Pop-up windows and redirects are blocked.

Exceptions...: Add websites on which pop-up windows and redirects are not blocked.

Load images automatically

☑ Images from websites are loaded automatically.

Exceptions...: Add websites on which images are not loaded automatically.

Type of download directory
Possible options:

- "Custom location": The user will be prompted for a location to download a file.
- "userhome": Files will be downloaded to `/userhome/Downloads`.

Location: Defines the path files are downloaded to. Only effective when **Type of download directory** is set to "Custom location".

JavaScript

☑ JavaScript is enabled.

Languages: One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With "de, en, fr, it", the website will be shown in German, if available, otherwise in English and so on.

Integrated translation service of Chromium

☑ When a web page has a language that differs from your system language, Chromium will offer to translate the page.

Autoplay

☑ Embedded audio and video content on a web page is played automatically when the page is loaded.

☐ Audio and video content is not played automatically.

Proxy

In this area, you can change the proxy configuration.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Proxy**

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** menu, select the type of proxy configuration.
   The following proxy configurations are available:
   - "Never use a proxy"
   - "Use fixed proxy servers"
   - "Use a .pac proxy script"
   - "Use system proxy settings"
   - "Auto detect proxy settings"
2. Enter the necessary configuration data for the selected proxy configuration.

"Never use a proxy"

With this proxy configuration, no proxy is used.

"Use fixed proxy servers"

The configuration data must be specified in the following fields.

- **FTP proxy**: URL of the proxy for FTP
- **Port**: Port of the proxy for FTP
- **HTTP proxy**: URL of the proxy for HTTP
- **Port**: Port of the proxy for HTTP
- **SSL proxy**: URL of the proxy for SSL
- **Port**: Port of the proxy for SSL
- **SOCKS host**: URL of the proxy for SOCKS
- **Port**: Port of the proxy for SOCKS
- **SOCKS protocol version**: Version of the SOCKS protocol used (default: SOCKS v5)
- **No proxy for**: List of URLs for which no proxy is to be used (default: `localhost, 127.0.0.1`)

"Use a .pac proxy script"

With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

- **URL**: URL of the proxy configuration file

"Use system proxy settings"

With this proxy configuration, the proxy configured under **Network > Proxy** will be used.

"Auto detect proxy settings"

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.

Privacy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Privacy**

Autofill addresses and more

☑ Entries in forms and search bars will be retained after Chromium restarts.

☐ Entries in forms and search bars will be retained only for the duration of the session.

Autofill payments

☑ Entries in payment forms will be retained after Chromium restarts.

☐ Entries in payment forms will be retained only for the duration of the session.

Autofill passwords

☑ Chromium will offer to save passwords entered and retain them after Chromium restarts.

☐ Passwords entered will be retained only for the duration of the session.

Clear browsing data

☑ Data entered will be deleted when Chromium is closed. What data are deleted is specified in the following options.

☐ Data entered will not be deleted when the browser is closed.

Browsing & download history

☑ Addresses (URLs) of visited websites and the list of downloads will be deleted when Chromium is closed.

Saved passwords

☑ Passwords entered will be deleted when Chromium is closed.

Cookies

☑ Cookies will be deleted when Chromium is closed.

Cache

☑ The cache for temporarily saving web pages will be emptied when Chromium is closed.

Allow incognito mode: When the incognito mode is active, all data from private windows will be deleted after Chromium is closed.

Possible options:

- **Enabled**: The user can open browser windows in incognito mode.
- **Disabled**: The user cannot open browser windows in incognito mode.
- **Forced**: All browser windows started by the user are in incognito mode.

Enable "Do Not Track" feature

☑ Chromium will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded.

The browser will use the `DNT` ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when `DNT` is set to 1.

Block third party cookies

☑ Third-party cookies are not accepted by Chromium. For details, see https://chromeenterprise.google/policies/#BlockThirdPartyCookies. (Default)

With some websites, the functionality might be limited if third-party cookies are blocked. For example, for Microsoft Teams to work, it is required to allow the use of some cookies. For further instructions, see Troubleshooting: Cannot Log in to MS Teams in Chromium Browser (see page 587).

Enable search suggestions

☑ Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history.

Security

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Security**

On this page, you can define settings for safe browsing and for the handling of files.

Safe browsing

☑ Chromium will check all web content, including e.g. images and scripts, against a continuously updated list of known phishing and malware websites. If Chromium finds suspicious content, you will be given a warning.

☐ Chromium will not check web content.

File access

☑ Chromium can access local files on the endpoint device. Downloads and uploads are allowed. Before a file is downloaded, a confirmation dialog is shown.

☐ Local files cannot be accessed by Chromium. Neither downloads nor uploads are allowed. When the user tries to download a file, a message informs the user that downloads are blocked.

Download allowlist: The MIME types listed here are not blocked even when **File access** is deactivated. The storage location is defined under **Sessions > Chromium Browser > Chromium Browser Global > Content**, parameter **Location**. If the file suffix matches with one of the entries in **Open file types automatically after downloading**, the file is opened immediately after download. The list entries are separated by semicolons ";".

Open file types automatically after downloading: Any file whose suffix is listed here will be opened immediately after download. The list entries are separated by semicolons ";".

Encryption Settings for the Chromium Browser in IGEL OS

Here, you can select the minimum and maximum SSL/TLS version for the Chromium Browser that is built into IGEL OS.

Note that it is always better to upgrade to a higher TLS version on the server than to downgrade to a lower version on the client.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Encryption**

Minimum SSL/TLS version

This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- TLS 1.2*
- TLS 1.3

Maximum SSL/TLS version

This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- TLS 1.2
- TLS 1.3*

*IGEL OS system default

Menus & Toolbars for the Chromium Browser Global in IGEL OS

In this area, you can change the browser's menus and toolbars.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Menus & Toolbars**

Hide home button

☑ The home button will not be shown.

☐ The home button will be shown.

Hide bookmarks toolbar

☑ The bookmarks menu will not be shown in the menu bar.

☐ The bookmarks menu will be shown in the menu bar.

Window

In this area, you can define the window settings for a Chromium session.

Menu path: **Sessions > Chromium Browser > Chromium Global > Window**

Enable kiosk mode

☑ Chromium starts in kiosk mode.

☐ Chromium starts in normal mode.

Start maximized

☑ Chromium starts in a maximized window.

☐ Chromium starts in a window with default size.

Chromium translation: Changes the default language when Chromium offers to translate a web page.

Block Chromium settings

☑ The settings menu of Chromium can not be accessed by the user.

☐ The user can access the settings menu.

Custom Setup

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup**

- Chromium Policies for Chromium Browser Global in IGEL OS (see page 1610)
- Custom Command-Line Options (see page 1612)

Chromium Policies for Chromium Browser Global in IGEL OS

Here, you can add, edit, and remove policies for the Chromium sessions on your IGEL OS device. Please note that the custom settings always win over the IGEL Setup, i.e. if a policy is defined both here and in the Setup, but with different values, the value defined here is effective.

For a complete list of available policies, see https://chromeenterprise.google/policies/.

> Please note that the enterprise policy URL pattern format that is defined by Chrome is not fully supported by the IGEL Setup.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Policies**

->Click on + **Add** to create a policy.

Policy name

Name of the policy as described in https://chromeenterprise.google/policies/.

Policy value

Value of the policy. The data format is described in https://chromeenterprise.google/policies/. Please note the following:

- Use the correct data type (see the right column of the relevant policy description, e. g. https://chromeenterprise.google/policies/#URLBlocklist)
- Use the Linux examples
- Make sure to separate the policy name from the policy value; some of the examples in the Chrome documentation include the policy name accidentally, e. g. https://chromeenterprise.google/policies/#PrintingPaperSizeDefault.

URL Blocklist Example

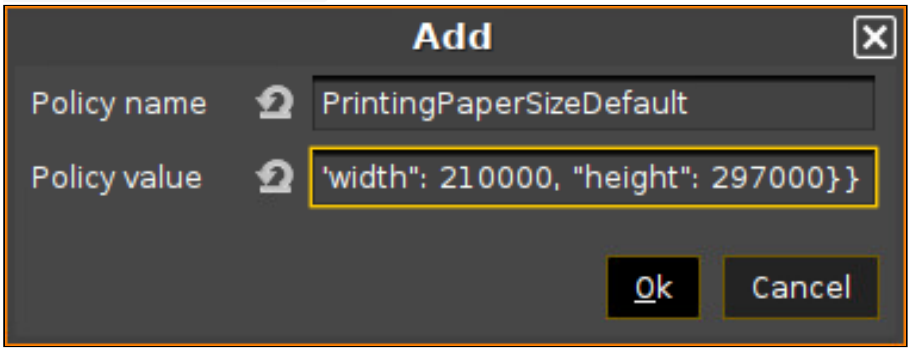
If you want to block the websites `badsite.com` and `malware.com`, define your policy as follows (see also https://chromeenterprise.google/policies/#URLBlocklist):

- **Policy name**: `URLBlocklist`
- **Policy value**: `["badsite.com", "malware.com"]`

Printing Paper Size Example

If you want to define a paper size for printing, define your policy as follows (see https://chromeenterprise.google/policies/#PrintingPaperSizeDefault):

- **Policy name**: `PrintingPaperSizeDefault`
- **Policy value**: `{"name": "custom", "custom_size": {"width": 210000, "height": 297000}}`



Custom Command-Line Options

Here, you can define command-line parameters that are passed to Chromium on startup.

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Custom Command-Line Options**

The syntax is exactly the same as if Chromium would be started from a terminal.

Custom command-line parameters: One or more command-line parameters. Multiple parameters are separated by whitespace.

Example:

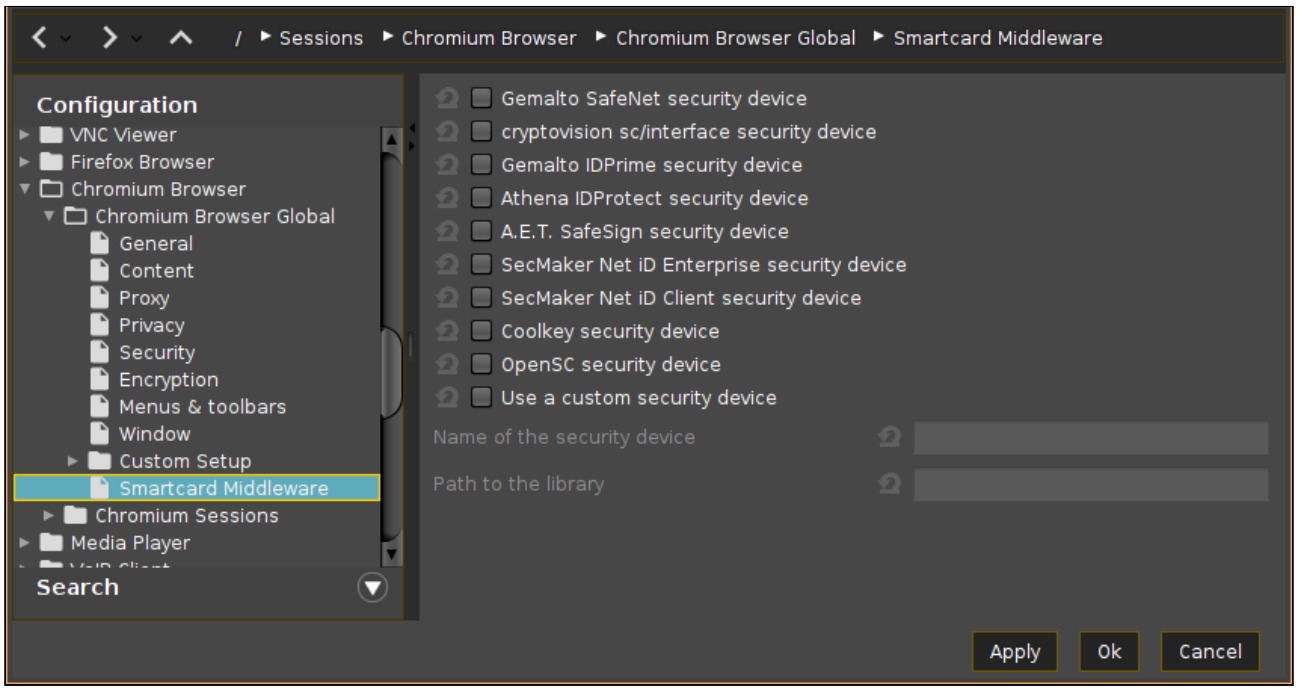
```
--proxy-server="socks://localhost:8080" --incognito
```

Smartcard Middleware for Chromium Browser in IGEL OS

In this area of the IGEL Setup, you can activate or deactivate smartcard middleware (PKCS#11 module) that is to be used for encryption. Alternatively, you can specify here your own PKCS#11 module that you want to use with the Chromium browser.

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS (see page 791).

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**



Gemalto SafeNet security device

☑ Gemalto/SafeNet eToken will be used for encryption.

☐ Gemalto/SafeNet eToken will not be used for encryption.*

cryptovision sc/interface security device

☑ cryptovision sc/interface will be used for encryption.

☐ cryptovision sc/interface will not be used for encryption.*

Gemalto IDPrime security device

☑ Gemalto IDPrime will be used for encryption. Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.

☐ Gemalto IDPrime will not be used for encryption.*

Athena IDProtect security device

☑ Athena IDProtect will be used for encryption.

☐ Athena IDProtect will not be used for encryption.*

A.E.T. SafeSign security device

☑ A.E.T. SafeSign will be used for encryption.

☐ A.E.T. SafeSign will not be used for encryption.*

Pointsharp Net iD Enterprise security device

☑ Pointsharp Net iD Enterprise, formerly known as "Pointsharp Net iD", will be used for encryption.

☐ Pointsharp Net iD Enterprise will not be used for encryption.*

Pointsharp Net iD Client security device

☑ Pointsharp Net iD Client will be used for encryption. For more on Pointsharp Net iD Client, see https://docs.pointsharp.com/net-id-client/latest/index.html

☐ Pointsharp Net iD Client will not be used for encryption.*

Coolkey security device

☑ Coolkey will be used for encryption.

☐ Coolkey will be not used for encryption.*

OpenSC security device

☑ OpenSC will be used for encryption.

☐ OpenSC will not be used for encryption.*

90meter security device

Licensed Feature

This feature requires an add-on license. Please contact your IGEL reseller.

☑ 90meter will be used for encryption.

☐ 90meter will not be used for encryption.*

Use a custom security device

☑ The PKCS#11 module stored under the **Path to the library** is used. See also Using a Custom PKCS#11 Library (see page 922).

☐ The custom security device will not be used for encryption.*

> ⚠ In case of the installation of a custom PKCS#11 library, the file(s) must be placed on the endpoint device either via UMS file transfer or Custom Partition Tutorial (see page 852).
> The use of the `/wfs` folder is NOT recommended because of its space limit.

Name of the security device

Name of the custom security device that uses the library specified under **Path to the library**

Path to the library

Path to the custom PKCS#11 module

---

* IGEL OS system default

Chromium Sessions

In this area, you can configure desktop integration for the Chromium session.

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name]**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- Settings (see page 1619)
- Desktop Integration (see page 1620)

Settings

In this area, you can change the following settings for Chromium Sessions:

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Settings**

On startup: Specifies what pages are shown when Chromium is launched.
Possible options:

- "Global setting"
- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

Startup page: Specifies the URL of the start page. You can specify a number of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **On startup.**

Desktop Integration

In this area, you can configure desktop integration for the Chromium session.

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Media Player Global

Menu path: **Sessions > Media Player > Media Player Global**

Here, you can change the global settings for the device's media player:

- Window (see page 1624)
- Playback (see page 1625)
- Video (see page 1626)
- Options (see page 1627)

Window

Menu path: **Setup > Sessions > Media Player > Media Player Global > Window**

Aspect ratio: Aspect ratio for video playback
Possible values:

- Auto: The aspect ratio of the playback window will adapt to the video being played. (Default)
- Square
- 4:3 (TV)
- 16:9 (widescreen)
- 2.11:1 (DVB)

Fullscreen

☑ The media player will be shown in full-screen mode.

☐ The media player will be shown in a standard window. (Default)

Automatically resize the player window when a new video is loaded

☑ The window size will adapt to the video being played.

☐ The window size will not change. (Default)

Main window should stay on top

☑ The media player window will always remain in the foreground. Other windows cannot be placed on top of the media player window.

☐ The media player window will behave like a standard window. Other windows can be placed on top of the media player window. (Default)

Show controls

☑ The media player operating components will be shown. (Default)

☐ The media player operating components will not be shown; only the playback window is visible.

Playback

Menu path: **Sessions > Media Player > Media Player Global > Playback**

Repeat mode

☑ The playlist will be repeated until the user stops playback.

☐ The playlist will be played back once only. (default)

Shuffle mode

☑ The playlist will be played back in a random order.

☐ The playlist will be played back in the set order. (default)

Show visual effects when an audio file is played

☑ Visual effects will be shown when playing back audio data.

☐ No visual effects will be shown. (default)

Type of visualization: The type of visual effects when playing back audio data
Possible values:

- Monoscope
- Goom!

Visualization size: The size of the visual effects shown

> This parameter is effective only if gstreamer 0.10 is selected as the multimedia framework, which results in Totem being selected as the media player. With the default setting for IGEL OS 10.05 and higher (gstreamer 1.x in combination with Parole) the parameter is not effective.
> The multimedia framework and media player can be changed in the Registry under **System > Registry > multimedia > gstreamer > version** (registry key: `multimedia.gstreamer.version`).

Possible values:

- Small
- Normal
- Large
- Extra large

Video

Menu path: **Setup > Sessions > Media Player > Media Player Global > Video**

- **Video output**: Specifies the video output method.
  Possible options:
  - Auto: The video output method will be set depending on availability. The following options will be queried in this order. Examples: If available, hardware acceleration will be used. If hardware acceleration is not available but the X video extension is, the X video extension will be used.
  - Hardware accelerated: Hardware acceleration will be used.
  - X video extension: The images will be written to the graphics card memory using *shared memory*. Hardware acceleration will be used.
  - X Window System: Video will be output via the X11 protocol. Hardware acceleration will not be used.

Options

Menu path: **Setup > Sessions > Media Player > Media Player Global > Options**

- **Disable screensaver when playing audio**
  ☑ The screensaver will not be started during audio playback. (Default)
  ☐ The screensaver will start after the set idling time, even is audio is being played back.
- **Network connection speed**
  Possible values:
  - 56 kBps modem/ISDN
  - 112 kBps dual ISDN/DSL
  - 256 kBps DSL/cache
  - 384 kBps DSL/cache
  - 512 kBps DSL/cache
  - 1.5 MBps T1/Intranet/LAN (Default)
  - Intranet/LAN
- **Buffer size**: The buffer compensates for fluctuations in the network speed. (Default: 3)
- **Autoload subtitle**
  ☑ Subtitles contained in the video will be shown automatically. (Default)
  ☐ Subtitles contained in the video will only be shown if the user has enabled them via **View > Subtitles**.
- **Subtitle encoding**: Character coding for the subtitles. The value is set to UTF-8. (Default)
- **Font name**: Font that is used for the subtitles
  Possible values:
  - Sans
  - Sans Bold (Default)
  - Serif
  - Serif Bold
- **Font size**: Size of the font that is used for the subtitles (Default: 20)

Media Player Session

In this area, you can configure desktop integration for the media player.

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name]**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Playback (see page 1631)
- Options (see page 1632)
- Desktop Integration (see page 1633)

Playback

In this area, you can specify which audio data or video data are played back with which window settings when the media player session starts.

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Playback**

- **Medium / filename**: Path to the audio data or video data that are to be played back when the media player session starts. This can be a local path or a URL.
- **Use default fullscreen mode configuration**
  ☑ The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (default)
  ☐ The setting will be set on a session-specific basis with **Play video in fullscreen**.
- **Play video in fullscreen**
  ☑ The media player will be shown in fullscreen mode.
  ☐ The media player will be shown in a standard window. (default)
- **Use image aspect ratio setting**
  ☑ The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (Default)
  ☐ The setting will be set on a session-specific basis with **Aspect ratio**.
- **Aspect ratio**: Aspect ratio for video playback
  Possible values:
  - Auto: The aspect ratio of the playback window will adapt to the video being played. (Default)
  - Square
  - 4:3 (TV)
  - 16:9 (widescreen)
  - 2.11:1 (DVB)

Options

Menu path: **Setup > Sessions > Media Player > Media Player Sessions > [Session Name] > Options**

- **Use default controls configuration**
  ☑ The setting under **Setup > Sessions > Media Player > Media Player Global > Window** will be used. (Default)
  ☐ The setting will be set on a session-specific basis with **Show controls**.
- **Show controls**
  ☑ The media player operating components will be shown. (Default)
  ☐ The media player operating components will not be shown; only the playback window is visible.

Desktop Integration

In this area, you can configure desktop integration for the media player.

Menu path: **Sessions > Media Player > Media Player Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

VoIP Client

Menu path: **Sessions > VoIP Client**

Ekiga Voice over IP client allows you to use the SIP (Session Initiation Protocol) and H.323; see http://ekiga.org[185].

You will find a detailed description of all Ekiga options under http://wiki.ekiga.org/index.php/Manual.

In this area, you can configure desktop integration for the VoIP session.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

185. http://ekiga.org/

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- User Account for the VoIP Client (see page 1639)
- Audio Settings for the VoIP client in IGEL OS (see page 1641)
- SIP for the VoIP Client in IGEL OS (see page 1643)
- H.323 for the VoIP Client in IGEL OS in IGEL OS (see page 1644)
- Call Options for VoIP Client in IGEL OS (see page 1645)
- Phone Book for the VoIP Client in IGEL OS (see page 1646)
- Preferences for the VoIP Client in IGEL OS (see page 1647)
- Desktop Integration (see page 1648)

User Account for the VoIP Client

You can set up or change one or more user accounts as well as specify the name displayed.

Menu path: **Setup > Sessions > VoIP Client > User Account**

- **Full Name**: Name of the user; this name will be shown to the other person. Example: John Doe

To set up an SIP user account, proceed as follows:

> Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click ＋.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
   - **Protocol**: Select **SIP**.
   - **Name**: Name for this user account.

     > Choose a name which allows a distinction to be made easily between a number of user accounts.

   - **Registrar**: URI with which the VoIP client registers. This can be a DNS name or an IP address.
   - **User name**: Numerical or alphanumerical value. The user name is part of the SIP address. Example: `john.doe` in `john.doe@example.com`
   - **Login Name**: Numerical or alphanumerical value. Name with which the VoIP client registers on the registrar. This name can differ from the name given under **user name**.
   - **Password**: Password with which the VoIP client registers on the registrar
   - **Registration Update Timeout**: Timeout after which the registration should be updated (Default: 3600)
4. Click **Ok**.
   The user account has been set up.

To set up an H.323 user account, proceed as follows:

> Ensure that the VoIP client was terminated before you start setting up or changing a user account. Changes will only be saved if the client is not running.

1. Click ＋.
2. If the user account is to be active once set up, enable the **Enable Account** option.
3. Enter the following data:
   - **Protokoll**: Wählen Sie **H323**.
   - **Name**: Name für dieses Benutzerkonto.

> Choose a name which allows a distinction to be made easily between a number of user accounts.

- **Gatekeeper**: URI with which the VoIP client registers. This can be a DNS name or an IP address.
- **User name**: Numerical or alphanumerical value. Example: `john.doe` in `john.doe@example.com`
- **Passwort**: Password with which the VoIP client logs on to the registrar
- **Registration Update Timeout**: Timeout after which the registration should be updated (Default: 3600)

4. Click **Ok**.
   The user account has been set up.

Audio Settings for the VoIP client in IGEL OS

You can change the audio settings of the VoIP client.

Menu path: **Setup > Sessions > VoIP Client > Audio**

> Recommendation: Configure the settings **Device for ringtone**, **Device for audio playback** and **Device for audio recording** in the VoIP client. All available audio devices of the thin client are shown in the VoIP client.

To configure the audio devices in the VoIP client, proceed as follows:

1. In the *IGEL* setup, ensure that the option **Save configuration changes made in the application** is enabled under **Sessions > VoIP Client > Preferences**.
2. Start the VoIP client.
3. Configure your desired settings in the VoIP client under **Edit > Preferences > Audio > Devices**.
4. To save your settings, close the VoIP client window, right-click on

   in the system tray and select **Close**.

The changes will be saved in the *IGEL* setup once the VoIP client is terminated.
Settings in the setup:

- **Sound event output device**: Specifies which audio device is used for the ringtone.

  > It is recommended that you select the audio device that is connected to the thin client's built-in loudspeaker.

- **Audio output device**: Specifies which audio device is used for playback. Example: the audio device that is connected to the loudspeakers of the headset.
- **Audio input device**: Specifies which audio device is used for recording. Example: the audio device that is connected to the microphone of the headset.
- **Enable silence detection**: If this option is enabled, audio transmission will be suppressed in the absence of voice activity. This helps to save bandwidth.

  > Voice activity detection can reduce the voice quality.

- **Enable echo cancelation**: If this option is enabled, the VoIP client will suppress echoes of your own voice.
- **Maximum jitter buffer (in milliseconds)**: The jitter buffer improves voice quality by compensating for delay variations when transmitting voice packets. The VoIP client continuously measures delay variations and automatically adjusts the buffer size. The bigger the delay variations are, the bigger the jitter buffer will be set. (Default: 500)

A bigger jitter buffer results in greater latency.

SIP for the VoIP Client in IGEL OS

You can change SIP-specific settings for the proxy, forwarding and the multi-frequency dialing process (DTMF).

Menu path: **Setup > Sessions > VoIP Client > SIP**

- **Outbound Proxy**: URI of the SIP proxy that handles outbound calls.
- **Forward URI**: SIP URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under Call Options (see page 1645).
- **Send DTMF as**: Specifies how key sequences are transmitted while a connection is in place. Possible values:
  - INFO: The key sequence is transmitted as SIP INFO.
  - RFC 2833: The key sequence is transmitted using RTP (Real-time Transport Protocol).

H.323 for the VoIP Client in IGEL OS in IGEL OS

You can change H.323-specific settings for forwarding, H.245, quick start and for the multi-frequency dialing process (DTMF).

Menu path: **Setup > Sessions > VoIP Client > H.323**

Forward URI: H.323 URI to which inbound calls are forwarded if forwarding is enabled. You will find further information on forwarding under Call Options for VoIP Client in IGEL OS (see page 1645).

Enable H.245 tunneling

☑ H.245 messages will be packaged in H.225 messages. In this way, no additional TCP connection must be established. (Default)

> For H.245 tunneling, port 1720 is required.

☐ A separate TCP connection is established for H.245.

Enable early H.245

☑ H.245 will be launched at an earlier point in the connection process. The voice connection can be established more quickly as a result. (Standard)

Enable Fast Start procedure

☑ The voice connection will be established in quick start mode (fast connect, part of H.323 v2). (Standard)

DTMF senden als: Specifies how key sequences are transmitted while a connection is in place.
Mögliche Werte:

String: The key sequence is transmitted using H.245 User Input Indication. (Default)

Tone: The key sequence is transmitted as a tone sequence in the audio data flow.

RFC 2833: The key sequence is transmitted using RTP (Real-time Transport Protocol).

Q.931: The key sequence is transmitted via the signaling channel.

Call Options for VoIP Client in IGEL OS

You can change settings for inbound calls.

Menu path: **Setup > Sessions > VoIP Client > Call Options**

- **Always forward calls to the given address**: If this option is enabled, inbound calls will immediately be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > Foward URI** (see SIP (see page 1643)) or **Setup > Sessions > VoIP Client > H.323> Forward URI** (see H.323[186]).
- **Forward calls to the given address if no answer**: If this option is enabled, inbound calls will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see SIP (see page 1643)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see H.323[187]) after the time specified under **Time limit for calls not taken**. If this option is disabled, inbound calls will be rejected after the time specified under **Time limit for calls not taken**.
- **Forward calls to the given address if busy**: If this option is enabled, inbound calls during a call will be forwarded to the address defined in **Setup > Sessions > VoIP Client > SIP > URI for Forwarding** (see SIP (see page 1643)) or **Setup > Sessions > VoIP Client > H.323> URI for Forwarding** (see H.323[188]).
- **No Answer Timeout**: Time in seconds after which calls not taken are rejected or forwarded.

186. https://kb.igel.com/en/igel-os/11.10.250/h-323-for-the-voip-client-in-igel-os-in-igel-os
187. https://kb.igel.com/en/igel-os/11.10.250/h-323-for-the-voip-client-in-igel-os-in-igel-os
188. https://kb.igel.com/en/igel-os/11.10.250/h-323-for-the-voip-client-in-igel-os-in-igel-os

Phone Book for the VoIP Client in IGEL OS

You can add one or more LDAP address books or local contacts.

Menu path: **Setup > Sessions > VoIP Client > Telephone Book**

To add an LDAP address book, proceed as follows:

1. In the **List of LDAP address books** area, click on +.
2. Enter the following data:
   - **Name**: Name with which the LDAP address book will be displayed in the VoIP client
   - **Server Name**: Host name of the LDAP server
   - **Port**: Port for the connection to the LDAP server (Default: 389)
   - **Base DN**: Basis for the search in the LDAP tree
   - **Scope**: Area for the LDAP search
     Possible options:
     - Single level
     - Subtree (Default)
   - **Display name attribute**: LDAP attribute that is displayed as the name of the contact in the VoIP client. (Default: cn)
   - **Call Attribute**: LDAP attribute that contains the telephone number (Standard: telephoneNumber)
   - **Filter Template**: Filter for the LDAP search (Default: (cn=$))
   - **Bind ID**: Identifier for the LDAP search. This identifier is sent to the LDAP server in a BIND request.
   - **Password**: Password for the user account for the LDAP search
3. Click **Ok**.

To add a contact to the local contact list, proceed as follows:

1. In the **List of Contacts** area, click on +.
2. Enter the following data:
   - **Name**: Name of the SIP or H.323 address displayed
   - **Address**: SIP or H.323 address. Example: `sip:500@example.com`
   - **Group**: Optional group name in order to group contacts
3. Click **Ok**.

Preferences for the VoIP Client in IGEL OS

Menu path: **Setup > Sessions > VoIP Client > Settings**

You can change VoIP client settings.

Save configuration changes made in the application

☑ changes made in the VoIP client will be saved in the *IGEL* setup when the VoIP client is terminated. This applies to all settings available in the *IGEL* setup, with the exception of settings for the LDAP address book. (Default)

Desktop Integration

In this area, you can configure desktop integration for the VoIP client session.

Menu path: **Sessions > VoIP Client > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

PCoIP Sessions with the HP Anyware Client in IGEL OS

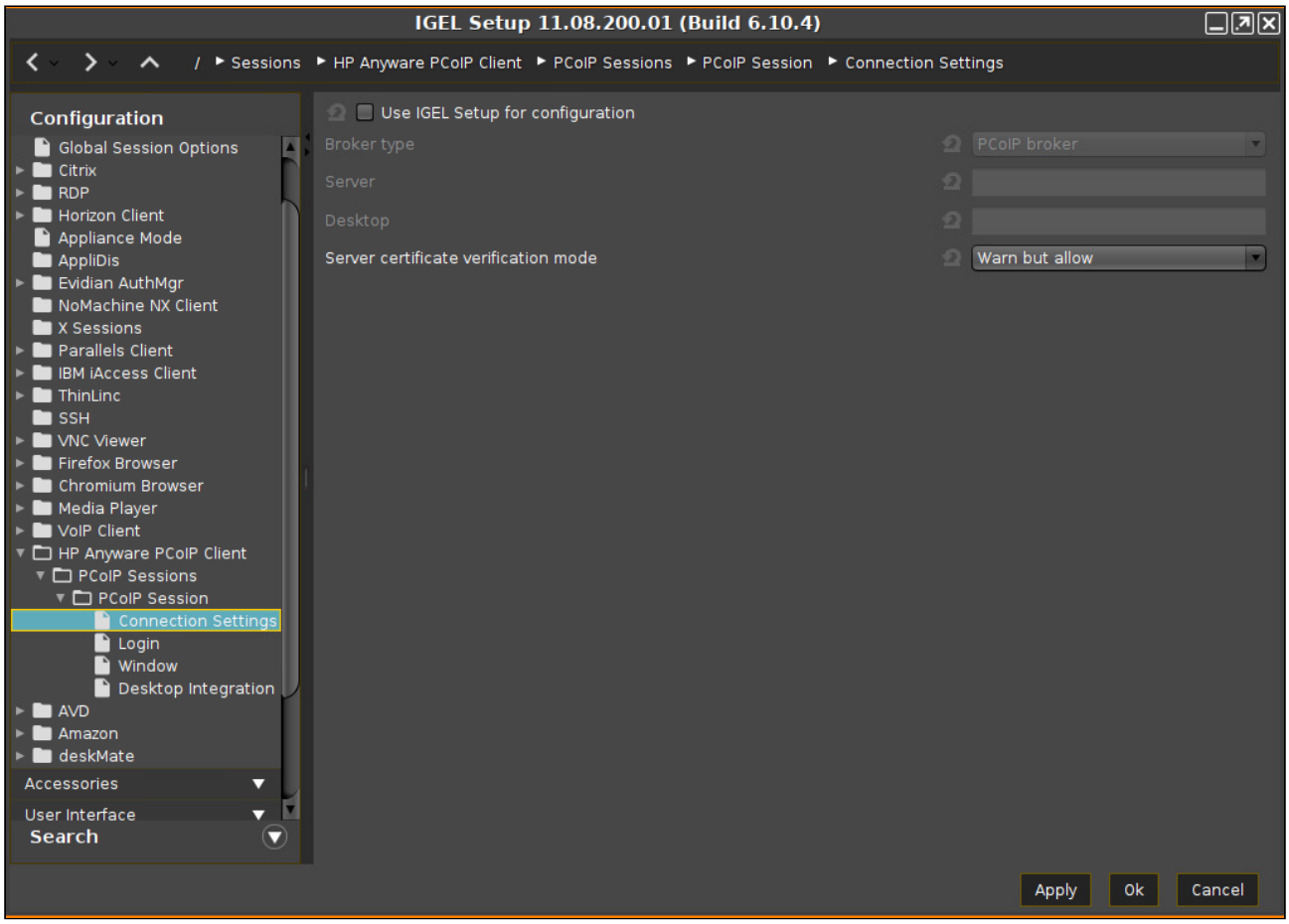
You can configure one or more HP Anyware PCoIP sessions on your IGEL OS device. If you want to use Amazon WorkSpaces via HP Anyware PCoIP, see Using Amazon WorkSpaces via the HP Anyware PCoIP Client (see page 539).

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions**

> If you are using Amazon WorkSpace, note that Linux connectivity is usually disabled by default, see Amazon WorkSpaces Linux Client Application[189]
> You will have to enable this before connecting.

Connection Settings

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Connection Settings**



189. https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-linux-client.html

Use IGEL Setup for configuration

☑ The connection settings are configured via IGEL Setup.

☐ IGEL Setup does not control the connection settings. (Default)

Broker type

Possible options:

- **PCoIP broker** (Default)
- **Direct hardhost**

Server

Host name or IP address of the PCoIP server

Desktop

Name of the virtual desktop. This parameter is only relevant if the user is assigned to more than one virtual desktop on the server, e. g. Amazon Web Services (AWS). If the user has several desktops and the field **Desktop** is empty, a selection of all available desktops is displayed after login. If the field **Desktop** contains the name of an available desktop, the session is started with this desktop.

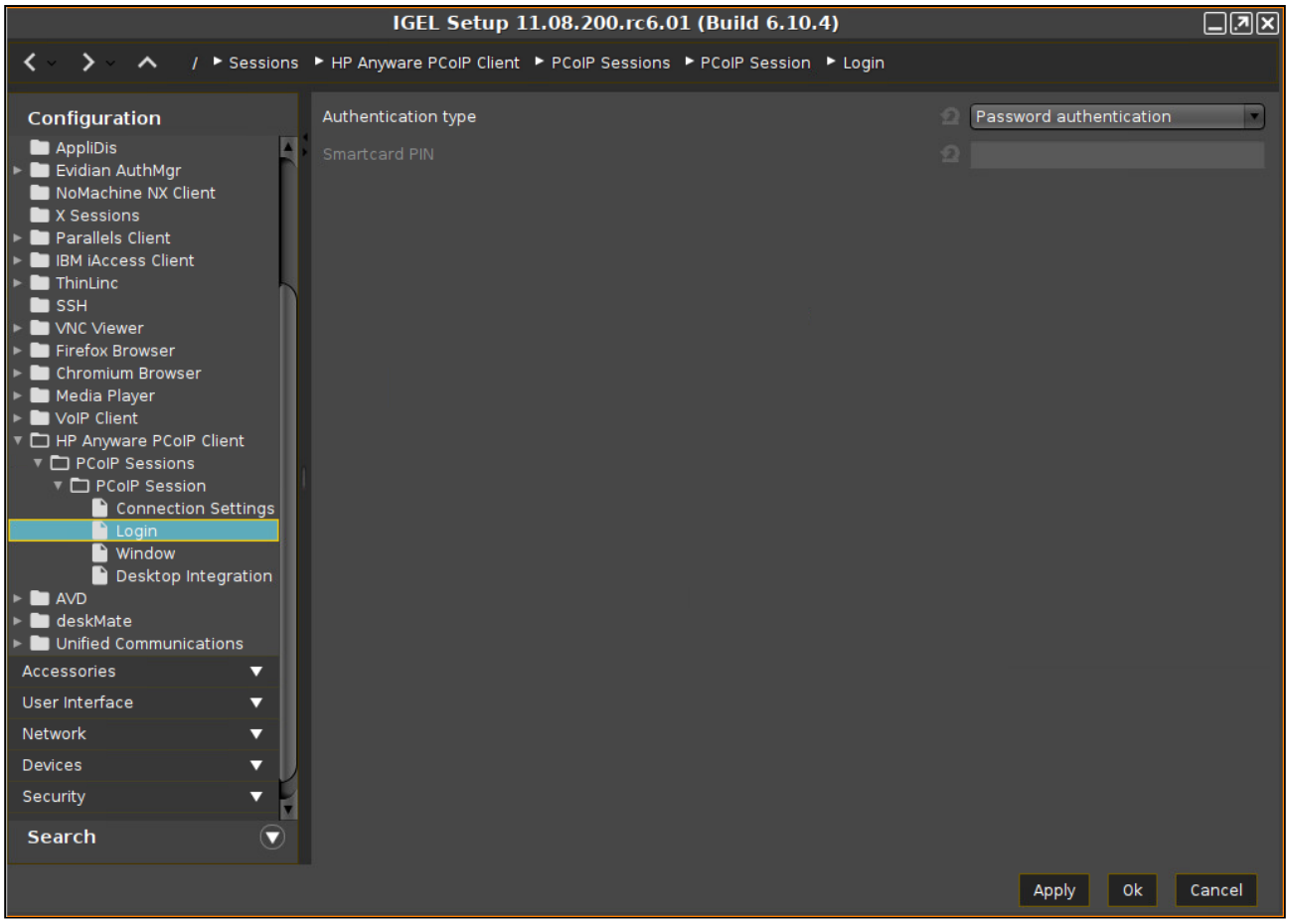
Server certificate verification mode

Possible options:

- **Not required**
- **Warn but allow** (Default)
- **Full verification**: For secure operation, this verification mode is recommended.

Login

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Login**



Authentication type

Possible options:

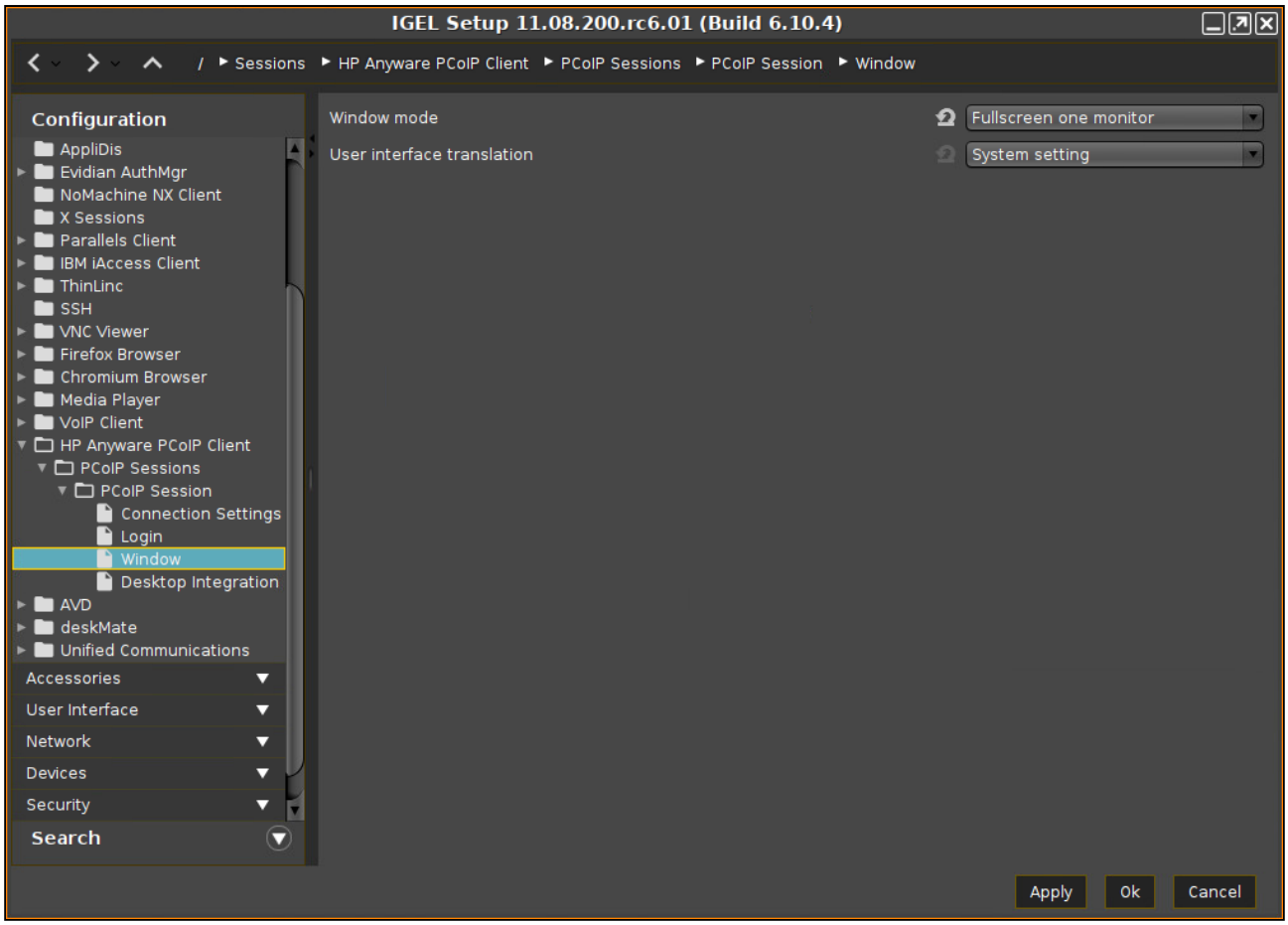
- **Password authentication** (default)
- **Smartcard authentication**

Smartcard PIN

PIN required for smartcard authentication; only valid if **Authentication type** is set to **Smartcard authentication**.

Window

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Window**



Window mode

Possible options:

- **User defined**: The user can change the window mode via the PCoIP client. The window mode that has been used last is stored. (Default)
- **Fullscreen one monitor**
- **Fullscreen all monitors**
- **Window**

User interface translation

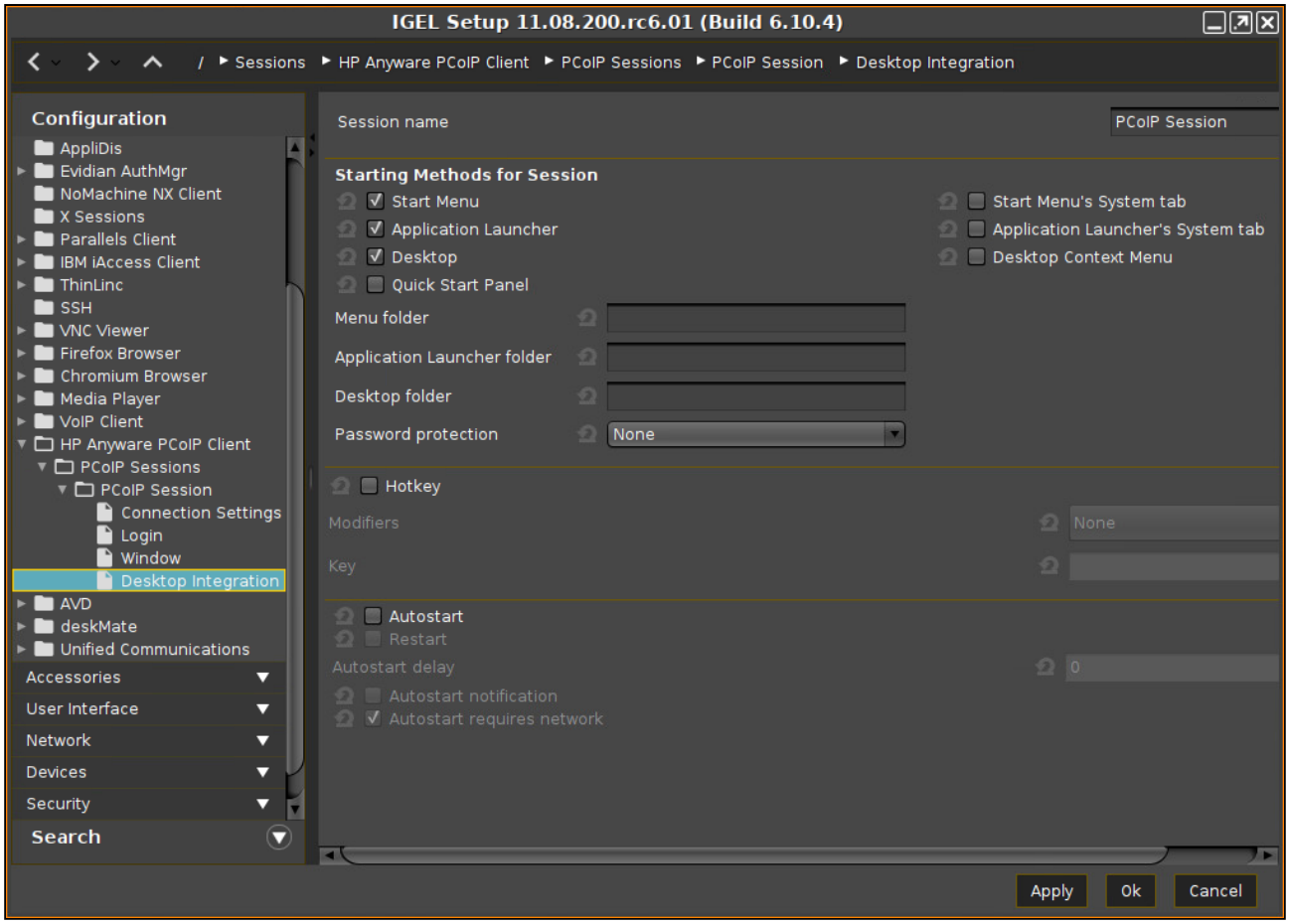
Possible options:

- **System setting** (default)
- **English**
- **German**
- **French**
- **Spanish**
- **Portuguese (EU)**
- **Portuguese (Brazil)**

- **Italian**
- **Japanese**
- **Chinese (Simplified)**
- **Chinese (Traditional)**

Desktop Integration

Menu path: **Sessions > HP Anyware PCoIP Client > PCoIP Sessions > PCoIP Session > Desktop Integration**



Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`

- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

> When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

AVD Global

Menu path: **Sessions > AVD > AVD Global**

- Plugins (see page 1659)

Plugins

Menu path: **Sessions > AVD > AVD Global > Plugins**

- Fabulatech Redirection for AVD in IGEL OS (see page 1660)

Fabulatech Redirection for AVD in IGEL OS

The Fabulatech redirection of webcams and scanners as well as the common Fabulatech USB redirection can be enabled or disabled. The Fabulatech USB redirection can be controlled based on class rules and device rules. The use of rules is described in detail under USB Access Control (see page 2010).

Important Notes

- For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see http://www.usb-over-network.com/partners/igel/. For details on the configuration, see https://www.usb-over-network.com/partners/igel/usb-for-remote-desktop-docs.html. Please note that licenses must be purchased from Fabulatech to enable this functionality.
- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

Menu path: **Sessions > AVD > AVD Global > Plugins > Fabulatech**

You can enable or disable all Fabulatech redirections for each individual session; go to **Sessions > AVD > AVD Sessions > [Session name] > Plugins** and set **Fabulatech Webcam/Scanner/USB Redirection** accordingly. For more information, see Plugins for IGEL OS AVD Sessions (see page 1677).

Fabulatech Webcam Redirection

☑ Fabulatech webcam redirection is enabled.

Fabulatech Scanner Redirection

☑ Fabulatech scanner redirection is enabled.

Fabulatech USB Redirection

☑ Fabulatech USB redirection is enabled.

Default rule

This rule will apply if no special rule was configured for a class or a device.
Possible options:

- **Deny** (Default)
- **Allow**

Tip

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

Managing rules:

Create a new entry

Remove the selected entry

Edit the selected entry

Copy the selected entry

Class rule properties:

Rule:

- Allow: Devices that have the properties defined here are redirected by the Fabulatech USB Redirection.
- Deny: Devices that have the properties defined here are not redirected.

Class ID: Device class

Subclass ID: Subclass relating to the specified device class

Name: Free text entry

Override serial: Serial number that will appear in the session

Override name: Device name that will appear in the session

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts.

☐ The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device).

☐ The USB device may not be removed. (Default)

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated.

☐ The device will be reset after the connection with the session has been terminated.

Device Rules

A device rule applies to a specific device that is identified by its serial number.

Device rule settings:

Rule:

- Allow
- Deny

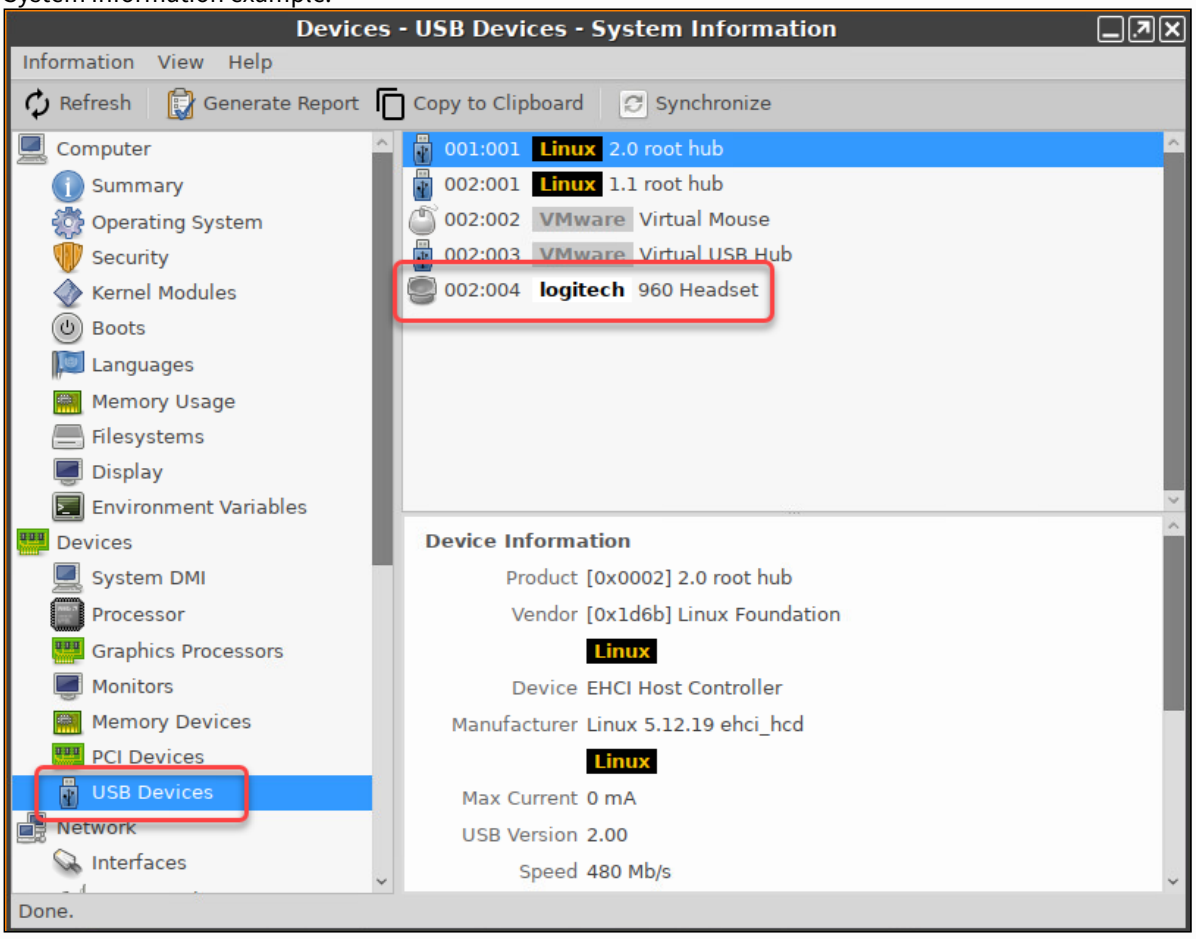
Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

Getting USB Device Information

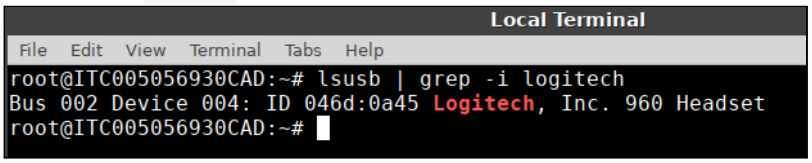
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb` :



Name: Free text entry

Override serial: Serial number that will appear in the session.

Override name: Device name that will appear in the session.

Postpone

☑ The USB device is only removed from the system (endpoint device) when the session starts.

☐ The USB device is no longer shown immediately after the system is booted.

This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

☑ The USB device may be removed from the system (endpoint device).

☐ The USB device may not be removed.

No Reset

☑ The device will not be automatically reset after the connection with the session has been terminated.

☐ The device will be reset after the connection with the session has been terminated.

AVD Session in IGEL OS

In this area, you can configure desktop integration for the AVD session.

Menu path: **Sessions > AVD > AVD Sessions > [Session Name]**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Logon (see page 1667)
- Options (see page 1670)
- Proxy Settings for IGEL OS AVD Sessions (see page 1671)
- Display for IGEL OS AVD Sessions (see page 1673)
- Printing for IGEL OS AVD Sessions (see page 1674)
- Plugins for IGEL OS AVD Sessions (see page 1677)
- Desktop Integration (see page 1678)

Logon

Here, you can configure login options for your Azure Virtual Desktop (AVD) sessions in IGEL OS. For an example configuration, see How to Connect IGEL OS to Azure Virtual Desktop (see page 513).

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Logon**

Username@domain or @domain: A user name or a preset domain name used for the automatic connection to the AVD session. The string after "@" is taken as a preset domain name.

Example:

`avd@your.domain.com` : To log in, the user does not need to enter the username and the domain name.

`@your.domain.com` : To log in, the user only needs to enter the username. The preset domain – `your.domain.com` – will automatically be appended.

> Overwriting the Preset Domain Name
>
> Use the following registry key to specify whether the user should be able to overwrite the preset domain, e.g. with `username@other-domain.com` :

Path	**System > Registry**
Registry	`sessions.wvd%.options.allow-preset-domain-overwrite`
Value	enabled / disabled
Note	If enabled: the domain entered by the user is accepted. If disabled: the domain entered by the user is replaced with the preset domain.

> Remember Username
> By default, the username that has been entered during the last login is remembered. If you want to disable the username cache, use the following registry key:

Path	**System > Registry**
Registry	`sessions.wvd%.options.cache-username`
Value	enabled / disabled
Note	If enabled: the username is cached. If disabled: the username is not cached.

Password: Password used for the automatic connection to the AVD session.

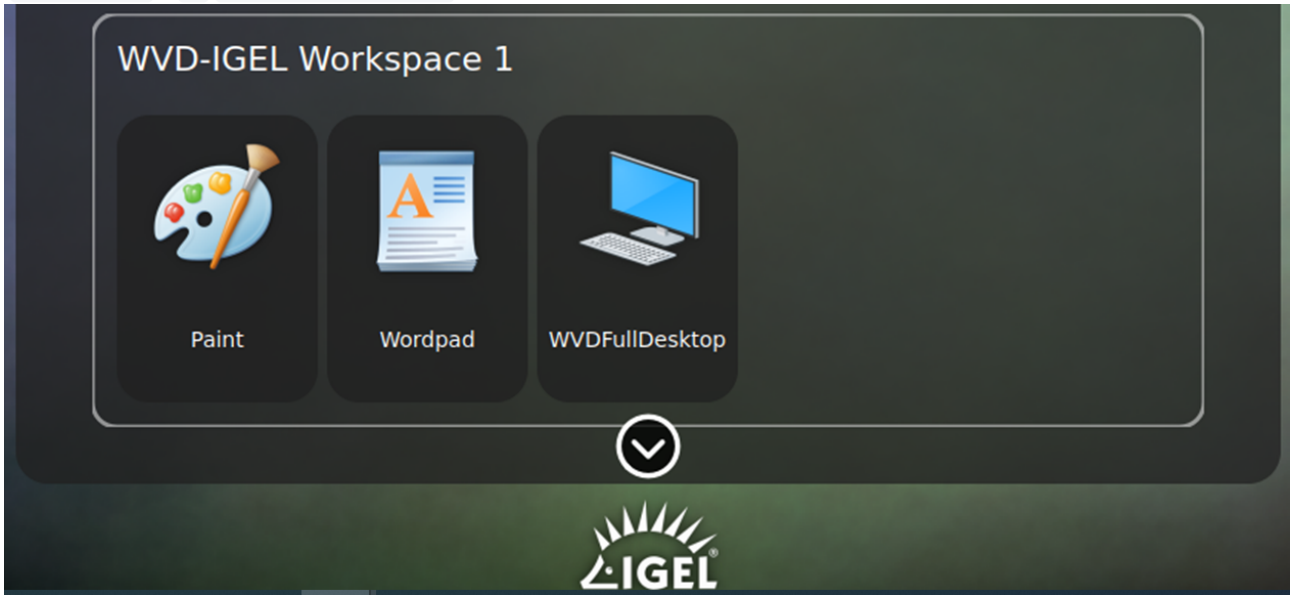
If the Login Credentials Should Not Be Applied Automatically

You can use the following registry key to always prompt for a user name and password or only for a password when connecting to an AVD session:

Path	**System > Registry**
Parameter	**Always prompt for username and password upon session host connection**
Registry	`sessions.wvd%.options.always-prompt-for-session-username-and-password`
Value	enabled / disabled
Path	**System > Registry**
Parameter	**Always prompt for password upon session host connection**
Registry	`sessions.wvd%.options.always-prompt-for-session-password`
Value	enabled / disabled
Note	On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result.

Workspace resource to automatically start when connected: Name of the resource that is to be started automatically. The name specified here must exactly match the name of the AVD resource that has been assigned to the user.

For example, the only valid names for the AVD resources from the screenshot below would be: `Paint` or `Wordpad` or `WVDFullDesktop`



Only one resource can be started automatically; the automatic start of multiple resources is not supported.

Options

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Options**

See also the list of implemented features: Feature Matrix: AVD (RDP3) for IGEL OS 11 (see page 509).

Clipboard redirection

☑ Text and images from the clipboard are shared between the AVD session and the local client.

Drive redirection

☑ Redirection is bound to the `/media` folder, so that locally mounted storage devices, including USB sticks, are forwarded to the AVD session. (Default)

Smartcard redirection

☑ Smartcards are forwarded to the AVD session.

Exit on last session closed

☑ When the last session window is closed, the entire IGEL AVD Client automatically closes. (Default)

In-session toolbar

☑ The in-session toolbar is enabled. (Default)

Audio output redirection

☑ The audio output is redirected between the AVD session and the local client. (Default)

AAC Codec

☑ The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

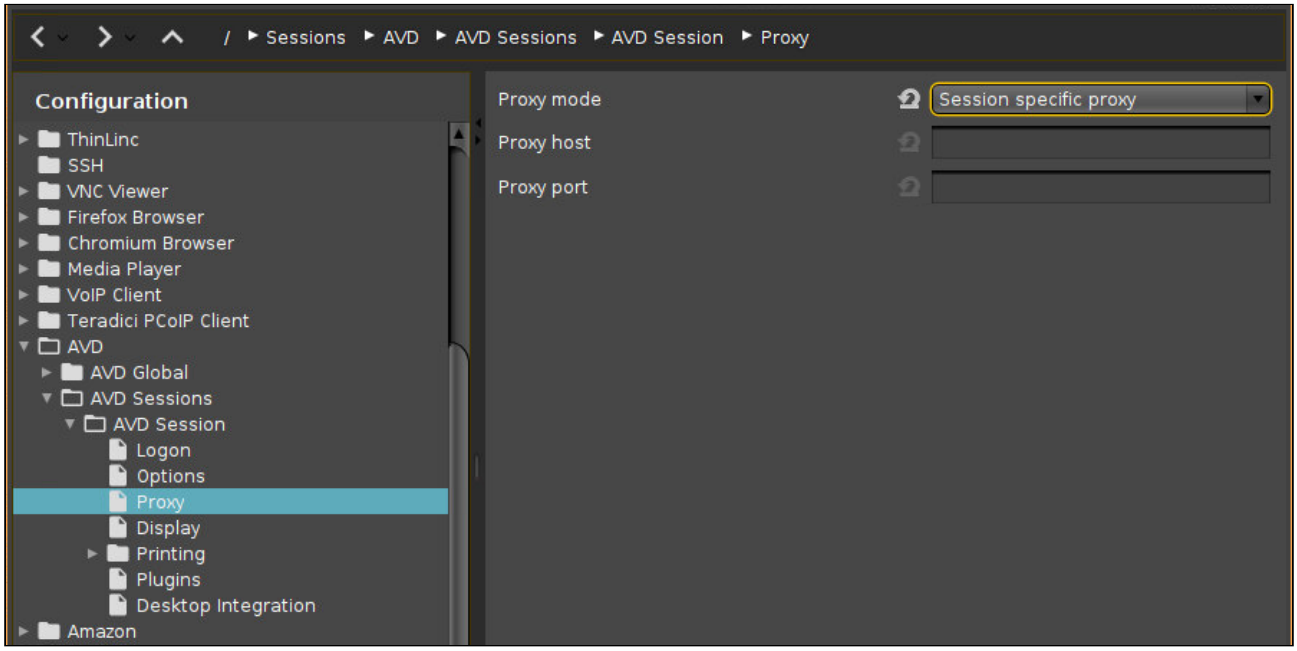
Audio input redirection

☑ The audio input (microphone) is redirected between the local client and the AVD session. (Default)

Proxy Settings for IGEL OS AVD Sessions

In the following area, you can configure proxy settings for your AVD sessions in IGEL OS.

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Proxy**



Proxy Configuration via a PAC File
If you want to use a PAC file, set **Proxy mode** to "Global proxy setting" and specify the **URL** of the PAC file under **Network > Proxy > Automatic proxy configuration**.

Proxy mode

Specifies if a proxy should be used.

Possible options:

- **Off***: A proxy is disabled. The direct connection to the Internet is used.
- **Global proxy setting**: The proxy configured under **Network > Proxy** is used, see Proxy 3 (see page 1928).
- **Session specific proxy**: The proxy configuration specified under **Proxy host** and **Proxy port** is used.

The following fields are active if **Proxy mode** is set to "Session specific proxy":

Proxy host

Hostname or IP address of the proxy server

Proxy port

Port on which the proxy service is available

*IGEL OS system default

Display for IGEL OS AVD Sessions

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Display**

Window size: Specifies the width and height of the window.
Possible options:

- "Full-screen": The session is shown on the full screen. The device's taskbar is not visible. (Default)
- "Work area": The session is shown on the full screen, minus the area needed by the device's taskbar.
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Start monitor: Specifies the monitor on which the session is displayed.
Possible options:

- "No configuration": The monitor is selected according to the current position of the mouse pointer. (Default)
- "1st monitor"
- "2nd monitor"

Multimonitor full-screen mode: This setting is relevant if more than one monitor is connected to the terminal.
Possible options:

- "Global setting": Currently the same as "Multiple monitors".
- "Single monitor": Restricts the full-screen session to one monitor.
- "Multiple monitors": Displays the full-screen session on multiple monitors. (Default)
- "Expand to all monitors": Expands the full-screen session across all monitors.

Scale factor: Specifies the desktop scaling in percent.
Possible values:

- "Automatic scale": The resolution set under **User Interface > Display > Options > Monitor-DPI** is used for the session. (Default)
- Numeric details: The display is magnified by the factor given here.

Printing for IGEL OS AVD Sessions

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing**

- CUPS Printer Redirection (see page 1675)
- ezeep by ThinPrint in IGEL OS (see page 1676)

CUPS Printer Redirection

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > CUPS Printer Redirection**

CUPS Printer Redirection

☑ CUPS printers configured under **Devices > Printer > CUPS > Printers** are redirected to the AVD session from the local endpoint. To disable/enable a CUPS printer for the AVD session, go to **Devices > Printer > CUPS > Printers > [printer name] > Mapping in sessions > Map printer in AVD sessions**, see Printers - Configure CUPS Printers in IGEL OS (see page 1976).

→ Set the printer driver name under **System > Registry > print.cups.printer%.wvd_printer_driver**:

- The default Windows driver name is "Microsoft PS Class Driver"; it is usually installed by default and works generically.
- In the case of a custom printer driver, make sure the driver is installed on the AVD side and enter the exact name of the driver.

ezeep by ThinPrint in IGEL OS

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Printing > ezeep by ThinPrint**

Printing with ezeep

☑ ezeep cloud printing is enabled for the AVD session. To add and enable/disable ezeep printers, go to **Devices > Printer > CUPS > Printer**, see Printers - Configure CUPS Printers in IGEL OS (see page 1976).

Required Custom Commands

You have to add some custom commands and disable workspace-1 option for the AVD session, or ezeep won't work.

Custom Command

(required for Versions 11.06.100 - 11.06.119)

1. Go to **System > Firmware Customization > Base > Initialization.**
2. Add the following custom command:

```
sed -i "s/wvd/avd/g" /usr/share/polkit-1/actions/com.igel.avd_ezeep_* /services/avd/bin/avd_ezeep_*
systemctl try-restart polkit.service
```

3. Restart your IGEL OS.

Disable Workspace-1 option

(required in all 11.06.xxx Versions)

1. Go to **System > Registry > Sessions > WVD0 > Options > Workspace-1 > enabled.**
2. remove the checkbox

Plugins for IGEL OS AVD Sessions

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Plugins**

Fabulatech Webcam/Scanner/USB Redirection

☑ The Fabulatech plugin is active for this session. Please note that the individual redirections enabled by the plugin, i.e. webcam redirection, scanner redirection, and USB redirection are configured system-wide under **Sessions > AVD > AVD Global > Plugins > Fabulatech**; see Fabulatech Redirection for AVD in IGEL OS (see page 1660).

☐ The Fabulatech plugin is not active for this session.

Zoom VDI Media Plugin

☑ The audio and video streams for Zoom are redirected between the endpoint devices resp. between the endpoint devices and the Zoom server. Audio and video data is not processed by the AVD server.

☐ The audio and video streams for Zoom are not redirected.

Desktop Integration

In this area, you can configure desktop integration for the AVD session.

Menu path: **Sessions > AVD > AVD Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Amazon WorkSpaces

Amazon WorkSpaces is a cloud-native desktop virtualization, which is built on the AWS Cloud and used to provide Windows or Linux desktops. For more information, see https://aws.amazon.com/workspaces/ .

With the integrated Amazon WorkSpaces Client, you can easily configure Amazon WorkSpaces sessions on IGEL OS.

In this area, you can configure desktop integration for the Amazon WorkSpaces session.

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name]**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Connection Settings (see page 1684)
- Local Settings (see page 1685)
- Network Settings for Amazon WorkSpaces in IGEL OS (see page 1686)
- Window (see page 1687)
- Desktop Integration (see page 1688)

Connection Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Connection Settings**

Registration code: The WorkSpaces registration code which you got from Amazon

WorkSpace name: Name of the WorkSpace, e.g. `AWS_TechDOC_RD`

Keep me logged in

☑ Login credentials will be saved.

Local Settings

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Local Settings**

Log level
Possible options:

- "Normal logging": Standard logging, which includes info-level details such as runtime events, authorization requests, etc. and is used for informative purposes.
- "Advanced logging": Detailed logging, which includes debug-level details and is used for diagnostic or troubleshooting purposes.
- "Verbose logging": The most detailed logging, which includes trace-level details and is used for very extended diagnostics.

Logs can be found under `/var/tmp/awsc#/Amazon Web Services/Amazon WorkSpaces/logs`.

Network Settings for Amazon WorkSpaces in IGEL OS

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Network Settings**

Use proxy

☑ A proxy will be used.

Proxy address: Hostname or IP address of the proxy server

Proxy port: Port on which the proxy service is available

Window

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Window**

Window size
Possible options:

- "Window mode": The session is shown in a standard window.
- "Full-screen mode": The entire display area is used for the session.

High DPI streaming mode

☑ The support for high pixel density (high DPI) displays is activated, and the screen resolution of the WorkSpace matches the high DPI resolution of the monitor. Note that this setting may affect the performance. For more information on high DPI mode, see WorkSpaces high DPI display support[190].

190. https://docs.aws.amazon.com/workspaces/latest/userguide/high_dpi_support.html

Desktop Integration

Menu path: **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces > [Session Name] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

deskMate Session

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name]**

In this area, you can configure desktop integration for the deskMate session.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

- Provider (see page 1694)
- Options (see page 1695)
- Network (see page 1696)
- Desktop Integration (see page 1697)

Provider

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Provider**

Provider URL: URL to the deskMate portal, issued by your deskMate provider. Example: `https://example.tocario.com`

Login email address: Email address used for logging in to the deskMate session.

Options

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Options**

Full-screen

☑ The entire display area will be used for the deskMate session.

Clipboard redirection

☑ Clipboard data can be shared between a session and the local computer. (Default)

Display scaling

☑ Local display of the deskMate session can be resized.

Adaptive resolution

☑ The remote desktop resolution will automatically be adjusted in accordance with the local resolution. (Default)

Enable logging

☑ Debug logs will be created.

Logfile destination: Path to the debug logs generated if **Enable logging** is activated. (Default: `/userhome/deskmate.log`)

Network

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Network**

Use a proxy server

☑ An HTTP proxy will be used.

Proxy host address: Hostname or IP address of the proxy server

Proxy host port: Port on which the proxy service is available

Desktop Integration

Menu path: **Sessions > deskMate > deskMate Sessions > [Session Name] > Desktop Integration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Unified Communications

Menu path: **Sessions > Unified Communications**

- Zoom Client Selection in IGEL OS (see page 1701)
- Cisco Webex Meetings VDI Selection in IGEL OS (see page 1702)

Zoom Client Selection in IGEL OS

If you use Zoom optimization, you have to select the required version of the Zoom VDI Media Plugin.

> The **Zoom VDI Media Plugin** version must be equal to or less than the version of the server-side Zoom VDI application; a plugin with a higher version is not supported. Zoom recommends updating the Zoom plugin after updating the Zoom VDI application since new features can require an updated plugin. For more information, see the Zoom article VDI backwards compatibility[191].

In addition, you can enable or disable the Smart Virtual Background feature of Zoom.

> The Smart Virtual Background feature has a high consumption of CPU power. On weakly equipped endpoint devices, performance issues can occur.

Menu path: **Sessions > Unified Communications > Zoom Client Configuration**

Zoom client version

Selects the Zoom client version to be used for the Zoom VDI Media Plugin. For the included Zoom client versions, see the "Component Versions" section in the IGEL OS release notes (see page 2282).

The Zoom client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions** (see page 1281), parameter **Zoom VDI Media Plugin**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions** (see page 1393), parameter **Zoom VDI Media Plugin**
- **Sessions > AVD > AVD Sessions > [session name] >** Plugins for IGEL OS AVD Sessions (see page 1677), parameter **Zoom VDI Media Plugin**

> When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

Smart Virtual Background Support

Controls whether the Smart Virtual Background feature can be activated by the user.

Possible Options:

- **Off**: Smart Virtual Background cannot be activated.
- **Auto** (default): The system checks whether the hardware supports Smart Virtual Background feature. If this is the case, the feature can be activated.
- **Always**: Smart Virtual Background can be activated irrespective of the hardware.

191. https://support.zoom.us/hc/en-us/articles/360041602711-VDI-backwards-compatibility

Cisco Webex Meetings VDI Selection in IGEL OS

When configuring Cisco Webex Meetings, you can select the required version of the Cisco Webex Meetings VDI plugin.

The Cisco Webex Meetings VDI plugin and your server-side application should have the same version. For details on backward compatibility, see Webex Meetings VDI Release Notes[192].

Menu path: **Sessions > Unified Communications > Cisco Webex Meetings VDI Selection**

Cisco Webex Meetings client version

Selects the version to be used for the Cisco Webex Meetings VDI client. For the included client versions, see the "Component Versions" section in the IGEL OS release notes (see page 2282).

The Cisco Webex Meetings VDI client for the relevant sessions can be activated as follows:

- **Sessions > Citrix > Citrix Global > Unified Communications > Cisco** (see page 1281), parameter **Cisco Webex Meetings VDI**
- **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco** (see page 1393), parameter **Cisco Webex Meetings VDI**

When using UMS profiles for configuration, make sure the firmware version the profile is **based on** matches the firmware actually installed on the device (see *Universal Management Suite > UMS Reference Manual > Profiles in the IGEL UMS*). If they do not match and the client version selected via the profile is not included in the firmware, the client version will fall back to default.

192. https://help.webex.com/en-us/article/glj57y/Release-Notes-for-Cisco-Webex-Meetings-Virtual-Desktop-Software-Release-42.x#Cisco_Reference.dita_fcb4e1d7-dbef-4bab-8842-9b1a8f84a9e5

Accessories

- ICA Connection Center (see page 1704)
- Local Terminals (see page 1708)
- Change Smartcard Password (see page 1712)
- Change Password (see page 1715)
- Setup (see page 1719)
- Quick Settings (see page 1726)
- Display Switch (see page 1730)
- Application Launcher (see page 1740)
- Sound Preferences (see page 1744)
- System Log Viewer (see page 1750)
- UMS Registration (see page 1755)
- Touchscreen Calibration (see page 1758)
- Task Manager (see page 1762)
- Screenshot Tool (see page 1769)
- On-Screen Keyboard (see page 1773)
- Monitor Calibration (see page 1777)
- Commands (see page 1780)
- Network Tools (see page 1783)
- Bluetooth Tool (see page 1788)
- System Information (see page 1794)
- Disk Utility (see page 1799)
- Disk Removal (see page 1803)
- Mobile Device Access (see page 1806)
- Firmware Update (see page 1809)
- Smartcard Personalization (see page 1813)
- Identify Monitors (see page 1817)
- Webcam Information (see page 1821)
- ICG Agent Setup (see page 1825)
- Licensing (see page 1829)
- Login Enterprise (see page 1832)
- Connector ID Key Software (see page 1833)
- OS 11 Upgrade (see page 1834)
- Conky System Monitor (see page 1837)

ICA Connection Center

With the *Citrix ICA Connection Center*, you are given an overview of the existing connections to *Citrix* servers as well as information regarding connection properties. You can also terminate server connections and log off from *Citrix* servers. For details of how to use the **ICA Connection Center**, see Using ICA Connection Center (see page 1707).

The settings for starting the function are described below.

Menu path: **Accessories > ICA Connection Center**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using ICA Connection Center (see page 1707)

Using ICA Connection Center

To obtain an overview of the existing connections to Citrix servers, proceed as follows:

->Start the ICA Connection Center. The start options are described under ICA Connection Center (see page 1704).
All applications are shown in a tree structure with the associated *Citrix* servers.

> With the help of the tree structure, you can see which applications run on which servers. If a number of applications run on the same server, this will make the exchanging of data between these applications easier.

To view the properties of a connection to a *Citrix* server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under ICA Connection Center (see page 1704).
2. Click on the server whose connection properties you want to view.
3. Click on the **Properties** button.
   The connection properties as well as constantly updated information regarding the number of incoming and outgoing bytes and frames will be shown.
4. If you would like to reset the counter for incoming and outgoing bytes to 0, click on **Reset**.

To terminate a server connection, proceed as follows:

1. Start the ICA Connection Center. The start options are described under ICA Connection Center (see page 1704).
2. Click on the server whose connection you want to terminate.
3. Click on **Terminate**.
   The connection to the server is terminated. The *Citrix* session will be interrupted. The applications will not be terminated on the server. As a result, the application status will be retained until the session is resumed.

To log off from the Citrix server, proceed as follows:

1. Start the ICA Connection Center. The start options are described under ICA Connection Center (see page 1704).
2. Click on the server from which you want to log off.
3. Click on **Log off**.
   The connection to the server is terminated. The *Citrix* session will end. The applications on the server will be terminated.

Local Terminals

Menu path: **Accessories > Terminals > Local Terminal**

With the local terminal, you can execute local commands on your device. For details of how to use the local terminal, see Using Local Terminal (see page 1711).

> It is also possible to access a local shell without a terminal session: Alternatively, you can switch to the virtual terminals `tty11` and `tty12` by pressing [Ctrl]+[Alt]+[F11]or [Ctrl]+[Alt]+[F12]. Pressing [Ctrl]+[Alt]+[F1] takes you back to the user interface.

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Local Terminal (see page 1711)

Using Local Terminal

To use the local terminal, proceed as follows:

1. Start the local terminal. The start options are described under Local Terminals (see page 1708).
2. Log in as `user` or `root`.

   If under **Setup > Security > Password**, in the **Administrator** area, the option **Use password** is enabled, you will need to enter the administrator password to access a local terminal as `root`.
   If an administrator password is set, accessing a local terminal as `user` is only possible if the following two conditions are met:
   - Access to local terminals has been activated for `user`. This is possible with the registry key `system.security.usershell`. The default setting of the registry key forbids terminal access for `user`.
   - Under **Setup > Security > Password**, in the **User** area, the option **Use password** is enabled.

   For accessing a local terminal as `user`, the user password will have to be entered.

   You can enter the shell commands supported by IGEL OS.

Change Smartcard Password

Menu path: **Accessories > Change Smartcard Password**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see Using "Change smartcard password" Function (see page 1714).

Further information regarding the IGEL smartcard can be found under Authentication with IGEL Smartcard (see page 782).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- Using Change Smartcard Password Function (see page 1714)

Using Change Smartcard Password Function

With this function, you can change the password for your IGEL smartcard. In order to do this, the **Logon with IGEL smartcard** option must be enabled under **Security > Logon > IGEL Smartcard**.

To change the password for your IGEL smartcard, proceed as follows:

1. Start the **Change Smartcard Password** function. The start options are described under Change Smartcard Password (see page 1712).
2. Enter the following data in the dialog:
   - **Old smartcard password**: Previous password
   - **New smartcard password**: Chosen password
   - **Reenter new smartcard password**: Chosen password (entered again)

   The password for your IGEL smartcard will be changed.

Change Password

Menu path: **Accessories > Change Password**

With this function, the user can change the password or PIN for the login method he used for his current session, provided one of the following login methods was used:

- Active Directory with username and password
- Active Directory with third-party smartcard
- IGEL smartcard
- Local user password

The **Change Password** function starts when the user clicks the password change button in the dialog informing him that a change of password is required. This dialog is presented after login.

For details of how to use the **Change Password** function, see Using "Change password" function (see page 1718).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- Using Change Password Function (see page 1718)

Using Change Password Function

To change your password for your current login method (Active Directory with user and password, Active Directory with third-party smartcard, IGEL smartcard, or local user with screenlock password), proceed as follows

1. Start the **Change password** function. The start options are described under Change password (see page 1715).
2. Enter the changed password or PIN in the dialog. The dialog differs according to the login method that is currently used.
3. Click **OK**.
   The password is changed.

Setup

Menu path: **Accessories > Setup**

With the IGEL Setup, you can configure your endpoint device. For details of how to allow the user access to the individual areas of the Setup, see Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721). For details of how to change the setup options, see Options (see page 1725).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721)
- Setup Administrator Permissions - Define Access to IGEL Setup Areas (see page 1723)
- Options (see page 1725)

Setup User Permissions - Define Access to IGEL Setup Areas

In the IGEL OS, you can define passwords for different authorization levels (e.g. administrator, setup administrator, setup user, etc.) to protect the system against unauthorized changes, see Password - Restrict Access to IGEL OS Components (see page 2017). If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e. after entering the administrator password. However, it can sometimes be necessary to provide access to individual areas of the IGEL Setup for the user. This is usually required to allow the user to change settings like the system language, right/left-handed mouse, keyboard layout, timezone, etc. if they are not preconfigured via a profile.

The following article explains how to specify which options in the IGEL Setup should be visible and/or configurable for the setup user. For details on configuring permissions for the setup administrator, see Setup Administrator Permissions - Define Access to IGEL Setup Areas (see page 1723).

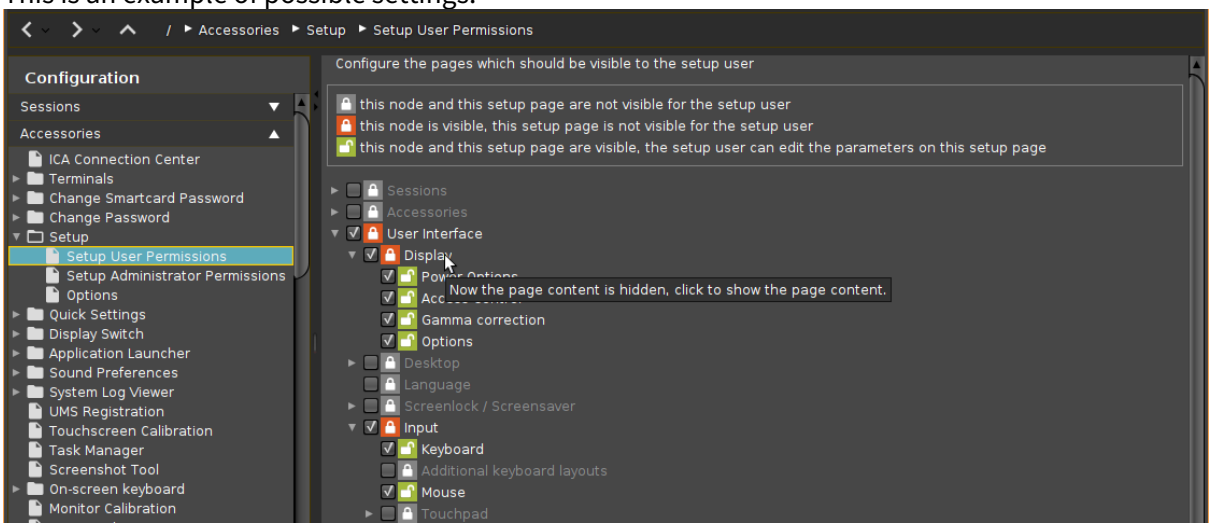
Menu path: **Accessories > Setup > Setup User Permissions**

To enable setup pages for the user, proceed as follows:

1. In the Setup, go to **Accessories > Setup > Setup User Permissions** and enable those areas to which the user is to have access.
   Possible settings:

	Node	Setup Page
	not visible	not visible
	visible	not visible
	visible	configurable

   This is an example of possible settings:



> If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

Example: If you activate all sub-nodes under **Display** (see the screenshot above), the higher-level **Display** node will still be marked as , and, therefore, settings on the **Display** page itself will be invisible for the setup user. This means you have to actively mark the higher-level node as if editing has to be enabled.

2. If not already done: Under **Security > Password** (see page 2017), enable the password for the **administrator** and the **setup user**.

   If users are to be allowed to edit parts of the Setup even without a password, create a quick setup (see page 1241) session, the password for the **setup user** will not be enabled in this case.

Setup Administrator Permissions - Define Access to IGEL Setup Areas

In the IGEL OS, you can define passwords for different authorization levels (e.g. administrator, setup administrator, setup user, etc.) to protect the system against unauthorized changes, see Password - Restrict Access to IGEL OS Components (see page 2017). If a password was set up for the administrator, the IGEL Setup can only be opened with administrator rights, i.e. after entering the administrator password. However, it can be necessary to provide access to individual areas of the IGEL Setup for administrators performing minor administrative tasks, so that they can change local settings if they are not configured by a profile. This may be required, for example, to allow modifying printer settings or custom commands, adding a new local session like a Chromium browser, etc.

The following article explains how to specify which options in the IGEL Setup should be visible and/or configurable for the setup administrator. For details on configuring permissions for the setup user, see Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721).

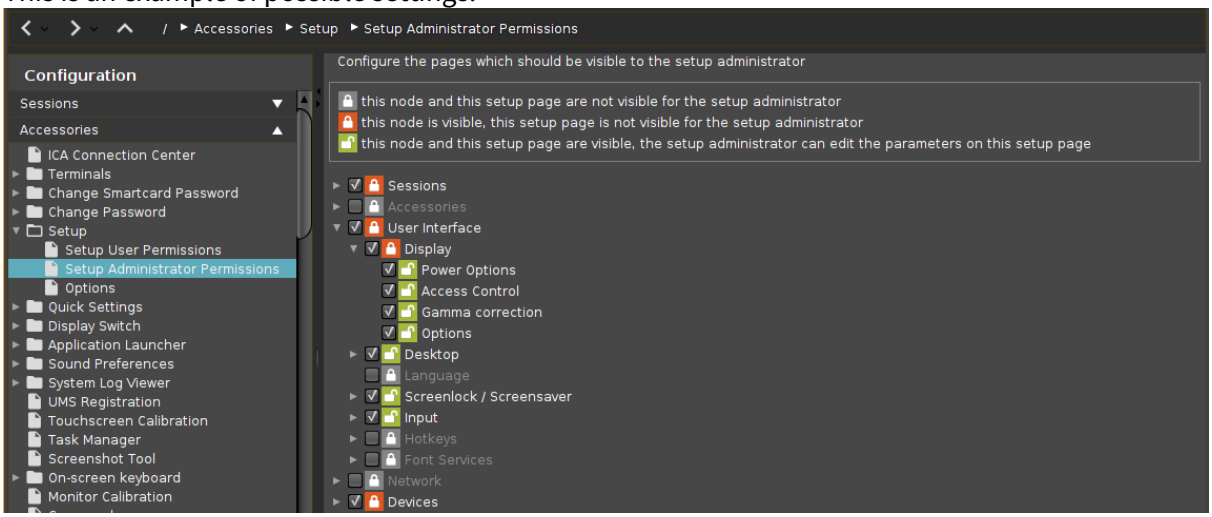
Menu path: **Accessories > Setup > Setup Administrator Permissions**

To enable setup pages for the setup administrator, proceed as follows:

1. In the Setup, go to **Accessories > Setup > Setup Administrator Permissions** and enable those areas to which the setup administrator is to have access.
   Possible settings:

	Node	Setup Page
	not visible	not visible
	visible	not visible
	visible	configurable

   This is an example of possible settings:



   If you enable a setup page on the lower levels, the node points required for access will automatically be marked as visible (but blocked for editing purposes).

Example: If you activate all sub-nodes under **Display** (see the screenshot above), the higher-level **Display** node will still be marked as , and, therefore, settings on the **Display** page itself will be invisible for the setup administrator. This means you have to actively mark the higher-level node as if editing has to be enabled.

2. If not already done: Under **Security > Password** (see page 2017), enable the password for the **administrator** and the **setup administrator**.

   If administrators are to be allowed to edit parts of the setup even without a password, create a quick setup (see page 1241) session, the password for the **setup administrator** will not be enabled in this case.

Options

You can configure the display of tooltips in the setup.

Menu path: **Accessories > Setup > Options**

Enable Tooltips

☑ When the mouse pointer is placed over a parameter, the associated tooltip will be shown after the set **delay**.

☐ No tooltip will be shown.

Tooltip Delay: Time interval in tenths of a second during which the mouse pointer must be placed over a parameter for the tooltip to be shown.

Quick Settings

With the IGEL Setup, you can allow the user access to individual areas of the Setup. Instructions can be found under Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721).

The settings for starting the function are described below.

Menu path: **Accessories > Quick Settings**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)

- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Setup User Permissions (see page 1729)

Setup User Permissions

Menu path: **Accessories > Quick Settings > Setup User Permissions**

Define which setup pages are visible to users.

You will find instructions for this function under Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721).

Display Switch

With this function, you can configure the display on several screens. For details of how to set the function, see Display Switch Options in IGEL OS[193]. For details of how to use the function, see Using "Display Switch" Function (see page 1737).

The settings for starting the function are described below.

Menu path: **Accessories > Display Switch**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

193. https://kb.igel.com/en/igel-os/11.10.250/options

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Options (see page 1733)
- Minimal Dialog (see page 1735)
- Advanced Dialog (see page 1736)
- Using Display Switch (see page 1737)

Options

You can change the way the **Display Switch** function behaves.

Menu path: **Accessories > Display Switch > Options**

Dialog type
Possible values:

- Minimal dialog: The **Display Switch** function starts with the simple dialog.
- Advanced dialog: The **Display Switch** function starts with the advanced dialog.

Smart display configuration

☑ Every configuration of your monitors will be saved.

☐ Monitor configurations will not be saved.

Preserve settings over reboot

☑ The settings for the **Display Switch** function will be preserved over a reboot.

☐ The settings for the **Display Switch** function will be reset to the default settings in the event of a reboot. (Default)

Configure new displays when connected

☑ The **Display Switch** function starts as soon as new screens are connected. You can then configure the new screens.

☐ The **Display Switch** function does not start automatically when new screens are connected. (Default)

Options in Minimal Dialog

Mirror displays

☑ The **Mirror screens** option is shown in the minimal dialog. (Default)

☐ The option is not shown in the minimal dialog.

Extend to the left

☑ The **Extend to the left** option is shown in the minimal dialog. (Default)

☐ The option is not shown in the minimal dialog.

Extend to the right

☑ The **Extend to the right** option is shown in the minimal dialog. (Default)

☐ The option is not shown in the minimal dialog.

Rotate displays (Page orientation)

☑ The **Rotate displays (Page orientation)** option is shown in the minimal dialog.

☐ The option is not shown in the minimal dialog. (Default)

Mouse options

☑ The **Left-handed mouse**, **Pointer speed** and **Double click interval** settings are shown.

☐ The mouse settings are not shown. (Default)

Advanced

☑ The **Advanced** button is shown. With **Advanced**, you can switch to the advanced dialog. (Default)

☐ The **Advanced** button is not shown.

Reset

☑ The **Reset** button is shown. With **Reset**, you can restore the default settings. (Default)

☐ The **Reset** button is not shown.

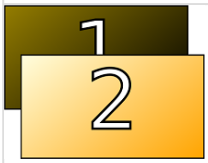
Timeout for confirmation dialog: Specifies how long a dialog for confirming the configuration should be shown. (Default: 10 seconds)

For more information, see the manual chapters

- Minimal Dialog (see page 1735)
- Advanced Dialog (see page 1736)
- Using Display Switch (see page 1737)

or the how-to Display Switch (see page 823).

Minimal Dialog

Selection	Function
	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the right.
	Extends the display area to the screen on the left
	Uses only display 2.
	Rotates the selected display to the left or to the right.

Identify Displays: Starts the monitor detection.

Advanced: Switches to **Advanced** mode of display configuration.

Reset: Restores the default settings.

Close: Closes the **IGEL Display Switch** window.

Mouse options

- **Lefthand Mode**
  ☑ Lefthand mode is active.
  ☐ Righthand mode is active. (Default)
- **Pointer speed**: Value for the mouse speed in percentage between 1 (slow) and 100 (fast). (Default: 50)
- **Double click**: Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click. (Default: 300)

For more information, see Using Display Switch (see page 1737) and Display Switch (see page 823).

Advanced Dialog

You can access the advanced settings by clicking **Advanced** in the minimal dialog.

Advanced settings (pan/scale/resolution) can be configured in a collapsible area on the right. To enlarge the **Advanced** modes window, click the arrow on the right side of the window.

The following parameters must be activated for the **Display Switch** function to be able to save the settings:

- **Display Switch > Options > Preserve settings over reboot**
- **Display Switch > Options > Smart display configuration**

In the collapsible area:

- **Use this display**
  ☑ Enables the selected display.
  ☐ Disables the selected display.
- **Index**: Give the selected display an order number.
- **Rotation**: Rotation of selected display
  Possible values:
  - None (Default)
  - Left
  - Inverted
  - Right
- **Resolution**: Select the resolution of the selected display. (Default: Automatic)
- **Refresh rate**: Depends on the resolution (Default: Automatic)
- **Panning**: Set up a virtual screen that is larger than your physical screen. It will look like an enlarged screen. By moving the mouse to the edge of the screen, hidden parts become visible. (Default: None)
- **Reflection**: Transforms the display as if being reflected by a mirror.
  Possible values:
  - None (Default)
  - Horizontal
  - Vertical
  - Horizontal and Vertical
- **Scale from**: A software variant of the resolution. This can be useful if you need a resolution that is not available on the hardware. (Default: None)

For more information, see the articles Using Display Switch (see page 1737) and Display Switch (see page 823).

Using Display Switch

The function **Display Switch** has been extended with IGEL OS 11.01.100. It is now possible to use several different profiles, which are automatically selected at runtime depending on the currently connected monitors.
A profile is created when the current monitor layout, or the current resolution, is configured via **Display Switch**. The profile is automatically assigned to the currently connected monitors and recognizes the manufacturer, model by plug and, if available, the status of the laptop cover. When the screen configuration changes (by hot (un)plugging), the system will automatically switch to the profile.
The **Display Switch** function has been redesigned in IGEL OS 11.01.100 with a new graphical user interface. All basic functions can be configured by drag-and-drop.

->Start the **Display Switch** function. The start options are described under Display Switch (see page 1730).

Identify Displays

->To start screen detection, click on **Identify Displays**
The names and properties of the screens will be detected. The connection, the assigned number (**1** = main screen) and the name will be shown on each screen. Example: **1: DVI-D(II): Samsung 24"**

Defining Main Screen

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Select the screen that you wish to define as the main screen.
3. Set the **Index** to 1.
   The display is now marked as the main screen.

Split Display over Several Screens

You have various options for using several screens. In the dialog, the connection, the assigned number (**1** = main screen) and the name is shown for each screen. Example: **1: DVI-D(II): Samsung 24"**

The procedure with the minimal dialog is described below. To switch from the advanced to the minimal dialog, click on **Simple**.

->To show the same content on all screens (Shadow screens), click on .

->If you would like to expand the display to all screens and the other screens are to the left of the main screen, click on .

->If you would like to expand the display to all screens and the other screens are to the right of the main screen, click on .

From IGEL OS 11.01.100, a drag-and-drop interface is available for individual customization. Click **Advanced** to show the drag-and-drop interface:

->Use drag-and-drop to move the displays to the desired configuration. They will snap together when they touch each other at the edge.

->If you no longer need a monitor, in **Advanced** mode you can simply drag it to the upper right corner to the **Disabled** area to disable it. To display the same content on multiple displays, drag them one on top the other. `Mirror \<other>` will be displayed. The mirroring monitor is displayed in the lower right corner.

->Click **Apply** to set the current status. Click **Yes** in the **Keep Configuration** window to save the configuration permanently and associate it with the profile.

Rotate Displays (Page Orientation)

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Rotate displays (Page orientation)** must be enabled. To switch from the advanced to the minimal dialog, click on **Basic**.

->To rotate the display counterclockwise, click on .

->To rotate the display clockwise, click on .

Change Mouse Settings

The procedure with the minimal dialog is described below; **Setup > Accessories > Display Switch > Options > Mouse Options** must be enabled. To switch from the advanced to the minimal dialog, click on **Simple**.

->To adjust the mouse for left-handed users, enable the **Lefthanded Mode**.

->To adjust the speed of the mouse pointer, change the value under **Pointer speed**. The higher the value, the further the mouse pointer will move when the mouse is moved.

->To change the time interval within which two consecutive mouse clicks are recognized as a double-click, change the number of milliseconds under **Double click interval**.

Zoom Display (Screen Magnifying Glass)

You can magnify the screen content. The effect is the same as with the screen magnifying glass in Microsoft Windows: All text and graphics are magnified by the same factor; this results in a virtual display area which is bigger than the monitor's available display area. The user therefore sees a magnified section of the entire screen; the section can be moved by moving the mouse to the edge of the screen.

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Under **Panning**, set the desired value. Example: 3860x2160
3. Under **Resolution**, set a low value. This value simulates the actual resolution of the screen.
   Example: `1280x800`
4. Click on **Apply**.
   The screen content will be magnified. The magnification factor results from the ratio of the virtual resolution and the simulated actual resolution.

   > If the same content is displayed on a number of screens (Shadow screens), all screens will show the same section. However, you can set a different magnification level for each of the screens.

Change Refresh Rate

> This is only possible if a resolution has been selected. The respective resolutions can be different. A refresh rate of 60 Hz is usually suitable for standard screens.

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Under **Refresh rate**, set the desired value.

Restore Default Settings

->Click on **Reset** to restore the default settings.

For more information, see the article Display Switch (see page 823).

Application Launcher

With the Application Launcher, you can launch predefined sessions and device functions/tools. You are also given information regarding the device and the licenses used.

Further information can be found under Application Launcher (see page 1230).

The settings for starting the function are described below.

Menu path: **Accessories > Application Launcher**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Application Launcher Configuration in IGEL OS (see page 1743)

Application Launcher Configuration in IGEL OS

Menu path: **Setup > Accessories > Application Launcher > Application Launcher Configuration**

You can hide individual areas and elements of the Application Launcher.

- **Hide system page**
  ☑ The button for displaying the system tools (accessories) will not be shown.
  ☐ The button for displaying the system tools (accessories) will be shown. (default)
- **Hide reboot button**
  ☑ The button for restarting the thin client will not be shown.
  ☐ The button for restarting the thin client will be shown. (default)
- **Hide shut down button**
  ☑ The button for shutting down the thin client will not be shown.
  ☐ The button for shutting down the thin client will be shown. (default)
- **Show current user name in about, application launcher and startmenu**
  ☑ The current user will be shown at the top edge of the relevant window.
  ☐ The current user will not be shown.

> In order for user names to be recognized and passed on, you must configure two settings beforehand:
> - Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
> - Enable local logon: **Security > Logon > Active Directory/Kerberos**

- **Single click mode:**
  ☑ Sessions are started with a single-click. This option was set up specially for users of touchscreen monitors.
  ☐ Sessions are started with a double-click. (default)

Sound Preferences

Menu path: **Accessories > Sound Preferences**

With this function, you can configure your device's audio system. For details of how to change the presets for the audio system, see Options (see page 1747). For details of how to use the function, see Using "Sound Preferences" Function (see page 1749).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Options (see page 1747)
- Using Sound Preferences Function (see page 1749)

Options

With this function, you can change presets for the audio system. The settings can be changed at any time via the "Sound Preferences" function; see Using Sound Preferences Function (see page 1749).

Menu path: **Accessories > Sound Preferences > Options**

Show volume control in taskbar

☑ The button is shown in the taskbar. When the user clicks on this button, the volume control will be shown. (Default)

☐ The button will not be shown. The user must start the Audio Settings function to change the volume. Further information can be found under Sound Preferences (see page 1744).

Remote volume settings

☑ The settings for the parameters **Mute**, **PCM volume**, **Input mute**, and **Input volume** are restored after each system restart.

☐ The last settings set by the user will remain after the next system start. (Default)

Mute

☑ Audio playback is off.

☐ Audio playback is on. (Default)

PCM volume: Preset volume in percent (default: 50)

Input mute

☑ The audio input is muted. Sounds from a microphone that are recorded are not transferred via the thin client.

☐ The audio input is switched on. Sounds from a microphone that are recorded can be transferred via the thin client. (Default)

Input volume: Volume in percent at which sounds at the audio input are recorded, for example from a microphone. (Default: 100)

Default Sound Output

Port name
Possible options:

- Automatic: The audio output is automatically assigned to a device. The following order applies here:
  1. USB devices
  2. PCI devices; this also includes the HDMI interface.
  3. Internal speaker

  Not connected ports will be ignored.
- HDMI / DisplayPort
- Speaker
- Headset

Device name: Select the device for audio output from a list of available devices. If the device is not present at the moment, you can type its name in. Examples: "Built-in Audio Analog Stereo", "Microsoft LifeChat LX-3000".

Default Sound Input

Port name
Possible options:

- Automatic: The audio input is automatically assigned to a device. The following order applies here:
  1. USB devices
  2. PCI devices
  Not connected ports will be ignored.
- Microphone
- Headset microphone

Device name: Select the device for audio input from a list of available devices. If the device is not present at the moment, you can type its name in. Example: "Microsoft LifeChat LX-3000".

Using Sound Preferences Function

-> Start the **Sound Preferences** function. The start options are described under Sound Preferences (see page 1744).

To change the playback volume, proceed as follows:

->Move the playback volume slider to the right to increase the volume or to the left to reduce the volume.

To select and configure the device for playback, proceed as follows:

1. Click on the **Output** tab.
2. Under **Play sound through**, select the device which is to be used for playback.
3. If necessary, adjust the **Balance**, **Fade** and **Subwoofer** settings.

To select and configure the device for recording, proceed as follows:

1. Click on the **Input** tab.
2. Under **Record sound from**, select the device which is to be used for recording.
3. Adjust the **Input volume** if necessary.

To change the playback volume for specific applications, proceed as follows:

1. Click on the **Applications** tab.
2. Adjust the volume control for the relevant application.

System Log Viewer

With this function, you can view your device's system logs. For details of how to add additional logs to the logs shown by default, see Options 18 (see page 1753). For details of how to use the function, see Using "System Log Viewer" function (see page 1754).

The settings for starting the function are described below.

Menu path: **Accessories > System Log Viewer**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Options (see page 1753)
- Using System Log Viewer Function (see page 1754)

Options

Menu path: **Setup > Accessories > System Log Viewer > Options**

Here, you can add additional files to the files shown by default. The **System Log Viewer** function shows the following files by default:

- `/config/Xserver/card0`
- `/config/Xserver/xorg.conf-0`
- `/config/sound/card0`
- `/config/sound/card1`
- `/config/sound/default_card_name`
- `/var/log/Xorg.0.log`

To add a further file to the display, proceed as follows:

1. Click on +.
2. In the **Add** dialog, enter the path and the file name of the desired file. Example: `/var/log/igfmount.log`

   If you want to add several files, you can also use the asterisk *. Example: `/var/log/ *.log` or `/var/log/ *.txt`

3. Click **OK**.
   When the **System Log Viewer** function is started, the file that you have added will be shown.

Using System Log Viewer Function

1. Start the **System Log Viewer** function. The start options are described under System Log Viewer (see page 1750).
2. In the left-hand column, select the file that you want to view.
   The selected file will be shown in the right-hand column.

UMS Registration

Menu path: **Accessories > UMS Registration**

With this function, you can register your endpoint device in the *UMS* (*IGEL Universal Management Suite*) locally. For details of how to use the function, see Using "UMS Registration" Function (see page 1757).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- Using UMS Registration Function (see page 1757)

Using UMS Registration Function

Menu path: **Accessories > UMS Registration**

1. Start the **UMS Registration** function. The start options are described under UMS Registration (see page 1755).
2. Enter the following data:
   - **Server address**: IP address or host name and port number of the UMS Server if it is not the default port. Example: `IP address:30002`
   - **Login**: User name for logging in to the UMS Console.
   - **Password**: Password for logging in to the UMS Console.

     > Any UMS user with sufficient rights can be specified under **Login** and **Password**.
     > Example:
     > If a device has to be registered in the root folder "Devices", "scan for devices" permission will suffice.
     > If a device has to be registered in a particular folder, the user must also have the "move" permission for this folder.

   - **Structure Tag**: Character string for assigning the device to a specific UMS directory.
   - **New host name**: Name under which the device is registered in the UMS. This name will also be displayed under **Network > LAN Interfaces > Terminal name**.
3. If you want to assign a specific UMS directory to the device, click on **Select** under **Directory** and select the desired directory from the list.
4. Click on **Register**.

Touchscreen Calibration

With this function, you can calibrate the touchscreen connected to your endpoint device. For details of how to use the function, see Using “Touchscreen Calibration” function (see page 1761).

The settings for starting the function are described below.

Menu path: **Accessories > Touchscreen Calibration**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Touchscreen Calibration (see page 1761)

Using Touchscreen Calibration

-> Ensure that **Enable touchscreen** is enabled under **User Interface > Input > Touchscreen**.

You will find a description of the touchscreen calibration procedure in the Touchscreen Calibration (see page 982) how-to.

Task Manager

This function provides an overview of the applications and other processes running on the device. You can also pause or end processes and change the priority of processes. For details of how to use the Task Manager, see Using Task Manager (see page 1765).

The settings for starting the function are described below.

Menu path: **Accessories > Task Manager**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Task Manager (see page 1765)

Using Task Manager

With the Task Manager, you can observe and influence applications and processes in the following ways:

- Determining thin client processor usage
- Determining thin client memory usage
- Determining processor usage by a specific application
- Determining memory usage by a specific application
- Pausing and continuing an application
- Closing an application
- Force closing an application
- Changing the priority of an application

->Launch the **Task Manager** function. The launch options are described under Task Manager (see page 1762).

To determine the thin client's total processor usage, proceed as follows:

->Read the percentage value under **CPU:**.

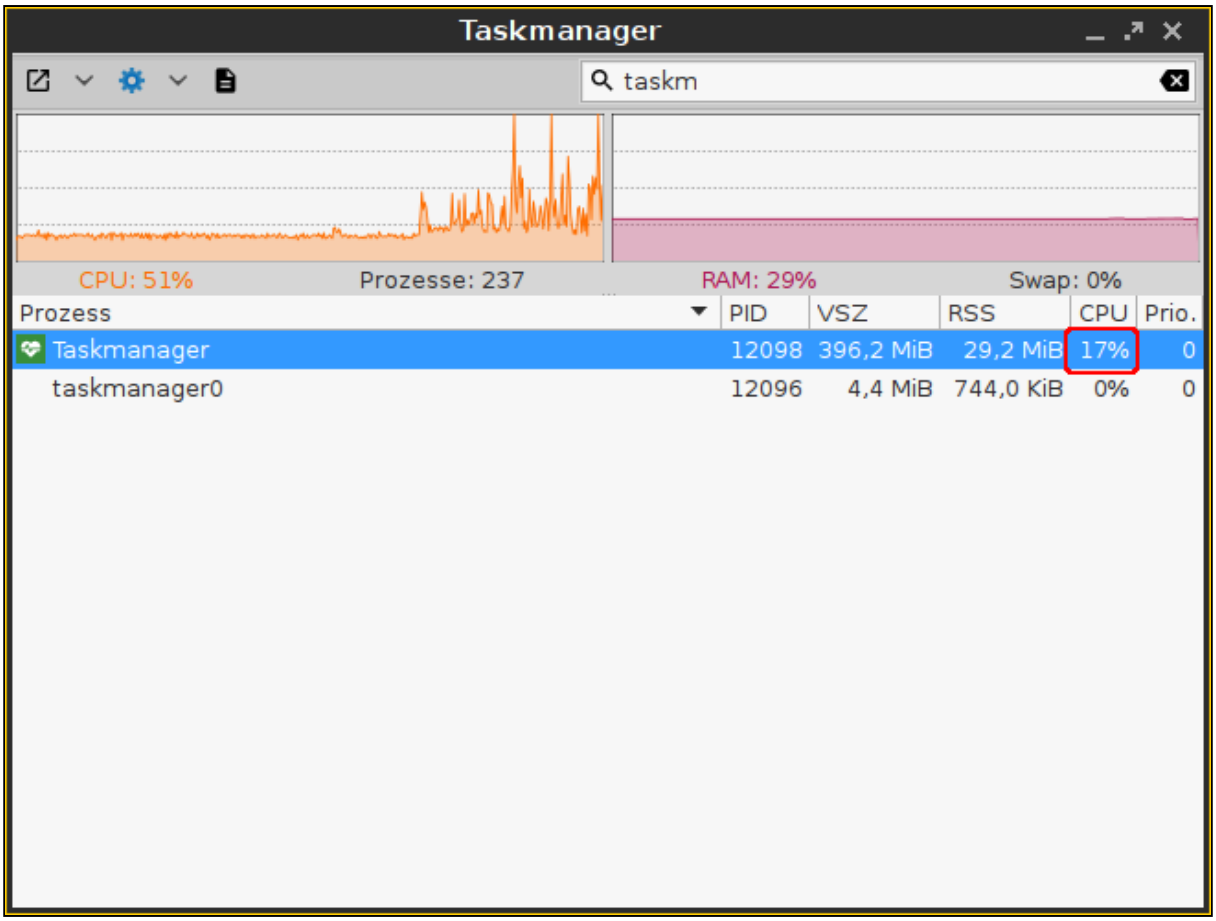
To determine the thin client's total memory usage, proceed as follows:

->Read the percentage value under **RAM:**.

->To calculate the value in bytes, click on and enable the option **Show memory usage in bytes**.

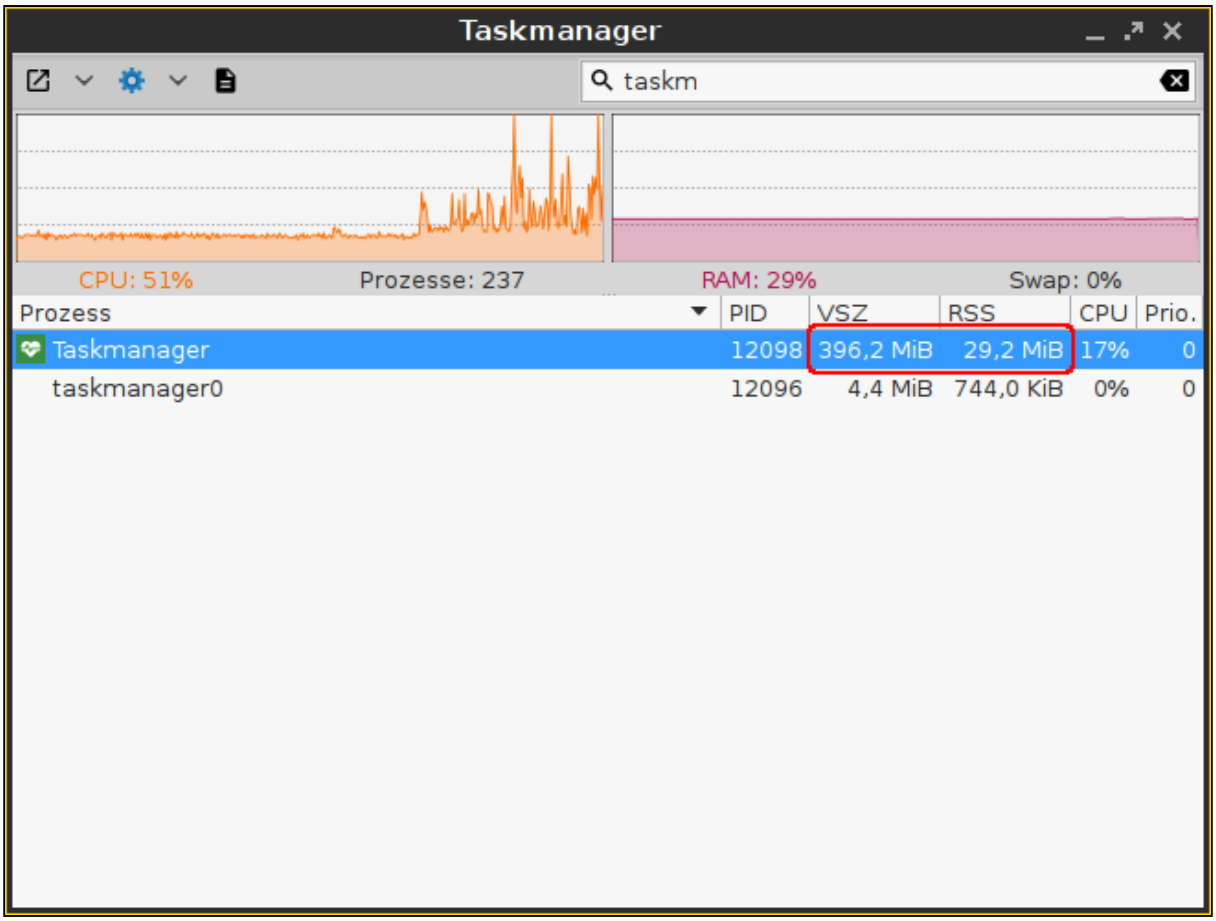
To determine the extent to which a specific application contributes to processor usage, proceed as follows:

1. In the search window, enter the name of the application or part of the name.
   The Task Manager will now show only the relevant applications and processes.
2. Read the percentage value for the relevant application in the **CPU** column.



To determine the extent to which a specific application contributes to memory usage, proceed as follows:

1. Click next to ⚙ on ⌄ and ensure that **Virtual Bytes** and **Private Bytes** are enabled.
2. In the search window, enter the name of the application or part of the name.
   The Task Manager will now show only the relevant applications and processes.
3. Read the values in the **VSZ** and **RSS** columns.
   The **VSZ** column shows how much memory is available for the application. The **RSS** column shows how much memory the application is currently using.



To pause an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Pause**.
   The application will be paused (Signal SIGSTOP). You can then continue the application.

To continue an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Continue**.
   The application will continue (Signal SIGCONT).

To close an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Close**.
   The application will close (Signal SIGTERM).

> In this case, the application is instructed to close by the operating system. If the application does not react to this instruction, you can force it to close with the **Kill** command.

To force an application to close, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Kill**.
   The application will be forced to close (Signal SIGKILL).

To change the priority of an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Priority**.
3. Select one of the following values for the priority:

> As a normal user, you can only change the priority from a higher value to a lower value. Example: If you have changed the priority from "Normal" to "Low", you can only then change it to "Very low" – you can no longer change it back to "Normal". The administrator can increase the priority.

> The priority corresponds to the nice value. High values result in a low priority, while low values result in a high priority.

- **Very low** (nice value: 15)
- **Low** (nice value: 5)
- **Normal** (nice value: 0)
- **High** (nice value: -5). This value can only be set by the administrator.
- **Very high** (nice value: -15) This value can only be set by the administrator.

Screenshot Tool

With this function, you can take a screenshot. For details of how to use the function, see Using “Screenshot Tool” (see page 1772).

The settings for starting the function are described below.

Menu path: **Accessories > Screenshot Tool**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Special Hotkeys

With the hotkeys defined under **User Interface > Hotkeys > Commands**, you can use the function as follows:

- **Screenshot of the active window**: This hotkey takes a screenshot of the window currently active.
- **Screenshot of the entire screen**: This hotkey takes a screenshot of the entire screen.

- Using Screenshot Tool (see page 1772)

Using Screenshot Tool

1. Launch the **Screenshot Tool** function. The launch options are described under Screenshot Tool (see page 1769).
2. Select the **area** you would like to photograph. You have the following options:

> If you start the function via **User Interface > Hotkeys > Commands > Screenshot of active window** or **User Interface > Hotkeys > Commands > Screenshot of entire screen**, no options will be shown.

- **Entire screen**
  ☑ The entire screen content will be photographed.
- **Active window**
  ☑ The window that is currently active will be photographed.
- **Select a region**
  ☑ You can select a section of the screen using the mouse.
- **Capture mouse pointer**
  ☑ The mouse pointer is visible on the screenshot.

3. Specify the **Delay before capturing** in seconds. The minimum value is 1.
4. Click on **OK**.
   If you have enabled **Entire screen** or **Active window**, the screenshot will be taken after the **Delay before capturing** has elapsed.
   If you have enabled **Select a region**, you can select the desired part of the screen using the mouse. To do this, press and hold the left mouse button while dragging the mouse across the screen.
5. Specify how the screenshot is to be used. You have the following options:
   - **Save**: If this option is enabled, the screenshot will be saved in PNG format via your thin client. You can save the screenshot locally, on a network drive or on a USB mass storage device.
   - **Copy to the clipboard**: If this option is enabled, the screenshot will be available in the thin client's local cache. You can access the local cache from an RDP session and open the image in an RDP session application.
   - **Open with**: If this option is enabled, the screenshot will be opened in your thin client's image viewer as soon as it is taken.

On-Screen Keyboard

Menu path: **Accessories > On-Screen Keyboard**

This function shows an on-screen keyboard on the desktop.

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.

- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Appearance (see page 1775)
- Application Integration in IGEL OS (see page 1776)

Appearance

Menu path: **Accessories > On-Screen Keyboard > Appearance**

- **Show Function Keys**
  ☑ The on-screen keyboard features the function keys [F1] ... [F12]. (default)
- **Show Navigation Keys**
  ☑ The on-screen keyboard features the arrow keys for navigating on the screen. (default)
- **Show Numpad**
  ☑ The on-screen keyboard features the number block.
  ☐ The on-screen keyboard does not feature the number block. (default)
- **Enable switching to alternative layout**

> This option is available from IGEL Linux *version 10.04.100* onwards.

☑ The on-screen keyboard has an additional key by which the user can toggle between the normal layout and a reduced layout. The reduced layout resembles the numpad, with the following differences:

- Additional backspace key [←]
- Additional tab key [⇆]
- Additional space key [ ]
- Additional escape key [Esc]
- Return key [⏎] instead of [Enter] key

☐ Switching to the reduced layout is not possible. (default)

Application Integration in IGEL OS

Taskbar settings for the login dialog

These settings are relevant if a login is necessary in order to use the device. This applies to all logon methods that are possible with the device.

Show on-screen keyboard button

☑ A button for launching the on-screen keyboard will be shown during the login dialog.

☐ The on-screen keyboard cannot be launched during the login dialog. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is shown during the login dialog. The on-screen keyboard can be used for input in the logon dialog.

☐ The on-screen keyboard is not shown during the login dialog. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

Taskbar settings when the screenlock is active

Show on-screen keyboard button

☑ If the screen is locked, a button for launching the on-screen keyboard will be shown.

☐ If the screen is locked, the on-screen keyboard cannot be launched. (Default)

Start on-screen keyboard automatically

☑ If the screen is locked, the on-screen keyboard will be shown.

☐ If the screen is locked, the on-screen keyboard will not be shown. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

On-Screen Keyboard Toggle Button

Show button

☑ A button for switching the on-screen keyboard on and off will be shown on the desktop.

☐ The button will not be shown. (Default)

Touch and hold delay: Time in milliseconds, after which the button reacts to movement. (Default: 1000 ms)

Button size: A size between 40 and 80 pixels can be chosen. (Default: 60px)

Automatically show on-screen keyboard when text field is selected

☑ The on-screen keyboard is shown automatically when an input field gets the focus.

☐ The on-screen keyboard is not shown automatically.

For further information, see Showing and Hiding the On-Screen Software Keyboard Automatically (see page 833).

Monitor Calibration

Menu path: **Accessories > Monitor Calibration**

With this function, you can calibrate the monitor connected to your endpoint device.

A test image which you can modify using the arrow keys will appear. Using this test image, you can automatically or manually recalibrate your screen. This applies to old, analog monitors in particular. New monitors calibrate themselves.

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Commands

The following system commands can be made accessible to the user

Menu path: **Accessories > Commands**

- **Logoff**: Logs the user off from the device.
- **Reboot Terminal**: Restarts the device.
- **Restart windowmanager**: Restarts the device's user interface.
- **Shutdown terminal**: Shuts down the device.
- **Sort icons**: Sorts the symbols on the desktop so that they form a block.

->To edit a user command, double click the relevant entry in the list.

If you have made changes to the hotkey, you can check these by clicking the relevant entry in the **Key** column.

You can change the following starting methods:

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)

- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Network Tools

Menu path: **Accessories > Network Tools**

This function provides the following tools for network analysis:

- **Devices**
- **Ping**
- **Netstat**
- **Traceroute**
- **Lookup**

For how to use the network tools, see Using Network Tools Function (see page 1786).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Network Tools Function (see page 1786)

Using Network Tools Function

->Start the **Network Tools** function. The start options are described under Network Tools (see page 1783).

> To start Network Tools, administrator credentials are required.

To obtain information regarding a network device available on your thin client, proceed as follows:

1. Click on the **Devices** tab.
2. Under **Network device**, select the network device for which you would like to obtain information.
   The information regarding the selected network device will be shown.

To send a ping query to a device in your network, proceed as follows:

1. Click on the **Ping** tab.
2. Under **Network address**, enter the IP address or the host name of the device to which you would like to send a ping query.
3. If necessary, add the number of ping queries under **Send**.
4. Click on the **Ping** button.
   The set number of ping queries will be sent. The results will then be shown.

To obtain information regarding the network status of your thin client, proceed as follows:

1. Click on the **Netstat** tab.
2. Select the desired information under Display:
   - **Routing Table Information**
   - **Active Network Services**
   - **Multicast Information**
3. Click on the **Netstat** button.
   The desired information will be shown.

To identify the router via which an IP data packet from your thin client reaches a specific target computer, proceed as follows:

1. Click on the **Traceroute** tab.
2. Under **Network address**, give the IP address of the target computer.
3. Click on the **Trace** button.
   The thin client will send IP packets to the target computer at short intervals, each with a TTL (Time To Live, i.e. maximum number of hops) increased by 1.
   When the packet reaches the target computer, "reached” will be shown in the last line and no further packet will be sent.
   If no computer replies, "no reply" will be shown.

With the **Lookup** function, you can request DNS information regarding any address on the Internet from your thin client.

Further information regarding the DNS (Domain Name System) can be found on Wikipedia under Domain Name System[194].

194. https://en.wikipedia.org/wiki/Domain_Name_System

Detailed descriptions of the Domain Name concept can be found in RFC 1034[195] and in related RFCs.

To obtain DNS information regarding an address on the Internet, proceed as follows:

1. Click on the **Lookup** tab.
2. Under **Network address**, give the IP address or the host name.
3. Under **Information type**, select which information is to be shown. The following information types are available:
    - Default information
    - Internet address
    - Canonical name
    - Processor type/operating system
    - Mailbox exchange
    - Mailbox information
    - Name server
    - Computer name for address
    - Text information
    - Generally known services
    - Any / all information
4. Click on **Lookup**.
   The desired information will be shown.

195. https://tools.ietf.org/html/rfc1034

Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your thin client. For details of how to use the function, see Using Bluetooth Tool (see page 1791).

In order to be able to use Bluetooth, it must be enabled under **Devices > Bluetooth**.

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Bluetooth Tool (see page 1791)

Using Bluetooth Tool

Menu path: **Accessories > Bluetooth Tool**

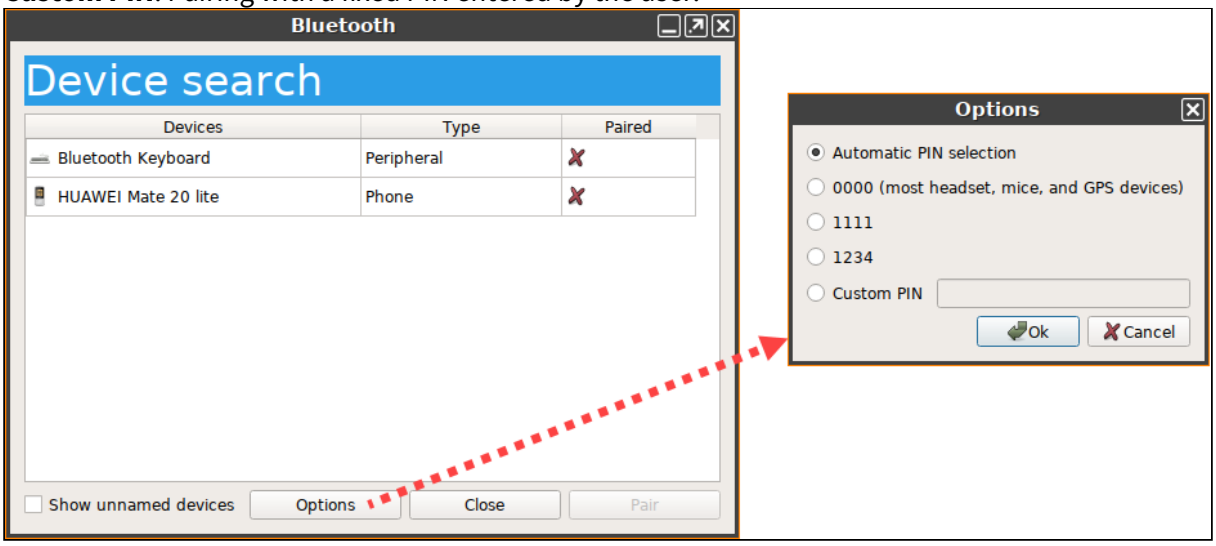
Overview

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your endpoint device.

> If your endpoint device (e.g. UD2 D220) does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

The **Bluetooth Tool** supports the following coupling methods, i.e. the mutual authentication of the Bluetooth device and endpoint device:

- **Automatic PIN selection**: Pairing with automatic PIN allocation
- **0000**, **1111**, **1234**: Pairing with a fixed PIN (for most headsets, mice, or GPS devices)
- **Custom PIN**: Pairing with a fixed PIN entered by the user.



In addition, also Bluetooth devices that do not require pairing are supported.

Connecting a Bluetooth Device with Automatic PIN Selection

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under Bluetooth Tool (see page 1788).
   The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
   After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, enable **Automatic PIN selection**.
6. Click on **Pair**.

7. A PIN will be shown in the dialog on your endpoint device.
   - If the PIN is identical to the PIN shown on your Bluetooth device, confirm the coupling.
   - If a Bluetooth device requires the manual entering of a PIN (e.g. keyboard), type in the PIN shown in the dialog.
     In a few seconds, the status of the connection will be shown.
8. On successful connection, close the dialog.

For an example on how to connect a Bluetooth device, see Bluetooth Tool (see page 1048).

Connecting a Bluetooth Device with a Fixed PIN

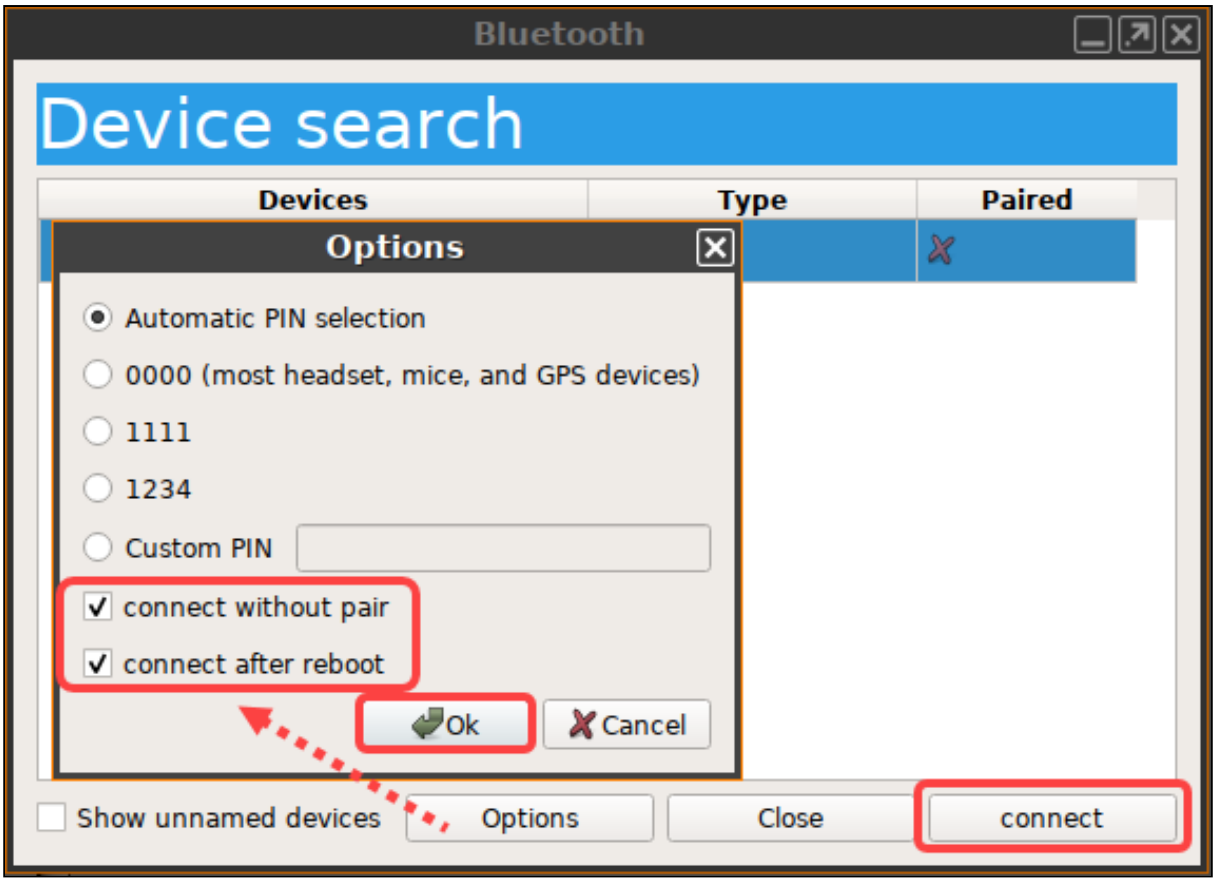
1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**. The start options are described under Bluetooth Tool (see page 1788).
   The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
   After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Highlight the desired Bluetooth device.
5. Under **Options**, select one of the specified PINs or enable **Custom PIN** and enter the PIN for the Bluetooth device. You will find this PIN in the documentation for your Bluetooth device.
6. Click on **Pair**.
   In a few seconds, the status of the connection will be shown.
7. On successful connection, close the dialog.

Canceling Coupling to a Bluetooth Device

1. Start the **Bluetooth Tool**. The start options are described under Bluetooth Tool (see page 1788).
   The connected Bluetooth device will be shown in the **Device search** dialog.
2. Highlight the connected Bluetooth device and click on **Unpair**.
   The status of the connection will be shown.
3. Close the dialog.

Enabling Support for Devices That Do Not Require Coupling

1. Open the Setup (or the configuration dialog of the UMS), go to **System > Registry > devices > bluetooth > connect_only** and activate **Connect devices without pairing** (registry key: `devices.bluetooth.connect_only`).
2. Click **Apply** or **Ok** to confirm the changes.
3. Start the **Bluetooth Tool**. The start options are described under Bluetooth Tool (see page 1788).
   The **Device search** dialog will be shown.
4. Highlight the desired Bluetooth device.
5. Under **Options**, enable **Connect without pair** and, if required, **Connect after reboot**.



6. Click on **Connect**.

> Some devices do not connect automatically after the reboot. To fix that, you can use the following command in a script:
> `bluetoothctl connect <device-ID>`
> The return value tells you if the device is connected (0) or not (1).

System Information

Menu path: **Accessories > System Information**

With this function, you can obtain information regarding the operating system of your device and the installed system components, internal and connected hardware and the network. You can also measure the performance of your device using various benchmarks.

The information shown can be copied to the clipboard in order to send it to the IGEL Support department for example.

For details of how to use the function, see Using “System Information” Function (see page 1797).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using System Information Function (see page 1797)

Using System Information Function

Menu path: **Accessories > System Information**

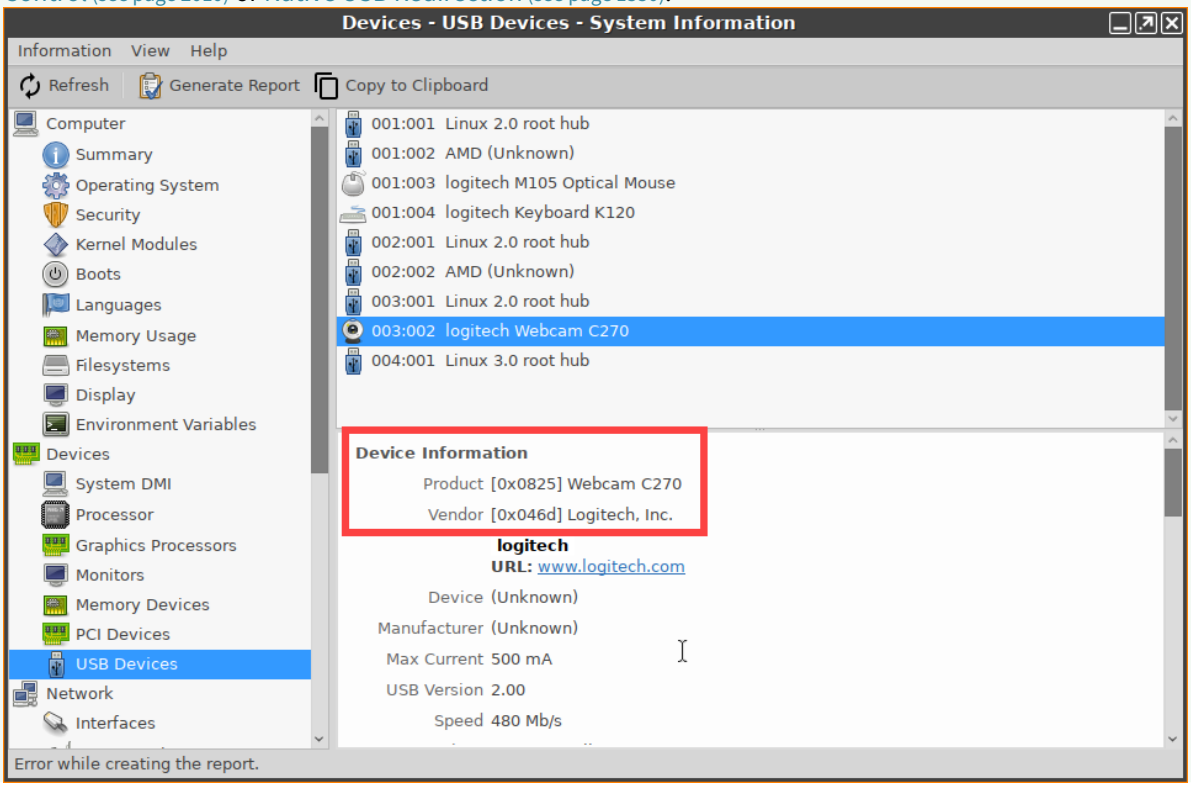
To obtain system information regarding a specific component of your IGEL OS device, proceed as follows:

1. Start the **System Information** function. The start options are described under System Information (see page 1794).

   > As of IGEL OS 11.08.290, an **administrator** password is by default required to open **System Information**. If necessary, you can change the default value in the IGEL Setup under **Accessories > System Information > Password protection**.

2. Click on the desired area, e.g. **Computer > Operating System**.
   The information regarding the desired area will be shown.
3. To send the information shown, e.g. to the IGEL Support department, click on the **Copy to Clipboard** button.
   The information is on your clipboard. With **Paste** or [Ctrl] + [V], you can paste the information into an e-mail or a web form.

You can use the **System Information** function to find out the **Vendor ID** and **Product ID** of your connected hardware. They are required, for example, if you want to configure **Device Rules**, see e.g. USB Access Control (see page 2010) or Native USB Redirection (see page 1330).



See also Issues with USB IDs in USB Devices Rules (see page 1100).

Disk Utility

With this function, you can obtain information regarding the hotplug storage devices connected to your thin client. You can also remove hotplug storage devices safely, i.e. without the risk of losing data.

> The **Disk Utility** function can only be started if the automatic mounting of hotplug storage devices is enabled. The automatic mounting of hotplug storage devices is enabled if the option "**Dynamic**" is selected under **Setup > Devices > Storage Devices > Storage Hotplug > Client drive mapping** or the number in **Setup > Devices > Storage Devices > Storage Hotplug > Number of drives** is greater than "0".

For details of how to use the function, see Using “Disk Utility” (see page 1802).

The settings for starting the function are described below.

Menu path: **Accessories > Disk Utility**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Disk Utility (see page 1802)

Using Disk Utility

To obtain information regarding a hotplug storage device connected to your thin client, proceed as follows:

1. Start the **Disk Utility** function. The start options are described under Disk Utility (see page 1799).
2. Click on the desired hotplug storage device in the left-hand column.
   The information regarding the hotplug storage device is shown in the right-hand column.

To remove a hotplug storage device safely, proceed as follows:

1. Start the **Disk Utility** function. The start options are described under Disk Utility (see page 1799).
2. Click on the **Safely Remove Hardware** button in the right-hand column.
   The hotplug storage device is disconnected from the thin client. Once it has been disconnected, the storage device can be removed from the thin client.

   If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug beep** is enabled, a signal tone will signal that the device has been disconnected successfully. If **Setup > Devices > Storage Devices > Storage Hotplug > Hotplug message** is enabled, a message window will signal that the device has been disconnected successfully. Further information can be found under Storage Hotplug (see page 1969).

Disk Removal

With this function, you can remove a hotplug storage device connected to your endpoint device safely without the risk of losing data.

The settings for starting the function are described below:

Menu path: **Accessories > Disk Removal**

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)

- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Disk utility in eject menu:

☑ Allows to start the disk utility from the eject menu.

See also Using Disk Utility (see page 1802).

Mobile Device Access

Menu path: **Accessories > Mobile Device Access**

> **Feature Not Available on IZ Devices**
>
> This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

With this function, you can access the directories and files of a mobile device. Mobile device access is available from IGEL OS 10.04.100 onwards.

Feature with limited support! The mobile device access feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The following device types can be used:

- Smartphones with Android (via MTP / PTP) or iOS
- Tablets with Android via MTP / PTP) or iOS
- Digital cameras

The functionality may differ according to the specific device and operating system version.

To use the mobile device access feature, you must first activate the function. For information about the activation and use, see Using Mobile Device Access (see page 1076).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Firmware Update

Menu path: **Accessories > Firmware Update**

With this function, you can update your endpoint device's firmware. For details of how to use the function, see Using "Firmware Update" (see page 1812).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Firmware Update Function (see page 1812)

Using Firmware Update Function

To launch the firmware update for your endpoint device, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. Further information can be found under Firmware Update Settings for IGEL OS (see page 2056).
2. Start the **Firmware Update** function. The start options are described under Firmware Update (see page 1809).
3. Confirm this by clicking **Yes**.
   The latest firmware will be loaded onto your endpoint device. The device will restart in the process.

Smartcard Personalization

Menu path: **Accessories > Smartcard Personalization**

With this function, you can change the password for your IGEL smartcard. For details of how to use the function, see Using “Smartcard Personalization” function (see page 1816).

Further information regarding the IGEL smartcard can be found in the Authentication with IGEL Smartcard (see page 782) how-to.

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- Using Smartcard Personalization Function (see page 1816)

Using Smartcard Personalization Function

With this function, you can change your user name, the associated password and sessions on your IGEL smartcard.

To personalize an IGEL smartcard, proceed as follows:

1. Start the **Smartcard Personalization** function. The start options are described under Smartcard Personalization (see page 1813).
2. Specify the access data on your IGEL smartcard:
   - **First name**: First name of the user
   - **Last name**: Surname of the user
   - **Require password**
     ☑ A password must be entered when logging on with this IGEL smartcard.
     ☐ No password must be entered when logging on.
   - **Password**: Password for logging on with this IGEL smartcard.
3. Select the sessions and functions that are to be available on this IGEL smartcard.
4. Specify the start behavior for the sessions and functions on this IGEL smartcard:
   - **Autostart**
     ☑ The session/function will automatically start after you log on. The application launchers configured in the desktop integration are available.
     ☐ The session will not automatically start. The application launchers configured in the desktop integration are available.
   - **Restart**
     ☑ The session/function will automatically restart after being closed.
     ☐ The session/function will not automatically restart.
5. Click on **Write smartcard**.

   Do not remove the IGEL smartcard before the writing operation is complete.

   A confirmation dialog will appear when the writing operation is complete.
   You can now remove the IGEL smartcard.

Identify Monitors

Menu path: **Accessories > Identify Monitors**

With this function, you can identify the monitors connected to your thin client. For details of how to use the function, see Using “Identify Monitors” function (see page 1820).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Identify Monitors Function (see page 1820)

Using Identify Monitors Function

To identify the monitors connected to your thin client, proceed as follows:

->Start the **Identify Monitors** function. The start options are described under Identify Monitors (see page 1817).
The following data are shown for each monitor:

- Socket to which the monitor is connected
- Type of monitor
- Resolution currently used
- Maximum resolution of the monitor if the resolution currently used is a different one

Webcam Information

Menu path: **Accessories > Webcam Information**

With this function, you can change and check the settings for a connected webcam. For details of how to use the **Webcam Information** function, see Using Webcam Information (see page 1824).

The settings for starting the function are described below.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Using Webcam Information (see page 1824)

Using Webcam Information

You can determine and change the width, height and frame rate for the webcam connected.

> Alternatively, you can determine the values supported by the webcam in the local terminal with the command `webcam-info -l`.

To determine and change the values for width, height and frame rate, proceed as follows:

1. Start the **Webcam Information** function.
   The following values will be shown:
   - **Width**: Width of the image in pixels
   - **Height**: Height of the image in pixels
   - **Rate**: Frame rate in fps (frames per second: individual images per second). Example: **1/30** means 30 individual images per second.
2. Click on one of the fields to change the value. The supported values will be shown in the process.
3. Click on **Test**.
   The video image generated by the webcam with the current settings will be shown.
   In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open https://www.onlinemictest.com/webcam-test/ in your browser within the session.

ICG Agent Setup

Menu path: **Accessories > ICG Agent Setup**

This tool helps you configure the connection to IGEL Cloud Gateway (ICG). To learn how to use it, please refer to Using ICG Agent Setup (see page 1828).

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

- Using ICG Agent Setup (see page 1828)

Using ICG Agent Setup

This assistant helps you configure the connection to IGEL Cloud Gateway (ICG):

->Start **ICG Agent Setup**. Start options are described in ICG Agent Setup (see page 1825).

- **Address**: IP address or DNS name of the server running ICG. You can specify a TCP port by appending a colon and the port number.

->After entering the server address, click **Connect**.

- If you are using an ICG certificate signed by an unknown CA:
  Root certificate fingerprint: Fingerprint identifying the root certificate - three of four fields are prefilled.
  Supply the missing fingerprint field from the credentials you received from your system administrator.
- **ICG One-Time Password**: The one-time-password you received from your system administrator.
  - Click this icon in order to make the one-time password readable.
  -

    Click this icon in order to change the keyboard layout for entering the password.
- **Login**: Click this button to connect the thin client to ICG.
- **Finish**: Click this button for instant connection to ICG. Otherwise, it will be started automatically on the next boot.

This cloud icon in the system tray indicates that the thin client is connected to ICG.

If you are switching between home office and company office often, it may be feasible to configure your IGEL OS so that it prefers the local UMS over the ICG. This prevents your device from connecting to the ICG instead of the local UMS although the device is located in the company network.
To make the device prefer the local UMS, make the following settings:

1. Go to **IGEL Setup > System > Registry > system > remotemanager > icg_try_ums_connect** (Search parameter: **system.remotemanager.icg_try_ums_connect**).
2. Enable **Prefer UMS over ICG**.
3. Confirm your setting with **Ok**.

Licensing

Menu path: **Accessories > Licensing**

With this function, you can acquire a license from IGEL. An internet connection is required. The following license types are supported:

- Enterprise Management Pack (EMP)
- Software Maintenance

For information on how to use the license browser, see "Alternative License Deployment" under Setup Assistant for IGEL OS (see page 2101).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? " < > | [ ] { } ( )`

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to

be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Login Enterprise

Menu path: **Setup > Accessories > Login Enterprise**

Login Enterprise Launcher

This accessory can be enabled to act as a remote endpoint that can launch test sessions for the purpose of evaluating the performance and availability of the resources it connects to. To use this feature, there must already be a Login Enterprise Virtual Appliance to which this Launcher can connect.

To learn more about using Login Enterprise with IGEL, see https://www.loginvsi.com/igel/. See also the how-to Login Enterprise Configuration (see page 548).

Server URL: URL of the Login Enterprise server

Secret: See How to Get the Secret for Login Enterprise Launcher (see page 554).

Connector ID Key Software

Menu path: **Accessories > Connector ID Key Software**

Stratusphere UX is used to assess or inventory the current environment as the basis for designing the target environment.

The Stratusphere IGEL agent will detect RDP/RFX, ICA/HDX, PCoIP and Blast protocols to precisely measure the user experience and validate that the new desktops meet performance and security demands.

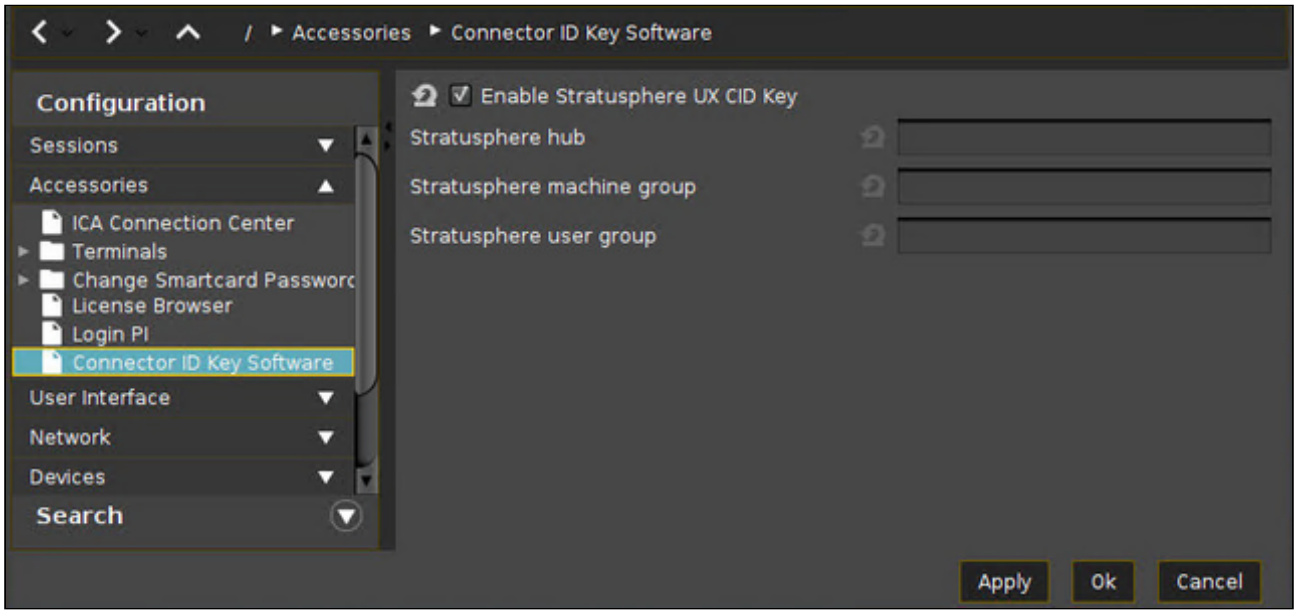
Enable Stratusphere UX CID Key

☑ Stratusphere UX CID Key is enabled.

Stratusphere hub: The hub (IP-address or DNS) of the Stratusphere.

Stratusphere machine group: Machine group of the Stratusphere.

Stratusphere user group: User group of the Stratusphere.



OS 11 Upgrade

Menu path: **Accessories > OS 11 Upgrade**

With this tool, you can upgrade a device from IGEL OS 10 to IGEL OS 11. For more information about this tool, see Testing the Upgrade[196]; for instructions on how to upgrade, see Upgrading IGEL Devices from IGEL OS 10 to IGEL OS 11 (see page 228).

The settings for starting the function are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

196. https://kb.igel.com/en/igel-os/11.10.250/testing-the-upgrade-3

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

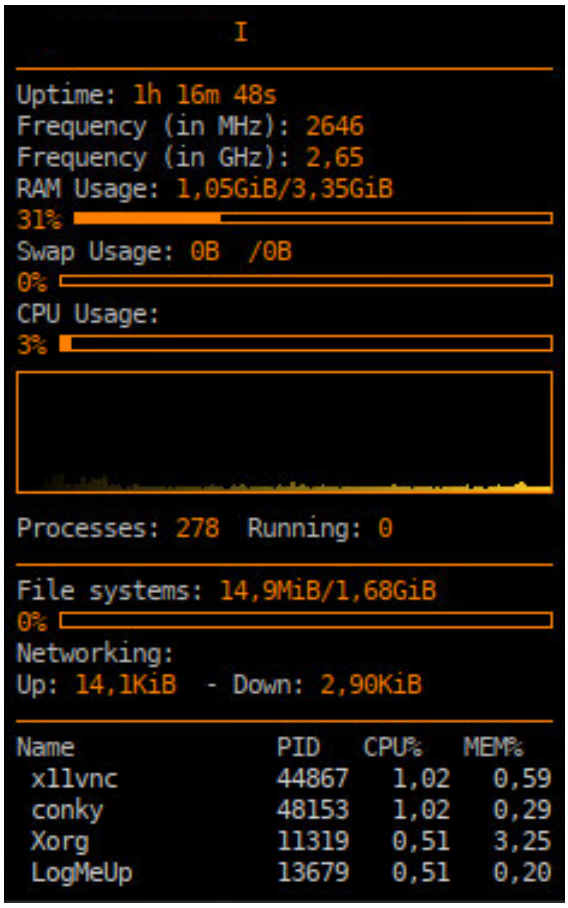
- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Conky System Monitor

Menu path: **Accessories > Conky System Monitor**

The Conky system monitor displays current system data such as uptime, CPU frequency, RAM usage, and process-specific data. For details of how to configure the Conky system monitor, see Options (see page 1841) and Custom Setup (see page 1842).



The settings for starting Conky are described below. The start icons also function as stop icons.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`

- [Ctrl] = `Ctrl`
- = `Mod4`

> When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**

- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Options (see page 1841)
- Custom Setup (see page 1842)

Options

Menu path: **Accessories > Conky System Monitor > Options**

Use IGEL Setup for configuration

☑ The settings on this Setup page are effective.

> The configuration under **Accessories > Conky System Monitor > Custom Setup** (see Custom Setup (see page 1842)) is always effective, regardless of whether **Use IGEL Setup for configuration** is activated or not.

Monitor: Monitor on which the Conky system monitor is to be displayed.

Window type
Possible options:

- "Normal": The window layout and behavior can be further specified by the following parameters:
  - **Layer**
  - **Decorations**
  - **Show in the taskbar**
  - **Opacity**
  - **Borders**
- "Desktop": No window decorations; always visible on the desktop; no appearance in the pager or taskbar; sticky across all workspaces. The parameters **Decorations** and **Show in taskbar** are not effective.
  - **Layer**
  - **Opacity**
  - **Borders**
- "Dock": Behavior as documented under https://linux.die.net/man/1/conky
- "Panel": The window reserves space along a desktop edge, just like panels and taskbars, preventing maximized windows from overlapping them.
- "Override": The window is not under the control of the window manager.

Alignment: Defines where the window is placed on the screen.

Layer: Defines whether the Conky window is displayed above or below other application windows.
Possible options:

- "Below": The Conky window is always below other application windows.
- "Above": The Conky window is always above other application windows.
- "None": The Conky window is above or below other application windows, depending on the focus.

Font type: Defines the font type for Conky.

Font size: Defines the font size for Conky.

Opacity: Defines the opacity for Conky. If the value is set to 0, the window is completely transparent; if the value is set to 255, there is no transparency.

Offset horizontal: Defines the horizontal offset from the position that is defined by **Alignment**.

Offset vertical: Defines the vertical offset from the position that is defined by **Alignment**.

Custom Setup

Menu path: **Accessories > Conky System Monitor > Custom Setup**

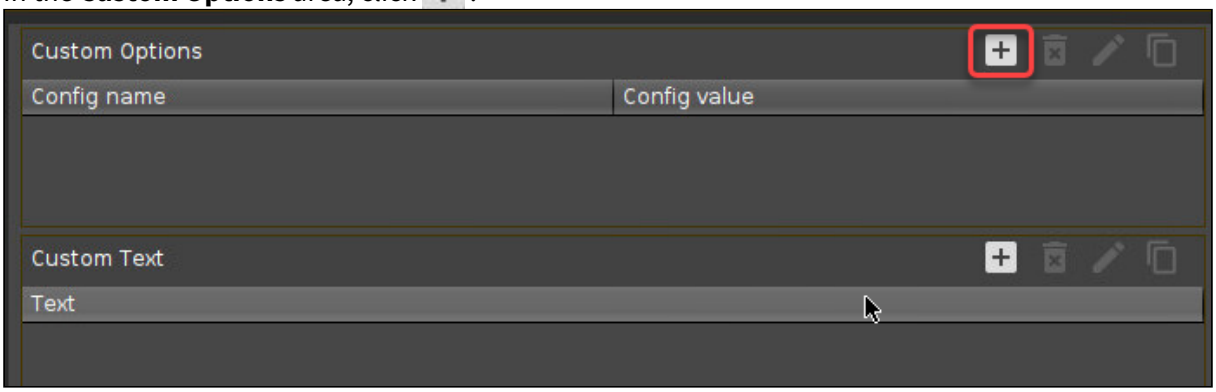
On this Setup page, you can customize Conky in full. For details, see https://linux.die.net/man/1/conky.

Custom Options

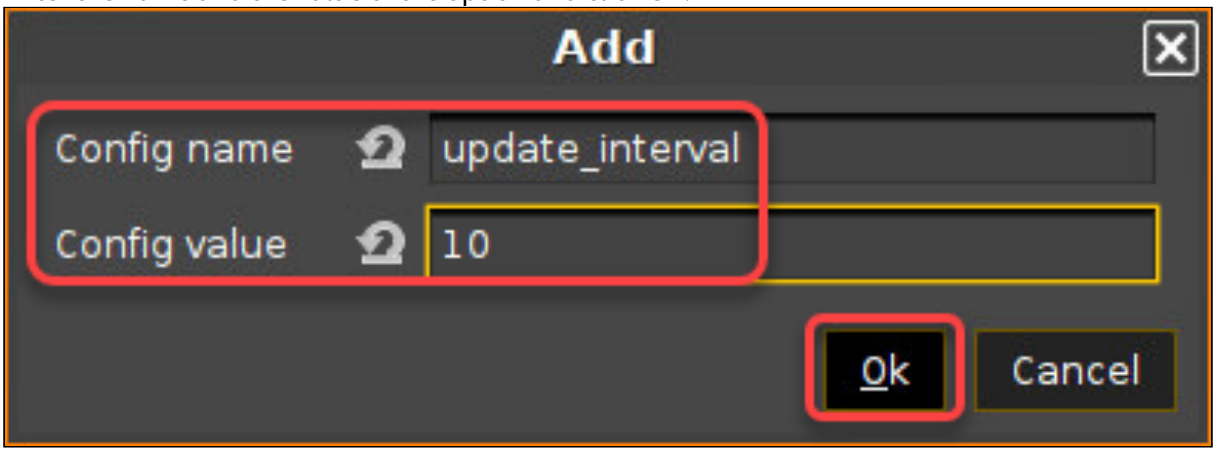
You can find the configuration options of Conky under https://linux.die.net/man/1/conky, section "Configuration Settings".

To add a custom option:

1. In the **Custom Options** area, click + .



2. Enter the name and the value of the option and click **Ok**.



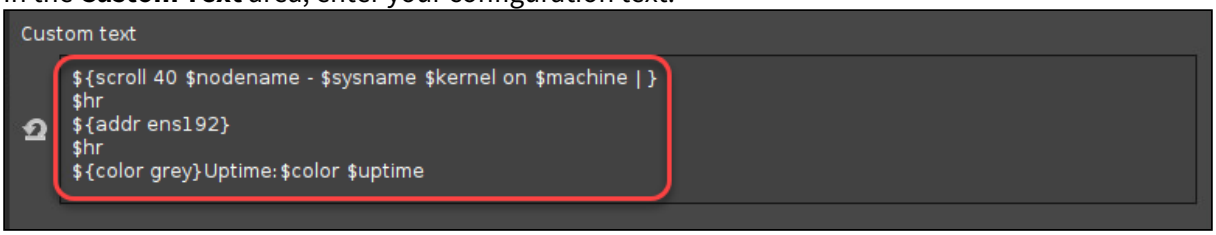
3. In the main window, click **Apply** or **Ok**.
   If Conky is already running, you can see the effect immediately.

Custom Text

In this area, you can define the complete text body of Conky. You can find the relevant details under https://linux.die.net/man/1/conky, section "OBJECTS/VARIABLES". The configuration is stored at `/etc/conky/conky.conf`

To add or edit the custom text:

1. In the **Custom Text** area, enter your configuration text.



2. In the main window, click **Apply** or **Ok**.
   If Conky is already running, you can see the effect immediately.

User Interface

- Language Settings for IGEL OS 11 (see page 1845)
- Screenlock / Screensaver (see page 1846)
- Font Services (see page 1854)
- Desktop (see page 1857)
- Input (see page 1873)
- Hotkeys (see page 1884)
- Display Settings in IGEL OS (see page 1889)

Language Settings for IGEL OS 11

In this area, you can configure the country-specific language settings.

Menu path: **Setup > User Interface > Language**

Language

The language of the user interface.

Keyboard layout

When the language is changed for the first time, the keyboard layout is automatically set to the same language.

Show indicator in taskbar

☑ Shows a country abbreviation for the keyboard layout in the taskbar.

☐ No indicator is shown. (System default)

Input language

The keyboard layout is used by default.

Standards and formats

Specifies how country-specific formats for the time and currency are displayed, for example. The default setting is geared to the input language selected.

Screenlock / Screensaver

Menu path: **User Interface > Desktop > Screen Lock/Saver**

You can set up the screen saver so that it is activated automatically after a time limit expires, via a button or in response to a key combination (hotkey). You can also select a password option. The look of the taskbar can be configured separately for the logon dialog and the locked screen.

The screen can be locked via icons in the Quick Start Panel and on the desktop or via the hotkey [Ctrl-Shift-L].

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Options (see page 1849)
- Taskbar (see page 1851)
- Screensaver (see page 1852)

Options

Menu path: **Setup > User Interface > Screenlock / Screensaver > Options**

Start automatically

☑ The screenlock or screensaver starts automatically if there is no activity on the endpoint device within this time limit. The screen can be unlocked by the user or, if the **Allow administrator password** is not disabled, the administrator with the relevant password (see: Password - Restrict Access to IGEL OS Components (see page 2017)). (Default)

Timeout: Period of time in minutes before the screenlock or the screensaver starts. (Default: 5)

Screenlock Password

- **None**: No password is set. A screenlock cannot be set up.
- **User password**: A user password is deployed to unlock the screen, see Password - Restrict Access to IGEL OS Components (see page 2017). If the user is Active Directory/Kerberos in IGEL OS (see page 2034), the AD credentials are used instead of the user password to unlock the screen.
- **Local user password**: A separate password specified under **Set** is deployed to unlock the screen. This password is also used for **Security > Logon > Local User > Login with local user password**, see Local User (see page 2039).
  If the user is Active Directory/Kerberos in IGEL OS (see page 2034), the AD credentials are used instead of the local user password to unlock the screen.

Different screenlock timeout

☑ You can specify a time limit of your own for the screenlock. (Default)

☐ The same time limit will be used for the screenlock as for the screensaver. This means that after the set time the screen will be locked and then the screensaver will appear.

Screenlock timeout: Period of time in minutes before the screenlock starts. (Default: 5)

Allow administrator password

☑ Access is allowed for the user and the administrator, see Password - Restrict Access to IGEL OS Components (see page 2017). (Default)

☐ Access is allowed for the user only.

Countdown duration in seconds: Countdown time with which the screenlock is initiated. If the value is 0, the screen is locked without a countdown. (Default: 0)

The appearance of the digits for the countdown is specified together with the settings for the clock display under **Setup > User Interface > Screenlock / Screensaver > Screensaver**; see Screensaver (see page 1852). The following parameters are relevant for the countdown:

- **Clock display monitor**
- **Show seconds**
- **Horizontal clock position**
- **Vertical clock position**
- **Clock background color**

- **Clock foreground color**

Countdown visual effect: While the countdown is running, a current screenshot is displayed in the background. This parameter determines the visual effect that the screenshot will be displayed with.
Possible options:

- Dark screenshot
- Gray screenshot

Countdown background image: Path and file name of an image file, which is displayed in the background while the countdown is running. This background image is displayed instead of the screenshot, if the path and file name are valid; if the field is empty, the screenshot is displayed. Supported file formats: JPEG, PNG, GIF. Example: `/images/image.jpg`

Taskbar

Menu path: **Setup > User Interface > Desktop > Screenlock / Screensaver > Taskbar**

Taskbar settings for the login dialog

- ☑ Show taskbar in login screen. (Default)
- ☑ Show clock. (Default)
- ☑ Show keyboard layout switcher. (Default)
- ☑ Show on-screen keyboard button.
- ☑ Start on-screen keyboard automatically.
- ☑ Show reboot button.
- ☑ Show shutdown button. (Default)

Taskbar settings when the screenlock is active

- ☑ Show taskbar in screenlock. (Default)
- ☑ Show clock. (Default)
- ☑ Show keyboard layout switcher. (Default)
- ☑ Show on-screen keyboard button.
- ☑ Start on-screen keyboard automatically.
- ☑ Show reboot button.
- ☑ Show shutdown button.
- ☑ Show logoff button.

There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1** (or **Interface 2**, **Wireless**) and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking.
The Wi-Fi icon invokes Switch for the Wi-Fi Connection (see page 1912) or the Wireless Manager (see page 1910) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.

Screensaver

Menu path: **Setup > User Interface > Desktop > Screen Lock/Saver > Screensaver**

- **Screen background color**: Color palette for determining the background color of the screen.
- **Enable image display**
  ☑ An image will be shown as the screensaver. (default)
- **File for screen saver logo**: Complete path for an individual image file or directory that contains an unlimited number of images. If no path is given, the IGEL logo will be used.

> If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show, the **display time** for the images can be configured.

- **One image per monitor**
  ☑ If a number of monitors are used, a different image will be shown on each one. (default)
  ☐ Images will be distributed over the monitors.
- **Image duration**: Time in seconds until the image is changed. (default: 10)
- **Image display mode**: Type of display. The following are available to choose from:
  - Small-sized hopping - Small images are shown in changing positions.
  - Medium-sized hopping - Larger images are shown in changing positions.
  - Full-screen center cut-out - The images are shown in full-screen size. However, they may be clipped.
  - Full-screen letterbox - The images are shown as large as possible in relation to the screen size.
- **Clock display monitor**: Selects the monitor on which the clock is to be shown. The following are available to choose from:
  - None
  - All
  - A specific monitor
- **Show seconds**: Shows the seconds too in digital format.
- **Clock display size**: The following sizes are available to choose from:
  - Tiny
  - Small
  - Medium
  - Large
  - Huge
- **Horizontal clock position**
  - Left
  - Center
  - Right
- **Vertical clock position**
  - Top
  - Center
  - Bottom
- **Clock background color**: Color palette for determining the background color of the clock.

- **Clock background opacity percentage**: 75% is preset.
- **Clock foreground color**: Color palette for determining the foreground color of the clock.

Font Services

Menu path: **Setup > User Interface > Font Services**

You can import further fonts in addition to the ones provided by IGEL:

- XC Font Service (see page 1855)
- NFS Font Service (see page 1856)

XC Font Service

Menüpfad: **Setup > User Interface > Font Services > XC Font Service**

In this area, you can configure the XC Font Service.

Enable XC Font Service

☑ The XC Font Service is enabled.

☐ Der XC Font Service is not enabled. (Default)

Once you have enabled the XC Font Service, you can define the following settings:

XC Font Server: The server on which the XC Font Service is running.

Port Number: The port number on which the XC Font Service is available. (Default: 7100)

Prefer Local Fonts

☑ Local fonts are used before a request is sent to the font server.

☐ Local fonts are not preferred. (Default)

NFS Font Service

Menu path: **Setup > User Interface > Font Services > NFS Font Service**

Using the NFS font service is another way to import additional fonts. The NFS font service also offers the advantage that the mount point for the fonts can be configured. This is necessary for a number of remote applications that search for your fonts in a specific directory.

To define and enable an NFS font path entry in order to use the NFS font service, proceed as follows.

1. Click on **Add** ⊞ to open the dialog window:
   - **Local Path**: Defines the local directory for the mount point
   - **NFS Server**: Name or IP address of the server that makes available the font directories via NFS.
   - **Remote Path**: Path on the server under which the fonts are available.
   - **Prefer Local Fonts**
     ☑ Local fonts are used before a request is sent to the font server.
2. Click on **OK** to enable the entry.
3. Export the font directory on the server via NFS read-only for the thin client.

Desktop

Menu path: **Setup > User Interface > Desktop**

On this page, you can configure general settings for the appearance of the desktop:

Local window manager for this display: Here, you can disable the window manager if you only work in full-screen sessions and do not require this service.

User interface theme: The colors of windows such as the Application Launcher, the start menu, the local terminal, the taskbar and messages can be varied. You can either select one of our predefined color schemes or define a color scheme of your own.

- IGEL Dark: The frame color is dark gray, IGEL logos are yellow.
- IGEL Light: The frame color is light gray, IGEL logos are dark gray.
- Custom Colors: Define your own color combinations below.

Desktop icon size: Specify the size in which you would like the icons to be displayed on the desktop.

Desktop icon font color: Specify the font color for the labels associated with the desktop icons. Click **Choose color** to open the color picker.

Monitor for desktop icons: If you use several monitors, select the one which is to display desktop icons.

- All monitors
- As taskbar
- 1st monitor
- 2nd monitor
- (other monitors if connected)

Single click mode:

☑ Open programs with a single click. This option was set up especially for users of touchscreen monitors.

Desktop fonts

Default font: Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans
- Sans bold
- Serif
- Serif Bold

Default font size: Specify your desired font size in pt (points) here.

Desktop icon font size: Specify your desired font size for desktop icons in pt (points) here.

Titlebarfont: Choose between serif and sans-serif text and between standard and bold. The following are available to choose from:

- Sans
- Sans bold
- Serif
- Serif Bold

Titlebar font size: Specify your desired font size in pt (points) here.

_____

- Background (see page 1859)
- Taskbar (see page 1862)
- Taskbar Background (see page 1864)
- Taskbar Items (see page 1865)
- Pager - Virtual Workspaces for Organizing the IGEL OS Desktop (see page 1866)
- Start Menu (see page 1871)
- In-Session Control Bar (see page 1872)

Background

In this area, you can configure the desktop background with predefined *IGEL* backgrounds, a fill color or a color gradient.

Menu path: **Setup > User Interface > Desktop > Background**

You can also use a background image of your own.

> You can set up a separate background image for each monitor that is connected to the thin client.

> **Wallpaper** selection options beginning with "Desktop Color" are transparent so that the background colors will shine through.

Wallpaper: Provides a selection of predefined IGEL backgrounds:

- Neutral
- Off
- Black
- Blue
- Gray
- Orange
- Green
- Yellow
- Desktop Color Light (Default)
- Desktop Color Dark
- Desktop Color Light Neutral
- Desktop Color Dark Neutral

Wallpaper Style: Provides various design versions:

- Auto
- Centered
- Tiled
- Stretched (Default)
- Scaled
- Zoomed

Color Style: Sets a fill color or a color gradient.

- Solid color (Default)
- Horizontal gradient
- Vertical gradient

Desktop Color: Select a background color if you have not selected an image.

2nd Desktop Color: Select a second background color if you have not selected an image.

Custom Wallpaper Download:

☑ You can provide a user-specific background image on a download server.

Custom Wallpaper file: Give a name for the background image file.

Specify the download server under **Desktop > Background > Custom Wallpaper Server**.

> If you have already defined a server for the system update files, you can use the same server setting for downloading the background image.

The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually (Update Background Image). The download can also be launched from the *IGEL Universal Management Suite* via **Update desktop changes**.

> A user-specific boot image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an **own background image** and **bootsplash**. A total storage area of 25 MB is available for all user-specific images.

Custom Wallpaper Server

Menu path: **Setup > User Interface > Desktop > Background > Custom Wallpaper Server**

In this area, you can configure the download server for your own background images.

- **Use firmware update server location**
  ☑ The same server and path configuration is used as for the firmware update.
  ☐ An own server location is used. (default)
- **Protocol**: Determines the protocol that is to be used. The following are available to choose from:
  - HTTP (Default)
  - HTTPS
  - FTP
  - SecureFTP
  - FTPS
  - File
- **Server Name**: Name or IP address of the server used.
- **Server Path**: Directory in which you saved the background image.
- **Port**: Port used (default: 80)
- **User name**: Name of the user account on the server
- **Password**: Password for this account
- **Wallpaper update**: Refreshes the background image.

Taskbar

Menu path: **Setup > User Interface > Desktop > Taskbar**

In this area, you can enable and configure the taskbar.

You can change the following settings:

Use Taskbar:

☑ The taskbar is displayed and the following taskbar settings options are available.

Taskbar Position: Specifies the position in which the taskbar is displayed.
Possible values:

- Bottom (Default)
- Top
- Left
- Right

Vertical Taskbar Mode: Specifies how items are shown in the taskbar. This parameter is available if **Taskbar Position** is set to **Left** or **Right**.
Possible values:

- Vertical: The session texts are rotated by 90°.
- Deskbar: The session texts are not shown. (Default)

Taskbar Height/Width: Specifies the height of the taskbar in pixels (default 40).

If **Maximum number of rows/columns in window button list** is set to **Automatic**, the window buttons as well as the icons in the Quick Start Panel will be shown in a number of rows depending on the height of the taskbar. The number of rows increases in increments of 55 pixels:

- 1 - 55 pixels: One row
- 56 - 110 pixels: Two rows
- 111 - 165 pixels: Three rows
- 166 - 220 pixels: Four rows
- 221 - 275 pixels: Five rows
- 276 or more pixels: Six rows

The **Maximum number of rows/columns in window button list** parameter is described under Taskbar Items[197].

Number of rows/columns in taskbar: Specifies the number of rows for the Quick Start Panel. The following taskbar items can be broken down into a number of rows and columns: Icons in the Quick Start Panel, window buttons. Possible values:

- Automatic: The number of rows for the Quick Start Panel depends on the height and width of the taskbar. (Default)
- Numeric value: The chosen value specifies the number of rows for the Quick Start Panel.

197. https://kb.igel.com/en/igel-os/11.10.270/taskbar-items

Multi Monitor Taskbar Size: Specifies whether the taskbar is expanded across a number of monitors or restricted to one monitor. Possible values:

- Restrict taskbar to one monitor (Default)
- Extend taskbar to all monitors

Monitor: Specifies the screen on which the taskbar is shown. This parameter is available if **Taskbar size in Multi Monitor** is set to **Restrict taskbar to one monitor** (default: 1st monitor).

Taskbar on top of all windows:

☑ The taskbar is accessible on all screens, even in sessions with a full-screen window.

Taskbar Auto Hide:

☑ The taskbar is hidden and will only be shown if the mouse pointer is moved to the position of the taskbar at the edge of the screen.

Auto Hide Behavior: Specifies when the taskbar is automatically hidden.
Possible values:

- Intelligent: The taskbar is shown as standard. The taskbar will be hidden if the space is needed by a window, e. g. a window in full-screen mode. (Default)
- Continuous: The taskbar is hidden as standard. The taskbar will be shown if the mouse pointer is moved to the edge of the screen.

Taskbar Show Delay: Time interval in milliseconds before the taskbar is shown. The mouse pointer must be at the edge of the screen constantly during this time interval. This setting is only effective if **Taskbar Auto Hide** is enabled (default: 600).

> With the show delay, you can prevent the taskbar for a full-screen session being covered by the thin client's taskbar. A show delay is necessary if the taskbar for the full-screen session is set to be shown automatically and both taskbars are positioned at the same screen edge. If no show delay is set and the user brings up the taskbar for the full-screen session, this will immediately be covered by the thin client's taskbar. During the show delay time interval, the user has time to move the mouse pointer away from the edge of the screen.

Taskbar Hide Delay: Time interval in milliseconds before the taskbar is hidden. This setting is only effective if **Automatically hide taskbar** is enabled (Default: 400).

Further settings options can be found under Screensaver and Screenlock[198].

198. https://kb.igel.com/en/igel-os/11.10.270/screenlock-screensaver

Taskbar Background

Menu path: **Setup > User Interface > Desktop > Taskbar Background**

You can specify the background style for the taskbar here.

- **Background Style**:
  Possible values:
  - System preset (Desktop)
  - Solid color
  - Color gradient
  - Background image

Depending of the above selection you can define following features:

- **Taskbar Color**: Choose the color for the taskbar.
- **2nd Taskbar Color**: Choose the 2nd color for the taskbar if you want to create gradient colors.
- **Reverse Gradient**
  ☑ The color gradient is reverse.
  ☐ The color gradient is normal. (Default)
- **Background Image Path**: Path of your background image

Taskbar Items

Menu path: **Setup > User Interface > Desktop > Taskbar Items**

- **Taskbar clock**:
  ☑ A clock is shown in the taskbar.
- **Sorting order in window button bar**: Specifies the criteria according to which the window buttons are sorted.
  Possible values:
  - Time stamp: The window buttons are sorted in the chronological order in which the windows were opened. (Default)
  - Group and time stamp: The window buttons are grouped according to the type of application. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted chronologically.
  - Window title: The window buttons are sorted alphabetically.
  - Group and window title: The window buttons are grouped according to type. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted alphabetically.
  - Drag and drop: You can order the buttons as you wish using drag and drop. You must drag a button over at least half of the button to be skipped.
- **Maximum number of rows/columns in window button bar**: Specifies the maximum number of rows available for window buttons.
  Possible values:
  - Automatic: The number of rows depends on the **Taskbar height/width** and **Number of rows/columns in taskbar** parameters, see Taskbar[199]. (Default)
  - Numeric values: This value specifies the maximum number of rows.
- **Show labels in window button bar**:
  ☑ The names of the ongoing sessions are displayed in the associated window buttons. (default)
  ☐ Only the icons are displayed.
- **Taskbar system tray**:
  ☑ The system tray is shown in the taskbar. (default)
- **Size of icons in system tray**: Specifies the size of system tray icons (volume, network connection etc.).
  You can choose a pre-defined value or enter a numeric value between 1 and 64.
  Predefined values:
  - Automatic: The size is adjusted to the height and width of the taskbar. (Default)
  - Small: 20 pixels
  - Medium: 40 pixels
  - Large: 60 pixels

  Further settings options can be found under On-screen Keyboard[200], Keyboard[201] and Additional Keyboard Layouts[202] and Screensaver and Screenlock[203].

199. https://kb.igel.com/en/igel-os/11.10.270/taskbar-1
200. https://kb.igel.com/en/igel-os/11.10.270/on-screen-keyboard
201. https://kb.igel.com/en/igel-os/11.10.270/keyboard
202. https://kb.igel.com/en/igel-os/11.10.270/additional-keyboard-layouts

Pager - Virtual Workspaces for Organizing the IGEL OS Desktop

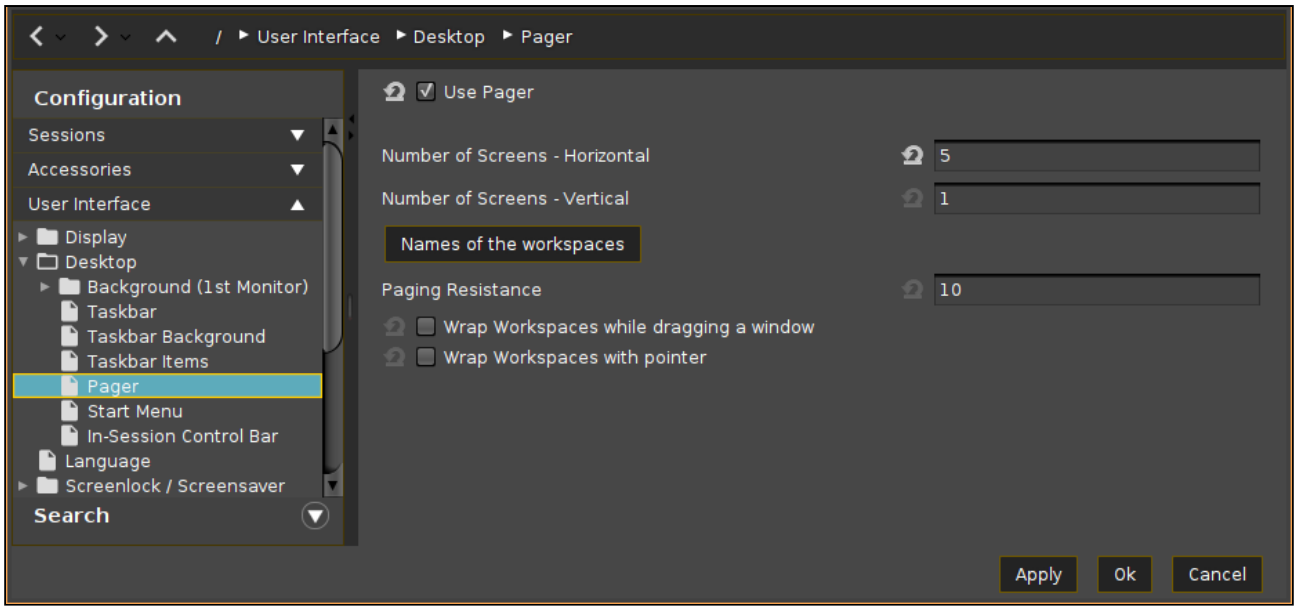
In IGEL OS, you can use the **Pager** tool to enable the use of multiple virtual desktops. The Pager allows you to divide one desktop into several virtual workspaces and, thus, to better organize your desktop: for example, you can open a certain type of applications in one workspace and another type of applications in the second workspace.

The Pager makes switching between multiple open applications easier – you can switch between full-screen applications at the click of a mouse. Instead of minimizing / maximizing sessions or switching between them using key combinations, you simply click on the desired workspace using the mouse. When you switch back, the virtual desktop is displayed exactly as before (unless you restarted the system or changed the language in the IGEL Setup).

Make sure you have enabled **User Interface > Desktop >** Taskbar (see page 1862) **> Taskbar on top of all windows**.

The Pager can be used only in non-appliance mode.

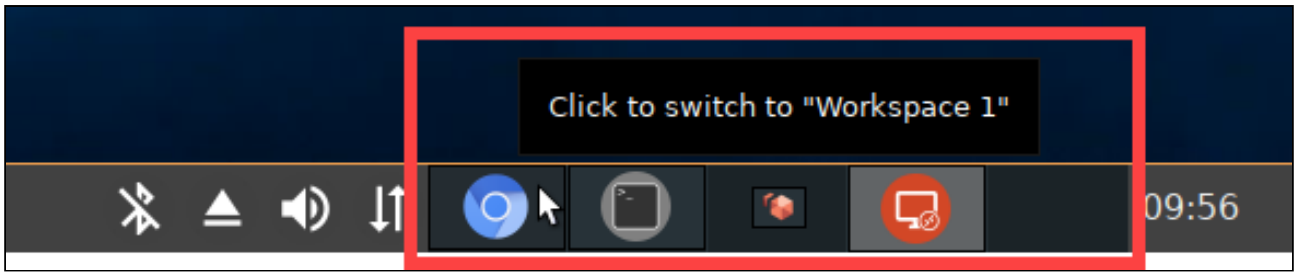
Menu path: **User Interface > Desktop > Pager**



Use Pager

☑ The Pager is enabled. You can configure up to 25 virtual desktops. The Pager will be displayed on the right of the taskbar:

203. https://kb.igel.com/en/igel-os/11.10.270/screenlock-screensaver



For details on how to use the pager, see the below section "Example for how to Use the Pager[204]".

☐ The Pager is disabled.*

Number of Screens - Horizontal

Specifies how many workspaces will be shown next to each other. (Default: 2)

Number of Screens - Vertical

Specifies how many workspaces will be shown above each other. (Default: 1)

Names of the workspaces

Specify names for the individual desktops.

Paging Resistance

Specifies how many pixels the cursor needs to be moved over the edge of the screen before it triggers a switch of the desktop. (Default: 10)

You only need to make this setting if you enable at least one of the following options – **Wrap workspaces while dragging a window** or **Wrap workspaces with pointer**.

Wrap workspaces while dragging a window

☑ The desktop is switched as soon as a window is dragged out of view.

☐ The desktop is not switched when a window is dragged out of view.*

Wrap workspaces with pointer

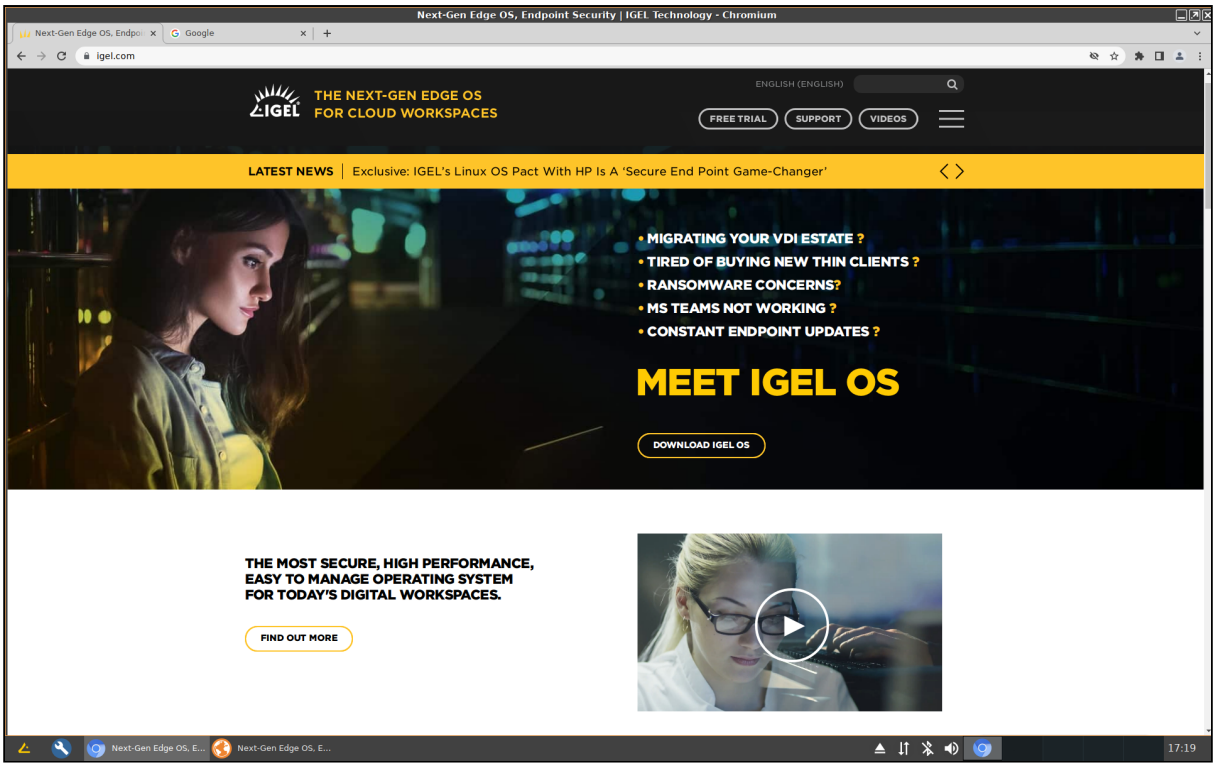
☑ The desktop is switched as soon as the mouse reaches the edge of the screen.

☐ The desktop is not switched when the mouse reaches the edge of the screen.*

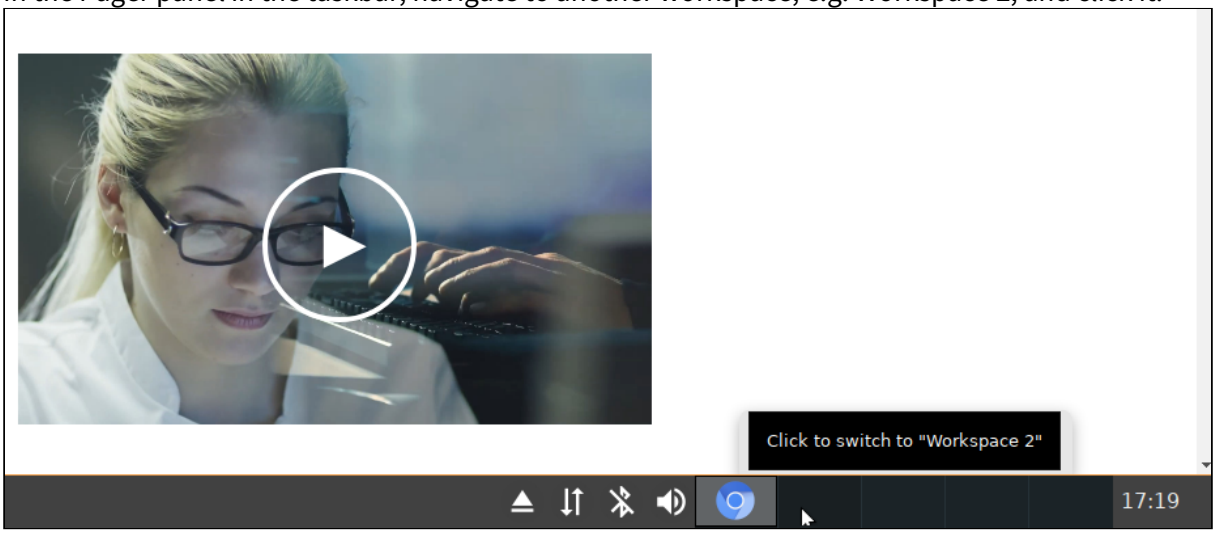
Example for how to Use the Pager

1. Start your endpoint device and launch the desired sessions / applications, e.g. Firefox and Chromium browsers.

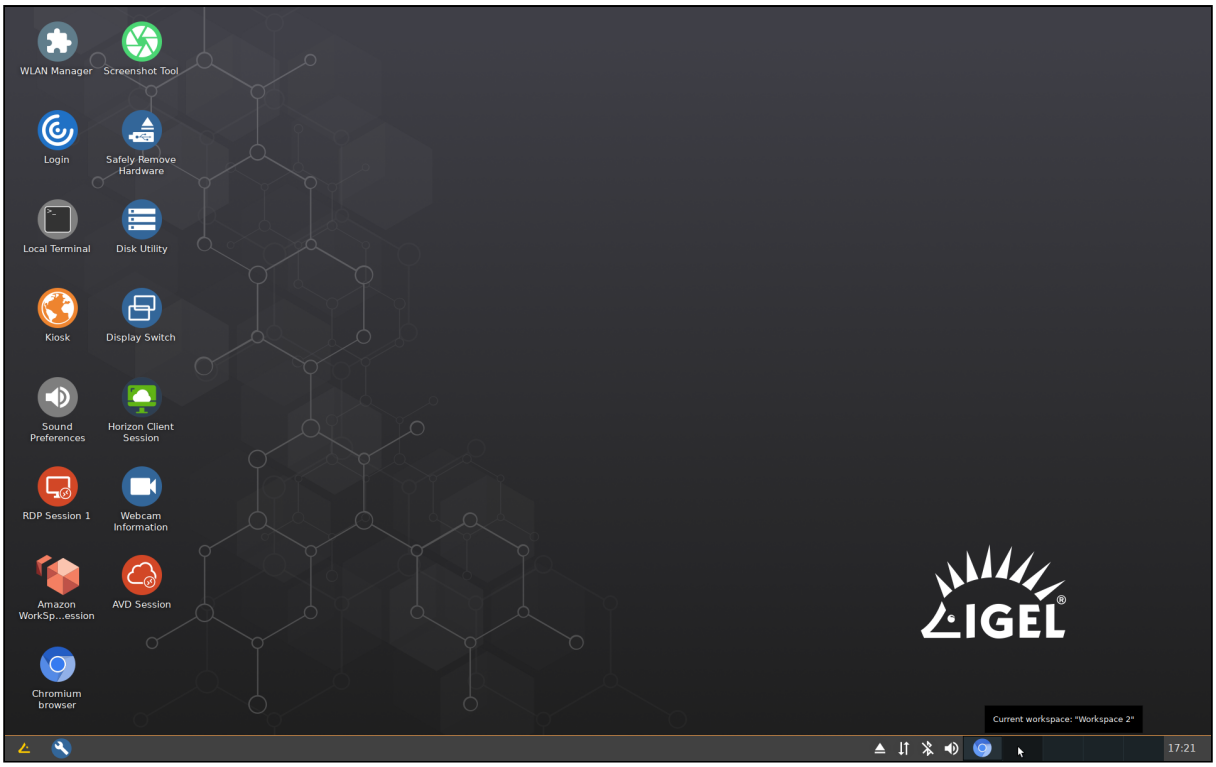
204. https://kb.igel.com/en/igel-os/11.10.270/pager-virtual-workspaces-for-organizing-the-igel-o#id-(11.10.270-en)Pager-VirtualWorkspacesforOrganizingtheIGELOSDesktop-HowToUseThePagerExampleforhowtoUsethePager



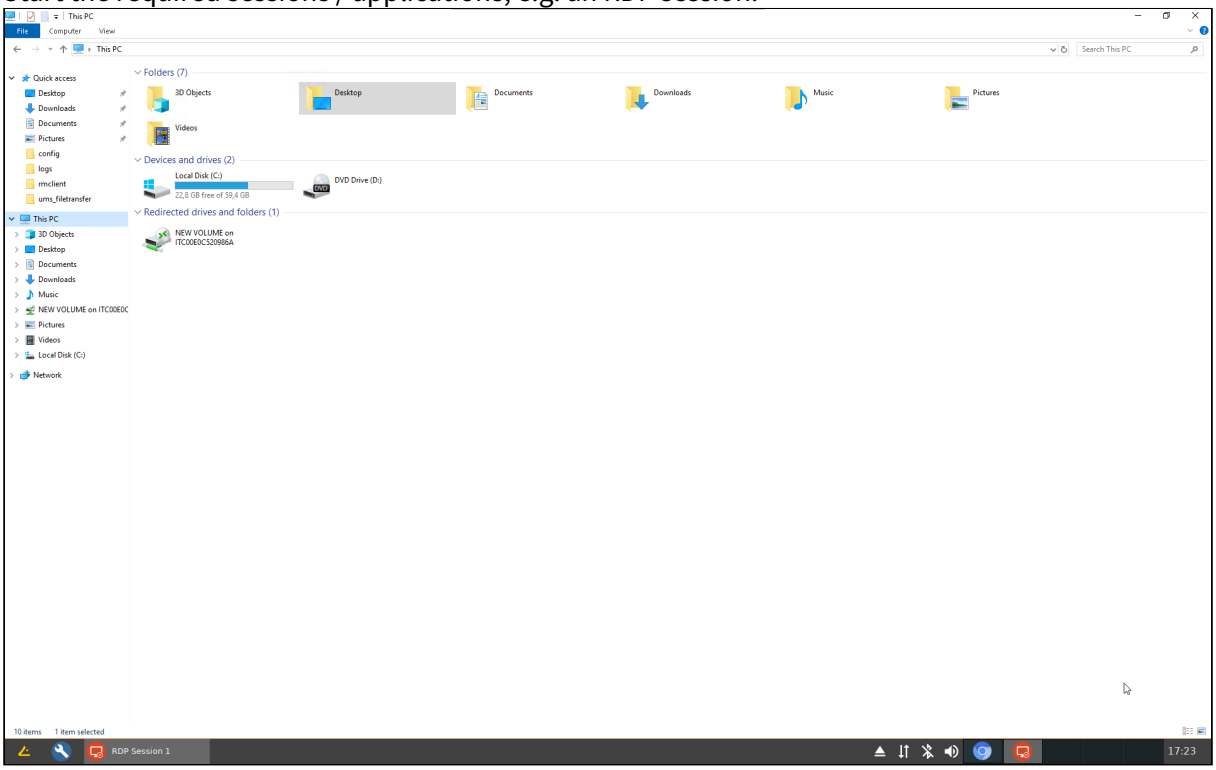
2. In the Pager panel in the taskbar, navigate to another workspace, e.g. Workspace 2, and click it.



You will see the "empty" desktop, i.e. without opened sessions / applications.



3. Start the required sessions / applications, e.g. an RDP session.



4. When you need to switch back to the Firefox and Chromium browsers, simply select the corresponding workspace (in this example, Workspace 1) in the Pager panel in the taskbar. Your desktop will be displayed exactly as before the switch to Workspace 2. Thus, you switch between your browser sessions and an RDP session without minimizing the latter.

Tip
You can use drag & drop to rearrange the sessions / applications between the workspaces: in the respective virtual desktop, click on the required application / session symbol on the left of the taskbar and drag it to the desired workspace.

*IGEL OS system default

Start Menu

Menu path: **Setup > User Interface > Desktop > Start Menu**

In this area, you can configure the desktop start menu:

Start menu type:

- **Auto**: A default setting that automatically selects the advanced or legacy type of the start menu depending on the processor. (Default)
- **Advanced**: An expanded start menu featuring a search function and a more attractive design. It requires more resources, which is particularly noticeable on slow devices.
- **Legacy**: A start menu resembles the one from Windows 95 – a list of available sessions and options.

Options in Start Menu

Select which options are to be shown in the start menu:

- **Screenlock**
- **Logout**
- **Reboot**
- **Shutdown**
- **System tab**
- **About**
- **Show current user name in About, Application Launcher and start menu**
  ☑ The current user will be shown at the top edge of the relevant window.
  ☐ The current user will not be shown.

  In order for user names to be recognized and passed on, you must configure two settings beforehand:
  - Enable Active Directory/Kerberos: **Security > Active Directory/Kerberos**
  - Enable local logon: **Security > Logon > Active Directory/Kerberos**

In-Session Control Bar

Menu path: **Setup > User Interface > Desktop > In-Session Control Bar**

In a full-screen session, the in-session control bar allows you

- to eject a USB drive,
- to start the wireless manager (only available in Appliance Mode),
- to start the Mobile Device Access USB tool (only available if the Mobile Device Access USB feature is enabled),
- to minimize the session view (not available in Appliance Mode),
- to end the session.

Use in-session control bar in all supported sessions

☑ The in-session control bar is shown. Depending on the configuration, the in-session control bar will be permanently visible or will be shown as soon as you move the cursor to the top edge of the screen.

☐ In-session control bar is not used. (default)

The in-session control bar is available for the following session types:

- **RDP** - see RDP Global (see page 1310)
- **Citrix** - see Citrix Global (see page 1248)
- **ThinLinc** - see ThinLinc Global (see page 1521)
- **NX** - see NoMachine NX Client (see page 1445)
- **Parallel 2X Client** - see Parallels Client Global (see page 1474)

To use the in-session control bar, proceed as follows:

→ To eject a USB device, click ⏏.

→ To start the wireless manager, click (only available in Appliance Mode).

→ To start the Mobile Device Access USB tool, click (only available if the Mobile Device Access USB feature is enabled).

→ To minimize the session view, click .

→ To end the session, click ✕.

→ To make the in-session control bar permanently visible, click .

Input

Menu path: **Setup > User Interface > Input**

These setup pages allow you to set the keyboard layout and other input options.

The following input devices can be set up:

- Keyboard (see page 1874)
- Additional Keyboard Layouts (see page 1875)
- Mouse (see page 1876)
- Touchpad (see page 1877)
- Touchscreen (see page 1881)
- Signature Pad (see page 1883)

Keyboard

Menu path: **User Interface > Input > Keyboard**

In this area, you can configure the keyboard.

Keyboard layout: Specify the keyboard layout. The selected layout applies to all parts of the system including emulations, window sessions and X applications.

Enable dead keys

☑ Dead keys can be used to enter special characters.

Keyboard type: Specifies the keyboard type.
Possible values:

- Default: Automatically selects the keyboard type according to the computer type (Macbook, Chromebook or PC105 for all others).
- Standard PC keyboard (105 keys)
- IBM keyboard (122 keys)
- Trimodal keyboard
- Sun Type 6 keyboard
- Chromebook
- Macbook
- Macbook international
- Thinkpad

Show indicator in taskbar

☑ Shows the language code for the keyboard in the taskbar.

Character Repeat

Repeat delay: Determines the delay (in milliseconds) before automatic repetition begins.

Repeat rate: Determines the number of times a character repeats per second.

Start with NumLock on

☑ NumLock will be enabled automatically during the boot process.

Secure keyboard input with Cherry SECURE BOARD

☑ A secure keyboard input mode will be enabled for the connected Cherry SECURE BOARD. In this mode, keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection. The standard keyboard channel will be locked, which means that keyboard input devices without the secure mode will be blocked; see https://www.cherry-world.com/cherry-secure-board-1-0.html.

Additional Keyboard Layouts

Menu path: **Setup > User Interface > Input > Additional Keyboard Layouts**

In this area, you can define additional keyboard layouts which can be selected by the user.

Enable this layout

☑ Keyboard layout is enabled and can be defined.

Keyboard layout: Selects the language for the keyboard layout.

Enable dead keys: Enable this function if the keyboard used supports dead keys for special characters.

Hotkey

☑ A hotkey allowing you to switch to this keyboard can be defined.

Key: Select a key for the key combination.

Modifier: If necessary, select an additional modifier.

Hotkey for default keyboard layout

Enable hotkey to switch to the default keyboard layout

☑ A hotkey which takes you back to the default keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.

Hotkey for next keyboard layout

Enable hotkey to switch between a number of keyboard layouts

☑ A hotkey which switches to the next keyboard layout can be defined. This is useful when a number of keyboard layouts are configured.

Further settings can be configured under On-screen Keyboard[205].

205. https://kb.igel.com/en/igel-os/11.10.250/on-screen-keyboard

Mouse

Menu path: **Setup > User Interface > Input > Mouse**

In this area, you can configure the mouse.

Lefthand mode

☑ The mouse is switched to left-handed mode.

Emulation 3 Button Mouse: Enables/disables emulation of the third (middle) mouse button for mice with only two physical buttons. This third button is emulated by pressing both buttons at the same time. If 3-button emulation was enabled, the emulation time limit determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.

Hide Cursor: The mouse pointer will be hidden after the defined time limit.

Pointer Speed: Determines the mouse resolution in counts per inch.

Double Click Interval: Changes the maximum interval in milliseconds between two consecutive mouse clicks which are to be recognized as a double-click.

Double Click Distance: Changes the maximum distance in pixels between two clicks which are to be recognized as a double-click. The object under the second click is double-clicked.

Touchpad

Here, you can configure touchpad settings for your IGEL OS devices.

Menu path: **Setup > User Interface > Input > Touchpad**

The actual settings depend on the hardware supported by the particular touchpad.

Enable Touchpad on Boot

☑ The touchpad is enabled on boot. This can be overridden by the hotkey configured below. (Default)

Hotkey

☑ Each time you press the hotkey, you toggle the touchpad on or off.

☐ No hotkey is used. (Default)

Modifiers

Modifiers for the hotkey

Key

Key for the hotkey

Custom configuration

☑ Using the following options, adapt the touchpad to your needs.

☐ No custom configuration (Default)

Tapping Mode (as of IGEL OS 11.08.290)

Switches the tapping mode on or off.
Possible values:

- **With tapping** (Default)
- **Without tapping**

Min speed

Minimum speed of the pointer in seconds. (Default: 1.00)

Max speed

Maximum speed of the pointer in seconds. (Default: 1.75)

Acceleration: Acceleration from the minimum to the maximum speed in seconds. (Default: 0.01)

The following settings apply by default:

- **Top Left Action**: No action
- **Bottom Left Action**: No action
- **Top Right Action**: Middle mouse button
- **Bottom Right Action**: Right mouse button

With some touchpads, you can assign functions to the four corners. Specify which mouse button is clicked by tapping in the relevant corner:

- No action
- Left mouse button
- Middle mouse button
- Right mouse button

Touchpad Scrolling

Define the properties for vertical and horizontal scrolling here.

Vertical

Vertical scrolling

☑ The right edge of the touchpad will be used as a vertical scrollbar. The vertical scroll speed can be set.

☐ The right edge is not enabled as a scrollbar. (default)

Vertical scroll speed: Specifies from what distance scrolling is recognized when moving in a vertical direction. (default: 25.00)

Scroll vertically with two fingers:

☑ Two-finger scrolling is enabled for vertical scrolling.

☐ Two-finger scrolling is disabled.

Horizontal

Horizontal scrolling:

☑ The bottom edge of the touchpad will be used as a horizontal scrollbar. The horizontal scroll speed can be set.

☐ The bottom edge is not enabled as a scrollbar. (default)

Horizontal scroll speed: Specifies from what distance scrolling is recognized when moving in a horizontal direction. (default: 25.00)

Scroll horizontally with two fingers:

☑ Two-finger scrolling is enabled for horizontal scrolling.

☐ Two-finger scrolling is disabled.

Touchpad Advanced

Further settings are possible here:

Corner coasting

☑ You can continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges.

Circular scrolling

☑ You can scroll in a circle. In the selection menu, specify where circular scrolling is to begin.

Circular scrolling enabled at
All Edges
Top Edge
Top Right Corner
Right Edge
Bottom Right Corner
Bottom Edge
Bottom Left Corner
Left Edge
Top Left Corner

Tap and drag gesture

☑ You can move items by tapping and dragging them.

Locked drags

☑ The tap and drag gesture ends only after an additional tap; it will otherwise end when you let go.

Palm detect

☑ Avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device.

ClickPad

☑ ClickPads are permitted. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.

Touchscreen

enu path: **Setup > User Interface > Input > Touchscreen**

Here, you can configure a touchscreen. To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected.

Enable touchscreen

☑ The touchscreen is enabled.

☐ The touchscreen is disabled. (Default)

Touchscreen type
Selects the touchscreen driver which is to be used.
Possible options:

- "EvTouch (USB)" (Default)
- "eGalax"
- "Elo Multitouch (USB)"
- "Elo Singletouch (USB)"
- "TSharc"

Touchscreen already calibrated
If you enable the touchscreen function, the touchscreen must be calibrated first.

☑ Calibration starts automatically after each system boot. (Default)

☐ Calibration does not start automatically after each system boot.

Swap X and Y values

☑ X values are interpreted as Y values and Y values as X values. Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction.

☐ X and Y values are not swapped. (Default)

Minimal X/Y value

These values are determined by the calibration tool. However, you can also change them manually. (Default: 0)

Maximal X/Y value

These values are determined by the calibration tool. However, you can also change them manually. (Default: 4000)

Untouch delay

The maximum permitted time (in milliseconds) between two instances of contact which are still registered as a single touch. When moving windows by drag & drop, for example, your contact with the screen may inadvertently be interrupted. Increasing this value prevents the thin client from recognizing two individual contacts if you let go in this way. (Default: 3)

Report delay

Determines how long (in milliseconds) the screen needs to be touched in order for the contact to be recognized. (Default: 2)

Emulate right button

☑ A right-click is generated by touching the screen for a long time.

☐ Touching the screen for a long time does not generate a right-click. (Default)

Right button timeout

Time (in milliseconds) after which a right-click is generated. (Default: 1000)

Set driver-specific defaults

Loads the preset for the driver currently selected under **Touchscreen type**. Click on this button once after changing the touchscreen type or to restore the default settings.

Multimonitor

Graphic card: Graphics card assigned to the selected touchscreen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

> If “Automatic” is set for the **Touchscreen monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

Touchscreen monitor: Assigns a monitor connection to the touchscreen. Example: **DisplayPort** (Default: Automatic)

To set up a touchscreen and on-screen keyboard, proceed as follows:

→ Enable the on-screen keyboard for the touchscreen use under **IGEL Setup > Accessories > On-Screen Keyboard**; see On-Screen Keyboard (see page 1773).

> The layout for the normal keyboard will also be used for the on-screen keyboard.

→ Calibrate the touchscreen for optimum contact recognition. The **touchscreen calibration** application can be found under **Application Launcher > System**.
In the calibration program, you will see a pattern with calibration points which must be touched one after another.

Signature Pad

Menu path: **Setup > User Interface > Input > Signature Pad**

You can connect signature pads from the following manufacturers here:

- StepOver;
- signotec.

StepOver

- **Enable StepOver TCP Client**
  ☑ The StepOver TCP Client is enabled and you can use USB signature pads from this manufacturer in sessions.
  ☐ The StepOver TCP Client is not enabled. (Default)
- **Listening TCP port**: If necessary, you can change the TCP port. (Default: 8888)

signotec

- **Enable signotec VCOM daemon**
  ☑ The signotec VCOM daemon is enabled and you can use USB signature pads from this manufacturer in sessions.
  ☐ The signotec VCOM daemon is not enabled. (Default)

See also the tip & trick Connecting Signature Pads (see page 1056).

Hotkeys

Menu path: **Setup > User Interface > Hotkeys > Commands**

In order to make it easier to use your thin client, hotkeys are available for frequent operating routines. A hotkey is a combination of one or more modifiers and an alphanumeric key.

You can enable or disable hotkeys and change the keys used. For more information, see Commands 1 (see page 1885).

_____

- Commands (see page 1885)

Commands

Menu path: **Setup > User Interface > Hotkeys > Commands**

You can activate, deactivate and change the hotkeys that are available to the user.

Settings in the Dialog

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Available Hotkeys and their Default Settings

Hide all windows and show desktop
Default:

- activated
- **Modifiers**: `Ctrl|Mod4`
- **Key**: `d`
- **Appliance Mode Access**: deactivated

Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions
Default:

- deactivated
- **Modifiers**: `Ctrl|Alt + End`
- **Key**: `End`
- **Appliance Mode Access**: deactivated

Open start menu
Default:

- deactivated
- **Modifiers**: `Shift + Super`
- **Key**: `Super_L`
- **Appliance Mode Access**: deactivated

Open start menu (alternative):
Default:

- deactivated
- **Modifiers**: `Shift + Super`
- **Key**: `Super_L`
- **Appliance Mode Access**: deactivated

Screenshot of active window
Default:

- deactivated
- **Modifiers**: `Ctrl|Alt`
- **Key**: `Print`

- **Appliance Mode Access**: deactivated

Screenshot of entire screen
Default:

- deactivated
- **Modifiers**: `Ctrl|Shift`
- **Key**: `Print`

Switch between active windows using Task Switcher
Default:

- activated
- **Modifiers**: `Ctrl|Alt`
- **Key**: Tab
- **Appliance Mode Access**: deactivated

Switch between active windows using Task Switcher (backwards)
Default:

- activated
- **Modifiers**: `Ctrl|Alt|Shift`
- **Key**: Tab
- **Appliance Mode Access**: deactivated

Switch focus to next window
Default:

- activated
- **Modifiers**: `Ctrl`
- **Key**: `Escape`
- **Appliance Mode Access**: deactivated

Switch focus to next window (alternative)
Default:

- activated
- **Modifiers**: `Ctrl|Alt`
- **Key**: `Up`
- **Appliance Mode Access**: deactivated

Switch focus to next window (reverse order)
Default:

- activated
- **Modifiers**: `Ctrl|Alt`
- **Key**: `Down`
- **Appliance Mode Access**: deactivated

Volume down (multimedia key)
Default:

- activated
- **Modifiers**: (none)
- **Key**: `XF86AudioLowerVolume`

Volume mute (multimedia key)
Default:

- activated
- **Modifiers**: (none)
- **Key**: `XF86AudioMute`
- **Appliance Mode Access**: deactivated

Volume up (multimedia key)
Default:

- activated
- **Modifiers**: (none)
- **Key**: `XF86AudioRaiseVolume`
- **Appliance Mode Access**: deactivated

Display Settings in IGEL OS

The following article describes the **Display** settings in IGEL OS, which you will require when configuring your monitors. Take notice that a successful and correct display configuration depends, however, on many factors. For example, cables, current driver / firmware versions, BIOS settings, etc. can influence your screen configuration and, thus, have to be considered when setting up the monitor environment.

For a quick display configuration, you can use also the Display Switch (see page 1730) function.

If you work in an environment with multiple monitors, see also the how-to article https://kb.igel.com/en/igel-os/11.10.270/multimonitor .

If you use the Shared Workplace (SWP)[206] feature with user-specific display resolutions, see https://kb.igel.com/en/igel-os/11.10.270/display-configuration-for-shared-workplace-swp .

Menu path: **User Interface > Display**

Screen Configuration

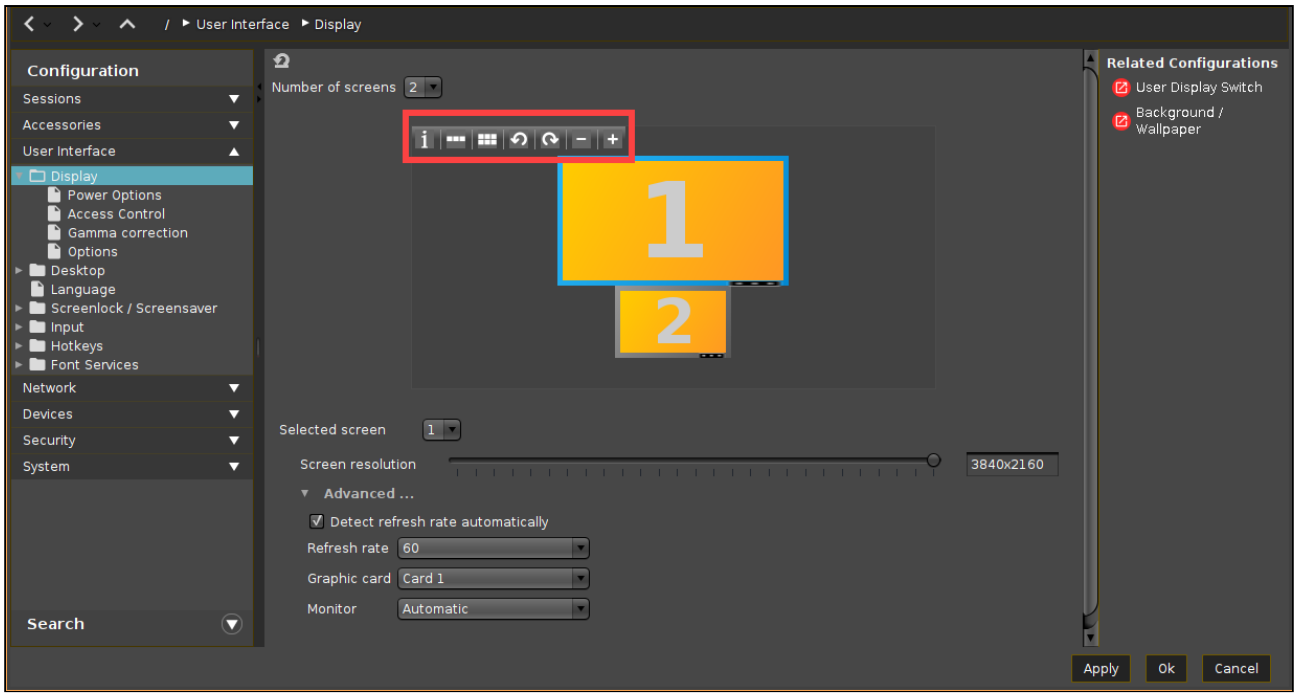
⚠ Always try the configuration locally before applying it to multiple devices via a profile: A faulty display configuration can cause your GUI to become unstable and lead to a black screen.
If you face a black screen problem because of the wrong display configuration, select one of the following recovery options:

- In the UMS: Edit the display configuration via **Devices > [device name] > [device's context menu] > Edit Configuration** or via a new profile.
  OR
- On the endpoint device: Restart the device and select **Emergency boot (setup only)** during the boot procedure, see Boot Menu (see page 1220) and Emergency Boot (see page 1223). In the Setup, you can then change the display configuration.

Every screen connected to the endpoint device can be configured independently. The position of the individual screens can be determined in relation to Screen 1.

→ Click on to show the screen identifier on each device. appears only locally on the device, not in the UMS.

206. https://kb.igel.com/en/universal-management-suite/current/igel-shared-workplace-swp



Number of screens

Select how many monitors you would like to use.

	Identifies each screen connected and shows the connection and display resolution for each screen. This function is available only locally on the device. It is not accessible from the UMS.
	Arranges the screens in a single row.
	Arranges the screens in two rows.
	Rotates the selected screen anti-clockwise.
	Rotates the selected screen clockwise.

	Removes the screen which was last added.
	Adds a screen.

The selected screen is highlighted with a blue frame. The black bar at the bottom edge of the screen represents the physical orientation of the monitor.

Configuring a vertically centered display layout, which may be required, for example, in the case of a primary monitor (top) and a touchscreen panel (bottom), is not possible if **Screen resolution** is set to "**Autodetect**". In this case, **Screen resolution** must be specified manually.

Selected screen

Selects a screen using this selection box to configure the following settings.

Screen resolution

Move the slider to the resolution which the selected screen is to have. The resolution is shown in the right-hand box.

You have the option of defining your own resolutions via the registry key `x.xserver0.custom_resolution`. In order for the values set there to take effect, the resolution must be set to "**Autodetect**" (slider at the far left). The following parameters apply to the entry in the registry:

- `WxH` : W = width, H = height (example: 1920x1080)
- `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

Be careful when changing resolutions manually. Excessively high resolutions can cause a black screen.

For details of the display resolution supported by your IGEL device, please see the relevant datasheet on igel.com[207] or in the datasheet archive for legacy IGEL devices[208].
Detailed instructions on MST configuration for UD3 and UD7, see:

- UD3 Model M350C: Multistream Transport[209]
- UD7 Model H860C: Multistream Transport Monitor Daisy Chaining[210]

Advanced...

Detect refresh rate automatically

☑ A refresh rate for the monitor is identified automatically.*
☐ A refresh rate for the monitor is to be set manually.

Refresh rate

Number of individual images per second.

Possible values:

- 30 ... 100. (Default: 60)

Be careful when changing the refresh rate manually since the faulty configuration can cause a black screen.

207. https://www.igel.com/igel-solution-family/igel-endpoint-hardware/
208. https://kb.igel.com/knowledge-base-archive/current/datasheet-archive
209. https://kb.igel.com/hardware/current/ud3-model-m350c-multistream-transport
210. https://kb.igel.com/hardware/current/ud7-model-h860c-multistream-transport-mst-monitor-

Graphic card

Graphics card assigned to the selected screen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

> If **Automatic** is set for the **Monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

Monitor

Assigns the screen selected under **Selected screen** to a monitor connection. Example: **HDMI(II)**. (Default: Automatic)

- Power Options (see page 1894)
- Access Control of the Display in IGEL OS (see page 1895)
- Gamma Correction in IGEL OS (see page 1896)
- Options (see page 1897)

*IGEL OS system default

Power Options

Menu path: **Setup > User Interface > Screen > Power Options**

In this area, you can handle display power management.

Please note: Your screen must support *Display power management signaling (DPMS)*.

- **Handle Display Power Management**
  ☑ The DPMS energy saving functions are enabled.

→ Specify separately for battery and mains operation the number of minutes before the screen switches to a specific energy-saving mode:
Three different modes are offered:

- **Standby Time** (standby mode)
- **Suspend Time** (sleep mode)
- **Off Time** (Off)

If a device is switched on but not used for some time, energy can also be saved by **Brightness Reduction**.

→ Specify by how many percent the brightness of the screen is to be reduced and how long the period of inactivity before brightness reduction should be. Values between 10 seconds and two minutes are available to choose from.

> Naturally, all stages are gone through only if the X-Server does not receive any new entries during this period.

Access Control of the Display in IGEL OS

Menu path: **Setup > User Interface > Screen > Access Control**

In this area, you can control access to the screen. Thin client access control is enabled by default.

Disable console switching

☑ Access to your terminal screen is possible from any UNIX host. You can no longer access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12].

☐ You can access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12]. (default)

Access Control

☑ Access to this display from other computers will be controlled. This access control is enabled by default. (default)

Disable TCP connections

☐ All TCP connections to the display are prohibited. Only local applications are displayed. The xhost mechanism no longer functions.
This parameter is ignored if XDMCP is configured.

Fixed X-Key

☑ You can grant specific users permanent remote access to the thin client:

1. Click on **Calculate**.
   A 32-digit key will appear in the **X-Key** field.
2. Enter this key in the Xauthority file on the user's computer.

List of trusted X hosts

Here, you can approve specific computers for console access:

1. Click on the **Add** button to open the entry mask.
2. Give the name of the remote host (not the IP address) you would like to add.
3. Confirm this by clicking **OK**.
   The computer will be entered in the list.

Gamma Correction in IGEL OS

Menu path: **Setup > User Interface > Screen > Gamma Correction**

In this area, you can increase or decrease the various brightness ranges in order to adjust the display on your screen to your preferences.

- **Selected screen**: Select the screen whose brightness you would like to adjust (default: First Screen).

You can then change the gamma values for red, green and blue. The scale ranges from 0.10 (dark) to 10 (light) and is set to 1.00 by default.

- **Gamma value Red**: Changes the brightness curve for the red color portion.
- **Gamma value Green**: Changes the brightness curve for the green color portion.
- **Gamma value Blue**: Changes the brightness curve for the blue color portion.
- **Link Sliders**
  ☑ All sliders are moved equally in order to change the brightness harmoniously. (default)
  ☐ Each slider can be moved individually. This way, you can also change the color ratio.

Options

Menu path: **Setup > User Interface > Screen > Options**

Configure the options for the display here:

- **Monitor probing (DDC)**
  ☑ You can share information between the system and the screen via the Display Data Channel. DDC is enabled by default and the native resolution supported by the screen is determined automatically. (default)
  ☐ Screen properties are not automatically detected.
- **Monitor DPI detection**: Defines how the DPI value should be determined.
  Possible options:
  - Off: The DPI value is defined by **Monitor DPI**. There is no automatic detection.
  - Smart: The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. The DPI value is set to either 96, 125, 150, 175, 200, 225, 250, 275 or 300, depending on which value is closest to the value calculated based on the monitor resolution. (Default)
  - Pixel-Precise: The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. Unlike the "Smart" option, the value calculated based on the monitor resolution is used directly.
- **Monitor DPI**: Enter the DPI resolution (dots per inch) for your monitor (default: 96). This parameter is only available if **Monitor DPI detection** is set to "Off".
- **Color Depth**: Selects the desktop color depth.
  The following options are available:
  - True Color (24) (Default)
  - True Color (32)

Make sure that all screens connected to the thin client support the color setting.

Network

In this area, you can configure network connections of the endpoint device.

- LAN Interfaces (see page 1899)
- Mobile Broadband (see page 1918)
- Routing (see page 1920)
- Hosts (see page 1922)
- Network Drives (see page 1923)
- Proxy (see page 1928)
- VPN (see page 1929)
- DHCP Client (see page 1959)
- SCEP Client (NDES) (see page 1962)

LAN Interfaces

Menu path: **Setup > Network > LAN Interfaces**

Here, you can configure the LAN interfaces.

Predictable Network Interface Names (PNINs)
As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[211]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump (see page 627)
  - **Bind interface** under **Security > Smartcard > Services**, see Services (see page 2025)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
  To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate default interface (Ethernet)

☑ The default interface is enabled. (Default)

☐ The Ethernet interface is not enabled.

Get IP from the DHCP server: The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under DHCP Client (see page 1959).

Specify an IP address: The IP address and the network mask are entered manually.

IP address: IP address of the device.

Network mask: Network mask of the device.

Default gateway: IP address of the default gateway.

211. https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

Enable

☑ Routing via the default gateway is enabled.

☐ Routing via the default gateway is not enabled. (Default)

Terminal name: Local name of the device. If the field is empty, the default name combined of '`ITC`' with a MAC address will be generated.

Enable DNS

☑ The manual DNS configuration will be used.

☐ The DNS configuration will be carried out by DHCP or BOOTP. (Default)

Default domain: Usually the name of the local network.

Name server: IP address of the name server to be used.

Name server: IP address of an alternative name server.

Manually overwrite DHCP settings

☑ The default route, the domain name, and the DNS server will be overwritten by manual entries.

☐ Manual entries will not overwrite DHCP settings. (Default)

Dynamic DNS registration:

☑ The terminal name will be registered dynamically via the DNS or DHCP server.

☐ The terminal name will not be registered dynamically. (Default)

Dynamic DNS registration method

- DHCP: Updates the terminal name through DHCP option 81.
- DNS: Sends updates to the DNS server in accordance with RFC 2136.

TSIG key file for additional DNS authentication: Path to the private key if TSIG-based DDNS registration is used.

- Individual Interface (see page 1901)
- Wireless (see page 1907)

Individual Interface

Menu path: **Setup > Network > LAN Interfaces > [Interface]**

Predictable Network Interface Names (PNINs)
As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[212]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump (see page 627)
  - **Bind interface** under **Security > Smartcard > Services**, see Services (see page 2025)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
  To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate default interface (Ethernet)

☑ The default interface will be enabled. (Default)

☐ The Ethernet interface will not be enabled.

Get IP from DHCP server

☑ The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under DHCP Client (see page 1959).

Specify an IP address: The IP address and the network mask are entered manually.

IP address: IP address of the device.

Network mask: Network mask of the device.

IPv6 Configuration

212. https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

- Compatibility mode: Behavior of earlier firmware versions.
- Disabled: IPv6 completely disabled.
- Automatic: IPv6 auto configuration based on router advertisements (can include DHCPv6). For further information, see RFC 4861.[213]
- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available. This is mentioned in RFC 4862 Section 5.5.2.[214]

Network link type

- Auto sense
- 1000 Mb/s full duplex
- 100 Mb/s full duplex
- 100 Mb/s half duplex
- 10 Mb/s full duplex
- 10 Mb/s half duplex

Force auto-negotiation

☑ With this option, problems with half/full duplex for specific switches that expect the auto-negotiation flag for fixed bandwidths can be addressed.

☐ Automatic negotiation will not be forced. (Default)

Enable tray icon

☑ A tray icon for the network interface will be shown. (Default)

Enable context menu

☑ A context menu will be shown when you click on the tray icon. (Default)

Enable network info dialog

☑ A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

- Authentication of the Network Port in IGEL OS (see page 1903)
- Configuring Wake-on-LAN on IGEL OS Devices (see page 1905)

213. https://tools.ietf.org/html/rfc4861
214. https://tools.ietf.org/html/rfc4862#section-5.5.2

Authentication of the Network Port in IGEL OS

Menu path: **Setup > Network > LAN Interfaces > [Interface] > Authentication**

Here, you can enable and configure network port authentication.

Enable IEEE-802.1x authentication

☑ Network port authentication is enabled.

☐ Network port authentication is not enabled. (Default)

If you enable authentication, further options are available:

EAP type: Here, you can select the authentication procedure:

- PEAP: Protected Extensible Authentication Protocol
- TLS: Transport Layer Security with client certificate
- TTLS: Tunneled Transport Layer Security
- FAST: Flexible Authentication via Secure Tunneling

Anonymous identity: This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

Auth method: The following authentication methods are available:

- MSCHAPV2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

Validate server certificate

☑ The server's certificate is checked cryptographically. (Default)

CA Root certificate: The path to the CA root certificate file. This can be in PEM or DER format.

Identity: User name for RADIUS

Password: Password for network access

> If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

The following settings are relevant if you have selected "TLS" as **EAP type**:

Manage certificates with SCEP (NDES)

☑ Client certificates will automatically be managed with SCEP Client (NDES) (see page 1962).

☐ Client certificates will not be managed with SCEP Client (NDES) (see page 1962). (Default)

Client certificate: Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

If a private key in the PKCS#12 format is used, leave this field empty.

Private key: Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

Identity: User name for network access

Private key password: Password for the **Private key** for the client certificate

The following setting is relevant if you have selected "FAST" as **EAP type**:

Automatic PAC provisioning: Specifies how the PAC (Protected Access Credential) is delivered to the client. Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.
- "unrestricted": Both authenticated and unauthenticated PAC provisioning is allowed. PAC files are automatically created after the first successful authentication.

PAC files are stored in `/wfs/eap_fast_pacs/`.
PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

In tests with `hostapd`, it has been necessary to disable TLS 1.2. To do that, enter the following command for **System > Registry > network.interfaces.ethernet.device%.ieee8021x.phase1_direct**: `tls_disable_tlsv1_2=1`

Configuring Wake-on-LAN on IGEL OS Devices

With Wake-on-Lan (WoL), you can switch on devices over the network. On this configuration page, you can select the packets or messages with which the endpoint device can be started.

For further information on the WoL functionality of the Universal Management Suite (UMS), see Wake-on-LAN[215].

> IGEL OS 11.08.290 or higher: WOL Setting in BIOS is Detected on Supported Lenovo Devices:
>
> On Lenovo devices that are supported by IGEL OS 11, the system can detect whether WoL is enabled in the BIOS or not. If the system detects that WoL is disabled in the BIOS, all WoL described on this configuration page is disabled.
> You can enable or disable the WoL detection with **System > Registry > network > interfaces > respect_bios_wol_setting** (registry key `network.interfaces.respect_bios_wol_setting`).

Menu path: **Network > LAN Interfaces > [Interface] > Wake-On-LAN**

Wake on magic packet

☑ The device can be started with a Wake-on-LAN magic packet. (Default)

Wake on ARP packet

☑ The device can be started with a Wake on ARP packet.

☐ The device cannot be started with a Wake on ARP packet. (Default)

Wake on broadcast message

☑ The device can be started with a Wake on broadcast message.

☐ The device cannot be started with a Wake on broadcast message. (Default)

Wake on multicast message

☑ The device can be started with a Wake on multicast message.

☐ The device cannot be started with a Wake on multicast message. (Default)

Wake on physical activity

☑ The device can be started with a physical activity.

☐ The device cannot be started with a physical activity. (Default)

Wake on unicast message

215. https://kb.igel.com/knowledge-base-archive/current/

☑ The device can be started with a Wake on unicast message.

☐ The device cannot be started with a Wake on unicast message. (Default)

Wireless

Menu path: **Setup > Network > LAN Interfaces > Wireless**

In this area, you can configure everything relating to your wireless connections.

Configure the Wireless Regulatory Domain (see page 1917) to ensure that your device meets the local regulations for wireless equipment.

You will find details of compatible wireless hardware in the IGEL Linux 3rd Party Hardware Database[216].

Predictable Network Interface Names (PNINs)
As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[217]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump (see page 627)
  - **Bind interface** under **Security > Smartcard > Services**, see Services (see page 2025)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
  To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate wireless interface

☑ The default interface is enabled.

☐ The wireless interface is not enabled. (Default)

Get IP from DHCP server: The IP address of the endpoint device will be obtained automatically using DHCP. (Default)

216. https://www.igel.com/linux-3rd-party-hardware-database/
217. https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

DHCP options can be specified under DHCP Client (see page 1959).

Specify IP address: The IP address and the network mask are entered manually

IP address: IP address of the endpoint device

Network mask: Network mask of the endpoint device

IPv6 configuration:

- Compatibility mode: Behavior of earlier firmware versions
- Disabled: IPv6 is completely disabled.
- Automatic: IPv6 auto-configuration is based on router advertisements (can include DHCPv6). You will find further information in RFC 4861[218].
- DHCPv6: IPv6 configuration using DHCPv6 if router advertisements are not available. You will find further information in RFC 4862 Section 5.5.2[219].

Enable tray icon

☑ A tray icon for the wireless interface will be shown. (Default)

Enable context menu

☑ A context menu will be shown when you click on the tray icon. (Default)

Enable network info dialog

☑ A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

Enable Wireless Manager

☑ The Wireless Manager (see page 1910) is enabled. This tool allows the user to establish a connection to a wireless network quickly.

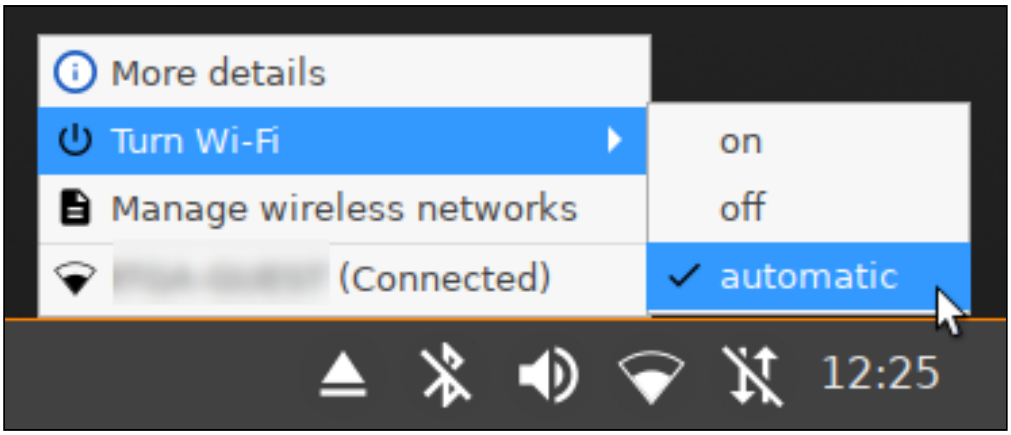
☐ The Wireless Manager is disabled. (Default)

Enable Wi-Fi automatic switch

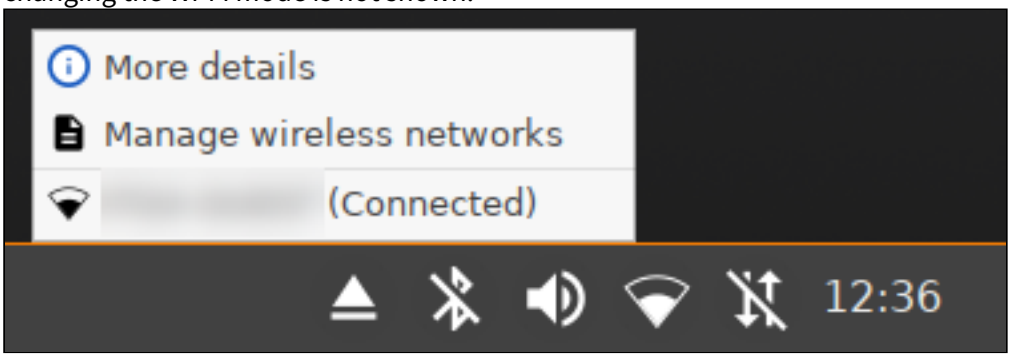
☑ When a device is disconnected from the network cable, Wi-Fi is automatically turned on. When the device is connected again to the network cable, Wi-Fi is automatically turned off.

- If the registry key **System > Registry > network.applet.wireless.enable_wifi_switch** (see Switch for the Wi-Fi Connection (see page 1912)) is enabled, automatic mode is added to the Wi-Fi switch.

218. https://tools.ietf.org/html/rfc4861
219. https://tools.ietf.org/html/rfc4862#section-5.5.2



- If the registry key **System > Registry > network.applet.wireless.enable_wifi_switch** is disabled, Wi-Fi automatic switch functionality will work in the background. The option for changing the Wi-Fi mode is not shown.



☐ An automatic connection to a wireless network is disabled. (Default)

If you use wireless regularly, it is recommended to enable the following options: **Enable tray icon**, **Enable context menu**, and **Enable Wireless Manager**. Via the **Wireless Manager**, you can use Café Wireless (Wi-Fi) (see page 2173).
If you have to frequently switch between LAN and WLAN networks, it is also useful to activate **Enable Wi-Fi automatic switch**.

- Wireless Manager (see page 1910)
- Switch for the Wi-Fi Connection (see page 1912)
- Default Wi-Fi Network in IGEL OS (see page 1913)
- Additional Wi-Fi Networks (see page 1916)
- Wireless Regulatory Domain (see page 1917)

Wireless Manager

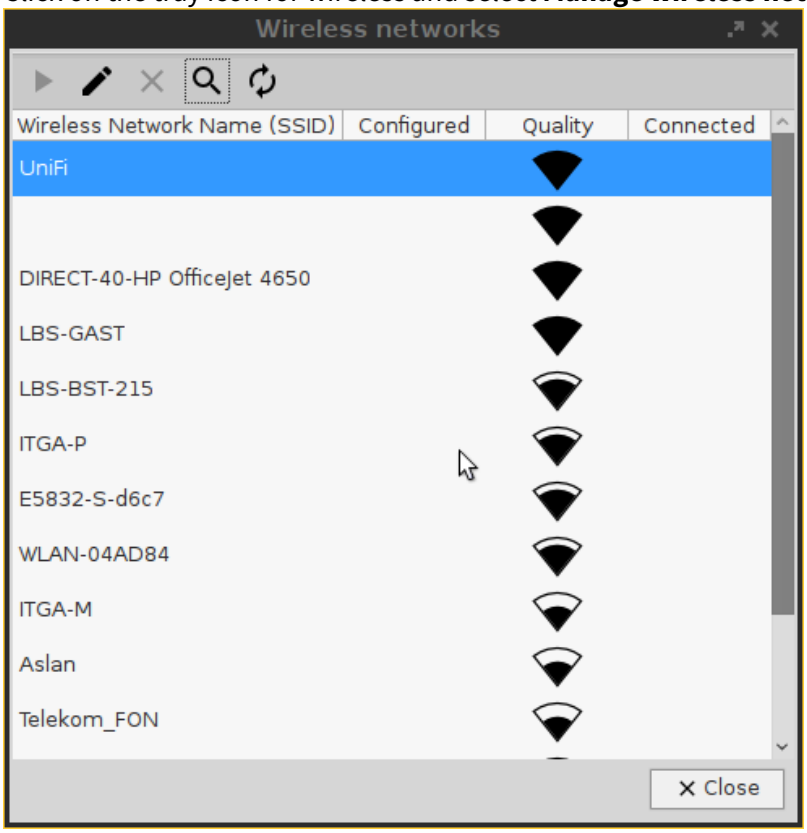
The Wireless Manager tool allows the user to connect quickly to available wireless networks.

> The Wireless Manager can be enabled under **Network > LAN Interfaces > Wireless.**

You can bring up the Wireless Manager from the tray icon for wireless:

See also How to Launch the Wireless Manager within IGEL OS when the Taskbar Is Hidden (see page 639).

1. Click on the tray icon for wireless and select **Manage wireless networks** from the context menu.



2. Search for available networks.
   - The list of active networks is sorted according to the quality of their signal strength.
   - Previously configured connections are flagged with a tick in the **Configured** column.
   - The connection currently active is likewise flagged with a symbol under **Connected**.
3. Double-click on a network in the list in order to open the entry mask.
   You can either **permanently save** the logon information or enter it each time you establish a connection to this network.

> Click on the key symbol in order to display the key phrase while you are typing.

4. Click on the **Connect network** button in order to establish the previously configured connection:
   The tray icon will change to show the connection quality.
   Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button.
   In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

   > If you have configured the available connections, you will no longer need the Wireless Manager in order to establish a connection.

   In the context menu for the tray icon, all available networks are listed and can be brought up from here.
5. The IGEL Setup shows all connections configured by the local user under **Network > LAN Interfaces > Wireless > Additonal Wi-Fi Networks**.

See also Café Wireless (Wi-Fi) (see page 2173).

Switch for the Wi-Fi Connection

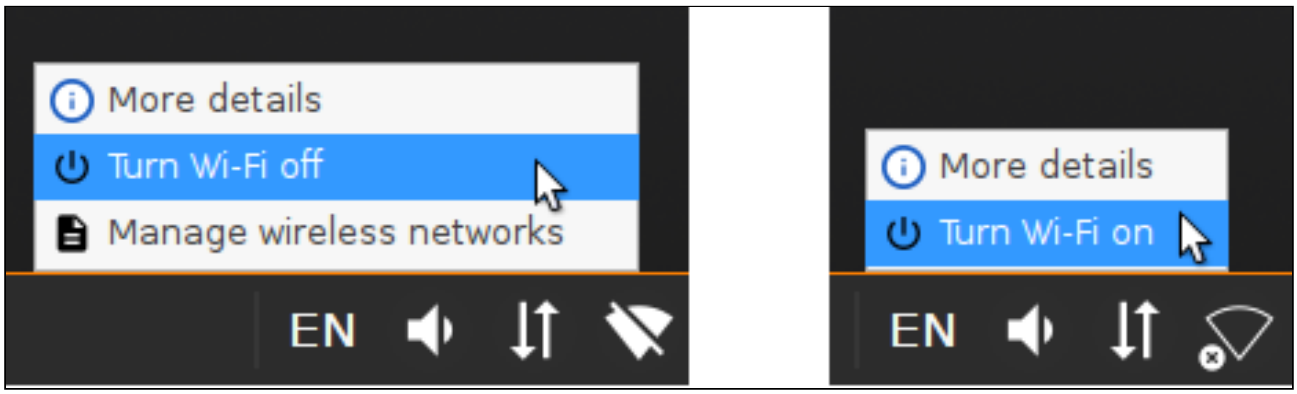
You can turn Wi-Fi off or on.

To use the switch for the Wi-Fi connection, **Enable Wi-Fi switch** under **Setup > System > Registry > Parameter > network > applet > wireless > enable_wifi_switch** must be activated. (Default)

Turning Wi-Fi Off or On

If You Are Logged In

->Select **Turn Wi-Fi off** / **Turn Wi-Fi on** from the context menu of the Wi-Fi tray icon.



If the Login Dialog Is Displayed or the Screen Is Locked

->To turn Wi-Fi off, click the tray icon and select **OK** in the **Turn Wi-Fi off** dialog. If the Wireless Manager (see page 1910) is activated, you can also use there the button .

->To turn Wi-Fi on, click and select **OK** in the **Turn Wi-Fi on** dialog.

Default Wi-Fi Network in IGEL OS

Menu path: **Setup > Network > LAN Interfaces > Wireless > Default Wi-Fi network**

Here, you can configure wireless network connections.

Disable Encryption: No encryption will be used. (Default)

Enable WEP Encryption: WEP encryption will be used.

Enable WPA Encryption: WPA encryption will be used.

> You will need to give further information depending on the encryption method chosen.

Wireless Network Name (SSID): Name of the wireless network (SSID)

For WEP Encryption

Transmit key ID: Choose from a maximum of four configurable keys. (Default: 1)

Key Format:

- ASCII
- Hexadecimal

Key [1-4]: Enter the key here.

> Characters to be entered for WEP keys:
> - For 64-bit encryption, 5 characters (ASCII) or 10 hex digits (hexadecimal)
> - For 128-bit encryption, 13 characters (ASCII) or 26 hex digits (hexadecimal)

For WPA/WPA2/WPA3 Personal Encryption

Network authentication

- WPA Personal: Wi-Fi Protected Access Pre-Shared Key (WPA / IEEE 802.11i/D3.0)
- WPA2 Personal: Wi-Fi Protected Access Pre-Shared Key (WPA2 / IEEE 802.11i/RSN)
- WPA3 Personal: Wi-Fi Protected Access SAE (Simultaneous Authentication of Equals)

Network key: WPA network key/passphrase as set at the dial-in point. This is either an ASCII character string with a length of 8...63 or exactly 64 hexadecimal digits.

Data encryption:

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.

- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

AP Scan mode: Scan mode for access points

- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

For WPA/WPA2 Enterprise Encryption

Network authentication:

- WPA Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
- WPA2 Enterprise: Wi-Fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)

Data encryption:

- Default: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2.
- TKIP: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- AES (CCMP): AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- AES (CCMP) + TKIP: One of two encryption methods is selected by the access point.
- Automatic: The access point can choose the encryption method freely – nothing is stipulated.

AP Scan mode: Scan mode for access points

- Default
- Broadcast: Alternative for access points which allow the SSID broadcast
- No broadcast: Alternative for access points which refuse the SSID broadcast (hidden access points)

EAP Type

- PEAP: Protected Extensible Authentication Protocol
- TLS: Transport Layer Security with client certificate
- TTLS: Tunneled Transport Layer Security
- FAST: Flexible Authentication via Secure Tunneling

Anonymous identity: This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP types**, except for "TLS".

Auth Method: Method for authentification that is available for the selected EAP type
Possible options:

- MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol
- TLS: Transport Layer Security with client certificate
- GTC: Generic Token Card
- MD5: MD5-Challenge
- PAP: Password Authentication Protocol

Validate Server Certificate

☑ The endpoint device validates the authenticity of the authentification server against the certificate file. This certificate file is stored under the path defined by **CA Root Certificate**.

☐ The authenticity of the authentification server is not validated.

CA Root Certificate: Path and file name of the file that contains the certificates with which the authentification server authenticates itself.

Identity: User name that is stored at the authentification server

Password: Password relevant to the user name

The following settings are relevant if you have selected "TLS" as **EAP type**:

Manage certificates with SCEP (NDES)

☑ Client certificates will automatically be managed with SCEP Client (NDES) (see page 1962).

☐ Client certificates will not be managed with SCEP Client (NDES) (see page 1962). (Default)

Client certificate: Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

> If a private key in the PKCS#12 format is used, leave this field empty.

Private key: Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PFX format. The **Private key password** may be required for access.

Identity: User name for network access

Private key password: Password for the **Private key** for the client certificate

Learn more from the how-to Using WPA Enterprise / WPA2 Enterprise with TLS Client Certificates (see page 618).

The following setting is relevant if you have selected "FAST" as **EAP type**:

Automatic PAC provisioning: Specifies how the PAC (Protected Access Credential) is delivered to the client. Possible options:

- "disabled": PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- "unauthenticated": An anonymous tunnel will be used for PAC provisioning.
- "authenticated": An authenticated tunnel will be used for PAC provisioning.
- "unrestricted": Both authenticated and unauthenticated PAC provisioning is allowed. PAC files are automatically created after the first successful authentication.

> PAC files are stored in `/wfs/eap_fast_pacs/` .
> PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

> In tests with `hostapd` , it has been necessary to disable TLS 1.2. To do that, enter the command `tls_disable_tlsv1_2=1` for the following registry keys:
>
> - **System > Registry > network.interfaces.wirelesslan.device0.wpa.phase1_direct**
> - **System > Registry > network.interfaces.wirelesslan.device0.alt_ssid%.wpa.phase1_direct**

Additional Wi-Fi Networks

Menu path: **Setup > Network > LAN Interfaces > Wireless > Additional Wi-Fi Networks**

You can add other wireless networks here. The settings options per wireless network correspond to those for the Default Wi-Fi Network.

To edit the wireless network list, proceed as follows:

->Click to create a new entry.

->Click to remove the selected entry.

->Click to edit the selected entry.

->Click to copy the selected entry.

Wireless Regulatory Domain

Menu path: **Setup > Network > LAN Interfaces > Wireless > Wireless Regulatory Domain**

This page allows you to set the wireless device in accordance with local regulations.

Wireless regulatory domains: Select the area in which the device is located.

- Not configured
- Africa
- Arctic
- Asia
- Australia
- Europe
- North America
- South America
- World

Location: Select the country in which the device is located.

- Not configured
- Albania
- Armenia
  [...]
- Cyprus
- Austria

The list below sets out the technical requirements for the selected location for your information.

Mobile Broadband

Menu path: **Setup > Network > Mobile Broadband Network**

Here, you can change the settings for a modem or a surf stick. This function is available from IGEL Linux *Version 10.03.100*.

Ensure that data traffic is adequately secured. You can do this in the following ways:
- Use a private APN.
- Use OpenVPN and block traffic that would circumvent VPN with firewall rules.

If the device is already inserted and has been configured, the network connection will be established after the thin client boots. It can take between a few seconds and around 1 minute to establish a connection. The network connection will remain in place until the surf stick is removed or the thin client is put on standby or shut down.

The status of the network connection is shown in the system tray:

- The network connection is established; the device is online This symbol is only shown if “Modem” is selected as the device type. If "Router” is selected as the device type, the symbol for a LAN connection will be shown.
- The network connection was interrupted; the device is offline This symbol is only shown if “Modem” is selected as the device type. If "Router” is selected as the device type, the corresponding symbol for a LAN connection will be shown.

You can change the following settings:

- **Enable mobile broadband**
  ☑ The mobile broadband network can be used if a supported modem is connected.
  ☐ The mobile broadband network cannot be used. (default)
- **Device type**
  Possible options:
  - Modem: The device will be operated as a modem. The access data can be changed with the parameters **number**, **user name**, **password**, **APN**, **network ID** and **PIN**.
  - Router: The device will be operated as a router. The device must be configured in advance in such a way that it is ready for use when it is inserted.

Select the "Router” device type if you use a device from Huawei in the HiLink mode; example: Huawei E3372.

- **Number**: Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.
- **User name**: User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.
- **Password**: Password for your network connection. If you do not know the password, ask your mobile communications operator for it.

- **APN**: APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.
- **Network ID**: Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.
- **PIN**: PIN for the SIM card used.
- **Enable tray icon**

  ☑ The current status of the network connection is shown with the symbol or .
  ☐ The current status of the network connection is not shown with a symbol.
- **Enable context menu**

  ☑ If you click on or , a context menu can be opened.
  ☐ No context menu can be opened.
- **Enable network info dialog**
  ☑ Via the context menu, you can bring up detailed information regarding the network connection.
  ☐ No detailed information regarding the network connection can be brought up.
- **Enable mobile broadband configuration dialog**
  ☑ Via the context menu, you can open a configuration dialog in order to change the access data.
  ☐ The configuration dialog cannot be opened.

Routing

Menu path: **Setup > Network > Routing**

Here, you can enter additional routes if necessary.

Enable: (default: disabled)

☑ Routing is enabled.

Default gateway: Gateway that routes the packets to the target network

Interface: The network interface via which the route is to run

Predictable Network Interface Names (PNINs)
As of IGEL OS 11.06, the names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[220]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As " `eth0` ", " `eth1` ", and " `wlan0` " have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0` , `eth2` , `wlan0` , have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0` , `eth1` , etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump (see page 627)
  - **Bind interface** under **Security > Smartcard > Services**, see Services (see page 2025)
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance.
  To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Routing [1-5]

Enable: (default: disabled)

☑ This route is enabled.

Network route / host route: Type of route

220. https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

- Network route: The routing relates to a (sub) network
- Host route: The routing relates to the address of a computer

Network / host IP or name: The address of the network (for a network route) or the IP address or the name of the host (for a host route)

Network mask: Mask for the desired IP range, e.g. 255.255.255.0

Gateway: Gateway that routes the packets to the target network

Interface: The network interface via which the route is to run

Hosts

Menu path: **Setup > Network > Hosts**

If no DNS (Domain Name Service) is used, you can specify a list with computers in order to allow translation between the fully qualified host name, the short host name and the IP address.

To manage the list of computers, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Add

- **IP address**: IP address of the host you would like to add
- **Fully qualified host name**: Host name along with the domain, e.g. `mail.example.com`
- **Short host name**: E.g. `mail`

Network Drives

Menu path: **Setup > Network > Network Drives**

Here, you can configure both the drives that are to be connected during booting and the associated login data.

_____

- NFS (see page 1924)
- Windows Drive (see page 1926)

NFS

Menu path: **Setup > Network > Network Drives > NFS**

In this area, you can integrate network drives using the Network File System (NFS).

You can find a sample configuration at the end of this page.

To manage the network drives, proceed as follows:

- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Add

Enabled: Here, you can enable and disable configured entries.

☑ The network drive will be integrated. (default)

Local Mount Point: The local directory under which the server directory is to be visible (default: `/nfsmount`)

Server: NFS server that exports the directory

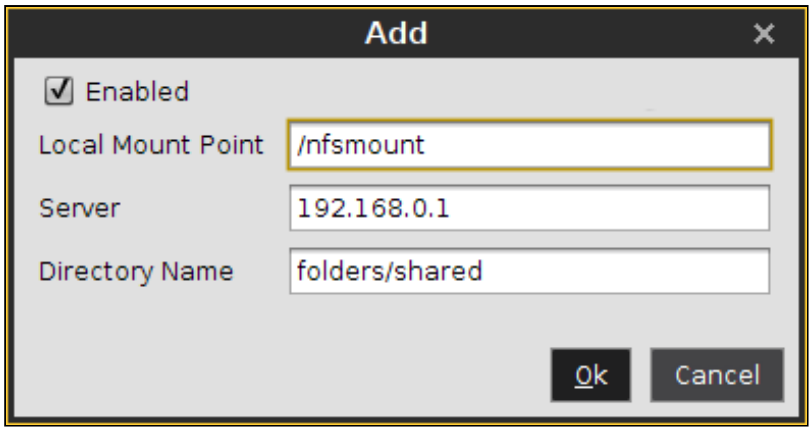
> For **Server**, you can provide an IP address, a hostname or a Fully-Qualified Domain Name (FQDN).

Directory name: Path under which the NFS server exports the directory

Sample configuration entry

The picture belows shows a sample configuration entry.

> In both the **Local Mount Point** and **Directory Name** only `/` (Linux/Unix-style forward slash) is permitted as a path separator.


Add
Enabled
Local Mount Point
/nfsmount
Server
192.168.0.1
Directory Name
folders/shared
Ok
Cancel

Windows Drive

Menu path: **Setup > Network > Network Drives > Windows Drive**

In this area, you can integrate network drives shared by Windows as well as those from Linux/Unix servers via the SMB protocol (Samba).

You can find a sample configuration at the end of this page.

To manage the drive list, proceed as follows:

- Click + to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Clicking + will bring up the **Add** dialogue, where you can define the following settings:

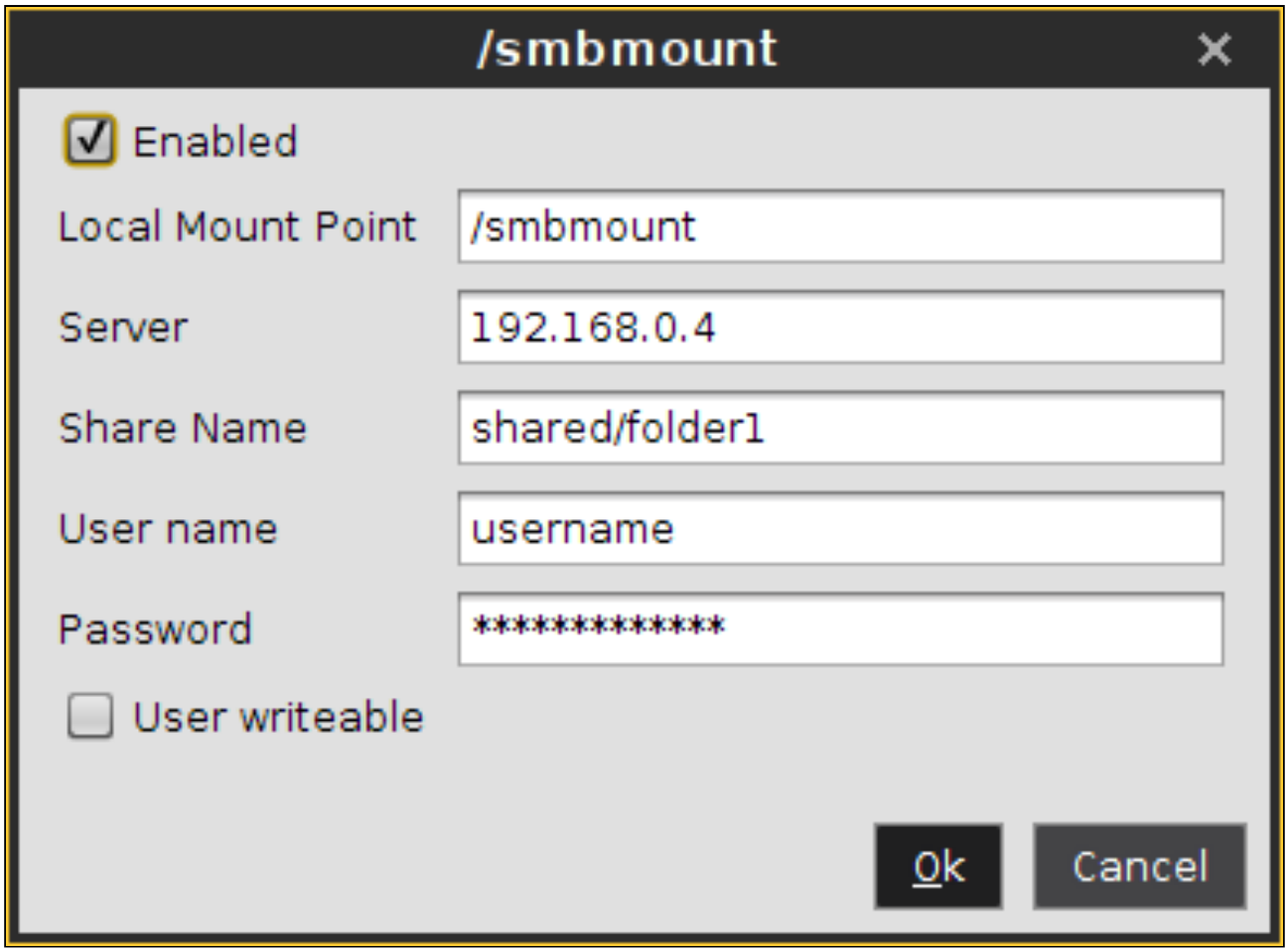
- **Enabled**: Defines whether the configuration entry will be applied.
  ☑ The network drive will be integrated.
- **Local Mount Point**: The local directory under which the server directory is to be visible (default: `/smbmount`)
- **Server**: The IP address, Fully-Qualified Domain Name (FQDN) or NetBIOS name of the server.
- **Share Name**: Path name as exported by the Windows or Unix Samba host.
- **User name**: User name for your user account on the Windows or Unix Samba host.
- **Password**: Password for your user account on the Windows or Unix Samba host.
- **User writable**
  ☑ The user can not only read but also write directory contents. Otherwise, only the local root user is able to do this.
  ☐ The user can only read directory contents. (default)

Sample configuration entry

The following picture shows a sample configuration entry.

If a NetBios name is provided for **Server**, make sure it is not preceded by slashes, e.g. `\\myComputer` (wrong) vs. `myComputer` (correct).

For **Local Mount Point**, only `/` (Linux/Unix-style forward slash) can be used as a path separator. Note that if you enter, for example, `\smbmount` as a moint point, a directory called `\smbmount` will be created, because `\` is a legal character in Linux directory names. For **Share Name**, however, `/` (Linux/Unix-style forward slash) or `\` (Windows-style backward slash) can be used as a path separator.


/smbmount
Enabled
Local Mount Point
/smbmount
Server
192.168.0.4
Share Name
shared/folder1
User name
username
Password
User writeable
Ok
Cancel

Proxy

Menu path: **Setup > Network > Proxy**

Here, you can select the communication protocols for which a system-wide proxy server is to be used.

Direct connection to the Internet: The endpoint device is directly connected to the Internet. No proxy is used.

Manual proxy configuration: You can configure one or more proxies in the fields from **FTP proxy** up to **SOCKS protocol version**.

Automatic proxy configuration: The proxy settings are dynamically retrieved via a PAC file (Proxy Auto Config) that you specify under **URL**. For more information on PAC, see e.g. https://en.wikipedia.org/wiki/Proxy_auto-config.

FTP proxy / **port**: FTP proxy server and port

HTTP proxy / **port**: HTTP proxy server and port

SSL proxy / **port**: SSL proxy server and port

SOCKS host / **port**: Socks proxy server and port

SOCKS protocol version: Selects the SOCKS protocol version. (Default: SOCKS v5)

URL: URL of the PAC file for **Automatic proxy configuration**

No proxy for: List of computers to which the endpoint device is to connect directly, separated by commas (Default: localhost, 127.0.0.1)

Proxy realm for browser: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication. See also Browser Global Proxy (see page 1566)

Use passthrough authentication

☑ The temporarily saved login information (user name and password) will be used to log in to the proxy server.

☐ The login information entered under **User name** and **Password** will be used to log in to the proxy server. (Default)

User name: User name for the proxy login

Password: Password for the proxy login

Enable client-side NTLM authenticating proxy

☑ Client-side proxy is enabled. It stands between the application and the corporate proxy, adding NTLM authentication at the corporate proxy. The credentials specified on this Setup page are used.

Listening port: Port for client-side proxy

VPN

Menu path: **Setup > Network > VPN**

Remote users securely access company networks via virtual private network protocols (VPN).

Enable tray icon

☑ A tray icon for the network interface will be shown. (default)

Enable context menu

☑ A context menu will be shown when you click on the tray icon. (default)

Enable network info dialog

☑ A dialog window with information regarding the network connection will be shown when you click on the context menu. (default)

- OpenVPN (see page 1930)
- NCP VPN Client (see page 1944)
- OpenConnect VPN (see page 1946)
- genucard (see page 1951)

OpenVPN

Menu path: **Setup > Network > VPN > OpenVPN**

The OpenVPN client puts in place a virtual private network using TLS encryption and requires OpenVPN 2.x as a VPN server.

If problems with OpenVPN occur, read the `/var/log/syslog` file with the System Log Viewer (see page 1754) accessory.

- **Enable Autostart During Boot**
  ☑ Shows the **Auto** column in the list of OpenVPN sessions. Highlight the desired session and click on **Set Auto** to enable this connection to be established during the boot procedure**.**
  ☐ Autostart is disabled. (default)
- **Restart connection when disconnected**:

To manage the list of OpenVPN session, proceed as follows:

→ Click + to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

_____

- Session (see page 1931)
- Options for OpenVPN Client-Server Communication on IGEL OS (see page 1933)
- TLS Options for IGEL OS OpenVPN (see page 1936)
- Proxy (see page 1938)
- IPv4 (see page 1939)
- Route (see page 1940)
- Desktop Integration (see page 1941)

Session

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Session**

OpenVPN Server(s): Name or public IP address of the *OpenVPN* server

Authentication type

- **TLS certificates**: Authentication with user certificate and private key
- **Name/password**: Authentication with user name and password
- **Name/password with TLS-certificates**: Combines name/password with user certificate.
- **Static key**: Authentication with a private key. No PKI infrastructure is needed for this.

TLS Certificates Authentication Type

> Persistent storage of files is possible in the folder `/wfs` resp. subfolders of `/wfs` only.
> Files stored under other paths will be lost when the thin client is rebooted.

Client certificate file: File with the client certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

CA certificate file: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Private key file: File with the private key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Private key password: Password in case one is set for the private key

> If you have a PKCS#12 file which contains the client certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the Securely Distributing Keys and Certificates[221] How-To.

Name/Password Authentication Type

Username: User name - if you leave this field empty, the user will be asked for it when establishing a connection.

Password required

☑ The user must enter a password. (default)

Password: Password - if you leave this field empty, the user will be asked for it when establishing a connection.

221. https://kb.igel.com/en/igel-os/11.10.250/securely-distributing-keys-and-certificates-for-op

CA certificate file: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Name/Password with TLS-Certificates Authentication Type

Username: User name - if you leave this field empty, the user will be asked for it when establishing a connection.

Password required

☑ The user must enter a password. (default)

Password: Password - if you leave this field empty, the user will be asked for it when establishing a connection.

CA certificate file: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Clientcertificate file: File with the user certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

CA certificate file: File with the CA certificate. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Private key file: File with the private key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Private key password: Password in case one is set for the private key

> If you have a PKCS#12 file which contains the user certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

For details of how to distribute certificates and keys securely to thin clients, see the Securely Distributing Keys and Certificates[222] How-To.

Static Key Authentication Type

Private key file: File with the static key. Enter a path relative to `/wfs/OpenVPN` or select using the file selection.

Key direction:

- None: No key direction
- 0: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- 1: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.

Remote IP address: The VPN IP address of the server

Local IP address: The VPN IP address of the client

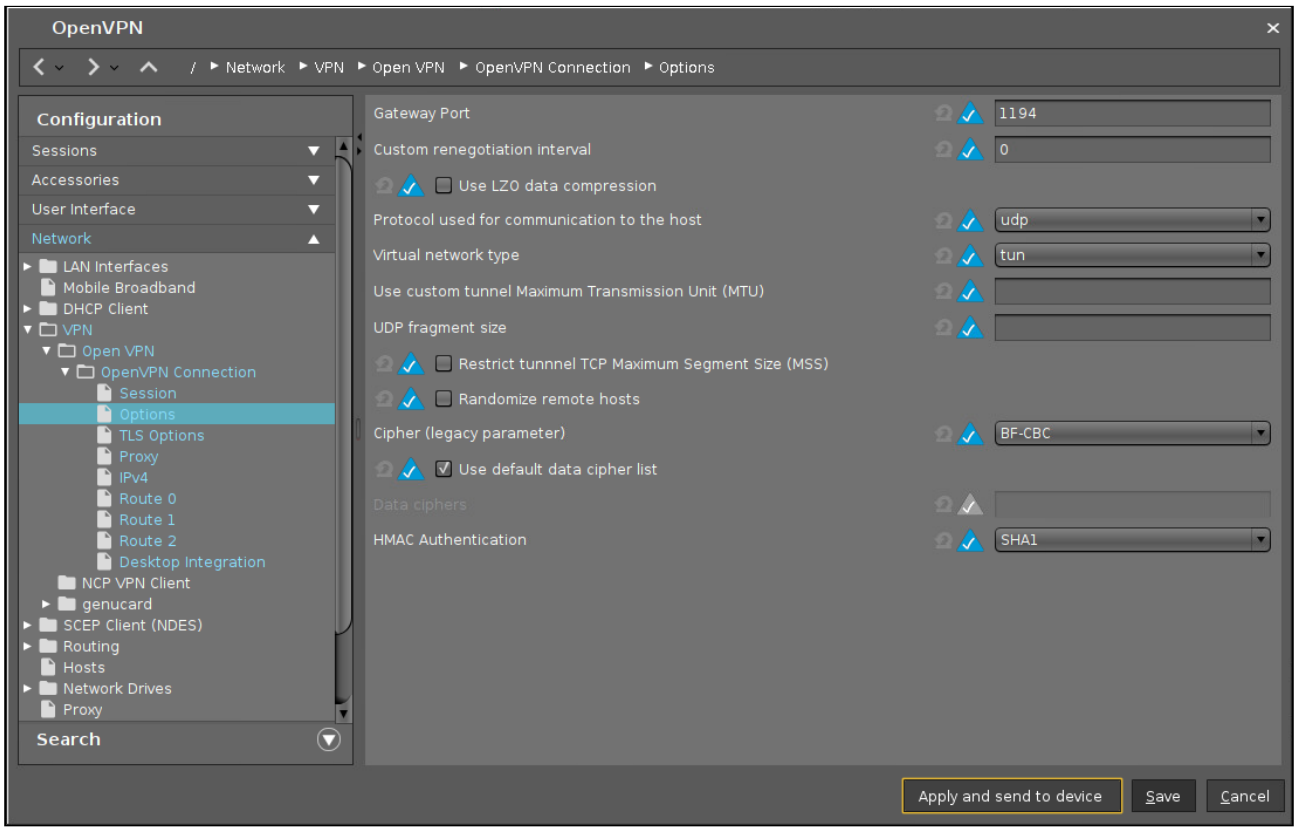
222. https://kb.igel.com/en/igel-os/11.10.250/securely-distributing-keys-and-certificates-for-op

Options for OpenVPN Client-Server Communication on IGEL OS

Here, you can configure the interaction between the OpenVPN client on IGEL OS and the server.

Further information regarding the options can be found in the OpenVPN documentation[223] which is maintained by the OpenVPN project.

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Options**



Gateway Port

Local gateway port. Default: 1194

Custom renegotiation interval

Renegotiate data channel key after a given number of seconds. (Default: 0)

Use LZO data compression

⚠ From OpenVPN v2.4, LZO data compression ("comp-lzo") is deprecated.

223. https://openvpn.net/index.php/open-source/documentation.html

☑ The client will use LZO compression. Necessary if the server uses compression.

☐ The client will not use LZO compression. (Default)

Protocol used for communication to the host

- **udp**: UDP will be used. (Default)
- **tcp-client**: TCP will be used.

If you use a proxy, select **tcp-client**.

Virtual network type

- **tun**: Routing will be used. (Default)
- **tap**: Bridging will be used.

Use custom tunnel maximum transmission unit (MTU)

The MTU of the TUN device will be used as a given value. The MTU of the interface will be derived from it.

UDP fragment size

Allow internal data fragmenting up to this size in bytes. Leave this field empty to keep the default value.

Restrict tunnel TCP maximum segment size (MSS)

☑ The TCP segment size (MSS) of the tunnel will be restricted.

☐ The TCP segment size (MSS) will not be restricted. (Default)

Randomize remote hosts

☑ The remote gateways will be ordered randomly as a simple type of load balancing.

☐ The remote computers will not be ordered randomly. (Default)

Cipher (legacy parameter)

Encryption algorithm for data packets. If you do not want to use any of the ciphers in this menu, select **unset**.
Default: **BF-CBC** (Blowfish in the Cipher Block Chaining mode)

Use default data cipher list

The default list of ciphers that are to be negotiated between client and server is "AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305".

☑ The default cipher list is used. (Default)

☐ The list provided in **Data ciphers** is used.

Data ciphers

You can enter enter a custom list of ciphers. The ciphers must be separated by a semicolon ';'. Example: "AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305"

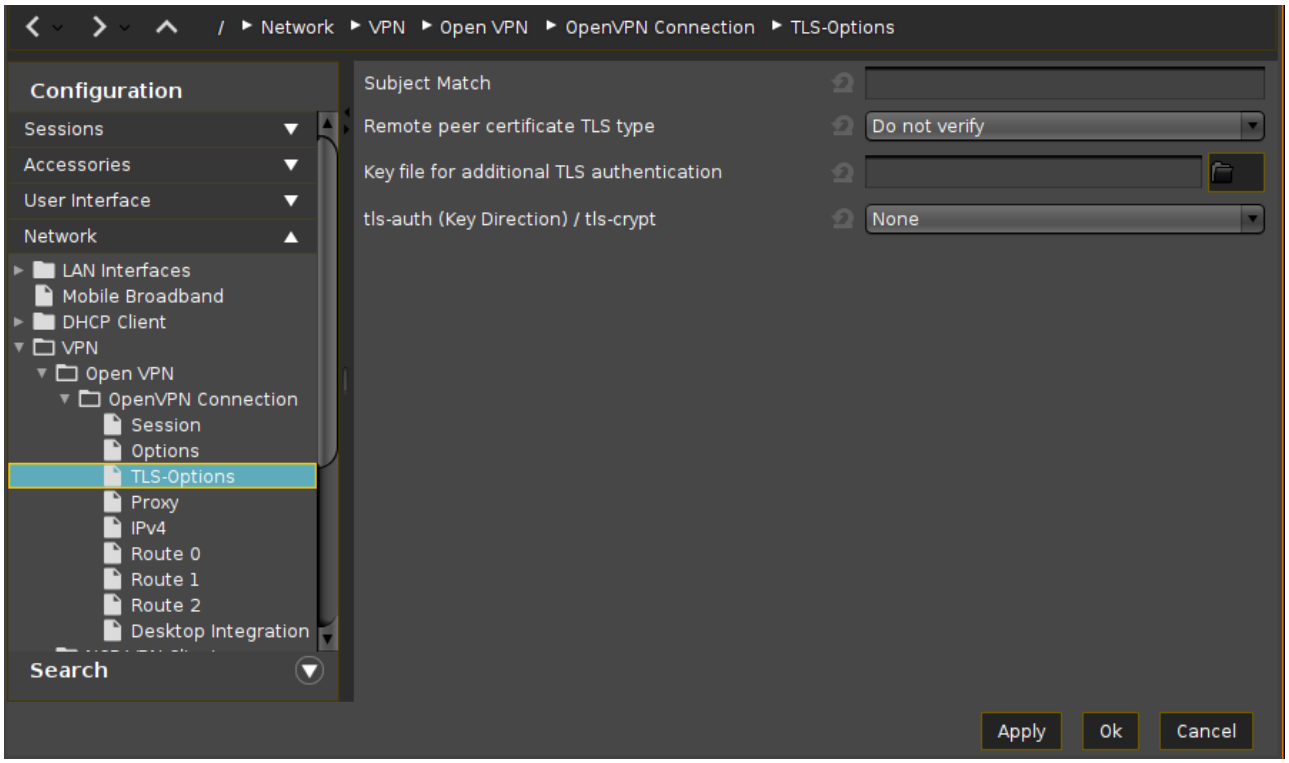
HMAC authentication: Hashing algorithm for packet authentication (default: SHA1)

TLS Options for IGEL OS OpenVPN

This article shows how to define the TLS options for the OpenVPN client in IGEL OS. Under TLS (Transport Layer Security) Options, you can customize the options for the OpenVPN protocol (tunnel). TLS is the successor to SSL (Secure Sockets Layer). It is a standard consisting of several protocols that can transmit encrypted data between authenticated communication partners over potentially insecure IP networks such as the Internet.

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > TLS Options**

TLS Options for OpenVPN Client in IGEL OS:



Subject match:

The Subject match accept/reject the server connection based on a custom test of the server certificate's embedded X509 subject details. The formatting of these fields changed into a more standardized format. It now looks like: **C=US, L=Somewhere, CN=John Doe, emailAddress=john@example.com.**

See also: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

Remote peer certificate TLS type:

Require that peer certificate was signed with an explicit key usage and extended key usage based on RFC3280 TLS rules.

This is a useful security option for clients, to ensure that the host they connect to is a designated server. Or the other way around; for a server to verify that only hosts with a client certificate can connect.

- **Do not verify*:** no remote certificate check
- **Check for server certificate:** The **--remote-cert-tls server** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Server Authentication"**
- **Check for client certificate:** The **--remote-cert-tls client** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Client Authentication"**

This is an important security precaution to protect against a man-in-the-middle attack, where an authorized client attempts to connect to another client by impersonating the server. The attack is easily prevented by having clients verify the server certificate using any one of **--remote-cert-tls, --verify-x509-name,** or **--tls-verify.**

Key file for additional TLS authentication:

As the path enter relative to `/wfs/OpenVPN` or select using the file selection. This adds an additional HMAC legitimization level above the TLS control channel in order to prevent DDOS attacks.

tls-auth (Key Direction) / tls-crypt:

- **None***: No key direction
- **tls-auth 0**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-auth 1**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-crypt**: In contrast to tls-auth, setting a key direction is not required. Use this option if the version of the OpenVPN server is 2.4 or higher. For more information on tls-crypt, see e.g., Reference manual for OpenVPN 2.4[224].

*IGEL OS system defaults

224. https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

Proxy

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy**

Here, you can set up an optional proxy server for the VPN connection.

If you use a proxy, select the value **tcp-client** under **Options > Communication protocol to the host**.

- **Proxy type**
  - None: Direct connection to the Internet.
  - HTTP: HTTP proxy will be used.
  - SOCKS: SOCKS proxy will be used.

Details for HTTP proxy

- **Proxy address**: Name or IP address of the proxy server
- **Proxy port**: Port on which the proxy service is available
- **Retry indefinitely when errors occur**
  ☑ In the event of errors, repeated attempts to establish a connection via proxy will be made.
  ☐ No further attempts to establish a connection will be made (default).

Ceredentials for HTTP

- **Proxy username**: User name for the proxy server
- **Proxy password**: Password for the proxy server

IPv4

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > IPv4**

By default, OpenVPN uses the server's DNS and routing settings. Here, you can change these settings.

Automatic DNS:

☑ The name server(s) will be carried over by the OpenVPN server. (default)

☐ Extra name servers (see below) will be used.

Extra name server(s): One or more name servers, IP addresses separated by commas.

Extra search domain(s): One or more search domains, separated by commas.

Automatic routes

☑ The routing table will be carried over by the OpenVPN server. (default)

☐ Extra routes will be configured.

VPN is the default route

☑ The default route leads to the VPN. (default)

☐ Extra routes will be configured.

Route

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Route [0,1,2]**

Here, you can configure extra routes.

- **Enable**
  ☑ This route is enabled.
  ☐ This route is not enabled. (default)
- **Network route / host route**: Type of route
  - Network route: The routing relates to a (sub) network
  - Host route: The routing relates to the address of a computer
- **Network / host IP**: The address of the network (for a network route) or the IP address or the name of the host (for a host route)
- **Network mask**: Mask for the desired IP range, e.g. 255.255.255.0
- **Gateway**: Gateway that routes the packets to the target network
- **Metric**: Here, you can enter a numerical quality assessment for routing decisions, 0 is the best value.

Desktop Integration

Menu path: **Setup > Network > VPN > OpenVPN > [OpenVPN Connection] > Desktop Integration**

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.

- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)

- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

NCP VPN Client

Menu path: **Network > VPN > NCP VPN Client**

NCP offers a 30-days trial period for IGEL customers.

The configuration parameters for the NCP Client are configured exclusively via the client program interface itself.

You will find the documentation regarding the NCP Secure Enterprise Client at https://www.ncp-e.com/en/service-resources/library/.

->Click + to add an NCP VPN client session and configure the start methods.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

> When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted automatically after the termination.

OpenConnect VPN

Menu Path: **Setup > Network > VPN > OpenConnect VPN**

> Feature Not Available on IZ Devices
>
> This feature is not available on IGEL IZ devices (IGEL Zero HDX, IGEL Zero RFX, or IGEL Zero Horizon).

The OpenConnect VPN Client puts in place a virtual private network using TLS encryption. This feature is available from IGEL *Linux 10.04.100* onwards.

Feature with limited support The OpenConnect VPN Client feature comes with limited support and without any warranty. Any support for this feature is provided on a non-binding, “best effort” basis.

The OpenConnect VPN Client feature needs to be enabled manually before you can use it, see Enabling the OpenConnect VPN Client (see page 1950).

- **Enable autostart during boot**
  ☑ Autostart is enabled.
  ☐ Autostart is disabled. (Default)
- **Restart connection when disconnected**
  ☑ Reconnect automatically when a disconnect occurs.
  ☐ Do not reconnect automatically when a disconnect occurs. (Default)

To manage the list of *OpenConnect VPN* sessions, proceed as follows:

→ Click to create a new entry.

→ Click to remove the selected entry.

→ Click to edit the selected entry.

→ Click to copy the selected entry.

———

- Session (see page 1947)
- Desktop Integration (see page 1948)
- Enabling the OpenConnect VPN Client (see page 1950)

Session

Menu path: **Setup > Network > VPN > OpenConnect VPN > [session name] > Session**

- **Gateway**: IP address, hostname or Fully Qualified Domain Name (FQDN) of the VPN gateway
- **Connect to Juniper Networks VPN**
  ☑ The protocol of Juniper Networks VPN is used.
  ☐ The protocol of Juniper Networks VPN is not used. (Default)
- **Name/Password Authentication**
  ☑ User name and password are used for authentication.
  ☐ User name and password are not used for authentication. (Default)
- **User name**: User name used for authentication
- **Password**: Password used for authentication
- **CA Certificate**: Path to the CA certificate
- **User Certificate**: Path to the user certificate

> The certificates should be stored in the directory `/wfs/OpenVPN/` if possible, then they will certainly be found after a reboot.

- **Private Key**: Path to the private key
- **Private Key password**: Password of the private key

Desktop Integration

Menüpfad: **Setup > Network > VPN > OpenConnect VPN > [session name] > Desktop Integration**

Session Name: Name for the session

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start Menu

☑ The session can be started from the start menu. (Default)

Application Launcher

☑ The session can be started with the application launcher. (Default)

Desktop:

☑ The session icon will appear on the desktop. (Default)

Quick Start Panel

☑ The session can be started from the quick start panel.

☐ The session cannot be started from the quick start panel. (Default)

Desktop Context Menu

☑ The session can be started form the desktop context menu.

☐ The session cannot be started from the desktop context menu. (Default)

Application Launcher folder: Path to the application launcher folder

Password Protection: Specifies which password will be requested when launching the session.
Possible values:

- None: No password is requested when launching the session.
- Administrator: The administrator password is requested when launching the session.
- User: The user password is requested when launching the session.
- Setup User: The setup user's password is requested when launching the session.

Hotkey:

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

> When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Enabling the OpenConnect VPN Client

To enable the OpenConnect VPN Client, proceed as follows:

1. Ensure that the settings under **System > Update > Firmware Update** are correct. The **Server Path** must point to the firmware version that is currently installed. This is required because the software package for the OpenConnect VPN client must be downloaded in order to deploy the feature.
2. Go to **System > Firmware Customization > Features** and activate **VPN OpenConnect (Limited support - functionality "as is", see product documentation for details)**.
3. Confirm the warning dialog with **Ok**.
4. Click **Ok** in the main window.
5. Reboot the thin client.
   On reboot, the client downloads and installs the software package for the OpenConnect VPN Client feature.

genucard

Menu path: **Network > VPN > genucard**

The *genucard* VPN hardware offers a choice of preconfigured Internet and VPN connections.

The settings for launching the session are described below.

Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)

- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- “Connections” Window (see page 1954)
- Options (see page 1955)
- Desktop Integration (see page 1956)
- Administrator Session (see page 1958)

“Connections” Window

The **Connections** window opens as soon as the *genucard* session is launched. You will find the following menu points there:

- **File**
  - **Change PIN**: Enter your previous PIN as well as your chosen new PIN twice.
  - **Rekeying**: Enter your PIN to generate a new key.
- **Wifi**: Opens the **Wifi** dialog which allows you to configure wireless access for the *genucard*.
  - Select a wireless network from the list. **Scan** updates the list (this can take up to a minute).
  - **Password**: The password for the selected wireless network. **Show** shows the entry in plain text.
  - **Save**: Saves the connection data entered along with the password on the *genucard*.
  - **Saved connections**: Select one of the previously saved connections.
  - **Delete**: Deletes the selected connection.
  - **Edit**: Changes the password for the selected connection.
- **Log**: Allows you to view the log
- **Network connection**: Select one of the network connections preconfigured on the *genucard*, for example LAN or WiFi.

> The network connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

->To start the selected network connection, click **Connect**.

- **VPN connection**: Select one of the VPN connections preconfigured on the *genucard*.

> The VPN connections listed here have been configured using a *genucard* administration session or the *genucenter*. Connections configured with the *genucenter* are marked with "(GCE)".

->To start the selected VPN connection, click **Connect**.

Options

Menu path: **Setup > Network > VPN > genucard > Options**

Here, you can prepopulate connection and user data for the genucard.

Autostart during boot

☑ The genucard application is launched during booting. This option increases the waiting time until the network is available.

> If the user name, password, default Internet connection and the default VPN connection are set in the setup, automatic launching allows firmware updates via VPN too.

☐ The genucard application is not launched during booting. (default)

Autostart after USB directory (requires restart)

☑ The genucard application is automatically launched as soon as the genucard is connected to the thin client. (default)

> Launching the genucard can take up to 60 seconds.

Default Internet connection: Name of an Internet connection configured on the genucard.

Default VPN connection: Name of an Internet connection configured on the genucard.

User name: User name for the genucard application

Password: Password for the genucard application

Internet connection timeout: Permitted waiting time in seconds (default: 120)

VPN connection timeout: Permitted waiting time in seconds (default: 120)

File path for private keys for machine connection: File path for the key file.

Desktop Integration

Menu path: **Setup > VPN > genucard > Desktop Integration**

- **Session name**: Name for the session

> The session name must not contain any of these characters: `\ / : * ? “ < > |` `[ ] { } ( )`

- **Start menu**:
  ☑ The session can be started with the start menu. (Default)
  ☐ The session cannot be found in the start menu.
- **Application Launcher**:
  ☑ The session can be started with the Application Launcher. (Default)
  ☐ The session cannot be found in the Application Launcher.
- **Desktop**:
  ☑ The session can be started with a program starter on the desktop. (Default)
  ☐ The session does not have a program starter on the desktop.
- **Quick start panel**:
  ☑ The session can be started with the quick start panel.
  ☐ The session cannot be found in the quick start panel. (Default)
- **Start menu's system tab**:
  ☑ The session can be started with the start menu’s system tab.
  ☐ The session cannot be found in the start menu’s system tab. (Default)
- **Application Launcher's system tab**:
  ☑ The session can be started with the Application Launcher’s system tab.
  ☐ The session cannot be found in the Application Launcher’s system tab. (Default)
- **Desktop context menu**:
  ☑ The session can be started with the desktop context menu.
  ☐ The session cannot be found in the desktop context menu. (Default)
- **Menu folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Desktop folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection**: Specifies which password will be requested when launching the session. Possible values:
  - None: No password is requested when launching the session. (Default)
  - **Administrator**: The administrator password is requested when launching the session.
  - **User**: The user password is requested when launching the session.
  - **Setup user**: The setup user's password is requested when launching the session.
- **Hotkey**: A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers**: One or two modifiers for the hotkey:

- `None`
- = `Shift`
- [Ctrl] = `Ctrl`
- = `Super_L`
- [Alt] = `Alt`

Modifiers can be combined by using the pipe character `|`:

- [Ctrl]+ = `Ctrl|Super_L`

- **Key**: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the character string for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Administrator Session

The genucard is configured and administered centrally via the genucenter management interface. While VPN profiles can only be configured via genucenter or other remote interfaces, Internet connection profiles can also be configured via a local administration session.

Further information is available from www.genua.de[225].

Optionally, an administrator session allowing the genucard Internet connection to be configured can be set up:

To configure an Internet connection profile via a local administration session, proceed as follows:

1. Click on **Add instance** under **System > Registry > Sessions > genucard%**.
   The genucard icon will appear on the desktop.
2. Click on the genucard icon.
   The genucard logon window will open.
3. Enter a **user name** and **password**.
4. Click on **Logon**.
   The Internet/VPN page will open.
5. In the **Internet** area, configure the connection with the help of the (Create), (Edit) and (Delete) buttons.

225. https://www.genua.de/en.html

DHCP Client

Menu path: **Setup > Network > DHCP Client**

Here, you can change the advanced settings for the firmware's built-in DCHP client.

_____

- Default Options (see page 1960)
- User-Defined Options (see page 1961)

Default Options

Menu path: **Setup > Network > DHCP Client > Default Options**

- **User Class**: A freely definable character string which can serve as a criterion for allocating specific settings for the DHCP server.
- **List of standard options**: Options with which the client can request information from the DHCP server.
  You will find information regarding the various DHCP options in RFC 2132 DHCP Options and BOOTP Vendor Extensions[226].

To edit the list, proceed as follows:

- Click on to create a new entry.
- Click on to remove the selected entry.
- Click on to edit the selected entry.
- Click on to copy the selected entry.

226. https://tools.ietf.org/html/rfc2132

User-Defined Options

Menu path: **Setup > Network > DHCP Client > User-Defined Options**

→ To create a new entry, click on + in the **List of custom options** area.

For more information regarding these options, see the manual for your DHCP server or your network components.

- **Enabled**
  ☑ The option is enabled. (default)
  ☐ The action is not enabled.
- **Option Name**: Add a prefix of your own in order to prevent a conflict with the default DHCP options. Example of the syntax: `[YourPrefix]-[OptionName]`. English letters, numbers and the special character “-” are allowed.
- **Code**: A number that is used by the DHCP server and DHCP client to reference an option. A number between 80 and 254 can be chosen. (default: 80)
- **Data Type**: Type of option. Possible values:
  boolean
  integer 8
  integer 16
  integer 32
  signed integer 8
  signed integer 16
  signed integer 32
  unsigned integer 8
  unsigned integer 16
  unsigned integer 32
  ip address
  text
  string

SCEP Client (NDES)

Menu path: **Setup > Network > SCEP Client (NDES)**

SCEP allows the automatic provision of client certificates via an SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x).

A Microsoft Windows Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification body). More information can be found at Microsoft, e.g. in the following Technet article: Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)[227]

Manage certificates with SCEP

☑ Certificate management via SCEP Client (NDES) is enabled. Now carry out the necessary configuration.

☐ Certificate management via SCEP Client (NDES) is not enabled. (Default)

_____

- Certificate (see page 1963)
- Certification Authority (see page 1965)
- SCEP (see page 1966)

227. http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

Certificate

Menu path: **Setup > Network > SCEP Client (NDES) > Certificate**

Here, you can specify the basic data for the certificate to be issued by the certification body.

Type of CommonName/SubjectAltName: The characteristic for linking the certificate to the device.

- IP address: The IP address of the device.
- DNS name: The DNS name of the device.
- IP address (auto): The IP address of the device (inserted automatically).
- DNS name (auto): The DNS name of the device (inserted automatically).
- Email address: An email address.
- DNS name as UPN (auto)

> If the client automatically obtains its network name, **DNS Name (auto)** is a good type for the client certificate.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**:

CommonName/SubjectAltName: Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

The following parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**:

CommonName/SubjectAltName Suffix: Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- "none": No suffix will be added.
- "dot + DNS domain (auto)": The system's current DNS domain name separated with a dot will be added. Example: `.igel.local`
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
  - `%D` is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: `@%D` will be changed into `@igel.de` if the system's current DNS domain name is `igel.de`.
  - %% will be replaced by %. Example: `A%%B` will be changed into `A%B`.
  - Other combinations with % are currently discarded. Example: `A%BC` will be changed into `AC`.

> If you have to specify the suffix manually, make sure you enter the separator.

Organizational unit: Stipulated by the certification authority.

Organization: A freely definable designation for the organization to which the client belongs.

Locality: Details regarding the device's locality. Example: "Augsburg".

State: Details regarding the device's locality. Example: "Bayern".

Country: Two-digit ISO 3166-1 country code. Example: "DE".

RSA key length (bits): Select a key length (one suited to the certification authority) for the certificate that is to be issued.
Possible values:

- "1024"
- "2048"
- "4096"

Certification Authority

Menu path: **Setup > Network > SCEP Client (NDES) > Certification Authority**

The details for the following fields can be obtained from the certification authority:

CA identifier

CA certificate fingerprint (MD5)

SCEP

Menu path: **Setup > Network > SCEP Client (NDES) > SCEP**

Here, you can give information regarding the SCEP server used.

> Because of the need to enter a fingerprint (CA root certificate) and the **Challenge password** (SCEP server), the configuration process is somewhat complicated. Ideally, it should be set up in the UMS as a profile and distributed to the devices. At the same time, the certificate cannot yet be used for communication purposes.

SCEP server URL: Address of the SCEP server. Examples: http://myserver.mydomain.com/certsrv/mscep/mscep.dll (Windows Server 2019); http://myserver.mydomain.com/certsrv/mscep (before Windows Server 2019)

Proxy server for SCEP requests: Proxy server in the format `host:port`. If this field is empty, no proxy will be used.

Challenge password: Password for queries.

Certificate renewal period (days): Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)

Certificate expiry check interval (days): Specifies how often the certificate is checked against its expiry date. (Default: 1)

> As an example, a certificate is valid until 31.12. of a year. If the period for renewal is set to 10 days, a new certificate will be requested for the first time on 21.12. of the same year.

For more information, see the how-to Providing the SCEP Server Data (see page 756). See also Configuration of the SCEP Client (see page 750).

Devices

Menu path: **Devices > Hardware Info**

->Click on **Hardware Info** to view the system information for your IGEL device.

In this area, you can make settings for the following options:

- Storage Devices (see page 1968)
- Printer (see page 1974)
- Unified Communications (see page 2002)
- Bluetooth (see page 2009)
- USB Access Control (see page 2010)

Storage Devices

Menu path: **Setup > Devices > Storage Devices**

Configure your hotplug storage devices here.

Show attached storage devices: Shows a list with registered storage devices.

_____

- Storage Hotplug (see page 1969)
- Options (see page 1972)
- DriveLock (see page 1973)

Storage Hotplug

Menu path: **Setup > Devices > Storage Devices > Storage Hotplug**

In this area you can set up the connection of hotplug storage devices to the device. These can be USB mass storage devices or MMC card readers for example.

Following file systems are officially supported:

ext2, ext3, ext4	Standard Linux file systems
squashfs	a packed read-only file system
vfat	supports all FAT variants
exFAT[1]	supports exFAT (found on SDXC SD-cards)
ISO 9660	CDROM/DVD file systems
udf	CDROM/DVD file systems
ntfs	supported with ntfs-3g (Fuse)

[1] With Firmware 11.03.100 or newer

You can change the following settings:

Storage Hotplug

☑ Hotplug storage devices will be be mounted and unmounted automatically. When mounted, a hotplug storage device can be used in sessions like ICA, RDP, VMware Horizon, or in local applications like browser / PDF viewer or media player.

Before you unplug a hotplug storage device from the thin client, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on ⏏ in the task bar. The taskbar is not available in a fullscreen session.
- Click on ⏏ in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session. For further information, see In-session Control Bar (see page 1872).
- Function **Accessories > Disk Removal** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Dont' remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

☐ Hotplug storage devices will be be mounted and unmounted automatically. (Default)

Default permission: Default access rights for hotplug storage devices.
Possible values:

- Read only
- Read/Write

Client Drive Mapping: Defines the creation of drives in ICA sessions, RDP sessions or Horizon sessions. The mounting of hotplug storage devices to the local file system is not influenced by this parameter.
Possible values:

- Dynamic: Drives are created automatically in a session when a hotplug storage device is connected to the device. When the device is removed, the corresponding drive is removed automatically.
- Static: The drives in a session are predefined by the parameters described under Static Client Drive Mapping (see page 1970).

Static Client Drive Mapping

Private drive letter for each storage drive

☑ A drive letter is assigned to each hotplug storage device.

☐ A single drive letter will be generated for all hotplug storage devices and each hotplug storage device will be assigned a sub-directory. (default)

Number of drives: The maximum number of hotplug storage devices that can be used simultaneously in the session.

> When this number is reached, no additional hotplug storage devices will be assigned.

Start storage drives with this drive letter: Letter that is assigned to the first hotplug storage device if automatic drive mapping is enabled (default: A). Further hotplug storage devices are assigned the next letter alphabetically.

ICA read access for storage hotplug devices: Specifies whether read access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Read access is allowed.
- No: Read access is not allowed.
- Ask user: Read access can be allowed on request.

ICA write access for storage hotplug devices: Specifies whether write access to hotplug storage devices is allowed in an ICA session.

Possible values:

- Yes: Write access is allowed.
- No: Write access is not allowed.
- Ask user: Write access can be allowed on request.

Notification

Hotplug beep

☑ A signal tone will be heard when connecting and disconnecting hotplug storage devices. (Default)

Hotplug message

☑ Hotplug messages will be shown when connecting and disconnecting hotplug storage devices. (Default)

Timeout: Period of time in seconds after which the window with the hotplug messages is hidden. If the parameter is set to **No timeout**, the window will be shown until it is closed manually. (Default: 15)

You will find further settings options in the HDX / ICA Global setup area under Drive mapping (see page 1256), in the RDP Global setup area under Drive mapping (see page 1318), in the Devices area under USB access control (see page 2010) and in the Accessories area under Disk Removal (see page 1803).

Options

Menu path: **Setup > Devices > Storage Devices > Options**

In this area, you can specify a directory in which external storage devices are accessible to the user. The devices are always mounted in the `/media` directory.

User browse directory

☑ The directory defined under **Browse directory** is linked to the `/media` directory. (Default)

Browse directory:/: Local directory in which the devices can be found. (Default: `userhome/media`)

Support for built-in floppy drives

☑ Built-in disk drives are active.

☐ Built-in disk drives are disabled (default)

> This option is only valid for drives which are not connected via USB.

DriveLock

Menu path: **Devices > Storage Devices > DriveLock**

DriveLock allows the control of your USB devices and helps to prevent BadUSB attacks. For details, see https://www.drivelock.com/.

Enable DriveLock agent

☑ DriveLock agent is activated.

DES server URL: URL of the DriveLock Enterprise Service server used for the distribution of policies

Tenant: Name of the DES user group to which the policy should apply. (Default: root)

Printer

Menu path: **Devices > Printers**

You can set up a printer for the device here.

The printers must be set up under **Devices > Printer > CUPS > Printers** and must be enabled there for mapping in sessions.

> Because the thin client merely places incoming print jobs in a queue, you need to install the printer on the server. Please note that you will need to be logged in as administrator to the terminal to which the printer is connected.

- CUPS (see page 1975)
- LPD (see page 1985)
- TCP/IP (see page 1986)
- ThinPrint (see page 1993)
- PrinterLogic (see page 1997)
- LRS (see page 1999)

CUPS

Menu path: **Devices > Printers > CUPS**

The Common UNIX Printing System™ (or CUPS) is the software that allows you to print from within applications, e.g. from this web browser.

CUPS converts the page descriptions produced by the application, e.g. "Insert Paragraph", "Draw Line" etc., into data that can be read by the printer, and then sends this information to the printer.

With the appropriate configuration, CUPS can use printing devices via the following connections:

- Parallel (LPT 1, LPT 2)
- Serial (COM1, COM2, USB COM1, USB COM2 – with a USB-to-serial adapter)
- USB (1st and 2nd USB printer)
- Network (TCP/IP, LPD, IPP, SMB)

Default Paper Size: Specify a default paper size for print jobs.

Possible values:

- Letter
- Legal
- Executive
- A5
- A4
- A3
- Autodetect (Default)

Additional information on CUPS printers can be found under How to Map a Local Printer to a Citrix or RDP Session on IGEL OS (see page 1121) and Installing a Custom CUPS Driver (see page 1130).

- Printers - Configure CUPS Printers in IGEL OS (see page 1976)
- IPP Printer Sharing (see page 1984)

Printers - Configure CUPS Printers in IGEL OS

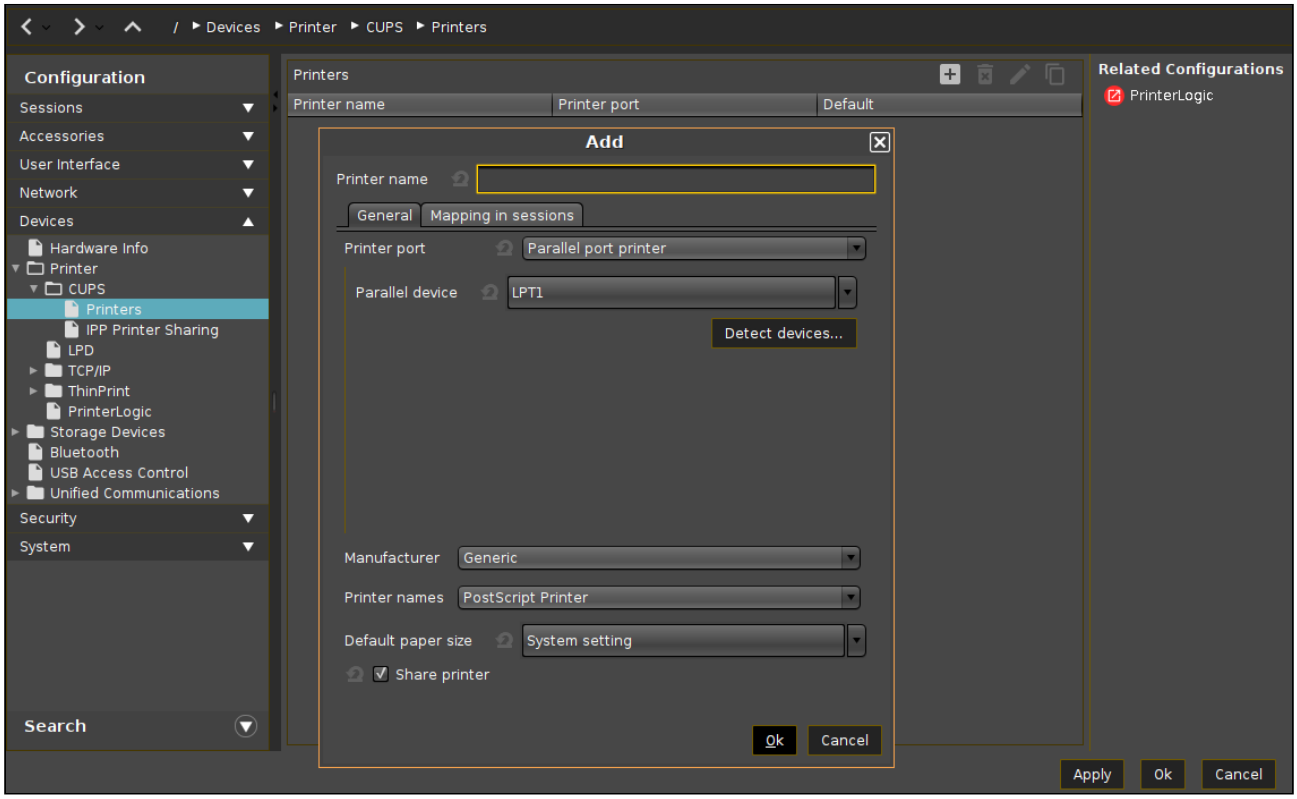
The following article describes settings for configuring CUPS printers for your IGEL OS devices. For general information on CUPS, see CUPS (see page 1975).

If you want to automatically set the currently connected printer as the default printer, see also Dynamic Selection of the Default Printer on IGEL OS (see page 1131).

Because the endpoint device merely places incoming print jobs in a queue, you need to install the printer on the server. Note that you will need to be logged in as an administrator to the terminal to which the printer is connected.

Settings made here apply to local printing (e.g. PDF, Firefox, etc.) and to mapping a local printer into a session.

Menu path: **Devices > Printer > CUPS > Printers**



Printers can be created and edited here.

→ Click on + to open the **Add** dialog.

→ In the edit dialog, specify a **Printer name** which begins with a letter.

General

Printer port

Interface type for locally connected printers or the network protocol for network printers.

Possible values:

- **Parallel port printer***
- **Serial port printer**
- **USB printer**
- **USB class printer**
- **LPD network printer**
- **TCP network printer**
- **IPP network printer**
- **SMB network printer**
- **LRS managed printer**

> Depending on the chosen **Printer port** type, different parameters have to be configured, see Settings to Be Configured for Each Printer Port Type (see page 1980).

Manufacturer

List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Printer names**. (Default: Generic)

If a custom printer driver is required, see Installing a Custom CUPS Driver (see page 1130).

Printer names

List of possible printer models. (Default: PostScript Printer)

Default paper size

Set the printer-specific paper size that you would like to use as a default.
Possible values:

- **Letter**
- **Legal**
- **Executive**
- **A5**
- **A4**
- **A3**
- **System setting***

Share printer

☑ You can access the printer via the network if you have enabled the print server under **IPP Printer Sharing**, see IPP Printer Sharing (see page 1984).*

Mapping in sessions

Map printer in NX sessions

☑ The printer is available in NX sessions.

☐ The printer is not available in NX sessions.*

Map printer in Parallels Client sessions

☑ The printer is available in Parallels Client sessions.

☐ The printer is not available in Parallels Client sessions.*

Map printer in ICA sessions

☑ The printer is available in ICA sessions.*

> Install the HP Color LaserJet 2800 Series PS driver on the server side to redirect the local printer to Citrix sessions, see https://support.citrix.com/article/CTX140208.

Map printer in RDP sessions

☑ The printer is available in RDP sessions.*

Map printer in AVD sessions

☑ The printer is available in AVD sessions.*

See also CUPS Printer Redirection (see page 1675) for AVD sessions.

Use Windows driver name from list

☑ A driver name from the following list will be used.*

Manufacturer

List of possible printer manufacturers. (Default: Generic)

Model

List of possible models. (Default: Generic PostScript)

Use custom Windows driver name

☑ Enter the name of your driver here if it is not mentioned in the list above.

Printer driver

Windows driver name for the printer.

> The name must not contain “;” or “:”.
> Note that special characters, spaces, and case-sensitive characters are relevant when specifying a driver name.

When printing in ICA and RDP sessions, the print data are normally prepared for the printer model by the Windows printer driver and are passed unchanged from the device to the printer. An exception is made when using the Windows driver in ICA sessions, **Manufacturer** is set to "Generic" and **Model** is set to "Generic PostScript." In this case, the print data are prepared on the device with the help of the printer driver defined above under **Printer** for the printer model. This requires device resources.

*IGEL OS system default

Settings to Be Configured for Each Printer Port Type

Menu path: **Devices > Printer > CUPS > Printers**

Here, you can find the parameters available for configuration for each **Printer Port** (**Devices > Printer > CUPS > Printers > Add > General > Printer port**).

Printer Port: "Parallel port printer"

Parallel device:

- "LPT1" (Default)
- "LPT2"

Detect devices...: Opens a dialog for selecting the available devices.

Printer Port: "Serial port printer"

Serial device:

- "COM1" (Default)
- "COM2"
- "USB COM1"
- "USB COM2"

Detect devices...: Opens a dialog for selecting the available devices.

Baud rate:

- "9600" (Default)
- "19200"
- "38400"
- "57600"
- "115200"

Character size:

- "5"
- "6"
- "7"
- "8" (Default)

Parity:

- "None" (Default)
- "Even"
- "Odd"

Flow control:

- "None" (Default)
- "XON/XOFF"
- "RTS/CTS"

- "DTR/DSR"

Printer Port: "USB printer"

USB device:

- "1st USB printer" (Default)
- "2nd USB printer"

Detect devices...: Opens a dialog for selecting the available devices.

Printer Port: "USB class printer"

If you use a lot of different printer models attached via USB, you can assign printer models to CUPS printers without specifying dependencies to a specific USB port. Instead, the USB printer is assigned by matching patterns specified under **Manufacturer pattern** and **Product pattern** with the specific model name. A single printer definition can thus work for a class of different USB printer models.

Pattern matching mode: Specifies the type of the search pattern.

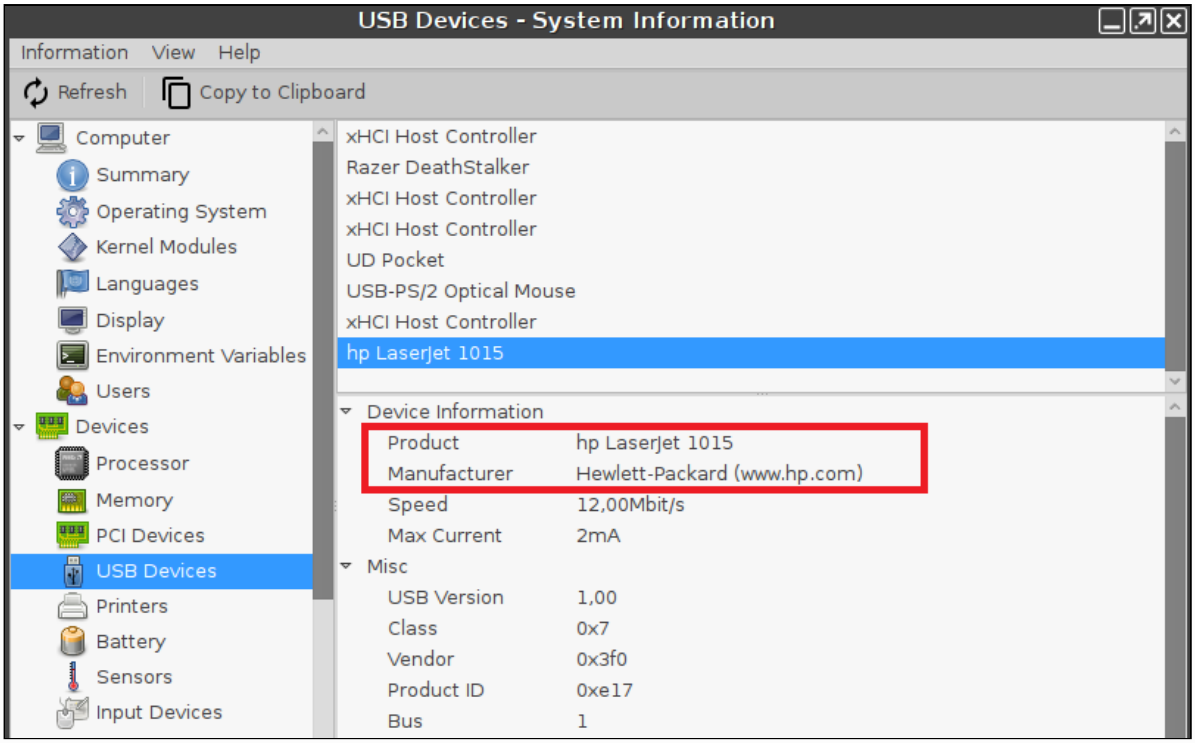
- "pattern": Standard wildcards are used for pattern matching, e.g. "*", "?". The matching is case sensitive. For detailed information on wildcards, see man7.org[228] and tldp.org[229]. (Default)
- "pattern, case insensitive": Standard wildcards are used for pattern matching, e.g. "*", "?". The matching is case insensitive.
- "regular expression": Regular expressions are used for pattern matching. For detailed information on regular expressions, see man7.org[230] and tldp.org[231].

Manufacturer pattern: Pattern matching the manufacturer name of the printer. If the pattern is empty, it is ignored.

Product pattern: Pattern matching the product name of the printer. If the pattern is empty, it is ignored.

Manufacturer and product names can be found in the accessories under **Devices** > **USB Devices > System Information**.

228. http://man7.org/linux/man-pages/man7/glob.7.html
229. http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm
230. http://man7.org/linux/man-pages/man7/glob.7.html
231. http://www.tldp.org/LDP/GNU-Linux-Tools-Summary/html/x11655.htm



Click to see examples...

Matching all printers whose product name contains "LaserJet":
Pattern matching mode: "pattern"
Product pattern: "*LaserJet*"

Matching all printers whose product name contains "LaserJet":
Pattern matching mode: "regular expression"
Product pattern: "LaserJet"

Matching all printers whose product name contains "LaserJet" or "DeskJet":
Pattern matching mode: "pattern"
Product pattern: "+(*LaserJet*|*DeskJet*)"

Matching all printers whose product name contains "LaserJet" or "DeskJet":
Pattern matching mode: "regular expression"
Product pattern: "LaserJet|DeskJet"

Printer Port: "LPD network printer"

LPD print server: Host name or IP address of the remote LPD printer.

LPD queue name: Name of the LPD printer queue.

Printer Port: "TCP network printer"

TCP print server: Host name or IP address of the remote TCP/JetDirect/Socket printer.

TCP port: TCP port number. (Default: 9100)

Printer Port: "IPP network printer"

IPP URI: URI of the IPP print server. Example: `ipp://myprinter.example.com/printers/printer1`

Printer Port: "SMB network printer"

SMB server: NetBIOS host name of the SMB server.

SMB workgroup: Workgroup or domain name. (Optional)

SMB printer: Share name of the printer.

SMB port: SMB port number. (Default: 0, which stands for standard ports 139 and 445)

Use Kerberos authentication

☑ Kerberos credentials are used for authentication on condition that Active Directory/Kerberos Logon has been configured. See Active Directory/Kerberos in IGEL OS (see page 2034).

☐ Kerberos credentials are not used for authentication. (Default)

Use passthrough authentication

☑ Single sign-on authentication is used on condition that Active Directory/Kerberos Logon or IGEL Shared Workplace have been configured. See Active Directory/Kerberos in IGEL OS (see page 2034) and Shared Workplace (see page 2037).

☐ Single sign-on authentication is not used. (Default)

SMB user name: User name used for authentication. (Optional)

SMB password: Password used for authentication. (Optional)

Printer Port: "LRS managed printer"

If you want to use LRS Virtual Session Printer Agent (VSPA) in IGEL OS, use the settings described under LRS (see page 1999). There is NO need to set **Printer port** to "LRS managed printer".

IPP Printer Sharing

Menu path: **Devices > Printer > CUPS > IPP Printer Sharing**

The IPP (Internet Printing Protocol) offers the following configuration options:

Network or host for sharing local printers: Access to the printer is possible from this network or host.

Possible options:

- "None" (Default)
- "Local network": Allows printing on the local device from the local network.

> This can also be given in the form `192.0.2.*` or `192.0.2.0/24` or `*.domain.com` or `192.0.2.1` or `host.domain.com`.

- "Global": Allows printing on the local device from the global network.

LPD

Menu path: **Setup > Devices > Printers > LPD**

LPD printers are used by the BSD printing system and are also supported by *Windows* servers.

- **Enable LPD Print Server**
  ☑ Local printers are provided in the network as LPD printers. The thin client is made the LPD print server. The CUPS printers defined under Printers (see page 1976) can be addressed under their printer name as a queue name via the LPD protocol. (default)
- **Print Filter**:
  - Automatic: Attempts to automatically recognize whether or not the print data need to be prepared by the local printer driver.
  - None: The print data are always forwarded unchanged to the printer.
- **Max. Consurrent Connections**: Limits the number of print jobs that can be accepted at the same time.
  - Unlimited
  - 1
  - 2
  - 3
- **Restrict LPD Access** - Specifies the sub-networks or hosts from which print jobs can be accepted.

→ Click on + to add an LPD network or a host to the list.

TCP/IP

Menu path: **Setup > Devices > Printers > TCP/IP**

You can assign printers connected to your device to a TCP/IP port.

_____

- COM 1 / 2 (see page 1987)
- Additional Serial Ports (see page 1989)
- LPT 1 (see page 1991)
- USBLP 1 (see page 1992)

COM 1 / 2

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

Activate TCP/IP printers on this port

☑ Maps the interface defined below in a TCP/IP port.

☐ Disabled (default)

TCP/IP port number
Port on which the interface is to be mapped (default: 3004).

Poll criterion
Criterion according to which the interfaces are mapped.

- Always: Maps constantly without polling.
- Online: Maps only if the printer is switched on.

Poll frequency
Amount of time between polls (default: 1 sec)

Speed
Input and output speed (default: 9600)

Parity
Parity bits that are to be used. Possible values:

- None
- Even
- Odd

Stop bits
Use up to two stop bits. (default: 1)

Word width
Sets the number of bits used per byte.

- 5
- 6
- 7
- 8

Use RTS/CTS flow control

☑ Hardware flow control will be used.

☐ Not used (default)

Use XON/XOFF flow control

☑ Software flow control by sending start/stop signs will be used.

☐ Not used (default)

Use DSR flow control

☑ Hardware flow control with DSR for output will be used.

☐ Not used (default)

Additional Serial Ports

Menu path: **Setup > Devices > Printers > TCP/IP > Additional Serial Ports**

TCP/IP printers on additional serial ports

→ Click on to add TCP/IP printers to the list.
A mask with the following settings options will open:

- **Activate TCP/IP printer on this interface**
  ☑ Maps the interface defined below in a TCP/IP port.
  ☐ Disabled (default)
- **Device name**: The printer can be connected to one of the following connections, provided that they are available on the device:
  - USB COM1
  - USB COM2
  - Perle COM1
  - Perle COM2

Data are forwarded bidirectionally at serial interfaces. This means that other serial devices such as barcode scanners or scales can be operated too.

- **Search for devices...**: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Designation** column shows the type of device file:
  - (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion. Example: `/dev/ttyUSB0`
  - (BY PORT) [device designation]: According to USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`
  - (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]`. Example: `/dev/usbserial/ttyUSB_V067b_P2303`
- **TCP/IP port number**: Port on which the interface is to be mapped (default: 9100).
- **Poll criterion**: Criterion according to which the interfaces are mapped.
  - Always: Maps constantly without polling.
  - DSR (M1): Maps only if the relevant line is set by the serial device.
  - DCD (M5): Maps only if the relevant line is set by the serial device.
- **Poll frequency**: Amount of time between polls (default: 1 sec)
- **Speed**: Input and output speed (default 9600 baud).
- **Parity**: Parity bits that are to be used. Possible values:
  - None
  - Even
  - Odd

- **Stop bits**: Use up to two stop bits. (default: 1)
- **Word width**: Sets the number of bits used per byte.
  - 5
  - 6
  - 7
  - 8
- **Use RTS/CTS flow control**
  ☑ Hardware flow control will be used.
  ☐ Not used (default)
- **Use XON/XOFF flow control**
  ☑ Software flow control by sending start/stop signs will be used.
  ☐ Not used (default)
- **Use DSR flow control**
  ☑ Hardware flow control with DSR for output will be used.
  ☐ Not used (default)

LPT 1

Menu path: **Setup > Devices > Printers > TCP/IP > COM 1**

- **Activate TCP/IP printers on this interface**
  ☑ Maps the interface defined below in a TCP/IP port.
  ☐ Disabled (default)
    - **TCP/IP port number**: Port on which the interface is to be mapped (default: 3004).
    - **Poll criterion**: Criterion according to which the interfaces are mapped.
      Always: Maps constantly without polling.
      Online: Maps only if the printer is switched on.
    - **Poll frequency**: Amount of time between polls (default: 1 sec)

USBLP 1

Menu path: **Setup > Devices > Printers > TCP/IP > USBLP 1**

Activate TCP/IP Printers on this Port:

☑ Maps the interface defined below in a TCP/IP port.

☐ Disabled (default)

- **TCP/IP Port Number**: Port on which the interface is to be mapped (default: 3004).
- **Poll Criterion**: Criterion according to which the interfaces are mapped.
  Always: Maps constantly without querying.
  Online: Maps only if the printer is switched on.
- **Poll Frequency**: Amount of time between status queries (default: 1 sec)

ThinPrint

Menu path: **Devices > Printer > ThinPrint**

ThinPrint allows the bandwidth provided for the transfer of print jobs to be reduced depending on the resources available. The ThinPrint client prints either on printers connected to a local interface (serial, parallel or USB), on an LPD network printer or on a CUPS printer defined on the thin client.

In this area, you will find the following parameters:

Port Number: Port number via which the ThinPrint daemon will communicate (default: 4000).

> Make sure that the port number on the ThinPrint client and the ThinPrint server is the same (communication will otherwise not be possible).

Bandwidth: A bandwidth value (in bits per second) which is lower than or equal to the value specified on the ThinPrint server. A higher value, the disabling of client control or no entry at all means that the ThinPrint server values will be used (default: 0).

Open Printer Interval: Maximum waiting time in seconds if a printer is unavailable (default: 165).

Open Printer Tries: Number of attempts to contact a printer in order to start a print job (default: 100).

- Printer (see page 1994)
- Connection Service (see page 1995)
- Encryption (see page 1996)

Printer

Menu path: **Devices > Printer > ThinPrint > Printer**

In this area, the **ThinPrint and ezeep Printers** are shown.

The page provides an overview of pre-configured ThinPrint printers.

->Click on + to add a printer to the list.
A mask with the following settings options will open:

Active: Indicates whether or not the printer is visible.

Printer Name: Name under which the printer can be addressed.

Printer Class Name: Name of the printer class - optional, max. 7 characters without spaces

Device: A device file or the printer name, e.g. /dev/ttyS1 (COM2).

Detect Devices...: Opens a mask for selecting the available devices.

Print Retries: Number of attempts to contact a printer in order to start a print job (default: 10).

Default: Defines the selected device as the default printer.

Connection Service

Menu path: **Setup > Devices > Printers > ThinPrint > Connection Service**

By default, the .print client waits for incoming connections from the print server. If the thin client is unavailable via the network from the print server, the connection can also be established from the thin client .

- **Connection Service ModeMode**:
  - Listen Mode: Receive print jobs without Connection Service. The .print client heeds incoming connections.
  - Static Mode: Use connection to receive print jobs. The .print client establishes a connection to the .print Connected Gateway.
  - Both: Use both modes.
- **Connection Server Address**: IP address of the computer on which the connection service runs.
- **Connection Service Port number**: The client port of the .print Connected Gateway (default: 4001)
- **Client D**: The ID of the client must be unique.
- **Connection Service Authentication key**: A value that is defined on the connection server.
- **Connection Service Retry Interval**: Waiting time in seconds until another connection attempt is made if the .print Connection Service is unavailable (default: 300)

Encryption

Menu path: **Setup > Devices > Printers > ThinPrint > Encryption**

In this area, you can enable encryption for print jobs.

- **Enable SSL Encryption**:
  ☑ The client can receive print jobs via an encrypted connection.
  ☐ Disabled (default)
- **SSL Root Certificate**: Path name of the file that receives the root certificate in the .pem format.
- **SSL Client Certificate**: Path name of the file that receives the client certificate in the .pem format.
- **SSL Client Certificate Password**

PrinterLogic

Menu path: **Setup > Devices > Printer > PrinterLogic**

If you are using PrinterLogic to provision printers, you are replacing the previous direct printer management from the Setup.

Instead, the administrator creates a website (on printercloud.com[232]) with the respective printers of the location(s). The setup user/administrator can then select the desired printers via the browser.

Manage printers by Printer Installer client:

☑ The printers will be managed by the Printer Installer client and not by the IGEL CUPS functionality (**IGEL Setup > Devices > Printers > CUPS**).

☐ No Printer Installer client is activated. The printers will be managed by the IGEL CUPS functionality. (default)

HomeURL protocol

Possible options:

- https://
- http://

HomeURL hostname: The host name of the web server running the printer cloud. Default: `printercloud.com`

Authorization code: Authorization code for the printer cloud; generated by the administrator.

> If you have successfully set up the printer cloud, this tray icon appears in the system tray.

Mapping in sessions

ICA sessions

☑ Include printers managed by PrinterLogic in ICA sessions. (default)

RDP sessions

☑ Include printers managed by PrinterLogic in RDP sessions. (default)

NX sessions

☑ Include printers managed by PrinterLogic in NX sessions.

☐ Don't printers managed by PrinterLogic in NX sessions. (default)

Parallels client sessions

☑ Include printers managed by PrinterLogic in Parallels client sessions.

☐ Don't include in Parallels client sessions. (default)

Show CUPS printers: Displays a list of installed printers that can be deleted.

232. http://printercloud.com

The PrinterLogic menu

Right-click the icon to get the following options:

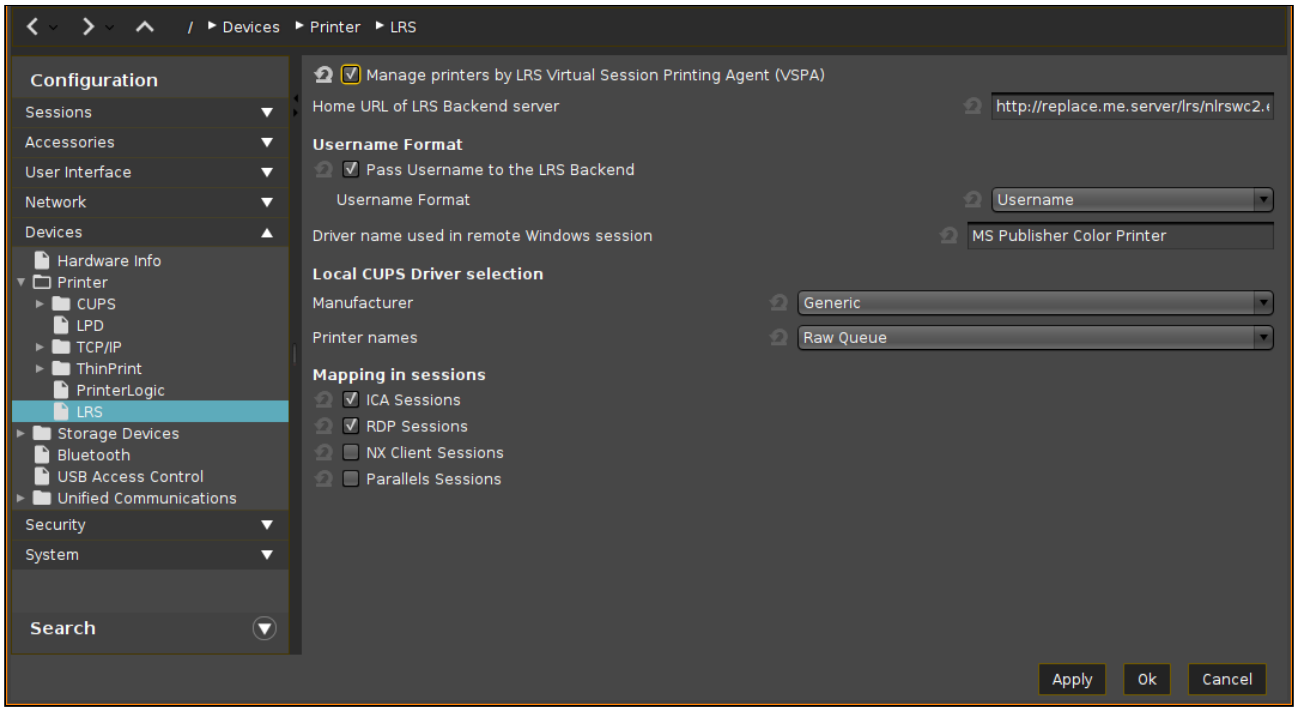
- **Add Printers...**: Opens the PrinterCloud in the browser. The installed printers are listed and can be installed via double-click.
- **Pull Printing...**: The print job is held and released by the user at each print device that supports this function.
  - **Print Job Management...**: Manages your print jobs.
  - **Secure Print Settings...**: Opens settings for secure printing.
- **Refresh Configurations**

LRS

The following article describes the settings for configuring LRS Printing Agent in IGEL OS. LRS Virtual Session Printer Agent (VSPA) allows you to redirect printers into remote sessions and associate users, terminals, and connected printers. For more information on LRS VSPA, see Virtual Session Printer Agent for VPSX[233]. See also IGEL Session Printer Agent for VPSX (ISPA)[234].

> To use LRS VSPA, make sure **LRS Output Management** is activated in the IGEL Setup under **System > Firmware Customization > Features**.

Menu path: **Setup > Devices > Printer > LRS**



Manage printers by LRS Virtual Session Printing Agent (VSPA)

☑ LRS Virtual Session Printer Agent is used.

☐ LRS Virtual Session Printer Agent is not used. (Default)

Home URL of LRS Backend server: Specify here the URL of your LRS Virtual Session Printer Agent server. (Default: http://replace.me.server/lrs/nlrswc2.exe/vpsx)

Username Format

Pass username to the LRS backend

233. https://www.lrsoutputmanagement.com/products/vpsx-product-extensions/vspa-for-vdi-environments/
234. https://www.lrsoutputmanagement.com/products/vpsx-product-extensions/igel-session-printer-agent-for-vpsx/

☑ The username is passed to the LRS backend. (Default)

☐ The username is not passed to the LRS backend. Any user can print.

Username format: Specify here the format in which the username should be passed to the LRS backend.
Possible values:

- **Username**
- **Domain\Username**
- **Username@Domain**

Driver name used in remote Windows session: Set the driver name for the printer to be used in remote sessions.

- By default, MS Publisher Color Printer is usually installed on Windows and works generically.
- In the case of a custom printer driver, make sure the driver is installed on the remote desktop (e.g. Citrix server, etc.) and enter here the exact name of the driver.

Local CUPS Driver Selection

The driver specified here will be used for local printing.

Manufacturer: List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Printer names**. (Default: Generic)

Printer names: List of possible printer models. (Default: Raw Queue)

Mapping in Sessions

ICA Sessions

☑ The printer is available in ICA sessions. (Default)

RDP Sessions

☑ The printer is available in RDP sessions. (Default)

NX Client Session

☑ The printer is available in NoMachine NX Client sessions.

☐ The printer is not available in NoMachine NX Client sessions. (Default)

Parallels Sessions

☑ The printer is available in Parallels Client sessions.

☐ The printer is not available in Parallels Client sessions. (Default)

If you want to use your own LRS solution, use the following registry key under **System > Registry**:

Parameter	Custom path to LRS software

Registry	`LRS.custom_path`
Type	string
Value	empty (default)

Unified Communications

- Jabra (see page 2003)
- EPOS Audio (see page 2006)

Jabra

- Jabra Xpress (see page 2004)
- Options (see page 2005)

Jabra Xpress

Menu path: **Devices > Unified Communications > Jabra > Jabra Xpress**

Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing a configuration of settings, firmware updates, etc. for Jabra devices. For more information, see https://www.jabra.com/supportpages/jabra-xpress#/.

For detailed information on how to deploy a Jabra Xpress package, see How to Deploy a Jabra Xpress Package (see page 1052).

Device Dashboard URL: URL of the dashboard server of the Jabra device.

Package: File name of the Jabra Xpress package. Example: `xpress_package_20190109_144111.zip`.

Source URL: URL to the directory containing the Xpress package. Example: `https://172.30.92.1:8443/ums_filetransfer/`

As a **Source URL**, you can specify any server, e.g. FTP(S) or HTTP(S), where you have placed the Xpress package downloaded from the Jabra Xpress portal.
If you want to use the UMS as a source location, your Jabra ZIP archive has to be registered as a file object in the UMS, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices (see page 2004). See also UMS and Thin Clients: File Transfer (see page 2004).

Check SSL certificate: Determines if the SSL certificate is checked. (Default: Enabled)

Disable SSL certificate checking if your HTTPS or FTPS server uses a self-signed certificate.

User name: User name for accessing the Xpress package that resides under the **Source URL**.

Password: Password for accessing the Xpress package that resides under the **Source URL**.

For the optimal performance of Jabra headsets (esp. relevant if Skype for Business is used), activate:

- in Citrix sessions: **HDX Realtime Media Engine** under **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**;
- in VMware Horizon sessions: **Virtualization Pack Skype for Business** under **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business**;
- in RDP sessions: **Compression** under **Sessions > RDP > RDP Global > Performance**.

Options

Menu path: **Devices > Unified Communications > Jabra > Options**

☑ **Suspend on idle**: Determines if the wireless Jabra USB audio device is set to the offline state after 5 seconds of idle time. (Default)

EPOS Audio

- EPOS Connect (see page 2007)

EPOS Connect

EPOS provides headset and conferencing solutions. For the supported EPOS headsets and speakerphones, see EPOS / Sennheiser Compatibility with IGEL OS (see page 12).

In IGEL OS, you can set up EPOS Connect, a client application that connects with EPOS Manager and sends device information and configuration to it. EPOS Manager performs the following tasks for EPOS devices that are connected to the endpoint:

- Firmware updates
- Remote asset management
- Remote configuration

> "Silent update" must be selected in EPOS Manager during the update. Otherwise, the update will not function.

For more information on EPOS Manager and EPOS Connect, see https://www.eposaudio.com/en/us/enterprise/software.

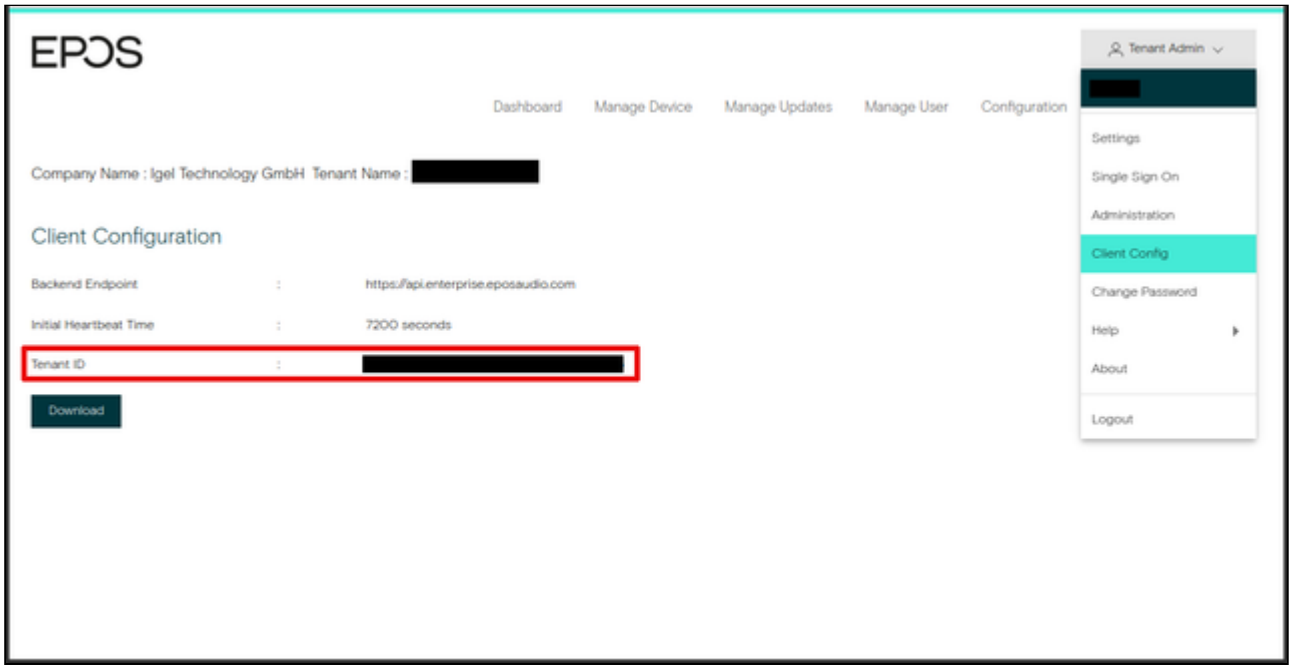
Menu path: **Devices > Unified Communications > EPOS Audio > EPOS Connect**

Enable EPOS Connect

☑ The EPOS Connect client is enabled.

Tenant ID

The customer-specific system ID for your EPOS Manager installation.



Backend Endpoint

URL of EPOS Manager

Proxy

URL of the proxy that connects to EPOS Manager, if applicable. The proxy URL must be provided in the format `[ADDRESS]:[PORT]`.

Bluetooth

Menu path: **Devices > Bluetooth**

In this area, you can set up a Bluetooth service.

Bluetooth

☑ The Bluetooth service is active. The Bluetooth Tool can be used.

☐ The Bluetooth service is inactive. The Bluetooth Tool cannot be used. (Default)

Tray Icon

☑ A Bluetooth icon will be shown in the system tray. You can launch the Bluetooth Tool by double-clicking on the Bluetooth icon. Right-clicking on the Bluetooth icon will bring up an overview as to which Bluetooth devices are connected to the thin client and you can enable or disable Bluetooth.

☐ A Bluetooth icon will not be shown in the system tray. (Default)

Details of the settings options for Bluetooth can be found under **Accessories >** Bluetooth Tool (see page 1788).

Here you can find information on the Bluetooth Assistant (see page 1217).

USB Access Control

Menu path: **Devices > USB Access Control**

You can allow or prohibit the use of USB devices on your endpoint. Specific rules for individual devices or device classes are possible. For an example, see How to Configure USB Access Control (see page 1097).

Enable

☑ USB access control is enabled and the following settings can be configured.

☐ USB access control is inactive. (Default)

> ⚠ The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.
> It is recommended to make settings for **USB Access Control** as the last step in the device configuration.
> Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.
> Note that the USB access control is completely separate than USB redirection for remote sessions, see When to Use USB Redirection (see page 1093).
> Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

Default rule: Specifies whether the use of USB devices is allowed or prohibited.

- Allow (Default)
- Deny

Default permission: Default access rights for USB devices.

- Read Only
- Read/Write (Default)

Class Rules

Class rules apply to USB device classes.

→ Click on + to create a new rule.
An input mask with the following options will open:

Rule: Specifies whether the use of the device class defined here is allowed or prohibited.

Class ID: Device class for which the rule should apply. (Examples: **Audio**, **Printers**, **Mass Storage**).

Name: Name of the rule

Device Rules

Device rules apply to specific USB devices.

→ Click on + to create a new rule.
An input mask with the following options will open:

Rule: Specifies whether the use of the device defined here is allowed or prohibited.

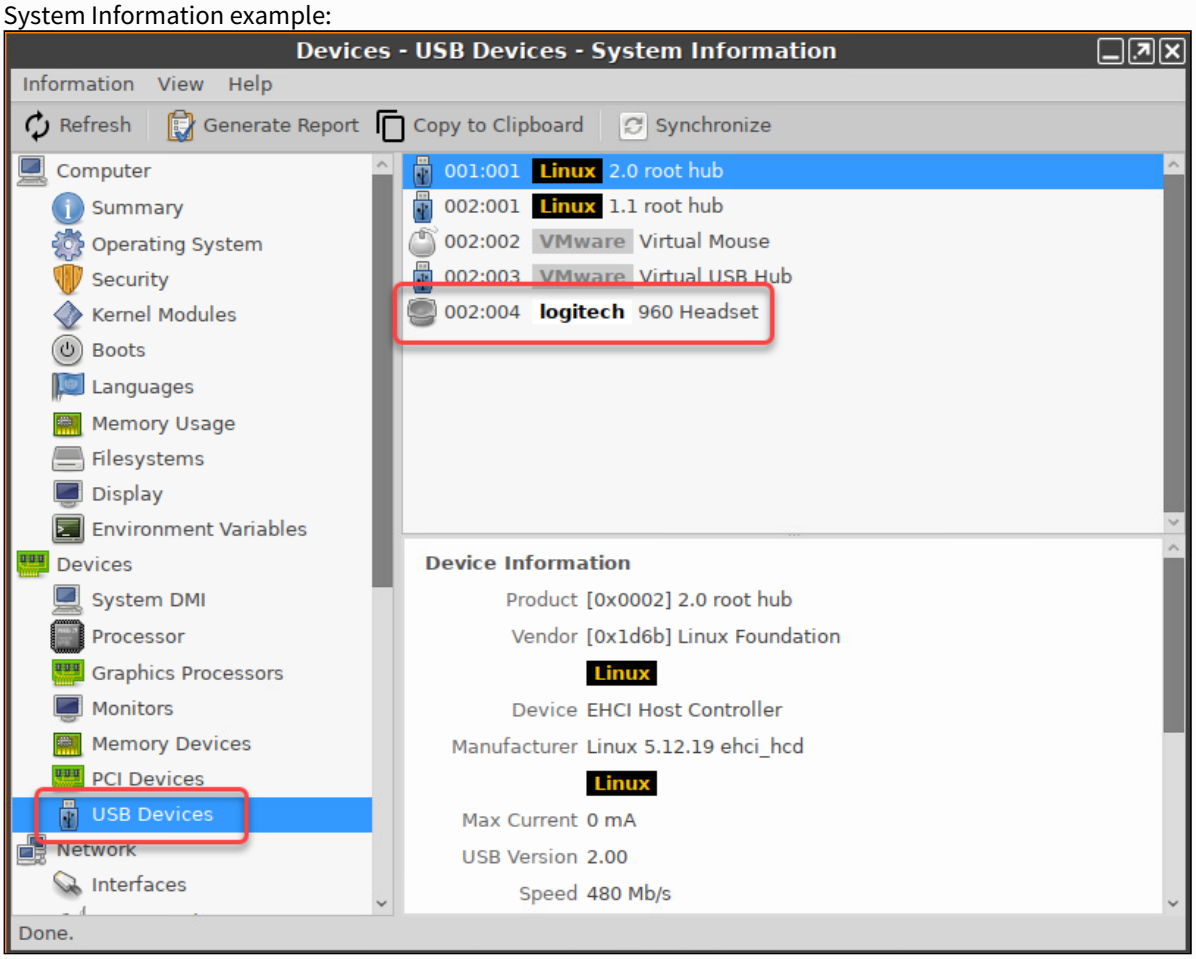
Vendor ID: Hexadecimal ID of the device manufacturer

Product ID: Hexadecimal ID of the device

Getting USB Device Information

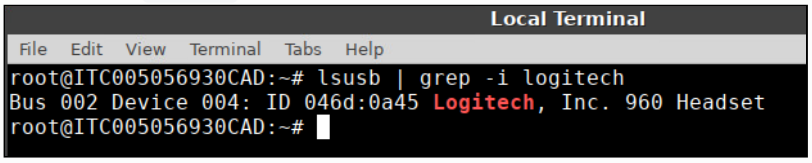
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see Using System Information Function (see page 1797).

System Information example:



Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



Device uuid: Universal Unique Identifier of the device

Permission: Authorizations for access to the device
Possible values:

- Global setting: The default setting for hotplug storage devices is used; see the **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**. (Default)
- Read only
- Read/Write

Name: Name of the rule

Further setting options can be found under Storage Hotplug (see page 1969).

Security

Menu path: **Setup > Security**

In order to prevent unauthorized access to the thin client setup, it is important to set up an administrator password after the initial configuration. With an additional user password, you can allow the user to make limited changes to the configuration.

Further information can be found under Password - Restrict Access to IGEL OS Components (see page 2017).

_____

- Active Directory/Kerberos (see page 2014)
- Password - Restrict Access to IGEL OS Components (see page 2017)
- Device Encryption for IGEL OS (see page 2021)
- Smartcard (see page 2024)
- Logon (see page 2030)

Active Directory/Kerberos

Menu path: **Setup > Security > Active Directory / Kerberos**

Enable

☑ The Kerberos basic configuration will be carried out.

☐ The Kerberos basic configuration will not be carried out. (default)

Default domain (Fully Qualified Domain Name): This value must match the Windows domain on which the logon is to take place, e.g. `EXAMPLE.COM`.

> The value must be entered in upper case letters.

DNS lookup for domain controller

☑ In order to find the key distribution centers (KDCs, domain controllers) and other servers for a realm, DNS SRV records are used if they are not explicitly indicated. (default)

☐ The key distribution centers entered under **Setup > Security > Active Directory/Kerberos > Domain 1** ... **Domain 4** will be used.

DNS lookup for domain

☑ In order to determine the Kerberos realm of a host, DNS TXT records are used. (default)

☐ The details under **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping** are used.

Obtain addressless tickets

☑ The first Kerberos ticket is addressless. This may be necessary if the client is located behind an NAT device (Network Address Translation). (default)

- Domain 1 ... Domain 4 (see page 2015)
- Domain Realm Mapping (see page 2016)

Domain 1 ... Domain 4

Menu path: **Setup > Security > Active Directory/Kerberos > Domain 1 ... Domain 4**

Up to 4 domains where a login is possible can be configured here.

To configure a domain, proceed as follows:

1. Under **Domain name**, give the name of the domain (Kerberos realm).
2. Click + to create a new entry.
3. Under **Domain controller**, give the name or IP address of the domain controller (Kerberos key distribution center). A port number can be added to the host name; the port name must be preceded by a colon.
4. Click on **Continue**.
   The domain controller will be added to the **Domain controller list**.

Domain Realm Mapping

Menu path: **Setup > Security > Active Directory / Kerberos > Domain Realm Mapping**

With domain realm assignment, a host name is translated into the corresponding Kerberos realm name.

- **Use default DNS domain - Active Directory domain mapping**
  ☑ The DNS name and Active Directory domain name match. (default)
  ☐ DNS name and Active Directory domain name assignments must be set up.

To set up a DNS name to Active Directory domain name assignment proceed as follows:

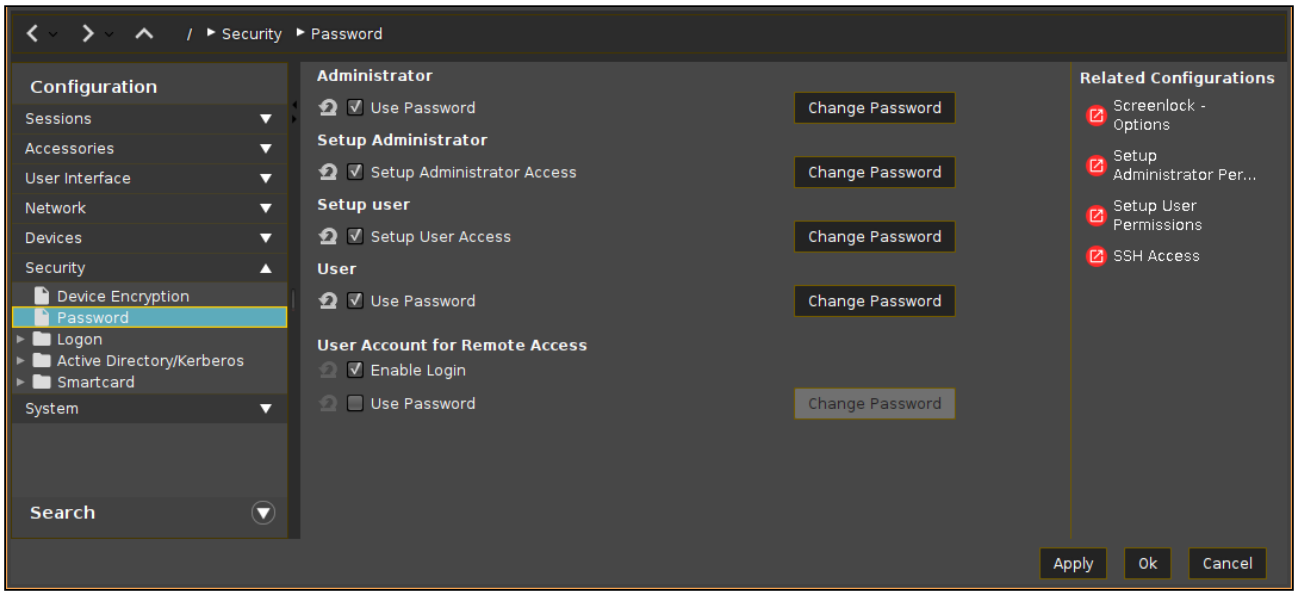
1. Click ⊞ to create a new entry.
2. Under **DNS host or domain name**, enter the host name that is to be assigned to an Active Directory domain name.
3. Under **Active Directory domain name**, enter the Active Directory domain name that is to be assigned to the host name.☑
4. Click on **Continue**.
   The data entered will be added to the **Domain realm mapping** list.

Password - Restrict Access to IGEL OS Components

The following article provides details on different authorization levels in IGEL OS, which you can configure to protect your endpoint devices against unwanted changes. You will learn the difference between the access for **administrator** and **setup administrator**, for **user** and **setup user**.

For a general overview on securing your devices, see Securing IGEL OS Endpoints (see page 666).

Menu path: **Security > Password**



You can assign four different authorization levels:

Administrator: The administrator has full access to the IGEL Setup.

> The assignment of the administrator password is a prerequisite for all other rights assignments. Even if the administrator wants to leave the administration of the IGEL Setup to the setup administrator, the administrator password must be set.
> An administrator password protects the following critical actions/areas from unauthorized access:
> - the reset to factory defaults (see page 1225) in the boot menu
> - the local terminal (see page 1711)
> - the virtual console access (see page 1895).

Setup Administrator: A user to whom rights are assigned for minor administrative tasks. You specify which pages the setup administrator can edit under **Accessories > Setup > Setup Administrator Permissions** (see page 1723).

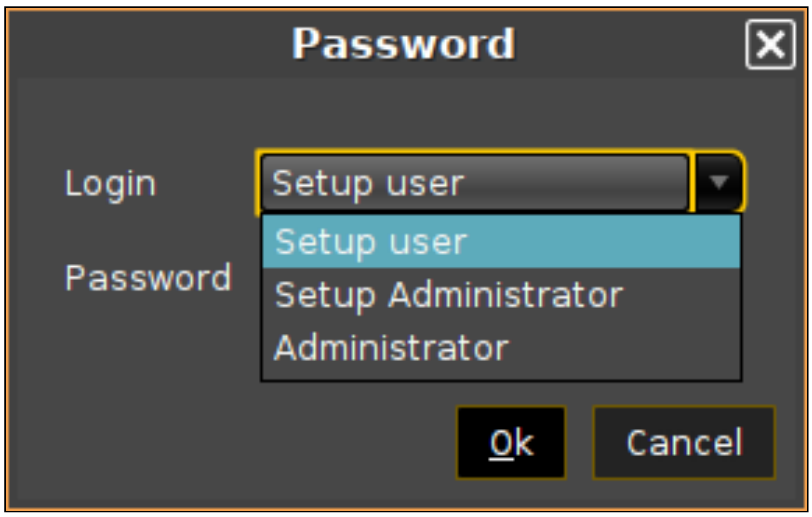
Setup User: A user who can make some unlocked user settings in the IGEL Setup. You specify which pages the setup user can edit under **Accessories > Setup > Setup User Permissions** (see page 1721).

User: This user has no access to the IGEL Setup. A user password is required in the following cases:

- when logging on to the terminal session (see page 1711)
- when logging on to sessions (see Desktop Integration)

- for unlocking the screenlock (see page 1846)

If you have defined passwords for different authorization levels, a login window appears at the start of the IGEL Setup in which you can select an authorization level:



When entering a password, ensure that the correct keyboard layout (see page 1874) is enabled.

Administrator

Use password

☑ A password is needed to log in as administrator (`root`).

- A password is also needed for the user, the setup user, and the setup administrator.
- The password is set by clicking **Change Password**.

☐ No password is needed to log in as an administrator. Also, no password is needed for the user (`user`), the setup user, and the setup administrator.*

Change Password

Sets a new password for the administrator (`root`).

Effects on local terminal access

Setting an administrator password has the following effects on the access to local terminals:

- For logging in as `root` , the administrator password must be entered.
- Logging in as `user` is no longer possible.

However, you can allow access for `user` by making the following settings:

- Enable the registry key `system.security.usershell` (Default: Disabled).
- Set a user password.

For logging in as `user`, the user password will have to be entered. (See the "User" section of this page).

Setup Administrator

Setup Administrator Access

This option is relevant if an administrator password is set.

☑ The setup administrator can access the areas of the IGEL Setup for which he has authorization. Further information can be found under Setup Administrator Permissions - Define Access to IGEL Setup Areas (see page 1723).

- A password is needed to log in as setup administrator.
- The password is set by clicking **Change Password**.

☐ The setup administrator cannot access the IGEL Setup.*

Change Password

Sets a new password for the setup administrator.

Setup User

Setup User Access

This option is relevant if an administrator password is set.

☑ The setup user can access the areas of the IGEL Setup for which he has authorization. Further information can be found under Setup User Permissions - Define Access to IGEL Setup Areas (see page 1721).

- A password is needed to log in as a setup user.
- The password is set by clicking **Change Password**.

☐ The user cannot access the IGEL Setup.*

Change Password

Sets a new password for the setup user.

User

Use Password

This option is relevant if an administrator password is set.

☑ The user (`user`) needs a password in order to log in to the device via the local terminal. The password is set by clicking **Change Password**.

☐ If an administrator password is set, the user (`user`) cannot log in to the device via the local terminal. If no administrator password is set, the user (`user`) can log in to the device via the local terminal without a password.*

Change Password

Sets a new password for the user (`user`).

User Account for Remote Access

Enable Login

☑ The remote user (`ruser`) can log in to the device via SSH. Further information can be found under SSH Access (see page 2044).*

☐ Logging in via SSH is not possible.

Use Password

☑ A password is needed to log in via SSH.

☐ No password is needed to log in via SSH.*

Change Password

Sets a new password for the remote user (`ruser`).

---

*IGEL OS system default

Device Encryption for IGEL OS

If you want to strengthen the security of your endpoint device, you can deploy strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

Menu path: **Security > Device Encryption**

Device encryption mode

Possible options:

- **Keep**: The default encryption scheme is maintained. If a password has been set, it will remain unchanged.
- **Activate**: The device will be re-encrypted using strong encryption methods when the user enters the password for the first time. It is strongly recommended to enforce the use of a strong password; see Minimum Password Length (see page 2022) and the subsequent password settings. The re-encryption may take about 10 to 60 seconds; the duration depends on the hardware performance and the size of the Custom Partition.
- **Deactivate**: The device will be re-encrypted back to the default device encryption scheme on the next boot. The re-encryption may take about 10 to 60 seconds.

  ⚠ If you want to switch back to the default device encryption, you must have the password. If the password gets lost, you must reinstall IGEL OS 11 on the device, e. g. via OSC (see Installation (see page 2125)).

Change password

Only applicable if device encryption is enabled. The user can change the password for device encryption.

Authentication type

Possible options:

- **PW**: Password authentication. In this version of IGEL OS, this is the only available authentication type.

Security level

Possible options:

- **Auto, constant-time**: The password aggregation function that fits best with the defined **Target time delay (ms)** is selected.
- **Auto, at least level**: The security level will be at least as high as the value selected by **Password aggregation function**; if the **Target time delay (ms)** allows for a higher security level, the higher security level will be used.

- **Manual**: The **Password aggregation function** can be set manually, irrespective of the delay time specified by **Target time delay (ms)**.

Target time delay (ms)

Maximum time that should be consumed by the password aggregation function. This delay is effective when the user enters the device encryption password on boot or changes the device encryption password.

Password aggregation function

Security level of the encryption.

Possible options:

- **I: Argon2id, 8M/7 ops**
- **II: Argon2id, 128M/3 ops**
- **III: Argon2id, 256M/3 ops**
- **IV: Argon2id, 512M/3 ops**
- **V: Argon2id, 1024M/4 ops**
- **VI: Argon2id, 128M/4 ops**

Minimum password length

Minimum number of characters the password must be composed of

Unwanted strings in password (comma separated)

Comma-separated list of strings that must not be contained in the password

The password must contain

Defines whether all of the subsequent minimum requirements (minimum amount of lower case letters etc.) must be fulfilled, or 2, or 3 of them.

- **all**
- **2 of**
- **3 of**

Minimum amount of lower case letters

The minimum amount of lower case letters

Minimum amount of upper case letters

The minimum amount of upper case letters

Minimum amount of numbers

The minimum amount of numbers

Minimum amount of special characters

The Minimum amount of special characters

Special characters allowed

List of all non-alphanumerical characters that are allowed in the password, without separators

Smartcard

Menu path: **Setup > Security > Smartcard**

Here, you can define settings for logging on using a smartcard.

_____

- Services (see page 2025)
- Middleware for Smartcards in IGEL OS (see page 2027)

Services

Menu path: **Setup > Security > Smartcard > Services**

The PC/SC service enables the smartcard reader to connect to the device, so that the smartcard is available to an application. This can be a server-side application where the data are forwarded via an RDP or ICA connection or a local application, e.g. the browser.

Enable PC/SC daemon

☑ The PC/SC service is enabled. The card reader is available for applications. (Default)

☐ The PC/SC service is disabled. The card reader is not available.

Currently active PC/SC devices: List of smartcard readers currently connected to the device. Internal smartcard readers and a variety of USB smartcard readers are supported.
You will find a list of supported smartcard readers in the IGEL Hardware Database[235].
See also Smartcard Readers Supported by IGEL Smartcards (see page 790).

Cherry USB2LAN proxy

☑ The Cherry USB2LAN proxy is active and makes Cherry electronic health card devices available in the network via SICCT and HTTPS.

☐ The Cherry USB2LAN proxy is disabled. (Default)

Bind interface: Network interface used for the proxy.
This parameter is available if **Cherry USB2LAN proxy** is enabled.
Possible options:

- "auto": The first network interface with IPv4 address will be used if **Bind IP** (see below) is set to "auto".
- "eth0": The Ethernet interface will be used.
- "wlan0": The WLAN interface will be used.
- Free text entry: The manually entered network interface will be used.

> The Ethernet and WLAN interfaces can be configured under **Network > LAN Interfaces**. See LAN Interfaces (see page 1899).

Bind IP: The IP address used for the proxy.
Possible options:

- "auto": The first network interface with an IPv4 address will be used if **Bind interface** is set to "auto".
- Free text entry: The manually entered IP address will be used instead of the network interface specified under **Bind interface**.

HTTPS server port: The TCP port for the HTTPS server. (Default: 443)

SICCT announce IP: The IP address to send the SICCT announce messages to.
Possible options:

235. https://www.igel.com/linux-3rd-party-hardware-database/

- "broadcast": SICCT announce messages are sent in a broadcast procedure, i.e. to all devices on the network.
- Free text entry: SICCT announce messages are sent to the manually entered IP address.

SICCT announce port: UDP port for SICCT announce messages. (Default: 4742)

SICCT announce interval: Time interval in seconds for sending out SICCT announce messages.
Value range: 5 to 1800 (Default: 30)

USB fast mode

☑ Faster connection to a Cherry eGK device is enabled.

☐ Faster connection to a Cherry eGK device is disabled. (Default)

In order for the changes of this setting to be applied, the device must be unplugged and connected again.

Alternative initialization method for G87-1505

☑ Alternative initialization method for Cherry eGK keyboard G87-1505 is enabled.

☐ Alternative initialization method for Cherry eGK keyboard G87-1505 is disabled. (Default)

Middleware for Smartcards in IGEL OS

In comparison to simply using passwords, two-factor authentication with a smartcard or smart token offers an additional layer of security. When configuring login with a smartcard, you have to define smartcard middleware to be used. In this area of the IGEL Setup, you select the middleware (PKCS#11 module) which matches your card or your token. Alternatively, you can specify here your own PKCS#11 module.

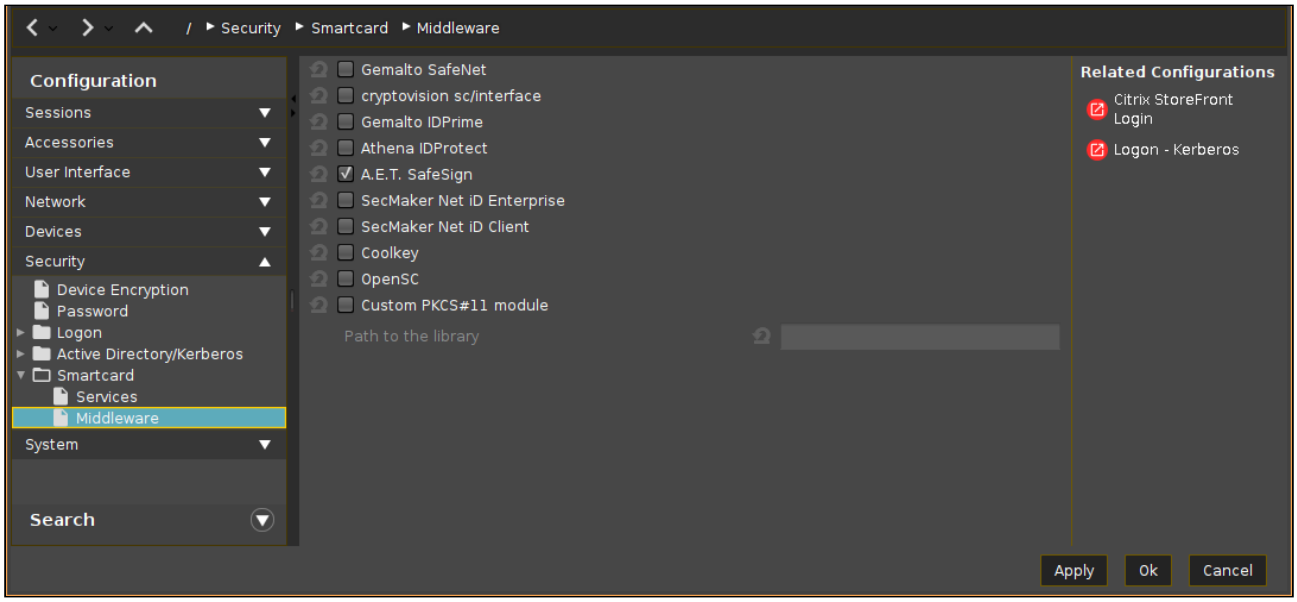
The middleware selected here will be used for the following logins:

- Login to Citrix sessions; see Citrix Global (see page 1248)
- Login to Citrix StoreFront; see Citrix StoreFront (see page 1294)
- Login to an endpoint device via Active Directory; see Active Directory/Kerberos[236]

For more information on smartcard authentication in IGEL OS, see the how-to Smartcard Authentication in IGEL OS (see page 791).

If you use IGEL smartcards, see Authentication with IGEL Smartcard (see page 782).

Menu path: **Security > Smartcard > Middleware**



For smartcard authentication to Citrix and Active Directory / Kerberos, you can use several middleware libraries at the same time. The concurrent usage of multiple smartcard middleware libraries may be required, for example, if multiple users with different smartcard types must have access to the device. **Note**: If no middleware is activated, OpenSC is used as a fallback.

Gemalto SafeNet

The middleware for Gemalto/SafeNet eToken, IDPrime smartcards and Token is used.

236. https://kb.igel.com/en/igel-os/11.10/active-directory-kerberos

cryptovision sc/interface

The middleware for cryptovision smartcards is used.

Gemalto IDPrime

The middleware for Gemalto IDPrime smartcards is used.

> Enable this Gemalto middleware when you want to operate Gemalto Common Criteria devices in unlinked mode.

Athena IDProtect

The middleware for Athena IDProtect smartcards is used.

A.E.T. SafeSign

The middleware for SafeSign smartcards is used.

SecMaker Net iD Enterprise

The SecMaker Net iD Enterprise middleware, formerly known as "Secmaker Net iD", is used.

> Enable this SecMaker middleware if you use Net iD implementation with CID (Certificate Identity Declaration).

SecMaker Net iD Client

The SecMaker Net iD Client middleware is used. SecMaker Net iD Client is the next generation of Net iD Enterprise, see http://docs.secmaker.com/net-id-client/latest/index.html.

> The SecMaker Net iD Client must also be installed on the server side.

Coolkey

The middleware Coolkey is used.

OpenSC

The middleware OpenSC is used.

90meter

The 90meter middleware is used.

Licensed Feature

This feature requires an add-on license. Please contact your IGEL reseller.

Custom PKCS#11 module

The PKCS#11 module stored under the **Path to the library** is used. See also Using a Custom PKCS#11 Library (see page 922).

In case of the installation of a custom PKCS#11 library, the file(s) (in `.so` format) must be placed on the endpoint device either via UMS file transfer or Custom Partition (see page 852).
The use of the `/wfs` folder is NOT recommended because of its space limit.

Path to the library

Path to the custom PKCS#11 module. Example: `/usr/lib/pkcs11/[name of the library].so`

Logon

Menu path: **Setup > Security > Logon**

_____

- IGEL Smartcard (see page 2031)
- Taskbar (see page 2032)
- Active Directory/Kerberos in IGEL OS (see page 2034)
- Shared Workplace (see page 2037)
- Local User (see page 2039)

IGEL Smartcard

Menu path: **Setup > Security > Logon > IGEL Smartcard**

Login with IGEL smartcard

☑ You can log in to the device using a smartcard. Depending on the configuration, a password may also be needed. Sessions stored on the smartcard become available.

☐ The desktop can be used without an IGEL smartcard. (Default)

Enable IGEL smartcard without locking desktop

☑ Enables sessions stored on the smartcard after entering an optional password. The device is not locked – even without a smartcard.

☐ The device will be locked after the removal of the smartcard. (Default)

On smartcard removal, terminate
This parameter is available if **Enable IGEL smartcard without locking desktop** is activated.
Possible options:

- "All sessions": When the card is removed, all sessions are ended.
- "Sessions originating from smartcard": When the card is removed, all sessions stored on the card are ended. Other sessions are not affected.

Company key: A shared code for a smartcard and a device. The code entered must match the code stored on the IGEL smartcard. If two codes do not match, the IGEL smartcard cannot be used on this terminal.

> Save the settings before starting to personalize the card.

Start application to write IGEL smartcards:

Smartcard personalization: Opens a window where you can set a login password and add sessions to the card.

> Session configurations are stored on the card's integrated circuit, and the session can be used on any IGEL device that reads the card.

> Smartcard personalization is possible via the local Setup only. The option is not available via the UMS.

For further information about the smartcard personalization function, see Using Smartcard Personalization Function (see page 1816).

For information on how to create IGEL smartcards via the UMS, see Authentication with IGEL Smartcard (see page 782).

See also Smartcard Readers Supported by IGEL Smartcards (see page 790).

Taskbar

Menu path: **Setup > Security > Logon > Taskbar**

There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, they appear automatically if the option **Enable tray icon** is activated under **Setup > Network > LAN Interfaces > Interface 1** (or **Interface 2**, **Wireless**) and/or under **Setup > Network > Mobile Broadband** (and/or **VPN**).

The network connection icons in the login dialog and on the locked screen, with the exception of the Wi-Fi icon, serve for information purposes only and thus are inactive on clicking.
The Wi-Fi icon invokes Switch for the Wi-Fi Connection (see page 1912) or the Wireless Manager (see page 1910) in case it is activated under **Setup > Network > LAN Interfaces > Wireless**.

Taskbar settings for the login dialog

- **Show taskbar in login screen**
  ☑ The taskbar will be shown during the login dialog. (Default)
  ☐ The taskbar will not be shown during the login dialog.
- **Show clock**
  ☑ The clock will be shown during the login dialog. (Default)
  ☐ The clock will not be shown during the login dialog.
- **Show keyboard layout switcher**
  ☑ The switch for the keyboard layout will be shown during the login dialog. (Default)
  ☐ The switch for the keyboard layout will not be shown during the login dialog.
- **Show on-screen keyboard button**
  ☑ The button for opening the on-screen keyboard is shown during the login dialog.
  ☐ The button for opening the on-screen keyboard is not shown during the login dialog. (Default)
- **Start on-screen keyboard automatically**
  ☑ The on-screen keyboard is open during the login dialog.
  ☐ The on-screen keyboard is not open during the login dialog. (Default)
- **Show reboot button**
  ☑ The button for rebooting the thin client is shown during the login dialog.
  ☐ The button for rebooting the thin client is not shown during the login dialog. (Default)
- **Show shutdown button**
  ☑ The button for shutting down the thin client is shown during the login dialog. (Default)
  ☐ The button for shutting down the thin client is not shown during the login dialog.

Taskbar settings when the screenlock is active

- **Show taskbar in screenlock**
  ☑ The taskbar is shown while the screen is locked. (Default)
  ☐ The taskbar is not shown while the screen is locked.
- **Show clock**
  ☑ The clock is shown while the screen is locked. (Default)

☐ The clock is not shown while the screen is locked.

- **Show keyboard layout switcher**
  ☑ The switch for the keyboard layout is shown while the screen is locked. (Default)
  ☐ The switch for the keyboard layout is not shown while the screen is locked.
- **Show on-screen keyboard button**
  ☑ The button for opening the on-screen keyboard will be shown while the screen is locked.
  ☐ The button for opening the on-screen keyboard will not be shown while the screen is locked. (Default)
- **Start on-screen keyboard automatically**
  ☑ The on-screen keyboard will remain open while the screen is locked.
  ☐ The on-screen keyboard is not open while the screen is locked. (Default)
- **Show reboot button**
  ☑ The button for rebooting the thin client is shown while the screen is locked.
  ☐ The button for rebooting the thin client is not shown while the screen is locked. (Default)
- **Show shutdown button**
  ☑ The button for shutting down the thin client is shown while the screen is locked.
  ☐ The button for shutting down the thin client is not shown while the screen is locked. (Default)
- **Show logoff button**
  ☑ The button for logging off is shown while the screen is locked.
  ☐ The button for logging off is not shown while the screen is locked. (Default)

Active Directory/Kerberos in IGEL OS

Menu path: **Setup > Security > Logon > Active Directory / Kerberos**

In this area, you can enable local login to the device via the Kerberos protocol. Active Directory/Kerberos must be configured, see Active Directory/Kerberos (see page 2014).

The login can be used for single sign-on in a number of session types (ICA, RDP).

- **Login to Active Directory domain**
  ☑ You can log in to the device via Active Directory.
  ☐ You cannot log in to the device via Active Directory. (Default)

Login Methods

- **Explicit**:
  ☑ You can log in with a user name and password. (Default)
  ☐ You cannot log in with a user name and password. If logging in with a smartcard is set up, you can log in with a smartcard.
- **Remember last user name**
  ☑ The login dialog will be prepopulated with the last user name that logged on. **Explicit** must be enabled for this.
  ☐ The login dialog will not be prepopulated. (Default)
- **Smartcard**
  ☑ You can log in using a smartcard.
  ☐ You cannot log in using a smartcard. (Default)

Select the smartcard type under **Security > Smartcard > Middleware**.

- **Smartcard removal action**: Specifies what action is performed when the smartcard via which the user is logged in is removed.
  Possible actions:
  - Log out: The user is logged out from the device.
  - Lock device: The screen is locked.

Logout Shortcut Locations

The start options for the logoff function are specified here.

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=JxGOEGAb3LI

Shared Workplace

Menu path: **Setup > Security > Logon > Shared Workplace**

- **Activate IGEL Shared Workplace**
  ☑ You can log in to the thin client via IGEL Shared Workplace.
  ☐ You cannot log in to the thin client via IGEL Shared Workplace. (Default)
- **Skip lGEL Shared Workplace login if UMS server is unavailable**
  ☑ If the *UMS* server is not available, the user can log in via Active Directory/Kerberos. In order to do this, logging in via Active Directory/Kerberos must be configured; further information can be found under Active Directory/Kerberos[237].
  ☐ Logging in is only possible if the *UMS* server is available. (Default)
- **Remember last user name**
  ☑ The login dialog will be prepopulated with the last user name that logged on.
  ☐ The login dialog will not be prepopulated. (Default)

Logout Shortcut Locations

The start options for the logoff function are specified here.

- **Start menu**: If this option is enabled, the session can be launched from the start menu.
- **Application Launcher**: If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop**: If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel**: If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system tab**: If this option is enabled, the session can be launched with the start menu's system tab.
- **Application Launcher's system tab**: If this option is enabled, the session can be launched with the Application Launcher's system tab.
- **Desktop context menu**: If this option is enabled, the session can be launched with the desktop context menu.
- **Menu folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.
- **Path in the Application Launcher**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.
- **Desktop folder**: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.
- **Password protection**: Specifies which password will be requested when launching the session. Possible values:
  - **None**: No password is requested when launching the session.
  - **Administrator**: The administrator password is requested when launching the session.

237. https://kb.igel.com/en/igel-os/11.10.270/active-directory-kerberos-in-igel-os

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

- **Hotkey**:
  ☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.
- **Modifiers**: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`. Here, you will find the available modifiers and the associated key symbols:
  - (No modifier) = `None`
  - = `Shift`
  - [Ctrl] = `Ctrl`
  - = `Super_L`
  - [Alt] = `Alt`

  Key combinations are formed as follows with `|`:
  - Ctrl + = `Ctrl|Super_L`
- **Key**: Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Local User

Menu path: **Setup > Security > Logon > Local User**

Login with local user password

☑ Upon the start of the device, a login screen is shown and authentication with a local user password is enabled. A password specified under **Set password** is deployed to log in. This password will also be used for **User Interface > Screenlock / Screensaver > Options > Local user password** (previously called **Screenlock password**), see Options (see page 1849).
If both Active Directory/Kerberos in IGEL OS (see page 2034) and login with local user password are enabled, you can choose on the login screen which login method you want to use.

☐ Authentication with a local user password upon device startup is disabled.

Logout Shortcut Locations

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

System

Menu path: **Setup > System**

You can configure basic system settings here.

_____

- Time and Date (see page 2042)
- Remote Access (see page 2043)
- Remote Management in IGEL OS 11 (see page 2050)
- Logging (see page 2053)
- Update (see page 2055)
- Power Options (see page 2062)
- Firmware Customization (see page 2068)
- Registry (see page 2099)

Time and Date

Menu path: **Setup > System > Time and Date**

- **Timezone Continent/Area**: Continent/Area for your location
  Possible values:
  - General: Under **Location**, you can select a time zone.
  - Africa... Pacific: Under **Location**, you can select a city for the selected continent/area.
- **Location**: Select your location or time zone.

  Please note that the GMT time zones under Linux are usually in POSIX format. This means that you need to invert the actual time difference (e.g. for New York you select the zone "GMT+5" for "5 hours west of Greenwich" although the time in New York is actually 5 hours behind GMT). Defining the time zone by selecting a **Continent** and **Location** is therefore preferable.

- **Use NTP Time Server**
  ☑ The system clock is set via NTP.
  ☐ The system clock is not set via NTP. (default)
- **Use NTP Time Server**: IP or name of an NTP time server. If you would like to enter a list of NTP time servers for redundancy purposes, separate the servers with spaces.
- **Set time and date**: Carries over the time and date and sets the hardware clock.
  You will find further information regarding the updating of time zone information (e.g. summer time adjustments) in the Updating Timezone Information (Daylight Saving Time, DST)[238] FAQ.

You can also use the registry key **system.time.hwclock_timezone** to set the hardware clock.
Possible options:
- **Auto** (default)
- **UTC**
- **Localtime**

IGEL OS and Windows have different default time settings, IGEL OS using UTC and Windows using local time. When using IGEL UD Pocket with Windows, this would lead to Windows interpreting the real time clock as set to local time and show the wrong time. To avoid this, the **Auto** setting looks for Windows partitions and, if present, assume that Windows is installed and the real time clock is automatically set to local time.

238. https://kb.igel.com/en/igel-os/11.10.270/updating-timezone-information-daylight-saving-time

Remote Access

Menu path: **Setup > System > Remote Access**

In order to allow central administration, the thin client can be configured in such a way that it can be accessed via the WAN.

_____

- SSH Access (see page 2044)
- Shadow Settings in IGEL OS (see page 2046)
- Secure Terminal (see page 2049)

SSH Access

Menu path: **Setup > System > Remote Access > SSH Access**

Remote access to the local system via SSH is permitted by default. However, you can restrict remote access to a specific user from a specific host.

Enable

☑ The SSH service is enabled. (default)

Permit empty passwords

☑ Logging on without a password is allowed.

☐ Logging on without a password is not allowed. (default)

Permit administrator logon:

☑ Logging on as an administrator is allowed.

☐ Logging on as an administrator is not allowed (default)

Port number: Port number for SSH (default: 22)

User access

User name: Permitted user
Possible values:

- root
- user
- ruser

> For the **user name** "ruser" a password has to be assigned under **Security > Password**. The names "root" and "user" work also without passwords.

Hostname: Name of the host from which SSH access takes place (example: `xterm.igel.de`)

Deny

☑ Access is denied.

☐ Access is allowed. (default)

Permit X11 forwarding:

☑ X11 forwarding is enabled.

☐ X11 forwarding is disabled. (default)

Enable applications access for remote user “ruser”

Command line: Command that is allowed or prohibited for the remote user

Enable application

☑ The application given under **command line** may be executed by the remote user. (default)

☐ The application given under **command line** may not be executed by the remote user.

Unlike **root** and **user**, the **ruser** is not intended for real SSH sessions, but only for starting X applications that are listed under **Applications Access for Remote User "ruser"**.
If you try to log on to the device as **ruser** via SSH, then you will never be able to connect. The connection will be closed immediately without anything happening. In this case you must add the parameter "-X" and the program to be started in the session call, like in this example:

```
ssh -X ruser@192.168.10.203 localshell
```

Shadow Settings in IGEL OS

IGEL OS offers the ability to observe the endpoint device via shadowing. This is handy for helpdesks, troubleshooting, etc. This is possible via IGEL Virtual Network Computing (VNC) Viewer in the Universal Management Suite (UMS) or another VNC client (e.g. TightVNC), see *Universal Management Suite (UMS) > UMS Reference Manual > Devices - Managing Devices in IGEL UMS > Shadowing - Observe IGEL OS Desktop via VNC*.

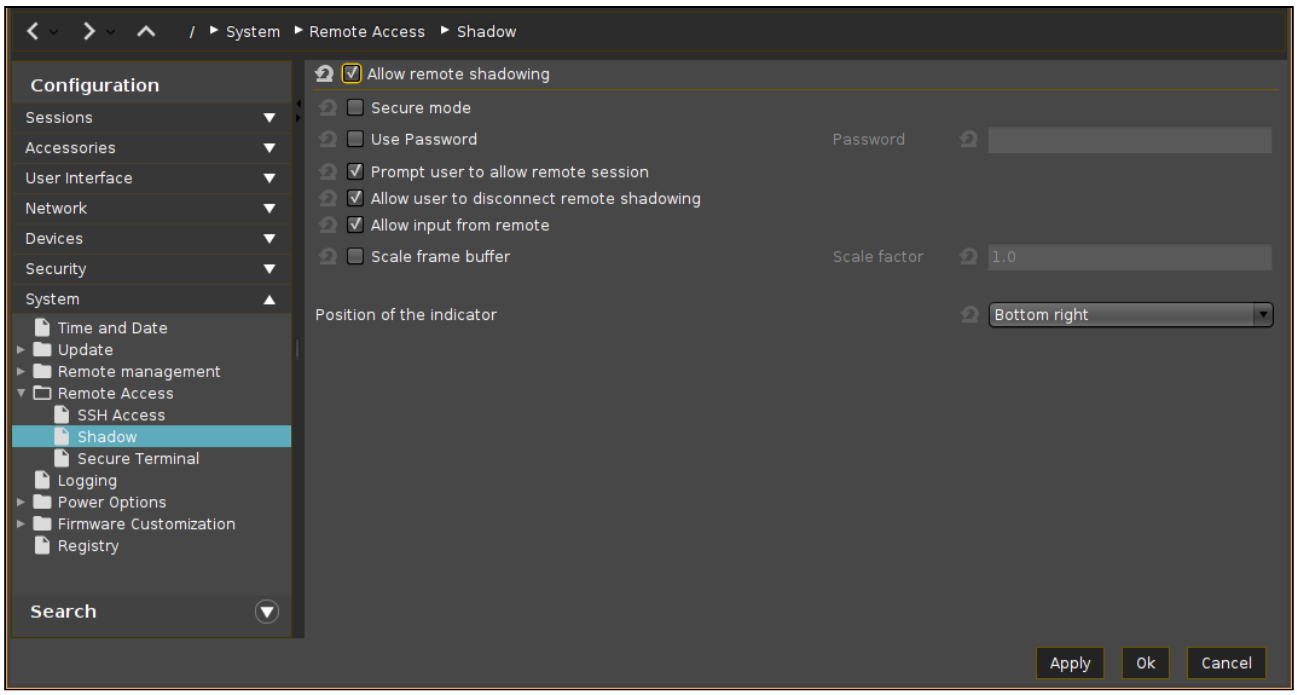
In the following article, you will learn about the **Shadow** settings, which you will require when configuring VNC access to your devices.

Menu path: **System > Remote Access > Shadow**

Remote Access to IGEL OS Devices via Shadowing

For Remote Working, Use Secure Shadowing

If the endpoint device is in a mobile or work-from-home environment, it is highly recommended to use secure shadowing only. Regular shadowing without encryption poses a security risk.



Allow remote shadowing

☑ Desktop content can be viewed from remote computers with VNC software.

☐ VNC shadowing is not allowed.*

If **Allow remote shadowing** is activated, you can change the following settings:

Secure mode

☑ Communication will be secured via SSL/TLS and shadowing will only be possible for UMS administrators.

☐ Communication will not be secured via SSL/TLS.*

Further information regarding secure shadowing can be found under Secure Shadowing (VNC with TLS/SSL) (see page 718).

Use password

☑ The remote user must enter a password before shadowing can begin.

☐ The remote user does not require a password for shadowing.*

Password

Password for the VNC connection

Prompt user to allow remote session

☑ The local user will be asked for permission before shadowing.*

In a number of countries, for example, Germany, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

Allow user to disconnect remote shadowing

☑ A **Disconnect** button with which the user can terminate the VNC connection is shown.*

Allow input from remote

☑ The remote user can make entries using the keyboard and mouse as if they were the local user.*

Scale frame buffer

☑ The screen content of the shadowed device is reduced or enlarged by the **scaling factor** before being transferred.

☐ The screen content is transferred in the original size.*

Scale factor

Factor by which the screen content of the shadowed device is enlarged or reduced. (Default: 1.0)

Position of the indicator

Defines the position of the popup notification about being shadowed.

Possible options:

- **Top right**

- **Top left**
- **Bottom left**
- **Bottom right***

Further parameters for the VNC server on the device are accessible under **System > Registry > network.vncserver**.

*IGEL OS system default

Secure Terminal

Menu path: **Setup > System > Remote Access > Secure Terminal**

You can establish a secure terminal connection to a thin client.

The thin client must meet the following requirements:

- The firmware of the thin clients is *IGEL* Linux *Version 5.11.100* or higher or IGEL Linux *Version 10.01.100* or higher.

For IGEL Linux Version 5.11.100 and 10.03.100:

1. In the thin client setup, go to **System > Remote Access > Secure Terminal**
2. Enable **Secure Terminal**

For IGEL Linux Version 10.01.100 or newer:

- Enable the following options in the thin client registry:
  - **network > telnetd > enabled > allow telnet access**
  - **network > telnetd > secure_mode > secure telnet**

> You can allow access via the secure terminal for all registered thin clients. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable Global Secure Terminal** option.

Remote Management in IGEL OS 11

Menu path: **Setup > System > Remote Management**

Here, you can configure settings relating to the remote administration of the device using the Universal Management Suite (UMS).

Enable remote management

☑ The endpoint device can be managed via the UMS. (Default)

☐ Remote management is not allowed.

Universal Management Suite: If the device is registered on a UMS Server, its IP address or hostname will be shown in the list.

> The list can contain more than one UMS instance. If the device cannot contact a UMS Server under the hostname `igelrmserver`, and the DHCP option 224 is not set, the device will go through the entries in the list until it can contact a UMS Server successfully.

To add another UMS instance, click on + :

- **UMS Server**: Name or IP of the UMS Server
- **Port Number**: Port number of the UMS Server (Default: 30001)

Display "Apply changes" dialog on boot: If new settings were made in the UMS, the device may receive them during the boot procedure. Here you can decide whether the user can influence the application of the new settings.

☑ During the boot procedure, the **Apply changes** dialog will be shown if new settings are available. The user can decide whether the new settings are applied immediately. If the user does not allow them to be applied immediately, they will automatically be applied when the system is next restarted.

☐ The dialog will not be shown. The new settings will be automatically applied or ignored depending on the setting under **Default action on boot**.

Timeout: Number of seconds for which the **Apply changes** dialog is shown (Default: 20). If the timeout is exceeded, the received settings will be automatically applied.
Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

Default action on boot: Configure the action that is to be performed if the dialog exceeds the time limit or if it is disabled.
Possible values:

- Apply changed configuration immediately: New settings will become active immediately and programs that are running may be restarted.
- Ignore changed configuration: New settings will not be applied. The new configuration will be saved on the device.

Prompt user on UMS actions

☑ The user will be informed via a message window if the device receives new settings from the UMS or is shut down. (Default)

☐ The user will not be informed if the device receives new settings from the UMS or is shut down.

Timeout: Number of seconds for which the notification window is shown
Possible values:

- No timeout: The dialog is shown until the user clicks on a button.
- 1 ... 120 seconds

Structure tag: You can define a structure tag in order to sort the device into a directory in accordance with the UMS directory rules.

UMS Registration: This button opens the UMS Registration (see page 1755) program from the accessories.

Further information regarding the use of structure tags can be found in the how-to *Universal Management Suite > Universal Management Suite (UMS) > UMS Articles > Customization > Using Structure Tags*.

- Options (see page 2052)

Options

Menu path: **Setup > System > Remote Management > Options**

- **Log login and logoff events**
  - ☑ If a user logs on or off via Citrix or Kerberos, details of this event will be sent to the UMS and can be used there, e.g. to process support queries.
    Logoffs from the Shared Workplace will also be logged (logons take place via the UMS anyway). (default)
  - ☐ Logon and logoff events will not be relayed. (default)

  > The event logs can be found under the system information for the thin clients in the UMS.

- **Delay session start at boot time in order to apply new UMS settings**: If new settings were made in the UMS, the thin client may receive them during the boot procedure.
  ☑ The session start will be delayed until the settings have been transferred or the time limit has been exceeded.
- **Timeout**: Delay in seconds (default: 10)
  Possible values:
  - No time limit: The dialog is shown until the user clicks on a button.
  - 1 ... 120 seconds

Logging

Menu path: **Setup > System > Logging**

Here you can configure local and remote logging for the device.

Local logging

☑ The log messages are stored locally in `/var/log`. The format is human-readable. Log rotation is applied.

☐ The log messages are not stored locally.

Persistent log partition: This parameter is effective only when **Local logging** is activated.

☑ The log messages are stored in a persistent partition on the device. This partition is encrypted.

☐ The log messages are stored in temporary files that are deleted on reboot.

Partition size in MB: Size of the persistent log partition

Remote mode
Possible options:

- "Server": The device receives log messages from a remote client.
- "Client": The device sends its log messages to a remote server.
- "Off": The device does not send or receive any log messages.

Remote Mode Switched to "Server"

You can configure the device to act as a syslog server. One or more other clients can send log files to this server; you can create a separate server configuration for each client.

Template for log file storage: Pattern from which the file path for storing the received log messages is created. `%HOSTNAME%` is the name of the sender which is configured under **Name**.

Server: A syslog server can be added by clicking ＋.

Local port: Port on which the local server listens for log messages

Transport protocol: Protocol to be used for the transmission of log messages

Name: Hostname of the sender (optional). This is useful for filtering the log messages based on the clients that have sent them.

Local address: Optional parameter; on multihomed machines (i. e. machines with multiple addresses), this specifies to which local address rsyslog is bound. If no address is specified it defaults to `0.0.0.0`, so that rsyslog listens on every network interface. For more information, see the official documentation at https://www.rsyslog.com/doc/v8-stable/configuration/modules/imtcp.html .

Remote Mode Switched to "Client"

You can configure one or more clients, e.g. one server for kernel messages and another server for authentication messages.

Clients: A client can be added by clicking ＋.

Remote address: IP address or hostname of the remote server

Remote port: Port on which the server listens for log messages

Transport protocol: Protocol to be used for the transmission of log messages

Syslog facility: Type of program for which log messages are created

Syslog level: Severity level of the event

Syslog style template: Format in which the messages are sent

TLS enabled

☑ TLS encryption for the transmission of log messages is enabled.

☐ Transmitted log messages are not encrypted.

CA certificate: Path to the local CA root certificate file in PEM format which is used to verify the authenticity of the X.509 certificate of your log collector and analyzer. If the UMS is used to transfer the certificate file to devices (see *Security & Safety > BSI Grundschutz > Anleitung zum IT-Grundschutz-konformen Betrieb von IGEL OS 11.03.100 > Logging and Log Evaluation*), the same path and file name as in the UMS must be entered. Example: `/wfs/ca-certs/ca.pem`

Update

Menu path: **Setup > System > Update**

Here, you can configure settings for the system update.

_____

- Firmware Update Settings for IGEL OS (see page 2056)
- Buddy Update (see page 2061)

Firmware Update Settings for IGEL OS

In the **Firmware Update** area, you can specify how the device obtains IGEL OS updates.

For more information on updates, see Firmware Update (see page 310) .

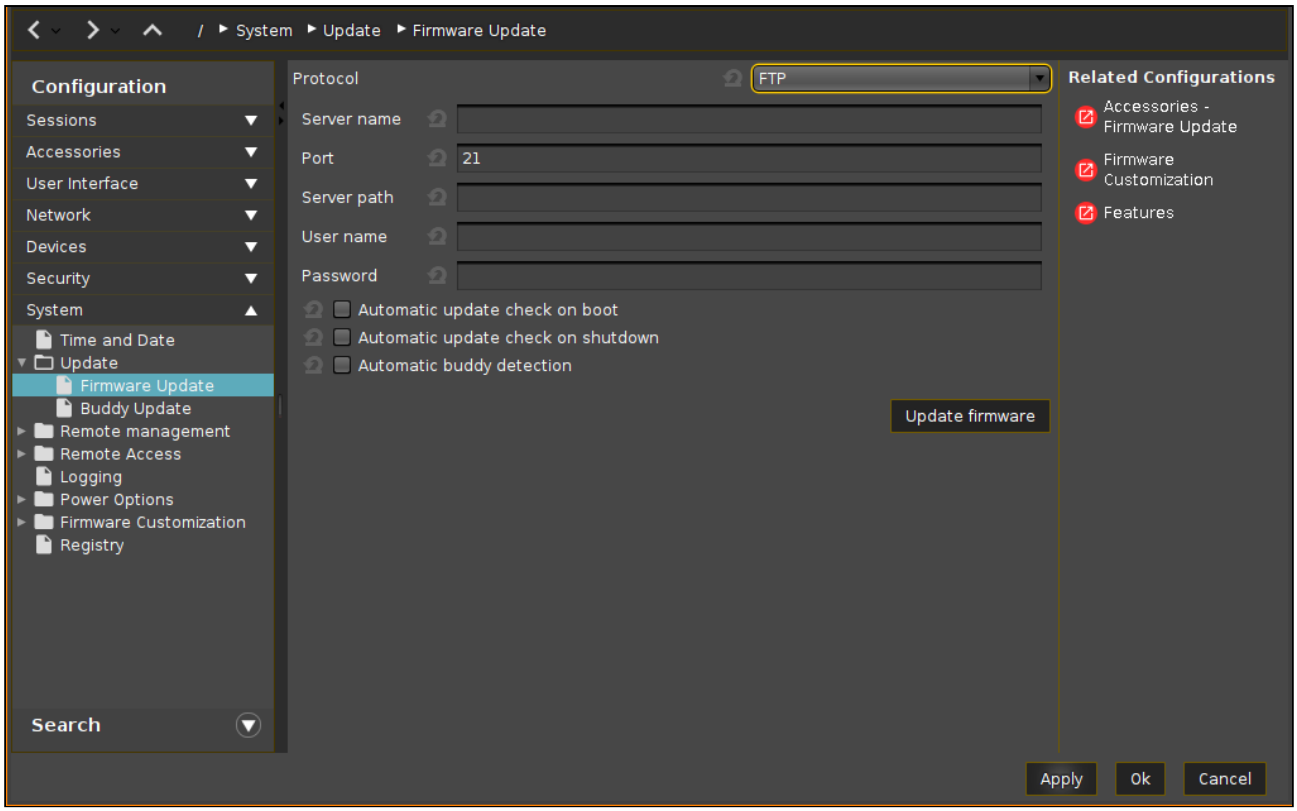
No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

Update Can Be Canceled After Timeout
An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

Menu path: **System > Update > Firmware Update**



Protocol

Select the method for accessing the updates.

Possible options:

- **HTTP**: Download from a web server.
- **HTTPS**: Download from a TLS/SSL-secured web server.
- **FTP**: Download from an FTP server. FTP passive mode is used. (Default)
- **Secure FTP**: Download via SSH-secured FTP.
- **FTPS**: Download from a TLS/SSL-secured FTP server.
- **FILE**: The update lies in the device file system, possibly as a shared NFS or Windows update. You can choose the location by selecting a file below. See also Updating IGEL OS Using a USB Storage Device (see page 314).

Server name

Name or IP address of the server.

Port

Port of the server on which the service is provided.

Server path

The path to the directory with the update files on the server.

User name

User name on the server.

Password

Password for the user account on the server.

Automatic update check on boot

☑ The device will automatically search for and install an updated firmware version each time that it boots.

☐ The device will not automatically search for an updated firmware version. (Default)

Automatic update check on shutdown

☑ The device will automatically search for and install an updated firmware version each time that it shuts down or it reboots.

☐ The device will not automatically search for an updated firmware version when it shuts down. (Default)

Automatic buddy detection

☑ The device will automatically search for further devices in the local network that offer firmware updates as Buddy Servers. For more information on buddy update, see the how-to Buddy Update (see page 303).

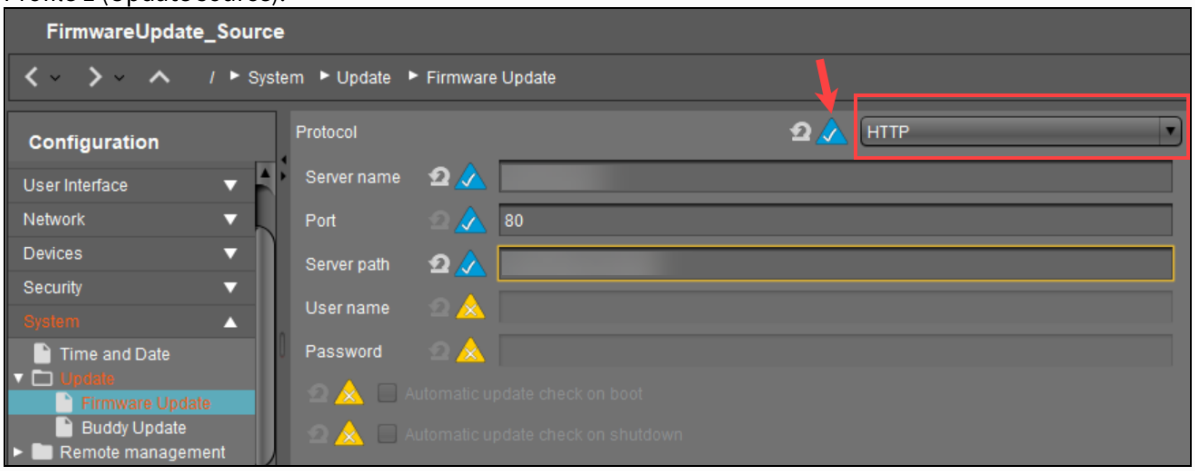
☐ The device will not automatically search for Buddy Servers. (Default)

Update firmware

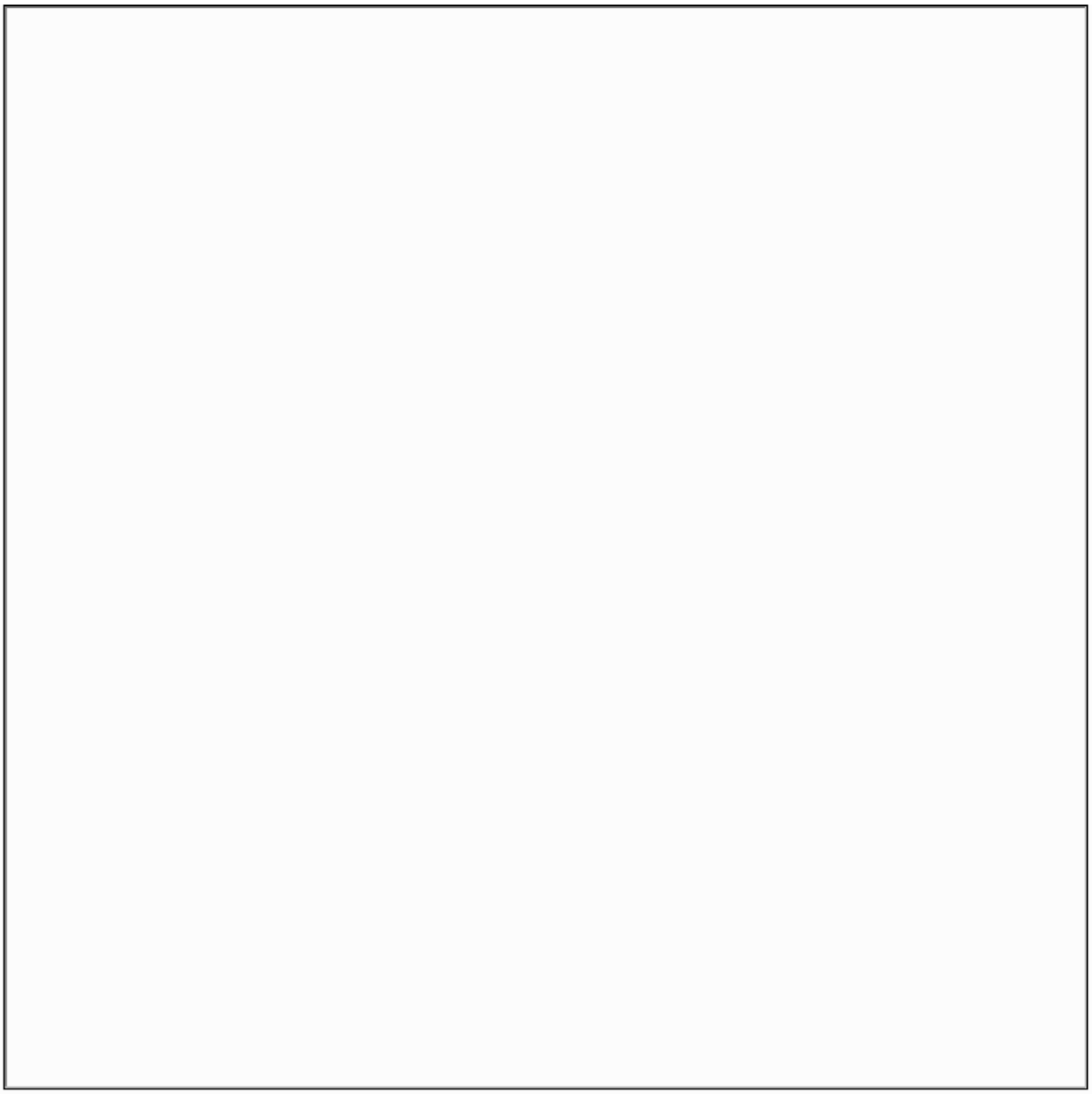
Launches the update process. If you have made changes on this setup page earlier on, click on **Apply** first.

Troubleshooting: The Firmware Update Does Not Function Properly When Configured via Multiple Profiles
If several profiles are used to configure the firmware update, make sure that ALL these profiles have the **Protocol** parameter activated and the same protocol is selected.
Example: There are two profiles configuring the firmware update for a device – the first profile defines the update source (via the HTTP protocol) and the second profile configures settings for the automatic update check. If the **Protocol** parameter in the second profile is left unconfigured, the automatic update check settings will apply only for FTP (since FTP is the default protocol); therefore, it is important to activate the **Protocol** parameter and select the same protocol as in the first profile – HTTP.

Profile 1 (Update source):



Profile 2 (Automatic update check)



Buddy Update

Menu path: **Setup > System > Update > Buddy Update**

Under **Buddy Update**, you can specify your device as an update server for other IGEL devices. If you use a device as an update server, only the FTP protocol can be used to update the firmware. A number of thin clients can be set up as buddy update servers within the network.

Thin clients without a specified update server search for available servers during the update. The first update server contacted then provides the update.

The minimal requirement for using the functionality with IGEL OS 11 is 4 GB storage. A device with less than 4 GB storage can run IGEL OS 11 with a reduced feature set but will malfunction when configured as a Buddy Update server.

No Downgrade from IGEL OS 11.03

It is not possible to downgrade from IGEL OS 11.03 or higher to any version before IGEL OS 11.03, except IGEL OS 11.02.200. This is because, from IGEL OS 11.03 onwards, the system partitions are signed to guarantee their integrity; it is not possible to change from a system with signed partitions to a system with unsigned partitions. IGEL OS 11.02.200 is a special variant of IGEL OS 11.02 that has signed system partitions. IGEL OS 11.02.200 is only available from the IGEL Support Team.

Update Can Be Canceled After Timeout
An ongoing update can be canceled by the user if the "network online" status could not be reached within 10 seconds after the firmware update has been started. When the user has canceled the update, the normal desktop environment is started, just as before the update. This applies to the following cases:

- Regular firmware update, e.g. from IGEL OS 11.03.500 to IGEL OS 11.04
- A feature has been activated, e.g. VPN OpenConnect.
- A Custom Partition has been activated or changed.

- **Enable Update Server**
  - ☑ This thin client serves as an FTP firmware update server for other thin clients.
  - ☐ This thin client does not serve as an FTP firmware update server for other thin clients. (default)
- **User Name**: User name for FTP access (default: anonymous)
- **Password**: Password for FTP access. The asterisk * allows any password.
- **Max. Concurrent Logins**: Maximum number of simultaneous logons on the FTP server. (default: 10)
  For further information, read the Buddy Update (see page 303) how-to.

Power Options

Menu path: **Setup > System > Power Options**

In this area, you will find the settings for energy management.

_____

- System Power Options in IGEL OS (see page 2063)
- Battery (see page 2065)
- Screen (see page 2066)
- Shutdown (see page 2067)

System Power Options in IGEL OS

Here, you can configure settings for energy saving on your IGEL OS endpoint device. This comprises the behavior after a configured time of inactivity and the CPU power plan.

> Display of Energy Star Logo on Selected HP Endpoint Devices
>
> With selected Hewlett-Packard (HP) endpoint devices, the Energy Star certification mark is displayed on this Setup page,

Menu path: **System > Power Options > System**

System suspend/shutdown on inactivity

Specify how long the user can be inactive before the system switches to standby mode or shuts down, dependent on the option selected under **System action on inactivity**.

Possible values:

- **Never***
- **After 1 minute**
- **...**
- **After 24 hours**

System action on inactivity

Possible options:

- **Suspend***: The system is set to standby mode after the timeout defined with **System suspend/shutdown on inactivity** has expired.

> If Suspend doesn't work, it might be related to a missing ACPI Support: https://01.org/linuxgraphics/gfx-docs/drm/admin-guide/pm/sleep-states.html

- **Shutdown**: The system is shut down after the timeout defined with **System suspend/shutdown on inactivity** has expired.

Without dialog

☑ The user is not asked if the system is to be set to standby mode.

☐ The dialog will be shown.*

Dialog timeout

Time in seconds, for which the dialog is to be displayed. (Default: 10 seconds)

CPU Power Plan

Specify here which CPU power plan (CPU Governor) the device is to use in battery mode and in AC mode.

- **On Battery**
  High Performance: full performance with maximum processor speed
  Balanced (Smooth): slower regulation of performance in a balanced manner according to the demands of programs. Suitable for users who are bothered by the fan frequently running at high speed.
  Balanced (Recommended)*: rapid regulation of performance according to the demands of programs.
  Power Saver: lowest processor speed
- **Plugged in**
  High Performance*
  Balanced (Smooth)
  Balanced (Recommended)
  Power Saver

Tray Icon

☑ A CPU icon will be shown in the system tray. This makes it easy to switch between power plans.

☐ No CPU icon will be shown.*

* IGEL OS system default

Battery

Menu path: **Setup > System > Power Options > Battery**

In this area, you can define the rechargeable battery messages.

Battery Notification

Critical battery level (percentage): Percentage of remaining battery charge deemed critical (default: 5)

Critical battery action: Action to be taken in the event of a critical battery level
Possible options:

- Do nothing
- Show warning
- Run command
- Run command in terminal

Critical command: Command that is executed when a critical charge level is reached (example: Shutdown)

Low battery level (percentage): Percentage of remaining battery charge deemed low (default: 10)

Low battery action: Here you can specify what action is to be taken in the event of a low battery level.
Possible options:

- Do nothing
- Show warning
- Run command
- Run command in terminal

Low command: Command that is executed when a low charge level is reached (example: Shutdown)

Battery Tray Icon

Display percentage:

☑ The percentage of remaining energy is shown in the taskbar. (default)

Display time

☑ The estimated remaining battery life is shown in the taskbar.

☐ The estimated remaining battery life is not shown. (default)

Screen

Menu path: **Setup > System > Power Options > Display**

In this area, you can configure screen settings which can help to reduce energy consumption.

Display Power Management Settings

- **Handle Display Power Management**:
  ☑ You can configure energy saving settings separately for battery or AC operation. (default)
  ☐ You cannot configure energy saving settings.
- **Standby Time**: Number of minutes after which the screen switches to standby mode if the user is inactive. (default: 6 minutes)
- **Suspend time**: Number of minutes after which the screen switches to suspend mode if the user is inactive. (default: 8 minutes)
- **Off Time**: Number of minutes after which the screen switches off if the user is inactive. (default: 10 minutes)

Brightness Reduction

> The brightness reduction controls have been added specifically for use of laptops. They have no effect on other devices connected to the power supply.

- **On inactivity reduce to**: Specify to how many percent the screen brightness should be reduced if you are not using the device for battery and AC operation. (default for battery: 20%, default for AC operation: 80%)
- **Reduce after**: Specify a time between 10 and 120 seconds after which the screen brightness will be reduced for battery and AC operation. (default: Never)

Shutdown

Menu path: **Setup > System > Power Options > Shutdown**

Here, you can change the behavior when the device shuts down manually or automatically.

Allow system shutdown

☑ The device can be shut down by the user. (Default)

☐ The device cannot be shut down by the user.

Allow system suspend

☑ The device can be suspended by the user. (Default)

☐ The device cannot be suspended by the user.

Allow canceling of shutdown process

☑ The user can cancel the procedure via a button. (Default)

☐ The user cannot cancel the procedure.

Default action: Action that is carried out when the time is set under **Dialog timeout**.
Possible options:

- Shutdown
- Suspend
- Cancel: No action will be carried out after the time set under **Dialog timeout** expires, see **Allow canceling of shutdown process** parameter.
- Nothing: No action will be carried out after the time set under **Dialog timeout** expires.

Without dialog

☑ The dialog will not be shown. The action selected under **Default action** will be carried out.

☐ The dialog will be shown. (Default)

Dialog timeout: After the time (in seconds) set here expires, the dialog will close and the action specified under **Default action** will be carried out. If the value is set to 0, the dialog will be shown until the user selects one of the possible actions. (Default: 10)

Firmware Customization

Menu path: **Setup > System > Firmware Customization**

You can configure the firmware according to your needs.

- Custom Partition (see page 2069)
- Custom Application (see page 2073)
- Custom Commands (see page 2080)
- Corporate Design (see page 2087)
- Environment Variables (see page 2095)
- Features (see page 2098)

Custom Partition

Menu path: **Setup > System > Firmware Customization > Custom Partition**

In IGEL OS, a custom data partition is available for use as required. A download/update function that loads data from a server and, where appropriate, updates them can be set up for this custom storage area.

The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

If the device is reset to the default settings (factory reset), the custom partition and all data stored on it will be deleted.

_____

- Partition (see page 2070)
- Download (see page 2071)

Partition

Menu path: **Setup > System > Firmware Configuration > Custom Partition > Partition**

Here, you can create a partition of your own.

- **Enable partition**
  - ☑ The customer partition is enabled in the *IGEL* Setup of the thin client or with the *IGEL Universal Management Suite* via the setup path.
  - ☐ The customer partition is not enabled. (default)
- **Size**: Size of the partition. A number must be followed by a multiplicative ending, without a space in between. Example: "100K" stands for 100 Kibibytes, that is, 100 * 1024 bytes.
  The following multiplicative endings are possible (capital letters required):
  K for kibibytes (number * 1024)
  M for mebibytes (number * 1024 * 1024)
  G for gibibytes (number * 1024 * 1024 * 1024)

  > Sensible values are for example "100K" (for 100 KiB = 100 * 1024 bytes) or "100M" (for 100 MiB = 100 * 1024 * 1024 bytes). The size of the partition should be set to at least 100 KiB. However, no more than 300 MiB should be reserved for the customer-specific partition (based on the 1 GB standard CF used in IGEL Linux thin clients). This is because subsequent firmware updates may require more storage space than the current version.

- **Mount point**: Path on which the partition is to be mounted. (default: `/custom`)
- **Partitions parameters**: From IGEL OS *Version 10.03.100*, you can enter name value pairs which are passed on to the custom partition for further processing.
  To manage the list, proceed as follows:
  - Click to create a new parameter.
  - Click to remove the selected parameter.
  - Click to edit the selected parameter.
  - Click to copy the selected parameter.

Add

- **Name**: Name of the parameter
- **Value**: Value of the parameter

Download

Menu path: **Setup > System > Firmware Configuration > Custom Partition > Download**

Sources for partition data

In order to load data onto the custom partition, at least one source for partition data must be set up here.

To manage the list, proceed as follows:

- Click to create a new source.
- Click to remove the selected source.
- Click to edit the selected source.
- Click to copy the selected source.

Add

- **Automatic update**
  - ☑ The contents from this source will be updated automatically.
  - ☐ The contents from this source will not be updated automatically. (default)

- **URL**: URL of the web server
- **User name**: User name for access to the web server
- **Password**: Password for access to the web server
- **Initialization action**: Action which is performed after mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be launched.
- **Finalizing action**: Action which is performed before mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be ended.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP and HTTPS. An `INF` file which in turn references a tar archive zipped using bzip2 must be referenced as the target.

The structure of the INF file is as follows:

`[INFO], [PART]`	Header information
`file="test.tar.bz2"`	File name of the compressed tar archive
`version="1"`	Version number - a higher version results in an update if Update automatically is enabled.

The files to be transferred must therefore be zipped in a tar archive which is then compressed using bzip2. This file is referenced in the INF file which is the target of the URL.

The tar archive can be created under Windows, e.g. with the open source program 7-Zip (www.7-zip.de[239]). This program also allows `bzip2` compression. Under Linux, tar and bz2 files can be created using onboard resources.

239. http://www.7-zip.de

The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The `Version` parameter in the `INF` file must be increased for this purpose.

Custom Application

Menu path: **System > Firmware Customization > Custom Application**

Applications that were loaded onto a customer partition for example can be launched via the Application Launcher or an icon on the desktop once they have been defined as custom applications. In order for this to be possible, a command to call up the application must be entered under Settings (see page 2076) .

→ Click on + to define a custom application.

→ Specify the launch options:

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.

- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413) .

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Settings (see page 2076)
- Desktop Integration (see page 2077)

Settings

Menu path: **System > Firmware Customization> Custom Application > [Session Name] > Settings**

Enter the command for calling up an application here:

Icon name: Select an icon provided. (Fefault: applications-other).

Command: Give the name and path of the application. (Example: `/usr/bin/gpicview`).

> Only the desktop icon of a session is customizable. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.

Desktop Integration

Menu path: **System > Firmware Customization > Custom Application > [Session Name] > Desktop Integration**

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Quick start panel

☑ The session can be launched with the quick start panel

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Menu folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Application Launcher folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop folder: If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Password protection: Specifies which password will be requested when launching the session.
Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user's password is requested when launching the session.

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers: A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

> ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- = `Mod4`

> ℹ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key: Key for the hotkey

> ℹ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay: Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification: This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively. For further information, see Appliance Mode (see page 1413).

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Custom Commands

Menu path: **Setup > System > Firmware Customization > Custom Commands**

You can define custom commands for specific points in time when the system is starting. You can use configured environment variables (see page 2095) in the commands.

> ⚠ The content of custom scripts used in the custom command fields cannot be supported by IGEL. Therefore, you may be requested to remove custom scripts as part of the troubleshooting/support process.

- Post Session Custom Commands in IGEL OS (see page 2081)
- Base (see page 2083)
- Network (see page 2084)
- Desktop (see page 2085)
- Reconfiguration (see page 2086)

Post Session Custom Commands in IGEL OS

In the following article, you will learn how you can configure post-session custom commands in IGEL OS. For a specific session type, you can define an action that is performed when the last session of this type is ended. The defined post-session command can also be used for multiple session types.

For an example of using post-session commands, see Shutdown/Suspend Devices Automatically at the End of a Session (see page 967).

Menu path: **System > Firmware Customization > Custom Commands > Post Session**

Session type

Session type for which the action is performed.

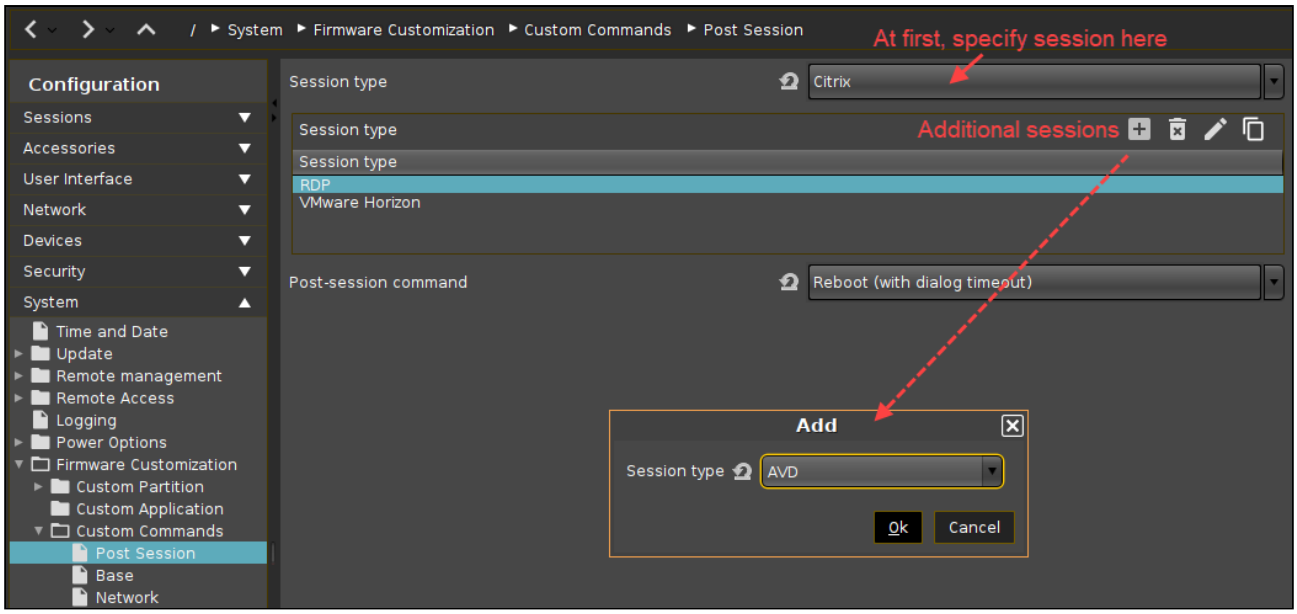
Possible values:

- **No post-session command***
- **Citrix**
- **Citrix via Browser**

> Post-session commands for **Citrix via Browser** are currently supported for Firefox browser only.

- **RDP (with login dialog)**
- **RDP**
- **VMware Horizon**
- **Browser**
- **NoMachine NX**
- **Parallels Client**
- **PowerTerm terminal emulation**
- **ThinLinc**
- **X session**
- **IBM iAccess**
- **Media player**
- **VNC viewer**
- **AVD**

→ If a post-session command has to be applied to multiple sessions, specify the main session in the above **Session type** field and use + to add additional sessions.



Post-session command

Action that is carried out after the end of the session(s) selected above.

Possible options:

- **Logoff***: The user is automatically logged off; a login method must be defined for this purpose. Further information can be found under IGEL Smartcard (see page 2031), Active Directory / Kerberos (see page 2034) and Smartcard (see page 2024).

> The “Logoff” option cannot be used if the Appliance Mode is in use. Further information can be found under Appliance Mode (see page 1413).

- **Shutdown/suspend (system default action)**: The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. A dialog allowing the user to cancel the procedure will be shown in the process. Further information can be found under Shutdown (see page 2067).
- **Shutdown/suspend (system default action without dialog)**: The device will be shut down or placed in a standby mode depending on the setting under **System > Power Options > Shutdown > Default action** selection. The user cannot cancel the procedure.
- **Reboot (with dialog timeout)**: The device will reboot. A dialog allowing the user to cancel the procedure will be shown in the process.
- **Reboot (without dialog)**: The device will reboot. The user cannot cancel the procedure.
- **Enter custom command here**: Command to be executed.

*IGEL OS system default

Base

Menu path: **Setup > System > Firmware Customization > Custom Commands > Base**

The commands defined here are executed on a one-off basis during the boot procedure. You can define commands for the execution times described below:

- **Initialization**
  - Not all drivers loaded, not all devices available
  - Network scripts not launched, network not available
  - Partitions available except *firefox profile, scim data, ncp data, custom partition*
- **Before session configuration**
  - Not all drivers loaded, not all devices available
  - Network scripts launched, network not available
  - Partitions available except *firefox profile, scim data, ncp data, custom partition*
  - Sessions not configured
- **After session configuration**
  - All drivers loaded, all devices available
  - Network available
  - Partitions available except *custom partition*
  - System daemons not launched (CUPS, ThinPrint etc.)
  - Sessions configured
  - UMS settings retrieved but not yet effective
- **Final initialization command**
  - All partitions available
  - All system daemons launched
  - UMS settings effective

Network

Menu path: **Setup > System > Firmware Customization > Custom Commands > Network**

You can define commands for the execution times described below:

Network initialization

- The commands defined here are executed at the beginning of the network configuration.

The commands in the below fields are executed each time the relevant network interface starts.
The `INTERFACE` environment variable contains the name of the network interface started.

After network DNS

- Runs after each change in the IP address or host name
- IP address / name server settings used (e.g. via DHCP)

Before network services

- IP address / name server settings used
- VPN connected (if VPN autostart was enabled in the setup)
- No network / host routing settings used

Final network command

- Network / host routing settings used
- NFS and SMB drives available
- System time synchronized with time server
- UMS settings retrieved but not effective yet

Desktop

Menu path: **Setup > System > Firmware Customization > Custom Commands > Desktop**

The commands defined here are executed when the X server is launched. You can define commands for the execution times described below:

- **Desktop initialization**
  - Runs once during the boot procedure
  - Desktop environment configured but not launched
  - User not logged on (Kerberos, smartcard etc.)
- **Before desktop start**
  - Runs once during the boot procedure
  - Desktop environment launched
  - Message service launched
  - Session D-Bus launched
  - User not logged on (Kerberos, smartcard etc.)
- **Final desktop command**
  - Runs after each user logon and desktop restart
  - User logged on (Kerberos, smartcard etc.)
  - User desktop launched

Reconfiguration

Menu path: **Setup > System > Firmware Customization > Custom Commands > Reconfiguration**

The commands defined here are executed after settings relating to the local setup or the UMS have been changed. You can define commands for the execution time described below.

- **After reconfiguration**: Runs after an effective change in the endpoint device settings (local setup, UMS)

Corporate Design

Menu path: **Setup > System > Firmware Customization > Corporate Design**

In this area, settings allowing you to adapt the user interface to your company layout are grouped together.

You can place your own logo in the following places:

- Custom Bootsplash (see page 2088)
- Background (1st Monitor) (see page 2090)
- Company Logos (see page 2093)

See also the how-to Customizing IGEL OS Desktop (see page 930).

Custom Bootsplash

Menu path: **Setup > System > Firmware Configuration > Corporate Design > Custom Bootsplash**

With a bootsplash, you can show your company logo or a specific image during the booting procedure. The bootsplash will be shown instead of the console messages.

Please note: You need to provide an image file for your custom bootsplash on a download server.

> The file types JPG, JPEG, BMP, PNG, SVG, GIF, and TIFF can be used for a bootsplash. A total storage area of 25 MB is available for all user-specific images. The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally.

Custom Bootsplash

Enable custom bootsplash

- [x] You can make the following settings in order to configure a custom bootsplash.
- [ ] No custom bootsplash is configured. (Default)

Custom Bootsplash - Server Location

Use firmware update server location

- [x] The server configuration will be carried over from the Firmware Update Settings for IGEL OS (see page 2056)
- [ ] You can carry out a custom configuration below. (Default)

Protocol: Access method for the image
Possible options:

- HTTP: Download from a web server
- HTTPS: Download from a TLS/SSL-secured web server
- FTP: Download from an FTP server
- Secure FTP: Download via SSH-secured FTP
- FTPS: Download from a TLS/SSL-secured FTP server
- FILE: The image file lies in the file system of the device, possibly as a shared NFS or Windows update. You can choose the location simply by selecting a file below.

Server name: Name or IP address of the server

Port: Port of the server on which the service is provided (Default: 21)

Server path: Path to the directory with the image file on the server

User name: User name on the server

Password: Password for the user account on the server

Custom Bootsplash - Settings

Custom bootsplash file: File name of the custom image
As regards positioning, the following applies: 0 = left-justified, 50 = centered, 100 = right-justified

Custom bootsplash style:

- Original
- Stretched
- Scaled
- Zoomed

Background color: Use the color picker to choose.

Horizontal position of the bootsplash image (Default: 50)

Vertical position of the bootsplash image (Default: 50)

Size of progress indicator (Default 72)

Horizontal position of the progress indicator (Default: 90)

Vertical position of the progress indicator (Default: 90)

Bootsplash update: The user-specific bootsplash will be downloaded from the given server.

If you change the image file or even just one of the settings for an existing bootsplash, be sure to click on **Bootsplash update** in order to regenerate the system files used and then on **Apply** or **OK**.

Background (1st Monitor)

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor)**

Decorate the desktop background with predefined IGEL backgrounds, a fill color or a color gradient or define a custom background image. You can set up a separate background image for each monitor that is connected to the thin client.

Prerequisite: You have provided a custom background image on a server; see Background Image Server (see page 2092).

The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for a background image. A total storage area of 25 MB is available for firmware customization images.

From IGEL Linux *Version 10.03.500* both background images and background image server can be defined user-customized via Shared Workplace. Please note the following for this:

- All user-customized background images will be saved on the thin client and therefore require a part of the available 25 MB storage space. Ensure that this storage limit is not exceeded. (When the storage limit is reached, all images except the one currently used will be deleted; with a new logon via Shared Workplace, the previously deleted images will be downloaded again until the storage limit is reached.)
  You will find further information on Shared Workplace and background images here:
- IGEL Linux user manual: Shared Workplace (see page 2037)
- IGEL UMS user manual: Shared Workplace
- How-To: Creating your own Wallpaper in the How-To Customizing the IGEL Linux Desktop

- **Wallpaper**: Select one of the predefined background images from the following list:
  - neutral
  - disabled
  - black (4x3)
  - blue (4x3)
  - gray (4x3)
  - orange (4x3)
  - green
  - black (16x9)
  - blue (16x9)
  - gray (16x9)
  - orange (16x9)
- **Wallpaper Style**: If you have set a custom background image, you can display it in a number of ways.
  Possible options:
  - Automatic
  - Centered

    - Tiled
    - Spread
    - Scaled
    - Zoomed
- **Color Style**: If you have chosen two different colors as the desktop background color, you can define color gradients here. Possible values:
  Possible options:
    - Solid color
    - Horizontal gradient
    - Vertical gradient
- **Desktop Color**: Click on **Choose color** to specify a custom background color for your desktop if you have not chosen a background image.
- **2nd Desktop Color**: Click on **Choose color** to specify a second background color for your desktop.
- **Custom wallpaper downlad**
    - ☑ You can set up a custom background image.
    - ☐ No custom background image will be used. (Default)
- **Custom Wallpaper file**: Name of the background image file

> If you would like to use a custom background image, you need to specify the download server under **System > Firmware Customization > Corporate Design > Background (1st Monitor) >** Custom Wallpaper Server (see page 2092). If you have already defined a server for the system update files, you can use the same server settings for downloading the background image.

Background Image Server

Menu path: **Setup > System > Firmware Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**

Custom Wallpaper - Server Configuration

- **Use firmware update server location**
  - ☑ The server configuration will be carried over from the Firmware Update Settings for IGEL OS (see page 2056).
  - ☐ You can carry out a custom configuration below. (default)
- **Protocol**: Select the method for accessing the image.
  - HTTP: Download from a web server.
  - HTTPS: Download from a TLS/SSL-secured web server.
  - FTP: Download from an FTP server.
  - Secure FTP: Download via SSH-secured FTP.
  - FTPS: Download from a TLS/SSL-secured FTP server.
  - FILE: The image lies in the thin client file system, possibly as a shared NFS or Windows file. You can choose the location simply by selecting a file below.
- **Server name**: Name or IP address of the server.
- **Port**: Port of the server on which the service is provided.
- **Server path**: The path to the directory with the image file on the server
- **User name**: User name on the server
- **Password**: Password for the user account on the server
- **Wallpaper update**: The user-specific background image will be downloaded from the given server.

Company Logos

Menu path: **Setup > System > Firmware Customization > Corporate Design > Company Logos**

You can show your company logo in the screensaver and in the start menu.

Screensaver

- **Enable image display**
  ☑ The image defined below will be shown as the screensaver. (default)
- **File for screen saver logo**: Complete path for an image file or a directory that contains a number of image files.

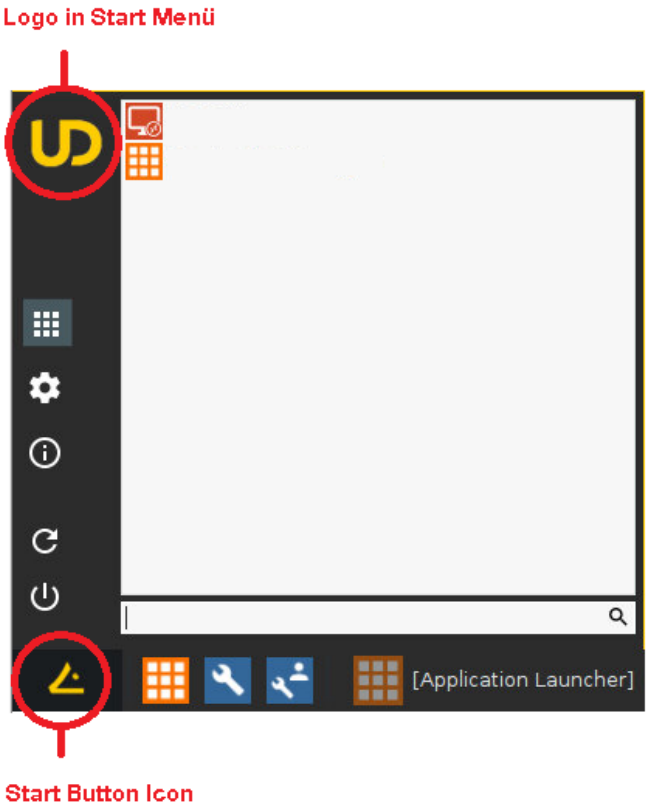
> - If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **image display time** for the images can be configured. If you do not specify a file of your own, the *IGEL* logo will be used.

- **One image per monitor**
  ☑ The image will be shown on each individual monitor rather than one image across all monitors. (default)
- **Image duration**: Time in seconds until the image changes (default: 10)
- **Image display mode**
  - Small-sized hopping: small image that jumps across the screen
  - Medium-sized hopping: larger image that jumps across the screen
  - Full screen center cut out: Image is displayed across whole screen, edges can be cut off.
  - Full screen letterbox: Complete image is shown. A black edge may be visible depending on the format.

Start menu

- **Start button icon**: File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels
- **Company logo in start menu**: File name with full path to show your company logo in the start menu window. Size: 64x64 pixels

> In order to see the company logo in the start menu window, you must set the start menu type to **Advanced**. To do this, click on **User Interface > Desktop > Start Menu**.


Logo in Start Menü
[Application Launcher]
Start Button Icon

Environment Variables

Menu path: **System > Firmware Customization > Environment Variables**

Environment variables allow you to use dynamic parameter values for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session.

Predefined variables can also be allocated and distributed via the IGEL UMS. Additionally, defined variables can only be used locally on the thin client and may be overwritten by a UMS configuration.

Enable variable substitution in session: (default: disabled)

☑ The use of variables in sessions such as ICA and RDP is enabled. If specific parameters contain a `$`, shell substitution will be carried out.

☐ The use of variables in sessions is not enabled. (default)

The environment variables are available in the setup under Custom Commands (see page 2080).

In addition, the following session parameters can be updated through variables:

- Legacy ICA sessions: Citrix Server or published application
- Legacy ICA sessions: User
- RDP session: Server
- RDP session: User

_____

- Predefined (see page 2096)
- Additional (see page 2097)

Predefined

Menu path: **System > Firmware Customization > Environment Variables > Predefined**

- **Variable name**: Name for the variable
- **Value**: Value for the variable

To use environment variables in sessions, proceed as follows:

1. Enable environment variables under **System > Firmware Customization > Environment Variables > Enable variable substitution in session**.
2. Define the variable name and content, e.g.
   - **Variable name**: `SERVERNAME`
   - **Value**: `testServer`
3. Enter the variable name in the parameter field of the session with the $ symbol before it. Example: `$SERVERNAME`

> In the case of RDP and ICA sessions, the value is entered in the session file after saving. With XenApp, the setting is not implemented until a session starts and is running.

Additional

Menu path: **System > Firmware Customization > Environment Variables > Additional**

You can define other variables in addition to the 10 predefined ones.

- **Variable name**: Name for the variable
- **Value**: Value for the variable

Features

Menu path: **System > Firmware Customization > Features**

Using this list of available services, you can quickly enable or disable firmware components such as Media Player, Extra Font Services, etc. By deactivating e.g. unused features, you can save storage space.

If a service was disabled, the associated session type will no longer be available when the system is restarted. Existing sessions will no longer be shown but will not be deleted either.

For further information, see How to Disable IGEL OS Features to Reduce Firmware Size (see page 602).

A disabled session type will not be updated during a firmware update. Therefore, you should disable unused services in order to speed up update processes.

Features with Limited Support
A number of products feature functions with “limited support”. These functions are offered 'as is' without any warranty. Any support for these functions is provided on a non-binding, “best effort” basis.

Registry

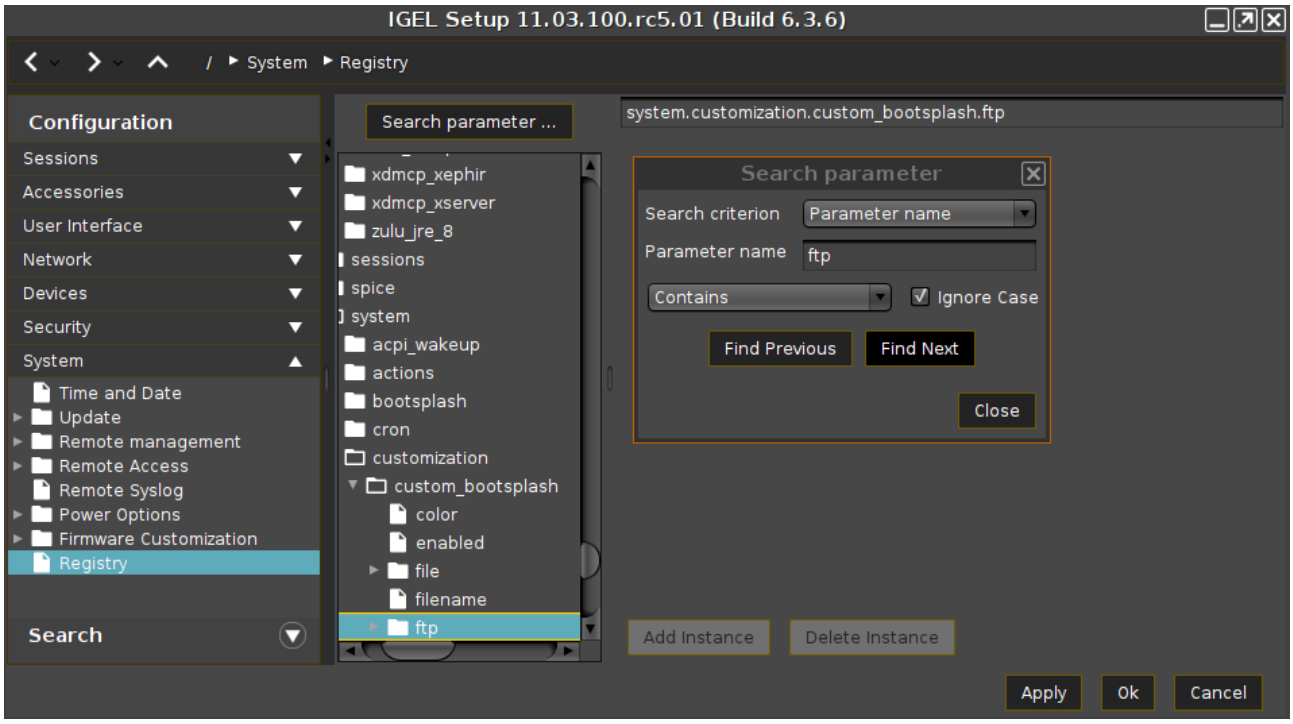
Menu path: **System > Registry**

In the registry, you can change virtually any firmware parameter. You will find information on the individual items in the tooltips.

> Changes to the registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the functionality is to reset the device to the factory defaults!

Search parameter...: Search for setup parameters in the registry.

- **Search criterion**: Criterion for searching.
  The following can be selected:
  - Parameter name
- **Parameter name**: Any search term.
- Logical search restriction:
  - Contains
  - Exact match
  - Use regular expressions
- **Ignore case**
- **Find previous**: Go back if there are a number of hits.
- **Find next**: Go forwards if there are a number of hits.
  Example: If you would like to find the FTP settings for updating the Linux firmware, you can search for the parameter name `ftp`. The parameter found in the registry structure is highlighted. Click on **Find next** until you find your desired parameter:



Add instance: Adds instances. This is possible with parameters which have a percent sign as their last character, e.g. `nfymount%`. The new instances are numbered consecutively: `nfymount1`, `nfymount2` etc.

Delete instance: Deletes a previously added instance.

Setup Assistant for IGEL OS

When you start an unconfigured device, you will be welcomed by the **Setup Assistant** for IGEL OS. This assistant takes you through the most important initial configuration steps.

The Setup Assistant starts automatically after booting IGEL OS if all the following requirements are met:

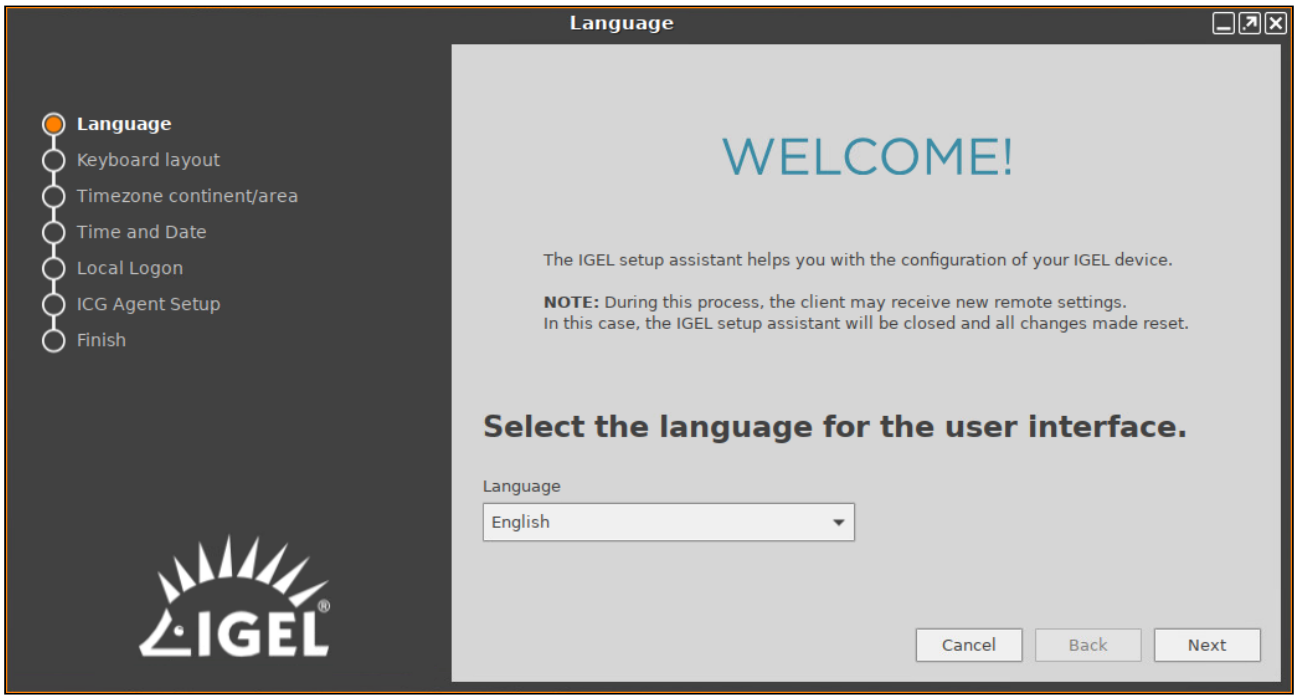
- The device is not yet configured.
- No IP address for the Universal Management Suite (UMS) was transferred using the DHCP option 224.
- No UMS can be accessed under the DNS name `igelrmserver`.

In the IGEL Setup Assistant, you will find the following buttons:

- **Next**: Go to the next configuration step.
- **Back**: Go back to the previous step.
- **Cancel**: Exit the Setup Assistant without saving changes to the configuration. However, changes to the time and date will remain effective.
- **Skip**: This button is shown if the current configuration step can be omitted. If you click on **Skip**, nothing will change during the configuration step. If the configuration is edited, the button will change to **Next**.

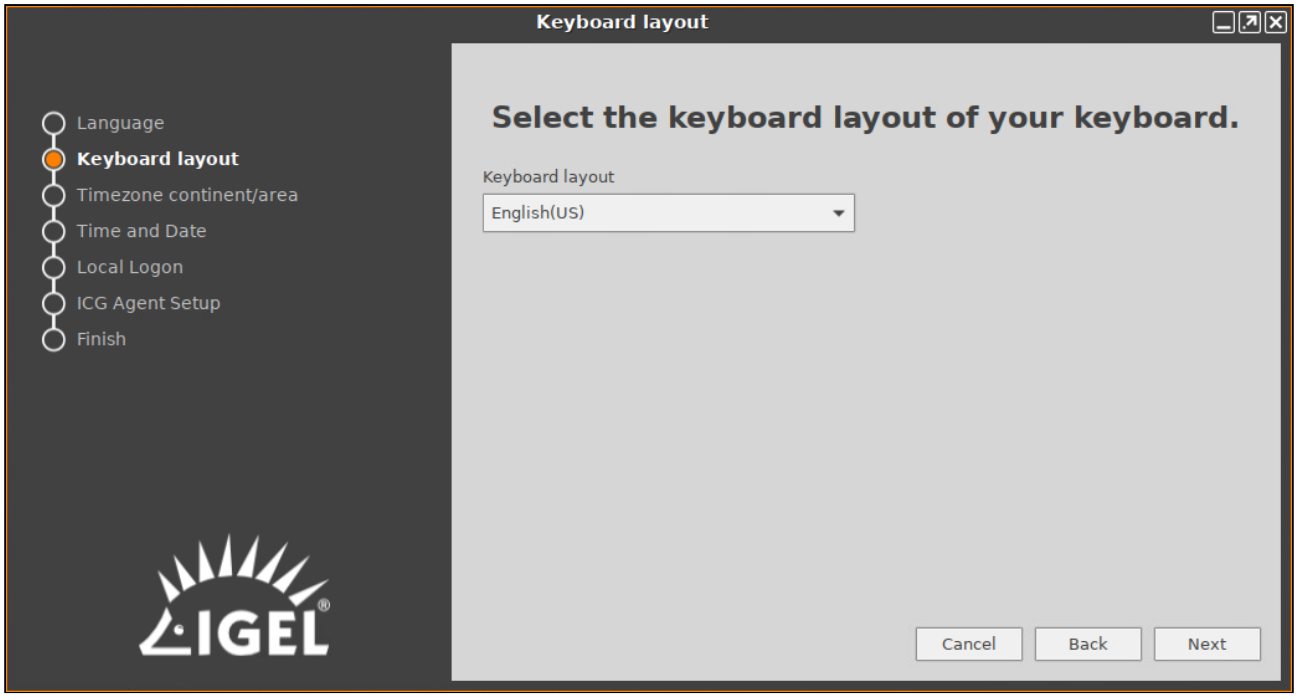
Instead of clicking **Skip**, the **ESC** key can also be clicked to skip this configuration step.

Language



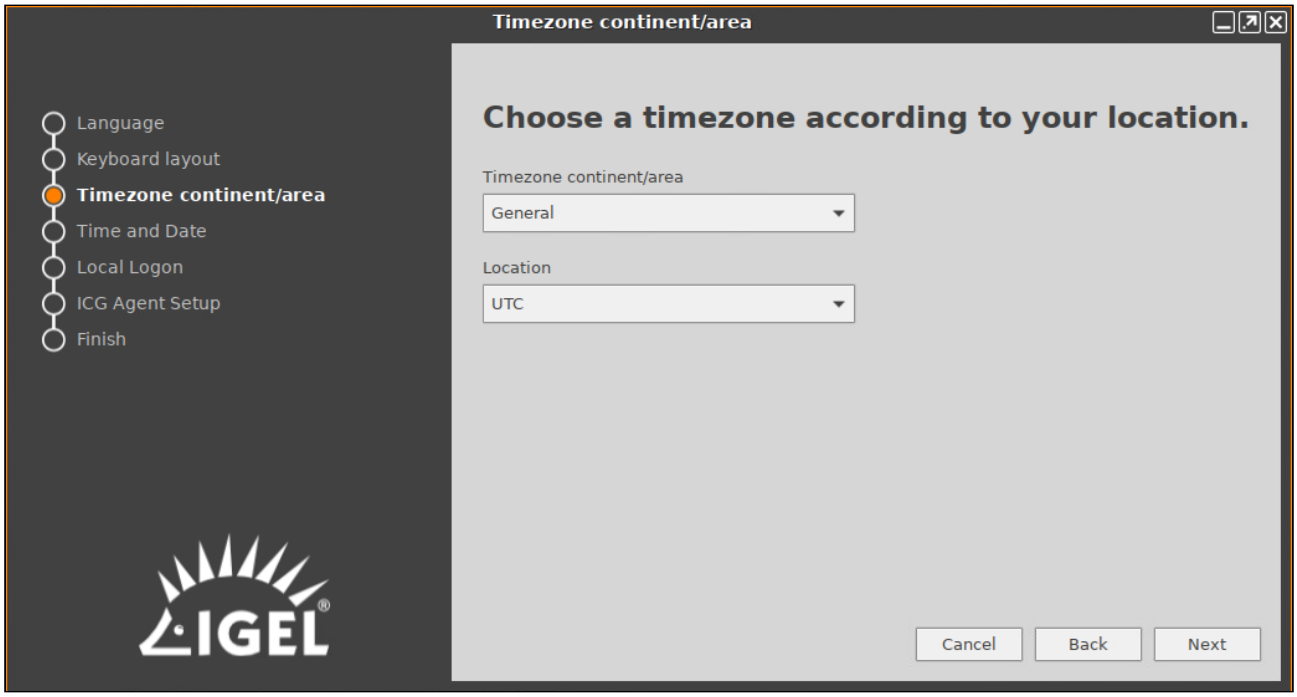
Here you can select the language for the user interface

Keyboard Layout



Select the keyboard layout. The selected layout applies to all parts of the system including emulations, window sessions, and X11 applications.

Timezone Continent/Area



Timezone Continent/Area

Select the continent/area for your location.

Possible values:

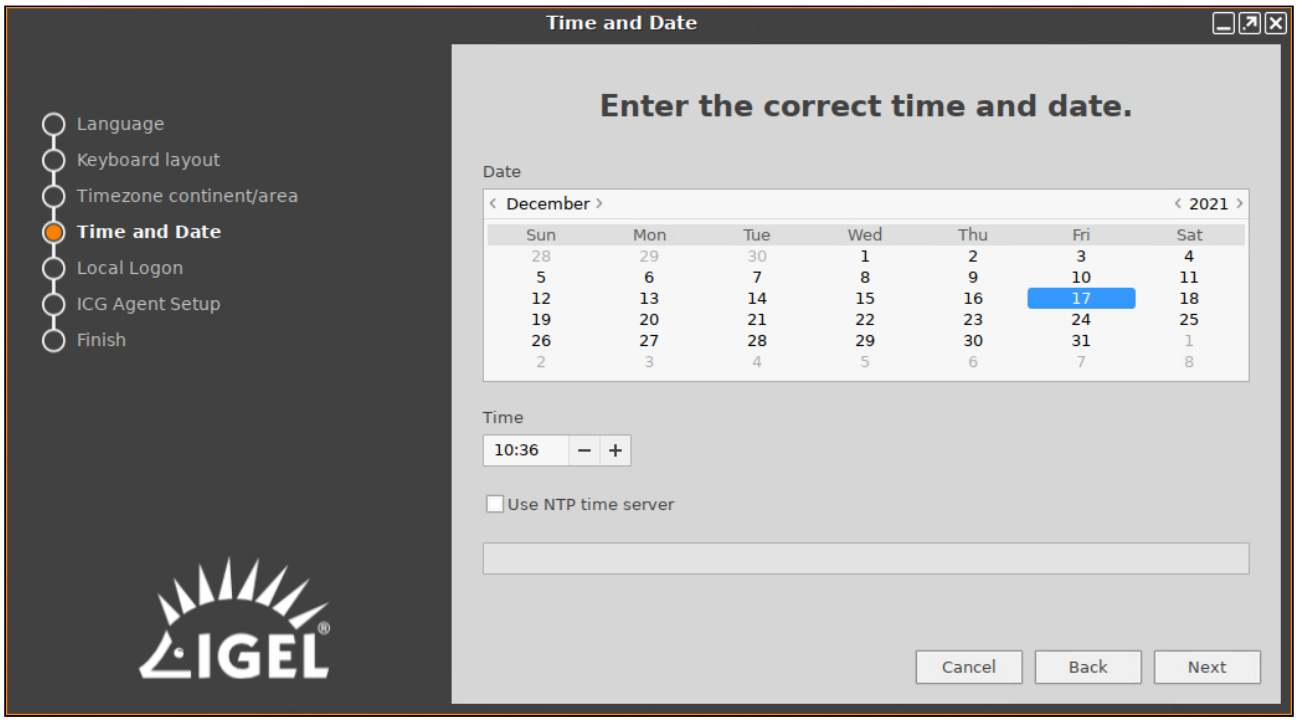
- **General**: Under **Location**, you can select a GMT time zone. (Default)
- **Africa... Pacific**: Under **Location**, you can select a city for the selected continent/area.

Location

Select your location or time zone.

> ### Location
>
> Summer time adjustment is taken into account here. Example: If you select "Berlin", the device will switch between summer time and normal time in accordance with the German adjustment rules. Time zone: The GMT time zones specify by how many hours the time zone for a particular location differs from the Greenwich time zone. The preceding symbol is used in accordance with the POSIX format. Examples: For New York City, select "GMT+5" which means "5 hours west of Greenwich". For Moscow, select "GMT-3" which means "3 hours east of Greenwich".

Time and Date



Date

Select the current date.

Time

Set the current local time.

Use NTP time server

☑ The device uses the NTP time server that is entered in the field. You can specify multiple NTP time servers separated by spaces. Example: `0.de.pool.ntp.org 1.de.pool.ntp.org`

> To configure an NTP server via a UMS profile, edit **Use NTP time server** and **NTP time server** under **System > Time and Date**. For details on profiles, see Using Profiles.

Next

Sets the system clock according to what is entered above.

Mobile Broadband

This configuration step is available if a surf stick / modem has been detected. If not detected, reboot your endpoint device.

Basic mode

In the basic mode (default), you can make the following settings:

Country or region

The country or region of your provider.

Provider

Provider (the possible options depend on what you choose for **Country or region**).

APN/Plan

APN/Plan (the possible options depend on what you select for **Provider**).

For more configuration options, click the **Expert Mode** button.

Expert mode

In the expert mode, you can make the following settings:

Enabled

Determines if the settings made in the expert mode are used. (Default: Enabled)

APN

APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.

Network ID

Network ID for your network connection. If you do not know the network ID, ask your mobile communications operator for it.

Number

Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.

User name

User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.

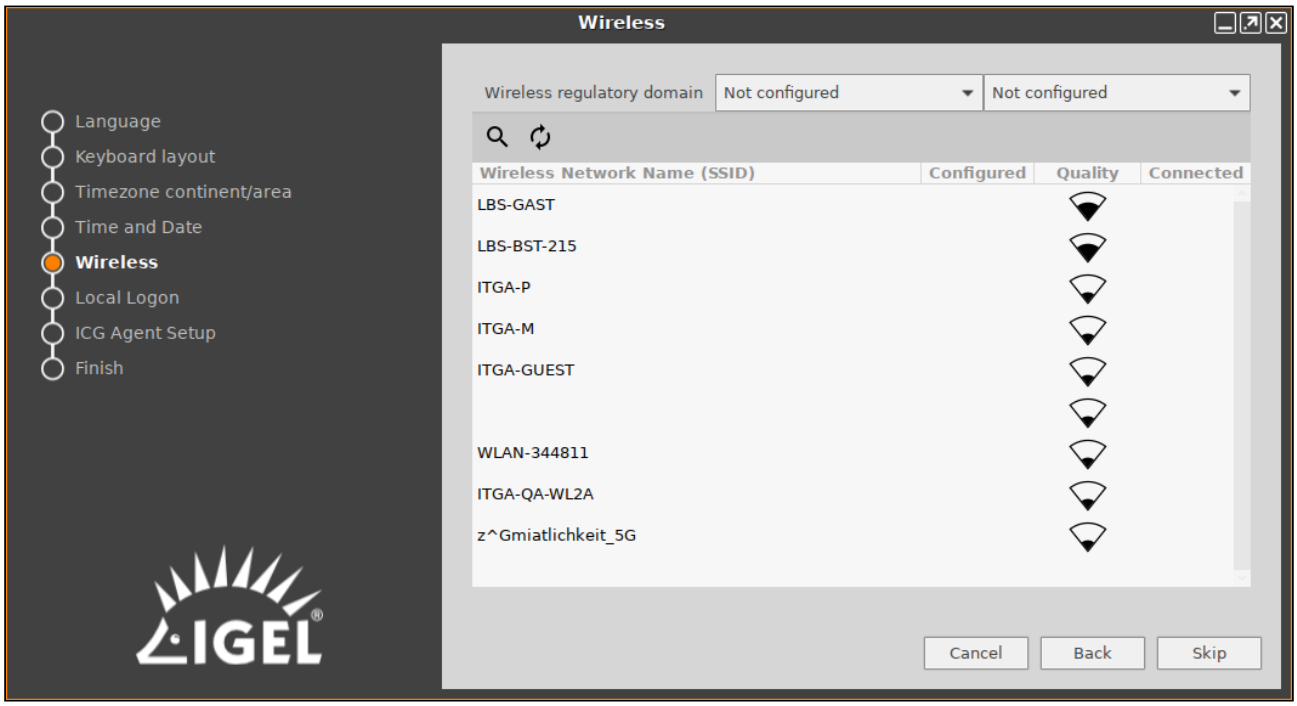
Password

Password for your network connection. If you do not know the password, ask your mobile communications operator for it.

PIN

PIN for the SIM card used.

Wireless



This configuration step is available if a WLAN adapter was found when starting the device. The device will search for available WLAN access points as soon as the configuration step is opened. The WLAN access points found will be listed. You can then connect to your desired WLAN access point.

If you carry out the WLAN configuration and exit the Setup Assistant by selecting **Finish**, the connection will be saved and WLAN will be permanently enabled. If you skip this configuration step or cancel the configuration, WLAN will not be permanently enabled.
If no Wi-Fi adapter is found, please check if:

1. There is a hardware switch on your device.
2. There is a BIOS setting that disables Wi-Fi if Ethernet is connected.
3. There is a BIOS update for your endpoint.

Wireless regulatory domain

In the first selection menu, select the world region (example: **Europe**) in which you are situated and in the second one the country (example: **United Kingdom**).

: Searches again for WLAN access points.

: Opens a dialog which allows you to enter the WLAN name (SSID) of a hidden WLAN access point.

(Name of a WLAN access point in the list): Click on your desired WLAN access point and enter your access data in the dialog.

Once the connection is established, the

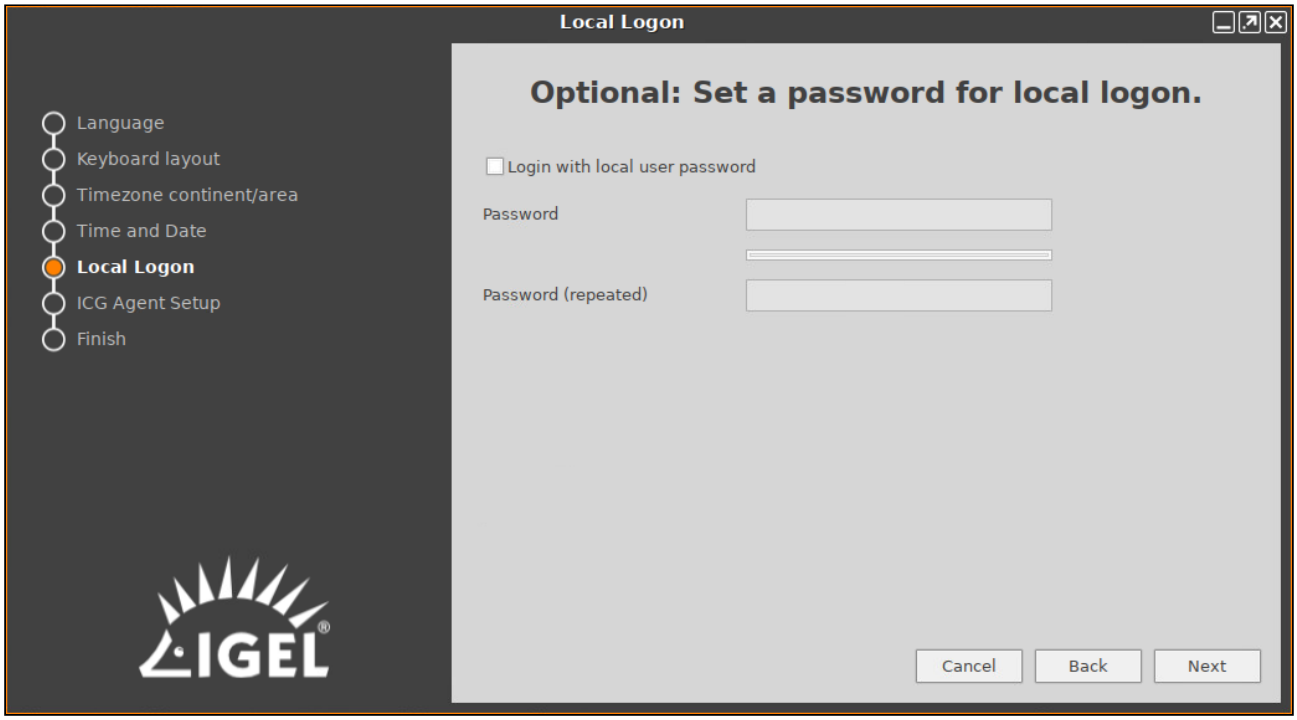
⇅ symbol will be shown in the **Connected** column.

Connectivity

This page is shown if for any reason no network connectivity is available.

Follow the instructions on the screen.

Local Logon



This step is optional. If you want to configure a local user password later, see Local User (see page 2039).

Login with local user password

☑ A login screen is shown upon the start of the device, and a local user password set under **Password** is used to log in.

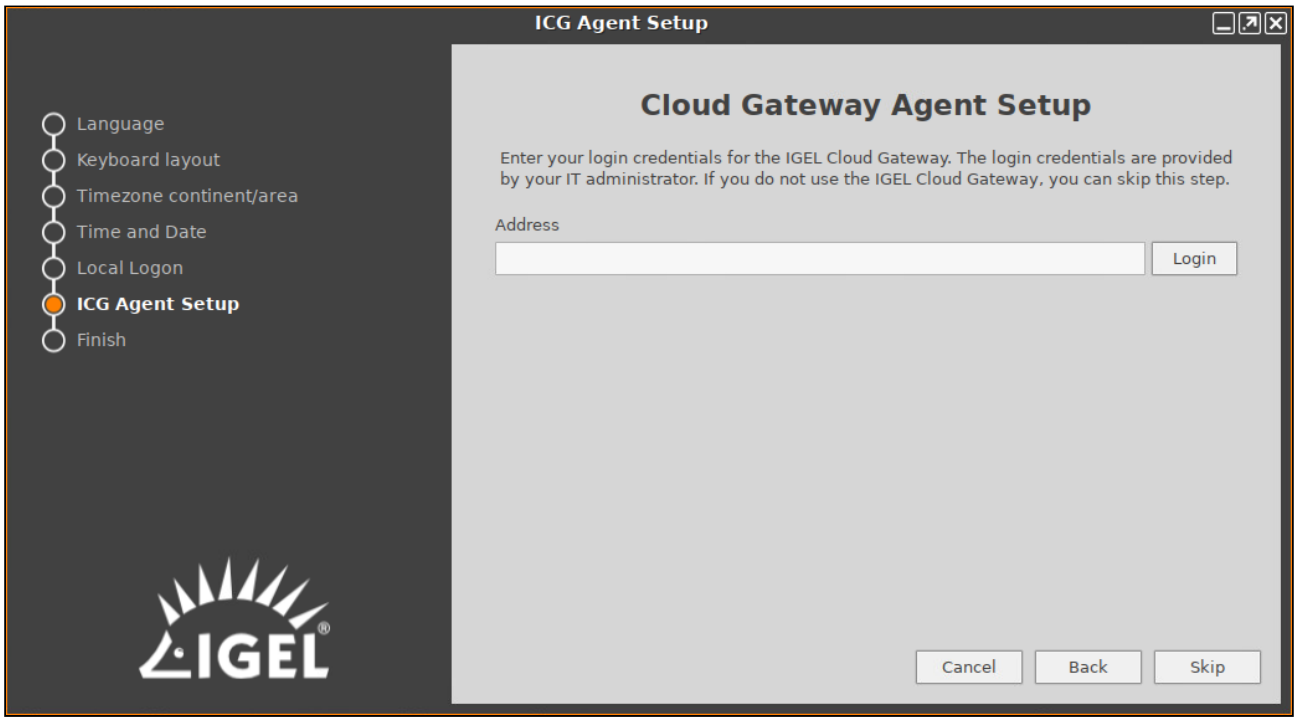
Password

Enter the desired password. The checker shown below assesses the strength of the password.

Password (repeated)

Repeat the password.

ICG Agent Setup

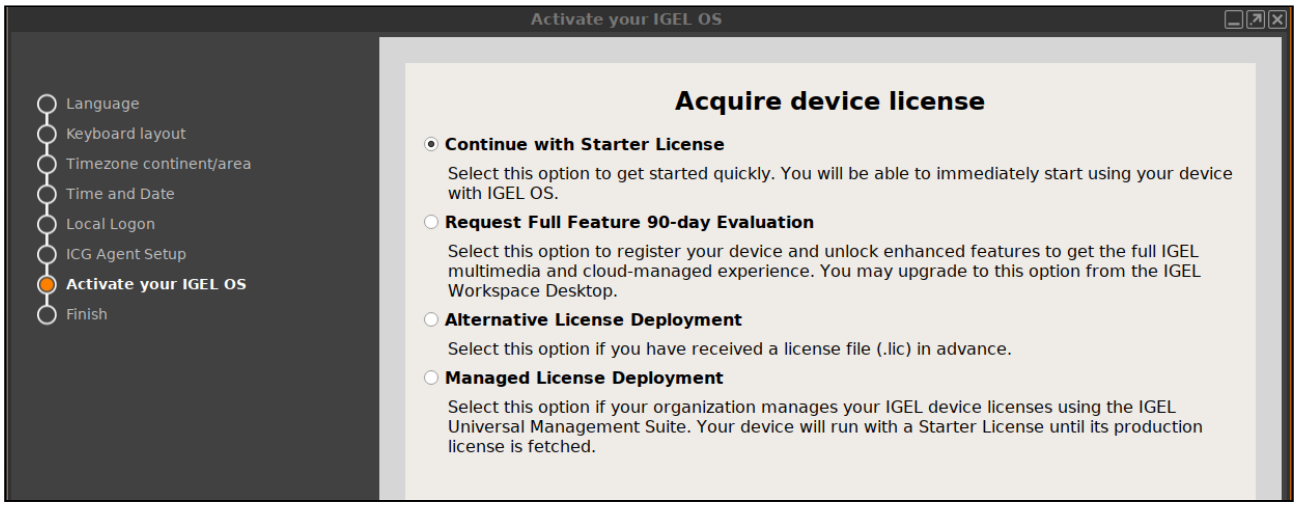


If your system administrator has given you access data for IGEL Cloud Gateway (ICG), you can connect the device to the gateway here.

You will find instructions for this under Using ICG Agent Setup (see page 1828).

Otherwise, do not touch this page and click on **Skip**.

Activate Your IGEL OS



In this step, you select the method for licensing your IGEL OS endpoint device. If the device has no license yet, the following options are available:

- **Continue with Starter License**
- **Request Full Feature 90-day Evaluation**
- **Alternative License Deployment** (Mostly needed if no IGEL UMS / ICG is in use)
- **Managed License Deployment** (Preferred if you use the IGEL UMS)

The options are described in detail further below.

Continue with Starter License

With the IGEL OS Starter License, you can use the endpoint device immediately. If the device is not managed by the IGEL Universal Management Suite (UMS), an End User License Agreement (EULA) must be accepted.

IMPORTANT: Multi-Media Codec Pack (MMCP) is not included, there is no Unified Communication or general performance optimization available.

Request Full Feature 90-Day Evaluation

With this evaluation license, all features of IGEL OS 11 are available for a fixed period. This period starts when the device has received the demo license.

For a demo license, you must accept the EULA to continue with setting up and using your device.

1. Make your choice as required and fill in all fields.
2. Activate the checkbox near **I agree to the terms + conditions and privacy policy**.
3. Click **ACTIVATE YOUR OS 11**.
   Your device fetches a demo license from IGEL.

Alternative License Deployment

You can deploy a license manually via HTTP download from a specific URL, via FTP, or from a USB memory stick.

To deploy a license from the HTTP server:

1. Enter the complete URL to the license file location in the text field, including the protocol.
2. Click **Install**.

To deploy a license from the FTP server:

1. Click **FTP**.
2. Define the access data for your FTP server:
   - **Host/Port**: URL of the FTP server on which the license file is located
   - **User**: User for accessing the FTP server
   - **Password**: Password associated with the **User**
3. Click **Browse**.
4. In the dialog, go to the license file and select it.
5. Click **Install**.

To deploy a license from a USB memory stick.

1. Click **File**.
2. Connect the USB flash drive that contains the license to the device.
3. Under **Storage Device**, select the USB flash drive that contains the license.
4. Click **Browse**.
5. In the dialog, go to the license file, select it and click **Open**.
6. Click **Install**.

Managed License Deployment

The device will request a license from the UMS. If the device is outside the company network, the IGEL Cloud Gateway (ICG) will be used for connecting the device to the UMS. In this case, ICG access must be set up; see the"ICG Agent Setup" section.

> Please note that the device will not immediately receive a license in this step.

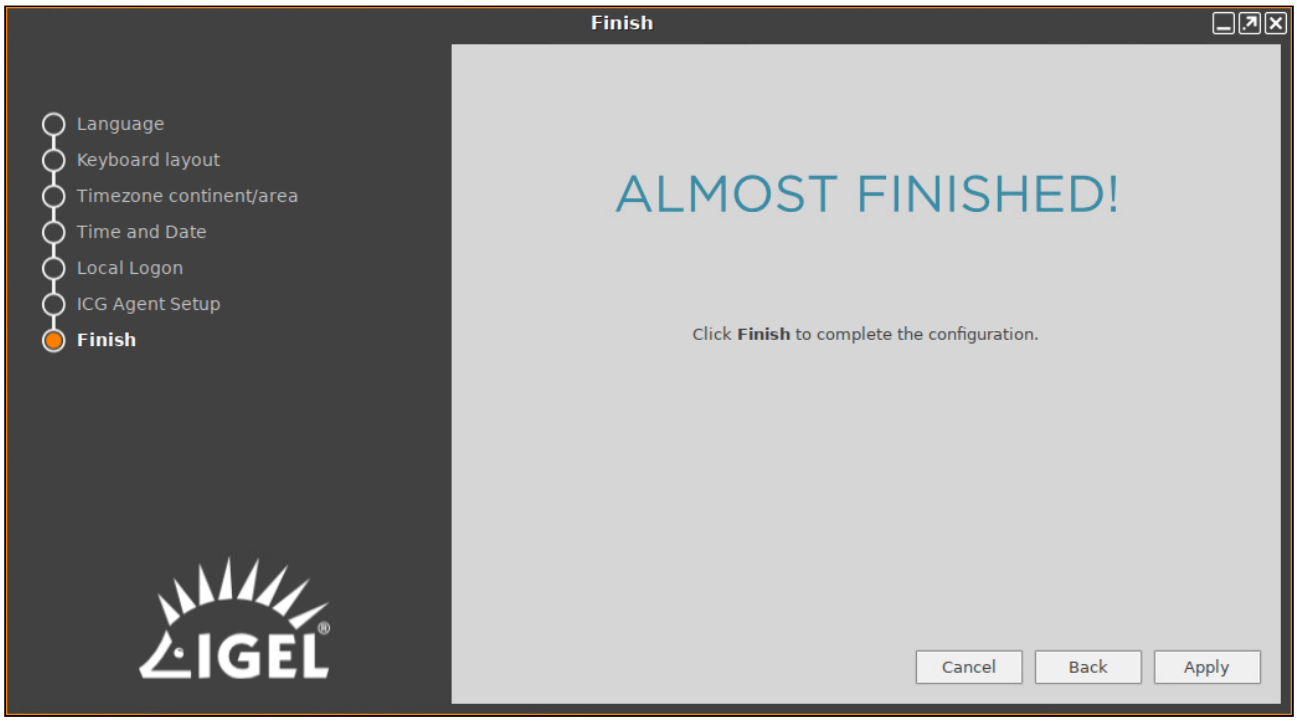
Troubleshooting: Proxy Configuration

If you get an error at this stage of the wizard, you may need to configure a proxy.

1. Click **Proxy configuration** in the upper right of the wizard to get to the proxy configuration dialog.
2. Edit the proxy settings as required:
   - **Use proxy server**: Activate this if a proxy is required.
   - **HTTP Proxy**: Address of the HTTP proxy
   - **Port**: Port of the HTTP proxy
   - **SSL Proxy**: Address of the SSL proxy
   - **Port**: Port of the SSL Proxy
   - **SOCKS Host**: Address of the SOCKS Host
   - **Port**: Port of the SOCKS host
   - **User name**: User name for authentication
   - **Password**: Password for authentication

     > **User name** and **Password** are the credentials for all proxy types configurable here (HTTP, SSL, and SOCKS).

Finish



Saves all settings and closes the Setup Assistant. If you have changed the language, the GUI X11 graphics system will restart; the screen will go black for a short time. If you have a UD Pocket Demo, a restart is required to finish the activation.

IGEL UD Pocket Manual

UD Pocket boots IGEL OS on your computer. However, it does not make any changes to the operating system already installed on the device's storage – UD Pocket runs entirely from the USB stick.

To facilitate booting your UD Pocket, you can use the IGEL UD Pocket Starter. The IGEL UD Pocket Starter creates a boot option for the UD Pocket so that there is no need to change the boot settings manually. You can install the IGEL UD Pocket Starter easily on an endpoint device running Microsoft Windows 10 or 11 - provided Microsoft BitLocker is not active on the device. When you uninstall the IGEL UD Pocket Starter, it is removed without any trace on the device.

UD Pocket, like all IGEL operating systems, can be managed centrally using the IGEL Universal Management Suite (UMS). UD Pocket uses IGEL OS, which is described in detail in the IGEL OS Reference Manual[240].

UD Pocket has a partition that contains this manual and is readable under Windows. The manual describes setting up and starting UD Pocket on your computer.

> This manual applies to https://kb.igel.com/hardware/current/technical-specification-of-ud-pocketand https://kb.igel.com/hardware/current/technical-specification-of-ud-pocket-2

Requirements

To use UD Pocket, your computer must meet the following requirements:

- USB 3.0 or 2.0 port from which the computer can boot
- Capability of booting from USB storage media
- Ethernet or wireless adapter. For a detailed list of supported graphics and network chips, see the IGEL Linux 3rd Party Hardware Database[241].
- The device is supported by IGEL OS; for details, see *Hardware* > *Supported Devices* > *Devices Supported by IGEL OS 11*.

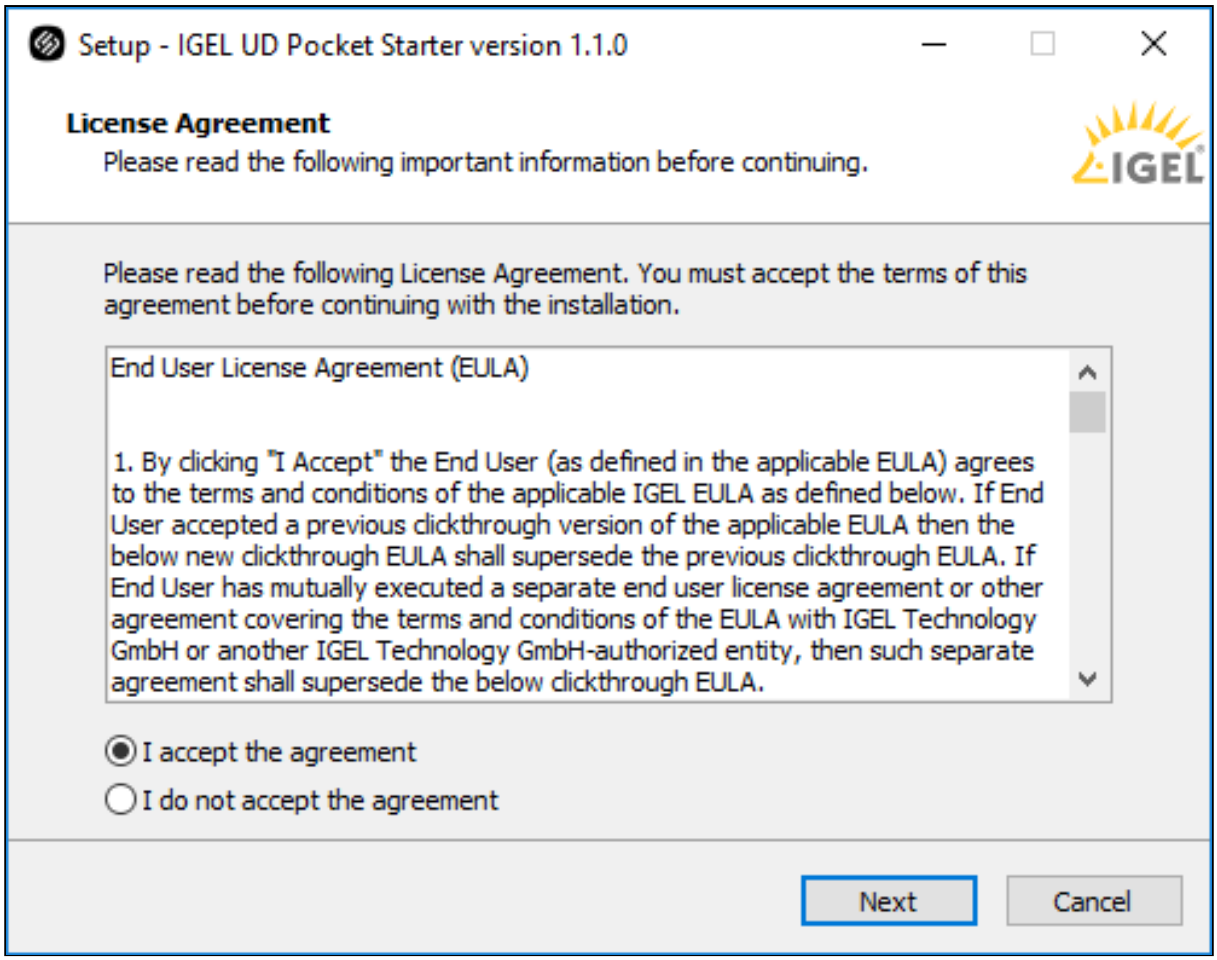
If you want to use the IGEL UD Pocket Starter, the following requirements apply:

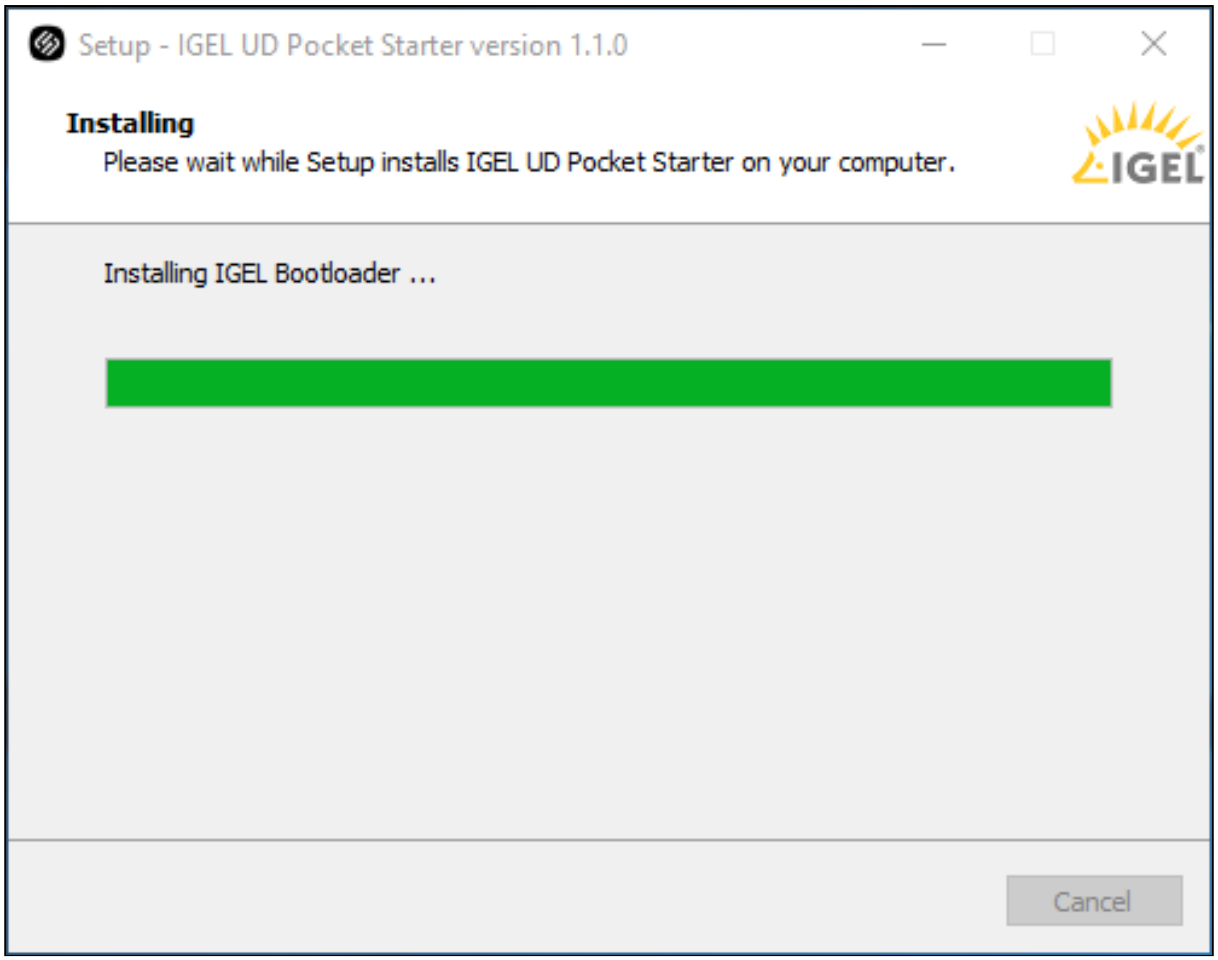
- Microsoft Windows 10 or 11 is installed on the endpoint device.
- The device has EFI BIOS
- Microsoft BitLocker is deactivated

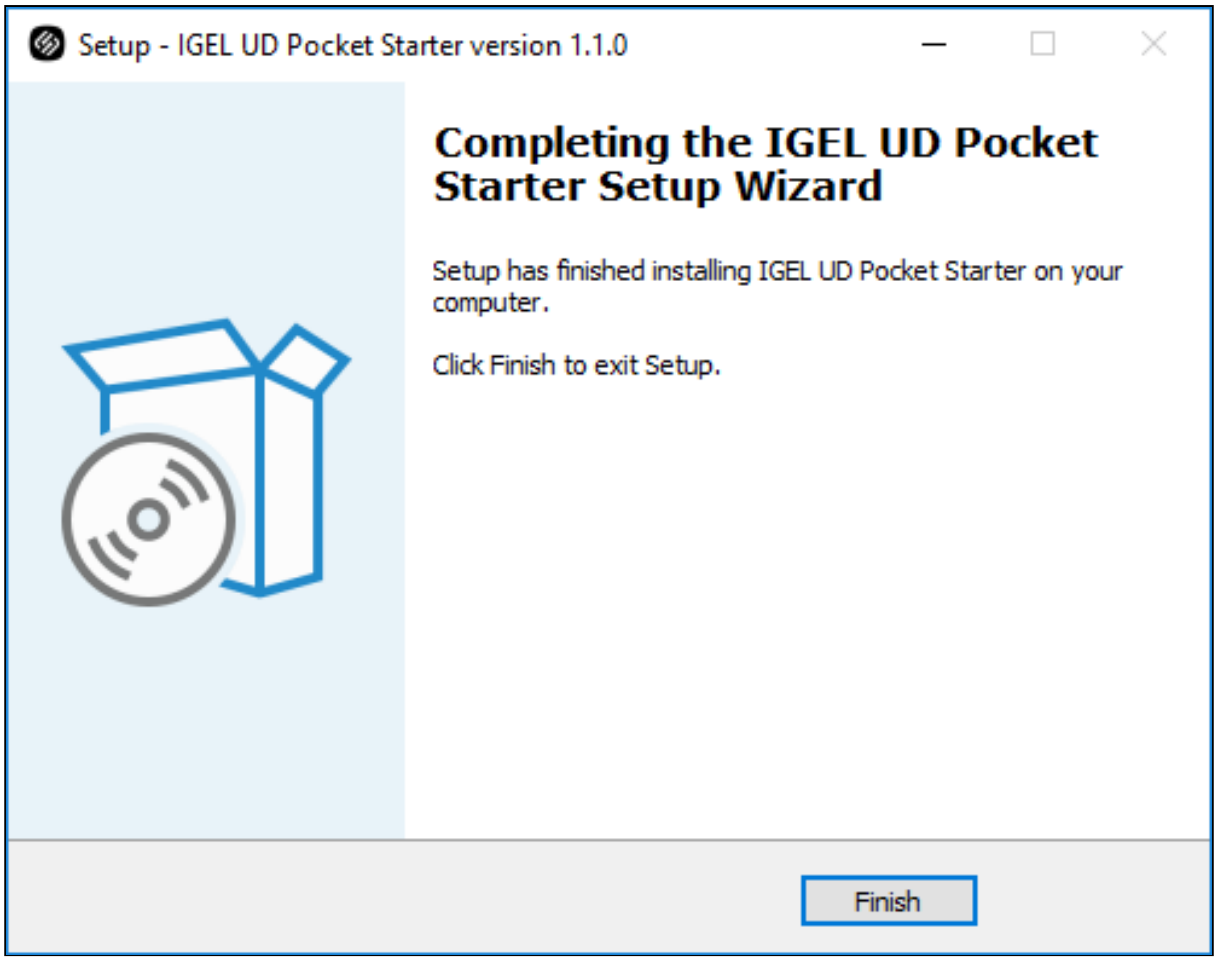
Installing the IGEL UD Pocket Starter

1. Download `setup-igel-udp_starter_<VERSION_NUMBER>.exe` from https://www.igel.com/software-downloads/
2. Copy the file to your endpoint device, double-click it, and follow the instructions of the IGEL UD Pocket Starter Setup Wizard.

240. https://kb.igel.com/en/igel-os/11.10.250/igel-os-reference-manual
241. https://www.igel.com/linux-3rd-party-hardware-database/


Setup - IGEL UD Pocket Starter version 1.1.0
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
End User License Agreement (EULA)
1. By clicking "I Accept" the End User (as defined in the applicable EULA) agrees to the terms and conditions of the applicable IGEL EULA as defined below. If End User accepted a previous clickthrough version of the applicable EULA then the below new clickthrough EULA shall supersede the previous clickthrough EULA. If End User has mutually executed a separate end user license agreement or other agreement covering the terms and conditions of the EULA with IGEL Technology GmbH or another IGEL Technology GmbH-authorized entity, then such separate agreement shall supersede the below clickthrough EULA.
I accept the agreement
I do not accept the agreement
Next
Cancel

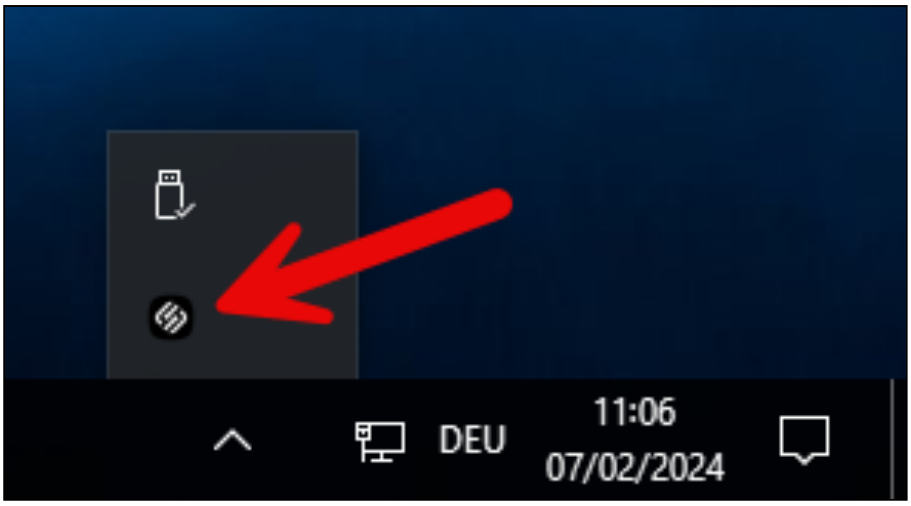

Setup - IGEL UD Pocket Starter version 1.1.0
Installing
Please wait while Setup installs IGEL UD Pocket Starter on your computer.
IGEL
Installing IGEL Bootloader ...
Cancel



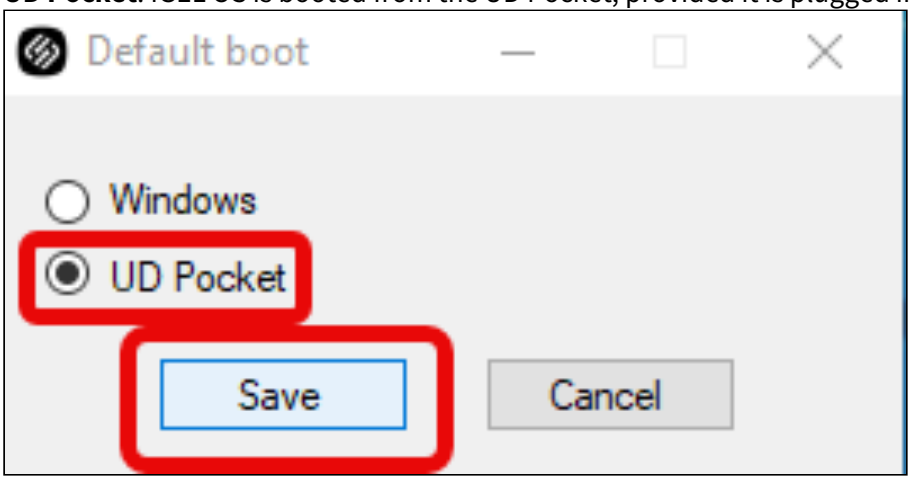
Configuring the Boot Order

You can define which operating system is booted by default, i.e. if the user does not make a selection in the boot menu.

1. In the system tray, double-click on the IGEL OS icon.



2. Choose the desired default operating system and click **Save**.
   - **Windows**: Windows is booted by default, even if a UD Pocket is plugged into the device.
   - **UD Pocket**: IGEL OS is booted from the UD Pocket, provided it is plugged in.



Starting Your IGEL UD Pocket (With IGEL UD Pocket Starter Installed)

1. Plug the UD Pocket into a free USB slot of your device.
2. Turn on your device; if the device is already switched on, restart it.
   Your device boots into IGEL OS, provided you have chosen this option when configuring the boot order (see page 2115).

Starting Your IGEL UD Pocket (Without IGEL UD Pocket Starter)

Booting from Your UD Pocket

1. Plug the UD Pocket into a free USB slot of your device.
2. Turn on your device; if the device is already switched on, restart it.
3. If a boot menu is presented that contains **IGEL UD Pocket** as an option, select this option. If not, proceed with Customizing the Boot Settings (see page 2117).

Customizing the Boot Settings

Booting from USB storage media may already be enabled on your device, or you may have to enable it yourself. The required key presses for this may vary from vendor to vendor. However, here are some hints:

→ While the device is booting, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access a list of boot devices and select **IGEL UD Pocket**.

→ If the above does not work, access the BIOS settings via pressing [Del], [F1], or [F2] during boot, activate booting from USB storage media, and/or change the boot order.

→ See the BIOS/UEFI documentation for your system for details on how to boot from USB storage media.

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft's 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see *Security & Safety > UEFI Secure Boot Enabling Guides > Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot.*

IGEL OS supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS. How to check whether Secure Boot has been properly enabled, you can learn under *Security & Safety > UEFI Secure Boot Enabling Guides > Verifying that Secure Boot is Enabled*.

If UD Pocket fails to boot in UEFI mode, try it in legacy/BIOS mode. If this does not help, try another endpoint device to verify that the UD Pocket is functional and/or check for BIOS updates for your endpoint device and for the latest IGEL OS updates.

Do not remove the UD Pocket from the computer until you have shut down the IGEL OS contained on it. Otherwise, you can damage the operating system on UD Pocket and lose your settings as well as data on other removable media.

After the First Boot-Up

The Setup Assistant guides you through the basic configuration. For a detailed description of each step, see Setup Assistant for IGEL OS (see page 2101).

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=iURhgESsn6k

Related Topics

How to Reflash Your IGEL UD Pocket (see page 1147)

UD Pocket (see page 1133)

IGEL OS Creator

- IGEL OS Creator Manual (see page 2120)
- IGEL OS Creator Articles (see page 2172)

IGEL OS Creator Manual

With the IGEL OS Creator (OSC), you can install IGEL OS 11 on any device that supports it. Moreover, you can use the IGEL OS Creator for recovering a broken installation of IGEL OS which is not able to boot anymore.

- General Information (see page 2121)
- Devices Supported by IGEL OS 11 (see page 2122)
- Licensing (see page 2124)
- Installation (see page 2125)

You can roll out IGEL OS also via the IGEL OS Deployment Appliance. For this purpose, you will need to install IGEL OS Deployment Appliance 11.0 or higher. See *IGEL OS Deployment Appliance*.

IGEL Tech Video

This is how you can reflash a device using IGEL OS Creator. See also How to Reflash Your IGEL UD Pocket (see page 1147).

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=z1Wp51KQ8tI

General Information

The IGEL OS Creator (OSC) software allows the migration of existing hardware to create a functionally standardized IGEL Workspace infrastructure. In the process, the existing operating system is replaced by IGEL OS. The devices can then be administered via the IGEL Universal Management Suite (UMS).

Installing the IGEL OS operating system via OSC destroys all data on the target device's mass storage device (hard disk, flash memory, SSD).

This manual describes the installation of IGEL OS 11 using OSC.

Devices Supported by IGEL OS 11

Core Requirements for IGEL OS 11

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

RAM size higher than 2 GB is recommended if you use any of the following:
Unified Communications optimizations (uses a client-side media engine)
- High-resolution graphics output
  For details on the supported graphics-related characteristics of IGEL devices, see Graphics on IGEL Devices or, for older devices, Graphics on Legacy IGEL Devices[242].
- More than two monitors

- Storage: 2 GB minimum; ≥ 4 GB recommended

Storage Requirements for IGEL OS 11.04 or Higher
IGEL OS 11.04.100 or higher requires at least 2.4 GB storage if the full feature set is applied. Thus, the feature set must be modified accordingly; for more information, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

IGEL Devices Supported by IGEL OS 11

IGEL UD (Universal Desktop)

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD2****	D220	40	Yes	2 GB	4 GB	Yes
UD2*	M250C	50	Yes	2 GB	4 GB	Yes
UD2	M250C	51 / 52***	Yes	2 or 4 GB	8 GB	Yes
UD3*	M340C	50	Yes	2 GB	4 GB	Yes
UD3*	M340C	51	Yes	2 GB	4 GB	Yes
UD3	M350C	60	Yes	4 GB	8 GB	Yes
UD5*	H830C	50	Yes	2 GB	4 GB	Yes
UD6*	H830C	51	Yes	2 GB	4 GB	Yes

242. https://kb.igel.com/knowledge-base-archive/current/

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	HW Video Acceleration
UD7	H850C	10	Yes	4 GB	4 GB	Yes
UD7**	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9*	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

*IGEL UD3-LX 50 and UD5-LX 50 are supported up to IGEL OS 11.05, incl. private builds.
IGEL UD9-LX 40 / 41 (Touch) devices are supported up to IGEL OS 11.07.910.
IGEL UD2-LX 50 devices are supported up to IGEL OS 11.09.160.
IGEL UD3-LX 51 devices are supported up to IGEL OS 11.09.160.
IGEL UD6-LX 51 devices are supported up to IGEL OS 11.09.160.

** As of December 2019, IGEL UD7 model H850C is equipped with the (en) AMD Secure Processor ; for further information, see (en) UD7 Model H850C .

*** IGEL UD2-LX 52 is supported with IGEL OS 11.06.140 and later.

**** UD2-LX 40 (model D220) is supported up to IGEL OS 11.08.200. For an overview of the end-of-sales (EOS) and end-of-maintenance (EOM) dates for IGEL devices, see Legacy IGEL OS Hardware Support[243] .

IGEL Zero

Note on IZ Devices
The IZ devices listed below can be upgraded to IGEL OS 11. To upgrade your IZ devices to IGEL OS 11, please contact your IGEL sales representative. See also https://www.igel.com/os11migration/ .

Product Line	Device Type	Hardware ID	64 Bit	Memory (RAM)	Storage	UEFI Secure Boot Support	HW Video Acceleration
IZ2	D220	40	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	50	Yes	2 GB	4 GB	Yes	Yes
IZ3	M340C	51	Yes	2 GB	4 GB	Yes	Yes

Third-Party Devices

For an up-to-date list, see Devices Supported by IGEL OS 12 .

243. https://kb.igel.com/knowledge-base-archive/current/

Licensing

For information on licensing, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses*.

Installation

- Installation Requirements (see page 2126)
- Create USB installation medium (Windows) (see page 2127)
- Create USB installation medium (Linux) (see page 2130)
- Create DVD installation medium (see page 2132)
- Boot Settings (see page 2133)
- Installation Procedure (see page 2137)
- Installation Procedure for Factory Images (see page 2150)

Installation Requirements

In order to install IGEL OS via OSC, the target device must meet the following requirements:

- 64-bit-capable CPU
- CPU speed ≥ 1 GHz

⚠ When using multimedia content (e.g. Unified Communications), a Dual Core CPU with at least 1.5 GHz is recommended.

- Minimum 2 GB RAM; higher RAM size is recommended if you use any of the following:
  - Unified Communications optimizations (uses a client-side media engine)
  - High-resolution graphics output
  - More than two monitors
- Storage: If the full feature set is applied, at least 4 GB of storage is required. For instructions on how to reduce the feature set, see Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318).
- Intel, ATI/AMD or Nvidia graphics chip

ℹ For information about supported graphics chipsets, see the IGEL Linux 3rd Party Hardware Database[244].

- USB 3.0 or 2.0 port from which the device can boot (alternatively a DVD drive)
- Ethernet or wireless adapter

ℹ If these requirements are not fulfilled, the full functionality of the device with IGEL OS can not be guaranteed, and technical support will not be provided by IGEL.

✖ Installing IGEL OS via OSC destroys all data on the target device's mass storage device (hard disk, flash memory, SSD).

244. https://www.igel.com/linux-3rd-party-hardware-database/

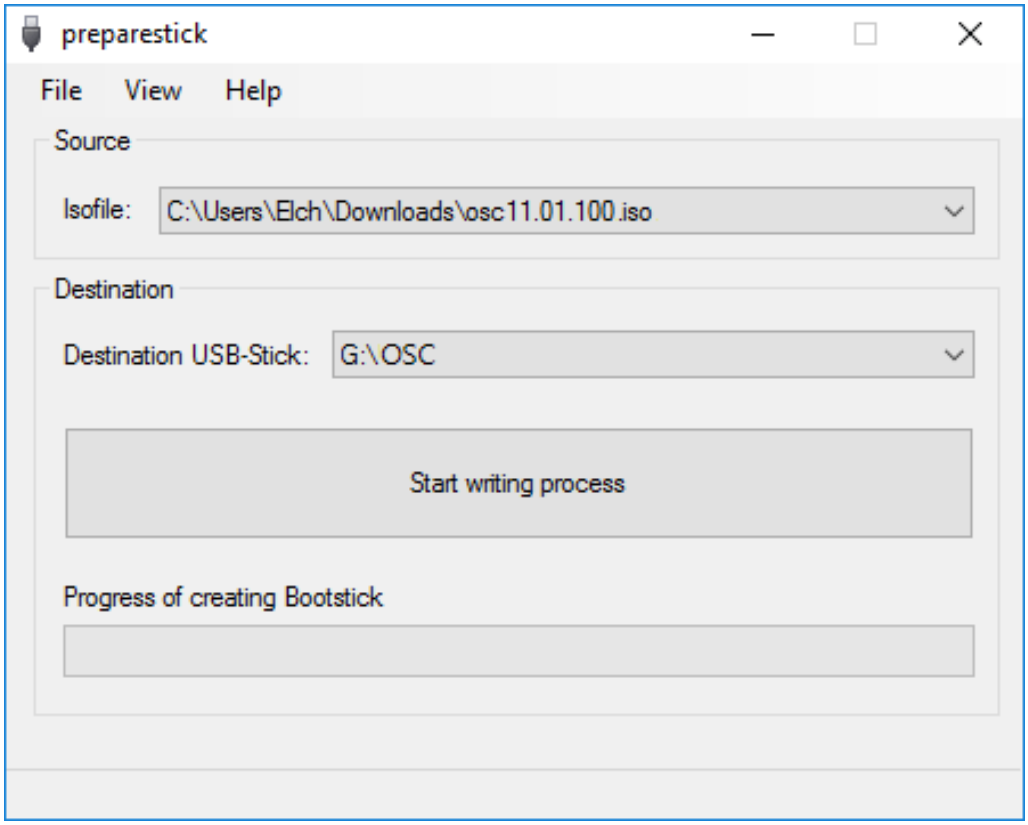
Create USB installation medium (Windows)

1. Download the ZIP archive for OS Creator from our download server[245]:
   - For new devices, use the standard installer (e. g. OSC_11.01.100.zip).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e. g. OSC_11.01.100_legacy.zip).
2. Unzip the contents into a local directory.
3. Connect a USB memory stick with at least 4 GB capacity to the computer.

All existing data on the USB memory stick will be destroyed.

4. Double-click the `preparestick.exe` file from the unzipped directory.

If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.



The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

5. Under **Isofile**, select the appropriate ISO file, e. g. `osc11.01.100.iso`

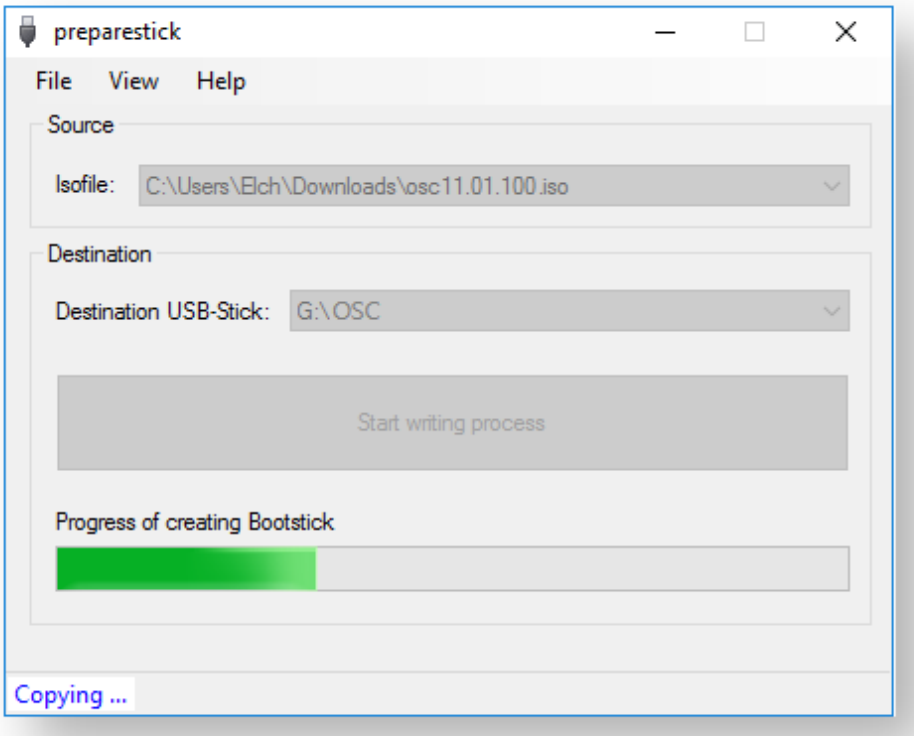
245. https://www.igel.com/software-downloads/workspace-edition/

6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.

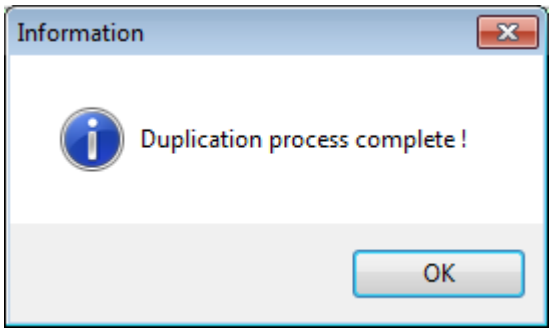
It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.

Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List.**

7. Click on **Start writing process**.
   In the program window, the progress of the process is shown.



When the process is finished, a message window is displayed.



8. Close the message window and the program.
9. After about 3 seconds, remove the USB memory stick.

If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

Create USB installation medium (Linux)

1. Download the ZIP archive for OS Creator from our download server[246]:
   - For new devices, use the standard installer (e. g. OSC_11.01.100.zip).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e. g. OSC_11.01.100_legacy.zip).
2. Unzip the contents into a local directory.
3. From this directory, you will need the ISO file (e. g. `osc11.01.100.iso` or `osc11.01.100_legacy.iso`) to create a bootable medium.
4. Connect a USB memory stick with at least 4 GB capacity to the computer.

> All existing data on the USB memory stick will be destroyed.

5. Open a terminal emulator and enter the command `dmesg` to determine the device name of the USB memory stick.
   Example output:

```
[...]
[19514.742229] scsi 3:0:0:0: Direct-Access JetFlash Transcend 8GB 1100 PQ: 0 ANSI: 6
[19514.742805] sd 3:0:0:0: Attached scsi generic sg1 type 0
[19514.744688] sd 3:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/7.35 GiB)
[19514.745370] sd 3:0:0:0: [sdb] Write Protect is off
[19514.745376] sd 3:0:0:0: [sdb] Mode Sense: 43 (0) 00 00 00
[19514.746040] sd 3:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[19514.752438] sdb: sdb1
```

   In this example, the device name searched for is `/dev/sdb`.

> Ensure that you have determined the correct device name. Use of the `dd` command in the next step can destroy your operating system if you use the wrong device name.

6. The following command writes the installation data to the USB memory stick:

```
dd if=osc11.01.100.iso of=/dev/sdX bs=1M oflag=direct
```

246. https://www.igel.com/software-downloads/workspace-edition/

Replace `sdX` with the device name of the USB memory stick that you have determined.

When the `dd` command has terminated, you can see the terminal emulator input prompt again.

7. Wait for about 3 seconds after the `dd` command has terminated, and remove the USB memory stick.

If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

The USB memory stick for OSC installation is ready for use.

Create DVD installation medium

The ISO file in the installation directory for OSC is a so-called hybrid image. It can not only be copied onto USB storage devices but can also be used to create a bootable DVD.

Burn ISO Image (Windows)

1. In Explorer, open the directory that contains the ISO file.
2. Right-click on the ISO file.
3. Select **Burn disc image**.

Burn ISO Image (Linux)

Under Linux, various burning programs with a graphical user interface or for the command line are available.

The Ubuntu Wiki[247] explains how to burn an ISO image onto a DVD using a number of programs.

247. https://help.ubuntu.com/community/BurningIsoHowto#Burning_from_Ubuntu

Boot Settings

OSC works on systems with BIOS and UEFI.

It is essential that your system supports booting from USB storage media or from DVD. This may already be enabled, or you may have to enable it yourself.

IGEL OS 11 supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS. How to check whether Secure Boot has been properly enabled, you can learn under *Security & Safety > UEFI Secure Boot Enabling Guides > Verifying that Secure Boot is Enabled*.
For UEFI Secure Boot on IGEL devices, see *Security & Safety > UEFI Secure Boot Enabling Guides*

If IGEL OS fails to boot in UEFI mode, try it in legacy/BIOS mode. IGEL OS will then be installed in legacy/BIOS mode.

For older devices or if you haven't been able to boot the installer at all, use the legacy installer under https://www.igel.com/software-downloads/workspace-edition/ **> OS 11 > OS CREATOR > LEGACY**.

Third-Party Devices

The required key presses for this may vary from vendor to vendor. However, here are some hints:

->While the device is booting, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) in order to access a list of boot devices and select your USB installation medium.

->If the above does not work, access the BIOS settings via pressing [Del], [F1], or [F2] during boot and activate booting from USB storage media and/or change the boot order.

->See the BIOS/UEFI documentation for your system for details of how to boot from USB storage media.

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft's 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see *Security & Safety > UEFI Secure Boot Enabling Guides > Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot.*

IGEL Devices

If the USB installation medium is not found, though the USB boot is enabled, try the following:

- Reconnect the USB installation medium and reboot the endpoint device.

- Use another USB port.

UD7 (H850C and H860C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD6 (H830C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD5 (H830C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select the **Boot** tab.
4. Select **Boot Options Priorities**.
5. Select the entry for the USB stick and move it to the first position using the [+] key.
6. Save the settings and exit.
7. You can continue with the Installation Procedure (see page 2137).

UD3 (M350C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.

6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD3 (M340C)

1. Power up the device while pressing [Del] button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD2 (M250C)

1. Power up the device while pressing [Del] button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD2 (D220)

1. Power up the device while pressing the [F2] (older devices) or [Del] (newer devices) button repeatedly in rapid succession.
2. Select **SCU**.
3. If a password prompt is shown, enter the BIOS password.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [F2] or [Del] (newer devices) button repeatedly in rapid succession.

9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the Installation Procedure (see page 2137).

UD9 (TC215B)

1. Power up the device while pressing the [F2] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select the **Boot** tab.
4. Select **Boot Option Priorities**.
5. Select the entry for the USB stick and move it to the first position using the [+] key.
6. Save the settings and exit.
7. You can continue with the Installation Procedure (see page 2137).

Installation Procedure

This article describes the regular installation procedure for single devices with the IGEL OS Creator (OSC). If you are an IGEL third-party endpoint partner (i.e. hardware manufacturer, independent hardware vendor, reseller) that has a factory ID from IGEL, please refer to Installation Procedure for Factory Images (see page 2150).

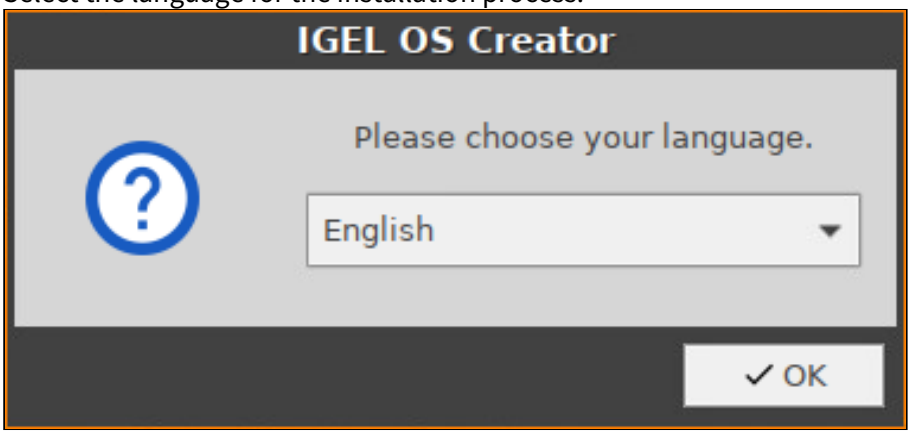
The installation will overwrite all existing data on the target drive.

1. Connect the prepared USB memory stick to the target device and switch the target device on.
2. Select one of the following options from the boot menu:

- **Standard Installation + Recovery**: Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery**: Boots the system from the USB memory stick and shows the Linux boot messages in the process. You can use a USB serial adapter for debugging purposes. For this purpose, the Registry key `system.kernel.bootparams.serial_console_debug` must be enabled (path: **System > Registry > system > kernel > bootparams > serial_console_debug > Enable**

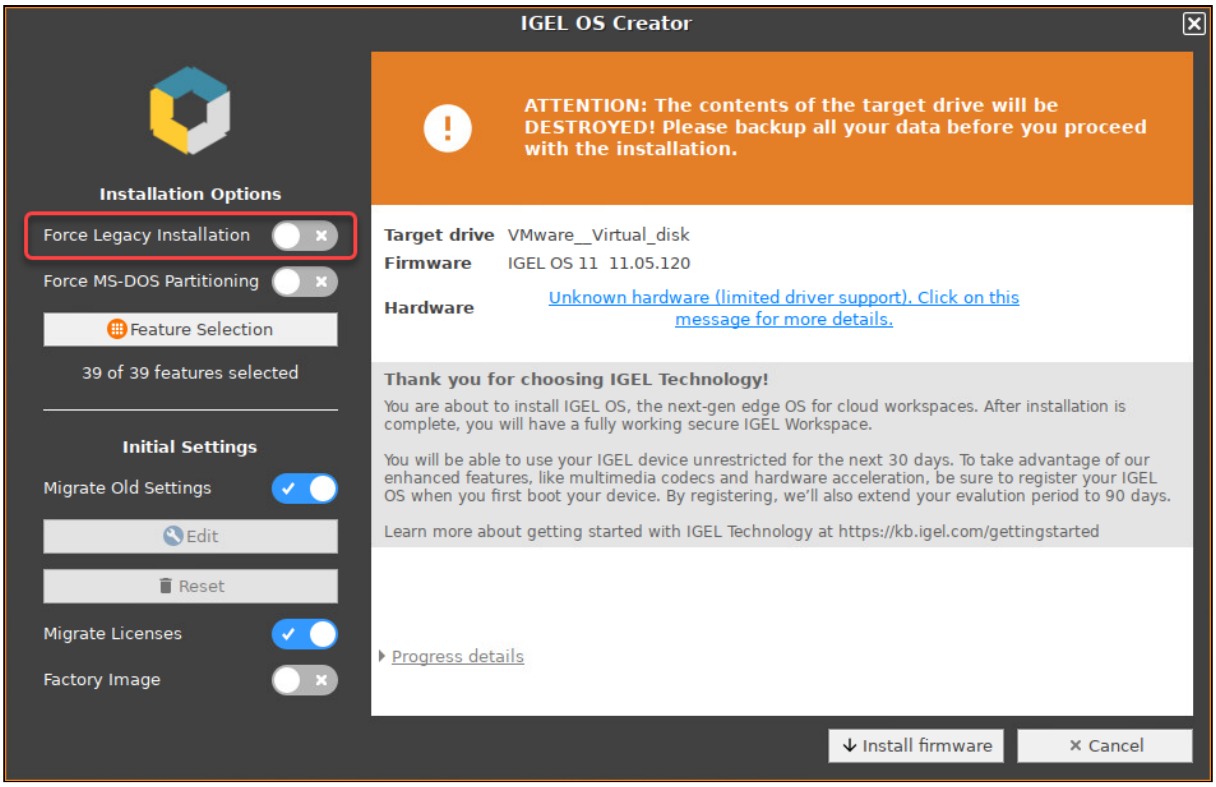
debug console on serial port 1). The serial port parameters are as follows: 115200 baud, 8 bits, 1 stop bit, no parity, no flow control.
- **Failsafe Installation + Recovery**: Fallback mode to be used if the graphical boot screen cannot be displayed.
- **Memory Test**: Memory test, only available in legacy/BIOS mode. This option does not carry out an installation.
- **EFI Debug Shell**: Available only in UEFI boot mode. If the hardware in use is EFI-capable, boot problems can be analyzed with that.

3. Select the language for the installation process.

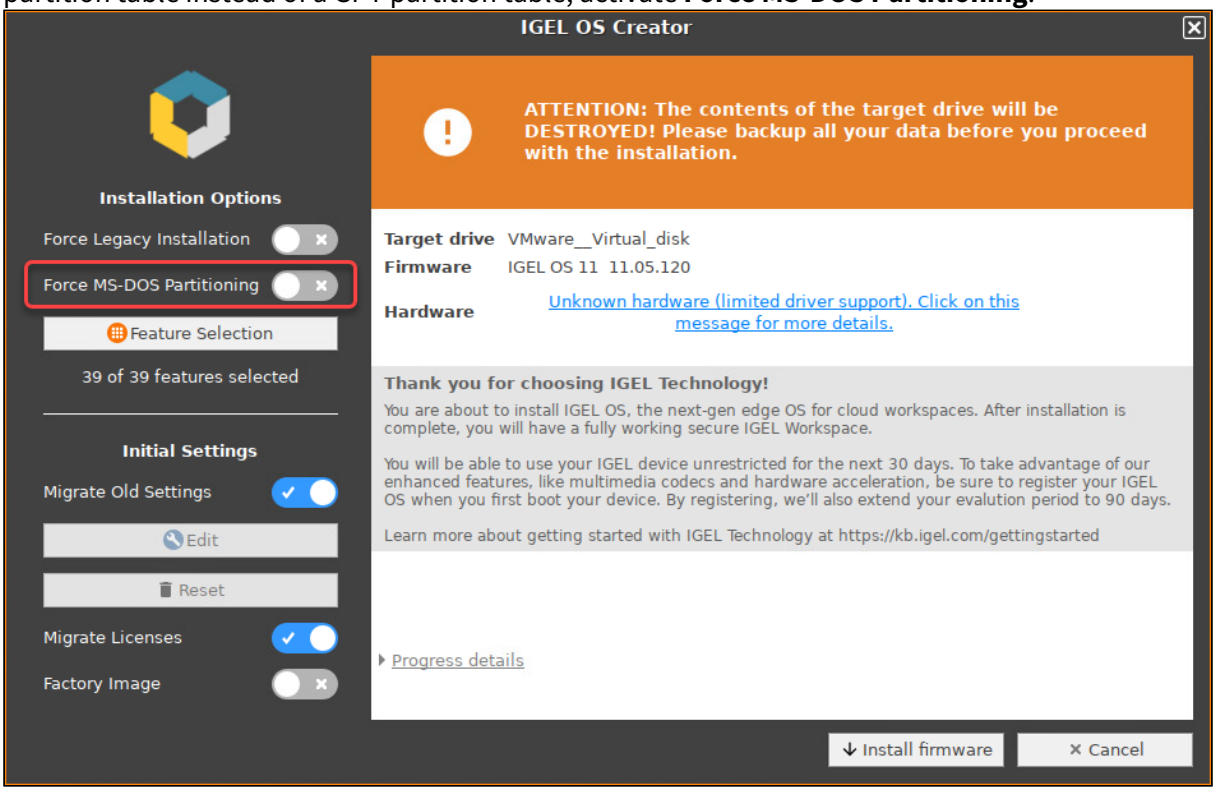


4. Optional, only available if your device has booted in UEFI mode: If you want to install the legacy/BIOS version of IGEL OS 11, activate **Force Legacy Installation**.

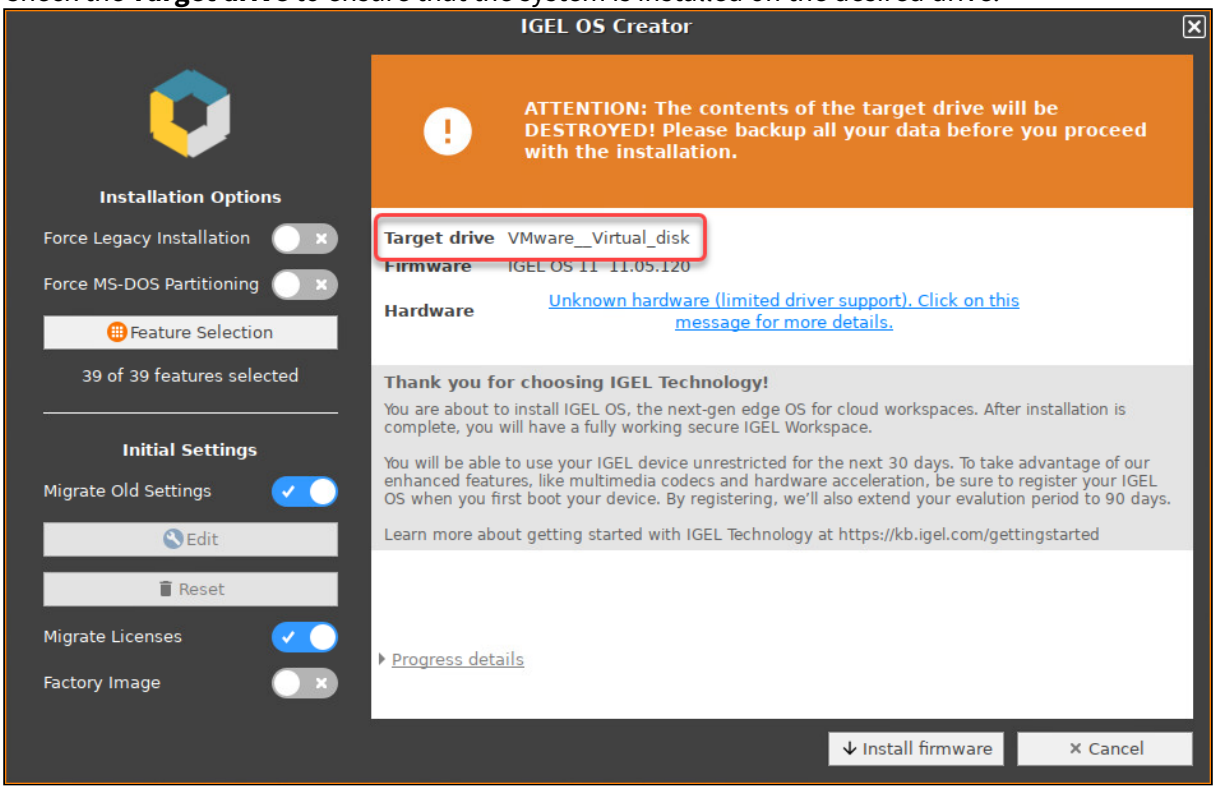
> If you have activated **Force Legacy Installation**, remember to set the system to legacy/BIOS mode after installation.



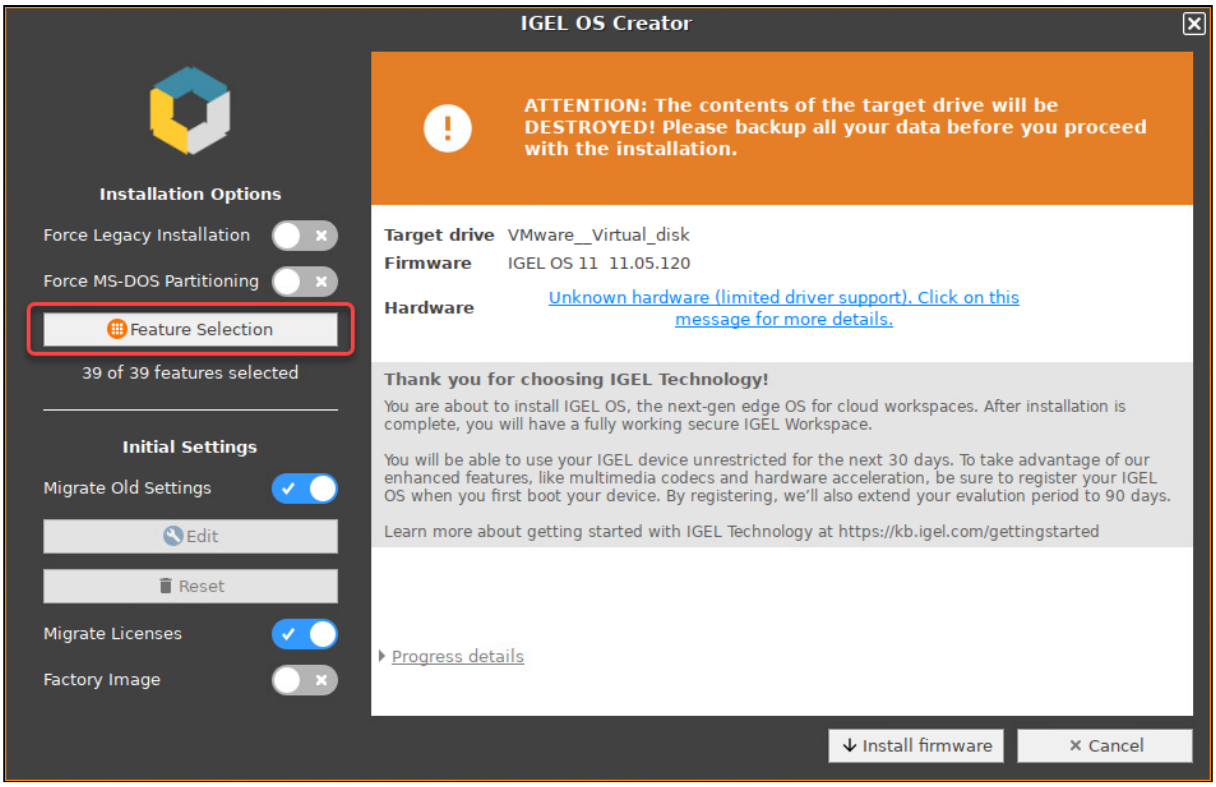
5. Optional, only available if your device has booted in UEFI mode: If you want to use an MS-DOS partition table instead of a GPT partition table, activate **Force MS-DOS Partitioning**.

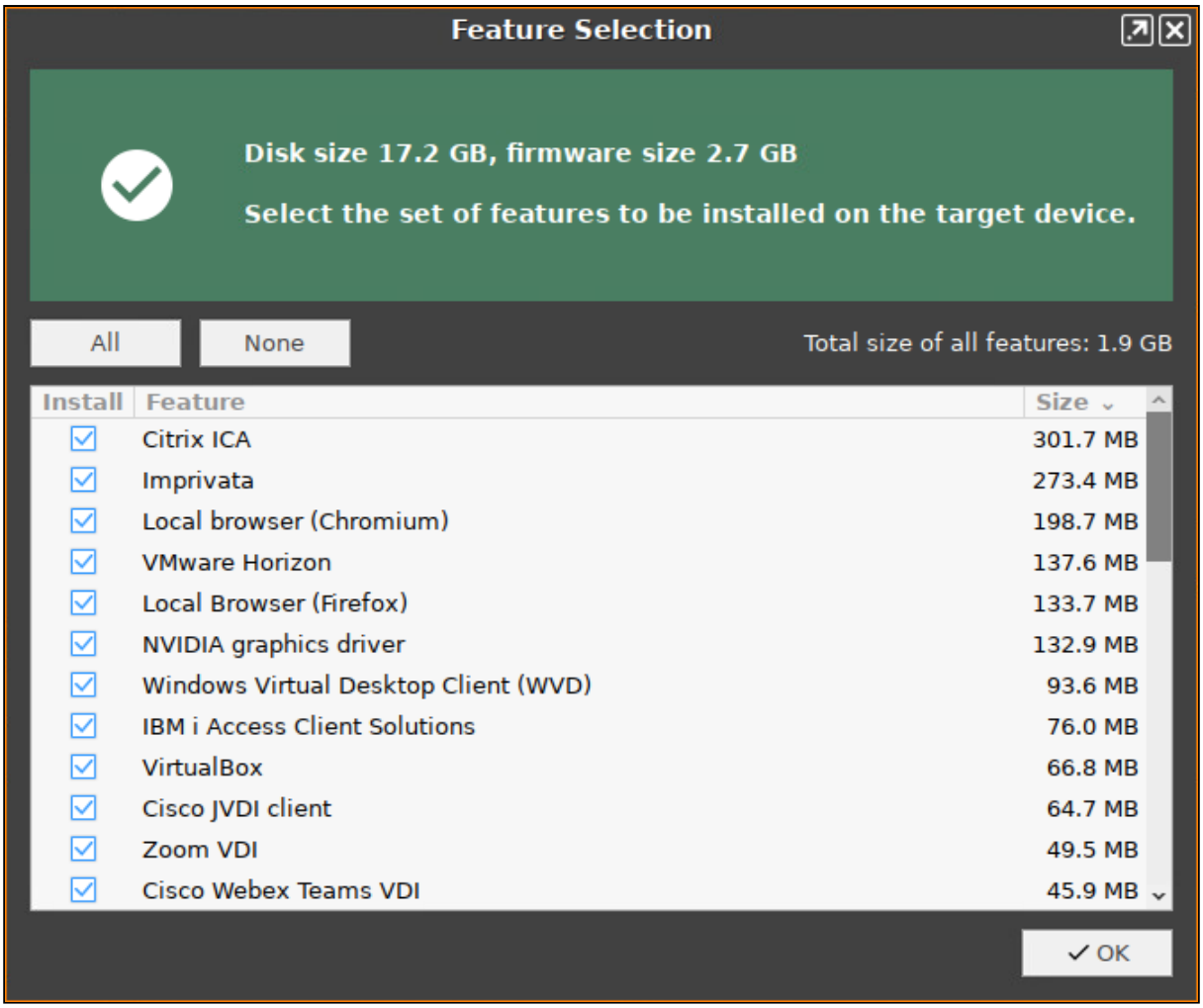


6. Check the **Target drive** to ensure that the system is installed on the desired drive.



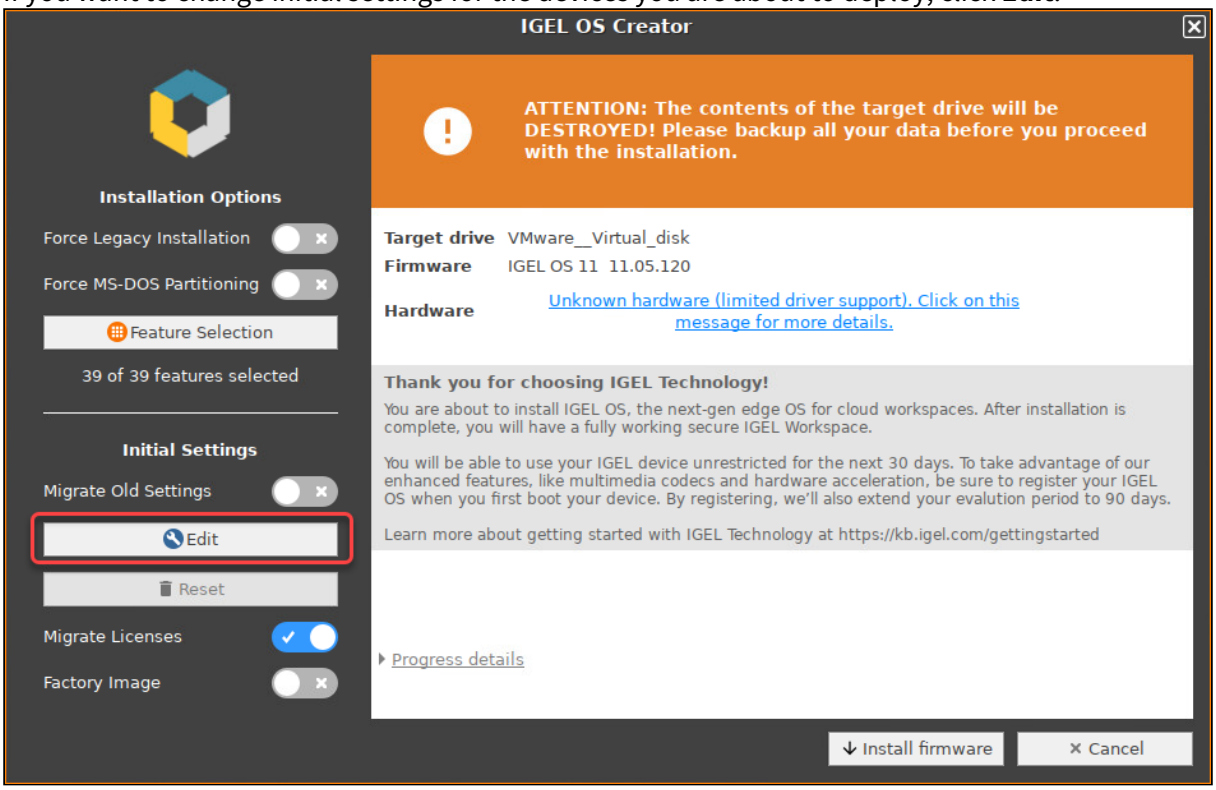
7. If you want to exclude features of IGEL OS, e.g. to save storage space, click **Feature Selection** and edit the settings as required.


IGEL OS Creator
Installation Options
Force Legacy Installation
Force MS-DOS Partitioning
Feature Selection
39 of 39 features selected
Initial Settings
Migrate Old Settings
Edit
Reset
Migrate Licenses
Factory Image
ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.
Target drive VMware__Virtual_disk
Firmware IGEL OS 11 11.05.120
Hardware
Unknown hardware (limited driver support). Click on this message for more details.
Thank you for choosing IGEL Technology!
You are about to install IGEL OS, the next-gen edge OS for cloud workspaces. After installation is complete, you will have a fully working secure IGEL Workspace.
You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.
Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted
Progress details
Install firmware
Cancel



- **All**: Select all features
- **None**: Select no feature
- **Feature**: Sort the list alphabetically
- **Size**: Sort the list by the memory requirements of the features

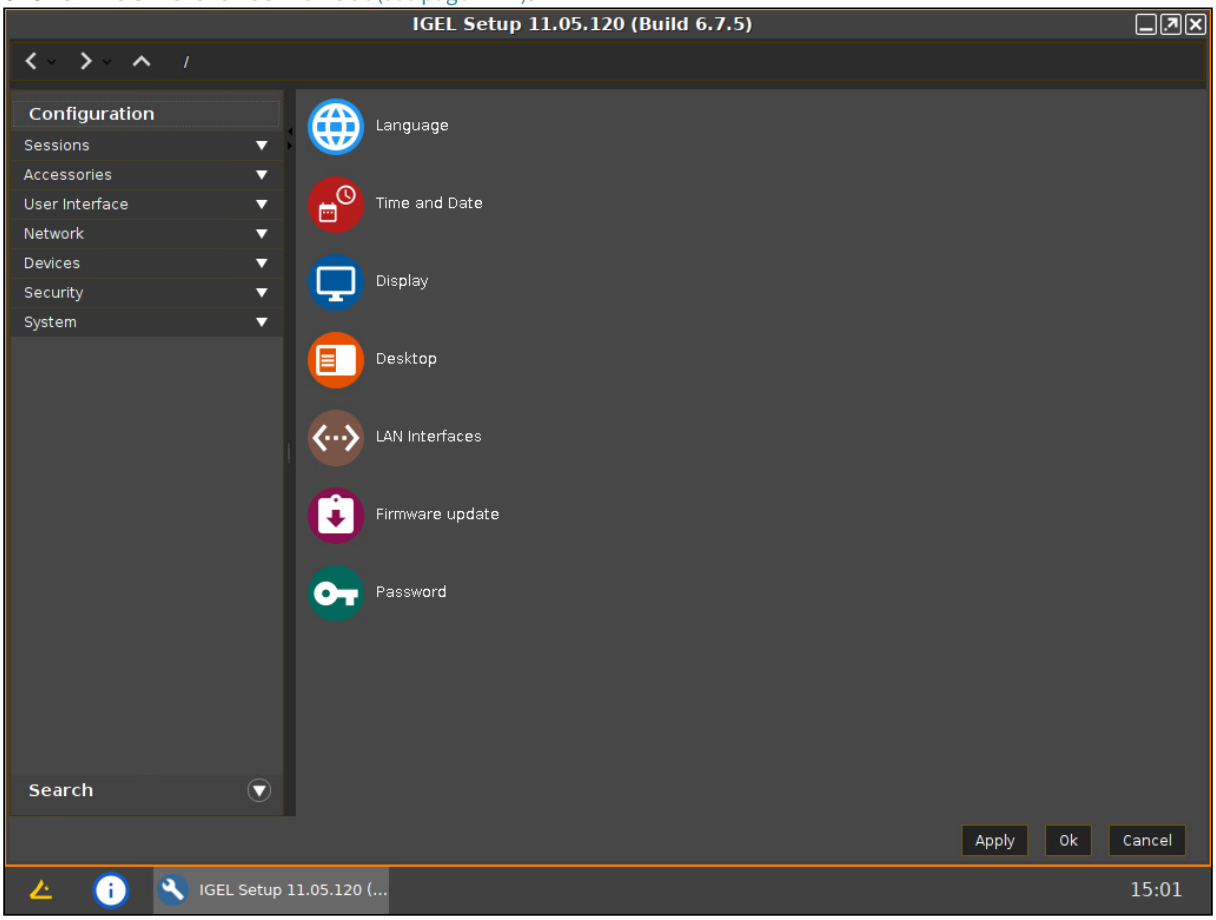
8. If you want to change initial settings for the devices you are about to deploy, click **Edit**.



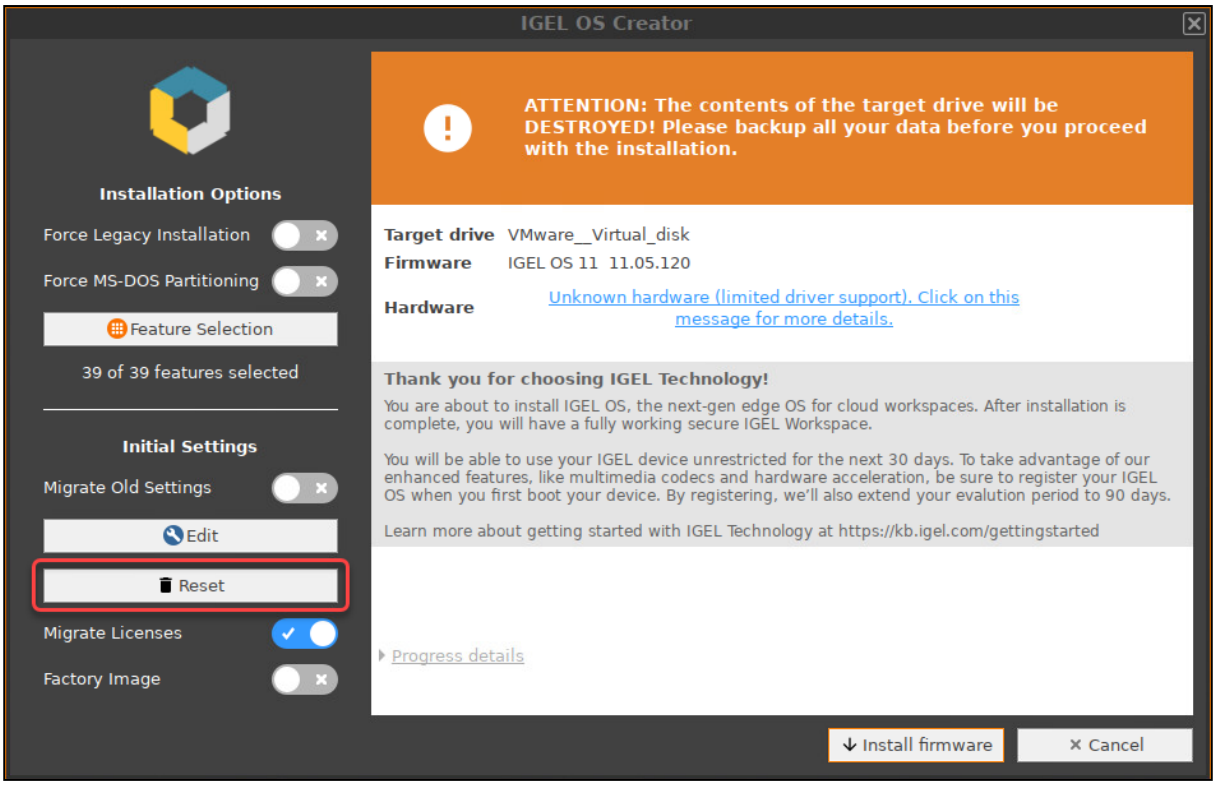
The IGEL Setup opens, enabling you to change the settings in the same way as with a regular IGEL OS installation.

The changes are stored on the USB memory stick from which the IGEL OS Creator (OSC) is executed. When you use this USB memory stick for subsequent OSC installations, your custom settings will be re-used. This allows you to easily create a number of IGEL OS installations with custom settings.

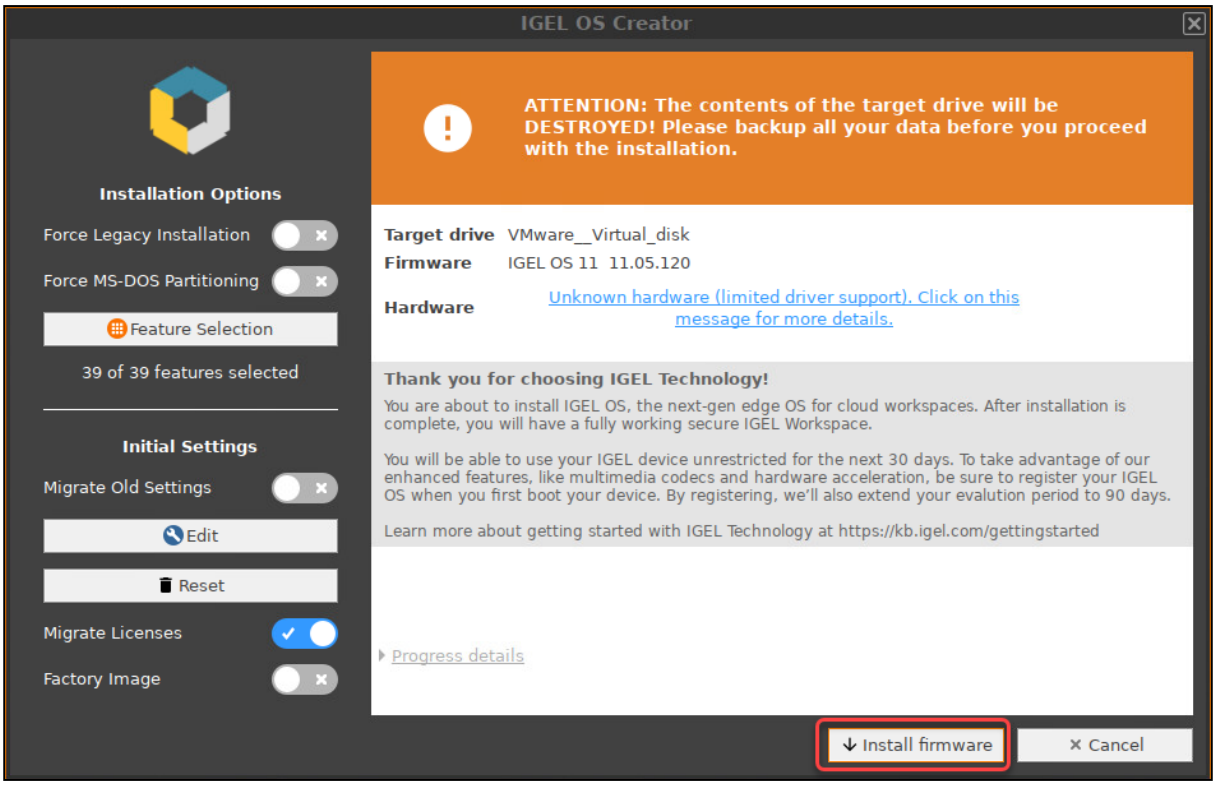
For details about the settings, see the chapters Setup (see page 1237) and the subsequent chapters in the IGEL OS Reference Manual (see page 1211).



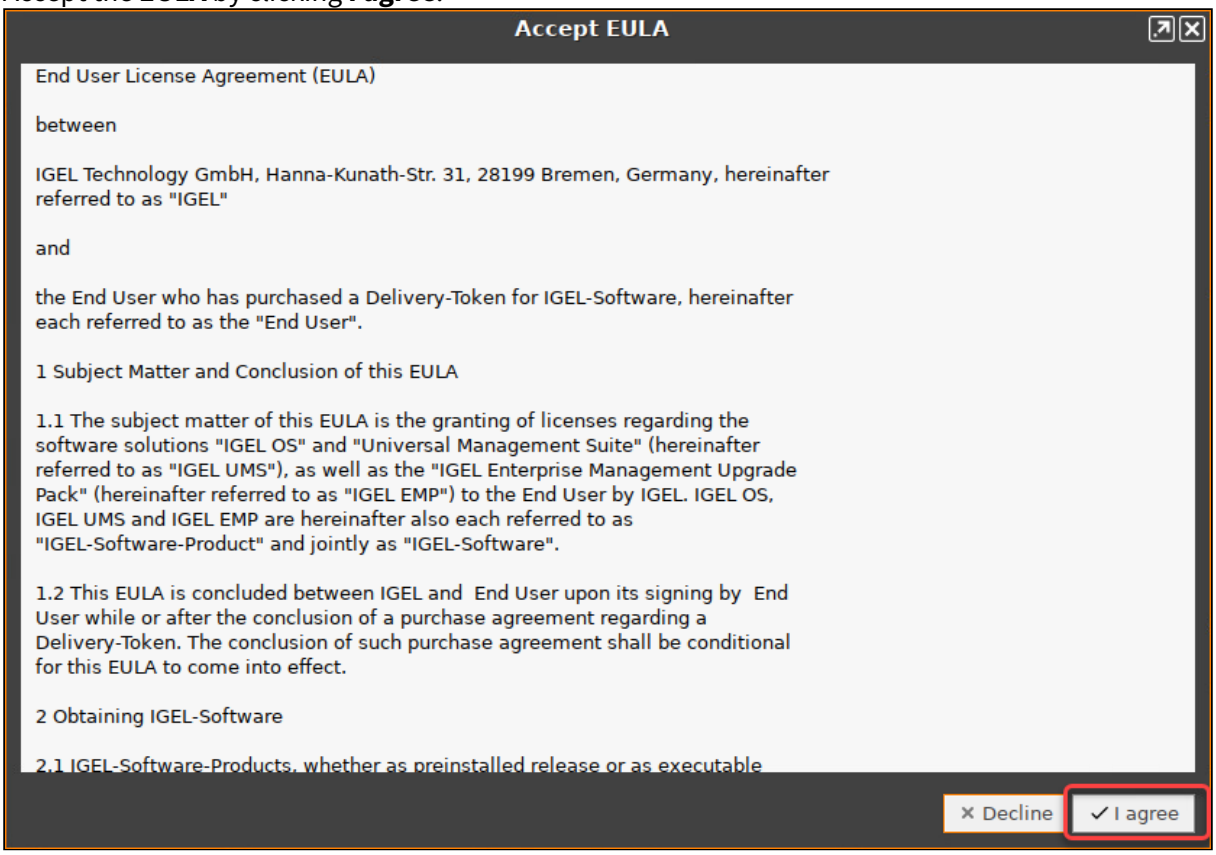
9. If you want to undo your changes and restore the original settings, click **Reset**.



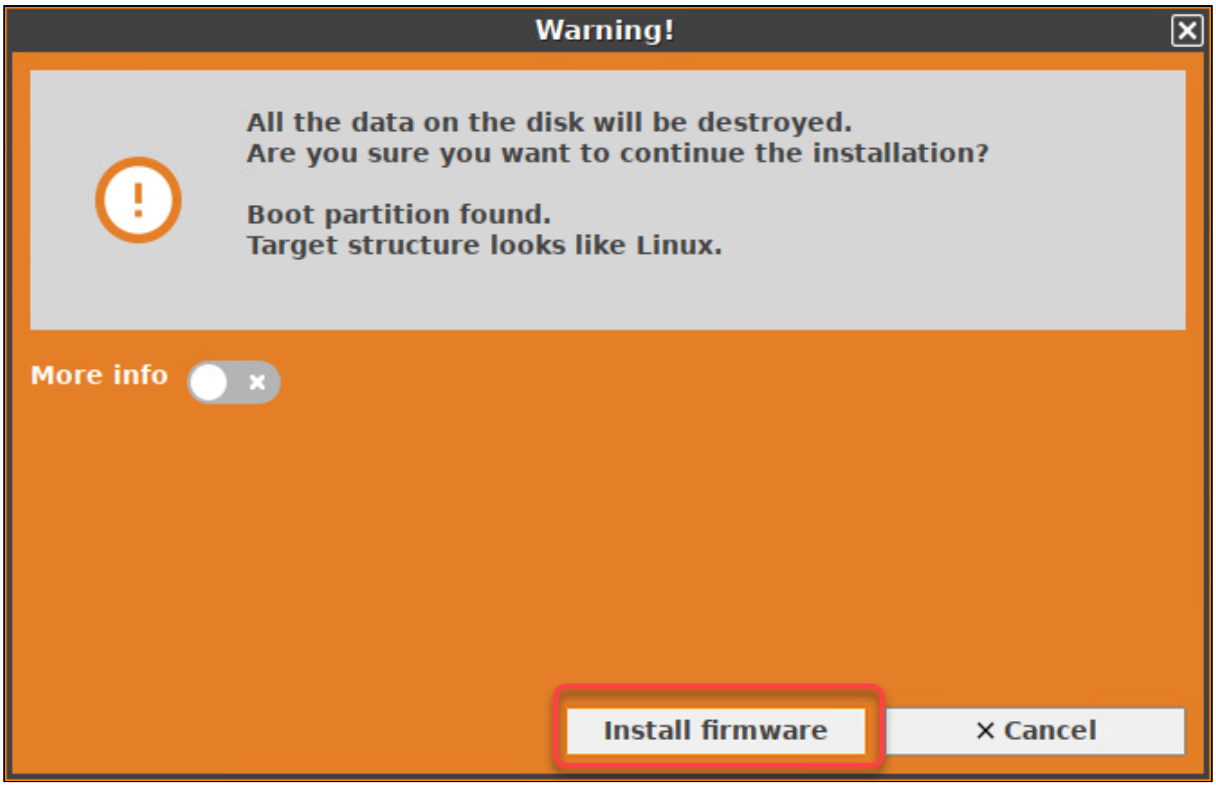
10. Click on **Install firmware**.



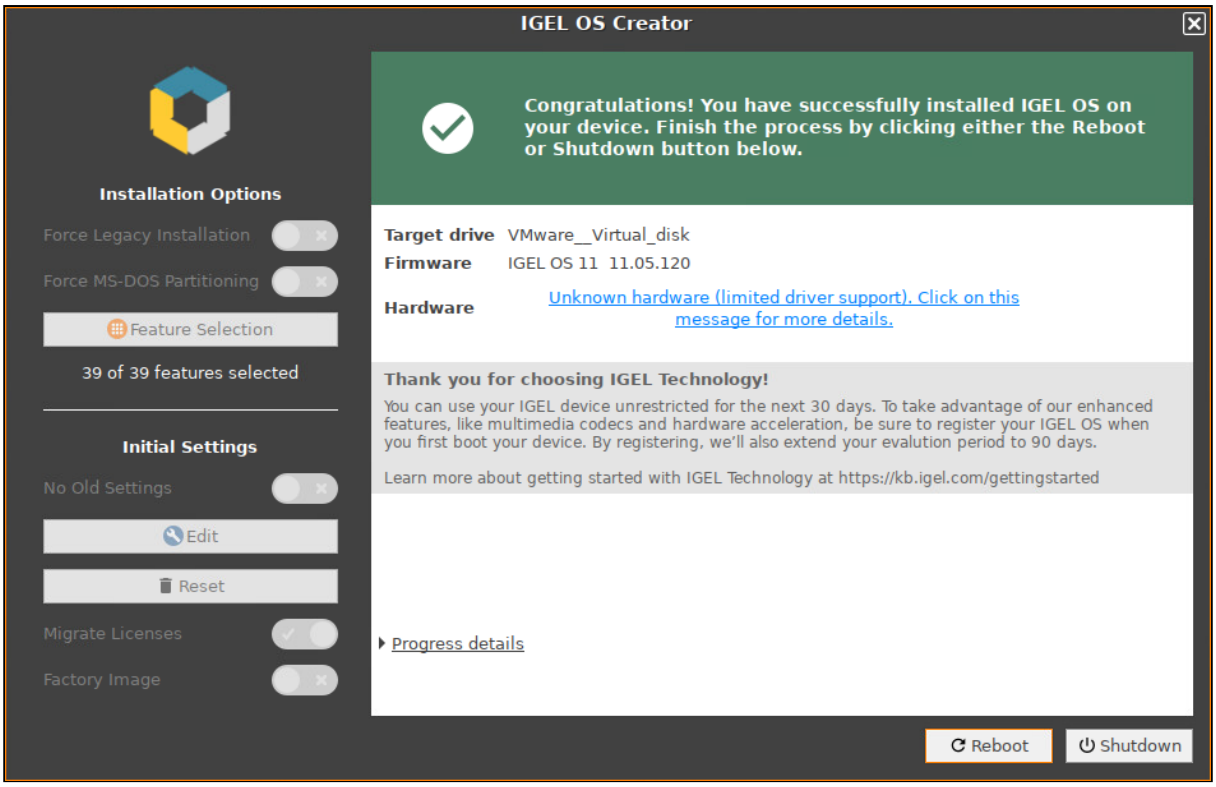
11. Accept the **EULA** by clicking **I agree**.



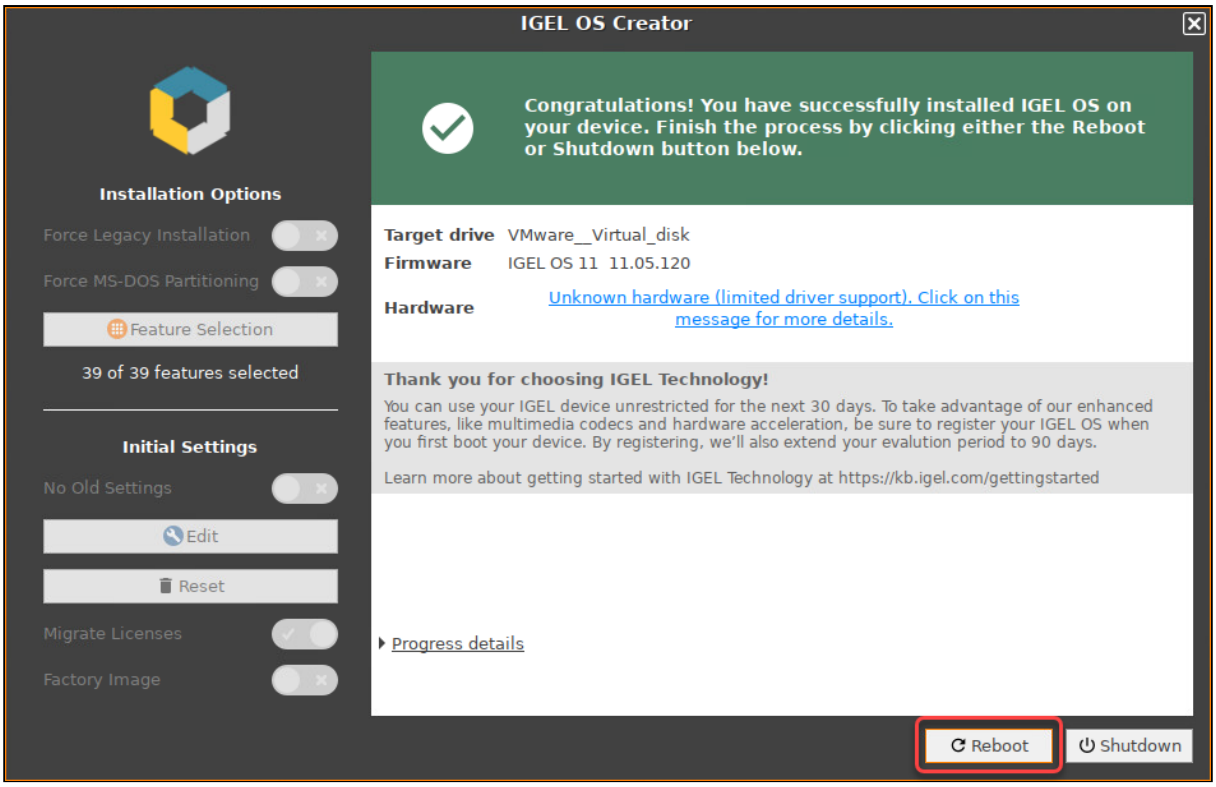
12. Confirm the warning dialog.



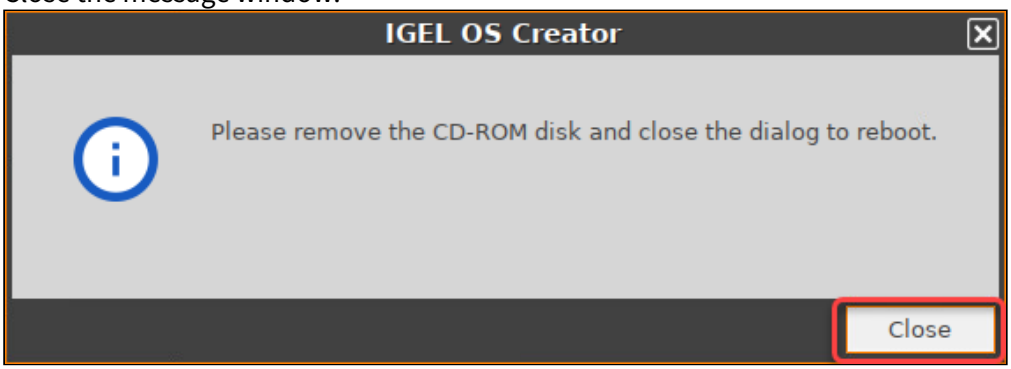
The installation program will install IGEL OS 11 on the target drive. If you see the success message, the installation is complete.



13. Detach any external network adapters from the device.
    In this way, you ensure that the unit ID for the device is derived from the built-in network adapter. The unit ID will be saved on the device persistently, regardless of any external network adapter that may be used in the future. This is important for licensing.
14. Click on **Reboot**.



15. Remove the USB memory stick.
16. Close the message window.



The system will shut down and then boot IGEL OS 11.

Installation Procedure for Factory Images

The installation will overwrite all existing data on the target drive.

Preparing the Image

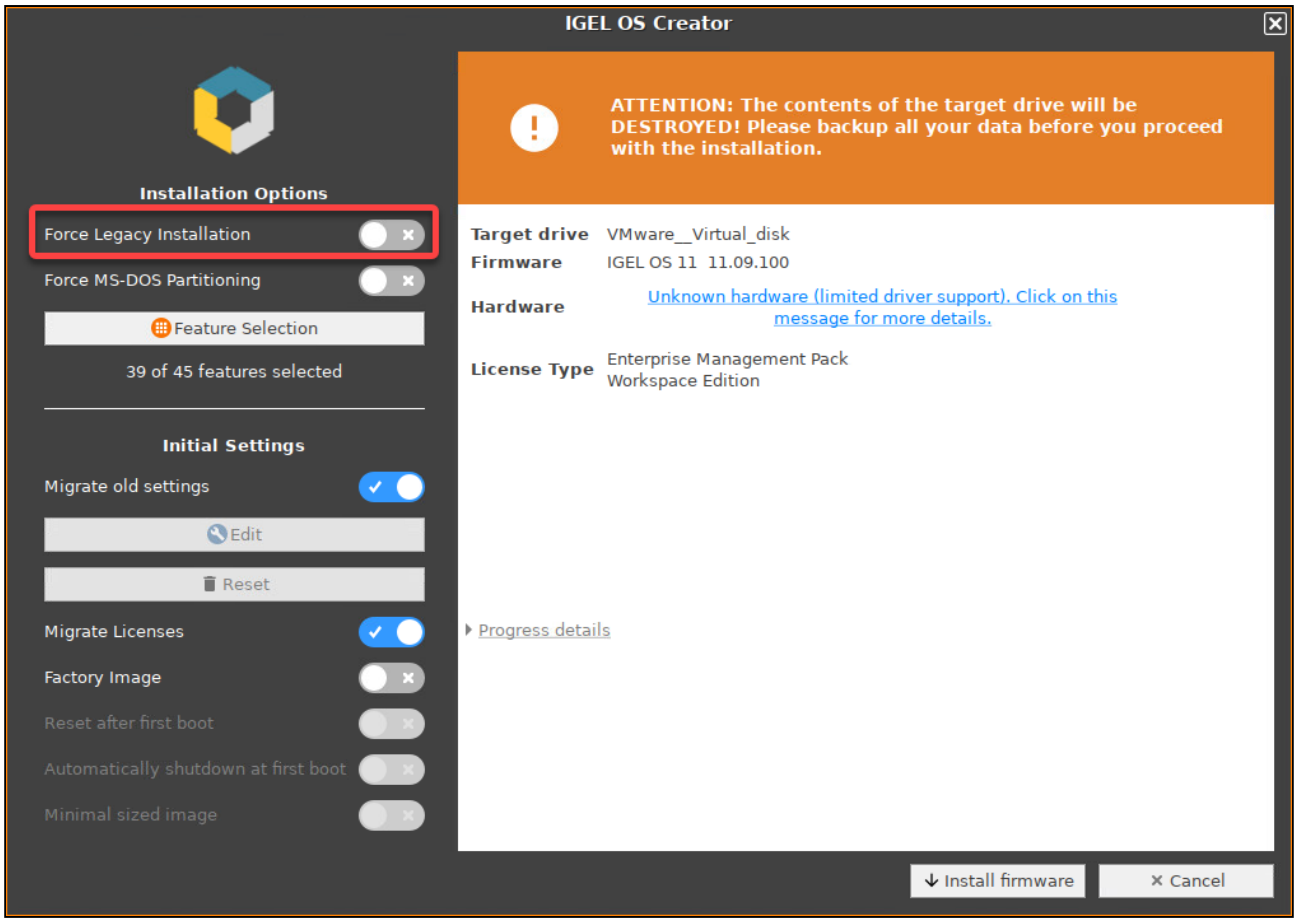
1. Connect the prepared USB memory stick to the target device and switch on the target device.
2. Select **Standard Installation + Recovery** or **Verbose Installation + Recovery**.

3. Select the language for the installation process.

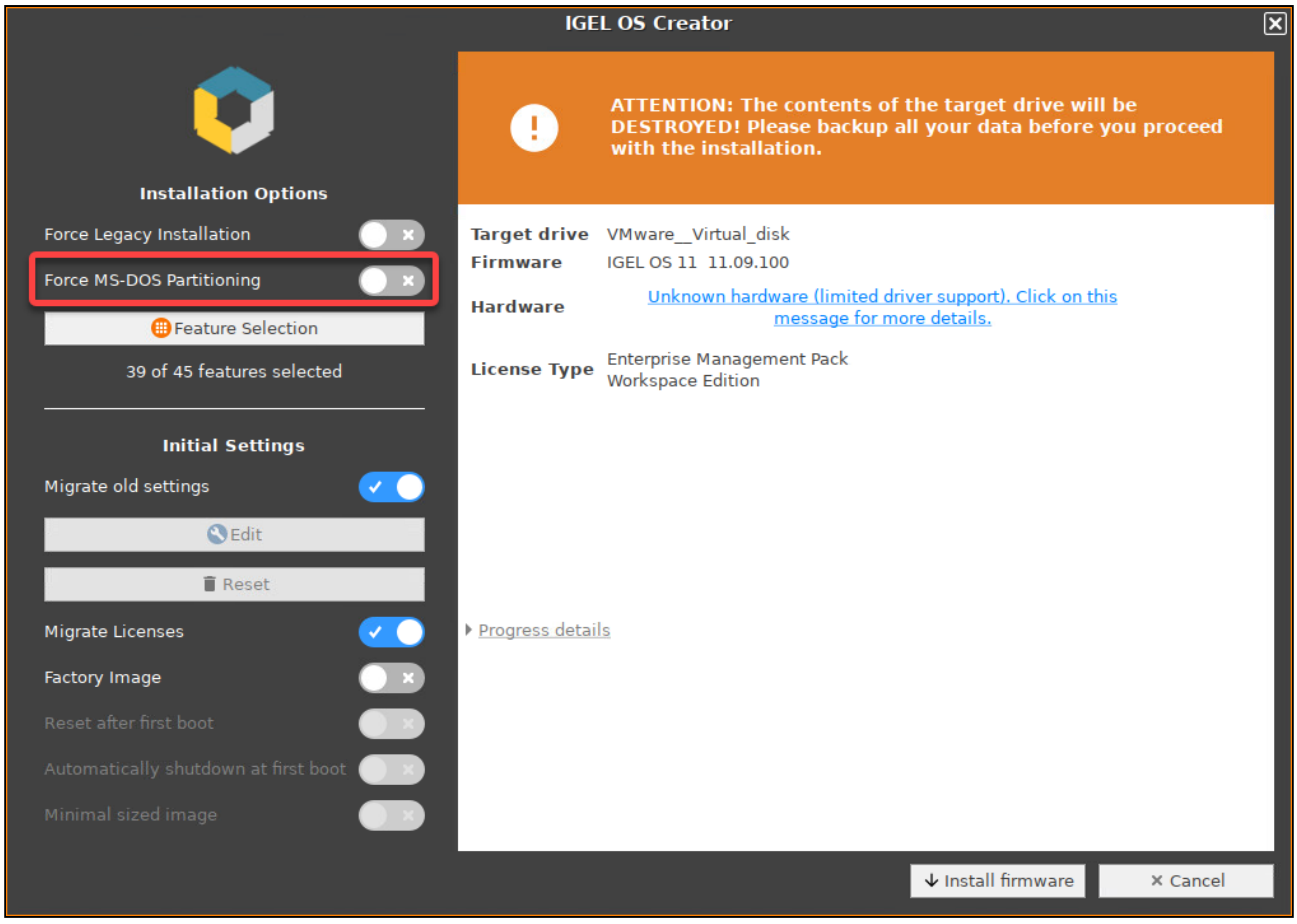
The installation program **IGEL OS Creator** opens. Here, you can configure settings for the installation process and start it.

4. Optional; only available if your device has booted in UEFI mode: If you want to install the legacy/BIOS version of IGEL OS 11, activate **Force Legacy Installation**.

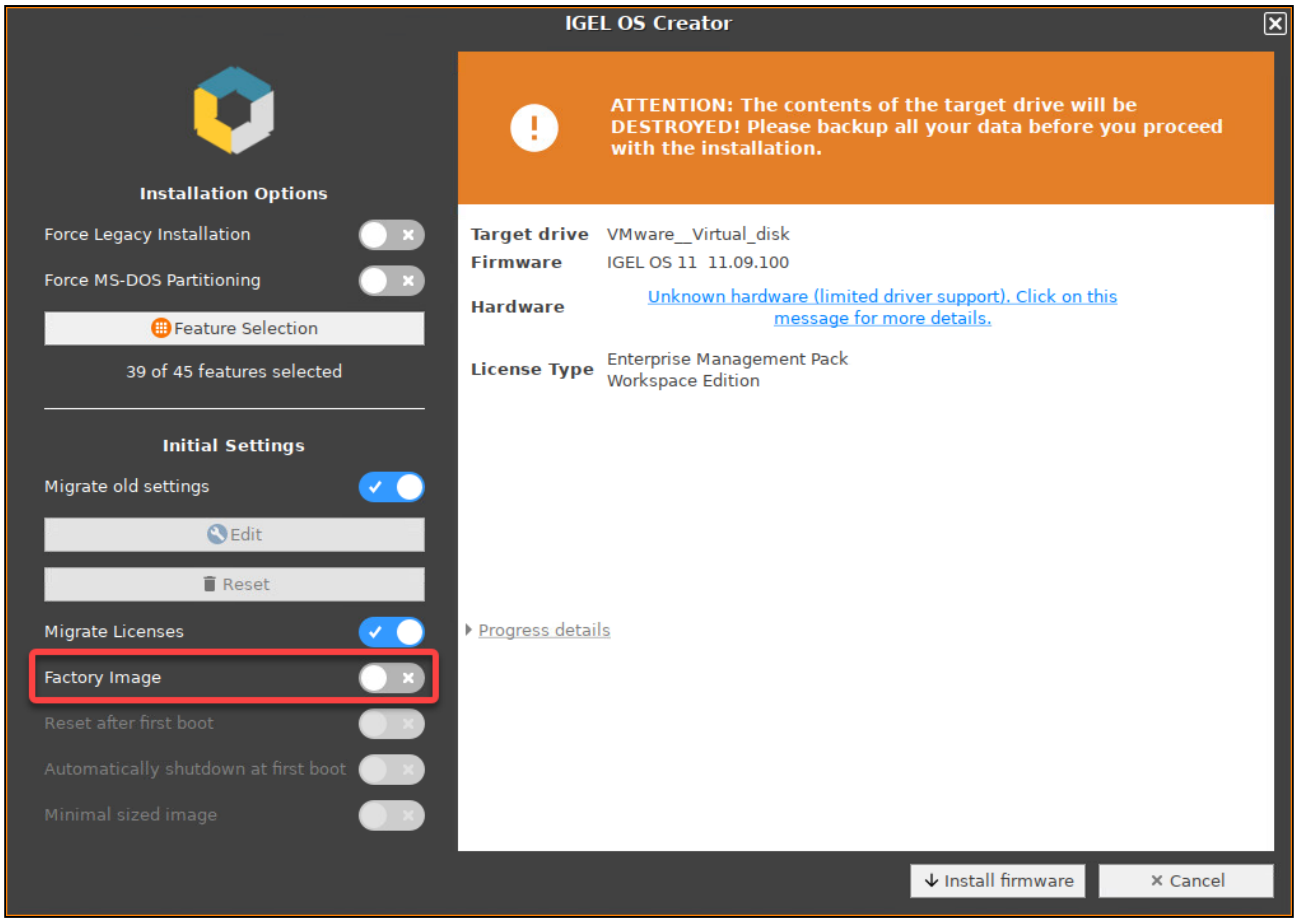
If you have activated **Force Legacy Installation**, remember to set the system to legacy/BIOS mode after installation.

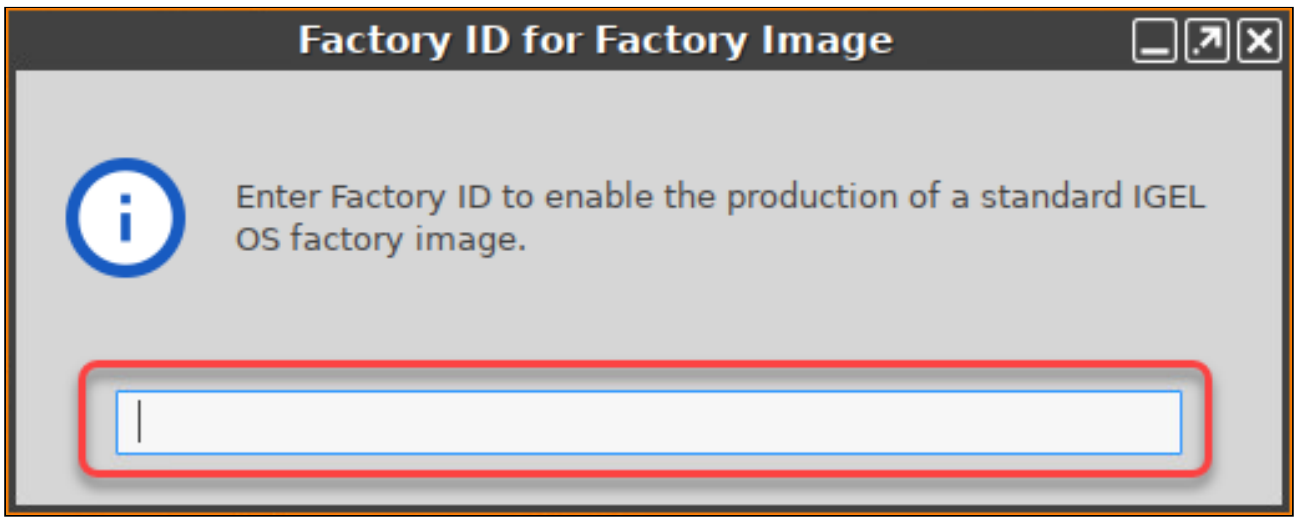


5. Optional; only available if your device has booted in UEFI mode: If you want to use an MS-DOS partition table instead of a GPT partition table, activate **Force MS-DOS Partitioning**.

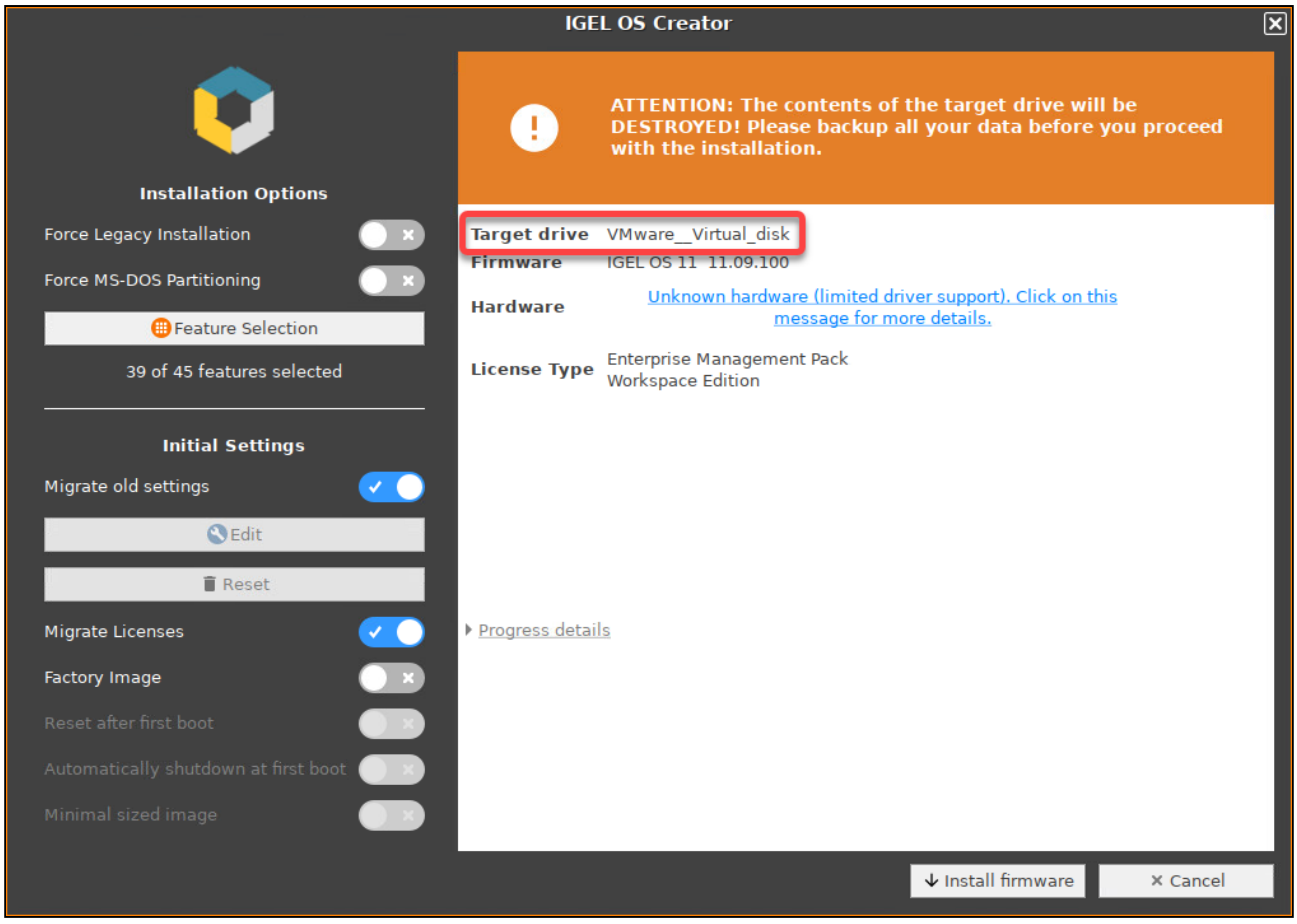


6. Activate **Factory Image** and enter your factory ID.

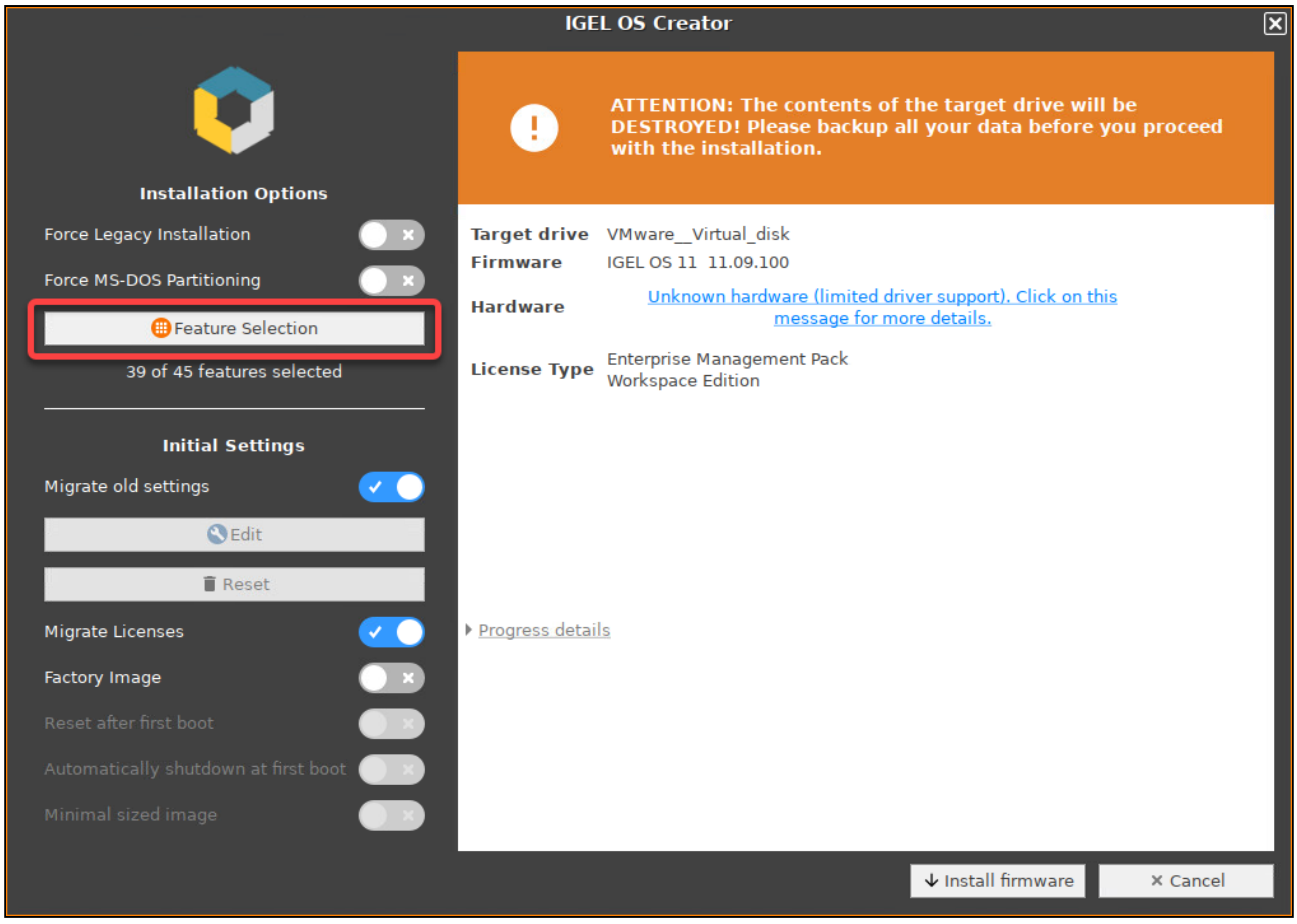


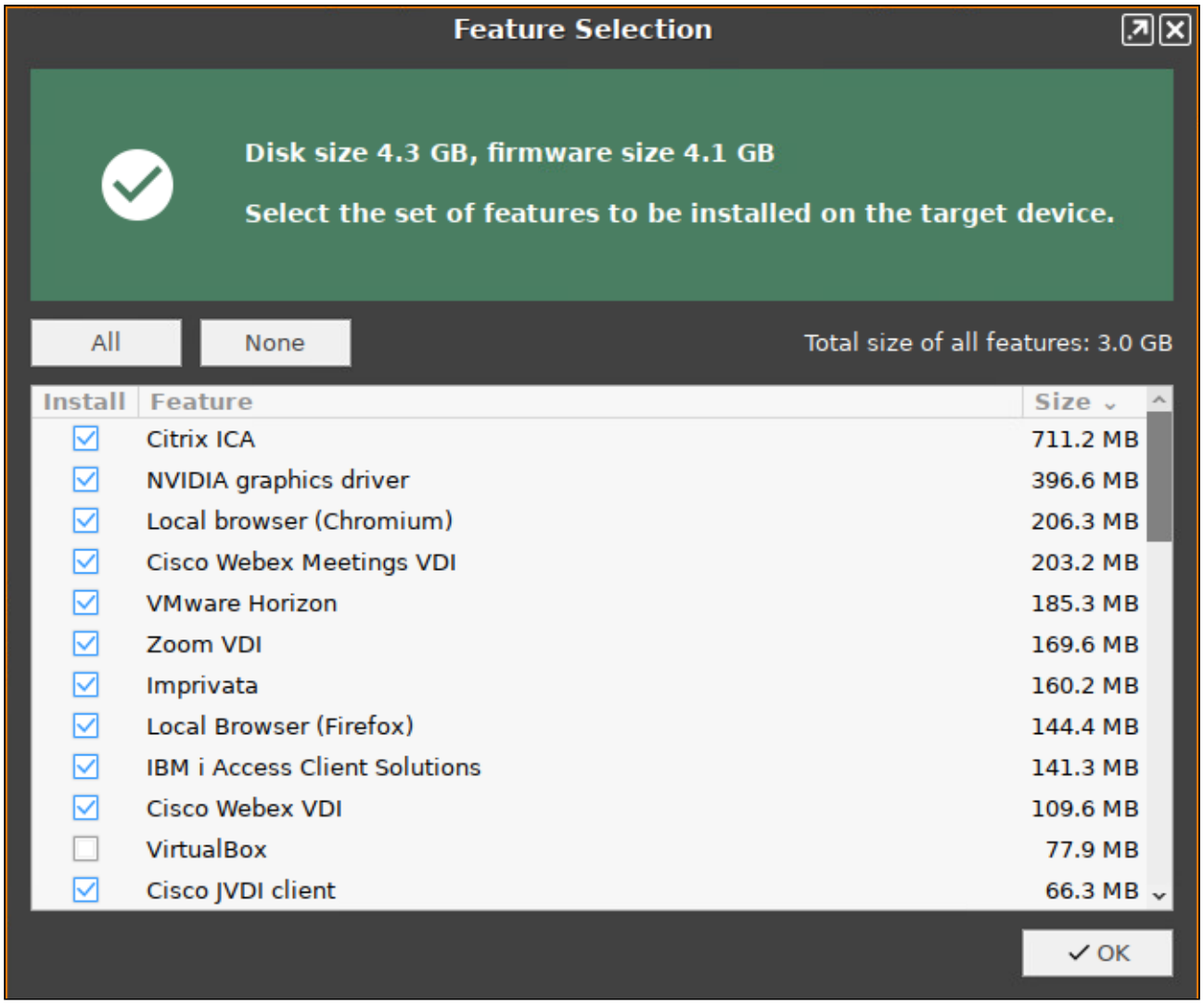


7. Check the **Target drive** to ensure that the system is installed on the desired drive.



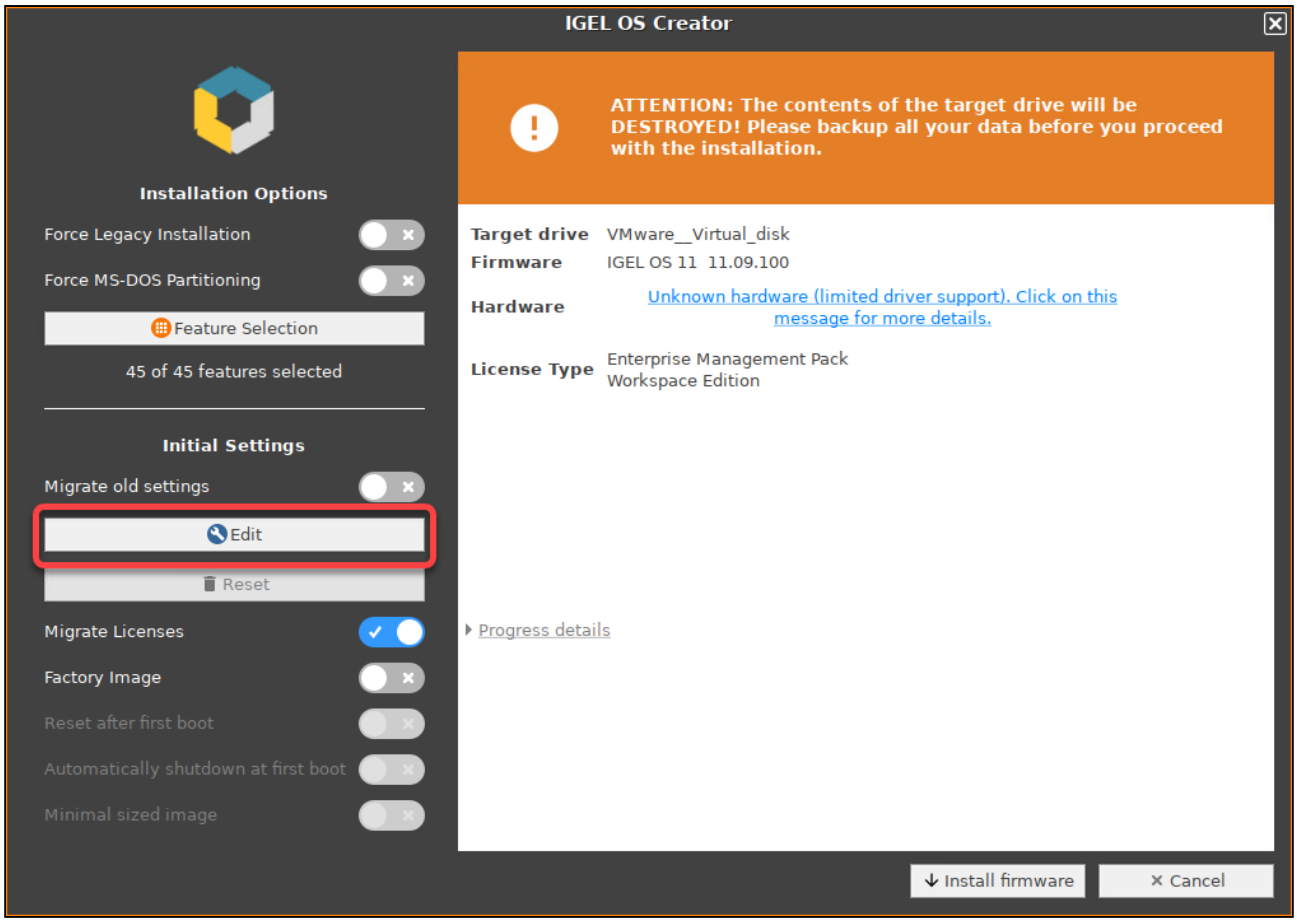
8. If you want to exclude features of IGEL OS, e.g. to save storage space, click **Feature Selection** and edit the settings as required.


IGEL OS Creator
Installation Options
Force Legacy Installation
Force MS-DOS Partitioning
Feature Selection
39 of 45 features selected
Initial Settings
Migrate old settings
Edit
Reset
Migrate Licenses
Factory Image
Reset after first boot
Automatically shutdown at first boot
Minimal sized image
ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.
Target drive VMware__Virtual_disk
Firmware IGEL OS 11 11.09.100
Hardware Unknown hardware (limited driver support). Click on this message for more details.
License Type Enterprise Management Pack Workspace Edition
Progress details
Install firmware
Cancel

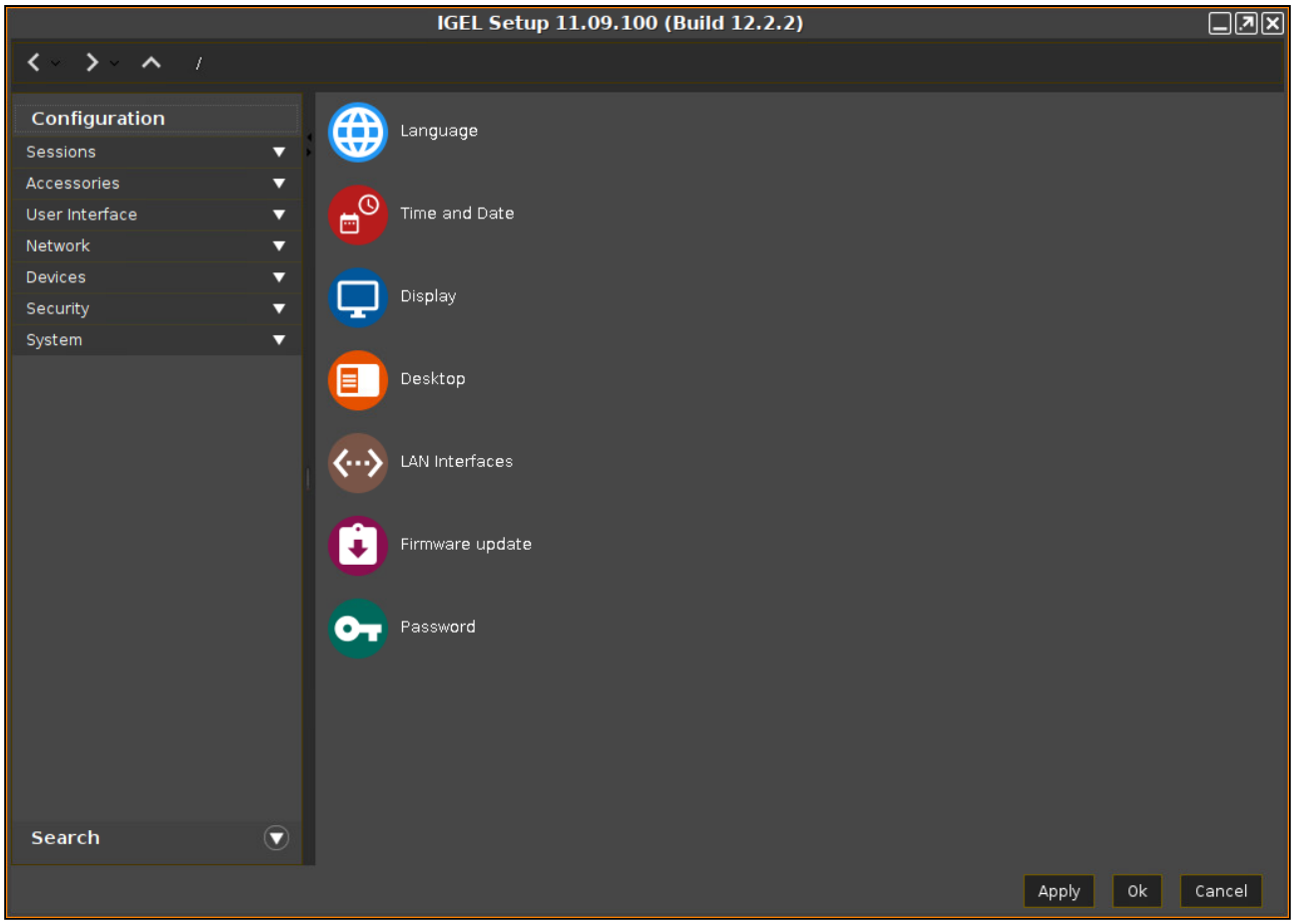


- **All**: Select all features
- **None**: Select no feature
- **Feature**: Sort the list alphabetically
- **Size**: Sort the list by the memory requirements of the features

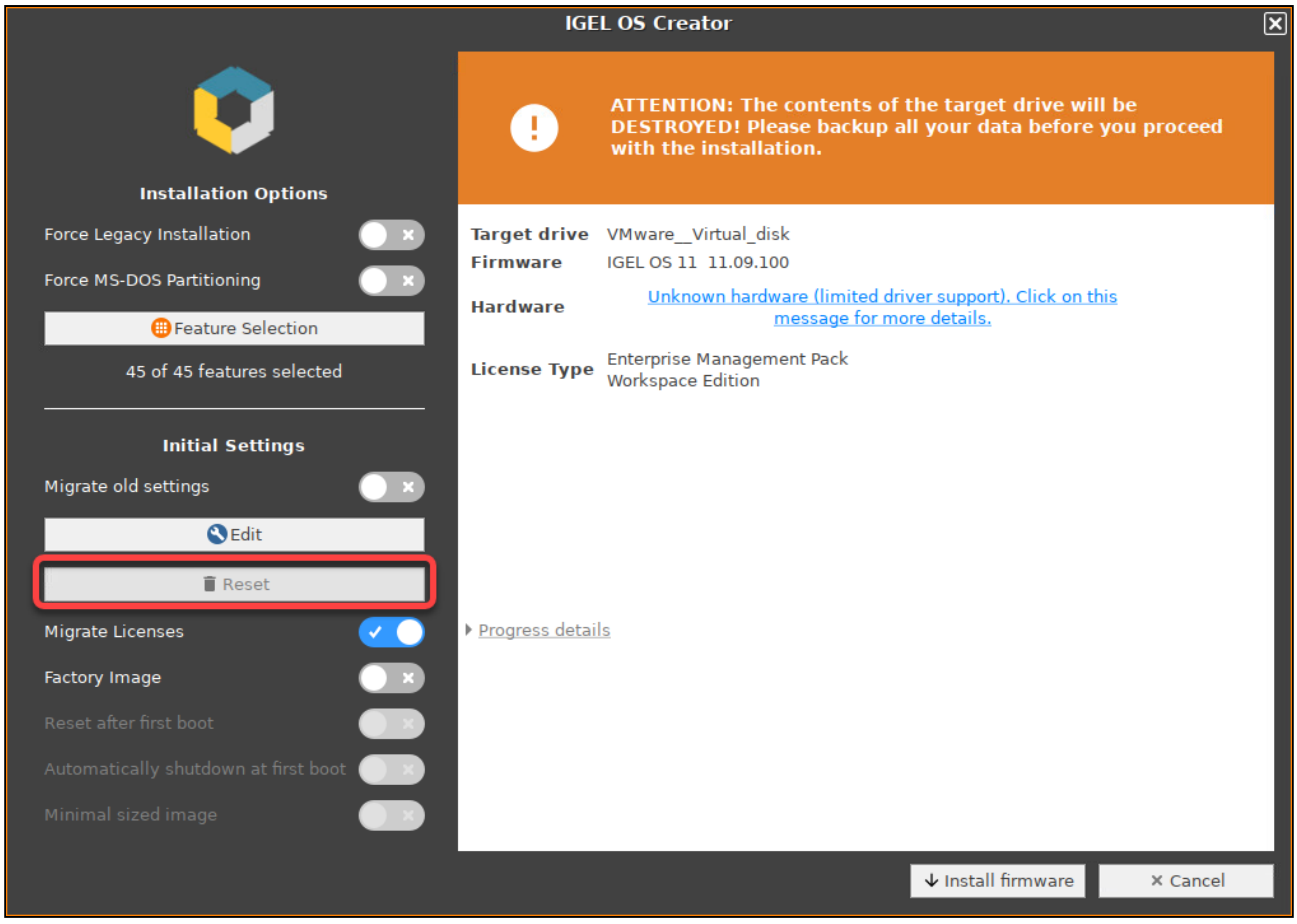
9. If you want to change the initial settings for the devices you are about to deploy, click **Edit**.



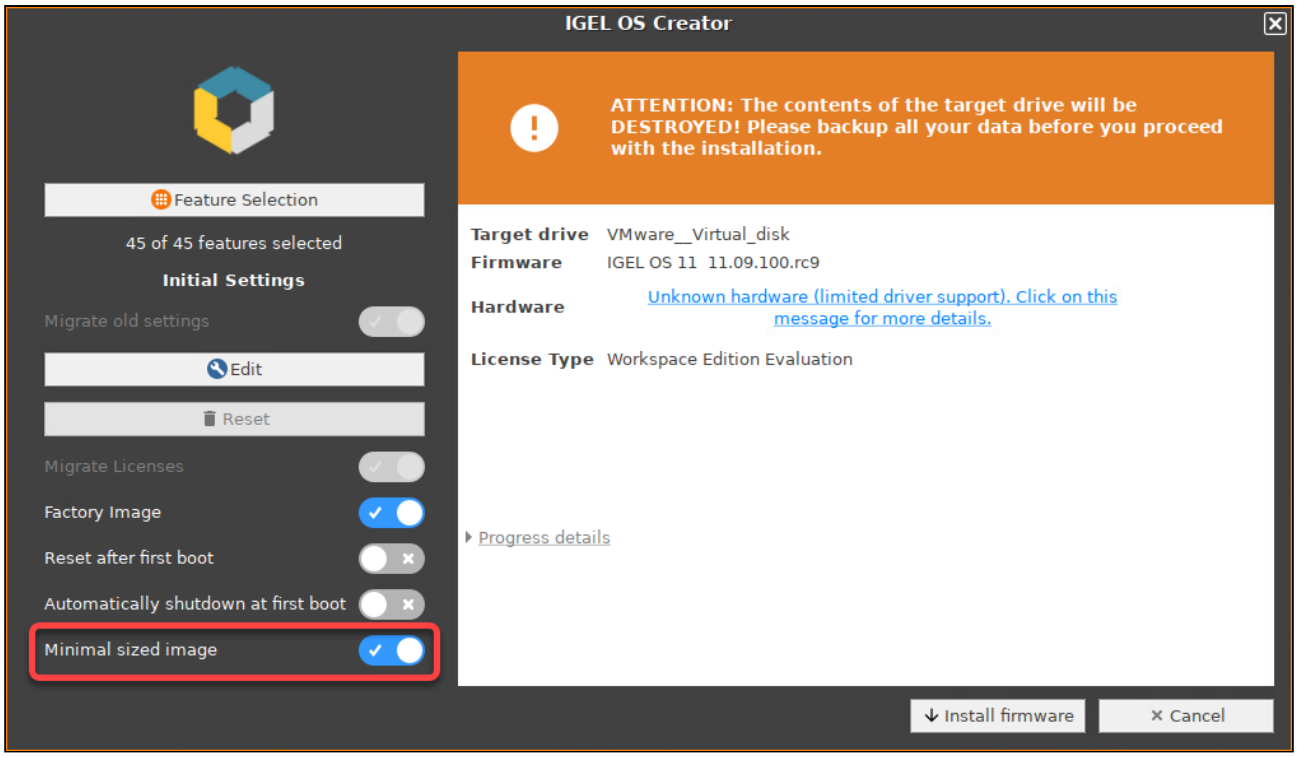
The IGEL Setup opens, enabling you to change the settings in the same way as with a regular IGEL OS installation. The changes are stored on the USB memory stick from which the IGEL OS Creator (OSC) is executed. For details about the settings, see the chapters Setup (see page 1237) and the subsequent chapters in the IGEL OS Reference Manual (see page 1211).



10. If you want to undo your changes and restore the original settings, click **Reset**.



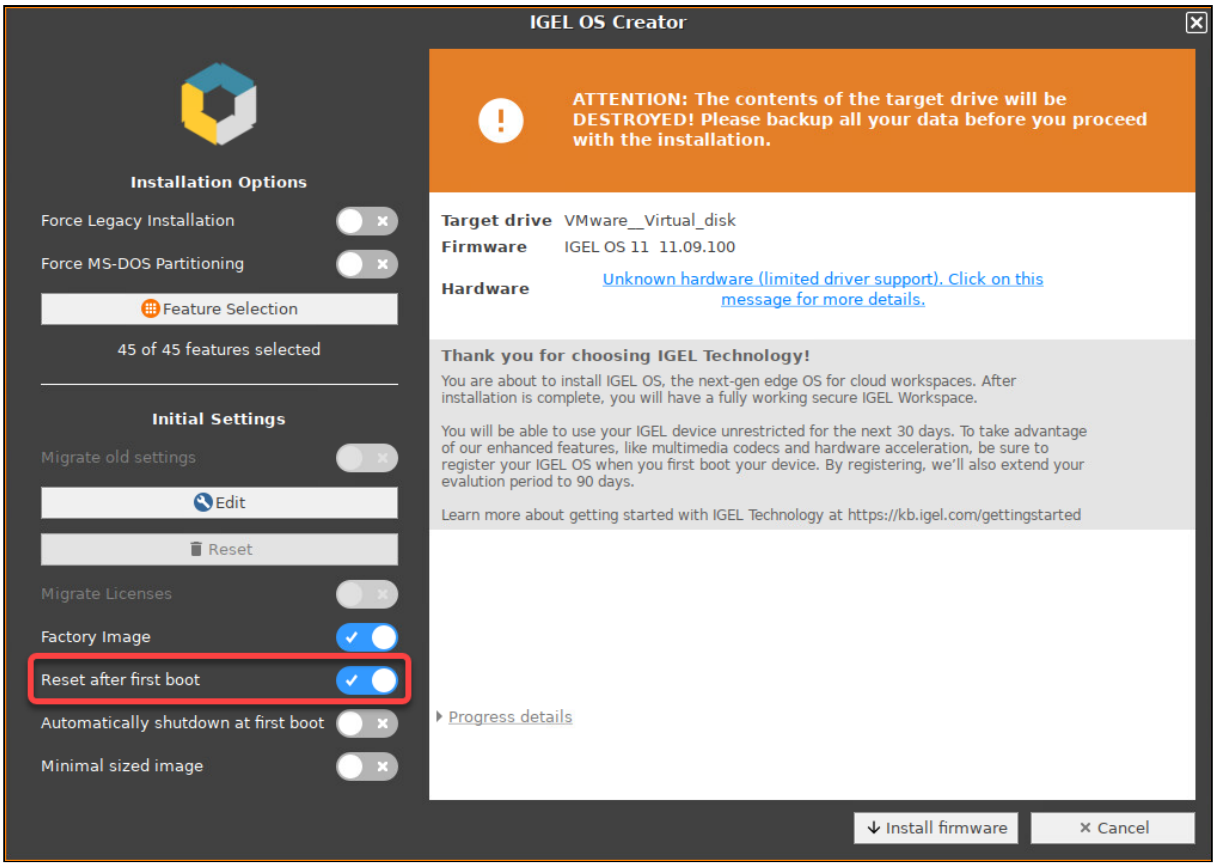
11. If you want to create an image that will resize itself on the first boot, following the device's storage size, enable **Minimal sized image**.



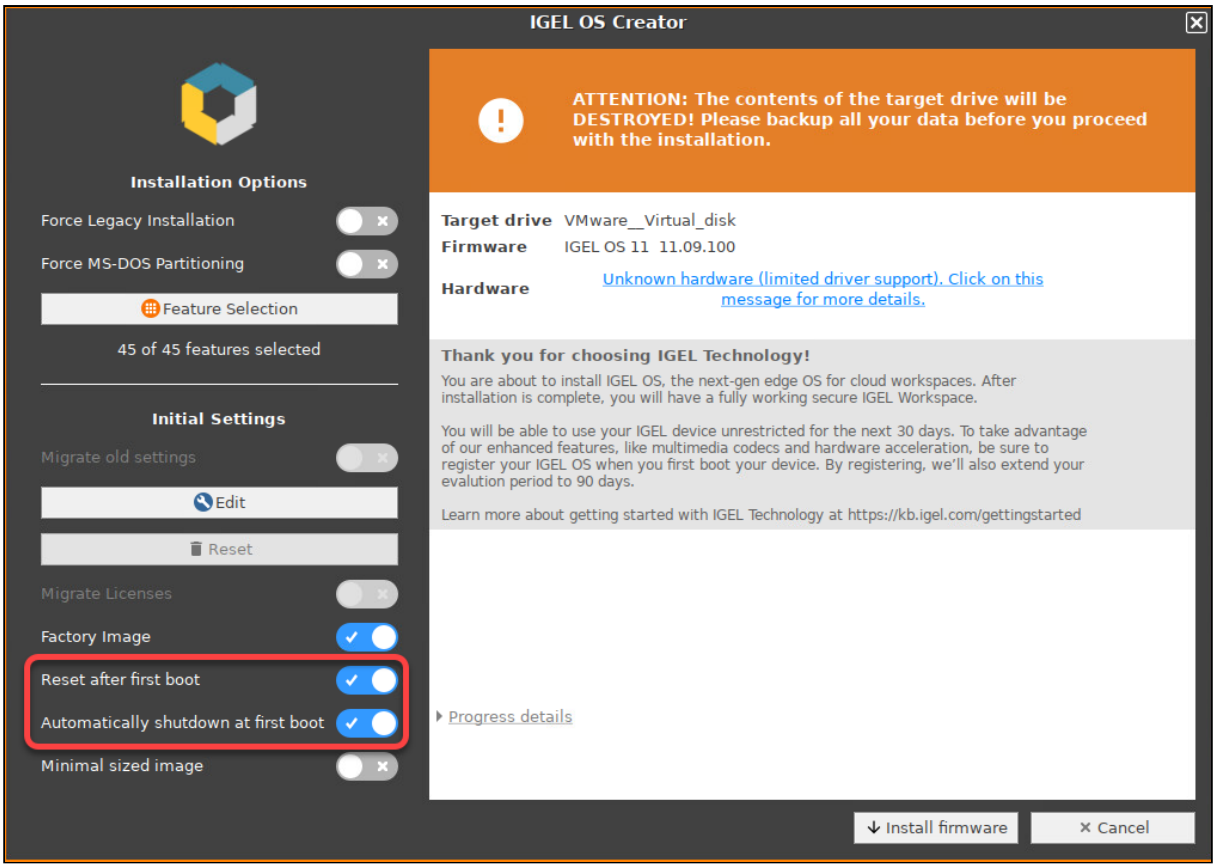
12. If you want to perform a functional test on each device, you have two possibilities:

> **Important Note**
>
> If **Reset after first boot** or **Automatically shutdown at first boot** is activated on your factory preload image, the first boot of your devices MUST take place BEFORE shipment to end customers!

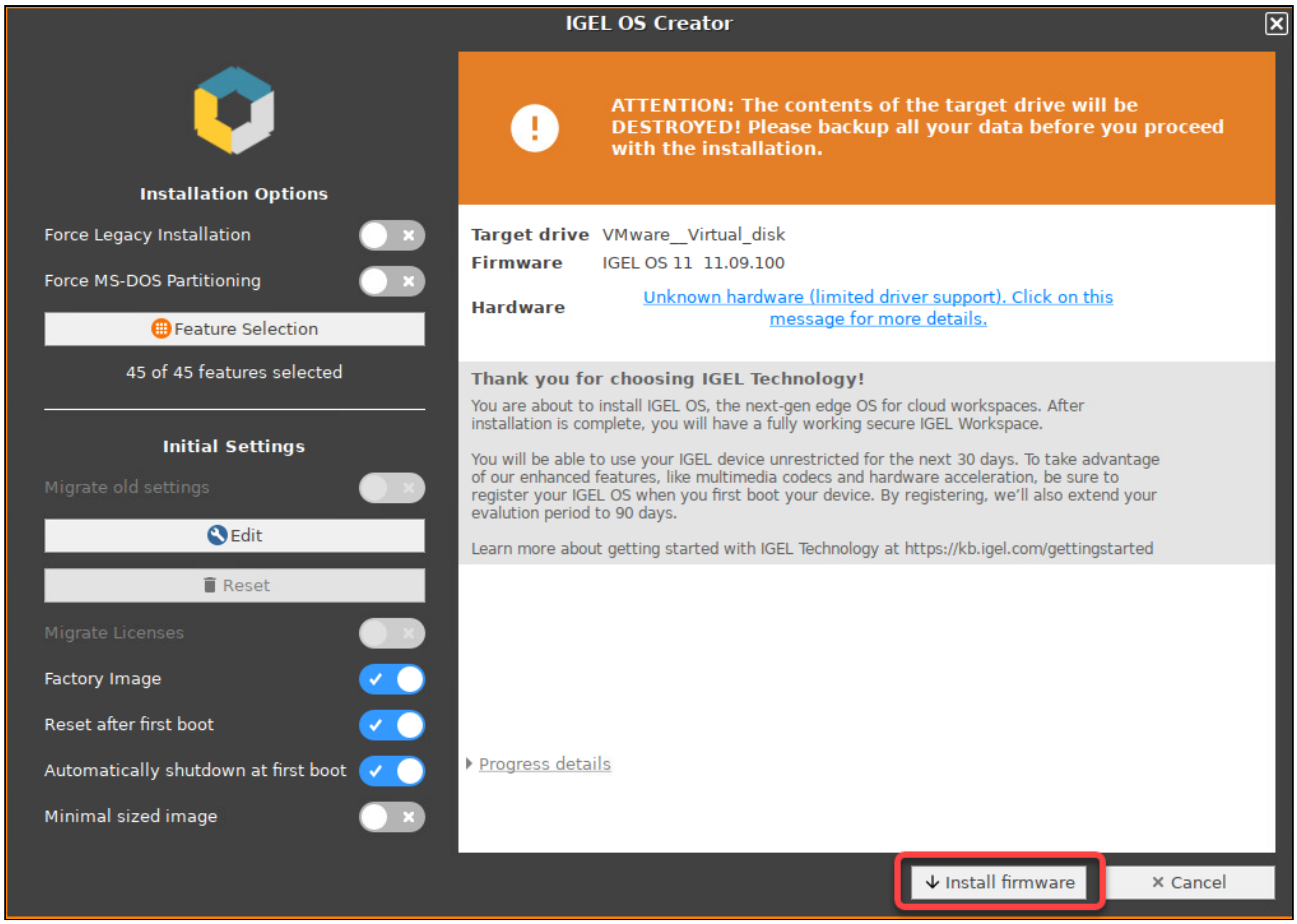
- Manual tests with visual feedback on each device: Enable **Reset after first boot**. The test procedure is described under Unit Testing.



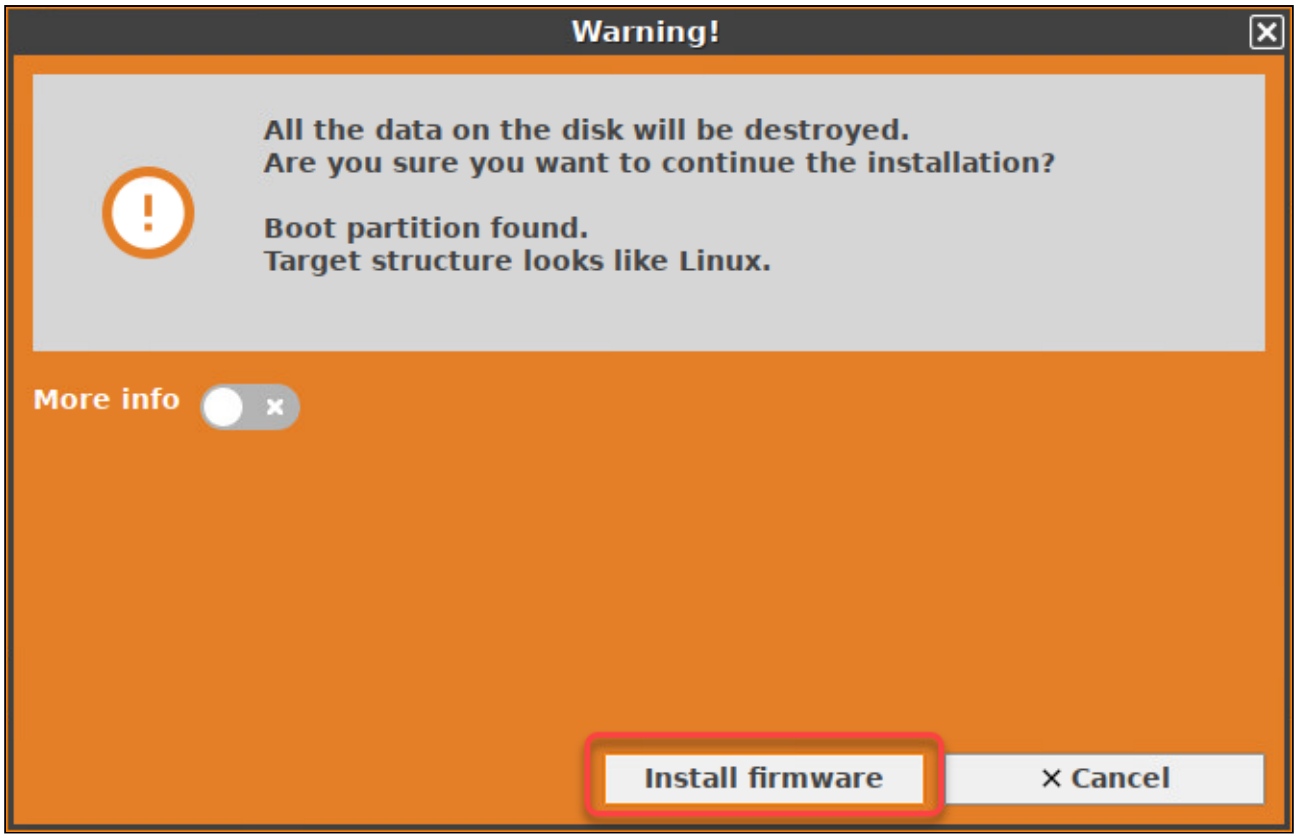
- Automatic tests (unattended): Enable both **Reset after first boot** and **Automatically shutdown at first boot**. The test procedure is described under Automatic Unit Testing.

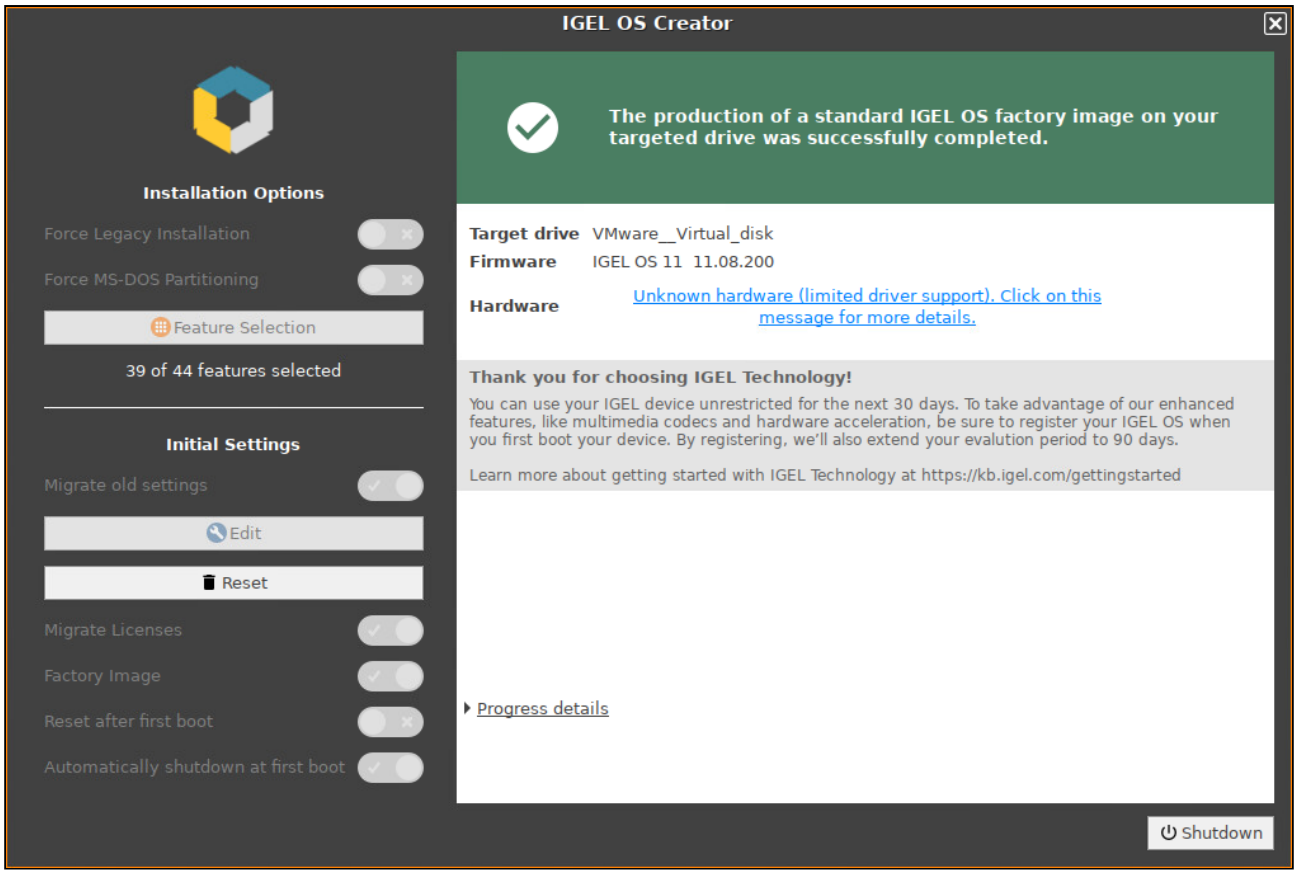


13. To start the installation, click **Install firmware**.



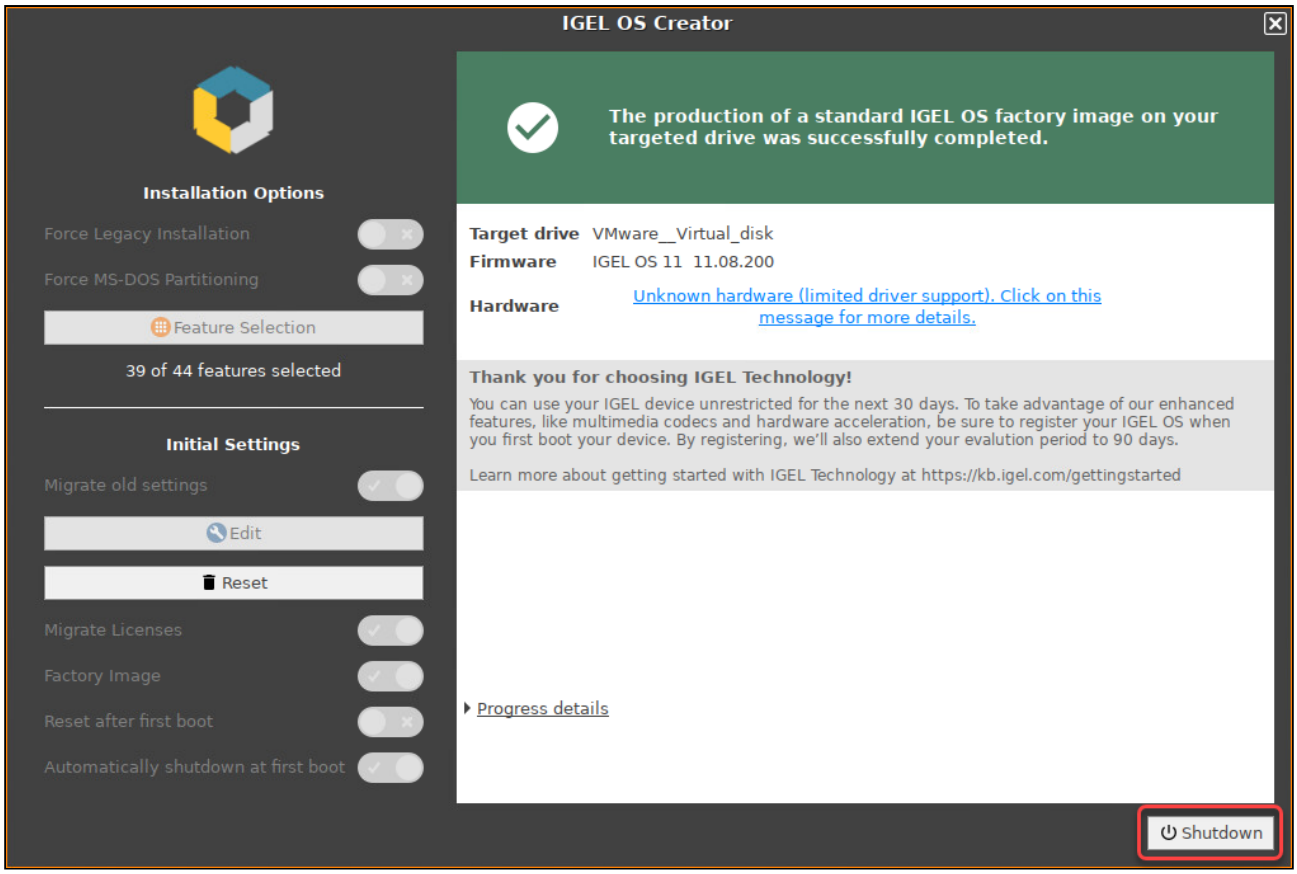
14. Confirm the warning dialog.


Warning!
All the data on the disk will be destroyed.
Are you sure you want to continue the installation?
Boot partition found.
Target structure looks like Linux.
More info
Install firmware
Cancel



The installation program will set up IGEL OS 11 on the target drive. If you see the success message, the installation is complete.

15. Click on **Shutdown**.



16. Read out the image from your device to deploy it on the units.

DO NOT BOOT THE EXACT FACTORY IMAGE THAT IS INTENDED FOR DEPLOYMENT ON YOUR DEVICES! ALL DEVICES TO WHICH THIS IMAGE HAS BEEN DEPLOYED WOULD SHARE ONE AND THE SAME UNIT ID. AS A RESULT, YOUR DEVICES WOULD BE PRACTICALLY UNUSABLE.
If you want to test the factory image before its deployment, transfer it to your target medium first and then boot the image on the machine on which you created it, or any other test machine. The important thing is that the factory image that will be mass-deployed to your units has not been booted before.

16 GiB Maximum Image Size

The maximum size of the image that is created by the IGEL OS Creator (OSC) is 16 GiB. Therefore, only the first 16 GiB of your storage medium is needed. If your devices have larger storage, this will allow for faster deployment.

17. To ensure the integrity of the image, you should create checksums of the original image and of the images that are deployed, and then compare them. For details, see IGEL Endpoint Partners: Ensuring Image Integrity with a Checksum (see page 1195).

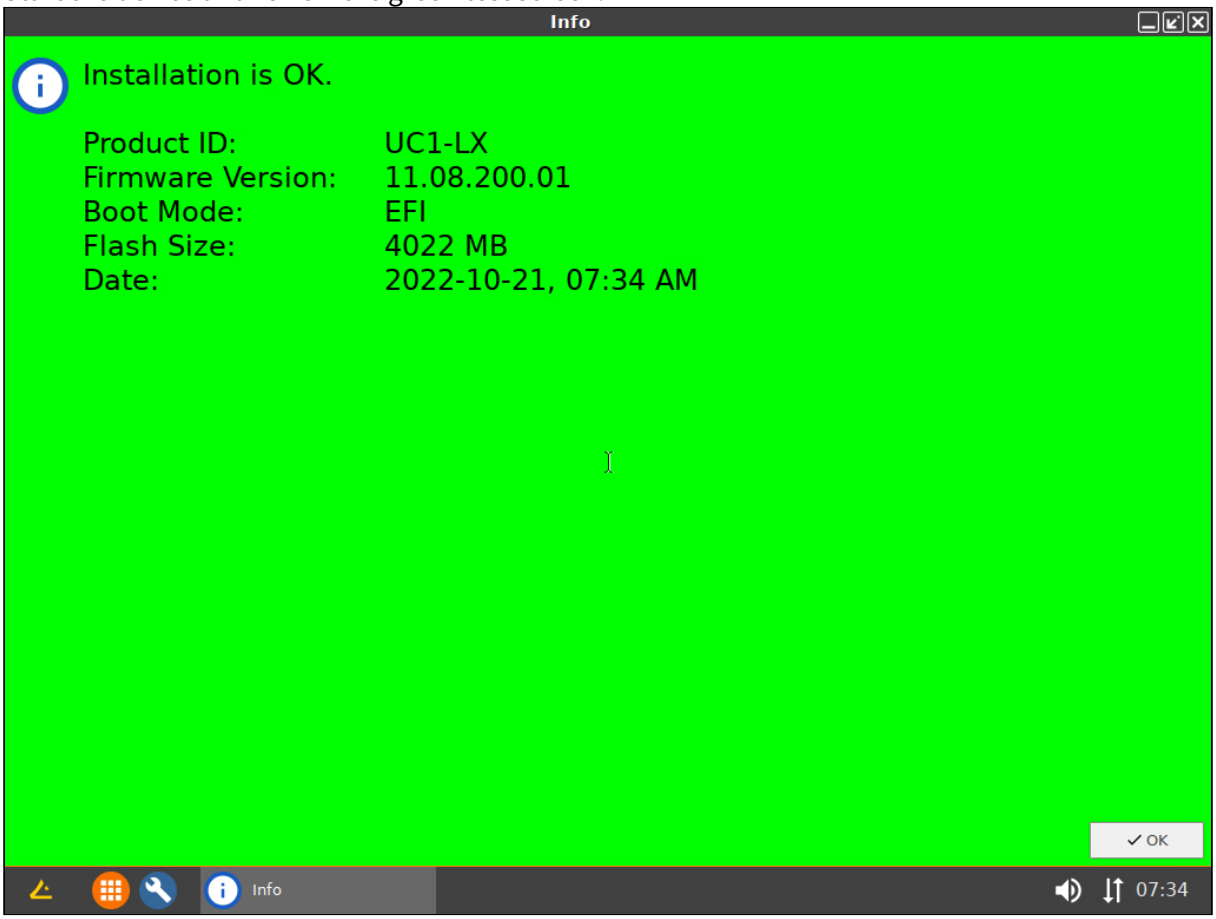
18. Proceed as appropriate:
    - If **Reset after first boot** is inactive, you can deploy the images on the units and roll them out straight away. The deployment should include a comparison of the checksums.
    - If **Reset after first boot** has been activated, deploy the images on the units and continue with Unit Testing.
    - If **Automatically shutdown at first boot** has been activated, deploy the images on the units and continue with Automatic Unit Testing.

Visual Unit Testing

Perform the following procedure on the original device and on every unit on which the image has been deployed.

> **Important Note**
>
> The first boot test MUST take place with each unit BEFORE it is rolled out. (Otherwise, the device would present the green test screen instead of the IGEL Setup Assistant.)

1. Start the device and review the green test screen.



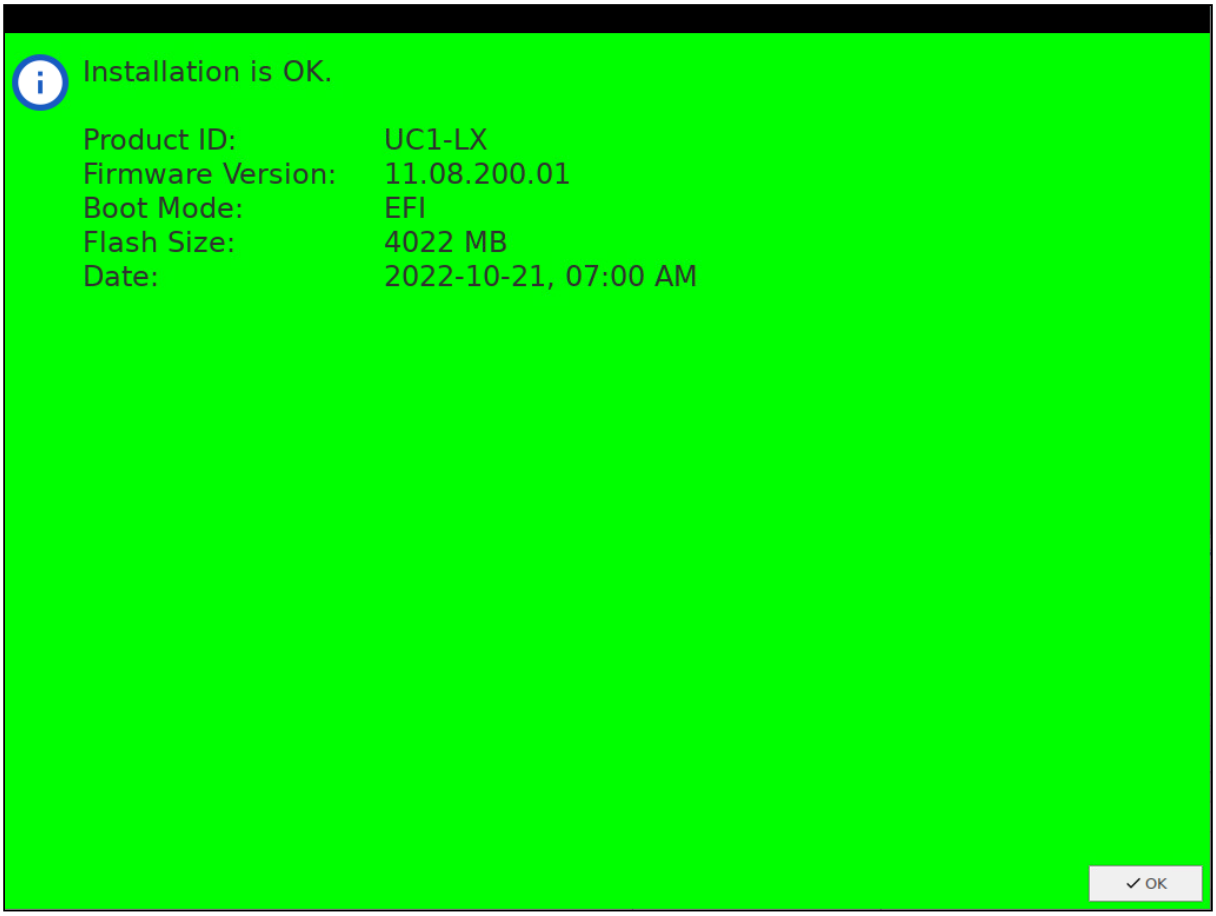
2. Click **OK**.
   You can regularly access IGEL OS and perform your tests.
3. Shut the device down.
   The device is ready for roll-out.

Automatic Unit Testing

When **Reset after first boot** and **Automatically shutdown at first boot** has been enabled, the device writes a log file on its first boot and then shuts down automatically.

Your test routine must perform the following procedure:

1. Start the device.
   The device will perform a check and write the results to a file on the first VFAT partition of the device's storage medium. The file format is JSON, and the file name is `check.log`. After a few seconds, the machine shuts down automatically. During the uptime, the green test screen is shown.



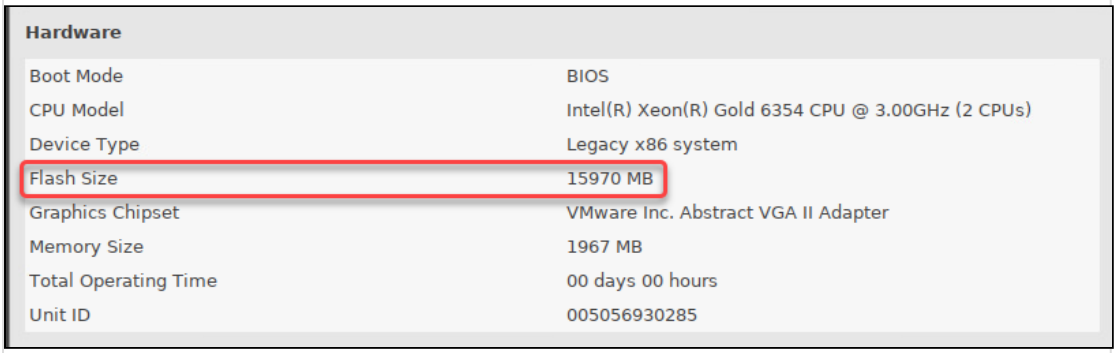
2. Get the file `check.log` from the first VFAT partition of the storage medium and analyze it. The contents of the file are described below.

Example Content of check.log


```
{
  "product": "34CN65",
  "serial": "601NTXXD009",
  "product_id": "UC3-LX No valid license",
  "version": "11.08.200.01",
  "bootmode": "UEFI Secure Boot",
  "flashsize": "14496 MB",
  "date": "2022-10-19, 07:29 AM",
  "status": "SUCCESS",
  "log": ""
}
```


Explanation of the JSON Fields

Field	Explanation
`product`	Product id from DMI
`serial`	Serial number from DMI
`product_id`	The IGEL product ID which also shown in the **About** window:
`version`	The version of the IGEL firmware
`bootmode`	The boot mode: `Legacy`, `UEFI`, or `UEFI Secure Boot`

Field	Explanation
`flashsize`	The size of the IGEL partition (not the complete available disk space). This value is also shown in the **About** window: 
`date`	Time and date of the check
`status`	`SUCCESS` if the check was successful
`log`	Empty if no error has occurred; otherwise, an error description is provided

IGEL OS Creator Articles

- Café Wireless (Wi-Fi) (see page 2173)
- Reduce CPU Power Consumption (see page 2178)
- Installing UDC3 on Secunet SINA Workstation (see page 2179)
- Setting up IGEL OS on Mobile Devices (see page 2181)
- Rolling out Initial Settings with IGEL OSC (see page 2190)

Café Wireless (Wi-Fi)

When you use your mobile device frequently at different Wi-Fi hotspots, automatic Wi-Fi roaming may be useful. This is what IGEL Café Wireless does. The IGEL Café Wireless feature can be used, for instance, with IGEL UDC3. After you have configured your wireless networks, your mobile device is ready to roam.

For optimizing the network switchover, please see How to Configure Wi-Fi Network Roaming (see page 608).

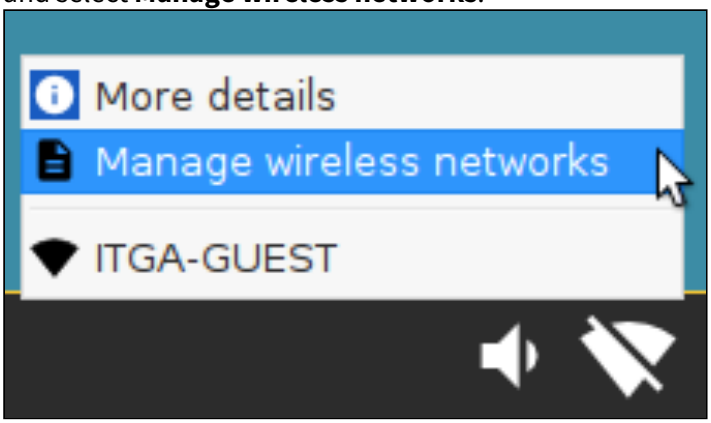
If the network's SSID is hidden, see How to Connect to a Wi-Fi Network with Hidden SSID (see page 653).

See also the manual chapter "Wireless (see page 1907)".

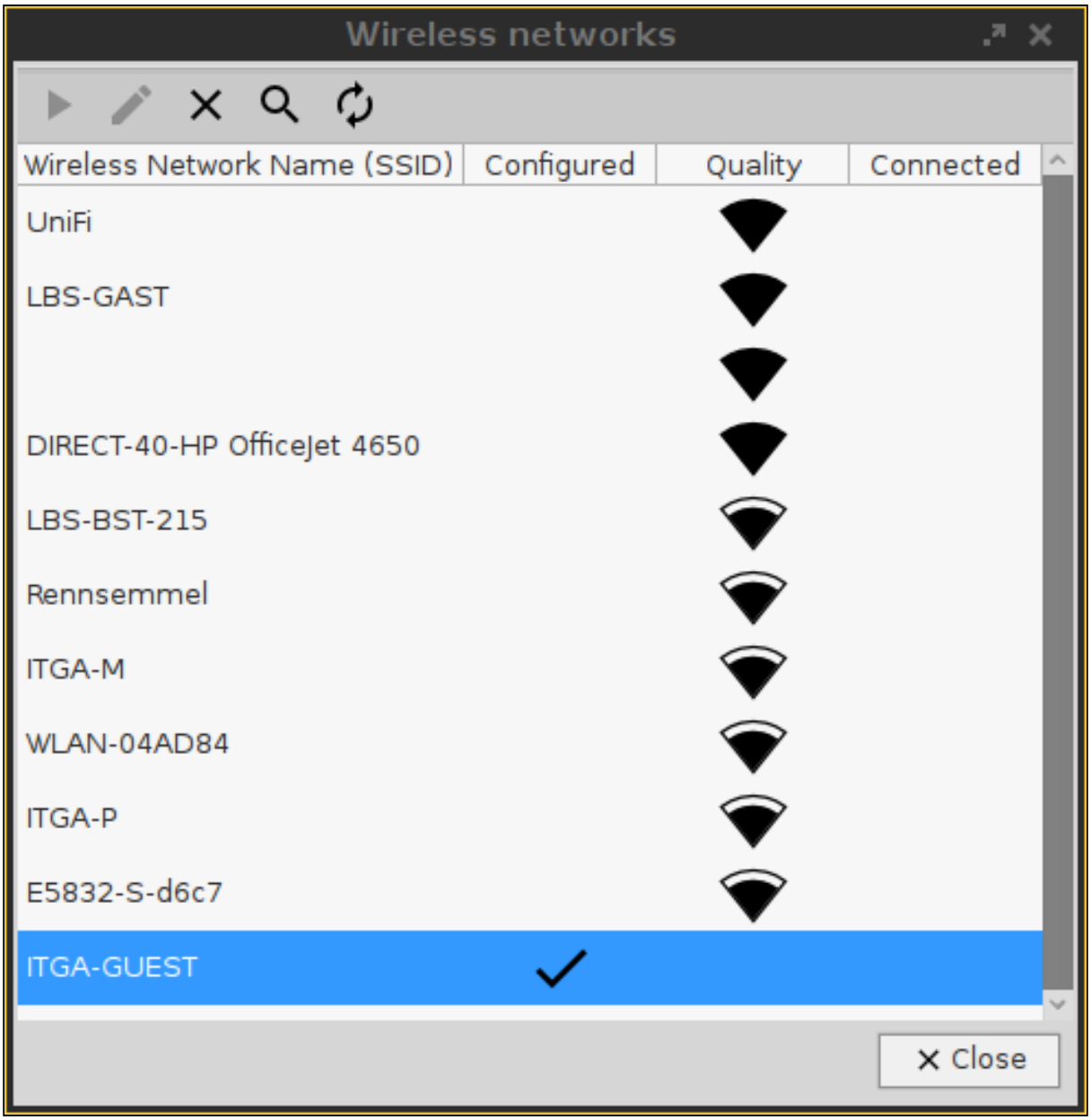
To configure a wireless network with the Wireless Manager:

1. Open **Network > LAN interfaces > Wireless** in the Setup.
2. Enable **Activate wireless interface**.
3. Activate **Enable Wireless Manager**.
4. Click the tray icon

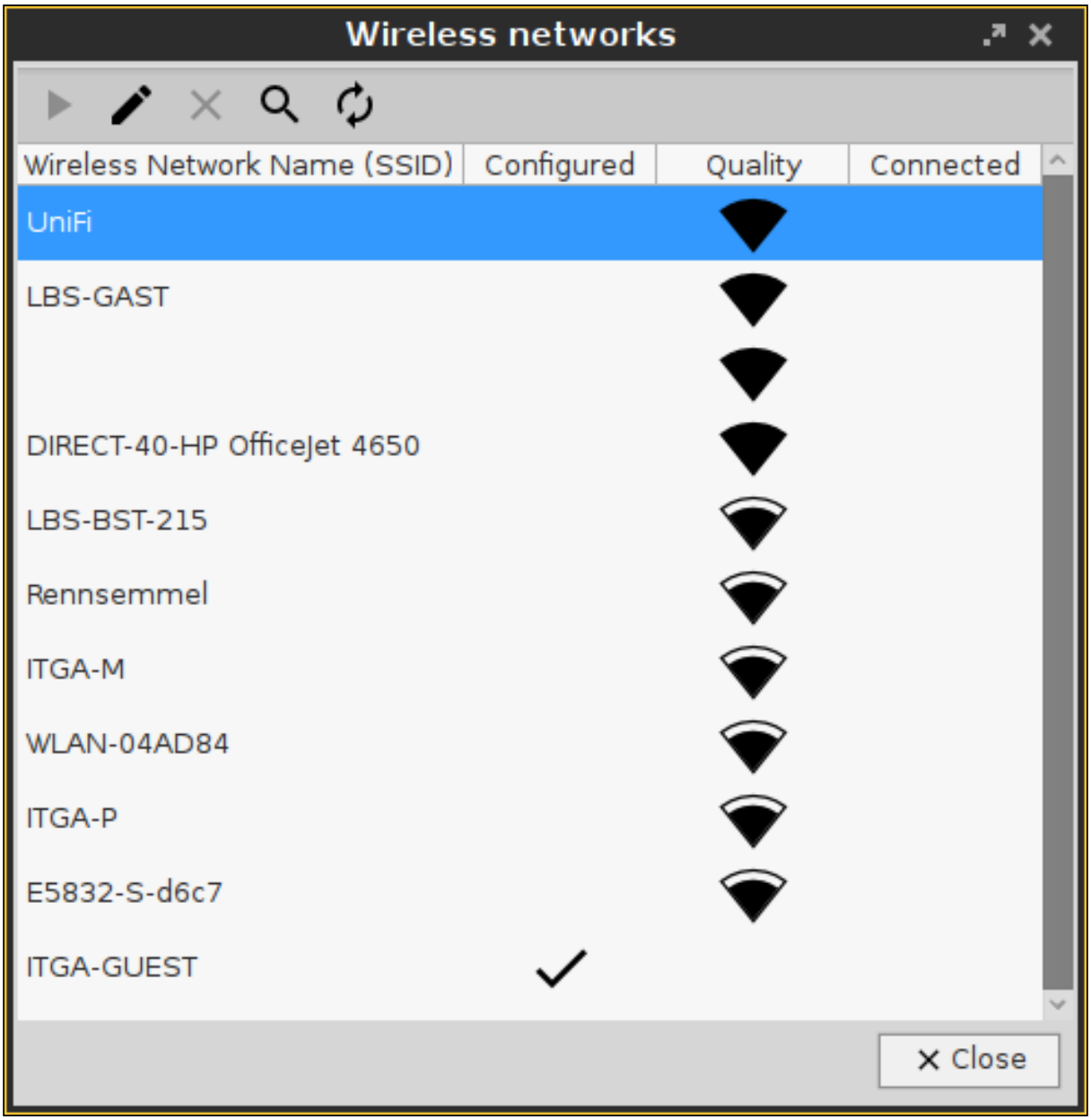
   and select **Manage wireless networks**.

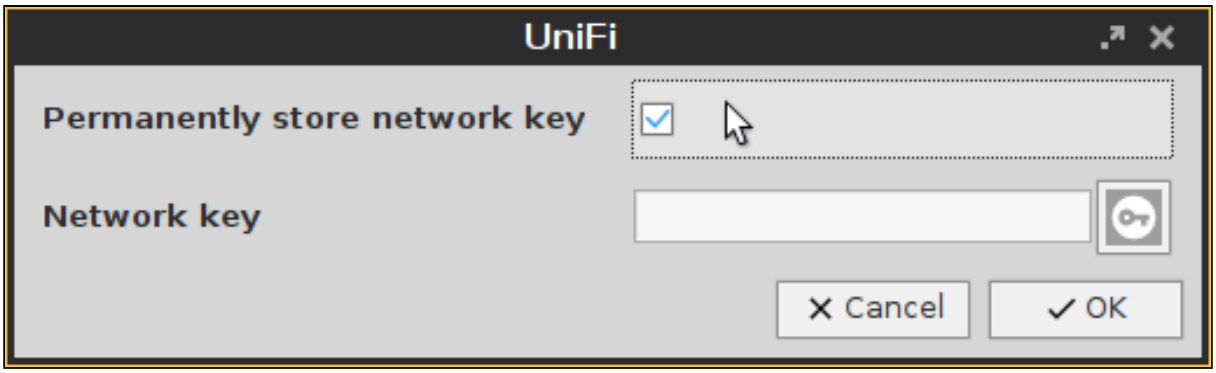
   The **Wireless networks** dialog opens. After a few seconds, all wireless networks within reach are shown, sorted by signal strength. Previously configured connections are flagged with a tick in the **Configured** column. The connection currently active is flagged with a symbol under **Connected**.



5. Double-click the network to be configured.



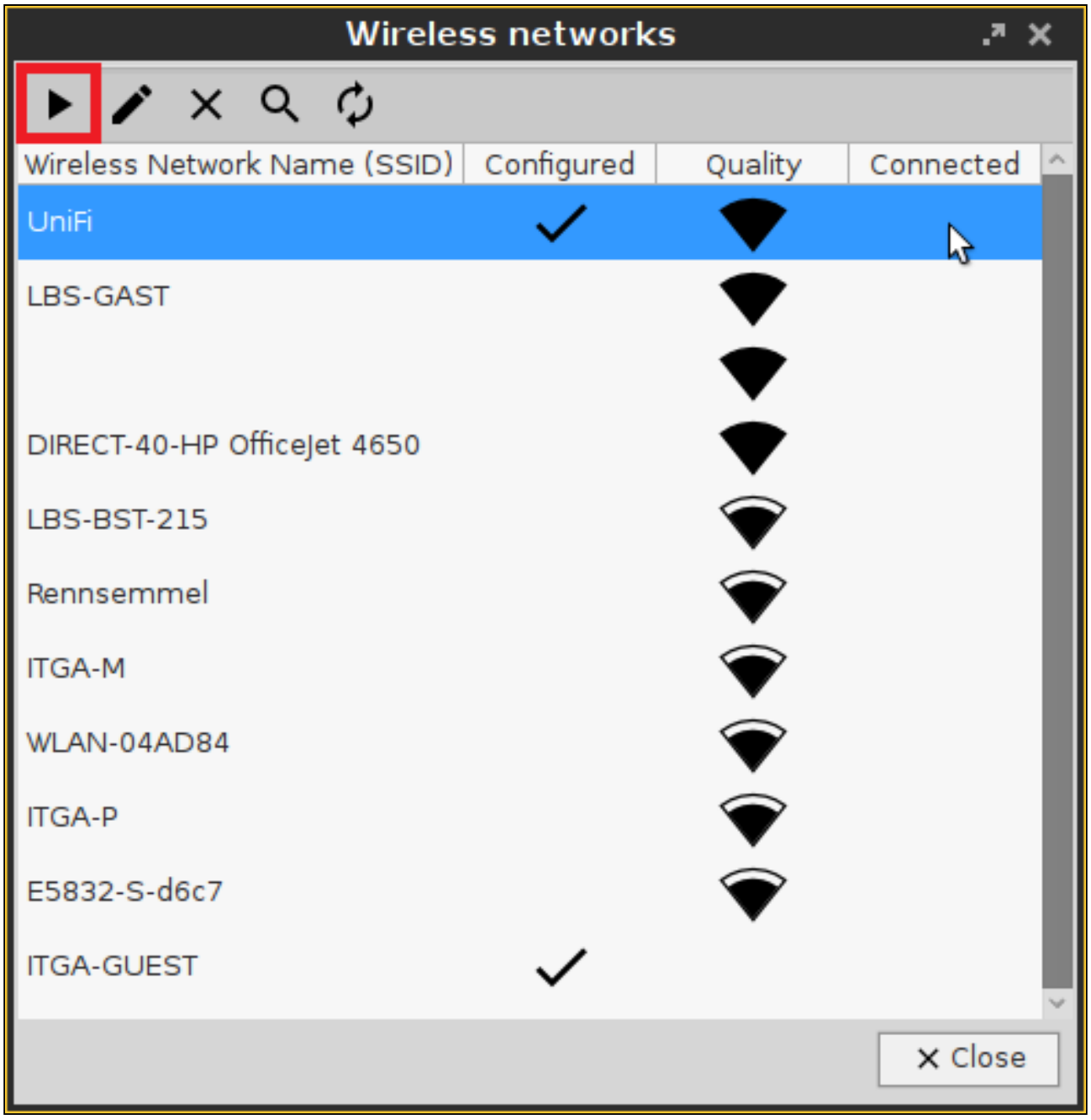
A dialog named with the name (SSID) of the desired network opens.



6. Activate **Permanently store network key** so that your mobile device remembers the network key.
7. Enter the **Network key**. To have the network key displayed while typing, click .
8. Click **OK**.
9. Repeat the steps described above for the remaining networks.

To connect to a configured network manually:

->Highlight the network and click on in the **Wireless networks** dialog.



Your mobile device is connected to the wireless network. The icon shows the network's current signal strength.

Reduce CPU Power Consumption

Reduce CPU Power Consumption

When you are using the *IGEL Universal Desktop Converter* (UDC2) on a mobile device in battery mode, you might want to reduce power consumption. One major power consumer is your CPU.

You can easily gain some control over the power consumption of your CPU using the tray icon (**CPU Power Plan**) on your taskbar.

->If the tray icon is not displayed, open the IGEL Setup, go to **System > Power Options > System** and activate **Tray Icon**.

To change the CPU power settings:

1. Click on .
2. Select the appropriate option. **High Performance** gives you the highest performance, but also the highest CPU power consumption, **Power Saver** results in lowest performance and lowest CPU power consumption. The other options are in between.
   For further information about the power plan settings, see the system (see page 2178) chapter in the manual.

Installing UDC3 on Secunet SINA Workstation

To install IGEL Universal Desktop Converter 3 on a SINA workstation, proceed as follows:

1. Download the UDC3 zip file under IGEL Software Download[248] and unzip the file.
2. Copy the ISO image to an USB stick.
3. Start the SINA workstation
4. Click **Administration > Volumes** in the navigation bar.
5. Click **+ Add item** at the bottom of the screen to add a new item.
6. Enter a distinct name for the volume in the **Name** field top right.
   The target drive is already specified.
7. Click **New CFS** under **Select volume type**.
   The form expands.
8. Choose the preconfigured **Security domain**, **Cipher algorithm** and **Hash algorithm**.
9. Click **Define Guest system** under **CFS content**.
   The form expands.
10. Enter a distinct name for the system under **Guest system name**.
11. Choose **2 GiB** as minimum for the **Guest system size**.
12. Select **Disabled** under **Quarantine**.
13. Click **Create**.

The system will now create the volume. This may take a while - depending on the size of the guest system.

1. Go to **Administration > Volumes** and click the new volume.
   Next to it a little form opens.
2. Open **Guest systems**.
   You will see the volume you've created.
3. Click **Local** under **Add guest system from...** to add the ISO image to this volume.
   The form expands.
4. Plug the USB Stick with the ISO image into the workstation.
5. Choose the stick as **Device** and the ISO image as **Guest system image**.
6. Click **Add** at the bottom of the form.

The system now adds the ISO image to your new volume. This will take a while.

1. Switch to the **Workplaces** menu.
2. Click **+ Add item** at the bottom of the screen.
3. Enter a distinct name for the workplace in the **Name** field top right.
4. Choose the **Guest system** you've created. It has a small hard disk icon.
5. Choose the ISO image under **Secondary guest system**. It should have a small CD icon.
6. Select **Secured networking** under **Network mode**.
7. Choose your prefered settings under **Display layout**, **Workplace hotkey** and **Audio mode**.
8. Select **CD/DVD** under **Boot order**.
9. Select **Automatic reservation** under **IP to claim** and **MAC to claim**.
10. Select **Ubuntu** as **OS type**.
11. It is not necessary to activate the **Detailed settings**.

248. https://www.igel.com/software-downloads/

12. Click **Create**.

The system now creates the workplace.

1. Klick on the new workplace.
   Next to it a little form opens.
2. Click **Launch** to start the workplace.
   The IGEL Universal Desktop Converter starts.
3. After a few second you will see this screen:

4. Keep the first selected item **Boot IGEL UD Converter**.
   The conversion process starts.
   Next you will see the blue IGEL Linux background.
   A little popup appears.
5. Choose your desired **language**.
6. Agree the **license agreement**.
7. Install the IGEL Linux OS to the workspace.

Be aware, that all data of the volume will be deleted. That's why you should always create a new volume for the IGEL Linux OS.

Setting up IGEL OS on Mobile Devices

- Multi Monitor Environment (see page 2182)
- Presentation Mode (see page 2183)
- Display Brightness (see page 2184)
- Power Management (see page 2185)
- Wireless Manager (Café Wireless) (see page 2186)
- Shortening Network Timeouts in Mobile Scenarios (see page 2187)
- Battery Level Control (see page 2189)

Multi Monitor Environment

If you use your notebook in an office workstation, you can use a multi monitor environment.

To configure the display for multiple screens, use the **Display Switch**.

Respective Tray Icon:

Tray Icon Name	Icon	Where to configure
Display Switch		Menu path: **Setup > Accessories > Display Switch**

Activating the Display Switch:

1. Enable the **Display Switch** in the **IGEL Setup** under **Accessories > Display Switch**.
2. Select **Quick Start Panel** as a starting method.
   The **Display Switch** icon is shown in the quick start panel.
3. Click the icon to open the display configuration dialogue.
4. Switch between simple and advanced settings.

For a detailed description, see the manual, chapter Display Switch (see page 1730).
Here you can find additional instructions concerning monitor settings:

- How-To Dual Screen (see page 835)
- Manual topic RDP Global > Window (see page 1314)

Presentation Mode

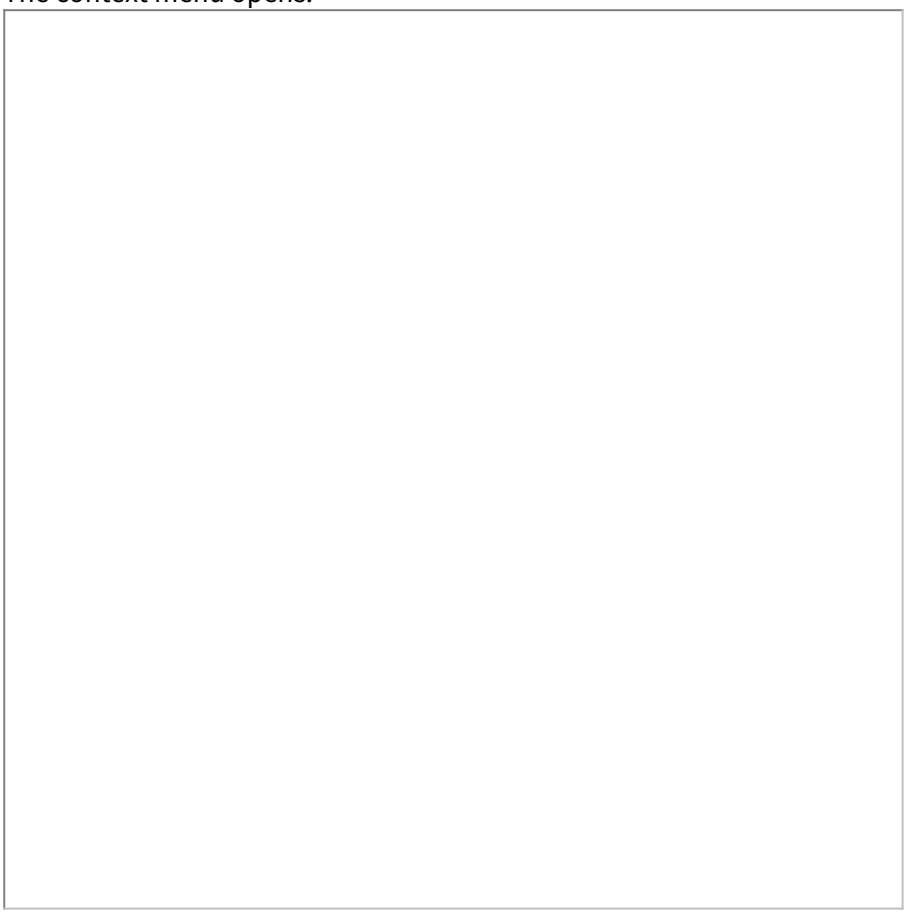
You are using your mobile device for a presentation. You neither want the monitor to enter power saving mode nor to start the screensaver during the presentation.

For this situation, use the **Presentation Mode** which disables the DPMS and the screen saver.

Respective Tray Icon:

Tray Icon Name	Icon	Where to configure
Notebook BAT		Menu path: **Setup > System > Power Options > Battery**

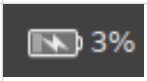
Activating the **Presentation Mode**:

1. Right-click the battery symbol in the system tray.
   The context menu opens:
   
2. Click **Presentation Mode** to enable/disable it.

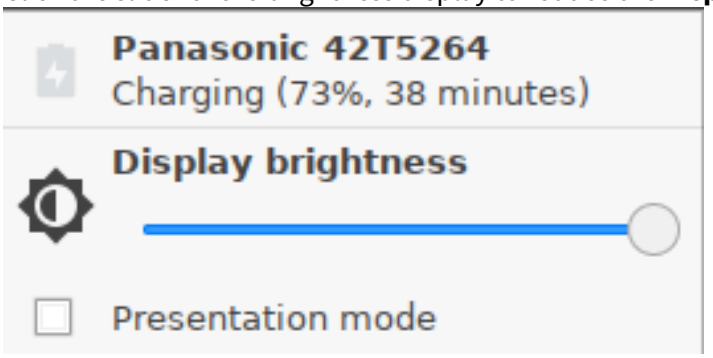
Display Brightness

In order to preserve the battery you want to reduce the display brightness.

Respective Tray Icon:

Tray Icon Name	Icon	Where to configure
Notebook BAT		Menu path: **Setup > System > Power Options > Battery**

1. Right-click the battery symbol in the system tray.
   The context menu opens.
2. Click the slider of the brightness display to reduce the **Display Brightness**.



Power Management

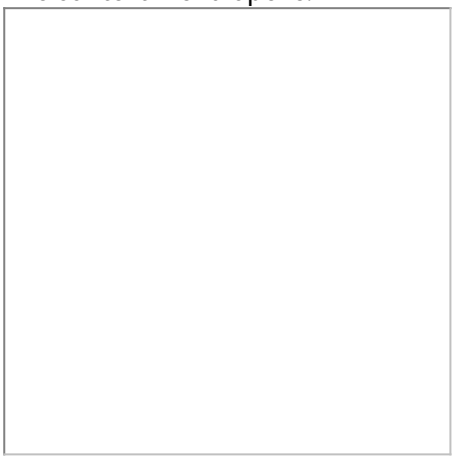
You are using your mobile device in battery mode and need to reduce power consumption to preserve the battery.

To save power, set CPU power options to scale the CPU frequency down.

Respective Tray Icon:

Tray Icon Name	Icon	Where to configure
CPU Power Plan		Menu path: **Setup > System > Power Options > System**

Setting CPU power options:

1. Click the CPU Power Plan icon in the system tray.
   The context menu opens.
   
2. Select the appropriate mode.

Here you can find additional instructions concerning the power management:

- Define the **CPU Power Plan, Critical Battery Level**, **Standby Time** or **Suspend Time, Brightness reduction**, and **Shut-down Options**. See the manual, chapter System Power Options in IGEL OS (see page 2063).

Wireless Manager (Café Wireless)

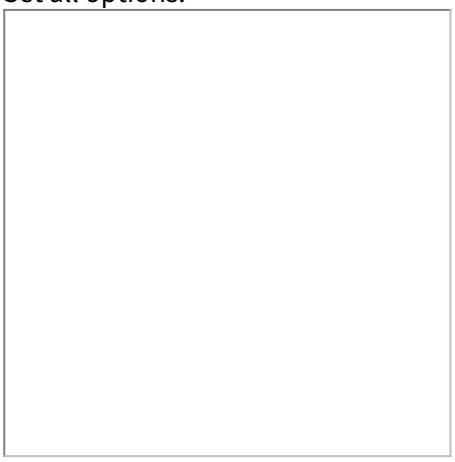
If you are traveling with your notebook, you need to handle different WiFi connections.

You can use **Café wireless** to configure different wireless network connections.

Respective Tray Icon:

Tray Icon Name	Icon	Where to configure
Wireless Network Connection		Menu path: **Setup > Network > LAN Interfaces > Wireless**

Defining **Café wireless**:

1. Enable the **Wireless Manager** under **Network > LAN Interface > Wireless**.
   Set all options:
   
2. Click the WiFi tray icon in the right corner of the panel.
3. Open the **Wireless Manager** dialog.

You can find the complete instruction in the manual, chapter Wireless Manager (see page 1910).

Shortening Network Timeouts in Mobile Scenarios

When on the road with their UDC2 mobile device, users often experience slow system startup. This is due to the system waiting for network connections or the UMS which are not available in the mobile scenario. This document describes how to minimize waiting by shortening various timeouts.

Don't Wait for Wired Network

When an Ethernet interface is configured but not physically connected, startup is delayed by default. The goal is to give the user an opportunity to plug in the network cable. If this is not desired, as of IGEL Linux version 5.10.100waiting can be turned off.

1. In Setup, go to **System > Registry.**
2. Go to the `network.interfaces.ethernet.device[number].nolink_nowait` registry key. Replace [number] with:
   - 0 for eth0, the first Ethernet interface
   - 1 for eth1, the second Ethernet interface
3. Enable **No waiting without physical link.** By default, this option is disabled.

Don't Contact UMS Unless Specific Network Devices Are Up

Startup is also delayed because the system tries to contact UMS by default, which may not be available in a mobile scenario. You can configure IGEL Linux version 5.10.100 to contact UMS only if one of the network devices in a whitelist is up.

1. In Setup, go to **System > Registry.**
2. Go to the `system.remotemanager.device_whitelist` registry key.
3. Put a space-separated device list into the **Network device whitelist** field. Only if at least one of these devices is up, the system will try to contact UMS. Device names:
   - First Ethernet adapter: `eth0`
   - Second Ethernet adapter: eth1
   - Wireless: wlan0
   - Mobile broadband: ppp10
   - OpenVPN: tun0

Don't Contact UMS Unless Specific Networks Are Available

You can configure IGEL Linux version 5.10.100 to contact UMS only if one of the networks in a whitelist is reachable.

1. In Setup, go to **System > Registry.**
2. Go to the `system.remotemanager.network_whitelist` registry key.
3. Enter a space-separated list of networks in CIDR notation into the **Network whitelist** input field, e.g. 172.30.0.0/16 192.168.100.0/24. If there are entries in this field, the system will only try to contact UMS if one of the device's current IP addresses happens to be in one of these ranges.

Shorten the UMS Timeout

When different environments cannot be distinguished by the previous two mechanisms, as of IGEL Linux version 5.10.100 the startup delay can be reduced by setting a shorter timeout for connections to the UMS.

1. In Setup, go to **System > Registry.**

2. Go to the `system.remotemanager.rmagent_timeout` registry key.
3. Enter an integer number of seconds into **IGEL Remote Management Timeout**. The default is 90.

Don't Wait for All Network Interfaces

You can configure IGEL Linux to wait only for one of the network interfaces to be up instead of all. This also means that error messages concerning Ethernet devices will only be displayed shortly.

1. In Setup, go to **System > Registry.**
2. Go to the `network.global.waitfor_interfaces` registry key.
3. Disable **Wait for interfaces to come up**. By default, this option is enabled.

Battery Level Control

Since Linux *version 10.03.100* it is possible to display the battery level of a mobile device via UMS. The frequency of the battery level reports sent by the device to the UMS can be adjusted: A report is triggered when the battery status has changed at a specified percentage compared to the previously reported status. The percentage is specified by the **Battery status update frequency** parameter.

Example use case: The IT administrator in a hospital has to take care of battery-powered medical devices. Using the new feature, he can easily keep track of all these devices via the UMS, without any need of physical access or mirroring VNC.

To adjust the report frequency:

1. In Setup, go to **System > Registry**.
2. Go to the `system.remotemanager.battery_report_frequency` registry key.
3. Select the **Battery status update frequency**:
    - Often
    - Normal
    - Rarely
    - Very Rarely
    - Never
4. Click **Apply** or **Ok**.

Rolling out Initial Settings with IGEL OSC

If you would like to roll out initial settings with your IGEL OS Creator (OSC) installation, you can do it through:

- modifying the OSC ISO file (see page 2190)
  Use this method to store initial settings and licenses on the ISO.
- modifying the Master Image (see page 2194)
  Use this method if you already have a master image at hand and you want to add initial settings, licenses, ca-certs to it, so that they get rolled out after the first boot.

Modification of an OSC ISO for Rolling out Settings

Overview

Overview of the process for initial settings and license rollout:

1. Extract your ISO.
2. Create initial-settings directory in the extracted ISO.
3. Copy or create a setup.ini with the settings you want to the initial-settings directory.

> ⚠ Do not add passwords.

4. Copy or create a ca-certs directory with certificates to the initial-settings directory you want to add to the installed system.
5. Copy or create a wfs-template directory in the initial-settings directory with files and directories you want to add to the /wfs directory of the installed system.
6. If you have license files, simply copy them to the initial-settings. All *.lic files in the / directory of the first partition will get copied to the /license/dsa/licenses directory.

> ⚠ The filesize of the licenses is limited to 1MiB.

7. Repack the ISO again.

> ℹ
> - You can gzip, bzip2 or xz the setup.ini file; it will get extracted if no setup.ini is present (if setup.ini is also present the packed file will be ignored).
> - You can gzip the license file also.

- The setup.ini and the *.lic files which are not packed will go through dos2unix to ensure a UNIX file format.

Detailed Description with Examples

You will need xorriso to do the below which is not part of the IGEL OS so you will need to use a other Linux system to do this.

1. Extract ISO content.
   This can be done with `xorriso -osirrox on -indev <iso file> -extract <target dir> <target name>`. In the example we use: `/isofiles/osc11.05.100.iso` for `<iso file>`, and as `<target dir>`, and `osc-data` as `<target name>` which leads to following command line:

```
xorriso -osirrox on -indev /isofiles/osc11.05.100.iso -extract . osc-data
xorriso 1.4.8 : RockRidge filesystem manipulator, libburnia project.

Copying of file objects from ISO image to disk filesystem is: Enabled
xorriso : NOTE : Loading ISO image tree from LBA 0
xorriso : UPDATE : 414 nodes read in 1 seconds
xorriso : NOTE : Detected El-Torito boot information which currently is set to
be discarded
Drive current: -indev '/isofiles/osc11.05.100.iso'
Media current: stdio file, overwriteable
Media status : is written , is appendable
Boot record  : El Torito , MBR isohybrid cyl-align-off GPT
Media summary: 1 session, 1458176 data blocks, 2848m data, 45.4g free
Volume id    : 'IGEL_OSC_TO'
xorriso : UPDATE : 356 files restored ( 777.9m) in 1 seconds , 588.9xD
xorriso : UPDATE : 377 files restored (1641.6m) in 2 seconds , 653.9xD
xorriso : UPDATE : 391 files restored (2578.4m) in 3 seconds , 709.2xD
xorriso : UPDATE : 414 files restored (2846.4m) in 3 seconds = 653.2xD
Extracted from ISO image: file ''='/tmp/osc-data'
```

   The complete ISO will get extracted to the osc-data directory.

2. Create initial-settings directory in the extracted ISO data.
   Above we extracted the data to `/tmp/osc-data`, so we need to create the directory in this directory:

```
mkdir /tmp/osc-data/initial-settings
```

3. Copy your files and directories to the initial-settings directory.
   In our example we use `/tmp/osc-data/initial-settings` as target directory. If, for example, you have the following you want to add to the ISO:
   - a `setup.ini`,
   - a ca-certs file `SSL+VPN+CA.crt`,
   - license files `782DAFC836185589DD6212375DC33C22.lic` `D5F47E9338C3A46A0D0F785B9F6A6926.lic`
   - a Wallpaper `wallpaper.jpg,`

   you can do the following:

   ```
   mkdir -p /tmp/osc-data/initial-settings/ca-certs
   mkdir -p /tmp/osc-data/initial-settings/wfs-template
   cp setup.ini /tmp/osc-data/initial-settings/
   cp 782DAFC836185589DD6212375DC33C22.lic
   D5F47E9338C3A46A0D0F785B9F6A6926.lic /tmp/osc-data/initial-settings/
   cp SSL+VPN+CA.crt /tmp/osc-data/initial-settings/ca-certs/
   cp wallpaper.jpg /tmp/osc-data/initial-settings/wfs-template
   ```

   The licenses files will get copied to the license partition. The `setup.ini` and `wallpaper.jpg` will be copied to `/wfs/` and the contents of the `ca-certs` directory will be copied to `/wfs/ca-certs`.

4. Repack the ISO again.
   a. First, check if the original ISO was a legacy version or not.
   For this, execute `xorriso -indev <iso file> -find / -name boot 2>&1` and search for the line with `Boot record`. If there is a `GPT` in this line, the ISO is not a legacy ISO.
   Example:

   ```
   xorriso -indev /isofiles/osc11.05.100.iso -find / -name boot 2>&1 | grep
   -E "^Boot record.*GPT"
   Boot record  : El Torito , MBR isohybrid cyl-align-off GPT
   ```

   b. Repack the non-legacy ISO with xorriso and with these additional parameters:
   `xorriso -as mkisofs -rock -omit-version-number -disable-deep-relocation -volid IGEL_OSC_TO -b boot/isolinux/isolinux.bin -c boot/isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-`

`info-table -eltorito-alt-boot -e igel_efi.img -no-emul-boot -isohybrid-mbr "<extracted iso dir>/boot/isolinux/isohdpfx.bin" -isohybrid-gpt-basdat -o "<target iso file>" "<extracted iso dir>"`.
Example:

```
xorriso -as mkisofs -rock -omit-version-number -disable-deep-relocation
-volid IGEL_OSC_TO -b boot/isolinux/isolinux.bin -c boot/isolinux/boot.cat
-no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e
igel_efi.img -no-emul-boot -isohybrid-mbr "/tmp/osc-data/boot/isolinux/
isohdpfx.bin" -isohybrid-gpt-basdat -o "osc11.05.100.iso" "/tmp/osc-data"
xorriso 1.4.8 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:osc11.05.100.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 43.7g free
Added to ISO image: directory '/'='/tmp/osc-data'
xorriso : UPDATE : 414 files added in 1 seconds
xorriso : UPDATE : 414 files added in 1 seconds
xorriso : NOTE : Copying to System Area: 432 bytes from file '/tmp/osc-
data/boot/isolinux/isohdpfx.bin'
xorriso : WARNING : Boot image load size exceeds 65535 blocks of 512
 bytes. Will record 0 in El Torito to extend ESP to end-of-medium.
libisofs: NOTE : Automatically adjusted MBR geometry to 1024/178/32
libisofs: NOTE : Aligned image size to cylinder size by 432 blocks
xorriso : UPDATE :  2.19% done
xorriso : UPDATE :  29.31% done
xorriso : UPDATE :  60.27% done, estimate finish Wed Feb 24 12:50:05 2021
xorriso : UPDATE :  91.42% done
ISO image produced: 1458176 sectors
Written to medium : 1458176 sectors at LBA 0
Writing to 'stdio:osc11.05.100.iso' completed successfully.
```

c. Repack the legacy ISO with xorriso and with these additional parameters:
`xorriso -as mkisofs -rock -omit-version-number -disable-deep-relocation -volid IGEL_OSC_TO -b boot/isolinux/isolinux.bin -c boot/isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -no-emul-boot -isohybrid-mbr "<extracted iso dir>/boot/isolinux/isohdpfx.bin" -isohybrid-gpt-basdat -o "<target iso file>" "<extracted iso dir>".`
Example:

```
xorriso -as mkisofs -rock -omit-version-number -disable-deep-relocation
-volid IGEL_OSC_TO -b boot/isolinux/isolinux.bin -c boot/isolinux/boot.cat
-no-emul-boot -boot-load-size 4 -boot-info-table -no-emul-boot -isohybrid-
mbr "/tmp/osc-data/boot/isolinux/isohdpfx.bin" -isohybrid-gpt-basdat -o
"osc11.05.100.iso" "/tmp/osc-data"
xorriso 1.4.8 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:osc11.05.100.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 43.7g free
Added to ISO image: directory '/'='/tmp/osc-data'
xorriso : UPDATE : 414 files added in 1 seconds
xorriso : UPDATE : 414 files added in 1 seconds
xorriso : NOTE : Copying to System Area: 432 bytes from file '/tmp/osc-
data/boot/isolinux/isohdpfx.bin'
libisofs: NOTE : Automatically adjusted MBR geometry to 1024/178/32
libisofs: NOTE : Aligned image size to cylinder size by 432 blocks
xorriso : UPDATE :  2.19% done
xorriso : UPDATE :  29.31% done
xorriso : UPDATE :  60.27% done, estimate finish Wed Feb 24 12:50:05 2021
xorriso : UPDATE :  91.42% done
ISO image produced: 1458176 sectors
Written to medium : 1458176 sectors at LBA 0
Writing to 'stdio:osc11.05.100.iso' completed successfully.
```

Modification of a Master Image for Rolling out Settings after First Boot

Overview

1. Check if the first partition is a VFAT marked partition and make sure that there are 4 partitions present.

⚠ Only the Master Images with 4 partitions support the rollout of initial settings.

2. Format the first partition with VFAT.
3. Mount the first partition.
4. Copy or create a setup.ini with the settings you want to the mounted partition.

⚠ Do not add passwords.

5. Copy or create a ca-certs directory with certificates to the mounted partition you want to add to the master image.
6. Copy or create a `wfs-template` directory on the mounted partition with files and directories you want to add to the `/wfs` directory of the installed system.

Only possible with OS version 11.05.100 and newer.

7. If you have license files, copy them to the first partition. All `*.lic` files in the / directory of the first partition will get copied to the `/license/dsa/licenses` directory.

The filesize of the licenses is limited to 1MiB.

8. Umount the first partition.

- You can gzip, bzip2 or xz the setup.ini file; it will get extracted if no setup.ini is present (if setup.ini is also present the packed file will be ignored).
- You can gzip the license file also
- The `setup.ini` and the `*.lic` files which are not packed will go through dos2unix to ensure a UNIX file format

Detailed Description with Examples

The easiest way is to write the master image to a device and do the changes on the device directly. Keep in mind if you boot once from the device this will not be a master image anymore.

Be very careful with choosing the correct `<device>` in the example steps below as this can harm your running system.

1. Check if the device contains 4 partitions and the first is usable for initial settings rollout.
   For example, use `fdisk -l <device>` to check the partitions from an IGEL system. If `<device>` is replaced with `/dev/sda` then the output should look like the below, which means, there are 4 partitions present and the first one is a FAT32 so this Master Image is capable of rolling out initial settings.

```
fdisk -l /dev/sda
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x144ad2c2

Device     Boot  Start     End Sectors Size Id Type
/dev/sda1         2048   22527   20480  10M  b W95 FAT32
/dev/sda2  *     22528   83967   61440  30M ef EFI (FAT-12/16/32)
/dev/sda3        83968  145407   61440  30M ef EFI (FAT-12/16/32)
/dev/sda4       145408 8382463 8237056   4G 83 Linux
```

2. Try to mount the first partition.
   For example, with `mount <device>1 <target dir>` from an IGEL system. If `<device>` is replaced with `/dev/sda` and `<target dir>` with `/mnt` (you must create the empty directory with `mkdir -p /mnt` first) then there should be no error message.
   If there is an error message like below, then the first partition is not formatted or it is not the correct one.

   ```
   mount /dev/sda1 /mnt
   mount: /mnt: wrong fs type, bad option, bad superblock on /dev/sda1, missing
   codepage or helper program, or other error.
   ```

   In case of an error message:
   a. Check the fdisk output again.

   b. If the mount failed but fdisk output shows 4 partitions and the first is marked as FAT32, format the first partition as VFAT with `mkfs.vfat <device>1` from an IGEL system. If `<device>` is replaced with `/dev/sda` this should look like:

      ```
      mkfs.vfat /dev/sda1
      mkfs.fat 4.1 (2017-01-24)
      ```

   c. If there are no error messages the partition should now be mountable, so call `mount <device>1 <target dir>` again. If `<device>` is replaced with `/dev/sda` and `<target dir>` with `/mnt` you should get no error or warning message at all:

```
mount /dev/sda1 /mnt
```

3. Copy your files and directories to the <target> directory.
   In this case `<target>` will be replaced with `/mnt`.
   If, for example, you have the following you want to add to the master image:
   - a `setup.ini`,
   - a ca-certs file `SSL+VPN+CA.crt`,
   - license files `782DAFC836185589DD6212375DC33C22.lic` `D5F47E9338C3A46A0D0F785B9F6A6926.lic`,
   - and a wallpaper `wallpaper.jpg,`
     you can do the following:

     ```
     mkdir -p /mnt/ca-certs
     mkdir -p /mnt/wfs-templates
     cp setup.ini /mnt/
     cp 782DAFC836185589DD6212375DC33C22.lic
     D5F47E9338C3A46A0D0F785B9F6A6926.lic /mnt/
     cp SSL+VPN+CA.crt /mnt/ca-certs/
     cp wallpaper.jpg /mnt/wfs-templates
     ```

     As a result, the licenses files will get copied to the license partition. The `setup.ini` and `wallpaper.jpg` will be copied to `/wfs/` and the contents of the `ca-certs` directory will be copied to `/wfs/ca-certs`.

4. Umount everything again with `umount <target dir>`.
   Example:

   ```
   umount /mnt
   ```

   There should be no error message after executing the command.

IGEL OS Creator for Windows (OSCW)

The IGEL OS Creator for Windows (OSCW) is able to convert Windows machines to IGEL OS 11, provided that they fulfill the Prerequisites (see page 2200).

Choose the instructions according to your needs:

- IGEL OS Creator for Windows (OSCW) on Windows 7/10 Workstations (see page 2199)
- IGEL OS Creator for Windows (OSCW) on IGEL Windows Embedded 7/7+ (see page 2245)
- IGEL OS Creator for Windows (OSCW) on IGEL Windows 10 IoT (see page 2272)

On modern computers such as secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), there may be a BIOS setting related to Secure Boot that allows the use of Microsoft's 3rd party UEFI Secure Boot Certificate. The usual description of such a BIOS setting is "Allow Microsoft 3rd Party UEFI CA". This setting must be set to enabled, as IGEL uses the 3rd party certificate to support UEFI Secure Boot. If UEFI Secure Boot is enabled, but "Allow Microsoft 3rd Party UEFI CA" is not enabled, you may be unable to boot IGEL OS Creator or UD Pocket. Similarly, if the setting "Allow Microsoft 3rd Party UEFI CA" is disabled after a previous installation of IGEL OS, IGEL OS will fail to boot. For how to enable the setting, see Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot[249].

249. https://kb.igel.com/security-safety/current/secured-core-pcs-microsoft-3rd-party-uefi-certific

IGEL OS Creator for Windows (OSCW) on Windows 7/10 Workstations

Introduction

The IGEL OS Creator (OSC) for Windows is able to convert any Windows 10 or Windows 7 machine to IGEL OS 11, provided that it fulfills the Prerequisites (see page 2200).

Read all the following chapters and follow the instructions in the order given.

- Prerequisites (see page 2200)
- Getting the Required Software (see page 2201)
- Transferring the IGEL OSC File to the UMS (see page 2202)
- Deploying the OSCW Installer on the Target Machines (see page 2203)
- Installing the OSCW Installer (see page 2204)
- Registering the Target Machines to the UMS (see page 2207)
- Configuring the OSCW Installer (see page 2210)
- Starting the Conversion (see page 2242)

Video

A video is available to illustrate the procedure.

Part I

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=NGA0FNLBid0&feature=youtu.be

Part II

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=uXDdQ6aGrZs&feature=youtu.be

Prerequisites

Hardware

- Memory: ≥ 4 GB RAM
- Storage: ≥ 3 GB free storage to store the ISO file containing IGEL OS Creator
- For supported hardware, see *Hardware* > *Supported Devices* > *Devices Supported by IGEL OS 11*.

Software

The following software must be present on the target machines:

- Windows 10 or Windows 7
- Microsoft Hotfix KB3140245 (Windows 7 x86/x64)

Network

- All machines are in a network that can be reached by the UMS.
- For buddy mode: All machines must be joined to a Microsoft Active Directory (AD) and be accessible by the same AD user with reading permissions.

Next Step

>> When all requirements are met, continue with Getting the Required Software[250].

250. https://kb.igel.com/en/igel-os/11.10/getting-the-required-software-1

Getting the Required Software

The following software must be downloaded resp. installed:

IGEL Universal Management Suite (UMS) 6.04.120 or Higher

1. Download UMS 6.04.120 or higher from https://www.igel.com/software-downloads/workspace-edition/ **> Universal Management Suite**.
2. Update your UMS to version 6.04.120 or later. For update instructions, see IGEL UMS Update[251].

OSCW Files

1. Download OSC for Windows 1.01.100 or higher (EXE or MSI installer)
   - EXE file: https://www.igel.com/software-downloads/workspace-edition/ **> OSC for Windows >** `setup-igel-osc-for-windows_1.01.100.exe`
   - MSI file: https://www.igel.com/software-downloads/workspace-edition/ **> OSC for Windows >** `setup-igel-osc-for-windows_1.01.100.msi`
2. Download IGEL OS 11.03.560 or higher (ISO): https://www.igel.com/software-downloads/workspace-edition/ **> OSC for Windows** > `OSC_11.03.560.zip`

Check List

- The UMS is updated to version 6.04.120 or higher.
- OSC for Windows 1.01.100 or higher is available.
- IGEL OS 11.03.560 or higher (ISO file) is available.

Next Step

>> Transferring the IGEL OSC File to the UMS (see page 2202)

251. https://kb.igel.com/en/universal-management-suite/current/igel-ums-update

Transferring the IGEL OSC File to the UMS

In this step, we will transfer the IGEL OS firmware file (ISO) to the UMS so that the UMS can deploy it to the target machines.

> ⚠ Do not register the file as a file object. This might lead to various issues, particularly in ICG and HA environments.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Copy `osc.iso` to `<UMS Installation directory>\rmguiserver\webapps\ums_filetransfer`

Next Step

>> Deploying the OSCW Installer on the Target Machines (see page 2203)

Deploying the OSCW Installer on the Target Machines

In this step, we will deploy the OSCW installer on the target machines.

→ Deploy the installer on all devices that are to be converted. The following methods are available for deployment:

- SCCM (System Center Configuration Manager): Use the MSI installer (`setup-igel-osc-for-windows_1.01.100.msi`) and deploy it just like any software. The OSCW installer is installed silently.
- Group policy: Use the MSI installer (`setup-igel-osc-for-windows_1.01.100.msi`) and deploy it just like any software. The OSCW installer is installed silently.
- File-based methods: Use the EXE file (`setup-igel-osc-for-windows_1.01.100.exe`). You can use file sources such as:
  - USB memory stick
  - Network drive
  - DVD

Check List

✅ The OSCW installer is deployed on all target machines. When SCCM or group policy was used, the installation has been executed silently.

Next Step

If the OSCW installer has been deployed via SCCM or group policy and has been installed silently:

>> Continue with Registering the Target Machines to the UMS (see page 2207).

If the OSCW installer has been deployed via a file-based method:

>> Continue with Installing the OSCW Installer (see page 2204).

Installing the OSCW Installer

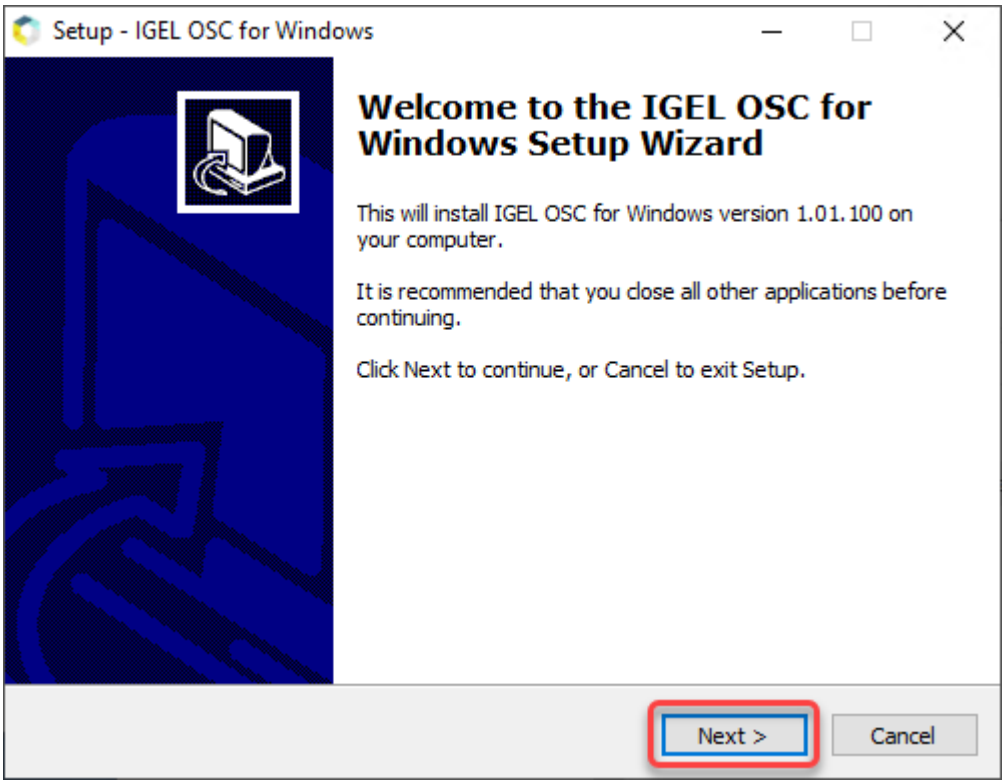
In this step, we will install the OSCW installer on the target machines. The method depends on how the OSCW installer has been deployed on the target machines.

OSCW Installer Has Been Deployed via SCCM or Group Policy

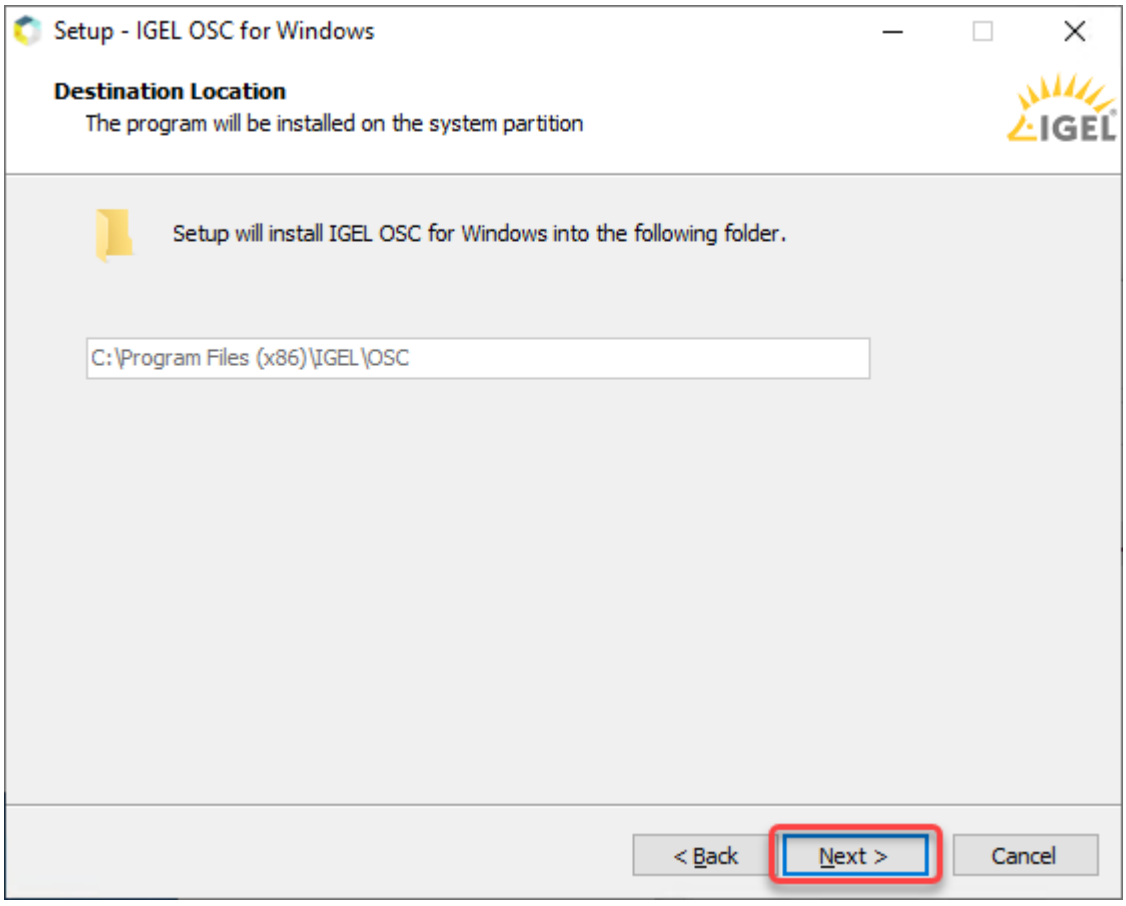
If you have used SCCM or group policy to deploy the OSCW installer, the installation has been executed silently; continue with Registering the Target Machines to the UMS (see page 2207).

OSCW Installer Has Been Deployed from a File

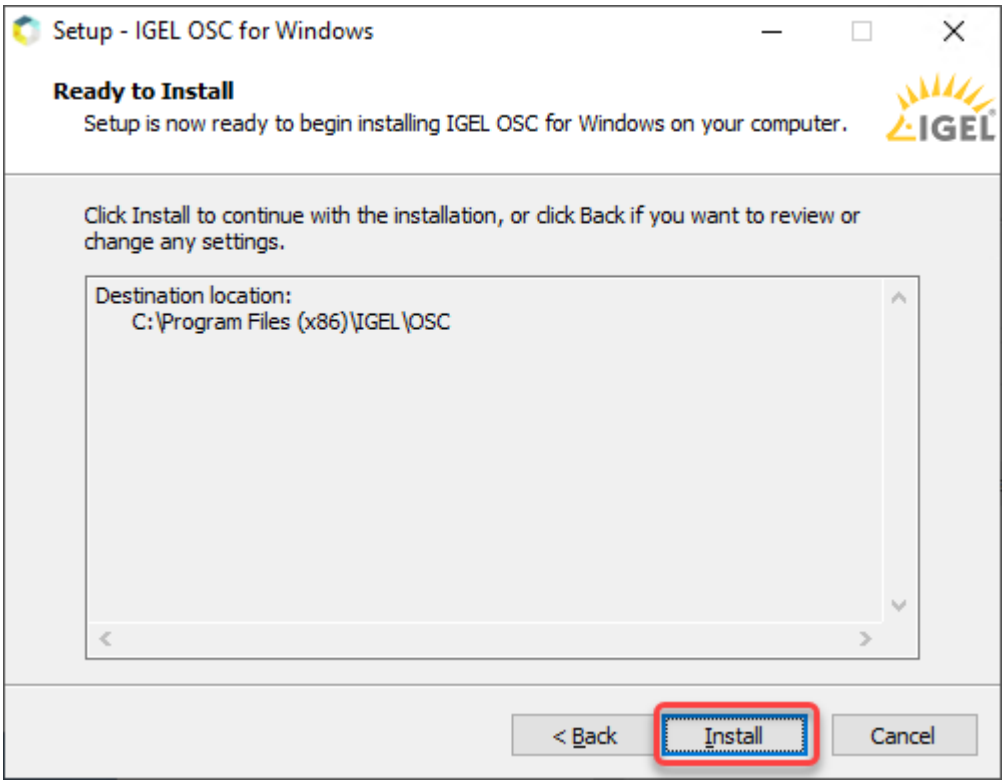
1. On the target machine, double-click `setup-igel-osc-for-windows_1.01.100.exe` and confirm the Windows UAC (user account control). The OSCW installer is digitally signed by "IGEL Technology GmbH".
   The setup wizard opens.
2. Click **Next**.



3. Review the installation folder and click **Next**.



4. Review the confirmed installation folder and click **Install**.



IGEL OSC for Windows is installed on the target machine.

5. The installer window is closed.

Check List

✅ The OSCW installer is installed on each target machine.

Next Step

>> Registering the Target Machines to the UMS (see page 2207)

Registering the Target Machines to the UMS

In this step, we will register all target machines to the UMS. This is necessary because the conversion to IGEL OS will be triggered by the UMS.

Two registration methods are available: a scan by the UMS and automatic registration.

- Registering by a UMS Scan (see page 2207)
- Registering by Automatic Registration (see page 2209)

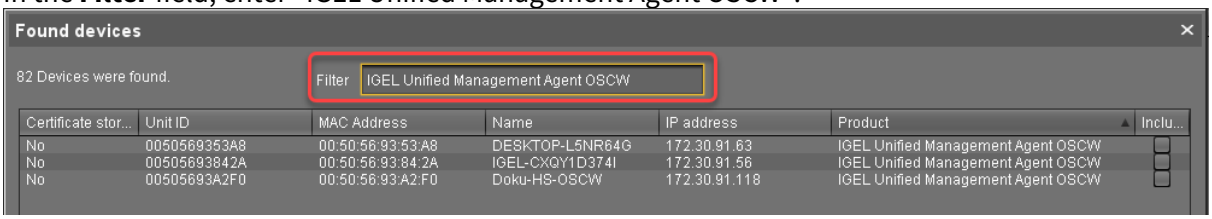
Registering by a UMS Scan

1. Open the UMS Console and click to scan for devices.

2. Select the scope in which the devices are located; for details, see Scanning the Network for Devices and Registering Devices on the IGEL UMS[252].

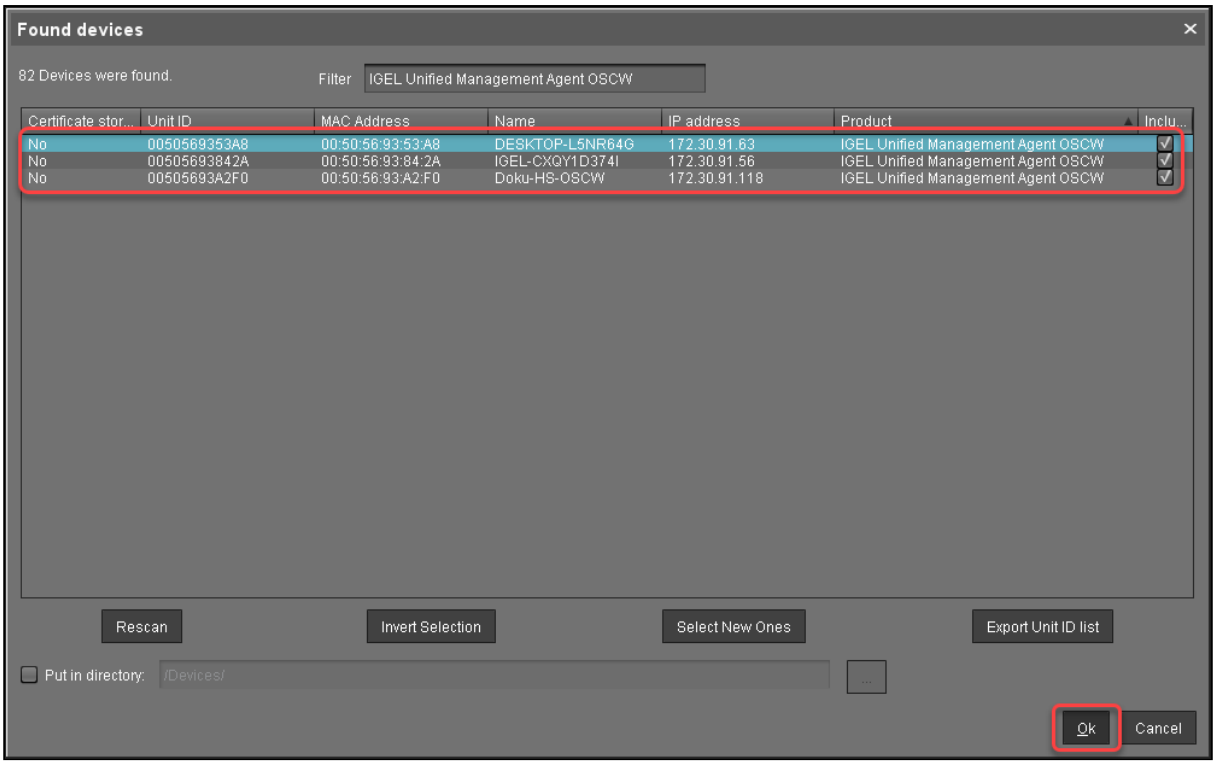
3. Click **Scan**.
   The dialog **Found devices** opens.

4. In the **Filter** field, enter "IGEL Unified Management Agent OSCW".



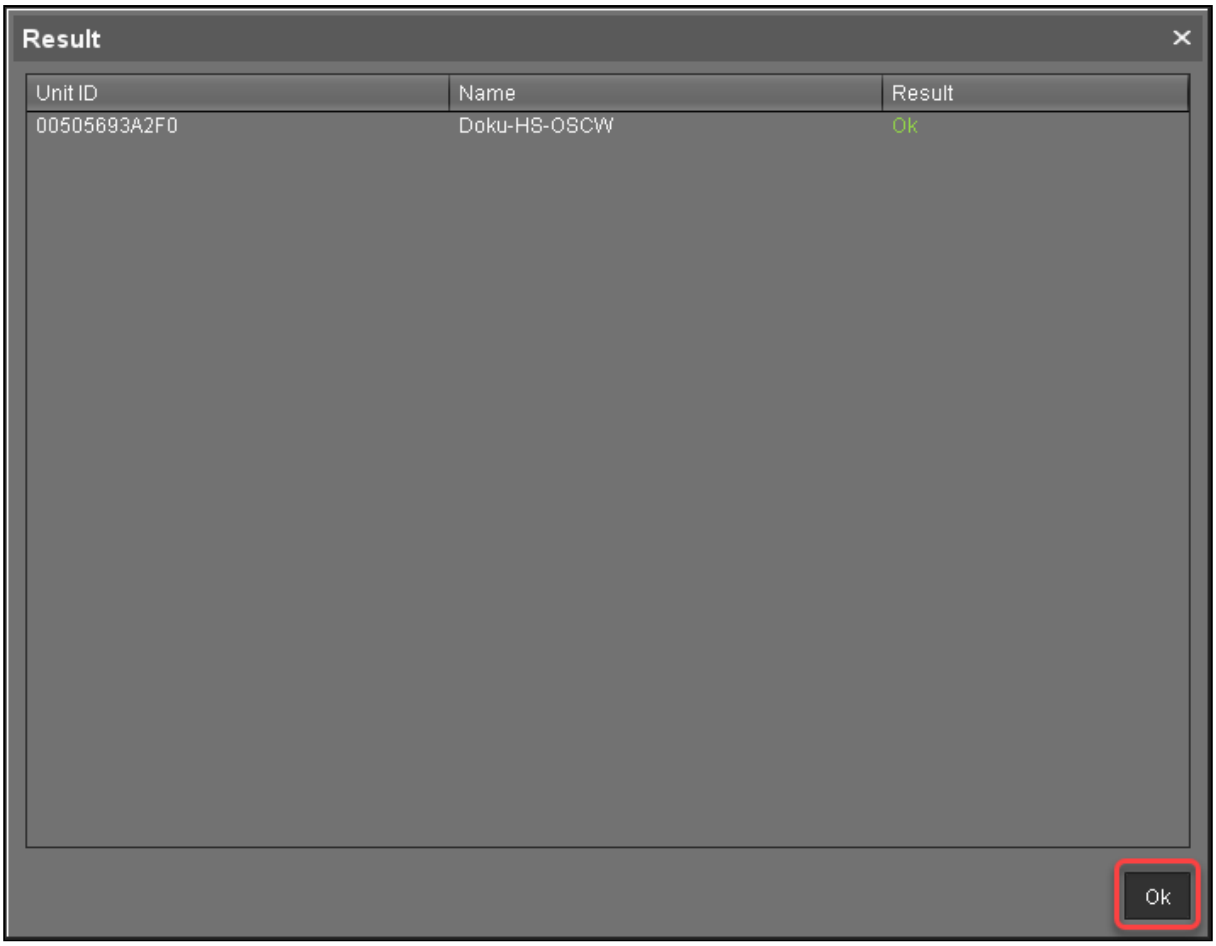
5. Select all target machines and click **Ok**.

252. https://kb.igel.com/en/universal-management-suite/current/how-to-scan-the-network-for-devices-and-register-d



The target machines are registered with the UMS.

6. In the **Result** dialog, click **Ok**.



Registering by Automatic Registration

For this method, a DNS entry or DHCP option must be set.

→ Follow the instructions in (12.06.110-en) Registering Devices Automatically on the IGEL UMS .

Check List

✅ All target machines are registered with the UMS.

Next Step

>> Configuring the Installer (see page 2210)

Configuring the OSCW Installer

In this step, we will provide the OSCW installer with the download source for the ISO file that contains the IGEL OS Creator.

Two methods are available:

- Configuring the OSCW Installer in Normal Mode (see page 2211): Each target machine downloads the ISO file from the server (UMS) individually. This increases the amount of outgoing traffic from the UMS.
- Configuring the OSCW Installer in Buddy Mode (see page 2224): This method is recommended if the connection bandwidth of the download source is limited; it ensures a more balanced use of network bandwidth during the distribution of the ISO file to the target machines. First, a group of target machines downloads the ISO file. Then, these machines serve as the download source ("update buddies") for the remaining target machines. As a requirement, all devices must be joined to a Microsoft Active Directory (AD) and be accessible by the same AD user with reading permissions.

Configuring the OSCW Installer in Normal Mode

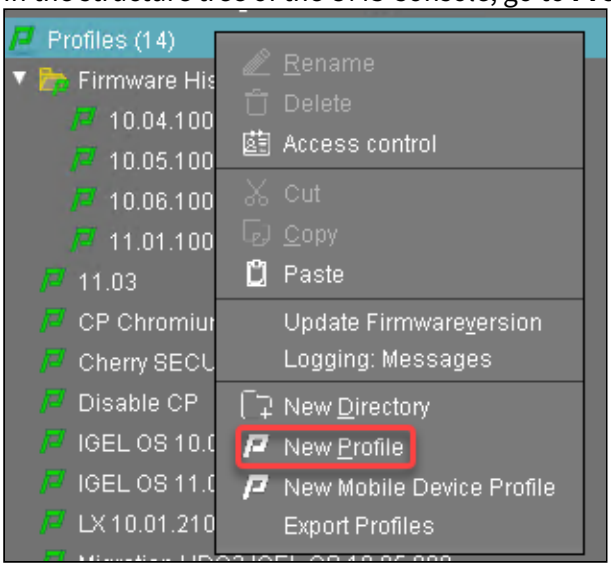
To provide the OSCW installer with the download source for the IGEL OS Creator file (ISO), we will create a profile that provides the path to that file. To assign the profile to the target machines, we will use a view that recognizes the target machines by their product ID.

The configuration comprises the following steps:

- Creating a Profile (see page 2211)
- Creating a View to Select All Target Machines (see page 2213)
- Assigning the Profile to the Target Machines (see page 2219)
- Monitoring the Process (see page 2221)

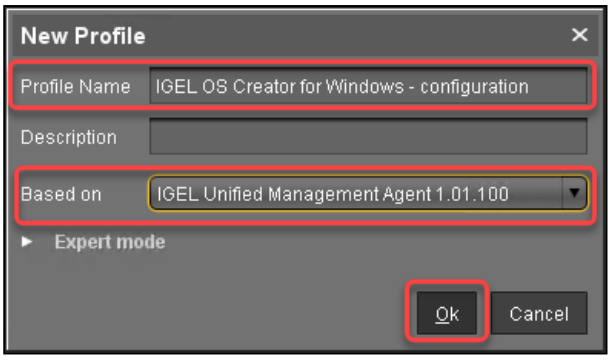
Creating a Profile

1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



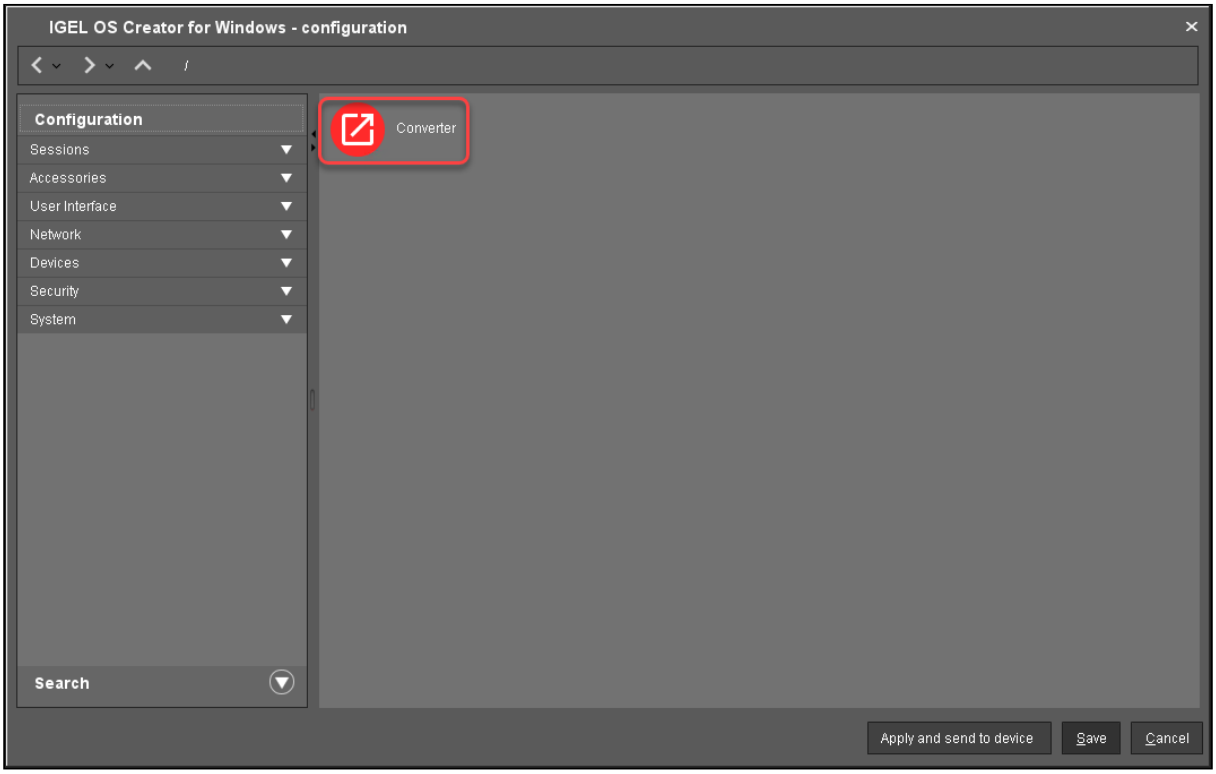
2. In the **New Profile** dialog, change the settings as follows:
   - **Profile Name**: A name for the profile, e. g. "IGEL OS Creator for Windows - configuration"
   - **Based on**: Select "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.



The configuration dialog opens.

4. Click **Converter**.



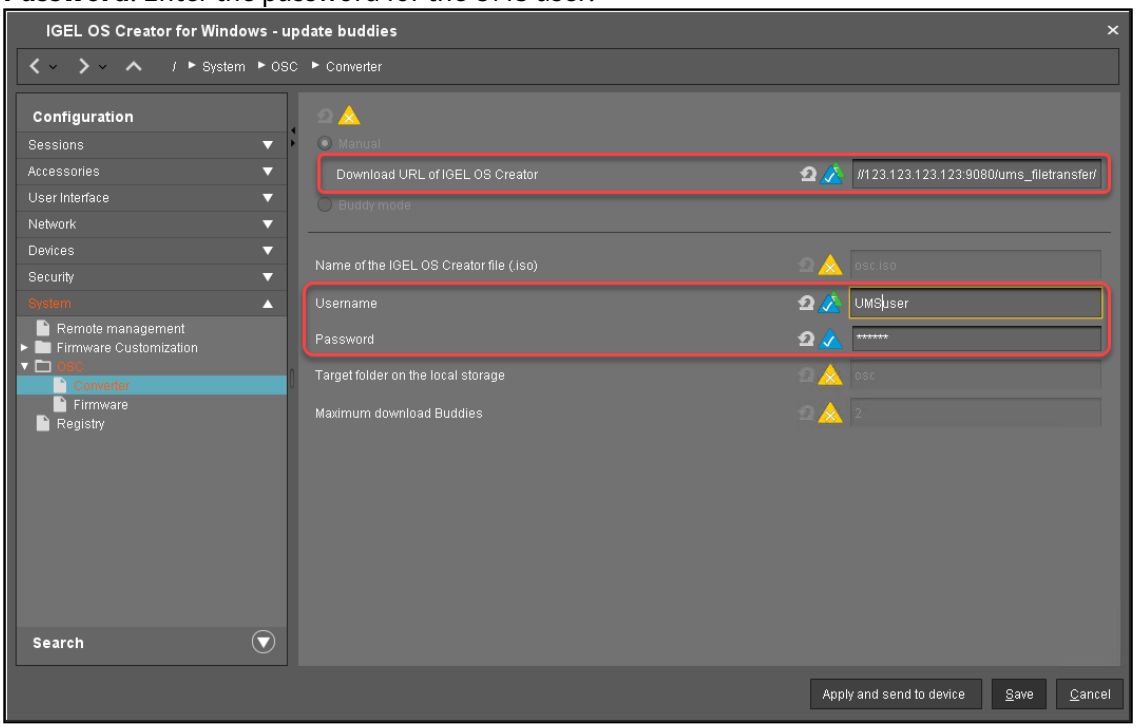
You are taken to **System > OSC > Converter** where you can set all relevant parameters.

5. Change the settings as follows (click the icon to enable the configuration; the icon will change to):
   - **Download URL of IGEL OS Creator**: Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer` / or `http://[IP address of your UMS`

`Server]:9080/ums_filetransfer/`

Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://192.168.178.100:9080/ums_filetransfer/`

- **Username**: Enter the username for the UMS.
- **Password**: Enter the password for the UMS user.

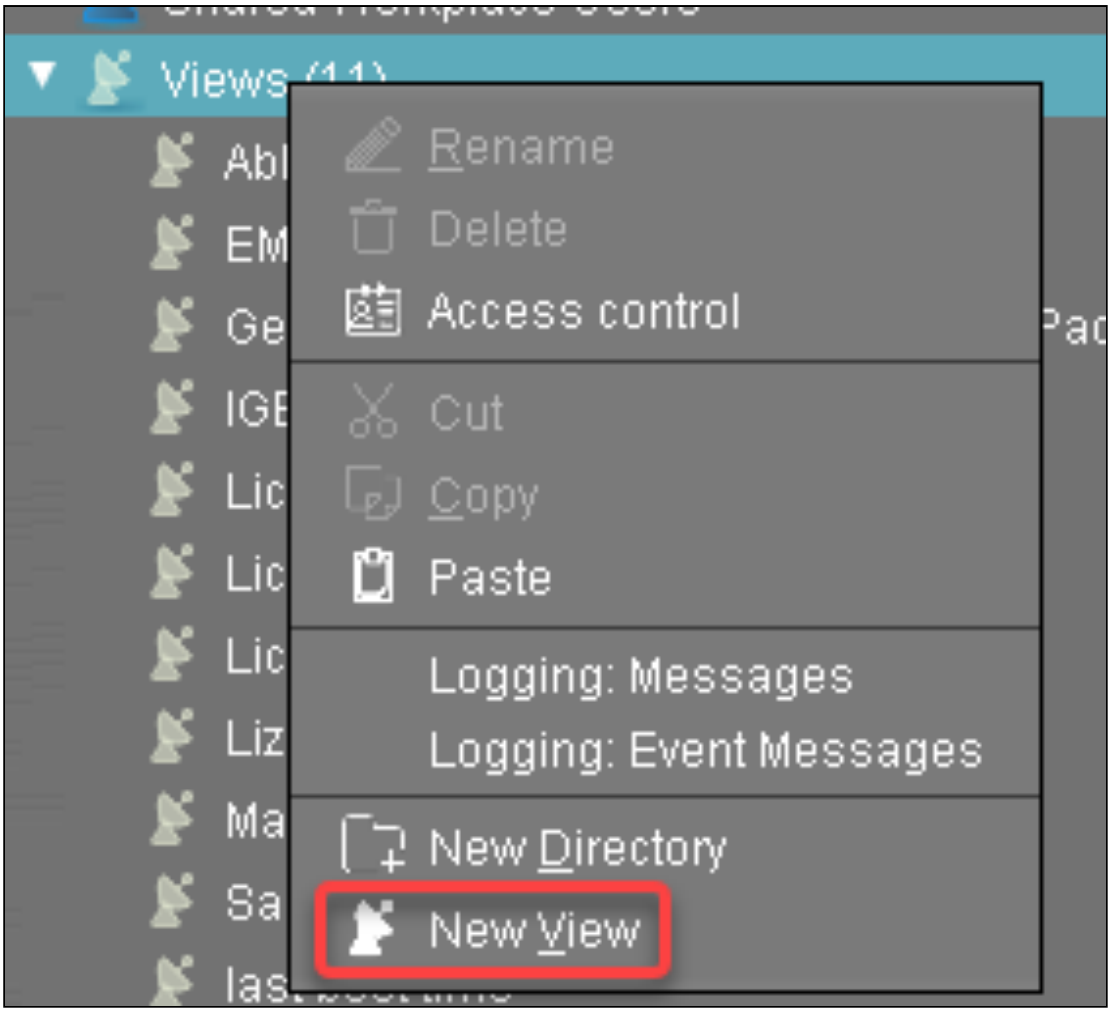


6. Click **Save**.

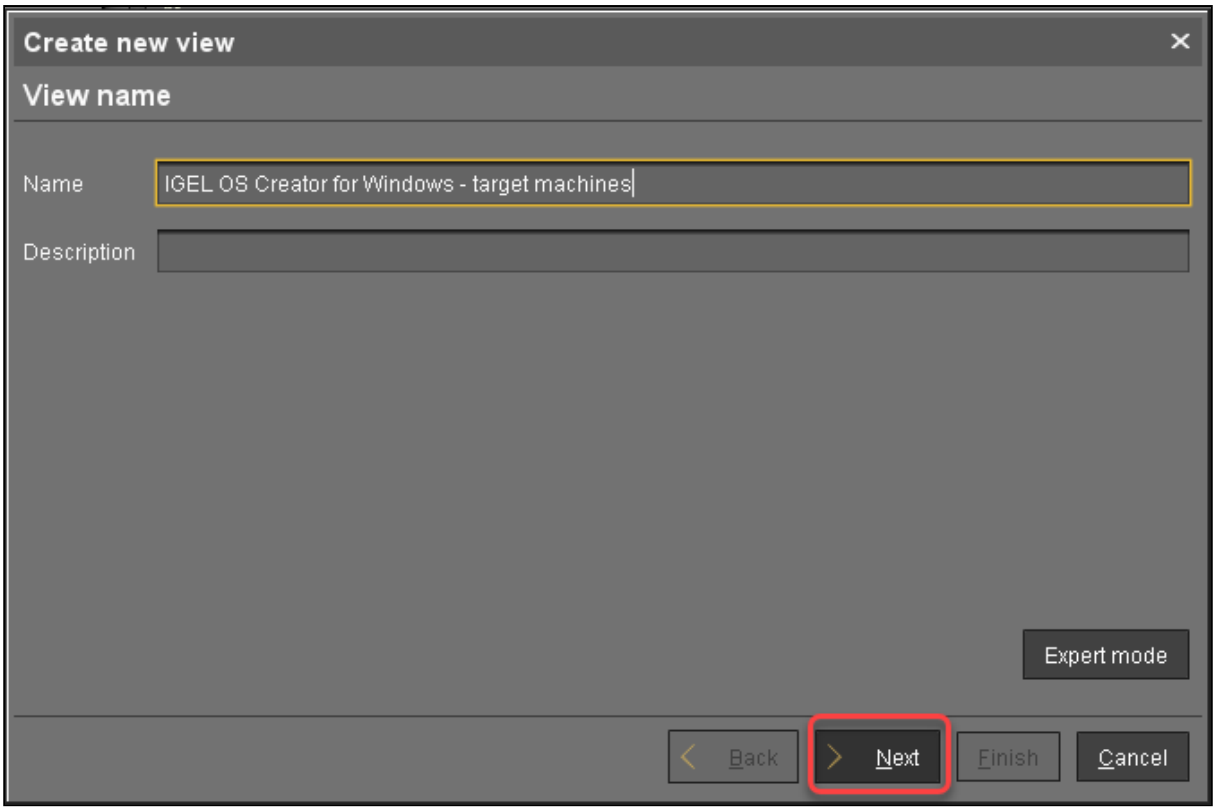
Creating a View to Select All Target Machines

The target machines must be selected in order to assign the profile to them. For the selection, a view will be used.

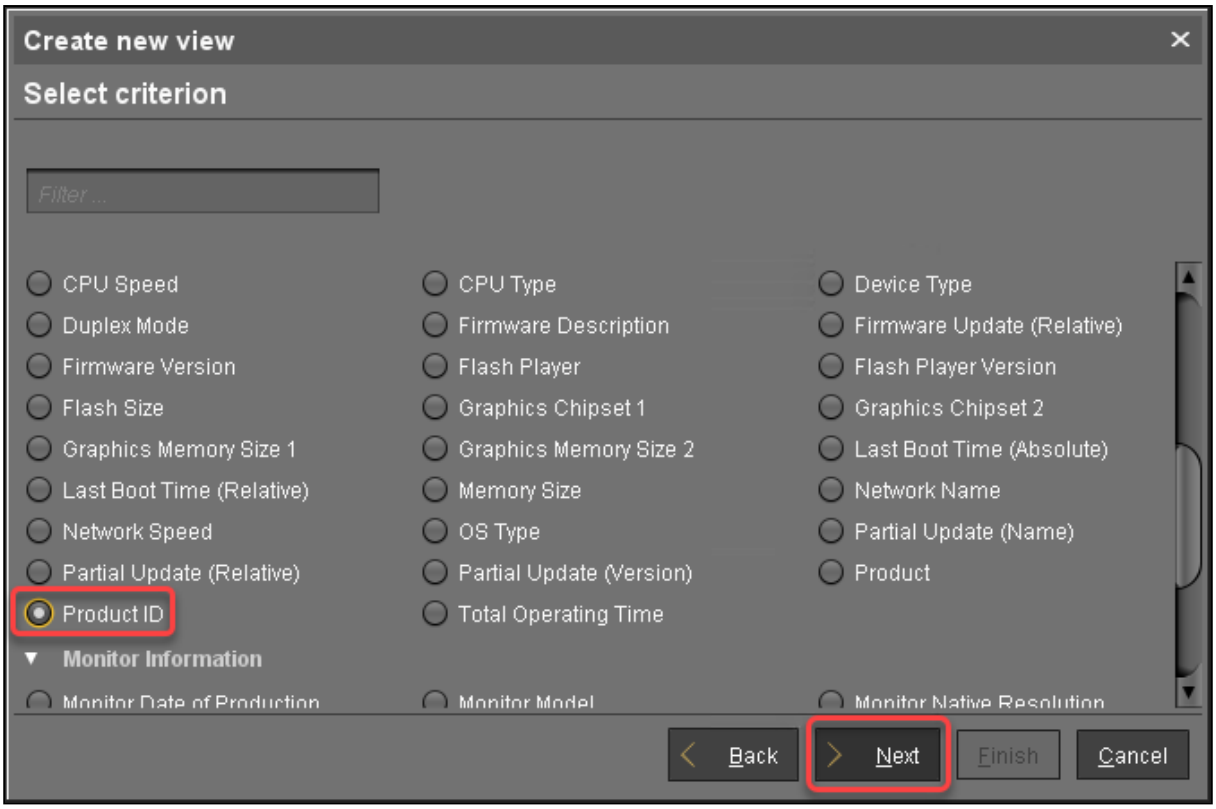
1. In the structure tree of the UMS Console, go to **Views** and select **New View** in the context menu.



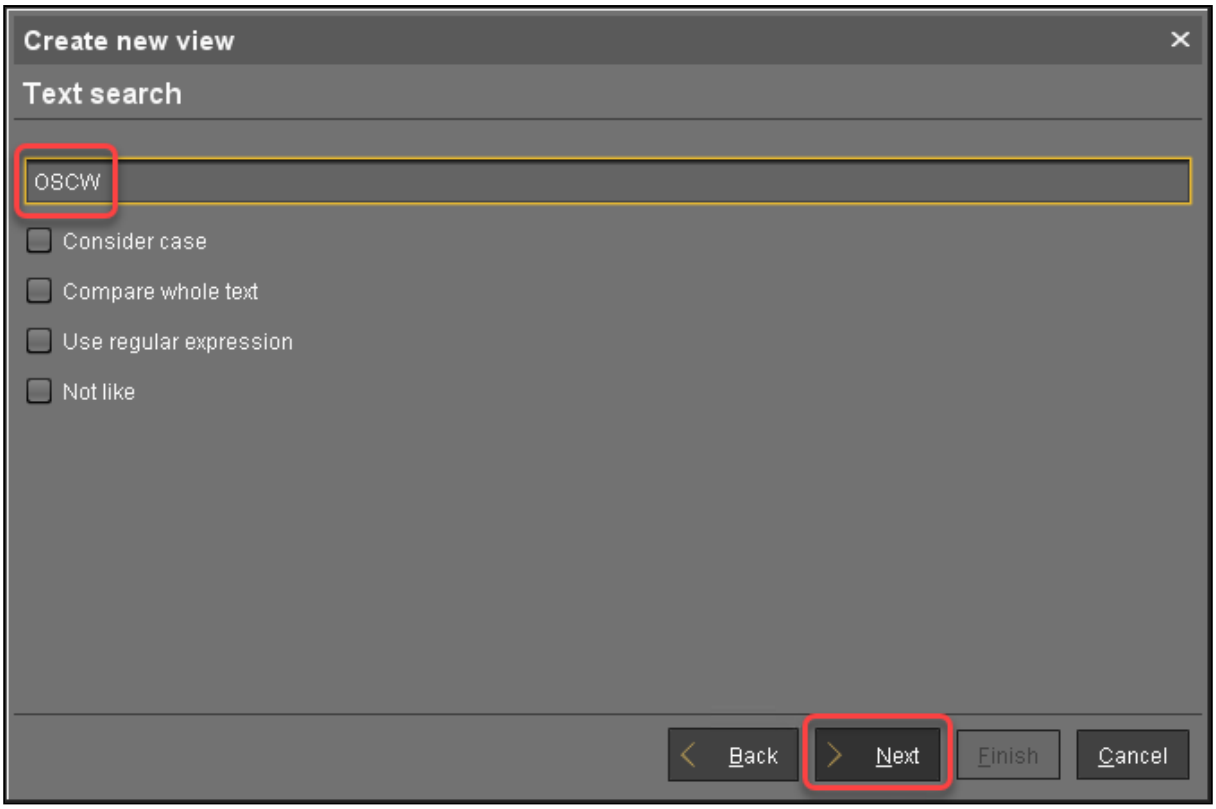
2. Enter a name for the view, e. g. "IGEL OS Creator for Windows - target machines" and click **Next**.



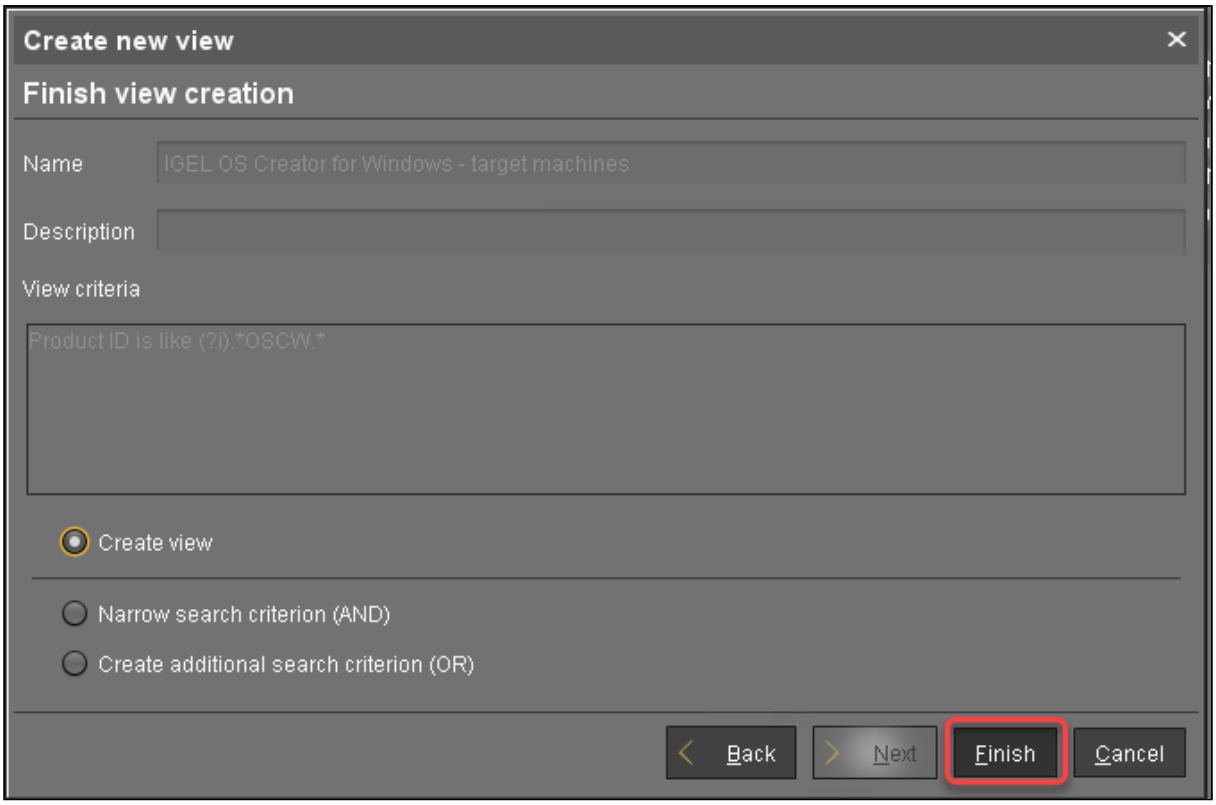
3. On the **Select criterion** page, select **Product ID** and click **Next**.



4. On the **Text search** page, enter "OSCW" and click **Next**.

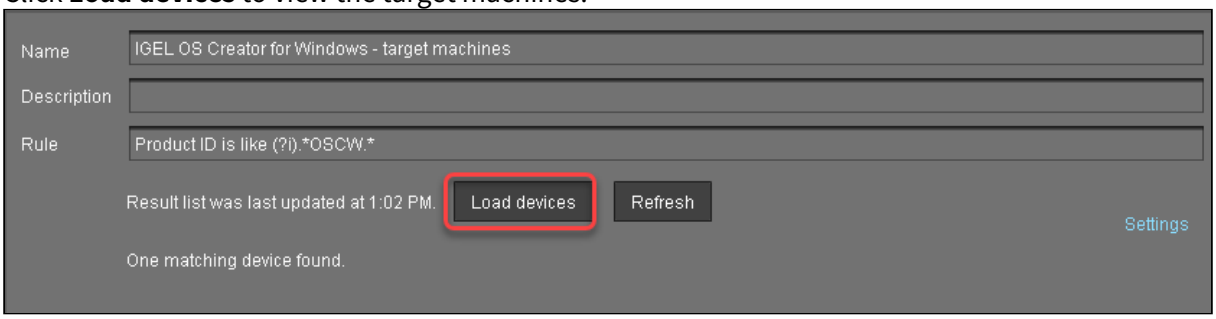


5. On the **Create new view** page, click **Finish**.

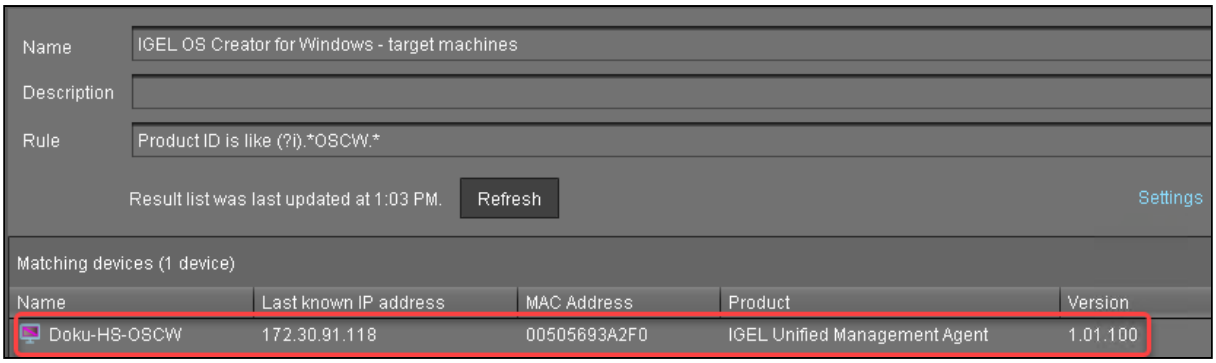


The number of matches is shown.

6. Click **Load devices** to view the target machines.

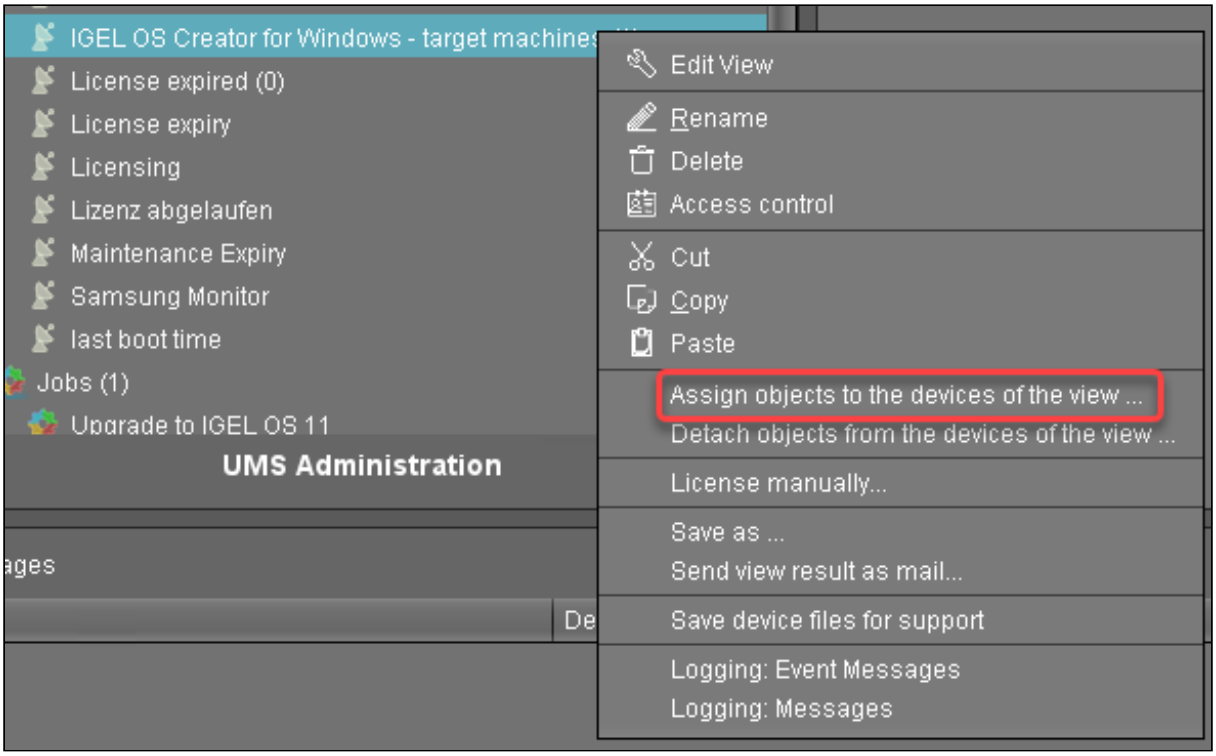


7. The target machines are shown.

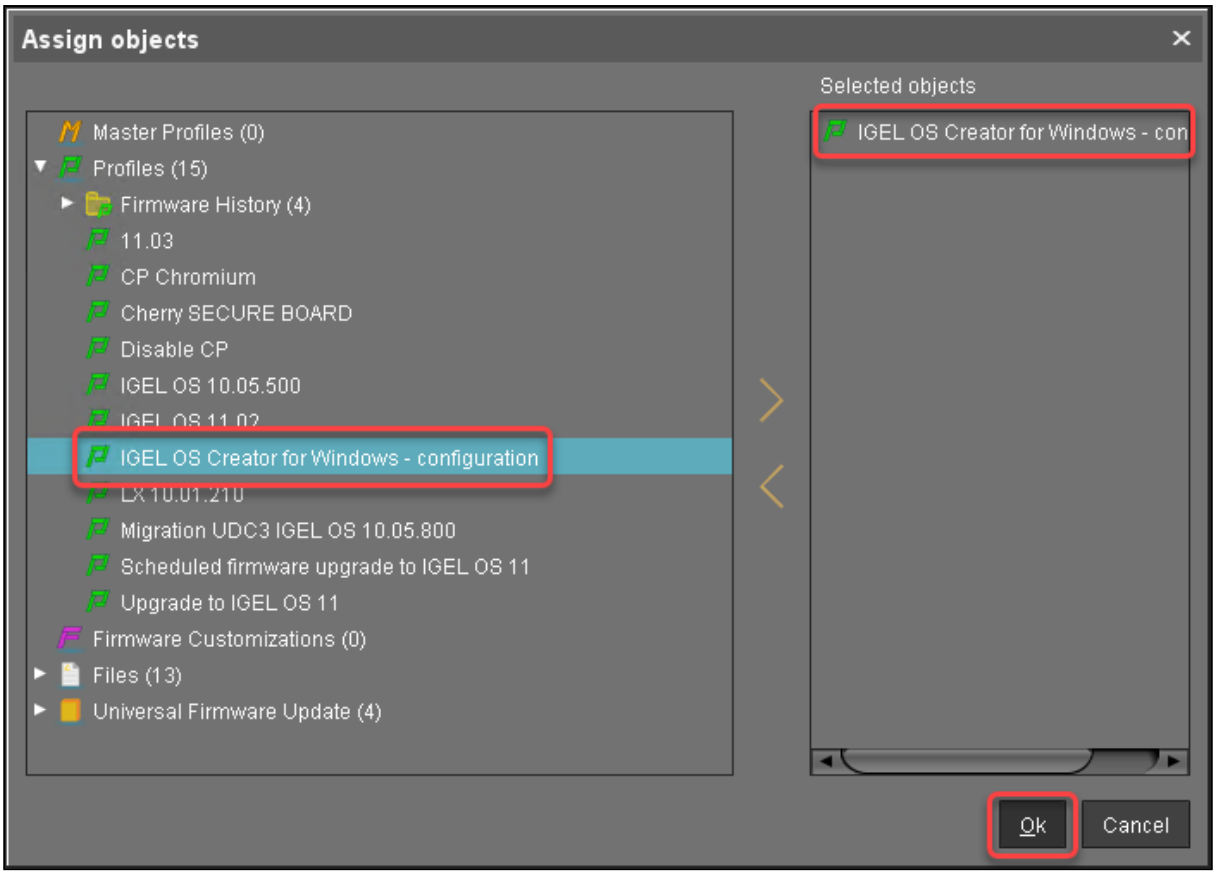


Assigning the Profile to the Target Machines

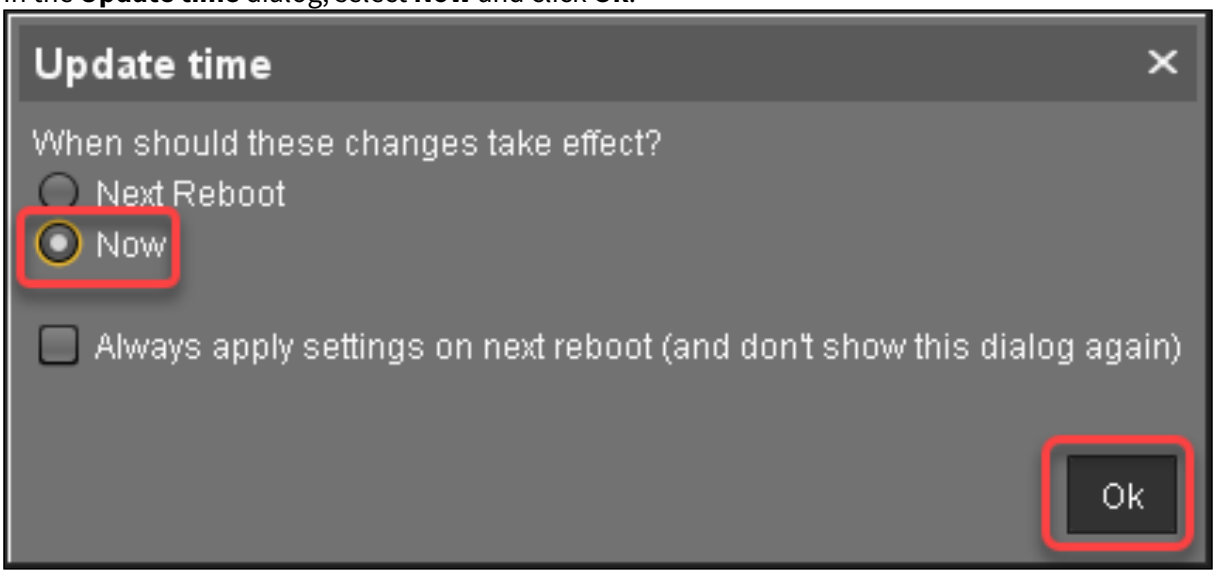
1. Select the view you have created beforehand and select **Assign objects to the devices of the view .....**



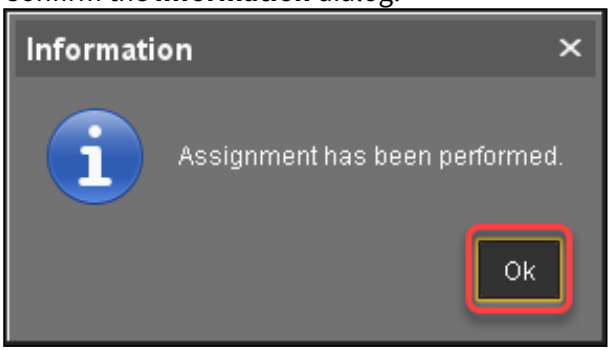
2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.



4. Confirm the **Information** dialog.

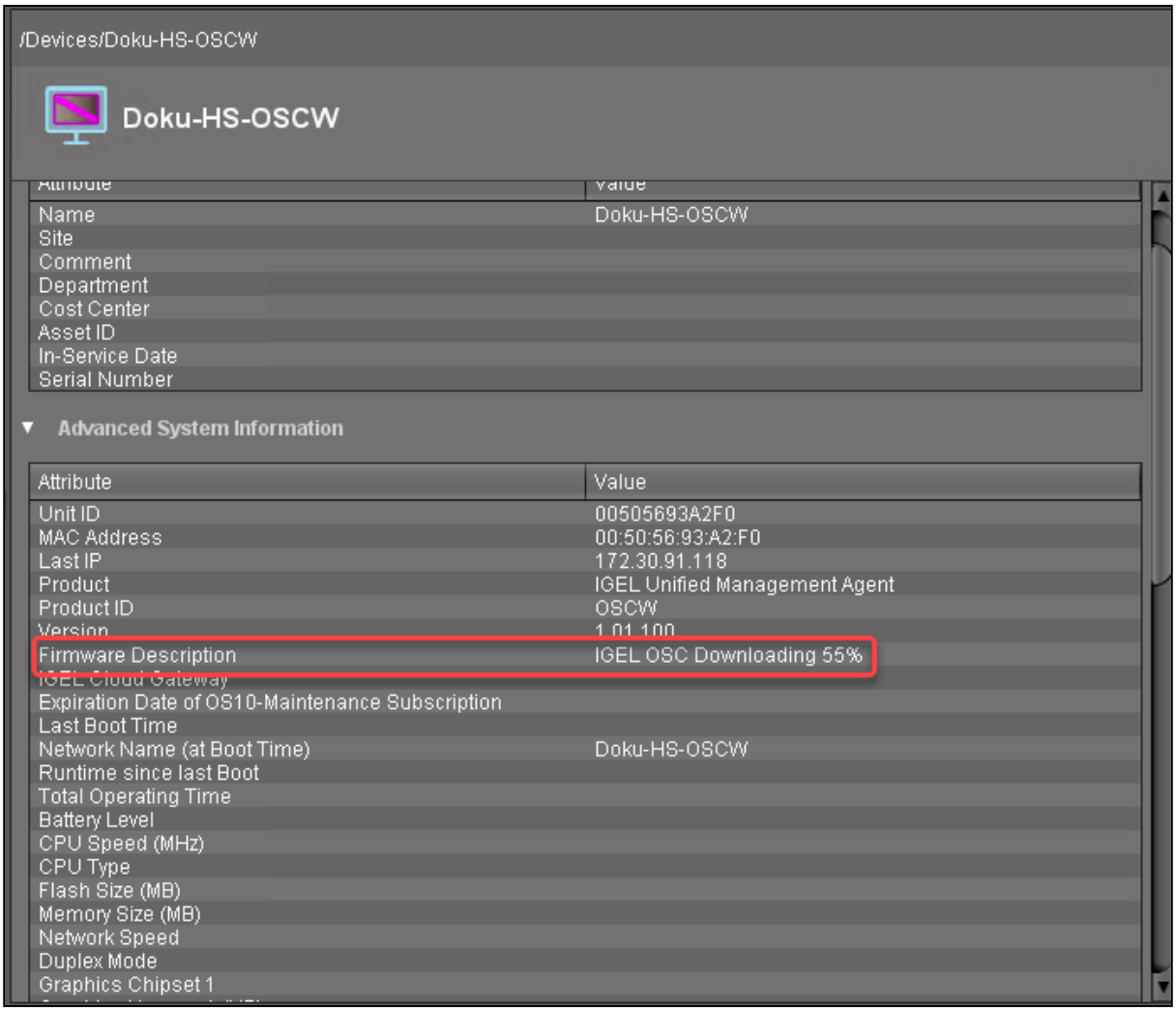


The target machines download the ISO file. This may take a few minutes.

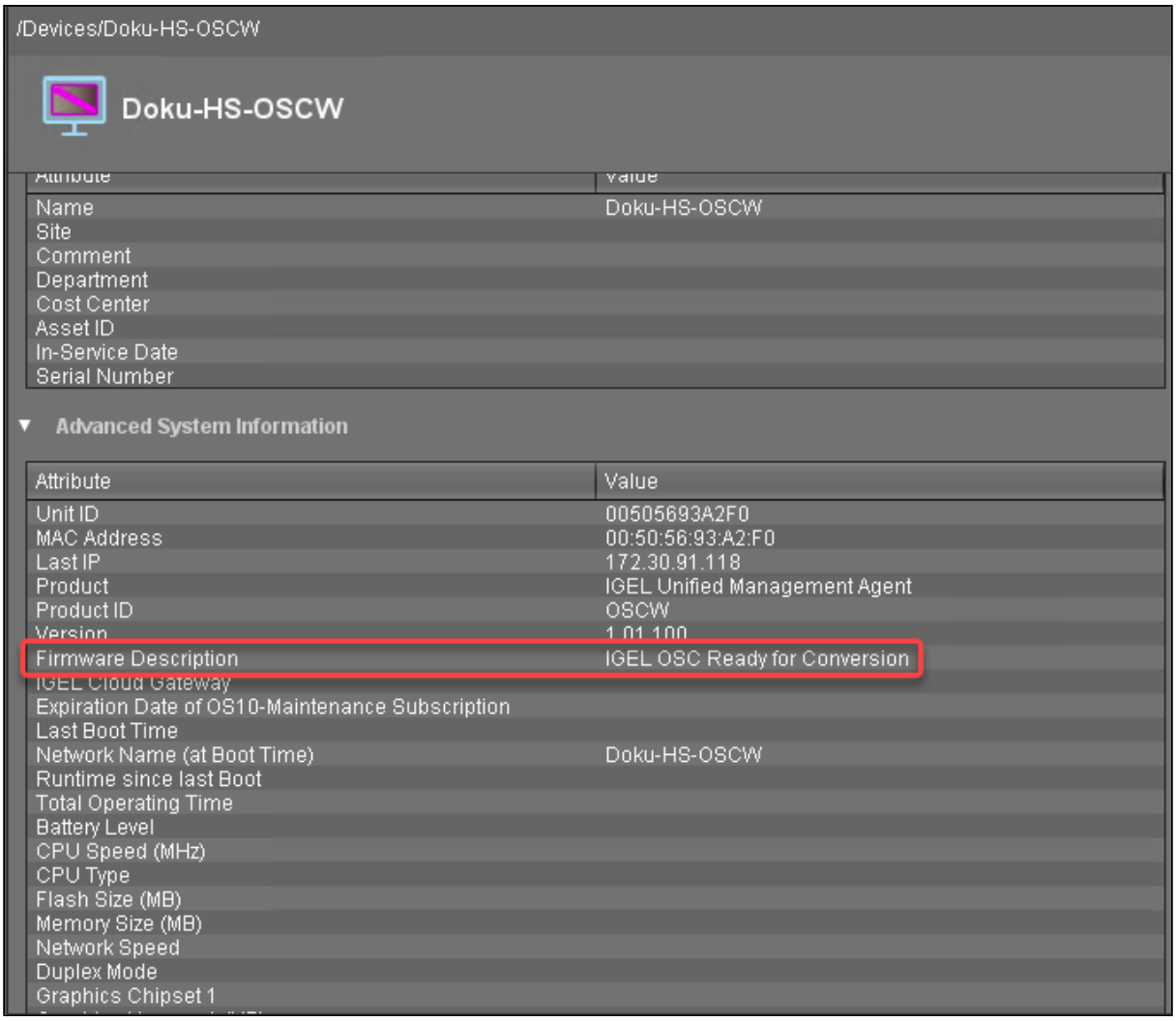
Monitoring the Process

1. In the structure tree of the UMS, open the context menu of one of the target machines and select **Other commands > Refresh system information**.

2. In the dialog, click **Refresh system information** and then from time to time.
In the **Attribute** area, under **Firmware Description**, the current status of the OSC installation is shown.



When a device is ready, the value of **Firmware Description** changes to "IGEL OSC Ready for Conversion".



3. When **Firmware Description** reads "IGEL OSC Ready for Conversion", continue with Starting the Conversion 1 (see page 2242).

Check List

✅ The conversion profile is assigned to all target machines.

✅ All target machines have downloaded the IGEL OS 11 Creator (ISO), which is indicated by the **Firmware Description** "IGEL OS Ready for Conversion".

Next Step

>> Starting the Conversion 1 (see page 2242)

Configuring the OSCW Installer in Buddy Mode

The target machines that are designated as update buddies download the ISO file containing the IGEL OS firmware from the UMS. When they have downloaded the file, the remaining target machines download it from the update buddies.

> ⚠ Make sure that all devices are joined to a Microsoft Active Directory and are accessible by the same AD user with reading permissions.

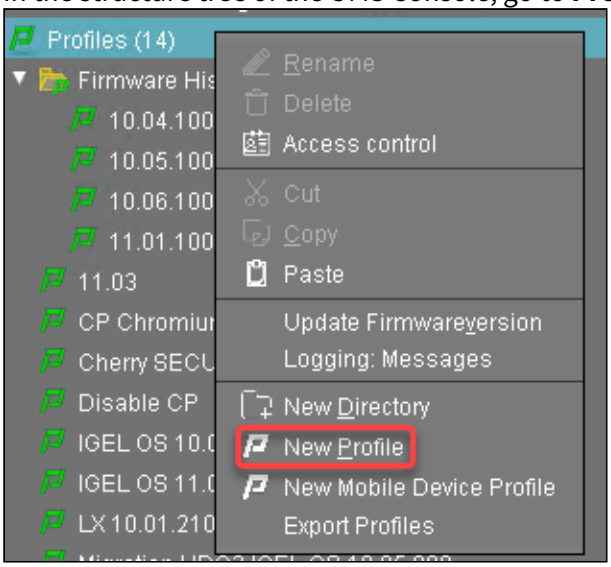
First, we create a profile for the update buddies that provides the OSCW installer with the download source for the ISO file. Then, we will assign this profile to the update buddies; the assignment of the profile triggers the update buddies to download the file. After that, we create a profile for the remaining target machines which configures them to use the update buddies. When the update buddies have downloaded the file, we can assign the profile to the remaining target machines. On assignment, each target machine selects an update buddy automatically and starts downloading the file from it.

The configuration comprises the following steps:

- Creating a Profile for the Update Buddies (see page 2224)
- Assigning the Profile to the Update Buddies (see page 2226)
- Checking if the Update Buddies are ready (see page 2228)
- Creating a Profile for the Remaining Target Machines (see page 2229)
- Creating a View to Select the Target Machines (see page 2232)
- Assigning the Profile to the Target Machines (see page 2237)
- Monitoring the Process (see page 2239)

Creating a Profile for the Update Buddies

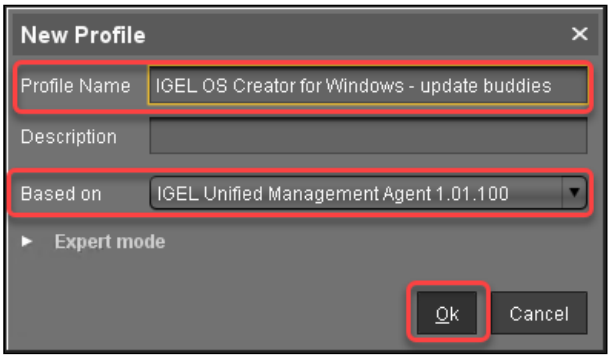
1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



2. In the **New Profile** dialog, change the settings as follows:

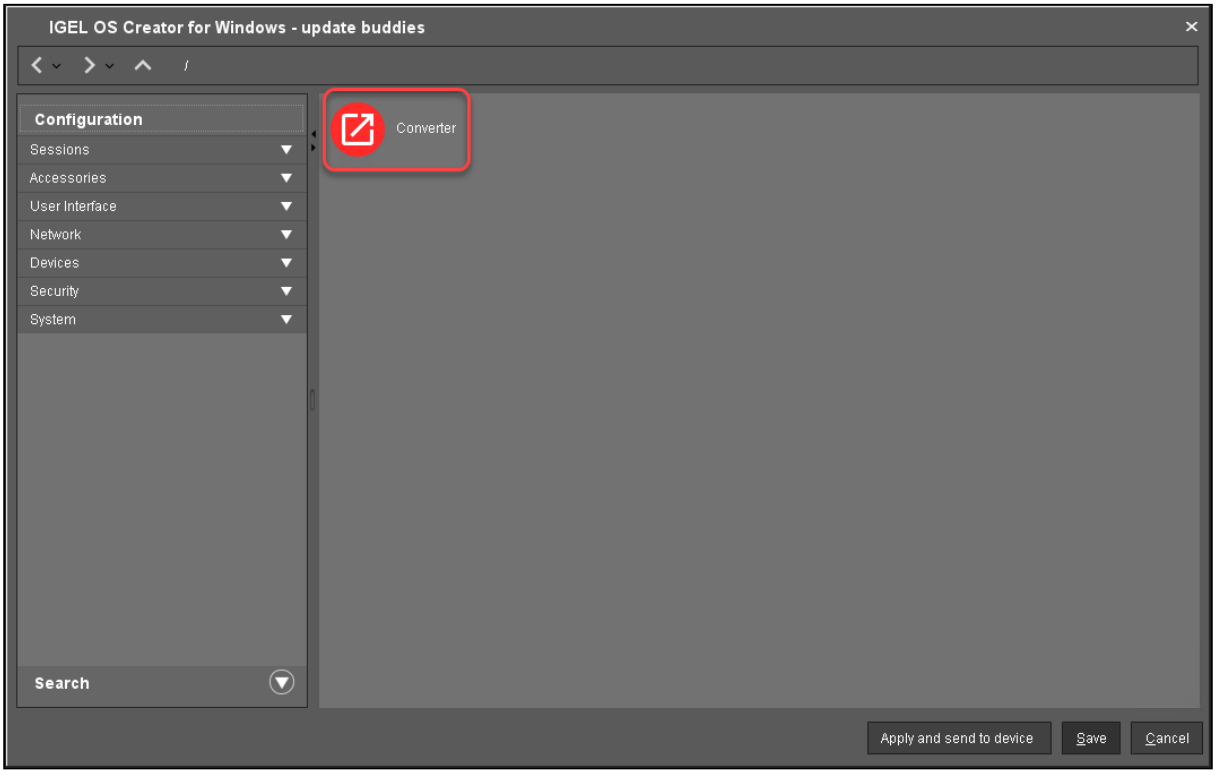
- **Profile Name**: A name for the profile, e. g. "IGEL OS Creator for Windows - update buddies"
- **Based on**: Select "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.



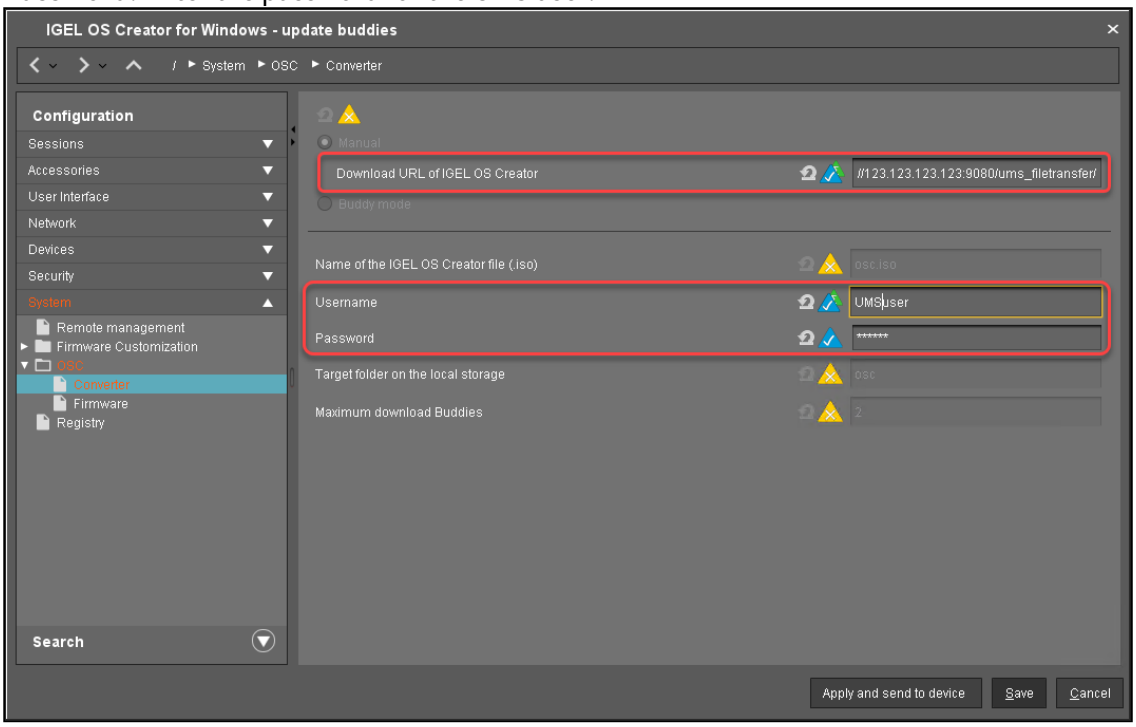
The configuration dialog opens.

4. Click **Converter**.



You are taken to **System > OSC > Converter** where you can set all relevant parameters.

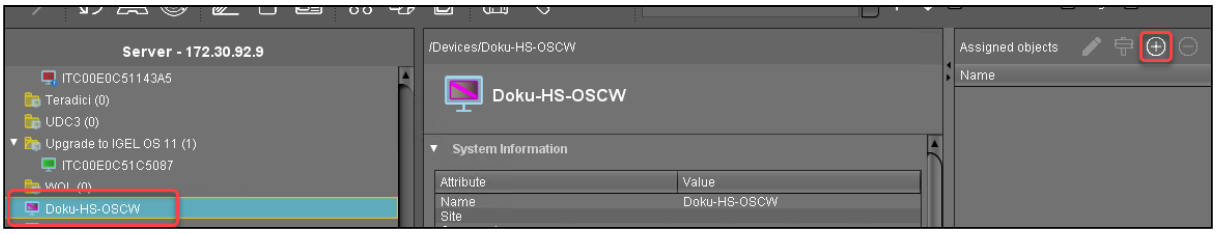
5. Change the settings as follows (click the icon to enable the configuration; the icon will change to):
   - **Download URL of IGEL OS Creator**: Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer/` or `http://[IP address of your UMS Server]:9080/ums_filetransfer/`
     Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://192.168.178.100:9080/ums_filetransfer/`
   - **Username**: Enter the username for the UMS.
   - **Password**: Enter the password for the UMS user.



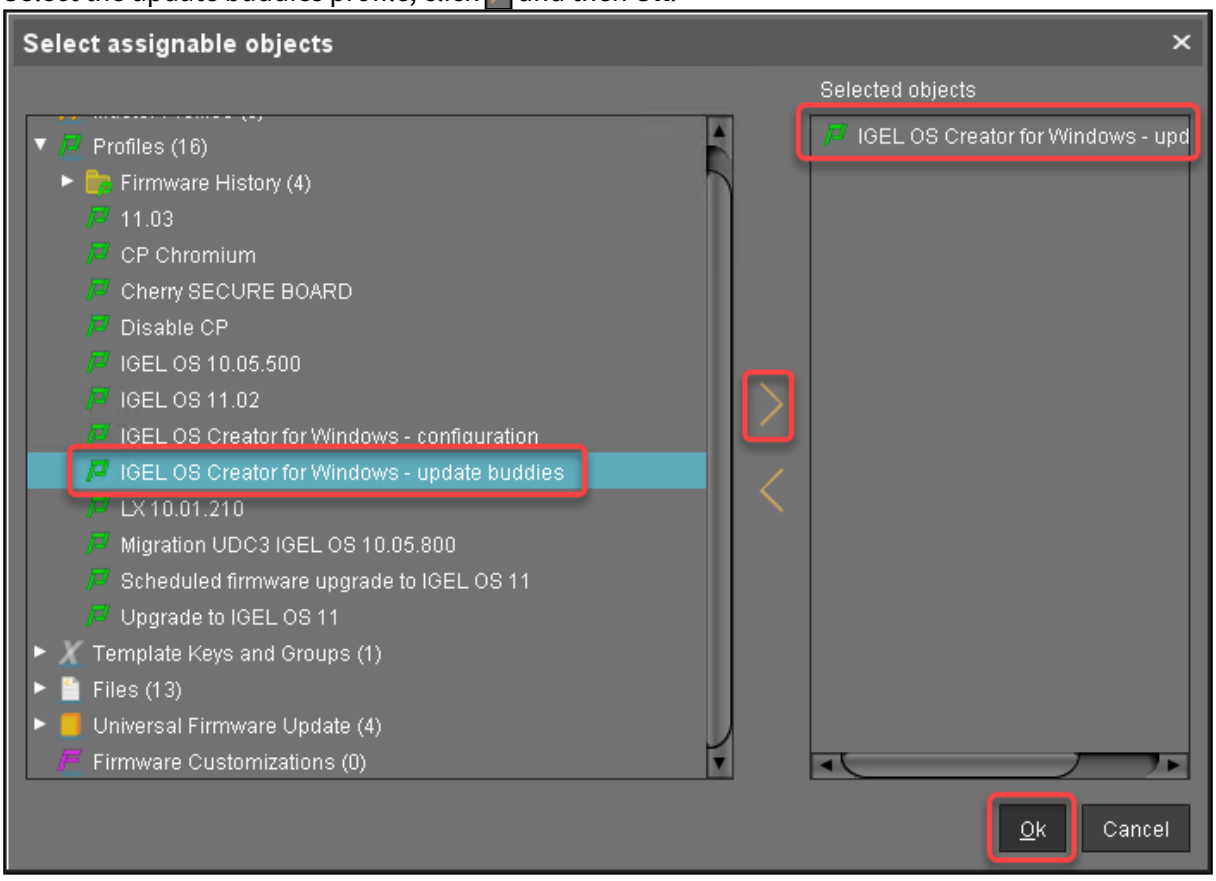
6. Click **Save**.

Assigning the Profile to the Update Buddies

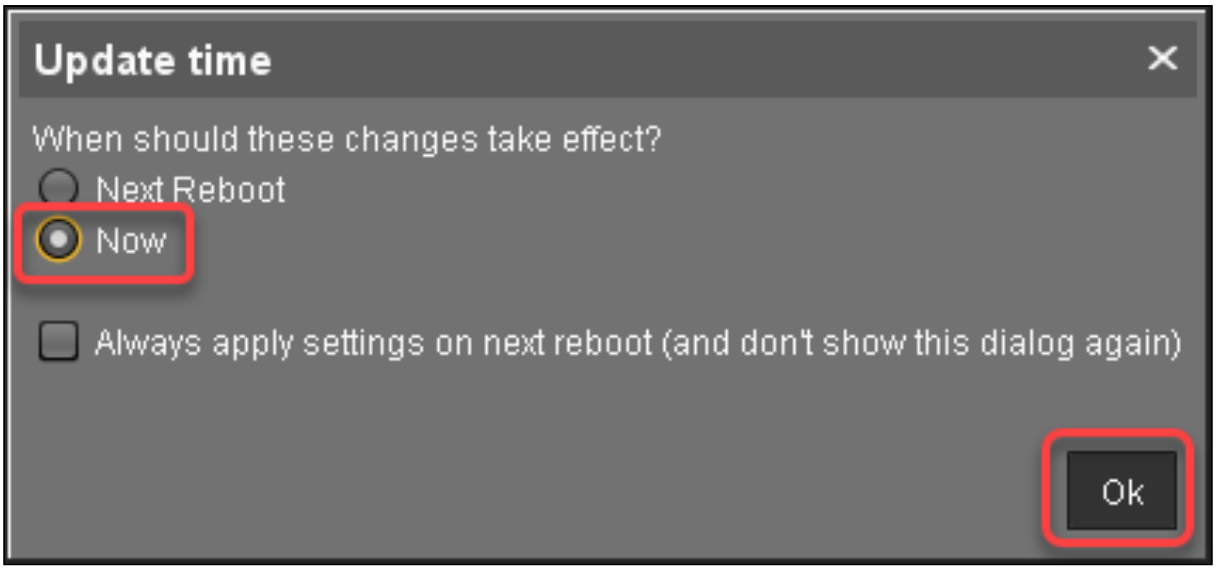
1. In the structure tree of the UMS console, select the machines that will serve as update buddies and click in the **Assigned objects** area.



2. Select the update buddies profile, click and then **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.

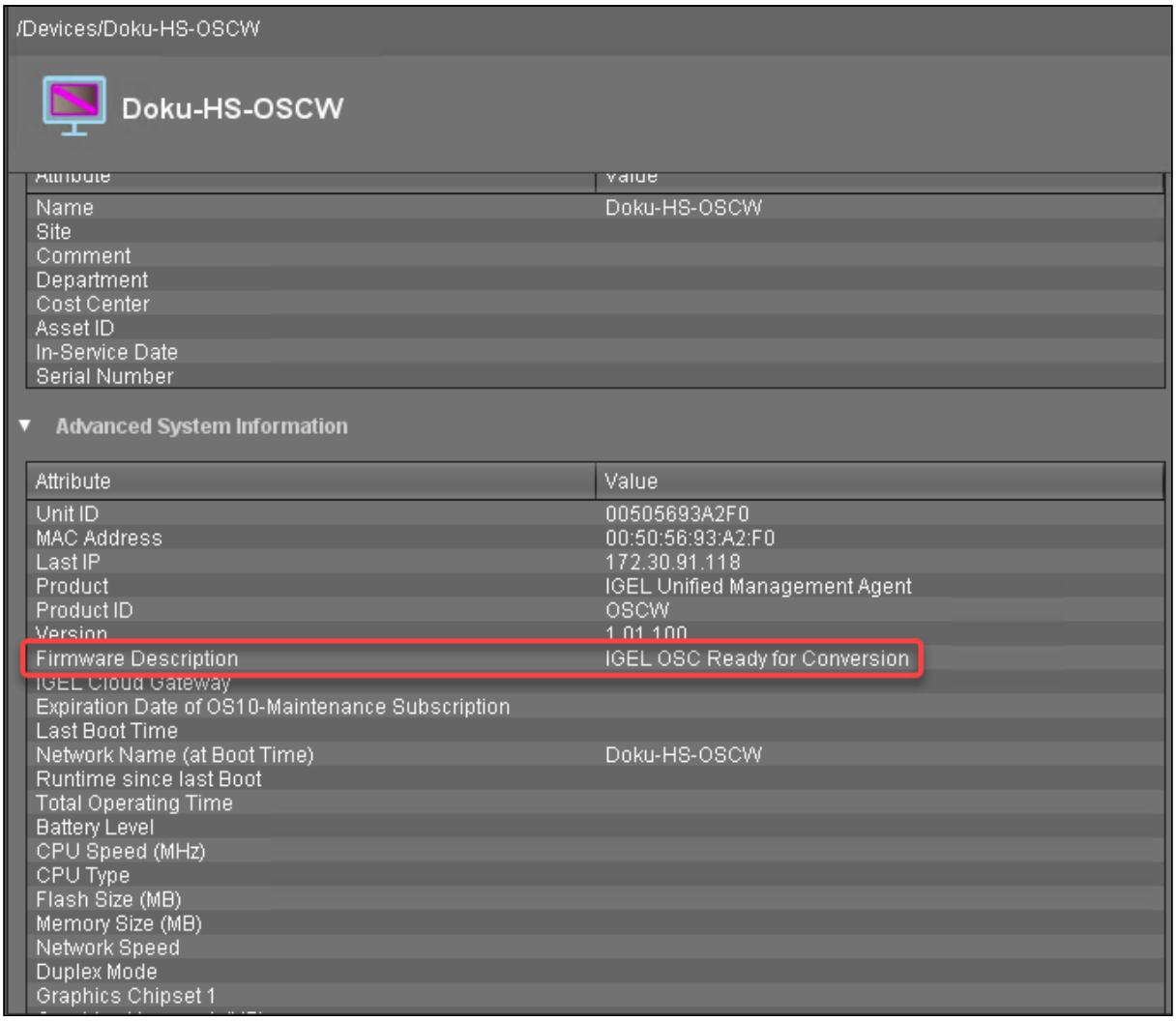


Checking If the Update Buddies Are Ready

Perform the following check for each update buddy:

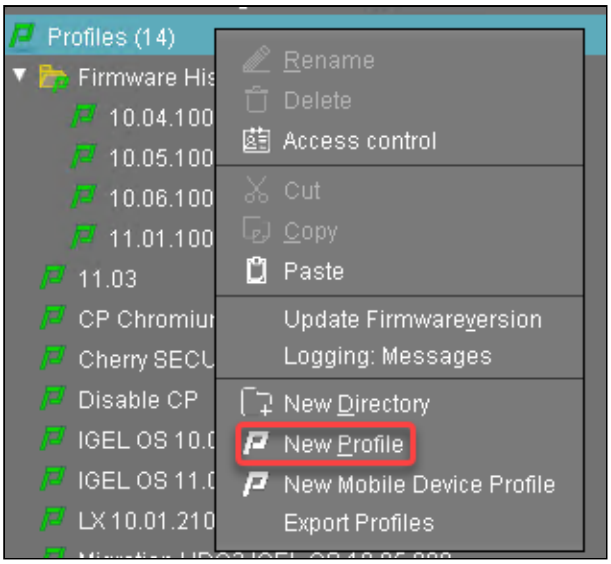
1. In the structure tree of the UMS, open the context menu of the update buddy and select **Other commands > Refresh system information**.

2. In the dialog, click **Refresh system information** and then every few seconds.
   In the **Attribute** area, under **Firmware Description**, the current status of the download is shown.
   When it reads "IGEL OSC Ready for Conversion", the update buddy is ready for use.



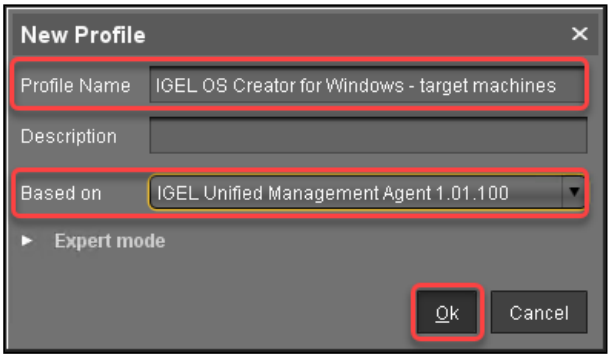
Creating a Profile for the Remaining Target Machines

1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



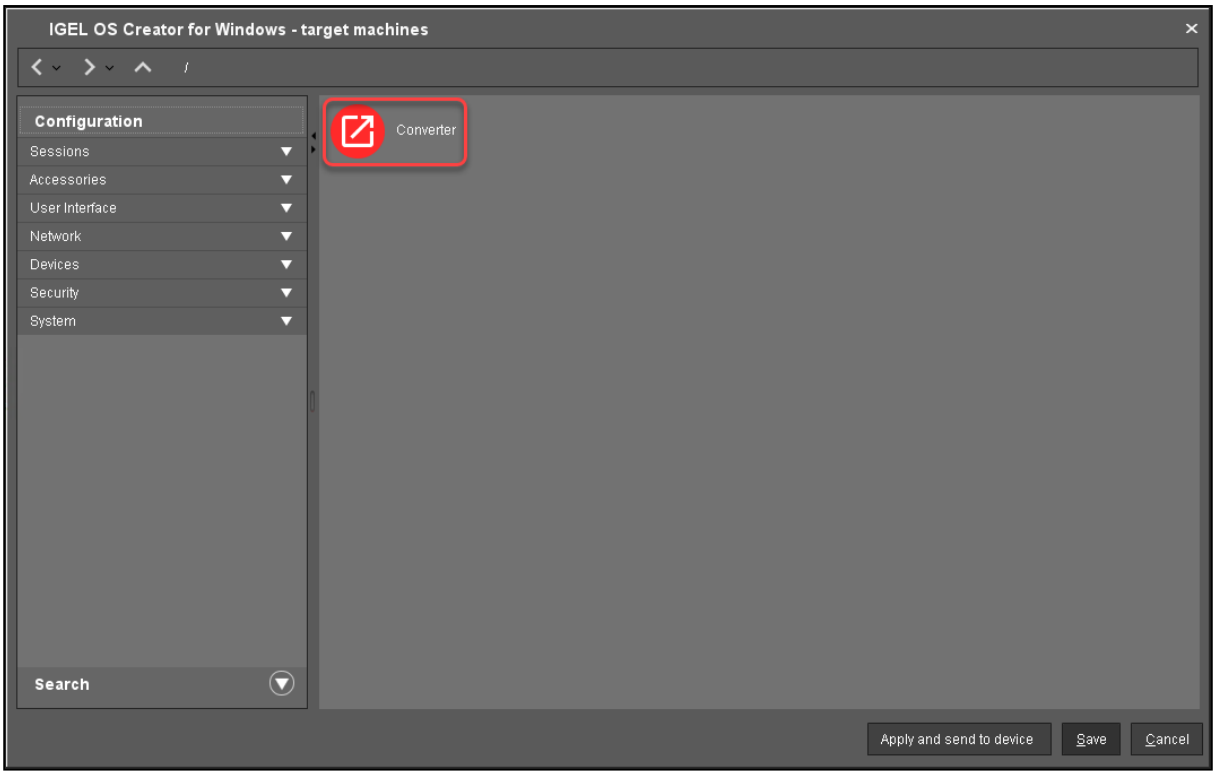
2. In the **New Profile** dialog, change the settings as follows:
   - **Profile Name**: A name for the profile, e. g. "IGEL OS Creator for Windows - target machines"
   - **Based on**: Select "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.



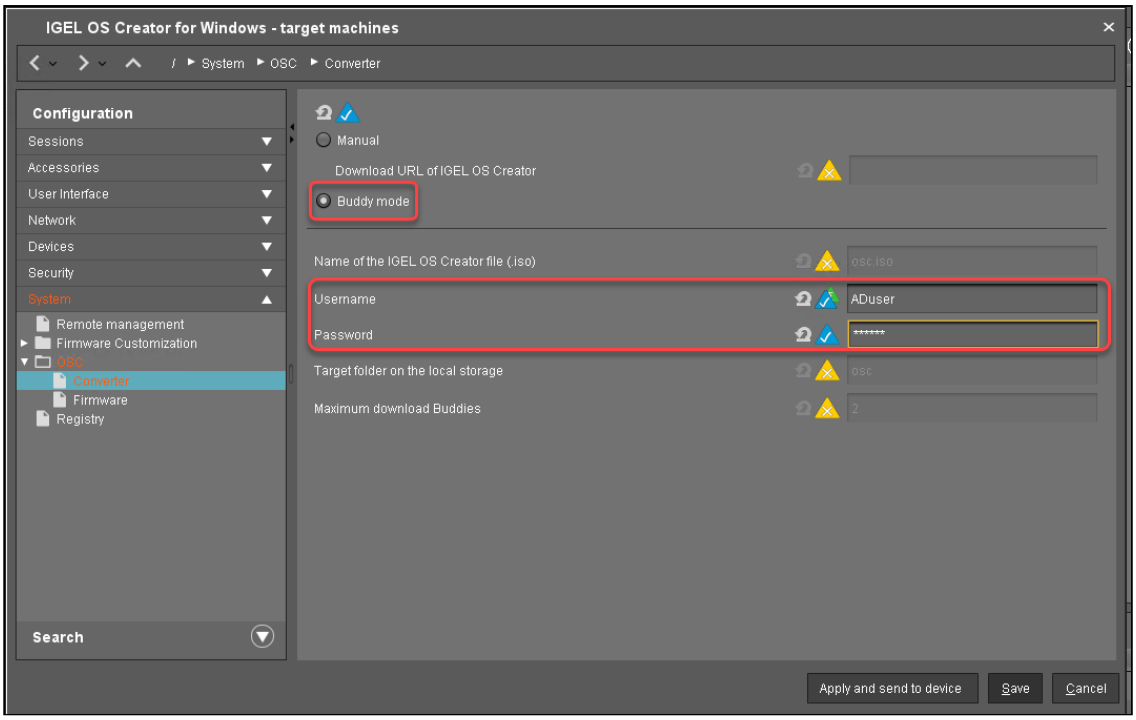
The configuration dialog opens.

4. Click **Converter**.



You are taken to **System > OSC > Converter** where you can set all relevant parameters.

5. Change the settings as follows (click the icon to enable the configuration; the icon will change to):
   - Select **Buddy Mode**.
   - **Username**: Common username in Microsoft Active Directory for all target machines, including the update buddies.
   - **Password**: Common password associated with the **Username**.

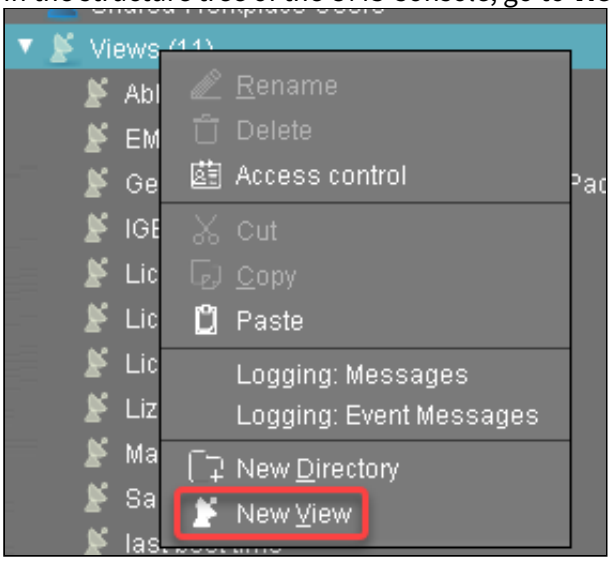


6. Click **Save**.

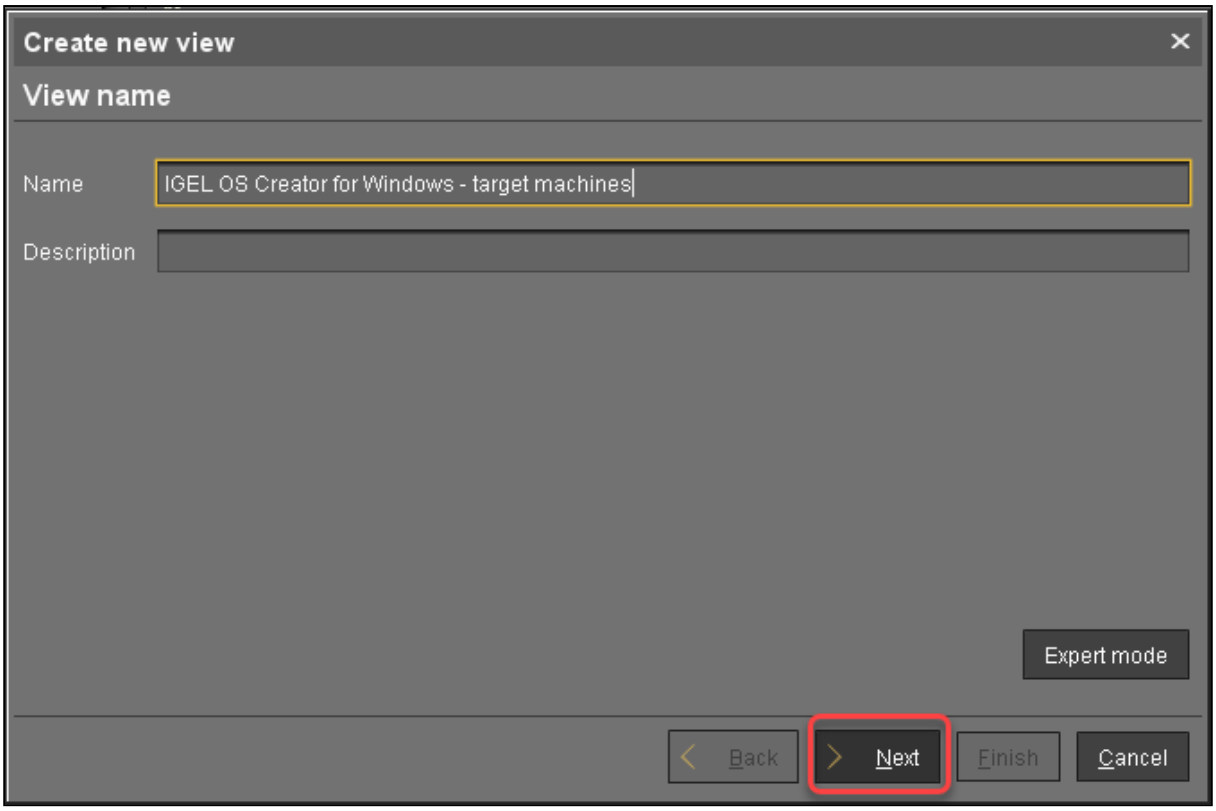
Creating a View to Select the Target Machines

The target machines must be selected in order to assign the profile to them. For the selection, a view will be used.

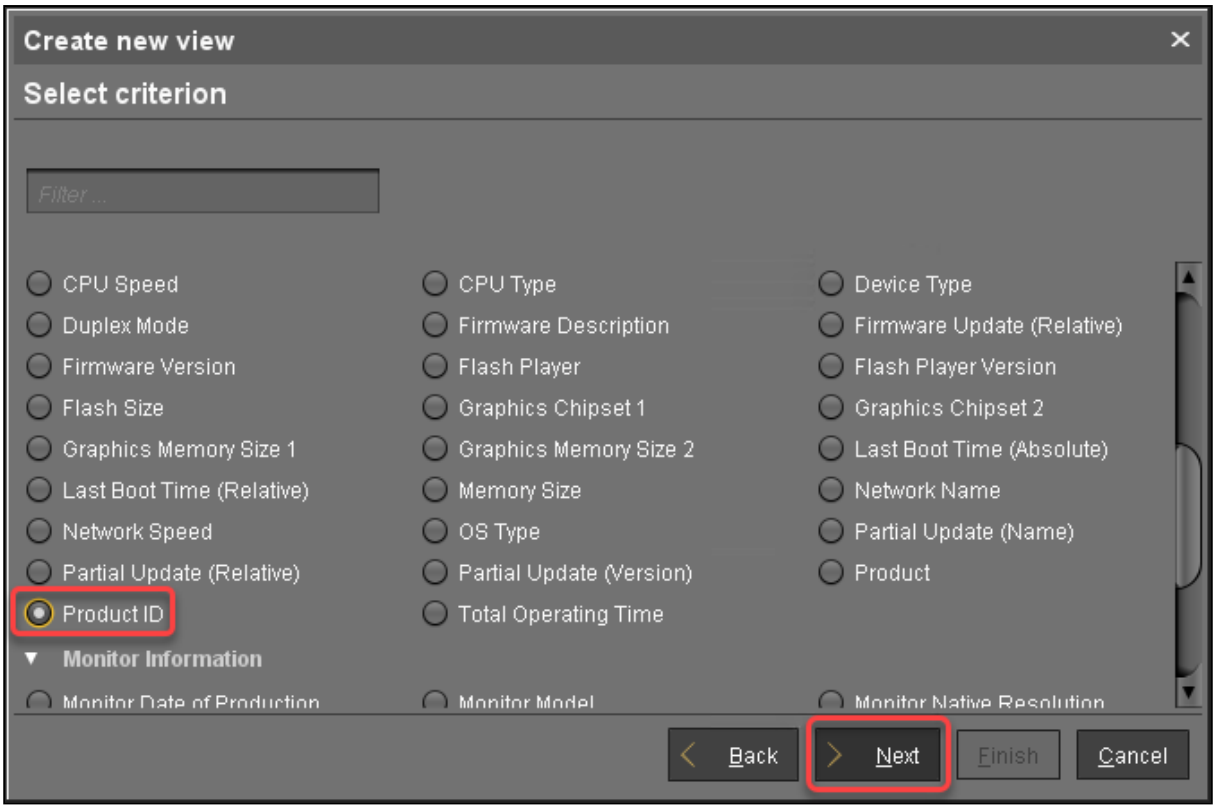
1. In the structure tree of the UMS Console, go to **Views** and select **New View** in the context menu.



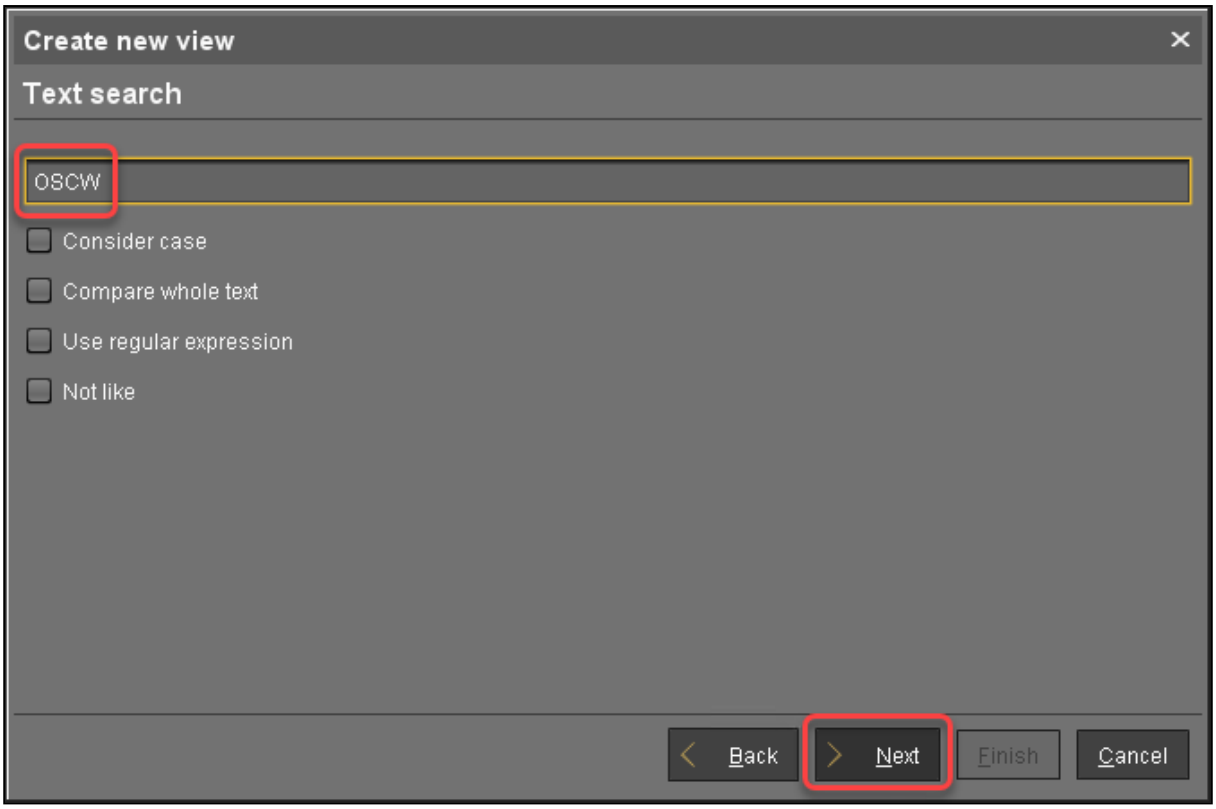
2. Enter a name for the view, e. g. "IGEL OS Creator for Windows - target machines" and click **Next**.



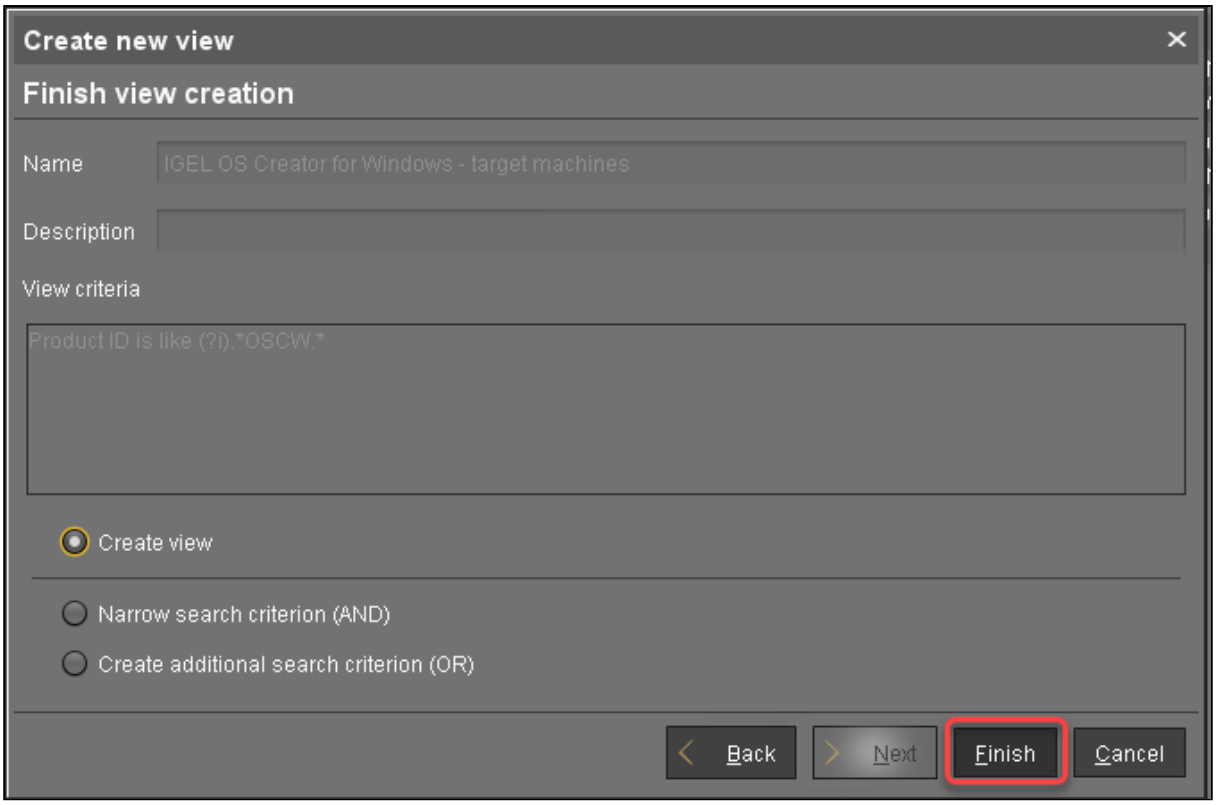
3. On the **Select criterion** page, select **Product ID** and click **Next**.



4. On the **Text search** page, enter "OSCW" and click **Next**.

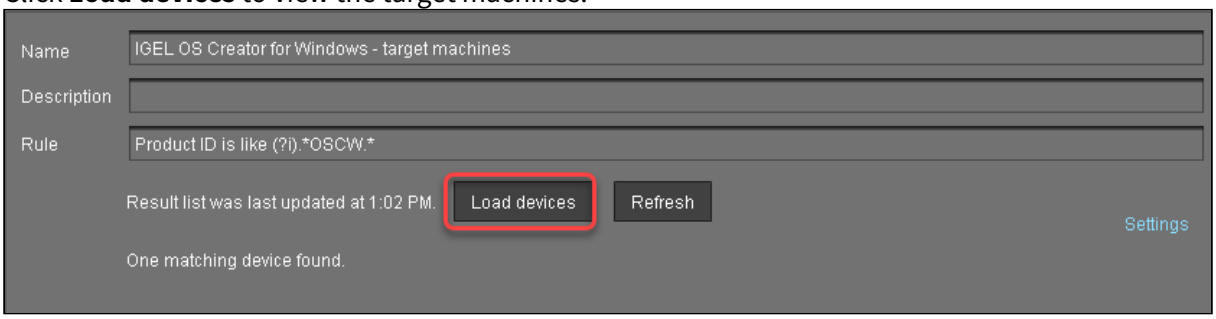


5. On the **Create new view** page, click **Finish**.

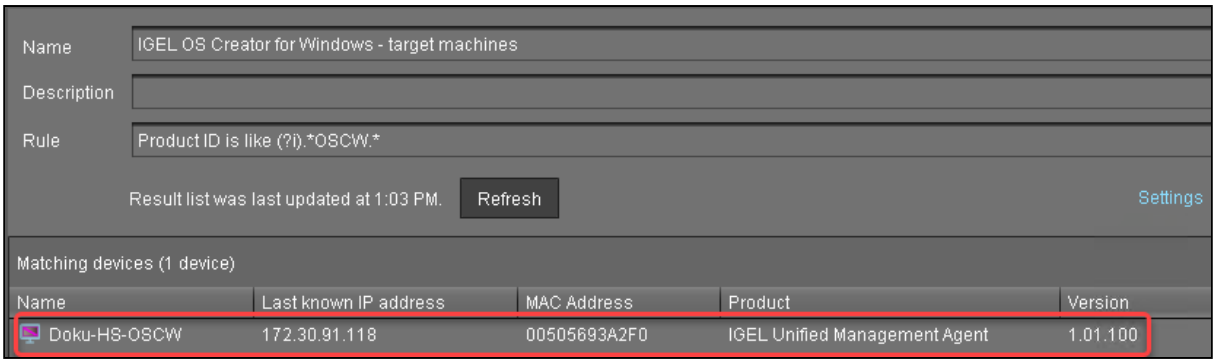


The number of matches is shown.

6. Click **Load devices** to view the target machines.

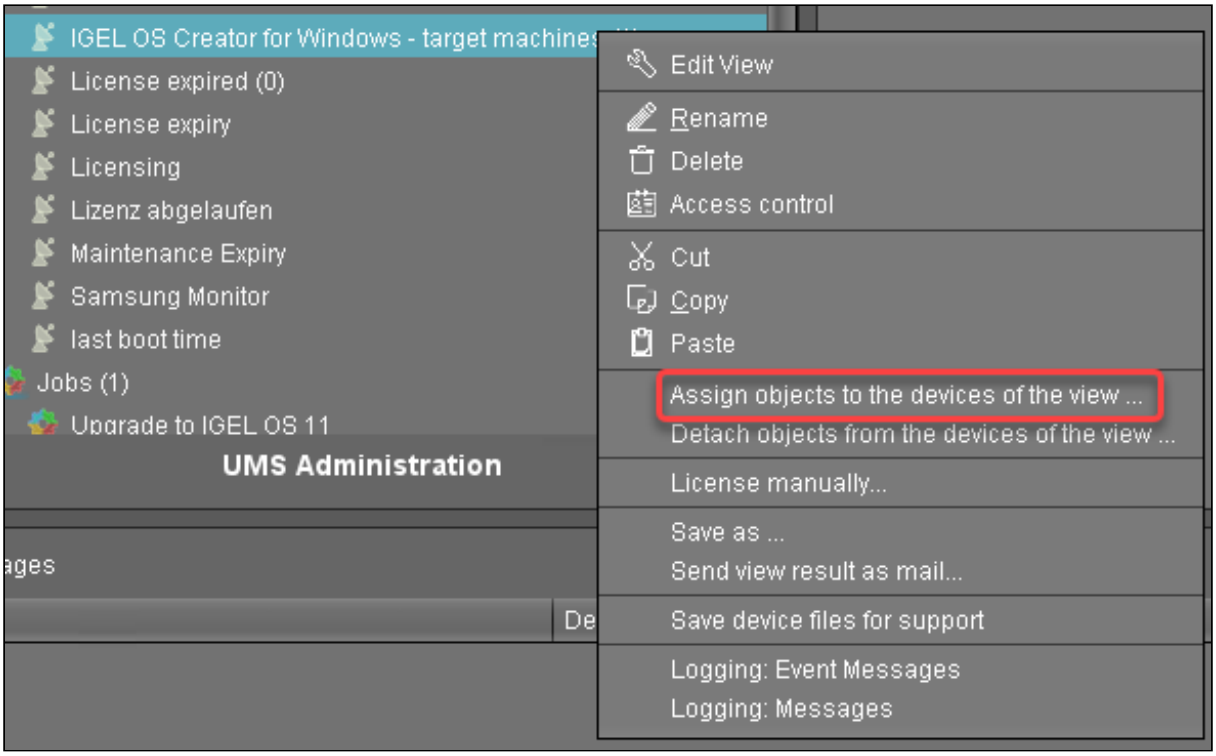


7. The target machines are shown.

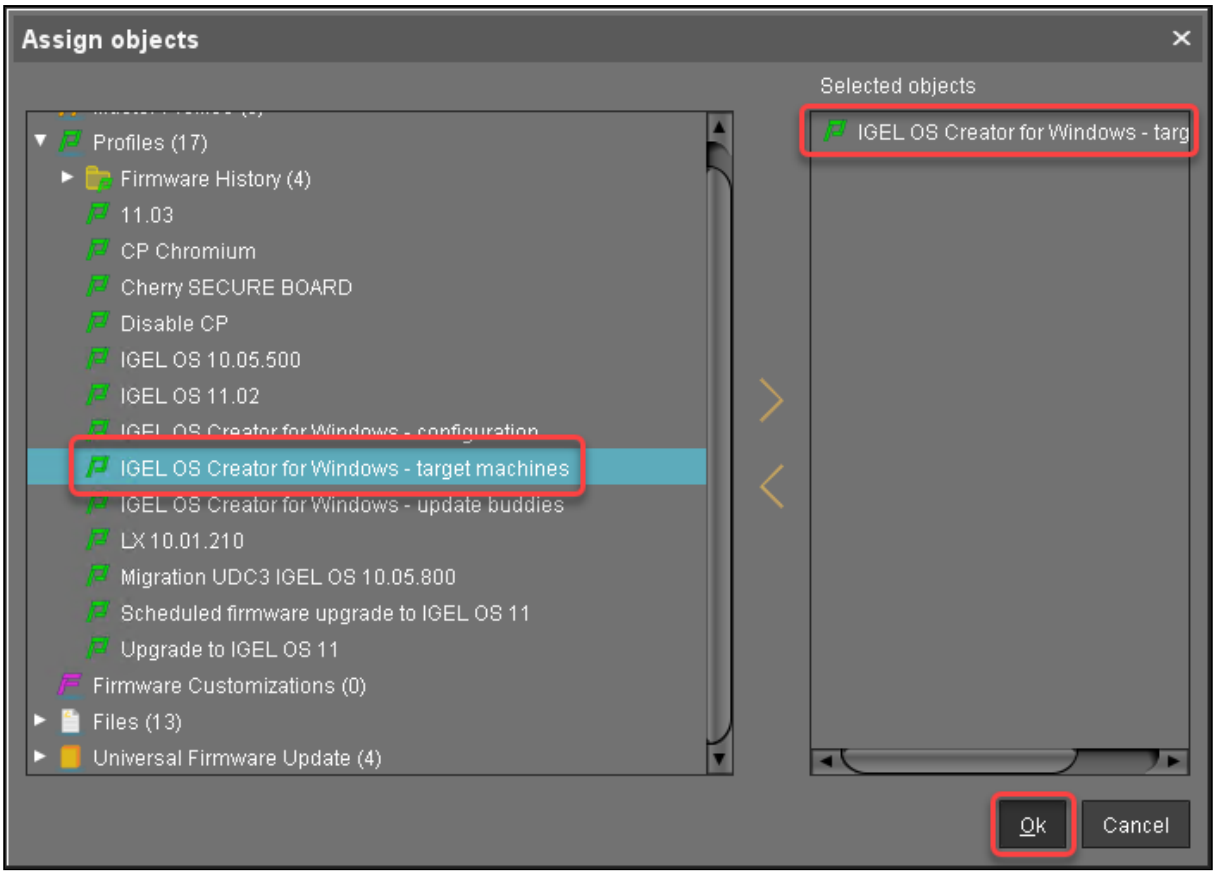


Assigning the Profile to the Target Machines

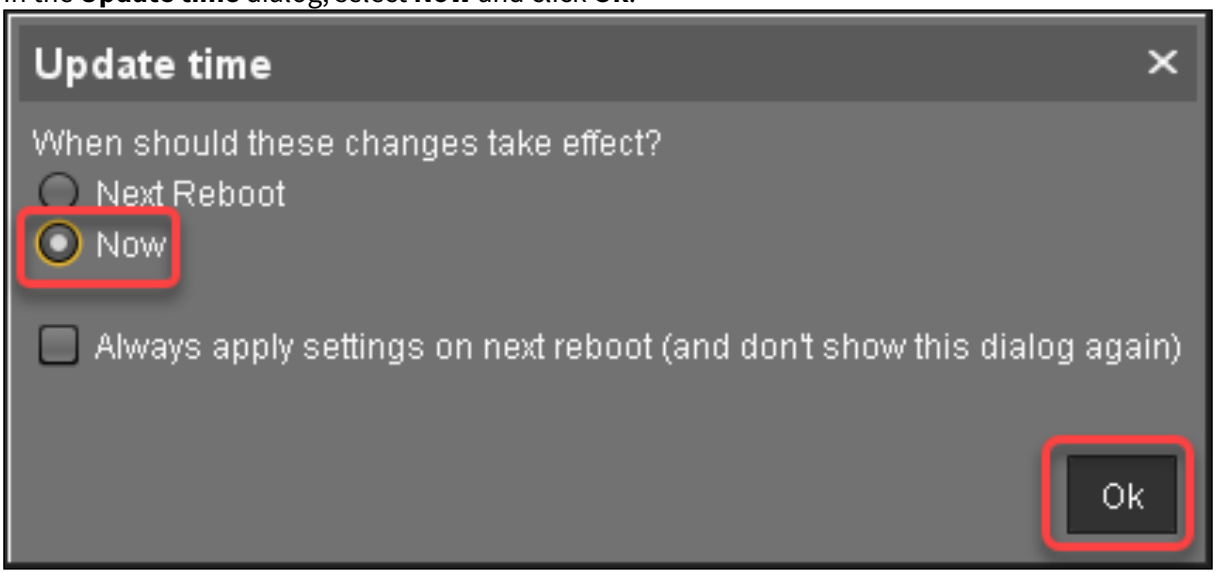
1. Select the view you have created beforehand and select **Assign objects to the devices of the view .....**



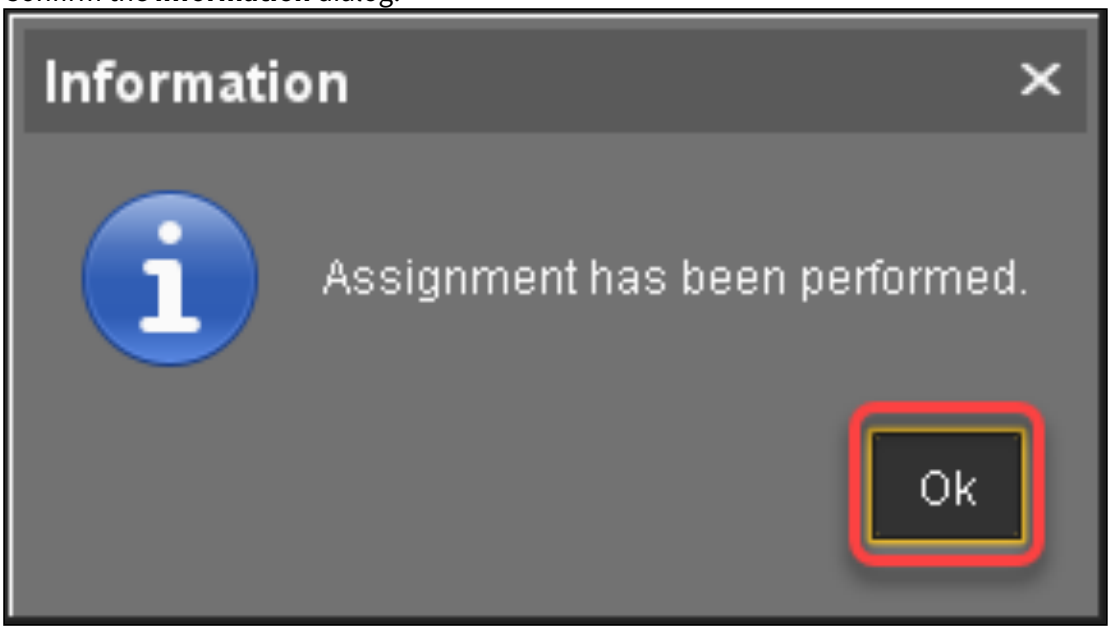
2. In the **Assign objects** dialog, select the profile for the target machines, click to assign it and then click **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.



4. Confirm the **Information** dialog.

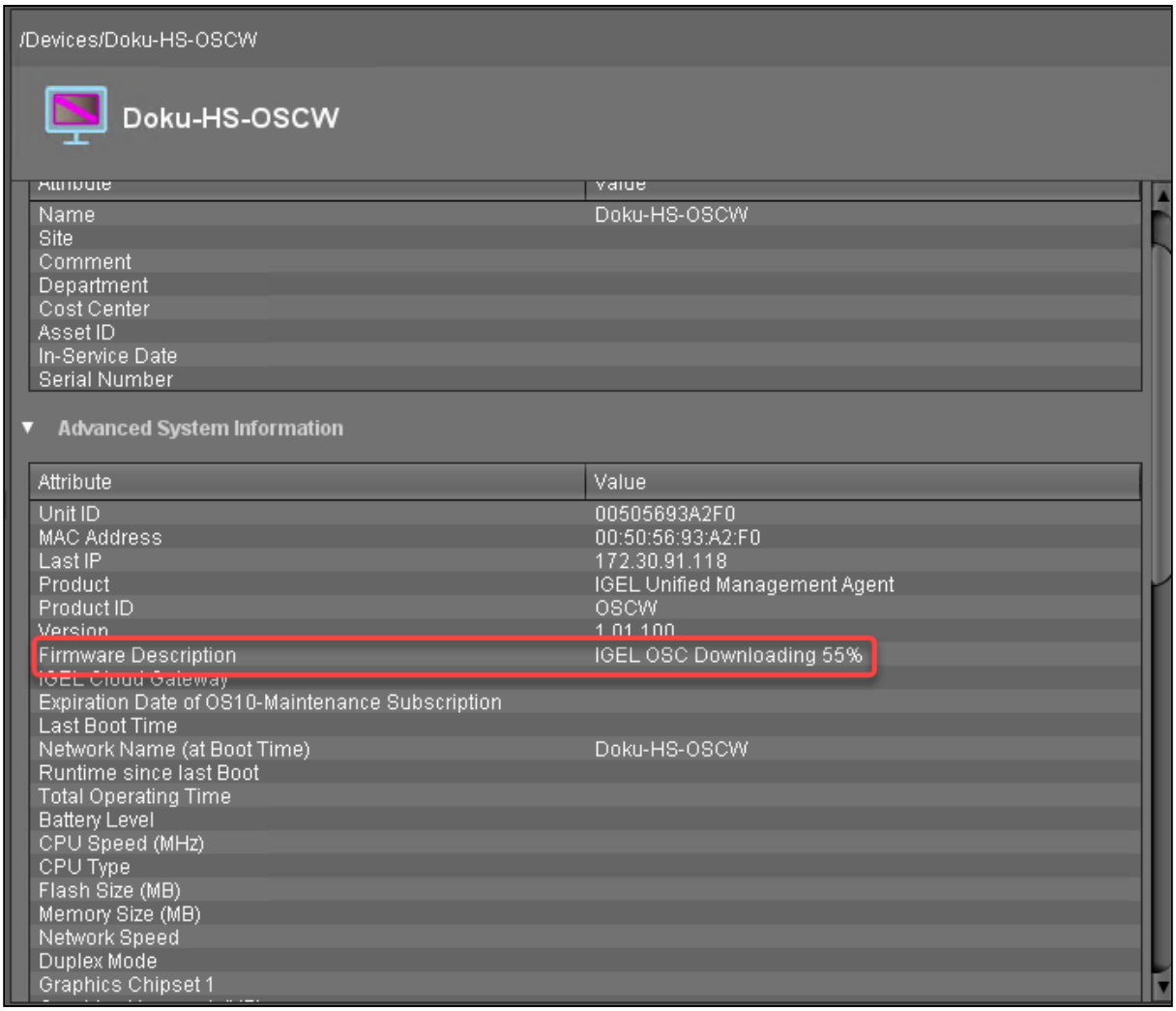


The target machines download the ISO file.

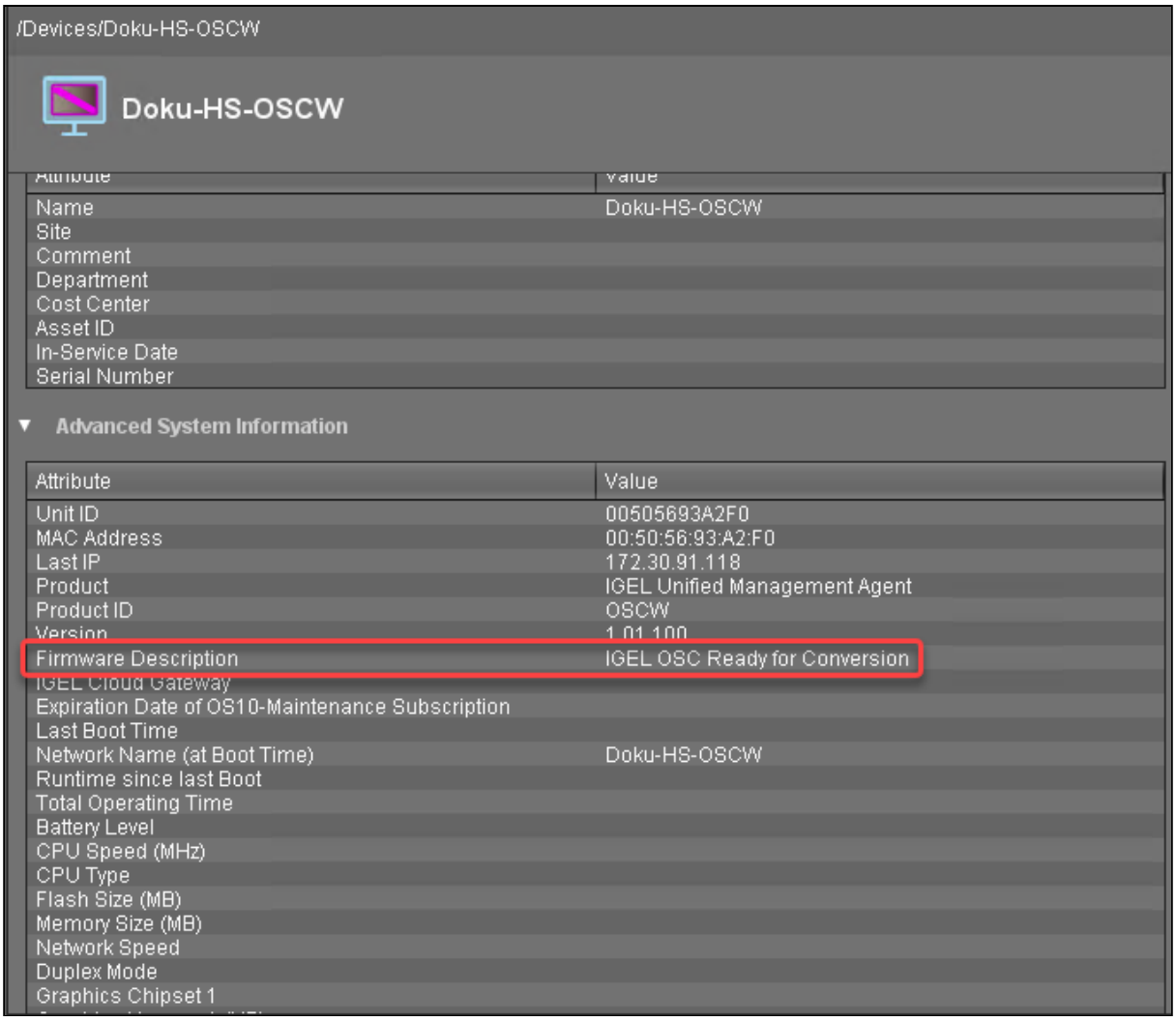
Monitoring the Process

1. In the structure tree of the UMS, open the context menu of one of the target machines and select **Other commands > Refresh system information**.

2. In the dialog, click **Refresh system information** and then every few seconds.
In the **Attribute** area, under **Firmware Description**, the current status of the download is shown.



When a device is ready, the value of **Firmware Description** changes to "IGEL OSC Ready for Conversion".



3. When **Firmware Description** reads "IGEL OSC Ready for Conversion", continue with Starting the Conversion 1 (see page 2242).

Check List

✅ The conversion profile is assigned to all target machines.

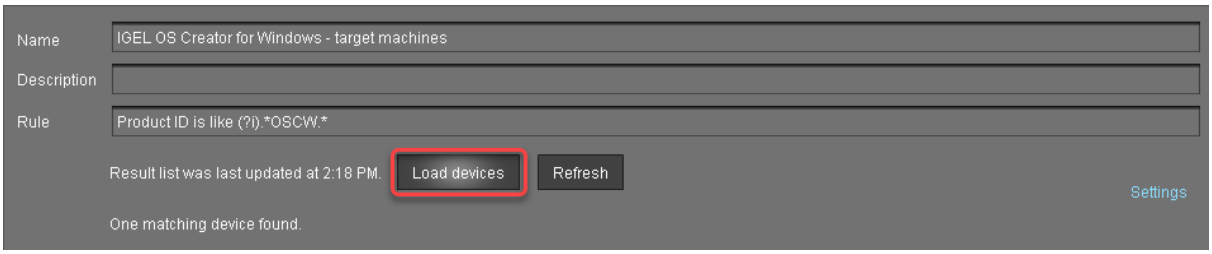
✅ All target machines have downloaded the OSCW ISO file, which is indicated by the **Firmware Description** "IGEL OS Ready for Conversion".

Next Step

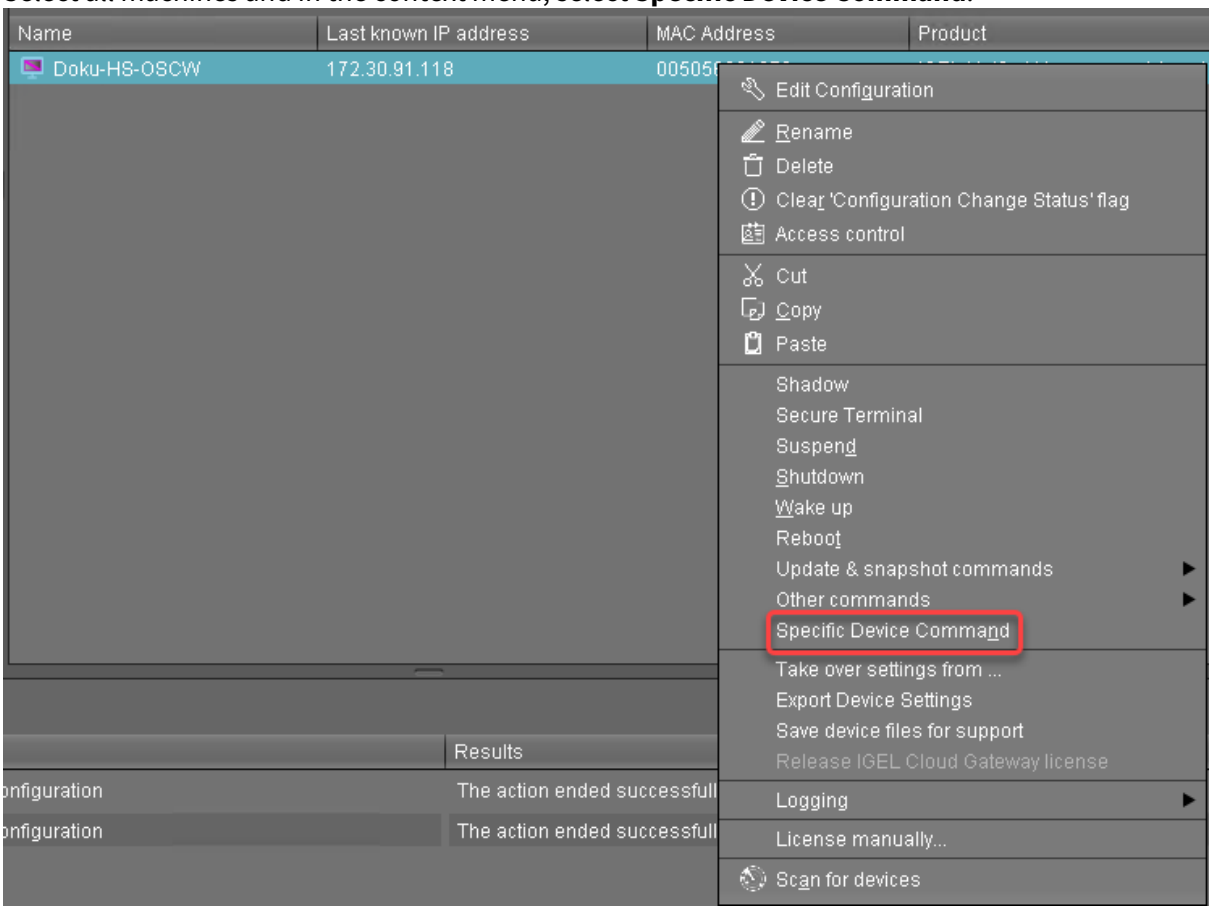
>> Starting the Conversion 1 (see page 2242)

Starting the Conversion

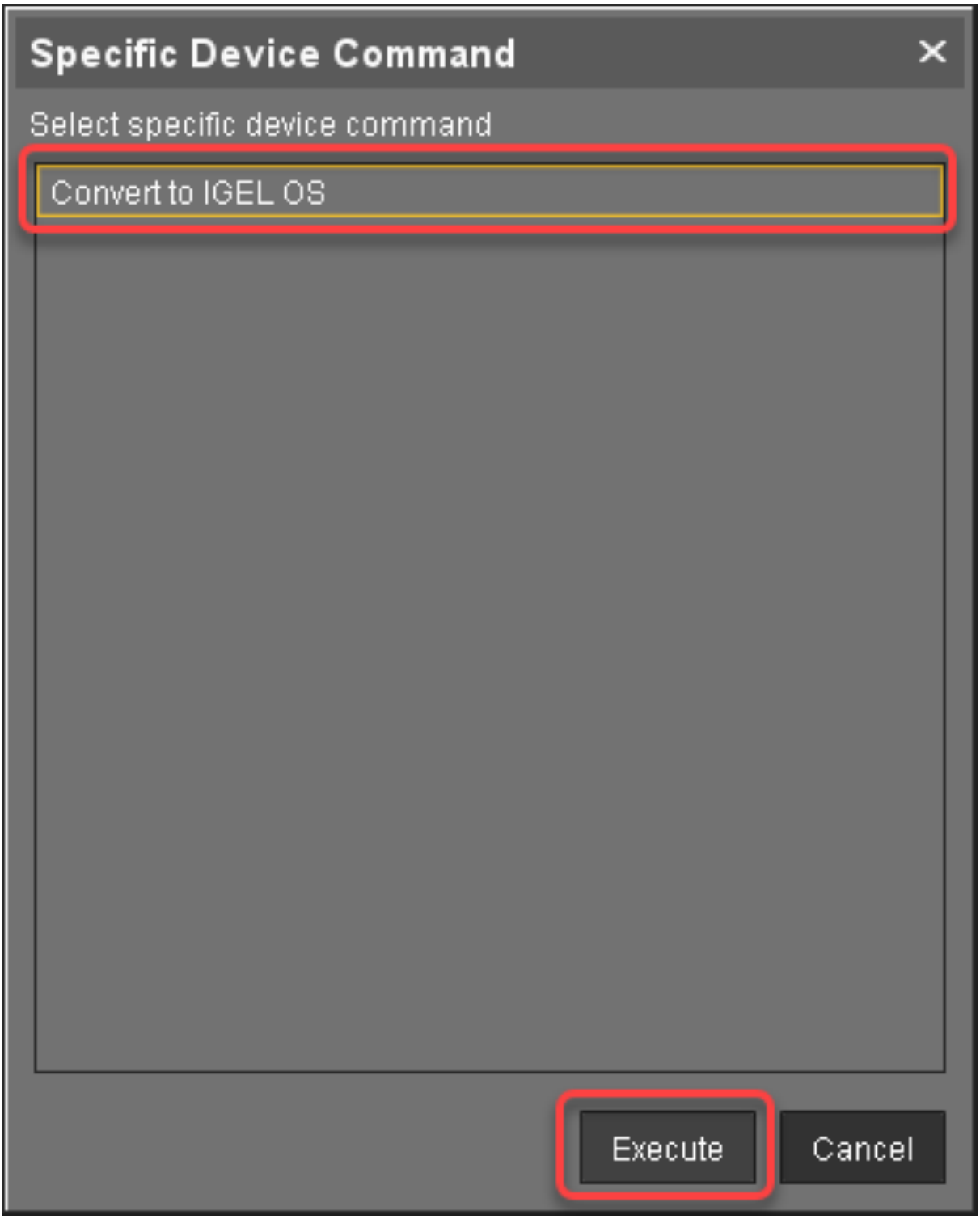
1. In the UMS structure tree, select the view you have created for selecting the target machines, and click **Load devices**.



2. Select all machines and in the context menu, select **Specific Device Command**.



3. In the **Specific Device Command** dialog, select **Convert to IGEL OS** and click **Execute**.



On the devices, a dialog is displayed. When the dialog is confirmed, the conversion starts

immediately. If the dialog is not confirmed, the conversion starts after 20 seconds.
When the conversion is complete, the **Product** information in the UMS is changed to "IGEL OS 11".

IGEL OS Creator for Windows (OSCW) on IGEL Windows Embedded 7/7+

The IGEL OS Creator (OSC) for Windows is able to convert any device that is running IGEL Windows Embedded 7/7+ to IGEL OS 11. The IGEL OS Creator (OSC) for Windows is integrated into version 3.13.150 of IGEL Windows Embedded 7 and into version 3.14.110 of IGEL Windows Embedded 7+.

Read all the following chapters and follow the instructions in the order given.

1. Prerequisites (see page 2246)
2. Getting the Required Software (see page 2247)
3. Updating the IGEL WES7/7+ Devices (see page 2248)
4. Transferring the IGEL OS 11 Firmware to the UMS (see page 2256)
5. Configuring the OSCW Installer (see page 2257)
6. Starting the Conversion (see page 2269)

Prerequisites

Network

- All machines are registered with the UMS.

Next Step

>> When all requirements are met, continue with Getting the Required Software 2 (see page 2247).

Getting the Required Software

The following software must be downloaded resp. installed:

IGEL Universal Management Suite (UMS) 6.04.120 or Higher

1. Download UMS 6.04.120 or higher from https://www.igel.com/software-downloads/workspace-edition/ **> Universal Management Suite**.
2. Update your UMS to version 6.04.120 or later. For update instructions, see IGEL UMS Update[253].

IGEL OS 11

->Download IGEL OS 11.03.500 or higher from https://www.igel.com/software-downloads/workspace-edition/ **> OS 11 > FIRMWARE UPDATES**.

IGEL WES 7/7+

->For IGEL WES 7 devices, download version 3.13.150.

->For IGEL WES 7+ devices, download version 3.14.110_W7+.

Check List

- The UMS is updated to version 6.04.120 or higher.
- The required firmware versions for IGEL WES7/7+ devices are available.
- The firmware files for IGEL OS 11.03.500 or higher are available.

Next Step

>> Updating the IGEL WES7/7+ Devices (see page 2248)

253. https://kb.igel.com/en/universal-management-suite/current/igel-ums-update

Updating the IGEL WES7/7+ Devices

In this step, we will update the devices to the IGEL WES 7/7+ version that is capable of converting the device to IGEL OS 11.

For IGEL WES 7 devices, you use `UniversalDesktopWES-3.13.150.snp`; for IGEL WES 7+ devices, you use `UniversalDesktopWES7+-3.14.110.snp` as the snapshot file. If you have both device types, perform the steps described below for each device type separately.

> ⚠ After the update, you can update to another firmware only via IGEL rescue shell!

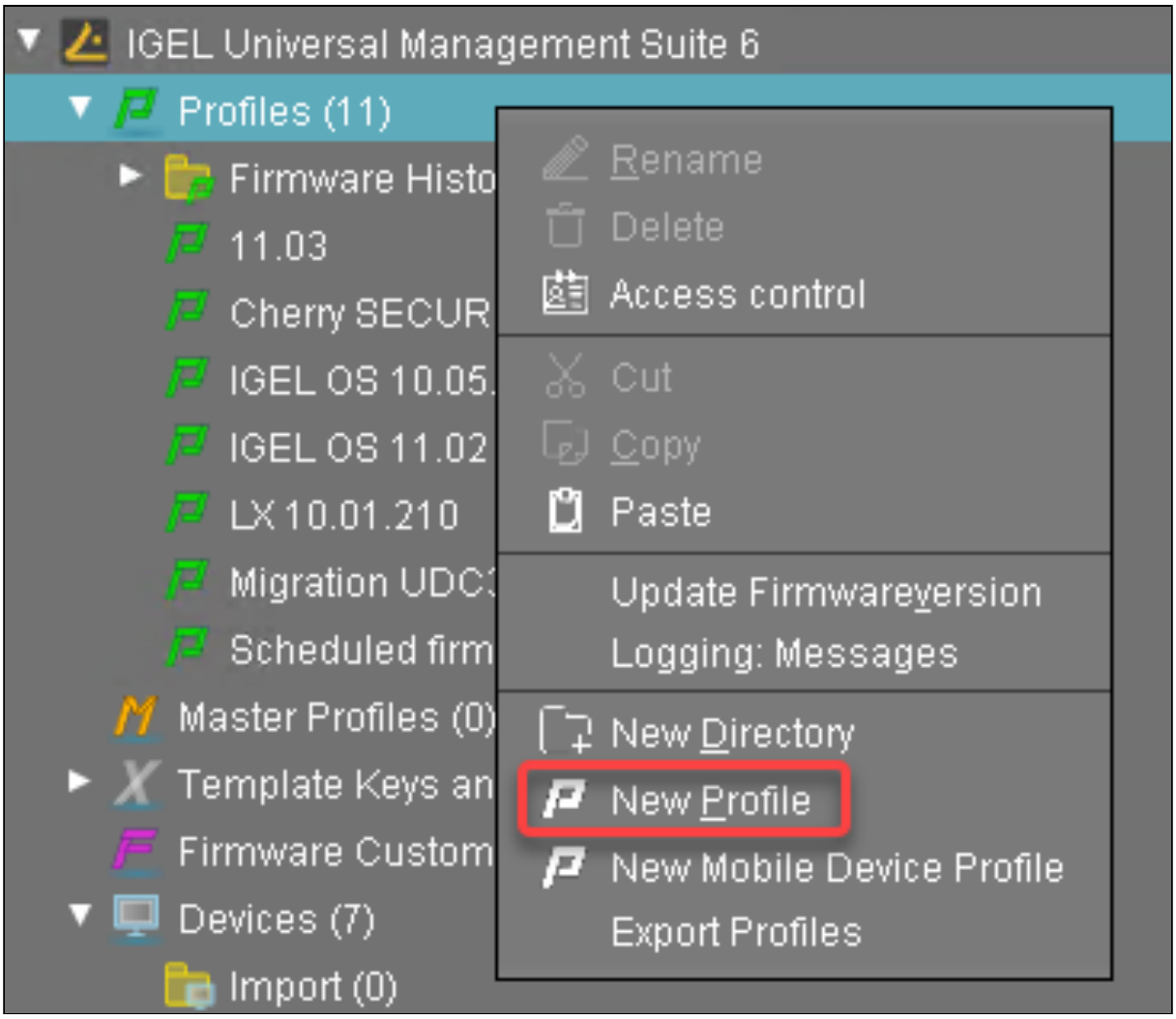
Transferring the Snapshot File to the UMS

The snapshot file must be placed in the file system of the UMS Server.

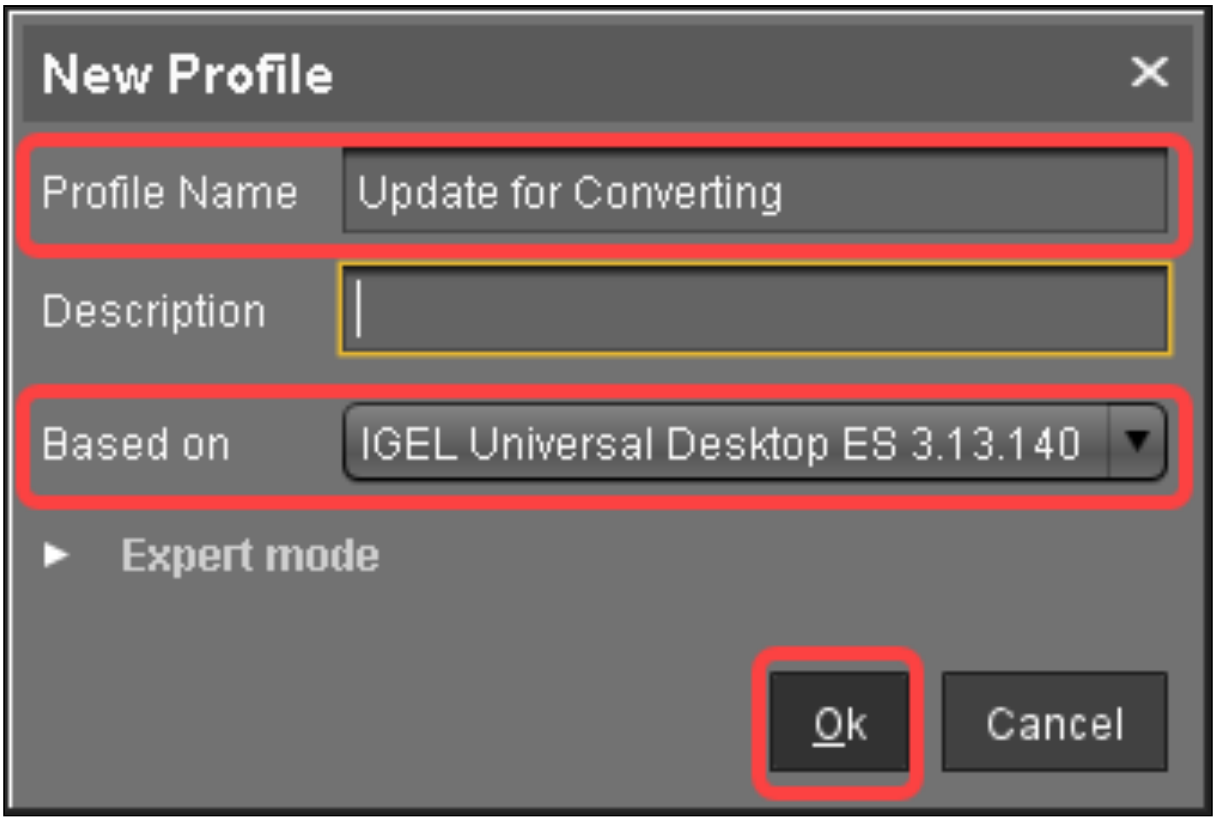
1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the snapshot file to `<UMS Installation directory>\rmguiserver\webapps\ums_filetransfer`

Creating an Update Profile

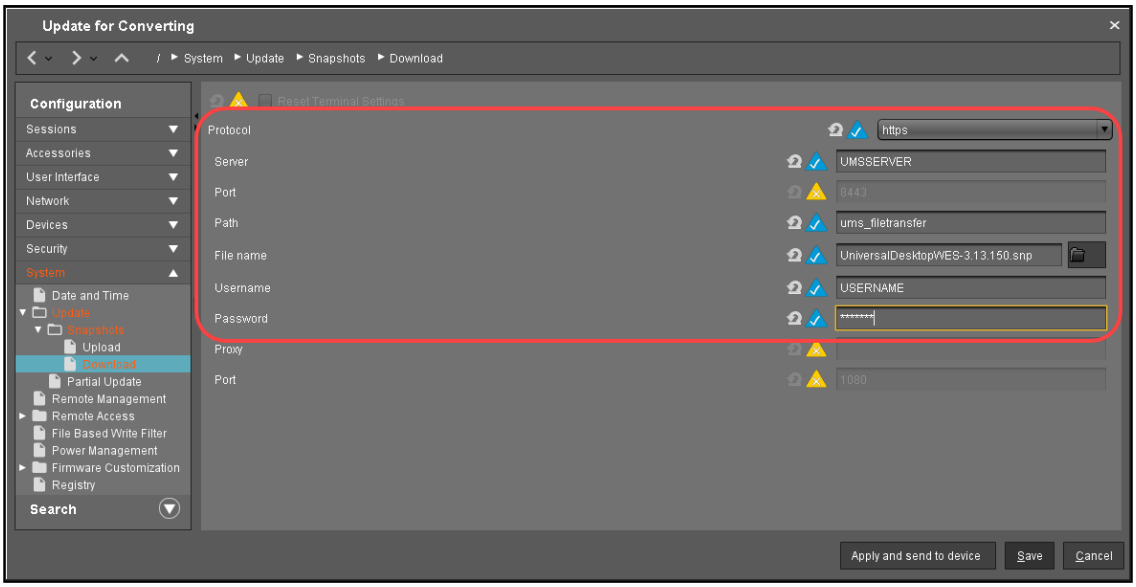
1. In the UMS structure tree, go to **Profiles**, open the context menu, and select **New Profile**.



2. Enter the following data:
   - **Profile Name**: Name for the profile, e. g. "Update for Converting".
   - **Description**: Optional description for the profile.
   - **Based on**: Firmware version for the profile; select the current firmware of your devices.
3. Click **Ok**.



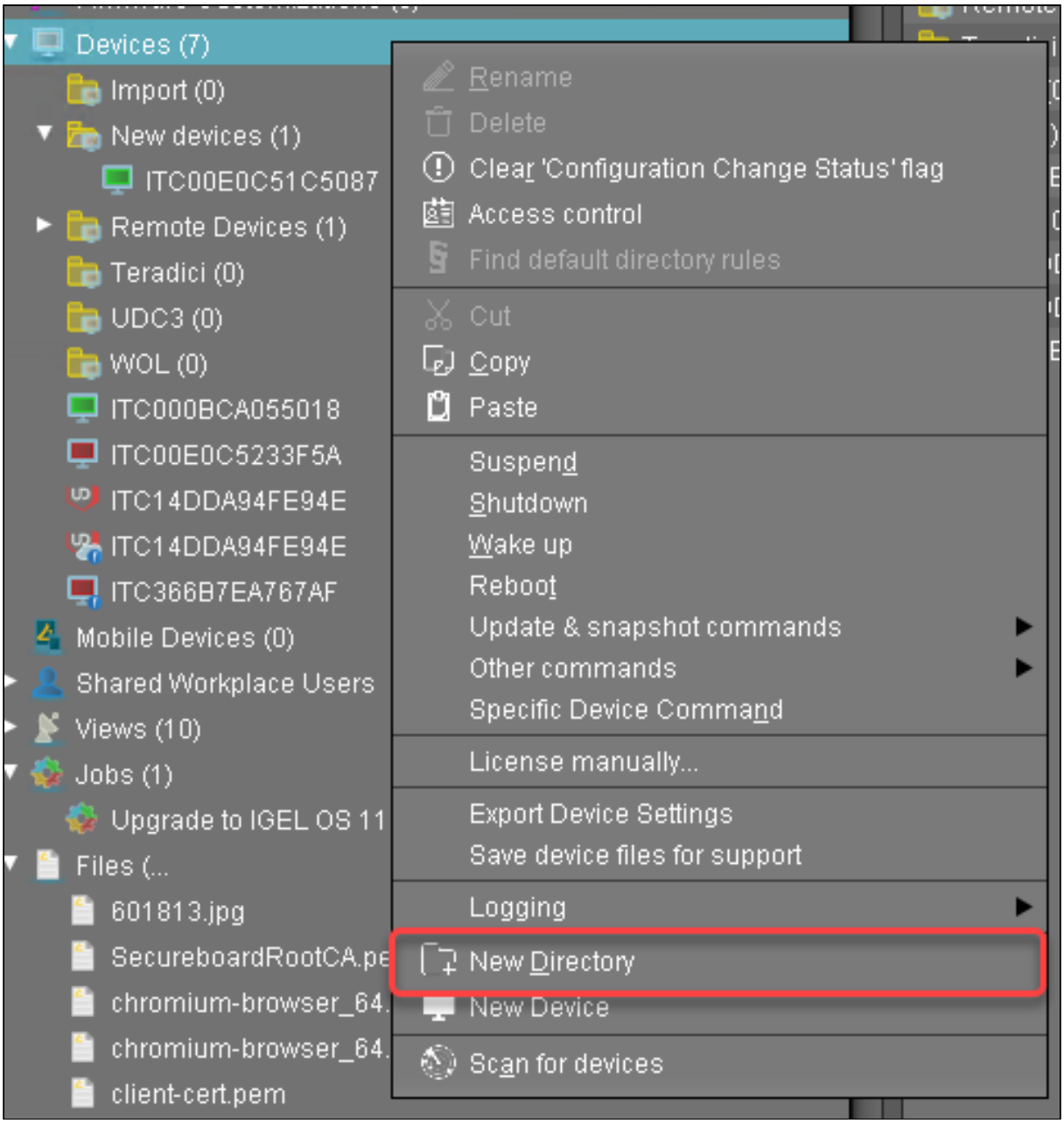
4. Go to **System > Update > Snapshots > Download** and change the settings as follows:
    - **Protocol**: Select "https".
    - **Server**: Enter the IP address or hostname of the UMS.
    - **Path**: Enter "ums_filetransfer".
    - **File name**: Enter the file name of the snapshot file.
    - **Username**: Enter your UMS user name.
    - **Password**: Enter your UMS password.



5. Click **Save** to save the profile.

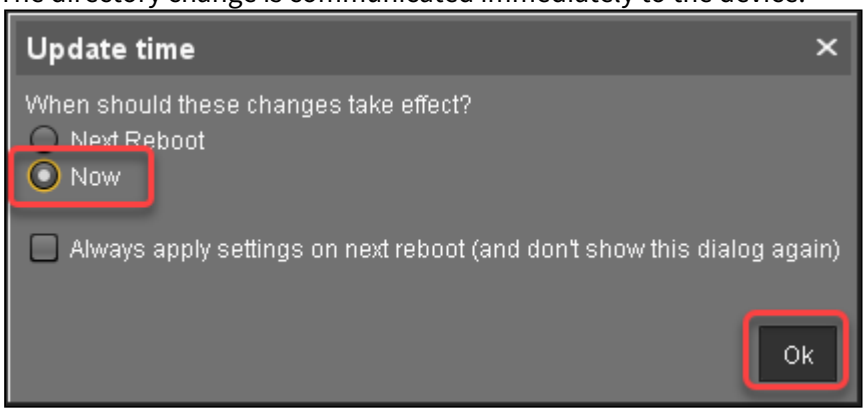
Starting the Update

1. Under **Devices**, create a directory and name it "Convert to IGEL OS 11", for instance.

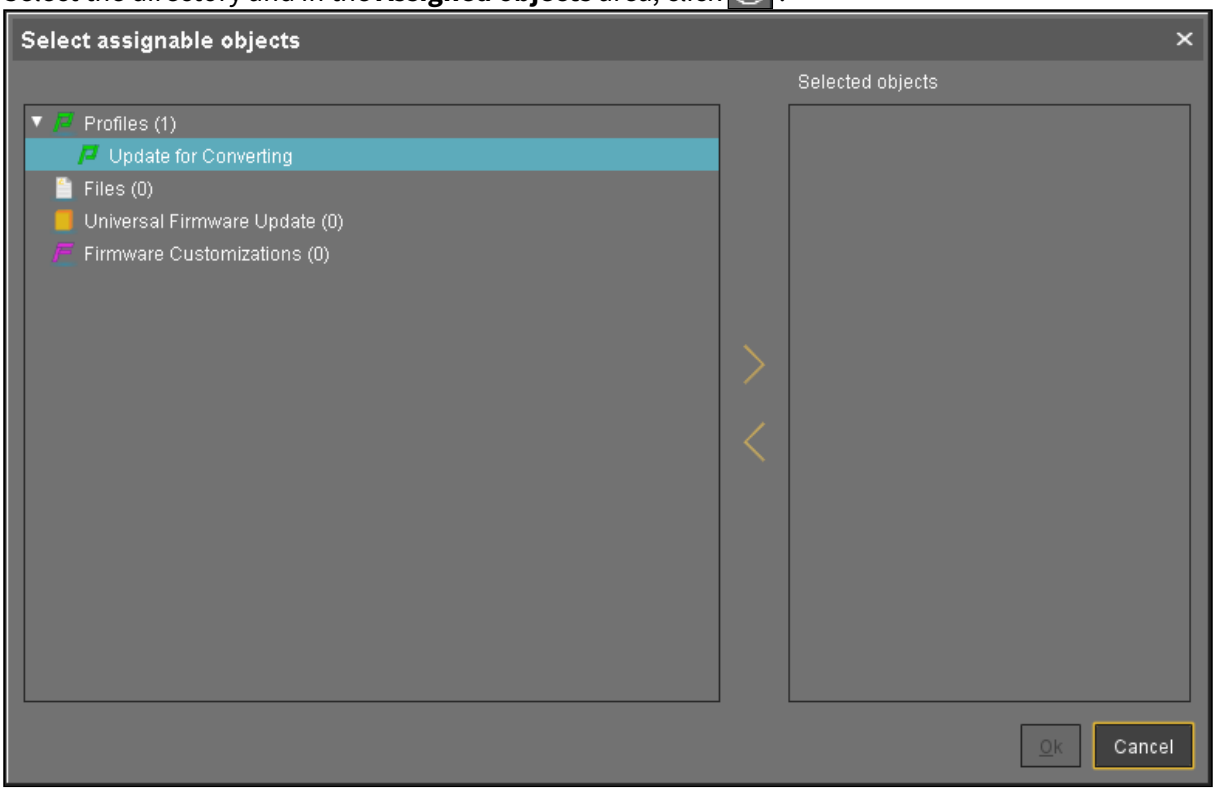


2. Put the devices that are to be updated into the new directory. You can use drag & drop.

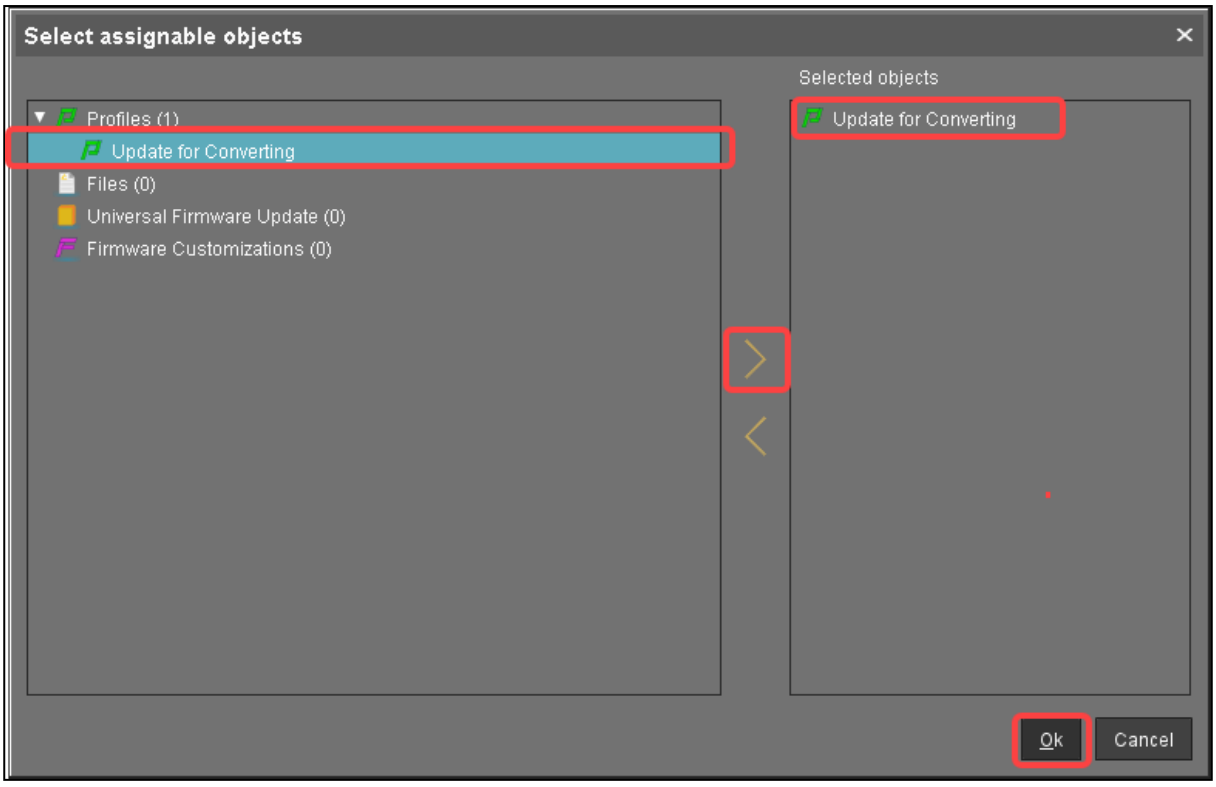
3. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change is communicated immediately to the device.



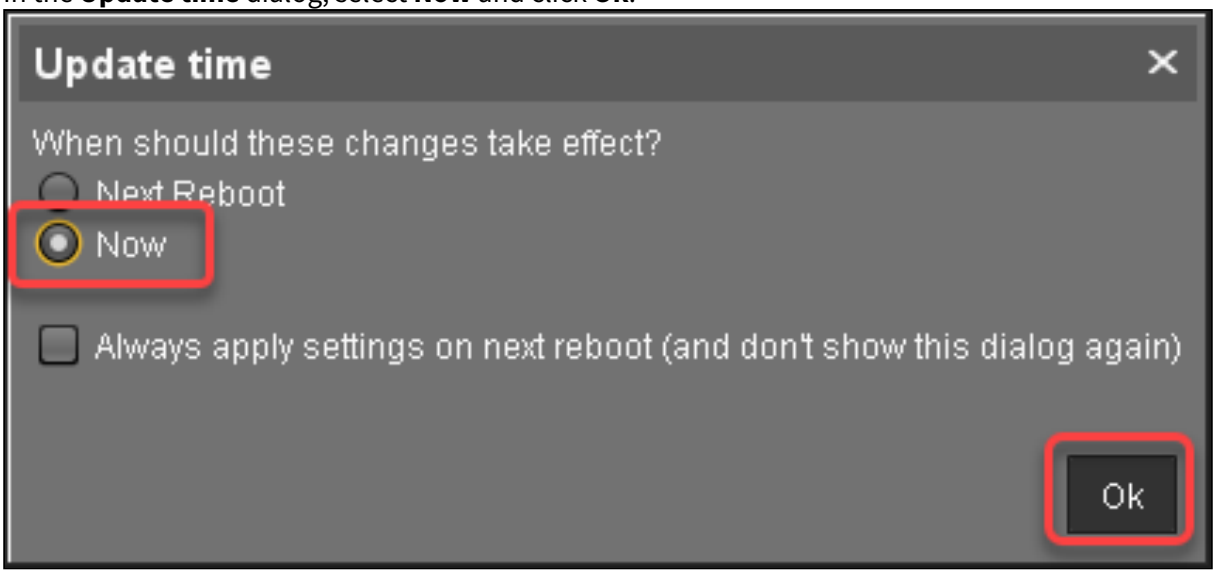
4. Select the directory and in the **Assigned objects** area, click .



5. Assign the update profile to the directory and click **Ok**.

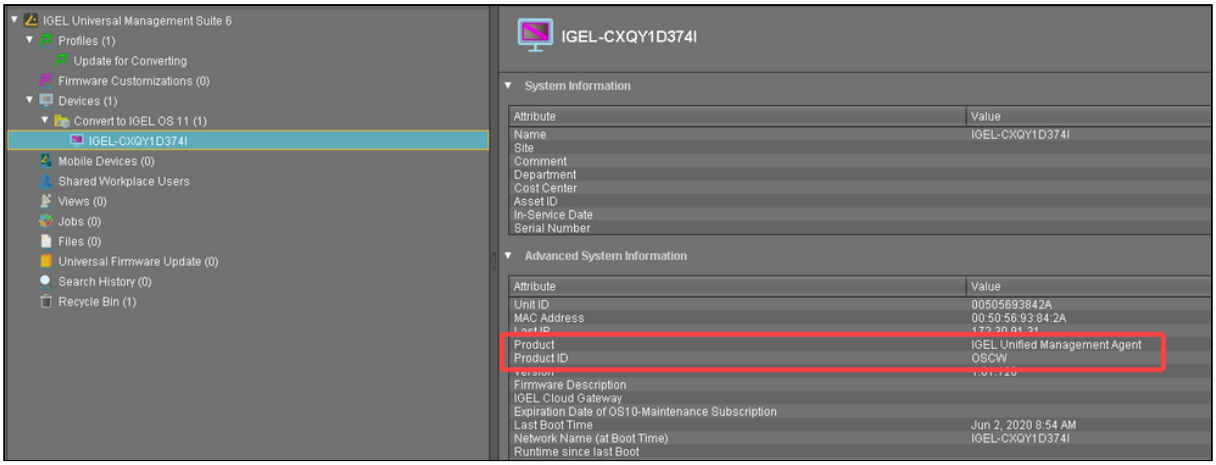


6. In the **Update time** dialog, select **Now** and click **Ok**.



   The changes are sent to the devices immediately.
7. Go to the directory that contains the devices that are to be updated, open the context menu, and select **Update & snapshot commands > Update**.
   The update process is started.

8. When the update process is finished, go to one of the devices and click to refresh the screen. In the **Advanced System Information** area, **Product** is set to "IGEL Unified Management Agent", and **Product ID** is set to "OSCW".



Check List

✅ The devices are updated to version 3.13.150 (WES 7) or 3.14.110 (WES 7+).

Next Step

>> Transferring the IGEL OS 11 Firmware to the UMS (see page 2256)

Transferring the IGEL OS 11 Firmware to the UMS

In this step, we will transfer the IGEL OS 11 firmware files to the UMS so that the target machines can fetch it from there.

1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the firmware files to `<UMS Installation directory>\rmguiserver\webapps\ums_filetransfer`

Check List

- The IGEL OS firmware files are located in the `/ums_filetransfer/` directory of the UMS.

Next Step

>> Configuring the OSCW Installer (see page 2257)

Configuring the OSCW Installer

In this step, we will provide the OSCW installer with the download source for the IGEL OS firmware.

Two methods are available:

- Configuring the OSCW Installer in Normal Mode (see page 2258): Each target machine downloads the firmware files from the UMS individually. This increases the amount of outgoing traffic from the UMS.
- Configuring the OSCW Installer in Buddy Mode (see page 2263): This method is recommended if the connection bandwidth of the download source is limited; it ensures a more balanced use of network bandwidth during the distribution of the firmware files to the target machines. First, a group of target machines is converted to IGEL OS 11. Then, these machines are configured to serve as buddy update servers for the remaining target machines.

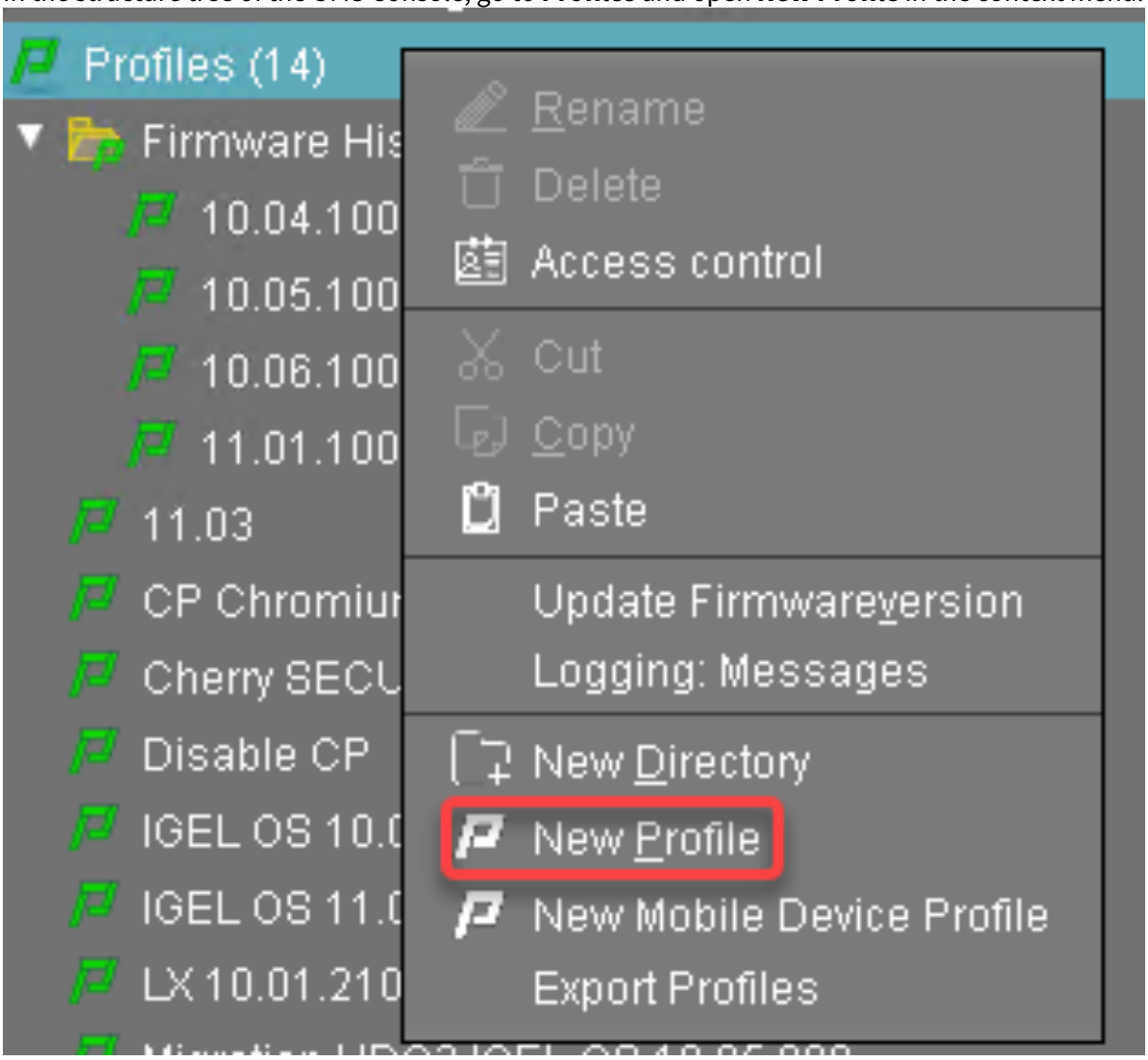
Configuring the OSCW Installer in Normal Mode

To provide the OSCW installer with the download source for the IGEL OS firmware files, we will create a profile that provides the path to those files.

The configuration comprises the following steps:

Creating a Profile

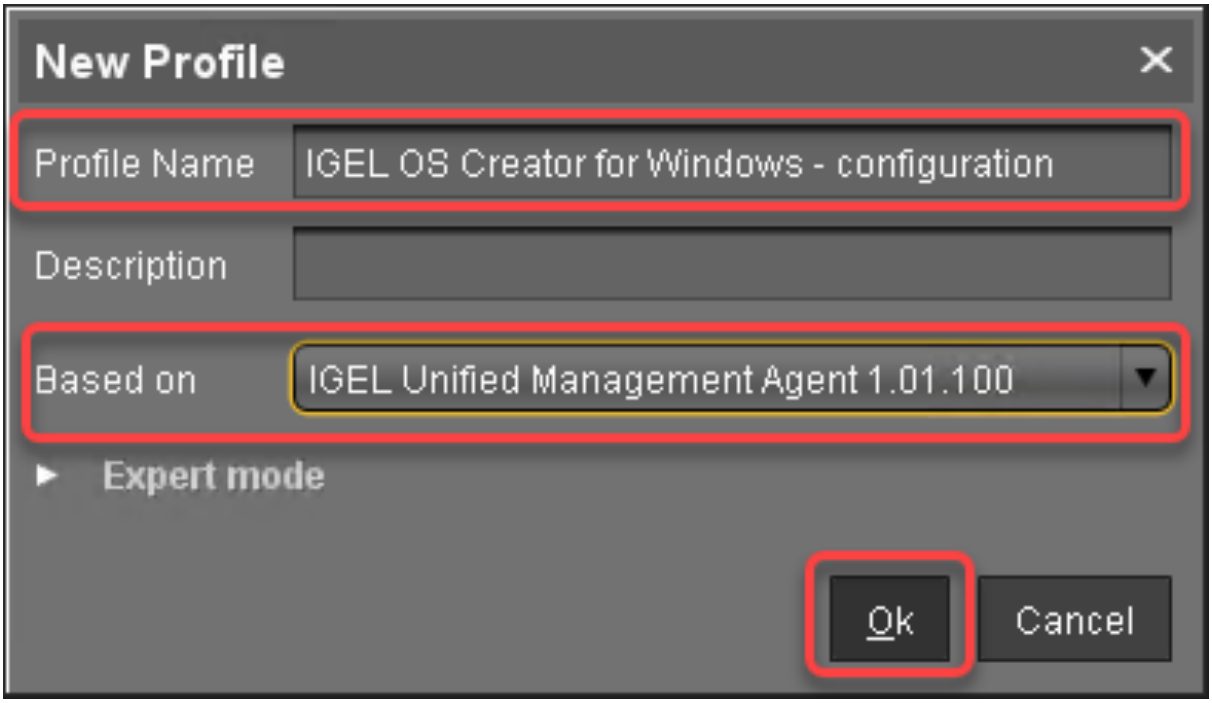
1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.



2. In the **New Profile** dialog, change the settings as follows:
   - **Profile Name**: A name for the profile, e. g. "IGEL OS Creator for Windows - configuration"

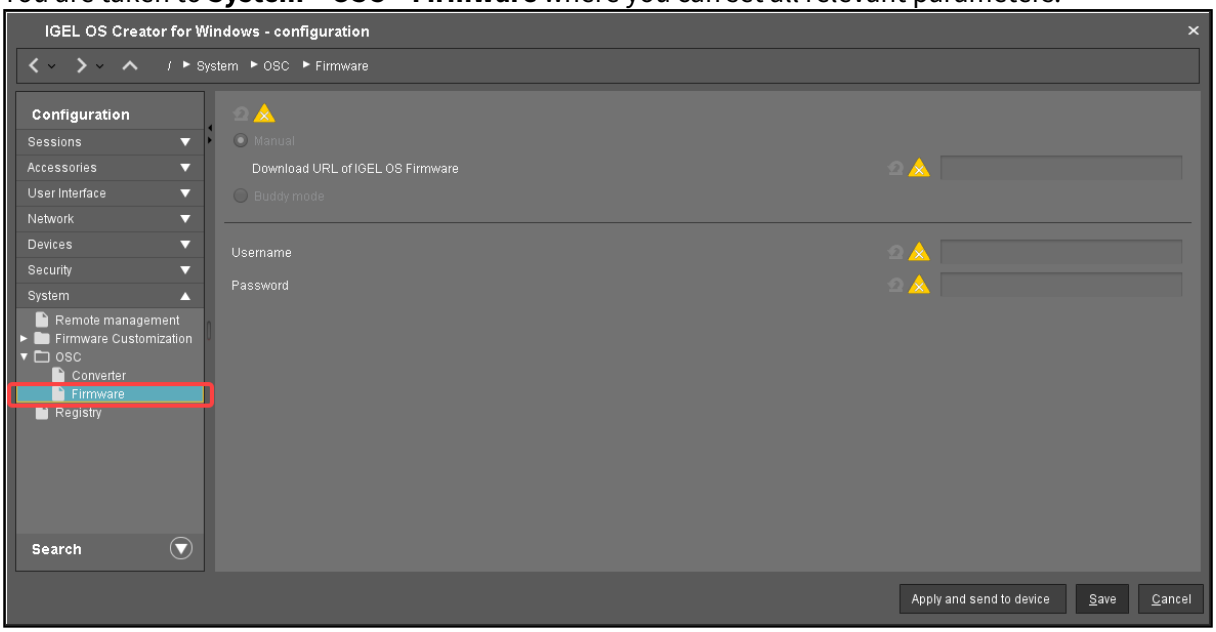
- **Based on**: Select "IGEL Unified Management Agent 1.xx.xxx", e. g. "IGEL Unified Management Agent 1.01.100".

3. Click **Ok**.

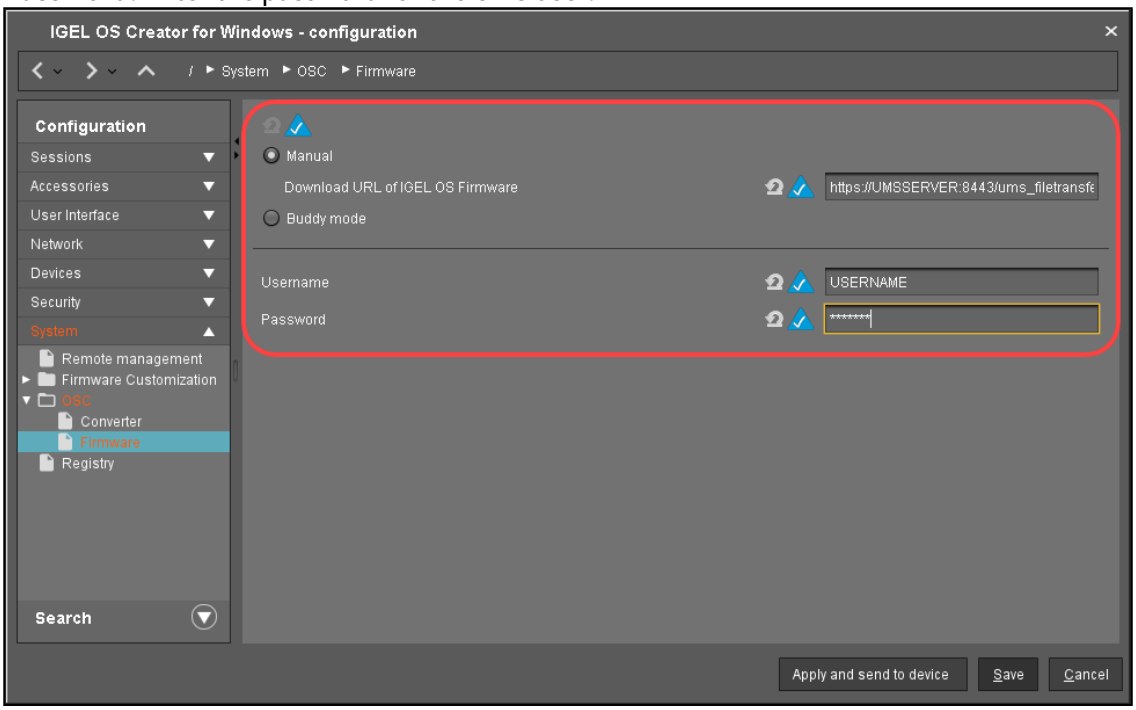


The configuration dialog opens.

4. Click **Firmware**.
You are taken to **System > OSC > Firmware** where you can set all relevant parameters.



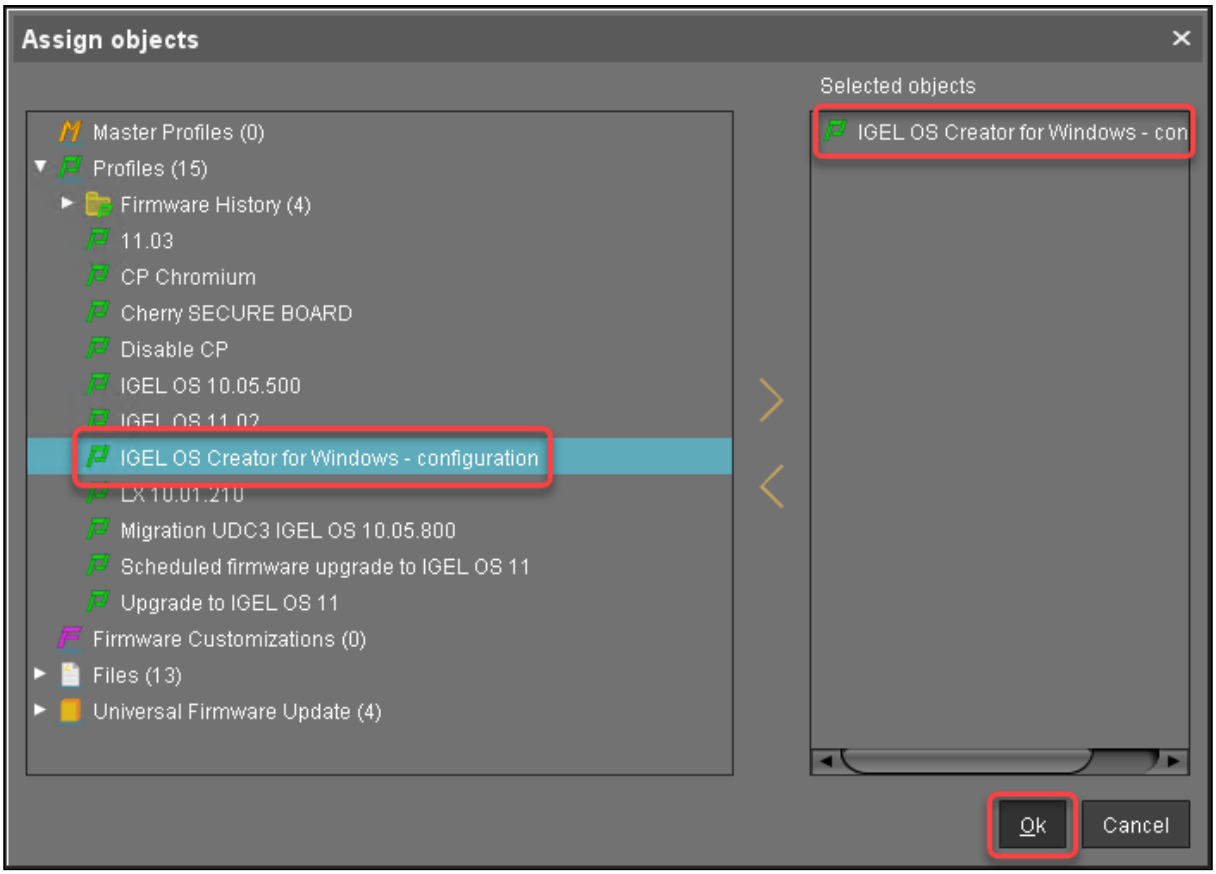
5. Change the settings as follows (click the icon to enable the configuration; the icon will change to):
   - **Download URL of IGEL OS Firmware**: Enter `https://[IP address of your UMS Server]:8443/ums_filetransfer` / or `http://[IP address of your UMS Server]:9080/ums_filetransfer` /
     Example: `https://192.168.178.100:8443/ums_filetransfer/` or `http://192.168.178.100:9080/ums_filetransfer/`
   - **Username**: Enter the username for the UMS.
   - **Password**: Enter the password for the UMS user.



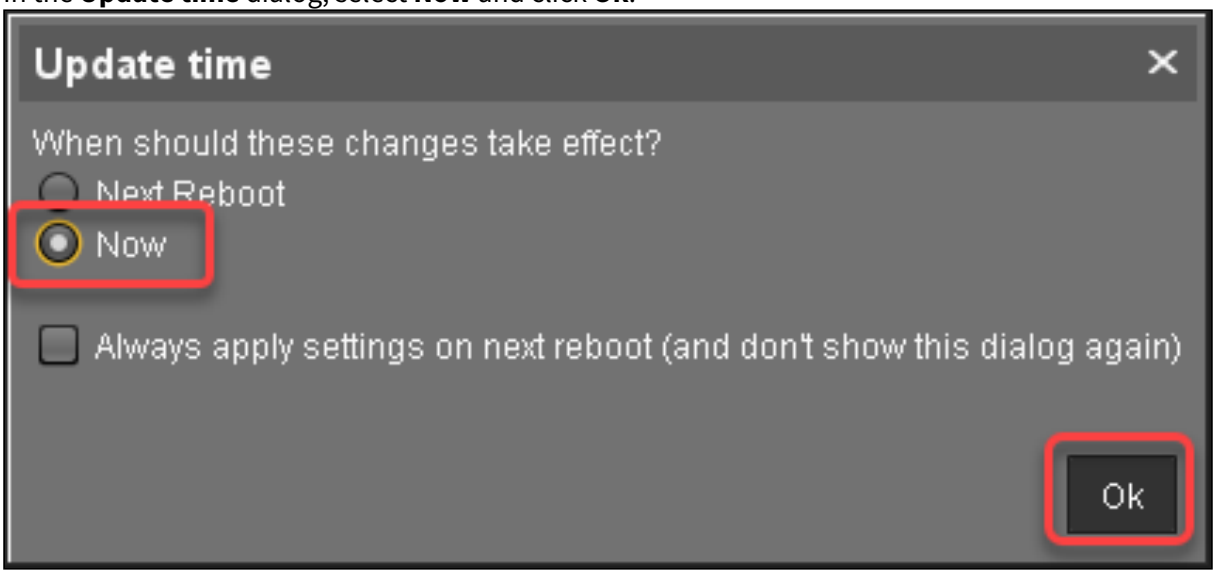
6. Click **Save**.

Assigning the Profile to the Target Machines

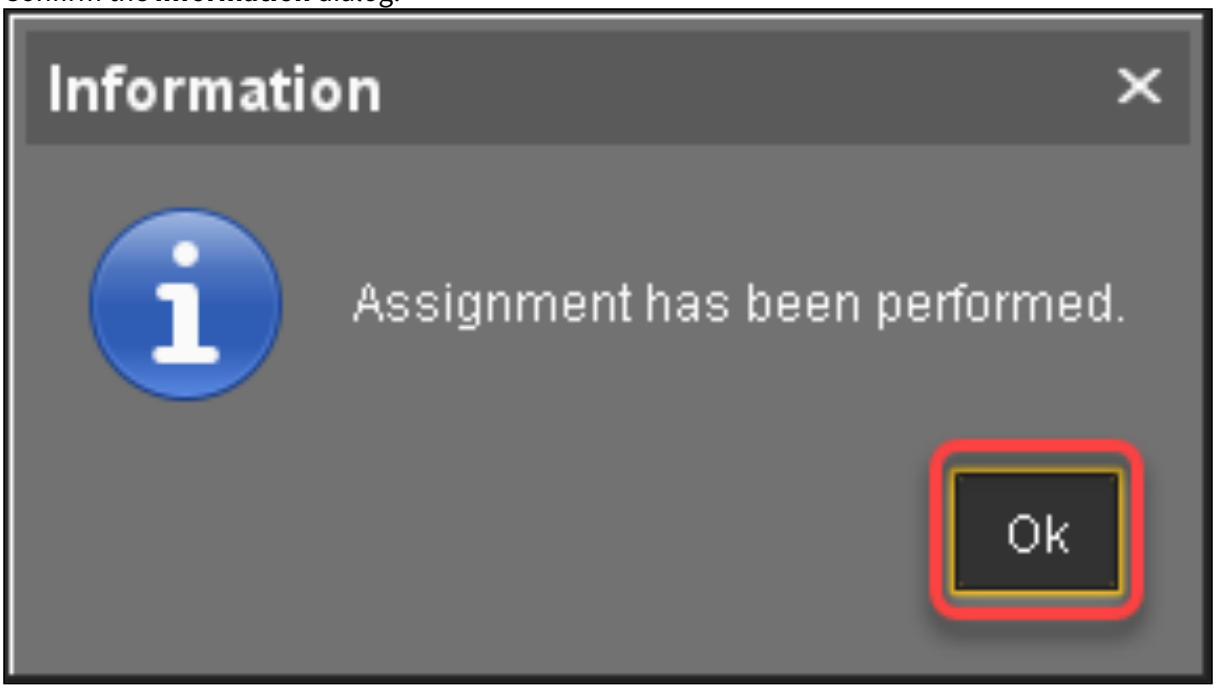
1. Select the directory that contains your target machines and in the **Assigned objects** area, click .
2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.



4. Confirm the **Information** dialog.



Check List

- The conversion profile is assigned to all target machines.

Next Step

>> Starting the Conversion (see page 2269)

Configuring the OSCW Installer in Buddy Mode

When buddy update is used, one or more machines convert to IGEL OS first and then serve as buddy update servers.

The configuration comprises the following steps:

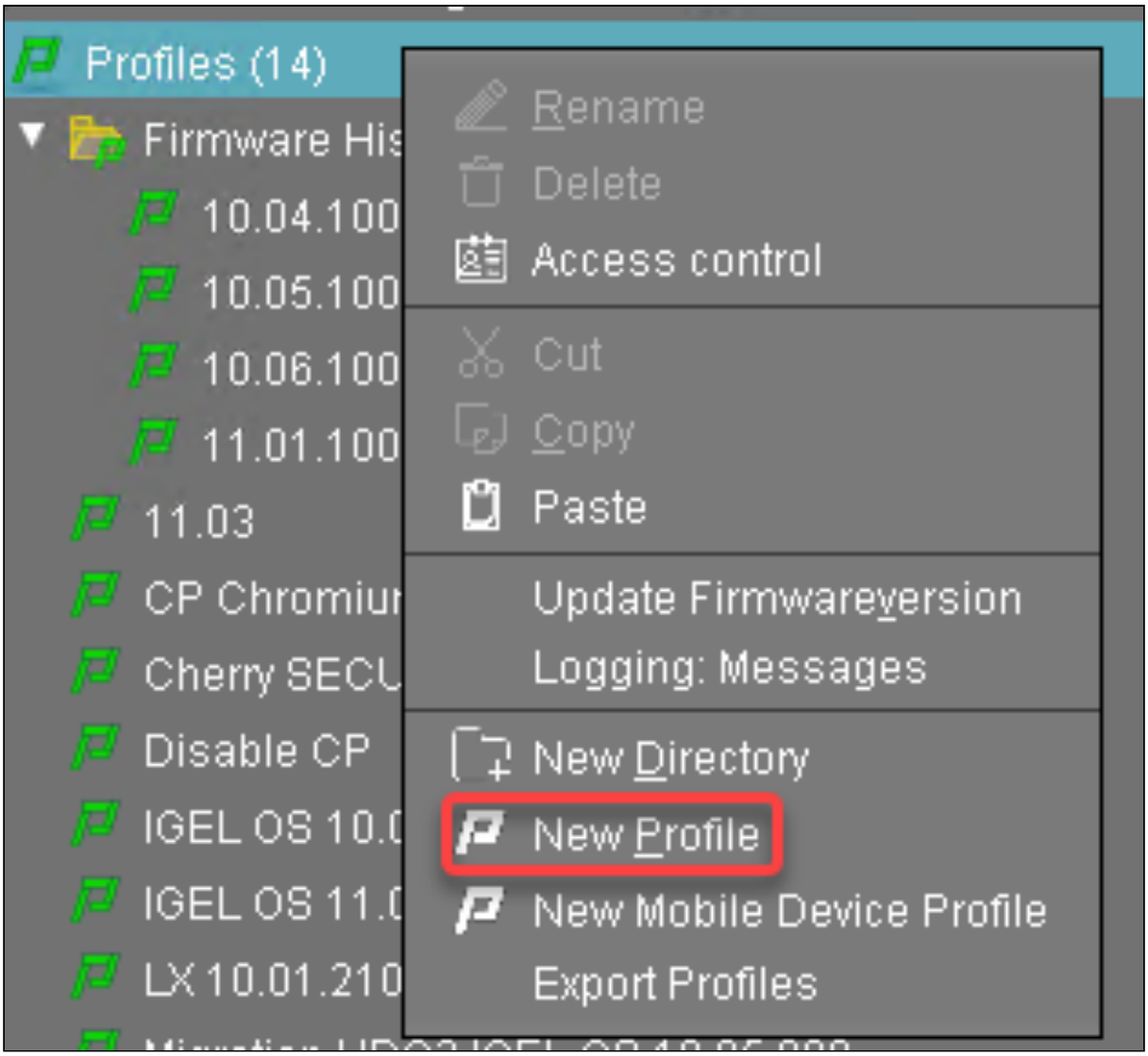
- Setting up the Buddy Update Servers (see page 2263)
- Creating a Profile for the Buddy Update Clients (see page 2263)
- Assigning the Profile to the Target Machines (see page 2266)

Setting Up the Buddy Update Servers

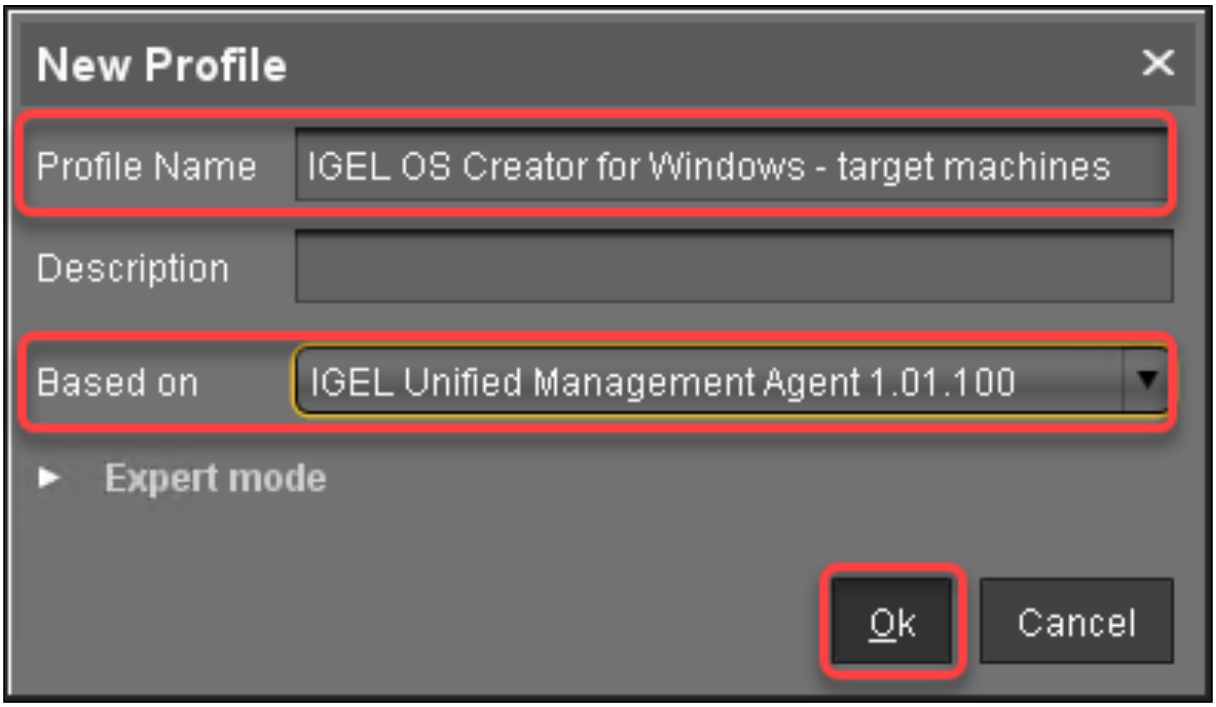
1. Convert the machines that are to be used as buddy update servers as described under Configuring the OSCW Installer in Normal Mode (see page 2258) and Starting the Conversion (see page 2269).
2. Configure the converted machines as buddy update servers as described under Configuring the Buddy Update Server (see page 306), "Basic Configuration".

Creating a Profile for the Buddy Update Clients

1. In the structure tree of the UMS Console, go to **Profiles** and open **New Profile** in the context menu.

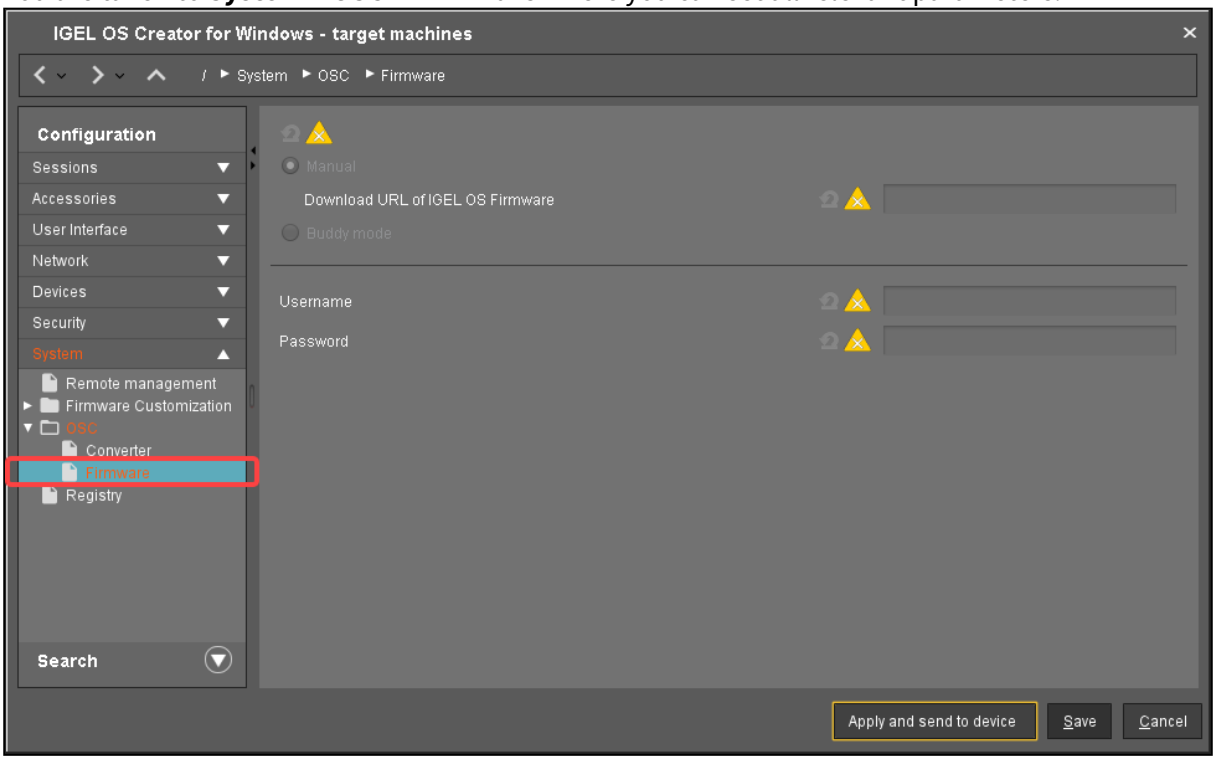


2. In the **New Profile** dialog, change the settings as follows:
   - **Profile Name**: A name for the profile, e. g. "IGEL OS Creator for Windows - target machines"
   - **Based on**: Select "IGEL Unified Management Agent 1.xx.xxx", e. g. "IGEL Unified Management Agent 1.01.100".
3. Click **Ok**.

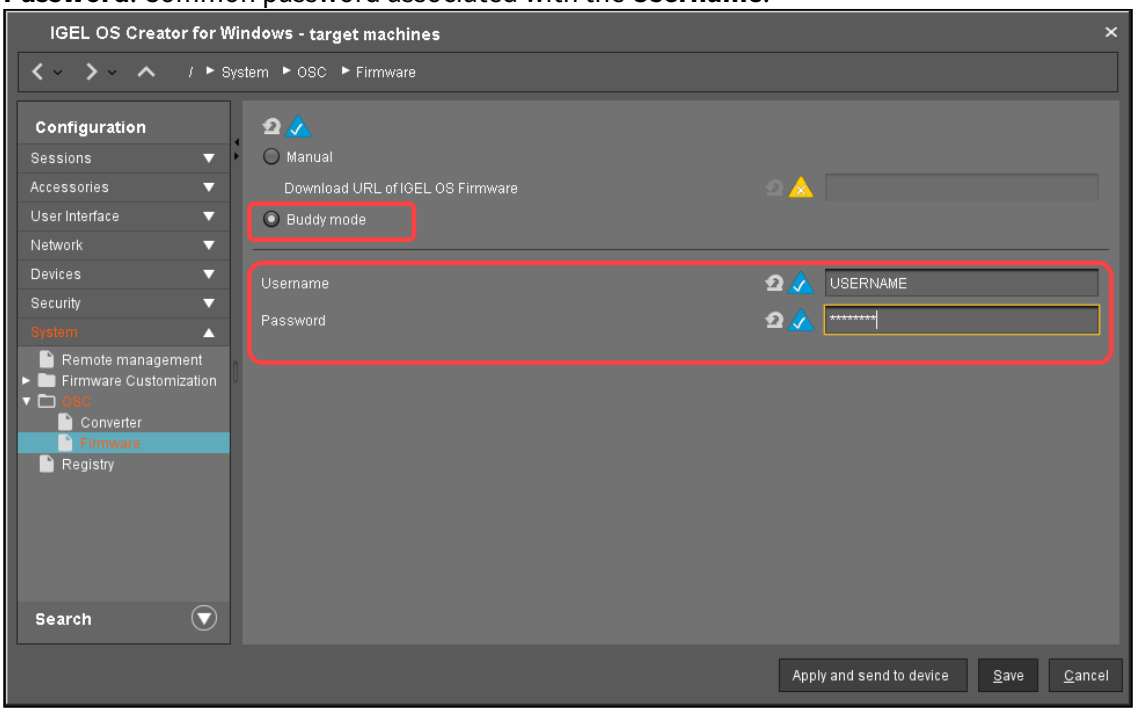


The configuration dialog opens.

4. Click **Firmware**.
   You are taken to **System > OSC > Firmware** where you can set all relevant parameters.



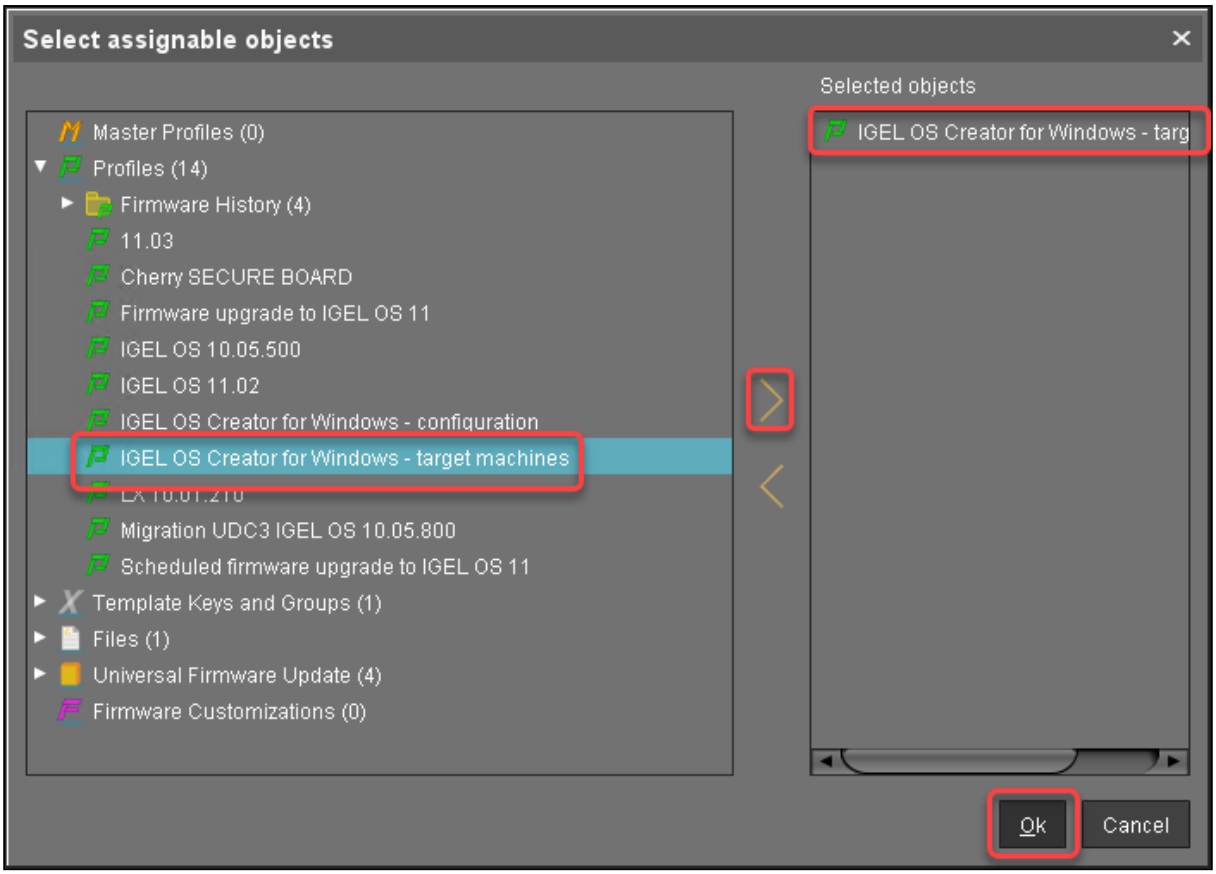
5. Change the settings as follows (click the icon to enable the configuration; the icon will change to):
   - Select **Buddy mode**.
   - **Username**: Username that is configured on the buddy update servers.
   - **Password**: Common password associated with the **Username**.



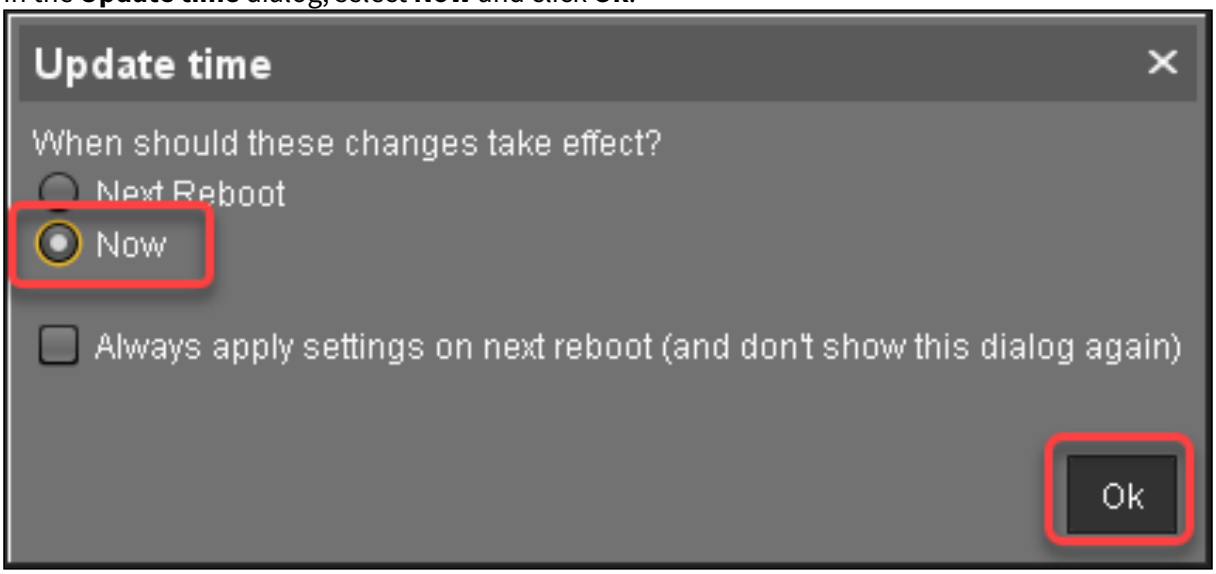
6. Click **Save**.

Assigning the Profile to the Buddy Update Clients

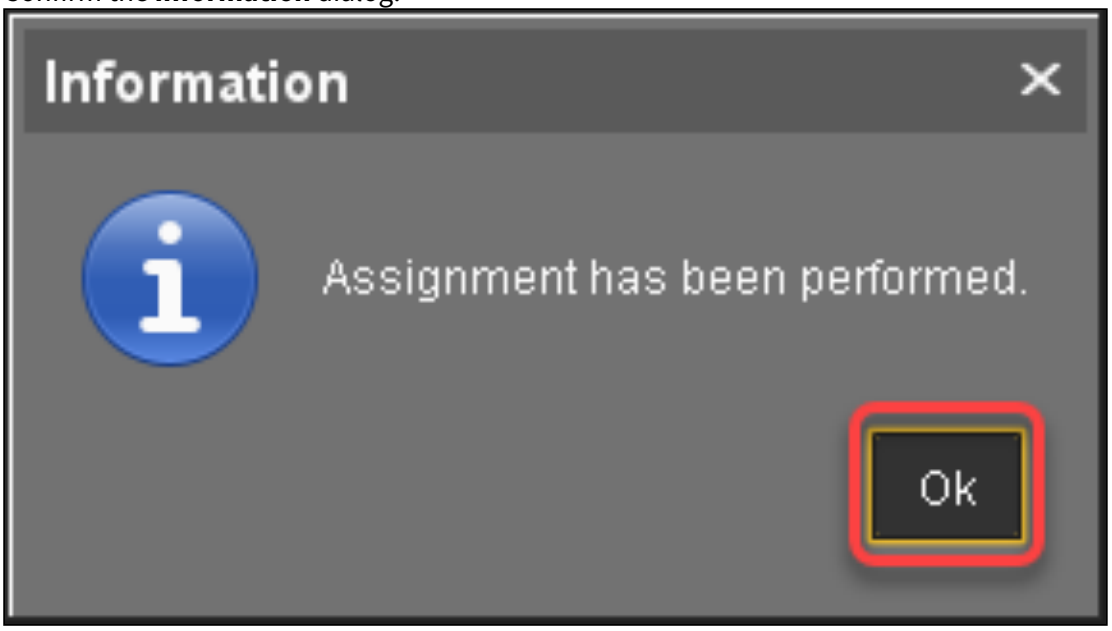
1. Select the directory that contains your target machines and in the **Assigned objects** area, click .
2. In the **Assign objects** dialog, select the profile you have created beforehand, click to assign it and then click **Ok**.



3. In the **Update time** dialog, select **Now** and click **Ok**.



4. Confirm the **Information** dialog.



The target machines download the firmware files. This may take a few minutes.

Check List

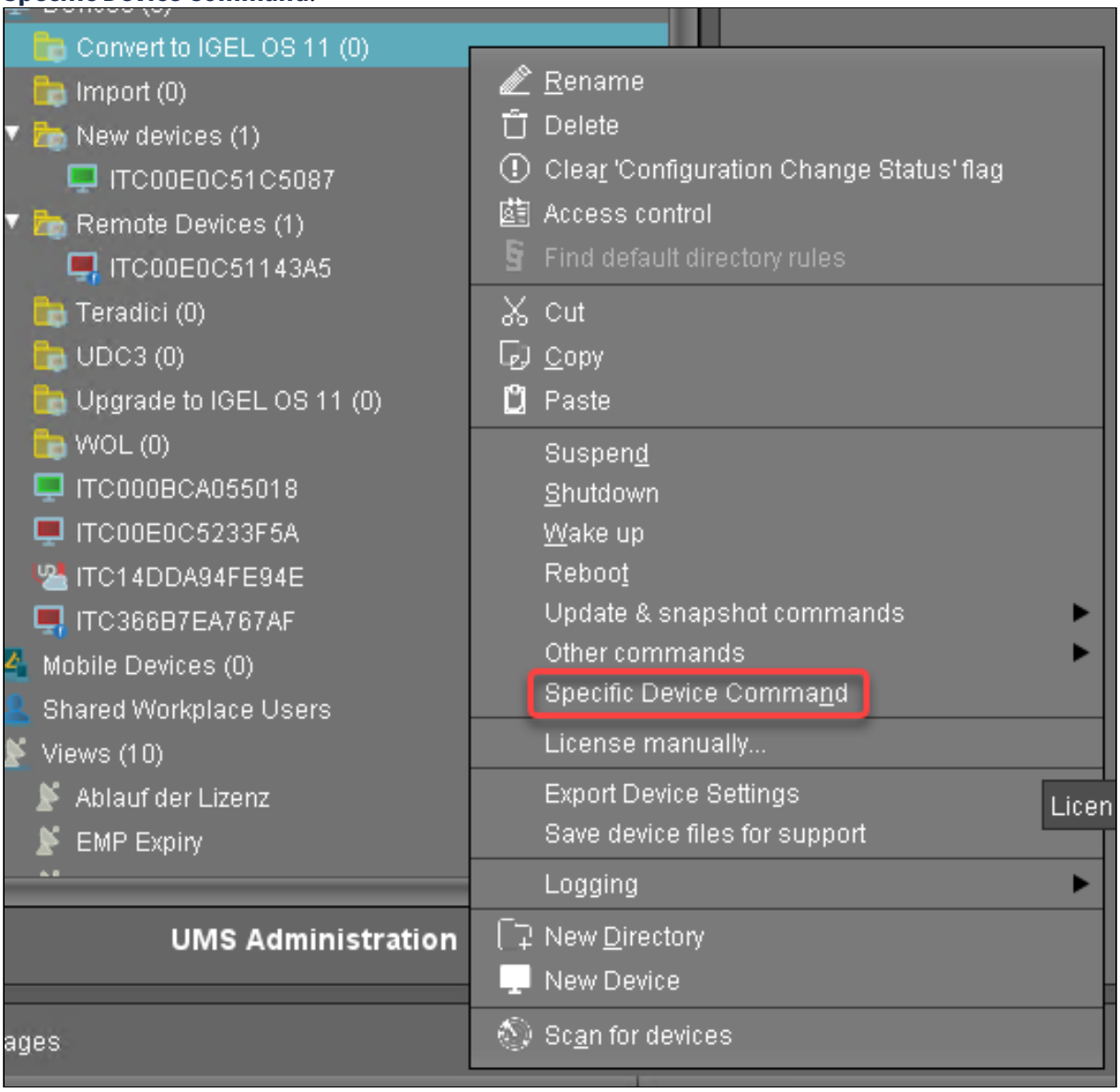
- The conversion profile is assigned to all target machines.
- All target machines have found a buddy update server, which is indicated by the **Firmware Description** "IGEL OSC Ready for Conversion".

Next Step

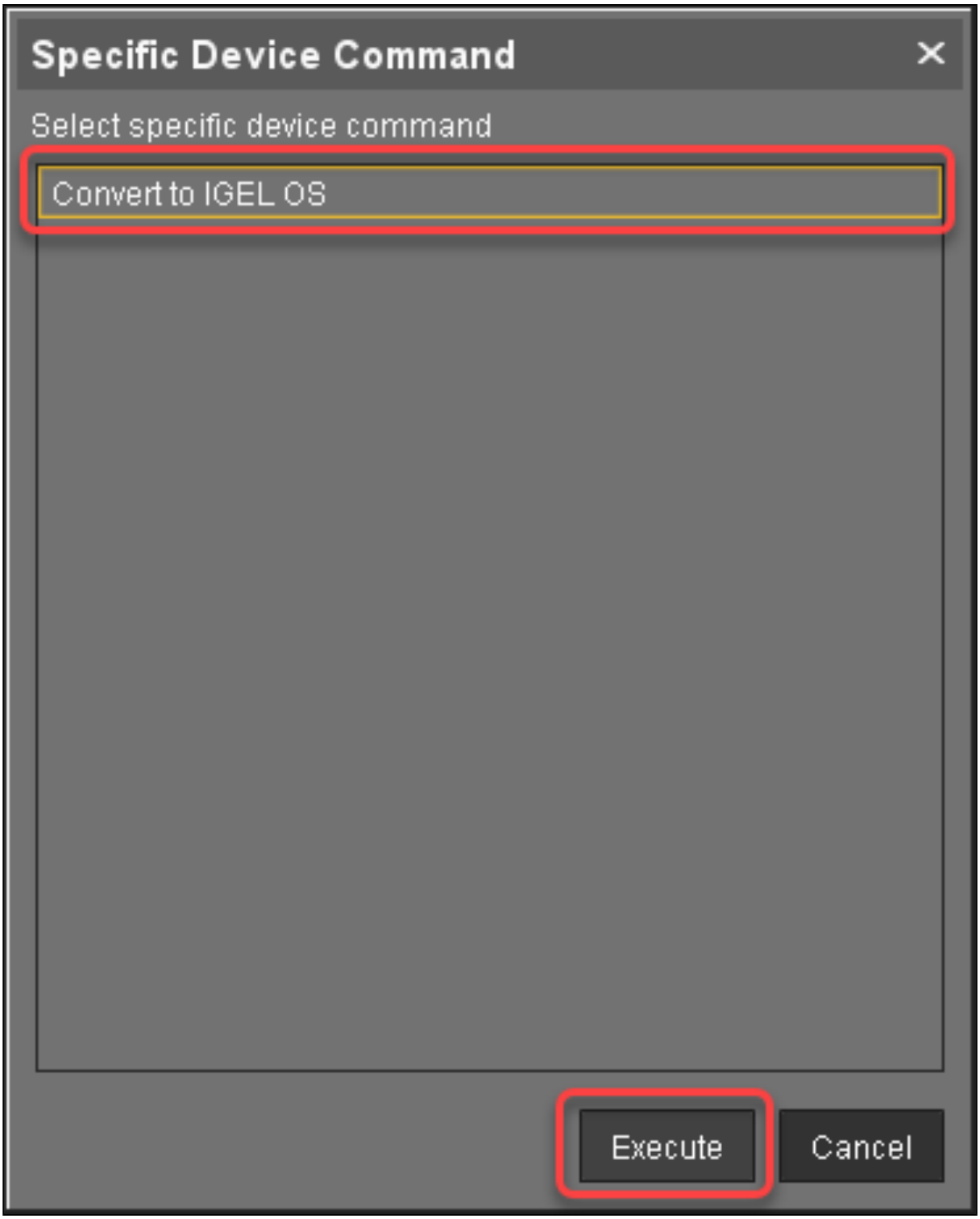
>> Starting the Conversion (see page 2269)

Starting the Conversion

1. Select the directory that contains your target machines, open the context menu, and select **Specific Device Command**.



2. In the **Specific Device Command** dialog, select **Convert to IGEL OS** and click **Execute**.



On the devices, a dialog is displayed. When the dialog is confirmed, the conversion starts

immediately. If the dialog is not confirmed, the conversion starts after 20 seconds.
When the conversion is complete, the **Product** information in the UMS is changed to "IGEL OS 11".

IGEL OS Creator for Windows (OSCW) on IGEL Windows 10 IoT

The IGEL OS Creator (OSC) for Windows is able to convert any device that is running IGEL Windows 10 IoT to IGEL OS 11. The IGEL OS Creator (OSC) for Windows is integrated into version 4.04.150 of IGEL Windows 10 IoT.

> ⚠ The devices will be converted to IGEL OS 11 automatically when the update is executed. The devices cannot be converted back to IGEL Windows 10 IoT.

Read all the following chapters and follow the instructions in the order given.

1. Prerequisites (see page 2273)
2. Getting the Required Software (see page 2274)
3. Starting the Conversion by Updating the Devices (see page 2275)

Prerequisites

Network

- All machines are registered with the UMS.

Next Step

>> When all requirements are met, continue with Getting the Required Software (see page 2274).

Getting the Required Software

The following software must be downloaded resp. installed:

IGEL Universal Management Suite (UMS)

→ Update your UMS to version 6.04.120 or later. For update instructions, see IGEL UMS Update[254].

IGEL Windows 10 IoT

→ Download version 10-4.04.150 from https://www.igel.com/software-downloads/workspace-edition/ **> OSC for Windows > UniversalDesktopW10-4.04.150.zip**.

Check List

- The UMS is available in the correct version.
- The required firmware version for IGEL Windows IoT devices is available.

Next Step

>> Starting the Conversion by Updating the Devices (see page 2275)

254. https://kb.igel.com/en/universal-management-suite/current/igel-ums-update

Starting the Conversion by Updating the Devices

In this step, we will update the devices, which includes the conversion to IGEL OS 11.

> ⚠ The devices will be converted to IGEL OS 11 automatically when the update is executed. The devices cannot be converted back to IGEL Windows 10 IoT.

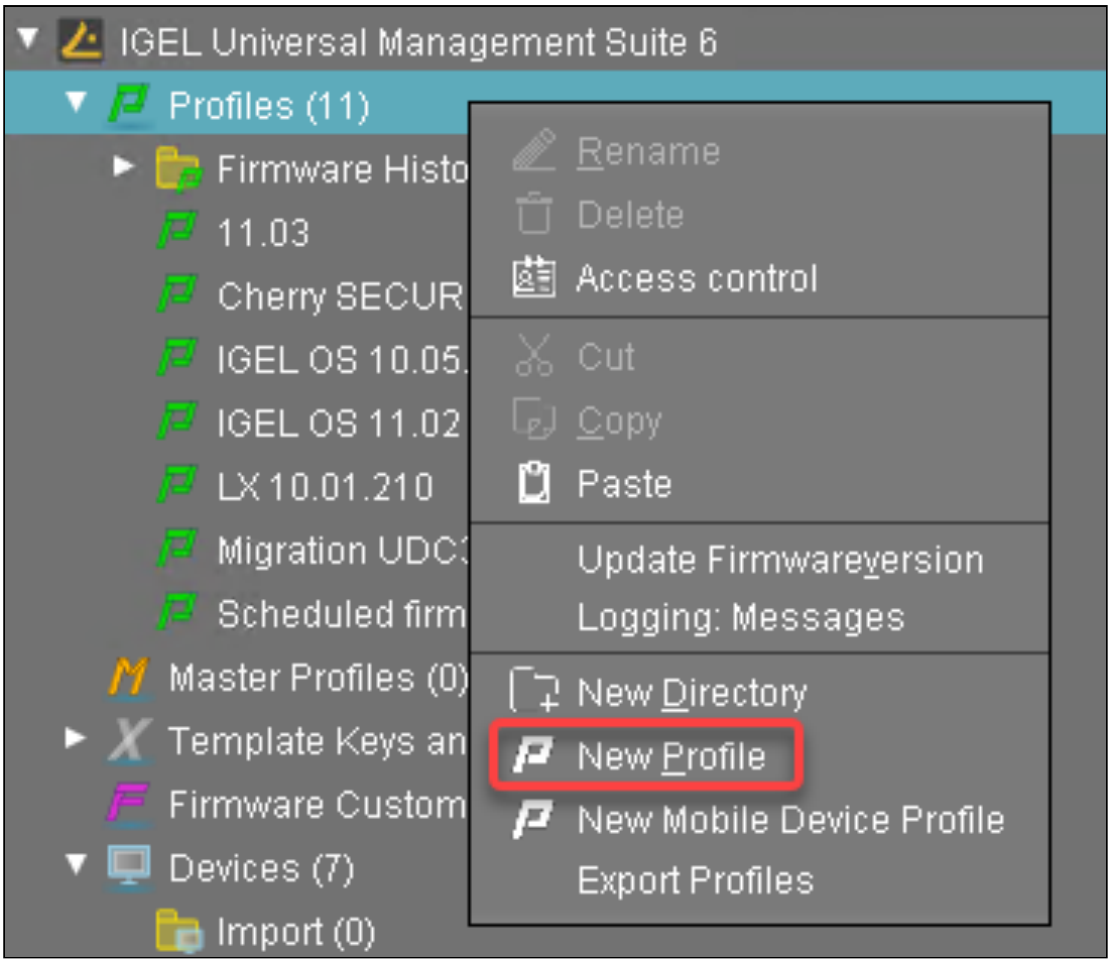
Transferring the Snapshot File to the UMS

The snapshot file must be placed in the file system of the UMS Server.

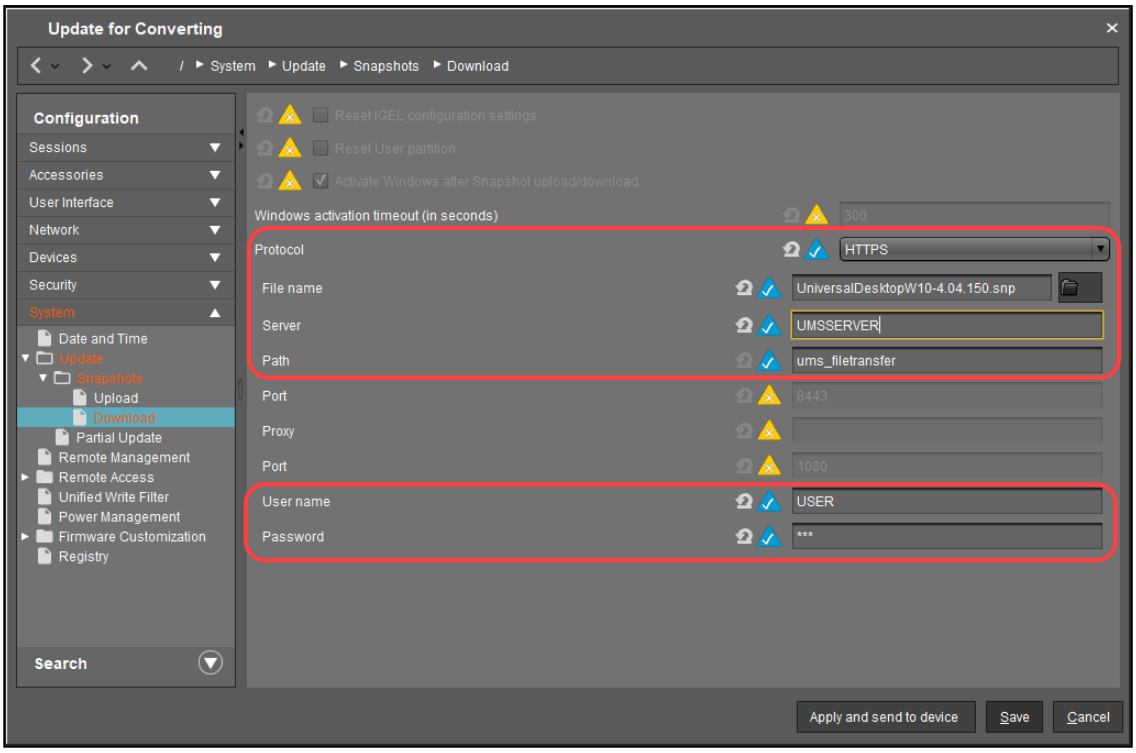
1. Get access to the file system of the machine on which your UMS Server is running.
2. Unzip the snapshot file to `<UMS Installation directory>\rmguiserver\webapps\ums_filetransfer`

Creating an Update Profile

1. In the UMS structure tree, go to **Profiles**, open the context menu, and select **New Profile**.



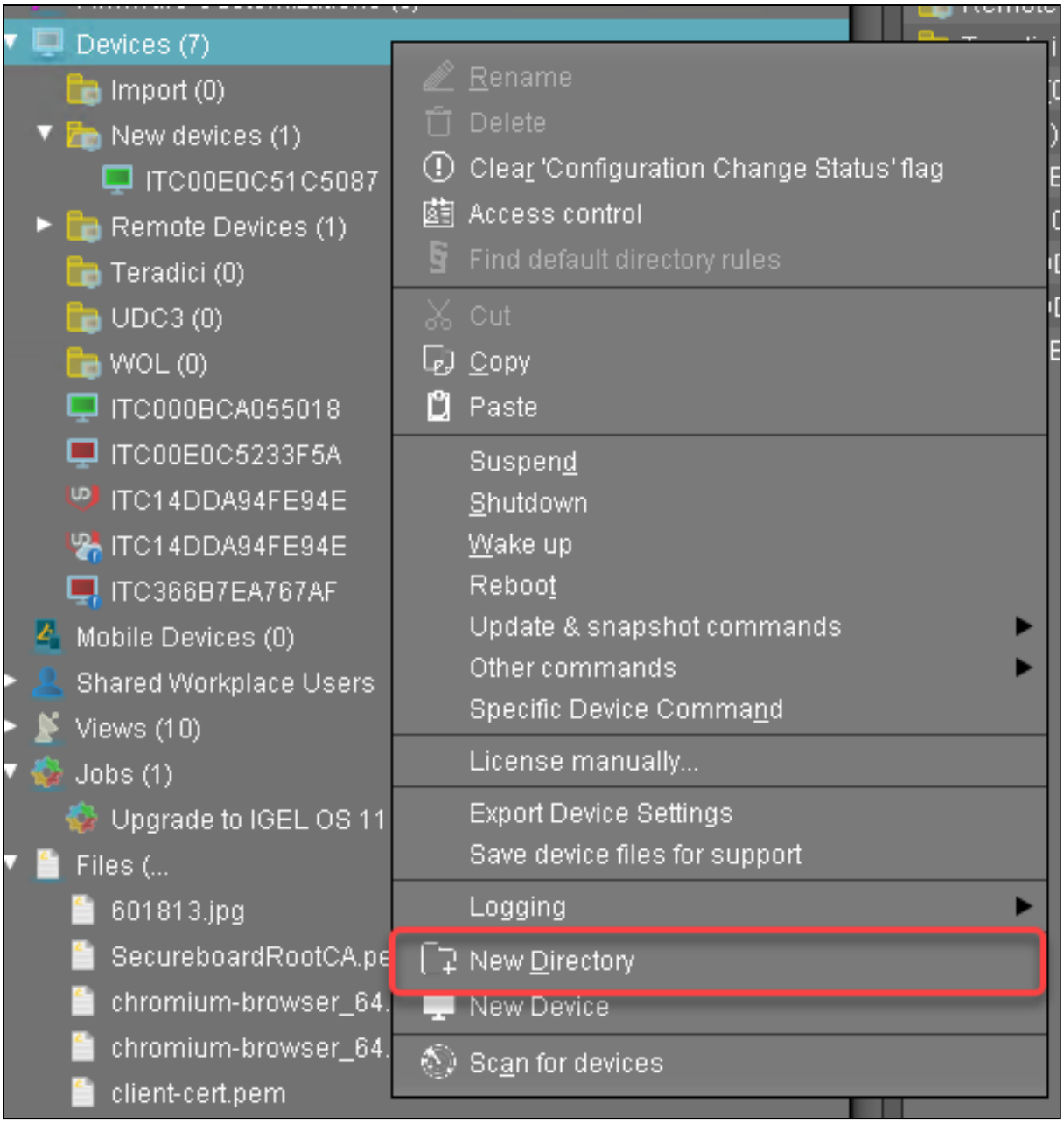
2. Enter the following data:
   - **Profile Name**: Name for the profile, e. g. "Update for Converting".
   - **Description**: Optional description for the profile.
   - **Based on**: Firmware version for the profile; select the current firmware of your devices.
3. Click **Ok**.
4. Go to **System > Update > Snapshots > Download** and change the settings as follows:
   - Select "https" as the **Protocol**.
   - **File name**: Enter the file name of the snapshot file.
   - **Server**: Enter the IP address or hostname of the UMS.
   - **Path**: Enter "ums_filetransfer".
   - **Username**: Enter the user name under which you have access to the UMS.
   - **Password**: Enter the password under which you have access to the UMS.



5. Click **Save** to save the profile.

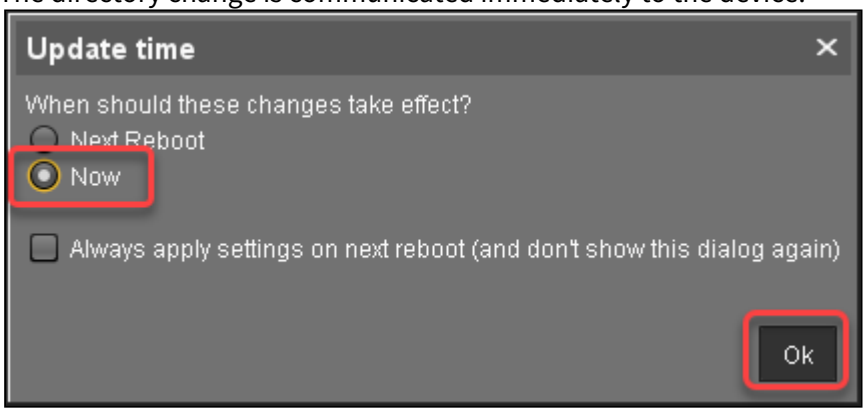
Starting the Update

1. Under **Devices**, create a directory and name it "Convert to IGEL OS 11", for instance.

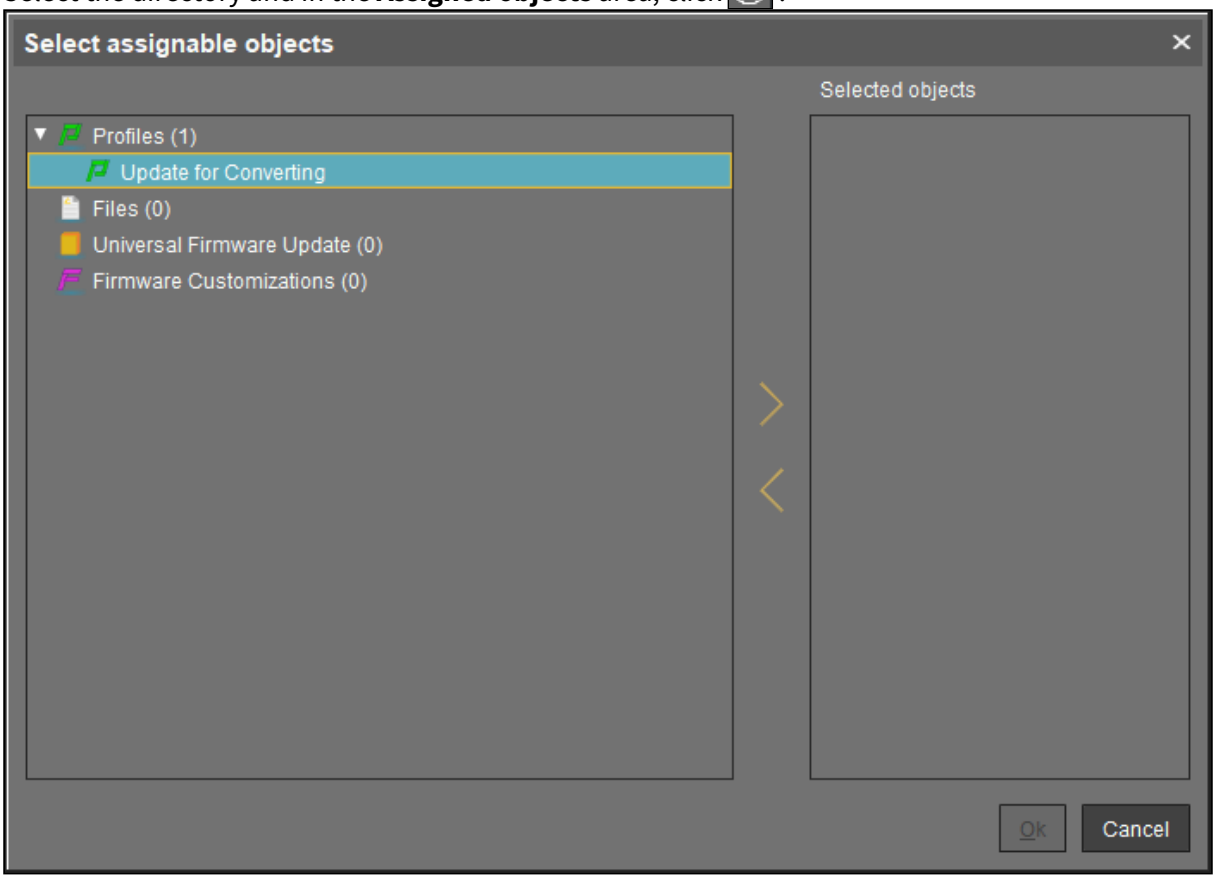


2. Put the devices that are to be updated into the new directory. You can use drag & drop.

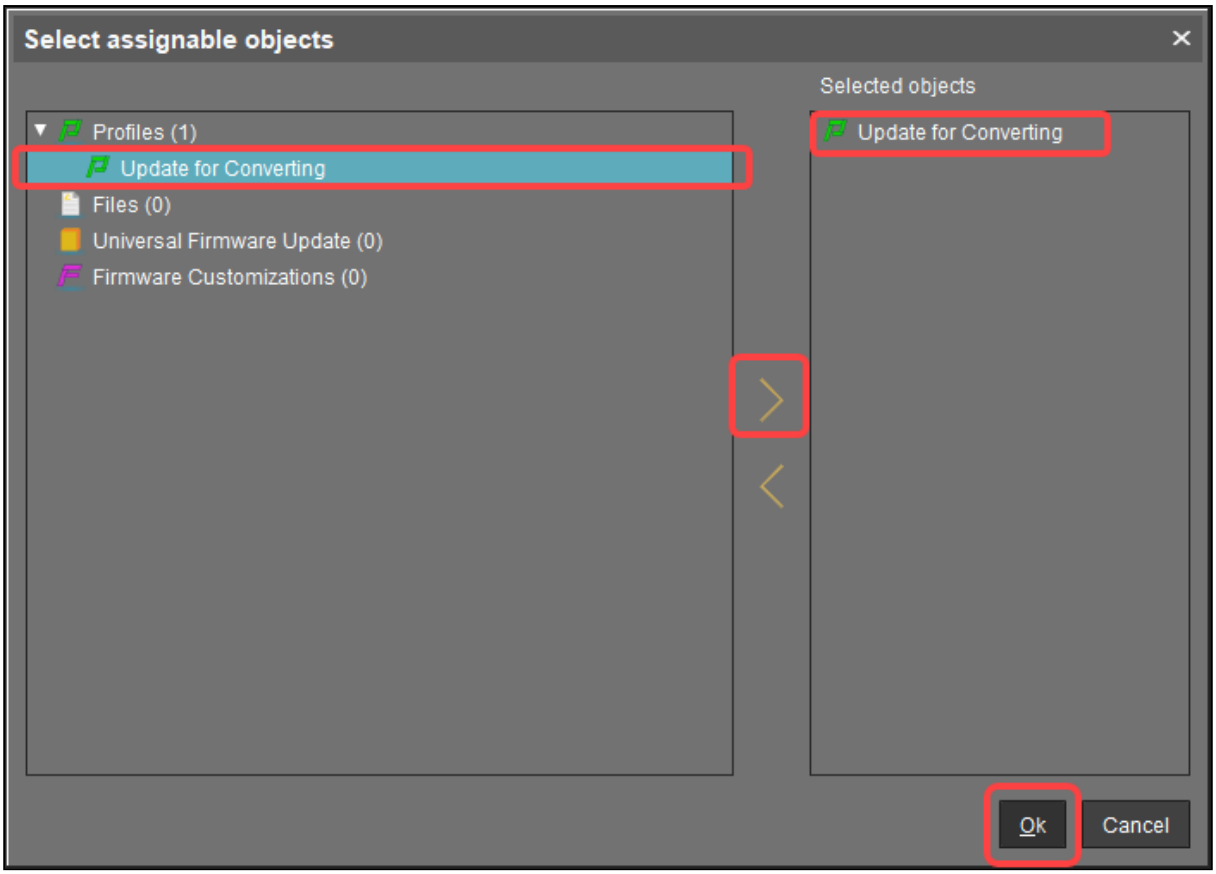
3. In the **Update time** dialog, select **Now** and click **Ok**.
   The directory change is communicated immediately to the device.



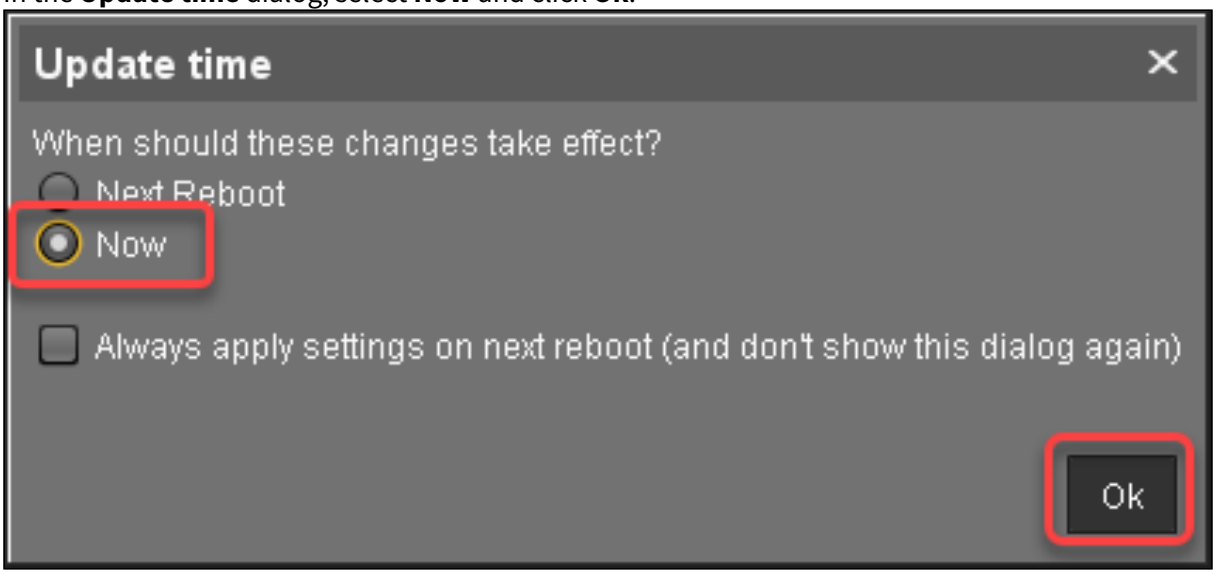
4. Select the directory and in the **Assigned objects** area, click .



5. Assign the update profile to the directory and click **Ok**.

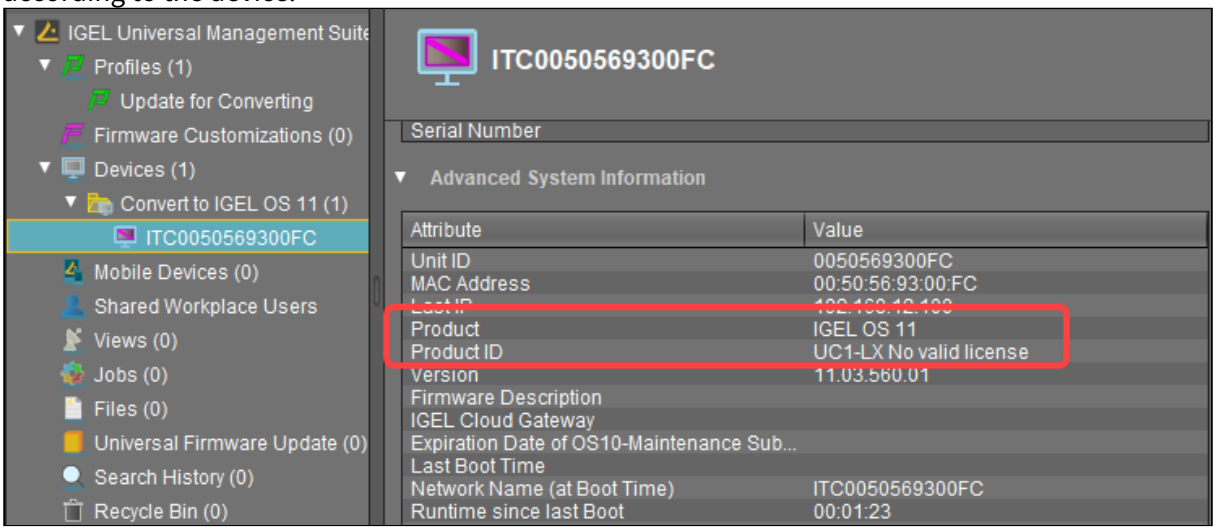


6. In the **Update time** dialog, select **Now** and click **Ok**.



The changes are sent to the devices immediately.

7. Go to the directory that contains the devices that are to be updated and select **Update & snapshot commands > Download Firmware Snapshot**.
   The update and conversion process is started.
8. When the update process is finished, go to one of the devices and click to refresh the screen.
   In the **Advanced System Information** area, **Product** is set to "IGEL OS 11", and **Product ID** is set according to the device.



IGEL OS Release Notes

- Notes for Release 11.10.430 (see page 2284)
- Notes for Release 11.10.410 (see page 2301)
- Notes for Release 11.10.270 (see page 2320)
- Notes for Release 11.10.250 (see page 2336)
- Notes for Release 11.10.210 (see page 2364)
- Notes for Release 11.10.190 (see page 2394)
- Notes for Release 11.10.150 (see page 2410)
- Notes for Release 11.10.120 (see page 2434)
- Notes for Release 11.10.100 (see page 2451)
- Notes for Release 11.09.310 (see page 2477)
- Notes for Release 11.09.260 (see page 2498)
- Notes for Release 11.09.210 (see page 2524)
- Notes for Release 11.09.160 (see page 2545)
- Notes for Release 11.09.150 (see page 2562)
- Notes for Release 11.09.110 (see page 2591)
- Notes for Release 11.09.100 (see page 2609)
- Notes for Release 11.08.440 (see page 2639)
- Notes for Release 11.08.360 (see page 2668)
- Notes for Release 11.08.330 (see page 2688)
- Notes for Release 11.08.290 (see page 2715)
- Notes for Release 11.08.230 (see page 2743)
- Notes for Release 11.08.200 (see page 2766)
- Notes for Release 11.08.110 (see page 2798)
- Notes for Release 11.07.920 (see page 2824)
- Notes for Release 11.07.170 (see page 2846)
- Notes for Release 11.07.140 (see page 2866)
- Notes for Release 11.07.110 (see page 2887)
- Notes for Release 11.07.100 (see page 2906)
- Notes for Release 11.06.250 (see page 2938)
- Notes for Release 11.06.210 (see page 2958)
- Notes for Release 11.05.133 (see page 2959)
- Notes for Release 11.05.120 (see page 2978)
- Notes for Release 11.05.100 (see page 3002)
- Notes for Release 11.04.270 (see page 3061)
- Notes for Release 11.04.240 (see page 3081)
- Notes for Release 11.04.200 (see page 3102)
- Notes for Release 11.04.100 (see page 3122)
- Notes for Release 11.03.500 (see page 3215)
- Notes for Release 11.03.110 (see page 3240)
- Notes for Release 11.03.100 (see page 3258)
- Notes for Release 11.02.150 (see page 3299)
- Notes for Release 11.02.130 (see page 3315)
- Notes for Release 11.02.100 (see page 3329)
- Notes for Release 11.01.130 (see page 3390)

- Notes for Release 11.01.120 (see page 3402)
- Notes for Release 11.01.110 (see page 3413)
- Notes for Release 11.01.100 (see page 3437)

Notes for Release 11.10.430

Software:	Version	11.10.430
Release Date	2025-10-01	
Release Note:	Version	RN-1110430
Last update:	2025-10-01	

- Supported Devices 11.10.430 (see page 2285)
- Security Fixes 11.10.430 (see page 2286)
- Component Versions 11.10.430 (see page 2287)
- Known Issues 11.10.430 (see page 2296)

Supported Devices 11.10.430

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

Security Fixes 11.10.430

Chromium

- Fixed chromium security issues CVE-2025-10585, CVE-2025-10502, CVE-2025-10501, CVE-2025-10500, CVE-2025-9867, CVE-2025-9866, CVE-2025-9865, CVE-2025-9864, CVE-2025-10201 and CVE-2025-10200.
- Updated Chromium Browser to version 140.0.7339.185.

Firefox

- Fixed firefox security issues CVE-2025-9179, CVE-2025-9180 and CVE-2025-9185.
- Updated firefox to version 115.27.0esr.

Component Versions 11.10.430

Clients	
Amazon WorkSpaces Client	4.1.0
Chromium	140.0.7339.185-1igel1758197212
Cisco JVDI Client	15.0.0
Cisco Webex VDI plugin	44.12.1.31417
Cisco Webex Meetings VDI plugin	43.6.8.4
Cisco Webex Meetings VDI plugin	44.10.1.3
Cisco Webex Meetings VDI plugin	44.6.5.1
Zoom Media Plugin	5.17.13.25060
Zoom Media Plugin	6.1.12.25370
Zoom Media Plugin	6.2.10.25600
Citrix EPA Client	24.10.1
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	24.10.1
Citrix Workspace App	20.10.0.6
Citrix Workspace App	24.08.0.98
Citrix Workspace App	24.11.0.85
Omnissa Horizon Client	2412-12437214089
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814

Clients	
Evidian AuthMgr	1.5.8825
Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.1.0.3
FabulaTech USB for Remote Desktop	6.2.1.8
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.27.0
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1730799204
IGEL AVD Client	1.3.0igel1738058087
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_23.2.0.711883_amd64
IGEL Agent for Imprivata	0.6.2igel1739194615
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.12-1igel1721712256
Zulu JRE	17.0.14-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.15.0-1igel1738736251
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17

Clients	
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.14.1+dfsg-1igel1732532698
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation	
Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.5
Philips Speech driver	13.2.3

Signature	
Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.3

Smartcard	
PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.2.3
PKCS#11 Library Thales SafeNet	10.8.1050

Smartcard	
PKCS#11 Library OpenSC	0.26.0-1igel1736250160
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.6.1-2igel1730368961
Reader Driver REINER SCT cyberJack	3.99.5final.sp17-0.1igel1727417566
Resource Manager PC/SC Lite	2.3.1-1igel1736249599
Cherry USB2LAN Proxy	3.2.0.3

System Components	
OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.23
OpenSSL	3.0.2-0ubuntu1.18
OpenSSH Client	9.9p1-3igel1730280218
OpenSSH Server	9.9p1-3igel1730280218
Bluetooth Stack (bluez)	5.79-1igel1732513543
MESA OpenGL Stack	24.2.8-1igel1736252923
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076

System Components	
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.11.0-1igel1738822597
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.3-1igel1738566034
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1751296216
Xorg X11 Server	21.1.15-2igel1736251484
Xorg Xephyr	21.1.15-2igel1736251484
CUPS Printing Daemon	2.4.10-2igel1727672599
PrinterLogic	25.2.0.16
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.12-1igel1738564007
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4

System Components	
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.46.6-1~deb12u1igel1739423750
Python3	3.10.12

VM Guest Support Components	
Virtualbox Guest Utils	7.0.20-dfsg-1igel1726735257
Virtualbox X11 Guest Utils	7.0.20-dfsg-1igel1726735257
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	9.2.0+ds-4igel1736508561

Features with Limited IGEL Support	
Mobile Device Access USB (MTP)	1.1.22-1igel1736514321
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-3igel1732526151
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.20-dfsg-1igel1726735257
Virtual Background for Webcam	

Services	Size	Reduced Firmware
Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.2M	Included
Citrix Appliance Citrix StoreFront Citrix Workspace app	711.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Citrix Appliance Local Browser (Firefox)	86.2M	Included
RDP Omnissa Horizon	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
Omnissa Horizon	213.5M	Included
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.0M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	129.2M	Not included
Imprivata Appliance	32.5M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	11.0M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included

Services	Size	Reduced Firmware
Cisco JVDI client	61.2M	Included
PrinterLogic	47.2M	Not included
Login VSI Login Enterprise	28.0M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.2M	Not included
AVD	48.5M	Included
Local Browser (Chromium)	153.8M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	103.2M	Not included
Cisco Webex Meetings VDI	176.8M	Not included
Zoom Media Plugin	201.5M	Not included
DriveLock	12.2M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.5M	Included
90meter Smart Card Support	512.0K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Scanner support / SANE (Limited support) Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support)	256.0K	Not included

Services	Size	Reduced Firmware
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	7.8M	Not included
Virtualbox (Limited support)	73.5M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.5M	Included

Known Issues 11.10.430

Citrix

- Keyboard sync mode selection **once/dynamic/off** results in unexpected behavior.
- Citrix Cloud login with Citrix Workspace app 20.10 not possible
- Citrix StoreFront login to the cloud stores with Password authentication type may not work due to the n-factor authentication enforced by Microsoft. Switch to Citrix login type as a workaround.
- If the user logs out via the Self-service drop down menu, the user data is not deleted correctly by Citrix. As a result, a re-login can be performed without new authentication. To remove all user credentials the self-service window should always be closed when logging off.
- Citrix proxy connections can fail if they are set up in an environment that only allows external connections through a proxy and restricts DNS queries.
- With the new Citrix toolbar, desktops may unexpectedly switch from windowed mode to full-screen mode when a monitor was suspended. As a workaround, you can revert to the previous version of the toolbar by setting the `ica.wfclient.toolbarversion` parameter to "Old".
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher .
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- AVD is not running on devices that do not support SSE4.1 at least. Use older IGEL OS firmware versions like 11.09.xxx or older!
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

Remote Desktop (RDP3)

- RDP3 is not running on devices that do not support SSE4.1 at least. Use the legacy RDP client instead.

RD Web Access

- Client is not running on devices that do not support SSE4.1 at least. Use RD Web Access with the legacy RDP client instead.

Horizon

- Horizon session uses the configured system proxy, even if "Direct connection to the Internet" is set for the session
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.

- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

IGEL Agent for Imprivata

- Filter horizon apps on chooser does not work, apps will show in any case. The recommendation is to set "`iia.hide_horizon_apps_on_chooser`" to "False"

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base System

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Migration

- The migration process may hang around 24% when attempting to upgrade from IGEL OS 11 versions earlier than 11.10.410, if the target IGEL OS 12 image includes partitions larger or equal to 1 GB. Target IGEL OS 12 versions 12.8.x and later will run in to this issue.

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher[255] for a possible solution and additional information.

Appliance Mode

- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some HP devices will shut down instead of restarting during the BIOS update procedure. After manual boot of the devices, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g. via UMS) does not seem to work in

255. https://kb.igel.com/en/igel-os/current/error-not-enough-space-on-local-drive-when-updatin

this state, either.
The BIOS is still updated successfully. This is currently known for HP mt645 G7 and mt645 G8.

- After updating the BIOS of the HP Elite mt645 G7 Mobile Thin Client to version 1.15 or higher, any attempt to update the BIOS is going to freeze the BIOS update process.
  Currently there is no way to change the BIOS version after the system has been updated to BIOS version 1.15 or higher.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 G3 and mt645 G7/G8.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-LAN via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  - It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Notes for Release 11.10.410

Software:	Version	11.10.410
Release Date	2025-07-23	
Release Note:	Version	RN-1110410
Last update:	2025-07-23	

- Supported Devices 11.10.410 (see page 2302)
- New Features 11.10.410 (see page 2303)
- Security Fixes 11.10.410 (see page 2304)
- Resolved Issues 11.10.410 (see page 2305)
- Component Versions 11.10.410 (see page 2306)
- Known Issues 11.10.410 (see page 2315)

Supported Devices 11.10.410

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

New Features 11.10.410

Base system

- Added downgrade limit - The IGEL OS11 can no longer be downgraded to versions older than 11.10.410. This restriction applies to IGEL UD Pocket devices and endpoints with Secure Boot enabled. In such cases, downgrade attempts to versions prior to 11.10.410 will be refused to maintain system integrity and boot security.
- Added migration restriction - The OS11 can no longer be migrated to versions older than 12.7.0. This restriction applies to IGEL UD Pocket devices and endpoints with Secure Boot enabled. In such cases, migration attempts to versions prior to 12.7.0 will be refused to maintain system integrity and boot security.

For details, see Upgrade and Downgrade Limit on IGEL OS 11.10.410 or Higher (see page 24) .

- Updated boot chain with
- New SHIM 15.8, signed by Microsoft
- New GRUB 2.12

Security Fixes 11.10.410

Chromium

- Fixed Chromium security issues CVE-2025-6557, CVE-2025-6556, CVE-2025-6555, CVE-2025-6554, CVE-2025-6192, CVE-2025-6191, CVE-2025-5959, CVE-2025-5958, CVE-2025-5419, CVE-2025-5283, CVE-2025-5281, CVE-2025-5280, CVE-2025-5068, CVE-2025-5067, CVE-2025-5066, CVE-2025-5065, CVE-2025-5064 and CVE-2025-5063.
- Updated chromium to version 138.0.7204.92.

Network

- Fixed ppp security issue CVE-2024-58250.

Base system

- Fixed ISN 2025-24: Command Execution in IGEL OS.

Resolved Issues 11.10.410

Base system

- Fixed an issue which caused the migration from OS 11 to OS 12 to fail if the OS 12 system partition is larger than 1 GB. So far, no OS 12 system partition falls into this category but future versions of OS 12 may be affected.

Component Versions 11.10.410

Clients	
Amazon WorkSpaces Client	4.1.0
Chromium	138.0.7204.92-1igel1751432214
Cisco JVDI Client	15.0.0
Cisco Webex VDI plugin	44.12.1.31417
Cisco Webex Meetings VDI plugin	43.6.8.4
Cisco Webex Meetings VDI plugin	44.10.1.3
Cisco Webex Meetings VDI plugin	44.6.5.1
Omnissa Horizon Client	2412-12437214089
Zoom Media Plugin	5.17.13.25060
Zoom Media Plugin	6.1.12.25370
Zoom Media Plugin	6.2.10.25600
Citrix EPA Client	24.10.1
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	24.10.1
Citrix Workspace App	20.10.0.6
Citrix Workspace App	24.08.0.98
Citrix Workspace App	24.11.0.85
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814

Clients	
Evidian AuthMgr	1.5.8825
Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.1.0.3
FabulaTech USB for Remote Desktop	6.2.1.8
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.24.0
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1730799204
IGEL AVD Client	1.3.0igel1738058087
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_23.2.0.711883_amd64
IGEL Agent for Imprivata	0.6.2igel1739194615
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.12-1igel1721712256
Zulu JRE	17.0.14-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.15.0-1igel1738736251
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17

Clients	
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.14.1+dfsg-1igel1732532698
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation	
Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.5
Philips Speech driver	13.2.3

Signature	
Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.3

Smartcard	
PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.2.3
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.26.0-1igel1736250160
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38

Smartcard	
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.6.1-2igel1730368961
Reader Driver REINER SCT cyberJack	3.99.5final.sp17-0.1igel1727417566
Resource Manager PC/SC Lite	2.3.1-1igel1736249599
Cherry USB2LAN Proxy	3.2.0.3

System Components	
OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.23
OpenSSL	3.0.2-0ubuntu1.18
OpenSSH Client	9.9p1-3igel1730280218
OpenSSH Server	9.9p1-3igel1730280218
Bluetooth Stack (bluez)	5.79-1igel1732513543
MESA OpenGL Stack	24.2.8-1igel1736252923
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009

System Components	
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.11.0-1igel1738822597
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.3-1igel1738566034
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1751296216
Xorg X11 Server	21.1.15-2igel1736251484
Xorg Xephyr	21.1.15-2igel1736251484
CUPS Printing Daemon	2.4.10-2igel1727672599
PrinterLogic	25.2.0.16
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.12-1igel1738564007
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1

System Components	
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.46.6-1~deb12u1igel1739423750
Python3	3.10.12

VM Guest Support Components	
Virtualbox Guest Utils	7.0.20-dfsg-1igel1726735257
Virtualbox X11 Guest Utils	7.0.20-dfsg-1igel1726735257
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	9.2.0+ds-4igel1736508561

Features with Limited IGEL Support	
Mobile Device Access USB (MTP)	1.1.22-1igel1736514321
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-3igel1732526151
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.20-dfsg-1igel1726735257
Virtual Background for Webcam	

Services	Size	Reduced Firmware
Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.2M	Included
Citrix StoreFront Citrix Appliance Citrix Workspace app	711.0 M	Included
Ericom PowerTerm InterConnect	10.0M	Included

Services	Size	Reduced Firmware
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.2M	Included
Omnissa Horizon RDP	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
Omnissa Horizon	213.5 M	Included
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.0M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	129.2 M	Not included
Imprivata Appliance	32.5M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	11.0M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.2M	Included
PrinterLogic	47.2M	Not included
Login VSI Login Enterprise	28.0M	Not included

Services	Size	Reduced Firmware
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.2M	Not included
AVD	48.5M	Included
Local Browser (Chromium)	156.0 M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	103.2 M	Not included
Cisco Webex Meetings VDI	176.8 M	Not included
Zoom Media Plugin	201.5 M	Not included
DriveLock	12.2M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.5M	Included
90meter Smart Card Support	512.0K	Included
Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) Virtual Background for Webcam (Limited IGEL Support) Scanner support / SANE (Limited support) VPN OpenConnect (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	7.8M	Not included

Services	Size	Reduced Firmware
Virtualbox (Limited support)	73.5M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.5M	Included

Known Issues 11.10.410

Citrix

- Keyboard sync mode selection once/dynamic/off results in unexpected behavior.
- Citrix Cloud login with Citrix Workspace app 20.10 not possible
- Citrix StoreFront login to the cloud stores with Password authentication type may not work due to the n-factor authentication enforced by Microsoft. Switch to Citrix login type as a workaround.
- If the user logs out via the Self-service drop down menu, the user data is not deleted correctly by Citrix. As a result, a re-login can be performed without new authentication. To remove all user credentials the self-service window should always be closed when logging off.
- Citrix proxy connections can fail if they are set up in an environment that only allows external connections through a proxy and restricts DNS queries.
- With the new Citrix toolbar, desktops may unexpectedly switch from windowed mode to full-screen mode when a monitor was suspended. As a workaround, you can revert to the previous version of the toolbar by setting the ica.wfclient.toolbarversion parameter to "Old".
- Citrix H.264 acceleration plugin does not work with enabled server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.

- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- AVD is not running on devices that don't support SSE4.1 at least. Use older IGEL OS firmware versions like 11.09.xxx or older!
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

Remote Desktop (RDP3)

- RDP3 is not running on devices that don't support SSE4.1 at least. Use the legacy RDP client instead.

RD Web Access

- Client is not running on devices that don't support SSE4.1 at least. Use RdWebAccess with the legacy RDP client instead.

Horizon

- Horizon session uses the configured system proxy, even if "Direct connection to the Internet" is set for the session
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  vmware.view.enable-serial-port-redir
  vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.

- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

IGEL Agent for Imprivata

- Filter horizon apps on chooser does not work, apps will show in any case. The recommendation is to set "iia.hide_horizon_apps_on_chooser" to "False"

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher[256] for a possible solution and additional information.

Appliance Mode

- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The **Console Invocation** has to allow **Native client** (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'`

Audio

- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some HP devices will shut down instead of restarting during the BIOS update procedure. After manual boot of the devices, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g. via UMS) does not seem to work in this state, either.
  The BIOS is still updated successfully. This is currently known for HP mt645 G7 and mt645 G8.
- After updating the BIOS of the HP Elite mt645 G7 Mobile Thin Client to version 1.15 or higher, any attempt to update the BIOS is going to freeze the BIOS update process.

256. https://kb.igel.com/en/igel-os/11.10.270/error-not-enough-space-on-local-drive-when-updatin

Currently there is no way to change the BIOS version after the system has been updated to BIOS version 1.15 or higher.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 G3 and mt645 G7/G8.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  ** It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Notes for Release 11.10.270

Software:	Version	11.10.270
Release Date	2025-04-03	
Release Note:	Version	RN-1110270
Last update:	2025-04-03	

- Support Devices 11.10.270 (see page 2321)
- Security Fixes 11.10.270 (see page 2322)
- Component Versions 11.10.270 (see page 2323)
- Known Issues 11.10.270 (see page 2331)

Support Devices 11.10.270

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

Security Fixes 11.10.270

Chromium

- Updated Chromium to version 134.0.6998.117
- Fixed Chromium security issues
  CVE-2025-2476, CVE-2025-24201, CVE-2025-2137, CVE-2025-2136, CVE-2025-2135, CVE-2025-1923, CVE-2025-1922, CVE-2025-1921, CVE-2025-1920, CVE-2025-1919, CVE-2025-1918, CVE-2025-1917, CVE-2025-1916, CVE-2025-1915, CVE-2025-1914, CVE-2025-1426, CVE-2025-1006, CVE-2025-0999, CVE-2025-0998, CVE-2025-0997, CVE-2025-0996 and CVE-2025-0995.

Component Versions 11.10.270

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	134.0.6998.117-1igel1742471945
Cisco JVDI Client	15.0.0
Cisco Webex VDI plugin	44.12.1.31417
Cisco Webex Meetings VDI plugin	43.6.8.4
Cisco Webex Meetings VDI plugin	44.10.1.3
Cisco Webex Meetings VDI plugin	44.6.5.1
Zoom Media Plugin	5.17.13.25060
Zoom Media Plugin	6.1.12.25370
Zoom Media Plugin	6.2.10.25600
Citrix EPA Client	24.10.1
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	24.10.1
Citrix Workspace App	20.10.0.6
Citrix Workspace App	24.08.0.98
Citrix Workspace App	24.11.0.85
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.1.0.3
FabulaTech USB for Remote Desktop	6.2.1.8
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.20.0
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1730799204
IGEL AVD Client	1.3.0igel1738058087
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_23.2.0.711883_amd64
IGEL Agent for Imprivata	0.6.2igel1739194615
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.12-1igel1721712256
Zulu JRE	17.0.14-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.15.0-1igel1738736251
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.14.1+dfsg-1igel1732532698
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.5
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.3

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.26.0-1igel1736250160
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.6.1-2igel1730368961
Reader Driver REINER SCT cyberJack	3.99.5final.sp17-0.1igel1727417566
Resource Manager PC/SC Lite	2.3.1-1igel1736249599
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.23
OpenSSL	3.0.2-0ubuntu1.18
OpenSSH Client	9.9p1-3igel1730280218
OpenSSH Server	9.9p1-3igel1730280218
Bluetooth Stack (bluez)	5.79-1igel1732513543
MESA OpenGL Stack	24.2.8-1igel1736252923
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.11.0-1igel1738822597
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.3-1igel1738566034

Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1738661271
Xorg X11 Server	21.1.15-2igel1736251484
Xorg Xephyr	21.1.15-2igel1736251484
CUPS Printing Daemon	2.4.10-2igel1727672599
PrinterLogic	25.2.0.16
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.12-1igel1738564007
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.46.6-1~deb12u1igel1739423750
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.20-dfsg-1igel1726735257
Virtualbox X11 Guest Utils	7.0.20-dfsg-1igel1726735257
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1

Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	9.2.0+ds-4igel1736508561

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.22-1igel1736514321
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-3igel1732526151
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.20-dfsg-1igel1726735257
Virtual Background for Webcam	

Services

Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.2M	Included
Citrix StoreFront Citrix Appliance Citrix Workspace app	711.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.2M	Included
RDP Omnissa Horizon	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
Omnissa Horizon	213.5M	Included
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.0M	Included

IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	129.2M	Not included
Imprivata Appliance	32.5M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	11.0M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.2M	Included
PrinterLogic	47.2M	Not included
Login VSI Login Enterprise	28.0M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.2M	Not included
AVD	48.5M	Included
Local Browser (Chromium)	114.8M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	103.2M	Not included
Cisco Webex Meetings VDI	176.8M	Not included

Zoom Media Plugin	201.5M	Not included
DriveLock	12.2M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.5M	Included
90meter Smart Card Support	512.0K	Included
Virtualbox (Limited support) Limited Support Features Scanner support / SANE (Limited support) VPN OpenConnect (Limited support) Virtual Background for Webcam (Limited IGEL Support) Mobile Device Access USB (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	7.8M	Not included
Virtualbox (Limited support)	73.5M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.5M	Included

Known Issues 11.10.270

Citrix

- Keyboard sync mode selection once/dynamic/off results in unexpected behavior.
- Citrix Cloud login with Citrix Workspace app 20.10 not possible
- Citrix StoreFront login to the cloud stores with Password authentication type may not work due to the n-factor authentication enforced by Microsoft. Switch to Citrix login type as a workaround.
- If the user logs out via the Self-service drop down menu, the user data is not deleted correctly by Citrix. As a result, a re-login can be performed without new authentication. To remove all user credentials the self-service window should always be closed when logging off.
- Citrix proxy connections can fail if they are set up in an environment that only allows external connections through a proxy and restricts DNS queries.
- With the new Citrix toolbar, desktops may unexpectedly switch from windowed mode to full-screen mode when a monitor was suspended. As a workaround, you can revert to the previous version of the toolbar by setting the ica.wfclient.toolbarversion parameter to "Old".
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.

- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- AVD is not running on devices that don't support SSE4.1 at least. Use older IGEL OS firmware versions like 11.09.xxx[257] or older!
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

Remote Desktop (RDP3)

- RDP3 is not running on devices that don't support SSE4.1 at least. Use the legacy RDP client instead.

RD Web Access

- Client is not running on devices that don't support SSE4.1 at least. Use RdWebAccess with the legacy RDP client instead.

Horizon

- Horizon session uses the configured system proxy, even if "Direct connection to the Internet" is set for the session
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  vmware.view.enable-serial-port-redir
  vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.

257. http://11.09.xxx

- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

IGEL Agent for Imprivata

- Filter horizon apps on chooser does not work, apps will show in any case. The recommendation is to set "iia.hide_horizon_apps_on_chooser" to "False"

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g.�if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://kb.igel.com/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow `Native` client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch`

Audio

- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some HP devices will shut down instead of restarting during the BIOS update procedure. After manual boot of the devices, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g.via UMS) does not seem to work in this state, either.
  The BIOS is still updated successfully. This is currently known for HP mt645 G7 and mt645 G8.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 G3 and mt645 G7/G8.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.

- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  ** It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Notes for Release 11.10.250

Software:	Version	11.10.250
Release Date	2025-03-11	
Release Note:	Version	RN-1110250
Last update:	2025-03-11	

Supported Devices 11.10.250

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

New Features 11.10.250

Citrix

Integrated Citrix Workspace app 24.08.0.98

New Features:

- Enhanced virtual desktop screen resizing experience:

Parameter	Enhanced virtual desktop screen resizing experience
Registry	ica.wfclient.EnhancedResizingEnabled
Value	false / true (default)

- Performance improvement of graphics usage by supporting OpenGL library:

Parameter	OpenGLEnabled
Registry	ica.wfclient.OpenGLEnabled
Value	false (default) / true

- Performance improvement using H265 encoding (requires OpenGLEnabled=true):

Parameter	H265Enabled
Registry	ica.wfclient.H265Enabled
Value	false (default) / true

- Multiple webcam resolutions support:

Parameter	HDXWebcamEnablePnp
Registry	ica.wfclient.hdxwebcamenablepnp
Type	bool
Value	true (default) / false

- Integrated Citrix Workspace app 24.11.0.85.
- The default value for the parameter “ica.module.enableechocancellation” was set to True and thus corresponds to the Citrix default value.
- Citrix Workspace app for Linux ensures a smooth transition and prevents black screens and flickers when resizing or stretching your virtual desktop screen.
  The two parameters ica.wfclient.DesktopLaunchEnhancement and ica.wfclient.EnhancedResizingEnabled are active by default.

Parameter	Enhanced desktop launch experience

Registry	ica.wfclient.DesktopLaunchEnhancement
Type	bool
Value	**true** (default)/ false

- Support for redirecting Human Interface Device (HID) devices from endpoint to Unified Communication SDK application on VDI

Parameter	EnableHDI
Registry	ica.teams.enablehid.enabled
Type	bool
Value	**false** (default)/ true

- The default value of the ica.wfclient.toolbarversion parameter has been changed to “New” to avoid random session interruptions when resizing the screen. This change will cause the newer Citrix toolbar to be used by default.
- Support for further customization of the new connection bar and new available connection button

Parameter	SwitchDesktopButtonVisible
Registry	ica.wfclient.switchdesktopbuttonvisible
Type	bool
Value	**true** (default)/ false
Parameter	FullscreenButtonVisible
Registry	ica.wfclient.FullscreenButtonVisible
Type	bool
Value	**true** (default)/ false
Parameter	MultiMonitorSelectionEnabled
Registry	ica.wfclient.multimonitorselectionenabled
Type	bool
Value	**true** (default)/ false

- The following 5 setlog parameters have been added.

Parameter	Google Analytics
Registry	ica.setlog.level.all_.an
Parameter	Multi Touch
Registry	ica.setlog.level.all_.mtch

Parameter	Fido2
Registry	ica.setlog.level.all_.fido2
Parameter	Service Continuity
Registry	ica.setlog.level.all_.svccont
Parameter	Storebrowse
Registry	ica.setlog.level.all_.stb

- In this version Citrix identifies monitor 1 as 0, so the code has been adjusted with the following parameter to work exactly like previous workspace apps.

Parameter	Left Shift Monitor Number
Registry	ica.destination_window.downshiftmonitors
Type	bool
Value	**true** (default)/ false

AVD

- Updated AVD client to version 1.3.0

Horizon

- Updated Horizon Client to version 2412-12437214089

HID

- Added new registry keys to influence mouse acceleration settings:

Parameter	Use new mouse accel variant
Registry	userinterface.mouse.use_new_accel_variant
Type	bool
Value	enabled / **disabled** (default)

Parameter	Enable mouse acceleration (only for new accel variant)
Registry	userinterface.mouse.enable_acceleration
Type	bool
Value	**enabled** (default) / disabled

CUPS Printing

- Updated Vasion Print (former PrinterLogic) Printer Installer Client to version 25.2.0.16.

- Reset writable partition in case of IGEL OS updates but keep printer mapping.

Cisco Webex

- Updated Cisco Webex VDI version to 44.12.1.31417

Base system

- Support for migration to IGEL OS 12 for the trust-based license (GOV) version has been added.
- Updated the End User License Agreement (EULA) to the February 2025 version.

Olympus

- Updated Olympus driver to 4.0.5 and added a new udev rule.
- New device names mapping

Old device name	New device name
Olympus DS	9000| OM SYSTEM DS9100
Olympus Re	cMic II 4010p| OM SYSTEM – RecMic II 4010n
Olympus Re	cMic II 4110s| OM SYSTEM – RecMic II 4110n
Olympus RS	28H| OM SYSTEM RS28N
Olympus RS	31H| OM SYSTEM RS31N

zoomvdi

- Updated Zoom Media Plugins for VDI to version 6.2.10.25600.

Fabulatech

- Updated FabulaTech USB to version 6.2.1.8.
- Updated FabulaTech Plugins to version 4.1.0.3.

Security Fixes 11.10.250

Chromium

- Fixed Chromium security issues
  CVE-2024-10488, CVE-2024-10487, CVE-2024-10231, CVE-2024-10230, CVE-2024-10229, CVE-2024-9966, CVE-2024-9965, CVE-2024-9964, CVE-2024-9963, CVE-2024-9962, CVE-2024-9961, CVE-2024-9960, CVE-2024-9959, CVE-2024-9958, CVE-2024-9957, CVE-2024-9956, CVE-2024-9955, CVE-2024-9954, CVE-2024-9603, CVE-2024-9602, CVE-2024-9370, CVE-2024-9369, CVE-2024-9123, CVE-2024-9122, CVE-2024-9121, CVE-2024-9120, CVE-2024-8909, CVE-2024-8908, CVE-2024-8907, CVE-2024-8906, CVE-2024-8905, CVE-2024-8904, CVE-2024-8639, CVE-2024-8638, CVE-2024-8637, CVE-2024-8636 and CVE-2024-7025.
- Fixed Chromium security issues
  CVE-2024-8362, CVE-2024-7970, CVE-2024-8198, CVE-2024-8194, CVE-2024-8193, CVE-2024-8035, CVE-2024-8034, CVE-2024-8033, CVE-2024-7981, CVE-2024-7980, CVE-2024-7979, CVE-2024-7978, CVE-2024-7977, CVE-2024-7976, CVE-2024-7975, CVE-2024-7974, CVE-2024-7973, CVE-2024-7972, CVE-2024-7971, CVE-2024-7969, CVE-2024-7968, CVE-2024-7967, CVE-2024-7966, CVE-2024-7965 and CVE-2024-7964.
- Fixed chromium security issues
  CVE-2025-0451, CVE-2025-0445, CVE-2025-0444, CVE-2025-0762, CVE-2025-0612, CVE-2025-0611, CVE-2025-0448, CVE-2025-0447, CVE-2025-0446, CVE-2025-0443, CVE-2025-0442, CVE-2025-0441, CVE-2025-0440, CVE-2025-0439, CVE-2025-0438, CVE-2025-0437, CVE-2025-0436, CVE-2025-0435, CVE-2025-0434, CVE-2025-0291, CVE-2024-12695, CVE-2024-12694, CVE-2024-12693, CVE-2024-12692, CVE-2024-12382, CVE-2024-12381, CVE-2024-12053, CVE-2024-11395, CVE-2024-11117, CVE-2024-11116, CVE-2024-11115, CVE-2024-11114, CVE-2024-11113, CVE-2024-11112, CVE-2024-11111, CVE-2024-11110, CVE-2024-10827 and CVE-2024-10826.
- Updated Chromium browser to version 133.0.6943.53.

Firefox

- Updated Firefox ESR to version 115.20
  - Fix for mfsa2025-08, also known as CVE-2025-1009, CVE-2025-1010, CVE-2025-1012 and CVE-2025-1016.
  - Fix for mfsa2025-03, also known as CVE-2025-0238 and CVE-2025-0242.
  - Fix for mfsa2024-65, also known as CVE-2024-11691 and CVE-2024-11694.
  - Fix for mfsa2024-57, also known as CVE-2024-10458, CVE-2024-10459 and CVE-2024-10463.

Base system

- Fixed bind9 security issues
  CVE-2024-4076, CVE-2024-1975, CVE-2024-1737, CVE-2024-0760, CVE-2023-5679, CVE-2023-5517, CVE-2023-50868, CVE-2023-50387, CVE-2023-4408, CVE-2023-4236 and CVE-2023-3341.

- Fixed python3.10 security issues CVE-2024-8088, CVE-2024-7592, CVE-2024-6923, CVE-2024-6232, CVE-2023-27043, CVE-2024-0450 and CVE-2023-6597.
- Fixed openssl security issue CVE-2022-40735.
- Fixed wget security issue CVE-2024-38428.
- Fixed aom security issue CVE-2024-5171.
- Fixed cups security issues CVE-2024-47175 and CVE-2024-35235.
- Fixed krb5 security issues CVE-2024-37371 and CVE-2024-37370.
- Fixed openvpn security issues CVE-2024-5594 and CVE-2024-28882.
- Fixed wpa security issues CVE-2024-5290 and CVE-2023-52160.
- Fixed ghostscript security issues CVE-2024-29511, CVE-2024-29509, CVE-2024-29508 and CVE-2024-29506.
- Fixed zulu17-ca security issues CVE-2024-21131, CVE-2024-21138, CVE-2024-21140, CVE-2024-21145 and CVE-2024-21147.
- Fixed gtk+2.0 security issue CVE-2024-6655.
- Fixed gtk+3.0 security issue CVE-2024-6655.
- Fixed openvpn security issue CVE-2024-5594.
- Fixed qtbase-opensource-src security issue CVE-2024-39936.
- Fixed python-zipp security issue CVE-2024-5569.
- Fixed poppler security issue CVE-2024-6239.
- Fixed openssl1.1 security issues CVE-2024-5535, CVE-2024-4741 and CVE-2024-2511.
- Fixed openssh security issue CVE-2024-39894.
- Fixed python3.10 security issues CVE-2024-4032 and CVE-2024-0397.
- Fixed openssl security issues CVE-2024-6119, CVE-2024-5535, CVE-2024-4741, CVE-2024-4603 and CVE-2024-2511.
- Fixed mysql-8.0 security issues CVE-2024-21185, CVE-2024-21179, CVE-2024-21177, CVE-2024-21173, CVE-2024-21171, CVE-2024-21165, CVE-2024-21163, CVE-2024-21162, CVE-2024-21142, CVE-2024-21134, CVE-2024-21130, CVE-2024-21129, CVE-2024-21127, CVE-2024-21125 and CVE-2024-20996.
- Fixed gnome-shell security issue CVE-2024-36472.
- Fixed orc security issue CVE-2024-40897.
- Fixed postgresql-14 security issue CVE-2024-7348.
- Fixed bubblewrap security issue CVE-2024-42472.
- Fixed curl security issues CVE-2024-8096, CVE-2024-7264, CVE-2024-6874 and CVE-2024-6197.
- Fixed vim security issues CVE-2024-43802, CVE-2024-43374 and CVE-2024-41957.
- Fixed webkit2gtk security issues CVE-2024-44187, CVE-2024-40866, CVE-2024-27851, CVE-2024-27838, CVE-2024-27833, CVE-2024-27820, CVE-2024-27808, CVE-2024-23271, CVE-2024-4558, CVE-2024-40794, CVE-2024-40789, CVE-2024-40785, CVE-2024-40782, CVE-2024-40780, CVE-2024-40779, CVE-2024-40776 and CVE-2024-27834.
- Fixed ffmpeg security issues CVE-2024-7272 and CVE-2024-7055.
- Fixed expat security issues CVE-2024-50602, CVE-2024-45492, CVE-2024-45491 and CVE-2024-45490.
- Fixed tiff security issue CVE-2024-7006.
- Fixed setuptools security issue CVE-2024-6345.
- Fixed apparmor security issue CVE-2016-1585.
- Fixed libvirt security issue CVE-2024-8235.

- Fixed qemu security issues CVE-2024-8612, CVE-2024-4467, CVE-2024-7409 and CVE-2024-6505.
- Fixed cups-filters security issues CVE-2024-47176 and CVE-2024-47076.
- Fixed nano security issue CVE-2024-5742.
- Fixed zulu17-ca security issues CVE-2023-42950, CVE-2024-25062, CVE-2024-21235, CVE-2024-21217, CVE-2024-21210 and CVE-2024-21208.
- Fixed libheif security issues CVE-2024-25269, CVE-2023-49464, CVE-2023-49463, CVE-2023-49462, CVE-2023-49460 and CVE-2023-0996.
- Fixed libvpx6 security issue CVE-2024-5197.
- Fixed xorg-server security issue CVE-2024-9632.
- Fixed python-urllib3 security issue CVE-2024-37891.
- Fixed libarchive security issue CVE-2024-20696.
- Fixed curl security issues CVE-2024-9681 and CVE-2024-11053.
- Fixed mpg123 security issue CVE-2024-10573.
- Fixed libgd2 security issue CVE-2021-40812.
- Fixed glib2.0 security issue CVE-2024-52533.
- Fixed ghostscript security issues CVE-2024-46956, CVE-2024-46955, CVE-2024-46953, CVE-2024-46952 and CVE-2024-46951.
- Fixed python3.10 security issue CVE-2024-9287.
- Fixed mysql-8.0 security issues CVE-2025-21559, CVE-2025-21555, CVE-2025-21546, CVE-2025-21540, CVE-2025-21529, CVE-2025-21523, CVE-2025-21522, CVE-2025-21519, CVE-2025-21505, CVE-2025-21503, CVE-2025-21501, CVE-2025-21500, CVE-2025-21497, CVE-2025-21491, CVE-2025-21490, CVE-2024-21241, CVE-2024-21239, CVE-2024-21237, CVE-2024-21236, CVE-2024-21231, CVE-2024-21230, CVE-2024-21219, CVE-2024-21213, CVE-2024-21212, CVE-2024-21201, CVE-2024-21199, CVE-2024-21198, CVE-2024-21197, CVE-2024-21196, CVE-2024-21194 and CVE-2024-21193.
- Fixed libsoup2.4 security issues CVE-2024-52532, CVE-2024-52531 and CVE-2024-52530.
- Fixed vim security issues CVE-2025-22134 and CVE-2024-47814.
- Fixed ngtcp2 security issue CVE-2024-52811.
- Fixed webkit2gtk security issues CVE-2024-54534, CVE-2024-54508, CVE-2024-54505, CVE-2024-54502, CVE-2024-54479, CVE-2024-44309 and CVE-2024-44308.
- Fixed iperf3 security issue CVE-2024-53580.
- Fixed libsndfile security issues CVE-2024-50612 and CVE-2022-33065.
- Fixed qemu security issue CVE-2023-2861.
- Fixed opensc security issues CVE-2024-8443, CVE-2024-45620, CVE-2024-45619, CVE-2024-45618, CVE-2024-45617, CVE-2024-45616 and CVE-2024-45615.
- Fixed postgresql-14 security issues CVE-2024-10979, CVE-2024-10978, CVE-2024-10977 and CVE-2024-10976.
- Fixed poppler security issue CVE-2024-56378.
- Fixed rsync security issues CVE-2024-12747, CVE-2024-12088, CVE-2024-12087, CVE-2024-12086, CVE-2024-12085 and CVE-2024-12084.
- Fixed python3.10 security issue CVE-2024-11168.
- Fixed zulu17-ca security issue CVE-2025-21502.
- Fixed openjpeg2 security issues CVE-2024-56827, CVE-2024-56826, CVE-2023-39327 and CVE-2021-3575.
- Fixed bind9 security issues CVE-2024-12705 and CVE-2024-11187.
- Fixed harfbuzz security issue CVE-2023-25193.

- Fixed glibc security issue CVE-2025-0395.
- Set nologin for system users tcpdump and unscd.
- Fixed webkit2gtk security issues CVE-2025-24162, CVE-2025-24158, CVE-2025-24150, CVE-2025-24143, CVE-2024-54658, CVE-2024-54543 and CVE-2024-27856.

Resolved Issues 11.10.250

Citrix

- Fixed ica.module.EnableVolumeListener has an effect on the EnableAudioListener of the module.ini file.
- Fixed mapping of hotkey ‘Ctrl + Alt + End’ to ‘Ctrl + Alt + Del’, configurable via IGEL Setup > Sessions > Citrix > Citrix Global > Keyboard > ‘Mapping Ctrl + Alt + End to Ctrl + Alt + Del for Citrix sessions’.
- Fixed password change within Citrix Workspace App with German user interface language.
- Option to disable Citrix connection dialogue (ica.pnlogin.suppressconnectiondialog) is fixed.
- Citrix: Configuration now works if no Citrix session is configured at all to enable a proper environment for browser sessions.
- In Citrix Workspace app 24.11, BCR cache is cleared after user disconnects/signout from the VDA.
- Enhanced Kerberos/AD and Last User/-Domain/Autologin for Citrix Cloud Services.

AVD

- Integrated new RdClientSDK to fix issues when connecting to host pools that use private endpoint.

RDP/IGEL RDP Client 2

- Fixed serial port redirection not working for COM10 and above.

Remote Desktop (RDP3)

- Fixed RD Web Access autostart not working when using client version RDP3.

RD Web Access

- Fixed disabling Verify Certificates not working for RD Web Access.

Horizon

- Fixed log collection.
- Fixed a bug in the Horizon login dialog for next-gen sessions where the user name couldn’t be changed.

Network

- Fixed Ethernet hotplug issue with the Lenovo USB-C Dock Type 40A9.
- Fixed sporadic no-link messages related to a deactivated Ethernet interface.
- ACME client:
    - Fixed CA certificate permission issue.
    - Fixed potential inconsistency after change of settings.

- Fixed issue with e1000e network card not working with powersave settings.
- Added new registry key to blacklist drivers for powersave settings:

Parameter	`List of drivers seperated by space which have issues with powersave settings.`
Registry	`system.powersave.powertop_drivers_blacklist`
Type	string
Value	empty **Default**

IGEL Agent for Imprivata

- Adjustments have been made to the new integrated Omnissa Horizon 2412 client.

Smartcard

- Fixed smart card resource manager pcsc-lite to make smart cards work with certain applications inside AVD, Remote Desktop and Windows 365 sessions.

HID

- Fixed touchscreen calibration not working.
- Fixed auto-suspend of HID devices after reboot.
- Fixed touchscreen right click by using touchegg gesture recognition for two finger tap. Further gestures are not supported.
  Added registry key to enable touchegg multitouch gesture support:

Parameter	Use touchegg for multitouch gestures handling.
Registry	userinterface.touchscreen.touchegg
Type	bool
Value	enabled / **disabled** (default)

CUPS Printing

- Fixed printing on DYMO LabelWriter 450.
- Fixed CUPS printing service not starting on boot.
- Added generic IPP Everywhere for driverless printing.

Cisco Webex

- Fixed Cisco Webex VDI not correctly applying for AVD sessions.

Base system

- Backported a kernel patch for devices with the Intel Goldmont microarchitecture, which is used for low-power Atom, Celeron and Pentium branded processors.
  - This fixes a potential freeze during the OSC installation process.
  - Additionally, this fixes an issue where affected devices were not shutting down correctly.
- Added new parameter to configure default for ‘Connect after reboot’:

Parameter	`Connect after reboot`
Registry	`devices.bluetooth.pair_on_reboot`
Type	bool
Value	**enabled** (default) / disabled

- Fixed not functional proxy if system-wide proxy was configured.
- Fixed displaying of custom boot splash on AMD platforms.
- Changed configuration of webcam priority. V4L Name is used for identifying the webcam. If only one webcam is present, no entry is needed. If multiple webcams are present without set priority, the first one is used.
- Added parameters in registry

Parameter	Camera name
Registry	multimedia.webcam.camera%.name
Type	string
Value	**camera** Default

Parameter	priority
Registry	multimedia.webcam.camera%.priority
Type	integer
Value	**0** Default

Parameter	V4L2 name
Registry	multimedia.webcam.camera%.v4lname
Type	string
Value	**v4l2-string** Default

- Lower number means higher priority.
- Obsolete Registry Parameters

Parameter	Select how the webcam to use should be choosen.

Registry	multimedia.webcam.virtual_background.choose_webcam_by
Range	[Use first webcam][Choose by name] [Choose by vendor_id:product_id][Choose by number] [Choose by devicename][Choose by priority]
Value	**Use first webcam**

Parameter	Select webcam by number (only valid if choose by number is used)
Registry	multimedia.webcam.virtual_background.webcam_number
Type	integer
Value	**1** Default

Parameter	Select webcam by name (only valid if choose by name is used)
Registry	multimedia.webcam.virtual_background.webcam_name
Type	string
Value	**empty** Default

Parameter	Select webcam by vendor_id:product_id (only valid if choose by vendor_id:product_id is used)
Registry	multimedia.webcam.virtual_background.webcam_vendor_product
Type	string
Value	**empty** Default

Parameter	Select webcam by devicename for example /dev/video0 or video0 (only valid if choose by devicename is used)
Registry	multimedia.webcam.virtual_background.webcam_device
Type	string
Value	**empty** Default

Parameter	Select webcam by priority list for example dev=video0;name=HD_Webcam_C270 (only valid if choose by priority is used)}}
Registry	multimedia.webcam.virtual_background.webcam_priority
Type	string
Value	**empty** Default

Firmware update

- Fixed FTP the server configuration to properly reflect the configured maximum number of connections. Please note that there's a hard limit of 100 concurrent connections in the FTP server.

- Fixed migration dbus timeout on slower devices if migration prepare is needed.

X11 system

- Fixed a bug that reset the display configuration to default on reboot.

Audio

- LG 24CN65x series audio fix for speaker and headphones.
- Added registry key to ignore decibel information given by the ALSA driver (useful if that information is wrong):

Parameter	`Ignore dB`
Registry	`multimedia.pulseaudio.daemon.ignore-db`
Type	bool
Value	enabled / **disabled** (default)

- Fixed internal microphone on Fujitsu Lifebook E5412.

Multimedia

- Fixed window distortions with video playback on Intel Meteor Lake chipsets.

Hardware

- Fixed ignition off on ADS-TEC VMT-9010.
- Fixed Wi-Fi on Lenovo Ideapad devices. The last ON/OFF state of the Wi-Fi is restored on each boot or reboot.
- Disabled system suspend on HP t240 as it is not supported.

Remote Management

- Fixed unreliable ICG status icon.
- Suppress confusing log messages while checking for upgrade readiness.
- Improved fallback switch to ICG in case of UMS is preferred over ICG.

Component Versions 11.10.250

Clients	
Amazon WorkSpaces Client	4.1.0
Chromium	133.0.6943.53-1igel1738850419
Cisco JVDI Client	15.0.0
Cisco Webex VDI plugin	44.12.1.31417
Cisco Webex Meetings VDI plugin	43.6.8.4
Cisco Webex Meetings VDI plugin	44.10.1.3
Cisco Webex Meetings VDI plugin	44.6.5.1
Zoom Media Plugin	5.17.13.25060
Zoom Media Plugin	6.1.12.25370
Zoom Media Plugin	6.2.10.25600
Citrix EPA Client	24.10.1
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	24.10.1
Citrix Workspace App	20.10.0.6
Citrix Workspace App	24.08.0.98
Citrix Workspace App	24.11.0.85
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825
Evince PDF Viewer	42.3-0ubuntu3.1

Clients	
FabulaTech Plugins	4.1.0.3
FabulaTech USB for Remote Desktop	6.2.1.8
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.20.0
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1730799204
IGEL AVD Client	1.3.0igel1738058087
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_23.2.0.711883_amd64
IGEL Agent for Imprivata	0.6.2igel1739194615
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.12-1igel1721712256
Zulu JRE	17.0.14-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.15.0-1igel1738736251
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Clients	
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.14.1+dfsg-1igel1732532698
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation	
Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.5
Philips Speech driver	13.2.3

Signature	
Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.3

Smartcard	
PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.26.0-1igel1736250160
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24

Smartcard	
Reader Driver MUSCLE CCID	1.6.1-2igel1730368961
Reader Driver REINER SCT cyberJack	3.99.5final.sp17-0.1igel1727417566
Resource Manager PC/SC Lite	2.3.1-1igel1736249599
Cherry USB2LAN Proxy	3.2.0.3

System Components	
OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.23
OpenSSL	3.0.2-0ubuntu1.18
OpenSSH Client	9.9p1-3igel1730280218
OpenSSH Server	9.9p1-3igel1730280218
Bluetooth Stack (bluez)	5.79-1igel1732513543
MESA OpenGL Stack	24.2.8-1igel1736252923
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.11.0-1igel1738822597
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.3-1igel1738566034
Input Driver ELO Multitouch	4.3.0.0

System Components	
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1738661271
Xorg X11 Server	21.1.15-2igel1736251484
Xorg Xephyr	21.1.15-2igel1736251484
CUPS Printing Daemon	2.4.10-2igel1727672599
PrinterLogic	25.2.0.16
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.12-1igel1738564007
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.46.6-1~deb12u1igel1739423750
Python3	3.10.12

VM Guest Support Components	
Virtualbox Guest Utils	7.0.20-dfsg-1igel1726735257
Virtualbox X11 Guest Utils	7.0.20-dfsg-1igel1726735257
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2

VM Guest Support Components	
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	9.2.0+ds-4igel1736508561

Features with Limited IGEL Support	
Mobile Device Access USB (MTP)	1.1.22-1igel1736514321
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-3igel1732526151
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.20-dfsg-1igel1726735257
Virtual Background for Webcam	

Services	Size	Reduced Firmware
Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.2M	Included
Citrix Workspace app Citrix Appliance Citrix StoreFront	711.0 M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.2M	Included
RDP Omnissa Horizon	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
Omnissa Horizon	213.5 M	Included
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.0M	Included

Services	Size	Reduced Firmware
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	129.2 M	Not included
Imprivata Appliance	32.5M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	11.0M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.2M	Included
PrinterLogic	47.2M	Not included
Login VSI Login Enterprise	28.0M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.2M	Not included
AVD	48.5M	Included
Local Browser (Chromium)	114.8 M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	103.2 M	Not included
Cisco Webex Meetings VDI	176.8 M	Not included
Zoom Media Plugin	201.5 M	Not included

Services	Size	Reduced Firmware
DriveLock	12.2M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.0M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.5M	Included
90meter Smart Card Support	512.0K	Included
Virtual Background for Webcam (Limited IGEL Support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	7.8M	Not included
Virtualbox (Limited support)	73.5M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.5M	Included

Known Issues 11.10.250

Citrix

- Keyboard sync mode selection once/dynamic/off results in unexpected behavior.
- Citrix Cloud login with Citrix Workspace app 20.10 not possible
- Citrix StoreFront login to the cloud stores with Password authentication type may not work due to the n-factor authentication enforced by Microsoft. Switch to Citrix login type as a workaround.
- If the user logs out via the Self-service drop down menu, the user data is not deleted correctly by Citrix. As a result, a re-login can be performed without new authentication. To remove all user credentials the self-service window should always be closed when logging off.
- Citrix proxy connections can fail if they are set up in an environment that only allows external connections through a proxy and restricts DNS queries.
- With the new Citrix toolbar, desktops may unexpectedly switch from windowed mode to full-screen mode when a monitor was suspended. As a workaround, you can revert to the previous version of the toolbar by setting the ica.wfclient.toolbarversion parameter to “Old”.
- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy “Optimize for 3D graphics workload” in combination with server policy “Use video codec compression” -> *“For the entire screen”**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.

- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- AVD is not running on devices that don't support SSE4.1 at least. Use older IGEL OS firmware versions like 11.09.xxx[258] or older!
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

Remote Desktop (RDP3)

- RDP3 is not running on devices that don't support SSE4.1 at least. Use the legacy RDP client instead.

RD Web Access

- Client is not running on devices that don't support SSE4.1 at least. Use RdWebAccess with the legacy RDP client instead.

Horizon

- Horizon session uses the configured system proxy, even if "Direct connection to the Internet" is set for the session
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  userinterface.softkeyboard.autoshow
  userinterface.softkeyboard.autohide
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.

258. http://11.09.xxx

- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  vmware.view.enable-serial-port-redir
  vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

IGEL Agent for Imprivata

- Filter horizon apps on chooser does not work, apps will show in any case. The recommendation is to set “iia.hide_horizon_apps_on_chooser” to “False”

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://kb.igel.com/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The “Console Invocation” has to allow ‘Native’ client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  ‘https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch’

Audio

- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.

- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some HP devices will shut down instead of restarting during the BIOS update procedure. After manual boot of the devices, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g. via UMS) does not seem to work in this state, either.
  The BIOS is still updated successfully. This is currently known for HP mt645 G7 and mt645 G8.
- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 G3 and mt645 G7/G8.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Notes for Release 11.10.210

Software:	Version	11.10.210
Release Date	2024-11-22	
Release Note:	Version	RN-1110210
Last update:	2024-11-26	

New Features 11.10.210

Citrix

- Updated Citrix Workspace App to version 2405.
  Available Citrix Workspace Apps in this release: 2405 (default), 2402, and 2010

Changed

- The default value of the parameter ica.authman.kiosksfuienhanced has been changed to true and thus corresponds to the value of Citrix.

Added

- [Technical Preview] Provision to manage multiple proxy servers
  You can use multiple proxy servers that allow the HDX sessions to select appropriate proxy servers for accessing specific resources.

Parameter	ProxyAutoConfigURL
Registry	ica.allregions.proxyautoconfigurl
Type	string
Value	""

Extend parameter range ica.allregions.proxytype with "Script".

- [Technical Preview] Multiple webcam resolutions support
  Webcam streaming supports all webcam resolutions that are available on the client side.

Parameter	HDXWebcamEnablePnp
Registry	ica.wfclient.hdxwebcamenablepnp
Type	bool
Value	enabled / **disabled** (default)

Citrix NSGClient

- Updated Citrix EPA Client to version 24.10.1

RD Web Access

- Added IGEL RDP3-based RD Web Access incl. support of seamless app(s).

VMware Horizon

- Updated Horizon Client to version 2406
- Added support for Horizon next-gen (v2) API
  If server URL of Horizon session matches the host name pattern defined in vmware.view.v2_host, next-gen API will be used for this session.

Parameter	Next-gen host name pattern
Registry	vmware.view.v2_host
Type	string
Value	.workspaceoneaccess.com .workspaceair.com
	.vmwareidentity.eu .vmwareidentity.de
	.vmwareidentity.co.uk .vmwareidentity.com.au
	.vmwareidentity.com .vmwareidentity.ca
	.vmwareidentity.asia .vidmpreview.com (*Default)*

Network

- Added ACME client - for usage of HTTP-01 challenge.

Registry keys

- This determines whether the feature is enabled as a whole:

Parameter	Manage certificates with ACME
Registry	network.acmeclient.enable
Type	bool
Value	enabled / *disabled* (default)

- The rest are members of instances of network.acmeclient.cert%. Instance 0 is available from the start.
- This is the name of the subdirectory of /wfs/acme_certificates/ where data for the respective instance is stored - only letters, digits, underscores, dashes and dots are allowed:

Parameter	Directory
Registry	network.acmeclient.cert%.directory
Type	string
Value	default *Default*

- The following are names (space-separated) for which a certificate shall be requested. In the case of success each will appear as subject alt name, the first one also as the common name (This is true at least with the Smallstep CA with default settings). %H will be replaced by `hostname -f`, %h by `hostname -s`.

Parameter	Names
Registry	network.acmeclient.cert%.names
Type	string
Value	%H *Default*

- This is the ACME server URL (something like https://my- stepca.example.com/acme/acme/directory):

Parameter	ACME server URL
Registry	network.acmeclient.cert%.serverurl
Type	string
Value	empty *Default*

Parameter	Account key length (bits)
Registry	network.acmeclient.cert%.accountkeylength
Range	[1024][2048][4096]
Value	*4096*

- This is for verifying the ACME servers certificate (installing any such certificate on the system is beyond the scope of the ACME client):

Parameter	CA Bundle
Registry	network.acmeclient.cert%.cabundle
Type	string
Value	empty *Default*

- This may be necessary for creating an account on the ACME server:

Parameter	Email address
Registry	network.acmeclient.cert%.email
Type	string
Value	empty *Default*

- The following is the length of the client key for which a certificate will be requested. Those with ecc-prefix mean ellipic curve keys, the remaining ones RSA keys.

Parameter	Key length (bits)
Registry	network.acmeclient.cert%.keylength
Range	[1024][2048][4096][8192][ec-256][ec-384][ec-512]
Value	*4096*

- This is the number of days between expiry checks:

Parameter	Certificate expiry check interval (days)
Registry	network.acmeclient.cert%.checkinterval
Type	integer
Value	1 *Default*

- This is the period before the certificates' expiry in which renewal attempts are performed:

Parameter	Certificate renewal period (days)
Registry	network.acmeclient.cert%.renewalperiod
Type	integer
Value	30 *Default*

- This is the debug level for acme.sh:

Parameter	Debug level
Registry	network.acmeclient.cert%.debuglevel
Range	[0][1][2][3]
Value	*0*

- The resulting client.cert and client.key can be used for EAP/TLS and EAP/PEAP/TLS via Ethernet and WLAN.
  Example:
  Assume the above is configured with directory="default" and EAP/TLS is wanted.
  On the respective setup panel the following should be configured then:
  EAP Type: TLS
  Validate Server Certificate/CA Root Certificate: for verifying the RADIUS server's certificate, a separate topic
  Manage certificates with SCEP (NDES): no
  Client Certificate: /wfs/acme_certificates/default/client.cert
  Private Key: /wfs/acme_certificates/default/client.key
  Identity: , will be automatically derived from the client certificate's subject
  Private Key Password:
- Added Wake on LAN support via USB-C-to-LAN adapters

- Activated by enabling any of the Wake on LAN settings of LAN Interfaces
- Only Wake on LAN from Suspend is supported
- Updated Lenovo FCC Unlock Tool to version 2.4

IGEL Agent for Imprivata

- Updated iia to 0.6.2igel1728370169 (content of IAFI 1.1.0).

Imprivata

- Updated Imprivata bootstrap loader to fix CVE-2022-37454.
- Updated PIE bootstrap loader to 23.2.0.711883

HID

- Added new registry keys to influence mouse acceleration settings:

Parameter	Use new mouse accel variant
Registry	userinterface.mouse.use_new_accel_variant
Type	bool
Value	enabled / *disabled* (default)
Parameter	Enable mouse acceleration (only for new accel variant)
Registry	userinterface.mouse.enable_acceleration
Type	bool
Value	*enabled* (default) / disabled

Cisco JVDI Client

- Updated Cisco JVDI to version 15.0.0

Cisco Webex

- Updated Webex VDI to version 44.8.1.30603
  Added support for AVD
  Fixed two critical issues (Crash, Audio for Webex Calling)
- Updated Webex Meetings VDI to version 44.6.5.1, available versions: 44.6.5.1, 43.6.8.4 and 42.10.8.14.

Base system

- Removed support for BioSec BS Login Hand Vein Sensor due to technical reasons (necessary removal of QT4).
- Updated grub bootloader to 2.12 version.
- Updated StepOver Client to version 2.4.3

Firmware update

- Added progress notification shown during migration from OS 11 to OS 12.

zoomvdi

- Updated Zoom VDI Client to version 6.1.12. Available versions in this release: 6.1.12.25370, 5.17.13.25060 and 5.17.6.24660.

Hardware

- Improved hardware detection of supported LG devices.
- Validated support for Intel i226, 2.5Gbps ethernet card (copper and fiber) for HP t755 devices. Validated support for Allied Telesis 2914SP Gbps PCIe network adapter with SFP Port for HP t755 devices.

TC Setup (Java)

- Upgraded TC Setup to version 12.6.1
- Added deviceTRUST and Cisco Webex VDI options to Sessions > AVD > AVD Sessions > AVD Session > Plugins page.

Remote Management

- Improved migration from OS 11 to OS 12.
  Upgrade of the remote management protocols is invoked as a separate step returning a specific reason in case of failure.

Fabulatech

- Updated Fabulatech USB redirection to version 6.2.0.9
- Added interfaces parameter to configure Fabulatech USB redirection to redirect certain interfaces only. The value is a space separated list of interface indices. The interfaces parameter is available in IGEL registry. After creation of device rule with VID and PID for the related device, the IGEL registry under rdp.usbredirection.devicepolicy.product_rule0.interfaces must be used to configure the interface indices to redirect. Leave interfaces empty to redirect the whole device.

Registry	`rdp.usbredirection.devicepolicy.product_rule%.interfaces`
Value	"" (default) / space separated list of interface indices to redirect, ie. "2 3"

Security Fixes 11.10.210

Chromium

- Updated Chromium browser to current mainline version 130.0.6723.91.
- Fixed Chromium security issues CVE-2024-10488, CVE-2024-10487, CVE-2024-10231, CVE-2024-10230, CVE-2024-10229, CVE-2024-9966, CVE-2024-9965, CVE-2024-9964, CVE-2024-9963, CVE-2024-9962, CVE-2024-9961, CVE-2024-9960, CVE-2024-9959, CVE-2024-9958, CVE-2024-9957, CVE-2024-9956, CVE-2024-9955, CVE-2024-9954, CVE-2024-9603, CVE-2024-9602, CVE-2024-9370, CVE-2024-9369, CVE-2024-9123, CVE-2024-9122, CVE-2024-9121, CVE-2024-9120, CVE-2024-8909, CVE-2024-8908, CVE-2024-8907, CVE-2024-8906, CVE-2024-8905, CVE-2024-8904, CVE-2024-8639, CVE-2024-8638, CVE-2024-8637, CVE-2024-8636 and CVE-2024-7025.
- Fixed Chromium security issues CVE-2024-8362, CVE-2024-7970, CVE-2024-8198, CVE-2024-8194, CVE-2024-8193, CVE-2024-8035, CVE-2024-8034, CVE-2024-8033, CVE-2024-7981, CVE-2024-7980, CVE-2024-7979, CVE-2024-7978, CVE-2024-7977, CVE-2024-7976, CVE-2024-7975, CVE-2024-7974, CVE-2024-7973, CVE-2024-7972, CVE-2024-7971, CVE-2024-7969, CVE-2024-7968, CVE-2024-7967, CVE-2024-7966, CVE-2024-7965 and CVE-2024-7964.

Firefox

- Updated Mozilla Firefox to version 115.16.1 ESR
- Fixes for mfsa2024-30, also known as: CVE-2024-7652, CVE-2024-6600, CVE-2024-6601, CVE-2024-6602, CVE-2024-6603, CVE-2024-6604.
- Fixes for mfsa2024-34, also known as: CVE-2024-7519, CVE-2024-7521, CVE-2024-7522, CVE-2024-7524, CVE-2024-7525, CVE-2024-7526, CVE-2024-7527, CVE-2024-7529, CVE-2024-7531.
- Fixes for mfsa2024-41, also known as: CVE-2024-8381, CVE-2024-8382, CVE-2024-8383, CVE-2024-8384.
- Fixes for mfsa2024-48, also known as: CVE-2024-9392, CVE-2024-9393, CVE-2024-9394, CVE-2024-9401.
- Fixes for mfsa2024-51, also known as: CVE-2024-9680.

Imprivata

- Updated Imprivata bootstrap loader to fix CVE-2022-37454.

Base system

- Fixed bind9 security issues CVE-2024-4076, CVE-2024-1975, CVE-2024-1737, CVE-2024-0760, CVE-2023-5679, CVE-2023-5517, CVE-2023-50868, CVE-2023-50387, CVE-2023-4408, CVE-2023-4236 and CVE-2023-3341.

- Fixed python3.10 security issues CVE-2024-8088, CVE-2024-7592, CVE-2024-6923, CVE-2024-6232, CVE-2023-27043, CVE-2024-0450 and CVE-2023-6597.
- Fixed openssl security issue CVE-2022-40735.
- Fixed wget security issue CVE-2024-38428.
- Fixed aom security issue CVE-2024-5171.
- Fixed cups security issues CVE-2024-47175 and CVE-2024-35235.
- Fixed krb5 security issues CVE-2024-37371 and CVE-2024-37370.
- Fixed openvpn security issues CVE-2024-5594 and CVE-2024-28882.
- Fixed wpa security issues CVE-2024-5290 and CVE-2023-52160.
- Fixed ghostscript security issues CVE-2024-29511, CVE-2024-29509, CVE-2024-29508 and CVE-2024-29506.
- Fixed zulu17-ca security issues CVE-2024-21131, CVE-2024-21138, CVE-2024-21140, CVE-2024-21145 and CVE-2024-21147.
- Fixed gtk+2.0 security issue CVE-2024-6655.
- Fixed gtk+3.0 security issue CVE-2024-6655.
- Fixed openvpn security issue CVE-2024-5594.
- Fixed qtbase-opensource-src security issue CVE-2024-39936.
- Fixed python-zipp security issue CVE-2024-5569.
- Fixed poppler security issue CVE-2024-6239.
- Fixed openssl1.1 security issues CVE-2024-5535, CVE-2024-4741 and CVE-2024-2511.
- Fixed openssh security issue CVE-2024-39894.
- Fixed python3.10 security issues CVE-2024-4032 and CVE-2024-0397.
- Fixed openssl security issues CVE-2024-6119, CVE-2024-5535, CVE-2024-4741, CVE-2024-4603 and CVE-2024-2511.
- Fixed mysql-8.0 security issues CVE-2024-21185, CVE-2024-21179, CVE-2024-21177, CVE-2024-21173, CVE-2024-21171, CVE-2024-21165, CVE-2024-21163, CVE-2024-21162, CVE-2024-21142, CVE-2024-21134, CVE-2024-21130, CVE-2024-21129, CVE-2024-21127, CVE-2024-21125 and CVE-2024-20996.
- Fixed gnome-shell security issue CVE-2024-36472.
- Fixed orc security issue CVE-2024-40897.
- Fixed postgresql-14 security issue CVE-2024-7348.
- Fixed bubblewrap security issue CVE-2024-42472.
- Fixed curl security issues CVE-2024-8096, CVE-2024-7264, CVE-2024-6874 and CVE-2024-6197.
- Fixed vim security issues CVE-2024-43802, CVE-2024-43374 and CVE-2024-41957.
- Fixed webkit2gtk security issues CVE-2024-44187, CVE-2024-40866, CVE-2024-27851, CVE-2024-27838, CVE-2024-27833, CVE-2024-27820, CVE-2024-27808, CVE-2024-23271, CVE-2024-4558, CVE-2024-40794, CVE-2024-40789, CVE-2024-40785, CVE-2024-40782, CVE-2024-40780, CVE-2024-40779, CVE-2024-40776 and CVE-2024-27834.
- Fixed ffmpeg security issues CVE-2024-7272 and CVE-2024-7055.
- Fixed expat security issues CVE-2024-50602, CVE-2024-45492, CVE-2024-45491 and CVE-2024-45490.
- Fixed tiff security issue CVE-2024-7006.
- Fixed setuptools security issue CVE-2024-6345.
- Fixed apparmor security issue CVE-2016-1585.
- Fixed libvirt security issue CVE-2024-8235.
- Fixed qemu security issues CVE-2024-8612, CVE-2024-4467, CVE-2024-7409 and CVE-2024-6505.

- Fixed cups-filters security issues CVE-2024-47176 and CVE-2024-47076.
- Fixed nano security issue CVE-2024-5742.
- Fixed zulu17-ca security issues CVE-2023-42950, CVE-2024-25062, CVE-2024-21235, CVE-2024-21217, CVE-2024-21210 and CVE-2024-21208.
- Fixed libheif security issues CVE-2024-25269, CVE-2023-49464, CVE-2023-49463, CVE-2023-49462, CVE-2023-49460 and CVE-2023-0996.
- Fixed libvpx6 security issue CVE-2024-5197.
- Fixed xorg-server security issue CVE-2024-9632.
- Fixed python-urllib3 security issue CVE-2024-37891.

Resolved Issues 11.10.210

Citrix

- Fixed ica.module.EnableVolumeListener has an effect at EnableAudioListener of file module.ini
- Fixed: Citrix processes does not run if no sessions are configured. The processes are restarted with changed configuration.

AVD

- Fixed PAUSE and Ctrl+PAUSE=BREAK keys to work as expected
- Fixed dynamic virtual channel initialization

RDP/IGEL RDP Client 2

- Added parameter to disable X11 autorepeat detection and handling:

Registry	`sessions.winconnect%.option.disable-autorepeat-detection`
Value	enabled / **disabled**(default)

- This fixes barcode reader dropping inputs when scanning labels with reoccuring characters.
- Fixed generic USB redirection for some devices (ie. ID 046d:0825 Logitech, Inc.Webcam C270)
- Fixed serial port redirection not working for COM10 and above.

RD Web Access

- Fixed RDP desktop session not working when published as a remote app.
- Fixed Remote Desktop Web Access login not working reliably.
- Fixed display filters not working for Rd Web Access.
- Fixed disabling Verify Certificates not working for RD Web Access.

VMware Horizon

- Fixed collection of logs.
- Fixed handling of audio preferences (vmware.view.audio-out-option)

Chromium

- Fixed custom policy URLBlocklist not working properly if file access and using IGEL Setup for configuration was disabled.
- Fixed system volume being automatically adjusted by Chromium Browser.

Firefox

- Fixed on-screen keyboard auto show / hide functionality.

Network

- Fixed SCEP: When the CA fingerprint or the CA identifier is changed, client certificate and client key are not discarded anymore. Only new CA and RA certificates will be downloaded.
- Added for SCEP: Content-Type: application/x-pki-message is sent according to RFC 8894 if the following option is enabled:

Parameter	Send Content-Type
Registry	network.scepclient.cert%.sscep.send_content_type
Type	bool
Value	enabled / *disabled* (default)

- Improved shutdown time by removing loopback interface from NetworkManager's managed interfaces.
- Fixed sporadic no-link messages regarding a deactivated Ethernet interface

HID

- Fixed auto-suspend of HID devices after reboot.
- Fixed touchscreen right click by using touchegg gesture recognition for two finger tap. Further gestures are not supported.
  Added registry key to enable touchegg multitouch gesture support.

Parameter	Use touchegg for multitouch gestures handling.
Registry	userinterface.touchscreen.touchegg
Type	bool
Value	enabled / *disabled* (default)

Base system

- Fixed: Wrong assignment of socks proxy port
- Fixed issue with license is not detected on some devices.
- Fixed issue with not using 2.5 Gbit/s or 5 Gbit/s if it would be possible.
- Fixed not functional proxy if system-wide proxy was configured.
- Fixed: Taskbar items blinking several times.
- Removed QT4 libraries from firmware.
- Changed configuration of webcam priority. V4L Name is used for identifying the webcam. If only one webcam is present, no entry is needed. If multiple webcams are present without set priority, the first one is used.

- Added parameters in registry

Parameter	Camera name
Registry	multimedia.webcam.camera%.name
Type	string
Value	camera *Default*
Parameter	priority
Registry	multimedia.webcam.camera%.priority
Type	integer
Value	0 *Default*
Parameter	V4L2 name
Registry	multimedia.webcam.camera%.v4lname
Type	string
Value	v4l2-string *Default*

- Lower number means higher priority.

Obsolete Registry Parameters

Parameter	Select how the webcam to use should be choosen.
Registry	multimedia.webcam.virtual_background.choose_webcam_by
Range	[Use first webcam][Choose by name] [Choose by vendor_id:product_id] [Choose by number] [Choose by devicename][Choose by priority]
Value	*Use first webcam*
Parameter	Select webcam by number (only valid if choose by number is used)
Registry	multimedia.webcam.virtual_background.webcam_number
Type	integer
Value	1 *Default*
Parameter	Select webcam by name (only valid if choose by name is used)
Registry	multimedia.webcam.virtual_background.webcam_name
Type	string
Value	empty *Default*

Parameter	Select webcam by vendor_id:product_id (only valid if choose by vendor_id:product_id is used)
Registry	multimedia.webcam.virtual_background.webcam_vendor_product
Type	string
Value	empty *Default*
Parameter	Select webcam by devicename for example /dev/video0 or video0 (only valid if choose by devicename is used)
Registry	multimedia.webcam.virtual_background.webcam_device
Type	string
Value	empty *Default*
Parameter	Select webcam by priority list for example dev=video0;name=HD_Webcam_C270 (only valid if choose by priority is used)}}
Registry	multimedia.webcam.virtual_background.webcam_priority
Type	string
Value	empty *Default*

Firmware update

- Fixed disk size detection of 8 GB flash sizes for OS 12 migration. With this fix migration works on UD Pockets again.
- Fixed OS11 to OS12 migration issue due to repartition not always working with non GPT partition tables.
- Fixed FTP server configuration to properly reflect the configured maxim number of connections. Please note that there is a hard limit of 100 concurrent connections in the FTP server.
- Fixed migration dbus timeout on slower devices if migration prepare is needed.

X11 system

- Fixed primary monitor configuration with new Display switcher implementation. The panel appears on the proper monitor again.

Audio

- Fixed USB headset support on LG CQ600i
- Added parameter to set output level of a headphone in ALSA to maximum at every start.

Parameter	Set headphone in alsa to maximum

Registry	multimedia.alsa.headphone_max_volume
Range	[auto][true][false]
Value	*auto*

Hardware

- Fixed issue with Intel and additional graphic cards:
- All graphic cards are now detected properly,
- All screens attached to all graphic cards are active.
- Fixed WiFi on Lenovo Ideapad devices. The last ON/OFF state of the WiFi is restored on each boot or reboot.
- Changed: Disabled suspend on HP t240.

Remote Management

- Fixed rmagent device registration.
- Added setup parameter to set connect timeout

IGEL Setup	**system > remotemanager**
Parameter	`IGEL Remote Management Connect Timeout`
Registry	`system.remotemanager.connect_timeout`
Type	integer
Value	timeout in sec / **45** (default)

Component Versions 11.10.210

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	130.0.6723.91-2igel1730698067
Cisco JVDI Client	15.0.0
Cisco Webex VDI plugin	44.8.1.30603
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	43.6.8.4
Cisco Webex Meetings VDI plugin	44.6.5.1
Zoom Media Plugin	5.17.13.25060
Zoom Media Plugin	5.17.6.24660
Zoom Media Plugin	6.1.12.25370
Citrix EPA Client	24.10.1
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	24.10.1
Citrix Workspace App	20.10.0.6
Citrix Workspace App	24.02.0.65
Citrix Workspace App	24.05.0.76
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.0.0.2
FabulaTech USB for Remote Desktop	6.2.0.9
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.16.1
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1730799204
IGEL AVD Client	1.2.0igel1729086829
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_23.2.0.711883_amd64
IGEL Agent for Imprivata	0.6.2igel1728370169
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.12-1igel1721712256
Zulu JRE	17.0.13-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.14.0-1igel1726733873
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2406-8.13.0-9995429239
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.3

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.25.1-2igel1726736707
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.6.1-1igel1726723739
Reader Driver REINER SCT cyberJack	3.99.5final.sp17-0.1igel1727417566
Resource Manager PC/SC Lite	2.3.0-1igel1726729422
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.23
OpenSSL	3.0.2-0ubuntu1.18
OpenSSH Client	9.9p1-2igel1729583438
OpenSSH Server	9.9p1-2igel1729583438
Bluetooth Stack (bluez)	5.77-1igel1727077136
MESA OpenGL Stack	24.2.4-1igel1728045443
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.147.05-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.2-3igel1726741272
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1731325402
Xorg X11 Server	21.1.14-1igel1730266598
Xorg Xephyr	21.1.14-1igel1730266598
CUPS Printing Daemon	2.4.10-2igel1727672599
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.8-1igel1727077652
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.46.0-2~deb12u1igel1729060771
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.20-dfsg-1igel1726735257

Virtualbox X11 Guest Utils	7.0.20-dfsg-1igel1726735257
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	9.1.1+ds-2igel1730101941

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-3.1igel1709728407
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-1+b1igel1709637921
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.14-dfsg-4igel1709105342
Virtual Background for Webcam	

Services

Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.2M	Included
Citrix Workspace app Citrix StoreFront Citrix Appliance	791.2M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Citrix Appliance Local Browser (Firefox)	86.2M	Included
RDP VMware Horizon	4.5M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
VMware Horizon	228.5M	Included
Voice over IP (Ekiga)	6.0M	Included

Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.0M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	370.8M	Not included
Imprivata Appliance	32.5M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	10.8M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.2M	Included
PrinterLogic	35.8M	Not included
Login VSI Login Enterprise	28.0M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.2M	Not included
AVD	39.8M	Included
Local Browser (Chromium)	116.2M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included

Cisco Webex VDI	102.2M	Not included
Cisco Webex Meetings VDI	206.5M	Not included
Zoom Media Plugin	197.0M	Not included
DriveLock	12.2M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.5M	Included
90meter Smart Card Support	512.0K	Included
Scanner support / SANE (Limited support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Virtual Background for Webcam (Limited IGEL Support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	7.8M	Not included
Virtualbox (Limited support)	73.8M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.5M	Included

Known Issues 11.10.210

Citrix

- Keyboard sync mode selection once/dynamic/off results in unexpected behavior.
- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

(This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.)

- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.

- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- AVD is not running on devices that do not support SSE4.1 at least. Use older IGEL OS firmware versions like 11.09.xxx or older.
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

Remote Desktop (RDP3)

- RDP3 is not running on devices that do not support SSE4.1 at least. Use the legacy RDP client instead.

RD Web Access

- RdWebAccess with RDP3 is not running on devices that do not support SSE4.1 at least. Use RdWebAccess with the legacy RDP client instead.

VMware Horizon

- Horizon session uses the configured system proxy, even if "Direct connection to the Internet" is set for the session.
- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  userinterface.softkeyboard.autoshow
  userinterface.softkeyboard.autohide

- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
  This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
  The respective settings can be found in the IGEL Registry:
  vmware.view.enable-serial-port-redir
  vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then.
  However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

IGEL Agent for Imprivata

- Filter horizon apps on chooser does not work, apps will show in any case. The recommendation is to set "iia.hide_horizon_apps_on_chooser" to "False"

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://kb.igel.com/en/igel-os/11.10/error-not-enough-space-on-local-drive-when-updatin for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow Native client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some HP devices will turn off instead of restarting during the BIOS update procedure. After turning the devices back on manually, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g. via UMS) doesn't seem to work in this state, either.
  The BIOS is still updated successfully. This is currently known for HP mt645 G7 and mt645 G8.
- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Supported Devices 11.10.210

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

Notes for Release 11.10.190

Software:	Version	11.10.190
Release Date	2024-10-23	
Release Note:	Version	RN-1110190
Last update:	2024-10-24	

Supported Devices 11.10.190

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

Component Versions 11.10.190

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	129.0.6668.100-1igel1728465922
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	44.4.0.29960
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Zoom Media Plugin	5.17.6.24660
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.11.0.82
Citrix Workspace App	24.02.0.65
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.0.0.2
FabulaTech USB for Remote Desktop	6.2.0.0
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.16.1
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1717589021
IGEL AVD Client	1.2.0igel1718803791
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.6.0igel1717406898
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.9-1+b1igel1709638175
Zulu JRE	17.0.11-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.13.0-2.1igel1709635747
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2312.1-8.12.1-23543969
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.25.0~rc1-1igel1709808441
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.5-1igel1704887471
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2+b1igel1704984443
Resource Manager PC/SC Lite	2.2.1-1igel1715329696
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.15
OpenSSH Client	9.7p1-7igel1719842129
OpenSSH Server	9.7p1-7igel1719842129
Bluetooth Stack (bluez)	5.73-1igel1713457475
MESA OpenGL Stack	24.0.6-1+b1igel1715159987
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.147.05-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-3igel1709642706
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1720435065
Xorg X11 Server	21.1.12-1igel1720008240
Xorg Xephyr	21.1.12-1igel1720008240
CUPS Printing Daemon	2.4.7-2igel1718171599
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.1-1igel1712123636
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.44.2-1~deb12u1igel1716390763
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.14-dfsg-4igel1709105342

Virtualbox X11 Guest Utils	7.0.14-dfsg-4igel1709105342
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	8.2.3+ds-2igel1715153009

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-3.1igel1709728407
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-1+b1igel1709637921
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.14-dfsg-4igel1709105342
Virtual Background for Webcam	

Services

Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.8M	Included
Citrix Appliance Citrix StoreFront Citrix Workspace app	813.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.5M	Included
VMware Horizon RDP	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included

VMware Horizon	194.5M	Included
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	372.5M	Not included
Imprivata Appliance	31.8M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.8M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.5M	Included
PrinterLogic	37.5M	Not included
Biosec BS Login	9.8M	Not included
Login VSI Login Enterprise	28.2M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.5M	Not included
AVD	39.8M	Included
Local Browser (Chromium)	117.5M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	100.2M	Not included
Cisco Webex Meetings VDI	193.5M	Not included
Zoom Media Plugin	180.8M	Not included

DriveLock	12.5M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	512.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	10.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.8M	Included
90meter Smart Card Support	512.0K	Included
Limited Support Features VPN OpenConnect (Limited support) Virtualbox (Limited support) Scanner support / SANE (Limited support) Virtual Background for Webcam (Limited IGEL Support) Mobile Device Access USB (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	8.0M	Not included
Virtualbox (Limited support)	74.0M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.8M	Included

Known Issues 11.10.190

Citrix

- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry: userinterface.softkeyboard.autoshow userinterface.softkeyboard.autohide
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry: vmware.view.enable-serial-port-redir vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled. If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems. Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount. As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://

kb.igel.com/en/igel-os/11.10/error-not-enough-space-on-local-drive-when-updatin for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow Native client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Audio- and mic mute function key led is not working on HP Elite mt645 G8.
- Some HP devices will turn off instead of restarting during the BIOS update procedure. After turning the devices back on manually, it may take up to three minutes before anything is displayed on the screen (the only indicator is the power LED). Wake on LAN (e.g. via UMS) doesn't seem to work in this state, either.
- The BIOS is still updated successfully.
- Affected devices as of the time of this writing: mt645 G7 ; mt645 G8
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.10.190

Chromium

- Fixed Chromium security issues

More...

CVE-2024-9603, CVE-2024-9602, CVE-2024-9370, CVE-2024-9369, CVE-2024-9123, CVE-2024-9122, CVE-2024-9121, CVE-2024-9120, CVE-2024-8909, CVE-2024-8908, CVE-2024-8907, CVE-2024-8906, CVE-2024-8905, CVE-2024-8904, CVE-2024-8639, CVE-2024-8638, CVE-2024-8637, CVE-2024-8636, CVE-2024-8362, CVE-2024-8198, CVE-2024-8194, CVE-2024-8193, CVE-2024-8035, CVE-2024-8034, CVE-2024-8033, CVE-2024-7981, CVE-2024-7980, CVE-2024-7979, CVE-2024-7978, CVE-2024-7977, CVE-2024-7976, CVE-2024-7975, CVE-2024-7974, CVE-2024-7973, CVE-2024-7972, CVE-2024-7971, CVE-2024-7970, CVE-2024-7969, CVE-2024-7968, CVE-2024-7967, CVE-2024-7966, CVE-2024-7965, CVE-2024-7964, CVE-2024-7550, CVE-2024-7536, CVE-2024-7535, CVE-2024-7534, CVE-2024-7533, CVE-2024-7532, CVE-2024-7256, CVE-2024-7255, CVE-2024-7025, CVE-2024-7005, CVE-2024-7004, CVE-2024-7003, CVE-2024-7001, CVE-2024-7000, CVE-2024-6999, CVE-2024-6998, CVE-2024-6997, CVE-2024-6996, CVE-2024-6995, CVE-2024-6994, CVE-2024-6993, CVE-2024-6992, CVE-2024-6991, CVE-2024-6990, CVE-2024-6989, CVE-2024-6988, CVE-2024-6779, CVE-2024-6778, CVE-2024-6777, CVE-2024-6776, CVE-2024-6775, CVE-2024-6774, CVE-2024-6773, CVE-2024-6772, CVE-2024-6293, CVE-2024-6292, CVE-2024-6291 and CVE-2024-6290

- Updated chromium browser to current mainline version 129.0.6668.100.

Firefox

- Updated Mozilla Firefox to version 115.16.1 ESR
- Fixes for mfsa2024-30, also known as:
  CVE-2024-7652, CVE-2024-6600, CVE-2024-6601, CVE-2024-6602, CVE-2024-6603, CVE-2024-6604.
- Fixes for mfsa2024-34, also known as:
  CVE-2024-7519, CVE-2024-7521, CVE-2024-7522, CVE-2024-7524, CVE-2024-7525, CVE-2024-7526, CVE-2024-7527, CVE-2024-7529, CVE-2024-7531.
- Fixes for mfsa2024-41, also known as:
  CVE-2024-8381, CVE-2024-8382, CVE-2024-8383, CVE-2024-8384.
- Fixes for mfsa2024-48, also known as:
  CVE-2024-9392, CVE-2024-9393, CVE-2024-9394, CVE-2024-9401.
- Fixes for mfsa2024-51, also known as:
  CVE-2024-9680.

Notes for Release 11.10.150

Software:	Version	11.10.150
Release Date	2024-07-10	
Release Note:	Version	RN-1110150
Last update:	2024-07-11	

Supported Devices 11.10.150

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

Component Versions 11.10.150

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	126.0.6478.114-1igel1718788521
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	44.4.0.29960
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Zoom Media Plugin	5.17.6.24660
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.11.0.82
Citrix Workspace App	24.02.0.65
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	4.0.0.2
FabulaTech USB for Remote Desktop	6.2.0.0
FabulaTech Scanner for Remote Desktop	3.6.1.3
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.12.0
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1717589021
IGEL AVD Client	1.2.0igel1718803791
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.6.0igel1717406898
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.9-1+b1igel1709638175
Zulu JRE	17.0.11-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.13.0-2.1igel1709635747
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2312.1-8.12.1-23543969
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.25.0~rc1-1igel1709808441
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.4.38
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.11-1igel1715329126
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.5-1igel1704887471
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2+b1igel1704984443
Resource Manager PC/SC Lite	2.2.1-1igel1715329696
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.15
OpenSSH Client	9.7p1-7igel1719842129
OpenSSH Server	9.7p1-7igel1719842129
Bluetooth Stack (bluez)	5.73-1igel1713457475
MESA OpenGL Stack	24.0.6-1+b1igel1715159987
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.147.05-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-3igel1709642706
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1720435065
Xorg X11 Server	21.1.12-1igel1720008240
Xorg Xephyr	21.1.12-1igel1720008240
CUPS Printing Daemon	2.4.7-2igel1718171599
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.1-1igel1712123636
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.44.2-1~deb12u1igel1716390763
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.14-dfsg-4igel1709105342

Virtualbox X11 Guest Utils	7.0.14-dfsg-4igel1709105342
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	8.2.3+ds-2igel1715153009

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-3.1igel1709728407
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-1+b1igel1709637921
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.14-dfsg-4igel1709105342
Virtual Background for Webcam	

Services

Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.8M	Included
Citrix Appliance Citrix StoreFront Citrix Workspace app	813.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.5M	Included
VMware Horizon RDP	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
VMware Horizon	194.5M	Included
Voice over IP (Ekiga)	6.0M	Included

Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	372.5M	Not included
Imprivata Appliance	31.8M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.8M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.5M	Included
PrinterLogic	37.5M	Not included
Biosec BS Login	9.8M	Not included
Login VSI Login Enterprise	28.2M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.5M	Not included
AVD	39.8M	Included
Local Browser (Chromium)	109.5M	Not included
Amazon WorkSpaces Client	32.2M	Included

deskMate Client	5.5M	Included
Cisco Webex VDI	100.2M	Not included
Cisco Webex Meetings VDI	193.5M	Not included
Zoom Media Plugin	180.8M	Not included
DriveLock	12.5M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	512.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	10.2M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.8M	Included
90meter Smart Card Support	512.0K	Included
Limited Support Features VPN OpenConnect (Limited support) Virtualbox (Limited support) Scanner support / SANE (Limited support) Virtual Background for Webcam (Limited IGEL Support) Mobile Device Access USB (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	8.0M	Not included
Virtualbox (Limited support)	74.0M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.8M	Included

Known Issues 11.10.150

Citrix

- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.

- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Self-Service is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- When closing the AVD client while audio input (microphone redirection) is in use, the client might crash. This will be fixed in future versions.
- Webcam redirection support is preliminary / experimental and may not work with all webcams yet.
- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  userinterface.softkeyboard.autoshow
  userinterface.softkeyboard.autohide
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  vmware.view.enable-serial-port-redir
  vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then.

However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

Cisco JVDI Client

- Citrix Workspace App 2010 may cause problems with Cisco JVDI. Newer ZoomVDI versions and App Protection are no longer supported with CWA 2010.

Base system

- After updating the BIOS on the HP mt645 G7 or HP mt645 G8, the device shuts down instead of rebooting.
- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g.�if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- A firmware update started on 11.10.100 can sporadically block, so that the device must be rebooted manually. The update continues without problem after reboot.
- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://kb.igel.com/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow `Native` client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch`

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Audio- and mic mute function key led is not working on HP Elite mt645 G8.
- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.

- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  ** It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.10.150

Chromium

- Fixed Chromium security issues

More...

CVE-2024-6103, CVE-2024-6102, CVE-2024-6101, CVE-2024-6100, CVE-2024-5847, CVE-2024-5846, CVE-2024-5845, CVE-2024-5844, CVE-2024-5843, CVE-2024-5842, CVE-2024-5841, CVE-2024-5840, CVE-2024-5839, CVE-2024-5838, CVE-2024-5837, CVE-2024-5836, CVE-2024-5835, CVE-2024-5834, CVE-2024-5833, CVE-2024-5832, CVE-2024-5831, CVE-2024-5830, CVE-2024-5499, CVE-2024-5498, CVE-2024-5497, CVE-2024-5496, CVE-2024-5495, CVE-2024-5494, CVE-2024-5493, CVE-2024-5274, CVE-2024-5160, CVE-2024-5159, CVE-2024-5158, CVE-2024-5157, CVE-2024-4950, CVE-2024-4949, CVE-2024-4948, CVE-2024-4947, CVE-2024-4761, CVE-2024-4671, CVE-2024-4559, CVE-2024-4558, CVE-2024-4368 and CVE-2024-4331

- Updated Chromium browser to version 126.0.6478.114.

Firefox

- Updated Mozilla Firefox to version 115.12 ESR
- Fixes for mfsa2024-26, also known as:
  CVE-2024-5702, CVE-2024-5688, CVE-2024-5690, CVE-2024-5691, CVE-2024-5693, CVE-2024-5696, CVE-2024-5700.
- Fixes for mfsa2024-22, also known as:
  CVE-2024-4367, CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4770, CVE-2024-4777.
- Fixes for mfsa2024-19, also known as:
  CVE-2024-3852, CVE-2024-3854, CVE-2024-3857, CVE-2024-2609, CVE-2024-3859, CVE-2024-3861, CVE-2024-3302, CVE-2024-3864.

Base system

- Fixed glibc security issues

More...

CVE-2024-33602, CVE-2024-33601, CVE-2024-33600, CVE-2024-33599 and CVE-2024-2961

- Fixed gnutls28 security issues CVE-2024-28835 and CVE-2024-28834.
- Fixed nghttp2 security issue CVE-2024-28182.
- Fixed pillow security issue CVE-2024-28219.
- Fixed less security issue CVE-2024-32487.
- Fixed tpm2-tss security issue CVE-2024-29040.
- Fixed libvirt security issues CVE-2024-4418 and CVE-2024-2494.
- Fixed qemu security issues
  CVE-2024-3567, CVE-2024-3447, CVE-2024-3446, CVE-2024-26328 and CVE-2024-26327.
- Fixed tpm2-tools security issues CVE-2024-29039 and CVE-2024-29038.

- Fixed xorg-server security issues CVE-2024-31083, CVE-2024-31082, CVE-2024-31081 and CVE-2024-31080.
- Fixed glib2.0 security issue CVE-2024-34397.
- Fixed zulu17-ca security issues

More...

- CVE-2024-21012, CVE-2023-41993, CVE-2024-21011, CVE-2024-21005, CVE-2024-21004, CVE-2024-21003, CVE-2024-21002, CVE-2024-21094 and CVE-2024-21068.
- Fixed webkit2gtk security issues

More...

CVE-2024-27834, CVE-2024-23284, CVE-2024-23280, CVE-2024-23263, CVE-2024-23254, CVE-2024-23252, CVE-2023-42956, CVE-2023-42950 and CVE-2023-42843.

- Fixed python-idna security issue CVE-2024-3651.
- Fixed libxml2 security issue CVE-2024-34459.
- Fixed postgresql-14 security issue CVE-2024-4317.
- Fixed iperf3 security issue CVE-2024-26306.
- Fixed libarchive security issue CVE-2024-26256.
- Fixed aom security issue CVE-2024-5171.
- Fixed gdk-pixbuf security issue CVE-2022-48622.
- Fixed giflib security issues CVE-2022-28506 and CVE-2021-40633.
- Fixed tiff security issue CVE-2023-3164.
- Fixed cups security issue CVE-2024-35235.
- Fixed mysql-8.0 security issues

More...

CVE-2024-21102, CVE-2024-21096, CVE-2024-21087, CVE-2024-21069, CVE-2024-21062, CVE-2024-21060, CVE-2024-21054, CVE-2024-21047, CVE-2024-21013, CVE-2024-21009, CVE-2024-21008, CVE-2024-21000, CVE-2024-20998 and CVE-2024-20994

- Fixed libndp security issue CVE-2024-5564.
- Fixed ntfs-3g security issue CVE-2023-52890.
- Fixed ffmpeg security issues

More...

CVE-2023-50010, CVE-2023-51793, CVE-2023-51794, CVE-2023-51795, CVE-2023-51798 and CVE-2024-31585.

- Fixed ghostscript security issues

More...

CVE-2024-33871, CVE-2024-33870, CVE-2024-33869, CVE-2024-29510 and CVE-2023-52722.

- Fixed privilege escalation in network management.
- Fixed openssh security issue CVE-2024-6387.

New Features 11.10.150

AVD

- Updated IGEL AVD to version 1.2.0
- Based on the latest RdClientSDK from Microsoft
- UI update for AVD sessions
- Added UDP shortpath

Registry	`sessions.wvd%.options.udp-short-path`
Value	**enabled** (default) / disabled

- Added smartcard support

Registry	`sessions.wvd%.options.enable-smartcard`
Value	enabled / **disabled** (default)

- Added network status

Registry	`sessions.wvd%.options.network-status-in-toolbar`
Value	**enabled** (default) / disabled
Registry	`sessions.wvd%.options.network-status-on-startpage`
Value	**enabled** (default) / disabled

- Added battery status (if battery exists)

Registry	`sessions.wvd%.options.battery-status-in-toolbar`
Value	**enabled** (default) / disabled
Registry	`sessions.wvd%.options.battery-status-on-startpage`
Value	**enabled** (default) / disabled

- Added hidden login

Registry	`sessions.wvd%.options.hidden-login`
Value	enabled / **disabled** (default)
Registry	`sessions.wvd%.options.hidden-login-timeout`

Value	**5000** (default)

- Added preliminary / experimental webcam redirection

Registry	`sessions.wvd%.options.enable-webcam-redirection`
Value	enabled / **disabled** (default)

- Added FPS (frames per second) indicator

Registry	`sessions.wvd%.options.show-fps`
Value	enabled / **disabled** (default)

VMware Horizon

- Updated VMware Horizon Client to version 2312.1-8.12.1-23543969.

IGEL Agent for Imprivata

- Added teardown screensaver on badge event
  - Added showing computername in lockscreen's upper right corner
  - Added support for cookieinsert method for Citrix virtual server on NetScaler.

Parameter	`NetScaler COOKIEINSERT`
Registry	`iia.cookieinsert`
Type	string
Value	""(default)

- Fixed Device Control Button's visibility not in sync with Computer Policy

Smartcard

- Updated Pointsharp Net iD Client to version 1.1.4.38. Detailed release notes via https://docs.pointsharp.com/net-id-client/latest/nic-release- notes/nic-114-release-notes.html
- Net iD user service now is configurable and disabled by default - set / enable via following registry parameter:

Parameter	Net iD Client user service
Registry	scard.pkcs11.netid-client.userservice
Value	false (default) / true

- Fixed AD/Kerberos login with username and password when login with Net iD Client smartcard is active. For this, Net iD SessionToken was disabled by default. It can be enabled via the following registry parameter:

Parameter	SessionToken
Registry	scard.pkcs11.netid-client.sessiontoken
Value	false (default) / true

Cisco Webex

- Updated Cisco Webex VDI to version 44.4.0.29960

Base system

- Added HP BIOS tools to update the BIOS version, BIOS settings and BIOS password on supported HP mobile devices HP Pro mt440 G3, HP Elite mt645 G7 and HP Elite mt645 G8. IGEL supports the BIOS update mechanism only - all BIOS updates are performed / executed at own risk!
- Added option to set hardware clock. The default, Auto, will look for Windows partitions and, if present, assume that Windows is installed and the real time clock is set to local time.

Parameter	`HW clock timezone`
Registry	`system.time.hwclock_timezone`
Range	[Auto (default)] [UTC] [localtime]

X11 system

- Added alternative Display Switcher implementation to solve issues with multiscreen setups on docking stations. This alternative implementation must be enabled by following parameter:

Parameter	`Use new user_display_xrandr`
Registry	`x.new_user_display_xrandr`
Value	enabled / **disabled** (default)

- The alternative implementation is only used if "Smart display configuration" parameter is enabled:

IGEL Setup	`Accessories / Display Switch / Options`
Parameter	`Smart display configuration`
Registry	`x.auto_associate`
Value	**enabled** (default) / disabled

- This implementation can not yet be used in multi GPU scenarios.

IgelDesktop

- Replaced IGEL company logo with new design in wallpaper and Setup Assistant.
- Replaced IGEL company logo with new design in screensaver.

Audio

- Added parameter to enable or disable audio overamplification:

Parameter	`Output overamplification`
Registry	`userinterface.sound.overamplification`
Type	bool
Value	*enabled* (default) / disabled
Parameter	`Input overamplification`
Registry	`userinterface.sound.input_overamplification`
Type	bool
Value	*enabled* (default) / disabled

Evidian

- Updated Evidian's rsUserAuth to version 1.5.8825.
  - Added RFIDeas PC/SC Mixed-Mode.
    Set "RFIDMixMode=on" in rsUserAuth.ini configuration file and handle RFIDeas badges as PC/SC one.
  - Added support for Read-only protection on the domain field.
    Set "GreyOutDomainField=on" in rsUserAuth.ini configuration file to set Domain field uneditable.
  - Fixed welcome screen not properly displayed with different DPI Settings. Homogenization of the entire interface.

Hardware

- IGEL UD7 H850C (UD7-LX 10, UD7-LX 11): Removed hardware support.
- Added support for Intel EC1000R network device.
- Added hardware support for HP Elite mt645 G8 Mobile Thin Client.
- Added hardware support for Lenovo Thinkpad L14 Intel Gen 5.
- Updated fwupd to version 1.9.19
- Updated IGEL LVFS bios tools to allow controlling CapsuleOnDisk updates via the new parameter: fwtools.bios-tools.disable_capsule_on_disk (default: true)

- Improved hardware detection of supported LG devices.
- Added support for Quectel CAT16 WW SKU - EM160R-GL Gen2 and Quectel CAT 6 WW SKU - EM061K-GL on Lenovo ThinkPad L14 Intel Gen5

Fabulatech

- Updated FabulaTech plugins to version 4.0.0.2
- Updated FabulaTech Scanner for Remote Desktop to version 3.6.1.3
- Updated FabulaTech USB for Remote Desktop to version 6.2.0.0

Resolved Issues 11.10.150

Citrix

- Fixed not working HDX webcam redirection for Citrix 2203 and later.
- Fixed Browser Content Redirection.

AVD

- Fixed AVD session when driven from IGEL Imprivata Agent

RDP/IGEL RDP Client 2

- Fixed RDP Session dropping characters when input occurs too fast.

RD Web Access

- Fixed Passthrough and Kerberos Authentication for RD Web Access.
- Added block for keyboard shortcuts containing windows key for RD Web Access apps. Can be disabled in IGEL Setup

Registry	`rdp.rd_web_access.suppress-windows-key-shortcuts`
Value	**enabled** (default) / disabled

- Fixed RD Web Access failing with Error 400 by providing a new RD Web Tool. A switch back to the old tool is possible via IGEL Setup Registry:

Registry	`rdp.rd_web_access.options.legacy_rdweb`
Value	enabled / **disabled** (default)

Chromium

- Fixed still being able to download files if file access was disabled - occured in combination with empty download directory.

Network

- On devices that support mobile broadband and eSim an automatic switch to the physical sim slot is now performed if eSim has no profile assigned

Base system

- Fixed Post Session Command `Shutdown.

- Fixed wrong assignment of socks proxy port

Hardware

- Fixed missing firmware file for Intel 9462NGW Wi-Fi.
- Fixed LVFS BIOS update on Lenovo ThinkCentre M70q Gen3.
- Fixed microphone mute function key on HP mt645 G8.

Remote Management

- Fixed resource leak in ICG reconnect mechanism.
- Fixed: All connections / device connectors are used during OS 12 migration now.
- Fixed ICG reconnecting - now it reliably invokes a reconnect whenever a device is not connected to configured ICG server.
- Fixed UMS registering via UMS registration tool in IGEL OS - if device is registered to root directory in UMS.

Notes for Release 11.10.120

Software:	Version	11.10.120
Release Date	2024-06-18	
Release Note:	Version	RN-1110120
Last update:	2024-06-18	

Known Issues 11.10.120

Citrix

- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.

- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Selfservice is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry: userinterface.softkeyboard.autoshow userinterface.softkeyboard.autohide
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry: vmware.view.enable-serial-port-redir vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled. If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems. Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives

but forcefully uses USB-redirection which results in an unclean unmount.
As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

Cisco JVDI Client

- Citrix Workspace app 2010 may cause problems with Cisco JVDI. New ZoomVDI versions and App Protection are no longer supported.

Base system

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The Console Invocation has to allow ‘Native’ client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  ** It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.

- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Resolved Issues 11.10.120

Hardware

- Updated bios-tools to fix BIOS updates on Lenovo ThinkCentre M70q Gen3
- Updated fwupd to version 1.9.19
- Updated IGEL bios-tools to allow controlling CapsuleOnDisk updates via the parameter fwtools.bios-tools.disable_capsule_on_disk (default: true)
- Fixed microphone mute function key on HP mt645 G8.

Component Versions 11.10.120

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	124.0.6367.78-1igel1714122855
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	44.2.0.28744
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Zoom Media Plugin	5.17.6.24660
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.11.0.82
Citrix Workspace App	24.02.0.65
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8825

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.9.1
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1707744600
IGEL AVD Client	1.1.40igel1708088233
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.6.0igel1717406898
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.9-1+b1igel1709638175
Zulu JRE	17.0.11-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.13.0-2.1igel1709635747
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2312.1-8.12.1-23543969
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.25.0~rc1-1igel1709808441
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.3.37
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.10-1+b1igel1704977815
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.5-1igel1704887471
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2+b1igel1704984443
Resource Manager PC/SC Lite	2.0.3-1igel1710836080
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.15
OpenSSH Client	9.7p1-3igel1712039309
OpenSSH Server	9.7p1-3igel1712039309
Bluetooth Stack (bluez)	5.71-1igel1704700934
MESA OpenGL Stack	24.0.4-1igel1712068279
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.147.05-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-3igel1709642706
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1717760843
Xorg X11 Server	21.1.11-2igel1706715999
Xorg Xephyr	21.1.11-2igel1706715999
CUPS Printing Daemon	2.4.7-1.2+b1igel1709630190
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.1-1igel1712123636
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.5-1igel1707372108
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.14-dfsg-4igel1709105342

Virtualbox X11 Guest Utils	7.0.14-dfsg-4igel1709105342
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	8.2.2+ds-2igel1709641050

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-3.1igel1709728407
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-1+b1igel1709637921
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.14-dfsg-4igel1709105342
Virtual Background for Webcam	

Services

Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.5M	Included
Citrix StoreFront Citrix Appliance Citrix Workspace app	813.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Citrix Appliance Local Browser (Firefox)	86.2M	Included
VMware Horizon RDP	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
VMware Horizon	195.0M	Included
Voice over IP (Ekiga)	6.0M	Included

Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	372.5M	Not included
Imprivata Appliance	31.8M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.8M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.5M	Included
PrinterLogic	37.5M	Not included
Biosec BS Login	9.8M	Not included
Login VSI Login Enterprise	28.2M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.5M	Not included
AVD	42.0M	Included
Local Browser (Chromium)	106.8M	Not included
Amazon WorkSpaces Client	32.2M	Included

deskMate Client	5.5M	Included
Cisco Webex VDI	99.8M	Not included
Cisco Webex Meetings VDI	193.5M	Not included
Zoom Media Plugin	180.8M	Not included
DriveLock	12.5M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	512.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	8.0M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.8M	Included
90meter Smart Card Support	512.0K	Included
VPN OpenConnect (Limited support) Mobile Device Access USB (Limited support) Limited Support Features Virtualbox (Limited support) Scanner support / SANE (Limited support) Virtual Background for Webcam (Limited IGEL Support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	8.0M	Not included
Virtualbox (Limited support)	74.0M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.8M	Included

Supported Devices 11.10.120

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11.

New Features 11.10.120

Base system

- Added support for Lenovo Thinkpad L14 Intel Gen 5.

Hardware

- End of support for IGEL UD7 H850C (UD7-LX 10, UD7-LX 11).
- Added support for Intel EC1000R network device.
- Added support for HP mt645 G8.

Notes for Release 11.10.100

Software:	Version	11.10.100
Release Date	2024-05-16	
Release Note:	Version	RN-1110100
Last update:	2024-05-16	

The Release Notes of IGEL OS 11.10.100 are available in the following format:

readme11.10.100.txt

Supported Devices 11.10.100

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11 (see page 2452).

Component Versions 11.10.100

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	124.0.6367.78-1igel1714122855
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	44.2.0.28744
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Zoom Media Plugin	5.17.6.24660
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.11.0.82
Citrix Workspace App	24.02.0.65
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8705

Evince PDF Viewer	42.3-0ubuntu3.1
FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.9.1
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1707744600
IGEL AVD Client	1.1.40igel1708088233
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.6.0igel1710929838
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.9-1+b1igel1709638175
Zulu JRE	17.0.10-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2+b1igel1709635434
Remote Viewer (Red Hat Virtualization)	11.0-3igel1704876668
Usbredir (Red Hat Virtualization)	0.13.0-2.1igel1709635747
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2312-8.12.0-23149323
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.25.0~rc1-1igel1709808441
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.3.37
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.10-1+b1igel1704977815
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.5-1igel1704887471
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2+b1igel1704984443
Resource Manager PC/SC Lite	2.0.3-1igel1710836080
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.15
OpenSSH Client	9.7p1-3igel1712039309
OpenSSH Server	9.7p1-3igel1712039309
Bluetooth Stack (bluez)	5.71-1igel1704700934
MESA OpenGL Stack	24.0.4-1igel1712068279
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	22.0.0-1igel1704966675
Graphics Driver ATI/AMDGPU	23.0.0-1igel1705669076
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.147.05-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.6.0-1igel1704966930
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-3igel1709642706
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.6.22 #mainline-lxos-g1712816145
Xorg X11 Server	21.1.11-2igel1706715999
Xorg Xephyr	21.1.11-2igel1706715999
CUPS Printing Daemon	2.4.7-1.2+b1igel1709630190
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.22.0-3igel1705908135
GStreamer 1.x	1.24.1-1igel1712123636
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.5-1igel1707372108
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.14-dfsg-4igel1709105342

Virtualbox X11 Guest Utils	7.0.14-dfsg-4igel1709105342
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-4+b1igel1704922460
Qemu Guest Agent	8.2.2+ds-2igel1709641050

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-3.1igel1709728407
Mobile Device Access USB (imobile)	1.3.0-7.1igel1704836660
Mobile Device Access USB (gphoto)	2.5.31-2.1igel1709726214
VPN OpenConnect	9.12-1+b1igel1709637921
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.14-dfsg-4igel1709105342
Virtual Background for Webcam	

Services

Service	Size	Reduced Firmware
Asian Language Support	21.8M	Included
Java SE Runtime Environment	53.5M	Included
Citrix Workspace app Citrix Appliance Citrix StoreFront	813.0M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	86.2M	Included
VMware Horizon RDP	4.8M	Included
Cendio ThinLinc	10.8M	Included
Printing (Internet printing protocol CUPS)	18.5M	Included
NoMachine NX	26.0M	Included
VMware Horizon	195.0M	Included

Service	Size	Reduced Firmware
Voice over IP (Ekiga)	6.0M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.5M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	5.8M	Included
NVIDIA graphics driver	372.5M	Not included
Imprivata Appliance	31.8M	Included
AppliDis	256.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.8M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	61.5M	Included
PrinterLogic	37.5M	Not included
Biosec BS Login	9.8M	Not included
Login VSI Login Enterprise	28.2M	Not included
Stratusphere UX CID Key software	5.2M	Not included
Elastic Filebeat	35.5M	Not included
AVD	42.0M	Included
Local Browser (Chromium)	106.8M	Not included
Amazon WorkSpaces Client	32.2M	Included
deskMate Client	5.5M	Included
Cisco Webex VDI	99.8M	Not included
Cisco Webex Meetings VDI	193.5M	Not included
Zoom Media Plugin	180.8M	Not included

Service	Size	Reduced Firmware
DriveLock	12.5M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	512.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	8.0M	Included
HP Factory deployment documentation	88.0M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	34.8M	Included
90meter Smart Card Support	512.0K	Included
Mobile Device Access USB (Limited support) Limited Support Features VPN OpenConnect (Limited support) Virtual Background for Webcam (Limited IGEL Support) Virtualbox (Limited support) Scanner support / SANE (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.0M	Not included
Scanner support / SANE (Limited support)	8.0M	Not included
Virtualbox (Limited support)	74.0M	Not included
Virtual Background for Webcam (Limited IGEL Support)	45.8M	Included

Known Issues 11.10.100

Citrix

- Adding smartcard readers during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> *"For the entire screen"**.
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.

- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.
- If Selfservice is closed when the credential window is active, it may happen that the session cannot be restarted. A reboot is necessary.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry: userinterface.softkeyboard.autoshow userinterface.softkeyboard.autohide
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry: vmware.view.enable-serial-port-redir vmware.view.enable-scanner-redir
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled. If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/ HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems. Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives

but forcefully uses USB-redirection which results in an unclean unmount.
As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

Cisco JVDI Client

- Citrix Workspace app 2010 may cause problems with Cisco JVDI. New ZoomVDI versions and App Protection are no longer supported.

Base system

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
Workaround: The horizontal offset should be set to the width of the monitor (e.g.&#65533;if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow `Native` client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  `https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch`

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Microphone (TRRS headset) is broken on LG 27CN650

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  ** It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.

- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.10.100

Chromium

- Updated Chromium browser to version 124.0.6367.78. (ISN 2024-11)

Base system

- Fixed aom security issues CVE-2021-30475, CVE-2021-30474, CVE-2021-30473, CVE-2020-36135, CVE-2020-36133, CVE-2020-36131 and CVE-2020-36130.
- Fixed openssl security issues CVE-2024-0727, CVE-2023-5678, CVE-2023-3817 and CVE-2023-3446.
- Fixed zlib security issues CVE-2022-37434 and CVE-2018-25032.
- Fixed pipewire security issue CVE-2022-4964.
- Fixed libuv1 security issue CVE-2024-24806.
- Fixed libwebp security issue CVE-2023-4863.
- Fixed iwd security issue CVE-2024-28084.
- Fixed qemu security issue CVE-2023-6683.
- Fixed opensc security issues CVE-2024-1454 and CVE-2023-5992.
- Fixed libde265 security issues CVE-2023-49468, CVE-2023-49467, CVE-2023-49465, CVE-2023-47471, CVE-2023-43887, CVE-2023-27103, CVE-2023-27102, CVE-2023-25221, CVE-2023-24758, CVE-2023-24757, CVE-2023-24756, CVE-2023-24755, CVE-2023-24754, CVE-2023-24752, CVE-2023-24751, CVE-2022-47665, CVE-2022-43250, CVE-2022-43249, CVE-2022-43245 and CVE-2022-43244.
- Fixed postgresql-14 security issue CVE-2024-0985.
- Fixed tiff security issues CVE-2023-6277, CVE-2023-6228 and CVE-2023-52356.
- Fixed dnsmasq security issues CVE-2023-50868 and CVE-2023-50387.
- Fixed python-cryptography security issue CVE-2023-50782.
- Fixed less security issue CVE-2022-48624.
- Fixed expat security issue CVE-2024-28757.
- Fixed libxml2 security issue CVE-2024-25062.
- Fixed texlive-bin security issues CVE-2024-25262 and CVE-2023-32668.
- Fixed vim security issues CVE-2024-22667 and CVE-2023-2426.
- Fixed unixodbc security issue CVE-2024-1013.
- Fixed bash security issue CVE-2022-3715.
- Fixed util-linux security issue CVE-2024-28085.
- Fixed curl security issues CVE-2024-2398 and CVE-2024-2004.
- Fixed libvirt security issue CVE-2024-1441.
- Updated intel-microcode to version 20240312.
- Removed custom command selection from application start dialog of file manager to prevent execution of arbitrary commands by user. (ISN 2024-09)
- Fixed a privilege escalation issue in the starter license. Acknowledgements to Zack Didcott for responsible disclosure. (ISN-2014-12)

New Features 11.10.100

Citrix

- Updated Citrix Workspace App to version 2402.
  Available Citrix Workspace Apps in this release: 2402 (default), 2311 and 2010
- New features:
- Synchronize multiple keyboards at session start. All available keyboards on client are synchronized with VDA after the session starts in full-screen mode.

Parameter	`Synchronize multiple keyboards at session start`
Registry	`ica.wfclient.SyncKbdLayoutList`
Value	false (default) / true

- Support for Audio volume synchronization. Synchronize audio volume between the VDA and connected audio devices.

Parameter	`Support for Audio volume synchronization`
Registry	`ica.module.EnableVolumeSync`
Value	true (default)/ false

- Default values of the following have been changed as per Citrix.
- Enable Packet Loss Concealment to improve audio performance.
  "ica.module.PacketLossConcealmentEnabled = True"
- Loss tolerant mode for audio. "ica.module.EdtUnreliableAllowed = True"
- Use system Audio in MS Teams while screen sharing.

Parameter	`Use system Audio in MS Teams while screen sharing`
Registry	`ica.module.EnableVolumeListener`
Value	false (default)/ true

- Enhanced Desktop Viewer toolbar [Technical Preview]

Parameter	`Enhanced Desktop Viewer toolbar`
Registry	`ica.wfclient.ToolbarVersion`
Value	0 (default)/ 1

- Customize toolbar [Technical Preview]. From this version onwards, it is possible to activate or deactivate each button individually instead of the entire toolbar.

Parameter	`Show USB device button`
Registry	`ica.module.DevicesButtonVisible`
Value	true (default)/ false

- Note: Similarly, you can activate or deactivate the following buttons in the toolbar. They are all activated by default.
  ica.module.CloseButtonVisible
  ica.module.FullscreenButtonVisible
  ica.module.MinimizeButtonVisible
  ica.module.PinButtonVisible
  ica.module.PreferencesButtonVisible
  ica.module.ShortcutsButtonVisible
  ica.module.SwitchDesktopButtonVisible
- Include system audio while screen sharing in MS Teams

Parameter	`Share system audio`
Registry	`ica.teams.sharesystemaudio`
Value	false (default)/ true

- Specify the minimum and maximum range of UDP ports for Microsoft Teams optimization. If the UDP Port cannot be allocated for any reason, the WebRTC falls back to TCP. Minimum range of UDP ports for Microsoft Teams optimization.

Parameter	`UDP Port range minimum`
Registry	`ica.teams.PortRangeMin`
Value	3000

- Maximum range of UDP ports for Microsoft Teams optimization.

Parameter	`UDP Port range max`
Registry	`ica.teams.PortRangeMax`
Value	3100

Firefox

- Fixed lock of browser in kiosk mode, when URL or navigation bar are blocked:
  Firefox asks the user using a dialog to query for permissions of the current website for location access, microphone and camera use, notifications and auto-play of media streams.

In recent Firefox versions this locks the browser in case the URL-input or even the whole navigation bar are not shown.

- To prevent, following policies / parameters are added:
- If permissions are needed, these must be granted for the specific websites in advance. Note that wild-cards in the URLs cannot be used.
  These websites, depending on the type of permission, must be added here:
  browserglobal.app.permissions.microphone.allowed%.origin
  browserglobal.app.permissions.webcam.allowed%.origin
  browserglobal.app.permissions.location.allowed%.origin
  browserglobal.app.permissions.notification.allowed%.origin
  browserglobal.app.permissions.autoplay.allowed%.origin
  More...

Parameter	{{Website with microphone access}}
Registry	{{browserglobal.app.permissions.microphone.allowed%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Website without microphone access}}
Registry	{{browserglobal.app.permissions.microphone.blocked%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Block new requests for microphone access}}
Registry	{{browserglobal.app.permissions.microphone.blocknew}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Microphone access settings locked}}
Registry	{{browserglobal.app.permissions.microphone.locked}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Website with webcam access}}
Registry	{{browserglobal.app.permissions.camera.allowed%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Website without webcam access}}

Registry	{{browserglobal.app.permissions.camera.blocked%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Block new requests for webcam access}}
Registry	{{browserglobal.app.permissions.camera.blocknew}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Webcam access settings locked}}
Registry	{{browserglobal.app.permissions.camera.locked}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Allow Website to send notifications}}
Registry	{{browserglobal.app.permissions.notification.allowed%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Deny Website to send notifications}}
Registry	{{browserglobal.app.permissions.notification.blocked%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Block new notification requests}}
Registry	{{browserglobal.app.permissions.notification.blocknew}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Notification settings locked}}
Registry	{{browserglobal.app.permissions.notification.locked}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Allow autoplay on Website}}
Registry	{{browserglobal.app.permissions.autoplay.allowed%.origin}}

Type	string
Value	empty *Default*
Parameter	{{Block autoplay on Website}}
Registry	{{browserglobal.app.permissions.autoplay.blocked%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Autoplay Default}}
Registry	{{browserglobal.app.permissions.autoplay.default}}
Range	[Allow Audio and Video][Block Audio][Block Audio and Video]
Value	*Block Audio*
Parameter	{{Autoplay settings locked}}
Registry	{{browserglobal.app.permissions.autoplay.locked}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Website with location access}}
Registry	{{browserglobal.app.permissions.location.allowed%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Website without location access}}
Registry	{{browserglobal.app.permissions.location.blocked%.origin}}
Type	string
Value	empty *Default*
Parameter	{{Block new location requests }}
Registry	{{browserglobal.app.permissions.location.blocknew}}
Type	bool
Value	enabled / *disabled* (default)
Parameter	{{Location settings locked}}
Registry	{{browserglobal.app.permissions.location.locked}}
Type	bool

Value	enabled / *disabled* (default)

IGEL Agent for Imprivata

- Updated IGEL Agent for Imprivata to version 1.0.0.
- Added Features:
- Changed FUS (Fast User Switching) to be a standalone IGEL Session.
- Removed `rfideas-only barrier for virtual channel.
- Changed running text to show only the username.
- Improved logging.
- Introduced new parameter to insert command to execute on FUS user switch or logout:

Registry	`iia.fus_user_change_cmd`
Type	string
Value	"" (default)

- Introduced new reg key to configure the LockScreen shortcut:

Registry	`iia.lockscreen_shortcut`
Type	string
Value	""(default)

Resolved Issues 11.10.100

Base system

- Fixed OS12 migration issues.
- Fixed display of German Umlauts (non-ascii chars).
- Fixed password change after 2nd factor is submitted.
- Changed initial default device name and hostname of UD Pockets to "UDP". Systems already in use will only be affected after reset to factory defaults.
- Updated OpenVPN client to version 2.6.9.
- Updated GStreamer to version 1.24.1.
- Updated Virtualbox guest tools to version 7.0.14.
- Updated MESA OpenGL Stack to version 24.0.4
- Updated ATI/RADEON Graphics Driver to version 22.0.0
- Updated NVIDIA Graphics Driver to version 525.147.05
- Updated VESA Graphics Driver to version 2.6.0
- Updated ModemManager to version 1.22.0.
- Updated kernel to version 6.6.22.

Citrix

- Added registry key ica.chrome-double-download to control flock feature at wfica_wrapper. `Enable flock blocks double app starts (due to double downloads by Chromium browser).

Parameter	`Control download mechanic for Citrix applications for Chrome web access`
Registry	`ica.chrome-double-download`
Range	[Enable Lock][Disable Lock]
Value	enable / **disable** (default)

- After connecting to Citrix VDA, support for multiple audio devices sometimes may not work. This problem has been fixed.
- New parameter since CWAL-2402: Availability of Credential Insertion SDK for cloud stores (see: https://docs.citrix.com/en-us/citrix-workspace-app-for- linux/sdk-and-api.html)

Parameter	`CredentialInsertionEnabled`
Registry	`ica.authman.CredentialInsertionEnabled`
Value	false (default) / true

- Changed / corrected parameter name from KioskFUIEnhanced to KioskSFUIEnhanced

Parameter	`KioskSFUIEnhanced`
Registry	`ica.authman.KioskSFUIEnhanced`
Type	bool
Value	enabled / **disabled** (default)

- Added parameter ica.authman.longLivedTokenSupport. Previously the value was set to constant "false", now it is possible to set / configure. "true" enables re-login with Selfservice.

Parameter	`longLivedTokenSupport`
Registry	`ica.authman.longLivedTokenSupport`
Value	false (default) / true

RD Web Access

- Fixed RD Web Access failing with Error 400 by providing a new RD Web Tool. A switch back to the old tool is possible via IGEL Setup Registry:

Registry	`rdp.rd_web_access.options.legacy_rdweb`
Value	enabled / **disabled** (default)

Chromium

- Fixed blocking file access was not working if URLBlocklist was defined as custom policy.
- Fixed RDP sessions did not properly start from Chromium Browser.

Firefox

- Fixed automatic restart of Firefox sessions.
- Fixed microphone pop-up.

Network

- Added configuration for PKCS#7 encryption and signature algorithms (see sscep options -E and -S)

Parameter	{{PKCS#7 encryption algorithm}}
Registry	{{network.scepclient.cert%.encalg}}
Range	[automatic][des][3des][blowfish][aes128][aes192][aes256]
Value	__ (automatic)

Parameter	{{PKCS#7 signature algorithm}}
Registry	{{network.scepclient.cert%.signalg}}
Range	[automatic][md5][sha1][sha224][sha256][sha384][sha512]
Value	__ (automatic)

- Fixed sporadic network connection problems on Lenovo L14/L15 Gen4 AMD if ethernet cable is un- and re-plugged.

Open VPN

- Added configuration to enable legacy cryptographic algorithms for openssl.

Parameter	`Enable legacy cryptographic algorithms`
Registry	`system.openssl.legacy-cryptographic-algorithms`
Type	bool
Value	**disabled** (default) / enabled

OpenConnect VPN

- Removed dependency on ipsec-tools

HID

- Fixed touchpad activation/deactivation via hotkey.

CUPS Printing

- Fixed PrinterLogic startup.

X11 system

- Fixed crash with HP t655 and two monitors connected to G5 docking station.
- Added registry key to change the connector order of intel GPUs. Newer kernels changed the order, this can be used to revert it to former state.

Parameter	{{Reverse the connector enumeration.}}
Registry	{{x.drivers.intel.reverse_connector_enumeration}}
Range	[Default][No][Yes]
Value	*Default*

Audio

- Fixed audio on HP t240: Removed internal speaker and microphone devices as not supported. Fixed hotplug of external headsets.
- Added new entry in registry to prevent automatic switching of bluetooth profile.

Parameter	{{Set pulseaudio auto switching headset to A2DP}}
Registry	{{multimedia.pulseaudio.daemon.module-bluetooth-autoswitch-to-a2dp}}
Type	bool
Value	*enabled* (default) / disabled

- Changed: On first boot (after installation) all devices are set to 50% volume.
- Fixed headset at LG CK500

Licensing

- Fixed IGEL license detection on hardware where network interface initialization takes more time.

Hardware

- Fixed missing firmware file for intel 9462ngw WiFi.
- Added hardware recognition to include LG 24CN670IK6N for fixing related audio issues.

Notes for Release 11.09.310

Software:	Version	11.09.310
Release Date	2024-04-04	
Release Note:	Version	RN-119310
Last update:	2024-04-04	

- Supported Devices 11.09.310 (see page 2478)
- Component Versions 11.09.310 (see page 2479)
- Known Issues 11.09.310 (see page 2487)
- Security Fixes 11.09.310 (see page 2492)
- New Features 11.09.310 (see page 2493)
- Resolved Issues 11.09.310 (see page 2497)

The Release Notes of IGEL OS 11.09.310 are also available in the following format:

readme11.09.310.txt

Supported Devices 11.09.310

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11 (see page 2478).

Component Versions 11.09.310

Clients

Amazon WorkSpaces Client	4.1.0
Chromium	122.0.6261.128-1igel1710342739
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	44.2.0.28744
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Zoom Media Plugin	5.17.6.24660
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.09.0.24
Citrix Workspace App	23.11.0.82
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8705

Evince PDF Viewer	42.3-0ubuntu3
FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.9.1
IBM i Access Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1707744600
IGEL AVD Client	1.1.40igel1708088233
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.5.4igel1710255518
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
Open VPN	2.6.7-1igel1699864452
Zulu JRE	17.0.10-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389
ThinPrint Client	7-7.6.126

Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon client	2312-8.12.0-23149323
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.23.0-2igel1699446988
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.3.37
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.14
OpenSSH Client	9.6p1-2igel1704719299
OpenSSH Server	9.6p1-2igel1704719299
Bluetooth Stack (bluez)	5.71-1igel1704700934
MESA OpenGL Stack	23.1.2-1igel1686636111
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1706791905
Xorg X11 Server	21.1.11-2igel1706715999
Xorg Xephyr	21.1.11-2igel1706715999
CUPS Printing Daemon	2.4.7-1igel1696845343
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.9-1igel1707141227
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.5-1igel1707372108
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222

Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.2.1+ds-1igel1706696821

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	Size	Reduced Firmware
Asian Language Support	22.0M	Included
Java SE Runtime Environment	54.2M	Included
Citrix StoreFront Citrix Appliance Citrix Workspace app	651.5M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Local Browser (Firefox) Citrix Appliance	87.0M	Included
RDP VMware Horizon	4.2M	Included
Cendio ThinLinc	11.0M	Included
Printing (Internet printing protocol CUPS)	19.0M	Included
NoMachine NX	27.0M	Included
VMware Horizon	197.0M	Included

Service	Size	Reduced Firmware
Voice over IP (Ekiga)	6.2M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.8M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	6.0M	Included
NVIDIA graphics driver	374.0M	Not included
Imprivata Appliance	32.8M	Included
AppliDis	512.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.5M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	63.2M	Included
PrinterLogic	38.0M	Not included
Biosec BS Login	10.0M	Not included
Login VSI Login Enterprise	28.8M	Not included
Stratusphere UX CID Key software	5.5M	Not included
Elastic Filebeat	36.0M	Not included
AVD	42.2M	Included
Local Browser (Chromium)	101.8M	Not included
Amazon WorkSpaces Client	33.0M	Included
deskMate Client	5.8M	Included
Cisco Webex VDI	100.8M	Not included
Cisco Webex Meetings VDI	195.2M	Not included
Zoom Media Plugin	182.5M	Not included

Service	Size	Reduced Firmware
DriveLock	13.0M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.5M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	35.2M	Included
90meter Smart Card Support	512.0K	Included
VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Mobile Device Access USB (Limited support) Virtualbox (Limited support) Virtual Background for Webcam (Limited IGEL Support) Limited Support Features	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.2M	Not included
Scanner support / SANE (Limited support)	9.2M	Not included
Virtualbox (Limited support)	74.8M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8M	Included

Known Issues 11.09.310

Citrix

- Adding **smartcard readers** during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> "**For the entire screen**".
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version **105.0.** or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher

- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- Regarding CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074: For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
- More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit- vulnerabilities-101066782.html
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.

- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.
- Firefox restart option currently not supported.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disabling system suspend at **IGEL Setup > System > Power Options > Shutdown**.

IGEL Agent for Imprivata

- IGEL Agent for Imprivata does not work in auth only - mode with VMware Horizon.

Cisco JVDI Client

- There may be a segfault shown in the logs (during logout of Citrix Desktop session). Occurs only when using Citrix Workspace App 2010 and Cisco JVDI.

Base system

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error-not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or-higher-101059051.html for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.09.310

Chromium

- Updated Chromium Browser to version 122.0.6261.128

Firefox

- Updated Mozilla Firefox to 115.9.1 ESR
- Fixes for mfsa2024-16, also known as CVE-2024-29944.
- Fixes for mfsa2024-13, also known as:
  CVE-2024-0743, CVE-2024-2607, CVE-2024-2608, CVE-2024-2616, CVE-2023-5388, CVE-2024-2610, CVE-2024-2611, CVE-2024-2612, CVE-2024-2614.
- Fixes for mfsa2024-06, also known as:
  CVE-2024-1546, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1551, CVE-2024-1552, CVE-2024-1553.

Base system

- Fixed libxml2 security issue CVE-2024-25062

New Features 11.09.310

Citrix

- Added parameters for enhanced configuration of Teams optimization within Citrix. Further details via Citrix documentation: https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#optimization-for-microsoft-teams https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#optimization-for-microsoft-teams|smart-link]
- Configure MS Teams either via custom or predefined options.
- Custom options:
  More...

Registry	`ica.teams.config%.enabled`
Value	**disabled** (default) / enabled

Registry	`ica.teams.config%.name`
Value	“ “

Registry	`ica.teams.config%.type`
Range	[**String**] [Integer]

Registry	`ica.teams.config%.value`
Value	“ “

- Predefined options:

Parameter	AdaptResolutionAllowCroppingVideo
Registry	`ica.teams.adaptresolutionallowcroppingvideo.enabled`
Value	**Disabled** (default) / Enabled

- Enable if video in optimized MS Teams call is stretched

Parameter	EnableAEC
Registry	`ica.teams.enableaec.enabled`
Value	**Disabled** (default) / Enabled

- Enables echo cancellation; used for troubleshooting audio issues

Parameter	EnableAGC

Registry	`ica.teams.enableagc.enabled`
Value	**Enabled** (default) / Disabled

- Disables gain control; used for troubleshooting audio issues

Parameter	EnableNS
Registry	`ica.teams.enablens.enabled`
Value	**Enabled** (default) / Disabled

- Disables noise suppression; used for troubleshooting audio issues

Parameter	ms_teams_remote_audio_notifications
Registry	`ica.teams.remoteaudionotifications.enabled`
Value	**Enabled** (default) / Disabled
Parameter	ms_teams_secondary_audio_notifications
Registry	`ica.teams.secondaryaudionotifications.enabled`
Value	**Enabled** (default) / Disabled

- Disables secondary ringtone

Parameter	UseGbufferScreenSharing
Registry	`ica.teams.usegbufferscreensharing.enabled`
Value	**Disabled** (default) / Enabled

- Enables desktop share option while app protection is active

Parameter	VideoHwEncode
Registry	`ica.teams.videohwencode.enabled`
Value	**Disabled** (default) / Enabled

- Enables hardware acceleration support

Parameter	WebrpcLogLevel
Registry	`ica.teams.webrpcloglevel.enabled`
Value	**Disabled** (default) / Enabled

- Enables log collection for webrpc library

Parameter	WebrtcLogLevel

Registry	`ica.teams.webrtcloglevel.enabled`
Value	**Disabled** (default) / Enabled

- Enables log collection for virtual channel

Firefox

- Added BTRFS (improved / more efficient storage format) for Firefox profile partition.
- Changed default of system.customization.ffpro.fs_type registry key from ntfs to btrfs.

Parameter	Firefox Profiles Partition Filesystem Type
Registry	`system.customization.ffpro.fs_type`
Range	[ext4]
Value	btrfs

WiFi

- Added options for configuration of rtw89core and rtw89pci kernel modules (used e.g by the rtw_8852be driver).
  More...

Parameter	disable_clkreq
Registry	`network.drivers.rtw89pci.options.disable_clkreq`
Type	bool
Value	enabled (default) / disabled
Parameter	disable_aspm_l1
Registry	`network.drivers.rtw89pci.options.disable_aspm_l1`
Type	bool
Value	enabled (default) / disabled
Parameter	disable_aspm_l1ss
Registry	`network.drivers.rtw89pci.options.disable_aspm_l1ss`
Type	bool
Value	enabled (default) / disabled
Parameter	disable_ps_mode

Registry	`network.drivers.rtw89core.options.disable_ps_mode`
Type	bool
Value	enabled (default) / disabled

- Changed default for DHCP refresh after roaming (within the same network).

Parameter	`Refresh DHCP after roaming`
Registry	`network.interfaces.wirelesslan.device0.roam_refresh_dhcp`
Type	bool
Value	enabled / **disabled** (default)

Cisco Webex

- Updated Cisco Webex VDI plugin to version 44.2.0.28744.

zoomvdi

- Updated Zoom VDI plugin to version 5.17.6 (24660).

Resolved Issues 11.09.310

Citrix

- Citrix keyboard layout synchronization requires set of ica.wfclient.keyboardmappingfile to the new value `automatic`. With that, the local keystrokes are locally interpreted and correctly sent to the Citrix session. Icon in taskbar (within Citrix session) of set language may be wrong displayed but input is correct. It it also required to set the following parameters: ica.wfclient.keyboardeventmode=Unicode and ica.wfclient.keyboardsyncmode=Dynamic.
- Change the parameter `Keyboard mapping file` to automatic:

Setup page	`Sessions > Citrix > Citrix Global > Keyboard`
Parameter	`Keyboard mapping file`
Registry	`ica.wfclient.keyboardmappingfile`
Type	range
Value	**generic** (default) / linux / automatic

Network

- Fixed respecting NTP server from DHCP

WiFi

- On HP mt645 network.drivers.realtek.use_8852be=auto is now equal to false (same as on other devices / platforms)

Base system

- Fixed startup of System Log Viewer.

Audio

- Increased master volume for internal speaker in HP t755

Misc

- Fixed IGEL Agent for Imprivata in auth only mode with VMware Horizon.

Notes for Release 11.09.260

Software:	Version	11.09.260
Release Date:	2024-03-07	
Release Note:	Version	RN-119260-1
Last update:	2024-03-07	

- Supported Devices 11.09.260 (see page 2499)
- Component Versions 11.09.260 (see page 2500)
- Known Issues 11.09.260 (see page 2508)
- Security Fixes 11.09.260 (see page 2513)
- New Features 11.09.260 (see page 2515)
- Resolved Issues 11.09.260 (see page 2521)

The Release Notes of IGEL OS 11.09.260 are also available in the following formats:

readme_11.09.260.txt

Supported Devices 11.09.260

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX:	UD7-LX 20

See also Devices Supported by IGEL OS 11 (see page 2499).

Component Versions 11.09.260

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	120.0.6099.216-1igel1704922120
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	43.12.0.28141
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.15.2.23760
Zoom Media Plugin	5.16.10.24420
Zoom Media Plugin	5.17.5.24630
Citrix EPA Client	23.10.3
Citrix HDX Realtime Media Engine	2.9.600
Citrix Secure Access Client	23.10.3
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.09.0.24
Citrix Workspace App	23.11.0.82
deviceTRUST Citrix Channel	23.1.200
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814

Evidian AuthMgr	1.5.8705
Evince PDF Viewer	42.3-0ubuntu3
FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.7.0
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1707744600
IGEL AVD Client	1.1.40igel1708088233
deviceTRUST RDP Channel	23.1.200
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.5.4igel169355015
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.7-1igel1699864452
Zulu JRE	17.0.10-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.16.0-3389

ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon Client	2312-8.12.0-23149323
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T. SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1050
PKCS#11 Library OpenSC	0.23.0-2igel1699446988
PKCS#11 Library Pointsharp NetID Enterprise	6.9.1.17
PKCS#11 Library Pointsharp NetID Client	1.1.3.37
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3

Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.22
OpenSSL	3.0.2-0ubuntu1.14
OpenSSH Client	9.6p1-2igel1704719299
OpenSSH Server	9.6p1-2igel1704719299
Bluetooth Stack (bluez)	5.71-1igel1704700934
MESA OpenGL Stack	23.1.2-1igel1686636111
VDPAU Library Version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825

Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1706791905
Xorg X11 Server	21.1.11-2igel1706715999
Xorg Xephyr	21.1.11-2igel1706715999
CUPS Printing Daemon	2.4.7-1igel1696845343
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.9-1igel1707141227
Gstreamer 1.0 Fluendo aacdec	1.0.1
Gstreamer 1.0 Fluendo asfdemux	1.0.1
Gstreamer 1.0 Fluendo h264dec	1.0.4
Gstreamer 1.0 Fluendo mp3dec	1.0.1
Gstreamer 1.0 Fluendo mpeg4videodec	1.0.1
Gstreamer 1.0 Fluendo vadec	1.0.2
Gstreamer 1.0 Fluendo wmadec	1.0.1
Gstreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.5-1igel1707372108
WebKit2Gtk	2.40.5-1igel1700725614
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222
Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.3.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.3.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.2.1+ds-1igel1706696821

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	Size	Reduced Firmware
Asian Language Support	22.0M	Included
Java SE Runtime Environment	54.2M	Included
Citrix StoreFront Citrix Appliance Citrix Workspace app	651.5M	Included
Ericom PowerTerm InterConnect	10.0M	Included
Media Player	256.0K	Included
Citrix Appliance Local Browser (Firefox)	87.0M	Included
VMware Horizon RDP	4.2M	Included
Cendio ThinLinc	11.0M	Included

Service	Size	Reduced Firmware
Printing (Internet printing protocol CUPS)	19.0M	Included
NoMachine NX	27.0M	Included
VMware Horizon	197.0M	Included
Voice over IP (Ekiga)	6.2M	Included
Citrix Appliance	768.0K	Included
NCP Enterprise VPN Client	11.8M	Not included
Fluendo GStreamer Codec Plugins	3.2M	Included
IBM i Access Client Solutions	134.8M	Not included
Red Hat Enterprise Virtualization	2.8M	Included
Parallels Client	6.0M	Included
NVIDIA graphics driver	374.0M	Not included
Imprivata Appliance	32.8M	Included
AppliDis	512.0K	Included
Evidian AuthMgr	2.8M	Included
Hardware Video Acceleration	14.5M	Included
Extra Font Package	1.0M	Included
Fluendo GStreamer AAC Decoder	768.0K	Included
x32 Compatibility Support	4.2M	Included
Cisco JVDI client	63.2M	Included
PrinterLogic	38.0M	Not included
Biosec BS Login	10.0M	Not included
Login VSI Login Enterprise	28.8M	Not included
Stratusphere UX CID Key software	5.5M	Not included
Elastic Filebeat	36.0M	Not included
AVD	42.2M	Included
Local Browser (Chromium)	100.0M	Not included
Amazon WorkSpaces Client	33.0M	Included
deskMate Client	5.8M	Included

Service	Size	Reduced Firmware
Cisco Webex VDI	100.5M	Not included
Cisco Webex Meetings VDI	195.2M	Not included
Zoom Media Plugin	231.5M	Not included
DriveLock	13.0M	Included
SpeechWrite Client	256.0K	Included
IGEL Agent for Imprivata	768.0K	Included
LRS Output Management	256.0K	Included
Fluendo Browser Codec Plugins	9.2M	Included
HP Factory deployment documentation	88.5M	Included
BIOS Tools	2.0M	Included
HP Anyware Client	35.2M	Included
90meter Smart Card Support	512.0K	Included
Limited Support Features Scanner support / SANE (Limited support) Virtual Background for Webcam (Limited IGEL Support) VPN OpenConnect (Limited support) Virtualbox (Limited support) Mobile Device Access USB (Limited support)	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0K	Not included
VPN OpenConnect (Limited support)	1.2M	Not included
Scanner support / SANE (Limited support)	9.2M	Not included
Virtualbox (Limited support)	74.8M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8M	Included

Known Issues 11.09.260

Citrix

- Adding **smartcard readers** during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> "**For the entire screen**".
- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content- redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.

- Regarding CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074: For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
- More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit- vulnerabilities-101066782.html
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10
- Browser Content Redirection (BCR) may not work with Citrix workspace app 23.11 and current Chrome versions.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote

session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.
- Firefox restart option currently not supported.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disabling system suspend at **IGEL Setup > System > Power Options > Shutdown**.

IGEL Agent for Imprivata

- IGEL Agent for Imprivata does not work in auth only mode with VMware Horizon.

Cisco JVDI Client

- There may be a segfault shown in the logs (during logout of Citrix Desktop session). Occurs only when using Citrix Workspace App 2010 and Cisco JVDI.

Base System

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)

- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware Update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html[259] for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.
- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.

259. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error-%20not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or-%20higher-101059051.html

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.09.260

Firefox

- Updated Mozilla Firefox to 115.7 ESR
- Fixes for mfsa2024-02, also known as:
  CVE-2024-0741, CVE-2024-0742, CVE-2024-0746, CVE-2024-0747, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0755.
- Fixes for mfsa2023-54, also known as:
  CVE-2023-6856, CVE-2023-6865, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6860, CVE-2023-6867, CVE-2023-6861, CVE-2023-6862, CVE-2023-6863, CVE-2023-6864.
- Fixes for mfsa2023-50, also known as:
  CVE-2023-6204, CVE-2023-6205, CVE-2023-6206, CVE-2023-6207, CVE-2023-6208, CVE-2023-6209, CVE-2023-6212.

Base system

- Updated **ca-certificates** to version 20240203.
- Fixed a **privilege escalation** in setup_cmd utility.
- Fixed **bluez** security issue CVE-2023-45866.
- Fixed **pam** security issue CVE-2024-22365.
- Fixed **xorg-server** security issues CVE-2024-21886, CVE-2024-21885, CVE-2024-0409, CVE-2024-0408, CVE-2024-0229 and CVE-2023-6816.
- Fixed **gnutls28** security issues CVE-2024-0567 and CVE-2024-0553.
- Fixed **openldap** security issue CVE-2023-2953.
- Fixed **openssl** security issues CVE-2024-0727, CVE-2023-6237, CVE-2023-6129 and CVE-2023-5678.
- Fixed **xerces-c** security issues CVE-2023-37536 and CVE-2018-1311.
- Fixed **mysql-8.0** security issues CVE-2024-20985, CVE-2024-20984, CVE-2024-20983, CVE-2024-20982, CVE-2024-20981, CVE-2024-20978, CVE-2024-20977, CVE-2024-20976, CVE-2024-20974, CVE-2024-20973, CVE-2024-20972, CVE-2024-20971, CVE-2024-20970, CVE-2024-20969, CVE-2024-20967, CVE-2024-20966, CVE-2024-20965, CVE-2024-20964, CVE-2024-20963, CVE-2024-20962, CVE-2024-20961 and CVE-2024-20960.
- Fixed **paramiko** security issue CVE-2023-48795.
- Fixed **pillow** security issues CVE-2023-50447 and CVE-2023-44271.
- Fixed **pycryptodome** security issue CVE-2023-52323.
- Fixed **qtbase-opensource-src** security issue CVE-2023-51714.
- Fixed **qemu** security issues CVE-2023-6693 and CVE-2023-6683.
- Fixed **zulu17-ca** security issues CVE-2024-20932, CVE-2024-20926, CVE-2024-20925, CVE-2024-20923, CVE-2024-20922, CVE-2024-20918, CVE-2024-20952, CVE-2024-20945, CVE-2024-20921 and CVE-2024-20919.
- Fixed **curl** security issue CVE-2024-0853.
- Fixed **expat** security issues CVE-2023-52426 and CVE-2023-52425.
- Fixed **webkit2gtk** security issues CVE-2024-23222, CVE-2024-23213, CVE-2024-23206, CVE-2023-42833, CVE-2023-40414 and CVE-2014-1745.

- Fixed **libde265** security issues CVE-2022-43253, CVE-2022-43252, CVE-2022-43248, CVE-2022-43243, CVE-2022-43242, CVE-2022-43241, CVE-2022-43240, CVE-2022-43239, CVE-2022-43238, CVE-2022-43237, CVE-2022-43236, CVE-2022-43235, CVE-2022-1253, CVE-2021-36411, CVE-2021-36410, CVE-2021-36409, CVE-2021-36408 and CVE-2021-35452.
- Fixed **gst-plugins-bad1.0** security issues CVE-2024-0444, CVE-2023-44446, CVE-2023-44429, CVE-2023-40476, CVE-2023-40475 and CVE-2023-40474.
- Fixed **bind9** security issues CVE-2023-5679, CVE-2023-5517, CVE-2023-50868, CVE-2023-50387 and CVE-2023-4408.
- Fixed **shadow** security issue CVE-2023-4641.
- Fixed **qtbase-opensource-src** security issue CVE-2024-25580.
- Fixed **libde265** security issues CVE-2023-25221, CVE-2023-24758, CVE-2023-24757, CVE-2023-24756, CVE-2023-24755, CVE-2023-24754, CVE-2023-24752, CVE-2023-24751, CVE-2022-47665, CVE-2022-43250, CVE-2022-43249, CVE-2022-43245 and CVE-2022-43244.
- Fixed **libpq5** security issue CVE-2024-0985.
- Fixed **libtiff5** security issues CVE-2023-6228, CVE-2023-6277 and CVE-2023-52356.
- Fixed **dnsmasq** security issues CVE-2023-50868 and CVE-2023-50387.
- Fixed **python-cryptography** security issue CVE-2023-50782.
- Fixed **less** security issue CVE-2022-48624.
- Fixed **libuv1** security issue CVE-2024-24806.
- Fixed **libssh1.1** security issues 2023-3446 and CVE-2023-3817.

New Features 11.09.260

AVD

- Updated AVD client to version 1.1.40.
- Improved login speed.
- Added support for Okta and Ping Identity IDPs.
- Fixed resizing if external monitor is disconnected while laptop lid is closed and opened again.

VMware Horizon

- Updated VMware Horizon client to version 2312-8.12.0-23149323
  More...

Parameter	`Lock user name`
Registry	`vmware.view.lock-user-name`
Range	[on][off]
Value	**off**

Parameter	`Lock user name`
Registry	`sessions.vdm_client%.options.lock-user-name`
Range	[Global setting][on][off]
Value	**Global setting**

ThinLinc

- Updated ThinLinc to version 4.16.0 to fix CVE-2023-3446, CVE-2023-3817, CVE-2023-4807, CVE-2023-5678.

deviceTRUST

- Updated deviceTRUST Client Extension to version 23.1.200.
- Added support for IGEL Remote Desktop (RDP3) sessions.
  More...

Parameter	deviceTRUST
Registry	sessions.msigelrdp.plugins.devicetrust

Value	disabled (default)/ enabled

Network

- Added WWAN support on HP mt440 device with BIOS v1.08.00 and Intel XMM7560 module Firmware v1.16.48.

Smartcard

- Updated Pointsharp Net iD Client to version 1.1.3.37. All details via https://docs.pointsharp.com/net-id-client/latest/nic-release-notes/nic-113-release-notes.html

Base system

- Added ready-made challenge password retrieval for Microsoft NDES
- Set the following to NDES for enabling the feature:
  More...

Parameter	`Ready-made Challenge Password Command`
Registry	`network.scepclient.cert%.use_ready_made_challenge_password_command`
Range	[none][NDES]
Value	**none**
Parameter	`User name`
Registry	`network.scepclient.cert%.ndes.challenge_password_retrieval.user`
Type	string
Value	empty **Default**
Parameter	`Password`
Registry	`network.scepclient.cert%.ndes.challenge_password_retrieval.crypt_password`
Type	string
Value	empty **Default**

- If the following is not 'none', https will be used. The default "getca" means the CA certificate received in the SCEP GetCA operation. The full path to a different CA certificate may also be specified
  More...

Parameter	`CA certificate`
Registry	`network.scepclient.cert%.ndes.challenge_password_retrieval.cacert`
Range	[none (not using https)][from getca operation]
Value	**from getca operation**
Parameter	`Debug level`
Registry	`network.scepclient.cert%.ndes.challenge_password_retrieval.debuglevel`
Type	integer
Value	0 **Default**

- Added registry key to prevent terrapin attack (mitigation is not active as default) on the SSH server:
  More...

Parameter	Disable weak MACs and Chipers to prevent terrapin attack.
Registry	network.ssh_server.enable_terrapin_mitigation
Type	bool
Value	enabled / *disabled* (default)

- Added registry key to prevent terrapin attack (mitigation is not active as default) on the SSH client:
  More...

Parameter	Disable weak MACs and Chipers to prevent terrapin attack.
Registry	network.ssh_client.enable_terrapin_mitigation
Type	bool
Value	enabled / *disabled* (default)

- Added power saving settings for Intel and AMD devices.
- Changed some powersave settings defaults to *Auto* so powersave is enabled as default on Lenovo laptops:
  More...

Parameter	Use powertop auto tune to reduce power usage
Registry	system.powersave.powertop_auto_tune
Range	[Auto][Enable][Disable]
Value	*Auto*

Parameter	Use laptop mode to reduce power usage
Registry	system.powersave.laptop_mode
Range	[Auto][Enable][Disable]
Value	*Auto*

Parameter	Clock down AMDGPU if system is idle (idle action time reached).
Registry	system.powersave.clock_down_amdgpu_on_idle
Range	[Auto][Enable][Disable]
Value	*Auto*

Parameter	Set Ryzen CPU to power save mode if system is idle (idle action time reached).
Registry	system.powersave.use_ryzenadj_on_idle
Range	[Auto][Enable][Disable]
Value	*Auto*

- Set idle action default time to 50 seconds:
  More...

Parameter	Call idle actions on AC after this time of inactivity (greater 10 seconds, value 9 or lower is never)
Registry	system.powersave.idle_action_on_ac
Type	integer
Value	50 *Default*

Parameter	Call idle actions on battery after this time of inactivity (greater 10 seconds, value 9 or lower is never)
Registry	system.powersave.idle_action_on_battery
Type	integer
Value	50 *Default*

- Added registry keys for Intel system specific power saving settings:
  More...

Parameter	Clock down Intel GPU if system is idle (idle action time reached).
Registry	system.powersave.clock_down_i915_on_idle
Range	[Auto][Enable][Disable]
Value	*Auto*

Parameter	Set Intel CPU to power save mode if system is idle (idle action time reached).
Registry	system.powersave.use_energy_policy_on_idle
Range	[Auto][Enable][Disable]
Value	*Auto*

- Changed default of power saving settings for screen getting dimmed to 20% after 120 seconds inactivity.
  More...

Setup page	`System > Power Options > Display > Brightness Reduction`
Parameter	`Reduce after`
Registry	`x.xserver%.brightness_on_ac`
Type	integer
Value	120 **Default**

Parameter	`Reduce after`
Registry	`x.xserver%.brightness_on_battery`
Type	integer
Value	120 **Default**

Parameter	`On inactivity reduce to`
Registry	`x.xserver%.brightness_level_ac`
Type	integer
Value	20 **Default**

Driver

- Updated Thales SafeNet Authentication Client to version 10.8.1050.

zoomvdi

- Updated Zoom VDI plugin to version 5.17.5 (24500).

Hardware

- Added support for Lenovo USB-C to Ethernet Adapter
- Added hardware support for HP Elite t755.
- Added BIOS configuration support for HP Elite t755. IGEL supports the BIOS update mechanism. The BIOS update itself is validated by the device manufacturer and performed at your own risk.

Resolved Issues 11.09.260

Citrix

- Missing icons are now displayed.

Remote Desktop (RDP3)

- Fixed IGEL Remote Desktop (RDP3) audio input redirection.

VMware Horizon

- Updated VMware Horizon Client to version 2312-8.12.0-23149323 which fixes setting the relative mouse feature

Network

- Added registry key for ignoring hostname received via DHCP

Parameter	Ignore hostname received via DHCP
Registry	network.dns.hostname_ignore_dhcp
Type	bool
Value	enabled / *disabled* (default)

WiFi

- Added certain module options for configuration of iwlwifi/iwlmvm drivers. For details the output of the modinfo command can be used.

Parameter	11n_disable
Registry	network.drivers.iwlwifi.options.o_11n_disable
Type	integer
Value	0 *Default*
Parameter	disable_11ac
Registry	network.drivers.iwlwifi.options.disable_11ac
Type	bool
Value	enabled / *disabled* (default)
Parameter	disable_11ax

-

Registry	network.drivers.iwlwifi.options.disable_11ax
Type	bool
Value	enabled / *disabled* (default)
Parameter	disable_11be
Registry	network.drivers.iwlwifi.options.disable_11be
Type	bool
Value	enabled / *disabled* (default)
Parameter	bt_coex_active
Registry	network.drivers.iwlwifi.options.bt_coex_active
Type	bool
Value	*enabled* (default) / disabled
Parameter	power_save
Registry	network.drivers.iwlwifi.options.power_save
Type	bool
Value	enabled / *disabled* (default)
Parameter	power_level
Registry	network.drivers.iwlwifi.options.power_level
Type	integer
Value	0 *Default*
Parameter	swcrypto
Registry	network.drivers.iwlwifi.options.swcrypto
Type	bool
Value	enabled / *disabled* (default)
Parameter	power_scheme
Registry	network.drivers.iwlmvm.options.power_scheme
Type	integer
Value	2 *Default*

HID

- Improved palm detection on certain newer laptops via change of default for parameter "userinterface.touchpad.driver". This has changed from "Synaptics" to 'Auto'. 'Auto' setting will set the actual driver to Synaptics for most devices but to Libinput for HP mt440 G3 and HP mt645 G7 notebooks. By changing 'userinterface.touchpad.driver' to 'Synaptics' or 'Libinput', the auto mechanism is overwritten.

Firmware Update

- Fixed firmware update process on encrypted devices. The PIN prompt is shown now before update starts - in case a reboot is needed during the update process.
- Fixed OS12 migration on devices with 4GB IGEL Partition.
- Fixed OS 12 Migration with HP_TOOLS partition present.
- Fixed fallback to IGEL App Portal in case of migrating to OS12 and usage UMS as App Proxy but UMS is not reachable.
- Fixed sporadic premature break while writing downloaded firmware data to the local storage.

VirtualBox

- Fixed mouse offset if using multimonitor setup as VirtualBox guest.

Audio

- Fixed internal microphone on Fujitsu E5412.
- Fixed: The headphone jack port on front of HP t755 is now the prioritized one
- in case the port on the back is also used.

Hardware

- Fixed screen lagging issue with Dell Latitude 7430
- Added possibility to configure Intel PSR setting via registry

Parameter	`Change settings for intel PSR (panel self refresh).`
Registry	`x.drivers.intel.psr`
Range	[Default][Disable][Enable][Use only up to PSR1][Use up to PSR2]
Value	**Default**

Remote Management

- Fixed handling of CA chains missing certificates of public CAs.
- Reworked the EST protocol implementing the TLS certificate enrollement.
- Fixed certificate verifying of the UMS server in case of using legacy weak keys.
- Fixed: Required session renegotiation on TLS v1.2 connections used in the IGEL remote management.

Notes for Release 11.09.210

Software:	Version	11.09.210
Release Date:	2024-01-25	
Release Note:	Version	RN-119210-1
Last update:	2024-01-25	

- Supported Devices 11.09.210 (see page 2525)
- Component Versions 11.09.210 (see page 2526)
- Known Issues 11.09.210 (see page 2534)
- Security Fixes 11.09.210 (see page 2538)
- New Features 11.09.210 (see page 2539)
- Resolved Issues 11.09.210 (see page 2543)

The Release Notes of IGEL OS 11.09.210 are also available in the following formats:

readme_11.09.210.txt

Supported Devices 11.09.210

UD2-LX:	UD2-LX 52 UD2-LX 51
UD3-LX:	UD3-LX 60
UD7-LX	UD7-LX 20

See also Devices Supported by IGEL OS 11 (see page 2525).

Component Versions 11.09.210

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	120.0.6099.216-1igel1704922120
Cisco JVDI Client	14.3.0
Cisco Webex VDI plugin	43.12.0.28141
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.8.4
Zoom Media Plugin	5.14.10.23670
Zoom Media Plugin	5.15.2.23760
Zoom Media Plugin	5.16.10.24420
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.09.0.24
Citrix Workspace App	23.11.0.82
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8705
Evince PDF Viewer	42.3-0ubuntu3

FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.4.0
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1700473865
IGEL AVD Client	1.1.37igel1703077078
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
IGEL Agent for Imprivata	0.5.4igel169355015
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.7-1igel1699864452
Zulu JRE	17.0.9-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269

VNC Viewer	1.13.1+igel-1igel1697962544
VMware Horizon Client	2309-8.11.0-22660930
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-2igel1699446988
PKCS#11 Library SecMaker NetID Enterprise	6.9.1.17
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	3.0.0.45
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.19
OpenSSL	3.0.2-0ubuntu1.12
OpenSSH Client	9.6p1-2igel1704719299
OpenSSH Server	9.6p1-2igel1704719299
Bluetooth stack (bluez)	5.66-1igel1669186181
MESA OpenGL stack	23.1.2-1igel1686636111
VDPAU Library version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1700545132
Xorg X11 Server	21.1.10-1igel1703307487
Xorg Xephyr	21.1.10-1igel1703307487
CUPS printing Daemon	2.4.7-1igel1696845343
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.4-1igel1690179327
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.4-1igel1702918021
WebKit2Gtk	2.40.5-1igel1700725614
Python2	2.7.18
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222
Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.1.5-3~ubuntu0.22.04.4
Open VM Desktop Tools	12.1.5-3~ubuntu0.22.04.4
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.1.1+ds-2igel1696844559

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.0 M	Included
Java SE Runtime Environment	54.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	651.5 M	Included
Ericom PowerTerm InterConnect	10.0 M	Included
Media Player	256.0 K	Included
Local Browser (Firefox) Citrix Appliance	86.8 M	Included

VMware Horizon RDP	4.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	19.0 M	Included
NoMachine NX	27.0 M	Included
VMware Horizon	190.5 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	11.8 M	Not included
Fluendo GStreamer Codec Plugins	3.2 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	378.2 M	Not included
Imprivata Appliance	32.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	768.0 K	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	63.2 M	Included
PrinterLogic	38.0 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	36.0 M	Not included
AVD	41.8 M	Included
Local Browser (Chromium)	100.0 M	Not included

Amazon WorkSpaces Client	32.5 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	100.5 M	Not included
Cisco Webex Meetings VDI	195.2 M	Not included
Zoom Media Plugin	208.5 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	768.0 K	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	9.2 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	35.2 M	Included
90meter Smart Card Support	512.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	9.2 M	Not included
VirtualBox (Limited support)	74.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8 M	Included

Known Issues 11.09.210

Citrix

- Adding **smartcard readers** during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> "**For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.
- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- Regarding CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074:
  For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
  More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit-vulnerabilities-101066782.html
- ZoomVDI version 5.16 or newer is no longer supported with Citrix Workspace app 20.10.
- Browser Content Redirection (BCR) may not work with Citrix Worspace app 23.11 and current Chrome versions.

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Chromium

- Hardware accelerated video decoding is currently not supported.

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.
- Firefox restart option currently not supported.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

Cisco JVDI Client

- There may be a segfault shown in the logs (during logout of Citrix Desktop session). Occurs only when using Citrix Workspace App 2010 and Cisco JVDI.

Base System

- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.
- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware Update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-08-or- higher-101059051.html for a possible solution and additional information.

Appliance Mode

- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Security Fixes 11.09.210

Base System

- Fixed **webkit2gtk** issues CVE-2023-42916, CVE-2023-42917, CVE-2023-42883 and CVE-2023-42890.
- Fixed **vim** security issues
  More...

  CVE-2023-48706, CVE-2023-48237, CVE-2023-48236, CVE-2023-48235, CVE-2023-48234, CVE-2023-48233, CVE-2023-48231, CVE-2023-46246, CVE-2022-2042, CVE-2022-2000, CVE-2022-1897, CVE-2022-1886, CVE-2022-1771 and CVE-2022-1725.
- Fixed **curl** security issues CVE-2023-46219 and CVE-2023-46218.
- Fixed **avahi** security issues CVE-2023-38473, CVE-2023-38472, CVE-2023-38471, CVE-2023-38470 and CVE-2023-38469.
- Fixed **glibc** security issues CVE-2023-5156, CVE-2023-4813 and CVE-2023-4806.
- Fixed **gnutls28** security issue CVE-2023-5981.
- Fixed **ghostscript** security issue CVE-2023-46751.
- Fixed **nghttp2** security issue CVE-2023-44487.
- Fixed **poppler** security issues CVE-2022-38349, CVE-2022-37052, CVE-2022-37051 and CVE-2022-37050.
- Fixed **postgresql-14** security issues CVE-2023-5870, CVE-2023-5869 and CVE-2023-5868.
- Fixed **python3.10** security issue CVE-2023-40217.
- Fixed **sqlite3** security issues CVE-2023-7104 and CVE-2022-46908.
- Fixed **tiff** security issues CVE-2023-3576 and CVE-2022-40090.
- Fixed **yajl** security issues CVE-2023-33460, CVE-2022-24795 and CVE-2017-16516.
- Fixed **python-cryptography** security issues CVE-2023-49083 and CVE-2023-23931.
- Fixed **tar** security issue CVE-2023-39804.
- Fixed **libssh2** security issue CVE-2023-48795.
- Fixed **libssh** security issues CVE-2023-6918, CVE-2023-6004 and CVE-2023-48795.
- Fixed **openssh** security issues CVE-2023-51385, CVE-2023-51384 and CVE-2023-48795.

X Server

- Fixed **xorg-server** security issues CVE-2023-6478 and CVE-2023-6377.

New Features 11.09.210

Citrix

- Added: Notification handling for applications launched via Citrix Self- Service, Browser or Storebrowse.
- Added Citrix Workspace App 2311
  Available Citrix Workspace Apps in this release: 2311, 2309 (default) and 2010
- Fast SmartCard Feature
  More...

Parameter	`SmartCardCryptographicRedirection`
Registry	`ica.module.virtualdriver.smartcard.SmartCardCryptographicRedirection`
Type	bool
Value	enabled / **disabled** (default)

Fast smartcard is an improvement over the existing HDX PC/SC-based smartcard redirection. It improves performance when smartcards are used in high-latency WAN environments.

- Improved loading experience for shared user mode
  More...

Parameter	`KioskFUIEnhanced`
Registry	`ica.authman.KioskFUIEnhanced`
Type	bool
Value	enabled / **disabled** (default)

The time taken to load the store is reduced and thus the loading experience for the shared user mode is improved.

- Collecting user activity logs
  More...

Parameter	`UserActivityLogsDisabled`
Registry	`ica.authman.UserActivityLogsDisabled`
Type	bool
Value	**enabled** (default) / disabled

It is now possible to collect the user activity logs. Activities related to most of the Storebrowse commands are saved in the log file.
/userhome/.ICAClient/logs/userActivitylog/

AVD

- Added full support for the secondary ringer feature for MS-Teams optimization.
- Updated IGEL AVD client to version 1.1.37.

VMware Horizon

- Updated VMware Horizon Client to version 2309 8.11.0-22660930
  More...

Parameter	`Disable network state display`
Registry	`vmware.view.blast-network-state`
Type	bool
Value	enabled / **disabled** (default)
Parameter	`Allow Blast connections to use proxy settings`
Registry	`vmware.view.blast-proxy`
Type	bool
Value	enabled / **disabled** (default)
Parameter	`Allow changing the use of HEVC decoding`
Registry	`vmware.view.allow-enable-hevc`
Type	bool
Value	**enabled** (default) / disabled
Parameter	`Blast HEVC decoding`
Registry	`vmware.view.blast-hevc`
Type	bool
Value	**enabled** (default) / disabled
Parameter	`Blast AV1 decoding`

Registry	`vmware.view.blast-av1`
Type	bool
Value	**enabled** (default) / disabled
Parameter	`High Color Accuracy mode for Blast/HEVC`
Registry	`vmware.view.high-color-accuracy-mode-hevc`
Type	bool
Value	enabled / **disabled** (default)

Chromium

- Updated Chromium Browser to version 120.0.6099.216.

Network

- Added Quectel EM05-G support for Lenovo ThinkPad L13 AMD Gen4 and L13 Intel Gen4.
- Added regional support with Quectel EM05-G for US SIM cards on supported Lenovo Laptop devices.

Smartcard

- Updated Pointsharp (SecMaker) Net iD Enterprise to version 6.9.1.17.
- Updated 90meter PKCS#11 library to version 3.0.0.45. Besides the SIPR version of the library, the NIPR version is added now. Additional smartcard types, specified by ATR, are possible to add to allow list.
  More...

Parameter	`Library type`
Registry	`scard.pkcs11.90meter.library_type`
Value	**SIPR**, NIPR
Parameter	`Log level`
Registry	`scard.pkcs11.90meter.loglevel`
Value	**none**, error, warn, trace
Parameter	`Log file`

Registry	`scard.pkcs11.90meter.logfile`
Value	**/var/log/lib90meterpk11.log**
Parameter	`Card name`
Registry	`scard.pkcs11.90meter.card%.name`
Value	**(empty)**
Parameter	`ATR`
Registry	`scard.pkcs11.90meter.card%.atr`
Value	**(empty)**
Parameter	`ATR mask`
Registry	`scard.pkcs11.90meter.card%.mask`
Value	**(empty)**

Cisco JVDI Client

- Updated Cisco JVDI to version 14.3.0.

Cisco Webex

- Integrated Cisco Webex Meetings VDI 43.6.8.4
- Updated Cisco Webex VDI to version 43.12.0.28141.

Zoomvdi

- Added Zoom VDI 5.16.10.24420.
- Available Zoom VDI plugins: 5.16.10.24420 (default), 5.15.2.23760, and 5.14.10.23670

Hardware

- Added hardware support for LG AiO 27CQ650.
- Added hardware support for LG AiO 34CR650.
- Removed: Support ended for UD2-LX 40 (D220), UD2-LX 50 (M250C 4GB eMMC), UD3-LX 51 (M340C) and UD6-LX 51 (H830C) .
- Added hardware support for Lenovo ThinkPad L13 Intel Gen4.
- Added hardware support for Lenovo ThinkPad L13 AMD Gen4.

Resolved Issues 11.09.210

Citrix

- Fixed: The error message **_Broken Pipe_* should no longer appears during login process.
- Fixed usage of Ctrl+Alt+End in Citrix sessions.

AVD

- Fixed issues when multiple workspace resources have the same name.
- Fixed AVD app taskbar issues when apps are closed.

RD Web Access

- Fixed possible error when starting Remote Desktop Web Access applications.

VMware Horizon

- Fixed switch for serial port- and scanner redirection in UMS Web App by using a checkbox instead of customized on/off dropdown box.

Network

- Added new registry key to switch between 8852be and rtw_8852be WiFi driver (Auto will use the 8852be on HP mt645 G7)
  More...

Parameter	Use 8852be driver instead of rtw_8852be for WLAN.
Registry	network.drivers.realtek.use_8852be
Range	[Auto][Yes][No]
Value	*Auto*

HID

- Fixed handling / calibration of ELO touch devices in multi-monitor configuration.

CUPS Printing

- Fixed handling of SMB network printers.

Base system

- Fixed: Post-Session Command for VMware Horizon and protocol RDP.

Notes for Release 11.09.160

Software:	Version	11.09.160
Release Date:	2023-12-20	
Release Note:	Version	RN-1109160-1
Last update:	2023-12-20	

- Supported Devices 11.09.160 (see page 2546)
- Component Version 11.09.160 (see page 2547)
- Known Issues 11.09.160 (see page 2555)
- Security Fixes 11.09.160 (see page 2560)
- Resolved Issues 11.09.160 (see page 2561)

The Release Notes of IGEL OS 11.09.160 are also available in the following formats:

readme11.09.160.txt

Supported Devices 11.09.160

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX	UD6-LX 51
UD7-LX	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also, Devices Supported by IGEL OS 11.

Component Version 11.09.160

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	119.0.6045.159-1igel1700049809
Cisco JVDI Client	14.2.1
Cisco Webex VDI plugin	43.10.0.27853
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.0.158
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.10.23670
Zoom Media Plugin	5.15.2.23760
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.07.0.17
Citrix Workspace App	23.09.0.24
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8705
Evince PDF Viewer	42.3-0ubuntu3

FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.4.0
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1700473865
IGEL AVD Client	1.1.35igel1700067194
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.7-1igel1699864452
Zulu JRE	17.0.9-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.08.1-22.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544

VMware Horizon Client	2306-8.10.0-21964631
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-2igel1699446988
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.19
OpenSSL	3.0.2-0ubuntu1.12
OpenSSH Client	9.4p1-1igel1697178356
OpenSSH Server	9.4p1-1igel1697178356
Bluetooth stack (bluez)	5.66-1igel1669186181
MESA OpenGL stack	23.1.2-1igel1686636111
VDPAU Library version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891

Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1700545132
Xorg X11 Server	21.1.9-1igel1698314180
Xorg Xephyr	21.1.9-1igel1698314180
CUPS printing Daemon	2.4.7-1igel1696845343
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.4-1igel1690179327
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.2-1igel1699738005
WebKit2Gtk	2.40.5-1igel1700725614
Python2	2.7.18
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222

Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.1.5-3~ubuntu0.22.04.4
Open VM Desktop Tools	12.1.5-3~ubuntu0.22.04.4
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.1.1+ds-2igel1696844559

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.0 M	Included
Java SE Runtime Environment	54.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	761.5 M	Included
Ericom PowerTerm InterConnect	10.0 M	Included
Media Player	256.0 K	Included
Local Browser (Firefox) Citrix Appliance	86.8 M	Included
VMware Horizon RDP	4.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	19.0 M	Included

NoMachine NX	27.0 M	Included
VMware Horizon	176.8 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	11.8 M	Not included
Fluendo GStreamer Codec Plugins	3.2 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	378.2 M	Not included
Imprivata Appliance	32.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	768.0 K	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	63.2 M	Included
PrinterLogic	38.0 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	36.0 M	Not included
AVD	41.8 M	Included
Local Browser (Chromium)	99.2 M	Not included
Amazon WorkSpaces Client	32.5 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	100.5 M	Not included
Cisco Webex Meetings VDI	193.2 M	Not included

Zoom Media Plugin	161.8 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	768.0 K	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	9.2 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	35.2 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	9.2 M	Not included
VirtualBox (Limited support)	74.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8 M	Included

Known Issues 11.09.160

Citrix

- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:
  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> "**For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.

- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- Regarding CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074:
  For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
  More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit-vulnerabilities-101066782.html

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
  This happens only with enabled scanner or serial port redirection.
  The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.

Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then.However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount. As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.
- Firefox restart option currently not supported.

Chromium

- Hardware accelerated video decoding is currently not supported.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disabling system suspend at IGEL Setup > System > Power Options > Shutdown.

Cisco JVDI Client

- There may be a segfault shown in the logs (during logout of Citrix Desktop session). Occurs only when using Citrix Workspace App 2010 and Cisco JVDI.

Base system

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.

- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or- higher-32870765.html[260] for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch

Audio

- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

260. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-%20not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or-%20higher-32870765.html

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.09.160

Base system

- Fixed **libminizip1** security issue CVE-2023-45853.
- Fixed **perl** security issues CVE-2022-48522, CVE-2023-47038.

Resolved Issues 11.09.160

RD Web Access

- Fixed possible error when starting Remote Desktop Web Access applications.

Notes for Release 11.09.150

Software:	Version	11.09.150
Release Date:	2023-12-06	
Release Note:	Version	RN-1109150-1
Last update:	2023-12-06	

- Supported Devices 11.09.150 (see page 2563)
- Component Version 11.09.150 (see page 2564)
- Known Issues 11.09.150 (see page 2572)
- Security Fixes 11.09.150 (see page 2577)
- New Features 11.09.150 (see page 2579)
- Resolved Issues 11.09.150 (see page 2587)

The Release Notes of IGEL OS 11.09.150 are also available in the following formats:

Addendum to the Notes for Release 11.09.150

Please note the following notes concerning the registry key `iia.hide_horizon_apps_on_chooser`:

- With `iia.hide_horizon_apps_on_chooser` enabled, if the user only has one desktop assigned, the desktop will be launched (honors Imprivata VDA policy setting).
- KNOWN ISSUE: With the `iia.high_horizon_apps_on_chooser` setting enabled, the app filter engages too quickly and you will see an error message: “Entitlement Not Found”.
  Resolution: Disable this setting.
  Result: If the user has more than one Horizon desktop resource, the chooser will show both desktops and apps (no filter applied).
  This will be fixed in an upcoming agent release.

Supported Devices 11.09.150

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50 ~~UD2-LX 40~~*
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX	UD6-LX 51
UD7-LX	UD7-LX 20 UD7-LX 11 UD7-LX 10

*This device is not supported and was listed incorrectly.

See also, Devices Supported by IGEL OS 11.

Component Version 11.09.150

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	119.0.6045.159-1igel1700049809
Cisco JVDI Client	14.2.1
Cisco Webex VDI plugin	43.10.0.27853
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.0.158
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.10.23670
Zoom Media Plugin	5.15.2.23760
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.07.0.17
Citrix Workspace App	23.09.0.24
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.7.0.44352
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8705
Evince PDF Viewer	42.3-0ubuntu3

FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.4.0
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1700473865
IGEL AVD Client	1.1.35igel1700067194
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.7-1igel1699864452
Zulu JRE	17.0.9-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.13.1+igel-1igel1697962544

VMware Horizon Client	2306-8.10.0-21964631
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B308
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-2igel1699446988
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.19
OpenSSL	3.0.2-0ubuntu1.12
OpenSSH Client	9.4p1-1igel1697178356
OpenSSH Server	9.4p1-1igel1697178356
Bluetooth stack (bluez)	5.66-1igel1669186181
MESA OpenGL stack	23.1.2-1igel1686636111
VDPAU Library version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891

Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1700545132
Xorg X11 Server	21.1.9-1igel1698314180
Xorg Xephyr	21.1.9-1igel1698314180
CUPS printing Daemon	2.4.7-1igel1696845343
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.4-1igel1690179327
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.2-1igel1699738005
WebKit2Gtk	2.40.5-1igel1700725614
Python2	2.7.18
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222

Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.1.5-3~ubuntu0.22.04.4
Open VM Desktop Tools	12.1.5-3~ubuntu0.22.04.4
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.1.1+ds-2igel1696844559

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.0 M	Included
Java SE Runtime Environment	54.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	761.5 M	Included
Ericom PowerTerm InterConnect	10.0 M	Included
Media Player	256.0 K	Included
Local Browser (Firefox) Citrix Appliance	86.8 M	Included
VMware Horizon RDP	4.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	19.0 M	Included

NoMachine NX	27.0 M	Included
VMware Horizon	176.8 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	11.8 M	Not included
Fluendo GStreamer Codec Plugins	3.2 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	378.2 M	Not included
Imprivata Appliance	32.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	768.0 K	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	63.2 M	Included
PrinterLogic	38.0 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	36.0 M	Not included
AVD	41.8 M	Included
Local Browser (Chromium)	99.2 M	Not included
Amazon WorkSpaces Client	32.5 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	100.5 M	Not included
Cisco Webex Meetings VDI	193.2 M	Not included

Zoom Media Plugin	161.8 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	768.0 K	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	9.2 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	35.2 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	9.2 M	Not included
VirtualBox (Limited support)	74.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8 M	Included

Known Issues 11.09.150

Citrix

- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:
  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active session does not work. The reader is visible, but cannot be used due to unknown reader status. Only relevant for CWA versions earlier than 2112.
- Browser Content Redirection (BCR) does not work if DRI3 and hardware accelerated H.264 deep compression codec is enabled.
- Citrix H.264 acceleration plugin does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" -> "**For the entire screen"**.
- Currently H.264 for Citrix sessions cannot be used in parallel with video input acceleration.
- While starting Self-Service, it is possible that process ServiceRecord segfaults -> Self-Service cannot be started afterwards.
  A cache cleanup with reboot is needed. In addition, the following parameters should set to true.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- Browser Content Redirection (BCR) may not work with Chrome version 105.0.* or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher
- White / green fragments may appear during desktop launch if JPEG graphical codec is used.

- MS Teams calls may stop if blurred background is enabled. This affects Citrix Workspace App 2305 and later.
- Regarding CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074:
  For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
  More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit-vulnerabilities-101066782.html

OSC Installer

- OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later is required for deploying IGEL OS 11.06. and following.

AVD

- H.264 hardware decoding for MS-Teams optimization is currently limited to non- AMD devices due to stability issues on AMD devices.

VMware Horizon

- After disconnect of an RDP-based session, the Horizon main window which contains the server or sessions overview, cannot be resized anymore.
- Copying text from Horizon Blast sessions is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout from remote session.
- This happens only with enabled scanner or serial port redirection.
- The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol is not affected by this bug.
- The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- Keyboard Input Source Language Synchronization works only with usage of local layout and deadkeys enabled.
  If a keyboard layout is used which has deadkeys disabled (which is the default on IGEL OS), Horizon client falls back to en-US layout.
- PCoIP sessions may crash in some cases, switch to Blast Protocol is recommended then. H.264/HEVC encoding can be disabled when overall performance is too low.
- Client drive mapping and USB redirection for storage devices can be enabled at the same time, but this could lead to sporadic problems.

Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then.However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount. As a work-around, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- Attached storage devices appear as network drives in the remote session
- USB device redirection is considered as experimental for the Parallels client for Linux

Firefox

- With enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support. Means, when codec support is needed in Firefox, BCR needs to be disabled. Citrix Browser Content Redirection is disabled by default.
- Firefox restart option currently not supported.

Chromium

- Hardware accelerated video decoding is currently not supported.

Network

- Wakeup from system suspend fails on DELL Latitude 5510

WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disabling system suspend at IGEL Setup > System > Power Options > Shutdown.

Cisco JVDI Client

- There may be a segfault shown in the logs (during logout of Citrix Desktop session). Occurs only when using Citrix Workspace App 2010 and Cisco JVDI.

Base system

- Update from memory stick requires network online state (at least when multiple update stages are triggered / necessary)
- It is not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary. The recommended upgrade version for unattended migration is base system 12.2.1.

- Due to suspend/resume issues of a Innodisk NVME we disabled the suspend support for systems where this NVME is present. The issue otherwise will lead to a complete loose of the storage device as the NVME will not work after resume.

Conky

- The right screen when using multiscreen environment may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On devices with 4 GB flash storage or smaller it could happen that there is not enough space for updating all features. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error- not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or- higher-32870765.html for a possible solution and additional information.

Appliance Mode

- When ending a Citrix session in browser appliance mode, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- Browser Appliance mode can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch

Audio

- IGEL UD2 (D220) fails to restore the volume level of the speaker when the device used firmware version 11.01.110 before.
- Audio jack detection on Advantec POC-W243L does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- UD3-M340C: Sound preferences are showing Headphone & Microphone, although not connected.

Multimedia

- Multimedia redirection with GStreamer could fail when using Nouveau GPU driver.

Hardware

- Some newer Delock 62599 active DisplayPort to DVI (4k) adapters only work on INTEL-based devices.
- Wake up from suspend via UMS does not work on HP mt645 devices. Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is not supported on HP mt440 and mt645.
- MAC-Address Passthrough not supported on Lenovo USB-C Hybrid Docking Station.
- Wake-on-Lan via docking stations is not supported.
- In some rare cases it is possible that connecting or booting Lenovo USB-C Hybrid Docking station over USB-C results in non working / faulty display output.
  It may help to (re-)connect via USB-A. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to HP G5 Docking Station may fail with HP t655.

Remote Management

- AIT feature with IGEL Starter License is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.09.150

Firefox

- Updated Mozilla Firefox browser to version 115.4.0 ESR.
  Fixes for mfsa2023-46, also known as:
  CVE-2023-5721, CVE-2023-5732, CVE-2023-5724, CVE-2023-5725, CVE-2023-5728, CVE-2023-5730.

Chromium

- Fixed Chromium browser security issues
  CVE-2023-5996, CVE-2023-5859, CVE-2023-5858, CVE-2023-5857, CVE-2023-5856, CVE-2023-5855, CVE-2023-5854, CVE-2023-5853, CVE-2023-5852, CVE-2023-5851, CVE-2023-5850, CVE-2023-5849, CVE-2023-5482, CVE-2023-5480, CVE-2023-6112 and CVE-2023-5997
- Updated Chromium browser to current version 119.0.6045.159.

Base system

- Fixed **open-vm-tools** security issues
  CVE-2023-34059, CVE-2023-34058, CVE-2023-20900 and CVE-2023-20867.
- Fixed **vim security** issues
  More...

  CVE-2023-5535, CVE-2023-5441, CVE-2023-5344, CVE-2023-4781, CVE-2023-4752, CVE-2023-4751, CVE-2023-4750, CVE-2023-4735, CVE-2023-4734, CVE-2023-4733, CVE-2022-4293, CVE-2022-4292, CVE-2022-3705, CVE-2022-3591, CVE-2022-3520, CVE-2022-3491, CVE-2022-3352, CVE-2022-3324, CVE-2022-3297, CVE-2022-3278, CVE-2022-3256, CVE-2022-3235, CVE-2022-3234, CVE-2022-3153, CVE-2022-3134, CVE-2022-3099, CVE-2022-3037, CVE-2022-3016, CVE-2022-2982, CVE-2022-2889, CVE-2022-2874, CVE-2022-2862, CVE-2022-2819, CVE-2022-2817, CVE-2022-2816, CVE-2022-2598, CVE-2022-2580 and CVE-2022-2522.
- Fixed **krb5** security issue CVE-2023-36054.
- Fixed **gawk** security issue CVE-2023-4156.
- Fixed **bind9** security issues
  CVE-2023-4236, CVE-2023-3341, CVE-2023-3341, CVE-2023-2911 and CVE-2023-2828.
- Fixed **flac** security issue CVE-2020-22219.
- Fixed **ghostscript** security issues CVE-2023-38559 and CVE-2023-43115.
- Fixed **file** security issue CVE-2022-48554.
- Fixed **postgresql-14** security issue CVE-2023-39417.
- Fixed **libtommath** security issue CVE-2023-36328.
- Fixed **mysql-8.0** security issues
  More...

  CVE-2023-22114, CVE-2023-22112, CVE-2023-22103, CVE-2023-22097, CVE-2023-22092, CVE-2023-22084, CVE-2023-22079, CVE-2023-22078, CVE-2023-22070, CVE-2023-22068, CVE-2023-22066, CVE-2023-22064, CVE-2023-22059, CVE-2023-22032, CVE-2023-22058, CVE-2023-22057, CVE-2023-22056, CVE-2023-22054,

CVE-2023-22053, CVE-2023-22048, CVE-2023-22046, CVE-2023-22038, CVE-2023-22033, CVE-2023-22008 and CVE-2023-22005.

- Fixed **procps** security issue CVE-2023-4016.
- Fixed **cairo** security issue CVE-2019-6462.
- Fixed **cups** security issues CVE-2023-4504 and CVE-2023-32360.
- Fixed **curl** security issues CVE-2023-38546, CVE-2023-38545 and CVE-2023-38039.
- Fixed **qemu** security issues CVE-2023-42467, CVE-2023-4135, CVE-2023-40360, CVE-2023-3019, CVE-2021-3750 and CVE-2021-20255.
- Fixed **webkit2gtk** security issues CVE-2023-41993, CVE-2023-41074, CVE-2023-40451, CVE-2023-39928, CVE-2023-39434 and CVE-2023-35074.
- Fixed **samba** security issues CVE-2023-42669, CVE-2023-4154 and CVE-2023-4091.
- Fixed **tiff** security issue CVE-2023-1916.
- Fixed **aom** security issue CVE-2023-39616.
- Fixed **zulu8-ca** security issues CVE-2023-22081 and CVE-2023-22025.
- Updated **Chromium to version 118.0.5993.117** which fixes following security issues

  More...

  CVE-2023-5472, CVE-2023-5487, CVE-2023-5486, CVE-2023-5485, CVE-2023-5484, CVE-2023-5483, CVE-2023-5481, CVE-2023-5479, CVE-2023-5478, CVE-2023-5477, CVE-2023-5476, CVE-2023-5475, CVE-2023-5474, CVE-2023-5473, CVE-2023-5346, CVE-2023-5218, CVE-2023-5217, CVE-2023-5187, CVE-2023-5186, CVE-2023-4909, CVE-2023-4908, CVE-2023-4907, CVE-2023-4906, CVE-2023-4905, CVE-2023-4904, CVE-2023-4903, CVE-2023-4902, CVE-2023-4901, CVE-2023-4900, CVE-2023-4764, CVE-2023-4763, CVE-2023-4762, CVE-2023-4761, CVE-2023-4572, CVE-2023-4431, CVE-2023-4430, CVE-2023-4429, CVE-2023-4428, CVE-2023-4427, CVE-2023-4368, CVE-2023-4367, CVE-2023-4366, CVE-2023-4365, CVE-2023-4364, CVE-2023-4363, CVE-2023-4362, CVE-2023-4361, CVE-2023-4360, CVE-2023-4359, CVE-2023-4358, CVE-2023-4357, CVE-2023-4356, CVE-2023-4355, CVE-2023-4354, CVE-2023-4353, CVE-2023-4352, CVE-2023-4351, CVE-2023-4350, CVE-2023-4349 and CVE-2023-2312.

- Fixed **openssl** security issues CVE-2023-5363, CVE-2023-3817, CVE-2023-3446 and CVE-2023-2975.
- Fixed **opensc** security issues CVE-2023-4535, CVE-2023-40661 and CVE-2023-40660.
- Fixed **python-urllib3** security issues CVE-2023-45803 and CVE-2023-43804.
- Fixed **openvpn** security issues CVE-2023-46850 and CVE-2023-46849.
- Fixed **ffmpeg** security issue CVE-2022-4907.
- Fixed **libvpx** security issue CVE-2023-44488.
- Updated **Intel-microcode to version 20231114** to fix security issue CVE-2023-23583.

X server

- Fixed **X.Org-server** security issues CVE-2023-5574, CVE-2023-5380 and CVE-2023-5367.

New Features 11.09.150

Citrix

- Integrated **Citrix Workspace app 2309**
  Available workspace apps in this release: 23.09 (default), 23.07, and 20.10
  New Features:
- Enhancement to multiple monitors [Technical Preview]
  More...

Parameter	`Multi Monitor enhancement`
Registry	`ica.wfclient.wfclient.MultiMonitorPnPEnabled`
Value	true / false (default)

- Support for 32-bit cursor
- Copy and paste files and folders between two virtual desktops
- Improved error messages
- Updated Citrix Workspace App to version 2308.
  Available Citrix Workspace Apps in this release: 2308 (default), 2307 and 2010
- New features:
- HDX Adaptive Transport over EDT

Parameter	`HDX Adaptive Transport over EDT`
Registry	`ica.allregions.hdxoverudp`
Value	<>(default), true, and false

- Note: Update "ica.wfclient.proxytype" = Secure, and "ica.wfclient.proxyhost" in the following format = <IP>:<PORT>. For example "192.168.101.37:6153".
- Enable Packet Loss Concealment to improve audio performance

Parameter	`Enable Packet Loss Concealment to improve audio performance`
Registry	`ica.module.PacketLossConcealmentEnabled`
Value	false (default)/ true

- Policy tampering detection feature prevents the user from accessing the Virtual App or Desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered with. If policy tampering is detected.
- Updated Citrix Workspace App to version 2309.
  Available Citrix Workspace Apps in this release: 2309 (default), 2307 and 2010

- Enhancement to multiple monitors [Technical Preview]

Parameter	`Multi Monitor enhancement`
Registry	`ica.wfclient.MultiMonitorPnPEnabled`
Value	true / false (default)

- HTTPS protocol support for proxy server

Parameter	`HTTPS protocol support for proxy server`
Registry	`ica.allregions.hdxoverudp`
Value	true (default)/ false

- Note: Update `ica.allregions.proxytype` = Secure, and `ica.allregions.proxyhost` in the following format = <IP>:<PORT>. For example " `192.168.101.37:6153` ".
- Policy tampering detection feature prevents the user from accessing the Virtual App or Desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered with. If policy tampering is detected.
- Support for 32-bit cursor
- Copy and paste files and folders between two virtual desktops
- Improved error messages
- Updated Citrix EPA client to version 23.10.3.
- Updated Citrix Secure Access client to version 23.10.3.
- Updated Citrix Workspace App to version 2308.
  Available Citrix Workspace Apps in this release: 2308 (default), 2307 and 2010
- New features:
- HDX Adaptive Transport over EDT

Parameter	`HDX Adaptive Transport over EDT`
Registry	`ica.allregions.hdxoverudp`
Value	<>(default), true, and false

- Note: Update `ica.wfclient.proxytype` = Secure, and `ica.wfclient.proxyhost` in the following format = <IP>:<PORT>. For example `192.168.101.37:6153` .
- Enable Packet Loss Concealment to improve audio performance

Parameter	`Enable Packet Loss Concealment to improve audio performance`
Registry	`ica.module.PacketLossConcealmentEnabled`

Value	false (default)/ true

- Policy tampering detection feature prevents the user from accessing the Virtual App or Desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered with. If policy tampering is detected.

OSC Installer

- Added support for custom Unit ID rules. This offers possibility to choose appropriate MAC address of an internal network interface as Unit ID. Please visit the IGEL Knowledge Base for further details / how-to use this feature.

AVD

- Updated IGEL AVD client to version 1.1.35.

Remote Desktop (RDP3)

- Added new Remote Desktop client (RDP3) based on Microsoft's RdClientSDK. RDP3 sessions have basically the same options like AVD sessions except for their connection details and their separate gateway settings.

Teradici PCoIP Client

- Updated HP Anyware PCoIP Client to version 23.08.

WiFi

- Added support for RTL8852CE WiFi chipset - validated on HP Pro t550 Thin Client.

IGEL Agent for Imprivata

- Added: In FUS and Follow Policies mode, only Citrix sessions being started by the IGEL Agent for Imprivata will be disconnected / signed out, others remain intact.
- Added: the resource chooser is now part of the lock screen (if lock screen is enabled).
- Changed chooser from a grid view to list view
- Added registry key for hiding Horizon apps on chooser (and thus show desktops only)

Registry	`iia.hide_horizon_apps_on_chooser`
Type	bool
Value	**enabled** (default) / disabled)

- Added reg key for hiding Citrix apps on chooser (and thus show desktops only)

Registry	`iia.hide_citrix_apps_on_chooser`

Type	bool
Value	**enabled** (default) / disabled

- Added the ability to run Horizon Apps
- Changed reg key 'iia.query_moniker' from bool to string to hold the moniker name to query for

Registry	`iia.query_moniker`
Type	string
Value	""

- Fixed: Program rfideas also in FUS mode
- Fixed: Password change

Cisco JVDI Client

- Updated Cisco JVDI to version 14.2.1.

Cisco Webex

- Updated Cisco Webex VDI plugin to version 43.10.0.27853.

Base system

- Added registry keys for changing Intel kernel graphic driver settings:
  More...

Parameter	`Change settings for Intel PSR (panel self refresh).`
Registry	`x.drivers.intel.psr`
Range	[Default][Disable][Enable][Use only up to PSR1][Use up to PSR2]
Value	**Default**

Parameter	`Allow PSR2 selective fetch.`
Registry	`x.drivers.intel.psr2_sel_fetch`
Range	[Default][Disable][Enable]
Value	**Default**

Parameter	`Enable GuC load for GuC submission and/or HuC load.`
Registry	`x.drivers.intel.guc`

Range	[Default][Disable][GuC submission][HuC load]
Value	**Default**

Parameter	`Disable display power wells when possible.`
Registry	`x.drivers.intel.power_well`
Range	[Default][Auto][always on][disable when possible]
Value	**Default**

- Added further options for Intel kernel graphic driver - via registry keys:
  More...

Parameter	`Power saving display C-States to use.`
Registry	`x.drivers.intel.dc_setting`
Range	[Default][Disable][Up to DC5][Up to DC6][Up to DC5 with DC3C0][Up to DC6 with DC3C0]
Value	**Default**

Parameter	`Use framebuffer compression.`
Registry	`x.drivers.intel.fbc_setting`
Range	[Default][Disable][Enable]
Value	**Default**

- Enabled DEBUG_INFO_BTF in the kernel.
- Added further registry keys for influencing power consumption:
  More...

Parameter	`Use powertop auto tune to reduce power usage`
Registry	`system.powersave.powertop_auto_tune`
Range	[Auto][Enable][Disable]
Value	**Disable**

Parameter	`Use laptop mode to reduce power usage`
Registry	`system.powersave.laptop_mode`
Range	[Auto][Enable][Disable]

Value	**Disable**
Parameter	`Clock down AMDGPU if system is idle (idle action time reached).`
Registry	`system.powersave.clock_down_amdgpu_on_idle`
Type	bool
Value	enabled / **disabled** (default)
Parameter	`Set Ryzen CPU to power save mode if system is idle (idle action time reached).`
Registry	`system.powersave.use_ryzenadj_on_idle`
Type	bool
Value	enabled / **disabled** (default)
Parameter	`Call idle actions on AC after this time of inactivity (greater 10 seconds, value 9 or lower is never)`
Registry	`system.powersave.idle_action_on_ac`
Type	integer
Value	9 **Default**
Parameter	`Call idle actions on battery after this time of inactivity (greater 10 seconds, value 9 or lower is never)`
Registry	`system.powersave.idle_action_on_battery`
Type	integer
Value	9 **Default**

- Integrated required versions for private build:
  - Webex Teams Plugin: 43.6.0.26643
  - Webex Meetings Plugins: 43.6.5.20, 2.10.8.14 and 42.6.11.6
  - Citrix Workspace Apps: 23.05.0.58, 23.09.02.24 and 20.10.0.6
  - Zoom Plugins: 5.12.6.22200, 5.13.10.23090, 5.14.10.23670

- Kernel with activated CONFIG_DEBUG_INFO_BTF option.

Driver

- Updated Nuance Citrix Client Audio Extension for dictation to version B308. This fixes several security issues and adds support for Nuance PowerMic 4.
- Updated dpmuxd of HID Global fingerprint reader driver to version 1114. This fixes sharing the reader in applications (rather than desktops) via Citrix.

Custom Partition

- Enabled DEBUG_INFO_BTF in the kernel.

X11 system

- Added new registry key quirk to fix screen stays black after reconfiguration issue on NVIDIA graphic cards.

Parameter	`Quirk to fix NVIDIA issues with screen stays black after reconfiguration.`
Registry	`x.xserver%.quirks.nvidia_screen_stay_black`
Type	bool
Value	enabled / **disabled** (default)

VNC Viewer

- Updated TigerVNC Viewer to version 1.13.1. This adds support for new RSA-AES connection security types. The list of connection security types to use is configurable now.
  More...

Setup	Sessions>VNC Viewer>VNC Viewer Sessions>Name>Connection
Parameter	`Security types`
Registry	`sessions.vncviewer<INST>.option.securitytype`
Value	{**}empty{**}{}
Setup	Sessions>VNC Viewer>VNC Viewer Sessions>Name>Connection
Parameter	`Pathname for CA certificates file`
Registry	`sessions.vncviewer<INST>.option.x509capath`

Value	{}**/etc/ssl/certs/ca-certificates.crt**{}
Setup	Sessions>VNC Viewer>VNC Viewer Sessions>Name>Connection
Parameter	`Pathname for certificate revocation list file`
Registry	`sessions.vncviewer<INST>.option.x509crlpath`
Value	{}**empty**{}

Audio

- Updated EPOS Connect to version 7.7.

Evidian

- Updated rsUserAuth to version 1.5.8705
- Support of RFIDeas reader on Authentication Manager for Linux
- RFIDeas PC/SC Mixed-Mode.
  Set " `RFIDMixMode=on` " in `rsUserAuth.ini` configuration file and handle RFIDeas badges as PC/SC one.
- Read-only protection on the domain field.
  Set " `GreyOutDomainField=on` " in `rsUserAuth.ini` configuration file to set Domain field uneditable.

Hardware

- Validated 256GB 2230 PCIe NVMe module for HP t550 and t655.
- Validated 256GB 2280 PCIe NVMe module for HP t550 and t655.
- Validated 512GB 2280 PCIe NVMe module for HP t550 and t655.
- Validated Fujitsu Futro S7011.
- Validated Fujitsu Lifebook E5412.
- Added hardware support for LG 24CR670I-6N.
- Added AMI BIOS tools support for HP t430, t550, t655 and t740. HP is responsible for the validation and approval of the BIOS update and BIOS settings change features.

Resolved Issues 11.09.150

Citrix

- Fixed MS Teams for Citrix Workspace App 2307 and higher
- Added registry key ica.chrome-double-download to control flock feature at wfica_wrapper. 'Enable flock' blocks double app starts (due to double downloads by Chromium browser).

Parameter	`Control download mechanic for Citrix applications for Chrome web access`
Registry	`ica.chrome-double-download`
Range	[Enable Lock][Disable Lock]
Value	enable / **disable** (default)

RDP/IGEL RDP Client 2

- Fixed RDWeb Access using gateway when direct connection is possible.
- Fixed RDP session crash after pressing CTRL + ALT + ENTER.

AVD

- Fixed Pause key to work as expected.
- Fixed: Calculator key on keyboards opens the calculator app in the AVD session.

VMware Horizon

- Added possibility to customize waiting time after unplugging a device from a usb port before re-plug - to ensure automatic redirection to remote desktop.

Parameter	`Customize delay time needed between unplug and replug of usb devices`
Registry	`vmware.view.usb-reconnect-delay`
Type	bool
Value	enabled / **disabled** (default)

Parameter	`Minimum time (in ms) you have to wait between unplug and replug of redirected usb devices`
Registry	`vmware.view.usb-reconnect-time`
Type	int
Value	6000 **Default**

- Added possibility to enable automatic connection for redirected usb devices which are excluded from this mechanism like HID bootable devices by also setting the Device Quirk option in the devices allow rule.

Parameter	`Device Quirk`
Registry	`vmware.view.usb.devicepolicy.product_rule%.devicequirk`
Type	bool
Value	enabled / **disabled** (default)

Network

- Fixed mobile broadband support on Lenovo L14/L15 Gen3 AMD with Quectel EM05.
- Fixed tcpdump debug logging functionality.

WiFi

- Fixed Mediatek WiFi not working after Suspend / Resume.

HID

- Fixed handling of ELO touch devices in multi-monitor configuration.
- Fixed touchscreen configuration for devices using standard mouse interface.

CUPS Printing

- Fixed CUPS printer model name used in IGEL OS.

ThinPrint

- Added definition of printer device **/dev/usblp** which is used for Thinprint printers.
  The need for such a device is due to the fact that a usb printer in some cases does not always get named **/dev/usblp0** - even if it's the only one.
  Note: With more than one usb printer connected at the same time, /dev/usblp should not be used

but rather a device specific name based on usb ids, the usb port, or a usb class based device selection.

Base system

- Fixed x.drivers.kms.debug_level configuration.
- Fixed user permission configuration of editor mousepad.

Custom Partition

- Fixed errors during removal of custom partitions.

X11 system

- Fixed issues with 4K monitors on Lenovo m75n IoT.

IgelDesktop

- Fixed hiding mouse cursor.

Audio

- Fixed Sound Mixer default setting.

Evidian

- Fixed: Domain pre-assignment for rollout RFID with PIN
- Fixed: UseUPN problems with Citrix logon
- Fixed: Welcome screen not properly displayed with different DPI Settings. Homogenization of the entire interface.

Multimedia

- Fixed virtual webcam - choosing webcam by device name.
- Added 640x360 as 16:9 resolution to possible webcam resolutions registry key:

Parameter	`Select resolution to use.`
Registry	`multimedia.webcam.virtual_background.resolution`
Range	[webcam default][webcam max][1920x1080][1280x720][640x480][640x360][480x360][424x240][320x240][320x180]
Value	**webcam default**

Java

- Fixed java runtime environment integration (certificate store)

Notes for Release 11.09.110

Software:	Version	11.09.110
Release Date:	2023-10-24	
Release Note:	Version	RN-1109110-1
Last update:	2023-10-24	

- Supported Devices 11.09.110 (see page 2592)
- Component Versions 11.09.110 (see page 2593)
- Known Issues 11.09.110 (see page 2601)
- Security Fixes 11.09.110 (see page 2606)
- New Features 11.09.110 (see page 2607)
- Resolved Issues 11.09.110 (see page 2608)

The Release Notes of IGEL OS 11.09.100 are also available in the following formats:

Supported Devices 11.09.110

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX	UD6-LX 51
UD7-LX	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also, Devices Supported by IGEL OS 11 (see page 2592).

Component Versions 11.09.110

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	118.0.5993.70-1igel1697046811
Cisco JVDI Client	14.1.4
Cisco Webex VDI plugin	43.6.0.26643
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.0.158
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.10.23670
Zoom Media Plugin	5.15.2.23760
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.05.0.58
Citrix Workspace App	23.07.0.17
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.4.0.37727
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	42.3-0ubuntu3

FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.3.1
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1687350866
IGEL AVD Client	1.1.30igel1695044534
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.3-2igel1684821787
Zulu JRE	17.0.8-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Parole Media Player	4.16.0-3igel1686304269
VNC Viewer	1.12.0+dfsg-8igel1675065715

VMware Horizon Client	2306-8.10.0-21964631
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-0.3igel1686055473
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.19
OpenSSL	3.0.2-0ubuntu1.10
OpenSSH Client	9.3p2-1igel1690097953
OpenSSH Server	9.3p2-1igel1690097953
Bluetooth stack (bluez)	5.66-1igel1669186181
MESA OpenGL stack	23.1.2-1igel1686636111
VDPAU Library version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726

Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1696246906
Xorg X11 Server	21.1.7-3igel1683808186
Xorg Xephyr	21.1.7-3igel1683808186
CUPS printing Daemon	2.4.2-5igel1687852452
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.4-1igel1690179327
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.42.1-2+b1igel1696854696
Python2	2.7.18
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222

Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222
Open VM Tools	12.1.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.1.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.0.4+dfsg-1igel1691991170

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.0 M	Included
Java SE Runtime Environment	54.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	710.5 M	Included
Ericom PowerTerm InterConnect	10.0 M	Included
Media Player	256.0 K	Included
Local Browser (Firefox) Citrix Appliance	86.8 M	Included
VMware Horizon RDP	4.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	19.0 M	Included

NoMachine NX	27.0 M	Included
VMware Horizon	176.8 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	11.8 M	Not included
Fluendo GStreamer Codec Plugins	3.2 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	378.2 M	Not included
Imprivata Appliance	32.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	768.0 K	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	63.2 M	Included
PrinterLogic	38.0 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	36.0 M	Not included
AVD	41.8 M	Included
Local Browser (Chromium)	98.2 M	Not included
Amazon WorkSpaces Client	32.5 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	104.5 M	Not included
Cisco Webex Meetings VDI	193.8 M	Not included

Zoom Media Plugin	161.8 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	768.0 K	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	10.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	18.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	9.2 M	Not included
VirtualBox (Limited support)	74.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8 M	Included

Known Issues 11.09.110

Citrix

- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:
  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active session does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- **Browser Content Redirection (BCR)** does not work if **DRI3 and hardware accelerated H.264 deep compression codec is enabled**.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy **"Use video codec compression" -> "For the entire screen".**
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- While starting Self-Service, it is possible that process **ServiceRecord segfaults -> Self-Service cannot be started afterwards**.
  A **cache cleanup with reboot** is needed. In addition, the **following parameters should set to true**.

  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- **Browser Content Redirection** (BCR) may not work with **Chrome** version **105.0.*** or later.
  See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher
- **White / green fragments** may appear during desktop launch if **JPEG graphical codec** is used.
- **MS Teams calls may stop if blurred background is enabled**. This affects **Citrix Workspace App 2305 and later**.
- Regarding **CVE-2023-41993, CVE-2023-39928 & CVE-2023-41074:**
  For compatibility with Citrix Self-Service, older Webkit libraries are used instead of the latest ones to continue working properly.
  More information: https://wiki.test.toolchain.igel.kreuzwerker.net/securitysafety/en/isn-2023-25-webkit-vulnerabilities-101066782.html

OSC installer

- **OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later** is **required** for deploying **IGEL OS 11.06. and following**.

AVD

- **H.264 hardware decoding for MS-Teams optimization is currently limited to non-AMD devices due to stability issues on AMD devices.**

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying text from Horizon Blast sessions** is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry: `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from a remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**. If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.

- **PCoIP sessions may crash** in some cases, **switch to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance is too low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadic problems. Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session
- **USB device redirection** is considered as **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection**, **Firefox has no H.264 and AAC multimedia codec support**. Means, **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend fails on **DELL Latitude 5510.**

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** does not work after system suspend/resume.
  Workaround: Disabling system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during logout of Citrix Desktop session). Occurs only when using **Citrix Workspace App 2010** and **Cisco JVDI**.

Base System

- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).
- It is **not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary**. The recommended upgrade version for **unattended migration is base system 12.2.1**.

Conky

- The **right screen when using multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware Update

- On **devices with 4 GB of flash** or smaller, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.htm[261] for a possible solution and additional information.

ppliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch

Audio

- **IGEL UD2 (D220**) **fails to restore the volume level** of the speaker when the device used **firmware version 11.01.110** before.

- **Audio jack detection on Advantec POC-W243L does not work**. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3-M340C:** Sound preferences are **showing Headphone & Microphone, although not connected**.

Multimedia

- Multimedia redirection with **GStreamer could fail when using Nouveau GPU driver**.

261. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k) adapters** only work on INTEL-based devices.
- **Wake up from suspend via UMS** does not work on **HP mt645 devices**.
  Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is **not supported on HP mt440 and mt645**.
- **MAC-Address Passthrough** not supported on **Lenovo USB-C Hybrid Docking Station**.
- **Wake-on-Lan via docking stations** is not supported.
- In some rare cases, it is possible that connecting or booting **Lenovo USB-C Hybrid Docking station over USB-C results in non-working / faulty display output**.
  It may help to **(re-)connect via USB-A**. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to **HP G5 Docking Station may fail with HP t655**.

Remote Management

- AIT feature with IGEL Starter License is only supported by **UMS version 6.05.100 or newer**.

Security Fixes 11.09.110

Base System

- Fixed **curl security issues**
  CVE-2023-38546, CVE-2023-38545, and CVE-2023-38039.
- Updated **Firefox to ESR version 115.3.1**
  Fixes for mfsa2023-44, also known as:
  CVE-2023-5217
  Fixes for mfsa2023-42, also known as:
  CVE-2023-5169, CVE-2023-5171, CVE-2023-5176.
- Updated **Chromium to version 118.0.5993.70** which fixes following security issues
  More...

  CVE-2023-5487, CVE-2023-5486, CVE-2023-5485, CVE-2023-5484,
  CVE-2023-5483, CVE-2023-5481, CVE-2023-5479, CVE-2023-5478, CVE-2023-5477,
  CVE-2023-5476, CVE-2023-5475, CVE-2023-5474, CVE-2023-5473, CVE-2023-5346,
  CVE-2023-5218, CVE-2023-5217, CVE-2023-5187, CVE-2023-5186, CVE-2023-4909,
  CVE-2023-4908, CVE-2023-4907, CVE-2023-4906, CVE-2023-4905, CVE-2023-4904,
  CVE-2023-4903, CVE-2023-4902, CVE-2023-4901, CVE-2023-4900, CVE-2023-4764,
  CVE-2023-4763, CVE-2023-4762, CVE-2023-4761, CVE-2023-4572, CVE-2023-4431,
  CVE-2023-4430, CVE-2023-4429, CVE-2023-4428, CVE-2023-4427, CVE-2023-4368,
  CVE-2023-4367, CVE-2023-4366, CVE-2023-4365, CVE-2023-4364, CVE-2023-4363,
  CVE-2023-4362, CVE-2023-4361, CVE-2023-4360, CVE-2023-4359, CVE-2023-4358,
  CVE-2023-4357, CVE-2023-4356, CVE-2023-4355, CVE-2023-4354, CVE-2023-4353,
  CVE-2023-4352, CVE-2023-4351, CVE-2023-4350, CVE-2023-4349 and CVE-2023-2312.

- Fixed **webkit2gtk** security issues
  CVE-2023-41993, CVE-2023-41074, CVE-2023-40451, CVE-2023-39928, CVE-2023-39434 and CVE-2023-35074.

New Features 11.09.110

Chromium

- Updated **Chromium to version 118.0.5993.70**

Firefox

- Updated **Firefox to ESR version 115.3.1**

Base System

- Added **new registry keys** to improve **power usage of the system** (not enabled as default)

Parameter	Use powertop auto tune to reduce power usage
Registry	`system.powersave.powertop_auto_tune`
Range	[Auto][Enable][Disable]
Value	**Disable**
Parameter	Use laptop mode to reduce power usage
Registry	`system.powersave.laptop_mode`
Range	[Auto][Enable][Disable]
Value	**Disable**
Parameter	Clock down AMDGPU if screen dims down (due to inactivity)
Registry	`system.powersave.clock_down_amdgpu_on_dim`
Type	bool
Value	disabled / enabled
Parameter	Set Ryzen CPU to power save mode if screen dims down (due to inactivity)
Registry	`system.powersave.use_ryzenadj_on_dim`
Type	bool
Value	disabled / enabled

Resolved Issues 11.09.110

Cisco Webex

- Fixed **Webex VDI/ Webex Meetings VDI** not connecting to the enterprise site.

Notes for Release 11.09.100

Software:	Version	11.09.100
Release Date:	2023-10-12	
Release Note:	Version	RN-1109100-1
Last update:	2023-10-12	

- Supported Devices 11.09.100 (see page 2610)
- Component Versions 11.09.100 (see page 2611)
- Known Issues 11.09.100 (see page 2619)
- Security Fixes 11.09.100 (see page 2624)
- New Features 11.09.100 (see page 2626)
- Resolved Issues 11.09.100 (see page 2633)

The Release Notes of IGEL OS 11.09.100 are also available in the following formats:

- Plain text:

Supported Devices 11.09.100

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX	UD6-LX 51
UD7-LX	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Devices Supported by IGEL OS 11 (see page 2610).

Component Versions 11.09.100

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	115.0.5790.170-2igel1695992905
Cisco JVDI Client	14.1.a
Cisco Webex VDI plugin	43.6.0.26643
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.0.158
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.10.23670
Zoom Media Plugin	5.15.2.23760
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.05.0.58
Citrix Workspace App	23.07.0.17
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.12.2-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.4.0.37727
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	42.3-0ubuntu3

FabulaTech Plugins	3.10.1.5
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	115.2.1
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1687350866
IGEL AVD Client	1.1.30igel1695044534
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.12.0.688624_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	6.00_rev29368
NX Client	7.8.2-4igel1685535669
OpenVPN	2.6.3-2igel1684821787
Zulu JRE	17.0.8-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.42-2igel1684932691
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.13.0-2igel1677968775
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-3igel1686304269

VNC Viewer	1.12.0+dfsg-8igel1675065715
VMware Horizon Client	2306-8.10.0-21964631
Voip Client Ekiga	4.0.1-9build1igel1685429059

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-0.3igel1686055473
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.10-1igel1691506428
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.2-1igel1678006273
Reader Driver REINER SCT cyberJack	3.99.5final.sp14-2igel1686635168
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13igel1686114423
OpenSSL	1.1.1f-1ubuntu2.19
OpenSSL	3.0.2-0ubuntu1.10
OpenSSH Client	9.3p2-1igel1690097953
OpenSSH Server	9.3p2-1igel1690097953
Bluetooth stack (bluez)	5.66-1igel1669186181
MESA OpenGL stack	23.1.2-1igel1686636111
VDPAU Library version	1.5-2igel1677954724
Graphics Driver INTEL	2.99.917+git20210115-1igel1654609037
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	23.0.0-1igel1677481842
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1654608979
Graphics Driver Nvidia	525.125.06-0ubuntu0.22.04.1
Graphics Driver VMware	13.3.0-3igel1654607153
Graphics Driver QXL (Spice)	0.1.6-1igel1687782644
Graphics Driver FBDEV	0.5.0-2igel1654609009
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Elographics	1.4.3-1igel1678083379
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.2-1+b1igel1683803726
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891

Input Driver Wacom	1.2.0-1igel1686600941
Input Driver ELO Multitouch	4.3.0.0
Input Driver ELO Singletouch	5.2
Kernel	6.1.42 #mainline-lxos-g1696246906
Xorg X11 Server	21.1.7-3igel1683808186
Xorg Xephyr	21.1.7-3igel1683808186
CUPS printing Daemon	2.4.2-5igel1687852452
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.30.0-0ubuntu5igel1685475374
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.4.1-2.3ubuntu2.4
NetworkManager	1.42.4-1igel1692869696
ModemManager	1.20.6-2igel1693224023
GStreamer 1.x	1.22.4-1igel1690179327
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.40.5-1igel1691399103
Python2	2.7.18
Python3	3.10.12

VM Guest Support Components

Virtualbox Guest Utils	7.0.8-dfsg-2igel1682408222
Virtualbox X11 Guest Utils	7.0.8-dfsg-2igel1682408222

Open VM Tools	12.1.5-3~ubuntu0.22.04.1
Open VM Desktop Tools	12.1.5-3~ubuntu0.22.04.1
Xen Guest Utilities	7.20.2-0ubuntu1~22.04.2
Spice Vdagent	0.22.1-3+b2igel1680584586
Qemu Guest Agent	8.0.4+dfsg-1igel1691991170

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.21-1igel1690183811
Mobile Device Access USB (imobile)	1.3.0-6+b3igel1677964762
Mobile Device Access USB (gphoto)	2.5.30-1igel1677966247
VPN OpenConnect	9.12-1igel1687783022
Scanner support	1.1.1-5
VirtualBox VM within IGEL OS	7.0.8-dfsg-2igel1682408222
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.0 M	Included
Java SE Runtime Environment	54.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	678.2 M	Included
Ericom PowerTerm InterConnect	10.0 M	Included
Media Player	256.0 K	Included
Local Browser (Firefox) Citrix Appliance	86.8 M	Included
VMware Horizon RDP	4.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	19.0 M	Included
NoMachine NX	27.0 M	Included

VMware Horizon	176.8 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	11.8 M	Not included
Fluendo GStreamer Codec Plugins	3.2 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	378.2 M	Not included
Imprivata Appliance	32.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	768.0 K	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	63.2 M	Included
PrinterLogic	38.0 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	36.0 M	Not included
AVD	41.8 M	Included
Local Browser (Chromium)	95.0 M	Not included
Amazon WorkSpaces Client	32.5 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	104.5 M	Not included
Cisco Webex Meetings VDI	193.8 M	Not included
Zoom Media Plugin	161.8 M	Not included

DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	768.0 K	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	10.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	18.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	9.2 M	Not included
VirtualBox (Limited support)	74.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	47.8 M	Included

Known Issues 11.09.100

Citrix

- To launch multiple desktop sessions with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:
  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Range	enabled / **disabled** (default)

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active session does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- **Browser Content Redirection (BCR)** does not work if **DRI3 and hardware accelerated H.264 deep compression codec is enabled**.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy **"Use video codec compression" -> "For the entire screen".**
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- While starting Self-Service, it is possible that process **ServiceRecord segfaults -> Self-Service cannot be started afterwards**.
  A **cache cleanup with reboot** is needed. In addition, the **following parameters should set to true**.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
Registry	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`
Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- **Browser Content Redirection** (BCR) may not work with **Chrome** version **105.0.*** or later. See https://support.citrix.com/article/CTX473065/hdx-browser-content-redirection-broken-with-google-chrome-browser-version-105-or-higher
- **White / green fragments** may appear during desktop launch if **JPEG graphical codec** is used.

OSC installer

- **OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **H.264 hardware decoding for MS-Teams optimization is currently limited to non-AMD devices due to stability issues on AMD devices.**

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying text from Horizon Blast sessions** is not possible.
- The on-screen keyboard in Horizon appliance mode does not work correctly with local logon. It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from a remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**. If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switch to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance is too low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadic problems. Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session
- **USB device redirection** is considered as **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection**, **Firefox has no H.264 and AAC multimedia codec support**. Means, **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend fails on **DELL Latitude 5510.**

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** does not work after system suspend/resume.
  Workaround: Disabling system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during logout of Citrix Desktop session). Occurs only when using **Citrix Workspace App 2010** and **Cisco JVDI**.

Base System

- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).
- It is **not possible to perform an unattended OS12 migration to base system 12.2.0 as an additional / manual reboot is necessary**. The recommended upgrade version for **unattended migration is base system 12.2.1**.

Conky

- The **right screen when using multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware Update

- On **devices with 4 GB of flash** or smaller, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-space-on-local-drive-

when-updating-to-igel-os-11-04-or-higher-32870765.htm[262] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the Web URL contains special control characters like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch

Audio

- **IGEL UD2 (D220**) **fails to restore the volume level** of the speaker when the device used **firmware version 11.01.110** before.

- **Audio jack detection on Advantec POC-W243L does not work**. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3-M340C:** Sound preferences are **showing Headphone & Microphone, although not connected**.

Multimedia

- Multimedia redirection with **GStreamer could fail when using Nouveau GPU driver**.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k) adapters** only work on INTEL-based devices.
- **Wake up from suspend via UMS** does not work on **HP mt645 devices**.
  Workaround: Disable system suspend and use shutdown instead.
- Built-in fingerprint sensor is **not supported on HP mt440 and mt645**.
- **MAC-Address Passthrough** not supported on **Lenovo USB-C Hybrid Docking Station**.
- **Wake-on-Lan via docking stations** is not supported.
- In some rare cases, it is possible that connecting or booting **Lenovo USB-C Hybrid Docking station over USB-C results in non-working / faulty display output**.
  It may help to **(re-)connect via USB-A**. If this is the case, USB-C should be also functional then.
- Display configuration of displays connected to **HP G5 Docking Station may fail with HP t655**.

262. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Remote Management

- AIT feature with IGEL Starter License is only supported by **UMS version 6.05.100 or newer**.

Security Fixes 11.09.100

IBM_5250

- Updated **IBM iAccess Client** Solutions to **version 1.1.9.2**. Complete changelog via [https://www.ibm.com/support/pages/ibm-i-access-acs-updates]

Chromium

- Updated **Chromium browser** to **version 115.0.5790.170**.

Firefox

- Updated **Mozilla Firefox browser** to **version 115.2.1**.

Base System

- Fixed **nss** security issue CVE-2023-0767.
- Fixed **libxml2** security issues CVE-2023-29469, CVE-2023-28484, CVE-2022-40304 and CVE-2022-40303.
- Fixed **wavpack** security issue CVE-2021-44269.
- Fixed **tar** security issue CVE-2022-48303.
- Fixed **python3.6** security issue CVE-2022-37454.
- Fixed **tiff** security issues CVE-2023-0804, CVE-2023-0803, CVE-2023-0802, CVE-2023-0801, CVE-2023-0800, CVE-2023-0799, CVE-2023-0798, CVE-2023-0797, CVE-2023-0796 and CVE-2023-0795.
- Fixed **rsync** security issue CVE-2022-29154.
- Fixed **vim** security issues
  More...

  CVE-2022-2946, CVE-2022-2923, CVE-2022-2849, CVE-2022-2845, CVE-2022-2581, CVE-2022-2571, CVE-2022-2345, CVE-2022-2304, CVE-2022-2206, CVE-2022-2183, CVE-2022-2175, CVE-2022-2129, CVE-2022-2126, CVE-2022-2125, CVE-2022-2124, CVE-2022-1968, CVE-2022-1942, CVE-2022-1898, CVE-2022-1851, CVE-2022-1796, CVE-2022-1785, CVE-2022-1735, CVE-2022-1733, CVE-2022-1720, CVE-2022-1674, CVE-2022-1629, CVE-2022-0413, CVE-2023-1175, CVE-2023-1170, CVE-2023-0433, CVE-2023-0288, CVE-2023-0054, CVE-2023-0049 and CVE-2022-47024.
- Fixed **systemd** security issues CVE-2022-4415 and CVE-2022-3821.
- Fixed **curl** security issues CVE-2023-27538, CVE-2023-27537, CVE-2023-27536, CVE-2023-27535, CVE-2023-27534 and CVE-2023-27533.
- Fixed **xorg-server** security issue CVE-2023-1393.

- Fixed **protobuf** security issues
  CVE-2022-1941 and CVE-2021-22570.
- Fixed **python2.7** security issue CVE-2023-24329.
- Fixed **python3.6** security issue CVE-2023-24329.
- Fixed **libtpms** security issues CVE-2023-1018 and CVE-2023-1017.
- Fixed **chromium-browser** security issues
- Fixed **sudo** security issues CVE-2023-28487, CVE-2023-28486 and CVE-2023-2848.
- Fixed **vim** security issues
  More...

  CVE-2022-2207, CVE-2022-0729, CVE-2022-0714,
  CVE-2022-0685, CVE-2022-0572, CVE-2022-0554, CVE-2022-0443, CVE-2022-0408,
  CVE-2022-0368, CVE-2022-0361, CVE-2022-0359, CVE-2022-0351, CVE-2022-0319,
  CVE-2022-0318, CVE-2022-0261, CVE-2022-0213, CVE-2021-4193 and CVE-2021-4192.
- Fixed **heimdal** security issue CVE-2022-45142.
- Fixed **ghostscript** security issue CVE-2023-28879.
- Fixed **dnsmasq** security issue CVE-2023-28450.
- Fixed **zulu8-ca** security issues
  CVE-2023-21930, CVE-2023-21937, CVE-2023-21938,
  CVE-2023-21939, CVE-2023-21954, CVE-2023-21967 and CVE-2023-21968.
- Updated **Intel microcode** to version 20230808.
- Updated **AMD microcode** to version 20230809.
- Fixed **libwebp** security issue
  CVE-2023-4863 (initial only Chromium related) and CVE-2023-5129.
- Fixed **libvpx** security issue CVE-2023-5217.
- Fixed **libx11** security issues
  CVE-2023-43787, CVE-2023-43786 and CVE-2023-43785.
- Fixed **Chromium** security issue CVE-2023-5217.
- Fixed **libxpm** security issues
  CVE-2023-43789, CVE-2023-43788, CVE-2023-43787 and CVE-2023-43786.
- Fixed **glibc** security issue CVE-2023-4911.

New Features 11.09.100

Citrix

- Updated **Citrix Workspace App to version 2307**. Available Citrix Workspace Apps in this release: **2307 (default), 2305, and 2010.** Added support for playing short tones in optimized **Microsoft Teams - requires an update to the latest version of Microsoft Teams**.
- Changes with **Citrix Workspace App 2305 and 2307**:
  New features:
- Copy and paste files and folders between two virtual desktops [Technical Preview]

Parameter	Copy and paste files and folders between two virtual desktops
Registry	`ica.module.vdgdt`
Value	**true** (default)/ false

- Enhancement on 32-bit cursor support [Technical Preview]

Parameter	Enhancement on 32-bit cursor support
Registry	`ica.wfclient.Cursor32bitSupport`
Value	**true** (default)/ false

- Change the default browser for FIDO2

Parameter	Change the default browser for FIDO
Registry	`ica.authman.fido2authbrowser`
Value	CEB (default), chromium, firefox, chromium-browser

- Support for authentication using FIDO2 when connecting to on-premises stores [Technical Preview]

Parameter	Support for authentication using FIDO2 when connecting to on-premises stores
Registry	`ica.authman.fido2enabled`
Value	false (default)/ true

- Fixed:
  - App Protection works with all the Citrix session types, including Firefox browser. Reboot of system after enabling/disabling the feature (ica.appprotection) is required.

OSC Installer

- Added possibility to create a minimal (self extracting) factory image with the OSC installer.

AVD

- Updated IGEL AVD Client to version 1.1.30.

Chromium

- Added possibility to use compressed **BTRFS for Chromium profile partition**. This is **enabled by default**.
- Enhanced registry key **system.customization.chpro.fs_type** with new option **btrfs**.

Parameter	Chromium Profiles Partition Filesystem Type
Registry	`system.customization.chpro.fs_type`
Range	[ext4][f2fs][ntfs][ntfs-3g][btrfs]
Value	btrfs

- Added registry key to block the restore popup which is shown if Chromium browser is (re-)started after a crash.

Firefox

- Added possibility to use compressed BTRFS and ntfs-3g for firefox profile partition.
- Enhanced registry key system.customization.chpro.fs_type with new options btrfs and ntfs-3g.

Parameter	Firefox Profiles Partition Filesystem Type
Registry	`system.customization.ffpro.fs_type`
Range	[ext4][f2fs][ntfs][ntfs-3g][btrfs]
Value	ntfs

Network

- Added MAC-address passthrough among Ethernet devices. With the following registry key a LAN device can be specified from which the MAC address shall be adopted. The donor device and any conflicting receiver device will be removed (by unbinding the driver) as long as the receiving device is present.

Parameter	MAC address source
Registry	`network.interfaces.ethernet.device%.mac_source`
Range	[none][LAN][LAN2][LAN3][LAN4]
Value	none

- Example: If LAN2 and LAN3 are configurations for docking stations that shall adopt the MAC address from LAN, the following two parameters must be set to "LAN":
  `network.interfaces.ethernet.device1.mac_source`
  `network.interfaces.ethernet.device2.mac_source`
  Warning: Misconfiguration may result in loss of connectivity
- Added Lenovo FCC unlock tool for Quectel EM05

NCP VPN

- Updated NCP Enterprise client to version 6.0 r29368.

OpenConnect VPN

- Added further supported protocols for OpenConnect VPN client by adding Fortinet, F5 and Array. OpenConnect VPN is a feature with limited support, and the new protocols are not validated by IGEL.

Setup	Network>VPN>OpenConnect VPN>Name>Session
Parameter	Protocol
Registry	`sessions.openconnect<INST>.vpnopts.protocol`
Value	`{**}anyconnect{**}/nc/pulse/gp/f5/fortinet/array`

Imprivata

- Updated Imprivata bootstrap loader to version 7.12.0.688624
  This version can only be used with G4 Appliance and PIE Agents 7.12 or later!!

IGEL Agent Imprivata

- Added: Computer policy affects showing shutdown and reboot buttons at lock screen.
- Added: Query email from standard principal information. The following registry key will override it with an email provided by the App Moniker - if available.

Parameter	Query Email from App Moniker
Registry	`iia.query_moniker`
Range	bool
Value	enabled / disabled

- Added: Reporting IGEL OS version to Imprivata Appliance
- Added: Display user name on 2nd factor query
- Added: Minor UI improvements

HID

- Updated ELO touch driver to version 5.4 for single touch and 4.3 for multitouch.
- Added support for usage or more than one touch screen (without calibration for now).

CUPS Printing

- Updated **PrinterLogic PrinterInstallerClient to version 25.1.0.637**. The update fixes the determination of AD user if Kerberos login is used.

Cisco JVDI Client

- Integrated Cisco JVDI 14.1.4

Base System

- Updated **kernel to version 6.1.42**.
- Added support for **migrating IGEL OS11 to IGEL OS12.** Details can be found here: https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.09/en/upgrading-from-igel-os-11-to-igel-os-12-101063106.html. **UMS 12.02.120 or later** is required.
  Migration related parameters:

Registry	`system.upgrade_igelos.ignore_memory_requirement`
Value	false / true
Hint	Force upgrade of the IGEL OS if the device does not meet the minimal hardware requirement regarding RAM. Upgrade is performed on own risk and without official support by IGEL.
Registry	`system.upgrade_igelos.delete_custom_partition`
Value	false / true
Hint	Automatically delete the existing custom partition while upgrading to the IGEL OS12.

- Changed: If firmware is reset to factory defaults or reinstalled with OSC, the IGEL Setup Assistant starts again.
- Added some additional resolutions to the webcam virtual background solution (see changed registry keys).

- Enables to choose webcams for virtual background by device name and priority.
- Added new registry keys:
  More...

Parameter	Select webcam by devicename for example /dev/video0 or video0 (only valid if choose by devicename is used)
Registry	Select webcam by devicename for example `/dev/video0 or video0` (only valid if choose by devicename is used)
Type	string
Value	empty
Parameter	Select webcam by priority list for example dev=video0;name=HD_Webcam_C270 (only valid if choose by priority is used)
Registry	`multimedia.webcam.virtual_background.webcam_priority`
Type	string
Value	empty

- Changed registry keys
  More...

Parameter	Select how the webcam to use should be choosen.
Registry	`[Use first webcam][Choose by name] [Choose by vendor_id:product_id][Choose by number] [Choose by devicename][Choose by priority]`
Value	Use first webcam
Parameter	Select resolution to use.
Registry	`multimedia.webcam.virtual_background.resolution`
Value	Use first webcam

- Updated base system to Ubuntu Jammy 22.04.
- Enabled Wifi Manager, Multi Monitor configuration and Display Switch to be fully functional also when endpoint is unlicensed.
- Updated NVIDIA driver to version 525.
- Added ddcutil and ddcui to firmware which are tools to reading and changing monitor settings.

- Changed: IGEL Setup Assistant will come up on every boot as long as the system has starter- or no license. Setup Assistant is not triggered anymore if demo- or productive license is deployed and / or device is connected to an UMS.
- Changed label of mobile broadband configuration dialogue in IGEL OS setup (Country or Region).

X11 System

- Changed default of DRI3 parameter. This is now enabled by default.

Parameter	Use DRI
Registry	`x.drivers.use_dri`
Type	bool
Value	enabled / disabled

Zoom VDI

- Updated **Zoom VDI plugin 5.15.2.23760**
  Available plugins in this release: 5.15.2.23760, 5.14.10.23670 and 5.14.10.23670

Multimedia

- Removed GStreamer 0.10 support.
- Changed: Backscrub package is still from Bionic compile. So, rebuilded against current Jammy libs to get rid of old dependencies.

Hardware

- Added hardware support for **LG USB Multi Port Hub**.
- Added hardware support for **Lenovo ThinkPad L14 (AMD) Gen 4**.
- Added hardware support for **Lenovo ThinkPad L15 (AMD) Gen 4**.
- Added hardware support for **Pepperl&Fuchs BTC12N and BTC14N**.
- Added hardware support for **HP Pro mt440 G3**.
- Added hardware support for **Lenovo ThinkPad L14 Intel Gen 4**.
- Added hardware support for **Lenovo ThinkPad L15 Intel Gen 4**.

Java

- Updated Java runtime environment to **Zulu JRE version 17.0.8-1**.

Remote Management

- Added: Transfer devices serial number to UMS on first boot of device.

- If requirements for upgrading to IGEL OS12 are fulfilled, the field **OS Type** in UMS is extended by the **OS12 Upgrade Ready** attribute - e.g. **IGEL Linux 11 (OS12 Upgrade Ready; Kernel Version 6.1.42)**

Resolved Issues 11.09.100

Citrix

- Fixed: Situations where hardware decoder has not enough memory to handle certain video formats properly, are optimized / better handled now.
- Fixed: In rare situations (observed when using teams app sharing) intermixed video frames appear which come from different H.264 streams. These frames are now being separated from each other and will be decoded separately.
- Added a new registry key to suppress such secondary frames entirely, as they render mostly duplicated content of the primary frames.

Parameter	In case of mixed up H264 streams: Don't display frames from secondary streams
Registry	`ica.hw-accelerated-h264-suppress-secondary-frames`
Type	bool
Value	enabled / disabled

- Fixed: **Refresh/Redraw issues of Citrix session windows.** Resuming from screensaver or uncovering a session window which was covered by another window works as expected now.
- Changed: Default for `ica.module.audioredirectionv4=true` due to connection problems with some VDI versions.
- Fixed: **H.264 streams** with multiple reference frames (as produced by hardware encoders) are supported properly and do not lead to a potential crash anymore.
- Fixed: In special situations, certain frames did not show up on the screen when **VDPAU** was configured.
- Fixed: **MS Teams optimization** (CWA 2307).

AVD

- Changed the **x264enc QP** setting to do less aggressive video quantization to improve outgoing video quality in MS Teams.
- Fixed **smartcard redirection** in AVD client.
- Fixed **crash when last audio device was removed**.
- Adaptive (average) **MS-Teams video playback** delay calculation and no key frame skipping on decoding to make playback more reliable.
- Changed: Raised `net.core.wmem_max` setting if **AVD sessions are configured to avoid TCP connection resets being triggered by the Linux Kernel on large RdClientSDK data transfers**.
- Fixed **screenshare issue** with direct MS Teams calls when screen share is already active.
- Fixed **potential client crash** when virtual backgrounds are enabled in MS Teams.
- Fixed **stale video window content in MS Teams** when video feeds are switched but incoming video is not directly decodable.

- Changed **quantization range for the x264enc** to allow a little more quantization being applied to outgoing MS Teams video streams.
- Fixed: Avoid large display delay of **incoming MS Teams video streams by measuring NTP latenc**y.
- Changed **MS-Teams video scaling default** to fill-frame, instead of fit-frame.
  Note that the related MS Teams settings are not redirected through the RdClientSDK, so it will always show in fill-frame mode in MS Teams.

RDP/IGEL RDP Client 2

- **Removed Multimedia Redirection** for **Windows Server2012r2 RDP Sessions**.

VMware Horizon

- Fixed: **Horizon session starter** cannot handle backslashes in password.

Parallels Client

- Fixed an issue with **multiple USB devices** not being redirected correctly.

Network

- Added possibility to **set an antenna bitmap** to configure **which antenna should be used** (for iwlwifi devices).
- Added **new registry key** to configure the antenna bitmap.
  More...

Parameter	Tx antenna bitmap
Registry	`network.interfaces.wirelesslan.device0.antenna_bitmap_tx`
Type	string
Value	None
Parameter	Rx antenna bitmap
Registry	`network.interfaces.wirelesslan.device0.antenna_bitmap_rx`
Type	string
Value	None

- Improved behaviour of WWAN devices on suspend/resume

WiFi

- Improved handling of WiFi network names with non-ASCII characters
- Added registry keys for restricting frequencies used by WPA Supplicant (see the WPA Supplicant documentation regarding the network-specific settings `freq_list` and `scan_freq`). In IGEL OS, the settings affect all configured WiFi´s - these may be useful to improve roaming behaviour.
  More...

Parameter	List of allowed frequencies
Registry	`network.interfaces.wirelesslan.device0.freq_list`
Type	string
Value	None
Parameter	List of frequencies to scan
Registry	`network.interfaces.wirelesslan.device0.scan_freq`
Type	string
Value	None

CUPS Printing

- Fixed **cups** not starting properly.

Cisco Webex

- Fixed **Webex Meetings VDI** not connecting to enterprise site.

Base System

- Fixed reconnect of Lenovo Docking Station TBT Gen 3.
- Added **new registry key** to `set acpi= kernel cmdline` options (some devices needs `acpi=off`).

Parameter	Set ACPI kernel parameters.
Registry	`system.kernel.bootparams.acpi`
Range	[No setting][Force][On][Off][Noirq][Strict][Rsdt][Copy_dsdt]
Value	None

- Added **new registry key to set reboot kernel** `cmdline` which can be used if reboot or shutdown issues are present.

Parameter	Set reboot kernel parameters.
Registry	`system.kernel.bootparams.reboot`
Range	[Default][Bios][Triple][Kbd][Acpi][Efi][Pci]
Value	Default

- Fixed **ELO AccuTouch** not picking up selection.
- Fixed r**eloading of license page** in IGEL Setup Assistant.
- Added licensing information for **Lenovo's FCC unlock tool**.
- Changed to **s2idle on HP mt440 G3** as it improves behavior.
- Changed **registry key** for use **mem sleep mode**, depending on hardware

Parameter	Set suspend mem sleep mode.
Registry	`system.suspend.sleep_mode`
Range	[Default][Suspend to RAM][Suspend to idle]
Value	Default

- Fixed **ELO multitouch** configuration: No kernel module is needed anymore.
- Fixed handling of **custom bootsplash** and wallpaper download-url
- Fixed feature selection in **OS Creator**.
- Changed the default setting for the `mirror mode` to the biggest common resolution (was Panning before)

Parameter	Choose the mode which should be used for mirroring monitors if resolution differs.
Registry	`x.xserver%.mirror_mod`
Range	[Panning][Biggest common resolution][Scaling][Scaling down]
Value	Biggest common resolution

- Changed the `handle_brightness_keys` default to **enabled** as this setting is needed for most of the current laptops anyways.

Parameter	Handle Brightness Keys
Registry	`x.xserver%.handle_brightness_keys`
Type	bool
Value	enabled / disabled

- Use new DP MST connector setup name handling as new default as this avoids issue with only one monitor could get configured. This may cause issues with already present display profiles so you may need to revert this but in most cases you will already have this key set.

Parameter	Use new DP MST connector setup name handling
Registry	`x.drm_daemon.use_new_dp_mst_handling`
Type	bool
Value	enabled / disabled

- Fixed suspend / resume support on **Lenovo L14 Intel Gen3** device.

H624

- Fixed: **H.264 streams with multiple reference frames** (as produced by hardware encoders) are supported properly and do not lead to a potential crash anymore.
- Fixed: In special situations, certain frames did not show up on the screen when **VDPAU** was configured.

X11 system

- Changed default setting for **DisplayLink Quirk** which solves an issue with long startup times
- **Registry key parameter** now defaults to true:

Parameter	Quirk to fix issues with Xorg start take ages with DisplayLink connected.
Registry	`x.xserver%.quirks.displaylink_crash_workaround`
Type	bool
Value	enabled / disabled

- Changed: Update of **screen configuration** after resume - to ensure changes while suspend are detected / effective.

Audio

- Fixed: Sound preferences not getting saved over reboot.

Misc

- Fixed **autostart notification of sessions** in case restart is also active.

Hardware

- Fixed screen lagging issue with **Dell Latitude 7430.**
- Added possibility to configure **Intel PSR setting** via registry.

Parameter	Change settings for intel PSR (panel self refresh).
Registry	`x.drivers.intel.psr`
Range	[Default][Disable][Enable][Use only up to PSR1][Use up to PSR2]
Value	Default

- Fixed immediate wakeup issue after shutdown on some **HP mt645 G7**

Remote Management

- Fixed submitting **device states to the UMS**.
- Fixed: **Web console shadowin**g via ICG.
- Fixed submitting **device's uptime and total usage over ICG.**

Notes for Release 11.08.440

Software:	Version	11.08.440
Release Date:	2023-08-16	
Release Note:	Version	RN-1108440-1
Last update:	2023-08-16	

- Supported Devices 11.08.440 (see page 2640)
- Component Versions 11.08.440 (see page 2641)
- Known Issues 11.08.440 (see page 2650)
- Security Fixes 11.08.440 (see page 2655)
- New Features 11.08.440 (see page 2656)
- Resolved Issues 11.08.440 (see page 2663)

The Release Notes of IGEL OS 11.08.440 are also available in the following formats:

- Plain text: readme_11.08.440.txt[263]

263. https://www.igel.de/wp-content/uploads/2023/08/lxos_11.08.440.txt

Supported Devices 11.08.440

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX	UD6-LX 51
UD7-LX	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Devices Supported by IGEL OS 11 (see page 2640).

Component Versions 11.08.440

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	114.0.5735.198-1igel1689190033
Cisco JVDI Client	14.1.3
Cisco Webex VDI plugin	43.6.0.26643
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.6.0.158
Zoom Media Plugin	5.12.6.22200
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.10.23670
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.05.0.58
Citrix Workspace App	23.07.0.17
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.4.0.37727
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2

FabulaTech Plugins	3.10.0.9
FabulaTech USB for Remote Desktop	6.1.3.1
FabulaTech Scanner for Remote Desktop	3.3.0.2
FabulaTech Webcam for Remote Desktop	2.8.11
Firefox	102.13.0
IBM iAccess Client Solutions	1.1.9.2
IGEL RDP Client	2.2igel1687350866
IGEL AVD Client	1.1.27igel1691066375
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.11.0.665541_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
OpenVPN	2.6.1-1igel1680534357
Zulu JRE	8.0.382-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324

ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-4igel1648284944
VMware Horizon Client	2306-8.10.0-21964631
Voip Client Ekiga	4.0.1-9build1igel1646743191

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.4
Philips Speech driver	13.2.3

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/ interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.23.0-0.3igel1686055473
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20

PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1667897461
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	2.0.0-1igel1691065840
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.13
OpenSSL	1.1.1-1ubuntu2.1~18.04.23
OpenSSH Client	9.3p2-1igel1690097953
OpenSSH Server	9.3p2-1igel1690097953
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534

Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos-g1690808458
Xorg X11 Server	21.1.7-2igel1680497175
Xorg Xephyr	21.1.7-2igel1680497175
CUPS printing daemon	2.2.7-1ubuntu2.10igel1687852140
PrinterLogic	25.1.0.637
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.4
NetworkManager	1.32.12-0ubuntu1igel1684263019
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229

GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.38.6-0+deb10u1igel1684758904
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu GuestAgent	8.0.3+dfsg-3igel1690307265

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743

Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	35.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	683.0 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	84.2 M	Included
VMware Horizon RDP	6.2 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	21.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	189.5 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	134.8 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.8 M	Not included
Imprivata Appliance	14.8 M	Included

AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	13.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	68.8 M	Included
PrinterLogic	43.5 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	22.2 M	Not included
AVD	133.0 M	Included
Local Browser (Chromium)	96.2 M	Not included
Amazon WorkSpaces Client	32.8 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	105. M	Not included
Cisco Webex Meetings VDI	194.0 M	Not included
Zoom Media Plugin	177.0 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	1.5 M	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	10.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	18.8 M	Included
90meter Smart Card Support	256.0 K	Included

Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	67.2 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	34.8 M	Included

Known Issues 11.08.440

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key needs to be enabled:
  More...

Parameter	`Activate workaround for dual RTME sessions and H264 acceleration`
Registry	`ica.workaround-dual-rtme`
Value	enabled / **disabled** (default)

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active session does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occure with **multimedia redirection of H.264, MPEG1 and MPEG2**. (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser Content Redirection** (BCR) does not work if **DRI3** and **hardware accelerated H.264 deep compression codec** is **enabled**.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** from this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression" -> > For the entire screen.**
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- While starting Self-Service, it is possible that process **ServiceRecord segfaults -> Self-Service cannot be started afterwards**.
  A **cache cleanup with reboot** is needed. In addition, the **following parameters should set to "true"**.
  More...

Parameter	`Clean up UI cache after Self-Service termination`
`Registry`	`ica.selfservice.cleanupwebui`
Value	**false** (default)/true
Parameter	`Clean up Store cache after Self-Service termination`

Registry	`ica.selfservice.cleanupstore`
Value	**false** (default)/true

- **Logoff of Self-Service causes a segfault with CWAL 2211** which ends the application. Restart of Self-Service is functional.
- **Browser Content Redirection (BCR)** may not work with **Chrome** version **105.0.*** or later
- **White/ green fragments** may appear during desktop launch if **JPEG graphical codec** is used.
- Under certain conditions, **webcam redirection may not work**.
  If this is the case, **GStreamer has to be set to version 1.0** via registry or by enabling **Browser Content Redirection (BCR)**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance: Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **H.264 hardware decoding for MS-Teams optimization is currently limited to non - AMD devices due to stability issues on AMD devices**.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window**, which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** when TC Setup is running at the same time.
- **With usage of PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.

If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadic problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for theses devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB-redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session
- **USB device redirection** is considered as **experimental for the Parallels client for Linux.**

Firefox

- With **enabled Citrix Browser Content Redirection, Firefox has no H.264 and AAC multimedia codec support**. Means, **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.
- **Multimedia playback** in Firefox is **unstable if GStreamer version 0.10 is active**. The default GStreamer version for Firefox sessions.browser<inst>.gstreamer_version was set to 1.0.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510.**
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** does not work after system suspend/resume.
  Workaround: Disabling system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during logout of Citrix Desktop session). Occurs only when using **Citrix Workspace App 2010** and **Cisco JVDI**.

Base system

- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary)

Conky

- The **right screen when using multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On **devices with 2 GB of flash** storage it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit [https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough- space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice (instead of once).
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersand (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. E.g.:
  'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3-M340C: Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.
- **Wake-up from suspend via UMS** does not work on **HP mt645 devices. Workaround: Disable system suspend and use shutdown** instead.
- **System suspend** is not supported on **Lenovo L14 Gen 3 Intel**-based device.
- **Built-in fingerprint sensor** is not supported on **HP mt440** and **mt645**.
- **Mac-Address Passthrough** not supported on **Lenovo USB-C Hybrid Docking Station**.
- **Wake on Lan via docking stations** is not supported.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.08.440

IBM_5250

- Updated **IBM iAccess Client** Solutions to version **1.1.9.2.** Complete changelog via [https://www.ibm.com/support/pages/ibm-i-access-acs-updates]

Chromium

- Updated **Chromium browser** to version **114** (for fixing CVE-2023-3079).

Firefox

- Updated **Mozilla Firefox** to version **102.13.0 ESR**:
- Fixes for **mfsa2023-23**, also known as: CVE-2023-37201, CVE-2023-37202, CVE-2023-37207, CVE-2023-37208, CVE-2023-37211.
- Fixes for **mfsa2023-19**, also known as: CVE-2023-34414, CVE-2023-34416.
- Fixes for **mfsa2023-17**, also known as: CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215.

Base System

- Fixed **cups** security issue CVE-2023-32324.
- Fixed **libx11** security issue CVE-2023-3138.
- Fixed **libxml2** security issue CVE-2022-2309.
- Fixed **openssh** security issue CVE-2023-28531.
- Fixed **dmidecode** security issue CVE-2023-30630.
- Fixed **opensc** security issue CVE-2023-2977.
- Fixed **texlive-bin** security issue CVE-2023-32700.
- Fixed **ncurses** security issues CVE-2023-29491, CVE-2022-29458, CVE-2021-39537, CVE-2019-17595 and CVE-2019-17594.
- Fixed **perl** security issue CVE-2023-31484.
- Fixed **openssl1.0** security issue, CVE-2023-2650.
- Fixed **openssl** security issue CVE-2023-2650.
- Fixed **libuv1** security issue CVE-2021-22918.
- Fixed **zulu8-ca** security issues CVE-2023-22049, CVE-2023-22043 and CVE-2023-22045.
- Fixed **openssh** security issue CVE-2023-38408.
- Fixed **qemu** security issues CVE-2023-2861, CVE-2023-1544, CVE-2023-0330 and CVE-2022-1050.

New Features 11.08.440

Citrix

- Updated **Citrix Workspace App to version 2307**.
  Available **Citrix Workspace Apps** in this release: **2307 (default), 2305 and 2010.** Added support for playing short tones in optimized **Microsoft Teams** - **requires update to the latest version of Microsoft Teams.**
- Changes with **Citrix Workspace App 2305 and 2307**:
  New features:
- Copy and paste files and folders between two virtual desktops [Technical Preview]

Parameter	`Copy and paste files and folders between two virtual desktops`
Registry	`ica.module.vdgdt`
Value	true (default)/ false

- Enhancement on 32-bit cursor support [Technical Preview]

Parameter	`Enhancement on 32-bit cursor support`
Registry	`ica.wfclient.Cursor32bitsupport`
Value	true (default)/ false

- Change the default browser fo FIDO2

Parameter	`Change the default browser for FIDO2`
Registry	`ica.authman.fido2authbrowser`
Value	CEB (default), chromium, firefox, chromium-browser

- Support for authentication using FIDO2 when connecting to on-premises stores [Technical Preview]

Parameter	`Support for authentication using FIDO2 when connecting to on-premises stores`
Registry	`ica.authman.fido2enabled`
Value	flase (default)/ true

- Fixed:

- App Protection works with all the Citrix session types, including Firefox browser. Reboot of system after enabling/disabling the feature (ica.appprotection) is required.

AVD

- Added WebRTC h264 encoder preset option:

Registry	`sessions.wvd%.options.webrtcencoderpreset`
Value	none / ultrafast / superfast / veryfast / faster / fast / **medium** (default) / slow / slower / veryslow / placebo

- Added initial secondary ringer support. But since the **RdClientSDK support** for it currently is **non-functional** (the sinkId does not change on the related MS- Teams setting), we added a command line option " `--webrtc-ring-all-devices` " and have set that as default in the **cmd_ext** setting. This makes MS-Teams ring on all audio output devices. **This default setting will be removed** as soon as the **RdClientSDK implementation works as expected!**
- Added clock to **appbar - enable** via **System > Registry >** `sessions.wvd%.options.cmd_ext = -a`
- If **appbar** is enabled, the **workarea of the session is reduced accordingly.**
- The **appbar is always visible now**

VMware Horizon

- Updated Horizon client to version 2306-8.10.0-21964631

Parameter	`Open local files in published applications`
Registry	`vmware.view.enable-file-association`
Type	bool
Value	**enabled** (default) / disabled
Parameter	`Auto-connect to remote desktop or published app in case there's only one of them`
Registry	`vmware.view.single-auto-connect`
Type	bool
Value	enabled / **disabled** (default)
Parameter	`Automatically connect to the desktop if there is only one or connect to the one which name is given`

Registry	`vmware.view.auto-connect-desktop`
Type	bool
Value	enabled / **disabled** (default)

Parameter	`Automatically connect to this server when starting the client`
Registry	`vmware.view.auto-connect-broker`
Type	string
Value	empty **Default**

Parameter	`Client behavior when all Sessions have been disconnected`
Registry	`vmware.view.all-sessions-disconnected-behavior`
Range	[Unconfigured][Quit client][Logoff from server][Keep current state]
Value	**Unconfigured**

Parameter	`Disconnect empty App session automatically`
Registry	`vmware.view.auto-disconnect-empty-app-session`
Type	bool
Value	**enabled** (default) / disabled

Parameter	`Maximum count of core dump files allowed`
Registry	`vmware.view.maxcoredumps`
Type	integer
Value	0 **Default**

Network

- **Added MAC-address** pass through among **Ethernet device**s. **With the following registry key a LAN device can be specified** from which the MAC address shall be adopted. **The donor device and any conflicting receiver devic**e will be removed (by unbinding the driver) as long as the receiving device is present.

Parameter	`MAC address source`
Registry	`network.interfaces.ethernet.device%.mac_source`
Range	[none][LAN][LAN2][LAN3][LAN4]
Value	**none**

- Example: If LAN2 and LAN3 are configurations for docking stations that shall adopt the MAC address from LAN, the following two parameters must be set to "LAN":
  `network.interfaces.ethernet.device1.mac_source`
  `network.interfaces.ethernet.device2.mac_source`
  Warning: Misconfiguration may result in loss of connectivity
- Added Lenovo FCC unlock tool for Quectel EM05

Open VPN

- Updated cipher configuration of Open VPN. Now it is possible to specify the data-ciphers list. By default, the default cipher list **AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305** is active. Otherwise, a custom list can be specified in the **Data ciphers parameter**. Enter the ciphers separated with **:.** The existing parameter **Cipher** was renamed to **Cipher (legacy parameter)** and now has a new value **unset** in range, which means that the parameter cipher will be omitted in the configuration.

Setup	`Network > VPN > Open VPN > Connection > Options`
Parameter	`Use default data cipher list`
Registry	`sessions.openvpn%.vpnopts.use_default_cipher_list`
Value	**on** / off
Setup	`Network > VPN > Open VPN > Connection > Options`
Parameter	`Data ciphers`
Registry	`sessions.openvpn%.vpnopts.data_ciphers`
Value	empty **Default**

OpenConnect VPN

- Added further supported protocols for **OpenConnect VPN client by adding Fortinet**, F5 and Array. **OpenConnect VPN** is a feature with limited support, and the new protocols are not validated by IGEL.

Setup	Network>VPN>OpenConnect VPN>Name>Session
Parameter	`Protocol`
Registry	`sessions.openconnect<INST>.vpnopts.protocol`
Value	{**}anyconnect{**}/nc/pulse/gp/f5/fortinet/array

Imprivata

- Added 'IGEL Agent for Imprivata'. This requires an addon license (request via [https://www.igel.com/imprivata-agent/]).

CUPS Printing

- Updated **PrinterLogic PrinterInstallerClient to version 25.1.0.637**
  Fixes the determination of the AD user when Kerberos login is used.

Cisco Webex

- Updated **Cisco Webex Meetings VDI plugin** to version **43.6.0.158**
  ** Available versions: **42.6.11.6, 42.10.8.14, 43.6.0.158**
- Updated **Cisco Webex VDI plugin** to version **43.6.0.26643**

Base system

- Added some additional resolutions to the **webcam virtual background solution** (see changed registry keys).
- Enables to choose webcams for virtual background by device name and priority.
- Added new registry keys:

Parameter	`Select webcam by devicename for example /dev/video0 or video0 (only valid if choose by devicename is used)`
Registry	`multimedia.webcam.virtual_background.webcam_device`
Type	string
Value	empty **Default**
Parameter	`Select webcam by priority list for example dev=video0;name=HD_Webcam_C270 (only valid if choose by priority is used)`

Registry	`multimedia.webcam.virtual_background.webcam_priority`
Type	string
Value	empty **Default**

- Changed registry keys

Parameter	`Select how the webcam to use should be choosen.`
Registry	`multimedia.webcam.virtual_background.choose_webcam_by`
Range	[Use first webcam][Choose by name] [Choose by vendor_id:product_id][Choose by number] [Choose by devicename][Choose by priority]
Value	**Use first webcam**

Parameter	`Select resolution to use.`
Registry	`multimedia.webcam.virtual_background.resolution`
Range	[webcam default][webcam max][1920x1080][1280x720][640x480][480x360][424x240][320x240][320x180]
Value	**webcam default**

- Enabled Wi-Fi Manager, Multi Monitor configuration and Display Switch to be fully functional also when endpoint is unlicensed.

Driver

- Updated **Olympus driver** for dictation to version **4.0.4**.
- Updated **Philips Speech driver** to version **13.2.3.** Update fixes a minor bug in the Linux drivers which possibly caused unexpected error messages in some target software products. Furthermore, driver supports usage of PulseAudio (contrary to ALSA) audio interface. To be enabled via following registry parameter:

Parameter	`Use PulseAudio`
Registry	`devices.philipsspeech.use_pulseaudio`
Type	bool
Value	enabled / **disabled** (default)

zoomvdi

- Updated **ZoomVDI** to version **5.14.10.23670**.
  Available versions: **5.14.10.23670 (default), 5.13.10.23090** and **5.12.6.22200**.

Hardware

- Added hardware support for the **Lenovo USB-C Universal Docking**
- Added hardware support for **Lenovo L14 (AMD) Gen 4**
- Added hardware support for **Lenovo L15 (AMD) Gen 4**
- Added hardware support for **HP Pro mt440 G3** (excluding WWAN support).

Remote Management

- Added: Transfer device's serial number to UMS on first boot of device.

Fabulatech

- Updated **FabulaTech USB** for Remote Desktop to version **6.1.3.1**.
- Updated **FabulaTech Plugins** to version **3.10.1.5**.
- Updated **FabulaTech Scanner** for Remote Desktop to version **3.3.0.2**.
- Updated **FabulaTech Webcam** for Remote Desktop to version **2.8.11**.

Resolved Issues 11.08.440

Citrix

- Fixed: **Situations where hardware decoder has not enough memor**y to handle certain video formats properly, are optimized / better handled now.
- Fixed: In rare situations (observed when using teams app sharing) **intermixed video frames appear which come from different H.264 streams**. These frames are now being separated from each other and will be decoded separately.
- Added a **new registry key to suppress such secondary frames entirely**, as they render mostly duplicated content of the primary frames.

Parameter	`In case of mixed up H264 streams: Don't display frames from secondary streams`
Registry	`ica.hw-accelerated-h264-suppress-secondary-frames`
Type	bool
Value	**enabled** (default) / disabled

- Fixed: **Refresh/Redraw issues of Citrix session windows**. Resuming from screensaver or uncovering a session window which was covered by another window works as expected now.
- Fixed: **dynamic e911 feature**.
- Added registry key `ica.chrome-double-download` to control flock feature at wfica_wrapper. **Enable flock** blocks double app starts (due to double downloads by Chromium browser).

Parameter	`Control download mechanic for Citrix applications for Chrome web access`
Registry	`ica.chrome-double-download`
Range	[Enable Lock][Disable Lock]
Value	enable / **disable** (default)

- Fixed: **Web-based Citrix Cloud authentication pages**.
- Changed: Default for `ica.module.audioredirectionv4=true` due to connection problems with some VDI versions.
- Fixed: **H.264 streams** with multiple reference frames (as produced by hardware encoders) are supported properly and do not lead to a potential crash any more.
- Fixed: In special situations, certain frames did not show up on the screen when **VDPAU** was configured.

AVD

- Improved: MS Teams video quality optimizations applied.
- Fixed broken appbar - which can be enabled with System > Registry > sessions.wvd%.options.cmd_ext = -a
- Changed the x264enc QP setting to do less aggressive video quantization to improve outgoing video quality in MS Teams.
- Fixed autostartsingle registry option.
- Fixed screenshare issue with direct MS Teams calls when a screenshare is already active.
- Fixed potential client crash when virtual backgrounds are enabled in MS Teams.
- Fixed stale video window content in MS Teams when video feeds are switched, but incoming video is not directly decodable.
- Adjusted the quantization range for the x264enc to allow a little more quantization being applied to outgoing MS Teams video streams.
- Fixed: Avoid large display delay of incoming MS Teams video streams by measuring NTP latency.

RDP/IGEL RDP Client 2

- Fixed RDP timezone redirection not working for some locations.
- Fixed fullscreen RDP session not starting with no monitor connected.

VMware Horizon

- Fixed: **Horizon session starter** cannot handle backslashes in password.

Chromium

- Added registry key to **toggle prompt** to accept downloads:

Parameter	`Enable IGEL Download Dialog`
Registry	`chromiumglobal.app.enable_download_dialog`
Type	bool
Value	**enabled** (default) / disabled

Network

- Fixed network configuration on **HyperV.**
- Added possibility to set an **antenna bitmap** to configure which antenna should be used (for iwlwifi devices)
- Added **new registry key to configure the antenna bitmap**

Parameter	`Tx antenna bitmap`

Registry	`network.interfaces.wirelesslan.device0.antenna_bitmap_tx`
Type	string
Value	empty **Default**
Parameter	`Rx antenna bitmap`
Registry	`network.interfaces.wirelesslan.device0.antenna_bitmap_rx`
Type	string
Value	empty **Default**

- Improved behaviour of **WWAN** devices on suspend/resume
- Fixed setting credentials for **system-wide proxy**.

Cisco Webex

- Renamed **libstdc++.so.6**, Webex Meetings client expects the highest version of **libstdc++.so.6.**

Base System

- Added new registry key to set **acpi= kernel cmdline** options (some devices needs acpi=off).

Parameter	`Set ACPI kernel parameters.`
Registry	`system.kernel.bootparams.acpi`
Range	[No setting][Force][On][Off][Noirq][Strict][Rsdt][Copy_dsdt]
Value	**No setting**

- Added new registry key to set **reboot kernel cmdline** which can be used if reboot or shutdown issues are present

Parameter	`Set reboot kernel parameters.`
Registry	`system.kernel.bootparams.reboot`
Range	[Default][Bios][Triple][Kbd][Acpi][Efi][Pci]
Value	**Default**

- Fixed issue with **ELO AccuTouch** not picking up selection.
- Changed the `handle_brightness_keys` **default to enabled,** as this setting is needed for most of the current laptops anyways.

Parameter	`Handle Brightness Keys`
Registry	`x.xserver%.handle_brightness_keys`
Type	bool
Value	**enabled** (default) / disabled

- Fixed instability in handling of **certain webcam devices**, e.g. Meeting Owl 3.
- Added licensing information for **Lenovo's FCC unlock tool.**
- Use **s2idle on HP mt440 G3** as it works better
- Changed registry key to be able to use **mem sleep** mode depending on hardware

Parameter	`Set suspend mem sleep mode.`
Registry	`system.suspend.sleep_mode`
Range	[Default][Suspend to RAM][Suspend to idle]
Value	**Default**

H264

- Fixed: **H.264 streams** with multiple reference frames (as produced by hardware encoders) are supported properly and do not lead to a potential crash anymore.
- Fixed: In special situations, certain frames did not show up on the screen when **VDPAU** was configured.

X11 System

- Changed default setting for **DisplayLink Quirk** which solves an issue with long startup times
- Registry key parameter now defaults to **true**:

Parameter	`Quirk to fix issues with Xorg start take ages with DisplayLink connected.`
Registry	`x.xserver%.quirks.displaylink_crash_workaround`
Type	bool
Value	**enabled** (default) / disabled

Audio

- Fixed: **Sound preferences** not getting saved over reboot.

Remote Management

- Added: Create log for support information if **rmagent has been requested to release the device from UMS**.
- Retrieve the device's unit **ID** in more robust way.
- The log file is **only accessible to root**

Notes for Release 11.08.360

Software:	Version	11.08.360
Release Date:	2023-06-14	
Release Notes:	Version	RN-1108360-1
Last update:	2023-06-14	

- Supported Devices 11.08.360 (see page 2669)
- Component Versions 11.08.360 (see page 2670)
- Known Issues 11.08.360 (see page 2679)
- Security Fixes 11.08.360 (see page 2684)
- New Features 11.08.360 (see page 2685)
- Resolved Issues 11.08.360 (see page 2686)

The Release Notes for IGEL OS 11.08.360 are also available in the following formats:

- Plain text: readme_11.08.360.txt

Supported Devices 11.08.360

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[264].

264. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.360

Clients

Product	Version
Amazon WorkSpaces Client	4.1.0
Chromium	112.0.5615.165-igel1686558208
Cisco JVDI Client	14.1.3
Cisco Webex VDI plugin	43.4.0.25788
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.2.1.18
Zoom Media Plugin	5.12.6.22200
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.14.0.23370
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.02.0.10
Citrix Workspace App	23.03.0.32
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.4.0.37727
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2

FabulaTech Plugins	3.10.0.9
FabulaTech USB for Remote Desktop	6.1.2.9
FabulaTech Scanner for Remote Desktop	3.0.1.0
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	102.10.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1685958191
IGEL AVD Client	1.1.17igel1683185301
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.11.0.665541_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
OpenVPN	2.6.1-1igel1680534357
Zulu JRE	8.0.372-1
Parallels Client	19.2.0.23906
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037

VNC Viewer	1.12.0+dfsg-4igel1648284944
VMware Horizon Client	2303-8.9.0-21435420
Voip Client Ekiga	4.0.1-9build1igel1646743191

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.3
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1667897461
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.9-1igel1677589353
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.12
OpenSSL	1.1.1-1ubuntu2.1~18.04.22
OpenSSH Client	9.0p1-1+b1igel1661867805
OpenSSH Server	9.0p1-1+b1igel1661867805
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891

Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos-g1681319724
Xorg X11 Server	21.1.7-2igel1680497175
Xorg Xephyr	21.1.7-2igel1680497175
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.625
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.4
NetworkManager	1.32.12-0ubuntu1igel1684263019
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1

GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.38.6-0+deb10u1igel1684758904
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu Guest Agent	7.2+dfsg-6igel1683015333

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	35.5 M	Included

Citrix Appliance Citrix Workspace app Citrix StoreFront	481.0 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	84.2 M	Included
VMware Horizon RDP	6.2 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	21.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	187.2 M	Included
Voice over IP (Ekiga)	6.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.8 M	Not included
Imprivata Appliance	14.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	68.8 M	Included
PrinterLogic	43.5 M	Not included

Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	22.2 M	Not included
AVD	133.0 M	Included
Local Browser (Chromium)	107.5 M	Not included
Amazon WorkSpaces Client	32.8 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	99.0 M	Not included
Cisco Webex Meetings VDI	177.2 M	Not included
Zoom Media Plugin	176.8 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	1.5 M	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	9.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	18.8 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included

VirtualBox (Limited support)	66.8 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	34.8 M	Included

Known Issues 11.08.360

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser Content Redirection** (BCR) does not work if **DRI3** and **hardware-accelerated H.264 deep compression codec** are **enabled**.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- When starting Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**.
  A **cache cleanup with a reboot** is needed. In addition, the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

- **Logoff of Self-Service causes a segfault with CWAL 2211** which ends the application. The restart of Self-Service is functional.
- **Browser Content Redirection (BCR)** may not work with **Chrome** version **105.0.*** or later.
- **White/ green fragments** may appear during desktop launch if **JPEG graphical codec** is used.
  -There may be problems with **webcam redirection at Citrix**. To fix the problem, **GStreamer 1.0** must be enabled - this can be done either via the registry for the session or by enabling the browser content redirection (BCR).
  - Under certain conditions, **webcam redirection** may not work. If this is the case, **GStreamer has to be set to version 1.0** via registry or by enabling **Browser Content Redirection** (BCR).

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: **Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.
- **Scanning images** within an AVD session (with the usage of FabulaTech Scanner Redirection) **might fail and cause a reconnection** if the compression level is set to high quality. As a **workaround**, the **compression level must be reduced**.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.

This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
The respective settings can be found in the IGEL Registry:
`vmware.view.enable-serial-port-redir`
`vmware.view.enable-scanner-redir`

- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.
- **Multimedia playback** in Firefox is **unstable if GStreamer version 0.10 is active**. The default GStreamer version for Firefox `sessions.browser\<inst>.gstreamer_version` was set to 1.0.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.
- **Set of credentials for manual system-wide proxy** is **broken**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[265] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

265. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.
- **Wake-up from suspend via UMS** does not work on **HP mt645 devices**. **Workaround**: **Disable system suspend** and **use shutdown** instead.
- **System suspend** is not supported on **Lenovo L14 Gen 3 Intel**-based device.
- If **bluetooth** is disabled via tray icon / menu on **Lenovo L14 Gen3 (Intel-based)**, bluetooth tray icon is permanently disabled. Can be solved / re-enabeld with console command `rfkill unblock bluetooth`
- **Built-in fingerprint sensor** is not supported on **HP mt645**.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Fabulatech

- **Scanning images within an AVD session** (with the usage of **FabulaTech Scanner Redirection**) might fail and cause a reconnection if the compression level is set to high quality.
  As a **workaround**, the **compression level must be reduced.**

Security Fixes 11.08.360

Base System

- For security reasons, the accessory '**Network Tools**' is enforced to run with **Administrator (root) privileges only**. Therefore, parameter 'Password protection on page **Accessories > Network Tools** was **removed**.
- Fixed **cups-filters** security issue CVE-2023-24805.
- Fixed **mysql-5.7** security issues CVE-2023-21980 and CVE-2023-21912.
- Fixed **libwebp** security issue CVE-2023-1999.
- Fixed **libssh** security issues CVE-2023-2283 and CVE-2023-1667.
- Fixed **webkit2gtk** security issues CVE-2023-28205, CVE-2023-27954, CVE-2023-27932, CVE-2022-32885, and CVE-2022-0108.
- Fixed **binutils** security issues CVE-2023-25588, CVE-2023-25585 and CVE-2023-25584.
- Fixed **postgresql-10** security issues CVE-2023-2455 and CVE-2023-2454.

New Features 11.08.360

Parallels Client

- Updated **Parallels client** to **version 19.2.0**

Network

- Added **support** for **WWAN chipset Quectel EM05 on Lenovo L14 Gen3**

Wi-Fi

- Added option for **DHCP refresh after roaming (within the same network)**.

Parameter	Refresh DHCP after roaming
Registry	`network.interfaces.wirelesslan.device0.roam_refresh_dhcp`
Type	bool
Value	enabled / disabled

Base System

- Added possibility to **clean-up IGEL licenses in license partition**. License files which are superseded by other licenses will be removed and not downloaded from the UMS again. This helps keeping free space for new license files. The following parameter activates the license cleanup:

Parameter	Clean up redundant licenses
Registry	`system.remotemanager.license_cleanup`
Value	true / false

zoomvdi

- Integrated **Zoom VDI 5.14.0.23370**
  Available Zoom VDI Clients: **5.12.6.22200**, **5.13.10.23090**, and **5.14.0.23370**

Hardware

- Added hardware support for **LG CQ601I**
- Added hardware support for **Lenovo ThinkEdge SE10**
- Added hardware support for **HP mt645 G7 with Ryzen 5**

Resolved Issues 11.08.360

RD Web Access

- Fixed **mouse pointer disappearing** in RemoteApp sessions.

VMware Horizon

- Fixed **Single Sign-On** feature in Horizon.
  The domain name is given by Kerberos in the format like in `domain.com`.
  This does not work for all Horizon installations.
- Therefore, configuration **option to specify / set domain format** is added:

Parameter	Fixup domain for Single Sign-On
Registry	`vmware.view.sso-cred-mode`
Range	[Derive domain from username] [Use fully qualified domain name] [Use short domain name] [Keep domain as is]
Value	Derive domain from username

Network

- Improved automatic connection with **LTE module Quectel EM05**.

Cisco JVDI Client

- Fixed issue, **Jabra Headset control button** is not working.

Base System

- Fixed the issue that on some devices the **Bluetooth stays off if once disabled over Bluetooth tray menu**.

Audio

- New parameter to disable the **time scheduling** in **pulseaudio module-udev-detect**.

Parameter	Disable timer scheduling for module-udev
Registry	`multimedia.pulseaudio.daemon.disable-module-udev-tsched`

Range	[auto] [true] [false]

Remote Management

- Fixed **assignment of the device's hostname by the UMS** while registering a device.

Notes for Release 11.08.330

Software:	Version	11.08.330
Release Date:	2023-05-17	
Release Notes:	Version	RN-1108330-1
Last update:	2023-05-17	

- Supported Devices 11.08.330 (see page 2689)
- Component Versions 11.08.330 (see page 2690)
- Known Issues 11.08.330 (see page 2699)
- Security Fixes 11.08.330 (see page 2704)
- New Features 11.08.330 (see page 2706)
- Resolved Issues 11.08.330 (see page 2712)

The Release Notes for IGEL OS 11.08.330 are also available in the following formats:

- Plain text: readme_11.08.330.txt

Supported Devices 11.08.330

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[266].

266. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.330

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	112.0.5615.165-igel1682056835
Cisco JVDI Client	14.1.3
Cisco Webex VDI plugin	43.4.0.25788
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.2.1.18
Zoom Media Plugin	5.12.6.22200
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.600
Citrix Workspace App	20.10.0.6
Citrix Workspace App	23.02.0.10
Citrix Workspace App	23.03.0.32
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
EPOS Connect	7.4.0.37727
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2

FabulaTech Plugins	3.10.0.9
FabulaTech USB for Remote Desktop	6.1.2.9
FabulaTech Scanner for Remote Desktop	3.0.1.0
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	102.10.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1683897932
IGEL AVD Client	1.1.17igel1683185301
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.11.0.665541_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.6.1-1igel1680534357
Zulu JRE	8.0.372-1
Parallels Client	19.1.1.23476
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037

VNC Viewer	1.12.0+dfsg-4igel1648284944
VMware Horizon Client	2303-8.9.0-21435420
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.3
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.1.0.37
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5

Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1667897461
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.9-1igel1677589353
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.12
OpenSSL	1.1.1-1ubuntu2.1~18.04.22
OpenSSH Client	9.0p1-1+b1igel1661867805
OpenSSH Server	9.0p1-1+b1igel1661867805
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891

Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos-g1681319724
Xorg X11 Server	21.1.7-2igel1680497175
Xorg Xephyr	21.1.7-2igel1680497175
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.625
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.4
NetworkManager	1.32.12-0ubuntu1igel1672314294
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1

GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.38.5-1igel1676531358
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu Guest Agent	7.2+dfsg-6igel1683015333

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	35.5 M	Included

Citrix Appliance Citrix Workspace app Citrix StoreFront	481.0 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	84.2 M	Included
VMware Horizon RDP	6.2 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	21.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	187.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.8 M	Not included
Imprivata Appliance	14.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	68.8 M	Included
PrinterLogic	43.5 M	Not included

Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	22.2 M	Not included
AVD	133.0 M	Included
Local Browser (Chromium)	144.2 M	Not included
Amazon WorkSpaces Client	32.8 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	99.0 M	Not included
Cisco Webex Meetings VDI	177.2 M	Not included
Zoom Media Plugin	164.5 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	1.5 M	Included
LRS Output Management	256.0 K	Included
Fluendo Browser Codec Plugins	9.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	2.0 M	Included
HP Anyware Client	18.8 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included

VirtualBox (Limited support)	66.8 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	34.8 M	Included

Known Issues 11.08.330

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser Content Redirection** (BCR) does not work if **DRI3** and **hardware-accelerated H.264 deep compression codec** are **enabled**.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- When starting Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**.
  A **cache cleanup with a reboot** is needed. In addition, the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

- **Logoff of Self-Service causes a segfault with CWAL 2211** which ends the application. The restart of Self-Service is functional.
- **Browser Content Redirection (BCR)** may not work with **Chrome** version **105.0.*** or later.
- **White/ green fragments** may appear during desktop launch if **JPEG graphical codec** is used.
  -There may be problems with **webcam redirection at Citrix**. To fix the problem, **GStreamer 1.0** must be enabled - this can be done either via the registry for the session or by enabling the browser content redirection (BCR).

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: **Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.
- **Scanning images** within an AVD session (with the usage of FabulaTech Scanner Redirection) **might fail and cause a reconnection** if the compression level is set to high quality.
  As a **workaround**, the **compression level must be reduced**.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this

bug.
The respective settings can be found in the IGEL Registry:
`vmware.view.enable-serial-port-redir`
`vmware.view.enable-scanner-redir`

- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.
- **Multimedia playback** in Firefox is **unstable if GStreamer version 0.10 is active**. The default GStreamer version for Firefox `sessions.browser\<inst>.gstreamer_version` was set to 1.0.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.
- **Set of credentials for manual system-wide proxy** is **broken**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[267] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

267. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.
- **Wake-up from suspend via UMS** does not work on **HP mt645 devices**. **Workaround**: **Disable system suspend** and **use shutdown** instead.
- **System suspend** is not supported on **Lenovo L14 Gen 3 Intel**-based device.
- If **bluetooth** is disabled via tray icon / menu on **Lenovo L14 Gen3 (Intel-based)**, bluetooth tray icon is permanently disabled. Can be solved / re-enabeld with console command `rfkill unblock bluetooth`

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Fabulatech

- **Scanning images within an AVD session** (with the usage of **FabulaTech Scanner Redirection**) might fail and cause a reconnection if the compression level is set to high quality.
  As a **workaround**, the **compression level must be reduced.**

Security Fixes 11.08.330

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2023-1236, CVE-2023-1235, CVE-2023-1234, CVE-2023-1233,
  CVE-2023-1232, CVE-2023-1231, CVE-2023-1230, CVE-2023-1229,
  CVE-2023-1228, CVE-2023-1227, CVE-2023-1226, CVE-2023-1225,
  CVE-2023-1224, CVE-2023-1223, CVE-2023-1222, CVE-2023-1221,
  CVE-2023-1220, CVE-2023-1219, CVE-2023-1218, CVE-2023-1217,
  CVE-2023-1216, CVE-2023-1215, CVE-2023-1214, and CVE-2023-1213
- Fixed Chromium browser security issues:
  More...

  CVE-2023-2137, CVE-2023-2136, CVE-2023-2135, CVE-2023-2134,
  CVE-2023-2133, CVE-2023-2033, CVE-2023-1534, CVE-2023-1533,
  CVE-2023-1532, CVE-2023-1531, CVE-2023-1530, CVE-2023-1529,
  CVE-2023-1528, CVE-2022-2136, and CVE-2022-2033
- Updated **Chromium** browser to version **112.0.5615.165**

Firefox

- Updated **Mozilla Firefo**x to version **102.10.0 ESR**
  Security fixes for **mfsa2023-14**, also known as:
  CVE-2023-29533, CVE-2023-29535, CVE-2023-29536, CVE-2023-29539,
  CVE-2023-29541, CVE-2023-1945, CVE-2023-29548, CVE-2023-29550

  Security fixes for **mfsa2023-10**, also known as:
  CVE-2023-25751, CVE-2023-28164, CVE-2023-28162, CVE-2023-25752, and CVE-2023-28176.

Base System

- Updated **Intel-microcode** from 20221108 **to 20230214** version for solving relevant security issues.
- Fixed **sudo** security issues CVE-2023-28487, CVE-2023-28486, and CVE-2023-2848.
- Fixed **vim** security issues:
  More...

  CVE-2023-1175, CVE-2023-1170, CVE-2023-0433,
  CVE-2023-0288, CVE-2023-0054, CVE-2023-0049, CVE-2022-47024, CVE-2022-2946,
  CVE-2022-2923, CVE-2022-2849, CVE-2022-2845, CVE-2022-2581, CVE-2022-2571,
  CVE-2022-2345, CVE-2022-2304, CVE-2022-2206, CVE-2022-2183, CVE-2022-2175,
  CVE-2022-2129, CVE-2022-2126, CVE-2022-2125, CVE-2022-2124, CVE-2022-1968,
  CVE-2022-1942, CVE-2022-1898, CVE-2022-1851, CVE-2022-1796, CVE-2022-1785,
  CVE-2022-1735, CVE-2022-1733, CVE-2022-1720, CVE-2022-1674, CVE-2022-1629, and CVE-2022-0413.

- Fixed **bubblewrap** security issue CVE-2021-41133.
- Fixed **heimdal** security issue CVE-2022-45142.
- Fixed **xorg-server** security issue CVE-2023-1393.
- Fixed **ghostscript** security issue CVE-2023-28879.
- Fixed **protobuf** security issues CVE-2022-1941 and CVE-2021-22570.
- Fixed **python2.7** security issue CVE-2023-24329.
- Fixed **python3.6** security issue CVE-2023-24329.
- Fixed **zulu8-ca** security issues:
  More...

  CVE-2023-21930, CVE-2023-21937, CVE-2023-21938,
  CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, and CVE-2023-21968
- Fixed **systemd** security issues CVE-2022-3821 and CVE-2022-4415.
- Fixed **openssl1.0** security issues CVE-2023-0466, CVE-2023-0465, and CVE-2023-0464.
- Fixed **openssl** security issues CVE-2023-0466, CVE-2023-0465, and CVE-2023-0464.
- Fixed **gnutls28** security issue CVE-2023-0361.
- Fixed **qemu** security issue CVE-2022-1050.
- Fixed **ffmpeg** security issues CVE-2022-48434, CVE-2022-3964, CVE-2022-3341, and CVE-2022-3109.

New Features 11.08.330

Citrix

- Integrated **Citrix Workspace App 2303**
  Available Workspace Apps in this release: **2303 (default)**, **2302**, and **2010**
- New features:
  - **Inactivity Timeout for Citrix Workspace app**

Parameter	Inactivity Timeout for Citrix Workspace app
Registry	`ica.authman.itoenabled`
Value	false / true

  - **Background blurring for webcam redirection**

Parameter	Background blurring for webcam redirection
Registry	`ica.wfclient.HDXWebCamEnableBackgndEffect`
Value	false / true

  - Integrated **RTME 2.9.600 for Skype for Business**

AVD

- Updated **IGEL AVD client** to version **1.1.17**
- Added: **Cache of last entered username for AVD sessions** if no other username preset is active.
- Added **parameter to disable the username cache**:

Registry	`sessions.wvd%.options.cache-username`
Value	enabled / disabled

VMware Horizon

- Updated **Horizon client** to version **2303-8.9.0-21435420**
- Added parameter for the **browser redirection** feature and **setting rtav-related audio out option**: **More...**

Parameter	Browser Redirection
Registry	`vmware.view.html5mmrbcr.enable-bcr`
Type	bool

Value	enabled / disabled

Parameter	Allow client webcam in Browser Redirection
Registry	`vmware.view.html5mmrbcr.media-stream-enabled`
Type	bool
Value	enabled / disabled

Parameter	Ignore website's certificate errors
Registry	`vmware.view.html5mmrbcr.ignore-certs`
Type	bool
Value	enabled / disabled

Parameter	Save Cookies for Browser Redirection
Registry	`vmware.view.html5mmrbcr.use-cache-enabled`
Type	bool
Value	enabled / disabled

Parameter	Select audio output devices
Registry	`vmware.view.audio-out-option`
Range	[Default] [All] [User selection]

Chromium

- Updated **Chromium** browser to version **112.0.5615.165**

Firefox

- Updated Mozilla **Firefox** to version **102.10.0 esr**

Wi-Fi

- Added **iwlwifi backport Wi-Fi driver** which can be used if issues with Intel Wi-Fi devices occur.
- Added registry key (reboot is required to become effective):

Parameter	Use the newer backport drivers for WLAN.
Registry	`network.drivers.use_backport_drivers`
Type	bool

Value	enabled / disabled

Smartcard

- Updated **Pointsharp (formerly SecMaker) Net iD Client** to version **1.1.0.37**.

CUPS Printing

- Added **LRS printing agent V1R1.0.000**
- Corresponding **configuration** options in the Setup - **Devices > Printing > LRS**:
  More...

Parameter	Custom path to LRS software
Registry	`LRS.custom_path`
Type	string
Value	empty
Parameter	Manage printers by LRS VPSA
Registry	`LRS.active`
Type	bool
Value	enabled / disabled

Parameter	Debug mode
Registry	`LRS.debug_mode`
Type	bool
Value	enabled / disabled

Parameter	Pass Username to the LRS Backend
Registry	`LRS.pass_username`
Type	bool
Value	enabled / disabled

Parameter	Username Format
Registry	`LRS.username_format`
Range	[Username] [Domain\Username] [Username@Domain]

Parameter	Cups printer model name for local printing
Registry	`LRS.cups_model`
Type	string
Value	Generic Raw Queue

Parameter	Driver name used in remote Windows session
Registry	`LRS.windows_driver`
Type	string
Value	MS Publisher Color Printer

Parameter	VSPA URL
Registry	`LRS.homeurl`
Type	string
Value	http://replace.me.server/lrs/nlrswc2.exe/vpsx

Parameter	ICA Sessions
Registry	`LRS.map_ica`
Type	bool
Value	enabled / disabled

Parameter	RDP Sessions
Registry	`LRS.map_rdp`
Type	bool
Value	enabled / disabled

Parameter	Parallels Sessions
Registry	`LRS.map_twox`
Type	bool
Value	enabled / disabled

Parameter	NX Client Sessions
Registry	`LRS.map_nxclient`
Type	bool

Value	enabled / disabled

Parameter	LRS Output Management
Registry	`services.printing_lrs.enabled`
Type	bool
Value	enabled / disabled

Cisco Webex

- Integrated **Cisco Webex VDI 43.4.0.25788**

Base System

- Added **Canadian Multilingual Standard keyboard layout**.
- Added **BIOS update and password management support for HP t540 and t640**. How-to guide via https://wiki.test.toolchain.igel.kreuzwerker.net/hp-ami-bios, added parameters:
  More...

Setup	**System > Firmware Customization > Features**
Parameter	BIOS Tools
Registry	`services.bios_tools.enabled`
Value	enabled / disabled

Registry	`fwtools.bios_tools.bios_update_file`
Value	empty

Registry	`fwtools.bios_tools.bios_settings_set_file`
Value	empty

Registry	`fwtools.bios_tools.bios_settings_get_file`
Value	empty

Registry	`fwtools.bios_tools.bios_pwd_file`
Value	empty

Registry	`fwtools.bios_tools.bios_pwd_file_old`
Value	empty

Registry	`fwtools.bios_tools.bios_download_username`
Value	empty
Registry	`fwtools.bios_tools.bios_download_crypt_password`
Value	empty

Driver

- Updated **Olympus driver for dictation** to version **4.0.3**.

Audio

- Updated **EPOS Connect** to version **7.4**

Hardware

- Added hardware support for **Lenovo ThinkPad L14 Gen3 (Intel)** - integrated **LTE is not supported yet**.
- Added hardware support for **HP Elite mt645 G7**, **includes WWAN Intel XMM 7560 R+**
- Added hardware support for **LG CQ600i-6N**.
- Added hardware support for **LG 24CQ650i-6N**.
- Added hardware support for **HP t550**.

Remote Management

- Remote management **evaluates an HTTP cookie** which is propagated to the device during the ICG handshake and uses this cookie in all HTTP and WebSocket connections belonging to the established ICG connection. This enables the load balancing mechanism involving an affinity HTTP cookie to relate device's HTTP and WebSocket requests to a particular ICG connection.
- Upgraded **libwebsockets** to **v4.1.6**
- IGEL remote manager agent exposes in all **ICG connections and HTTP(s) requests** the **User-Agent HTTP header** in the form: `igel-rmagent/\<RMAGENTVERSION>`

Fabulatech

- Updated **Fabulatech** plugins to version **3.10.0.9**

Resolved Issues 11.08.330

AVD

- Fixed **MS-Teams video color issue**s for remote video feeds and screenshares.
- Optimized **h.264 encoder settings for MS-Teams VDI calls**.
- Added a registry parameter to **change the x264enc speed-preset property** used **for MS-Teams VDI**:

Registry	`sessions.wvd%.options.webrtcencoderpreset`
Value	[none] [ultrafast] [superfast] [veryfast] [faster] [fast] [medium] [slow] [slower] [veryslow] [placebo]

- **Removed smartcard option** until smartcard support is stabilized. **Smartcard redirection** can still be enabled by setting `sessions.wvd%.options.cmd_ext = --smartcard`

RDP/IGEL RDP Client 2

- Fixed RDP **sessions not starting on configured monitor**.
- Fixed RDP **sessions no longer starting on multiple monitors when using different resolutions**.
- Fixed **cursor position** not updated correctly in RDP sessions.

Firefox

- Fixed browser **startup behavior if multiple browser sessions are started**. As example, different autostarted browser sessions on different monitors.
  For that browser's remote interface is required to start the next session which takes time on slow endpoints.
  A configurable timeout is implemented:

Parameter	Timeout for starting next browser session
Registry	`browserglobal.app.startup-timeout`
Range	[0][2][4][6][8][10][12][14][16][18][20]
Value	0

- Fixed **usage of more than one Firefox session**. This was prevented by **app-armor** lacking an additional exception for Firefox 102 ESR.
- Fixed **handling of ica files** - required to start Citrix sessions (restored former behavior).
- Fixed **typo in browser start script** which could corrupt URL in some cases.

Network

- Fixed: Set third-party **r8125 as the default driver on Lenovo L14 Gen 3** (Intel-based)

- Added new registry key to **prefer** third-party **r8125 over r8169** network driver.

Parameter	Use thirdparty r8125 kernel module.
Registry	`network.drivers.r8169.prefer_r8125`
Range	[Auto] [Yes] [No]

- Fixed tray icon for **Fibocom L860-GL-16 LTE Module**
- SCEP:
  - Fixed **SCEP via proxy**
  - **Added separator definition** to use if multiple values of distinguished name attributes are desired, e.g. multiple organizational units. The separator also affects organization, state, locality, and potentially more in the future.

Parameter	Name separator
Registry	`network.scepclient.cert%.multivalueseparator`
Range	[<none>]
Value	<none>

Wi-Fi

- Fixed: **Wi-Fi IP setting changes** become **effective immediately** now.

Base System

- Fixed **serial port support for TSharc touch devices**.
- Added new registry key:

Parameter	Set serial interface for TSharc touch (None for USB device).
Registry	`userinterface.touchscreen.tsharc_serial_device`
Range	[None] [COM1] [COM2] [COM3][COM4] [COM1 (USB)] [COM2 (USB)]
Value	None

- Fixed **missing node actions for changing Device Encryption** settings
- **Disabled suspend support on Intel-based Lenovo L14 Gen 3** as it does not work currently.
- Fixed handling of **certificate files in PEM format** which do not include a final newline character.

Custom Partition

- Fixed: **Creating or updating a custom partition is decoupled from the partition's mounting** so that the creating process doesn't interrupt the boot process and runs in the background now. This fixes problems with premature abort while creating the custom partition by a timeout during boot.

X11 System

- Fixed **out-of-range issue for NEC EA223WM monitors**.
- Added **quirk for DisplayLink** leads to **long Xorg start** on boot.
- Added new registry key `x.xserver0.quirks.displaylink_crash_workaround`

Parameter	Quirk to fix issues with Xorg start take ages with DisplayLink connected.
Registry	`x.xserver0.quirks.displaylink_crash_workaround`
Type	bool
Value	enabled / disabled

VNC Viewer

- Added VNC viewer parameter to **control if current or all monitors are used when switching to full-screen mode**.

Parameter	Use all monitors in full-screen mode
Registry	`sessions.vncviewer<num>.option.fullscreenallmonitors`
Value	disabled / enabled

Remote Management

- **IGEL remote management reacts now on every change among the all available network interfaces** in the running IGEL OS. So if a network interface becomes online or offline, then the remote management tries to connect the UMS or the ICG server.

Notes for Release 11.08.290

Software:	Version	11.08.290
Release Date:	2023-03-30	
Release Notes:	Version	RN-1108290-1
Last update:	2023-03-30	

- Supported Devices 11.08.290 (see page 2716)
- Component Versions 11.08.290 (see page 2717)
- Known Issues 11.08.290 (see page 2726)
- Security Fixes 11.08.290 (see page 2731)
- New Features 11.08.290 (see page 2733)
- Resolved Issues 11.08.290 (see page 2739)

The Release Notes for IGEL OS 11.08.290 are also available in the following formats:

- Plain text: readme_11.08.290.txt

Supported Devices 11.08.290

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[268].

268. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.290

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	110.0.5481.177-igel1677133876
Cisco JVDI Client	14.1.3
Cisco Webex VDI plugin	43.2.0.25211
Cisco Webex Meetings VDI plugin	42.10.8.14
Cisco Webex Meetings VDI plugin	42.6.11.6
Cisco Webex Meetings VDI plugin	43.2.1.18
Zoom Media Plugin	5.12.6.22200
Zoom Media Plugin	5.13.10.23090
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.11.0.19
Citrix Workspace App	23.02.0.10
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.2.2.42489
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.1.2.9
FabulaTech Scanner for Remote Desktop	3.0.1.0
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	102.8.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1679036889
IGEL AVD Client	1.1.12igel1677413961
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-generic-bootstrap-loader_7.11.0.665541_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.6.0~git20220818-1igel1661859138
Zulu JRE	8.0.362-3
Parallels Client	19.1.1.23476
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.2-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	23.01.1-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-4igel1648284944

VMware Horizon Client	2212-8.8.0-21079016
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24

Reader Driver MUSCLE CCID	1.5.0-2igel1667897461
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.9-1igel1677589353
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.11
OpenSSL	1.1.1-1ubuntu2.1~18.04.21
OpenSSH Client	9.0p1-1+b1igel1661867805
OpenSSH Server	9.0p1-1+b1igel1661867805
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980

Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos-g1677144800
Xorg X11 Server	21.1.7-1igel1677744226
Xorg Xephyr	21.1.7-1igel1677744226
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.625
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.4
NetworkManager	1.32.12-0ubuntu1igel1672314294
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.4
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2

GStreamer 1.0 Fluendo wmadec	1.0.1
GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.38.5-1igel1676531358
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu Guest Agent	7.2+dfsg-1+b2igel1673334696

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	35.5 M	Included

Citrix Appliance Citrix Workspace app Citrix StoreFront	326.2M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	83.2 M	Included
VMware Horizon RDP	6.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	21.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	270.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.8 M	Not included
Imprivata Appliance	14.8 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	68.8 M	Included
PrinterLogic	43.5 M	Not included

Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	5.5 M	Not included
Elastic Filebeat	22.2 M	Not included
AVD	132.0 M	Included
Local Browser (Chromium)	106.0 M	Not included
Amazon WorkSpaces Client	32.8 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	102.2 M	Not included
Cisco Webex Meetings VDI	177.2 M	Not included
Zoom Media Plugin	164.5 M	Not included
DriveLock	13.0 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	1.5 M	Included
Fluendo Browser Codec Plugins	9.5 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	256.0 K	Included
HP Anyware Client	18.8 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	66.8 M	Not included

Virtual Background for Webcam (Limited IGEL Support)	34.8 M	Included

Known Issues 11.08.290

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- When starting Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**.
  A **cache cleanup with a reboot** is needed. In addition, the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

- **Logoff of Self-Service causes a segfault with CWAL 2211** which ends the application. The restart of Self-Service is functional.
- **Browser Content Redirection (BCR)** may not work with **Chrome** version **105.0.*** or later.
- When the **Jpeg graphical codec is in use**, **white/ green fragments** may appear **during the desktop launch**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: **Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`

- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.
- **Multimedia playback** in Firefox is **unstable if GStreamer version 0.10 is active**. The default GStreamer version for Firefox `sessions.browser\<inst>.gstreamer_version` was set to 1.0.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.
- **Set of credentials for manual system-wide proxy** is **broken**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[269] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.

269. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.
- **Wake-up from suspend via UMS** does not work on **HP mt645 devices**. **Workaround**: **Disable system suspend** and **use shutdown** instead.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.08.290

Chromium

- Fixed **forbidden file access**. If enabled, downloads, bookmarks and printing in Chromium are disabled.
- Fixed Chromium browser **security issues**
  More...

  CVE-2023-0941, CVE-2023-0933,
  CVE-2023-0932, CVE-2023-0931, CVE-2023-0930, CVE-2023-0929, CVE-2023-0928,
  CVE-2023-0927, CVE-2023-0705, CVE-2023-0704, CVE-2023-0703, CVE-2023-0702,
  CVE-2023-0701, CVE-2023-0700, CVE-2023-0699, CVE-2023-0698, CVE-2023-0697,
  CVE-2023-0696, CVE-2023-0474, CVE-2023-0473, CVE-2023-0472, CVE-2023-0471,
  CVE-2023-0141, CVE-2023-0140, CVE-2023-0139, CVE-2023-0138, CVE-2023-0137,
  CVE-2023-0136, CVE-2023-0135, CVE-2023-0134, CVE-2023-0133, CVE-2023-0132,
  CVE-2023-0131, CVE-2023-0130, CVE-2023-0129, CVE-2023-0128, CVE-2022-4440,
  CVE-2022-4439, CVE-2022-4438, CVE-2022-4437, and CVE-2022-4436
- Updated **Chromium** browser to **version 110.0.5481.177**.

Network

- Fixed **privilege escalation** in network management.

Base System

- Fixed **privilege escalation** in `setup_cmd` tool.
  Changed: For security reasons, the **default password protection value for the System Information** accessory **is** set to **Administrator**.

IGEL Setup	Accessories > System Information
Parameter	Password protection
Registry	`sessions.device_manager0.pwprotected`
Value	Administrator (default)

- Fixed **empty password** entry for **floppy group**.
- Fixed **sysstat** security issue CVE-2022-39377.
- Fixed **binutils** security issue CVE-2022-38533.
- Fixed **libarchive** security issues CVE-2022-36227 and CVE-2022-28066.
- Fixed **curl** security issues
  More...

  CVE-2023-23916, CVE-2023-23915, CVE-2023-23914, CVE-2022-43552,
  CVE-2022-43551, CVE-2022-42916, CVE-2022-42915, CVE-2022-35260, and CVE-2022-32221

- Fixed **xorg-server** security issues CVE-2022-46344, CVE-2022-46343, CVE-2022-46342, CVE-2022-46341, CVE-2022-46340, and CVE-2022-46283.
- Fixed **libksba** security issue CVE-2022-47629.
- Fixed **nautilus** security issue CVE-2022-37290.
- Fixed **python2.7** security issue CVE-2022-45061.
- Fixed **python3.6** security issue CVE-2022-45061.
- Fixed **net-snmp** security issues CVE-2022-44793, CVE-2022-44792, and CVE-2022-4479.
- Fixed **tiff** security issue CVE-2022-3970.
- Fixed **webkit2gtk** security issues
  More...

  CVE-2023-23518, CVE-2023-23517, CVE-2022-42826, CVE-2022-46700, CVE-2022-46699, CVE-2022-46698, CVE-2022-46692, CVE-2022-46691, CVE-2022-42867, CVE-2022-42863, CVE-2022-42856, and CVE-2022-42852
- Fixed **qemu** security issues CVE-2022-4172 and CVE-2022-3165.
- Fixed **vim** security issue CVE-2022-0392.
- Fixed **sudo** security issue CVE-2023-22809.
- Fixed **libxpm** security issues CVE-2022-4883, CVE-2022-46285, and CVE-2022-44617.
- Fixed **zulu8-ca** security issues CVE-2023-21830, CVE-2023-21835, and CVE-2023-21843.
- Fixed **heimdal** security issues CVE-2022-45142, CVE-2022-44640, CVE-2022-42898, CVE-2022-41916, CVE-2022-3437, and CVE-2021-44758.
- Fixed **python-setuptools** security issue CVE-2022-40897.
- Fixed **pam** security issue CVE-2022-28321.
- Fixed **mysql-5.7** security issue CVE-2023-21840.
- Fixed **xorg-server** security issue CVE-2023-0494.
- Fixed **e2fsprogs** security issue CVE-2022-1304.
- Fixed **openssl1.0** security issues CVE-2023-0286 and CVE-2023-0215.
- Fixed **openssl** security issues CVE-2023-0286, CVE-2023-0215, CVE-2022-4450, and CVE-2022-4304.
- Fixed **tpm2-tss** security issue CVE-2023-22745.
- Fixed **nss** security issue CVE-2023-0767.
- Fixed **python3.6** security issue CVE-2022-37454.
- Fixed **tiff** security issues
  More...

  CVE-2023-0804, CVE-2023-0803, CVE-2023-0802, CVE-2023-0801, CVE-2023-0800, CVE-2023-0799, CVE-2023-0798, CVE-2023-0797, CVE-2023-0796, and CVE-2023-0795
- Fixed **rsync** security issue CVE-2022-29154.
- Fixed **tar** security issue CVE-2022-48303.
- Updated **ca-certificates** to version 20230311.

New Features 11.08.290

Citrix

- Added Citrix Workspace App 2302.
- New features:
- **Screen pinning** in custom web stores **[Technical Preview]**

Parameter	Multi-monitor support
Registry	`ica.authman.screenpinenabled`
Value	disabled / enabled

- Available **Citrix Workspace apps**: **23.02** (default), **22.11**, and **20.10**

Citrix NSGClient

- Added **Citrix EPA client** for **Netscaler analysis**.
  No configuration is necessary. When the Netscaler URL is opened in the browser (Chromium or Firefox), the NSEPA checks configured in Netscaler are performed automatically.
  Dynamic updates are not possible in IGEL OS, due to the read-only system. Therefore, the **option "Linux EPA Plugin Upgrade" must be set to "Never" in Netscaler**.
- Added **Citrix NSGClient client for Netscaler VPN connections**.
  No configuration is necessary. When the Netscaler URL is called in the browser (Chromium or Firefox), the NSGClient is configured automatically. Additionally, a desktop icon can be configured by adding an instance of `sessions.nsgclient%`

AVD

- Updated **AVD** client to **version 1.1.12** with **MS-Teams screen share** and **tcp buffer bump fixes**.

VMware Horizon

- Updated **VMware Horizon** client to **version 2212-8.8.0-21079016**.
- Fixed **vmware-view protocol handler** used for federated (SAML-based) authentication.
- Added support for the monitor's option to specify **which monitors (and in what order) are to be used for an all-monitors fullscreen mode**.
  Furthermore, added **minimized launch of the client window** and the use of the `useExisting` option for letting the client use an already running client to start a new desktop or app session.
  More...

Parameter	Specify a list of monitor numbers you want to use in all-monitors fullscreen mode

Registry	`vmware.view.use-monitors`
Type	string
Value	empty (default)
Parameter	Specify a list of monitor numbers you want to use in all-monitors fullscreen mode
Registry	`sessions.vdm_client%.options.use-monitors`
Type	string
Value	empty (default)

Parameter	Use an already running Horizon session to start apps or desktops
Registry	`vmware.view.use-existing`
Range	[on] [off]

Parameter	Use an already running Horizon session to start apps or desktops
Registry	`sessions.vdm_client%.options.use-existing`
Range	[Global setting] [on] [off]

Parameter	Run Horizon client in minimized mode
Registry	`vmware.view.launch-minimized`
Range	[on] [off]

Parameter	Run Horizon client in minimized mode
Registry	`sessions.vdm_client%.options.launch-minimized`
Range	[Global setting] [on] [off]

Parallels Client

- Updated **Parallels** client to **version 19.1.1**.

HP Anyware

- Updated **HP Anyware PCoIP Software Client** to version **23.01.1**
- Added a new parameter in the registry for enabling high-performance options:
  More...

Parameter	Enable high performance on endpoint
Registry	`pcoip.high_performance`
Type	bool
Value	enabled / disabled

Parameter	Enable PCoIP Ultra on host
Registry	`pcoip.ultra`
Range	[Off] [CPU Offload] [GPU Offload] [Auto]

Firefox

- Updated **Firefox** to version **102.8.0**.

Network

- Added **check if BIOS has Wake-on-LAN disabled**. If disabled, it is not recommended to configure the network interface to use WoL.
  - Registry key:

Parameter	Respect the BIOS WoL setting so if disabled reflect this for the linux network devices settings.
Registry	`network.interfaces.respect_bios_wol_setting`
Type	bool
Value	enabled / disabled

- This check is only **supported / possible on Lenovo devices with official IGEL OS hardware support**.

Wi-Fi

- Added: Set **default wireless regulatory domain on HP devices**, based on product option code.

HID

- **Changed** touchpad parameter **name** from "**Enable Touchpad**" to "**Enable Touchpad on Boot**" - just to clarify what is meant here.

Setup	**User Interface > Input > Touchpad**
Parameter	Enable Touchpad on Boot

Setup	User Interface > Input > Touchpad
Tooltip	Can be overruled by Hotkey.
Registry	`userinterface.touchpad.general.TouchpadEnable`
Type	bool
Value	enabled / disabled

- Furthermore, **changed the function** of `TouchpadOff` registry key. This is **now only used for switching on and off tapping**.

Setup	User Interface > Input > Touchpad
Parameter	Tapping Mode
Registry	`userinterface.touchpad.general.TouchpadOff`
Range	[With tapping] [Without tapping]

CUPS Printing

- Updated **PrinterLogic (Vasion) PrinterInstallerClient** to version **25.1.0.625**

Cisco Webex

- Integrated **Cisco Webex VDI 43.2**

  Note: Webex VDI requires a compatible Webex Meetings plugin installed in the client.

- Integrated **Cisco Webex Meetings VDI Plugin 43.2.1.18**
  Available **Webex Meetings Plugins** in this release: **43.2.1.18** (default), **42.10.8.14**; and **42.6.11.6**

Cisco JVDI Client

- Integrated **Cisco JVDI 14.1.3.307560**

Base System

- Updated **sscep to version 0.10.0**
- Added **CPU temperature monitoring tools**:
  Graphical tool `/usr/bin/psensor`
  Command line tool `/usr/bin/sensors`
- **Changed the default mem sleep mode** to deep as some devices defaults to `s2idle` which cases issues.
- Added a new registry key to set the suspend mem sleep mode.

Parameter	Set suspend mem sleep mode.
Registry	`system.suspend.sleep_mode`
Range	[Suspend to RAM] [Suspend to idle]

- Updated **DriveLock Agent** to version **22.2.2.42489 (2022.2)**.
- Added for **LVFS BIOS update** support:
  - **Improved version detection of installed BIOS** version with `fwupd`.
  - Added registry key for **enabling installation of not signed BIOS files**

Parameter	Allow only signed cab files (sometimes this must be switched off as not all BIOS files are signed).
Registry	`fwtools.bios_tools.allow_only_trusted`
Type	bool
Value	enabled / disabled

  - Added registry key to **enable bluetooth debugging messages**.

Parameter	Activate bluetooth debugging.
Registry	`devices.bluetooth.debug`
Type	bool
Value	enabled / disabled

CID Key Agent

- Update of **Stratusphere Connector ID Key to version 6.6.2-3**

X11 System

- Added new registry key to activate **tear-free for modesetting driver**:

Parameter	Enable tear free option for modesetting driver
Registry	`x.drivers.modesetting.use_tear_free`
Type	bool
Value	enabled / disabled

Multimedia

- Added **VP9 video hardware acceleration**.

- Added new registry key to **switch from fluendo to vaapi gstreamer plugin for h264 hardware acceleration**.

Parameter	Switch from Fluendo to VAAPI h264 hardware accelerated decoder.
Registry	`multimedia.gstreamer.use_vaapi_for_h264`
Type	bool
Value	enabled / disabled

zoomvdi

- Updated Zoom VDI plugin to version **5.13.10.23090**
  Available Zoom VDI plugins in this release: **5.13.10.23090** (default), **5.12.6.22200**, and **5.8.4.21112**

Hardware

- Added hardware support for **HP USB-C G5 ESSENTIAL DOCK**
- Added hardware support for **Lenovo ThinkCentre Neo50q Gen 4 (Celeron)** device.
- Added hardware support for **Lenovo ThinkCentre Neo50q Gen 4 (i3)** device.
- Added hardware support for **Lenovo ThinkCentre M75q Gen 2** device.
- Added hardware support for **Lenovo K14 Gen 1 (AMD-based)** device.
- Added hardware support for **Lenovo ThinkCentre M70q Gen 3** device.
- Added hardware support for **HP t740**.
- Added hardware support for **Lenovo K14 Gen1 (INTEL)** device.

TC Setup (Java)

- Added **usage of long(er) device names - with port name in Audio Setup now**. This affects "**Default Sound Output**" and "**Default Sound Input**" configuration at the Setup page **Accessories > Sound Preferences > Options**. The change is backwards-compatible.

Fabulatech

- Updated **Fabulatech USB for Remote Desktop version 6.1.2.9**

Resolved Issues 11.08.290

Citrix

- Fixed **H264 codec**: When the server was configured to update only regions which have changed, sometimes **massive glitches in the shape of green rectangles** appeared.
- Fixed: Expired DigiCertSHA2SecureServerCA certificate was **replaced with a valid one**.

RDP/IGEL RDP Client 2

- Fixed **RDP fullscreen-toggle** not working when trying to switch from fullscreen to windowed mode.

AVD

- Fixed **MS Teams optimized video playback** to not slow down on high CPU load.
- Fixed **percentage (%) window size settings**.
- Fixed **workarea session window size**.
- Fixed **multimonitor switching during the session**.
- Supports all kinds of **multimonitor constellations**.
- **MS Teams optimization stability** fixes.
- Fixed **Zoom VDI support for multimonitor**.
- Fixed **video encoder buffer queuing up endlessly and crashing the client** when it runs out of memory. Instead, we drop webcam frames when the CPU cannot catch up with encoding.
- Fixed **MS Teams screen share on multimonitor**.
- Fixed s**ession size preset to take effect when not multimonitor**.
- Added f**ixes from the latest RdClientSDK including the TCP buffer bump** to avoid unwanted client session dis-/reconnections.

NX Client

- The value of `sessions.nxclient%.general.commandline` is **not converted to lowercase** anymore when being written to a session config file

Chromium

- Fixed **Chromium** browser **could not be restarted after closing it too quickly**.
- Fixed **ClearBrowsingDataOnExitList policy** for Chromium browser.
- Fixed **Chromium** browser **not starting if persistent partition was missing**.

Firefox

- Mozilla **Firefox 102 ESR starting Citrix Desktops**, **requires an ica file** to start sessions.

- In normal browser session, the following parameter must be disabled: **Sessions > Firefox Browser > Firefox Browser Global > Security > Hide local filesystem**
- If **browser appliance mode** is used, it is required to activate the following:

Parameter	File system access needed for ica file handling
Registry	`browserglobal.app.ica-file-access-needed`
Type	bool
Value	enabled / disabled

- Fixed Registry parameter `sessions.browser\<instance>.gstreamer_version`: **If set to 1.0 via setup, 0.10 was activated and vice versa**.

Network

- Added registry key for choosing the base of decisions regarding **automatically switching on and off enabling Wi-Fi carrier**: either completed IP configuration of an Ethernet interface (default, traditional implementation) or just Ethernet carrier. The new key has no effect if `network.applet.wireless.enable_wifi_auto_switch` is false.

Parameter	Enable Wi-Fi automatic switch on Ethernet carrier change
Registry	`network.applet.wireless.enable_wifi_auto_switch_on_carrier`
Type	bool
Value	enabled / disabled

- Fixed **set of 100Mbps ethernet modes**.
- Improved **reliability of Ethernet** configuration on **IGEL D220** devices.
- Fixed **disabling of WoL** - which was not applied without a reboot.

Wi-Fi

- Fixed: **System regulatory domain** now also set on the self-managed **driver rtl8852be**
- Fixed **default wireless regulatory domain for HP devices delivered to Indonesia** - by detecting the HP option code.
- Fixed: **HP Probook 450 G8** with Intel AX201 Wi-Fi.
- Improved finding **hidden SSIDs with MT7922 WLAN adapter** (e.g. in Lenovo ThinkPad L14 Gen 3)
- Improved restoration of Wi-Fi `rfkill` state on startup

Imprivata

- Improved **error messages on PIN enrollment**.

Smartcard

- Fixed **cryptas TicTok v3 smartcards** for usage within **Horizon** sessions.
- Fixed sporadic **duplicated smartcard user entries at login screen**.

Cisco Webex

- Integrated C**isco Webex Meetings VDI Plugin 42.6.11.6**

Base System

- Added new registry key to **set left-hand on touchpad devices**

Parameter	Left hand
Registry	`userinterface.touchpad.general.LeftHand`
Type	bool
Value	disabled (default)

- Fixed sporadic **delayed local logon when logon logging is enabled**.
- Fixed **German translation of "Enter new password"** in password change dialog of local login window.
- Fixed **Starter license** on devices with multiple network interfaces.
- Fixed **autostart notification**.
- Fixed **error message on login screen** in case Kerberos KDC (domain controller) is unreachable.
- Added **Fluendo h264 codec version 24012023**, which **fixes stability issues with AVD MS Teams optimization**.
- **Changed default** of registry key `devices.bluetooth.connect_only` **to true** to make connect after reboot for bluetooth the new default.

Parameter	Connect devices without pairing
Registry	`devices.bluetooth.connect_only`
Type	bool
Value	enabled / disabled

- Fixed **WoL BIOS setting detection for Lenovo M75q Gen 2**.
- Fixed "**fwupdmgr get-devices" command**.
- Fixed **disabling of the "BIOS Tools"** feature **on** the Setup page **System > Firmware Customization > Features**.
- Improved **Bluetooth auto connect**.

X11 System

- Fixed **monitor refresh rate handling in Display Switcher**.

- Fixed issue that **display switcher** settings were overwritten by UMS if network connection changed and the display switcher is still open.
- Added registry key to influence the **graphic card order in IGEL Setup**.

Parameter	Preserve card order in setup even if the X11 order of the cards was changed.
Registry	`x.drivers.preserve_order_if_swapped`
Type	bool
Value	enabled / disabled

- Changed **default X11 graphic driver** from **modesetting** to **intel** on **Dell Wyse 5070**.

Audio

- Added new registry key to **limit max headphone volume** (setting will survive a reset to factory defaults)

Parameter	Limit max headphone volume (use auto or 0 - 100 as values).
Registry	`multimedia.alsa.limit_headphone_volume`
Type	string
Value	auto (default)

- Fixed **audio output** on jack in **LG 24CN650N** device.

Hardware

- Fixed issue on specific **monitors stayed black after resume (DPMS off)**.

Notes for Release 11.08.230

Software:	Version	11.08.230
Release Date:	2022-12-13	
Release Notes:	Version	RN-1108230-1
Last update:	2022-12-13	

- Supported Devices 11.08.230 (see page 2744)
- Component Versions 11.08.230 (see page 2745)
- Known Issues 11.08.230 (see page 2753)
- Security Fixes 11.08.230 (see page 2758)
- New Features 11.08.230 (see page 2760)
- Resolved Issues 11.08.230 (see page 2763)

The Release Notes for IGEL OS 11.08.230 are also available in the following formats:

- Plain text: readme_11.08.230.txt

Supported Devices 11.08.230

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[270].

270. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.230

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	108.0.5359.94-igel1670091085
Cisco JVDI Client	14.1.2
Cisco Webex VDI plugin	42.10.0.23814
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.2.10.7
Cisco Webex Meetings VDI plugin	42.6.8.5
Zoom Media Plugin	5.11.2.21530
Zoom Media Plugin	5.12.1.21950
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.07.0.20
Citrix Workspace App	22.11.0.19
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	22.1.2.38801
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	3.0.1.0
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.13.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1663073494
IGEL AVD Client	1.1.6igel1670568183
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.6.0~git20220818-1igel1661859138
Zulu JRE	8.0.352-1
Parallels Client	19.1.0
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	22.07.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-4igel1648284944
VMware Horizon Client	2206-8.6.0-20094634

Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.5.20
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1667897461

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.8-1igel1655196158
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	9.0p1-1+b1igel1661867805
OpenSSH Server	9.0p1-1+b1igel1661867805
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0

Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos-g1666777173
Xorg X11 Server	21.1.4-3igel1668497029
Xorg Xephyr	21.1.4-3igel1668497029
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.4
NetworkManager	1.32.12-0ubuntu1igel1656495558
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.3
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1

GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.38.2-1igel1667805620
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu Guest Agent	7.1+dfsg-2igel1663754599

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	373.8 M	Included

Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	81.5 M	Included
VMware Horizon RDP	6.0 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	21.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	256.0 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.8 M	Not included
Imprivata Appliance	14.2 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	66.8 M	Included
PrinterLogic	47.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included

Stratusphere UX CID Key software	7.5 M	Not included
Elastic Filebeat	22.2 M	Not included
AVD	132.2 M	Included
Local Browser (Chromium)	103.8 M	Not included
Amazon WorkSpaces Client	32.8 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	69.0 M	Not included
Cisco Webex Meetings VDI	119.0 M	Not included
Zoom Media Plugin	127.8 M	Not included
DriveLock	12.8 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	1.5 M	Included
Fluendo Browser Codec Plugins	4.0 M	Included
HP Factory deployment documentation	88.5 M	Included
BIOS Tools	256.0 K	Included
HP Anyware Client	16.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	66.5 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	34.8 M	Included

Known Issues 11.08.230

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- When starting Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**.
  A **cache cleanup with a reboot** is needed. In addition, the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

- **Logoff of Self-Service causes a segfault with CWAL 2211** which ends the application. The restart of Self-Service is functional.
- **BCR may not work with Chrome** version **107.0.**. or later**.
- When the **Jpeg graphical codec is in use**, **white/ green fragments** may appear **during the desktop launch**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: **Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.
- For the case "`sessions.wvd%.options.workspace-1.enabled`" is explicitly set to "true", although there are no legacy WVD resources availabe for a certain user, **the workspace download (that happens after the Azure-AD login) will take 5 minutes before it actually comes back showing the available workspaces for the user**. This is an issue in the RdClientSDK and will be fixed in upcoming versions!

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this

bug.
The respective settings can be found in the IGEL Registry:
`vmware.view.enable-serial-port-redir`
`vmware.view.enable-scanner-redir`

- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.
- **Set of credentials for manual system-wide proxy** is **broken**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[271] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.

271. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.
- **Wake-up from suspend via UMS** does not work on **HP mt645 devices**. **Workaround**: **Disable system suspend** and **use shutdown** instead.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.08.230

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2022-4262, CVE-2022-4195,
  CVE-2022-4194, CVE-2022-4193, CVE-2022-4192, CVE-2022-4191, CVE-2022-4190,
  CVE-2022-4189, CVE-2022-4188, CVE-2022-4187, CVE-2022-4186, CVE-2022-4185,
  CVE-2022-4184, CVE-2022-4183, CVE-2022-4182, CVE-2022-4181, CVE-2022-4180,
  CVE-2022-4179, CVE-2022-4178, CVE-2022-4177, CVE-2022-4176, CVE-2022-4175,
  CVE-2022-4174, CVE-2022-4135, CVE-2022-3890, CVE-2022-3889, CVE-2022-3888,
  CVE-2022-3887, CVE-2022-3886, CVE-2022-3885, CVE-2022-3450, CVE-2022-3449,
  CVE-2022-3448, CVE-2022-3447, CVE-2022-3446, CVE-2022-3445, CVE-2022-3444,
  CVE-2022-3443, CVE-2022-3373, CVE-2022-3370, CVE-2022-3318, CVE-2022-3317,
  CVE-2022-3316, CVE-2022-3315, CVE-2022-3314, CVE-2022-3313, CVE-2022-3312,
  CVE-2022-3311, CVE-2022-3310, CVE-2022-3309, CVE-2022-3308, CVE-2022-3307,
  CVE-2022-3306, CVE-2022-3305, CVE-2022-3304, CVE-2022-3201, CVE-2022-3661,
  CVE-2022-3660, CVE-2022-3659, CVE-2022-3658, CVE-2022-3657, CVE-2022-3656,
  CVE-2022-3655, CVE-2022-3654, CVE-2022-3653, CVE-2022-3652, and CVE-2022-3723
- Updated Chromium browser to **version 108.0.5359.94**.

Base System

- Fixed **beacown** vulnerability
- Fixed **kernel Wi-Fi stack** security issues CVE-2022-41674, CVE-2022-42719, CVE-2022-42720, CVE-2022-42721, and CVE-2022-42722.
- Fixed **bind9** security issues CVE-2022-38178, CVE-2022-38177, and CVE-2022-2795.
- Fixed **gmp** security issue CVE-2021-43618.
- Fixed **ghostscript** security issue CVE-2020-27792.
- Fixed **libksba** security issue CVE-2022-3515.
- Fixed **sqlite3** security issues CVE-2020-35525 and CVE-2022-35737.
- Fixed **isc-dhcp** security issues CVE-2022-2929 and CVE-2022-2928.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2022-42824, CVE-2022-42823, CVE-2022-42799, CVE-2022-32923,
  CVE-2022-32888, CVE-2022-32912, CVE-2022-32891, and CVE-2022-32886
- Fixed **zulu8-cd** security issues CVE-2022-21628, CVE-2022-21626, CVE-2022-21624, and CVE-2022-21619.
- Fixed **expat** security issue CVE-2022-43680.
- Fixed **pillow** security issue CVE-2022-22817.
- Fixed **perl** security issue CVE-2020-16156.
- Fixed **mysql-5.7** security issues CVE-2022-21617, CVE-2022-21608, CVE-2022-21592, and CVE-2022-21589.

- Fixed **dbus** security issues CVE-2022-42012, CVE-2022-42011, and CVE-2022-42010.
- Fixed **ntfs-3g** security issue CVE-2022-40284.
- Fixed **libxml2** security issues CVE-2022-40304 and CVE-2022-40303.
- Fixed **pixman** security issue CVE-2022-44638.
- Fixed **tiff** security issues:
  More...

  CVE-2022-3599, CVE-2022-3598, CVE-2022-3570, CVE-2022-34526, CVE-2022-2869, CVE-2022-2868, and CVE-2022-2867
- Fixed **xorg-server** security issues CVE-2022-3550 and CVE-2022-3551.
- Fixed **krb5** security issue CVE-2022-42898.
- Fixed **libvncserver** security issue CVE-2020-29260.
- Fixed **libarchive** security issues CVE-2022-36227 and CVE-2022-26280.
- Fixed **heimdal** security issues CVE-2022-44640, CVE-2022-42898, CVE-2022-3437, and CVE-2021-44758.
- Fixed **libice** security issue CVE-2017-2626.
- Fixed **jbigkit** security issue CVE-2017-9937.
- Updated **ca-certificates** to version **20211016ubuntu0.20.04.1**.

New Features 11.08.230

Citrix

- Integrated **Citrix Workspace App 2211**.
  Available Citrix Workspace apps in this release: **2211** (default), **2207**, and **2010**.
- New features:
  - Support for **Authentication using FIDO2 (Technical Preview)**

Parameter	FIDO2 Authentication
Registry	`ica.module.virtualdriver.fido2.enable`
Value	enabled / disabled

AVD

- Added **max-threads** option **for WebRTC H.264 decoder module fluh264dec**.

Registry	`sessions.wvd%.options.webrtcdecodermaxthreads`
Value	1 (default) / 0-16

- Updated **AVD client**
- **Based on** Microsoft's new **RdClientSDKv2** that includes stability and performance fixes
- **MS Teams stability fixes**
- **MS Teams background blur** and **virtual background support**
- Preliminary **UDP short path** support (disabled by default, **enable on your own risk**)

Registry	`sessions.avd%.options.udp-short-path`
Value	enabled / disabled

VMware Horizon

- Added **support of deviceTRUST virtual channel**:

Parameter	deviceTRUST virtual channel
Registry	`vmware.view.vcdevicetrust.enable`
Type	bool
Value	enabled / disabled

Parallels Client

- Updated **Parallels client** to version **19.1**

Wi-Fi

- Added **registry key for controlling kernel parameters** `arp_evict_nocarrier` and `ndisc_evict_nocarrier` **for WLAN with WPA Supplicant**.
  The **default "1" leaves the traditional behavior unchanged**, i.e. the respective tables are evicted particularly during roaming.
  "0" results in quicker resumption of sending packets after roaming, but it also **leads to some packet loss**.

Parameter	ARP/NDP evict on nocarrier
Registry	`network.interfaces.wirelesslan.device0.arp_ndisc_evict_nocarrier`
Range	[0] [1]
Value	1

Imprivata

- Added **support for smartcard reader RFIDEAS CCID** (USB vid=0x0C27, pid=0xCCDB).
- Added registry key for **enabling "auto-open-grid-menu"**:

Parameter	Published application chooser to cover persistent application
Registry	`imprivata.auto-open-grid-menu`
Type	bool

Smartcard

- Updated **SecMaker Net iD Enterprise** to version **6.8.5.20** with support for Thales ID Prime 940.
  Beginning with this version, the **admin console** has **to be started with command** `iid -admin` .

Cisco Webex

- Integrated **Cisco WebEx VDI plugin** version **42.10.0.23814**

Base System

- **Updated IGEL EULA** to version August 2022.

Audio

- Added new registry key which possibly fixes **microphone issues on newer Intel devices**.

Parameter	Use PDM1 topology files (can help with microphone issues).
Registry	`system.sound_driver.use_pdm1_tplg`
Type	bool
Value	enabled / disabled

zoomvdi

- Integrated **Zoom VDI** plugin **5.12.1.21950**
  Available plugins in this release: **5.12.1.21950** (default), **5.11.2.21530**, and **5.8.4.21112**

Misc

- Updated **DriveLock Agent** to version **2022.1 (22.1.2.38801)**.
  "Fixed issues:
  On IgelOS, the DriveLock Linux Agent can not reset/disconnect USB drives during policy updates.
  The Linux Agent now handles Unicode characters correctly."
  New parameter:

Parameter	Join Token
Registry	`devices.drivelock.jointoken`
Value	empty

Hardware

- Added hardware support for **HP mt645 G7** (without LTE support).
- Added hardware support for **Lenovo L14 Gen 3** (without LTE support).

Resolved Issues 11.08.230

AVD

- Fixed **umlaut keys for Swiss keyboard** layout
- Fixed **crash of AVD** client **if Fabulatech plugins** were **enabled**.
- Fixed **smartcard redirection**
- Fixed possibly **frozen incoming video in MS Teams**.
- Added **paths where AVD searches for static, dynamic-1.1 and dynamic-2.0 virtual channel plugins and automatically loads all of them**:

  `/usr/lib/igelrdp3/plugins/automatic/static-channels`

  `/usr/lib/igelrdp3/plugins/automatic/dynamic-1.1-channels`

  `/usr/lib/igelrdp3/plugins/automatic/dynamic-2.0-channels`

  This is used by all AVD sessions automatically on session startup.

- **Disabled legacy workspace download by default**. It still can be enabled under `options.workspace-1.enabled` per AVD session. This slightly speeds up workspace download time.
- Fixed **MS Teams background FX-related client crashes**.
- Fixed **immediate AVD session crash on M350C and similar hardware** - caused by some compiler optimization applied at build time. This optimization has been removed for the sake of compatibility.

Firefox

- Fixed passthrough authentication for Firefox manual proxy.

Network

- Fixed **shutdown** getting stuck if local logon was configured and the network (LAN) was not connected.
- Fixed mounting of **NFS version 3** shares at boot time

Smartcard

- Fixed **smartcard access in the Firefox** browser **with activated AppArmor**.

Base System

- Fixed **power line frequency configuration** upon plug/unplug of a camera device.
- Fixed **battery notification** on other language than English.

- Fixed **on-screen keyboard** being broken after Kerberos logon.
- Fixed persistence of **brightness**, changed by function keys, over reboot.
- Fixed handling of **BIOS update** files.
- Fixed **LVFS BIOS update** did not work **with enabled secure boot**.
- Enhance possibilities to **set cstate kernel parameters**:
  - Allow 0 for `max_cstate` now too which sets `intel_idle.max_cstate` kernel cmdline parameter

Parameter	Set maximum allowed cstate on intel cpus.
Registry	`system.kernel.bootparams.max_cstate`
Range	[No limit] [0] [1] [2] [3] [4] [5] [6]
Value	No limit

  - Added new registry key to set `processor.max_cstate` kernel cmdline parameter.

Parameter	Set maximum allowed processor cstate.
Registry	`system.kernel.bootparams.max_proc_cstate`
Range	[No limit] [1] [2] [3] [4] [5] [6] [7] [8] [9]
Value	No limit

X11 System

- Fixed **DisplaySwitcher UI bug** that displayed the **wrong frequency**.
- Fixed **monitor** went to **sleep after resolution change on HP docking stations**.
- Added quirks to overcome **Hotplug or DP MST** issues.
- Added new registry keys:

Parameter	Quirk to improve DP MST hotplug behaviour.
Registry	`x.xserver%.quirks.dp_mst_hotplug`
Type	bool
Value	enabled / disabled
Parameter	Quirk to fix issues with screen stays black after DPMS off or DP MST hotplug.
Registry	`x.xserver%.quirks.screen_stay_black`
Type	bool
Value	enabled / disabled
Parameter	Quirk to fix issues with screen stays black by switch screen off and on again.

Registry	`x.xserver%.quirks.screen_stay_black_on_off`
Type	bool
Value	enabled / disabled

Audio

- Fixed **audio** support on **HP T240** hardware.

Hardware

- Fixed **bluetooth** support on **Lenovo L14 Gen 3** hardware.

Notes for Release 11.08.200

Software:	Version	11.08.200
Release Date:	2022-10-18	
Release Notes:	Version	RN-1108200-1
Last update:	2022-10-17	

- Supported Devices 11.08.200 (see page 2767)
- Component Versions 11.08.200 (see page 2768)
- Known Issues 11.08.200 (see page 2776)
- Security Fixes 11.08.200 (see page 2781)
- New Features 11.08.200 (see page 2784)
- Resolved Issues 11.08.200 (see page 2793)

The Release Notes for IGEL OS 11.08.200 are also available in the following formats:

- Plain text: readme_11.08.200.txt

Supported Devices 11.08.200

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[272].

272. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.200

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	105.0.5195.125-igel1663653255
Cisco JVDI Client	14.1.2
Cisco Webex VDI plugin	42.8.0.23214
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.2.10.7
Cisco Webex Meetings VDI plugin	42.6.8.5
Zoom Media Plugin	5.10.6.21295
Zoom Media Plugin	5.11.2.21530
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.05.0.16
Citrix Workspace App	22.07.0.20
deviceTRUST Citrix Channel	21.1.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.3.71814
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	3.0.1.0
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.13.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1663073494
IGEL AVD Client	1.1.0igel1663740227
deviceTRUST RDP Channel	21.1.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.6.0~git20220818-1igel1661859138
Zulu JRE	8.0.345-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.41-2igel1661863274
Remote Viewer (Red Hat Virtualization)	11.0-2igel1661863477
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.1.4-17
HP Anyware PCoIP Software Client	22.07.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-4igel1648284944
VMware Horizon Client	2206-8.6.0-20094634

Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.1013
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.8-1igel1655196158
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	9.0p1-1+b1igel1661867805
OpenSSH Server	9.0p1-1+b1igel1661867805
Bluetooth stack (bluez)	5.65-1igel1663161703
MESA OpenGL stack	22.1.7-0igel1661885230
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-3igel1661860347
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0

Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos_dev-g1663242518
Xorg X11 Server	21.1.4igel1657689370
Xorg Xephyr	21.1.4igel1657689370
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1656495558
ModemManager	1.18.10-2igel1662722763
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.20.3-2igel1655908747
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.3
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1

GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.36.7-1igel1661518099
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.38-dfsg-3igel1662536482
Virtualbox X11 Guest Utils	6.1.38-dfsg-3igel1662536482
Open VM Tools	11.0.5-4ubuntu0.18.04.2
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.2
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-3igel1661859915
Qemu Guest Agent	7.1+dfsg-2igel1663754599

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.38-dfsg-3igel1662536482
Virtual Background for Webcam	

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	24.8 M	Included
Java SE Runtime Environment	43.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	370.2 M	Included

Ericom PowerTerm InterConnect	11.5 M	Included
Media Player	768.0 K	Included
Local Browser (Firefox) Citrix Appliance	94.5 M	Included
VMware Horizon RDP	7.0 M	Included
Cendio ThinLinc	12.8 M	Included
Printing (Internet printing protocol CUPS)	22.5 M	Included
NoMachine NX	30.8 M	Included
VMware Horizon	295.8 M	Included
Voice over IP (Ekiga)	7.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	30.8 M	Not included
Fluendo GStreamer Codec Plugins	7.2 M	Included
IBM i Access Client Solutions	128.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	6.8 M	Included
NVIDIA graphics driver	280.2 M	Not included
Imprivata Appliance	16.0 M	Included
AppliDis	512.0 K	Included
Evidian AuthMgr	3.0 M	Included
Hardware Video Acceleration	16.5 M	Included
Extra Font Package	1.2 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	76.0 M	Included
PrinterLogic	53.2 M	Not included
Biosec BS Login	10.2 M	Not included
Login VSI Login Enterprise	32.8 M	Not included

Stratusphere UX CID Key software	8.5 M	Not included
Elastic Filebeat	25.0 M	Not included
AVD	130.5 M	Included
Local Browser (Chromium)	112.0 M	Not included
Amazon WorkSpaces Client	37.2 M	Included
deskMate client	6.5 M	Included
Cisco Webex VDI	75.0 M	Not included
Cisco Webex Meetings VDI	130.5 M	Not included
Zoom Media Plugin	138.8 M	Not included
DriveLock	14.8 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	256.0 K	Included
Fluendo Browser Codec Plugins	4.5 M	Included
HP Factory deployment documentation	90.0 M	Included
BIOS Tools	256.0 K	Included
HP Anyware Client	18.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtual Background for Webcam (Limited IGEL Support) Limited Support Features Mobile Device Access USB (Limited support) Virtualbox (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support)	256.0 K	Not included
Mobile Device Access USB (Limited support)	512.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.8 M	Not included
VirtualBox (Limited support)	74.0 M	Not included
Virtual Background for Webcam (Limited IGEL Support)	38.0 M	Included

Known Issues 11.08.200

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- With start of Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**. A **cache cleanup with reboot** should help, also the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: **Version 11.3 or later** is **required** for deploying IGEL OS 11.06. and following.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.

- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[273] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

273. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.08.200

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2022-3075, CVE-2022-3058,
  CVE-2022-3057, CVE-2022-3056, CVE-2022-3055, CVE-2022-3054, CVE-2022-3053,
  CVE-2022-3052, CVE-2022-3051, CVE-2022-3050, CVE-2022-3049, CVE-2022-3048,
  CVE-2022-3047, CVE-2022-3046, CVE-2022-3045, CVE-2022-3044, CVE-2022-3043,
  CVE-2022-3042, CVE-2022-3041, CVE-2022-3040, CVE-2022-3039, CVE-2022-3038,
  CVE-2022-2861, CVE-2022-2860, CVE-2022-2859, CVE-2022-2858, CVE-2022-2857,
  CVE-2022-2856, CVE-2022-2855, CVE-2022-2854, CVE-2022-2853, and CVE-2022-2852
- Fixed Chromium browser security issues:
  More...

  CVE-2022-3195, CVE-2022-3196, CVE-2022-3197, CVE-2022-3198,
  CVE-2022-3199, CVE-2022-3200, and CVE-2022-3201
- Updated **Chromium browser** to version **105.0.5195.125**.

Firefox

- Updated **Mozilla Firefox** to version **91.13.0 ESR**
- Fixes for **mfsa2022-35**, also known as CVE-2022-38472, CVE-2022-38473, CVE-2022-38478.
- Fixes for **mfsa2022-29**, also known as CVE-2022-36319, CVE-2022-36318.
- Fixes for **mfsa2022-25**, also known as:
  CVE-2022-34479, CVE-2022-34470, CVE-2022-34468, CVE-2022-34481,
  CVE-2022-31744, CVE-2022-34472, CVE-2022-2200, CVE-2022-34484
- Fixes for **mfsa2022-21**, also known as:
  CVE-2022-31736, CVE-2022-31737, CVE-2022-31738, CVE-2022-31740,
  CVE-2022-31741, CVE-2022-31742, CVE-2022-31747.

Base System

- Fixed **libinput** security issue CVE-2020-1215.
- Fixed **libarchive** security issue CVE-2022-26280.
- Fixed **ntfs-3g** security issues:
  More...

  CVE-2022-30789, CVE-2022-30788, CVE-2022-30787, CVE-2022-30786,
  CVE-2022-30785, CVE-2022-30784, CVE-2022-30783, and CVE-2021-46790
- Fixed **openssl1.0** security issues CVE-2022-2068 and CVE-2022-1292.
- Fixed **openssl** security issues CVE-2022-2097, CVE-2022-2068, and CVE-2022-1292.
- Fixed **gnupg2** security issues CVE-2022-34903 and CVE-2019-13050.
- Fixed **webkit2gtk** security issues:

More...

CVE-2022-26710, CVE-2022-22677, CVE-2022-22662, CVE-2022-30294, CVE-2022-30293, CVE-2022-26719, CVE-2022-26717, CVE-2022-26716, CVE-2022-26709, and CVE-2022-26700

- Fixed **nss** security issues CVE-2022-34480 and CVE-2022-22747.
- Fixed **Nvidia** graphics driver 470 security issues CVE-2022-31607 and CVE-2022-31608.
- Updated **Nvidia** graphics driver to version **470.141.03**.
- Fixed **curl** security issues CVE-2022-32208, CVE-2022-32207, CVE-2022-32206, and CVE-2022-32205.
- Fixed **curl** security issue CVE-2022-35252.
- Fixed **unzip** security issues CVE-2022-0530 and CVE-2022-0529.
- Fixed **freetype** security issues CVE-2022-31782, CVE-2022-27406, CVE-2022-27405, and CVE-2022-27404.
- Fixed **gnutls28** security issues CVE-2022-2509 and CVE-2021-4209.
- Fixed **mysql-5.7** security issue CVE-2022-21515.
- Fixed **python2.7** security issue CVE-2015-20107.
- Fixed **python3.6** security issue CVE-2015-20107.
- Fixed **net-snmp** security issues:
  More...

  CVE-2022-24810, CVE-2022-24809, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806, CVE-2022-24805, and CVE-2022-248

- Fixed **zulu8-ca** security issues CVE-2022-34169, CVE-2022-25647, CVE-2022-21541, and CVE-2022-21540.
- Updated **zulu8-ca JRE** to version **8.0.345**.
- Fixed **libtirpc** security issue CVE-2021-46828.
- Updated **Intel microcode** to version **20220809** which fixed security issue CVE-2022-21233.
- Fixed **postgresql-10** security issue CVE-2022-1552.
- Fixed **webkit2gtk** security issues CVE-2022-32816, CVE-2022-32792, and CVE-2022-2294.
- Updated **webkit2gtk** to version **2.36.6**.
- Fixed **open-vm-tools** security issue CVE-2022-31676.
- Fixed **postgresql-10** security issue CVE-2022-2625.
- Fixed **libxslt** security issues CVE-2021-30560 and CVE-2019-5815.
- Fixed **zlib** security issue CVE-2022-37434.
- Fixed **rsync** security issue CVE-2022-37434.
- Fixed **webkit2gtk** security issue CVE-2022-32893.
- Fixed **gnutls28** security issues CVE-2022-2509 and CVE-2021-4209.
- Fixed **flac** security issues CVE-2017-6888, CVE-2020-0499, and CVE-2021-0561.
- Fixed **libsndfile** security issue CVE-2021-4156.
- Fixed **gst-plugins-good1.0** security issues
  More...

  CVE-2022-1920, CVE-2022-1921, CVE-2022-1922, CVE-2022-1923, CVE-2022-1924, CVE-2022-1925, and CVE-2022-2122

- Updated **GStreamer 1.x** to version 1.20.3.
- Fixed **vim** security issues CVE-2022-1621, CVE-2022-1620, CVE-2022-1619, CVE-2022-1616, CVE-2022-1154, and CVE-2022-0943.
- Fixed **tiff** security issues:

More...

CVE-2022-22844, CVE-2022-2058, CVE-2022-2057,CVE-2022-2056,
CVE-2022-1355, CVE-2022-0924, CVE-2022-0909, CVE-2022-0908,
CVE-2022-0907, CVE-2020-19144, and CVE-2020-19131.

- Fixed **qemu** security issues CVE-2022-35414, CVE-2022-2962, CVE-2022-1050, CVE-2022-0216, and CVE-2020-14394.
- Fixed **expat** security issue CVE-2022-40674.

X Server

- Fixed **Xorg** security issues CVE-2022-2319 and CVE-2022-2320.
- Updated **Xorg** server to version **21.1.4**.

New Features 11.08.200

Citrix

- Support for **dynamic emergency calling within MS Teams**

Parameter	Citrix Support for dynamic e911
Registry	`ica.emergencycalling`
Value	false /true

- Integrated **Citrix Workspace App 2207**.
  Available Citrix Workspace Apps in this release: **2207** (default), **2205** and **2010**.
  - **Composite USB redirection**

Parameter	Native USB Redirection class rule
Registry	`ica.usbredirection.devicepolicy.class_rule%.rule`
Value	Deny, Allow, Connect
Parameter	Native USB Redirection product rule
Registry	`ica.usbredirection.devicepolicy.product_rule%.rule`
Value	Deny, Allow, Connect

  - Citrix Workspace app allows the **splitting of composite USB devices**. A composite USB device can perform more than one function. These functions are accomplished by exposing each of those functions using different interfaces.
    An example of a composite USB device is the Bloomberg keyboard which consists of a keyboard, fingerprint reader, an audio device, and USB hub, etc.
  - The **Composite USB redirection** feature adds the **CONNECT value to the rules for USB devices**.
  - **CONNECT** – Set the “CONNECT” keyword to enable **auto-redirect of a device when a session starts**.
  - **ALLOW** – Set the “ALLOW” keyword to allow **auto-redirect of a device only after a session starts**. However, if the “CONNECT” or “ALLOW” keyword is set, the device is auto-redirected when it is unplugged and plugged in during a session.
  - When redirect the composite USB device, normally the whole device is forwarded to the virtual host. However, now there is the possibility to **split and forward only the child interfaces that use a generic USB channel.** To do this, it is necessary to **add the following filter parameters** (`split` and `intf`) **to the device rules**. The `split` parameter specifies whether a composite device must be forwarded as separate devices or as a single composite device. "Split=1" means that the selected child interfaces of a composite device must be forwarded as split devices, while split=0 must not be forwarded (If the split

parameter is omitted, Split=0 is assumed). The `intf` parameter selects the specific child interfaces of the composite unit to which the action is to be applied.

- In IGEL Setup, the device rules can be added under **Sessions > Citrix > Citrix Global > Native USB Redirection > Device Rules.** Adding the first two filter parameters Vendor id/ vid and Product id/ pid, which redirects the entire composite device in the session. If splitting of the composite device is required, adding additional parameters in the "Extra config" as shown in the example is required.
  Example:
  `CONNECT: vid=047F pid=C039 split=1 intf=03` # Allow HID device and connect automatically.
  `DENY: vid=047F pid=C039 split=1 intf=00` # Deny audio endpoints
  `ALLOW: vid=047F pid=C039 split=1 intf=05` # Allow mgmt intf but do not connect automatically
- Note: Native USB Redirection for Citrix Sessions in IGEL OS (see page 2784) - the third **option "connect" has been added to the class and device rules. Composite USB redirection can change the behavior. If a device is no longer redirected with CWA 2207, the rule should be changed to 'Connect'.**

- Enhancement to **improve audio quality**
  - Playback **Delay Thresh**

Parameter	Playback Delay Thresh
Registry	`ica.module.PlaybackDelayThreshV4`
Value	50 (default)

With this enhancement, **the maximum output buffering value is decreased from 200 ms to 50 ms in Citrix Workspace app**. As a result, the user experience of the interactive audio application is improved. Also, the Round trip time (RTT) is decreased by 150 ms. This parameter is **valid only when "AudioRedirectionV4" is set to "True"**.

  - **Audio Temp Latency Boost**

Parameter	Audio Temp Latency Boost
Registry	`ica.module.AudioTempLatencyBoostV4`
Value	100 (default)

When the audio throughput undergoes a sudden spike or is not enough for an unstable network, this value increases the output buffering value. This increase in the output buffering value provides smooth audio. However, the audio might be slightly delayed. This parameter is **only valid when "AudioRedirectionV4" and "AudioLatencyControlEnabled" are set to "True".**

- Improved **audio echo cancellation** support

Parameter	Improved audio echo cancellation support
Registry	`ica.module.enableechocancellation`

Value	false / true

- Support for **DPI matching**

Parameter	Support for DPI matching
Registry	`ica.wfclient.dpimatchingenabled`
Value	false / true

The display resolution and DPI scale values set in the Citrix Workspace app match the corresponding values in the virtual apps and desktops session. DPI scaling is mostly used with large size and high-resolution monitors to display
applications, text, images, and other graphical elements in a size that can be viewed comfortably.

- **App Protection**

Parameter	Citrix App Protection
Registry	`ica.appprotection`
Value	false / true

App protection is an add-on feature for the Citrix Workspace app that provides enhanced security when using Citrix Virtual Apps and Desktops published resources. Two policies provide **anti-keylogging and anti-screen-capturing**
capabilities for a Citrix HDX session. This feature is **fully supported only for workspace app 2207**, with older workspace apps, you may experience x11vnc crashes.

- Updated **deviceTRUST Client Extension** to version **21.1.310.0**.

OSC Installer

- Added **option in factory mode for an automatical shutdown after self-check**. Log file of this deployment self-check is written to dummy partition.

AVD

- Added **SIGTERM and SIGHUP signal handlers to disconnect sessions** once received these signals. Since remote log-off is not supported in RDP, both signal handlers perform a session disconnect.
- Fixed **audio crackling**
- Added potential fix for the **ClaimsTokenAuthChallenge issue that dialog pops up too often**.
- Added SIGTERM and SIGHUP. As soon as the **RdCoreSDK** supports session log-off as well, **SIGHUP handler will be used instead of the disconnect**.
- Added potential fixes for **crashes with enabled printer redirection**
- Fixed **MS-Teams VDI** the local video **window went black** occasionally.
- Applied patch to fix bug in boost 1.69.0 that caused the "User cancelled" issue. https://github.com/boostorg/container/commit/90de9533ecef08e98d82e8f8c26fad57839e4184 at boost 1.74.0
- Added two parameters regarding **MS-Teams (WebRTC) redirection video decoding**:

Registry	`sessions.wvd0.options.webrtchardwaredecoding`
Value	on / auto / off
Registry	`sessions.wvd0.options.webrtcdecodermaxthreads`
Value	1 (default) / 0 (auto) / 0-16

RDP/IGEL RDP Client 2

- Updated **deviceTRUST Client Extension** to version **21.1.310.0**.

RD Web Access

- Added new parameter to enable support for **Interactive Logon Messages**.

Registry	`rdp.rd_web_access.options.remote_app_interactive_logon_message`
Type	bool
Value	enabled / disabled

VMware Horizon

- Updated **VMware Horizon** client to version **2206-8.6.0-20094634**

PowerTerm

- Updated **Ericom PowerTerm LTC** to version **14.0.3.71814**. This fixes scaling the emulation window to large sizes.

IBM_5250

- Added **startup splash screen** to IBM iAccess client. Thus, the user gets visual feedback of sessions about to start.

Parameter	Show splash screen at session startup
Registry	`ibm.iaccess.showsplash`
Value	true / false

HP Anyware

- **Renamed Teradici PCoIP Ultra** to **HP Anyware PCoIP**
  Updated HP Anyware PCoIP client to version **22.07.0-18.04**

Network

- Updated Modemmanager and libraries to improve **LTE device support**.

Wi-Fi

- Added **initial support for Realtek 8852ce Wi-Fi chipset**.

AppliDis

- Updated **Applidis SLB Linux client** to version **6.1.4.17**.

Smartcard

- Updated **Thales SafeNet Authentication client** to version **10.8.1013**.

CUPS Printing

Parameter	Make connected printer default printer
Registry	`print.cups.dynamic_default`
Type	bool
Value	enabled / disabled

- Added the **dynamic default printer** feature: If several printers are defined, the last plugged printer will be set as the default printer.
  On boot, the printer will be selected which is connected at the time.
  If more than one printer is connected at boot, the one which is the last in the list of printers defined in the OS gets the default.
  If a printer which was default is removed, the remaining printer will be elected as default.
  If more than one remains, the last in the list of printers defined in the OS, gets the default.
- Fixed **printer activation on USB hotplug** which could fail in rare occasions.
- Fixed cases where **choosing the first USB printer fails** as not named `usblp0` by the kernel as expected, as higher numbers were used (e.g. usblp2) even if no other USB printers were connected. The first USB printer is now defined as the one which is the first in the (sorted) list of all connected USB printers.
  Accordingly, the second USB printer is the second in the list of USB printers.
  For the case more than one USB printer is used at the same time, the first or second printer should

not be used as a selection method, as the numbering is also depending on the timing the printer is registered on the endpoint. On the next boot, the numbering can be different especially if the devices are switched on individually.
In this case, it's recommended to use instead the `usbclass` backend or selection by the USB Port on the endpoint or by the printer's USB IDs.

- Updated **HP Linux Imaging and Printing (HPLIP)** to version **3.22.6**
- Updated printer list to include **all new printers from HPLIP 3.22.6** (which do not require a proprietary plugin).

Cisco Webex

- Integrated **Cisco WebEx Meetings VDI plugins 42.6.8.5** and **42.2.10.7**
  Available plugins in this release: **42.6.8.5** (default), **42.2.10.7** and **41.12.6.12**
- Integrated C**isco WebEx VDI plugin 42.8.0.23214**

Cisco JVDI Client

- Integrated **Cisco JVDI 14.1.2**

Base System

- Updated **kernel** to version **5.17.15**.
- Updated **VDPAU** library to version **1.5**.
- Updated **gphoto** library to version **2.5.29**.
- Updated **OpenConnect VPN** client to version **9.01**.
- Updated **bluetooth stack (bluez)** to version **5.64**.
- Updated **OpenVPN** client to version **2.6.0 (with OpenVPN DCO support)**.
- Updated **MESA OpenGL stack** to version **22.1.5**.
- Updated **wireless regdb** to version **2022.06.06**.
- Added support for **webcam virtual background** (must be activated in **System > Fimware Customization > Features > Virtual Background for Webcam**)
  Minimum hardware requirements:
  - 4 GB RAM
  - Quad Core CPU with 1.5 GHz or higher
    - Also added new registry keys (to use the feature, `multimedia.webcam.virtual_background.enabled` must be set to **true**)

Parameter	Enable virtual background for webcam.
Registry	`multimedia.webcam.virtual_background.enabled`
Type	bool
Value	enabled / disabled

Parameter	Replace default webcam with virtual one.
Registry	`multimedia.webcam.virtual_background.replace_video0`
Type	bool
Value	enabled / disabled
Parameter	Select how the webcam to use should be choosen.
Registry	`multimedia.webcam.virtual_background.choose_webcam_by`
Range	[Use first webcam] [Choose by name] [Choose by vendor_id:product_id] [Choose by number]
Parameter	Select webcam by number (only valid if choose by number is used)
Registry	`multimedia.webcam.virtual_background.webcam_number`
Type	integer
Value	1
Parameter	Select webcam by name (only valid if choose by name is used)
Registry	`multimedia.webcam.virtual_background.webcam_name`
Type	string
Value	empty
Parameter	Select webcam by vendor_id:product_id (only valid if choose by vendor_id:product_id is used)
Registry	`multimedia.webcam.virtual_background.webcam_vendor_product`
Type	string
Value	empty
Parameter	Background picture file to use as virtual background

Registry	multimedia.webcam.virtual_background.background_file
Type	string
Value	empty

Parameter	Strength of background blurring
Registry	multimedia.webcam.virtual_background.blur
Type	integer
Value	25

Parameter	Select type of virtual background.
Registry	multimedia.webcam.virtual_background.type
Range	[Use blur] [Use background picture]

Parameter	Select resolution to use.
Registry	multimedia.webcam.virtual_background.resolution
Range	[webcam default] [webcam max] [1280x720] [640x480] [480x360]

Parameter	Select model for background segmentation.
Registry	multimedia.webcam.virtual_background.backscrub.model
Range	[segm_full] [selfiesegmentation] [segm_lite] [deeplabv3]
Value	segm_full

- Added possibility to **use ntfs with compression as Chromium and Firefox profile partition filesystem**.
- Changed registry keys (**added ntfs option**):

Parameter	Firefox Profiles Partition Filesystem Type
Registry	system.customization.ffpro.fs_type
Range	[reiser4] [ext4] [f2fs] [ntfs]

Parameter	Chromium Profiles Partition Filesystem Type
Registry	system.customization.chpro.fs_type

Range	[reiser4] [ext4] [f2fs] [ntfs]

zoomvdi

- Added **Smart Virtual Background support** for zoomvdi.

IGEL Setup	**Sessions > Unified Communication > Zoom Client Selection**
Parameter	Smart Virtual Background Support
Registry	`multimedia.zoomvdi.smartvb`
Type	string
Value	[Off][Auto][Always]

- Integrated **Zoom VDI plugin 5.11.2.21530**
  Available plugins in this release: **5.11.2.21530** (default), **5.10.6.21295** and **5.8.4.21112**

Hardware

- Updated **DisplayLink driver** to version **5.6.0**.
- Improved **performance of AMD devices and DisplayLink solutions**.
- Added hardware support for **Dell Optiplex 3000TC**

TC Setup (Java)

- Updated **TC Setup** to version **6.10.4**.

Fabulatech

- Updated **FabulaTech Scanner for Remote Desktop** to version **3.0.1.0**

Resolved Issues 11.08.200

OSC Installer

- Fixed **wrong icon** in OSC installer.
- Fixed deploying **IGEL OS GPT images** to **Fujitsu Lifebook U7311** via IGEL **SCCM Add-On**.

RDP/IGEL RDP Client 2

- Fixed RDP Client displaying a **wrong error message when the account is locked**.

Amazon Workspace Client

- Fixed **deviceTRUST virtual channel** configuration.

Chromium

- Fixed **hardware-accelerated video decoding** on newer **Intel chipsets using the iHD VA-API backend**.

Firefox

- Fixed Firefox **tabs crashing if the system uses iHD VAAPI driver**.

Network

- Fixed **MBB connection editor**

Wi-Fi

- Fixed: **System regulatory domain** now also set on the **self-managed driver rtl8852be**
- Fixed: **HP Probook 450 G8** with **Intel AX201 Wi-Fi**.
- Fixed: **Realtek 8852BE** Wi-Fi chipsets **(included in HP T655**)
- Fixed missing firmware files of **iwlwifi driver for INTEL chipsets**.

Imprivata

- Improved **disconnect/reconnect speed with Imprivata and Horizon**. Fixes Imprivata/Horizon roaming issue.
- Added: Minor improvements on **Vendor Launch Scripts**.

AppliDis

- Fixed wrong **port for HTTPS**.

Smartcard

- Fixed startup of **SecMaker Net iD service**.

Base System

- Fixed confusing **touchpad functions** if changed between right- and left-hand mouse.
- Fixed **touchpad enable / disable by hotkey**.
- Fixed **battery notification**.
- Fixed: Not rotate **SystemInformation.log** at startup. Rotation is only done with a successful upload.
- Fixed failed **firmware update from servers with low bandwidth**
- Fixed **NTP** time configuration **in Setup Assistant** if time was set before issued starter license.
- Fixed **corrupted BIOS update** where relevant files were missing in rare cases.
- Added **experimental DSC over DP MST** support to Intel graphic driver.
- Added new registry key:

Parameter	Enable DSC over DP MST support (experimental).
Registry	`x.drivers.intel.dsc_over_dp_mst`
Type	bool
Value	enabled / disabled

- Updated **fwupd** tool to fix possible issue with **LVFS BIOS update**.

X11 System

- Updated **xprintidle** to version **0.2.4**, which offers reasonable output also when DPMS state is not On.
- Added **support for HDMI4 to HDMI8 connectors** as newer devices possibly have these connectors.
- Changed registry keys to **allow HDMI connectors up to HDMI8**:

More...

Parameter	Monitor
Registry	`x.xserver%.connector`

Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen1.connector`
Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen2.connector`
Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen3.connector`

Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen4.connector`
Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen5.connector`
Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen6.connector`

Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic
Parameter	Monitor
Registry	`x.xserver%.screen7.connector`
Range	[Automatic][VGA][VGA(II)][DVI-D][DVI-D(II)][DisplayPort] [DisplayPort(II)][DisplayPort(III)][DisplayPort(IV)] [DisplayPort(V)][DisplayPort(VI)][DisplayPort(VII)] [DisplayPort(VIII)][HDMI][HDMI(II)][HDMI(III)][HDMI(IV)][HDMI(V)] [HDMI(VI)][HDMI(VII)][HDMI(VIII)][Internal Panel(LVDS)] [Internal Panel(LVDS II)][Internal Panel(eDP)] [Internal Panel(eDP II)][DVI-D(III)][DVI-D(IV)][DVI-D(V)] [DVI-D(VI)][DVI-D(VII)][DVI-D(VIII)]
Value	Automatic

- Updated **ATI / Radeon graphic driver** to version **19.1.0** which fixed issues with radeon Xorg driver and rotation.
- Updated **amdgpu graphic driver** to version **22.0.0** which improves performance with DisplayLink USB solutions.

Audio

- Fixed audio output via **display port/HDMI for HP Elitedesk 800 G6**
- Fixed issues with **3.5mm audio jack on LG AiO 24CN67** and **24CN65** devices.

Hardware

- Improved **bluetooth stability**.

Notes for Release 11.08.110

Software:	Version	11.08.110
Release Date:	2022-09-15	
Release Notes:	Version	RN-1108110-1
Last update:	2022-09-15	

- Supported Devices 11.08.110 (see page 2799)
- Component Versions 11.08.110 (see page 2800)
- Known Issues 11.08.110 (see page 2808)
- Security Fixes 11.08.110 (see page 2813)
- New Features 11.08.110 (see page 2815)
- Resolved Issues 11.08.110 (see page 2819)

The Release Notes for IGEL OS 11.08.110 are also available in the following formats:

- Plain text: readme_11.08.110.txt

Supported Devices 11.08.110

UD2-LX:	UD2-LX 52 UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10

See also Third-Party Devices Supported by IGEL OS 11[274].

274. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.08.110

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	104.0.5112.79-igel1659897252
Cisco JVDI Client	14.1.1
Cisco Webex VDI plugin	42.6.0.22645
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Cisco Webex Meetings VDI plugin	42.5.5.9
Zoom Media Plugin	5.10.0.21068
Zoom Media Plugin	5.10.6.21295
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.03.0.24
Citrix Workspace App	22.05.0.16
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.9.1
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1648540238
IGEL AVD Client	1.0.99.7igel1651063614
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.8.6
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.5.6-1igel1647855849
Zulu JRE	8.0.345-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	22.04.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-3igel1644994551
VMware Horizon Client	2203-8.5.0-19586897

Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0igel1647863644
MESA OpenGL stack	21.3.7-1igel1646288715
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-1igel1645768768
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.129.06-0ubuntu0.21.10.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0

Input Driver ELO Singletouch	5.1.0
Kernel	5.15.26 #mainline-lxos_dev-g1657794738
Xorg X11 Server	21.1.4igel1657689370
Xorg Xephyr	21.1.4igel1657689370
CUPS printing daemon	2.2.7-1ubuntu2.9igel1654064309
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1656495558
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	1.0.1
GStreamer 1.0 Fluendo asfdemux	1.0.1
GStreamer 1.0 Fluendo h264dec	1.0.3
GStreamer 1.0 Fluendo mp3dec	1.0.1
GStreamer 1.0 Fluendo mpeg4videodec	1.0.1
GStreamer 1.0 Fluendo vadec	1.0.2
GStreamer 1.0 Fluendo wmadec	1.0.1

GStreamer 1.0 Fluendo wmvdec	1.0.1
WebKit2Gtk	2.36.6-1igel1660197492
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	7.0+dfsg-7igel1654064676

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.20-1igel1645458039
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	24.8 M	Included
Java SE Runtime Environment	43.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	373.8 M	Included
Ericom PowerTerm InterConnect	11.5 M	Included

Media Player	768.0 K	Included
Local Browser (Firefox) Citrix Appliance	94.5 M	Included
VMware Horizon RDP	6.5 M	Included
Cendio ThinLinc	12.8 M	Included
Printing (Internet printing protocol CUPS)	23.8 M	Included
NoMachine NX	30.8 M	Included
VMware Horizon	281.5 M	Included
Voice over IP (Ekiga)	7.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	30.8 M	Not included
Fluendo GStreamer Codec Plugins	7.2 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	6.8 M	Included
NVIDIA graphics driver	280.0 M	Not included
Imprivata Appliance	16.0 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	3.0 M	Included
Hardware Video Acceleration	16.2 M	Included
Extra Font Package	1.2 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	76.0 M	Included
PrinterLogic	53.2 M	Not included
Biosec BS Login	10.2 M	Not included
Login VSI Login Enterprise	32.8 M	Not included
Stratusphere UX CID Key software	8.5 M	Not included

Elastic Filebeat	25.0 M	Not included
AVD	129.5 M	Included
Local Browser (Chromium)	112.0 M	Not included
Amazon WorkSpaces Client	36.8 M	Included
deskMate client	6.5 M	Included
Cisco Webex VDI	78.2 M	Not included
Cisco Webex Meetings VDI	140.8 M	Not included
Zoom Media Plugin	136.5 M	Not included
DriveLock	14.8 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	256.0 K	Included
Fluendo Browser Codec Plugins	4.5 M	Included
HP Factory deployment documentation	90.0 M	Included
Teradici PCoIP Client	17.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	512.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.8 M	Not included
VirtualBox (Limited support)	72.8 M	Not included

Known Issues 11.08.110

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- With start of Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**. A **cache cleanup with reboot** should help, also the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.

- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[275] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

275. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.08.110

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2022-2624, CVE-2022-2623, CVE-2022-2622, CVE-2022-2621, CVE-2022-2620, CVE-2022-2619, CVE-2022-2618, CVE-2022-2617, CVE-2022-2616, CVE-2022-2615, CVE-2022-2614, CVE-2022-2613, CVE-2022-2612, CVE-2022-2611, CVE-2022-2610, CVE-2022-2609, CVE-2022-2608, CVE-2022-2607, CVE-2022-2606, CVE-2022-2605, CVE-2022-2604, CVE-2022-2603, CVE-2022-2481, CVE-2022-2480, CVE-2022-2479, CVE-2022-2478, CVE-2022-2477, and CVE-2022-2163
- Fixed Chromium browser security issues:
  More...

  CVE-2022-2296, CVE-2022-2295, CVE-2022-2294, CVE-2022-2165, CVE-2022-2164, CVE-2022-2163, CVE-2022-2162, CVE-2022-2161, CVE-2022-2160, CVE-2022-2158, CVE-2022-2157, CVE-2022-2156, CVE-2022-2011, CVE-2022-2010, CVE-2022-2008, and CVE-2022-2007
- **Google** is **aware** that an **exploit for CVE-2022-2294 exists in the wild**.
- Updated **Chromium** browser to version **104.0.5112.79**

Base System

- Fixed **gnupg2** security issues CVE-2019-13050 and CVE-2022-34903.
- Fixed **cups** security issues CVE-2022-26691, CVE-2020-10001, and CVE-2019-8842.
- Fixed **ntfs-3g** security issues:
  More...

  CVE-2022-30789, CVE-2022-30788, CVE-2022-30787,CVE-2022-30786, CVE-2022-30785, CVE-2022-30784, CVE-2022-30783, and CVE-2021-46790
- Fixed **libvirt** security issue CVE-2022-0897.
- Fixed **qemu** security issue CVE-2021-3611.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2022-26710, CVE-2022-22677, CVE-2022-22662, CVE-2022-30294, CVE-2022-30293, CVE-2022-26719, CVE-2022-26717, CVE-2022-26716, CVE-2022-26709, and CVE-2022-26700
- Fixed **openssl1.0** security issue CVE-2022-2068.
- Fixed **openssl** security issues CVE-2022-2097 and CVE-2022-2068.
- Fixed **libarchive** security issue CVE-2022-26280.
- Fixed **ffmpeg** security issues DSA-5124-1 and DSA-5126-1.
- Fixed **nss** security issues CVE-2022-34480 and CVE-2022-22747.
- Fixed **kernel** security issue CVE-2022-32250.
- Fixed **libtirpc** security issue CVE-2021-46828.
- Fixed **unzip** security issues CVE-2022-0530 and CVE-2022-0529.

- Fixed **freetype** security issues CVE-2022-31782, CVE-2022-27406, CVE-2022-27405, and CVE-2022-27404.
- Fixed **gnutls28** security issues CVE-2022-2509 and CVE-2021-4209.
- Fixed **mysql-5.7** security issue CVE-2022-21515.
- Fixed **python2.7** security issue CVE-2015-20107.
- Fixed **python3.6** security issue CVE-2015-20107.
- Fixed **net-snmp** security issues:
  More...

  CVE-2022-24810, CVE-2022-24809, CVE-2022-24808,
  CVE-2022-24807, CVE-2022-24806, CVE-2022-24805, and CVE-2022-248
- Fixed **zulu8-ca** security issues CVE-2022-34169, CVE-2022-25647, CVE-2022-21541, and CVE-2022-21540.
- Fixed **curl** security issues CVE-2022-32208, CVE-2022-32207, CVE-2022-32206, and CVE-2022-32205.
- Fixed **postgresql-10** security issue CVE-2022-1552.
- Fixed **webkit2gtk** security issues CVE-2022-32816, CVE-2022-32792, and CVE-2022-2294.

X Server

- Fixed **xorg** security issues CVE-2022-2319 and CVE-2022-2320.
- Updated **Xorg** server to version **21.1.4**.

New Features 11.08.110

VMware Horizon

- Added system-wide handler to **start links which use the vmware-view protocol**.
  View session can now be started by Chromium or any other application which uses xdg-open.

Chromium

- Added **list and dictionary support for custom policies**.

Smartcard

- Added **support for Cherry eHealth ST-1506 in USB RNDIS mode**. There is a systray icon per device. The tooltip says whether it is connected or disconnected in terms of network configuration. **Per device, one instance** of the template `devices.cherry.terminal%` **must be created and configured. By default, none is configured and so the feature is essentially disabled.**
- This is for potentially distinguishing multiple connected devices and **may contain a MAC address or the value of the udev property** `ID_NET_NAME_PATH`. It **may be left empty if only one device shall be supported**:

Parameter	Device ID
Registry	`devices.cherry.terminal%.rndis.device_id`
Type	string
Value	empty (Default)

Parameter	Device IP address
Registry	`devices.cherry.terminal%.rndis.device_ipaddress`
Type	string
Value	192.168.42.42 (Default)

Parameter	Host IP address
Registry	`devices.cherry.terminal%.rndis.host_ipaddress`
Type	string
Value	192.168.42.1 (Default)

- This port on the host will be passed through to the same port on the device:

Parameter	Device TCP port
Registry	`devices.cherry.terminal%.rndis.device_tcpport`
Type	string
Value	4742 (Default)

- This port on the host will be passed through to the same port on the device:

Parameter	Passed through device UDP port
Registry	`devices.cherry.terminal%.rndis.device_udpport`
Type	string
Value	4742 (Default)

- This port on the host will be forwarded to the device's port 443:

Parameter	Host SSL port
Registry	`devices.cherry.terminal%.rndis.host_sslport`
Type	string
Value	empty (Default)

- Added support for **concurrent usage of multiple smartcard middleware libraries for authentication with smartcard to Active Directory / Kerberos and Citrix**.
  In the Setup on page **Security > Smartcard > Middleware**, multiple libraries can be activated. **If none is activated, OpenSC is taken as fallback**.

Cisco Webex

- Integrated **WebEx VDI Client 42.6.0.22645**

Base System

- Added **LVFS utility for BIOS update**. For detailed instructions, see BIOS Update for Devices Supported by LVFS (see page 2815).

  ⚠ Please note: IGEL supports just the mechanism – BIOS updates are executed at own risk (as usual).

Parameter	Allow installation of bios version that's older than current.
Registry	`fwtools.bios_tools.allow_downgrade`
Value	enabled / disabled

Parameter	Allow installation of bios version that's equivalent to current.
Registry	`fwtools.bios_tools.allow_reinstall`
Value	enabled / disabled

- Added parameter for LVFS BIOS update:

IGEL Setup	**System > Firmware Customization > Features**
Parameter	BIOS Tools
Registry	`services.bios_tools.enabled`
Value	enabled / disabled
Parameter	BIOS Update file
Registry	`fwtools.bios_tools.bios_update_file`
Value	empty (Default)
Note	The URL or path to the BIOS Update binary must be entered here (e.g. any `*.cab` file for LVFS). LVFS BIOS Updates can be downloaded at https://fwupd.org/lvfs/.

- Download credentials:

Parameter	Download Username
Registry	`fwtools.bios_tools.bios_download_username`
Value	empty (Default)
Parameter	Download Password
Registry	`fwtools.bios_tools.bios_download_crypt_password`
Value	empty (Default)

- **Known issue**: **No support for BIOS password handling**.

- Added a Generic Device **Command "BIOS - Trigger update" to trigger BIOS updates via UMS**.
- Added new registry key to **disable DisplayPort MST support of amdgpu driver**:

Parameter	Disable DP MST support of the AMDPU DRM driver.
Registry	`x.drivers.amdgpu.disable_dp_mst_support`
Type	bool
Value	enabled / disabled

X11 System

- Updated **ATI/Radeon graphic driver** to version **19.1.0**.
- Updated **amdgpu graphic driver** to version **22.0.0**.

Login Enterprise

- Updated **Login VSI Enterprise** to version **4.8.6**.

zoomvdi

- Integrated **Zoom VDI client 5.10.6.21295**
  Available Zoom Media Plugins in this release: **5.8.4.21112, 5.10.0.21068**, and **5.10.6.21295** (default)

Multimedia

- Updated **Fluendo GStreamer 1.x multimedia codecs** to **fix stability problems with AVD Teams** Optimization:
  More...

gst-fluendo-aacdec	1.0.1
gst-fluendo-asfdemux	1.0.1
gst-fluendo-h264dec	1.0.3
gst-fluendo-mp3	1.0.1
gst-fluendo-mpeg4video	1.0.1
gst-fluendo-vadec - h264_mpeg4	1.0.2
gst-fluendo-wmadec	1.0.1
gst-fluendo-wmvdec	1.0.1

Hardware

- Added hardware support for **HP T655 Elite Thin Client**.

TC Setup (Java)

- Updated **TC Setup** to version **6.10.3**.

Resolved Issues 11.08.110

Citrix

- Fixed: **Random disconnects, segfaults or session freezes with enabled H.264 decoding** in Citrix sessions.
- Improved **keyboard layout synchronization**:
  - required setting: `ica.module.virtualdriver.keyboardsync.enable=true` (**changed to default=true)**
  - for configuring the **new KeyboardSyncMode**. Windows Server may require config, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.htm#keyboard-layout-synchronization:
    default for `ica.wfclient.keyboardsyncmode` **changed to "dynamic"**
  - for configuring **new KeyboardEventMode**:
    default for `ica.wfclient.keyboardeventmode` **changed to "Unicode"**

AVD

- Fixed stability issues of **MS Teams Optimization in AVD with enabled H.264 decoding** via updated Fluendo codec pack and switch of Radeon(SI) driver from **vdpau to vaapi**.

Chromium

- Added : User is **asked where to save each file before downloading** for the case no download location is set.
- Fixed **hardware accelerated video decoding on** newer **Intel chipsets** using **the iHD VA-API backend**.

Network

- Fixed **MBB connection editor**
- Fixed negotiation of inner method for **802.1X PEAP authentication**

Wi-Fi

- Added registry key for **set of WPA supplicant parameter** `wpa_deny_ptk0_rekey` .
  This **should be changed to "driver-dependent"** (i.e. deny unless driver explicitly asserts capability) **or "always"** if WLAN problems are associated with messages of the form " `kernel: Rekeying PTK for STA ... but driver can't safely do that` ".
  The default "**never**" preserves the traditional behavior.
  More...

Parameter	Deny PTK0 rekey
Registry	`network.interfaces.wirelesslan.device0.wpa_deny_ptk0_rekey`
Range	[never] [driver-dependent] [always]
Value	never

- Added missing **German text for Wi-Fi passphrase**.
- Added missing **firmware files for Intel AX210 Wi-Fi adapters**.

HID

- Fixed **touchpad acceleration** if **libinput** driver is used.

Base System

- Fixed failed **firmware update from servers with low bandwidth**.
- Fixed **touchpad** enable / disable by **hotkey**.
- Fixed **sporadic downgrade issue** - as occured **with 11.07.191**.
- Added several registry keys to **set new kernel commandline options**:
  More...

Parameter	Use polling for IRQs.
Registry	`system.kernel.bootparams.irqpoll`
Type	bool
Value	enabled / disabled

Parameter	Disable use of Hyperthreading.
Registry	`system.kernel.bootparams.nosmt`
Type	bool
Value	enabled / disabled

Parameter	Enable debug output for i8042 driver.
Registry	`system.kernel.bootparams.i8042.debug`
Type	bool
Value	enabled / disabled
Parameter	Do not use muxing for i8042 driver.

Registry	`system.kernel.bootparams.i8042.nomux`
Type	bool
Value	enabled / disabled
Parameter	Disable use of PnP configuration for i8042 driver.
Registry	`system.kernel.bootparams.i8042.nopnp`
Type	bool
Value	enabled / disabled
Parameter	Disable use of AUX loopback command for i8042 driver.
Registry	`system.kernel.bootparams.i8042.noloop`
Type	bool
Value	enabled / disabled
Parameter	Ignore timeout signaled by controller for i8042 driver.
Registry	`system.kernel.bootparams.i8042.notimeout`
Type	bool
Value	enabled / disabled
Parameter	Reset controller during init for i8042 driver.
Registry	`system.kernel.bootparams.i8042.reset`
Type	bool
Value	enabled / disabled
Parameter	Set PCI kernel parameters.
Registry	`system.kernel.bootparams.pci`
Range	[No setting] [Conf1] [Conf2] [Nodomains] [Nommconf] [Nomsi] [Nocrs] [Noacpi] [Routeirq]
Value	No setting
Parameter	Set kernel clocksource to use.
Registry	`system.kernel.bootparams.clocksource`

Range	[Default] [Jiffies] [ACPI PM] [HPET] [TSC]
Value	no

Parameter	PCIe Active State Power Management setting.
Registry	`system.kernel.bootparams.pcie_aspm`
Range	[On] [Off]
Value	On

Parameter	Dynamic ticks setting.
Registry	`system.kernel.bootparams.nohz`
Range	[On] [Off]
Value	On

Parameter	Delay in seconds before new devices are scanned.
Registry	`system.kernel.bootparams.usb_storage_delay`
Type	integer
Value	0 (Default)

X11 System

- Added a new registry key to enable the old monitor connector scheme:
  More...

Parameter	Use old DP connector setup name handling.
Registry	`x.drm_daemon.use_legacy_dp_handling`
Type	bool
Value	enabled / disabled

- Updated **ati/radeon** graphic driver to **version 19.1.0** which **fixed issues with radeon Xorg driver and rotation**.

X Server

- Fixed **DisplayPort on Shuttle DS77U** device.
- Some **older ATI/Radeon cards have issues with current Xorg servers**. For that reason, switch to an older one was added.
  Added a new registry key to switch to an older Xorg server version:

More...

Parameter	Use older xorg server version.
Registry	`x.server.use_legacy_xorg_server`
Type	bool
Value	enabled / disabled

Audio

- Fixed **audio output via display port/HDMI for HP Elitedesk 800 G6**
- Use this registry key to **set the default audio device as fallback device after device unplug**:
  More...

Parameter	Use default audio device as fallback device
Registry	`multimedia.use_default_fallback`
Type	bool
Value	enabled / disabled

Hardware

- Fixed **ADS-TEC front key**.
- Fixed issue with **Intel Elkhart devices like HP t550**.

Notes for Release 11.07.920

Software:	Version	11.07.920
Release Date:	2022-09-15	
Release Notes:	Version	RN-1107920-1
Last update:	2022-09-15	

- Supported Devices 11.07.920 (see page 2825)
- Component Versions 11.07.920 (see page 2826)
- Known Issues 11.07.920 (see page 2834)
- Security Fixes 11.07.920 (see page 2839)
- New Features 11.07.920 (see page 2841)
- Resolved Issues 11.07.920 (see page 2842)

The Release Notes for IGEL OS 11.07.920 are also available in the following formats:

- Plain text: readme_11.07.920.txt

Supported Devices 11.07.920

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[276].

276. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.07.920

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	104.0.5112.79-igel1659897252
Cisco JVDI Client	14.1.1
Cisco Webex VDI plugin	42.4.0.21893
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Cisco Webex Meetings VDI plugin	42.5.5.9
Zoom Media Plugin	5.10.0.21068
Zoom Media Plugin	5.10.6.21295
Zoom Media Plugin	5.8.4.21112
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.03.0.24
Citrix Workspace App	22.05.0.16
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.9.1
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1648540238
IGEL AVD Client	1.0.99.7igel1651063614
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.5.11
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.6.0~git20220808-1igel1660123886
Zulu JRE	8.0.345-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	22.04.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-3igel1644994551
VMware Horizon Client	2203-8.5.0-19586897

Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0ubuntu1igel1660041146
MESA OpenGL stack	22.1.5-1igel1659869061
VAAPI ABI Version	0.40
VDPAU Library version	1.5-1igel1646992192
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-3igel1657777718
Graphics Driver ATI/AMDGPU	22.0.0-2igel1657776223
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.141.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0

Input Driver ELO Singletouch	5.1.0
Kernel	5.17.15 #mainline-lxos_dev-g1659943300
Xorg X11 Server	21.1.4igel1657689370
Xorg Xephyr	21.1.4igel1657689370
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1656495558
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70

GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.36.6-1igel1660197492
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	6.2+dfsg-3igel1646036781

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622
VPN OpenConnect	9.01-1igel1657119743
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	24.8 M	Included
Java SE Runtime Environment	43.2 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	373.8 M	Included
Ericom PowerTerm InterConnect	11.5 M	Included

Media Player	768.0 K	Included
Local Browser (Firefox) Citrix Appliance	94.5 M	Included
VMware Horizon RDP	6.5 M	Included
Cendio ThinLinc	12.8 M	Included
Printing (Internet printing protocol CUPS)	23.8 M	Included
NoMachine NX	30.8 M	Included
VMware Horizon	281.5 M	Included
Voice over IP (Ekiga)	7.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	30.8 M	Not included
Fluendo GStreamer Codec Plugins	7.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	6.8 M	Included
NVIDIA graphics driver	280.2 M	Not included
Imprivata Appliance	16.0 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	3.0 M	Included
Hardware Video Acceleration	15.0 M	Included
Extra Font Package	1.2 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	4.2 M	Included
Cisco JVDI client	76.0 M	Included
PrinterLogic	53.2 M	Not included
Biosec BS Login	10.2 M	Not included
Login VSI Login Enterprise	32.8 M	Not included
Stratusphere UX CID Key software	8.5 M	Not included

Elastic Filebeat	25.0 M	Not included
AVD	129.5 M	Included
Local Browser (Chromium)	112.0 M	Not included
Amazon WorkSpaces Client	36.8 M	Included
deskMate client	6.5 M	Included
Cisco Webex VDI	77.0 M	Not included
Cisco Webex Meetings VDI	140.8 M	Not included
Zoom Media Plugin	136.5 M	Not included
DriveLock	14.8 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	256.0 K	Included
Fluendo Browser Codec Plugins	4.5 M	Included
HP Factory deployment documentation	90.0 M	Included
Teradici PCoIP Client	17.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	512.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.8 M	Not included
VirtualBox (Limited support)	72.5 M	Not included

Known Issues 11.07.920

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- With start of Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**. A **cache cleanup with reboot** should help, also the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.

- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[277] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail when using **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

277. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.07.920

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2022-2624, CVE-2022-2623, CVE-2022-2622, CVE-2022-2621, CVE-2022-2620, CVE-2022-2619, CVE-2022-2618, CVE-2022-2617, CVE-2022-2616, CVE-2022-2615, CVE-2022-2614, CVE-2022-2613, CVE-2022-2612, CVE-2022-2611, CVE-2022-2610, CVE-2022-2609, CVE-2022-2608, CVE-2022-2607, CVE-2022-2606, CVE-2022-2605, CVE-2022-2604, CVE-2022-2603, CVE-2022-2481, CVE-2022-2480, CVE-2022-2479, CVE-2022-2478, CVE-2022-2477, and CVE-2022-2163
- Fixed Chromium browser security issues:
  More...

  CVE-2022-2296, CVE-2022-2295, CVE-2022-2294, CVE-2022-2165, CVE-2022-2164, CVE-2022-2163, CVE-2022-2162, CVE-2022-2161, CVE-2022-2160, CVE-2022-2158, CVE-2022-2157, CVE-2022-2156, CVE-2022-2011, CVE-2022-2010, CVE-2022-2008, and CVE-2022-2007
- **Google** is aware that an **exploit for CVE-2022-2294 exists in the wild**.
- Updated **Chromium** browser to **version 104.0.5112.79**

Base System

- Fixed **libinput** security issue CVE-2020-1215.
- Fixed **libarchive** security issue CVE-2022-26280.
- Fixed **ntfs-3g** security issues:
  More...

  CVE-2022-30789, CVE-2022-30788, CVE-2022-30787, CVE-2022-30786, CVE-2022-30785, CVE-2022-30784, CVE-2022-30783, and CVE-2021-46790
- Fixed **openssl1.0** security issues CVE-2022-2068 and CVE-2022-1292.
- Fixed **openssl** security issues CVE-2022-2097, CVE-2022-2068, and CVE-2022-1292.
- Fixed **gnupg2** security issues CVE-2022-34903 and CVE-2019-13050.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2022-26710, CVE-2022-22677, CVE-2022-22662, CVE-2022-30294, CVE-2022-30293, CVE-2022-26719, CVE-2022-26717, CVE-2022-26716, CVE-2022-26709, and CVE-2022-26700
- Fixed **nss** security issues CVE-2022-34480 and CVE-2022-22747.
- Fixed **Nvidia** graphics driver 470 security issues CVE-2022-31607 and CVE-2022-31608.
- Updated **Nvidia** graphics driver to **version 470.141.03**.
- Fixed **curl** security issues CVE-2022-32208, CVE-2022-32207, CVE-2022-32206, and CVE-2022-32205.
- Fixed **unzip** security issues CVE-2022-0530 and CVE-2022-0529.

- Fixed **freetype** security issues CVE-2022-31782, CVE-2022-27406, CVE-2022-27405, and CVE-2022-27404.
- Fixed **gnutls28** security issues CVE-2022-2509 and CVE-2021-4209.
- Fixed **mysql-5.7** security issue CVE-2022-21515.
- Fixed **python2.7** security issue CVE-2015-20107.
- Fixed **python3.6** security issue CVE-2015-20107.
- Fixed **net-snmp** security issues:
  More...

  CVE-2022-24810, CVE-2022-24809, CVE-2022-24808,
  CVE-2022-24807, CVE-2022-24806, CVE-2022-24805, and CVE-2022-248
- Fixed **zulu8-ca** security issues CVE-2022-34169, CVE-2022-25647, CVE-2022-21541, and CVE-2022-21540.
- Updated **zulu8-ca JRE** to **version 8.0.345**.
- Fixed **libtirpc** security issue CVE-2021-46828.
- Updated **Intel microcode** to **version 20220809** which fixed security issue CVE-2022-21233.
- Fixed **postgresql-10** security issue CVE-2022-1552.
- Fixed **webkit2gtk** security issues CVE-2022-32816, CVE-2022-32792, and CVE-2022-2294.
- Updated **webkit2gtk** to **version 2.36.6**.

X Server

- Fixed **xorg** security issues CVE-2022-2319 and CVE-2022-2320.
- Updated **Xorg server** to **version 21.1.4**.

New Features 11.07.920

Chromium

- Added **list and dictionary support for custom policies**.

Base System

- Added new registry key to disable **DisplayPort MST** support of **amdgpu driver**.
  More...

Parameter	Disable DP MST support of the AMDPU DRM driver.
Registry	`x.drivers.amdgpu.disable_dp_mst_support`
Type	bool
Value	enabled / disabled

- Updated **kernel** to version **5.17.15**.
- Updated **VDPAU** library to version **1.5**.
- Updated **gphoto** library to version **2.5.29**.
- Updated **OpenConnect VPN** client to version **9.01**.
- Updated **bluetooth stack (bluez)** to version **5.64**.
- Updated **OpenVPN** client to version **2.6.0 (with OpenVPN DCO support)**.
- Updated **MESA OpenGL stack** to version **22.1.5**.
- Updated **wireless regdb** to version **2022.06.06**.

X11 System

- Updated **ATI/Radeon** graphic driver to version **19.1.0**.
- Updated **amdgpu** graphic driver to version **22.0.0**.

zoomvdi

- Integrated **Zoom VDI** client **5.10.6.21295**
  Available Zoom Media Plugins in this release: **5.8.4.21112**, **5.10.0.21068**, and **5.10.6.21295** (default)

Hardware

- Updated **DisplayLink** driver to version **5.6.0**.
- Improved **performance of AMD devices** and **DisplayLink** solutions.

Resolved Issues 11.07.920

Chromium

- Added: User is **asked where to save each file before downloading** for the case no download location is set.
- Fixed **hardware accelerated video decoding** on newer **Intel chipsets** using the **iHD VA-API backend**.

Network

- Fixed **MBB connection editor**
- Fixed negotiation of inner method for **802.1X PEAP authentication**

Wi-Fi

- Added registry key for **set of WPA supplicant parameter** `wpa_deny_ptk0_rekey`.
  This should be changed to "**driver-dependent**" (i.e. deny unless driver explicitly asserts capability) or "**always**" if WLAN problems are associated with messages of the form "**kernel: Rekeying PTK for STA ... but driver can't safely do that**".
  The default "**never**" preserves the traditional behavior.
  More...

Parameter	Deny PTK0 rekey
Registry	`network.interfaces.wirelesslan.device0.wpa_deny_ptk0_rekey`
Range	[never] [driver-dependent] [always]
Value	never

- Added missing **German text for Wi-Fi passphrase**.
- Added missing **firmware files for Intel AX210 Wi-Fi adapters**.

HID

- Fixed **touchpad acceleration** if **libinput** driver is used.

Base System

- Fixed failed **firmware update from servers with low bandwidth**.
- Fixed **touchpad** enable / disable by **hotkey**.
- Fixed **sporadic downgrade issue** - as occured **with 11.07.191**.
- Added several registry keys to **set new kernel commandline options**:

More...

Parameter	Use polling for IRQs.
Registry	`system.kernel.bootparams.irqpoll`
Type	bool
Value	enabled / disabled
Parameter	Disable use of Hyperthreading.
Registry	`system.kernel.bootparams.nosmt`
Type	bool
Value	enabled / disabled
Parameter	Enable debug output for i8042 driver.
Registry	`system.kernel.bootparams.i8042.debug`
Type	bool
Value	enabled / disabled
Parameter	Do not use muxing for i8042 driver.
Registry	`system.kernel.bootparams.i8042.nomux`
Type	bool
Value	enabled / disabled
Parameter	Disable use of PnP configuration for i8042 driver.
Registry	`system.kernel.bootparams.i8042.nopnp`
Type	bool
Value	enabled / disabled
Parameter	Disable use of AUX loopback command for i8042 driver.
Registry	`system.kernel.bootparams.i8042.noloop`
Type	bool
Value	enabled / disabled
Parameter	Ignore timeout signaled by controller for i8042 driver.
Registry	`system.kernel.bootparams.i8042.notimeout`

Type	bool
Value	enabled / disabled
Parameter	Reset controller during init for i8042 driver.
Registry	`system.kernel.bootparams.i8042.reset`
Type	bool
Value	enabled / disabled
Parameter	Set PCI kernel parameters.
Registry	`system.kernel.bootparams.pci`
Range	[No setting] [Conf1] [Conf2] [Nodomains] [Nommconf] [Nomsi] [Nocrs] [Noacpi] [Routeirq]
Value	No setting
Parameter	Set kernel clocksource to use.
Registry	`system.kernel.bootparams.clocksource`
Range	[Default] [Jiffies] [ACPI PM] [HPET] [TSC]
Value	no
Parameter	PCIe Active State Power Management setting.
Registry	`system.kernel.bootparams.pcie_aspm`
Range	[On] [Off]
Value	On
Parameter	Dynamic ticks setting.
Registry	`system.kernel.bootparams.nohz`
Range	[On] [Off]
Value	On
Parameter	Delay in seconds before new devices are scanned.
Registry	`system.kernel.bootparams.usb_storage_delay`
Type	integer

Value	0 (Default)

X11 System

- Added a new registry key to enable the old monitor connector scheme:
  More...

Parameter	Use old DP connector setup name handling.
Registry	`x.drm_daemon.use_legacy_dp_handling`
Type	bool
Value	enabled / disabled

- Updated **ati/radeon** graphic driver to **version 19.1.0** which **fixed issues with radeon Xorg driver and rotation**.
- Updated **amdgpu** graphic driver to v**ersion 22.0.0** which **improves performance with DisplayLink USB solutions**.

X Server

- Fixed **DisplayPort on Shuttle DS77U** device.
- Some **older ATI/Radeon cards have issues with current Xorg servers**. For that reason, switch to an older one was added.
  Added a new registry key to switch to an older Xorg server version:
  More...

Parameter	Use older xorg server version.
Registry	`x.server.use_legacy_xorg_server`
Type	bool
Value	enabled / disabled

Audio

- Fixed **audio output via display port/HDMI for HP Elitedesk 800 G6**

Hardware

- Fixed issue with **Intel Elkhart devices like HP t550**.

Notes for Release 11.07.170

Software:	Version	11.07.170
Release Date:	2022-06-28	
Release Notes:	Version	RN-1107170-1
Last update:	2022-06-28	

- Supported Devices 11.07.170 (see page 2847)
- Component Versions 11.07.170 (see page 2848)
- Known Issues 11.07.170 (see page 2856)
- Security Fixes 11.07.170 (see page 2861)
- New Features 11.07.170 (see page 2862)
- Resolved Issues 11.07.170 (see page 2864)

The Release Notes for IGEL OS 11.07.170 are also available in the following formats:

- Plain text: readme11.07.170.txt

Supported Devices 11.07.170

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[278].

278. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.07.170

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	102.0.5005.61-igel1653480432
Cisco JVDI Client	14.1.1
Cisco Webex VDI plugin	42.4.0.21893
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Cisco Webex Meetings VDI plugin	42.5.5.9
Zoom Media Plugin	5.10.0.21068
Zoom Media Plugin	5.4.59458
Zoom Media Plugin	5.9.6.20931
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.03.0.24
Citrix Workspace App	22.05.0.16
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
Conky System Monitor	1.10.8-1
ControlUp Agent	8.1.5.500
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.8134
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0

FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.9.1
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1648540238
IGEL AVD Client	1.0.99.7igel1651063614
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
Login VSI Enterprise	4.5.11
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.5.6-1igel1647855849
Zulu JRE	8.0.332-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	22.04.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-3igel1644994551
VMware Horizon Client	2203-8.5.0-19586897

Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.9
OpenSSL	1.1.1-1ubuntu2.1~18.04.17
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0igel1647863644
MESA OpenGL stack	21.3.7-1igel1646288715
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-2igel1629135948
Graphics Driver ATI/AMDGPU	22.0.0-1igel1645768768
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.129.06-0ubuntu0.21.10.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0

Input Driver ELO Singletouch	5.1.0
Kernel	5.15.26 #mainline-lxos-g1652790891
Xorg X11 Server	21.1.3igel1645782509
Xorg Xephyr	21.1.3igel1645782509
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70

GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.34.6-1igel1645163872
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	6.2+dfsg-3igel1646036781

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.20-1igel1645458039
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	322.0 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included

Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	81.5 M	Included
VMware Horizon RDP	5.5 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	243.0 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.5 M	Not included
Imprivata Appliance	14.2 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	66.8 M	Included
PrinterLogic	47.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	7.5 M	Not included

Elastic Filebeat	22.2 M	Not included
AVD	113.8 M	Included
Local Browser (Chromium)	97.5 M	Not included
Amazon WorkSpaces Client	32.2 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	70.8 M	Not included
Cisco Webex Meetings VDI	129.2 M	Not included
Zoom Media Plugin	124.0 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
IGEL Imprivata Agent	256.0 K	Included
Fluendo Browser Codec Plugins	4.0 M	Included
HP Factory deployment documentation	88.5 M	Included
Teradici PCoIP Client	15.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	65.2 M	Not included

Known Issues 11.07.170

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.
- With start of Self-Service, it is possible that the process **ServiceRecord is segfaulted** - **Self-Service cannot be started afterwards**. A **cache cleanup with reboot** should help, also the **following parameters should be set to "true"**.
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.
- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.

- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).
- **Glibc** has a serious **memcpy performance regression on AMD Zen-based systems**.

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[279] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (**auto** is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

279. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

Security Fixes 11.07.170

Firefox

- **Updated Firefox** to version **91.9.1**
  Fixes critical CVEs as below:
  CVE-2022-1802: **Prototype pollution in Top-Level Await implementation**
  CVE-2022-1529: **Untrusted input used in JavaScript object indexing, leading to prototype pollution**

Chromium

- Fixed Chromium browser security issues:
  CVE-2022-1876, CVE-2022-1875,
  CVE-2022-1874, CVE-2022-1873, CVE-2022-1872, CVE-2022-1871, CVE-2022-1870, CVE-2022-1869, CVE-2022-1868, CVE-2022-1867, CVE-2022-1866, CVE-2022-1865, CVE-2022-1864, CVE-2022-1863, CVE-2022-1862, CVE-2022-1861, CVE-2022-1860, CVE-2022-1859, CVE-2022-1858, CVE-2022-1857, CVE-2022-1856, CVE-2022-1855, CVE-2022-1854, and CVE-2022-1853
- **Updated** to **Chromium** version **102.0.5005.61**.

New Features 11.07.170

Citrix

- Integrated **Citrix Workspace App 2205**.
  Available Citrix Workspace apps in this release: **2205** (default), **2203** and **2010**
- Added registry keys for Citrix Workspace app 2205:
  - **Authentication enhancement** for Storebrowse:
    More...

Parameter	Disable Authentication enhancement for Storebrowse
Registry	`ica.authman.StorebrowseIPCDisabled`
Value	true / false

    An authentication dialog is present inside Citrix Workspace app and the store details are displayed on the login screen. The authentication tokens are encrypted and stored so that it is not necessary to re-enter credentials when the system or session restarts.

  - **Email-based auto-discovery** of store:
    More...

Parameter	Email-based auto-discovery of store
Registry	`ica.authman.AppConfigEnabled`
Value	true / false

    Automatically discovers the store associated with the email address.
  - **Feature Flag Management**:
    More...

Parameter	Feature flag management
Registry	`ica.module.enablelaunchdarkly`
Value	disable / enable

    For the case an issue occurs with Citrix Workspace app in production, it is possible to disable an affected feature dynamically in Citrix Workspace app during runtime. For that feature flags and a third-party service called LaunchDarkly are used.

Imprivata

- **Improved reconnect/disconnect times** with Imprivata and Horizon
- Added parameter for **inserting Citrix NetScaler cookie**:

More...

Parameter	NetScaler COOKIEINSERT
Registry	`imprivata.cookieinsert`
Type	string

Cisco JVDI Client

- Integrated **Cisco JVDI client 14.1.1**

Cisco Webex

- Integrated **Cisco WebEx Meetings VDI Plugin 42.5.5.9**
  Available Webex Meetings Plugins in this release: **42.5.5.9** (default), **42.3.1.12**, and **41.12.6.12**

Base system

- Updated **glibc** to version **2.31-0ubuntu9.9** with **memcpy** improvements.
- Updated **IGEL EULA** to **version of 1st July 2022**.

Evidian

- Updated **rsUserAuth** to version **1.5.8134**

Remote Management

- Added new **generic UMS job to update HP G5 USB-C docking stations**.
  More...

Parameter	The path to the firmware file on the device
Registry	`update.devices.hp_g5_dock.path`
Value	**/wfs/hp_g5_dock_firmware.cab**
Parameter	Whether the update should proceed even if the provided firmware is older than the current one on the Dock.
Registry	`update.devices.hp_g5_dock.allow_downgrade`
Value	enabled / disabled

Resolved Issues 11.07.170

RD Web Access

- **Fixed virtual channel plugins** in RD Web Access sessions: **PhilipsSpeech**, **deviceTRUST**, **Diktamen**, **Grundig**, **Lakeside**, and **Olympus**.

Imprivata

- Fixed Imprivata **data partition not fully populated/created**.
- Fixed **FUS password not being accepted**.

CUPS Printing

- Fixed **support for usb-to-parallel adapters**

Base system

- Fixed **sporadic firmware downgrade** issues from 11.07 to 11.05.

Conky

- Fixed **special characters** in **custom_text**.

Storage Devices

- Added parameter for **Mobile Device Access USB** to **ignore exposed PTP interface**:
  More...

Parameter	Don't query the PTP interface
Registry	`sessions.mtp-devices0.omit_ptp`
Type	bool
Value	enabled / disabled

X11 system

- Added new registry key to fix issues with **DP MST** handling:
  More...

Parameter	Use new DP MST connector setup name handling.
Tooltip	Use this if you have issues with not getting all displays configured.

Registry	`x.drm_daemon.use_new_dp_mst_handling`
Type	bool
Value	enabled / disabled

Window manager

- Fixed **random restart** of the panel **when dragging around taskbar items**.

Notes for Release 11.07.140

Software:	Version	11.07.140
Release Date:	2022-05-31	
Release Notes:	Version	RN-1107140-1
Last update:	2022-05-27	

- Supported Devices 11.07.140 (see page 2867)
- Component Versions 11.07.140 (see page 2868)
- Known Issues 11.07.140 (see page 2876)
- Security Fixes 11.07.140 (see page 2880)
- New Features 11.07.140 (see page 2883)
- Resolved Issues 11.07.140 (see page 2884)

The Release Notes for IGEL OS 11.07.140 are also available in the following formats:

- Plain text: RNs_11.07.140.txt

Supported Devices 11.07.140

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[280].

280. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.07.140

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	101.0.4951.64-igel1652263123
Cisco JVDI Client	14.1.0
Cisco Webex VDI plugin	42.4.0.21893
Cisco Webex Meetings VDI plugin	41.10.11.5
Cisco Webex Meetings VDI plugin	42.2.4.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Zoom Media Plugin	5.10.0.21068
Zoom Media Plugin	5.4.59458
Zoom Media Plugin	5.9.6.20931
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.02.0.20
Citrix Workspace App	22.03.0.24
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.7789
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0
FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1

FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.9.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1648540238
IGEL AVD Client	1.0.99.7igel1651063614
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.5.6-1igel1647855849
Zulu JRE	8.0.332-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	22.04.0-18.04
ThinLinc Client	4.14.0-2324
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-3igel1644994551
VMware Horizon Client	2203-8.5.0-19586897
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15

Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.9
OpenSSL	1.1.1-1ubuntu2.1~18.04.17
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0igel1647863644
MESA OpenGL stack	21.3.7-1igel1646288715
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-2igel1629135948
Graphics Driver ATI/AMDGPU	22.0.0-1igel1645768768
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.129.06-0ubuntu0.21.10.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0

Kernel	5.15.26 #mainline-lxos-g1652790891
Xorg X11 Server	21.1.3igel1645782509
Xorg Xephyr	21.1.3igel1645782509
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66

WebKit2Gtk	2.34.6-1igel1645163872
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	6.2+dfsg-3igel1646036781

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.20-1igel1645458039
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	320.2 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included

Local Browser (Firefox) Citrix Appliance	81.5 M	Included
VMware Horizon RDP	5.5 M	Included
Cendio ThinLinc	11.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	243.0 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	260.5 M	Not included
Imprivata Appliance	14.2 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	66.5 M	Included
PrinterLogic	47.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	7.5 M	Not included
Elastic Filebeat	22.2 M	Not included

AVD	113.8 M	Included
Local Browser (Chromium)	97.8 M	Not included
Amazon WorkSpaces Client	32.2 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	70.8 M	Not included
Cisco Webex Meetings VDI	111.5 M	Not included
Zoom Media Plugin	124.0 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Fluendo Browser Codec Plugins	4.0 M	Included
HP Factory deployment documentation	88.5 M	Included
Teradici PCoIP Client	15.5 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	65.2 M	Not included

Known Issues 11.07.140

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.

- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only with usage of **local layout and deadkeys enabled**.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).
- **Glibc** has a serious **memcpy performance regression on AMD Zen-based systems**.

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[281] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

281. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Security Fixes 11.07.140

VMware Horizon

- Updated **Horizon Client** to version **2203 8.5.0-19586897**

Teradici PCoIP Client

- Updated **Teradici PCoIP Ultra** client to version **22.04**.

Chromium

- Fixed Chromium browser security issues:
  More...

  CVE-2022-1641, CVE-2022-1640,
  CVE-2022-1639, CVE-2022-1638, CVE-2022-1637, CVE-2022-1636, CVE-2022-1635,
  CVE-2022-1634, CVE-2022-1633, CVE-2022-1501, CVE-2022-1500, CVE-2022-1499,
  CVE-2022-1498, CVE-2022-1497, CVE-2022-1496, CVE-2022-1495, CVE-2022-1494,
  CVE-2022-1493, CVE-2022-1492, CVE-2022-1491, CVE-2022-1490, CVE-2022-1489,
  CVE-2022-1488, CVE-2022-1487, CVE-2022-1486, CVE-2022-1485, CVE-2022-1484,
  CVE-2022-1483, CVE-2022-1482, CVE-2022-1481, CVE-2022-1480, CVE-2022-1479,
  CVE-2022-1478, CVE-2022-1477, CVE-2022-1314, CVE-2022-1313, CVE-2022-1312,
  CVE-2022-1311, CVE-2022-1310, CVE-2022-1309, CVE-2022-1308, CVE-2022-1307,
  CVE-2022-1306, CVE-2022-1305, and CVE-2022-1364
- Updated **Chromium** browser to version **101.0.4951.64**

Firefox

- Updated Mozilla **Firefox** to version **91.9.0 ESR**
- Fixes for **mfsa2022-17**, also known as
  CVE-2022-29914, CVE-2022-29909, CVE-2022-29916,
  CVE-2022-29911, CVE-2022-29912, CVE-2022-29917.
- Fixes for **mfsa2022-14**, also known as
  CVE-2022-1097, CVE-2022-28281, CVE-2022-1196, CVE-2022-28282,
  CVE-2022-28285, CVE-2022-28286, CVE-2022-24713, CVE-2022-28289.
- Fixes for **mfsa2022-11**, also known as
  CVE-2022-26383, CVE-2022-26384, CVE-2022-26387,
  CVE-2022-26381, CVE-2022-26386.

Base system

- Fixed **curl** security issues:
  More...

CVE-2022-2777, CVE-2022-30115, CVE-2022-27782,
CVE-2022-27781, CVE-2022-27780, CVE-2022-27779,
CVE-2022-27778, CVE-2022-27775, CVE-2022-27774, CVE-2022-22576

- Fixed **ghostscript** security issue CVE-2019-25059.
- Fixed **libsdl1.2** security issue CVE-2021-33657.
- Fixed **libsepol** security issues CVE-2021-36087, CVE-2021-36086, CVE-2021-36085, and CVE-2021-36084.
- Fixed **bash** security issue CVE-2019-18276.
- Fixed **zulu8-ca** security issues:
  More...

  CVE-2022-21426, CVE-2022-21434, CVE-2022-21443,
  CVE-2022-21476, CVE-2022-21496, and CVE-2018-25032

- Fixed **rsyslog** security issue CVE-2022-24903.
- Fixed **mysql-5.7** security issues:
  More...

  CVE-2022-21460, CVE-2022-21454, CVE-2022-21451,
  CVE-2022-21444, CVE-2022-21427, and CVE-2022-21417

- Fixed **sqlite3** security issue CVE-2021-36690.
- Fixed **openssl1.0** security issue CVE-2022-1292.
- Fixed **openssl** security issue CVE-2022-1292.
- Fixed **dbus** security issue CVE-2020-35512.
- Fixed **nss** security issue CVE-2020-25648.
- Fixed **dnsmasq** security issue CVE-2022-0934.
- Fixed **cifs-utils** security issues CVE-2022-29869 and CVE-2022-27239.
- Fixed **libxml2** security issue CVE-2022-29824.
- Fixed **cifs-utils** security issues CVE-2022-29869 and CVE-2022-27239.
- Fixed **openldap** security issue CVE-2022-29155.
- Fixed **pcre3** security issues CVE-2020-14155 and CVE-2019-20838.
- Fixed **tiff** security issues:
  More...

  CVE-2022-0891, CVE-2022-0865, CVE-2022-0562,
  CVE-2022-0561, and CVE-2020-35522

- Updated **Intel microcode** to version **20220510**.
- Updated **AMD microcode** to version from **20220408**.
- Fixed security issue CVE-2022-21151.
- Fixed **sshd** security issue CVE-2002-20001 (Denial of Service).
- Added new registry key to **prevent D(HE)ater CVE-2002-20001 DoS attacks**:
  More...

Parameter	Disable Diffie Hellman key exchange algorithms
Registry	`network.ssh_server.disable_dhe_kexalgorithms`
Type	bool

Value	enabled / disabled

- Fixed **Nvidia** security issues CVE-2022-28181, CVE-2022-28182, CVE-2022-28183, and CVE-2022-28184.

New Features 11.07.140

ThinLinc

- Updated **ThinLinc** client to **version 4.14.0**

Chromium

- Changed **Safe Browsing default** value to "**enabled**".

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global > Security**
Parameter	Safe Browsing
Registry	`chromiumglobal.app.safebrowsing_enabled`
Type	bool
Value	enabled / disabled

Smartcard

- Added support for **concurrent usage of multiple smartcard middleware libraries** for authentication with a smartcard to **Active Directory / Kerberos and Citrix**.
  In the Setup on page **Security > Smartcard > Middleware**, multiple libraries can be activated. **If none is activated, OpenSC is taken as fallback.**

Cisco Webex

- Integrated **Cisco WebEx VDI** plugin **42.4.0.21893**

zoomvdi

- Integrated **Zoom VDI** plugin **5.10.0.21068**
  Available plugins in this release: **5.10.0.21068 (default)**, **5.9.6.20931**, and **5.4.59458**

TC Setup (Java)

- Updated **TC Setup** to version **6.10.2**

Resolved Issues 11.07.140

Citrix

- Added parameter for **Citrix Workspace app 2203 Keyboard sync feature**:
  - Parameter to configure new **KeyboardSyncMode** as following.
    Windows Server may require config as well, further information via https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#keyboard-layout-synchronization:
    More...

Parameter	Configure KeyboardSyncMode
Registry	`ica.wfclient.keyboardsyncmode`
Value	no / dynamic / once
Note	**no** – indicates that the client uses the keyboard layout present on the server. **dynamic** – synchronizes the client keyboard layout to the server when client keyboard layout is changed. **once** – when session launches

  - to configure **new KeyboardEventMode**:
    More...

Parameter	Configure KeyboardEventMode
Registry	`ica.wfclient.keyboardeventmode`
Value	Unicode / Scancode
Note	Citrix recommends **"Scancode" for KeyboardSyncMode=no** and **"Unicode" for the other values**.

RDP/IGEL RDP Client 2

- Fixed **RDP drive redirection** redirecting the same drive twice if storage hotplug is set to static.

RD Web Access

- Fixed RD Web **ignoring RD Gateway when starting apps from browser**.

Chromium

- Fixed an issue with the **startup URL containing a '&'** character.

Network

- Fixed **802.1X authentication method PEAP-TLS** - was broken since 11.07.100 due to incompatibility with Network Manager 1.32.

Application Launcher

- Fixed application launcher **starting multiple times if auto-restart was enabled**.

Base system

- Fixed non-working **DRM/KMS driver on Zebra ET51 tablet**.
- Fixed **downgrading from 11.07. to 11.05.** firmware versions
- Fixed **XServer startup for Device Encryption login screen** on devices with Intel-powered graphics, such as H830.

Driver

- Added **bluetooth driver for Realtek RTL8852BE** device.

X11 system

- Add option to **force special handling of Nvidia graphics cards**.
  More...

Parameter	Force X injected DRM data with nvidia driver
Registry	`x.drivers.nvidia.force_quack`
Value	enabled / disabled

X server

- Fixed **detection of** some **Nvidia Quadro T400 graphic cards**.

Remote Management

- **Deallocate resources used for Websocket connection** after closing the connection.
- Added parameter to **control ICG reconnecting**:
  More...

Parameter	Reconnect Interval (seconds)
Registry	`system.remotemanager.reconnect_interval`
Value	20 (default)

Notes for Release 11.07.110

Software:	Version	11.07.110
Release Date:	2022-04-29	
Release Notes:	Version	RN-1107110-1
Last update:	2022-04-29	

- Supported Devices 11.07.110 (see page 2888)
- Component Versions 11.07.110 (see page 2889)
- Known Issues 11.07.110 (see page 2897)
- Security Fixes 11.07.110 (see page 2901)
- New Features 11.07.110 (see page 2902)
- Resolved Issues 11.07.110 (see page 2904)

The Release Notes for IGEL OS 11.07.110 are also available in the following formats:

- Plain text: RNs_1107110.txt

Supported Devices 11.07.110

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[282].

282. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.07.110

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	100.0.4896.75-igel1649171874
Cisco JVDI Client	14.1.0
Cisco Webex VDI plugin	42.2.0.21338
Cisco Webex Meetings VDI plugin	41.10.11.5
Cisco Webex Meetings VDI plugin	42.2.4.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Zoom Media Plugin	5.4.59458
Zoom Media Plugin	5.8.4.21112
Zoom Media Plugin	5.9.6.20931
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	22.02.0.20
Citrix Workspace App	22.03.0.24
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.7789
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0
FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1

FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.6.1
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1648540238
IGEL AVD Client	1.0.99.7igel1651063614
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.5.6-1igel1647855849
Zulu JRE	8.0.322-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	21.03.0-18.04
ThinLinc Client	4.13.0-2172
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	11.12.0+dfsg-3igel1644994551
VMware Horizon Client	2111.1-8.4.1-19480456
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15

Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.8
OpenSSL	1.1.1-1ubuntu2.1~18.04.15
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0igel1647863644
MESA OpenGL stack	21.3.7-1igel1646288715
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-2igel1629135948
Graphics Driver ATI/AMDGPU	22.0.0-1igel1645768768
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.103.01-0ubuntu0.21.10.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0

Kernel	5.15.26 #mainline-lxos-g1647514766
Xorg X11 Server	21.1.3igel1645782509
Xorg Xephyr	21.1.3igel1645782509
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66

WebKit2Gtk	2.34.6-1igel1645163872
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	6.2+dfsg-3igel1646036781

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.20-1igel1645458039
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	320.2 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included

Local Browser (Firefox) Citrix Appliance	81.8 M	Included
VMware Horizon RDP	5.5 M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	216.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	261.0 M	Not included
Imprivata Appliance	14.2 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	66.5 M	Included
PrinterLogic	47.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	7.5 M	Not included
Elastic Filebeat	22.2 M	Not included

AVD	113.8 M	Included
Local Browser (Chromium)	94.2 M	Not included
Amazon WorkSpaces Client	32.2 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	60.0 M	Not included
Cisco Webex Meetings VDI	111.5 M	Not included
Zoom Media Plugin	127.8 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Fluendo Browser Codec Plugins	4.0 M	Included
HP Factory deployment documentation	88.5 M	Included
Teradici PCoIP Client	16.0 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	65.2 M	Not included

Known Issues 11.07.110

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

AVD

- **AVD MS-Teams optimization can crash the AVD client if H264 software decoder is used** (fluh264dec). AVD prefers the hardware decoders (fluvadec) but when there are no hardware decoders or when all hardware decoders are in use already, the software decoder is utilized, which may randomly crash the AVD client. It is likely when it crashes in a certain MS-Teams call, it might crash quite soon again when rejoining the same call. A fix for that is under development.
  A **workaround** is to **disable incoming video** in such MS-Teams calls, which is an option in the "..." menu from the control bar during an active call.

- **H264 hardware decoding for MS-Teams optimization** is currently **limited to non-AMD devices** due to stability issues on AMD devices.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only when using a local layout with deadkeys enabled.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **workaround**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.
- If applications are configured to start after established network connection and network mounts are configured, **spurious "Failed to start application" notifications** may be shown. The applications still start.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware Update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[283] for a possible solution and additional information.

283. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3 M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

---

updating-to-igel-os-11-04-or-higher-32870765.html

Security Fixes 11.07.110

Chromium

- Fixed security issue CVE-2022-1096.
- Fixed security issues:
  CVE-2022-1232, CVE-2022-1146, CVE-2022-1145,
  CVE-2022-1144, CVE-2022-1143, CVE-2022-1142, CVE-2022-1141, CVE-2022-1139,
  CVE-2022-1138, CVE-2022-1137, CVE-2022-1136, CVE-2022-1135, CVE-2022-1134,
  CVE-2022-1133, CVE-2022-1132, CVE-2022-1131, CVE-2022-1130, CVE-2022-1129,
  CVE-2022-1128, CVE-2022-1127, and CVE-2022-1125
- **Updated** Chromium browser to version **100.0.4896.75**

Base system

- Fixed **kernel** security issues CVE-2022-1015 and CVE-2022-1016.
- Fixed **python2.7** security issues CVE-2022-0391 and CVE-2021-4189.
- Fixed **python3.6** security issues CVE-2022-0391, CVE-2021-4189, and CVE-2021-3426.
- Fixed **zlib** security issue CVE-2018-25032.
- Fixed **rsync** security issue CVE-2018-25032.
- Fixed **paramiko** security issue CVE-2022-24302.
- Fixed **xz-utils** security issue CVE-2022-1271.
- Fixed **tcpdump** security issues CVE-2020-8037 and CVE-2018-16301.
- Fixed **gzip** security issue CVE-2022-1271.

New Features 11.07.110

Citrix

- Integrated **Citrix Workspace App 2203**.
- Available Citrix Workspace apps in this release: **2203** (default), **2202** and **2010**
- Added registry keys for Citrix Workspace App 2203:
  - for configuring the **new KeyboardSyncMode**. Windows Server may require config, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#keyboard-layout-synchronization
    More...

Parameter	Configure KeyboardSyncMode
Registry	`ica.wfclient.keyboardsyncmode`
Value	no / dynamic / once
Note:	**no** - Indicates that the client uses the keyboard layout present on the server. **dynamic** - This option synchronizes the client keyboard layout to the server when you change the client keyboard layout. **once** - when the session launches

  - for configuring **new KeyboardEventMode**:
    More...

Parameter	Configure KeyboardEventMode
Registry	`ica.wfclient.keyboardeventmode`
Value	Unicode/ Scancode
Note:	Citrix recommends "**Scancode**" for **KeyboardSyncMode=no** and "**Unicode**" for the other values.

  - Fixed implementation for **DNSCacheEnabled**.

AVD

- Updated **AVD client** to version **1.0.99.7**
- Added and enabled **MS-Teams optimization**

VMware Horizon

- Added system-wide handler to **start links which use the vmware-view protocol**.
  View session can now be **started by Chromium or** any **other application** which **uses xdg-open**.
- Updated **Horizon Client** to version **2111.1-8.4.1-19480456** which **fixes the typematic (key-repeat)** issue

Wi-Fi

- Added support for **Realtek 8852be WiFi cards**.

Cisco JVDI Client

- Updated **Cisco JVDI** to version **14.1.0**

Base system

- Added new field netmask to **SystemInformationLog** - only relevant for specific customer.

zoomvdi

- Updated **Zoom Media Plugin** to version **5.9.6.20931**
  Available Zoom Media Plugins in this release: **5.4.59458**, **5.8.4.21112**, and **5.9.6.20931**

Resolved Issues 11.07.110

Citrix

- Fix for **Self-Service enumeration** problem with consecutive users **when Multi user is off**. Introduced new parameters to **enable cleanup after Self-Service termination**:
  More...

Parameter	Clean up UI cache after Self-Service termination
Registry	`ica.selfservice.cleanupwebui`
Value	false / true
Parameter	Clean up Store cache after Self-Service termination
Registry	`ica.selfservice.cleanupstore`
Value	false / true

RD Web Access

- Fixed RD Web Access **autostart error**.

Chromium

- Fixed **custom downloads** not working **when the path was invalid**
- Fixed '**custom location**' for Chromium Browser downloads

Imprivata

- Fixed VMware **disconnect delay**

HID

- Fixed issues with **non working touchpads**, **touchscreens**, and **multimedia keys**.

CUPS Printing

- Fixed **printer selection by pattern** where manufacturer or product pattern could be left empty.

Base system

- Fixed **loss of settings on certain hardware devices** after update from a 11.05.xxx or older firmware version.
- Fixed **reliability of power off** in case **UD Pocket** stick is removed.
- Fixed / stabilized **factory reset with enabled device encryption**.

Driver

- Fixed **Olympus Dictation** devices **DS-5000**, **DS-7000**, and **DS-9500** buttons disturbing client side window handling.

Hardware

- Fixed non working **Bluetooth with Mediatek MT7961**.
- Fixed issue with **suspend/resume on Lenovo K14 Gen1 with Mediatek WiFi card**.

Remote Management

- Reduced **UMS communication load for asset inventory tracker (AIT)** feature.

Notes for Release 11.07.100

Software:	Version	11.07.100
Release Date:	2022-03-29	
Release Notes:	Version	RN-1107100-1
Last update:	2022-03-29	

- Supported Devices 11.07.100 (see page 2907)
- Component Versions 11.07.100 (see page 2908)
- Known Issues 11.07.100 (see page 2916)
- Security Fixes 11.07.100 (see page 2919)
- New Features 11.07.100 (see page 2923)
- Resolved Issues 11.07.100 (see page 2930)

The Release Notes for IGEL OS 11.07.100 are also available in the following formats:

- Plain text: RNs_1107100.txt
- HTML: lxos_11.07.100.html

Supported Devices 11.07.100

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[284].

284. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.07.100

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	99.0.4844.74-igel1647438342
Cisco JVDI Client	14.0.3
Cisco Webex VDI plugin	42.2.0.21338
Cisco Webex Meetings VDI plugin	41.10.11.5
Cisco Webex Meetings VDI plugin	42.2.4.12
Cisco Webex Meetings VDI plugin	42.3.1.12
Zoom Media Plugin	5.4.59458
Zoom Media Plugin	5.8.4.21112
Zoom Media Plugin	5.9.0.20720
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	21.11.0.20
Citrix Workspace App	21.12.0.18
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.7789
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.8.0
FabulaTech USB for Remote Desktop	6.0.35
FabulaTech Scanner for Remote Desktop	2.7.0.1

FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.6.1
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1643693920
IGEL AVD Client	1.0.39igel1646773894
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.8.2-4igel1644853628
Open VPN	2.5.6-1igel1647855849
Zulu JRE	8.0.322-1
Parallels Client	18.3.1
Spice GTK (Red Hat Virtualization)	0.39-3igel1633543285
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.11.0-2igel1633506980
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.6.0-3
Systancia AppliDis	6.0.0-4
Teradici PCoIP Software Client	21.03.0-18.04
ThinLinc Client	4.13.0-2172
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.12.0+dfsg-3igel1644994551
VMware Horizon Client	2111-8.4.0-18957622
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29
Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.2
Philips Speech driver	13.1.10

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.10
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	8.0.13
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.22.0-2igel1643799581
PKCS#11 Library SecMaker NetID Enterprise	6.8.3.21
PKCS#11 Library SecMaker NetID Client	1.0.2.67
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.5.0-2igel1646035471
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15

Resource Manager PC/SC Lite	1.9.5-3igel1646034250
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.8
OpenSSL	1.1.1-1ubuntu2.1~18.04.15
OpenSSH Client	8.9p1-3igel1646033299
OpenSSH Server	8.9p1-3igel1646033299
Bluetooth stack (bluez)	5.64-0igel1647863644
MESA OpenGL stack	21.3.7-1igel1646288715
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20210115-1igel1647326046
Graphics Driver ATI/RADEON	19.1.0-2igel1629135948
Graphics Driver ATI/AMDGPU	22.0.0-1igel1645768768
Graphics Driver Nouveau (Nvidia Legacy)	1.0.17-2igel1644486678
Graphics Driver Nvidia	470.103.01-0ubuntu0.21.10.1
Graphics Driver VMware	13.3.0-3igel1628859075
Graphics Driver QXL (Spice)	0.1.5-2build1igel1634304534
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1igel1628504011
Input Driver Evdev	2.10.6-2igel1629196047
Input Driver Elographics	1.4.2-1igel1629196349
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-2igel1646823146
Input Driver VMMouse	13.1.0-1ubuntu2igel1628499891
Input Driver Wacom	0.39.0-0ubuntu1igel1629136980
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0

Kernel	5.15.26 #mainline-lxos-g1647852051
Xorg X11 Server	21.1.3igel1645782509
Xorg Xephyr	21.1.3igel1645782509
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66

WebKit2Gtk	2.34.6-1igel1645163872
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.32-dfsg-1igel1643178233
Virtualbox X11 Guest Utils	6.1.32-dfsg-1igel1643178233
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.22.1-1igel1646032976
Qemu Guest Agent	6.2+dfsg-3igel1646036781

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.19-1igel1633453264
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.20-1igel1645458039
Scanner support	1.0.27-1
VirtualBox VM within IGEL OS	6.1.32-dfsg-1igel1643178233

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.5 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	311.0 M	Included
Ericom PowerTerm InterConnect	10.2 M	Included
Media Player	512.0 K	Included

Local Browser (Firefox) Citrix Appliance	81.8 M	Included
VMware Horizon RDP	5.5 M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	27.2 M	Included
VMware Horizon	216.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	2.8 M	Included
Parallels Client	6.0 M	Included
NVIDIA graphics driver	261.0 M	Not included
Imprivata Appliance	14.2 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	14.2 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.8 M	Included
Cisco JVDI client	66.2 M	Included
PrinterLogic	47.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	7.5 M	Not included
Elastic Filebeat	22.2 M	Not included

AVD	105.8 M	Included
Local Browser (Chromium)	94.2 M	Not included
Amazon WorkSpaces Client	32.2 M	Included
deskMate client	5.8 M	Included
Cisco Webex VDI	60.0 M	Not included
Cisco Webex Meetings VDI	111.5 M	Not included
Zoom Media Plugin	127.8 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Fluendo Browser Codec Plugins	4.0 M	Included
HP Factory deployment documentation	88.5 M	Included
Teradici PCoIP Client	16.0 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0 K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	65.2 M	Not included

Known Issues 11.07.100

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** in combination with Citrix. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** on an **AMD GPU with enabled Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- Currently, **H.264** for Citrix sessions **cannot be used in parallel with video input acceleration**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required** for deployment of IGEL OS 11.06. and later.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.

- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.
  This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
  The respective settings can be found in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`
- **Keyboard Input Source Language Synchronization** works only when using a local layout with deadkeys enabled.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices** can be enabled at the same time, but this could lead to sporadical problems.
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, means USB redirection is not used for these devices then. However, in case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **work-around**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Attached storage devices appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

- **Update from memory stick requires network online state** (at least when multiple update stages are triggered / necessary).

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly.
  Workaround: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920).

Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[285] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character).
  Workaround: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3-M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

285. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Security Fixes 11.07.100

Chromium

- Fixed **chromium-browser** security issues:
  More...

  CVE-2021-37973, CVE-2021-37972,
  CVE-2021-37971, CVE-2021-37970, CVE-2021-37969, CVE-2021-37968,
  CVE-2021-37967, CVE-2021-37966, CVE-2021-37965, CVE-2021-37964,
  CVE-2021-37963, CVE-2021-37962, CVE-2021-37961, CVE-2021-37960,
  CVE-2021-37959, CVE-2021-37958, CVE-2021-37957, CVE-2021-37956,
  CVE-2021-30633, CVE-2021-30632, CVE-2021-30631, CVE-2021-30630,
  CVE-2021-30629, CVE-2021-30628, CVE-2021-30627, CVE-2021-30626,
  CVE-2021-30625, CVE-2021-30624, CVE-2021-30623, CVE-2021-30622,
  CVE-2021-30621, CVE-2021-30620, CVE-2021-30619, CVE-2021-30618,
  CVE-2021-30617, CVE-2021-30616, CVE-2021-30615, CVE-2021-30614,
  CVE-2021-30613, CVE-2021-30612, CVE-2021-30611, CVE-2021-30610,
  CVE-2021-30609, CVE-2021-30608, CVE-2021-30607, CVE-2021-30606,
  CVE-2021-30604, CVE-2021-30603, CVE-2021-30602, CVE-2021-30601,
  CVE-2021-30600, CVE-2021-30599, CVE-2021-30598, CVE-2021-30597,
  CVE-2021-30596, CVE-2021-30594, CVE-2021-30593, CVE-2021-30592,
  CVE-2021-30591, CVE-2021-30590, CVE-2021-30589, CVE-2021-30588,
  CVE-2021-30587, CVE-2021-30586, CVE-2021-30585, CVE-2021-30584,
  CVE-2021-30583, CVE-2021-30582, CVE-2021-30581, CVE-2021-30580,
  CVE-2021-30579, CVE-2021-30578, CVE-2021-30577, CVE-2021-30576,
  CVE-2021-30575, CVE-2021-30574, CVE-2021-30573, CVE-2021-30572,
  CVE-2021-30571, CVE-2021-30569, CVE-2021-30568, CVE-2021-30567,
  CVE-2021-30566, CVE-2021-30565, CVE-2021-37976, CVE-2021-37975,
  CVE-2021-37974, CVE-2021-37977, CVE-2021-37979, CVE-2021-37980,
  CVE-2021-37981, CVE-2021-37982, CVE-2021-37983, CVE-2021-37984,
  CVE-2021-37985, CVE-2021-37986, CVE-2021-37987, CVE-2021-37988,
  CVE-2021-37989, CVE-2021-37990, CVE-2021-37991, CVE-2021-37992,
  CVE-2021-37993, CVE-2021-37996, CVE-2021-37994, CVE-2021-37995,
  CVE-2021-38003, CVE-2021-38002, CVE-2021-38001, CVE-2021-38000,
  CVE-2021-37999, CVE-2021-37998, and CVE-2021-37997

Base system

- Fixed **binutils** security issues CVE-2021-3487 and CVE-2020-16592.
- Fixed **bind9** security issues CVE-2021-25219 and CVE-2021-25220.
- Fixed **libcaca** security issues CVE-2021-30499 and CVE-2021-30498.
- Fixed **icu** security issue CVE-2020-21913.
- Fixed **mysql-5.7** security issues:
  More...

  CVE-2021-35624, CVE-2021-35604, CVE-2022-21367,
  CVE-2022-21344, CVE-2022-21304, CVE-2022-21303,
  CVE-2022-21270, and CVE-2022-21245

- Fixed **postgresql-10** security issues CVE-2021-23222 and CVE-2021-23214.
- Fixed **nfs-utils** security issue CVE-2019-3689.

- Fixed **openssh** security issue CVE-2021-41617.
- Fixed **qemu** security issues:
  More...

  CVE-2021-3748, CVE-2021-3713, CVE-2021-3682,
  CVE-2021-3638, CVE-2021-3608, CVE-2021-3607, CVE-2021-3582, CVE-2021-3546,
  CVE-2021-3545, CVE-2021-3544, CVE-2021-3527, CVE-2021-3416, CVE-2021-3409,
  CVE-2021-3392, CVE-2021-20263, CVE-2021-20257, CVE-2021-20221, CVE-2021-20181,
  CVE-2020-35517, CVE-2020-35506, CVE-2020-35505, CVE-2020-35504,
  CVE-2020-29443, CVE-2020-25085, CVE-2020-17380, CVE-2021-20203,
  CVE-2021-20196, CVE-2021-20255, and CVE-2021-4158

- Fixed **tpm2-tools** security issue CVE-2021-3565.
- Fixed **chromium-browser** security issues:
  More...

  CVE-2021-38022, CVE-2021-38021,
  CVE-2021-38020, CVE-2021-38019, CVE-2021-38018, CVE-2021-38017,
  CVE-2021-38016, CVE-2021-38015, CVE-2021-38014, CVE-2021-38013,
  CVE-2021-38012, CVE-2021-38011, CVE-2021-38010, CVE-2021-38009,
  CVE-2021-38008, CVE-2021-38007, CVE-2021-38006, CVE-2021-38005, CVE-2021-4102,
  CVE-2021-4101, CVE-2021-4100, CVE-2021-4099, CVE-2021-4098, CVE-2021-4078,
  CVE-2021-4068, CVE-2021-4066, CVE-2021-4065, CVE-2021-4064, CVE-2021-4063,
  CVE-2021-4062, CVE-2021-4059, CVE-2021-4058, CVE-2021-4057, CVE-2021-4056,
  CVE-2021-4055, CVE-2021-4054, CVE-2021-4053, CVE-2021-4052, CVE-2022-0120,
  CVE-2022-0118, CVE-2022-0117, CVE-2022-0116, CVE-2022-0115, CVE-2022-0114,
  CVE-2022-0113, CVE-2022-0112, CVE-2022-0111, CVE-2022-0110, CVE-2022-0109,
  CVE-2022-0108, CVE-2022-0107, CVE-2022-0106, CVE-2022-0105, CVE-2022-0104,
  CVE-2022-0103, CVE-2022-0102, CVE-2022-0101, CVE-2022-0100, CVE-2022-0099,
  CVE-2022-0098, CVE-2022-0097, CVE-2022-0096, CVE-2022-0311, CVE-2022-0310,
  CVE-2022-0309, CVE-2022-0308, CVE-2022-0307, CVE-2022-0306, CVE-2022-0305,
  CVE-2022-0304, CVE-2022-0302, CVE-2022-0301, CVE-2022-0300, CVE-2022-0298,
  CVE-2022-0297, CVE-2022-0296, CVE-2022-0295, CVE-2022-0294, CVE-2022-0293,
  CVE-2022-0292, CVE-2022-0291, CVE-2022-0290, CVE-2022-0289, CVE-2022-0980,
  CVE-2022-0979, CVE-2022-0978, CVE-2022-0977, CVE-2022-0976, CVE-2022-0975,
  CVE-2022-0974, CVE-2022-0973, CVE-2022-0972, and CVE-2022-0971

- Fixed **vim** security issues:
  More...

  CVE-2021-3928, CVE-2021-3927, CVE-2021-3903,
  CVE-2021-4069, CVE-2021-4019, and CVE-2021-3984

- Fixed **hivex** security issue CVE-2021-3504.
- Fixed **heimdal** security issue CVE-2021-3671.
- Fixed **nss** security issue CVE-2021-43527.
- Fixed **glib2.0** security issue CVE-2021-3800.
- Fixed **python3.6** security issues CVE-2021-3737 and CVE-2021-3733.
- Fixed **samba** security issues:
  More...

  CVE-2021-3671, CVE-2020-25722, CVE-2020-25717,
  CVE-2016-2124, and CVE-2021-44142

- Fixed **xorg-server** security issues CVE-2021-4011, CVE-2021-4010, CVE-2021-4009, and CVE-2021-4008.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2021-30809, CVE-2021-30836, CVE-2021-30818, CVE-2021-30823, CVE-2021-30884, CVE-2021-30888, CVE-2021-30889, CVE-2021-30897, CVE-2021-30887, CVE-2021-30890, CVE-2021-45482, CVE-2021-45481, CVE-2021-45483, CVE-2021-30934, CVE-2021-30936, CVE-2021-30951, CVE-2021-30952, CVE-2021-30953, CVE-2021-30954, CVE-2021-30984, CVE-2022-22592, CVE-2022-22590, CVE-2022-22589, and CVE-2022-22620
- Fixed **policykit-1** security issue CVE-2021-4034.
- Fixed **bluez** security issues CVE-2021-43400 and CVE-2021-41229.
- Fixed **ghostscript** security issues CVE-2021-45949 and CVE-2021-45944.
- Fixed **lxml** security issue CVE-2021-43818.
- Fixed **pillow** security issues:
  More...

  CVE-2022-22817, CVE-2022-22816, CVE-2022-22815, CVE-2021-34552, and CVE-2021-23437
- Fixed **systemd** security issue CVE-2021-3997.
- Fixed **bubblewrap** security issue CVE-2020-5291.
- Fixed **libgcrypt20** security issues CVE-2021-40528, CVE-2021-33560, and CVE-2019-13627.
- Fixed **ntfs-3g** security issues:
  More...

  CVE-2021-39263, CVE-2021-39262, CVE-2021-39261, CVE-2021-39260, CVE-2021-39259, CVE-2021-39258, CVE-2021-39257, CVE-2021-39256, CVE-2021-39255, CVE-2021-39254, CVE-2021-39253, CVE-2021-39252, CVE-2021-39251, CVE-2021-35269, CVE-2021-35268, CVE-2021-35267, CVE-2021-35266, CVE-2021-33289, CVE-2021-33287, CVE-2021-33286, and CVE-2021-33285
- Fixed **cifs-utils** security issues CVE-2021-20208 and CVE-2020-14342.
- Fixed **qtsvg-opensource-src** security issues CVE-2021-45930, CVE-2021-3481, and CVE-2018-19869.
- Fixed **shadow** security issue CVE-2018-7169.
- Fixed **ldns** security issues CVE-2020-19861 and CVE-2020-19860.
- Fixed **expat** security issues:
  More...

  CVE-2022-23990, CVE-2022-23852, CVE-2022-22827, CVE-2022-22826, CVE-2022-22825, CVE-2022-22824, CVE-2022-22823, CVE-2022-22822, CVE-2021-46143, CVE-2021-45960, CVE-2019-15903, CVE-2018-20843, CVE-2013-0340, CVE-2022-25315, CVE-2022-25314, CVE-2022-25313, CVE-2022-25236, and CVE-2022-25235
- Fixed **libvirt** security issues CVE-2021-4147 and CVE-2021-3667.
- Fixed **libproxy** security issues CVE-2020-26154 and CVE-2020-25219.
- Fixed **libssh** security issues:
  More...

CVE-2020-1730, CVE-2019-14889, CVE-2018-10933,
CVE-2021-3634, and CVE-2020-16135

- Fixed **speex** security issue CVE-2020-23903.
- Fixed **libxml2** security issue CVE-2022-23308.
- Fixed **cyrus-sasl2** security issue CVE-2022-24407.
- Fixed **glibc** security issues:
  More...

  CVE-2022-23219, CVE-2022-23218, CVE-2021-3999,
  CVE-2021-35942, CVE-2021-3326, CVE-2021-27645, CVE-2020-6096, CVE-2020-29562,
  CVE-2020-27618, CVE-2019-25013, and CVE-2016-10228
- Fixed **openssl1.0** security issue CVE-2022-0778.
- Fixed **openssl** security issue CVE-2022-0778.
- Fixed **tar** security issue CVE-2021-20193.
- Fixed **openvpn** security issue CVE-2022-0547.
- Fixed **duplicated User IDs**.
- Fixed **kernel** security issue CVE-2022-0847, also **known as Dirty Pipe**.
- Fixed security issues CVE-2021-0127 and CVE-2021-0146 via **updated intel-microcode** to version **20220207**

New Features 11.07.100

Citrix

- Changed: For **Browser Content Redirection**, the **Chromium Embedded Framework** is used by default now - Parameter `ica.allregions.usecefbrowser` is set to **true** (as default).
- Added **Citrix Workspace App 2112**
  Available Citrix Workspace Apps in this release: 2112 (default), 2111, and 2010
- New features:
  - The **cursor color inverts based on the background color of a text**.
    More...

Parameter	Support for cursor color inverting
Registry	`ica.wfclient.invertcursorenabled`
Value	false / true

  - Enhancement on **smartcard support**.
    More...

Parameter	SmartCard driver
Registry	`ica.module.VirtualDriver.SmartCard.drivername`
Value	VDSCARD.DLL / VDSCARDV2.DLL
Note	VDSCARDV2.DLL supports the Plug and Play functionality for smartcard reader

  - The **PulseAudio library** is **used instead of ALSA** to access multiple audio devices within a session (Experimental).
    More...

Parameter	Multiple Audio Device support
Registry	`ica.module.audioredirectionv4`
Value	false / true

- Note: The **VdcamVersion4Support** is **renamed** to **AudioRedirectionV4**, so registry key `ica.module.vdcamversion4support` is removed.
- **UDP audio through Citrix Gateway** (Experimental).
  More...

Parameter	UDP audio through Citrix Gateway
Registry	`ica.module.enableudpthroughgateway`
Value	false / true

- **Webcam redirection for 64-bit apps** (Technical Preview)
  For 64-bit webcam redirection, the following parameters must be enabled:
  `ica.wfclient.allowaudioinput = True` (default)
  `ica.wfclient.hdxh264inputenabled = True`
- Added a registry key to enable **hardware acceleration for webcam redirection with 64-bit applications**. The effect is based on prerequisites as following:
  `ica.wfclient.allowaudioinput=true`
  (default), `ica.wfclient.hdxh264inputenabled=true`,
  `ica.wfclient.hdxwebcamenabled=true` and available acceleration hardware plus license.
  More...

Parameter	Enable gstreamer input hardware encoder
Registry	`ica.wfclient.gstread_encoder`
Value	false / true

- **Known issue**: Currently, **H.264 for Citrix sessions in parallel with the above video acceleration will fail**, only either or is possible.
- Updated **signotec Virtual Channel Driver** to version **8.0.10**

AVD

- Added **global proxy setting via Automatic Proxy Configuration** (`pac` file).
- The following parameters need to be set accordingly:
  More...

IGEL Setup	**Network > Proxy**
Parameter	Automatic proxy configuration
IGEL Setup	**Sessions > AVD > AVD Sessions > AVD Session > Proxy**
Parameter	Global Proxy Setting

- Added **version notification when new IGEL AVD client versions are available**. To disable the notification, the following parameter has been added:
  More...

Registry	`sessions.wvd%.options.version-check`
Value	enabled / disabled

Parallels Client

- Updated **Parallels client** to version **18.3.1**

NX client

- Updated **NX client** to version **7.8.2**

Chromium

- **Removed** support for **TLS 1.0 and 1.1**.
- Updated **Chromium** Browser to version **99.0.4844.74**.

Firefox

- Updated **Mozilla Firefox** to version **91.6.1 ESR**.

Network

- Updated **Network Manager** to version **1.32**.

Wi-Fi

- Updated **Network Manager** to version **1.32**.
- Added **ath11k** Wi-Fi driver.
- Updated **wpa_supplicant** to version **2.10**.

Smartcard

- Updated **cryptovision sc/interface** to version **8.0.13**. Changes are:
  - Support for CardOS 5.4 / 5.5
  - Support for DTRUST 4.x
  - Support for Bayern-PKI Legacy-Karte
  - Support for ePasslet-Suite-3.5 on NXP JCOP4
  - Integration of CardOS based "PKIBw-Karte 7.1" (tPKI)
- Added new **smartcard middleware SecMaker Net iD Client**. The existing middleware **SecMaker Net iD** remains in the firmware and is **renamed to SecMaker Net iD Enterprise** (no need for configuration changes).
  More...

IGEL Setup	**Security > Smartcard > Middleware**
Parameter	Secmaker Net iD Client
Registry	`scard.pkcs11.use_netid-client`
Value	false / true

IGEL Setup	**Sessions > Horizon Client > Horizon Client Global > Smartcard**
Parameter	Horizon logon with SecMaker Net iD Client smartcards
Registry	`vmware.view.pkcs11.use_netid-client`
Value	false / true

IGEL Setup	**Sessions > Firefox Browser > Firefox Browser Global > Smartcard Middleware**
Parameter	SecMaker Net iD Client Security Device

Registry	`browserglobal.security_device.use_netid-client`
Value	false / true
IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**
Parameter	SecMaker Net iD Client Security Device
Registry	`chromiumglobal.security_device.use_netid-client`
Value	false / true

- Updated **Athena IDProtect smartcard library** to version **7-20210902**. This fixes smartcard logon using Horizon client and CRYPTAS TicTok v2 cards.
- Added configuration parameters for options of **PC/SC lite smartcard daemon** which are needed in some cases:
  More...

Parameter	Maximum number of threads
Registry	`scard.pcscd.max_thread`
Value	200 (default)

Parameter	Maximum number of card handles per thread
Registry	`scard.pcscd.max_card_handle_per_thread`
Value	200 (default)
Parameter	Maximum number of card handles per reader
Registry	`scard.pcscd.max_card_handle_per_reader`
Value	200 (default)

Parameter	Keep card always powered on
Registry	`scard.pcscd.power_on`
Value	false (default)

Cisco Webex

- Updated **Cisco WebEx VDI plugin** to version **42.2**
- Updated **Cisco WebEx Meeting VDI plugins**. Available plugins in this release: **42.3.1.12** (default), **42.2.4.12**, and **41.10.11.5**

Base system

- Added support for **Thai keyboard layout and localization**.
- Updated **kernel** to version **5.15.26**
- Fixed security issue **CVE-2022-0185**.
- Updated **intel-microcode** to version **20220207** to fix security issues CVE-2021-0127 and CVE-2021-0146.
- Updated **mesa** to version **21.3.7**.
- Switched to **Ubuntu Focal version** of **glibc**.
- Switched to **Ubuntu Focal version** of **libstdc++6**
- Updated **HP documentation for devices deployed directly by HP**.
- Added new registry key to include **systemd** information **in the support files**.
  More...

Parameter	Collect systemd information for support files
Registry	`debug.collect_sysd_info_for_support`
Value	enabled / disabled

- Added new registry key to include **systemd-analyze plot in the support files**.
  More...

Parameter	Include systemd-analyze plot svg-image in support files
Registry	`debug.create_sysd_plot_for_support`
Value	enabled / disabled

- **Teradici PCoIP Client** does **not require an Add-On license anymore**, this is now part of the Workspace Edition license.
- Added new registry key to **switch between the default (igel) and the unchanged asound2 pulse plugin** type:
  More...

Parameter	Asound2 plugins type
Registry	`multimedia.alsa.asound2_plugin_type`
Range	[default] [igel] [vanilla]

CID Key Agent

- Updated **Stratusphere UX Agent** to version **6.6.0-3**

Driver

- Updated **Philips Speech dictation drivers** to version **13.1.10**. Changes are amongst others:
  - Increased robustness in session switching/roaming use cases
  - Support of Philips SmartMike Duo USB devices
  - RDP plugins now use native freerdp instead of elusiva interface

X server

- Updated **Xorg** server to version **21.1**

Window manager

- Added: The l**ocation of the notification pop-up window** is now configurable.
  More...

Parameter	Location of notifications
Registry	`windowmanager.wm%.variables.notifications.location`
Range	[Top left] [Bottom left] [Top right] [Bottom right] [Center]

Audio

- Added audio support for **LG AiO with Realtek ALC256 chipset**.
- Updated **EPOS** Connect to version **7.0.0.19714**.

Multimedia

- Added a parameter to control the **webcam powerline frequency**. The "**Auto**" option **uses the camera's default settings**.
  More...

IGEL Setup	**Registry > multimedia > webcam**
Parameter	powerline_frequency
Registry	`multimedia.webcam.powerline_frequency`
Range	[Auto] [50 HZ] [60 HZ]

zoomvdi

- Updated **Zoom VDI plugin** to version **5.9.0.20720**
  Available plugins in this release: **5.9.0.20720** (default), **5.8.4.21112**, and **5.4.59458**

Misc

- Added **representation of all systemd-units installed in the firmware** is **now included in the support_information**, which can be created in the UMS.

Hardware

- Added **HP mt46 Mobile Thin Client** into supported hardware list.
- Updated **NVIDIA** driver to version **470.86**.
- Added **gddccontrol** to **control monitor parameters** like brightness, contrast, and so on.

TC Setup (Java)

- Updated **TC Setup** to version **6.10.1**.

Remote Management

- Added: Transfer **details** (MAC addresses etc.) **of all available network adapters**.

- Added support for **device-specific attributes defined by the UMS**. The list of device attributes is received from the UMS during boot. To access the data, the new rmagent commands are available:

/sbin/rmagent-devattrs-enum
Enumerate the list in the form: **ATTR_NAME:ATTR_TYPE:ATTR_VALUE**. The enumeration is ordered according to the attribute's order id.

/sbin/rmagent-devattrs-enum-range \<ATTR_NAME>
Enumerate entries of the given range. The enumeration is ordered according to the range item's order id.

/sbin/rmagent-devattrs-get-type \<ATTR_NAME>
Print type of the given attribute. Known types are string, number, data or range.

/sbin/rmagent-devattrs-get \<ATTR_NAME>
Print value of the given attribute.

/sbin/rmagent-devattrs-set \<ATTR_NAME> \<ATTR_VALUE>
Set the given attribute to the specified value. The command doesn't check value type but permission rule defined for the attribute.

/sbin/rmagent-devattrs-reset \<ATTR_NAME>
Reset the given attribute, the attribute doesn't have then an empty value.

/sbin/rmagent-devattrs-sync
Calculate current checksum and send the attribute list to the UMS if the checksum is different than the sum received from the UMS.

/sbin/rmagent-write-device-attributes
Send the attribute list to the UMS.

As attribute name, the UMS internal name of the attribute must be used. See Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You (see page 2923).

Fabulatech

- Updated **Fabulatech USB Redirection Client** plugins to **3.8.0**
- Updated **FabulaTech USB for Remote Desktop** to version **6.0.35**.
- Added: **FabulaTech device redirection** now **works with Horizon Blast**

Resolved Issues 11.07.100

Citrix

- With **CWA 2012**, **Citrix** has **revised** the **client drive mapping**, with which we can no longer preset the right of the drives. Since then, the user can assign these rights in the session itself. So that this selection remains also over a
reboot, we store the necessary file persistently on our system.
- Updated **window manager** so that the proxy Authentication window comes to the foreground and is focused when the Citrix Brower content redirection with Cef is used.
- Fixed **window settings** for Citrix Desktop sessions
- Added parameter for **Browser Content Redirection with CEF** to enable global proxy support. **More...**

Parameter	Browser content redirection with CEF via proxy
Registry	`ica.module.virtualdriver.webpageredirection.cef_proxy_env`
Value	true / false

- Fixed **multimedia support** for Citrix **when used HWA in Firefox**.
- Fixed **high CPU load in MS Teams** and **Citrix Workspace App 2112**.

OSC Installer

- Fixed **OSC Recovery with enabled "Migrate Old Settings"**
- Fixed OSC issue with **bogus character in license type field and not shown add-on licenses**.
- Fixed returning to installer after **closing Factory ID window**.

AVD

- Added several **performance optimizations**.

RDP/IGEL RDP Client 2

- Fixed **wrong error message** when RDP session was closed by idle timeout.

RD Web Access

- Fixed RD Web Access **windows moving out of the screen**.
- Fixed **downloading published applications**.

Parallels Client

- Fixed **multi-monitor** issues.

X session (Xephyr)

- Fixed **segfault with xdmcp sessions** to an OpenVMS environment.
- Fixed **fullscreen and workarea x sessions** that are **expanded over 2 or more monitors**: The session window opens properly and the single monitors are detected inside the x session.
- Fixed **host chooser button events** in x sessions with connection type "indirect via localhost".

Firefox

- Fixed usage of **Athena IDProtect** smartcards.
- Fixed **usage of IGEL extensions when private browsing is enabled**. These are important to set restricted kiosk mode settings.
- Fixed installed **translations for user interface**.
- Fixed **download prevention with restricted / hidden file system access**. Without the fix, the current browser implicitly put the file into the standard Downloads folder - without the possibility to interfere.
- Fixed **crash** which always occurred **during the internal probing of 3D support for WebGL**. So WebGL is now available again for the supported display drivers.
- Fixed client **certificate management via IGEL TC Setup**. Firefox's standard certificate dialog is used now.

Chromium

- Fixed **comma-separated strings in custom policies** broke some Chromium Browser policies.
- Fixed **emojis have not been loaded** in Chromium (also affects Chromium Embedded Framework).
- **Removed "What's new" tab** showing on the first start and after Chromium updates.

Network

- Fixed **could not mount** issue **with some NFS 4.1 and 4.2 servers (QNAP)**.
- Fixed **global no-proxy list** getting effective via gconf2. This e.g. can help Citrix Workspace App using the right proxy configuration.
- **Removed** now **unsupported samba security modes** (NTLM, NTLMi, and LanMan) as these would cause mount failures. This removes also support for very old SMB v1 servers. Changed the following registry key to:
  More...

Parameter	Security Mode
Registry	`network.smbmount%.security_mode`
Range	[default] [ntlmv2] [NTLMSSP] [ntlmv2i] [NTLMSSPi]

Wi-Fi

- Added setup registry key to **select between wpa_supplicant/iwd as Wireless back-end**.
- **AVM Fritz!WLAN N v2 USB Stick**, only works with iNet Wireless Daemon (iwd) as Wi-Fi back-end.
  More...

Parameter	Wi-Fi backend
Registry	`network.interfaces.wirelesslan.wireless_backend`
Range	[iNet Wireless Daemon (iwd)]
Value	Wi-Fi Protected Access client and IEEE 802.1X supplicant (wpa_supplicant)

- Fixed issue with **TP-Link AC600** not working on 5GHz (8821au driver).
- Improved **reconfiguring regulatory domain** settings at runtime

Open VPN

- Added **config parameter for extending arguments of VPN command**:
  More...

Registry	`sessions.openvpn%.vpnopts.extend_opts`
Value	extend parameter as string

- Enter parameter starting with `--`.
  Example: `` `--ping 10 --ping-restart 120` ``
- Parameters that are already set in the GUI must not be used.

Imprivata

- Fixed **Imprivata data partition**: remove outdated artefacts, keep latest version of the configuration-editor

Smartcard

- Added **option to unlock screen lock in case of Kerberos smartcard login** by only checking the PIN of the smart card.
  More...

Parameter	Only check smartcard PIN on unlock
Registry	`auth.login.pkcs11_screenlock_unlock`
Value	false / true

- Fixed: Maximum **number of simultaneous smartcard context**s were **raised in smartcard resource manager PC/SC lite**.

HID

- **Changed default** of `userinterface.touchpad.tapping.TapButton1` registry key **to 1** so tapping is active as default again (if set to 0 tapping is disabled).

CUPS Printing

- Fixed handling of **more than one printer and printer selection by USB IDs.**
  - Fixed **classification of some HP printers as scanners only** which made printing impossible because of missing access rights.
- Fixed **TCP/IP print server** functionality **with USB printers**. Printing was not possible in some cases, e.g. when certain other USB devices were connected.

Base system

- Added driver for several **Intel SOC NVME controller**. Required for e.g. HP G8 250.
- Added new parameter for **custom font path configuration**. Add a new instance for each custom font path:
  More...

Parameter	Enable Custom Font Path

Registry	`x.fontpaths.custom<instance nr>.enabled`
Value	enabled / disabled
Parameter	Custom Font Path
Registry	`x.fontpaths.custom<instance nr>.path`
Parameter	Font Path Position
Registry	`x.fontpaths.custom<instance nr>.position`
Value	99 (default)

- Fixed **display configuration problems caused by wrong access permissions** of `/wfs/user/graphic` folder.
- Fixed **battery indicator**.
- Fixed **Setup Assistant** - After acceptance of EULA, **Demo License flow was not available**.
- Fixed **wrongly shown Starter license info in Product ID** on fully licensed devices.
- Fixed product id for **IGEL UD6**.
- Fixed issues with **global proxy configuration**.
- Fixed sporadic failures while **custom partition initialisation**.
- Fixed **Finish** button **label in Setup Assistant.**
- Fixed **missing generation number in Product ID** (About and UMS).
- Fixed **applications from custom partition get killed** when network is up.
- Fixed IGEL system uses **far too much RAM inside a VM**.
- Added **registry key to allow old weak public key algorithms for older SSH** servers.
  More...

Parameter	Disable weak Pubkey algorithms
Registry	`network.ssh_client.disable_weak_pubkey_algos`
Type	bool
Value	enabled / disabled

- Added registry key to **switch between the default (igel) and the unchanged asound2 pulse plugin** type:
  More...

Parameter	Asound2 plugins type
Registry	`multimedia.alsa.asound2_plugin_type`
Range	[default] [igel] [vanilla]

Driver

- Fixed **Citrix terminate** with Olympus RM4010P connected and hardware button pressed.

- Fixed **Olympus FootSwitch** being detected **as mouse buttons.**
- Added driver for **MediaTek MT7921**.
- Fixed several problems of **MediaTek MT7921** driver.

X11 system

- Added new registry keys which can be useful to fix issues with **monitors not waking up after DPMS off events**.
  More...

Parameter	Quirk for DPMS Off to On event.
Registry	`x.dpms_quirks.off_on.quirk`
Range	[none] [refresh-change]
Parameter	Wait time in seconds before executing quirk after DPMS event.
Registry	`x.dpms_quirks.off_on.wait_before`
Type	string
Value	1
Parameter	Wait time in seconds between two quirk states.
Registry	`x.dpms_quirks.off_on.wait_between`
Type	string
Value	3
Parameter	Wait time in seconds after execution of quirk.
Registry	`x.dpms_quirks.off_on.wait_after`
Type	string
Value	1
Parameter	Xrandr connector names where quirk should apply (empty means all)
Registry	`x.dpms_quirks.off_on.connectors_to_quirk`
Type	string
Value	empty

X server

- Fixed **monitor configuration when modesetting graphics driver is enabled**.
- Added new registry keys for **xorg modesetting** options:
  More...

Parameter	Use linear framebuffer instead of tiling one.
Registry	`x.drivers.modesetting.use_linear_framebuffer`
Range	[Default] [True] [False]
Parameter	Use variable refresh rate.
Registry	`x.drivers.modesetting.use_variable_refresh`
Range	[Default] [True] [False]
Parameter	Use async flips for secondary video outputs on multi-display setups.
Registry	`x.drivers.modesetting.use_async_flip_secondaries`
Range	[Default] [True] [False]
Parameter	Use DRI3 page flipping.).
Registry	`x.drivers.modesetting.use_page_flip`
Range	[Default] [True] [False]
Parameter	Use shadow framebuffer layer (default on).
Registry	`x.drivers.modesetting.use_shadow_fb`
Range	[Default] [True] [False]
Parameter	Use double buffer for shadow updates (default depends on hardware).
Registry	`x.drivers.modesetting.use_double_shadow`
Range	[Default] [True] [False]
Parameter	Use software cursor (default off).
Registry	`x.drivers.modesetting.use_sw_cursor`
Range	[Default] [True] [False]
Parameter	Use gamma look up table (warning some devices have problems with this).
Registry	`x.drivers.modesetting.use_gamma_lut`
Range	[Default] [True] [False]

Window manager

- Fixed **taskbar clock is displaying seconds** (again) if enabled in system registry.
- Fixed **taskbar** was displayed incorrectly in some special configuration cases.

VirtualBox

- Added new registry key to **disable initial boot framebuffer**
  More...

Parameter	Disable use of initial boot framebuffer.
Registry	`system.kernel.bootparams.vga_off`
Type	bool
Value	enabled / disabled

Audio

- Fixed `multimedia.disable_audio.pci` registry key setting.
- Fixed **switch of Speaker / Headsets**

Multimedia

- Added new registry key to **prefer i965 VAAPI driver over iHD** (if usage of iHD cause trouble)
  More...

Parameter	Prefer i965 over iHD VAAPI driver
Registry	`multimedia.vaapi.prefer_i965`
Range	[Default] [Prefer] [Force]

Remote Management

- Fixed opening communication ports in rmagent - **now all network ports use IPv4 only**.
- Fixed **keepalive mechanism** in rmagent. The mechanism must prevent premature closing connection by the UMS if a remote command takes a time period over 30 seconds.
- Fixed **removing files in the file transfer** mechanism. Files are properly removed from the file system, when files are not assigned anymore to a device in the UMS.
- Fixed **UMS file transfer of trusted certificates** which have spaces in file names.
- Fixed **IP address retrieving of a WLAN interface**.
- Fixed **losing ICG connection on switching from LAN to WLAN** - now a new ICG connection is established.
- Fixed spurious **creation of empty directories** `/wfs/ca-certs?*` and `/wfs/user?*` when using certificates with spaces in filenames for file transfer.
- **Changed applying of remote settings received during boot** - the settings are synced with the current local settings at the end of the boot process. If these changes require a system interaction to be applied (like restart of some
  services) then the user is asked about applying. The dialog is optional and quits after a timeout. This bugfix solves the problem, that the "Apply changes" dialog is shown on every boot.
- Fixed **evaluation of the exit status of a UMS generic job** if the corresponding generic command is implemented as a systemd service.

IGEL Cloud Gateway

- Fixed exchange of the **ICG certificate chain**.

VNC

- Fixed **keyboard mapping in shadowing sessions**, especially with backslash, euro and at keys in French keyboard layout.

Notes for Release 11.06.250

Software:	Version	11.06.250
Release Date:	2022-02-07	
Release Notes:	Version	RN-1106250-1
Last update:	2022-02-07	

- Supported Devices 11.06.250 (see page 2939)
- Component Versions 11.06.250 (see page 2940)
- Known Issues 11.06.250 (see page 2948)
- Security Fixes 11.06.250 (see page 2951)
- New Features 11.06.250 (see page 2952)
- Resolved Issues 11.06.250 (see page 2954)

Supported Devices 11.06.250

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[286].

286. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.06.250

Clients

Product	Version
Amazon WorkSpaces Client	3.1.9
Chromium	95.0.4638.69-igel1635513789
Cisco JVDI Client	14.0.3
Cisco Webex VDI plugin	41.12.0.20899
Cisco Webex Meetings VDI plugin	41.10.9.15
Cisco Webex Meetings VDI plugin	41.12.6.12
Cisco Webex Meetings VDI plugin	42.1.1.20
Zoom Media Plugin	5.4.59458
Zoom Media Plugin	5.8.4.21112
Zoom Media Plugin	5.9.0.20720
Citrix HDX Realtime Media Engine	2.9.400
Citrix Workspace App	20.10.0.6
Citrix Workspace App	21.11.0.20
Citrix Workspace App	21.12.0.18
deviceTRUST Citrix Channel	20.2.310.0
Crossmatch DP Citrix Channel	0125
deskMate Client	2.1.3
DriveLock Agent	20.1.4.30482
Ericom PowerTerm	14.0.1.62267
Evidian AuthMgr	1.5.7789
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech Plugins	3.7.3
FabulaTech USB for Remote Desktop	6.0.28
FabulaTech Scanner for Remote Desktop	2.7.0.1

FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	91.3.0
IBM iAccess Client Solutions	1.1.8.6
IGEL RDP Client	2.2igel1639469055
IGEL AVD Client	1.0.37igel1639058670
deviceTRUST RDP Channel	20.2.310.0
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
Lakeside SysTrack Channel	9.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	7.1.3-1igel9
Open VPN	2.5.1-3igel1621236751
Zulu JRE	8.0.302-1
Parallels Client	18.2.0
Spice GTK (Red Hat Virtualization)	0.39-1igel106
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
SpeechWrite	1.0
Stratusphere UX Connector ID Key software	6.5.0-2
Teradici PCoIP Software Client	21.03.0-18.04
ThinLinc Client	4.13.0-2172
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	4.16.0-1igel1611217037
VNC Viewer	1.11.0+dfsg-2igel19
VMware Horizon Client	2111-8.4.0-18957622
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	2017/09/29

Grundig Business Systems dictation driver	0.12/21-12-21
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	4.0.1
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7-20210902
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Thales SafeNet	10.8.28
PKCS#11 Library OpenSC	0.21.0-1igel39
PKCS#11 Library SecMaker NetID	6.8.3.21
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.8-1igel1632136057
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.36-2igel1636006599
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.1-1igel18
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.7
OpenSSL	1.1.1-1ubuntu2.1~18.04.13
OpenSSH Client	8.4p1-5igel6
OpenSSH Server	8.4p1-5igel6
Bluetooth stack (bluez)	5.56-0ubuntu2igel12
MESA OpenGL stack	21.1.5-1igel145
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20210202igel1122
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	460.91.03-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.2-1igel1113
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.12.19 #mainline-lxos_dev-g1634042087
Xorg X11 Server	1.20.11-1igel1120

Xorg Xephyr	1.20.11-1igel1120
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.500
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel14
XFCE4 Window Manager	4.14.5-1~18.04igel1600422786
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.30.0-2igel114
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.92
GStreamer 0.10 Fluendo h264dec	0.10.59
GStreamer 0.10 Fluendo mp3dec	0.10.41
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.229
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.5-1igel1633086114
GStreamer 1.0 Fluendo aacdec	0.10.42
GStreamer 1.0 Fluendo asfdemux	0.10.92
GStreamer 1.0 Fluendo h264dec	0.10.59
GStreamer 1.0 Fluendo mp3dec	0.10.41
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.229
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.32.4-1igel1632209494
Python2	2.7.17

Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.22-dfsg-1igel55
Virtualbox X11 Guest Utils	6.1.22-dfsg-1igel55
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.3.0-6igel12
Mobile Device Access USB (gphoto)	2.5.27-1igel8
VPN OpenConnect	8.10-2igel6
Scanner support	1.0.27-1
VirtualBox	6.1.22-dfsg-1igel55

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	24.8 M	Included
Java SE Runtime Environment	43.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	361.2 M	Included
Ericom PowerTerm InterConnect	11.5 M	Included
Media Player	768.0 K	Included
Local Browser (Firefox) Citrix Appliance	94.8 M	Included

VMware Horizon RDP	6.2 M	Included
Cendio ThinLinc	11.5 M	Included
Printing (Internet printing protocol CUPS)	23.8 M	Included
NoMachine NX	31.8 M	Included
VMware Horizon	251.0 M	Included
Voice over IP (Ekiga)	7.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	30.8 M	Not included
Fluendo GStreamer Codec Plugins	7.5 M	Included
IBM i Access Client Solutions	128.2 M	Not included
Red Hat Enterprise Virtualization	3.5 M	Included
Parallels Client	6.8 M	Included
NVIDIA graphics driver	181.5 M	Not included
Imprivata Appliance	16.0 M	Included
AppliDis	256.0 K	Included
Evidian AuthMgr	3.0 M	Included
Hardware Video Acceleration	15.8 M	Included
Extra Font Package	1.2 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	4.0 M	Included
Cisco JVDI client	75.5 M	Included
PrinterLogic	53.2 M	Not included
Biosec BS Login	10.2 M	Not included
Login VSI Login Enterprise	32.8 M	Not included
Stratusphere UX CID Key software	3.2 M	Not included
Elastic Filebeat	25.0 M	Not included
AVD	120.5 M	Included
Local Browser (Chromium)	105.5 M	Not included

Amazon WorkSpaces Client	36.8 M	Included
deskMate client	6.5 M	Included
Cisco Webex VDI	55.0 M	Not included
Cisco Webex Meetings VDI	103.8 M	Not included
Zoom Media Plugin	145.0 M	Not included
DriveLock	14.8 M	Included
SpeechWrite Client	256.0 K	Included
Fluendo Browser Codec Plugins	4.5 M	Included
HP Factory deployment documentation	27.5 M	Included
Teradici PCoIP Client	18.2 M	Included
90meter Smart Card Support	256.0 K	Included
Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0K	Not included
Mobile Device Access USB (Limited support)	512.0 K	Not included
VPN OpenConnect (Limited support)	1.2 M	Not included
Scanner support / SANE (Limited support)	2.8 M	Not included
VirtualBox (Limited support)	70.8 M	Not included

Known Issues 11.06.250

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** during running / active sessions does not work. The **reader is visible, but cannot be used due to unknown reader status**. Only relevant for **CWA versions earlier than 2112**.
- There are known issues with **GStreamer 1.0** and **usage in Citrix**. These occur with **multimedia redirection of H.264, MPEG1, and MPEG2.** (GStreamer 1.0 is used if browser content redirection is enabled active.)
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec enabled.
- Enabled **DRI3** and an **AMD GPU Citrix H.264 acceleration** could lead to a **freeze**. **Selective H.264 mode (API v2) is not affected** by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

OSC Installer

- **OSC not deployable with IGEL Deployment Appliance**: New version **11.3 is required for 11.06 deployment**.

VMware Horizon

- After **disconnect of an RDP-based session**, the **Horizon main window** which contains the server or sessions overview, **cannot be resized** anymore.
- **Copying Text from Horizon Blast sessions** is not possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  It is necessary to switch off local logon and enable the following two keys via IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin** versions **below 5.8.0** make **Horizon Client crash upon connection to the remote desktop** in cases when TC Setup is running at the same time.
- **With the usage of the PCoIP protocol, the virtual channel provided by VMware used for serial port and scanner redirection could freeze on logout** from the remote session.

This **happens only with enabled scanner or serial port redirection**. The freeze does not occur if both redirection methods are enabled or none of them. **The Blast Protocol is not affected** by this bug.
The respective settings can be found in the IGEL Registry:
`vmware.view.enable-serial-port-redir`
`vmware.view.enable-scanner-redir`

- **Keyboard Input Source Language Synchronization** works only when using a local layout with deadkeys enabled.
  If a **keyboard layout is used which has deadkeys disabled** (which is the default on IGEL OS), **Horizon client falls back to en-US layout**.
- **PCoIP sessions may crash** in some cases, **switching to Blast Protocol is recommended** then. **H.264/HEVC encoding** can be **disabled** when **overall performance** is too **low**.
- **Client drive mapping and USB redirection for storage devices can be switched on at the same time**, but could lead to problems under some circumstances:
  Horizon Client tracks the drives which are dynamically mounted and adds them to the remote session using client drive mapping, i.e. USB redirection is then not used for these devices. However, in the case of devices like USB SD card readers, Horizon does not map them as client drives but forcefully uses USB redirection which results in an unclean unmount.
  As a **work-around**, the IDs of these card readers can be added to IGEL USB access rules and denied.

Parallels Client

- **Storage devices** attached to the thin client will **appear as network drives** in the remote session.
- **USB device redirection** is considered **experimental for the Parallels client for Linux**.

Firefox

- With **enabled Citrix Browser Content Redirection (BCR)**, **Firefox has no H.264 and AAC multimedia codec support**. This means **when codec support is needed in Firefox, BCR needs to be disabled**. Citrix Browser Content Redirection is disabled by default.

Network

- **Wakeup** from system suspend **fails on DELL Latitude 5510**.

Wi-Fi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 2010** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are involved.

- **Wrong license information** may be shown **in Product ID**. In detail, ‘Starter License’ is indicated sporadically by Product ID suffix ‘Starter‘, even with deployed and enabled WE license.

Conky

- The **right screen when using a multiscreen environment** may not be shown correctly. **Workaround**: The horizontal offset should be set to the width of the monitor (e.g. if the monitor has a width of 1920, the offset should be set to 1920)

Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[287] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.
- **Browser Appliance mode** can fail when the **Web URL contains special control characters** like ampersands (& character). **Workaround**: Add quotes at the beginning and the end of an affected URL. Example: 'https://www.google.com/search?q=aSearchTerm&source=lnms&tbm=isch'

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantech POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.
- **UD3-M340C**: **Sound preferences** are **showing Headphone & Microphone**, although not connected.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

287. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Security Fixes 11.06.250

Base system

- Update **policykit-1 package** for CVE-2021-4034 (fixes **Polkit Escalation of Privilege**).

Citrix

- **Removed registry key** `ica.appprotection` due to possible security vulnerability. Please follow this document for more information: https://support.citrix.com/article/CTX338435.

New Features 11.06.250

Smartcard

- Updated smartcard reader driver **MUSCLE CCID** to version **1.4.36**.
- Updated smartcard reader driver **ACS CCID** to version **1.1.8**.

Cisco JVDI Client

- Updated **Cisco JVDI** to version **14.0.3**

Base system

- Added support for **Thai keyboard layout and localization**.

Zoom VDI

- Integrated **Zoom Plugin 5.9.0.20720**
  Available Zoom Plugins in this release: **5.9.0.20720** (default), **5.8.4.21112**, and **5.4.59458**

Citrix

- Integrated **Citrix Workspace app 21.12**
  Available Citrix Workspace Apps in this release: **21.12** (default), **21.11**, and **20.10**
- New features:
  - The **cursor color inverts based on the background color of a text**.
    More...

Parameter	Support for cursor color inverting
Registry	`ica.wfclient.invertcursorenabled`
Value	false / true

  - Enhancement on s**martcard support**.
    More...

Parameter	SmartCard driver
Registry	`ica.module.VirtualDriver.SmartCard.drivername`
Value	VDSCARD.DLL / VDSCARDV2.DLL
Note	VDSCARDV2.DLL supports the Plug and Play functionality for smartcard reader

  - The **PulseAudio library** is **used instead of ALSA** to access multiple audio devices within a session (Experimental).
    More...

Parameter	Multiple Audio Device support
Registry	`ica.module.audioredirectionv4`

Value	false / true

- Note: The **VdcamVersion4Support** is **renamed** to **AudioRedirectionV4**, so registry key `ica.module.vdcamversion4support` is removed.
- **UDP audio through Citrix Gateway** (Experimental).
  More...

Parameter	UDP audio through Citrix Gateway
Registry	`ica.module.enableudpthroughgateway`
Value	false / true

- **Webcam redirection for 64-bit apps** (Technical Preview)
  For 64bit webcam redirection the following parameters must be enabled:
  `ica.wfclient.allowaudioinput = True` (default)
  `ica.wfclient.hdxh264inputenabled = True`

- For **Browser Content Redirection**, the **Chromium Embedded Framework** is **used by default now**. Parameter `ica.allregions.usecefbrowser` was **set to default value "true"**.

VMware Horizon

- Updated **Horizon Client** to version **2111 8.4.0-18957622**

Cisco Webex

- Available **Cisco Webex Meetings VDIs** in this release: **42.1.1.20** (default), **41.12.6.12**, and **41.10.9.15**
- Integrated **Cisco Webex VDI 41.12.0.20899**

Multimedia

- Added **libcam-tools** to firmware.

Resolved Issues 11.06.250

Citrix

- Fixed **window settings** for Citrix Desktop sessions
- Fixed, no useless **"to" icon** is created **with the StoreFront session**.
- Fixed **startup of Self-Service after reboot** in some cases.
- Added a parameter to **control** if the **cache of Self-Service files is persistent over reboots**:
  More...

Parameter	Persistent cache of configuration and UI
Registry	`ica.selfservice.persistentcache`
Value	true / false

- In 2112 CWA, Citrix introduced a **fix for a video flicker by always capturing the camera at maximum resolution** (1080 or 720p depending on the camera's capabilities) **and then scaling down dynamically to match the constraints set by Teams servers**. Example: in a conference call, the Teams servers might only require 360p at the beginning of the call and 480p as the call progresses.
  This scaling causes high CPU usage on thin clients as we are capturing HD video constantly, even if the endpoint is low-powered.
  Workaround: Add the following custom command under **System > Firmware Customization > Custom Commands > Desktop > Final desktop command**:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine
touch /var/.config/citrix/hdx_rtc_engine/config.json
echo "{" > /var/.config/citrix/hdx_rtc_engine/config.json
echo "\"UseDefaultCameraConfig\":0" >> /var/.config/citrix/hdx_rtc_engine/config.json
echo "}" >> /var/.config/citrix/hdx_rtc_engine/config.json
```

Base system

- Fixed **Product ID for IGEL UD6**.
- Fixed prevented **detection of USB device by its UUID**
- Fixed missing **generation number in Product ID** (**About** and **UMS**)
- Added new registry key to include **systemd information in the support files**.
  More...

Parameter	Collect systemd information for support files
Registry	`debug.collect_sysd_info_for_support`
Value	disabled / enabled

- Added new registry key to include **systemd-analyze plot in the support files**.

More...

Parameter	Include systemd-analyze plot svg-image in support files
Registry	`debug.create_sysd_plot_for_support`
Value	disabled / enabled

OSC Installer

- Fixed **OSC Recovery with enabled "Migrate Old Settings"**

RDP/IGEL RDP Client 2

- Fixed **native USB redirection of Elatec TWN4 MultiTech 2 LF RFID reader**
- Fixed wrong error message when **RDP session was closed by idle timeout**

AVD

- Added full **support for Thai (Kedmanee) keyboard layout**
- Added **support for Thai (Pattachote)** only with `sessions.wvd%.options.remote-keymapping=on`
- Added potential support for **other keyboard layouts** when the **special key codes** are of the type `0xeXX`
- Added new **parameter for avoiding incompatibilities between the AAD login and the QWebEngine** we use. **Enablement** of this new parameter is **needed when AAD login hangs** (likely showing a white screen after the username has been entered):
  More...

Registry	`sessions.wvd%.options.compact-login-view`
Value	enabled / disabled

RD Web Access

- Fixed **downloading published applications**

VMware Horizon

- Fixed **not starting Firefox if called by Horizon client for 2FA**. Libraries from Horizon installation were prevented by **apparmor**.

Firefox

- Added **apparmor exception to fix webrtc**
- Fixed usage of **Athena IDProtect smartcards**
- **Removed superfluous permission dialog** before **starting Horizon** client **or Citrix receiver from the browser**.

Network

- Fixed: **Network interfaces** were unusable when name assignment failed due to length. In such cases, **names are now determined according to NamePolicy=mac**.
- Improved **synchronization of IPv4 and IPv6** when both are desired

- Added a **registry key for specifying a period in seconds to wait for Ethernet link settings**. A value greater than "0" can be beneficial in the case where applying the link settings would interfere with 802.1X authentication.
  More...

Parameter	Wait for Ethernet link configuration
Registry	`network.interfaces.ethernet.device%.wait_for_link_config`
Type	integer
Value	1 (default)

Wi-Fi

- Fixed "bestsignal" in `network.interfaces.wirelesslan.device0.bssid` and `network.interfaces.wirelesslan.device0.alt_ssid%.bssid` had no effect.
- Improved reconfiguring **regulatory domain settings at runtime**
- Fixed: **Enabling wpa supplicant's background scan** was broken (settings `network.interfaces.wirelesslan.device0.bgscan.**`) since the step to Network Manager 1.30.0

Smartcard

- Fixed **smartcard PIN** verify with **HP Skylab smartcard keyboard**.
- Fixed **pcsc_scan** and **ATR_analysis** tools and **updated list of known smartcards**.

Base system

- Fix **USB deny rules** not working in certain situations.
- Added new parameter to **enable English international dead keys**:
  More...

Parameter	English (International) dead keys
Registry	`userinterface.keyboard.us_intl_compose`
Value	disabled / enabled

- Added parameter to enable **dead keys**:
  More...

IGEL Setup	**User Interface > Input > Keyboard**
Parameter	Enable dead keys
Registry	`userinterface.keyboard.usedeadkeys`
Value	disabled / enabled

- Fixed **Setup Assistant** - After acceptance of EULA, **Demo License flow** was **not available**.

- Fixed removal of **Kerberos credential cache after session logoff**.
- Fixed **faulty suspend with locked screen**.

Firmware update

- Implemented support for **FTP over implicit TLS (port 990)**

Driver

- Updated **Grundig Dictation** driver to version **0.12/21-12-21**
  - Fix crashes with newer Citrix clients
  - Add support to set up default speaker & microphone in Citrix & RDP session
  - Add support for Olympus DS-xxxx configuration
  - Various bug fixes

X server

- Fixed **XC font service support**

Audio

- Fixed `multimedia.disable_audio.pci` registry key setting
- Fixed **switch of Speaker / Headsets**

Remote Management

- Fixed **evaluation of the exit status of a UMS generic job** if the corresponding generic command is implemented as a `systemd` service.

Notes for Release 11.06.210

Software:	Version	11.06.210
Release Date:	2021-11-30	
Release Notes:	Version	RN-1106210-1
Last update:	2021-11-30	

The Release Notes for IGEL OS 11.06.210 are available in the following formats:

- Plain text: RNs_1106210.txt
- HTML: lxos_11.06.210.html

Notes for Release 11.05.133

Software:	Version	11.05.133
Release Date:	2021-04-29	
Release Notes:	Version	RN-1105133-1
Last update:	2021-04-26	

- Supported Devices 11.05.133 (see page 2960)
- Component Versions 11.05.133 (see page 2961)
- General Information 11.05.133 (see page 2969)
- Known Issues 11.05.133 (see page 2970)
- Security Fixes 11.05.133 (see page 2973)
- New Features 11.05.133 (see page 2974)
- Resolved Issues 11.05.133 (see page 2976)

Supported Devices 11.05.133

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[288].

288. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.05.133

Clients

Product	Version
Chromium (experimental)	88.0.4324.150-igel1612763117
CID Key	6.5.0-2
Cisco JVDI Client	14.0.0
Cisco Webex Teams VDI Client	41.4.0.18516
Cisco Webex Meetings VDI Client	41.4.0.162
Zoom Media Plugin	5.5.12716
Citrix HDX Realtime Media Engine	2.9.300
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.12.0.12
Citrix Workspace App	21.03.0.38
deskMate Client	2.1.3
deviceTRUST Citrix Channel	20.1.200.0
Crossmatch DP Citrix Channel	0125
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7617
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	6.0.28
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	78.6.1
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1605251065
IGEL WVD Client	1.0.24igel1619015530

Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	20.1.200.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8
Open VPN	2.5.0-1igel1606475118
Zulu JRE	8.48.0.51-2
Parallels Client	17.1.3
Spice GTK (Red Hat Virtualization)	0.39-1igel106
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
SpeechWrite	1.0
Teradici PCoIP Software Client	21.03.0-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-9igel17
VMware Horizon Client	2012-8.1.0-17349998
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20201118
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0

signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.21.0-1igel39
PKCS#11 Library SecMaker NetID	6.8.3.21
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel12
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.0-1igel18
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.5
OpenSSL	1.1.1-1ubuntu2.1~18.04.7
OpenSSH Client	8.4p1-3igel4
OpenSSH Server	8.4p1-3igel4
Bluetooth stack (bluez)	5.55-0ubuntu1.1igel10

MESA OpenGL stack	20.2.6-1igel131
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20200828igel1064
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	450.102.04-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.9.16 #mainline-lxos-g1615563496
Xorg X11 Server	1.20.10-2igel1100
Xorg Xephyr	1.20.10-2igel1100
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel109

ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.90
GStreamer 0.10 Fluendo h264dec	0.10.58
GStreamer 0.10 Fluendo mp3dec	0.10.40
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.224
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.3-1igel283
GStreamer 1.0 Fluendo aacdec	0.10.42.2-8d6d
GStreamer 1.0 Fluendo asfdemux	0.10.90
GStreamer 1.0 Fluendo h264dec	0.10.58
GStreamer 1.0 Fluendo mp3dec	0.10.40
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.224
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.30.4-1igel40
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.18-dfsg-3igel52
Virtualbox X11 Guest Utils	6.1.18-dfsg-3igel52
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1

Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.3.0-5igel11
Mobile Device Access USB (gphoto)	2.5.26-2igel7
VPN OpenConnect	8.10-2igel6
Scanner support	1.0.27-1
VirtualBox	6.1.18-dfsg-3igel52

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	329.0M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	76.5 M	Included
VMware Horizon RDP	4.5 M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	131.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included

NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	72.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included
NVIDIA graphics driver	126.8 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.5 M	Included
Hardware Video Acceleration	13.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.5 M	Included
Cisco JVDI client	61.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	89.2 M	Included
Local Browser (Chromium)	87.8 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	43.8 M	Not included
Cisco Webex Meetings VDI	32.8 M	Not included
Zoom VDI Media Plugin	47.2 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Teradici PCoIP Client	16.0 M	Included
90meter Smart Card Support	256.0 K	Included

Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.0 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	63.8 M	Not included

General Information 11.05.133

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.05.133

Citrix

- To launch **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** while the session is ongoing does not work. The reader is visible, but **cannot be used due to permanently unknown reader status**.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1, and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec.
- With activated DRI3 and an AMD GPU, **Citrix H.264 acceleration plugin could freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices **should not be enabled both at the same time**.
  - On the one hand, when using USB redirection for storage devices:
    The USB on-insertion feature is only working when the client drive mapping is switched off.
    In the IGEL Setup client drive mapping can be found in:
    Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping.
    It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules.
    Furthermore, Horizon Client relies on the OS to mount the storage devices themselves.
    Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the remote desktop.
  Workaround: **map the directory /media as a drive**. Then the external devices will show up inside the media drive.

- After disconnect of an RDP-based session, the **Horizon main window** which contains the server or sessions overview, **cannot be resized anymore**.
- **Copying Text from Horizon Blast sessions** isn't possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  You have to switch off the local logon and switch on these two keys in the IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases when TCSetup is running at the same time.
- **When using the PCoIP protocol the virtual channel provided by VMware used for serial port and scanner redirection can make Horizon client hang** on logout from the remote session.
  This happens if you enable only one of scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol isn't affected by this bug.
  The respective settings can be found here in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Chromium

- **H.264 decoding is not supported** anymore.

WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 20.10** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are involved)
- **Unreliable messages** in user dialog for applying settings during boot. Could occur when new settings were fetched from the UMS.

deskMate

- Some **stability issues** may remain.

Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[289] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers will not work with VirtualBox 5.2.x or older hosts**. This results in a black screen and non-working graphic.
  Possible workaround: Installation with **Failsafe Installation + Recovery** and set of `x.drivers.force_vesa` registry key to "true".

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantec POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU** driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

289. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

Security Fixes 11.05.133

Remote Management

- Fixed a **possible privilege escalation** while sending **user logoff event to the UMS**.

New Features 11.05.133

Citrix

- Integrated **Zoom Media Plugin 5.5.12716.0227**
- Added: In **StoreFront** sessions, **HTTP can now be selected for the URL** in addition to HTTPS.
- Implement "**Synchronize Citrix password with screensaver**" for **SelfService**. The parameter for StoreFront was reused.

UD Pocket

- Added official support for **Secured Kobra Stick from DIGITTRADE**.

VMware Horizon

- Added **switch for enabling Cisco Webex Meetings** within VMware Horizon.
  More...

Parameter	Cisco Webex Meetings VDI
Registry	`vmware.view.vdciscomeetings.enable`
Type	bool
Value	enabled / disabled

- **Removed** deprecated **ThinPrint virtual channel (tprpdp.so)** from Horizon sessions used for virtual printing. It is **replaced by Horizon's integrated printing mechanism**.

Imprivata

- Added registry key to overcome the **window overlap**. That occurred when using local setup or hotkeyed applications like the 'Display switch'.
  More...

IGEL Setup	**Registry**
Registry	`imprivata.avoid_focus_ownership`
Type	bool
Value	enabled / disabled

Smartcard

- Added smartcard reader driver for **DIGITTRADE** "**Secured Kobra Stick**".

WVD

- Added **WVD printer redirection**.
  More...

Registry	`sessions.wvd%.printing.cups`

Value	enabled / disabled
Registry	`print.cups.printer%.map_wvd`
Value	enabled / disabled
Registry	`print.cups.printer%.wvd_printer_driver`
Value	""

- The **default Windows driver name is "Microsoft PS Class Driver"**, which should be installed by default and work generically.
  To install a **custom printer driver**, the exact name must be set and the driver must be installed on the WVD side.

Base system

- **Post-session commands**: Added support to monitor multiple sessions and have a post-session command triggered if all sessions exited successfully.

Resolved Issues 11.05.133

Citrix

- Integrated **HDX Realtime Optimization Pack 2.9.300**
- Updated **Grundig Dictation driver** to version **20-09-16**. This **fixes termination of Citrix sessions when USB devices are plugged or unplugged** - happens with Citrix Workspace App versions newer than 20.09.
- **Citrix Hardware Decoder doesn't crash** anymore **when using 12 CPU cores** (or even more) at the server.

WVD

- Fixed **forced Azure re-authentication** (every 30 minutes)

Parallels Client

- Updated **Parallels client** to version **17.1.3**

Teradici PCoIP Client

- **Teradici client** update **21.03**

Imprivata

- Fixed **missing vendor logo**

Firefox

- Fixed **apparmor** rule for allowing Firefox to use **widevine DRM plugin**.

Smartcard

- Fixed **smartcard resource manager**: Reset is triggered when eject of smartcard fails.

Cisco Webex

- Updated **Cisco Webex Teams VDI** to **41.4.0.18516**
- Updated **Cisco Webex Meetings VDI** to **41.4.0.162**
- Please **make sure your Webex meetings client version is WBS 41.4.0 or later**, otherwise it will fail to launch Webex VDI optimized meeting.

Cisco JVDI Client

- Updated **Cisco JVDI** to **14.0.0**

IBM_5250

- Fixed **error** in **iAccess configuration**.

Base system

- Fixed **bootcode update** is **done on each reboot** on some **EFI** devices.
- Changed: Minimized **periodic write access to permanent storage**.

Firmware update

- Added: **sftp** protocol supports now the following **key exchange methods**: `ecdh-sha2-nistp256 (BSI)`

`ecdh-sha2-nistp384 (BSI)`
`ecdh-sha2-nistp521 (BSI)`
`curve25519-sha256 (BSI)`
`curve25519-sha256@libssh.org (BSI)`
`diffie-hellman-group-exchange-sha256`
`diffie-hellman-group-exchange-sha1`
`diffie-hellman-group14-sha1`
`diffie-hellman-group1-sha1`

X11 system

- Fixed **monitor sorting order** to be independent from montior startup time (GTK-3)
- Fixed **panel on wrong monitor**, when original monitor takes longer to come online
- Fixed **Turkish (Q) and Turkish (F) keyboard layout** configuration.
- Fixed **panel keyboard layout** indicator for **French (Switzerland), Turkish (Q) and Turkish (F)** keyboard layouts.
- Added **inhibit screensaver** while a **Cisco Webex Meetings** session is active in Citrix Workspace App.

Audio

- Fixed **not working** audio on **Intel Tiger Lake-based** devices.
- Fixed **automatic start of output audio** stream in **ALSA Pulse PCM**. The bug caused a complete **freeze of a Parallels session** while playback audio data.
- Bugfix for USB audio **default device switch** and update of **igel-sound-control**

Hardware

- Fixed **touchpad** issues for some **Dynabook laptops**.

Remote Management

- Fixed **execution of generic commands (Deploy Jabra Xpress package)** if they invoked as a UMS scheduled job.
- Fixed **handling of UMS scheduled jobs during boot** process.

Network

- Improved **network device order** for **LG CL600N, LG CN650N**
- The currently used parameter `tls-remote` is **deprecated** and was **removed in openVPN 2.4**. It was be **changed to** `verify-x509-name`.

H264

- **Citrix Hardware Decoder doesn't crash** anymore **when using 12 CPU cores** (or even more) at the server.

Notes for Release 11.05.120

Software:	Version	11.05.120
Release Date:	2021-03-25	
Release Notes:	Version	RN-1105120-1
Last update:	2021-03-23	

- IGEL OS 11 (see page 2979)
- IGEL OS Creator (OSC) (see page 2997)

IGEL OS 11

- Supported Devices 11.05.120 (see page 2980)
- Component Versions 11.05.120 (see page 2981)
- General Information 11.05.120 (see page 2989)
- Known Issues 11.05.120 (see page 2990)
- New Features 11.05.120 (see page 2993)
- Resolved Issues 11.05.120 (see page 2995)

Supported Devices 11.05.120

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[290].

290. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.05.120

Clients

Product	Version
Chromium (experimental)	88.0.4324.150-igel1612763117
CID Key	6.5.0-2
Cisco JVDI Client	12.9.3
Cisco Webex Teams VDI Client	41.1.0.17621
Cisco Webex Meetings VDI Client	41.2.0.142
Zoom Media Plugin	5.4.59458.0109
Citrix HDX Realtime Media Engine	2.9.200-2506
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.12.0.12
Citrix Workspace App	21.03.0.38
deskMate Client	2.1.3
deviceTRUST Citrix Channel	20.1.200.0
Crossmatch DP Citrix Channel	0125
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7617
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	6.0.28
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	78.6.1
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1605251065
IGEL WVD Client	1.0.22igel1612537530
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64

deviceTRUST RDP Channel	20.1.200.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8
Open VPN	2.5.0-1igel1606475118
Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.2.1
Spice GTK (Red Hat Virtualization)	0.39-1igel106
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
SpeechWrite	1.0
Teradici PCoIP Software Client	20.10.0-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-9igel17
VMware Horizon Client	2012-8.1.0-17349998
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20201118
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0

StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.21.0-1igel39
PKCS#11 Library SecMaker NetID	6.8.3.21
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel12
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.0-1igel16
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.5
OpenSSL	1.1.1-1ubuntu2.1~18.04.7
OpenSSH Client	8.4p1-3igel4
OpenSSH Server	8.4p1-3igel4
Bluetooth stack (bluez)	5.55-0ubuntu1.1igel10
MESA OpenGL stack	20.2.6-1igel131
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099

Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20200828igel1064
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	450.102.04-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.9.16 #mainline-lxos-g1615563496
Xorg X11 Server	1.20.10-2igel1100
Xorg Xephyr	1.20.10-2igel1100
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel109
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42

GStreamer 0.10 Fluendo asfdemux	0.10.90
GStreamer 0.10 Fluendo h264dec	0.10.58
GStreamer 0.10 Fluendo mp3dec	0.10.40
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.224
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.3-1igel283
GStreamer 1.0 Fluendo aacdec	0.10.42.2-8d6d
GStreamer 1.0 Fluendo asfdemux	0.10.90
GStreamer 1.0 Fluendo h264dec	0.10.58
GStreamer 1.0 Fluendo mp3dec	0.10.40
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.224
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.30.4-1igel40
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.18-dfsg-3igel52
Virtualbox X11 Guest Utils	6.1.18-dfsg-3igel52
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.3.0-5igel11
Mobile Device Access USB (gphoto)	2.5.26-2igel7
VPN OpenConnect	8.10-2igel6
Scanner support	1.0.27-1
VirtualBox	6.1.18-dfsg-3igel52

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	329.0M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	76.5 M	Included
VMware Horizon RDP	4.5 M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	131.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	72.5 M	Not included

Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included
NVIDIA graphics driver	126.8 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.5 M	Included
Hardware Video Acceleration	13.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.5 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	88.2 M	Included
Local Browser (Chromium)	87.8 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	36.8 M	Not included
Cisco Webex Meetings VDI	32.2 M	Not included
Zoom VDI Media Plugin	42.2 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Teradici PCoIP Client	14.5 M	Included
90meter Smart Card Support	256.0 K	Included

Virtualbox (Limited support) Mobile Device Access USB (Limited support) VPN OpenConnect (Limited support) Scanner support / SANE (Limited support) Limited Support Features	256.0K	Not included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.0 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	63.8 M	Not included

General Information 11.05.120

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.05.120

Citrix

- For using **multiple desktop sessions** with Citrix HDX RTME and Citrix H.264 acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

- This workaround is not applicable when **Enable Secure ICA** is active for the specific delivery group.
- Adding **smartcard readers** while the session is ongoing does not work. The reader is visible, but **cannot be used due to permanently unknown reader status**.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1, and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated DRI3 and hardware-accelerated H.264 deep compression codec.
- With activated DRI3 and an AMD GPU, **Citrix H.264 acceleration plugin could freeze**. Selective H.264 mode (API v2) is not affected by this issue.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices **should not be enabled both at the same time**.
  - On the one hand, when using USB redirection for storage devices:
    The USB on-insertion feature is only working when the client drive mapping is switched off.
    In the IGEL Setup client drive mapping can be found in:
    Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping.
    It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules.
    Furthermore, Horizon Client relies on the OS to mount the storage devices themselves.
    Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the remote desktop.
  Workaround: **map the directory /media as a drive**. Then the external devices will show up inside the media drive.

- After disconnect of an RDP-based session, the **Horizon main window** which contains the server or sessions overview, **cannot be resized anymore**.
- **Copying Text from Horizon Blast sessions** isn't possible.
- The **on-screen keyboard in Horizon appliance mode** does not work correctly with the local logon.
  You have to switch off the local logon and switch on these two keys in the IGEL registry:
  `userinterface.softkeyboard.autoshow`
  `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases when TCSetup is running at the same time.
- **When using the PCoIP protocol the virtual channel provided by VMware used for serial port and scanner redirection can make Horizon client hang** on logout from the remote session.
  This happens if you enable only one of scanner or serial port redirection. The freeze does not occur if both redirection methods are enabled or none of them. The Blast Protocol isn't affected by this bug
  The respective settings can be found here in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Chromium

- **H.264 decoding is not supported anymore / in this release**.

WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Cisco JVDI Client

- There may be a **segfault** shown in the logs (during log out of Citrix Desktop session). Occurs only when using **Citrix Workspace app 20.10** and **Cisco JVDI**.

Base system

- **Hyper-V (Generation 2) needs a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.
- **Update from memory stick requires network online state** (at least when multiple update stages are involved)
- **Unreliable messages** in user dialog for applying settings during boot. Could occur when new settings were fetched from the UMS.

deskMate

- Some **stability issues** may remain.

Firmware update

- On **devices with 2 GB of flash** storage, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Please visit Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher[291] for a possible solution and additional information.

Appliance Mode

- When ending a **Citrix session in browser appliance mode**, the browser is restarted twice instead of once.
- Appliance mode RHEV/Spice: **spice-xpi firefox plugin** is no longer supported.
  The **Console Invocation** has to allow **Native** client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers will not work with VirtualBox 5.2.x or older hosts**. This results in a black screen and non-working graphic.
  Possible workaround: Installation with **Failsafe Installation + Recovery** and set of `x.drivers.force_vesa` registry key to true.

Audio

- **IGEL UD2 (D220)** fails to restore the **volume level** of the speaker when the device used firmware version 11.01.110 before.
- **Audio jack detection** on **Advantec POC-W243L** does not work. Therefore, sound output goes through a possibly connected headset and also the internal speakers.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the Nouveau GPU driver.

Hardware

- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work on INTEL-based devices.

Remote Management

- **AIT feature** with **IGEL Starter License** is only supported by UMS version 6.05.100 or newer.

291. https://wiki.test.toolchain.igel.kreuzwerker.net/igelos-11.04/en/error-not-enough-%C2%A0space-on-local-drive-when-updating-to-igel-os-11-04-or-higher-32870765.html

New Features 11.05.120

OSC Installer

- Enhanced OSC Installer for **creating so-called factory preload images** (master images)
- Added possibility to **add initial settings** to OSC Installer ISO.

Citrix

- Added **automatic configuration of the Citrix webcam redirection** in ICA sessions.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
Parameter	Automatic HDX webcam configuration
Registry	ica.igel_hdxwebcam.enabled
Value	enabled / disabled
IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
Parameter	Resolution grade
Registry	ica.igel_hdxwebcam.quality
Range	[Very low][Low][Normal] [High][Very high][Best]
IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
Parameter	Minimal frame rate
Registry	ica.igel_hdxwebcam.framerate
Value	15

- Added **configuration for h264 encoding** in the Citrix webcam redirection.
  More...

Parameter	HDX Webcam H264 encoding
Registry	ica.wfclient.hdxh264inputenabled
Value	enabled / disabled

- Added configuration for **native h264 encoding** provided by webcam and used in the Citrix webcam redirection. This parameter requires the `ica.wfclient.hdxh264inputenabled` to be set to true.
  More...

Parameter	HDX Webcam H264 native

Registry	ica.wfclient.hdxh264enablenative
Value	enabled / disabled

- Available **Citrix Workspace apps** in this release: **21.03(default), 20.12 and 19.12**
- Added new Citrix feature for an enhanced experience of **multi-monitor scenarios**.
  You can save the selection for a multi-monitor screen layout. Pinning helps to relaunch a session with the selected layout, resulting in an optimized user experience.
  Note: Works only with Self Service.
  More...

Parameter	Enhanced Experience of Multi-Monitor scenarios
Registry	ica.authman.screenpinenabled
Value	enabled / disabled

- **All parameters of the Citrix set log program** are now available via setup under `ica.logging.setlog`. Logging can be set easier and permanent.
  Therefore, changed the structure of parameters to show the inheritance.

VMware Horizon

- Fixed **broken session handling** when using Webex Teams, Horizon session could only be started once.

WVD

- New **WVD icon**.

Network

- Added **Realtek RTL8125 2.5Gigabit Ethernet** driver.

WiFi

- Added support for **Realtek RTW8852AE WiFi** device.

Hardware

- Added hardware support for **LG 34CN650N AiO**.

Resolved Issues 11.05.120

OSC Installer

- Fixed OSC 11.05.xxx **not deployable with Deployment Appliance (ODA)**.

Citrix

- Fixed link to icacontrol
- Fixed: **Several audio device problems** through an enabled registry key `ica.module.vdcamversion4support`. The default was changed to disabled. This ensures that Citrix CWA behaves as before.
  More...

Parameter	Multiple Audio Device support
Registry	ica.module.vdcamversion4support
Value	enabled / disabled

- Fixed **Citrix logging**, the log file is written as expected.

RDP/IGEL RDP Client 2

- Added parameter to enable **serverside audio for RDP** sessions.
  More...

Parameter	Enable serverside audio
Registry	sessions.winconnect%.option.enable-serverside-audio
Value	enabled / disabled

Parallels Client

- Fixed an issue where the **post-session command** got triggered too early when using the Parallels Client.

Network

- Fixed network device order for **LG 34CN650W** and **CL600W** devices.
- Fixed a **graphics distortion in Setup Assistant**

WiFi

- Added registry key for **tweaking the WPA supplicant**. In general, the value is a comma-separated list of names. If it contains LATESUCCESS, a late EAP-Success message will be ignored.
  More...

Parameter	IGEL Tweaks
Registry	network.interfaces.wirelesslan.device0.wpa.igel_tweaks
Value	" "

- Added registry key to **activate the use of Broadcom sta driver** (needed for older Broadcom WiFi devices).
  More...

Parameter	Use Broadcom sta driver instead of b43 for WLAN
Registry	network.drivers.broadcom.use_broadcom_sta
Value	enabled / disabled

NCP VPN

- Fixed **NCP session start**.

Smartcard

- Fixed: Usage of **Nexus Personal** smartcard in combination with **Gemalto IDBridge CT30** reader, in Citrix and RDP

Base system

- Fixed **custom environment variables** when an administrator password is set.
- Fixed **boot problems** due to 2 partitions are marked active (legacy boot with GPT partition table).
- Fixed **RDP not triggering the post-session command** on session disconnect.
- Fixed **grub boot code and boot error message**: Unknown TPM error.
- Fixed **Demo License browser crashes after EULA**.

X11 system

- Fixed **taskbar hide/show delay** has no effect

VirtualBox

- Fixed **screen resolution issues with SINA OS 3.5.1 version**.
- Fixed **screen remains black after started multi-monitor configuration in VirtualBox**.
- Fixed **second screen in VirtualBox environment only is configured with 1024x768**.
- Fixed issue when getting **screen resolution from special VirtualBox version**.

Audio

- Improved **playback function** in the **ALSA Pulse PCM** - for applications using ALSA API (e.g. Citrix Workspace App).

Hardware

- Fixed **microphone detection on Dell Optiplex devices**.

Remote Management

- Fixed WOL proxy command.

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[292].

- Component Versions 11.05.120 (see page 2998)
- New Features 11.05.120 (see page 3000)
- Resolved Issues 11.05.120 (see page 3001)

292. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.05.120

Clients

Product	Version
Zulu JRE	8.48.0.51-2

System Components

OpenSSL	1.0.2n-1ubuntu5.5
OpenSSL	1.1.1-1ubuntu2.1~18.04.7
Bluetooth stack (bluez)	5.55-0ubuntu1.1igel10
MESA OpenGL stack	20.2.6-1igel131
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20200828igel1064
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	450.102.04-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Kernel	5.9.16 #mainline-lxos-g1615563496
Xorg X11 Server	1.20.10-2igel1100
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13

XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.18-dfsg-3igel52
Virtualbox X11 Guest Utils	6.1.18-dfsg-3igel52
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Services

Service	Size	Reduced Firmware
Java SE Runtime Environment	36.0 M	Included
NVIDIA graphics driver	122.5 M	Included

New Features 11.05.120

OSC Installer

- Enhanced OSC Installer for **creating so-called factory preload images** (master images)
- Added possibility to **add initial settings to OSC Installer ISO**.

Resolved Issues 11.05.120

OSC Installer

- Fixed OSC 11.05.xxx **not deployable with Deployment Appliance (ODA)**.

Notes for Release 11.05.100

Software:	Version	11.05.100
Release Date:	2021-02-25	
Release Notes:	Version	RN-1105100-1
Last update:	2021-03-08	

- IGEL OS Creator (OSC) (see page 3003)
- IGEL OS 11 (see page 3008)

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[293].

- Component Versions 11.05.100 (see page 3004)
- New Features 11.05.100 (see page 3006)
- Resolved Issues 11.05.100 (see page 3007)

293. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.05.100

Clients

Product	Version
Zulu JRE	8.48.0.51-2

System Components

OpenSSL	1.0.2n-1ubuntu5.5
OpenSSL	1.1.1-1ubuntu2.1~18.04.7
Bluetooth stack (bluez)	5.55-0ubuntu1.1igel10
MESA OpenGL stack	20.2.6-1igel131
VDPAU Library version	1.4-3igel1099
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20200828igel1064
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	450.102.04-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Kernel	5.9.16 #mainline-lxos-g1613995475
Xorg X11 Server	1.20.10-2igel1100
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13

XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.18-dfsg-1igel49
Virtualbox X11 Guest Utils	6.1.18-dfsg-1igel49
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Services

Service	Size	Reduced Firmware
Java SE Runtime Environment	36.0 M	Included
NVIDIA graphics driver	122.5 M	Included

New Features 11.05.100

Base system

- Updated **Linux kernel** to version **5.9.16**.

Hardware

- Added hardware support for new **IGEL UD7-LX 20 (H860C)**.
- Added hardware support for **LG 34CN650N AiO**.
- Added hardware support for **Dell Wyse Z Class thin client**.
- Added hardware support for **Lenovo ThinkCentre M70q**.
- Added hardware support for **Dell Wyse 5470**.
- Added hardware support for **Lenovo L14**.
- Added hardware support for **Lenovo ThinkCentre M75n**.
- Added hardware support for **Lenovo 14w**.
- Added hardware support for **LG CN65 All in one**.
- Added hardware support for **DELL LATITUDE 5510**.
- Added hardware support for **ELO i2 Touch all-in-one (15 and 22) inch**.
- Added detection of **UD Pocket UC5-LX 2**.

Resolved Issues 11.05.100

OSC Installer

- Fixed **warning** message a**fter feature deselection for installations on 2 GB flashes**.
- Fixed a **display** issue **with Intel** and **Nvidia GPU**.

IGEL OS 11

- Supported Devices 11.05.100 (see page 3009)
- Component Versions 11.05.100 (see page 3010)
- General Information 11.05.100 (see page 3017)
- Known Issues 11.05.100 (see page 3018)
- Security Fixes 11.05.100 (see page 3021)
- New Features 11.05.100 (see page 3025)
- Resolved Issues 11.05.100 (see page 3037)
- CA Certificates Contained in IGEL OS 11.05 (see page 3047)

Supported Devices 11.05.100

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 20 UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also IGEL OS 11 Hardware Support.

Component Versions 11.05.100

Clients

Product	Version
Chromium	88.0.4324.150-igel1612763117
CID Key	6.5.0-2
Cisco JVDI Client	12.9.3
Cisco Webex Teams VDI Client	41.1.0.17621
Cisco Webex Meetings VDI Client	41.2.0.142
Zoom Media Plugin	5.4.59458.0109
Citrix HDX Realtime Media Engine	2.9.200-2506
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.10.0.6
Citrix Workspace App	20.12.0.12
deskMate Client	2.1.3
deviceTRUST Citrix Channel	20.1.200.0
Crossmatch DP Citrix Channel	0125
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7617
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	6.0.28
FabulaTech Scanner for Remote Desktop	2.7.0.1
FabulaTech Webcam for Remote Desktop	2.8.10
Firefox	78.6.1
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1605251065
IGEL WVD Client	1.0.22igel1612537530
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64

deviceTRUST RDP Channel	20.1.200.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8
Open VPN	2.5.0-1igel1606475118
Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.2.1
Spice GTK (Red Hat Virtualization)	0.39-1igel106
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
SpeechWrite	1.0
Teradici PCoIP Software Client	20.10.0-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7-7.6.126
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-9igel17
VMware Horizon Client	2012-8.1.0-17349998
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20201118
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0

StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000
PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.21.0-1igel39
PKCS#11 Library SecMaker NetID	6.8.3.21
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.0-1igel16
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.5
OpenSSL	1.1.1-1ubuntu2.1~18.04.7
OpenSSH Client	8.4p1-3igel4
OpenSSH Server	8.4p1-3igel4
Bluetooth stack (bluez)	5.55-0ubuntu1.1igel10
MESA OpenGL stack	20.2.6-1igel131
VAAPI ABI Version	0.40
VDPAU Library version	1.4-3igel1099

Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-2igel1066
Graphics Driver ATI/AMDGPU	19.1.0-2+git20200828igel1064
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	450.102.04-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-2igel1037
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.39.0-0ubuntu1igel1036
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.9.16 #mainline-lxos-g1613995475
Xorg X11 Server	1.20.10-2igel1100
Xorg Xephyr	1.20.10-2igel1100
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel105
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42

GStreamer 0.10 Fluendo asfdemux	0.10.90
GStreamer 0.10 Fluendo h264dec	0.10.58
GStreamer 0.10 Fluendo mp3dec	0.10.40
GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.224
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.18.3-1igel283
GStreamer 1.0 Fluendo aacdec	0.10.42.2-8d6d
GStreamer 1.0 Fluendo asfdemux	0.10.90
GStreamer 1.0 Fluendo h264dec	0.10.58
GStreamer 1.0 Fluendo mp3dec	0.10.40
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.224
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.30.4-1igel40
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.18-dfsg-1igel49
Virtualbox X11 Guest Utils	6.1.18-dfsg-1igel49
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-2igel104
Qemu Guest Agent	5.2+dfsg-3igel17

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.3.0-5igel11
Mobile Device Access USB (gphoto)	2.5.26-2igel7
VPN OpenConnect	8.10-2igel6
Scanner support	1.0.27-1
VirtualBox	6.1.18-dfsg-1igel49

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	235.8 M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	76.5 M	Included
VMware Horizon RDP	4.5 M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	131.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.5 M	Included
IBM i Access Client Solutions	72.5 M	Not included

Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included
NVIDIA graphics driver	126.8 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.5 M	Included
Hardware Video Acceleration	13.5 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	3.5 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	88.2 M	Included
Local Browser (Chromium)	87.8 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	36.8 M	Not included
Cisco Webex Meetings VDI	32.2 M	Not included
Zoom VDI Media Plugin	42.2 M	Not included
DriveLock	13.2 M	Included
SpeechWrite Client	256.0 K	Included
Teradici PCoIP Client	14.5 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.0 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	63.8 M	Not included

General Information 11.05.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.07.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.05.100

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check Updating to IGEL OS 11.04 or Higher on a Device with Small Storage (see page 3018) for a solution.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Adding smartcard readers** while the **session is ongoing** does not work. The **reader** is **visible**, **but cannot be used** due to permanently unknown reader status.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local **Storage Hotplug** on Setup page **Devices > Storage Devices > Storage Hotplug**.

- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Copying a text from Horizon Blast** sessions is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon. Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:
  - `userinterface.softkeyboard.autoshow`
  - `userinterface.softkeyboard.autohide`
- **Zoom VDI Media Plugin makes Horizon Client crash** upon connection to the remote desktop in cases **when TC Setup is running at the same time**.

Chromium

- **H.264 decoding is not supported** anymore.

Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Cisco JVDI Client

- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).
- **Unreliable messages in user dialog for applying settings during boot**. Could occur when new settings were fetched from the UMS.

deskMate

- Some stability issues may remain.

Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Security Fixes 11.05.100

Citrix

- Fixed file properties for `/var/log/.ctxlogconf` adjusted, **so no code can be executed by the user**.

Firefox

- **Added** `view-source:file:///` **to the blocklist** in case the browser should not have random access to the local file system.

Base system

- Fixed **bluez** security issue CVE-2020-0556.
- Fixed **librsvg** security issue CVE-2019-20446.
- Fixed **ppp** security issue CVE-2020-15704.
- Fixed **chromium-browser** security issues:
  More...

  CVE-2020-6541, CVE-2020-6540,
  CVE-2020-6539, CVE-2020-6538, CVE-2020-6537, CVE-2020-6536, CVE-2020-6535,
  CVE-2020-6534, CVE-2020-6533, CVE-2020-6532, CVE-2020-6531, CVE-2020-6530,
  CVE-2020-6529, CVE-2020-6528, CVE-2020-6527, CVE-2020-6526, CVE-2020-6525,
  CVE-2020-6524, CVE-2020-6523, CVE-2020-6522, CVE-2020-6521, CVE-2020-6520,
  CVE-2020-6519, CVE-2020-6518, CVE-2020-6517, CVE-2020-6516, CVE-2020-6515,
  CVE-2020-6514, CVE-2020-6513, CVE-2020-6512, CVE-2020-6511, CVE-2020-6510,
  CVE-2020-6509, CVE-2020-6507, CVE-2020-6506, CVE-2020-6505, CVE-2020-6496,
  CVE-2020-6495, CVE-2020-6494, CVE-2020-6493, CVE-2020-6571, CVE-2020-6570,
  CVE-2020-6569, CVE-2020-6568, CVE-2020-6567, CVE-2020-6566, CVE-2020-6565,
  CVE-2020-6564, CVE-2020-6563, CVE-2020-6562, CVE-2020-6561, CVE-2020-6560,
  CVE-2020-6559, CVE-2020-6558, CVE-2020-6556, CVE-2020-6555, CVE-2020-6554,
  CVE-2020-6553, CVE-2020-6552, CVE-2020-6551, CVE-2020-6550, CVE-2020-6549,
  CVE-2020-6548, CVE-2020-6547, CVE-2020-6546, CVE-2020-6545, CVE-2020-6544,
  CVE-2020-6543, CVE-2020-6542, CVE-2020-6576, CVE-2020-6575, CVE-2020-6574,
  CVE-2020-6573, CVE-2020-15966, CVE-2020-15965, CVE-2020-15964, CVE-2020-15963,
  CVE-2020-15962, CVE-2020-15961, CVE-2020-15960, CVE-2020-15959, CVE-2020-6557,
  CVE-2020-15992, CVE-2020-15991, CVE-2020-15990, CVE-2020-15989,
  CVE-2020-15988, CVE-2020-15987, CVE-2020-15986, CVE-2020-15985,
  CVE-2020-15984, CVE-2020-15983, CVE-2020-15982, CVE-2020-15981,
  CVE-2020-15980, CVE-2020-15979, CVE-2020-15978, CVE-2020-15977,
  CVE-2020-15976, CVE-2020-15975, CVE-2020-15974, CVE-2020-15973,
  CVE-2020-15972, CVE-2020-15971, CVE-2020-15970, CVE-2020-15969,
  CVE-2020-15968, CVE-2020-15967, CVE-2020-16017, CVE-2020-16013,
  CVE-2020-16011, CVE-2020-16009, CVE-2020-16008, CVE-2020-16007,
  CVE-2020-16006, CVE-2020-16005, CVE-2020-16003, CVE-2020-16002,
  CVE-2020-16001, CVE-2020-16000, CVE-2020-15999, CVE-2020-16036,
  CVE-2020-16035, CVE-2020-16034, CVE-2020-16033, CVE-2020-16032,
  CVE-2020-16031, CVE-2020-16030, CVE-2020-16029, CVE-2020-16028,
  CVE-2020-16027, CVE-2020-16026, CVE-2020-16025, CVE-2020-16024,
  CVE-2020-16023, CVE-2020-16022, CVE-2020-16021, CVE-2020-16020,

CVE-2020-16019, CVE-2020-16018, CVE-2020-16015, CVE-2020-16014, CVE-2020-16012, CVE-2019-8075, CVE-2020-16042, CVE-2020-16041, CVE-2020-16040, CVE-2020-16039, CVE-2020-16038, CVE-2020-16037, CVE-2021-21116, CVE-2021-21115, CVE-2021-21114, CVE-2021-21113, CVE-2021-21112, CVE-2021-21111, CVE-2021-21110, CVE-2021-21109, CVE-2021-21108, CVE-2021-21107, CVE-2021-21106, CVE-2020-16043, CVE-2020-15995, CVE-2021-21148, CVE-2021-21147, CVE-2021-21146, CVE-2021-21145, CVE-2021-21144, CVE-2021-21143, CVE-2021-21142, CVE-2021-21141, CVE-2021-21140, CVE-2021-21139, CVE-2021-21138, CVE-2021-21137, CVE-2021-21136, CVE-2021-21135, CVE-2021-21134, CVE-2021-21133, CVE-2021-21132, CVE-2021-21131, CVE-2021-21130, CVE-2021-21129, CVE-2021-21128, CVE-2021-21127, CVE-2021-21126, CVE-2021-21125, CVE-2021-21124, CVE-2021-21123, CVE-2021-21122, CVE-2021-21121, CVE-2021-21120, CVE-2021-21119, CVE-2021-21118, CVE-2021-21117, and CVE-2020-16044.

- Fixed **ffmpeg** security issues CVE-2020-14212, CVE-2020-13904, CVE-2020-35965, and CVE-2020-35964.
- Fixed **pulseaudio** security issues CVE-2020-11931 and CVE-2020-16123.
- Fixed **nss** security issues CVE-2020-6829, CVE-2020-12401, CVE-2020-12400, and CVE-2020-12403.
- Fixed libvirt security issues CVE-2020-14301, CVE-2020-12430, CVE-2020-10701, and CVE-2020-14339.
- Fixed **libslirp** security issues CVE-2020-10756, CVE-2020-29130, and CVE-2020-29129.
- Fixed **samba** security issues:
  More...

  CVE-2020-14303, CVE-2020-1472, CVE-2020-1472, CVE-2020-14383, CVE-2020-14323, and CVE-2020-14318.

- Fixed **qemu** security issues:
  More...

  CVE-2020-16092, CVE-2020-14364, CVE-2020-15863, CVE-2020-13800, CVE-2020-13791, CVE-2020-13754, CVE-2020-13659, CVE-2020-13362, CVE-2020-13361, CVE-2020-13253, CVE-2020-12829, CVE-2020-10761, CVE-2020-28916, CVE-2020-27821, CVE-2020-27661, CVE-2020-27617, CVE-2020-27616, CVE-2020-25723, CVE-2020-25707, CVE-2020-25625, CVE-2020-25624, CVE-2020-25085, CVE-2020-25084, and CVE-2020-15859.

- Fixed **bind9** security issues CVE-2020-8624, CVE-2020-8623, and CVE-2020-8622.
- Fixed **grub2** security issues:
  More...

  CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15706, and CVE-2020-15707.

- Fixed **sane-backends** security issues:
  More...

  CVE-2020-12867, CVE-2020-12866, CVE-2020-12865, CVE-2020-12864, CVE-2020-12863, CVE-2020-12862, and CVE-2020-12861.

- Fixed **ghostscript** security issues:
  More...

CVE-2020-17538, CVE-2020-16310, CVE-2020-16309, CVE-2020-16308, CVE-2020-16307, CVE-2020-16306, CVE-2020-16305, CVE-2020-16304, CVE-2020-16303, CVE-2020-16302, CVE-2020-16301, CVE-2020-16300, CVE-2020-16299, CVE-2020-16298, CVE-2020-16297, CVE-2020-16296, CVE-2020-16295, CVE-2020-16294, CVE-2020-16293, CVE-2020-16292, CVE-2020-16291, CVE-2020-16290, CVE-2020-16289, CVE-2020-16288, CVE-2020-16287, CVE-2020-16, CVE-2020-8112, CVE-2020-6851, CVE-2020-27845, CVE-2020-27843, CVE-2020-27842, CVE-2020-27841, CVE-2020-27824, CVE-2020-27814, and CVE-2018-5727.

- Fixed **net-snmp** security issues CVE-2020-15862 and CVE-2020-15861.
- Fixed **curl** security issues:
  More...

  CVE-2020-8231, CVE-2020-8177, CVE-2020-8169, CVE-2020-8286, CVE-2020-8285, and CVE-2020-8284.

- Fixed **chrony** security issue CVE-2020-14367.
- Fixed **libx11** security issue CVE-2020-14344.
- Fixed **xorg-server** security issues:
  More...

  CVE-2020-14347, CVE-2020-25712, CVE-2020-14360, CVE-2020-14362, CVE-2020-14361, CVE-2020-14346, and CVE-2020-14345.

- Fixed **cairo** security issues CVE-2018-19876 and CVE-2020-35492.
- Fixed **openssl1.0** security issues:
  More...

  CVE-2020-1968, CVE-2019-1563, CVE-2019-1551, CVE-2019-1547, and CVE-2020-1971.

- Fixed **libproxy** security issues CVE-2020-25219 and CVE-2020-26154.
- Fixed **gnupg2** security issue CVE-2019-14855.
- Fixed **util-linux** security issue CVE-2018-7738.
- Fixed **ntp** security issue CVE-2019-8936.
- Fixed **tigervnc** security issue CVE-2020-26117.
- Fixed **brotli** security issue CVE-2020-8927.
- Fixed **vim** security issue CVE-2019-20807.
- Fixed **python2.7** security issue CVE-2020-26116.
- Fixed **python3.6** security issue CVE-2020-26116.
- Fixed **freetype** security issue CVE-2020-15999.
- Fixed **perl** security issues CVE-2020-12723, CVE-2020-10878 and CVE-2020-10543.
- Fixed **spice** security issue CVE-2020-14355.
- Fixed **glibc** security issue CVE-2017-18269.
- Fixed **python-cryptography** security issue CVE-2020-25659.
- Fixed **openldap** security issues CVE-2020-25692, CVE-2020-25710, and CVE-2020-25709.
- Fixed **libexif** security issue CVE-2020-0452.
- Fixed **krb5** security issue CVE-2020-28196.
- Fixed **libvncserver** security issues CVE-2018-21247, and CVE-2020-14396.
- Fixed **poppler** security issues CVE-2020-27778, CVE-2019-9959, CVE-2019-10871, and CVE-2018-21009.

- Fixed **xdg-utils** security issue CVE-2020-27748.
- Fixed **wpa** security issue CVE-2020-12695.
- Fixed **x11vnc** security issue CVE-2020-29074.
- Fixed **spice-gtk** security issue CVE-2020-14355.
- Fixed **libssh2** security issues CVE-2019-17498 and CVE-2019-13115.
- Fixed **spice-vdagent** security issues:
  More...

  CVE-2020-25653, CVE-2020-25652, CVE-2020-25651, CVE-2020-25650, and CVE-2020-2565.
- Fixed **openssl** security issue CVE-2020-1971.
- Fixed **libxml2** security issue CVE-2020-24977.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2020-9983, CVE-2020-9952, CVE-2020-9951, CVE-2020-9948, and CVE-2020-13584.
- Fixed **lxml** security issue CVE-2020-27783.
- Fixed **p11-kit** security issues CVE-2020-29363, CVE-2020-29362, and CVE-2020-29361.
- Fixed **wavpack** security issue CVE-2020-35738.
- Fixed **nvidia-graphics-drivers-450** security issues CVE-2021-1053 and CVE-2021-1052.
- Fixed **tar** security issues CVE-2019-9923 and CVE-2018-20482.
- Fixed **pillow** security issues CVE-2020-35655 and CVE-2020-35653.
- Fixed **dnsmasq** security issues:
  More...

  CVE-2020-25687, CVE-2020-25686, CVE-2020-25685, CVE-2020-25684, CVE-2020-25683, CVE-2020-25682, CVE-2020-25681 and CVE-2019-14834.
- Fixed **sudo** security issues CVE-2021-3156 and CVE-2021-23239.
- Fixed **privilege escalation via** environment variable `PATH` in `/bin/usershell` binary.
- Fixed **privilege escalation via** environment variables in the `/bin/update` binary.
- Fixed **BleedingTooth** security issue which means CVE-2020-12351, CVE-2020-12352 and CVE-2020-24490.
- Fixed **kernel** security issues named **Platypus** (CVE-2020-8694 and CVE-2020-8695).
- Fixed possible security issue
- Fixed a **local command injection with SSH** session.

Remote Management

- Added **secure channel** for following commands
  `show_message`, `get_file_from_url`, `write_file_to_url` and `upload_tc_support_information`
  sends all relevant data in a secured way.

VNC

- Fixed a **secure terminal** and **secure VNC shadowing** remote code execution vulnerability.

New Features 11.05.100

Citrix

- The new "**screen pinning**" feature **for Citrix desktop sessions** has been integrated. With this feature, it is possible to **start multiple Citrix desktop sessions on different screens**.
  The following parameters have been added for this purpose:
  - This parameter **defines** the **session name** on which the settings are to be used. Also the known **wildcards like * and ? are possible** here.
    More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Window**
Parameter	Citrix session name
Registry	`ica.destination_window.session%.name`
Value	""

  - The parameter **defines** which **mode** should be **used**.
    More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Window**
Parameter	Multimonitor full-screen mode
Registry	`ica.destination_window.session%.multimonitor_mode`
Range	[Restrict full-screen session to one monitor] [Expand full-screen session across all monitors] [Expand the session over a self-selected number of monitors]

  - For "**Restrict full-screen session to one monitor**"
    also `ica.destination_window.session%.monitor` needs **to be set**.
    For "**Expand the session over a self-selected number of monitors**"
    also `ica.destination_window.session%.multimonitor_selection` needs **to be set**.
    Further information is also offered **via tooltip**.
    More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Window**
Parameter	Desktop session start monitor
Registry	`ica.destination_window.session%.monitor`
Range	[1st Monitor][2nd Monitor][3rd Monitor][4rd ...]
IGEL Setup	**Sessions > Citrix > Citrix Global > Window**

Parameter	Monitor selection
Registry	`ica.destination_window.session%.multimonitor_selection`
Value	""

- Integrated **HDX RTME 2.9.200** for the usage of SfB (Skype for Business).
- Available **Citrix Workspace apps** in this release: **20.12 (default)**, **20.10** and **19.12**.
- Added new feature, where **multiple audio devices could be mapped inside the sessions**. This will display audio devices with their device name and not only HDX audio.
  More...

Parameter	Multiple Audio Device support
Registry	`ica.module.vdcamversion4support`
Value	true/false

- Note: **Bluetooth devices** are currently **not supported for Device Redirection**.
- New **centralized Citrix logging in IGEL OS**, only one parameter is needed to activate logging.
  More...

Parameter	Enable logging for Citrix sessions
Registry	`ica.logging.debug`
Value	on/off

- Since **Workspace app 20.09**, the tool **setlog** is **used to configure the logging**. For this purpose, parameters are provided in the registry `ica.logging.setlog`, but usually nothing needs to be changed.
- Fixed issue: **mic** and **webcam** devices can be **redirected using Browser Content Redirection**.
  More...

Parameter	Enables mic and webcam redirection using BCR
Registry	`ica.allregions.cefenablemediadevices`
Value	[Factory default is "**"] [False][True]

- Added new parameter **Readers Status Poll Period** to **specify the delay**, in milliseconds, **for reading information from a smartcard** after the card is inserted or removed, or a reader is disconnected, etc.
  More...

Parameter	Readers Status Poll Period
Registry	`ica.wfclient.ReadersStatusPollPeriod`

Type	Integer
Value	250/Range 100..5000

- Integrated **Zoom** Media Plugin **5.4.59458.0109**
- The **default** value of the parameter `ica.module.vdcamversion4support` was **set to "true"**.

WVD

- Added option to **always prompt for password upon session host connection**.
  More...

Parameter	Always prompt for password upon session host connection
Registry	`sessions.wvd%.options.always-prompt-for-session-password`
Type	bool
Value	enabled / disabled
Note:	The same can be achieved on the server side by setting the RDP group policy of "Always prompt for password upon connection".

- Added options to configure **Fabulatech for WVD**. This includes **Webcam redirection**, **Scanner redirection**, and **USB redirection**.
- The **USB redirection** configuration is **still to be done** via **Sessions > RDP > RDP Global > Fabulatech USB Redirection**. Later releases should mirror that under WVD as well.
- There are **global WVD settings** to select which redirections (Webcam, Scanner, USB) should be enabled for WVD.
- There is a **switch per WVD session** that allows **to enable/disable Fabulatech for that sessions** respectively.
- Note: Technically, the **Fabulatech redirections** are **selected system-wide**. That means, when **Scanner redirection** is enabled for Citrix and **Webcam redirection** is enabled for WVD, both these redirections are visible in Citrix and in WVD sessions. Only disabling Fabulatech support in general for a WVD session is possible.
  More...

IGEL Setup	**Sessions > WVD > WVD Global > Plugins > Fabulatech**
Parameter	Fabulatech Webcam Redirection
Registry	`wvd.plugins.fabulatech.webcam`
Value	enabled / disabled
IGEL Setup	**Sessions > WVD > WVD Global > Plugins > Fabulatech**
Parameter	Fabulatech Scanner Redirection

Registry	`wvd.plugins.fabulatech.scanner`
Value	enabled / disabled
IGEL Setup	**Sessions > WVD > WVD Global > Plugins > Fabulatech**
Parameter	Fabulatech USB Redirection
Registry	`wvd.plugins.fabulatech.usb`
Value	enabled / disabled
IGEL Setup	**Sessions > WVD > WVD Sessions > WVD Session > Plugins > Fabulatech**
Parameter	Fabulatech Webcam/Scanner/USB Redirection
Registry	`sessions.wvd%.plugins.fabulatech`
Value	enabled / disabled

- Integrated **Zoom** Media Plugin **5.4.59458.0109** with support for WVD.
More...

IGEL Setup	**Sessions > WVD > WVD Sessions > WVD Session > Plugins > Fabulatech**
Parameter	Zoom VDI Media Plugin
Registry	`sessions.wvd%.plugins.zoomvdi`
Value	enabled / disabled

- Added option to **always prompt for username and password upon session host connection**.
More...

Parameter	Always prompt for username and password upon session host connection
Registry	`sessions.wvd%.options.always-prompt-for-session-username-and-password`
Type	bool
Value	enabled / disabled

- Added option to **preset the workspace view zoom**
More...

Parameter	Initial workspace zoom
Registry	`sessions.wvd%.options.workspacezoom`
Type	string

Value	100

- Added option to **select specific monitors in a multimonitor session**.
  Only monitors matching this mask are used.
  - Monitors start with zero (0).
  - If empty all monitors are enabled, which is the default.
  - Can be one or a comma-separated list of the following specifiers without the quotes:
    - "1-2": An inclusive range of monitor indexes.
    - "-2": An inclusive range beginning from 0 to the given monitor index.
    - "2-": An inclusive range beginning with the specified monitor up to index 63, which is the maximum monitor index supported.
    - "2,3,5": A comma-separated list of monitor indexes.
      More...

Parameter	Multimonitor enable mask
Registry	`sessions.wvd%.options.multimonitormask`
Type	string
Value	(empty by default)

- If the **username** is **preset with a string that starts with "@"**, the **rest of the string** is **taken as** a **preset domain** name. The user then only needs to enter her/his username and the domain name is automatically appended for AAD login.
- Additionally, the following parameter has been added to **allow/disallow the preset domain being overwritten when the username enters a name that contains an @** symbol itself. If this option is enabled, the entered domain is accepted. Otherwise, the entered domain is replaced by the preset domain.
  More...

Parameter	Allow preset domain overwrite
Registry	`sessions.wvd%.options.allow-preset-domain-overwrite`
Type	bool
Value	enabled / disabled

- Added **company logo customization**, but the download of custom images to the local filesystem needs to be defined. So **at the moment, the settings are not really useful, except for disabling the IGEL logo** maybe.
  More...

Parameter	Disable company logo
Registry	`sessions.wvd%.options.no`[294]`-logo`

294. http://options.no

Type	bool
Value	enabled / disabled

Parameter	Logo image filename
Registry	`sessions.wvd%.options.logo-image`
Type	string
Value	(empty by default)

- Added **background customization**, but download of custom images to the local filesystem needs to be defined. So **at the moment, the settings are not really useful, except for disabling the background image or defining a solid color for the background**.
  More...

Parameter	Disable background image
Registry	`sessions.wvd%.options.no`[295]`-background`
Type	bool
Value	enabled / disabled

Parameter	Background image filename or color (#rrggbb)
Registry	`sessions.wvd%.options.background-image`
Type	string
Value	(empty by default) / filename / #rrggbb

VMware Horizon

- Updated **Horizon** Client to version **2012-8.1.0-17349998**
- Integrated **Zoom** Media Plugin **5.4.59458.0109**
- Fixed failure to **start Horizon serial port redirection service at boot time**

Chromium

- Updated **Chromium** browser to version **88.0.4324.150**.
- **H.264 decoding** is **not supported** anymore.
- **Custom preferences** setup is **not supported** anymore.
- Reworked **custom commandline** setup: Enter **all commandline parameters in a single entry field**.

Wi-Fi

- Added support for **WPS push button connect method**

Imprivata

295. http://options.no

- Added: The **FUS Username** is an **editable combobox with prefilled values** now. Set of an **own string** is also **possible**.
  - Hostname of the endpoint
  - MAC address of the endpoint
  - Serial number of the endpoint

  More...

IGEL Setup	**Sessions > Appliance mode > Imprivata**
Parameter	FUS User
Registry	`imprivata.fus.user`

Smartcard

- Updated **A.E.T. Europe SafeSign Identity Client** to version **3.6.0.0**.
- Added **Smartcard PIN passthrough** in **Firefox** and **Chromium**. The PIN will be cached while logging on via Active Directory/Kerberos with smartcard. In Firefox and Chromium, no further PIN input is necessary to use the smartcard.

  More...

Parameter	Smartcard PIN caching
Registry	`scard.pkcs11.pin_cache.enable`
Value	enabled / disabled

- Updated **SecMaker Net iD** to version **6.8.3**. New features are:
  - Support for Thales IDPrime 940 SIS & IDPrime 3940 SIS
  - Support for FIPS level 3 versions of Thales IDPrime MD smart cards (based on MD830B and MD840)
  - Support for FINEID 3.0
  - Updated support for Yubico YubiKey serial numbers (version 5 and later)
  - Updated support for Feitian ePass FIDO serial numbers (version 99 and later)

  For detailed release information, see https://docs.secmaker.com/net-id-enterprise/6.8/nie-release-notes/nie-683-release-notes.html.

ThinPrint

- Added **ezeep by ThinPrint** support **for WVD**

  More...

IGEL Setup	**Sessions > WVD > WVD Sessions > WVD Session > Printing > ezeep by ThinPrint**
Parameter	Printing with ezeep
Registry	`sessions.wvd%.printing.thinprint-ezeep`
Value	enabled / disabled

Note	• Ezeep is directly related to the ThinPrint configuration under **Devices > Printer > ThinPrint > ...** • When ThinPrint configuration is changed, you need to close running WVD sessions and reconnect to make ThinPrint/Ezeep work again for the related session.

Application Launcher

- Added **optional custom message in 'About' page of application launcher**. The message is displayed **below** the **License Information** section. The text can be plain text or HTML, supported HTML subset are mentioned in Qt RichText.
  More...

Parameter	Custom message
Registry	`userinterface.launcher.custom_message`
Value	empty

Cisco Webex

- Integrated **Cisco Webex Meetings 41.2.0.142**
- Integrated **Cisco Webex Teams 41.1.0.17621**

Cisco JVDI Client

- Integrated **Cisco JVDI 12.9.3** client

Base system

- Added **post-session command** support **for WVD** sessions.
- Updated **OpenVPN** to version **2.5.0**.
- Updated **OpenSSH** to version **8.4p1-2**.
- Added **warning at boot** time **if Workspace Edition maintenance has expired**.
- Updated **Fluendo multimedia codecs**.
- Updated **Linux kernel** to version **5.9.16**.
- Added **inhibit screensaver** when **Zoom**, **Teams** or **Skype for Business** meeting is **active**. Possible for native clients and Citrix optimization plugins.
  More...

Parameter	Enable debug logging for igel-screensaver-monitor
Registry	`debug.tools.igel-screensaver-monitor.enable`
Value	enabled / disabled

- Added functionality to **change the desktop icon font color** via new Setup parameter.
  More...

IGEL Setup	**User Interface > Desktop**
Parameter	Desktop Icon Font Color

Registry	`windowmanager.defaulttheme.desktop.iconfont_color`

CID Key Agent

- Update of **CID Key Agent** to version **6.5.0-2**

Driver

- Updated **Olympus dictation driver** for **Citrix** and **RDP** to version **20201118**.
  The changes are:
  - Support motion events for Olympus RecMic devices
  - Support integration with the Olympus AudioSDK for limited server-side device communication
- Updated **Crossmatch driver** to version **0125**.
  The changes are:
  - Improved USB encryption for the 4500 readers
  - Support for the 5300-101 reader (the 5300-100 was already supported)
- Updated **deviceTRUST** client plugin for **Citrix** and **RDP** to version **20.1.200.0**. Detailed release notes can be found at https://docs.devicetrust.com/docs/releases-igel-20.1.200/.

X11 system

- Enhanced `x.xserver%.mirror_mode` registry key with new **Scaling down mode** (Scales all monitors to the monitor with the lowest resolution)
  More...

Parameter	Choose the mode which should be used for mirroring monitors if resolution differs
Registry	`x.xserver%.mirror_mode`
Range	[Default] [Biggest common resolution] [Scaling] [Scaling down]

Audio

- Added **EPOS Connect 5.0.1.2795**
  More...

IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Enable EPOS Connect
Registry	`devices.epos.connect.enable`
Type	bool
Value	enabled / disabled
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Tenant ID

Registry	devices.epos.connect.tenant_id
Type	string
Value	''
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Backend Endpoint
Registry	devices.epos.connect.tenant_url
Type	string
Value	''
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Proxy
Registry	devices.epos.connect.proxy
Type	string
Value	''
Registry	devices.epos.connect.log_level
Value	Trace / Debug / Information / Warnings / Errors / Exceptions / No logs

- **Pulseaudio** upgraded to the **13.99** version.
- Added parameter to **differentiate sound volume for applications**. If the parameter is set to true, each application can set its own volume level. Otherwise, the sound volume is set to the same value as the default volume for output and input device respectively.
  More...

Registry	userinterface.sound.app_volume_ctrl
Value	true / false

Misc

- Added **DriveLock Agent 20.1.4.30482** for USB device access control.
  More...

IGEL Setup	**Devices > Storage Devices > DriveLock**
Parameter	Enable DriveLock agent
Registry	devices.drivelock.enable
Value	enabled / disabled

IGEL Setup	**Devices > Storage Devices > DriveLock**
Parameter	DES server URL
Registry	`devices.drivelock.server`
Value	(empty)
IGEL Setup	**Devices > Storage Devices > DriveLock**
Parameter	Tenant
Registry	`devices.drivelock.tenant`
Value	root

Evidian

- Added **new** session type **RD Web Access**.
- Updated **Evidian** to version **1.5.7617**.

Hardware

- Added hardware support for new **IGEL UD7-LX 20 (H860C)**.
- Added hardware support for **LG 34CN650N AiO**.
- Added hardware support for **Dell Wyse Z Class thin client**.
- Added hardware support for **Lenovo ThinkCentre M70q**.
- Added hardware support for **Dell Wyse 5470**.
- Added hardware support for **Lenovo L14**.
- Added hardware support for **Lenovo ThinkCentre M75n**.
- Added hardware support for **Lenovo 14w**.
- Added hardware support for **LG CN65 All in one**.
- Added hardware support for **DELL LATITUDE 5510**.
- Added hardware support for **ELO i2 Touch all-in-one (15 and 22) inch**.
- Added detection of **UD Pocket UC5-LX 2**.
- Added support for headset **Jabra Evolve2 65**.

Remote Management

- Added support for **Reportable Heartbeats to the UMS**.
- Added support for **exchanging ICG certificates**.
- The remote management of the endpoint device automatically installs TLS certificates provided by the UMS into the local trusted CA certificates storage. **The automatic deployment of TLS certificates to endpoint** devices **requires UMS 6.06.100 or higher**. This feature allows verifying certificates used in downloading files from the UMS, downloading of a firmware update and custom partition archives over HTTPS or FTPS protocols. The **verifying of certificates must be enabled by** the parameter `system.security.remote_management.tls_verify_peer`.
  More...

Registry	`system.security.remote_management.tls_verify_peer`
Value	true / <u>false</u>
Registry	`system.security.remote_management.tls_hostname_validation`
Value	<u>true</u> / false

- Added support for UMS commands to **store and remove ICG configuration**.
- Introduced parameters for **ICG Websocket connections**: **debug log**, **network timeout** (in seconds) and **ping-pong interval** (in seconds). The parameters are applied on the next established ICG agent connection and ICG tunnel connections: VNC and Secure Terminal.
  More...

Registry	`system.icg.websocket.debug`
Value	<u>off</u> / all / tunnel / agent
Registry	`system.icg.websocket.network_timeout`
Value	<u>30</u>
Registry	`system.icg.websocket.pingpong_interval`
Value	<u>120</u>

- IGEL Remote Management agent sends now **keep-alive packets to the ICG server to prevent the Websocket connection to the ICG server from being closed by networking infrastructure**. The Websocket's ping-pong mechanism is used for that purpose (see RFC6455). The **keep-alive interval** in seconds can be **configured by** the parameter `system.icg.websocket.pingpong_interval`, 0 disables the keep-alive mechanism.
  More...

Registry	`system.icg.websocket.pingpong_interval`
Value	<u>120</u>

Fabulatech

- Updated **FabulaTech USB for Remote Desktop** to version **6.0.28**
- Updated **FabulaTech Scanner for Remote Desktop** to version **2.7.0.1**
- Fixed **FabulaTech scanner redirection not working for Citrix** if it's exclusively enabled in IGEL Setup.

Resolved Issues 11.05.100

Citrix

- Fixed the problem with **apparmor** and the **Citrix MS Teams** workaround
- Following registry keys help to **edit horizontal and vertical window size** (works only for desktops not for applications).
  More...

Parameter	Set desired horizontal window dimension
Registry	`ica.allregions.desiredhres`
Value	[**] [640] [800] [1024] [1280] [1600]
Parameter	Set desired vertical window dimension
Registry	`ica.allregions.desiredvres`
Value	[**] [480] [600] [768] [1024] [1200]

- Citrix **Desktop** sessions **have a sound device** again, when using **smartcard watch daemon**.
  `scard.scwatchd.insert_action = su user -c /config/sessions/pnlogin0`
- Parameter `ica.module.virtualdrivers.vdwebrtc.keyboard_workaround` has been removed. This workaround is no longer needed because the problem is **solved as of CWA 20.10**.
- Added new parameters to **add config parameters** for **Citrix USB devices**: the parameter string is appended to the config line in `usb.conf`, when the **device is explicitly allowed**. Citrix introduced this to handle special behavior with single devices, e.g. to set "`disableselectconfig=1`".
  More...

Parameter	Extra Config
Registry	`ica.usbredirection.devicepolicy.product_rule%.parameter`
Type	String
Value	""
Parameter	Extra Config
Registry	`ica.usbredirection.devicepolicy.product_rule_igel%.parameter`
Type	String

Value	""

- Improved **Fabulatech USB Redirection** and **Scanner** Support
- New parameter added:
  More...

Parameter	Fabulatech loglevel
Registry	`ica.module.virtualdriver.fabulatech.loglevel`
Value	1

- Added new parameter **AckDelayThresh**: Max time (in milliseconds) between sending "resource free" message if any resources free. Default=350
  More...

Parameter	AckDelayThresh
Registry	`ica.module.AckDelayThresh`
Type	Integer
Value	350

- Added new parameter **AudioBufferSizeMilliseconds**: Audio buffer size, in ms. Default=200 ms
  More...

Parameter	AudioBufferSizeMilliseconds
Registry	`ica.module.AudioBufferSizeMilliseconds`
Type	Integer
Value	200

- Added new parameter **AudioLatencyControlEnabled**: Enables latency control. Default=False
  More...

Parameter	AudioLatencyControlEnabled
Registry	`ica.module.AudioLatencyControlEnabled`
Type	Boolean
Value	true / false

- Added new parameter **AudioMaxLatency**: Sets the maximum latency (in ms) before trying to discard audio data. Default=300 ms
  More...

Parameter	AudioMaxLatency
Registry	`ica.module.AudioMaxLatency`

Type	Integer
Value	300

- Added new parameter **AudioLatencyCorrectionInterval**: Defines how often to correct the latency (in ms). Default=300 ms
More...

Parameter	AudioLatencyCorrectionInterval
Registry	`ica.module.AudioLatencyCorrectionInterval`
Type	Integer
Value	300

- Added new parameter **AudioTempLatencyBoost**: Sets the higher latency band (in ms) above the lower PlaybackDelayThresh band. Default=300 ms
More...

Parameter	AudioTempLatencyBoost
Registry	`ica.module.AudioTempLatencyBoost`
Type	Integer
Value	300

- Added new parameter **CommandAckThresh**: Number of free client command buffers causing a "resource free" message to be sent to the server. Default=10
More...

Parameter	CommandAckThresh
Registry	`ica.module.CommandAckThresh`
Type	Integer
Value	10

- Added new parameter **DataAckThresh**: Number of free client data buffers causing a "resource free" message to be sent to the server. Default=10
More...

Parameter	DataAckThresh
Registry	`ica.module.DataAckThresh`
Type	Integer
Value	10

- Added new parameter **MaxDataBufferSize**: Maximum size of each data buffer. Default=2048 bytes
More...

Parameter	MaxDataBufferSize
Registry	`ica.module.MaxDataBufferSize`
Type	Integer
Value	2048

- Added new parameter **NumCommandBuffers**: Number of client buffers to use for audio commands. Default=64
  More...

Parameter	NumCommandBuffers
Registry	`ica.module.NumCommandBuffers`
Type	Integer
Value	64

- Added new parameter **PlaybackDelayThresh**: Delay (in ms) between being asked to start audio playback and actually starting audio playback in order to build up a backlog of sound. Default=150
  More...

Parameter	PlaybackDelayThresh
Registry	`ica.module.PlaybackDelayThresh`
Type	Integer
Value	150

- Fixed: **ICA Connection Center** starts again as expected.
- Fixed **Citrix Kerberos Passthrough** authentication.
- Added: When the **password has expired** but the **password change is not allowed** on the Citrix server, the **Citrix error message** is displayed.
- Added: The parameter for `mouseinput ica.wfclient.mousesendcontrolv` is available with this release on the Setup page **Sessions > Citrix > Citrix Global > Keyboard**.
- Added: The parameter for the **Citrix Connection bar** `ica.allregions.connectionbar` is available on the Setup page **Sessions > Citrix > Citrix Global > Window**.
- Fixed **Citrix sessions with H.264 hardware acceleration on and DRI3** off that crashed with error message: `The X Request 130.1 caused error: 10 BadAccess`.

OSC Installer

- Fixed **warning message after feature deselection for installations on 2 GB flashes**.
- Fixed a **display** issue with **Intel and Nvidia GPU**.

RDP/IGEL RDP Client 2

- Fixed **USB redirection** for RDP sessions.
- Added new parameter to enable/disable **dynamic drive mapping**.

More...

Registry	`rdp.winconnect.enable-dynamic-drivemapping`
Value	enabled / disabled
Registry	`sessions.winconnect%.option.enable-dynamic-drivemapping`
Range	Global Setting / On / Off

- Fixed **login information not** being **set after reboot**.
- Improved **error logging**.

WVD

- WVD now comes with **Qt 5.12.10** in order **to get fixes mainly for QWebEngine**. This should **fix** issues with **.htaccess protected login pages**.
- Fixed **proxy usage** for WVD feed download.

RD Web Access

- Fixed **RD Web Access Login** not working with **user@domain**.
- Fixed **RD Web Access username** not being set correctly **after reboot**.

VMware Horizon

- Fixed **remember last user** functionality in Horizon **local logon**
- Fixed **Local Logon Window** for visibility in **appliance mode**
- When using the **PCoIP** protocol, the **virtual channel** provided by VMware used **for both serial port and scanner redirection** may **hang on logout**.
  The virtual channel is not used when both redirection methods are set to "false" which is the default.
  For the usage of either one of these redirection methods, enable the corresponding parameter below **to prevent the logout freeze**.
  These settings can be found here in the IGEL Registry:
  `vmware.view.enable-serial-port-redir`
  `vmware.view.enable-scanner-redir`

Firefox

- Fixed **smartcard access** in Firefox. Before this fix, smartcards were not recognized in seldom cases.
- Fixed possibility to use the **pre-installed spellcheckers** in Firefox input fields.

Chromium

- Fixed **browser** and **download history not** being **cleared**.
- Fixed Chromium browser was not clearing browsing history properly.
- Fixed: **Custom Chromium Policies** datatypes now written in the correct way to `policies.json`
- Fixed **resetting kiosk mode** would only work **after reboot**
- Fixed: Chromium settings were **parent settings did not influence the child settings**

Network

- Added registry keys for enabling/disabling **sending of hostname in DHCPv4** and **DHCPv6 requests**.
  More...

Parameter	Send hostname in DHCP requests
Registry	`network.dhcp.send_hostname`
Range	[Disabled][Network Manager default]
Value	Network Manager default

Parameter	Send hostname in DHCPv6 requests
Registry	`network.dhcp6.send_hostname`
Range	[Disabled][Network Manager default]
Value	Network Manager default

- Fixed: **SCEP** failed when `scep_getca` received only a single certificate.
- Added registry key specifying **the number of 802.1X authentication attempts on Ethernet**.
  More...

Registry	`network.interfaces.ethernet.device%.ieee8021x.auth_attempts`
Type	Integer
Value	1

- The **default** value of `network.interfaces.ethernet.device%.nm_disable_link_config` (forbidding Network Manager to modify Ethernet link settings) has been **changed to "true"**.
- Fixed handling of **DNS default domain**
- Added registry key for **disabling Ethernet link reconfiguration by Network Manager**.
  More...

Parameter	Disable NetworkManager link configuration
Registry	`network.interfaces.ethernet.device%.nm_disable_link_config`
Type	bool
Value	true / false

- **Setting** this **to "true"** can be **beneficial when 802.1X authentication is disturbed**. It is currently enforced automatically in the case of e1000e drivers.

- **Changed default** value of **minimum size of a TCP packet** from 750 **to 500 bytes** as a result this would allow a **minimal MTU size of 576 bytes**.

Wi-Fi

- Added missing **iwlwifi-6000-4 firmware file**.
- Fixed issues with **D-Link DWA-131 WLAN dongle**.
- **Removed** `network.drivers.use_backport_drivers` IGEL registry key as this is not used anymore.
- Added some missing **iwlwifi firmware files** to IGEL OS.

Open VPN

- Fixed **segmentation fault** when nameserver is used.
  Now it is allowed to use an empty password for the private key. **Important**: **Not enter a password** when the private key doesn't have one.
- OpenConnect VPN: Different protocols are selectable:
  More...

Parameter	protocol
Registry	`sessions.openconnect%.vpnopts.protocol`
Value	Cisco AnyConnect / Juniper Network / Junos Pulse / PAN GlobalProtect

Imprivata

- Fixed: Usage the **Horizon Window Size** settings
- Fixed: Set **keyboard repeat rate** correctly on Horizon session end
- Added Imprivatas "**grid-theme**" feature
  More...

Parameter	PIE Application Launcher for Citrix
Registry	`imprivata.grid_theme`
Value	enabled / disabled

Smartcard

- Added parameter to **disable HID Global OMNIKEY smartcard reader driver**. **If** this driver is **disabled**, some of the readers are **handled by the MUSCLE CCID driver**. This can help when problems with OMNIKEY reader driver occur.
  More...

Parameter	HID Global OMNIKEY driver for smart card readers
Registry	`scard.pcscd.omnikey_enable`
Value	enabled / disabled

HID

- Fixing **double tapping of desktop icons** on **touchscreen** devices.

CUPS Printing

- Fixed **CUPS printer spooling configuration** where printjob files were preserved in the spooling directory too long and could fill up the file system.

Logging

- Fixed: **Filebeat** now **starts after the hostnames are set** so they will be shown in the logs.

Base system

- Fixed problems with **hostnames containing one or more "_"** characters.
- **Post-session command binaries and return codes are now customizable** via registry. Allows post-session commands if a binary doesn't return 0.
  - Name of the binary:
    More...

Parameter	Binary
Registry	`pcom.valid_return_codes%.binary`
Value	binary name

  - Comma-separated return codes (e.g. 7,99) or/and return code ranges (e.g. 3..5 for 3,4,5) to be accepted:
    More...

Parameter	Return Codes
Registry	`pcom.valid_return_codes%.returncodes`
Value	e.g. 3,5,10..15 for 3,5,10,11,12,13,14,15

- Improved **post-session** command parameter `pcom.valid_return_codes%.returncodes` to handle **ranges a la 1..255** (see tooltip).
- Fixed **remembering last user name with Active Directory/Kerberos** logon. Before this fix, the user name could not be stored in UMS to appear again after a reboot.
- Fixed possibility to **add certificates to Chromium and Firefox** which are given **in DER** format.
- Fixed **default browser** not being set properly **after reboot**.
- Fix **GtkMessage** dialog localization.
- Fixed: **Fluendo vadec codec** update closed a **memory leak** with AMD devices using VAAPI acceleration.
- Fixed possible USB issues with **suspend/resume on IGEL M350C** devices.
- Fixed: **Shutdown delay** when post-session command is enabled.
- Fixed **NetworkManager** could not create **ipv6 pid/lease file** while **apparmor** is active.
- Bugfix for missing **bluetooth tray icon** after suspend

Storage Devices

- Fixed display of **hotplug eject menu in appliance mode**

X11 system

- Fixed display **hotplug detection** not working in some situations.
- Fixed **Display Switch** sometimes **losing config** after reboot.
- Fixed missing **custom background image after migration** from OS 10.
- Fixed **sporadic hang in logoff session restart**.
- Updated **Display Switch rotate buttons** to have usable size.
- Added registry key to solve an issue with **buggy monitors connected over a DP-to-DVI adapter** (only works for Radeon devices like UD3 LX50).
  More...

Parameter	Fix issues with buggy monitors connected over DP-DVI adapter
Registry	`x.drivers.ati.dp_dvi_probe_workaround`
Type	bool
Value	enabled / disabled

- Fixed **touchpad** enable and disable **with hotkey**.
- Fixed issues if **2 DisplayPort MST Hubs** are connected behind each other.
- Fixed **notifications** not being hidden properly when **in do-not-disturb mode**.
- Fixed **monitor configuration** issues with **DisplayLink-based Dockingstations** with more than one independent monitor output.
- Fixed issue with non-correctly working **default mirror mode**.
- Fixed **screen** configuration issues with **Nvidia** and I**ntel graphics cards in one device**.
- Added: Allowance of **up to 8** different **custom wallpapers** (was limited to 4 up to now).
- Added notification mute-all parameter in Setup to **mute all notifications including urgent ones**.

X server

- Fixed tearing issue of **UD7 with additional graphic card**.

Window manager

- Fixed **desktop icons not** being **restricted to one monitor**.
- Fixed a bug where **icons** were **missing or miss-aligned** in some multiscreen setups.
- Fixed **notify window width** not remaining constant.
- Fixed **crash of start menu** when it is not populated with any items.
- Fixed **start monitor mapping for Firefox**.
- Fixed **notification urgency** for **critical background color**.

VirtualBox

- Fixed **authentication window popup** if screen configuration is changed in Virtualbox.

Audio

- Fixed erroneous **closing of the Pulse PCM device** as well as a possible **deadlock in the ALSA Pulse PCM**.
- Fixed the ALSA Pulse PCM - a possible deadlock while writing audio data and closing Pulse PCM.
- Fixed audio for **HP Elitebook TRRS 840 G7**
- Fixed **internal microphone** in **Elitebook TRRS 840 G7**
- Fixed **headset not** properly **detected** if connected on boot in **UD2-LX50**.
- Fixed microphone issues with **UD3-LX60** device.

- Fixed a **sporadic aborting of an application** on closing **ALSA Pulse PCM**. The problem concerns only applications using ALSA API directly, like Citrix Receiver.
- Added **debug output to the ALSA Pulse PCM** which must be **enabled by** the environment variable `ALSA_PULSE_PCM_DEBUG=1`, the debug output is collected then by the system logging facility (journalctl).
- Fixed **missing audio tray icon** after suspend

Evidian

- Fixed **error on restart**.

Hardware

- Added script to fix issues with **DP MST KVM** and **connected DaisyChaining monitors**.
- Fixed: When KVM is used, **mishandling of connectors** can occur.
  Added **possible workaround** via adding `/etc/igel/kms/kvm-workaround.sh` to the `userinterface.rccustom.custom_cmd_x11_init` registry key.

TC Setup (Java)

- Fixed problems with **passwords** of a length **longer than 127 characters**.

Remote Management

- Fixed **automatic establishment of the configured ICG connection** if the UMS Server is unreachable.
- Fixed **sending the user logoff message** to the UMS.
- Fixed: Disabled **Nagle caching algorithm** on the underlying TCP socket used for SSL connection between IGEL rmagent and UMS.
- Fixed **sporadic failures while retrieving the Unit ID** by the IGEL Remote Management agent.
- Fixed **ICG HA functionality** broken in the **11.04.100 release**.

VNC

- Fixed handling of **CapsLock status in VNC server**. Keyboard input now appears correctly also when CapsLock is active on the client or server side. This especially fixes upper case "umlaut" characters with Swiss German keyboard layout.

CA Certificates Contained in IGEL OS 11.05

IGEL OS 11.05 contains the following CA certificates:

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	`ACCVRAIZ1.crt`
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	`AC_RAIZ_FNMT-RCM.crt`
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	`Actalis_Authentication_Root_CA.crt`
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	`AffirmTrust_Commercial.crt`
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	`AffirmTrust_Networking.crt`
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	`AffirmTrust_Premium.crt`
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	`AffirmTrust_Premium_ECC.crt`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`AmazonRootCA1.pem`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`Amazon_Root_CA_1.crt`
Amazon Root CA 2	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Amazon Root CA 3	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_3.crt`
Amazon Root CA 4	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_4.crt`
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	`Atos_TrustedRoot_2011.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt`
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`BTCTRoot.pem`
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`Baltimore_CyberTrust_Root.crt`
Buypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	`Buypass_Class_2_Root_CA.crt`
Buypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	`Buypass_Class_3_Root_CA.crt`
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	`CA_Disig_Root_R2.crt`
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	`CFCA_EV_ROOT.crt`
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	`COMODO_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_ECC_Certification_Authority.crt`
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_RSA_Certification_Authority.crt`
Certigna	Jun 29 15:13:05 2027 GMT	`Certigna.crt`
Certigna Root CA	Oct 1 08:32:27 2033 GMT	`Certigna_Root_CA.crt`
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	`Certum_Trusted_Network_CA.crt`
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	`Certum_Trusted_Network_CA_2.crt`
Chambers of Commerce Root - 2008	Jul 31 12:29:50 2038 GMT	`Chambers_of_Commerce_Root_-_2008.crt`
Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	`Class3PCA_G2_v2.pem`
Class 4 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	`Class4PCA_G2_v2.pem`
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_AAA_Services_root.crt`
Cybertrust Global Root	Dec 15 08:00:00 2021 GMT	`Cybertrust_Global_Root.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	`D-TRUST_Root_Class_3_CA_2_2009.crt`
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	`D-TRUST_Root_Class_3_CA_2_EV_2009.crt`
DST Root CA X3	Sep 30 14:01:15 2021 GMT	`DST_Root_CA_X3.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCertGlobalRootCA.pem`
DigiCert Global Root CA	Mar 8 12:00:00 2023 GMT	`DigiCertSHA2SecureServerCA.pem`
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Assured_ID_Root_CA.crt`
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G2.crt`
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G3.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Global_Root_CA.crt`
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G3.crt`
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_High_Assurance_EV_Root_CA.crt`
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	`DigiCert_Trusted_Root_G4.crt`
E-Tugra Certification Authority	Mar 3 12:09:48 2023 GMT	`E-Tugra_Certification_Authority.crt`
EC-ACC	Jan 7 22:59:59 2031 GMT	`EC-ACC.crt`
Entrust.net[296] Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	`Entrust.net_Premium_2048_Secure_Server_CA.crt`
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	`Entrust_Root_Certification_Authority.crt`
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	`Entrust_Root_Certification_Authority_-_EC1.crt`
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	`Entrust_Root_Certification_Authority_-_G2.crt`
Entrust Root Certification Authority - G4	Dec 27 11:41:16 2037 GMT	`Entrust_Root_Certification_Authority_-_G4.crt`

296. http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	`GDCA_TrustAUTH_R5_ROOT.crt`
GlobalSign	Dec 15 08:00:00 2021 GMT	`GSR2.pem`
GTE CyberTrust Global Root	Aug 13 23:59:00 2018 GMT	`GTECTGlobalRoot.pem`
GTS Root R1	Jun 22 00:00:00 2036 GMT	`GTS_Root_R1.crt`
GTS Root R2	Jun 22 00:00:00 2036 GMT	`GTS_Root_R2.crt`
GTS Root R3	Jun 22 00:00:00 2036 GMT	`GTS_Root_R3.crt`
GTS Root R4	Jun 22 00:00:00 2036 GMT	`GTS_Root_R4.crt`
GeoTrust Global CA	May 21 04:00:00 2022 GMT	`GeoTrust_Global_CA.pem`
GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	`GeoTrust_Primary_Certification_Authority_-_G2.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R5.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	`GlobalSign_Root_CA.crt`
GlobalSign	Dec 15 08:00:00 2021 GMT	`GlobalSign_Root_CA_-_R2.crt`
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.crt`
GlobalSign	Dec 10 00:00:00 2034 GMT	`GlobalSign_Root_CA_-_R6.crt`
Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	`Global_Chambersign_Root_-_2008.crt`
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	`Go_Daddy_Class_2_CA.crt`
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Go_Daddy_Root_Certificate_Authority_-_G2.crt`
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	`Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt`
Hellenic Academic and Research Institutions RootCA 2011	Dec 1 13:49:52 2031 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt`
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	`Hongkong_Post_Root_CA_1.crt`
Hongkong Post Root CA 3	Jun 3 02:29:46 2042 GMT	`Hongkong_Post_Root_CA_3.crt`
ISRG Root X1	Jun 4 11:04:38 2035 GMT	`ISRG_Root_X1.crt`
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	`IdenTrust_Commercial_Root_CA_1.crt`
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	`IdenTrust_Public_Sector_Root_CA_1.crt`
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	`Imprivata.crt`
Izenpe.com[297]	Dec 13 08:27:25 2037 GMT	`Izenpe.com.crt`
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	`Microsec_e-Szigno_Root_CA_2009.crt`
Microsoft ECC Root Certificate Authority 2017	Jul 18 23:16:04 2042 GMT	`Microsoft_ECC_Root_Certificate_Authority_2017.crt`
Microsoft RSA Root Certificate Authority 2017	Jul 18 23:00:23 2042 GMT	`Microsoft_RSA_Root_Certificate_Authority_2017.crt`
NAVER Global Root Certification Authority	Aug 18 23:59:59 2037 GMT	`NAVER_Global_Root_Certification_Authority.crt`

297. http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
NetLock Arany (Class Gold) Főtanúsítvány	Dec 6 15:08:21 2028 GMT	`NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt`
Network Solutions Certificate Authority	Dec 31 23:59:59 2029 GMT	`Network_Solutions_Certificate_Authority.crt`
OISTE WISeKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	`OISTE_WISeKey_Global_Root_GB_CA.crt`
OISTE WISeKey Global Root GC CA	May 9 09:58:33 2042 GMT	`OISTE_WISeKey_Global_Root_GC_CA.crt`
Class 3 Public Primary Certification Authority	Aug 1 23:59:59 2028 GMT	`Pcs3ss_v4.pem`
QuoVadis Root Certification Authority	Mar 17 18:33:33 2021 GMT	`QuoVadis_Root_CA.crt`
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	`QuoVadis_Root_CA_1_G3.crt`
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	`QuoVadis_Root_CA_2.crt`
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	`QuoVadis_Root_CA_2_G3.crt`
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	`QuoVadis_Root_CA_3.crt`
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	`QuoVadis_Root_CA_3_G3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
SSL.com[298] EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	`SSL.com_EV_Root_Certification_Authority_ECC.crt`
SSL.com[299] EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	`SSL.com_EV_Root_Certification_Authority_RSA_R2.crt`
SSL.com[300] Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	`SSL.com_Root_Certification_Authority_ECC.crt`
SSL.com[301] Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	`SSL.com_Root_Certification_Authority_RSA.crt`
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	`SZAFIR_ROOT_CA2.crt`
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	`SecureSign_RootCA11.crt`
SecureTrust CA	Dec 31 19:40:55 2029 GMT	`SecureTrust_CA.crt`
Secure Global CA	Dec 31 19:52:06 2029 GMT	`Secure_Global_CA.crt`
Security Communication RootCA2	May 29 05:00:39 2029 GMT	`Security_Communication_RootCA2.crt`
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	`Security_Communication_Root_CA.crt`

298. http://SSL.com
299. http://SSL.com
300. http://SSL.com
301. http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
Sonera Class2 CA	Apr 6 07:29:40 2021 GMT	`Sonera_Class_2_Root_CA.crt`
Staat der Nederlanden EV Root CA	Dec 8 11:10:28 2022 GMT	`Staat_der_Nederlanden_EV_Root_CA.crt`
Staat der Nederlanden Root CA - G3	Nov 13 23:00:00 2028 GMT	`Staat_der_Nederlanden_Root_CA_-_G3.crt`
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	`Starfield_Class_2_CA.crt`
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Root_Certificate_Authority_-_G2.crt`
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Services_Root_Certificate_Authority_-_G2.crt`
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	`SwissSign_Gold_CA_-_G2.crt`
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	`SwissSign_Silver_CA_-_G2.crt`
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_2.crt`
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	`TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt`
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	`TWCA_Global_Root_CA.crt`
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	`TWCA_Root_Certification_Authority.crt`
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	`TeliaSonera_Root_CA_v1.crt`
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	`TrustCor_ECA-1.crt`
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	`TrustCor_RootCert_CA-1.crt`
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	`TrustCor_RootCert_CA-2.crt`
Trustis FPS Root CA	Jan 21 11:36:54 2024 GMT	`Trustis_FPS_Root_CA.crt`
Trustwave Global Certification Authority	Aug 23 19:34:12 2042 GMT	`Trustwave_Global_Certification_Authority.crt`
Trustwave Global ECC P256 Certification Authority	Aug 23 19:35:10 2042 GMT	`Trustwave_Global_ECC_P256_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Trustwave Global ECC P384 Certification Authority	Aug 23 19:36:43 2042 GMT	`Trustwave_Global_ECC_P384_Certification_Authority.crt`
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	`UCA_Extended_Validation_Root.crt`
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	`UCA_Global_G2_Root.crt`
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_ECC_Certification_Authority.crt`
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_RSA_Certification_Authority.crt`
VeriSign Universal Root Certification Authority	Dec 1 23:59:59 2037 GMT	`VeriSign_Universal_Root_Certification_Authority.crt`
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	`XRamp_Global_CA_Root.crt`
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	`certSIGN_ROOT_CA.crt`
certSIGN ROOT CA G2	Feb 6 09:27:35 2042 GMT	`certSIGN_Root_CA_G2.crt`
e-Szigno Root CA 2017	Aug 22 12:07:06 2042 GMT	`e-Szigno_Root_CA_2017.crt`
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	`ePKI_Root_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
emSign ECC Root CA - C3	Feb 18 18:30:00 2043 GMT	`emSign_ECC_Root_CA_-_C3.crt`
emSign ECC Root CA - G3	Feb 18 18:30:00 2043 GMT	`emSign_ECC_Root_CA_-_G3.crt`
emSign Root CA - C1	Feb 18 18:30:00 2043 GMT	`emSign_Root_CA_-_C1.crt`
emSign Root CA - G1	Feb 18 18:30:00 2043 GMT	`emSign_Root_CA_-_G1.crt`

Notes for Release 11.04.270

Software:	Version	11.04.270
Release Date:	2021-02-11	
Release Notes:	Version	RN-1104270-1
Last update:	2021-02-10	

- Supported Devices 11.04.270 (see page 3062)
- Component Versions 11.04.270 (see page 3063)
- General Information 11.04.270 (see page 3070)
- Known Issues 11.04.270 (see page 3071)
- Security Fixes 11.04.270 (see page 3075)
- New Features 11.04.270 (see page 3076)
- Resolved Issues 11.04.270 (see page 3078)

Supported Devices 11.04.270

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[302].

302. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.04.270

Clients

Product	Version
Chromium	83.0.4103.61-0ubuntu0.18.04.1
Cisco JVDI Client	12.9.3
Cisco Webex Teams VDI Client	41.1.0.17621
Cisco Webex Meetings VDI Client	41.2.0.142
Zoom Media Plugin	5.4.53376
Citrix HDX Realtime Media Engine	2.9.0-2330
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.10.0.6
Citrix Workspace App	20.12.0.12
deviceTRUST Citrix Channel	20.1.200.0
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7617
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	6.0.28
Firefox	68.12.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1600249269
IGEL WVD Client	1.0.21igel1608136172
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	20.1.200.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8

Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.2.1
Spice GTK (Red Hat Virtualization)	0.38-2igel93
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	20.10.0-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7.5.88
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-4igel13
VMware Horizon Client	5.5.0-16946361
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20200323
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000

PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.20.0-3igel37
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.3
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth stack (bluez)	5.52-1igel6
MESA OpenGL stack	20.0.8-1igel117
VAAPI ABI Version	0.40
VDPAU Library version	1.4-1igel1003
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-1+git20200220igel987
Graphics Driver ATI/AMDGPU	19.1.0-1+git20200318igel986

Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	440.100-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.36.1-0ubuntu2igel888
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.4.48 #mainline-lxos-g1607354578
Xorg X11 Server	1.20.8-2igel1016
Xorg Xephyr	1.20.8-2igel1016
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel105
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.90
GStreamer 0.10 Fluendo h264dec	0.10.58
GStreamer 0.10 Fluendo mp3dec	0.10.40

GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.224
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.16.2-4igel239
GStreamer 1.0 Fluendo aacdec	0.10.42.2-8d6d
GStreamer 1.0 Fluendo asfdemux	0.10.90
GStreamer 1.0 Fluendo h264dec	0.10.58
GStreamer 1.0 Fluendo mp3dec	0.10.40
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.224
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.28.3-2igel36
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.10-dfsg-1igel41
Virtualbox X11 Guest Utils	6.1.10-dfsg-1igel41
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-1igel95
Qemu Guest Agent	5.0-5igel12

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5

Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-2igel4
VPN OpenConnect	8.10-1igel4
Scanner support	1.0.27-1
VirtualBox	6.1.10-dfsg-1igel41

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	235.5 M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	70.5 M	Included
VMware Horizon RDP	4.2. M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	123.2 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	7.5 M	Included
IBM i Access Client Solutions	72.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included

NVIDIA graphics driver	115.0 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.5 M	Included
Hardware Video Acceleration	13.0 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	48.0 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	14.0 M	Included
Local Browser (Chromium)	81.2 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	36.8 M	Not included
Cisco Webex Meetings VDI	32.2 M	Not included
Zoom Media Plugin	40.5 M	Not included
Teradici PCoIP Client	14.5 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.5 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	62.5 M	Not included

General Information 11.04.270

To be beneficial to all new features and implementations, it is recommended to use UMS 6.06.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.04.270

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check Updating to IGEL OS 11.04 or Higher on a Device with Small Storage (see page 3071) for a solution.

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.09**, **webcam redirection** or **screen sharing** may lead to **display errors** like black stripes or flickering.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- **Modifier keys** (`Shift/Ctrl/Win/Alt`) in session windows using **RDP protocol** do not send the keyup event and **keep being pressed**, even when actually released. Only when closing the session with a mouse, the modifiers are reset.
- **Copying a text from Horizon Blast** sessions is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon. Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:
  - `userinterface.softkeyboard.autoshow`
  - `userinterface.softkeyboard.autohide`

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

Cisco JVDI Client

- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).

deskMate

- Some stability issues may remain.

Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Security Fixes 11.04.270

VNC

- Fixed **Secure Terminal** and **Secure VNC Shadowing** remote code execution vulnerability.

New Features 11.04.270

Citrix

- Integrated **Zoom Media Plugin 5.4.53376.1029**
- Integrated **Citrix Workspace App 20.12**
  Available Citrix Workspace apps in this release: **20.12** (default), **20.10**, and 19.12.
- New Feature: **App Protection [Experimental]**. App Protection is an add-on feature that provides **enhanced security when using Citrix Virtual Apps and Desktops**. The feature **restricts the ability of clients to be compromised by keylogging and screen capturing malware**.
  More...

Parameter	Citrix App Protection
Registry	`ica.appprotection`
Value	enabled / disabled
Note:	Experimental feature This feature is **currently only available for Self-Service sessions**.

- Fixed Issue: **mic** and **webcam** devices can be **redirected using Browser Content Redirection**.
  More...

Parameter	Enables mic and webcam redirection using BCR
Registry	`ica.allregions.cefenablemediadevices`
Value	[Factory default is "*"] [False][True]

VMware Horizon

- Integrated **Zoom Media Plugin 5.4.53376.1029**
- Updated VMware Horizon Client to version **5.5.0-16946361**

Smartcard

- Added **Smartcard PIN passthrough in Firefox** and **Chromium**. The PIN will be **cached while logging on via Active Directory/Kerberos** with a smartcard. In Firefox and Chromium, no further PIN input is necessary to use the smartcard.
  More...

Parameter	Smartcard PIN caching
Registry	`scard.pkcs11.pin_cache.enable`
Value	enabled / disabled

Cisco JVDI Client

- Integrated **Cisco JVDI 12.9.3** client

Cisco Webex

- Integrated **Cisco Webex Meetings 41.2.0.142**
- Integrated **Cisco Webex Teams 41.1.0.17621**

Evidian

- New session type **RD Web Access**.
- Updated Evidian to version **1.5.7617**.

Audio

- Added parameter to **control applying of sound volume to application's streams**. If the parameter is set to "true", each application can set its own volume level. Otherwise, the sound volume is set to the same value as the default volume for output and input device respectively. **More...**

Registry	`userinterface.sound.app_volume_ctrl`
Value	enabled / disabled

Resolved Issues 11.04.270

Citrix

- Fixed Citrix **Kerberos Passthrough authentication**.
- The parameter `ica.module.virtualdrivers.vdwebrtc.keyboard_workaround` has been **removed**. This workaround is **no longer needed** because **the problem is solved as of CWA 20.10**.

VMware Horizon

- Fixed failure to start Horizon **serial port redirection service at boot time**.
- Fixed **remember last user functionality in Horizon local logon**.
- Fixed **VMware integrated printing**.

RDP/IGEL RDP Client 2

- Added **new parameter** to enable/disable **dynamic drive mapping**.
  More...

Registry	`rdp.winconnect.enable-dynamic-drivemapping`
Value	enabled / disabled
Registry	`sessions.winconnect%.option.enable-dynamic-drivemapping`
Range	Global setting / on / off

- Fixed **login information** not being set after reboot.

RD Web Access

- Fixed RD Web Access **login not working with user@domain**.

WVD

- Fixed **proxy usage for WVD feed download**.

Parallels Client

- Fixed a bug with Parallels not working if the **Parallels RAS omits the machine name in the application list**.

Evidian

- Fixed **error on restart**.

Firefox

- Fixed usage of a **pre-installed spellchecker in Firefox** input fields.
- Added **TLS 1.3** to the range of "**Maximum supported encryption protocol**" from **Sessions > Firefox Browser > Firefox Browser Global > Encryption**.
  More...

Parameter	Maximum supported encryption protocol

Registry	`browserglobal.app.security_tls_version_max`
Range	[SSL3] [TLS 1.0] [TLS 1.1] [TLS 1.2] [TLS 1.3]

Chromium

- Fixed: **Custom Chromium Policies** datatypes now **written** in the correct way to **policies.json**.
- Fixed **browser** and **download history not** being **cleared**.

Audio

- Fixed a **sporadic aborting** of an application **on closing ALSA Pulse PCM**. The problem affects only applications using ALSA API directly like Citrix Workspace App.
- Added **debug output to the ALSA Pulse PCM** which **must be enabled by** the environment variable `ALSA_PULSE_PCM_DEBUG=1`, the debug output is collected by the system logging facility (`journalctl`).
- Fixed **missing default setup device** after **reboot**.

VNC

- Fixed handling of **CapsLock status in VNC server**. Keyboard input now appears correctly, also if CapsLock is active on the client or server side. **This especially fixes upper case 'umlaut' characters** with Swiss and German keyboard layouts.

Network

- Fixed bug: SCEP **failed** when `scep_getca` **received only a single certificate**.

Base system

- Fixed issue with early **IGEL UD3-LX 60** (M350C) revisions that can lead to **read error from MMC**.
- Fixed **crash of IGEL monitoring agent**.
- Fixed possibility to **add certificates** to **Chromium** and **Firefox** which are given in **DER format**.
- The **Options dialog** keeps the **settings** that were **previously set**.
- Fix **GtkMessage dialog localization**.
- Fixed: **Shutdown delay** when **Post-session command** is enabled.
- Fixed **remembering last user name with Active Directory/Kerberos logon**. Before this fix, the user name could not be stored in the UMS to appear again after a reboot.

X11 system

- Added registry key to solve an issue with **buggy screens connected over a DP-to-DVI adapter** (only works for Radeon devices like IGEL UD3-LX 50).
  More...

Parameter	Fix issues with buggy monitors connected over DP-DVI adapter
Registry	`x.drivers.ati.dp_dvi_probe_workaround`
Value	enabled / disabled

- Updated **Display Switch rotate buttons** to usable size.

- Fixed **notifications not being hidden properly** when in **do-not-disturb mode**.

Window manager

- Fixed `notifyd` window **width not** remaining **constant**.
- Fixed **notification urgency critical background color**.

OS Converter

- Fixed **language chooser** in installations via **Deployment Appliance**.

Notes for Release 11.04.240

Software:	Version	11.04.240
Release Date:	2020-11-16	
Release Notes:	Version	RN-1104240-1
Last update:	2020-11-16	

- Supported Devices 11.04.240 (see page 3082)
- Component Versions 11.04.240 (see page 3083)
- General Information 11.04.240 (see page 3090)
- Known Issues 11.04.240 (see page 3091)
- Security Fixes 11.04.240 (see page 3095)
- New Features 11.04.240 (see page 3096)
- Resolved Issues 11.04.240 (see page 3099)

Supported Devices 11.04.240

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[303].

303. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.04.240

Clients

Product	Version
Chromium	83.0.4103.61-0ubuntu0.18.04.1
Cisco JVDI Client	12.9.1
Cisco Webex Teams VDI Client	3.0.16605.0
Cisco Webex Meetings VDI Client	40.10.5.2377
Zoom Media Plugin	5.4.53376
Citrix HDX Realtime Media Engine	2.9.0-2330
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.09.0.15
Citrix Workspace App	20.10.0.6
deviceTRUST Citrix Channel	20.1.200.0
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	6.0.28
Firefox	68.12.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1600249269
IGEL WVD Client	1.0.16igel1605091446
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	20.1.200.0
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8

Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.2.1
Spice GTK (Red Hat Virtualization)	0.38-2igel93
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	20.10.0-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7.5.88
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-4igel13
VMware Horizon Client	5.4.1-15988340
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20200323
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000

PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.20.0-3igel37
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.3
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth stack (bluez)	5.52-1igel6
MESA OpenGL stack	20.0.8-1igel117
VAAPI ABI Version	0.40
VDPAU Library version	1.4-1igel1003
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-1+git20200220igel987
Graphics Driver ATI/AMDGPU	19.1.0-1+git20200318igel986

Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	440.100-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.8825
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.36.1-0ubuntu2igel888
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.4.48 #mainline-lxos-g1605521351
Xorg X11 Server	1.20.8-2igel1016
Xorg Xephyr	1.20.8-2igel1016
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel105
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 0.10 Fluendo aacdec	0.10.42
GStreamer 0.10 Fluendo asfdemux	0.10.90
GStreamer 0.10 Fluendo h264dec	0.10.58
GStreamer 0.10 Fluendo mp3dec	0.10.40

GStreamer 0.10 Fluendo mpegdemux	0.10.85
GStreamer 0.10 Fluendo mpeg4videodec	0.10.44
GStreamer 0.10 Fluendo vadec	0.10.224
GStreamer 0.10 Fluendo wmadec	0.10.70
GStreamer 0.10 Fluendo wmvdec	0.10.66
GStreamer 1.x	1.16.2-4igel239
GStreamer 1.0 Fluendo aacdec	0.10.42.2-8d6d
GStreamer 1.0 Fluendo asfdemux	0.10.90
GStreamer 1.0 Fluendo h264dec	0.10.58
GStreamer 1.0 Fluendo mp3dec	0.10.40
GStreamer 1.0 Fluendo mpeg4videodec	0.10.44
GStreamer 1.0 Fluendo vadec	0.10.224
GStreamer 1.0 Fluendo wmadec	0.10.70
GStreamer 1.0 Fluendo wmvdec	0.10.66
WebKit2Gtk	2.28.3-2igel36
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.10-dfsg-1igel41
Virtualbox X11 Guest Utils	6.1.10-dfsg-1igel41
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-1igel95
Qemu Guest Agent	5.0-5igel12

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5

Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-2igel4
VPN OpenConnect	8.10-1igel4
Scanner support	1.0.27-1
VirtualBox	6.1.10-dfsg-1igel41

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	235.8 M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Local Browser (Firefox) Citrix Appliance	70.5 M	Included
VMware Horizon RDP	4.2. M	Included
Cendio ThinLinc	10.0 M	Included
Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	116.0 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	7.5 M	Included
IBM i Access Client Solutions	72.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included

NVIDIA graphics driver	115.0 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	13.0 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	48.0 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	14.0 M	Included
Local Browser (Chromium)	81.2 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	33.2 M	Not included
Cisco Webex Meetings VDI	40.8 M	Not included
Zoom Media Plugin	40.5 M	Not included
Teradici PCoIP Client	14.5 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.5 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	62.5 M	Not included

General Information 11.04.240

To be beneficial to all new features and implementations, it is recommended to use UMS 6.06.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.04.240

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check Updating to IGEL OS 11.04 or Higher on a Device with Small Storage (see page 3091) for a solution.

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.09**, **webcam redirection** or **screen sharing** may lead to **display errors** like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.
  A possible **workaround** is to **disable** the **virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - `ica.module.virtualdriver.vdwebrtc.enable`
  - `ica.module.virtualdriver.nsap.enable`

  The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- **Modifier keys** (`Shift/Ctrl/Win/Alt`) in session windows using **RDP protocol** do not send the keyup event and **keep being pressed**, even when actually released. Only when closing the session with a mouse, the modifiers are reset.
- **Copying a text from Horizon Blast** sessions is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** does not work correctly with local logon. Workaround: **Switch off local logon** and switch on the corresponding two keys via IGEL registry:

- `userinterface.softkeyboard.autoshow`
- `userinterface.softkeyboard.autohide`

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

Cisco JVDI Client

- There may be a **segfault shown in the logs** (during logout of Citrix Desktop session). This occurs only when using **Citrix Workspace app 20.10 and Cisco JVDI**.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is only **supported** by **UMS version 6.05.100 or newer**.

Base system

- **Update from memory stick** requires network online state (at least when multiple update stages are involved).

deskMate

- Some stability issues may remain.

Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Security Fixes 11.04.240

Base system

- Fixed **BleedingTooth** security issue which means CVE-2020-12351, CVE-2020-12352, and CVE-2020-24490.

New Features 11.04.240

Citrix

- Integrated **Citrix Workspace app 20.10**.
  Available Citrix Workspace apps in this release: **20.10 (default)**, **20.09**, and **19.12**
- Added: **Multiple audio devices can be mapped inside the sessions**. This will display audio devices with their device name and not only HDX audio anymore:
  More...

Parameter	Multiple Audio Device support
Registry	`ica.module.vdcamversion4support`
Type	bool
Value	enabled / disabled

  Note: Bluetooth devices are currently not supported for device redirection.

- Updates **Zoom Media Plugin** to version **5.4.53376.1029**

VMware Horizon

- Updated **Zoom Media Plugin** to version **5.4.53376.1029**
- Added support for **VMware Integrated Printing**.
  More...

Parameter	Integrated Printing
Registry	`vmware.view.integrated-printing`
Type	bool
Value	enabled / disabled

WVD

- New parameter to set **HTTP user agent string for AAD login requests**.
  More...

Parameter	HTTP user agent string
Registry	`sessions.wvd%.options.http-user-agent`
Type	editable
Value	System Default / Windows / Android / iOS / macOS / <custom-string>

Cisco Webex VDI

- Updated **Cisco Webex Teams VDI** to version **3.0.16605.0**
- Updated **Cisco Webex Meetings VDI** to version **40.10**

Cisco JVDI Client

- Updated **Cisco JVDI client** to version **12.9.1**

Fabulatech

- Updated **FabulaTech USB for Remote Desktop** to version **6.0.28**
- Updated **FabulaTech Scanner for Remote Desktop** to version **2.5.0.7**

Driver

- Updated **deviceTRUST** client plugin for Citrix and RDP to version **20.1.200.0**. Detailed release notes can be found at https://docs.devicetrust.com/docs/releases-igel-20.1.200/

Remote Management

- Added **support for exchanging ICG certificates**.
- The remote management of the endpoint device **automatically installs TLS certificates provided by the UMS into the local trusted CA certificates storage**. The **automatic deployment** of TLS certificates to endpoint devices **requires UMS 6.06.100 or higher**. This feature allows verifying certificates used when downloading files from the UMS, downloading a firmware update and custom partition archives over HTTPS or FTPS protocols. **The verifying of certificates must be enabled** by the parameter `system.security.remote_management.tls_verify_peer`.
  More...

Registry	`system.security.remote_management.tls_verify_peer`
Value	enabled / disabled
Registry	`system.security.remote_management.tls_hostname_validation`
Value	enabled / disabled

- Added support for **UMS commands to store and remove ICG configuration**.
- Introduced parameters for **ICG Websocket connections**: debug log, network timeout (in seconds), and ping-pong interval (in seconds). The **parameters** are **applied on the next** established **ICG agent connection** and **ICG tunnel connections**: VNC and Secure Terminal. The **ping-pong** mechanism is supported **only for ICG tunnel connections**.
  More...

Registry	`system.icg.websocket.debug`
Value	off / all / tunnel / agent
Registry	`system.icg.websocket.network_timeout`
Value	30
Registry	`system.icg.websocket.pingpong_interval`

Value	120

Resolved Issues 11.04.240

Citrix

- Fixed issue with **Workspace app 2010**: **Screen flickering** while running a video call or sharing the screen in Microsoft Teams.
- Fixed Issue with **Workspace app 2010**: **Microsoft Teams** calls are now working with **different keyboard layouts**.
- Fixed: **Improved pcom** parameter `pcom.valid_return_codes%.returncodes` to handle ranges a la 1..255 (see tooltip).

Wi-Fi

- Fixed issues with **D-Link DWA-131 WLAN dongle**.

X11 system

- Fixed a problem with **display hotplug detection** when the display switch is not used.
- Fixed issues if **2 DisplayPort MST Hubs** are connected behind each other.

WVD

- **WVD memory leak(s**) fixed.
- Switched back to **the local login mask when the AAD login fails** for whatever reason. At the moment, there is no error message shown. This will come in one of the next versions.

VMware Horizon

- Fixed **post-session behavior** for VMware Horizon sessions where some **exit codes of the client were discarded** and therefore did not trigger the post-session action.
- Fixed **Local Logon Window** in that now we prevent it to get iconified because it always needs to be visible, especially in appliance mode where there is no panel to de-iconify it.

CID Key Agent

- Update of **CID Key Agent** to version **6.5.0-1**

Teradici PCoIP Client

- Updated **Teradici PCoIP** client to version **20.10**

Network

- Changed: Usage of **r8168** as default network driver **on Lenovo M75 Nano**.
- Added support for some newer I**ntel e1000e network cards**.
- Fixed **logon by 802.1X authentication**.
- Fixed: Failing **Ethernet connection does not delay online state** reached by other means anymore.
- Added registry keys for enabling/disabling **sending of hostname in DHCPv4 and DHCPv6** requests.
  More...

Parameter	Send hostname in DHCP requests

Registry	`network.dhcp.send_hostname`
Range	[Disabled][Network Manager default]
Parameter	Send hostname in DHCPv6 requests
Registry	`network.dhcp6.send_hostname`
Range	[Disabled][Network Manager default]

- Added registry key for **disabling Ethernet link reconfiguration by Network Manager**.
More...

Parameter	Disable NetworkManager link configuration
Registry	`network.interfaces.ethernet.device%.nm_disable_link_config`
Type	bool
Value	true / false
Note	Setting this to "true" can be beneficial when 802.1X authentication is disturbed by link. It is currently set automatically when e1000e drivers are used.

Open VPN

- Fixed **segmentation fault** if the nameserver is used.
Now it is allowed to use an empty password for the private key. Not needed to enter a password when the private key does not have one.

Base system

- Fixed: The **fluendo vadec** update closed a **memory leak with AMD devices** using VAAPI acceleration.
- **Updated Fluendo multimedia codecs** to the following versions:
More...

gst-fluendo-aacdec	8/10/2020
gst-fluendo-asfdemux	17/9/2020
gst-fluendo-h264dec	22/9/2020
gst-fluendo-mp3	17/9/2020
gst-fluendo-mpeg4video	18/9/2020
gst-fluendo-vadec	02/11/2020
gst-fluendo-wmadec	17/9/2020
gst-fluendo-wmvdec	17/9/2020

- Fixed possible **USB issues with suspend/resume on IGEL M350C** devices.
- Fixed: **Custom applications** did not run **while being offline** even if they did not need network.

Audio

- Fixed the **ALSA Pulse PCM** - a possible **deadlock** while writing audio data and closing Pulse PCM.
- Fixed **microphone** issues with **UD3-LX60** device.

Remote Management

- Fixed sporadic **failures while retrieving the Unit ID** by the IGEL Remote Management agent.
- Fixed **sending the user logoff message to the UMS**.

HID

- Updated **eGTouch (eGalax) drivers and xorg** configuration.
- Fixing **double tapping of desktop icons on touchscreen** devices.

Window manager

- Fixed **desktop icons** not being restricted to one monitor at all.

Notes for Release 11.04.200

Software:	Version	11.04.200
Release Date:	2020-10-08	
Release Notes:	Version	RN-1104200-1
Last update:	2020-10-08	

- Supported Devices 11.04.200 (see page 3103)
- Component Versions 11.04.200 (see page 3104)
- General Information 11.04.200 (see page 3111)
- Known Issues 11.04.200 (see page 3112)
- Security Fixes 11.04.200 (see page 3116)
- New Features 11.04.200 (see page 3117)
- Resolved Issues 11.04.200 (see page 3120)

Supported Devices 11.04.200

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[304].

304. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.04.200

Clients

Product	Version
Chromium	83.0.4103.61-0ubuntu0.18.04.1
Cisco JVDI Client	12.9.0
Cisco Webex Teams VDI Client	3.0.15711.0
Cisco Webex Meetings VDI Client	40.10.0.171
Zoom Media Plugin	5.2.456413
Citrix HDX Realtime Media Engine	2.9.0-2330
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.09.0.15
deviceTRUST Citrix Channel	19.1.200.2
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.12.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2igel1600249269
IGEL WVD Client	1.0.13igel1596142398
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8

Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.2.1
Spice GTK (Red Hat Virtualization)	0.38-2igel93
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	20.04.2-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7.5.88
Totem Media Player	2.30.2-0ubuntu1igel55
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-4igel13
VMware Horizon Client	5.4.1-15988340
Voip Client Ekiga	4.0.1-9build1igel6

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20200323
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.6.0.0-AET.000

PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.20.0-3igel37
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.3
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth stack (bluez)	5.52-1igel6
MESA OpenGL stack	20.0.8-1igel117
VAAPI ABI Version	0.40
VDPAU Library version	1.4-1igel1003
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-1+git20200220igel987
Graphics Driver ATI/AMDGPU	19.1.0-1+git20200318igel986

Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	440.100-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.7413
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.36.1-0ubuntu2igel888
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.4.48 #mainline-lxos_dev-g1595410170
Xorg X11 Server	1.20.8-2igel1016
Xorg Xephyr	1.20.8-2igel1016
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1600339249
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel100
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 1.x	1.16.2-4igel239
WebKit2Gtk	2.28.3-2igel36
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.10-dfsg-1igel41
Virtualbox X11 Guest Utils	6.1.10-dfsg-1igel41
Open VM Tools	11.0.5-4ubuntu0.18.04.1
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-1igel95
Qemu Guest Agent	5.0-5igel12

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-2igel4
VPN OpenConnect	8.10-1igel4
Scanner support	1.0.27-1
VirtualBox	6.1.10-dfsg-1igel41

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	24.8 M	Included
Java SE Runtime Environment	42.8 M	Included
Citrix Appliance Citrix Workspace app Citrix StoreFront	258.5 M	Included
Ericom PowerTerm InterConnect	17.8 M	Included
Media Player	768.0 K	Included
Local Browser (Firefox) Citrix Appliance	81.8 M	Included
VMware Horizon RDP	5.5. M	Included

Cendio ThinLinc	11.5 M	Included
Printing (Internet printing protocol CUPS)	23.8 M	Included
NoMachine NX	31.5 M	Included
VMware Horizon	193.2 M	Included
Voice over IP (Ekiga)	7.2 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	30.8 M	Not included
Fluendo GStreamer Codec Plugins	8.5 M	Included
IBM i Access Client Solutions	96.2 M	Not included
Red Hat Enterprise Virtualization	3.5 M	Included
Parallels Client	6.2 M	Included
NVIDIA graphics driver	128.5 M	Not included
Imprivata Appliance	16.0 M	Included
Evidian AuthMgr	3.0 M	Included
Hardware Video Acceleration	15.0 M	Included
Extra Font Package	1.2 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	54.8 M	Included
Cisco JVDI client	56.0 M	Included
PrinterLogic	50.8 M	Not included
Biosec BS Login	10.2 M	Not included
Login VSI Login Enterprise	32.8 M	Not included
Stratusphere UX CID Key software	3.2 M	Not included
Elastic Filebeat	25.0 M	Not included
WVD	16.2 M	Included
Local Browser (Chromium)	91.0 M	Not included
deskMate client	6.5 M	Included
Cisco Webex Teams VDI	40.2 M	Not included
Cisco Webex Meetings VDI	46.0 M	Not included

Zoom Media Plugin	42.0 M	Not included
Teradici PCoIP Client	8.8 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	512.0 K	Not included
VPN OpenConnect (Limited support)	1.8 M	Not included
Scanner support / SANE (Limited support)	2.8 M	Not included
VirtualBox (Limited support)	69.0 M	Not included

General Information 11.04.200

To be beneficial to all new features and implementations, it is recommended to use UMS 6.05.110 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.04.200

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs. Check Error: "Not enough space on local drive" when Updating to IGEL OS 11.08 or Higher (see page 318) for a solution.

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06/20.09**, **webcam redirection** or **screen sharing** may lead to **display error**s like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.
  A possible **workaround** is to **disable** the **virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - `ica.module.virtualdriver.vdwebrtc.enable`
  - `ica.module.virtualdriver.nsap.enable`

  The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.
- When using the **RDP protocol**, the remote session has a fixed offset of approximately the height of the menu bar. That means you have a black bar on top of the window and as a result of that, the **Windows panel on the bottom is cut off**.
- **Modifier keys** (`Shift/Ctrl/Win/Alt`) in session windows using **RDP protocol** do not send the keyup event and thus **keep being pressed even when actually released**. Only when you leave the session with the mouse, the modifiers are reset.
- **Copying a text from Horizon Blast** sessions is not possible.
- The **on-screen keyboard** in **Horizon appliance mode** doesn't work correctly with local logon. You have to switch off the local logon and switch on these two keys in the IGEL registry:

- `userinterface.softkeyboard.autoshow`
- `userinterface.softkeyboard.autohide`

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is **supported** by the **UMS version 6.05.100**.

Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

deskMate

- Some stability issues may remain.

Appliance Mode

- When **ending a Citrix session** in browser appliance mode, the **browser is restarted twice** instead of once.
- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Security Fixes 11.04.200

Firefox

- Updated Mozilla Firefox to **68.12.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819, CVE-2020-6820.
  - Fixes for **mfsa2020-13**, also known as
    More...

    CVE-2020-6828, CVE-2020-6827, CVE-2020-6821,
    CVE-2020-6822, and CVE-2020-6825
  - Fixes for **mfsa2020-17** also known as:
    More...

    CVE-2020-12387, CVE-2020-12388, CVE-2020-12389,
    CVE-2020-6831, CVE-2020-12392, CVE-2020-12393,
    and CVE-2020-1239
  - Fixes for **mfsa2020-21** also known as:
    More...

    CVE-2020-12399, CVE-2020-12405,
    CVE-2020-12406, CVE-2020-12410
  - Fixes for **mfsa2020-25** also known as:
    More...

    CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,
    CVE-2020-12420, CVE-2020-12421
  - Fixes for **mfsa2020-31** also known as:
    More...

    CVE-2020-15652, CVE-2020-6514, CVE-2020-6463,
    CVE-2020-15650, CVE-2020-15649, and CVE-2020-15659
  - Fixes for **mfsa2020-37** also known as: CVE-2020-15663, CVE-2020-15664, and CVE-2020-15669

Base system

- Fixed privilege escalation via environment variables in the `/bin/update` binary.
- Fixed privilege escalation via environment variable `PATH` in `/bin/usershell` binary.
- Fixed privilege escalation via `PATH` environment variable in the `/bin/update` binary.

New Features 11.04.200

Citrix

- Integrated **Citrix Workspace app 20.09**. **Removed** Citrix Workspace app **18.10**.
  Available Citrix Workspace apps in this release: **20.09 (default)**, **20.06** and **19.12**.
  The **performance** of the Citrix Workspace app **20.09** was **improved** and a **more detailed logging** was implemented.
- Citrix **logging** was **summarized**. Now, only **one parameter** is needed to **activate logging**.
  More...

Parameter	Enable logging for Citrix sessions
Registry	`ica.logging.debug`
Value	on / off

- Since Workspace app 20.09, the tool **setlog** is used to **configure the logging**. For this purpose, parameters are provided in the registry `ica.logging.setlog`; usually, nothing needs to be changed.
- After **disabling logging**, the system must be **restarted** once.
- Integrated **Zoom Media Plugin 5.2.456413.0902**
- Added **PAC proxy auto configuration support** for Zoom Media Plugin (ZoomVDI).
  To configure, the following parameters need to be set:
  - `network.proxy.settings.sys_proxy_type="Automatic proxy configuration"`
  - `network.proxy.settings.sys_proxy_autoconfig_url="http://..."`

  Alternatively, the **manual HTTP/HTTPS proxy setting** configured at **IGEL Setup > Network > Proxy** is now used for Zoom Media Plugin.
- **Improved** configuration of **ZoomVDI** client.

Cisco Webex

- Integrated **Cisco Webex Meetings 40.10**.

Parallels Client

- Updated **Parallels** Client to version **17.1.2.1**.
  Fixed security vulnerability issue disclosed in the Parallels KB article https://kb.parallels.com/en/125112.

Audio

- Added **EPOS Connect 5.0.1.2795**.
  More...

IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Enable EPOS Connect

Registry	`devices.epos.connect.enable`
Type	bool
Value	enabled / disabled
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Tenant ID
Registry	`devices.epos.connect.tenant_id`
Type	string
Value	''
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Backend Endpoint
Registry	`devices.epos.connect.tenant_url`
Type	string
Value	''
IGEL Setup	**Devices > Unified Communications > EPOS Audio > EPOS Connect**
Parameter	Proxy
Registry	`devices.epos.connect.proxy`
Type	string
Value	''
Registry	`devices.epos.connect.log_level`
Value	Trace / Debug / Information / Warnings / Errors / Exceptions / No logs

Smartcard

- Updated **A.E.T. Europe SafeSign Identity Client** to version **3.6.0.0**.

Multimedia

- Added possibility to fetch **log files of the Zoom Media Plugin (ZoomVDI)** via **UMS support information**.

Hardware

- Added detection of **UD Pocket UC5-LX 2**.

Misc

- Updated **Login Enterprise** to version **4.2**.

Resolved Issues 11.04.200

Citrix

- Fixed the problem with **apparmor** and the **Citrix MS Teams workaround**.
- Fixed: In some Citrix sessions, there have been **sporadic appearances of black rectangles** when the feature "**Accelerated H.264 Deep Compression Codec**" is **active**.
- Integrated parameter to activate the workaround for the **keyboard language issue with MS Teams Optimization**.
  More...

Parameter	Microsoft Teams optimization keyboard language workaround
Registry	`ica.module.virtualdriver.vdwebrtc.keyboard_workaround`
Value	on / off

RDP/IGEL RDP Client 2

- Improved **error logging**.
- Fixed **USB redirection** for RDP sessions.

Firefox

- Fixed **smartcard access in Firefox**. Before this fix, **smartcards** were **not recognized occasionally**.

Network

- Fixed handling of **DNS default domain**.
- Added **registry** key specifying the **number of 802.1X authentication attempts on Ethernet**.
  More...

Registry	`network.interfaces.ethernet.device%.ieee8021x.auth_attempts`
Type	integer
Value	1

- **SCEP**: Fixed derivation of **802.1X identity** from client certificate.

Window manager

- Fixed **crash of start menu**, where it was not populated with any items.
- Fixed **start monitor mapping** for **Firefox**.

Wi-Fi

- **Added** missing **iwlwifi-6000-4 firmware file**.

Open VPN

- Fixed **segmentation fault** when **nameserver was used**.
- Added: **Different protocols** are now **selectable**:

More...

Parameter	protocol
Registry	`sessions.openconnect%.vpnopts.protocol`
Value	Cisco AnyConnect / Juniper Network / Junos Pulse / PAN GlobalProtect

Base system

- Fixed **panels clock format** via registry key `windowmanager.wm%.variables.clock_time`.
- **Post-session command binaries** and **return codes** are **now customizable** via registry. Allows post-session commands if a binary doesn't return 0.
  Name of the binary:
  More...

Parameter	Binary
Registry	`pcom.valid_return_codes<NR>.binary`
Value	binary name

  Comma seperated return codes (e.g. **7,99**) or/and **return code ranges** (e.g. **3..5** for 3,4,5) to be accepted:
  More...

Parameter	Return Codes
Registry	`pcom.valid_return_codes<NR>.returncodes`
Value	e.g. 3,5,10..15 for 3,5,10,11,12,13,14,15

- Fixed problems with **hostnames containing** one or more **"_" characters**.
- Added: Show **AMD Memory Guard in Boot Mode**, when enabled.

Storage Devices

- Fixed **display of hotplug eject menu** in appliance mode.

Remote Management

- Fixed **ICG HA functionality broken** in **11.04.100**.
- Fixed **automatic establishment of the configured ICG connection** if the UMS Server is unreachable.

Notes for Release 11.04.100

Software:	Version	11.04.100
Release Date:	2020-08-05	
Release Notes:	Version	RN-1104100-1
Last update:	2020-08-05	

- IGEL OS Creator (OSC) (see page 3123)
- IGEL OS 11 (see page 3163)

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[305].

- Component Versions 11.04.100 (see page 3124)
- General Information 11.04.100 (see page 3131)
- Known Issues 11.04.100 (see page 3132)
- Security Fixes 11.04.100 (see page 3136)
- New Features 11.04.100 (see page 3137)
- Resolved Issues 11.04.100 (see page 3155)

305. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.04.100

Clients

Product	Version
Chromium	83.0.4103.61-0ubuntu0.18.04.1
Cisco JVDI Client	12.9.0
Cisco Webex Teams VDI Client	3.0.15711.0
Cisco Webex Meetings VDI Client	40.7.0.375
Citrix HDX Realtime Media Engine	2.9.0-2330
Citrix Workspace App	18.10.0.11
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.06.0.15
deviceTRUST Citrix Channel	19.1.200.2
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.10.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
IGEL WVD Client	1.0.13igel1596142398
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64 Qualification at Imprivata in progress
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8
Open VPN	2.4.4-2ubuntu1.3

Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.1
Spice GTK (Red Hat Virtualization)	0.38-2igel93
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	20.04.2-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-4igel13
VMware Horizon Client	5.4.1-15988340
Voip Client Ekiga	4.0.1

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20200323
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	7

PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.20.0-3igel37
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.3
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth stack (bluez)	5.52-1igel6
MESA OpenGL stack	20.0.8-1igel117
VAAPI ABI Version	0.40
VDPAU Library version	1.4-1igel1003
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-1+git20200220igel987
Graphics Driver ATI/AMDGPU	19.1.0-1+git20200318igel986
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867

Graphics Driver Nvidia	440.100-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.7413
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.36.1-0ubuntu2igel888
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.4.48 #mainline-lxos-g1595410170
Xorg X11 Server	1.20.8-2igel1016
Xorg Xephyr	1.20.8-2igel1016
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel100
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 1.x	1.16.2-4igel239
WebKit2Gtk	2.28.3-2igel36
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.10-dfsg-1igel41
Virtualbox X11 Guest Utils	6.1.10-dfsg-1igel41
Open VM Tools	11.0.5-4ubuntu0.18.04.13
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-1igel95
Qemu Guest Agent	5.0-5igel12

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-2igel4
VPN OpenConnect	8.10-1igel4
Scanner support	1.0.27-1
VirtualBox	6.1.10-dfsg-1igel41

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Workspace app Citrix Appliance Citrix StoreFront	219.5 M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Citrix Appliance Local Browser (Firefox)	70.2 M	Included
RDP VMware Horizon	4.2 M	Included
Cendio ThinLinc	10.0 M	Included

Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	114.5 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.8 M	Included
IBM i Access Client Solutions	72.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included
NVIDIA graphics driver	115.0 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	13.0 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	48.0 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	13.8 M	Included
Local Browser (Chromium)	81.2 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	32.0 M	Not included
Cisco Webex Meetings VDI	36.8 M	Not included
Zoom Media Plugin	39.8 M	Not included

Teradici PCoIP Client	7.8 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.5 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	62.5 M	Not included

General Information 11.04.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.04.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.04.100

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs and unused features must be disabled in IGEL Setup under **System > Firmware Customization > Features** to perform the firmware update.

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`

Value	enabled / <u>disabled</u>

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop. Workaround: **Use CWA 18.10.0**.
- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06**, **webcam redirection** or **screen sharing** may lead to **display error**s like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.
  A possible **workaround** is to **disable** the **virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - `ica.module.virtualdriver.vdwebrtc.enable`
  - `ica.module.virtualdriver.nsap.enable`
  - The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is not enough space to enable the **Imprivata partition after the update to 11.04.100**. In this case, a corresponding error

message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.
- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is **supported** by the **UMS version 6.05.100**.

Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

deskMate

- Integrated deskMate solution. Some stability issues may remain.

Security Fixes 11.04.100

Firefox

- Updated Mozilla **Firefox** to **68.10.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819 and CVE-2020-6820
  - Fixes for **mfsa2020-13**, also known as:
    More...

    CVE-2020-6828, CVE-2020-6827, CVE-2020-6821,
    CVE-2020-6822, and CVE-2020-6825
  - Fixes for **mfsa2020-17** also known as:
    More...

    CVE-2020-12387, CVE-2020-12388, CVE-2020-12389,
    CVE-2020-6831, CVE-2020-12392,
    CVE-2020-12393, and CVE-2020-1239
  - Fixes for **mfsa2020-21** also known as:
    More...

    CVE-2020-12399, CVE-2020-12405,
    CVE-2020-12406, and CVE-2020-12410
  - Fixes for **mfsa2020-25** also known as:
    More...

    CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,
    CVE-2020-12420, and CVE-2020-12421
- Changed option to **deny local file browsing** via file:// URI per default now.
  More...

IGEL Setup	**Firefox Browser > Firefox Browser Global > Window**
Parameter	Hide local filesystem
Registry	`browserglobal.app.filepicker_dialog_hidden`
Value	enabled / disabled

Base system

- **SSH protocol version 1 is now disabled.** All remote connections via SSH must use SSHv2.

Driver

- Updated **Nvidia driver** to version **440.100**.

New Features 11.04.100

Citrix

- Integrated **Citrix Workspace App 20.06**.
  Available Citrix Workspace Apps in this release: **20.06** (default), **19.12**, and **18.10**
- Added a registry key to enable optimization for **Microsoft Teams**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**
Parameter	Microsoft Teams optimization
Registry	`ica.module.virtualdriver.vdwebrtc.enable`
Value	on / off

- Added a registry key to enable support for **NetScaler App Experience (NSAP)** virtual channel.
  More...

Parameter	HDX uses the NSAP virtual channel
Registry	`ica.module.virtualdriver.nsap.enable`
Value	on / off

- Integrated **Citrix HDX/RTME 2.9**.
- Integrated **ZOOM Media Plugin for Citrix** to optimize performance for ZOOM video calls and conferences.
- IGEL x64: 5.0.415463.0619 requires Windows x86 or x64: 5.0.24002.0619. https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**
Parameter	Zoom Media Plugin
Registry	`ica.module.virtualdriver.vdzoom.enable`
Value	enabled / disabled

- Updated **signotec Virtual Channel** to version **8.0.9**.
  The corresponding changes are:
  - Logging has been improved.
  - A problem with the communication with the signature pads was fixed.
  - USB communication via bulk transfer is model-independent (improved speed).
- Removed parameter **Content redirection** / `ica.wfclient.crenabled` from TC Setup (**Sessions > Citrix > Citrix Global > HDX Multimedia**).

OSC Installer

- Added **dialog "Feature Selection" in IGEL OS Creator** for the selection of features to be installed on the target device. It interactively shows if the current selection of features fits onto the device. The selection of features is saved on the OSC installer medium (when allowed) and set as the default selection for the next installation. If **"Migrate Old Settings"** is selected, the set of features of the old installation is set as the default selection.
- **Reduced memory requirements** of OSC installer for **machines without Nvidia graphic card**.

WVD

- Added **AAC Codec support** to Audio Output redirection.
  More...

Registry	`sessions.wvd%.options.enable-aac`
Value	enabled / disabled

RDP/IGEL RDP Client 2

- Added the **possibility to add a black background** to the RDP auto-reconnect window.
  More...

Registry	`sessions.rdp.options.reconnect-black-fullscreen`
Type	bool
Value	enabled / disabled

- Added configuration option for the **amount of RDP auto-reconnect retries**. The default value will remain "20". A value of "0" means infinite retries.
  More...

Registry	`sessions.rdp.winconnect%.options.reconnect-max-retries`
Type	Integer
Value	20

VMware Horizon

- Updated **VMware Horizon** to version **5.4.1**.
  For usage with **Blast protocol**, it is recommended to enable **DRI3 graphics mode**:
  More...

Parameter	Use DRI3
Registry	`x.driver.use_dri3`
Value	enabled / disabled

- Fixed **handling of RDP's fullscreen mode span**, which means to combine all local monitors for one big remote session.

PowerTerm

- Updated **Ericom PowerTerm** LTC to version **14.0.0.45623**.

Parallels Client

- Updated **Parallels Client** to version **17.1.1**.

Teradici PCoIP Client

- Updated **Teradici PCoIP** Client to version **20.04.2-18.04**. The new version supports **hardware-accelerated H.264 decoding with Ultra PCoIP**.
- New parameters:
  More...

Parameter	Log level
Registry	`pcoip.log-level`
Value	0 / 1 / 2 / 3 / 4

  PCoIP sessions **can now use the global setting**.
  More...

Parameter	Show codec indicator
Registry	`pcoip.codec_indicator`
Value	disabled / enabled
Info	Show a small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec. This setting is only available globally.

XEN

- Added support to run as **XEN guest system**.

NX client

- Updated **NoMachine NX Client** to version **6.11.2**.

ThinLinc

- Updated **ThinLinc** to version **4.12**.

Network

- **DHCP** changes:
  The system now sends a **vendor-class-identifier(option 60) "igel-dhcp-1"**. Furthermore, it requests **vendor-encapsulated-options (43)**. Those can be used to transfer IGEL-specific options **igelrmserver(224) and umsstructuretag(226)** in the vendor namespace (with the same option numbers and types) instead of in the global namespace.
  The former way is also still functional, but values transferred in the new way override those which were transferred the old way.
  Apart from 224 and 226 one more option is defined in the vendor space: **"exclusive", option 1,**

type byte. Its presence means that global options 224 and 226 shall not be interpreted in the traditional way and only settings in the vendor space apply.
IPv6 is not involved.

- Added support for **LTE module HP lt4132**.
- Updated **Network Manager** to version **1.20.4**.
  - The range of **network.interfaces.wirelesslan.device0.bgscan.module** now **includes "default" for** using **original upstream Network Manager settings**.
- Added some **additional Ethernet network drivers**.
  More...
  - amd-xgbe : AMD 10 Gigabit Ethernet driver
  - ec_bhf : Beckhoff EtherCAT
  - liquidio_vf : Cavium LiquidIO Intelligent Server Adapter Virtual Function driver
  - liquidio : Cavium LiquidIO Intelligent Server Adapter driver
  - thunder_bgx : Cavium Thunder BGX/MAC driver
  - nicvf : Cavium Thunder NIC Virtual Function driver
  - nicpf : Cavium Thunder NIC Physical Function driver
  - thunder_xcv : Cavium Thunder RGX/XCV driver
  - atlantic : aQuantia Corporation(R) network driver
  - be2net : Emulex OneConnect NIC driver 12.0.0.0
  - ixgb : Intel(R) PRO/10GbE network driver
  - igc : Intel(R) 2.5G Ethernet Linux driver
  - ice : Intel(R) Ethernet Connection E800 Series Linux driver
  - i40e : Intel(R) Ethernet Connection XL710 network driver
  - iavf : Intel(R) Ethernet Adaptive Virtual Function network driver
  - ixgbe : Intel(R) 10 Gigabit PCI Express network driver
  - igbvf : Intel(R) Gigabit Virtual Function network driver
  - ixgbevf : Intel(R) 10 Gigabit Virtual Function network driver
  - ena : Elastic Network Adapter (ENA)
  - nfp : The Netronome Flow Processor (NFP) driver
  - bna : QLogic BR-series 10G PCIe Ethernet driver
  - enic : Cisco VIC Ethernet NIC driver
  - mlx5_core : Mellanox 5th generation network adapters (ConnectX series) core driver
  - mlx4_en : Mellanox ConnectX HCA Ethernet driver
  - ionic : Pensando Ethernet NIC driver
  - sfc-falcon : Solarflare Falcon network driver
  - sfc : Solarflare network driver
  - dwc-xlgmac : Synopsys DWC XLGMAC driver
  - hinic : Huawei Intelligent NIC driver
  - cassini : Sun Cassini Ethernet driver
  - niu : NIU Ethernet driver
  - samsung-sxgbe : SAMSUNG 10G/2.5G/1G Ethernet PLATFORM driver
  - cxgb : Chelsio 10Gb Ethernet driver
  - qede : QLogic FastLinQ 4xxxx Ethernet driver
  - qlcnic : QLogic 1/10 GbE Converged/Intelligent Ethernet driver
  - qed : QLogic FastLinQ 4xxxx Core module
  - netxen_nic : QLogic/NetXen (1/10) GbE Intelligent Ethernet driver

- vxge : Neterion's X3100 Series 10GbE PCIe I/OVirtualized Server adapter
- myri10ge : Myricom 10G driver (10GbE)
- tehuti : Tehuti Networks(R) network driver
- bnxt_en : Broadcom BCM573xx network driver
- bnx2x : QLogic BCM57710/57711/57711E/57712/57712_MF/57800/57800_MF/57810/57810_MF/57840/57840_MF driver

- Added a registry key for specifying a **space-separated list of DNS resolver options**. See "**man resolv.conf**".
  More...

Parameter	Option list
Registry	`network.dns.options`
Type	string
Value	empty

Wi-Fi

- Added support for **WPA3 Personal network authentication**.
- Added a registry key for **preferring WPA3 Personal** (i.e. SAE) or **WPA2 Personal** at the time a connection is created with Wireless Manager when the access point offers both:
  More...

Parameter	Prefer WPA3 Personal to WPA2 Personal
Registry	`network.applet.wireless.prefer_sae`
Range	[default] [yes] [no]
Info	"default" currently means "no"

- Added **captive portal support for Wi-Fi**. Passing through a captive portal (which is basically a web application) is sometimes **necessary to achieve full network connectivity** (here also referred to as online state).
  - The **feature is disabled when** the following **registry key** is **empty**. Otherwise, it should be a **URI** that is **suitable for NetworkManager connectivity check**.
    More...

Parameter	Online check URI
Registry	`network.global.onlinecheck.uri`
Range	[] [http://connectivity-check.ubuntu.com/]
Value	http://connectivity-check.ubuntu.com/

  - The following key specifies the **conditions of the online check**. It is also required that **no Ethernet cable is plugged in** and **DHCP is not set** in the UMS.
    More...

Parameter	Condition for online check
Registry	`network.global.onlinecheck.condition`
Range	[None] [Network is user-defined] [Network is open]

- This key determines **how many seconds to wait for full network connectivity** before the network connection is considered complete with incomplete connectivity. The timeout should allow a user to do what is necessary for passing through the captive portal.
  More...

Parameter	Online check timeout
Registry	`network.global.onlinecheck.timeout`
Type	integer
Value	120

- Enabled **use of 802.11r**, also known as **fast BSS transition** or FT. This is confirmed to work at least in the **mode "over the air"**.

Smartcard

- Updated **OpenSC** to version **0.20.0**. See https://github.com/OpenSC/OpenSC/releases/tag/0.20.0 for detailed release notes.

Cisco JVDI Client

- Updated **Cisco JVDI** client to version **12.9.0**.

Cisco Webex VDI

- Integrated the new feature **Cisco Webex Teams VDI for Citrix** and **Horizon** sessions.
  Cisco Webex Teams version: **3.0.15711.0**
- Added a parameter to activate the feature within **Citrix**:
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > Cisco**
Parameter	Cisco Webex Teams VDI
Registry	`ica.module.virtualdriver.vdciscoteams.enable`
Value	enabled / disabled

- Added a parameter to activate the feature within **VMware**:
  More...

IGEL Setup	**Sessions > Horizon > Horizon Client Global > Unified Communications > Cisco**
Parameter	Cisco Webex Teams VDI - Horizon

Registry	`vmware.view.vdciscoteams.enable`
Value	enabled / disabled

- Integrated the new feature **Cisco Webex Meetings VDI for Citrix** sessions.
  Client Version: **40.7.0.375**
- Added a parameter to activate the feature within **Citrix**:
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > Cisco**
Parameter	Cisco Webex Meetings VDI
Registry	`ica.module.virtualdriver.vdciscomeetings.enable`
Value	enabled / disabled

Base system

- Updated base system to **Ubuntu LTS** version **18.04**.
- Updated **kernel** to version **5.4.48**.
- Added **notification for critical system out-of-memory state** when the available **system memory is lower than 40 MB** and **processes were killed** to prevent the system from freezing.
- Display **AMD Memory Guard in Boot Mode** when it's active.
- Added **notification option for Session Autostart** when a autostart delay is configured. It is possible to cancel the session autostart or to start immediately.
  More...

IGEL Setup	*** > Desktop integration**
Parameter	Autostart notification
Value	enabled / disabled

- Added correct **UI handling** for **Wacom DTU-1141B**.
- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version **2.30**). The following authorities were added:
  More...
  - "Certigna Root CA"
  - "GTS Root R1"
  - "GTS Root R2"
  - "GTS Root R3"
  - "GTS Root R4"
  - "UCA Extended Validation Root"
  - "UCA Global G2 Root"
  - "GlobalSign Root CA - R6"
  - "OISTE WISeKey Global Root GC CA"
  - "GDCA TrustAUTH R5 ROOT"
  - "SSL.com[306] EV Root Certification Authority ECC"
  - "SSL.com[307] EV Root Certification Authority RSA R2"

- "SSL.com[308] Root Certification Authority ECC"
- "SSL.com[309] Root Certification Authority RSA"
- "TrustCor ECA-1"
- "TrustCor RootCert CA-1"
- "TrustCor RootCert CA-2"

- The following authorities were removed:
  More...
  - "Certplus Root CA G1"
  - "Certplus Root CA G2"
  - "OpenTrust Root CA G1"
  - "OpenTrust Root CA G2"
  - "OpenTrust Root CA G3"
  - "TÜRKTRUST Elektronik Sertifika Hizmet Saglayicisi H5"
  - "Visa eCommerce Root"
  - "ACEDICOM Root"
  - "AddTrust Low-Value Services Root"
  - "AddTrust Public Services Root"
  - "AddTrust Qualified Certificates Root"
  - "CA Disig Root R1"
  - "CNNIC ROOT"
  - "Camerfirma Chambers of Commerce Root"
  - "Camerfirma Global Chambersign Root"
  - "Certinomis - Autorit, Racine"
  - "Certum Root CA"
  - "China Internet Network Information Center EV Certificates Root"
  - "Comodo Secure Services root"
  - "Comodo Trusted Services root"
  - "DST ACES CA X6"
  - "GeoTrust Global CA 2"
  - "PSCProcert"
  - "Security Communication EV RootCA1"
  - "Swisscom Root CA 1"
  - "Swisscom Root CA 2"
  - "Swisscom Root EV CA 2"
  - "TURKTRUST Certificate Services Provider Root 2007"
  - "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
  - "UTN USERFirst Hardware Root CA"
- Added parameter to override **rate limit of debug messages** in journal. It should be enabled for debugging processes which generate a big amount of messages in order to avoid skipping of messages.
  More...

306. http://SSL.com
307. http://SSL.com
308. http://SSL.com
309. http://SSL.com

Parameter	No rate limit
Registry	`system.journald.no_rate_limit`
Value	enabled / disabled

- It's possible to **extend the login options of the Kerberos** login window now.
  There are several new registry keys:
  More...

Parameter	extended login
Registry	`sessions.xlock0.options.login_extension_active`
Value	enabled / disabled

  If enabled, an "**Associate Type" combo box is shown**. The **entries of the combo box** are **configured with** the following **login_feature1**, **login_feature2**, and **login_feature3 keys**.
  - Configure the **label of the "Associate Type" combo box**:
    More...

Parameter	login features label
Registry	`sessions.xlock0.options.login_features_label`
Value	Default: empty which means "Associate Type"

  - **The first entry of the "Associate Type" combo box**. To enable the combo box entry, add e.g. the text "Store associate at home store".
    More...

Parameter	login_feature1
Registry	`sessions.xlock0.options.login_feature1`

    If the entry is selected, the **username is expanded by a fixed string** defined in `login_extension_default` registry key.
  - The **fixed username extension** for the first feature. It can be set e.g. by a script.
    More...

Parameter	login extension default value
Registry	`sessions.xlock0.options.login_extension_default`

  - **The second entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate visiting this store".
    More...

Parameter	login_feature2
Registry	`sessions.xlock0.options.login_feature2`

If the entry is selected, the **username is expanded by a suffix** that is **entered in a separate entry widget**.

- The **label of the entry field for the username suffix.** Set it e.g. to "Store Number".
  More...

Parameter	login_extension_label
Registry	`sessions.xlock0.options.login_extension_label`
Value	Default: empty which means "no label"

- **The third entry of the "Associate Type" combo box**. To enable the combo box entry, add e.g. the text "Homeoffice associate visiting this store".
  More...

Parameter	login_feature3
Registry	`sessions.xlock0.options.login_feature3`

If the entry is selected, **another domain** can be **selected from an appended domain combo box**.

- The **label for the domain entry field**.
  More...

Parameter	login domain label
Registry	`sessions.xlock0.options.login_domain_label`
Value	Default: empty which means "domain"

- The **extension to the username** is **added after a dot** ('.').
- For the **domain drop-down box**, **four different domains are configurable** here:
  More...

IGEL Setup	**Security > Active Directory/Kerberos > Domain 1 - 4**
Parameter	Fully qualified domain name
Registry	`auth.krb5.realms.realm0.realm`
Registry	`auth.krb5.realms.realm1.realm`
Registry	`auth.krb5.realms.realm2.realm`
Registry	`auth.krb5.realms.realm3.realm`

- There are keys to **add more domain names**:
  More...

Parameter	Domain

Registry	auth.krb5.extended_domain%.name
Info	Add a new instance for each domain entry.

- In the Kerberos login window, it's now possible to turn on or off **numlock** and/or **capslock for password input**.
  Registry keys:
  More...

Parameter	Handling of numlock
Registry	sessions.xlock0.options.numlock_approach
Range	[don't change] [set on] [set off]
Info	"set on": force numlock on when password is entered "set off": force numlock off when password is entered
Parameter	Handling of capslock
Registry	sessions.xlock0.options.capslock_approach
Range	[don't change] [set on] [set off]
Info	"set on": force capslock on when password is entered "set off": force capslock off when password is entered

- It's now possible to **show a message in the Kerberos login window**. Registry key:
  More...

Parameter	banner text
Registry	sessions.xlock0.options.banner_text
Info	The user will see the message on the top border.

- In the Kerberos login window, there is a **mode to convert passwords always to upper case**. To turn it on, use:
  More...

Parameter	case-insensitive password
Registry	sessions.xlock0.options.case_insensitive_password
Value	enabled / disabled

- With this key, the text for the **case-insensitive indicator** can be modified:
  More...

Parameter	case-insensitive text
Registry	sessions.xlock0.options.case_insensitive_text

Value	Default: empty which means "case-insensitive"

- Fixed **ThinkPad Brazil keyboard layout**.
- It is possible to **show a custom logo** in the Kerberos login window. Also, the **background and text color is customizable** now.
  Registry keys:
  More...

Parameter	path for login image
Registry	`sessions.xlock0.options.login_image`
Value	/usr/share/pixmaps/greeter-user.svg
Info	Supported image formats include: PNG, JPG, SVG
Parameter	set specific colors for greeter
Registry	`sessions.xlock0.options.set_color`
Value	enabled / disabled
Parameter	text color
Registry	`sessions.xlock0.options.text_color`
Value	#ffffff
Info	Text color in the format #rrggbb Example: #ff0077
Parameter	background color
Registry	`sessions.xlock0.options.background_color`
Value	#000000
Info	Background color in the format #rrggbb Example: #7700ff

- Added **new local logon method "Login with Smart Card Certificate"**. It implements the **pam_pkcs11 smartccard authentication module**. For a successful configuration, the following has to be provided via **UMS file transfer**:
  - **root and intermediate CA certificates** for verification of the client certificates in folder `/etc/pam_pkcs11/cacerts`
  - file `/etc/pam_pkcs11/cn_map` which contains **mappings of Common Names to UPN names**.
    Each line is in the format `\<common name> -> \<logon name>`
    where

`\<common name>` is the common name part of the subject of the certificate

`\<logon name>` is

- in case of **Kerberos Enterprise** (`auth.login.krb5_enterprise`) **disabled**: the UPN name of the SubjectAltName extension of the certificate, e.g. user@MY.DOMAIN[310]
- in case of **Kerberos Enterprise** (`auth.login.krb5_enterprise`) **enabled**: the UPN name of the SubjectAltName extension of the certificate with Default Domain (`auth.krb5.libdefaults.default_realm`) suffix, e.g. user@DOMAIN.SUFFIX@DEFAULT.DOMAIN[311]

- The logon method **can** either **be used standalone or together with Kerberos logon** as a fallback if Kerberos does not succeed.
  More...

Parameter	Login with Smart Card Certificate
Registry	`auth.login.pkcs11`
Value	false / true

Parameter	Certificate verification policy
Registry	`auth.login.pkcs11_cert_policy`
Value	ca,ocsp_on,signature

Parameter	Enable Debugging of Smart Card Certificate Logon
Registry	`auth.login.pkcs11_debug`
Value	false / true

- It is possible to expand the store number by a registry key:
  More...

Parameter	expand store
Registry	`sessions.xlock0.options.expand_store`
Value	enabled / disabled

- Fixed: The **login screen** is **adjusted to lower resolutions**.
- It is possible to activate enter key to login on all fields.
  More...

Parameter	auto login on all fields

310. mailto:user@MY.DOMAIN
311. mailto:DOMAIN.SUFFIX@DEFAULT.DOMAIN

Registry	`sessions.xlock0.options.auto_login`
Value	enabled / disabled

X11 system

- Changed: Use **modesetting graphics driver** on **devices with newer intel GPUs**.
- Changed registry key:
  More...

Parameter	Use generic modesetting driver for INTEL hardware
Registry	`x.drivers.intel.use_modesetting`
Range	[Auto] [True] [False]

- Updated **DisplayLink driver** to version **5.3.1.34**.
- Added new registry key for **Nvidia cards** (use this **if you want to use PRIME**):
  More...

Parameter	Enable/Disable NVIDIA Kernel Modesetting support
Registry	`x.drivers.nvidia.use_modeset`
Range	[Default] [Enabled] [Disabled]
Info	"Default" is currently the same as "disabled"

- Updated **florence soft keyboard** to version **0.6.3**.
- **Removed 640x480** from possible **display resolution range**.
- Added possibility to **change the order of primary** and **secondary graphic card**.
  New registry key:
  More...

Parameter	Make the secondary graphic card to the primary one
Registry	`x.drivers.swap_card0_with_card1`
Value	true / false

- Added possibility to **invert the order of all graphic card**s.
  New registry key:
  More...

Parameter	Invert default graphic card ordering
Registry	`x.drivers.swap_all`
Value	true / false

- Added possibility to **choose the driver** which should become **the primary graphic card**.
  New registry key:

More...

Parameter	Choose which drivers should be preferred to become the primary graphic card
Registry	`x.drivers.preferred_driver`
Value	

X server

- Added possibility to influence **mode used for mirroring screens with different resolutions**. (Notice: here scaling may not always work).
  New registry key:
  More...

Parameter	Choose the mode which should be used for mirroring monitors if resolution differs
Registry	`x.xserver0.mirror_mode`
Range	[Default] [Biggest common resolution] [Scaling]
Value	Default (use panning if needed)

Driver

- Updated **Grundig Dictation driver for Citrix** and **RDP** to version **0.10**.
  The changes are:
  - Support **third-party USB HID devices** in a more flexible way
  - Fixed USB transfer overflow for **Philips LFH 9620**
  - Remove **erroneous debug output** in release configuration
  - Allow to **control** also **"Headphone" volume & switches**
- Updated **Olympus driver for dictation** to version **2020-03-23-143654**.
  Changelog:

  New:

  - DR-1200: PID 0225
  - DR-2300: PID 0256

  Changed:

  - PID 0253 from DR-2100 to DR-1200
- Updated **Philips Speech driver** to version **G12.9**.
  The changes are:
  - Support for **Philips SpeechLive**
  - Faster and more reliable remote session connection status check
  - **Shutdown of** the **PSPDispatcher.exe** on the server if it's not in use anymore.
- Updated **StepOver TCP client** and **Citrix plugin** to version **2.4.2**. Fixed **crash of Citrix** session while **using** the **signature pad**.

Audio

- Integrated **new sound mixer**.

- New combo box for **audio device selection in TC Setup** available:
  - **Accessories > Sound Preferences > Options > Default Sound Output**
  - **Accessories > Sound Preferences > Options > Default Sound Input**

Appliance Mode

- Integrated: The **new Browser Appliance mode** is the successor for the XenDesktop appliance mode. The Browser is configured as in XenDesktop appliance mode, but **does not use the upstream SAS window**.
  More...

IGEL Setup	**Sessions > Appliance Mode**
Parameter	Browser
Registry	`xen.xenapp-morph.enabled`
Type	Bool
Value	enabled / disabled

IGEL Setup	**Sessions > Appliance Mode > Browser**
Parameter	Web URL
Registry	`xen.xenapp-morph.xendeliveryserverurl`
Type	string

- A **hyperlink to the "On-screen Keyboard"** is available on the right side **under "Related Configurations"**.

Multimedia

- Added **ffmpeg support** for following codecs:
  - Added support for **new decoders**:
    More...

    flac, gif, libaom_av1, mjpeg, mjpegb,
    mp1,mp1float, mp2, mp3, mp3adu,
    mp3adufloat, mp3float, opus, theora, vorbis,
    vp2, vp8, vp9, and wavepack
  - Added support for **new encoder**: libopus
  - Added support for **new hwaccels**:
    More...

    mjpeg_vaapi, mpeg1_vdpau, mpeg2_vaapi,
    mpeg2_vdpau, vp8_vaapi, and vp9_vaapi
  - Added support for **new parsers**: avi, flac, gif, matroska, mp3, ogg, and wav
  - Added support for **new demuxers**: avi, flac, gif, matroska, ogg, and wav
  - Added support for **new muxers**: ogg and opus

Chromium Browser

- Integrated **Chromium** browser version **83.0.4103.61** as experimental feature.
  Configurable at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global** and **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Sessions**
- Main switch to enable and disable **IGEL configuration**:
  More...

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global**
Parameter	Use IGEL Setup for configuration
Registry	`chromiumglobal.app.igelsetupconfig`
Value	disabled / enabled
Info	With disabled IGEL configuration, you can use the generic Custom Setup to configure Chromium. The Custom Setup can be found at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global > Custom Setup: Policies**, **Preferences**, **Commandline Options**.

- Parameter for **enabling** and **disabling** the **H.264 decoding**:
  More...

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global**
Parameter	H.264 decoding
Registry	`chromiumglobal.app.h264_decoding`
Value	enabled / disabled
Info	Enable Audio/Video playback of non-free codecs (H.264+AAC) - the support is in a beta state and therefore disabled by default.

Evidian

- Added the Evidian **built-in option 'Process To Spy**'.
  More...

Registry	`evidian.processtospy`
Value	YOUR-PROCESS / disabled

ControlUp

- Integrated **ControlUp Monitoring Tool for Citrix** and **Horizon** sessions.

Hardware

- Added hardware support for **Lenovo M625q**.
- Added hardware support for **LG CL600N**.
- Added hardware support for **HP Engage Go Mobile System**.

- Added hardware support for **Fujitsu FUTRO S740**.
- Added hardware support for **OnLogic CL210G-10**.
- Added hardware support for **OnLogic KARBON 300**.
- Added hardware support for **Rein Medical Clinio S 522TCT** and **S 524TCT**.
- Added hardware support for **HP t640 Thin Client**.
- Added basic support for **Macbook models 2018** and **newer**.
- Added support for **Sennheiser MB 660**, **SC 630**, **SC 45**, **SC 160 headsets**.
- Added support for **Plantronics Savi 8245 Office**, **Voyager 6200 UC**, **Savi 8220 headsets**.
- Added serial port driver for **Exar UART PCIe card**.
- Added driver for **GSPCA based webcams**.

TC Setup (Java)

- Added Setup page **Sessions > Horizon Client > Horizon Client Global > Window**. Settings for "**Window size**" and "**Multimonitor full-screen mode**" can be set.
  These settings are repeated and originate in RDP Global but are now presented in a more obvious place for Horizon sessions.

IGEL Cloud Gateway

- Added support for **Secure Terminal over ICG**.
- **Changed default order of connecting to the IGEL Remote Management** - an available UMS Server is preferred now by default. The device establishes a configured ICG connection only if the UMS Server is not reachable. This behavior can be changed by the parameter:
  More...

Registry	`system.remotemanager.icg_try_ums_connect`
Value	true / false

Fabulatech

- Updated **FabulaTech Scanner for Remote Desktop** client to version **2.4.0.11**.
- Updated **FabulaTech plugins** to version **3.6.2**.
- Updated **Fabulatech USB for Remote Desktop plugins** to version **3.6.8**.

Jabra

- **Jabra Xpress** (JDU) is upgraded to the **7.2.0-509** version. List of the newly introduced parameters:
  More...

Registry	`jabra.xpress.show_jdu_gui`
Value	true / false
Registry	`jabra.xpress.device_dashboard.autopost`
Value	true / false

Resolved Issues 11.04.100

Citrix

- "**Green artifacts**" problem in Citrix sessions (most probably) fixed.
- Citrix **hardware video acceleration** supports the **latest Intel hardware**.

OSC Installer

- Fixed issue with **filesystems not** always get detected correctly in **initramfs OSC Installer** (needed for using iso file boot parameter).
- Fixed: **username and password in the error message** are not shown anymore when firmware file could not be downloaded.
- Get **URLs** with **username:password@** working.

RDP/IGEL RDP Client 2

- Fixed error when **renaming a non-empty shared folder**.

WVD

- Includes **WVD client with** fixed **RDcoreSDK** version.
- **Clipboard redirection** has potential privacy and security risks and is therefore **disabled by default**.
- **IGEL WVD Client** integrated

VMware Horizon

- Fixed missing **support for ThinPrint** and **Skype for Business** when starting **Horizon from Firefox browser**.

Firefox

- Fixed Firefox **block extension missing tabs** created via command line argument.
- Fixed **rtsp media stream** with enabled apparmor.
- **Show "blocked" page instead of closing tab** when blocked page is viewed in Firefox.
- Fixed functionality in the local setup to start the **certificate manager of the Firefox browser**.
- Fixed functionality in the local setup to **start the Firefox** browser **with the internal page to show the installed plugins**.
- Fixed **restart mechanism in the Firefox** browser where the browser could not be closed on suspend resulting in a superfluous browser window on resume.

Network

- Improved **Wi-Fi DHCP lease handling**: Leases are discarded when the network changes. The former behavior caused problems with certain iPhone IOS versions.
- **802.1X failures** now generally **result in falling back to a connection without authentication**, e.g. also in the case of 802.1X settings that don't make sense at all. This only **applies if the fallback is allowed** of course.
- **wpa_supplicant** now adds **timestamps to entries of its log file**.
- Use **e1000e driver** out of the kernel **as default** instead of the third-party driver.
- Added a registry key that determines whether **lldpd is in receive-only mode**.
  More...

Parameter	Disable sending LLDP packets
Registry	`network.lldp.rxonly`
Value	true
Attention:	If the behavior since 10.06.100 shall be preserved, this key must be set to "false".

- Updated **scep** to version **0.7.0**.

Wi-Fi

- Fixed non-working **Marvell WLAN device 8997** (SDIO version).

NCP VPN

- Added fix for **NCP Secure Client**.

genucard VPN

- **genucard 3 is supported** now.

Imprivata

- **Control the visibility** of the **Horizon session control bar** via registry parameter:
  More...

Registry	`vmware.view.menu-bar`
Value	enabled / disabled

- Honor the Citrix Window Configuration in **Imprivata Appliance Mode**.
- Fixed **Lock key** and **Tap out** behavior.
- Fixed **MS RDSH** session.
- Simplified the configuration of **Imprivata FUS**.
- **Enable the following** if you use **Imprivata** versions **above 6.3**:
  More...

Registry	`imprivata.gain_permission`
Value	enabled / disabled

- Fixed **bug regarding Imprivata** and **On-Screen Keyboard**.
- **Restore the keyboard map** after Horizon sessions.

Smartcard

- Fixed not working **90meter in Firefox** when **apparmor is active**.
- Fixed problem in **smartcard resource manager PC/SC-Lite** which caused **disconnects of VMware Horizon sessions** when using smartcards with certain applications.
- Added **driver for** smartcard reader **Elatec TWN4 CCID** (USB 0x09D8:0x0425).
- Updated **cryptovision scInterface** to version **7.3.1**.
  The changes are:
  More...

    - Consolidated features of the last versions 7.2 and 7.1
    - Malta eID Release
    - Added Admin Card Gemalto V3
- Updated **PC/SC-Lite smartcard resource manager** to version **1.8.26**.

HID

- Fixed: **Switching touchpad to other driver** via IGEL registry key.

CUPS Printing

- Added new version **25.1.0.425** of **Printerlogic Printer Installer Client**.
- Added **new printer models** into IGEL OS from the current CUPS drivers.

Base System

- Fixed bug in **folder generation of the Application Launcher**.
- Fixed **TLS certificate verification** problem of **certificates signed by "USERTrust RSA CA"** or **"COMODO RSA CA"**. The problem could occur in clients like Citrix Workspace App and VMWare Horizon client.
- Fixed **password change with AD/Kerberos**. Before this fix, the password complexity rules were not enforced for users with the Reset Password permission for their account.
- You can now **connect to Bluetooth devices without pairing**. For this a new registry key is available.
  More...

Parameter	connect devices without pairing
Registry	`devices.bluetooth.connect_only`
Value	enabled / disabled

- **Some devices do not connect automatically after reboot**. To fix that, `bluetoothctl connect \<device-ID>` can be executed via script. If the **device is connected (0)** or **not (1)** can be seen in return value.
  Known devices that do not connect:
    - dialog semiconductor IoT Multi Sensor DK
- **SSHv1 support is now removed** due to newer openssh libraries.
- **Forcing** protocol **version 1** via **SSH Session > Options** is **no longer possible**.
- The `network.ssh_server.server_key_bits` registry key parameter is **removed** due to **deprecation of SSHv1**.
- Updates **systemd** to **Ubuntu Focal version**.
- Improved **stability of mounting network shares** when using a **static network configuration**.
- Fixed **apparmor cache** issue **after update with OSC installer**.
- Bug fix: **touchscreen calibration** on 1 or more normal screen with 1 touch screen environment.
- Fixed **syslog**, **kern.log**, **auth.log**, and **daemon.log** entries are **not shown in IGEL System Log Viewer**.
- Updated **Grub2** to current Debian SID/Bullseye version **2.04**.
- **Removed** deprecated registry keys `system.idlecommand`.
- New **Bluetooth pairing tool** and **Bluetooth tray icon** for Bionic.

- Updated **kernel** to mainline version **5.4.48**.
- If used as master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only on first boot and never again.
- Possible **rollout of initial settings, certificates or licenses placed on first partition** for this you need to:
    a. Write image to your USB/Flash medium.
    b. Mount or simply access the **1. VFAT partition** which is present (should be empty).
    c. Copy your **setup.ini** and/or ****.lic files** to the 1st partition (no directories).
    d. Create a `ca-certs` directory and copy your certificates into it. They will be copied to the `/wfs/ca-certs` directory on first boot.
    e. You can now copy the USB/Flash medium several times if needed.
    f. On first boot, the device will reboot out of the splash screen (reread changed partition table)
    g. The settings, certificates and/or licenses will get rolled out and deleted from the 1st partition.
- Added initial support for **Thunderbolt devices** (only limited support here, may work but is not guaranteed).
- Updated IGEL **EULA**.
- Updated **AMD Microcode** to version **3.20191218.1**.
- Updated **Intel Microcode** to version **20200520** and a special update for **J1900 devices**.
- Updated **Intel Microcode** to **20200616** version.
- Added a **userspace oom killer** to the firmware.

Firmware Update

- An **ongoing firmware update can now be canceled by the use**r when the network online status could not be reached after 10 seconds (since start of the firmware update).

H264

- **Citrix hardware video acceleration** supports the latest Intel hardware.

Storage Devices

- Fixed mount issues with **Iphone XR/XE/11PRO**.
- **Mobile Device Access** feature respects USB Access Control now.
- Fixed unwanted **ownership change** of automounted Linux filesystem root directories.

X11 System

- Fixed **Display Switch not saving settings over reboot**.
    - **Default to settings from Setup** instead of mirror when no Display Switch profile is available.
- Prevent misconfiguration that **picks GPU without render capability as primary** (e.g. Displaylink).
- Improved **Nvidia** with **additional GPU handling**.
- Fixed error with s**ingle-gpu Nvidia card support**.

X server

- Fixed a **Xorg crash** due to a **NULL pointer dereference in the Intel drive**r.

Window Manager

- Fixed **random login** (greeter) **window focus** issues.

Shadowing/VNC

- Added the **"snapfb" option for the VNC server**.
  More...

Registry	`network.vncserver.snapfb`
Value	enabled / disabled
Info	This option should only be enabled with experienced delays in remote or shadowing session.

- Improved **security of the password authentication method** - the VNC server does not require anymore a file holding the password. **During client authentication**, the **server retrieves** now the **password from the IGEL Setup**.

VNC Viewer

- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now **the session gets unlocked again after about 20 seconds**.
  More...

Parameter	Unlock X server in case of shadowing session freeze
Registry	`network.vncserver.grab_buster`
Type	bool
Value	enabled / disabled

VirtualBox

- Fixed **no automatic resolution changes** as **virtualbox guest** issue.

Audio

- Fixed **headset microphone using 3.5mm audio jack** in **Dell Wyse 3040**.
- Added possibility to **set** some **snd_hda_intel kernel module parameter** to overcome possible issues with sound devices.
  New registry keys:
  More...

Parameter	Enable Message Signaled Interrupt
Registry	`system.sound_driver.snd_hda_intel.enable_msi`
Type	bool
Value	enabled / disabled
Parameter	Force enable device

Registry	system.sound_driver.snd_hda_intel.enable
Type	bool
Value	enabled / disabled
Parameter	Position fix quirk
Registry	system.sound_driver.snd_hda_intel.position_fix
Range	[Default] [Auto (0)] [LPIB (1)] [POSBUF (2)] [VIACOMBO (3)] [COMBO (4)] [SKL+ (5)] [FIFO (6)]
Parameter	Change sound card order
Registry	system.sound_driver.snd_hda_intel.index
Type	integer
Value	empty
Parameter	Detection of DMIC devices
Registry	system.sound_driver.snd_hda_intel.dmic_detect
Range	[Default] [Disabled] [Enabled]
Parameter	Enable this if you encounter sound card problems
Registry	system.sound_driver.snd_hda_intel.single_cmd
Type	bool
Value	enabled / disabled
Parameter	Automatic power save timeout
Registry	system.sound_driver.snd_hda_intel.power_save
Type	integer
Value	empty
Parameter	Reset controller in power save mode
Registry	system.sound_driver.snd_hda_intel.power_save_controller
Type	bool
Value	enabled / disabled

Parameter	Choose sound model to use
Registry	`system.sound_driver.snd_hda_intel.model`
Type	string
Value	Auto

Parameter	If you encounter sound problems try to choose one of the alternative masks
Registry	`system.sound_driver.snd_hda_intel.probe_mask`
Range	[Auto] [1] [8]

- Old settings. **Command at startup removed**.

Jabra

- **Avoid deploying of the same Jabra Xpress package several times** on the same Jabra device.

Evidian

- Evidian now **triggers the regular Horizon session script**.

Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.

TC Setup (Java)

- **Removed "default" button** left of selection box IGEL Setup: **Sessions > Citrix > Citrix Global > Window > Multimonitor full-screen mode**.

Remote Management

- Fixed **repeated firmware registering over the ICG** which can occur after a new firmware was successfully registered in the UMS. The device invokes firmware registering again after every settings transfer from the device to the UMS. This behavior lasts until reboot.
- Fixed **syncing settings changed on the device if** the **UMS wasn't reachable**.
- Fixed handling of the **structure tag** if it was **configured in the system dialog "UMS Registering"**.

IGEL Cloud Gateway

- **Maximum waiting time for a response from the ICG server** can now be **configured by** the parameter **system.remotemanager.rmagent_timeout** (default: 90 seconds).

VNC

- **Shadowing notification** is **restricted to primary monitor** and **cannot be moved outside of the monitor's visible range**.
- Fixed **sporadic connection failure** in VNC server.
- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now the session gets unlocked again after about 20 seconds.
  More...

Parameter	Unlock X server in case of shadowing session freeze

Registry	`network.vncserver.grab_buster`
Type	bool
Value	enabled / disabled

IGEL OS 11

- Supported Devices 11.04.100 (see page 3164)
- Component Versions 11.04.100 (see page 3165)
- General Information 11.04.100 (see page 3172)
- Known Issues 11.04.100 (see page 3173)
- Security Fixes 11.04.100 (see page 3177)
- New Features 11.04.100 (see page 3178)
- Resolved Issues 11.04.100 (see page 3196)
- CA Certificates Contained in IGEL OS 11.04.100 (see page 3204)

Supported Devices 11.04.100

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[312].

312. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.04.100

Clients

Product	Version
Chromium	83.0.4103.61-0ubuntu0.18.04.1
Cisco JVDI Client	12.9.0
Cisco Webex Teams VDI Client	3.0.15711.0
Cisco Webex Meetings VDI Client	40.7.0.375
Citrix HDX Realtime Media Engine	2.9.0-2330
Citrix Workspace App	18.10.0.11
Citrix Workspace App	19.12.0.19
Citrix Workspace App	20.06.0.15
deviceTRUST Citrix Channel	19.1.200.2
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	14.0.0.45623
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.28.4-0ubuntu1.2
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.10.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
IGEL WVD Client	1.0.13igel1596142398
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64 Qualification at Imprivata in progress
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.11.2-1igel8
Open VPN	2.4.4-2ubuntu1.3

Zulu JRE	8.48.0.51-2
Parallels Client (64 bit)	17.1.1
Spice GTK (Red Hat Virtualization)	0.38-2igel93
Remote Viewer (Red Hat Virtualization)	8.0-2git20191213.e4bacb8igel83
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	20.04.2-18.04
ThinLinc Client	4.12.0-6517
ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.10.1+dfsg-4igel13
VMware Horizon Client	5.4.1-15988340
Voip Client Ekiga	4.0.1

Dictation

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20200323
Philips Speech driver	12.9.1

Signature

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.9
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.4.2

Smartcard

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	7

PKCS#11 Library cryptovision sc/interface	7.3.1
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.20.0-3igel37
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel11
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14
Cherry USB2LAN Proxy	3.2.0.3

System Components

OpenSSL	1.0.2n-1ubuntu5.3
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth stack (bluez)	5.52-1igel6
MESA OpenGL stack	20.0.8-1igel117
VAAPI ABI Version	0.40
VDPAU Library version	1.4-1igel1003
Graphics Driver INTEL	2.99.917+git20200515-igel1013
Graphics Driver ATI/RADEON	19.1.0-1+git20200220igel987
Graphics Driver ATI/AMDGPU	19.1.0-1+git20200318igel986
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867

Graphics Driver Nvidia	440.100-0ubuntu0.20.04.1
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1+b6igel952
Input Driver eGalax	2.5.7413
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel957
Input Driver Wacom	0.36.1-0ubuntu2igel888
Input Driver ELO Multitouch	3.0.0
Input Driver ELO Singletouch	5.1.0
Kernel	5.4.48 #mainline-lxos-g1595410170
Xorg X11 Server	1.20.8-2igel1016
Xorg Xephyr	1.20.8-2igel1016
CUPS printing daemon	2.2.7-1ubuntu2.8igel32
PrinterLogic	25.1.0.425
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel13
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.20.4-2ubuntu2.2igel100
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 0.10	0.10.36-2ubuntu0.1igel201
GStreamer 1.x	1.16.2-4igel239
WebKit2Gtk	2.28.3-2igel36
Python2	2.7.17
Python3	3.6.9

VM Guest Support Components

Virtualbox Guest Utils	6.1.10-dfsg-1igel41
Virtualbox X11 Guest Utils	6.1.10-dfsg-1igel41
Open VM Tools	11.0.5-4ubuntu0.18.04.13
Open VM Desktop Tools	11.0.5-4ubuntu0.18.04.1
Xen Guest Utilities	7.10.0-0ubuntu1
Spice Vdagent	0.20.0-1igel95
Qemu Guest Agent	5.0-5igel12

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-2igel4
VPN OpenConnect	8.10-1igel4
Scanner support	1.0.27-1
VirtualBox	6.1.10-dfsg-1igel41

Services

Service	**Size**	**Reduced Firmware**
Asian Language Support	22.5 M	Included
Java SE Runtime Environment	36.0 M	Included
Citrix Workspace app Citrix Appliance Citrix StoreFront	219.5 M	Included
Ericom PowerTerm InterConnect	15.5 M	Included
Media Player	512.0 K	Included
Citrix Appliance Local Browser (Firefox)	70.2 M	Included
RDP VMware Horizon	4.2 M	Included
Cendio ThinLinc	10.0 M	Included

Printing (Internet printing protocol CUPS)	22.2 M	Included
NoMachine NX	26.8 M	Included
VMware Horizon	114.5 M	Included
Voice over IP (Ekiga)	6.5 M	Included
Citrix Appliance	768.0 K	Included
NCP Enterprise VPN Client	27.0 M	Not included
Fluendo GStreamer Codec Plugins	6.8 M	Included
IBM i Access Client Solutions	72.5 M	Not included
Red Hat Enterprise Virtualization	3.0 M	Included
Parallels Client	5.5 M	Included
NVIDIA graphics driver	115.0 M	Not included
Imprivata Appliance	10.8 M	Included
Evidian AuthMgr	2.8 M	Included
Hardware Video Acceleration	13.0 M	Included
Extra Font Package	1.0 M	Included
Fluendo GStreamer AAC Decoder	1.2 M	Included
x32 Compatibility Support	48.0 M	Included
Cisco JVDI client	45.8 M	Included
PrinterLogic	40.8 M	Not included
Biosec BS Login	10.0 M	Not included
Login VSI Login Enterprise	28.8 M	Not included
Stratusphere UX CID Key software	2.8 M	Not included
Elastic Filebeat	15.8 M	Not included
WVD	13.8 M	Included
Local Browser (Chromium)	81.2 M	Not included
deskMate client	5.8 M	Included
Cisco Webex Teams VDI	32.0 M	Not included
Cisco Webex Meetings VDI	36.8 M	Not included
Zoom Media Plugin	39.8 M	Not included

Teradici PCoIP Client	7.8 M	Included
90meter Smart Card Support	256.0 K	Included
Mobile Device Access USB (Limited support)	256.0 K	Not included
VPN OpenConnect (Limited support)	1.5 M	Not included
Scanner support / SANE (Limited support)	2.5 M	Not included
VirtualBox (Limited support)	62.5 M	Not included

General Information 11.04.100

To be beneficial to all new features and implementations, it is recommended to use UMS 6.05.100 or higher and update the corresponding profiles.

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.04.100

Firmware Update

- On **devices with 2 GB of flash storag**e, it could happen that there is **not enough space for updating all features**. In this case, a corresponding error message occurs and unused features must be disabled in IGEL Setup under **System > Firmware Customization > Features** to perform the firmware update. For instructions on how to prevent issues with updating, see Adapting IGEL OS 11.04 or Higher for Devices with Small Storage (see page 61).

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.xxx to 11.04.100, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC received the new setting, **reboot** and **set** the `mimetypes_template` registry key to **"Standard"** again.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`

Value	enabled / <u>disabled</u>

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop. Workaround: **Use CWA 18.10.0**.
- During the running **Microsoft Teams Optimization of Citrix Workspace App 20.06**, **webcam redirection** or **screen sharing** may lead to **display error**s like black stripes or flickering.
- The **performance** of Citrix sessions when using **Workspace App 20.06** may be lower on some devices.
  A possible **workaround** is to **disable** the **virtual channels for Microsoft Teams** and **NSAP** or to set the **HDX transport protocol** to **TCP** only.
  - `ica.module.virtualdriver.vdwebrtc.enable`
  - `ica.module.virtualdriver.nsap.enable`
  - The protocol can be set via the Setup parameter **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT** or via the **server policy** 'HDX Adaptive Transport'.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on Setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After the disconnect of an RDP-based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is not enough space to enable the **Imprivata partition after the update to 11.04.100**. In this case, a corresponding error

message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- **Citrix Certificate Identity Declaration login** does not work with **SecMaker** smartcards.
- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory (RAM)**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to a black screen and non-working graphics.
  Possible workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to 'true'.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L** doesn't work. Therefore, sound output goes through a possibly connected headset and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort-to-DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is **supported** by the **UMS version 6.05.100**.

Base system

- **Update from memory stick** requires network online state (when multiple update stages are involved).

deskMate

- Integrated deskMate solution. Some stability issues may remain.

Security Fixes 11.04.100

Firefox

- Updated Mozilla **Firefox** to **68.10.0esr**:
  - Fixes for **mfsa2020-11**, also known as CVE-2020-6819 and CVE-2020-6820
  - Fixes for **mfsa2020-13**, also known as:
    More...

    CVE-2020-6828, CVE-2020-6827, CVE-2020-6821,
    CVE-2020-6822, and CVE-2020-6825
  - Fixes for **mfsa2020-17** also known as:
    More...

    CVE-2020-12387, CVE-2020-12388, CVE-2020-12389,
    CVE-2020-6831, CVE-2020-12392,
    CVE-2020-12393, and CVE-2020-1239
  - Fixes for **mfsa2020-21** also known as:
    More...

    CVE-2020-12399, CVE-2020-12405,
    CVE-2020-12406, and CVE-2020-12410
  - Fixes for **mfsa2020-25** also known as:
    More...

    CVE-2020-12417, CVE-2020-12418, CVE-2020-12419,
    CVE-2020-12420, and CVE-2020-12421
- Changed option to **deny local file browsing** via file:// URI per default now.
  More...

IGEL Setup	**Firefox Browser > Firefox Browser Global > Window**
Parameter	Hide local filesystem
Registry	`browserglobal.app.filepicker_dialog_hidden`
Value	enabled / disabled

Base system

- **SSH protocol version 1 is now disabled.** All remote connections via SSH must use SSHv2.

Driver

- Updated **Nvidia driver** to version **440.100**.

New Features 11.04.100

Citrix

- Integrated **Citrix Workspace App 20.06**.
  Available Citrix Workspace Apps in this release: **20.06** (default), **19.12**, and **18.10**
- Added a registry key to enable optimization for **Microsoft Teams**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**
Parameter	Microsoft Teams optimization
Registry	`ica.module.virtualdriver.vdwebrtc.enable`
Value	on / off

- Added a registry key to enable support for **NetScaler App Experience (NSAP)** virtual channel.
  More...

Parameter	HDX uses the NSAP virtual channel
Registry	`ica.module.virtualdriver.nsap.enable`
Value	on / off

- Integrated **Citrix HDX/RTME 2.9**.
- Integrated **ZOOM Media Plugin for Citrix** to optimize performance for ZOOM video calls and conferences.
- IGEL x64: 5.0.415463.0619 requires Windows x86 or x64: 5.0.24002.0619. https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions**
Parameter	Zoom Media Plugin
Registry	`ica.module.virtualdriver.vdzoom.enable`
Value	enabled / disabled

- Updated **signotec Virtual Channel** to version **8.0.9**.
  The corresponding changes are:
  - Logging has been improved.
  - A problem with the communication with the signature pads was fixed.
  - USB communication via bulk transfer is model-independent (improved speed).
- Removed parameter **Content redirection** / `ica.wfclient.crenabled` from TC Setup (**Sessions > Citrix > Citrix Global > HDX Multimedia**).

OSC Installer

- Added **dialog "Feature Selection" in IGEL OS Creator** for the selection of features to be installed on the target device. It interactively shows if the current selection of features fits onto the device. The selection of features is saved on the OSC installer medium (when allowed) and set as the default selection for the next installation. If **"Migrate Old Settings"** is selected, the set of features of the old installation is set as the default selection.
- **Reduced memory requirements** of OSC installer for **machines without Nvidia graphic card**.

WVD

- Added **AAC Codec support** to Audio Output redirection.
  More...

Registry	`sessions.wvd%.options.enable-aac`
Value	enabled / disabled

RDP/IGEL RDP Client 2

- Added the **possibility to add a black background** to the RDP auto-reconnect window.
  More...

Registry	`sessions.rdp.options.reconnect-black-fullscreen`
Type	bool
Value	enabled / disabled

- Added configuration option for the **amount of RDP auto-reconnect retries**. The default value will remain "20". A value of "0" means infinite retries.
  More...

Registry	`sessions.rdp.winconnect%.options.reconnect-max-retries`
Type	Integer
Value	20

VMware Horizon

- Updated **VMware Horizon** to version **5.4.1**.
  For usage with **Blast protocol**, it is recommended to enable **DRI3 graphics mode**:
  More...

Parameter	Use DRI3
Registry	`x.driver.use_dri3`
Value	enabled / disabled

- Fixed **handling of RDP's fullscreen mode span**, which means to combine all local monitors for one big remote session.

PowerTerm

- Updated **Ericom PowerTerm** LTC to version **14.0.0.45623**.

Parallels Client

- Updated **Parallels Client** to version **17.1.1**.

Teradici PCoIP Client

- Updated **Teradici PCoIP** Client to version **20.04.2-18.04**. The new version supports **hardware-accelerated H.264 decoding with Ultra PCoIP**.
- New parameters:
  More...

Parameter	Log level
Registry	`pcoip.log-level`
Value	0 / 1 / 2 / 3 / 4

  PCoIP sessions **can now use the global setting**.
  More...

Parameter	Show codec indicator
Registry	`pcoip.codec_indicator`
Value	disabled / enabled
Info	Show a small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec. This setting is only available globally.

XEN

- Added support to run as **XEN guest system**.

NX client

- Updated **NoMachine NX Client** to version **6.11.2**.

ThinLinc

- Updated **ThinLinc** to version **4.12**.

Network

- **DHCP** changes:
  The system now sends a **vendor-class-identifier(option 60) "igel-dhcp-1"**. Furthermore, it requests **vendor-encapsulated-options (43)**. Those can be used to transfer IGEL-specific options **igelrmserver(224) and umsstructuretag(226)** in the vendor namespace (with the same option numbers and types) instead of in the global namespace.
  The former way is also still functional, but values transferred in the new way override those which were transferred the old way.
  Apart from 224 and 226 one more option is defined in the vendor space: **"exclusive", option 1,**

type byte. Its presence means that global options 224 and 226 shall not be interpreted in the traditional way and only settings in the vendor space apply.
IPv6 is not involved.

- Added support for **LTE module HP lt4132**.
- Updated **Network Manager** to version **1.20.4**.
  - The range of **network.interfaces.wirelesslan.device0.bgscan.module** now **includes "default" for** using **original upstream Network Manager settings**.
- Added some **additional Ethernet network drivers**.
  More...
  - amd-xgbe : AMD 10 Gigabit Ethernet driver
  - ec_bhf : Beckhoff EtherCAT
  - liquidio_vf : Cavium LiquidIO Intelligent Server Adapter Virtual Function driver
  - liquidio : Cavium LiquidIO Intelligent Server Adapter driver
  - thunder_bgx : Cavium Thunder BGX/MAC driver
  - nicvf : Cavium Thunder NIC Virtual Function driver
  - nicpf : Cavium Thunder NIC Physical Function driver
  - thunder_xcv : Cavium Thunder RGX/XCV driver
  - atlantic : aQuantia Corporation(R) network driver
  - be2net : Emulex OneConnect NIC driver 12.0.0.0
  - ixgb : Intel(R) PRO/10GbE network driver
  - igc : Intel(R) 2.5G Ethernet Linux driver
  - ice : Intel(R) Ethernet Connection E800 Series Linux driver
  - i40e : Intel(R) Ethernet Connection XL710 network driver
  - iavf : Intel(R) Ethernet Adaptive Virtual Function network driver
  - ixgbe : Intel(R) 10 Gigabit PCI Express network driver
  - igbvf : Intel(R) Gigabit Virtual Function network driver
  - ixgbevf : Intel(R) 10 Gigabit Virtual Function network driver
  - ena : Elastic Network Adapter (ENA)
  - nfp : The Netronome Flow Processor (NFP) driver
  - bna : QLogic BR-series 10G PCIe Ethernet driver
  - enic : Cisco VIC Ethernet NIC driver
  - mlx5_core : Mellanox 5th generation network adapters (ConnectX series) core driver
  - mlx4_en : Mellanox ConnectX HCA Ethernet driver
  - ionic : Pensando Ethernet NIC driver
  - sfc-falcon : Solarflare Falcon network driver
  - sfc : Solarflare network driver
  - dwc-xlgmac : Synopsys DWC XLGMAC driver
  - hinic : Huawei Intelligent NIC driver
  - cassini : Sun Cassini Ethernet driver
  - niu : NIU Ethernet driver
  - samsung-sxgbe : SAMSUNG 10G/2.5G/1G Ethernet PLATFORM driver
  - cxgb : Chelsio 10Gb Ethernet driver
  - qede : QLogic FastLinQ 4xxxx Ethernet driver
  - qlcnic : QLogic 1/10 GbE Converged/Intelligent Ethernet driver
  - qed : QLogic FastLinQ 4xxxx Core module
  - netxen_nic : QLogic/NetXen (1/10) GbE Intelligent Ethernet driver

- vxge : Neterion's X3100 Series 10GbE PCIe I/OVirtualized Server adapter
- myri10ge : Myricom 10G driver (10GbE)
- tehuti : Tehuti Networks(R) network driver
- bnxt_en : Broadcom BCM573xx network driver
- bnx2x : QLogic BCM57710/57711/57711E/57712/57712_MF/57800/57800_MF/57810/57810_MF/57840/57840_MF driver

- Added a registry key for specifying a **space-separated list of DNS resolver options**. See "**man resolv.conf**".
  More...

Parameter	Option list
Registry	`network.dns.options`
Type	string
Value	empty

Wi-Fi

- Added support for **WPA3 Personal network authentication**.
- Added a registry key for **preferring WPA3 Personal** (i.e. SAE) or **WPA2 Personal** at the time a connection is created with Wireless Manager when the access point offers both:
  More...

Parameter	Prefer WPA3 Personal to WPA2 Personal
Registry	`network.applet.wireless.prefer_sae`
Range	[default] [yes] [no]
Info	"default" currently means "no"

- Added **captive portal support for Wi-Fi**. Passing through a captive portal (which is basically a web application) is sometimes **necessary to achieve full network connectivity** (here also referred to as online state).
  - The **feature is disabled when** the following **registry key** is **empty**. Otherwise, it should be a **URI** that is **suitable for NetworkManager connectivity check**.
    More...

Parameter	Online check URI
Registry	`network.global.onlinecheck.uri`
Range	[] [http://connectivity-check.ubuntu.com/]
Value	http://connectivity-check.ubuntu.com/

  - The following key specifies the **conditions of the online check**. It is also required that **no Ethernet cable is plugged in** and **DHCP is not set** in the UMS.
    More...

Parameter	Condition for online check
Registry	`network.global.onlinecheck.condition`
Range	[None] [Network is user-defined] [Network is open]

- This key determines **how many seconds to wait for full network connectivity** before the network connection is considered complete with incomplete connectivity. The timeout should allow a user to do what is necessary for passing through the captive portal.
More...

Parameter	Online check timeout
Registry	`network.global.onlinecheck.timeout`
Type	integer
Value	120

- Enabled **use of 802.11r**, also known as **fast BSS transition** or FT. This is confirmed to work at least in the **mode "over the air"**.

Smartcard

- Updated **OpenSC** to version **0.20.0**. See https://github.com/OpenSC/OpenSC/releases/tag/0.20.0 for detailed release notes.

Cisco JVDI Client

- Updated **Cisco JVDI** client to version **12.9.0**.

Cisco Webex VDI

- Integrated the new feature **Cisco Webex Teams VDI for Citrix** and **Horizon** sessions.
Cisco Webex Teams version: **3.0.15711.0**
- Added a parameter to activate the feature within **Citrix**:
More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > Cisco**
Parameter	Cisco Webex Teams VDI
Registry	`ica.module.virtualdriver.vdciscoteams.enable`
Value	enabled / disabled

- Added a parameter to activate the feature within **VMware**:
More...

IGEL Setup	**Sessions > Horizon > Horizon Client Global > Unified Communications > Cisco**
Parameter	Cisco Webex Teams VDI - Horizon

Registry	`vmware.view.vdciscoteams.enable`
Value	enabled / disabled

- Integrated the new feature **Cisco Webex Meetings VDI for Citrix** sessions.
  Client Version: **40.7.0.375**
- Added a parameter to activate the feature within **Citrix**:
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Unified Communications > Cisco**
Parameter	Cisco Webex Meetings VDI
Registry	`ica.module.virtualdriver.vdciscomeetings.enable`
Value	enabled / disabled

Base system

- Updated base system to **Ubuntu LTS** version **18.04**.
- Updated **kernel** to version **5.4.48**.
- Added **notification for critical system out-of-memory state** when the available **system memory is lower than 40 MB** and **processes were killed** to prevent the system from freezing.
- Display **AMD Memory Guard in Boot Mode** when it's active.
- Added **notification option for Session Autostart** when a autostart delay is configured. It is possible to cancel the session autostart or to start immediately.
  More...

IGEL Setup	*** > Desktop integration**
Parameter	Autostart notification
Value	enabled / disabled

- Added correct **UI handling** for **Wacom DTU-1141B**.
- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version **2.30**). The following authorities were added:
  More...
  - "Certigna Root CA"
  - "GTS Root R1"
  - "GTS Root R2"
  - "GTS Root R3"
  - "GTS Root R4"
  - "UCA Extended Validation Root"
  - "UCA Global G2 Root"
  - "GlobalSign Root CA - R6"
  - "OISTE WISeKey Global Root GC CA"
  - "GDCA TrustAUTH R5 ROOT"
  - "SSL.com EV Root Certification Authority ECC"
  - "SSL.com EV Root Certification Authority RSA R2"

- "SSL.com Root Certification Authority ECC"
- "SSL.com Root Certification Authority RSA"
- "TrustCor ECA-1"
- "TrustCor RootCert CA-1"
- "TrustCor RootCert CA-2"

- The following authorities were removed:
  More...
  - "Certplus Root CA G1"
  - "Certplus Root CA G2"
  - "OpenTrust Root CA G1"
  - "OpenTrust Root CA G2"
  - "OpenTrust Root CA G3"
  - "TÜRKTRUST Elektronik Sertifika Hizmet Saglayicisi H5"
  - "Visa eCommerce Root"
  - "ACEDICOM Root"
  - "AddTrust Low-Value Services Root"
  - "AddTrust Public Services Root"
  - "AddTrust Qualified Certificates Root"
  - "CA Disig Root R1"
  - "CNNIC ROOT"
  - "Camerfirma Chambers of Commerce Root"
  - "Camerfirma Global Chambersign Root"
  - "Certinomis - Autorit, Racine"
  - "Certum Root CA"
  - "China Internet Network Information Center EV Certificates Root"
  - "Comodo Secure Services root"
  - "Comodo Trusted Services root"
  - "DST ACES CA X6"
  - "GeoTrust Global CA 2"
  - "PSCProcert"
  - "Security Communication EV RootCA1"
  - "Swisscom Root CA 1"
  - "Swisscom Root CA 2"
  - "Swisscom Root EV CA 2"
  - "TURKTRUST Certificate Services Provider Root 2007"
  - "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
  - "UTN USERFirst Hardware Root CA"
- Added parameter to override **rate limit of debug messages** in journal. It should be enabled for debugging processes which generate a big amount of messages in order to avoid skipping of messages.
  More...

Parameter	No rate limit
Registry	`system.journald.no_rate_limit`

Value	enabled / disabled

- It's possible to **extend the login options of the Kerberos** login window now.
  There are several new registry keys:
  More...

Parameter	extended login
Registry	`sessions.xlock0.options.login_extension_active`
Value	enabled / disabled

  If enabled, an "**Associate Type" combo box is shown**. The **entries of the combo box** are **configured with** the following **login_feature1**, **login_feature2**, and **login_feature3 keys**.
  - Configure the **label of the "Associate Type" combo box**:
    More...

Parameter	login features label
Registry	`sessions.xlock0.options.login_features_label`
Value	Default: empty which means "Associate Type"

  - **The first entry of the "Associate Type" combo box**. To enable the combo box entry, add e.g. the text "Store associate at home store".
    More...

Parameter	login_feature1
Registry	`sessions.xlock0.options.login_feature1`

    If the entry is selected, the **username is expanded by a fixed string** defined in `login_extension_default` registry key.
  - The **fixed username extension** for the first feature. It can be set e.g. by a script.
    More...

Parameter	login extension default value
Registry	`sessions.xlock0.options.login_extension_default`

  - **The second entry of the "Associate Type" combo box.** To enable the combo box entry, add e.g. the text "Store associate visiting this store".
    More...

Parameter	login_feature2
Registry	`sessions.xlock0.options.login_feature2`

    If the entry is selected, the **username is expanded by a suffix** that is **entered in a separate entry widget**.
  - The **label of the entry field for the username suffix.** Set it e.g. to "Store Number".

More...

Parameter	login_extension_label
Registry	`sessions.xlock0.options.login_extension_label`
Value	Default: empty which means "no label"

- **The third entry of the "Associate Type" combo box**. To enable the combo box entry, add e.g. the text "Homeoffice associate visiting this store".
  More...

Parameter	login_feature3
Registry	`sessions.xlock0.options.login_feature3`

  If the entry is selected, **another domain** can be **selected from an appended domain combo box**.
- The **label for the domain entry field**.
  More...

Parameter	login domain label
Registry	`sessions.xlock0.options.login_domain_label`
Value	Default: empty which means "domain"

- The **extension to the username** is **added after a dot** ('.').
- For the **domain drop-down box**, **four different domains are configurable** here:
  More...

IGEL Setup	**Security > Active Directory/Kerberos > Domain 1 - 4**
Parameter	Fully qualified domain name
Registry	`auth.krb5.realms.realm0.realm`
Registry	`auth.krb5.realms.realm1.realm`
Registry	`auth.krb5.realms.realm2.realm`
Registry	`auth.krb5.realms.realm3.realm`

- There are keys to **add more domain names**:
  More...

Parameter	Domain
Registry	`auth.krb5.extended_domain%.name`
Info	Add a new instance for each domain entry.

- In the Kerberos login window, it's now possible to turn on or off **numlock** and/or **capslock for password input**.
  Registry keys:
  More...

Parameter	Handling of numlock
Registry	`sessions.xlock0.options.numlock_approach`
Range	[don't change] [set on] [set off]
Info	"set on": force numlock on when password is entered "set off": force numlock off when password is entered
Parameter	Handling of capslock
Registry	`sessions.xlock0.options.capslock_approach`
Range	[don't change] [set on] [set off]
Info	"set on": force capslock on when password is entered "set off": force capslock off when password is entered

- It's now possible to **show a message in the Kerberos login window**. Registry key:
  More...

Parameter	banner text
Registry	`sessions.xlock0.options.banner_text`
Info	The user will see the message on the top border.

- In the Kerberos login window, there is a **mode to convert passwords always to upper case**. To turn it on, use:
  More...

Parameter	case-insensitive password
Registry	`sessions.xlock0.options.case_insensitive_password`
Value	enabled / disabled

- With this key, the text for the **case-insensitive indicator** can be modified:
  More...

Parameter	case-insensitive text
Registry	`sessions.xlock0.options.case_insensitive_text`
Value	Default: empty which means "case-insensitive"

- Fixed **ThinkPad Brazil keyboard layout**.

- It is possible to **show a custom logo** in the Kerberos login window. Also, the **background and text color is customizable** now.
  Registry keys:
  More...

Parameter	path for login image
Registry	`sessions.xlock0.options.login_image`
Value	/usr/share/pixmaps/greeter-user.svg
Info	Supported image formats include: PNG, JPG, SVG

Parameter	set specific colors for greeter
Registry	`sessions.xlock0.options.set_color`
Value	enabled / disabled

Parameter	text color
Registry	`sessions.xlock0.options.text_color`
Value	#ffffff
Info	Text color in the format #rrggbb Example: #ff0077

Parameter	background color
Registry	`sessions.xlock0.options.background_color`
Value	#000000
Info	Background color in the format #rrggbb Example: #7700ff

- Added **new local logon method "Login with Smart Card Certificate"**. It implements the **pam_pkcs11 smartccard authentication module**. For a successful configuration, the following has to be provided via **UMS file transfer**:
  - **root and intermediate CA certificates** for verification of the client certificates in folder `/etc/pam_pkcs11/cacerts`
  - file `/etc/pam_pkcs11/cn_map` which contains **mappings of Common Names to UPN names**.
    Each line is in the format `\<common name> -> \<logon name>`
    where
    `\<common name>` is the common name part of the subject of the certificate
    `\<logon name>` is

- in case of **Kerberos Enterprise** (`auth.login.krb5_enterprise`) **disabled**: the UPN name of the SubjectAltName extension of the certificate, e.g. user@MY.DOMAIN
- in case of **Kerberos Enterprise** (`auth.login.krb5_enterprise`) **enabled**: the UPN name of the SubjectAltName extension of the certificate with Default Domain (`auth.krb5.libdefaults.default_realm`) suffix, e.g. user@DOMAIN.SUFFIX@DEFAULT.DOMAIN[313]

- The logon method **can** either **be used standalone or together with Kerberos logon** as a fallback if Kerberos does not succeed.
  More...

Parameter	Login with Smart Card Certificate
Registry	`auth.login.pkcs11`
Value	false / true

Parameter	Certificate verification policy
Registry	`auth.login.pkcs11_cert_policy`
Value	ca,ocsp_on,signature

Parameter	Enable Debugging of Smart Card Certificate Logon
Registry	`auth.login.pkcs11_debug`
Value	false / true

- It is possible to expand the store number by a registry key:
  More...

Parameter	expand store
Registry	`sessions.xlock0.options.expand_store`
Value	enabled / disabled

- Fixed: The **login screen** is **adjusted to lower resolutions**.
- It is possible to activate enter key to login on all fields.
  More...

Parameter	auto login on all fields
Registry	`sessions.xlock0.options.auto_login`
Value	enabled / disabled

313. mailto:DOMAIN.SUFFIX@DEFAULT.DOMAIN

X11 system

- Changed: Use **modesetting graphics driver** on **devices with newer intel GPUs**.
- Changed registry key:
  More...

Parameter	Use generic modesetting driver for INTEL hardware
Registry	`x.drivers.intel.use_modesetting`
Range	[Auto] [True] [False]

- Updated **DisplayLink driver** to version **5.3.1.34**.
- Added new registry key for **Nvidia cards** (use this **if you want to use PRIME**):
  More...

Parameter	Enable/Disable NVIDIA Kernel Modesetting support
Registry	`x.drivers.nvidia.use_modeset`
Range	[Default] [Enabled] [Disabled]
Info	"Default" is currently the same as "disabled"

- Updated **florence soft keyboard** to version **0.6.3**.
- **Removed 640x480** from possible **display resolution range**.
- Added possibility to **change the order of primary** and **secondary graphic card**.
  New registry key:
  More...

Parameter	Make the secondary graphic card to the primary one
Registry	`x.drivers.swap_card0_with_card1`
Value	true / false

- Added possibility to **invert the order of all graphic card**s.
  New registry key:
  More...

Parameter	Invert default graphic card ordering
Registry	`x.drivers.swap_all`
Value	true / false

- Added possibility to **choose the driver** which should become **the primary graphic card**.
  New registry key:
  More...

Parameter	Choose which drivers should be preferred to become the primary graphic card
Registry	`x.drivers.preferred_driver`

Value	

X server

- Added possibility to influence **mode used for mirroring screens with different resolutions**. (Notice: here scaling may not always work).
  New registry key:
  More...

Parameter	Choose the mode which should be used for mirroring monitors if resolution differs
Registry	`x.xserver0.mirror_mode`
Range	[Default] [Biggest common resolution] [Scaling]
Value	Default (use panning if needed)

Driver

- Updated **Grundig Dictation driver for Citrix** and **RDP** to version **0.10**.
  The changes are:
  - Support **third-party USB HID devices** in a more flexible way
  - Fixed USB transfer overflow for **Philips LFH 9620**
  - Remove **erroneous debug output** in release configuration
  - Allow to **control** also **"Headphone" volume & switches**
- Updated **Olympus driver for dictation** to version **2020-03-23-143654**.
  Changelog:

  New:

  - DR-1200: PID 0225
  - DR-2300: PID 0256

  Changed:

  - PID 0253 from DR-2100 to DR-1200
- Updated **Philips Speech driver** to version **G12.9**.
  The changes are:
  - Support for **Philips SpeechLive**
  - Faster and more reliable remote session connection status check
  - **Shutdown of** the **PSPDispatcher.exe** on the server if it's not in use anymore.
- Updated **StepOver TCP client** and **Citrix plugin** to version **2.4.2**. Fixed **crash of Citrix** session while **using** the **signature pad**.

Audio

- Integrated **new sound mixer**.
- New combo box for **audio device selection in TC Setup** available:
  - **Accessories > Sound Preferences > Options > Default Sound Output**
  - **Accessories > Sound Preferences > Options > Default Sound Input**

Appliance Mode

- Integrated: The **new Browser Appliance mode** is the successor for the XenDesktop appliance mode. The Browser is configured as in XenDesktop appliance mode, but **does not use the upstream SAS window**.
  More...

IGEL Setup	**Sessions > Appliance Mode**
Parameter	Browser
Registry	`xen.xenapp-morph.enabled`
Type	Bool
Value	enabled / disabled

IGEL Setup	**Sessions > Appliance Mode > Browser**
Parameter	Web URL
Registry	`xen.xenapp-morph.xendeliveryserverurl`
Type	string

- A **hyperlink to the "On-screen Keyboard"** is available on the right side **under "Related Configurations"**.

Multimedia

- Added **ffmpeg support** for following codecs:
  - Added support for **new decoders**:
    More...

    flac, gif, libaom_av1, mjpeg, mjpegb, mp1,mp1float, mp2, mp3, mp3adu, mp3adufloat, mp3float, opus, theora, vorbis, vp2, vp8, vp9, and wavepack
  - Added support for **new encoder**: libopus
  - Added support for **new hwaccels**:
    More...

    mjpeg_vaapi, mpeg1_vdpau, mpeg2_vaapi, mpeg2_vdpau, vp8_vaapi, and vp9_vaapi
  - Added support for **new parsers**: avi, flac, gif, matroska, mp3, ogg, and wav
  - Added support for **new demuxers**: avi, flac, gif, matroska, ogg, and wav
  - Added support for **new muxers**: ogg and opus

Chromium Browser

- Integrated **Chromium** browser version **83.0.4103.61** as experimental feature. Configurable at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global** and **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Sessions**
- Main switch to enable and disable **IGEL configuration**:
  More...

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global**
Parameter	Use IGEL Setup for configuration
Registry	`chromiumglobal.app.igelsetupconfig`
Value	disabled / enabled
Info	With disabled IGEL configuration, you can use the generic Custom Setup to configure Chromium. The Custom Setup can be found at **IGEL Setup > Sessions > Chromium Browser > Chromium Browser Global > Custom Setup: Policies**, **Preferences**, **Commandline Options**.

- Parameter for **enabling** and **disabling** the **H.264 decoding**:
  More...

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global**
Parameter	H.264 decoding
Registry	`chromiumglobal.app.h264_decoding`
Value	enabled / disabled
Info	Enable Audio/Video playback of non-free codecs (H.264+AAC) - the support is in a beta state and therefore disabled by default.

Evidian

- Added the Evidian **built-in option 'Process To Spy'**.
  More...

Registry	`evidian.processtospy`
Value	YOUR-PROCESS / disabled

ControlUp

- Integrated **ControlUp Monitoring Tool for Citrix** and **Horizon** sessions.

Hardware

- Added hardware support for **Lenovo M625q**.
- Added hardware support for **LG CL600N**.
- Added hardware support for **HP Engage Go Mobile System**.
- Added hardware support for **Fujitsu FUTRO S740**.
- Added hardware support for **OnLogic CL210G-10**.
- Added hardware support for **OnLogic KARBON 300**.
- Added hardware support for **Rein Medical Clinio S 522TCT** and **S 524TCT**.
- Added hardware support for **HP t640 Thin Client**.

- Added basic support for **Macbook models 2018** and **newer**.
- Added support for **Sennheiser MB 660**, **SC 630**, **SC 45**, **SC 160 headsets**.
- Added support for **Plantronics Savi 8245 Office**, **Voyager 6200 UC**, **Savi 8220 headsets**.
- Added serial port driver for **Exar UART PCIe card**.
- Added driver for **GSPCA based webcams**.

TC Setup (Java)

- Added Setup page **Sessions > Horizon Client > Horizon Client Global > Window**. Settings for "**Window size**" and "**Multimonitor full-screen mode**" can be set.
  These settings are repeated and originate in RDP Global but are now presented in a more obvious place for Horizon sessions.

IGEL Cloud Gateway

- Added support for **Secure Terminal over ICG**.
- **Changed default order of connecting to the IGEL Remote Management** - an available UMS Server is preferred now by default. The device establishes a configured ICG connection only if the UMS Server is not reachable. This behavior can be changed by the parameter:
  More...

Registry	`system.remotemanager.icg_try_ums_connect`
Value	true / false

Fabulatech

- Updated **FabulaTech Scanner for Remote Desktop** client to version **2.4.0.11**.
- Updated **FabulaTech plugins** to version **3.6.2**.
- Updated **Fabulatech USB for Remote Desktop plugins** to version **3.6.8**.

Jabra

- **Jabra Xpress** (JDU) is upgraded to the **7.2.0-509** version. List of the newly introduced parameters:
  More...

Registry	`jabra.xpress.show_jdu_gui`
Value	true / false
Registry	`jabra.xpress.device_dashboard.autopost`
Value	true / false

Resolved Issues 11.04.100

Citrix

- "**Green artifacts**" problem in Citrix sessions (most probably) fixed.
- Citrix **hardware video acceleration** supports the **latest Intel hardware**.

OSC Installer

- Fixed issue with **filesystems not** always get detected correctly in **initramfs OSC Installer** (needed for using iso file boot parameter).
- Fixed: **username and password in the error message** are not shown anymore when firmware file could not be downloaded.
- Get **URLs** with **username:password@** working.

RDP/IGEL RDP Client 2

- Fixed error when **renaming a non-empty shared folder**.

WVD

- Includes **WVD client with** fixed **RDcoreSDK** version.
- **Clipboard redirection** has potential privacy and security risks and is therefore **disabled by default**.
- **IGEL WVD Client** integrated

VMware Horizon

- Fixed missing **support for ThinPrint** and **Skype for Business** when starting **Horizon from Firefox browser**.

Firefox

- Fixed Firefox **block extension missing tabs** created via command line argument.
- Fixed **rtsp media stream** with enabled apparmor.
- **Show "blocked" page instead of closing tab** when blocked page is viewed in Firefox.
- Fixed functionality in the local setup to start the **certificate manager of the Firefox browser**.
- Fixed functionality in the local setup to **start the Firefox** browser **with the internal page to show the installed plugins**.
- Fixed **restart mechanism in the Firefox** browser where the browser could not be closed on suspend resulting in a superfluous browser window on resume.

Network

- Improved **Wi-Fi DHCP lease handling**: Leases are discarded when the network changes. The former behavior caused problems with certain iPhone IOS versions.
- **802.1X failures** now generally **result in falling back to a connection without authentication**, e.g. also in the case of 802.1X settings that don't make sense at all. This only **applies if the fallback is allowed** of course.
- **wpa_supplicant** now adds **timestamps to entries of its log file**.
- Use **e1000e driver** out of the kernel **as default** instead of the third-party driver.
- Added a registry key that determines whether **lldpd is in receive-only mode**.

More...

Parameter	Disable sending LLDP packets
Registry	`network.lldp.rxonly`
Value	true
Attention:	If the behavior since 10.06.100 shall be preserved, this key must be set to "false".

- Updated **scep** to version **0.7.0**.

Wi-Fi

- Fixed non-working **Marvell WLAN device 8997** (SDIO version).

NCP VPN

- Added fix for **NCP Secure Client**.

genucard VPN

- **genucard 3 is supported** now.

Imprivata

- **Control the visibility** of the **Horizon session control bar** via registry parameter:
  More...

Registry	`vmware.view.menu-bar`
Value	enabled / disabled

- Honor the Citrix Window Configuration in **Imprivata Appliance Mode**.
- Fixed **Lock key** and **Tap out** behavior.
- Fixed **MS RDSH** session.
- Simplified the configuration of **Imprivata FUS**.
- **Enable the following** if you use **Imprivata** versions **above 6.3**:
  More...

Registry	`imprivata.gain_permission`
Value	enabled / disabled

- Fixed **bug regarding Imprivata** and **On-Screen Keyboard**.
- **Restore the keyboard map** after Horizon sessions.

Smartcard

- Fixed not working **90meter in Firefox** when **apparmor is active**.
- Fixed problem in **smartcard resource manager PC/SC-Lite** which caused **disconnects of VMware Horizon sessions** when using smartcards with certain applications.
- Added **driver for** smartcard reader **Elatec TWN4 CCID** (USB 0x09D8:0x0425).
- Updated **cryptovision scInterface** to version **7.3.1**.
  The changes are:
  More...

    - Consolidated features of the last versions 7.2 and 7.1
    - Malta eID Release
    - Added Admin Card Gemalto V3
- Updated **PC/SC-Lite smartcard resource manager** to version **1.8.26**.

HID

- Fixed: **Switching touchpad to other driver** via IGEL registry key.

CUPS Printing

- Added new version **25.1.0.425** of **Printerlogic Printer Installer Client**.
- Added **new printer models** into IGEL OS from the current CUPS drivers.

Base System

- Fixed bug in **folder generation of the Application Launcher**.
- Fixed **TLS certificate verification** problem of **certificates signed by "USERTrust RSA CA"** or **"COMODO RSA CA"**. The problem could occur in clients like Citrix Workspace App and VMWare Horizon client.
- Fixed **password change with AD/Kerberos**. Before this fix, the password complexity rules were not enforced for users with the Reset Password permission for their account.
- You can now **connect to Bluetooth devices without pairing**. For this a new registry key is available.
  More...

Parameter	connect devices without pairing
Registry	`devices.bluetooth.connect_only`
Value	enabled / disabled

- **Some devices do not connect automatically after reboot**. To fix that, `bluetoothctl connect \<device-ID>` can be executed via script. If the **device is connected (0)** or **not (1)** can be seen in return value.
  Known devices that do not connect:
    - dialog semiconductor IoT Multi Sensor DK
- **SSHv1 support is now removed** due to newer openssh libraries.
- **Forcing** protocol **version 1** via **SSH Session > Options** is **no longer possible**.
- The `network.ssh_server.server_key_bits` registry key parameter is **removed** due to **deprecation of SSHv1**.
- Updates **systemd** to **Ubuntu Focal version**.
- Improved **stability of mounting network shares** when using a **static network configuration**.
- Fixed **apparmor cache** issue **after update with OSC installer**.
- Bug fix: **touchscreen calibration** on 1 or more normal screen with 1 touch screen environment.
- Fixed **syslog**, **kern.log**, **auth.log**, and **daemon.log** entries are **not shown in IGEL System Log Viewer**.
- Updated **Grub2** to current Debian SID/Bullseye version **2.04**.
- **Removed** deprecated registry keys `system.idlecommand`.
- New **Bluetooth pairing tool** and **Bluetooth tray icon** for Bionic.

- Updated **kernel** to mainline version **5.4.48**.
- If used as master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only on first boot and never again.
- Possible **rollout of initial settings, certificates or licenses placed on first partition** for this you need to:
    a. Write image to your USB/Flash medium.
    b. Mount or simply access the **1. VFAT partition** which is present (should be empty).
    c. Copy your **setup.ini** and/or ****.lic files** to the 1st partition (no directories).
    d. Create a `ca-certs` directory and copy your certificates into it. They will be copied to the `/wfs/ca-certs` directory on first boot.
    e. You can now copy the USB/Flash medium several times if needed.
    f. On first boot, the device will reboot out of the splash screen (reread changed partition table)
    g. The settings, certificates and/or licenses will get rolled out and deleted from the 1st partition.
- Added initial support for **Thunderbolt devices** (only limited support here, may work but is not guaranteed).
- Updated IGEL **EULA**.
- Updated **AMD Microcode** to version **3.20191218.1**.
- Updated **Intel Microcode** to version **20200520** and a special update for **J1900 devices**.
- Updated **Intel Microcode** to **20200616** version.
- Added a **userspace oom killer** to the firmware.

Firmware Update

- An **ongoing firmware update can now be canceled by the use**r when the network online status could not be reached after 10 seconds (since start of the firmware update).

H264

- **Citrix hardware video acceleration** supports the latest Intel hardware.

Storage Devices

- Fixed mount issues with **Iphone XR/XE/11PRO**.
- **Mobile Device Access** feature respects USB Access Control now.
- Fixed unwanted **ownership change** of automounted Linux filesystem root directories.

X11 System

- Fixed **Display Switch not saving settings over reboot**.
    - **Default to settings from Setup** instead of mirror when no Display Switch profile is available.
- Prevent misconfiguration that **picks GPU without render capability as primary** (e.g. Displaylink).
- Improved **Nvidia** with **additional GPU handling**.
- Fixed error with s**ingle-gpu Nvidia card support**.

X server

- Fixed a **Xorg crash** due to a **NULL pointer dereference in the Intel drive**r.

Window Manager

- Fixed **random login** (greeter) **window focus** issues.

Shadowing/VNC

- Added the **"snapfb" option for the VNC server**.
  More...

Registry	`network.vncserver.snapfb`
Value	enabled / disabled
Info	This option should only be enabled with experienced delays in remote or shadowing session.

- Improved **security of the password authentication method** - the VNC server does not require anymore a file holding the password. **During client authentication**, the **server retrieves** now the **password from the IGEL Setup**.

VNC Viewer

- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now **the session gets unlocked again after about 20 seconds**.
  More...

Parameter	Unlock X server in case of shadowing session freeze
Registry	`network.vncserver.grab_buster`
Type	bool
Value	enabled / disabled

VirtualBox

- Fixed **no automatic resolution changes** as **virtualbox guest** issue.

Audio

- Fixed **headset microphone using 3.5mm audio jack** in **Dell Wyse 3040**.
- Added possibility to **set** some **snd_hda_intel kernel module parameter** to overcome possible issues with sound devices.
  New registry keys:
  More...

Parameter	Enable Message Signaled Interrupt
Registry	`system.sound_driver.snd_hda_intel.enable_msi`
Type	bool
Value	enabled / disabled
Parameter	Force enable device

Registry	system.sound_driver.snd_hda_intel.enable
Type	bool
Value	enabled / disabled
Parameter	Position fix quirk
Registry	system.sound_driver.snd_hda_intel.position_fix
Range	[Default] [Auto (0)] [LPIB (1)] [POSBUF (2)] [VIACOMBO (3)] [COMBO (4)] [SKL+ (5)] [FIFO (6)]
Parameter	Change sound card order
Registry	system.sound_driver.snd_hda_intel.index
Type	integer
Value	empty
Parameter	Detection of DMIC devices
Registry	system.sound_driver.snd_hda_intel.dmic_detect
Range	[Default] [Disabled] [Enabled]
Parameter	Enable this if you encounter sound card problems
Registry	system.sound_driver.snd_hda_intel.single_cmd
Type	bool
Value	enabled / disabled
Parameter	Automatic power save timeout
Registry	system.sound_driver.snd_hda_intel.power_save
Type	integer
Value	empty
Parameter	Reset controller in power save mode
Registry	system.sound_driver.snd_hda_intel.power_save_controller
Type	bool
Value	enabled / disabled

Parameter	Choose sound model to use
Registry	`system.sound_driver.snd_hda_intel.model`
Type	string
Value	Auto

Parameter	If you encounter sound problems try to choose one of the alternative masks
Registry	`system.sound_driver.snd_hda_intel.probe_mask`
Range	[Auto] [1] [8]

- Old settings. **Command at startup removed**.

Jabra

- **Avoid deploying of the same Jabra Xpress package several times** on the same Jabra device.

Evidian

- Evidian now **triggers the regular Horizon session script**.

Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.

TC Setup (Java)

- **Removed "default" button** left of selection box IGEL Setup: **Sessions > Citrix > Citrix Global > Window > Multimonitor full-screen mode**.

Remote Management

- Fixed **repeated firmware registering over the ICG** which can occur after a new firmware was successfully registered in the UMS. The device invokes firmware registering again after every settings transfer from the device to the UMS. This behavior lasts until reboot.
- Fixed **syncing settings changed on the device if** the **UMS wasn't reachable**.
- Fixed handling of the **structure tag** if it was **configured in the system dialog "UMS Registering"**.

IGEL Cloud Gateway

- **Maximum waiting time for a response from the ICG server** can now be **configured by** the parameter **system.remotemanager.rmagent_timeout** (default: 90 seconds).

VNC

- **Shadowing notification** is **restricted to primary monitor** and **cannot be moved outside of the monitor's visible range**.
- Fixed **sporadic connection failure** in VNC server.
- Fixed **occasional freeze of shadowing session** e.g. when resizing a window. Now the session gets unlocked again after about 20 seconds.
  More...

Parameter	Unlock X server in case of shadowing session freeze

Registry	`network.vncserver.grab_buster`
Type	bool
Value	enabled / disabled

CA Certificates Contained in IGEL OS 11.04.100

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	`ACCVRAIZ1.crt`
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	`AC_RAIZ_FNMT-RCM.crt`
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	`Actalis_Authentication_Root_CA.crt`
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	`AffirmTrust_Commercial.crt`
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	`AffirmTrust_Networking.crt`
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	`AffirmTrust_Premium.crt`
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	`AffirmTrust_Premium_ECC.crt`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`AmazonRootCA1.pem)`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`Amazon_Root_CA_1.crt`
Amazon Root CA 2	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_2.crt`
Amazon Root CA 3	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_3.crt`
Amazon Root CA 4	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_4.crt`
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	`Atos_TrustedRoot_2011.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt`
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`BTCTRoot.pem)`

Certificate name	Expiry date	File in /etc/ssl/certs
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`Baltimore_CyberTrust_Root.crt`
Buypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	`Buypass_Class_2_Root_CA.crt`
Buypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	`Buypass_Class_3_Root_CA.crt`
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	`CA_Disig_Root_R2.crt`
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	`CFCA_EV_ROOT.crt`
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	`COMODO_Certification_Authority.crt`
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_ECC_Certification_Authority.crt`
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_RSA_Certification_Authority.crt`
Certigna	Jun 29 15:13:05 2027 GMT	`Certigna.crt`
Certigna Root CA	Oct 1 08:32:27 2033 GMT	`Certigna_Root_CA.crt`
Certinomis - Root CA	Oct 21 09:17:18 2033 GMT	`Certinomis_-_Root_CA.crt`
Class 2 Primary CA	Jul 6 23:59:59 2019 GMT	`Certplus_Class_2_Primary_CA.crt`
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	`Certum_Trusted_Network_CA.crt`
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	`Certum_Trusted_Network_CA_2.crt`
Chambers of Commerce Root - 2008	Jul 31 12:29:50 2038 GMT	`Chambers_of_Commerce_Root_-_2008.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	`Class3PCA_G2_v2.pem)`
Class 4 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network	Aug 1 23:59:59 2028 GMT	`Class4PCA_G2_v2.pem)`
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_AAA_Services_root.crt`
Cybertrust Global Root	Dec 15 08:00:00 2021 GMT	`Cybertrust_Global_Root.crt`
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	`D-TRUST_Root_Class_3_CA_2_2009.crt`
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	`D-TRUST_Root_Class_3_CA_2_EV_2009.crt`
DST Root CA X3	Sep 30 14:01:15 2021 GMT	`DST_Root_CA_X3.crt`
Deutsche Telekom Root CA 2	Jul 9 23:59:00 2019 GMT	`Deutsche_Telekom_Root_CA_2.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCertGlobalRootCA.pem)`
DigiCert Global Root CA	Mar 8 12:00:00 2023 GMT	`DigiCertSHA2SecureServerCA.pem)`
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Assured_ID_Root_CA.crt`
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G2.crt`
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Global_Root_CA.crt`
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G2.crt`
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G3.crt`
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_High_Assurance_EV_Root_CA.crt`
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	`DigiCert_Trusted_Root_G4.crt`
E-Tugra Certification Authority	Mar 3 12:09:48 2023 GMT	`E-Tugra_Certification_Authority.crt`
EC-ACC	Jan 7 22:59:59 2031 GMT	`EC-ACC.crt`
EE Certification Centre Root CA	Dec 17 23:59:59 2030 GMT	`EE_Certification_Centre_Root_CA.crt`
Entrust.net[314] Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	`Entrust.net_Premium_2048_Secure_Server_CA.crt`
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	`Entrust_Root_Certification_Authority.crt`
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	`Entrust_Root_Certification_Authority_-_EC1.crt`
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	`Entrust_Root_Certification_Authority_-_G2.crt`
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	`GDCA_TrustAUTH_R5_ROOT.crt`

314. http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
GlobalSign	Dec 15 08:00:00 2021 GMT	`GSR2.pem)`
GTE CyberTrust Global Root	Aug 13 23:59:00 2018 GMT	`GTECTGlobalRoot.pem)`
GTS Root R1	Jun 22 00:00:00 2036 GMT	`GTS_Root_R1.crt`
GTS Root R2	Jun 22 00:00:00 2036 GMT	`GTS_Root_R2.crt`
GTS Root R3	Jun 22 00:00:00 2036 GMT	`GTS_Root_R3.crt`
GTS Root R4	Jun 22 00:00:00 2036 GMT	`GTS_Root_R4.crt`
GeoTrust Global CA	May 21 04:00:00 2022 GMT	`GeoTrust_Global_CA.crt`
GeoTrust Global CA	May 21 04:00:00 2022 GMT	`GeoTrust_Global_CA.pem)`
GeoTrust Primary Certification Authority	Jul 16 23:59:59 2036 GMT	`GeoTrust_Primary_Certification_Authority.crt`
GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	`GeoTrust_Primary_Certification_Authority_-_G2.crt`
GeoTrust Primary Certification Authority - G3	Dec 1 23:59:59 2037 GMT	`GeoTrust_Primary_Certification_Authority_-_G3.crt`
GeoTrust Universal CA	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA.crt`
GeoTrust Universal CA 2	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA_2.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R5.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	`GlobalSign_Root_CA.crt`
GlobalSign	Dec 15 08:00:00 2021 GMT	`GlobalSign_Root_CA_-_R2.crt`
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.crt`
GlobalSign	Dec 10 00:00:00 2034 GMT	`GlobalSign_Root_CA_-_R6.crt`
Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	`Global_Chambersign_Root_-_2008.crt`
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	`Go_Daddy_Class_2_CA.crt`
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Go_Daddy_Root_Certificate_Authority_-_G2.crt`
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	`Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt`
Hellenic Academic and Research Institutions RootCA 2011	Dec 1 13:49:52 2031 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt`
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt`
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	`Hongkong_Post_Root_CA_1.crt`
ISRG Root X1	Jun 4 11:04:38 2035 GMT	`ISRG_Root_X1.crt`
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	`IdenTrust_Commercial_Root_CA_1.crt`
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	`IdenTrust_Public_Sector_Root_CA_1.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	`Imprivata.crt`
Izenpe.com[315]	Dec 13 08:27:25 2037 GMT	`Izenpe.com`[316]`.crt`
LuxTrust Global Root 2	Mar 5 13:21:57 2035 GMT	`LuxTrust_Global_Root_2.crt`
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	`Microsec_e-Szigno_Root_CA_2009.crt`
NetLock Arany (Class Gold) Főtanúsítvány	Dec 6 15:08:21 2028 GMT	`NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt`
Network Solutions Certificate Authority	Dec 31 23:59:59 2029 GMT	`Network_Solutions_Certificate_Authority.crt`
OISTE WISeKey Global Root GA CA	Dec 11 16:09:51 2037 GMT	`OISTE_WISeKey_Global_Root_GA_CA.crt`
OISTE WISeKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	`OISTE_WISeKey_Global_Root_GB_CA.crt`
OISTE WISeKey Global Root GC CA	May 9 09:58:33 2042 GMT	`OISTE_WISeKey_Global_Root_GC_CA.crt`
Class 3 Public Primary Certification Authority	Aug 1 23:59:59 2028 GMT	`Pcs3ss_v4.pem)`
QuoVadis Root Certification Authority	Mar 17 18:33:33 2021 GMT	`QuoVadis_Root_CA.crt`
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	`QuoVadis_Root_CA_1_G3.crt`
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	`QuoVadis_Root_CA_2.crt`

315. http://Izenpe.com
316. http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	`QuoVadis_Root_CA_2_G3.crt`
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	`QuoVadis_Root_CA_3.crt`
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	`QuoVadis_Root_CA_3_G3.crt`
SSL.com[317] EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	`SSL.com_EV_Root_Certification_Authority_ECC.crt`
SSL.com[318] EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	`SSL.com_EV_Root_Certification_Authority_RSA_R2.crt`
SSL.com[319] Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	`SSL.com_Root_Certification_Authority_ECC.crt`
SSL.com[320] Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	`SSL.com_Root_Certification_Authority_RSA.crt`
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	`SZAFIR_ROOT_CA2.crt`
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	`SecureSign_RootCA11.crt`
SecureTrust CA	Dec 31 19:40:55 2029 GMT	`SecureTrust_CA.crt`
Secure Global CA	Dec 31 19:52:06 2029 GMT	`Secure_Global_CA.crt`
Security Communication RootCA2	May 29 05:00:39 2029 GMT	`Security_Communication_RootCA2.crt`
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	`Security_Communication_Root_CA.crt`

317. http://SSL.com
318. http://SSL.com
319. http://SSL.com
320. http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
Sonera Class2 CA	Apr 6 07:29:40 2021 GMT	`Sonera_Class_2_Root_CA.crt`
Staat der Nederlanden EV Root CA	Dec 8 11:10:28 2022 GMT	`Staat_der_Nederlanden_EV_Root_CA.crt`
Staat der Nederlanden Root CA - G2	Mar 25 11:03:10 2020 GMT	`Staat_der_Nederlanden_Root_CA_-_G2.crt`
Staat der Nederlanden Root CA - G3	Nov 13 23:00:00 2028 GMT	`Staat_der_Nederlanden_Root_CA_-_G3.crt`
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	`Starfield_Class_2_CA.crt`
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Root_Certificate_Authority_-_G2.crt`
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Services_Root_Certificate_Authority_-_G2.crt`
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	`SwissSign_Gold_CA_-_G2.crt`
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	`SwissSign_Silver_CA_-_G2.crt`
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_2.crt`
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_3.crt`
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	`TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt`
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	`TWCA_Global_Root_CA.crt`
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	`TWCA_Root_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Government Root Certification Authority	Dec 5 13:23:33 2032 GMT	`Taiwan_GRCA.crt`
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	`TeliaSonera_Root_CA_v1.crt`
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	`TrustCor_ECA-1.crt`
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	`TrustCor_RootCert_CA-1.crt`
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	`TrustCor_RootCert_CA-2.crt`
Trustis FPS Root CA	Jan 21 11:36:54 2024 GMT	`Trustis_FPS_Root_CA.crt`
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	`UCA_Extended_Validation_Root.crt`
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	`UCA_Global_G2_Root.crt`
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_ECC_Certification_Authority.crt`
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_RSA_Certification_Authority.crt`
VeriSign Class 3 Public Primary Certification Authority - G4	Jan 18 23:59:59 2038 GMT	`VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt`
VeriSign Class 3 Public Primary Certification Authority - G5	Jul 16 23:59:59 2036 GMT	`VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt`
VeriSign Universal Root Certification Authority	Dec 1 23:59:59 2037 GMT	`VeriSign_Universal_Root_Certification_Authority.crt`
VeriSign Class 3 Public Primary Certification Authority - G3	Jul 16 23:59:59 2036 GMT	`Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	`XRamp_Global_CA_Root.crt`
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	`certSIGN_ROOT_CA.crt`
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	`ePKI_Root_Certification_Authority.crt`
thawte Primary Root CA	Jul 16 23:59:59 2036 GMT	`thawte_Primary_Root_CA.crt`
thawte Primary Root CA - G2	Jan 18 23:59:59 2038 GMT	`thawte_Primary_Root_CA_-_G2.crt`
thawte Primary Root CA - G3	Dec 1 23:59:59 2037 GMT	`thawte_Primary_Root_CA_-_G3.crt`

Notes for Release 11.03.500

Software:	Version	11.03.500
Release Date:	2020-04-01	
Release Notes:	Version	RN-1103500-1
Last update:	2020-04-01	

- IGEL OS 11 (see page 3216)
- IGEL OS Creator (OSC) (see page 3235)

IGEL OS 11

- Supported Devices 11.03.500 (see page 3217)
- Component Versions 11.03.500 (see page 3218)
- General Information 11.03.500 (see page 3222)
- Security Fixes 11.03.500 (see page 3223)
- Known Issues 11.03.500 (see page 3224)
- New Features 11.03.500 (see page 3227)
- Resolved Issues 11.03.500 (see page 3231)

Supported Devices 11.03.500

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[321].

321. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.500

- **Clients**

Product	Version
Cisco JVDI Client	12.7.1
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Workspace App	18.10.0.11
Citrix Workspace App	19.10.0.15
Citrix Workspace App	19.12.0.19
deviceTRUST Citrix Channel	19.1.200.2
Crossmatch DP Citrix Channel	0515.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.6.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
IGEL WVD Client	1.0.5
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.44.0.11
Parallels Client (64 bit)	17.0.21474
Spice GTK (Red Hat Virtualization)	0.37-1igel62
Remote Viewer (Red Hat Virtualization)	8.0-1igel49

Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71
Teradici PCoIP Software Client	19.05.9-18.04
ThinLinc Client	4.10.1-6197
ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.5-1igel1583919770
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.3.0-15208949
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.8.5

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	7
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.7.77
PKCS#11 Library OpenSC	0.19.0-2igel35
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver Gemalto eToken	10.7.77

Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel11
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VAAPI ABI Version	0.40
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.7413

Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2875
Xorg X11 Server	1.20.5-1igel914
Xorg Xephyr	1.20.5-1igel914
CUPS printing daemon	2.1.3-4ubuntu0.10igel29
PrinterLogic	25.1.0.381
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.1-1igel222
WebKit2Gtk	2.26.2-1igel27
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1igel7
Mobile Device Access USB (gphoto)	2.5.23-2igel2
VPN OpenConnect	7.08-1
Scanner support	1.0.27-1
VirtualBox	6.0.14-dfsg-1igel33

General Information 11.03.500

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Security Fixes 11.03.500

Firefox

- Updated Mozilla Firefox to **68.6.0 ESR**.
- Fixes for **mfsa2020-09**, also known as:
  More...

  CVE-2020-6805, CVE-2020-6806, CVE-2020-6807, CVE-2020-6811, CVE-2019-20503, CVE-2020-6812, and CVE-2020-6814
- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as:
  More...

  CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024
- Fixes for **mfsa2019-37**, also known as:
  More...

  CVE-2019-17008, CVE-2019-11745, CVE-2019-17010, CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012

Base system

- Fixed **libxml2** security issues CVE-2020-7595 and CVE-2019-19956.
- Fixed **nss** security issues CVE-2019-17007, CVE-2019-17006, and CVE-2019-11745.
- Fixed **libvncserver** security issue CVE-2019-15681.
- Fixed **libexif** security issues CVE-2019-9278, CVE-2017-7544, and CVE-2016-6328.
- Fixed **cyrus-sasl2** security issue CVE-2019-19906.
- Fixed **samba** security issues CVE-2019-14907, CVE-2019-14870, and CVE-2019-14861.
- Fixed **zulu** security issues:
  More...

  CVE-2020-2583, CVE-2020-2590, CVE-2020-2593,CVE-2020-2601, CVE-2020-2604, CVE-2020-2659, and CVE-2020-2654

Known Issues 11.03.500

Firmware Update

- On **devices with 2 GB of flash storage**, it could happen that there is **too little space for updating all features**. In this case, a corresponding error message occurs and **unused features** must be **disabled** in IGEL Setup **under System > Firmware Customization > Features** to perform the firmware update.

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.10x to 11.03.500, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off Hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

  As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC got the new setting, **reboot** and **set** the `mimetypes_template` registry key **back to "Standard"**.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin, the following registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`

Value	enabled / disabled

This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- Using **CWA 19.x** sometimes **freezes the session** while session logoff from a published desktop. Workaround: **Use CWA 18.10.0**.

VMware Horizon

- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.
- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app, a new iconified window appears in the taskbar, and only if you click on it, the application will show up.
  On some hardware (UD7-H850, UD2-M250, UD2-D220), however, the client aborts when this new window is de-iconified.

Imprivata

- On **devices with 2 GB of flash storage**, it could happen that there is too little space to enable the **Imprivata partition after the update to 11.03.500**. In this case, a corresponding error message occurs and **unused features must be disabled** (in IGEL Setup under **System > Firmware Customization > Features**). Imprivata has to be (re-)enabled after a reboot then.

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- In seldom cases, the **authentication** hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Hyper-V

- **Hyper-V** (Generation 2) needs **a lot of memory**. The machine needs a sufficient amount of memory allocated.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non-working graphic.
  Workaround: Install with 'Failsafe Installation + Recovery' and set the registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Audio

- **Audio jack detection on Advantech POC-W243L doesn't work**. Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occurs, the registry key `x.drivers.kms.best_console_mode` has to be set to **disabled**.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

Remote Management

- **AIT feature with IGEL Starter License** is **supported** by the next **UMS version 6.05.100**.

New Features 11.03.500

Citrix

- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.
    More...

Parameter	Show Citrix Desktop Viewer screen
Registry	`ica.module.cdviewerscreen`
Value	off / on

  - Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].
    More...

Parameter	Use Chromium Embedded Framework (CEF)
Registry	`ica.allregions.usecefbrowser`
Value	factory default is "*" / false / true

  - "factory default" impact can be set by config file.
  - Changed default:
    More...

Parameter	VDTUI protocol
Registry	`ica.module.virtualdriver.vdtui.enable`
Value	off / on

WVD

- Integrated IGEL **WVD Client**.

VMware Horizon

- Updated **VMware Horizon Client** to version **5.3.0**.

ThinLinc

- Updated **ThinLinc Client** to version **4.11.0**.

Smartcard

- Updated **Gemalto / Safenet smartcard middleware** to version **10.7.7**.
- Added **support for** smartcard reader **HP Business Slim Smartcard CCID Keyboard**.

- Added **configuration parameter to disable PIN pad functionality of smartcard readers**, driven by Open Source CCID driver. This might work to solve problems with PIN pads, but lowers security level.
More...

Parameter	Disable PIN pad
Registry	`scard.pcscd.ccid.disable_pinpad`
Value	disabled / enabled

- Added possibility to **add custom CCID smartcard readers to Open Source CCID driver**. Readers can be specified by USB Vendor, Product Id, and custom name:
More...

Parameter	USB Vendor Id
Registry	`scard.pcscd.ccid.custom_reader<num>.vid`
Value	
Parameter	USB Product Id
Registry	`scard.pcscd.ccid.custom_reader<num>.pid`
Value	
Parameter	Reader name
Registry	`scard.pcscd.ccid.custom_reader<num>.name`
Value	

- Updated **Athena IDProtect library** to version **7**. This version **supports CRYPTAS TicTok V3 cards**. Known issue: The **detection of locked PIN does not work**.

CUPS Printing

- Added **CUPS Printer port "USB class printer"**. The USB printer is assigned, in this case, by **matching patterns of USB Manufacturer** and **Product name strings**. In this way, a single printer definition could work for a class of different USB printer models.
More...

IGEL Setup	**Devices > Printer > CUPS > Printers**
Parameter	Printer port
Registry	`print.cups.printer<num>.backend`
Value	USB class printer
IGEL Setup	**Devices > Printer > CUPS > Printers**

Parameter	Pattern matching mode
Registry	`print.cups.printer<num>.usbclass_mode`
Value	pattern / pattern, case insensitive / regular expression
IGEL Setup	**Devices > Printer > CUPS > Printers**
Parameter	Manufacturer pattern
Registry	`print.cups.printer<num>.usbclass_manufacturer`
IGEL Setup	**Devices > Printer > CUPS > Printers**
Parameter	Product pattern
Registry	`print.cups.printer<num>.product`

- Updated **PrinterLogic Printer-Installer-Client** to version **25.1.0.381**. Fixed tray icon functionality.

Cisco JVDI Client

- Integrated **Cisco JVDI 12.7.1 client**. Cisco JVDI 12.7.0 has been removed.

Base system

- Added **Starter License functionality**.
  This license is now part of every new IGEL OS installation and is **valid for 30 days**. The license will be activated with the first boot after the initial installation. More and detailed information via https://wiki.test.toolchain.igel.kreuzwerker.net/licensing.
- Added '**Licensing**' tool to '**System**' in **local Start menu**. Disable the tool by key:
  More...

IGEL Setup	**Accessories > License Browser**
Parameter	Start Menu's System tab
Registry	`sessions.license_browser0.startmenu_system`
Value	enabled / disabled

  If there is only the Starter License and no UMS connection, the **Licensing tool is shown on the desktop by default**.
- Added feature **Custom Partition** to **Workspace Edition license**.
- Updated **Fluendo multimedia codecs** to the following versions: **gst-fluendo-vadec - 30/01/2020 0.10.212**.
- **Kerberos Logon**:
  You can now **turn on/off numlock** and/or **capslock** for password input. Registry keys:
  More...

Parameter	Handling of numlock

Registry	`sessions.xlock0.options.numlock_approach`
Value	don't change / set on / set off
Note	"set on": force numlock on when password is entered "set off": force numlock off when password is entered
Parameter	Handling of capslock
Registry	`sessions.xlock0.options.capslock_approach`
Value	don't change / set on / set off
Note	"set on": force capslock on when password is entered "set off": force capslock off when password is entered

- Added configuration for special **thinkpad keyboard model**:
  More...

IGEL Setup	**User Interface > Input > Keyboard**
Parameter	Keyboard type
Registry	`userinterface.keyboard.type`
Range	[Default] [Standard PC Keyboard (105 Keys)] [IBM Keyboard (122 Keys)] [Trimodal Keyboard] [Sun Type 6 Keyboard] [Chromebook] [Macbook] [Macbook international] [Thinkpad]

Wi-Fi

- Added **driver for Realtek 8822ce** and **8822be** Wi-Fi hardware.
- Added driver for **Realtek 8821cu** Wi-Fi hardware.

Driver

- Updated **Crossmatch DP driver for fingerprint**. The new version allows the **fingerprint image** to be **sent via the Citrix channel**. With this change, customers will be able to develop their own SW using the Crossmatch DP SDK.

Misc

- Updated **Login PI 3.6** to the new **Login Enterprise 4.0**.

Resolved Issues 11.03.500

Citrix

- Fixed **video playback on BBC websites** redirected via Citrix Browser Content Redirection.
- Fixed **Multimedia redirection** and **HDX RealTime Media Engine** may used concurrently.

OSC Installer

- Fixed issue with **failed partitioning**.

RDP/IGEL RDP Client 2

- Added a new parameter to control **audio latency** (in milliseconds) which **defines the amount of buffered audio data in the RDP client**.
  More...

Registry	`rdp.winconnect.sound-latency`
Value	125 (msec)

WVD

- Improved overall sound quality.
- Fixed issue caused **audio redirection to fail randomly**.
- **Clipboard redirection has potential privacy and security risks** and is therefore disabled by default.
- Fixed **dead key support** (key composition).
- Fixed **sound getting choppy** after a while.
- Several **bugfixes** for all kind of **stability issues**.

VMware Horizon

- Fixed: **Save VMWare Horizon user from last login** when **in appliance mode**.
  Reduced the options for "**Preset login information**" to either "**from last login**" or "**from session setup**". The redundant option "from appliance mode" **is removed** because the appliance mode is also treated as a session.
  More...

IGEL Setup	**Sessions > Horizon Client > Horizon Client Global > Local Logon**
Parameter	Preset login information
Registry	`vmware.login.saveusertype`
Range	[Set user/domain from last login] [Set user/domain from session setup]

- Fixed **Skype for Business** integration.

Firefox

- Fixed **switching off** firmware feature **PrinterLogic removes browser policies file**.
- Fixed **hiding the URL input** results in **disappearing web content**.

- Fixed **browser startscript** which was waiting for a new window even when browser was not configured to open an extra one.

Network

- Use **e1000e driver out-of-the-kernel as default** instead of the third-party driver.

Wi-Fi

- Fixed **connection problems by updating the regulatory domain database**.
- Improved **persistence of Wi-Fi switch state** across reboots.
- Fixed problems with **Wi-Fi backports driver** and older **Wi-Fi adapters** or **adapters with external kernel drivers**.

Open VPN

- Fixed **timing in OpenVPN credential dialogs** to prevent **focus loss** when started too early at system boot.
- Fixed **session management** where **VPN connections could get stuck when wrong passwords** were entered with no possibility of retry.

Imprivata

- Hide the **Imprivata session templates on the desktop** as this is misleading.

Smartcard

- Fixed smartcard reader **VASCO/OneSpan Digipass 905**. **Disabled USB auto suspend** for all smart card readers.
- Added **parameter to control the used smartcard protocol** when connecting with raw and other protocols allowed. Enable to read smartcards using **NHS Identity Agent**.
  More...

Parameter	Avoid raw protocol
Registry	`scard.pcscd.avoid_raw_protocol`
Value	false / true

- Fixed use of **IDPrime smartcards inside sessions** with readers driven by **Open Source CCID** smartcard reader driver: implemented attribute `SCARD_ATTR_CHANNEL_ID`.
- Added parameter to **delay smartcard insertion events** (in milliseconds). This solves issues reading smartcards within the **Citrix Workspace App**. Issue occured when inserting the card after already started StoreFront login.
  More...

Parameter	Delay smart card insertion event time
Registry	`scard.pcscd.card_insert_event_delay`
Value	0

Base system

- Fixed **NTP sync problem** with some **Windows Timeservers**.
  New registry key:
  More...

Parameter	NTP max allowed distance
Tooltip	Set this to a larger value can help to synchronize with unreliable NTP servers
Registry	`system.time.ntp_max_distance`
Type	Integer
Value	16 (new default 16 seconds instead of 3 before)

- Added `_diag` **kernel modules** needed by **Stratusphere IPS**.
- Fixed **Next** button usage in **Setup Assistant** while r**egistering for an evaluation license**.
- Fixed issue with **mounting USB devices in** the **Licensing tool**.
- If used as a master image, the **image will expand itself to full size** (limited to 16 GiB) on flash. This is done only **on first boot** and never again.
- Possible **rollout of initial settings, certificates, or licenses placed on the first partition**. The necessary steps are:
  - Writing image to USB or Flash medium
  - Mount or simply access the 1. VFAT partition which is present (should be empty)
  - Copying the modified `setup.ini` and/or `**.lic` files to the 1st partition (no directories)
  - For copying certificates, a `ca-certs` directory must be created where the desired certificates can be inserted. These will be copied to the `/wfs/ca-certs` directory on first boot.
  - The USB/Flash medium can be copied several times as needed
  - With the initial boot, the device will reboot out of the splash screen (re-read changed partition table)
  - The settings, certificates and/or licenses will be deployed and also deleted from the 1st partition.

Firmware update

- Improve **download speed for SFTP update sources**.

Appliance Mode

- Fixed **RHEV/Spice appliance mode**.

X11 system

- Fixed **displays not being automatically set up on boot**.

Media Player (Parole)

- Fixed **handling of player latency** (stream buffering).

Hardware

- Fixed non-working **Prolific PL2303 USB-to-serial adapters**.

- Fixed non-working **keyboard and touchpad on Microsoft Surface 3 Laptop**.

IGEL Cloud Gateway

- Handle **UMS jobs** intended to be executed on the next boot. This feature requires **UMS 6.05.100 or later**.

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[322].

- Component Versions 11.03.500 (see page 3236)
- New Features 11.03.500 (see page 3238)
- Resolved Issues 11.03.500 (see page 3239)

322. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.500

- **Clients**

Product	Version
Zulu JRE	8.44.0.11

- **Smartcard**

Reader Driver MUSCLE CCID	1.4.31-1igel10
Resource Manager PC/SC Lite	1.8.23-1igel11

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel975
Input Driver Elographics	1.4.1-1build5igel633
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2875
Xorg X11 Server	1.20.5-1igel914

Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
WebKit2Gtk	2.24.2-0ubuntu0.19.04.1igel18
Python2	2.7.12
Python3	3.5.2

New Features 11.03.500

OSC Installer

- Added **Starter License** functionality.
  This license is now part of every new IGEL OS installation and is **valid for 30 days**. The license will be **activated with the first boot** after the initial installation. For more information, see https://wiki.test.toolchain.igel.kreuzwerker.net/licensing.

Resolved Issues 11.03.500

OSC Installer

- Fixed issue with **failed partitioning**.

Notes for Release 11.03.110

Software:	Version	11.03.110
Release Date:	2020-01-15	
Release Notes:	Version	RN-1103110-1
Last update:	2020-01-16	

- IGEL OS 11 (see page 3241)
- IGEL OS Creator (OSC) (see page 3254)

IGEL OS 11

See here the list of contained CA certificates:

- Supported Devices 11.03.110 (see page 3242)
- Component Versions 11.03.110 (see page 3243)
- General Information 11.03.110 (see page 3247)
- Known Issues 11.03.110 (see page 3248)
- Security Fixes 11.03.110 (see page 3251)
- New Features 11.03.110 (see page 3252)
- Resolved Issues 11.03.110 (see page 3253)

Supported Devices 11.03.110

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[323].

323. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.110

- **Clients**

Product	Version
Cisco JVDI Client	12.7.0
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Workspace App	18.10.0.11
Citrix Workspace App	19.10.0.15
Citrix Workspace App	19.12.0.19
deviceTRUST Citrix Channel	19.1.200.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.4.1
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64 Qualification in progress
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.42.0.23
Parallels Client (64 bit)	17.0.21474
Spice GTK (Red Hat Virtualization)	0.37-1igel62
Remote Viewer (Red Hat Virtualization)	8.0-1igel49
Usbredir (Red Hat Virtualization)	0.8.0-1+b1igel71

Teradici PCoIP Software Client	19.05.9-18.04
ThinLinc Client	4.10.1-6197
ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel18
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.2.0-14604769
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.8.5

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library OpenSC	0.19.0-2igel35
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3

Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel6
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel9
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VAAPI ABI Version	0.40
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.1-1ubuntu1igel866

Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2872
Xorg X11 Server	1.20.5-1igel914
Xorg Xephyr	1.20.5-1igel914
CUPS printing daemon	2.1.3-4ubuntu0.10igel29
PrinterLogic	25.1.0.303
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.1-1igel222
WebKit2Gtk	2.26.2-1igel27
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20181030.92c5462-1igel5
Mobile Device Access USB (gphoto)	2.5.23-2igel2
VPN OpenConnect	7.08-1
Scanner support / Sane	1.0.27-1
VirtualBox	6.0.14-dfsg-1igel33

General Information 11.03.110

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.03.110

Firefox

- **Firefox IGEL extensions are not updated automatically** under some circumstances. After an update from 11.03.10x to 11.03.110, the IGEL extensions will stay on the old version.
  In this case, the following settings concerning **kiosk mode** cannot be executed:
  - Switch off Hotkey for new window/tab
  - Blocking of internal browser pages like preferences, file picker, specific local directories

As a workaround:

- a **reset to defaults** should be performed
- or the **browser's mimetype template** can be switched **from "Standard" to "Minimal"** by registry key `browserglobal.app.mimetypes_template`. There, the browser profile is renewed as well.
  After the TC got the new setting, **reboot** and **set** the `mimetypes_template` registry key **back to "Standard"**.

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work if server policy **Optimize for 3D graphics workload** is enabled together with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin a registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Multimedia redirection** isn't working if "HDX RealTime Media Engine" is enabled at the same time.
  Workaround: Switch off **HDX RealTime Media Engine**.

More...

IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia** **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**
Parameter	HDX RealTime Media Engine
Registry	`ica.module.virtualdriver.hdxrtme.enable`
Value	enabled / disabled

- With Citrix **Workspace App 19.10.0** or **19.8.0** the session sometimes freezes while session logoff from a published desktop:
  Workaround: Use **CWA 18.10.0**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Citrix Client Selection**
Parameter	Citrix client version
Registry	`ica.activeversion`
Range	Default (19.10.0) / 18.10.0 / 19.8.0 / 19.10.0

VMware Horizon

- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app a new iconified window appears in the taskbar and only if you click on it the application will show up.
- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

Wi-Fi

- TP-Link Archer T2UH Wi-Fi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- In seldom cases the **authentication** hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Audio

- **Audio jack detection on Advantech POC-W243L doesn't work**. Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non working graphic.
  Workaround: Install with 'Failsafe Installation + Recovery' and set registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occors, the registry `key` `x.drivers.kms.best_console_mode` has to be set to disabled.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

Security Fixes 11.03.110

Firefox

- Updated Mozilla Firefox to **68.4.1esr**.
- Fix for **mfsa2020-03**, also known as CVE-2019-17026.
- Fixes for **mfsa2020-02**, also known as: CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, and CVE-2019-17024.
- Fixes for **mfsa2019-37**, also known as:
  More...

  CVE-2019-17008, CVE-2019-11745, CVE-2019-17010,
  CVE-2019-17005, CVE-2019-17011, and CVE-2019-17012.

New Features 11.03.110

Citrix

- Integrated **Citrix Workspace App 19.12**
- Available **Citrix Workspace Apps** in this release: **19.12** (default), **19.10**, and **18.10**
- New **registry keys**:
  - Added a registry key for enabling **full-screen banner "Citrix Desktop Viewer"** when starting a Desktop or Application session.
    More...

Parameter	Show Citrix Desktop Viewer screen
Registry	`ica.module.cdviewerscreen`
Value	off / on

  - Added a registry key to enable usage of **Chromium Embedded Framework (CEF) for Browser Content Redirection (BCR)** [Experimental].
    More...

Parameter	Use Chromium Embedded Framework (CEF)
Registry	`ica.allregions.usecefbrowser`
Value	factory default / false / true

  - "factory default" means that can be set by config file.
  - Changed default:
    More...

Parameter	VDTUI protocol
Registry	`ica.module.virtualdriver.vdtui.enable`
Value	off / on

Resolved Issues 11.03.110

OSC Installer

- Fixed deployment of IGEL OS with **IGEL Deployment Appliance**.

Firefox

- Fixed **possibility to remove the browser's navigation bar**. In 11.03.100, the whole browser content was invisible without the navigation bar.

Wi-Fi

- Fixed **support for** some **newer Wi-Fi chipsets**.
- Fixed **Wi-Fi backport driver** instability problems with updating them to **5.4-rc8-1**.

Imprivata

- Fixed **race condition** that may lead to unexpected behavior with RDP connections.
- Fixed **VMware Horizon session disconnect**.

Smartcard

- Fixed bug in **smartcard transaction locking**.

Cisco JVDI Client

- The **Cisco EULA** must be accepted together with the IGEL EULA before installing IGEL OS and also within IGEL Setup Assistant when requesting an IGEL OS demo license.

Base system

- Fixed potential **temporary settings loss when resuming from standby**.

RDP/IGEL RDP Client 2

- Fixed **Fabulatech Scanner Redirection** not working for **RDP Remote Apps**.

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[324].

- Component Versions 11.03.110 (see page 3255)
- Resolved Issues 11.03.110 (see page 3257)

324. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.110

- **Clients**

Product	Version
Zulu JRE	8.42.0.23

- **Smartcard**

Reader Driver MUSCLE CCID	1.4.31-1igel6
Resource Manager PC/SC Lite	1.8.23-1igel9

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
Bluetooth Stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2872
Xorg X11 Server	1.20.5-1igel914

Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
WebKit2Gtk	2.26.2-1igel27
Python2	2.7.12
Python3	3.5.2

Resolved Issues 11.03.110

OSC Installer

- Fixed deployment of **IGEL OS with IGEL Deployment Appliance**.

Notes for Release 11.03.100

Software:	Version	11.03.100
Release Date:	2019-12-10	
Release Notes:	Version	RN-1103100-1
Last update:	2019-12-06	

- IGEL OS 11 (see page 3259)
- IGEL OS Creator (OSC) (see page 3295)

IGEL OS 11

See here the list of contained CA certificates:

- Supported Devices 11.03.100 (see page 3260)
- Component Versions 11.03.100 (see page 3261)
- General Information 11.03.100 (see page 3265)
- Security Fixes 11.03.100 (see page 3266)
- Known Issues 11.03.100 (see page 3269)
- New Features 11.03.100 (see page 3272)
- Resolved Issues 11.03.100 (see page 3281)
- CA Certificates Contained in IGEL OS 11.03 (see page 3284)

Supported Devices 11.03.100

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[325].

325. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.100

- **Clients**

Product	Version
Cisco JVDI Client	12.7.0
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Workspace App	18.10.0.11
Citrix Workspace App	19.10.0.15
Citrix Workspace App	19.8.0.20
deviceTRUST Citrix Channel	19.1.200.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	68.2.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.42.0.23
Parallels Client (64 bit)	17.0.21474
Spice GTK (Red Hat Virtualization)	0.37-1igel62
Remote Viewer (Red Hat Virtualization)	8.0-1igel49
Usbredir (Red Hat Virtualization)	0.8.0-1igel49
Teradici PCoIP Software Client	19.05.9-18.04

ThinLinc Client	4.10.1-6197
ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel18
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.2.0-14604769
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.8.5

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library OpenSC	0.19.0-2igel35
PKCS#11 Library SecMaker NetID	6.8.1.31
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35

Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.31-1igel6
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel8
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VAAPI ABI Version	0.40
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635

Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2872
Xorg X11 Server	1.20.5-1igel914
Xorg Xephyr	1.20.5-1igel914
CUPS printing daemon	2.1.3-4ubuntu0.10igel29
PrinterLogic	25.1.0.303
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.1-1igel222
WebKit2Gtk	2.26.2-1igel27
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20181030.92c5462-1igel5
Mobile Device Access USB (gphoto)	2.5.23-2igel2
VPN OpenConnect	7.08-1
Scanner support / Sane	1.0.27-1
VirtualBox	6.0.14-dfsg-1igel33

General Information 11.03.100

Firmware downgrade to older versions (11.01 or 11.02) is not possible, due to the unsigned firmware update files.

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Security Fixes 11.03.100

Firefox

- Updated Mozilla Firefox to **68.2.0esr**
  - Fixes for **mfsa2019-33**.
    More...

    CVE-2019-15903, CVE-2019-11757, CVE-2019-11758, CVE-2019-11759, CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763, CVE-2019-11764.
  - Fixes for **mfsa2019-26**.
    More...

    CVE-2019-11746, CVE-2019-11744, CVE-2019-11742, CVE-2019-11752, CVE-2019-9812, CVE-2019-11743, CVE-2019-11748, CVE-2019-11749, CVE-2019-11750, CVE-2019-11738, CVE-2019-11747, CVE-2019-11735, CVE-2019-11740.

Base system

- Added **cryptographic signatures** to OS 11 firmware files to prevent reading from corrupt images or disks.
  - Updates to firmwares without valid signatures are blocked.
  - When a signature error on the system partition is detected, the system is halted immediately. For system recovery a reinstallation via the OS Creator tool (OSC) is required. A signature error during early boot is signalized by a beep sequence.
  - When a signature error in another partition is detected the partition is removed and a firmware update is triggered to reinstall the corrupt partition.
  - Added user visible notification about partition signature errors.
- Fixed **admin logout from rescue shell** after suspend.
- Fixed security issue **CVE-2019-15902** in **4.19.x kernel**.
- Updated **Intel microcodes** to version **20191115** to fix various security issues (CVE-2019-11135, CVE-2019-0117 and CVE-2019-11139).
- Fixed **cups** security issues CVE-2019-8696, CVE-2019-8675 and CVE-2019-86.
- Fixed **openjpeg2** security issues CVE-2018-6616, CVE-2018-5785, CVE-2018-18088, CVE-2018-14423 and CVE-2017-17480.
- Fixed **xorg-server** security issue CVE-2018-14665.
- Fixed **expat** security issue CVE-2019-15903.
- Fixed **freetype** security issue CVE-2015-9383.
- Fixed **ghostscript** security issues.
  More...

  CVE-2019-14817, CVE-2019-14813, CVE-2019-14812, CVE-2019-14811, CVE-2019-10216 and CVE-2019-14869.
- Fixed **python2.7** security issues.

More...

CVE-2019-9948, CVE-2019-9947, CVE-2019-9740, CVE-2019-9636,

CVE-2019-5010, CVE-2019-10160 , CVE-2018-20852, CVE-2019-16935 and CVE-2019-16056.

- Fixed **python3.5** security issues.
  More...

  CVE-2019-9948, CVE-2019-9947, CVE-2019-9740, CVE-2019-9636,

  CVE-2019-5010, CVE-2019-10160, CVE-2018-20852, CVE-2018-20406, CVE-2019-16935 and CVE-2019-16056.
- Fixed **giflib** security issues CVE-2019-15133 and CVE-2018-11490.
- Fixed **libvirt** security issues.
  More...

  CVE-2019-3886, CVE-2019-11091, CVE-2019-10168, CVE-2019-10167,

  CVE-2019-10166, CVE-2019-10161, CVE-2019-10132, CVE-2018-6764,

  CVE-2018-5748, CVE-2018-12130, CVE-2018-12127, CVE-2018-12126,

  CVE-2018-1064, CVE-2017-2635, CVE-2017-1000256 and CVE-2016-5008.
- Fixed **e2fsprogs** security issue CVE-2019-5094.
- Fixed **rpcbind** security issues CVE-2017-8779 and CVE-2015-7236.
- Fixed **wpa** security issues CVE-2019-16275 and CVE-2019-13377.
- Fixed **tiff** security issues CVE-2019-17546 and CVE-2019-14973.
- Fixed **aspell** security issue CVE-2019-17544.
- Fixed **libsdl1.2** security issues.
  More...

  CVE-2019-7638, CVE-2019-7637, CVE-2019-7636,

  CVE-2019-7635, CVE-2019-7578, CVE-2019-7577,

  CVE-2019-7576, CVE-2019-7575, CVE-2019-7574,

  CVE-2019-7573, CVE-2019-7572 and CVE-2019-13616.
- Fixed **libsoup2.4** security issues CVE-2019-17266, CVE-2018-12910 and CVE-2017-2885.
- Fixed **rtlwifi driver** security issue CVE-2019-17666 .
- Fixed **libxslt** security issues CVE-2019-18197, CVE-2019-13118 and CVE-2019-13117.
- Fixed **opus** security issue CVE-2017-0381.
- Fixed **curl** security issues CVE-2019-5482 and CVE-2019-5481.
- Fixed **libidn2** security issues CVE-2019-18224 and CVE-2019-12290.
- Fixed **libarchive** security issue CVE-2019-18408.
- Fixed **samba** security issues CVE-2019-14847 and CVE-2019-10218.
- Fixed **file** security issue CVE-2019-18218.
- Fixed **imagemagick** security issues.
  More...

  CVE-2019-16713, CVE-2019-16711, CVE-2019-16710, CVE-2019-16709,

  CVE-2019-16708, CVE-2019-15140, CVE-2019-15139,

  CVE-2019-14981, CVE-2019-13454, CVE-2019-13391,

CVE-2019-13311, CVE-2019-13310, CVE-2019-13309, CVE-2019-13307,

CVE-2019-13306, CVE-2019-13305, CVE-2019-13304, CVE-2019-13301,

CVE-2019-13300, CVE-2019-13297, CVE-2019-13295, CVE-2019-13137,

CVE-2019-13135, CVE-2019-12979, CVE-2019-12978, CVE-2019-12977,

CVE-2019-12976, CVE-2019-12975 and CVE-2019-12974.

- Fixed **libjpeg-turbo** security issues CVE-2019-2201, CVE-2018-20330 and CVE-2018-19664.
- Fixed **python-ecdsa** security issues CVE-2019-14859, CVE-2019-14853 and CVE-2019-1485.
- Restricted access to **journalctl log** file for root only.
- Limit list of allowed **TLS ciphers** according to the Germany BSI recommendation (TR-0210202 Version 2019-01). The functionality is controlled by a parameter.
  More...

Registry	`system.security.remote_management.tls_policy`
Value	Default / BSI

The limited cipher list is applied on TLS (SSL) connections in:

- IGEL RM Agent
- Secure Shadowing
- Secure Terminal
- Firmware Update
- Custom Partition

Known Issues 11.03.100

Citrix

- With activated **DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H.264, MPEG1 and MPEG2**. GStreamer1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront login** with **Gemalto smartcard** middleware does not detect smartcard correctly if the card is inserted after start of login.
  Workaround: Insert the smartcard before starting the StoreFront login.
- **Citrix H.264 acceleration plugin** does not work if server policy **Optimize for 3D graphics workload** is enabled together with server policy **Use video codec compression > For the entire screen**.
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264** acceleration plugin a registry key must be enabled.
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

- **Multimedia redirection** isn't working if "HDX RealTime Media Engine" is enabled at the same time.
  Workaround: Switch off **HDX RealTime Media Engine**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia** **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business**
Parameter	HDX RealTime Media Engine
Registry	`ica.module.virtualdriver.hdxrtme.enable`
Value	enabled / disabled

- With Citrix **Workspace App 19.10.0 or 19.8.0** the session sometimes freezes while session logoff from a published desktop. :
  Workaround: Use **CWA 18.10.0**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Citrix Client Selection**
Parameter	Citrix client version
Registry	`ica.activeversion`
Range	Default (19.10.0) / 18.10.0 / 19.8.0 / 19.10.0

VMware Horizon

- **After disconnect of an RDP based session**, the Horizon main **window** which contains the server or sessions overview **cannot be resized anymore**.
- **Seamless application windows in Horizon Client may not be displayed correctly**. When starting the first seamless app a new iconified window appears in the taskbar and only if you click on it the application will show up.
- **Client drive mapping** and **USB redirection** for storage devices should not be enabled both at the same time.
  - On the one hand, when using USB redirection for storage devices: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using drive mapping instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore Horizon Client relies on the OS to mount the storage devices itself. Enable local `Storage Hotplug` on setup page **Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection do not appear in the **remote desktop**. Workaround: map the directory /media as a drive. Then the external devices will show up inside the media drive.

WiFi

- TP-Link Archer T2UH WiFi adapters does not work after system suspend/resume. Workaround: Disable system suspend at **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.

Smartcard

- In seldom cases the **authentication** hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: **spice-xpi firefox plugin** is no longer supported. The **Console Invocation** has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Audio

- **Audio jack detection on Advantec POC-W243L doesn't work**. Sound output goes through the headset connection and the internal speakers.
- **IGEL UD2 (D220)** fails to restore the volume level of the speaker when the device used **firmware version 11.01.110** before.

VirtualBox

- The current **VirtualBox Guest Tools/Drivers** will not work with **VirtualBox 5.2.x or older** hosts which leads to black screen and non working graphic.
  Workaround: Install with 'Failsafe Installation + Recovery' and set registry key `x.drivers.force_vesa` to true.
- When running in VirtualBox virtualization, **resizing the window will not automatically change desktop resolution** of IGEL OS guest.

Hardware

- **HP t730** could freeze when monitors with **different resolutions** are connected (1920x1200 + 2560x1440 + 3840x1600 for example). When this occors, the registry `key x.drivers.kms.best_console_mode` has to be set to disabled.
- Some newer **Delock 62599 active DisplayPort to DVI (4k)** adapters only work with INTEL devices.

New Features 11.03.100

Citrix

- Integrated **Citrix Workspace app 19.10**
- Available Citrix Workspace apps in this release: 19.10 (default), 19.08 and 18.10
- Added a registry key to enable **Transparent User Interface [TUI] Virtual Channel [VC]** protocol.
  More...

Parameter	Enable VDTUI protocol
Registry	`ica.module.virtualdriver.vdtui.enable`
Value	enabled / disabled

- Updated **libwebkit2gtk-4.0-37** to version **2.26.2**. It is now possible to **enable debug output for Citrix Browser Content Redirection** by running the script `/config/bin/install-webkit-debug`. The debug output is written to `/var/log/user/webcontainer.debug`.

  Only short sessions with enabled debug output can be tracked, due to the huge amount of debugging data which is written to the log file.

- Added support for **FabulaTech Scanner for Remote Desktop**.
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Fabulatech Scanner Redirection**
Parameter	Fabulatech Scanner for Remote Desktop
Registry	`ica.module.virtualdriver.fabulatech_scanner.enable`
Value	enabled / disabled

RDP/IGEL RDP Client 2

- Added support for **FabulaTech Scanner for Remote Desktop**.
  More...

IGEL Setup	**Sessions > RDP > RDP Global > Fabulatech Scanner Redirection**
Parameter	Fabulatech Scanner for Remote Desktop
Registry	`rdp.fabulatech_scanner.enable`
Value	enabled / disabled

VMware Horizon

- Updated Horizon Client to version **5.2.0-14604769**.

- Added **local scanner redirection** for VMWare Horizon Client.
  More...

Parameter	Scanner Redirection
Registry	`vmware.view.enable-scanner-redir`
Value	enabled / disabled

- Added support for **FabulaTech Scanner for Remote Desktop**.
  More...

IGEL Setup	**Sessions > Horizon Client > Horizon Client Global > Fabulatech Scanner Redirection**
Parameter	Fabulatech Scanner for Remote Desktop
Registry	`vmware.view.usb.enable-fabulatech-scanner`
Value	enabled / disabled

ThinLinc

- Updated ThinLinc Client to version **4.10.1**.

Parallels Client

- Updated Parallels Client to Version **17.0.1** .
  For using the FIPS 140-2 compliance mode no special handling is needed anymore.

Teradici PCoIP Client

- Updated Teradici PCoIP client to **19.05.9**.

Imprivata

- Added: When **available flash** is **bigger than 2GB**, 500 MB will be used for the Imprivata data partition.

Cisco JVDI Client

- Integrated new **Cisco Jabber Softphone for VDI** (Cisco JVDI Client) version 12.7 in 64bit.
  More...

IGEL Setup	**Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Unified Communications > Cisco Jabber**
Parameter	Cisco JVDI client
Registry	`ica.module.virtualdriver.vdcisco.enable`
Value	enabled / disabled
IGEL Setup	**Sessions > Horizon Client > Horizon Global > Unified Communications > Cisco Jabber**

Parameter	Cisco JVDI client
Registry	`vmware.view.vdcisco.enable`
Value	enabled / disabled

> Registry path for Common JVDI options: `multimedia.ciscovxme.**`

Logging

- Added **Elastic FIlebeat 7.3.0**. This is a lightweight way to forward and centralize logs and files. There are new registry keys to enable and configure **Elastic FIlebeat**.
  More...

IGEL Setup	**System > Firmware Customization > Features**
Parameter	Elastic Filebeat
Registry	`services.elastic_filebeat.enabled`
Value	enabled / disabled
Parameter	Use custom configuration
Registry	`network.filebeat.custom.enabled`
Value	enabled / disabled
Parameter	Custom Configuration
Registry	`network.filebeat.custom.config`
Value	filebeat.inputs: ...

Base system

- Added support for **exFAT filesystem**.
- Updated **Kernel to version 4.19.85** with **WiFi backport drivers 5.3.6.1**.
- Updated **Intel microcodes to version 20191115** to fix various security issues (CVE-2019-11135, CVE-2019-0117 and CVE-2019-11139).
- Updated **Xorg Xserver** from version 1.19.6 to **1.20.5**.
- Updated **Mesa OpenGL stack** from version 19.0.8 to **19.2.5**.
- Updated the **X11 video** and **input drivers** to their most current available versions.
- Added functionality to **enable or disable touchpad with a hotkey**.
  More...

IGEL Setup	**User Interface > Input > Touchpad**
Parameter	Enable Touchpad
Registry	`userinterface.touchpad.general.touchpadenable`

Value	enabled / disabled
IGEL Setup	**User Interface > Input > Touchpad**
Parameter	Hotkey
Registry	`userinterface.touchpad.general.usehotkey`
Value	enabled / disabled
IGEL Setup	**User Interface > Input > Touchpad**
Parameter	Modifiers
Registry	`userinterface.touchpad.general.hotkeymodifier`
IGEL Setup	**User Interface > Input > Touchpad**
Parameter	Hotkey
Registry	`userinterface.touchpad.general.hotkey`

- Added feature to **log into different files** and to **store log files on a persistent encrypted partition**.
More...

IGEL Setup	**System > Logging**
Parameter	Local logging
Registry	`system.syslog.enabled`
Value	enabled / disabled
IGEL Setup	**System > Logging**
Parameter	Use persistent log partition
Registry	`system.syslog.persistent`
Value	enabled / disabled
IGEL Setup	**System > Logging**
Parameter	Partition size in MB
Registry	`system.syslog.partsize`
Value	100

Create /var/log/auth.log:

Registry	system.syslog.sinks.auth
Value	enabled / disabled

Create /var/log/daemon.log:

Registry	system.syslog.sinks.daemon
Value	enabled / disabled

Create /var/log/kern.log:

Registry	system.syslog.sinks.kern
Value	enabled / disabled

Create /var/log/syslog:

Registry	system.syslog.sinks.syslog
Value	enabled / disabled

- Updated **Fluendo multimedia codecs** to the following versions:

  gst-fluendo-h264dec - 18/09/2019 0.10.54

  gst-fluendo-vadec - 16/10/2019 0.10.210

- Added **beep sequence** to signalize a **missing system partition** during early boot.

CUPS Printing

- Updated **Printer Installer** client to version **25.1.0.303**.
- Added missing **cups model names** for some printers.

Smartcard

- Updated **MUSCLE Open Source CCID** driver to version **1.4.31**. Added additional smartcard reader **Cherry SECURE BOARD**.
- Updated **SecMaker Net iD** smartcard library to version **6.8.1.31**. The changes are:
  - Support for **Gemalto IDPrime 940** and **3940**.
  - Support for new **VRK card** (IDEMIA IAS ECC, spec: FINEID S1 - FINEID S1 Electronic ID Application v4.0).
  - Support for **Aventra MyEID v4.0** (customer specific card profile with read support only).
  - Fixed problem with **detection of cards in Net iD Card Portal**.
  - Other fixes, see release notes at **SecMaker**[326].

WiFi

- Added **backports kernel drivers** with version **5.3.6-1** for better WiFi support.

326. https://service.secmaker.com/releasenotes/

- Disabled **backports drivers** for **Microsoft Surface** Laptop 3.
- Added new registry key to enable or disable the use of the **backport drivers** (reboot is needed).
  More...

Parameter	Use the newer backport drivers for WiFi
Registry	`network.drivers.use_backport_drivers`
Range	Default (normally use backport drivers) / False / True

- Added switch for more aggressively search of configured **hidden WiFi networks**.
  More...

Parameter	Force connection to hidden network
Registry	`network.interfaces.wirelesslan.device0.mssid_force_hidden`
Value	never / once / continuously

The default value **never** preserves the old behaviour.

Changing can be useful in situations where the system cannot detect any configured WiFi in the environment. If **once** is selected, the system will blindly try to connect to all configured hidden networks once (until the network as a whole gets started again). In the case of **continuously**, it will continue trying to connect to hidden networks.

Remarks: An access point found in this way will be remembered next time and its reconnecting will be faster. Search for hidden networks in the Wireless Manager is not affected.

Driver

- Updated **Philips Speech Driver** to version **12.8.5**.
- Added login with **BioSec BS Login Hand Vein Recognition** software. The parameters have to be set in IGEL Setup Registry.
  More...

Parameter	Login with Biosec BS Login
Registry	`auth.login.biosec_bslogin`
Value	enabled / disabled
Parameter	URL of LifePassServer
Registry	`auth.biosec.lifepassserverurl`
Value	localhost:10100
IGEL Setup	**System > Firmware Customization > Features**
Parameter	Biosec BS Login

Registry	`services.biosec_bslogin.enabled`
Value	enabled / disabled

- Added **Broadcom Tigon3** network driver.

X11 system

- Added support for secure keyboard input with **Cherry SECURE BOARD 1.0**.
  In secure mode all keyboard input devices are suppressed except pre-personalized Cherry SECURE BOARD 1.0 devices. For the encrypted communication certificates and keys in directories `/wfs/cherry/ca-certs` and `/wfs/cherry/client-certs` are required.
  More...

IGEL Setup	**User Interface > Input > Keyboard**
Parameter	Secure keyboard input with Cherry SECURE BOARD
Registry	`devices.cherry_secureboard.enable`
Value	enabled / disabled
Parameter	Debug messages for Cherry SECURE BOARD
Registry	`devices.cherry_secureboard.debug`
Value	enabled / disabled

- Added the possibility to configure the **screen brightness** with registry keys.
  More...

Parameter	Brightness value
Registry	`x.xserver0.brightness` `x.xserver0.screen[1-7].brightness`
Range	0.1 - 1.0 (darker) 1.0 - 3.0 (brighter)

- Added new registry keys to be able to configure some **modesetting graphics driver options** if needed.
  More...

Parameter	Use DRI3 PageFlip feature
Registry	`x.drivers.modesetting.use_page_flip`
Range	Default (normally use page flip feature) / disabled / enabled
Parameter	Use shadow framebuffer layer

Registry	`x.drivers.modesetting.use_shadow_fb`
Range	Default (normally use shadow framebuffer) / disabled / enabled
Parameter	Use double shadow framebuffer to improve VNC performance
Registry	`x.drivers.modesetting.use_double_shadow`
Range	disabled / enabled
Parameter	Use software cursor for modesetting driver
Registry	`x.drivers.modesetting.use_sw_cursor`
Range	Default (normally disabled)
Parameter	Choose acceleration method
Registry	`x.drivers.modesetting.accel_method`
Range	Default (normally Glamor is used) / Glamor / None
Parameter	Force usage of DRI3 regardless of x.drivers.use_dri3 setting
Registry	`x.drivers.modesetting.force_dri3`
Range	disabled / enabled

Misc

- Added support for **Stratusphere UX** from Liquidware.
  More...

IGEL Setup	**Accessories > Connector ID Key Software**
Parameter	Enable Stratusphere UX CID Key
Registry	`stratusphere_ux.cid_key_software.enable`
IGEL Setup	**Accessories > Connector ID Key Software**
Parameter	Stratusphere hub
Registry	`stratusphere_ux.cid_key_software.hub`
IGEL Setup	**Accessories > Connector ID Key Software**
Parameter	Stratusphere machine group
Registry	`stratusphere_ux.cid_key_software.machine_group`
IGEL Setup	**Accessories > Connector ID Key Software**

Parameter	Stratusphere user group
Registry	`stratusphere_ux.cid_key_software.user_group`

- Added the launcher of Login VSI's monitoring tool **Login PI** to the IGEL OS which can be configured from setup via parameters and started from the UMS.
  Besides of specifying the parameters given below, a SSL certificate must be provided and deployed via the UMS. This has to be obtained from the Login PI server manually. Given the parameters and the certificate, **the launcher can be started via job from the UMS**.
  More...

IGEL Setup	**Accessories > Login PI**
Parameter	Server URL
Registry	`debug.tools.login_pi.server_url`
IGEL Setup	**Accessories > Login PI**
Parameter	Secret
Registry	`debug.tools.login_pi.crypt_password`

Hardware

- Added recognition for **IGEL UD2 M250C** with **8 GB eMMC** with product id **UD2-LX 51**.
- Added support for **IGEL UD3 M350C** with product id **UD3-LX 60**.
- **UD7** with active **AMD Secure Processor** feature uses new product id **UD7-LX 11**.
- Improved support for **ADS-Tec VMT9000** devices:
  - Enable **rs-232 additional power supply** without restart.
  - Enable **external wifi antenna** without restart.
  - Enable **shutdown by ignition off**.
  - Enable **watchdog service**.
- Added hardware support for **LG CL600N**.
- Added hardware support for **LG CL600W**.
- Added new registry keys to be able to configure some **new i915 parameter**.
  More...

Parameter	Disable the use of limited color range for DisplayPort 1
Registry	`x.drivers.intel.dp1_no_limited_color_range`
Range	Default / disabled / enabled
Info: Only for M250C the use of limited color range for DP1 is disabled.	

- Added support for newer Prolific PL2303 USB serial adapters (used in UD3-LX 60).

Resolved Issues 11.03.100

Citrix

- Fixed **video playback** with enabled **Citrix Browser Content Redirection**.

RDP/IGEL RDP Client 2

- Fixed **RDP graphics issues** with **Windows 2008(R2)** Server (when RemoteFX is not enabled).
- Fixed **RDP Web Access Domain Visibility** not working correctly.
- Fixed **sound glitch** while using **PulseAudio** system. PulseAudio is now the default sound driver.

VMware Horizon

- Fixed **sound issue** in **Horizon client 5.x using PCoIP protocol**.

Firefox

- Fixed: **Homepage** cannot be set
- Fixed: **RTSP media stream** with enabled apparmor.

Network

- Fixed issue with configuration of more then one **NTP server**.
- Fixed network interface device order for **Dell Wyse 5070 Thin Client** so that the onboard interface always is the first one.

  When endpoint is updated from a previous firmware version, network interface device order might change

- Changed **minimal allowed MSS size to 750** to avoid problems with some VPN solutions.
- Added new registry keys to be able to configure the **minimal allowed TCP MSS size**.
  More...

Parameter	Minimal TCP send MSS size
Registry	`system.sysctl.tcp_min_snd_mss`
Range	750

Smartcard

- Fixed not working **90meter** in **Firefox** when apparmor is enabled.
- Fixed handling of smartcards in **pcsc-lite**: Improved transaction locking. A new parameter was introduced to control the new behavior (enabled by default).
  More...

Parameter	Abort stalled transactions
Registry	`scard.pcscd.abort_stalled_transactions`
Range	enabled / disabled

- Fixed **bug in smartcard transaction locking**.

- Fixed **IGEL Smartcard** to be able to handle **VoIP client Ekiga** sessions.
- Fixed **smartcard usernames displayed on login screen**: non-ASCII characters were not shown correctly before.
- Fixed **error message on login screen**, shown when smart card PIN is locked.

Base system

- Fixed **license handling**: Add-on licenses can be used on top of Workspace Edition evaluation licenses now.
- Fixed **warnings when evaluation license is about to expire**. In detail, removed warning when **Enterprise Management Pack** is about to expire and WE is already licensed.
- Fixed **ActiveDirectory/Kerberos password** change with **Change Password** accessory for users which are member of many (~300+) AD groups.
- Fixed **IGEL License retrieval via FTP protocol** in **IGEL Setup Assistant** and **Licenses Browser tool**.
- Fixed **bug in reboot message** where not all available translations were used.
- Fixed problems with **missing library** if using **OpenConnect** feature.
- Changed: **Bluetooth is off by default again**. It wiil be temporary enabled for auto pairing before the initial Setup Assistant runs. Only if a device is paired during this phase, Bluetooth is enabled afterwards. To enable Bluetooth support by configuration use this parameter:
  More...

IGEL Setup	**Devices > Bluetooth**
Parameter	Bluetooth
Registry	`devices.bluetooth.enable`
Value	enabled / disabled

- Fixed **license information** of Add-On licenses in category evaluation.
- Re-fixed broken **custom bootsplash** when doing a reset to factory defaults via UMS.

Custom Partition

- Automatic constrain of minimum size for **custom partition to 5MB**.

Firmware update

- **Automatic firmware update** is now checked after retrieval of UMS settings.
- If there are some not executed changes in the network configuration, these **changes are applied automatically** before performing firmware update.

Storage Devices

- Fixed bug: **udiskd mounted storage devices** on behalf of user processes (e.g. parole) even if Storage Hotplug was disabled in the setup.

X11 system

- Fixed issue with **Wacom Signing Pads** not being recognized as displays.
- Solved issues with certain **monitors** on **UD2 LX50**.
- Fixed **Multi-GPU NVIDIA** setups with **Display Switch**.
- Prevent configuration of **Display Switch** utility on unlicensed device.

- Fixed an issue with **modesetting driver** and **DisplayLink USB graphic adapters**.

X server

- Fixed **Xorg freezes** when usage of **modesetting driver** and **video acceleration**.

Shared Workplace

- Fixed broken **Shared Workplace** authentication when ICG is used.

Hardware

- Fixed **EFI freeze** problem **after bootcode update** on devices like the HP t630 and probably others too.
- Added: **Bluetooth tool shows now a message when no device is connected**.
- Fixed issue with **limited colors** on the **DisplayPort 1 of UD2-LX50**.

Remote Management

- Fixed **automatic registering** in the UMS using DNS entry or DHCP tag during initial rollout.

IGEL Cloud Gateway

- Fixed search for an available **buddy update server** when devices are managed over **ICG**.

VNC

- Fixed **sporadic connection failure** in VNC server.

CA Certificates Contained in IGEL OS 11.03

IGEL OS 11.03 contains the following CA certificates:

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	`ACCVRAIZ1.crt`
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	`AC_RAIZ_FNMT-RCM.crt`
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	`Actalis_Authentication_Root_CA.crt`
AddTrust External CA Root	May 30 10:48:38 2020 GMT	`AddTrust_External_Root.crt`
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	`AffirmTrust_Commercial.crt`
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	`AffirmTrust_Networking.crt`
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	`AffirmTrust_Premium.crt`
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	`AffirmTrust_Premium_ECC.crt`
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	`Amazon_Root_CA_1.crt`
Amazon Root CA 2	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_2.crt`
Amazon Root CA 3	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_3.crt`
Amazon Root CA 4	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_4.crt`
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	`Atos_TrustedRoot_2011.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`Baltimore_CyberTrust_Root.crt`
Buypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	`Buypass_Class_2_Root_CA.crt`
Buypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	`Buypass_Class_3_Root_CA.crt`
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	`CA_Disig_Root_R2.crt`
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	`CFCA_EV_ROOT.crt`
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	`COMODO_Certification_Authority.crt`
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_ECC_Certification_Authority.crt`
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`COMODO_RSA_Certification_Authority.crt`
Certigna	Jun 29 15:13:05 2027 GMT	`Certigna.crt`
Certigna Root CA	Oct 1 08:32:27 2033 GMT	`Certigna_Root_CA.crt`
Certinomis - Root CA	Oct 21 09:17:18 2033 GMT	`Certinomis_-_Root_CA.crt`
Class 2 Primary CA	Jul 6 23:59:59 2019 GMT	`Certplus_Class_2_Primary_CA.crt`
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	`Certum_Trusted_Network_CA.crt`
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	`Certum_Trusted_Network_CA_2.crt`
Chambers of Commerce Root - 2008	Jul 31 12:29:50 2038 GMT	`Chambers_of_Commerce_Root_-_2008.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_AAA_Services_root.crt`
Cybertrust Global Root	Dec 15 08:00:00 2021 GMT	`Cybertrust_Global_Root.crt`
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	`D-TRUST_Root_Class_3_CA_2_2009.crt`
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	`D-TRUST_Root_Class_3_CA_2_EV_2009.crt`
DST Root CA X3	Sep 30 14:01:15 2021 GMT	`DST_Root_CA_X3.crt`
Deutsche Telekom Root CA 2	Jul 9 23:59:00 2019 GMT	`Deutsche_Telekom_Root_CA_2.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCertGlobalRootCA.pem`
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Assured_ID_Root_CA.crt`
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G2.crt`
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G3.crt`
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Global_Root_CA.crt`
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G2.crt`
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G3.crt`
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_High_Assurance_EV_Root_CA.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	`DigiCert_Trusted_Root_G4.crt`
E-Tugra Certification Authority	Mar 3 12:09:48 2023 GMT	`E-Tugra_Certification_Authority.crt`
EC-ACC	Jan 7 22:59:59 2031 GMT	`EC-ACC.crt`
EE Certification Centre Root CA	Dec 17 23:59:59 2030 GMT	`EE_Certification_Centre_Root_CA.crt`
Entrust.net[327] Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	`Entrust.net_Premium_2048_Secure_Server_CA.crt`
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	`Entrust_Root_Certification_Authority.crt`
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	`Entrust_Root_Certification_Authority_-_EC1.crt`
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	`Entrust_Root_Certification_Authority_-_G2.crt`
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	`GDCA_TrustAUTH_R5_ROOT.crt`
GTS Root R1	Jun 22 00:00:00 2036 GMT	`GTS_Root_R1.crt`
GTS Root R2	Jun 22 00:00:00 2036 GMT	`GTS_Root_R2.crt`
GTS Root R3	Jun 22 00:00:00 2036 GMT	`GTS_Root_R3.crt`
GTS Root R4	Jun 22 00:00:00 2036 GMT	`GTS_Root_R4.crt`

327. http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
GeoTrust Global CA	May 21 04:00:00 2022 GMT	`GeoTrust_Global_CA.crt`
GeoTrust Primary Certification Authority	Jul 16 23:59:59 2036 GMT	`GeoTrust_Primary_Certification_Authority.crt`
GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	`GeoTrust_Primary_Certification_Authority_-_G2.crt`
GeoTrust Primary Certification Authority - G3	Dec 1 23:59:59 2037 GMT	`GeoTrust_Primary_Certification_Authority_-_G3.crt`
GeoTrust Universal CA	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA.crt`
GeoTrust Universal CA 2	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA_2.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R5.crt`
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	`GlobalSign_Root_CA.crt`
GlobalSign	Dec 15 08:00:00 2021 GMT	`GlobalSign_Root_CA_-_R2.crt`
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.crt`
GlobalSign	Dec 10 00:00:00 2034 GMT	`GlobalSign_Root_CA_-_R6.crt`
Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	`Global_Chambersign_Root_-_2008.crt`
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	`Go_Daddy_Class_2_CA.crt`
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Go_Daddy_Root_Certificate_Authority_-_G2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	`Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt`
Hellenic Academic and Research Institutions RootCA 2011	Dec 1 13:49:52 2031 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt`
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	`Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt`
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	`Hongkong_Post_Root_CA_1.crt`
ISRG Root X1	Jun 4 11:04:38 2035 GMT	`ISRG_Root_X1.crt`
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	`IdenTrust_Commercial_Root_CA_1.crt`
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	`IdenTrust_Public_Sector_Root_CA_1.crt`
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	`Imprivata.crt`
Izenpe.com[328]	Dec 13 08:27:25 2037 GMT	`Izenpe.com`[329]`.crt`
LuxTrust Global Root 2	Mar 5 13:21:57 2035 GMT	`LuxTrust_Global_Root_2.crt`
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	`Microsec_e-Szigno_Root_CA_2009.crt`
NetLock Arany (Class Gold) FÅ‘tanÃºsÃtvÃ¡ny	Dec 6 15:08:21 2028 GMT	`NetLock_Arany_=Class_Gold=_FÅ‘tanÃºsÃtvÃ¡ny.crt`

328. http://Izenpe.com
329. http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
Network Solutions Certificate Authority	Dec 31 23:59:59 2029 GMT	`Network_Solutions_Certificate_Authority.crt`
OISTE WISeKey Global Root GA CA	Dec 11 16:09:51 2037 GMT	`OISTE_WISeKey_Global_Root_GA_CA.crt`
OISTE WISeKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	`OISTE_WISeKey_Global_Root_GB_CA.crt`
OISTE WISeKey Global Root GC CA	May 9 09:58:33 2042 GMT	`OISTE_WISeKey_Global_Root_GC_CA.crt`
QuoVadis Root Certification Authority	Mar 17 18:33:33 2021 GMT	`QuoVadis_Root_CA.crt`
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	`QuoVadis_Root_CA_1_G3.crt`
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	`QuoVadis_Root_CA_2.crt`
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	`QuoVadis_Root_CA_2_G3.crt`
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	`QuoVadis_Root_CA_3.crt`
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	`QuoVadis_Root_CA_3_G3.crt`
SSL.com[330] EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	`SSL.com_EV_Root_Certification_Authority_ECC.crt`
SSL.com[331] EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	`SSL.com_EV_Root_Certification_Authority_RSA_R2.crt`
SSL.com[332] Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	`SSL.com_Root_Certification_Authority_ECC.crt`

330. http://SSL.com
331. http://SSL.com
332. http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
SSL.com[333] Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	`SSL.com_Root_Certification_Authority_RSA.crt`
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	`SZAFIR_ROOT_CA2.crt`
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	`SecureSign_RootCA11.crt`
SecureTrust CA	Dec 31 19:40:55 2029 GMT	`SecureTrust_CA.crt`
Secure Global CA	Dec 31 19:52:06 2029 GMT	`Secure_Global_CA.crt`
Security Communication RootCA2	May 29 05:00:39 2029 GMT	`Security_Communication_RootCA2.crt`
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	`Security_Communication_Root_CA.crt`
Sonera Class2 CA	Apr 6 07:29:40 2021 GMT	`Sonera_Class_2_Root_CA.crt`
Staat der Nederlanden EV Root CA	Dec 8 11:10:28 2022 GMT	`Staat_der_Nederlanden_EV_Root_CA.crt`
Staat der Nederlanden Root CA - G2	Mar 25 11:03:10 2020 GMT	`Staat_der_Nederlanden_Root_CA_-_G2.crt`
Staat der Nederlanden Root CA - G3	Nov 13 23:00:00 2028 GMT	`Staat_der_Nederlanden_Root_CA_-_G3.crt`
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	`Starfield_Class_2_CA.crt`
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Root_Certificate_Authority_-_G2.crt`

333. http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	`Starfield_Services_Root_Certificate_Authority_-_G2.crt`
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	`SwissSign_Gold_CA_-_G2.crt`
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	`SwissSign_Silver_CA_-_G2.crt`
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_2.crt`
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_3.crt`
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	`TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt`
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	`TWCA_Global_Root_CA.crt`
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	`TWCA_Root_Certification_Authority.crt`
Government Root Certification Authority	Dec 5 13:23:33 2032 GMT	`Taiwan_GRCA.crt`
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	`TeliaSonera_Root_CA_v1.crt`
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	`TrustCor_ECA-1.crt`
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	`TrustCor_RootCert_CA-1.crt`
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	`TrustCor_RootCert_CA-2.crt`
Trustis FPS Root CA	Jan 21 11:36:54 2024 GMT	`Trustis_FPS_Root_CA.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	`UCA_Extended_Validation_Root.crt`
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	`UCA_Global_G2_Root.crt`
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_ECC_Certification_Authority.crt`
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_RSA_Certification_Authority.crt`
VeriSign Class 3 Public Primary Certification Authority - G4	Jan 18 23:59:59 2038 GMT	`VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt`
VeriSign Class 3 Public Primary Certification Authority - G5	Jul 16 23:59:59 2036 GMT	`VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt`
VeriSign Universal Root Certification Authority	Dec 1 23:59:59 2037 GMT	`VeriSign_Universal_Root_Certification_Authority.crt`
VeriSign Class 3 Public Primary Certification Authority - G3	Jul 16 23:59:59 2036 GMT	`Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt`
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	`XRamp_Global_CA_Root.crt`
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	`certSIGN_ROOT_CA.crt`
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	`ePKI_Root_Certification_Authority.crt`
thawte Primary Root CA	Jul 16 23:59:59 2036 GMT	`thawte_Primary_Root_CA.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
thawte Primary Root CA - G2	Jan 18 23:59:59 2038 GMT	`thawte_Primary_Root_CA_-_G2.crt`
thawte Primary Root CA - G3	Dec 1 23:59:59 2037 GMT	`thawte_Primary_Root_CA_-_G3.crt`

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 51 UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 60 UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 11 UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[334].

- Component Versions 11.03.100 (see page 3296)
- New Features 11.03.100 (see page 3298)

334. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.03.100

- **Clients**

Product	Version
Zulu JRE	8.42.0.23

- **Smartcard**

Reader Driver MUSCLE CCID	1.4.31-1igel6
Resource Manager PC/SC Lite	1.8.23-1igel8

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
Bluetooth Stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.2.5-1igel93
VDPAU Library version	1.2-1igel911
Graphics Driver INTEL	2.99.917+git20191117-igel939
Graphics Driver ATI/RADEON	19.0.1-3igel936
Graphics Driver ATI/AMDGPU	19.0.1-5igel924
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build2-igel925
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.85 #mainline-lxos-r2872
Xorg X11 Server	1.20.5-1igel914

Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
WebKit2Gtk	2.26.2-1igel27
Python2	2.7.12
Python3	3.5.2

New Features 11.03.100

Hardware

- Added hardware support for **LG CL600N**.
- Added hardware support for **LG CL600W**.

Notes for Release 11.02.150

Software:	Version	11.02.150
Release Date:	2019-09-09	
Release Notes:	Version	RN-1102150-1
Last update:	2019-09-09	

- Supported Devices 11.02.150 (see page 3300)
- Component Versions 11.02.150 (see page 3301)
- General Information 11.02.150 (see page 3305)
- Security Fixes 11.02.150 (see page 3306)
- Known Issues 11.02.150 (see page 3310)
- New Features 11.02.150 (see page 3312)
- Resolved Issues 11.02.150 (see page 3313)

Supported Devices 11.02.150

IGEL devices:	
UD2-LX:	UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

For supported IGEL OS 11 third-party devices, see Devices Supported by IGEL OS 11[335].

335. https://wiki.test.toolchain.igel.kreuzwerker.net/os11-supported-hardware

Component Versions 11.02.150

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.6.0.60
deviceTRUST Citrix Channel	19.1.200.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.9.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.40.0.25
Parallels Client (64 bit)	17.0.21282
Spice GTK (Red Hat Virtualization)	0.36-1~git20190601igel61
Remote Viewer (Red Hat Virtualization)	8.0-1igel49
Usbredir (Red Hat Virtualization)	0.8.0-1igel49
Teradici PCoIP Software Client	19.05.5-18.04
ThinLinc Client	4.10.0-6068

ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel18
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.7.11

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.2.36
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24

Reader Driver MUSCLE CCID	1.4.30-1igel3
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.0.8-1igel73
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190724-igel907
Graphics Driver ATI/RADEON	19.0.1-2igel890
Graphics Driver ATI/AMDGPU	19.0.1-4igel894
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.65 #mainline-lxos-r2782

Xorg X11 Server	1.19.7-1igel913
Xorg Xephyr	1.19.7-1igel913
CUPS printing daemon	2.1.3-4ubuntu0.9igel27
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.0-1igel214
WebKit2Gtk	2.24.2-0ubuntu0.19.04.1igel18
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20181030.92c5462-1igel5
Mobile Device Access USB (gphoto)	2.5.22-3igel1
VPN OpenConnect	7.08-1
Scanner support / Sane	1.0.27-1
VirtualBox	6.0.10-dfsg-4igel31

- **Features with Limited Functionality**

Cisco JVDI Client	12.1.0

General Information 11.02.150

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Security Fixes 11.02.150

Firefox

- Updated **Firefox** browser to version **60.9.0 ESR**.
  Including Fixes from **Security Advisory 2019-27**:
  More...

  CVE-2019-11746, CVE-2019-11744, CVE-2019-11753, CVE-2019-11752, CVE-2019-9812, CVE-2019-11743, and CVE-2019-11740.
- Fixes for **mfsa2019-22**, also known as:
  More...

  CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.
- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.
- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.
- Fixes for **mfsa2019-08**, also known as:
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.
- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

Base system

- Fixed security issue **CVE-2019-15902** in **4.19.x kernel**.
- Set default **umask to 0077** for all non-root users.
- Remote users home is now **/home/ruser**.
- Fixed **policykit-1** security issue CVE-2019-6133.
- Fixed **tiff** security issues:
  More...

  CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:
  More...

  CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.
- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.

- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **poppler** security issues:
  More...

  CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293, CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019, CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.
- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:
  More...

  CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.
- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:
  More...

  CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.
- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and CVE-2014-9913.
- Fixed **curl** security issues:
  More...

  CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.
- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and CVE-2018-15518.
- Fixed **libssh2** security issues:
  More...

CVE-2019-3863, CVE-2019-3862, CVE-2019-3861,
CVE-2019-3860, CVE-2019-3859, CVE-2019-3858,
CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues:
  More...

  CVE-2019-7665, CVE-2019-7150, CVE-2019-7149,
  CVE-2018-18521, CVE-2018-18520, CVE-2018-18310,
  CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues:
  More...

  CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661,
  CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457,
  CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246,
  and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **glib2.0** security issue CVE-2019-12450.
- Fixed **openssl (1.1.x)** security issues:
  More...

  CVE-2019-1543, CVE-2018-0737, CVE-2018-0735,
  CVE-2018-0734, and CVE-2018-0732.

- Fixed **sqlite3** security issues:
  More...

  CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506,
  CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518,
  CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **systemd** security issues:
  More...

  CVE-2019-6454, CVE-2019-6454, CVE-2018-1049,
  CVE-2018-15686, and CVE-2019-3842.

- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **imagemagick** security issues:
  More...

  CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396,
  CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472,
  CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467,
  CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966,
  CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806,
  and CVE-2017-12805.

- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.

- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.
  Security fixes:
  More...

  CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.
- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

Known Issues 11.02.150

Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264**, **MPEG1** and **MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.
  As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compressin" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

VMware Horizon

- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.
    In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.
    It is also recommended to disable local **Storage Hotplug** under Setup **> Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.
    Furthermore, Horizon Client relies on the OS to mount the storage devicesitself. Enable local **Storage Hotplug** under Setup **>Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection **do not appear in the remote desktop**.
  Workaround: map the directory `/` media as a drive. Then the external devices will show up inside the media drive.

Wi-Fi

- **TP-Link Archer T2UH Wi-Fi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.

New Features 11.02.150

Hardware

- Improved support for **ADS-Tec VMT9000** devices:
  - Enable **rs-232 additional power supply** without restart.
  - Enable an **external Wi-Fi antenna** without restart.
  - Enable **shutdown by ignition off**.
- Added hardware support for **Dell WYSE 5020**.

Resolved Issues 11.02.150

DP/IGEL RDP Client 2

- Fixed **RDP graphics** issues with **Windows 2008(R2) Server** (when **RemoteFX** is not enabled).
- Fixed some smaller **graphical RDP issues** with **Windows 2012 R2** if using **Clearcodec**.

Network

- Changed **minimally allowed MSS size** to "**750**" to avoid problems with some VPN solutions.
- Added a new registry key to be able to configure the **minimally allowed TCP MSS size**.
  A new registry key:
  More...

Parameter	Minimal TCP send MSS size
Registry	`system.sysctl.tcp_min_snd_mss`
Type	Integer
Value	750
Tooltip	Minimal TCP send MSS size (configurable value in the area from 200 to 1450)

Hardware

- Fixed **EFI freeze** problem **after bootcode update on** devices like the **HP t630** and probably others too.
- Added support for newer **Prolific PL2303 USB serial adapters** (used in UD3 LX60).

Firefox

- Fixed: **Homepage cannot be set**.

X11 system

- Fixed **Multi-GPU NVIDIA** setups **with Display Switch**.
- Prevent configuration of **Display Switch** utility **on unlicensed devices**.
- Added **new registry keys** to be able **to configure some modesetting options** if needed.
  New registry keys:
  More...

Parameter	Use DRI3 PageFlip feature
Registry	`x.drivers.modesetting.use_page_flip`
Range	[Default] [False] [True]
Info	"Default" (normally use page flip feature)
Parameter	Use shadow framebuffer layer

Registry	`x.drivers.modesetting.use_shadow_fb`
Range	[Default] [False] [True]
Info	"Default" (normally use shadow framebuffer)
Parameter	Use double shadow framebuffer to improve VNC performance
Registry	`x.drivers.modesetting.use_double_shadow`
Range	[False] [True]
Parameter	Use software cursor for modesetting driver
Registry	`x.drivers.modesetting.use_sw_cursor`
Range	[Default] [False] [True]
Info	"Default" (normally false)
Parameter	Choose acceleration method
Registry	`x.drivers.modesetting.accel_method`
Range	[Default] [Glamor] [None]
Info	"Default" (normally Glamor is used)
Parameter	Force usage of DRI3 regardless of x.drivers.use_dri3 setting
Registry	`x.drivers.modesetting.force_dri3`
Type	Bool
Value	False

Notes for Release 11.02.130

Software:	Version	11.02.130
Release Date:	2019-08-23	
Release Notes:	Version	RN-1102130-1
Last update:	2019-08-23	

- Supported Devices 11.02.130 (see page 3316)
- Component Versions 11.02.130 (see page 3317)
- General Information 11.02.130 (see page 3321)
- Security Fixes 11.02.130 (see page 3322)
- Known Issues 11.02.130 (see page 3326)
- Resolved Issues 11.02.130 (see page 3328)

Supported Devices 11.02.130

IGEL devices:	
UD2-LX:	UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

For supported IGEL OS 11 third-party devices, see Devices Supported by IGEL OS 11[336].

336. https://wiki.test.toolchain.igel.kreuzwerker.net/os11-supported-hardware

Component Versions 11.02.130

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.6.0.60
deviceTRUST Citrix Channel	19.1.200.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.8.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.40.0.25
Parallels Client (64 bit)	17.0.21282
Spice GTK (Red Hat Virtualization)	0.36-1~git20190601igel61
Remote Viewer (Red Hat Virtualization)	8.0-1igel49
Usbredir (Red Hat Virtualization)	0.8.0-1igel49
Teradici PCoIP Software Client	19.05.5-18.04
ThinLinc Client	4.10.0-6068

ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel18
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.7.11

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.2.36
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24

Reader Driver MUSCLE CCID	1.4.30-1igel3
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.0.8-1igel73
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190724-igel907
Graphics Driver ATI/RADEON	19.0.1-2igel890
Graphics Driver ATI/AMDGPU	19.0.1-4igel894
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.65 #mainline-lxos-r2782

Xorg X11 Server	1.19.6-1ubuntu4.3igel910
Xorg Xephyr	1.19.6-1ubuntu4.3igel910
CUPS printing daemon	2.1.3-4ubuntu0.9igel27
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.0-1igel214
WebKit2Gtk	2.24.2-0ubuntu0.19.04.1igel18
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20181030.92c5462-1igel5
Mobile Device Access USB (gphoto)	2.5.22-3igel1
VPN OpenConnect	7.08-1
Scanner support / Sane	1.0.27-1
VirtualBox	6.0.10-dfsg-4igel31

- **Features with Limited Functionality**

Cisco JVDI Client	12.1.0

General Information 11.02.130

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

Security Fixes 11.02.130

Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixes for **mfsa2019-22**, also known as:
  More...

  CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.
- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.
- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.
- Fixes for **mfsa2019-08**, also known as:
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.
- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

Base system

- Set default **umask to 0077** for all non-root users.
- Remote users home is now **/home/ruser**.
- Fixed **policykit-1** security issue CVE-2019-6133.
- Fixed **tiff** security issues:
  More...

  CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:
  More...

  CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.
- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.
- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.
- Fixed **poppler** security issues:

More...

CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293, CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019, CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.

- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:
  More...

  CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.

- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:
  More...

  CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.

- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and CVE-2014-9913.
- Fixed **curl** security issues:
  More...

  CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.

- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and CVE-2018-15518.
- Fixed **libssh2** security issues:
  More...

  CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.

- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues:
  More...

  CVE-2019-7665, CVE-2019-7150, CVE-2019-7149, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues:
  More...

  CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661, CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457, CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246, and CVE-2017-14245.
- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **glib2.0** security issue CVE-2019-12450.
- Fixed **openssl (1.1.x)** security issues:
  More...

  CVE-2019-1543, CVE-2018-0737, CVE-2018-0735, CVE-2018-0734, and CVE-2018-0732.
- Fixed **sqlite3** security issues:
  More...

  CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506, CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518, CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.
- Fixed **systemd** security issues:
  More...

  CVE-2019-6454, CVE-2019-6454, CVE-2018-1049, CVE-2018-15686, and CVE-2019-3842.
- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **imagemagick** security issues:
  More...

  CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396, CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472, CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467, CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966, CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806, and CVE-2017-12805.
- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.
- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.
  Security fixes:
  More...

  CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,

CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

Known Issues 11.02.130

Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264**, **MPEG1** and **MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.
  As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

VMware Horizon

- **Sound redirection in PCoIP** is broken when the so-called lightweight-client is used, which has become the new default.
  Sound redirection can still be used by choosing the rollback-client instead. This can be done by setting the IGEL Registry key:
  More...

Parameter	Allow rollback to former client variant
Registry	`vmware.view.allow-client-rollback`
Value	enabled / disabled

- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.
    In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.

It is also recommended to disable local **Storage Hotplug** under Setup **> Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.
    Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under Setup **>Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection **do not appear in the remote desktop**.
  Workaround: map the directory `/media` as a drive. Then the external devices will show up inside the media drive.

WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.

Resolved Issues 11.02.130

Base system

- Fixed **ActiveDirectory/Kerberos password change** with "Change Password" accessory for users who are members of many (~300+) AD groups.
- Fixed **IGEL license retrieval** via FTP protocol in IGEL Setup Assistant and integrated license browser.

Remote Management

- Fixed **automatic registering in the UMS** using DNS entry or DHCP tag.

Notes for Release 11.02.100

Software:	Version	11.02.100
Release Date:	2019-08-14	
Release Notes:	Version	RN-1102100-1
Last update:	2019-08-14	

- IGEL OS Creator (OSC) (see page 3330)
- IGEL OS 11 (see page 3334)

IGEL OS Creator (OSC)

Supported Devices

UD2-LX:	UD2-LX 40 UD2-LX 50
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[337].

- Component Versions 11.02.100 (see page 3331)
- New Features 11.02.100 (see page 3333)

337. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.02.100

- **Clients**

Product	Version
Zulu JRE	8.40.0.25

- **Smartcard**

Reader Driver MUSCLE CCID	1.4.30-1igel3
Resource Manager PC/SC Lite	1.8.23-1igel1

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.0.8-1igel73
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190724-igel907
Graphics Driver ATI/RADEON	19.0.1-2igel890
Graphics Driver ATI/AMDGPU	19.0.1-4igel894
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.65 #mainline-lxos-r2782
Xorg X11 Server	1.19.6-1ubuntu4.3igel910

Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
WebKit2Gtk	2.24.2-0ubuntu0.19.04.1igel18
Python2	2.7.12
Python3	3.5.2

New Features 11.02.100

Hardware

- Added hardware support for **Rein Medical Silenio 122CT** and **124CT**.
- Added hardware support for **Advantech POC-W213L** and **POC-W243L**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **Fujitsu Esprimo Q957**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **LG AiO Cloud Device 38"**.
- Added hardware support for **HP t430**.
- Added hardware support for **HP t420**.

IGEL OS 11

- Supported Devices 11.02.100 (see page 3335)
- Component Versions 11.02.100 (see page 3336)
- General Information 11.02.100 (see page 3340)
- Security Fixes 11.02.100 (see page 3341)
- Known Issues 11.02.100 (see page 3345)
- New Features 11.02.100 (see page 3347)
- Resolved Issues 11.02.100 (see page 3376)
- CA Certificates Contained in IGEL OS 11.02.100 (see page 3386)

Supported Devices 11.02.100

UD2-LX:	UD2-LX 40 UD2-LX 50
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Third-Party Devices Supported by IGEL OS 11[338].

338. https://wiki.test.toolchain.igel.kreuzwerker.net/hardware/en/third-party-devices-supported-by-igel-os-11-10328463.html

Component Versions 11.02.100

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.6.0.60
deviceTRUST Citrix Channel	19.1.200.2
Ericom PowerTerm	12.0.1.0.20170219.2-_dev_-34574
Ericom PowerTerm	12.5_x64_20190619_12.5.1.40008
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.6
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.8.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	onesign-bootstrap-loader_1.0.523630_amd64
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	6.7.6
Open VPN	2.3.10-1ubuntu2.2
Zulu JRE	8.40.0.25
Parallels Client (64 bit)	17.0.21282
Spice GTK (Red Hat Virtualization)	0.36-1~git20190601igel61
Remote Viewer (Red Hat Virtualization)	8.0-1igel49
Usbredir (Red Hat Virtualization)	0.8.0-1igel49
Teradici PCoIP Software Client	19.05.5-18.04
ThinLinc Client	4.10.0-6068

ThinPrint Client	7.5.88
Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel18
VNC Viewer	1.9.0+dfsg-3igel8
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B301
Olympus driver for dictation	20180621
Philips Speech driver	12.7.11

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.8
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.3.2

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.20
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.2.36
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24

Reader Driver MUSCLE CCID	1.4.30-1igel3
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.2.0.3

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.15
OpenSSH Client	7.2p2-4ubuntu2.8
OpenSSH Server	7.2p2-4ubuntu2.8
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	19.0.8-1igel73
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190724-igel907
Graphics Driver ATI/RADEON	19.0.1-2igel890
Graphics Driver ATI/AMDGPU	19.0.1-4igel894
Graphics Driver Nouveau (Nvidia Legacy)	1.0.16-1igel867
Graphics Driver Nvidia	418.56-0ubuntu1
Graphics Driver Vboxvideo	1.0.0-igel798
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.6-1igel888
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.1-1ubuntu1igel866
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu2igel888
Kernel	4.19.65 #mainline-lxos-r2782

Xorg X11 Server	1.19.6-1ubuntu4.3igel910
Xorg Xephyr	1.19.6-1ubuntu4.3igel910
CUPS printing daemon	2.1.3-4ubuntu0.9igel27
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.3igel74
ModemManager	1.10.0-1~ubuntu18.04.2igel3
GStreamer 0.10	0.10.36-2ubuntu0.2
GStreamer 1.x	1.16.0-1igel214
WebKit2Gtk	2.24.2-0ubuntu0.19.04.1igel18
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB (MTP)	1.1.16-2igel1
Mobile Device Access USB (imobile)	1.2.1~git20181030.92c5462-1igel5
Mobile Device Access USB (gphoto)	2.5.22-3igel1
VPN OpenConnect	7.08-1
Scanner support / Sane	1.0.27-1
VirtualBox	6.0.10-dfsg-4igel31

- **Features with Limited Functionality**

Cisco JVDI Client	12.1.0

General Information 11.02.100

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

Security Fixes 11.02.100

Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixes for **mfsa2019-22**, also known as:
  More...

  CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730, and CVE-2019-11709.
- Fixes for **mfsa2019-19**, also known as: CVE-2019-11708.
- Fixes for **mfsa2019-18**, also known as: CVE-2019-11707.
- Fixes for **mfsa2019-08**, also known as:
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, and CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, and CVE-2018-18501.
- Added allowance for Firefox to access **Yubikey (FIDO/U2F)** if apparmor is active.

Base system

- Set default **umask to 0077** for all non-root users.
- Remote users home is now **/home/ruser**.
- Fixed **policykit-1** security issue CVE-2019-6133.
- Fixed **tiff** security issues:
  More...

  CVE-2019-7663, CVE-2019-6128, CVE-2018-19210, CVE-2018-17000, CVE-2018-12900, and CVE-2018-10779.
- Fixed **lcms2** security issue CVE-2018-16435.
- Fixed **libpng1.6** security issues CVE-2019-7317 and CVE-2018-13785.
- Fixed **nss** security issues CVE-2018-18508, CVE-2019-11729, and CVE-2019-11719.
- Fixed **procps** security issues:
  More...

  CVE-2018-1126, CVE-2018-1125, CVE-2018-1124, CVE-2018-1123 and CVE-2018-1122.
- Fixed **evince** security issues CVE-2019-11459 and CVE-2019-1010006.
- Fixed **gdk-pixbuf** security issue CVE-2017-12447.
- Fixed **gst-plugins-base0.10** security issue CVE-2019-9928.
- Fixed **bind9** security issues CVE-2019-6465, CVE-2018-5745 and CVE-2018-5743.
- Fixed **libgd2** security issues CVE-2019-6978 and CVE-2019-6977.
- Fixed **ghostscript** security issues CVE-2019-3839, CVE-2019-3838 and CVE-2019-3835.
- Fixed **ldb** security issue CVE-2019-3824.
- Fixed **file** security issues CVE-2019-8907 and CVE-2019-8905.

- Fixed **poppler** security issues:
  More...

  CVE-2019-9200, CVE-2019-9903, CVE-2019-9631, CVE-2019-12293, CVE-2019-10872, CVE-2019-10023, CVE-2019-10021, CVE-2019-10019, CVE-2019-10018, CVE-2018-20662, CVE-2018-18897, and CVE-2017-9865.
- Fixed **samba** security issues CVE-2019-3880 and CVE-2018-16860.
- Fixed **openssl** security issue CVE-2019-1559.
- Fixed **libxslt** security issue CVE-2019-11068.
- Fixed **openssh** security issue CVE-2019-6111.
- Fixed **wget** security issue CVE-2019-5953.
- Fixed **wpa** security issues:
  More...

  CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, and CVE-2019-11555.
- Fixed **gtk+2.0** security issue CVE-2013-7447.
- Fixed **heimdal** security issues CVE-2019-12098 and CVE-2018-16860.
- Fixed **webkit2gtk** security issues CVE-2019-8615, CVE-2019-8607, and CVE-2019-8595.
- Fixed **gimp** security issues:
  More...

  CVE-2017-17786, CVE-2017-17789, CVE-2017-17784, CVE-2017-17787, CVE-2017-17785, and CVE-2017-17788.
- Fixed **libtomcrypt** security issue CVE-2018-12437.
- Fixed **unzip** security issues CVE-2019-13232, CVE-2018-1000035, CVE-2016-9844, and CVE-2014-9913.
- Fixed **curl** security issues:
  More...

  CVE-2018-16840, CVE-2018-16839, CVE-2019-3823, CVE-2019-3822, CVE-2018-16890, and CVE-2019-5346.
- Fixed **gnutls28** security issues CVE-2018-10846, CVE-2018-10845, CVE-2018-10844, and CVE-2018-1084.
- Fixed **db5.3** security issue CVE-2019-8457.
- Fixed **qtbase-opensource-src** security issues CVE-2018-19873, CVE-2018-19870, and CVE-2018-15518.
- Fixed **libssh2** security issues:
  More...

  CVE-2019-3863, CVE-2019-3862, CVE-2019-3861, CVE-2019-3860, CVE-2019-3859, CVE-2019-3858, CVE-2019-3857, CVE-2019-3856, and CVE-2019-3855.
- Fixed **network-manager** security issue CVE-2018-15688.
- Fixed **elfutils** security issues:
  More...

CVE-2019-7665, CVE-2019-7150, CVE-2019-7149,
CVE-2018-18521, CVE-2018-18520, CVE-2018-18310,
CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.

- Fixed **libsndfile** security issues:
  More...

  CVE-2019-3832, CVE-2018-19758, CVE-2018-19662, CVE-2018-19661,
  CVE-2018-19432, CVE-2018-13139, CVE-2017-6892, CVE-2017-17457,
  CVE-2017-17456, CVE-2017-16942, CVE-2017-14634, CVE-2017-14246,
  and CVE-2017-14245.

- Fixed **dbus** security issue CVE-2019-12749.
- Fixed **vim** security issues CVE-2019-12735 and CVE-2017-5953.
- Fixed **glib2.0** security issue CVE-2019-12450.
- Fixed **openssl (1.1.x)** security issues:
  More...

  CVE-2019-1543, CVE-2018-0737, CVE-2018-0735,
  CVE-2018-0734, and CVE-2018-0732.

- Fixed **sqlite3** security issues:
  More...

  CVE-2019-9937, CVE-2019-9936, CVE-2019-8457, CVE-2018-20506,
  CVE-2018-20346, CVE-2017-2520, CVE-2017-2519, CVE-2017-2518,
  CVE-2017-13685, CVE-2017-10989, and CVE-2016-6153.

- Fixed **systemd** security issues:
  More...

  CVE-2019-6454, CVE-2019-6454, CVE-2018-1049,
  CVE-2018-15686, and CVE-2019-3842.

- Fixed **libseccomp** security issue CVE-2019-9893.
- Fixed **bzip2** security issues CVE-2019-12900 and CVE-2016-3189.
- Fixed **imagemagick** security issues:
  More...

  CVE-2019-9956, CVE-2019-7398, CVE-2019-7397, CVE-2019-7396,
  CVE-2019-7175, CVE-2019-11598, CVE-2019-11597, CVE-2019-11472,
  CVE-2019-11470, CVE-2019-10650, CVE-2019-10131, CVE-2018-20467,
  CVE-2018-18025, CVE-2018-18024, CVE-2018-18016, CVE-2018-17966,
  CVE-2018-17965, CVE-2018-16413, CVE-2018-16412, CVE-2017-12806,
  and CVE-2017-12805.

- Fixed **expat** security issue CVE-2018-20843.
- Fixed **glib2.0** security issue CVE-2019-13012.
- Fixed **libvirt** security issues CVE-2019-10167 and CVE-2019-10161.
- Fixed **gvfs** security issue CVE-2019-12795.
- Fixed **libmspack** security issue CVE-2019-1010305.
- Fixed **bash** security issue CVE-2019-9924.
- Fixed **openldap** security issues CVE-2019-13565 and CVE-2019-13057.
- Updated **libwebkit2gtk-4.0-37** to version **2.24.2**.
  Security fixes:

More...

CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345, CVE-2018-4386, and CVE-2018-4372.

- Fixed a vulnerability in the **custom environment variable framework**.
- Fixed possible malicious **owner change within TC setup configuration**.
- Fixed **kernel TCP** vulnerabilities CVE-2019-11477: **SACK Panic**, CVE-2019-11478: **SACK Slowness**, and CVE-2019-11479: **Excess resource consumption due to low MSS values**.
- Changed minimally allowed **MSS size** to **1000** to prevent possible Denial of Service attacks.
- Fixed a vulnerability in **Java configuration script**.

Known Issues 11.02.100

Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264**, **MPEG1** and **MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.
  As a workaround, insert the smartcard before starting StoreFront login.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Range	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

VMware Horizon

- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.
    In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.
    It is also recommended to disable local **Storage Hotplug** under Setup **> Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the USB class rules.
    Furthermore, Horizon Client relies on the OS to mount the storage device itself. Enable local **Storage Hotplug** under Setup **>Devices > Storage Devices > Storage Hotplug**.
- **External drives** mounted already before connection **do not appear in the remote desktop**.
  Workaround: map the directory `/` media as a drive. Then the external devices will show up inside the media drive.

WiFi

- **TP-Link Archer T2UH WiFi adapters** do not work after system suspend/resume.
  Workaround: Disable system suspend under **IGEL Setup > System > Power Options > Shutdown**.

Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

Appliance Mode

- Appliance mode **RHEV/Spice**: spice-xpi firefox plugin is no longer supported. The "Console Invocation" has to allow 'Native' client (auto is also possible) and should be started in fullscreen to prevent any opening windows.

Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

Audio

- IGEL **UD2 (D220)** fails to restore the **volume level of the speaker** when the device used firmware version **11.01.110** before.

New Features 11.02.100

Citrix

- Integrated **Citrix Workspace app 19.06**.
  Available Citrix Workspace apps in this release: 19.06, 13.10 and 13.5.
- Added a new registry key to support **1536-bit RSA keys** for client authentication. Factory default for this release is "true".
  More...

Parameter	Enables RSA 1536 cipher suite
Registry	`ica.allregions.enable_rsa_1536`
Range	factory default / false / true

- Added a new **registry key** to enable **different cipher suites** for client authentication. Factory default for this release is "ALL".
  More...

Parameter	Enables different cipher suite
Registry	`ica.allregions.sslciphers`
Range	factory default / ALL / GOV / COM

> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL
> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL
> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL

- Added a new **registry key** to support **keyboard layout synchronization**.
  More...

Parameter	Keyboard layout synchronization
Registry	`ica.modules.virtualdriver.keyboardsync.enable`
Value	false/ true

- Updated **Citrix HDX RTME** used for optimization of Skype for Business to version **2.8.0-2235**.
- Added support for **Citrix Workspace Launcher** functionality as described at https://support.citrix.com/article/CTX237727.
- Added **Citrix Farm Selection**, a facility to manually select one of the configured services / farms for StoreFront login.
  More...

Parameter	Citrix store selection
Registry	`ica.pnlogin.farm_selection.enabled`
Value	off / on

Info:
Off: All servers are used in parallel. If switched on, a user has to select the store via a dialog box before entering the login data.

- **Timeout** for the selection dialog:
  More...

Parameter	Timeout
Registry	`ica.pnlogin.farm_selection.timeout`
Value	0 (no timeout) seconds

- **Width** of the dialog window:
  More...

Parameter	Selection box window width
Registry	`ica.pnlogin.farm_selection.win_width`
Value	400 pixel

- **Height** of the dialog window:
  More...

Parameter	Selection box window height
Registry	`ica.pnlogin.farm_selection.win_height`
Value	400 pixel

- **Changed the defaults** for following parameters:
  More...

IGEL Setup	**Sessions > Citrix > Citrix Global > Window**
Parameter	Multimonitor full-screen mode
Registry	`ica.wfclient.usexdgfullscreen` `ica.wfclient.spanmonitorenable`
Range	[Restrict full-screen session to one monitor] [Expand full-screen session across all monitors] [Expand the session over a self-selected number of monitors]
IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
Parameter	Multimedia redirection
Registry	`ica.module.virtualdriver.multimedia.enable`
Value	enabled / disabled

IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
	Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business
Parameter	HDX Realtime Media Engine
Registry	`ica.module.virtualdriver.hdxrtme.enable`
Value	enabled / disabled

- Updated the **Nuance virtual channel** for ICA to version **B301**.

RDP/IGEL RDP Client 2

- Added a field '**Collection**' to RDP session server page.
  More...

IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Server	
IGEL Setup > Sessions > RDP > RDP Sessions > RDP Session > Options	
Parameter	Collection
Registry	`sessions.winconnect<NR>.option.load-balance-info`

VMware Horizon

- Added parameters to specify **webcam frame size** and **rate for RTAV**.
  More...

Parameter	Webcam frame width
Registry	`vmware.view.rtav-frame-width`
Value	<empty_string>
Parameter	Webcam frame height
Registry	`vmware.view.rtav-frame-height`
Value	<empty_string>
Parameter	Webcam frame rate
Registry	`vmware.view.rtav-frame-rate`
Value	<empty_string>

- Updated **Horizon Client** to version **5.0.0-12557422**.
- Added a possibility to easily evaluate **Horizon Blast decoder states**. By default, sessions are evaluated after usage, and the result is written into the journal log. This can also be used with GUI notifications at runtime.

- Added **new USB classes** to **Horizon USB Redirection** class configuration: **Audio (input)**, **Audio (Output)**, **Imaging**, **Video (Input)**.

Parallels Client

- Updated **Parallels Client** to version **17.0**.
- Added a possibility to set apps to **autostart on Parallels RAS**.

PowerTerm

- Added **Ericom PowerTerm** terminal emulation. This feature requires an **additional license**. The following **versions** are available:
  12.0.1.0.20170219.2-_dev_-34574
  12.5_x64_20190619_12.5.1.40008

IBM_525

- **Improved startup time** of IBM iAccess Client.
- **Improved configuration** of IBM iAccess Client **via IGEL Setup**.
  More...

Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Connection > Advanced
Parameter	Bypass signon
Registry	`sessions.iaccess<NR>.options.ssoenabled`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Font
Parameter	Antialiasing
Registry	`sessions.iaccess<NR>.options.textantialiasing`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor
Parameter	Allow blinking cursor
Registry	`sessions.iaccess<NR>.options.blinkcursor`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor
Parameter	Show blinking text with

Registry	sessions.iaccess<NR>.options.blinkstate
Value	[Blinking Text] [Host Color] [Mapped Color]
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor
Parameter	Blink Color
Registry	sessions.iaccess<NR>.options.blinkcolor_fg
Value	#ffc800
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Cursor
Parameter	Blink Color Background
Registry	sessions.iaccess<NR>.options.blinkcolor_bg
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line
Parameter	Rule Line
Registry	sessions.iaccess<NR>.options.ruleline
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line
Parameter	Follow Cursor
Registry	sessions.iaccess<NR>.options.rulelinefollows
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Rule Line
Parameter	Style
Registry	sessions.iaccess<NR>.options.rulelinestyle
Value	[Crosshair] [Vertical] [Horizontal]
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color

Parameter	Green
Registry	`sessions.iaccess<NR>.options.color_fgn_fg`
Value	#00ff00
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Green Background
Registry	`sessions.iaccess<NR>.options.color_fgn_bg`
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	White
Registry	`sessions.iaccess<NR>.options.color_fwt_fg`
Value	#ffffff
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	White Background
Registry	`sessions.iaccess<NR>.options.color_fwt_bg`
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Red
Registry	`sessions.iaccess<NR>.options.color_frd_fg`
Value	#ff0000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Red Background
Registry	`sessions.iaccess<NR>.options.color_frd_bg`
Value	#000000

Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Turquoise
Registry	`sessions.iaccess<NR>.options.color_ftq_fg`
Value	#00ffff
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Turquoise Background
Registry	`sessions.iaccess<NR>.options.color_ftq_bg`
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Yellow
Registry	`sessions.iaccess<NR>.options.color_fyw_fg`
Value	#ffff00
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Yellow Background
Registry	`sessions.iaccess<NR>.options.color_fyw_bg`
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Pink
Registry	`sessions.iaccess<NR>.options.color_fpk_fg`
Value	#ff00ff
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Pink Background
Registry	`sessions.iaccess<NR>.options.color_fpk_bg`

Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Blue
Registry	`sessions.iaccess<NR>.options.color_fbl_fg`
Value	#7890f0
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Blue Background
Registry	`sessions.iaccess<NR>.options.color_fbl_bg`
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Status Indicators
Registry	`sessions.iaccess<NR>.options.color_osi`
Value	#7890f0
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Information Indicators
Registry	`sessions.iaccess<NR>.options.color_oii`
Value	#ffffff
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Attention Indicators
Registry	`sessions.iaccess<NR>.options.color_oai`
Value	#ffff00
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Error Indicators

Registry	sessions.iaccess<NR>.options.color_oei
Value	#ff0000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	OIA Background
Registry	sessions.iaccess<NR>.options.color_oob
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Screen Background
Registry	sessions.iaccess<NR>.options.color_sbg
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Highlight active field
Registry	sessions.iaccess<NR>.options.actfieldhilite
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Active Field
Registry	sessions.iaccess<NR>.options.color_actf_fg
Value	#000000
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Active Field Background
Registry	sessions.iaccess<NR>.options.color_actf_bg
Value	#ffff00
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color

Parameter	Crosshair Ruler Color
Registry	`sessions.iaccess<NR>.options.color_crc`
Value	#00ff00
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Screen > Color
Parameter	Column Separator
Registry	`sessions.iaccess<NR>.options.color_ccs`
Value	#ffffff
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences
Parameter	Start window maximized
Registry	`sessions.iaccess<NR>.options.ismaximized`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Keyboard
Parameter	Keyboard Remapping File
Registry	`sessions.iaccess<NR>.options.keyremapfile`
Value	IBMi.kmp
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Popup Keypad
Parameter	Popup Keypad File
Registry	`sessions.iaccess<NR>.options.poppadfile`
Setup	Sessions > IBM iAccess Client > iAccess Sessions > Session Name > Preferences > Toolbar
Parameter	Toolbar File
Registry	`sessions.iaccess<NR>.options.toolbarfile`
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Open new sessions in a new tab

Registry	`ibm.iaccess.acssm.opensessionintab`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Always display the tab bar
Registry	`ibm.iaccess.acssm.alwaysshowtabbar`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Switch to new tab when created
Registry	`ibm.iaccess.acssm.switchtonewtab`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Send a warning when closing multiple tabs
Registry	`ibm.iaccess.acssm.closemultipletabwarning`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Do not start tabbed sessions until the tab is selected
Registry	`ibm.iaccess.acssm.tabdelayedstart`
Value	enabled / disabled
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	New Tab Action
Registry	`ibm.iaccess.acssm.newtabaction`
Value	[Disable and Hide] [Run the Same] [Run Other...]
Setup	Sessions > IBM iAccess Client > iAccess Global > Tab Setup
Parameter	Tab Placement
Registry	`ibm.iaccess.acssm.tabplacement`
Value	[Top] [Bottom] [Left] [Right]

NX client

- Updated **NoMachine Client** to version **6.7.6**.

ThinLinc

- Updated **Cendio ThinLinc** to version **4.10**.
- Added support for all of **ThinLinc's login methods**: **password**, **public key**, **smartcard** and **Kerberos**. Additional parameters can be set when smartcard is chosen.
  More...

IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Method of authentication
Registry	`sessions.thinlinc%.login.authentication_method`
Value	password / publickey / scpublickey / kerberos
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	User
Registry	`sessions.thinlinc%.options.user`
Value	
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Password
Registry	`sessions.thinlinc%.option.crypt_password`
Value	
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Use certificate subject as name for login
Registry	`sessions.thinlinc%.login.smartcard_subject_as_name`
Value	enabled / disabled
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Connect the client automatically when a smartcard is found
Registry	`sessions.thinlinc%.login.smartcard_autoconnect`
Value	enabled / disabled

IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Disconnect the client automatically when the smartcard is removed
Registry	`sessions.thinlinc%.login.smartcard_disconnect`
Value	enabled / disabled
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Allow transmission of the smartcard's passphrase for logging in
Registry	`sessions.thinlinc%.login.smartcard_passphrase_sso`
Value	enabled / disabled
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Smartcard filter
Registry	`sessions.thinlinc%.login.smartcard_filter_1`
Value	
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Smartcard filter
Registry	`sessions.thinlinc%.login.smartcard_filter_2`
Value	
IGEL Setup	**Sessions > ThinLinc > ThinLinc Sessions > ThinLinc Session > Login**
Parameter	Smartcard filter
Registry	`sessions.thinlinc%.login.smartcard_filter_3`
Value	

Teradici PCoIP Client

- Added **Teradici PCoIP Client** version **19.05.5**. This feature requires an **additional license**.
  The following parameters are available:
  More...

IGEL Setup	**System > Firmware Customization > Features**
Parameter	Teradici PCoIP Client
Registry	`services.addition_teradici_pcoip_client.enabled`
Value	enabled / disabled

IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Use IGEL Setup for configuration
Registry	`sessions.pcoip<NR>.options.igel-connection`
Value	disabled / enabled
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Server
Registry	`sessions.pcoip<NR>.options.address`
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Server certificate verification mode
Registry	`sessions.pcoip<NR>.options.security-mode`
Range	[Not required] [Warn but allow] [Full verification]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Login**
Parameter	Authentication type
Registry	`sessions.pcoip<NR>.options.auth-type`
Range	[Password authentication] [Smartcard authentication]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**
Parameter	Window mode
Registry	`sessions.pcoip<NR>.options.window-mode`
Range	[User defined] [Fullscreen One Monitor] [Fullscreen All Monitors] [Window]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**
Parameter	User interface translation
Registry	`sessions.pcoip<NR>.options.language`

Range	[System setting] [English] [German] [French] [Spanish] [Portuguese (EU)] [Portuguese (Brazil)] [Italian] [Japanese] [Chinese(Simplified)] [Chinese(Traditional)]
Parameter	Log level
Registry	`sessions.pcoip<NR>.options.log-level`
Range	[Global setting] [Critical] [Error] [Info] [Debug]

- Added support for **global settings**:
  More...

Parameter	Log level
Registry	`pcoip.log-level`
Range	[Critical] [Error] [Info] [Debug]

Parameter	Show codec indicator
Registry	`pcoip.codec_indicator`
Value	disabled / enabled
Info: Added small dot in the bottom left corner during the session to indicate which codec is being used. Green indicates simple codec; blue indicates tic2 codec. This is only available as global setting.	

- UMS option "**Save device files for support**" now includes Teradici PCoIP client's data.

Firefox

- Added new parameters: **Allow a custom command before and after browser session**.
  More...

Parameter	init_action
Registry	`sessions.browser%.init_action`
Value	<empty_string>
Parameter	final_action
Registry	`sessions.browser%.final_action`
Value	<empty_string>

Network

- New feature regarding **lock** and **logon screen**: Network icons are shown on the panel and appear under the same conditions as during normal operation. None of them has a context menu though. Clicking on the Wi-Fi icon directly invokes the Wireless Manager when it is enabled.
  If blocking/unblocking Wi-Fi by the user is enabled, there is an additional button on the Wireless Manager for blocking and a preceding dialog for unblocking.
- **SCEP**: Added a registry key for specifiying **a suffix for CommonName/SubjectAltName** when the type is "**DNS Name (auto)**" or "**DNS Name as UPN (auto)**".
  More...

Parameter	CommonName/SubjectAltName Suffix
Registry	`network.scepclient.cert%.subjectaltnamesuffix`
Value	<empty>
Info: Automatic replacements in the value: %D -> the system's DNS domain name at the time the CSR is created %% -> % Other %X are currently discarded.	

- Added a mechanism for **retrieving the SCEP challenge password with a custom script.** Setting the following registry key to "true" enables the use of the script. The registry key `network.scepclient.cert%.crypt_password` will be ignored. (The script may use it for its own purpose though.)
  More...

Parameter	Use Challenge Password Command
Registry	`network.scepclient.cert%.use_challenge_password_command`
Value	enabled / disabled

If the above key is enabled, the value of this key will be passed to bash for execution. It happens when the SCEP challenge password is needed for creating a certificate signing request. The script is supposed to output the challenge password on its standard output. For convenience, any Carriage-Return characters are stripped off the script before execution by bash.
More...

Parameter	Challenge Password Command
Registry	`network.scepclient.cert%.challenge_password_command`
Value	<empty_string>

- Added **NCP Secure Enterprise VPN Client** version **5.10_rev40552** (configurable under **IGEL Setup > Network > VPN > NCP VPN Client**).

Wi-Fi

- Added: **Wi-Fi adapters can be turned off** and **on** by the tray icon context menu when the following registry key is enabled:
  More...

Parameter	Enable Wi-Fi switch
Registry	`network.applet.wireless.enable_wifi_switch`
Value	enabled / disabled

- Added support for **Realtek 8821CE wireless cards**.

Imprivata

- **Imprivata Appliance 6.3** or higher is needed now.
  Please see the Imprivata Supported Components guide (http://documentation.imprivata.com/01RefArch/Content/Topics/OSSupportedComponents.htm#ProveID) for support and upgrade considerations.
- Added a new parameter to Imprivata.conf: "**Redirection of Smartcards**".
  More...

IGEL Setup > Sessions > Appliance Mode > Imprivata	
Parameter	Redirection of Smartcards
Registry	`imprivata.native_smartcard_redirection`
Value	enabled / disabled

- Added a new parameter: "**Path to Certificate**".
  More...

IGEL Setup > Sessions > Appliance Mode > Imprivata	
Parameter	Path to Certificate
Registry	`imprivata.path_to_certificate`

Smartcard

- Added **90meter** smartcard library. This feature requires an **additional license**.
  Use the following parameters to activate:
  More...

IGEL Setup	**System > Firmware Customization > Features**

Parameter	90meter Smart Card Support
Registry	`services.addition_smartcard_90meter.enabled`
Value	enabled / disabled
IGEL Setup	**Sessions > Horizon Client > Horizon Client Global > Smartcard**
Parameter	Horizon logon with smartcards supported by 90meter library
Registry	`vmware.view.pkcs11.use_90meter`
Value	enabled / disabled
IGEL Setup	**Sessions > Browser > Browser Global > Smartcard Middleware**
Parameter	90meter Security Device
Registry	`browserglobal.security_device.90meter`
Value	enabled / disabled
IGEL Setup	**Security > Smartcard > Middleware**
Parameter	90meter
Registry	`scard.pkcs11.use_90meter`
Value	enabled / disabled

- New **IGEL Smartcard** mode **without Locking Desktop** (reintroduced feature of Linux 5.x firmware).
  More...

IGEL Setup > Security > Logon > IGEL Smartcard	
Parameter	Enable IGEL Smartcard without Locking Desktop
Registry	`scard.scardd.enable_nolock`
Value	enabled / disabled
IGEL Setup > Security > Logon > IGEL Smartcard	
Parameter	On Smartcard Removal, terminate
Registry	`scard.scardd.session_termination`
Value	all / smartcard

- Updated **SecMaker NetID** to version **6.7.2.36**: now **YubiKey 5** is supported.
- Updated **CHERRY USB-LAN Proxy** to version **3.2.0.3**. This version provides enhanced configuration.

More...

IGEL Setup > Security > Smartcard > Services	
Parameter	Bind IP
Registry	`devices.cherry.usblanproxy.bind-ip`
Value	auto
IGEL Setup > Security > Smartcard > Services	
Parameter	Https Server Port
Registry	`devices.cherry.usblanproxy.https-port`
Value	443
IGEL Setup > Security > Smartcard > Services	
Parameter	SICCT Announce IP
Registry	`devices.cherry.usblanproxy.sicct-announce-ip`
Value	broadcast
IGEL Setup > Security > Smartcard > Services	
Parameter	SICCT Announce Port
Registry	`devices.cherry.usblanproxy.sicct-announce-port`
Value	4742
IGEL Setup > Security > Smartcard > Services	
Parameter	SICCT Announce Interval
Registry	`devices.cherry.usblanproxy.sicct-announce-interval`
Value	30
IGEL Setup > Security > Smartcard > Services	
Parameter	USB Fast Mode
Registry	`devices.cherry.usblanproxy.usb-fast-mode`
Value	enabled /disabled
IGEL Setup > Security > Smartcard > Services	

Parameter	Alternate Initialization Method for G87-1505
Registry	devices.cherry.usblanproxy.usb-1505-alt-setup
Value	enabled /disabled

- Added a command line tool **pcsc_scan** for smartcard debugging.
- Added configuration parameters for some settings of **smartcard library OpenSC**.
  More...

Parameter	Debug level
Registry	scard.pkcs11.opensc.default.debug
Value	0
Parameter	Debug file
Registry	scard.pkcs11.opensc.default.debug_file
Value	stderr
Parameter	Max. send size
Registry	scard.pkcs11.opensc.default.pcsc.max_send_size
Value	255
Parameter	Max. receive size
Registry	scard.pkcs11.opensc.default.pcsc.max_recv_size
Value	256
Parameter	Connect exclusive
Registry	scard.pkcs11.opensc.default.pcsc.connect_exclusive
Value	enabled / disabled
Parameter	Disconnect action
Registry	scard.pkcs11.opensc.default.pcsc.disconnect_action
Value	leave / reset / unpower
Parameter	Transaction end action
Registry	scard.pkcs11.opensc.default.pcsc.transaction_end_action

Value	leave / reset / unpower
Parameter	Reconnect action
Registry	`scard.pkcs11.opensc.default.pcsc.reconnect_action`
Value	leave / reset / unpower
Parameter	Enable pinpad
Registry	`scard.pkcs11.opensc.default.pcsc.enable_pinpad`
Value	enabled / disabled
Parameter	Use PIN caching
Registry	`scard.pkcs11.opensc.default.pkcs15.use_pin_caching`
Value	enabled / disabled
Parameter	How many times to use a PIN from cache before re-authenticating it
Registry	`scard.pkcs11.opensc.default.pkcs15.pin_cache_counter`
Value	10
Parameter	PIN caching ignores user consent
Registry	`scard.pkcs11.opensc.default.pkcs15.pin_cache_ignore_user_consent`
Value	enabled / disabled

- Updated **cryptovision sc/interface PKCS#11** smartcard library to version **7.1.20**.
  Changes in this revision:
  - Fixed a possible **deadlock** in the PKCS#11 module on Linux, if **C_Finalize** is called during a PCSC event, for example C_WaitForSlotEvent.
  - **ROCA check** in the Smartcard Manager, based on the "ROCA detection tool", see https://github.com/crocs-muni/roca.
  - **Renaming** of the container label in Smartcard Manager **with F2** is now possible.

CUPS Printing

- Added **SMB Network Print** client function.
  More...

IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	Printer Port

Registry	`print.cups.printer<NR>.backend`
Value	smb
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	SMB Server
Registry	`print.cups.printer<NR>.smb_server`
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	SMB Workgroup
Registry	`print.cups.printer<NR>.smb_workgroup`
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	SMB Printer
Registry	`print.cups.printer<NR>.smb_printer`
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	SMB Port
Registry	`print.cups.printer<NR>.smb_port`
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	Use Kerberos Authentication
Registry	`print.cups.printer<NR>.smb_kerberos`
Value	enabled / disabled
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	Use Passthrough Authentication
Registry	`print.cups.printer<NR>.smb_passthrough`
Value	enabled /disabled
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	
Parameter	SMB User
Registry	`print.cups.printer<NR>.smb_user`
IGEL Setup > Devices > Printer > CUPS > Printers > Dialog	

Parameter	SMB Password
Registry	`print.cups.printer<NR>.crypt_password`

Base system

- Added a possibility to configure **scheduled commands**. Registry keys: `system.cron.**`
- **Buddy update** enhancements:
  - **Automatic load balancing**:
    A client collects up to eight server candidates from which one is selected randomly. Collection stops when the number specified in the following registry key is reached. Otherwise collection stops after a timeout.
    More...

Parameter	Buddy Update Server Candidates
Registry	`update.ftp.buddy_server_candidates`
Value	1

  - **Grouping**:
    Buddy update servers and clients only interact with each other when they are in the same group determined by the following registry key (a non-negative integer number). This feature is mainly useful when different firmware versions shall be used in parallel.
    More...

Parameter	Buddy Group ID
Registry	`update.ftp.buddy_group_id`
Value	0

- Added: **Firmware update** scheduled **on shutdown** is now **invoked on reboot** too.
- Added package **ldap-utils** which can be used by custom scripts.
- Updated **Kernel** to mainline version **4.19.65**.
- Moved the **EULA** page in IGEL Setup Assistant into the **demo activation workflow**.
- **Updated EULA** displayed in OSC and IGEL Setup Assistant.
- Added: When IGEL Setup Assistant is used to download **a demo license via Wi-Fi**, the **local Wi-Fi manager** will be **enabled by default**.
- Updated **Fluendo multimedia codecs** to the following versions:
  More...

gst-fluendo-aacdec	21/03/2019	0.10.39
gst-fluendo-asfdemux	21/03/2019	0.10.89
gst-fluendo-h264dec	21/03/2019	0.10.53
gst-fluendo-mp3	21/03/2019	0.10.39
gst-fluendo-mpeg4video	21/03/2019	0.10.43

gst-fluendo-vadec	21/03/2019	0.10.208
gst-fluendo-wmadec	21/03/2019	0.10.68
gst-fluendo-wmvdec	20/03/2019	0.10.65

- Replaced **timesyncd** with **chrony NTP**. Added a new registry key:
  More...

Parameter	Use NTP Servers from DNS SRV record
Registry	`system.time.ntp_use_dnssrv_timeservers`
Value	enabled / disabled

- Updated **CA Certificates** to version **20190122** (Mozilla authority bundle version 2.30).
  The following authorities were added:
  More...
  - "Certigna Root CA"
  - "GTS Root R1"
  - "GTS Root R2"
  - "GTS Root R3"
  - "GTS Root R4"
  - "UCA Extended Validation Root"
  - "UCA Global G2 Root"
  - "GlobalSign Root CA - R6"
  - "OISTE WISeKey Global Root GC CA"
  - "GDCA TrustAUTH R5 ROOT"
  - "SSL.com EV Root Certification Authority ECC"
  - "SSL.com EV Root Certification Authority RSA R2"
  - "SSL.com Root Certification Authority ECC"
  - "SSL.com Root Certification Authority RSA"
  - "TrustCor ECA-1"
  - "TrustCor RootCert CA-1"
  - "TrustCor RootCert CA-2"

  The following authorities were removed:
  More...
  - "Certplus Root CA G1"
  - "Certplus Root CA G2"
  - "OpenTrust Root CA G1"
  - "OpenTrust Root CA G2"
  - "OpenTrust Root CA G3"
  - "TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5"
  - "Visa eCommerce Root"
  - "ACEDICOM Root"
  - "AddTrust Low-Value Services Root"
  - "AddTrust Public Services Root"

- "AddTrust Qualified Certificates Root"
- "CA Disig Root R1"
- "CNNIC ROOT"
- "Camerfirma Chambers of Commerce Root"
- "Camerfirma Global Chambersign Root"
- "Certinomis - Autorité Racine"
- "Certum Root CA"
- "China Internet Network Information Center EV Certificates Root"
- "Comodo Secure Services root"
- "Comodo Trusted Services root"
- "DST ACES CA X6"
- "GeoTrust Global CA 2"
- "PSCProcert"
- "Security Communication EV RootCA1"
- "Swisscom Root CA 1"
- "Swisscom Root CA 2"
- "Swisscom Root EV CA 2"
- "TURKTRUST Certificate Services Provider Root 2007"
- "TUBITAK UEKAE Kok Sertifika Hizmet Saglayicisi - Surum 3"
- "UTN USERFirst Hardware Root CA"

Driver

- Added registry keys to modify the Intel graphic driver usage of **framebuffer compression** and **power management**.
  New registry keys:
  More...

Parameter	Power saving display C-States to use
Registry	`x.drivers.intel.dc_setting`
Range	[Default] [Disable] [Up to DC5] [Up to DC6]
Info: "Default" - driver default	

Parameter	Use framebuffer compression
Registry	`x.drivers.intel.fbc_setting`
Range	[Default] [Disable]
Info: "Default" - driver default	

- Updated **Philips Speech Driver** to version **12.7.11**.
- Updated **signotec Citrix Virtual Channel** driver to version **8.0.8**.
- Updated **StepOver TCP Client** to version **2.3.2**.
- Updated **deviceTRUST Client** to version **19.1.200**. These are the release notes:
  Welcome to the release of the deviceTRUST 19.1.200 IGEL client, providing the context of IGEL thin

client and UD Pocket devices into your virtual sessions. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.

Logical Disks
We've added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint. This includes:
More...

DEVICE_LOGICALDISK_X_TYPE – Either Fixed or Removable.
DEVICE_LOGICALDISK_X_LABEL – The volume label.
DEVICE_LOGICALDISK_X_FILESYSTEM – The type of file system.
DEVICE_LOGICALDISK_X_PATHS – The paths that the disk is mounted.
DEVICE_LOGICALDISK_X_TOTALMB – The total space available on the disk. This property is only available for mounted disks.
DEVICE_LOGICALDISK_X_FREEMB – The free space available on the disk. This property is only available for mounted disks.
DEVICE_LOGICALDISK_X_NAME – The name of the underlying physical disk.
DEVICE_LOGICALDISK_X_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.
DEVICE_LOGICALDISK_X_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.
DEVICE_LOGICALDISK_X_SERIALNUMBER – The serial number of the physical disk.
DEVICE_LOGICALDISK_X_BUSTYPE – The storage bus type linked to the physical disk.
DEVICE_LOGICALDISK_COUNT – The number of logical disks.

X11 system

- Added a new parameter to allow configuration of '**Display Switch' confirmation dialog timeout**.
  More...

IGEL Setup	**Accessories > Display Switch > Options**
Parameter	Timeout for confirmation dialog
Registry	`sessions.user_display0.options.confirm_timeout`
Value	10

- Re-Enable 'Display Switch' session start script to cycle simple modes.
- Added new options for **lid handling**.
  More...

Parameter	Lid close action while plugged in
Registry	`system.actions.lid.ac`
Range	[Turn off display] [Suspend]
Parameter	Lid close action while not plugged in
Registry	`system.actions.lid.battery`

Range	[Turn off display] [Suspend]

- Added new registry keys to change the xorg input driver for an input device class.
  New registry keys:

  For keyboards:
  More...

Parameter	Xorg driver to use
Registry	`userinterface.keyboard.driver`
Range	[Evdev] [Libinput]

  For touchpads:
  More...

Parameter	Xorg driver to use
Registry	`userinterface.touchpad.driver`
Range	[Evdev] [Synaptics] [Libinput]

  For touchscreens:
  More...

Parameter	Xorg driver to use
Registry	`userinterface.touchscreen.xorg_driver`
Range	[Evdev] [Libinput]

  For mouse:
  More...

Parameter	Xorg driver to use
Registry	`userinterface.mouse.driver`
Range	[Evdev] [Libinput]

- Added some registry keys to disable loading of **DRM kernel modules** (graphic).
  More...

Parameter	Disable the loading of the RADEON DRM driver
Registry	`x.drivers.ati.disable`
Value	0
Parameter	Disable the loading of the AMDGPU DRM driver
Registry	`x.drivers.amdgpu.disable`

Value	0
Parameter	Disable the loading of the i915 DRM driver
Registry	`x.drivers.intel.disable`
Value	0
Parameter	Disable the loading of the NVIDIA kernel driver
Registry	`x.drivers.nvidia.disable`
Value	0
Parameter	Disable the loading of the NOUVEAU DRM driver
Registry	`x.drivers.nouveau.disable`
Value	0
Parameter	Disable the loading of the QXL DRM driver
Registry	`x.drivers.qxl.disable`
Value	0
Parameter	Disable the loading of the VMGFX DRM driver
Registry	`x.drivers.vmware.disable`
Value	0
Parameter	Disable the loading of the VBOXVIDEO DRM driver
Registry	`x.drivers.vboxvideo.disable`
Value	0

- Updated **DisplayLink** driver to version **5.1.26** to solve some startup issues.

Evidian

- Updated **Evidian rsUserAuth** to version **1.5.7116**.

Hardware

- Added hardware support for **Rein Medical Silenio 122CT and 124CT**.
- Added hardware support for **Advantech POC-W213L** and **POC-W243L**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **Fujitsu Esprimo Q957**.
- Added hardware support for **ADS-TEC VMT 9000 Serie**.
- Added hardware support for **LG AiO Cloud Device 38"**

- Added hardware support for the following **headsets**:
  More...
  - Jabra Engage 50
  - Jabra Engage 65
  - Jabra Engage 75
  - Jabra Evolve 30 II (Ver. B)
  - Jabra Evolve 30 II (Ver. C)
  - Jabra Evolve 40 (Ver. B) - USB-C
  - Jabra Evolve 40 (Ver. D)
  - Jabra Evolve 65
  - Jabra Evolve 75
  - Plantronics Voyager 5200 UC
  - Plantronics Voyager 6200 UC
  - Plantronics Voyager 8200 UC
  - Plantronics ENCOREPRO 720 + DA70
  - Plantronics ENCOREPRO 720 + DA80
  - Plantronics ENCOREPRO 520D + DA90
  - Sennheiser SC70
- Added hardware support for **HP t430**.
- Added hardware support for **HP t420**.

Java

- Replaced Oracle JRE by **AZUL's Zulu JRE**.
- Updated **Zulu JRE** to version **8.40.0.25**.

Remote Management

- **Connection order between UMS and ICG** can now be configured.
  More...

Registry	`system.remotemanager.icg_try_ums_connect`
Value	enabled / disabled

  When an ICG connection is configured and the parameter is enabled, the device tries to connect directly to UMS. If the connection was established successfully, the device is managed by UMS and not over ICG until new start of the device or network.

IGEL Cloud Gateway

- Added **VNC Shadowing** support **over ICG**. To use this feature, **UMS 6.02.110 or later** and **ICG 2.01.100 or later** are required.

Resolved Issues 11.02.100

Citrix

- Improved **USB handling of SpaceMouse**.
- Improved **USB redirection** handling with **Citrix Workspace App 19.06**.
- Fixed **stability issues** with **Citrix Browser Content Redirection**.

OSC Installer

- Fixed: OSC Installer does not disable **EFI** when **MSDOS partitioning** was chosen.

Citrix Receiver 13

- Added a **switch** to enable the possibility to **launch multiple desktop sessions with RTME and h.264 acceleration**. This switch should not be used when "**Enable Secure ICA**" is active for specific delivery group.
  More...

Registry	`ica.workaround-dual-rtme`
Value	enabled / disabled

RDP/IGEL RDP Client 2

- Added a registry key to use **rdpglobal window settings for remote apps**.
  More...

Parameter	Enable global windwos settings for remote app
Registry	`rdp.winconnect.enable-global-window-settings-for-remote-app`
Value	enabled / disabled

- Added negotiation: **Kerberos as fallback for disabled NTLM authentication**. This only works when **Active Directory/Kerberos Logon** is enabled.
- Fixed **RD Web Access** not working with special characters in name or password. This only works when **Active Directory/Kerberos Logon** is enabled.
- Fixed **smartcard redirection in RDP**: **SCardGetAttrib** was failing if **pbAttr** was NULL. The fix should help running Dutch Zorg-ID applications.

RD Web Access

- Fixed **not starting RDP Remote Applications**.

VMware Horizon

- Added **recognition** for **password change** and **password expired** dialog in Horizon local logon sessions or appliance mode.
- Fixed configuration choice for usage of **relative mouse feature**.
- Added possibility to use the **rollback variant of the Horizon Client**.
  More...

Parameter	Allow rollback to former client variant
Registry	`vmware.view.allow-client-rollback`
Value	enabled / disabled

- Fixed a problem with the client where connection to the **remote desktop using PCoIP protocol failed** occasionally.

Teradici PCoIP Client

- Fixed unwanted **restart of login window** after session logoff or disconnect.

Firefox

- Fixed Firefox **not accepting proxy credentials** from setup.
- Fixed **print hotkey** disable option not working with Firefox 60.
- Fixed **browserglobal.app.local_subdirs_whitelist** not working.

Network

- Fixed: **Failure to reach SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- Changed **e1000e driver** to out of tree version **3.4.2.3** directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** directly from Intel.
- Added possibility to **switch between third-party** and **kernel Intel IGB network driver**.
  New registry key:
  More...

Parameter	Use thirdparty igb kernel module
Registry	`network.drivers.igb.prefer_thirdparty`
Range	[Auto] [Yes] [No]
Info: "Auto" (use thirdparty in most cases)	

- Added possibility to **switch between third-party** and **kernel intel E1000E network driver**.
  New registry key:
  More...

Parameter	Use thirdparty e1000e kernel module
Registry	`network.drivers.e1000e.prefer_thirdparty`
Range	[Auto] [Yes] [No]
Info: "Auto" (use thirdparty in most cases)	

- Fixed **instability of netmounts** with static IP configuration.
- Added possibility to **switch between third-party r8168** and **kernel r8169 realtek network driver**.
  New registry key:
  More...

Parameter	Use thirdparty r8168 kernel module
Registry	`network.drivers.r8169.prefer_r8168`
Range	[Auto] [Yes] [No]
Info: "Auto" (use r8168 in most cases)	

- Added a possibility to choose the **variant of the realtek r8168 driver**.
  A new registry key:
  More...

Parameter	Choose realtek r8168 variant (only if "prefer r8168" is chosen)
Registry	`network.drivers.r8169.r8168_variant`
Range	[Default] [No NAPI] [NAPI]
Info: "Dafault" (use NAPI in most cases)	

- Fixed: **Second Ethernet** interface **did not get configured** when the first one was disabled.
- Fixed: **802.1X Ethernet** configuration **with user interaction** was broken.

Wi-Fi

- Fixed not working **TP Link Archer T2UH**.
- Fixed not working **Broadcom SDIO WLAN cards** as present in Advantech AIM8IAC device for example.

Smartcard

- Updated **cryptovision sc/interface PKCS#11 smartcard library** to version **7.1.20**.
- Fixed a possible **deadlock** in the **PKCS#11 module** on Linux if **C_Finalize** is called during a PCSC event, for example C_WaitForSlotEvent.
- Fixed **OpenSC** setting **max_send_size** for reader driver pcsc in **/etc/opensc/opensc.conf**.
- Fixed **Dell KB813 Smartcard Keyboard** in combination with certain smartcards driven by OpenSC PKCS#11 module. Before this fix, **authentication to Citrix StoreFront** and **VMWare Horizon failed**.

Base system

- Improved: Ensured that the **Unit ID for IGEL devices is the MAC address of the onboard network card**.
- Fixed **license expiry warning at boot**. Before this fix, in some cases the warning wrongly appeared at every boot.
- Fixed **unmounting storage devices** via **In-session control bar**.
- Fixed **server-dependent crash** when installing license via FTP.
- Fixed retrieving of **serial number of a connected screen**.
- Fixed random **90 seconds shutdown delay** (systemd).
- Fixed wrong behavior with **expired evaluation licenses** in some cases.
- Added message in **bootsplash** when a custom partition will get created.
- Fixed **bug in the screenlock countdown** that occurred, when display of remaining seconds was not desired.

- Fixed **shortcut configuration for shutdown**, **restart** and **icon** sort to be applied without reboot.
- Added **apparmor** rule to allow **tcpdump** to write to /debuglog.
- Fixed **hotkey** configuration **to be applied without reboot**.
- Fixed: **UD2** screen **goes black** with certain multimonitor configurations.
- Improved new **license detection** in **IGEL Setup Assistant**.
- Fixed **AD/Kerberos logon** in case parameter **auth.login.krb5_enterprise** is set to false.
- Fixed: **System logoff waits for Citrix logoff** now.
- Fixed **NTP synchronization** problems **when changing the NTP client** from **timesyncd** to **chrony**.
- Added **switch** to enable **DNS hostname lookup for SSH server**:
  More...

Parameter	Use DNS to resolve client hostnames
Registry	`network.ssh_server.use_dns`
Value	enabled / disabled

- Fixed **USB printer aliases**.
- Fixed **gtk-3 icon sizes** for **High DPI** configurations.
- Enhanced **bootloader** to allow the setting of some kernel command line parameters with registry keys.
  New registry keys:
  More...

Parameter	Disable use of APIC controller.
Registry	`system.kernel.bootparams.noapic`
Value	enabled / disabled
Parameter	Disable use of ACPI.
Registry	`system.kernel.bootparams.noacpi`
Value	enabled / disabled
Parameter	Use only one CPU core and disable all others.
Registry	`system.kernel.bootparams.nosmp`
Value	enabled / disabled
Parameter	Enable debug console on serial port 1.
Registry	`system.kernel.bootparams.serial_console_debug`
Value	enabled / disabled
Parameter	Limit CPU core usage (0 means no limit).

Registry	`system.kernel.bootparams.maxcpus`
Value	"0"
Parameter	Set maximum allowed cstate on intel cpus.
Registry	`system.kernel.bootparams.max_cstate`
Range	[No limit] [1] [2] [3] [4] [5] [6]
Info: do not limit intel cstate	
Parameter	IOMMU usage setting.
Registry	`system.kernel.bootparams.iommu`
Range	[On] [Off] [Passthrough] [Force]
Info: Use IOMMU passthrough possible	
Parameter	IOMMU usage setting for AMD systems.
Registry	`system.kernel.bootparams.amd_iommu`
Range	[On] [Off]
Info: Use IOMMU if possible	
Parameter	IOMMU usage setting for Intel systems.
Registry	`system.kernel.bootparams.intel_iommu`
Range	[On] [Off]
Info: Use IOMMU if possible	

- Added a new registry key to set **USB quirks:**
  More...

Parameter	Set XHCI USB quirks to fix some hardware issues
Registry	`system.kernel.bootparams.xhci-hcd_quirks`
Range	[No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk] [Spurious Reboot Wakeup quirk]

- Lenovo **ThinkCentre M73** needs the **system.kernel.bootparams.xhci-hcd_quirks** registry key set to `**Spurious Reboot quirk**` to fix reboot after shutdown problem.
- Added column "**Syslog style template**" to **Remote Syslog setup page**. This allows to change rsyslog output style e.g. to newer SyslogProtocol23Format which is supported by graylog.
- Disable **martian packet logging**.

Driver

- Updated **deviceTRUST Client** to version **19.1.200**.
  - Fixed an issue reading the D**EVICE_IGEL_ICG_SERVER** property.
  - Fixed an issue where the **NETWORK** and **LOCATION** property providers **could cause the client to freeze** if a disconnection occurred whilst these property providers were checking for changes.
  - Fixed an **open file handle leak** which led to the client process reaching its file handle limits when left running for a long period of time.
- Fixed not working **WACOM** device **DTU-1141B**.

Custom Partition

- Added **message in bootsplash** when **a custom partition** will get **created**.
- Fixed **ownership of extracted data**: don't preserve original owner while extracting data into custom partition.

Storage Devices

- Fixed **automounting of storage devices** inside of **Olympus DS-9500 Digital Voice Recorder**.

Appliance Mode

- Fixed: **In-session control bar** could not be deactivated in **Citrix SelfService appliance mode**.

X11 system

- There is now **a registry key to ignore a 3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the SpaceMouse is only passed through to the desktop session. If disabled, it acts like a standard mouse.
  More...

IGEL Setup	**System > Registry**
Parameter	Deactivates a 3Dconnexion SpaceMouse as a standard mouse
Registry	`userinterface.mouse.spacemouse.x11_ignore`
Value	enabled / disabled

- The following **SpaceMouse** products are included:
  More...

VID	PID	Vendor	Product
0x046D	0xC603	Logitech, Inc.	3Dconnexion SpaceMouse Plus XT
0x046D	0xC605	Logitech, Inc.	3Dconnexion CADman
0x046D	0xC606	Logitech, Inc.	3Dconnexion SpaceMouse Classic
0x046D	0xC621	Logitech, Inc.	3Dconnexion SpaceBall 5000
0x046D	0xC623	Logitech, Inc.	3Dconnexion SpaceTraveller 3D Mouse
0x046D	0xC625	Logitech, Inc.	3Dconnexion SpacePilot 3D Mouse

VID	PID	Vendor	Product
0x046D	0xC626	Logitech, Inc.	3Dconnexion SpaceNavigator 3D Mouse
0x046D	0xC627	Logitech, Inc.	3Dconnexion SpaceExplorer 3D Mouse
0x046D	0xC628	Logitech, Inc.	3Dconnexion SpaceNavigator for Notebooks
0x046D	0xC629	Logitech, Inc.	3Dconnexion SpacePilot Pro 3D Mouse
0x046D	0xC62B	Logitech, Inc.	3Dconnexion SpaceMouse Pro
0x256F	**	3Dconnexion	SpaceMouse

- **USB device reset** via USB powercycle is now available on **UD6/UD7**.
- Fixed: Problems with i**nternal graphic cards** and **Nvidia graphic cards**.
- **Display Switch** application will now use some settings from 'Advanced' dialog in 'Simple' mode.
- Fixed **display hotplug failing** on initial lock screen with Active Directory logon.
- Fixed **screen corruption** with DPMS and enabled composite manager.
- Fixed **screen flickering** in some cases when "**Force NumLock On**" (x.global.forcenumlock) is active.
- Fixed **Display Switch** utility not starting with some translations.
- Fixed an issue with the **noDDC mode** which was not always working as expected.
- Fixed **wrongly detected embedded DisplayPort** on **Dell Wyse 5070** Extended hardware.
- Added the possibility to change an **embedded DisplayPort** to a normal **DisplayPort**.
  More...

Parameter	Use embedded displayport as normal displayport (reboot required)
Registry	`x.drivers.intel.edp_is_dp`
Range	[default] [enable] [disable]

- Fixed some **multimonitor** (>4) issues with **Nvidia graphic cards**.
- Fixed **monitor screen ID** shown with **Nvidia nvs810 GPU**.
- Added consideration of **hardware limits for choosing automatic resolution** in **Xorg config** (currently only for IGEL hardware).
- Fixed problem with **modesetting driver** and **two 2160x1440 monitors** in extended configuration.
- Added a new registry key to enable use of **linear framebuffer for modesetting driver**.
  New registry key:
  More...

Parameter	Use linear instead of tiled framebuffer
Registry	`x.drivers.modesetting.use_linear_framebuffer`
Range	[Default] [False] [True]
Info: Use linear framebuffer only in special cases.	

- Fixed configuration where old **Display Switch** took precedence over configuration from new Display Switch and preventing changes.

X Server

- Fixed issue with **primary / secondary screens** were switched in some cases.

Audio

- Fixed **bad quality sound over DisplayPort** in a Citrix ICA session or other applications using ALSA API.
- Fixed **jack detection of the headphone port** in **Dell Wyse 3040**.
- Fixed **configuration of default audio output** and **input**.

Media Player (Parole)

- Fixed a problem where **parole media player** would **hang** instead of playing audio **while audio-visualization** is enabled.
- Fixed parole media player **not handling audio hotkeys in fullscreen mode**.

Misc

- **Monitoring Agent** uses now **only the half size of the debuglog partition**.
  When the setup option **log_max_size** with the option **log_rotation** creates an overall consumption that is bigger than 50% of the debuglog partition size, the size for each log automatically will be decreased to a value that allows a full rotation which occupies exactly 50% of the partition size.

Hardware

- Fixed not working **network** on **Beckhoff CB3163, CB6263** and **CB6363** systems.
- Fixed not working network on **Lex 3I380D**.
- Fixed **shutdown** issue of **Lenovo ThinkCentre M73** (rebooted 2 - 3 seconds after power off).
- Added a **possibility to change** some **DRM settings** and **limit the DisplayPort lane bandwidth** on Intel devices.
  Added new registry keys:
  More...

Parameter	Use best graphic mode for all screens on console.
Registry	`x.drivers.kms.best_console_mode`
Range	[Default] [Enabled] [Disabled]
Info: "Default" is enabled in most cases.	

Parameter	Limit the maximum console resolution width to this value.
Registry	`x.drivers.kms.max_console_width`
Type	Integer
Value	"0"
Info: "0" means default setting. Use the default setting.	

Parameter	Limit the maximum console resolution height to this value.
Registry	`x.drivers.kms.max_console_height`
Type	Integer
Value	"0"
Info: "0" means default setting. Use the default setting.	

Parameter	Set graphic kernel driver debug level.
Registry	`x.drivers.kms.debug_level`
Range	[No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full]
Info: Warning log will grow very fast.	

Only for Intel i915 driver:

Parameter	Limit the maximum DisplayPort lane link rate.
Registry	`x.drivers.intel.max_dp_link_rate`
Range	[default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps] [4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps]
Info: "Default" means hardware default limit.	

Parameter	Disable the DP audio support in the i915 DRM driver.
Registry	`x.drivers.intel.disable_dp_audio`
Range	[Default][No][Yes]
Info: "Default" - support is enabled.	

Parameter	Disable the HDMI audio support in the i915 DRM driver.
Registry	`x.drivers.intel.disable_hdmi_audio`
Range	[Default][No][Yes]
Info: "Default" - support is enabled.	

- Fixed **black screen** issue with some monitors and 2560x1440 resolution - occurred on **UD2 LX50** and **other Intel GPUs**.
- Fixed detection of **Dell Wyse 5070** for the non-extended version.
- Fixed issues with **not working Touchpad** and **Trackpoint** on Lenovo laptops.
- Fixed **vanishing mouse cursor on Ryzen 3** devices.
- Fixed problems with **2 or more monitors** on a **DisplayLink** adapter.
- Added possibility to use **AMDGPU PRO** driver instead of the kernel integrated driver.

- **Ryzen 3** devices (1200, 1300X, 2200G, 2200U and 2300U) **will use the AMDGPU PRO driver** if registry key x.drivers.amdgpu.use_amdgpu_pro is set to auto (default).
- A new registry key (settings to this key will only work after reboot):
  More...

Parameter	Use AMDGPU PRO driver
Registry	`x.drivers.amdgpu.use_amdgpu_pro`
Range	[Auto] [True] [False]

Remote Management

- When **TC is managed over ICG**, settings received in the connection stage does not apply immediately. The settings must be applied after user prompt dialog.
- Fixed **UMS synchronization** of configuration changes made in "Emergency mode". Fixed sporadically failures while sending data over ICG.
- Fixed **wallpaper configuration** if ICG protocol is used.
- Fixed **releasing from UMS** when the device was offline during removal from UMS.
- Added: The **endpoint can now report up to 8 monitors** in UMS information.
- Fixed **UMS jobs** have not been executed when delivered at the next system boot.

CA Certificates Contained in IGEL OS 11.02.100

Contained CA certificates:
- ACCVRAIZ1, expires Dec 31 09:37:37 2030 GMT (ACCVRAIZ1.crt)
- AC RAIZ FNMT-RCM, expires Jan 1 00:00:00 2030 GMT (AC_RAIZ_FNMT-RCM.crt)
- Actalis Authentication Root CA, expires Sep 22 11:22:02 2030 GMT (Actalis_Authentication_Root_CA.crt)
- AddTrust External CA Root, expires May 30 10:48:38 2020 GMT (AddTrust_External_Root.crt)
- AffirmTrust Commercial, expires Dec 31 14:06:06 2030 GMT (AffirmTrust_Commercial.crt)
- AffirmTrust Networking, expires Dec 31 14:08:24 2030 GMT (AffirmTrust_Networking.crt)
- AffirmTrust Premium, expires Dec 31 14:10:36 2040 GMT (AffirmTrust_Premium.crt)
- AffirmTrust Premium ECC, expires Dec 31 14:20:24 2040 GMT (AffirmTrust_Premium_ECC.crt)
- Amazon Root CA 1, expires Jan 17 00:00:00 2038 GMT (Amazon_Root_CA_1.crt)
- Amazon Root CA 2, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_2.crt)
- Amazon Root CA 3, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_3.crt)
- Amazon Root CA 4, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_4.crt)
- Atos TrustedRoot 2011, expires Dec 31 23:59:59 2030 GMT (Atos_TrustedRoot_2011.crt)
- Autoridad de Certificacion Firmaprofesional CIF A62634068, expires Dec 31 08:38:15 2030 GMT (Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt)
- Baltimore CyberTrust Root, expires May 12 23:59:00 2025 GMT (Baltimore_CyberTrust_Root.crt)
- Buypass Class 2 Root CA, expires Oct 26 08:38:03 2040 GMT (Buypass_Class_2_Root_CA.crt)
- Buypass Class 3 Root CA, expires Oct 26 08:28:58 2040 GMT (Buypass_Class_3_Root_CA.crt)
- CA Disig Root R2, expires Jul 19 09:15:30 2042 GMT (CA_Disig_Root_R2.crt)
- CFCA EV ROOT, expires Dec 31 03:07:01 2029 GMT (CFCA_EV_ROOT.crt)
- COMODO Certification Authority, expires Dec 31 23:59:59 2029 GMT (COMODO_Certification_Authority.crt)
- COMODO ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO_ECC_Certification_Authority.crt)
- COMODO RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO_RSA_Certification_Authority.crt)
- Certigna, expires Jun 29 15:13:05 2027 GMT (Certigna.crt)
- Certigna Root CA, expires Oct 1 08:32:27 2033 GMT (Certigna_Root_CA.crt)
- Certinomis - Root CA, expires Oct 21 09:17:18 2033 GMT (Certinomis_-_Root_CA.crt)
- Class 2 Primary CA, expires Jul 6 23:59:59 2019 GMT (Certplus_Class_2_Primary_CA.crt)
- Certum Trusted Network CA, expires Dec 31 12:07:37 2029 GMT (Certum_Trusted_Network_CA.crt)
- Certum Trusted Network CA 2, expires Oct 6 08:39:56 2046 GMT (Certum_Trusted_Network_CA_2.crt)
- Chambers of Commerce Root - 2008, expires Jul 31 12:29:50 2038 GMT (Chambers_of_Commerce_Root_-_2008.crt)
- AAA Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo_AAA_Services_root.crt)
- Cybertrust Global Root, expires Dec 15 08:00:00 2021 GMT (Cybertrust_Global_Root.crt)
- D-TRUST Root Class 3 CA 2 2009, expires Nov 5 08:35:58 2029 GMT (D-TRUST_Root_Class_3_CA_2_2009.crt)
- D-TRUST Root Class 3 CA 2 EV 2009, expires Nov 5 08:50:46 2029 GMT (D-TRUST_Root_Class_3_CA_2_EV_2009.crt)
- DST Root CA X3, expires Sep 30 14:01:15 2021 GMT (DST_Root_CA_X3.crt)
- Deutsche Telekom Root CA 2, expires Jul 9 23:59:00 2019 GMT (Deutsche_Telekom_Root_CA_2.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCertGlobalRootCA.pem)
- DigiCert Assured ID Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_Assured_ID_Root_CA.crt)
- DigiCert Assured ID Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert_Assured_ID_Root_G2.crt)
- DigiCert Assured ID Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert_Assured_ID_Root_G3.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_Global_Root_CA.crt)
- DigiCert Global Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert_Global_Root_G2.crt)
- DigiCert Global Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert_Global_Root_G3.crt)
- DigiCert High Assurance EV Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_High_Assurance_EV_Root_CA.crt)
- DigiCert Trusted Root G4, expires Jan 15 12:00:00 2038 GMT (DigiCert_Trusted_Root_G4.crt)

- E-Tugra Certification Authority, expires Mar 3 12:09:48 2023 GMT (E-Tugra_Certification_Authority.crt)
- EC-ACC, expires Jan 7 22:59:59 2031 GMT (EC-ACC.crt)
- EE Certification Centre Root CA, expires Dec 17 23:59:59 2030 GMT (EE_Certification_Centre_Root_CA.crt)
- Entrust.net[339] Certification Authority (2048), expires Jul 24 14:15:12 2029 GMT (Entrust.net_Premium_2048_Secure_Server_CA.crt)
- Entrust Root Certification Authority, expires Nov 27 20:53:42 2026 GMT (Entrust_Root_Certification_Authority.crt)
- Entrust Root Certification Authority - EC1, expires Dec 18 15:55:36 2037 GMT (Entrust_Root_Certification_Authority_-_EC1.crt)
- Entrust Root Certification Authority - G2, expires Dec 7 17:55:54 2030 GMT (Entrust_Root_Certification_Authority_-_G2.crt)
- GDCA TrustAUTH R5 ROOT, expires Dec 31 15:59:59 2040 GMT (GDCA_TrustAUTH_R5_ROOT.crt)
- GTS Root R1, expires Jun 22 00:00:00 2036 GMT (GTS_Root_R1.crt)
- GTS Root R2, expires Jun 22 00:00:00 2036 GMT (GTS_Root_R2.crt)
- GTS Root R3, expires Jun 22 00:00:00 2036 GMT (GTS_Root_R3.crt)
- GTS Root R4, expires Jun 22 00:00:00 2036 GMT (GTS_Root_R4.crt)
- GeoTrust Global CA, expires May 21 04:00:00 2022 GMT (GeoTrust_Global_CA.crt)
- GeoTrust Primary Certification Authority, expires Jul 16 23:59:59 2036 GMT (GeoTrust_Primary_Certification_Authority.crt)
- GeoTrust Primary Certification Authority - G2, expires Jan 18 23:59:59 2038 GMT (GeoTrust_Primary_Certification_Authority_-_G2.crt)
- GeoTrust Primary Certification Authority - G3, expires Dec 1 23:59:59 2037 GMT (GeoTrust_Primary_Certification_Authority_-_G3.crt)
- GeoTrust Universal CA, expires Mar 4 05:00:00 2029 GMT (GeoTrust_Universal_CA.crt)
- GeoTrust Universal CA 2, expires Mar 4 05:00:00 2029 GMT (GeoTrust_Universal_CA_2.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign_ECC_Root_CA_-_R4.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign_ECC_Root_CA_-_R5.crt)
- GlobalSign Root CA, expires Jan 28 12:00:00 2028 GMT (GlobalSign_Root_CA.crt)
- GlobalSign, expires Dec 15 08:00:00 2021 GMT (GlobalSign_Root_CA_-_R2.crt)
- GlobalSign, expires Mar 18 10:00:00 2029 GMT (GlobalSign_Root_CA_-_R3.crt)
- GlobalSign, expires Dec 10 00:00:00 2034 GMT (GlobalSign_Root_CA_-_R6.crt)
- Global Chambersign Root - 2008, expires Jul 31 12:31:40 2038 GMT (Global_Chambersign_Root_-_2008.crt)
- Go Daddy Class 2 Certification Authority, expires Jun 29 17:06:20 2034 GMT (Go_Daddy_Class_2_CA.crt)
- Go Daddy Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Go_Daddy_Root_Certificate_Authority_-_G2.crt)
- Hellenic Academic and Research Institutions ECC RootCA 2015, expires Jun 30 10:37:12 2040 GMT (Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt)
- Hellenic Academic and Research Institutions RootCA 2011, expires Dec 1 13:49:52 2031 GMT (Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt)
- Hellenic Academic and Research Institutions RootCA 2015, expires Jun 30 10:11:21 2040 GMT (Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt)
- Hongkong Post Root CA 1, expires May 15 04:52:29 2023 GMT (Hongkong_Post_Root_CA_1.crt)
- ISRG Root X1, expires Jun 4 11:04:38 2035 GMT (ISRG_Root_X1.crt)
- IdenTrust Commercial Root CA 1, expires Jan 16 18:12:23 2034 GMT (IdenTrust_Commercial_Root_CA_1.crt)
- IdenTrust Public Sector Root CA 1, expires Jan 16 17:53:32 2034 GMT (IdenTrust_Public_Sector_Root_CA_1.crt)
- Imprivata Embedded Code Signing CA, expires Sep 7 16:20:00 2033 GMT (Imprivata.crt)
- Izenpe.com[340], expires Dec 13 08:27:25 2037 GMT (Izenpe.com[341].crt)
- LuxTrust Global Root 2, expires Mar 5 13:21:57 2035 GMT (LuxTrust_Global_Root_2.crt)

339. http://Entrust.net
340. http://Izenpe.com
341. http://Izenpe.com

- Microsec e-Szigno Root CA 2009, expires Dec 30 11:30:18 2029 GMT (Microsec_e-Szigno_Root_CA_2009.crt)
- NetLock Arany (Class Gold) Főtanúsítvány, expires Dec 6 15:08:21 2028 GMT (NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt)
- Network Solutions Certificate Authority, expires Dec 31 23:59:59 2029 GMT (Network_Solutions_Certificate_Authority.crt)
- OISTE WISeKey Global Root GA CA, expires Dec 11 16:09:51 2037 GMT (OISTE_WISeKey_Global_Root_GA_CA.crt)
- OISTE WISeKey Global Root GB CA, expires Dec 1 15:10:31 2039 GMT (OISTE_WISeKey_Global_Root_GB_CA.crt)
- OISTE WISeKey Global Root GC CA, expires May 9 09:58:33 2042 GMT (OISTE_WISeKey_Global_Root_GC_CA.crt)
- QuoVadis Root Certification Authority, expires Mar 17 18:33:33 2021 GMT (QuoVadis_Root_CA.crt)
- QuoVadis Root CA 1 G3, expires Jan 12 17:27:44 2042 GMT (QuoVadis_Root_CA_1_G3.crt)
- QuoVadis Root CA 2, expires Nov 24 18:23:33 2031 GMT (QuoVadis_Root_CA_2.crt)
- QuoVadis Root CA 2 G3, expires Jan 12 18:59:32 2042 GMT (QuoVadis_Root_CA_2_G3.crt)
- QuoVadis Root CA 3, expires Nov 24 19:06:44 2031 GMT (QuoVadis_Root_CA_3.crt)
- QuoVadis Root CA 3 G3, expires Jan 12 20:26:32 2042 GMT (QuoVadis_Root_CA_3_G3.crt)
- SSL.com[342] EV Root Certification Authority ECC, expires Feb 12 18:15:23 2041 GMT (SSL.com_EV_Root_Certification_Authority_ECC.crt)
- SSL.com[343] EV Root Certification Authority RSA R2, expires May 30 18:14:37 2042 GMT (SSL.com_EV_Root_Certification_Authority_RSA_R2.crt)
- SSL.com[344] Root Certification Authority ECC, expires Feb 12 18:14:03 2041 GMT (SSL.com_Root_Certification_Authority_ECC.crt)
- SSL.com[345] Root Certification Authority RSA, expires Feb 12 17:39:39 2041 GMT (SSL.com_Root_Certification_Authority_RSA.crt)
- SZAFIR ROOT CA2, expires Oct 19 07:43:30 2035 GMT (SZAFIR_ROOT_CA2.crt)
- SecureSign RootCA11, expires Apr 8 04:56:47 2029 GMT (SecureSign_RootCA11.crt)
- SecureTrust CA, expires Dec 31 19:40:55 2029 GMT (SecureTrust_CA.crt)
- Secure Global CA, expires Dec 31 19:52:06 2029 GMT (Secure_Global_CA.crt)
- Security Communication RootCA2, expires May 29 05:00:39 2029 GMT (Security_Communication_RootCA2.crt)
- Security Communication RootCA1, expires Sep 30 04:20:49 2023 GMT (Security_Communication_Root_CA.crt)
- Sonera Class2 CA, expires Apr 6 07:29:40 2021 GMT (Sonera_Class_2_Root_CA.crt)
- Staat der Nederlanden EV Root CA, expires Dec 8 11:10:28 2022 GMT (Staat_der_Nederlanden_EV_Root_CA.crt)
- Staat der Nederlanden Root CA - G2, expires Mar 25 11:03:10 2020 GMT (Staat_der_Nederlanden_Root_CA_-_G2.crt)
- Staat der Nederlanden Root CA - G3, expires Nov 13 23:00:00 2028 GMT (Staat_der_Nederlanden_Root_CA_-_G3.crt)
- Starfield Class 2 Certification Authority, expires Jun 29 17:39:16 2034 GMT (Starfield_Class_2_CA.crt)
- Starfield Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield_Root_Certificate_Authority_-_G2.crt)
- Starfield Services Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield_Services_Root_Certificate_Authority_-_G2.crt)
- SwissSign Gold CA - G2, expires Oct 25 08:30:35 2036 GMT (SwissSign_Gold_CA_-_G2.crt)
- SwissSign Silver CA - G2, expires Oct 25 08:32:46 2036 GMT (SwissSign_Silver_CA_-_G2.crt)
- T-TeleSec GlobalRoot Class 2, expires Oct 1 23:59:59 2033 GMT (T-TeleSec_GlobalRoot_Class_2.crt)
- T-TeleSec GlobalRoot Class 3, expires Oct 1 23:59:59 2033 GMT (T-TeleSec_GlobalRoot_Class_3.crt)
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, expires Oct 25 08:25:55 2043 GMT (TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt)
- TWCA Global Root CA, expires Dec 31 15:59:59 2030 GMT (TWCA_Global_Root_CA.crt)
- TWCA Root Certification Authority, expires Dec 31 15:59:59 2030 GMT (TWCA_Root_Certification_Authority.crt)

342. http://SSL.com
343. http://SSL.com
344. http://SSL.com
345. http://SSL.com

- Government Root Certification Authority, expires Dec 5 13:23:33 2032 GMT (Taiwan_GRCA.crt)
- TeliaSonera Root CA v1, expires Oct 18 12:00:50 2032 GMT (TeliaSonera_Root_CA_v1.crt)
- TrustCor ECA-1, expires Dec 31 17:28:07 2029 GMT (TrustCor_ECA-1.crt)
- TrustCor RootCert CA-1, expires Dec 31 17:23:16 2029 GMT (TrustCor_RootCert_CA-1.crt)
- TrustCor RootCert CA-2, expires Dec 31 17:26:39 2034 GMT (TrustCor_RootCert_CA-2.crt)
- Trustis FPS Root CA, expires Jan 21 11:36:54 2024 GMT (Trustis_FPS_Root_CA.crt)
- UCA Extended Validation Root, expires Dec 31 00:00:00 2038 GMT (UCA_Extended_Validation_Root.crt)
- UCA Global G2 Root, expires Dec 31 00:00:00 2040 GMT (UCA_Global_G2_Root.crt)
- USERTrust ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust_ECC_Certification_Authority.crt)
- USERTrust RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust_RSA_Certification_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G4, expires Jan 18 23:59:59 2038 GMT (VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt)
- VeriSign Class 3 Public Primary Certification Authority - G5, expires Jul 16 23:59:59 2036 GMT (VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt)
- VeriSign Universal Root Certification Authority, expires Dec 1 23:59:59 2037 GMT (VeriSign_Universal_Root_Certification_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G3, expires Jul 16 23:59:59 2036 GMT (Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt)
- XRamp Global Certification Authority, expires Jan 1 05:37:19 2035 GMT (XRamp_Global_CA_Root.crt)
- certSIGN ROOT CA, expires Jul 4 17:20:04 2031 GMT (certSIGN_ROOT_CA.crt)
- ePKI Root Certification Authority, expires Dec 20 02:31:27 2034 GMT (ePKI_Root_Certification_Authority.crt)
- thawte Primary Root CA, expires Jul 16 23:59:59 2036 GMT (thawte_Primary_Root_CA.crt)
- thawte Primary Root CA - G2, expires Jan 18 23:59:59 2038 GMT (thawte_Primary_Root_CA_-_G2.crt)
- thawte Primary Root CA - G3, expires Dec 1 23:59:59 2037 GMT (thawte_Primary_Root_CA_-_G3.crt)

Notes for Release 11.01.130

Software:	Version	11.01.130
Release Date:	2019-07-24	
Release Notes:	Version	RN-1101130-1
Last update:	2019-07-23	

- Supported Devices 11.01.130 (see page 3391)
- Component Versions 11.01.130 (see page 3392)
- General Information 11.01.130 (see page 3396)
- Known Issues 11.01.130 (see page 3397)
- Security Fixes 11.01.130 (see page 3399)
- New Features 11.01.130 (see page 3400)
- Resolved Issues 11.01.130 (see page 3401)

Supported Devices 11.01.130

IGEL devices:	
UD2-LX:	UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Devices Supported by IGEL OS 11 (see page 3391).

Component Versions 11.01.130

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.3.0.5
deviceTRUST Citrix Channel	19.1.200.2
Evidian AuthMgr	1.5.7116
Evince PDF Viewer	3.18.2-1ubuntu4.3
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.8.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	5.3.12
Open VPN	2.3.10-1ubuntu2.1
Zulu JRE	8.38.0.13
Parallels Client (64 bit)	16.5.2.20595
Remote Viewer (Red Hat Virtualization)	7.0-igel47
Spice GTK (Red Hat Virtualization)	0.35
Spice Protocol (Red Hat Virtualization)	0.12.14
Usbredir (Red Hat Virtualization)	0.8.0
Teradici PCoIP Software Client	19.05.4-18.04
ThinLinc Client	4.9.0-5775
ThinPrint Client	7.5.88

Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel16
VNC Viewer	1.8.0+git20180123-igel1
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B048
Olympus driver for dictation	20180621
Philips Speech Driver	12.6.36

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.6
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.1.0

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.9.620
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.0.23
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.30-1igel3

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.0.0.6

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.14
OpenSSH Client	7.2p2-4ubuntu2.7
OpenSSH Server	7.2p2-4ubuntu2.7
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	18.3.3-1igel57
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190301-igel870
Graphics Driver ATI/RADEON	18.1.0-1igel854
Graphics Driver ATI/AMDGPU	18.1.0-1igel853
Graphics Driver Nouveau (Nvidia Legacy)	1.0.15-2igel775
Graphics Driver Nvidia	410.93-0ubuntu1
Graphics Driver Vboxvideo	5.2.18-dfsg-2igel17
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.5-1ubuntu1igel750
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.0-1ubuntu1igel748
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu1igel813
Kernel	4.18.20 #mainline-udos-r2755
Xorg X11 Server	1.19.6-1ubuntu4.2igel842

Xorg Xephyr	1.19.6-1ubuntu4.2igel842
CUPS Printing Daemon	2.1.3-4ubuntu0.7igel23
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.2igel58
ModemManager	1.6.8-2ubuntu1igel2
GStreamer 0.10	0.10.36-2ubuntu0.1
GStreamer 1.x	1.14.4-1ubuntu1igel203
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB
VPN OpenConnect
Scanner support
VirtualBox

- **Features with Limited Functionality**

Cisco JVDI Client

General Information 11.01.130

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver.

Known Issues 11.01.130

Citrix

- With activated DRI3 and AMD GPU, Citrix **H.264 acceleration** plugin could **freeze**. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection of H264**, **MPEG1** and **MPEG2**. GStreamer 1.0 is used if browser content redirection is active.
- **Browser content redirection** does not work with **activated DRI3** and hardware accelerated **H.264 deep compression codec**.
- Citrix **StoreFront** login with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is **inserted after start** of Login.
  As a workaround, insert the smartcard before starting StoreFront login.
- When using **Citrix Workspace App 19.03** in combination with **Philips Speech** driver, the session occasionally terminates improperly at logout and hangs.
  As a workaround, the usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- Citrix **H.264 acceleration plugin** does not work with **enabled** server policy "Optimize for 3D graphics workload" in combination with server policy "Use video codec compression" > "For the entire screen".
- To launch **multiple desktop sessions** with **Citrix HDX RTME** and **Citrix H.264 acceleration plugin**, the following registry key must be enabled:
  More...

Parameter	Activate workaround for dual RTME sessions and H264 acceleration
Registry	`ica.workaround-dual-rtme`
Range	enabled / disabled

  This workaround is not applicable when "Enable Secure ICA" is active for the specific delivery group.

VMware Horizon

- **External drives** mounted already before connection **do not appear in the remote desktop**.
  Workaround: mapping the directory / media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, if you want to use **USB redirection** for your storage devices: Note that the **USB on-insertion feature** is only working if the **client drive mapping** is switched off.
    In the IGEL Setup client, **drive mapping** can be found under **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping**.
    It is also recommended to disable local **Storage Hotplug** under Setup **> Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, if you use **drive mapping** instead, it is recommended to either **switch off USB redirection entirely** or at least to **deny storage devices** by adding a filter to the

USB class rules.
Furthermore, Horizon Client relies on the OS to mount the storage devices itself. Enable **Storage Hotplug** under Setup **>Devices > Storage Devices > Storage Hotplug**. The **Number of storage hotplug devices** has to be set to at least 1.

Parallels Client

- **Native USB redirection does not work** with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with disabled FIPS support.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign smartcards**.

Multimedia

- Multimedia **redirection with GStreamer** could fail with the **Nouveau GPU driver**.

Base system

- On **NVIDIA GPU drivers**, the reported **resolutions of a display** may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

Security Fixes 11.01.130

Firefox

- Updated **Firefox** browser to version **60.8.0 ESR**.
- Fixed **mfsa2019-22** security issues:
  More...

  CVE-2019-9811, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11729, CVE-2019-11715, CVE-2019-11717, CVE-2019-11719, CVE-2019-11730 and CVE-2019-11709.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues:
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9795, CVE-2019-9796, CVE-2018-18506 and CVE-2019-9788.
- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

New Features 11.01.130

Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at https://support.citrix.com/article/CTX237727.

Base system

- Replaced **timesyncd** with **chrony NTP**.
  A new registry key:
  More...

Parameter	Use NTP Servers from DNS SRV record
Registry	`system.time.ntp_use_dnssrv_timeservers`
Value	enabled / disabled

Evidian

- Integrated **Evidian AuthMgr** version **1.5.7116**.

Resolved Issues 11.01.130

VMware Horizon

- Added a possibility to use the **rollback variant of the Horizon Client**.
  More...

Parameter	Allow rollback to former client variant
Registry	`vmware.view.allow-client-rollback`
Value	enabled / disabled

Base system

- Fixed **NTP synchronization problems** with changing the NTP client from **timesyncd** to **chrony**.
- Fixed **USB printer aliases**.

X11 system

- Fixed **screen corruption with DPMS** and enabled **composite manager**.
- Added consideration of **hardware limits** for choosing **automatic resolution in Xorg config** (currently only for IGEL hardware).

Hardware

- Fixed **black screen** issue with some monitors and 2560x1440 resolution (occurred on **UD2 LX50** and **other Intel GPUs**).

Notes for Release 11.01.120

Software:	Version	11.01.120
Release Date:	2019-07-05	
Release Notes:	Version	RN-1101120-1
Last update:	2019-07-05	

- Supported Devices 11.01.120 (see page 3403)
- Component Versions 11.01.120 (see page 3404)
- General Information 11.01.120 (see page 3408)
- Security Fixes 11.01.120 (see page 3409)
- New Features 11.01.120 (see page 3410)
- Resolved Issues 11.01.120 (see page 3411)

Supported Devices 11.01.120

IGEL devices:	
UD2-LX:	UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

See also Devices Supported by IGEL OS 11 (see page 3403).

Component Versions 11.01.120

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.3.0.5
deviceTRUST Citrix Channel	19.1.200.2
Evidian AuthMgr	1.5.6840
Evince PDF Viewer	3.18.2-1ubuntu4.3
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.7.2
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	5.3.12
Open VPN	2.3.10-1ubuntu2.1
Zulu JRE	8.38.0.13
Parallels Client (64 bit)	16.5.2.20595
Remote Viewer (Red Hat Virtualization)	7.0-igel47
Spice GTK (Red Hat Virtualization)	0.35
Spice Protocol (Red Hat Virtualization)	0.12.14
Usbredir (Red Hat Virtualization)	0.8.0
Teradici PCoIP Software Client	19.05.4-18.04
ThinLinc Client	4.9.0-5775
ThinPrint Client	7.5.88

Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel16
VNC Viewer	1.8.0+git20180123-igel1
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B048
Olympus driver for dictation	20180621
Philips Speech Driver	12.6.36

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.6
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.1.0

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.9.620
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.0.23
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.30-1igel3

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.0.0.6

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.14
OpenSSH Client	7.2p2-4ubuntu2.7
OpenSSH Server	7.2p2-4ubuntu2.7
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	18.3.3-1igel57
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190301-igel870
Graphics Driver ATI/RADEON	18.1.0-1igel854
Graphics Driver ATI/AMDGPU	18.1.0-1igel853
Graphics Driver Nouveau (Nvidia Legacy)	1.0.15-2igel775
Graphics Driver Nvidia	410.93-0ubuntu1
Graphics Driver Vboxvideo	5.2.18-dfsg-2igel17
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.5-1ubuntu1igel750
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.0-1ubuntu1igel748
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu1igel813
Kernel	4.18.20 #mainline-udos-r2755
Xorg X11 Server	1.19.6-1ubuntu4.2igel842

Xorg Xephyr	1.19.6-1ubuntu4.2igel842
CUPS Printing Daemon	2.1.3-4ubuntu0.7igel23
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.2igel58
ModemManager	1.6.8-2ubuntu1igel2
GStreamer 0.10	0.10.36-2ubuntu0.1
GStreamer 1.x	1.14.4-1ubuntu1igel203
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB
VPN OpenConnect
Scanner support
VirtualBox

- **Features with Limited Functionality**

Cisco JVDI Client	12.1

General Information 11.01.120

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Security Fixes 11.01.120

Firefox

- Updated Firefox browser to version **60.7.2 ESR**.
- Fixed **mfsa2019-19** security issue CVE-2019-11708.
- Fixed **mfsa2019-18** security issue CVE-2019-11707.
- Fixed **mfsa2019-08** security issues.
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,
  CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.

Base system

- Fixed kernel TCP vulnerabilities **CVE-2019-11477**: SACK Panic, **CVE-2019-11478**: SACK Slowness and **CVE-2019-11479**: Excess Resource Consumption Due to Low MSS Values.
- Changed **minimally allowed MSS size** to **'1000'** to prevent possible Denial-of-Service attacks.

New Features 11.01.120

Citrix

- Added support for **Citrix Workspace Launcher** functionality as described at https://support.citrix.com/article/CTX237727.

Teradici PCoIP Client

- Updated **Teradici PCoIP Client** to version **19.05.4**.

Resolved Issues 11.01.120

Citrix

- SpaceMouse: Improved **USB handling**.
- Citrix Workspace App 19.03: Improved **USB redirection handling**.

Network

- Fixed: The **second Ethernet interface** did not get configured when the first one was disabled.

Base system

- Fixed **license expiry warning** at boot. Before this fix, in some cases the warning wrongly appeared at every boot.
- Fixed: **System logout** waits for Citrix logout now.

Appliance Mode

- Fixed: **In-session control bar** could not be deactivated in **Citrix Self-Service appliance mode**.

X11 system

- Fixed: Problems with **internal graphic cards** and **Nvidia graphic cards**.

RD Web Access

- Fixed not starting **RDP Remote Applications**.

Hardware

- Fixed **not working network** on Beckhoff CB3163, CB6263 and CB6363 systems.
- Fixed **not working network** on Lex 3I380D.
- Fixed **black screen** issue with some monitors and 2560x1440 resolution (occurred on UD2 LX50).
- Added possibility to **change** some **DRM settings** and limit the **DisplayPort lane bandwidth** on Intel devices.
- Added **new registry keys**:
  More...

Parameter	Use best graphic mode for all screens on console.
Registry	`x.drivers.kms.best_console_mode`
Range	[Default] [Enabled] [Disabled]
Info: "Default" is enabled in most cases.	

Parameter	Limit the maximum console resolution width to this value.
Registry	`x.drivers.kms.max_console_width`
Type	Integer
Value	"0"

Info: "0" means default setting. Use the default setting.	
Parameter	Limit the maximum console resolution height to this value.
Registry	`x.drivers.kms.max_console_height`
Type	Integer
Value	"0"
Info: "0" means default setting. Use the default setting.	
Parameter	Set graphic kernel driver debug level.
Registry	`x.drivers.kms.debug_level`
Range	[No debug] [Basic] [Basic + core] [Basic + core + atomic] [Full]
Info: Warning log will grow very fast.	

Only for Intel i915 driver:

Parameter	Limit the maximum DisplayPort lane link rate.
Registry	`x.drivers.intel.max_dp_link_rate`
Range	[default] [1.62Gbps] [2.16Gbps] [2.7Gbps] [3.24Gbps] [4.32Gbps] [5.4Gbps] [6.48Gbps] [8.1Gbps]
Info: "Default" means hardware default limit.	

Notes for Release 11.01.110

Software:	Version	11.01.110
Release Date:	2019-06-06	
Release Notes:	Version	RN-1101110-1
Last update:	2019-06-06	

- Supported Devices 11.01.110 (see page 3414)
- Component Versions 11.01.110 (see page 3415)
- General Information 11.01.110 (see page 3419)
- Security Fixes 11.01.110 (see page 3420)
- Known Issues 11.01.110 (see page 3421)
- New Features 11.01.110 (see page 3423)
- Resolved Issues 11.01.110 (see page 3431)

Supported Devices 11.01.110

IGEL devices:	
UD2-LX:	UD2-LX 50 UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

For supported IGEL OS 11 third-party devices, see Devices Supported by IGEL OS 11.[346]

346. https://wiki.test.toolchain.igel.kreuzwerker.net/os11-supported-hardware

Component Versions 11.01.110

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.8.0-2235
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	19.3.0.5
deviceTRUST Citrix Channel	19.1.200.2
Evidian AuthMgr	1.5.6840
Evince PDF Viewer	3.18.2-1ubuntu4.3
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.7.0
IBM iAccess Client Solutions	1.1.8.1
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	
deviceTRUST RDP Channel	19.1.200.2
NCP Secure Enterprise Client	5.10_rev40552
NX Client	5.3.12
Open VPN	2.3.10-1ubuntu2.1
Zulu JRE	8.36.0.1
Parallels Client (64 bit)	16.5.2.20595
Remote Viewer (Red Hat Virtualization)	7.0-igel47
Spice GTK (Red Hat Virtualization)	0.35
Spice Protocol (Red Hat Virtualization)	0.12.14
Usbredir (Red Hat Virtualization)	0.8.0
Teradici PCoIP Software Client	19.05.1-18.04
ThinLinc Client	4.9.0-5775
ThinPrint Client	7.5.88

Totem Media Player	2.30.2
Parole Media Player	1.0.1-0ubuntu1igel16
VNC Viewer	1.8.0+git20180123-igel1
VMware Horizon Client	5.0.0-12557422
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Grundig Business Systems dictation driver	
Nuance Audio Extensions for dictation	B048
Olympus driver for dictation	20180621
Philips Speech Driver	12.6.36

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.6
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.1.0

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.9.620
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.0.23
PKCS#11 Library 90meter	20190522
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.30-1igel3

Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1
Cherry USB2LAN Proxy	3.0.0.6

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.14
OpenSSH Client	7.2p2-4ubuntu2.7
OpenSSH Server	7.2p2-4ubuntu2.7
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	18.3.3-1igel57
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20190301-igel870
Graphics Driver ATI/RADEON	18.1.0-1igel854
Graphics Driver ATI/AMDGPU	18.1.0-1igel853
Graphics Driver Nouveau (Nvidia Legacy)	1.0.15-2igel775
Graphics Driver Nvidia	410.93-0ubuntu1
Graphics Driver Vboxvideo	5.2.18-dfsg-2igel17
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.5-1ubuntu1igel750
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.0-1ubuntu1igel748
Input Driver VMMouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu1igel813
Kernel	4.18.20 #mainline-udos-r2519
Xorg X11 Server	1.19.6-1ubuntu4.2igel842

Xorg Xephyr	1.19.6-1ubuntu4.2igel842
CUPS Printing Daemon	2.1.3-4ubuntu0.7igel23
PrinterLogic	18.2.1.128
Lightdm Graphical Login Manager	1.18.3-0ubuntu1.1
XFCE4 Window Manager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.2igel58
ModemManager	1.6.8-2ubuntu1igel2
GStreamer 0.10	0.10.36-2ubuntu0.1
GStreamer 1.x	1.14.4-1ubuntu1igel203
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB
VPN OpenConnect
Scanner support
VirtualBox

- **Features with Limited Functionality**

Cisco JVDI Client	12.1

General Information 11.01.110

The following clients and features are not supported anymore

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Security Fixes 11.01.110

Firefox

- Updated Mozilla Firefox to version **60.7.0esr**.
- Fixed **mfsa2019-08** security issues.
  More...

  CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,

  CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixed **mfsa2019-05** security issues CVE-2018-18356 and CVE-2019-5785.
- Fixed **mfsa2019-02** security issues CVE-2018-18500, CVE-2018-18505 and CVE-2018-18501.
- Firefox is now allowed to access **YubiKey** (FIDO/U2F) if **AppArmor** is active.

Base system

- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.
  More...

  CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,

  CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,

  CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,

  CVE-2018-4386 and CVE-2018-4372.

Known Issues 11.01.110

Citrix

- With an **activated DRI3** and an **AMD GPU**, **Citrix H.264 acceleration plugin** could freeze. A selective H.264 mode (API v2) is not affected by this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with **multimedia redirection** of H.264, MPEG1 and MPEG2. GStreamer1.0 is used if **browser content redirection** is active.
- **Browser content redirection** does not work with **activated DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront Login** with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is inserted after the start of Login.
  As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs.
  As a workaround, the usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- **Citrix H.264 acceleration plugin** does not work with the **enabled** server policy **Optimize for 3D graphics workload** in combination with the server policy **Use video codec compression > For the entire screen**.

VMware Horizon

- **External drives** are mounted already before connection, do not appear in the **remote desktop**. Workaround: Mapping the directory/media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using **USB redirection for storage devices**: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using **drive mapping** instead, it is recommended either to switch off USB redirection entirely or at least to deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug** has to be enabled and the **Number of storage hotplug devices** has to be set to at least 1.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with **disabled FIPS support**.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign** smartcards.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the **Nouveau GPU driver**.

Base system

- On **NVIDIA GPU** drivers, the **reported resolutions** of a display may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

New Features 11.01.110

Citrix

- Integrated **Citrix Workspace app 19.03**.
  Added new registry key to support **1536-bit RSA** keys for client authentication.
  More...

Parameter	Enable RSA 1536 cipher suit
Registry	`ica.allregions.enabl_rsa_1536`
Range	factory default / false / true

- Added new registry key to enable **different cipher suites** for client authentication.
  More...

Parameter	Enables different cipher suites
Registry	`ica.allregions.sslciphers`
Range	factory default / ALL / GOV / COM

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL
- Added new registry key to support **keyboard layout syncroniyation**.

More...

Parameter	Keyboard layout synchronization
Registry	`ica.modules.virtualdriver.keyboardsync.enable`
Value	enabled / disabled

- Updated **Citrix HDX RTME**, used for optimization of Skype for Business, to version **2.8.0-2235**

RDP/IGEL RDP Client 2

- Added **Field Collection to RDP** session server page

VMware Horizon

- Added parameters to **specify webcam frame size** and **rate for RTAV**.
  More...

Parameter	Webcam frame width
Registry	`vmware.view.rtav-frame-width`
Value	<empty_string>
Parameter	Webcam frame height

Registry	`vmware.view.rtav-frame-height`
Value	<empty_string>
Parameter	Webcam frame rate
Registry	`vmware.view.rtav-frame-rate`
Value	<empty_string>

- Updated **Horizon Client** to version **5.0.0-12557422**
- Added possibility to easily evaluate **Horizon Blast decoder states**. By default sessions are evaluated after usage and the result is written into the journal log.
  This can also be used with GUI notifications at runtime.

Teradici PCoIP Client

- Added **Teradici PCoIP** Client version **19.05.1**. This feature requires an additional license.
  More...

IGEL Setup	**System > Firmware Customization > Features**
Parameter	Teradici PCoIP Client
Registry	`services.addition_teradici_pcoip_client.enabled`
Value	enabled / disabled
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Use IGEL Setup for configuration
Registry	`sessions.pcoip<NR>.options.igel-connection`
Value	enabled / disabled
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Server
Registry	`sessions.pcoip<NR>.options.address`
Value	<empty_string>
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Connection settings**
Parameter	Server certificate verification mode
Registry	`sessions.pcoip<NR>.options.security-mode`

Range	[Not required][Warn but allow][Full verification]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Login**
Parameter	Authentication type
Registry	`sessions.pcoip<NR>.options.auth-type`
Range	[Password authentication][Smartcard authentication]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**
Parameter	Window mode
Registry	`sessions.pcoip<NR>.options.window-mode`
Range	[User defined][Fullscreen One Monitor][Fullscreen All Monitors] [Window]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**
Parameter	User interface translation
Registry	`sessions.pcoip<NR>.options.language`
Range	[System setting][English] [German] [French][Spanish] [Portuguese (EU)] [Portuguese (Brazil)] [Italian][Japanese] [Chinese(Simplified)] [Chinese(Traditional)]
IGEL Setup	**Sessions > Teradici PCoIP Client > PCoIP Sessions > PCoIP Session > Window**
Parameter	Log level
Registry	`sessions.pcoip<NR>.options.log-level`
Range	[Critical][Error][Info][Debug]

Network

- Added a mechanism for retrieving the **SCEP challenge password** with a **custom script**. Setting the following registry key to true enables the use of the script. The registry key `network.scepclient.cert%.crypt_password` will be ignored. (The script may use it for its own purpose though.)
  More...

Parameter	Use Challenge Password Command

Registry	`network.scepclient.cert%.use_challenge_password_command`
Value	enabled / disabled

- If the above key is **true**, the value of this key will be passed to **bash for execution**. It happens when the SCEP challenge password is needed for creating a **certificate signing request**. The script is supposed to output the challenge password on its standard output. For convenience any carriage return characters are stripped off the script before execution by bash.
  More...

Parameter	Challenge Password Command
Registry	`network.scepclient.cert%.challenge_password_command`
Value	<empty_string>

Wi-Fi

- Added support for **Realtek 8821CE wireless cards**.

Smartcard

- Added **90meter** smart card library. This feature requires an additional license.
  More...

IGEL Setup	**System > Firmware Customization > Features**
Parameter	90meter Smart Card Support
Registry	`services.addition_smartcard_90meter.enabled`
Value	enabled / disabled
IGEL Setup	**Sessions > Horizon Client > Horizon Client Global > Smartcard**
Parameter	Horizon logon with smartcards supported by 90meter library
Registry	`vmware.view.pkcs11.use_90meter`
Value	enabled / disabled
IGEL Setup	**Sessions > Browser > Browser Global > Smartcard Middleware**
Parameter	90meter Security Device
Registry	`browserglobal.security_device.90meter`
Value	enabled / disabled
IGEL Setup	**Security > Smartcard > Middleware**

Parameter	90meter
Registry	`scard.pkcs11.use_90meter`
Value	enabled / disabled

Base System

- Added package **ldap-utils** which can be used by **custom scripts**.
- Updated **libwebkit2gtk-4.0-37** to version **1.24.2**.
  More...

  CVE-2019-8595, CVE-2019-8607, CVE-2019-8615, CVE-2019-6251,

  CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378,

  CVE-2018-4382, CVE-2018-4392, CVE-2018-4416, CVE-2018-4345,

  CVE-2018-4386, CVE-2018-4372
- Updated **EULA** displayed in **OSC** and **IGEL Setup Assistant**.
- When the **IGEL Setup Assistant** is used to download a demo license via WiFi, the **local WiFi manager** will be enabled by default.
- Added possibility to **configure scheduled commands**. Registry keys: `system.cron.*`

Driver

- Updated **deviceTRUST** Client to version **19.1.200**. This release includes support for logical disks attached to the IGEL endpoint, plus bug fixes and stability improvements over the previous 19.1.100 release.
  Logical Disks
  Added support for real-time properties representing the LOGICAL DISKS attached to the IGEL endpoint.
  This includes...
  - DEVICE_LOGICALDISK_X_TYPE – Either Fixed or Removable.
  - DEVICE_LOGICALDISK_X_LABEL – The volume label.
  - DEVICE_LOGICALDISK_X_FILESYSTEM – The type of file system.
  - DEVICE_LOGICALDISK_X_PATHS – The paths that the disk is mounted.
  - DEVICE_LOGICALDISK_X_TOTALMB – The total space available on the disk. This property is only available for mounted disks.
  - DEVICE_LOGICALDISK_X_FREEMB – The free space available on the disk. This property is only available for mounted disks.
  - DEVICE_LOGICALDISK_X_NAME – The name of the underlying physical disk.
  - DEVICE_LOGICALDISK_X_VENDORID – The vendor identifier uniquely identifying the manufacturer. This property is only available for USB or PCI connected devices.
  - DEVICE_LOGICALDISK_X_PRODUCTID – The product identifier uniquely identifying the product. This property is only available for USB or PCI connected devices.
  - DEVICE_LOGICALDISK_X_SERIALNUMBER – The serial number of the physical disk.
  - DEVICE_LOGICALDISK_X_BUSTYPE – The storage bus type linked to the physical disk.
  - DEVICE_LOGICALDISK_COUNT – The number of logical disks.

- Added registry keys to **modify the intel graphic driver usage** of framebuffer compression and power management.
  More...

Parameter	Power saving display C-States to use.
Registry	`x.drivers.intel.dc_setting`
Range	[Default][Disable][Up to DC5][Up to DC6]
Parameter	Use framebuffer compression.
Registry	`x.drivers.intel.fbc_setting`
Range	[Default][Disable]

X11 System

- Added new registry keys to **change the xorg input driver** for a input device class.
  More...

  For keyboards:

Parameter	Xorg driver to use
Registry	`userinterface.keyboard.driver`
Range	[Evdev] [Libinput]

  For touchpads:

Parameter	Xorg driver to use
Registry	`userinterface.touchpad.driver`
Range	[Evdev] [Synaptics] [Libinput]

  For touchscreens:

Parameter	Xorg driver to use
Registry	`userinterface.touchscreen.xorg_driver`
Range	[Evdev][Libinput]

  For mouse:

Parameter	Xorg driver to use
Registry	`userinterface.mouse.driver`
Range	[Evdev][Libinput]

- Added some registry keys to **disable loading of DRM kernel modules** (graphic).

More...

Parameter	Disable the loading of the RADEON DRM driver.
Registry	`x.drivers.ati.disable`
Value	enabled / disabled
Parameter	Disable the loading of the AMDGPU DRM driver.
Registry	`x.drivers.amdgpu.disable`
Value	enabled / disabled
Parameter	Disable the loading of the i915 DRM driver.
Registry	`x.drivers.intel.disable`
Value	enabled / disabled
Parameter	Disable the loading of the NVIDIA kernel driver.
Registry	`x.drivers.nvidia.disable`
Value	enabled / disabled
Parameter	Disable the loading of the NOUVEAU DRM driver.
Registry	`x.drivers.nouveau.disable`
Value	enabled / disabled
Parameter	Disable the loading of the QXL DRM driver.
Registry	`x.drivers.qxl.disable`
Value	enabled / disabled
Parameter	Disable the loading of the VMGFX DRM driver.
Registry	`x.drivers.vmware.disable`
Value	enabled / disabled
Parameter	Disable the loading of the VBOXVIDEO DRM driver.
Registry	`x.drivers.vboxvideo.disable`
Value	enabled / disabled

Java

- Replaced **Oracle JRE** by **AZUL's Zulu JRE** version **8.36.0.1**.

Resolved Issues 11.01.110

OSC Installer

- Fixed OSC Installer to **not disable EFI**, if MSDOS partitioning was choosen.

Citrix

- Fixed stability issues with **Citrix Browser Content Redirection**.
- Fixed crash when **H264 acceleration** and **RTME** will be used on two or more concurrent **VDI sessions**.

RDP/IGEL RDP Client 2

- Added registry key to use **rdpglobal window settings** for remote apps.
  More...

Parameter	Enable global windows settings for remote app
Registry	`rdp.winconnect.enable-global-window-settings-for-remote-app`
Value	enabled / disabled

VMware Horizon

- Added recognition for **password change** and **password expired dialog** in **Horizon local logon sessions** or **appliance mode**
- Fixed the configuration choice to use the **relative mouse feature**

Firefox

- Fixed firefox not accepting **proxy credentials** from setup.
- Fixed **print hotkey disable option** not working with Firefox 60.
- Fixed `browserglobal.app.local_subdirs_whitelist` not working.
- Updated **Firefox** browser to version **60.7.0esr**.
- Fixes for **mfsa2019-08**.
  More...
  - CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793,
  - CVE-2019-9795, CVE-2019-9796, CVE-2018-18506, CVE-2019-9788.
- Fixes for **mfsa2019-05**, also known as: CVE-2018-18356, CVE-2019-5785.
- Fixes for **mfsa2019-02**, also known as: CVE-2018-18500, CVE-2018-18505, CVE-2018-18501.

Network

- Fixed: Failure to reach **SCEP server** in the client certificate renewal phase resulted in loss of SCEP server and client certificates.
- Changed **e1000e driver** to out of tree version **3.4.2.3** - directly from Intel.
- Changed **igb driver** to out of tree version **5.3.5.22** - directly from Intel.
- Added possibility to switch between **thirdparty** and **kernel intel IGB network driver**.
  More...

Parameter	Use thirdparty igb kernel module.
Registry	`network.drivers.igb.prefer_thirdparty`
Value	[Auto] [Yes] [No]
Info: "Auto" uses thirdparty in most cases	

- Added possibility to switch between **thirdparty** and **kernel intel E1000E network driver**.
  More...

Parameter	Use thirdparty e1000e kernel module.
Registry	`network.drivers.e1000e.prefer_thirdparty`
Value	[Auto] [Yes] [No]
Info: "Auto" uses thirdparty in most cases	

- Fixed instability with **netmounts with static ip configuration**.
- Added possibility to switch between **thirdparty r8168** and **kernel r8169 realtek network driver**.
  More...

Parameter	Use thirdparty r8168 kernel module.
Registry	`network.drivers.r8169.prefer_r8168`
Value	[Auto] [Yes] [No]
Info: "Auto" uses r8169 in most cases	

- Added possibility to choose the variant of the **realtek r8168 driver**.
  More...

Parameter	Choose realtek r8168 variant (only if prefer r8168 is chosen).
Registry	`network.drivers.r8169.r8168_variant`
Value	[Default][No NAPI][NAPI]
Info: "Auto" uses NAPI in most cases	

Wi-Fi

- Fixed non working **TP Link Archer T2UH**.

Imprivata

- Fixed **Fast User Switching** with **Citrix** connections.

Smartcard

- Fixed **OpenSC** setting `max_send_size` for reader driver pcsc in `/etc/opensc/opensc.conf`.

- Fixed **Dell KB813 smartcard keyboard** in combination with certain smartcards driven by **OpenSC PKCS#11** module. Before this fix authentication to **Citrix StoreFront** and **VMWare Horizon** failed.

Base system

- Fixed retrieving of **serial number** from display.
- Fixed **random 90 seconds shutdown delay** (systemd).
- Fixed wrong behavior with **expired evaluation licenses** in some cases.
- Fixed a bug in the **screenlock countdown** that occurred when display of remaining seconds was not desired.
- Added **apparmor rule** to allow tcpdump to write to `/debuglog`.
- Bugfix **hotkey setting need reboot**.
- Fixed **UD2 screen goes black** problem with certain multimonitor configurations.
- Fixed **gtk-3 icon sizes** for **High-DPI** configurations.
- Enhanced **bootloader** to allow the setting of some kernel commandline parameters with registry keys.
  More...

Parameter	Disable use of APIC controller.
Registry	`system.kernel.bootparams.noapic`
Value	enabled / disabled
Parameter	Disable use of ACPI.
Registry	`system.kernel.bootparams.noacpi`
Value	enabled / disabled
Parameter	Use only one CPU core and disable all others.
Registry	`system.kernel.bootparams.nosmp`
Value	enabled / disabled
Parameter	Enable debug console on serial port 1.
Registry	`system.kernel.bootparams.serial_console_debug`
Value	enabled / disabled
Parameter	Limit CPU core usage (0 means no limit).
Registry	`system.kernel.bootparams.maxcpus`
Value	"0"
Parameter	Set maximum allowed cstate on intel cpus.

Registry	`system.kernel.bootparams.max_cstate`
Range	[No limit] [1] [2] [3] [4] [5] [6]
Info: Do not limit intel cstate	
Parameter	IOMMU usage setting.
Registry	`system.kernel.bootparams.iommu`
Range	[On] [Off] [Passthrough] [Force]
Info: Use IOMMU if possible	
Parameter	IOMMU usage setting for AMD systems.
Registry	`system.kernel.bootparams.amd_iommu`
Range	[On] [Off]
Info: Use IOMMU if possible	
Parameter	IOMMU usage setting for Intel systems.
Registry	`system.kernel.bootparams.intel_iommu`
Range	[On] [Off]
Info: Use IOMMU if possible	

- Moved the **EULA** page in **IGEL Setup Assistant** into the **demo activation workflow**.
- Added new registry key to set **USB quirks**.
  More...

Parameter	Set XHCI USB quirks to fix some hardware issues.
Registry	`system.kernel.bootparams.xhci-hcd_quirks`
Range	[No quirk] [Spurious Reboot quirk] [Spurious Wakeup quirk][Spurious Reboot Wakeup quirk]

- Lenovo **ThinkCentre M73** needs the `system.kernel.bootparams.xhci-hcd_quirks` registry key set to **Spurious Reboot quirk** to fix reboot after shutdown problem.

Driver

- Updated **deviceTRUST** Client to version **19.1.200**.
  Bug Fixes:
  - Fixed an issue reading the **DEVICE_IGEL_ICG_SERVER** property.
  - Fixed an issue where the **NETWORK** and **LOCATION** property providers could cause the client to freeze if a disconnection occurred whilst these property providers were checking for changes.

- Fixed an **open file handle leak** which lead to the client process reaching its file handle limits when left running for a long period of time.
- Fixed non working **WACOM device DTU-1141B**.

Custom Partition

- Fixed **ownership of extracted data**: don't preserve original owner while extracting data into custom partition.

Storage Devices

- Fixed **auto mounting** of storage devices inside of **Olympus DS-9500 Digital Voice Recorder**.

X11 system

- There is now a registry key to ignore a **3Dconnexion SpaceMouse** for IGEL graphical use (X11). If activated, the **SpaceMouse** is only passed through to the desktop session. If false, it acts also as the standard mouse.
  More...

Parameter	Deactivates a 3Dconnexion SpaceMouse as a standard mouse.
Registry	`userinterface.mouse.spacemouse.x11_ignore`
Value	enabled / disabled

- The following SpaceMouse products are included (VID, PID, Vendor, Product).
  More...

  0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT

  0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman

  0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic

  0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000

  0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse

  0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse

  0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse

  0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse

  0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks

  0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse

  0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro

  0x256F; **; 3Dconnexion; SpaceMouse

- USB device reset via USB powercycle on UD6/UD7 available.
- Fixed screen flicker in some cases if "Force NumLock On" (x.global.forcenumlock) is active.
- Fixed Display Switch utility not starting with some translations.
- Fixed an issue with the noDDC mode not always working as expected.
- Fixed wrongly detected embedded DisplayPort on Dell Wyse 5070 Extended hardware.
- Added the possibility to change an embedded DisplayPort to a normal DisplayPort.

More...

Parameter	Use embedded displayport as normal displayport (reboot required).
Registry	`x.drivers.intel.edp_is_dp`
Range	[default][enable][disable]

- Fixed some multimonitor (>4) issues with Nvidia graphic cards.
- Updated DisplayLink driver to version 5.1.26 to solve some startup issues.
- Fixed configuration from the old Display Switch taking precedence over
- configuration from new Display Switch and preventing changes.

Audio

- Fixed bad quality sound over DisplayPort in a Citrix ICA session or other applications using ALSA API.
- Fixed jack detection of the headphone port in Dell Wyse 3040.
- Fixed configuration of default audio output and input.

Media Player (Parole)

- Fixed a problem where parole media player would hang instead of playing audio while audio-visualization is enabled.

Hardware

- Fixed vanishing mouse cursor on Ryzen 3 devices.
- Fixed issues with non working Touchpad and Trackpoint on Lenovo laptops.
- Hardware detect HP t430.
- Added possibility to use AMDGPU PRO driver instead of the kernel integrated driver.
  Ryzen 3 devices (1200, 1300X, 2200G, 2200U and 2300U) will use the AMDGPU PRO driver if registry key x.drivers.amdgpu.use_amdgpu_pro is set to auto (default).
  New registry key (settings to this key will only work after reboot):
  More...

Parameter	Use AMDGPU PRO driver.
Registry	`x.drivers.amdgpu.use_amdgpu_pro`
Range	[Auto] [True] [False]

Remote Management

- If TC is managed over ICG, then settings do not apply immediately when received in connection stage. The settings must be applied after user prompt dialog.

Notes for Release 11.01.100

Software:	Version 11.01.100
Release Date:	2019-02-15
Release Notes:	RN-1101100-1
Last update:	2019-02-15

- IGEL OS Creator (OSC) (see page 3438)
- IGEL OS 11 (see page 3442)

IGEL OS Creator (OSC)

Supported Devices

IGEL devices:
UD2-LX 40
UD3-LX 51
UD3-LX 50
UD5-LX 50
UD6-LX 51
UD7-LX 10
UD9-LX Touch 41
UD9-LX 40

For supported devices, see Devices Supported by IGEL OS 11 (see page 3438).

- General Information 11.01.100 (see page 3439)
- Component Versions 11.01.100 (see page 3440)

General Information 11.01.100

- **IGEL OS Creator** is used for **IGEL OS 11** installation and recovery on:
  - Supported IGEL hardware
  - IGEL UD Pocket
  - Supported x86 hardware
- Find details in the IGEL OS Creator manual at https://wiki.test.toolchain.igel.kreuzwerker.net/osc-manual

Component Versions 11.01.100

- **Clients**

Product	Version
Oracle JRE	1.8.0_202

- **Smartcard**

Product	Version
Reader Driver MUSCLE CCID	1.4.30-1igel3
Resource Manager PC/SC Lite	1.8.23-1igel1

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.14
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	18.3.3-1igel57
VDPAU Library Version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20181113-igel856
Graphics Driver ATI/RADEON	18.1.0-1igel854
Graphics Driver ATI/AMDGPU	18.1.0-1igel853
Graphics Driver Nouveau (Nvidia Legacy)	1.0.15-2igel775
Graphics Driver Vboxvideo	5.2.18-dfsg-2igel17
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.5-1ubuntu1igel750
Input Driver Elographics	1.4.1-1build5igel633
Input Driver Synaptics	1.9.0-1ubuntu1igel748
Input Driver Vmmouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu1igel813
Kernel	4.18.20 #mainline-udos-r2517
Xorg X11 Server	1.19.6-1ubuntu4.2igel842

Lightdm graphical login manager	1.18.3-0ubuntu1.1
XFCE4 Windowmanager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
Python2	2.7.12
Python3	3.5.2

IGEL OS 11

Supported Devices

IGEL devices:	
UD2-LX:	UD2-LX 40
UD3-LX:	UD3-LX 51 UD3-LX 50
UD5-LX:	UD5-LX 50
UD6-LX:	UD6-LX 51
UD7-LX:	UD7-LX 10
UD9-LX:	UD9-LX Touch 41 UD9-LX 40

For supported IGEL OS 11 third-party devices, see Devices Supported by IGEL OS 11 (see page 3442).

- Component Versions 11.01.100 (see page 3443)
- General Information 11.01.100 (see page 3447)
- Known Issues 11.01.100 (see page 3448)
- New Features 11.01.100 (see page 3450)
- CA Certificates Contained in IGEL OS 11.01.100 (see page 3455)

Component Versions 11.01.100

- **Clients**

Product	Version
Citrix HDX Realtime Media Engine	2.7.0-2113
Citrix Receiver	13.10.0.20
Citrix Receiver	13.5.0.10185126
Citrix Workspace App	18.10.0.11
deviceTRUST Citrix Channel	19.1.100.0
deviceTRUST RDP Channel	19.1.100.0
Evidian AuthMgr	1.5.6840
Evince PDF Viewer	3.18.2-1ubuntu4.3
FabulaTech USB for Remote Desktop	5.2.29
Firefox	60.4.0
IBM iAccess Client Solutions	1.1.8.0
IGEL RDP Client	2.2
Imprivata OneSign ProveID Embedded	
NX Client	5.3.12
Open VPN	2.3.10-1ubuntu2.1
Oracle JRE	1.8.0_202
Parallels Client (32 bit)	16.5.2.20595
Parole Media Player	1.0.1-0ubuntu1igel16
Remote Viewer (RedHat Virtualization)	7.0-igel47
Spice GTK (Red Hat Virtualization)	0.35
Spice Protocol (Red Hat Virtualization)	0.12.14
Usbredir (Red Hat Virtualization)	0.8.0
Thinlinc Client	4.9.0-5775
ThinPrint Client	7.5.88
Totem Media Player	2.30.2

VMware Horizon Client	4.10.0-11053294
VNC Viewer	1.8.0+git20180123-igel1
Voip Client Ekiga	4.0.1

- **Dictation**

Diktamen driver for dictation	
Driver for Grundig Business Systems dictation devices	
Nuance Audio Extensions for dictation	B048
Olympus driver for dictation	20180621
Philips Speech Driver	12.6.36

- **Signature**

Kofax SPVC Citrix Channel	3.1.41.0
signotec Citrix Channel	8.0.6
signotec VCOM Daemon	2.0.0
StepOver TCP Client	2.1.0

- **Smartcard**

PKCS#11 Library A.E.T SafeSign	3.0.101
PKCS#11 Library Athena IDProtect	623.07
PKCS#11 Library cryptovision sc/interface	7.1.9.620
PKCS#11 Library Gemalto SafeNet	10.0.37-0
PKCS#11 Library SecMaker NetID	6.7.0.23
Reader Driver ACS CCID	1.1.6-1igel1
Reader Driver Gemalto eToken	10.0.37-0
Reader Driver HID Global Omnikey	4.3.3
Reader Driver Identive CCID	5.0.35
Reader Driver Identive eHealth200	1.0.5
Reader Driver Identive SCRKBC	5.0.24
Reader Driver MUSCLE CCID	1.4.30-1igel3
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.23-1igel1

Cherry USB2LAN Proxy	3.0.0.6

- **System Components**

OpenSSL	1.0.2g-1ubuntu4.14
OpenSSH Client	7.2p2-4ubuntu2.7
OpenSSH Server	7.2p2-4ubuntu2.7
Bluetooth stack (bluez)	5.50-0ubuntu1igel5
MESA OpenGL stack	18.3.3-1igel57
VAAPI ABI Version	0.40
VDPAU Library version	1.1.1-3ubuntu1
Graphics Driver INTEL	2.99.917+git20181113-igel856
Graphics Driver ATI/RADEON	18.1.0-1igel854
Graphics Driver ATI/AMDGPU	18.1.0-1igel853
Graphics Driver Nouveau (Nvidia Legacy)	1.0.15-2igel775
Graphics Driver Nvidia	410.93-0ubuntu1
Graphics Driver Vboxvideo	5.2.18-dfsg-2igel17
Graphics Driver VMware	13.3.0-2igel857
Graphics Driver QXL (Spice)	0.1.5-2build1igel775
Graphics Driver FBDEV	0.5.0-1igel819
Graphics Driver VESA	2.4.0-1igel855
Input Driver Evdev	2.10.5-1ubuntu1igel750
Input Driver Elographics	1.4.1-1build5igel633
Input Driver eGalax	2.5.5814
Input Driver Synaptics	1.9.0-1ubuntu1igel748
Input Driver Vmmouse	13.1.0-1ubuntu2igel635
Input Driver Wacom	0.36.1-0ubuntu1igel813
Kernel	4.18.20 #mainline-udos-r2517
Xorg X11 Server	1.19.6-1ubuntu4.2igel842
Xorg Xephyr	1.19.6-1ubuntu4.2igel842
CUPS printing daemon	2.1.3-4ubuntu0.7igel23

PrinterLogic	18.2.1.128
Lightdm graphical login manager	1.18.3-0ubuntu1.1
XFCE4 Windowmanager	4.12.3-1ubuntu2igel675
ISC DHCP Client	4.3.3-5ubuntu12.10igel7
NetworkManager	1.2.6-0ubuntu0.16.04.2igel58
ModemManager	1.6.8-2ubuntu1igel2
GStreamer 0.10	0.10.36-2ubuntu0.1
GStreamer 1.x	1.14.4-1ubuntu1igel203
Python2	2.7.12
Python3	3.5.2

- **Features with Limited IGEL Support**

Mobile Device Access USB
VPN OpenConnect
Scanner support
VirtualBox

- **Features with Limited Functionality**

Cisco JVDI Client	12.1

General Information 11.01.100

The following clients and features are not supported anymore:

- Caradigm
- Citrix Legacy Sessions
- Citrix Web Interface
- Citrix StoreFront Legacy
- Citrix HDX Flash Redirection
- Citrix XenDesktop Appliance Mode
- Flash Player Download
- Ericom PowerTerm
- JAVA Web Start
- Leostream Java Connect
- Systancia AppliDis
- VIA graphics driver

Known Issues 11.01.100

Citrix

- With **activated DRI3** and an **AMD GPU Citrix H.264 acceleration plugin** could freeze. Selective H.264 mode (API v2) is not affected from this issue.
- Citrix has known issues with **GStreamer1.0** which describe problems with multimedia redirection of H.264, MPEG1 and MPEG2. GStreamer1.0 is used if **browser content redirection** is active.
- **Browser content redirection** does not work with activated **DRI3** and **hardware accelerated H.264 deep compression codec**.
- **Citrix StoreFront Login** with **Gemalto smartcard middleware** does not detect smartcard correctly if the card is inserted after start of Login.
  As a workaround, insert the smartcard before starting StoreFront Login.
- When using **Citrix Workspace App 18.10** in combination with **Philips Speech driver**, the session occasionally does not properly terminate at logoff and hangs.
  As a workaround, usage of Citrix Receiver 13.10 is recommended when Philips Speech driver is needed.
- **Citrix H.264 acceleration plugin** does not work with **enabled** server policy **Optimize for 3D graphics workload** in combination with server policy **Use video codec compression > For the entire screen**.

VMware Horizon

- **External drives** are mounted already before connection, do not appear in the **remote desktop**. Workaround: Mapping the directory/media as a drive on desktop. The external devices will show up within the media drive then.
- **Client drive mapping** and **USB redirection for storage devices** should not be enabled both at the same time.
  - On the one hand, when using **USB redirection for storage devices**: The USB on-insertion feature is only working when the client drive mapping is switched off. In the IGEL Setup client drive mapping can be found in: **Sessions > Horizon Client > Horizon Client Global > Drive Mapping > Enable Drive Mapping**. It is also recommended to disable local **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug**.
  - On the other hand, when using **drive mapping** instead, it is recommended to either switch off USB redirection entirely or at least deny storage devices by adding a filter to the USB class rules. Furthermore, Horizon Client relies on the OS to mount the storage devices itself. **Storage Hotplug** on setup page **Devices > Storage Devices > Storage Hotplug** has to be enabled and the **Number of storage hotplug devices** has to set to at least 1.

Parallels Client

- **Native USB redirection** does not work with Parallels Client.
- For using the new **FIPS 140-2 compliance mode**, it is necessary to connect to the **Parallels RAS** once with **disabled FIPS support**.

Smartcard

- In seldom cases, the authentication hung when using **A.E.T. SafeSign** smartcards.

Multimedia

- Multimedia redirection with **GStreamer** could fail with the Nouveau GPU driver.

Base system

- On **NVIDIA GPU** drivers, the **reported resolutions** of a display may contain unsupported resolutions. When any of those are configured, there are visual bugs (e.g. the desktop does not render properly).

New Features 11.01.100

Base system

- Support for **IGEL OS 11 license deployment** with **IGEL UMS 6** (via 'Automatic License Deployment')
- Support for **manual license deployment** in IGEL Setup Assistant
- Support for **demo license registration** in IGEL Setup Assistant
- Unified **IGEL OS 11 firmware** for IGEL and third-party hardware (New update file prefix: lxos)
- **Writable partitions are encrypted now**
- Use **IGEL OS Creator** for IGEL OS 11 installation and recovery (Download file: OSC_11.01.100.zip)

X11 system

- Reworked **user interface**
- **New wallpapers** have been added with **transparent background** so that the custom desktop color shows through. Selection of one of the new **Desktop Color** wallpapers in combination with an adjustment of desktop colors will provide this individual effect. The 2nd desktop color and the gradients also work with that.
- The new **Display Switch** tool can use **multiple different profiles**, automatically chosen at runtime depending on the currently connected monitors. A profile is created, when the current monitor layout/resolution is configured via the Display Switch utility. The profile will be associated with the currently connected displays automatically (manufacturer, model and used connector are used for allocation) and if applicable, the state of the laptop lid. The setup will be restored by hot-(un)plugging known displays, means the system will automatically switch to the already configured profile. The Display Switch utility itself got a new interface. All base functionality can be configured via Drag&Drop.
  An example workflow:
  - Connect the hardware and close/open lid
  - Open the Display Switch Utility

    - A quick (simple) setting can be selected directly.

    - Should the desired use case be different from the provided choices, the **Advanced** button opens a drag and drop interface for further settings.

  - In this interface, the **displays can be dragged and dropped** for the intended configuration. The display will snap adjacent to others.
  - If a display should not be used, it can be dragged to the **Disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
  - To show the same content on multiple displays, one display should be dragged onto an other active screen. The interface will show **Mirror**. The mirroring monitor will be displayed on the lower right.
  - With the **Apply** button the current state will be set, with ‘Yes’ on the “Keep configuration” dialog the current settings will be saved to persistent storage and associated with the profile.
  - **Advanced functionality** (panning/scaling/resolutions) can be configured in drop-down boxes, hidden in a **drawer on the right side**. The drawer can be expanded by clicking the ‘<’ button on the right edge.

- For the **Display Switch** functionality the following parameters should be enabled for proper usage.
  More...

IGEL Setup	**Accessories > Display Switch > Options**
Parameter	Preserve settings over reboot
Registry	`sessions.user_display0.options.preserve_settings`
Value	enabled / disabled
IGEL Setup	**Accessories > Display Switch > Options**
Parameter	Smart display configuration
Registry	`x.auto_associate`
Value	enabled / disabled

- The **IGEL Display Switch** utility is now used for **NVIDIA graphics** devices as well.
- **Automatic DPI detection** has been added by the following parameter.
  More...

IGEL Setup	**User Interface > Display > Options**
Parameter	Monitor DPI Detection
Registry	`x.xserver0.auto_dpi`
Value	Off / Smart / Pixel-Precise

  With the **Smart** automatic DPI detection the user interface is now usable out of the box on 4k displays.

  Smart: Auto detect the DPI but only use a few values whichever is closest to the calculated DPI value. Used DPI values: 96, 125, 150, 175, 200, 225, 250, 275, 300.

  Off: No auto DPI detection, fixed Monitor DPI value is used.

  Pixel-Precise: Auto detect the DPI value and use it when it is within 65-300 DPI. Otherwise, 96 DPI is used.

- Improved **High DPI** support for various applications.
- Added **xprintidle** tool to firmware.
- Added a parameter to **delay DisplayPort handling** by a certain number of seconds to mitigate disabled outputs causing a reconfiguration.
  More...

Parameter	Delay DisplayPort disconnect events by N seconds to prevent reconfiguration with weird monitors
Registry	`sessions.user_display0.options.delay_dp_hotplug`

Value	2

Firefox

- The Firefox configuration is now only done by global parameters found at setup pages: **IGEL Setup > Sessions > Browser > Browser Global**
- Session specific parameters are: **startup page**, **start monitor** and **autostart**

Audio

- Added support for deployment of **Jabra Xpress** packages with **IGEL UMS 6**.
  More...

IGEL Setup	**Devices > Unified Communications > Jabra > Jabra Xpress**
Parameter	Device Dashboard URL
Registry	`jabra.xpress.device_dashboard.server_url`
IGEL Setup	**Devices > Unified Communications > Jabra > Jabra Xpress**
Parameter	Package
Registry	`jabra.xpress.package_name`
IGEL Setup	**Devices > Unified Communications > Jabra > Jabra Xpress**
Parameter	Source URL
Registry	`jabra.xpress.package_url`
IGEL Setup	**Devices > Unified Communications > Jabra > Jabra Xpress**
Parameter	Check SSL certificate
Registry	`jabra.xpress.package_url_ssl_cert_check`
Value	enabled / disabled
IGEL Setup	**Devices > Unified Communications > Jabra > Jabra Xpress**
Parameter	Password
Registry	`jabra.xpress.package_url_crypt_password`

- Added support of **automatic suspend for wireless Jabra USB audio devices**. A device will be suspended after idle time over 5 seconds and automatically resumed again, when an application wants to playback or record audio data over the device.
  More...

IGEL Setup	**Devices > Unified Communications > Jabra > Options**

Parameter	Suspend on idle
Registry	`devices.jabra.suspend_on_idle`
Value	enabled / disabled

TC Setup (Java)

- **Local TC setup theme** can be configured now.
  More...

Parameter	Color Theme
Registry	`userinterface.setup.theme`
Value	Auto / Dark / Dark & Light / Light / Ocean

- Added **High DPI scaling**

On-screen keyboard

- Added new parameters to **auto show and hide the on-screen keyboard**. To use this feature, the on-screen keyboard should be set to **autostart** and **restart**. The on-screen keyboard will start in a hidden state and automatically appears when a text field is selected. Confirmed to work within Firefox and on lockscreen.
  More...

IGEL Setup	**Accessories > On-Screen Keyboard > Application Integration**
Parameter	Automatically show On-Screen Keyboard when text field is selected
Registry	`userinterface.softkeyboard.autoshow`
Value	enabled / disabled
Parameter	Automatically hide On-Screen Keyboard when text field is deselected
Registry	`userinterface.softkeyboard.autohide`
Value	enabled / disabled

Appliance Mode

- Streamlined the **on-screen keyboard** settings for appliance mode.
- Add new parameter to enable the on-screen keyboard in appliance mode. With **enabled Appliance Mode Access** the on-screen keyboard should set to auto start.
  More...

IGEL Setup	**Accessories > On-Screen Keyboard**
Parameter	Appliance Mode Access

Registry	`sessions.gtkeyboard0.appliance_mode_access`
Value	enabled / disabled

- Alternatively, the button to **show/hide** the on-screen keyboard can be displayed in **appliance mode**, to provide a quick method to turn the keyboard on or off.
  More...

IGEL Setup	**Accessories > On-Screen Keyboard > Application Integration > On-Screen Keyboard Toggle Button**
Parameter	Show button
Registry	`userinterface.touchscreen.keyboard.touchkey.enable`
Value	enabled / disabled

- **Removed the old options** to individually enable/disable and position the on-screen keyboard for various appliance mode settings.

Hardware

- Added hardware support for **HP t530**.

CA Certificates Contained in IGEL OS 11.01.100

Contained CA certificates:
- ACCVRAIZ1, expires Dec 31 09:37:37 2030 GMT (ACCVRAIZ1.crt)
- ACEDICOM Root, expires Apr 13 16:24:22 2028 GMT (ACEDICOM_Root.crt)
- AC RAIZ FNMT-RCM, expires Jan 1 00:00:00 2030 GMT (AC_RAIZ_FNMT-RCM.crt)
- Actalis Authentication Root CA, expires Sep 22 11:22:02 2030 GMT (Actalis_Authentication_Root_CA.crt)
- AddTrust External CA Root, expires May 30 10:48:38 2020 GMT (AddTrust_External_Root.crt)
- AddTrust Class 1 CA Root, expires May 30 10:38:31 2020 GMT (AddTrust_Low-Value_Services_Root.crt)
- AddTrust Public CA Root, expires May 30 10:41:50 2020 GMT (AddTrust_Public_Services_Root.crt)
- AddTrust Qualified CA Root, expires May 30 10:44:50 2020 GMT (AddTrust_Qualified_Certificates_Root.crt)
- AffirmTrust Commercial, expires Dec 31 14:06:06 2030 GMT (AffirmTrust_Commercial.crt)
- AffirmTrust Networking, expires Dec 31 14:08:24 2030 GMT (AffirmTrust_Networking.crt)
- AffirmTrust Premium, expires Dec 31 14:10:36 2040 GMT (AffirmTrust_Premium.crt)
- AffirmTrust Premium ECC, expires Dec 31 14:20:24 2040 GMT (AffirmTrust_Premium_ECC.crt)
- Amazon Root CA 1, expires Jan 17 00:00:00 2038 GMT (Amazon_Root_CA_1.crt)
- Amazon Root CA 2, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_2.crt)
- Amazon Root CA 3, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_3.crt)
- Amazon Root CA 4, expires May 26 00:00:00 2040 GMT (Amazon_Root_CA_4.crt)
- Atos TrustedRoot 2011, expires Dec 31 23:59:59 2030 GMT (Atos_TrustedRoot_2011.crt)
- Autoridad de Certificacion Firmaprofesional CIF A62634068, expires Dec 31 08:38:15 2030 GMT (Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt)
- Baltimore CyberTrust Root, expires May 12 23:59:00 2025 GMT (Baltimore_CyberTrust_Root.crt)
- Buypass Class 2 Root CA, expires Oct 26 08:38:03 2040 GMT (Buypass_Class_2_Root_CA.crt)
- Buypass Class 3 Root CA, expires Oct 26 08:28:58 2040 GMT (Buypass_Class_3_Root_CA.crt)
- CA Disig Root R1, expires Jul 19 09:06:56 2042 GMT (CA_Disig_Root_R1.crt)
- CA Disig Root R2, expires Jul 19 09:15:30 2042 GMT (CA_Disig_Root_R2.crt)
- CFCA EV ROOT, expires Dec 31 03:07:01 2029 GMT (CFCA_EV_ROOT.crt)
- CNNIC ROOT, expires Apr 16 07:09:14 2027 GMT (CNNIC_ROOT.crt)
- COMODO Certification Authority, expires Dec 31 23:59:59 2029 GMT (COMODO_Certification_Authority.crt)
- COMODO ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO_ECC_Certification_Authority.crt)
- COMODO RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (COMODO_RSA_Certification_Authority.crt)
- Chambers of Commerce Root, expires Sep 30 16:13:44 2037 GMT (Camerfirma_Chambers_of_Commerce_Root.crt)
- Global Chambersign Root, expires Sep 30 16:14:18 2037 GMT (Camerfirma_Global_Chambersign_Root.crt)
- Certigna, expires Jun 29 15:13:05 2027 GMT (Certigna.crt)
- Certinomis - Autorité Racine, expires Sep 17 08:28:59 2028 GMT (Certinomis_-_Autorité_Racine.crt)
- Certinomis - Root CA, expires Oct 21 09:17:18 2033 GMT (Certinomis_-_Root_CA.crt)
- Class 2 Primary CA, expires Jul 6 23:59:59 2019 GMT (Certplus_Class_2_Primary_CA.crt)
- Certplus Root CA G1, expires Jan 15 00:00:00 2038 GMT (Certplus_Root_CA_G1.crt)
- Certplus Root CA G2, expires Jan 15 00:00:00 2038 GMT (Certplus_Root_CA_G2.crt)
- Certum CA, expires Jun 11 10:46:39 2027 GMT (Certum_Root_CA.crt)
- Certum Trusted Network CA, expires Dec 31 12:07:37 2029 GMT (Certum_Trusted_Network_CA.crt)
- Certum Trusted Network CA 2, expires Oct 6 08:39:56 2046 GMT (Certum_Trusted_Network_CA_2.crt)
- Chambers of Commerce Root - 2008, expires Jul 31 12:29:50 2038 GMT (Chambers_of_Commerce_Root_-_2008.crt)
- China Internet Network Information Center EV Certificates Root, expires Aug 31 07:11:25 2030 GMT (China_Internet_Network_Information_Center_EV_Certificates_Root.crt)
- AAA Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo_AAA_Services_root.crt)
- Secure Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo_Secure_Services_root.crt)

- Trusted Certificate Services, expires Dec 31 23:59:59 2028 GMT (Comodo_Trusted_Services_root.crt)
- Cybertrust Global Root, expires Dec 15 08:00:00 2021 GMT (Cybertrust_Global_Root.crt)
- D-TRUST Root Class 3 CA 2 2009, expires Nov 5 08:35:58 2029 GMT (D-TRUST_Root_Class_3_CA_2_2009.crt)
- D-TRUST Root Class 3 CA 2 EV 2009, expires Nov 5 08:50:46 2029 GMT (D-TRUST_Root_Class_3_CA_2_EV_2009.crt)
- DST ACES CA X6, expires Nov 20 21:19:58 2017 GMT (DST_ACES_CA_X6.crt)
- DST Root CA X3, expires Sep 30 14:01:15 2021 GMT (DST_Root_CA_X3.crt)
- Deutsche Telekom Root CA 2, expires Jul 9 23:59:00 2019 GMT (Deutsche_Telekom_Root_CA_2.crt)
- DigiCert Assured ID Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_Assured_ID_Root_CA.crt)
- DigiCert Assured ID Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert_Assured_ID_Root_G2.crt)
- DigiCert Assured ID Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert_Assured_ID_Root_G3.crt)
- DigiCert Global Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_Global_Root_CA.crt)
- DigiCert Global Root G2, expires Jan 15 12:00:00 2038 GMT (DigiCert_Global_Root_G2.crt)
- DigiCert Global Root G3, expires Jan 15 12:00:00 2038 GMT (DigiCert_Global_Root_G3.crt)
- DigiCert High Assurance EV Root CA, expires Nov 10 00:00:00 2031 GMT (DigiCert_High_Assurance_EV_Root_CA.crt)
- DigiCert Trusted Root G4, expires Jan 15 12:00:00 2038 GMT (DigiCert_Trusted_Root_G4.crt)
- E-Tugra Certification Authority, expires Mar 3 12:09:48 2023 GMT (E-Tugra_Certification_Authority.crt)
- EC-ACC, expires Jan 7 22:59:59 2031 GMT (EC-ACC.crt)
- EE Certification Centre Root CA, expires Dec 17 23:59:59 2030 GMT (EE_Certification_Centre_Root_CA.crt)
- Entrust.net[347] Certification Authority (2048), expires Jul 24 14:15:12 2029 GMT (Entrust.net_Premium_2048_Secure_Server_CA.crt)
- Entrust Root Certification Authority, expires Nov 27 20:53:42 2026 GMT (Entrust_Root_Certification_Authority.crt)
- Entrust Root Certification Authority - EC1, expires Dec 18 15:55:36 2037 GMT (Entrust_Root_Certification_Authority_-_EC1.crt)
- Entrust Root Certification Authority - G2, expires Dec 7 17:55:54 2030 GMT (Entrust_Root_Certification_Authority_-_G2.crt)
- GeoTrust Global CA, expires May 21 04:00:00 2022 GMT (GeoTrust_Global_CA.crt)
- GeoTrust Global CA 2, expires Mar 4 05:00:00 2019 GMT (GeoTrust_Global_CA_2.crt)
- GeoTrust Primary Certification Authority, expires Jul 16 23:59:59 2036 GMT (GeoTrust_Primary_Certification_Authority.crt)
- GeoTrust Primary Certification Authority - G2, expires Jan 18 23:59:59 2038 GMT (GeoTrust_Primary_Certification_Authority_-_G2.crt)
- GeoTrust Primary Certification Authority - G3, expires Dec 1 23:59:59 2037 GMT (GeoTrust_Primary_Certification_Authority_-_G3.crt)
- GeoTrust Universal CA, expires Mar 4 05:00:00 2029 GMT (GeoTrust_Universal_CA.crt)
- GeoTrust Universal CA 2, expires Mar 4 05:00:00 2029 GMT (GeoTrust_Universal_CA_2.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign_ECC_Root_CA_-_R4.crt)
- GlobalSign, expires Jan 19 03:14:07 2038 GMT (GlobalSign_ECC_Root_CA_-_R5.crt)
- GlobalSign Root CA, expires Jan 28 12:00:00 2028 GMT (GlobalSign_Root_CA.crt)
- GlobalSign, expires Dec 15 08:00:00 2021 GMT (GlobalSign_Root_CA_-_R2.crt)
- GlobalSign, expires Mar 18 10:00:00 2029 GMT (GlobalSign_Root_CA_-_R3.crt)
- Global Chambersign Root - 2008, expires Jul 31 12:31:40 2038 GMT (Global_Chambersign_Root_-_2008.crt)
- Go Daddy Class 2 Certification Authority, expires Jun 29 17:06:20 2034 GMT (Go_Daddy_Class_2_CA.crt)
- Go Daddy Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Go_Daddy_Root_Certificate_Authority_-_G2.crt)
- Hellenic Academic and Research Institutions ECC RootCA 2015, expires Jun 30 10:37:12 2040 GMT (Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt)
- Hellenic Academic and Research Institutions RootCA 2011, expires Dec 1 13:49:52 2031 GMT (Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt)
- Hellenic Academic and Research Institutions RootCA 2015, expires Jun 30 10:11:21 2040 GMT

347. http://Entrust.net

(Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt)
- Hongkong Post Root CA 1, expires May 15 04:52:29 2023 GMT (Hongkong_Post_Root_CA_1.crt)
- ISRG Root X1, expires Jun 4 11:04:38 2035 GMT (ISRG_Root_X1.crt)
- IdenTrust Commercial Root CA 1, expires Jan 16 18:12:23 2034 GMT (IdenTrust_Commercial_Root_CA_1.crt)
- IdenTrust Public Sector Root CA 1, expires Jan 16 17:53:32 2034 GMT (IdenTrust_Public_Sector_Root_CA_1.crt)
- Imprivata Embedded Code Signing CA, expires Sep 7 16:20:00 2033 GMT (Imprivata.crt)
- Izenpe.com[348], expires Dec 13 08:27:25 2037 GMT (Izenpe.com[349].crt)
- LuxTrust Global Root 2, expires Mar 5 13:21:57 2035 GMT (LuxTrust_Global_Root_2.crt)
- Microsec e-Szigno Root CA 2009, expires Dec 30 11:30:18 2029 GMT (Microsec_e-Szigno_Root_CA_2009.crt)
- NetLock Arany (Class Gold) Főtanúsítvány, expires Dec 6 15:08:21 2028 GMT
(NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt)
- Network Solutions Certificate Authority, expires Dec 31 23:59:59 2029 GMT
(Network_Solutions_Certificate_Authority.crt)
- OISTE WISeKey Global Root GA CA, expires Dec 11 16:09:51 2037 GMT (OISTE_WISeKey_Global_Root_GA_CA.crt)
- OISTE WISeKey Global Root GB CA, expires Dec 1 15:10:31 2039 GMT (OISTE_WISeKey_Global_Root_GB_CA.crt)
- OpenTrust Root CA G1, expires Jan 15 00:00:00 2038 GMT (OpenTrust_Root_CA_G1.crt)
- OpenTrust Root CA G2, expires Jan 15 00:00:00 2038 GMT (OpenTrust_Root_CA_G2.crt)
- OpenTrust Root CA G3, expires Jan 15 00:00:00 2038 GMT (OpenTrust_Root_CA_G3.crt)
- Autoridad de Certificacion Raiz del Estado Venezolano, expires Dec 25 23:59:59 2020 GMT (PSCProcert.crt)
- QuoVadis Root Certification Authority, expires Mar 17 18:33:33 2021 GMT (QuoVadis_Root_CA.crt)
- QuoVadis Root CA 1 G3, expires Jan 12 17:27:44 2042 GMT (QuoVadis_Root_CA_1_G3.crt)
- QuoVadis Root CA 2, expires Nov 24 18:23:33 2031 GMT (QuoVadis_Root_CA_2.crt)
- QuoVadis Root CA 2 G3, expires Jan 12 18:59:32 2042 GMT (QuoVadis_Root_CA_2_G3.crt)
- QuoVadis Root CA 3, expires Nov 24 19:06:44 2031 GMT (QuoVadis_Root_CA_3.crt)
- QuoVadis Root CA 3 G3, expires Jan 12 20:26:32 2042 GMT (QuoVadis_Root_CA_3_G3.crt)
- SZAFIR ROOT CA2, expires Oct 19 07:43:30 2035 GMT (SZAFIR_ROOT_CA2.crt)
- SecureSign RootCA11, expires Apr 8 04:56:47 2029 GMT (SecureSign_RootCA11.crt)
- SecureTrust CA, expires Dec 31 19:40:55 2029 GMT (SecureTrust_CA.crt)
- Secure Global CA, expires Dec 31 19:52:06 2029 GMT (Secure_Global_CA.crt)
- Security Communication EV RootCA1, expires Jun 6 02:12:32 2037 GMT
(Security_Communication_EV_RootCA1.crt)
- Security Communication RootCA2, expires May 29 05:00:39 2029 GMT (Security_Communication_RootCA2.crt)
- Security Communication RootCA1, expires Sep 30 04:20:49 2023 GMT (Security_Communication_Root_CA.crt)
- Sonera Class2 CA, expires Apr 6 07:29:40 2021 GMT (Sonera_Class_2_Root_CA.crt)
- Staat der Nederlanden EV Root CA, expires Dec 8 11:10:28 2022 GMT (Staat_der_Nederlanden_EV_Root_CA.crt)
- Staat der Nederlanden Root CA - G2, expires Mar 25 11:03:10 2020 GMT (Staat_der_Nederlanden_Root_CA_-_G2.crt)
- Staat der Nederlanden Root CA - G3, expires Nov 13 23:00:00 2028 GMT (Staat_der_Nederlanden_Root_CA_-_G3.crt)
- Starfield Class 2 Certification Authority, expires Jun 29 17:39:16 2034 GMT (Starfield_Class_2_CA.crt)
- Starfield Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT (Starfield_Root_Certificate_Authority_-_G2.crt)
- Starfield Services Root Certificate Authority - G2, expires Dec 31 23:59:59 2037 GMT
(Starfield_Services_Root_Certificate_Authority_-_G2.crt)
- SwissSign Gold CA - G2, expires Oct 25 08:30:35 2036 GMT (SwissSign_Gold_CA_-_G2.crt)
- SwissSign Silver CA - G2, expires Oct 25 08:32:46 2036 GMT (SwissSign_Silver_CA_-_G2.crt)
- Swisscom Root CA 1, expires Aug 18 22:06:20 2025 GMT (Swisscom_Root_CA_1.crt)
- Swisscom Root CA 2, expires Jun 25 07:38:14 2031 GMT (Swisscom_Root_CA_2.crt)

348. http://Izenpe.com
349. http://Izenpe.com

- Swisscom Root EV CA 2, expires Jun 25 08:45:08 2031 GMT (Swisscom_Root_EV_CA_2.crt)
- T-TeleSec GlobalRoot Class 2, expires Oct 1 23:59:59 2033 GMT (T-TeleSec_GlobalRoot_Class_2.crt)
- T-TeleSec GlobalRoot Class 3, expires Oct 1 23:59:59 2033 GMT (T-TeleSec_GlobalRoot_Class_3.crt)
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, expires Oct 25 08:25:55 2043 GMT (TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt)
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı, expires Dec 22 18:37:19 2017 GMT (TURKTRUST_Certificate_Services_Provider_Root_2007.crt)
- TWCA Global Root CA, expires Dec 31 15:59:59 2030 GMT (TWCA_Global_Root_CA.crt)
- TWCA Root Certification Authority, expires Dec 31 15:59:59 2030 GMT (TWCA_Root_Certification_Authority.crt)
- Government Root Certification Authority, expires Dec 5 13:23:33 2032 GMT (Taiwan_GRCA.crt)
- TeliaSonera Root CA v1, expires Oct 18 12:00:50 2032 GMT (TeliaSonera_Root_CA_v1.crt)
- Trustis FPS Root CA, expires Jan 21 11:36:54 2024 GMT (Trustis_FPS_Root_CA.crt)
- TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3, expires Aug 21 11:37:07 2017 GMT (TÜBİTAK_UEKAE_Kök_Sertifika_Hizmet_Sağlayıcısı_-_Sürüm_3.crt)
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5, expires Apr 28 08:07:01 2023 GMT (TÜRKTRUST_Elektronik_Sertifika_Hizmet_Sağlayıcısı_H5.crt)
- USERTrust ECC Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust_ECC_Certification_Authority.crt)
- USERTrust RSA Certification Authority, expires Jan 18 23:59:59 2038 GMT (USERTrust_RSA_Certification_Authority.crt)
- UTN-USERFirst-Hardware, expires Jul 9 18:19:22 2019 GMT (UTN_USERFirst_Hardware_Root_CA.crt)
- VeriSign Class 3 Public Primary Certification Authority - G4, expires Jan 18 23:59:59 2038 GMT (VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt)
- VeriSign Class 3 Public Primary Certification Authority - G5, expires Jul 16 23:59:59 2036 GMT (VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt)
- VeriSign Universal Root Certification Authority, expires Dec 1 23:59:59 2037 GMT (VeriSign_Universal_Root_Certification_Authority.crt)
- VeriSign Class 3 Public Primary Certification Authority - G3, expires Jul 16 23:59:59 2036 GMT (Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt)
- Visa eCommerce Root, expires Jun 24 00:16:12 2022 GMT (Visa_eCommerce_Root.crt)
- XRamp Global Certification Authority, expires Jan 1 05:37:19 2035 GMT (XRamp_Global_CA_Root.crt)
- certSIGN ROOT CA, expires Jul 4 17:20:04 2031 GMT (certSIGN_ROOT_CA.crt)
- ePKI Root Certification Authority, expires Dec 20 02:31:27 2034 GMT (ePKI_Root_Certification_Authority.crt)
- thawte Primary Root CA, expires Jul 16 23:59:59 2036 GMT (thawte_Primary_Root_CA.crt)
- thawte Primary Root CA - G2, expires Jan 18 23:59:59 2038 GMT (thawte_Primary_Root_CA_-_G2.crt)
- thawte Primary Root CA - G3, expires Dec 1 23:59:59 2037 GMT (thawte_Primary_Root_CA_-_G3.crt)

IGEL OS SCCM Add-On

The IGEL OS SCCM add-on facilitates deploying IGEL OS via Microsoft SCCM. The package contains a minimized IGEL OS image that will be booted initially. If the target devices have enough RAM, a full-featured IGEL OS can be used as an alternative; see Deploying an Alternative IGEL OS Image (see page 3469).

With the installation of the package, a customized Windows PE image and a task sequence for deploying IGEL OS are created, and the IGEL OS Image Manager is installed.

Short Video Summary

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=6nrTmW0ECyk&feature=youtu.be

Prerequisites

- Microsoft Endpoint Configuration Manager (see https://docs.microsoft.com/en-us/mem/configmgr/)

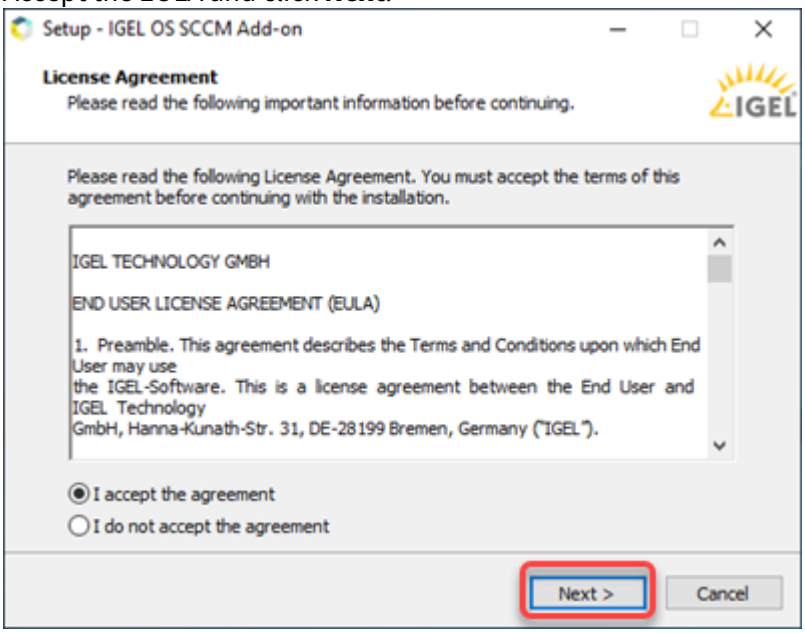
  The solution presented here has been developed and tested with the current version of Microsoft Endpoint Configuration Manager (status 01/2024). For details on the versioning of Microsoft Endpoint Configuration Manager, see https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/changes/whats-new-incremental-versions.

- Configured PXE environment for OS deployment; all target devices must be in a network where they are available either from the main site server or a distribution point. (For further information, see https://docs.microsoft.com/en-us/mem/configmgr/osd/plan-design/infrastructure-requirements-for-operating-system-deployment)
- All target devices have a minimum of 2 GB RAM.
- On the host on which Microsoft Endpoint Configuration Manager is running, Microsoft Power Shell Script execution must be allowed, at least for signed scripts (the Powershell scripts that come with the IGEL OS SCCM add-on are signed by IGEL).

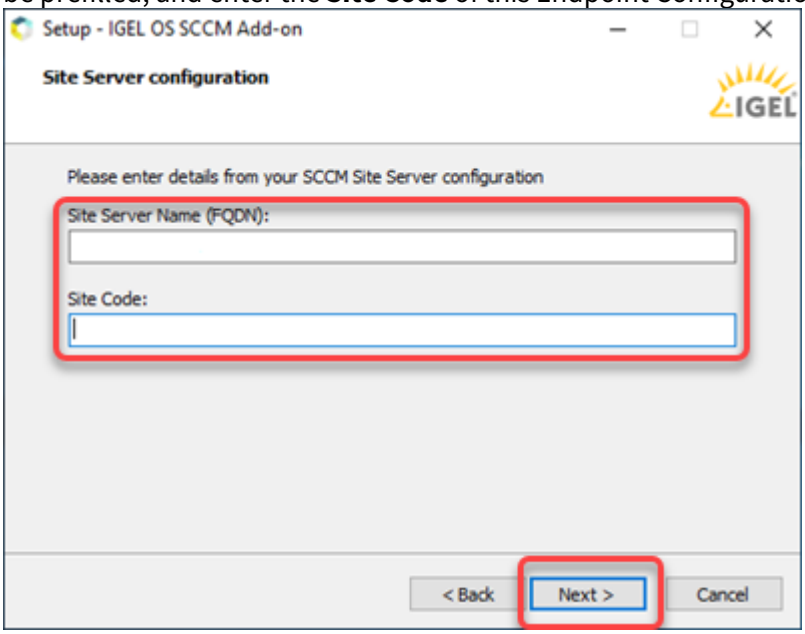
Installing the IGEL OS SCCM Add-On

1. Go to https://www.igel.com/software-downloads/workspace-edition/ **> OS DEPLOYMENT TOOL FOR SCCM** and download the executable file (`setup-igel_os-sccm_add_on_[version].exe`) to the host on which Microsoft Endpoint Configuration Manager is running.
2. Start the executable file.

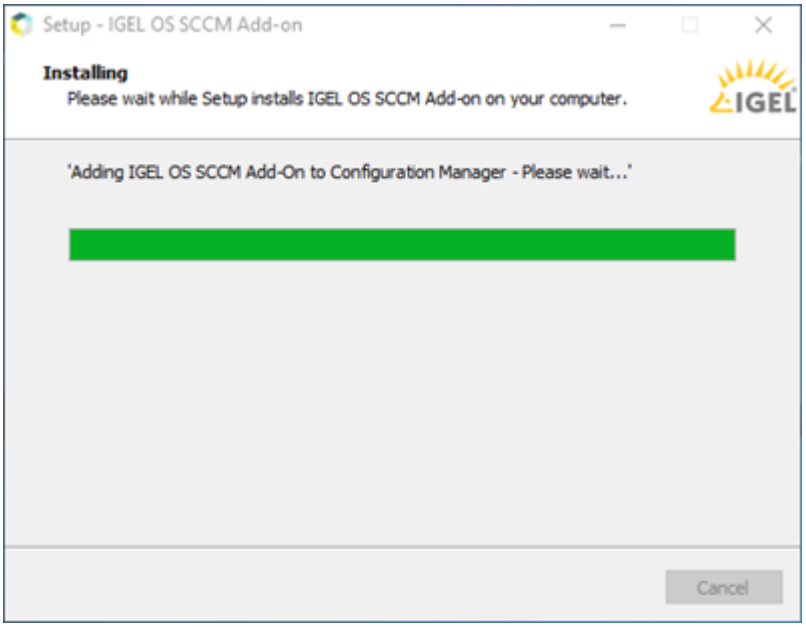
3. Accept the EULA and click **Next**.



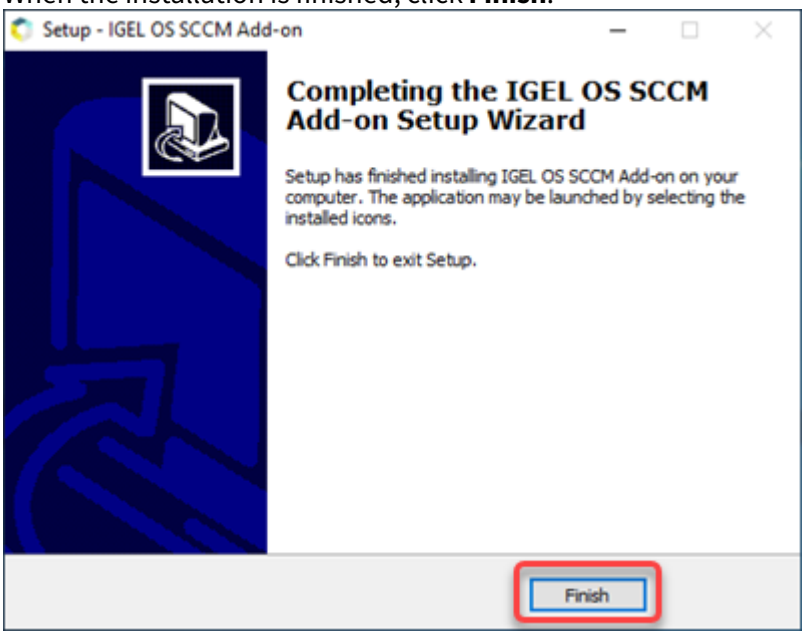
4. On the **Site Server configuration** page, review the field **Site Server Name (FQDN)**, which should be prefilled, and enter the **Site Code** of this Endpoint Configuration Manager site. Then, click **Next**.



The installation of the IGEL OS SCCM add-on starts.

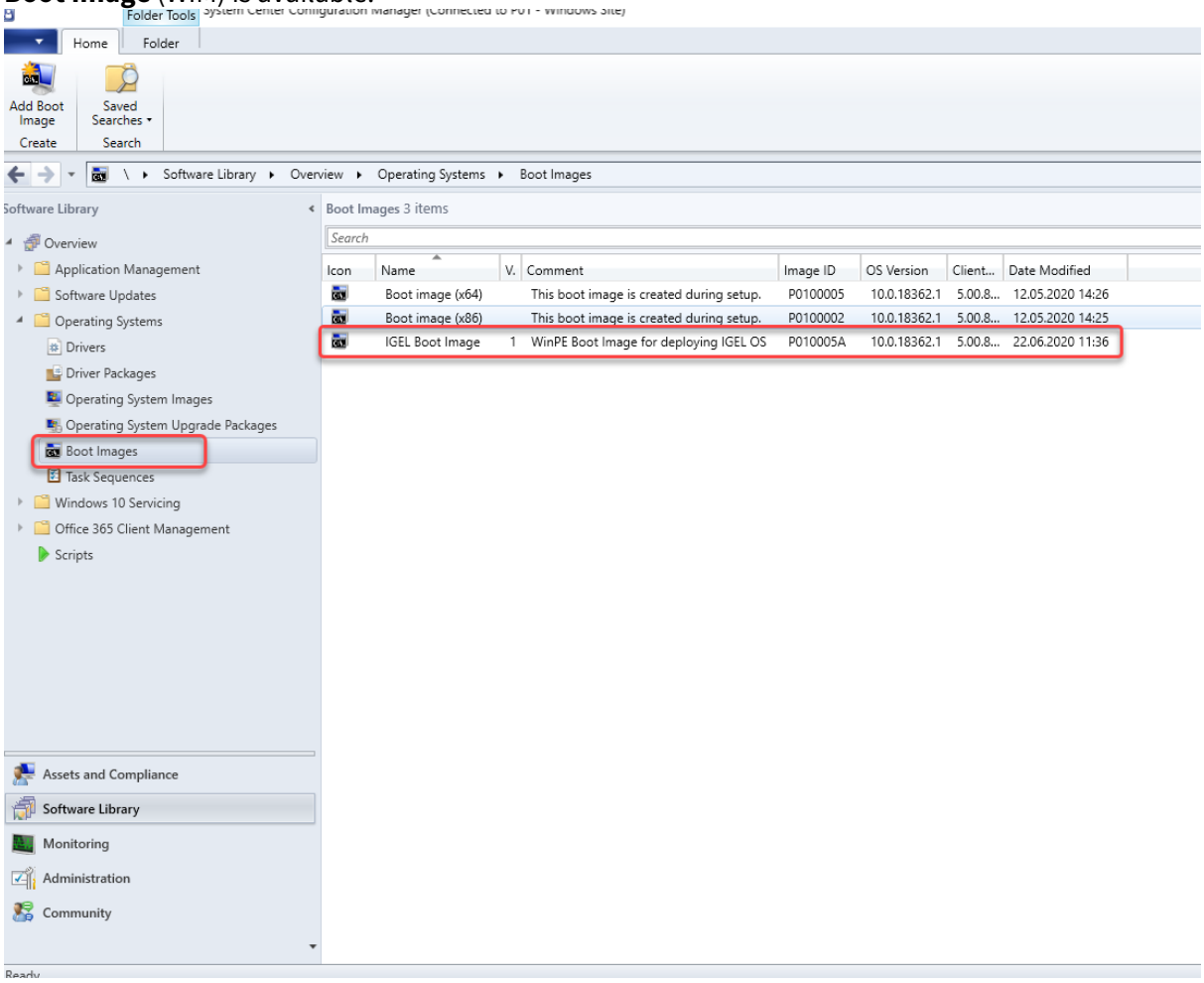


5. When the installation is finished, click **Finish**.

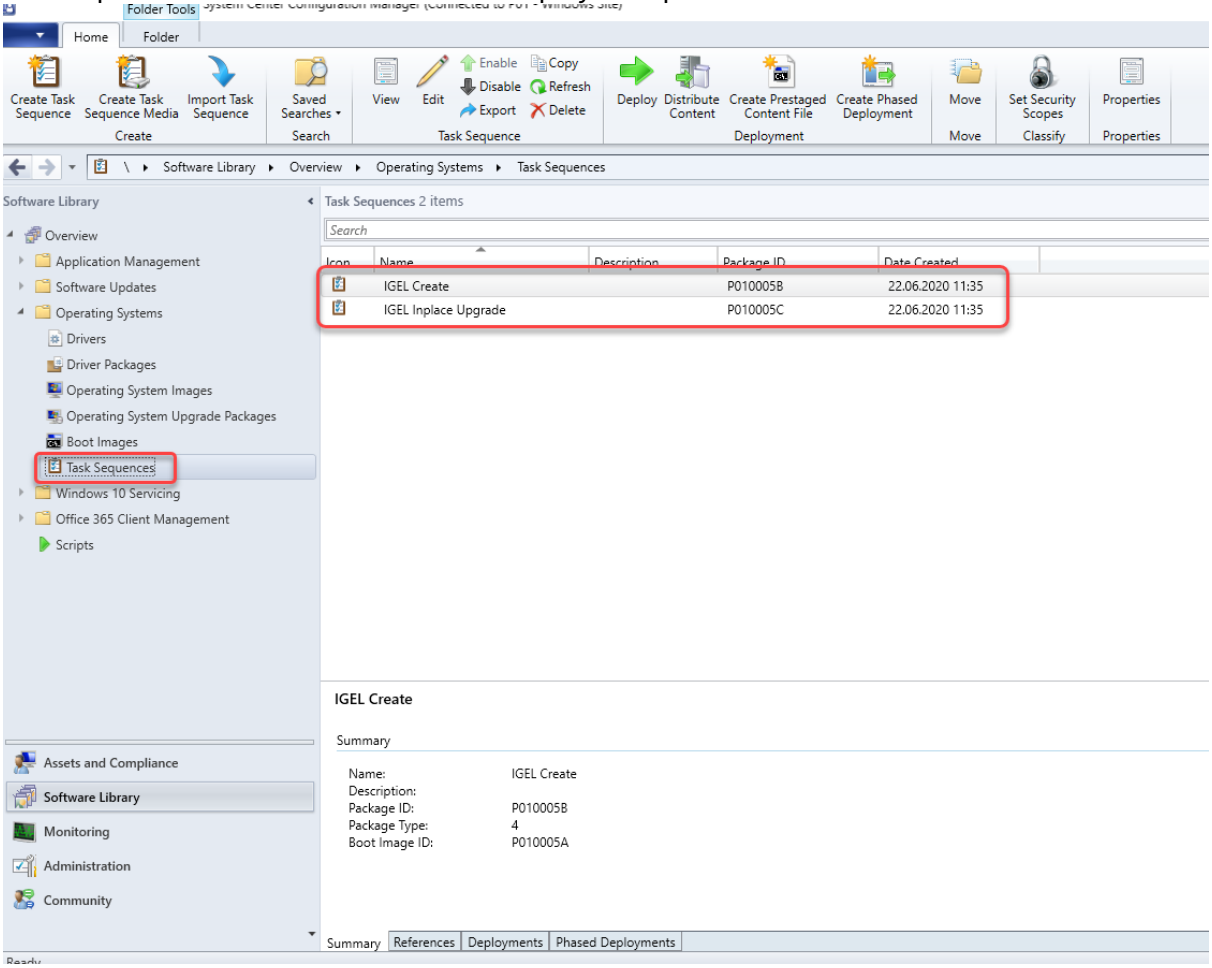


Verifying the Installation

1. In the **Home** tab of the Endpoint Configuration Manager, go to **Boot Images** and check if the **IGEL Boot Image** (WIM) is available.



2. Go to **Task Sequences** and check if **IGEL Create** and **IGEL Inplace Upgrade** are available. These task sequences will drive and control the deployment process.



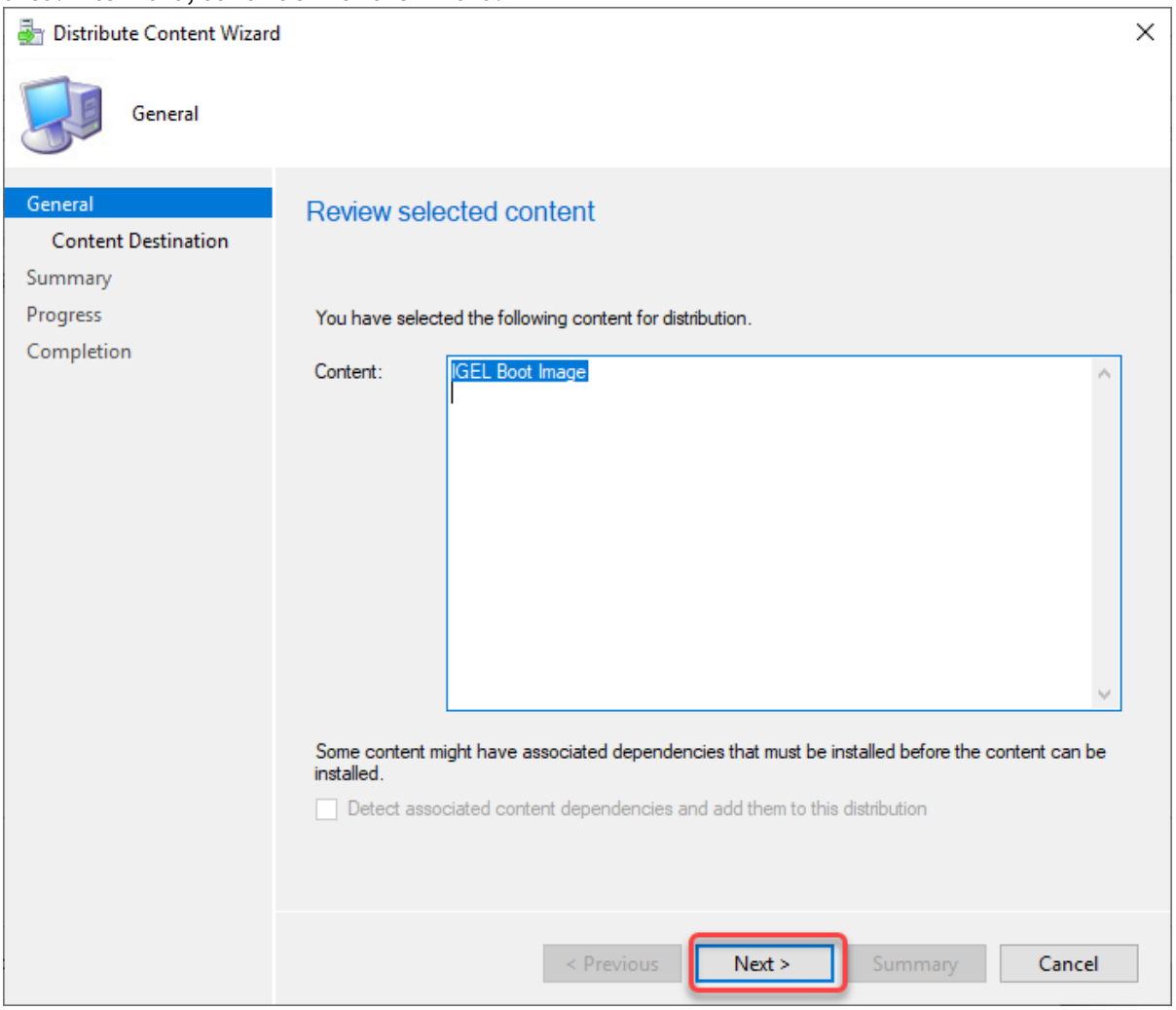
Provisioning IGEL OS via a PXE Boot Environment

The task sequence "IGEL Create" will deploy IGEL OS to a device collection via a PXE boot environment. The task sequence will be executed after the device has booted into the IGEL OS Boot Image (WIM).

To deploy the PXE boot environment:

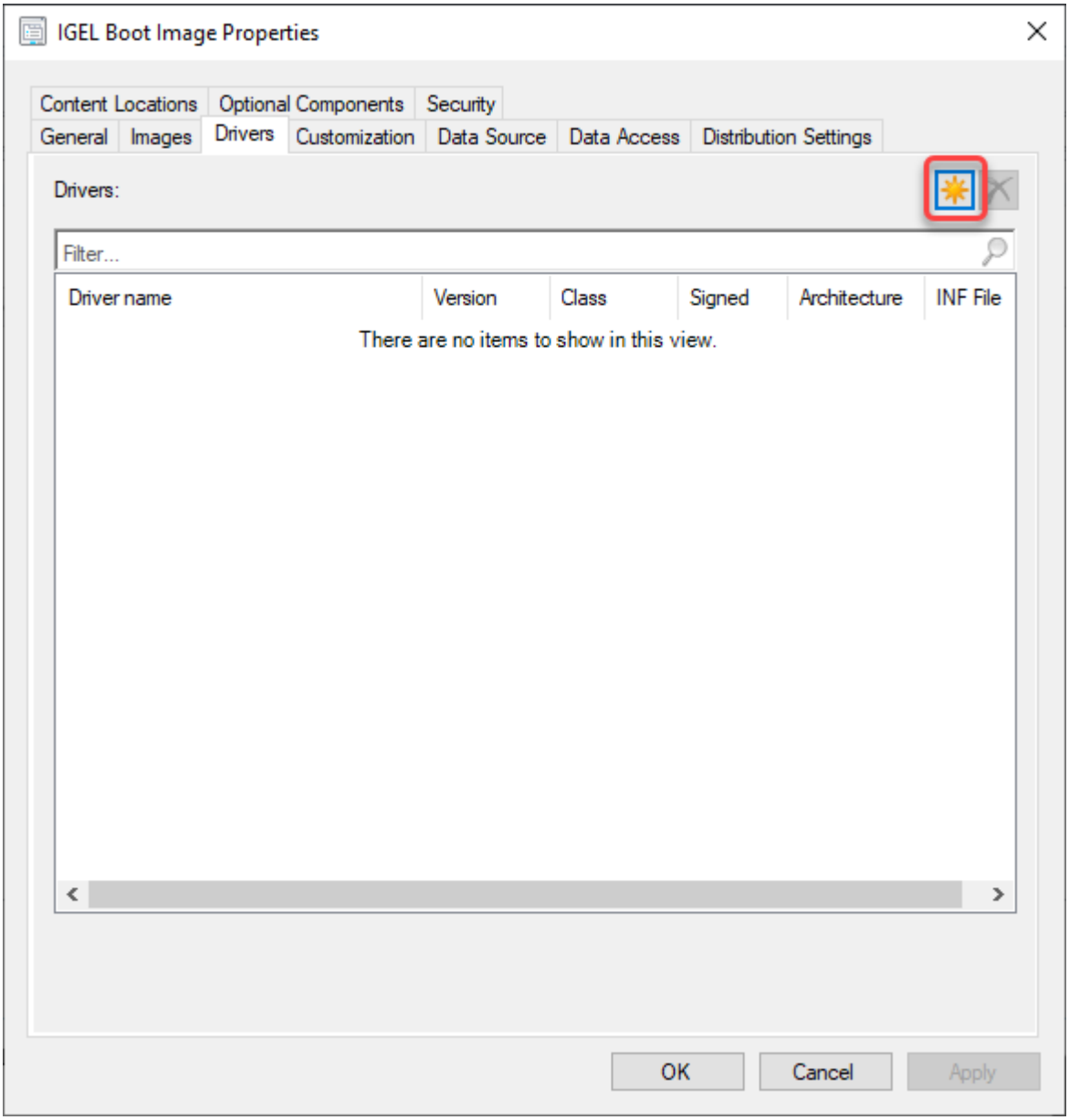
1. Check if you need to define your own custom device collection to allocate your target devices or if you can use one of the preconfigured collections.
2. In the **Home** tab of the Endpoint Configuration Manager, select **Boot Images**, open the context menu for **IGEL Boot Image**, and select **Distribute content**.

3. Open the **Distribute Content Wizard** and check if "IGEL Boot Image" is shown in the **Content** area. Afterward, continue with the wizard.

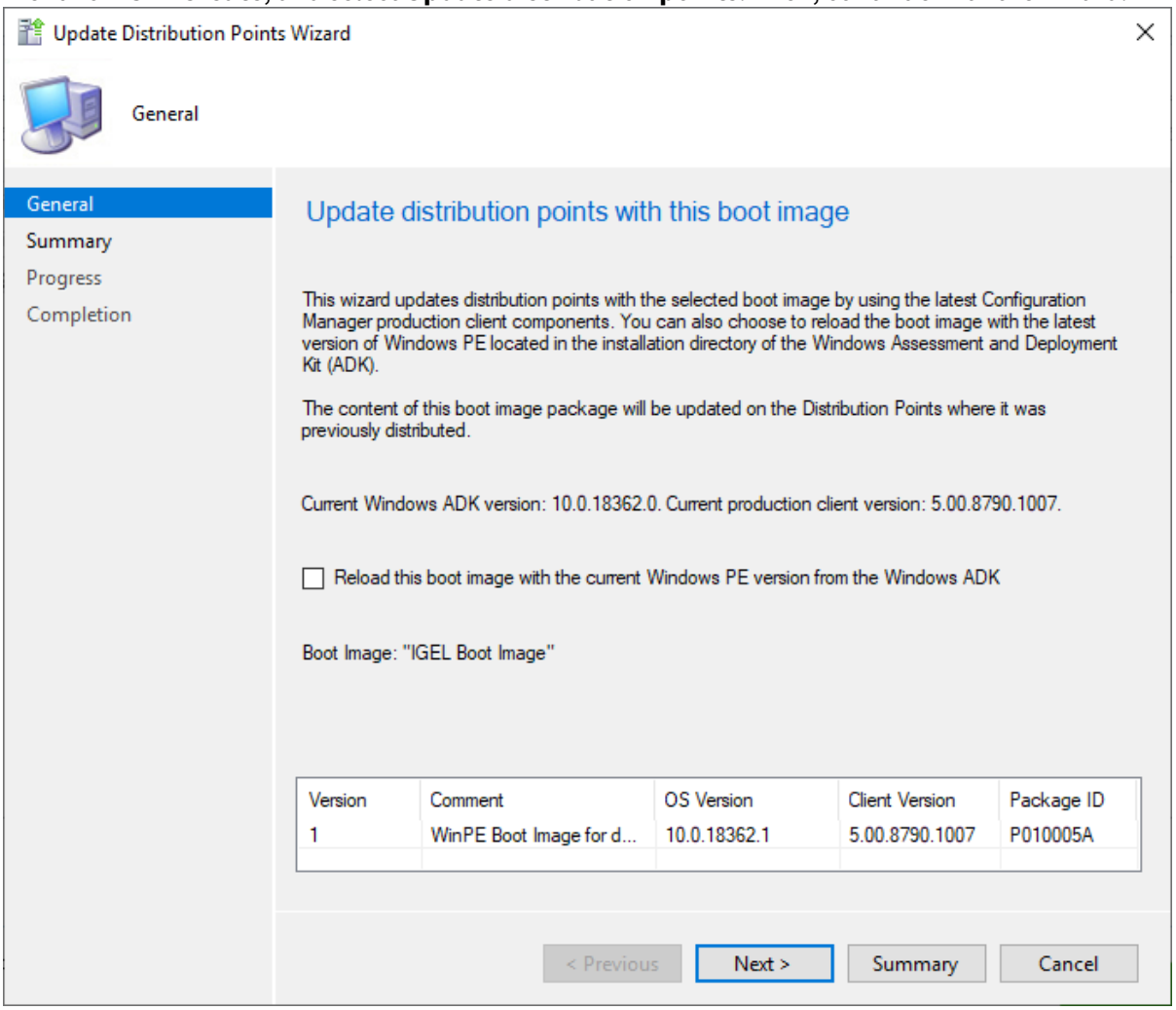


4. If your device requires a specific network driver: In the **Home** tab of the Endpoint Configuration Manager, select **Boot Images**, open the context menu for **IGEL Boot Image**, and select **Properties**. Then,

select the **Drivers** tab and add the driver.

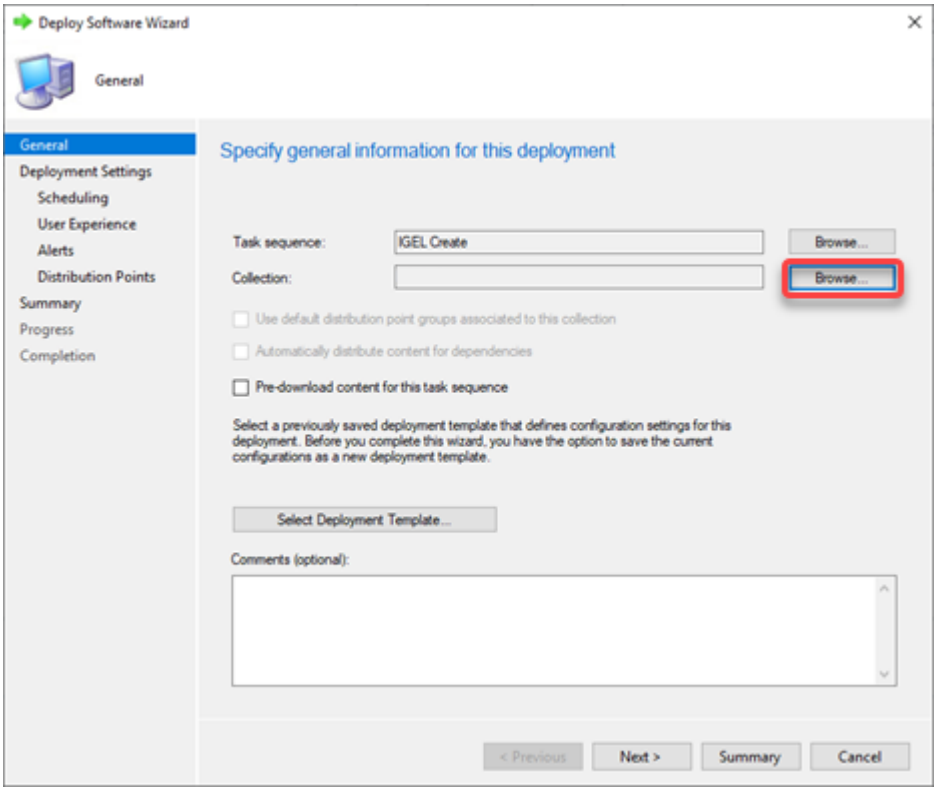


5. In the **Home** tab of the Endpoint Configuration Manager, select **Task Sequences**, open the context menu for **IGEL Create**, and select **Update distribution points**. Then, continue with the wizard.



6. In the **Home** tab of the Endpoint Configuration Manager, select **Task Sequences**, open the context menu for **IGEL Create**, and select **Deploy**.
   The **Deploy Software Wizard** opens.

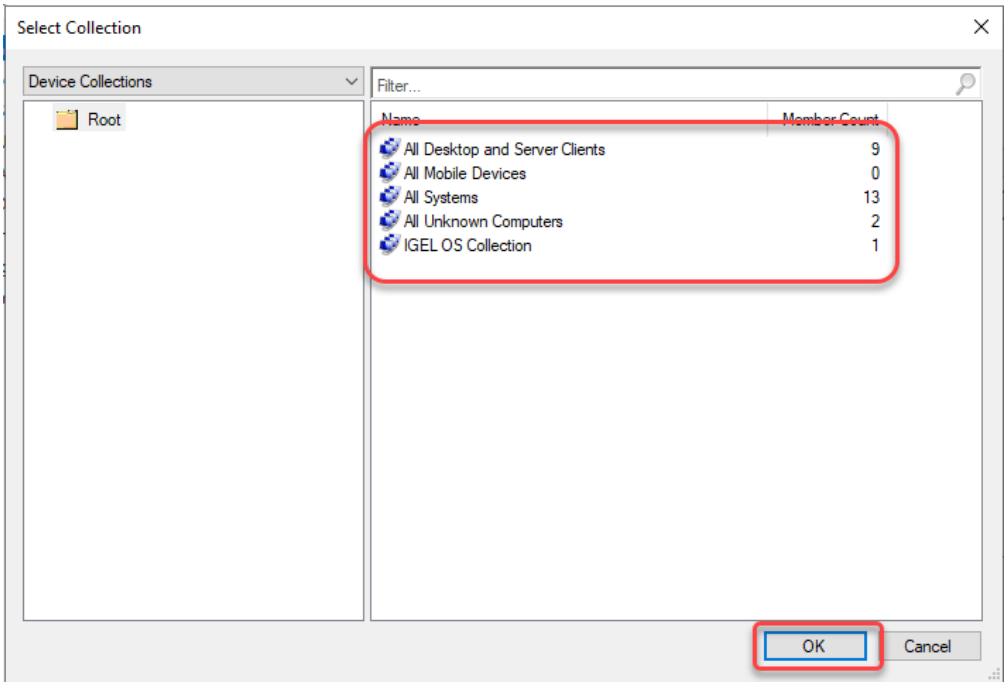
7. Click the **Browse** button next to **Collection:**.



The **Select Collection** dialog opens.

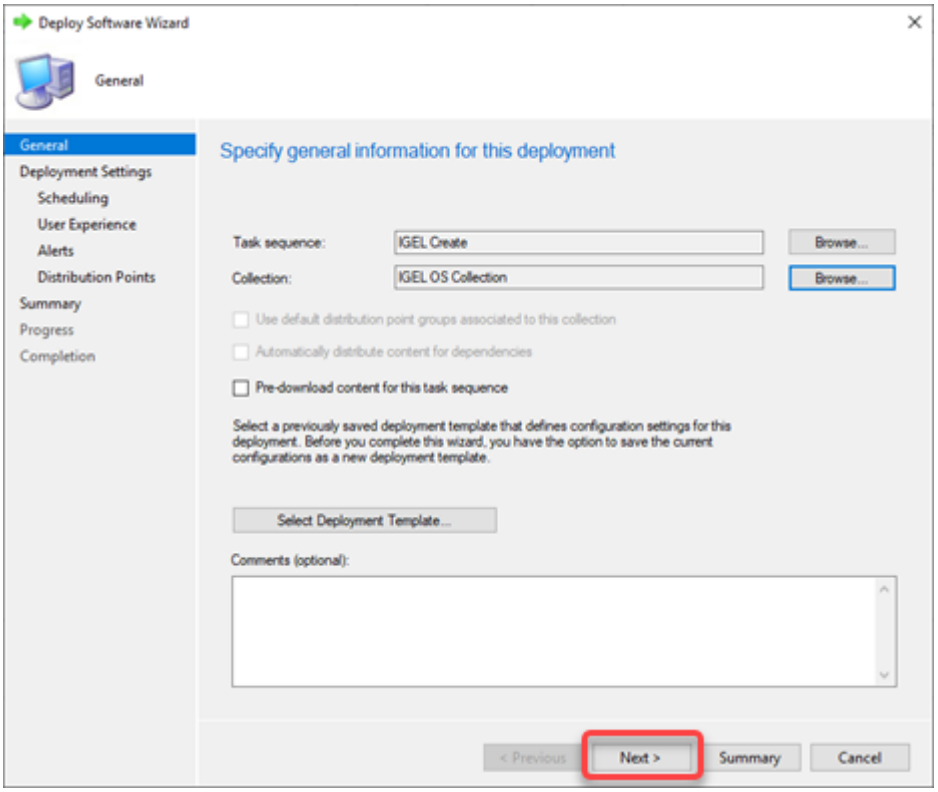
8. From the list of collections, select the collection that contains your target devices and click **OK**.

> If you want to deploy IGEL OS to all new devices on the network and any existing third-party devices running IoT, use the pre-existing collection "All Unknown Computers".

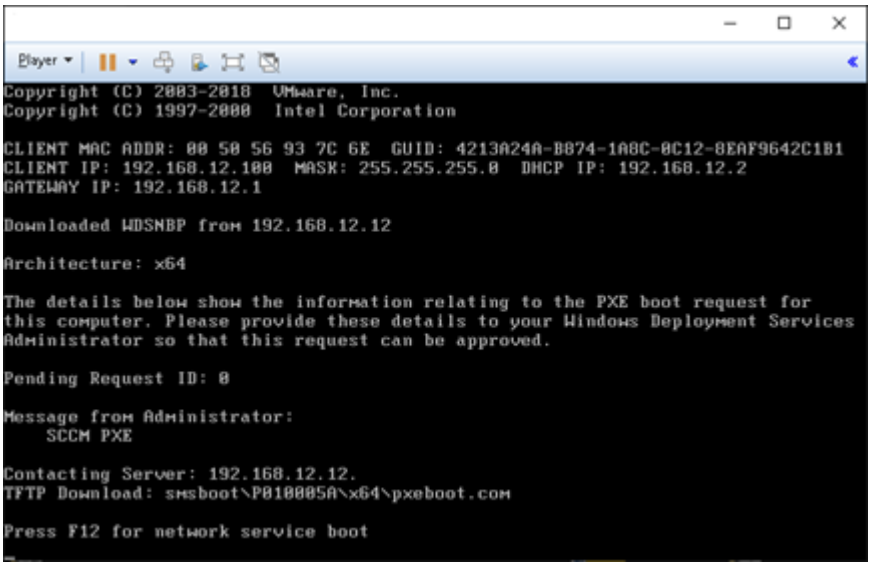


In the following example, a user-created collection named "IGEL OS Collection" has been selected:

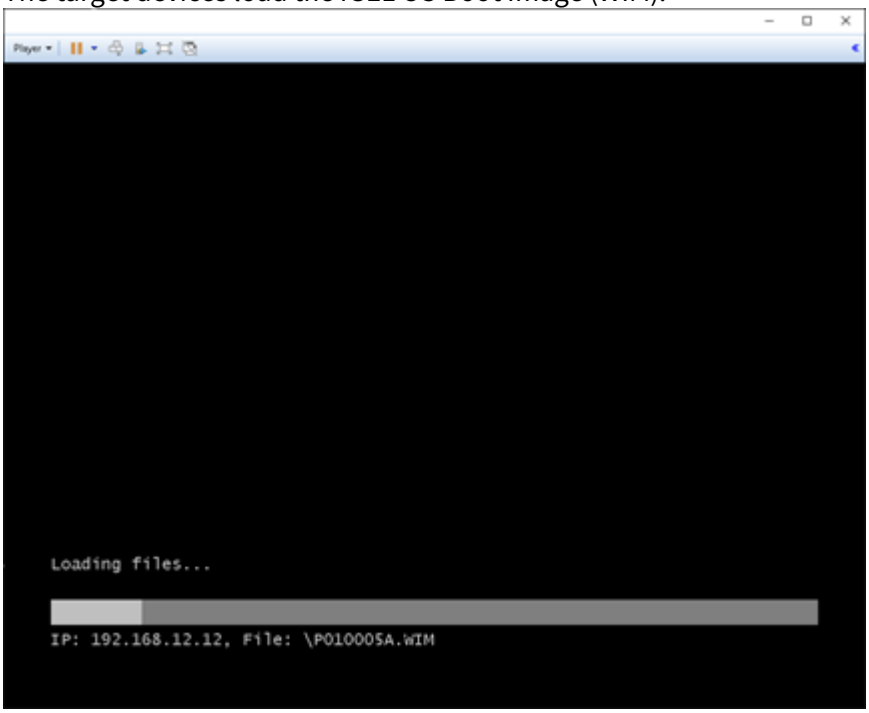
9. Click **Next** to continue with the wizard.



All target devices receive the PXE boot request that triggers them to boot the IGEL OS Boot Image (WIM).



The target devices load the IGEL OS Boot Image (WIM).

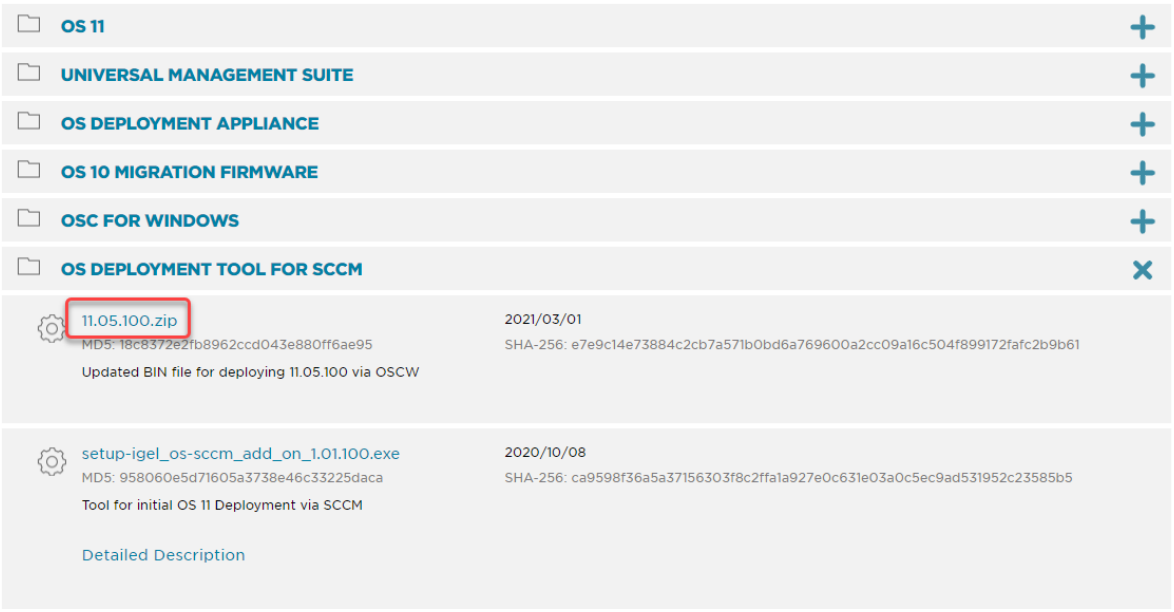


Deploying an Alternative IGEL OS Image

As an alternative to the minimized IGEL OS image that comes with the IGEL OS SCCM add-on, you can deploy a full-featured IGEL OS image. The current main version is available from igel.com. Optionally, you can add pre-configured settings and certificates to the image.

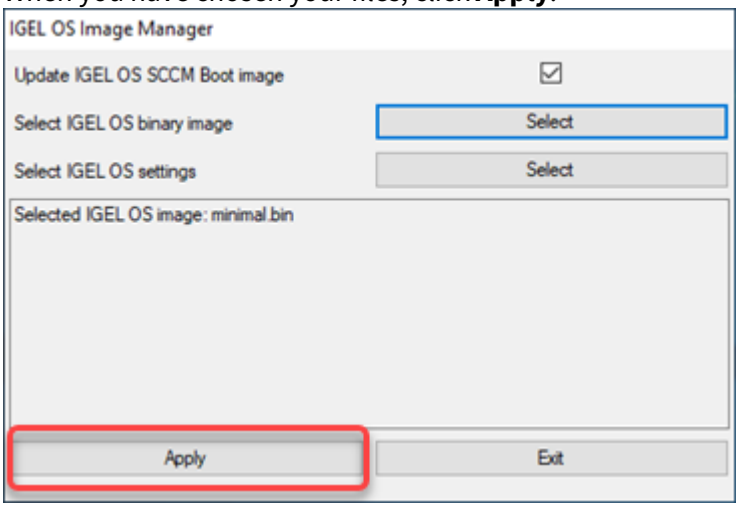
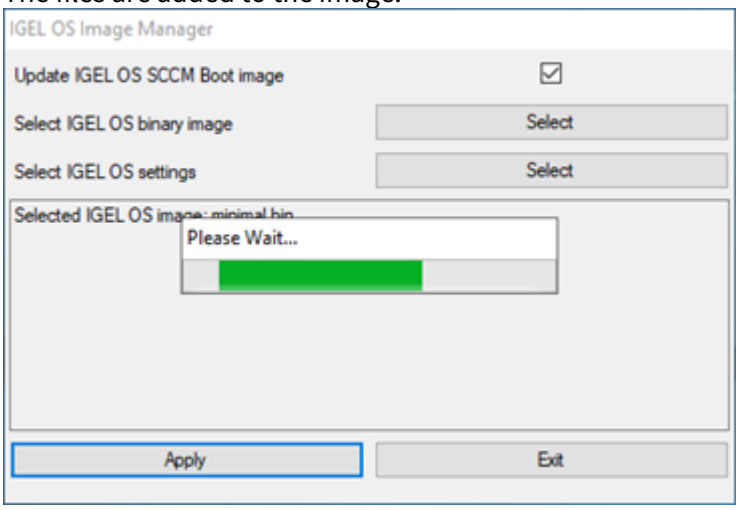
The RAM size of the target device must be equal to or greater than the storage size required by the IGEL OS image plus the initial size of the IGEL OS Boot Image (WIM), which is between 300 and 400 MB. For deploying an alternative IGEL OS Image, at least 4 GB RAM is needed.

1. Open a web browser, go to https://www.igel.com/software-downloads/workspace-edition/ **> OS DEPLYOMENT TOOL FOR SCCM**, download the current IGEL OS file, and unzip it.



   The IGEL OS image is ready for deployment (example: `11.05.100.bin`).
2. Start the IGEL OS Image Manager by clicking on the desktop icon.
3. Click **Select** next to **Select IGEL OS binary image** and choose your image file.
4. If you want to add settings or certificates, click **Select** next to **Select IGEL OS settings** and choose the relevant files. You can add the following files:
   - `setup.ini`: The settings for IGEL OS; these are the settings that can be configured via IGEL Setup, the UMS configuration dialog, or a UMS profile.
   - Certificate files

5. When you have chosen your files, click **Apply**.



The files are added to the image.