IGEL OS Articles

Update and Upgrade

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 4)
2. Reducing the feature set by one of the following methods:
   - Using a UMS Profile (see page 4)
   - Using the Preconfigured Reduced INF File (see page 5)
   - Customizing the INF File (see page 5)

Determining Which Features to Deactivate

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

- Go to IGEL OS 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 Creating Profiles.
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 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.

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.

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: 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 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[1]. For more solutions compatible with IGEL OS, see Partner Solutions.

HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[2] 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.

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

ADS-Tec

Name	Endpoint Type	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

[1] https://www.igel.com/linux-3rd-party-hardware-database/
[2] https://www.igel.com/technology-partners/

Advantech

Name	Endpoint Type	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 18)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 18)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
(AiO) 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	

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

Fujitsu

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100	
t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100	
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100	
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100	
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100	
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
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)
Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	
Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Support for WWAN Intel XMM 7560 R+ (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	
t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	
Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	

HP Docking Stations

Name	Supported from IGEL OS Version
HP USB-C Docking Station G5	11.08.230
HP USB-C G5 Essential Dock	11.08.290

Intel

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
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	

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
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	Excluding support for WWAN
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	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	

Lenovo Docking Stations

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

LG

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
(AiO) 24CK550 N** (see page 18)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK550 W** (see page 18)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK560 N** (see page 18)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950 N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900 N	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
(AiO) 34CN650 N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600I	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650I	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601I	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360

OnLogic

Name	Endpoint Type	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	Endpoint Type	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

Rein Medical

Name	Endpoint Type	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	Endpoint Type	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 Alternative UD Pocket Hardware

DIGITTRADE

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

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

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 19)

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 21)

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 instructions, see Updating a UMS Installation.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter Registering Devices on the UMS Server in the UMS Manual.

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 (see page 22)

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 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 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 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 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 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 23)

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.

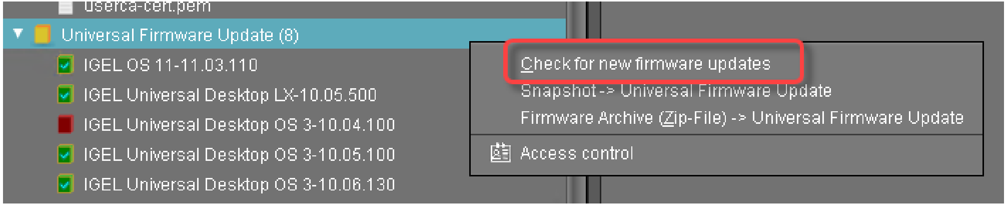
> If you use the High Availability Extension, note that Universal Firmware Updates are NOT synchronized, that is why you have to either download them to all HA nodes or configure an external (FTP) server.

Choose the procedure that suits your needs:

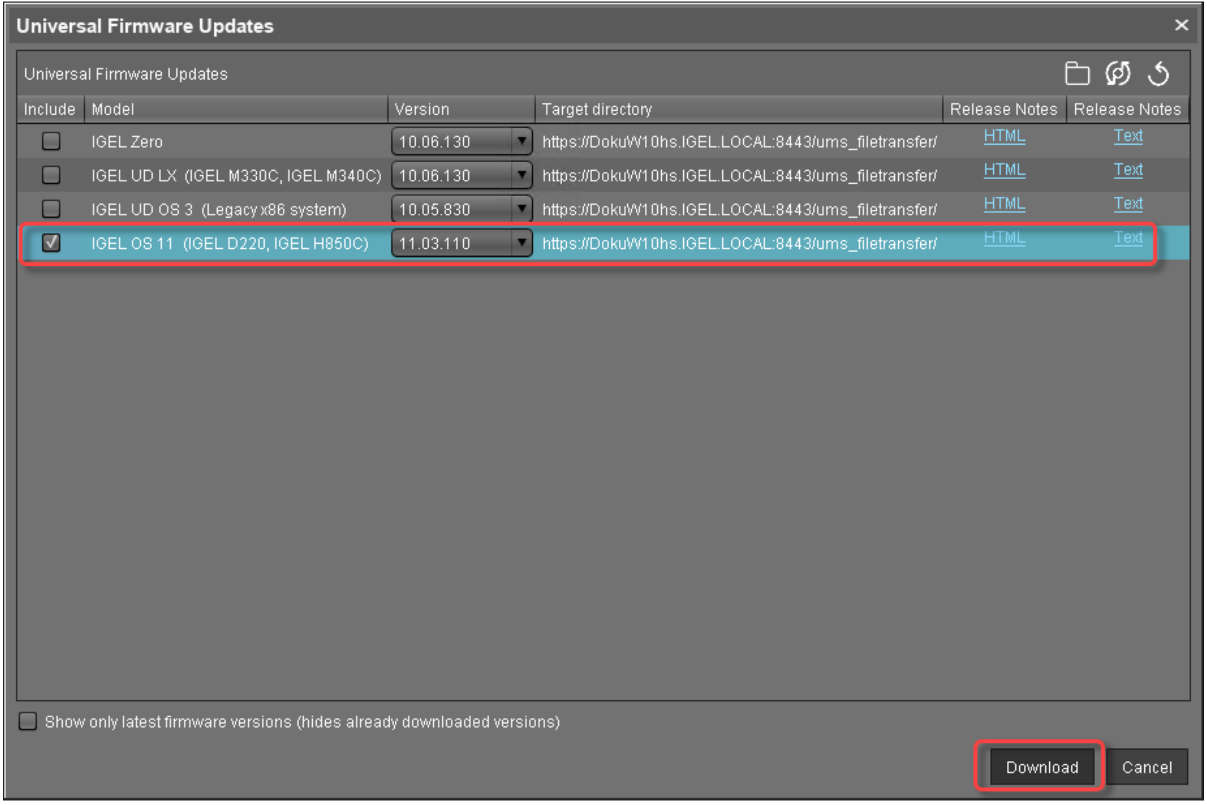
- Configuring the Universal Firmware Update with Files Hosted by the UMS (see page 23)
- Configuring the Universal Firmware Update with Files Hosted by FTP Server (Required for ICG) (see page 28)

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**.


userca-cert.pem
Universal Firmware Update (8)
IGEL OS 11-11.03.110
IGEL Universal Desktop LX-10.05.500
IGEL Universal Desktop OS 3-10.04.100
IGEL Universal Desktop OS 3-10.05.100
IGEL Universal Desktop OS 3-10.06.130
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

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

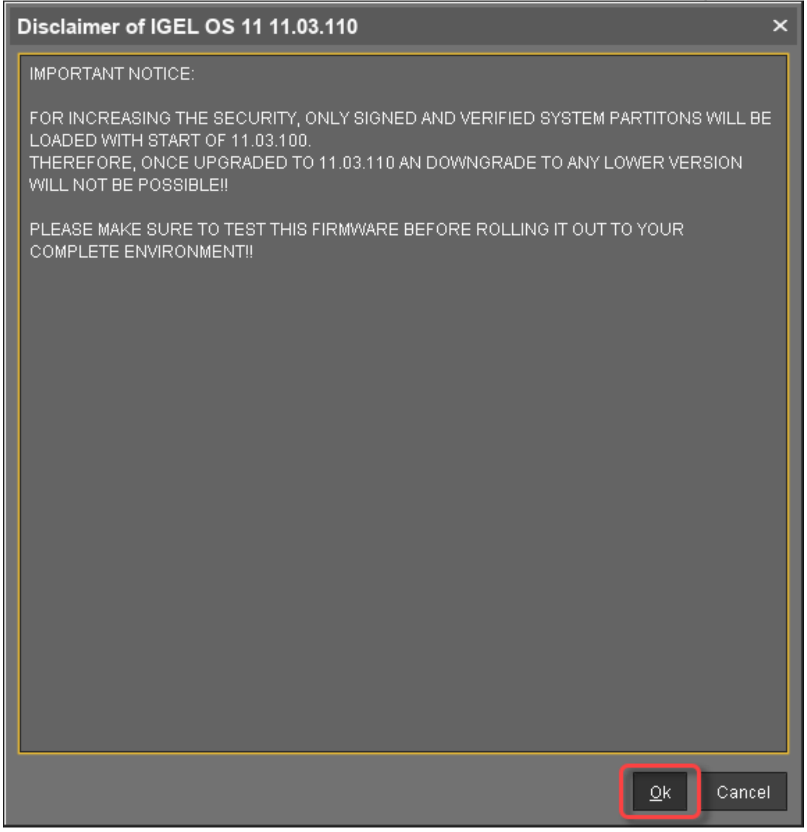


Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
☐	IGEL Zero	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
☐	IGEL UD LX (IGEL M330C, IGEL M340C)	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
☐	IGEL UD OS 3 (Legacy x86 system)	10.05.830	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
☑	IGEL OS 11 (IGEL D220, IGEL H850C)	11.03.110	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text

☐ Show only latest firmware versions (hides already downloaded versions)

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



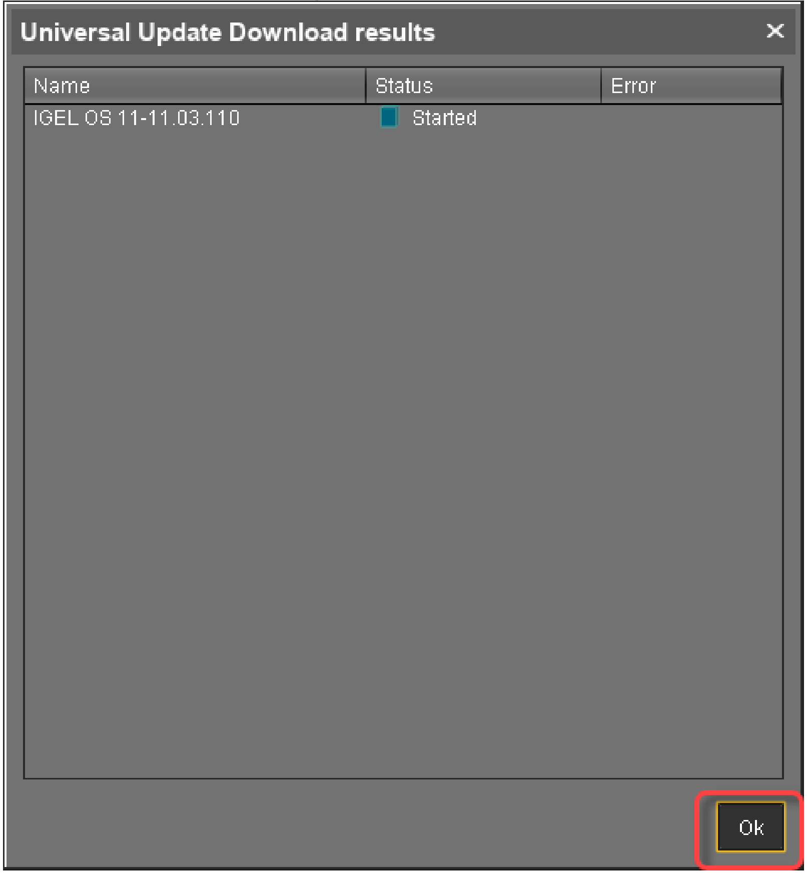
Disclaimer of IGEL OS 11 11.03.110

IMPORTANT NOTICE:

FOR INCREASING THE SECURITY, ONLY SIGNED AND VERIFIED SYSTEM PARTITONS WILL BE LOADED WITH START OF 11.03.100.
THEREFORE, ONCE UPGRADED TO 11.03.110 AN DOWNGRADE TO ANY LOWER VERSION WILL NOT BE POSSIBLE!!

PLEASE MAKE SURE TO TEST THIS FIRMWARE BEFORE ROLLING IT OUT TO YOUR COMPLETE ENVIRONMENT!!

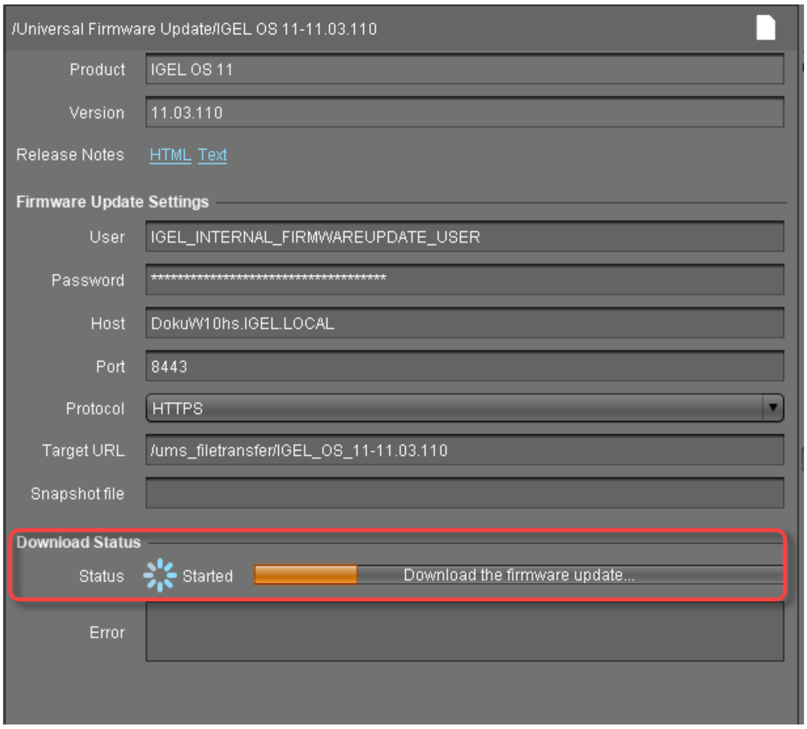
4. Confirm the status message.



Universal Update Download results

Name	Status	Error
IGEL OS 11-11.03.110	Started	

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



/Universal Firmware Update/IGEL OS 11-11.03.110

Product: IGEL OS 11

Version: 11.03.110

Release Notes: HTML Text

Firmware Update Settings

User: IGEL_INTERNAL_FIRMWAREUPDATE_USER

Password: **

Host: DokuW10hs.IGEL.LOCAL

Port: 8443

Protocol: HTTPS

Target URL: /ums_filetransfer/IGEL_OS_11-11.03.110

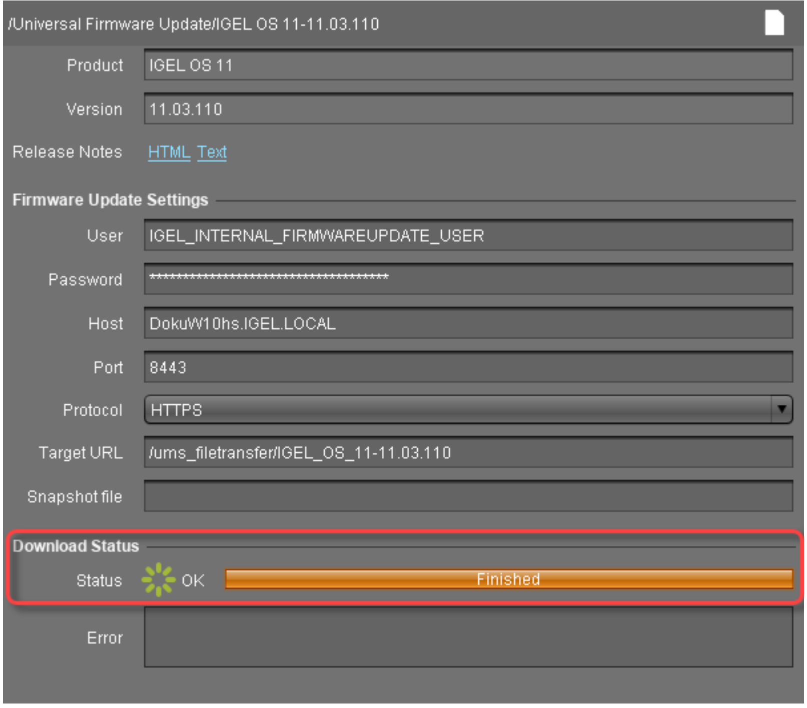
Snapshot file:

Download Status

Status: Started — Download the firmware update...

Error:

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



/Universal Firmware Update/IGEL OS 11-11.03.110

Product: IGEL OS 11

Version: 11.03.110

Release Notes: HTML Text

Firmware Update Settings

User: IGEL_INTERNAL_FIRMWAREUPDATE_USER

Password: **

Host: DokuW10hs.IGEL.LOCAL

Port: 8443

Protocol: HTTPS

Target URL: /ums_filetransfer/IGEL_OS_11-11.03.110

Snapshot file:

Download Status

Status: OK — Finished

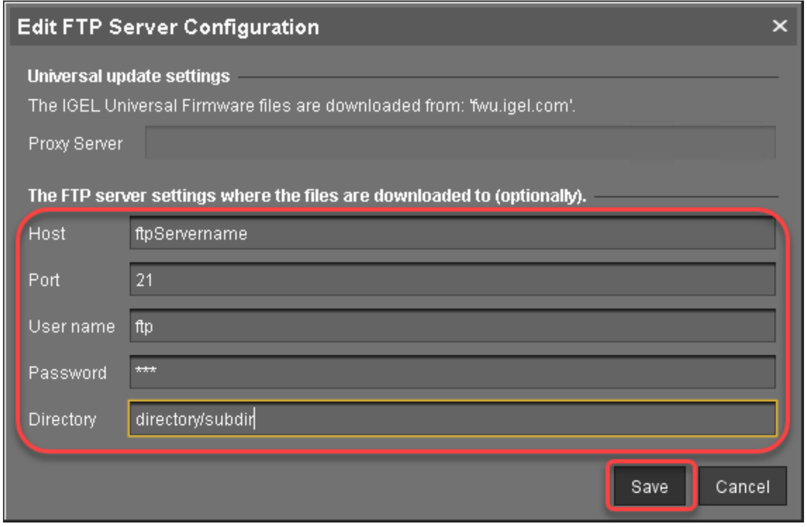
Error:

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**.



Edit FTP Server Configuration ×

Universal update settings

The IGEL Universal Firmware files are downloaded from: 'fwu.igel.com'.

Proxy Server

The FTP server settings where the files are downloaded to (optionally).

Host: ftpServername

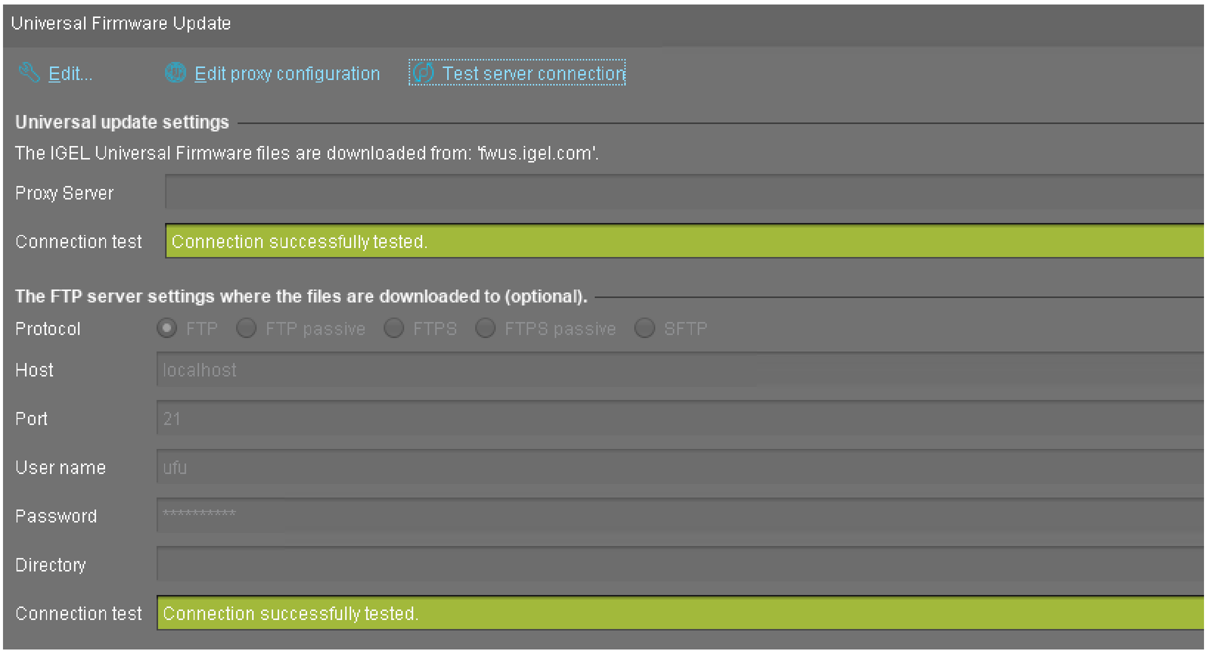
Port: 21

User name: ftp

Password: ***

Directory: directory/subdir

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:



Universal Firmware Update

Universal update settings

The IGEL Universal Firmware files are downloaded from: 'fwus.igel.com'.

Proxy Server

Connection test: Connection successfully tested.

The FTP server settings where the files are downloaded to (optional).

Protocol: ● FTP ○ FTP passive ○ FTPS ○ FTPS passive ○ SFTP

Host: localhost

Port: 21

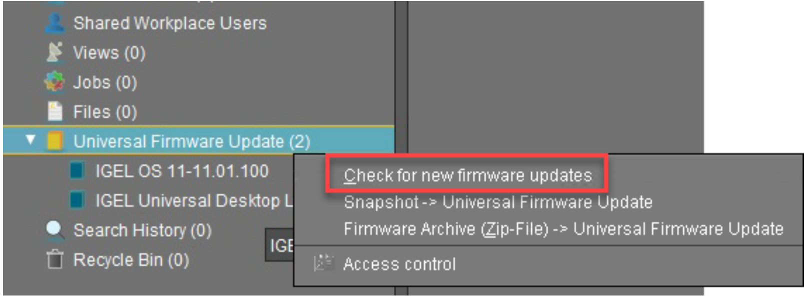
User name: ufu

Password: **********

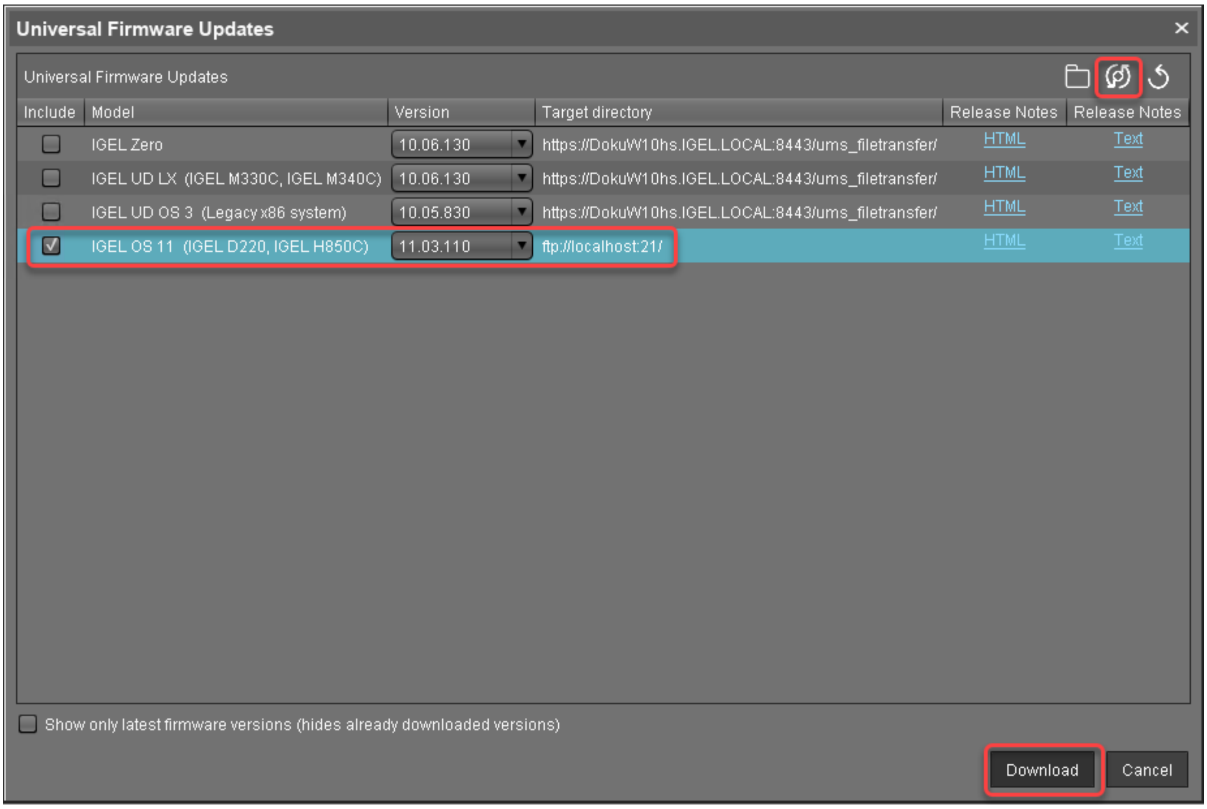
Directory

Connection test: Connection successfully tested.

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


Shared Workplace Users
Views (0)
Jobs (0)
Files (0)
Universal Firmware Update (2)
IGEL OS 11-11.01.100
IGEL Universal Desktop L
Search History (0)
Recycle Bin (0)
IGE
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

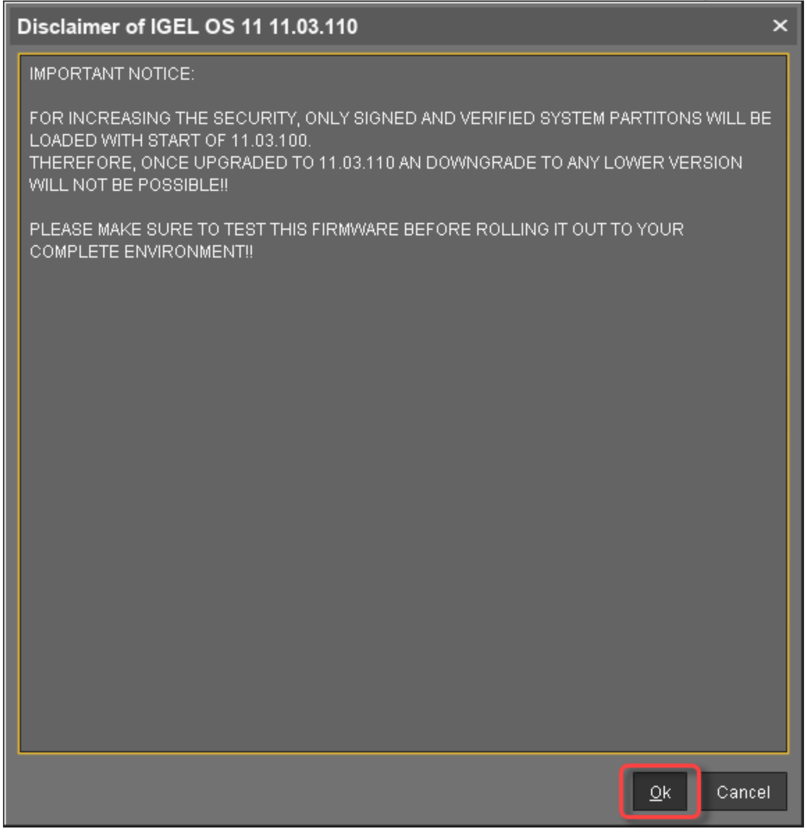
5. Select the entry for the IGEL OS 11 firmware, click to select the FTP server selected in step 2 and then select **Download**.



Include	Model	Version	Target directory	Release Notes	Release Notes
□	IGEL Zero	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
□	IGEL UD LX (IGEL M330C, IGEL M340C)	10.06.130	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
□	IGEL UD OS 3 (Legacy x86 system)	10.05.830	https://DokuW10hs.IGEL.LOCAL:8443/ums_filetransfer/	HTML	Text
☑	IGEL OS 11 (IGEL D220, IGEL H850C)	11.03.110	ftp://localhost:21/	HTML	Text

□ Show only latest firmware versions (hides already downloaded versions)

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



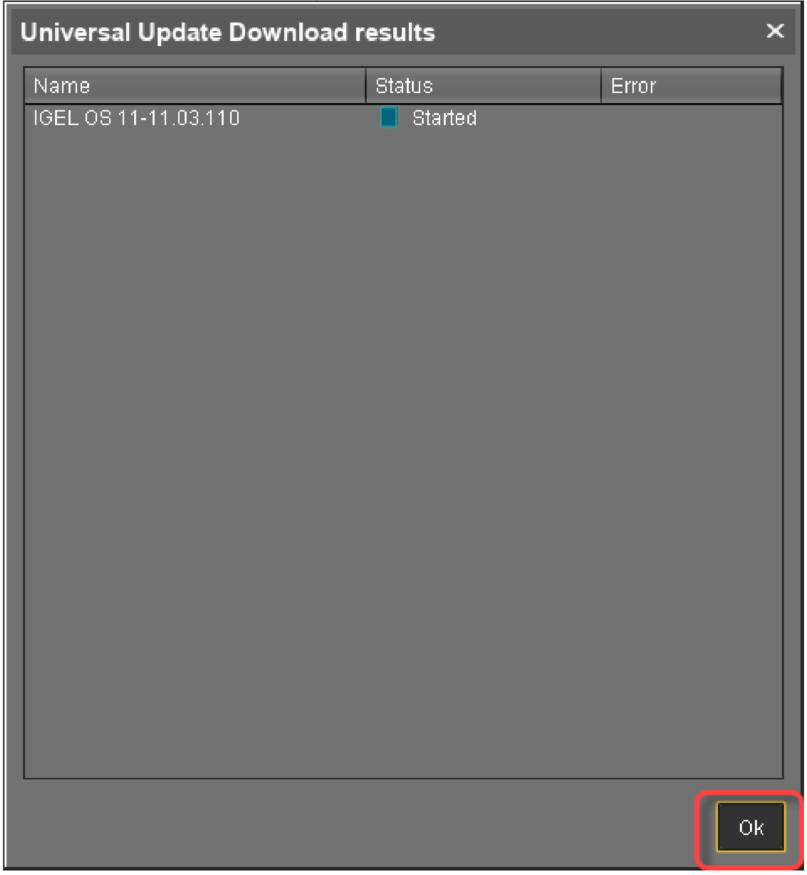
Disclaimer of IGEL OS 11 11.03.110

IMPORTANT NOTICE:

FOR INCREASING THE SECURITY, ONLY SIGNED AND VERIFIED SYSTEM PARTITONS WILL BE LOADED WITH START OF 11.03.100.
THEREFORE, ONCE UPGRADED TO 11.03.110 AN DOWNGRADE TO ANY LOWER VERSION WILL NOT BE POSSIBLE!!

PLEASE MAKE SURE TO TEST THIS FIRMWARE BEFORE ROLLING IT OUT TO YOUR COMPLETE ENVIRONMENT!!

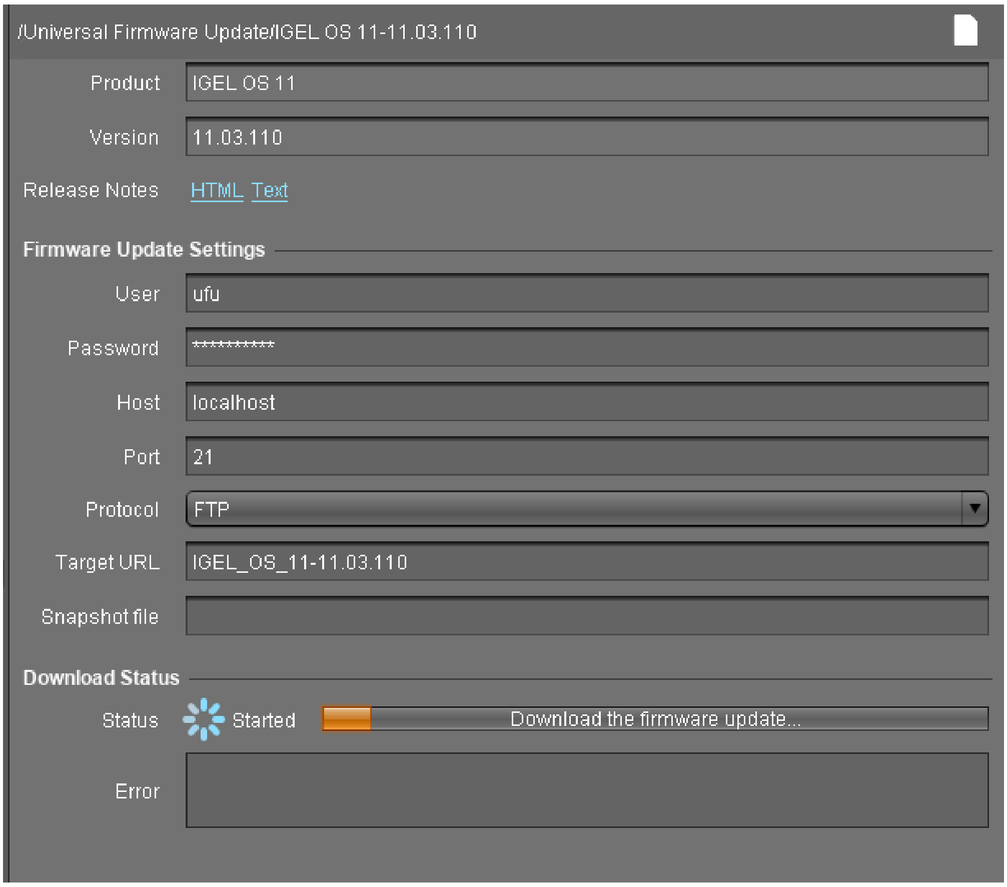
7. Confirm the status message.



Universal Update Download results

Name	Status	Error
IGEL OS 11-11.03.110	■ Started	

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



/Universal Firmware Update/IGEL OS 11-11.03.110

Product: IGEL OS 11

Version: 11.03.110

Release Notes: HTML Text

Firmware Update Settings

User: ufu

Password: ***********

Host: localhost

Port: 21

Protocol: FTP

Target URL: IGEL_OS_11-11.03.110

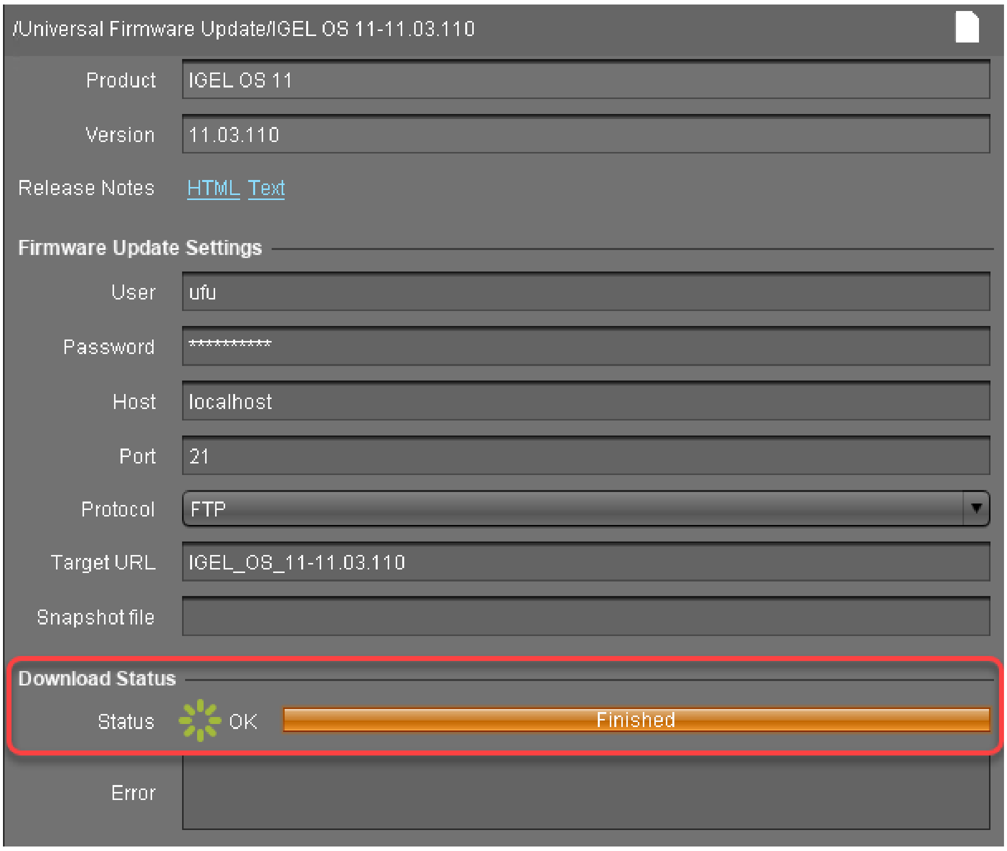
Snapshot file:

Download Status

Status: Started — Download the firmware update...

Error:

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



/Universal Firmware Update/IGEL OS 11-11.03.110

Product	IGEL OS 11
Version	11.03.110
Release Notes	HTML Text

Firmware Update Settings

User	ufu
Password	***********
Host	localhost
Port	21
Protocol	FTP
Target URL	IGEL_OS_11-11.03.110
Snapshot file	

Download Status

Status	OK Finished
Error	

Check List

✓ The Universal Firmware Update has been created successfully.

Next Step

>> Creating an Upgrade Profile (see page 34)

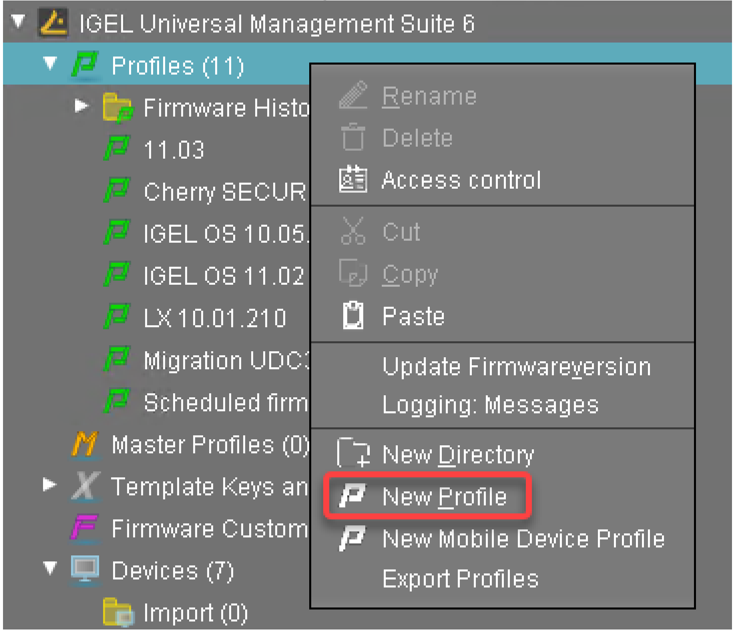
Creating an Upgrade Profile

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 34)
- For Devices that Are Connected via ICG (see page 38)

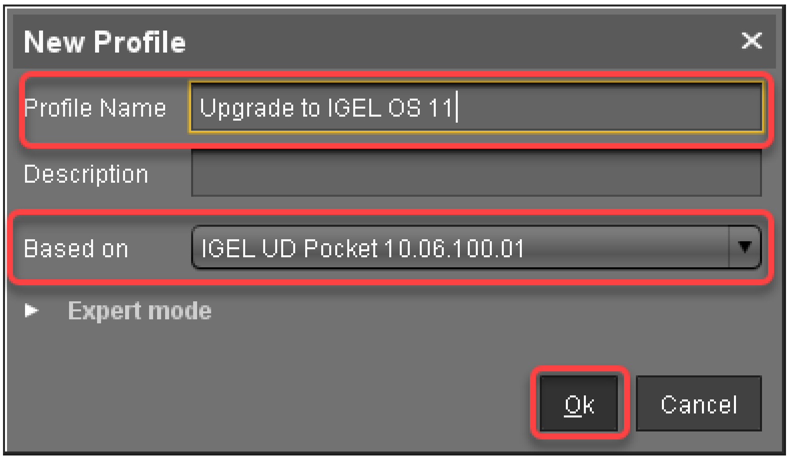
For Devices That Are in the UMS Network

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**.



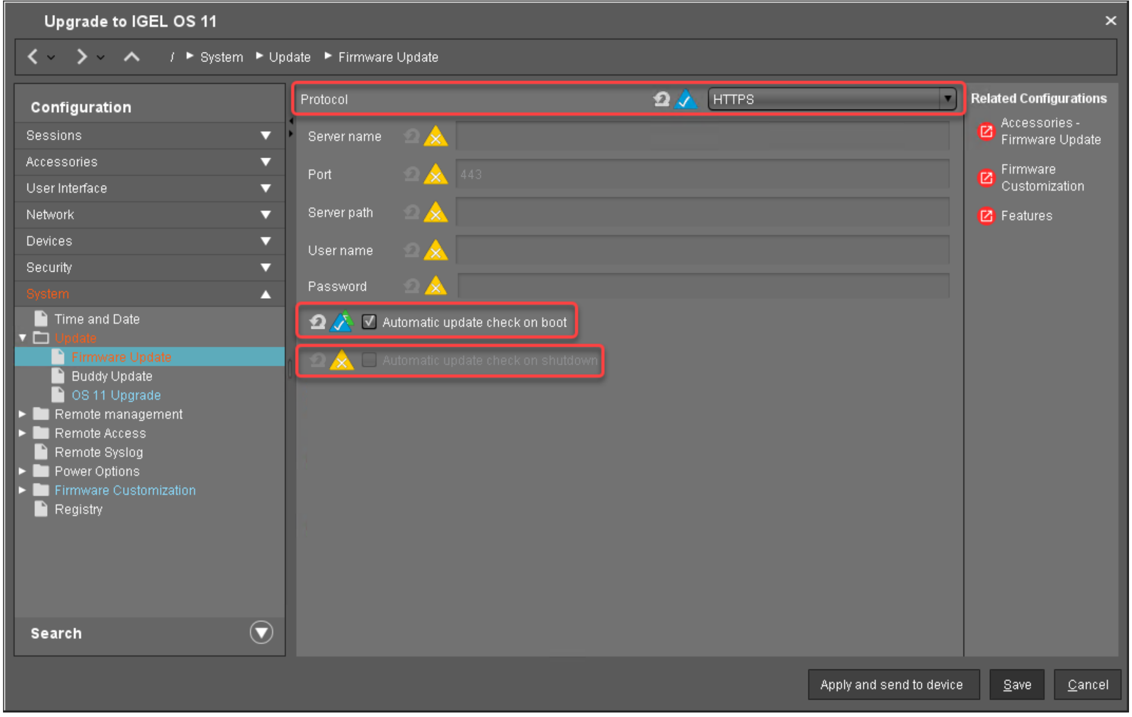
New Profile

Profile Name: Upgrade to IGEL OS 11

Description:

Based on: IGEL UD Pocket 10.06.100.01

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.



Upgrade to IGEL OS 11

/ ► System ► Update ► Firmware Update

Protocol: HTTPS

Server name:

Port: 443

Server path:

User name:

Password:

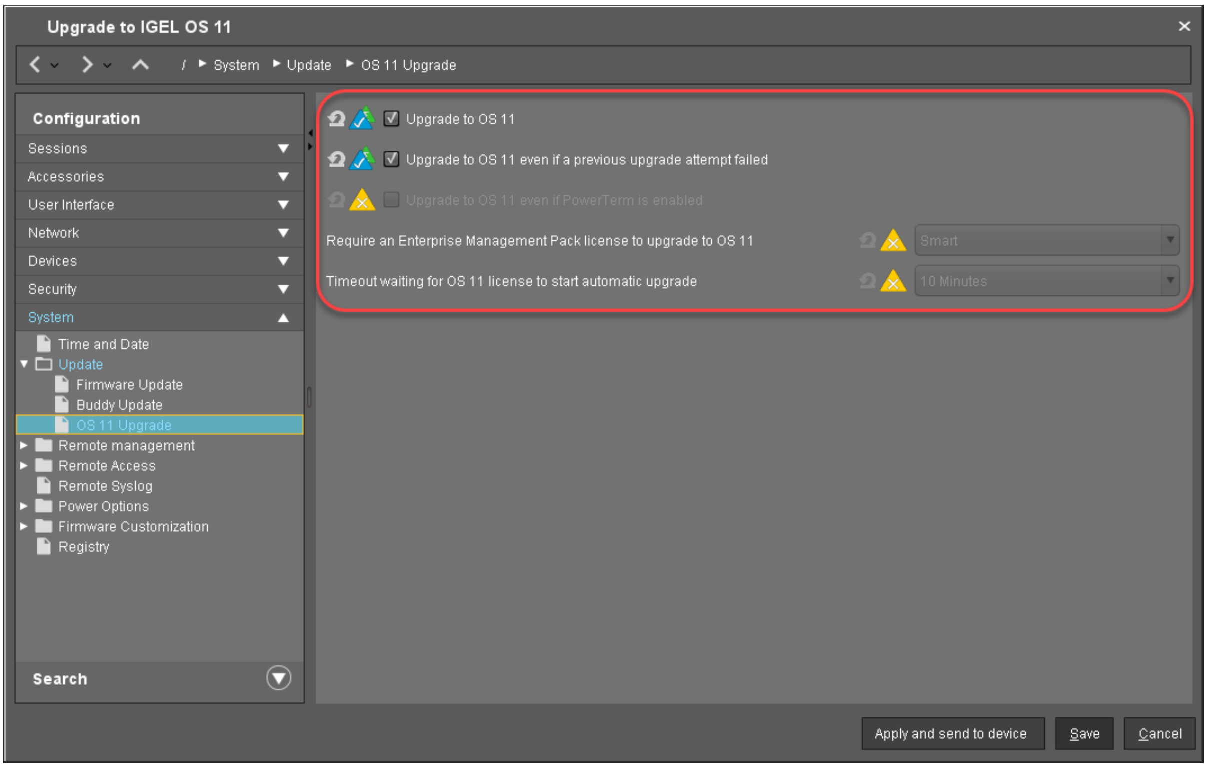
☑ Automatic update check on boot

□ Automatic update check on shutdown

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.



Upgrade to IGEL OS 11

/ ▸ System ▸ Update ▸ OS 11 Upgrade

☑ Upgrade to OS 11

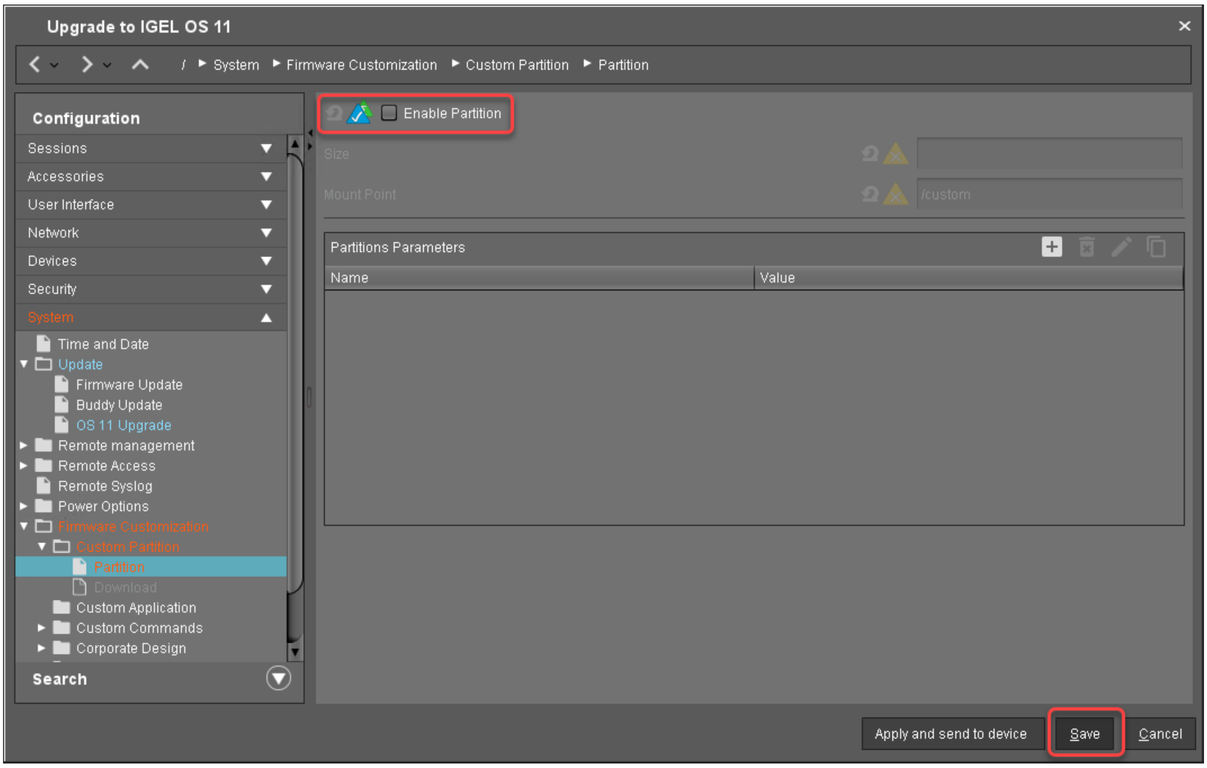
☑ Upgrade to OS 11 even if a previous upgrade attempt failed

□ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for OS 11 license to start automatic upgrade: 10 Minutes

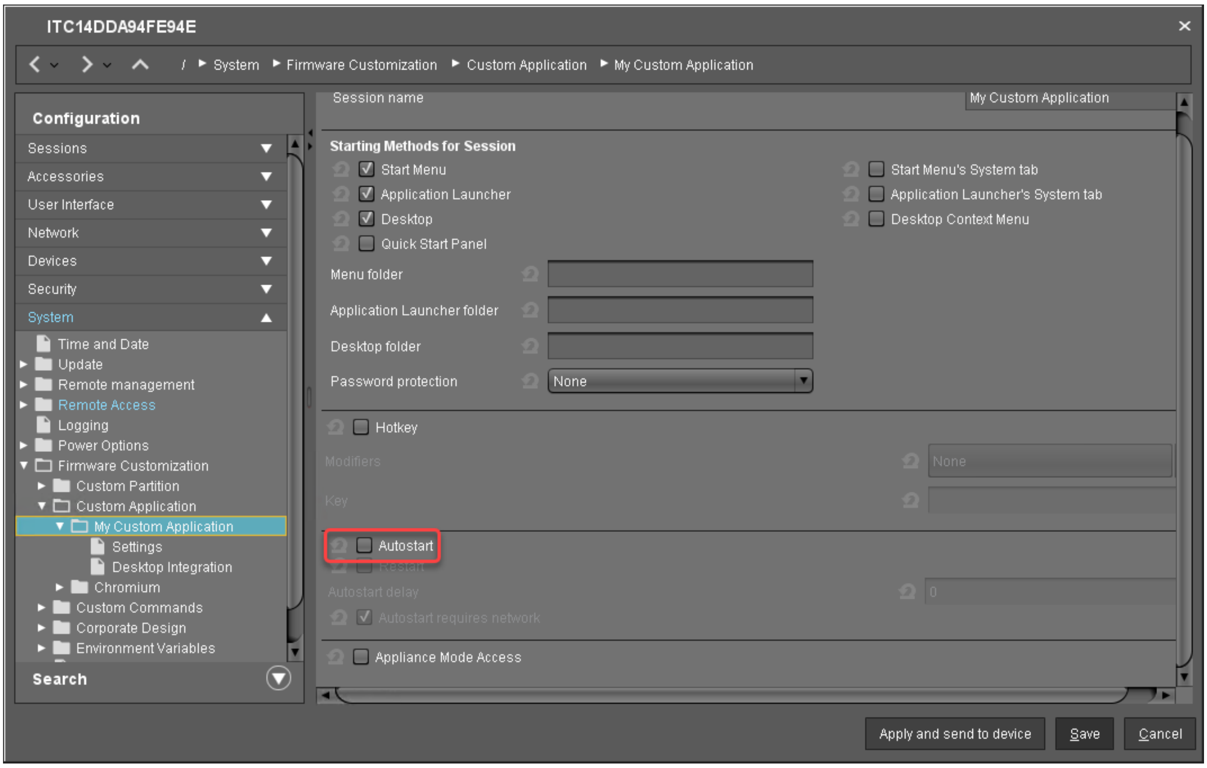
9. If you have a Custom Partition, go to **Firmware Customization > Custom Partition > Partition** and deactivate **Enable Partition**.



□ Enable Partition

Mount Point: /custom

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.



Session name: My Custom Application

Starting Methods for Session

☑ Start Menu

☑ Application Launcher

☑ Desktop

☐ Quick Start Panel

☐ Start Menu's System tab

☐ Application Launcher's System tab

☐ Desktop Context Menu

Menu folder:

Application Launcher folder:

Desktop folder:

Password protection: None

☐ Hotkey

Modifiers: None

Key:

☐ Autostart

☐ Restart

Autostart delay: 0

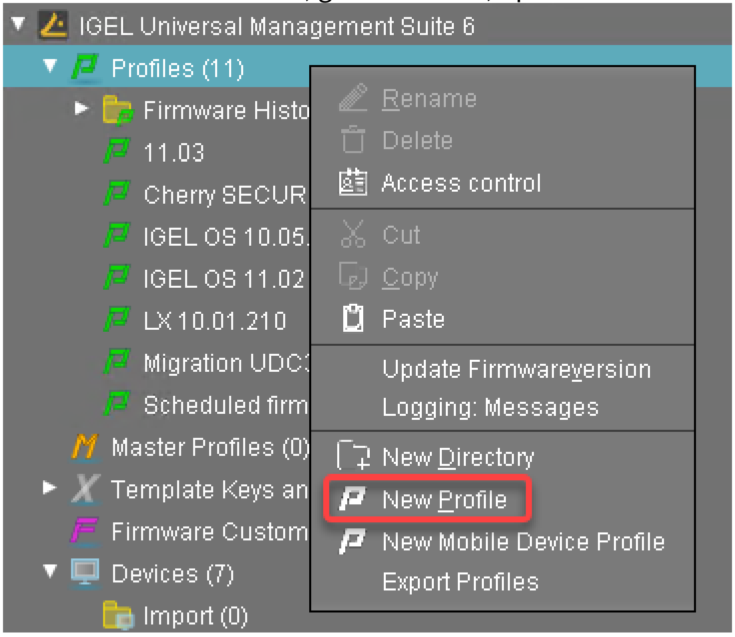
☑ Autostart requires network

☐ Appliance Mode Access

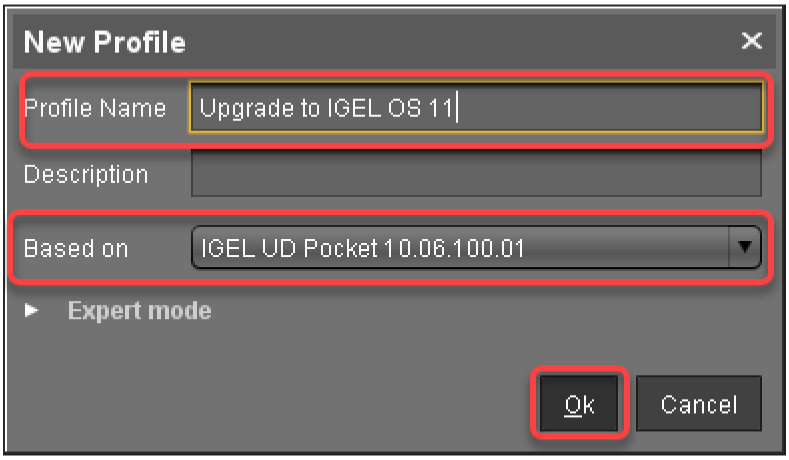
11. Click **Save**.

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**.



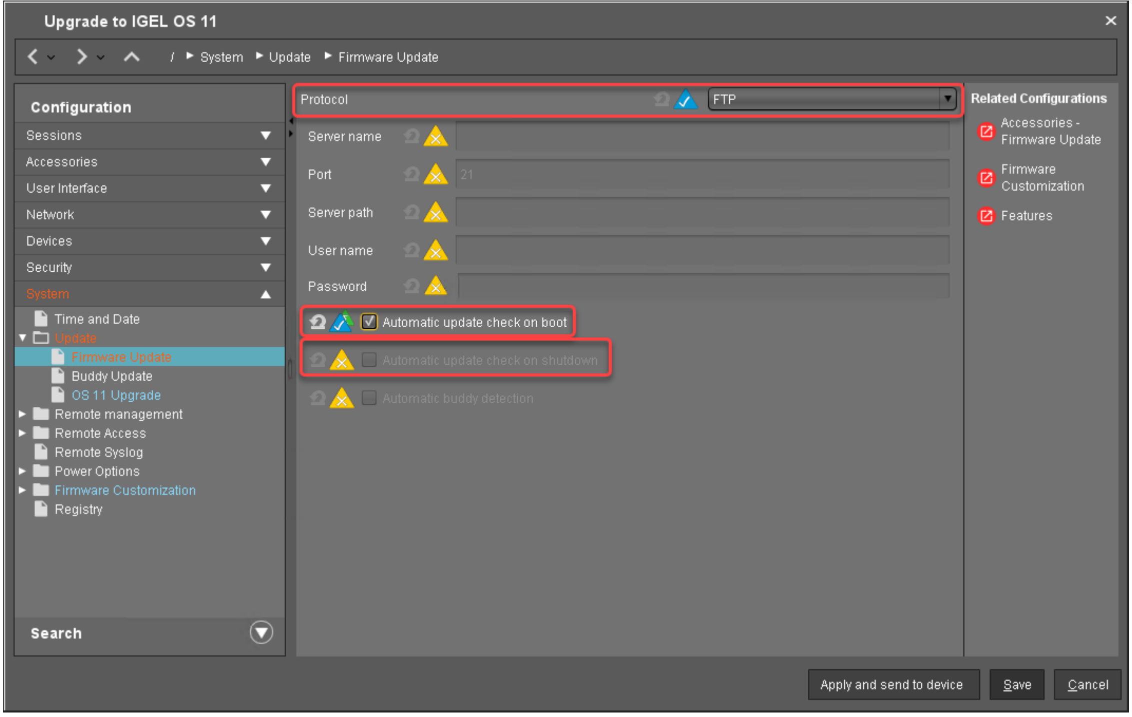
New Profile

Profile Name: Upgrade to IGEL OS 11

Description:

Based on: IGEL UD Pocket 10.06.100.01

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.



Upgrade to IGEL OS 11

/ ▸ System ▸ Update ▸ Firmware Update

Protocol: FTP

Server name:

Port: 21

Server path:

User name:

Password:

☑ Automatic update check on boot

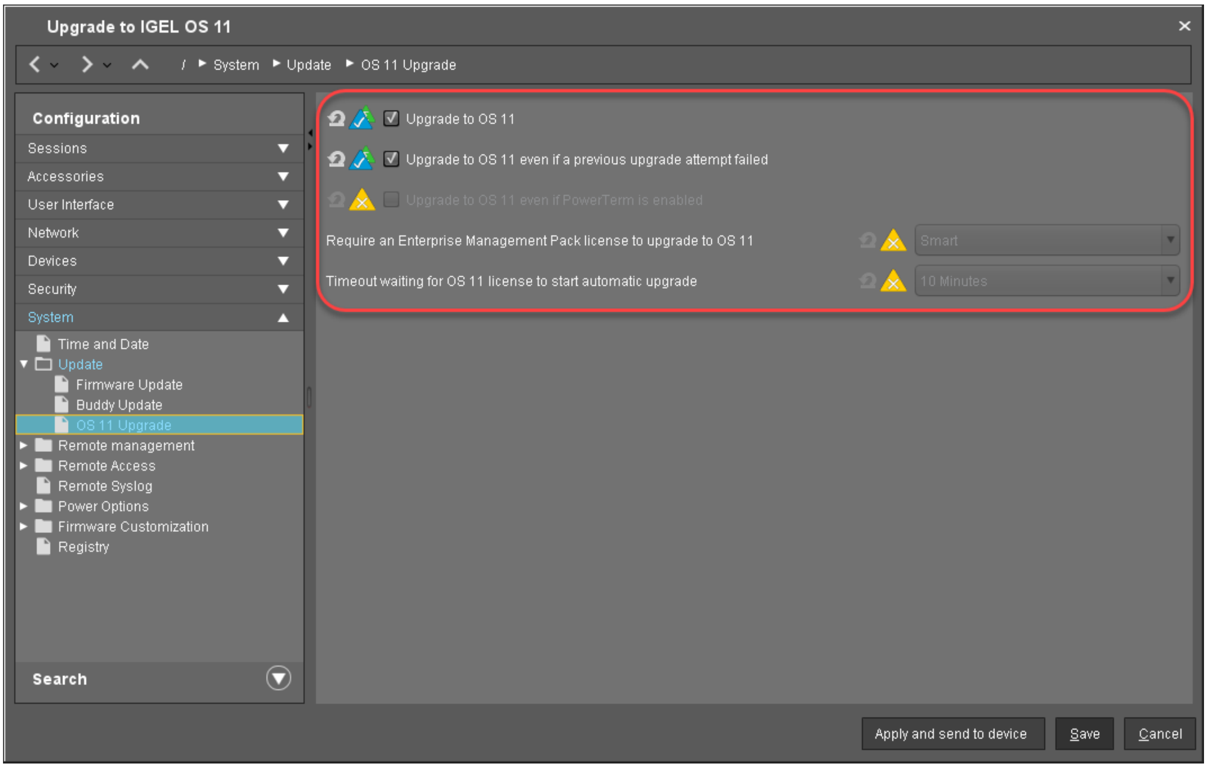
□ Automatic update check on shutdown

□ Automatic buddy detection

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.



Upgrade to IGEL OS 11

System ▸ Update ▸ OS 11 Upgrade

☑ Upgrade to OS 11

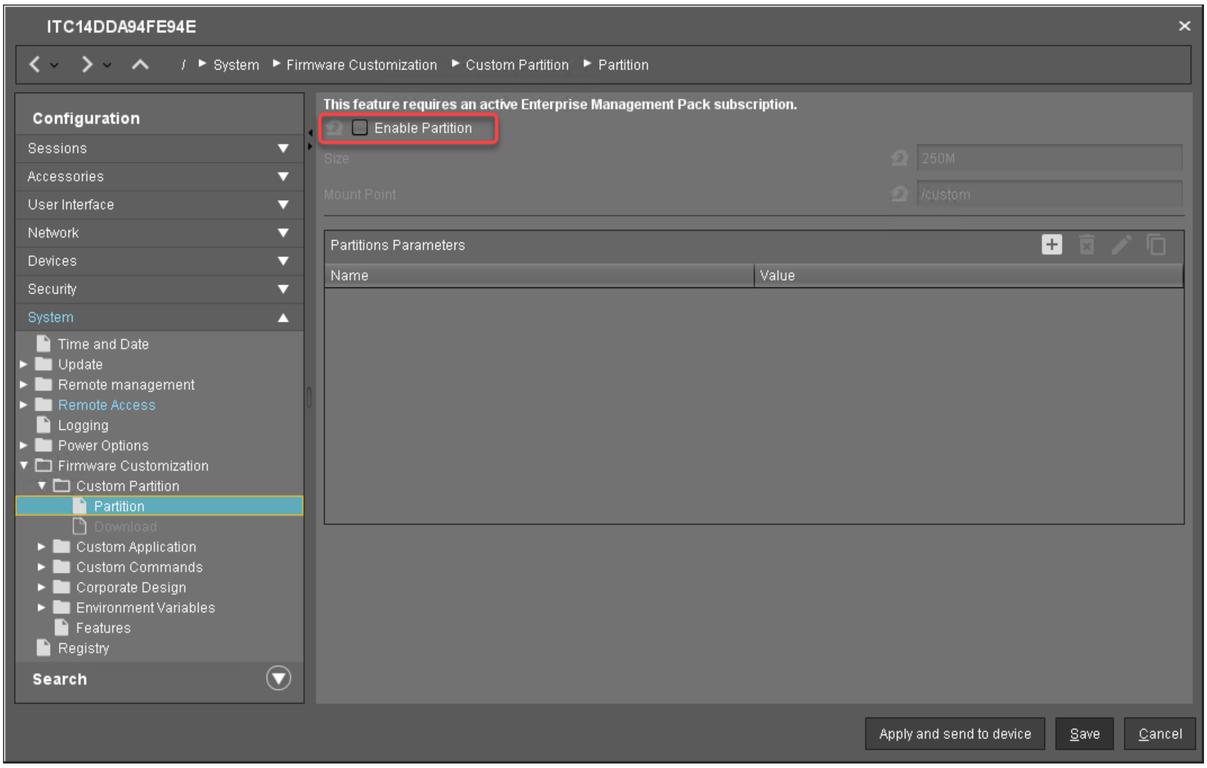
☑ Upgrade to OS 11 even if a previous upgrade attempt failed

□ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for OS 11 license to start automatic upgrade: 10 Minutes

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



ITC14DDA94FE94E

System ▸ Firmware Customization ▸ Custom Partition ▸ Partition

This feature requires an active Enterprise Management Pack subscription.

□ Enable Partition

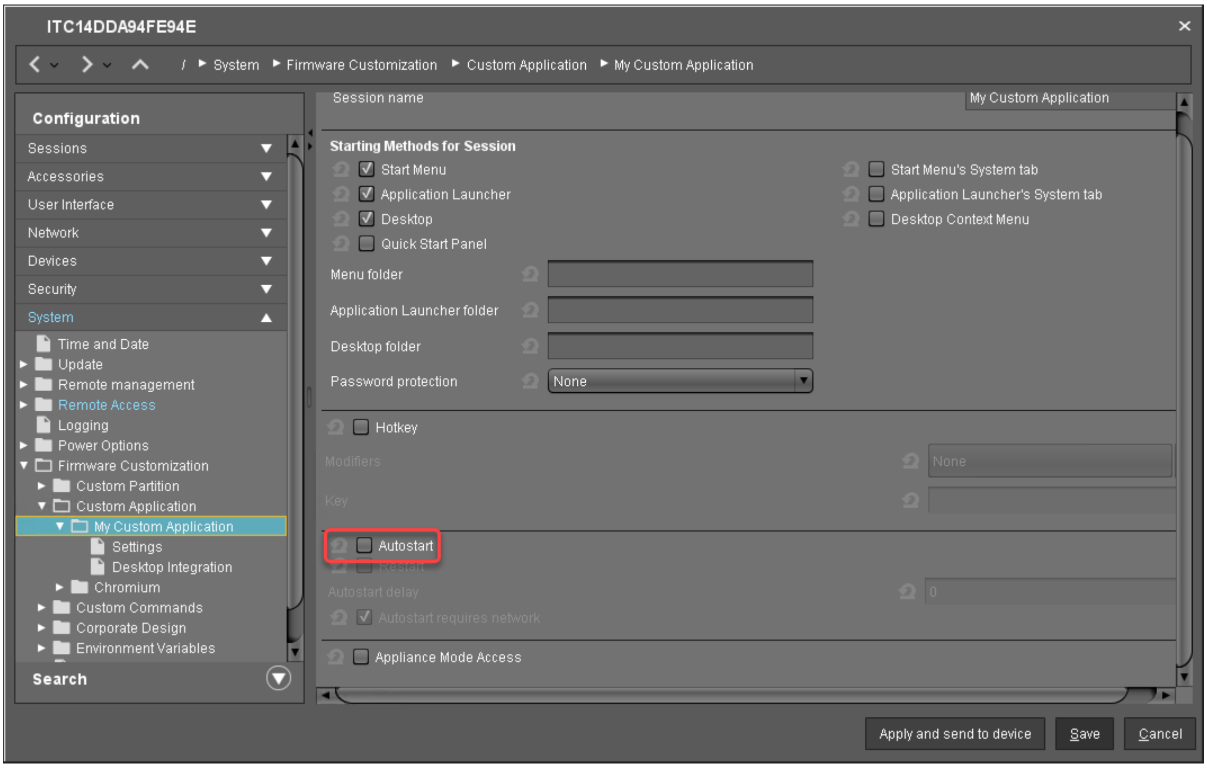
Size: 250M

Mount Point: /custom

Partitions Parameters

Name	Value

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.



Session name: My Custom Application

Starting Methods for Session

☑ Start Menu
☑ Application Launcher
☑ Desktop
□ Quick Start Panel
□ Start Menu's System tab
□ Application Launcher's System tab
□ Desktop Context Menu

Menu folder:
Application Launcher folder:
Desktop folder:
Password protection: None

□ Hotkey
Modifiers: None
Key:

□ Autostart
□ Restart
Autostart delay: 0
☑ Autostart requires network

□ Appliance Mode Access

11. Click **Save**.

Check List

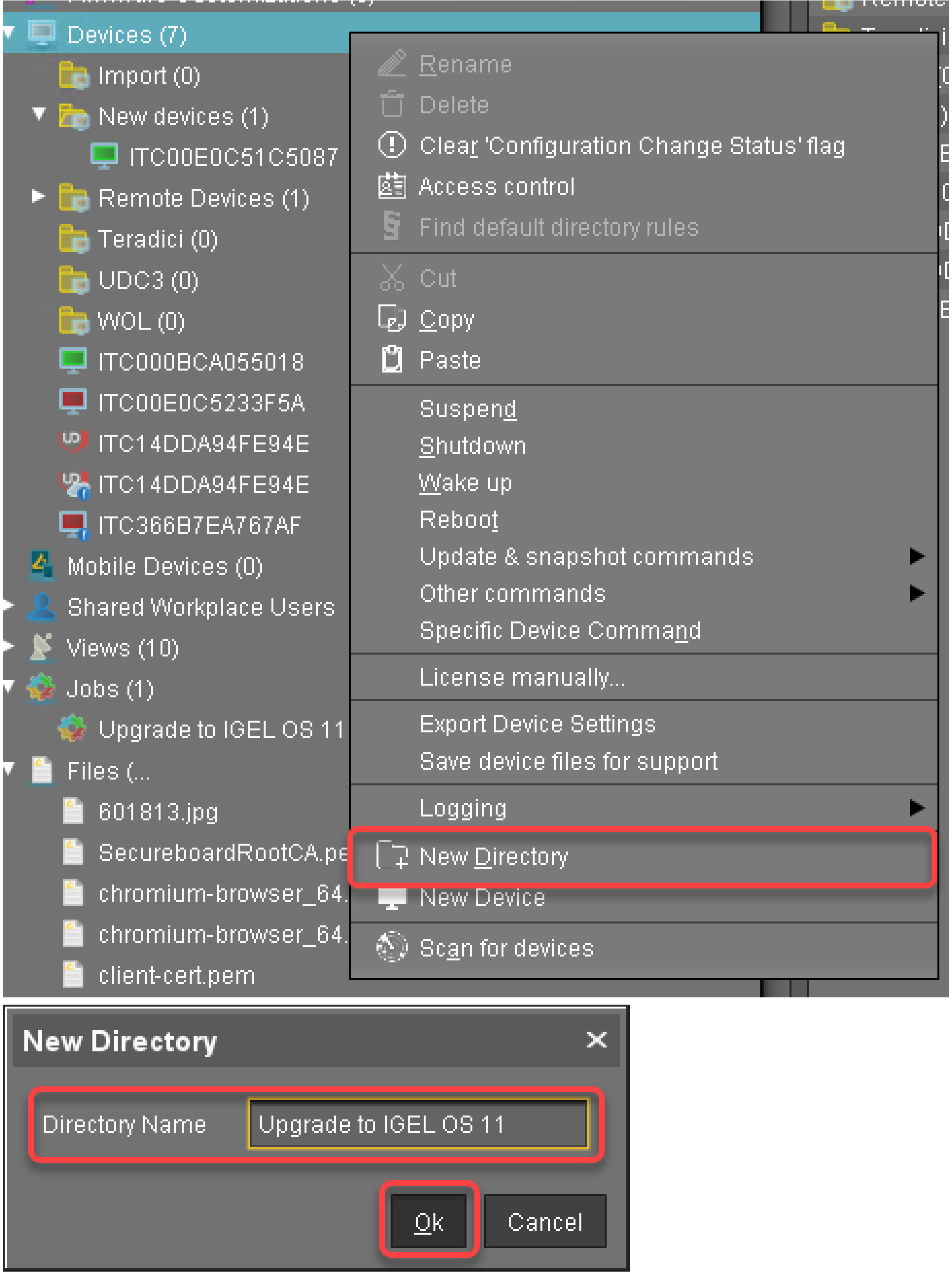
✓ The upgrade profile is configured properly for your needs.

Next Step

>> Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices (see page 43)

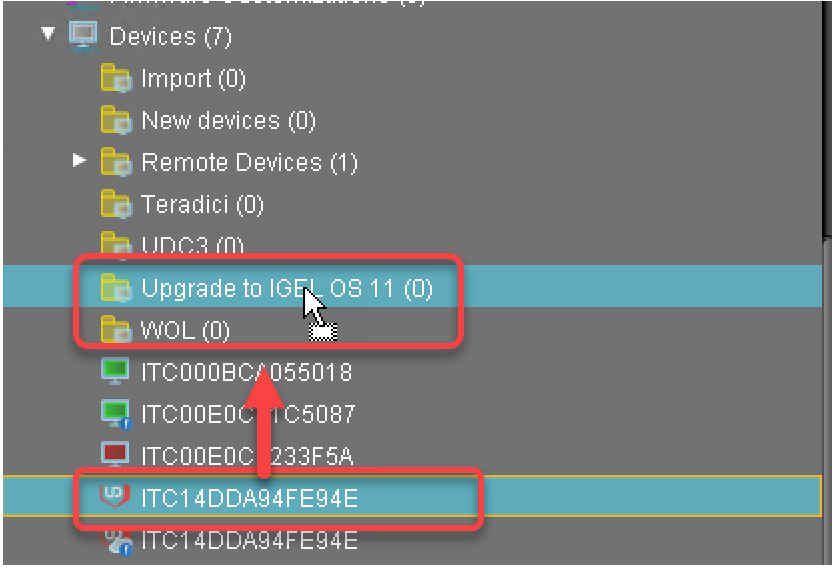
Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices

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 Configuring the Distribution Conditions, section "Distributing Licenses to Devices in a Specified Directory".

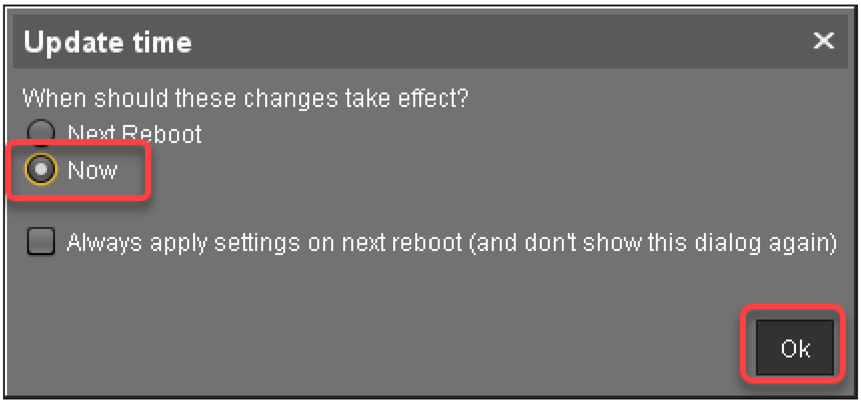


Directory Name: Upgrade to IGEL OS 11

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.



Update time

When should these changes take effect?

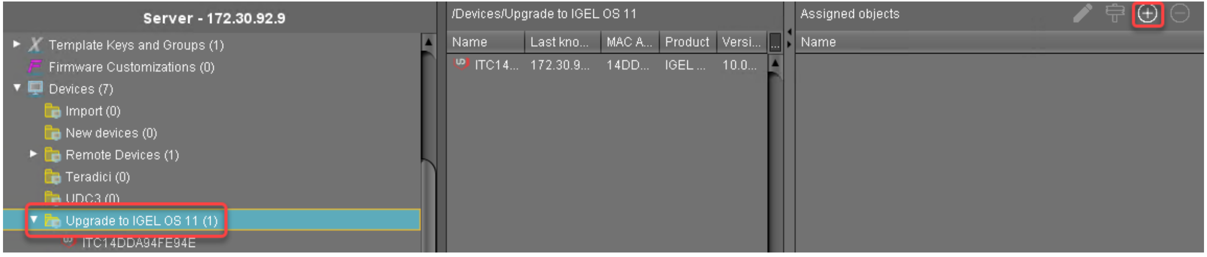
○ Next Reboot

● Now

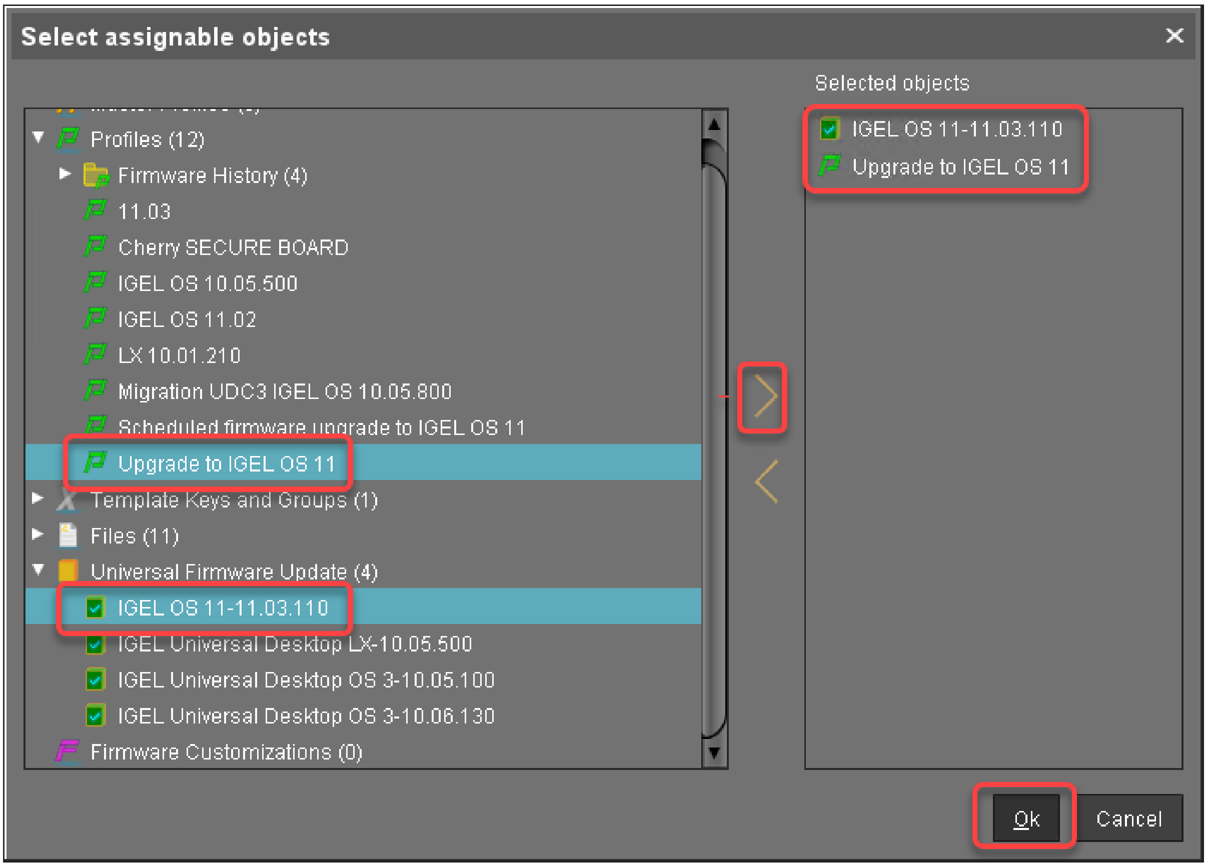
□ Always apply settings on next reboot (and don't show this dialog again)

Ok

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**.

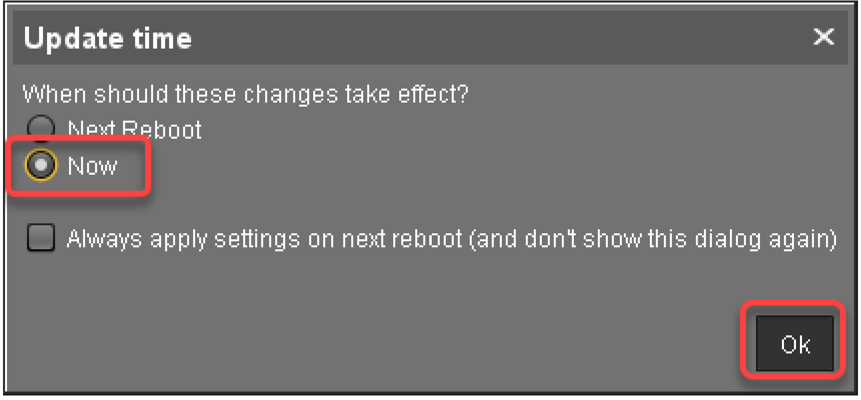


Select assignable objects

Selected objects: IGEL OS 11-11.03.110, Upgrade to IGEL OS 11

Profiles (12)
Firmware History (4)
11.03
Cherry SECURE BOARD
IGEL OS 10.05.500
IGEL OS 11.02
LX 10.01.210
Migration UDC3 IGEL OS 10.05.800
Scheduled firmware upgrade to IGEL OS 11
Upgrade to IGEL OS 11
Template Keys and Groups (1)
Files (11)
Universal Firmware Update (4)
IGEL OS 11-11.03.110
IGEL Universal Desktop LX-10.05.500
IGEL Universal Desktop OS 3-10.05.100
IGEL Universal Desktop OS 3-10.06.130
Firmware Customizations (0)
Ok
Cancel

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



Update time

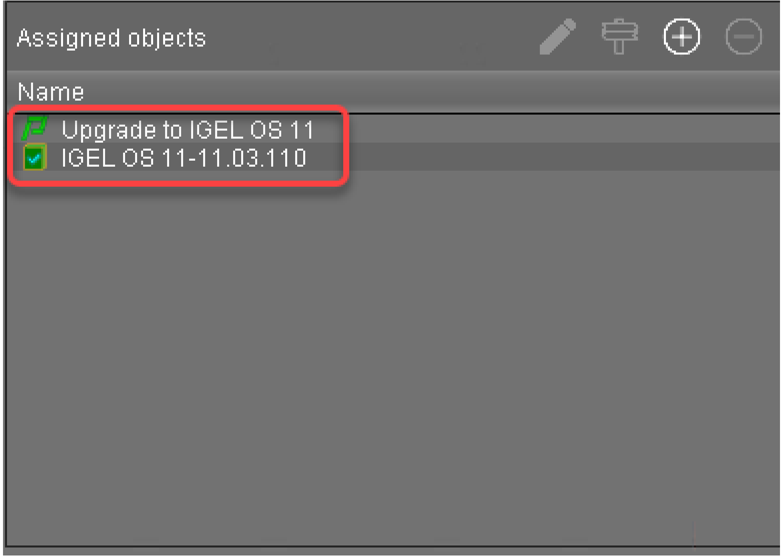
When should these changes take effect?

○ Next Reboot

● Now

□ Always apply settings on next reboot (and don't show this dialog again)

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



Assigned objects

Name

Upgrade to IGEL OS 11

IGEL OS 11-11.03.110

ⓘ 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, section "Distributing Licenses to Devices in a Specified Directory".

Check List

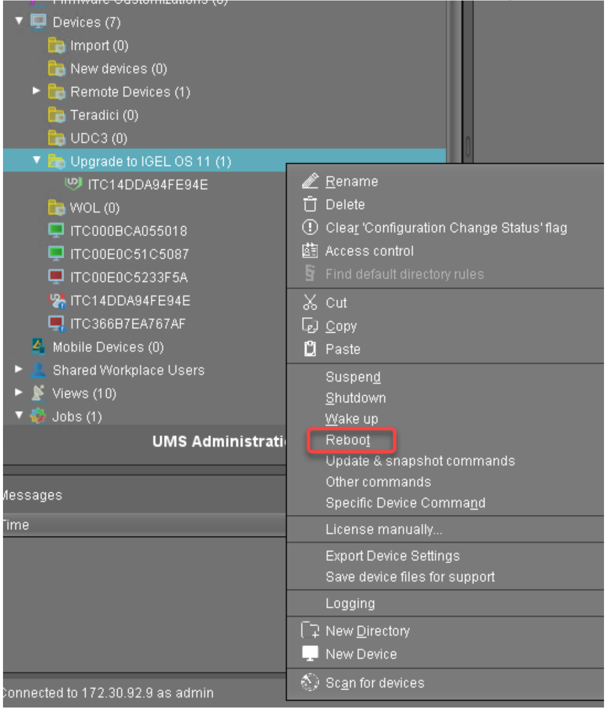
✓ The test devices are in a directory to which the upgrade profile and the Universal Firmware Update are assigned.

Next Step

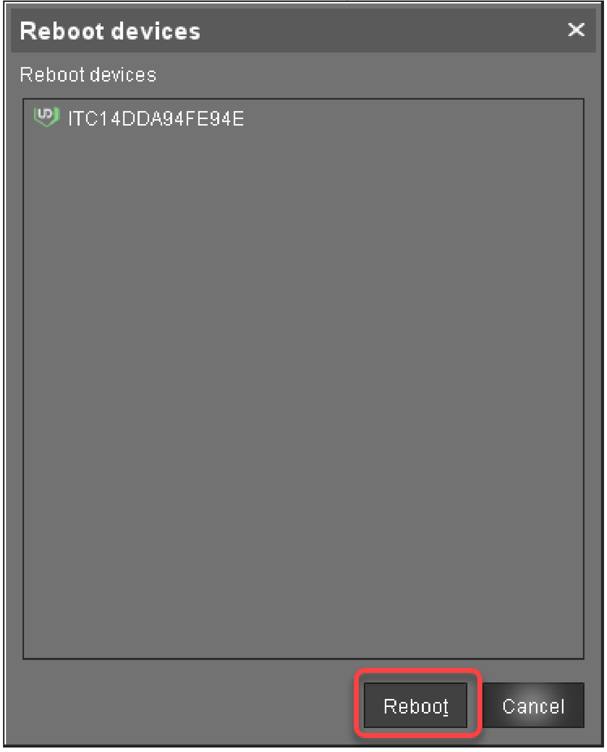
>> Testing the Upgrade (see page 47)

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 34), 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

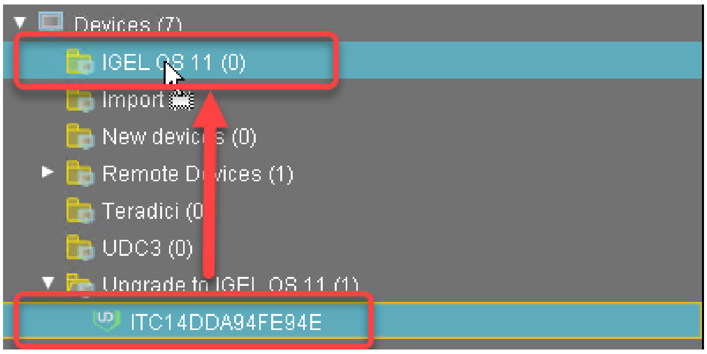
>> Unassigning the Upgrade Profile and the Universal Firmware Update (see page 49)

Unassigning the Upgrade Profile and the Universal Firmware Update

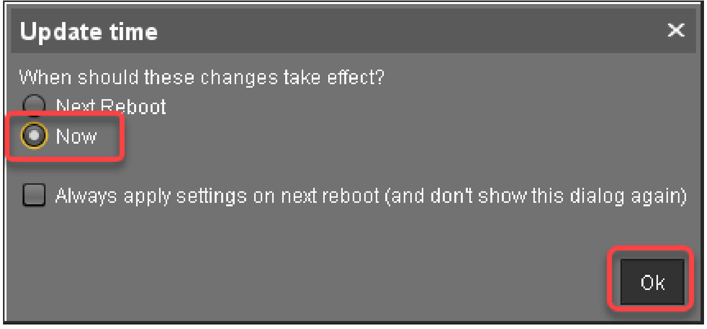
The upgrade profile and the Universal Firmware Update should be unassigned from the devices after they have been upgraded to IGEL OS 11 successfully.

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.



Update time

When should these changes take effect?

○ Next Reboot

● Now

□ Always apply settings on next reboot (and don't show this dialog again)

Ok

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 50)

If no device has a Custom Partition:

>> Upgrading All Devices (see page 51)

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 49). 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.

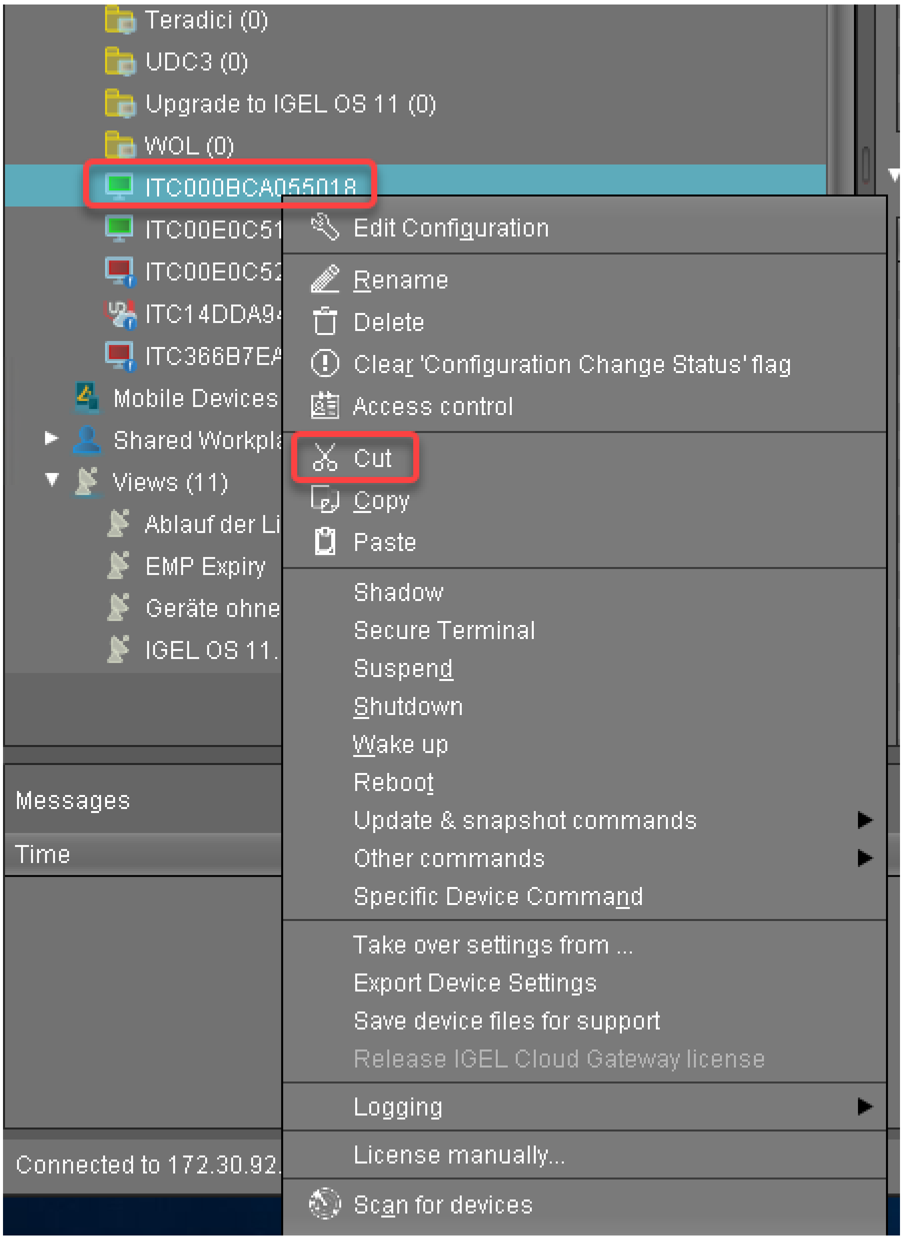
Next Step

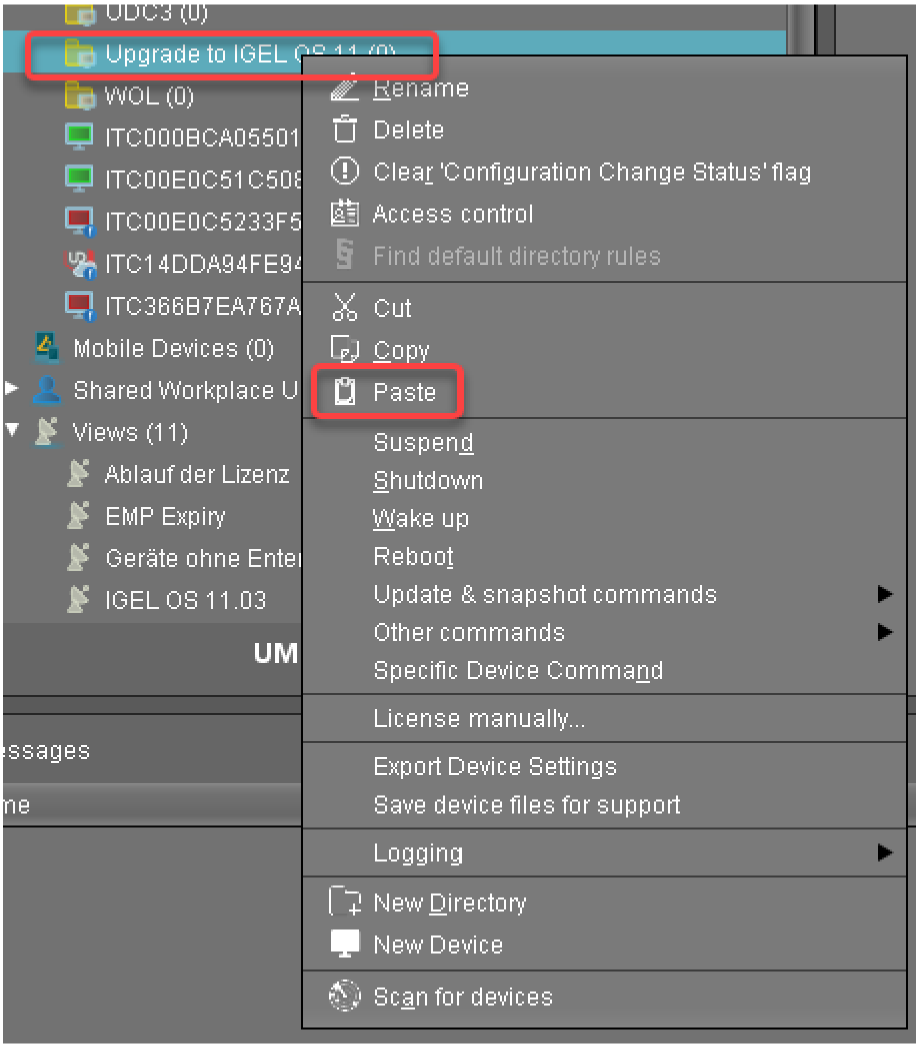
>> Upgrading All Devices (see page 51)

Upgrading All Devices

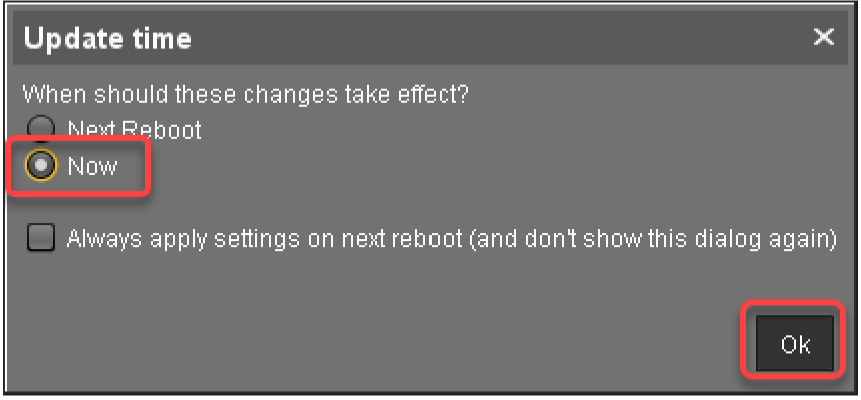
Assigning the Upgrade Profile and the Universal Firmware Update to the Devices

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.


Teradici (0)
UDC3 (0)
Upgrade to IGEL OS 11 (0)
WOL (0)
ITC000BCA055018
ITC00E0C51
ITC00E0C52
ITC14DDA94
ITC366B7EA
Mobile Devices
Shared Workpla
Views (11)
Ablauf der Li
EMP Expiry
Geräte ohne
IGEL OS 11.
Messages
Time
Connected to 172.30.92.
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



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.



Update time

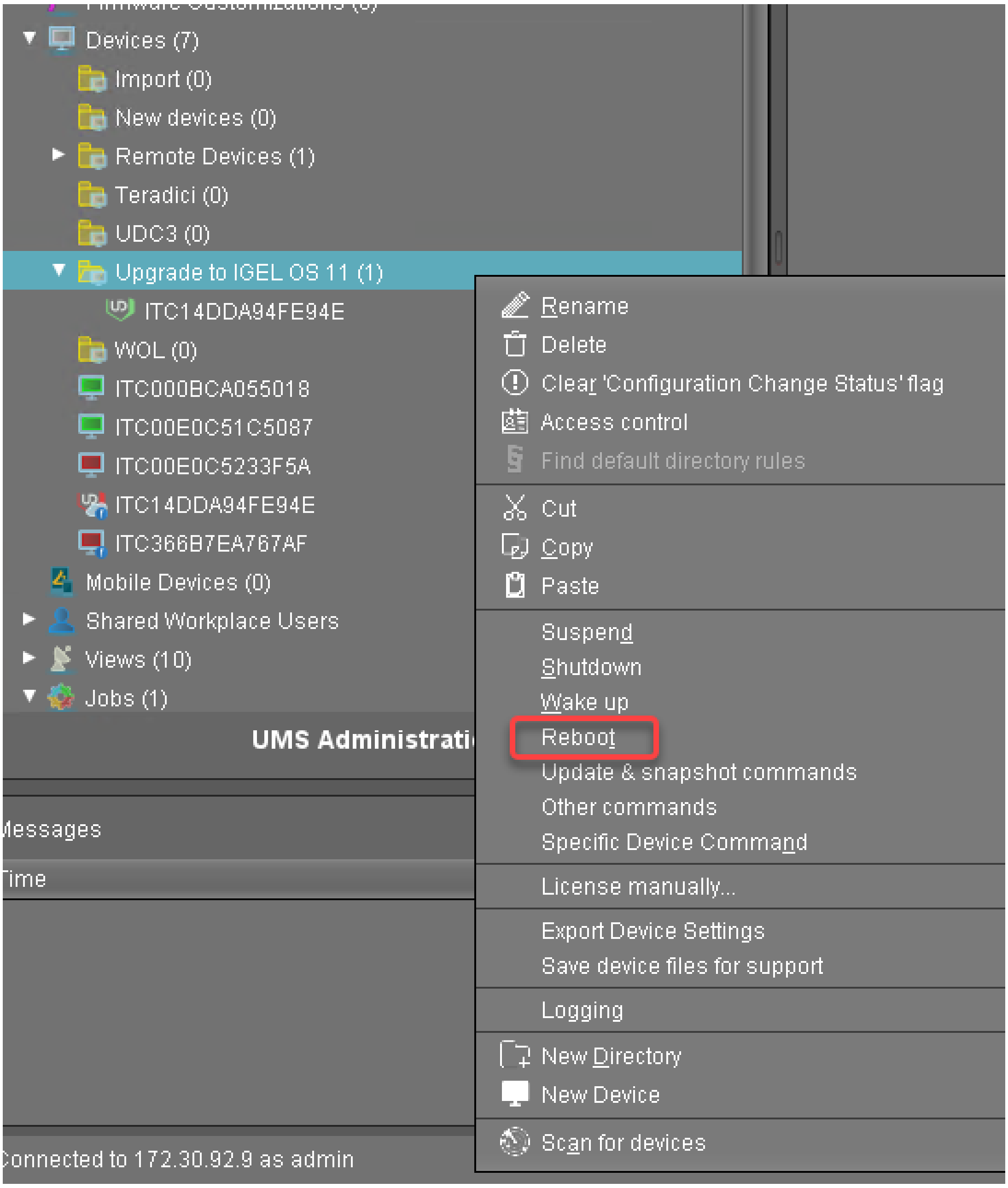
When should these changes take effect?

○ Next Reboot

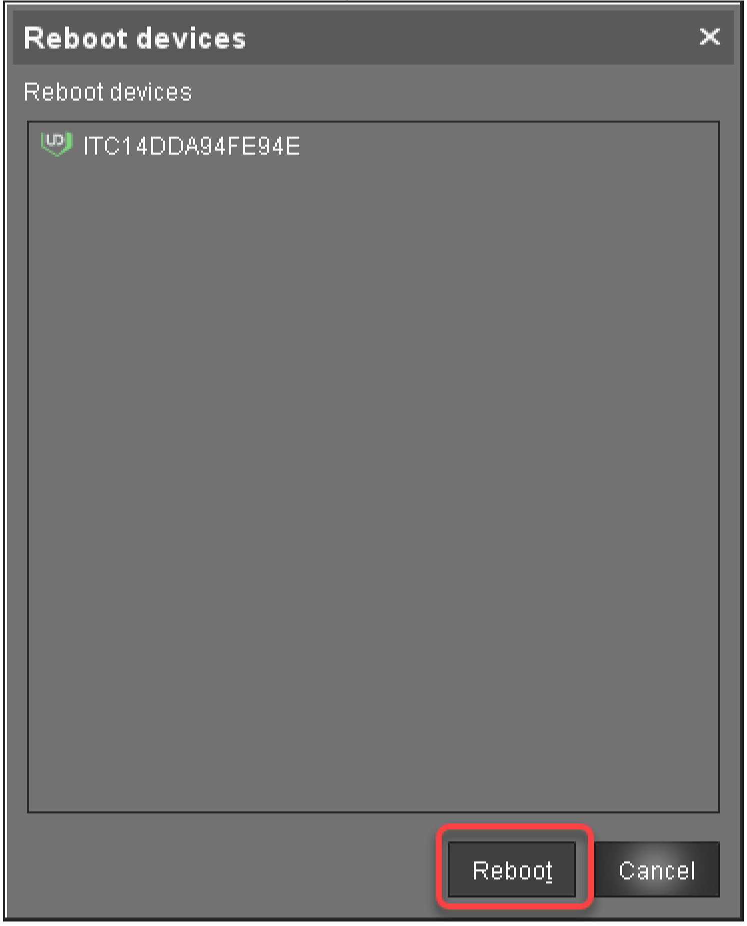
● Now

□ Always apply settings on next reboot (and don't show this dialog again)

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


Devices (7)
Import (0)
New devices (0)
Remote Devices (1)
Teradici (0)
UDC3 (0)
Upgrade to IGEL OS 11 (1)
ITC14DDA94FE94E
WOL (0)
ITC000BCA055018
ITC00E0C51C5087
ITC00E0C5233F5A
ITC14DDA94FE94E
ITC366B7EA767AF
Mobile Devices (0)
Shared Workplace Users
Views (10)
Jobs (1)
UMS Administrati
lessages
ime
onnected to 172.30.92.9 as admin
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

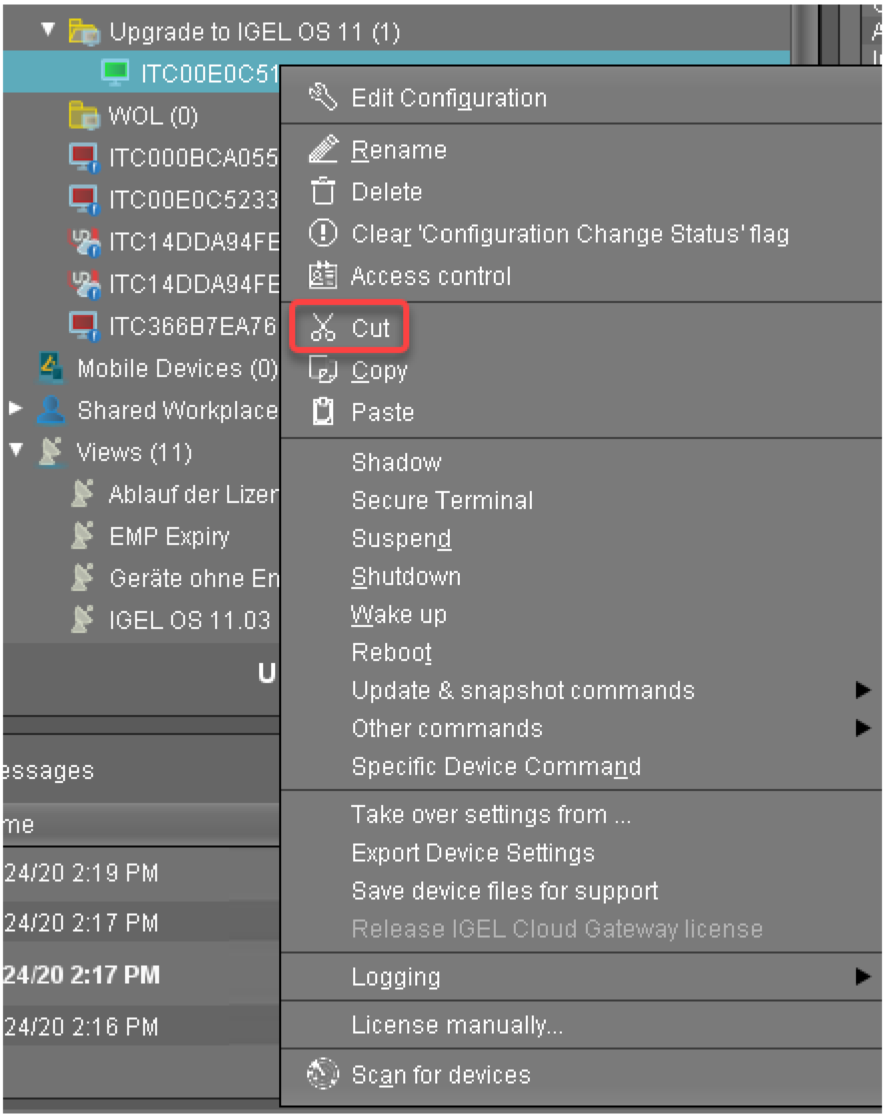
4. In the **Reboot devices** dialog, click **Reboot**.

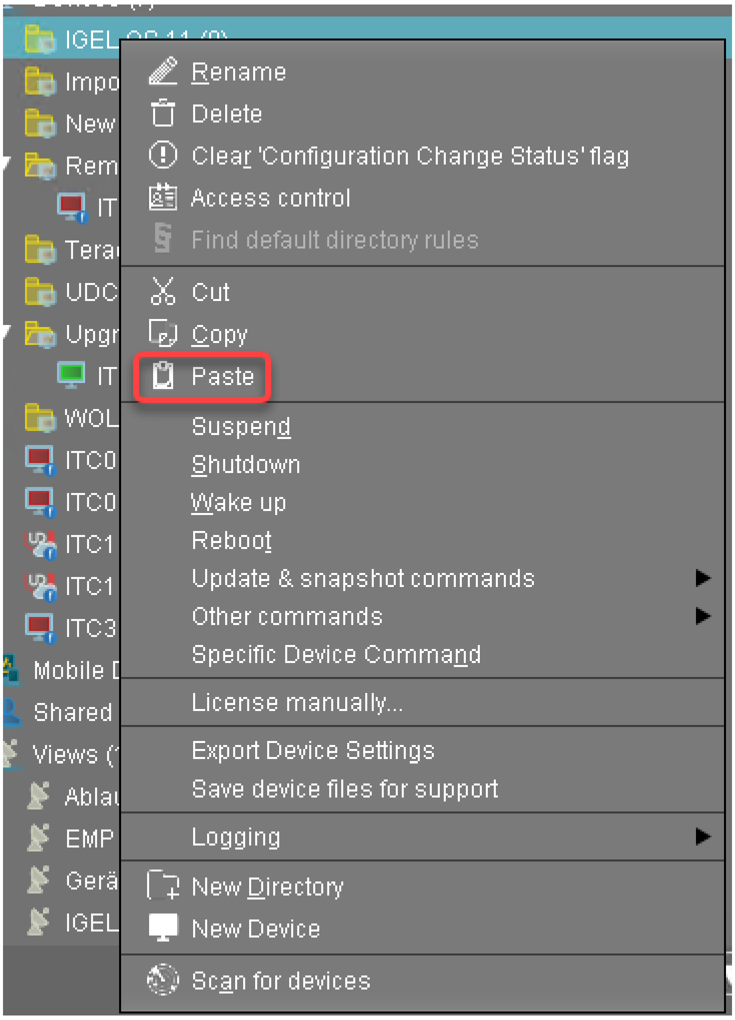


If no IGEL OS 11 licenses have been deployed on the devices yet, the licenses are deployed within a few minutes. The upgrade will be started when the licenses are deployed. The maximum time period a device will wait for a license is configured by the parameter **Timeout waiting for OS 11 license to start automatic upgrade**; for details, see Creating an Upgrade Profile (see page 34), 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.

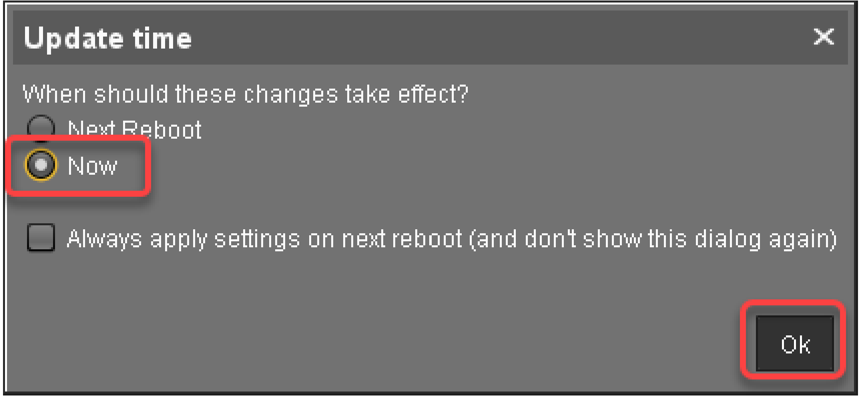
Unassigning the Upgrade Profile and the Universal Firmware Update

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
essages
me
24/20 2:19 PM
24/20 2:17 PM
24/20 2:17 PM
24/20 2:16 PM
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



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


Update time

When should these changes take effect?

○ Next Reboot
● Now

□ Always apply settings on next reboot (and don't show this dialog again)

Ok

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 50).

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

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 Converting UDC3 or UD Pocket Licenses for Upgrading to IGEL OS 11.

The following methods of mass deployment are described here:

- Zero-Touch Deployment Using Universal Firmware Update (see page 61): 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 98): 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 (see page 127): Upgrade devices that are already running IGEL OS 10.05.800 (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.

Devices That Can Be Upgraded to Igel OS 11

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: 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 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[3]. For more solutions compatible with IGEL OS, see Partner Solutions.

[3] https://www.igel.com/linux-3rd-party-hardware-database/

HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[4] 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.

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

ADS-Tec

Name	Endpoint Type	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

[4] https://www.igel.com/technology-partners/

Name	Endpoint Type	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 72)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 72)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
(AiO) 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	

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

Fujitsu

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100	
t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100	
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100	
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100	
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100	
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	
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)

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	
Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Support for WWAN Intel XMM 7560 R+ (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	
t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	
Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	

HP Docking Stations

Name	Supported from IGEL OS Version
HP USB-C Docking Station G5	11.08.230
HP USB-C G5 Essential Dock	11.08.290

Intel

Name	Endpoint Type	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

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
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	

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Excluding support for WWAN
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	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	

Lenovo Docking Stations

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

LG

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
(AiO) 24CK550 N** (see page 72)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
(AiO) 24CK550 W** (see page 72)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK560 N** (see page 72)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950 N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900 N	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
(AiO) 34CN650 N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600I	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650I	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601I	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360

OnLogic

Name	Endpoint Type	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	Endpoint Type	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

Rein Medical

Name	Endpoint Type	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	Endpoint Type	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 Alternative UD Pocket Hardware

DIGITTRADE

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

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 (see page 73).

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 74).

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 75)
2. Adjusting the Setup (see page 76)
3. Deploying a License (see page 77)
4. Configuring the Update Source (see page 78)

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 Updating UMS.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter Registering IGEL OS Devices on the UMS Server in the UMS Manual.

When the UMS is ready, continue with Adjusting the Setup (see page 76).

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 61), Zero-Touch Deployment Using Buddy Update (see page 98) and Mass Deployment Using a Scheduled Job (see page 200)). 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 77).

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. For further information, see Workspace Edition
- If IGEL Cloud Gateway (ICG), or Shared Workplace (SWP) will be used: One Enterprise Management Pack license. For further information, see Enterprise Management Pack.
- 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.

▶ 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 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 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 78).

Configuring the Update Source

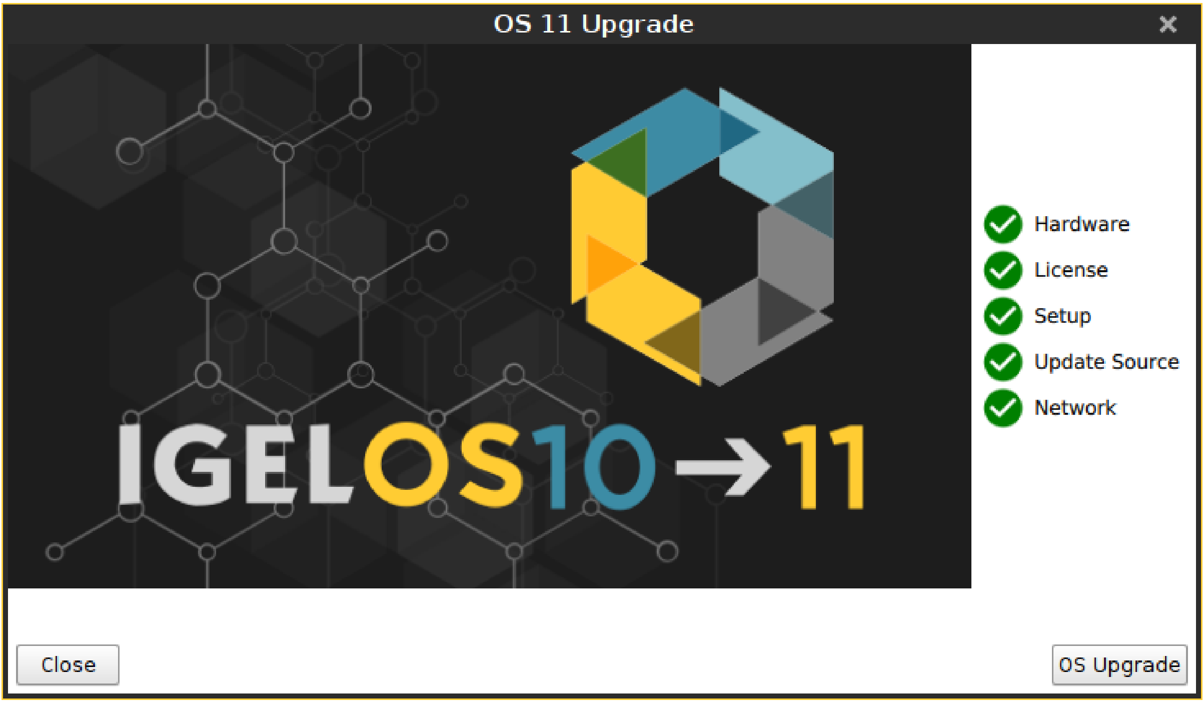
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade (see page 79).

Testing the Upgrade

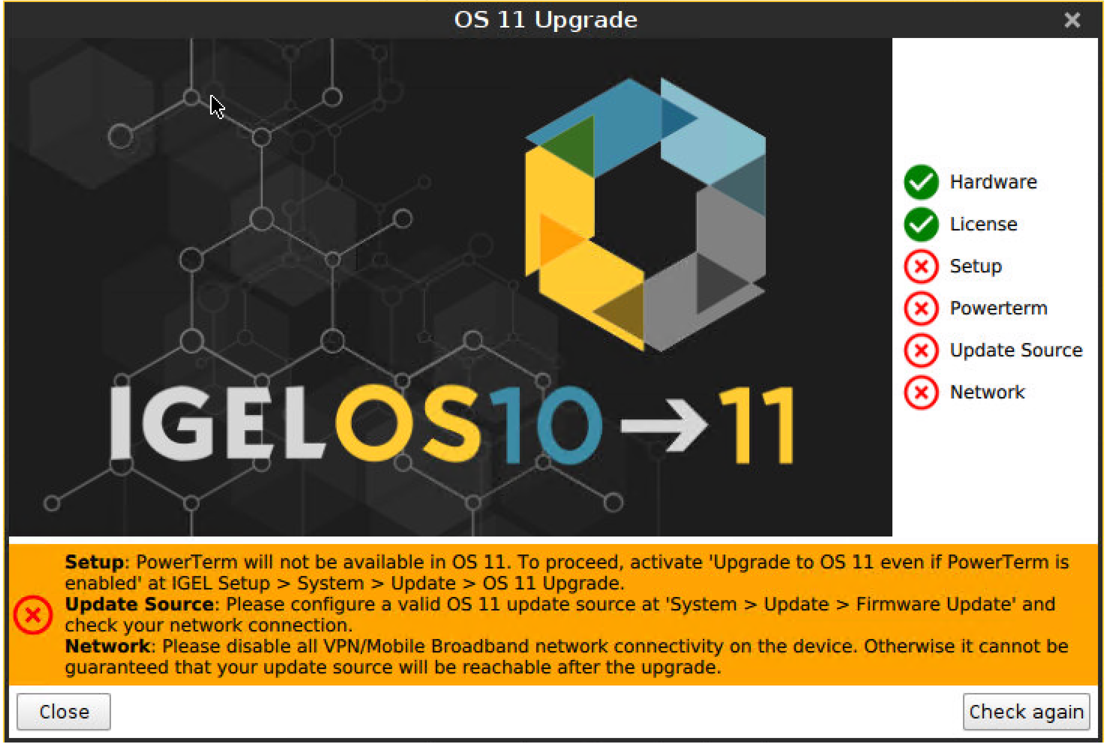
1. Click ⚙ System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

> ⓘ 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**

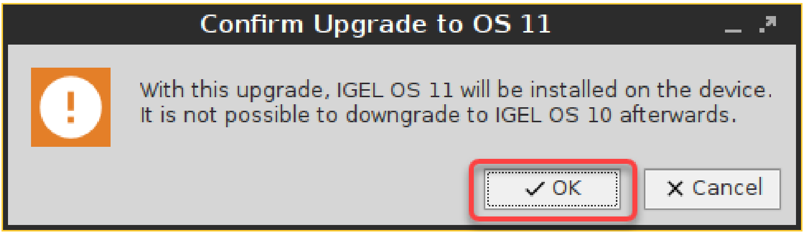
Upgrade, and you can start the upgrade.



Setup: PowerTerm will not be available in OS 11. To proceed, activate 'Upgrade to OS 11 even if PowerTerm is enabled' at IGEL Setup > System > Update > OS 11 Upgrade.
Update Source: Please configure a valid OS 11 update source at 'System > Update > Firmware Update' and check your network connection.
Network: Please disable all VPN/Mobile Broadband network connectivity on the device. Otherwise it cannot be guaranteed that your update source will be reachable after the upgrade.

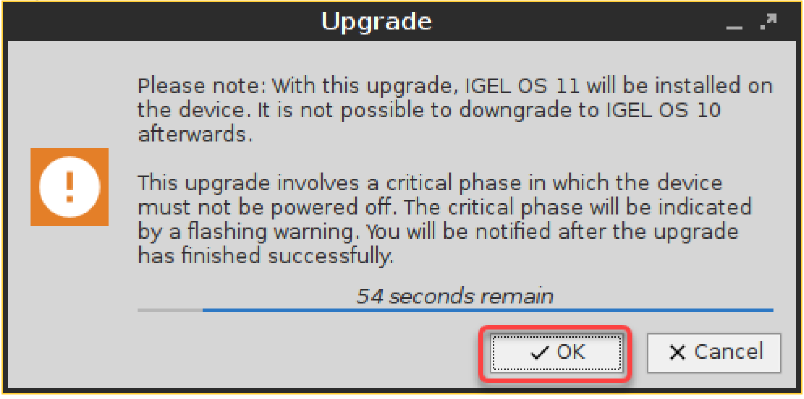
When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



With this upgrade, IGEL OS 11 will be installed on the device.
It is not possible to downgrade to IGEL OS 10 afterwards.

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



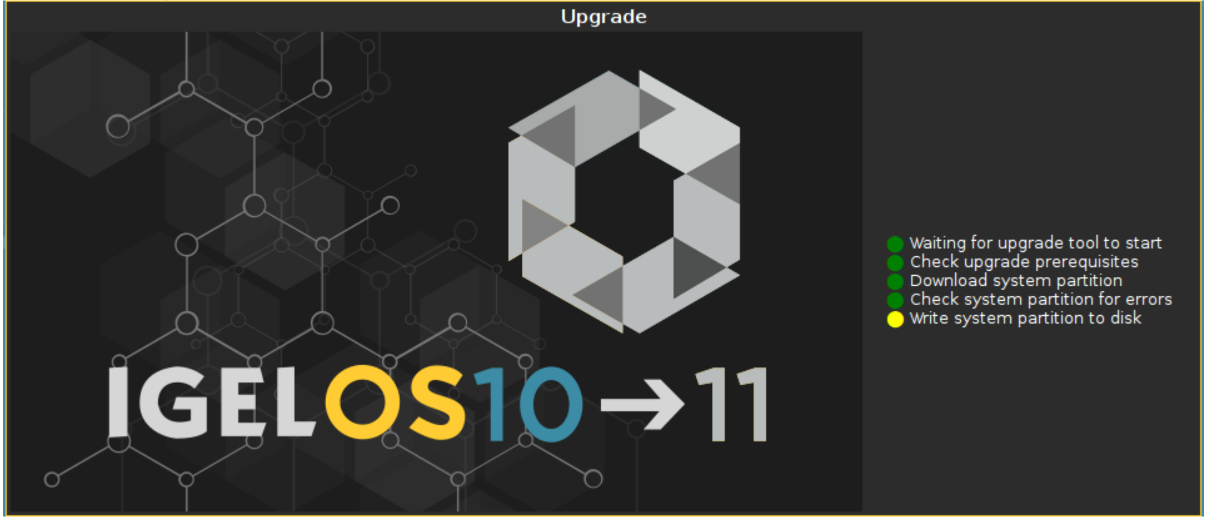
Please note: With this upgrade, IGEL OS 11 will be installed on the device. It is not possible to downgrade to IGEL OS 10 afterwards.

This upgrade involves a critical phase in which the device must not be powered off. The critical phase will be indicated by a flashing warning. You will be notified after the upgrade has finished successfully.

54 seconds remain

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

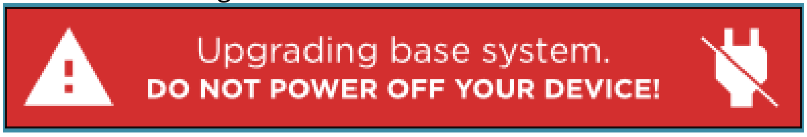
show the progress.



Upgrade

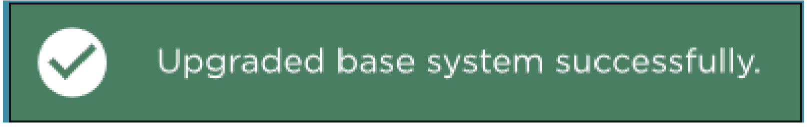
- 🟢 Waiting for upgrade tool to start
- 🟢 Check upgrade prerequisites
- 🟢 Download system partition
- 🟢 Check system partition for errors
- 🟡 Write system partition to disk

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



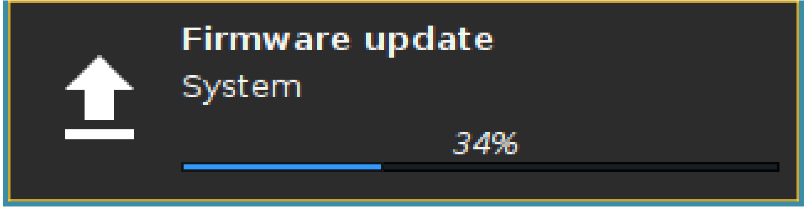
Upgrading base system.
DO NOT POWER OFF YOUR DEVICE!

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



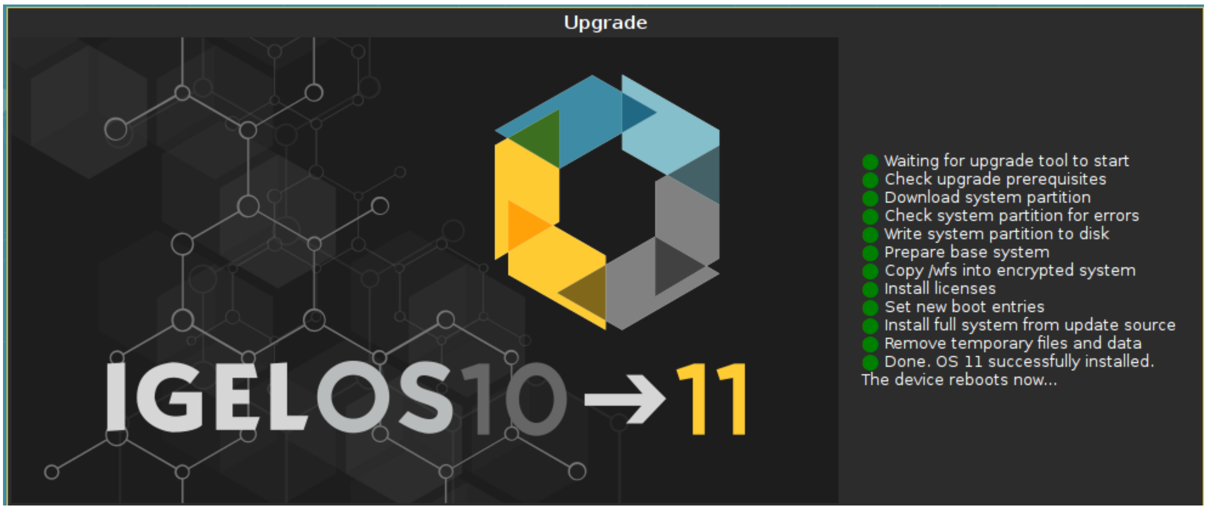
Upgraded base system successfully.

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



Firmware update
System
34%

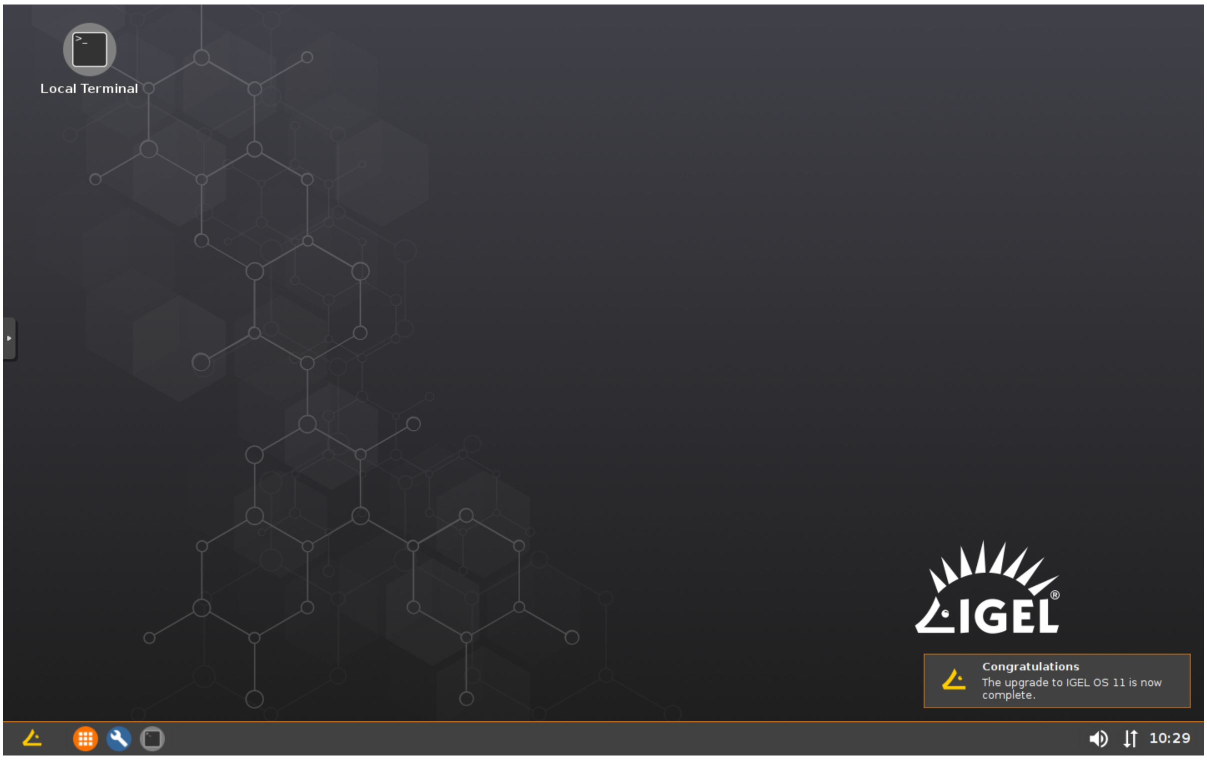
When the installation is completed, the **Upgrade** window looks like this:



Upgrade

● Waiting for upgrade tool to start
● Check upgrade prerequisites
● Download system partition
● Check system partition for errors
● Write system partition to disk
● Prepare base system
● Copy /wfs into encrypted system
● Install licenses
● Set new boot entries
● Install full system from update source
● Remove temporary files and data
● Done. OS 11 successfully installed.
The device reboots now...

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



Congratulations
The upgrade to IGEL OS 11 is now complete.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 83).

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 the Universal Firmware Updates (see page 84).

Creating the Universal Firmware Updates

For detailed information, see the chapter Universal Firmware Update in the UMS Manual.

> ⓘ If you use the 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.

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.

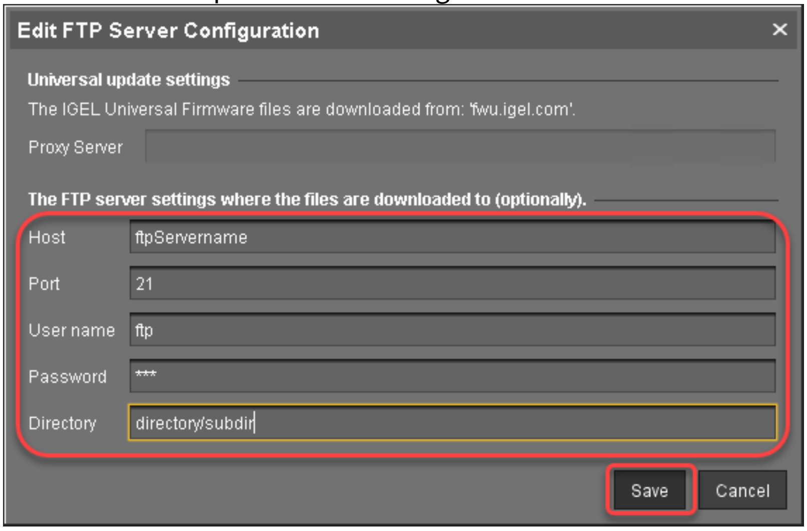
   > The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see Executing the Upgrade (see page 96).

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



Edit FTP Server Configuration

Universal update settings

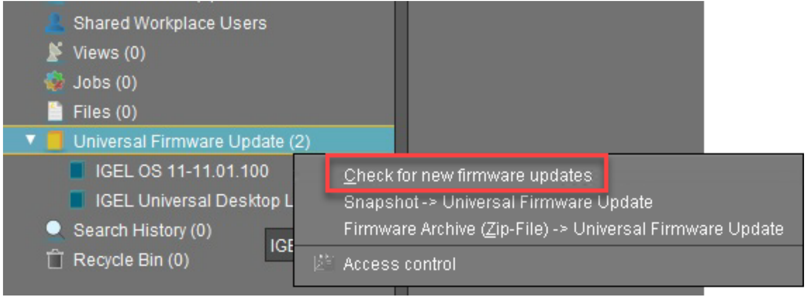
The IGEL Universal Firmware files are downloaded from: 'fwu.igel.com'.

Proxy Server

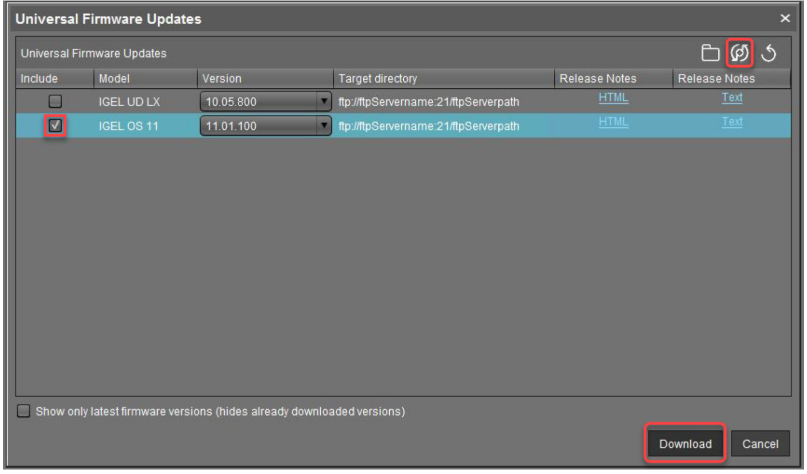
The FTP server settings where the files are downloaded to (optionally).

Host	ftpServername
Port	21
User name	ftp
Password	***
Directory	directory/subdir

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


Shared Workplace Users
Views (0)
Jobs (0)
Files (0)
Universal Firmware Update (2)
IGEL OS 11-11.01.100
IGEL Universal Desktop L
Search History (0)
Recycle Bin (0)
IGE
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

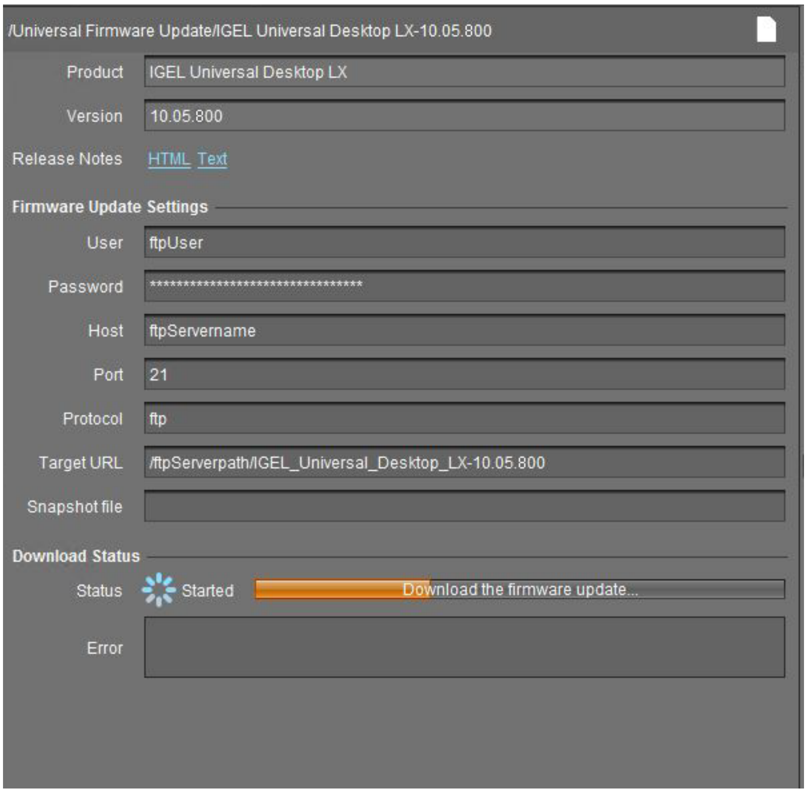
4. Select the entry for the IGEL OS 10.05.800 (or higher) firmware, click to select the FTP server selected in step 2 and then select **Download**.



Include	Model	Version	Target directory	Release Notes	Release Notes
□	IGEL UD LX	10.05.800	ftp://ftpServername:21/ftpServerpath	HTML	Text
☑	IGEL OS 11	11.01.100	ftp://ftpServername:21/ftpServerpath	HTML	Text

□ Show only latest firmware versions (hides already downloaded versions)

5. The firmware is transferred to the FTP server.



/Universal Firmware Update/IGEL Universal Desktop LX-10.05.800

Product: IGEL Universal Desktop LX

Version: 10.05.800

Release Notes: HTML Text

Firmware Update Settings

User: ftpUser

Password: ********************************

Host: ftpServername

Port: 21

Protocol: ftp

Target URL: /ftpServerpath/IGEL_Universal_Desktop_LX-10.05.800

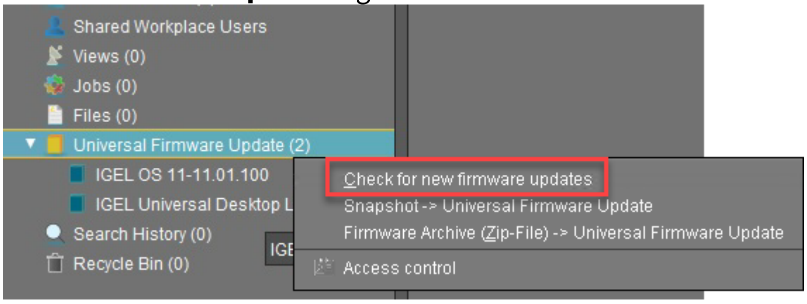
Snapshot file:

Download Status

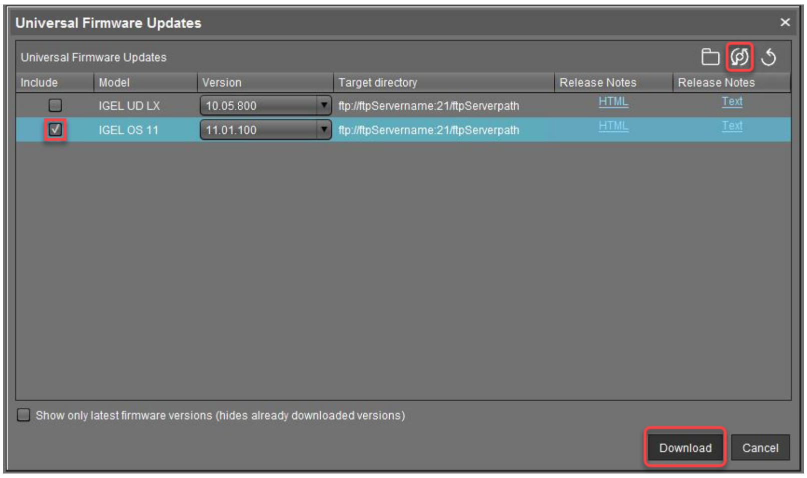
Status: Started — Download the firmware update...

Error:

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


Shared Workplace Users
Views (0)
Jobs (0)
Files (0)
Universal Firmware Update (2)
IGEL OS 11-11.01.100
IGEL Universal Desktop L
Search History (0)
Recycle Bin (0)
IGE
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

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



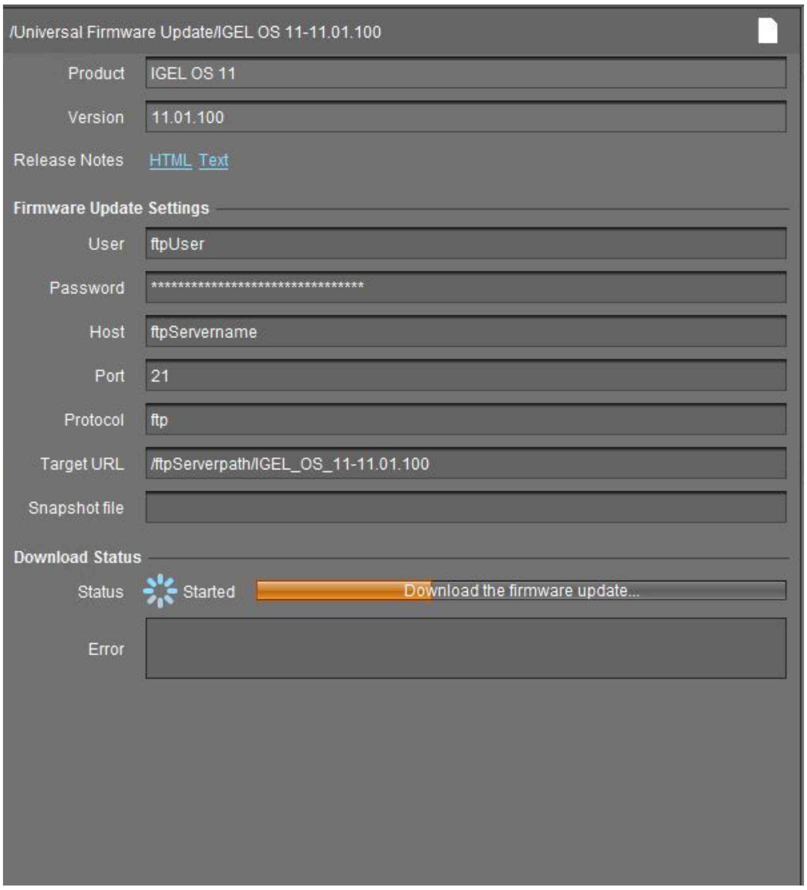
Universal Firmware Updates

Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
☐	IGEL UD LX	10.05.800	ftp://ftpServername:21/ftpServerpath	HTML	Text
☑	IGEL OS 11	11.01.100	ftp://ftpServername:21/ftpServerpath	HTML	Text

☐ Show only latest firmware versions (hides already downloaded versions)

8. The firmware is transferred to the FTP server.



/Universal Firmware Update/IGEL OS 11-11.01.100

Product: IGEL OS 11

Version: 11.01.100

Release Notes: HTML Text

Firmware Update Settings

User: ftpUser

Password: ********************************

Host: ftpServername

Port: 21

Protocol: ftp

Target URL: /ftpServerpath/IGEL_OS_11-11.01.100

Snapshot file:

Download Status

Status: Started Download the firmware update...

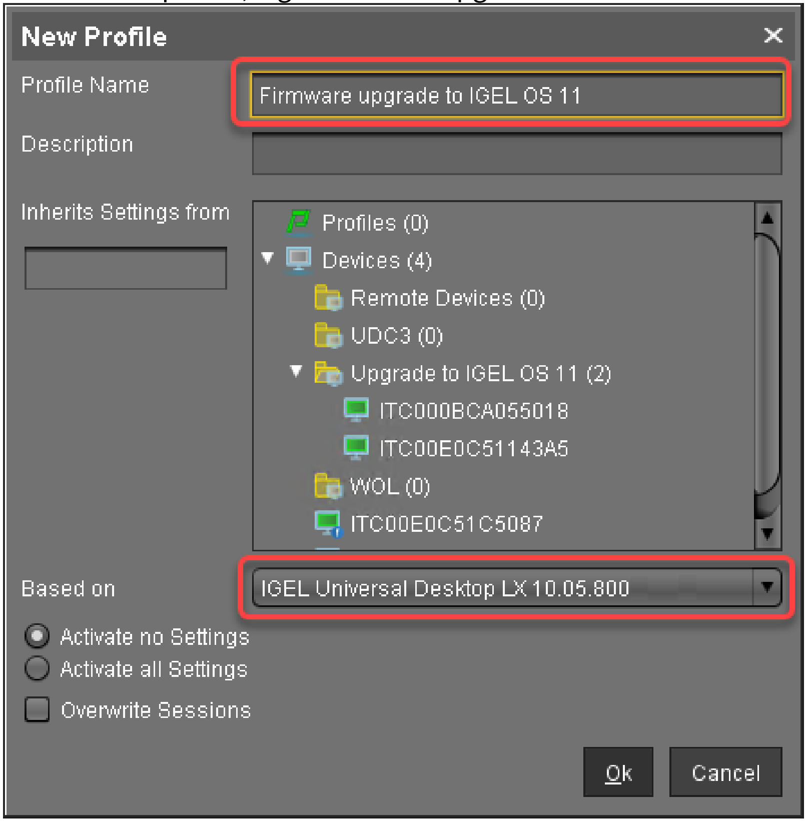
Error:

The devices can download the firmware from the FTP server,

When the Universal Firmware Update is ready, continue with Creating a Profile (see page 88).

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".



New Profile

Profile Name: Firmware upgrade to IGEL OS 11

Description:

Inherits Settings from

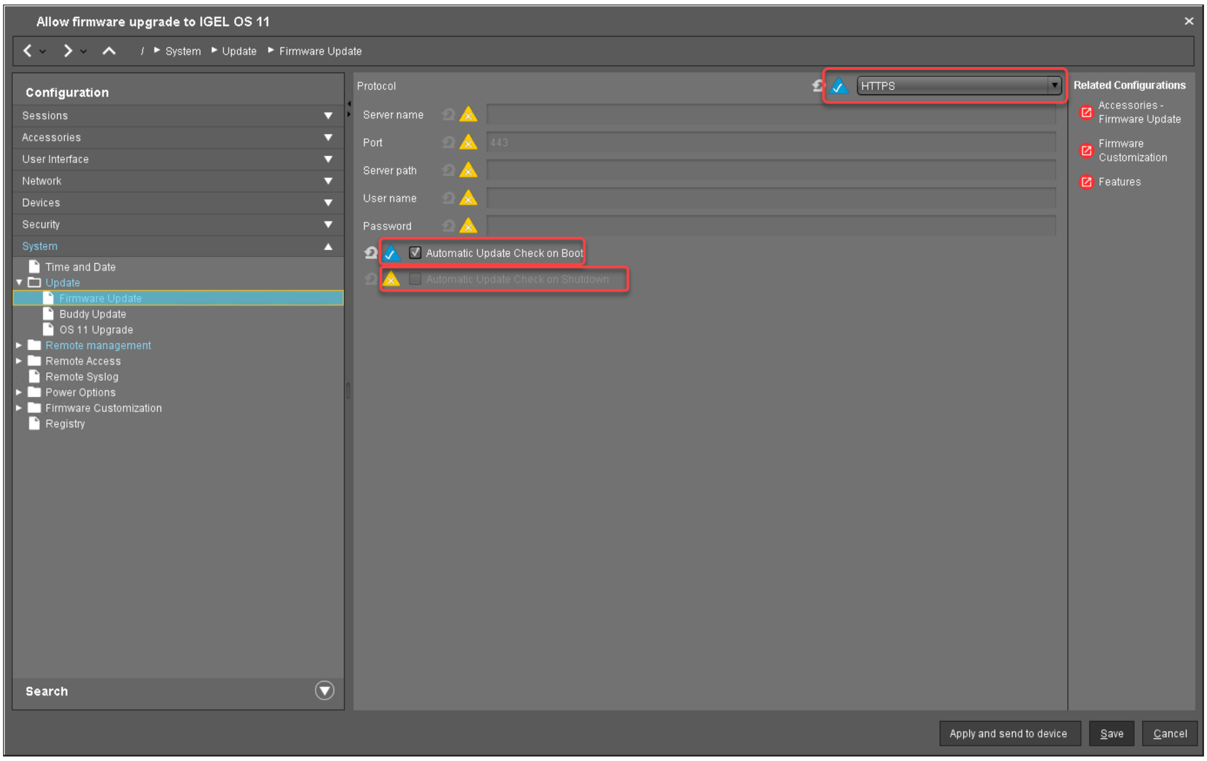
Based on: IGEL Universal Desktop LX 10.05.800

● Activate no Settings

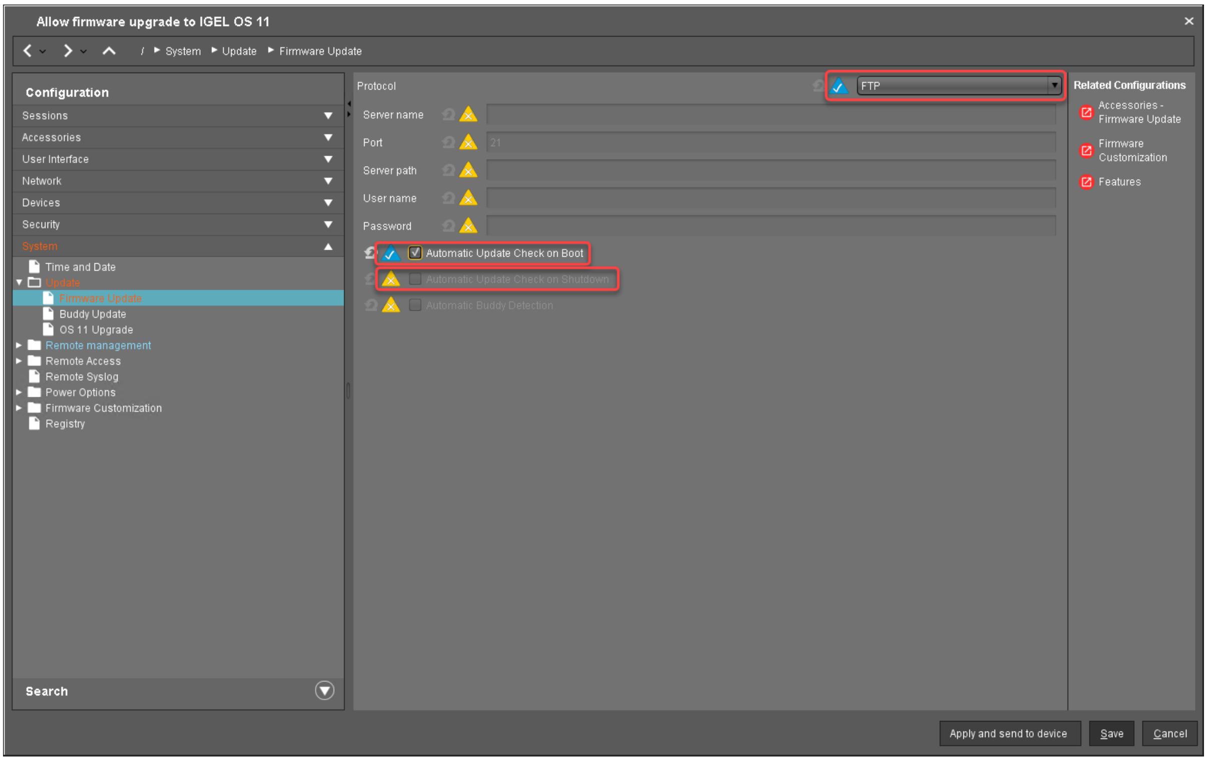
○ Activate all Settings

□ Overwrite Sessions

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.



Allow firmware upgrade to IGEL OS 11

/ ▸ System ▸ Update ▸ Firmware Update

Protocol: FTP

Server name

Port: 21

Server path

User name

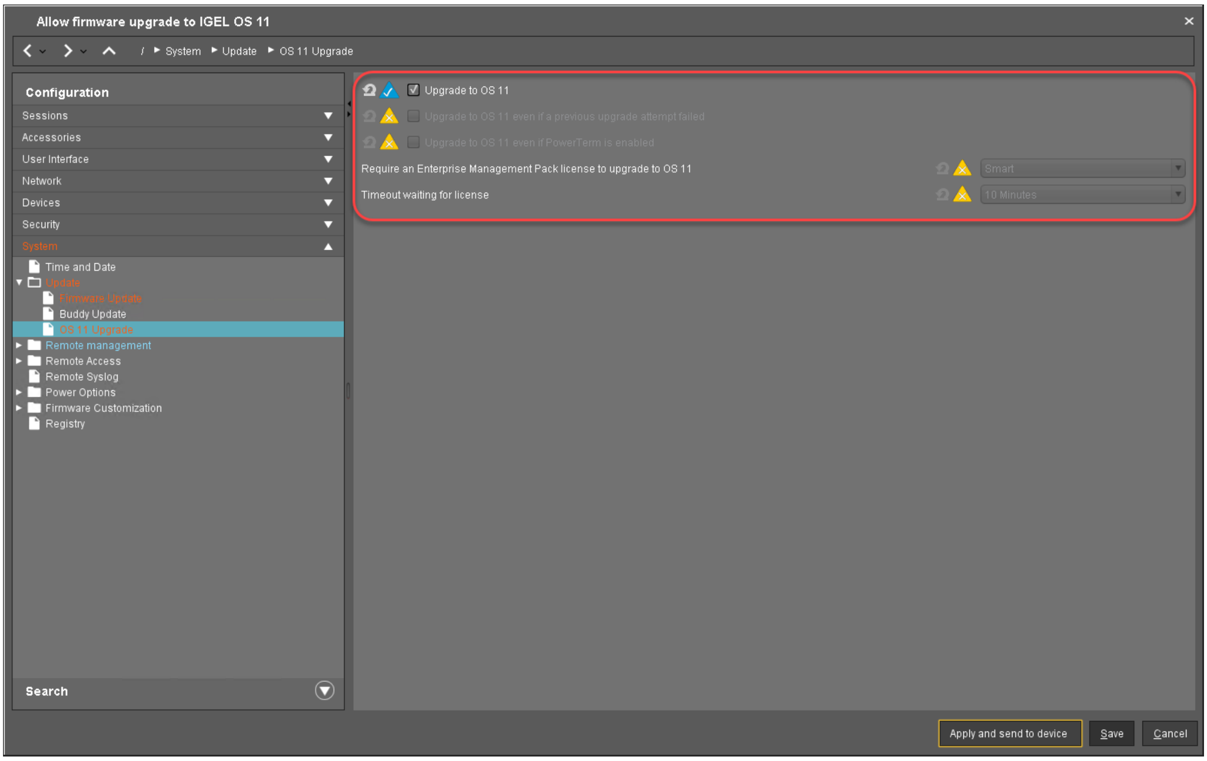
Password

☑ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

□ Automatic Buddy Detection

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 76)):
   - 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**.



☑ Upgrade to OS 11

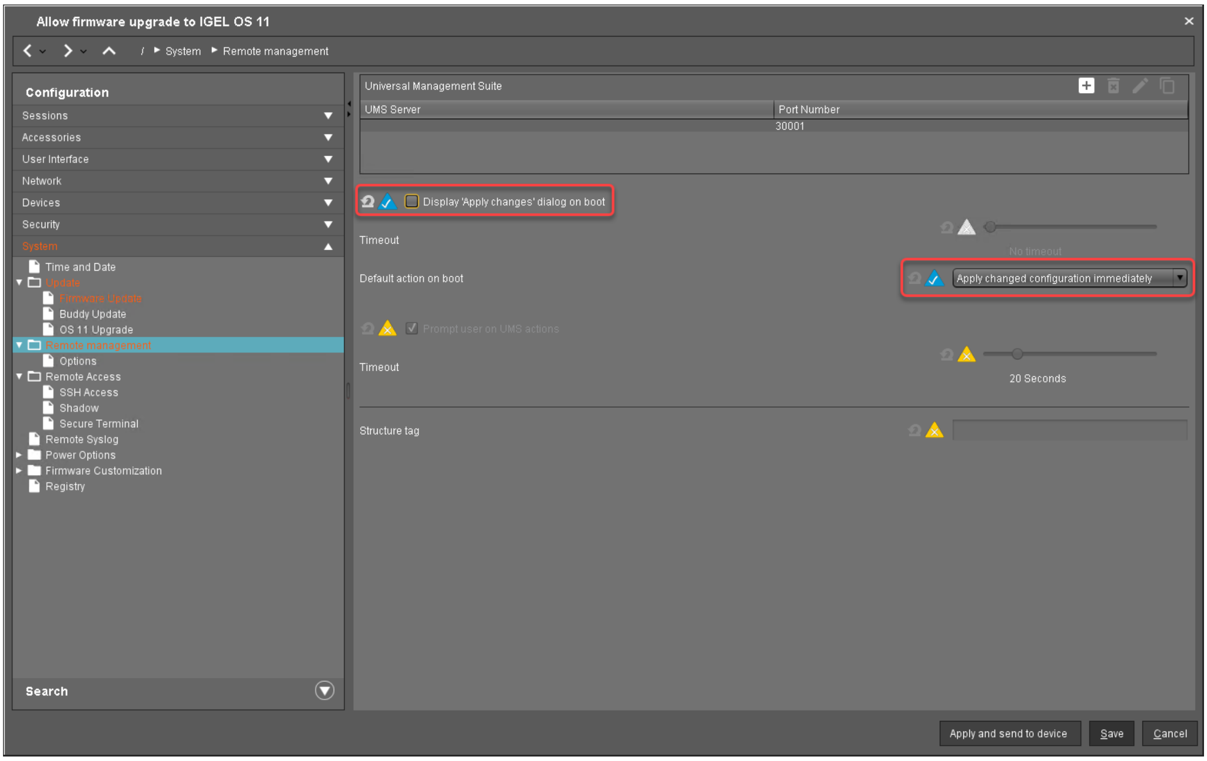
□ Upgrade to OS 11 even if a previous upgrade attempt failed

□ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for license: 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**.



Universal Management Suite

UMS Server	Port Number
	30001

□ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag

5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 93).

Deploying the Licenses

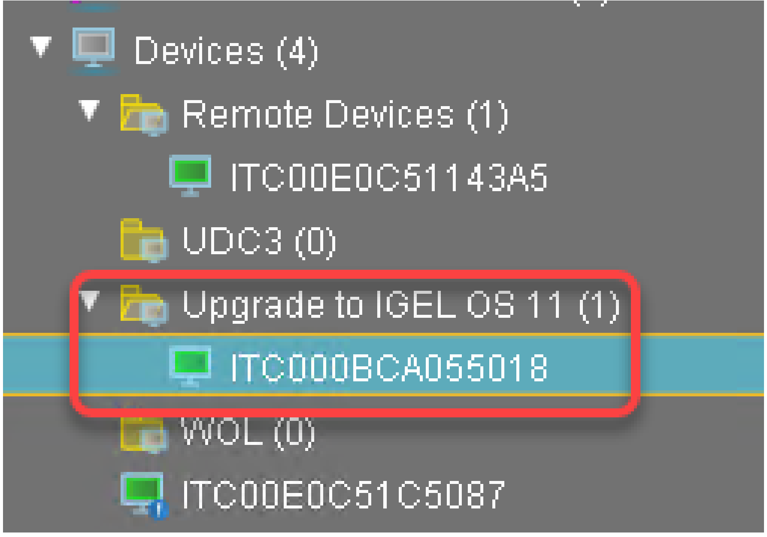
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

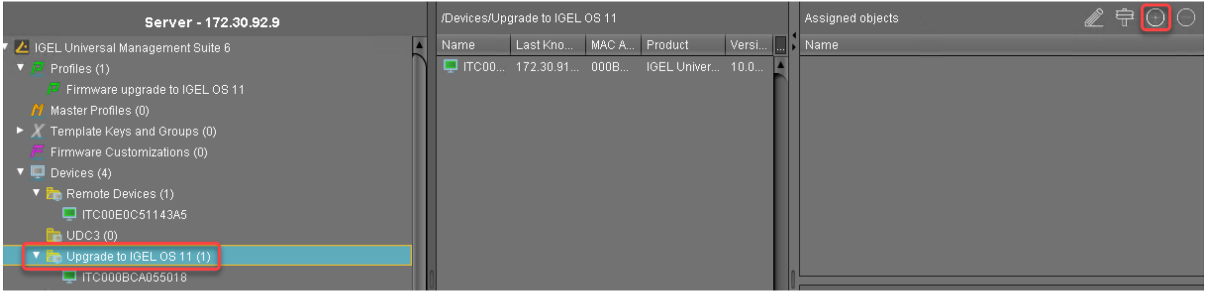
When the license deployment is set up, continue with Putting It All Together (see page 94).

Putting It All Together

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

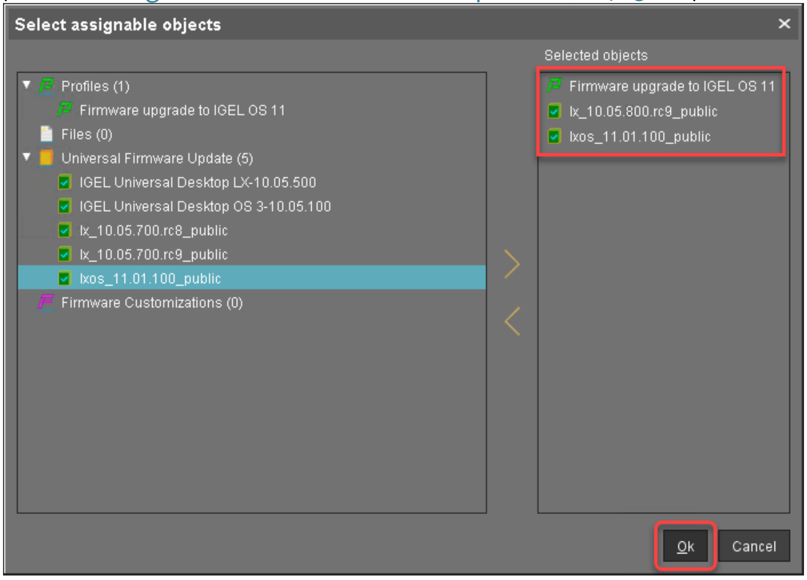


2. Select the directory and in the **Assigned objects** area, click ⊕.

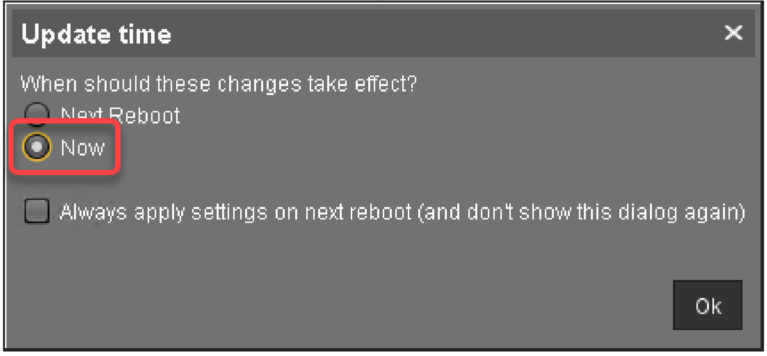

Server - 172.30.92.9
IGEL Universal Management Suite 6
Profiles (1)
Firmware upgrade to IGEL OS 11
Master Profiles (0)
Template Keys and Groups (0)
Firmware Customizations (0)
Devices (4)
Remote Devices (1)
ITC00E0C51143A5
UDC3 (0)
Upgrade to IGEL OS 11 (1)
ITC000BCA055018
/Devices/Upgrade to IGEL OS 11
Assigned objects
Name

Name	Last Kno...	MAC A...	Product	Versi...
ITC00...	172.30.91...	000B...	IGEL Univer...	10.0...

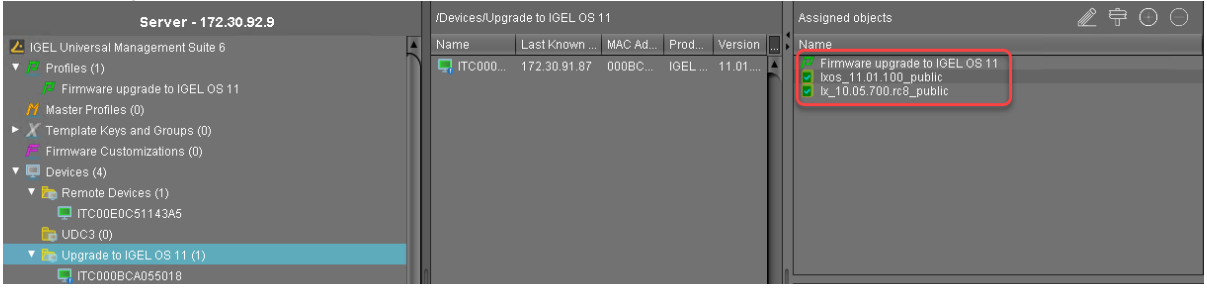
3. Assign the profile (see Creating a Profile (see page 88)) and the two Universal Firmware Updates (see Creating the Universal Firmware Updates (see page 84)) to the directory and click **Ok**.


Select assignable objects
Profiles (1)
Firmware upgrade to IGEL OS 11
Files (0)
Universal Firmware Update (5)
IGEL Universal Desktop LX-10.05.500
IGEL Universal Desktop OS 3-10.05.100
lx_10.05.700.rc8_public
lx_10.05.700.rc9_public
lxos_11.01.100_public
Firmware Customizations (0)
Selected objects
Firmware upgrade to IGEL OS 11
lx_10.05.800.rc9_public
lxos_11.01.100_public
Ok
Cancel

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


Update time
When should these changes take effect?
○ Next Reboot
● Now
□ Always apply settings on next reboot (and don't show this dialog again)
Ok

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



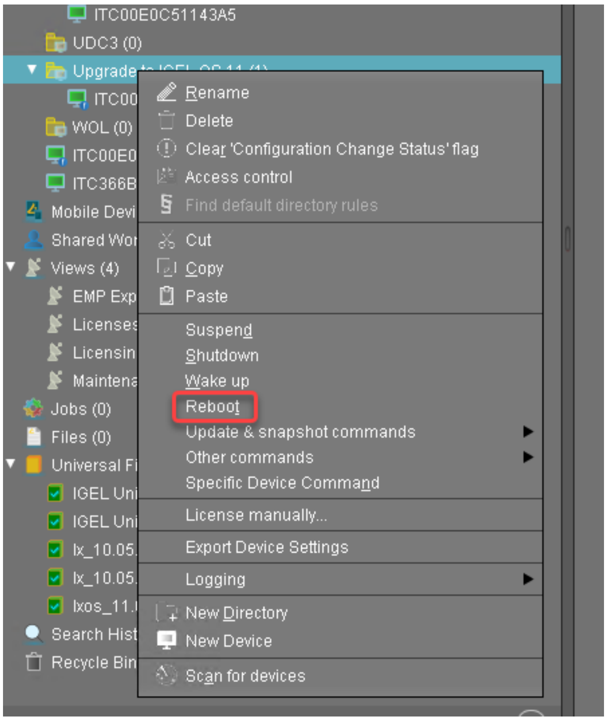
5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see Configuring the Distribution Conditions, section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with Executing the Upgrade (see page 96).

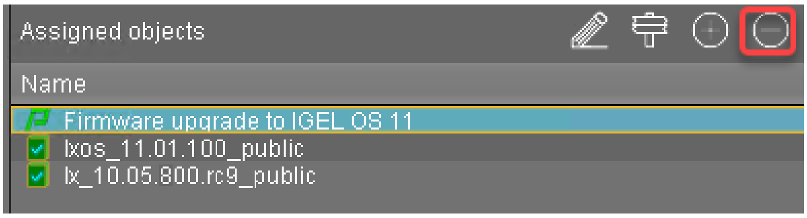
Executing the Upgrade

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

   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 76).
   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.
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.



Assigned objects

Name

Firmware upgrade to IGEL OS 11

☑ lxos_11.01.100_public

☑ lx_10.05.800.rc9_public

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

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: 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 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[5]. For more solutions compatible with IGEL OS, see Partner Solutions.

[5] https://www.igel.com/linux-3rd-party-hardware-database/

ⓘ HP, Lenovo, and LG device models are available from the factory with pre-installed IGEL OS 11. Please contact IGEL Ready[6] 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.

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

ADS-Tec

Name	Endpoint Type	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

[6] https://www.igel.com/technology-partners/

Name	Endpoint Type	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 109)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 109)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

Advantech-DLoG

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
(AiO) 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	

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

Fujitsu

Name	Endpoint Type	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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100	
t430	Thin Client	2 GB	16 GB	Intel®Celeron® N4020	11.01.110	
t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100	
t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100	
t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100	
t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100	
t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	
t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	
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)

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version	Note
Elite t655	Thin Client	4 GB / 8 GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	
Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Support for WWAN Intel XMM 7560 R+ (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	
t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	
Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	

HP Docking Stations

Name	Supported from IGEL OS Version
HP USB-C Docking Station G5	11.08.230
HP USB-C G5 Essential Dock	11.08.290

Intel

Name	Endpoint Type	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

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
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	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
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	

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Wi-Fi Chip	Supported from IGEL OS Version	Note
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Excluding support for WWAN
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	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	

Lenovo Docking Stations

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

LG

Name	Endpoint Type	Minimum Memory (RAM) Size	Storage Size	Processor	Supported from IGEL OS Version
(AiO) 24CK550 N** (see page 109)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK550 W** (see page 109)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 24CK560 N** (see page 109)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500W	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
(AiO) 38CK950 N	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
(AiO) 38CK900 N	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
(AiO) 34CN650 N	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650N	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
CQ600I	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650I	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601I	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360

OnLogic

Name	Endpoint Type	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	Endpoint Type	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

Rein Medical

Name	Endpoint Type	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	Endpoint Type	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 Alternative UD Pocket Hardware

DIGITTRADE

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

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 (see page 110).

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 111).

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 112)
2. Adjusting the Setup (see page 113)
3. Deploying a License (see page 114)
4. Configuring the Update Source (see page 115)

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 Updating UMS.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter Registering IGEL OS Devices on the UMS Server in the UMS Manual.

When the UMS is ready, continue with Adjusting the Setup (see page 113).

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 61), Zero-Touch Deployment Using Buddy Update (see page 98) and Mass Deployment Using a Scheduled Job (see page 200)). 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 114).

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. For further information, see Workspace Edition
- If IGEL Cloud Gateway (ICG), or Shared Workplace (SWP) will be used: One Enterprise Management Pack license. For further information, see Enterprise Management Pack.
- 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.

▶ 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 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 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 115).

Configuring the Update Source

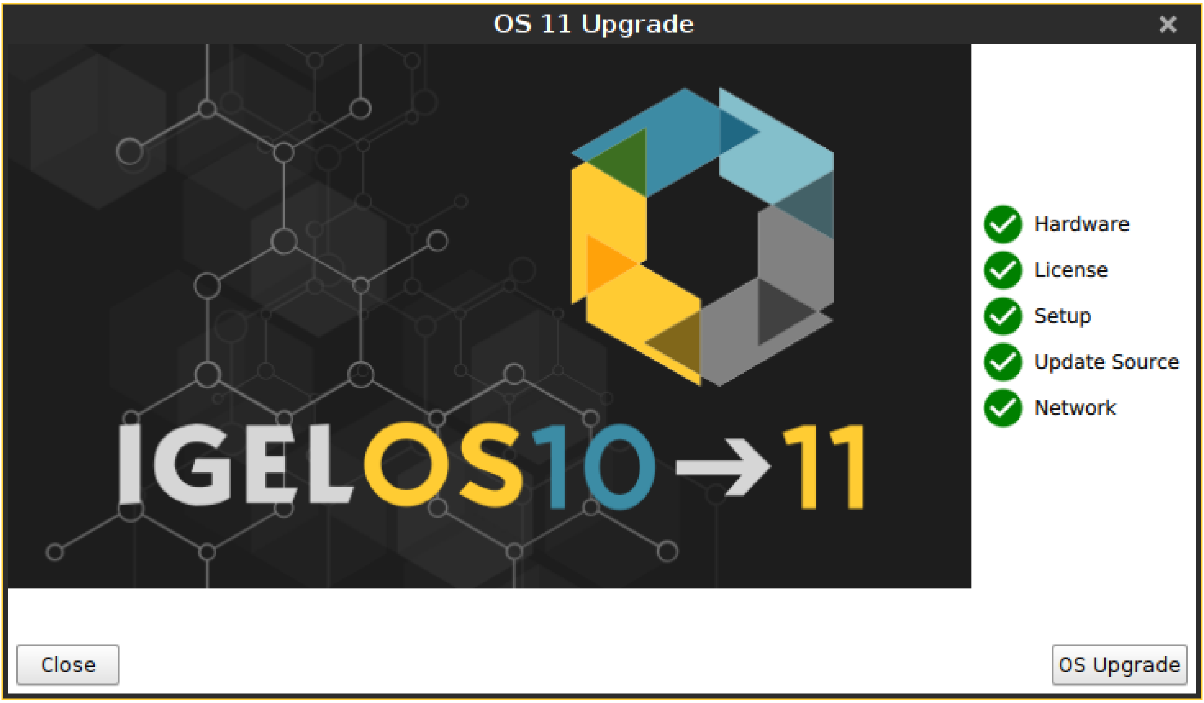
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade (see page 116).

Testing the Upgrade

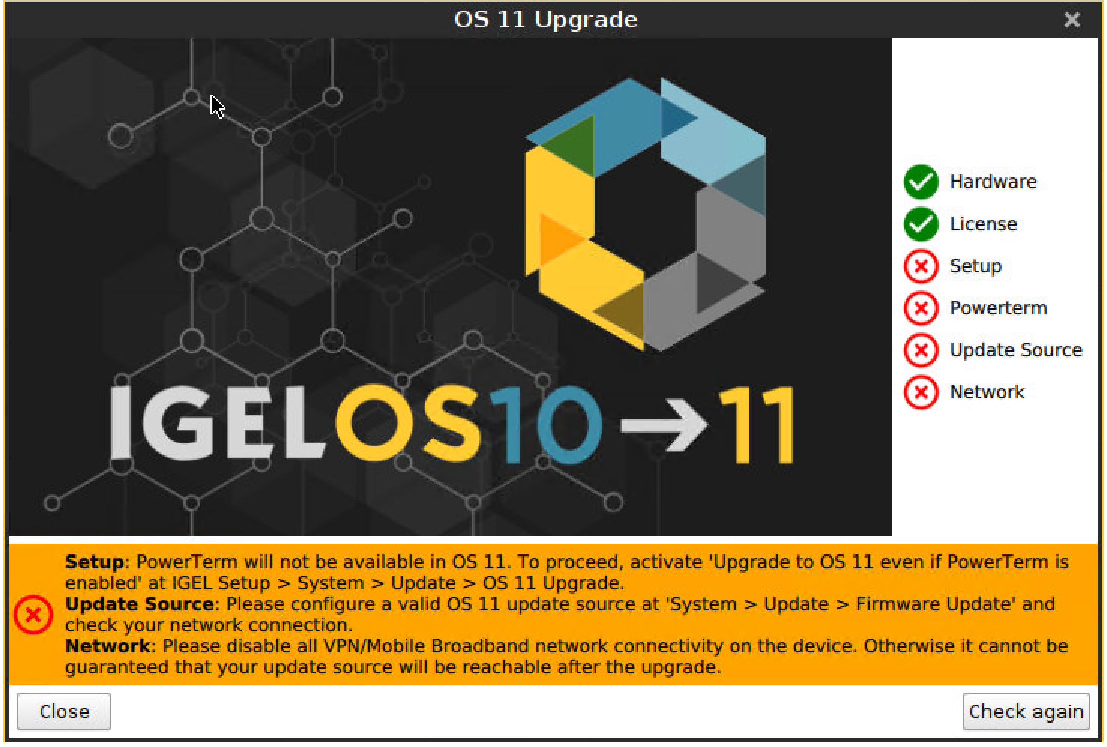
1. Click ⚙ System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

> ⓘ 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.



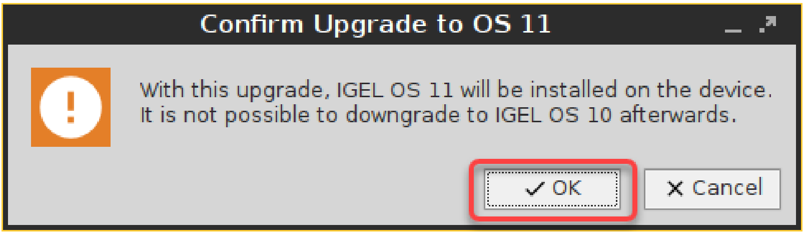
OS 11 Upgrade

- ✓ Hardware
- ✓ License
- ✗ Setup
- ✗ Powerterm
- ✗ Update Source
- ✗ Network

Setup: PowerTerm will not be available in OS 11. To proceed, activate 'Upgrade to OS 11 even if PowerTerm is enabled' at IGEL Setup > System > Update > OS 11 Upgrade.
Update Source: Please configure a valid OS 11 update source at 'System > Update > Firmware Update' and check your network connection.
Network: Please disable all VPN/Mobile Broadband network connectivity on the device. Otherwise it cannot be guaranteed that your update source will be reachable after the upgrade.

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

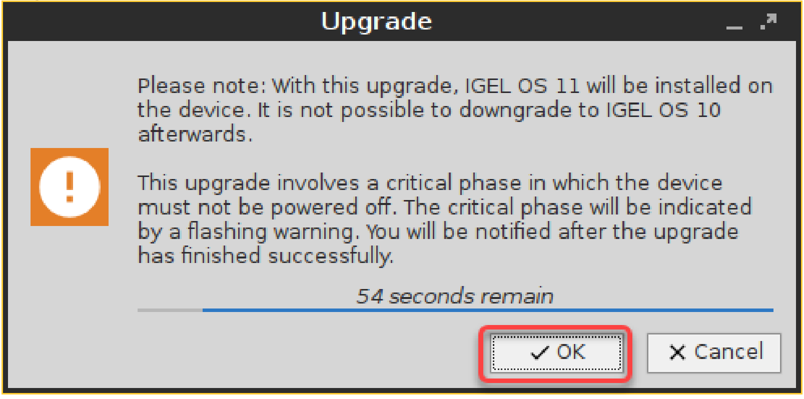
3. Click **OK** to continue.



Confirm Upgrade to OS 11

With this upgrade, IGEL OS 11 will be installed on the device.
It is not possible to downgrade to IGEL OS 10 afterwards.

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



Upgrade

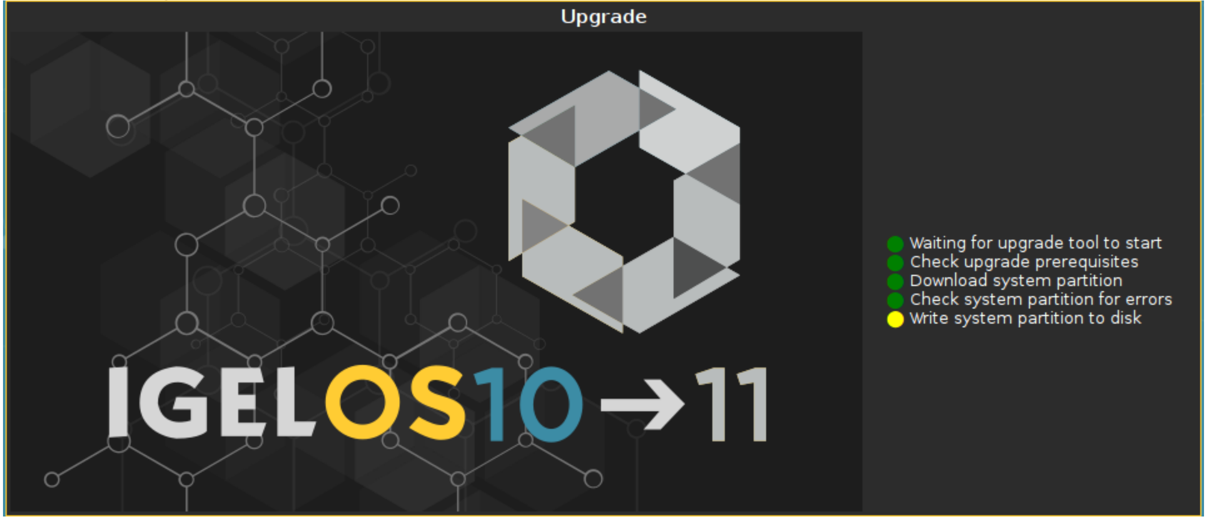
Please note: With this upgrade, IGEL OS 11 will be installed on the device. It is not possible to downgrade to IGEL OS 10 afterwards.

This upgrade involves a critical phase in which the device must not be powered off. The critical phase will be indicated by a flashing warning. You will be notified after the upgrade has finished successfully.

54 seconds remain

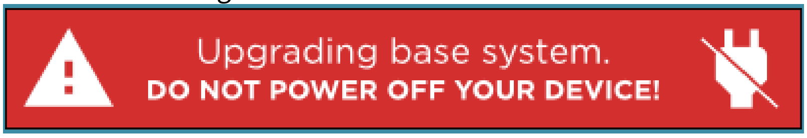
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window

show the progress.



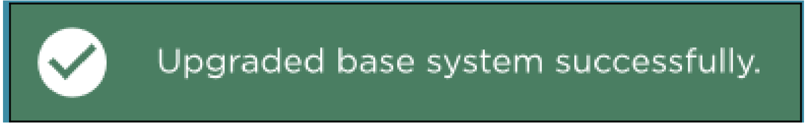
● Waiting for upgrade tool to start
● Check upgrade prerequisites
● Download system partition
● Check system partition for errors
● Write system partition to disk

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



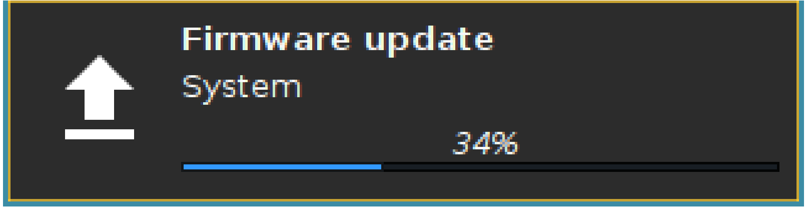
Upgrading base system.
DO NOT POWER OFF YOUR DEVICE!

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



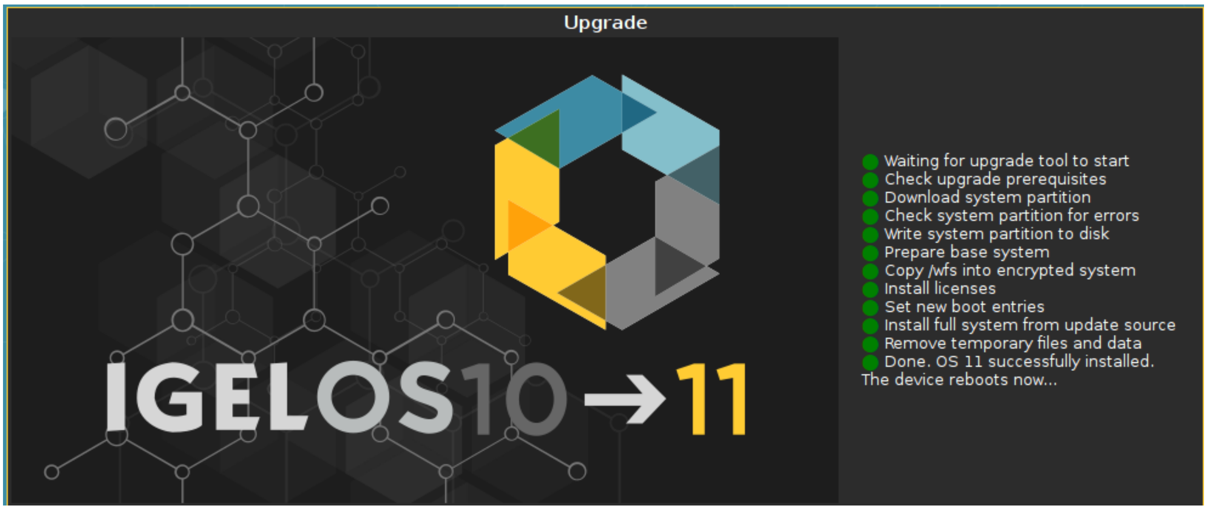
Upgraded base system successfully.

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



Firmware update
System
34%

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

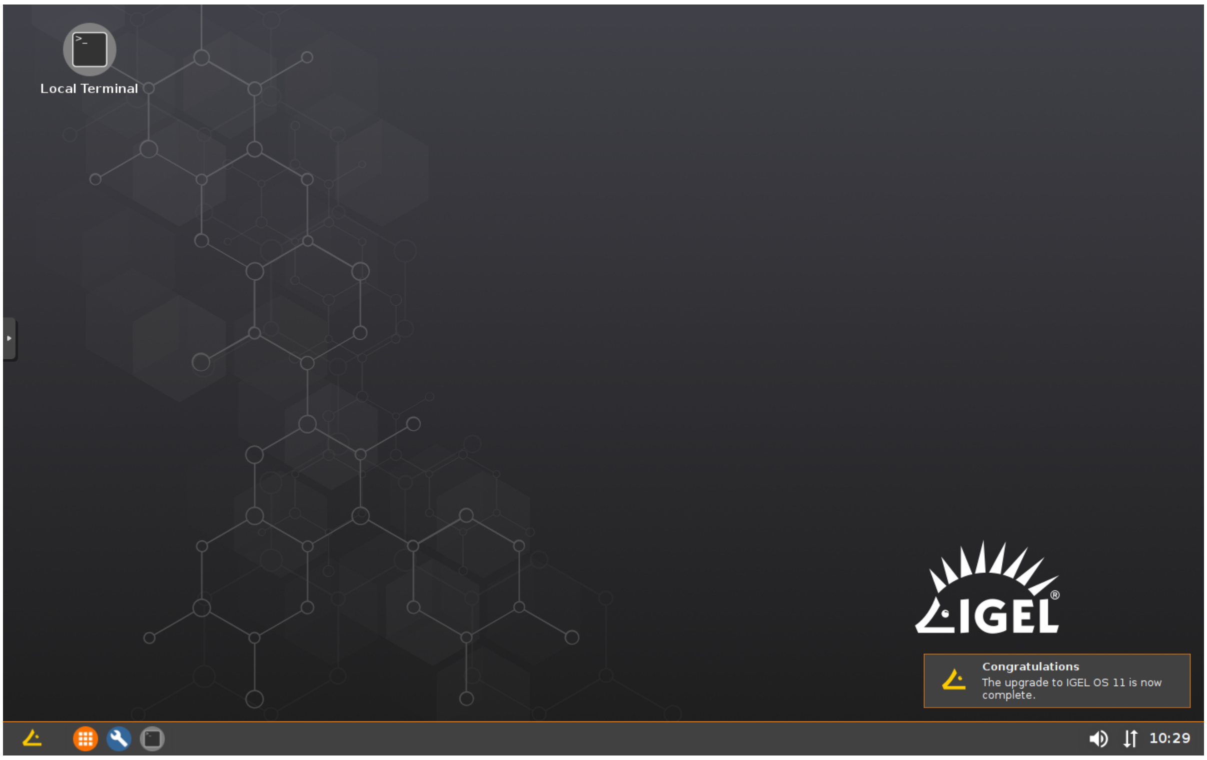


Upgrade

- ● Waiting for upgrade tool to start
- ● Check upgrade prerequisites
- ● Download system partition
- ● Check system partition for errors
- ● Write system partition to disk
- ● Prepare base system
- ● Copy /wfs into encrypted system
- ● Install licenses
- ● Set new boot entries
- ● Install full system from update source
- ● Remove temporary files and data
- ● Done. OS 11 successfully installed.

The device reboots now...

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



Congratulations
The upgrade to IGEL OS 11 is now complete.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 120).

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 Configuring Two Update Buddies (see page 121).

Configuring Two Update Buddies

For setting up buddy updates, see the how-to Buddy Update (see page 217).

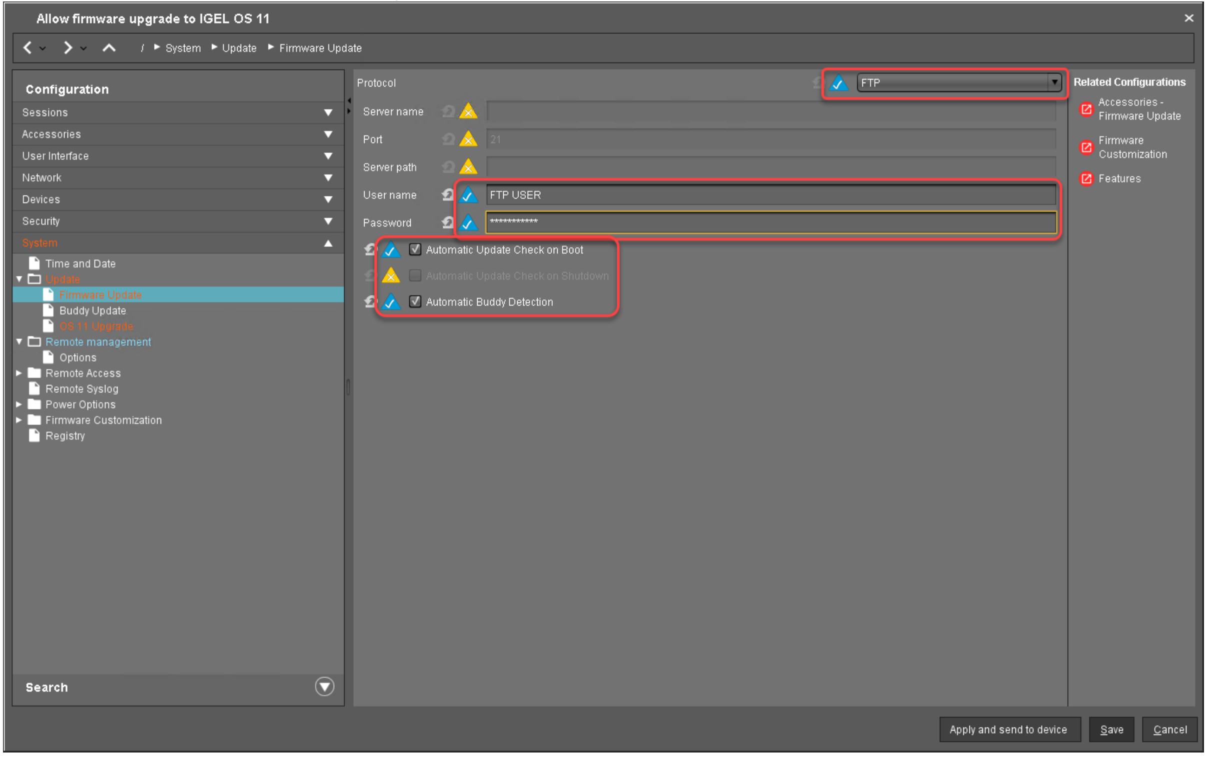
> ❗ Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

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 Creating a Profile (see page 122).

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**.



Allow firmware upgrade to IGEL OS 11

Protocol: FTP

Server name:

Port: 21

Server path:

User name: FTP USER

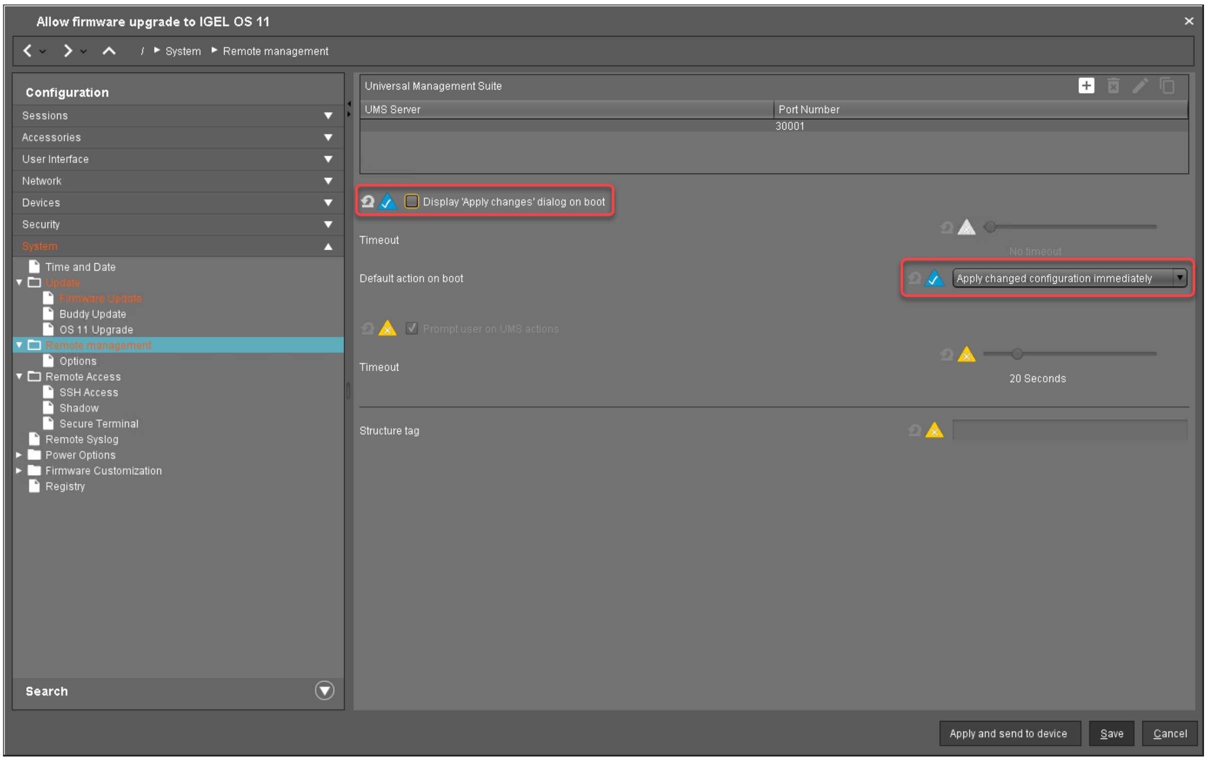
Password: ************

☑ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

☑ 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 113)):
   - 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**.



Universal Management Suite

UMS Server	Port Number
	30001

□ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag

5. Click **Save**.

When the profile es created, continue with Deploying the Licenses (see page 124).

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 Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

When the license deployment is set up, continue with Putting It All Together (see page 125).

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".

When everything is in place, continue with Executing the Upgrade (see page 126).

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.

   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 (see page 113).
   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. 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 128)
2. Creating a Profile (see page 129)
3. Deploying the Licenses (see page 133)
4. Assigning the Profile (see page 134)
5. Creating the Scheduled Job (see page 136)

Checking the Requirements

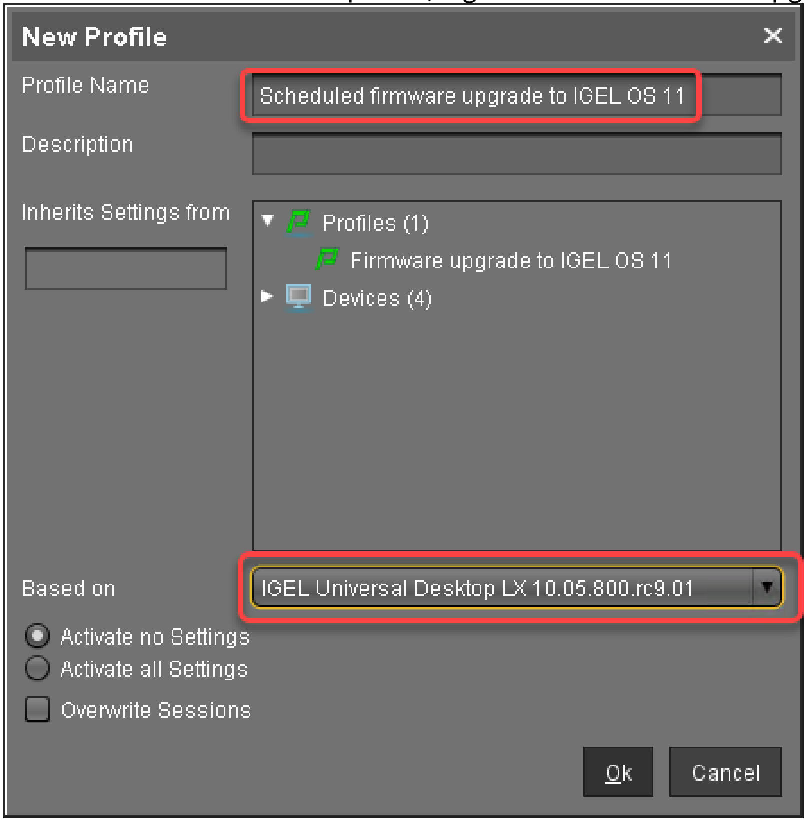
The following requirements must be met:

- 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 129).

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".



New Profile

Profile Name: Scheduled firmware upgrade to IGEL OS 11

Description:

Inherits Settings from

Based on: IGEL Universal Desktop LX 10.05.800.rc9.01

● Activate no Settings
○ Activate all Settings
□ Overwrite Sessions

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

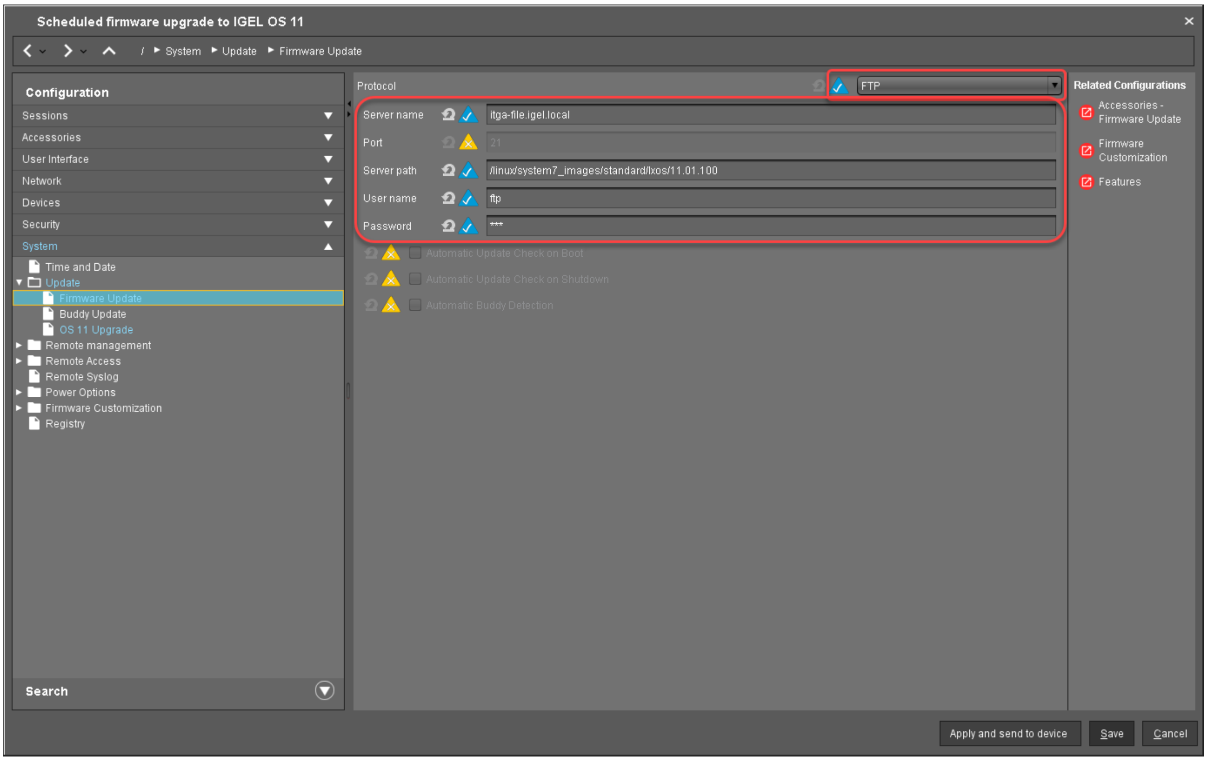
   > ⓘ If you use Universal Firmware Update (see page 163) for OS 11, you do not need to configure the settings described in this step.

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

     > ⓘ 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.



Scheduled firmware upgrade to IGEL OS 11

Protocol: FTP

Server name: itga-file.igel.local

Port: 21

Server path: /linux/system7_images/standard/lxos/11.01.100

User name: ftp

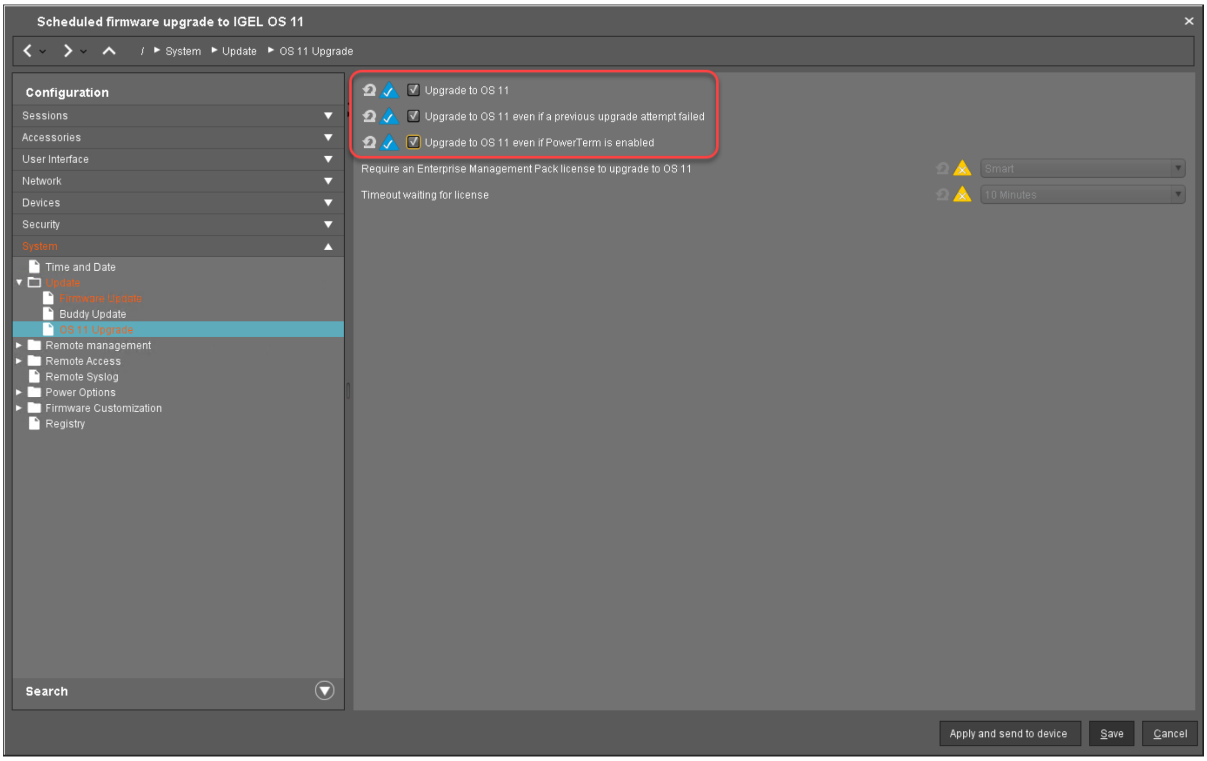
Password: ***

□ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

□ 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 **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**.



☑ Upgrade to OS 11

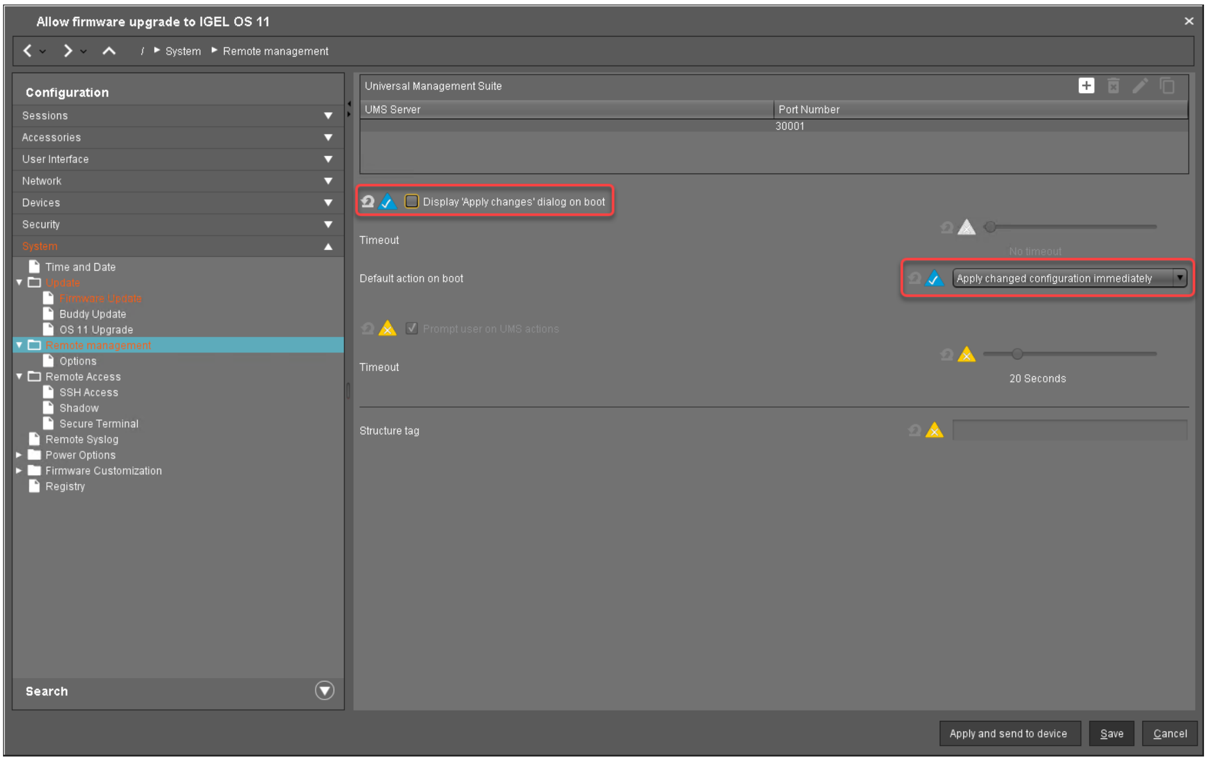
☑ Upgrade to OS 11 even if a previous upgrade attempt failed

☑ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for license: 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**.



Universal Management Suite

UMS Server	Port Number
	30001

☐ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag

5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 93).

Deploying the Licenses

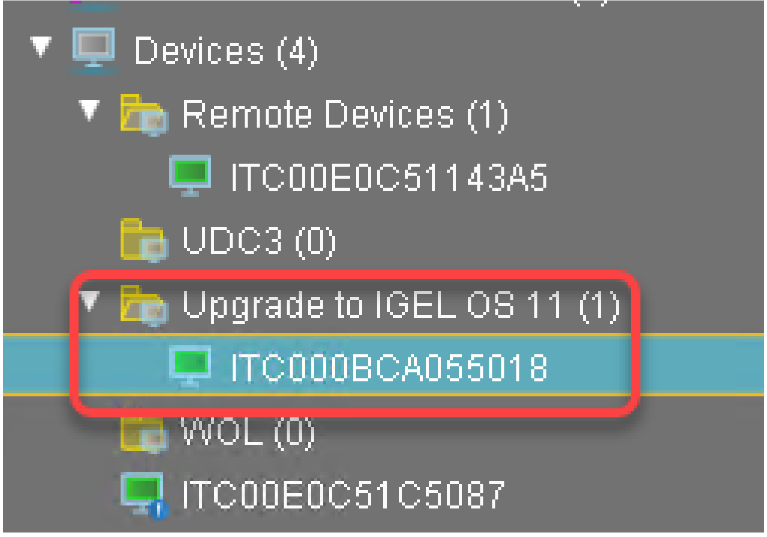
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

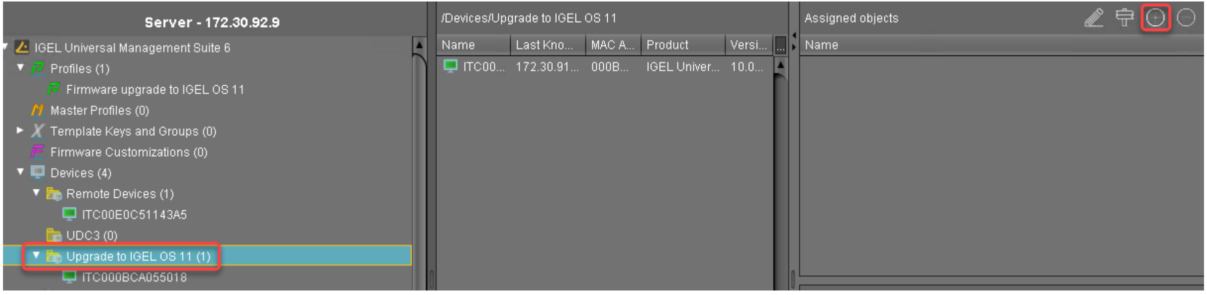
When the license deployment is set up, continue with Assigning the Profile (see page 134).

Assigning the Profile

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

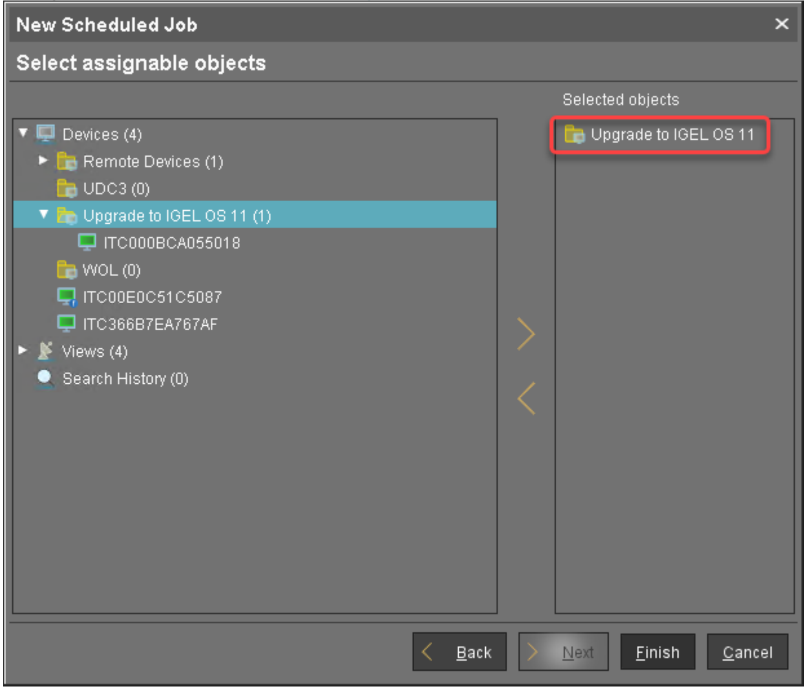


2. Select the directory and in the **Assigned objects** area, click ⊕.

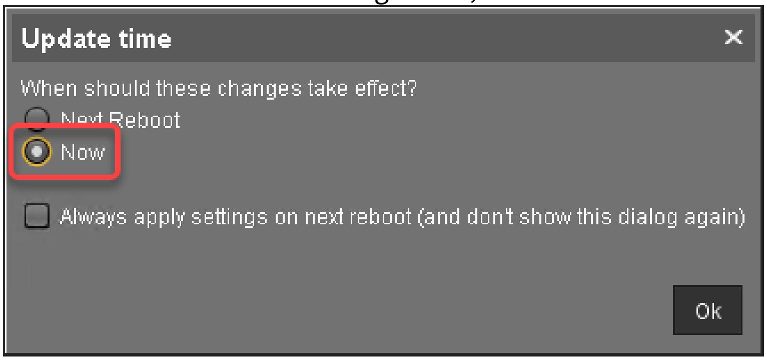

Server - 172.30.92.9
IGEL Universal Management Suite 6
Profiles (1)
Firmware upgrade to IGEL OS 11
Master Profiles (0)
Template Keys and Groups (0)
Firmware Customizations (0)
Devices (4)
Remote Devices (1)
ITC00E0C51143A5
UDC3 (0)
Upgrade to IGEL OS 11 (1)
ITC000BCA055018
/Devices/Upgrade to IGEL OS 11
Assigned objects
Name

Name	Last Kno...	MAC A...	Product	Versi...
ITC00...	172.30.91...	000B...	IGEL Univer...	10.0...

3. Assign the profile (see Creating a Profile (see page 129)) to the directory and click **Ok**.



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



When should these changes take effect?

○ Next Reboot

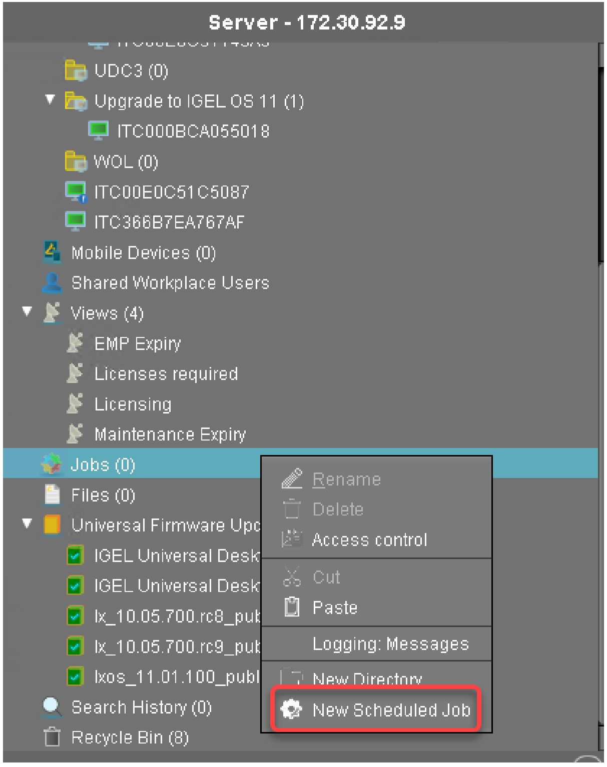
● Now

□ Always apply settings on next reboot (and don't show this dialog again)

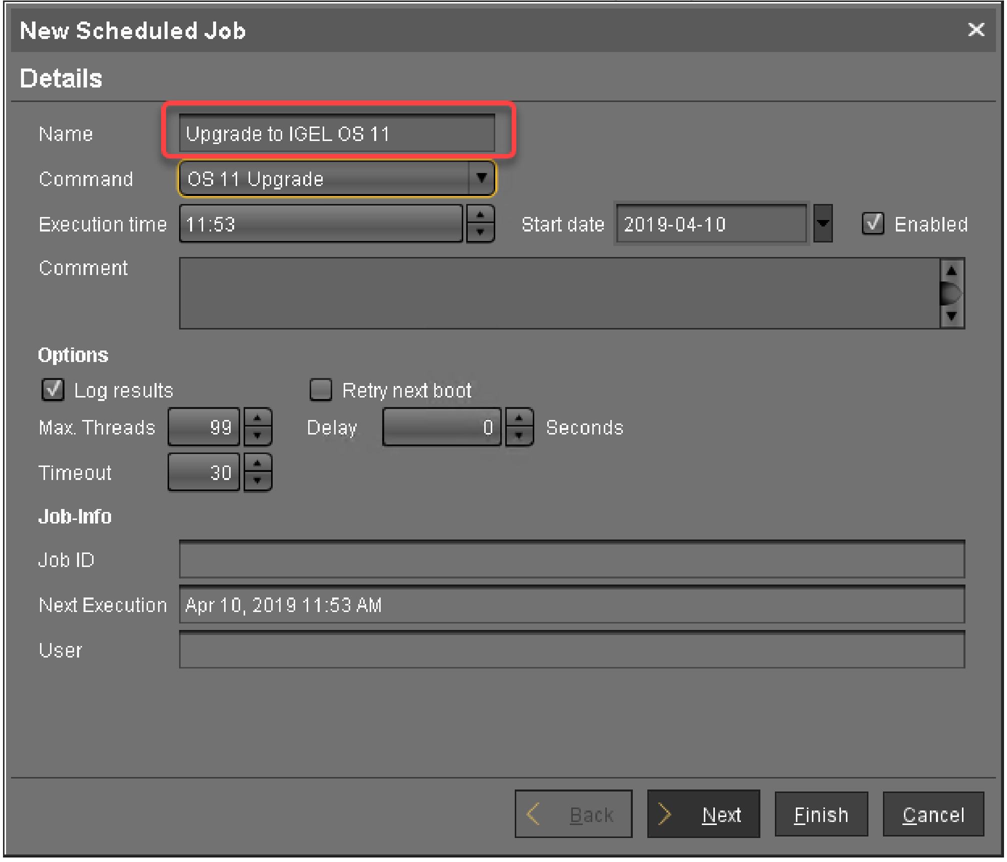
When the profile is assigned, continue with Creating the Scheduled Job (see page 136).

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".



New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:53

Start date: 2019-04-10

☑ Enabled

Comment:

Options

☑ Log results

☐ Retry next boot

Max. Threads: 99

Delay: 0 Seconds

Timeout: 30

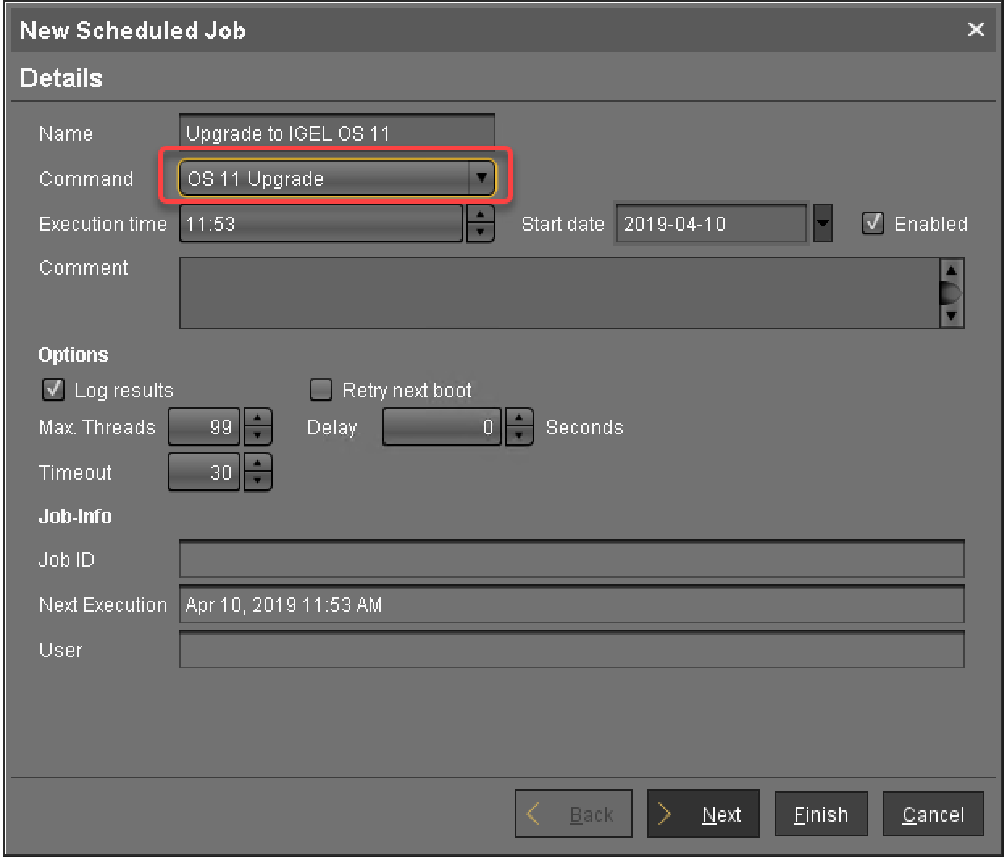
Job-Info

Job ID:

Next Execution: Apr 10, 2019 11:53 AM

User:

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



New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:53 Start date: 2019-04-10 ☑ Enabled

Comment:

Options

☑ Log results □ Retry next boot

Max. Threads: 99 Delay: 0 Seconds

Timeout: 30

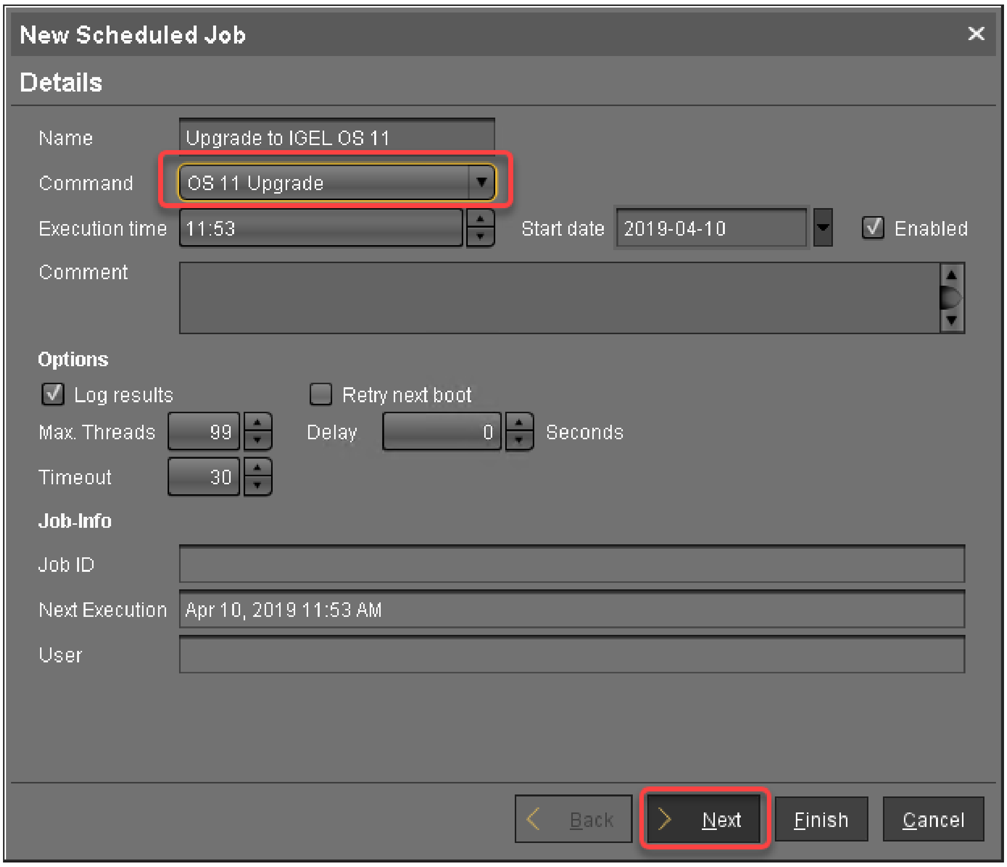
Job-Info

Job ID:

Next Execution: Apr 10, 2019 11:53 AM

User:

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



New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:53

Start date: 2019-04-10

☑ Enabled

Comment:

Options

☑ Log results

□ Retry next boot

Max. Threads: 99

Delay: 0 Seconds

Timeout: 30

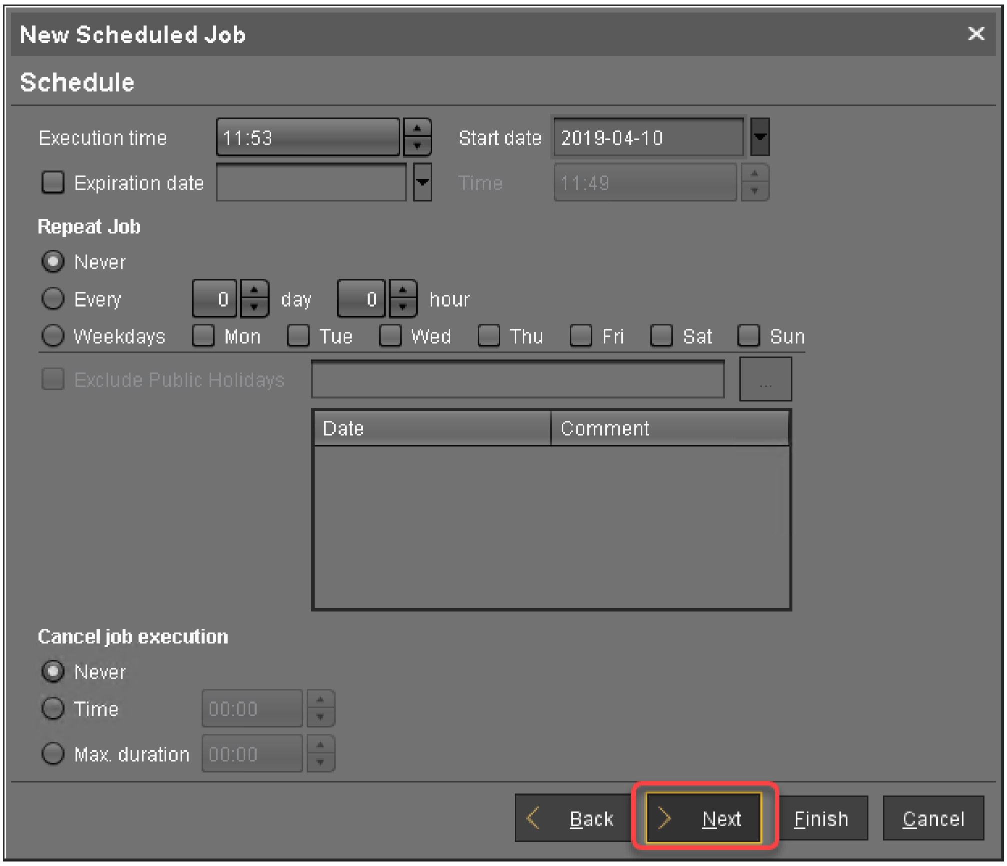
Job-Info

Job ID:

Next Execution: Apr 10, 2019 11:53 AM

User:

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



New Scheduled Job

Schedule

Execution time 11:53 Start date 2019-04-10

□ Expiration date Time 11:49

Repeat Job

● Never

○ Every 0 day 0 hour

○ Weekdays □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

□ Exclude Public Holidays

Date	Comment

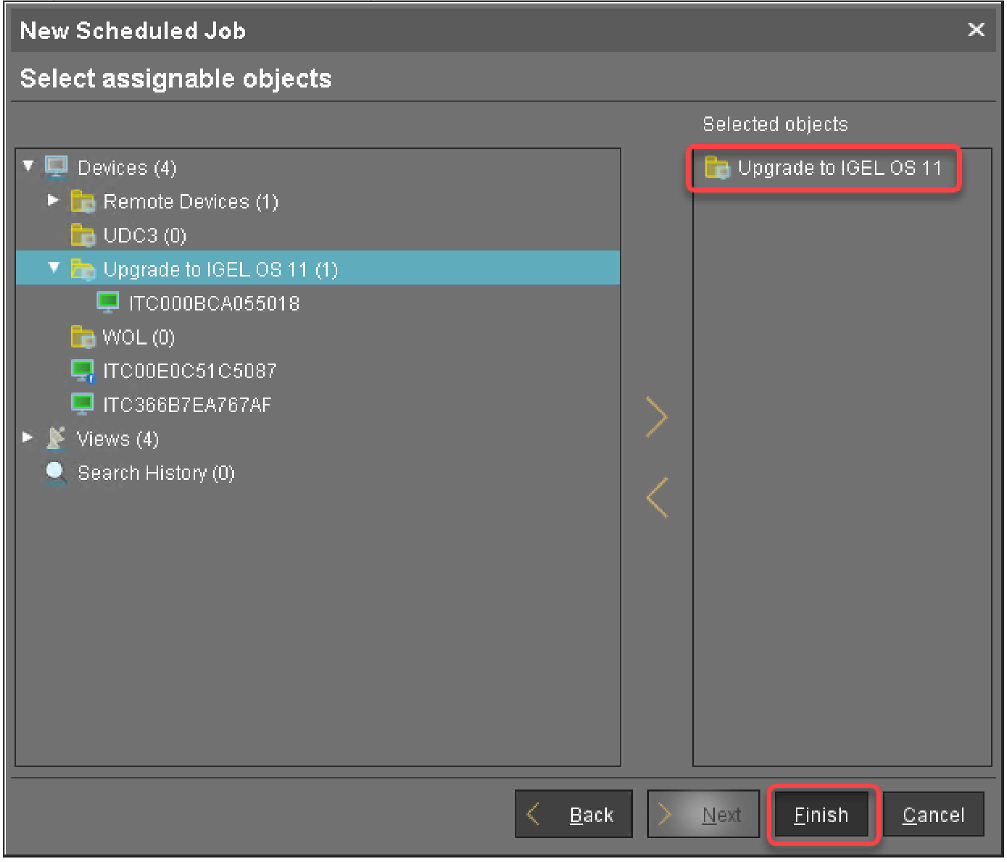
Cancel job execution

● Never

○ Time 00:00

○ Max. duration 00:00

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



The upgrade is completed.

Troubleshooting

This section describes possible error cases and solutions.

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.

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).

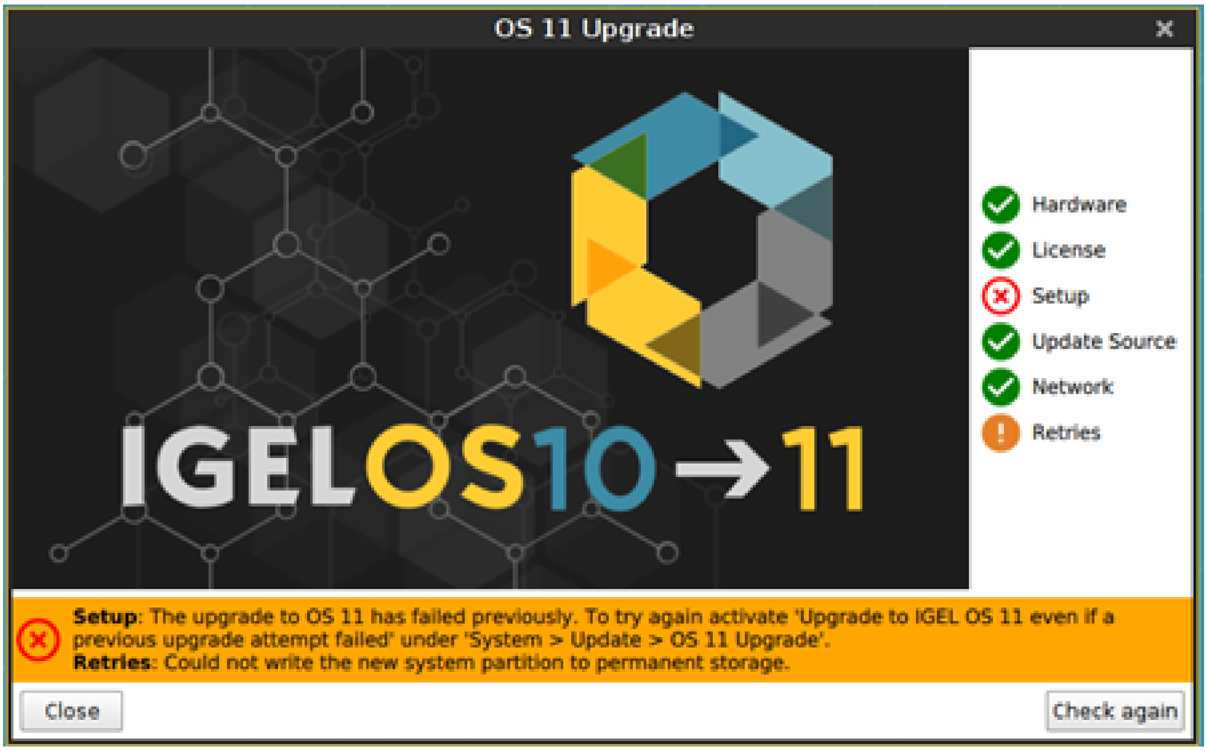
Or:

▶ 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:



Setup: The upgrade to OS 11 has failed previously. To try again activate 'Upgrade to IGEL OS 11 even if a previous upgrade attempt failed' under 'System > Update > OS 11 Upgrade'.
Retries: Could not write the new system partition to permanent storage.

- 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 in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see the chapter Save Device 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 148): 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 179): 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 200): 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

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 Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.

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*** (see page 150)	Yes	2 or 4 GB	8 GB	Yes
UD3* (see page 150)	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* (see page 150)	H830C	50	Yes	2 GB	4 GB	Yes

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** (see page 150)	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9* (see page 150)	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

* IGEL UD3-LX 50 and UD5-LX 50 are officially supported up to IGEL OS 11.05, incl. private builds. IGEL UD9-LX 40 / 41 (Touch) devices are officially supported up to IGEL OS 11.07.910.

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

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

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 151).

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 IGEL 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.

License

- A valid license from an IGEL Workspace Edition (WE) Product Pack must be available for each device. For general information, see IGEL Software License Overview. For deploying licenses, see 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 153).

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 154).

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 Updating a UMS Installation.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter Registering Devices on the UMS Server in the UMS Manual.

When the UMS is prepared, continue with Adjusting the Setup (see page 155).

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 148), Zero-Touch Deployment Using Buddy Update (see page 179) and Mass Deployment Using a Scheduled Job (see page 200)). 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 (see page 156).

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 Workspace Edition
- If one of the following features is used, one Enterprise Management Pack license is required (see Enterprise Management Pack):
  - 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 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 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 157).

Configuring the Update Source

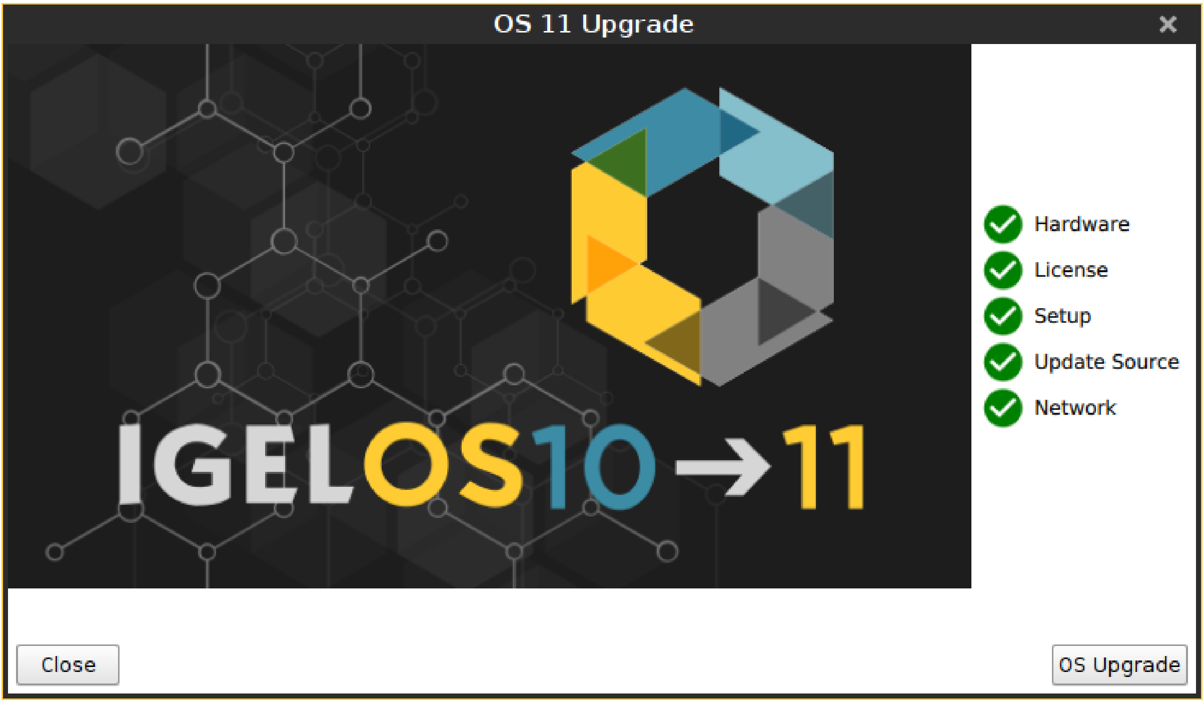
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade (see page 158).

Testing the Upgrade

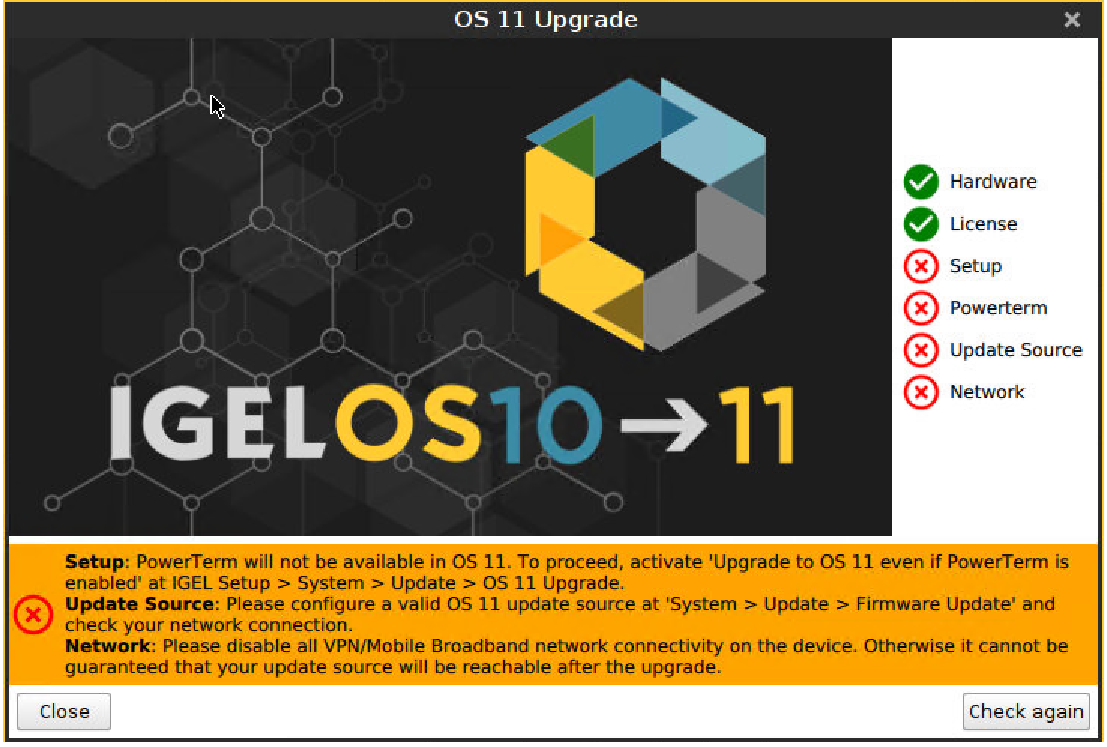
1. Click ⚙ System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

> ⓘ 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.



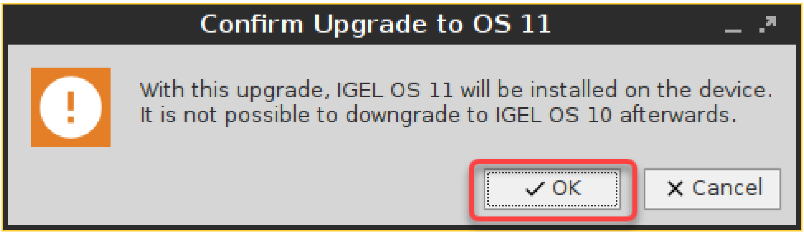
OS 11 Upgrade

✓ Hardware
✓ License
✗ Setup
✗ Powerterm
✗ Update Source
✗ Network

Setup: PowerTerm will not be available in OS 11. To proceed, activate 'Upgrade to OS 11 even if PowerTerm is enabled' at IGEL Setup > System > Update > OS 11 Upgrade.
Update Source: Please configure a valid OS 11 update source at 'System > Update > Firmware Update' and check your network connection.
Network: Please disable all VPN/Mobile Broadband network connectivity on the device. Otherwise it cannot be guaranteed that your update source will be reachable after the upgrade.

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

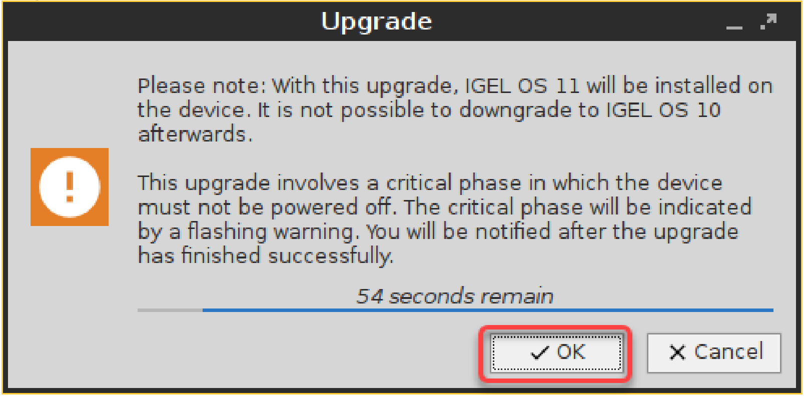
3. Click **OK** to continue.



Confirm Upgrade to OS 11

With this upgrade, IGEL OS 11 will be installed on the device.
It is not possible to downgrade to IGEL OS 10 afterwards.

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



Upgrade

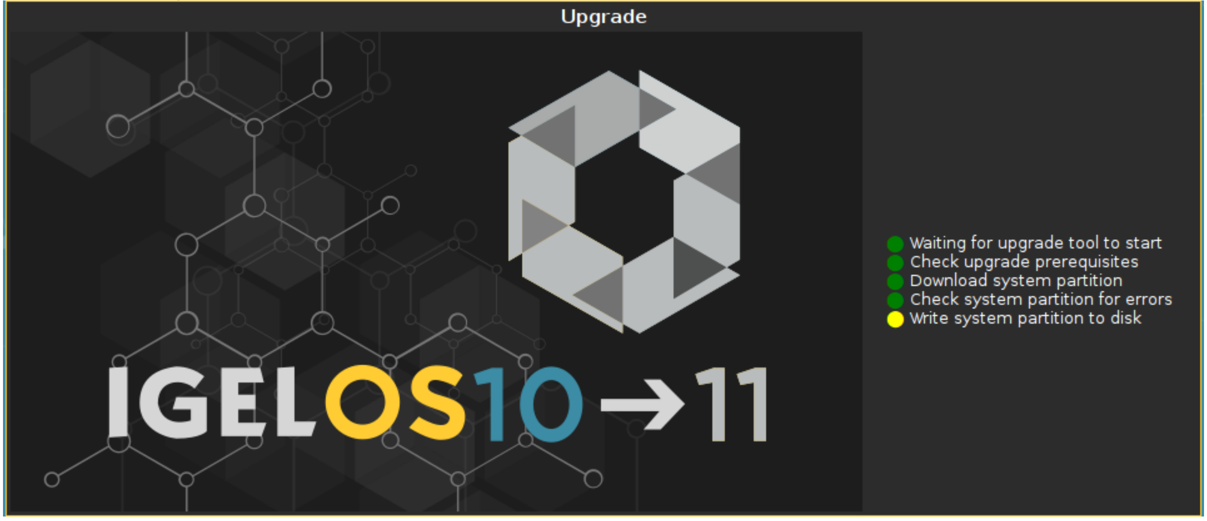
Please note: With this upgrade, IGEL OS 11 will be installed on the device. It is not possible to downgrade to IGEL OS 10 afterwards.

This upgrade involves a critical phase in which the device must not be powered off. The critical phase will be indicated by a flashing warning. You will be notified after the upgrade has finished successfully.

54 seconds remain

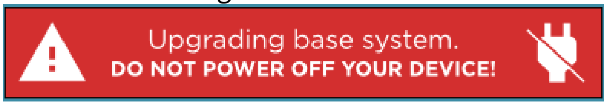
After the warning dialog has been confirmed or the timeout has expired, the device reboots into a special IGEL OS 10 environment, in which the system upgrade is executed. The **Upgrade** window

shows the progress.



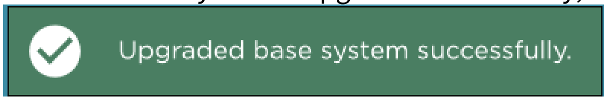
Waiting for upgrade tool to start
Check upgrade prerequisites
Download system partition
Check system partition for errors
Write system partition to disk

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



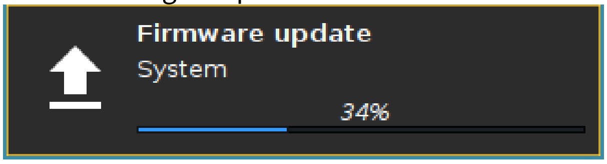
Upgrading base system.
DO NOT POWER OFF YOUR DEVICE!

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



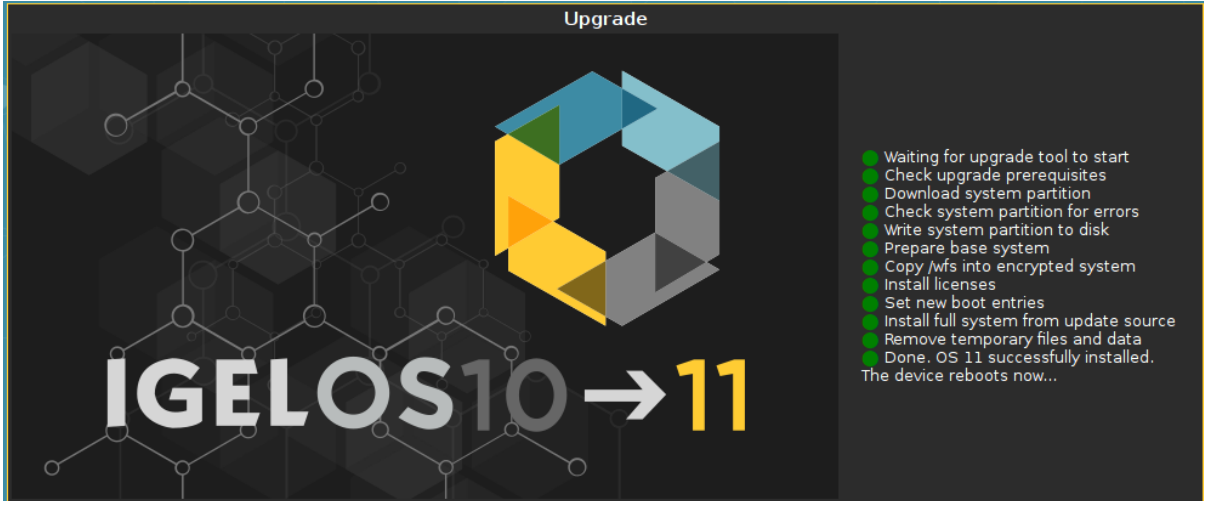
Upgraded base system successfully.

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



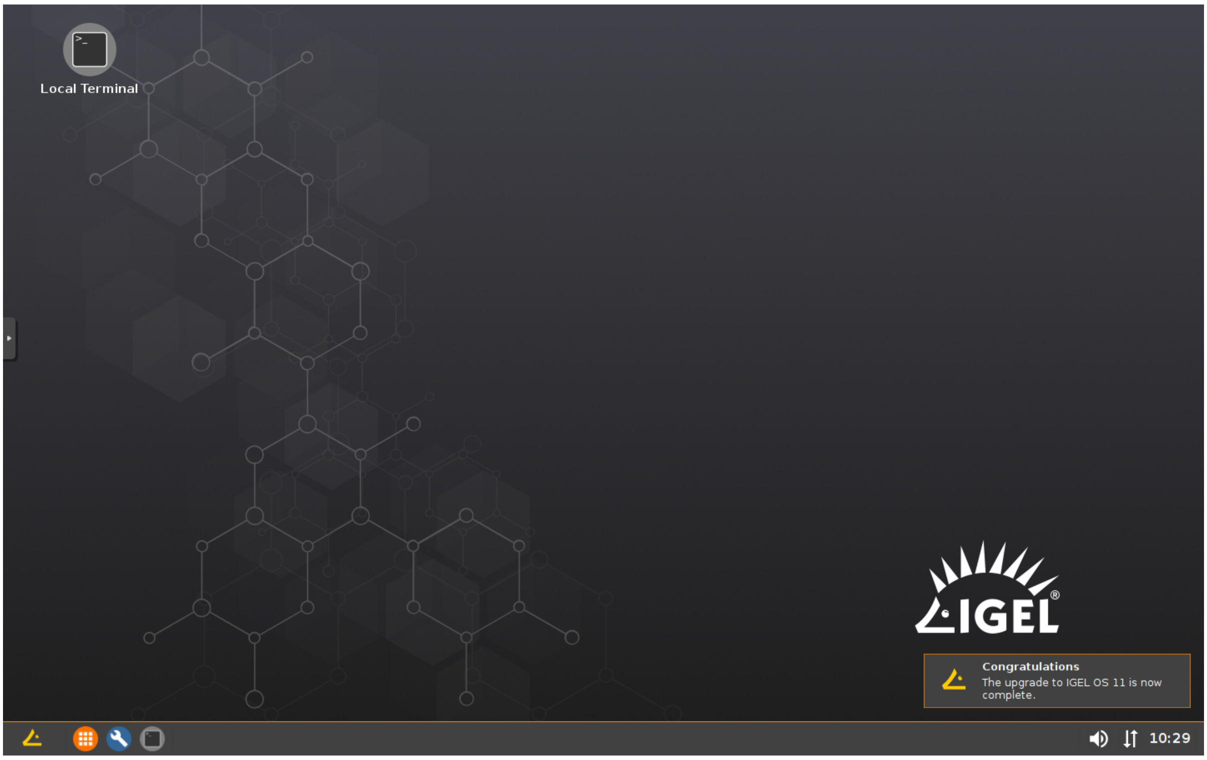
Firmware update
System
34%

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



Waiting for upgrade tool to start
Check upgrade prerequisites
Download system partition
Check system partition for errors
Write system partition to disk
Prepare base system
Copy /wfs into encrypted system
Install licenses
Set new boot entries
Install full system from update source
Remove temporary files and data
Done. OS 11 successfully installed.
The device reboots now...

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



Congratulations
The upgrade to IGEL OS 11 is now complete.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 162).

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 the requirements are met, continue with Creating the Universal Firmware Updates (see page 163).

Creating the Universal Firmware Updates

For detailed information, see the chapter Universal Firmware Update in the UMS Manual.

> ⓘ If you use the 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.

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.

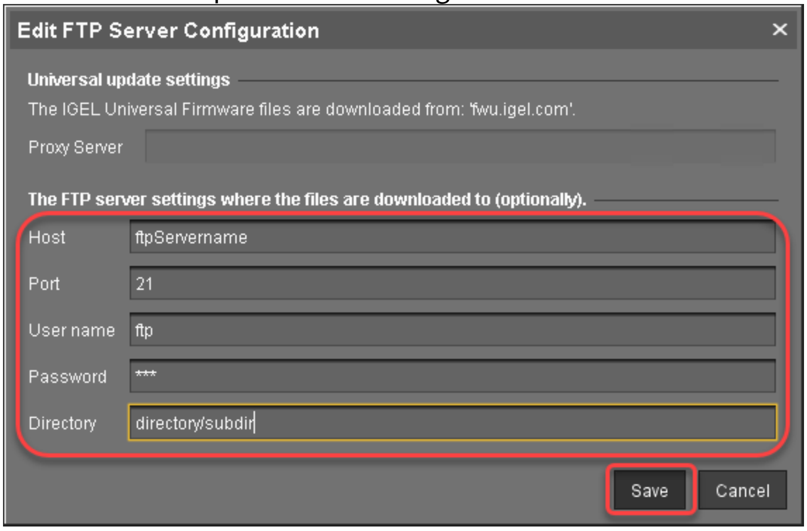
   > The order of creation is crucial because the IGEL OS 11 firmware must have a higher ID in order to be chosen by the device. For details, see Executing the Upgrade (see page 177).

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



Edit FTP Server Configuration

Universal update settings

The IGEL Universal Firmware files are downloaded from: 'fwu.igel.com'.

Proxy Server

The FTP server settings where the files are downloaded to (optionally).

Host: ftpServername

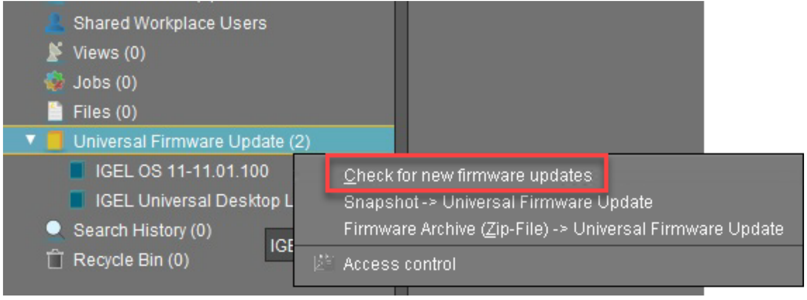
Port: 21

User name: ftp

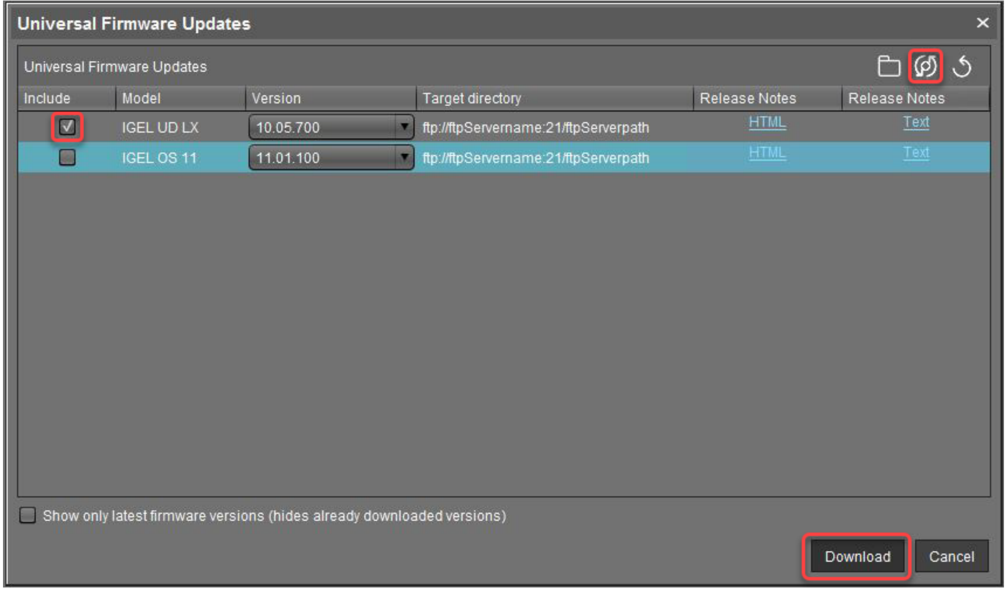
Password: ***

Directory: directory/subdir

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


Shared Workplace Users
Views (0)
Jobs (0)
Files (0)
Universal Firmware Update (2)
IGEL OS 11-11.01.100
IGEL Universal Desktop L
Search History (0)
Recycle Bin (0)
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

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



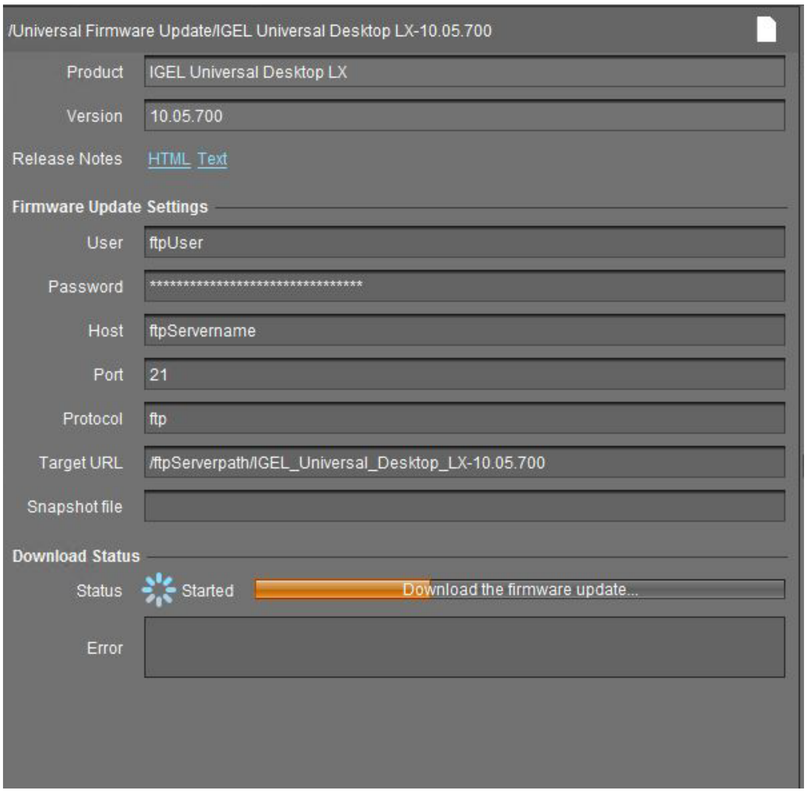
Universal Firmware Updates

Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
☑	IGEL UD LX	10.05.700	ftp://ftpServername:21/ftpServerpath	HTML	Text
□	IGEL OS 11	11.01.100	ftp://ftpServername:21/ftpServerpath	HTML	Text

□ Show only latest firmware versions (hides already downloaded versions)

5. The firmware is transferred to the FTP server.



/Universal Firmware Update/IGEL Universal Desktop LX-10.05.700

Product: IGEL Universal Desktop LX

Version: 10.05.700

Release Notes: HTML Text

Firmware Update Settings

User: ftpUser

Password: ********************************

Host: ftpServername

Port: 21

Protocol: ftp

Target URL: /ftpServerpath/IGEL_Universal_Desktop_LX-10.05.700

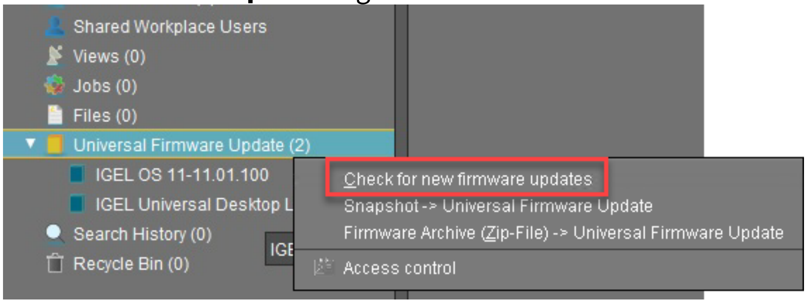
Snapshot file:

Download Status

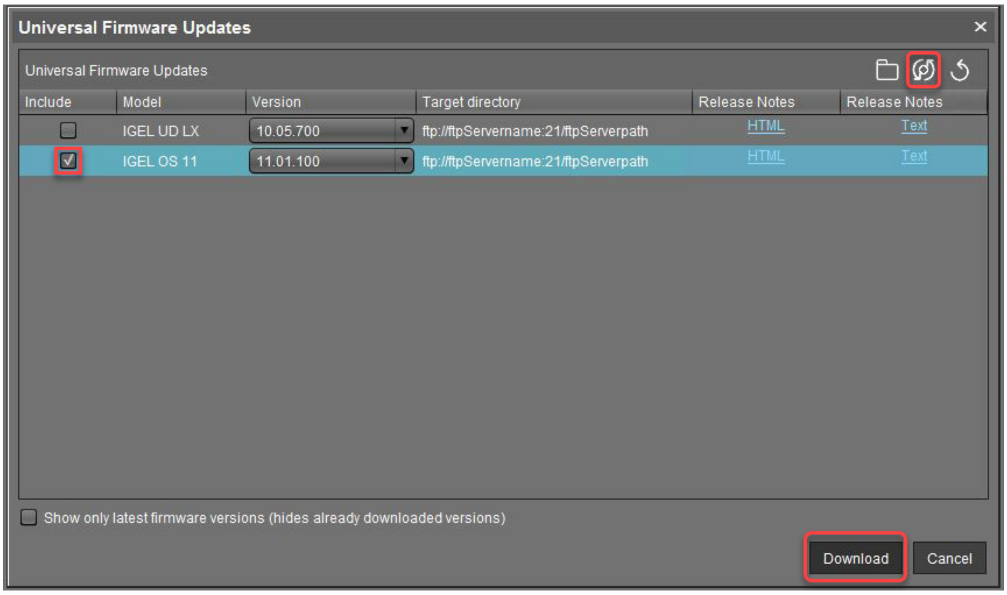
Status: Started Download the firmware update...

Error:

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


Shared Workplace Users
Views (0)
Jobs (0)
Files (0)
Universal Firmware Update (2)
IGEL OS 11-11.01.100
IGEL Universal Desktop L
Search History (0)
Recycle Bin (0)
IGE
Check for new firmware updates
Snapshot -> Universal Firmware Update
Firmware Archive (Zip-File) -> Universal Firmware Update
Access control

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



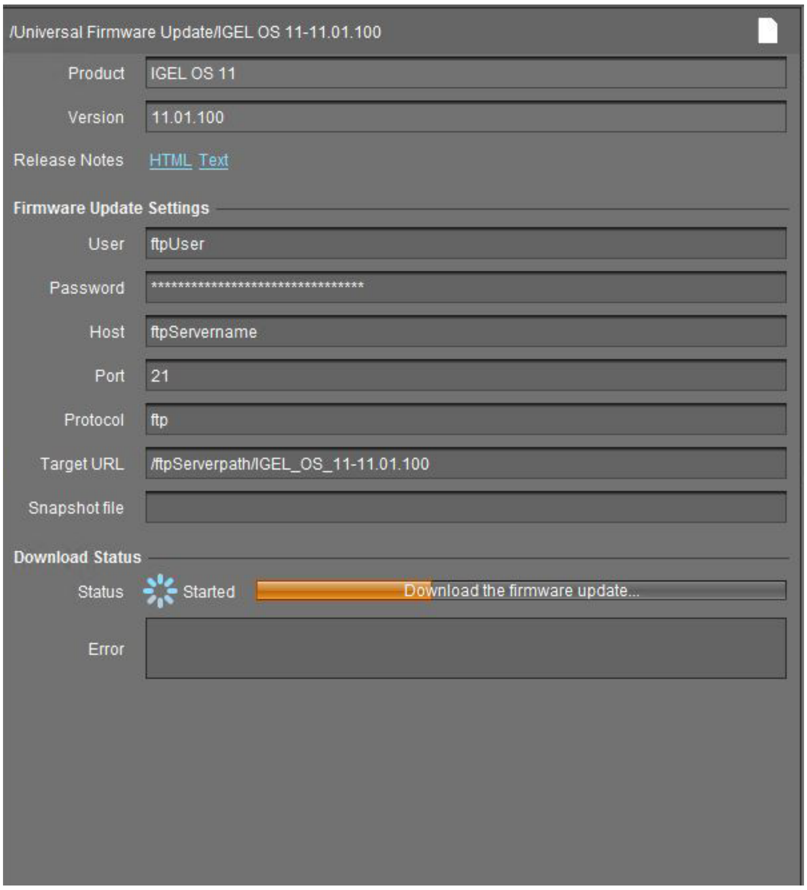
Universal Firmware Updates

Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
□	IGEL UD LX	10.05.700	ftp://ftpServername:21/ftpServerpath	HTML	Text
☑	IGEL OS 11	11.01.100	ftp://ftpServername:21/ftpServerpath	HTML	Text

□ Show only latest firmware versions (hides already downloaded versions)

8. The firmware is transferred to the FTP server.



/Universal Firmware Update/IGEL OS 11-11.01.100

Product: IGEL OS 11

Version: 11.01.100

Release Notes: HTML Text

Firmware Update Settings

User: ftpUser

Password: ********************************

Host: ftpServername

Port: 21

Protocol: ftp

Target URL: /ftpServerpath/IGEL_OS_11-11.01.100

Snapshot file:

Download Status

Status: Started Download the firmware update...

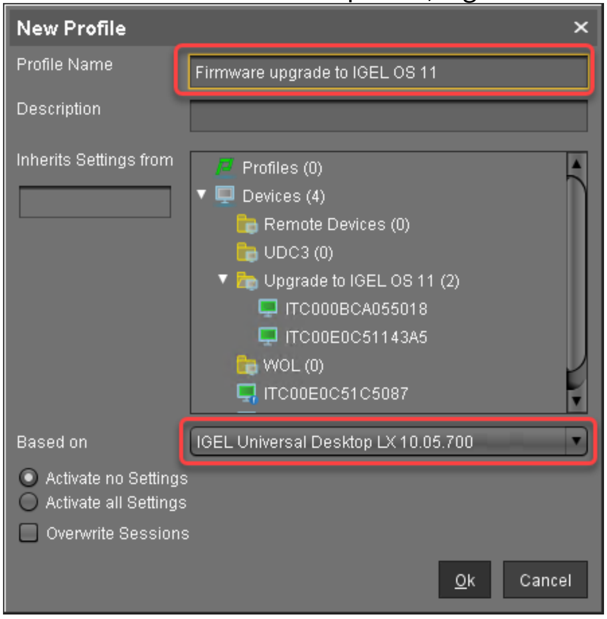
Error:

The devices can download the firmware from the FTP server.

When the Universal Firmware Update is ready, continue with Creating a Profile (see page 168).

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".



New Profile

Profile Name: Firmware upgrade to IGEL OS 11

Description:

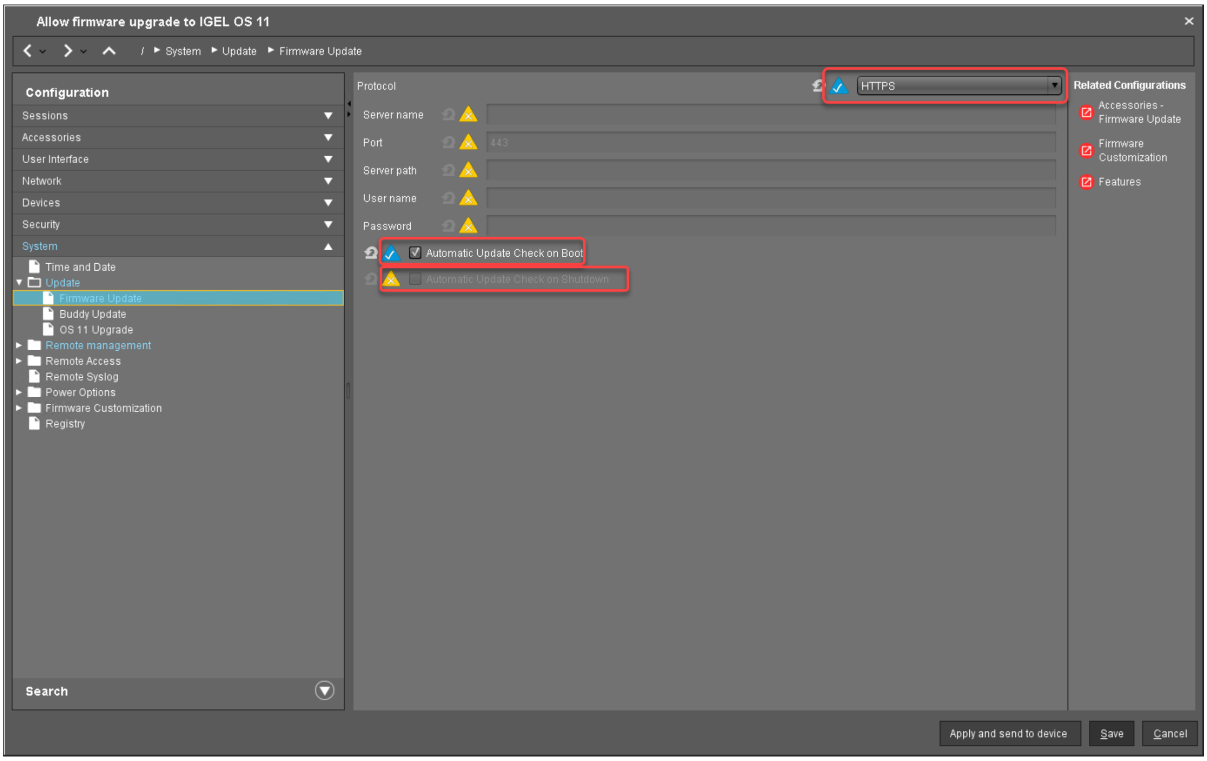
Inherits Settings from:

- Profiles (0)
- Devices (4)
  - Remote Devices (0)
  - UDC3 (0)
  - Upgrade to IGEL OS 11 (2)
    - ITC000BCA055018
    - ITC00E0C51143A5
  - WOL (0)
  - ITC00E0C51C5087

Based on: IGEL Universal Desktop LX 10.05.700

● Activate no Settings
○ Activate all Settings
□ Overwrite Sessions

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.



Protocol: HTTPS

Server name

Port: 443

Server path

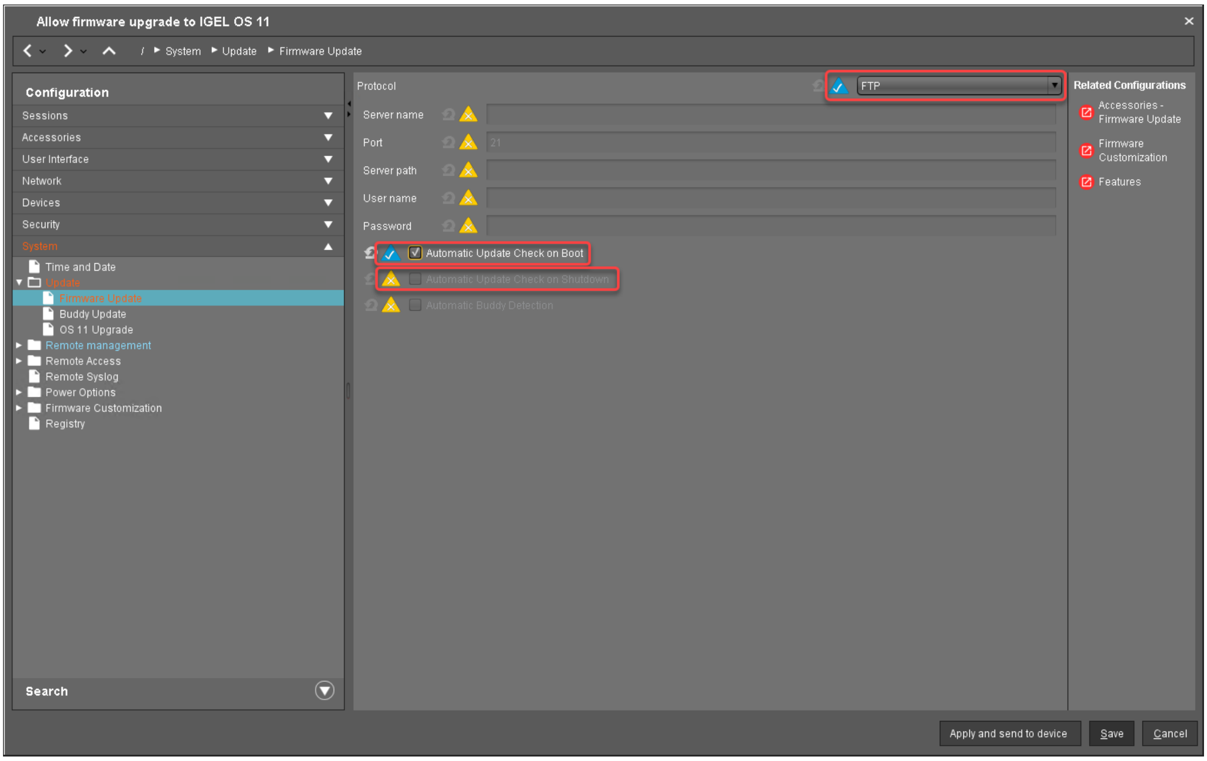
User name

Password

☑ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

- 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.



Allow firmware upgrade to IGEL OS 11

Protocol: FTP

Server name

Port: 21

Server path

User name

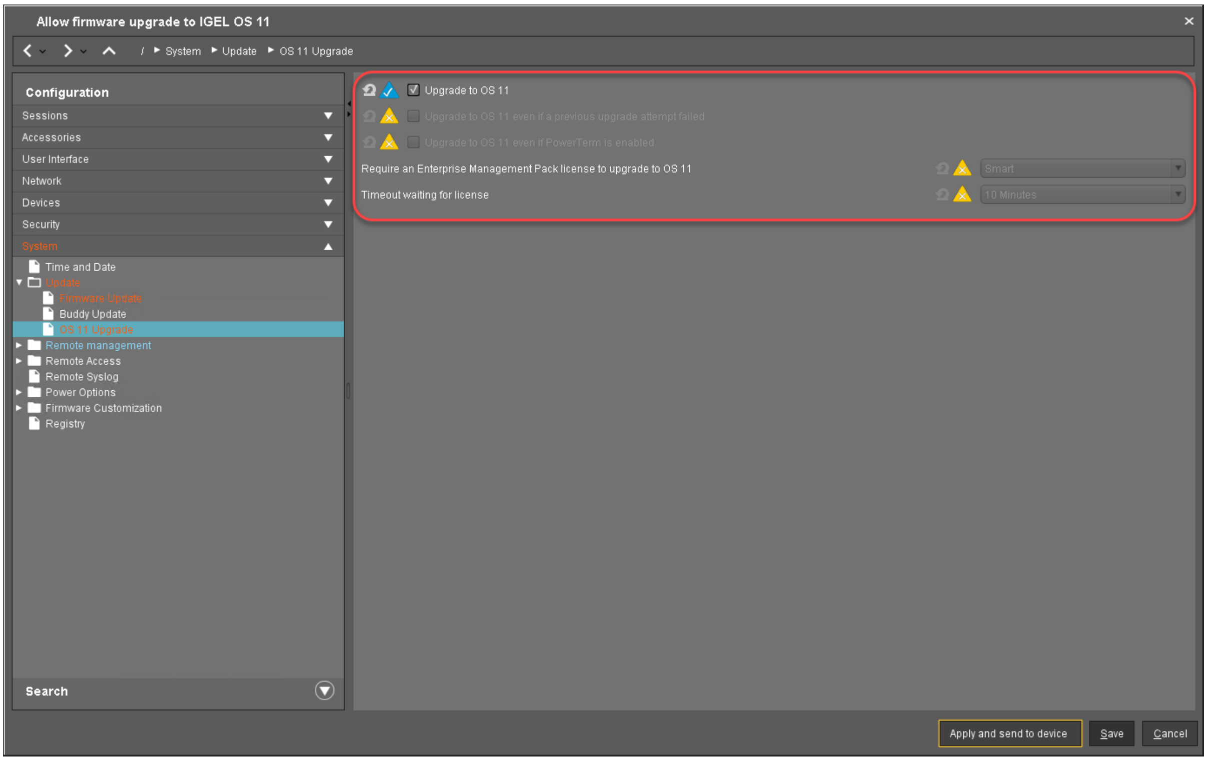
Password

☑ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

□ 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 **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**.



Allow firmware upgrade to IGEL OS 11

☑ Upgrade to OS 11

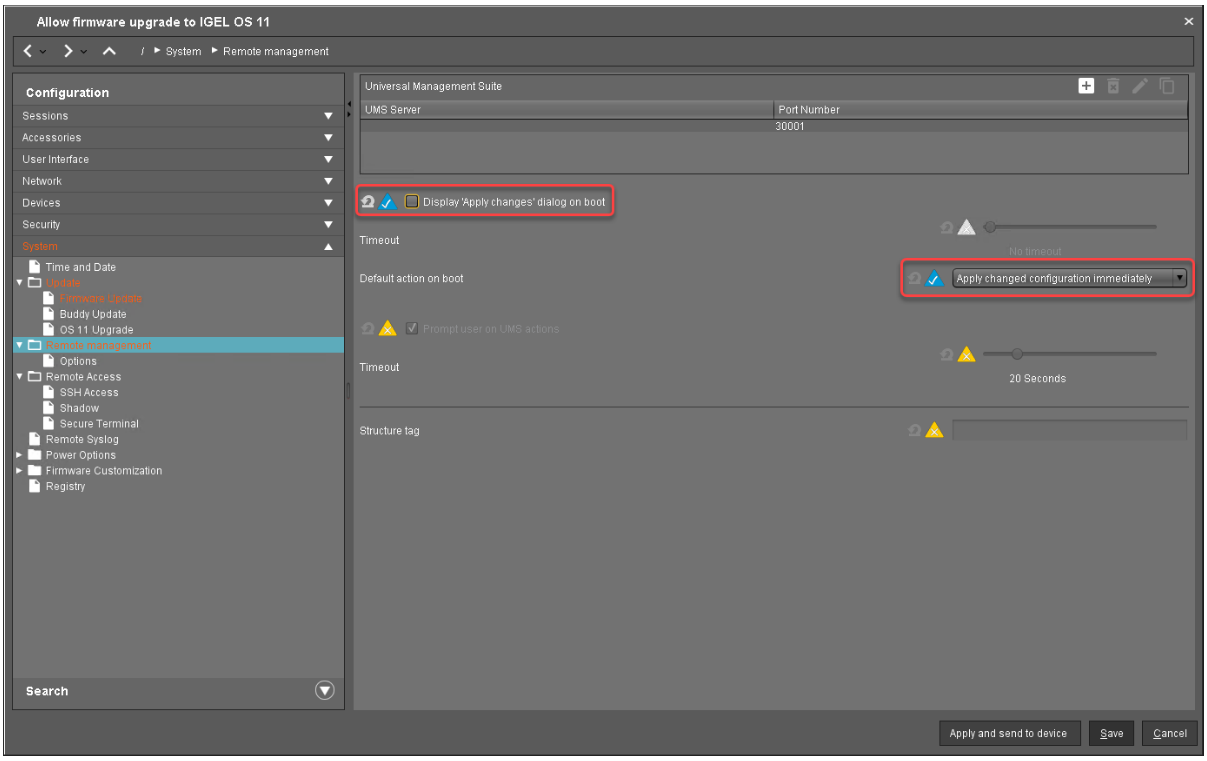
□ Upgrade to OS 11 even if a previous upgrade attempt failed

□ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for license: 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**.



UMS Server	Port Number
	30001

☐ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag

5. Click **Save**.

When the profile es created, continue with Deploying the Licenses (see page 173).

Deploying the Licenses

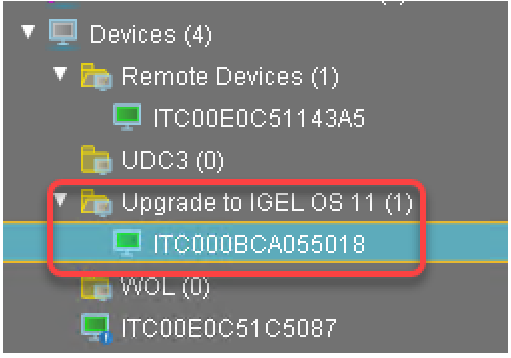
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

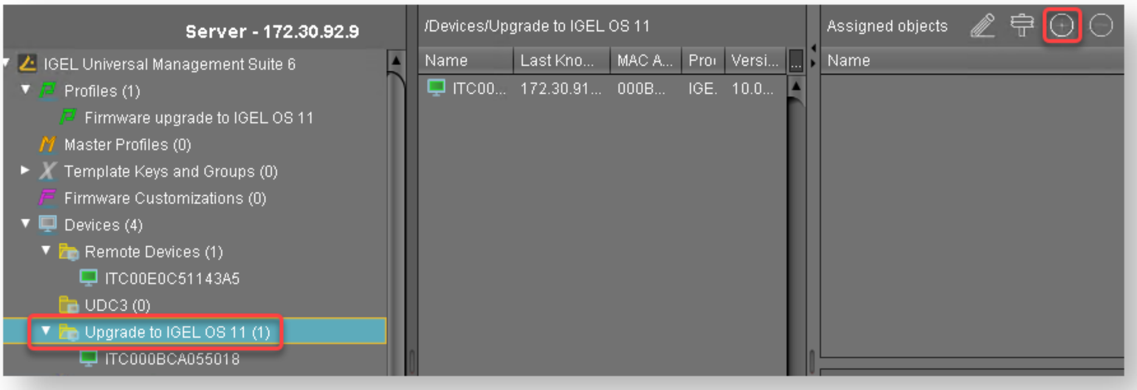
When the license deployment is setup up, continue with Putting It All Together (see page 174).

Putting It All Together

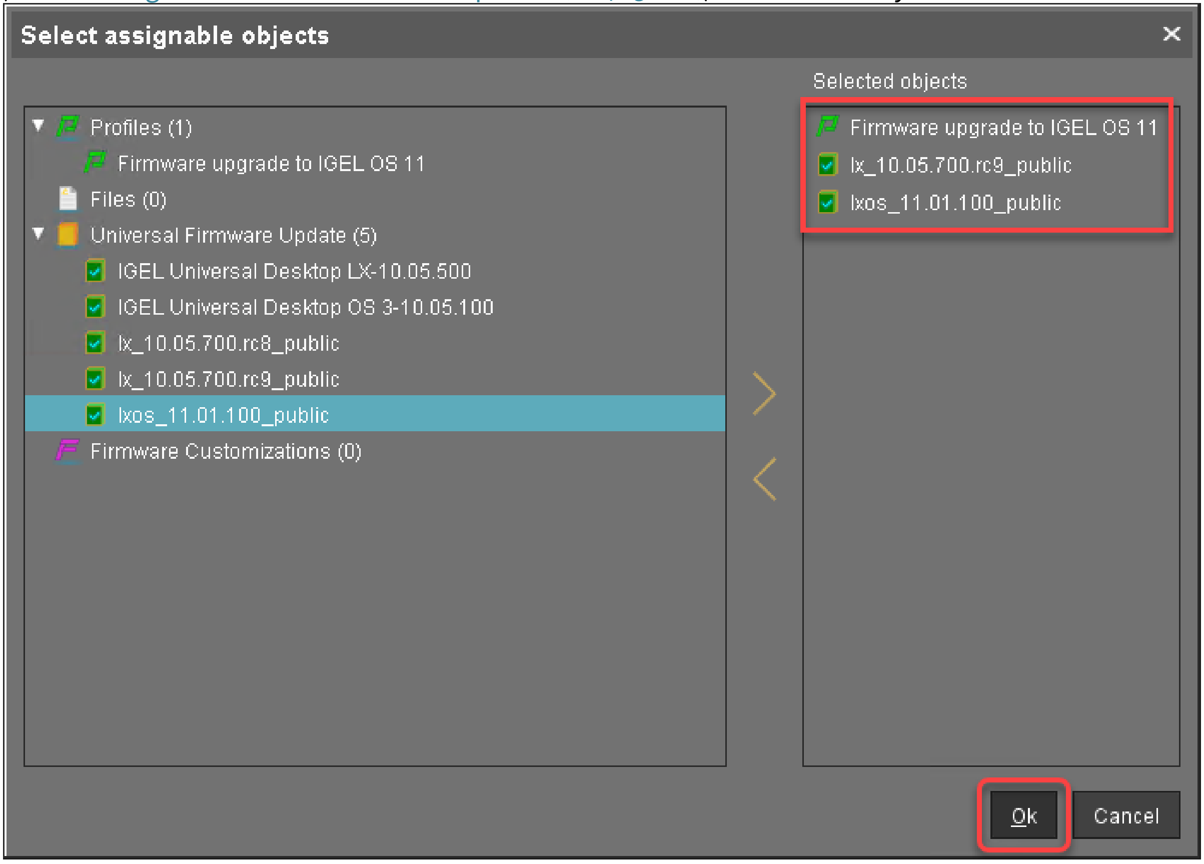
1. Put all devices that are to be updated into a directory.



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



3. Assign the profile (see Creating a Profile (see page 168)) and the two Universal Firmware Updates (see Creating the Universal Firmware Updates (see page 163)) to the directory and click **Ok**.



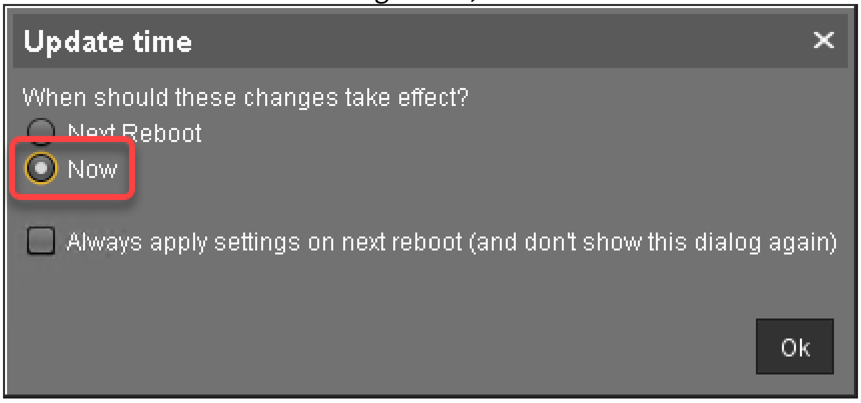
Select assignable objects

- Profiles (1)
  - Firmware upgrade to IGEL OS 11
- Files (0)
- Universal Firmware Update (5)
  - IGEL Universal Desktop LX-10.05.500
  - IGEL Universal Desktop OS 3-10.05.100
  - lx_10.05.700.rc8_public
  - lx_10.05.700.rc9_public
  - lxos_11.01.100_public
- Firmware Customizations (0)

Selected objects

- Firmware upgrade to IGEL OS 11
- lx_10.05.700.rc9_public
- lxos_11.01.100_public

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



Update time

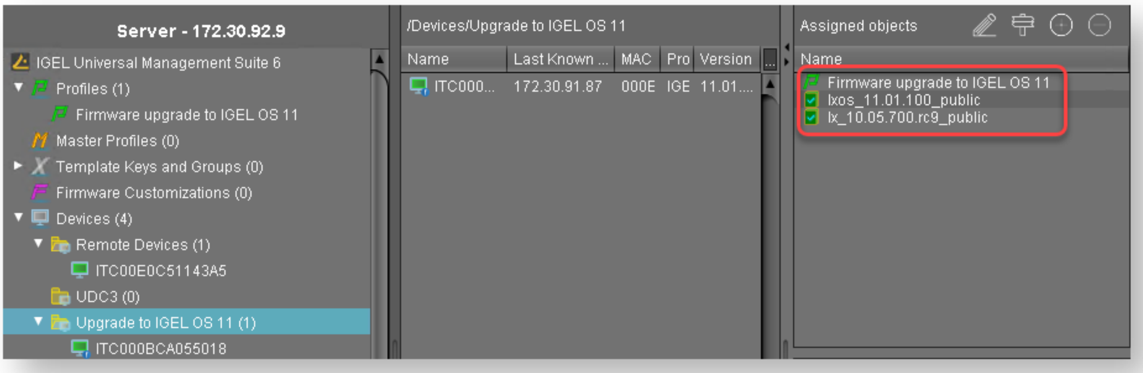
When should these changes take effect?

○ Next Reboot

● Now

□ Always apply settings on next reboot (and don't show this dialog again)

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


Server - 172.30.92.9
IGEL Universal Management Suite 6
Profiles (1)
Firmware upgrade to IGEL OS 11
Master Profiles (0)
Template Keys and Groups (0)
Firmware Customizations (0)
Devices (4)
Remote Devices (1)
ITC00E0C51143A5
UDC3 (0)
Upgrade to IGEL OS 11 (1)
ITC000BCA055018
/Devices/Upgrade to IGEL OS 11
Assigned objects
Name
Firmware upgrade to IGEL OS 11
lxos_11.01.100_public
lx_10.05.700.rc9_public

Name	Last Known ...	MAC	Pro	Version
ITC000...	172.30.91.87	000E	IGE	11.01....

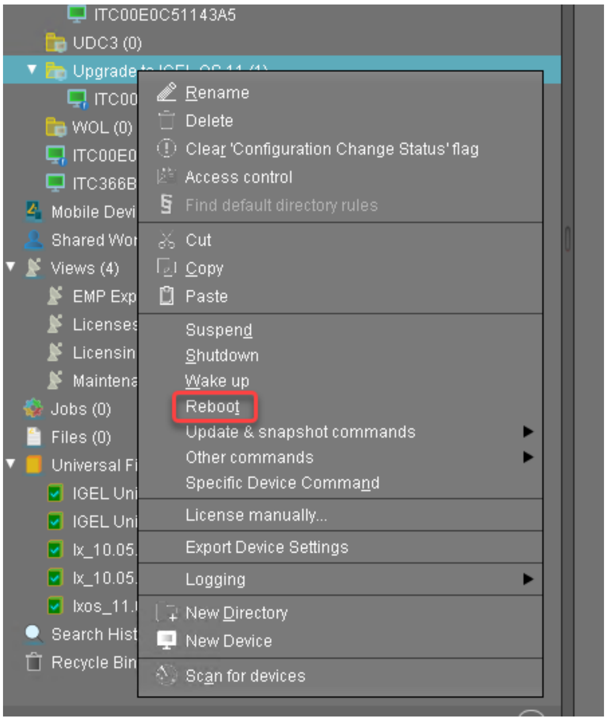
5. If you are using Automatic License Deployment (ALD), it might be feasible to confine the distribution of licenses to the current directory. For more information, see Configuring the Distribution Conditions, section "Distributing Licenses to Devices in a Specified Directory".

When everything is in place, continue with Executing the Upgrade (see page 177).

Executing the Upgrade

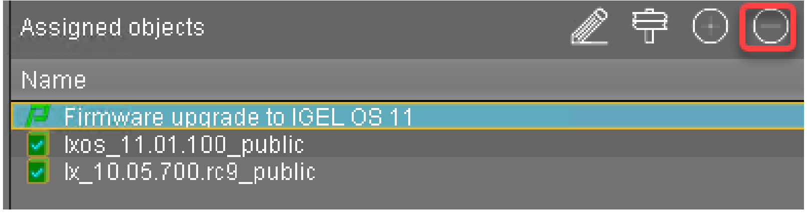
1. In the UMS, select the directory containing all devices that are to be upgraded and reboot them.

   > ⓘ 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.



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 155).
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. 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.



Assigned objects

Name

Firmware upgrade to IGEL OS 11

lxos_11.01.100_public

lx_10.05.700.rc9_public

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.

1. IGEL Devices That Can Be Upgraded to IGEL OS 11 (see page 180)
2. Important! Consider This Before Upgrading (see page 151)
3. Preparing the Upgrade (see page 153)
4. Testing the Upgrade (see page 158)
5. Checking the Requirements (see page 162)
6. Configuring Two Update Buddies (see page 194)
7. Creating a Profile (see page 195)
8. Deploying the Licenses (see page 197)
9. Putting It All Together (see page 198)
10. Executing the Upgrade (see page 199)

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 Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.

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*** (see page 181)	Yes	2 or 4 GB	8 GB	Yes
UD3* (see page 181)	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* (see page 181)	H830C	50	Yes	2 GB	4 GB	Yes

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** (see page 181)	H850C	11	Yes	4 GB	4 GB	Yes
UD7	H860C	20	Yes	8 GB	8 GB	Yes
UD9* (see page 181)	TC215B	40 / 41 (Touch)	Yes	2 GB	4 GB	Yes

* IGEL UD3-LX 50 and UD5-LX 50 are officially supported up to IGEL OS 11.05, incl. private builds. IGEL UD9-LX 40 / 41 (Touch) devices are officially supported up to IGEL OS 11.07.910.

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

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

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 182).

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 IGEL 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.

License

- A valid license from an IGEL Workspace Edition (WE) Product Pack must be available for each device. For general information, see IGEL Software License Overview. For deploying licenses, see 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 184).

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 185)
2. Adjusting the Setup (see page 186)
3. Deploying a License (see page 187)
4. Configuring the Update Source (see page 188)

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 Updating a UMS Installation.
2. Make sure that your devices are registered with the UMS. For more information, see the chapter Registering Devices on the UMS Server in the UMS Manual.

When the UMS is ready, continue with Adjusting the Setup (see page 186).

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 148), Zero-Touch Deployment Using Buddy Update (see page 179) and Mass Deployment Using a Scheduled Job (see page 200)). 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 187).

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 Workspace Edition
- If one of the following features is used, one Enterprise Management Pack license is required (see Enterprise Management Pack):
  - 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 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 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 188).

Configuring the Update Source

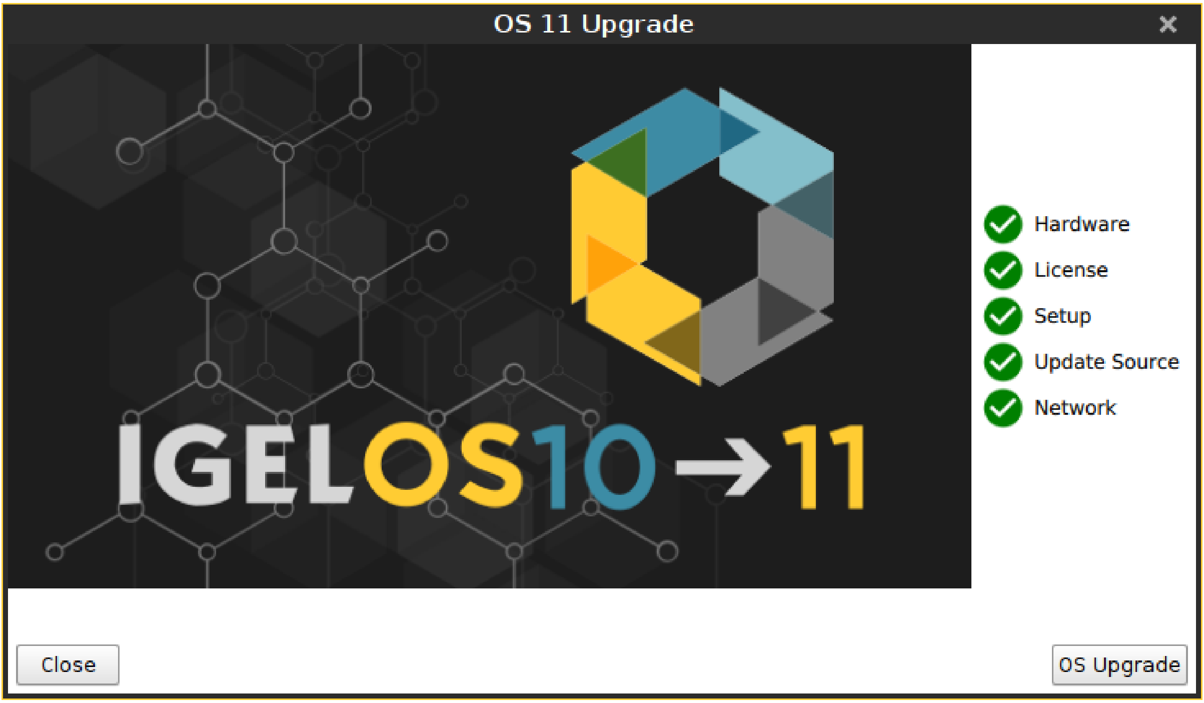
1. In the Setup, go to **System > Update > Firmware Update** and configure the update source for IGEL OS 11. For more information, see the Firmware Update chapter in the IGEL OS Manual.
2. Click **Ok**.

When the correct update source is configured, continue with Testing the Upgrade (see page 189).

Testing the Upgrade

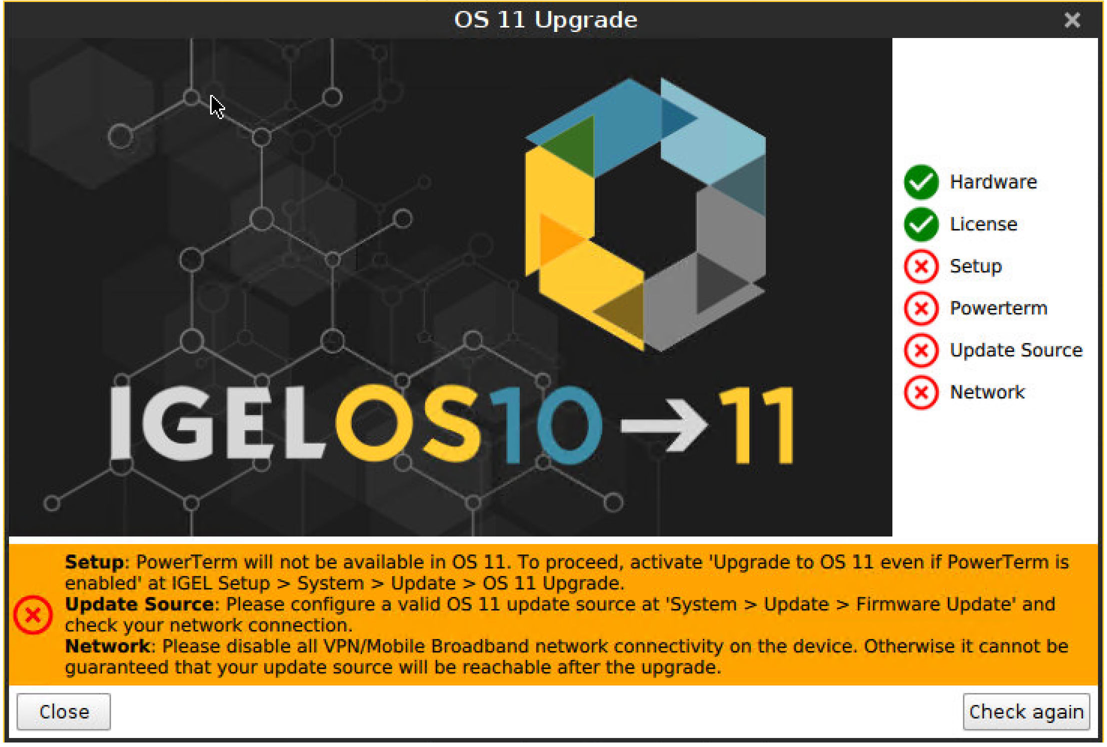
1. Click ⚙ System and then **Upgrade to OS 11**. The OS 11 Upgrade Tool starts and indicates whether all requirements are met.

   > ⓘ 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**

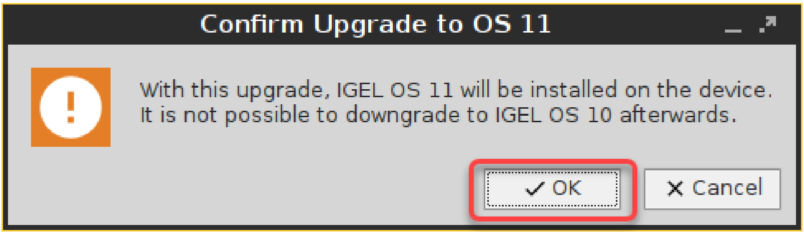
Upgrade, and you can start the upgrade.



Setup: PowerTerm will not be available in OS 11. To proceed, activate 'Upgrade to OS 11 even if PowerTerm is enabled' at IGEL Setup > System > Update > OS 11 Upgrade.
Update Source: Please configure a valid OS 11 update source at 'System > Update > Firmware Update' and check your network connection.
Network: Please disable all VPN/Mobile Broadband network connectivity on the device. Otherwise it cannot be guaranteed that your update source will be reachable after the upgrade.

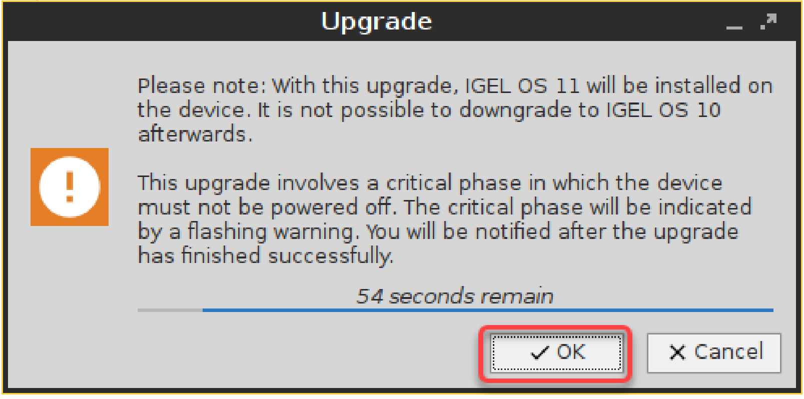
When you start the upgrade, a warning dialog is shown.

3. Click **OK** to continue.



With this upgrade, IGEL OS 11 will be installed on the device.
It is not possible to downgrade to IGEL OS 10 afterwards.

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



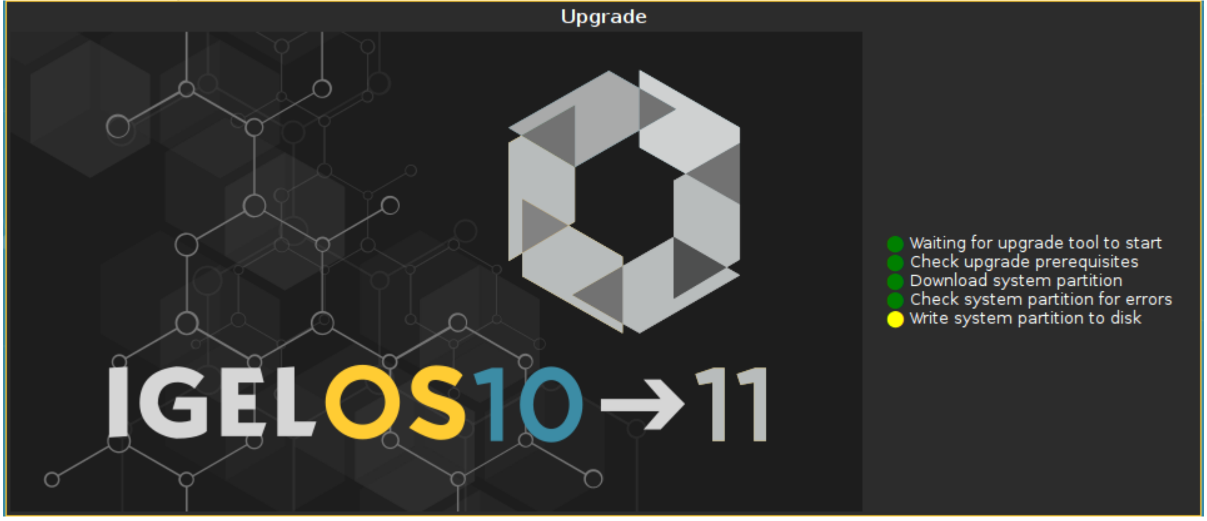
Please note: With this upgrade, IGEL OS 11 will be installed on the device. It is not possible to downgrade to IGEL OS 10 afterwards.

This upgrade involves a critical phase in which the device must not be powered off. The critical phase will be indicated by a flashing warning. You will be notified after the upgrade has finished successfully.

54 seconds remain

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

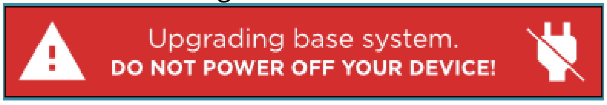
shows the progress.



Upgrade

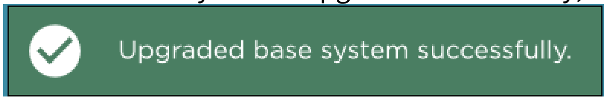
● Waiting for upgrade tool to start
● Check upgrade prerequisites
● Download system partition
● Check system partition for errors
● Write system partition to disk

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



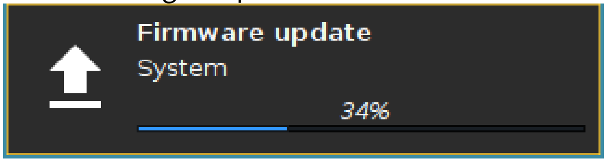
Upgrading base system.
DO NOT POWER OFF YOUR DEVICE!

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



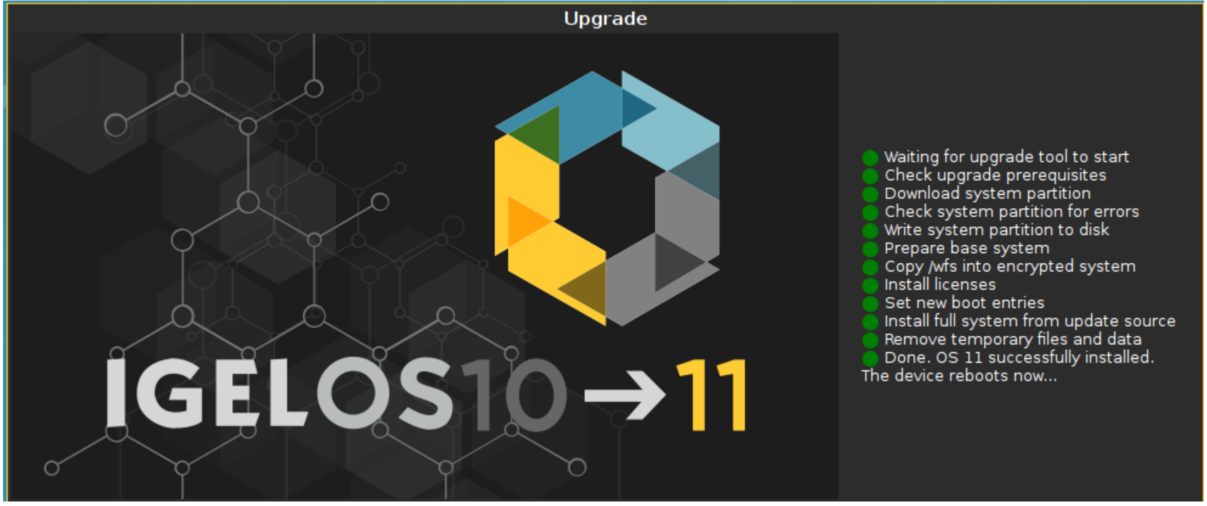
Upgraded base system successfully.

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



Firmware update
System
34%

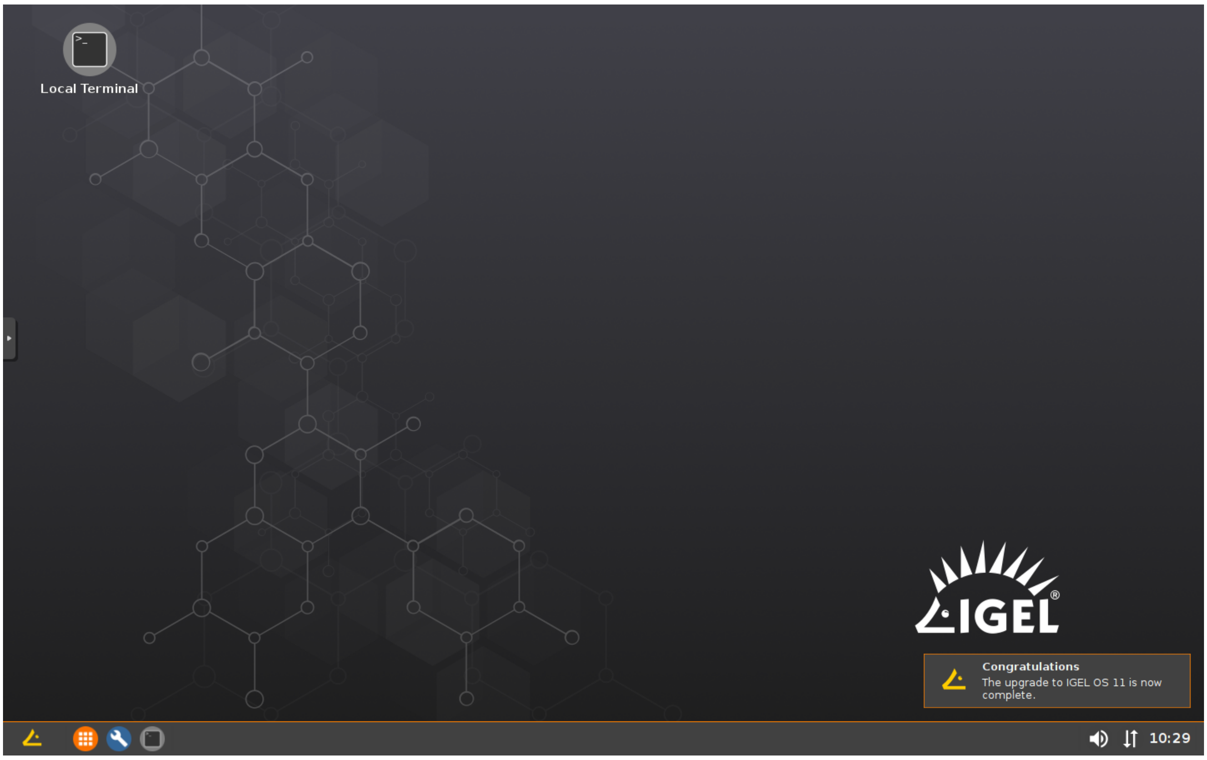
When the installation is completed, the **Upgrade** window looks like this:



Upgrade

● Waiting for upgrade tool to start
● Check upgrade prerequisites
● Download system partition
● Check system partition for errors
● Write system partition to disk
● Prepare base system
● Copy /wfs into encrypted system
● Install licenses
● Set new boot entries
● Install full system from update source
● Remove temporary files and data
● Done. OS 11 successfully installed.
The device reboots now...

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



Congratulations

The upgrade to IGEL OS 11 is now complete.

When the upgrade test has been successful, you are ready to set up the mass upgrade. Continue with Checking the Requirements (see page 193).

Checking the Requirements

The following requirements must be met:

- The upgrade has been tested with characteristic devices; see Testing the Upgrade (see page 158).
- 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 (see page 158)) 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.

Configuring Two Update Buddies

For setting up buddy updates, see the How-To Buddy Update (see page 217).

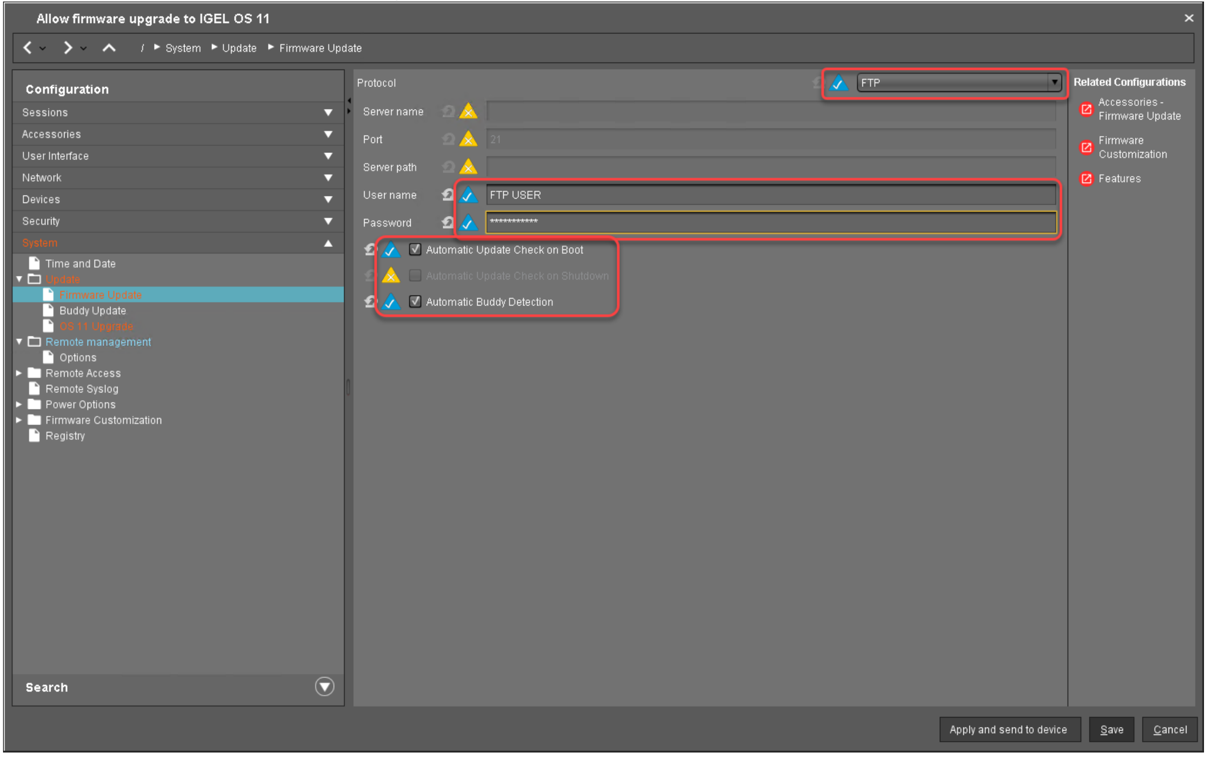
> Ensure that the network contains only the update buddies and the devices that are to be updated. This prevents other devices from updating inadvertently.

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 195).

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**.



Allow firmware upgrade to IGEL OS 11

Protocol: FTP

Server name:

Port: 21

Server path:

User name: FTP USER

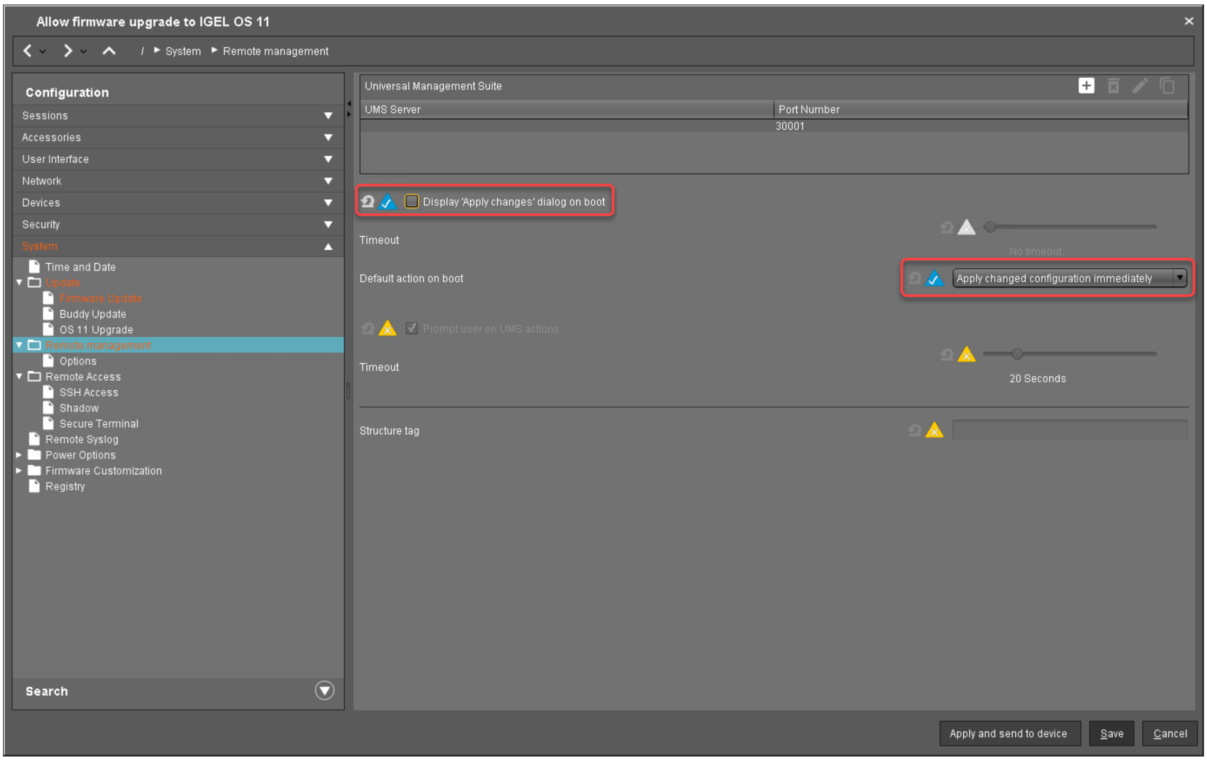
Password: ************

☑ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

☑ 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**.



Allow firmware upgrade to IGEL OS 11

/ ▸ System ▸ Remote management

Universal Management Suite

UMS Server	Port Number
	30001

□ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag:

5. Click **Save**.

When the profile is created, continue with Deploying the Licenses (see page 197).

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 Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

When the license deployment is set up, continue with Putting It All Together (see page 198).

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".

When everything is in place, continue with Executing the Upgrade (see page 199).

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.

   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 155).
   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. When all devices have been upgraded successfully, remove the "Firmware upgrade to IGEL OS 11" profile.

The upgrade is complete.

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.

1. Checking the Requirements (see page 201)
2. Creating a Profile (see page 202)
3. Deploying the Licenses (see page 206)
4. Assigning the Profile (see page 207)
5. Executing the Upgrade (see page 177)

Checking the Requirements

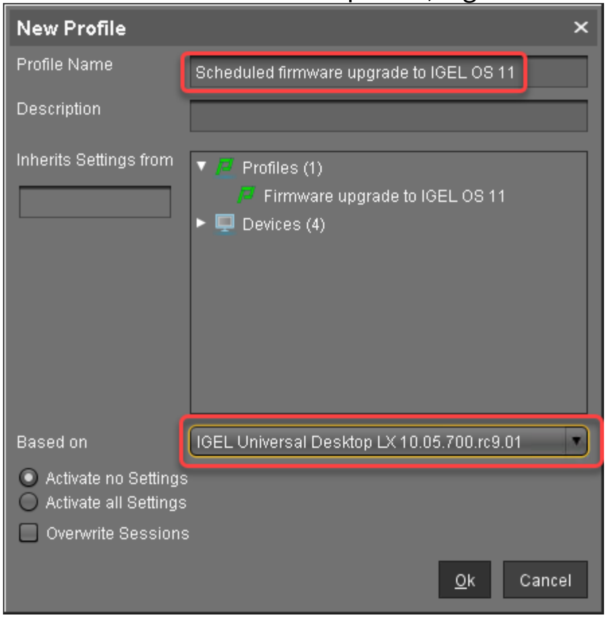
The following requirements must be met:

- 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 202).

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".



New Profile

Profile Name: Scheduled firmware upgrade to IGEL OS 11

Description:

Inherits Settings from:

- Profiles (1)
  - Firmware upgrade to IGEL OS 11
- Devices (4)

Based on: IGEL Universal Desktop LX 10.05.700.rc9.01

● Activate no Settings

○ Activate all Settings

□ Overwrite Sessions

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

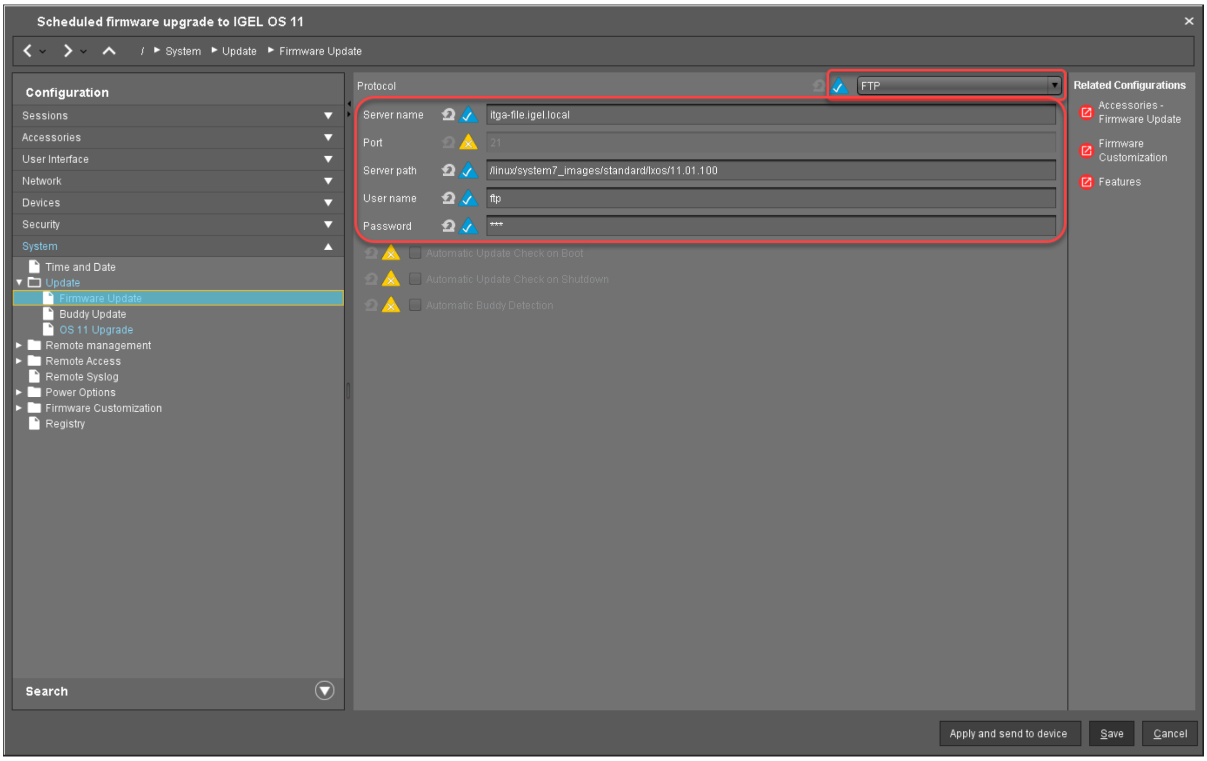
> If you use Universal Firmware Update (see page 163) for OS 11, you do not need to configure the settings described in this step.

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

> 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.



Protocol: FTP

Server name: itga-file.igel.local

Port: 21

Server path: /linux/system7_images/standard/lxos/11.01.100

User name: ftp

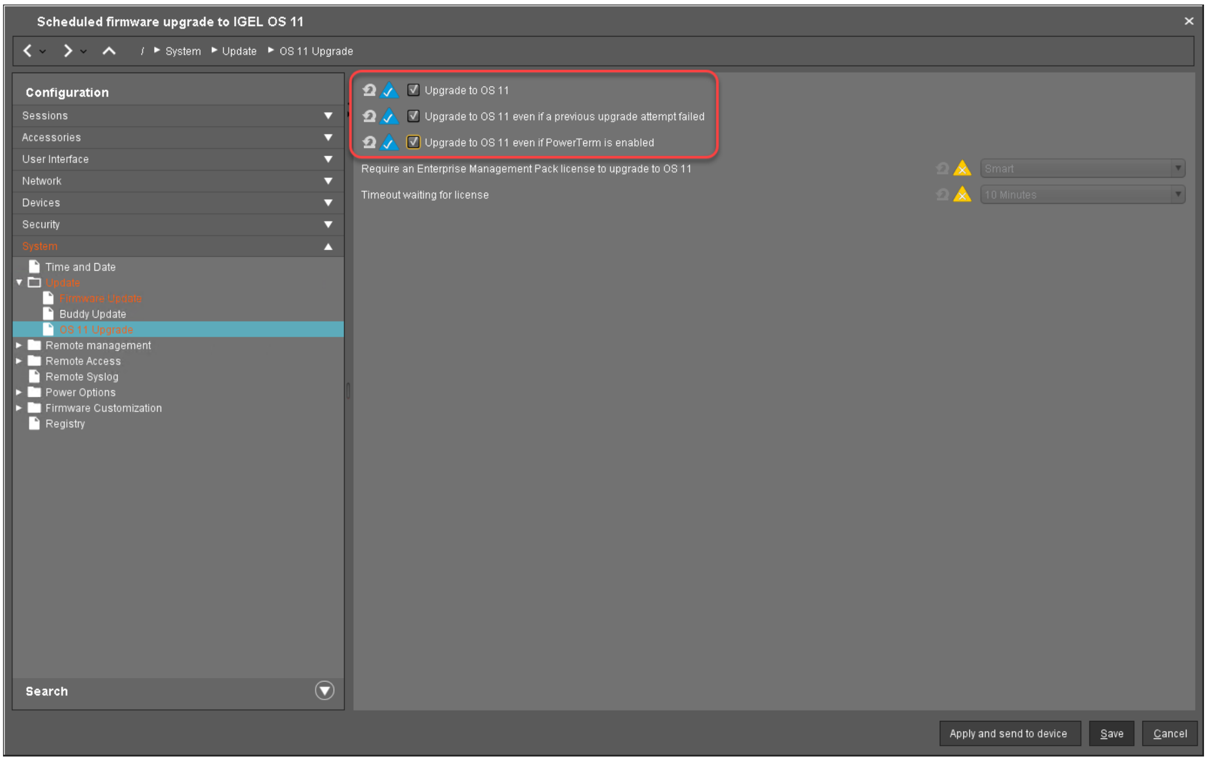
Password: ***

□ Automatic Update Check on Boot

□ Automatic Update Check on Shutdown

□ Automatic Buddy Detection

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 155)):
   - 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**.



Scheduled firmware upgrade to IGEL OS 11

☑ Upgrade to OS 11

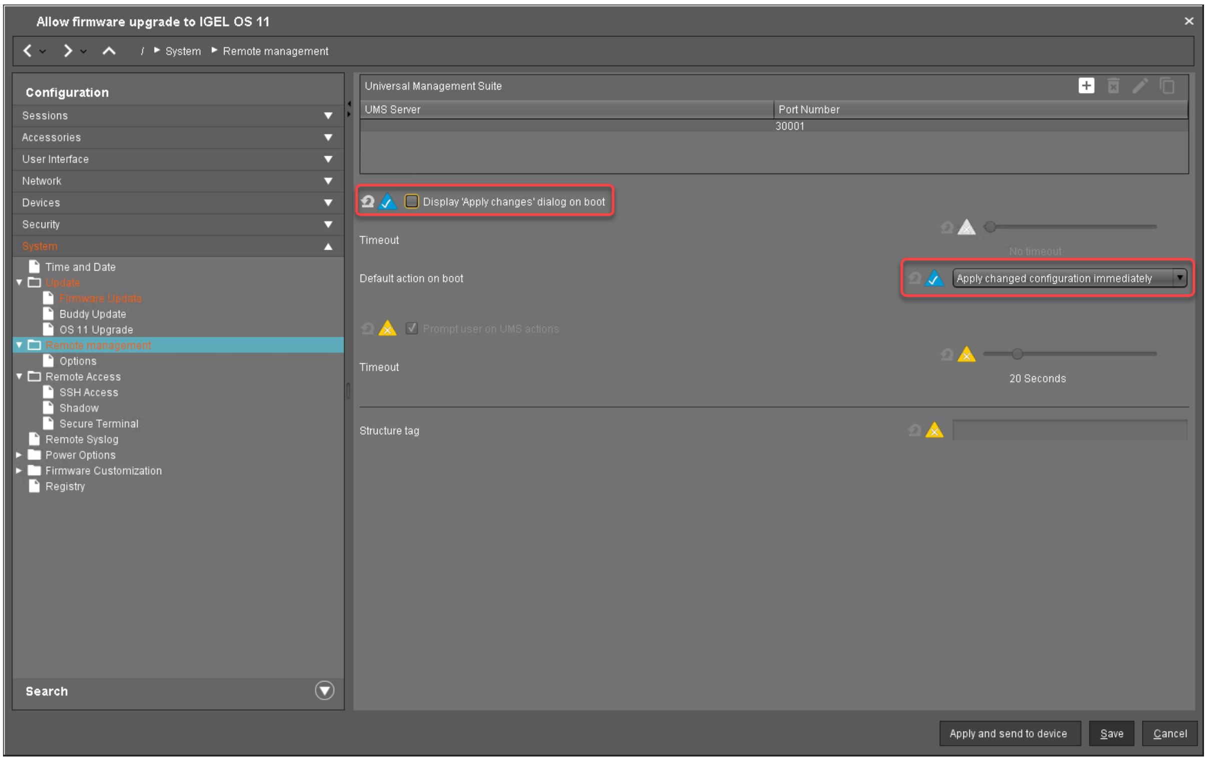
☑ Upgrade to OS 11 even if a previous upgrade attempt failed

☑ Upgrade to OS 11 even if PowerTerm is enabled

Require an Enterprise Management Pack license to upgrade to OS 11: Smart

Timeout waiting for license: 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**.



Universal Management Suite

UMS Server	Port Number
	30001

□ Display 'Apply changes' dialog on boot

Timeout: No timeout

Default action on boot: Apply changed configuration immediately

☑ Prompt user on UMS actions

Timeout: 20 Seconds

Structure tag

5. Click **Save**.

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

Deploying the Licenses

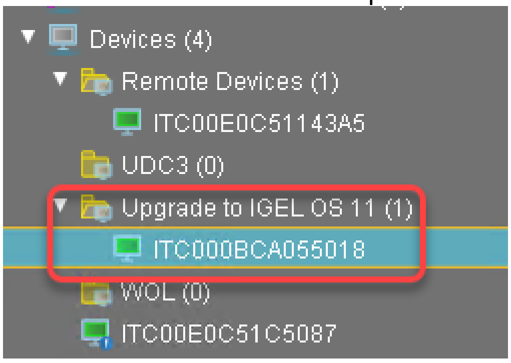
Deploy the licenses for IGEL OS 11 using the method that suits your needs:

- Automatic License Deployment (ALD): Licenses are created and deployed automatically to each device that needs a license. For instructions, see Setting up Automatic License Deployment (ALD).
- Manual License Deployment: Licenses are created and deployed manually. For instructions, see Manual License Deployment for IGEL OS.

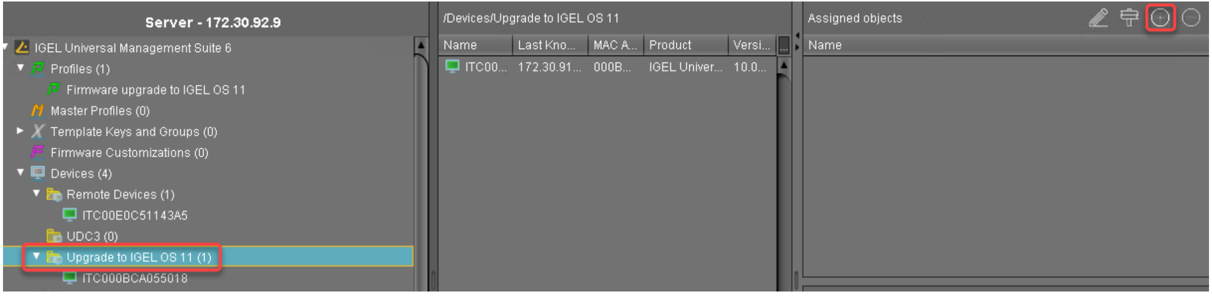
When the license deployment is set up, continue with Assigning the Profile (see page 207).

Assigning the Profile

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

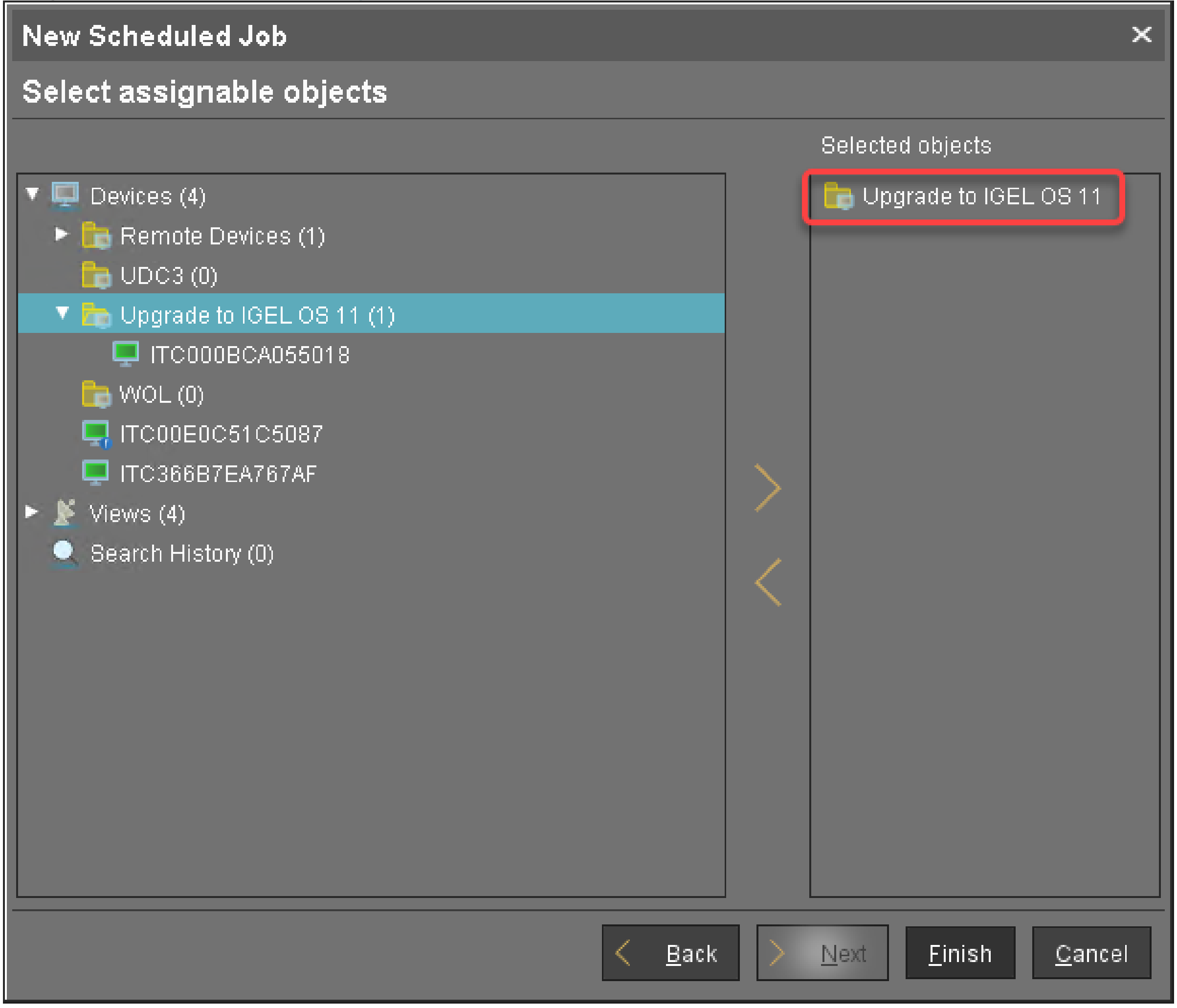


2. Select the directory and in the **Assigned objects** area, click ⊕.


Server - 172.30.92.9
IGEL Universal Management Suite 6
Profiles (1)
Firmware upgrade to IGEL OS 11
Master Profiles (0)
Template Keys and Groups (0)
Firmware Customizations (0)
Devices (4)
Remote Devices (1)
ITC00E0C51143A5
UDC3 (0)
Upgrade to IGEL OS 11 (1)
ITC000BCA055018
/Devices/Upgrade to IGEL OS 11
Assigned objects
Name

Name	Last Kno...	MAC A...	Product	Versi...
ITC00...	172.30.91...	000B...	IGEL Univer...	10.0...

3. Assign the profile (see Creating a Profile (see page 202)) to the directory and click **Ok**.



New Scheduled Job ✕

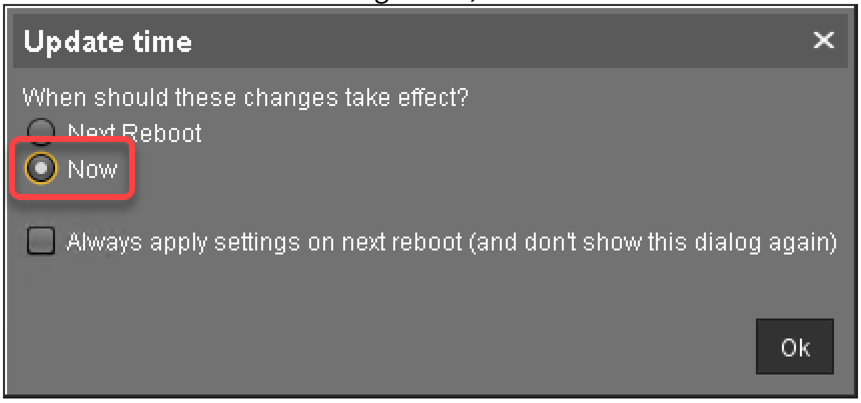
Select assignable objects

- ▼ Devices (4)
  - ▶ Remote Devices (1)
  - UDC3 (0)
  - ▼ Upgrade to IGEL OS 11 (1)
    - ITC000BCA055018
  - WOL (0)
  - ITC00E0C51C5087
  - ITC366B7EA767AF
- ▶ Views (4)
- Search History (0)

Selected objects

- Upgrade to IGEL OS 11

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



Update time ✕

When should these changes take effect?

○ Next Reboot

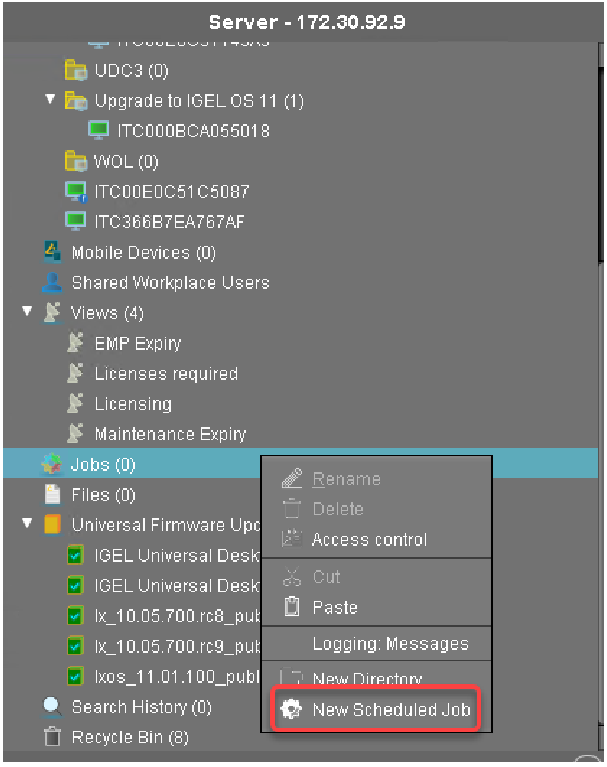
● Now

□ Always apply settings on next reboot (and don't show this dialog again)

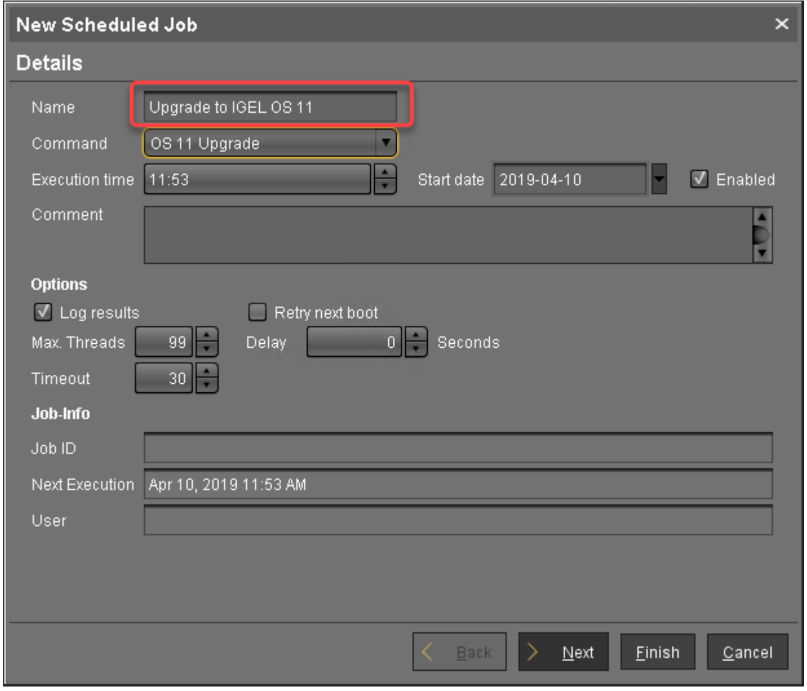
When the profile is assigned, continue with Creating the Scheduled Job (see page 209).

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".


New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:53   Start date: 2019-04-10   ☑ Enabled

Comment:

Options

☑ Log results   □ Retry next boot

Max. Threads: 99   Delay: 0 Seconds

Timeout: 30

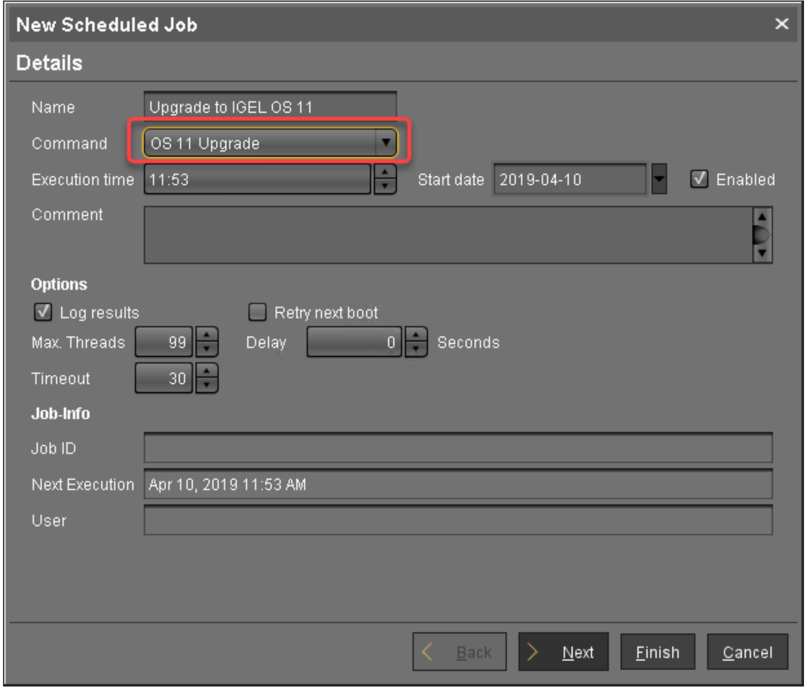
Job-Info

Job ID:

Next Execution: Apr 10, 2019 11:53 AM

User:

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



New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:53 Start date: 2019-04-10 ☑ Enabled

Comment:

Options

☑ Log results □ Retry next boot

Max. Threads: 99 Delay: 0 Seconds

Timeout: 30

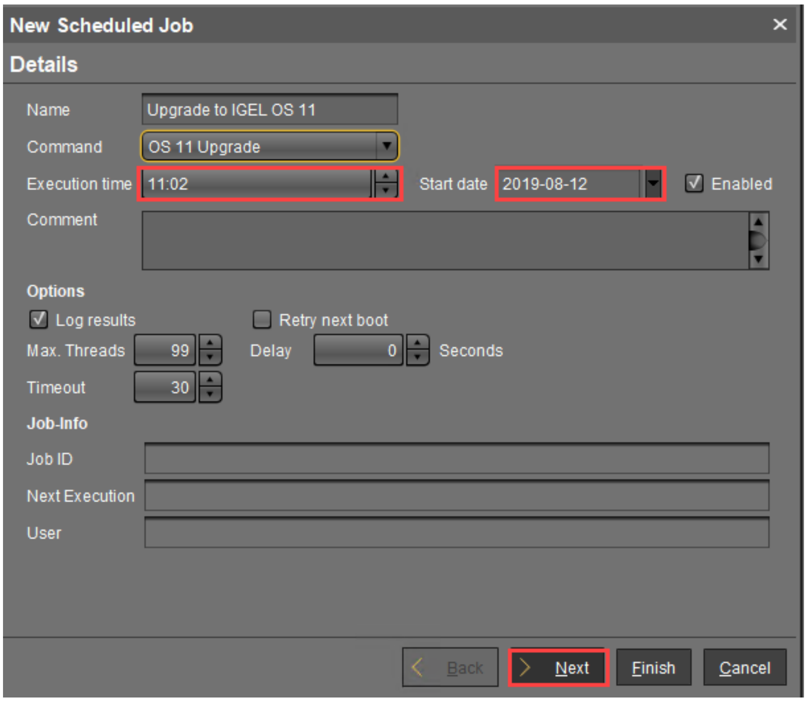
Job-Info

Job ID:

Next Execution: Apr 10, 2019 11:53 AM

User:

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



New Scheduled Job

Details

Name: Upgrade to IGEL OS 11

Command: OS 11 Upgrade

Execution time: 11:02 Start date: 2019-08-12 ☑ Enabled

Comment:

Options

☑ Log results □ Retry next boot

Max. Threads: 99 Delay: 0 Seconds

Timeout: 30

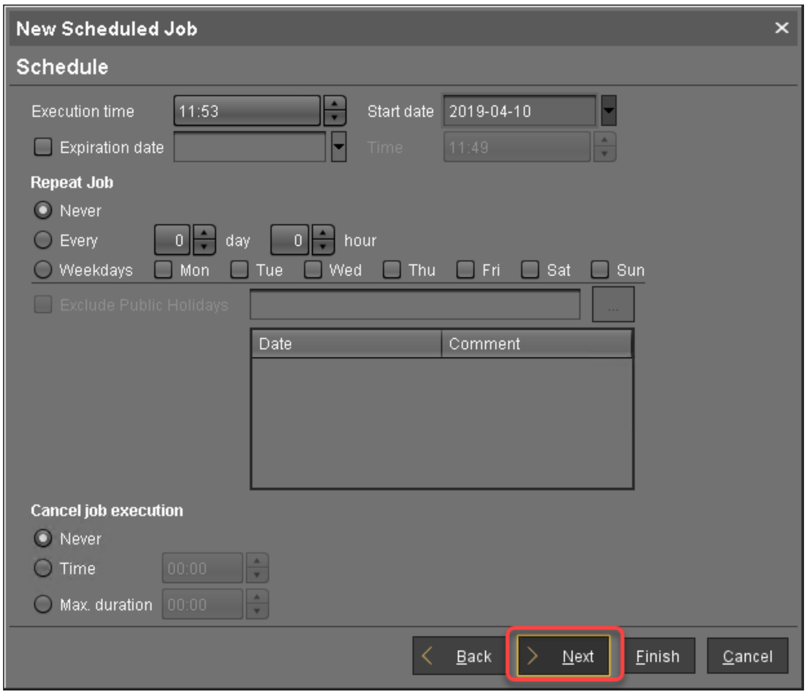
Job-Info

Job ID:

Next Execution:

User:

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



New Scheduled Job

Schedule

Execution time: 11:53

Start date: 2019-04-10

□ Expiration date

Time: 11:49

Repeat Job

● Never

○ Every 0 day 0 hour

○ Weekdays □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

□ Exclude Public Holidays

Date	Comment

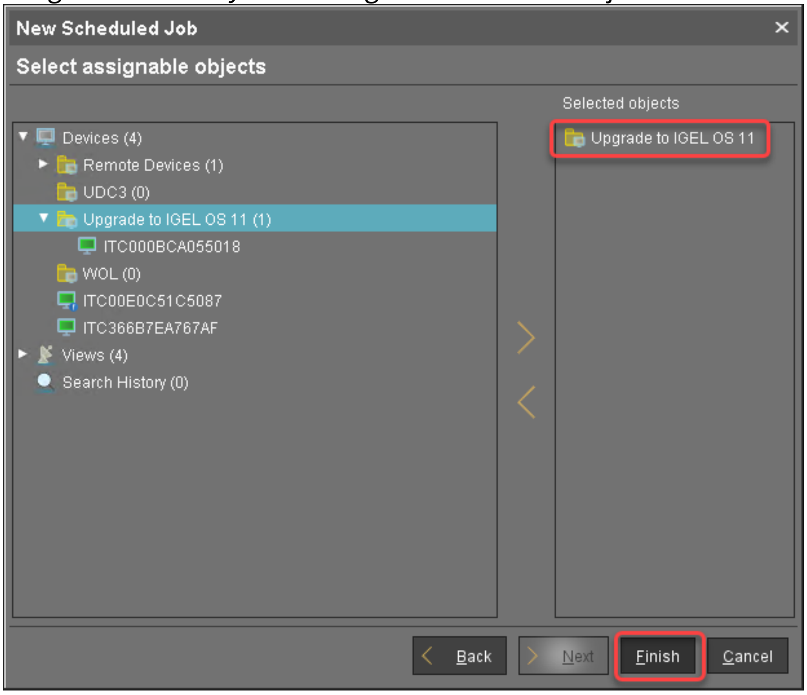
Cancel job execution

● Never

○ Time 00:00

○ Max. duration 00:00

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



New Scheduled Job

Select assignable objects

- Devices (4)
  - Remote Devices (1)
  - UDC3 (0)
  - Upgrade to IGEL OS 11 (1)
    - ITC000BCA055018
  - WOL (0)
  - ITC00E0C51C5087
  - ITC366B7EA767AF
- Views (4)
- Search History (0)

Selected objects

- Upgrade to IGEL OS 11

Troubleshooting

This section describes possible error cases and solutions.

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.

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).

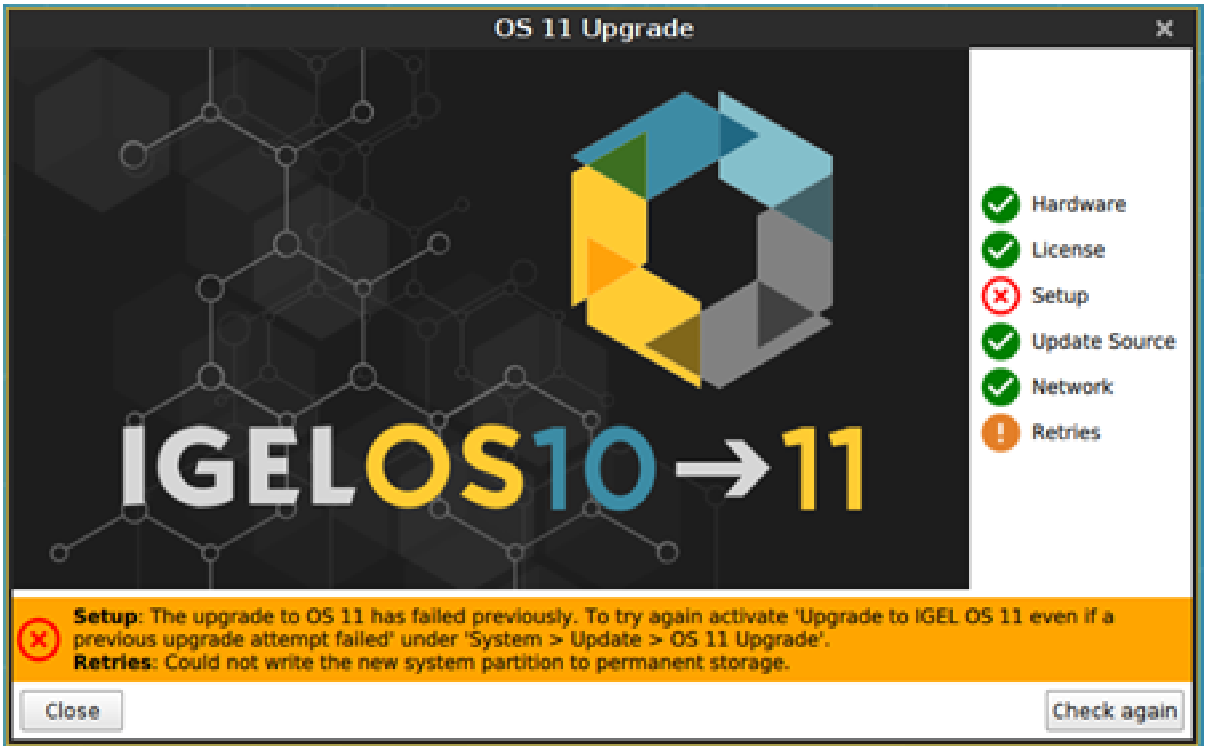
Or:

▶ 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:



Setup: The upgrade to OS 11 has failed previously. To try again activate 'Upgrade to IGEL OS 11 even if a previous upgrade attempt failed' under 'System > Update > OS 11 Upgrade'.
Retries: Could not write the new system partition to permanent storage.

- 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 in the IGEL OS Manual) or save the log files in order to send them to the IGEL Support Team (see the chapter Save Device Files for Support 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

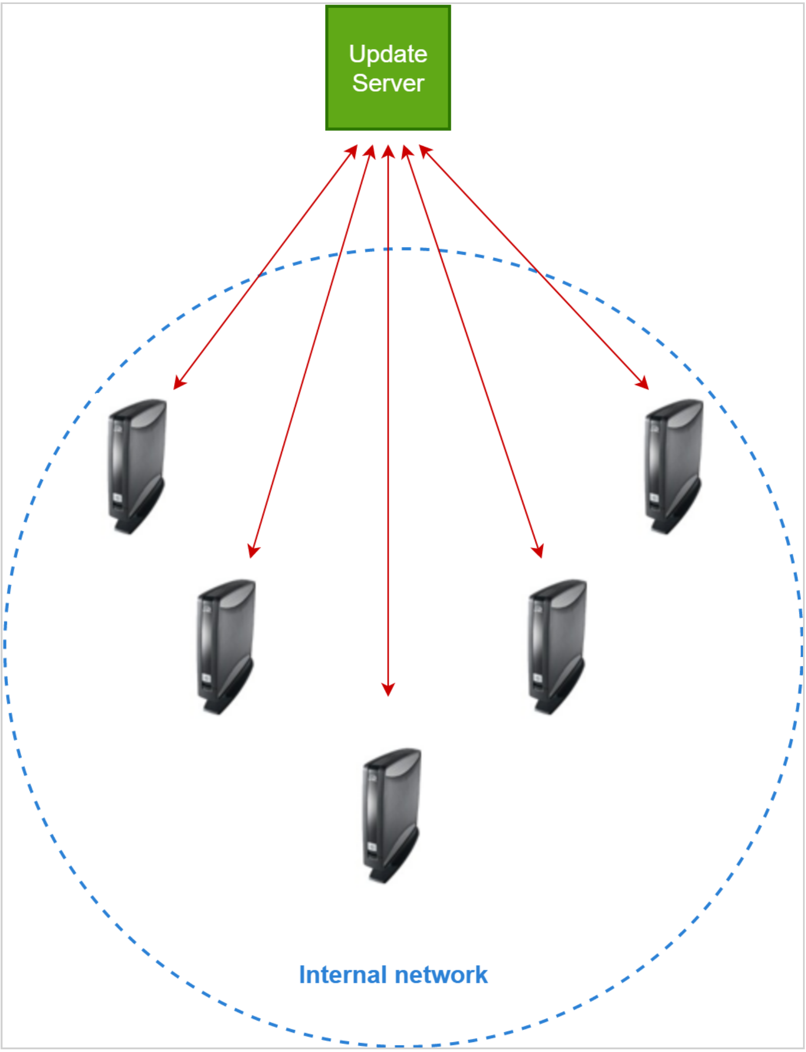
When the **Upgrade to OS 11 even if a previous upgrade attempt failed** option is set and the upgrade has failed each time, the system will stop trying after 5 attempts.

To reset the retry counter:

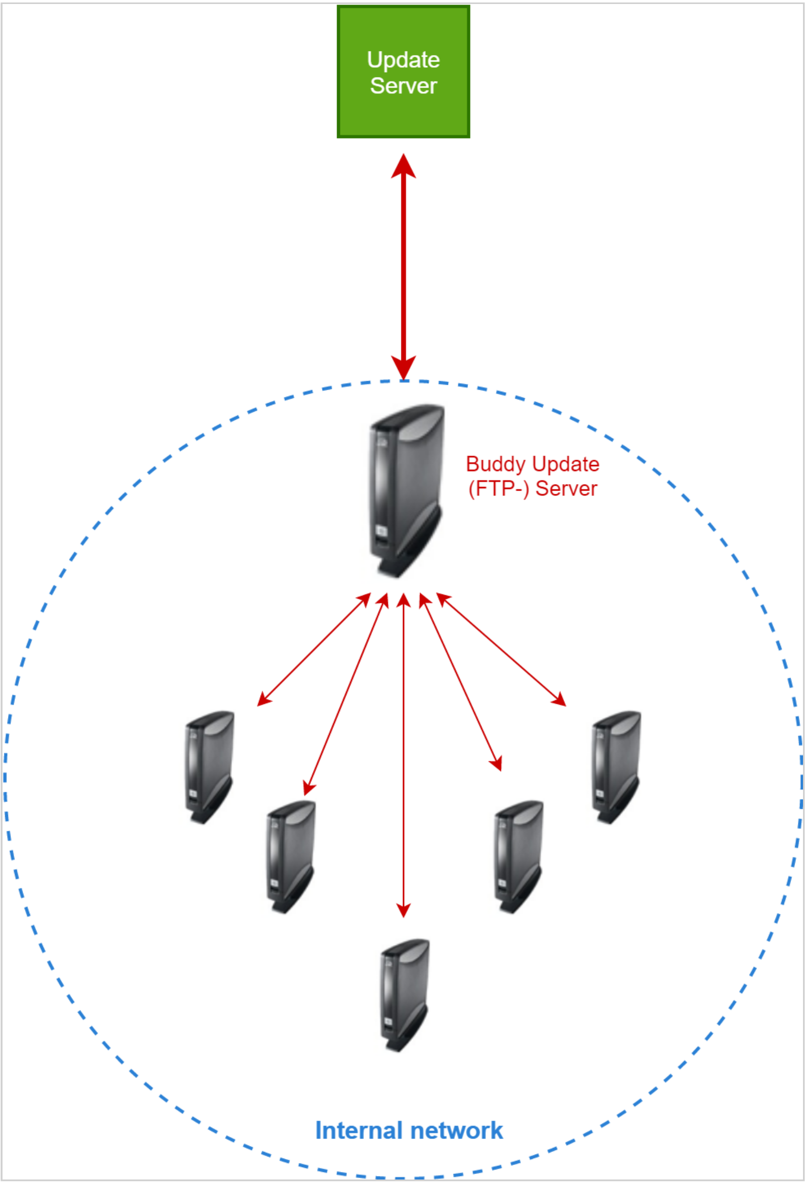
1. In the Setup or the UMS profile, go to **System > Update > OS 11 Upgrade** and deactivate **Upgrade to OS 11 even if a previous upgrade attempt failed**.
2. When the setting is effective on the devices, go to **System > Update > OS 11 Upgrade** again and activate **Upgrade to OS 11 even if a previous 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 220)
- Configuring the Buddy Update Client (see page 221)

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

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 Profiles.

To assign a server to a group:

1. Configure the server as described above (Basic Configuration (see page 220)), 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 221), "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 220), "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 Profiles.

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.

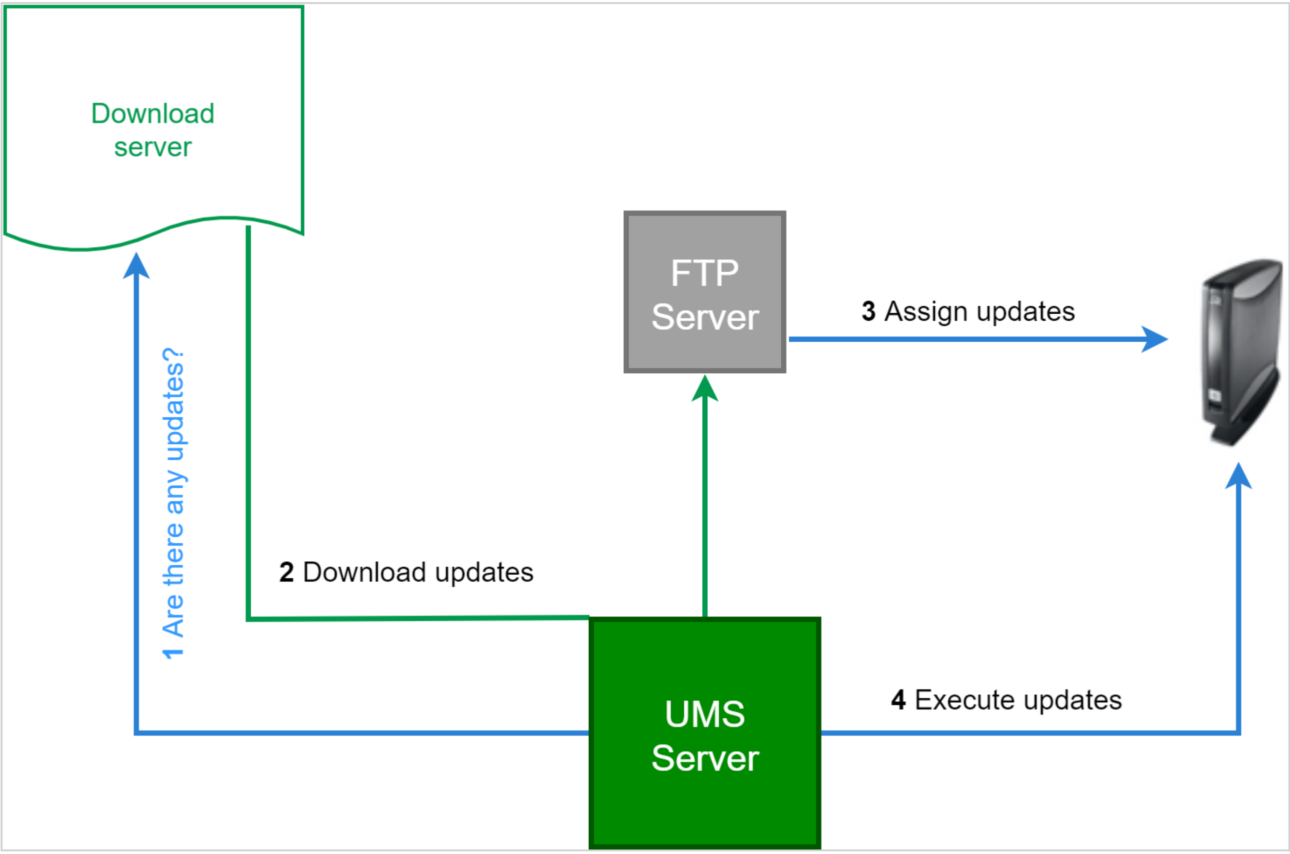
To configure a client for balancing the server load:

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[7] 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 225).



- Downloading Updates and Storing them on an FTP Server (see page 224)
- Executing an Update Process (see page 225)

[7] 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.

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.

Updating the Firmware using a USB Storage Device

You can use a USB storage device to update the firmware 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. Proceed as follows:

1. Download the update file (.zip) for your device from the IGEL download server[8].
2. Unpack the update files and save them to a USB storage device.

   ⓘ You can find the officially supported file systems under Storage Hotplug.

3. In the local setup application 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 informations in the chapter Storage Hotplug.

8. Connect the USB storage device to the thin client 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 file system` / `udlx.inf` and click **Open**.
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.

To update the device's firmware without having access to the local setup, follow FAQ Updating the Firmware using the Linux Console (see page 227).

[8] 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: "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.

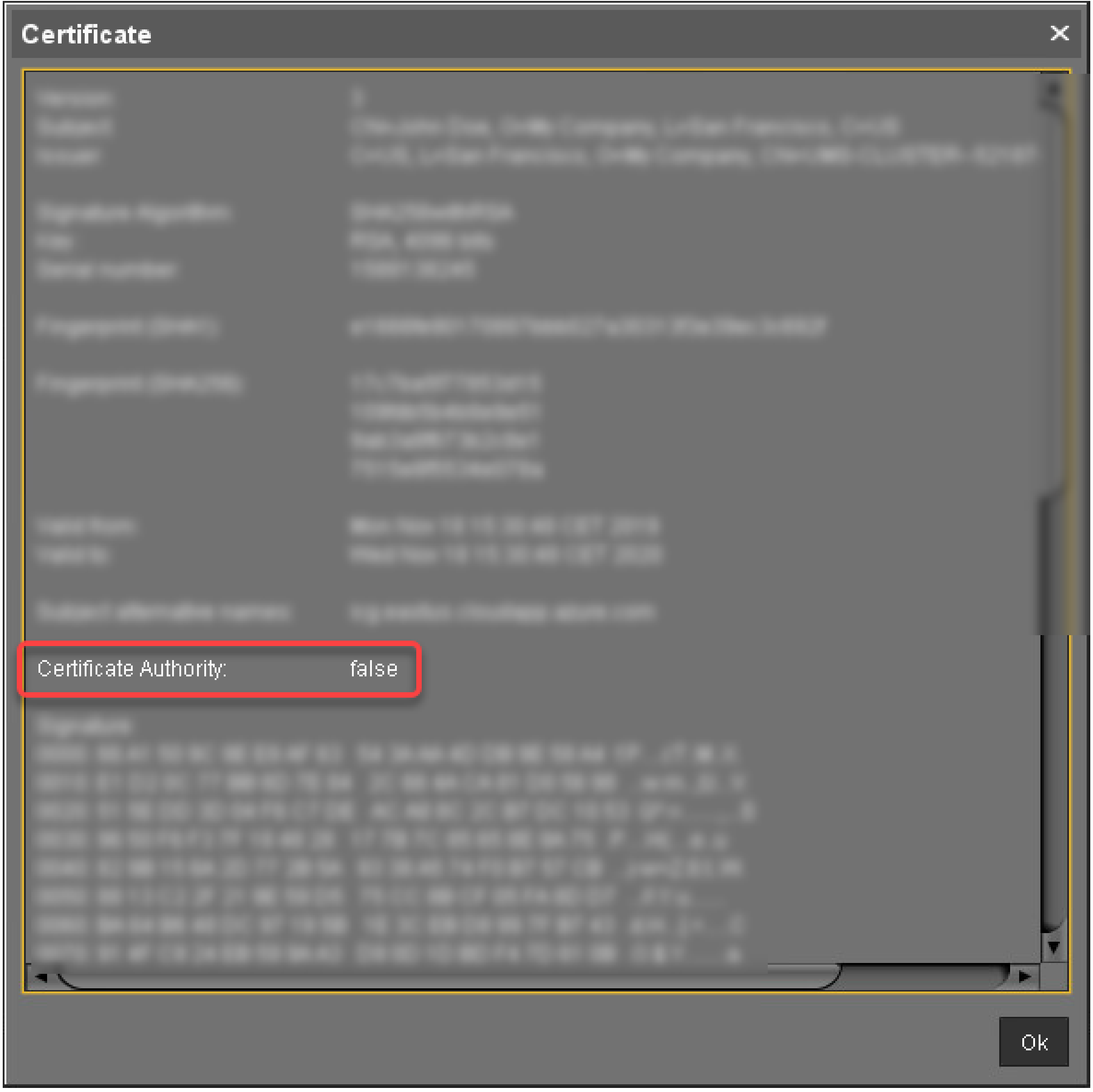
Environment

- 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 Solution (see page 231).



Certificate

Certificate Authority: false

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 Exchanging the Root Certificate for ICG.
5. Update your devices to IGEL OS 11.04.240 or higher.

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

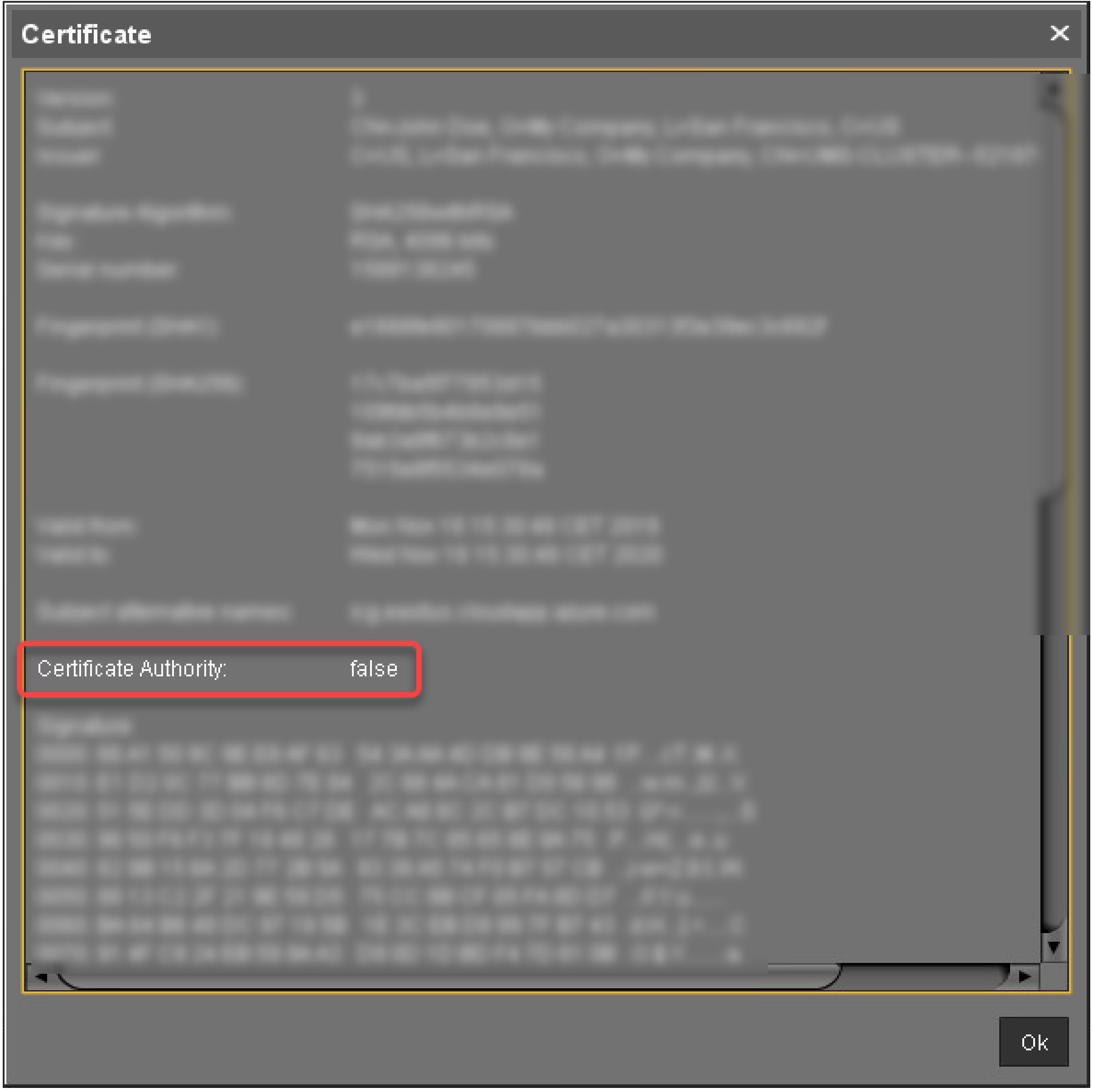
Problem/Possible Cause

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 233).



Certificate Authority: false

Solution

1. ReInstall the ICG using an appropriate root certificate. For details, see the following articles:
   - Providing the Certificates
   - Installing the IGEL Cloud Gateway
2. Register the devices again. For details, see Connecting the Devices.

Citrix

Performance

Citrix Performance Enhancements

Symptom

Citrix users have performance issues (bad user experience).

Problem

IMPORTANT: There is a big difference between locally defined ICA sessions on one hand, and *Program Neighborhood* or Webinterface sessions on the other in terms of configuration:

- Locally defined ICA sessions are configured in the Thin Client Setup or *IGEL Universal Management Suite* (UMS), either with the configuration pages or in the registry.
- *Program Neighborhood* sessions are configured on the server side, by editing the file `default.ica` (create a backup first!) that is located in the folder `c:\inetpub\wwwroot\Citrix\PNAgent\conf` (if you did not use the default settings during *Cirix Webinterface* installation, the path may vary).
- Webinterface sessions (which are started via browser or in Appliance Mode) are similar to *Program Neighborhood* sessions, but the file `default.ica` is located in `c:\inetpub\wwwroot\Citrix\XenApp\conf` (default path).

Solution

Reducing network load:

- Compression:
  Enabling the parameter **Compression** lowers used network bandwidth at the cost of increased cpu load.
  - ICA sessions: Go to **Citrix > Citrix Legacy ICA Sessions > ICA Session > Options**, parameter **Compression**
  - PN/Webinterface: Add **Compress** in the section **[Application]**, values: **On/Off**
- Persistent Cache:
  Setting the parameter **Persistent cache** has the potential to greatly reduce network load in later sessions when using the same applications.
  - ICA sessions: Go to **Citrix > Citrix Legacy ICA Sessions > ICA Session > Options**, parameter **Persistent Cache**
  - PN/Webinterface: Add **PersistentCacheEnabled** in the section **[Application]** , values: **On/Off**

  Please note that the persistent cache is located in the system's RAM by default - meaning it will survive a suspend, but not a reboot or shutdown. If you want it to be truly persistent (may lower lifetime of the system's flash module) you have to create a custom partition and set the parameter **PersistentCachePath** accordingly.

- ICA sessions: Go to **Citrix > Citrix Global > Options** , parameter **Persistent cache path**
- PN/Webinterface: Add **PersistentCachePath** in the section **[Thinwire3.0]**, value: **File system path**

The size of the cache can be controlled with the parameter **Cache Size**.

- ICA sessions: Go to **Citrix > Citrix Global > Options**, parameter **Cache size in kB**
- PN/Webinterface: Add **PersistentCacheSize** in the section **[Thinwire3.0]**, value: **Cache size** (kB)

The minimum size of a bitmap to be cached can be controlled using the parameter **Minimum Bitmap Size**.

- ICA sessions: Go to **Citrix > Citrix Global > Options**, parameter **Minimum bitmap size in bytes**
- PN/Webinterface: Add **PersistentCacheMinBitmap** in the section **[Thinwire3.0].** value: **Minimum bitmap size** (Byte)

- Audio Bandwidth:
  Adjusting the parameter **Audio bandwidth limit** directly affects network load for published applications with much audio output.
  - ICA sessions: Go to **Citrix > Citrix Legacy ICA Sessions > ICA Session > Options**, parameter **Audio bandwidth limit**
  - PN/Webinterface: Add **AudioBandwidthLimit** in the section **[Application]**, values: **0/1/2** for High/Medium/Low
- MouseTimer/Keyboard Timer:
  The parameters **MouseTimer** and **KeyboardTimer** reduce the number of network packets by gathering several mouse/keyboard events and putting them together into one network packet. For the mouse, in older versions of IGEL Linux the default value was 100 (milliseconds), but this lead to strange behavior in some applications. Now the default value is 0 (for mouse and keyboard). It is not recommended to change this value for the keyboard, but if you have problems with your network load and want to reduce the number of network packets, you could try a higher value like 100 or even more for the mouse.
  - Locally defined ICA sessions:
    Registry path **ica.wfclient.mousetimer** (globally for all ICA sessions) or **sessions.icaN.appsrv.mousetimer** (for single session N), value: **Time** (milliseconds) to gather events
    Registry **path ica.wfclient.keyboardtimer** (globally for all ICA sessions) or **sessions.icaN.appsrv.keyboardtimer** (for single session N), value: **Time** (milliseconds) to gather events
  - PN/Webinterface: Add **MouseTimer** or **KeyboardTimer** in the section **[Application]**, value: **Time** (milliseconds) to gather events

Improving performance/user experience:

- Speedscreen Latency Reduction:
  The parameters **Mouse Click Feedback** and **Local Text Echo** could improve the user experience for high latency network connections. **Mouse Click Feedback** shows a busy cursor when the user presses a mouse button to give him an immediate visual feedback and prevent him from clicking

again. **Local Text Echo** lets the client pre-render the characters the user types to give the impression of a smooth text input.

  - ICA sessions: Go to **Citrix > Citrix Legacy ICA Sessions > ICA Session > Options,** parameter **Mouse click feedback** or **Local text echo**
  - PN/Webinterface: Add **ZLMouseMode** or **ZLKeyboardMode** in the section **[Application]**, values: **0/1/2** for Off/On/Automatic

- Deferred screen update mode:
  The parameter **Deferred screen update mode** defers graphical updates to the screen so that several updates are done in one batch operation. This speeds up the updates especially on slow machines with a poor refresh rate. The effect is very noticeable when the screen contents refreshes rapidly, e.g. during scrolling.
  - ICA sessions: Go to **Citrix > Citrix Global > Options**, parameter **Deferred screen update mode**
  - PN/Webinterface: Add **DeferredUpdateMode** in the section **[WFClient]**, values: **True/False**

> Caution: Deactivating this parameter is not recommended. When it is disabled it is not guaranteed that the write process has finished when the software indicates it. Some data might still reside in the write buffer. If the user disconnects the USB device too early, the written data might not be complete and the data file(s) may be corrupt. Some USB devices have an LED that blinks when data is written. When it stops blinking, the write process should be completed, but it is not guaranteed.

  - Go to IGEL registry **devices.autofs.sync_option**
  - Deactivate the parameter **sync_option**

Poor Performance: Black Blocks and Stripes in Citrix Sessions

Symptom

In the Citrix session, you sometimes experience a problem with black blocks, frames, or stripes.

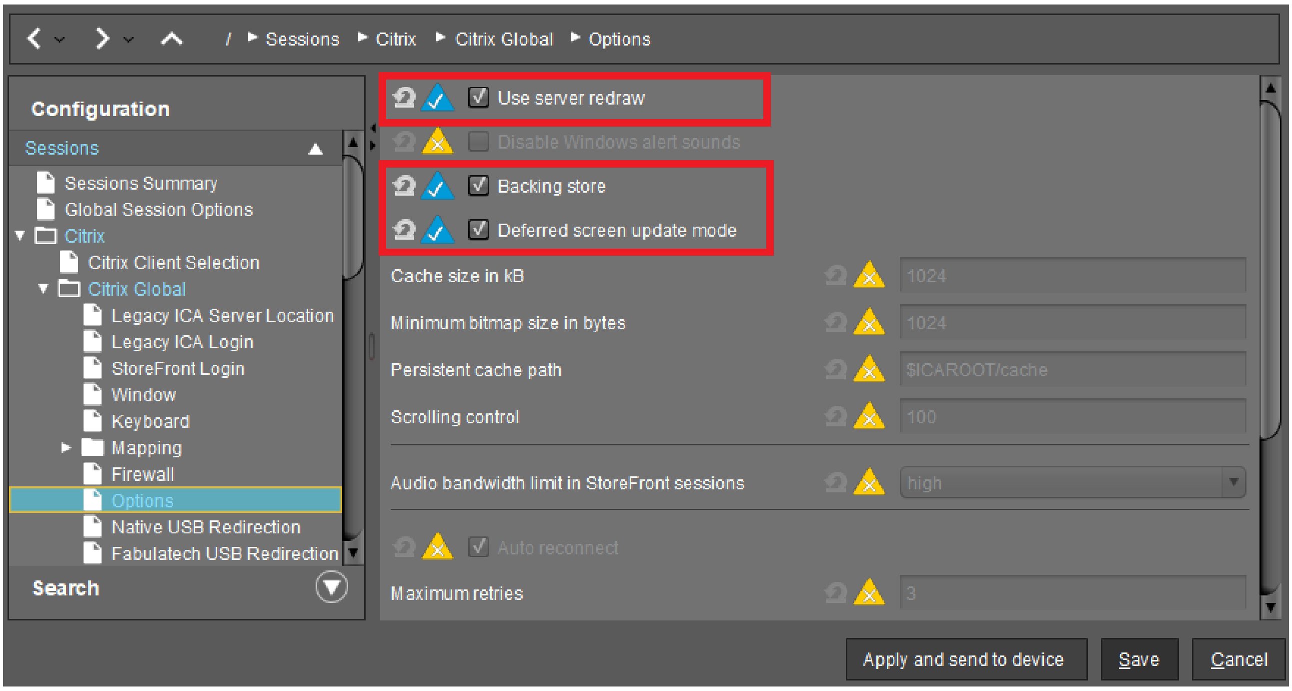
Problem

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**



☑ Use server redraw

□ Disable Windows alert sounds

☑ Backing store

☑ Deferred screen update mode

Cache size in kB: 1024

Minimum bitmap size in bytes: 1024

Persistent cache path: $ICAROOT/cache

Scrolling control: 100

Audio bandwidth limit in StoreFront sessions: high

☑ Auto reconnect

Maximum retries: 3

See also Options in the manual chapter for Citrix.

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.

Citrix: Deep Compression Flickers

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, the Windows start menu button flickers.

Problem

Known issue on the server side.

Solution

Enable the legacy graphics mode on the XenDesktop 7.6 server via a policy.

Citrix Receiver: Grey Blocks in Excel 2013

Symptom

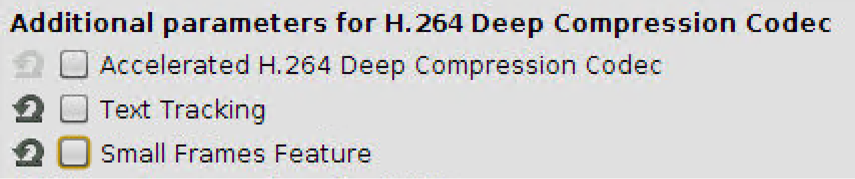
When using Microsoft Excel 2013 on XenDesktop 7.6 with Citrix Receiver 13.1.3, 13.1.4 or 13.2, grey blocks appear especially if you mark multiple cells.

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**.



Additional parameters for H.264 Deep Compression Codec

□ Accelerated H.264 Deep Compression Codec

□ Text Tracking

□ Small Frames Feature

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.

Citrix Webinterface 5.x Delay on First Page

Symptom

When opening the Citrix Webinterface in IGEL Linux Appliance Mode you only see an empty page.

Problem

The Webinterface is slow.

Solution:

See the following Citrix Support Knowledge Center entry: http://support.citrix.com/article/CTX117273

Slow Performance of Citrix Session in a Cloud Environment

Symptom

Your cloud-based Citrix session is very slow.

Environment

- IGEL OS 10.05 or higher, up to IGEL OS 11.05 (with IGEL OS 11.06 or higher, the default setting has changed)
- Citrix client is connected to a cloud server. NOT affected: On-premises and Netscaler environments

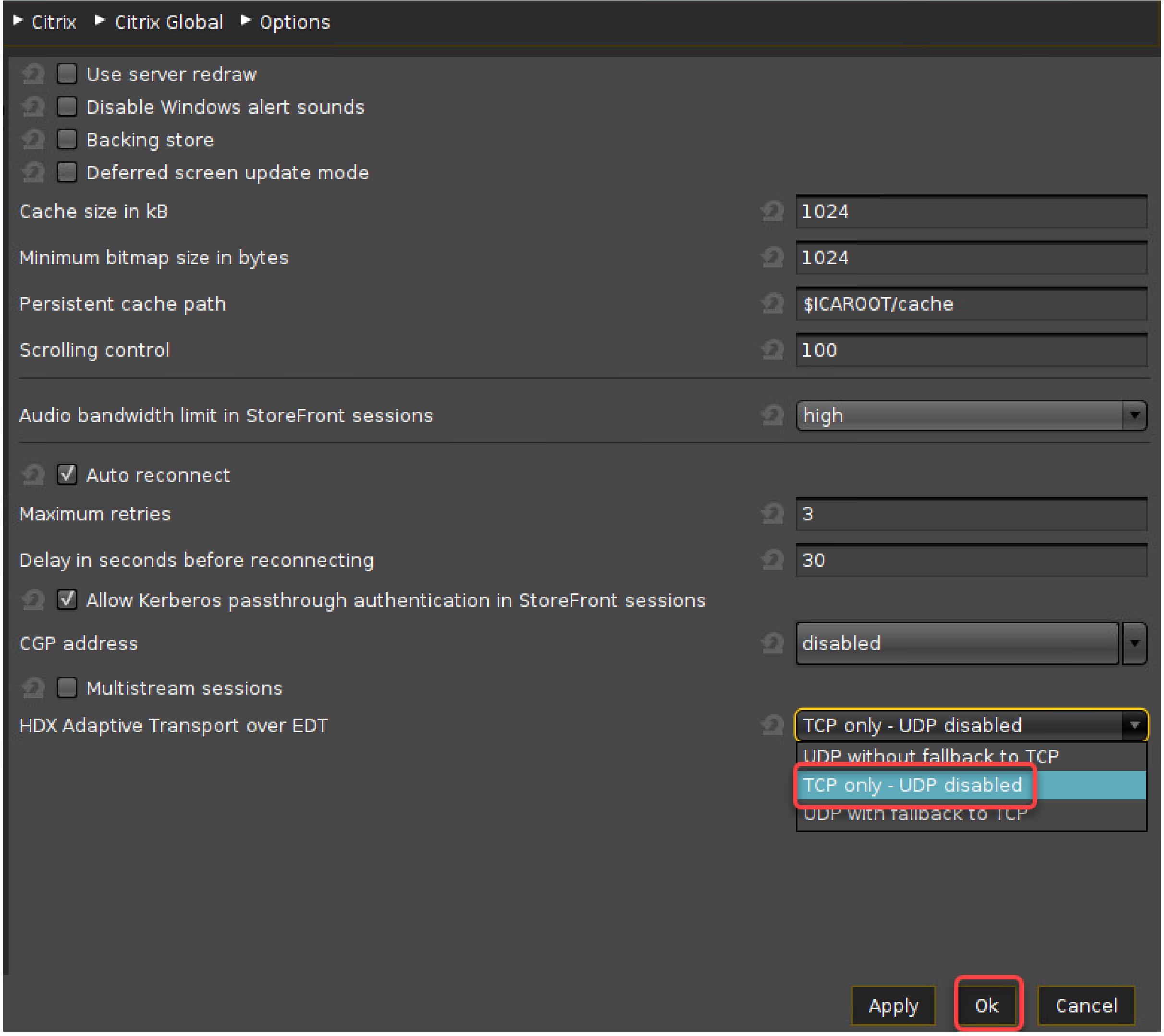
Problem

The HDX transport protocol is set to "UDP with fallback to TCP", which causes slow performance.

Solution

1. Open the UMS configuration dialog or the local Setup and go to **Citrix > Citrix Global > Options**.

2. Set **HDX Adaptive Transport over EFT** to"TCP only UDP disabled" and click **Apply** or **Ok**.



▶ Citrix ▶ Citrix Global ▶ Options

□ Use server redraw
□ Disable Windows alert sounds
□ Backing store
□ Deferred screen update mode

Cache size in kB: 1024
Minimum bitmap size in bytes: 1024
Persistent cache path: $ICAROOT/cache
Scrolling control: 100

Audio bandwidth limit in StoreFront sessions: high

☑ Auto reconnect
Maximum retries: 3
Delay in seconds before reconnecting: 30
☑ Allow Kerberos passthrough authentication in StoreFront sessions
CGP address: disabled
□ Multistream sessions
HDX Adaptive Transport over EDT: TCP only - UDP disabled

When the Citrix client is started again, the performance should be better.

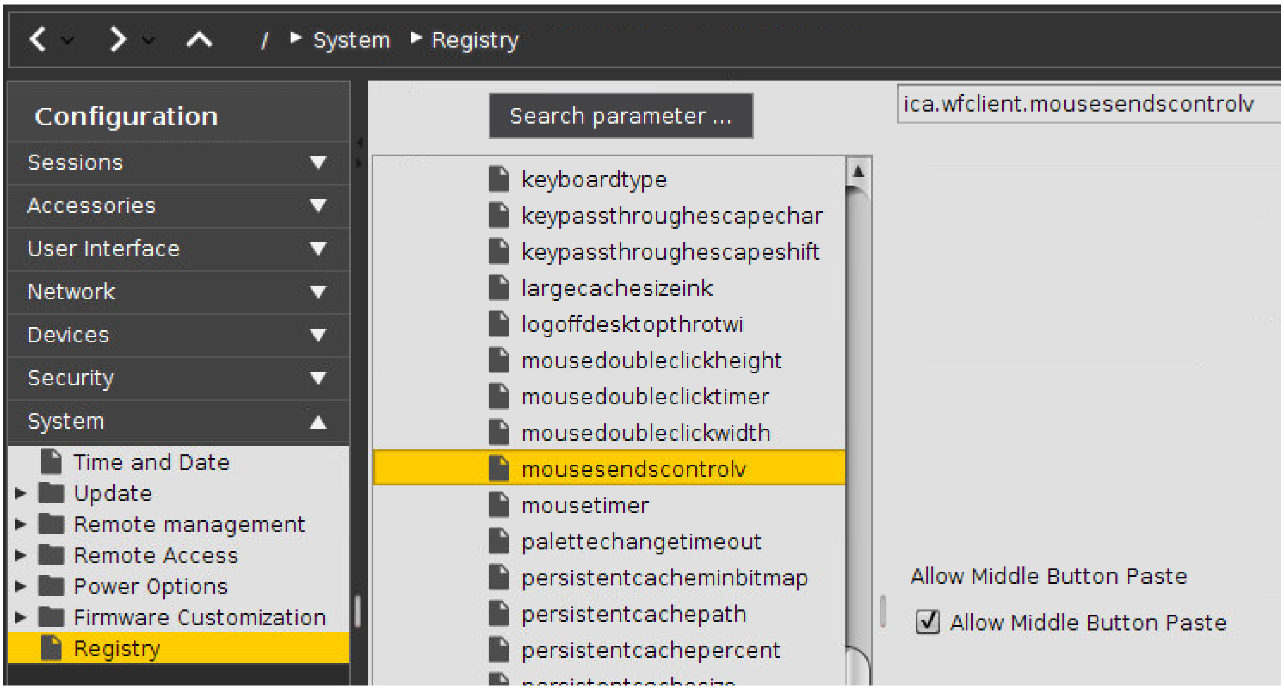
Mouse

Changing 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* browser.

The default function of the middle mouse button is *copy and paste*.

▶ Open IGEL registry in local client setup or UMS.



ica.wfclient.mousesendscontrolv

Allow Middle Button Paste

☑ Allow Middle Button Paste

▶ For Citrix sessions change:

- **System > Registry > ica.wfclient.mousesendscontrolv**
- **System > Registry > sessions.ica%.appsrv.mousesendscontrolv**

▶ For local Firefox browser change:

- **System > Registry > browserglobal.app.middlemouse_contentloadurl**
- **System > Registry > browserglobal.app.middlemouse_paste**

More information on the Firefox parameters can be found at

http://kb.mozillazine.org/Middlemouse.contentLoadURL

http://kb.mozillazine.org/Middlemouse.paste

The changes will take effect after rebooting the thin client.

How to Connect a SpaceMouse with a Citrix Session

This article describes how to use a 3Dconnexion SpaceMouse in a Citrix session.

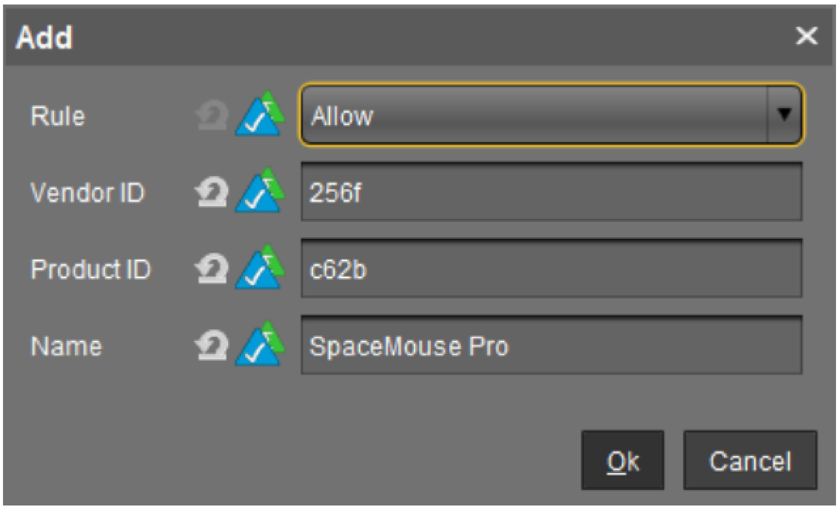
Always use a SpaceMouse only as an additional, i.e. second, mouse.

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


Add

Rule: Allow

Vendor ID: 256f

Product ID: c62b

Name: SpaceMouse Pro

5. Save the settings.

Now, the SpaceMouse is ready for use.

⚠ 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 Solve SpaceMouse USB Reset Problem (see page 252).

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 250).

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.

Black Box Next to the Mouse Cursor

Symptom

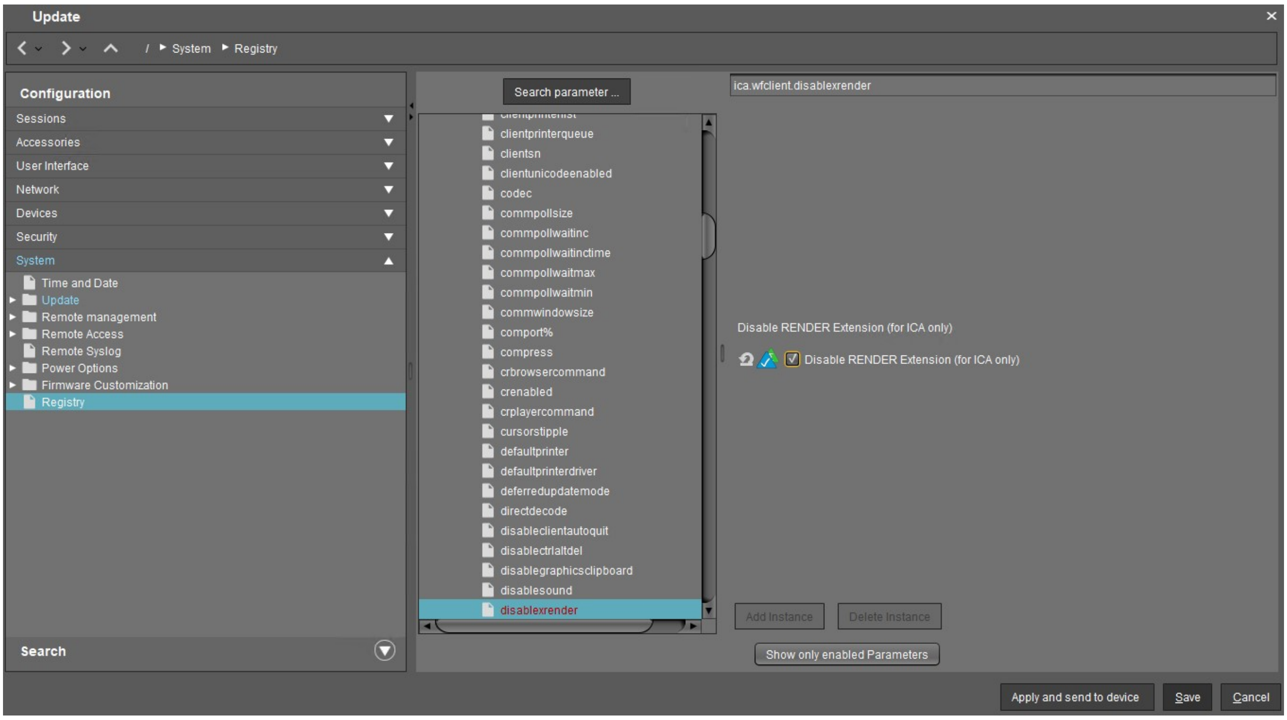
With certain programs (Adobe Reader, Visual Studio, ...) a black box is always displayed next to the cursor in XenDesktop VMs.

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:**



ica.wfclient.disablexrender

Disable RENDER Extension (for ICA only)

☑ Disable RENDER Extension (for ICA only)

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[9]
- Generic USB redirection and client drive considerations[10]

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

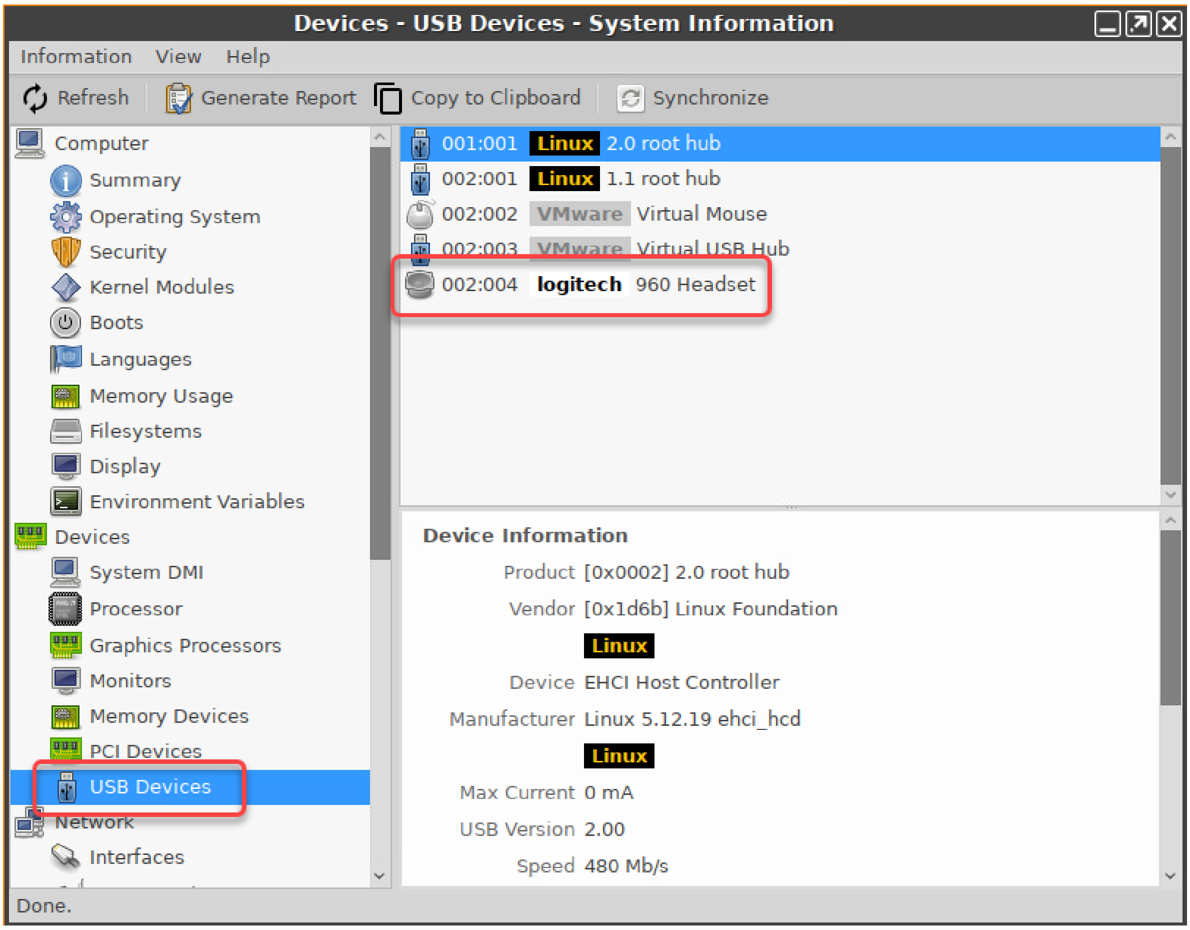
In addition to the server policies, the USB redirection must also be activated at the client:

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.
> System Information example:

[9] https://support.citrix.com/article/CTX137939
[10] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/general-content-redirection/usb.html



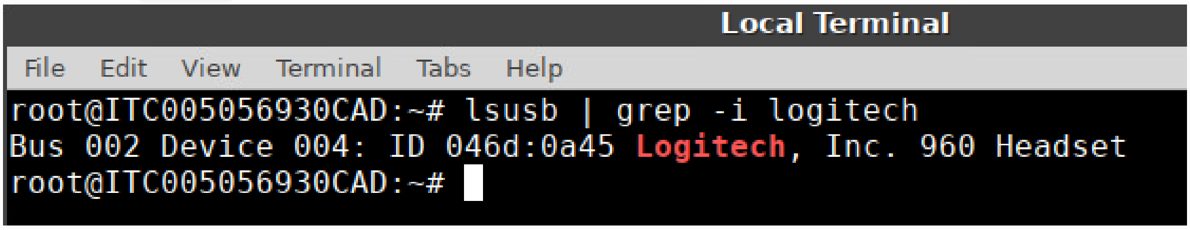
001:001 Linux 2.0 root hub
002:001 Linux 1.1 root hub
002:002 VMware Virtual Mouse
002:003 VMware Virtual USB Hub
002:004 logitech 960 Headset

Device Information

Product [0x0002] 2.0 root hub
Vendor [0x1d6b] Linux Foundation
Linux
Device EHCI Host Controller
Manufacturer Linux 5.12.19 ehci_hcd
Linux
Max Current 0 mA
USB Version 2.00
Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



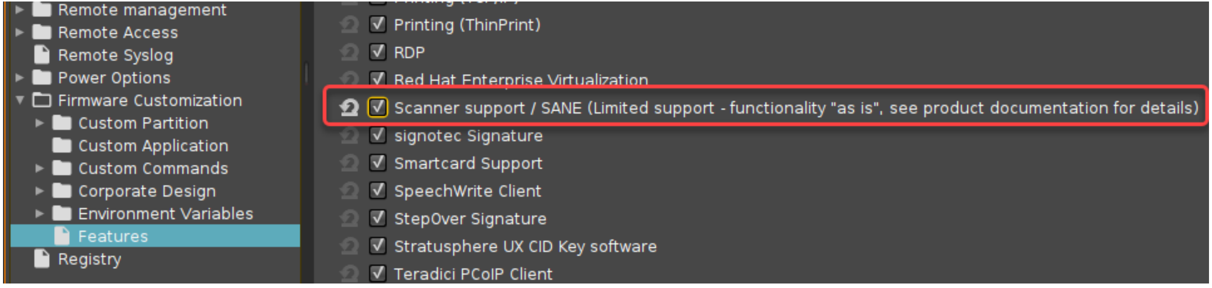
```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

For a device exception rule, use the SpaceMouse Guide (see page 250).
For more information about USB redirection rules, see Native USB Redirection and the documentation of the respective Citrix Workspace app.

Citrix Fabulatech Scanner Redirection

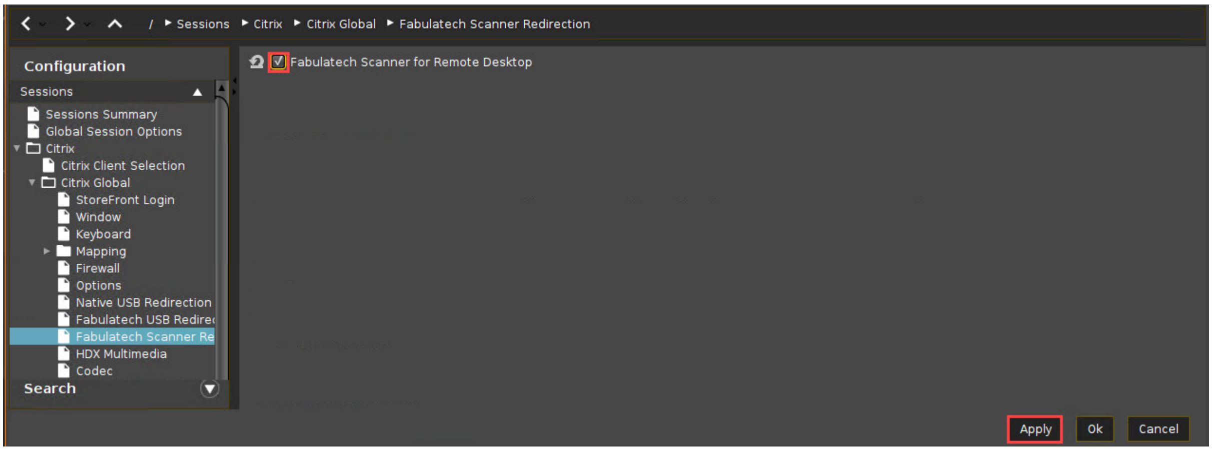
Enabling Fabulatech Scanner Redirection

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.



☑ Printing (ThinPrint)
☑ RDP
☑ Red Hat Enterprise Virtualization
☑ Scanner support / SANE (Limited support - functionality "as is", see product documentation for details)
☑ signotec Signature
☑ Smartcard Support
☑ SpeechWrite Client
☑ StepOver Signature
☑ Stratusphere UX CID Key software
☑ Teradici PCoIP Client

   - 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.
   - 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**.



☑ Fabulatech Scanner for Remote Desktop

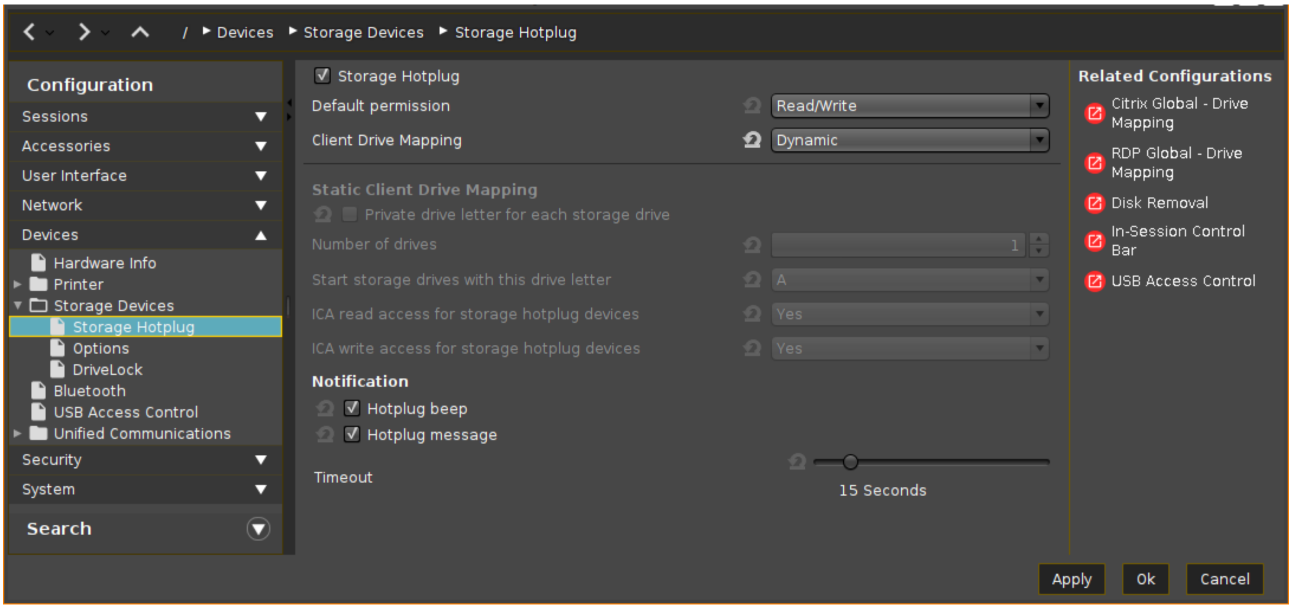
4. Click **Apply** or **Ok** to confirm the settings.

Mapping 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 874).

Basic Configuration of the Client



☑ Storage Hotplug

Default permission: Read/Write

Client Drive Mapping: Dynamic

Static Client Drive Mapping

□ Private drive letter for each storage drive

Number of drives: 1

Start storage drives with this drive letter: A

ICA read access for storage hotplug devices: Yes

ICA write access for storage hotplug devices: Yes

Notification

☑ Hotplug beep

☑ Hotplug message

Timeout: 15 Seconds

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**, the **Disk Removal** 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

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.

Changing Appliance Mode Picture

The following shows you how to change the Appliance Mode appearance: pictures (*XenDesktop* and *Horizon View* appliances), picture style (*XenDesktop* appliances), and desktop background color (*XenDesktop* appliances).

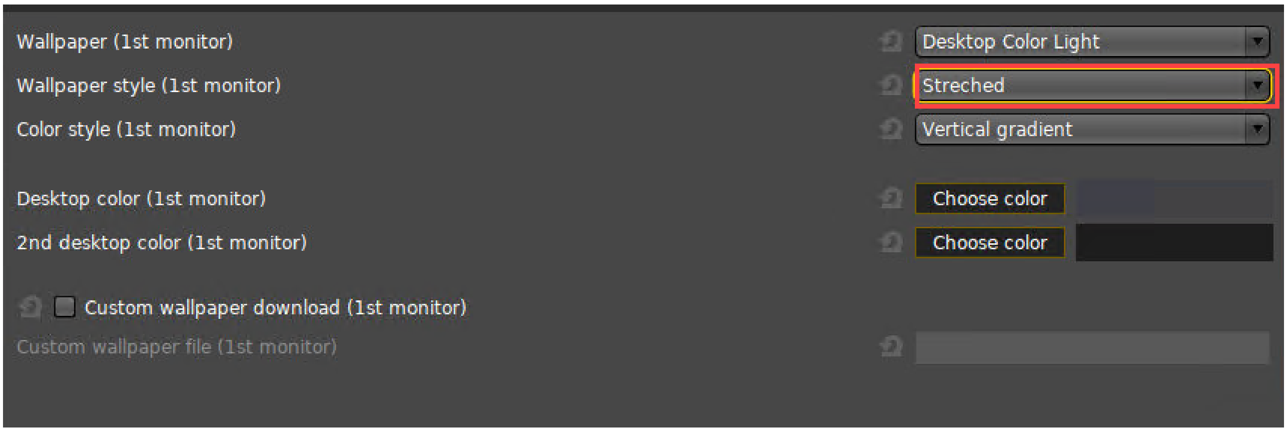
Pictures:

The pictures can be changed via **Custom Command** or **UMS File Transfer**.

- *XenDesktop* Appliance Mode uses following pictures located in `/services/xen/share/pixmaps` (depending on **User Interface > Language** setting; "en_US" is used if there is no png for selected language):
  - Standard **Ctrl-Alt-Del** dialogue picture:
    `ctrlaltdel_en_US.png`
    `ctrlaltdel_de_DE.png`
    `ctrlaltdel_zh_CN.png`
    `ctrlaltdel_zh_HK.png`
  - Smartcard setting if registry key **xen.xenapp-morph.smartcard_enable** is enabled:
    `smartcard_en_US.png`
    `smartcard_de_DE.png`
  - Error message if server is unreachable:
    `serverunreach_en_US.png`
    `serverunreach_de_DE.png`
    `serverunreach_zh_CN.png`
    `serverunreach_zh_HK.png`
- *Horizon View* Appliance Mode picture: `/usr/share/pixmaps/vmware-view-bg.png`

Picture Style:

For *XenDesktop* Appliance Mode, the style of the dialog pictures can be adapted to the wallpaper style of the first monitor. The wallpaper style of the first monitor can be configured under **User Interface > Desktop > Background (1st Monitor) >** selection list **Wallpaper style**.



Wallpaper (1st monitor): Desktop Color Light

Wallpaper style (1st monitor): Streched

Color style (1st monitor): Vertical gradient

Desktop color (1st monitor): Choose color

2nd desktop color (1st monitor): Choose color

□ Custom wallpaper download (1st monitor)

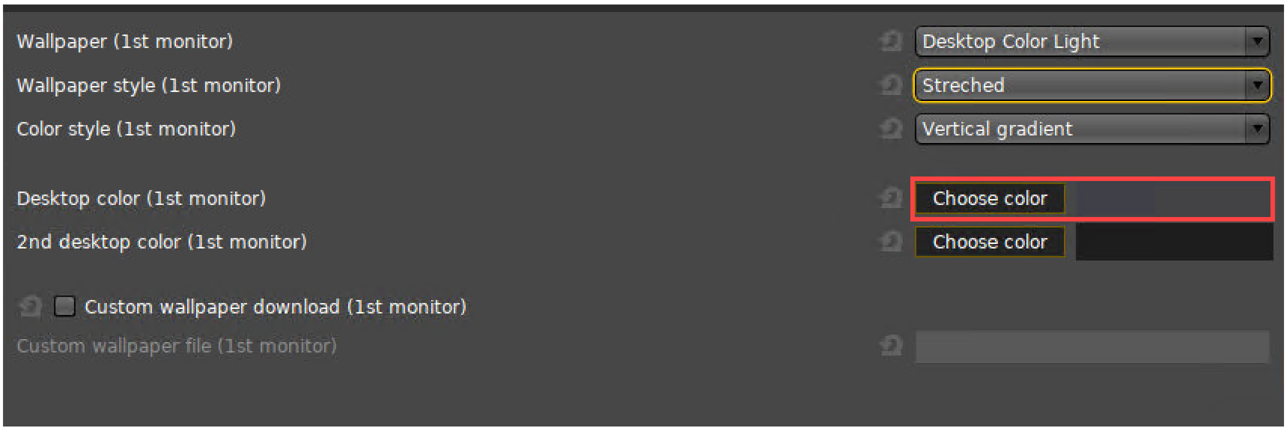
Custom wallpaper file (1st monitor)

▶ To make the style of the dialog pictures adapt to the first monitor's wallpaper style, activate the registry key **xen.xenapp-morph.customization.use_wallpaper_style** (**xen > xenapp-morph > customization > use_wallpaper_style**).

If the registry key is deactivated, the dialog images are displayed centered without being resized.

Desktop Background:

For *XenDesktop* Appliance Mode, the background color can be adapted to the background color of the first monitor. The background color of the first monitor can be configured under **User Interface > Desktop > Background (1st Monitor) >** color picker **Desktop Color (1st Monitor)**.



Wallpaper (1st monitor): Desktop Color Light

Wallpaper style (1st monitor): Streched

Color style (1st monitor): Vertical gradient

Desktop color (1st monitor): Choose color

2nd desktop color (1st monitor): Choose color

□ Custom wallpaper download (1st monitor)

Custom wallpaper file (1st monitor)

▶ To make the background color adapt to the desktop background color, activate the registry key **xen.xenapp-morph.customization.use_desktop_color** (**xen > xenapp-morph > customization > use_desktop_color**).

If the registry key is deactivated, the background color is black.

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 Virtual Desktops (for published desktops only, not for published applications)
- Citrix Self-Service (for published desktops only, not for published applications)
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- Caradigm
- 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.

Connecting to a Citrix Farm

By connecting to 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 265): Integrates published applications into the IGEL GUI.
- Citrix Self-Service (see page 266): 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 277): Shows only the web interface of the farm and hides the IGEL GUI completely.

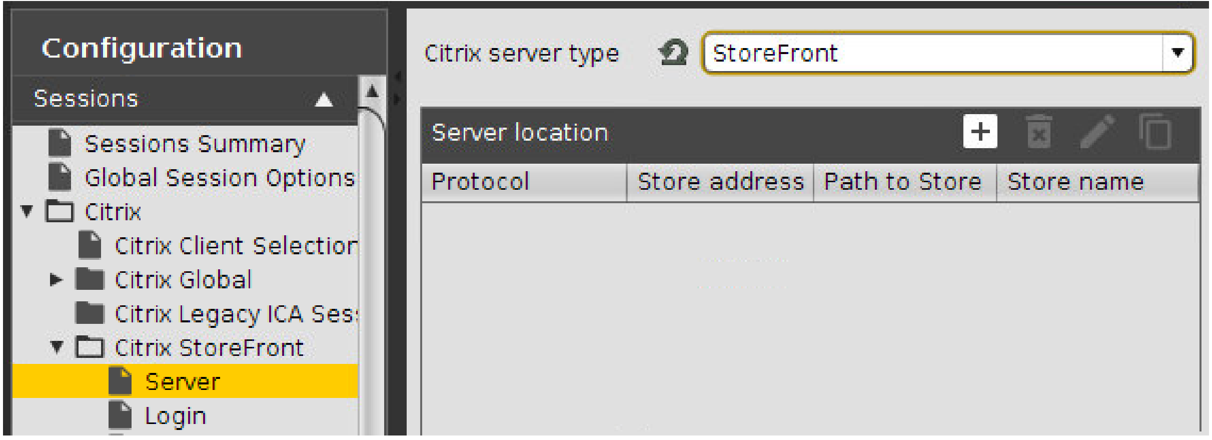
StoreFront/Web Interface

Prerequisites:

- Citrix XenDesktop 7.5 or newer
- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates)

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix StoreFront > Server**.
3. Choose **StoreFront** as **Citrix server type**.



Citrix server type: StoreFront

4. Click the **ADD** icon in the **Server location** window.
   The **ADD** mask opens.
5. Enter the names or IP addresses of the services sites.
6. Confirm with **OK**.
7. Click **Citrix StoreFront > Desktop Integration**.
8. Enter "Citrix Storefront" under **Login Session Name**.
9. Choose **Desktop** as the starting method.
10. Click **OK** to save the changes.
    Setup closes.
11. Doubleclick the Citrix icon on the desktop.
    The login window opens.
12. Enter the credentials of a user in the login window.
    The published applications of the Citrix farm will appear on the desktop.
13. Doubleclick an application icon on the desktop to start the program.

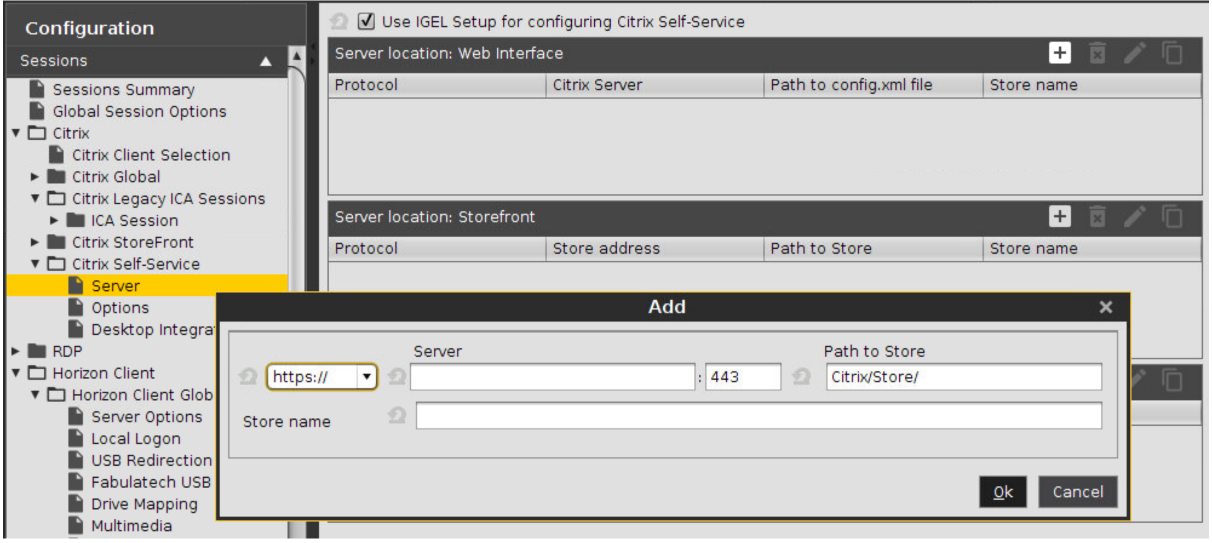
Citrix Self-Service

Prerequisites:

- Citrix XenDesktop 7.5 or newer
- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates)

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix Self-Service > Server**.
3. Click the **ADD** icon in the **Server location: Storefront** field.
   The **ADD** mask opens.



☑ Use IGEL Setup for configuring Citrix Self-Service

https:// : 443 Citrix/Store/

4. Enter the **Server**, the **Path to Store** and the **Store name** of the services sites.
5. Confirm with **OK**.
6. Click **Citrix Self-Service > Desktop Integration**.
7. Enter "Citrix Self-Service" 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 application icons of the Citrix farm will appear in the Self-Service UI.
12. Doubleclick an application icon to start the program.

Prerequisites

Requirements and restrictions for using *Citrix Self-Service*:

ⓘ As of *IGEL* Linux 5.09.100 Citrix Self-Service can be configured easily in *IGEL* Setup. See Citrix Self-Service in the *IGEL* Linux 5 Manual.

- *IGEL Linux* firmware is 5.03.100 or newer
- *Citrix Receiver 13* is enabled
- *Program Neighborhood* / *Storefront* is configured on the *Citrix* server
- *IGEL's Citrix XenApp/Storefront* feature can not be used concurrently with *Self-Service*
- Global ICA settings such as mapping of devices or redirection of content are effective for *Self-Service* as well
- The local cache for XenApp 6.5 servers will store user-defined applications for all users (cumulated cache)

ⓘ Please note the known issues regarding *Citrix Receiver* mentioned in the release notes of your *IGEL Linux* firmware.

Client Configuration

Citrix Self-Service configuration will be done by a **Custom Command** creating a personalized script. In the following the different parts of the command will be explained - you will not need to use the complete section but only the parts that are applicable to your solution.

> **Comments** in the command are tagged with a leading **#** . The comments can be skipped when copying relevant parts of the script into the **Custom Command** field.
> For more information please refer to *Citrix'* Linux OEM Guide (see page 268) (see comments below).

Preparation:

1. Make sure you are using *IGEL Linux* 5.03.100 or newer on your thin client
2. Enable *Citrix Receiver 13* in **Setup > Sessions > Citrix > Citrix Receiver Selection**.
3. Go to **Setup > System > Firmware Customization > Custom Application**.
4. Add new application *Citrix Self-Service* and set

   Settings > Icon Name = `/usr/lib/ICAClient/icons/manager.png`

   Settings > Command = `/config/sessions/selfservice`
5. Go to **Setup > System > Firmware Customization > Custom Commands > Base Commands**.
6. Enter applicable parts of the command options below to **Custom Command Session Final**.
7. Apply settings to the thin client and reboot the device.

The following template is available as plain text file as well: Citrix Self-Service Template (see page 268)

#

# The Custom Command template:

#

# IGEL Setup > System > Firmware Customization > Custom Command > Base Commands > Custom Command Session Final

#

# Get Citrix Receiver 13 directory:

```
ICADIR="/usr/lib/ICAClient"
```

#

# Create Citrix Receiver 13 cache directory:

```
mkdir -p /userhome/.ICAClient/cache/
```

#

# Remove (hide) Citrix Receiver configuration dialog (optional):

```
rm $ICADIR/util/configmgr
```

```
echo "#!/bin/sh" > $ICADIR/util/configmgr
echo "gtkmessage -m \"You are not allowed to open the configuration dialog.\"" >> $ICADIR/util/configmgr
chmod a+x $ICADIR/util/configmgr
#
# Store Citrix Receiver cache permanently (optional):
# The cache is NOT user-specific but cumulates the settings for all users who have logged on to a Citrix server via Citrix Self-Service.
# The cache contains:
# - Configured server URLs
# - Selected published applications for XenApp 6.5 server
# XenDesktop 7.x selections are stored on server side and haven't to be cached.
# It is not necessary to store the cache, if you use Self-Service
# in kiosk mode and the user can not change anything.
if [ ! -d /wfs/user/Stores ] ; then
mkdir -p /wfs/user/Stores
chown user:users /wfs/user/Stores
fi
ln -s /wfs/user/Stores /userhome/.ICAClient/cache/Stores
chown -R /userhome/.ICAClient/cache/
#
# Set one ore more server URLs:
SERVER_URL="http://./citrix/pnagent/config.xml"
SERVER_URL2="https://."
# If using HTTPS connections do not forget to store the SSL certificate on your thin client.
# See IGEL Knowledge Base for more information https://kb.igel.com/igelos/en/deploying-trusted-root-certificates-2720919.html (see page 574)
#
# Create user script /config/sessions/selfservice to be started as Custom Application.
# (Up to next EOF at the end)
# Do not delete the hash sign (#) in the command below!
```

```
cat < /config/sessions/selfservice
#!/bin/sh
#
# Storebrowse is not yet working stable, kill the running daemons and
# kill the AuthManagerDaemon, so the credentials of the last user are cleared:
killall storebrowse AuthManagerDaemon ServiceRecord
#
# See Linux-OEM-Guide-13.0-12-13-13.pdf page 58
# for ALL storebrowse options.
#
# Configure server URLs to be used in selfservice (optional:)
# If no URLs are configured, the Citrix Receiver will ask the user to enter a URL.
# See Linux-OEM-Guide-13.0-12-13-13.pdf page 20
# IMPORTANT: Do not forget to install the root certificate for HTTPS connections!
# Configure a DefaultStore. Only one store can be default!
# In the example below STORE2 is set as default:
STORE=\`$ICADIR/storebrowse -a $SERVER_URL\`
#if [ "\$?" = "0" ] ; then
# eval $ICADIR/storebrowse -c DefaultStore=\$STORE
#fi
STORE2=\`$ICADIR/storebrowse -a $SERVER_URL2\`
if [ "\$?" = "0" ] ; then
eval $ICADIR/storebrowse -c DefaultStore=\$STORE2
fi
#
# Delete dispensable server URLs (optional):
# In case the cache directory is stored permanently (see above) and
# a server URL should not be used anymore.
#$ICADIR/storebrowse -d
#
# Configure gateway (optional, see Linux-OEM-Guide-13.0-12-13-13.pdf page 22):
```

```
#$ICADIR/storebrowse -g
```

#

# Preset published applications to be shown in Citrix Receiver (optional):

# Only valid for XenApp 6.5 and previous.

# For XenDesktop 7.x see section below.

# Especially needed if Self-Service runs in kiosk mode and the user can not add

# applications on his own.

# Get the "Resourcename" by running

```
# "/usr/lib/ICAClient/storebrowse -E "
```

# in your Linux console (local terminal session).

# Example configuration with Windows Command Prompt (cmd) and Paint preset:

```
if [ ! -f /userhome/.ICAClient/cache/Stores/PNAApplications.ctx ] ; then
mkdir -p /userhome/.ICAClient/cache/Stores
echo "" > /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t\t:cmd" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t\t:Paint" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo -e "\t" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
echo "" >> /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
chown user:users /userhome/.ICAClient/cache/Stores/PNAApplications.ctx
fi
```

#

# Preset published applications to be shown in Citrix Receiver (optional):

# Only valid for XenDesktop 7.x.

# For XenApp 6.5 and previous see section above.

# Especially needed if Self-Service runs in kiosk mode and the user can not add

# applications on his own.

# Get the "desktop or application ID" by running

```
# "/usr/lib/ICAClient/storebrowse -E "
# in your Linux console (local terminal session).
# Subscribe: $ICADIR/storebrowse -s
# Unsubscribe: $ICADIR/storebrowse -u
# List subscriptions: $ICADIR/storebrowse -S
#
# Add subscriptions which have not been added before:
$ICADIR/storebrowse -S $SERVER_URL2 > /tmp/.subs.\$\$
# Example configuration with Windows Command Prompt (cmd), Calculator and WordPad preset:
grep "'XD71DevSite.Cmd'" /tmp/.subs.\$\$ || $ICADIR/storebrowse -s "XD71DevSite.Cmd" $SERVER_URL2
grep "'XD71DevSite.Write'" /tmp/.subs.\$\$ || $ICADIR/storebrowse -s "XD71DevSite.Write" $SERVER_URL2
grep "'XD71DevSite.Calc'" /tmp/.subs.\$\$ || $ICADIR/storebrowse -s "XD71DevSite.Calc" $SERVER_URL2
rm /tmp/.subs.\$\$
#
# Configure Self-Service GUI options such as full-screen mode (optional):
# See Linux-OEM-Guide-13.0-12-13-13.pdf page 46
$ICADIR/storebrowse -c SharedUserMode=False
$ICADIR/storebrowse -c FullscreenMode=0
$ICADIR/storebrowse -c SelfSelection=True
#
# Configure reconnection options:
# See Linux-OEM-Guide-13.0-12-13-13.pdf page 23.
$ICADIR/storebrowse -c ReconnectOnLogon=False
$ICADIR/storebrowse -c ReconnectOnLaunchOrRefresh=False
#
# Display desktop sessions in full screen or window mode
#$ICADIR/storebrowse -c SessionWindowedMode=True/False
```

#

# Run command to open the gui

```
$ICADIR/selfservice
```

#

# End of user script /config/sessions/selfservice to be started as Custom Application:

```
EOF
```

#

# Change access rights for user script (executable):

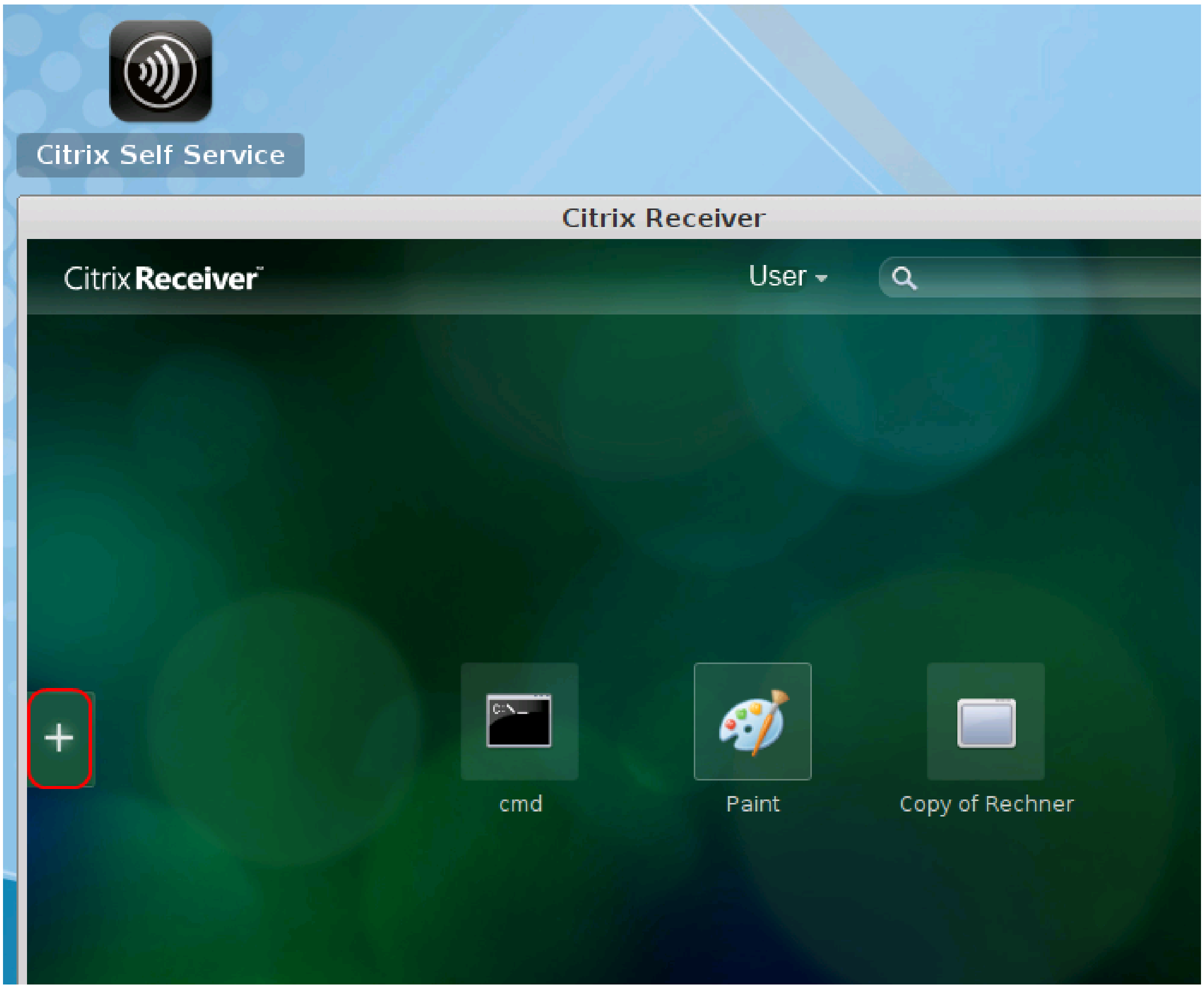
```
chmod a+x /config/sessions/selfservice
```

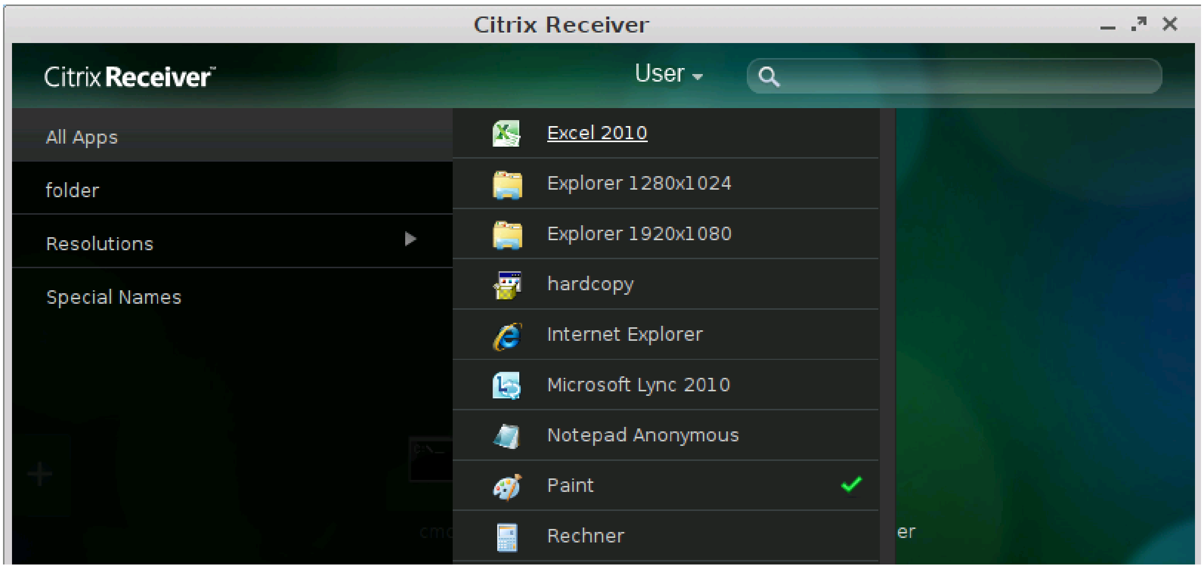
#

# End of Custom Command template.

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 276)

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

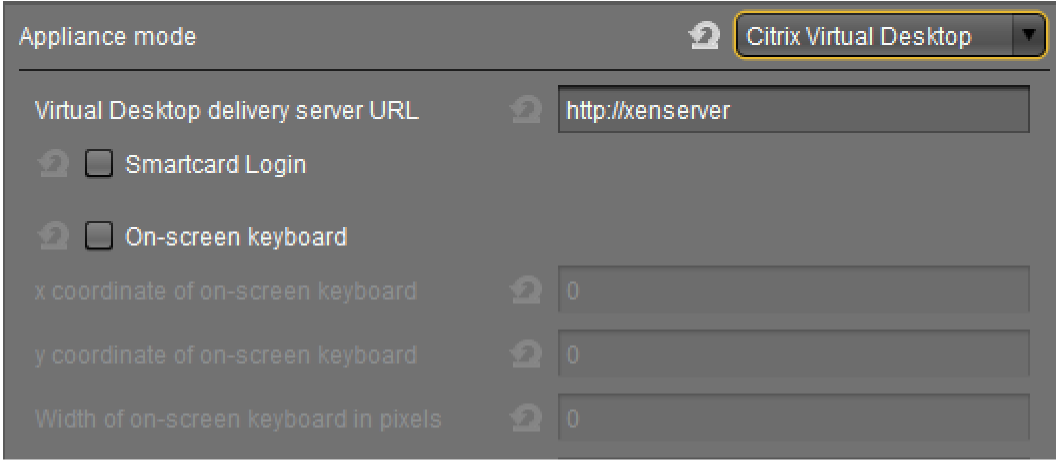
Appliance Mode

There are two ways to connect to the Citrix Server in Appliance mode:

- **Citrix Virtual Desktop**: Connect to Citrix Farm via your browser.
- **Citrix Selfservice**: Connect to Citrix Farm via your Selfservice GUI.

Connecting Citrix via Browser

1. Click **Sessions > Appliance Mode** in the configuration tree of the IGEL setup.
2. Select **Citrix Virtual Desktop** under **Appliance mode**.



Appliance mode: Citrix Virtual Desktop ▼

Virtual Desktop delivery server URL: http://xenserver

□ Smartcard Login

□ On-screen keyboard

x coordinate of on-screen keyboard: 0

y coordinate of on-screen keyboard: 0

Width of on-screen keyboard in pixels: 0

3. Enter the **URL** of the delivery server.
4. Activate **Smartcard Login** if necessary.
5. Click **OK** to save the changes and close setup.
6. Follow the instructions on the screen.

Connecting Citrix via Selfservice

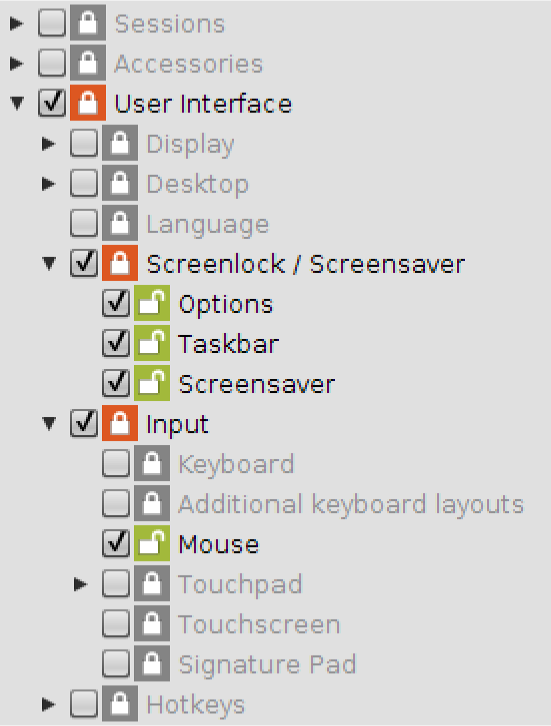
1. Click **Sessions > Appliance Mode** in the configuration tree of the IGEL setup.
2. Select **Citrix Self-Service** under **Appliance mode**.
3. Enter the **URL** of the delivery server.
4. Click **OK** to save the changes and close setup.
5. Follow the instructions on the screen.

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**.

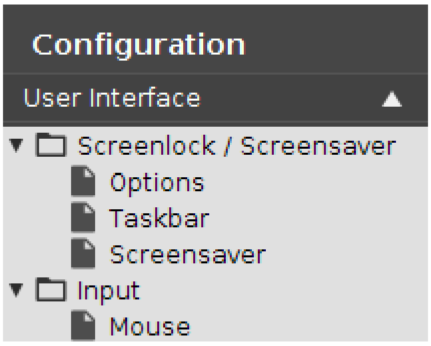
Here is how to select setup pages for quick setup:

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**.



- □ Sessions
- □ Accessories
- ☑ User Interface
  - □ Display
  - □ Desktop
  - □ Language
  - ☑ Screenlock / Screensaver
    - ☑ Options
    - ☑ Taskbar
    - ☑ Screensaver
  - ☑ Input
    - □ Keyboard
    - □ Additional keyboard layouts
    - ☑ Mouse
    - □ Touchpad
    - □ Touchscreen
    - □ Signature Pad
  - □ Hotkeys

3. Click **Apply** or **Ok**.
When the user starts **Quick Settings**, the previously selected options are presented.



Configuration

User Interface

- Screenlock / Screensaver
  - Options
  - Taskbar
  - Screensaver
- Input
  - Mouse

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.

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[11]

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.

[11] 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.

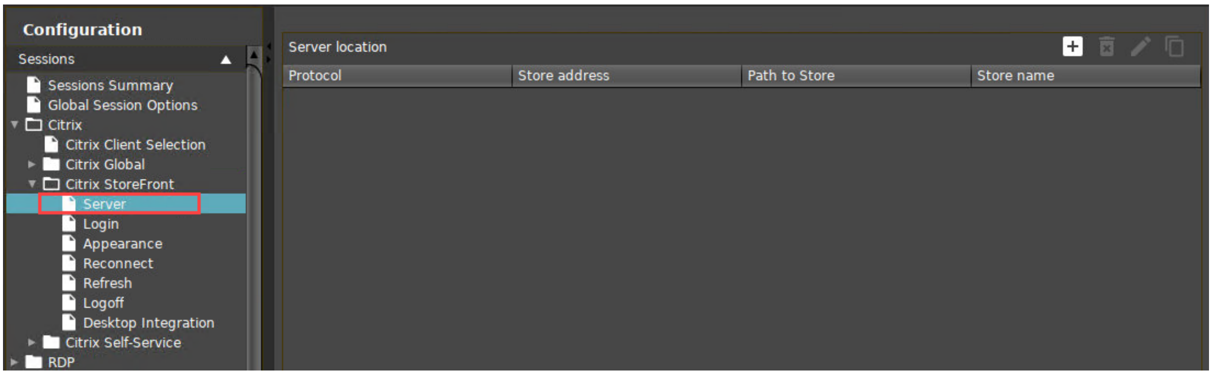
The AD password must be entered to activate the IGEL clients.

Configuring Auto Logon for Citrix Virtual Desktops

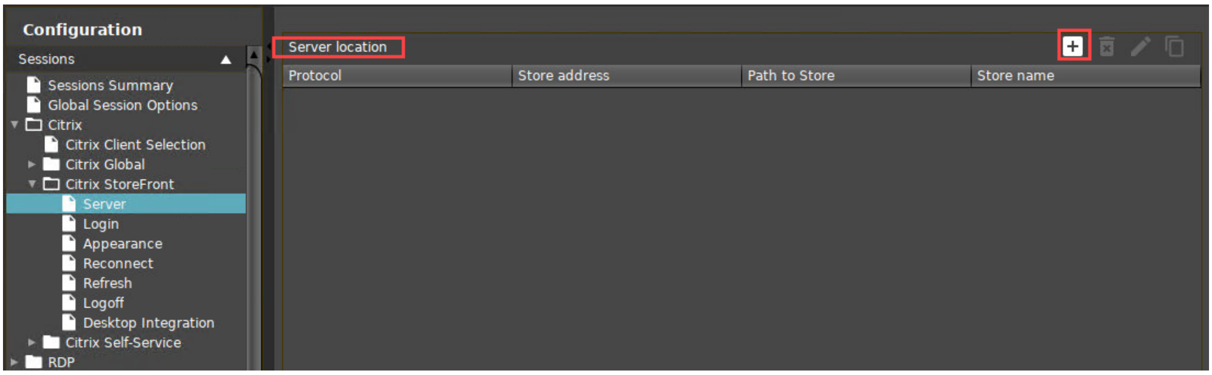
This how-to describes how to configure Auto Logon for Citrix Virtual Desktops.

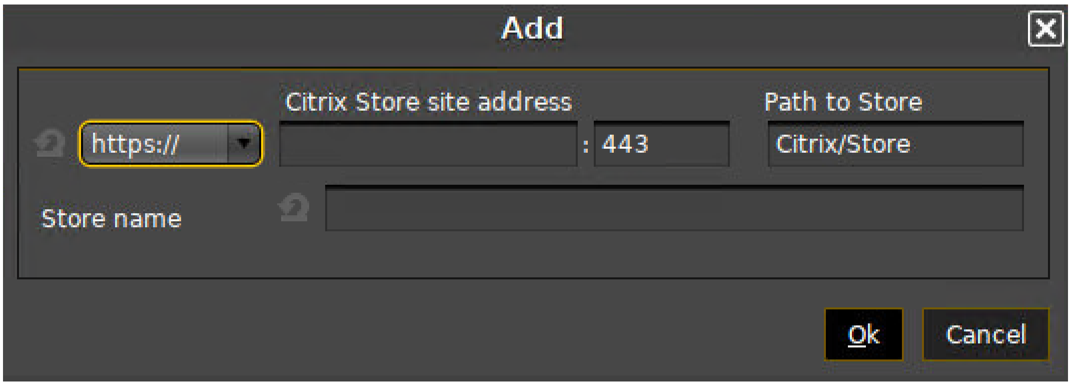
Steps

1. In IGEL Setup, go to **Sessions > Citrix > Citrix StoreFront > Server**.

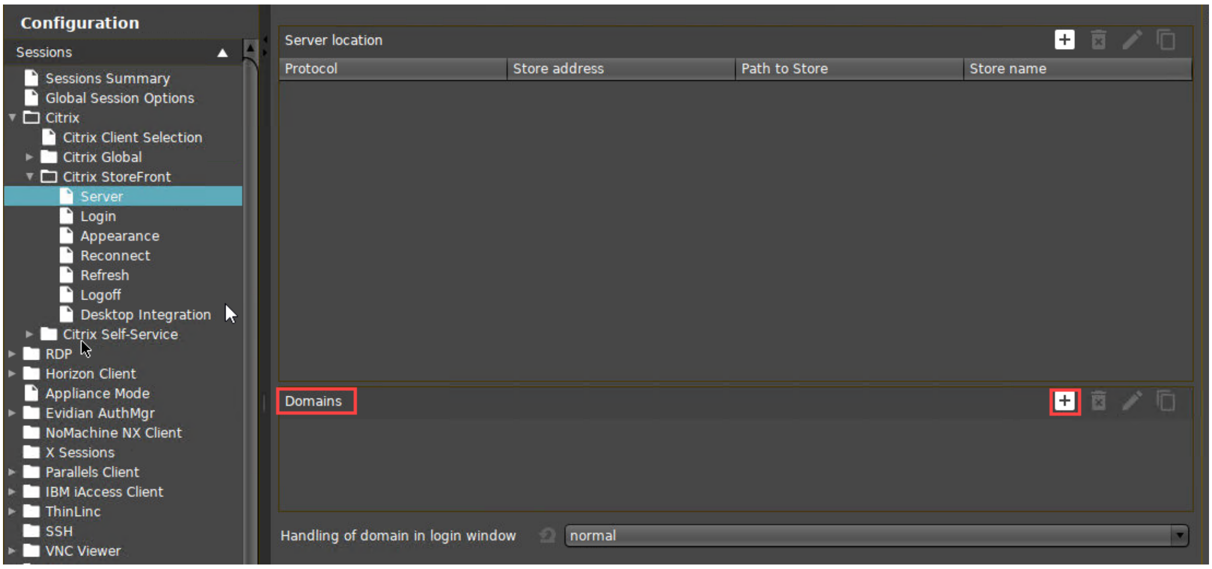


2. Add your **Server Location**.

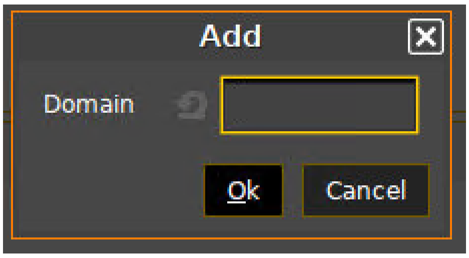




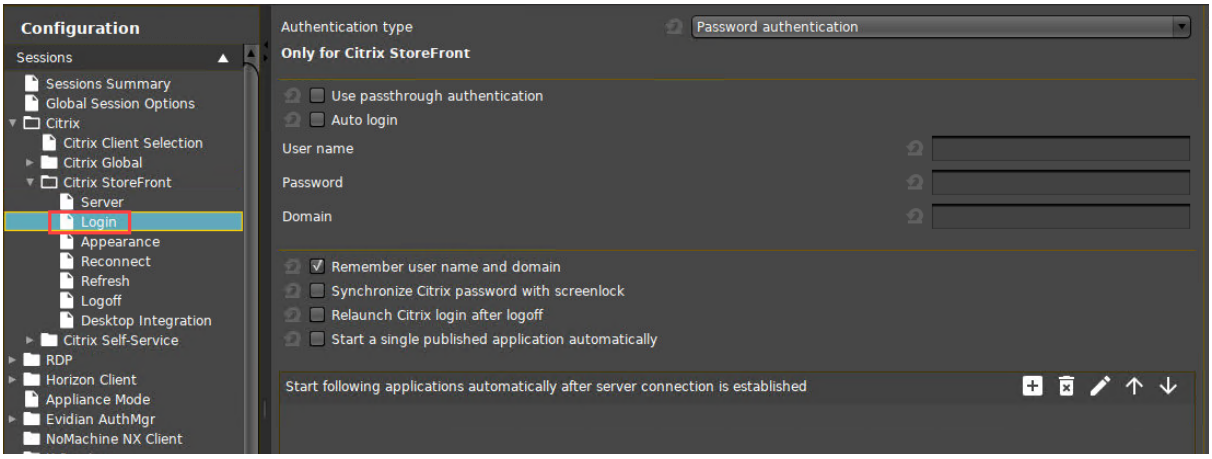
3. Add your Active Directory domain to **Domains**, making sure that you use its Fully Qualified Domain Name (FQDN).



Handling of domain in login window: normal



4. Go to **Sessions > Citrix > Citrix StoreFront > Login**.



Authentication type: Password authentication

Only for Citrix StoreFront

- ☐ Use passthrough authentication
- ☐ Auto login

User name

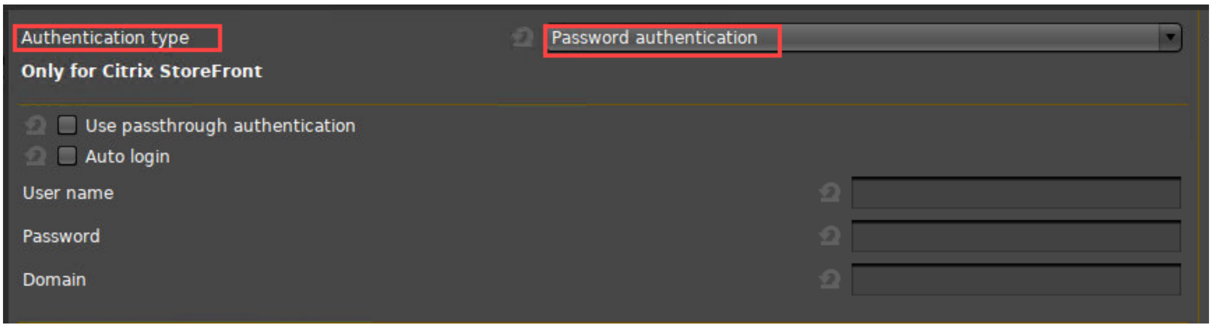
Password

Domain

- ☑ Remember user name and domain
- ☐ Synchronize Citrix password with screenlock
- ☐ Relaunch Citrix login after logoff
- ☐ Start a single published application automatically

Start following applications automatically after server connection is established

5. Set **Authentication type** to **Password authentication**.

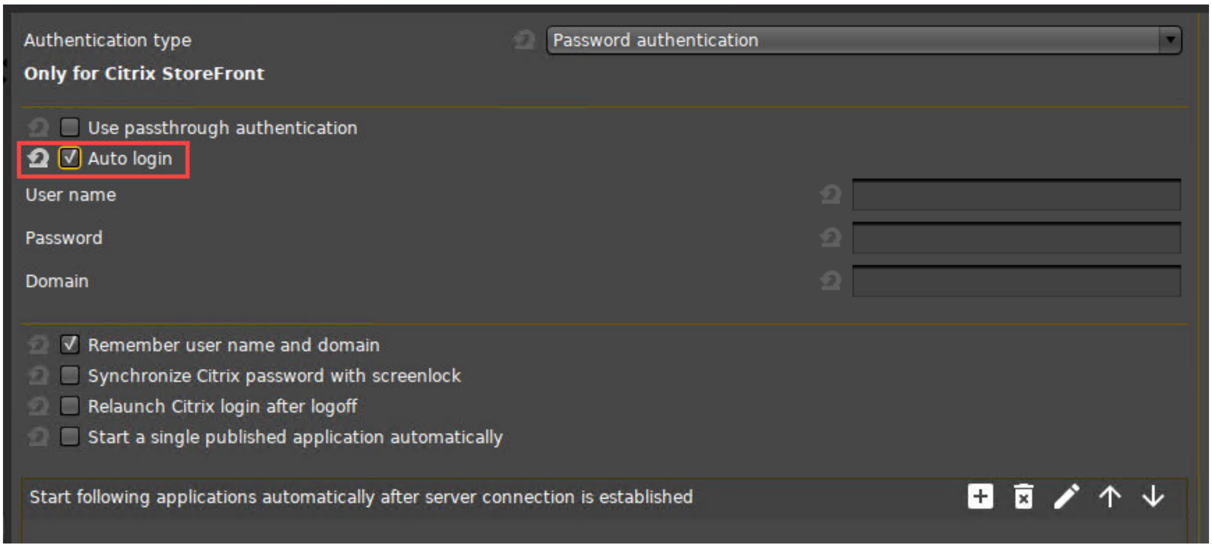


Authentication type: Password authentication

Only for Citrix StoreFront

□ Use passthrough authentication
□ Auto login
User name
Password
Domain

6. Activate **Auto Login**.



Authentication type: Password authentication

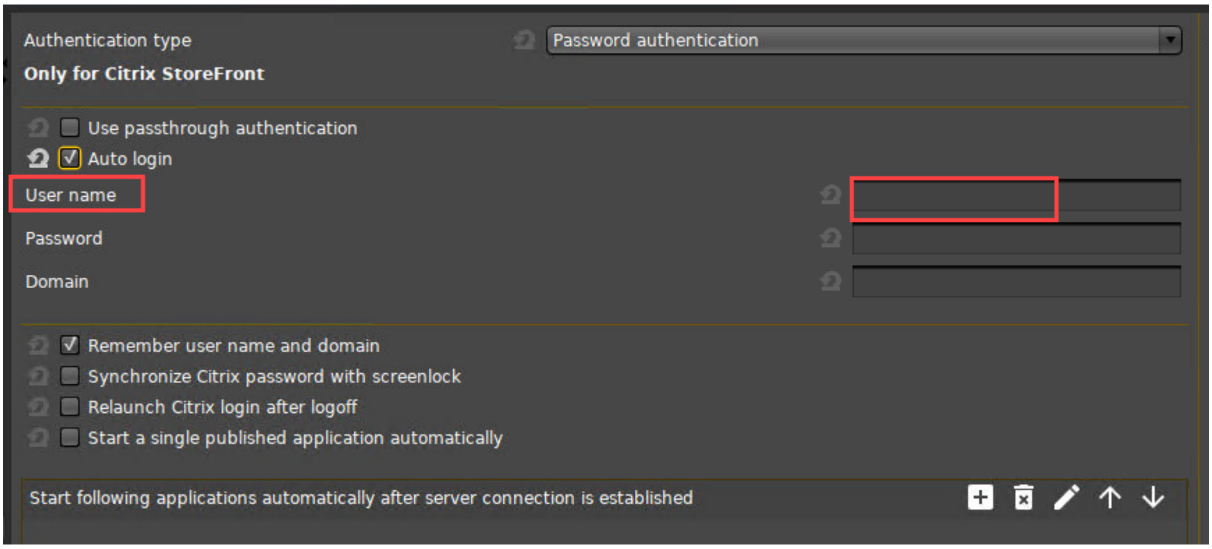
Only for Citrix StoreFront

□ Use passthrough authentication
☑ Auto login
User name
Password
Domain

☑ Remember user name and domain
□ Synchronize Citrix password with screenlock
□ Relaunch Citrix login after logoff
□ Start a single published application automatically

Start following applications automatically after server connection is established

7. Set **User Name** to the Active Directory user name.



Authentication type: Password authentication

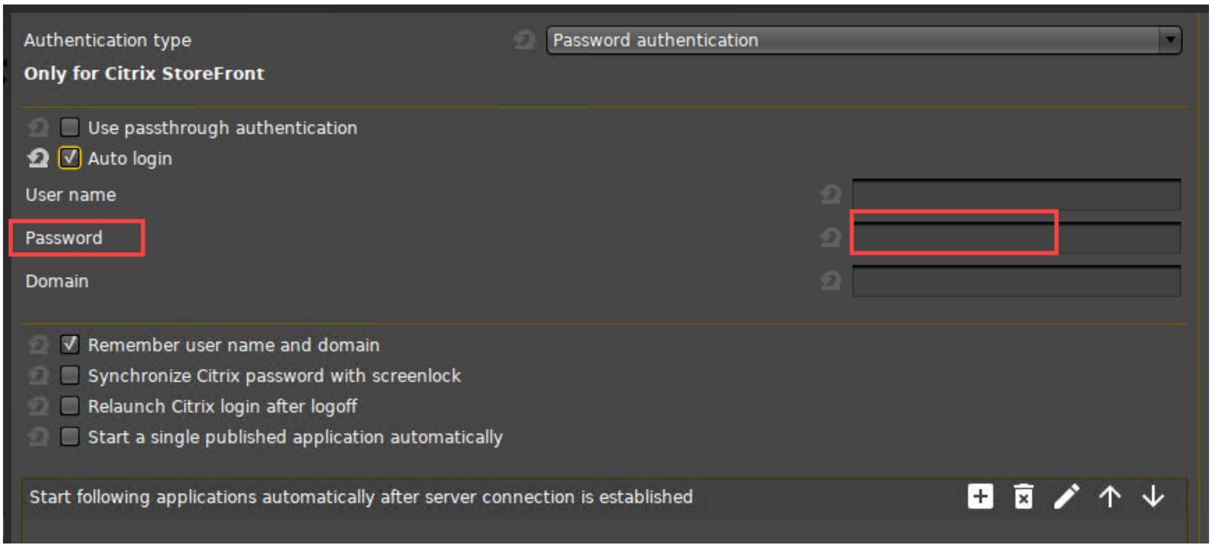
Only for Citrix StoreFront

□ Use passthrough authentication
☑ Auto login
User name
Password
Domain

☑ Remember user name and domain
□ Synchronize Citrix password with screenlock
□ Relaunch Citrix login after logoff
□ Start a single published application automatically

Start following applications automatically after server connection is established

8. Set the **Password**.



Authentication type: Password authentication

Only for Citrix StoreFront

☐ Use passthrough authentication
☑ Auto login

User name

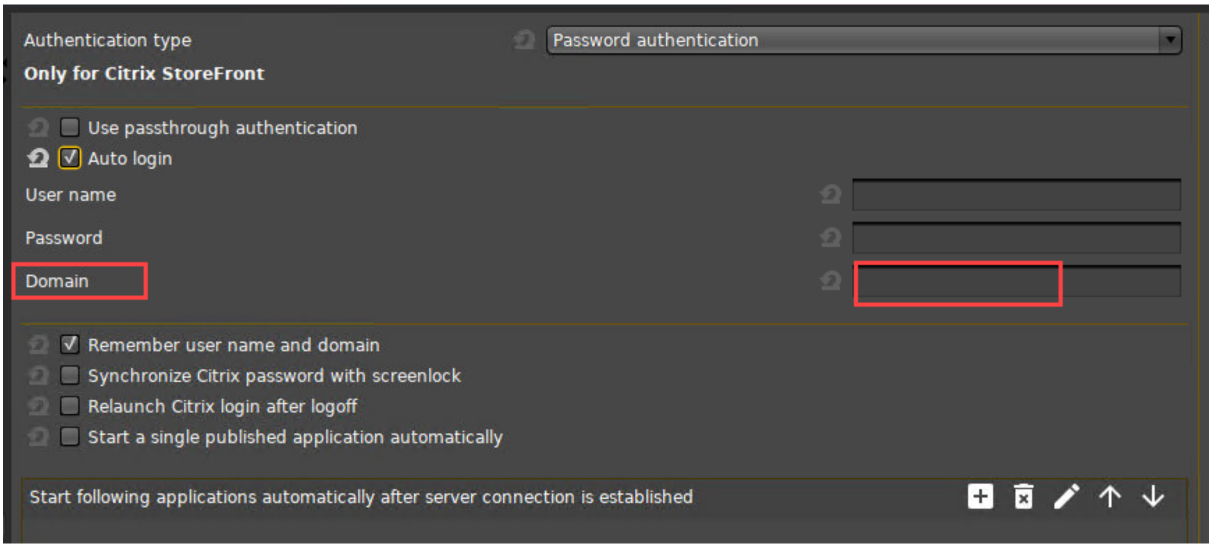
Password

Domain

☑ Remember user name and domain
☐ Synchronize Citrix password with screenlock
☐ Relaunch Citrix login after logoff
☐ Start a single published application automatically

Start following applications automatically after server connection is established

9. Set **Domain** to your Active Directory domain's FQDN, the same as in step 3.



Authentication type: Password authentication

Only for Citrix StoreFront

☐ Use passthrough authentication
☑ Auto login

User name

Password

Domain

☑ Remember user name and domain
☐ Synchronize Citrix password with screenlock
☐ Relaunch Citrix login after logoff
☐ Start a single published application automatically

Start following applications automatically after server connection is established

Force Citrix Logout Using Hotkey

You will find the instructions under Citrix: Freeze at Logout (see page 287).

⚠ 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

▶ Select **TCP only - UDP disabled** under **Sessions > Citrix > Citrix Global > Options > HDX Adaptive Transport over EDT**.

OR

▶ 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.

Here you can learn how to import a profile: Importing a Profile and Firmware.

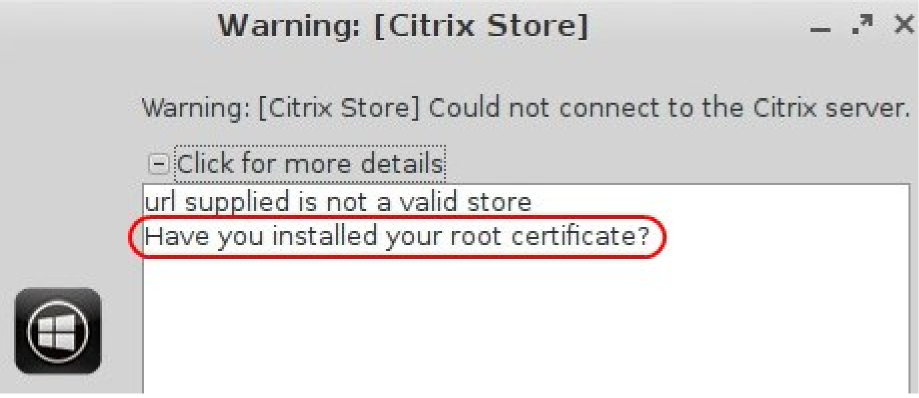
Warning Message: [Citrix Store] Could Not Connect to the Citrix Server

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.`

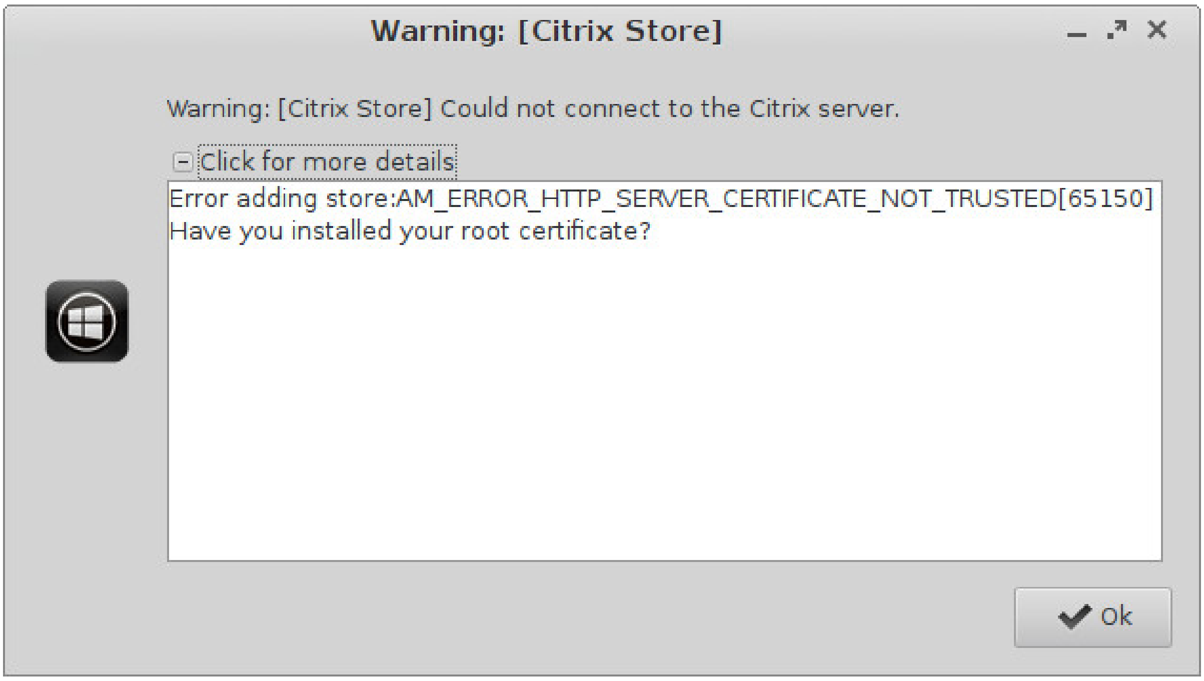


Warning: [Citrix Store]

Warning: [Citrix Store] Could not connect to the Citrix server.

url supplied is not a valid store
Have you installed your root certificate?

or



Warning: [Citrix Store]

Warning: [Citrix Store] Could not connect to the Citrix server.

⊟ Click for more details

```
Error adding store:AM_ERROR_HTTP_SERVER_CERTIFICATE_NOT_TRUSTED[65150]
Have you installed your root certificate?
```

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 (see page 574).

Setting 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.
- 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**.

If your Desktop sessions on rotated screens flicker or the graphic is not good enough, you can **Enable HW accelerated H264 vdpau codec (experimental)** in the IGEL Setup under **System > Registry > ica > hw-accelerated-h264-vdpau-codec** (Search parameter: **ica.hw-accelerated-h264-vdpau-codec)**

Important is, that you activate **Use video codec for compression** → **For the entire screen** in the citrix server policy.

Using 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[12] apply.

[12] https://www.igel.com/terms-conditions/

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.

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[13].

[13] https://discussions.citrix.com/topic/393872-possible-workaround-citrix-receiver-x-error-on-linux-thin-clients/

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.

ICA screen artifacts in Lotus Notes, OpenOffice, etc.

Symptom:

Some remote applications such as *Lotus Notes* or OpenOffice have artifacts, so that menus may look damaged. This happens in *IGEL Linux* 5.05.x or newer on hardware with the Intel Sandy Bridge chipset in ICA Sessions with old Citrix server versions such as *Presentation Server* or *XenApp* <= 6.0.

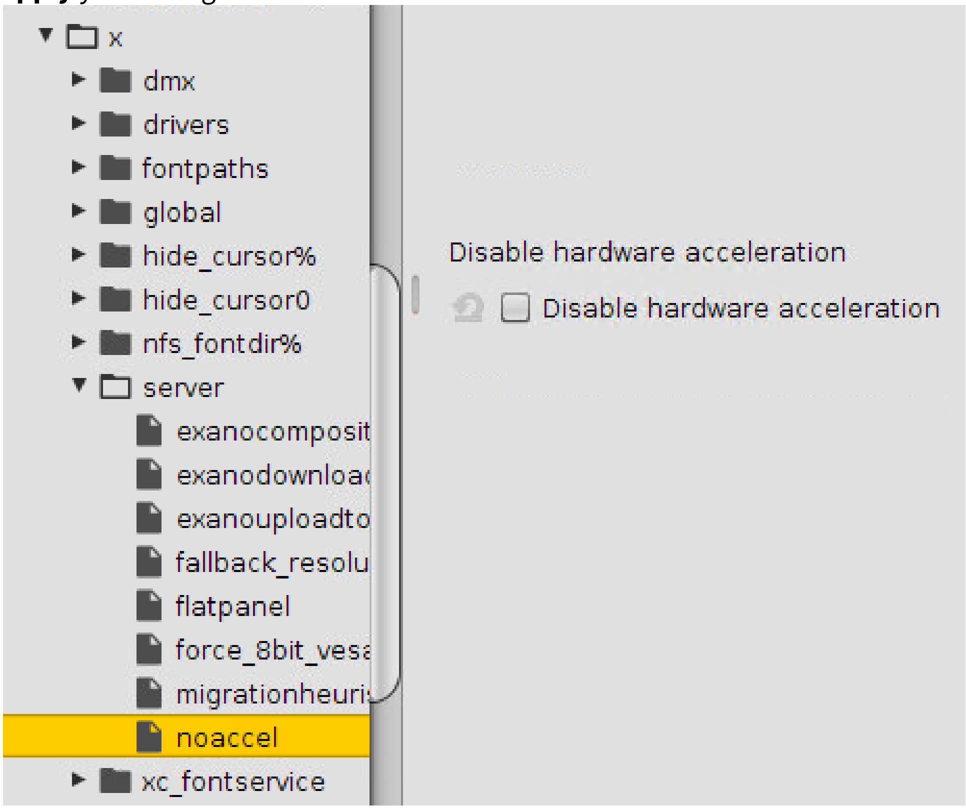
Problem:

The graphics driver has issues.

Solution:

As a workaround, disable hardware acceleration:

1. In *IGEL Setup*, go to **System > Registry**
2. Locate the `x.server.noaccel` entry
3. Check **Disable hardware acceleration**
4. **Apply** your changes



Disable hardware acceleration

□ Disable hardware acceleration

Legal Note

IGEL's Terms & Conditions[14] apply.

[14] https://www.igel.com/terms-conditions/

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.

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 > 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/Azure AD)	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

Using 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.

- IGEL OS 11.02.100 and 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[15].

[15] https://docs.citrix.com/en-us/hdx-optimization/

RDP

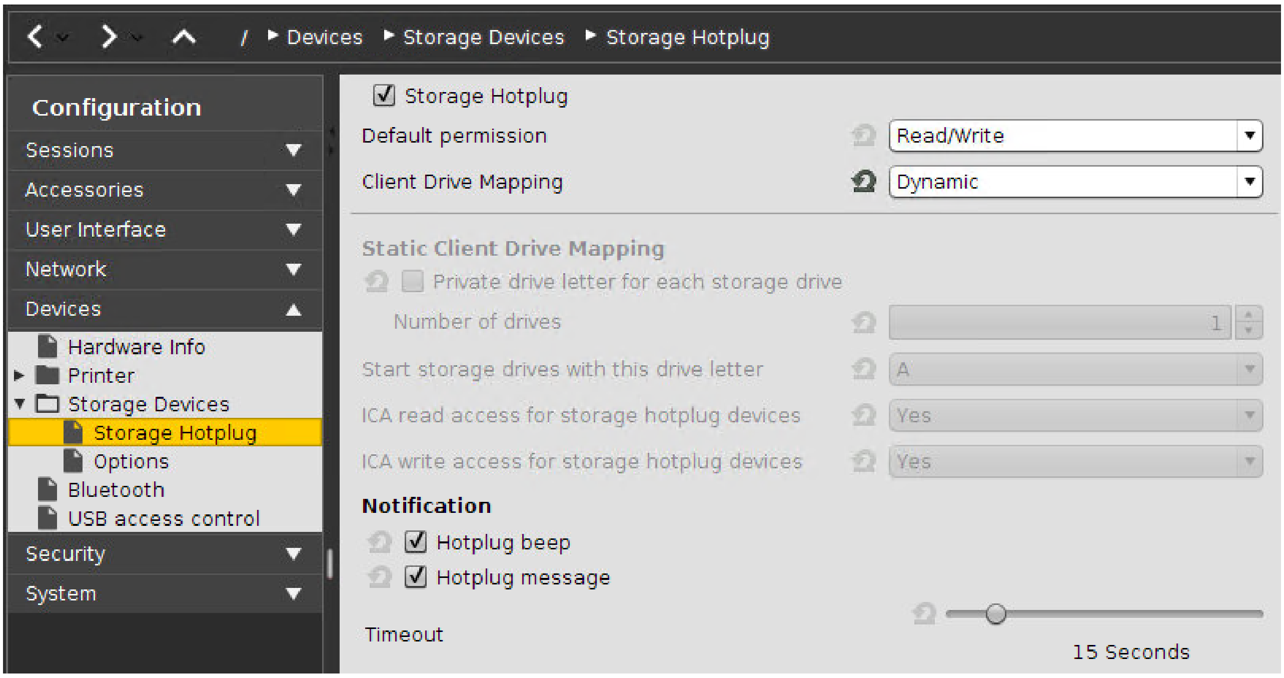
Mapping USB Storage Media into RDP Sessions

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.

Basic Configuration of the Client



☑ Storage Hotplug

Default permission: Read/Write

Client Drive Mapping: Dynamic

Static Client Drive Mapping

□ Private drive letter for each storage drive

Number of drives: 1

Start storage drives with this drive letter: A

ICA read access for storage hotplug devices: Yes

ICA write access for storage hotplug devices: Yes

Notification

☑ Hotplug beep

☑ Hotplug message

Timeout: 15 Seconds

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

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

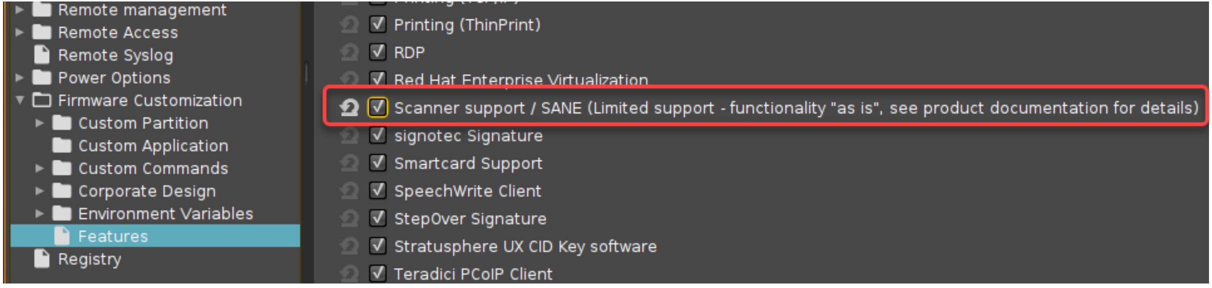
▶ Under **Sessions > RDP > RDP Sessions > [Session name] > Options > Load balancing routing token**, enter `tsv://MS Terminal Services Plugin.1.[collection name]`, where

- `tsv://MS Terminal Services Plugin.1.` is the routing token
  and
- `[collection name]` is the name of the RDS collection, defined by the server administrator.

RDP Fabulatech Scanner Redirection

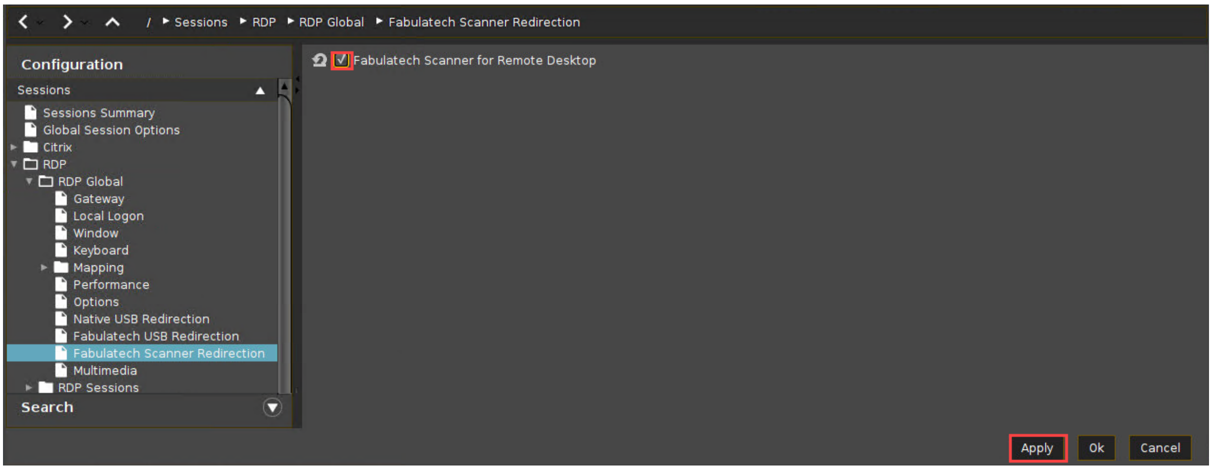
Enabling Fabulatech Scanner Redirection

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.



☑ Printing (ThinPrint)
☑ RDP
☑ Red Hat Enterprise Virtualization
☑ Scanner support / SANE (Limited support - functionality "as is", see product documentation for details)
☑ signotec Signature
☑ Smartcard Support
☑ SpeechWrite Client
☑ StepOver Signature
☑ Stratusphere UX CID Key software
☑ Teradici PCoIP Client

   - 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.
   - 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.**
3. Check **Fabulatech Scanner for Remote Desktop.**



☑ Fabulatech Scanner for Remote Desktop

4. Click **Apply** or **Ok** to confirm the settings.

RDP RemoteApp Parameter Settings

Symptom

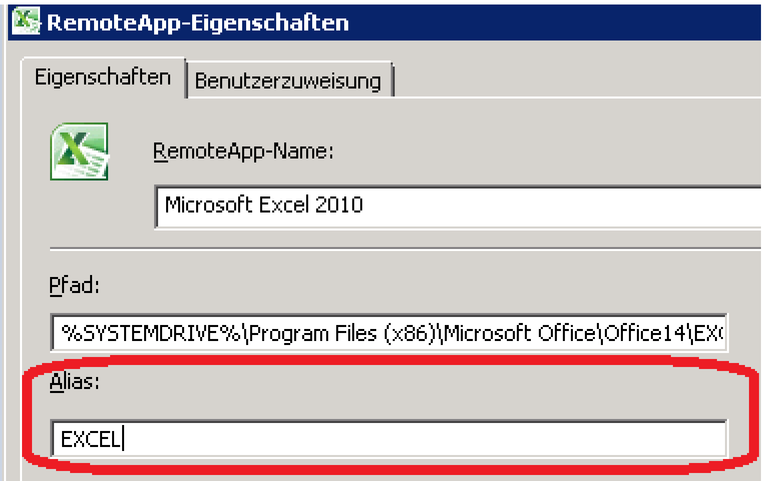
RemoteApp is not starting or closes immediately after login.

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.



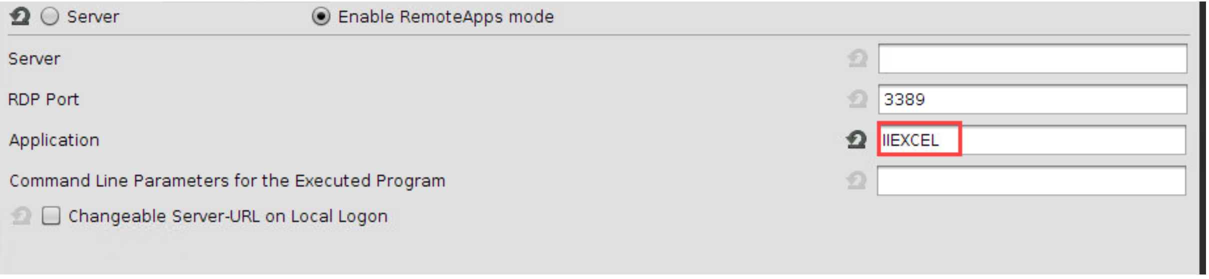
RemoteApp-Eigenschaften

RemoteApp-Name: Microsoft Excel 2010

Pfad: %SYSTEMDRIVE%\Program Files (x86)\Microsoft Office\Office14\EX(

Alias: EXCEL

2. Use that ALIAS value in the device's setting in **Setup > Sessions > RDP > RDP Sessions > (Session Name) > Server > Application.**



○ Server ● Enable RemoteApps mode

Server:

RDP Port: 3389

Application: ||EXCEL

Command Line Parameters for the Executed Program:

□ Changeable Server-URL on Local Logon

ⓘ Add two pipe-characters (||) at the beginning of the ALIAS value.

RDP Performance Enhancements

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".

IZ1 RFX Performance Enhancement

Symptom

RDP session with IGEL IZ1 RFX client to Microsoft Windows Server 2012/2012 R2 does not support RemoteFX 7 (Calista Codec) resulting in low session performance.

Problem

RemoteFX 7 (Calista Codec) is not active on the server.

Solution

Activate RemoteFX 7 (Calista Codec) on Microsoft Windows Server:

1. Change following parameters of your group policy (either local or as domain policy):
    a. Go to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment**
    b. Enable **Limit maximum Color Depth**
    c. Set **Color Depth = Client Compatible**
    d. Enable **RemoteFX encoding for RemoteFX client designed for Windows Server 2008 R2 SP1**
2. In the thin client's setup (or UMS profile) enable **Sessions > RDP > RDP Global > Performance > RemoteFX**

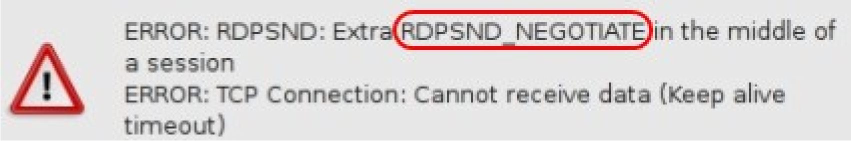
> ⓘ Make sure your server provides sufficient amount of RAM.

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)
```



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**

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

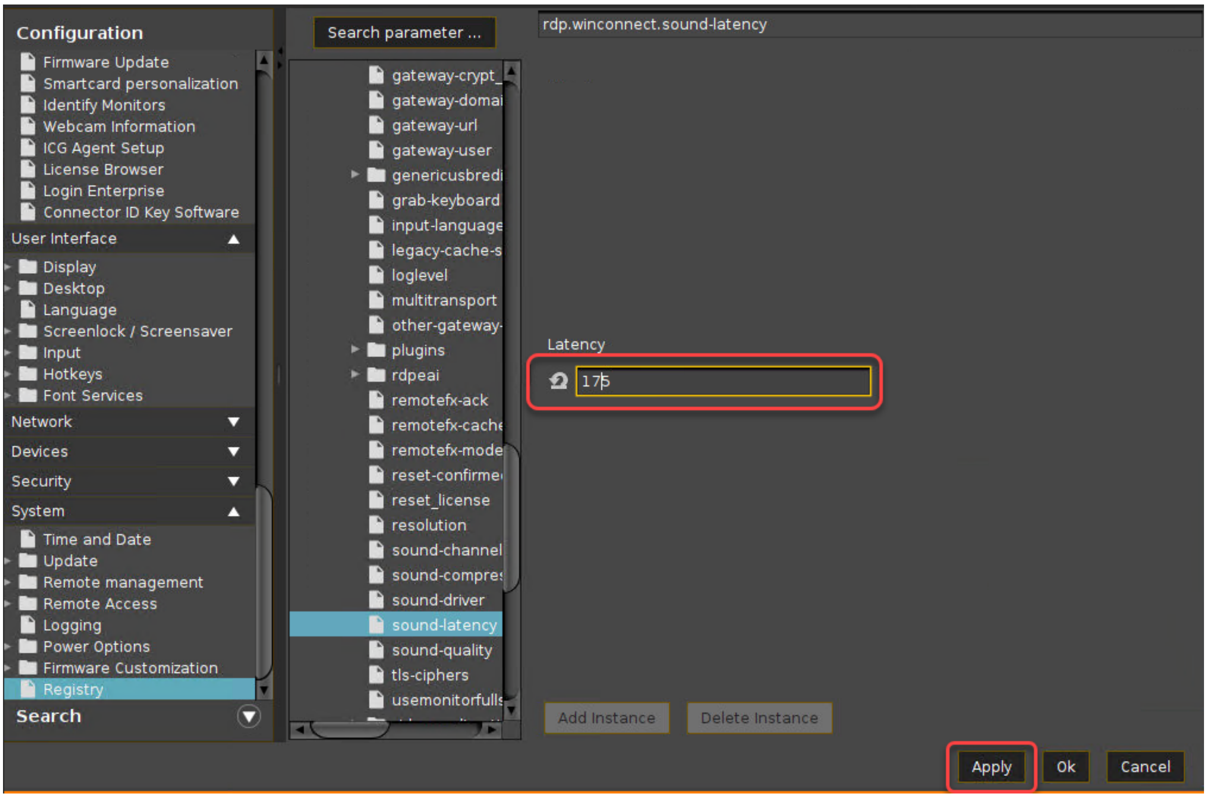
The crackling noises, or audio glitches, result from buffer underruns. This occurs when new audio data are not delivered fast enough and the sound card buffer has no more audio data left to play. Thus, it is not possible to bridge the replay gap. This is more likely to happen with sound cards that have 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**.



rdp.winconnect.sound-latency

Latency

175

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.

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[16]

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.

[16] 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 "I".
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.

User Has to Provide Credentials Twice for RDP Logon

Issue

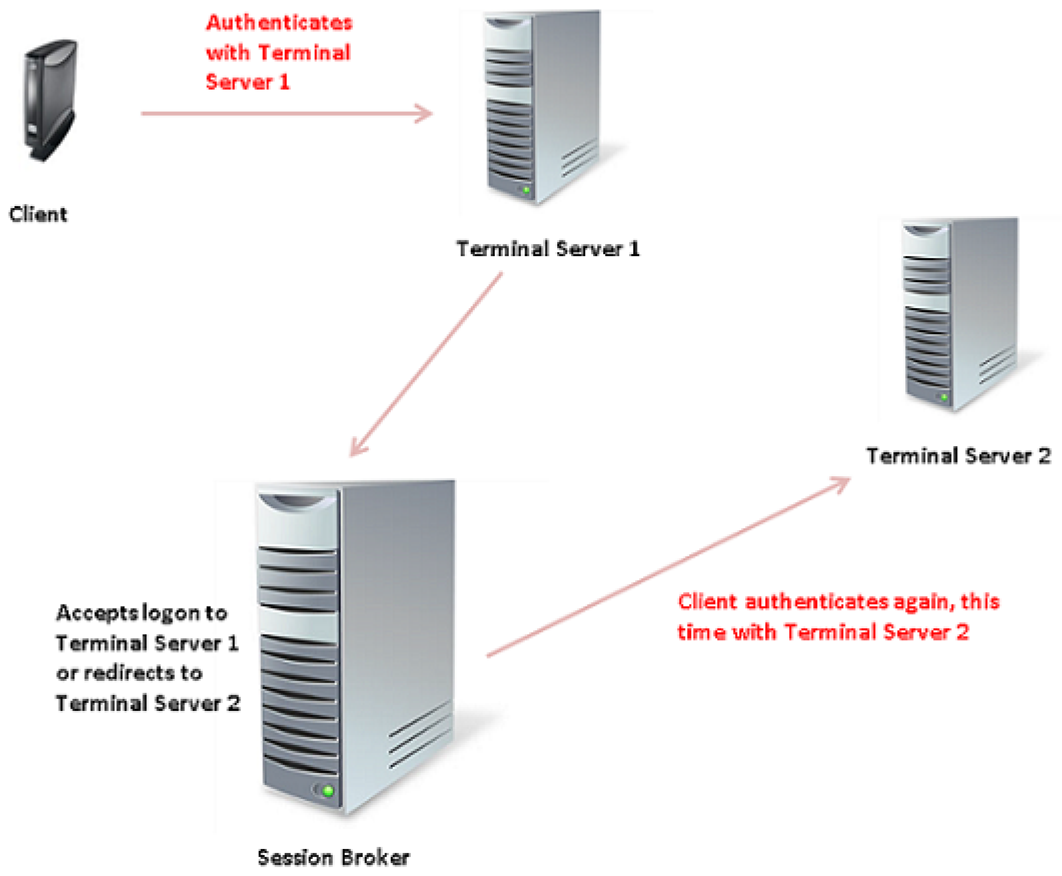
When you connect to a Windows terminal server, you are asked to provide your credentials twice.

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.


Authenticates with Terminal Server 1
Client
Terminal Server 1
Terminal Server 2
Accepts logon to Terminal Server 1 or redirects to Terminal Server 2
Client authenticates again, this time with Terminal Server 2
Session Broker

Solution

The issue can be resolved by activating Kerberos/Active Directory authentication. For further information, see Active Directory/Kerberos.

VMware Horizon

Setting up VMware Blast Sessions

Prerequisites

- Licensed IGEL Multimedia Codec Pack
- Device offering hardware video acceleration, see the FAQ Hardware Video Acceleration on IGEL OS.
- 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**.

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]. But, by default, hotkeys have no effect in VMware Horizon sessions.

Solution

Create a custom command that adds the hotkey the system. It is recommended to use a profile:

1. Create a new profile. For more information about profiles, see Profiles.
2. Go to **System > Firmware Customization > Custom Commands > Base**.
3. Under **Initialization** enter this command: `echo '<ctrl><super>0x020' >> /etc/vmware/view-keycombos-config`

   ⓘ For more information about hotkeys, see VMware Docs[17].

4. Assign the profile to your device and reboot.

[17] https://docs.vmware.com/en/VMware-Horizon-Client-for-Linux/4.6/linux-client-installation/GUID-05FE2CCC-9D84-4B37-AC9B-D8CEC43D8567.html

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.[18]

You can also access IGEL's 3rd party hardware support database[19] to find fully supported graphic chips.

[18] http://edocs.igel.com/index.htm#11873.htm
[19] 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 > Notes for Release [your version] > Component Versions [your version].
See also the original document at https://kb.vmware.com/s/article/78810.

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

Category	Feature	Supported
	Log in as current user	no
	Nested log in as current user	no
	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

Category	Feature	Supported
	Non Interactive Mode	yes
	GPO-based customization	no
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

Category	Feature	Supported
	Local buffer text input box	no
	Keyboard Mapping	yes
	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**.

Evidian

Authenticating 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 thin client.
- An installed and running *Evidian SSO Controller.*
- When using HTTPS (*IGEL Linux* 5.07.100 or newer), the *User Access Server's* CA root certificate saved locally on the thin client.
- The thin client 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 thin client
- RFID badges that are already enrolled.

Configuring an Evidian Authentication Manager Session

1. Go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions** in the thin client setup.
2. Add a new session.
3. Go to **Sessions > Evidian AuthMgr > Evidian AuthMgr Sessions > [Session Name] > Connection**.
4. Enter the **User Access Service URL** including protocol, name or IP address and port number (`[protocol]://[host]:[port]/soap`).
5. Enter the **Roaming Session Secret**.
6. When using HTTPS, select the *User Access Server's* CA root certificate on the thin client as **CA certificate**.
7. Select the desired **Session Type** in **Options**.
   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 **Custom commands** you need to supply the commands (see page 338). You can find further options in the *IGEL Universal Desktop Linux* manual.

8. Start the new session by clicking on its icon in the **Start Menu**. Alternatively, reboot the thin client. 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. **Related Configurations** provide shortcuts to these settings.

Using a Custom Configuration File

Instead of using the settings provided by *IGEL* setup you can enable a **Custom configuration file** under **Options**. 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**.

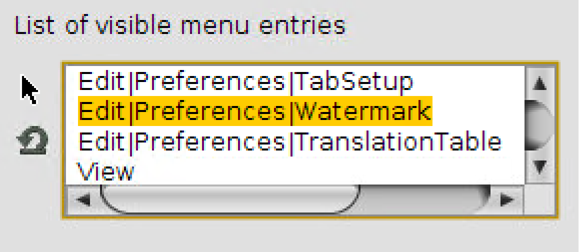
IBM iAccess

Editing 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

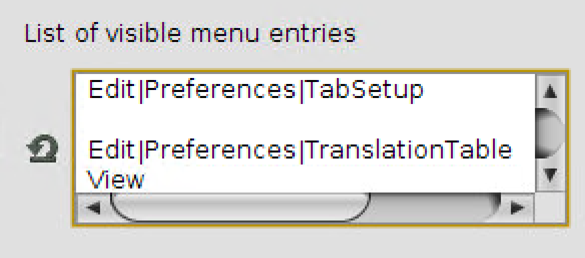
1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: `sessions.iaccess[NUMBER].options.deletemenus`). [NUMBER] is the instance number of the session you want to configure; 0, for instance, stands for the first session, 1 for the the second session, etc.
2. In the **List of visible menu entries**, using the mouse, mark the line with the entry you want to delete:



List of visible menu entries

Edit|Preferences|TabSetup
Edit|Preferences|Watermark
Edit|Preferences|TranslationTable
View

3. Press the backspace [←] or delete [Del] key.
The menu item is deleted:



List of visible menu entries

Edit|Preferences|TabSetup

Edit|Preferences|TranslationTable
View

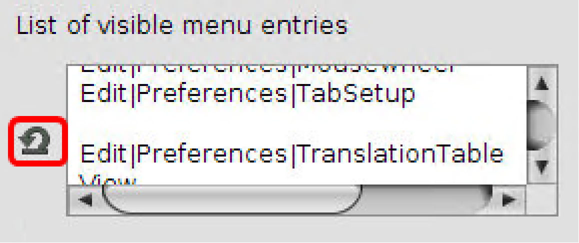
ⓘ If you delete a menu item that has subitems, the subitems will be invisible, too.

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:



List of visible menu entries

Edit|Preferences|MouseWheel
Edit|Preferences|TabSetup
Edit|Preferences|TranslationTable
View

The original menu is restored.

3. Click **Apply** or **Ok**.

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.

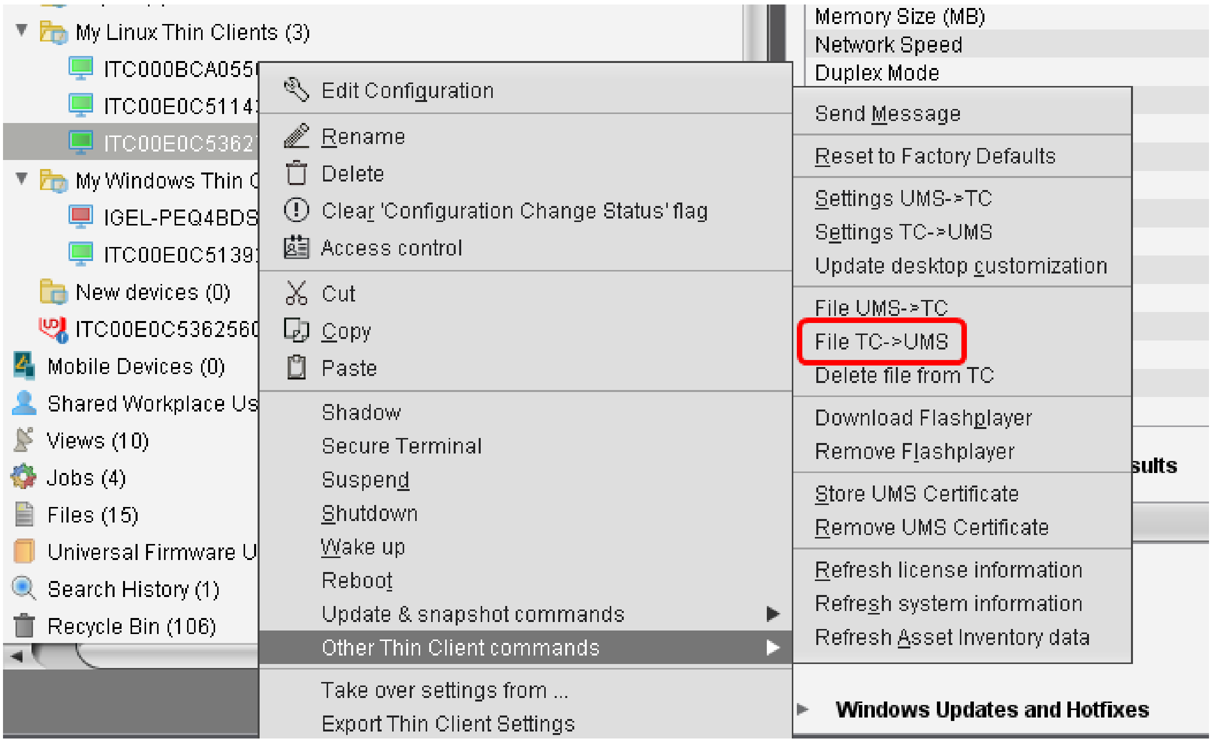
Editing the Key Mappings

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.

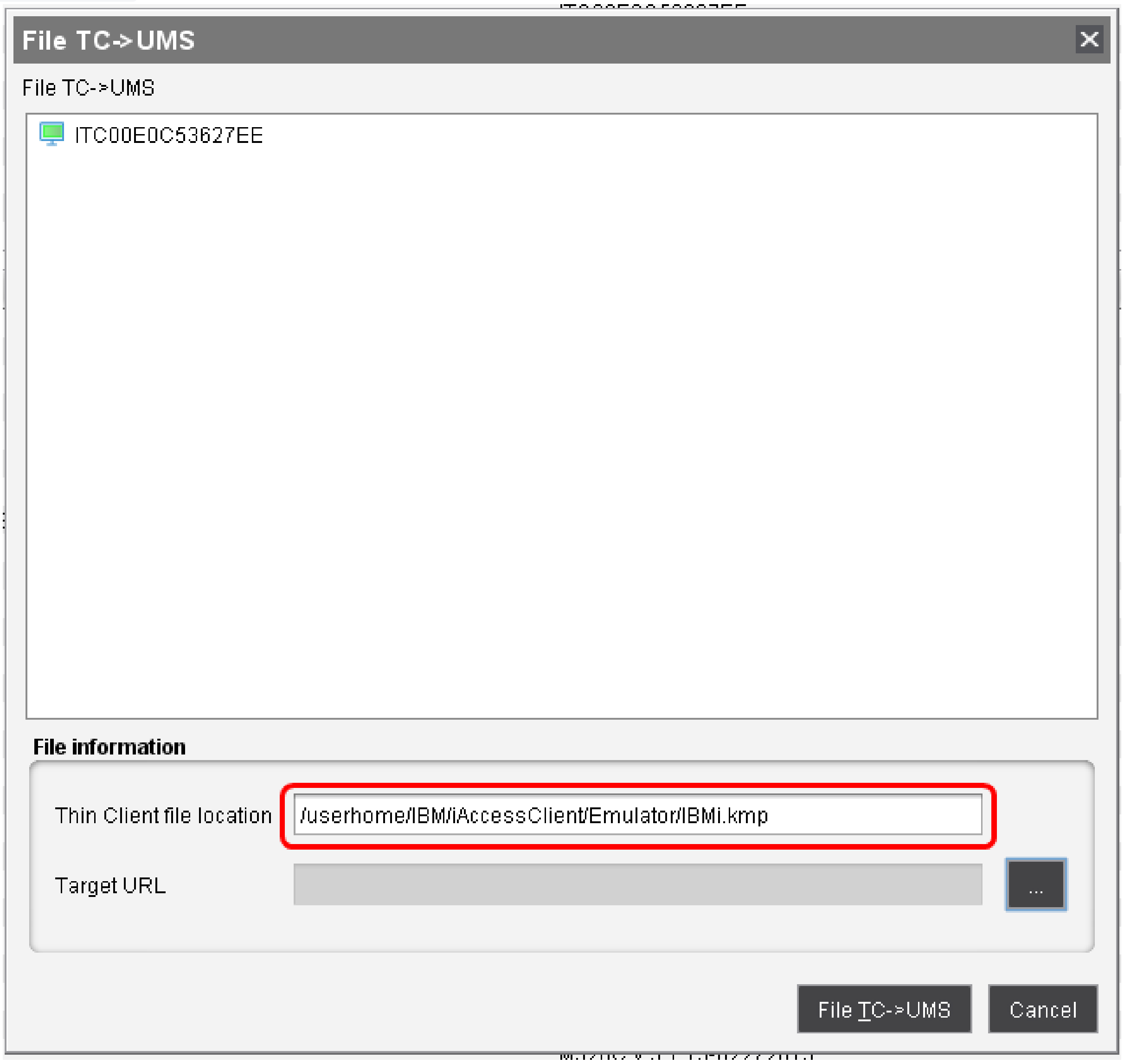
Importing the Configuration File to the UMS

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`



File TC->UMS

File TC->UMS

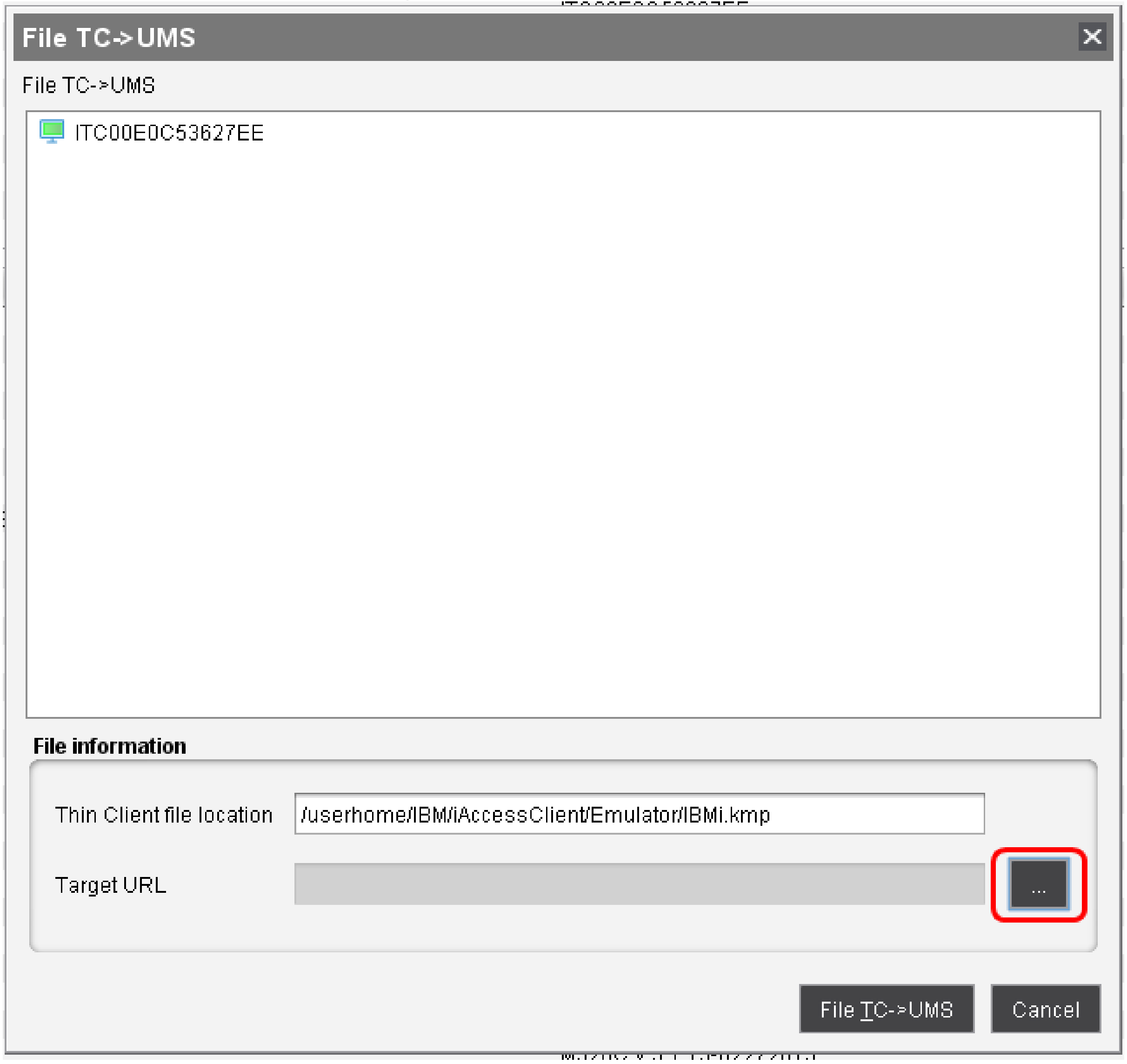
ITC00E0C53627EE

File information

Thin Client file location: /userhome/IBM/iAccessClient/Emulator/IBMi.kmp

Target URL:

4. Click ... to open the **Save** dialog.



File TC->UMS

File TC->UMS

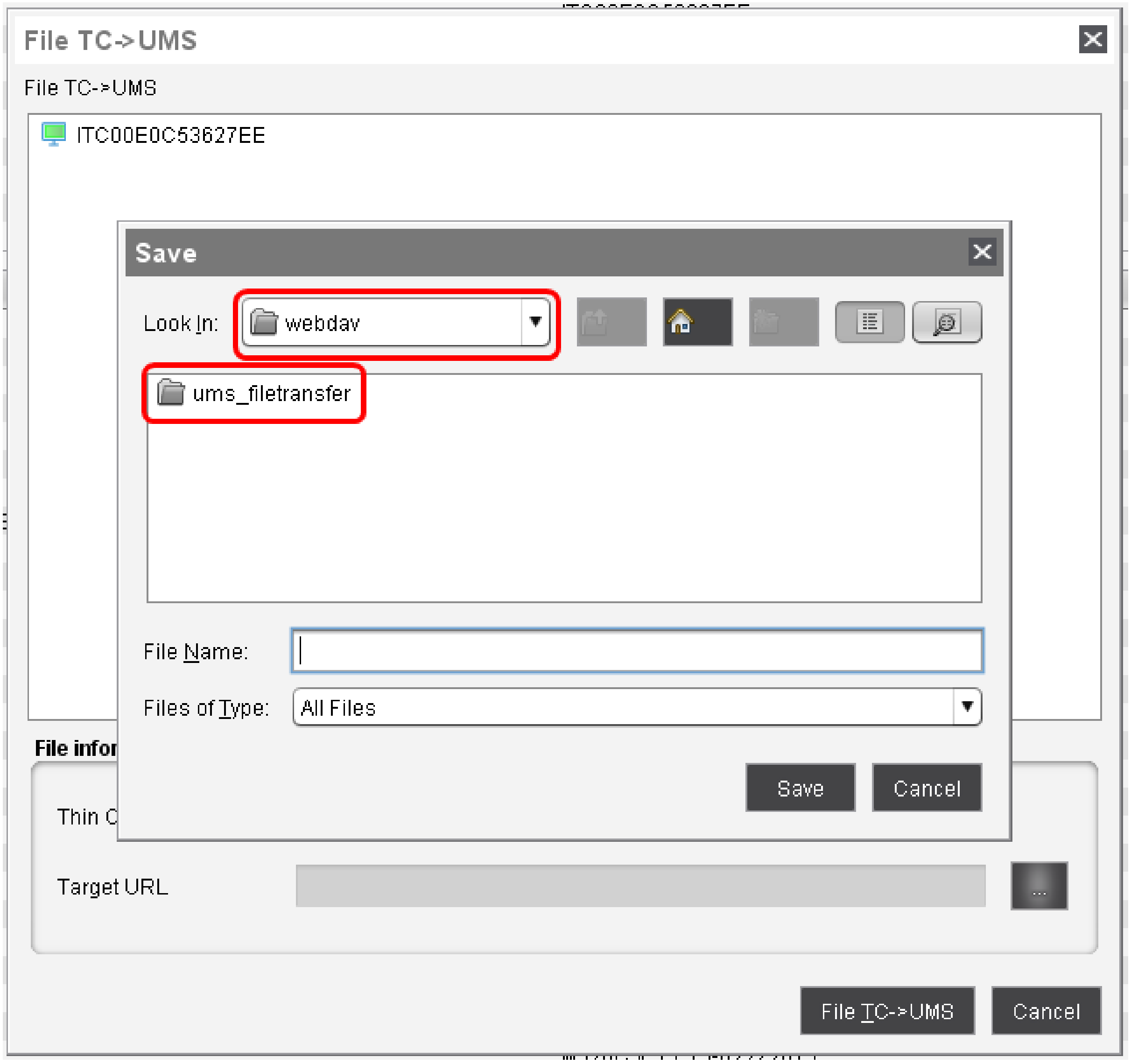
ITC00E0C53627EE

File information

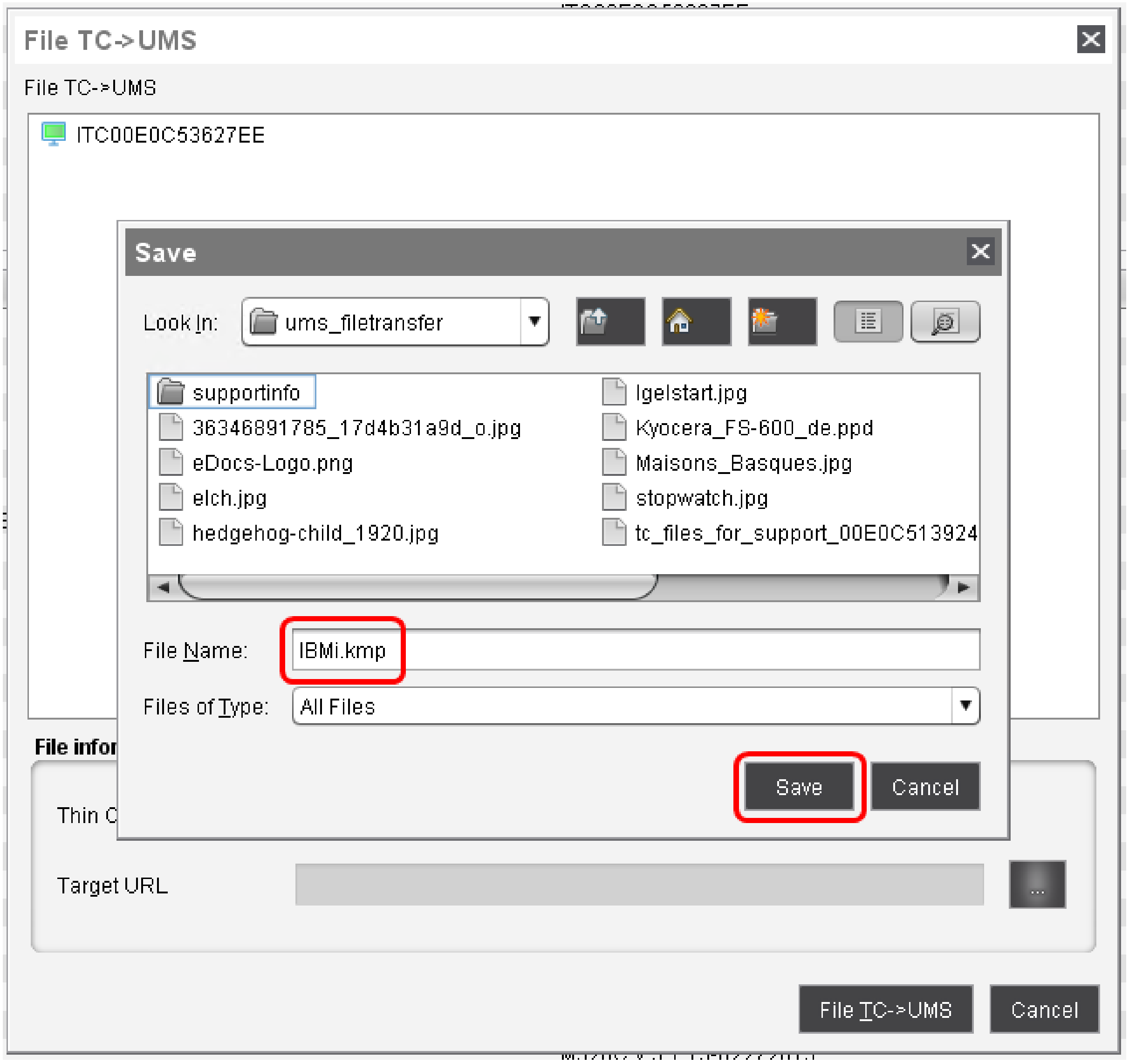
Thin Client file location: /userhome/IBM/iAccessClient/Emulator/IBMi.kmp

Target URL:

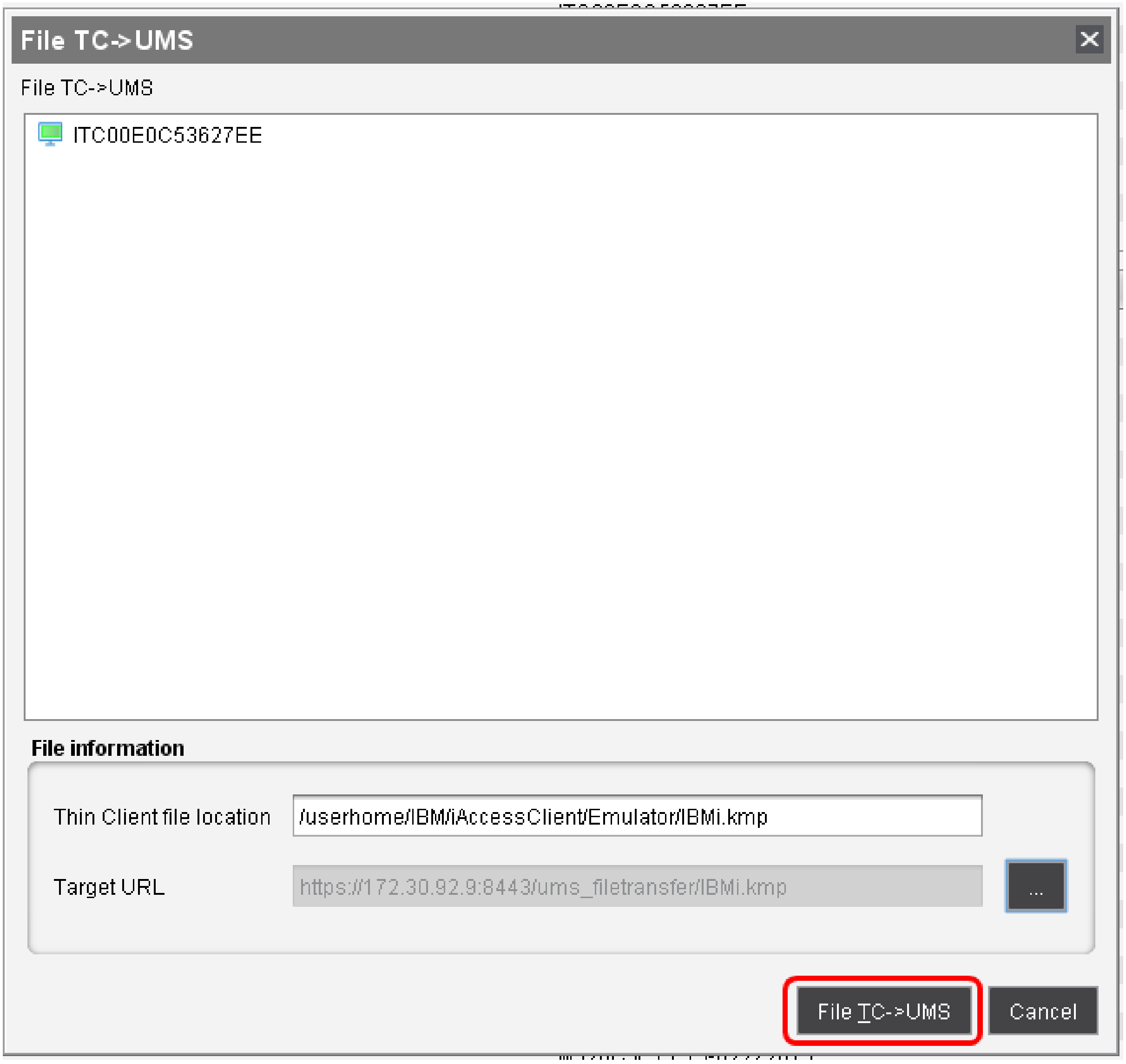
5. Choose a file location within the `ums_filetransfer` folder.



6. Under **File Name**, enter `IBMi.kmp` and click **Save**.



7. Click **TC->UMS**.



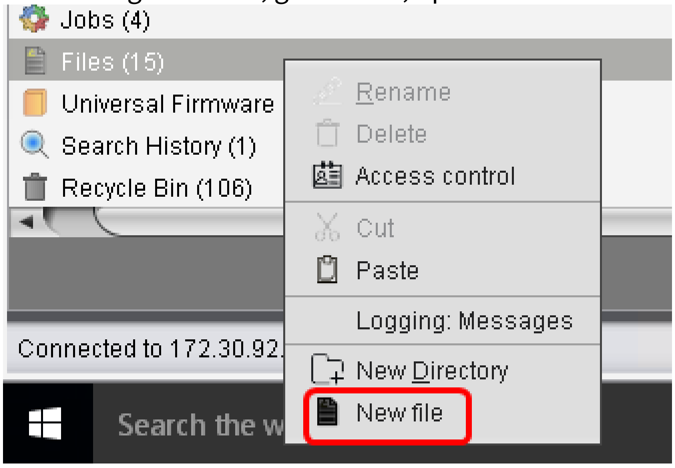
Thin Client file location: /userhome/IBM/iAccessClient/Emulator/IBMi.kmp

Target URL: https://172.30.92.9:8443/ums_filetransfer/IBMi.kmp

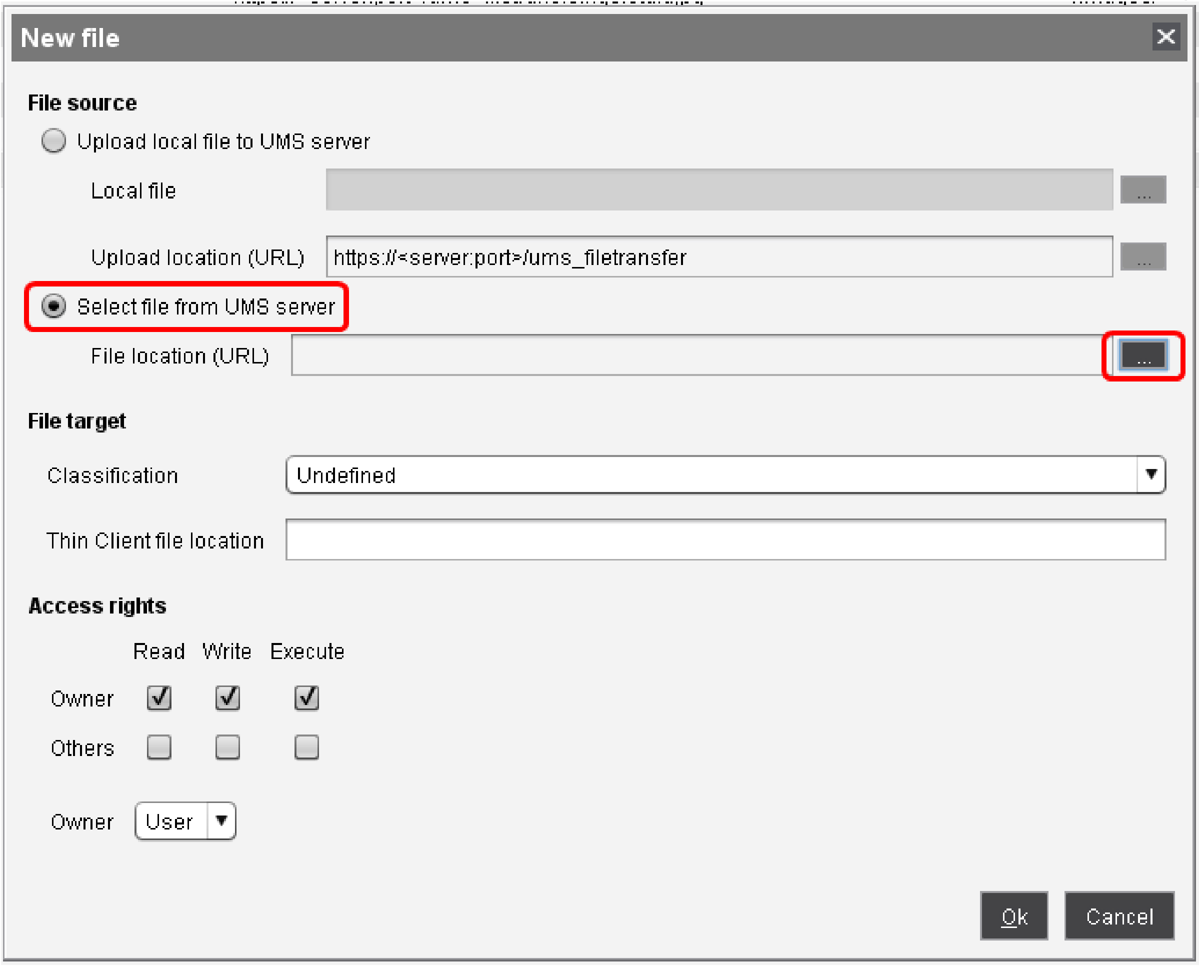
The file is stored within the UMS. Next, we will make it available as an object.

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.



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)

File target

Classification: Undefined

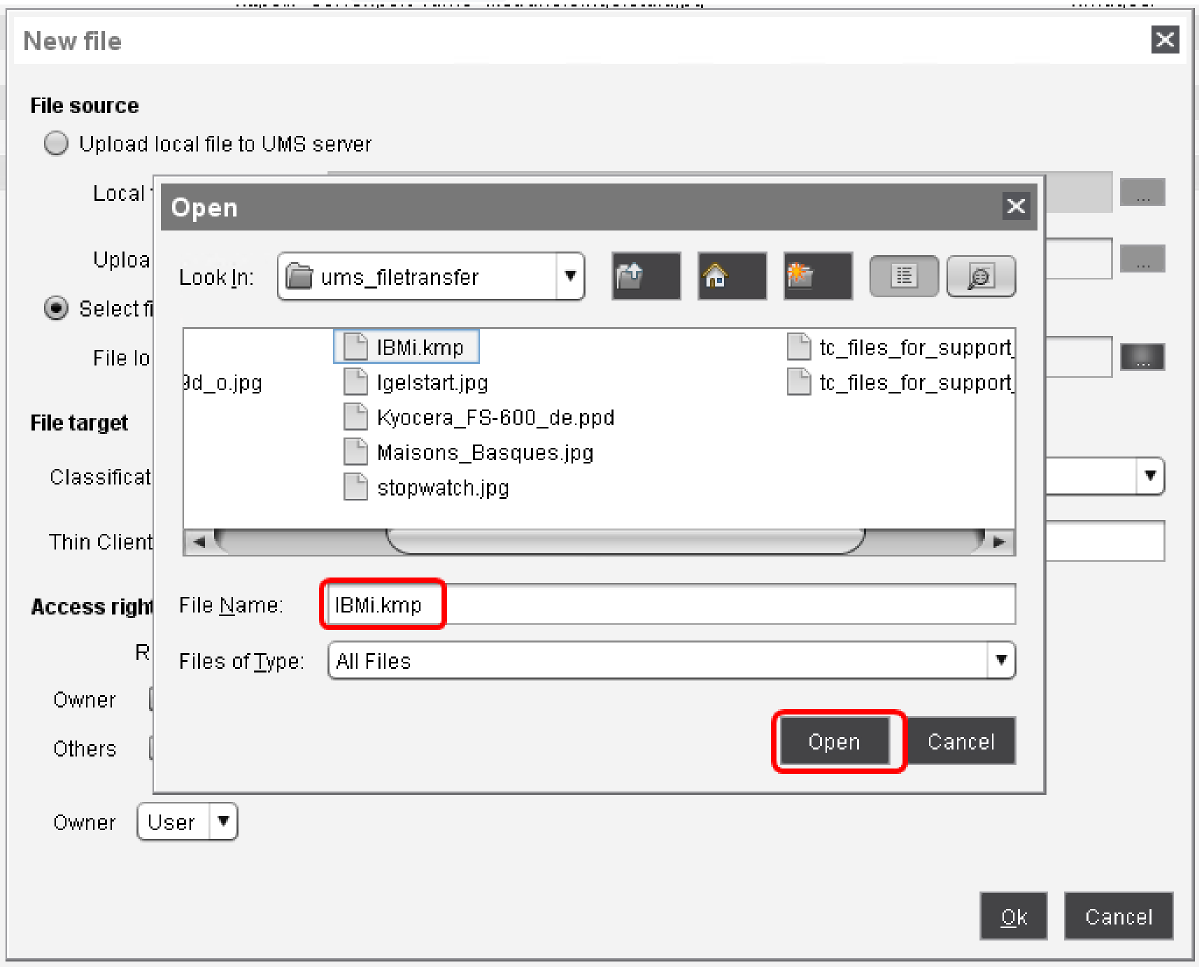
Thin Client file location

Access rights

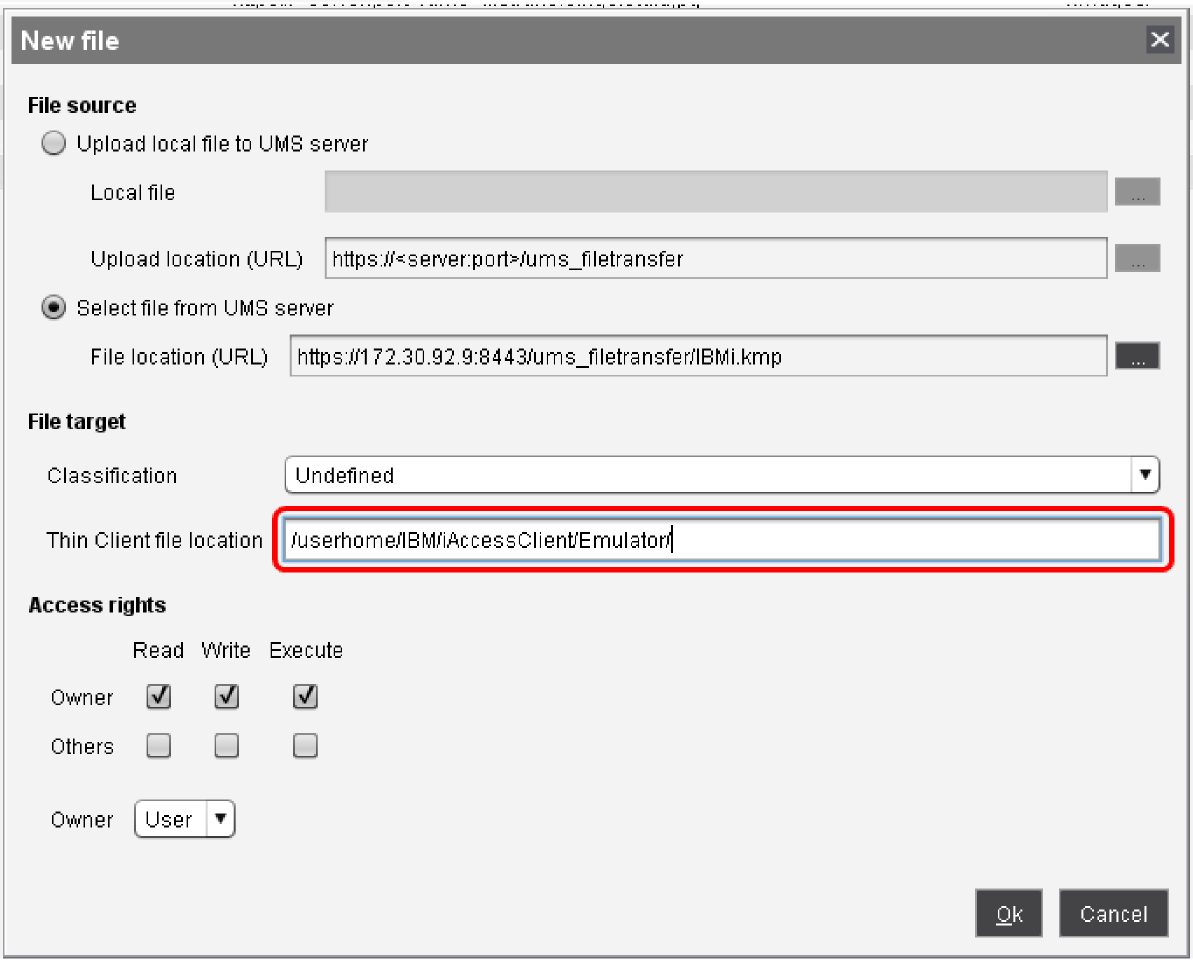
	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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/`



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

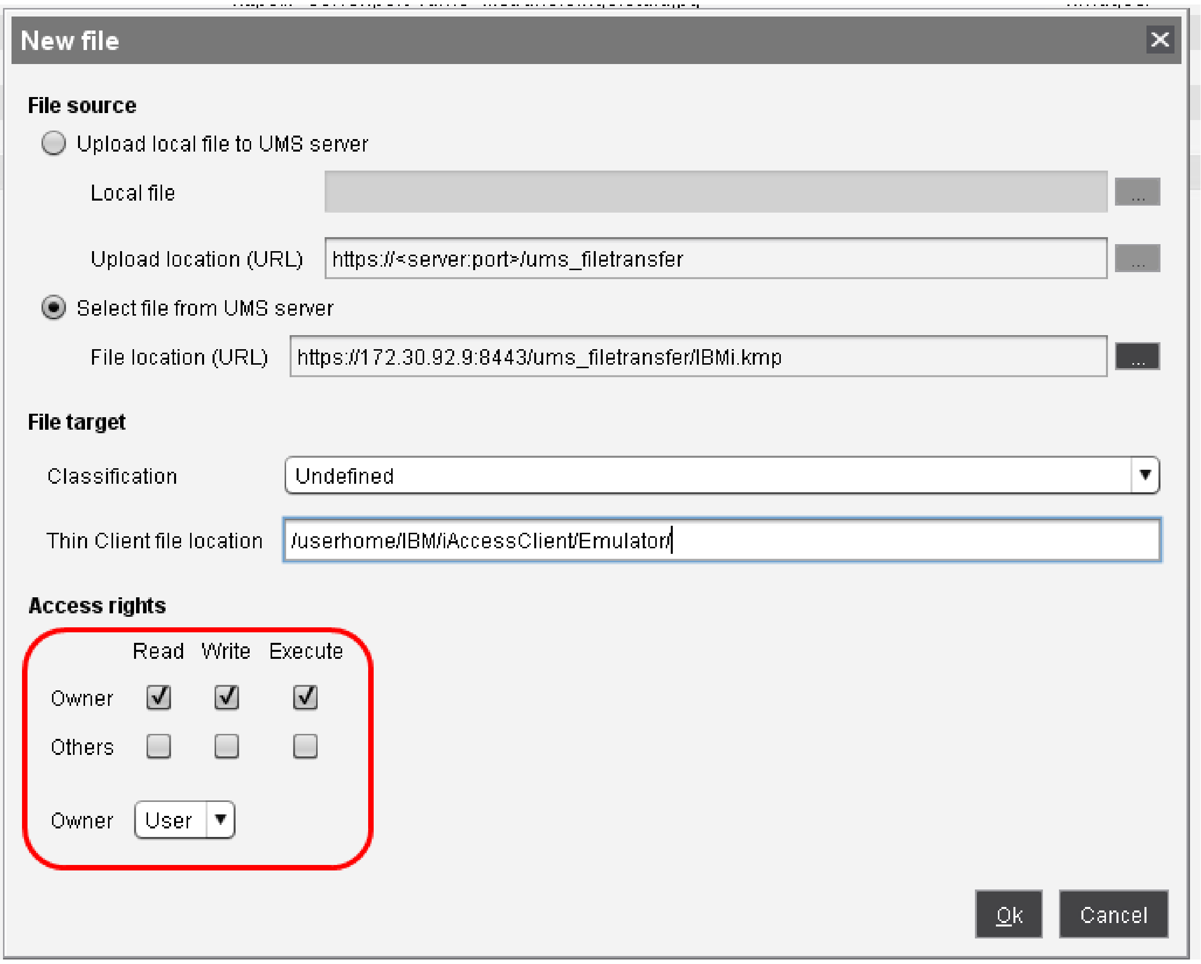
Thin Client file location: /userhome/IBM/iAccessClient/Emulator/

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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

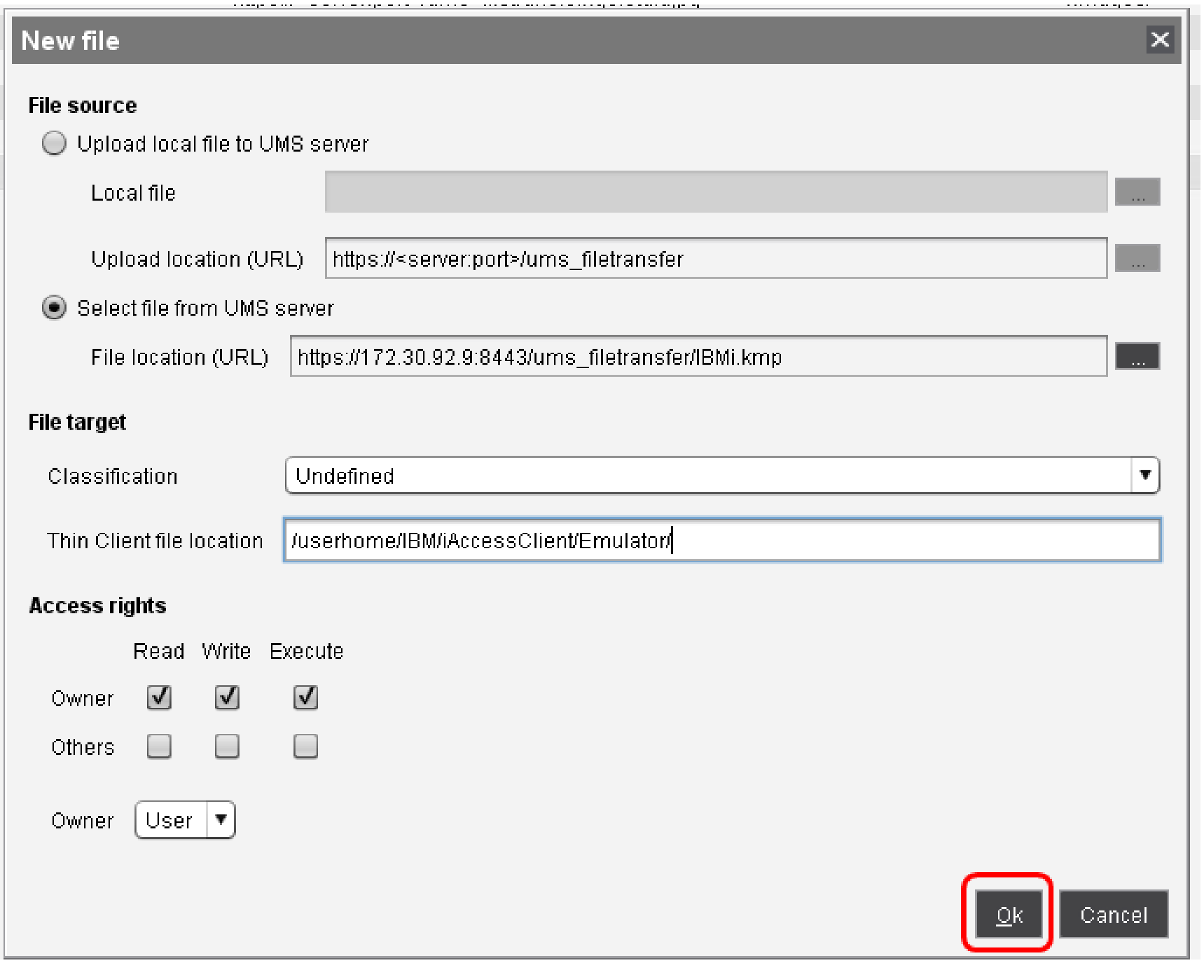
Thin Client file location /userhome/IBM/iAccessClient/Emulator/

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner User

6. Click **Ok**.



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	□	□	□

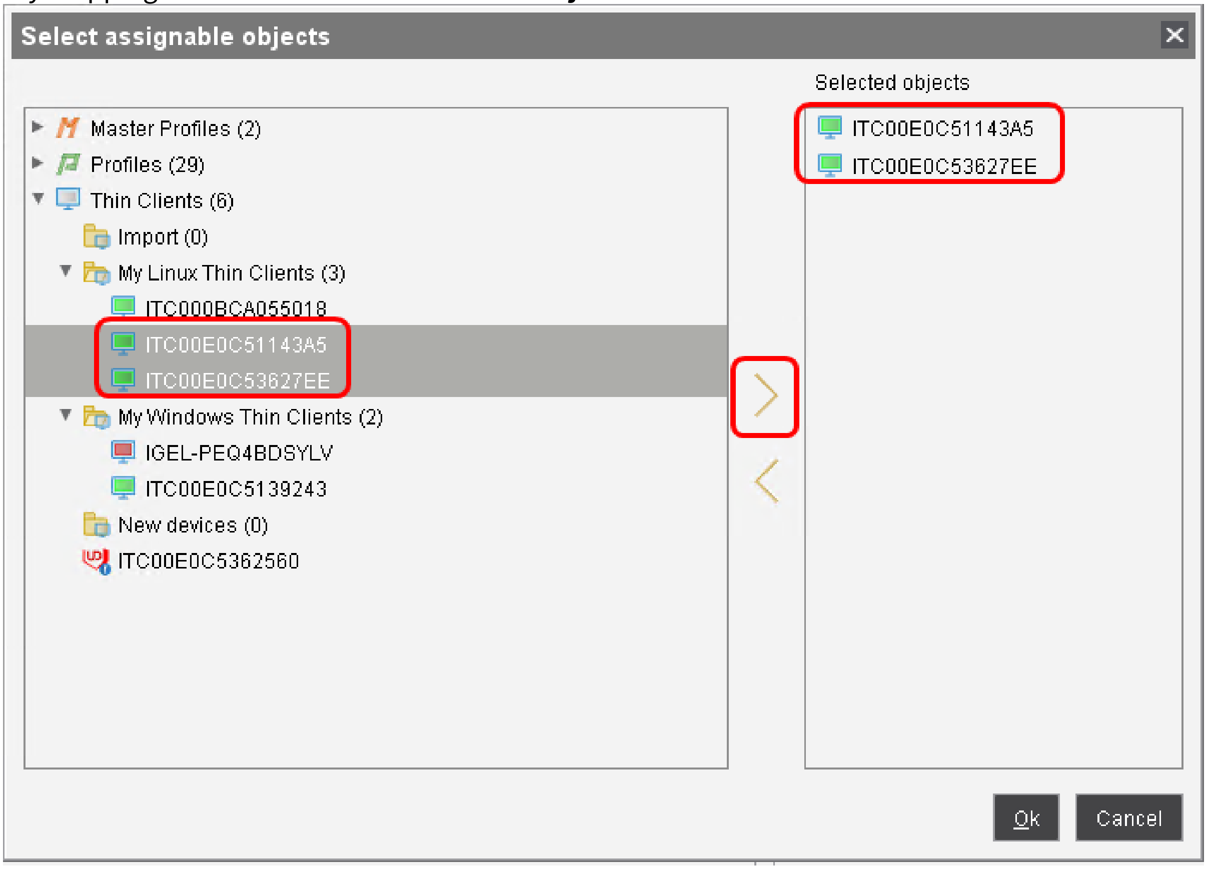
Owner User

The file object "IBMi.kmp" is created.

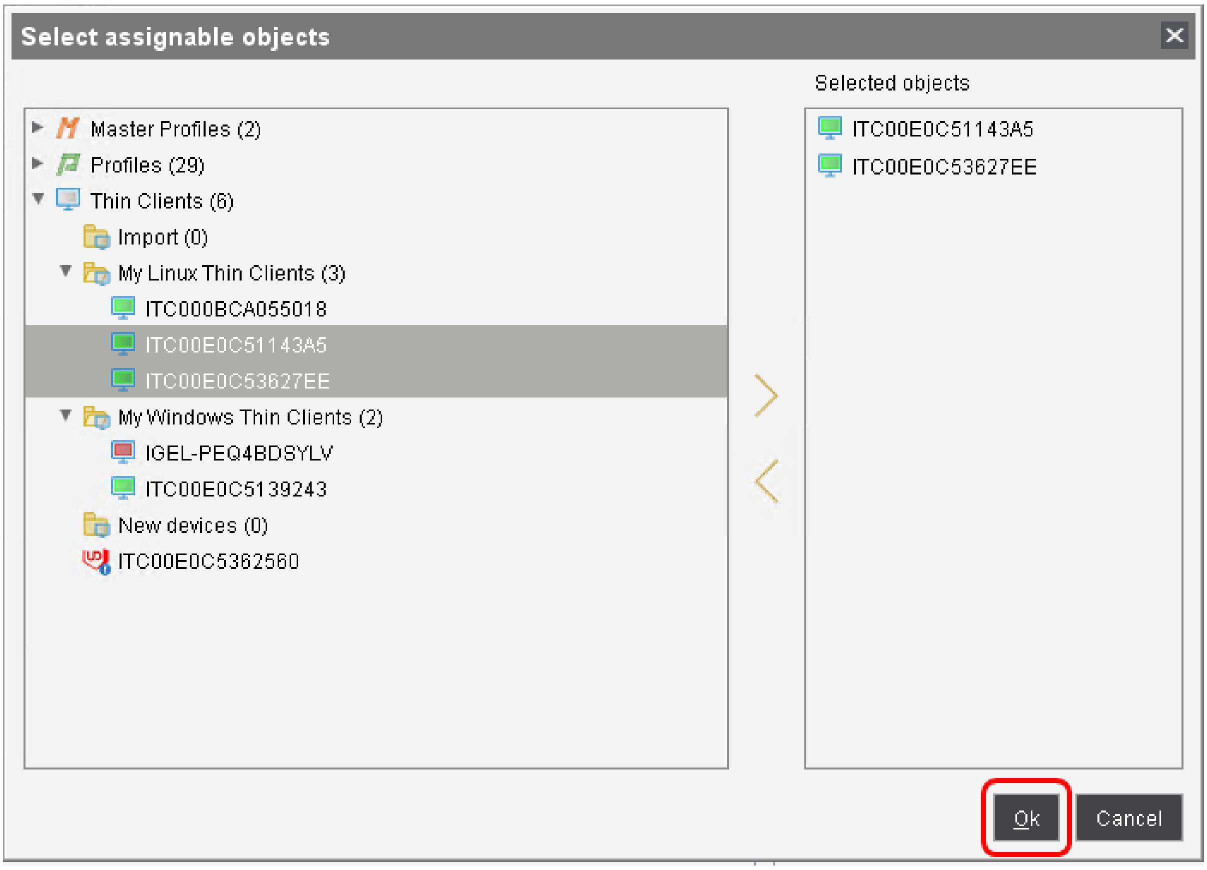
Assigning the File Object to Thin Clients

1. In the navigation tree, select the file object "IBMi.kmp" and click □ in the **Assigned objects** area (upper right).

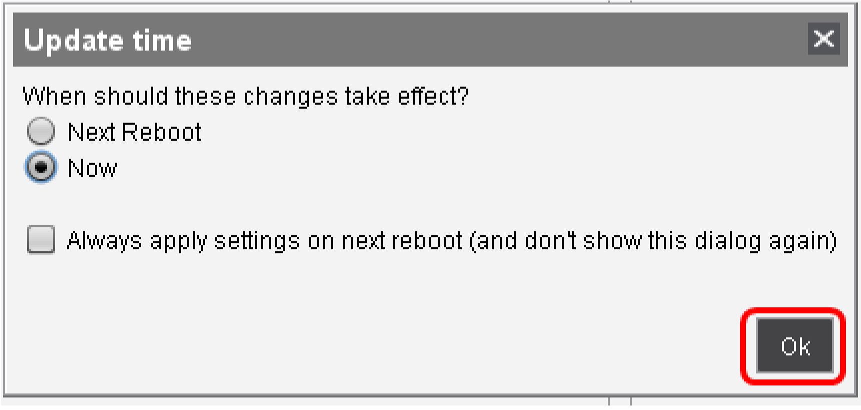
2. In the **Select assignable objects** dialog, select the thin clients to which you want to assign the new key mapping and add them to the **Selected objects** area.



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**.



Update time

When should these changes take effect?

○ Next Reboot

● Now

□ Always apply settings on next reboot (and don't show this dialog again)

The file is transferred to the thin clients.

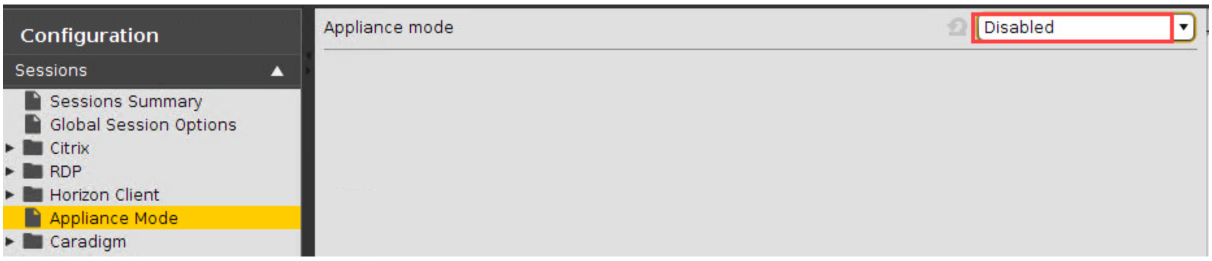
Imprivata

Imprivata: 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.

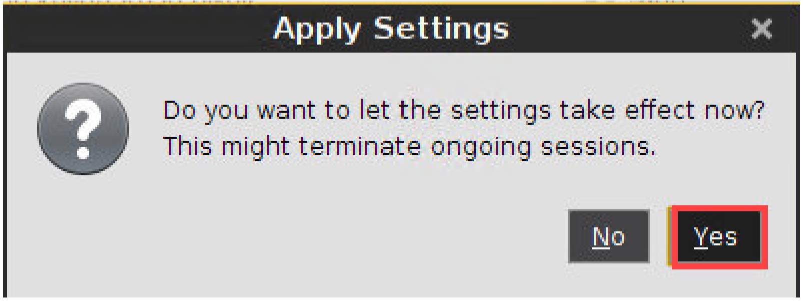
If you already have a valid appliance running and want to delete the Imprivata data partition, take the following steps:

1. In the IGEL Setup, go to **Sessions > Appliance Mode.**
2. Set **Appliance mode** to "**Disabled**".



Appliance mode: Disabled

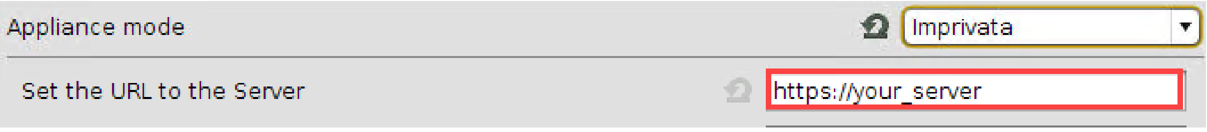
3. Click **Ok** to save the setting.
4. Click **Yes** to confirm the **Apply Settings** dialog.



Do you want to let the settings take effect now?
This might terminate ongoing sessions.

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.



Appliance mode: Imprivata

Set the URL to the Server: https://your_server

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 and Horizon Client Session).

> ⓘ **IMPRIVATA_RDP** and **IMPRIVATA_VMware** will be shown in the IGEL Setup when **Imprivata** is selected under **Setup > Sessions > Appliance Mode**, see Imprivata.

However, the changes under the following subsections will be ignored:

Imprivata_VMware Session

- **Connection Settings**

Imprivata_RDP Session

- **Server**
- **Logon**

SSH

Enable Weaker Algorithms in the Built-in OpenSSH Server

Problem

You are trying to connect to IGEL Linux's built-in OpenSSH server 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

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 363) and/or Enable Weaker Algorithms in the Built-in OpenSSH Server (see page 362).

Amazon WorkSpaces – Teradici PCoIP Sessions

As of IGEL OS 11.06, you can configure an Amazon WorkSpaces session under **Sessions > Amazon > WorkSpaces > Amazon WorkSpaces Session**, see Amazon WorkSpaces (see page 365).

Alternatively, you can use Amazon WorkSpaces via Teradici PCoIP. The articles below will show you how you can do that.

- Connecting IGEL OS Devices with Amazon WorkSpaces via PCoIP (see page 366)
- Use IGEL Setup for Configuration – Connecting with AWS via PCoIP (see page 370)
- Broker Types – Amazon WorkSpaces (see page 372)
- How Can I Use H.264 Acceleration in a Teradici PCoIP Session? (see page 373)

Connecting IGEL OS Devices with Amazon WorkSpaces via PCoIP

You can set up and use IGEL OS devices via PCoIP with Amazon WorkSpaces.

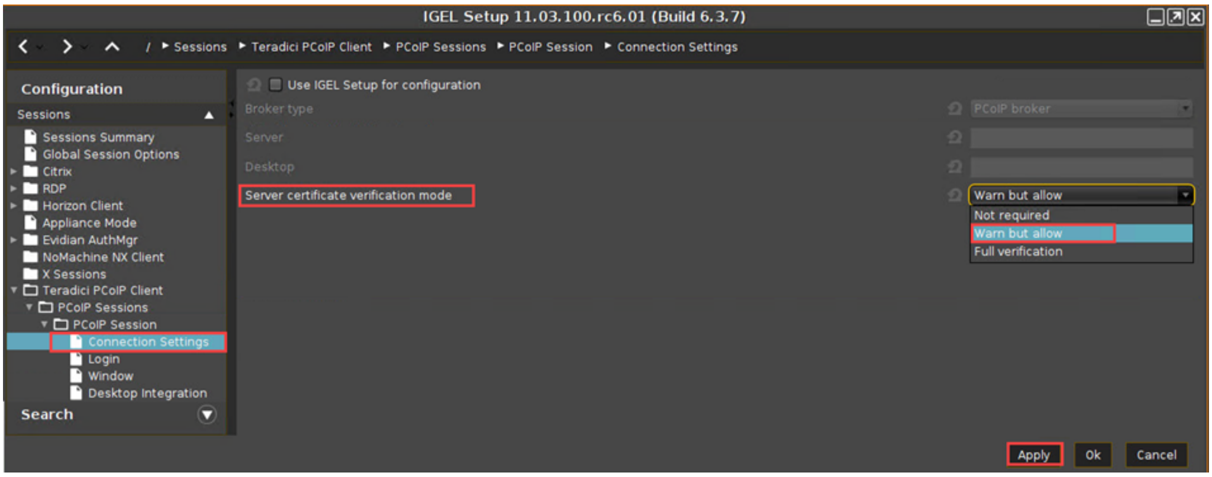
Set Up the Device Connection

Before you connect the device to the 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 needed for your particular environment.

Session Connection

To set the session connection:

1. In the IGEL Setup, go to **Sessions > Teradici 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".



IGEL Setup 11.03.100.rc6.01 (Build 6.3.7)

/ ▸ Sessions ▸ Teradici PCoIP Client ▸ PCoIP Sessions ▸ PCoIP Session ▸ Connection Settings

□ Use IGEL Setup for configuration

Broker type: PCoIP broker

Server:

Desktop:

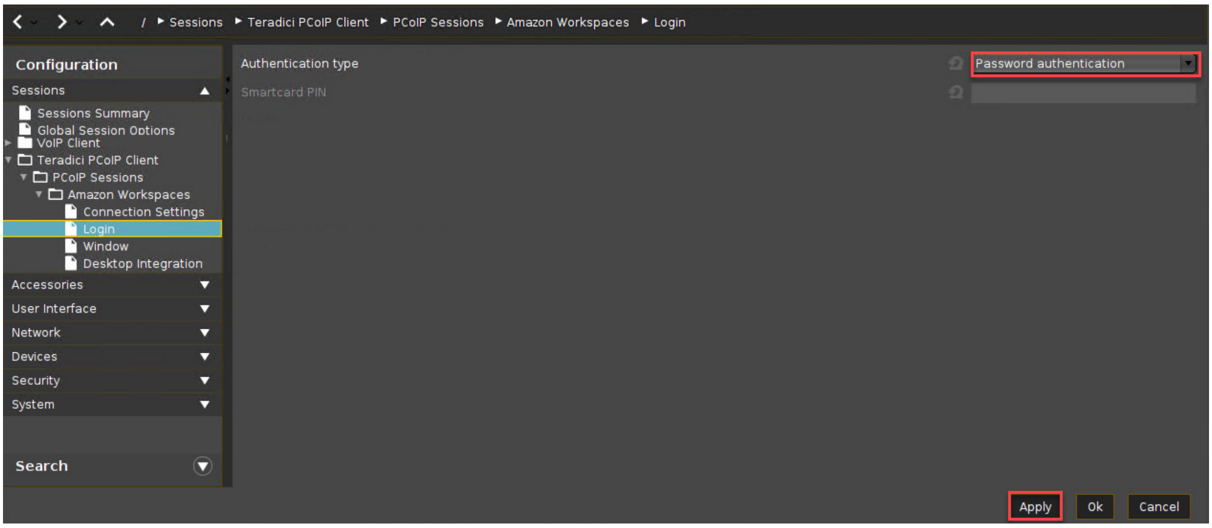
Server certificate verification mode: Warn but allow

> ⓘ If you do not enable **Use IGEL Setup for configuration**, you have to enter the host address or code in the Teradici PCoIP Client login window. See the screenshot under "Connecting to Amazon WorkSpaces".
> If you activate **Use IGEL Setup for configuration**, see Use IGEL Setup for Configuration – Connecting with AWS via PCoIP (see page 370).

> ⓘ For more information about the connection with the **Broker type** "PCoIP broker" or "Hardhost", see Broker Types – Amazon WorkSpaces (see page 372).

5. Click **Apply**.

6. Go to **Login** and set **Authentication type** to "Password authentication". Afterwards, click **Apply**.

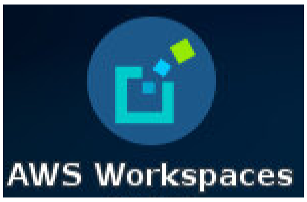


Authentication type: Password authentication

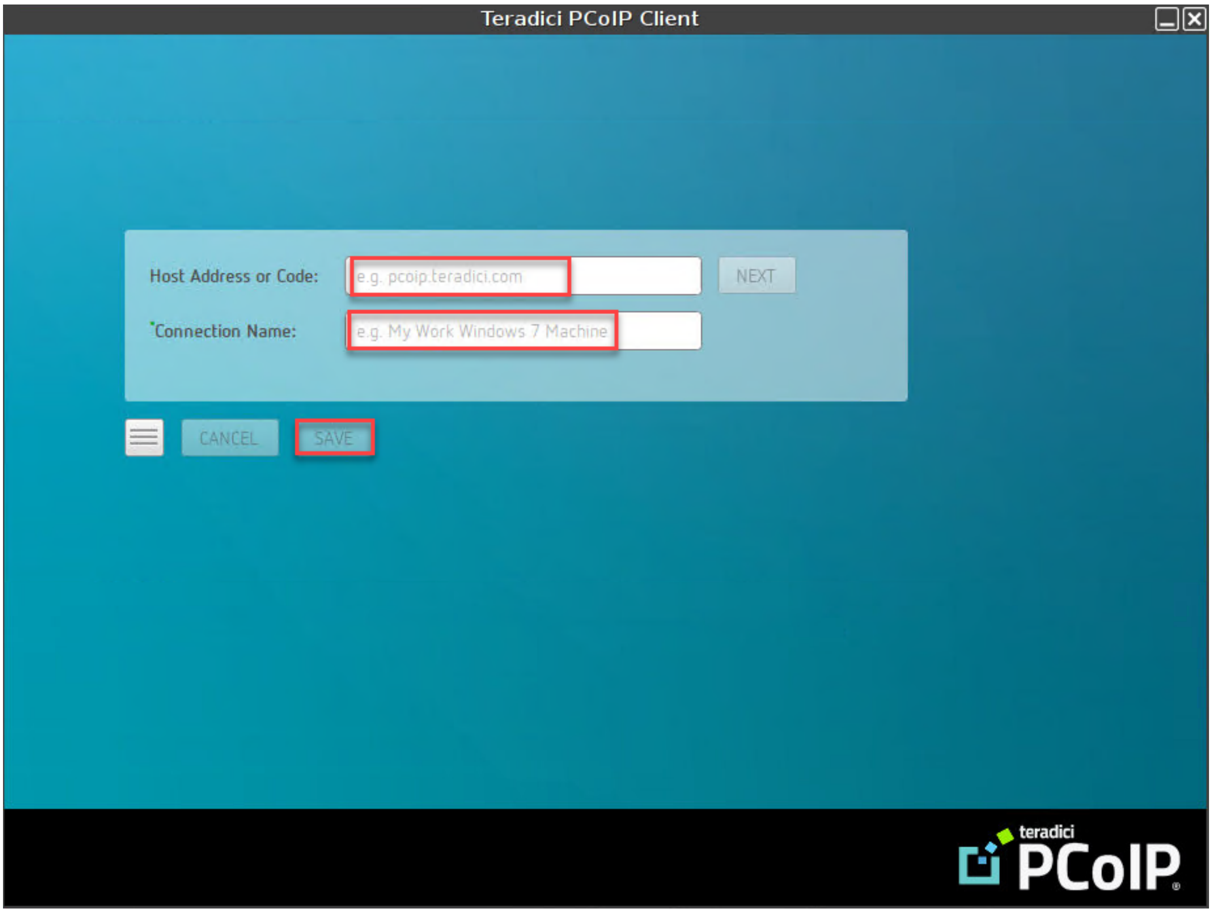
Smartcard PIN

Connecting to Amazon WorkSpaces

1. Double-click on the **Amazon WorkSpaces** icon on your desktop.



The **Teradici 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 which combines two different components (factors) that are independent from 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:

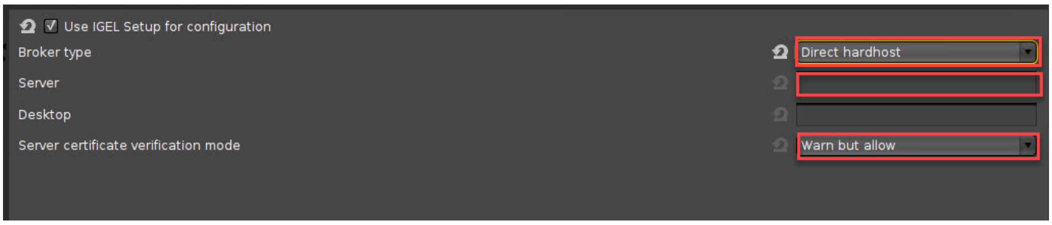
Sorry, the widget is not supported in this export.
But you can reach it using the following URL:
https://www.youtube.com/watch?v=NDQxTEKLPZE

Use IGEL Setup for Configuration – Connecting with AWS via PCoIP

Configuring 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 AWS WorkSpace's Registration Code as **Server**.
        - Set **Server certificate verification mode** to "Warn but allow".



☑ Use IGEL Setup for configuration

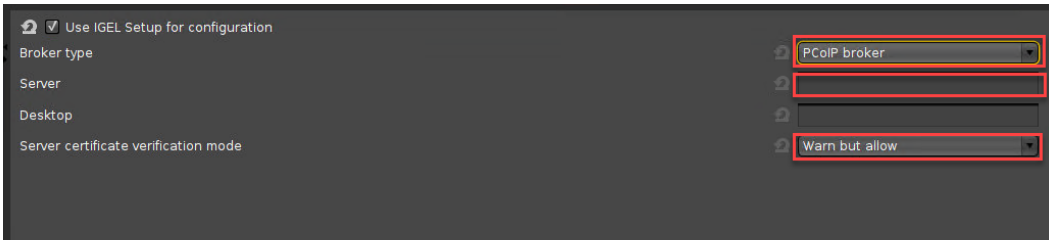
Broker type: Direct hardhost

Server:

Desktop:

Server certificate verification mode: 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".



☑ Use IGEL Setup for configuration

Broker type: PCoIP broker

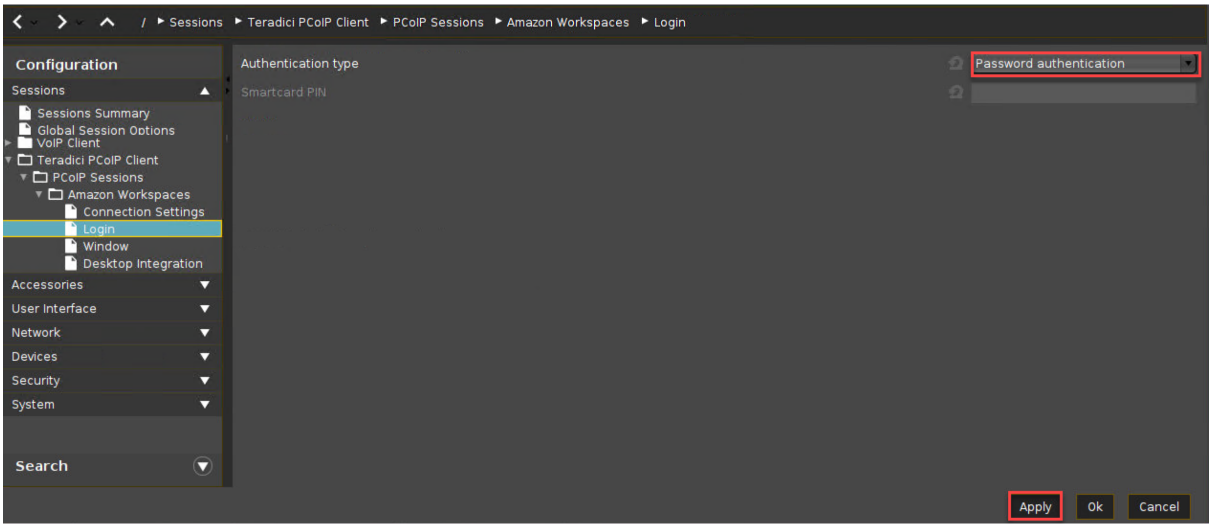
Server:

Desktop:

Server certificate verification mode: Warn but allow

> For more information about the broker types, see Broker Types – Amazon WorkSpaces (see page 372).

3. Click **Apply**.
4. Go to **Login** and set **Authentication type** to "Password authentication".
5. Click **Apply**.



Authentication type: Password authentication

Smartcard PIN

Connecting to Amazon WorkSpaces

1. Double-click on the **AWS WorkSpaces** icon on your desktop.

2. The Teradici 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[20].

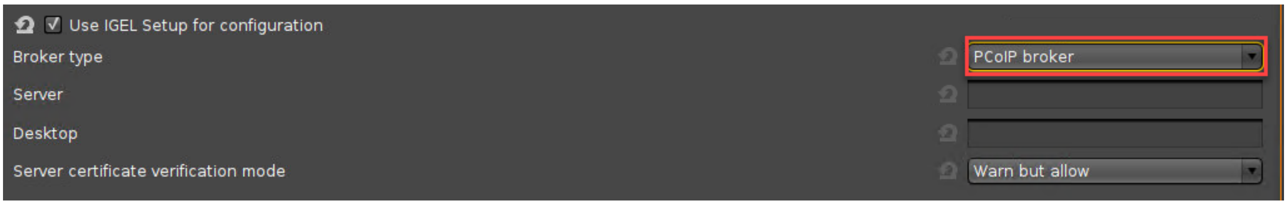
[20] https://aws.amazon.com/de/?nc2=h_lg

Broker Types – Amazon WorkSpaces

You can choose between two broker types with which you connect to Amazon WorkSpaces.

PCoIP Broker

PCoIP broker is a resource manager that dynamically assigns host PCs to zero clients based on the identity of the user establishing 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 are configured to always connect to the same host (i.e., a static one-to-one pairing), then a connection broker is not required.



☑ Use IGEL Setup for configuration

Broker type: PCoIP broker

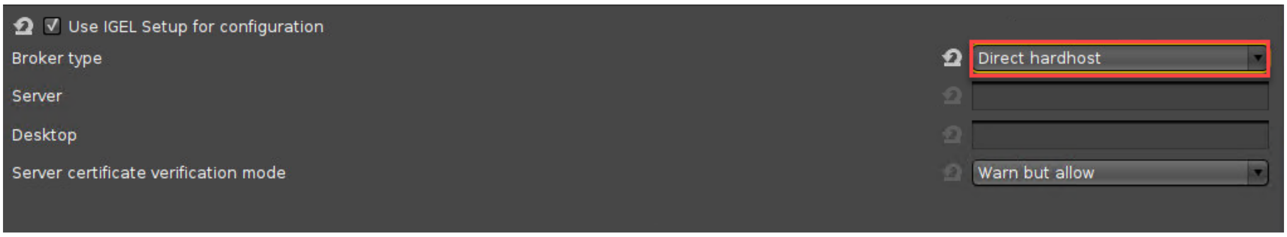
Server:

Desktop:

Server certificate verification mode: Warn but allow

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 Service Location Protocol (SLP) to discover a host. You can also configure clients to automatically reconnect to a host when a session is lost.



☑ Use IGEL Setup for configuration

Broker type: Direct hardhost

Server:

Desktop:

Server certificate verification mode: Warn but allow

How Can I Use H.264 Acceleration in a Teradici PCoIP Session?

Question

How must I configure the client and the server to get H.264 acceleration in a Teradici PCoIP Session?

Environment

This article is valid for the following environment:

- IGEL OS 11.04 or higher
- UMS 6.04 or higher
- Teradici 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.

- Login Enterprise Launcher in IGEL OS (see page 375)
- Getting the Secret for Login Enterprise Launcher (see page 380)
- Using the Login Enterprise Launcher within a VMware Horizon Session (see page 383)

Login Enterprise Launcher in IGEL OS

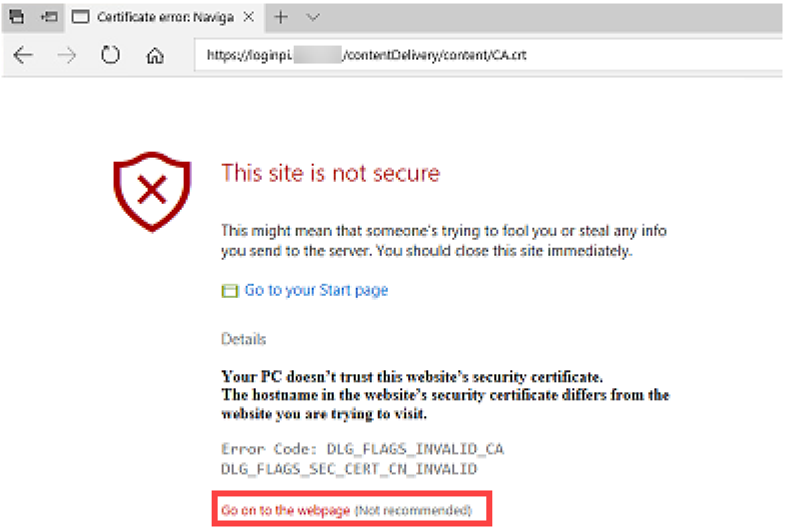
Requirements

- 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 `https://loginpi.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`.


Certificate error: Naviga
https://loginpi.[redacted]/contentDelivery/content/CA.crt

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

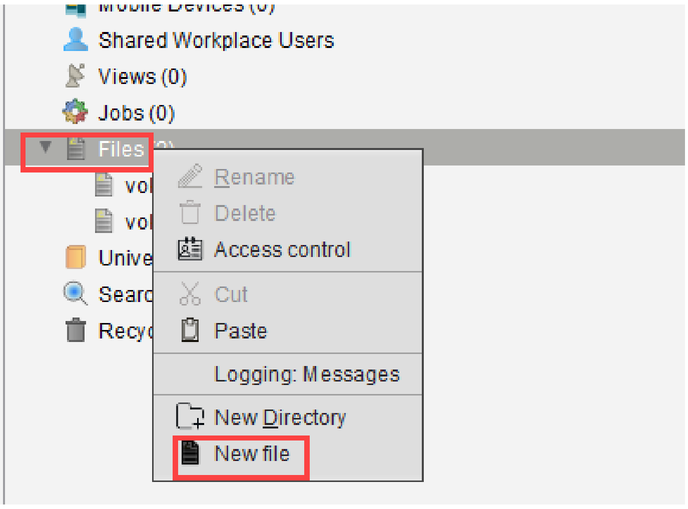
Details

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

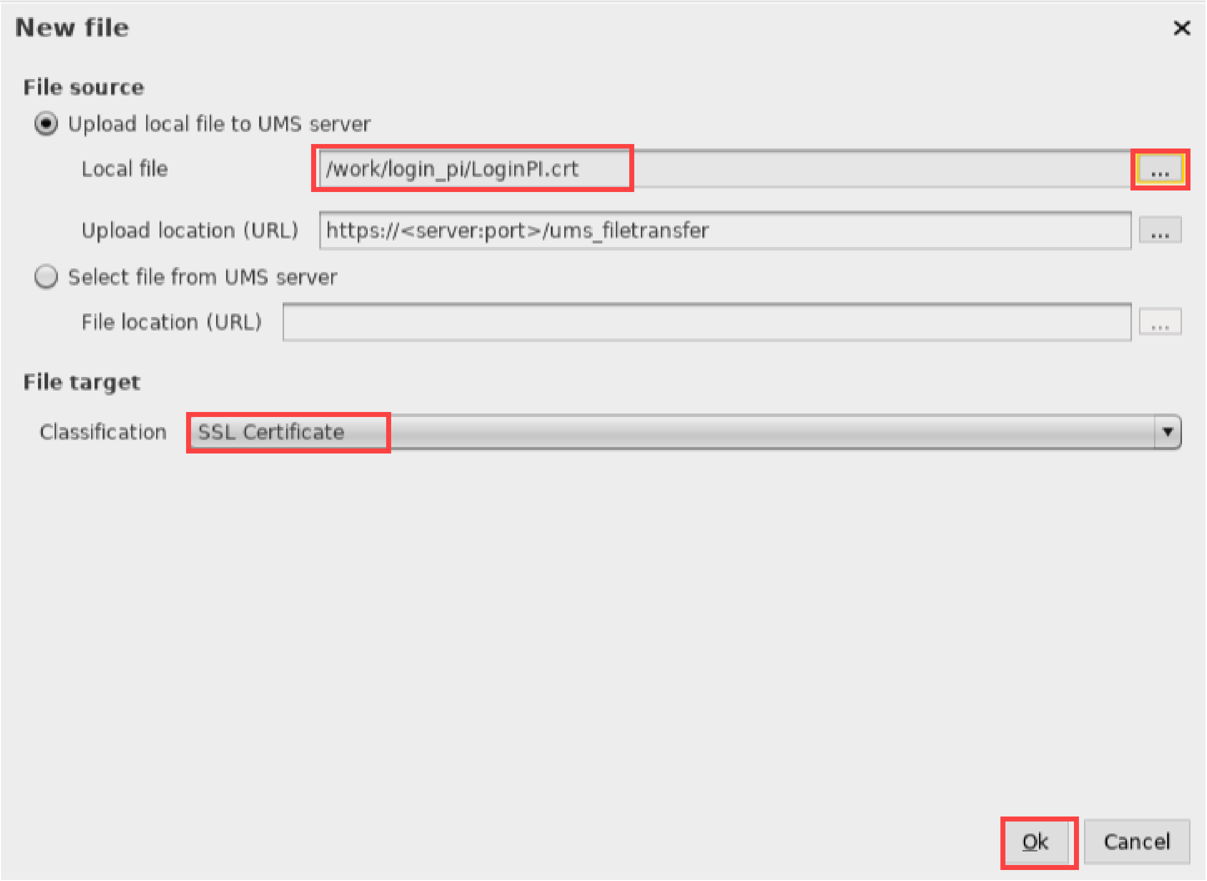
Go on to the webpage (Not recommended)

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**.


New file

File source

● Upload local file to UMS server

Local file: /work/login_pi/LoginPI.crt

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

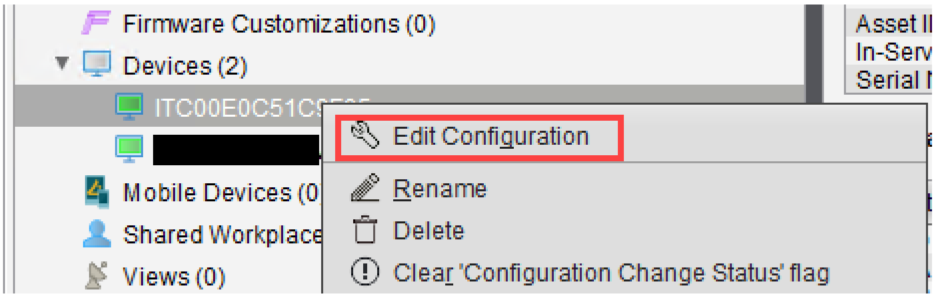
File location (URL):

File target

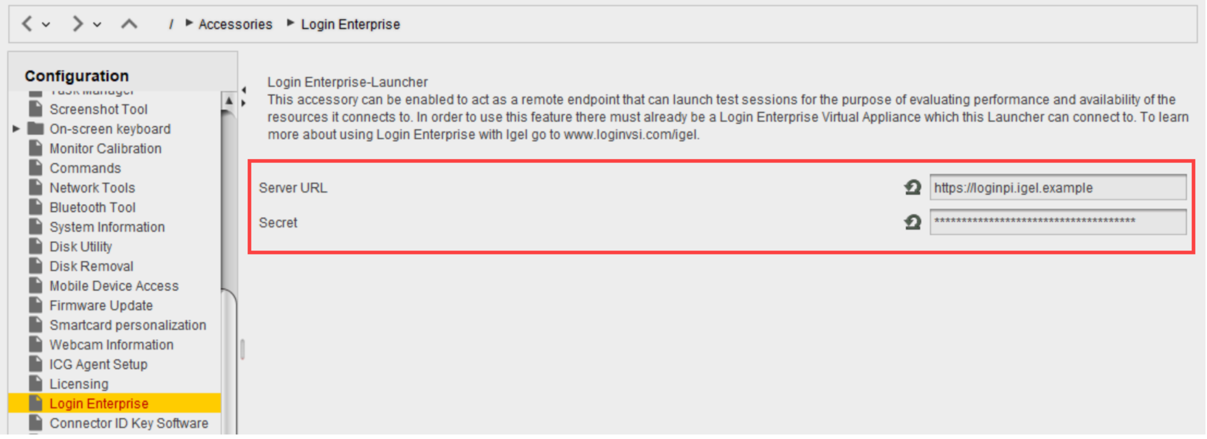
Classification: SSL Certificate

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.



2. Go to **Accessories > Login Enterprise**.
3. Enter the **Server URL** of your Login Enterprise server.
4. Enter the **Secret**, see Getting the Secret for Login Enterprise Launcher (see page 380).



Login Enterprise-Launcher
This accessory can be enabled to act as a remote endpoint that can launch test sessions for the purpose of evaluating performance and availability of the resources it connects to. In order to use this feature there must already be a Login Enterprise Virtual Appliance which this Launcher can connect to. To learn more about using Login Enterprise with Igel go to www.loginvsi.com/igel.

Server URL https://loginpi.igel.example

Secret ************************************

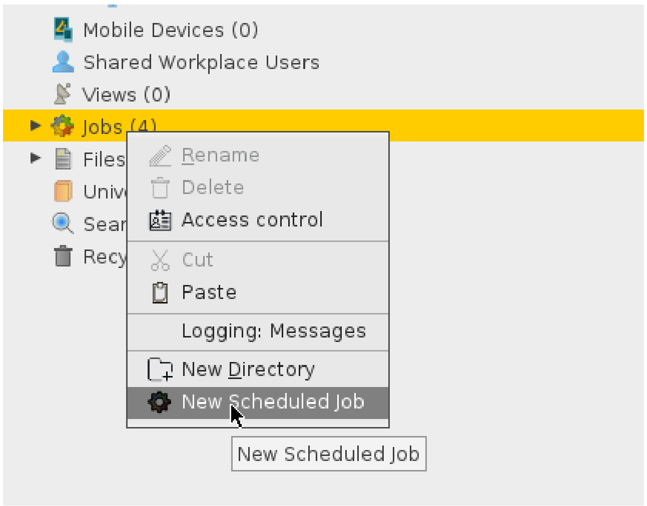
5. Save the settings.

If you want to use the Login Enterprise Launcher within a VMware session, see Using the Login Enterprise Launcher within a VMware Horizon Session (see page 383).

Starting the Login Enterprise Launcher from the UMS

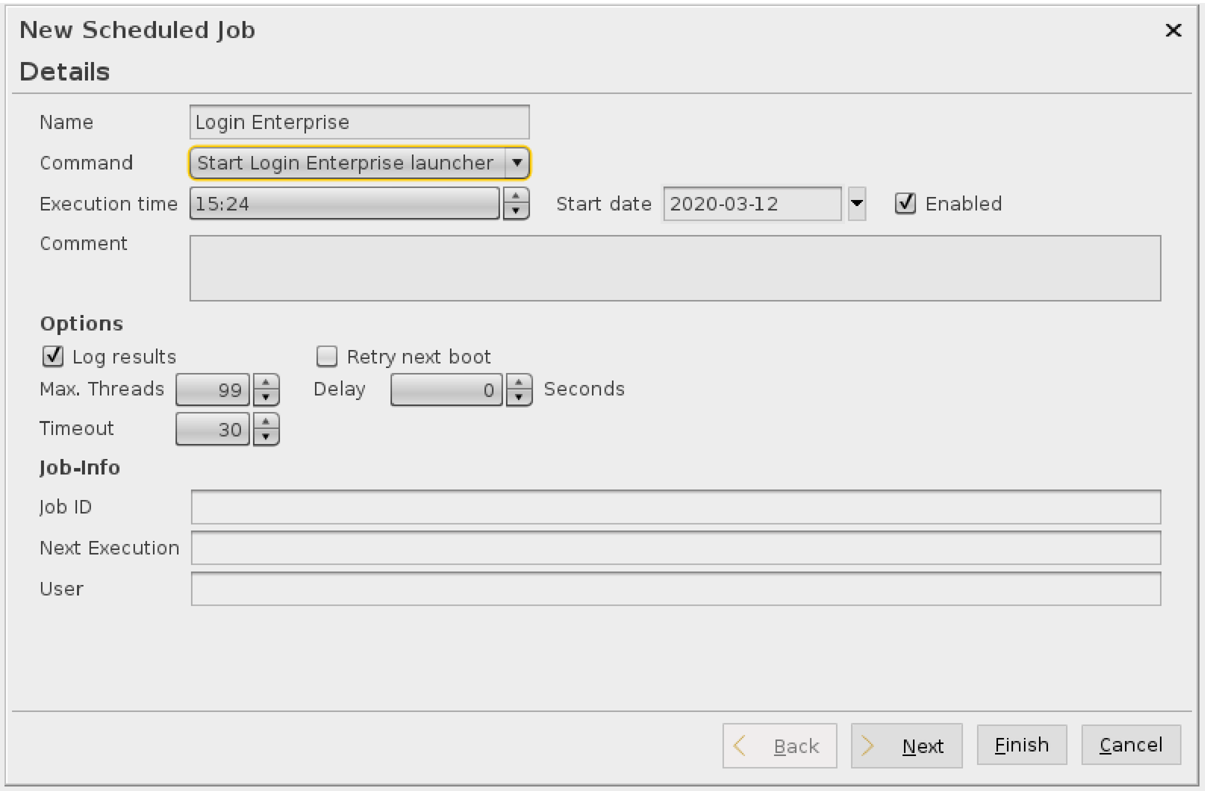
After the Login Enterprise server has been set up, you can create a job in the UMS for the automatic start of your Login Enterprise Launcher at a defined time.

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**.



New Scheduled Job

Details

Name	Login Enterprise
Command	Start Login Enterprise launcher
Execution time	15:24
Start date	2020-03-12
☑ Enabled	
Comment	

Options

☑ Log results

□ Retry next boot

Max. Threads	99
Delay	0 Seconds
Timeout	30

Job-Info

Job ID	
Next Execution	
User	

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/ and the following webinar:

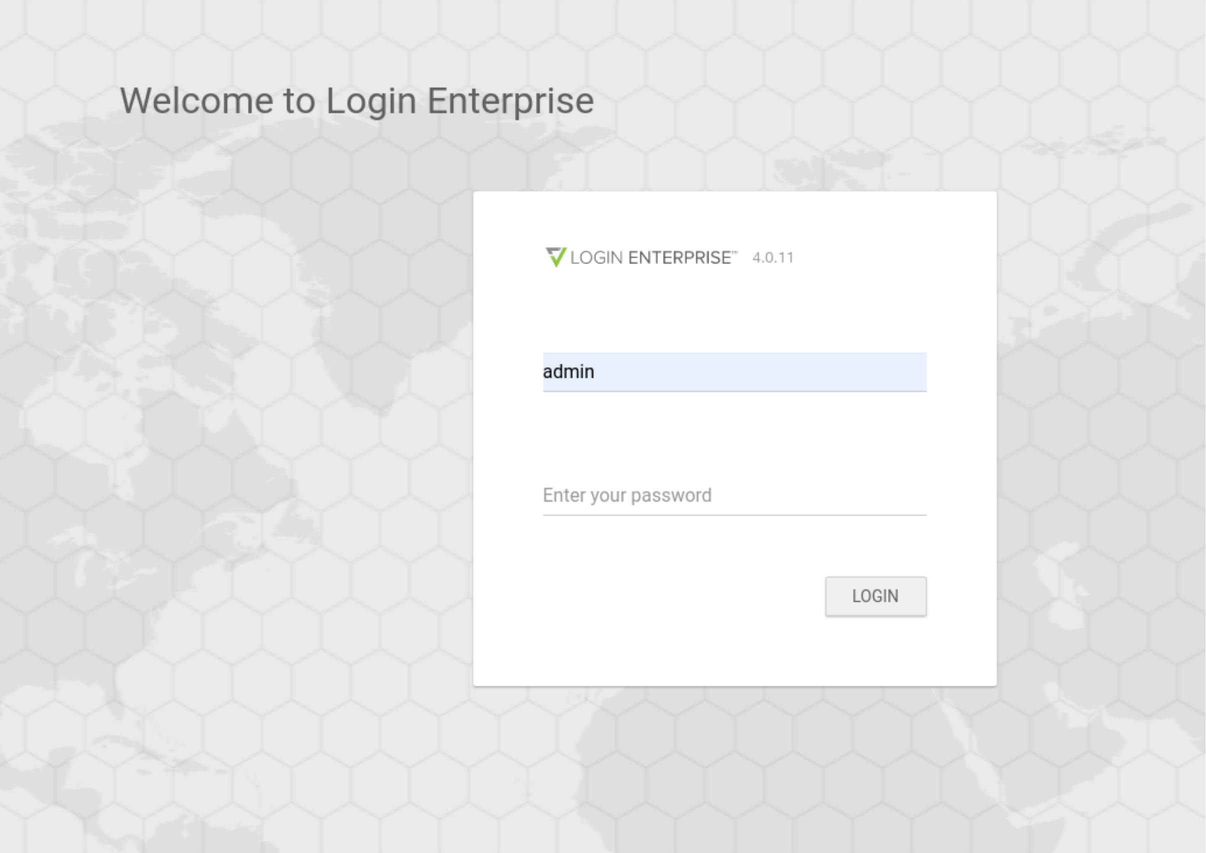
Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=N2L6z4nk8zQ

Getting the Secret for Login Enterprise Launcher

This how-to explains how to get a Secret (see page 377) to configure Login Enterprise Launcher.

1. Go to `https://loginpi.yourserverURL`.
   Enter `admin` as a username and password and click **LOGIN**.

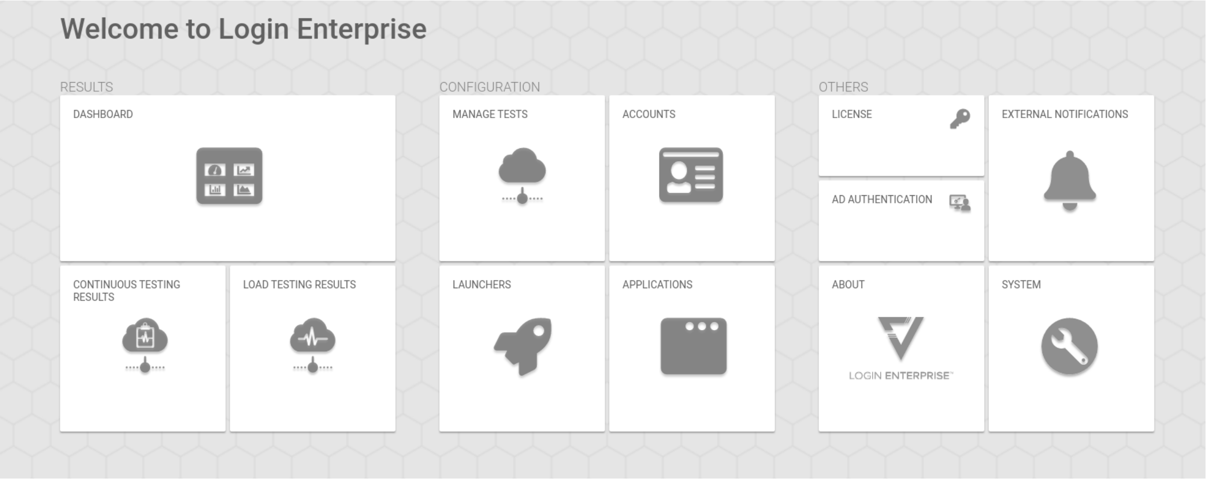


Welcome to Login Enterprise

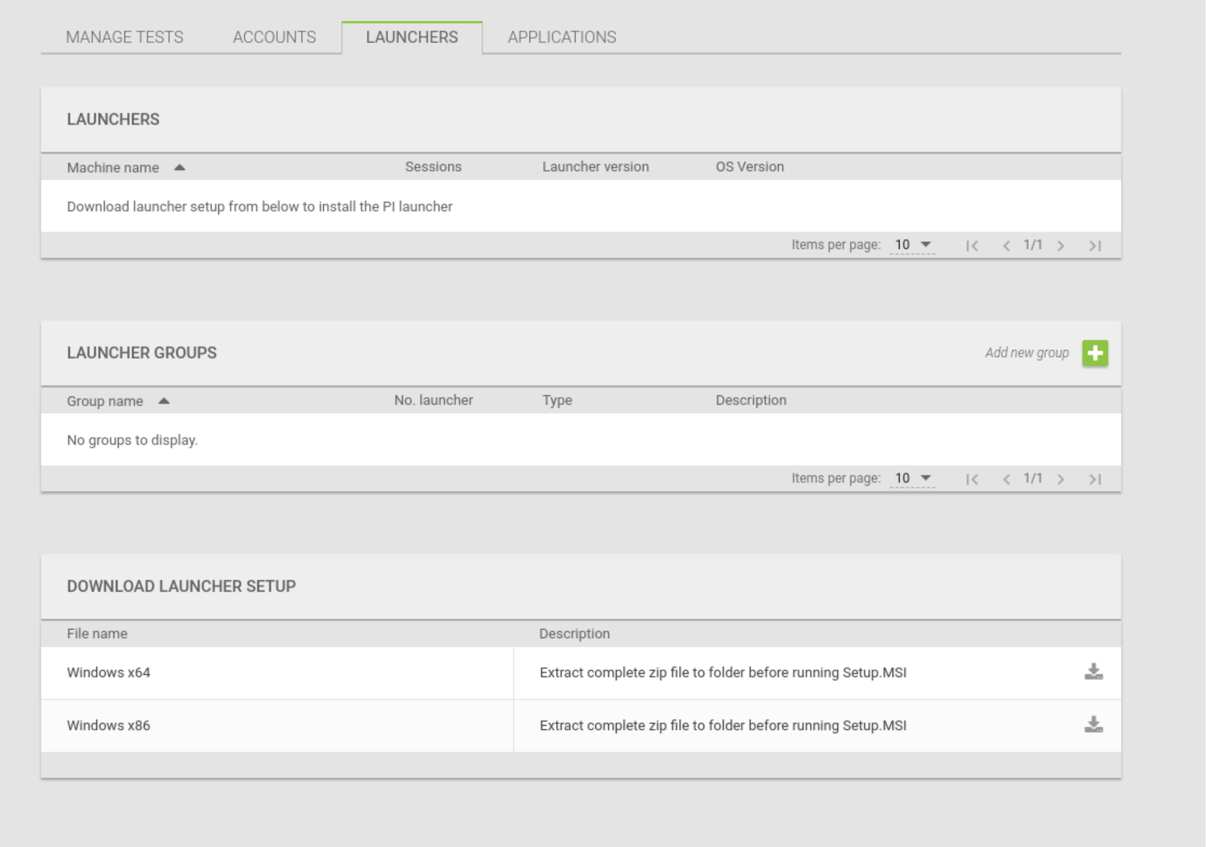
LOGIN ENTERPRISE™ 4.0.11

admin

2. Go to **Launchers**.



3. Download a required `.zip` file under **Download Launcher Setup** and unpack it.



LAUNCHERS

Machine name ▲	Sessions	Launcher version	OS Version
Download launcher setup from below to install the PI launcher			

Items per page: 10 ▾ 1/1

LAUNCHER GROUPS

Add new group +

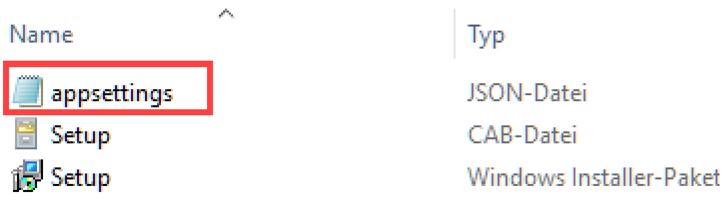
Group name ▲	No. launcher	Type	Description
No groups to display.			

Items per page: 10 ▾ 1/1

DOWNLOAD LAUNCHER SETUP

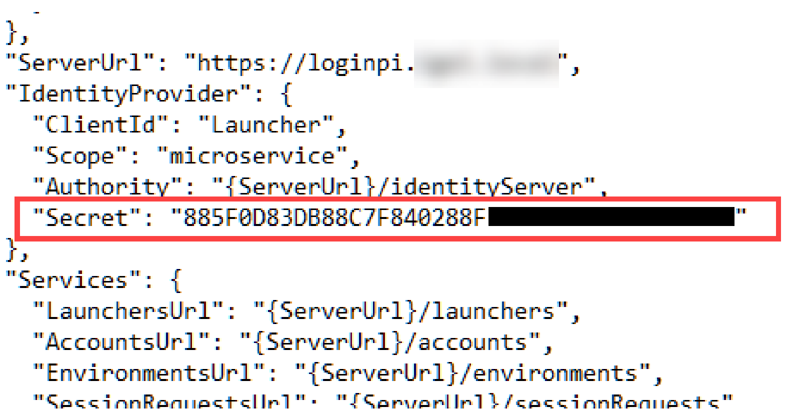
File name	Description
Windows x64	Extract complete zip file to folder before running Setup.MSI
Windows x86	Extract complete zip file to folder before running Setup.MSI

4. Open the `appsettings.json` file in the editor.



Name	Typ
appsettings	JSON-Datei
Setup	CAB-Datei
Setup	Windows Installer-Paket

Here you find the **Secret** for your Login Enterprise Launcher.



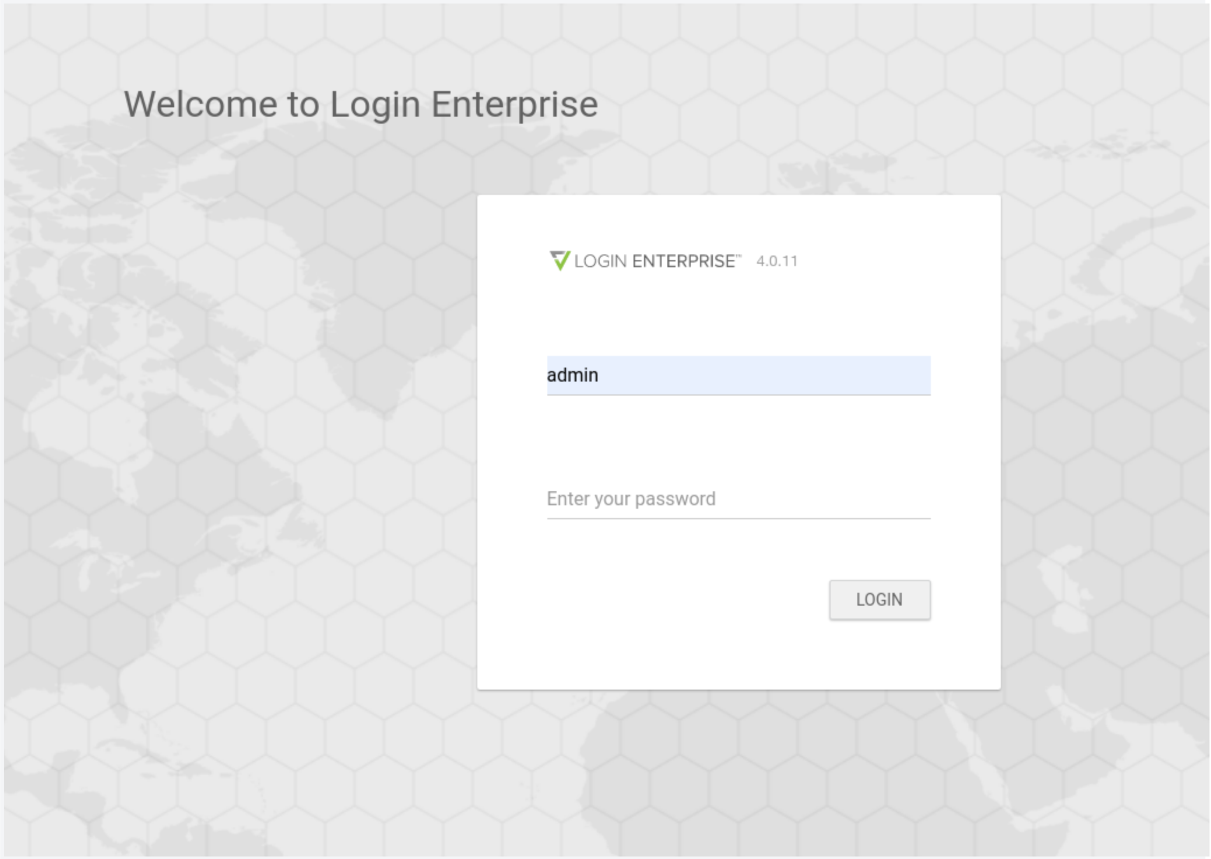
```
},
"ServerUrl": "https://loginpi.[redacted]",
"IdentityProvider": {
  "ClientId": "Launcher",
  "Scope": "microservice",
  "Authority": "{ServerUrl}/identityServer",
  "Secret": "885F0D83DB88C7F840288F[redacted]"
},
"Services": {
  "LaunchersUrl": "{ServerUrl}/launchers",
  "AccountsUrl": "{ServerUrl}/accounts",
  "EnvironmentsUrl": "{ServerUrl}/environments",
  "SessionRequestsUrl": "{ServerUrl}/sessionRequests"
```

Use the **Secret** without the quotation marks "".

Using 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://loginentprise.yourserverURL` and log in.



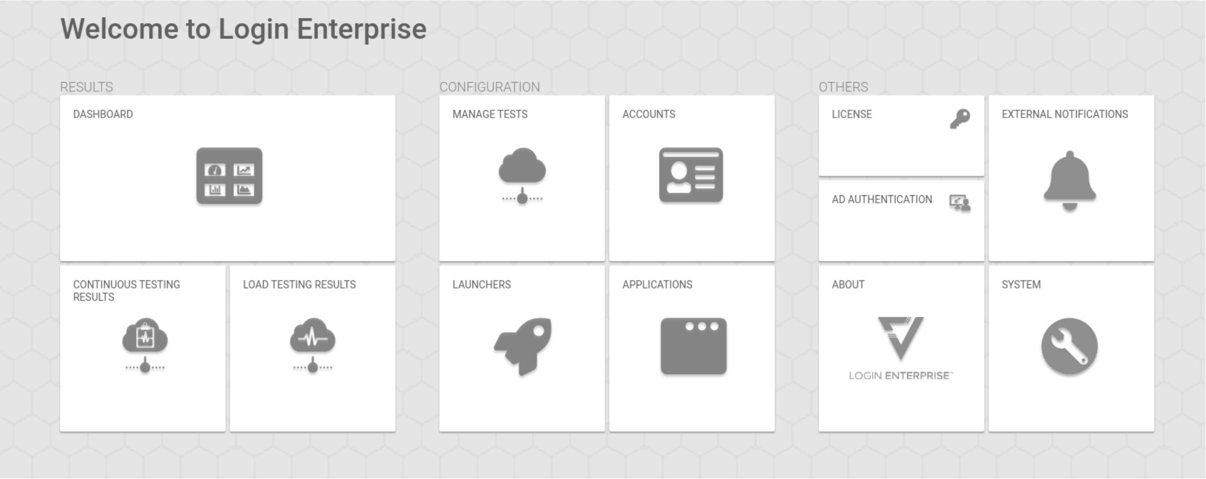
Welcome to Login Enterprise

LOGIN ENTERPRISE™ 4.0.11

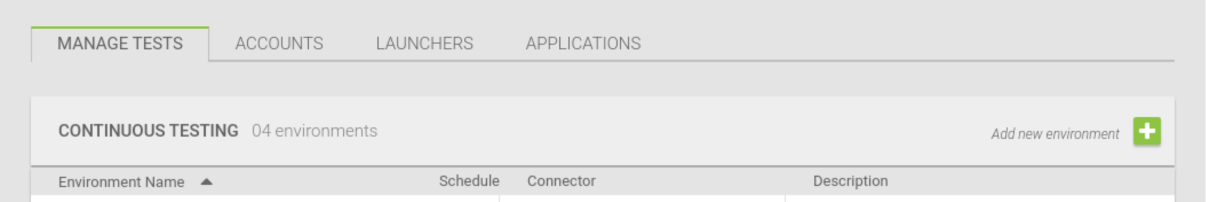
admin

Enter your password

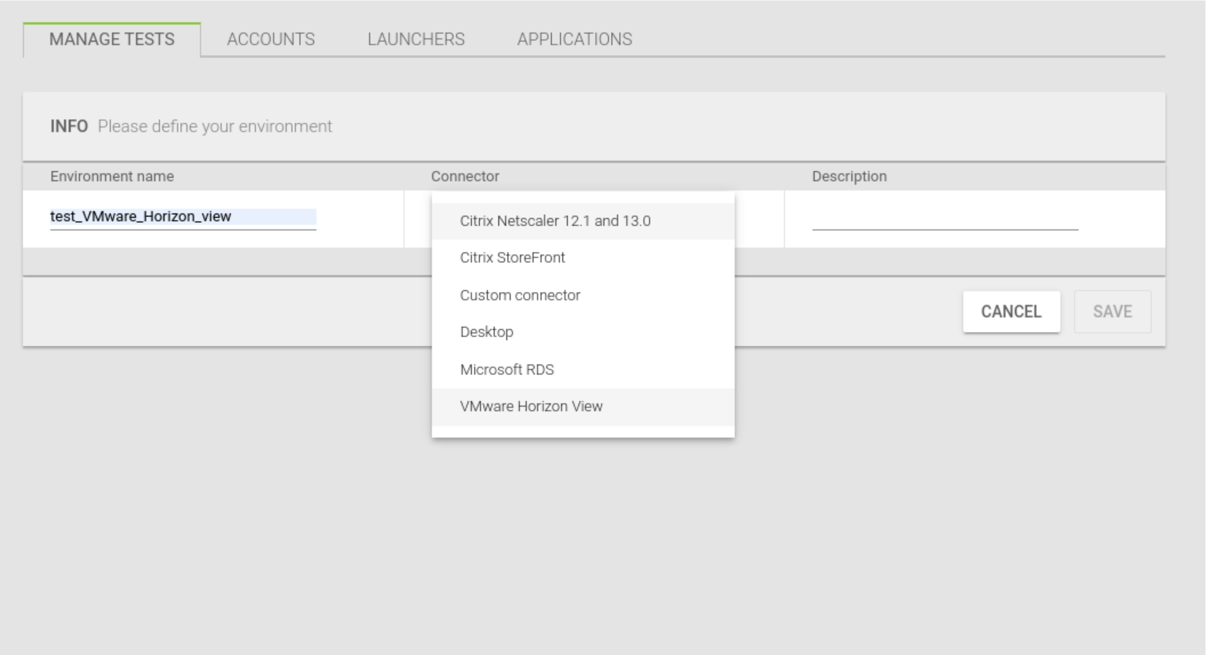
2. Go to **Manage Tests**.



3. Click **Add new environment**.

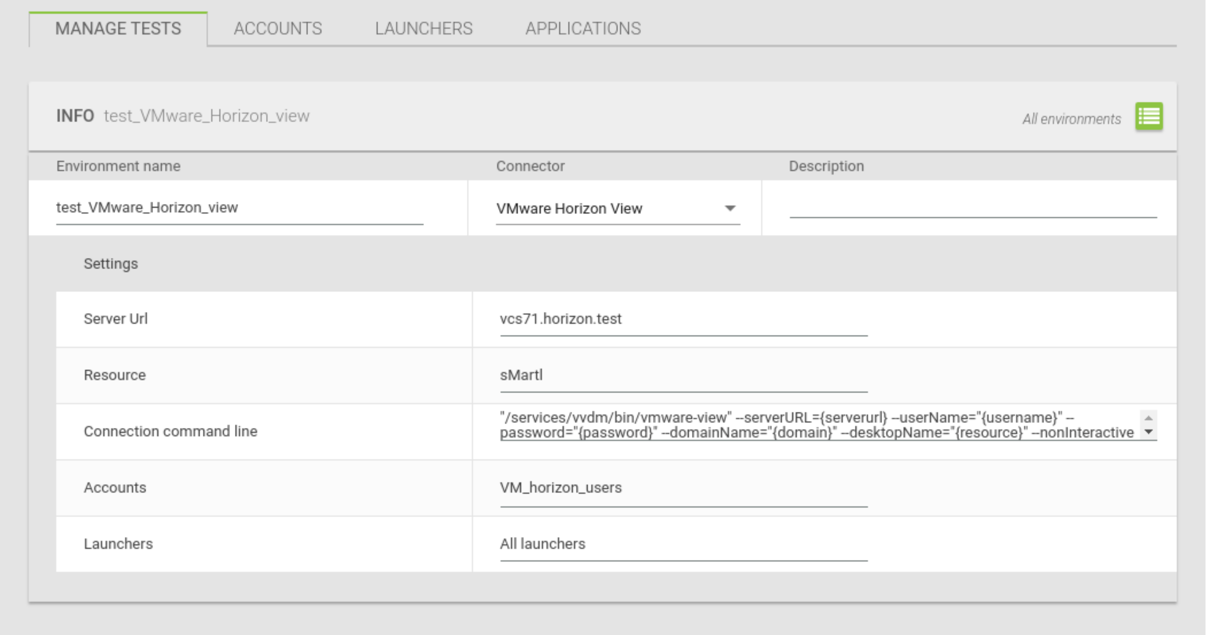


4. Enter an **Environment name**.
5. Select **VMware Horizon View** under **Connector**.



Environment name: test_VMware_Horizon_view

6. Enter the **Server URL** and the **Resource**.



INFO test_VMware_Horizon_view

Environment name	Connector	Description
test_VMware_Horizon_view	VMware Horizon View	

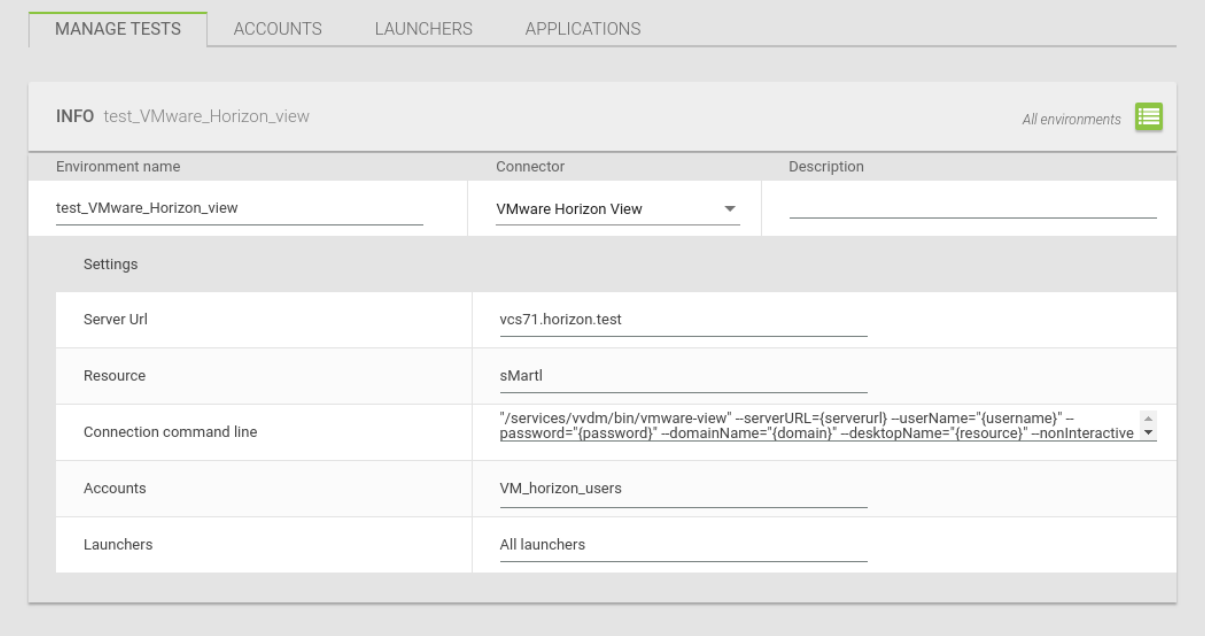
Settings

Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" –serverURL={serverurl} –userName="{username}" –password="{password}" –domainName="{domain}" –desktopName="{resource}" –nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers

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**.



Environment name	Connector	Description
test_VMware_Horizon_view	VMware Horizon View	

Settings

Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" --password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers

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[21].

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.

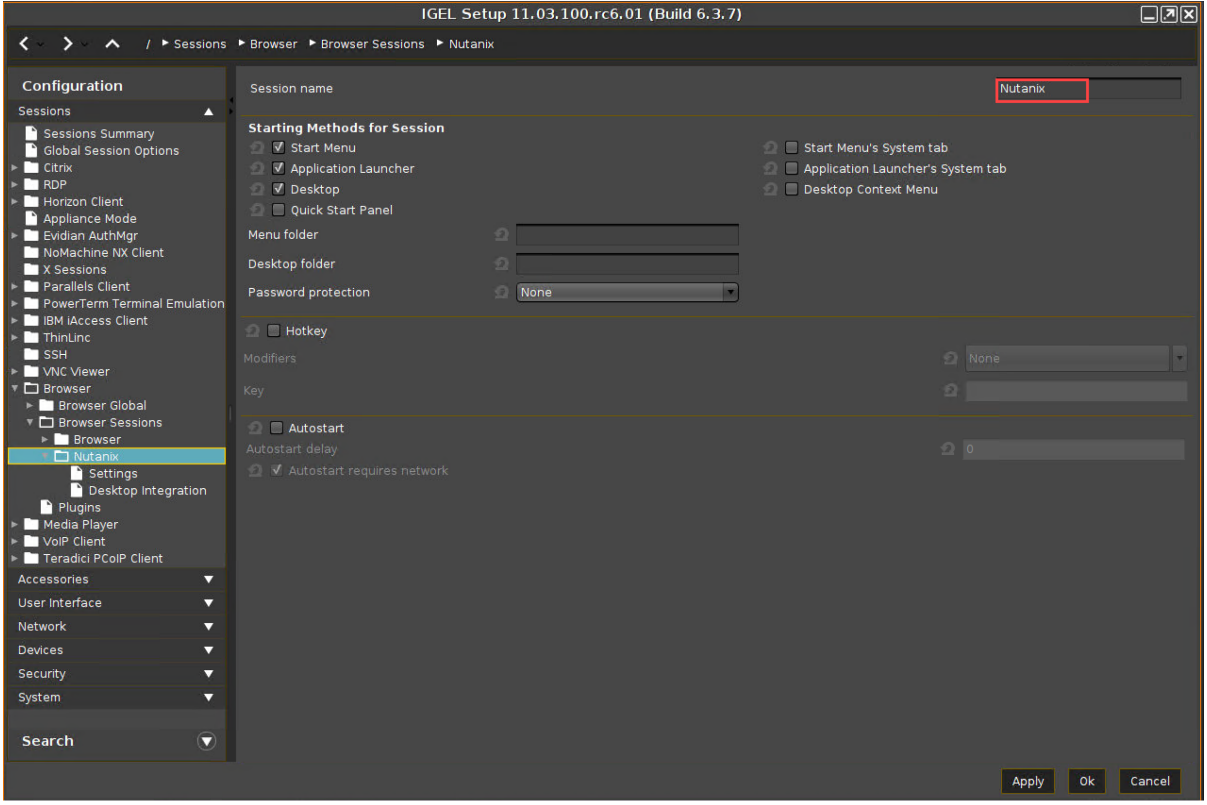
You have to create a browser profile and put in the address of your frame broker.

Setting Up Frame Connection

1. In the IGEL Setup, go to **Sessions > Firefox Browser > Firefox Browser Sessions**.

[21] https://www.nutanix.com/en

2. Click ⊞ to add a browser session.
   For more information about the setup, see Browser Session.



IGEL Setup 11.03.100.rc6.01 (Build 6.3.7)

Session name: Nutanix

Starting Methods for Session

☑ Start Menu ☐ Start Menu's System tab
☑ Application Launcher ☐ Application Launcher's System tab
☑ Desktop ☐ Desktop Context Menu
☐ Quick Start Panel

Menu folder

Desktop folder

Password protection: None

☐ Hotkey

Modifiers: None

Key

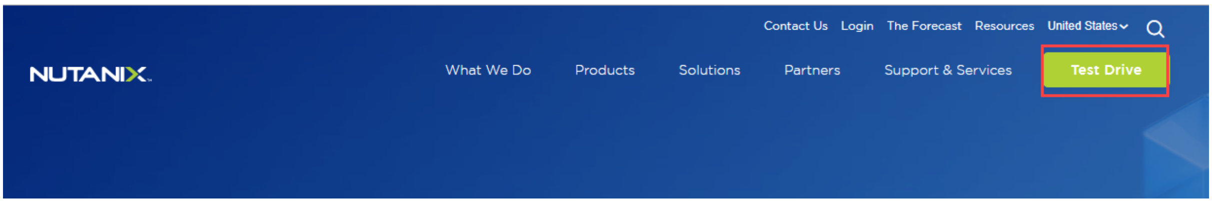
☐ Autostart

Autostart delay: 0

☑ Autostart requires network

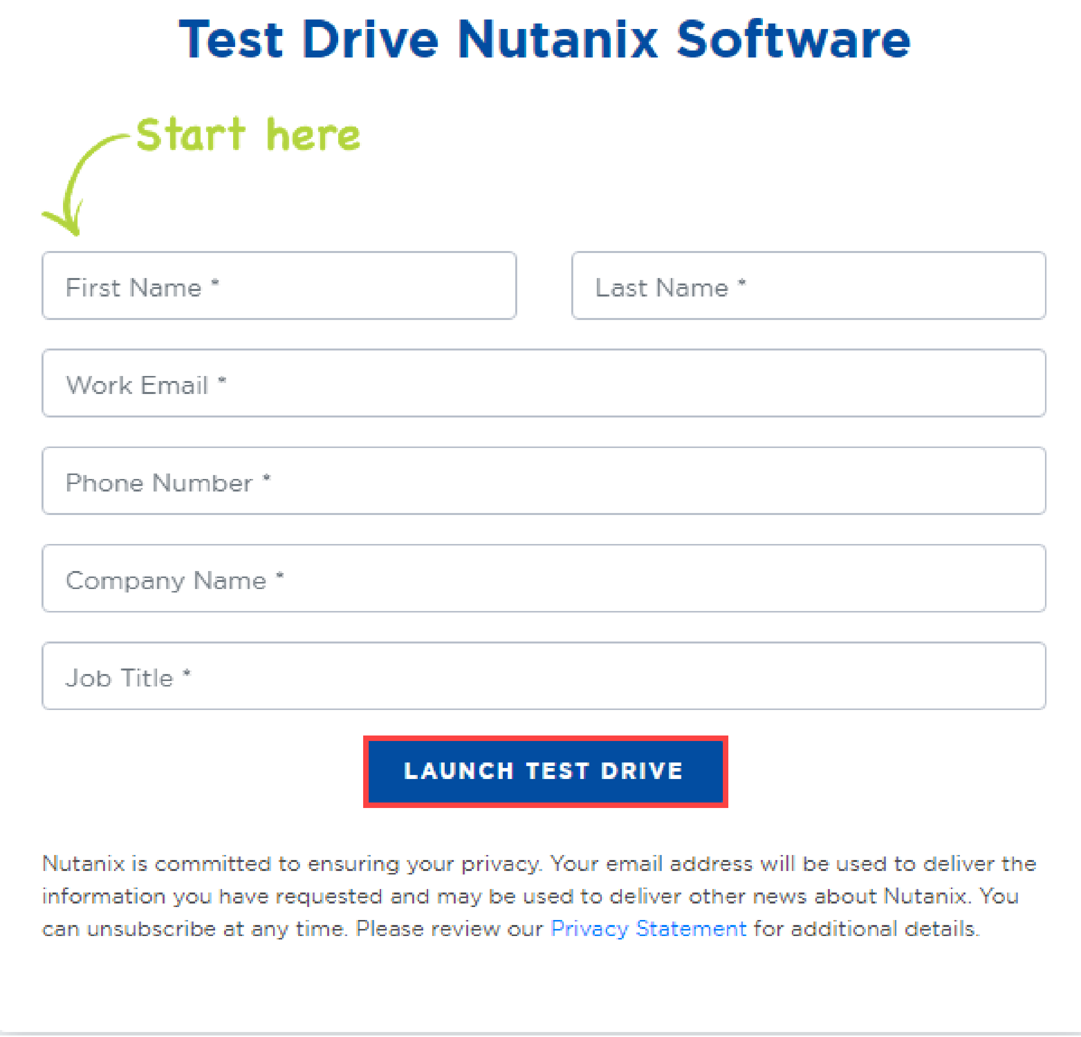
Running the Nutanix Test Drive on IGEL

1. Open the Firefox browser.
2. Enter https://www.nutanix.com[22].
3. Click **Test Drive.**



4. Enter the required data.
5. Click **Launch Test Drive.**

[22] https://www.nutanix.com/en

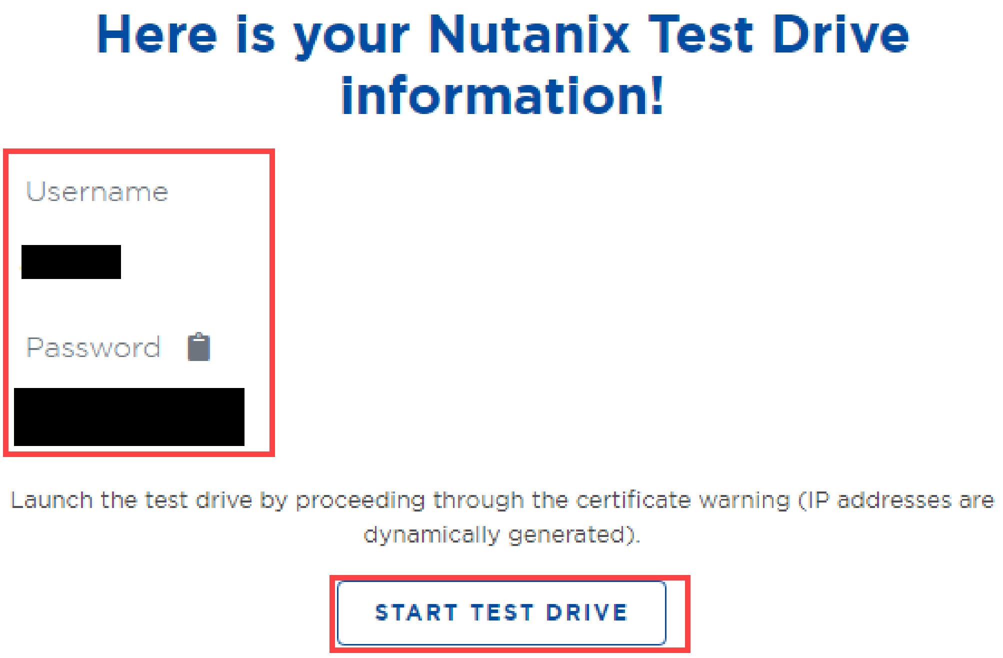

Test Drive Nutanix Software

First Name *	Last Name *
Work Email *	
Phone Number *	
Company Name *	
Job Title *	

Nutanix is committed to ensuring your privacy. Your email address will be used to deliver the information you have requested and may be used to deliver other news about Nutanix. You can unsubscribe at any time. Please review our Privacy Statement for additional details.

6. Your **Nutanix Test Drive information** is shown.

7. Click **Start Test Drive.**



Here is your Nutanix Test Drive information!

Username

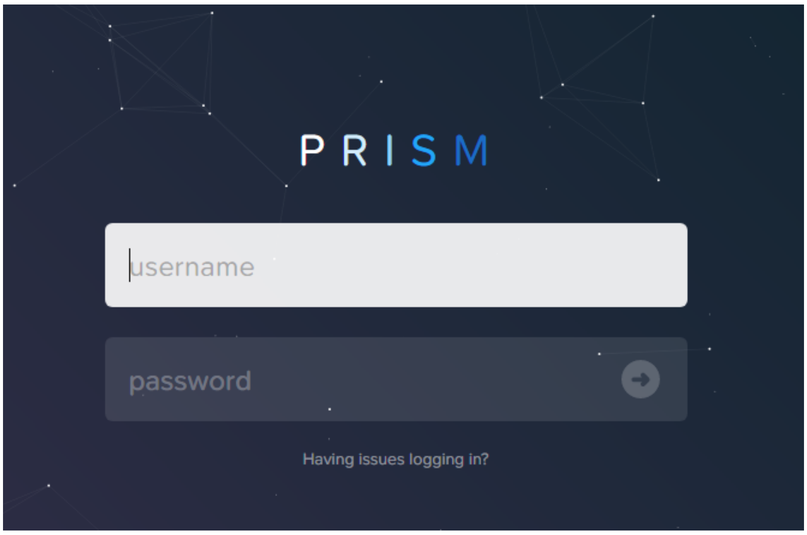
[redacted]

Password

[redacted]

Launch the test drive by proceeding through the certificate warning (IP addresses are dynamically generated).

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.

Caradigm

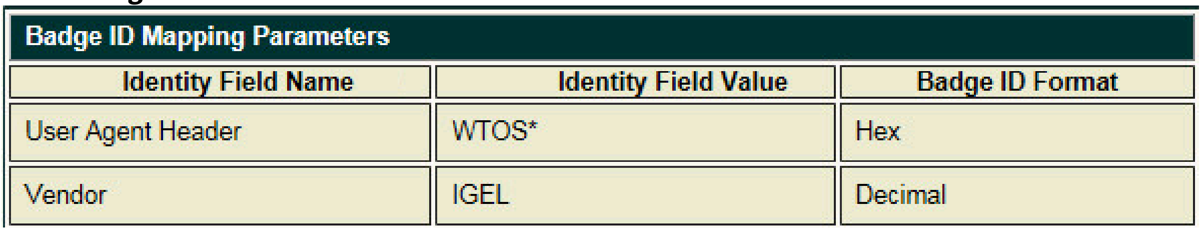
How to Prepare Caradigm

Basic Configuration

This document explains how to configure certificates for *Caradigm* using a Windows server environment.

First of all, you have to give basic information to the *Caradigm* authentication server:

1. Go to the *Caradigm* authentication server (Vault).
2. Go to the **SSO & Context Management** tab.
3. Click **Tap Server**.
   The **Tap Server** screen opens.
4. Check the values for the **Way2Care Parameters**:
   - **Default Group Name**
   - **Default Grace Period**
5. Add the values for the **Badge ID Mapping Parameters**:
   - **Identity Field Name**: Vendor
   - **Identity Field Value**: IGEL
   - **Badge ID Format**: Decimal



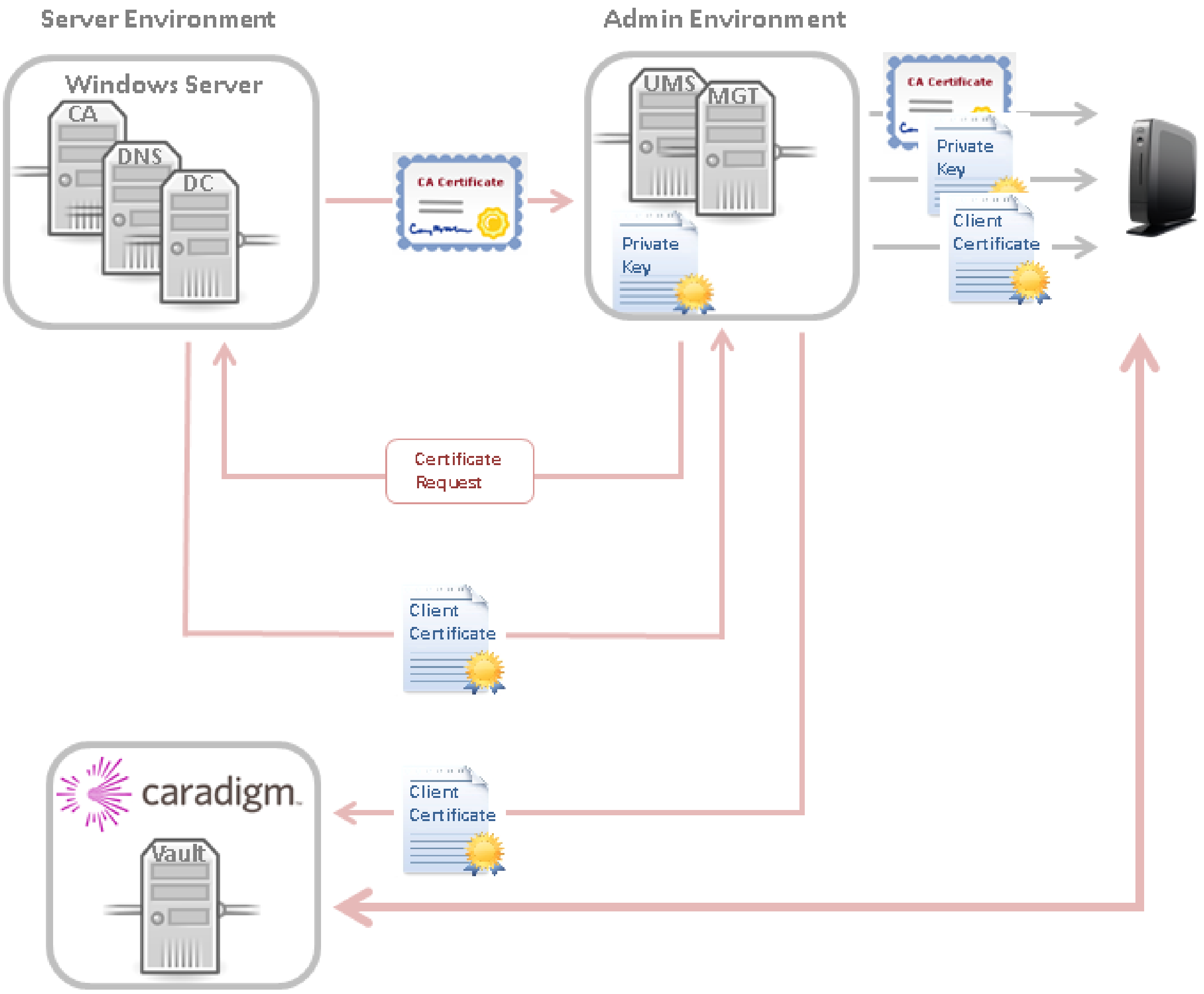
Badge ID Mapping Parameters

Identity Field Name	Identity Field Value	Badge ID Format
User Agent Header	WTOS*	Hex
Vendor	IGEL	Decimal

- Enrollment of Certificates (see page 393)

Enrollment of Certificates

This is an overview of the files and hosts involved in certificate enrollment:



Three files are required:

- SSL client private key
- SSL client certificate
- CA certificate

ⓘ The thin client needs all three files. The *Caradigm* authentication server requires only the SSL client certificate for SSL certification validation.

These are the steps for rolling out the certificates:

- Getting the CA Certificate from Certificate Authority (see page 395)
- Requesting the Client Certificate (see page 396)
- Sending all Certificates to TC (see page 400)
- Transferring the public Certificate to the Caradigm Vault (see page 401)

Getting the CA Certificate from Certificate Authority

In your environment you need to meet the following requirements:

- An enterprise certificate authority (CA) running *Windows Server 2008 R2*.
- A *Certificate Enrollment Web Service* running *Windows Server 2008 R2*.

Getting the CA certificate from your CA:

1. In your web browser, visit the URL `http://` with `/certsrv` to go to the certificate authority.
2. Enter the **User Name** and **Password**.
   The *Windows* server welcome page opens.
3. Select the task **Download a CA certificate, certificate chain, or CRL**.
4. IMPORTANT: Choose **BASE 64** as **Encoding method**.
5. Click **Download CA certificate**.
   You will receive a file with the CA certificate.

Requesting the Client Certificate

Generating a certificate signing request (CSR) with OpenSSL

```
openssl req -out igel_tc.csr -new -newkey rsa:2048 -nodes -keyout
igel_tc.key
```

This produces the following files:

- a private key: `igel_tc.key`
- a certificate signing request (CSR): `igel_tc.csr`

Example for the creation of a certificate request:

```
Generating a 2048 bit RSA private key
................................+++
................................+++
writing new private key to 'igel_tc.key'
```

▶ Generating a 2048 bit RSA private key

................................+++

................................+++

writing new private key to 'igel_tc.key'

> ⓘ You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN.
> There are quite a few fields but you can leave some blank. For some fields there will be a default value.
> If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Augsburg
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IGEL Technology GmbH
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:igeltc
Email Address []:
```

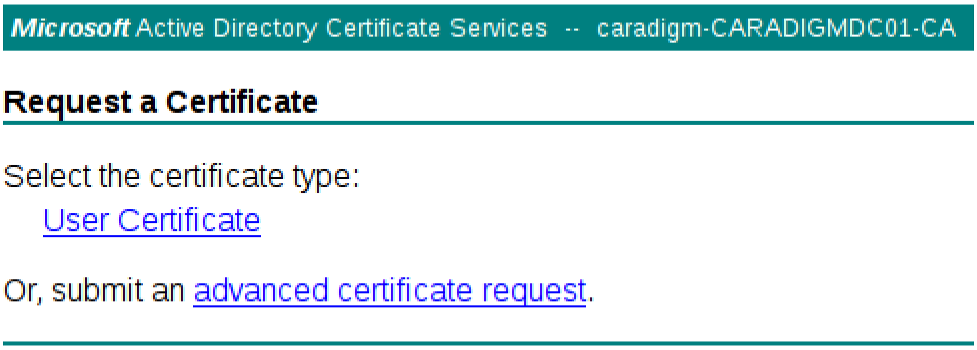
▶ Please enter the following 'extra' attributes to be sent with your certificate request

- A challenge password []:
- An optional company name []:

ⓘ It is also possible to create a so called wildcard certificate. A wildcard certifcate contains a possible common name including a * character. It can be used for all thin clients.

Wildcard SSL certs could cause a security issue.

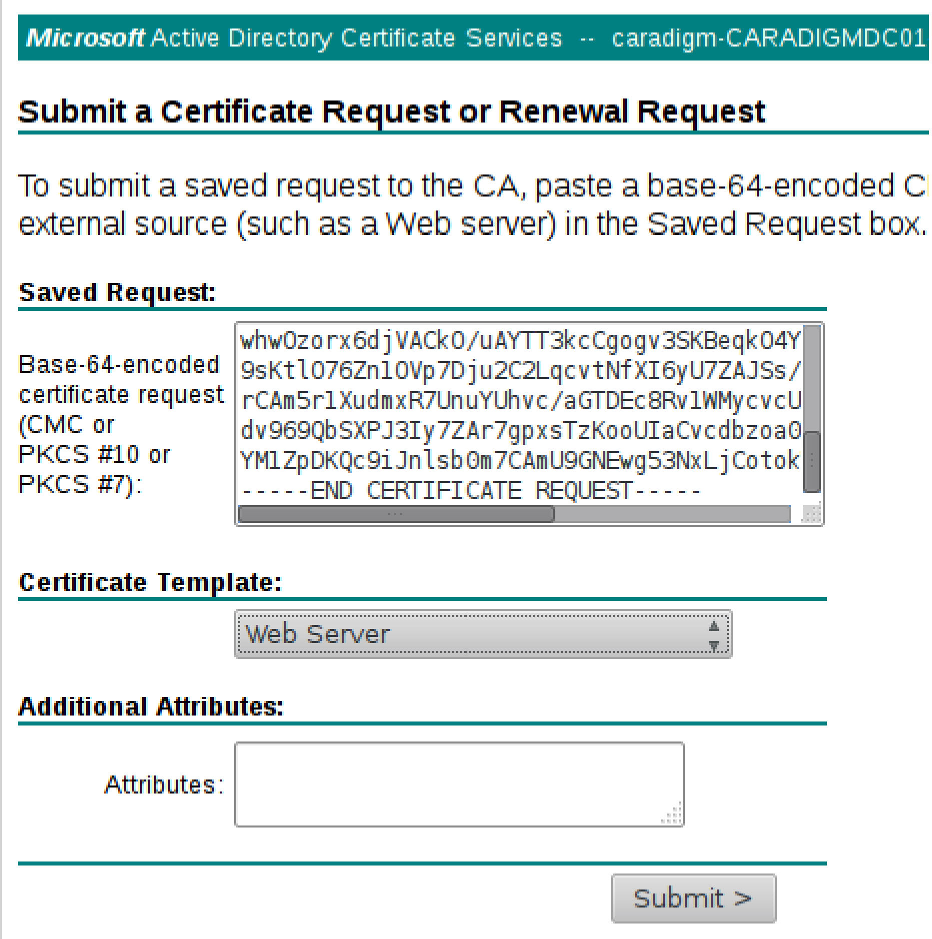
Requesting a certificate

1. Go back to the welcome page of the *Windows* server.
2. Select the task **Request a certificate**.
   The **Request a Certificate** mask opens:
   
   Microsoft Active Directory Certificate Services -- caradigm-CARADIGMDC01-CA

   Request a Certificate

   Select the certificate type:
   User Certificate

   Or, submit an advanced certificate request.
3. Click **advanced certificate request**.
   The **Submit a Certificate Request or Renewal Request** mask opens:



Microsoft Active Directory Certificate Services -- caradigm-CARADIGMDC01

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded C
external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
whw0zorx6djVACk0/uAYTT3kcCgogv3SKBeqk04Y
9sKtl076Znl0Vp7Dju2C2LqcvtNfXI6yU7ZAJSs/
rCAm5rlXudmxR7UnuYUhvc/aGTDEc8RvlWMycvcU
dv969QbSXPJ3Iy7ZAr7gpxsTzKooUIaCvcdbzoa0
YMlZpDKQc9iJnlsb0m7CAmU9GNEwg53NxLjCotok
-----END CERTIFICATE REQUEST-----
```

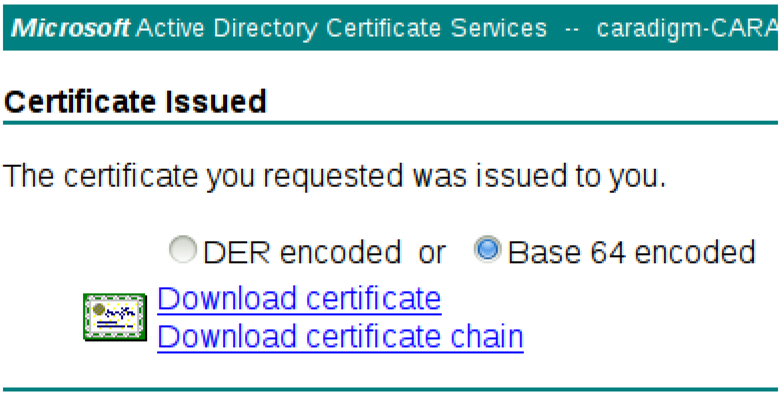
Certificate Template:

Web Server

Additional Attributes:

Attributes:

4. Copy the plain text content of the `.csr`-file into the **Saved Request** input field.
5. Choose **Web Server** under **Certificate Template**.
6. Click **Submit**.
   The **Certificate Issued** screen opens:



Microsoft Active Directory Certificate Services -- caradigm-CARA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

7. Choose **Base 64 encoded**.

8. Click **Download certificate**.
   You receive a file with the public certificate for your thin clients.

Sending all Certificates to TC

Now you have generated these three files:

- CA certificate
- SSL client private key
- SSL client certificate

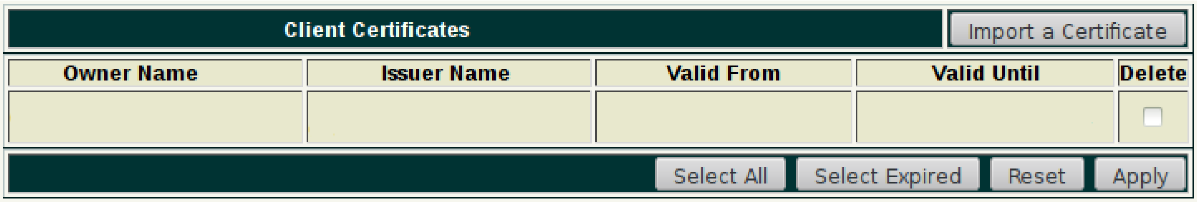
1. Copy these three files into the directory `/wfs/ca-certs` of your thin clients.

   > ⓘ Preferably roll them out via UMS file transfer.

2. Reboot the clients.

Transferring the public Certificate to the Caradigm Vault

1. Go to the *Caradigm* authentication server (Vault).
2. Go to tab **Appliance**.
3. Click **Thin Client Certificates**.
   The **Thin Client Certificates** screen opens.



Owner Name	Issuer Name	Valid From	Valid Until	Delete
				□

4. Click **Import a Certificate**.
5. Copy and paste the plain text contents of the client certificate.
6. Click **Apply**.
   The **Thin Client Certificates** screen has been filled with the certificate's values.

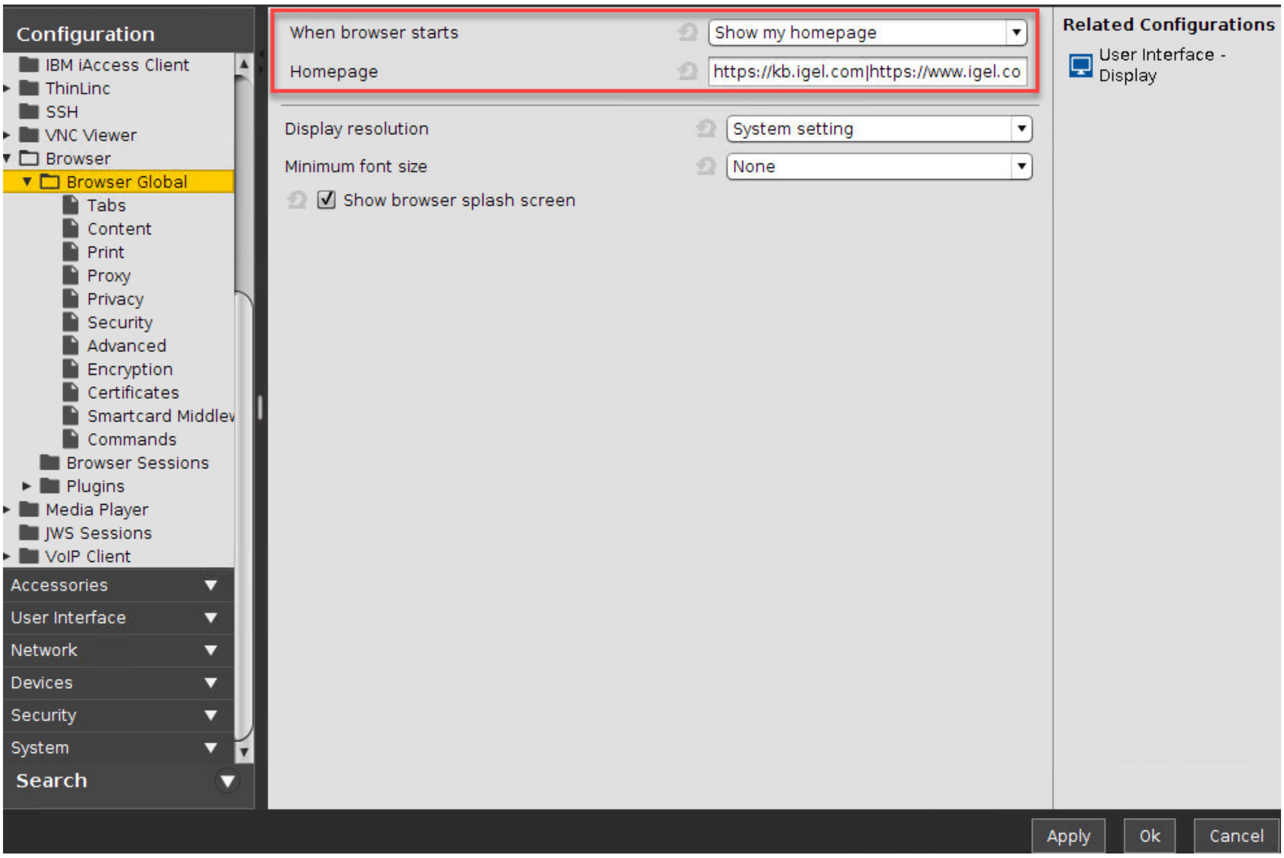
Now everything is prepared for secure communication with the *Caradigm* appliance.

Browser

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:



When browser starts: Show my homepage

Homepage: https://kb.igel.com|https://www.igel.co

Display resolution: System setting

Minimum font size: None

☑ Show browser splash screen

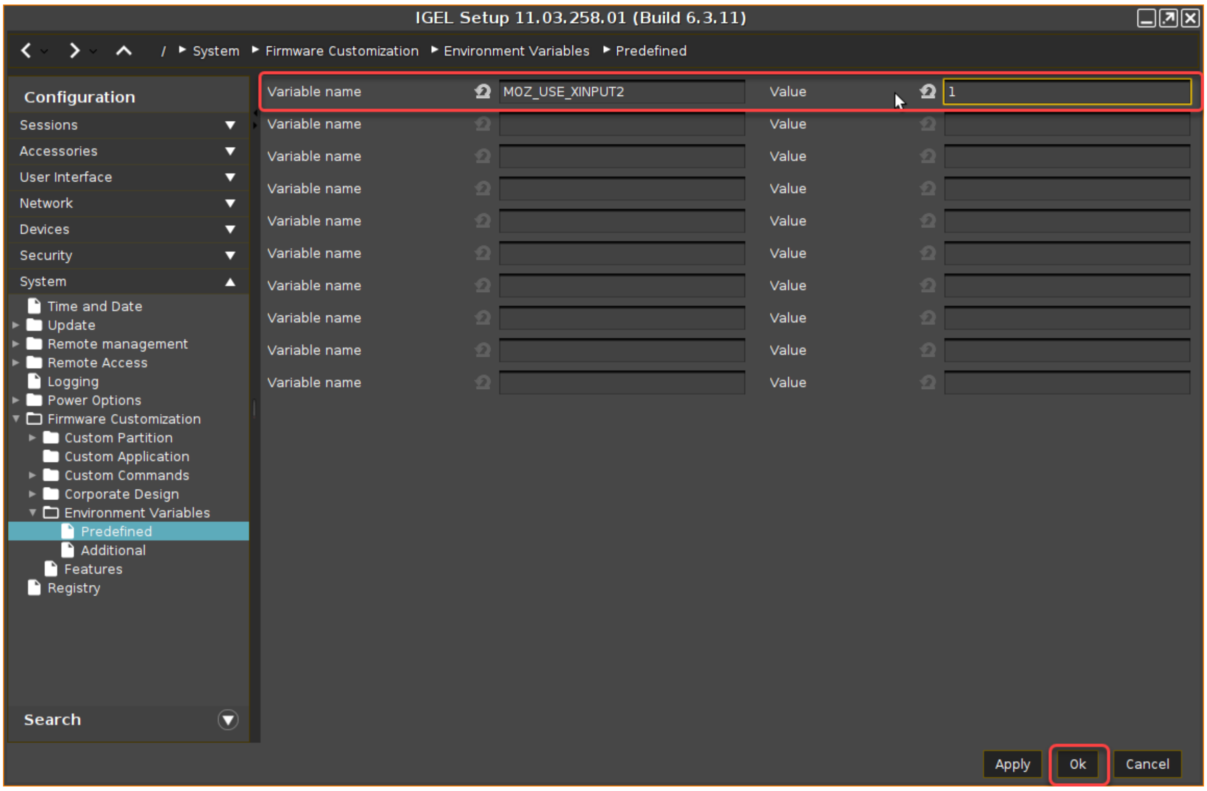
1. Open the setup and go to **Browser > Browser Global.**
2. Set **When Firefox starts** to **Show my home page**.
3. Set **Homepage** to the URLs that the browser should open at startup. Use "|" as a separator.
4. Click **Apply** or **Ok**.

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**.



IGEL Setup 11.03.258.01 (Build 6.3.11)

/ ▸ System ▸ Firmware Customization ▸ Environment Variables ▸ Predefined

Variable name: MOZ_USE_XINPUT2 Value: 1

5. Reboot the device.
6. To check if multitouch is working, open the Firefox browser and go to https://www.paulirish.com/demo/multi.

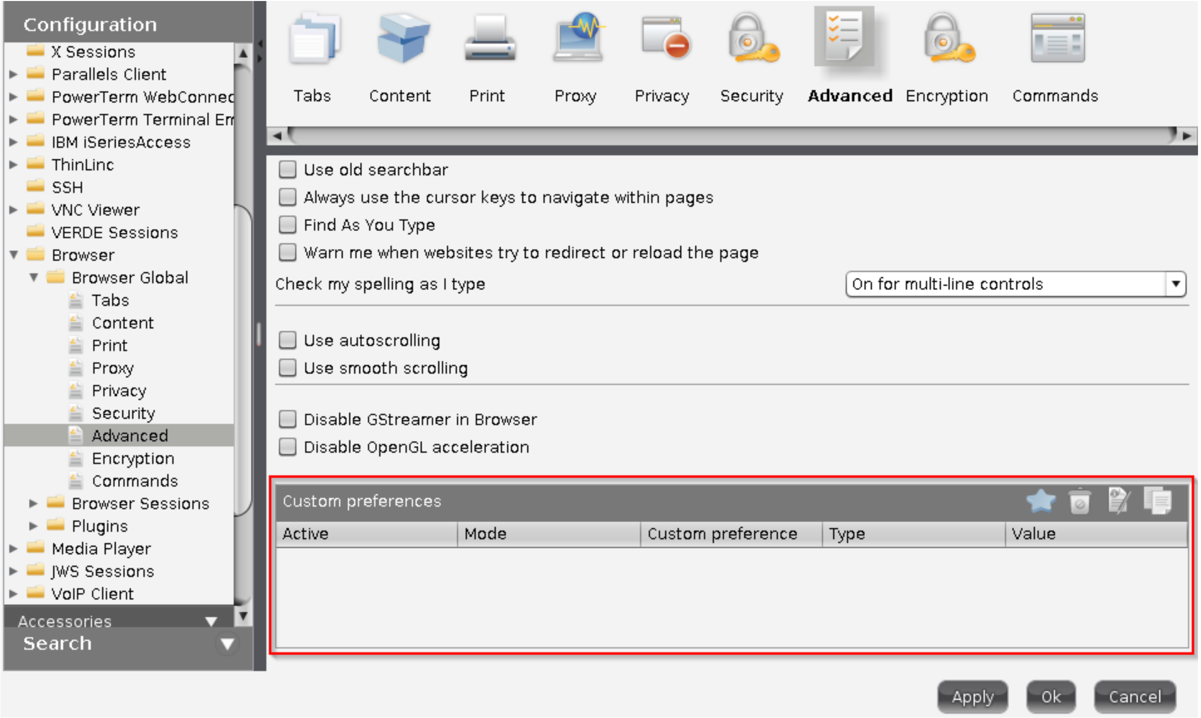
Set Advanced User Preferences for the Browser

The Mozilla Firefox browser included in *IGEL* Linux 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 a re 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[23].

1. In **Setup**, go to **Sessions > Browser > Browser Global > Advanced**.
2. In the **Custom preferences** area, click on **Add**.



□ Use old searchbar
□ Always use the cursor keys to navigate within pages
□ Find As You Type
□ Warn me when websites try to redirect or reload the page

Check my spelling as I type: On for multi-line controls

□ Use autoscrolling
□ Use smooth scrolling

□ Disable GStreamer in Browser
□ Disable OpenGL acceleration

Custom preferences

Active	Mode	Custom preference	Type	Value

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:

[23] http://kb.mozillazine.org/About:config_entries

   - **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.
   For more details on Browser configuration, refer to its section in the *IGEL* Linux manual.

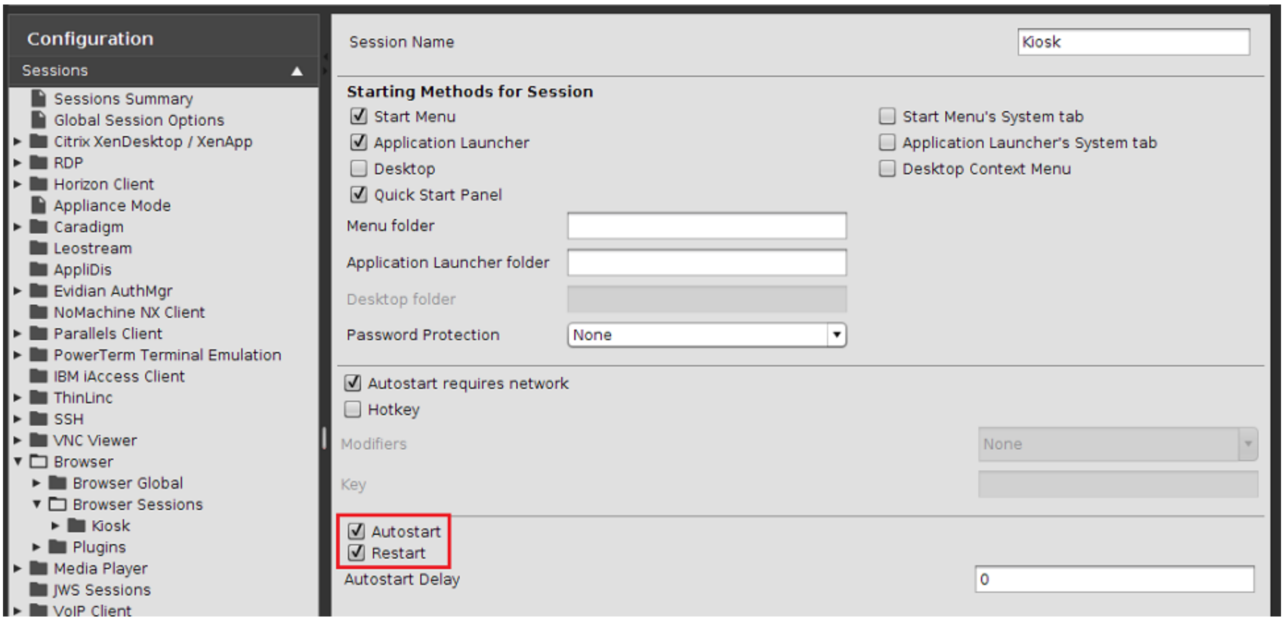
Use the Browser in Kiosk Mode

Browser kiosk mode is an option when you are operating any kind public terminal with anonymous access, e. g.:

- Educational service in a musem
- Service terminals or ticket vending machines for public transport
- Entry portal for a corporate intranet

Albeit configuring an *IGEL* Linux thin client for browser kiosk mode may seem quite extensive, you have the possibility to define your own flavour of kiosk mode. Consider the following settings.

Settings in Setup > Sessions > Browser Sessions > [Session Name]



Session Name: Kiosk

Starting Methods for Session

☑ Start Menu
☑ Application Launcher
☐ Desktop
☑ Quick Start Panel
☐ Start Menu's System tab
☐ Application Launcher's System tab
☐ Desktop Context Menu

Menu folder:

Application Launcher folder:

Desktop folder:

Password Protection: None

☑ Autostart requires network
☐ Hotkey

Modifiers: None

Key:

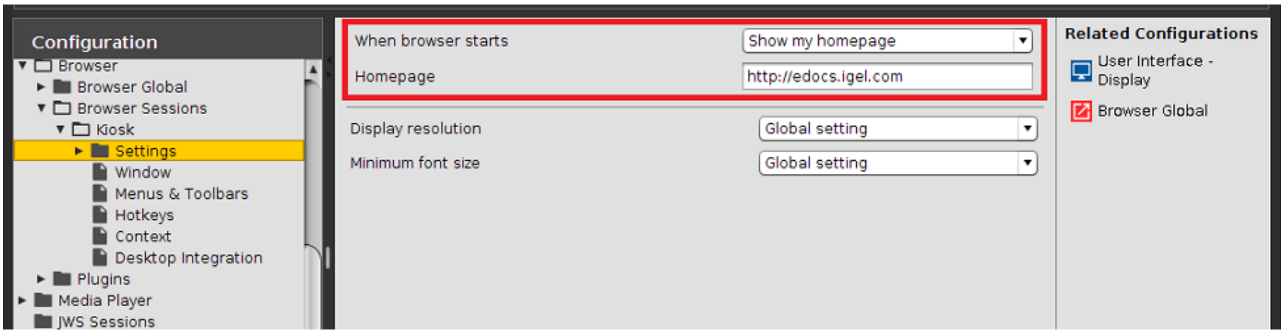
☑ Autostart
☑ Restart

Autostart Delay: 0

▶ Activate **Autostart**.

▶ Activate **Restart**.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings



When browser starts: Show my homepage

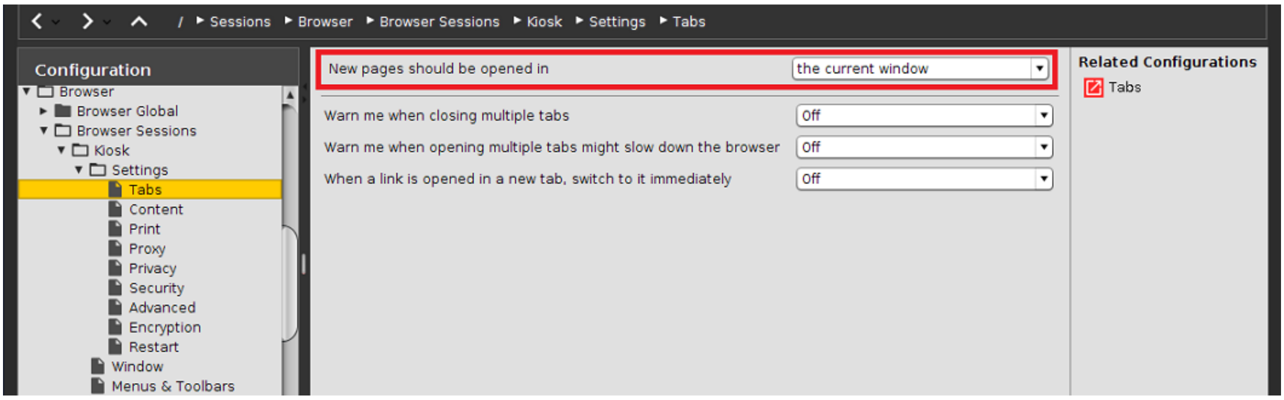
Homepage: http://edocs.igel.com

Display resolution: Global setting

Minimum font size: Global setting

- Set **When browser starts** to **Show my home page**.
- Set **Home Page** to the desired home page.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Tabs



New pages should be opened in: the current window

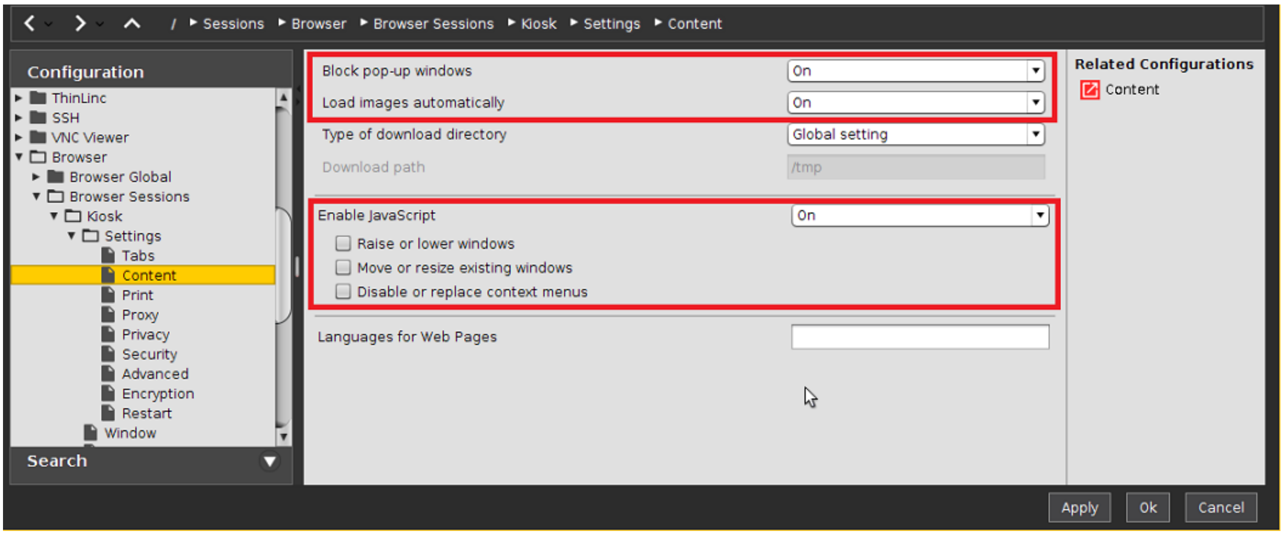
Warn me when closing multiple tabs: Off

Warn me when opening multiple tabs might slow down the browser: Off

When a link is opened in a new tab, switch to it immediately: Off

- Set **New pages should be opened in** to **the current window** or to **a new tab**.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Content

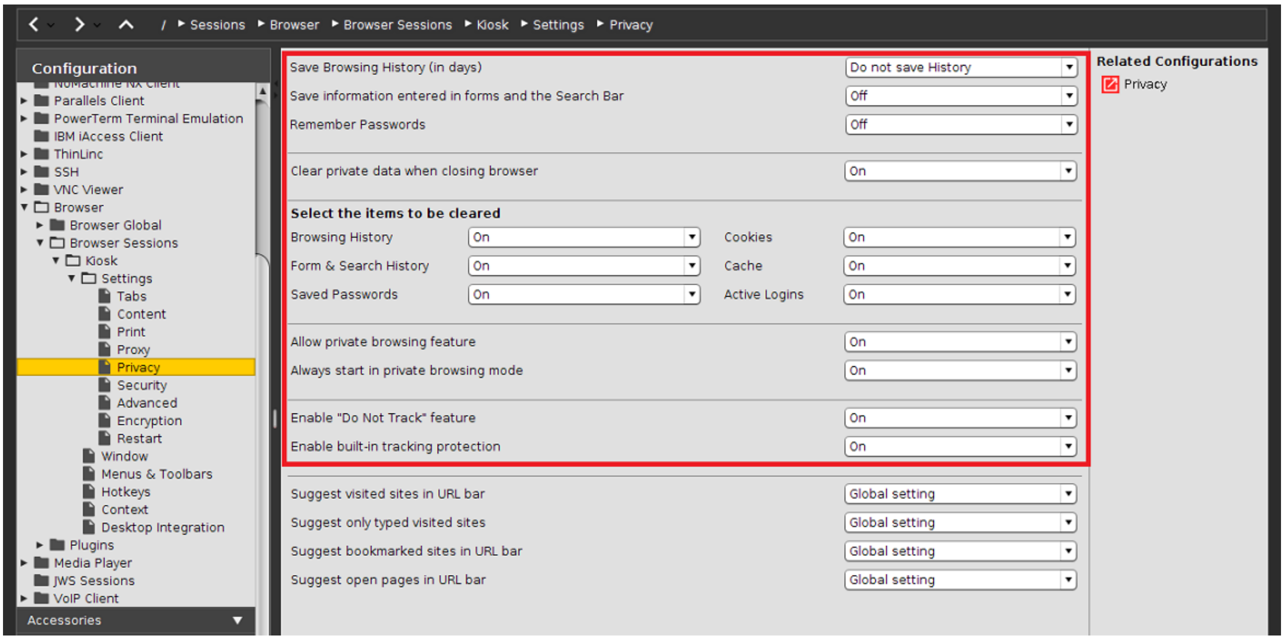


Block pop-up windows: On
Load images automatically: On
Type of download directory: Global setting
Download path: /tmp
Enable JavaScript: On
- □ Raise or lower windows
- □ Move or resize existing windows
- □ Disable or replace context menus

Languages for Web Pages:

- If applicable, activate **Block pop-up windows**.
- Activate **Load images automatically**.
- Activate **Enable JavaScript** if desired, and adapt the actions permitted for JavaScript according to your needs.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Privacy



Save Browsing History (in days)	Do not save History
Save information entered in forms and the Search Bar	Off
Remember Passwords	Off
Clear private data when closing browser	On

Select the items to be cleared

Browsing History	On	Cookies	On
Form & Search History	On	Cache	On
Saved Passwords	On	Active Logins	On

Allow private browsing feature	On
Always start in private browsing mode	On
Enable "Do Not Track" feature	On
Enable built-in tracking protection	On
Suggest visited sites in URL bar	Global setting
Suggest only typed visited sites	Global setting
Suggest bookmarked sites in URL bar	Global setting
Suggest open pages in URL bar	Global setting

▶ 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**.

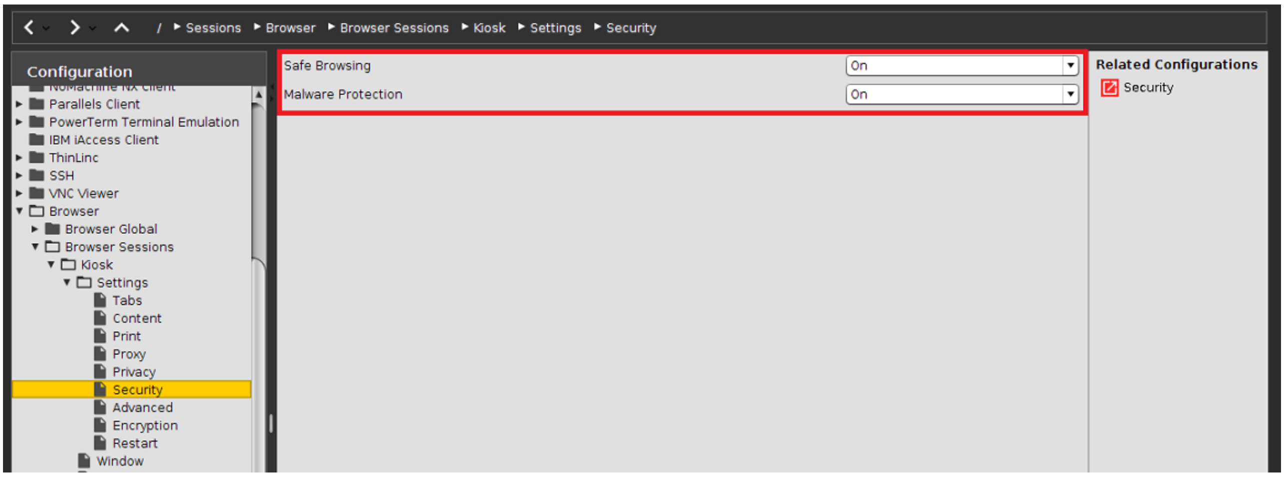
▶ Activate all items in the area **Select the items to be cleared**.

▶ 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 in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Security

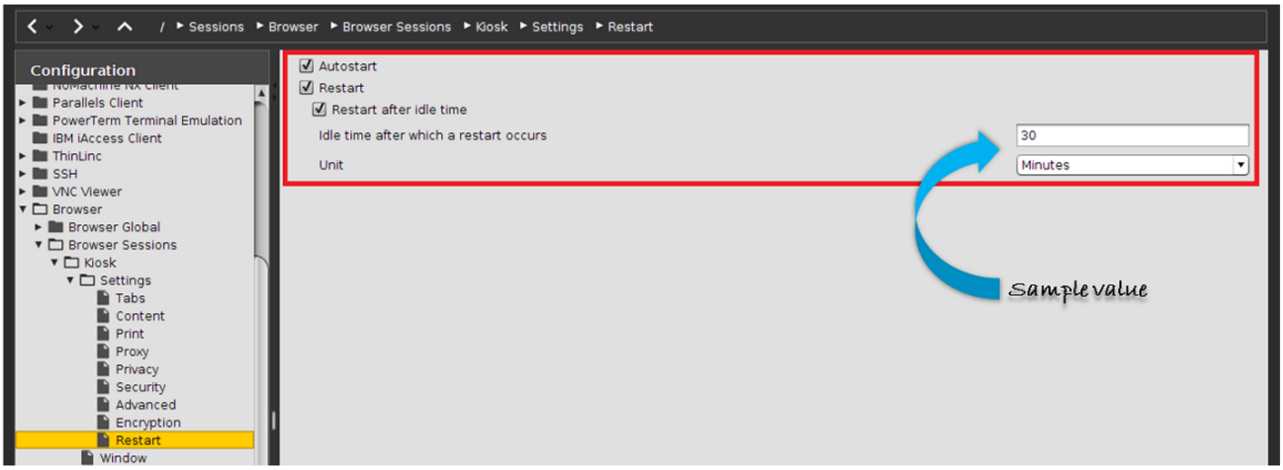


Safe Browsing: On

Malware Protection: On

- To enable phishing protection, activate **Safe Browsing**.
- To enable protection against malicious downloads, activate **Malware Protection**.

Settings in Setup > Browser Sessions > [Session Name] > Settings > Restart



☑ Autostart

☑ Restart

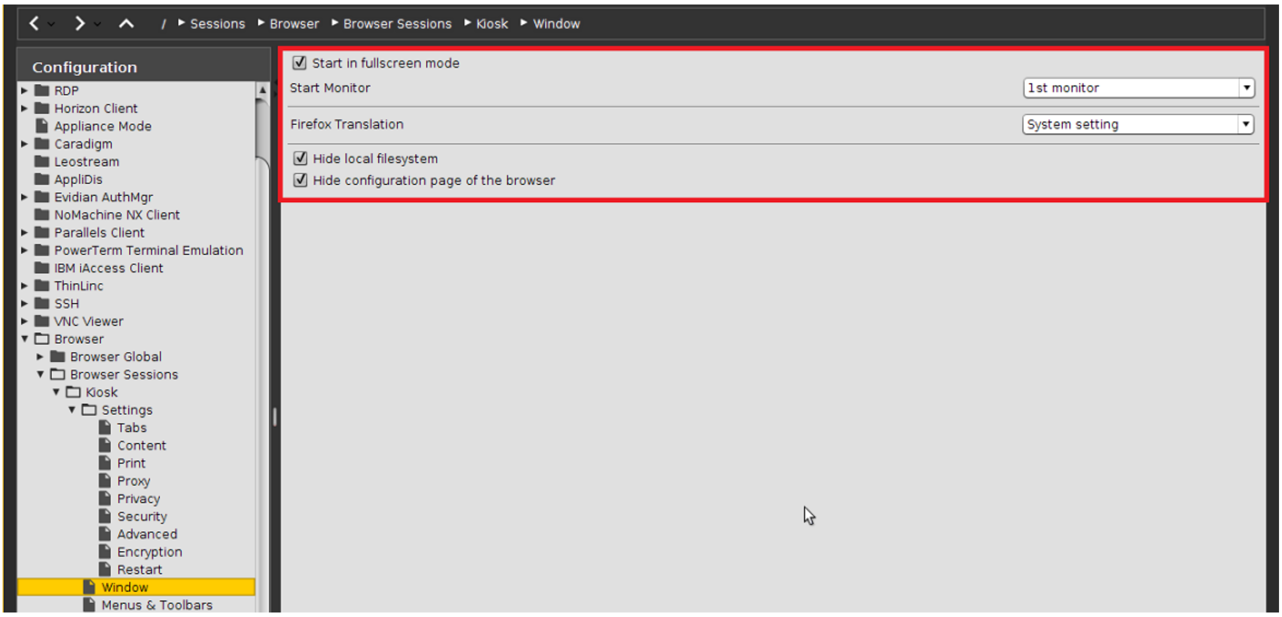
☑ Restart after idle time

Idle time after which a restart occurs: 30

Unit: Minutes

- 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 Timeout enabled** and set a **Restart Timeout** in minutes.

Settings in Setup > Browser Sessions > [Session Name] > Window



☑ Start in fullscreen mode

Start Monitor: 1st monitor

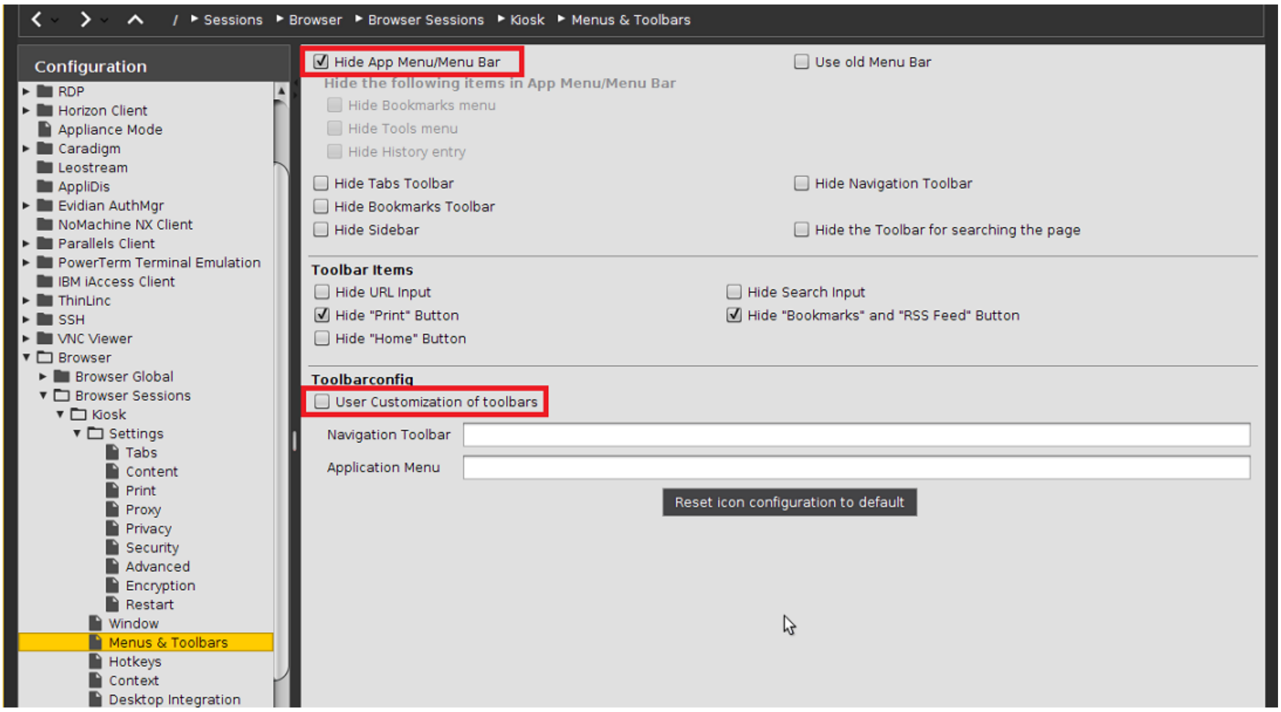
Firefox Translation: System setting

☑ Hide local filesystem

☑ Hide configuration page of the browser

- If the browser shall run in fullscreen mode, activate **Start in Fullscreen Mode**.
- If necessary, select the correct **Start Monitor**.
- Activate **Hide local filesystem**.
- Activate **Hide configuration page of the browser**.

Settings in Setup > Browser Sessions > [Session Name] > Settings > Menus & Toolbar



☑ Hide App Menu/Menu Bar
☐ Use old Menu Bar

Hide the following items in App Menu/Menu Bar
☐ Hide Bookmarks menu
☐ Hide Tools menu
☐ Hide History entry

☐ Hide Tabs Toolbar
☐ Hide Navigation Toolbar
☐ Hide Bookmarks Toolbar
☐ Hide Sidebar
☐ Hide the Toolbar for searching the page

Toolbar Items
☐ Hide URL Input
☐ Hide Search Input
☑ Hide "Print" Button
☑ Hide "Bookmarks" and "RSS Feed" Button
☐ Hide "Home" Button

Toolbarconfig
☐ User Customization of toolbars
Navigation Toolbar
Application Menu

- Activate **Hide App Menu/Menu Bar**.
- Select which menus and toolbars are to be hidden.
- Deactivate **User Customization of toolbars**.

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 Set Advanced User Preferences for the Browser (see page 405).

Mode	`pref`
Custom pference	`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 Set Advanced User Preferences for the Browser (see page 405).

Mode	`pref`
Custom pference	`datareporting.policy.dataSubmission`
Type	`Boolean`
Value	`false`

Mode	`pref`
Custom pference	`datareporting.healthreport.upload`
Type	`Boolean`
Value	`false`

Mode	`pref`
Custom pference	`toolkit.telemetry`
Type	`Boolean`
Value	`false`

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.

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.
- Network drive which is mounted to `/mnt/[folder name]`
- Folder `/userhome` in the local file system; not persistent

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.

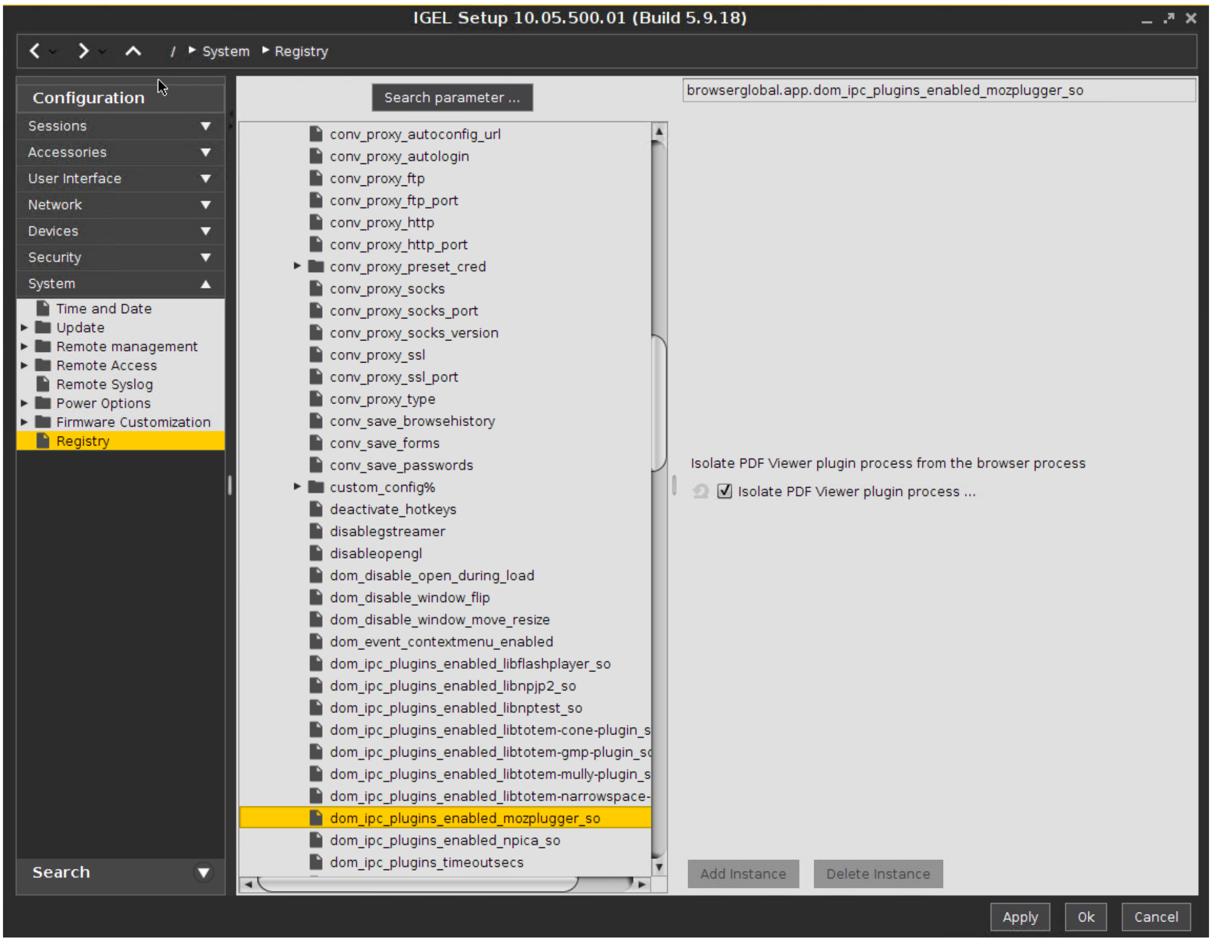
Problem

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.



browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so

Isolate PDF Viewer plugin process from the browser process

☑ Isolate PDF Viewer plugin process ...

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.

System

Resetting 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.

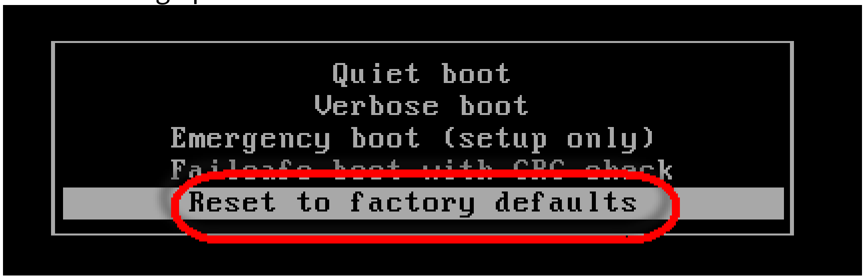
Problem

The local setup is not accessible without the password. Also, resetting the device to factory defaults seems impossible.

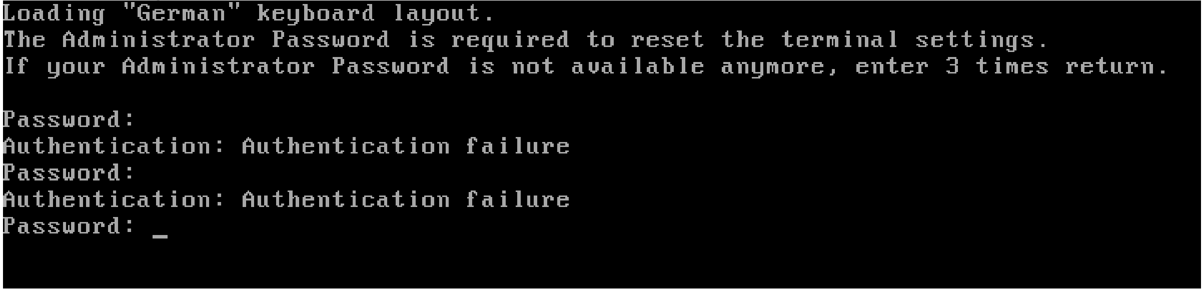
Solution

- Change the administrator password using IGEL UMS via **Setup > Security > Password > Administrator**
  or
- Reset the device using IGEL UMS via **Thin Clients > 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):

1. Press the [ESC] key repeatedly in rapid succession while the device is booting.
   This will bring up the boot menu.

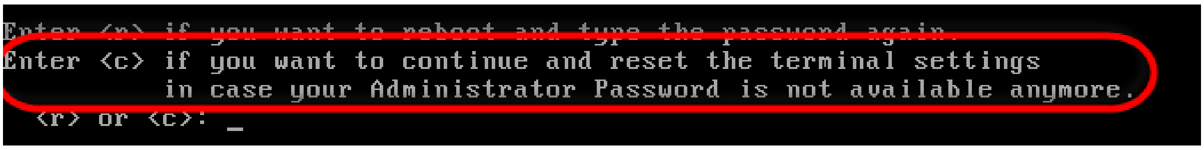

Quiet boot
Verbose boot
Emergency boot (setup only)
Failsafe boot with CRC check
Reset to factory defaults

2. Choose **Reset to factory defaults** and press [Enter].
   The following will be displayed:



```
Loading "German" keyboard layout.
The Administrator Password is required to reset the terminal settings.
If your Administrator Password is not available anymore, enter 3 times return.

Password:
Authentication: Authentication failure
Password:
Authentication: Authentication failure
Password: _
```

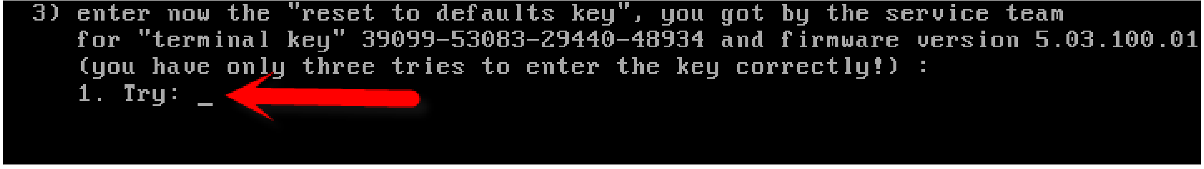
3. Press [Enter] three times without supplying a password.



```
Enter <r> if you want to reboot and type the password again.
Enter <c> if you want to continue and reset the terminal settings
         in case your Administrator Password is not available anymore.
  <r> or <c>: _
```

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[24] 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.



```
  3) enter now the "reset to defaults key", you got by the service team
     for "terminal key" 39099-53083-29440-48934 and firmware version 5.03.100.01
     (you have only three tries to enter the key correctly!) :
     1. Try: _
```

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.

[24] mailto:license@igel.com

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 chapter of the UDC3 Reference Manual.

> **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.

> **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.

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
   ```

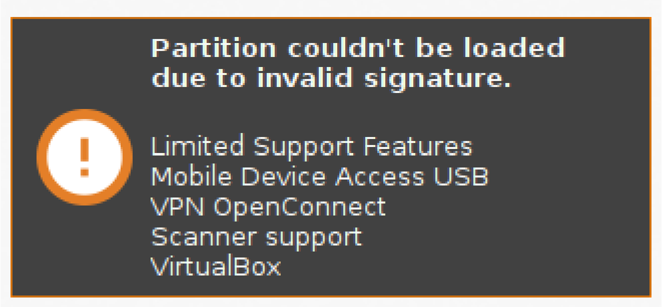
For further information about custom boot commands, see Custom Boot Command.

Solving Issues with Signed Partitions

Error: "Partition couldn't be loaded due to invalid signature"

Symptom

During operation, a system message like this appears:



Partition couldn't be loaded due to invalid signature.

Limited Support Features
Mobile Device Access USB
VPN OpenConnect
Scanner support
VirtualBox

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.) 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

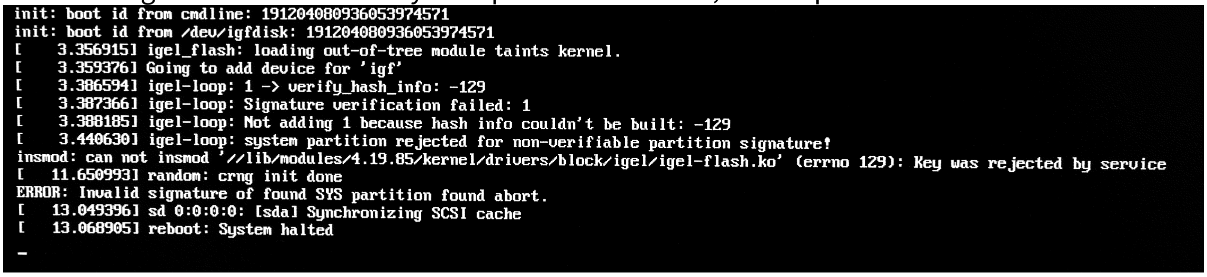
Problem

- 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

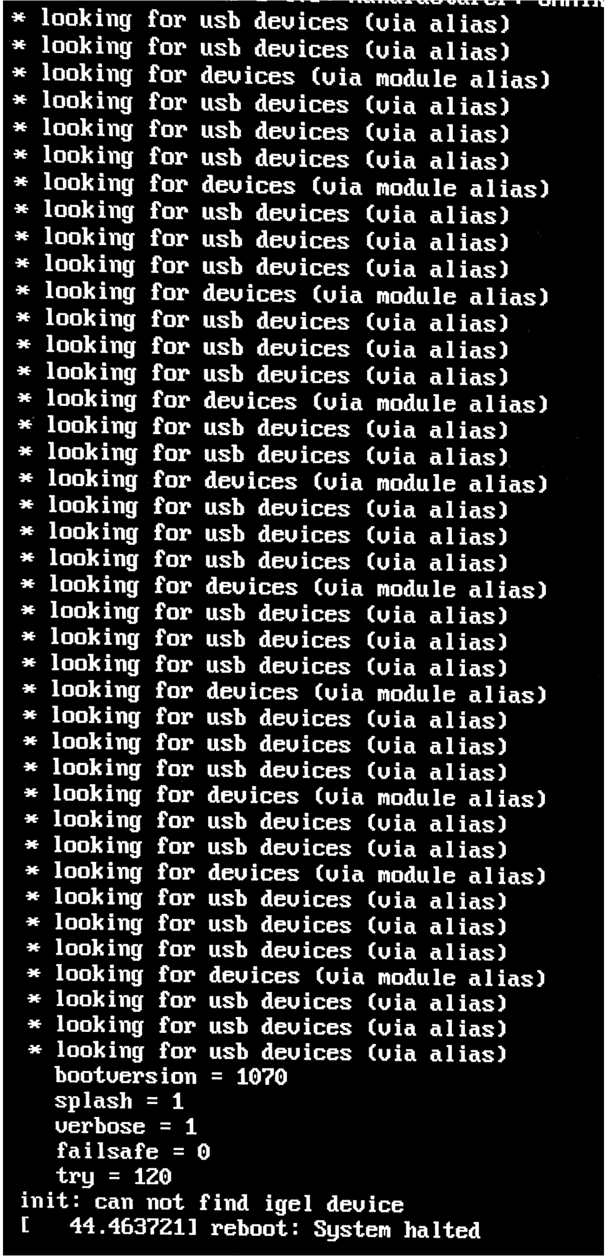
To obtain further details:

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:



```
init: boot id from cmdline: 1912040809360539745 71
init: boot id from /dev/igfdisk: 19120408093605397457 1
[    3.356915] igel_flash: loading out-of-tree module taints kernel.
[    3.359376] Going to add device for 'igf'
[    3.386594] igel-loop: 1 -> verify_hash_info: -129
[    3.387366] igel-loop: Signature verification failed: 1
[    3.388185] igel-loop: Not adding 1 because hash info couldn't be built: -129
[    3.440630] igel-loop: system partition rejected for non-verifiable partition signature!
insmod: can not insmod '//lib/modules/4.19.85/kernel/drivers/block/igel/igel-flash.ko' (errno 129): Key was rejected by service
[   11.650993] random: crng init done
ERROR: Invalid signature of found SYS partition found abort.
[   13.049396] sd 0:0:0:0: [sda] Synchronizing SCSI cache
[   13.068905] reboot: System halted
_
```

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 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 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 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)
  bootversion = 1070
  splash = 1
  verbose = 1
  failsafe = 0
  try = 120
init: can not find igel device
[   44.463721] reboot: System halted
```

Solution

▶ Install IGEL OS anew on the device with IGEL OS Creator (OSC). For instructions, see the Installation chapter of the UDC3 Reference Manual.

ⓘ **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.

ⓘ **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.

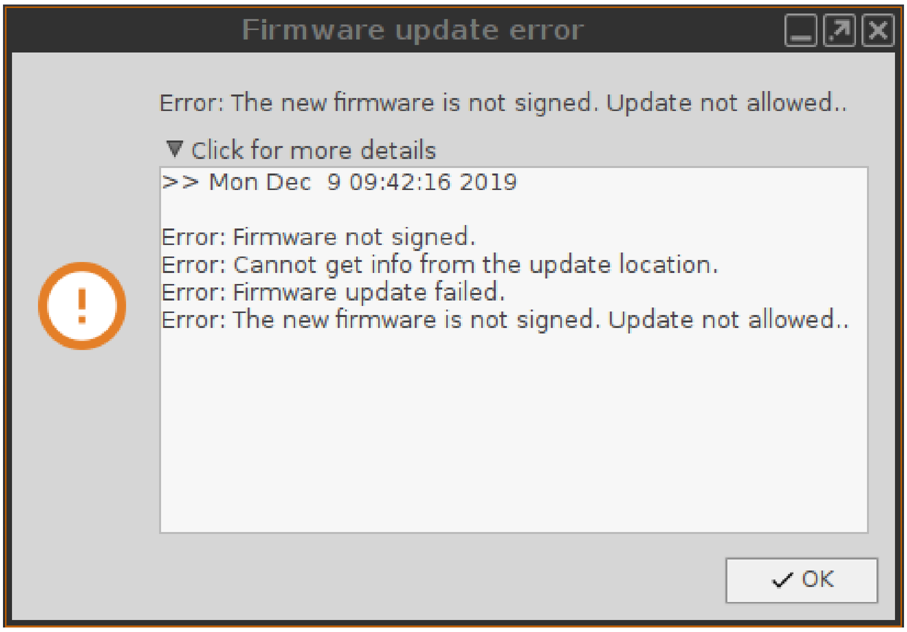
ⓘ **Preservation of Licenses**

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:



Error: The new firmware is not signed. Update not allowed..

```
>> Mon Dec  9 09:42:16 2019

Error: Firmware not signed.
Error: Cannot get info from the update location.
Error: Firmware update failed.
Error: The new firmware is not signed. Update not allowed..
```

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

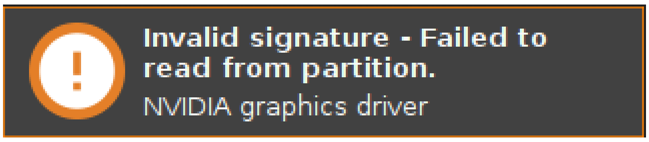
▶ If you want to downgrade from IGEL OS 11.03 to IGEL OS 11.02, e. g. because you need certain older client versions, set the update source to IGEL OS 11.02.200.

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:



Invalid signature - Failed to read from partition.

NVIDIA graphics driver

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.) If the local Setup is not accessible, use the UMS.
2. Reboot the device.
   The device fetches the valid partition from the update source.

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

Disabling Features to Reduce Firmware Size

Symptom

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 Adobe Flash plugin partition
- 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 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. Activate your settings with **Apply** or **OK**.
4. Reboot the device.
5. Update the device.

ⓘ Use profiles with UMS in order to deactivate features on a group of devices.

Fabulatech USB Redirection Server Component

Issue

For Fabulatech USB Redirection, a special Fabulatech server component must be installed on the *Citrix* or RDP server (USB for Remote Desktop IGEL Edition). More detailed information on the function can be found on the Fabulatech partner site[25]. On this site the server component is available for download.

Current versions are (as of 2017-05-29):

- USB for Remote Desktop IGEL Edition Ver.3.1.5
- USB for Remote Desktop IGEL Edition V5 Ver. 5.0.2

Problem

Which version is suitable for which IGEL Linux device?

Release notes of IGEL Linux only name the version of the *Fabulatech* client included but miss out the necessary server component version.

Solution

▶ All Fabulatech clients version 3.x require server component version 3.x

▶ All Fabulatech clients version 5.x require server component version 5.x

So for IGEL Linux thin clients following requirements apply:

- IGEL Linux v4 devices up to current version 4.13.270 require server component version 3.x
- IGEL Linux v5 devices up to version 5.02.100 require server component version 3.x
- IGEL Linux v5 devices from version 5.03.100 and later require server component version 5.x
- IGEL Linux 10.x requires server component version 5.x.

[25] http://www.usb-over-network.com/partners/igel/

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 Shared Workplace (SWP)

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

Network

Configuring Open VPN Sessions

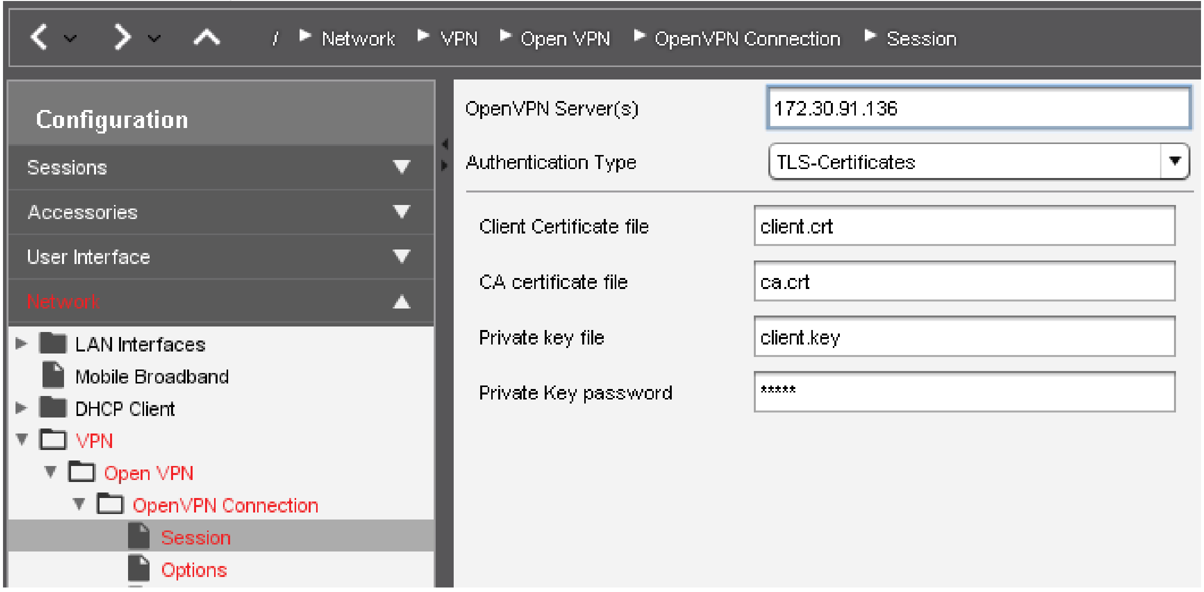
This document describes how to configure the *OpenVPN* Client on *IGEL Linux*.

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 448)".

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.



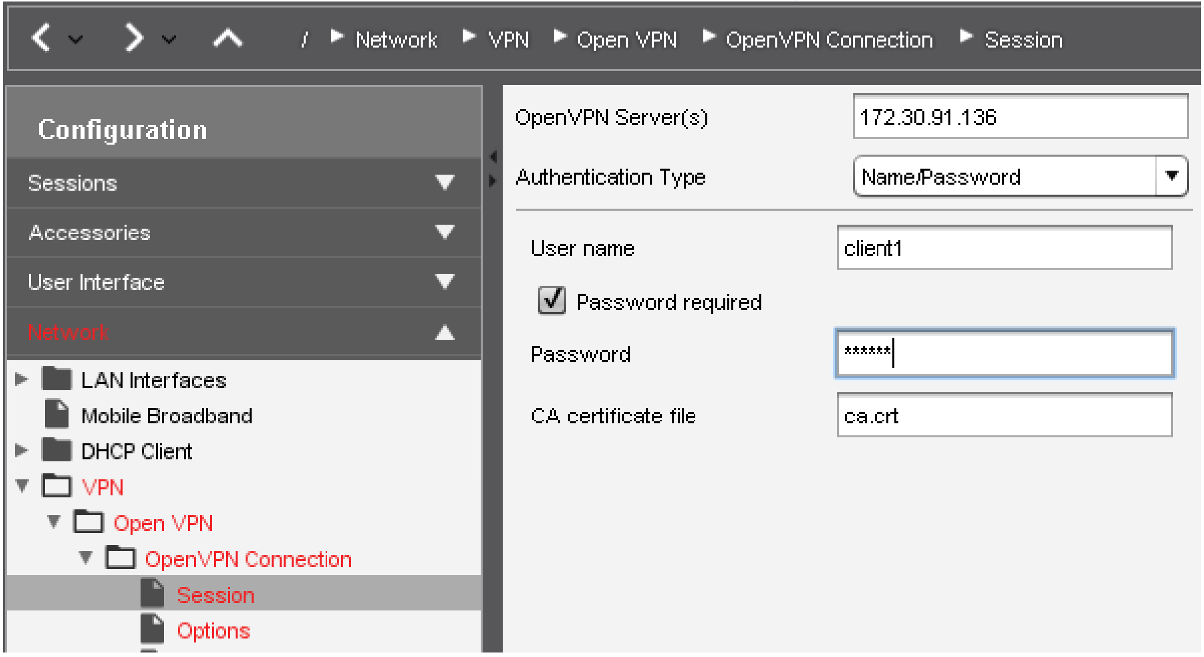
OpenVPN Server(s): 172.30.91.136
Authentication Type: TLS-Certificates
Client Certificate file: client.crt
CA certificate file: ca.crt
Private key file: client.key
Private Key password: *****

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**.



OpenVPN Server(s): 172.30.91.136

Authentication Type: Name/Password

User name: client1

☑ Password required

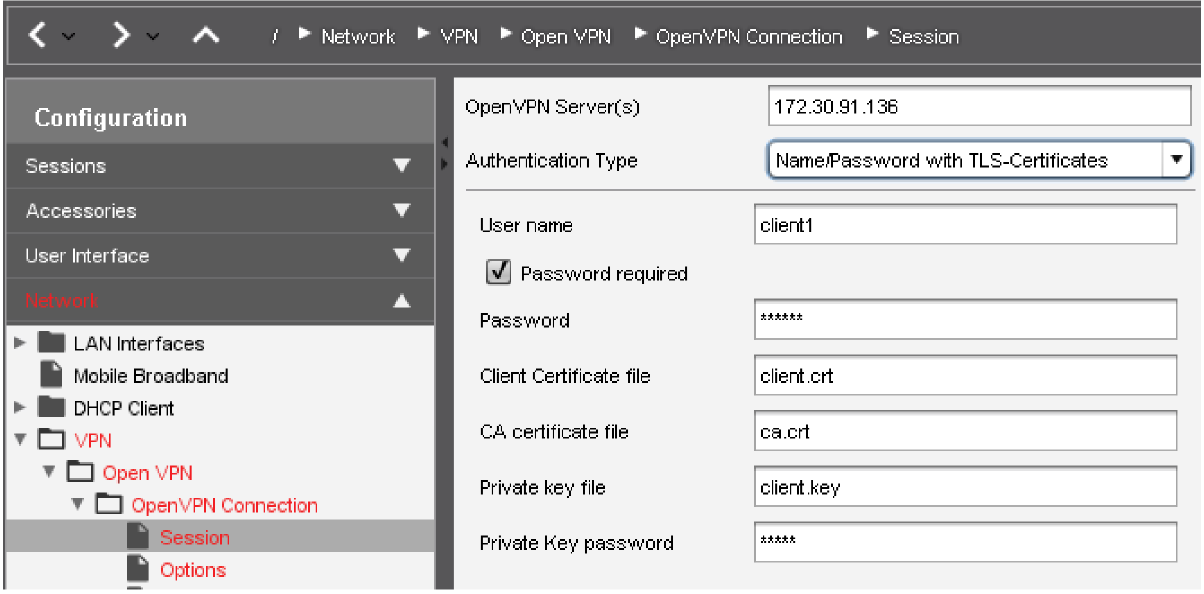
Password: ******

CA certificate file: ca.crt

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.



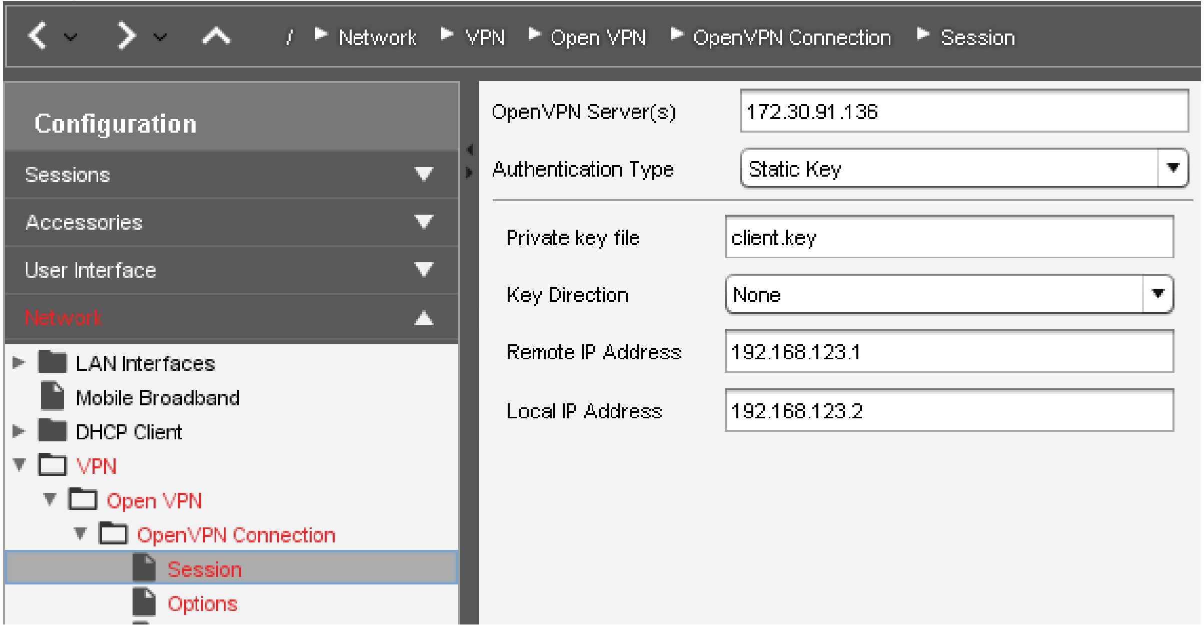
OpenVPN Server(s): 172.30.91.136
Authentication Type: Name/Password with TLS-Certificates
User name: client1
☑ Password required
Password: ******
Client Certificate file: client.crt
CA certificate file: ca.crt
Private key file: client.key
Private Key password: *****

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**.



OpenVPN Server(s): 172.30.91.136

Authentication Type: Static Key

Private key file: client.key

Key Direction: None

Remote IP Address: 192.168.123.1

Local IP Address: 192.168.123.2

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**.

> ⓘ 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 Configuring Open VPN Sessions (see page 437) or OpenVPN.

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:

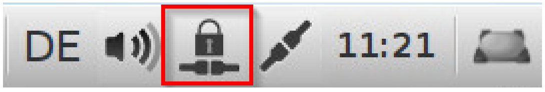
- **Proxy Username**
- **Proxy Password**

> ⓘ 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**.

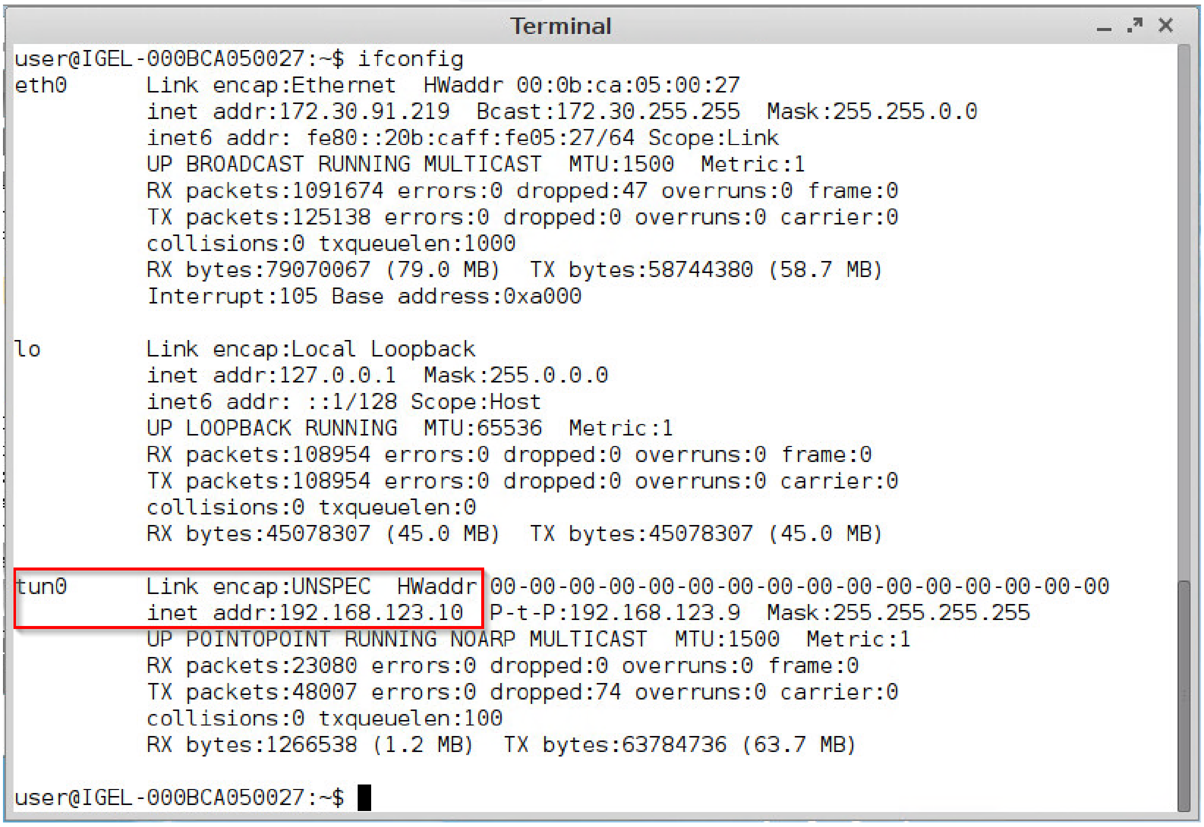
Checking the VPN Connection

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.



```
user@IGEL-000BCA050027:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0b:ca:05:00:27
          inet addr:172.30.91.219  Bcast:172.30.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20b:caff:fe05:27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1091674 errors:0 dropped:47 overruns:0 frame:0
          TX packets:125138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79070067 (79.0 MB)  TX bytes:58744380 (58.7 MB)
          Interrupt:105 Base address:0xa000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:108954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108954 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:45078307 (45.0 MB)  TX bytes:45078307 (45.0 MB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.123.10  P-t-P:192.168.123.9  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:23080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48007 errors:0 dropped:74 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1266538 (1.2 MB)  TX bytes:63784736 (63.7 MB)

user@IGEL-000BCA050027:~$
```

4. Additionally, check whether you can ping the VPN server's private IP address.

Automatically Starting 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

Further information about *OpenVPN* can be found in

- the OpenVPN how-to[26] and
- the OpenVPN manual page[27]

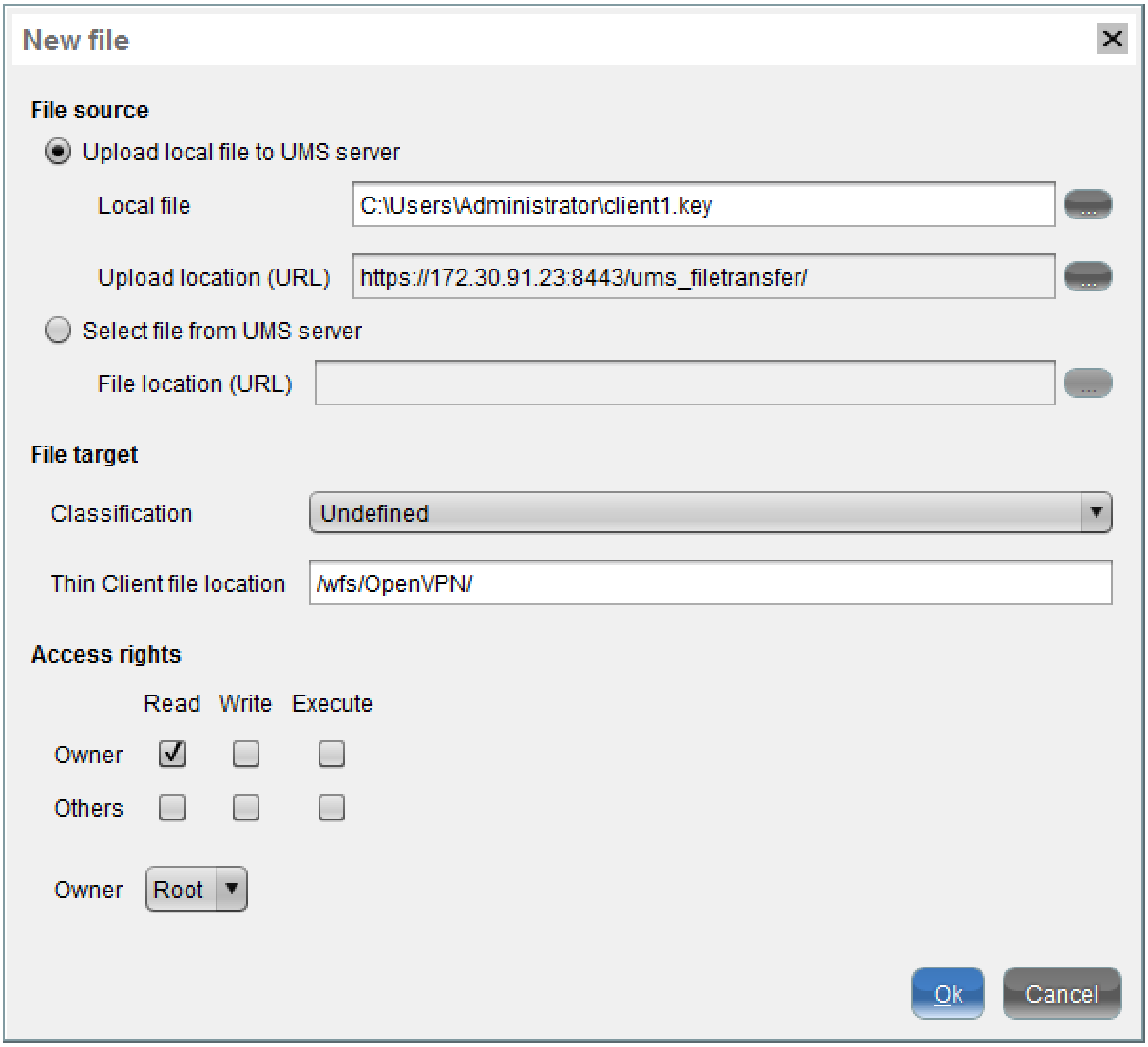
maintained by the *OpenVPN* project.

[26] https://openvpn.net/index.php/open-source/documentation/howto.html
[27] 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.**



New file

File source

● Upload local file to UMS server

Local file: C:\Users\Administrator\client1.key

Upload location (URL): https://172.30.91.23:8443/ums_filetransfer/

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Thin Client file location: /wfs/OpenVPN/

Access rights

	Read	Write	Execute
Owner	☑	□	□
Others	□	□	□

Owner: Root

Running 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 Can I Configure OpenVPN with an .ovpn or .conf File?

Solution Based on Experience from the Field

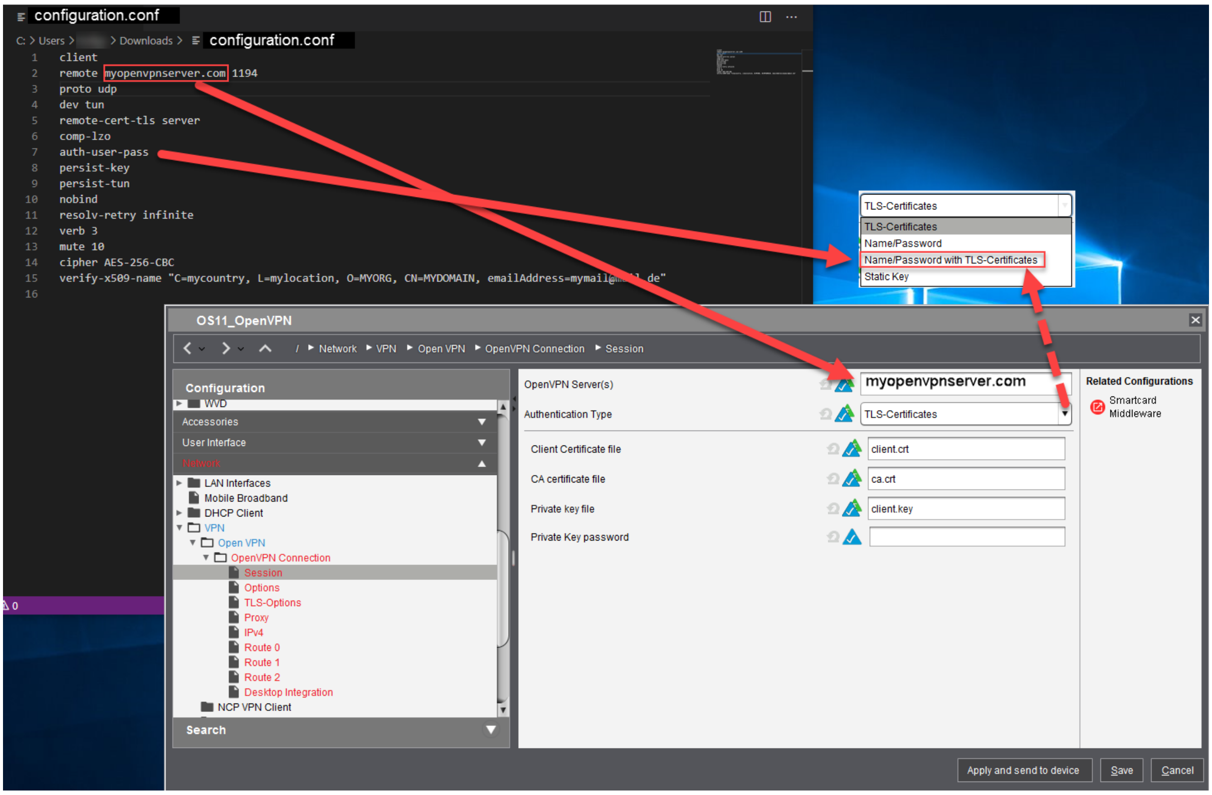
This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Overview

You can use the `.ovpn` or the `.conf` file from your firewall to configure OpenVPN for your IGEL OS device.

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:



configuration.conf

C: > Users > [redacted] > Downloads > configuration.conf

```
client
remote myopenvpnserver.com 1194
proto udp
dev tun
remote-cert-tls server
comp-lzo
auth-user-pass
persist-key
persist-tun
nobind
resolv-retry infinite
verb 3
mute 10
cipher AES-256-CBC
verify-x509-name "C=mycountry, L=mylocation, O=MYORG, CN=MYDOMAIN, emailAddress=mymail@[redacted].de"

```

OS11_OpenVPN

/ ▸ Network ▸ VPN ▸ Open VPN ▸ OpenVPN Connection ▸ Session

OpenVPN Server(s): myopenvpnserver.com

Authentication Type: TLS-Certificates

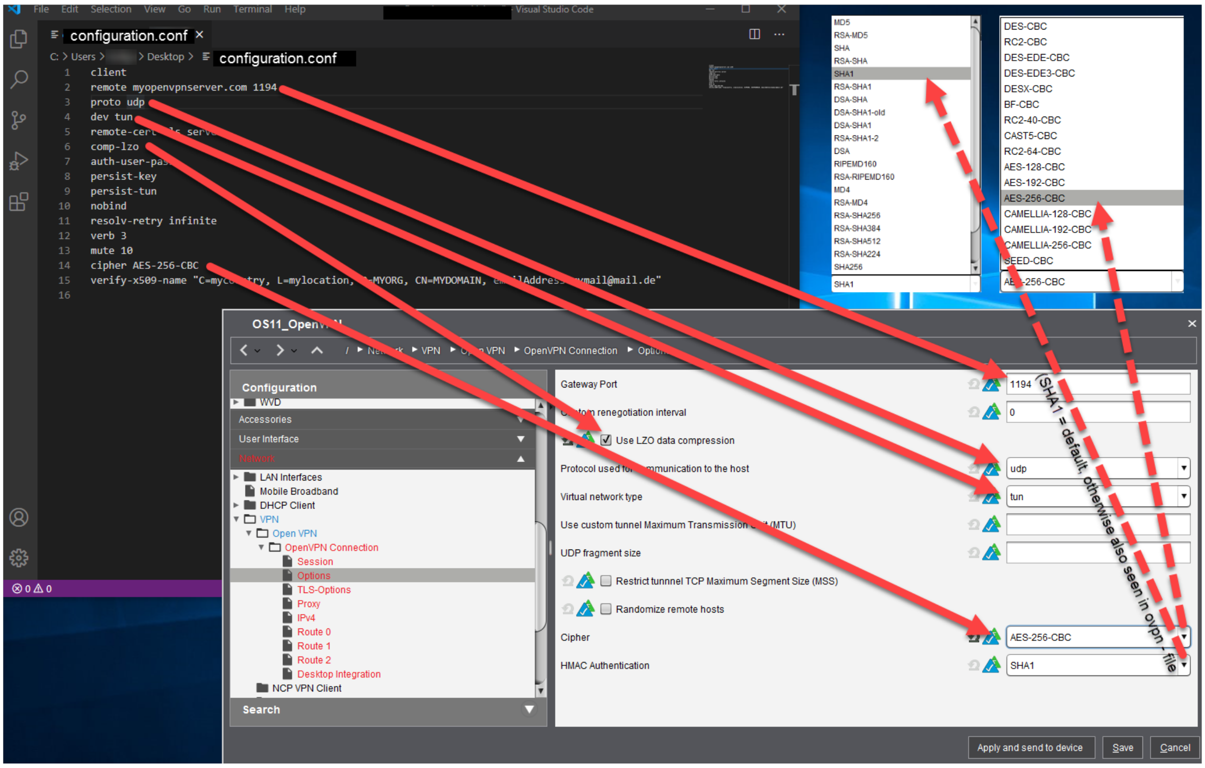
Client Certificate file: client.crt

CA certificate file: ca.crt

Private key file: client.key

Private Key password:

5. Go to **Network > VPN > Open VPN >** [your OpenVPN session] **> Options** and edit the settings as follows:



[redacted] - Visual Studio Code

configuration.conf

C: > Users > Desktop > configuration.conf

```
client
remote myopenvpnserver.com 1194
proto udp
dev tun
remote-cert-tls server
comp-lzo
auth-user-pass
persist-key
persist-tun
nobind
resolv-retry infinite
verb 3
mute 10
cipher AES-256-CBC
verify-x509-name "C=mycountry, L=mylocation, O=MYORG, CN=MYDOMAIN, emailAddress=mymail@mail.de"

```

OS11_OpenVPN

Network ▸ VPN ▸ Open VPN ▸ OpenVPN Connection ▸ Options

Gateway Port: 1194

Custom renegotiation interval: 0

☑ Use LZO data compression

Protocol used for communication to the host: udp

Virtual network type: tun

Use custom tunnel Maximum Transmission Unit (MTU):

UDP fragment size:

☐ Restrict tunnnel TCP Maximum Segment Size (MSS)

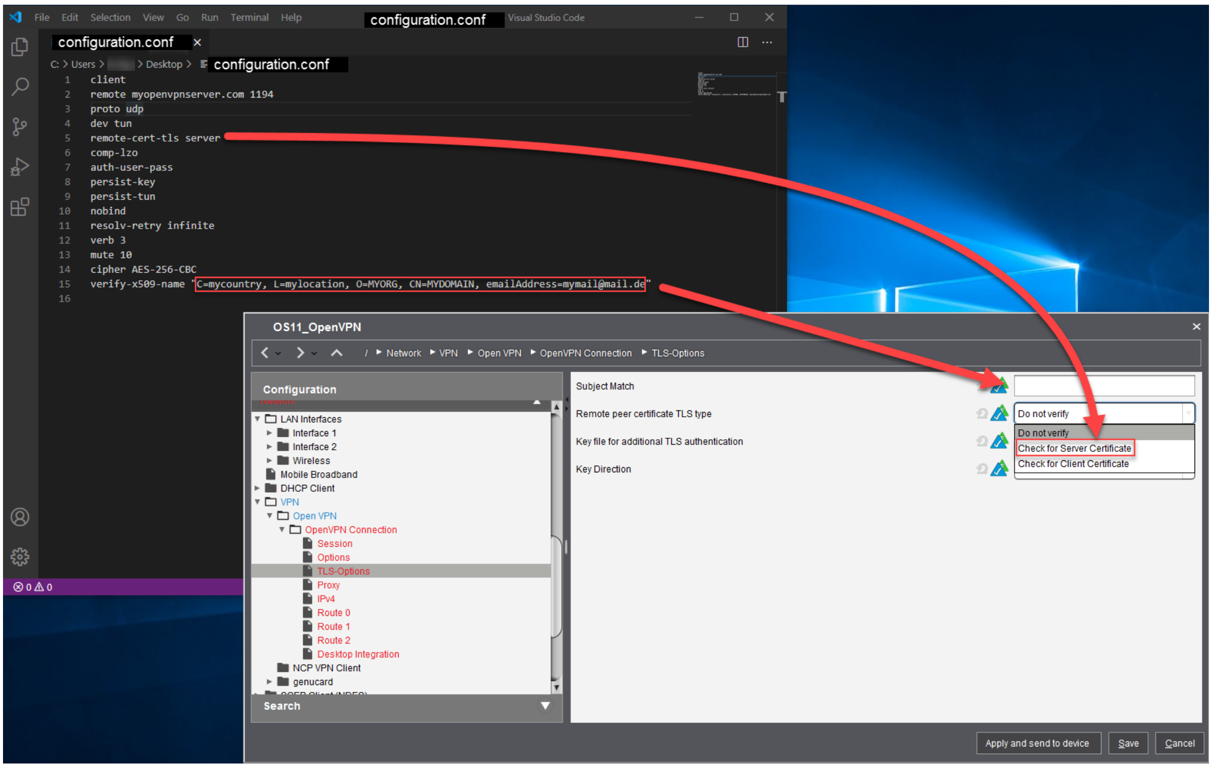
☐ Randomize remote hosts

Cipher: AES-256-CBC

HMAC Authentication: SHA1

(SHA1 = default, otherwise also seen in ovpn - file)

6. Go to **Network > VPN > Open VPN >** [your OpenVPN session] **> TLS Options** and edit the settings as follows:



configuration.conf

```
client
remote myopenvpnserver.com 1194
proto udp
dev tun
remote-cert-tls server
comp-lzo
auth-user-pass
persist-key
persist-tun
nobind
resolv-retry infinite
verb 3
mute 10
cipher AES-256-CBC
verify-x509-name "C=mycountry, L=mylocation, O=MYORG, CN=MYDOMAIN, emailAddress=mymail@mail.de"

```

OS11_OpenVPN

/ ▸ Network ▸ VPN ▸ Open VPN ▸ OpenVPN Connection ▸ TLS-Options

Subject Match:

Remote peer certificate TLS type: Do not verify

- Do not verify
- Check for Server Certificate
- Check for Client Certificate

Key file for additional TLS authentication

Key Direction

Creating the Certificate/Key Files

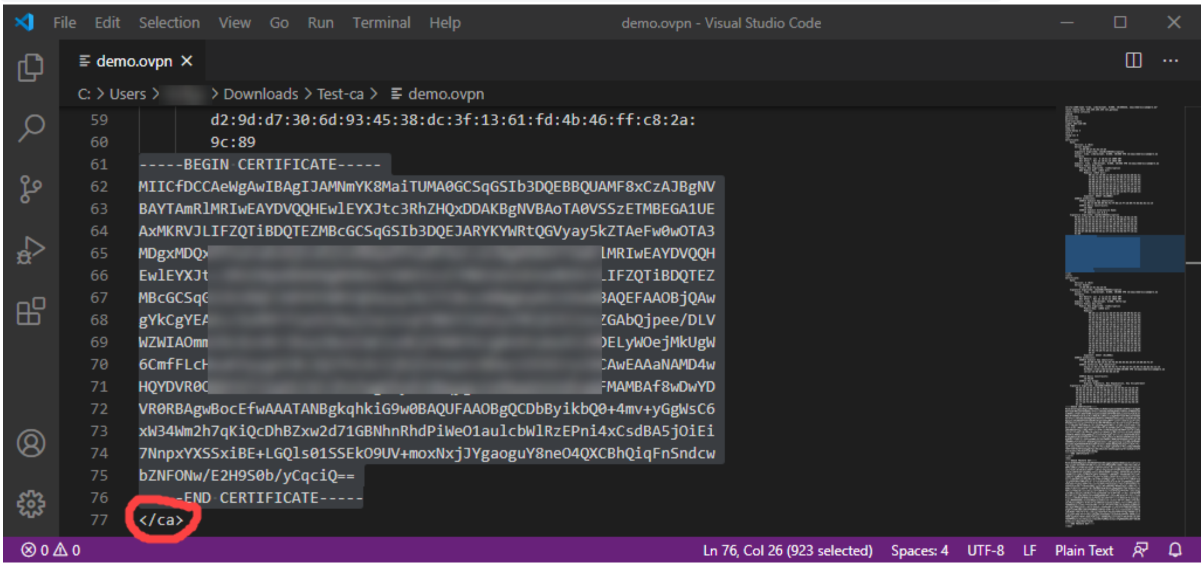
If you already have the following files, you can skip this section and jump to Transferring the Files to the UMS (see page 455):

- `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).

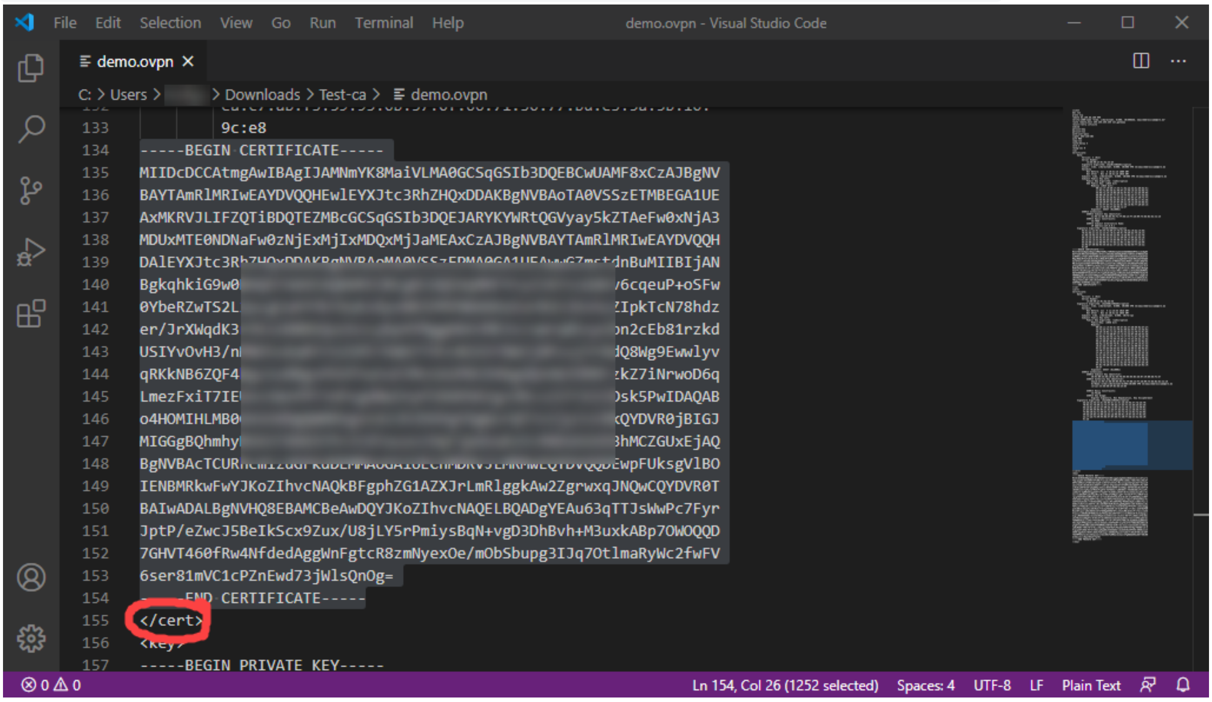
2. Go to the section tagged as `<ca> ... </ca>` and copy the marked certificate, including `----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.


File
Edit
Selection
View
Go
Run
Terminal
Help
demo.ovpn - Visual Studio Code
demo.ovpn
C: > Users > [redacted] > Downloads > Test-ca > demo.ovpn
Ln 76, Col 26 (923 selected)
Spaces: 4
UTF-8
LF
Plain Text

```
        d2:9d:d7:30:6d:93:45:38:dc:3f:13:61:fd:4b:46:ff:c8:2a:
        9c:89
-----BEGIN CERTIFICATE-----
MIICfDCCAeWgAwIBAgIJAMNmYK8MaiTUMA0GCSqGSIb3DQEBBQUAMF8xCzAJBgNV
BAYTAmRlMRIwEAYDVQQHEwlEYXJtc3RhZHQxDDAKBgNVBAoTA0VSSzETMBEGA1UE
AxMKRVJLIFZQTiBDQTEZMBcGCSqGSIb3DQEJARYKYWRtQGVyay5kZTAeFw0wOTA3
MDgxMDQx[redacted]lMRIwEAYDVQQH
EwlEYXJt[redacted]LIFZQTiBDQTEZ
MBcGCSqG[redacted]BAQEFAAOBjQAw
gYkCgYEA[redacted]ZGAbQjpee/DLV
WZWIAOmm[redacted]DELyWOejMkUgW
6CmfFLcH[redacted]CAwEAAaNAMD4w
HQYDVR0O[redacted]FMAMBAf8wDwYD
VR0RBAgwBocEfwAAATANBgkqhkiG9w0BAQUFAAOBgQCDbByikbQ0+4mv+yGgWsC6
xW34Wm2h7qKiQcDhBZxw2d71GBNhnRhdPiWeO1aulcbWlRzEPni4xCsdBA5jOiEi
7NnpxYXSSxiBE+LGQls01SSEkO9UV+moxNxjJYgaoguY8neO4QXCBhQiqFnSndcw
bZNFONw/E2H9S0b/yCqciQ==
-----END CERTIFICATE-----
</ca>
```

3. Paste the text to the editor and save it to a file named `ca.crt` (file type "All files").

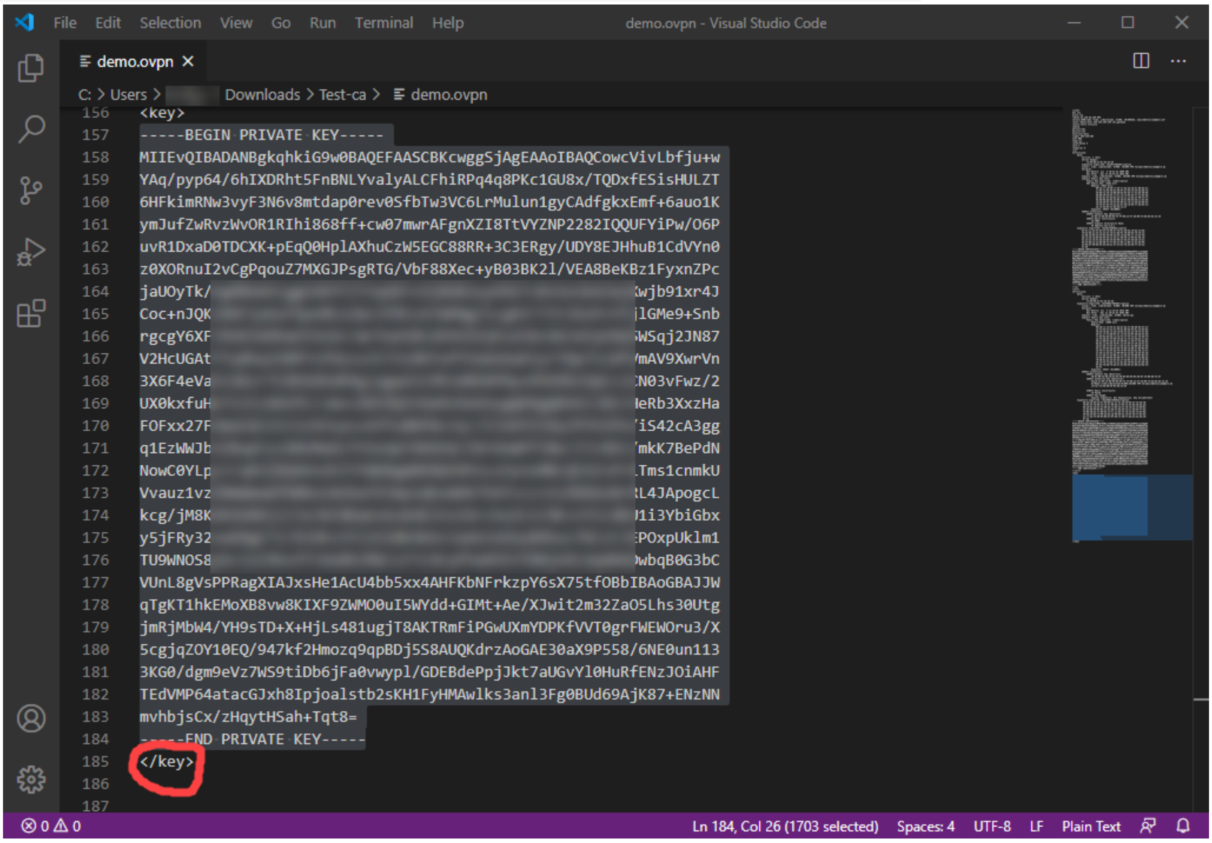
4. Go to the section tagged as `<cert> ... </cert>` and copy the marked certificate, including `----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.


File
Edit
Selection
View
Go
Run
Terminal
Help
demo.ovpn - Visual Studio Code
demo.ovpn
C: > Users > [redacted] > Downloads > Test-ca > demo.ovpn
Ln 154, Col 26 (1252 selected)
Spaces: 4
UTF-8
LF
Plain Text

```
        9c:e8
-----BEGIN CERTIFICATE-----
MIIDcDCCAtmgAwIBAgIJAMNmYK8MaiVLMA0GCSqGSIb3DQEBCwUAMF8xCzAJBgNV
BAYTAmRlMRIwEAYDVQQHEwlEYXJtc3RhZHQxDDAKBgNVBAoTA0VSSzETMBEGA1UE
AxMKRVJLIFZQTiBDQTEZMBcGCSqGSIb3DQEJARYKYWRtQGVyay5kZTAeFw0xNjA3
MDUxMTE0NDNaFw0zNjExMjIxMDQxMjJaMEAxCzAJBgNVBAYTAmRlMRIwEAYDVQQH
DAlEYXJtc3R[redacted]dnBuMIIBIjAN
BgkqhkiG9w0[redacted]/6cqeuP+oSFw
0YbeRZwTS2L[redacted]ZIpkTcN78hdz
er/JrXWqdK3[redacted]pn2cEb81rzkd
USIYvOvH3/n[redacted]dQ8Wg9Ewwlyv
qRKkNB6ZQF4[redacted]zkZ7iNrwoD6q
LmezFxiT7IE[redacted]Dsk5PwIDAQAB
o4HOMIHLMB0[redacted]kQYDVR0jBIGJ
MIGGgBQhmhy[redacted]3hMCZGUxEjAQ
BgNVBAcTCUR[redacted]EwpFUksgV1BO
IENBMRkwFwYJKoZIhvcNAQkBFgphZG1AZXJrLmRlggkAw2ZgrwxqJNQwCQYDVR0T
BAIwADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADgYEAu63qTTJsWwPc7Fyr
JptP/eZwcJ5BeIkScx9Zux/U8jLY5rPmiysBqN+vgD3DhBvh+M3uxkABp7OWOQQD
7GHVT460fRw4NfdedAggWnFgtcR8zmNyexOe/mObSbupg3IJq7OtlmaRyWc2fwFV
6ser81mVC1cPZnEwd73jWlsQnOg=
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
```

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-----`.



File
Edit
Selection
View
Go
Run
Terminal
Help
demo.ovpn - Visual Studio Code
demo.ovpn ×
C: > Users > [redacted] Downloads > Test-ca > demo.ovpn
⊗ 0 ⚠ 0
Ln 184, Col 26 (1703 selected)
Spaces: 4
UTF-8
LF
Plain Text

```
<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCowcVivLbfju+w
YAq/pyp64/6hIXDRht5FnBNLYvalyALCFhiRPq4q8PKc1GU8x/TQDxfESisHULZT
6HFkimRNw3vyF3N6v8mtdap0rev0SfbTw3VC6LrMulun1gyCAdfgkxEmf+6auo1K
ymJufZwRvzWvOR1RIhi868ff+cw07mwrAFgnXZI8TtVYZNP2282IQQUFYiPw/O6P
uvR1DxaD0TDCXK+pEqQ0HplAXhuCzW5EGC88RR+3C3ERgy/UDY8EJHhuB1CdVYn0
z0XORnuI2vCgPqouZ7MXGJPsgRTG/VbF88Xec+yB03BK2l/VEA8BeKBz1FyxnZPc
jaUOyTk/[redacted]wjb91xr4J
Coc+nJQK[redacted]lGMe9+Snb
rgcgY6XF[redacted]WSqj2JN87
V2HcUGAt[redacted]mAV9XwrVn
3X6F4eVa[redacted]N03vFwz/2
UX0kxfuH[redacted]eRb3XxzHa
FOFxx27F[redacted]iS42cA3gg
q1EzWWJb[redacted]mkK7BePdN
NowC0YLp[redacted]Tms1cnmkU
Vvauz1vz[redacted]L4JApogcL
kcg/jM8K[redacted]1i3YbiGbx
y5jFRy32[redacted]POxpUklm1
TU9WNOS8[redacted]wbqB0G3bC
VUnL8gVsPPRagXIAJxsHe1AcU4bb5xx4AHFKbNFrkzpY6sX75tfOBbIBAoGBAJJW
qTgKT1hkEMoXB8vw8KIXF9ZWMO0uI5WYdd+GIMt+Ae/XJwit2m32ZaO5Lhs30Utg
jmRjMbW4/YH9sTD+X+HjLs481ugjT8AKTRmFiPGwUXmYDPKfVVT0grFWEWOru3/X
5cgjqZOY10EQ/947kf2Hmozq9qpBDj5S8AUQKdrzAoGAE30aX9P558/6NE0un113
3KG0/dgm9eVz7WS9tiDb6jFa0vwypl/GDEBdePpjJkt7aUGvYl0HuRfENzJOiAHF
TEdVMP64atacGJxh8Ipjoalstb2sKH1FyHMAwlks3anl3Fg0BUd69AjK87+ENzNN
mvhbjsCx/zHqytHSah+Tqt8=
-----END PRIVATE KEY-----
</key>
```

7. Paste the text to the editor and save it to a file named `client.key` (file type "All files").

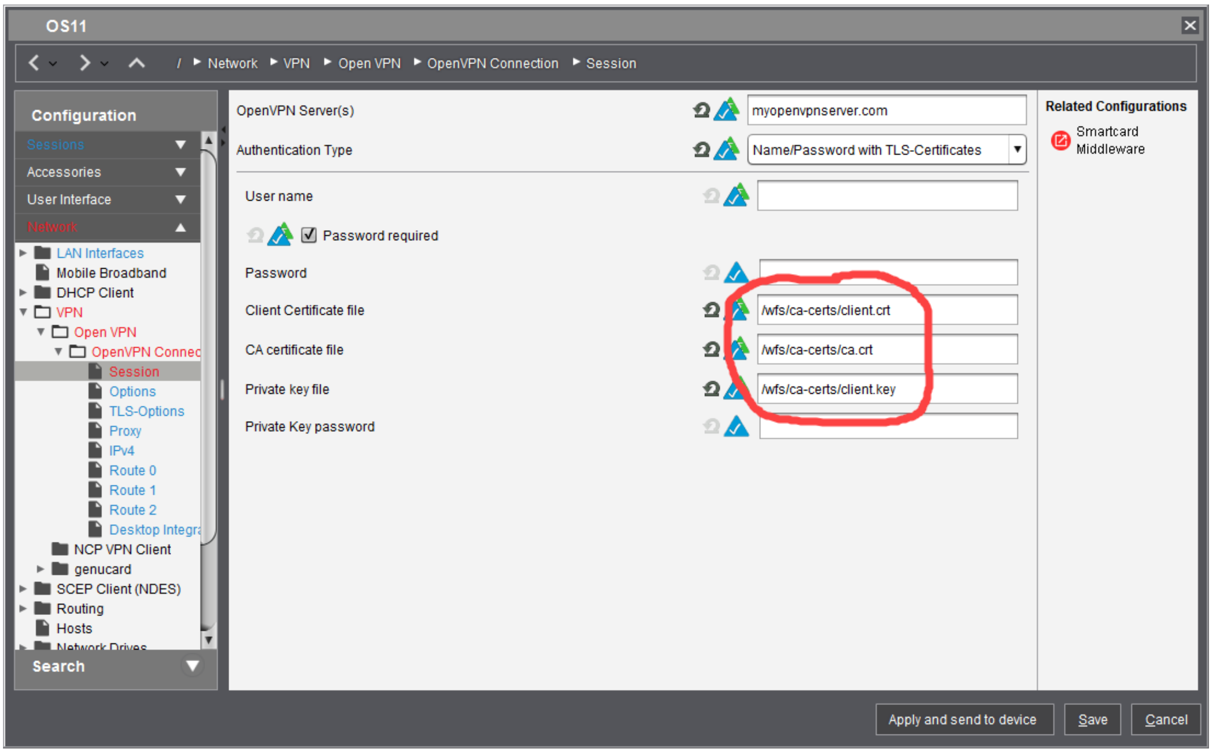
Transferring the Files to the UMS

1. In the UMS, create a file object for each certificate/key file; set **Classification** to "Common Certificate (all purpose)". For details, see Registering a File on the UMS Server.
2. Assign the file objects to the endpoint devices on which you want to use the OpenVPN connection. For details, see Transferring a File to a Device.

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:



OpenVPN Server(s): myopenvpnserver.com

Authentication Type: Name/Password with TLS-Certificates

User name:

☑ Password required

Password:

Client Certificate file: /wfs/ca-certs/client.crt

CA certificate file: /wfs/ca-certs/ca.crt

Private key file: /wfs/ca-certs/client.key

Private Key password:

3. Apply the profile to the endpoint devices on which you want to use the OpenVPN connection.

Configuring 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`

Connecting to a Wi-Fi Network with Hidden SSID

Symptom

The device does not connect to a wireless network with hidden SSID.

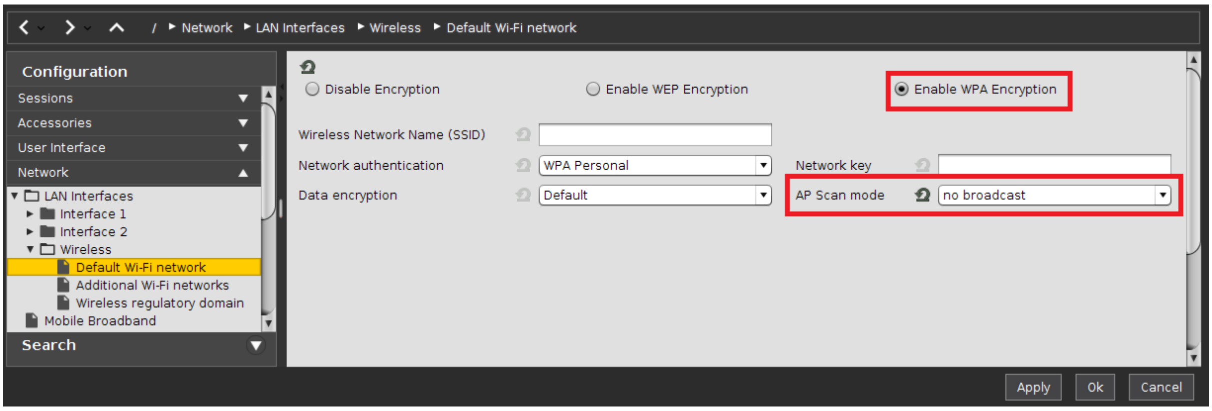
Problem

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.



○ Disable Encryption ○ Enable WEP Encryption ● Enable WPA Encryption

Wireless Network Name (SSID):

Network authentication: WPA Personal

Data encryption: Default

Network key:

AP Scan mode: no broadcast

Improving 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 Configuring Wi-Fi Network Roaming (see page 457).

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.

Preventing 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.

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 554).

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.

Deploying 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.

Configuring the Network Interface

This describes how to configure the WiFi interface.

> ⓘ In both cases, SCEP and files from UMS, the device needs to have a working Ethernet or WiFi connection to the SCEP server or the UMS first, so that it can fetch the necessary certificates, before it can connect to the target WiFi.

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 574).
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 574).

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**.

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.

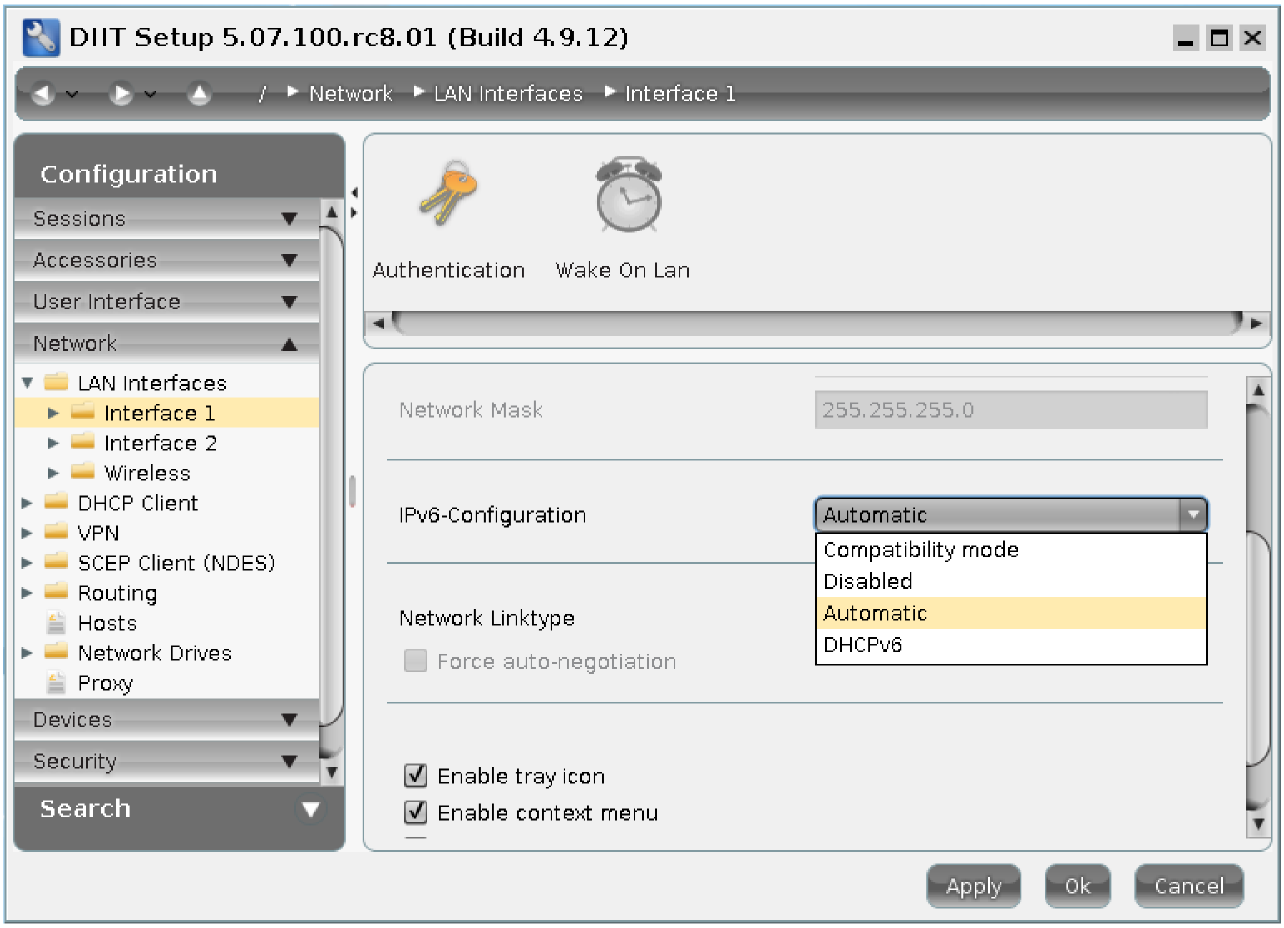
Application Scenario

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 Configurations

IPv6 support is configured by network interface in **Network > LAN Interfaces:**



Network Mask: 255.255.255.0

IPv6-Configuration: Automatic

Network Linktype

□ Force auto-negotiation

☑ Enable tray icon

☑ Enable context menu

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.

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 913).

- Debuglog Partition (see page 474)
- Syslog (see page 476)
- Tcpdump (see page 477)
- Netlog (see page 480)

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 480) 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[28].

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
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		

[28] 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)[29] manpage.

[29] 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

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 / false
	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	true / 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	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 > Registry		
	> Logfile rotate size in MiB	debug.tools.netlog.ethtool.rotate_size	2, 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 / false
	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,error_counter,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	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.ifconfig.rotate_size	2, 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 / false
	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 / false
	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 / false
	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 / false
	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	ping_errors, no_trigger
	• **ping_errors**: log only if ping test fails • **no_trigger**: log on every netlog run		

Making a Telnet Connection from IGEL Linux

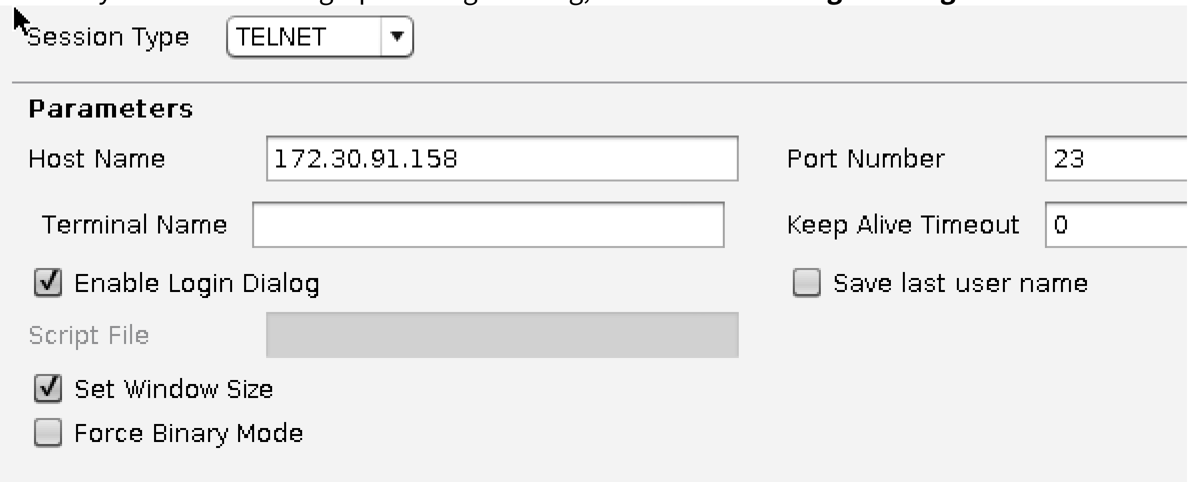
Issue

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.**



Session Type: TELNET

Parameters

Host Name: 172.30.91.158

Port Number: 23

Terminal Name:

Keep Alive Timeout: 0

☑ Enable Login Dialog

□ Save last user name

Script File

☑ Set Window Size

□ Force Binary Mode

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.

Configuring 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.

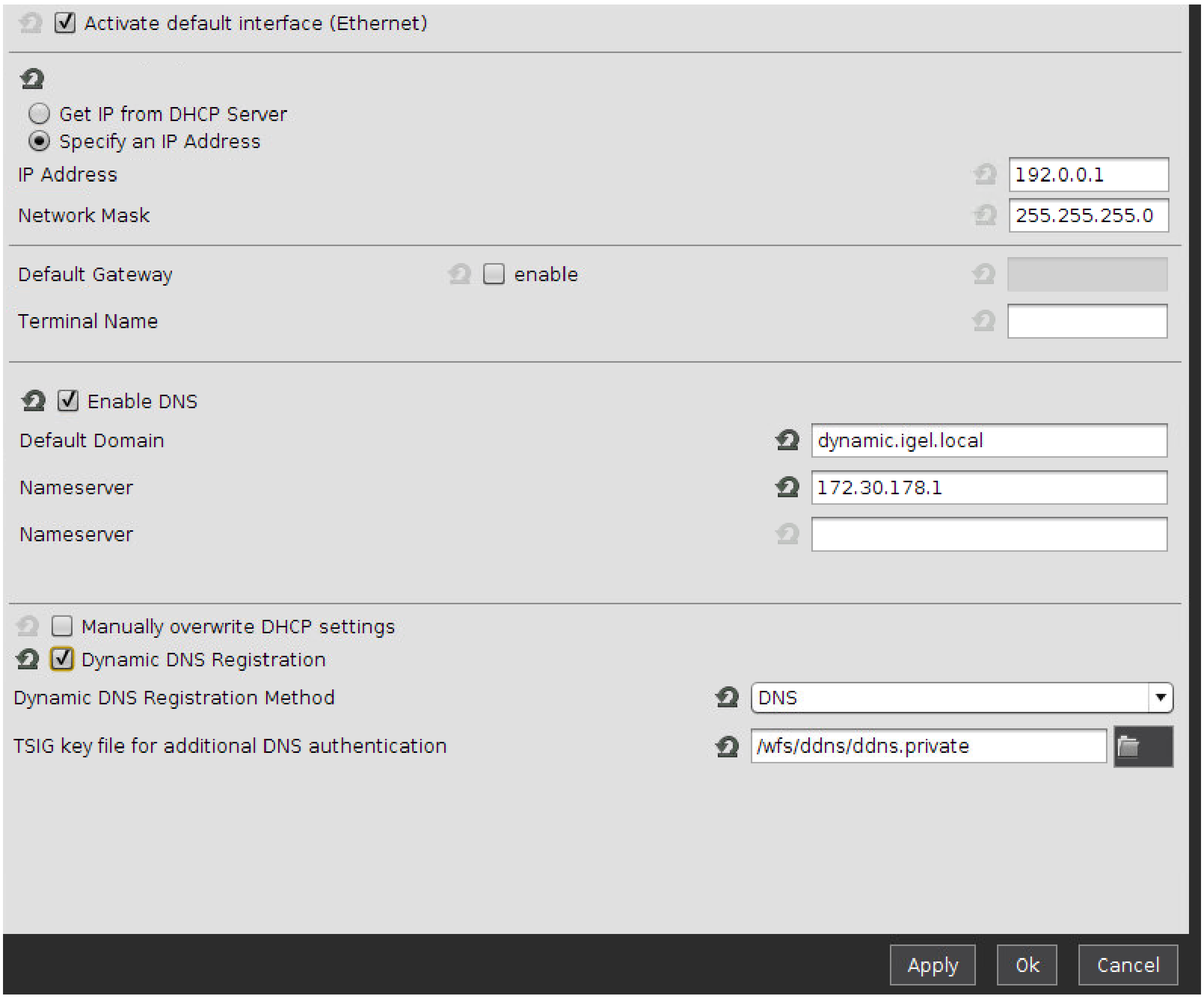
> ⓘ This only works for BIND9 or other nameservers supporting TSIG, not for Microsoft Active Directory servers.

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

Changing 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 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 can't be accessed anymore, and the user can't manage wireless networks.

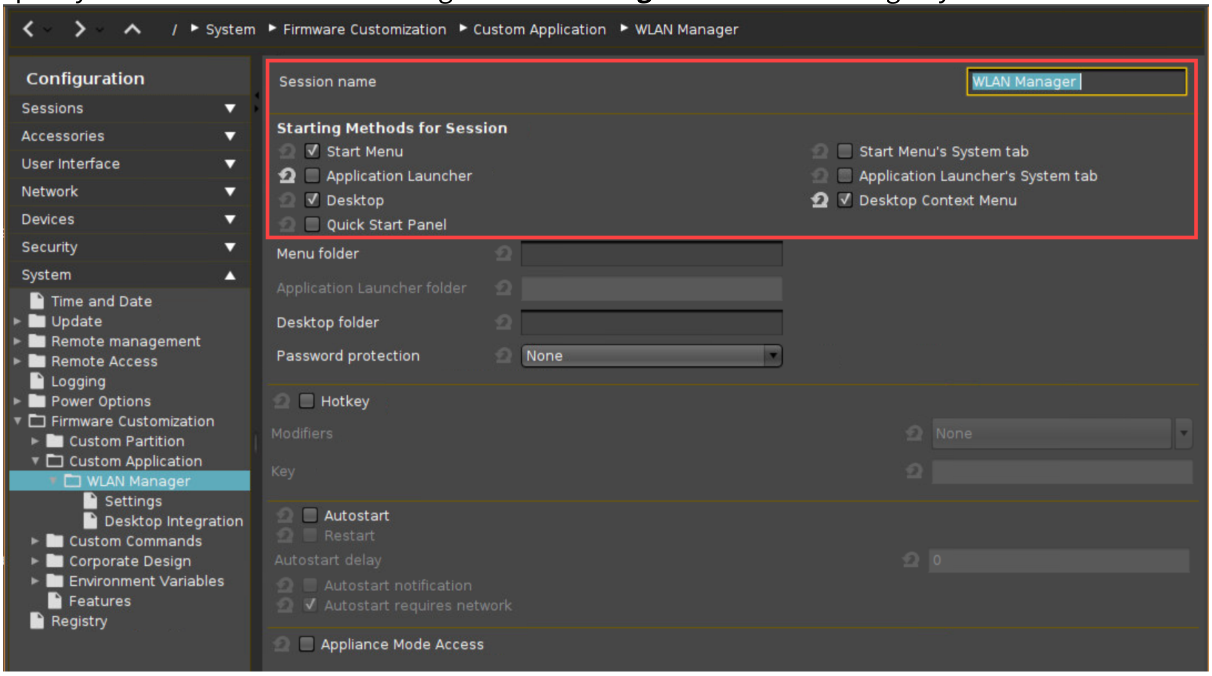
Environment

- 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.



Session name: WLAN Manager

Starting Methods for Session

☑ Start Menu
□ Application Launcher
☑ Desktop
□ Quick Start Panel
□ Start Menu's System tab
□ Application Launcher's System tab
☑ Desktop Context Menu

Menu folder:

Application Launcher folder:

Desktop folder:

Password protection: None

□ Hotkey

Modifiers: None

Key:

□ Autostart

□ Restart

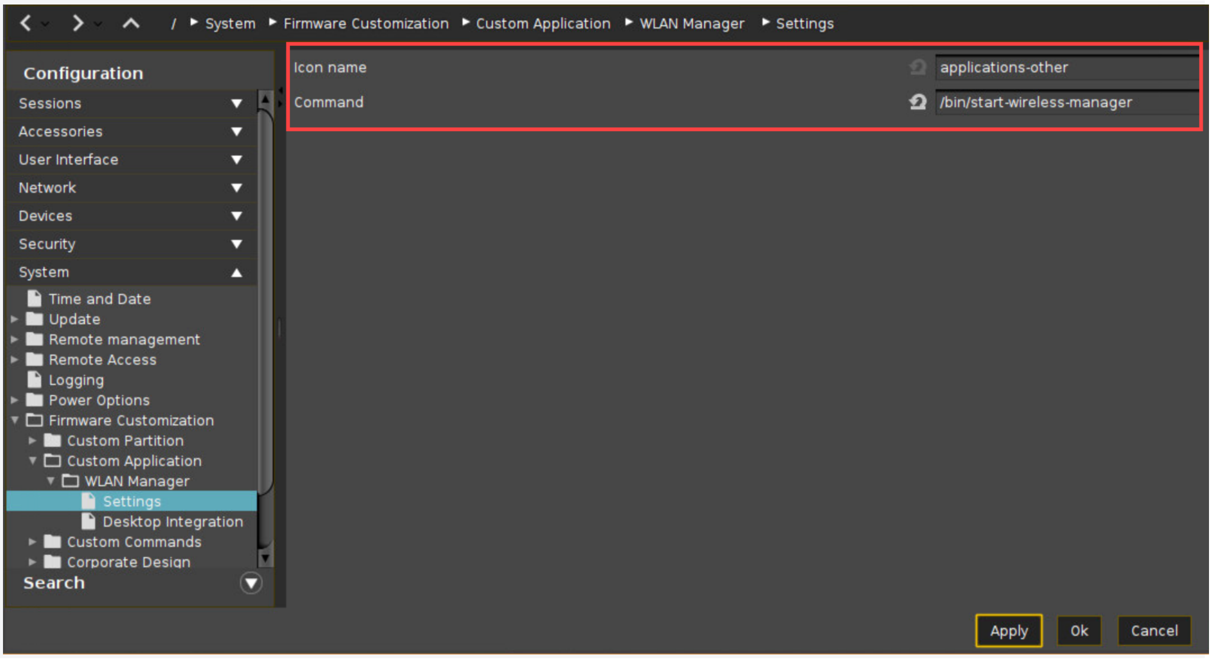
Autostart delay: 0

□ Autostart notification

☑ Autostart requires network

□ Appliance Mode Access

4. Under **Settings**, specify the **Icon name** and enter the following **Command**: `/bin/start-wireless-manager`



Icon name: applications-other

Command: /bin/start-wireless-manager

5. Click **Apply** or **OK**.
   The Wireless Manager can now be launched via the configured starting methods.

Security

Securing IGEL OS Endpoints

This document describes settings for IGEL OS that will increase security.

It applies to the following:

- IGEL UD LX and IZ devices
- UD Pocket
- Devices converted with UDC3

____

Introduction

This document describes various settings to make IGEL OS more secure. In general the more of these settings you apply the better endpoint 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 more than one thin client, put one or more settings presented here into a Universal Management Suite (UMS) master profile, which you can assign to any number of thin clients, enforcing the security settings as a consequence.

Learn more about using master profiles here.

Setting Passwords

You can restrict access to various system components by setting passwords.

- Setting Local Passwords (see page 497)
- Password-Protecting Sessions and Accessories (see page 498)
- Using Screenlock (see page 499)
- Do Not Save Session Passwords (see page 500)
- Setting a UEFI Password (see page 501)
- Using Two-Factor Authentication (2FA) (see page 502)

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 526).

Find further information on the Passwords page in the IGEL OS manual.

Password-Protecting Sessions and Accessories

Rationale

Sessions can be used to access corporate resources, 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. To enable password protection for a session, follow these instructions:

1. In IGEL Setup go to **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 IGEL Setup go to **User Interface > Screenlock / Screensaver**
2. Do one or both of the following:
    - Activate the **Quickstart 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 > 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. (Default: 5)
4. As a password select **User password** (see Setting Local Passwords (see page 497)) or a separate **Screenlock password** (and set one). (Default: none)
5. Optionally, check **Allow administrator password** to allow the administrator to unlock a user's screen. (Default: enabled)
6. Click **Apply**.

Do Not Save Session Passwords

Rationale

Passwords for sessions should not be saved on the endpoint device.

Instructions

▶ When configuring a session, under **Logon** leave the **Password** field empty. The user will then be prompted interactively for the password.

▶ Wherever possible use Two-Factor Authentication (2FA) (see page 502).

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 UD LX devices

▶ If UEFI is not enabled, see the instructions under UEFI Secure Boot Enabling Guides.

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 UDC3

▶ 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.

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 605)
  - Citrix Legacy ICA Sessions (1)
  - Citrix Legacy ICA Sessions with Local Logon Window (see page 610)
  - Citrix Storefront (see page 611)
  - Citrix Xen Desktop Appliance Mode (see page 616)
  - RDP Sessions (see page 613)
  - Horizon Sessions (see page 614)
  - Web browser (see page 615)
- (Kerberos) Passthrough Authentication (see page 931)

Keeping 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 or the Universal Firmware Update feature of the Universal Management Suite (UMS).

Instructions

▶ To be notified of security-critical IGEL OS updates and to receive the IGEL Technical Newsletter, subscribe to IGEL communications on www.igel.com[30].

ⓘ You can use the Universal Firmware Update feature in UMS to check for updates for your devices managed by UMS.

Test an IGEL OS update on one or more sample devices to see whether all features you require work, before you roll the update out to production.

1. Assign an update to one or more devices:
   - In UMS, drag and drop a Universal Firmware Update onto a device or a directory to assign the update. See also Assigning Thin Client Updates.
     OR
   - In IGEL Setup, go to **System > Update > Firmware Update** and configure an update source. See Firmware Update.
2. Launch the update process:
   - Manually: In UMS, right-click a device or a directory and select **Update & snapshot commands > Update** or **Update on Shutdown** from the context menu.
     OR
   - As a scheduled job in UMS:
   a. Right-click **Jobs** in the structure tree.
   b. Select **New Scheduled Job**.
   c. Enter a **Name**.
   d. Select **Update**, **Update on Boot** or **Update on Shutdown** as the **Command**.
   e. Complete the configuration of the task.
   f. Assign the task to devices or directories.

[30] http://www.igel.com/

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

Rationale

The local terminal accessory allows the user to execute commands or make changes to the system. Leave it disabled.

Instructions

By default, the user does not find a local terminal session in the start menu or on the desktop. To remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session.
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 terminal, see Password-Protecting Sessions and Accessories (see page 498).

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
- Browser
- Citrix Virtual Desktops
- Citrix Self-Service
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- Caradigm
- XDMCP for This Display

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.

> ⓘ You can combine most of the appliance mode sessions with Two-factor Authentication (see page 502) 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 for the Start Menu

By default the user can find a wide selection of accessories under the **System** icon of the start menu.To hide individual accessories in the start menu:

1. Go to **Accessories > [accessory name]** in IGEL Setup.
2. Disable all **Starting Methods for Session**.
3. Click **Apply**.

   Alternatively, you can set a password for the accessories, see Password-Protecting Sessions and Accessories (see page 498).

To hide the complete **System** icon, which contains the accessories:

1. Go to **User Interface > Desktop > Start Menu** in IGEL Setup.
2. Uncheck **System tab**. (Default: enabled)
3. Click **Apply**.

Instructions for the Application Launcher

A wide selection of accessories can also be found under the **System** icon of the Application Launcher. To hide individual accessories in the Application Launcher:

1. Go to **Accessories > [accessory name]** in IGEL Setup.
2. Disable all **Starting Methods for Session**.
3. Click **Apply**.

   Alternatively, you can set a password for the accessories, see Password-Protecting Sessions and Accessories (see page 498).

To hide the complete Application Launcher's **System** icon, which contains the accessories:

1. Go to **Accessories > Application Launcher > Application Launcher Configuration** in IGEL Setup.
2. Activate **Hide system page**. (Default: visible)
3. Click **Apply**.

Minimizing the Attack Surface

Removing unused features and disabling unneeded network services minimizes the parts of the system that can be attacked.

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) installed, even if no web browser session is configured. To remove the browser, follow these instructions:

1. In the IGEL Setup go to **System > Firmware Customization > Features**.
2. Uncheck the **Local Browser (Firefox)** feature.
3. Click **Apply**.
4. Reboot the endpoint 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:

1. In the IGEL Setup go to **Sessions > Browser > Browser Global > Security**
2. Activate **Safe Browsing** (default: deactivated)
3. Activate **Malware Protection** (default: deactivated)
4. Go to **Sessions > Browser > Browser Sessions > [session name] > Settings > Restart**
5. Enable **Autostart** (default: deactivated)
6. Enable **Restart**(default: deactivated)
7. Go to **Sessions > Browser > Browser Sessions > [session name] > Window**
8. Enable **Start in Fullscreen Mode** (default: deactivated)
9. Enable **Hide local filesystem** (default: deactivated)
10. Enable **Hide configuration page of the browser** (default: enabled)
11. Go to **Sessions > Browser > Browser Sessions > [session name] > Settings > Menus & Toolbar**
12. Activate **Hide App Menu/Menu Bar** (default: deactivated)
13. Go to **Sessions > Browser > Browser Sessions > [session name] > Context**
14. Check **Hide the browser's context menu** (default: deactivated)
15. Click **Apply**.
16. Reboot the endpoint 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

By default, the PC/SC daemon is activated. Follow these steps to deactivate it.

1. In the IGEL Setup go to **Security > Smartcard > PC/SC**
2. Uncheck **Activate PC/SC Daemon** (default: Activated).
3. Click **Apply**.

> ❗ Do not disable the PC/SC daemon if you use smartcard readers that rely on it.

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 enabled (default)
3. Make sure that **Disable TCP connections** is checked (default)
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 10 is to remove all unused features.

Instructions

By default IGEL OS comes with a wide variety of features enabled. To disable any of these, do the following:

1. In the IGEL Setup go to **System > Firmware Customization > Features**.
2. Uncheck all the features that you do not intend to use.
   If you do not use local printers on the endpoint device that you want to share with others, uncheck:
   - **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, see the FAQ IGEL Linux Features that Require the Multimedia Codec Pack.
3. Click **Apply**.
4. Reboot the endpoint device.

Disabling Storage Hotplug

Rationale

Removable USB media can be used to steal data or to execute unauthorized software or even malware on the endpoint 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. Uncheck **Enable dynamic client drive mapping** (default: disabled)
3. Set **Number of storage hotplug devices** to `0` (default: 0)
4. Click **Apply**.
   Storage devices are now 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 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 894).
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 UD LX Devices

USB Boot is disabled in the factory settings on IGEL UD LX devices. If you want to disable it at any time in the devices lifetime, 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. Optional: 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?**
8. The device boots.

> Additionally, set a UEFI Password so the boot settings cannot be changed back.

Instructions for 3rd-party devices converted with UDC3

▶ 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

Rationale

Endpoint 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 endpoint devices on your network

Instructions

By default, Remote Management is enabled on IGEL OS endpoints. Use Autoregistration to catch all endpoint devices in your corporate network:

1. Assign the DNS entry `igelrmserver` to the UMS host.
2. In UMS Console go to **UMS Administration > Global Configuration > Thin Client Network Settings.**
3. Activate **Enable automatic registration (without mac address import)**
   Now all new IGEL thin clients and devices converted with UDC3 booting up in the network will automatically register with your UMS instance.
4. Optionally, put newly registered endpoint devices into a quarantine directory automatically with UMS Default Directory Rules[31].
5. Optionally, assign a Master Profile[32] 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 endpoints.

[31] http://edocs.igel.com/index.htm#9531.htm
[32] http://edocs.igel.com/manuals/en/en_prof/index.htm

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**)
   - 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 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. Uncheck **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

1. In IGEL Setup go to **System > Remote Access > SSH**.
2. Make as many of the following settings as possible for your use case. Each one improves security:
   - Uncheck **Permit empty passwords**. (Default: deactivated)
   - Uncheck **Permit administrator login**. (Default: deactivated)
   - Deny **User access** for `user`, who can execute any command with regular user privileges. (Default: denied)
   - Instead, allow **User access** for `ruser`, whose access is restricted by the list **Applications access for remote user 'ruser'**. (Default: allowed)
   - Optional: Edit the list **Applications access for remote user 'ruser'**. It defines the commands that `ruser` can run from remote. (Default: a local shell and IGEL Setup).
   - Click **Apply**.
   - Go to **Security > Password**, under **User Account for Remote Access** activate **Use Password** and set a password
   - 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 Secure Terminal by design enables a remote user to execute commands on the system.

Instructions

By default, 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. Uncheck **Secure Terminal**.
3. Click **Apply**.

> ⓘ Secure Terminal can be enabled globally in **UMS under UMS Administration > Global Configuration > Remote Access**. There you can also enable logging of users of 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 529)
- Disabling Bluetooth (see page 530)

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. Check **Activate Wireless Interface**.
3. Do not check **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 the IGEL OS Manual.
9. Click **Apply**.
10. Optional: Configure **Additional Wi-Fi networks**.

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. Disable **Activate Bluetooth**. (Default: disabled)
3. Click **Apply**.

Using UD Pocket for BYOD Devices

Rationale

Letting users access company resources with their own devices (BYOD) 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, see UD Pocket (UDP) Reference Manual.

For how to select the UD Pocket during the boot procedure, see Boot Settings and Starting Your UD Pocket.

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

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[33].

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.

[33] 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):

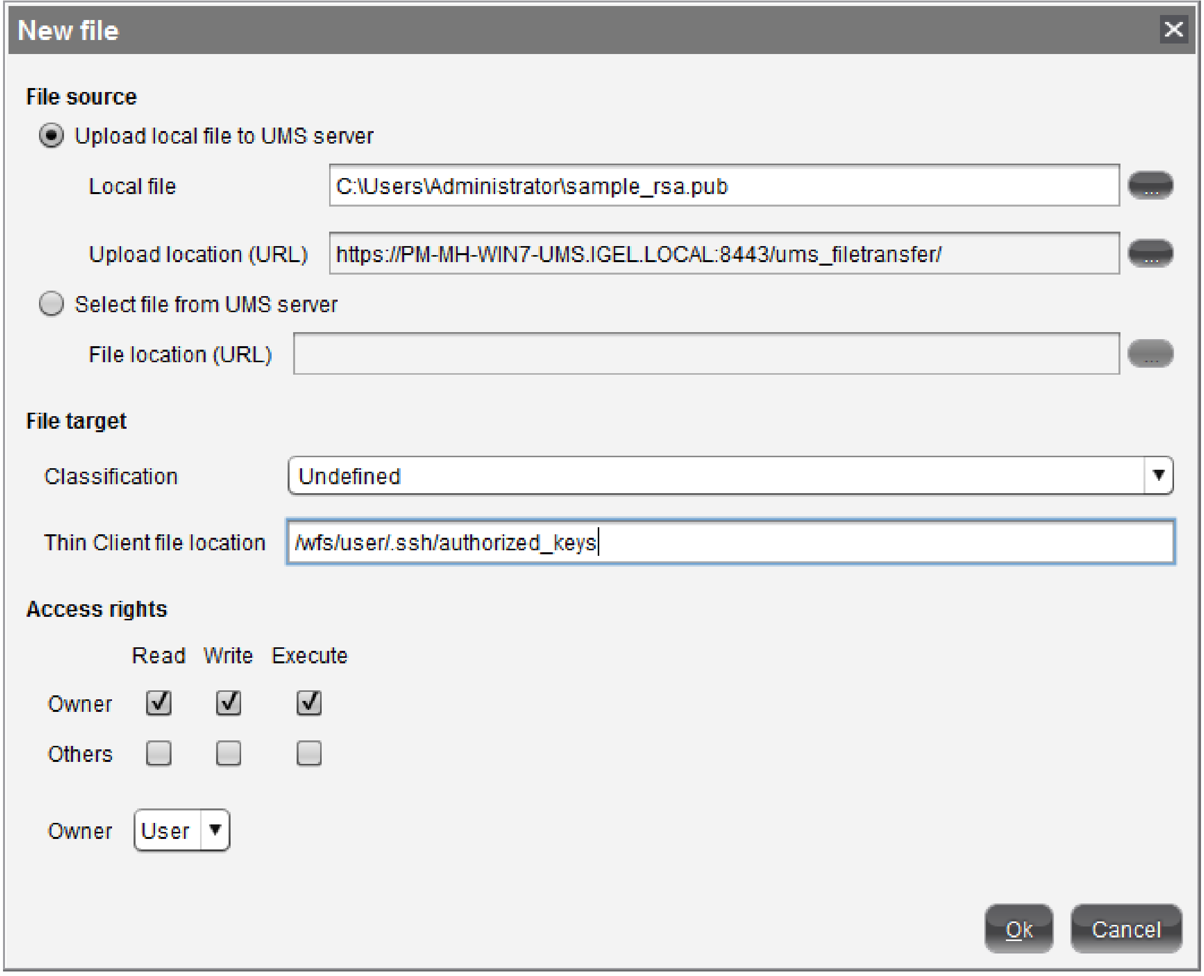
- `id_rsa` - the private key file
- `id_rsa.pub` - the public key file

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.



New file

File source

● Upload local file to UMS server

Local file: C:\Users\Administrator\sample_rsa.pub

Upload location (URL): https://PM-MH-WIN7-UMS.IGEL.LOCAL:8443/ums_filetransfer/

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Thin Client file location: /wfs/user/.ssh/authorized_keys

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

ⓘ 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 539), 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 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) 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**.

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.

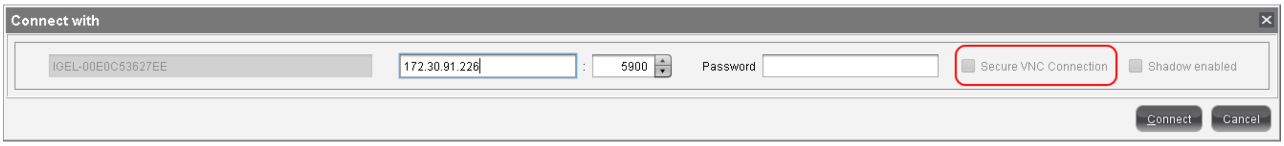
Only when these connections have been established, the console calls up the VNC viewer which then connects to the console proxy. The VNC client and VNC server are now connected via the two proxies which transfer data with TLS/SSL encryption.

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.

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.



Connect with

IGEL-00E0C53627EE

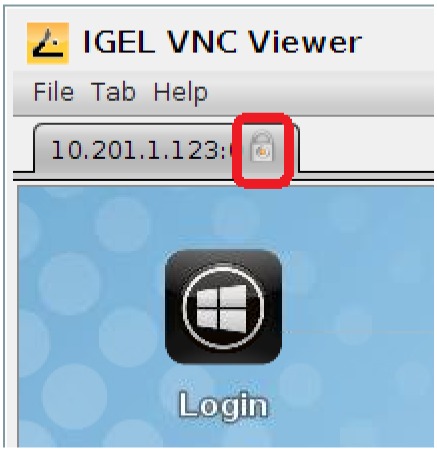
172.30.91.226 : 5900

Password

□ Secure VNC Connection

□ Shadow enabled

When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:

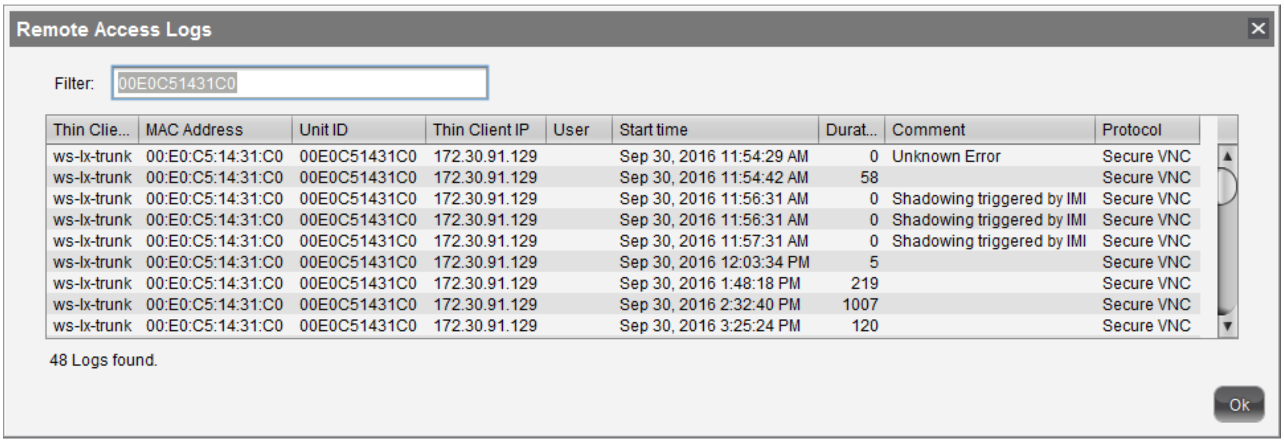


VNC Logging

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.



Remote Access Logs

Filter: 00E0C51431C0

Thin Clie...	MAC Address	Unit ID	Thin Client IP	User	Start time	Durat...	Comment	Protocol
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:29 AM	0	Unknown Error	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:42 AM	58		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:57:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 12:03:34 PM	5		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 1:48:18 PM	219		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 2:32:40 PM	1007		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 3:25:24 PM	120		Secure VNC

48 Logs found.

▶ 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.

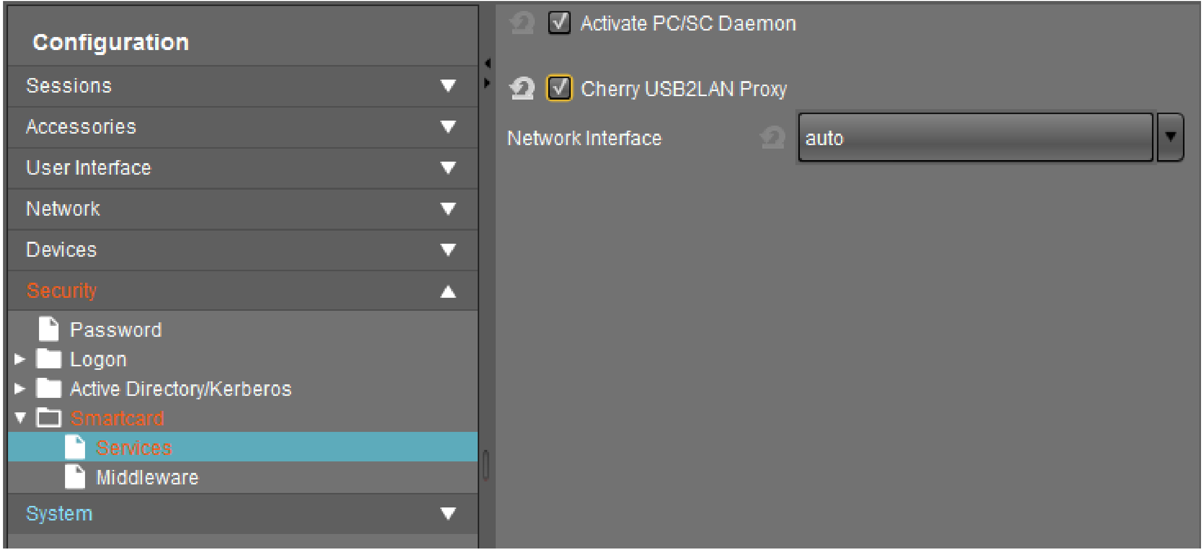
Using the G87-1504/ST-1503 with firmware version 10.05.100 and higher:

- 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**.


☑ Activate PC/SC Daemon

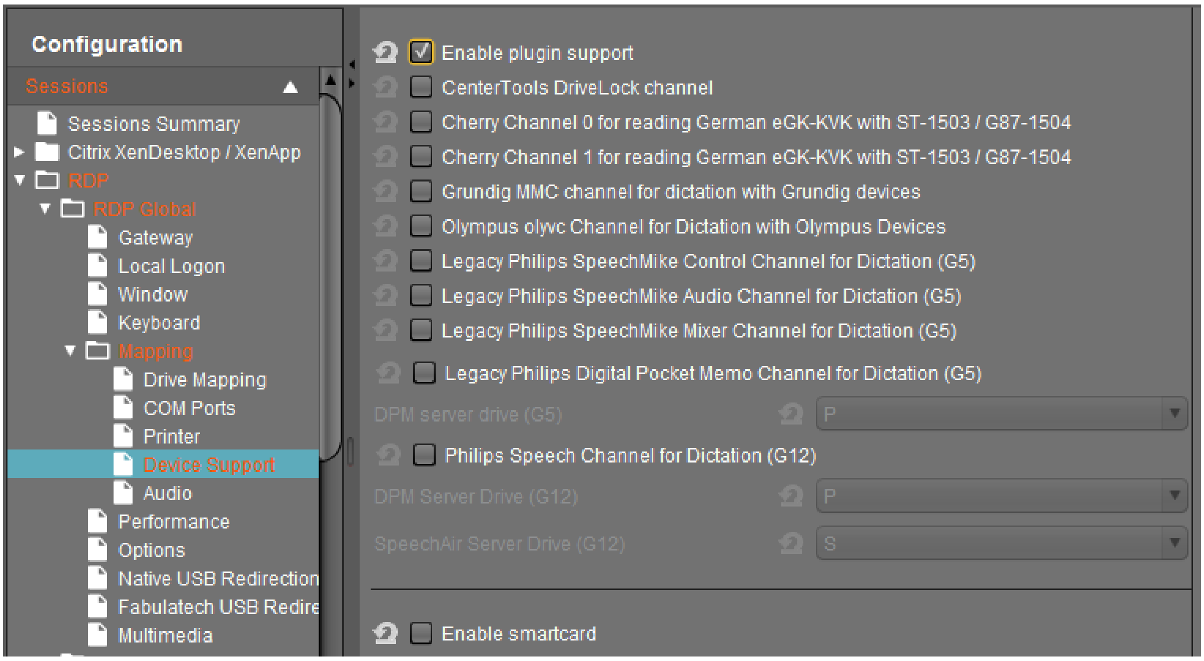
☑ Cherry USB2LAN Proxy

Network Interface: auto

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.



☑ Enable plugin support

□ CenterTools DriveLock channel

□ Cherry Channel 0 for reading German eGK-KVK with ST-1503 / G87-1504

□ Cherry Channel 1 for reading German eGK-KVK with ST-1503 / G87-1504

□ Grundig MMC channel for dictation with Grundig devices

□ Olympus olyvc Channel for Dictation with Olympus Devices

□ Legacy Philips SpeechMike Control Channel for Dictation (G5)

□ Legacy Philips SpeechMike Audio Channel for Dictation (G5)

□ Legacy Philips SpeechMike Mixer Channel for Dictation (G5)

□ Legacy Philips Digital Pocket Memo Channel for Dictation (G5)

DPM server drive (G5): P

□ Philips Speech Channel for Dictation (G12)

DPM Server Drive (G12): P

SpeechAir Server Drive (G12): S

□ Enable 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

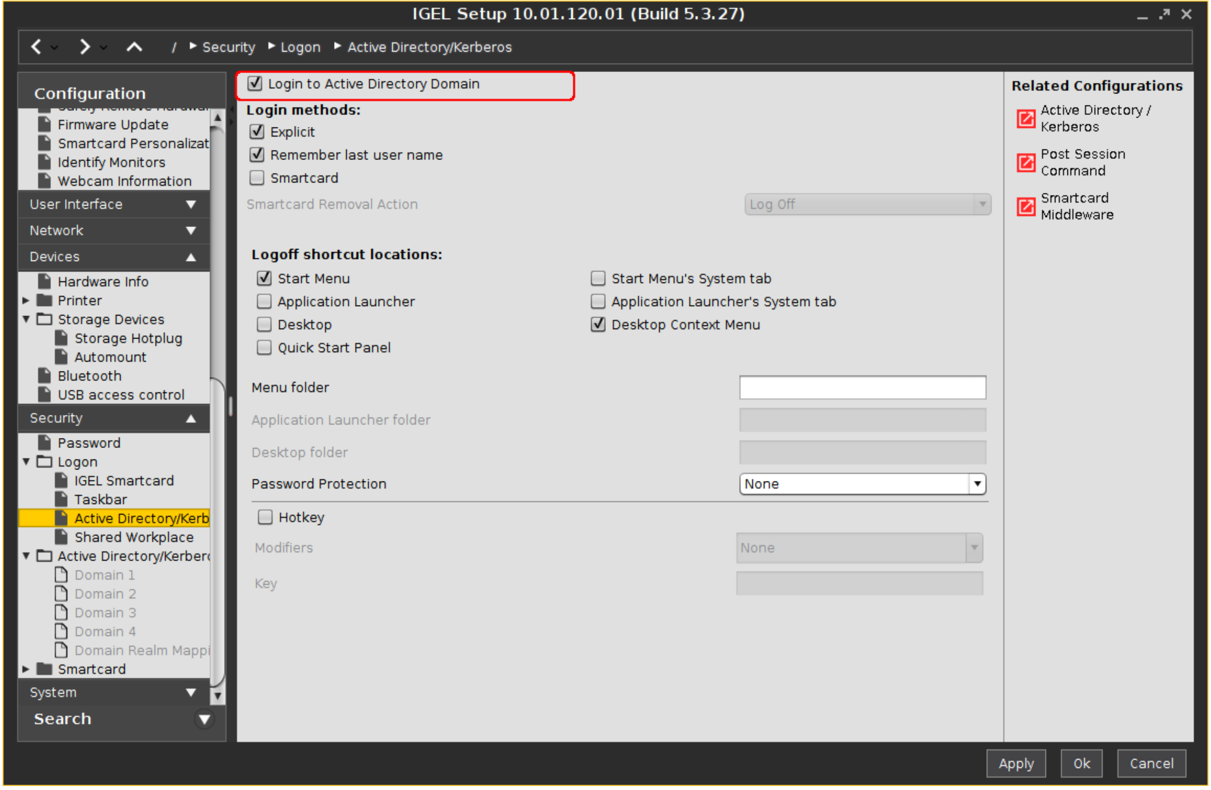
Single Sign-on for the Browser Proxy

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**.



☑ Login to Active Directory Domain

Login methods:

☑ Explicit

☑ Remember last user name

□ Smartcard

Smartcard Removal Action: Log Off

Logoff shortcut locations:

☑ Start Menu

□ Application Launcher

□ Desktop

□ Quick Start Panel

□ Start Menu's System tab

□ Application Launcher's System tab

☑ Desktop Context Menu

Menu folder

Application Launcher folder

Desktop folder

Password Protection: None

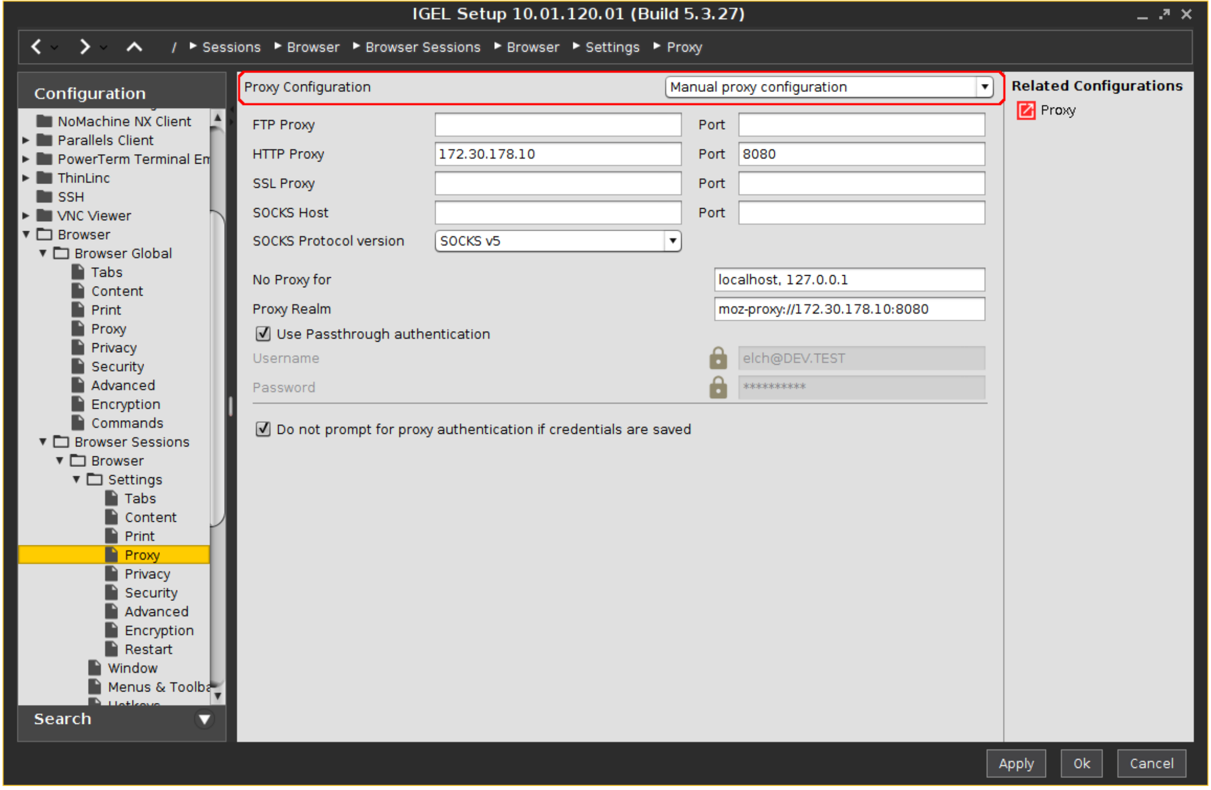
□ Hotkey

Modifiers: None

Key

3. Go to **Sessions > Browser > Browser Sessions >** [name of the browser session] **> Settings > Proxy**.

4. In the **Proxy Configuration** choice, select **Manual proxy configuration**.



Proxy Configuration: Manual proxy configuration

FTP Proxy: Port:

HTTP Proxy: 172.30.178.10 Port: 8080

SSL Proxy: Port:

SOCKS Host: Port:

SOCKS Protocol version: SOCKS v5

No Proxy for: localhost, 127.0.0.1

Proxy Realm: moz-proxy://172.30.178.10:8080

☑ Use Passthrough authentication

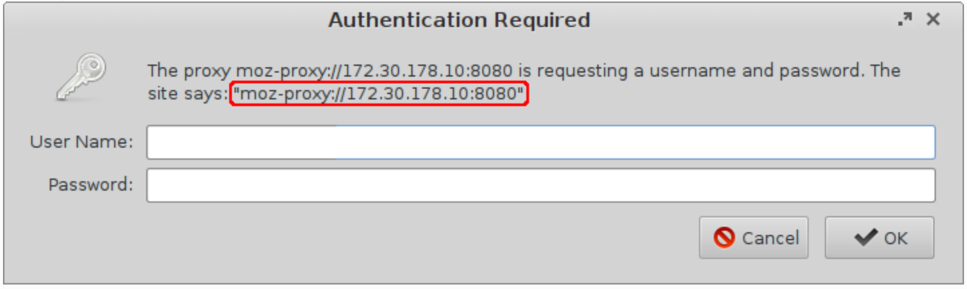
Username: elch@DEV.TEST

Password: **********

☑ Do not prompt for proxy authentication if credentials are saved

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:



The proxy moz-proxy://172.30.178.10:8080 is requesting a username and password. The site says: "moz-proxy://172.30.178.10:8080"

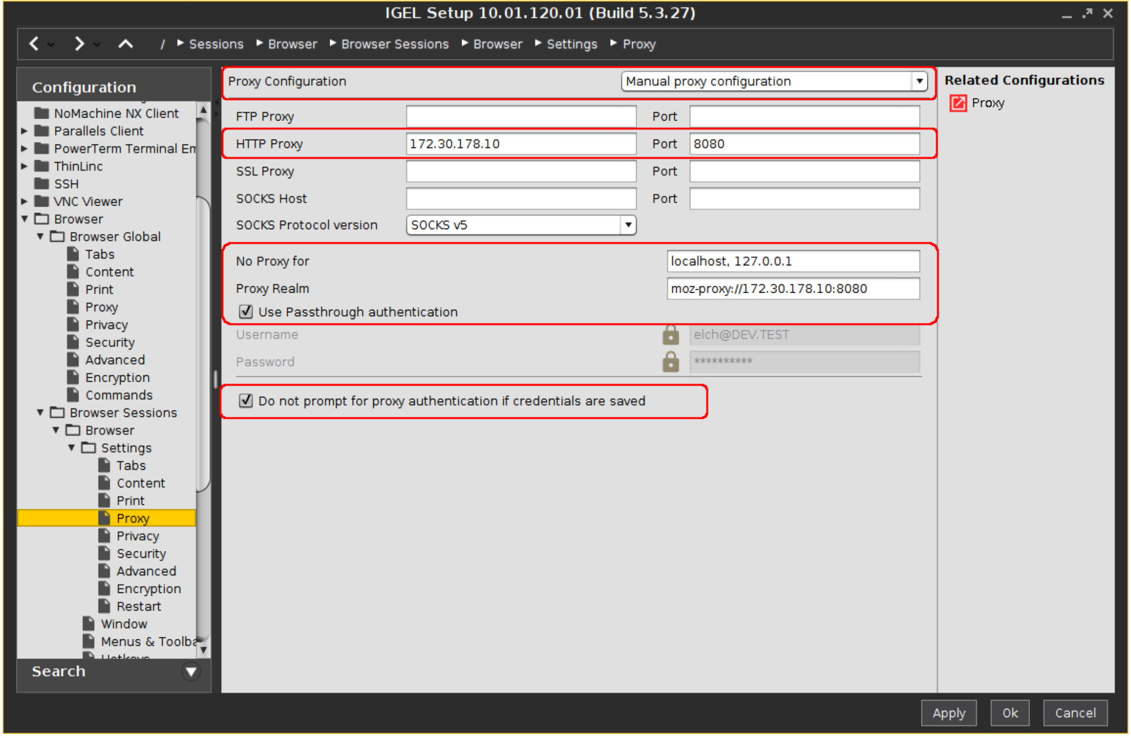
User Name:

Password:

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.



IGEL Setup 10.01.120.01 (Build 5.3.27)

/ ▸ Sessions ▸ Browser ▸ Browser Sessions ▸ Browser ▸ Settings ▸ Proxy

Proxy Configuration: Manual proxy configuration

FTP Proxy		Port	
HTTP Proxy	172.30.178.10	Port	8080
SSL Proxy		Port	
SOCKS Host		Port	
SOCKS Protocol version	SOCKS v5		

No Proxy for: localhost, 127.0.0.1

Proxy Realm: moz-proxy://172.30.178.10:8080

☑ Use Passthrough authentication

Username: elch@DEV.TEST

Password: **********

☑ Do not prompt for proxy authentication if credentials are saved

The next time the user logs in to the device, the browser proxy is ready to use.

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

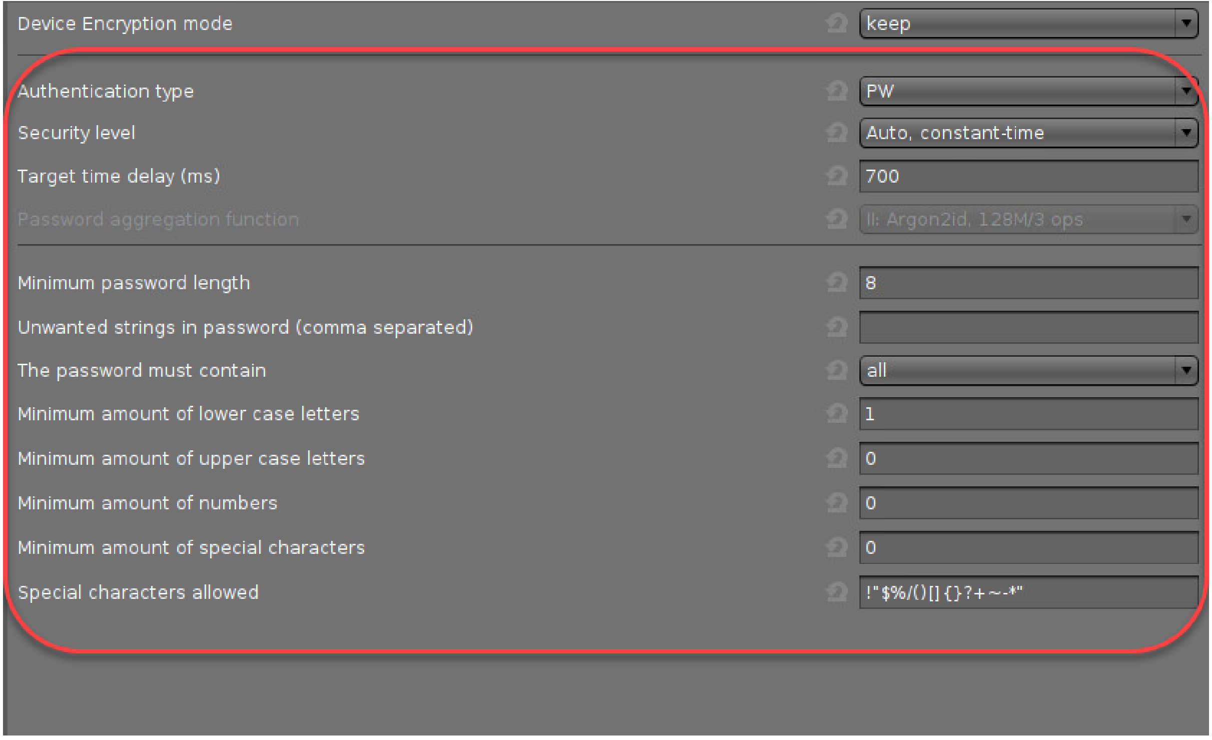
IGEL OS 11.06 or higher offers strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

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.

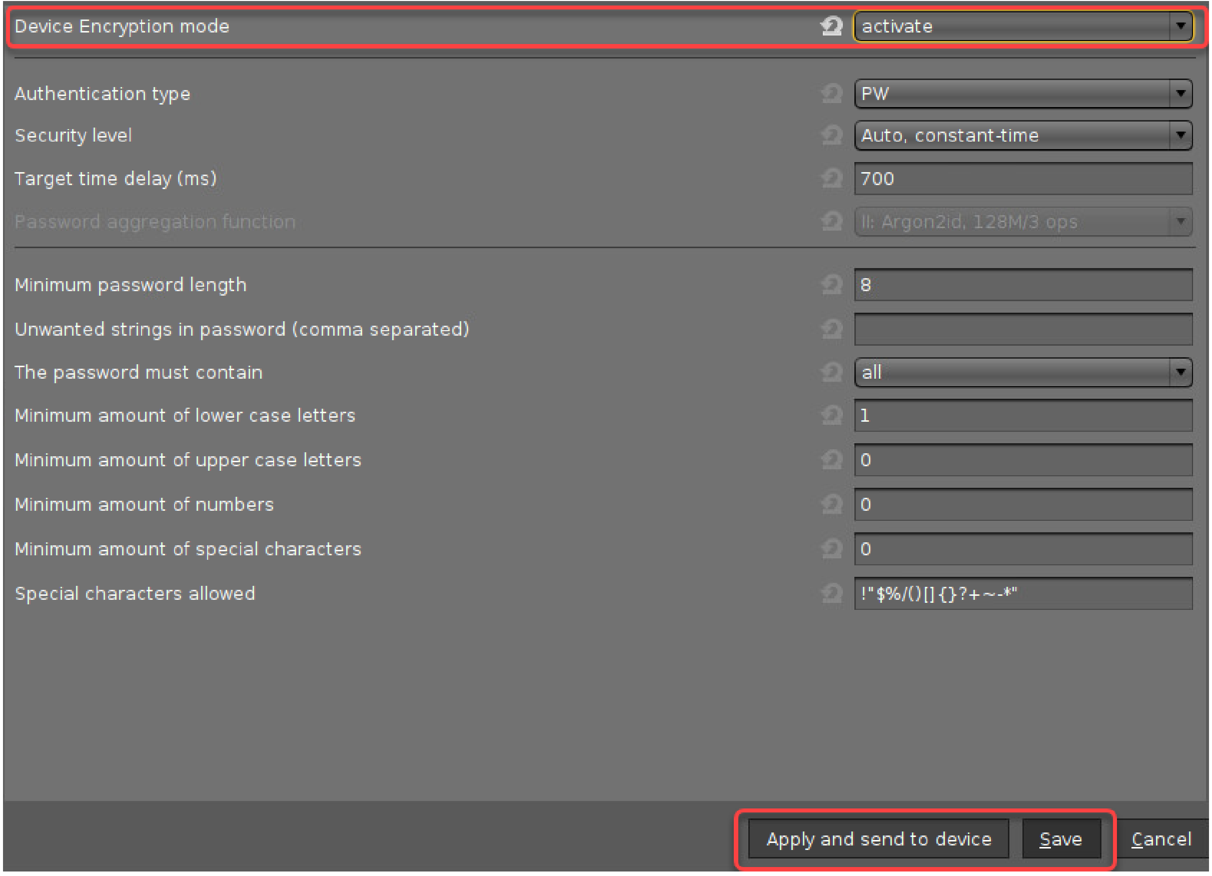
Instructions

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.



Device Encryption mode	keep
Authentication type	PW
Security level	Auto, constant-time
Target time delay (ms)	700
Password aggregation function	II: Argon2id, 128M/3 ops
Minimum password length	8
Unwanted strings in password (comma separated)	
The password must contain	all
Minimum amount of lower case letters	1
Minimum amount of upper case letters	0
Minimum amount of numbers	0
Minimum amount of special characters	0
Special characters allowed	!"$%/()[]{}?+~-*"

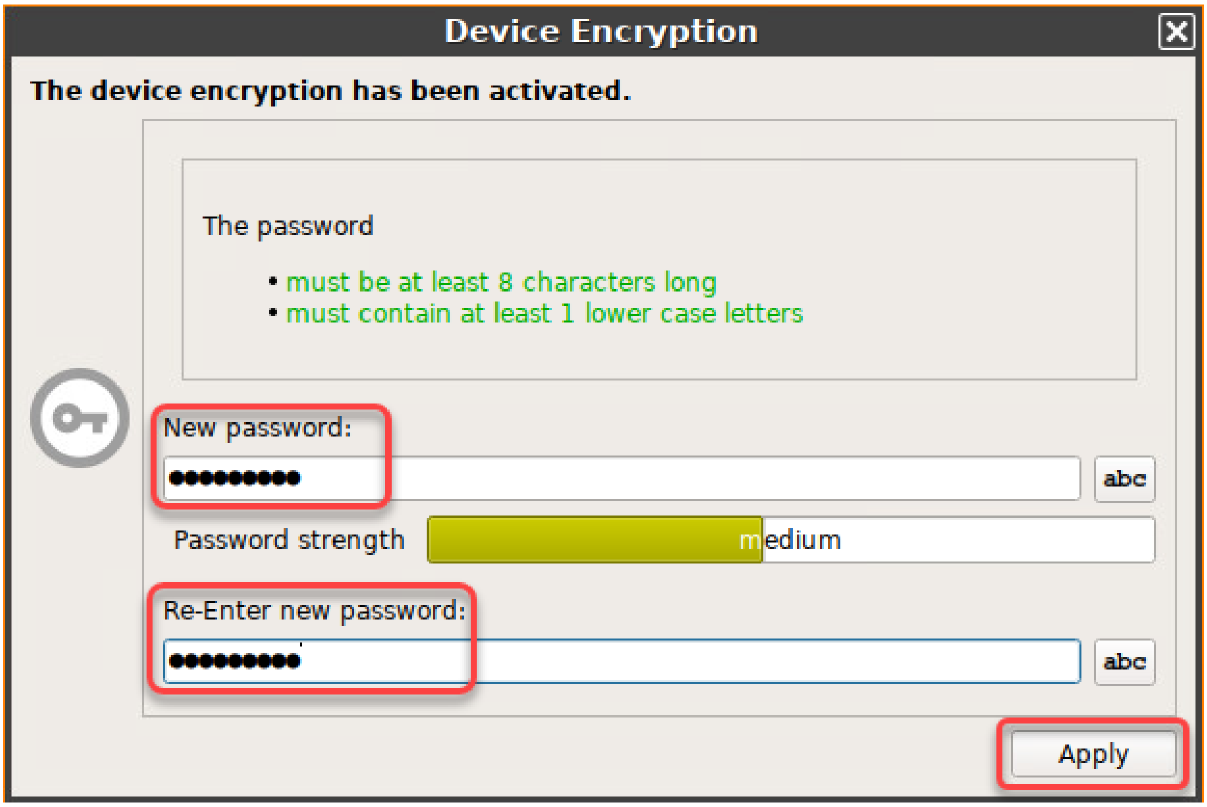
3. Set **Device encryption mode** to "activate" and click **Apply and send to device** or **Save**.



Device Encryption mode	activate
Authentication type	PW
Security level	Auto, constant-time
Target time delay (ms)	700
Password aggregation function	II: Argon2id, 128M/3 ops
Minimum password length	8
Unwanted strings in password (comma separated)	
The password must contain	all
Minimum amount of lower case letters	1
Minimum amount of upper case letters	0
Minimum amount of numbers	0
Minimum amount of special characters	0
Special characters allowed	!"$%/()[]{}?+~-*"

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**.



Device Encryption

The device encryption has been activated.

The password

- must be at least 8 characters long
- must contain at least 1 lower case letters

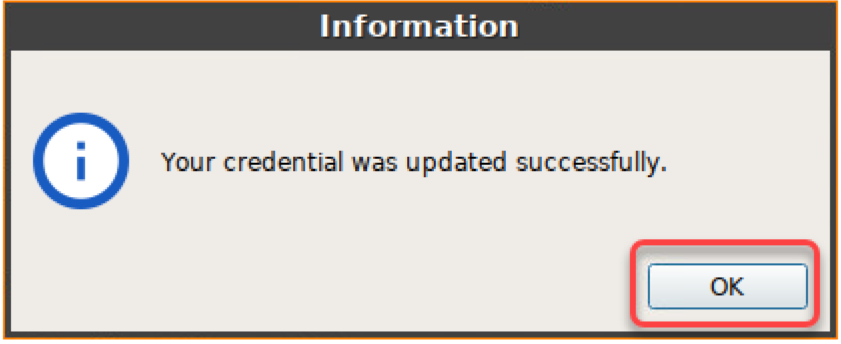
New password: ●●●●●●●●●

Password strength: medium

Re-Enter new password: ●●●●●●●●●

Several partitions are re-encrypted. This might take up to 60 seconds, depending on your hardware capabilities and the size of your Custom Partition.

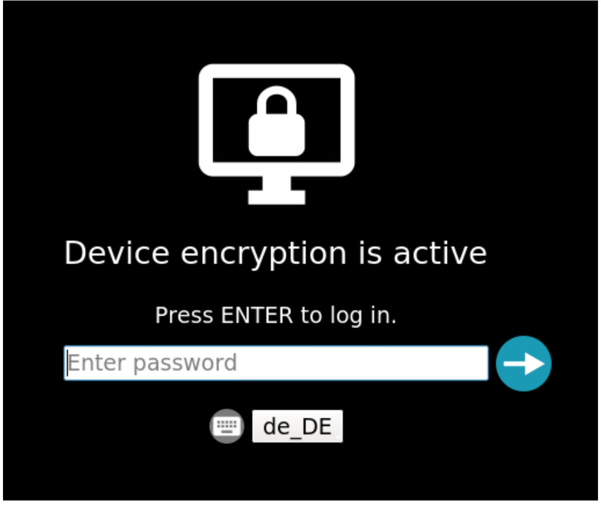
5. The user confirms the success message.



Information

Your credential was updated successfully.

6. On system start, the user must enter the device encryption password.



Device encryption is active

Press ENTER to log in.

Certificates

Certificate Enrollment and Renewal with SCEP (NDES)

SCEP is a protocol for certificate management which supports the secure issuance of certificates to network devices.

Requirements

- SCEP server
  The following SCEP server implementations can be used with IGEL Linux v5 or IGEL Linux 10:
  - 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 http://aka.ms/ndes.
- Connection between the SCEP server and the certification authority (CA).

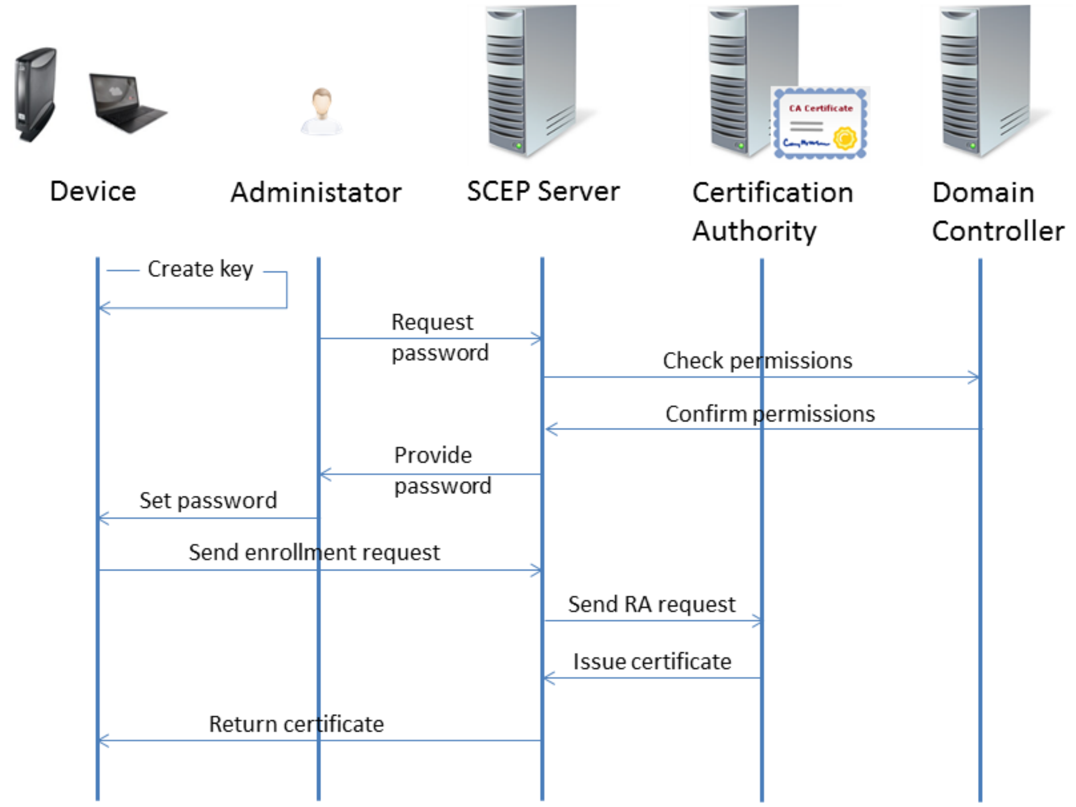
This document explains the enrollment of certificates with SCEP.

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-deep description, see the Microsoft technet article "Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)" under http://aka.ms/ndes.

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.

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.

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 555).

> ⓘ 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 564).
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		

Configuration of the SCEP Client

The configuration of the SCEP client on the IGEL OS device is carried out as follows:

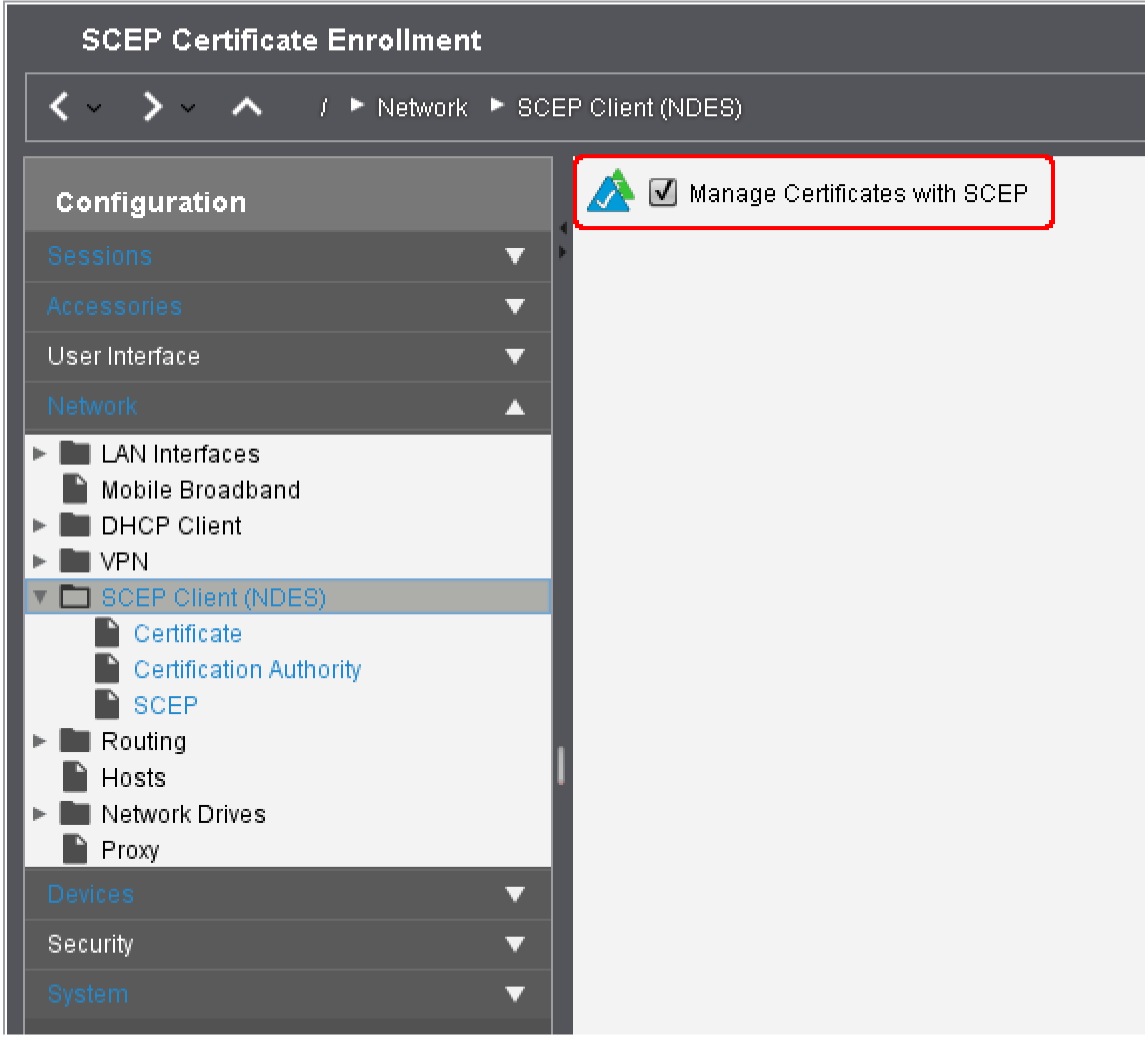
- Creating a Profile in the UMS (see page 560)
- Activating the SCEP Client (see page 561)
- Entering the Data for the Certificate Signing Request (CSR) (see page 562)
- Defining the Certification Authority (CA) (see page 564)
- Providing the SCEP Server Data (see page 565)
- Applying the Profile to the Devices (see page 566)

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**.



SCEP Certificate Enrollment

/ ▸ Network ▸ SCEP Client (NDES)

☑ 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.

CommonName/SubjectAltName: Give a designation which matches the **Type of CommonName/SubjectAltName**. For certain types, this occurs automatically. No entry is then required.

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".

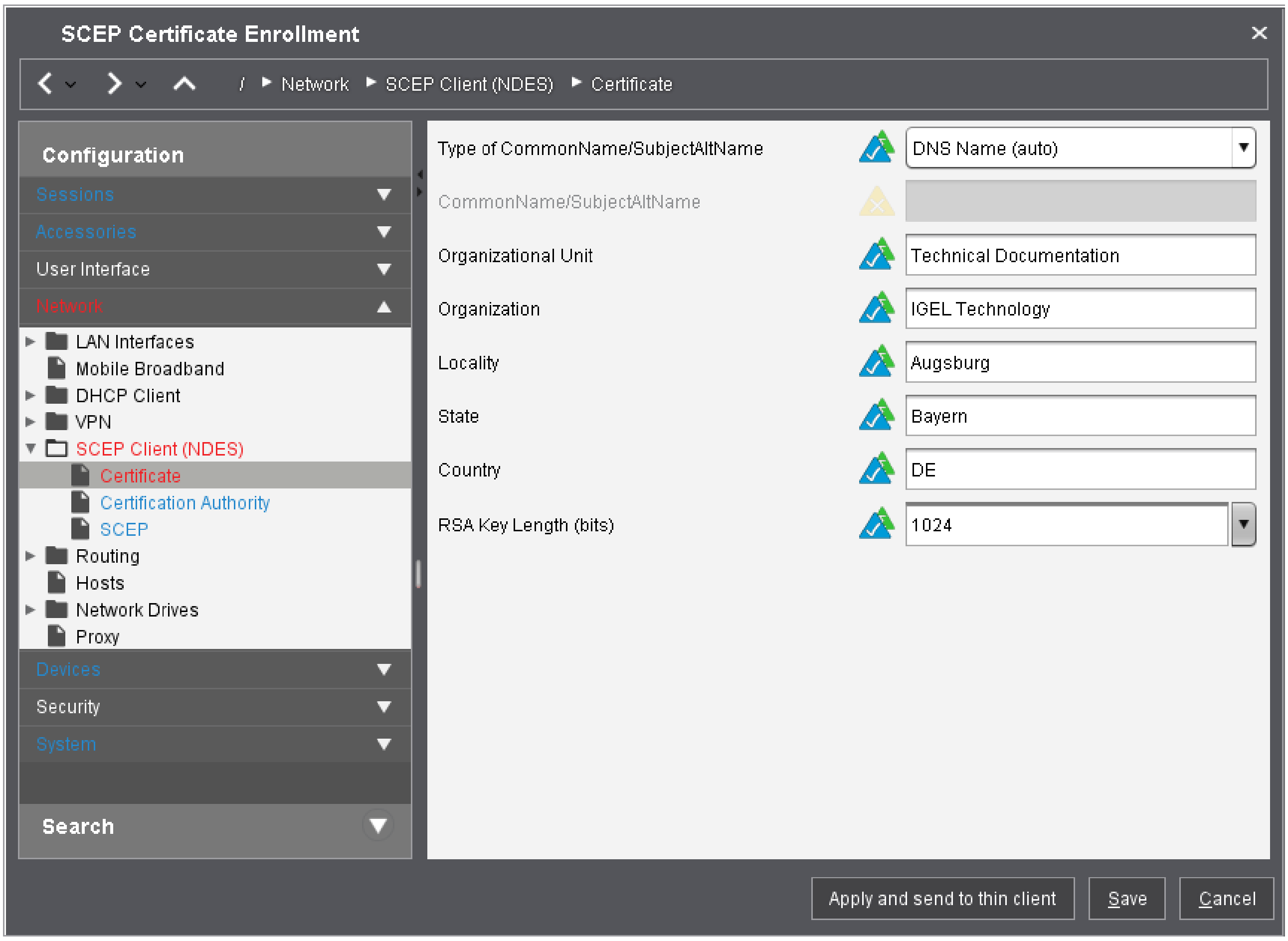
State: Details regarding the device’s locality. Example: "Bayern".

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.



Type of CommonName/SubjectAltName: DNS Name (auto)

CommonName/SubjectAltName:

Organizational Unit: Technical Documentation

Organization: IGEL Technology

Locality: Augsburg

State: Bayern

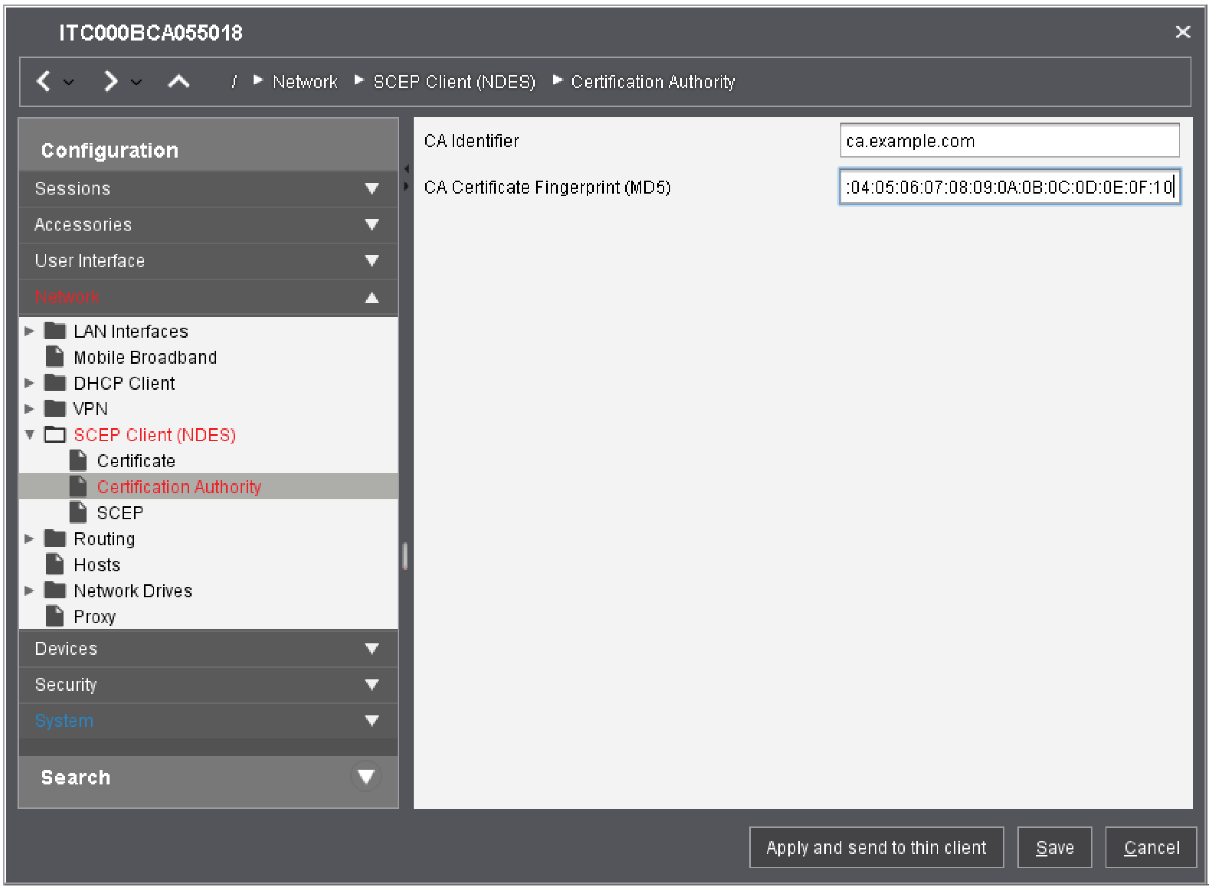
Country: DE

RSA Key Length (bits): 1024

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`



CA Identifier: ca.example.com

CA Certificate Fingerprint (MD5): :04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10

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[34].

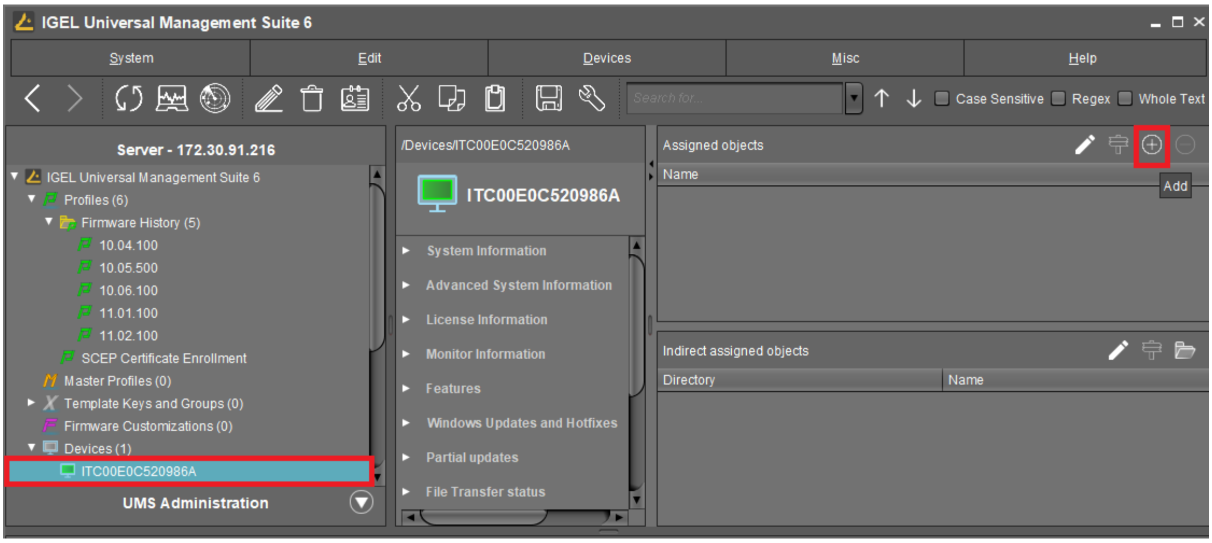
   - **Certificate renewal period (days)**: Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)
   - **Certificate expiry check interval (days)**: Specifies how often the certificate is checked against its expiry date. (Default: 1)

3. Save the settings.

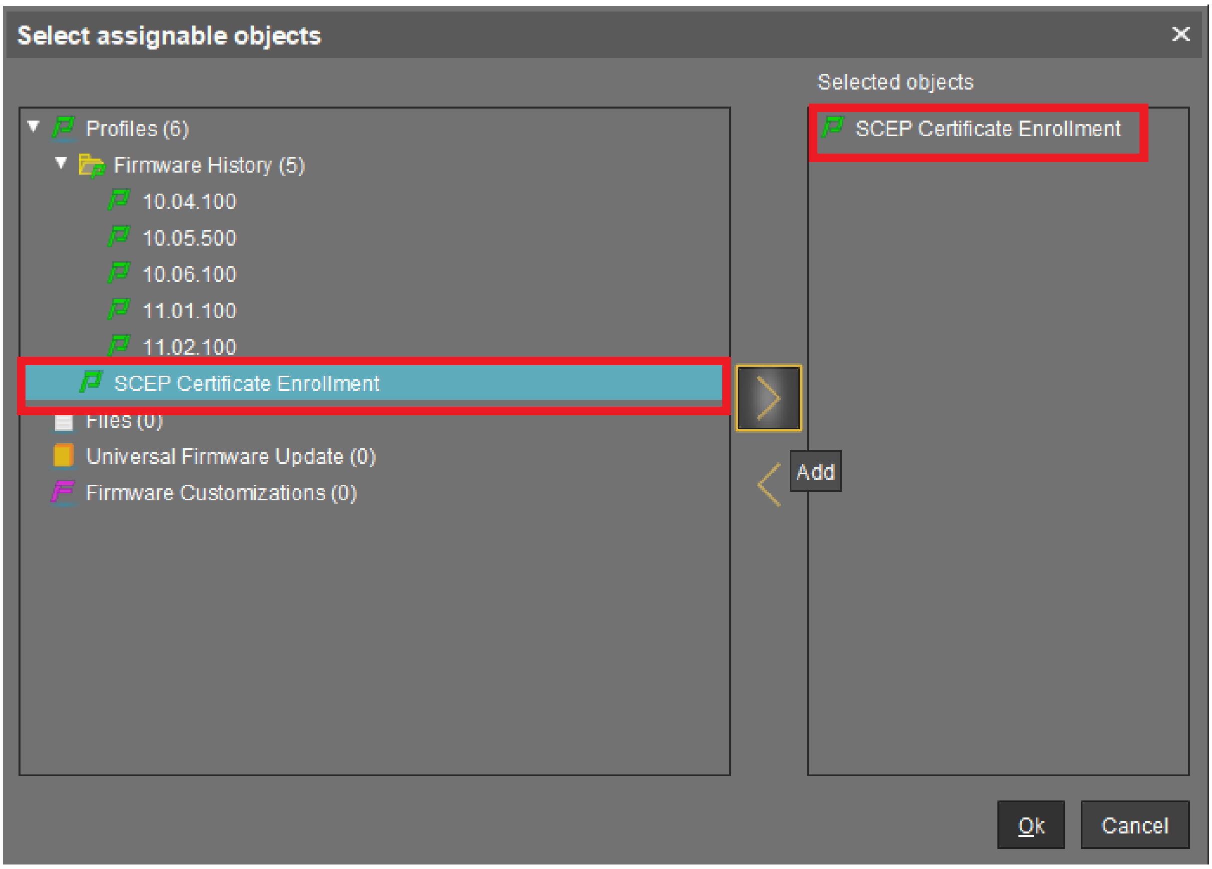
[34] https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx

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.


Select assignable objects
Profiles (6)
Firmware History (5)
10.04.100
10.05.500
10.06.100
11.01.100
11.02.100
SCEP Certificate Enrollment
Files (0)
Universal Firmware Update (0)
Firmware Customizations (0)
Add
Selected objects
SCEP Certificate Enrollment
Ok
Cancel

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 557).

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

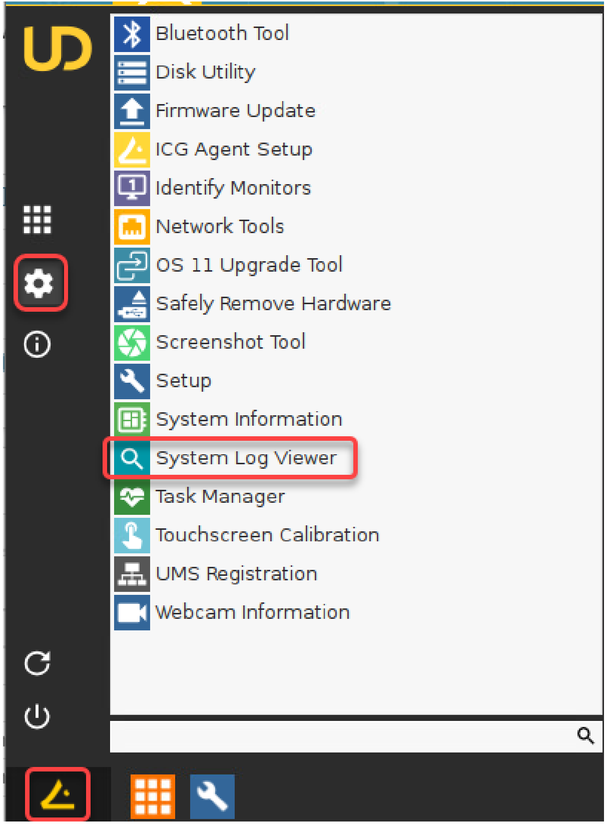
- Diagnostics (see page 570)

Diagnostics

Preliminary: Tools

System Log Viewer

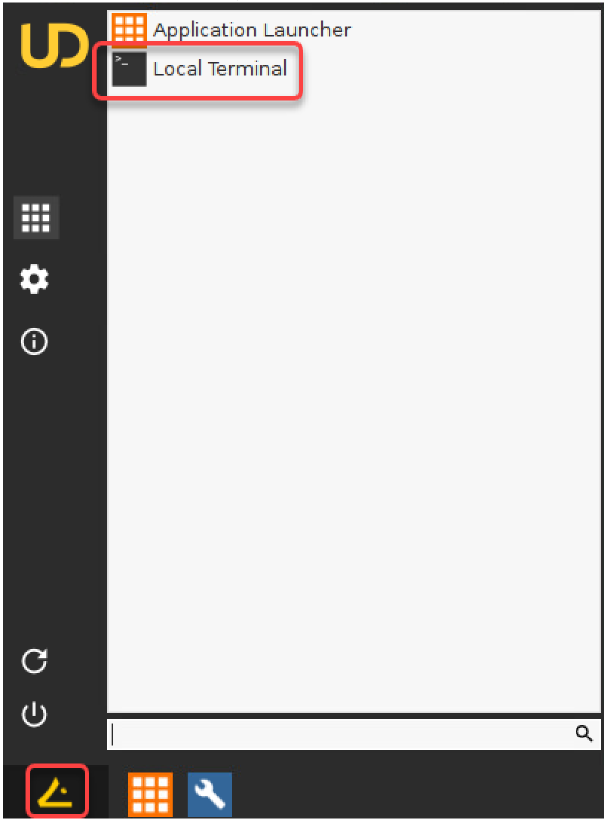
- In the start menu, select the system icon and then **System Log Viewer** to open the system log viewer.



For more information on starting, using, and configuring the system log viewer, see the System Log Viewer chapter of the IGEL OS Manual.

Local Terminal

▶ In the start menu, select the **Local Terminal**.



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 chapter of the IGEL OS Manual.

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

Purpose

IGEL OS firmware comes with a number of trusted root certificates from certain Certificate Authorities (CA) pre-installed. Lists of these root certificates can be found on the download server, in the `IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX/` directory[35]. They are named `[version]_CA-certificates.txt` - for example, the list for IGEL OS version 10.03.100[36].

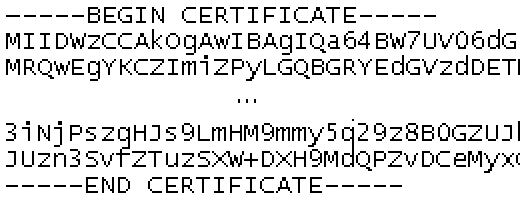
Certificates signed with these root certificates can be used for server authentication and encryption in ICA, RDP, Horizon and browser sessions. You can also verify the origin of Java applications.

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:



```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIQa64Bw7UV06dG
MRQwEgYKCZImiZPyLGQBGRYEdGVzdDET
                ...
3iNjPszgHJs9LmHM9mmy5q29z8B0GZUJ
JUzn3SvfZTuzSXW+DXH9MdQPZvDCeMyx
-----END CERTIFICATE-----
```

Solution

We advise you to use the following file transfer types for distributing the certificates via the UMS; see also Registering a File on the UMS Server:

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

[35] http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX/V10/
[36] http://myigel.biz/public/IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX/V10/lx_10.03.100_CA-certificates.txt?forcedownload

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.

- Deploying Certificates via UMS (see page 576)
- Installing Certificates Manually (see page 579)

Deploying Certificates via UMS

We advise you to use the Universal Management Suite for deploying certificates when you have a certain number of clients to be addressed.

Certificates can be deployed via the UMS in two steps:

- Loading Certificates in the UMS (see page 577)
- Assigning Certificates to IGEL Thin Clients (see page 578)

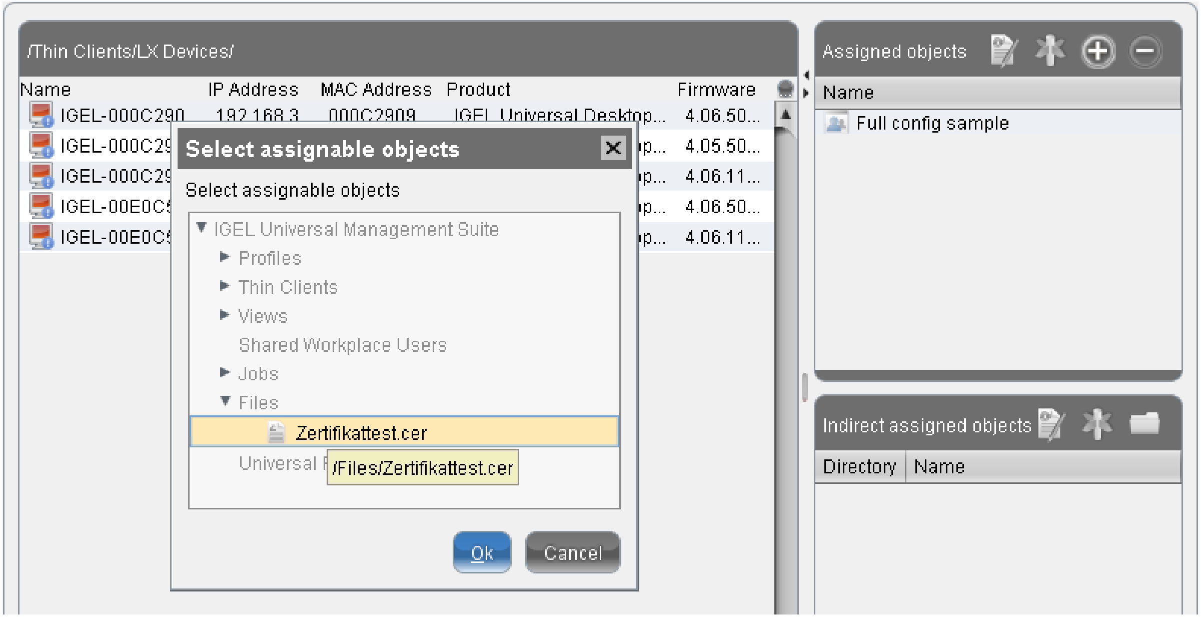
Loading Certificates in the UMS

1. Open the **UMS console**.
2. Right-click **Files**.
3. Choose **New file** to open the **New file** mask.
4. Activate **Upload local file to UMS server**.
5. Browse your new certificate file under **Local file**.
6. Select the suitable **Classification** of the certificate under **File target**.
7. Confirm with **OK**.
   Your certificate is now listed in the **Files** window.

Assigning Certificates to IGEL Thin Clients

After integrating the new certificates, you distribute them to the thin clients:

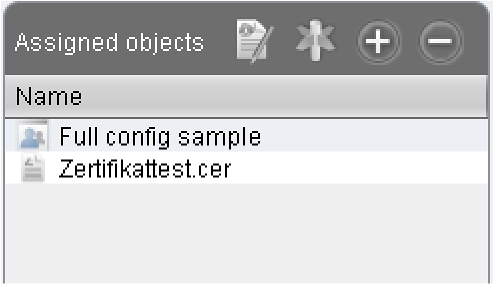
1. Choose one thin client or a group of thin clients in the UMS tree.
2. Click **Add** under **Assigned objects**.
   The **Select assignable object** window opens.


/Thin Clients/LX Devices/
Assigned objects
Select assignable objects
Select assignable objects
IGEL Universal Management Suite
Profiles
Thin Clients
Views
Shared Workplace Users
Jobs
Files
Zertifikattest.cer
Universal F
/Files/Zertifikattest.cer
Ok
Cancel
Indirect assigned objects
Directory
Name

Name	IP Address	MAC Address	Product	Firmware
IGEL-000C290	192.168.3	000C2909	IGEL Universal Desktop...	4.06.50...
IGEL-000C29			...p...	4.05.50...
IGEL-000C29			...p...	4.06.11...
IGEL-00E0C5			...p...	4.06.50...
IGEL-00E0C5			...p...	4.06.11...

Name
Full config sample

3. Select the new certificate and confirm by clicking on **OK**.
4. Select the **Update time** and confirm by clicking on **OK**.
   The new certificate is now assigned to every thin client of the group and is listed under **Assigned objects**.



Name
Full config sample
Zertifikattest.cer

Installing Certificates Manually

Use the **Firefox Certificate Manager** in order to install web browser certificates; see Installing Web Browser Certificates (see page 581).

Also a USB flash drive can be used for the manual import.

Importing SSL Certificates (ICA, RDP, Horizon)

If a CA certificate is missing for *RDP*, *ICA* or *Horizon*, you can copy it from a USB storage device to the thin client:

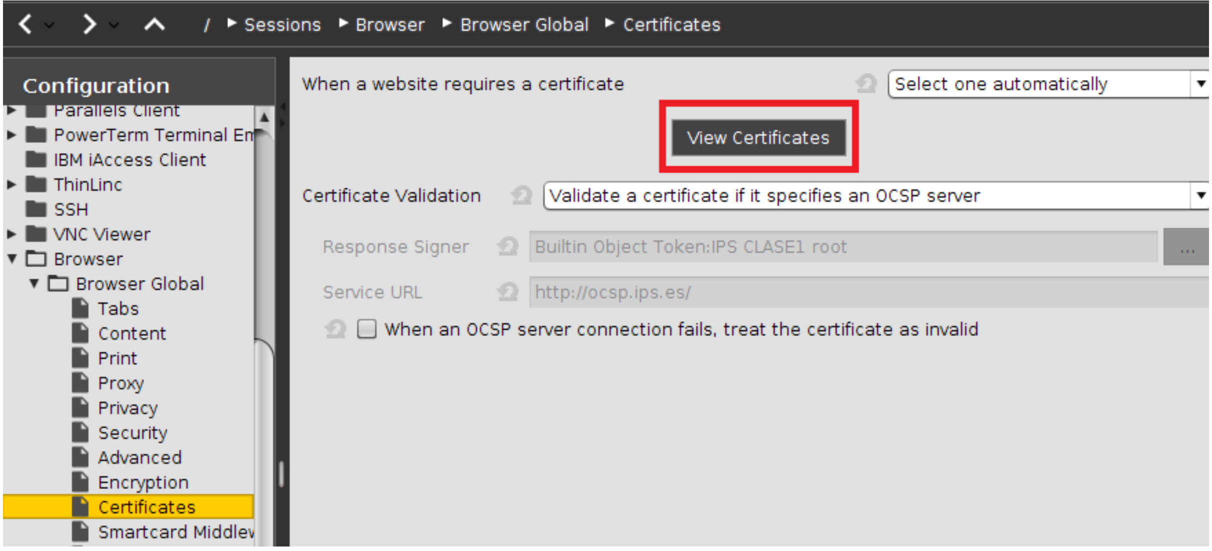
1. Connect your USB storage device to the thin client.
2. Launch a **Terminal** session or press [CTRL]+[ALT]+[F11] to log in as **ROOT** on the Linux console of the thin client.
3. Create a directory for certificates:
   ```
   mkdir /wfs/ca-certs
   ```
4. Change to the directory:
   ```
   cd /wfs/ca-certs
   ```
5. Get the name of your USB storage device:
   ```
   ls /userhome/media
   ```
6. Copy the certificate to the client:
   ```
   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 thin client next time.

Installing Web Browser Certificates

Installing web browser certificates manually:

1. Open the IGEL Setup.
2. Click **Sessions > Browser > Browser Global > Certificates > View Certificates** to open the **Firefox Certificate Manager**.



When a website requires a certificate: Select one automatically

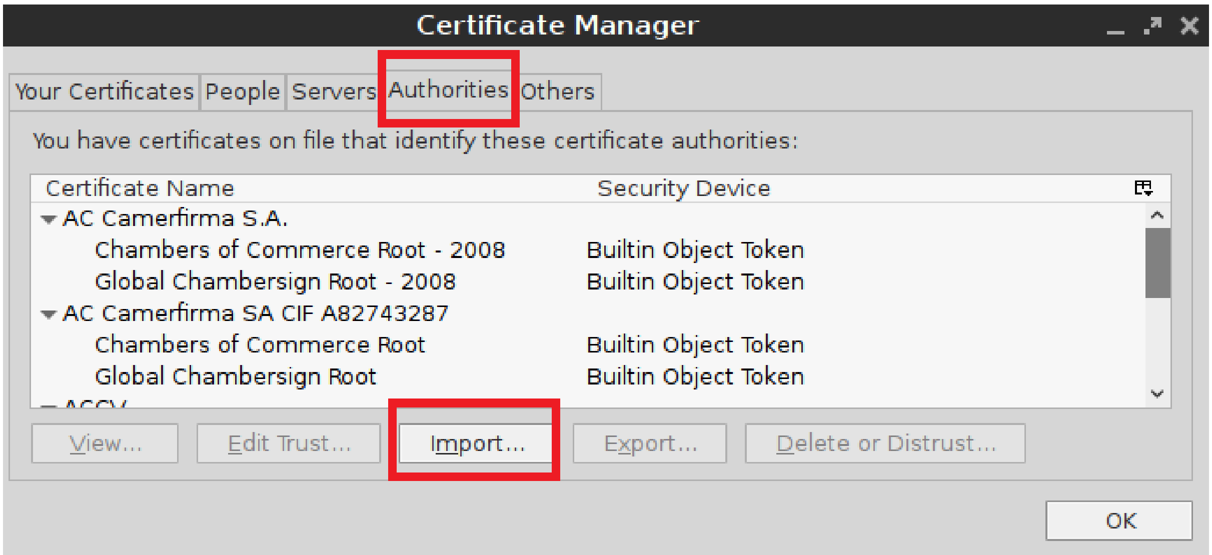
Certificate Validation: Validate a certificate if it specifies an OCSP server

Response Signer: Builtin Object Token:IPS CLASE1 root

Service URL: http://ocsp.ips.es/

□ When an OCSP server connection fails, treat the certificate as invalid

3. Click **Import...** in the **Authorities** tab to import a new certificate from a directory or a USB flash drive.



You have certificates on file that identify these certificate authorities:

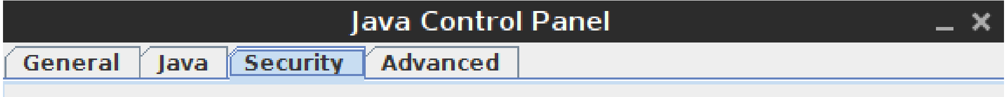
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token

ⓘ Manually installed certificates will be saved permanently without any further configuration.

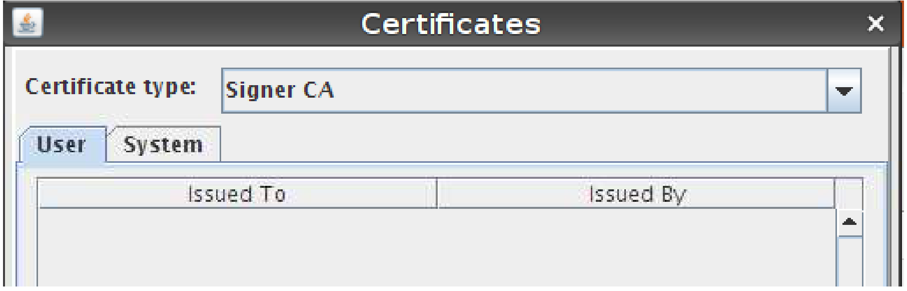
Installing JRE Certificates

Installing Java Runtime Environment (JRE) certificates manually:

1. Activate the registry key `java.deployment.save_certificates` to permanently save the JRE certificates.
2. Click **Accessories > Java Manager**.
3. Activate **Desktop** and click **OK**.
4. Open the Java Manager (Java Control Panel) from the desktop.
5. Click **Manage Certificates...** in the **Security** tab.



6. Choose **Signer CA** under **Certificate type**.



Certificate type: Signer CA

7. Import the certificate.

> ⓘ In the UD2-MultiMedia, the commando `su user -c "javaws -viewer"` must be used. Choose **Trusted Certificates** as **Certificate type** and import the certificate.

Which CA Certificates Are Contained in IGEL OS?

The following CA certificates are contained in IGEL OS 10.06.100:

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`
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`

Certificate name	Expiry date	File in /etc/ssl/certs
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	`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`
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`
Certplus Root CA G1	Jan 15 00:00:00 2038 GMT	`Certplus_Root_CA_G1.crt`
Certplus Root CA G2	Jan 15 00:00:00 2038 GMT	`Certplus_Root_CA_G2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
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`
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`

Certificate name	Expiry date	File in /etc/ssl/certs
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 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[37] 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`

[37] http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
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`
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`

Certificate name	Expiry date	File in /etc/ssl/certs
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.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`
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	`Imprivata.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
Izenpe.com[38]	Dec 13 08:27:25 2037 GMT	`Izenpe.com`[39]`.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`
OpenTrust Root CA G1	Jan 15 00:00:00 2038 GMT	`OpenTrust_Root_CA_G1.crt`
OpenTrust Root CA G2	Jan 15 00:00:00 2038 GMT	`OpenTrust_Root_CA_G2.crt`
OpenTrust Root CA G3	Jan 15 00:00:00 2038 GMT	`OpenTrust_Root_CA_G3.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`

[38] http://Izenpe.com

[39] http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
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[40] EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	`SSL.com_EV_Root_Certification_Authority_ECC.crt`
SSL.com[41] EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	`SSL.com_EV_Root_Certification_Authority_RSA_R2.crt`
SSL.com[42] Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	`SSL.com_Root_Certification_Authority_ECC.crt`
SSL.com[43] 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`

[40] http://SSL.com
[41] http://SSL.com
[42] http://SSL.com
[43] http://SSL.com

Certificate name	Expiry date	File in /etc/ssl/certs
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`
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`

Certificate name	Expiry date	File in /etc/ssl/certs
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`
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5	Apr 28 08:07:01 2023 GMT	`TÜRKTRUST_Elektronik_Sertifika_Hizmet_Sağlayıcısı_H5.crt`
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_ECC_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
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`
Visa eCommerce Root	Jun 24 00:16:12 2022 GMT	`Visa_eCommerce_Root.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`
thawte Primary Root CA - G2	Jan 18 23:59:59 2038 GMT	`thawte_Primary_Root_CA_-_G2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
thawte Primary Root CA - G3	Dec 1 23:59:59 2037 GMT	`thawte_Primary_Root_CA_-_G3.crt`

Smartcard

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".

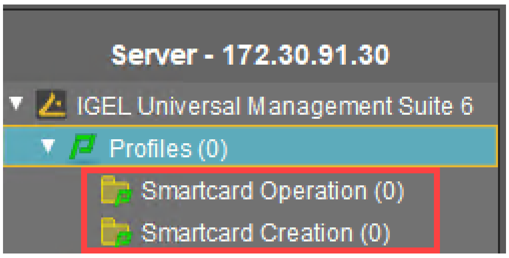
▶ Create the profile "Smartcard Login" for "Smartcard Operation".

▶ Create the profile "Smartcard Key" for "Smartcard Creation".

Creating IGEL Smartcard Folders

First, add two new profile folders for creating profiles and assigning them to devices:

- "Smartcard Operation";
- "Smartcard Creation".



Server - 172.30.91.30

▼ IGEL Universal Management Suite 6

▼ Profiles (0)

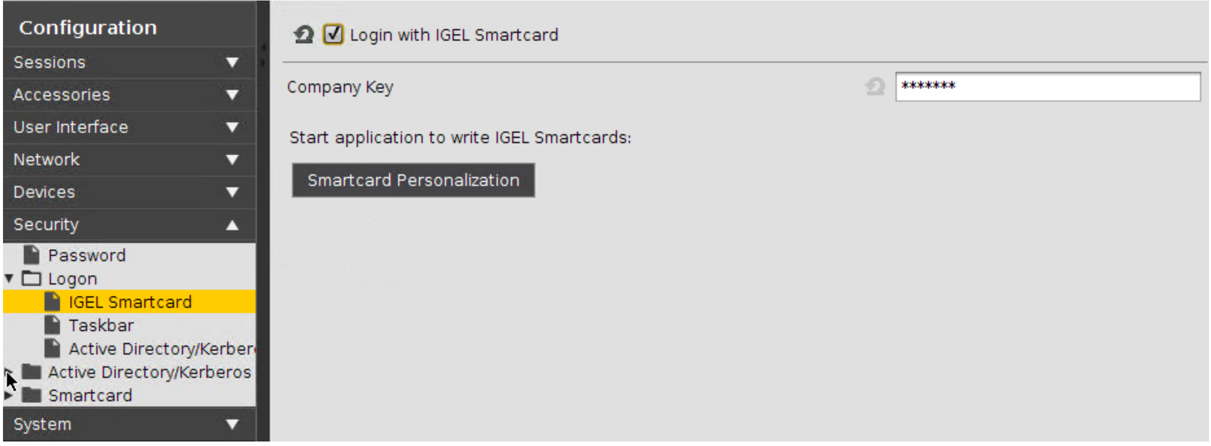
Smartcard Operation (0)

Smartcard Creation (0)

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**.



☑ Login with IGEL Smartcard

Company Key *******

Start application to write IGEL Smartcards:

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.

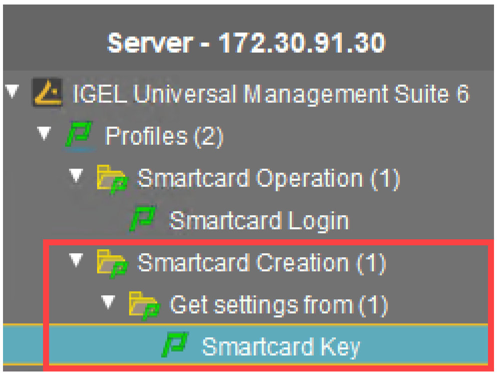
Folder "Smartcard Creation"

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.



Server - 172.30.91.30
▼ IGEL Universal Management Suite 6
▼ Profiles (2)
▼ Smartcard Operation (1)
Smartcard Login
▼ Smartcard Creation (1)
▼ Get settings from (1)
Smartcard Key

ⓘ 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.

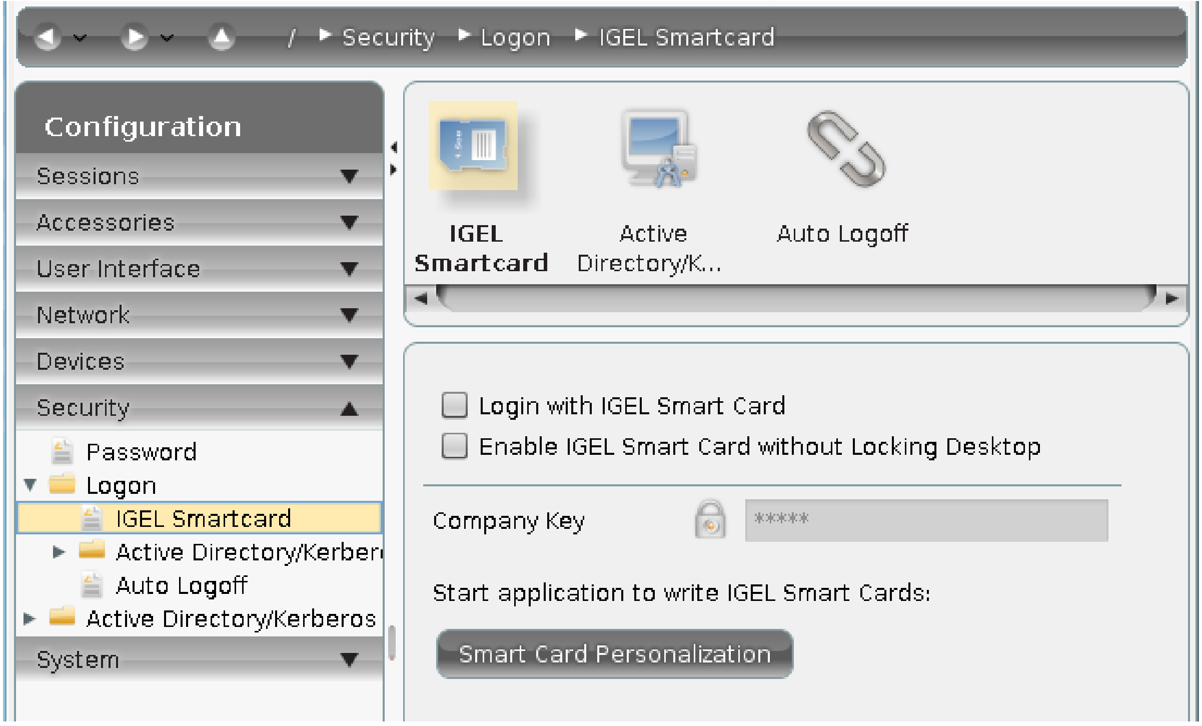
Writing the IGEL Smartcard

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.



□ Login with IGEL Smart Card

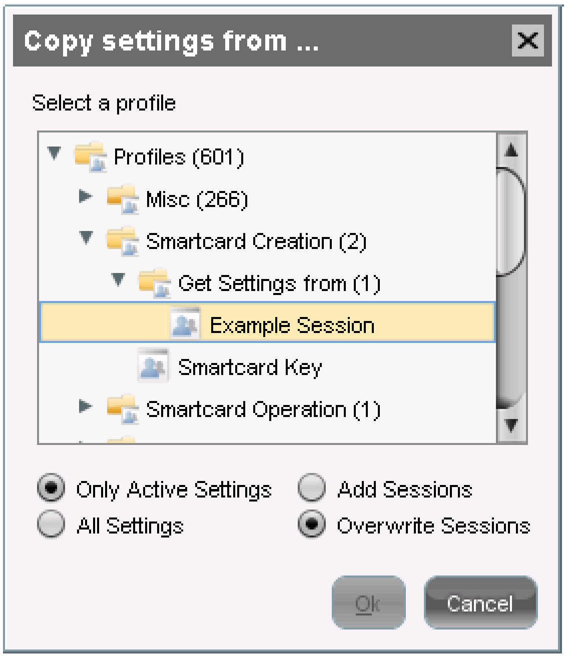
□ Enable IGEL Smart Card without Locking Desktop

Company Key *****

Start application to write IGEL Smart Cards:

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**.



Copy settings from ...

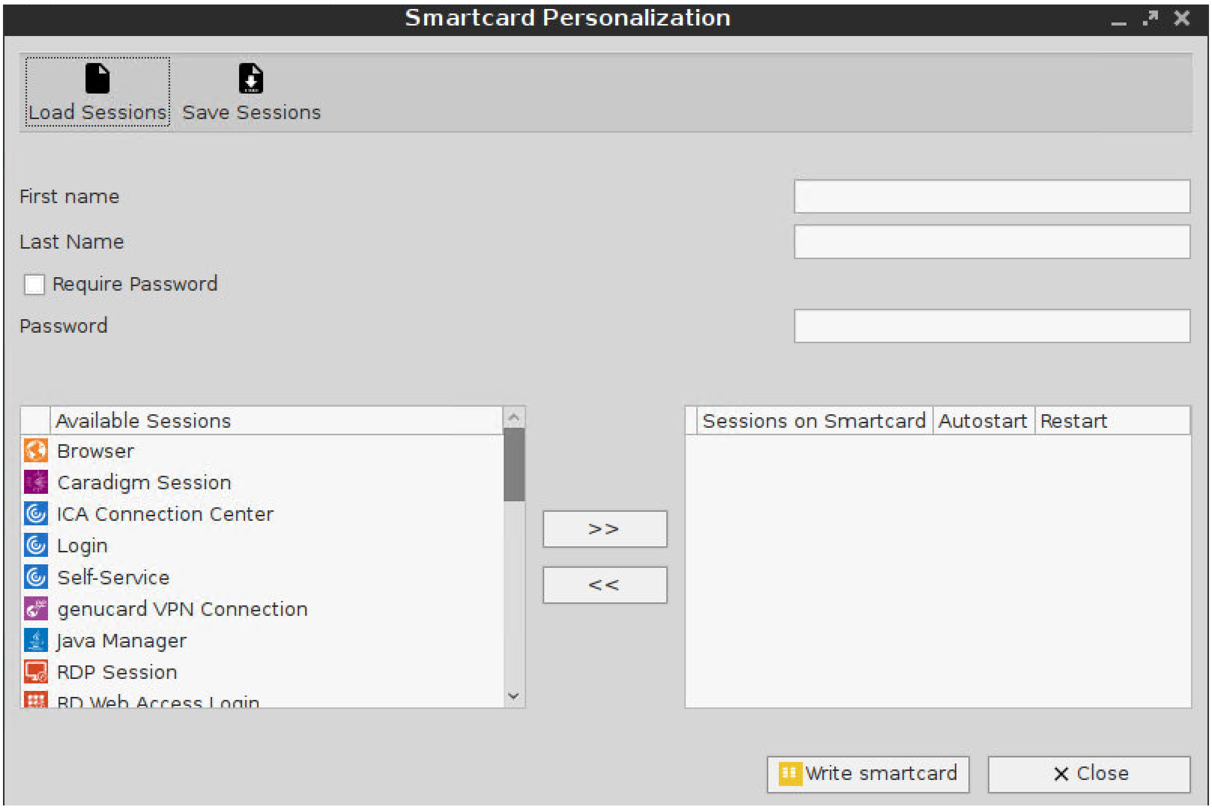
Select a profile

● Only Active Settings ○ Add Sessions
○ All Settings ● 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.



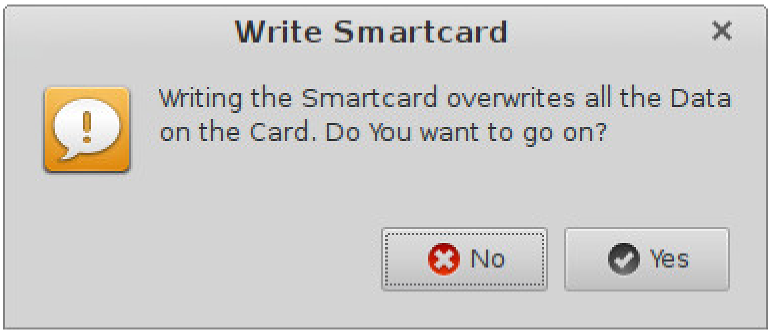
4. Enter the **First name** and the **Last name** of the smartcard holder that should appear at the login prompt.
5. Activate **Require password** and specify the **Password** if a password has to be required for the smartcard login.
6. Select the local sessions you want to write to the smartcard.

> ⓘ 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.

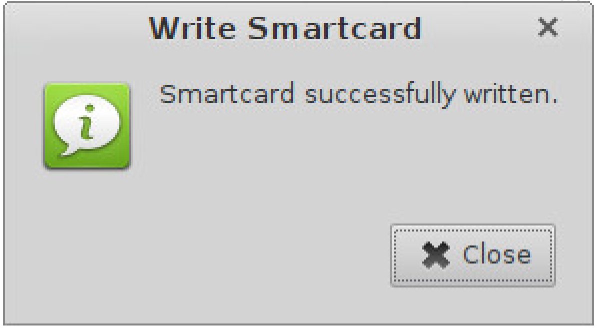
8. Click **Write smartcard** to start the writing process with the defined settings.
9. Confirm the security question with **Yes**.



Write Smartcard

Writing the Smartcard overwrites all the Data on the Card. Do You want to go on?

The notice **Smartcard successfully written** appears.



Write Smartcard

Smartcard successfully written.

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

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. For instructions on deploying certificate files, see Registering a File on the UMS Server (set **Classification** to "SSL Certificate") and Transferring a File to a Device.

Smartcard Readers

Smartcards are accessed via smartcard readers, using either a contact or contactless interface. The IGEL Third Party Database[44] lists the readers that are supported by the *Linux* firmware.

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 the *Linux*-based firmware and can be controlled via the **Activate PC/SC Daemon** parameter on **IGEL Setup > Devices > Smartcard > PC/SC** or **IGEL Setup > Security > Smartcard > PC/SC** or **IGEL Setup > Security > Smartcard > Services** (depending on the firmware version).

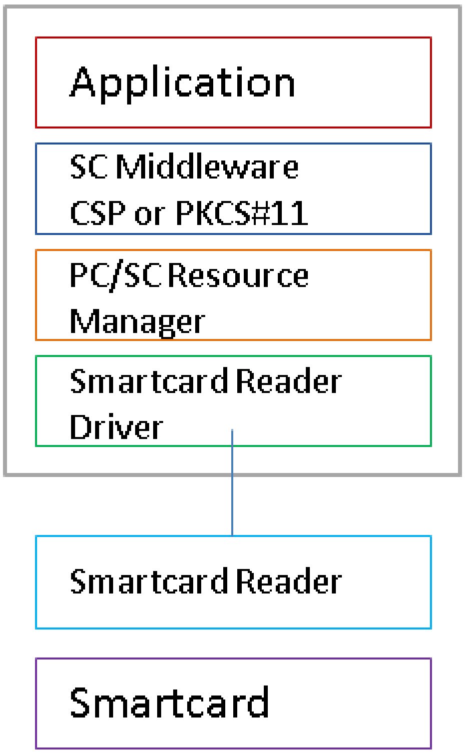
Smartcard Middleware

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	✓	✓

[44] 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*
- *Coolkey*
- *OpenSC*
- *TCOS3 (IGEL Linux v5* only*)*
  For information on how to use a custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 728).

- Active Directory Logon with Smartcard (see page 608)
- Citrix Legacy ICA Sessions (see page 609)
- Citrix Legacy ICA Sessions with Local Logon Window (see page 610)
- Citrix StoreFront (see page 611)
- RDP Sessions (see page 613)
- Horizon Sessions (see page 614)
- Smartcard Authentication in Browser (see page 615)

- Citrix XenDesktop Appliance Mode (see page 616)
- Local Login with Smartcard Certificate (see page 617)

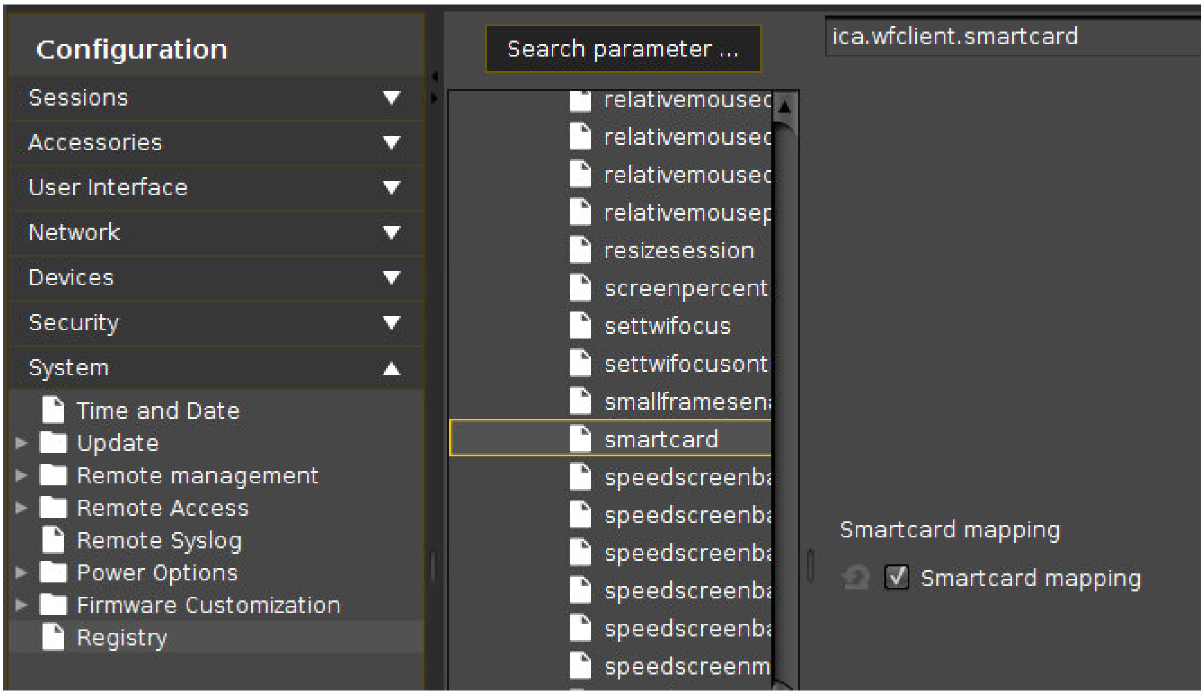
Active Directory Logon with Smartcard

See the how-to Passthrough Authentication (see page 923).

Citrix Legacy ICA Sessions

In this scenario, the *smartcard middleware* has to be installed on the server side.

1. Enable **Activate PC/SC Daemon** on the **Smartcard > PC/SC** page under **Device** or **Security**.
2. In IGEL Setup, check parameter `ica.wfclient.smartcard` under **System > Registry**.



ica.wfclient.smartcard

Smartcard mapping

☑ Smartcard mapping

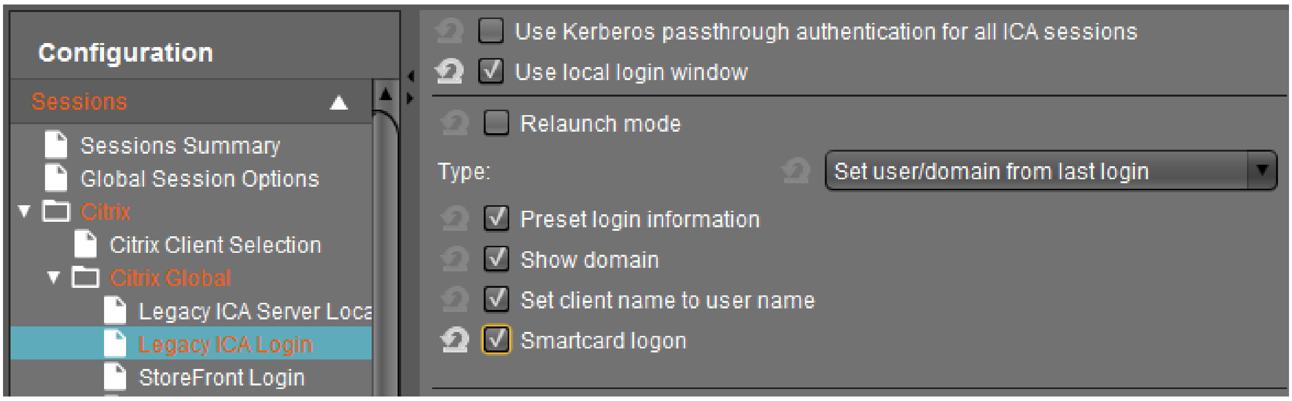
ⓘ Both settings are active by default!

Citrix Legacy ICA Sessions with Local Logon Window

This scenario allows ICA session roaming with a smartcard.

In addition to the configuration of the ICA Session, the following settings are necessary:

▶ Check to **Use local login window** and **Smartcard logon** under **Sessions > Citrix > Citrix Global > Legacy ICA Login**.



□ Use Kerberos passthrough authentication for all ICA sessions

☑ Use local login window

□ Relaunch mode

Type: Set user/domain from last login

☑ Preset login information

☑ Show domain

☑ Set client name to user name

☑ Smartcard logon

▶ Select the appropriate PKCS#11 module for the smartcard under **Security > Smartcard > Middleware**.

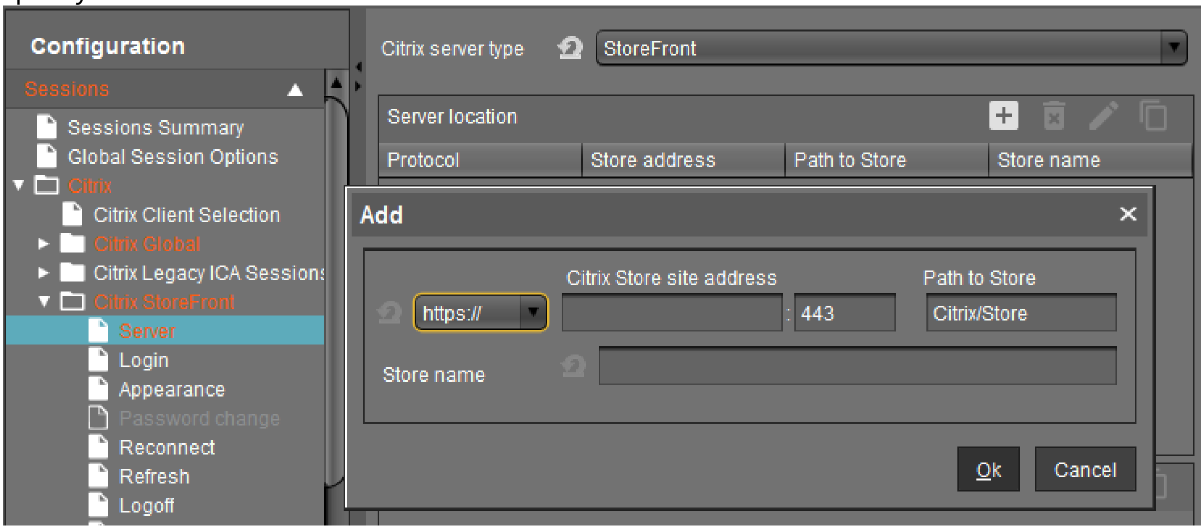
- Gemalto/SafeNet eToken
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- Secmaker Net iD
- Coolkey
- OpenSC
- Custom PKCS#11 Module

For details about the CoolKey cryptographic library, see Using a Custom PKCS#11 Library (see page 728).

Citrix StoreFront

In this scenario, *Citrix Receiver 13.1* or newer is required. 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 (see page 574), Certificate Type **SSL Certificate**.

1. Choose **StoreFront** as **Citrix server type** under **Sessions > Citrix > Citrix StoreFront > Server**.
2. Specify the **Server location**.



Citrix server type: StoreFront

Server location

Protocol	Store address	Path to Store	Store name

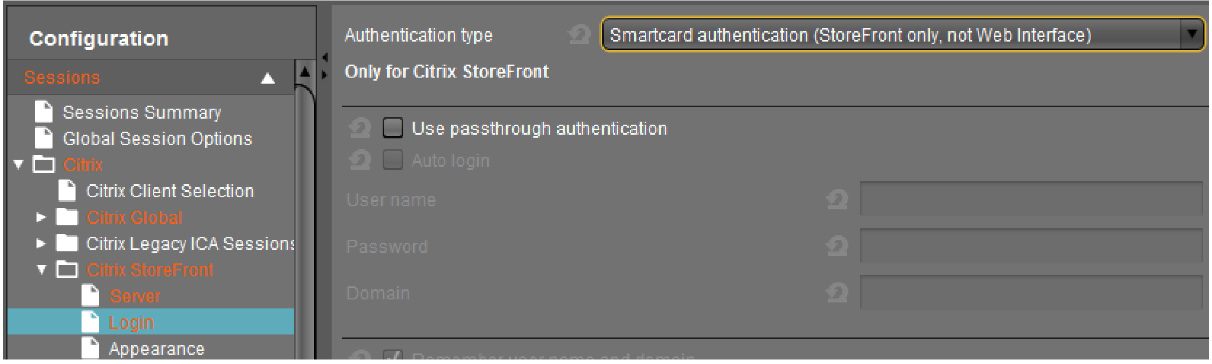
Add

Citrix Store site address: https:// : 443

Path to Store: Citrix/Store

Store name

3. Choose **Smartcard authentication** as **Authentication type** under **Sessions > Citrix > Citrix StoreFront > Login**.



Authentication type: Smartcard authentication (StoreFront only, not Web Interface)

Only for Citrix StoreFront

□ Use passthrough authentication

□ Auto login

User name

Password

Domain

> ⓘ When used in combination with **Active Directory Logon** the enabled **Use Passthrough authentication** activates single sign-on with smartcard.

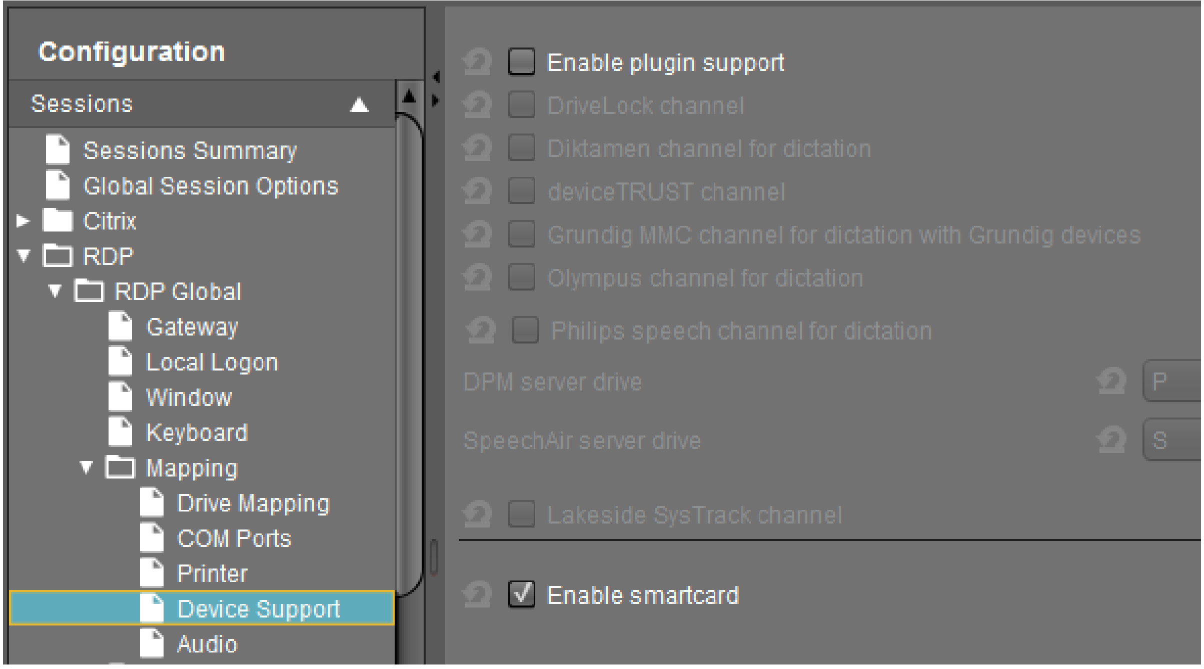
4. Select the appropriate PKCS#11 module for the smartcard **Security > Smartcard > Middleware**.
   - Gemalto/SafeNet eToken
   - cryptovision sc/interface
   - Gemalto IDPrime
   - Athena IDProtect
   - A.E.T. SafeSign
   - Secmaker Net iD

- Custom PKCS#11 module. See here also Using a Custom PKCS#11 Library (see page 728).

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**.



□ Enable plugin support
□ DriveLock channel
□ Diktamen channel for dictation
□ deviceTRUST channel
□ Grundig MMC channel for dictation with Grundig devices
□ Olympus channel for dictation
□ Philips speech channel for dictation
DPM server drive P
SpeechAir server drive S
□ Lakeside SysTrack channel
☑ Enable smartcard

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 (see page 574), certificate type **SSL Certificate**).

1. Select the appropriate PKCS#11 support for the smartcard under **Sessions > Horizon Client > Horizon Client Global > Smartcard**.
   - Gemalto/SafeNet eToken
   - cryptovision sc/interface
   - Gemalto IDPrime
   - Athena IDProtect
   - A.E.T. SafeSign
   - Secmaker Net iD
   - Coolkey
   - OpenSC

   For details on the custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 728).
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 (see page 574), certificate types **Web Browser Certificate** and (!) **SSL Certificate**.

▶ Select the appropriate PKCS#11 module (security device) for the smartcard under **Sessions > Browser > Browser Global > Smartcard Middleware**.

- Gemalto/SafeNet eToken
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- Secmaker Net iD
- Coolkey
- OpenSC

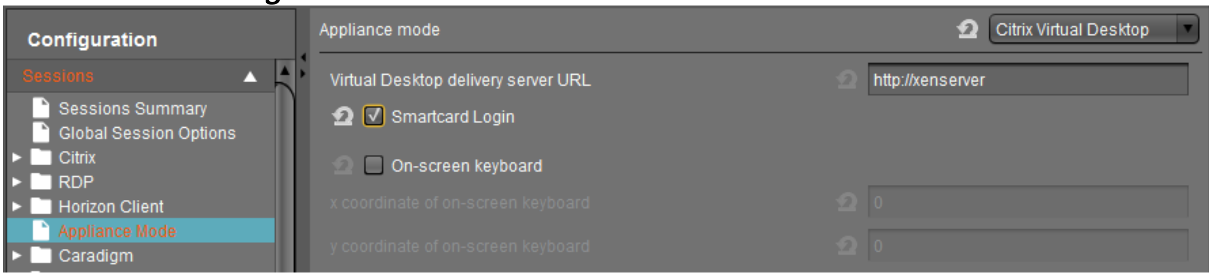
For details on the custom PKCS#11 library, refer to the article Using a Custom PKCS#11 Library (see page 728).

Citrix XenDesktop Appliance Mode

First configure the Smartcard authentication as described in Smartcard Authentication in Browser.

Additionally:

1. Activate **Enable Citrix Virtual Desktop** under **Sessions > Appliance Mode**.
2. Enter the **Virtual Desktop delivery server URL**.
3. Enable **Smartcard Login**.



Appliance mode: Citrix Virtual Desktop

Virtual Desktop delivery server URL: http://xenserver

☑ Smartcard Login

□ On-screen keyboard

x coordinate of on-screen keyboard: 0

y coordinate of on-screen keyboard: 0

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 618)
- In combination with AD/Kerberos; see Combination with the "AD/Kerberos with Smartcard" Method (see page 626) (see also Passthrough Authentication (see page 923)). 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

Prerequisites

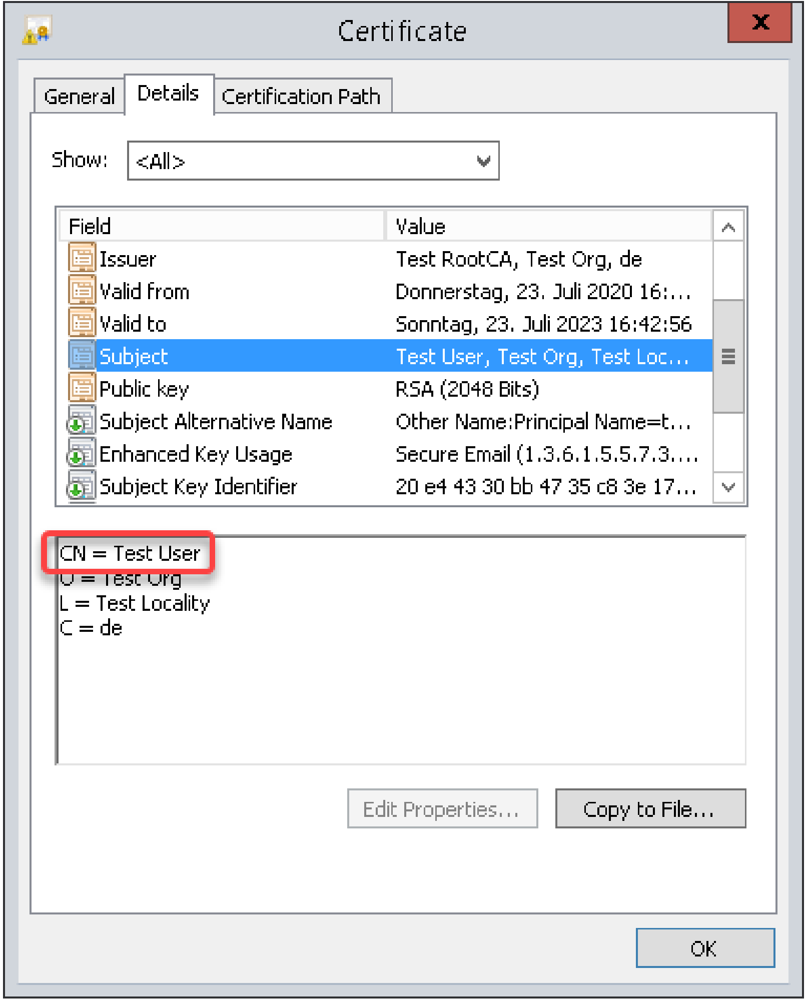
The following files are required:

- 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:

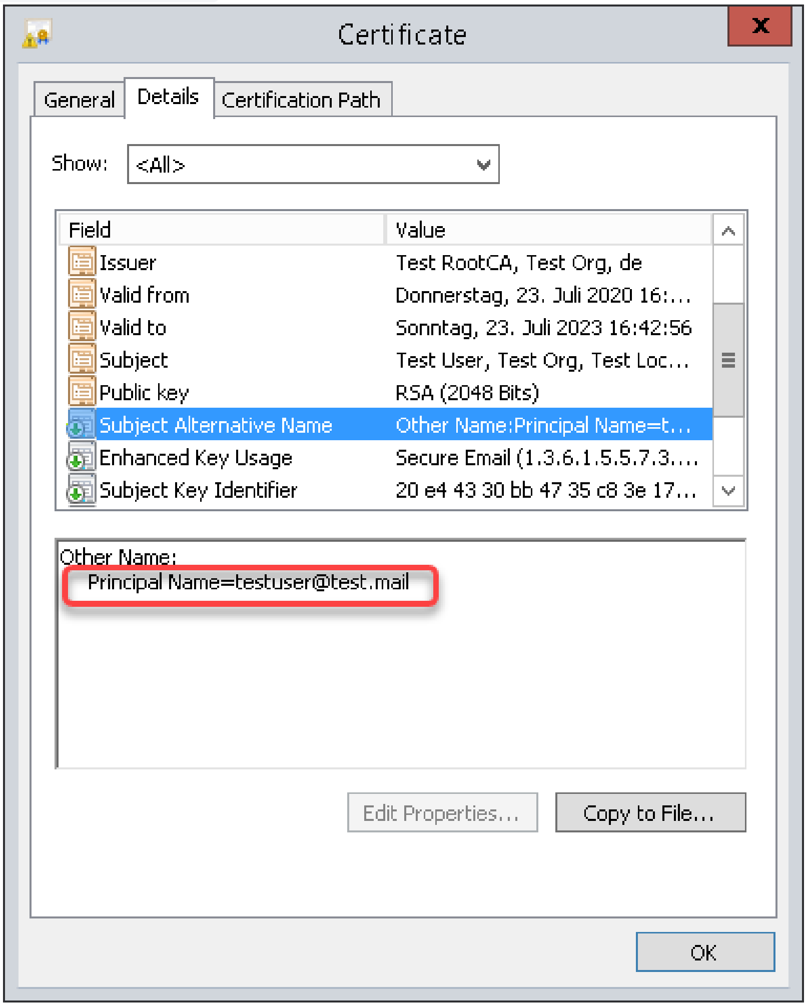


Field	Value
Issuer	Test RootCA, Test Org, de
Valid from	Donnerstag, 23. Juli 2020 16:...
Valid to	Sonntag, 23. Juli 2023 16:42:56
Subject	Test User, Test Org, Test Loc...
Public key	RSA (2048 Bits)
Subject Alternative Name	Other Name:Principal Name=t...
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3....
Subject Key Identifier	20 e4 43 30 bb 47 35 c8 3e 17...

CN = Test User
O = Test Org
L = Test Locality
C = de

- `<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 624)):
  - 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:

Field	Value
Issuer	Test RootCA, Test Org, de
Valid from	Donnerstag, 23. Juli 2020 16:...
Valid to	Sonntag, 23. Juli 2023 16:42:56
Subject	Test User, Test Org, Test Loc...
Public key	RSA (2048 Bits)
Subject Alternative Name	Other Name:Principal Name=t...
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3....
Subject Key Identifier	20 e4 43 30 bb 47 35 c8 3e 17...

    Other Name:
    Principal Name=testuser@test.mail

  - When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example:

    ```
    testuser@MY.DOMAIN
    ```

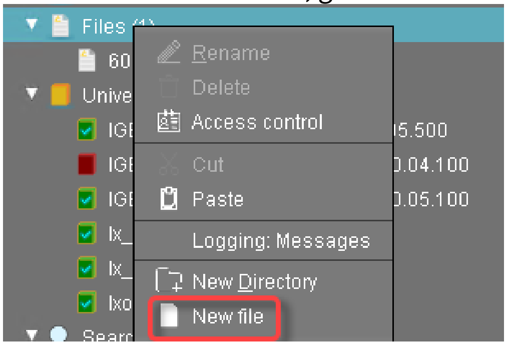
Example line: `Test User -> testuser@test.mail@MY.DOMAIN`

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.

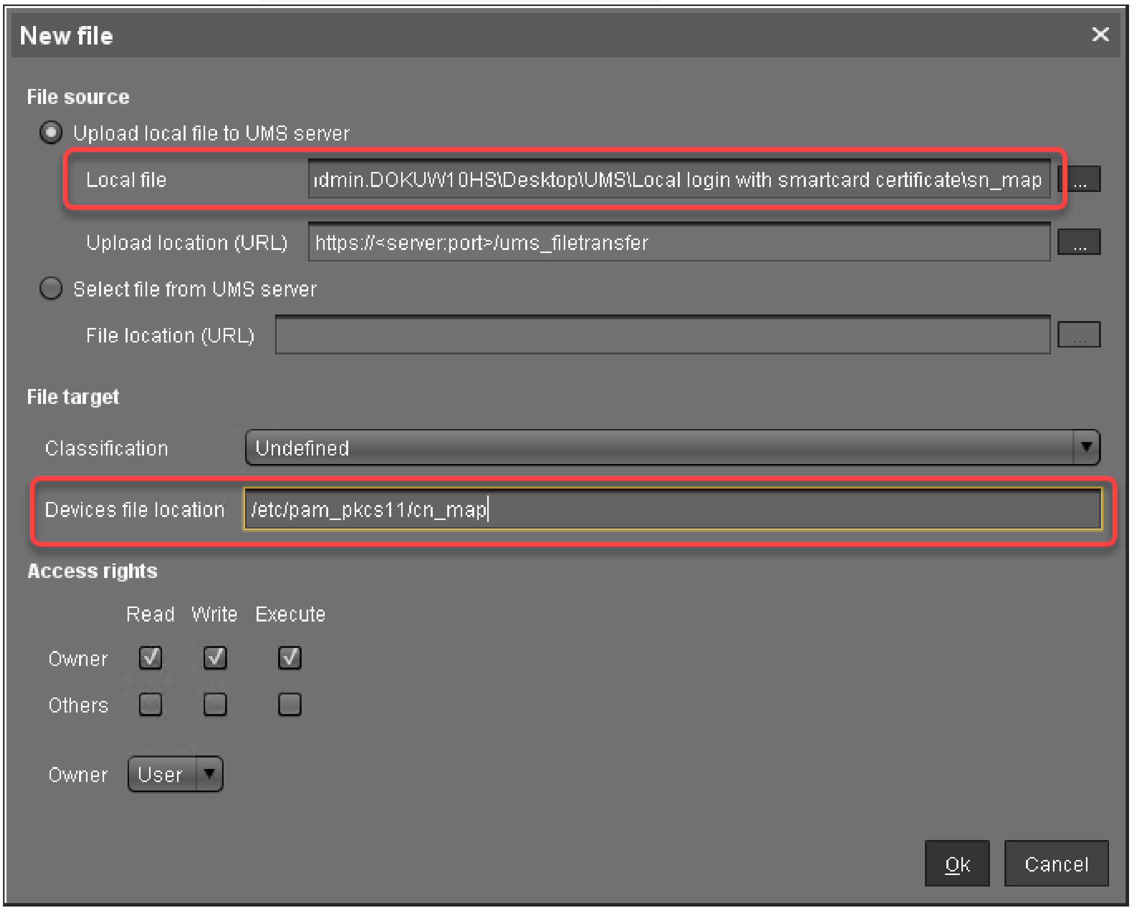
To transfer the `cn_map` file to the devices:

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`



New file

File source

● Upload local file to UMS server

Local file: ıdmin.DOKUW10HS\Desktop\UMS\Local login with smartcard certificate\sn_map

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /etc/pam_pkcs11/cn_map

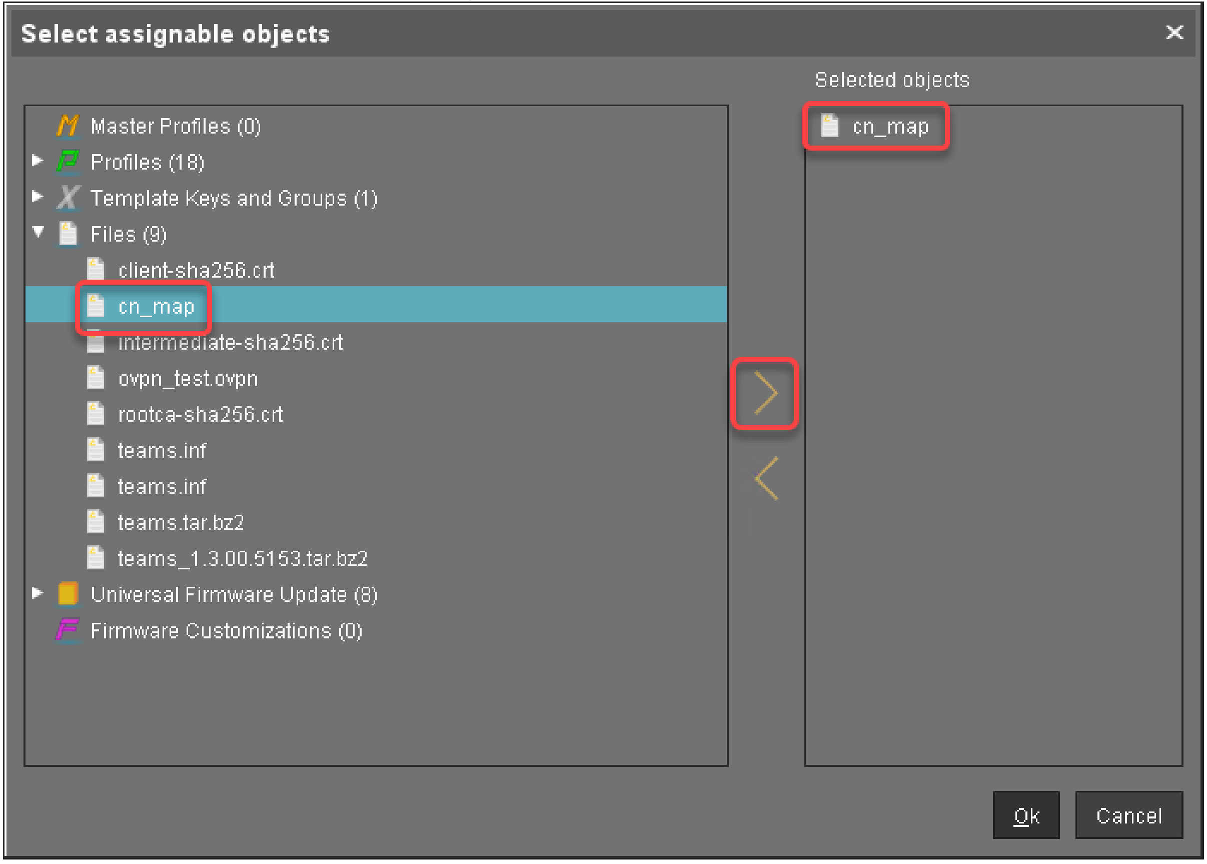
Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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 Creating Profiles).
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**.

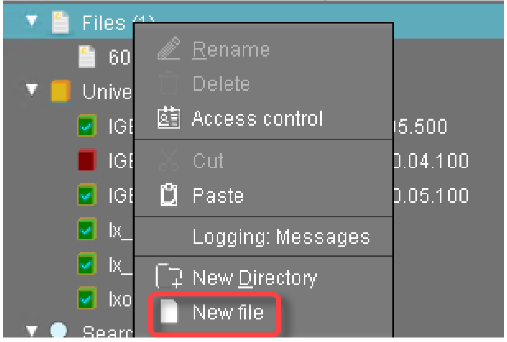
   The `cn_map` file is transferred to the endpoint device.

Transferring the Certificate Files to the Devices

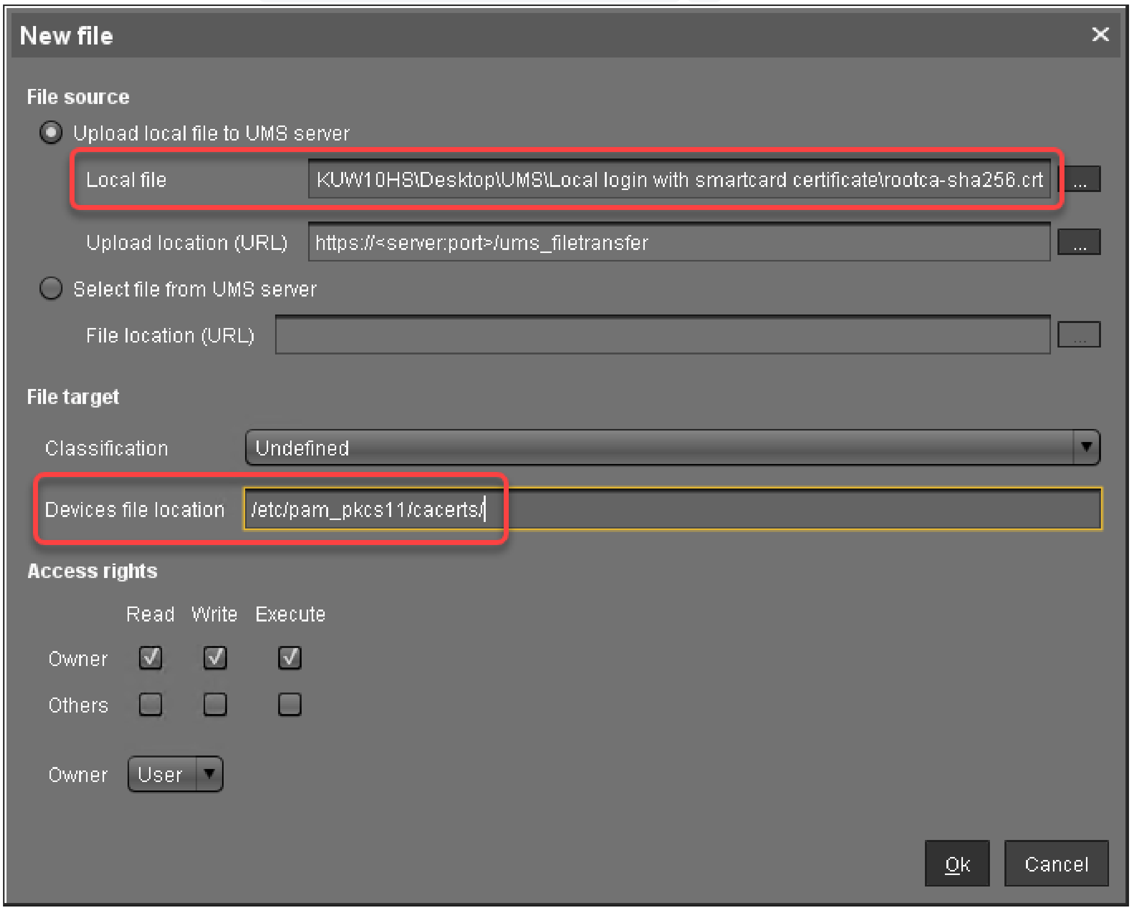
Registering the Certificate Files as File Objects

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` `/`



New file

File source

● Upload local file to UMS server

Local file: KUW10HS\Desktop\UMS\Local login with smartcard certificate\rootca-sha256.crt

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /etc/pam_pkcs11/cacerts/

Access rights

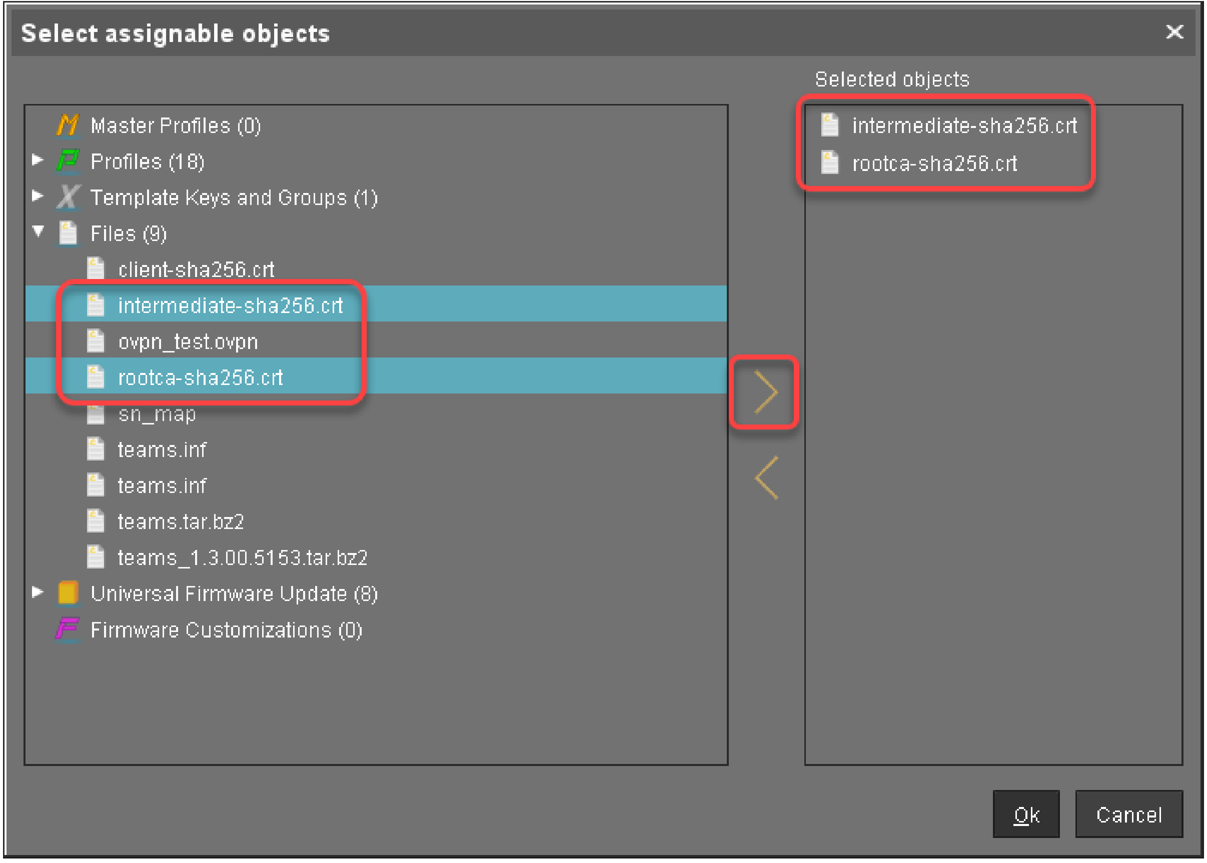
	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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 Creating Profiles).
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 **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

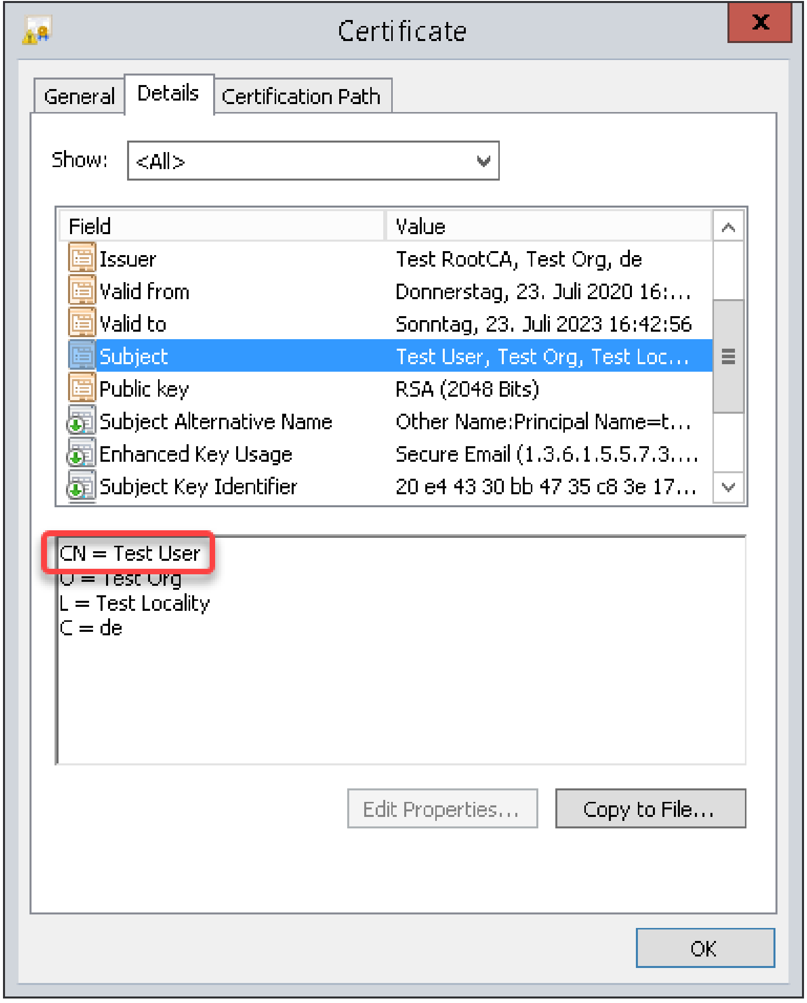
The following files are required:

- 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:

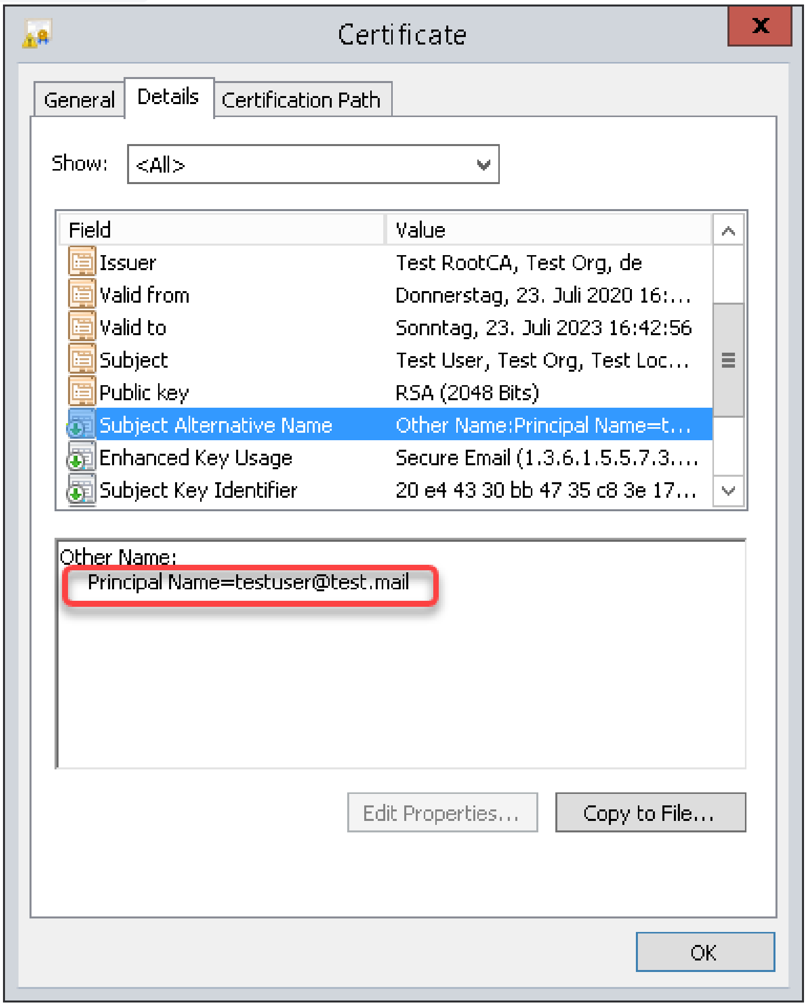


Field	Value
Issuer	Test RootCA, Test Org, de
Valid from	Donnerstag, 23. Juli 2020 16:...
Valid to	Sonntag, 23. Juli 2023 16:42:56
Subject	Test User, Test Org, Test Loc...
Public key	RSA (2048 Bits)
Subject Alternative Name	Other Name:Principal Name=t...
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3....
Subject Key Identifier	20 e4 43 30 bb 47 35 c8 3e 17...

CN = Test User
O = Test Org
L = Test Locality
C = de

- `<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 632)):
    - 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:

      Certificate

      General | Details | Certification Path

      Show: <All>

Field	Value
Issuer	Test RootCA, Test Org, de
Valid from	Donnerstag, 23. Juli 2020 16:...
Valid to	Sonntag, 23. Juli 2023 16:42:56
Subject	Test User, Test Org, Test Loc...
Public key	RSA (2048 Bits)
Subject Alternative Name	Other Name:Principal Name=t...
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3....
Subject Key Identifier	20 e4 43 30 bb 47 35 c8 3e 17...

      Other Name:
      Principal Name=testuser@test.mail

    - When Enterprise Kerberos names are disabled, the user domain is the same as the default domain. Example: `testuser@MY.DOMAIN`

Example line:

```
   Test User ->
```

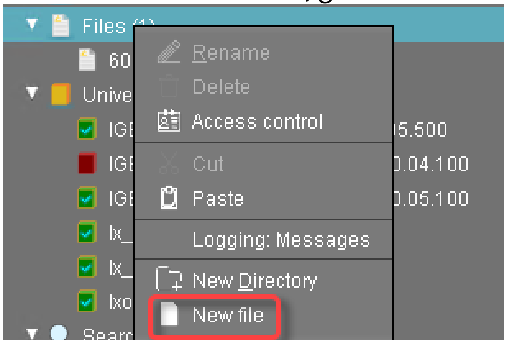
```
testuser@test.mail@MY.DOMAIN
```

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.

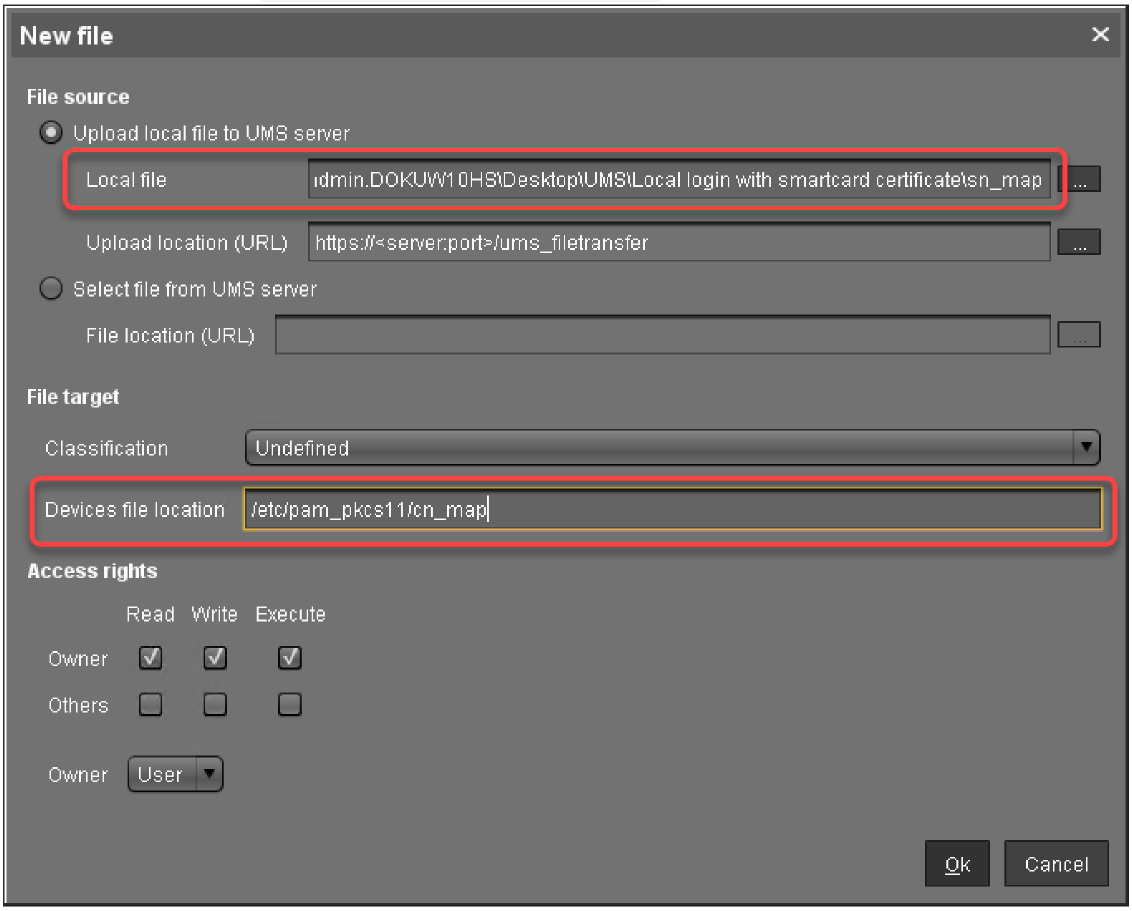
To transfer the `cn_map` file to the devices:

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`



New file

File source

● Upload local file to UMS server

Local file: ıdmin.DOKUW10HS\Desktop\UMS\Local login with smartcard certificate\sn_map

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /etc/pam_pkcs11/cn_map

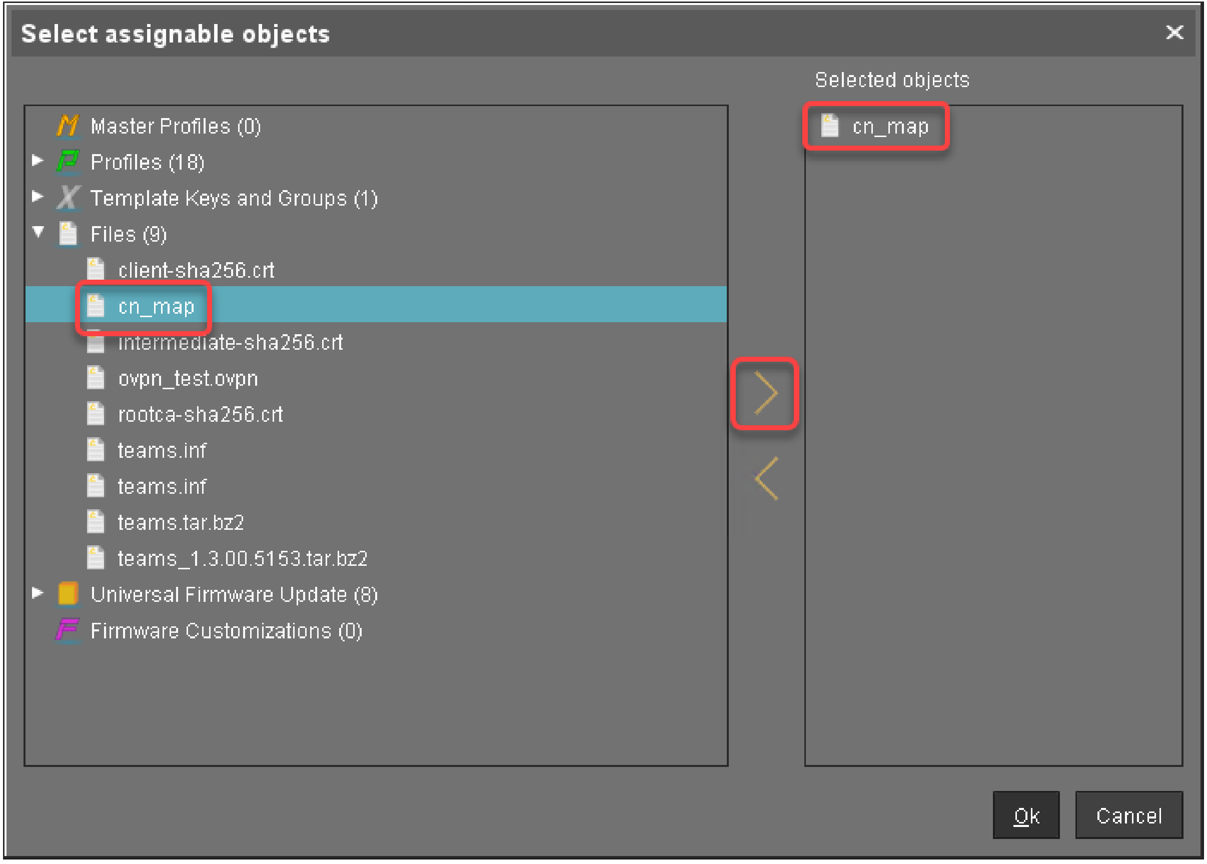
Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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 Creating Profiles).
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**.

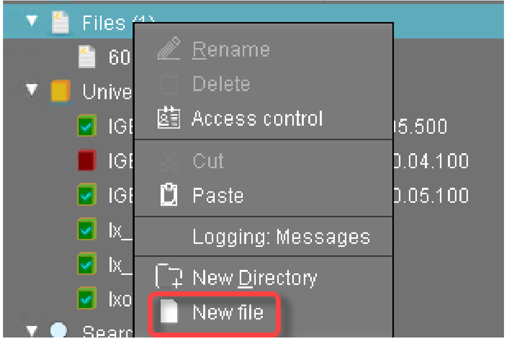
   The `cn_map` file is transferred to the endpoint device.

Transferring the Certificate Files to the Devices

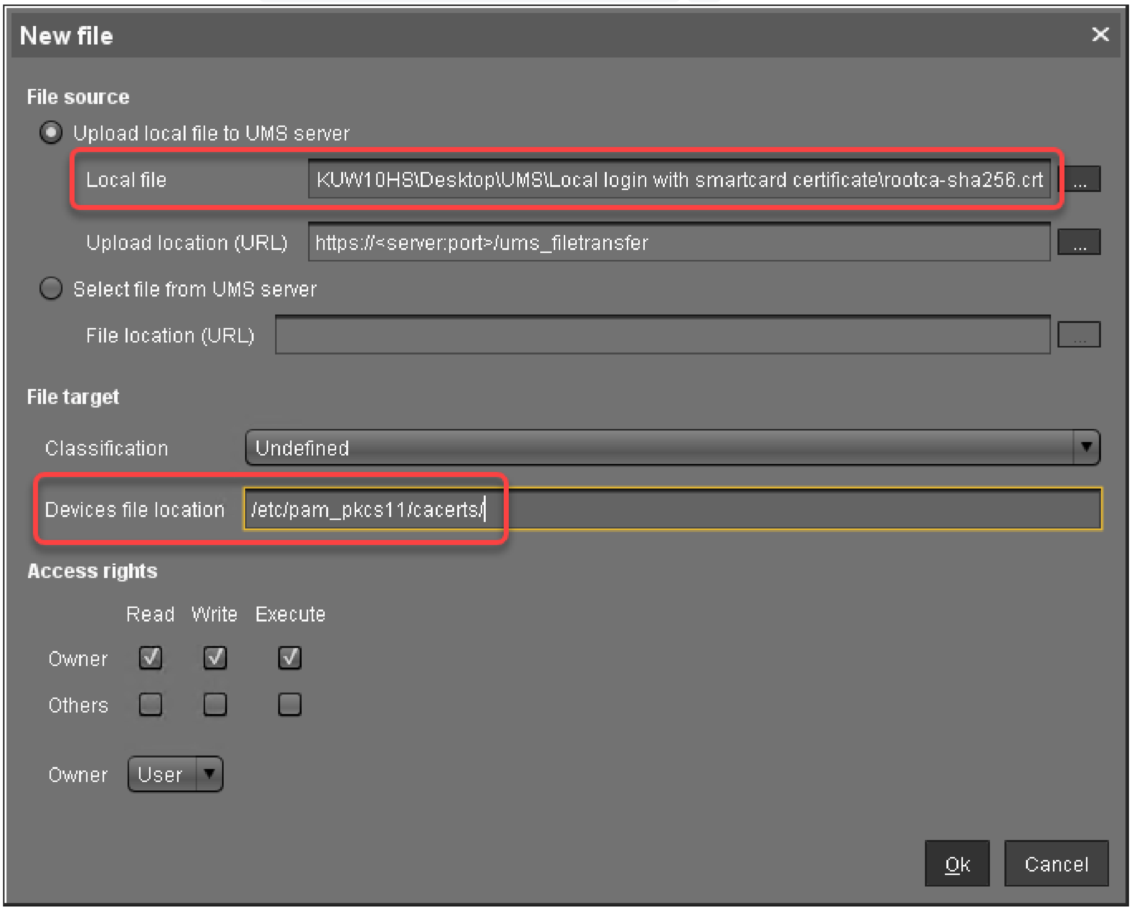
Registering the Certificate Files as File Objects

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` `/`



New file

File source

● Upload local file to UMS server

Local file: KUW10HS\Desktop\UMS\Local login with smartcard certificate\rootca-sha256.crt

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /etc/pam_pkcs11/cacerts/

Access rights

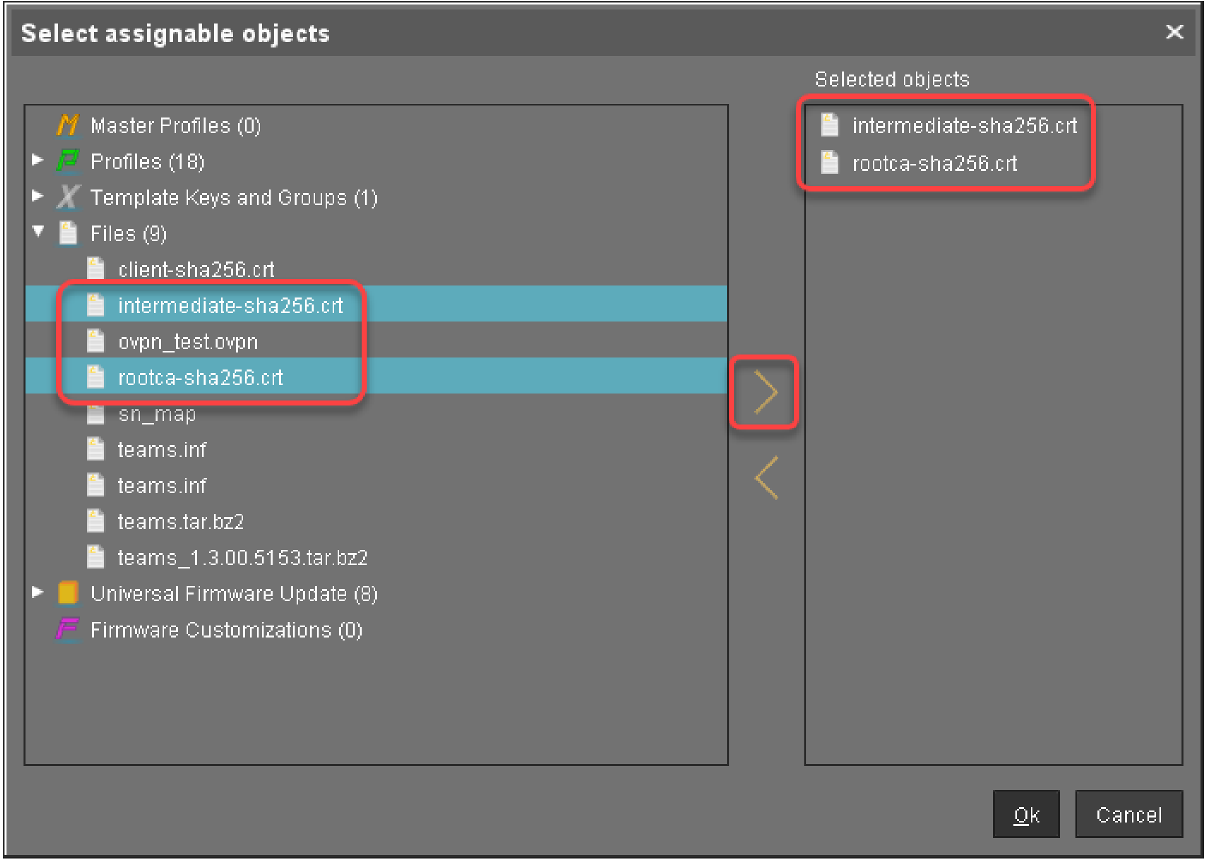
	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

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 Creating Profiles).
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.
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

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])
```

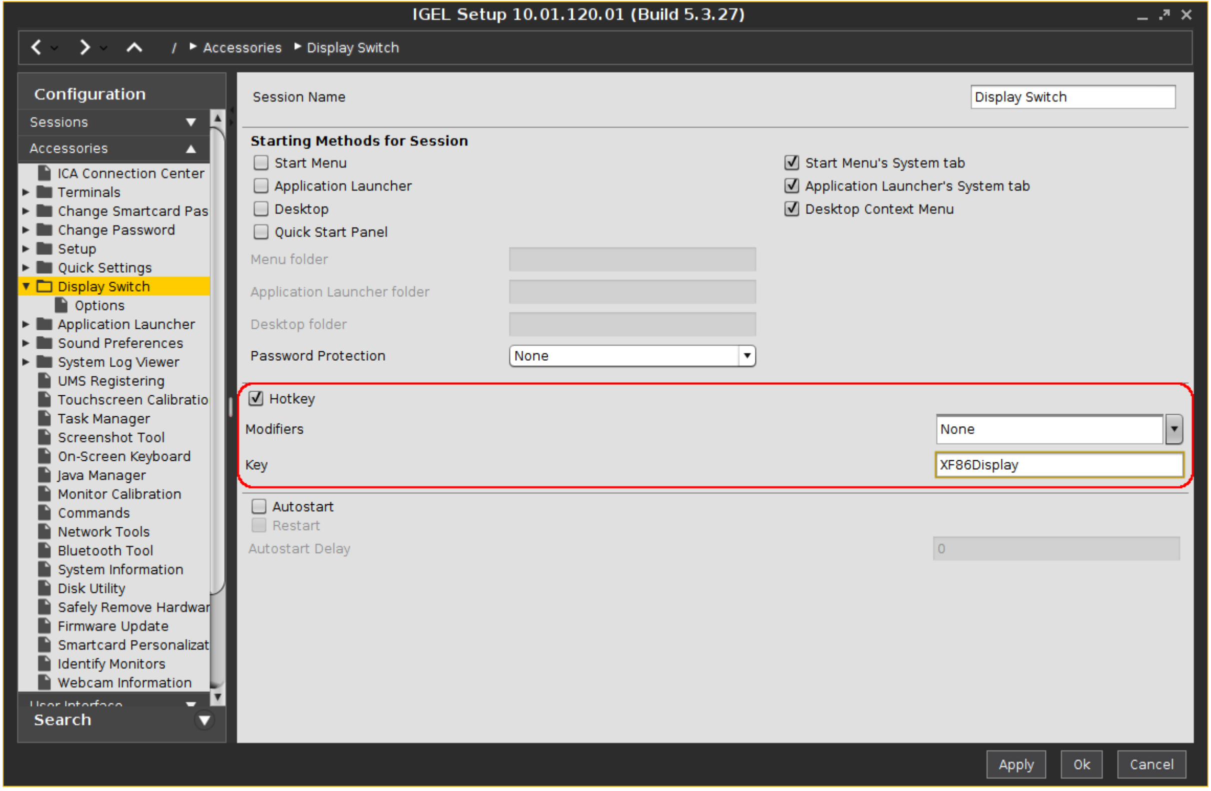
Display Switch

If you are using a notebook with IGEL UDC2, UDC3, or UD Pocket, you might want to connect an addtional 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**.



IGEL Setup 10.01.120.01 (Build 5.3.27)

Session Name: Display Switch

Starting Methods for Session

- ☐ Start Menu
- ☐ Application Launcher
- ☐ Desktop
- ☐ Quick Start Panel
- ☑ Start Menu's System tab
- ☑ Application Launcher's System tab
- ☑ Desktop Context Menu

Menu folder

Application Launcher folder

Desktop folder

Password Protection: None

☑ Hotkey

Modifiers: None

Key: XF86Display

☐ Autostart

☐ Restart

Autostart Delay: 0

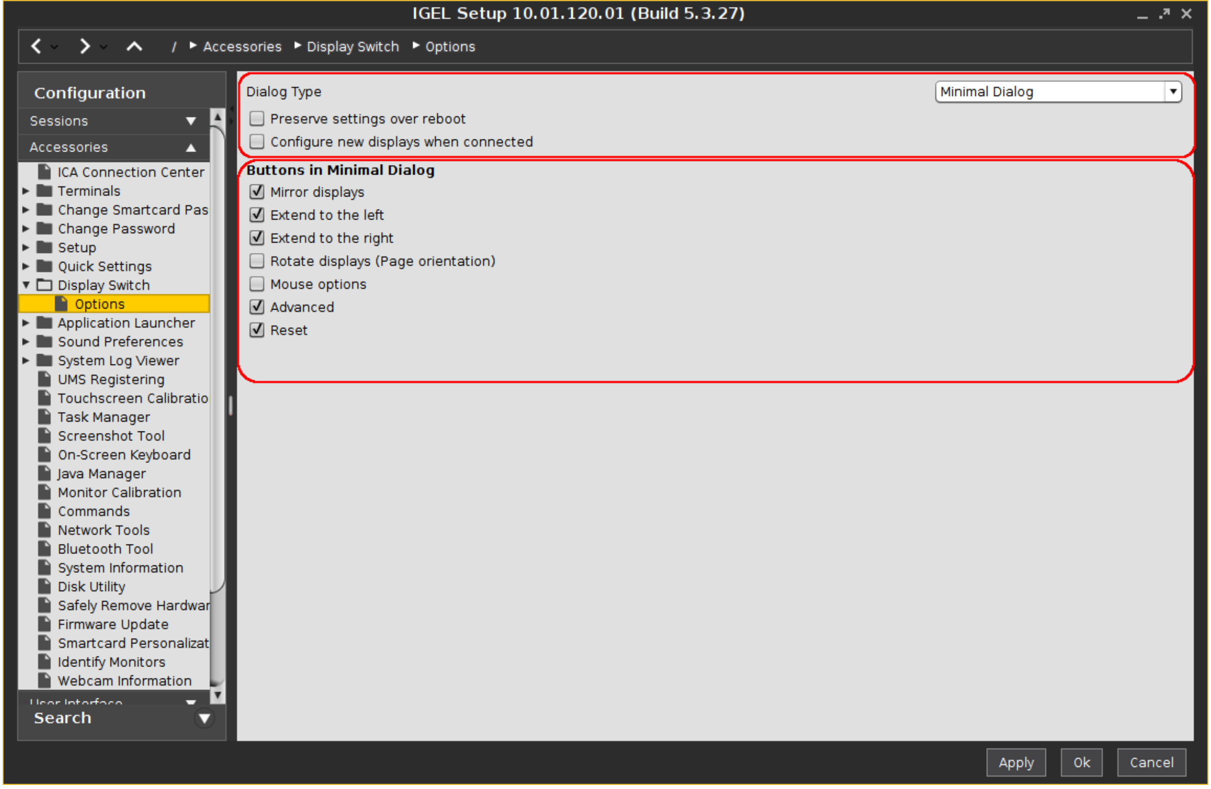
By default, [Fn]+[F7] (`XF86Display`) is defined as the hotkey for starting the display switch. You can change the hotkey by selecting or entering different keys in **Modifiers** and **Key**.

> ⓘ 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 **Buttons in Minimal Dialog** area is activated.
    - **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**.



Dialog Type: Minimal Dialog

☐ Preserve settings over reboot

☐ Configure new displays when connected

Buttons in Minimal Dialog

☑ Mirror displays

☑ Extend to the left

☑ Extend to the right

☐ Rotate displays (Page orientation)

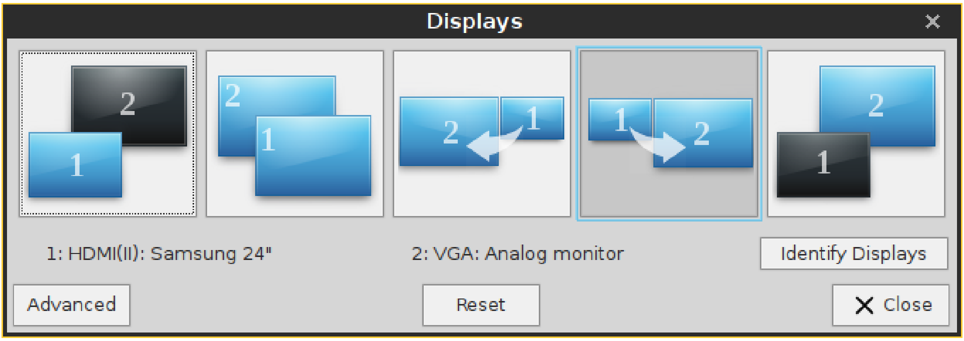
☐ Mouse options

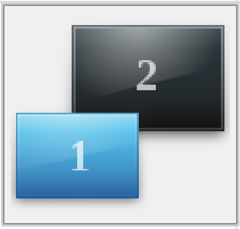
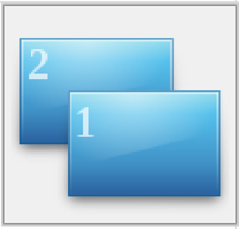
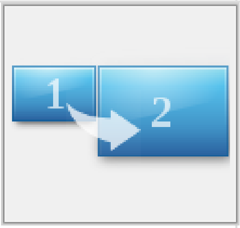
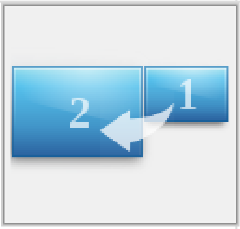
☑ Advanced

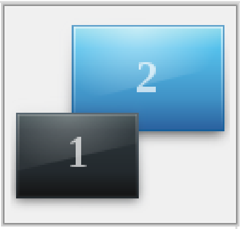
☑ Reset

Use the Display Switch

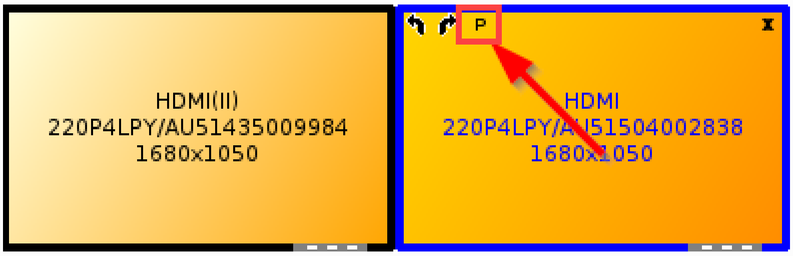
The minimal dialog will look similar to this; details depend on your specific setup:



Button	Function
Identify Displays	Starts the monitor detection.
	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.

For more information, see the manual chapter Using Display Switch.



HDMI(II)
220P4LPY/AU51435009984
1680x1050

HDMI
220P4LPY/AU51504002838
1680x1050

The **P** marks the **primary Desktop.**

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 641)
- Manual Configuration (see page 643)
- Additional Settings (see page 645)
- Auto Switch Monitor Configuration for Notebooks (see page 650)

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[45] for supported graphic cards.

[45] https://www.igel.com/linux-3rd-party-hardware-database/

Automatic Configuration

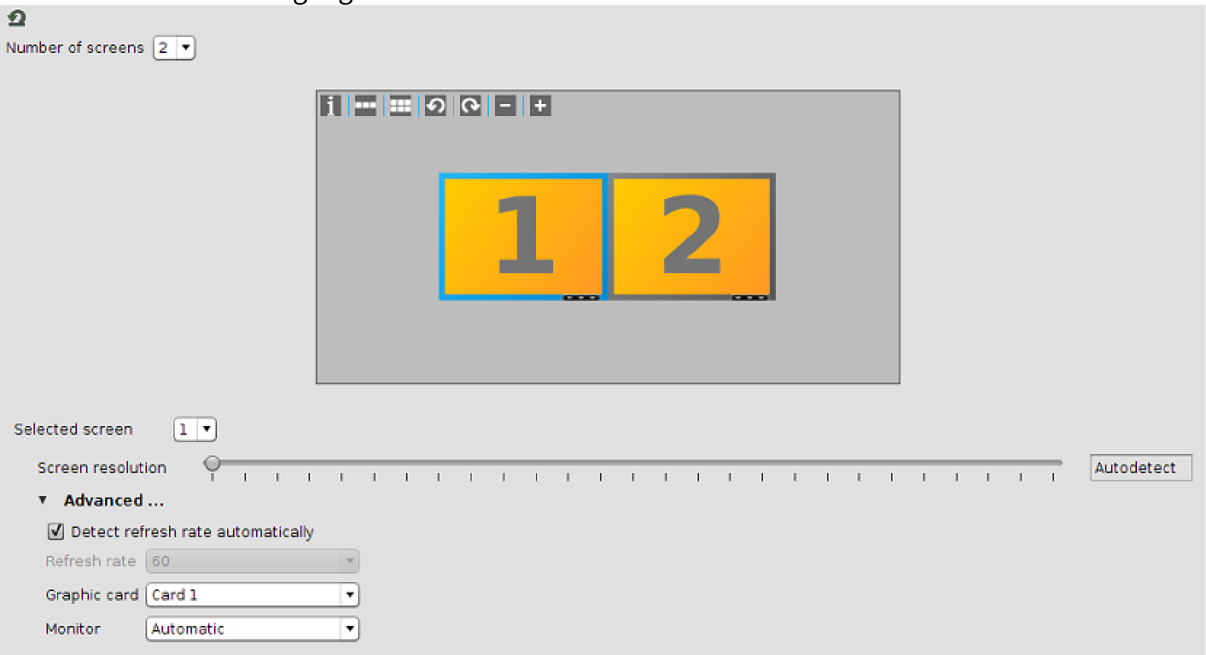
The firmware recognizes the native graphic driver and will apply the screens automatically by default.

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:



Number of screens 2

Selected screen 1

Screen resolution Autodetect

▾ Advanced ...

☑ Detect refresh rate automatically

Refresh rate 60

Graphic card Card 1

Monitor Automatic

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 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.

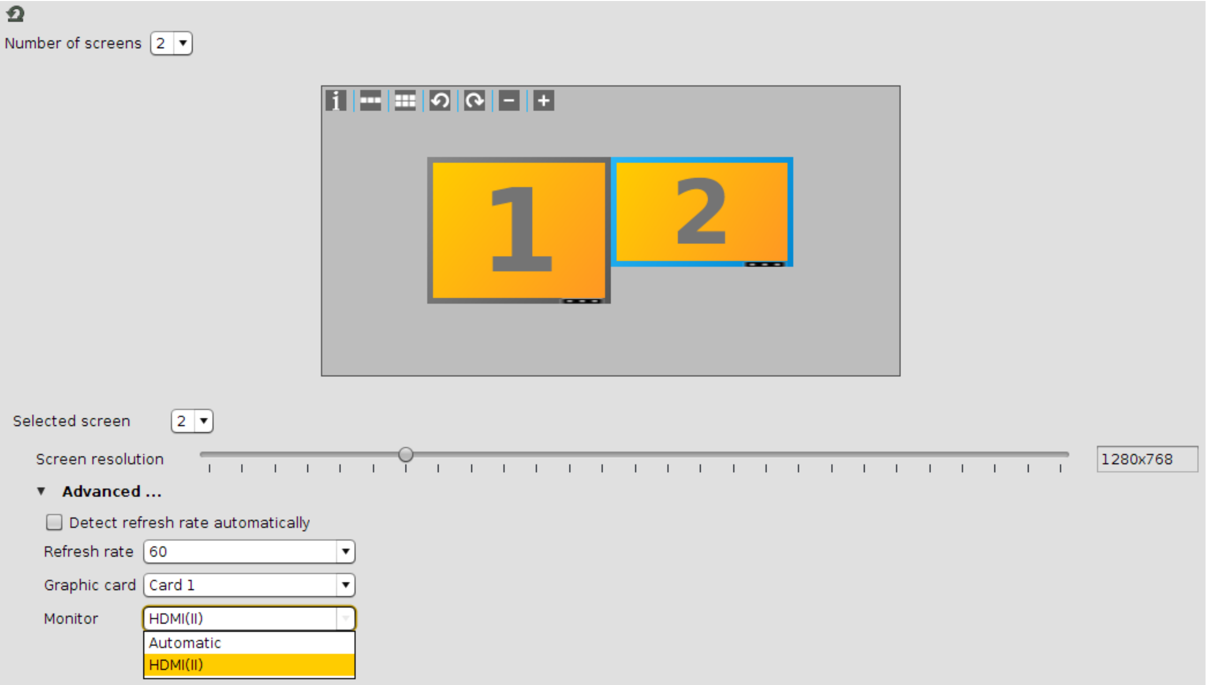
Manual Configuration

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.



Number of screens 2

Selected screen 2

Screen resolution 1280x768

Advanced ...

□ Detect refresh rate automatically

Refresh rate 60

Graphic card Card 1

Monitor HDMI(II)

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.

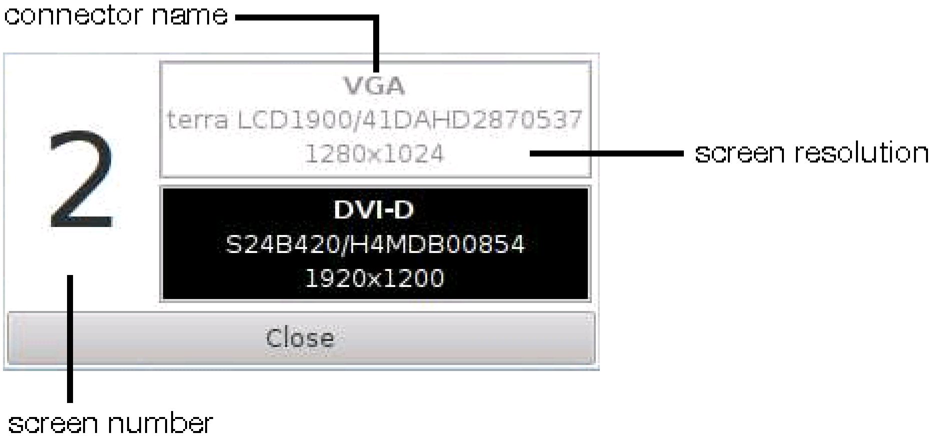
   > ⓘ If you adjust the settings directly in IGEL Setup, only the connected monitors will be available in the selection list. If you want to configure the screens using the UMS profile, all possible connectors will be shown in the selection list and you will not know which one is relevant for your device.

Tip:

▶ Click i 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:



2

VGA
terra LCD1900/41DAHD2870537
1280x1024

DVI-D
S24B420/H4MDB00854
1920x1200

Close

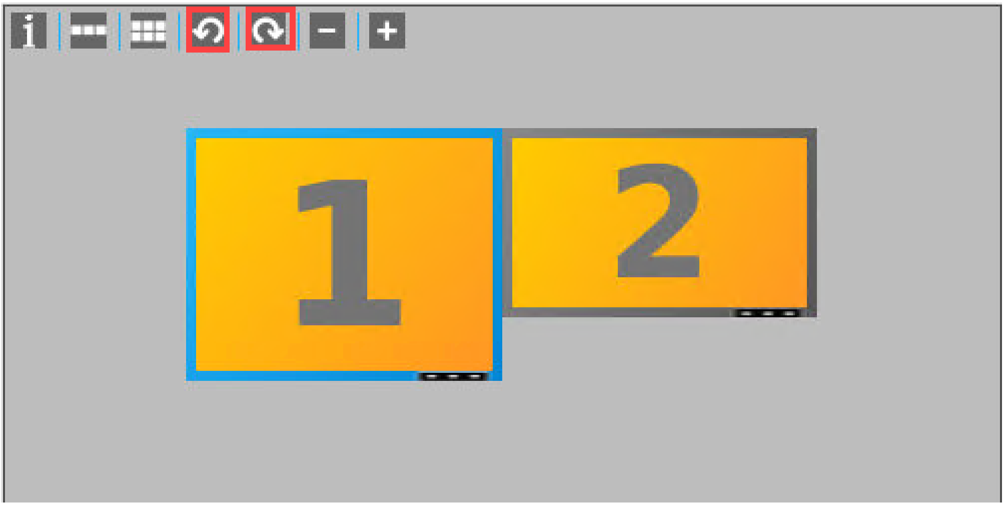
Additional Settings

A number of useful tips are provided below:

- Rotating a Screen (Pivot) (see page 646)
- Setting Different Backgrounds (see page 647)
- Useful Window Settings (see page 648)

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.

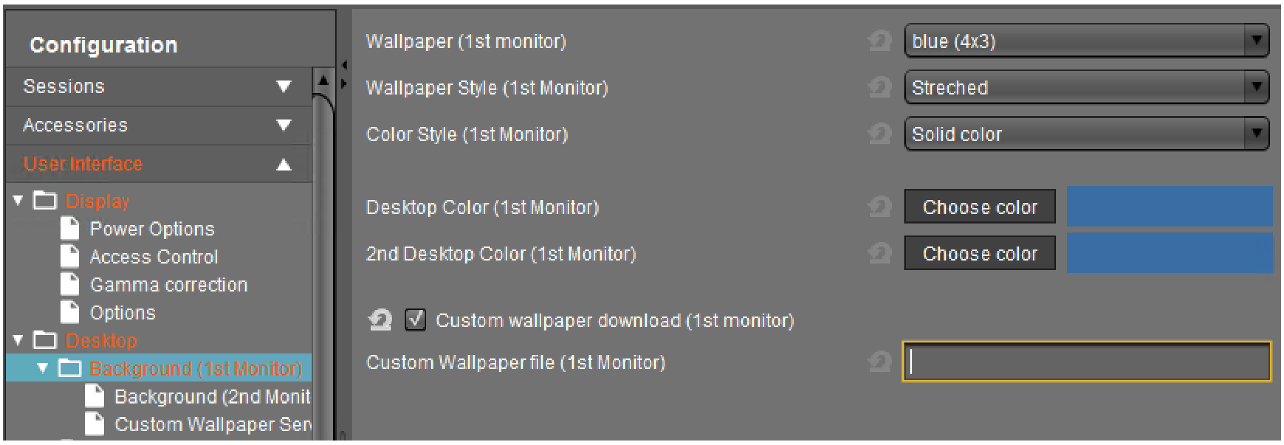
ⓘ The individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap.

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.



Wallpaper (1st monitor): blue (4x3)

Wallpaper Style (1st Monitor): Streched

Color Style (1st Monitor): Solid color

Desktop Color (1st Monitor): Choose color

2nd Desktop Color (1st Monitor): Choose color

☑ Custom wallpaper download (1st monitor)

Custom Wallpaper file (1st Monitor):

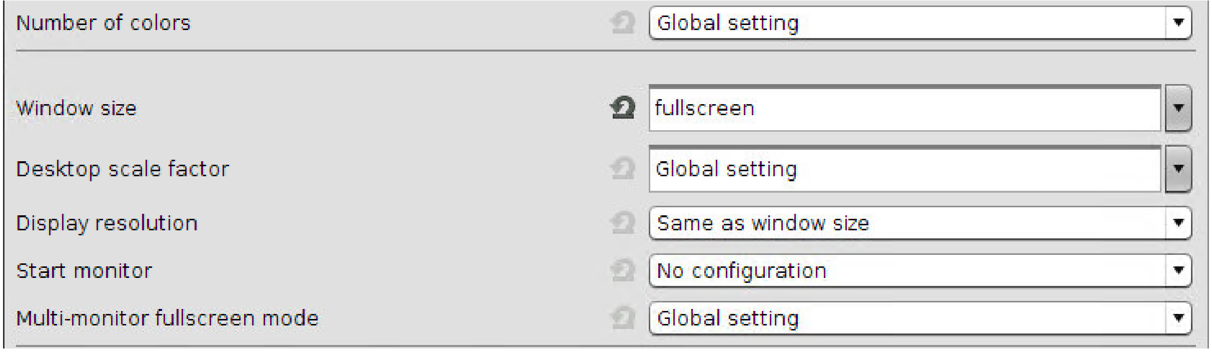
- Select the wallpaper and define the style.

ⓘ You may also upload your own **Custom Wallpaper**, e.g. a background with your corporate design. See Creating Your Own Wallpaper (see page 740).

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.

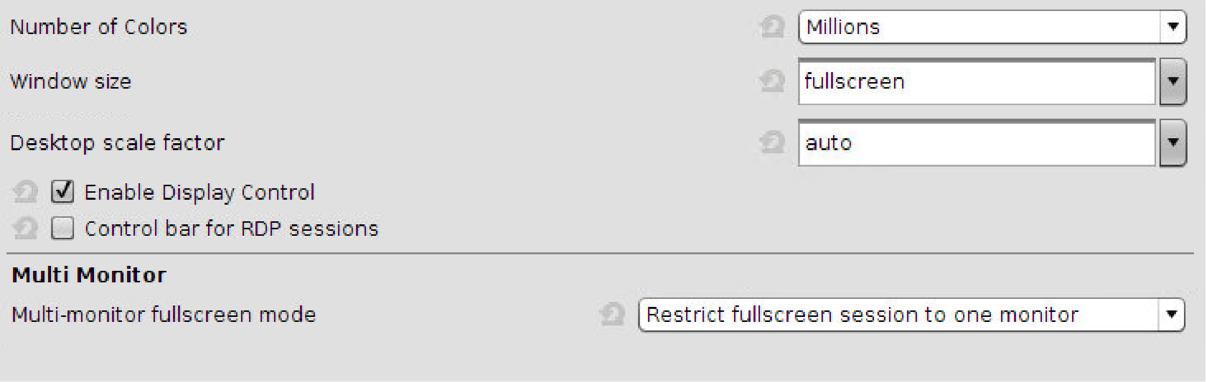


Number of colors	Global setting
Window size	fullscreen
Desktop scale factor	Global setting
Display resolution	Same as window size
Start monitor	No configuration
Multi-monitor fullscreen mode	Global setting

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.



Number of Colors	Millions
Window size	fullscreen
Desktop scale factor	auto

☑ Enable Display Control

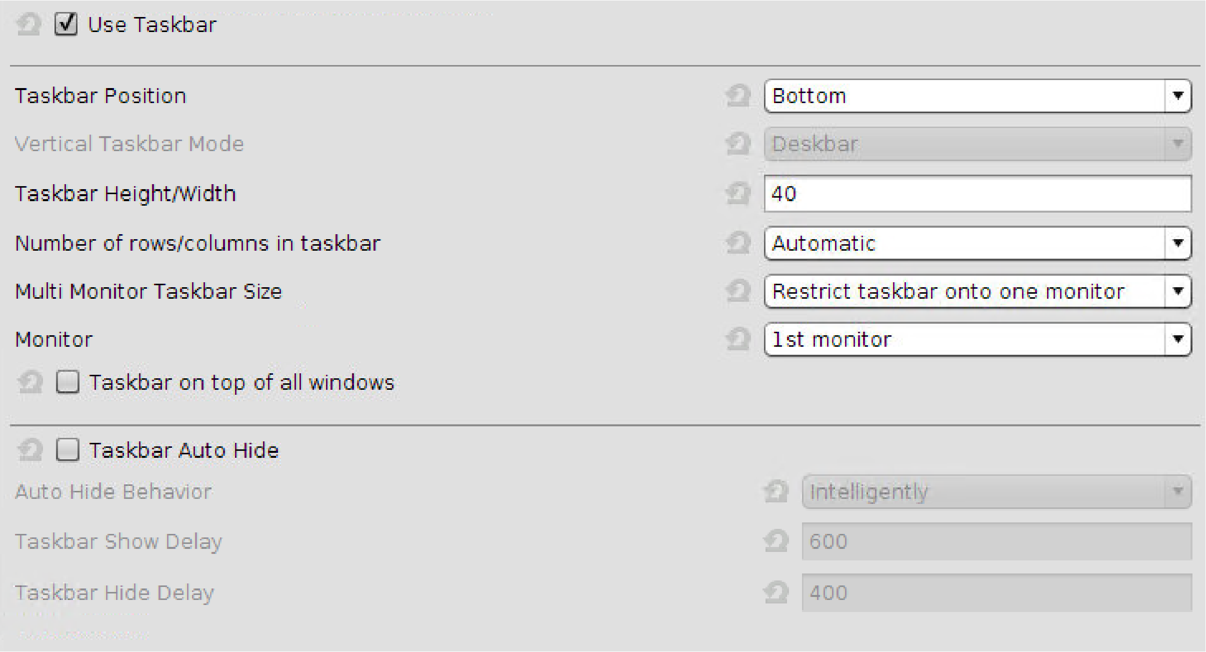
□ Control bar for RDP sessions

Multi Monitor

Multi-monitor fullscreen mode	Restrict fullscreen session to one monitor

Defining the Taskbar

1. Click **User Interface > Desktop > Taskbar**.
2. Define the **Taskbar** settings.



☑ Use Taskbar

Taskbar Position: Bottom

Vertical Taskbar Mode: Deskbar

Taskbar Height/Width: 40

Number of rows/columns in taskbar: Automatic

Multi Monitor Taskbar Size: Restrict taskbar onto one monitor

Monitor: 1st monitor

□ Taskbar on top of all windows

□ Taskbar Auto Hide

Auto Hide Behavior: Intelligently

Taskbar Show Delay: 600

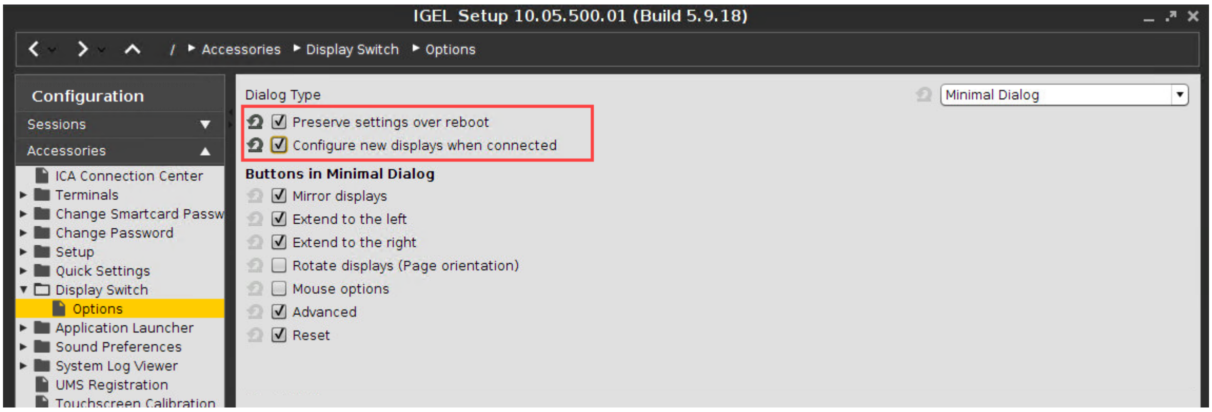
Taskbar Hide Delay: 400

> ⓘ 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 Notebooks

This how-to provides an example for configuring the automatic monitor switch for notebooks.

1. Connect the notebook and open the lid.
2. Open the Display Switch Utility.
3. Drag & drop the displays according to your intended configuration.
   The display will snap adjacent to others.
4. If a display should not be used, drag it to the **disabled** area on the top right. The screen will be reactivated when it is dragged back to the active area.
5. If the same content is to be shown on multiple displays, drag one display onto the other.
   The interface will show **mirror**. 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.
8. If you want to configure advanced settings (e. g. panning, scaling and resolutions), click the **>** button on the right side. The drop-down menus are on the right side.
9. In the Setup, go to **Accessories > Display Switch > Options.**
10. Enable **Preserve settings over reboot** and **Smart display configuration.**



IGEL Setup 10.05.500.01 (Build 5.9.18)

/ ▸ Accessories ▸ Display Switch ▸ Options

Dialog Type: Minimal Dialog

☑ Preserve settings over reboot
☑ Configure new displays when connected

Buttons in Minimal Dialog

☑ Mirror displays
☑ Extend to the left
☑ Extend to the right
☐ Rotate displays (Page orientation)
☐ Mouse options
☑ Advanced
☑ Reset

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 when the lid is closed, 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 on closing the lid while your notebook is plugged in, change the settings as follows:

1. In the Setup, go 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 on closing the lid while your notebook is not plugged in, change the settings as follows:

1. In the Setup, go to **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 to turn off the display after the lid has been closed, change the following setting to switch off the notebook internally:
> 1. In the Setup, go 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.

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:

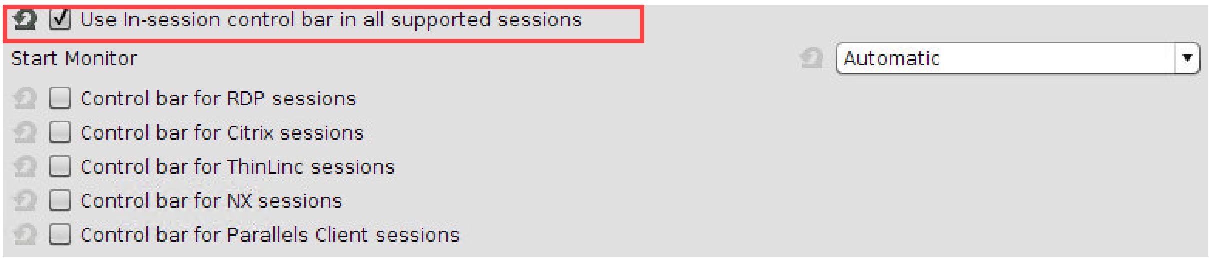
- **Accessories > On-Screen Keyboard > Autostart**
- **Accessories > On-Screen Keyboard > Restart**

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**.



☑ Use In-session control bar in all supported sessions

Start Monitor: Automatic

☐ Control bar for RDP sessions

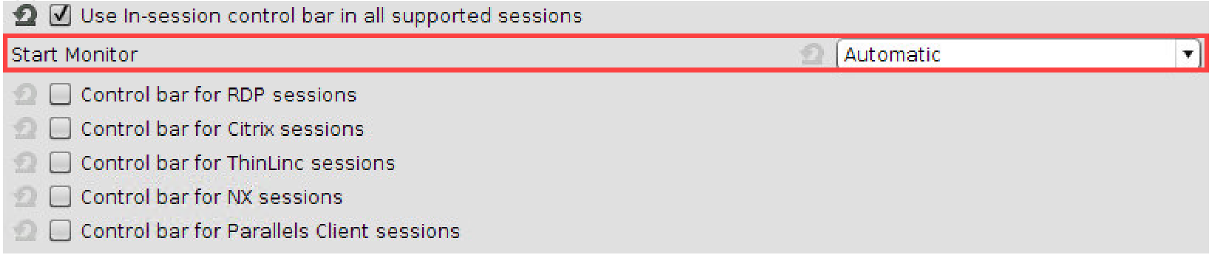
☐ Control bar for Citrix sessions

☐ Control bar for ThinLinc sessions

☐ Control bar for NX sessions

☐ Control bar for Parallels Client 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**.



☑ Use In-session control bar in all supported sessions

Start Monitor: Automatic

☐ Control bar for RDP sessions

☐ Control bar for Citrix sessions

☐ Control bar for ThinLinc sessions

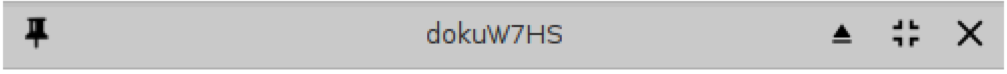
☐ Control bar for NX sessions

☐ Control bar for Parallels Client sessions

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 📌 .

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.
4. Click **Ok** to save the settings.

   ⚠ **Legal Note**

   IGEL's Terms & Conditions[46] apply.

[46] https://www.igel.com/terms-conditions/

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 and Display Switch.

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

The Custom Partition (CP) 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 contents for a Custom Partition for IGEL OS *version 10.03.100* or newer. You may also find it useful for updating existing custom partitions in order to make them work on IGEL OS *version 10.03.100* 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 license agreements and respect them.

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.

Development Environment

For this first simple Custom Partition, you only need access to a thin client or converted device with IGEL OS version *10.03.100* or newer. And you need to be `root`.

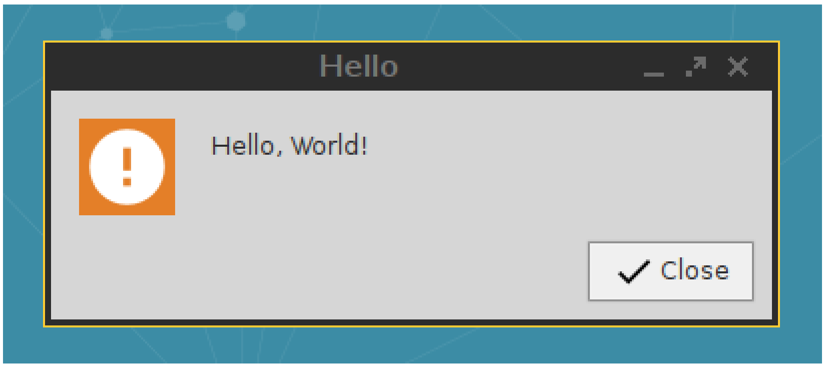
Activating the Custom Partition

By default the Custom Partition is disabled on IGEL OS. Activate it in order to start working on its contents.

1. In Setup 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 mass storage.

Custom Partition with a Shell Script

Your first CP will contain a simple shell script that displays the message "Hello, world!" with the help of the `gtkmessage` utility.



Hello

Hello, World!

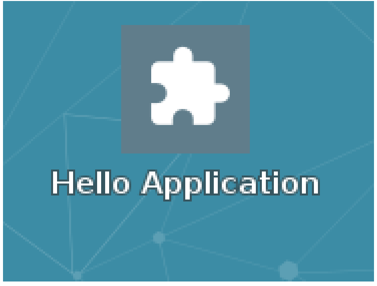
1. Log into **Local Terminal** as `root`.
2. Change into the `/custom` directory: `cd /custom`
3. Make a hello directory for your CP contents: `mkdir hello`
4. Change into the hello directory: `cd hello/`
5. Open a new plaintext file using the GNU Nano editor: `nano hello.sh`
6. Put this content into 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`
10. Run the shell script from the command line to test it: `./hello.sh`

    A message window like the one pictured above should open. You can close it with the **Close** button.

Creating a Custom Application

In the previous step you have created a little application and executed it form the command line. Now make it more convenient for end users to run it: Create a custom application and place an icon on the desktop that users can click.

1. In 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` into 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 message window should open.

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.

> ⓘ Partition Parameters are a new feature in IGEL OS *version 10.03.100* and newer.

This is how you add a Partiton Parameter to the sample CP.

Setting a Partition Parameter in Setup

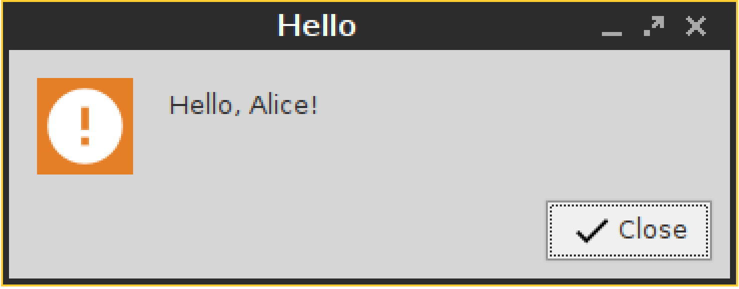
1. Go to **System > Firmware Customization > Custom Partition > Partition**.
2. In the **Partition Parameters** list, click **[+]** (Add).
3. In the dialog that opens, enter `NAME` as the **Name** and `Alice` as the **Value**. Click **OK**.
4. Click **Apply**.

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:



Hello, Alice!

Packaging a Simple Custom Partition

In the previous section, you developed Custom Partition contents locally on a thin client. Now package it in order to deploy it to many thin clients via the Universal Management Suite (UMS).

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 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 where to mount network drives in the IGEL OS Manual.

Compressing the Custom Partition Contents

The contents of a Custom Partition are packaged as a compressed `tar` file. You can easily create it on the Linux command line, e.g. on the thin client:

1. In the **Local Terminal** change in to the `/custom/` directory: `cd /custom`
2. Compress the contents of the `hello/` directory into an archive file named `hello.tar.bz2`:
   `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.

Writing the *.inf Metadata File

The compressed archive that you created in the previous step is accompanied by a plain text file with some additional information for the thin client. You can use GNU Nano on the thin client or your favorite text editor elsewhere to produce it.

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="10.03.100"
```

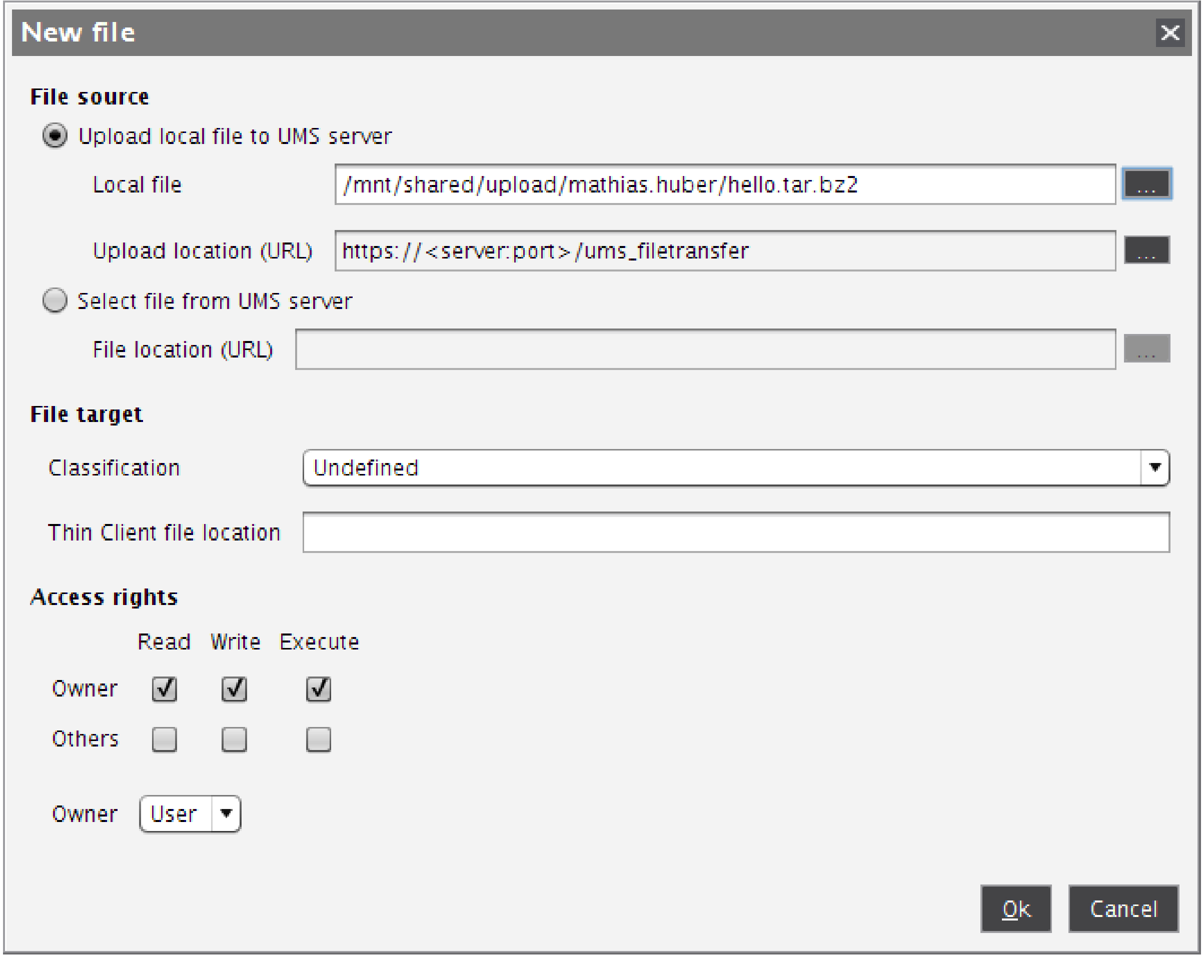
The individual entries and their meaning are:

- **[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

Uploading the Files to the UMS

Upload the compressed `hello.tar.bz2` archive and the `hello.inf` metadata file to the UMS, which will serve them to other thin clients via HTTPS.

1. In 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. Under **Upload local file to UMS server** select the `hello.tar.bz2` file with the file chooser.
3. Click **OK**.
4. Repeat the steps above for the `hello.inf` file.
   The new files show up in the **Files** folder.



New file

File source

● Upload local file to UMS server

Local file: /mnt/shared/upload/mathias.huber/hello.tar.bz2

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Thin Client file location:

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

Creating a Profile for the Custom Partition

After you have uploaded the Custom Partition files to UMS, you can now make the settings that will install the Custom Partition on a thin client. Put them into a profile that you can assign to any number of thin clients.

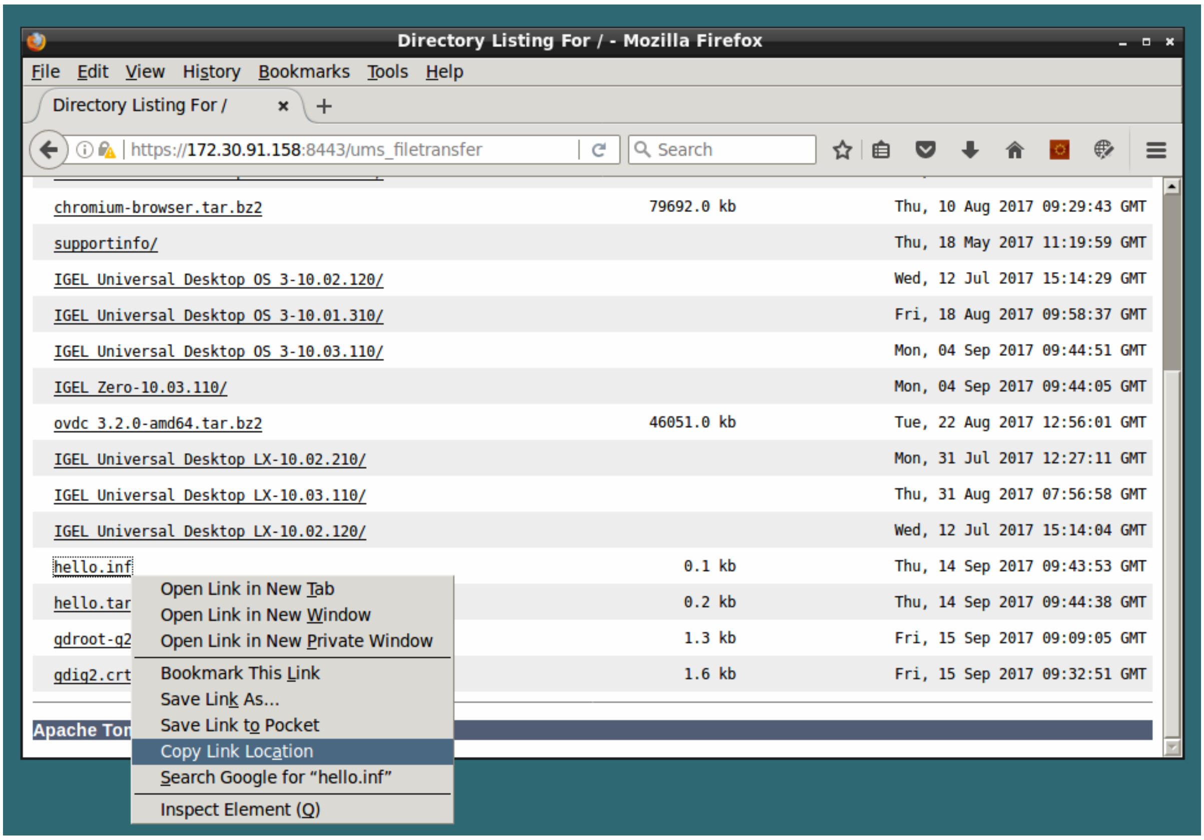
Activating the Custom Partition

1. In UMS Console right-click the **Profiles** folder and select **New Profile** from the context menu.
   The **New Profile** dialog opens.
2. Enter `Hello CP` as the **Profile Name** and `Installs the Hello Custom Partition` as the **Description**. You can leave the remaining fields.
3. Click **OK**.
   The Setup window 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`
9. Click **OK**.

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 Setup. You will find the UMS server your client is registered with there, and its IP.
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 UMS.


Directory Listing For / - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Directory Listing For /
https://172.30.91.158:8443/ums_filetransfer
Search
Open Link in New Tab
Open Link in New Window
Open Link in New Private Window
Bookmark This Link
Save Link As...
Save Link to Pocket
Copy Link Location
Search Google for "hello.inf"
Inspect Element (Q)
Apache Tom

chromium-browser.tar.bz2	79692.0 kb	Thu, 10 Aug 2017 09:29:43 GMT
supportinfo/		Thu, 18 May 2017 11:19:59 GMT
IGEL_Universal_Desktop_OS_3-10.02.120/		Wed, 12 Jul 2017 15:14:29 GMT
IGEL_Universal_Desktop_OS_3-10.01.310/		Fri, 18 Aug 2017 09:58:37 GMT
IGEL_Universal_Desktop_OS_3-10.03.110/		Mon, 04 Sep 2017 09:44:51 GMT
IGEL_Zero-10.03.110/		Mon, 04 Sep 2017 09:44:05 GMT
ovdc_3.2.0-amd64.tar.bz2	46051.0 kb	Tue, 22 Aug 2017 12:56:01 GMT
IGEL_Universal_Desktop_LX-10.02.210/		Mon, 31 Jul 2017 12:27:11 GMT
IGEL_Universal_Desktop_LX-10.03.110/		Thu, 31 Aug 2017 07:56:58 GMT
IGEL_Universal_Desktop_LX-10.02.120/		Wed, 12 Jul 2017 15:14:04 GMT
hello.inf	0.1 kb	Thu, 14 Sep 2017 09:43:53 GMT
hello.tar	0.2 kb	Thu, 14 Sep 2017 09:44:38 GMT
gdroot-g2	1.3 kb	Fri, 15 Sep 2017 09:09:05 GMT
gdig2.crt	1.6 kb	Fri, 15 Sep 2017 09:32:51 GMT

4. Right-click the `hello.inf` entry and select **Copy Link Location**.
5. In the profile's settings go to **System > Firmware Customization > Custom Partition > Download**.
6. Click [+] to add a **Partition Download Source**.
7. The **Add** dialog opens.
8. Paste the URL you copied from the browser into **URL**.
9. Enter the **User name** and **Password** for the access to your UMS.
   You can ignore the **Initializing Action** and **Finalizing 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 a Custom Application (see page 663).

Assigning the Profile

Now that you have put all the settings for installing the Custom Partition on a thin client 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 thin client.
   The **When should these changes take effect?** dialog opens.
2. Select **Now** and click **OK**.
   The thin client receives new settings.
   The **Hello Application** icon appears on the desktop.
3. In the thin client'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. Click the icon to test the application.
6. It should open, displaying a text containing the name of your choice.

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

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.[47]

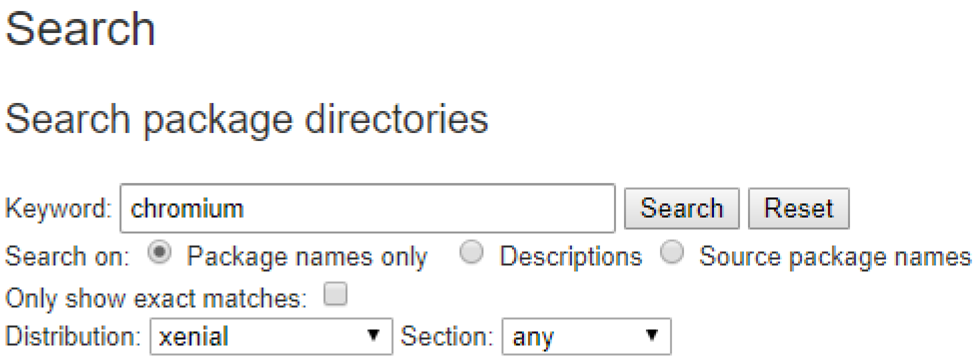
[47] http://edocs.igel.com/11105.htm

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**.



Search

Search package directories

Keyword: chromium

Search on: ● Package names only ○ Descriptions ○ Source package names

Only show exact matches: □

Distribution: xenial ▾ Section: any ▾

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:

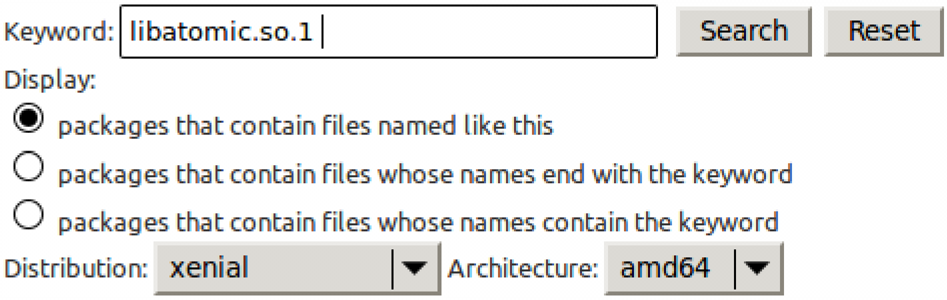
   ```
   /usr/lib/chromium-browser/chromium-browser: error while loading shared libraries:
   libatomic.so.1: cannot open shared object file: No such file or directory
   ```

   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**.



Keyword: libatomic.so.1

Display:

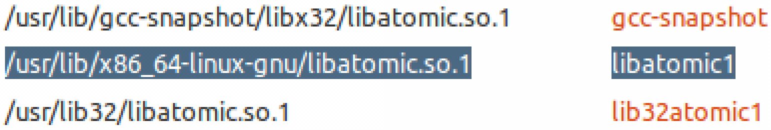
● packages that contain files named like this

○ packages that contain files whose names end with the keyword

○ packages that contain files whose names contain the keyword

Distribution: xenial Architecture: amd64

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.

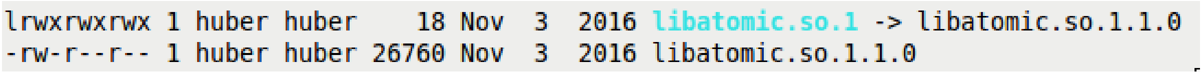


/usr/lib/gcc-snapshot/libx32/libatomic.so.1	gcc-snapshot
/usr/lib/x86_64-linux-gnu/libatomic.so.1	libatomic1
/usr/lib32/libatomic.so.1	lib32atomic1

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

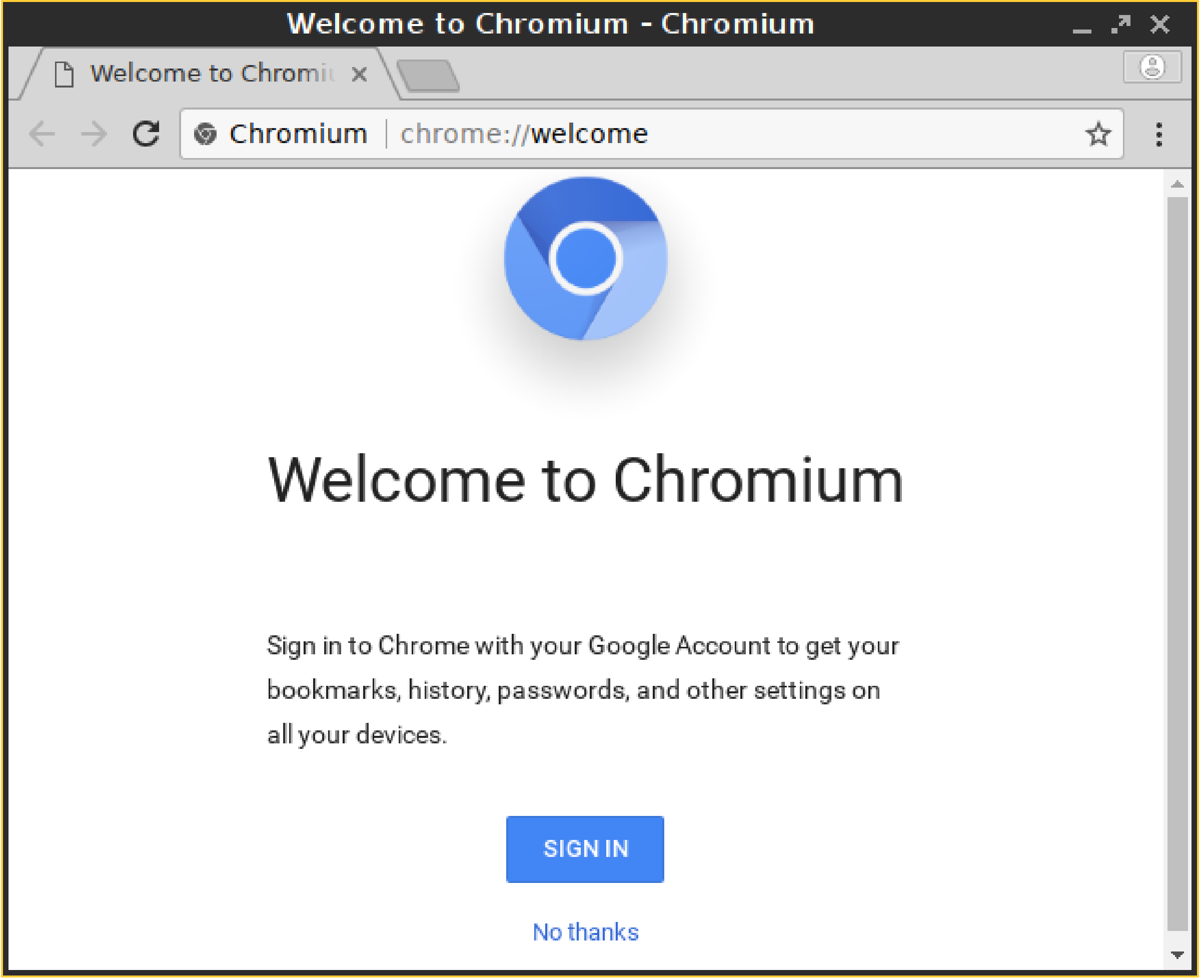
To obtain Libffmpeg, repeat the process for obtaining Libatomic (see page 681). Hint: The Ubuntu package is named `chromium-codecs-ffmpeg`. It contains the file `libffmpeg.so`, which you need to transfer to the thin client. Place it in `/custom/chromium-browser/usr/lib/chromium-browser/.`

ⓘ 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.
   

   Welcome to Chromium

   Sign in to Chrome with your Google Account to get your bookmarks, history, passwords, and other settings on all your devices.

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 667) into `chromium-browser.tar.bz2`
2. Upload the compressed file to UMS as a new **File**.
3. Write the *.inf Metadata File (see page 668) 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 670) 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 663) 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.

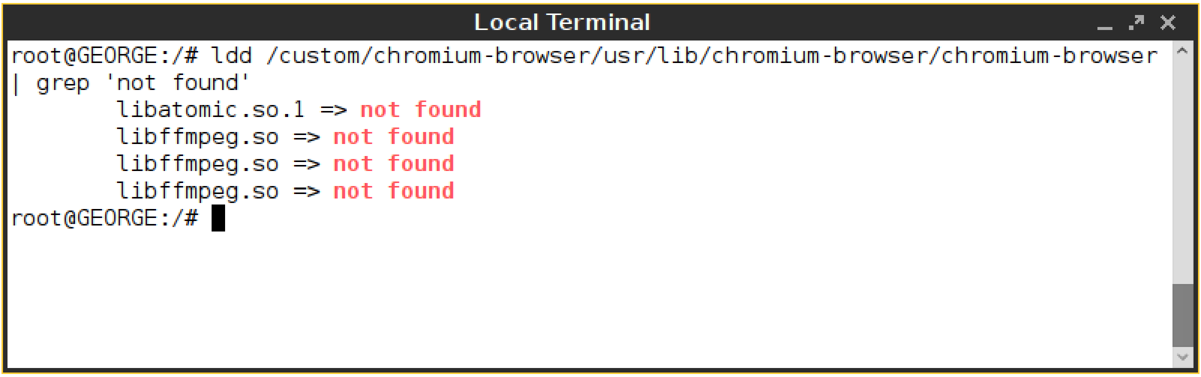
Advanced

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.



```
root@GEORGE:/# ldd /custom/chromium-browser/usr/lib/chromium-browser/chromium-browser
| grep 'not found'
        libatomic.so.1 => not found
        libffmpeg.so => not found
        libffmpeg.so => not found
        libffmpeg.so => not found
root@GEORGE:/# 
```

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 689)
2. Getting the Packages (see page 690)
3. Unpacking the Packages (see page 691)
4. Creating the Initialization Script (see page 692)
5. Compressing the Custom Partition Contents (see page 695)
6. Writing the *.inf Metadata File (see page 696)
7. Uploading the Files to the UMS (see page 697)
8. Creating a Profile for the Custom Partition (see page 700)
9. Assigning the Profile and Testing the Application (see page 707)

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.

Next Step

>> Getting the Packages (see page 690)

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 691)

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 692)

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 (see page 695)

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 (see page 696)

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 668).

Next Step

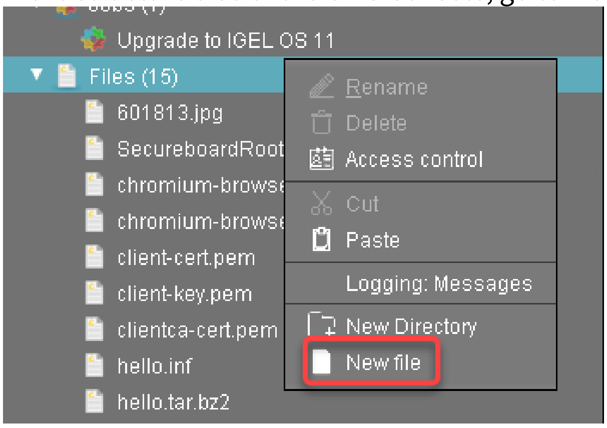
>> Uploading the Files to the UMS (see page 697)

Uploading the Files to the UMS

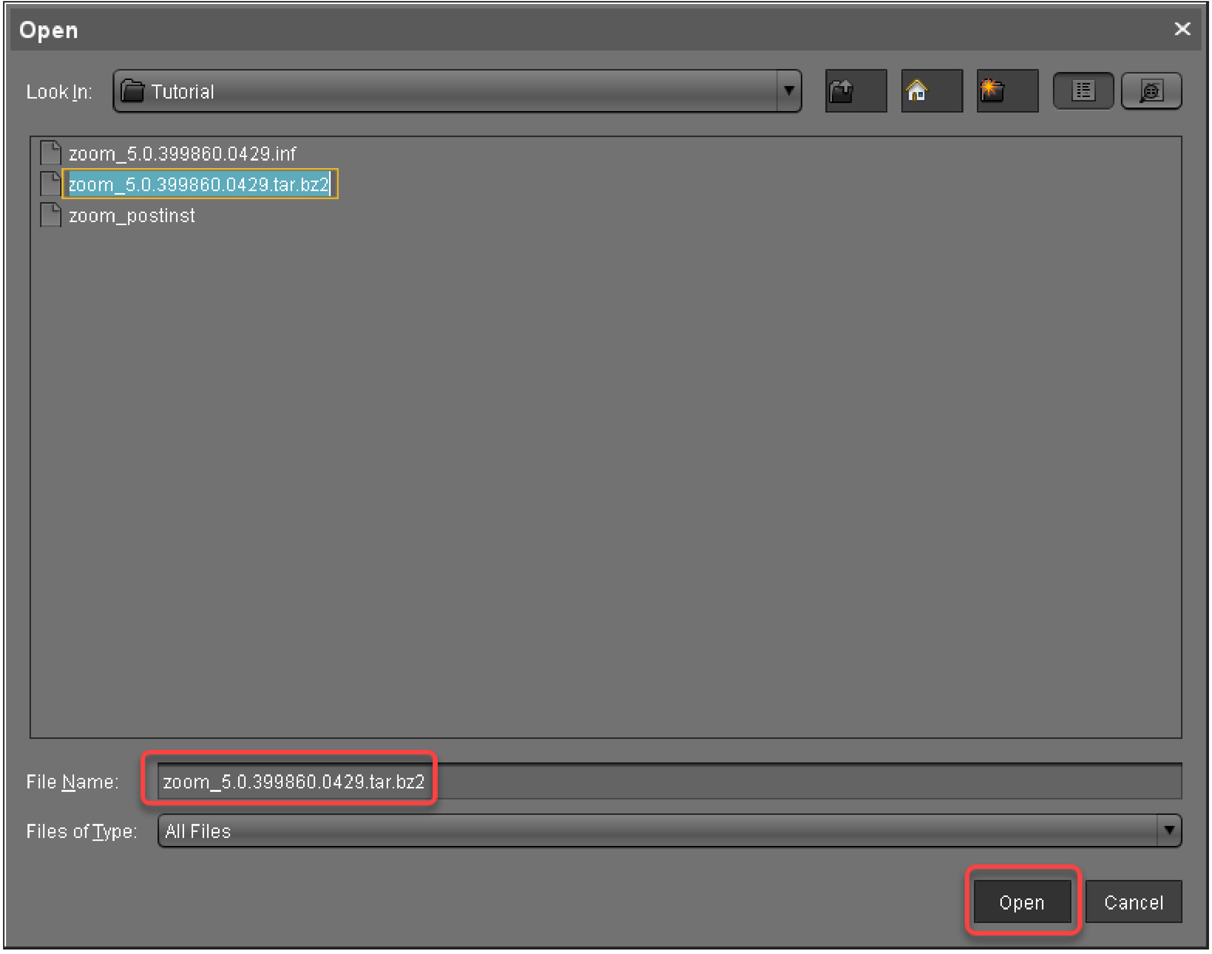
In this step, you upload the compressed `zoom_[version].tar.bz2` archive and the `zoom_[version].inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

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.

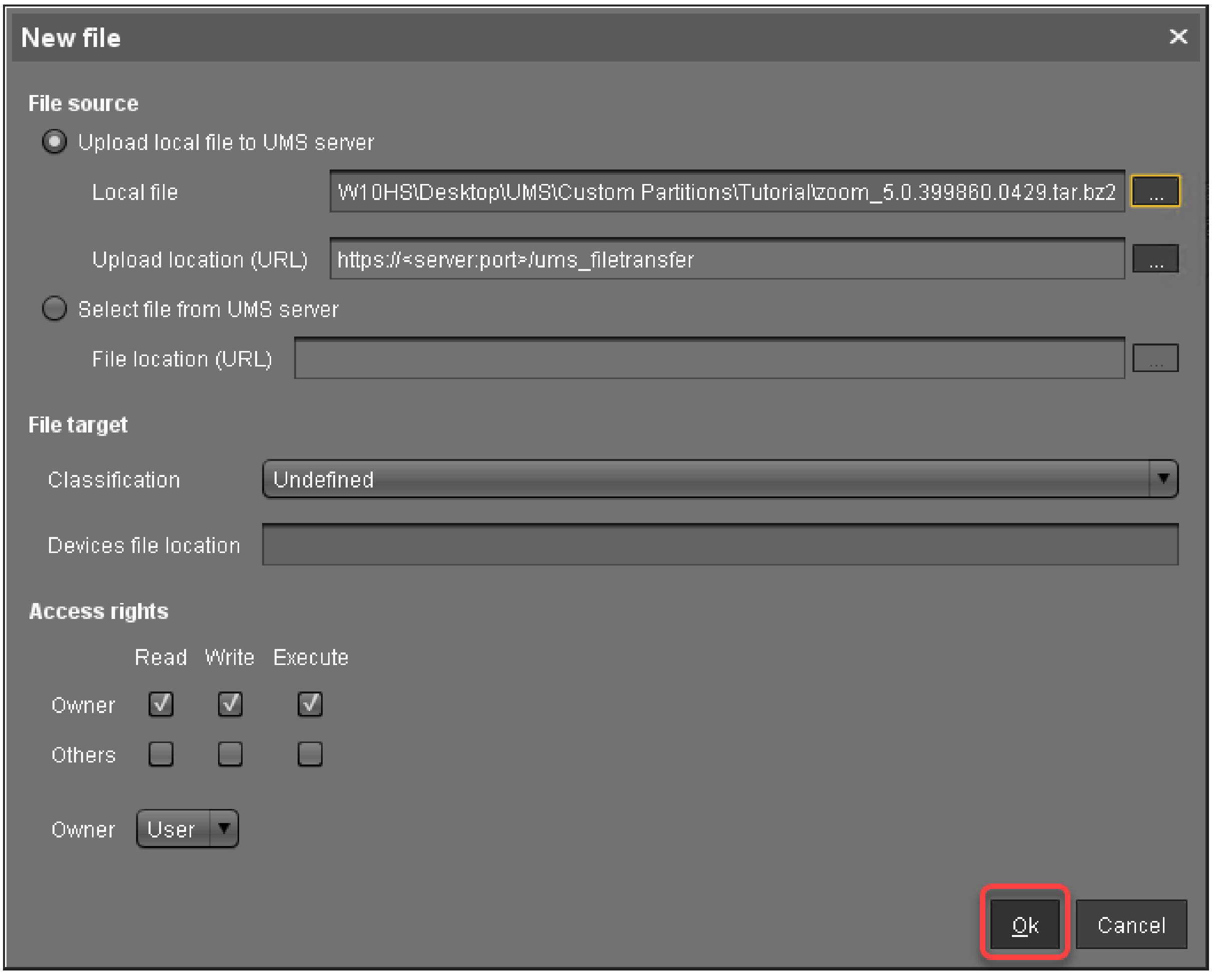


3. Click ... next to the **Local file** field, select `zoom_[version].tar.bz2` on your local machine, and click **Open**.



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**.



New file

File source

● Upload local file to UMS server

Local file: W10HS\Desktop\UMS\Custom Partitions\Tutorial\zoom_5.0.399860.0429.tar.bz2

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location:

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

6. Repeat steps 1 to 5 for `zoom_[version].inf`

Next Step

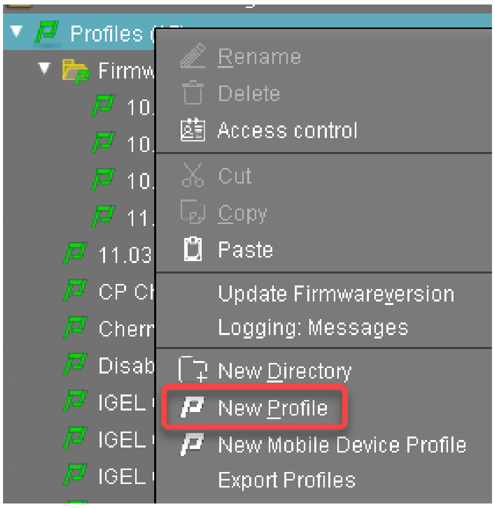
>> Creating a Profile for the Custom Partition (see page 700)

Creating a Profile for the Custom Partition

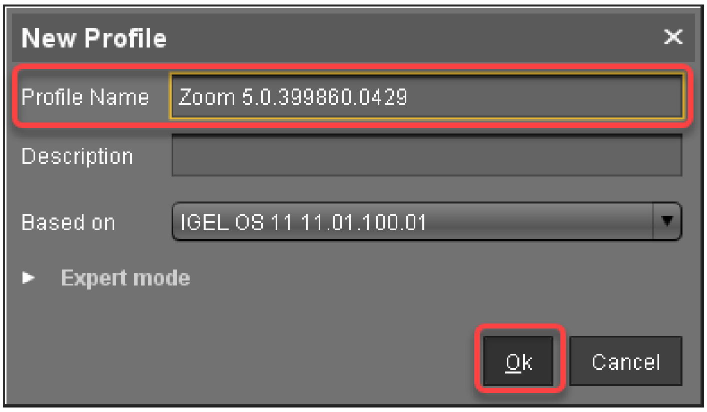
After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, you create a profile.

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**.


New Profile

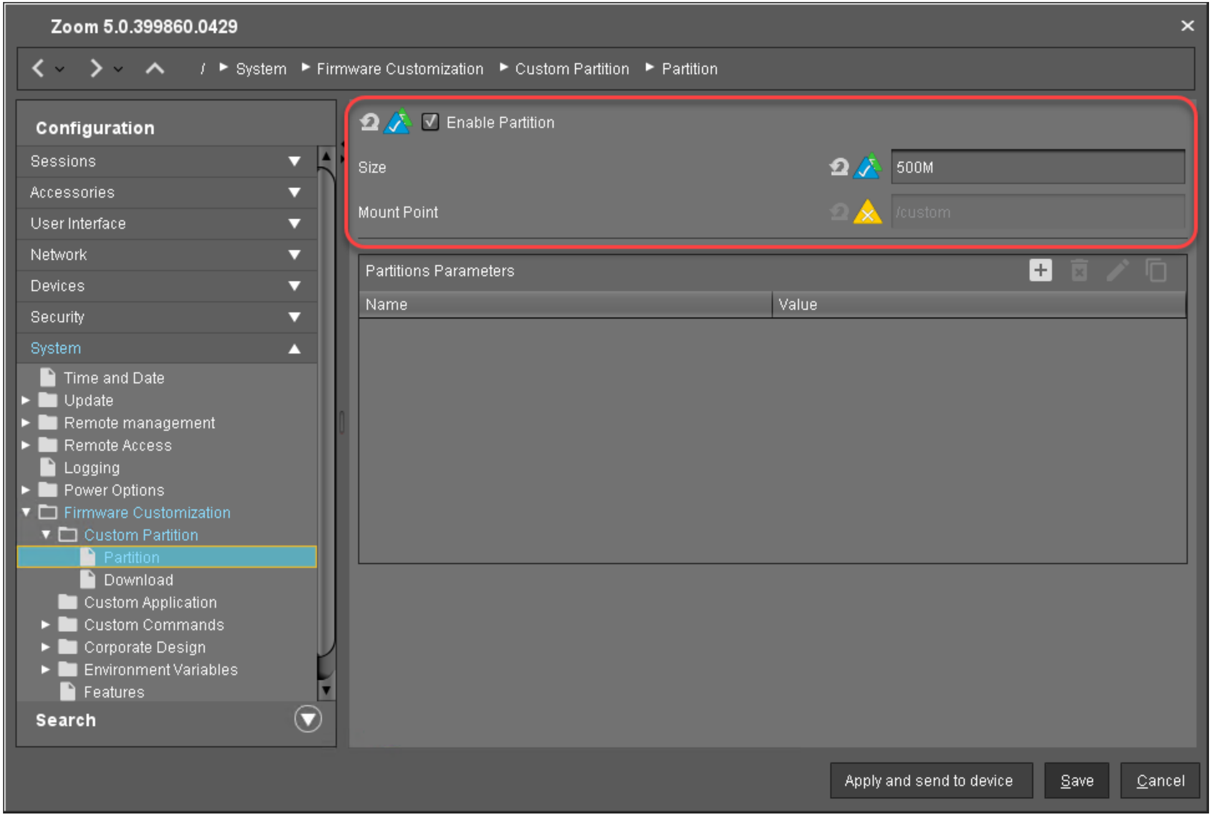
Profile Name: Zoom 5.0.399860.0429

Description:

Based on: IGEL OS 11 11.01.100.01

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".



☑ Enable Partition

Size: 500M

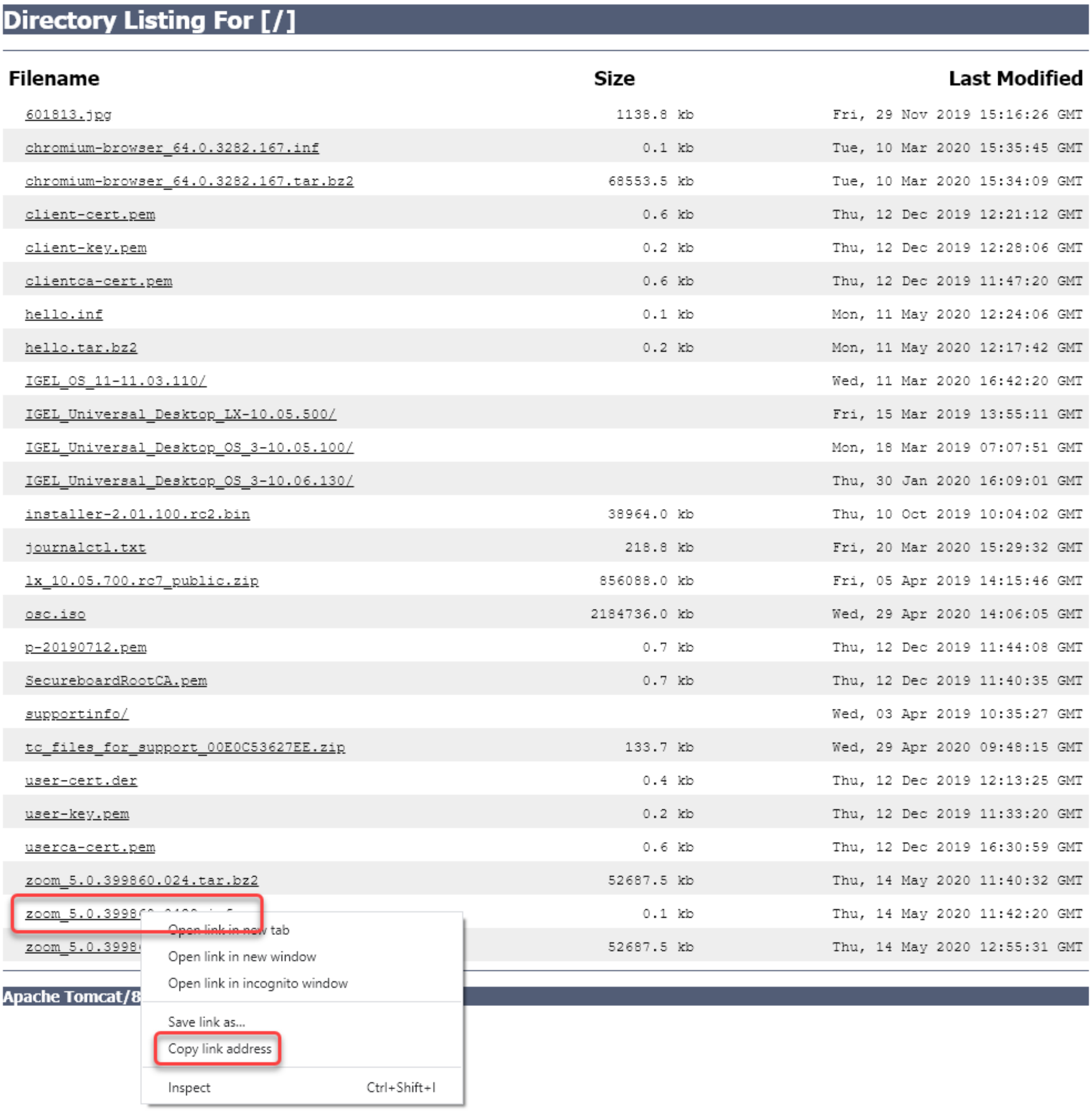
Mount Point: /custom

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).



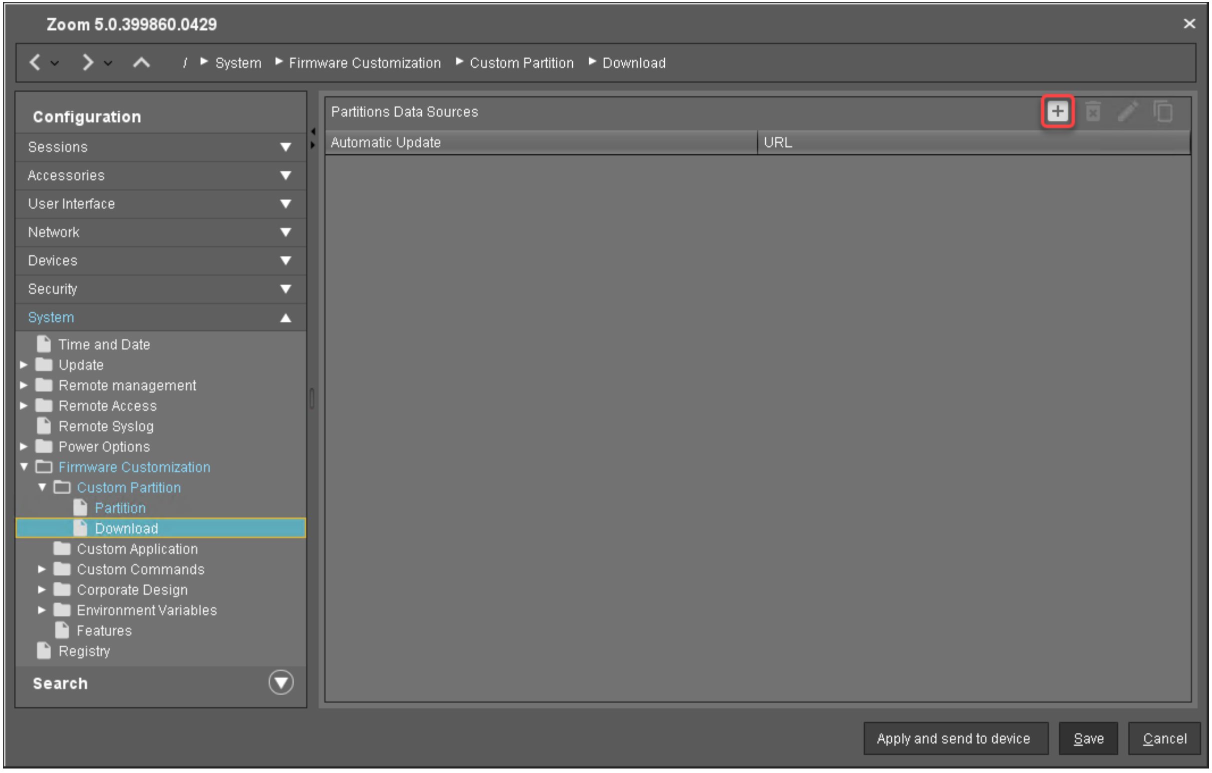
Directory Listing For [/]

Filename	Size	Last Modified
601813.jpg	1138.8 kb	Fri, 29 Nov 2019 15:16:26 GMT
chromium-browser_64.0.3282.167.inf	0.1 kb	Tue, 10 Mar 2020 15:35:45 GMT
chromium-browser_64.0.3282.167.tar.bz2	68553.5 kb	Tue, 10 Mar 2020 15:34:09 GMT
client-cert.pem	0.6 kb	Thu, 12 Dec 2019 12:21:12 GMT
client-key.pem	0.2 kb	Thu, 12 Dec 2019 12:28:06 GMT
clientca-cert.pem	0.6 kb	Thu, 12 Dec 2019 11:47:20 GMT
hello.inf	0.1 kb	Mon, 11 May 2020 12:24:06 GMT
hello.tar.bz2	0.2 kb	Mon, 11 May 2020 12:17:42 GMT
IGEL_OS_11-11.03.110/		Wed, 11 Mar 2020 16:42:20 GMT
IGEL_Universal_Desktop_LX-10.05.500/		Fri, 15 Mar 2019 13:55:11 GMT
IGEL_Universal_Desktop_OS_3-10.05.100/		Mon, 18 Mar 2019 07:07:51 GMT
IGEL_Universal_Desktop_OS_3-10.06.130/		Thu, 30 Jan 2020 16:09:01 GMT
installer-2.01.100.rc2.bin	38964.0 kb	Thu, 10 Oct 2019 10:04:02 GMT
journalctl.txt	218.8 kb	Fri, 20 Mar 2020 15:29:32 GMT
lx_10.05.700.rc7_public.zip	856088.0 kb	Fri, 05 Apr 2019 14:15:46 GMT
osc.iso	2184736.0 kb	Wed, 29 Apr 2020 14:06:05 GMT
p-20190712.pem	0.7 kb	Thu, 12 Dec 2019 11:44:08 GMT
SecureboardRootCA.pem	0.7 kb	Thu, 12 Dec 2019 11:40:35 GMT
supportinfo/		Wed, 03 Apr 2019 10:35:27 GMT
tc_files_for_support_00E0C53627EE.zip	133.7 kb	Wed, 29 Apr 2020 09:48:15 GMT
user-cert.der	0.4 kb	Thu, 12 Dec 2019 12:13:25 GMT
user-key.pem	0.2 kb	Thu, 12 Dec 2019 11:33:20 GMT
userca-cert.pem	0.6 kb	Thu, 12 Dec 2019 16:30:59 GMT
zoom_5.0.399860.024.tar.bz2	52687.5 kb	Thu, 14 May 2020 11:40:32 GMT
zoom_5.0.3998	0.1 kb	Thu, 14 May 2020 11:42:20 GMT
zoom_5.0.3998	52687.5 kb	Thu, 14 May 2020 12:55:31 GMT

Apache Tomcat/8

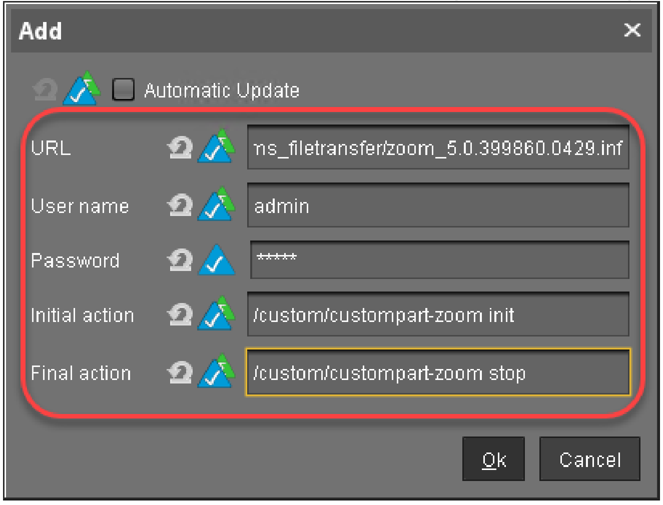
5. Back in the profile, go to **System > Firmware Customization > Custom Partition > Download**.

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".



Add

□ Automatic Update

URL: ms_filetransfer/zoom_5.0.399860.0429.inf

User name: admin

Password: *****

Initial action: /custom/custompart-zoom init

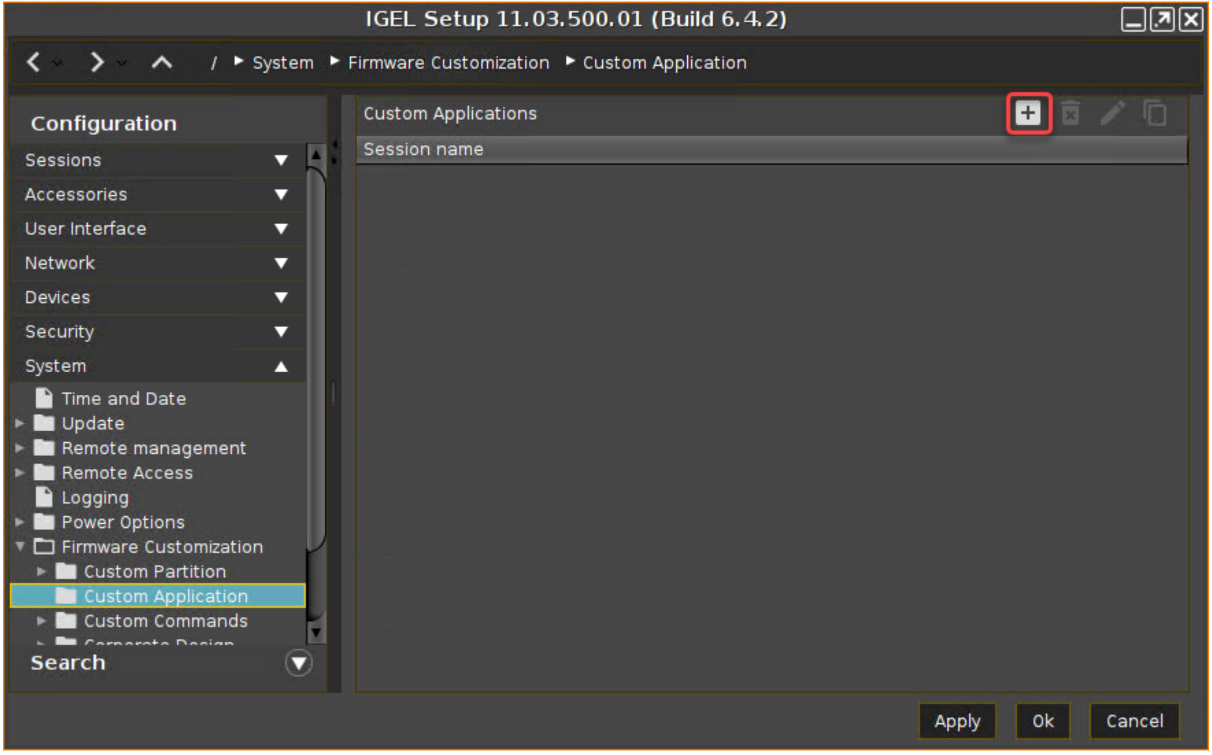
Final action: /custom/custompart-zoom stop

8. Click **OK**.

Configuring the Custom Application

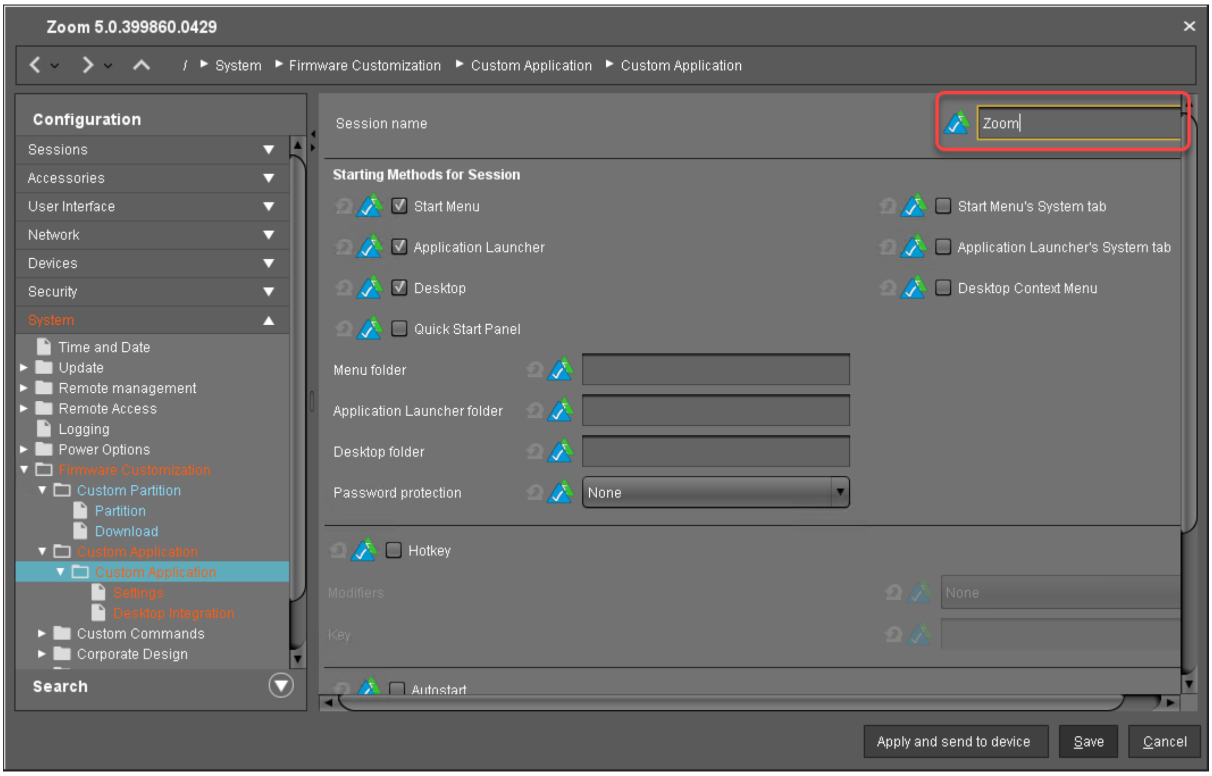
To create a convenient starting method for the user, create a custom application that includes a starter icon on the desktop.

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**.



Zoom 5.0.399860.0429

Session name: Zoom

Starting Methods for Session

☑ Start Menu
☐ Start Menu's System tab
☑ Application Launcher
☐ Application Launcher's System tab
☑ Desktop
☐ Desktop Context Menu
☐ Quick Start Panel

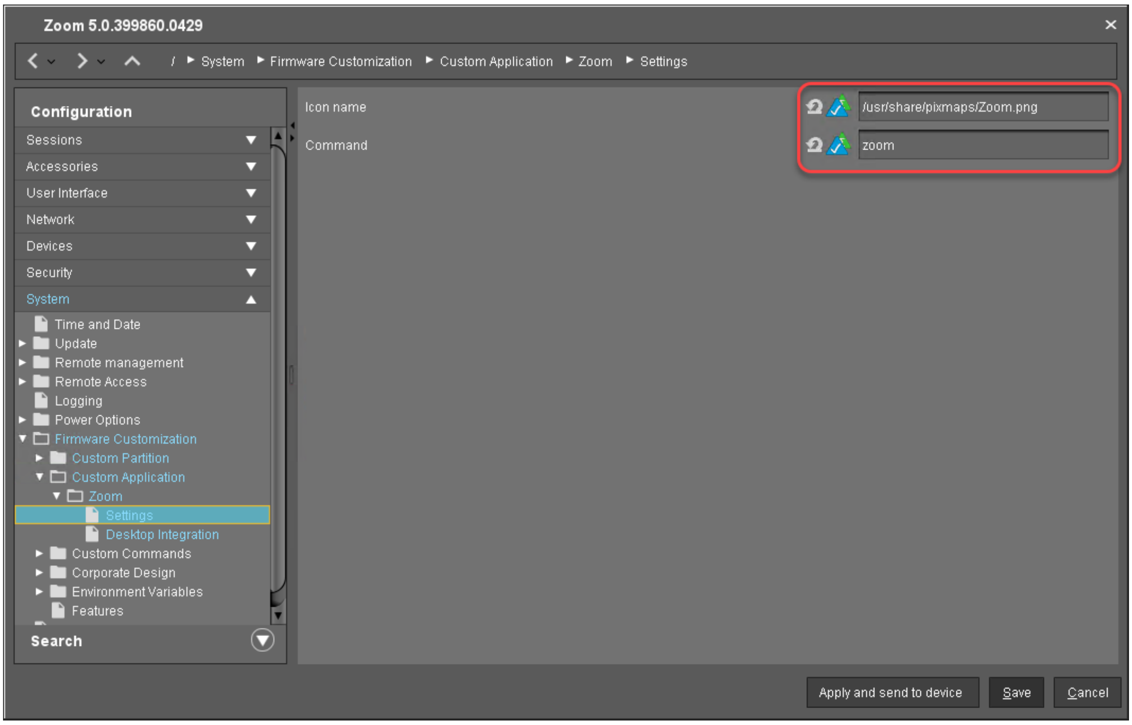
Menu folder:
Application Launcher folder:
Desktop folder:
Password protection: None

☐ Hotkey
Modifiers: None
Key:

☐ Autostart

4. Go to **Settings**.
5. Edit the settings as follows:
   - **Icon name**: Enter "/usr/share/pixmaps/Zoom.png".

- **Command**: Enter "zoom".



Zoom 5.0.399860.0429

/ ▸ System ▸ Firmware Customization ▸ Custom Application ▸ Zoom ▸ Settings

Icon name: /usr/share/pixmaps/Zoom.png

Command: zoom

6. Click **Save**.

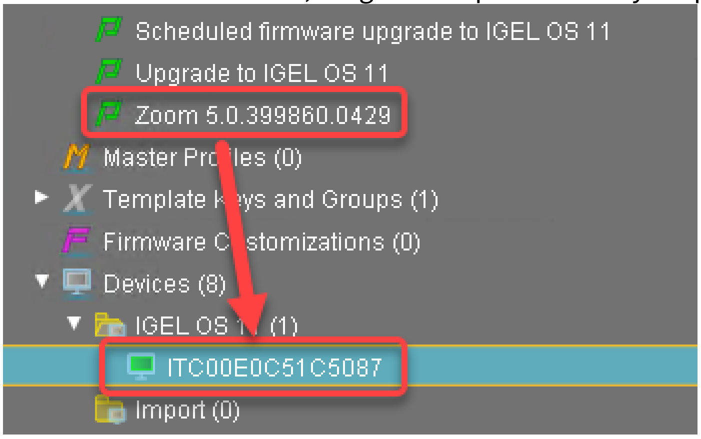
Next Step

>> Assigning the Profile and Testing the Application (see page 707)

Assigning the Profile and Testing the Application

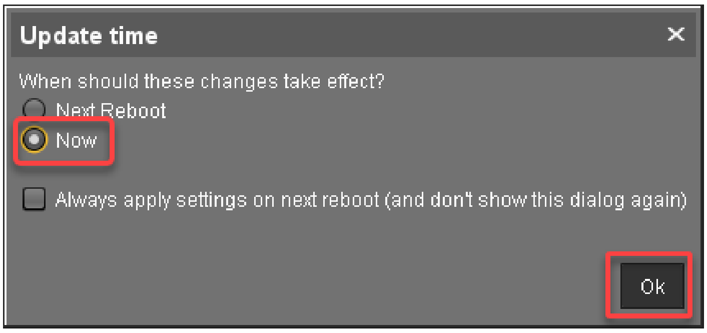
Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

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**.


Update time
When should these changes take effect?
○ Next Reboot
● Now
□ Always apply settings on next reboot (and don't show this dialog again)
Ok

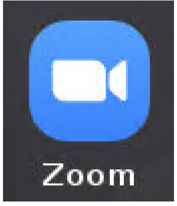
The device receives the settings of the profile, creates the Custom Partition, downloads the contents of the Custom Partition, and uncompresses them.

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.

Microsoft Teams 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: Microsoft Teams.

If you want to get an impression of how Microsoft Teams works on IGEL OS, watch this video:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://m.youtube.com/watch?v=3X0IKKu5eZY

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

1. Development Environment (see page 710)
2. Getting the Package (see page 711)
3. Unpacking the Packages (see page 712)
4. Creating the Initialization Script (see page 713)
5. Compressing the Custom Partition Contents+1 (see page 715)
6. Writing the *.inf Metadata File 1 (see page 716)
7. Uploading the Files to the UMS (see page 717)
8. Creating a Profile for the Custom Partition (see page 720)
9. Assigning the Profile and Testing the Application (see page 726)

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.

Next Step

>> Getting the Package (see page 711)

Getting the Package

Get the required package for Ubuntu.

1. Open https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/download-app#allDevicesSection in a browser and click **Linux DEB (64-bit)**.

   > ⓘ When you open the URL from a Windows machine, the Linux download button will probably not appear.

2. Download the package `teams_[version]_amd64.deb` (example: `teams_1.3.00.5153_amd64.deb`)
3. Change to the download directory on your workstation (typically `/home/[username]/Downloads`).

Next Step

>> Unpacking the Package (see page 712)

Unpacking the Packages

In this step, you extract the 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 teams
   ```
4. Extract the packages to the new directory:
   ```
   dpkg -x teams*.deb teams/
   ```
5. Run the following command to see how much space the package contents need in total (in MB):
   ```
   du -cms teams/*
   ```
   The total is 237 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 713)

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 Teams application would be located in `/usr`, whereas in the Custom Partition, they are located under `/custom/teams/usr`. The initialization script will fix this by creating symbolic links so that for example `/custom/teams/usr/share/libffmpeg.so` will appear to be in `/usr/share/libffmpeg.so`, where Teams expects it.

1. On your workstation, go to the directory where the `teams` directory is located.
2. Open your text editor of choice and enter the following script:

```
#!/bin/sh

ACTION="custompart-teams_${1}"

# mount point path
MP=$(get custom_partition.mountpoint)

# custom partition path
CP="${MP}/teams"

# only needed if application has an executable
BIN="/usr/bin/teams"

# 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
;;
stop)
```

```
        # unlink linked files
        find ${CP} | while read LINE
            do
                DEST=$(echo -n "${LINE}" | sed -e "s|${CP}||g")
            unlink $DEST | $LOGGER
        done
;;
esac

echo "Finished" | $LOGGER

exit 0
```

3. Save the file as `custompart-teams`

Next Step

>> Compressing the Custom Partition Contents (see page 715)

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 `teams/` directory with the application files and the initialization script `custompart-teams`
2. Make the files in `teams/` and the initialization script executable:

   ```
   chmod -R +x teams
   chmod +x custompart-teams
   ```

3. Compress the `teams/` directory and the initialization script into an archive file named `teams_[version].tar.bz2` (in our example: `teams_1.3.00.5153.tar.bz2`):

   ```
   tar cjvf teams_1.3.00.5153.tar.bz2 teams custompart-teams
   ```

Next Step

>> Writing the *.inf Metadata File (see page 716)

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 `teams.inf` file.

1. Change to the directory that contains the compressed contents of our Custom Partition.
2. Create a new file named `teams.inf` and put the following into it:

```
[INFO]
[PART]
file="teams_1.3.00.5153.tar.bz2"
version="1.3.00.5153_igel1"
size="500M"
name="teams"
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 668).

Next Step

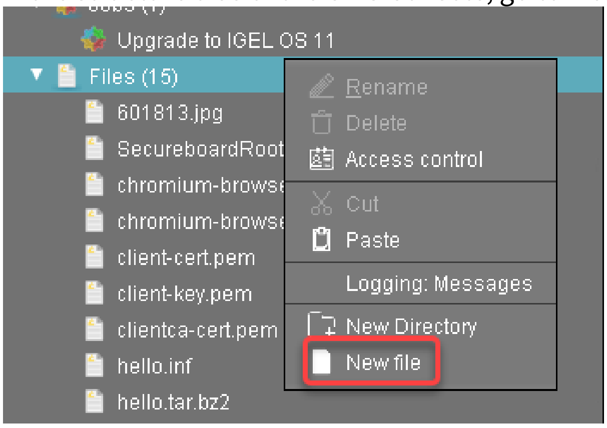
>> Uploading the Files to the UMS (see page 717)

Uploading the Files to the UMS

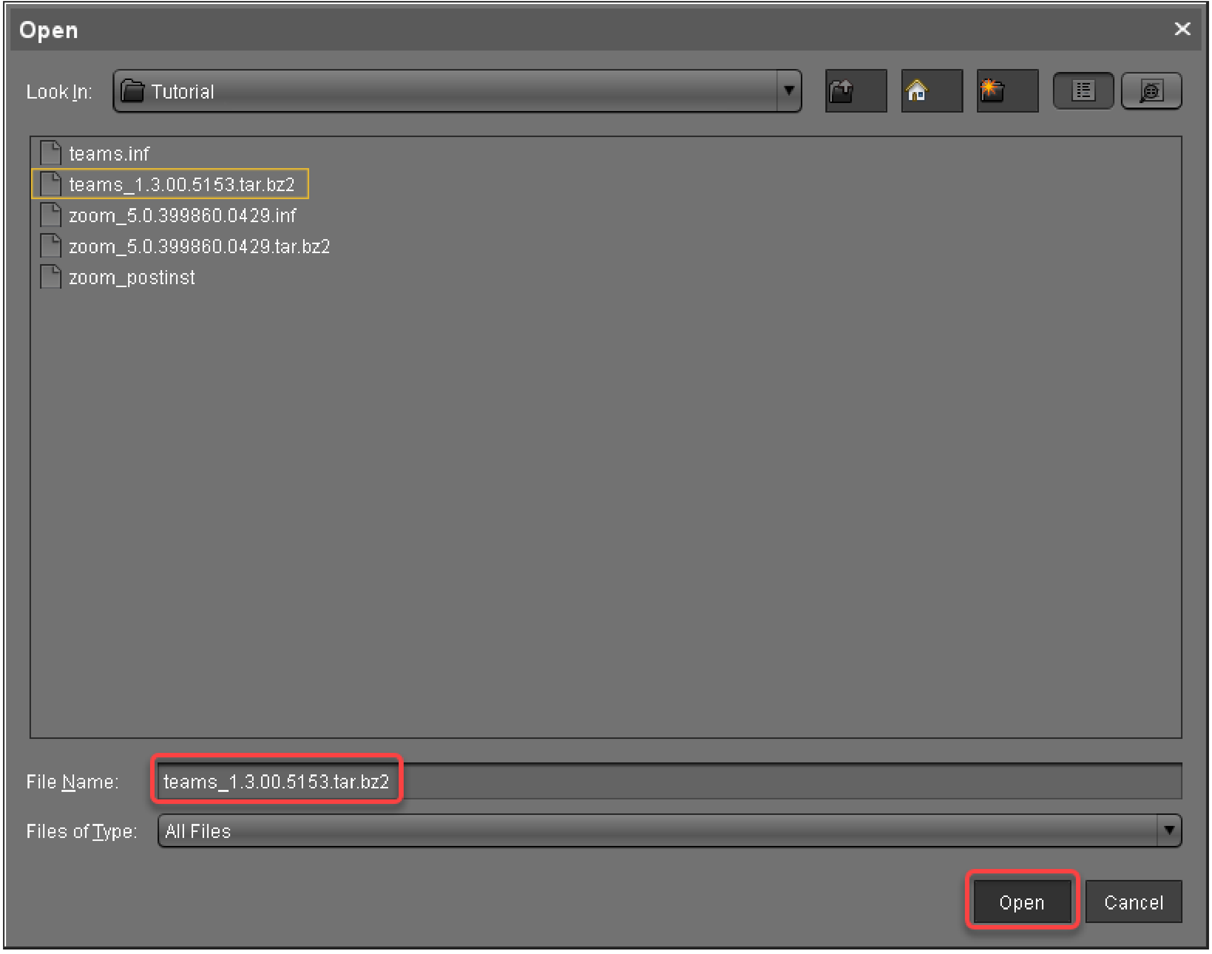
In this step, you upload the compressed `teams_[version].tar.bz2` archive and the `teams_[version] .inf` metadata file to the UMS, which will serve them to other devices via HTTPS. To make the file available, you have to create a file object after transferring the physical file.

Transferring the Files to the UMS

1. Make sure that the Teams 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.



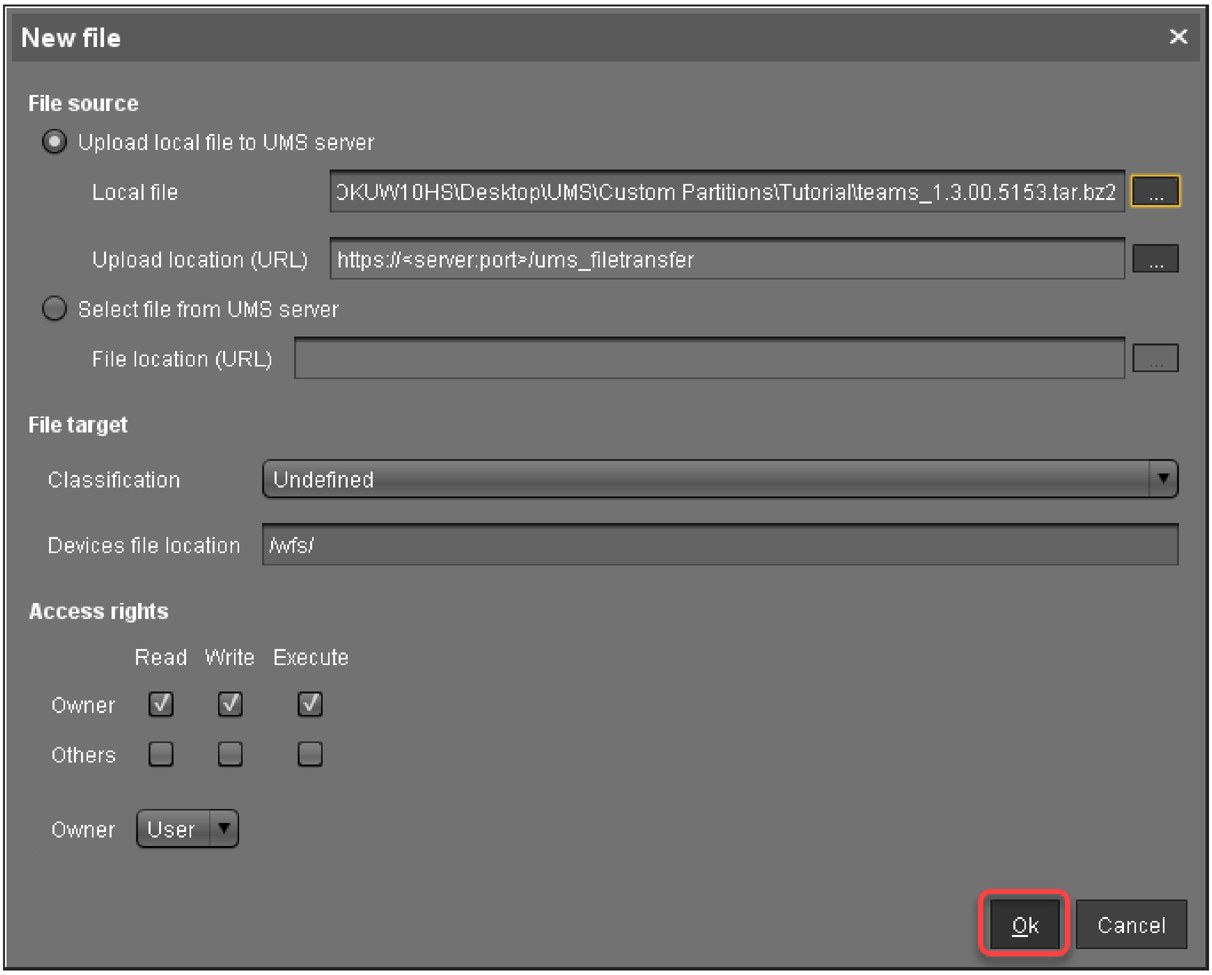
3. Click ... next to the **Local file** field, select `teams_[version].tar.bz2` on your local machine, and click **Open**.



File Name: teams_1.3.00.5153.tar.bz2

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**.



New file

File source

● Upload local file to UMS server

Local file: ƆKUW10HS\Desktop\UMS\Custom Partitions\Tutorial\teams_1.3.00.5153.tar.bz2

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: User

6. Repeat steps 1 to 5 for `teams_[version].inf`

Next Step

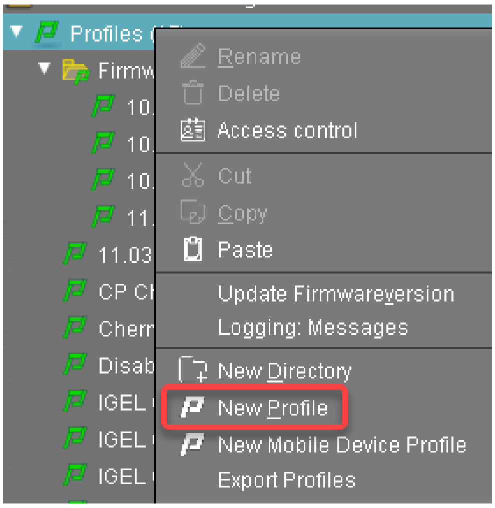
>> Creating a Profile for the Custom Partition (see page 720)

Creating a Profile for the Custom Partition

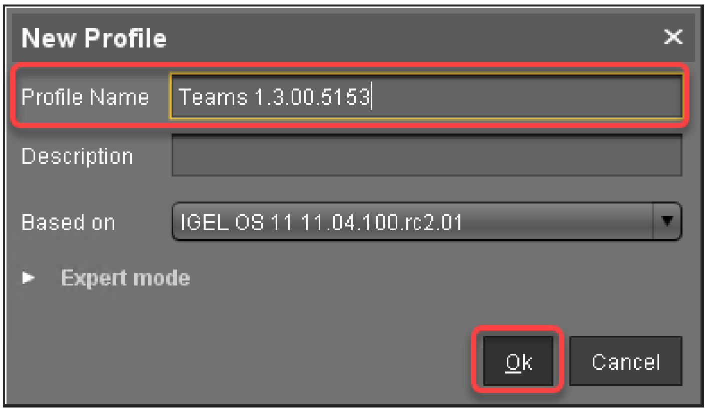
After you have uploaded the Custom Partition files to the UMS, you can now make the settings that will install the Custom Partition on any number of devices. For this purpose, you create a profile.

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. "Teams" followed by the version name, and click **Ok**.


New Profile

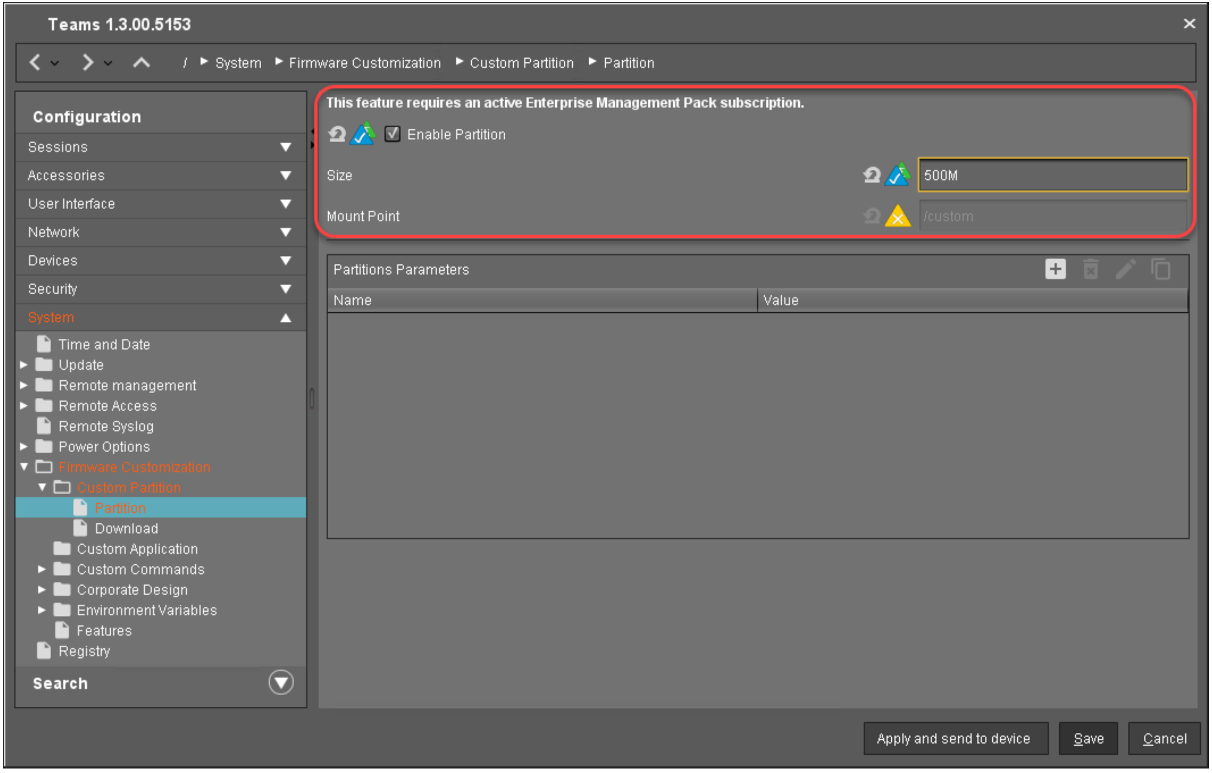
Profile Name: Teams 1.3.00.5153

Description:

Based on: IGEL OS 11 11.04.100.rc2.01

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".



This feature requires an active Enterprise Management Pack subscription.

☑ Enable Partition

Size: 500M

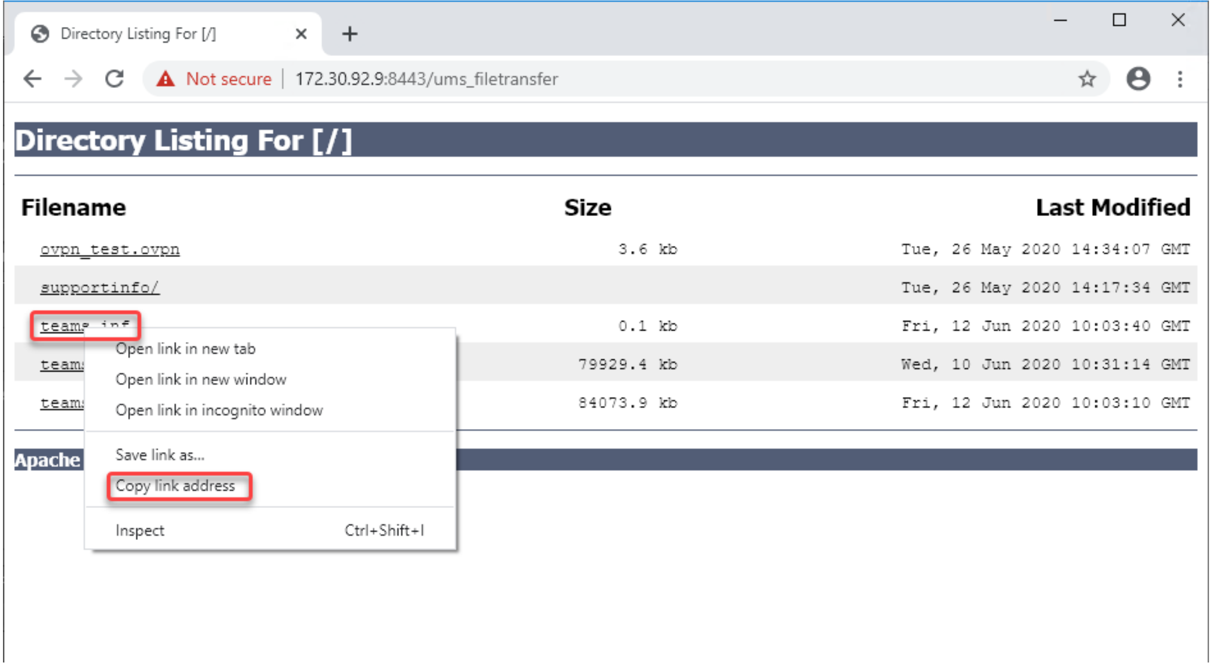
Mount Point: /custom

Setting the Download Source

For this step, you need to determine the HTTPS download address for the `teams.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.

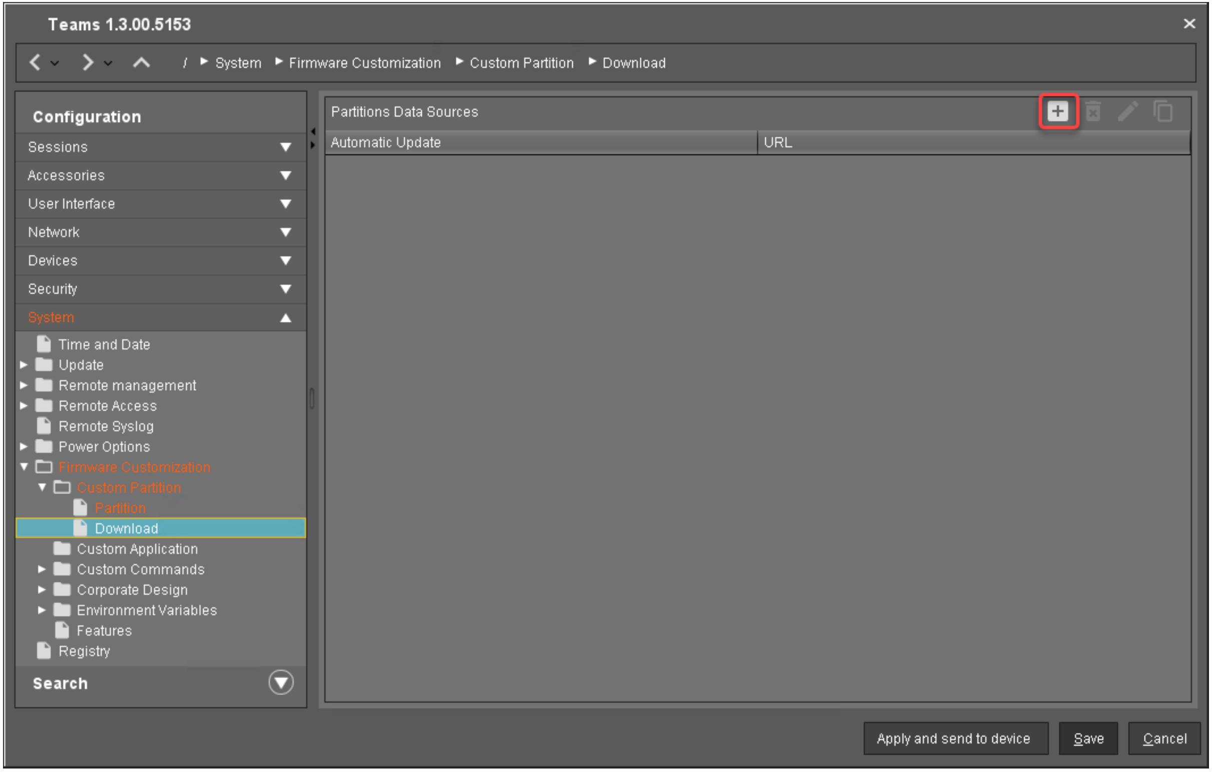
4. Right-click the **teams_[version].inf** entry and select **Copy link address** (or the like, depending on your browser).



Directory Listing For [/]

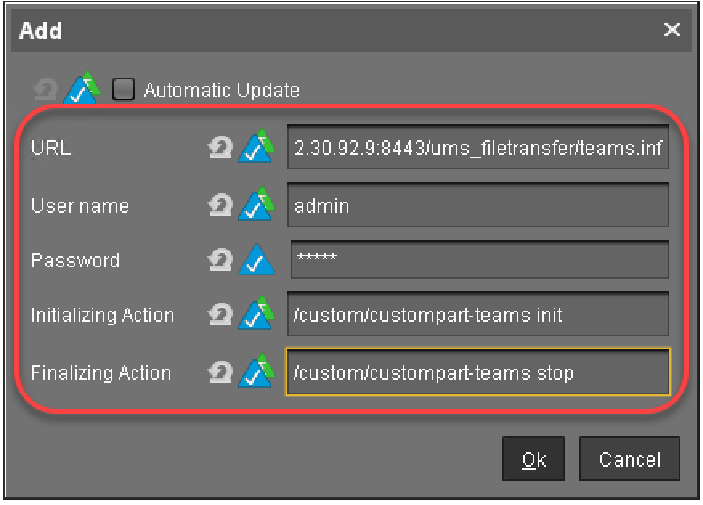
Filename	Size	Last Modified
ovpn_test.ovpn	3.6 kb	Tue, 26 May 2020 14:34:07 GMT
supportinfo/		Tue, 26 May 2020 14:17:34 GMT
teams_inf	0.1 kb	Fri, 12 Jun 2020 10:03:40 GMT
team	79929.4 kb	Wed, 10 Jun 2020 10:31:14 GMT
team	84073.9 kb	Fri, 12 Jun 2020 10:03:10 GMT

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
   - **Initializing action**: Enter "/custom/custompart-teams init".
   - **Finalizing action**: Enter "/custom/custompart-teams stop".



☐ Automatic Update

URL: 2.30.92.9:8443/ums_filetransfer/teams.inf

User name: admin

Password: *****

Initializing Action: /custom/custompart-teams init

Finalizing Action: /custom/custompart-teams stop

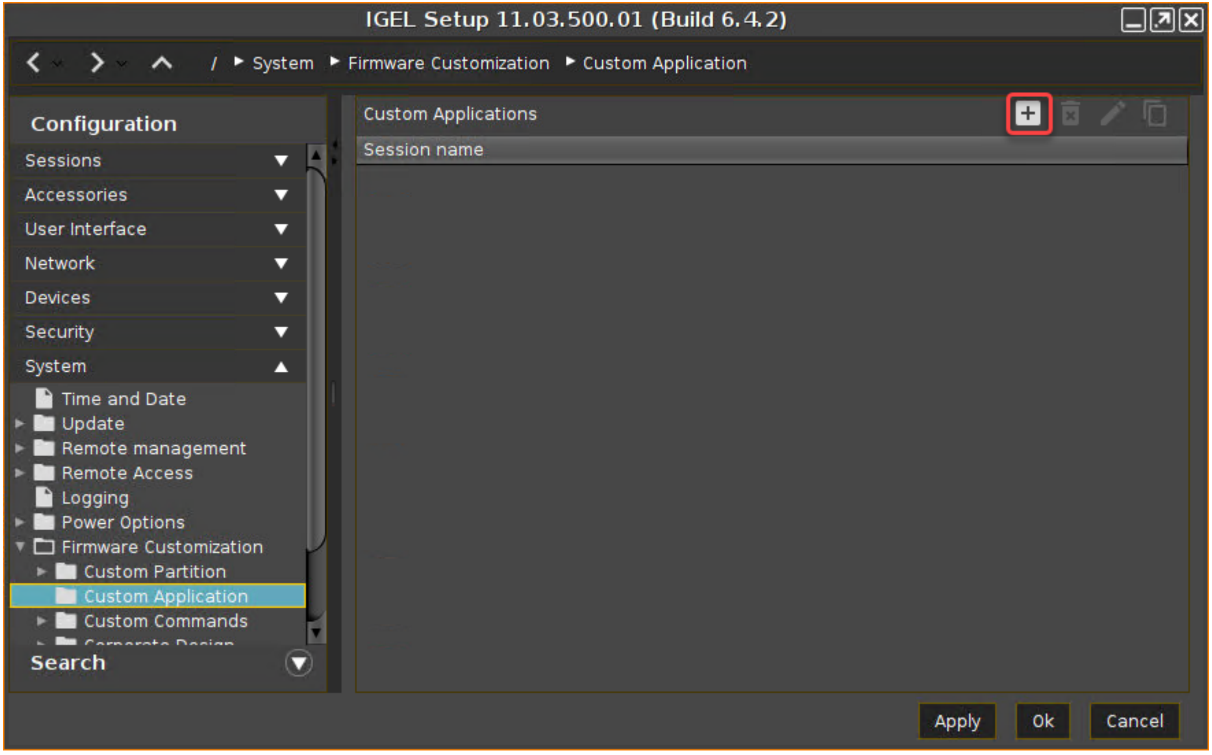
8. Click **OK**.

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.

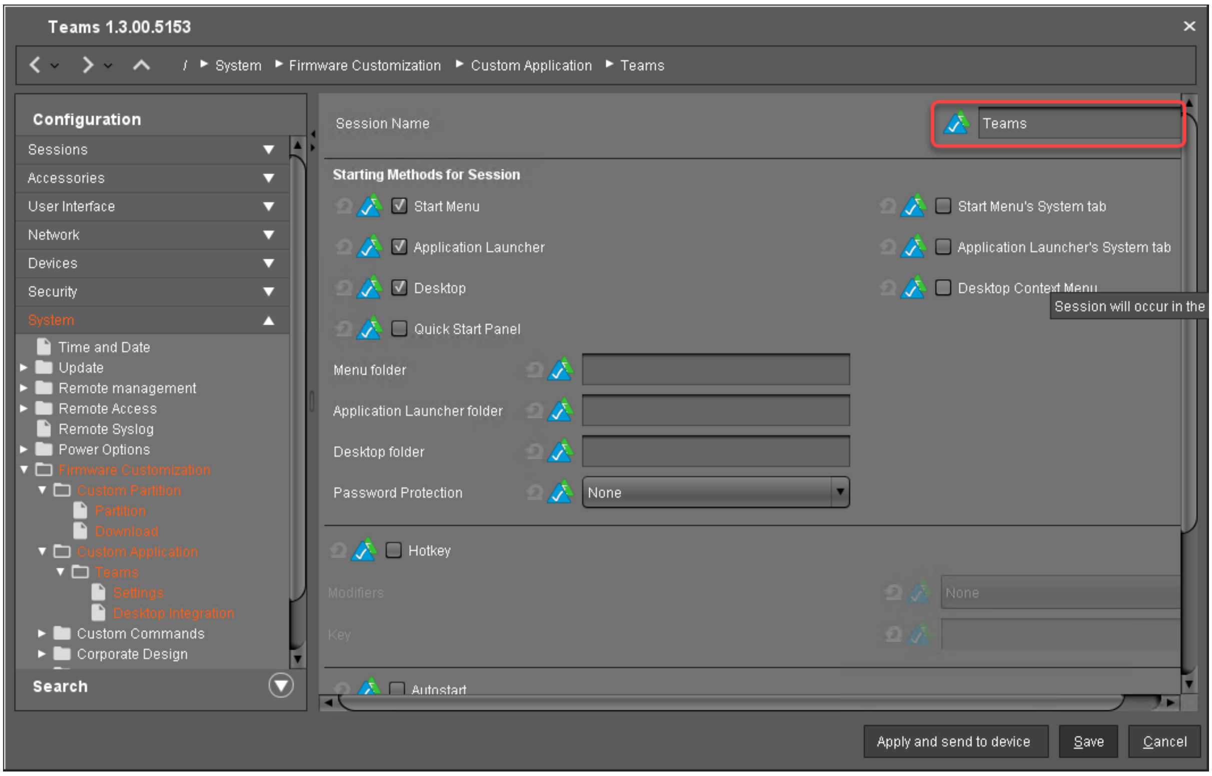
1. Go to **System > Firmware Customization > Custom Application**.

2. In the **Custom Applications** list, click + to add an application.



The **Desktop Integration** page opens.

3. Enter "Teams" as the **Session name**.



Session Name: Teams

Starting Methods for Session

☑ Start Menu
☐ Start Menu's System tab
☑ Application Launcher
☐ Application Launcher's System tab
☑ Desktop
☐ Desktop Context Menu
☐ Quick Start Panel

Session will occur in the

Menu folder:

Application Launcher folder:

Desktop folder:

Password Protection: None

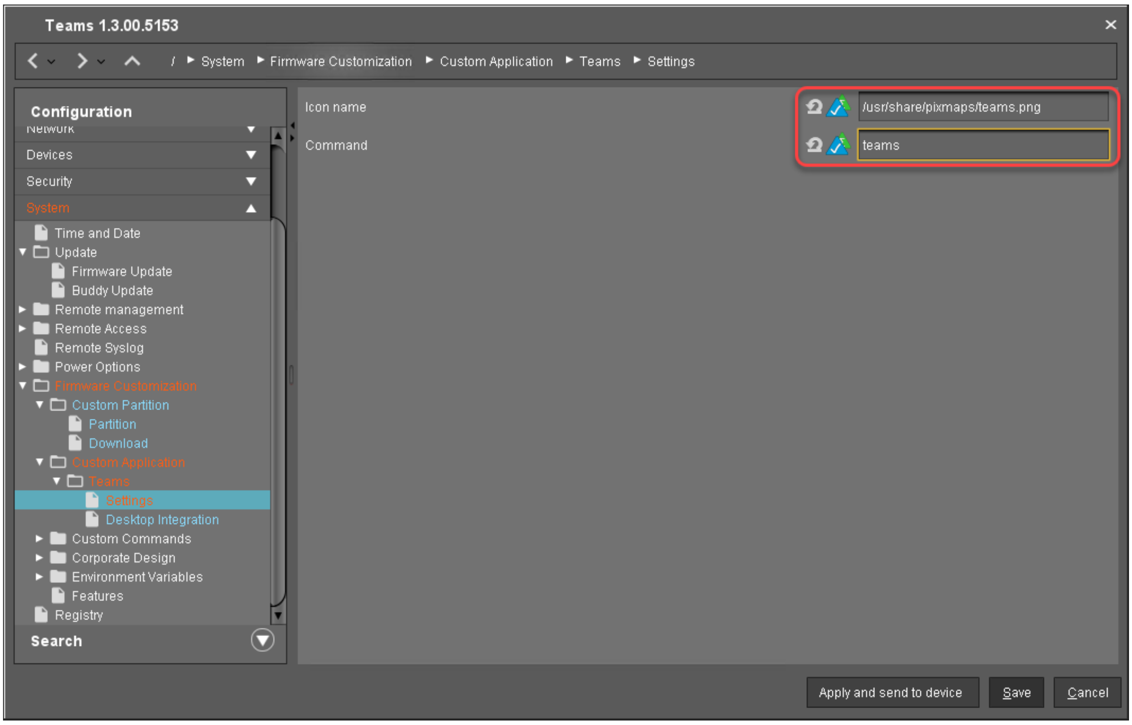
☐ Hotkey

Modifiers: None

Key:

☐ Autostart

4. Go to **Settings**.
5. Edit the settings as follows:
   - **Icon name**: Enter "/usr/share/pixmaps/teams.png".
   - **Command**: Enter "teams".



Icon name: /usr/share/pixmaps/teams.png

Command: teams

6. Click **Save**.

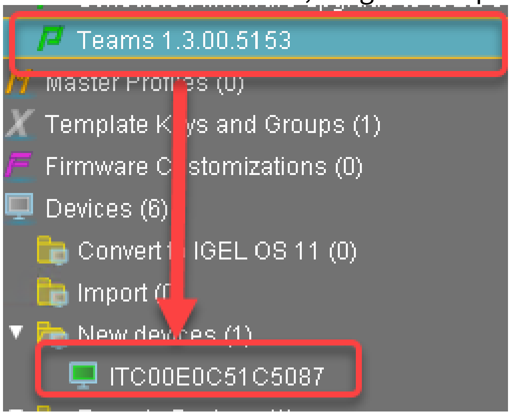
Next Step

>> Assigning the Profile and Testing the Application (see page 726)

Assigning the Profile and Testing the Application

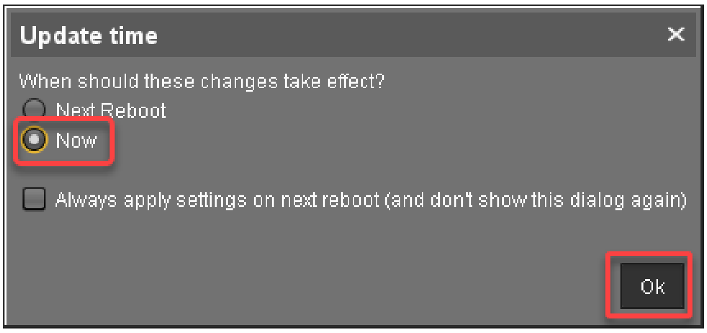
Now that you have put all the settings for installing the Custom Partition on a device into a profile, it is time to assign the profile.

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**.



Update time ✕

When should these changes take effect?

○ Next Reboot

● Now

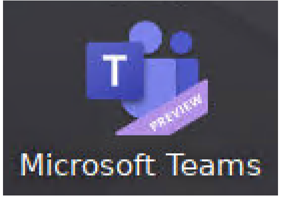
□ Always apply settings on next reboot (and don't show this dialog again)

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 Microsoft Teams icon should appear:



3. Click on the Microsoft Teams icon to test the 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 UMS file transfer or Custom Partition (see page 658).
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`

Adding an Icon for Browsing Removable Storage

Symptom

There is no obvious way of viewing files from removable media locally on the thin client.

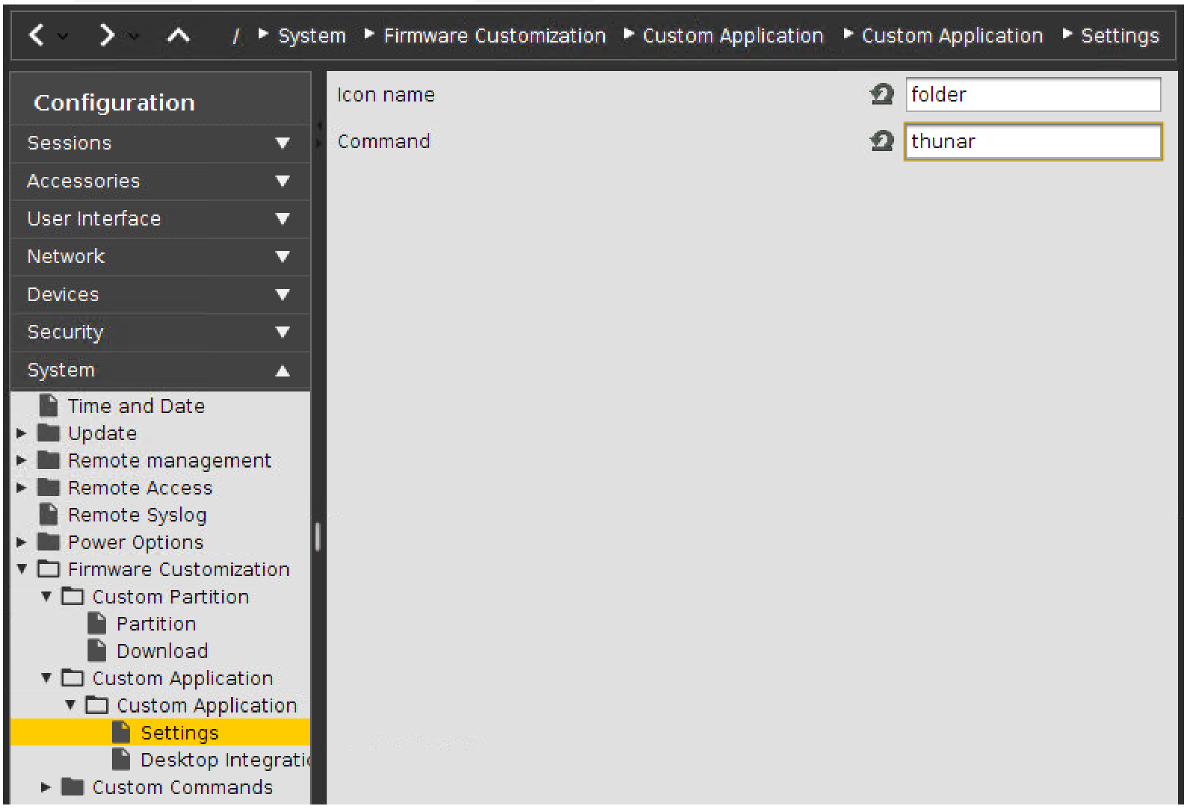
Problem

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:

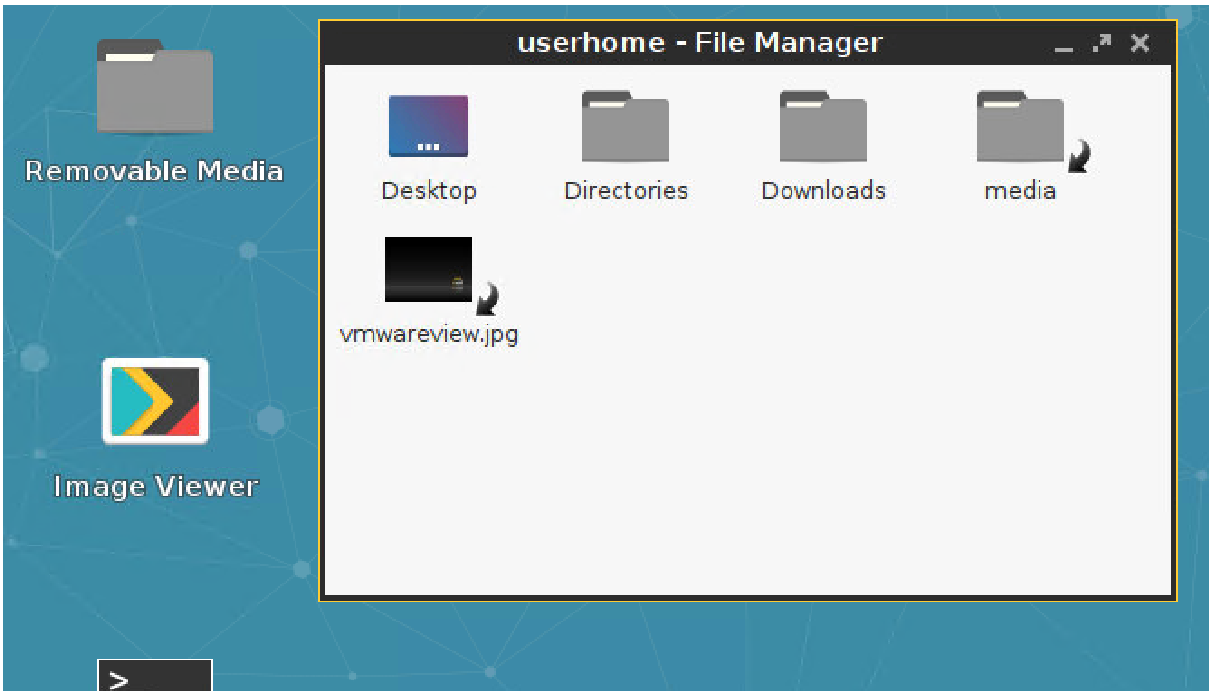


Icon name: folder

Command: thunar

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, see FAQ (see page 783)).

Adding an Icon for the Image Viewer

Symptom

You want to view images locally on the thin client.

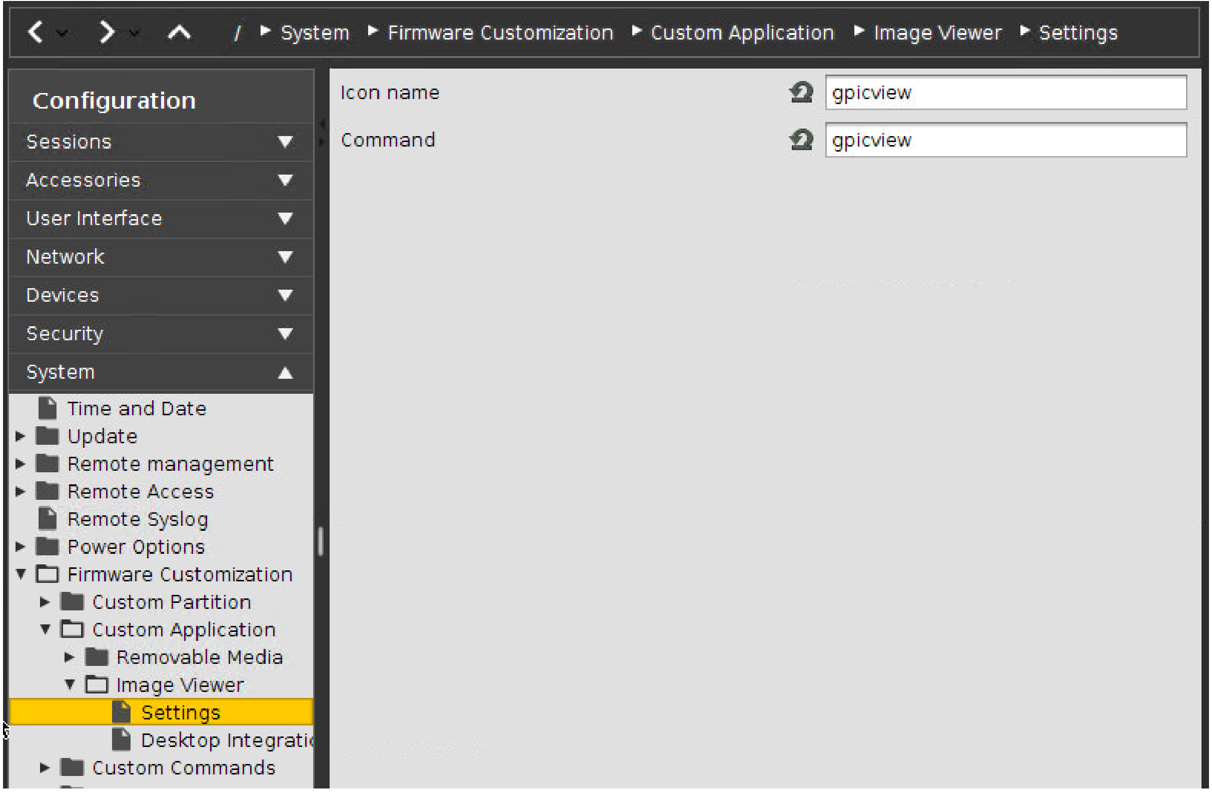
Problem

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**:

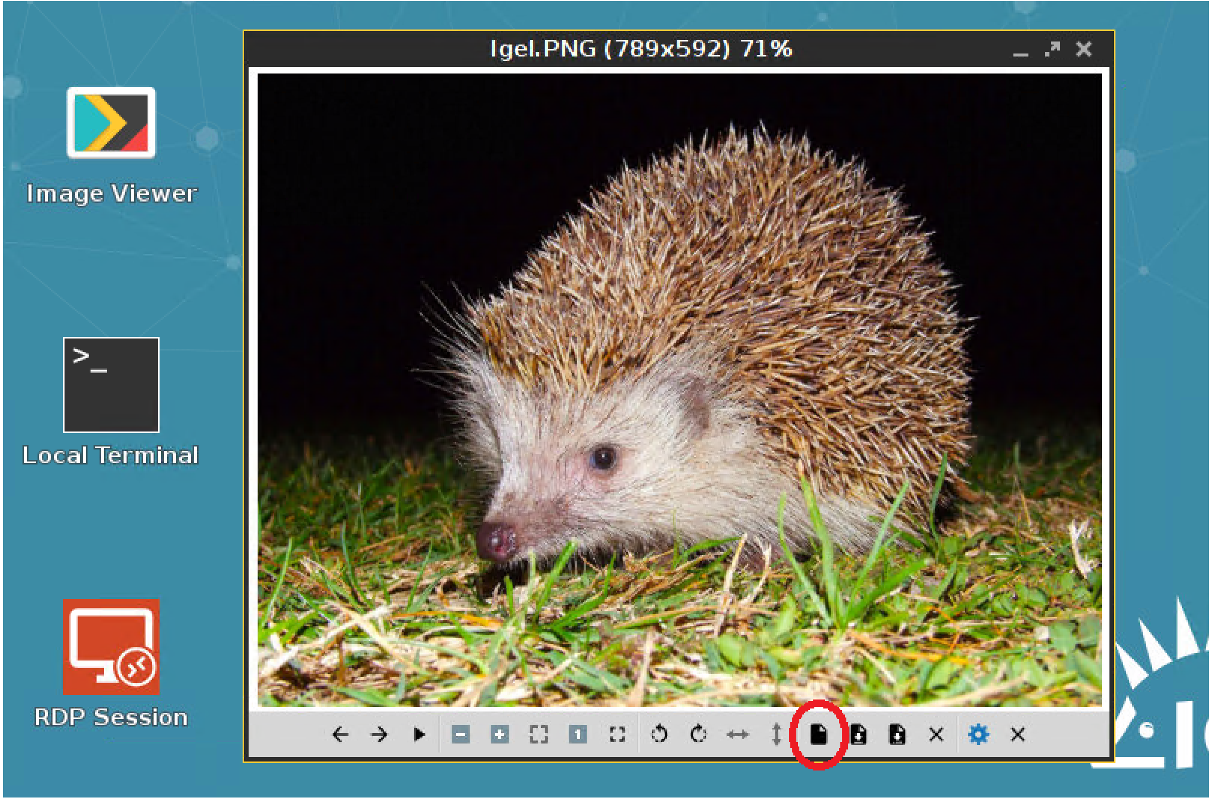


Icon name: gpicview

Command: gpicview

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 741). See also Firmware Customizations and Create Firmware Customization in the UMS Reference Manual.

For information on customizing IGEL OS desktops via a profile, see:

- Introduction (see page 737)
- Creating Your Own Wallpaper (see page 740)
- Creating a New Bootsplash (see page 744)
- Creating Your Own Screensaver (see page 746)
- Assigning Your Own Company Logos (see page 751)
- Creating Your Own Taskbar (see page 753)
- Customizing Desktop Icons (see page 754)

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

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 738)
- Creating a Profile (see page 739)

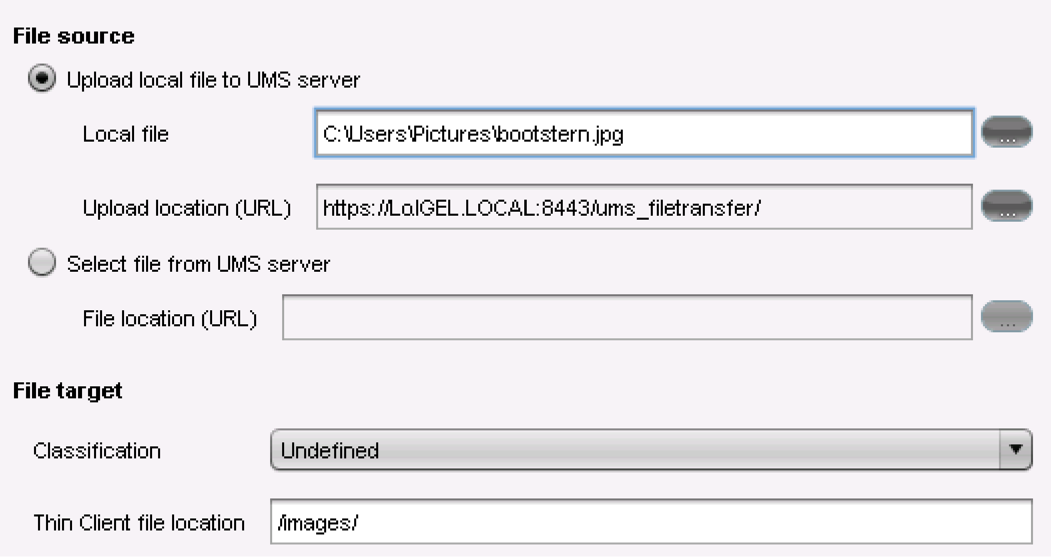
Uploading a Picture

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**.



File source

● Upload local file to UMS server

Local file: C:\Users\Pictures\bootstern.jpg

Upload location (URL): https://LoIGEL.LOCAL:8443/ums_filetransfer/

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Thin Client file location: /images/

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**, one after the other.

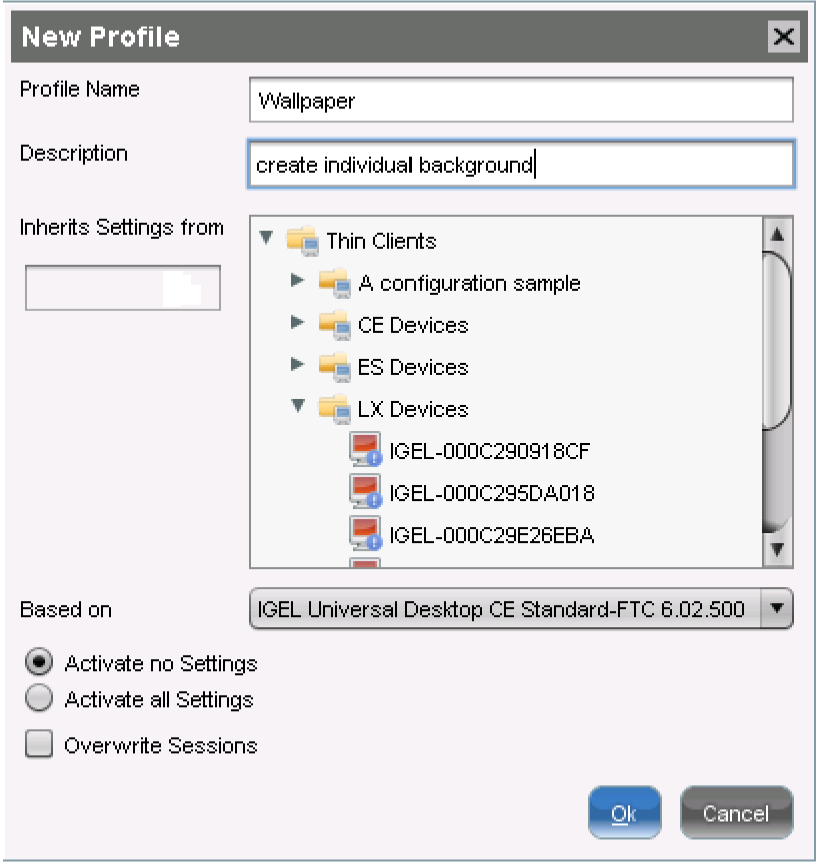
Creating a Profile

You have already uploaded your image file (see page 738).

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:

Based on: IGEL Universal Desktop CE Standard-FTC 6.02.500

● Activate no Settings
○ Activate all Settings
□ Overwrite Sessions

4. Click **OK**.

Creating Your Own Wallpaper

There are two ways how to create an own wallpaper:

- Via a Firmware Customization (see page 741)
- Via a Profile (see page 742)

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 blank spaces or 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.

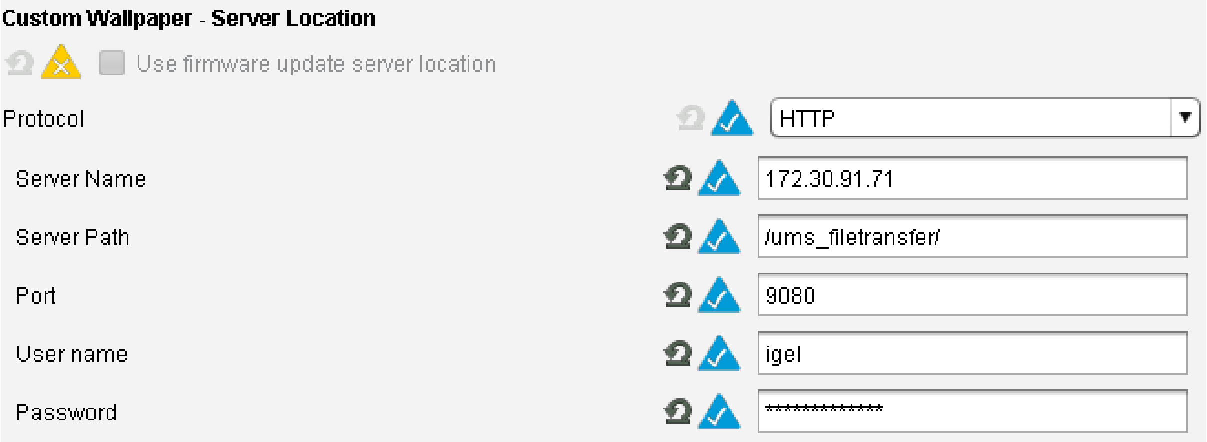
Creating Your Own Wallpaper via a Profile

You have already uploaded your wallpaper picture; see Uploading a Picture (see page 738).

1. Create a profile and name it, for example, **Wallpaper**; see Creating a Profile (see page 739). 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**.



Custom Wallpaper - Server Location

□ Use firmware update server location

Protocol	HTTP
Server Name	172.30.91.71
Server Path	/ums_filetransfer/
Port	9080
User name	igel
Password	**************

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**.

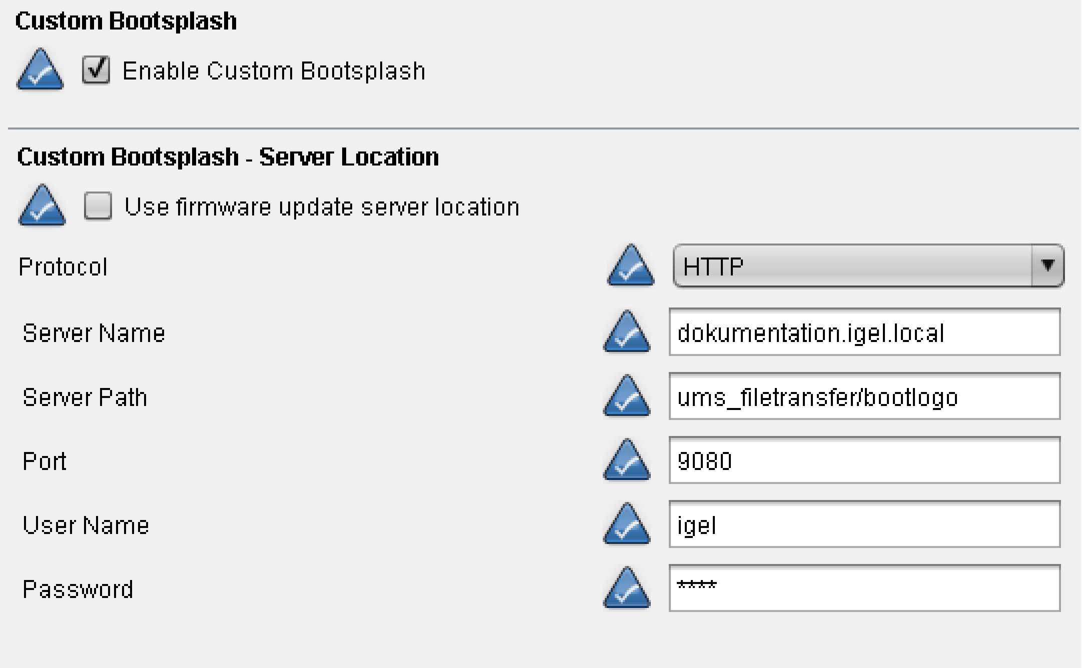
Checking the Results

1. Choose the device in the **Thin Clients** directory of the structure tree.
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 a New Bootsplash

1. Upload your logo to the UMS server; see Uploading a Picture (see page 738).
2. Create a new profile named **Bootlogo**; seeCreating a Profile (see page 739).
3. In the profile configuration window, click **System > Firmware Customization > Corporate Design > Custom Bootsplash** to create your own bootsplash.



Custom Bootsplash

☑ Enable Custom Bootsplash

Custom Bootsplash - Server Location

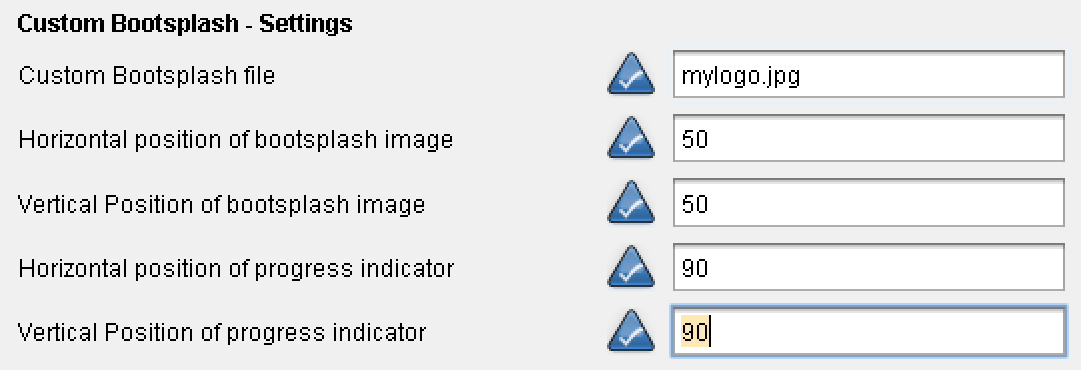
□ Use firmware update server location

Protocol	HTTP
Server Name	dokumentation.igel.local
Server Path	ums_filetransfer/bootlogo
Port	9080
User Name	igel
Password	****

4. Activate **Enable Custom Bootsplash**.
5. Choose HTTP as **Protocol**.
6. Enter the **Server Name** 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.

9. Enter your UMS administrator **User Name** and **Password**.



Custom Bootsplash - Settings

Custom Bootsplash file	mylogo.jpg
Horizontal position of bootsplash image	50
Vertical Position of bootsplash image	50
Horizontal position of progress indicator	90
Vertical Position of progress indicator	90

10. Enter the name of your logo image in **Custom Bootsplash file**.

    ⓘ The optimum size of the picture is **800 x 600 pixels**.

11. Apply **vertical and horizontal position** for the image and progress indicator.
    The scale goes from 0 (left) to 100 (right); the default setting is 50 (centered).
12. **Save** the settings.
13. Assign the profile to your devices by dragging and dropping it or by adding it under **Assigned objects**.

ⓘ After changing the image file or any setting of an existing custom bootsplash, the bootsplash code has to be rebuilt. You can trigger this from UMS via **Jobs > New Scheduled Job** with the command **Update desktop customization**.

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 738).

   ⓘ 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 739).
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 747)
   - Setting a Timeout for Autostart (see page 748)
   - Assigning the Custom Logo (see page 749)
   - Assigning the Custom Clock (see page 750)
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 738).

   > ⓘ 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.

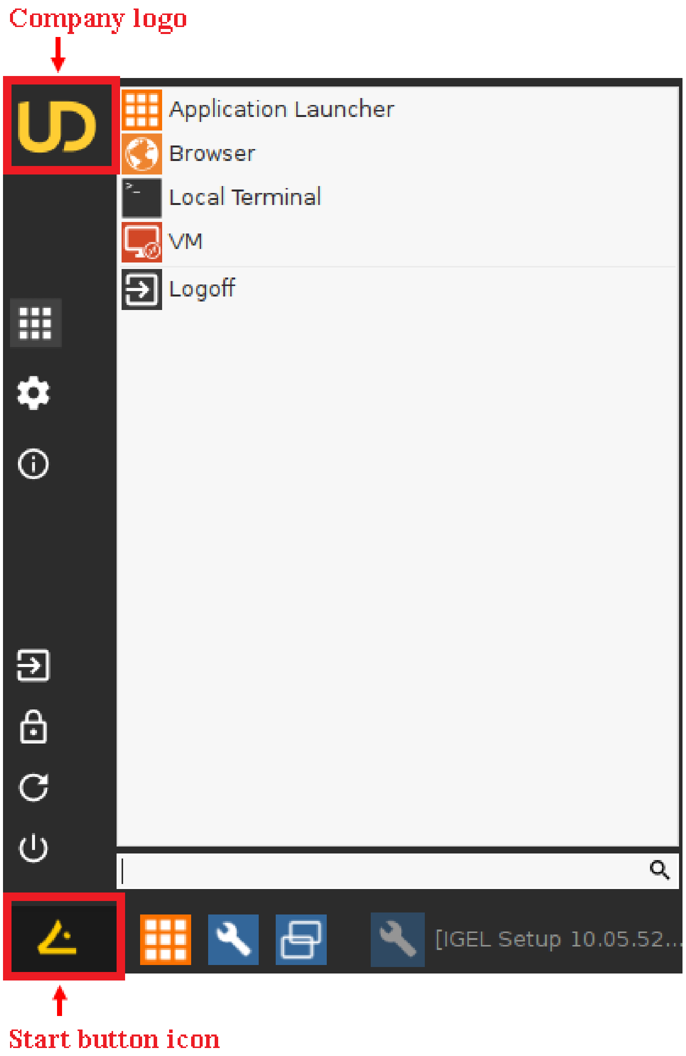
Assigning the Custom Clock

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.

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:

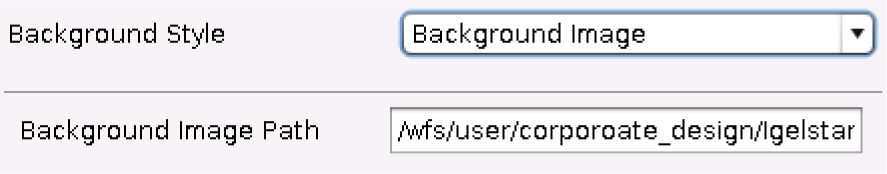
1. Upload your logos to the UMS server. For details, see Uploading a Picture (see page 738).
2. Create a new profile. For details, see Creating a Profile (see page 739).
   The profile configuration window opens.
3. Go to **System > Firmware Customization > Corporate Design > Company Logos > Start Menu.**
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 Create Firmware Customization in the UMS manual. Here you will find further configuration options for adapting the UMS to your requirements.

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 738).
2. Create a new profile, seeCreating a Profile (see page 739).
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**.



Background Style: Background Image

Background Image Path: /wfs/user/corporoate_design/Igelstar

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.

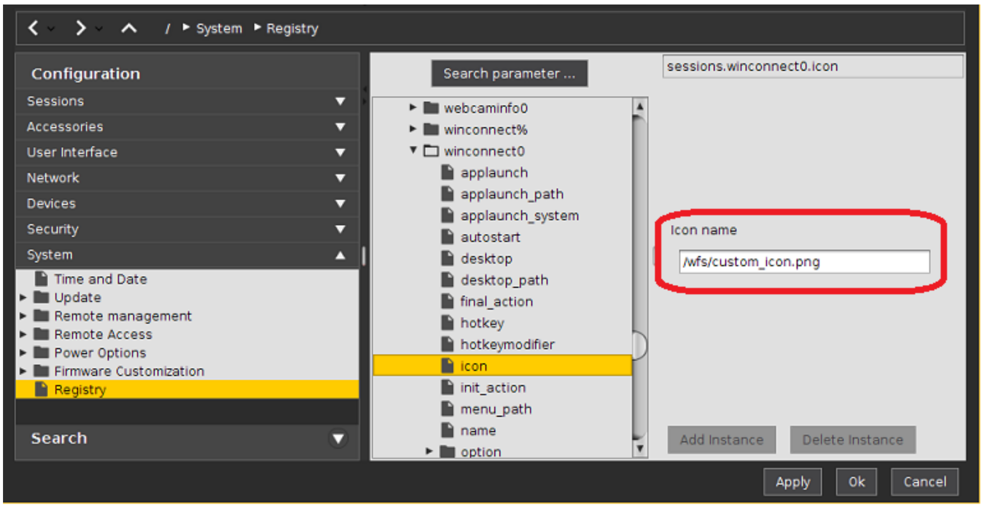
ⓘ Even though other formats like BMP or JPEG are supported, only PNG and SVG are recommended because these formats support transparency.

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.



sessions.winconnect0.icon

Icon name: /wfs/custom_icon.png

4. Click **Ok** to save the changes.

How to Change the Font Color of the Desktop Icons

Overview

You want to alter the font color of the desktop icons.

Environment

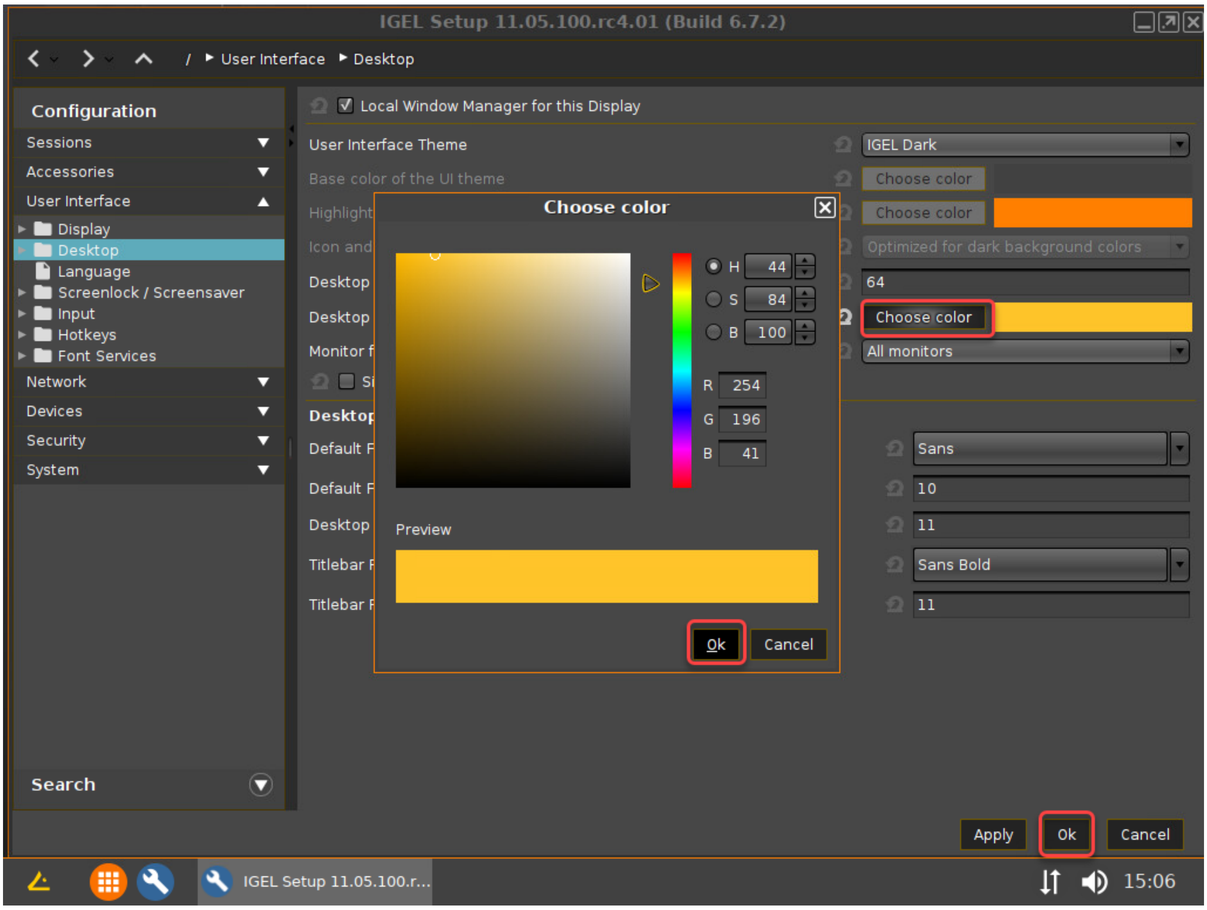
- IGEL OS 11.05.100 or higher

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**.



☑ Local Window Manager for this Display

User Interface Theme: IGEL Dark

Base color of the UI theme: Choose color

Highlight: Choose color

Icon and: Optimized for dark background colors

Desktop: 64

Desktop: Choose color

Monitor f: All monitors

□ Si

Desktop

Default F: Sans

Default F: 10

Desktop: 11

Titlebar F: Sans Bold

Titlebar F: 11

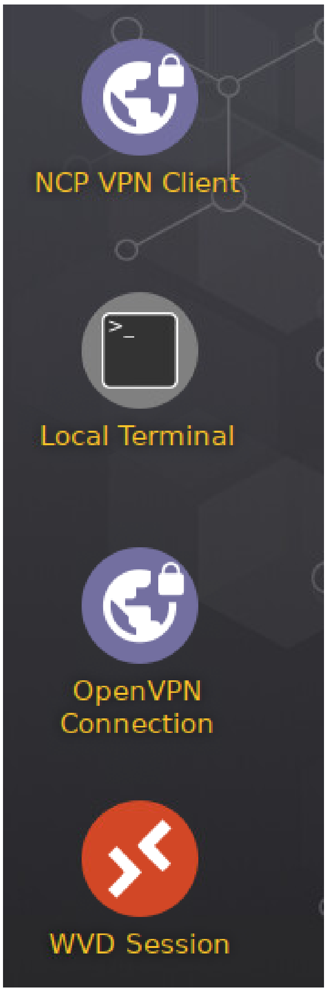
Choose color

● H 44
○ S 84
○ B 100
R 254
G 196
B 41

Preview

Ok Cancel

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 and Screen.

The configuration is described in the following sections:

- Defining the Countdown's Behavior (see page 759)
- Defining the Countdown's Appearance (see page 761)

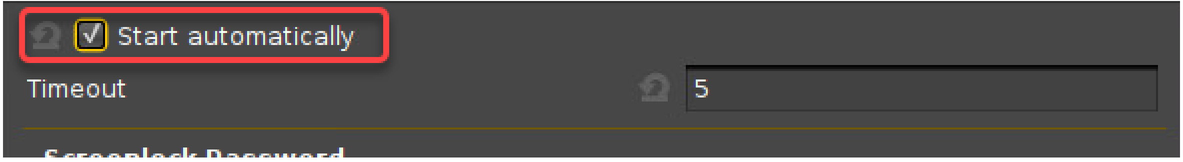
For special purposes, like closing a remote session to prevent it from running unattended, you can configure an additional set of commands. It consists of a command that determines whether the countdown should be started (typically, check whether the remote session is running) and a command that will 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 763)

Defining the Countdown's Behavior

For a description of all options, see Options.

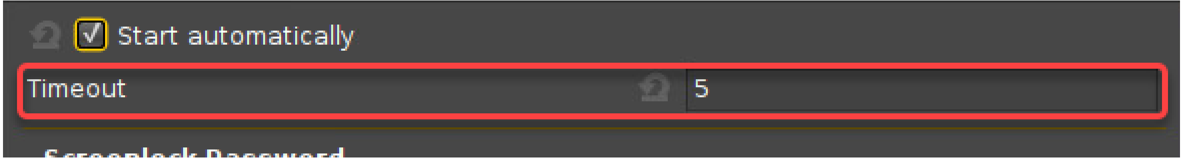
1. In the Setup or UMS configuration dialog, go to **User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.



☑ Start automatically

Timeout 5

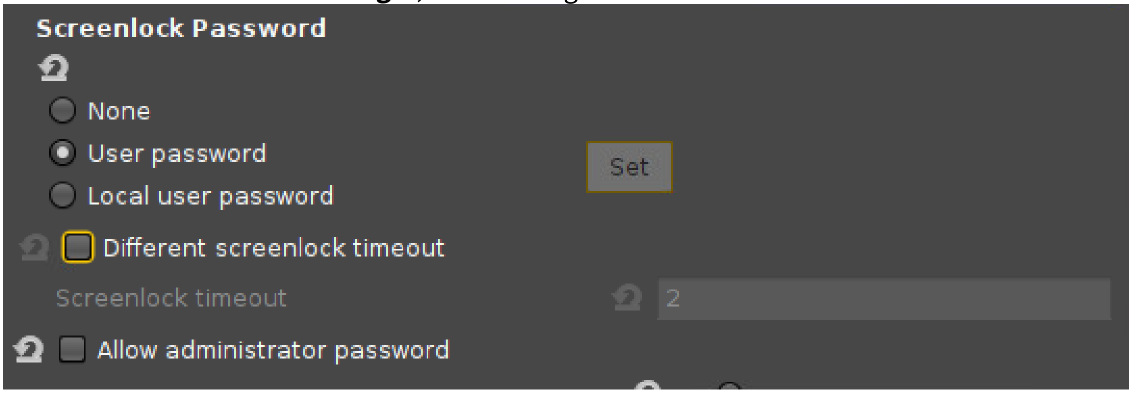
3. In the **Timeout** field, specify after how many minutes the countdown should start.



☑ Start automatically

Timeout 5

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. 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.
      If the user is logged in via Active Directory (AD), 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.



Screenlock Password

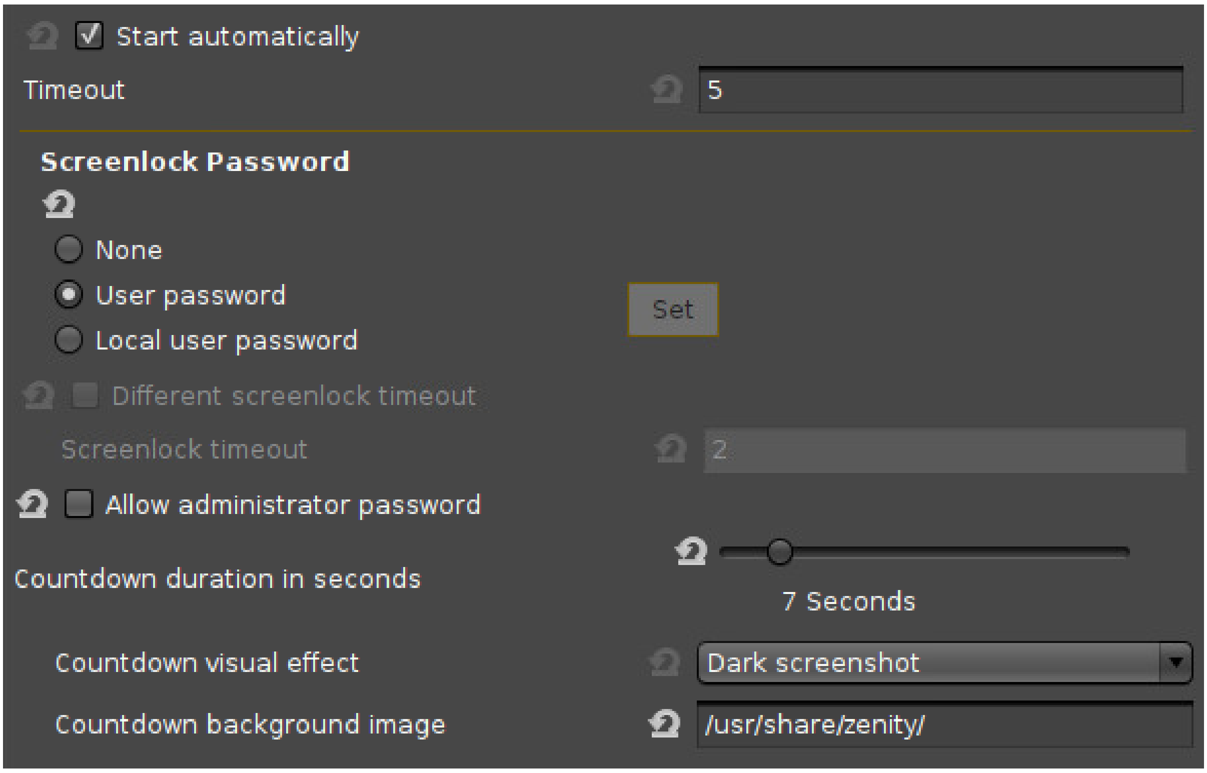
○ None
● User password
○ Local user password

□ Different screenlock timeout

Screenlock timeout: 2

□ Allow administrator password

5. Set the **Countdown duration in seconds**. The range is from 1 to 60.
   Configuration example:



☑ Start automatically

Timeout: 5

Screenlock Password

○ None
● User password
○ Local user password

□ Different screenlock timeout

Screenlock timeout: 2

□ Allow administrator password

Countdown duration in seconds: 7 Seconds

Countdown visual effect: Dark screenshot

Countdown background image: /usr/share/zenity/

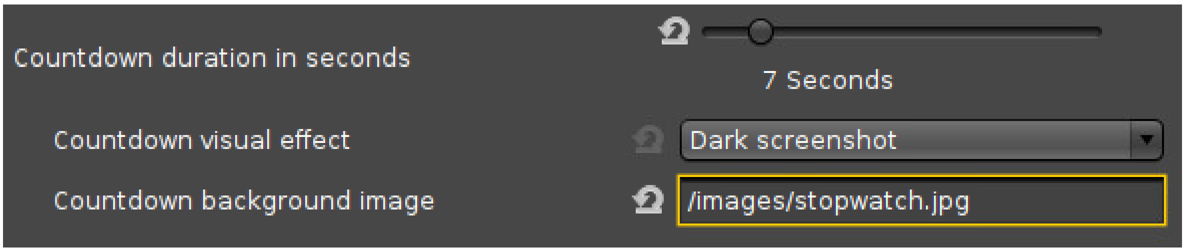
6. Apply the settings to your devices or to your profile.

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 738).
   Configuration example with custom image:



Countdown duration in seconds: 7 Seconds

Countdown visual effect: Dark screenshot

Countdown background image: /images/stopwatch.jpg

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.
   - **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:

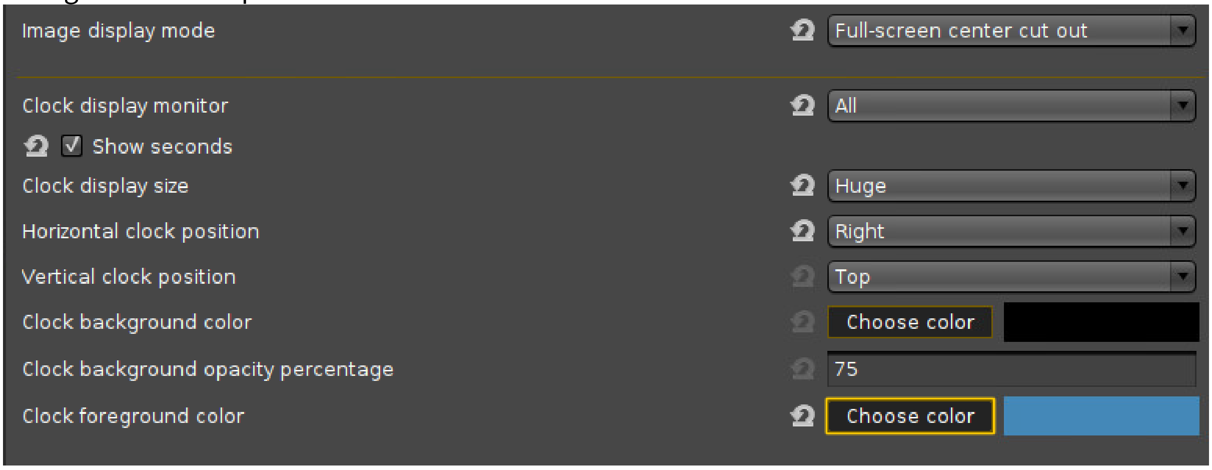


Image display mode: Full-screen center cut out

Clock display monitor: All

☑ Show seconds

Clock display size: Huge

Horizontal clock position: Right

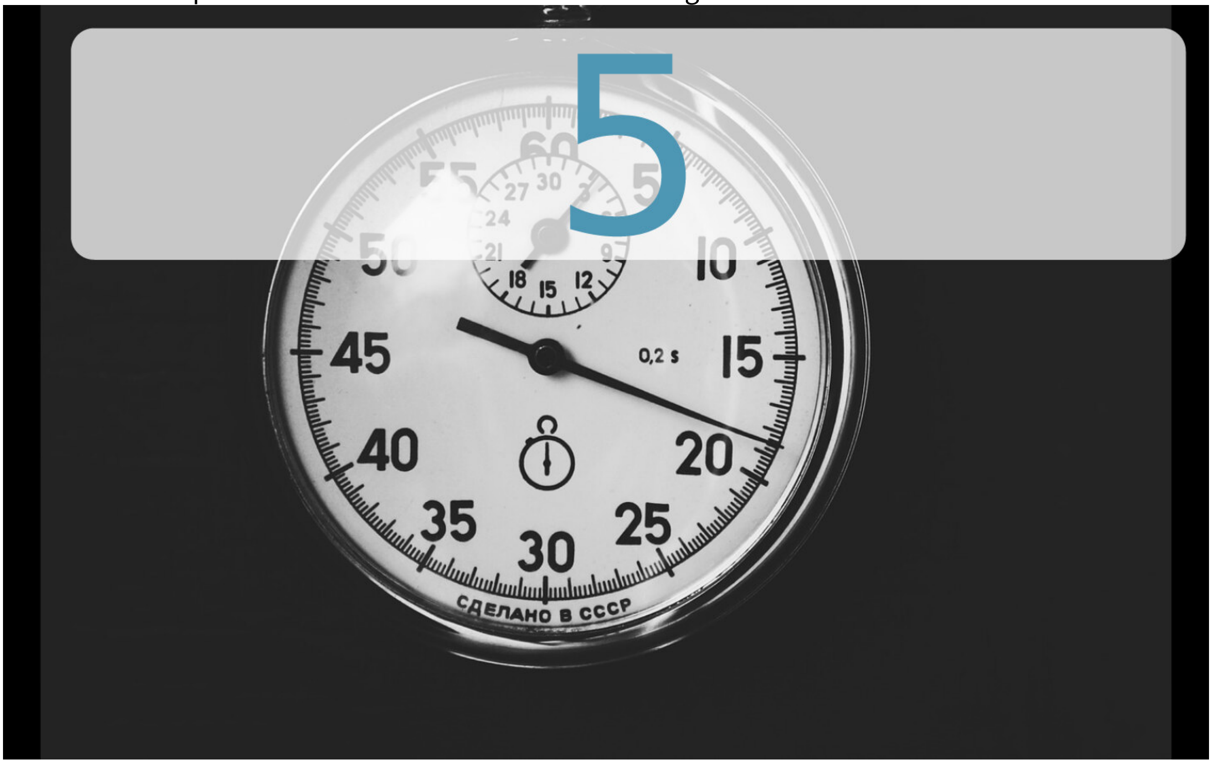
Vertical clock position: Top

Clock background color: Choose color ⬛

Clock background opacity percentage: 75

Clock foreground color: Choose color 🟦

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.

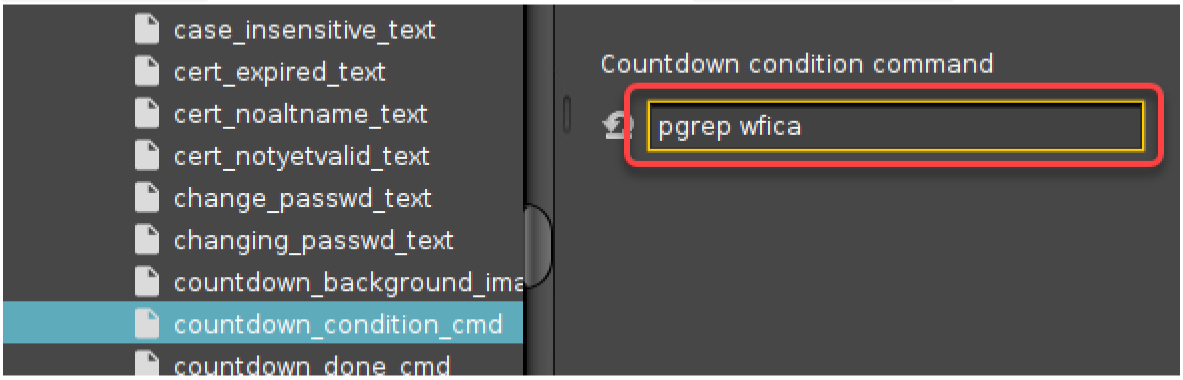
In the following, we will first specify the command that determines whether the countdown should be started. Then, we will specify the command that is executed when the countdown has reached 0.

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 764).

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`



Countdown condition command

pgrep wfica

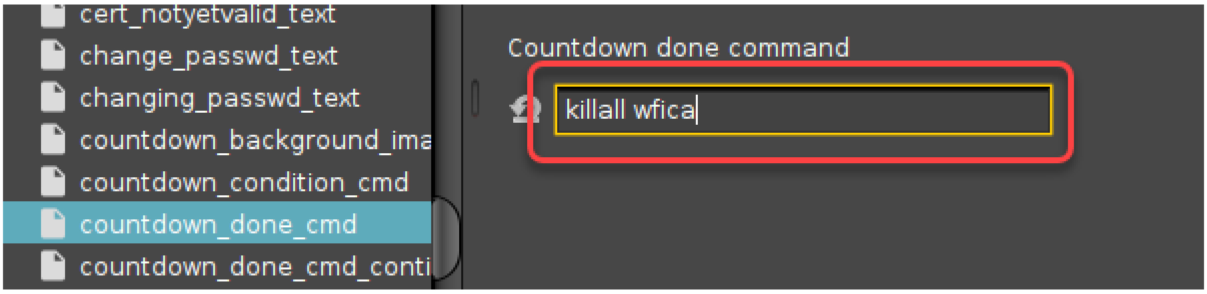
3. Click **Apply** or **Ok**.
If the command returns 0, the countdown is started. When the countdown has reached 0, the command specified with **System > Registry > sessions > xlock0 > options > countdown_done_cmd** is executed (see Command to Be Executed after the Countdown (see page 764)).
If the command 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 " `&` ".

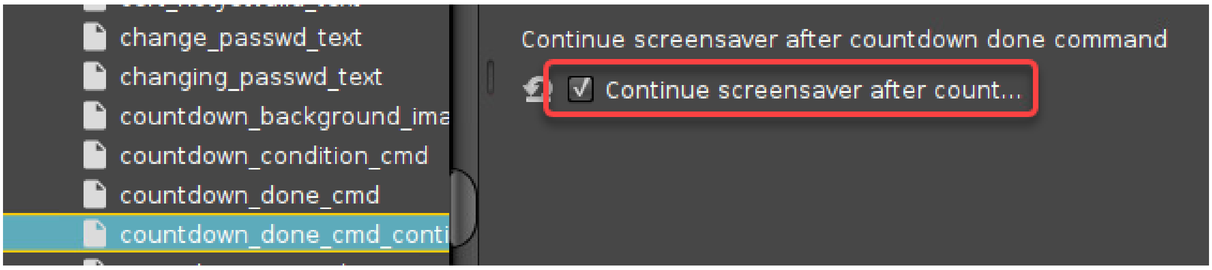


Countdown done command

killall wfica

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.

   Continue screensaver after countdown done command

   ☑ Continue screensaver after count...

4. Click **Apply** or **Ok**.

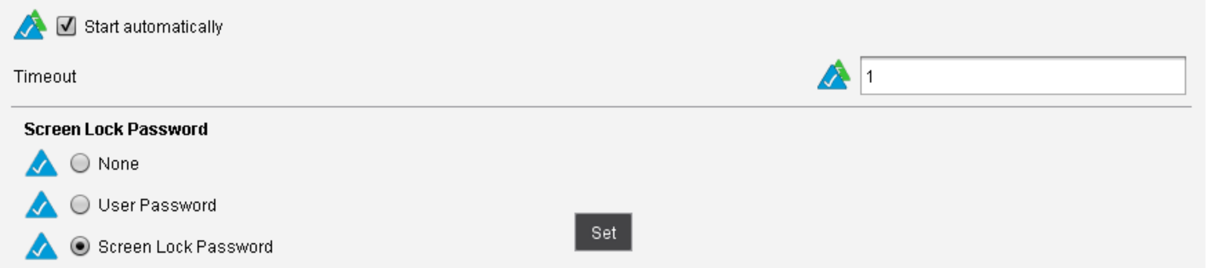
How to Set Up a Countdown in the IGEL OS

You can set up the countdown via the device's local Setup or via the IGEL Universal Management Suite (UMS). It is recommended to use the IGEL UMS and store your settings in a profile; this allows you to apply your settings to a random number of devices in one go.

For more information about profiles, see the Profiles chapter in the IGEL UMS reference manual.

Defining the Countdown's Behavior

1. In the Setup, go to **User Interface > Screenlock / Screensaver > Options**.
2. Activate **Start automatically**.
3. In the **Timeout** field, set the idle timeout in minutes, after which 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.
    - **User password**: The user must enter the user password to unlock the screen. The user password is configured in **Security > Password**.
    - **Screenlock password**: The user must enter a special screenlock password to unlock the screen. Click **Set** to define the screenlock password.
5. Set the **Countdown duration** in seconds. The range is from 1 to 60.
   Configuration example:



☑ Start automatically

Timeout: 1

Screen Lock Password

○ None

○ User Password

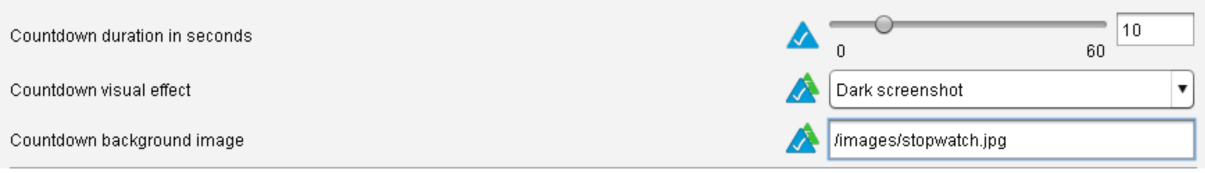
● Screen Lock Password

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 738).
Configuration example with custom image:



Countdown duration in seconds	10 (0–60)
Countdown visual effect	Dark screenshot
Countdown background image	/images/stopwatch.jpg

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.
   - **Image display mode**: Position and scaling for the background image

> This parameter is only relevant for IGEL Linux v5. With IGEL Linux *version 10.03.500* or higher, the **Image display mode** is set to "Full-screen letterbox".

   - **Clock display monitor**: Selects the monitor(s) on which the countdown is to be shown.
   - **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 foreground color**: Color of the countdown digits

Configuration example:

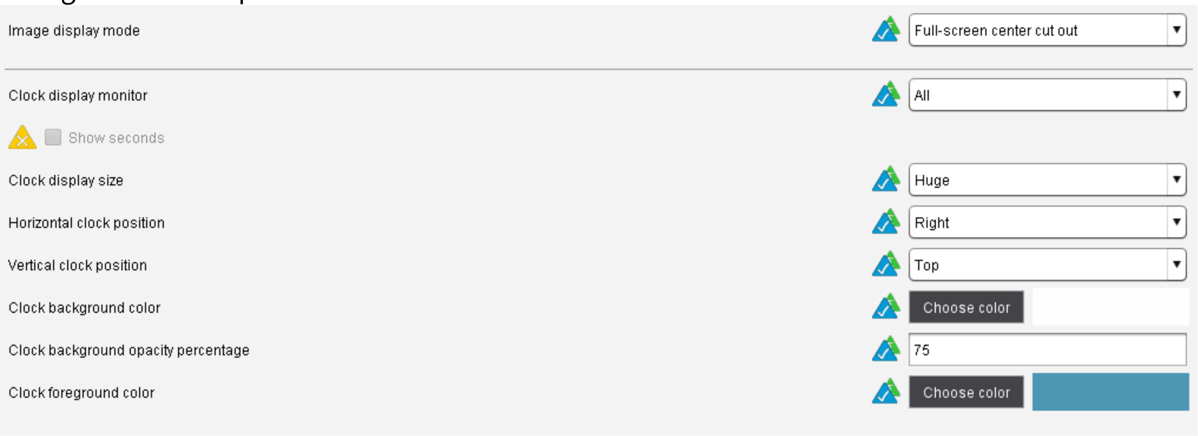
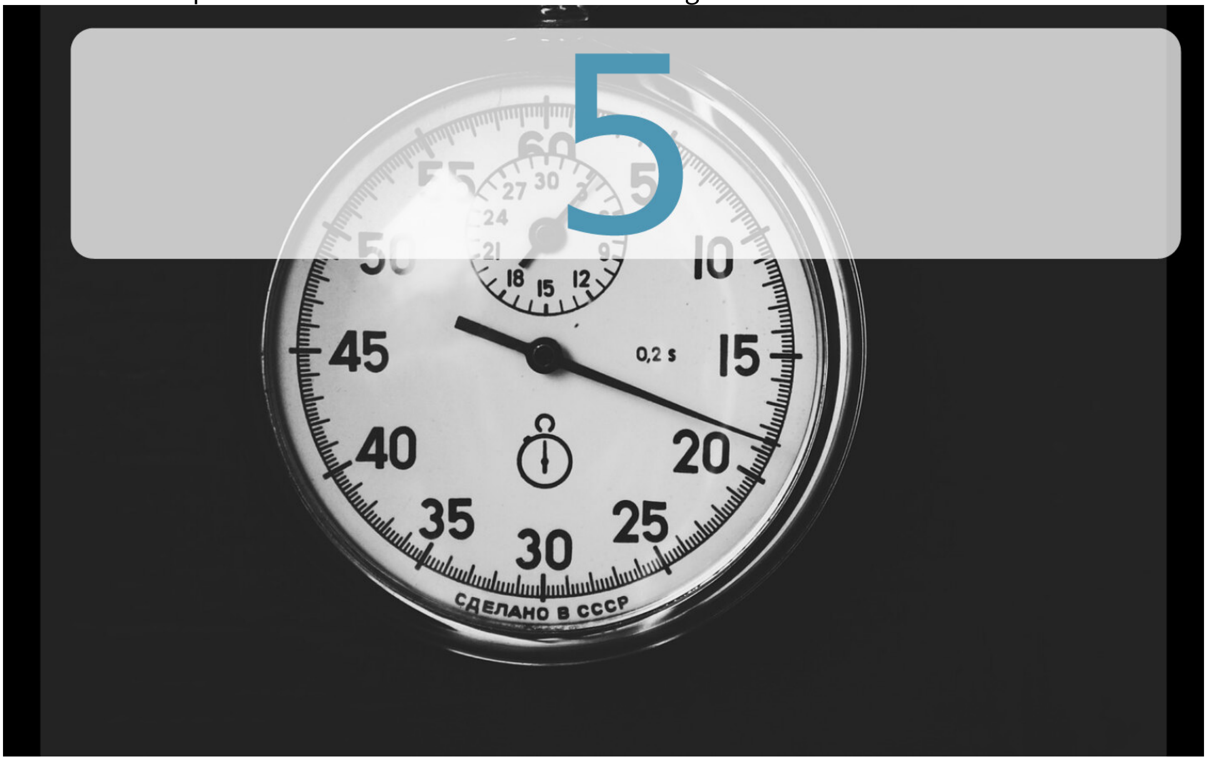


Image display mode	Full-screen center cut out
Clock display monitor	All
□ Show seconds	
Clock display size	Huge
Horizontal clock position	Right
Vertical clock position	Top
Clock background color	Choose color
Clock background opacity percentage	75
Clock foreground color	Choose color

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

You can specify an arbitrary command that is executed when the countdown has reached 0.

Additionally, you can specify a command that determines whether the countdown is to be started.

Example use case: The countdown is running, but the user does not interact with the device in order to make the countdown stop. When the countdown has reached 0, the system checks whether a session is running, e.g. an appliance mode Citrix session. If yes, the user is logged off from this session.

If no command is set to be executed after countdown, the screen will be locked instead.

The user that issues the commands depends on the firmware version in use:

- With IGEL Linux v5, the user is `root`.
- With IGEL OS Linux 10, the user is `user`.

To specify the command that determines the condition:

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**. Example: `pgrep wfica` (determines if a Citrix session is present)
3. Click **Apply** or **Ok**.
   If the command returns 0, the countdown or commando is started.
   If the command returns a non-zero value, the countdown or commando is not started.

To specify the 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**. Example: `killall wfica` (terminates the Citrix ICA client)

   ⓘ 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. Open the registry key **sessions > xlock0 > options > countdown_done_cmd_continue** (`sessions.xlock0.options.countdown_done_cmd_continue`) and specify whether the screensaver should be started after the command has been started.

   ⓘ With IGEL Linux v5, the screensaver does not start immediately. It will be started after the idle timeout defined under **User Interface > Screen Lock/Saver > Options > Timeout**.
   With IGEL OS Linux 10, the screensaver is started immediately.

☑ The screensaver is started after the command has been started.
☐ The screensaver will not be started.

4. Click **Apply** or **Ok**.

Installing a Calculator on IGEL Linux

Issue

You may want to have a desktop calculator.

Solution

1. Download the opensource java calculator from: http://sourceforge.net/projects/simpcalc/

   > ⓘ The default download location of the local Firefox browser is `/tmp/` .

2. Open a **Local Terminal** and log in as `root`
3. Copy the downloaded `.jar` file from the `/tmp/` directory to `/wfs/simplecalc.jar:`
   `cp /tmp/ /wfs/simplecalc.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/simplecalc.jar in` **Settings**
6. Click the newly created icon on the desktop to run the custom application.

   > ⓘ To distribute this application to several thin clients please use the file transfer option in IGEL UMS and set up a profile with the custom application configuration.

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

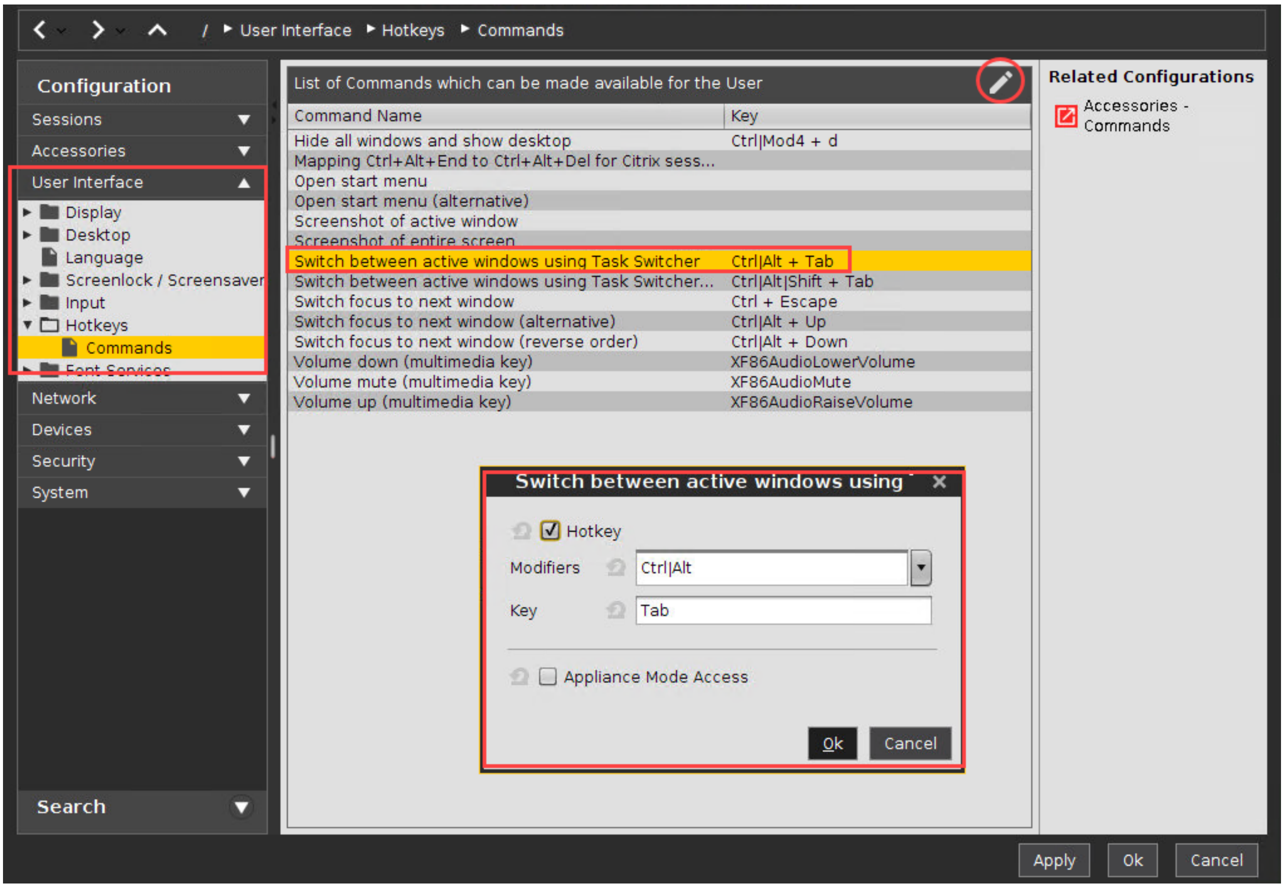
ⓘ Go to IGEL Setup > User Interface > Hotkeys > Commands to change these shortcut combinations.

ⓘ 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:



List of Commands which can be made available for the User

Command Name	Key
Hide all windows and show desktop	Ctrl|Mod4 + d
Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sess...	
Open start menu	
Open start menu (alternative)	
Screenshot of active window	
Screenshot of entire screen	
Switch between active windows using Task Switcher	Ctrl|Alt + Tab
Switch between active windows using Task Switcher...	Ctrl|Alt|Shift + Tab
Switch focus to next window	Ctrl + Escape
Switch focus to next window (alternative)	Ctrl|Alt + Up
Switch focus to next window (reverse order)	Ctrl|Alt + Down
Volume down (multimedia key)	XF86AudioLowerVolume
Volume mute (multimedia key)	XF86AudioMute
Volume up (multimedia key)	XF86AudioRaiseVolume

Switch between active windows using

☑ Hotkey

Modifiers: Ctrl|Alt

Key: Tab

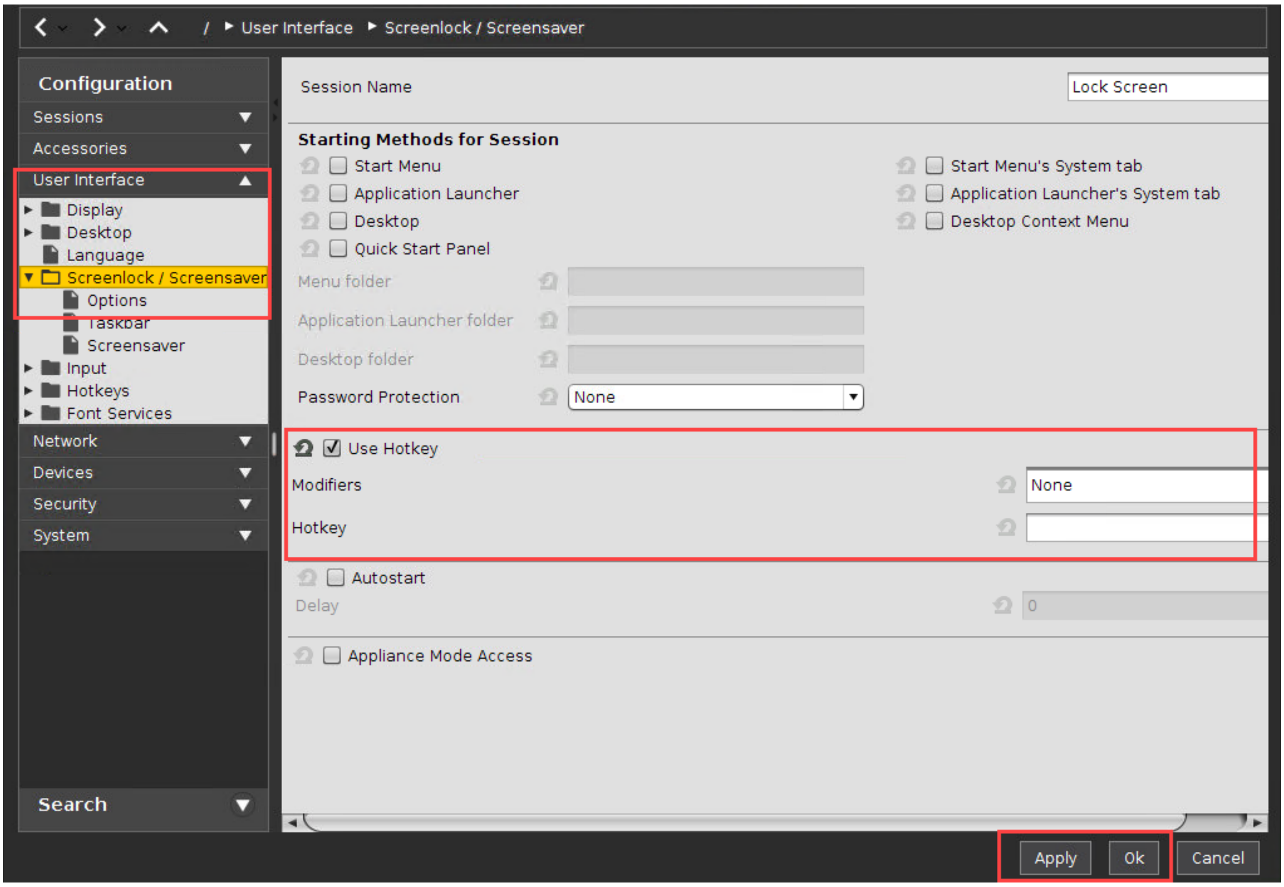
☐ Appliance Mode Access

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:



Session Name: Lock Screen

Starting Methods for Session

☐ Start Menu
☐ Application Launcher
☐ Desktop
☐ Quick Start Panel
☐ Start Menu's System tab
☐ Application Launcher's System tab
☐ Desktop Context Menu

Menu folder

Application Launcher folder

Desktop folder

Password Protection: None

☑ Use Hotkey

Modifiers: None

Hotkey

☐ Autostart

Delay: 0

☐ Appliance Mode Access

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 Thin Clients automatically at the End of a Session

Issue

You may want to shutdown, suspend, restart or log off from the thin client 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 thin client's local setup (or its UMS configuration or profile) navigate to **System > Firmware Customization > Custom Commands** > **After End of Session**.
2. Choose a **Session type**.
3. Choose an auto logoff command.
4. Save the changes with **Apply** or **OK**.

If the last instance of the chosen session type is ended, the auto logoff command will be processed.

See also IGEL OS manual: Post Session

ⓘ The auto logoff command **Shutdown** will perform the default action defined in **System > Power Options > Shutdown >Default action**. Please check this parameter before using auto logoff.

ⓘ The auto logoff command **Logoff** is futile unless you define a logon method in **Security > Logon** (Smartcard, Active Directory/Kerberos or IGEL Shared Workplace). The Logoff command also can not 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.

On earlier versions:

1. Download the tool Rapid Screenshot[48].

   > 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` .

> Please note the licenses for both screenshot capture tools mentioned on the websites of these specific tools!

[48] https://sourceforge.net/projects/screenshot/?source=directory

Setting the Device's System Time

Problem

The device's system time is not correct.

Solution

1. Open the device'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**

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). This is known to work for

- IGEL Linux version 10.01.100 or newer
- IGEL Linux version 5.04.100 or newer
- IGEL Linux version 4.14.100 or newer
- IGEL Linux ARM version 1.09.100 or newer.

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
  - http://packages.ubuntu.com/trusty-updates/all/tzdata/download (for IGEL Linux version 5.x)
  - http://packages.ubuntu.com/precise-updates/all/tzdata/download (for IGEL Linux version 4.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.

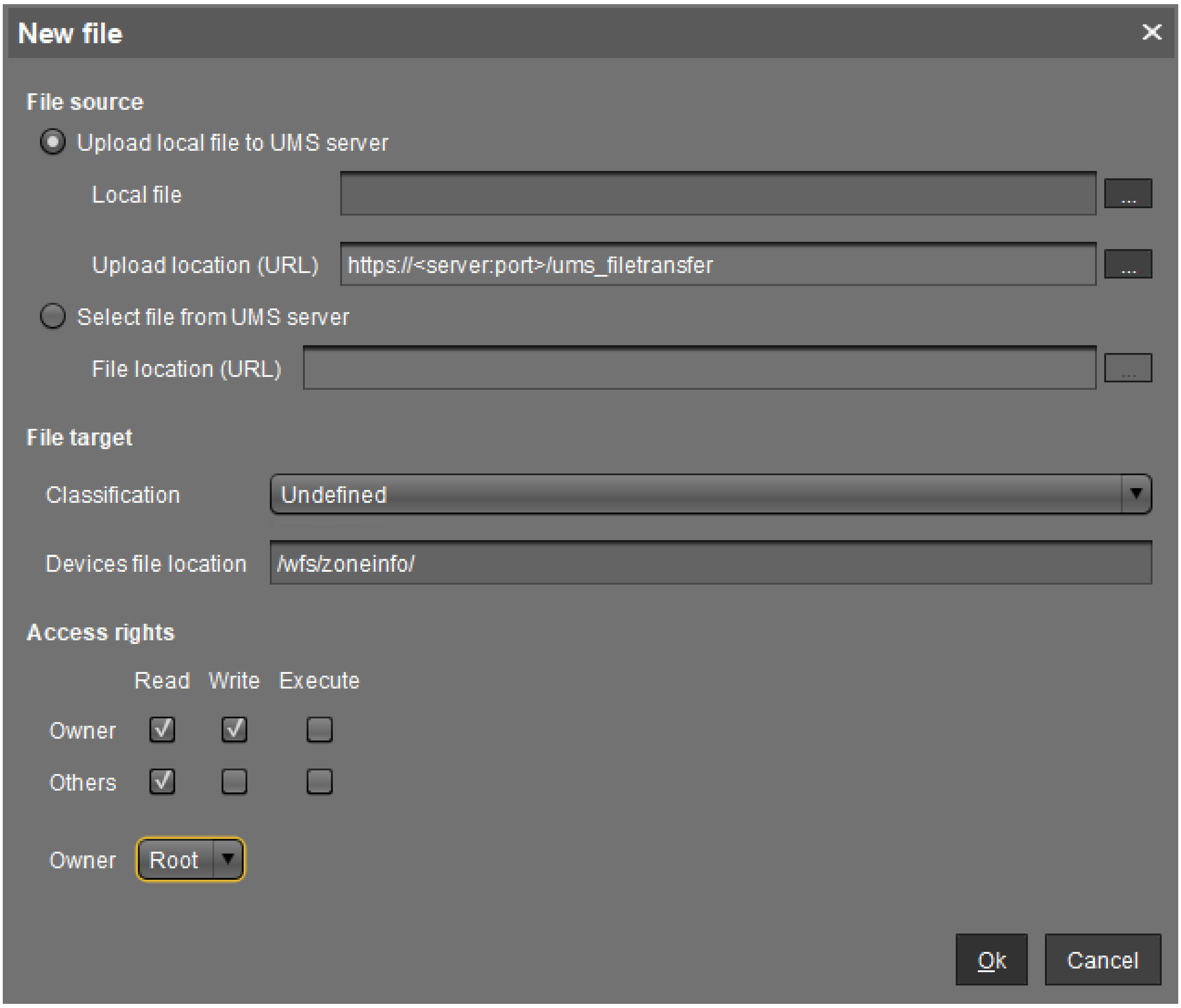
On Linux

- 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.



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):

File target

Classification: Undefined

Devices file location: /wfs/zoneinfo/

Access rights

	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

Owner: Root

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 783).

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

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 791)
- eGalax (see page 795)
- Elo Multitouch (USB) (see page 797)
- Elo Singletouch (USB) (see page 799)
- TSHARC (USB) (see page 801)

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

Vendor	Product	Name
0x0596	0x0001	MicroTouch Systems, Inc., Touchscreen
0x134C	0x0004	PanJit International Inc., Touch Panel Controller
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 / <u>disabled</u>

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 / <u>disabled</u>

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

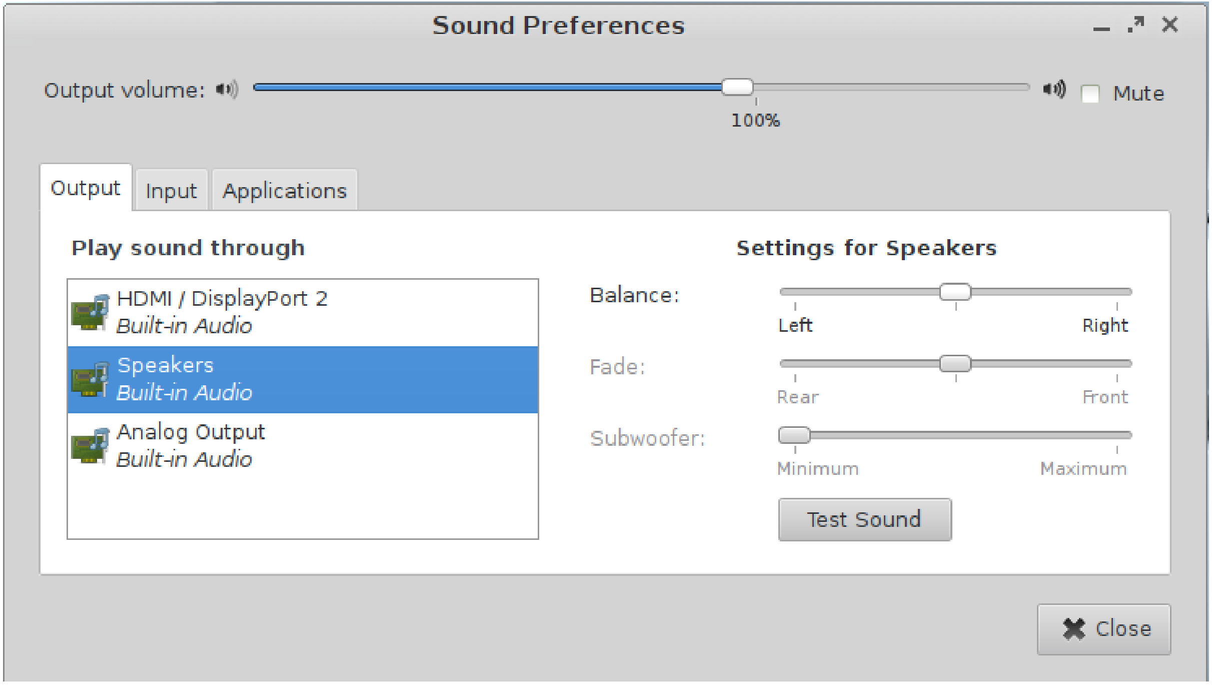
You do not hear any sound from your *IGEL UD5* or *UD6* device. You are using a monitor connected via DisplayPort.

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**.



Sound Preferences

Output volume: 100% □ Mute

Output | Input | Applications

Play sound through

HDMI / DisplayPort 2
Built-in Audio

Speakers
Built-in Audio

Analog Output
Built-in Audio

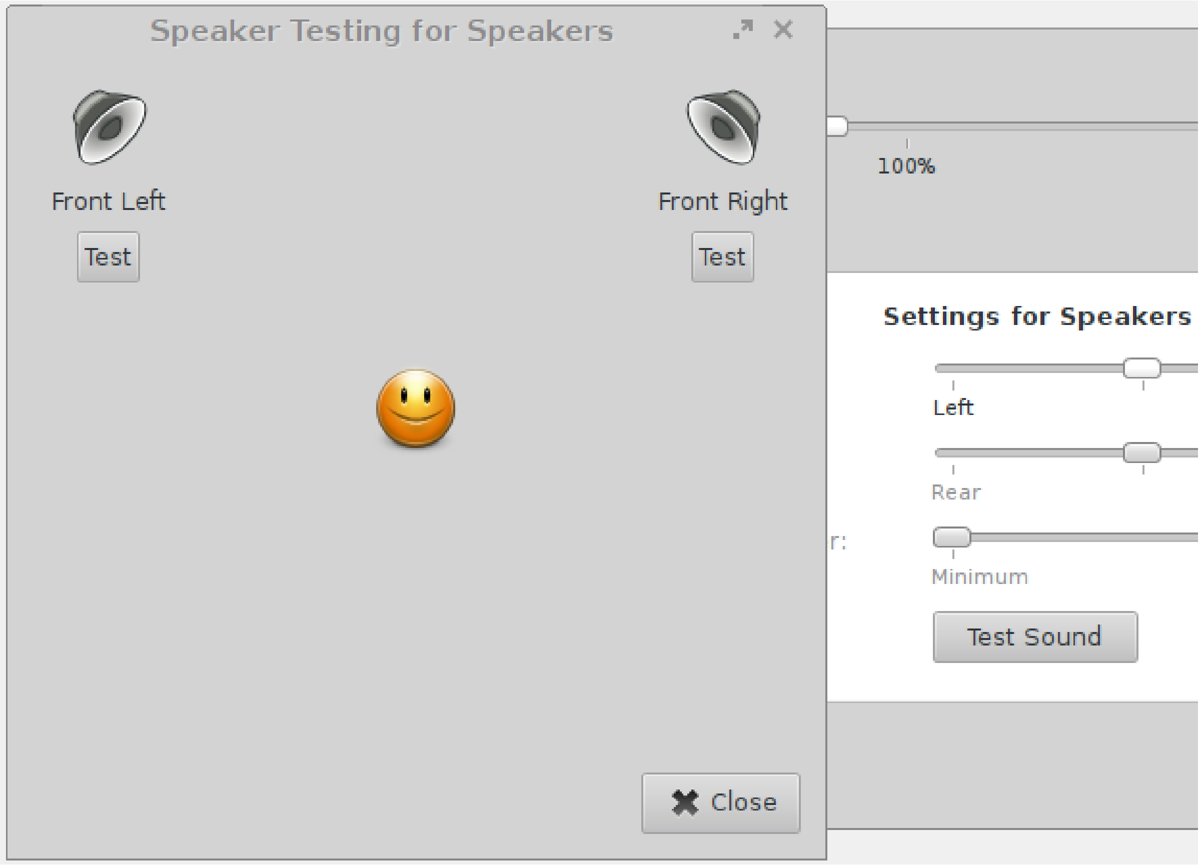
Settings for Speakers

Balance: Left Right

Fade: Rear Front

Subwoofer: Minimum Maximum

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
r:
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 810)
2. Setting Up the Personalization Machine (see page 825)
3. Personalizing the Cherry SECURE BOARD (see page 827)
4. Setting Up the Endpoints (see page 831)

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 835).

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 https://www.cherry.de/files/manual/SECUREBOARD_SwDev_Guide_en-0.4.pdf. Also, the SECURE BOARD 1.0 Quick Installation Package contains a ready-made shell script that creates example certificates. Download the package from https://www.cherry.de/files/software/Cherry_Secureboard_1.0_Quick_Installation_Package_V1.0.zip, 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).

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 812)	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 812)	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 812)	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

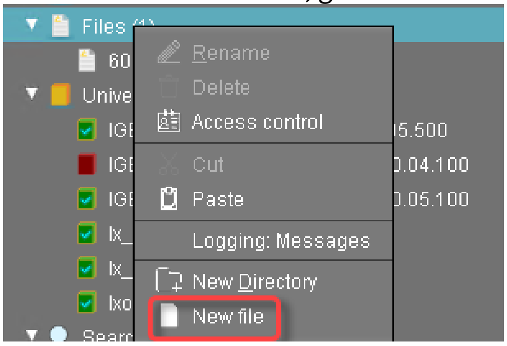
The following instructions describe how to transfer the required certificates to the personalization machine. The personalization machine will deploy the certificates to the keyboard. The UMS will be used for this purpose.

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.

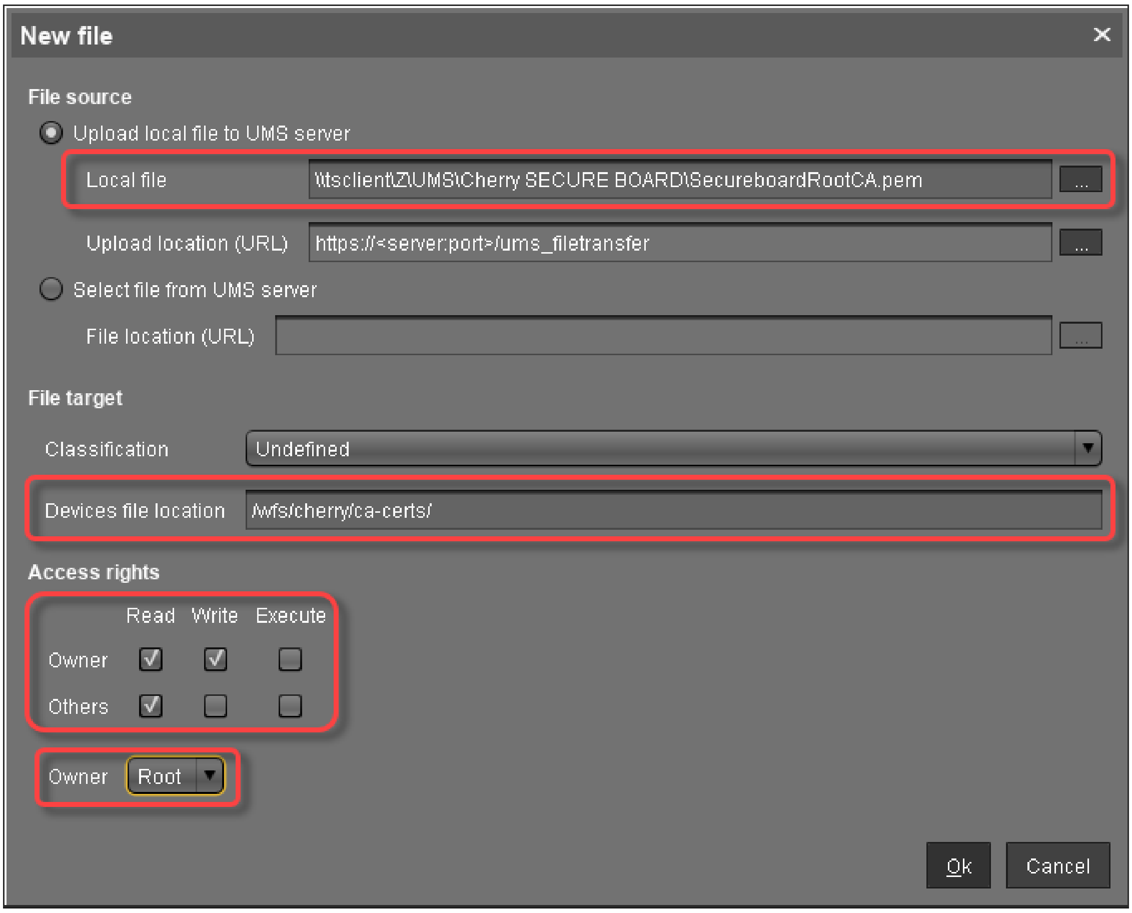
Creating the File Object for the Device Root CA Certificate

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:

- **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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\SecureboardRootCA.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/ca-certs/

Access rights

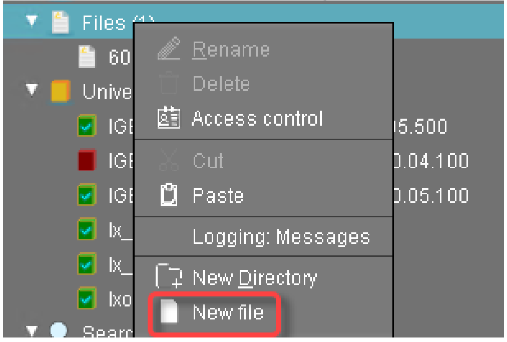
	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

Owner: Root

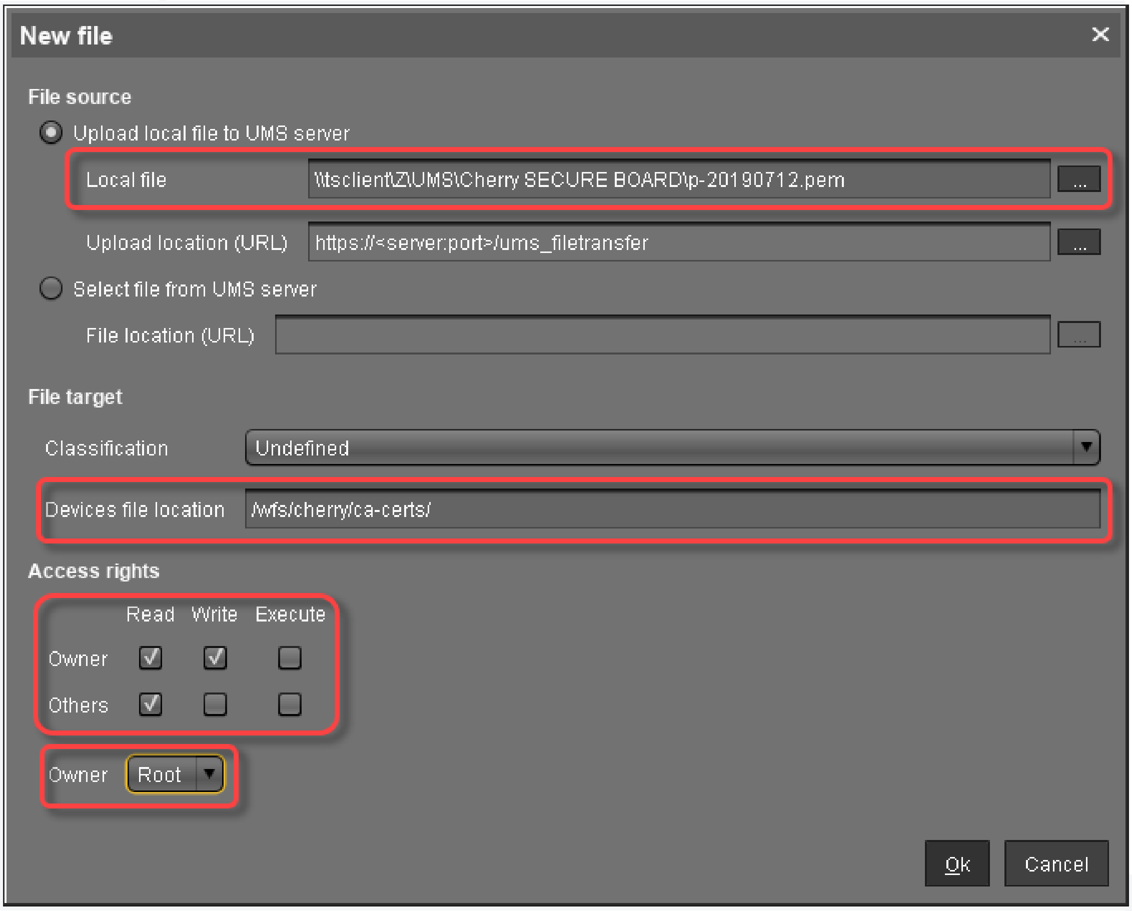
3. Click **Ok**.
   In the UMS, the file object **SecureBoardRootCA.pem** is created.

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:
   - **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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\p-20190712.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/ca-certs/

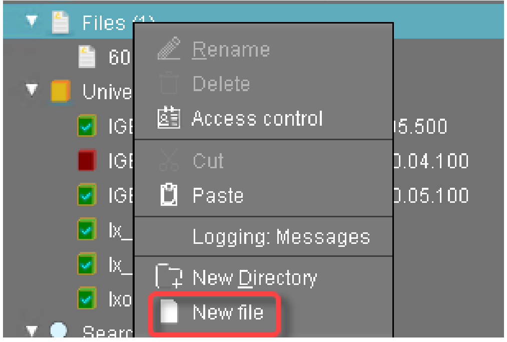
Access rights

	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

Owner: Root

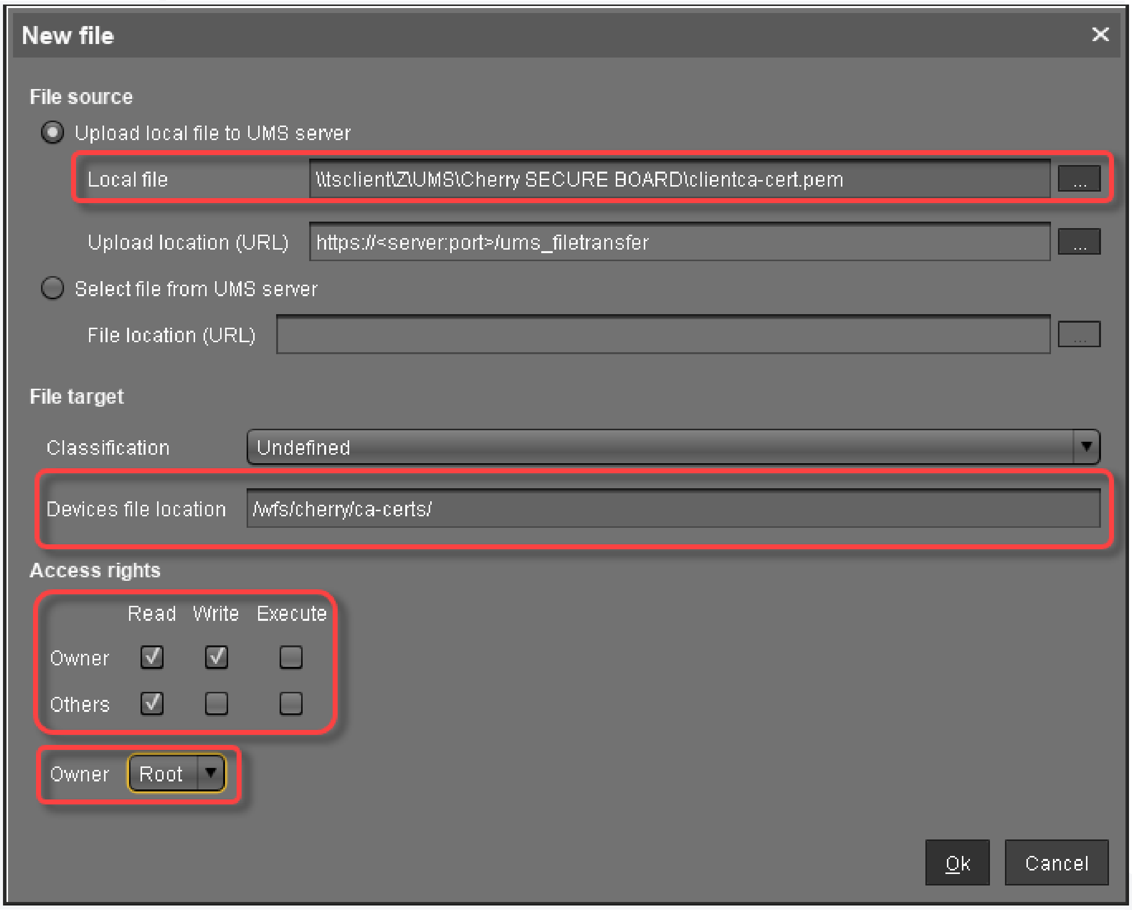
3. Click **Ok**.
   In the UMS, the file object **p-20190712.pem** is created.

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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\clientca-cert.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/ca-certs/

Access rights

	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

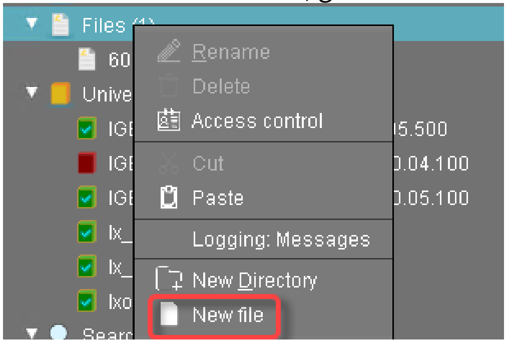
Owner: Root

3. Click **Ok**.
   In the UMS, the file object **clientca-cert.pem** is created.

Creating the File Object for the User Certificate (Keyboard)

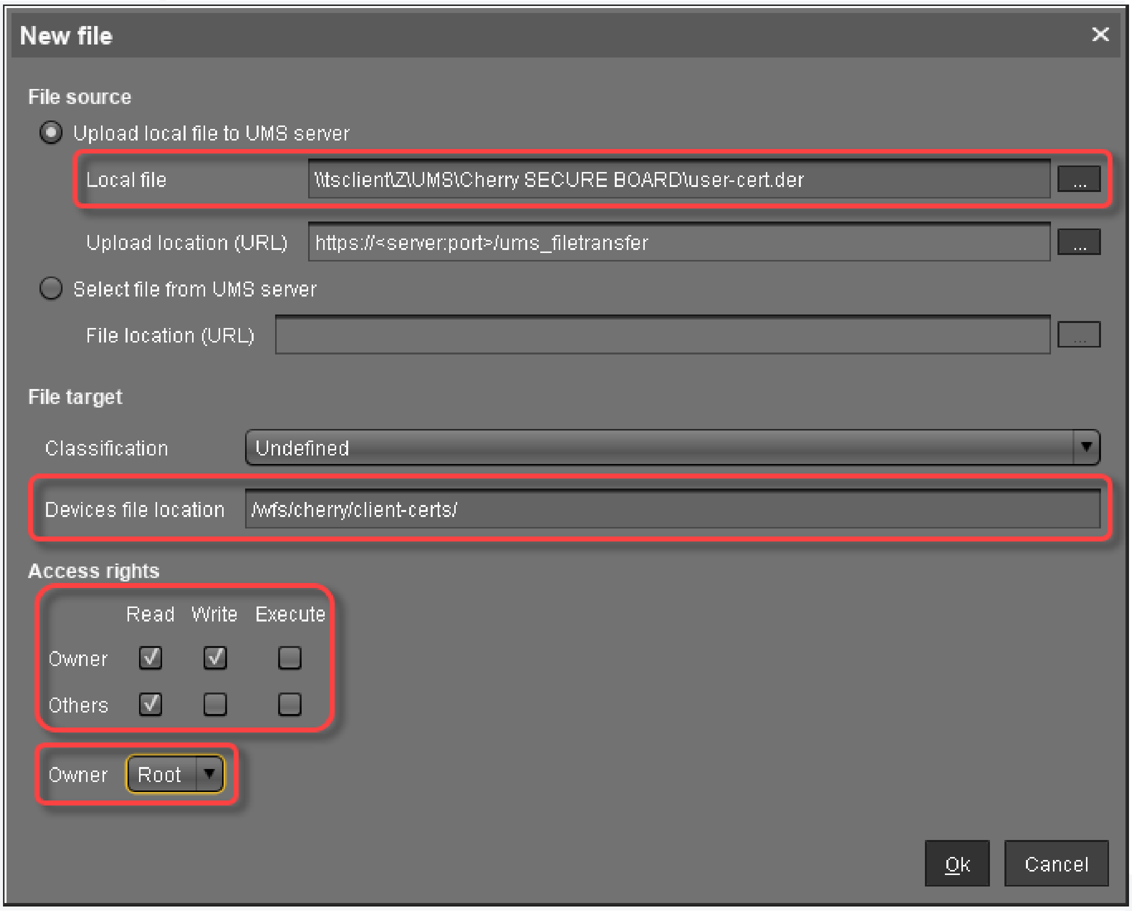
To transfer the certificate file `user-cert.der` to the directory `/wfs/cherry/client-certs/` on the personalization machine, proceed as follows:

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



New file ✕

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\user-cert.der ...

Upload location (URL): https://<server:port>/ums_filetransfer ...

○ Select file from UMS server

File location (URL): ...

File target

Classification: Undefined ▼

Devices file location: /wfs/cherry/client-certs/

Access rights

	Read	Write	Execute
Owner	☑	☑	☐
Others	☑	☐	☐

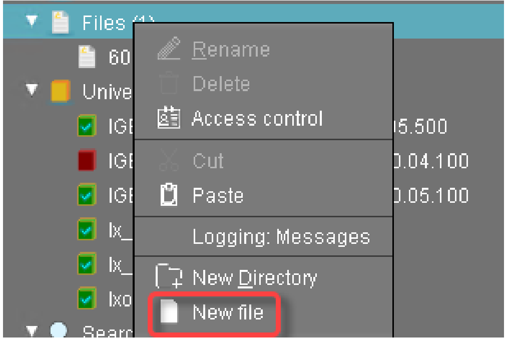
Owner: Root ▼

Ok Cancel

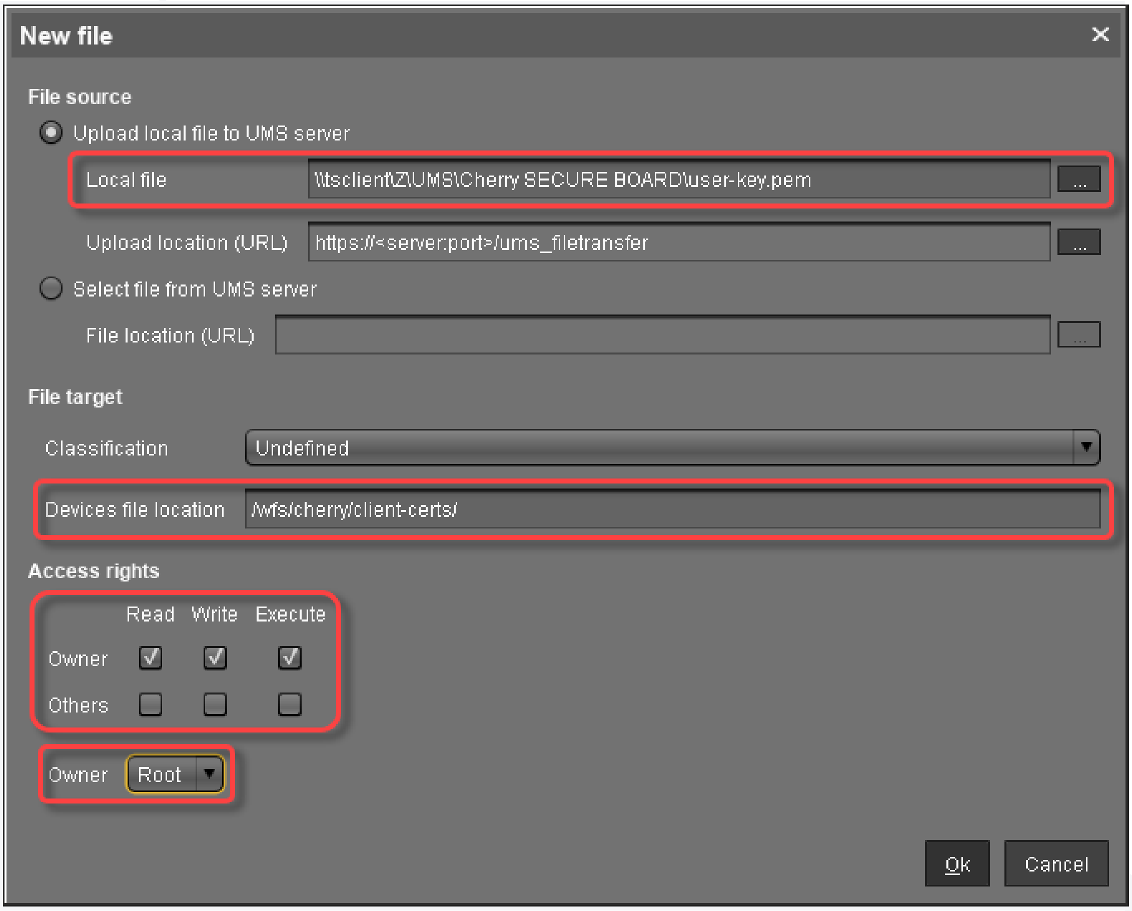
3. Click **Ok**.
   In the UMS, the file object **user-cert.der** is created.

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:
   - **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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\user-key.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/client-certs/

Access rights

	Read	Write	Execute
Owner	☑	☑	☑
Others	□	□	□

Owner: Root

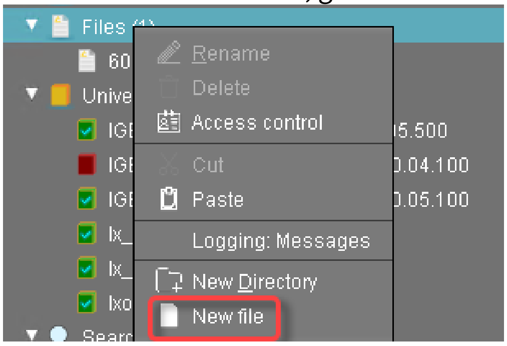
2. Click **Ok**.
   In the UMS, the file object **user-key.pem** is created.

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.

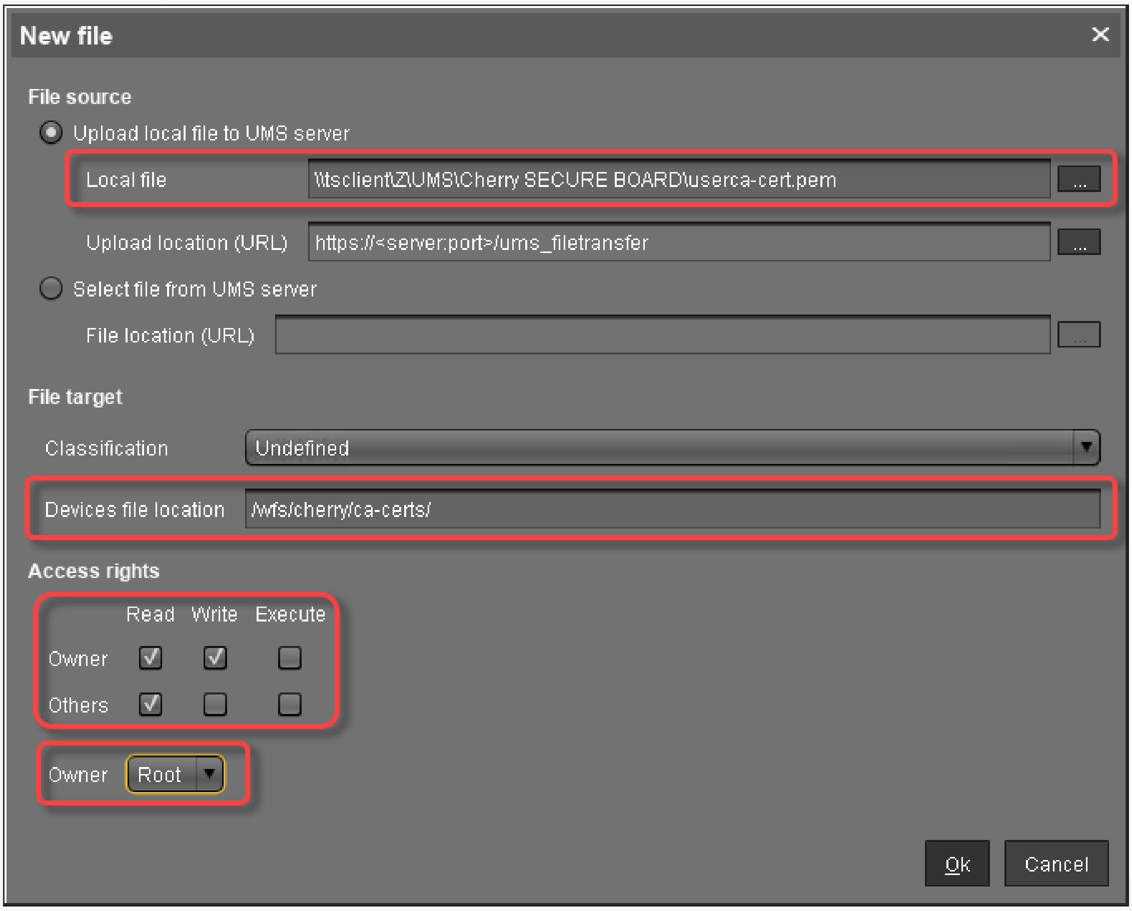
Creating the File Object for the User Root CA Certificate

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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\userca-cert.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/ca-certs/

Access rights

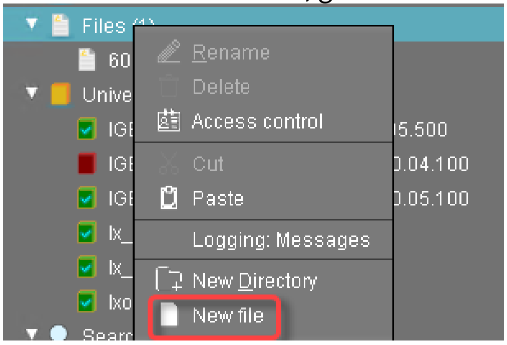
	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

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.

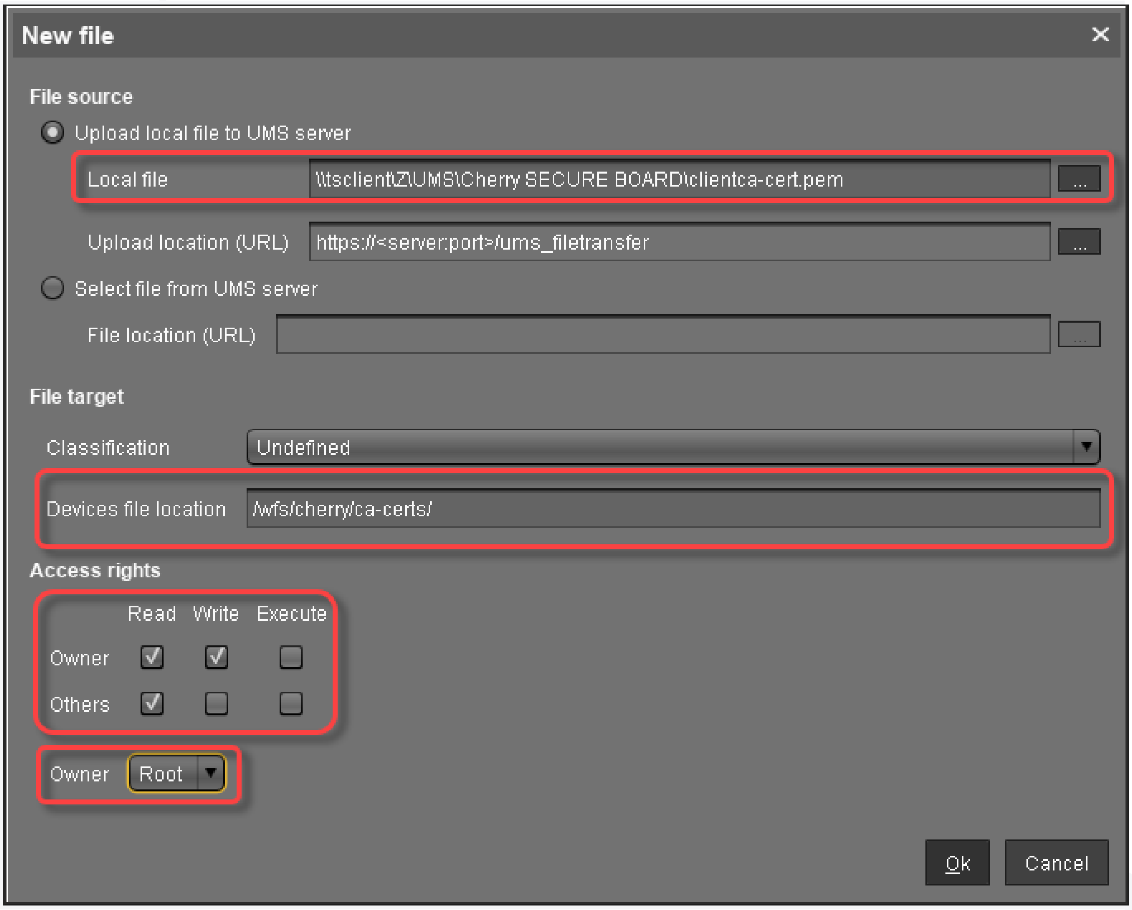
Creating the File Object for the Client Root CA Certificate (Optional)

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



New file

File source

● Upload local file to UMS server

Local file \\tsclient\Z\UMS\Cherry SECURE BOARD\clientca-cert.pem

Upload location (URL) https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL)

File target

Classification Undefined

Devices file location /wfs/cherry/ca-certs/

Access rights

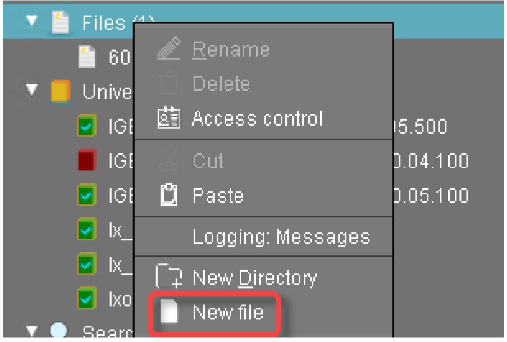
	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

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.

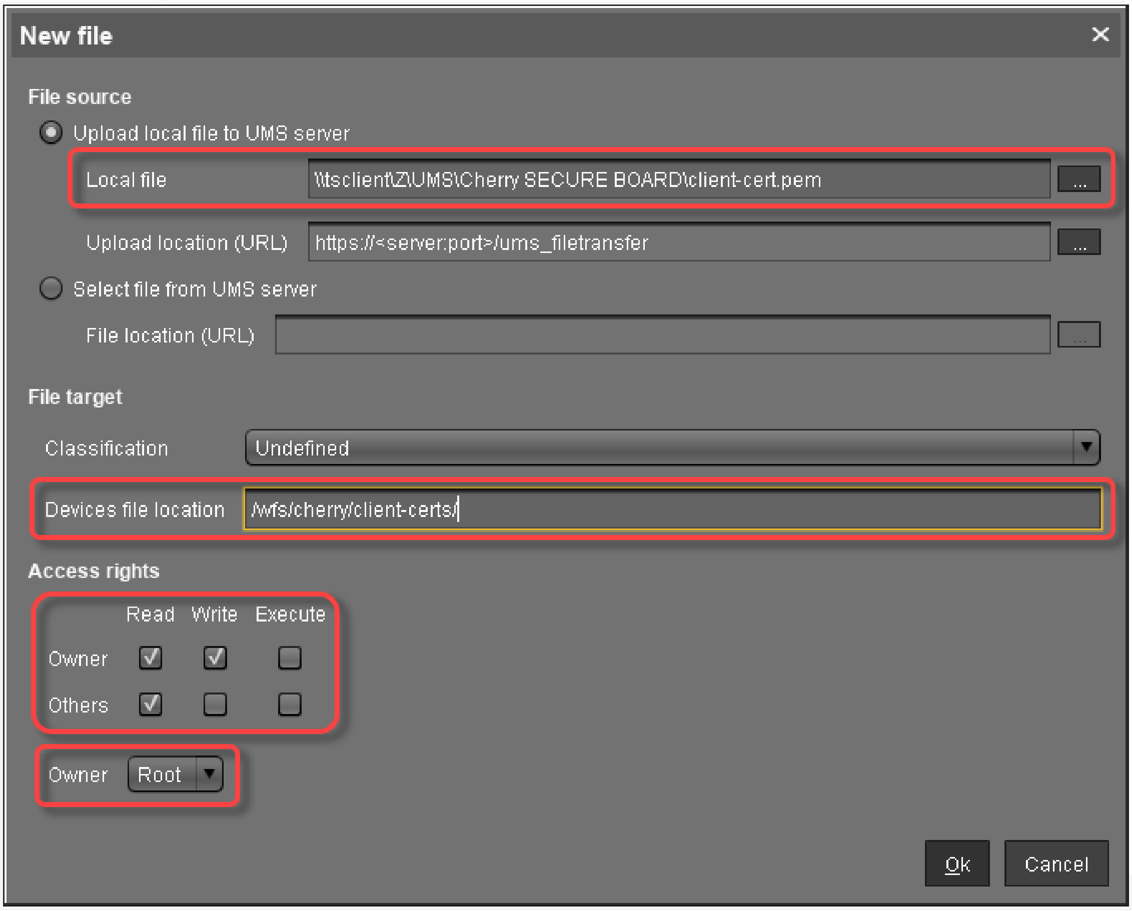
Creating the File Object for the Client Certificate (Endpoint) (Optional)

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:

- **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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\client-cert.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/client-certs/

Access rights

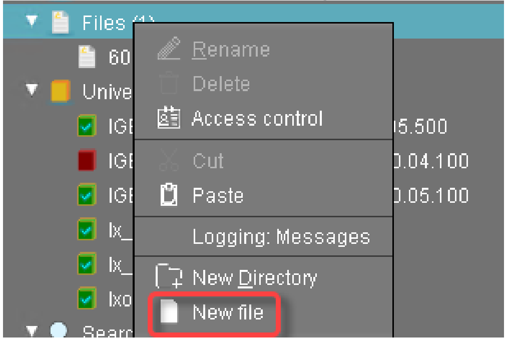
	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

Owner: Root

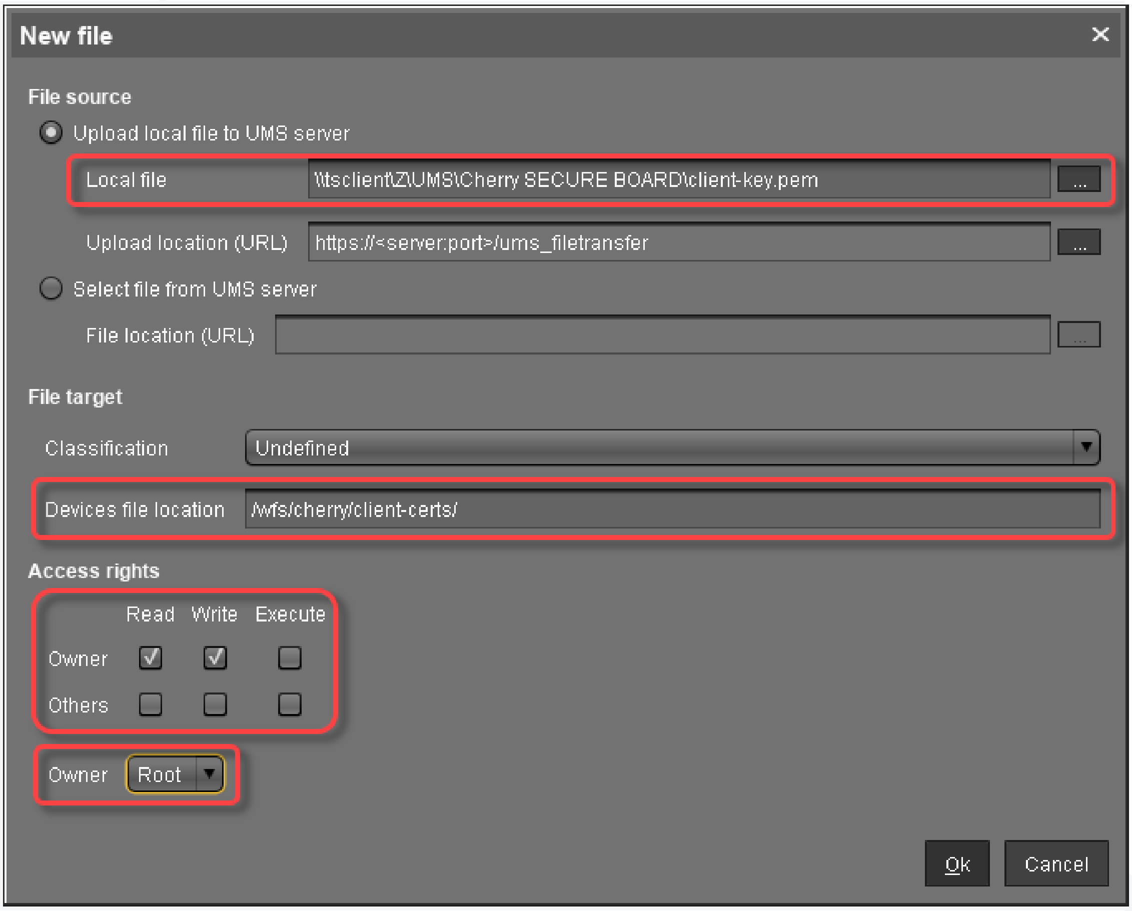
3. Click **Ok**.
   In the UMS, the file object is created. The name of the file object is derived from the file name.

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



New file

File source

● Upload local file to UMS server

Local file: \\tsclient\Z\UMS\Cherry SECURE BOARD\client-key.pem

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/client-certs/

Access rights

	Read	Write	Execute
Owner	☑	☑	□
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

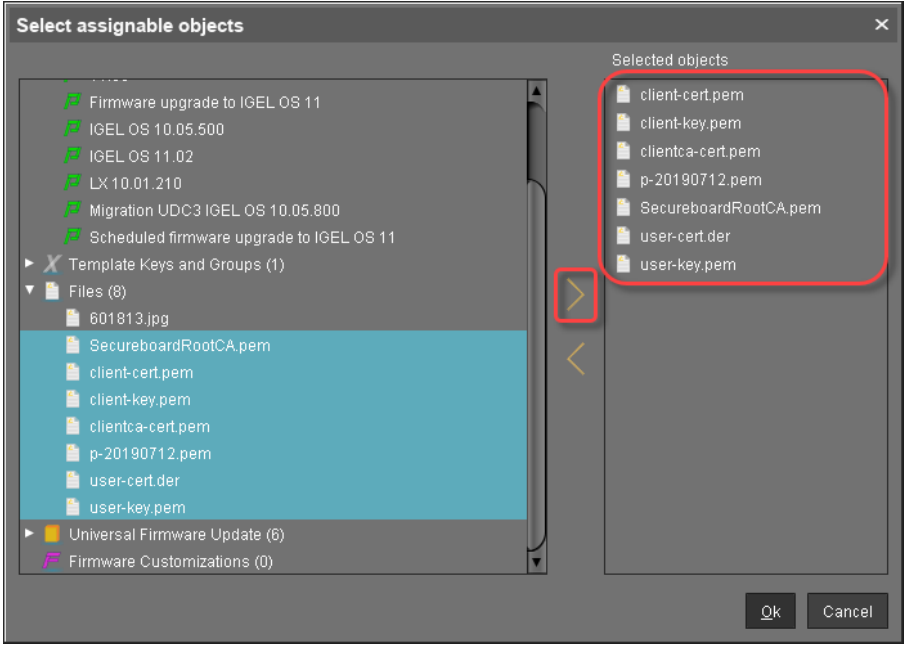
Setting Up the Local Terminal

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)



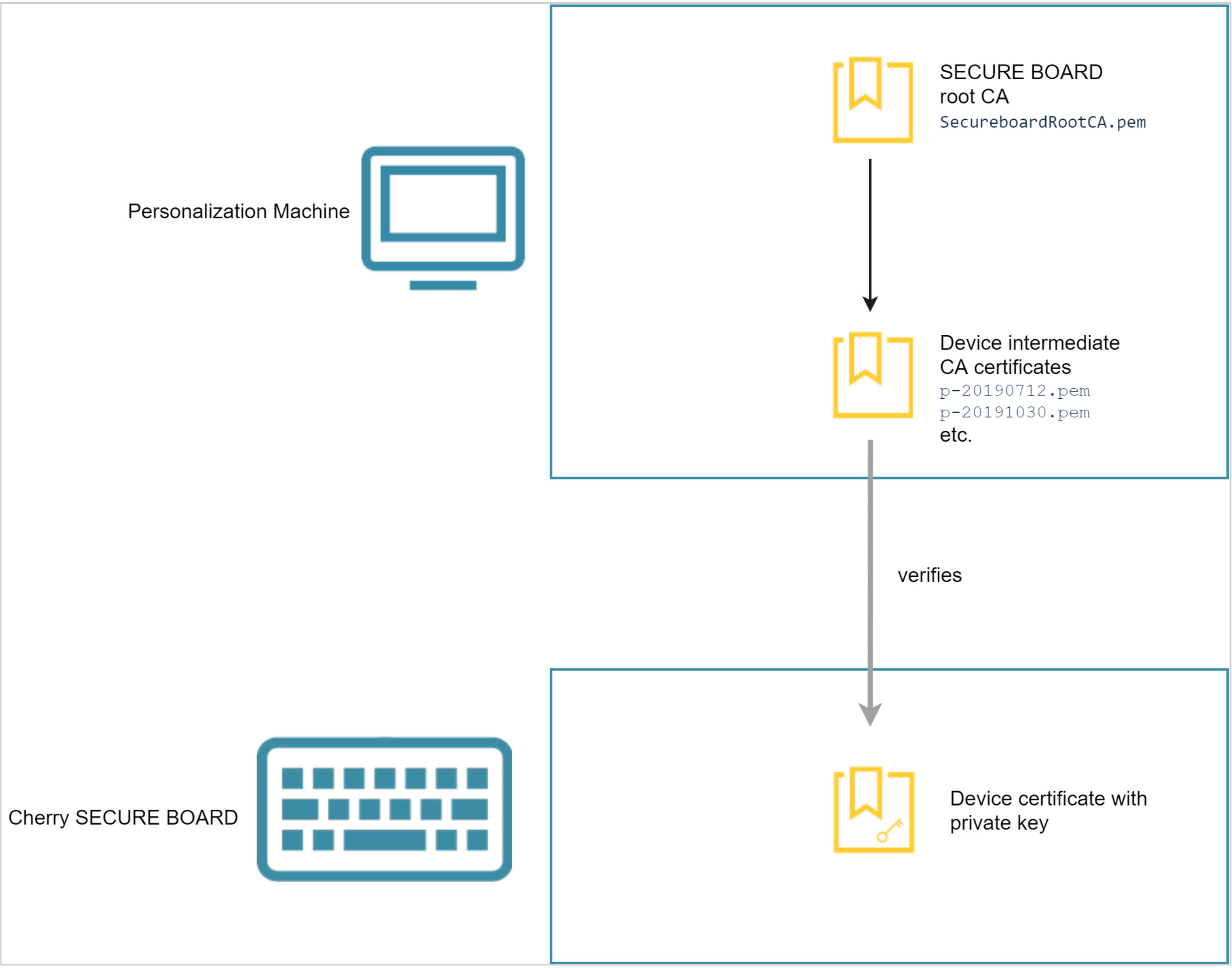
4. Click **Ok**.

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.

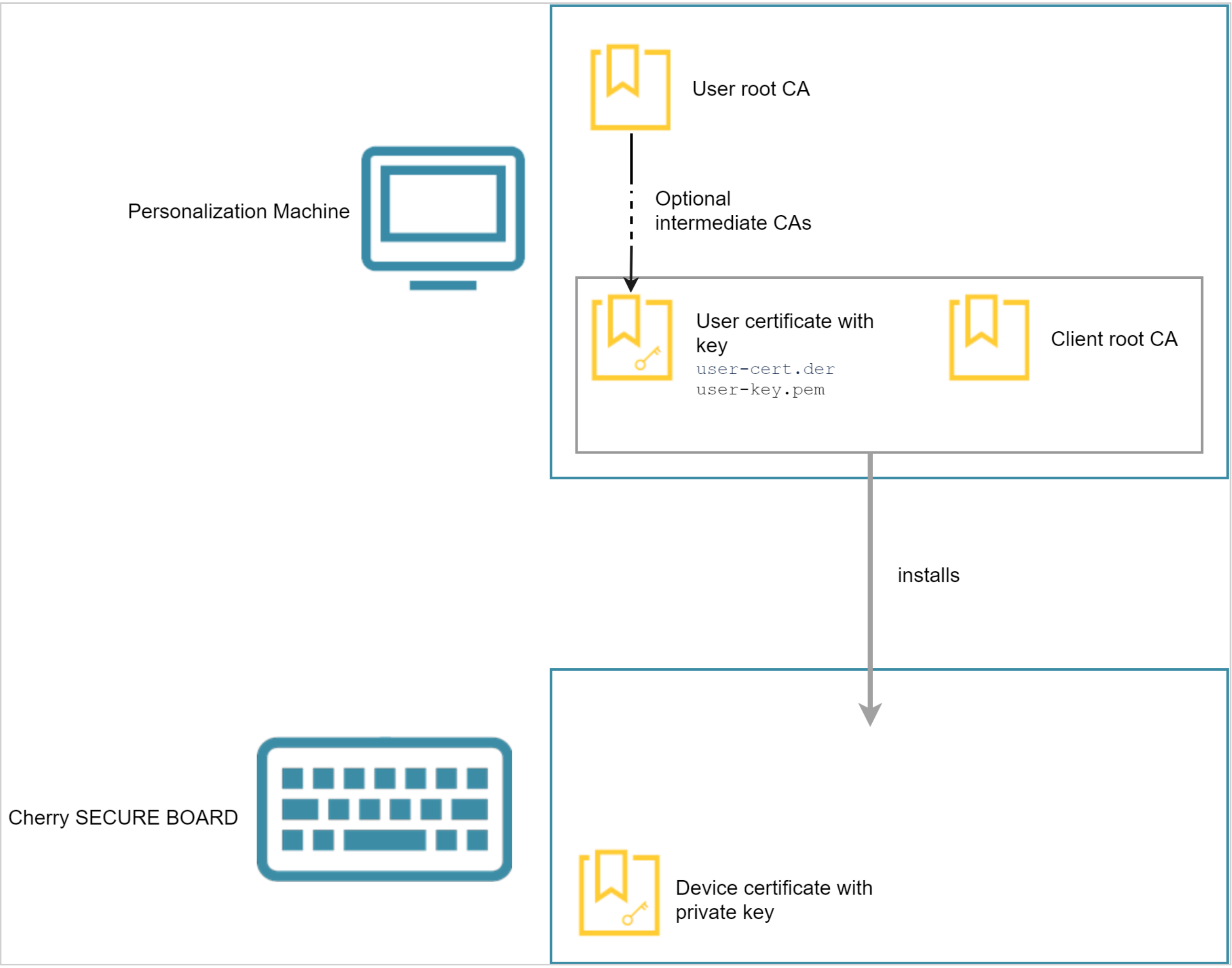
Personalizing the Cherry SECURE BOARD

Overview

Personalization Machine Verifies if the Keyboard Is a Genuine Cherry SECURE BOARD



Personalization Machine Installs the Certificates on the Keyboard

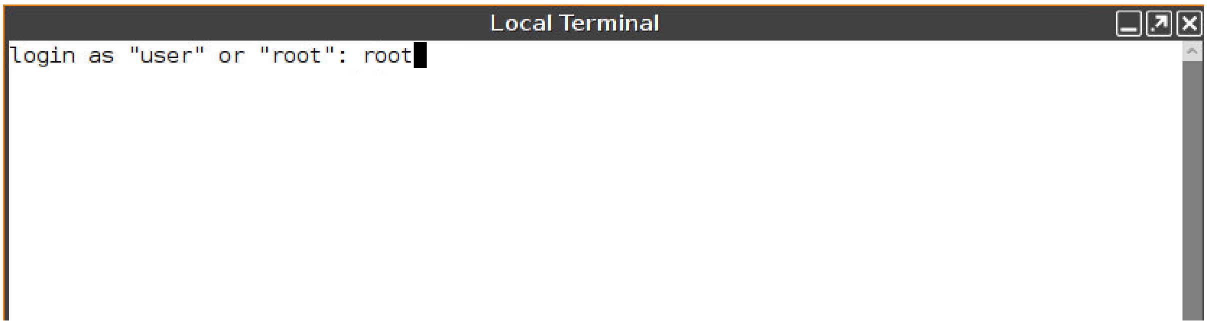


Prerequisites

- The machine has been prepared as described under Setting Up the Personalization Machine (see page 825).
- 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 835)).

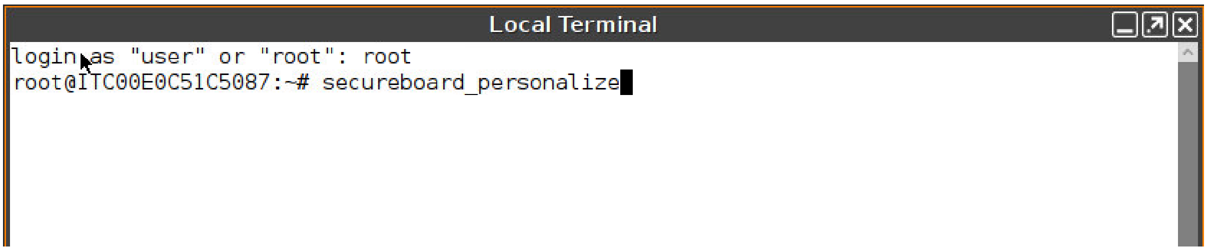
Instructions

1. Start the local terminal and log in as `root` .



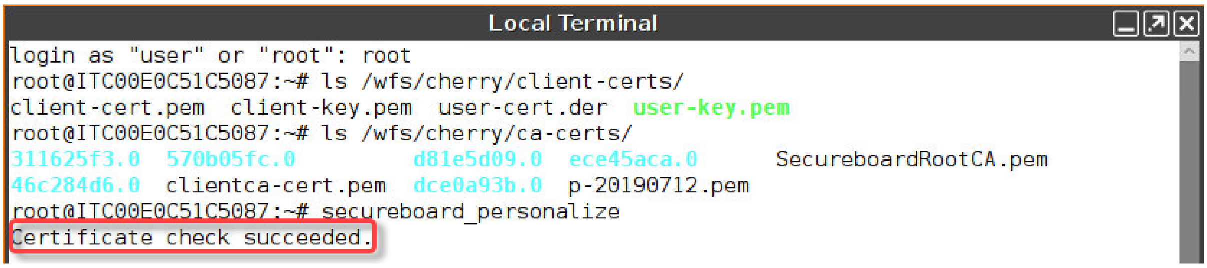
```
login as "user" or "root": root
```

2. Enter the command `secureboard_personalize`



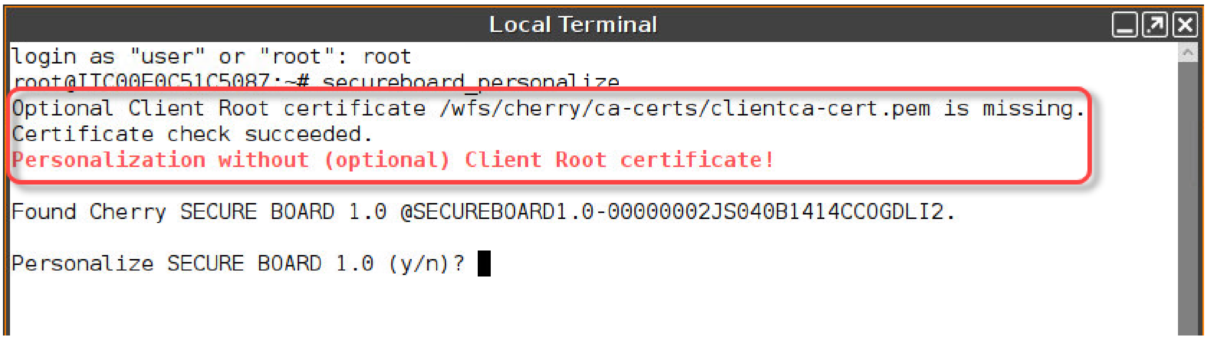
```
login as "user" or "root": root
root@ITC00E0C51C5087:~# secureboard_personalize
```

If all required certificates and the optional certificates for mutual authentication are present, the personalization facility is ready.



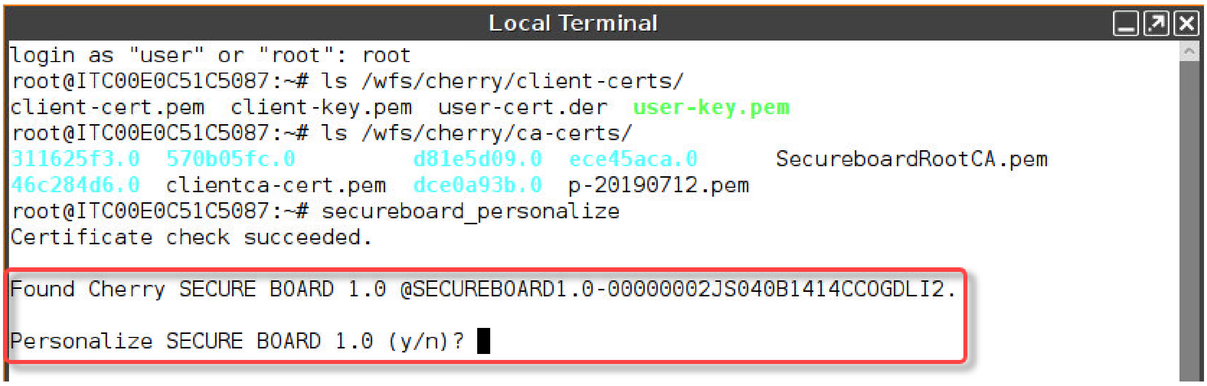
```
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem  client-key.pem  user-cert.der  user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0  570b05fc.0          d81e5d09.0  ece45aca.0      SecureboardRootCA.pem
46c284d6.0  clientca-cert.pem  dce0a93b.0  p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.
```

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:



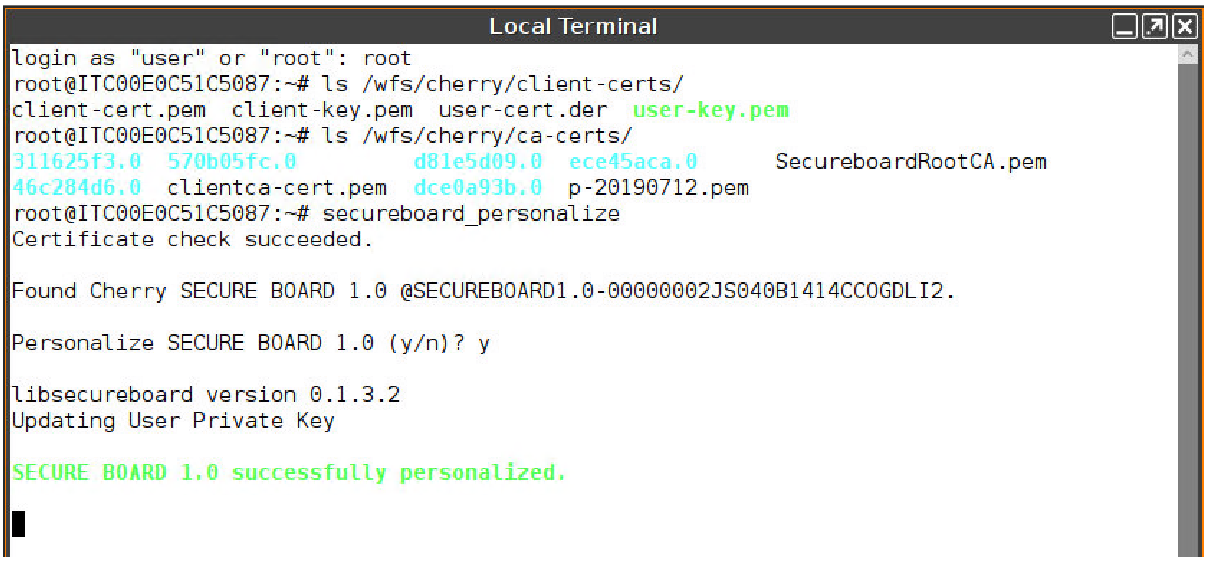
```
login as "user" or "root": root
root@ITC00E0C51C5087:~# secureboard_personalize
Optional Client Root certificate /wfs/cherry/ca-certs/clientca-cert.pem is missing.
Certificate check succeeded.
Personalization without (optional) Client Root certificate!

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGDLI2.

Personalize SECURE BOARD 1.0 (y/n)?
```

3. Plug in a Cherry SECURE BOARD.
   A message confirms that the keyboard has been detected; you are prompted to start the personalization.



```
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem  client-key.pem  user-cert.der  user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0  570b05fc.0         d81e5d09.0  ece45aca.0      SecureboardRootCA.pem
46c284d6.0  clientca-cert.pem  dce0a93b.0  p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGDLI2.

Personalize SECURE BOARD 1.0 (y/n)?
```

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.



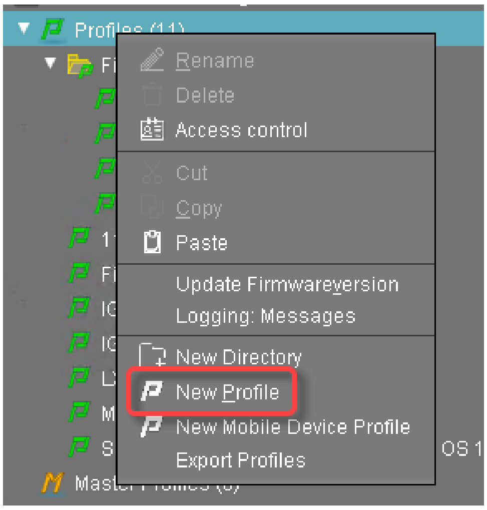
```
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem  client-key.pem  user-cert.der  user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0  570b05fc.0         d81e5d09.0  ece45aca.0      SecureboardRootCA.pem
46c284d6.0  clientca-cert.pem  dce0a93b.0  p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGDLI2.

Personalize SECURE BOARD 1.0 (y/n)? y

libsecureboard version 0.1.3.2
Updating User Private Key

SECURE BOARD 1.0 successfully personalized.
```

5. Unplug the personalized Cherry SECURE BOARD and proceed with the next Cherry SECURE BOARD.

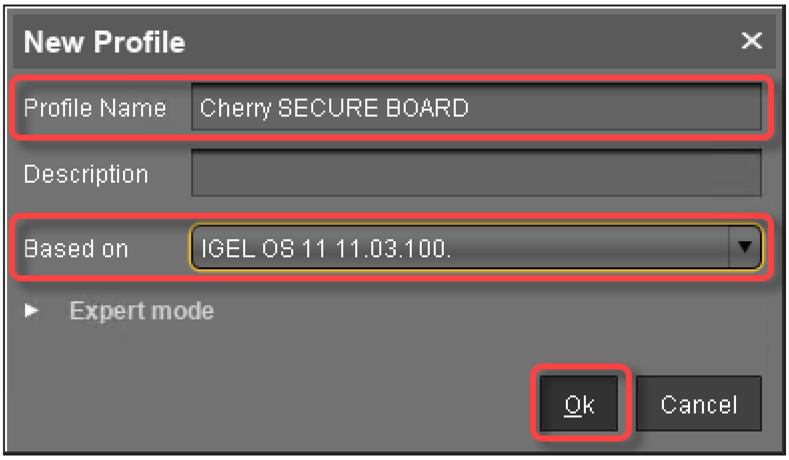
Setting Up the Endpoints

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).

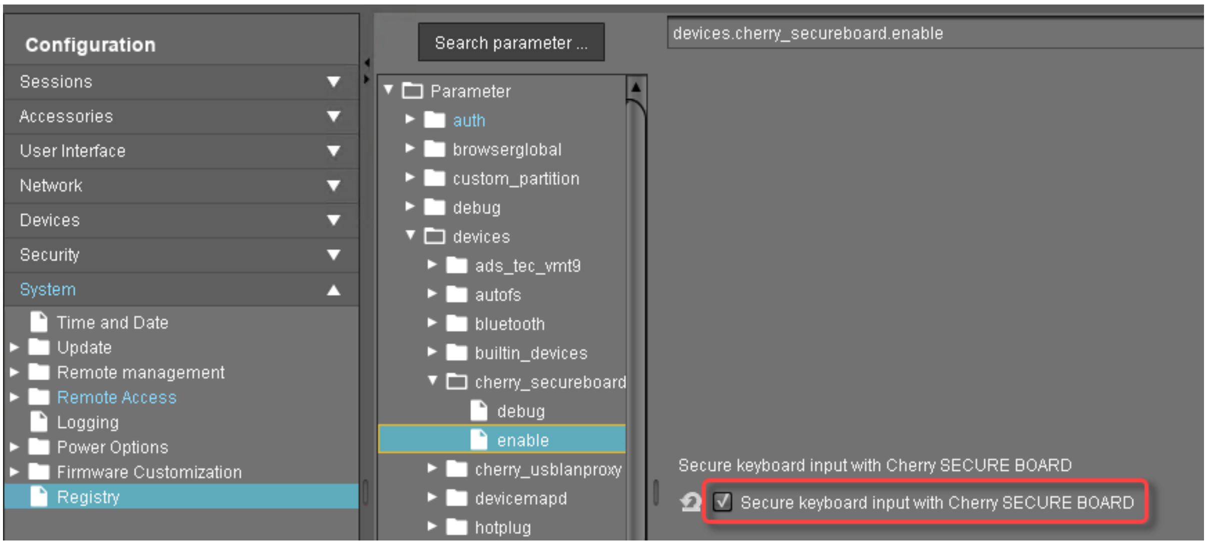

New Profile

Profile Name: Cherry SECURE BOARD

Description:

Based on: IGEL OS 11 11.03.100.

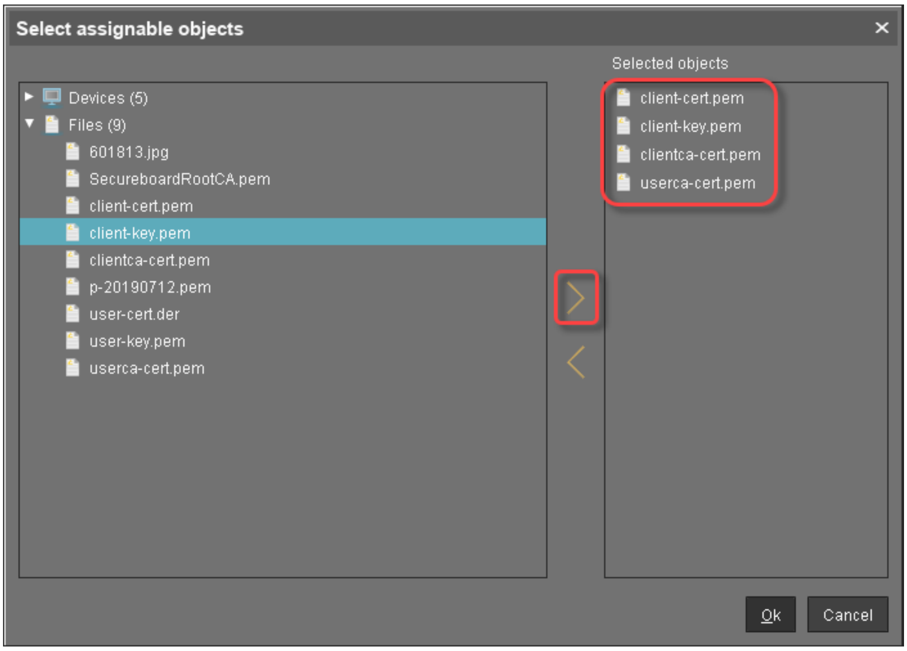
3. In the configuration dialog of the profile, go to **System > Registry > devices > cherry_secureboard > enable** and activate **Secure keyboard input with Cherry SECURE BOARD** (registry key: `devices.cherry_secureboard.enable`). (From UMS 6.03.130 or higher, the parameter can be found under **User Interface > Input > Keyboard**)



Secure keyboard input with Cherry SECURE BOARD

☑ Secure keyboard input with Cherry SECURE BOARD

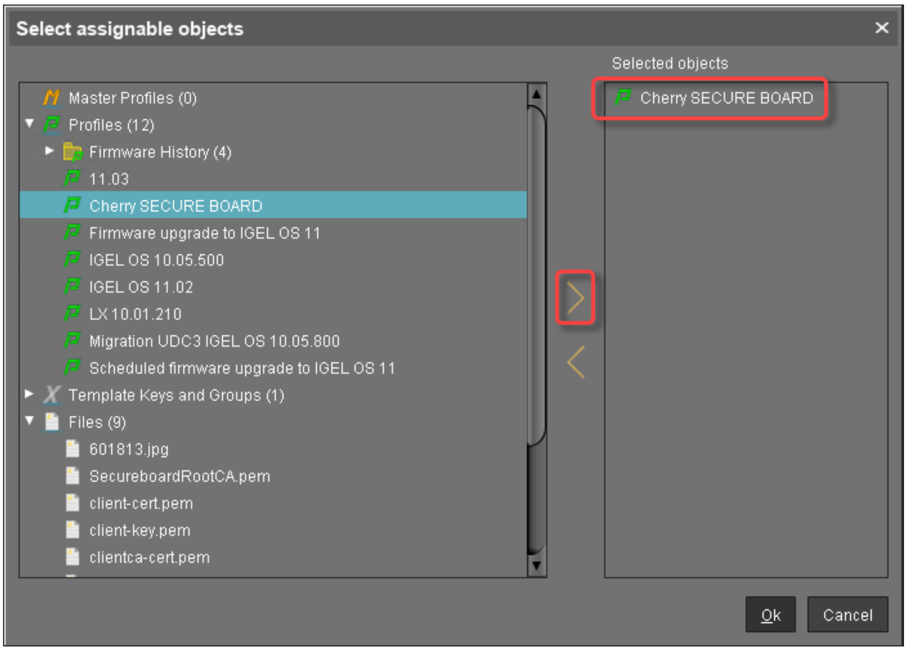
4. Click **Ok** to save and close the profile.
5. Make sure that the profile is selected in the UMS structure tree.
6. In the **Assigned objects** area, click ⊕.
7. Under **Files**, select the file objects using the > button:
   - User root CA certificate; here: **userca-cert.pem**
   - Client root CA 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.



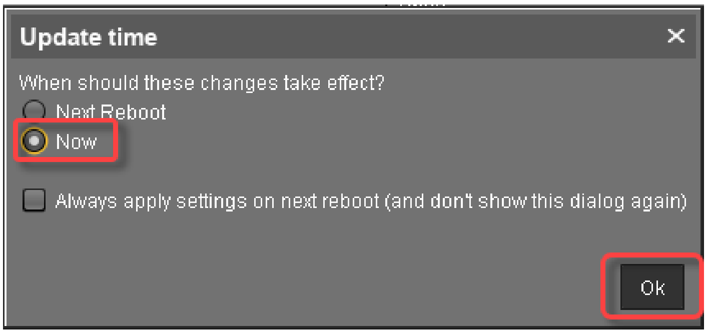
Select assignable objects ✕

- Master Profiles (0)
- ▼ Profiles (12)
  - ▶ Firmware History (4)
  - 11.03
  - Cherry SECURE BOARD
  - Firmware upgrade to IGEL OS 11
  - IGEL OS 10.05.500
  - IGEL OS 11.02
  - LX 10.01.210
  - Migration UDC3 IGEL OS 10.05.800
  - Scheduled firmware upgrade to IGEL OS 11
- ▶ Template Keys and Groups (1)
- ▼ Files (9)
  - 601813.jpg
  - SecureboardRootCA.pem
  - client-cert.pem
  - client-key.pem
  - clientca-cert.pem

Selected objects

- Cherry SECURE BOARD

4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.



Update time ✕

When should these changes take effect?

○ Next Reboot
● Now

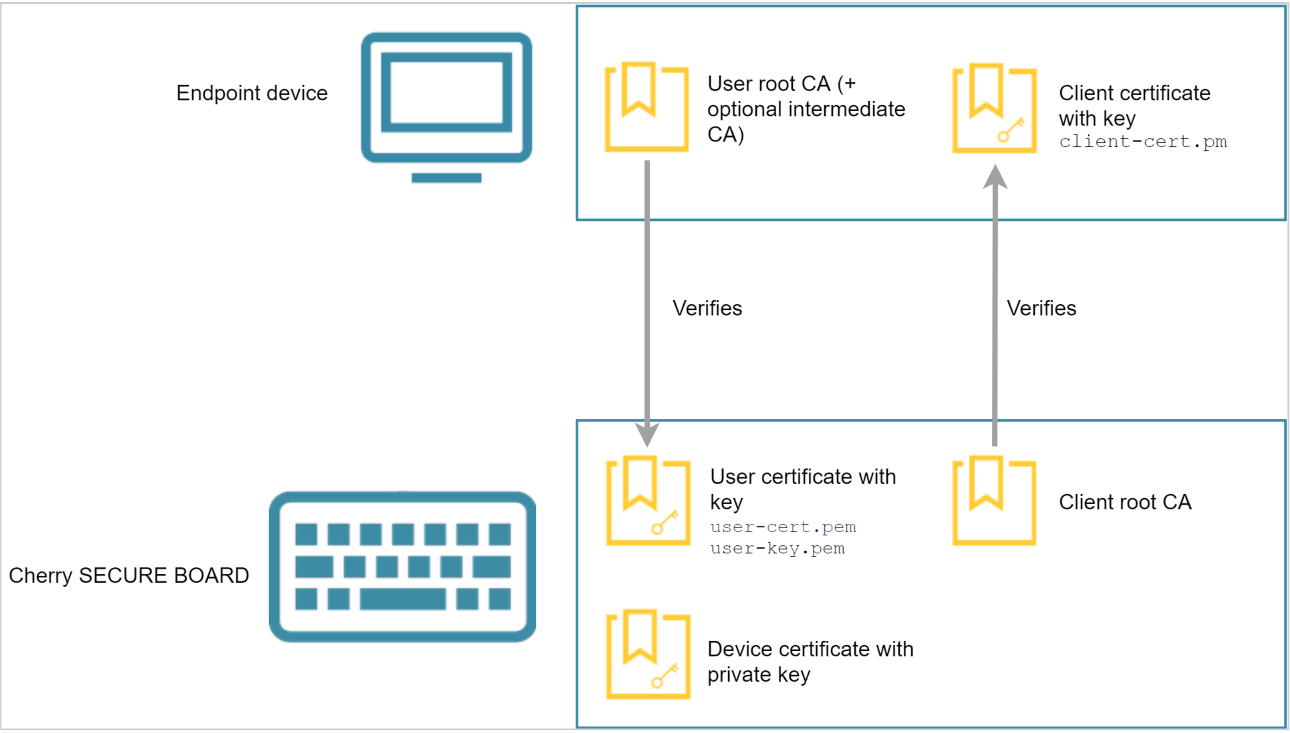
□ Always apply settings on next reboot (and don't show this dialog again)

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.


Endpoint device
User root CA (+ optional intermediate CA)
Client certificate with key
client-cert.pm
Verifies
Verifies
Cherry SECURE BOARD
User certificate with key
user-cert.pem
user-key.pem
Client root CA
Device certificate with private key

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

Overview

This article provides an overview and best-practice recommendations for the use of webcams on IGEL OS within remote sessions such as Citrix, VMware Horizon, and RDP.

In general, webcam support on 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.

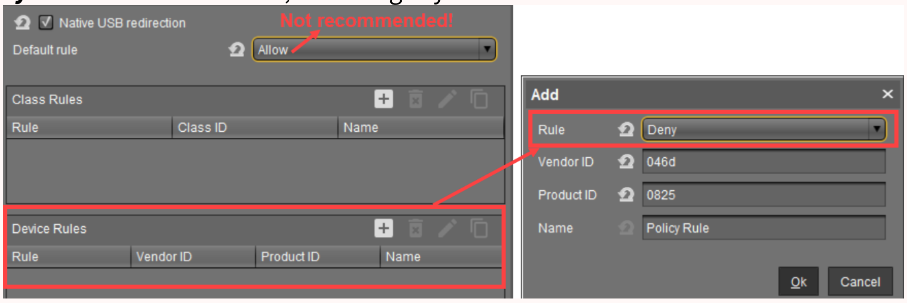
General Recommendations

For optimal performance of webcams on IGEL OS, the correct optimization pack has to be enabled for the specific application, e.g. **Microsoft Teams optimization**, **Zoom Media plugin**, **Cisco Webex Teams 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.



☑ Native USB redirection

Not recommended!

Default rule: Allow

Rule: Deny
Vendor ID: 046d
Product ID: 0825
Name: Policy Rule

This is necessary because USB redirection will block the webcam from being correctly optimized (if optimization is possible).

Always check the IGEL OS release notes for specific remarks, especially in the case of private builds. Always try to use the latest firmware, see IGEL download server[49].

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.

[49] 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** (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. For server-side requirements for Microsoft Teams optimization, see Microsoft Teams installation[50]. To troubleshoot Microsoft Teams optimization in Citrix, see: - Troubleshooting HDX Optimization for Microsoft Teams[51] - Peripherals in Microsoft Teams[52]
Zoom Media Plugin	Path: **Sessions > Citrix > Citrix Global > Unified Communications > VDI Solutions > Zoom Media Plugin** - Available as of IGEL OS version 11.04.100 - For the Zoom Media Plugin versions included, see IGEL OS release notes. For more information about Zoom Media Plugin, including server-side requirements, see Getting started with VDI[53].

[50] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-teams-installation
[51] https://support.citrix.com/article/CTX253754
[52] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#peripherals-in-microsoft-teams
[53] https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI

Cisco Webex Meetings / Teams VDI	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco > Cisco Webex Meetings VDI** or **Cisco Webex Teams VDI** • Available as of IGEL OS version 11.04.100 • For the Cisco Webex Meetings / Teams VDI versions included, see IGEL OS release notes. For more information about Cisco Webex products for VDI, including supported environments, see: • Cisco Webex Meetings Virtual Desktop Software[54] • Overview of Webex Teams for VDI[55]
Cisco JVDI Client	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Cisco > Cisco JVDI client** • For the Cisco JVDI client versions included, see IGEL OS release notes. For more information about Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI[56].
Skype for Business	Path: **Sessions > Citrix > Citrix Global > Unified Communications > Skype for Business > HDX RealTime Media Engine** (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[57]. After this, it will no longer be available, and Microsoft Teams must be used instead.

[54] https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software

[55] 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

[56] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html

[57] 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 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** should not be enabled at the same time.
> - If you use HDX or an application-specific optimization pack (e.g. **Zoom 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. For more information, see How to Configure Webcam settings When Webcams are Not Redirected Through HDX Real-Time[58]. 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 837).

Dependencies

- **HDX RealTime Webcam Redirection** is only 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[59]. See also https://support.citrix.com/article/CTX223199.

[58] https://support.citrix.com/article/CTX134772

[59] http://www.webcamtests.com

- 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 838))
- 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 838))
- 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 838).

> ✓ **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)

Zoom Media Plugin	Path: **System > Registry > vmware > view > vdzoom > enable** • Available as of IGEL OS version 11.04.200 • For the Zoom Media Plugin versions included, see IGEL OS release notes. ⚠ Zoom Media Plugin will NOT function if you enable **HTML5 multimedia redirection** (**System > Registry > vmware > view > html5mmr**, disabled by default). For more information about Zoom Media Plugin, including server-side requirements, see Getting started with VDI[60].
Cisco Webex Teams VDI	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Cisco > Cisco Webex Teams VDI** • Available as of IGEL OS version 11.04.100 • For the Cisco Webex Teams VDI versions included, see IGEL OS release notes. For more information, see Overview of Webex Teams for VDI[61].
Cisco JVDI Client	Path: **Sessions > Horizon Client > Horizon Client Global> Unified Communications > Cisco > Cisco JVDI client** • For the Cisco JVDI client versions included, see IGEL OS release notes. For more information about Cisco JVDI client, see Deployment and Installation Guide for Cisco Jabber Softphone for VDI[62].

[60] https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI

[61] 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

[62] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/12_9/dig/jvdi_b_deploy-install-jvdi-12-9/jvdi_b_deploy-install-jvdi-12-9_chapter_01.html

Skype for Business	Path: **Sessions > Horizon Client > Horizon Client Global > Unified Communications > Skype for Business > Virtualization Pack Skype for Business** (enabled by default) **IMPORTANT:** Skype for Business Online will be retired by Microsoft on July 31, 2021[63]. 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.

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)**.

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[64].

For more information about RTAV, see Configuring Real-Time Audio-Video[65].

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[66].
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[67].

[63] https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833
[64] https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-remote-desktop-features/GUID-C8C17975-AA1E-4378-A305-00E02FF93201.html
[65] https://docs.vmware.com/en/VMware-Horizon-7/7.6/horizon-remote-desktop-features/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html
[66] https://docs.vmware.com/en/VMware-Horizon/2006/horizon-remote-desktop-features/GUID-E64B3E85-BA1E-4FB7-9DB4-FF9B7B7A892C.html
[67] https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon

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

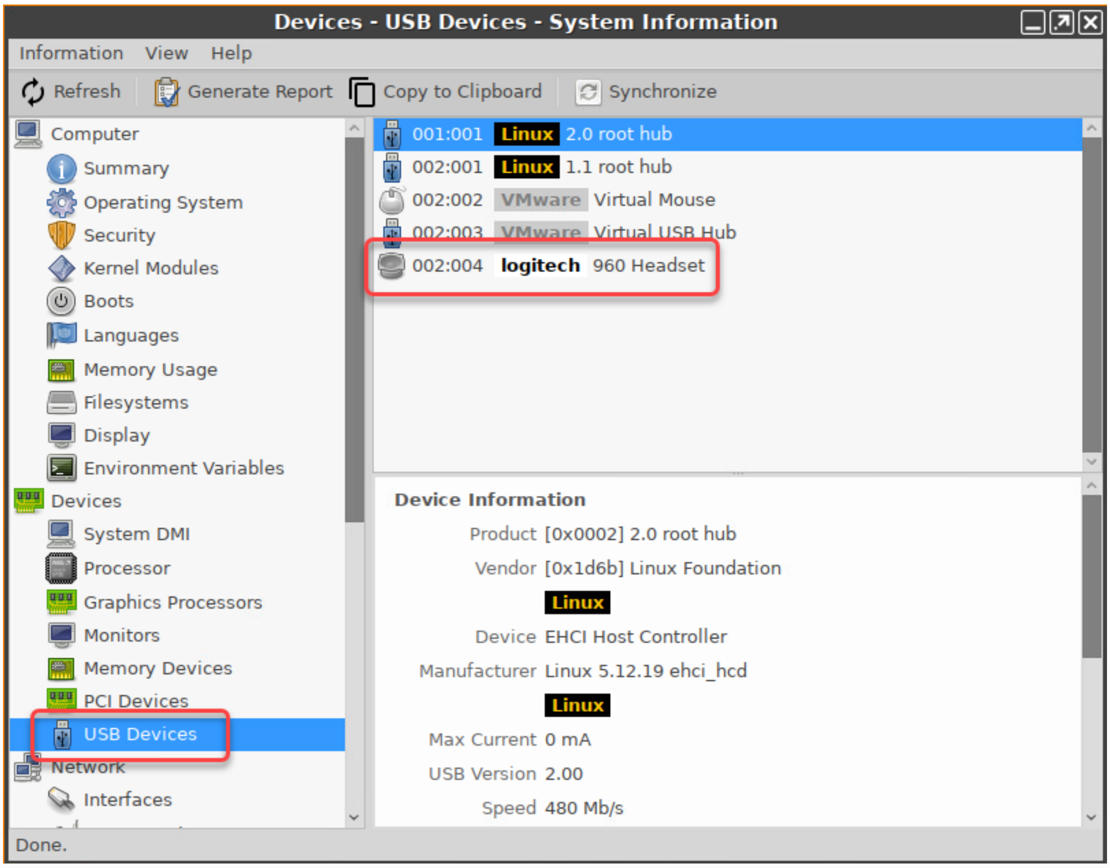
- Note that because USB redirection is not designed for redirecting video devices, the bandwidth usage and server CPU load may increase significantly.
- For this reason, it is recommended to use webcams that output directly H.264 or H.265 streams, and not MJPEG, in order to reduce the data volume.

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.
System Information example:



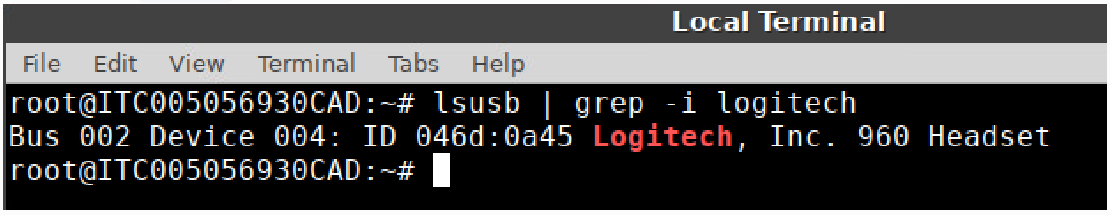
001:001 Linux 2.0 root hub
002:001 Linux 1.1 root hub
002:002 VMware Virtual Mouse
002:003 VMware Virtual USB Hub
002:004 logitech 960 Headset

Device Information

Product	[0x0002] 2.0 root hub
Vendor	[0x1d6b] Linux Foundation Linux
Device	EHCI Host Controller
Manufacturer	Linux 5.12.19 ehci_hcd Linux
Max Current	0 mA
USB Version	2.00
Speed	480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~# 
```

ⓘ 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 658) 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 Microsoft Teams as a Custom Partition (see page 709), Zoom as a Custom Partition (see page 688).
- 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[68].

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

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

[68] 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.

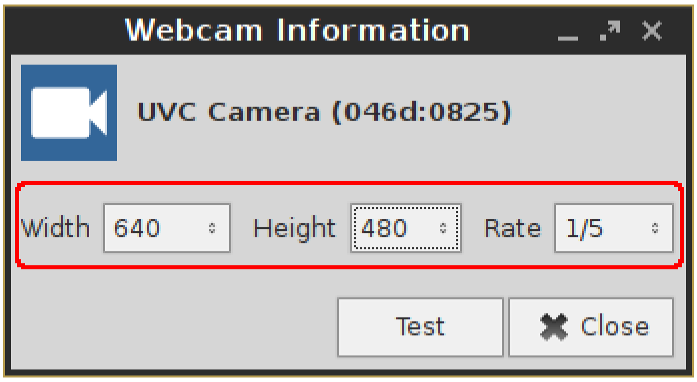
Webcam Information

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.

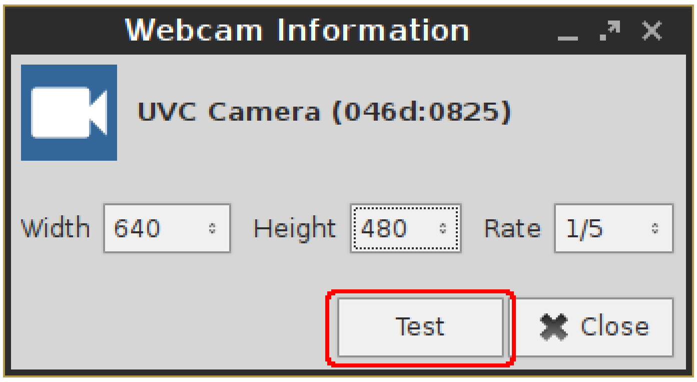


Webcam Information

UVC Camera (046d:0825)

Width 640 Height 480 Rate 1/5

2. Click on on one of the fields to change the value. In doing so, the supported values are shown.
3. Click **Test**.

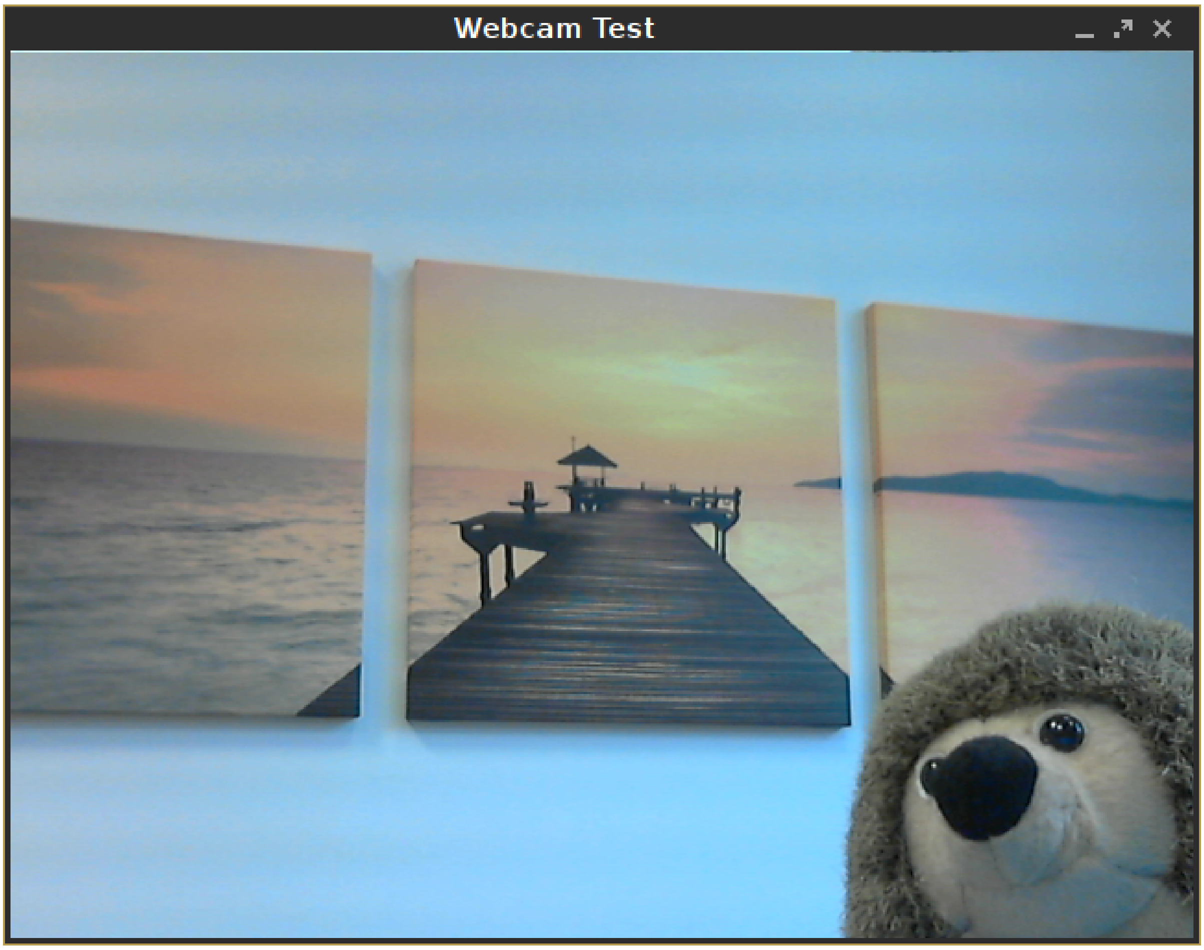


Webcam Information

UVC Camera (046d:0825)

Width 640 Height 480 Rate 1/5

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/.

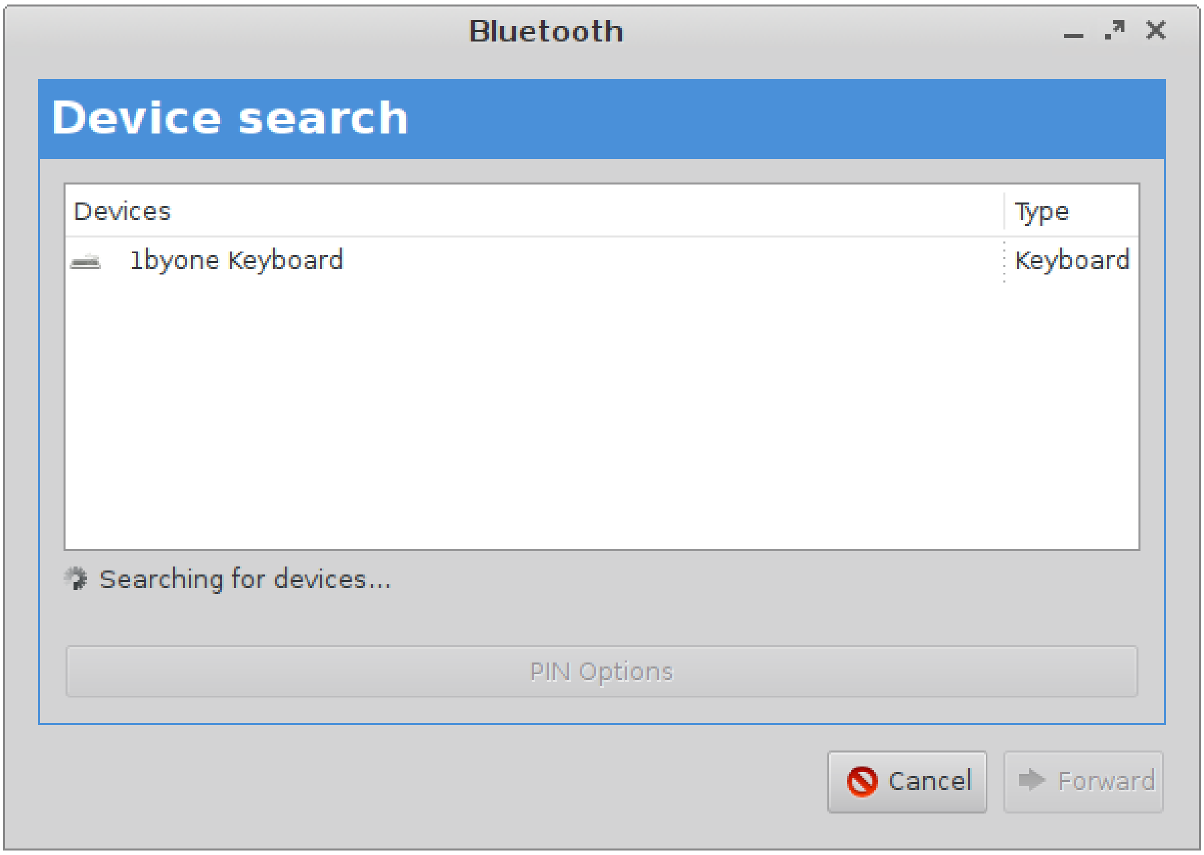
Bluetooth Tool

As of *IGEL Linux* version *5.10.100*, you can connect or disconnect Bluetooth devices conveniently using the Bluetooth tool. The Bluetooth tool supports the following pairing methods:

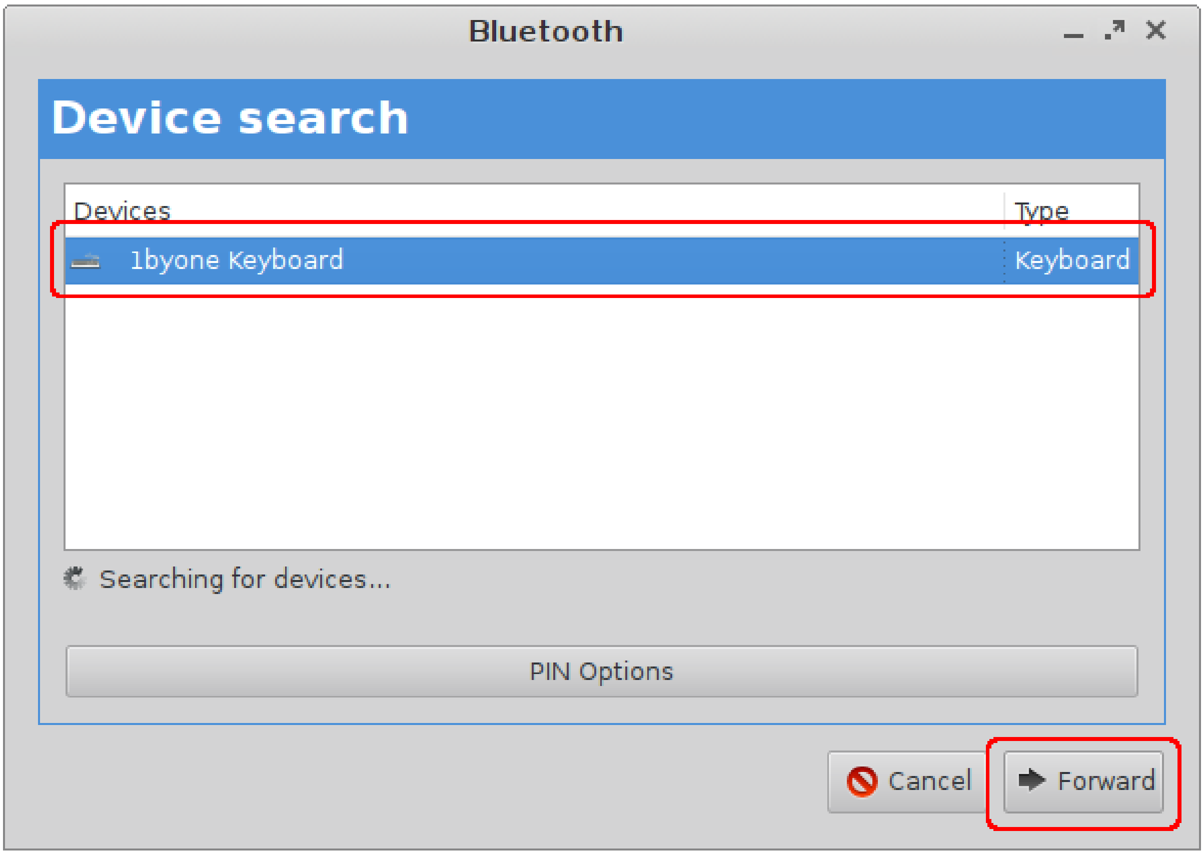
- Pairing with PIN entry (for most keyboards)
- Pairing with fixed PIN (for most headsets, mice or GPS devices)
- Pairing with automatic PIN allocation
  For further information, please refer to the manual chapter Bluetooth Tool.

In the following example, we will connect a Bluetooth device with PIN entry:

1. Make sure that the following preconditions are met:
   - A Bluetooth USB adapter is connected to your device.
   - The Bluetooth device is ready.
   - The options **Setup > Devices > Activate Bluetooth** and **Setup > Devices > Tray Icon** are enabled.
2. Launch the **Bluetooth Tool** via **> System > Bluetooth Tool** or another launch option, if available.
   The **Device search** dialog will be shown. After a few seconds, the Bluetooth devices found by the device are displayed.



3. Highlight the desired Bluetooth device and click on **Forward**.



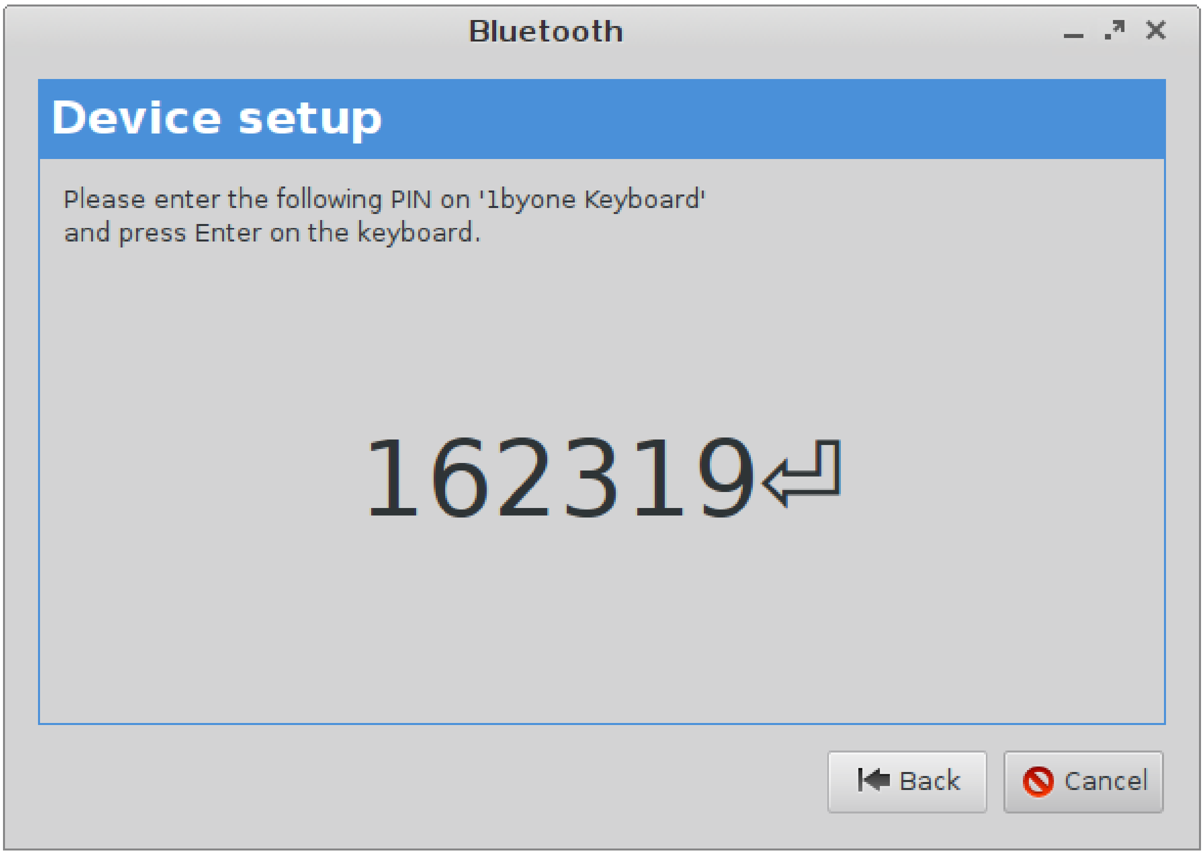
Bluetooth

Device search

Devices	Type
1byone Keyboard	Keyboard

Searching for devices...

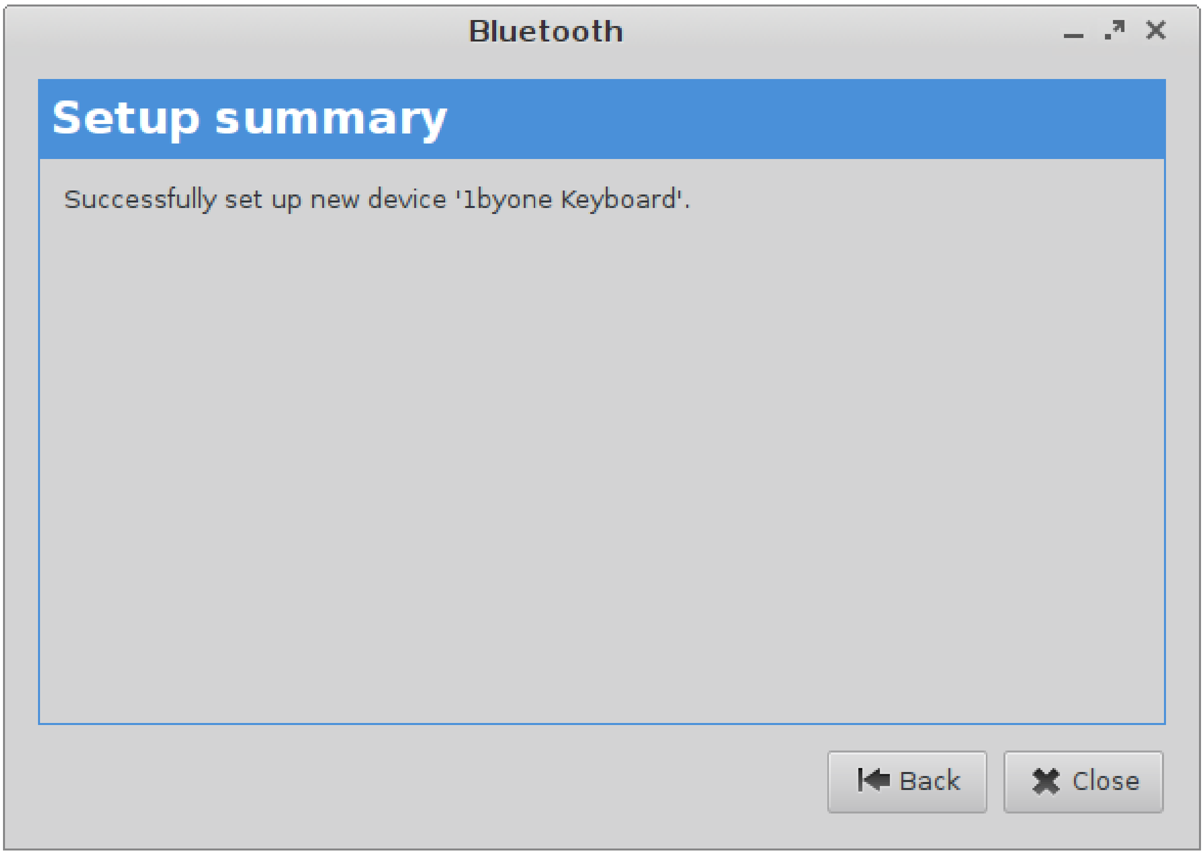
A PIN will be shown on the **Device setup** dialog.



Please enter the following PIN on '1byone Keyboard'
and press Enter on the keyboard.

162319⏎

4. Enter the PIN into your Bluetooth device.
   If everything went well, the status of the connection will be shown.



Successfully set up new device '1byone Keyboard'.

5. Click on **Close**.

   Your Bluetooth device is ready for use. By right-clicking the ✱ icon in the system tray, you can to start the Bluetooth tool again, e.g. to pair another Bluetooth device or to unpair a device.

How to Deploy a Jabra Xpress Package

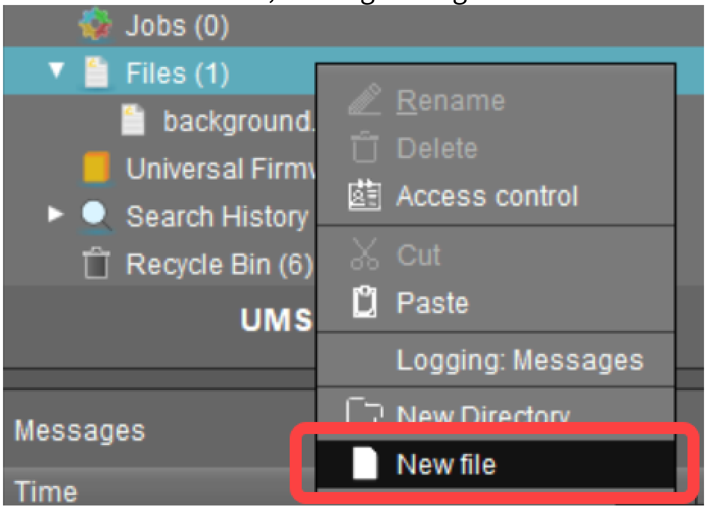
Jabra Xpress is a solution for the remote mass-deployment of Jabra USB headsets that enables creating and deploying packages containing settings, firmware updates, etc. for Jabra devices. For more information, see https://www.jabra.com/supportpages/jabra-xpress#/.

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 854)
2. Configuring the source URL in the IGEL Setup (see page 854)
3. Triggering the deployment process in the UMS (see page 855)

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 > New file**. For details, see Registering a File on the UMS Server.

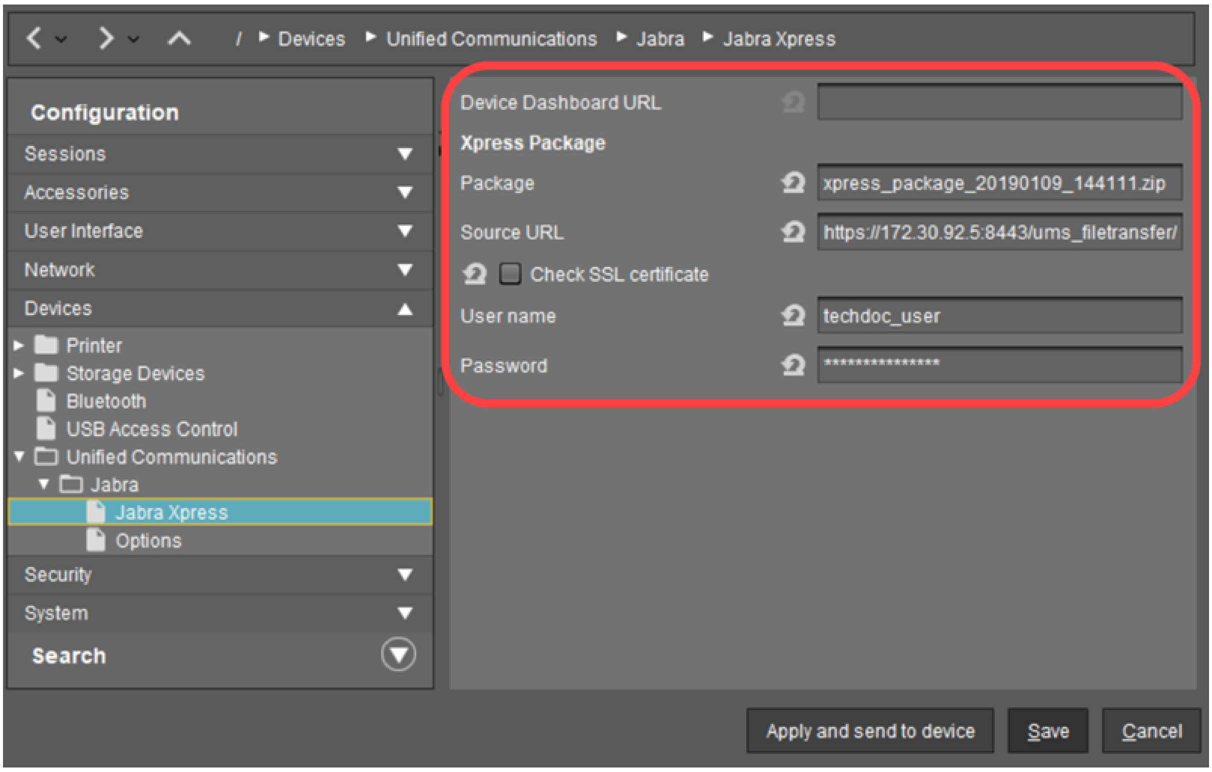


Configuring the Source URL

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 you use the UMS as the source for your Xpress package or 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**.



Device Dashboard URL:

Xpress Package

Package: xpress_package_20190109_144111.zip

Source URL: https://172.30.92.5:8443/ums_filetransfer/

□ Check SSL certificate

User name: techdoc_user

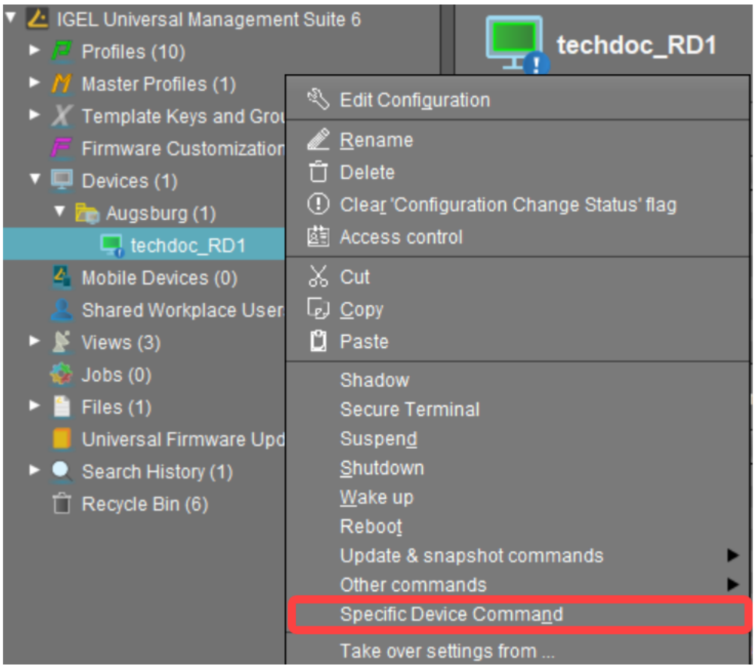
Password: ***************

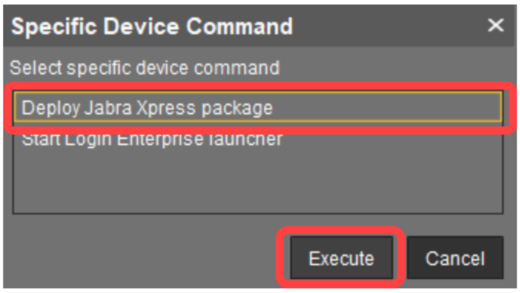
8. Save the settings.

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**.



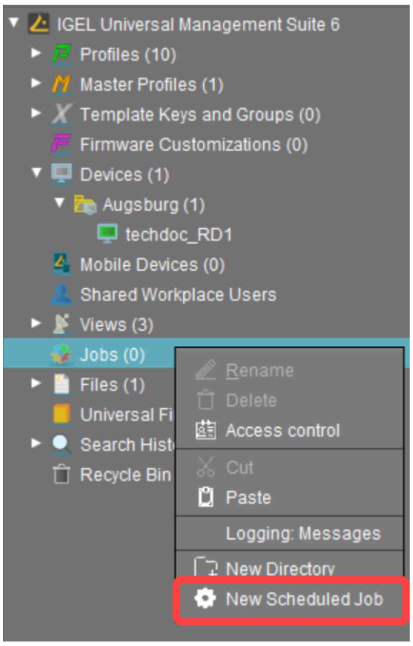


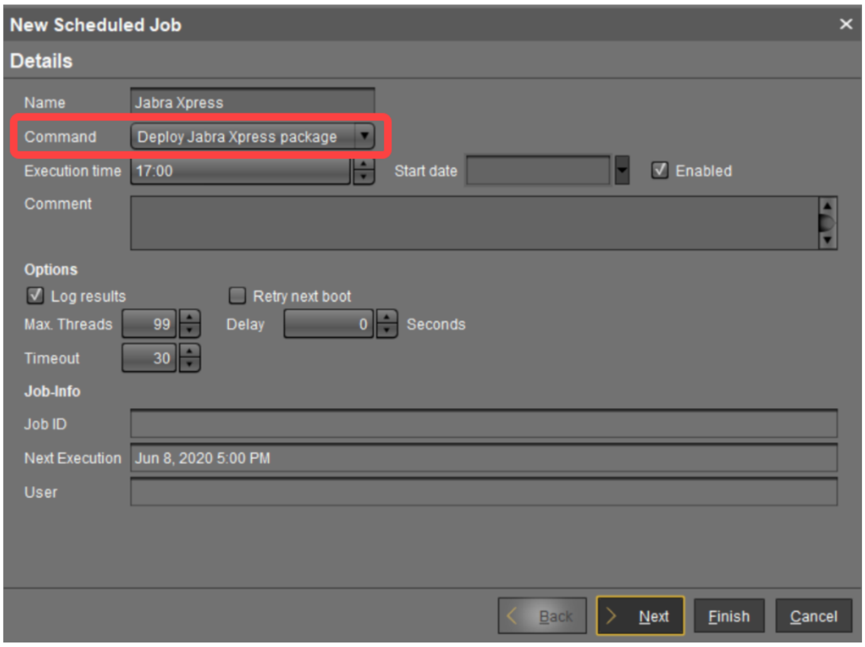
Select specific device command

Deploy Jabra Xpress package
Start Login Enterprise launcher

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.





Name: Jabra Xpress
Command: Deploy Jabra Xpress package
Execution time: 17:00
Start date:
☑ Enabled
Comment:

Options
☑ Log results
□ Retry next boot
Max. Threads: 99
Delay: 0 Seconds
Timeout: 30

Job-Info
Job ID:
Next Execution: Jun 8, 2020 5:00 PM
User:

ⓘ 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 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:

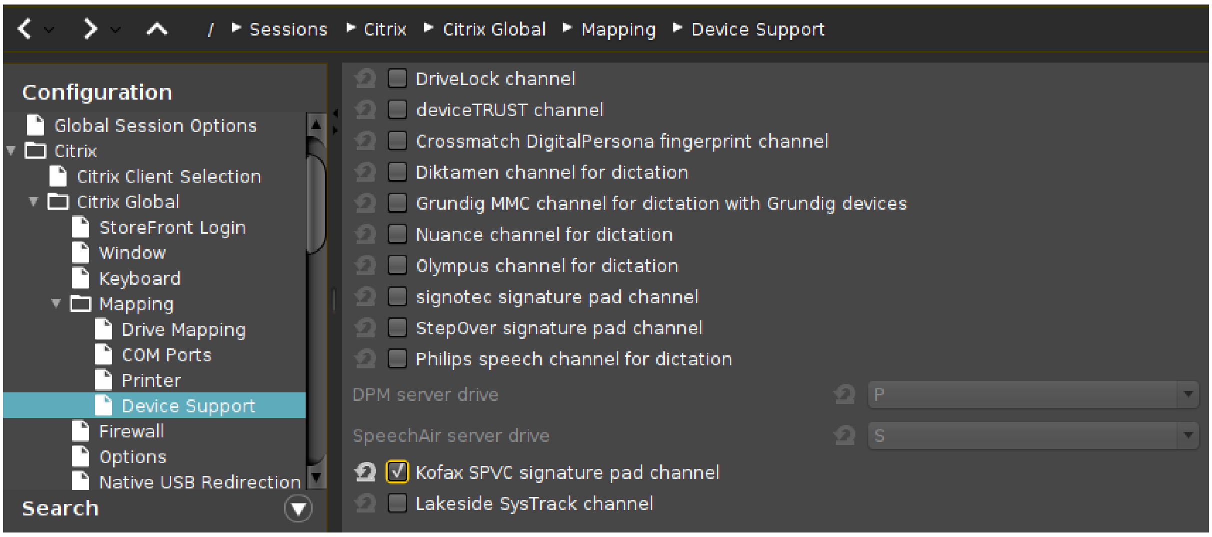
1. Enable **COM port mapping** under:
    - Setup **> Sessions > Citrix > Citrix Global > Mapping > COM Ports** for Citrix sessions;
    - Setup **> Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP sessions.
2. Click on **Add** ⊞.
3. Click **Detect Devices...**.
4. Select your device.
   Your 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**.



☐ DriveLock channel
☐ deviceTRUST channel
☐ Crossmatch DigitalPersona fingerprint channel
☐ Diktamen channel for dictation
☐ Grundig MMC channel for dictation with Grundig devices
☐ Nuance channel for dictation
☐ Olympus channel for dictation
☐ signotec signature pad channel
☐ StepOver signature pad channel
☐ Philips speech channel for dictation
DPM server drive: P
SpeechAir server drive: S
☑ Kofax SPVC signature pad channel
☐ Lakeside SysTrack 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 861)
- With StepOver Signature Pad Channel (see page 865)

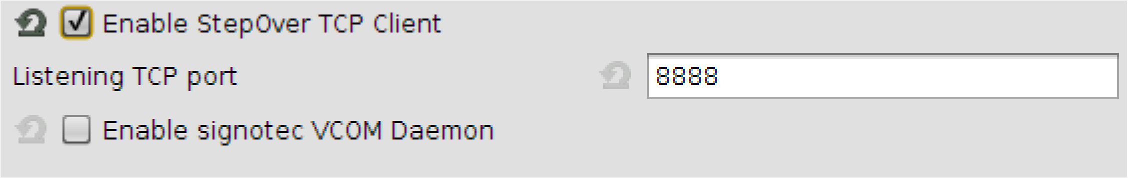
Only one of the methods can be used at a given time. Which of the two you need is determined by your applications on the server side.

See also StepOver Signature Pads Compatibility.

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)



☑ Enable StepOver TCP Client

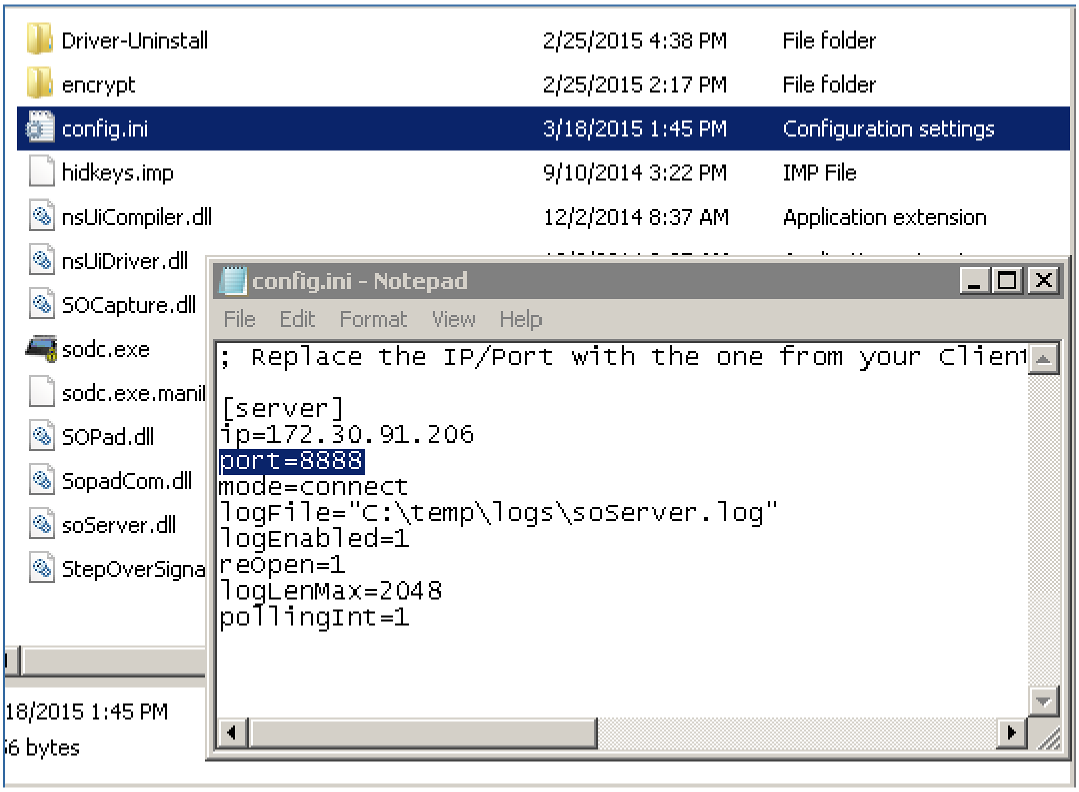
Listening TCP port: 8888

□ Enable signotec VCOM Daemon

> 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.

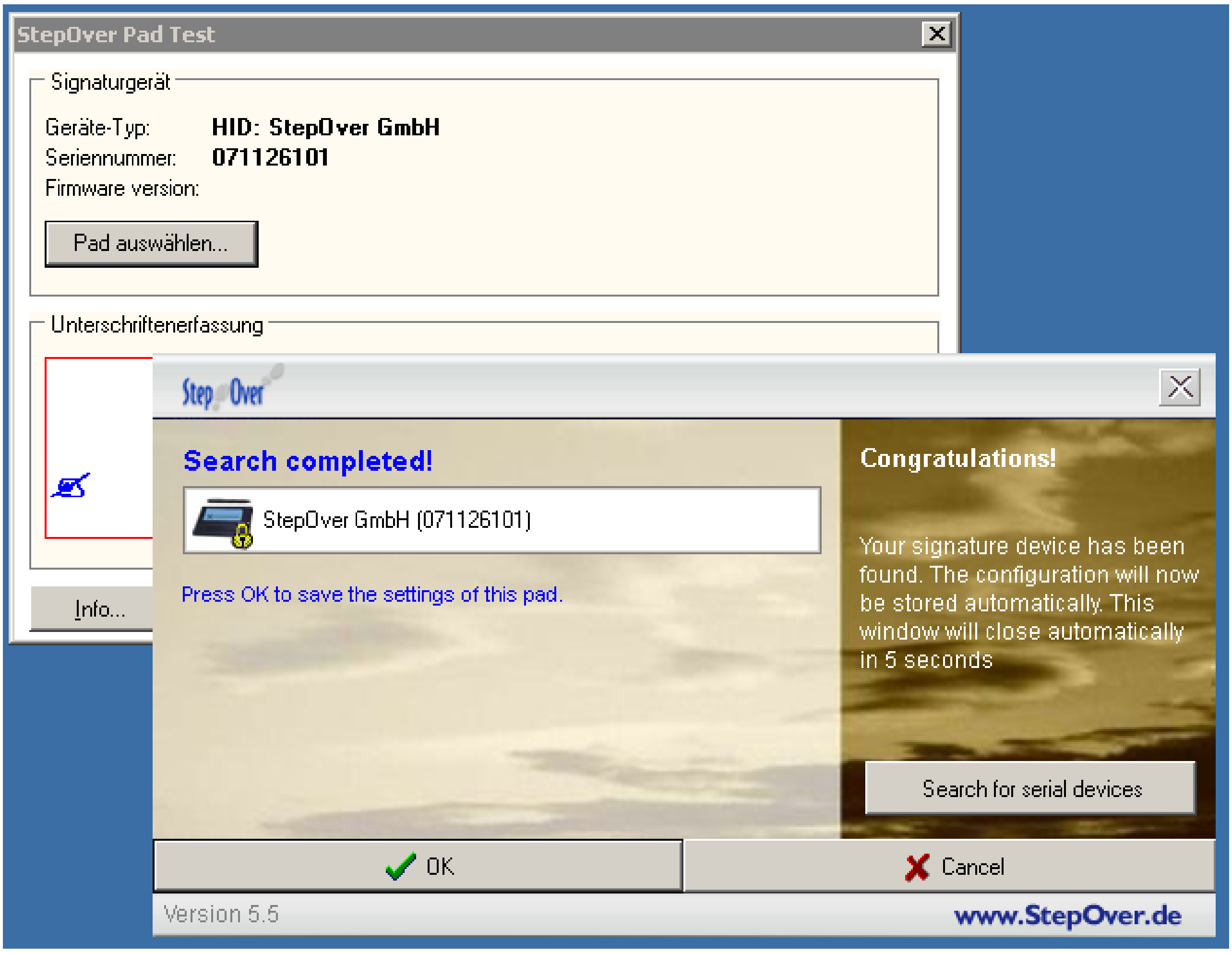


Driver-Uninstall	2/25/2015 4:38 PM	File folder
encrypt	2/25/2015 2:17 PM	File folder
config.ini	3/18/2015 1:45 PM	Configuration settings
hidkeys.imp	9/10/2014 3:22 PM	IMP File
nsUiCompiler.dll	12/2/2014 8:37 AM	Application extension
nsUiDriver.dll		
SOCapture.dll		
sodc.exe		
sodc.exe.mani		
SOPad.dll		
SopadCom.dll		
soServer.dll		
StepOverSigna		

18/2015 1:45 PM
6 bytes

```
; Replace the IP/Port with the one from your Client

[server]
ip=172.30.91.206
port=8888
mode=connect
logFile="C:\temp\logs\soServer.log"
logEnabled=1
reOpen=1
logLenMax=2048
pollingInt=1
```

▶ 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:

Search completed!

StepOver GmbH (071126101)

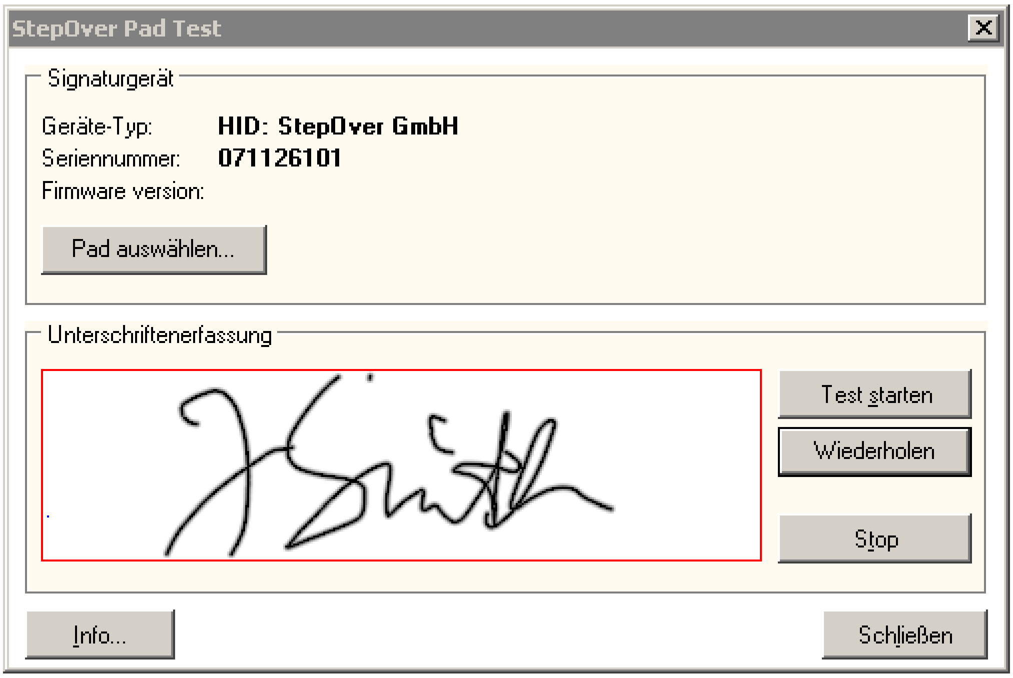
Press OK to save the settings of this pad.

Congratulations!

Your signature device has been found. The configuration will now be stored automatically. This window will close automatically in 5 seconds

Version 5.5

www.StepOver.de



StepOver Pad Test

Signaturgerät

Geräte-Typ: **HID: StepOver GmbH**

Seriennummer: **071126101**

Firmware version:

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

The IGEL Linux thin clients 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-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 867)
- Cherry ST-2052 (see page 868)
- Cherry ST-1503 und G87-1504 (USB) (see page 869)
- Orga 910/920 M (see page 870)
- Orga 6041 L eGK eHealth-BC S (see page 871)
- celectronic CARD STAR / medic2 (see page 872)
- celectronic CARD STAR/ memo3 (see page 873)

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 http://www.cherry.de/files/manual/Cherry_G80-1502_mit_eGK.pdf.

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

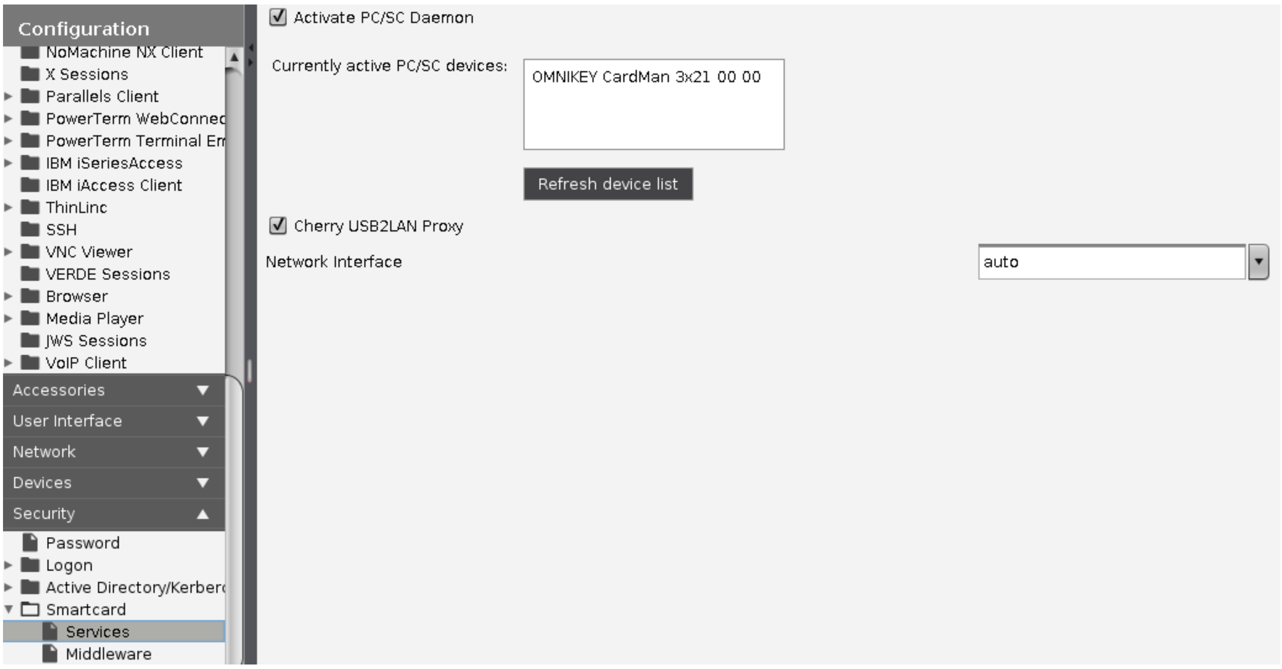
1. Install the eGK-KVK software by *Cherry*.
   See also http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf
2. Start the program CT-API configuration.
3. Select the appropriate port number for the G80-1502.

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**:



☑ Activate PC/SC Daemon

Currently active PC/SC devices: OMNIKEY CardMan 3x21 00 00

☑ Cherry USB2LAN Proxy

Network Interface: auto

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.

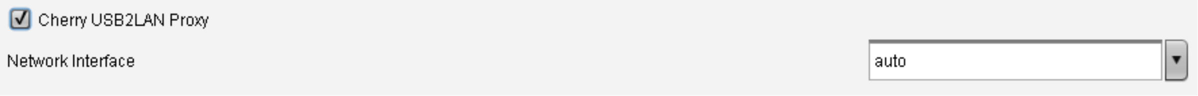
Cherry ST-1503 und G87-1504 (USB)

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**:



☑ Cherry USB2LAN Proxy

Network Interface: auto

Configuring the Server for the Cherry USB2LAN Proxy

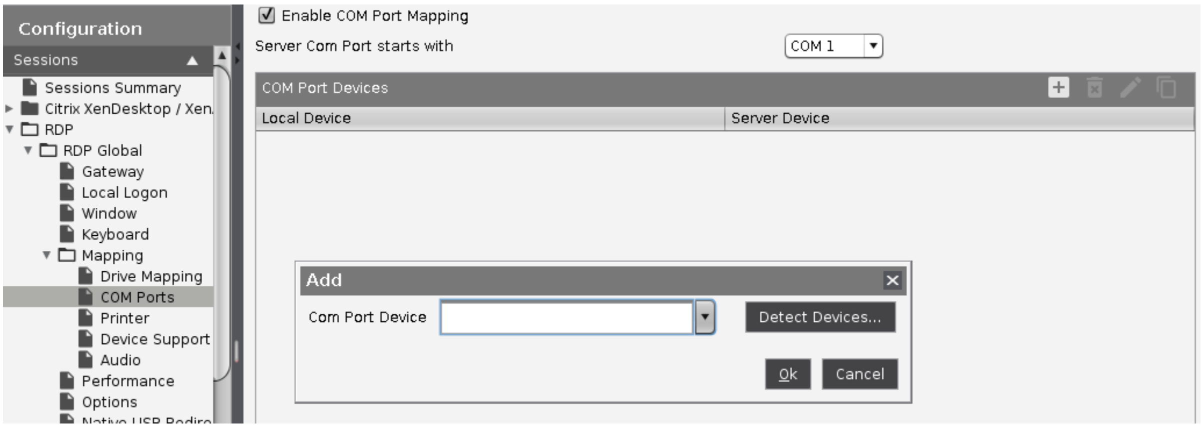
1. Install the eGK-KVK software by Cherry.
2. Configuration according to chapter 6 in http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf.

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 ⊞.



☑ Enable COM Port Mapping

Server Com Port starts with: COM 1

Com Port Device:

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[69]
2. Install the driver.

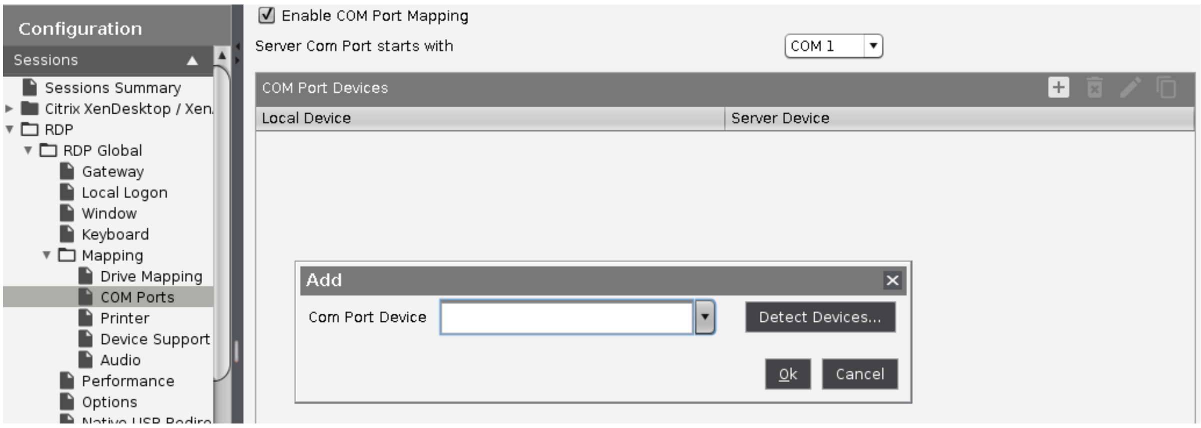
[69] https://ingenico.de/healthcare/downloads

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 ⊕.



☑ Enable COM Port Mapping

Server Com Port starts with: COM 1

Com Port Device:

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[70]
2. Install the driver.

[70] https://ingenico.de/healthcare/downloads

celectronic CARD STAR / medic2

Connecting the reader

▶ Connect the reader to the COM port of the thin client.

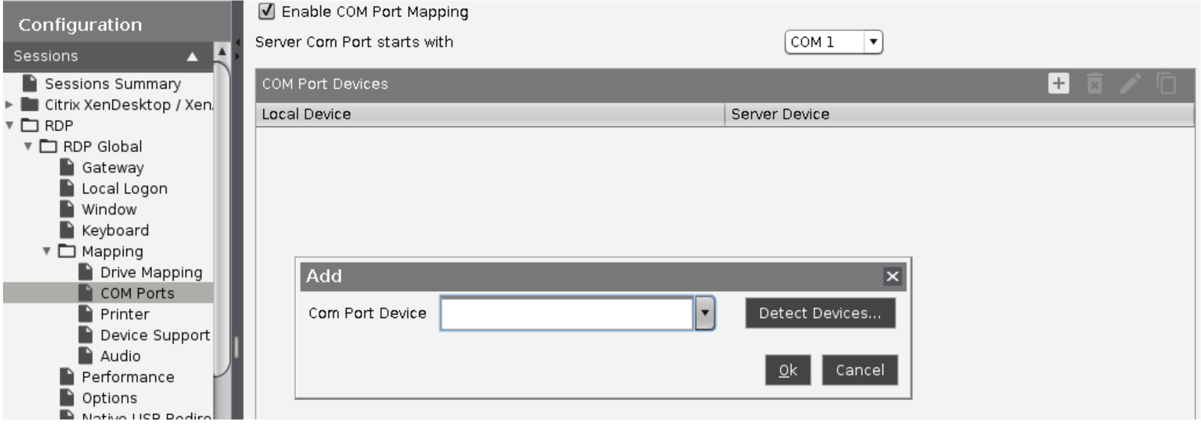
ⓘ The reader must be set to host/PC serial interface.

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.



☑ Enable COM Port Mapping

Server Com Port starts with: COM 1

Com Port Device:

2. Click ⊕.
3. Select a **COM port device** (COM1, COM2,...).

Configuring the server

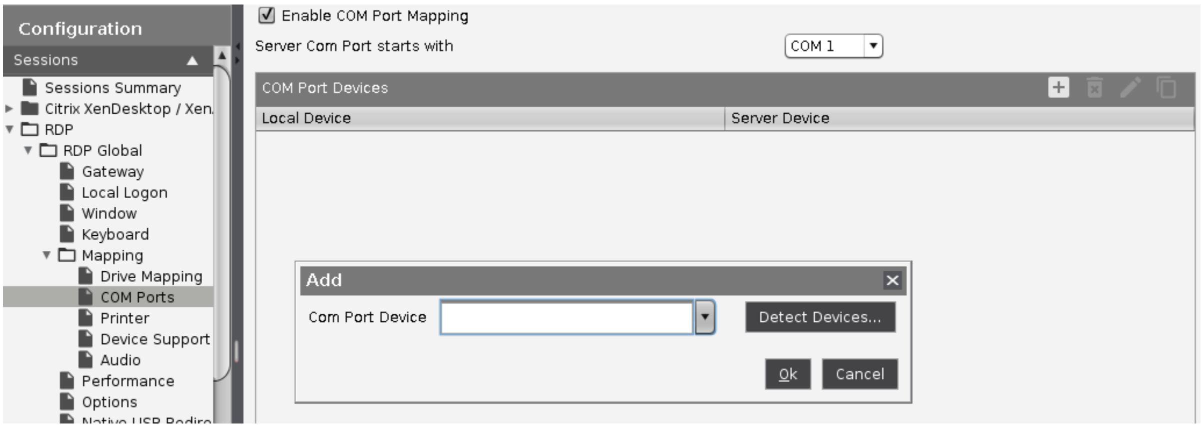
1. Download the appropriate driver for *celectronic CARD STAR /medic2* from the download page: https://www.ccv.eu/de/
2. Install the driver.

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 ⊕.



☑ Enable COM Port Mapping

Server Com Port starts with: COM 1

Local Device	Server Device

Com Port Device:

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/[71]
2. Install the driver.

[71] 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

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.

   > ⓘ If you want to use mobile device access in appliance mode, you must enable autostart or configure a hotkey. Autostart is recommended.

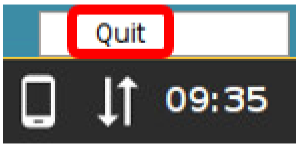
7. Configure the start options for mobile device access according to your requirements.
8. If you have activated **Autostart** as the only start option, restart the device.

   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 879).

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.

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 875).
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 880).
   You can remove the mobile device securely; see Safely Removing the Mobile Device (see page 882).

Accessing the Mobile Device USB Window from a Session

Non-Fullscreen Session

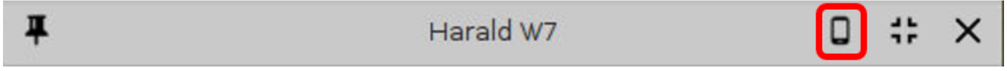
- Click 📱 to open the **Mobile Device Access USB** window.

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 882).

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.

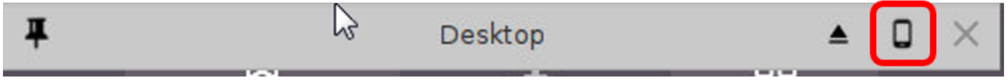


2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

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.

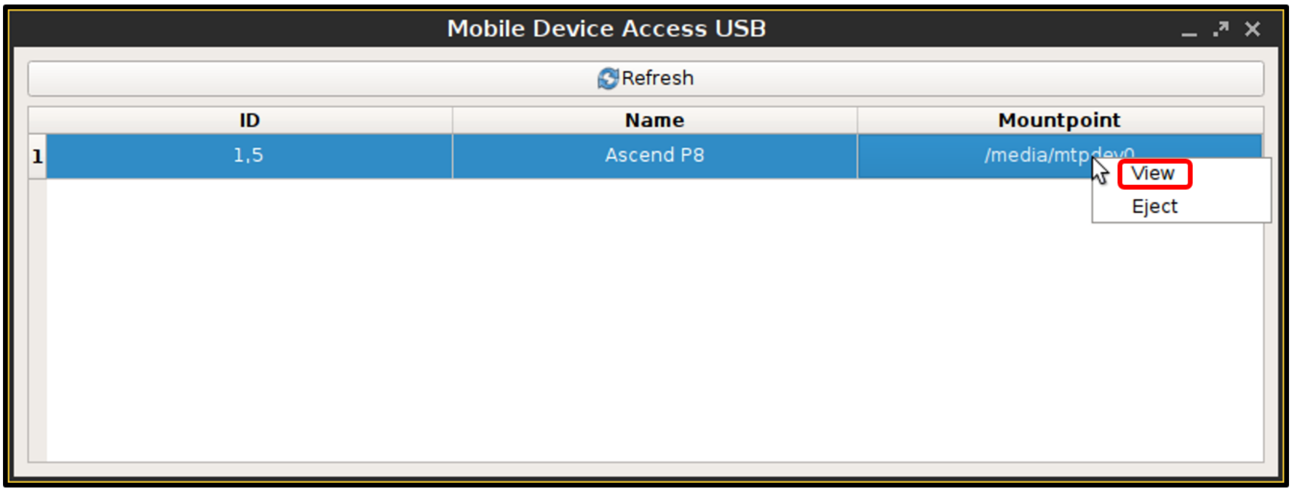
1. Move the mouse pointer to the upper edge of the screen.
   The in-session control bar appears.



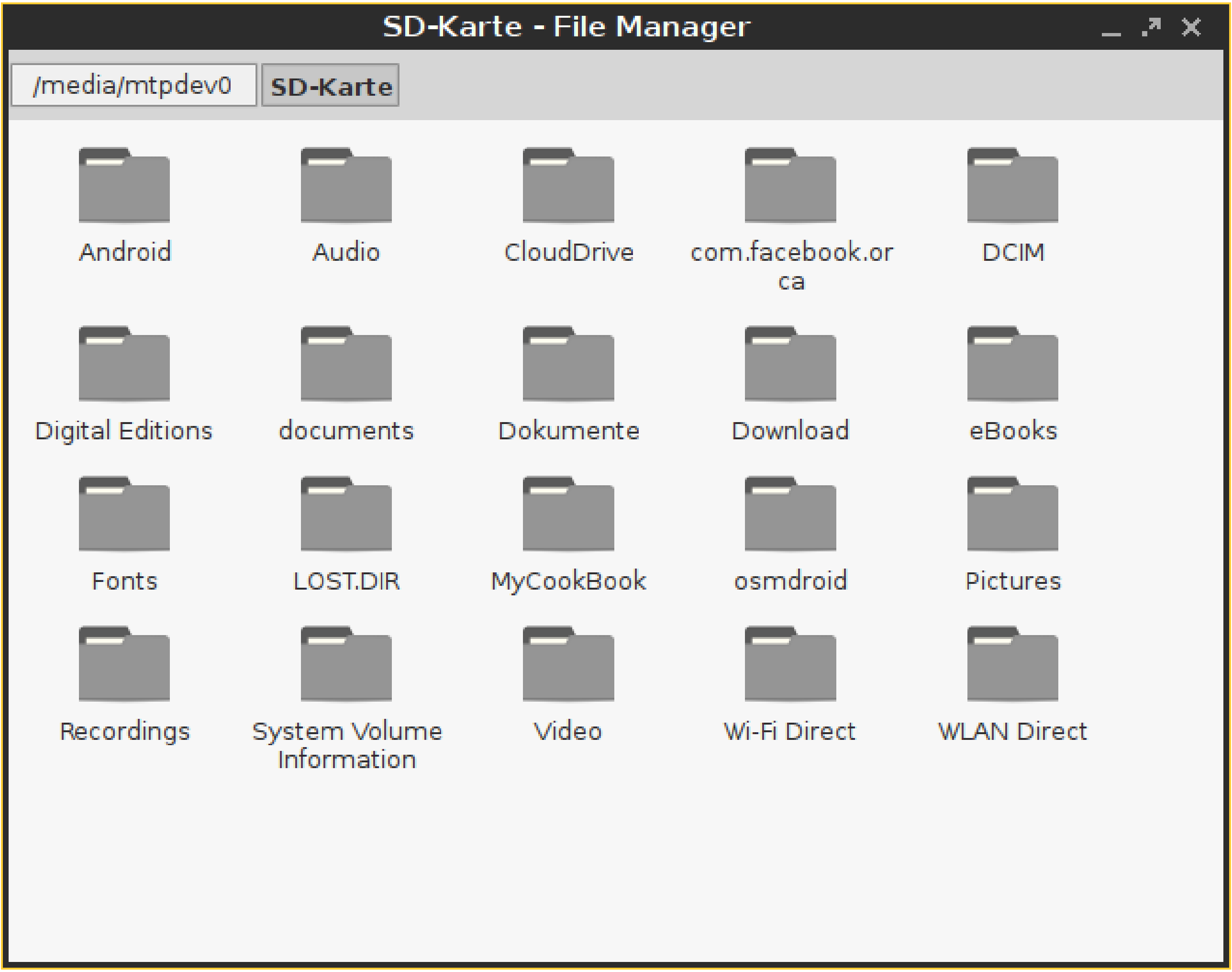
2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

Viewing the Files and Directories Locally

- Select **View** in the context menu.

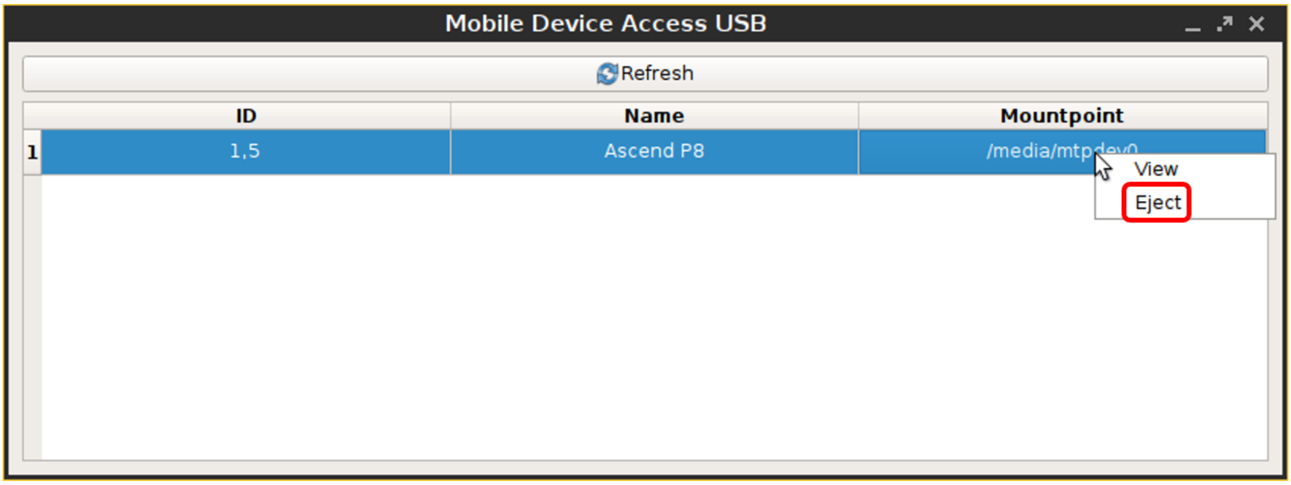


The directories on your smartphone are displayed. Access is read-only, i. e. you can only view the directories and files.


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.



	ID	Name	Mountpoint
1	1,5	Ascend P8	/media/mtpdev0

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 pointerid=2[master pointer (3)]` `|- Virtual core XTEST pointer id=4[slave pointer (2)]` `|- Logitech USB Optical Mouse id=10[slave pointer (2)]` `- Virtual core keyboardid=3[master keyboard (2)]` `- Virtual core XTEST keyboard id=5[slave keyboard (3)]` `- Power Buttonid=6[slave keyboard (3)]` `- Video Busid=7[slave keyboard (3)]` `- Power Buttonid=8[slave keyboard (3)]` `- Sleep Buttonid=9[slave keyboard (3)]` `- Logitech USB Keyboardid=11[slave keyboard (3)]` `- Logitech USB Keyboardid=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)

Issue

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 **System > Firmware Customization > Custom Commands > Desktop > Final desktop command**.
3. Enter the following command:
   ```
   echo "pointer = 1 2 3 5 4 6 7 8 9 10 11 12" > ~/.Xmodmap && xmodmap ~/.Xmodmap
   ```
4. Save the settings and restart your device.

   > ⚠ This will reverse the scrolling direction of a mouse wheel as well. Swapping 4 and 5 will reverse vertical scrolling, swapping 6 and 7 will reverse horizontal scrolling as well (if supported).

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 simple procedure (see page 886). If you are lucky, this will do it. If not, continue with the extended procedure (see page 887).

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 Terminals.
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 extended procedure (see page 887) 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

⚠ **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.

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, see Webcam Redirection and Optimization (see page 836).

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

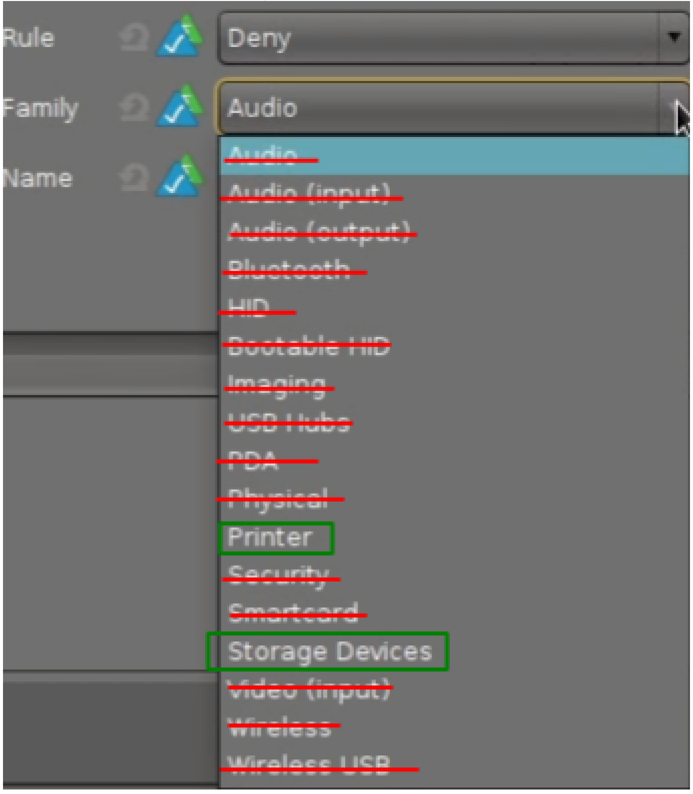
Below are some general rules that, if followed, will provide the best performance and reliability when using USB redirection.

- 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



Rule: Deny

Family: Audio

Name

ⓘ 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

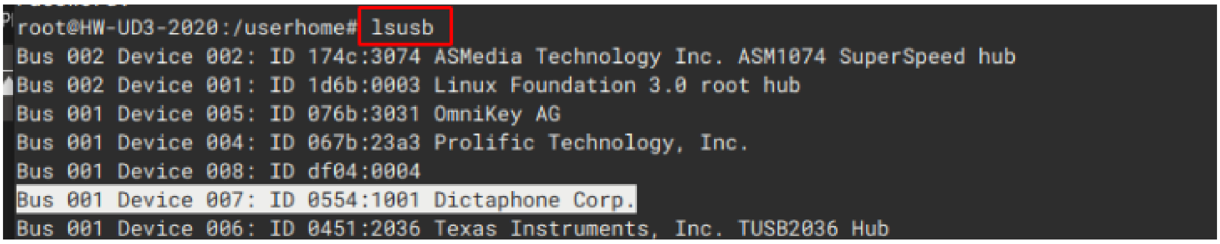
1. Make sure that **Devices > USB Access Control** is disabled on the IGEL devices, or make sure there are no USB access control rules restricting access to the USB device. More information about IGEL USB access can be found under USB Access Control.
2. USB redirection policies for Horizon/Citrix/RDS 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 an IGEL terminal.
2. Connect to the IGEL 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).



```
root@HW-UD3-2020:/userhome# lsusb
Bus 002 Device 002: ID 174c:3074 ASMedia Technology Inc. ASM1074 SuperSpeed hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 076b:3031 OmniKey AG
Bus 001 Device 004: ID 067b:23a3 Prolific Technology, Inc.
Bus 001 Device 008: ID df04:0004
Bus 001 Device 007: ID 0554:1001 Dictaphone Corp.
Bus 001 Device 006: ID 0451:2036 Texas Instruments, Inc. TUSB2036 Hub
```

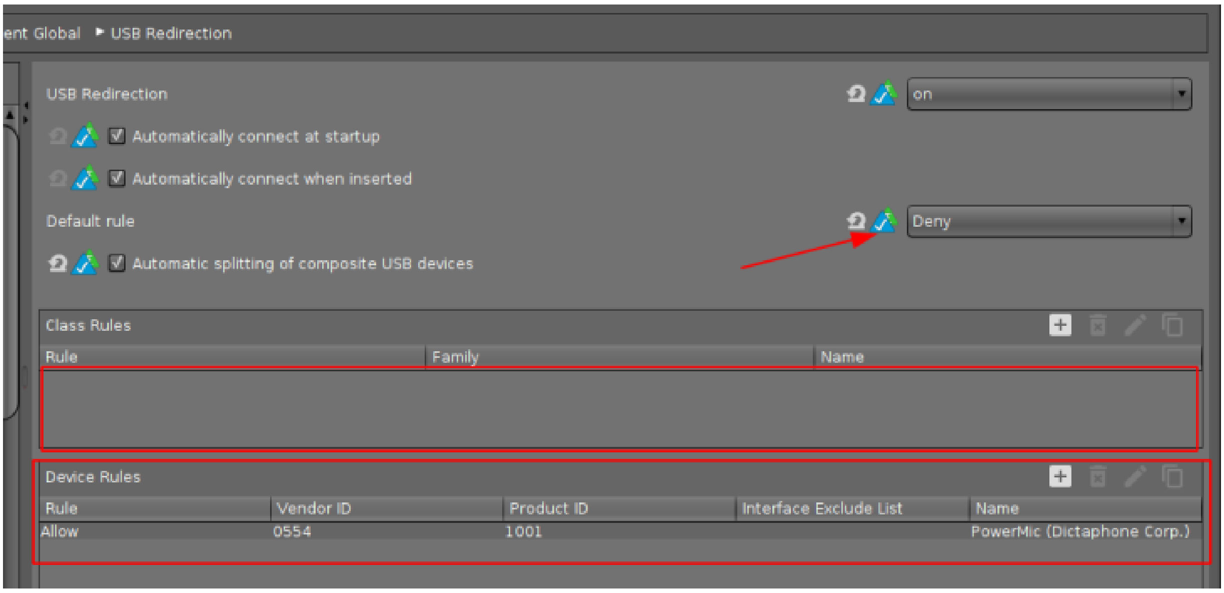
If the device cannot be easily identified by name, then disconnect the device and run `lsusb` again to see which one disappeared.

Configuring the IGEL Profile

1. Create a new profile in 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.



ent Global ▸ USB Redirection

USB Redirection: on

☑ Automatically connect at startup

☑ Automatically connect when inserted

Default rule: Deny

☑ Automatic splitting of composite USB devices

Class Rules

Rule	Family	Name

Device Rules

Rule	Vendor ID	Product ID	Interface Exclude List	Name
Allow	0554	1001		PowerMic (Dictaphone Corp.)

⚠ 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 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

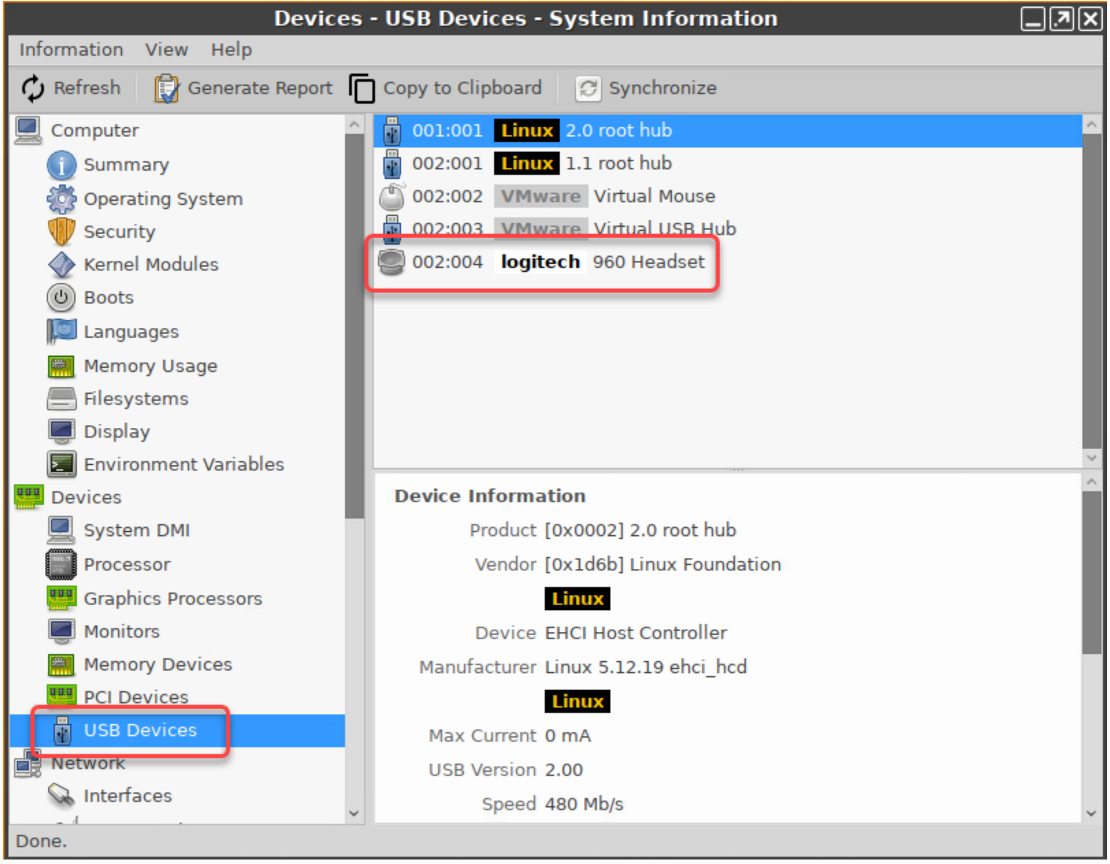
> When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **UUID** must be given.

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.

System Information example:



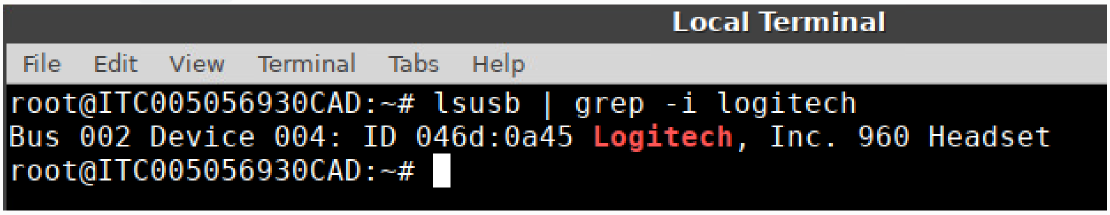
001:001 Linux 2.0 root hub
002:001 Linux 1.1 root hub
002:002 VMware Virtual Mouse
002:003 VMware Virtual USB Hub
002:004 logitech 960 Headset

Device Information

Product [0x0002] 2.0 root hub
Vendor [0x1d6b] Linux Foundation
Linux
Device EHCI Host Controller
Manufacturer Linux 5.12.19 ehci_hcd
Linux
Max Current 0 mA
USB Version 2.00
Speed 480 Mb/s

Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.

Example for `lsusb`:



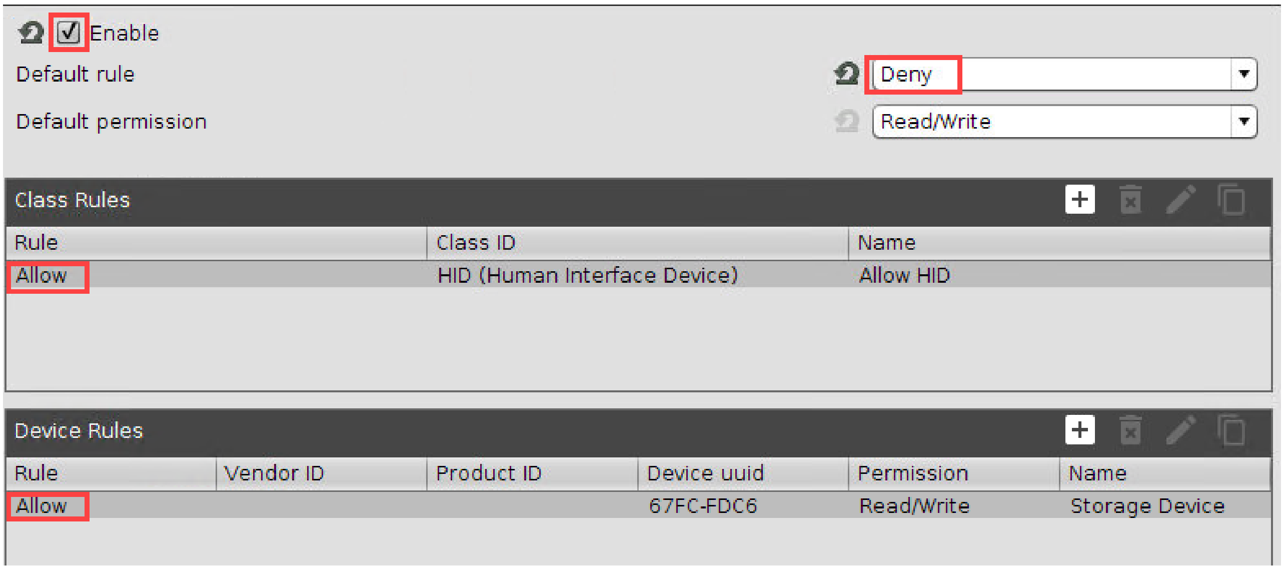
```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 004: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~# 
```

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.



☑ Enable

Default rule: Deny

Default permission: Read/Write

Class Rules

Rule	Class ID	Name
Allow	HID (Human Interface Device)	Allow HID

Device Rules

Rule	Vendor ID	Product ID	Device uuid	Permission	Name
Allow			67FC-FDC6	Read/Write	Storage Device

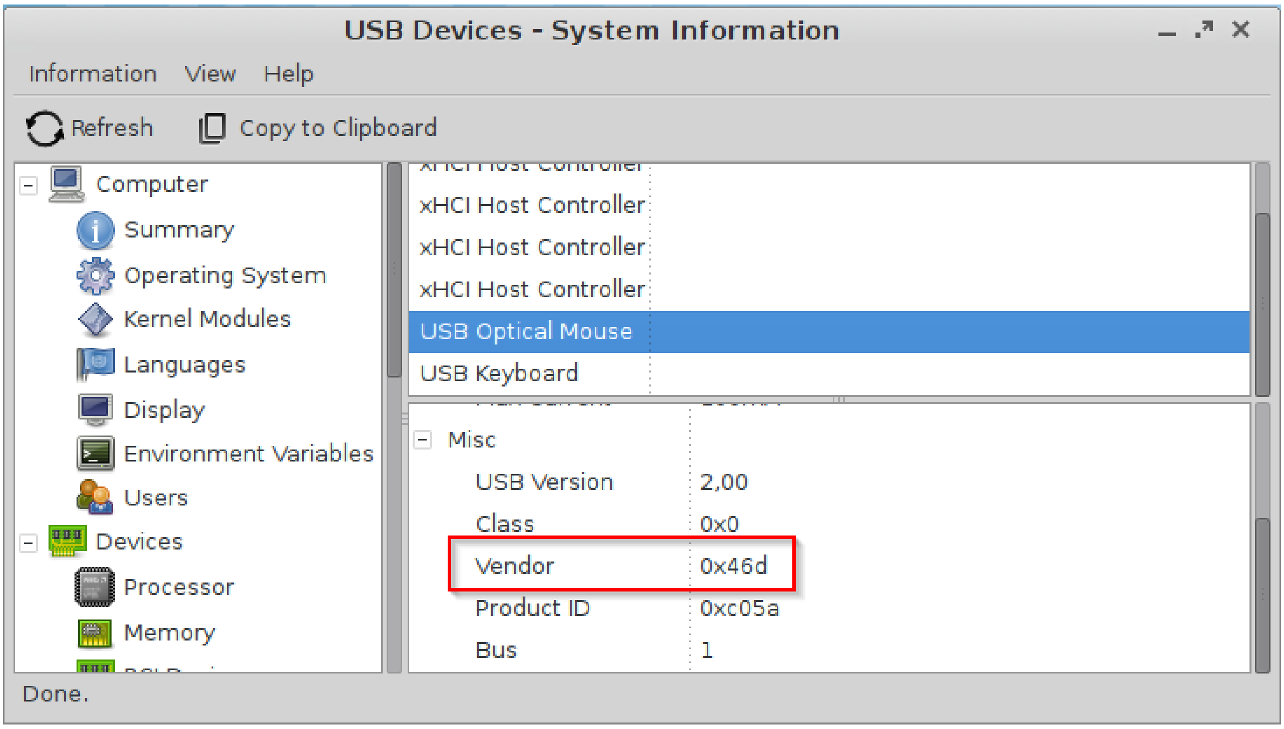
Issues with USB IDs in USB Devices Rules

Symptom

USB Device Rules you configured do not take effect.

Problem

The **System Information** 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.



- Computer
  - Summary
  - Operating System
  - Kernel Modules
  - Languages
  - Display
  - Environment Variables
  - Users
- Devices
  - Processor
  - Memory

xHCI Host Controller
xHCI Host Controller
xHCI Host Controller
USB Optical Mouse
USB Keyboard

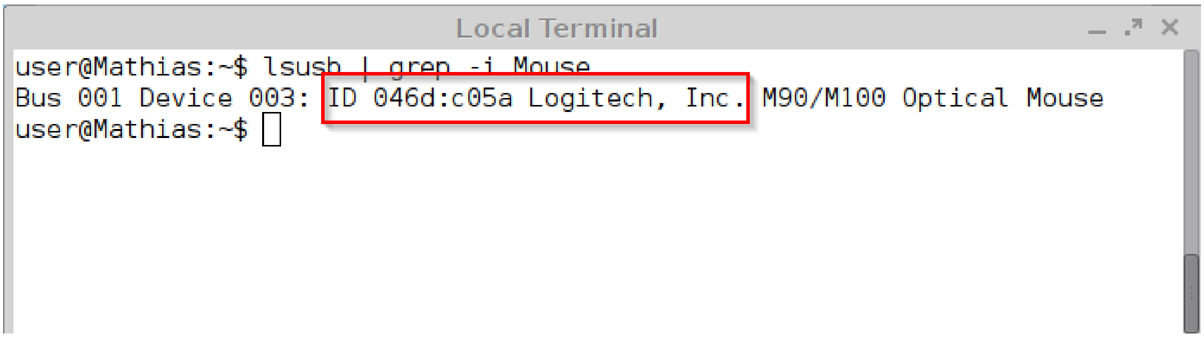
Misc	
USB Version	2,00
Class	0x0
Vendor	0x46d
Product ID	0xc05a
Bus	1

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]
   ```



```
user@Mathias:~$ lsusb | grep -i Mouse
Bus 001 Device 003: ID 046d:c05a Logitech, Inc. M90/M100 Optical Mouse
user@Mathias:~$
```

4. Use the four-digit IDs that `lsusb` reports.

Powerterm Session: USB scanner issues after update to LX 5.07.100

Symptom

A Powerterm session is used in combination with a USB scanner.

After an update to LX 5.07.100, the scanner does not function like before.

Problem

The scanner does not function as before, missing characters, etc.

Solution

1. In Setup, go to **Sessions > Powerterm Terminal Emulation > PowerTerm Selection**
2. Select **PowerTerm Version 9.2.x**

Printer

CUPS: Mapping Local Printer to Citrix or RDP Sessions

Issue

How to map a locally connected PCL/PS-based printer to a Citrix or RDP session?

Problem

The CUPS driver does not support all printer functions such as duplex, color profiles, etc.

Solution

1. Open local IGEL Setup or UMS configuration or profile.
2. Go to **Devices > Printer > CUPS > Printers**.
3. Create a new printer and define a **Printer Name**.
4. Select the **Printer Port** your printer is connected to.
5. Set **Manufacturer = Generic**.
6. Set **Printer names = Raw Queue**.
7. Switch to the tab **Mapping in sessions**.
8. Enable **Map Printer in ICA Sessions** or **Map Printer in RDP Sessions**.
9. Enable the radio button **Use Custom Windows Driver Name**.
10. Enter the exact name of the Windows driver installed on the server.
11. Check if **Sessions > Citrix > Citrix Global > Mapping > Printer > Client printer mapping** or **Sessions > RDP > RDP Global > Mapping > Printer > Enable Client Printer Mapping** is enabled.
12. Start the ICA or RDP session and install the printer driver with the redirected port named `TS00x/ClientPort`.

Print Server Configuration

Prerequisites

- IGEL OS version 10 or higher
- Printer with the integrated PCL/PS controller.

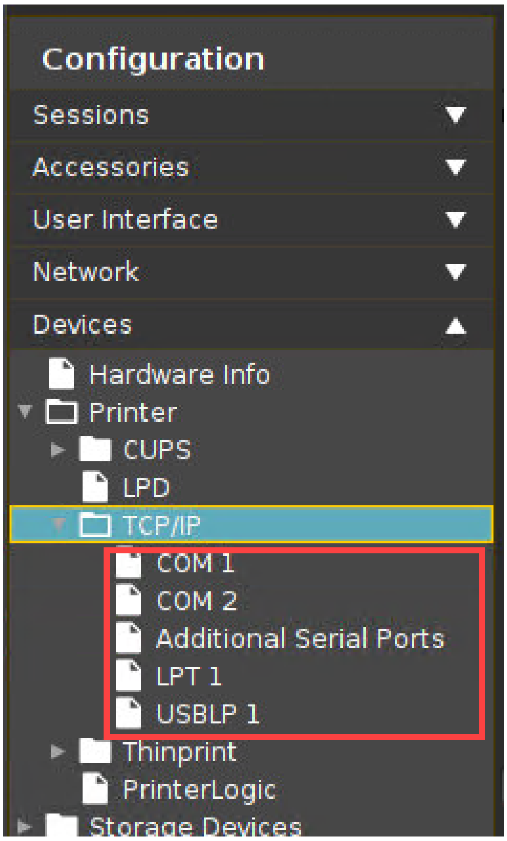
Recommendation

Assign a fixed IP address to the IGEL device or reserve one for it via DHCP.

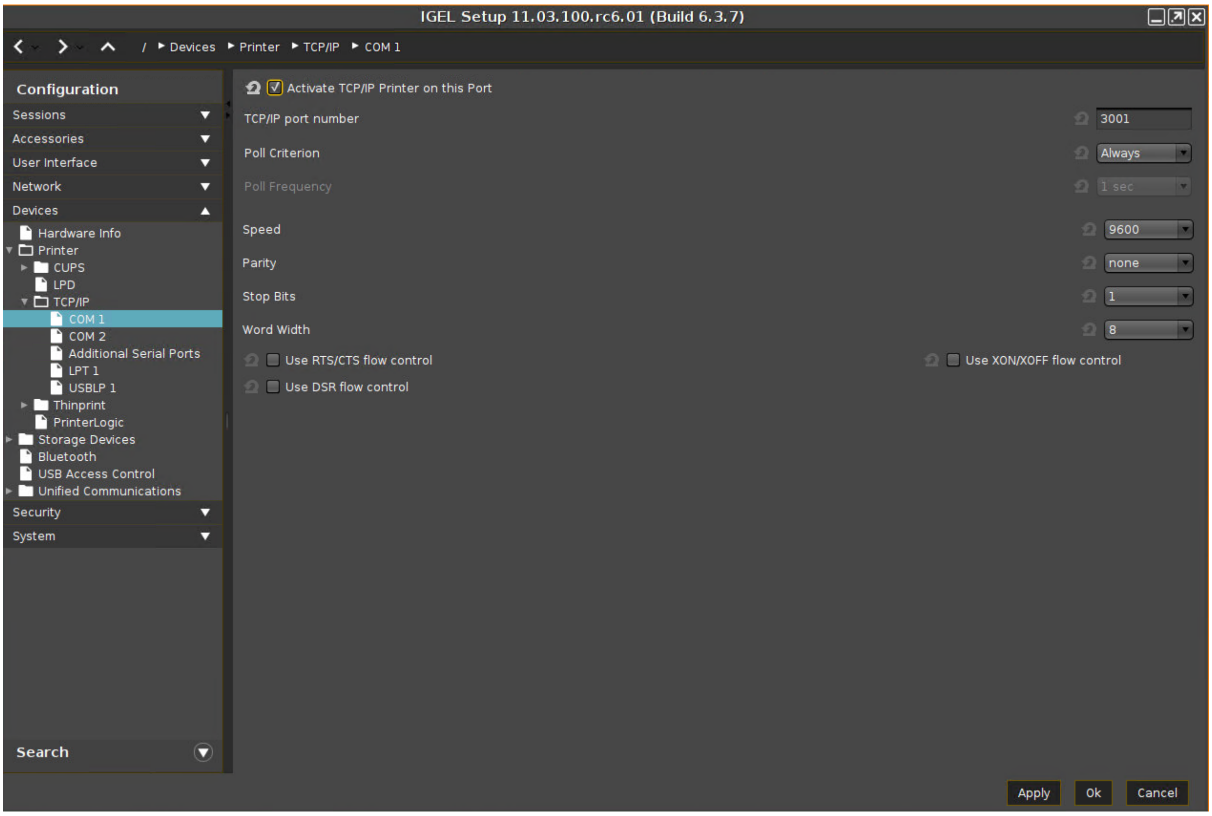
Instructions

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.



☑ Activate TCP/IP Printer on this Port

TCP/IP port number: 3001

Poll Criterion: Always

Poll Frequency: 1 sec

Speed: 9600

Parity: none

Stop Bits: 1

Word Width: 8

□ Use RTS/CTS flow control

□ Use XON/XOFF flow control

□ Use DSR flow control

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 Files.

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.

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.

UD Pocket

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[72].

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.

[72] 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

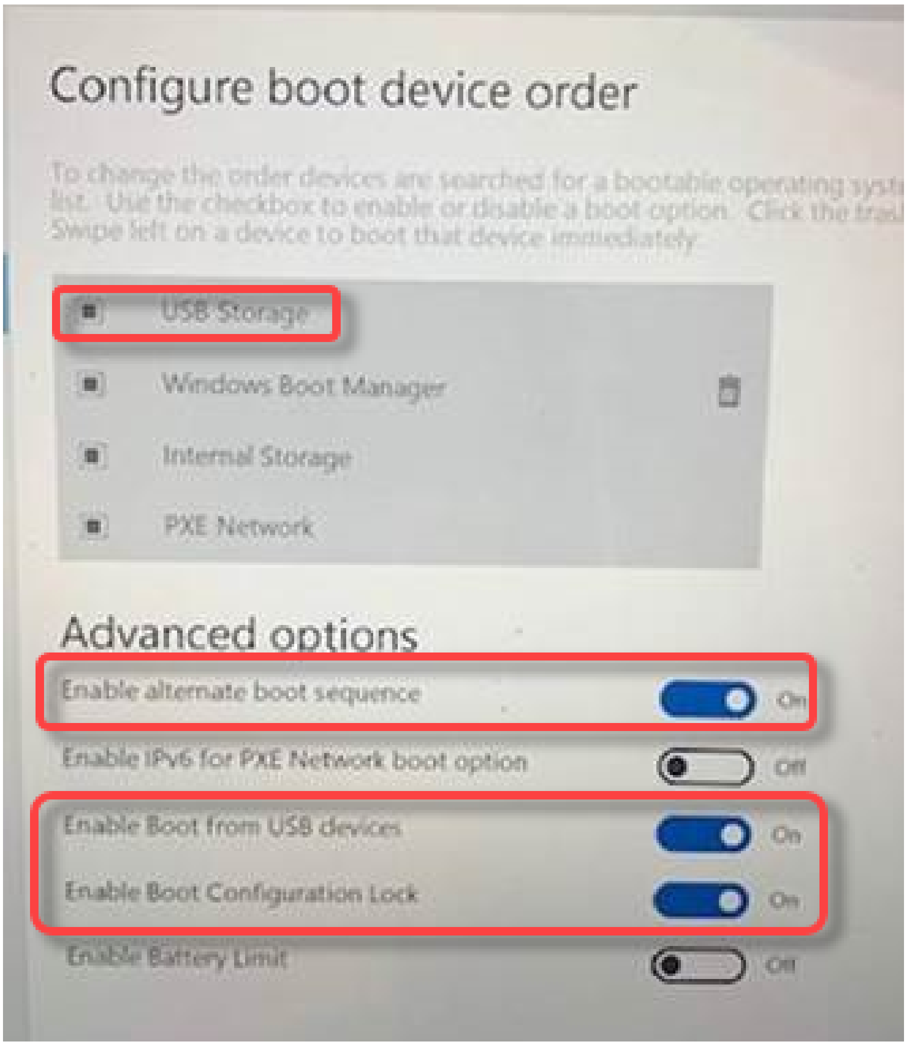
With the following procedures, you can set your Microsoft Surface to boot from USB storage permanently or, alternatively, on-demand.

For detailed information, see How do I use the BIOS/UEFI?[73] 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:

[73] https://support.microsoft.com/en-ae/help/4023532/surface-how-do-i-use-the-bios-uefi



Configure boot device order

To change the order devices are searched for a bootable operating syst
list. Use the checkbox to enable or disable a boot option. Click the tras
Swipe left on a device to boot that device immediately

☑ USB Storage

☑ Windows Boot Manager

☑ Internal Storage

☑ PXE Network

Advanced options

Enable alternate boot sequence — On

Enable IPv6 for PXE Network boot option — Off

Enable Boot from USB devices — On

Enable Boot Configuration Lock — On

Enable Battery Limit — Off

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.

Miscellaneous

Sending Device Log Files to IGEL Support

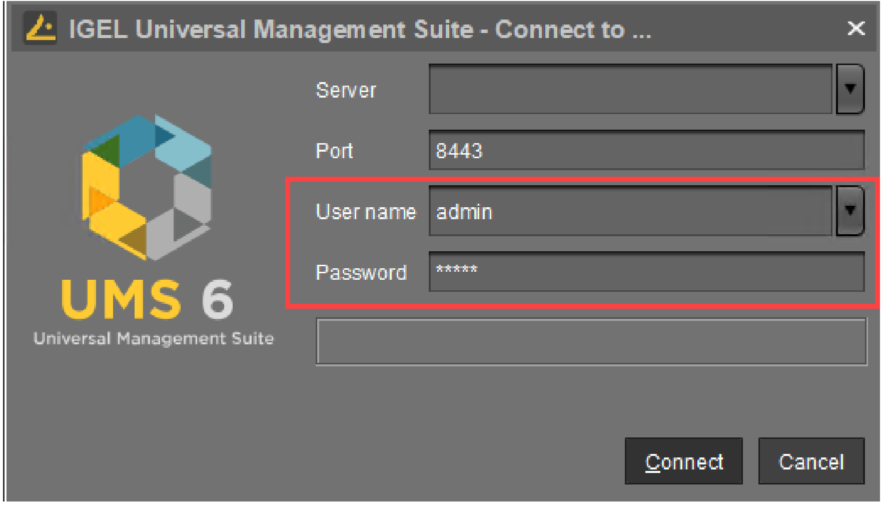
When the IGEL support team asks you to provide your device's log files, follow the instructions below.

There are two opportunities to send log files to the support team:

- With UMS (see page 913)
- Without UMS (see page 917)

With UMS

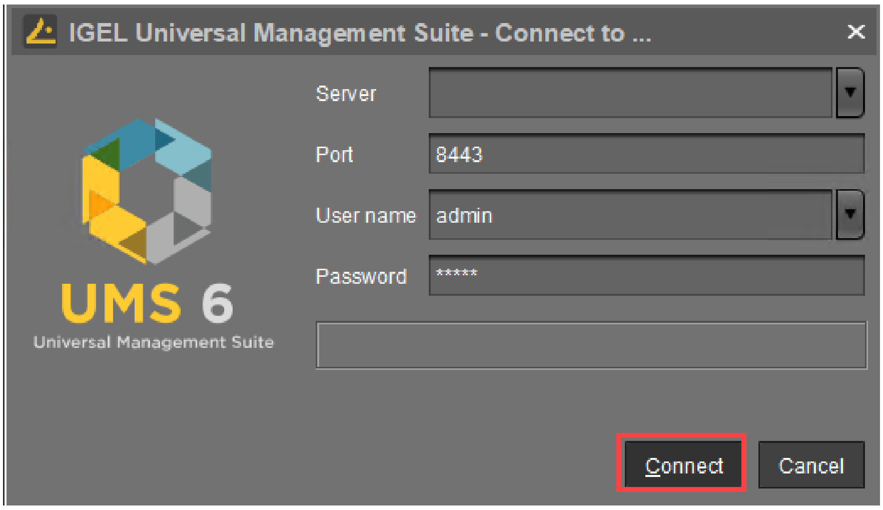
1. Start the UMS Console and enter your **User Name** and **Password**.



IGEL Universal Management Suite - Connect to ...
UMS 6
Universal Management Suite
Connect
Cancel

Server:
Port: 8443
User name: admin
Password: *****

2. Click **Connect**.

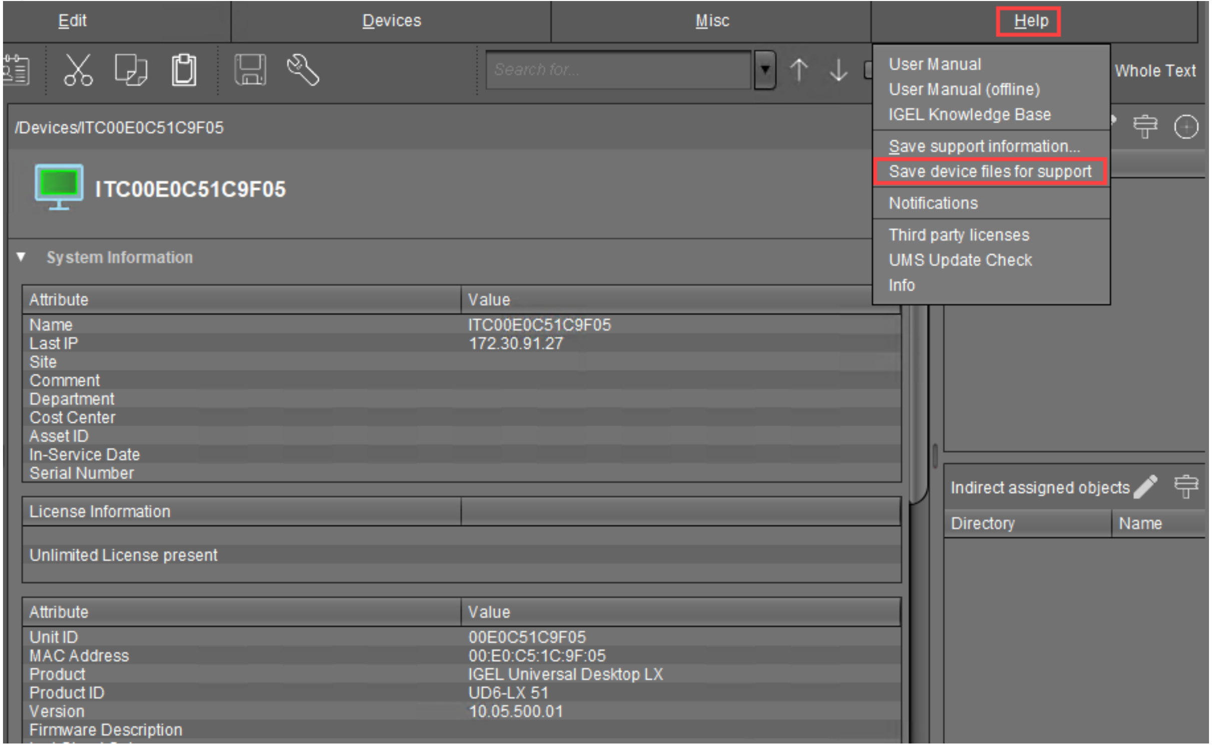


IGEL Universal Management Suite - Connect to ...
UMS 6
Universal Management Suite
Connect
Cancel

Server:
Port: 8443
User name: admin
Password: *****

The UMS Console window opens.

3. Open the **Help** submenu and select **Save TC files for support**.



/Devices/ITC00E0C51C9F05

ITC00E0C51C9F05

System Information

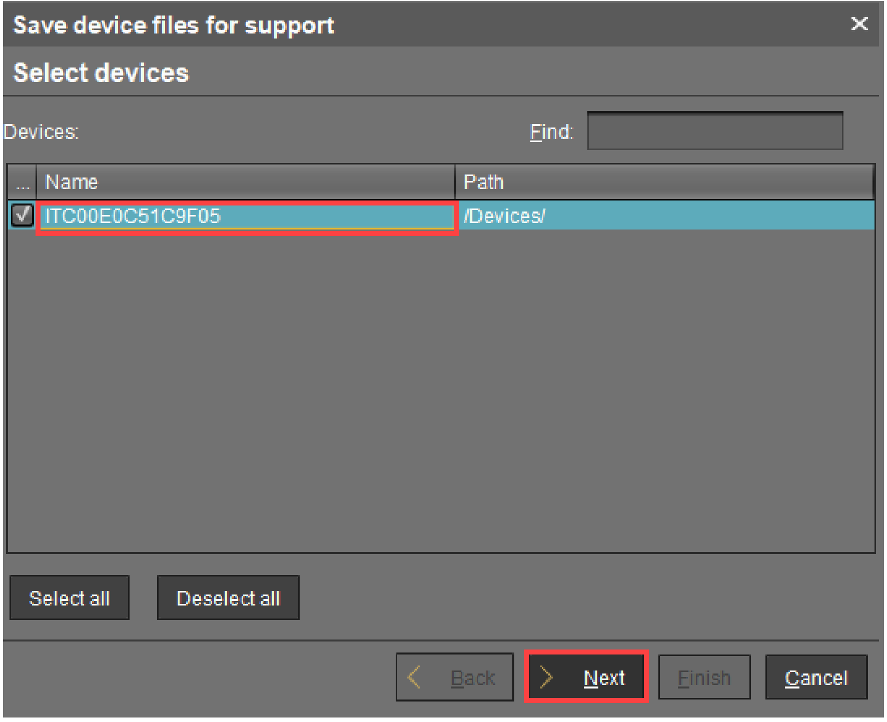
Attribute	Value
Name	ITC00E0C51C9F05
Last IP	172.30.91.27
Site	
Comment	
Department	
Cost Center	
Asset ID	
In-Service Date	
Serial Number	

License Information	
Unlimited License present	

Attribute	Value
Unit ID	00E0C51C9F05
MAC Address	00:E0:C5:1C:9F:05
Product	IGEL Universal Desktop LX
Product ID	UD6-LX 51
Version	10.05.500.01
Firmware Description	

The dialog **Save TC files for support** opens.

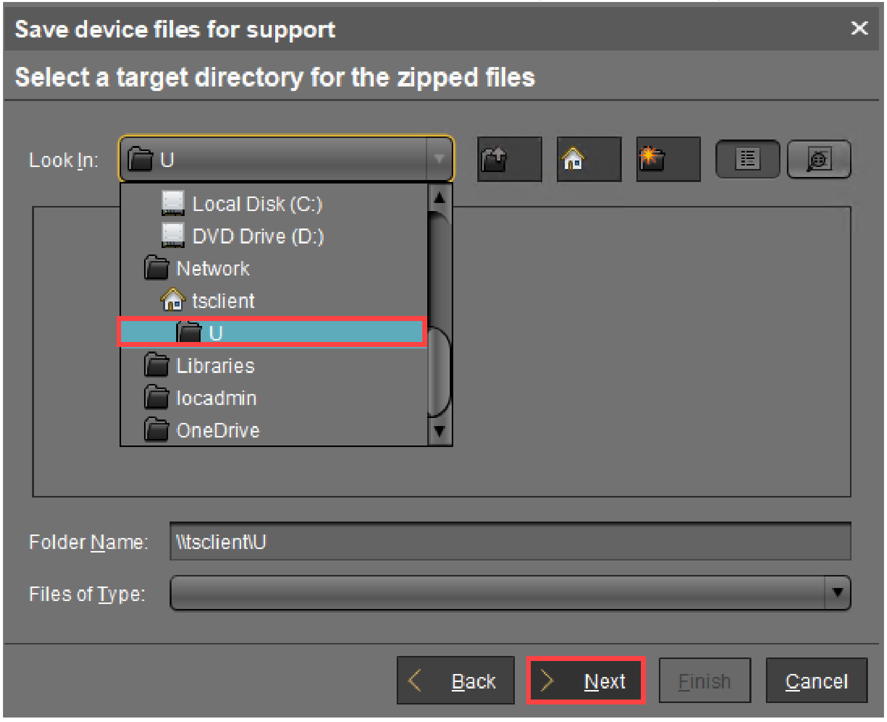
4. Select the device in question and click **Next**.



...	Name	Path
☑	ITC00E0C51C9F05	/Devices/

The dialog **Select a target directory for the zipped files** opens.

5. Select a directory which is suitable for saving the zipped log files, and click **Next**.



Save device files for support

Select a target directory for the zipped files

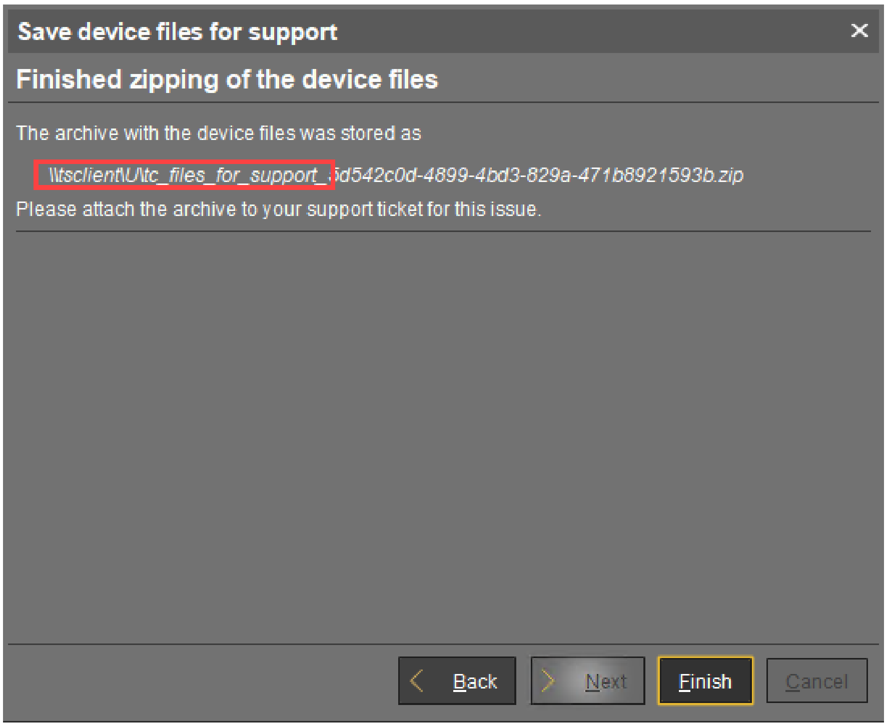
Look In: U

Folder Name: \\tsclient\U

Files of Type:

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 [Ctl] + [C] and paste it into the File Explorer's address bar.



Save device files for support

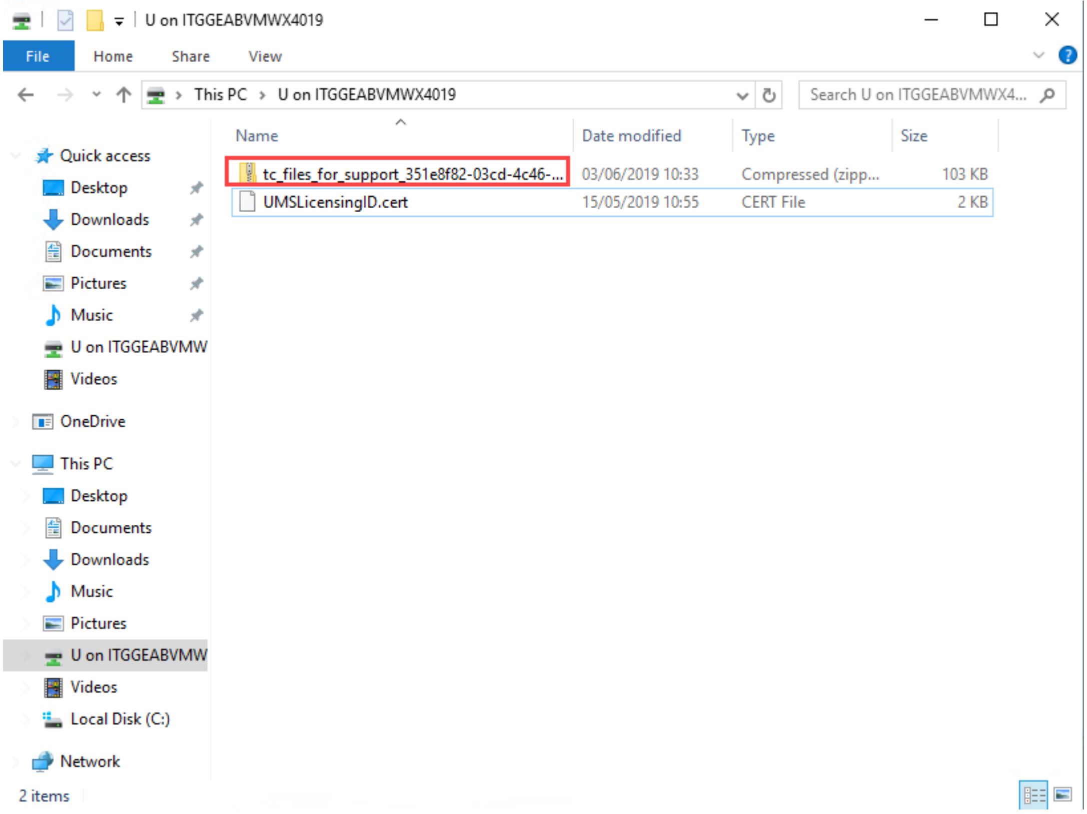
Finished zipping of the device files

The archive with the device files was stored as

\\tsclient\U\tc_files_for_support_5d542c0d-4899-4bd3-829a-471b8921593b.zip

Please attach the archive to your support ticket for this issue.

6. Open your system's File Explorer, go to the path portion of the file location.



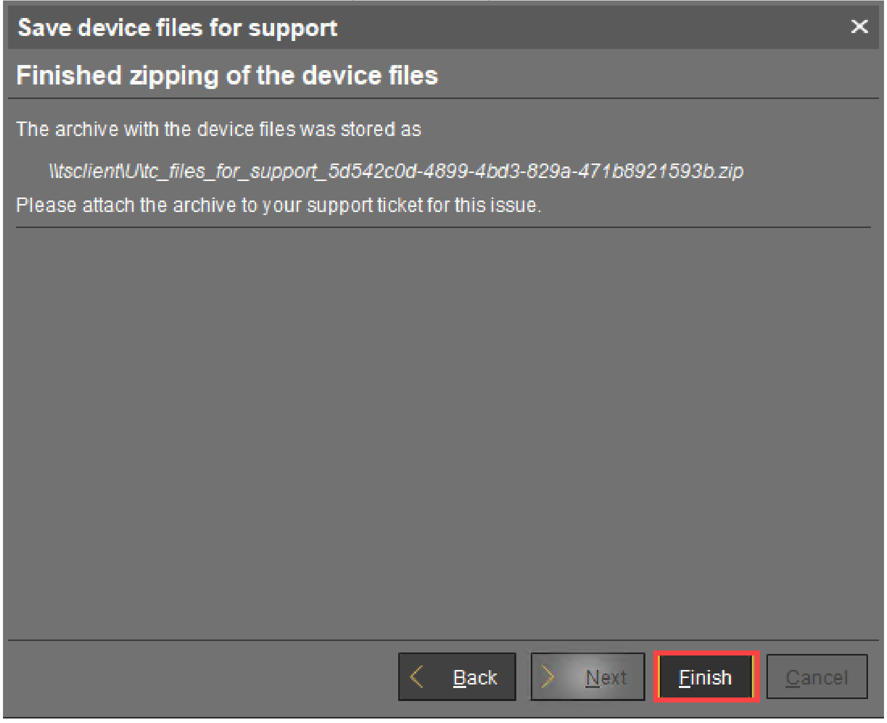
U on ITGGEABVMWX4019

This PC > U on ITGGEABVMWX4019

Name	Date modified	Type	Size
tc_files_for_support_351e8f82-03cd-4c46-...	03/06/2019 10:33	Compressed (zipp...	103 KB
UMSLicensingID.cert	15/05/2019 10:55	CERT File	2 KB

7. Send the ZIP file to the IGEL support team.

8. Close the confirmation dialog by clicking **Finish**.



Save device files for support

Finished zipping of the device files

The archive with the device files was stored as

\\tsclient\U\tc_files_for_support_5d542c0d-4899-4bd3-829a-471b8921593b.zip

Please attach the archive to your support ticket for this issue.

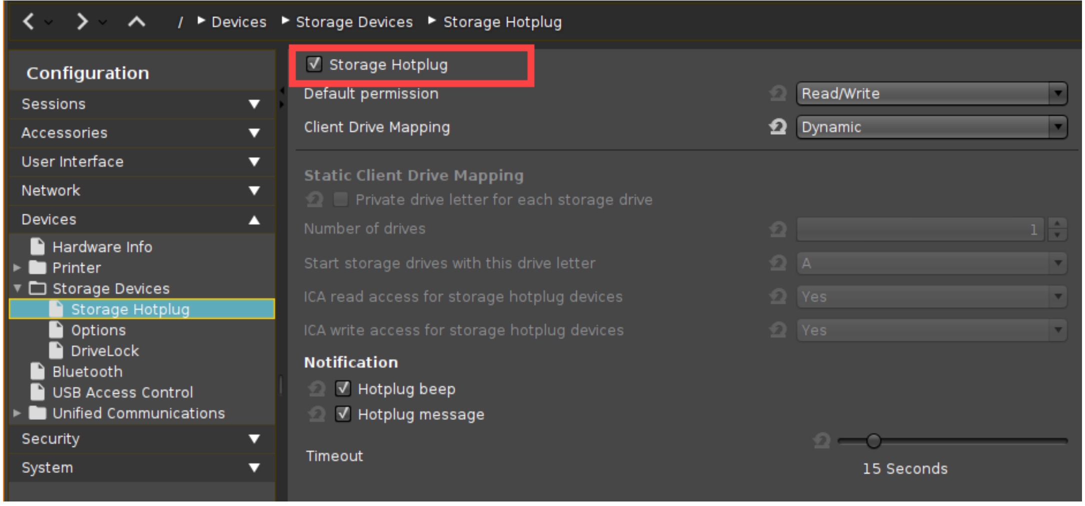
ⓘ The above procedure collects only those logs that have been written since the last system start. To allow persistent logs, you can configure a dedicated partition for debug logs. For more information, also on adding additional logs, see Extended Logging With Syslog, Tcpdump and Netlog (see page 473).

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**.



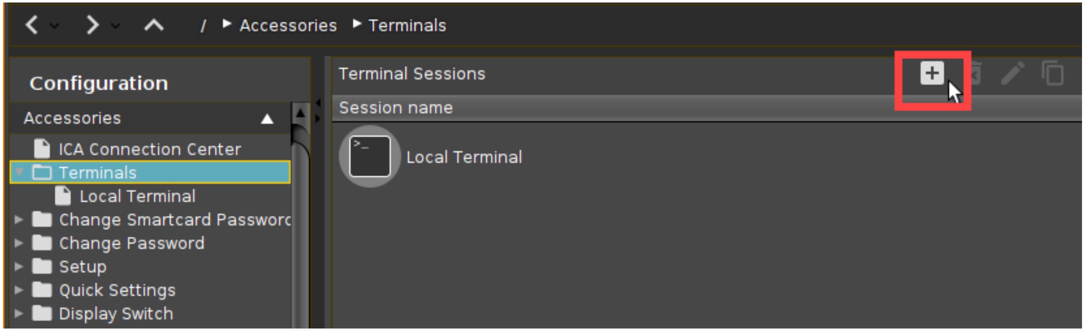
☑ Storage Hotplug
Default permission: Read/Write
Client Drive Mapping: Dynamic

Static Client Drive Mapping
☐ Private drive letter for each storage drive
Number of drives: 1
Start storage drives with this drive letter: A
ICA read access for storage hotplug devices: Yes
ICA write access for storage hotplug devices: Yes

Notification
☑ Hotplug beep
☑ Hotplug message

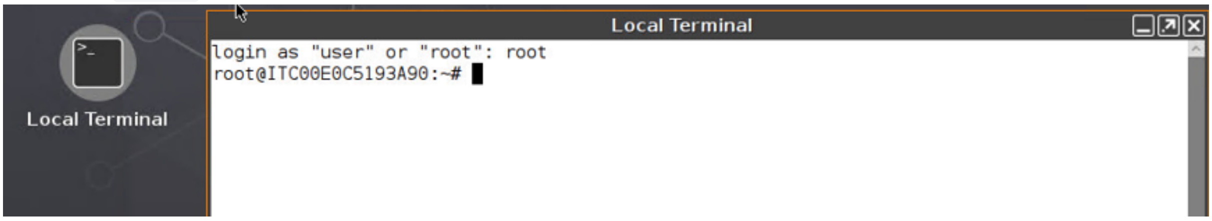
Timeout: 15 Seconds

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).



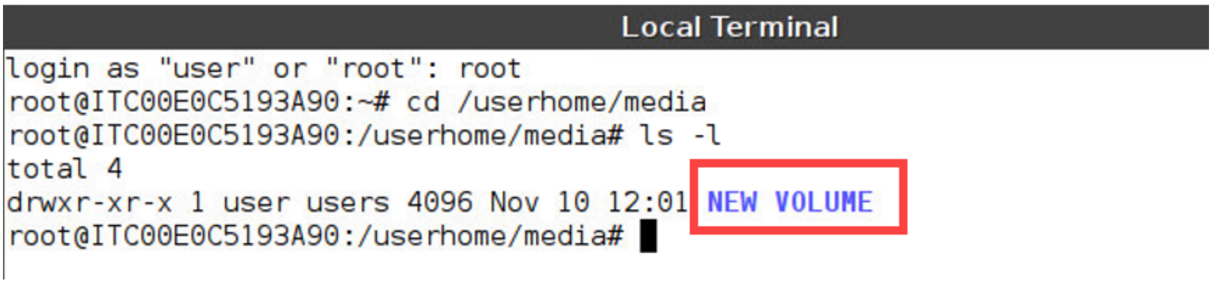
```
login as "user" or "root": root
root@ITC00E0C5193A90:~# █
```

3. Enter the following commands:

```
cd /userhome/media
```

```
ls -l
```

4. Note the name of the USB stick:

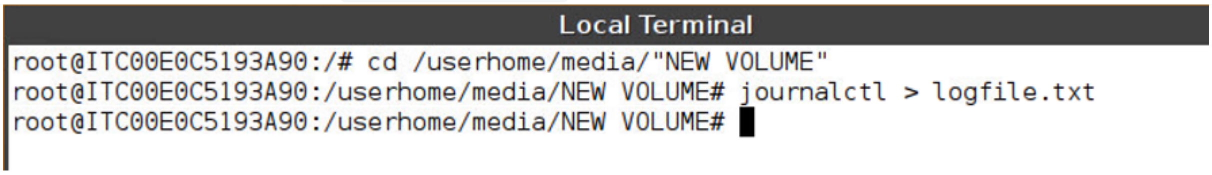


```
Local Terminal
login as "user" or "root": root
root@ITC00E0C5193A90:~# cd /userhome/media
root@ITC00E0C5193A90:/userhome/media# ls -l
total 4
drwxr-xr-x 1 user users 4096 Nov 10 12:01 NEW VOLUME
root@ITC00E0C5193A90:/userhome/media#
```

Writing the Log File

1. In the terminal, run the command `cd /userhome/media/[Name of your USB stick]`.

   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 `journalctl > logfile.txt`. This will create the system log files on the USB stick with the file name `logfile.txt`.



```
Local Terminal
root@ITC00E0C5193A90:/# cd /userhome/media/"NEW VOLUME"
root@ITC00E0C5193A90:/userhome/media/NEW VOLUME# journalctl > logfile.txt
root@ITC00E0C5193A90:/userhome/media/NEW VOLUME#
```

3. 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 device Configuration

Issue

There is a specific support case and you need to read out the current local configuration of the device.

Solution

If you need to read out the current local configuration of the device (e.g. during a support case), you can copy the two local files `setup.ini` and `group.ini` either locally or via the *IGEL Universal Management Suite*.

1. With UMS 4.07.100 or newer you can transfer the `setup.ini` and `group.ini` files together with the device's log files as described in Sending Device Log Files to IGEL Support (see page 913).
2. To save the files locally on a FAT32-formatted USB storage device, proceed as follows:
    a. Enable the use of storage hotplug (setting the **number of USB storage devices** to greater than zero) under **Devices > Storage Devices > USB Storage Hotplug**.
    b. Connect the FAT32-formatted USB storage device.
    c. Create a terminal session under **Accessories > Terminals**.
    d. Open the terminal and login as `root`.
    e. Type `cp /wfs/*.ini /media/[name of USB device]/` and press [Return]to copy the `setup.ini` as well as the `group.ini` from your device to the USB drive.
    f. Type `sync` , press [Return]and wait a few seconds before unplugging the USB storage device.
3. Alternatively (with UMS before 4.07.100) you can transmit the data from the device to the UMS as follows:
    a. In *UMS* console start command **File TC > UMS** in context menu of your device or in **Device** menu of the menu bar (**Other Device commands**).
    b. Enter local file on thin client, e.g. **Device file location** = `/wfs/setup.ini` .
    c. Select **Target URL**, e.g. `webdav/ums_filetransfer` and
    d. Enter **File Name** of the transferred file in UMS.
    e. Click **File TC > UMS** .
    f. The file will be transferred to `/rmguiserver/webapps/ums_filetransfer\`

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.

Hardware

- Jabra Handsets / Headsets
- Poly Headsets
- EPOS/Sennheiser

Virtual Desktop Optimizations

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.

For Citrix Sessions

- Skype for Business; for configuration, see the chapter Skype for Business in the IGEL OS Reference Manual.
- Cisco Jabber (JVDI Client); for configuration, see the chapter Cisco Jabber in the IGEL OS Reference Manual.
- Cisco WebEx Teams and Cisco WebEx Meetings; for configuration, see the chapter Cisco Jabber in the IGEL OS Reference Manual.
- Microsoft Teams; for configuration, see the chapter VDI Solutions in the IGEL OS Reference Manual.
- Zoom Media Plugin; for configuration, see the chapter VDI Solutions in the IGEL OS Reference Manual.

For Horizon Sessions

- Skype for Business; for configuration, see the chapter Skype for Business in the IGEL OS Reference Manual.
- Cisco Jabber (JVDI Client); for configuration, see the chapter Cisco in the IGEL OS Reference Manual.
- Cisco Teams

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 658).

You can acquire any of the following Custom Partitions free of cost; ask contact your IGEL contact:

- TeamViewer
- Zoom (see also Zoom as a Custom Partition (see page 688) in the Custom Partition Tutorial (see page 658))

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.

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

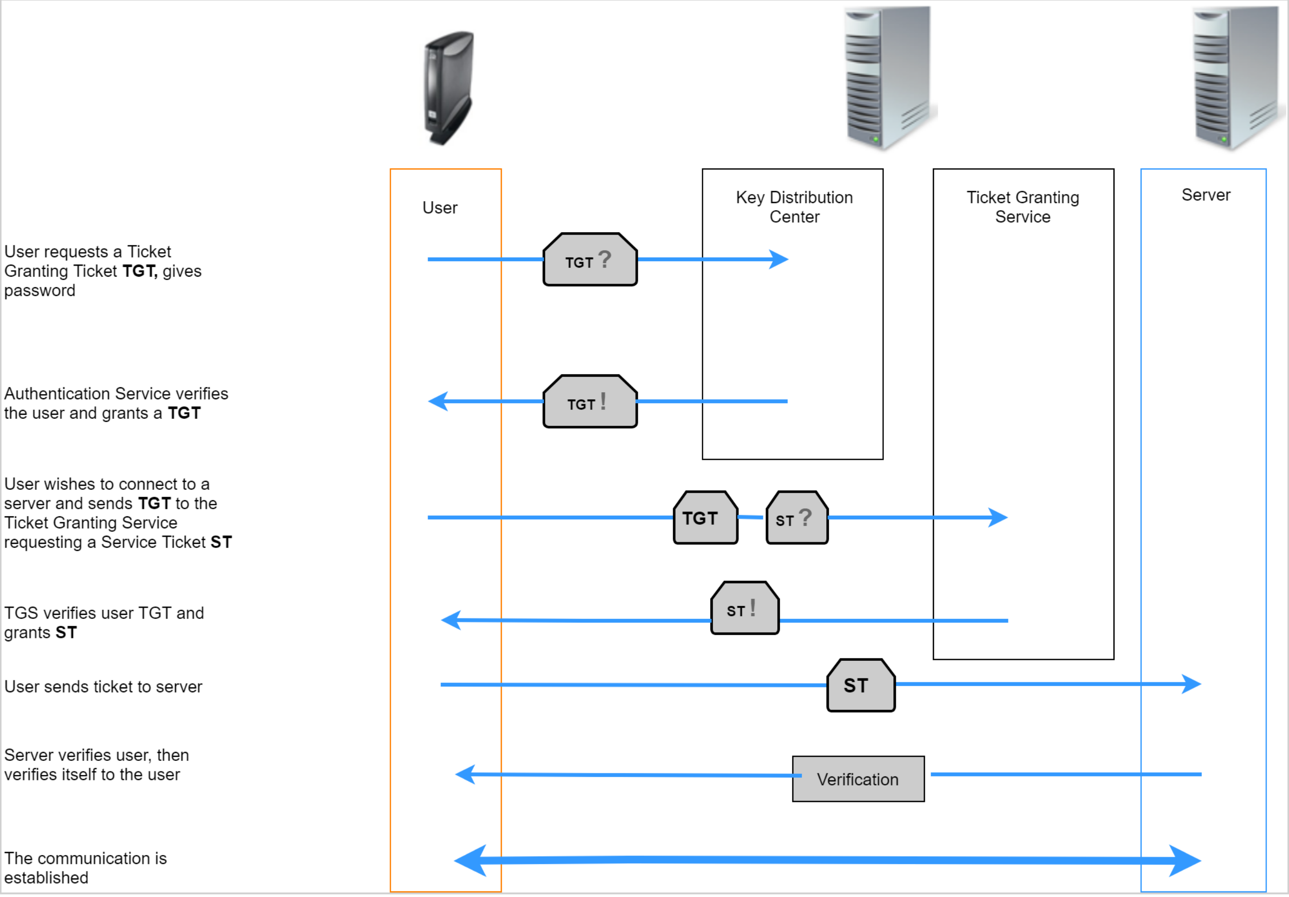
Two methods of single sign-on for a session are available:

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.


User
Key Distribution Center
Ticket Granting Service
Server
User requests a Ticket Granting Ticket **TGT,** gives password
TGT ?
Authentication Service verifies the user and grants a **TGT**
TGT !
User wishes to connect to a server and sends **TGT** to the Ticket Granting Service requesting a Service Ticket **ST**
TGT
ST ?
TGS verifies user TGT and grants **ST**
ST !
User sends ticket to server
ST
Server verifies user, then verifies itself to the user
Verification
The communication is established

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 926)
2. Enable passthrough authentication in the relevant session. (see page 933)

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 927)
- Configure the domain. (see page 928)
- Activate login to the Active Directory domain. (see page 930)

ⓘ When activating the **Smartcard** login method, some additional configuration may be necessary (see page 931).

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

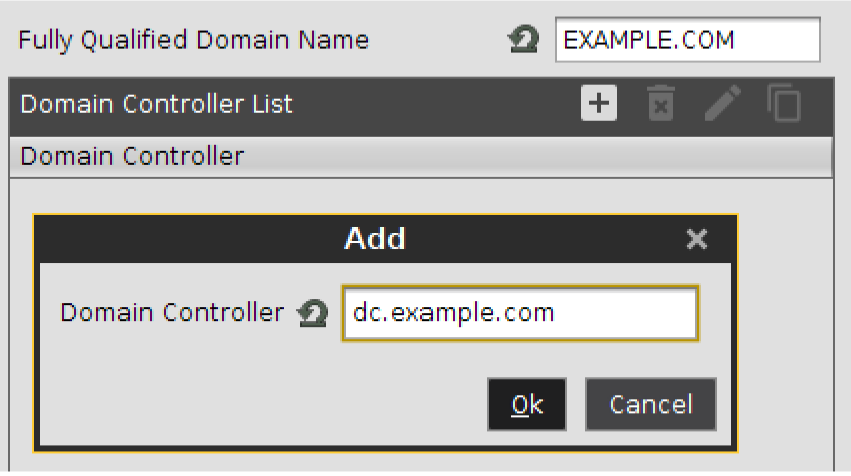
To configure the domain(s) proceed as follows:

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.



Fully Qualified Domain Name: EXAMPLE.COM

Domain Controller List

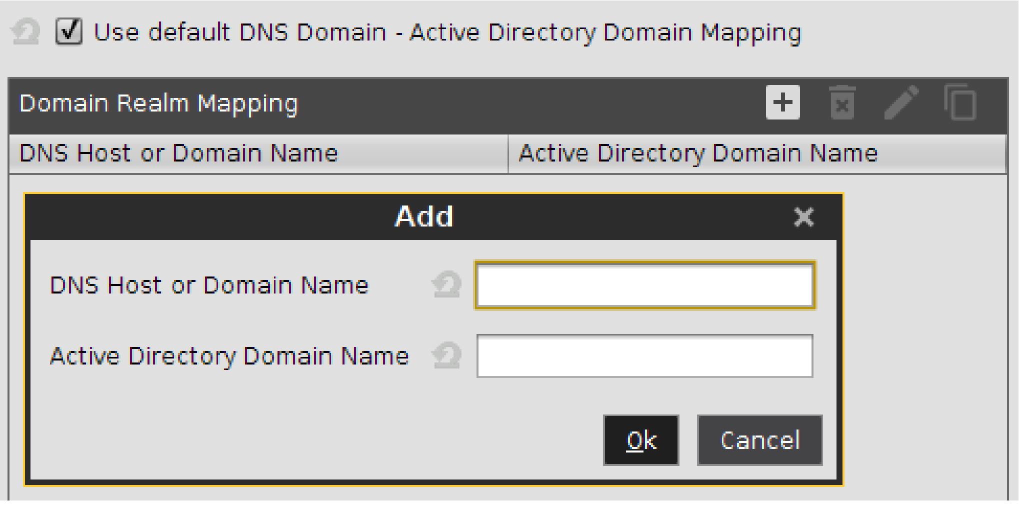
Domain Controller

Add

Domain Controller: dc.example.com

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**.



☑ Use default DNS Domain - Active Directory Domain Mapping

Domain Realm Mapping

DNS Host or Domain Name	Active Directory Domain Name

Add

DNS Host or Domain Name

Active Directory Domain Name

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 (see page 574).

> ⓘ 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 Legacy ICA Sessions (see page 934)
- Citrix StoreFront/Web Interface (see page 935)
- RDP (see page 936)
- Horizon Client (see page 937)
- Parallels Client (see page 938)

Citrix Legacy ICA Sessions

To activate Kerberos passthrough for all ICA sessions:

1. Go to **Sessions > Citrix XenDesktop / XenApp > HDX/ICA Global > Local Logon**.
2. Activate **Use Kerberos Passthrough authentication for all ICA sessions**.

To activate passthrough for a specific ICA session:

1. Go to **Sessions > Citrix XenDesktop / XenApp > Legacy ICA Sessions > [session name] > Logon**.
2. Select the passthrough method:
   - To use Kerberos passthrough, activate **Use Kerberos Passthrough authentication for this session**.
   - To use passthrough (with the cached local thin client credentials), activate **Use Passthrough authentication for this session**.

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**: This will only work with Web Interface, not with StoreFront.
   - **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.

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.

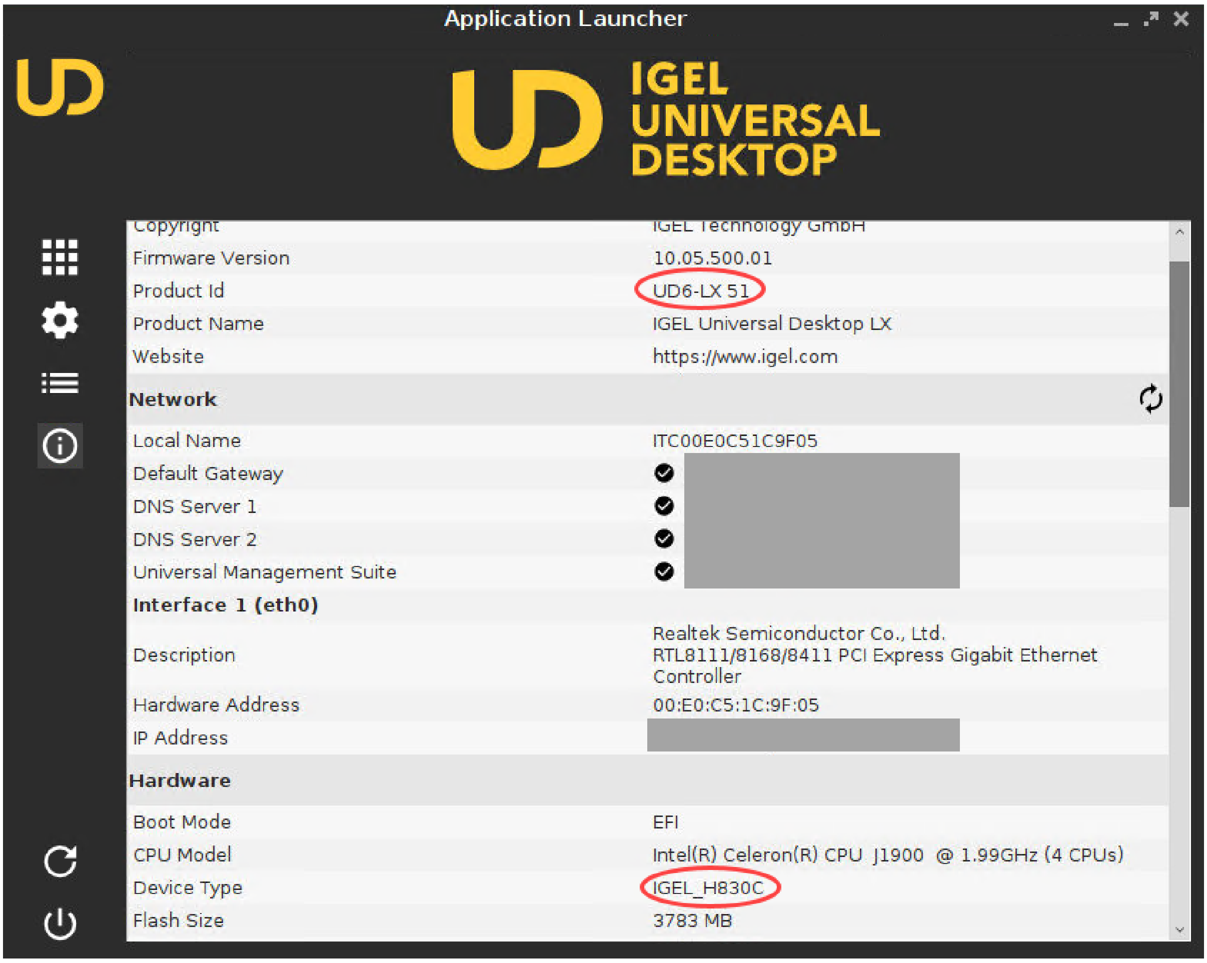
Hardware Video Acceleration on IGEL OS

Question

Does my hardware with IGEL OS offer video acceleration?

Answer

Open **Application Launcher > About** to look up your product ID and device type:



Copyright	IGEL Technology GmbH
Firmware Version	10.05.500.01
Product Id	UD6-LX 51
Product Name	IGEL Universal Desktop LX
Website	https://www.igel.com
Network	
Local Name	ITC00E0C51C9F05
Default Gateway	✓ [redacted]
DNS Server 1	✓ [redacted]
DNS Server 2	✓ [redacted]
Universal Management Suite	✓ [redacted]
Interface 1 (eth0)	
Description	Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
Hardware Address	00:E0:C5:1C:9F:05
IP Address	[redacted]
Hardware	
Boot Mode	EFI
CPU Model	Intel(R) Celeron(R) CPU J1900 @ 1.99GHz (4 CPUs)
Device Type	IGEL_H830C
Flash Size	3783 MB

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
IZ2-HDX/RFX/ HORIZON 40	IGEL D220	Intel Bay Trail	✓	✓	✓
IZ3-HDX/RFX/ HORIZON 41, 42	IGEL M330C	VIA VX900	✓		
IZ3-HDX/RFX/ HORIZON 50	IGEL M340C	ATI Mullins		✓	✓
IZ3-HDX/RFX/ HORIZON 51	IGEL M340C	ATI Mullins			✓
UD2-LX 40	IGEL D220	Intel Bay Trail	✓	✓	✓
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			✓
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			✓
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

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`

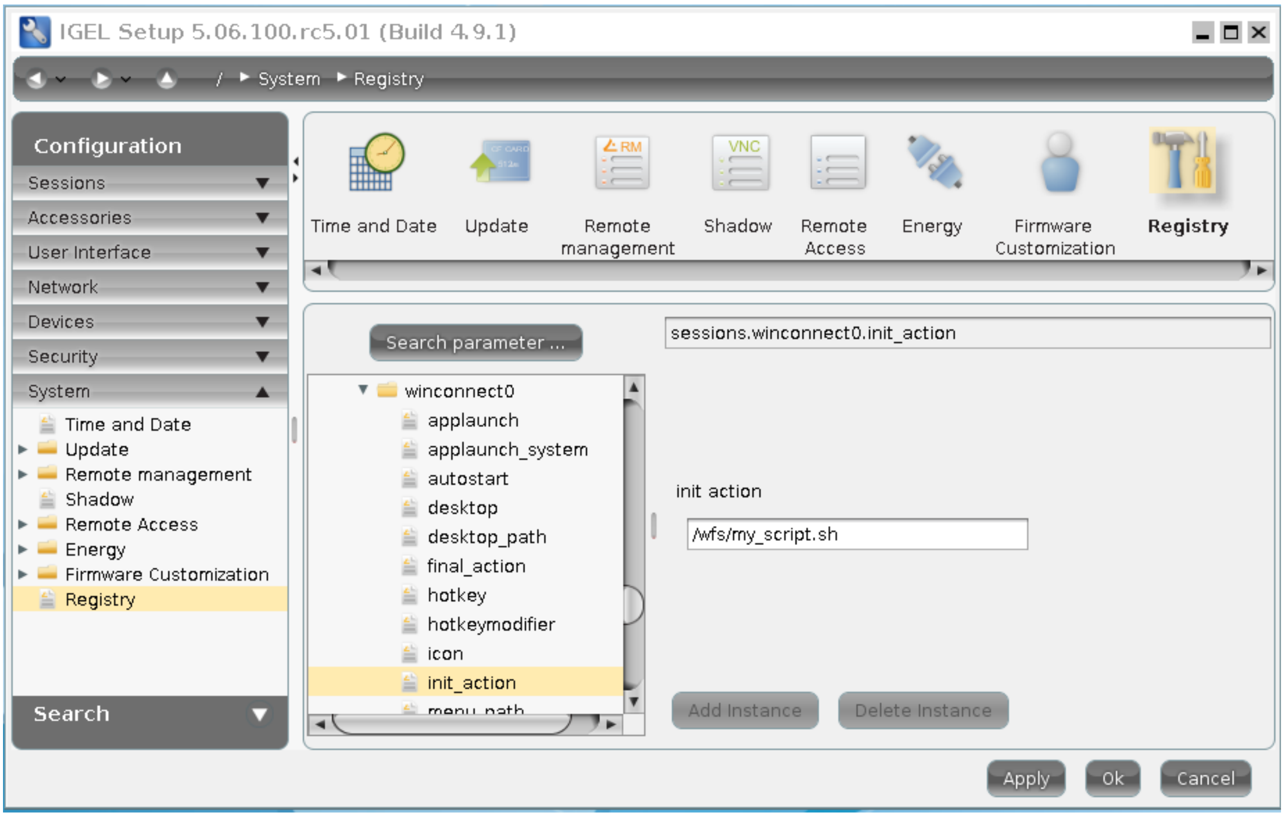
for Citrix/ICA:

`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:



IGEL Setup 5.06.100.rc5.01 (Build 4.9.1)

sessions.winconnect0.init_action

init action: /wfs/my_script.sh

ⓘ 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

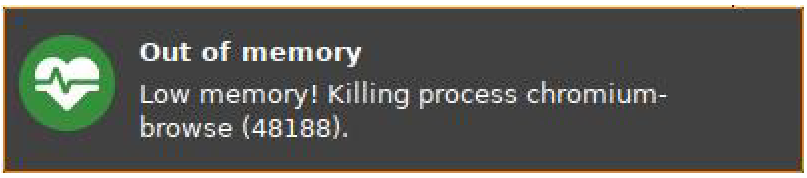
To start the IGEL Setup within the appliance mode, press hotkey [Ctrl+Alt+F2].

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:



Out of memory

Low memory! Killing process chromium-browse (48188).

Environment

- IGEL OS 11.04 or higher

Problem

The system is running out of memory. As a countermeasure, the system has terminated the application.

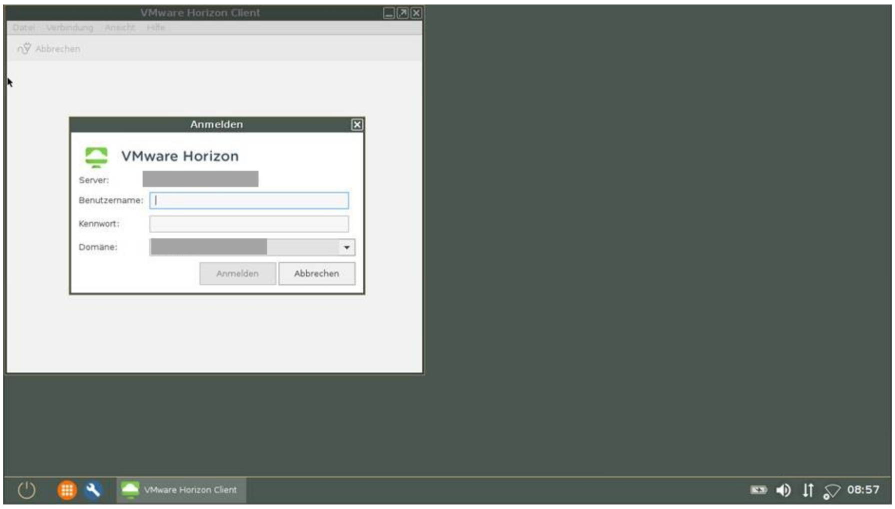
Solution

- ▶ 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.



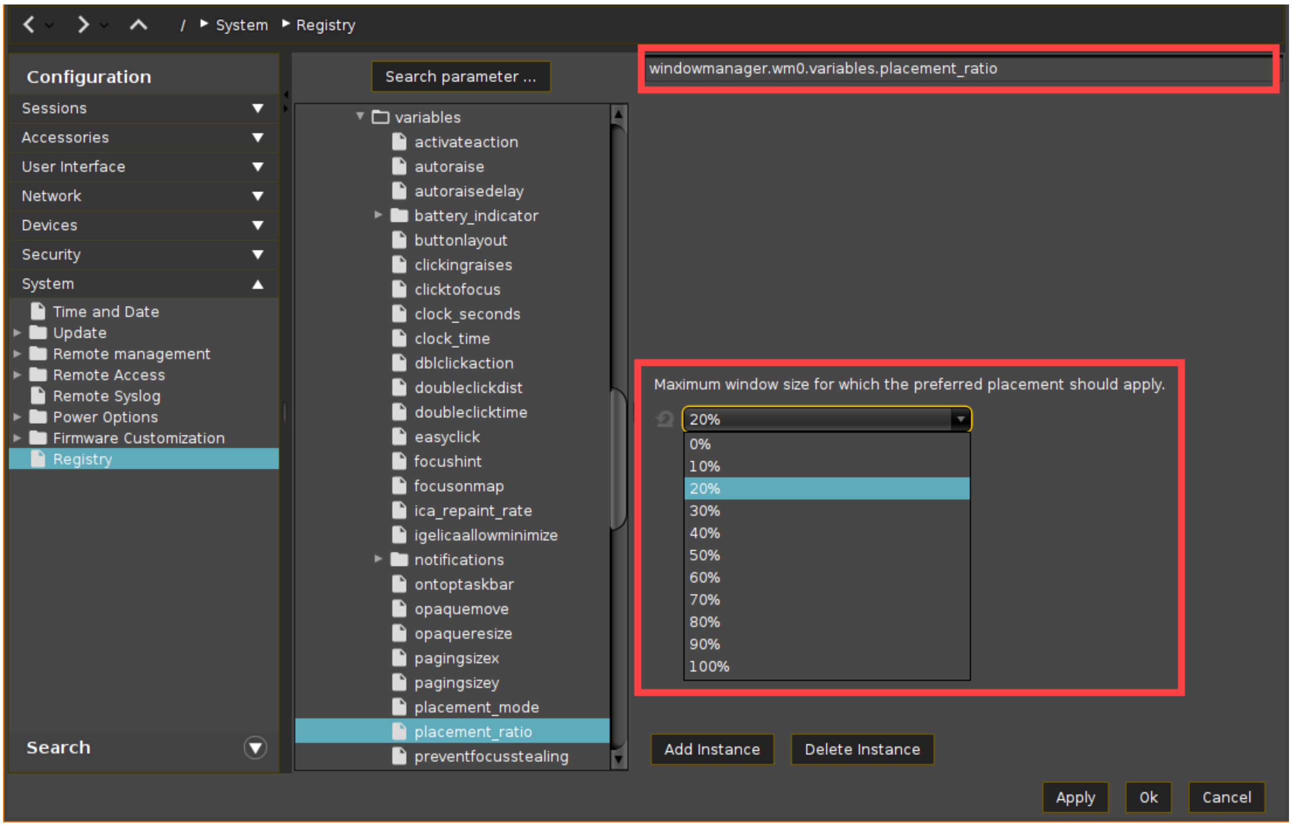
Problem

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`.



windowmanager.wm0.variables.placement_ratio

Maximum window size for which the preferred placement should apply.

20%

Example

Session: VMware Horizon Client
Screen resolution: 1366x768
Value for **Maximum window size for which the preferred placement should apply**: at least 40%

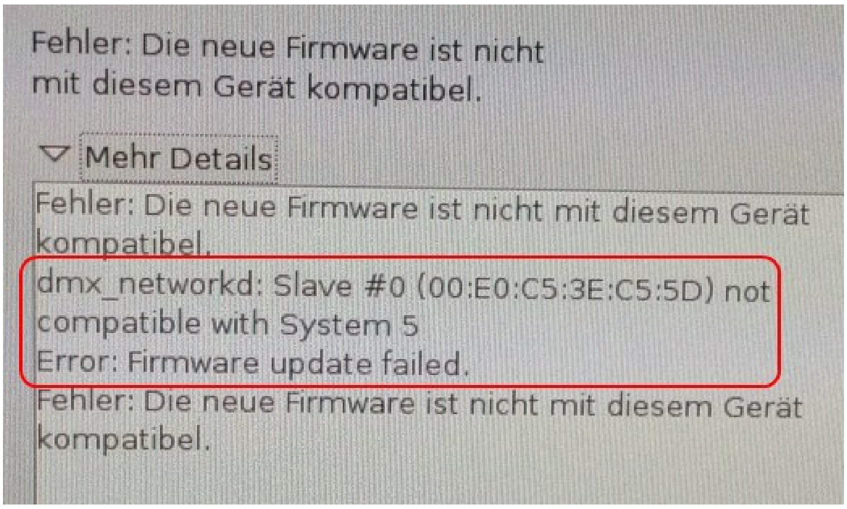
Updating IGEL UMD: Error "not compatible with System5"

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
```



Fehler: Die neue Firmware ist nicht
mit diesem Gerät kompatibel.

Fehler: Die neue Firmware ist nicht mit diesem Gerät kompatibel.
dmx_networkd: Slave #0 (00:E0:C5:3E:C5:5D) not compatible with System 5
Error: Firmware update failed.
Fehler: Die neue Firmware ist nicht mit diesem Gerät kompatibel.

Solution

Delete file `/tmp/NOT_SYS_5_COMPATIBLE` from UMD master client and update again without rebooting.

IGEL OS Features that Require the Multimedia Codec Pack

Some features in IGEL OS require the separately available Multimedia Codec Pack. These codecs enable multimedia redirection in remote sessions, faster rendering of remote screen contents, and multimedia playback in the browser and media player.

ⓘ IGEL zero clients contain the Multimedia Codec Pack by default.

ⓘ On selected IGEL devices, hardware video acceleration (see page 939) is available.

Here is an overview of the affected IGEL setup pages and parameters:

Use Case	Setup Page	Parameter	Feature
Citrix Session	**Sessions > Citrix > Citrix Global > HDX Multimedia**	**Multimedia redirection**	Redirection of H.264, WMV, MPEG-1, MPEG-2, MPEG-4 ASP (DivX, Xvid) videos, WMA and MP3 audio
	Sessions > Citrix > Citrix Global > Codec	**Graphical codec**	Citrix H.264 deep compression codec support
	Sessions > Citrix > Citrix Global > HDX Multimedia	**HDX RealTime Media Engine**	Skype for Business H.264 with HDX Realtime Media Engine (RTME)

RDP Session	**Sessions > RDP > RDP Global > Multimedia**	**Enable Video Redirection**	Redirection of H.264, WMV, MPEG-4 ASP (DivX) videos, WMA and MP3 audio
	Sessions > RDP > RDP Global > Performance	**Enable RemoteFX**	RemoteFX 8 EVOR support
	Sessions > RDP > RDP Sessions > [session name] > Performance	**Enable RemoteFX**	RemoteFX 8 EVOR support

Horizon Session	**Sessions > Horizon Client > Horizon Client Global > Multimedia**	**VMware Multimedia Redirection**	Redirection of H.264, WMV, MPEG-4 ASP (DivX), WMA and MP3 audio with RDP
	Sessions > Horizon Client > Horizon Client Sessions > [session name] > Multimedia	**Multimedia Redirection**	Redirection of H.264, WMV, MPEG-4 ASP (DivX) videos, WMA and MP3 audio with RDP
	Sessions > Horizon Client > Horizon Client Global > Server Options	**Preferred desktop protocol > VMware Blast**	H.264 hardware acceleration

Web Browser	**Sessions > Browser**		Playback of embedded H.264 videos, playback of H.264, WMV, MPEG-1, MPEG-2, MPEG-4 ASP (DivX, Xvid), WMA and MP3 audio with media player plugin

Media Player	**Sessions > Media Player**		Playback of H.264, WMV, MPEG-1, MPEG-2, MPEG-4 ASP (DivX, Xvid) videos, WMA and MP3 audio; AAC audio