IGEL OS Articles

Update and Upgrade

Buddy Update

A certain number of IGEL thin clients or UDC3 converted devices 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.
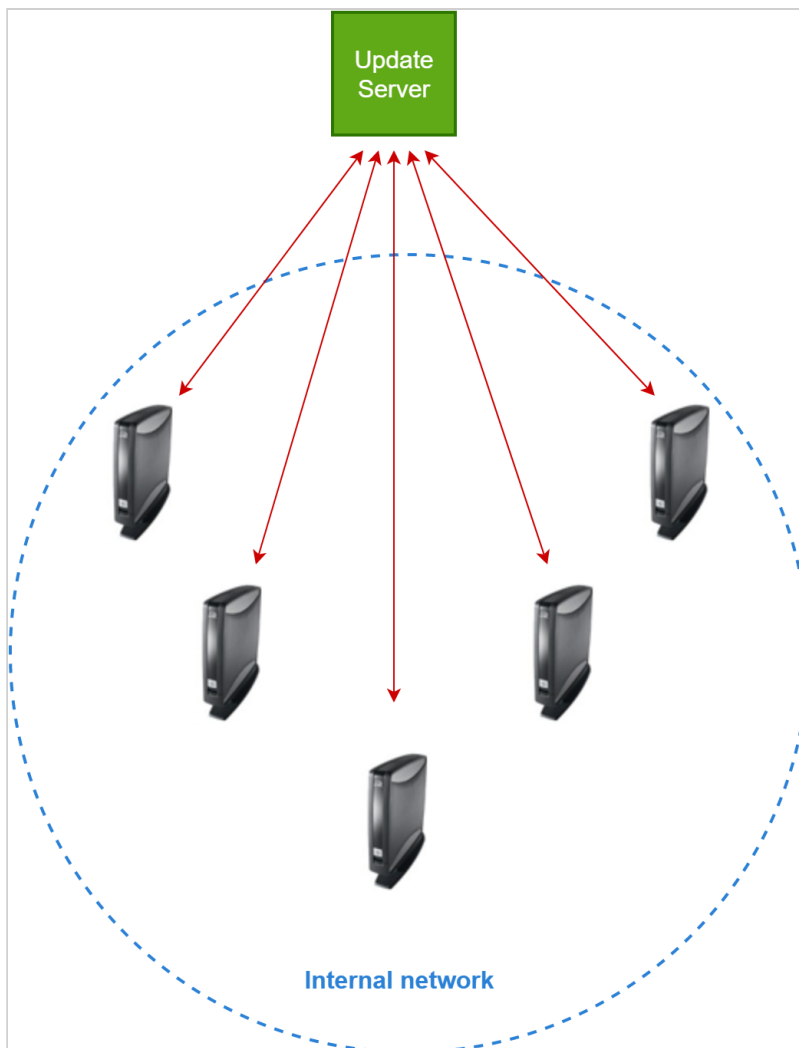
Set up one of your clients as a so-called buddy update server. In the future, only this client will access the main server to download the updates. All other clients access the local buddy update server from within the network and will no longer offload the network outside.
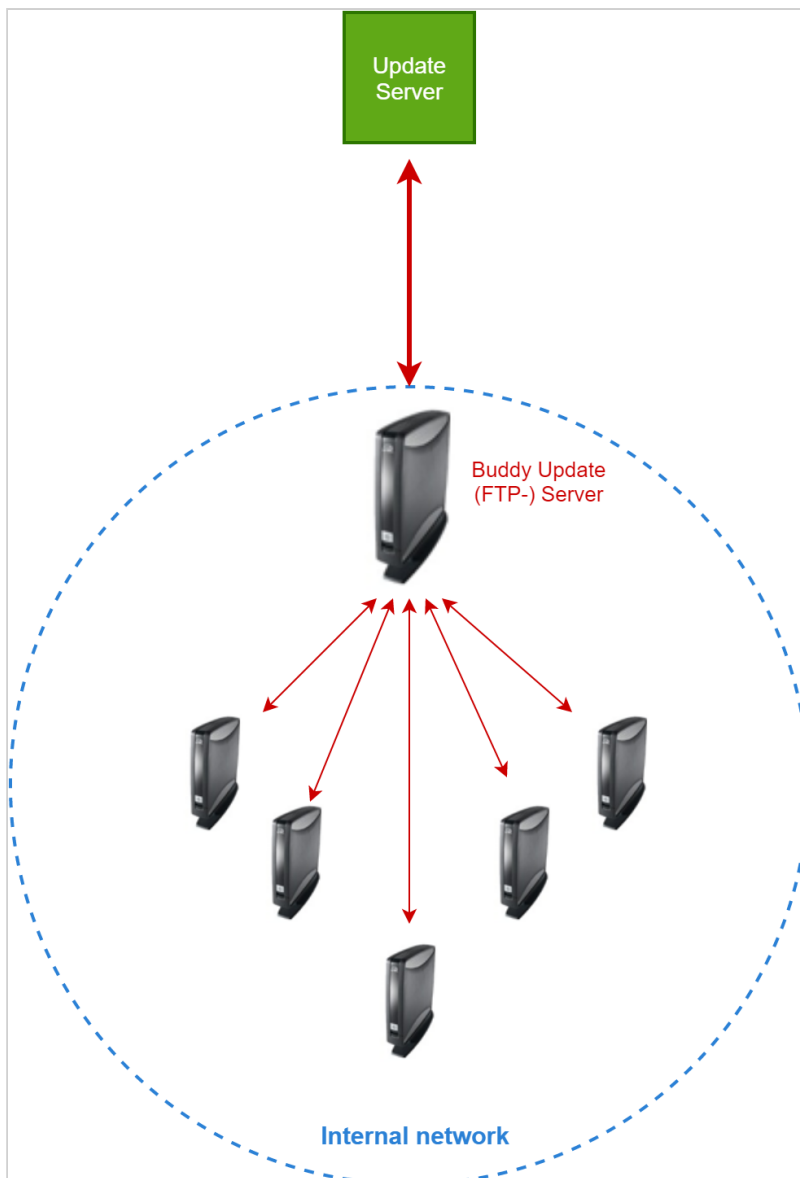
> ⓘ The buddy update server is always an FTP server.

For the configuration details, see:

- Settings on the Buddy Update Server (see page 7)
- Settings on the Client Side (see page 8)

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

Settings on the Buddy Update Server

Configure the Buddy Update Server:

1. Click **System > Update > Buddy Update**.
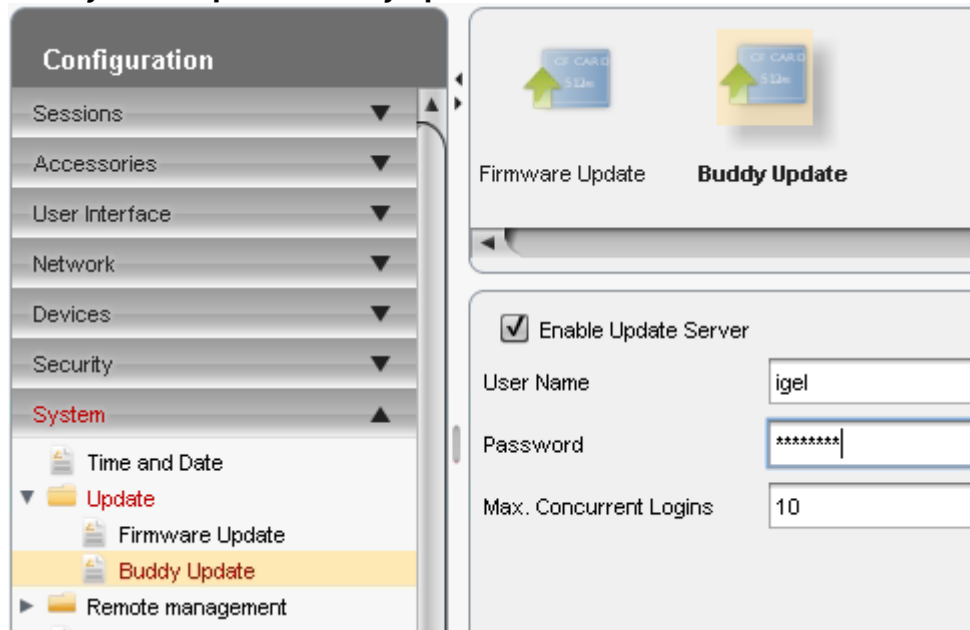
2. Activate **Enable Update Server**.
3. Enter the credentials **User Name** and **Password**.
4. Specify the maximum number of **Concurrent Logins** allowed.
5. Click **Save** to confirm the changes.
6. Perform a complete Firmware Update on the server.
7. Reboot the server.

> ⓘ Whenever a buddy update server has received a firmware update, it needs to be rebooted before it can distribute the new firmware to other clients.

Settings on the Client Side

Configure your clients:

1. Click **System > Update > Firmware Update**.
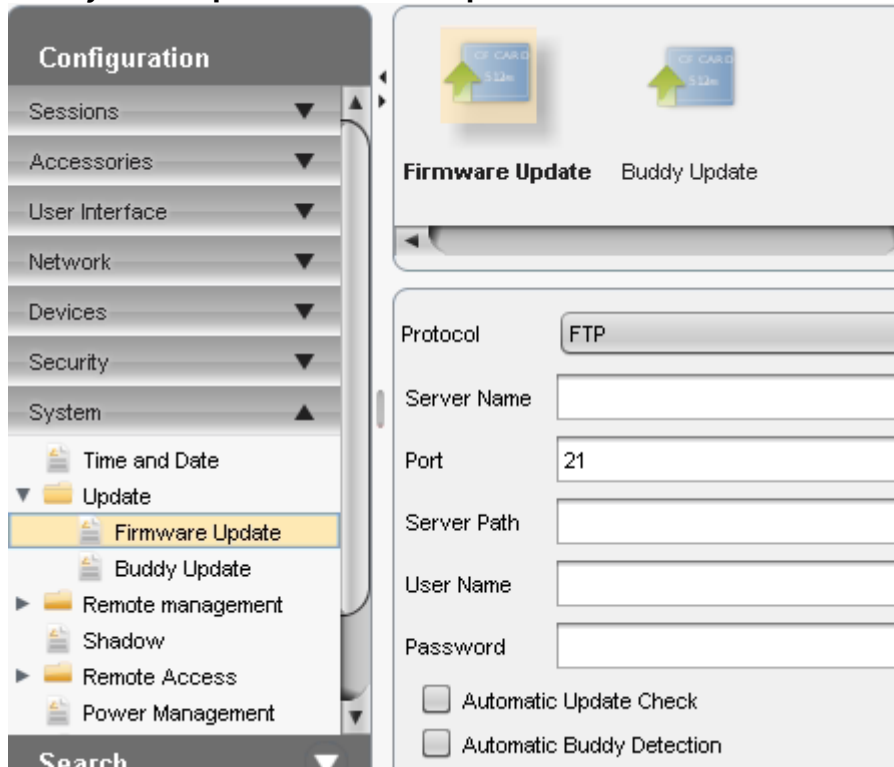
2. Set the following parameters:
   Server Name: IP-address of the buddy update server
   Port: 21 (default with FTP protocol)
   Server Path: -
   User Name, **Password** of the buddy update server.
3. Activate **Automatic Update Check** if you want the client to check automatically during the boot 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.
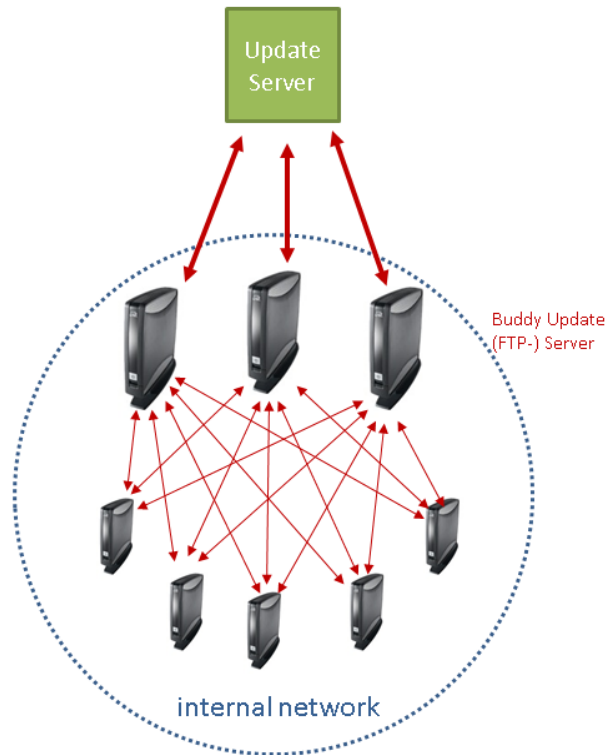
In this case, you do not need to define the **Server Name**, **Port,** and **Server Path**. If you enter a server name anyway, the system treats this server as a fall-back. Thus, you can be sure that the system accesses at least this one server if it cannot find any others.

> ⓘ 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 certain server.

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[1] 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 12).
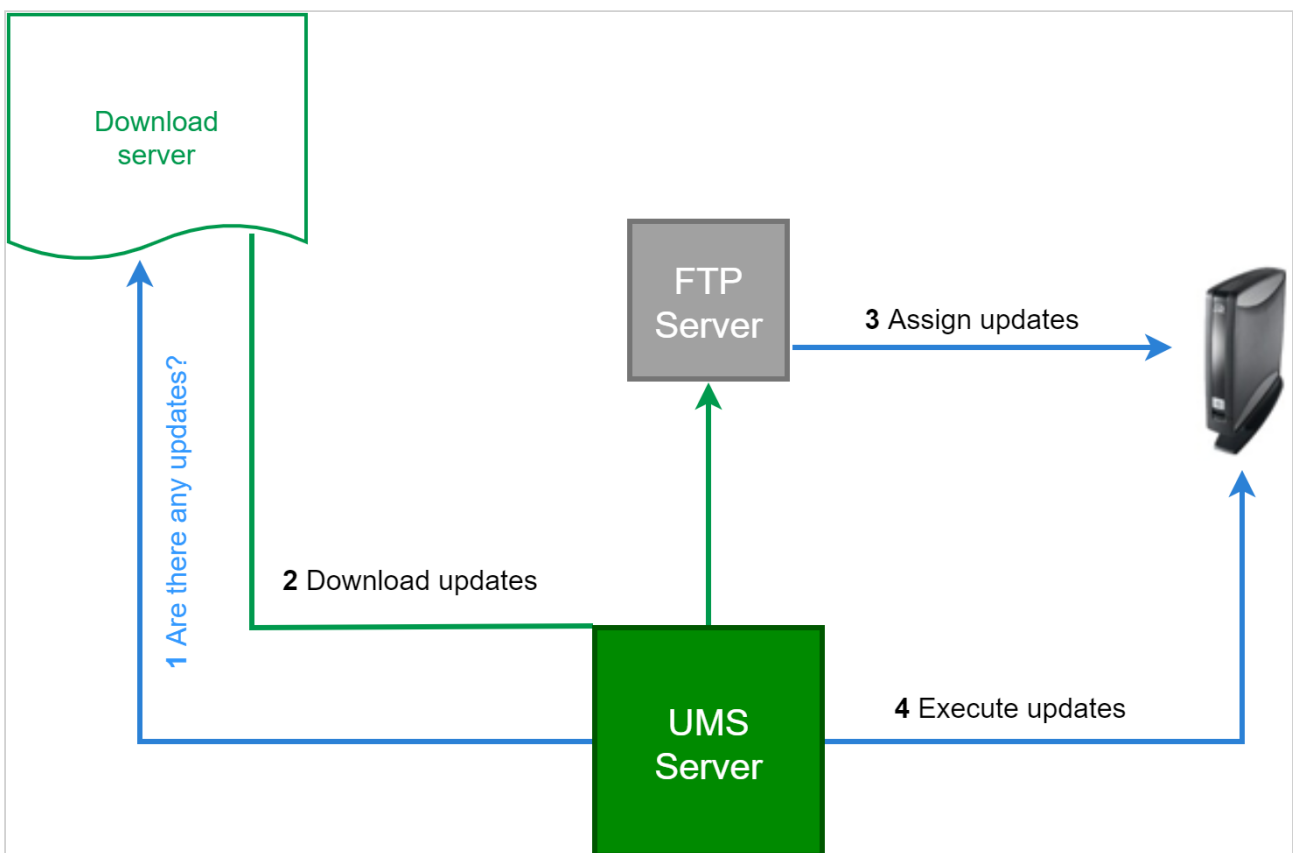
- Downloading Updates and Storing them on an FTP Server (see page 11)
- Executing an Update Process (see page 12)

---

[1] 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.

IGEL

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.

IGEL

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[2].
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 .

---

2 https://www.igel.com/software-downloads/workspace-edition/

IGEL

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`

Citrix

IGEL

Performance

IGEL

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

1. Reducing network load:

- Compression:
  Enabling the parameter **Compression** lowers used network bandwidth at the cost of increased cpu load.
    - ICA sessions: Go to **ICA > ICA Sessions > Name > Options**, parameter **Compress**
    - PN/Webinterface: Add **Compress** in the section **[Application]**, values: **On/Off**
- Persistent Cache:
  Setting the parameter **Persistent Cache Enabled** has the potential to greatly reduce network load in later sessions when using the same applications.
    - ICA sessions: Go to **ICA > ICA Sessions > Name > Options**, parameter **Persistent Cache Enabled**
    - 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 **ICA > ICA 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 **ICA > ICA Global > Options**, parameter **Cache Size** (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** (Byte).
  - ICA sessions: Go to **ICA > ICA Global > Options**, parameter **Minimum Bitmap Size** (Byte)
  - 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 **ICA > ICA Sessions > Name > 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

1. 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 ICA > **ICA Sessions > Name > 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 noticable when the screen contents refreshes rapidly, e.g. during scrolling.
  - ICA sessions: Go to **ICA > ICA Global > Options**, parameter **Deferred screen update mode**
  - PN/Webinterface: Add **DeferredUpdateMode** in the section **[WFClient]**, values: **True/False**
- Improve writing performance for redirected USB devices:
  To speed up writing on redirected USB media, it is possible to deactivate the parameter sync_option.

  > ⛔ 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**

IGEL

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 XenDesktop/XenApp > HDX / ICA Global > Options**:

- **Use server redraw**
- **Allow backing store**
- **Deferred screen update mode**
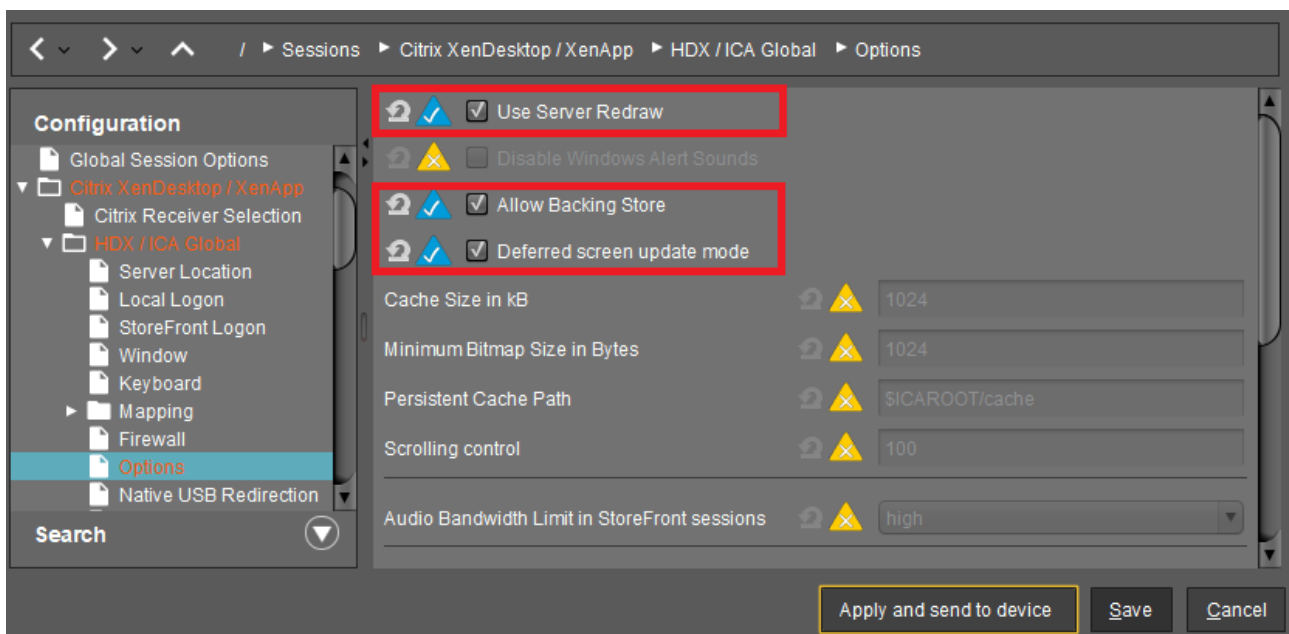
See also Options in the manual chapter for Citrix.

IGEL

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.

IGEL

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

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 XenDesktop / XenApp > HDX / ICA Global > Codec**.
2. Disable **Text Tracking**.
3. Disable **Small Frames Feature**.

Graphical Codec	H.264 Deep Compression Codec ▼

Additional parameters for H.264 Deep Compression Codec
- ☐ Text Tracking
- ☐ Small Frames Feature
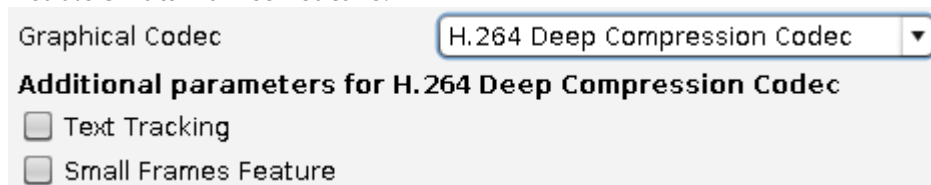
IGEL

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

IGEL

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

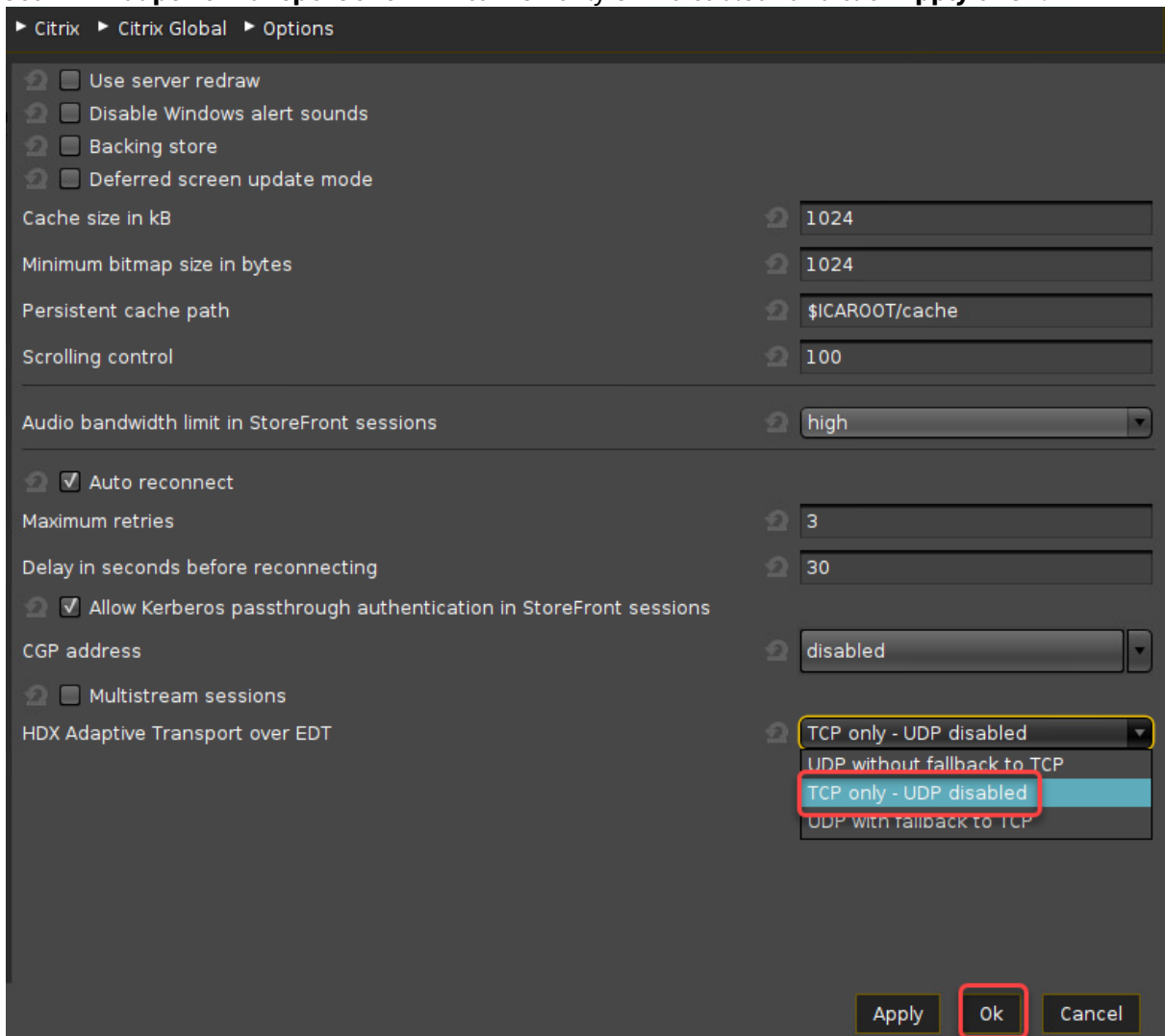The HDX transport protocol is set to "UDP with fallback to TCP", which causes slow performance.

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**.

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

IGEL

Mouse

IGEL

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 b*rowser.

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

▶ Open IGEL registry in local client setup or UMS.
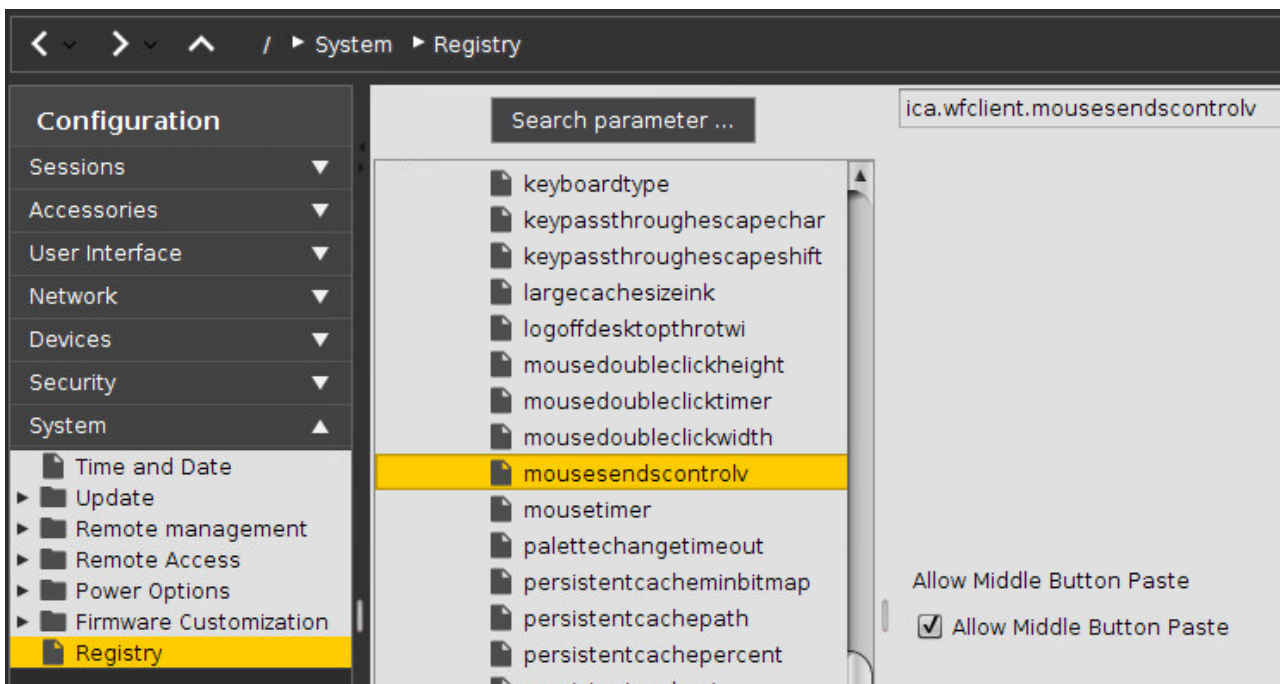
▶ For Citrix sessions change:

- **System > Registry > ica.wfclient.mousesendscontrolv**
- **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.

IGEL

How to Connect a SpaceMouse with a Citrix Session

This article describes how to use a *3Dconnexion SpaceMouse* in a Citrix HDX Session.

> ⛔ Citrix Workspace App 13.9 or older: Do not redirect the SpaceMouse if it is the only mouse connected to your thin client! After redirecting, the local system would be without a mouse. Make sure to use a second mouse for the local device in this scenario.

1. In Setup, go to **Sessions > Citrix XenDesktop/ XenApp > HDX/ ICA Global > Native USB Redirection**
2. Activate the checkbox **Enable native USB Redirection**
3. Set the **Default Rule** to **Deny**.
4. Add a device exception rule as in the following screenshot with the Product- and Vendor-ID of your specific SpaceMouse:
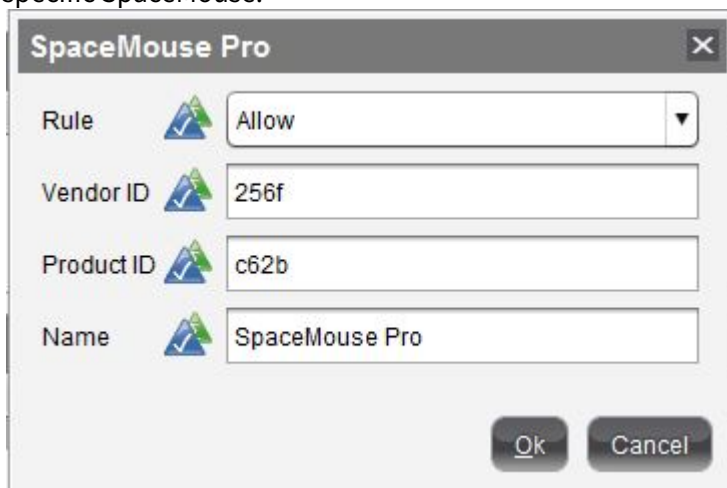
> ⓘ In order to find out the Vendor ID and Product ID, open a **Local Terminal** and issue the command `lsusb`. This will show a list containing the connected USB-Devices and their IDs.

The SpaceMouse is ready for use.

Additional Steps for IGEL Linux 10

If your device has IGEL Linux 10 / IGEL OS 10, the SpaceMouse is used as an additional mouse for the local system. Because of this, the SpaceMouse will interfere with the local mouse pointer. You can prevent this by denying local USB access.

To prevent the SpaceMouse from interfering:

1. In Setup, go to **Devices > USB access control** and activate **Enable**.
2. In the **Device Rules** area, click ⊞ to add a new device rule.

IGEL

3. Set the device rule as follows:
   - **Rule**: Deny
   - **Vendor ID**: 256f
   - **Product ID**: c62b
4. Click **Ok** in the dialog and then **Apply** or **Ok** in the Setup.

IGEL

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 LX Client within Citrix sessions?

> ℹ 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 Device
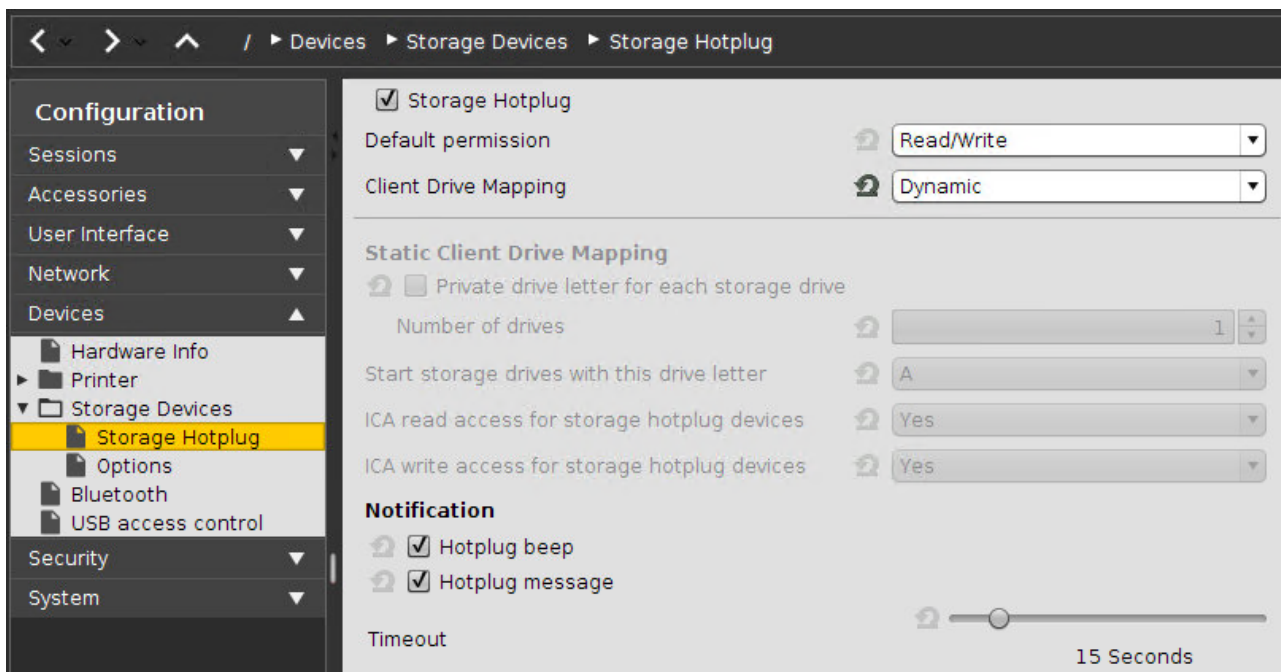
Within the IGEL Setup or a UMS profile, you basically need to configure these parameters:

▶ 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 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 **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 > ICA/HDX 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 (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 RDP 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

IGEL

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.

IGEL

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).
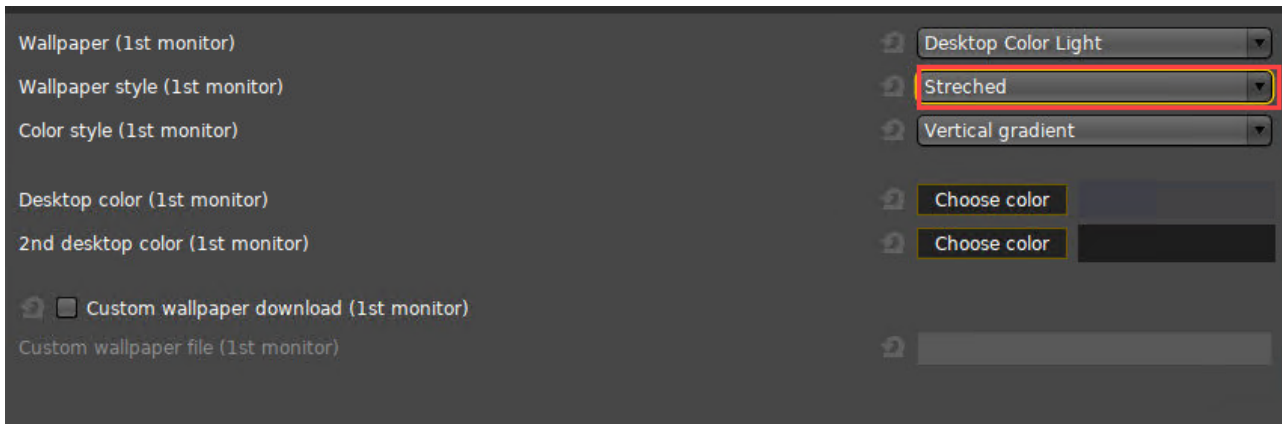
Pictures:

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**.

IGEL

▶ 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)**.

▶ 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.

IGEL

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 XenDesktop (for published desktops only, not for published applications)
- Citrix Self-Service
- 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:

- StoreFront/Web Interface (see page 42): Integrates published applications into the IGEL GUI.
- Citrix Self-Service (see page 43): 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 54): Shows only the web interface of the farm and hides the IGEL GUI completely.
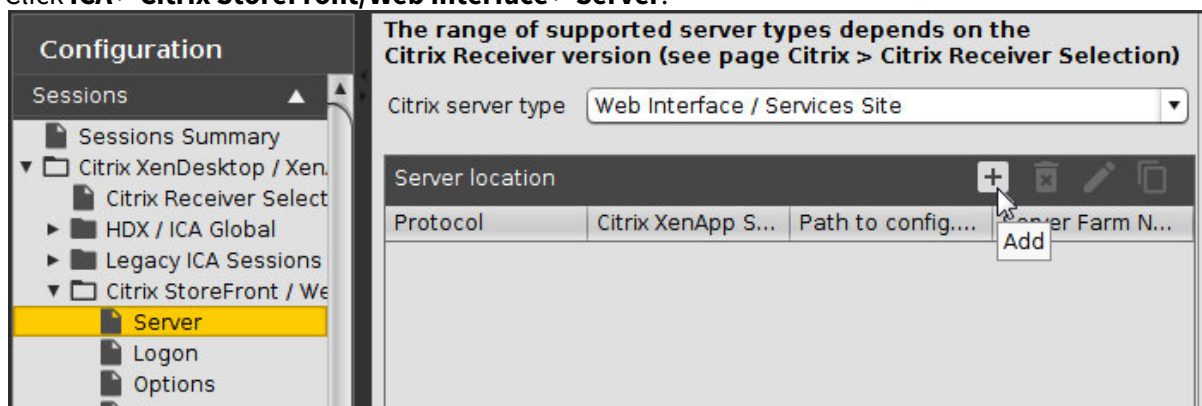
IGEL

StoreFront/Web Interface

Prerequisites:

- Citrix XenDesktop 7.5 or newer
- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates (see page 280))

Connecting via **StoreFront/Web Interface**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **ICA > Citrix StoreFront/Web Interface > Server**.

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

IGEL

Citrix Self-Service

Problem

You want your *Citrix* users to select the published applications they need to work with themselves instead of defining applications for every single user profile.

Solution

Citrix Self-Service is the solution to go with. 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. You can configure the system to cache the user's selection of applications or reset available applications to a defined default set. Activating the kiosk mode will restrict the user to preset applications.

> ⓘ 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.

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 45) (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 45)

#

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

#

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.

![IGEL](IGEL logo)

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](#)

IGEL
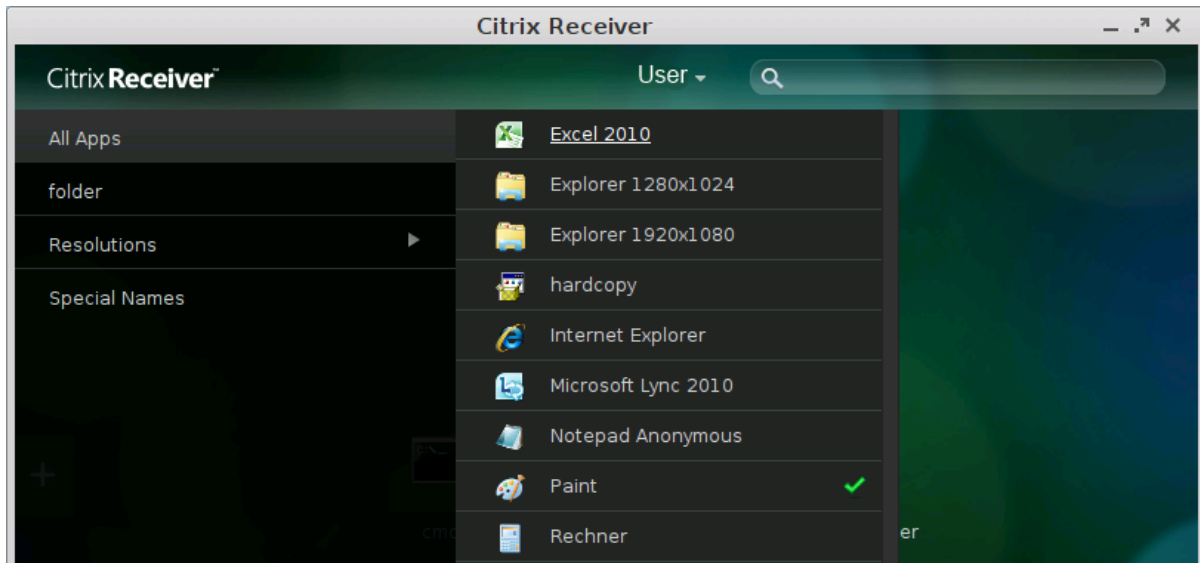
Configure Full-Screen Mode

Use following parameter in your Custom Command script (see page 45) 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
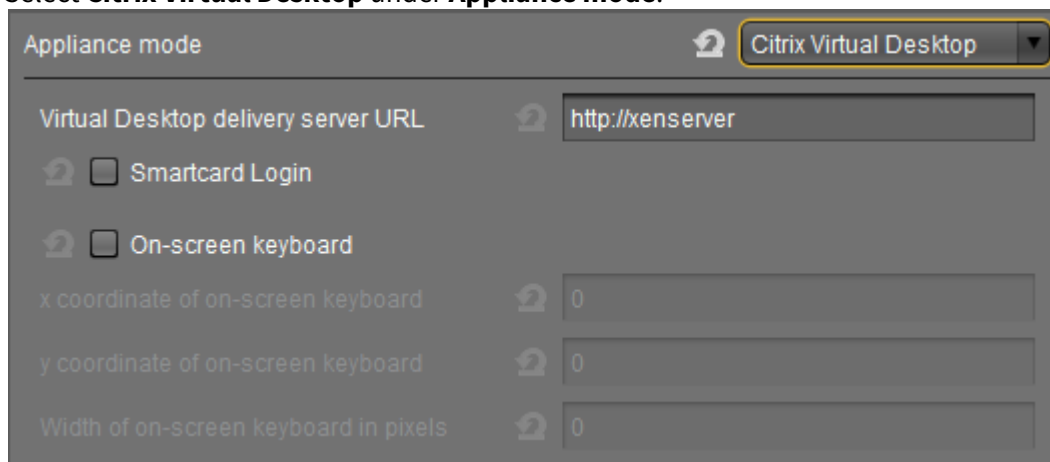
Appliance Mode

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**.

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.

IGEL

## Create a Self-Service Setup for the User with Quick Settings

Usually, the user should not have full access to the device'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 **Screen Lock/Saver**.
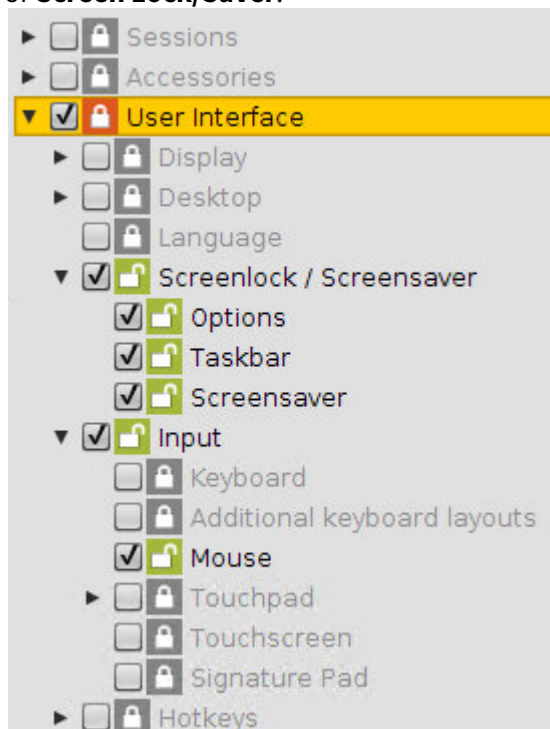
3. Click **Apply** or **Ok**.
   When the user starts **Quick Settings**, the previously selected options are presented.
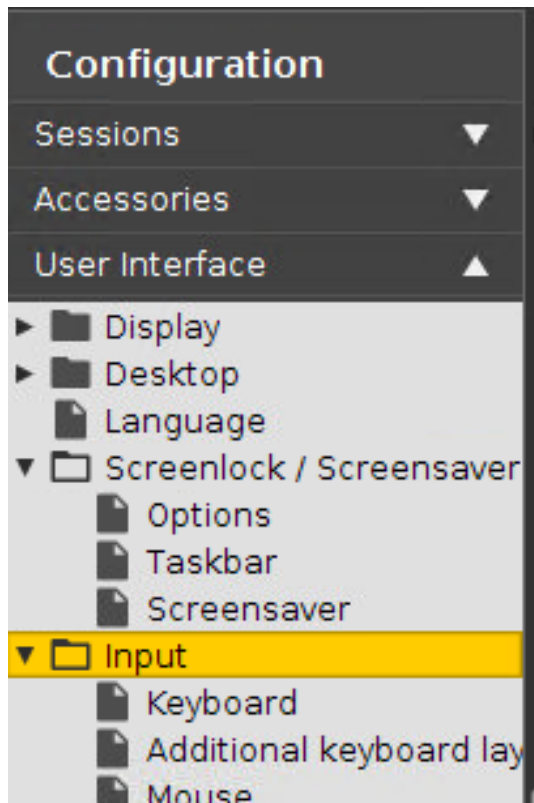
Quick settings set permissions for setup screens. If you want to set permissions for individual parameters, you can use UMS profiles. For more information, see Profiles.

IGEL

Citrix: Changing Password Issue

Symptom

A user has to change the password within session to Citrix XenDesktop 7.x or Virtual Desktop server and receives an error message during the process: `Warning: Could not connect to the Citrix server.`
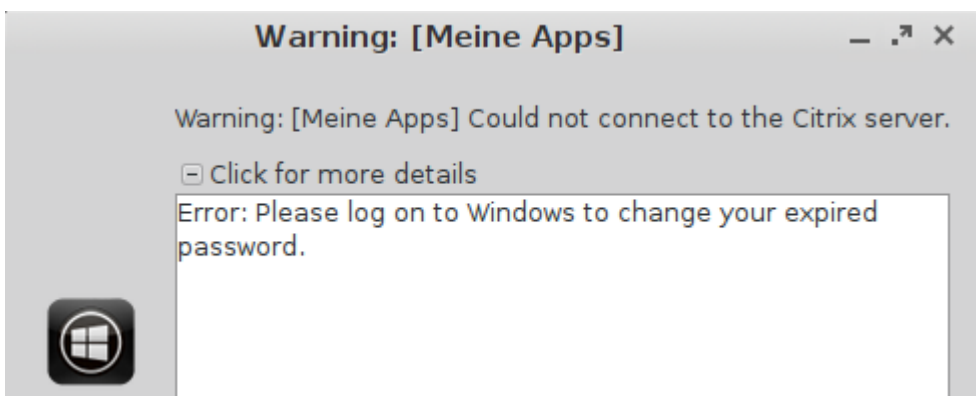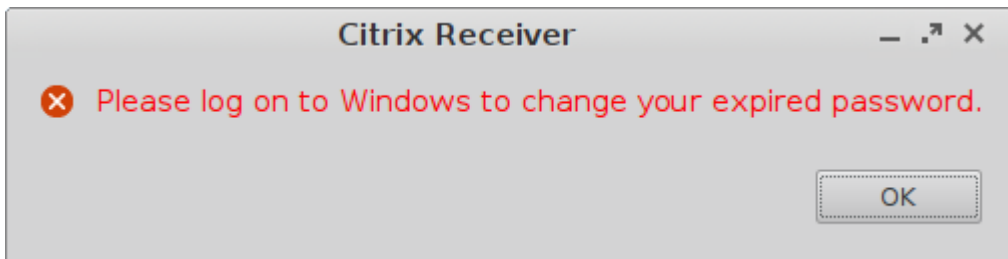
Problem

The password change option is disabled on XenDesktop 7.x server (server default setting!).

Solution

Enable password change option on your Citrix server:

1. Go to **Citrix StoreFront MMC**
2. Open page **Authentication**
3. Set **Authentication Method = User name and password**
4. Click **Manage Password Options** (right panel)
5. Enable an option allowing the password change (**Any time** or **When expired**)

IGEL

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[3]

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.

---

3 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.

IGEL

Configuring Auto Logon for XenDesktop

This how-to describes how to configure Auto Logon for XenDesktop.

Steps

1. In IGEL Setup, go to **Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Server**.
2. Add your **Server Location**.
3. Add your Active Directory domain to **Domains**, making sure that you use its Fully Qualified Domain Name (FQDN).
4. Go to **Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront / Web Interface > Logon**.
5. Set **Authentication type** to **Password authentication**.
6. Activate **Auto Logon**.
7. Set **User Name** to the Active Directory user name.
8. Set the **Password**.
9. Set **Domain** to your Active Directory domain's FQDN, the same as in step 3.

Force Citrix Logout Using Hotkey

You will find the instructions under Citrix: Freeze at Logout .

⚠ This page is due for deletion. Please check the above link and use it in the future.

IGEL

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.

IGEL

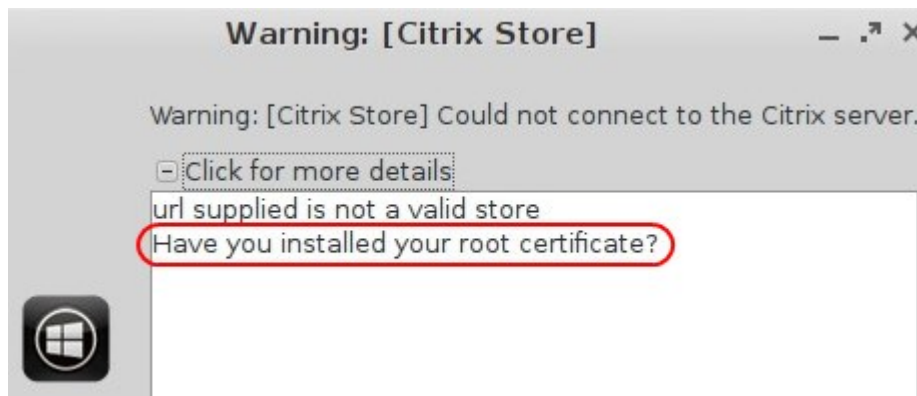# Warning Message: [Citrix Store] Could Not Connect to the Citrix Server

Environment

- You are using Citrix Receiver 13.0.x or newer.
- You have a session of the type Citrix StoreFront configured.

Symptom

- When establishing the connection, a warning message appears:
  ```
  Warning: [Citrix Store] Could not connect to the Citrix server.
  ```


  or

IGEL

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 280).

IGEL

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 XenDesktop / XenApp > Citrix Receiver Selection.**
4. Select **Citrix Receiver Version**.
5. Go to **Sessions > Citrix XenDesktop / XenApp > HDX / ICA 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 **Build to Lossless** option for **Visual Quality** 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**.

IGEL

Using Font Smoothing (ClearType) in Citrix Sessions

Symptom

- You have set **Font Smoothing** to *ClearType* in
  IGEL Setup > Sessions > ICA > ICA 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)

IGEL

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[4].

---

4 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
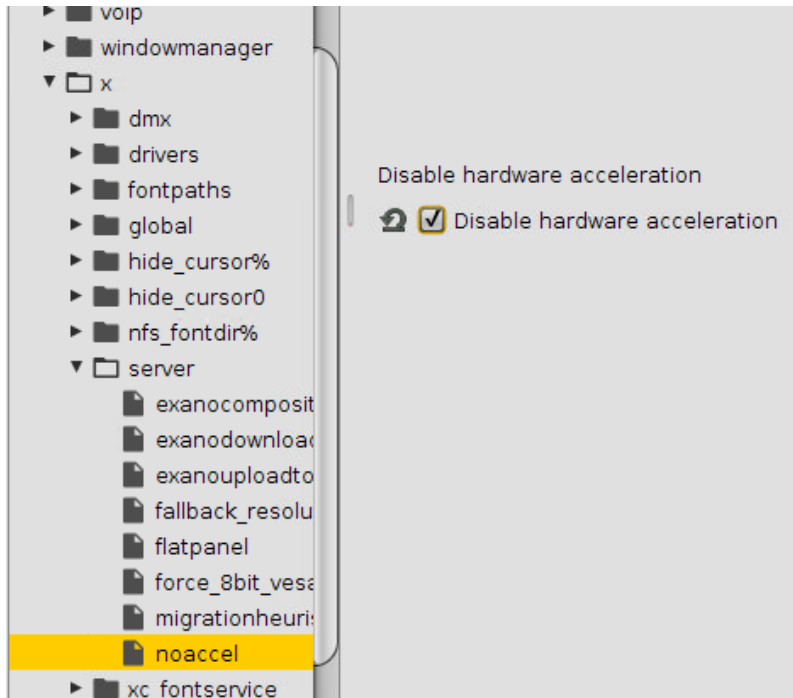
Macbook Keyboard Layout inside Citrix Session

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.

IGEL

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[5].

---

5 https://docs.citrix.com/en-us/hdx-optimization/

RDP

![IGEL logo]

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
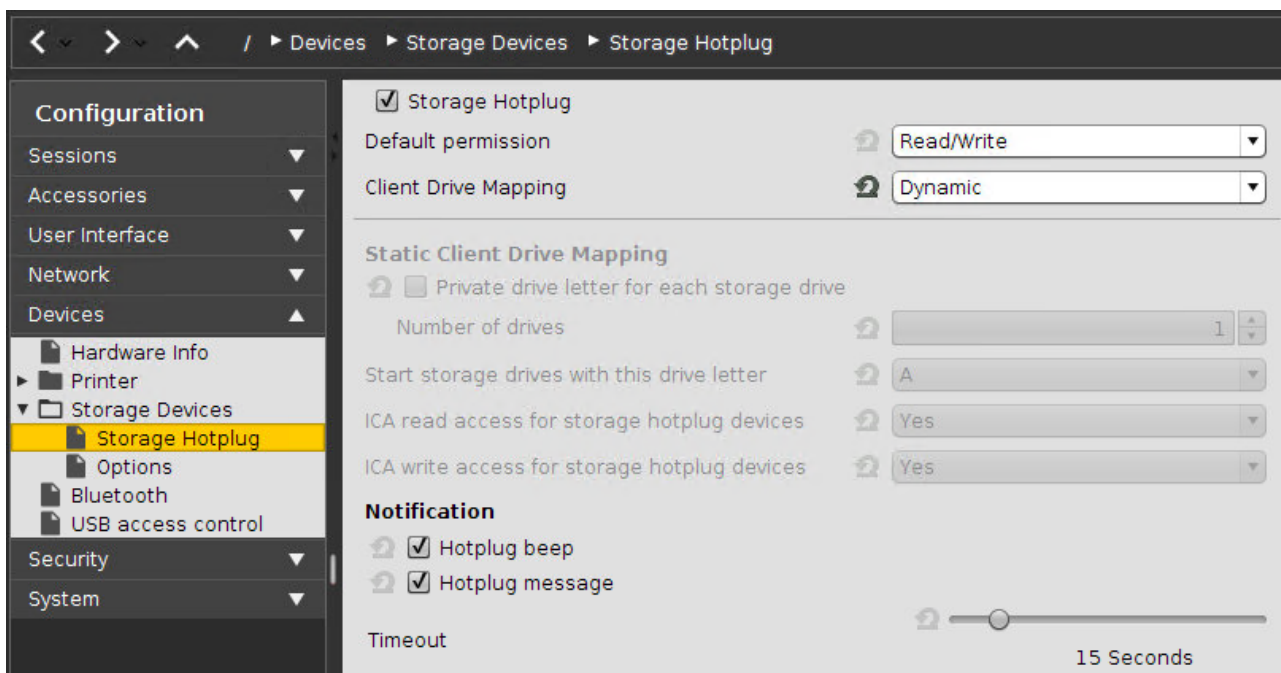
Within the IGEL Setup or an UMS profile you basically need to configure these parameters:

▶ 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 10.01 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.

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.

RDP RemoteApp Parameter Settings

Symptom

RemoteApp is not starting or closes immediately after login.

Problem

Missing or incomplete session settings on server or device

Solution

1. Set an ALIAS for the RemoteApp with the **RemoteApp Management Console** on the Terminalserver.
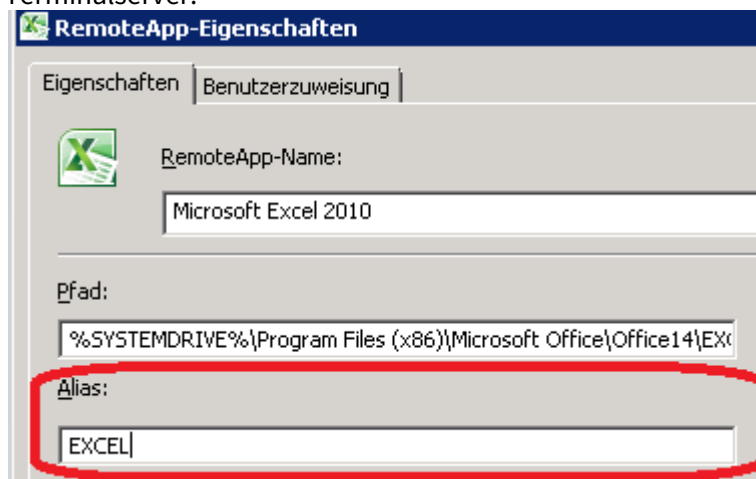
2. Use that ALIAS value in the device's setting in **Setup > Sessions > RDP > RDP Sessions > (Session Name) > Server > Application.**
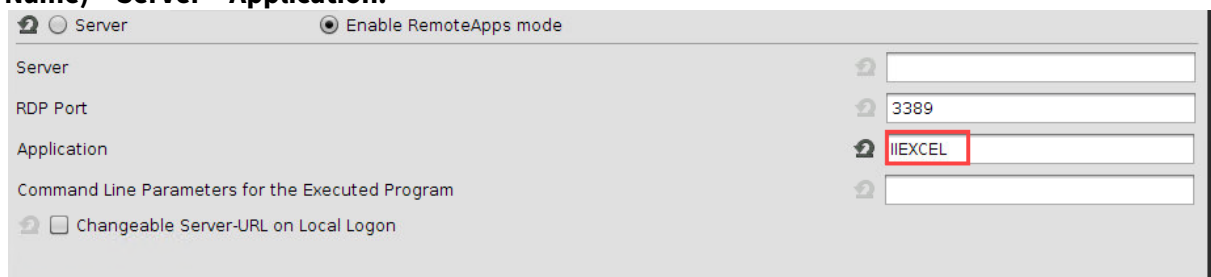
> ⓘ Add two pipe-characters (‖) at the beginning of the ALIAS value.

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".

IGEL

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)
```
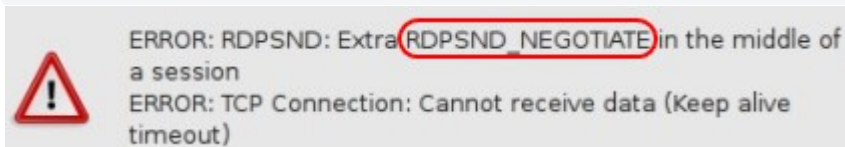

Problem

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**

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[6]

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.

---

6 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.

IGEL
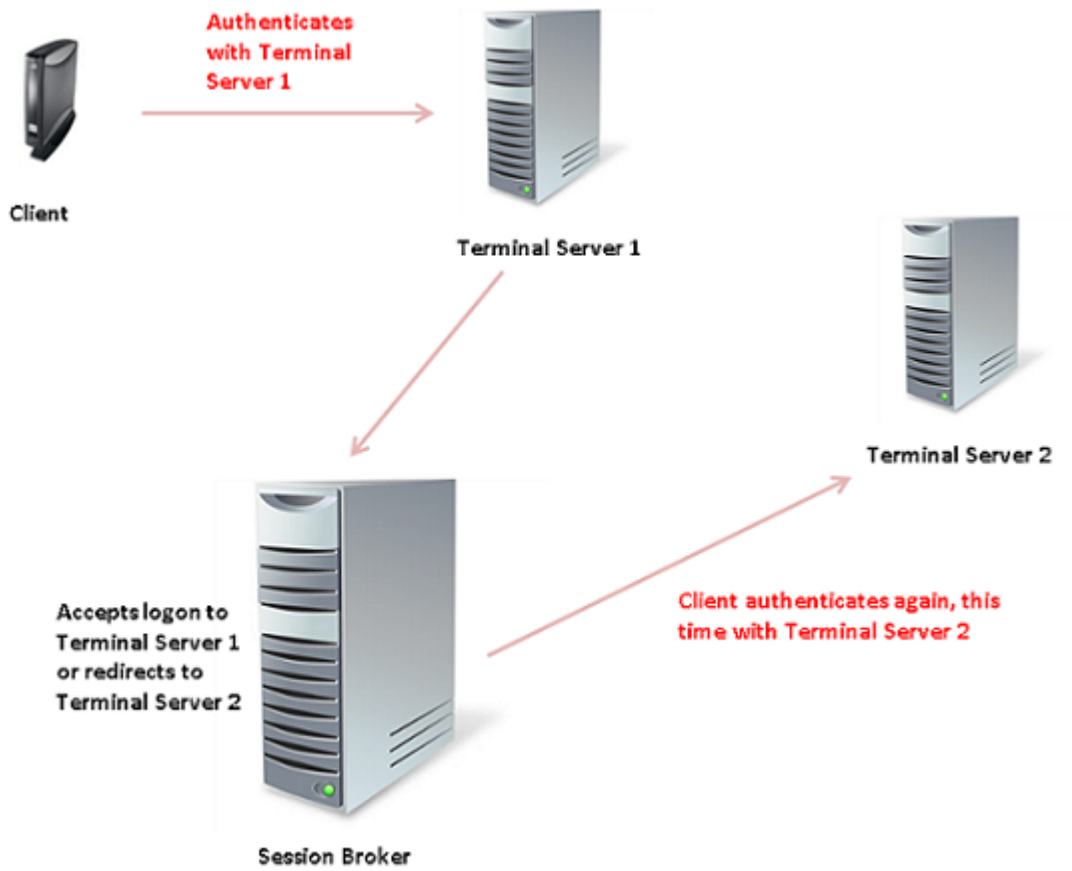
Solution

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

VMware Horizon

IGEL

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**.

IGEL

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**.

IGEL

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[7].

4. Assign the profile to your device and reboot.

---

7 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.[8]

You can also access IGEL's 3rd party hardware support database[9] to find fully supported graphic chips.

---

8 http://edocs.igel.com/index.htm#11873.htm
9 https://www.igel.com/linux-3rd-party-hardware-database/

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

-

IGEL

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 . 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
```

IGEL

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.**

   > (i) 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

IGEL

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:
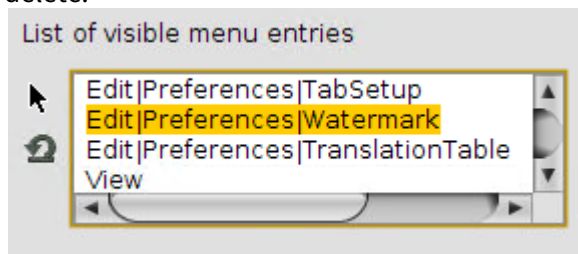
3. Press the backspace [←] or delete [Del] key.
   The menu item is deleted:
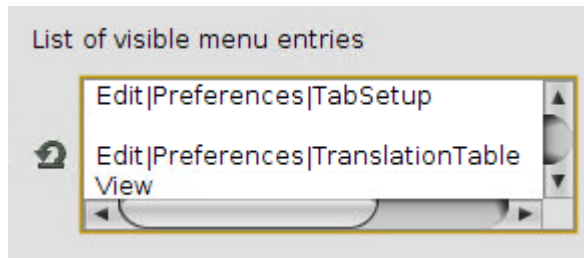
   ⓘ If you delete a menu item that has subitems, the subitems will be invisible, too.

4. To remove further menu items, repeat steps 2 and 3.
5. Click **Apply** or **Ok**.
6. Start or restart the IBM iAccess client to check your changes.

Restoring the Original Menu

1. In the IGEL Setup, go to **System > Registry > sessions > iaccess[NUMBER] > options > deletemenus** (Registry key: `sessions.iaccess[NUMBER].options.deletemenus`). [NUMBER] is the instance number of the session whose menu you want to restore; 0, for instance, stands for the first session, 1 for the the second session, etc.

2. In the **List of visible menu entries**, click the following symbol:
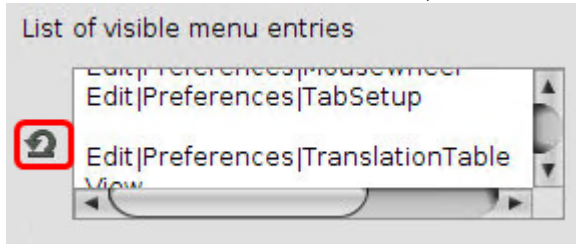
The original menu is restored.

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

IGEL

Key Mapping for IBM iAccess Client

Problem

When you change the key mapping in the IBM iAccess client, the changes are not retained when the client is restarted.

Applying the changes via IGEL Setup is not possible.

Environment/Prerequisites

- IGEL OS 10.05.100 or higher
- UMS 5.09.110 or higher
- IBM iAccess Client session is set up

Solution

Save the settings made in the IBM iAccess client in a file and distribute that file via the UMS.

Editing the Key Mappings

1. Open the IBM iAccess session and log on to your remote environment.
2. In the IBM iAccess client, go to **Edit > Preferences > Keyboard**.
3. On the **Key Assignment** tab, create the desired key bindings.
4. When you are finished creating key bindings, click **Save as...**.
5. In the save dialog, choose **File** and edit the file path as follows: `/userhome/IBM/ iAccessClient/Emulator/IBMi.kmp`
6. Click **OK**.

   The IBM iAccess client will recognize the file `IBMi.kmp` as the default key.

Importing the Configuration File to the UMS

1. Open the UMS.

2. In the navigation tree, find the thin client with the `IBMi.kmp` file and select **Other Thin Client commands > File TC->UMS** in the context menu.
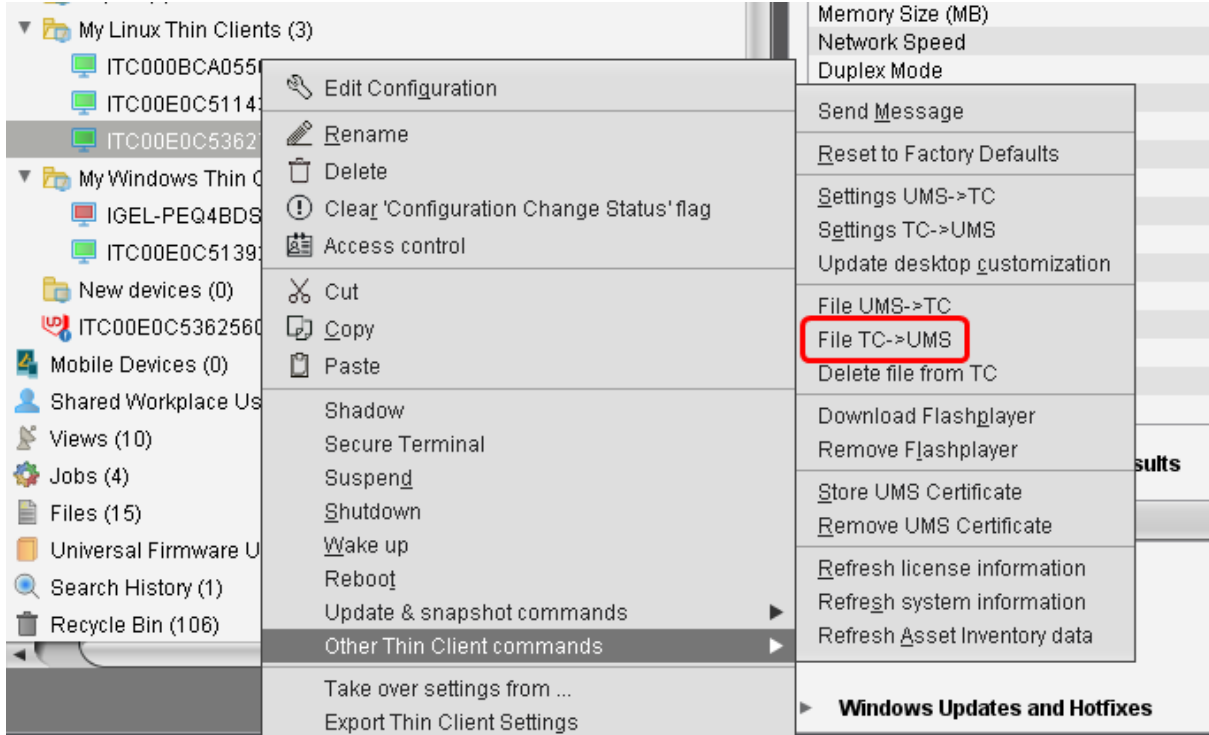
3. Under **Thin Client file location**, enter `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp`
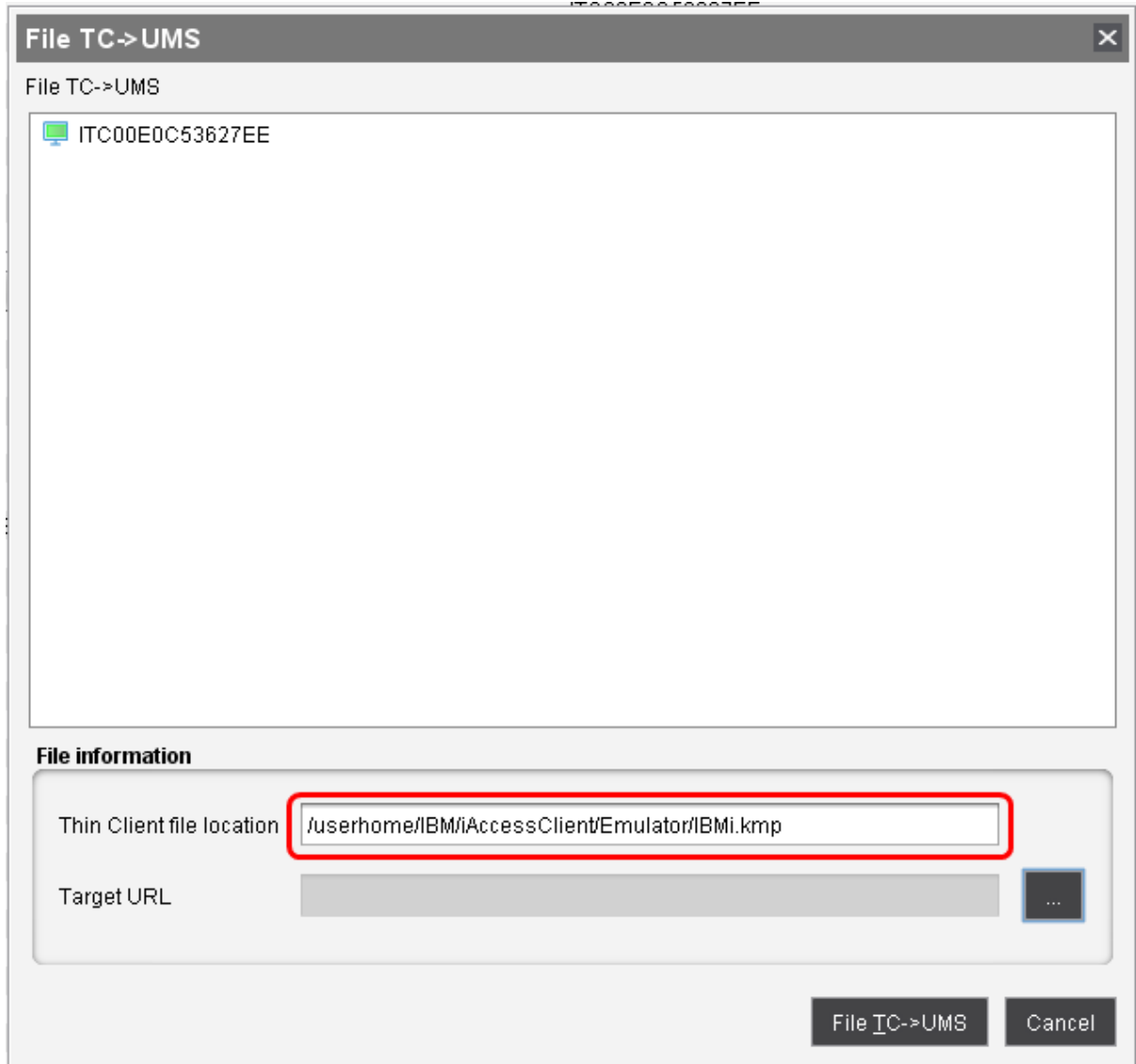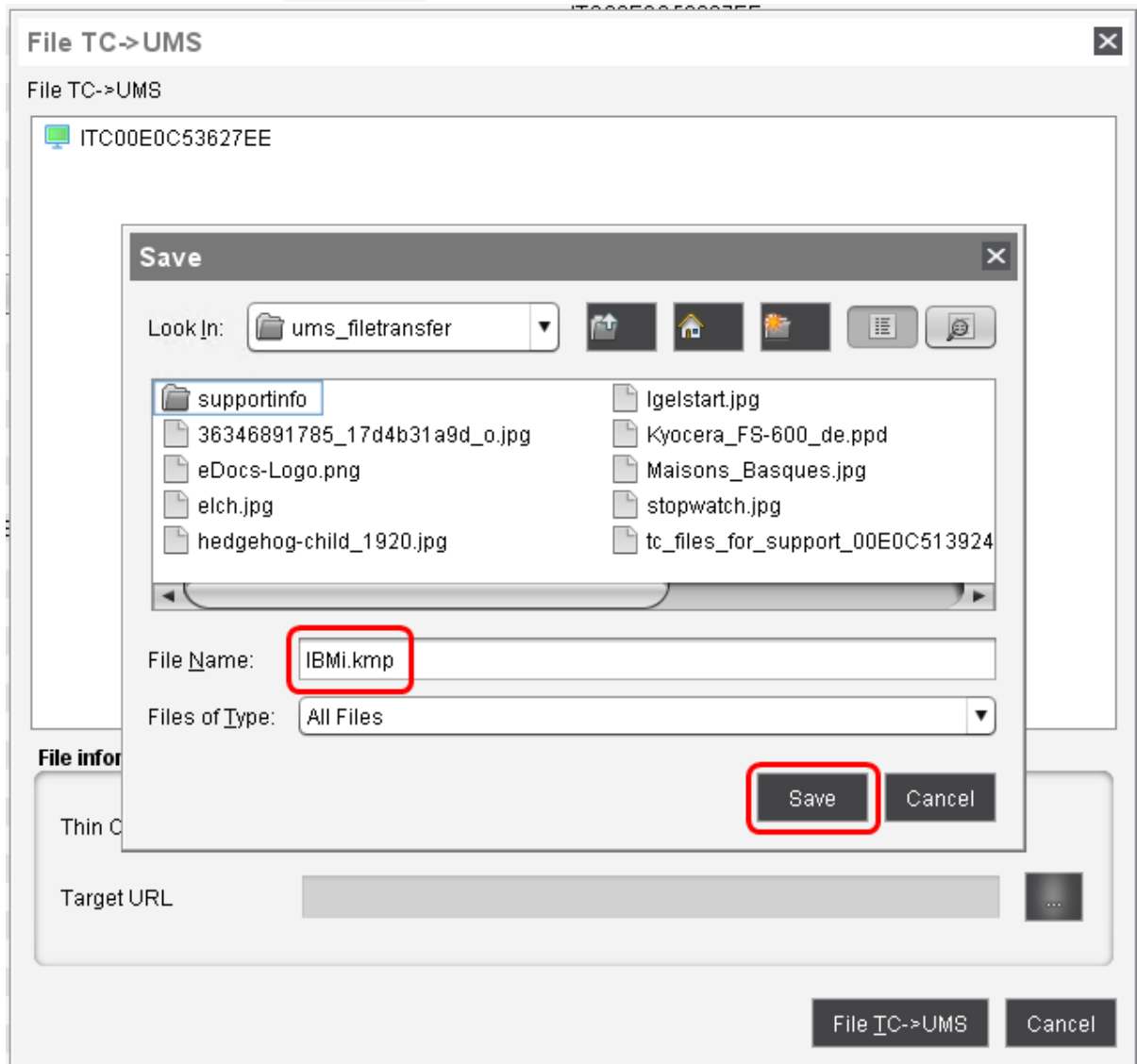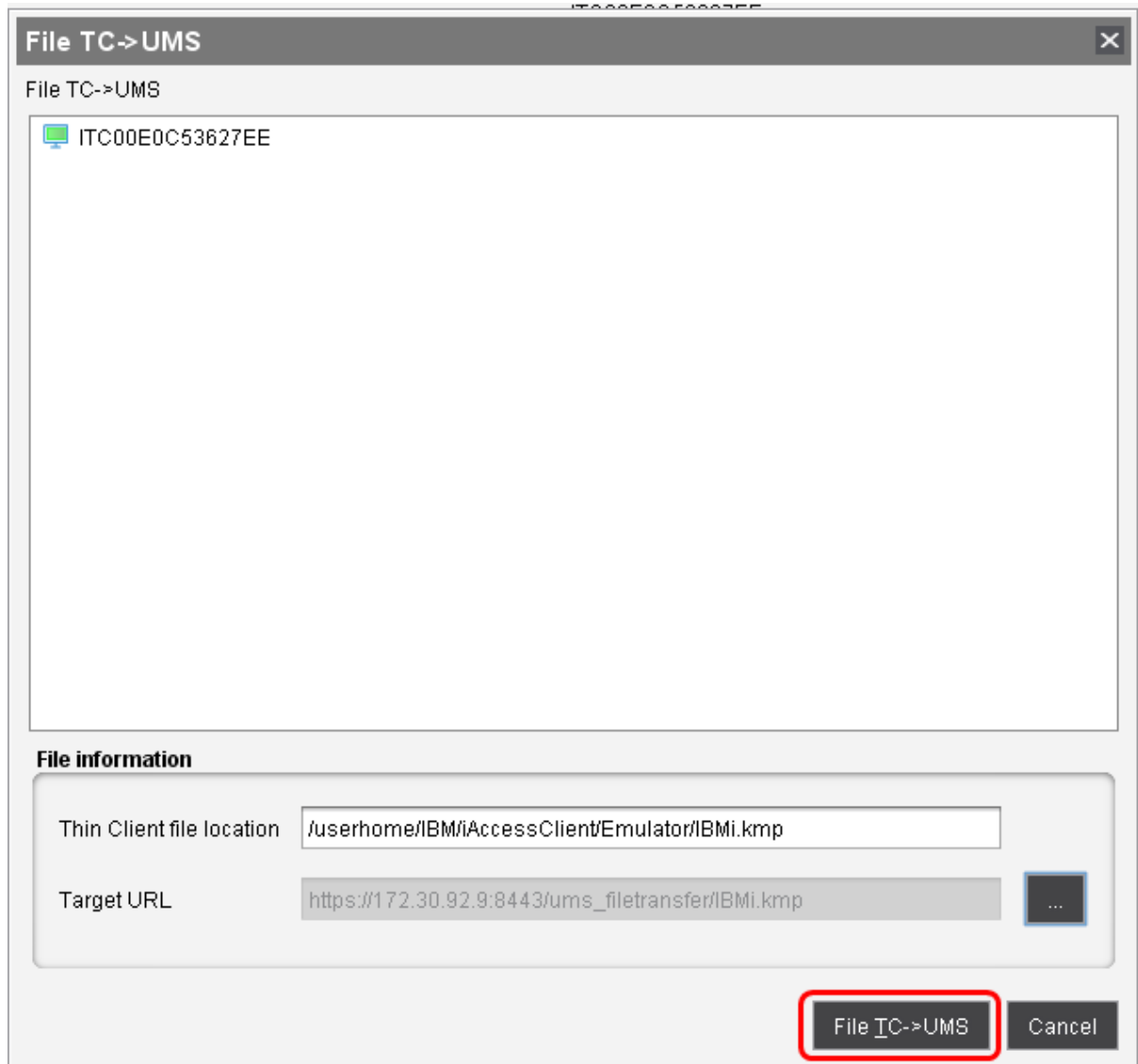
4. Click ⬚ to open the **Save** dialog.
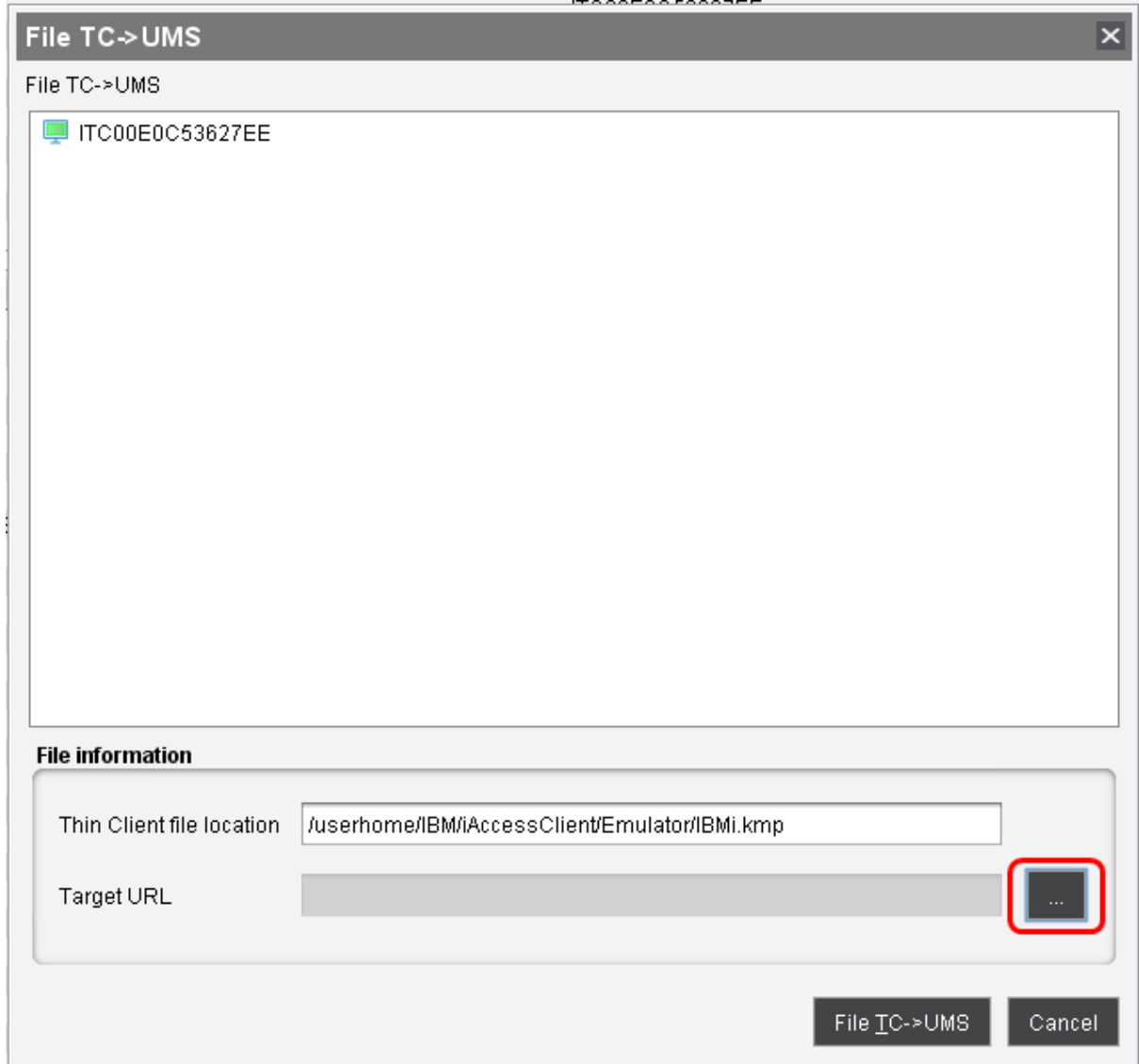
5. Choose a file location within the `ums_filetransfer` folder.
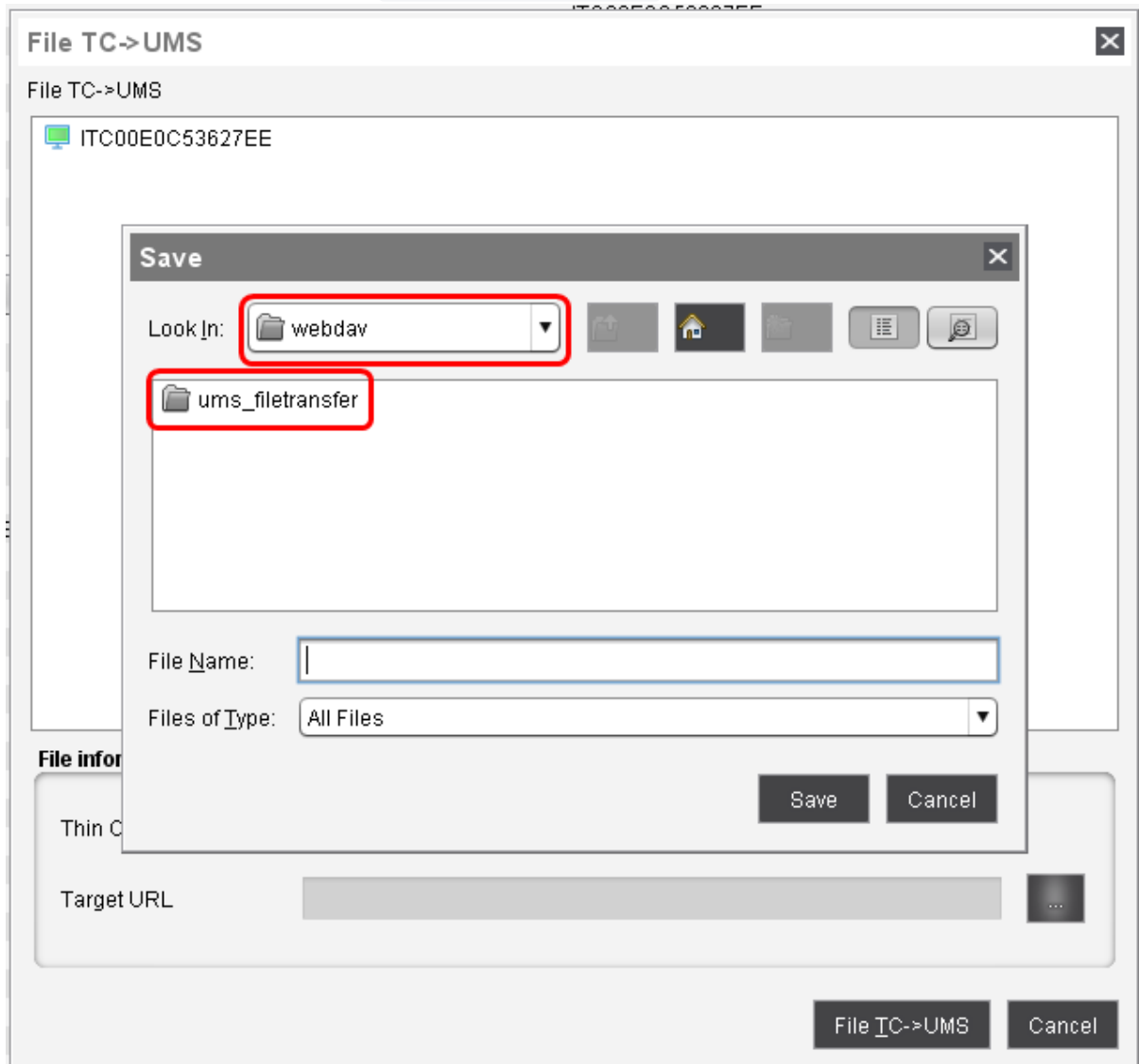
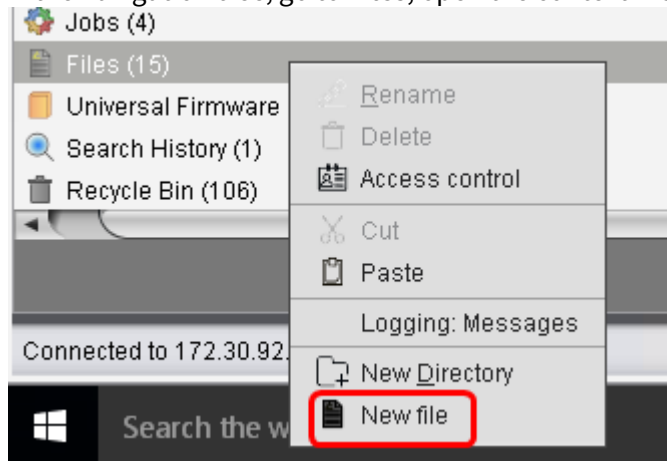6. Under **File Name**, enter `IBMi.kmp` and click **Save**.

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

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

Creating the File Object in the UMS

1. In the navigation tree, go to **Files**, open the context menu and choose **New file**.

2. In the **New file** dialog, choose **Select file from UMS server** and click [...] to open the file dialog.

3. In the file dialog, find the file `IBMi.kmp` you created previously, and click **Open**.
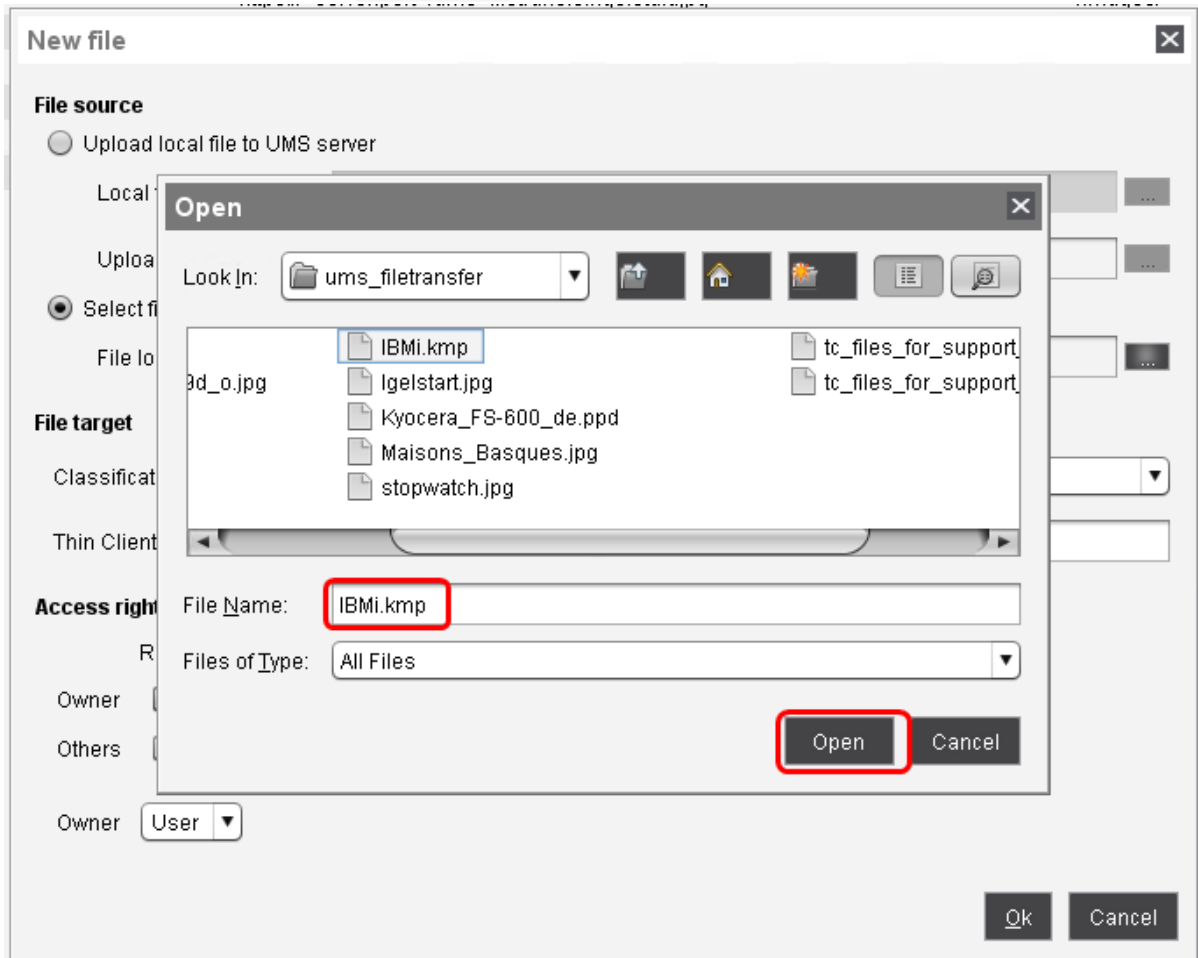
4. Back in the **New file** dialog, enter the **Thin Client file location** as follows: `/userhome/IBM/ iAccessClient/Emulator/`
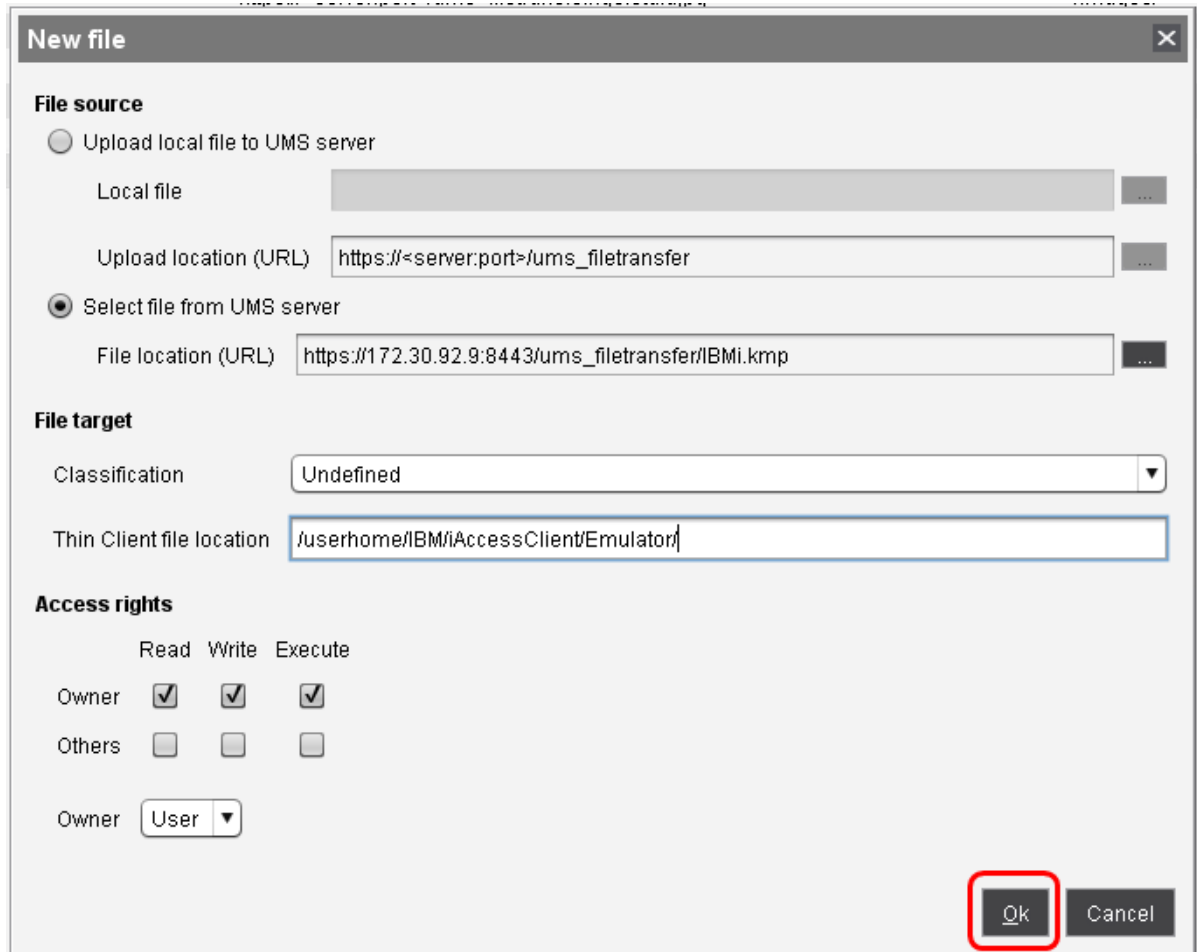
5. Ensure that the **Access rights** and **Owner** are set as follows:
   - **Owner** rights: **Read**, **Write**, **Execute**
   - **Owner**: "User"

6. Click **Ok**.

The file object "IBMi.kmp" is created.

Assigning the File Object to Thin Clients

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

2. In the **Select assignable objects** dialog, select the thin clients to which you want to assign the new key mapping and add them to the **Selected objects** area.
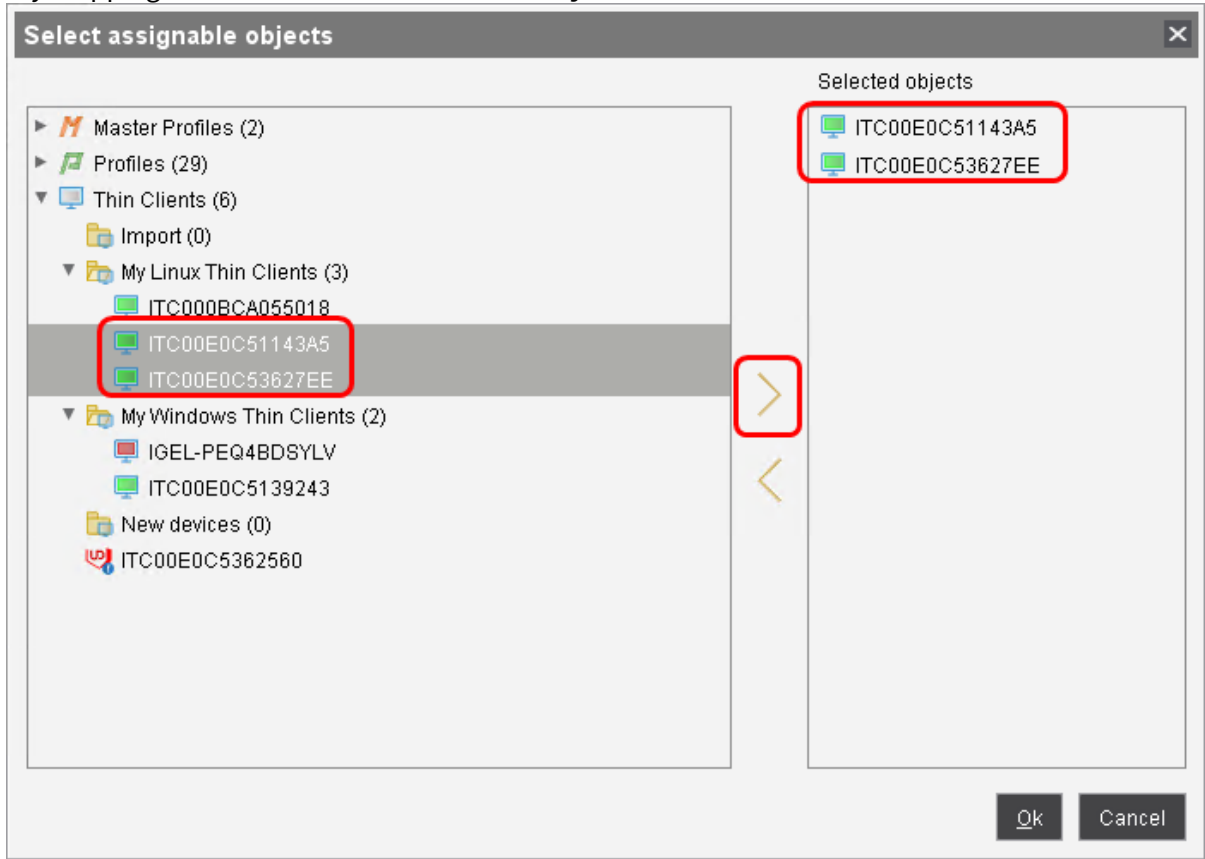
3. Click **Ok**.
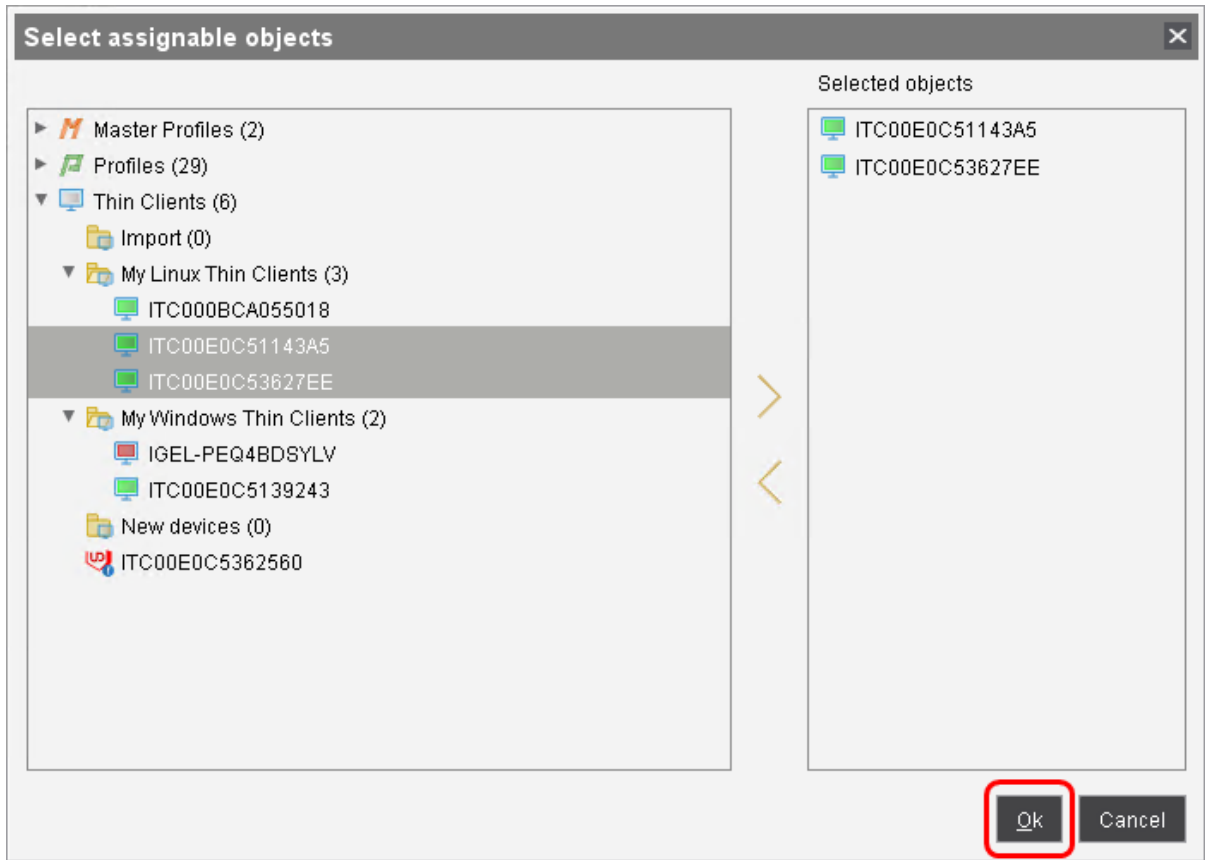
4. In the **Update time** dialog, choose whether the file should be assigned to the thin clients at next reboot or immediately; then, click **Ok**.

The file is transferred to the thin clients.

Imprivata

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.
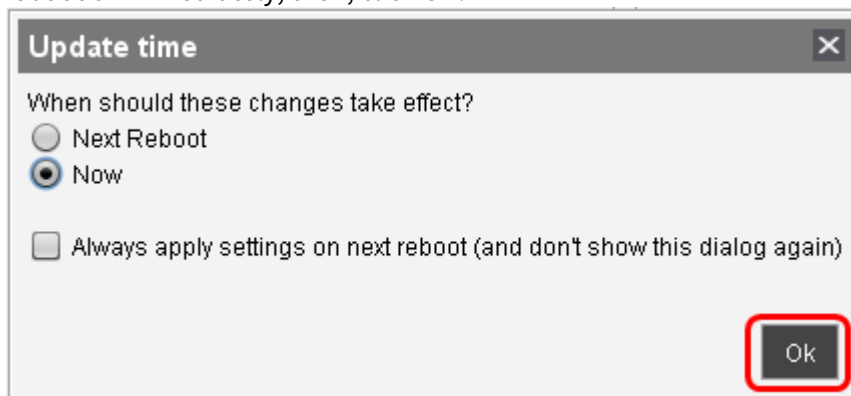
Solution

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

IGEL

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 and/or Enable Weaker Algorithms in the Built-in OpenSSH Server .

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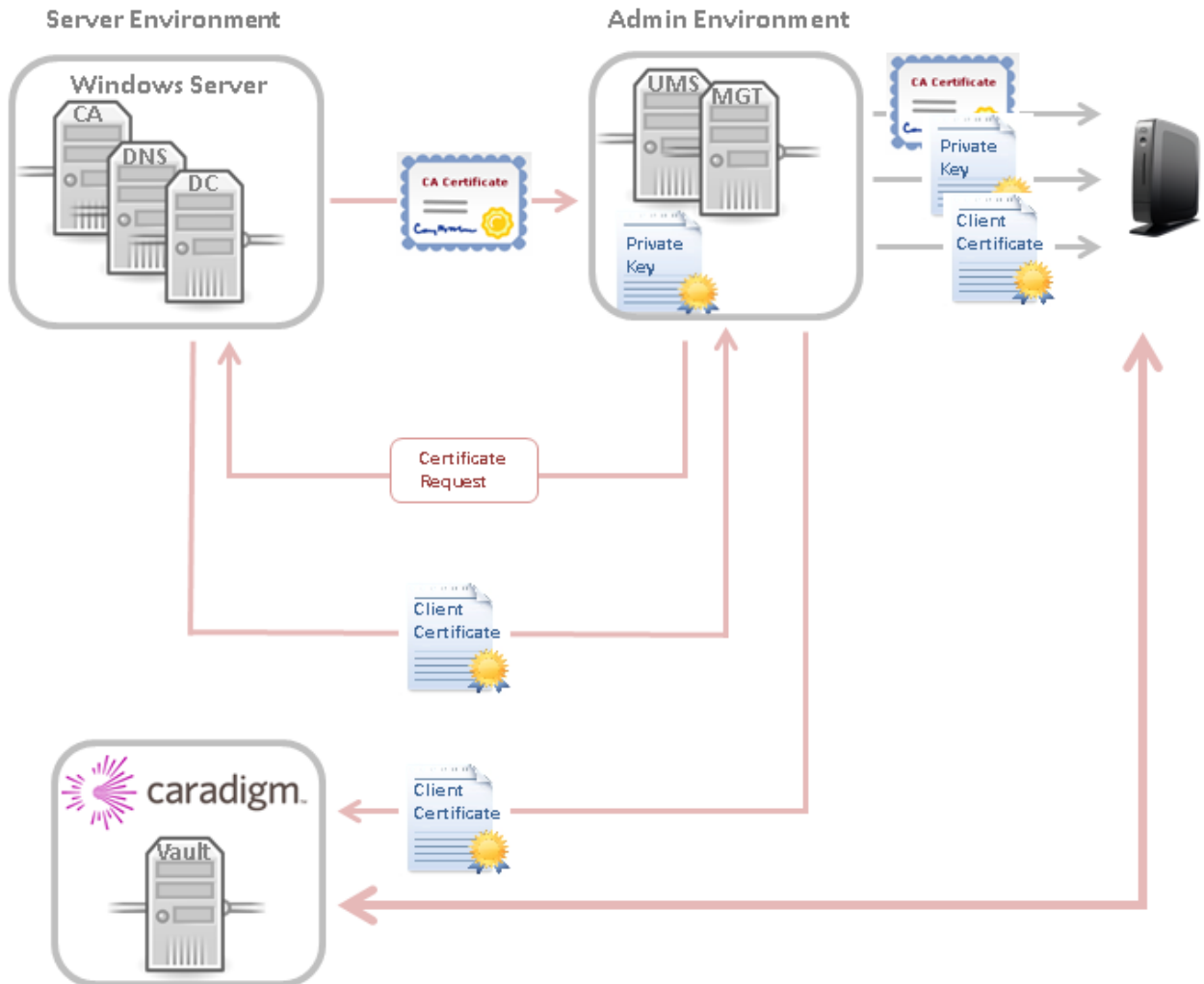
1. Go to the *Caradigm* authentication server (Vault).
2. Go to the **SSO & Context Management** tab.
3. Click **Tap Server**.
   The **Tap Server** screen opens.
4. Check the values for the **Way2Care Parameters**:
   - **Default Group Name**
   - **Default Grace Period**
5. Add the values for the **Badge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

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
- Requesting the Client Certificate
- Sending all Certificates to TC
- Transferring the public Certificate to the Caradigm Vault

IGEL

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

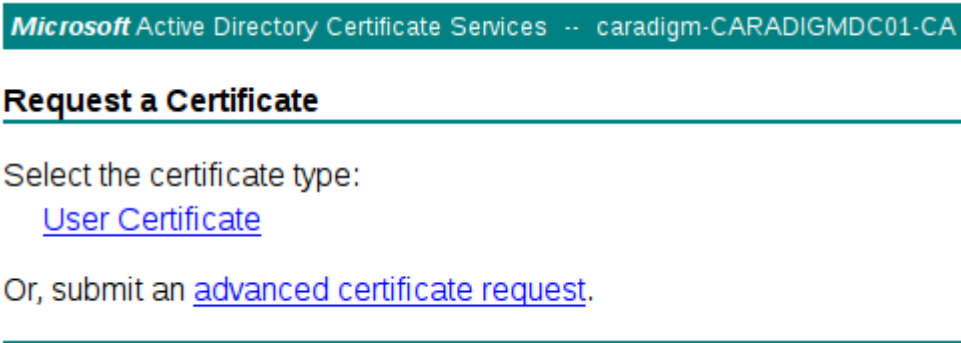- A challenge password []:
- An optional company name []:

> ℹ 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:

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:

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.

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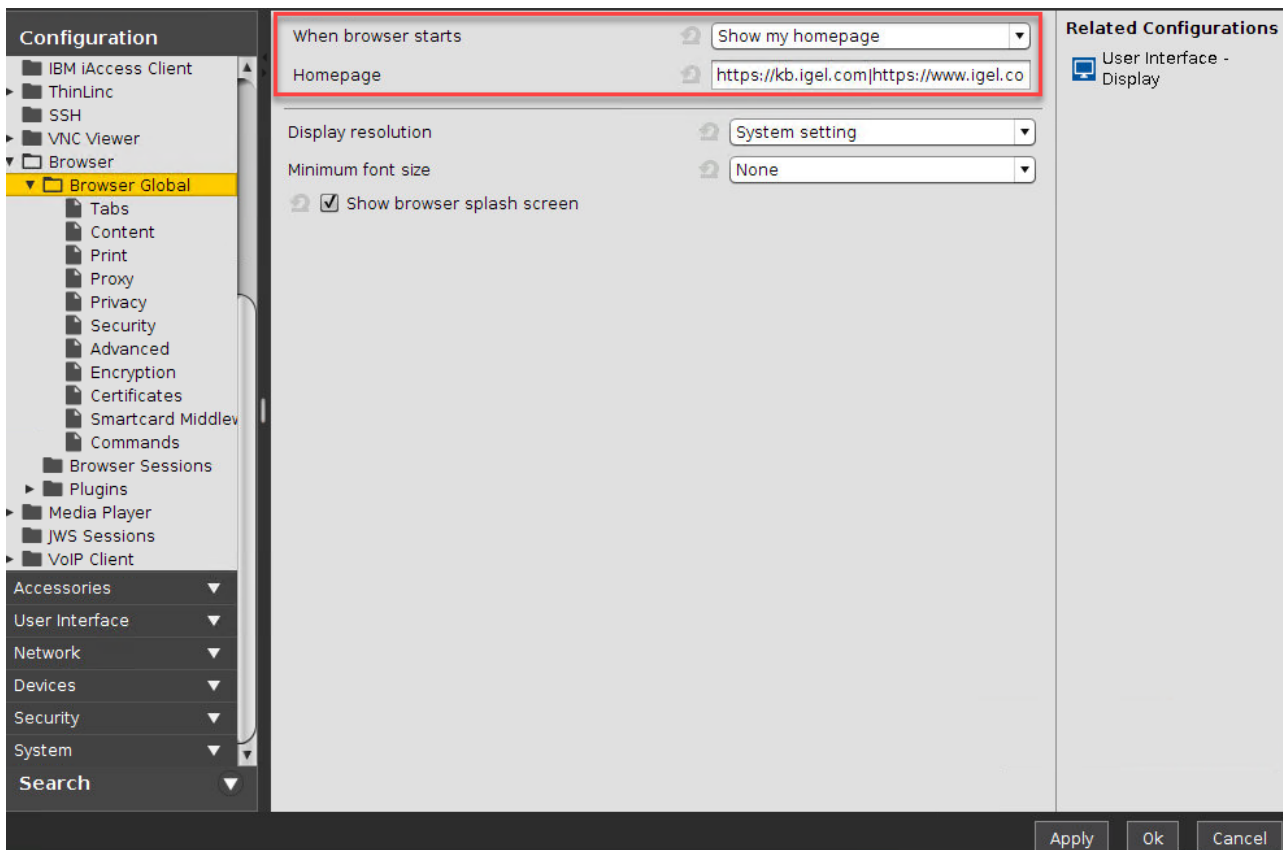
1. Open the setup and go to **Browser > Browser Global.**
2. Set **When Firefox starts** to **Show my home page**.
3. Set **Homepage** to the URLs that the browser should open at startup. Use "|" as a separator.
4. Click **Apply** or **Ok**.

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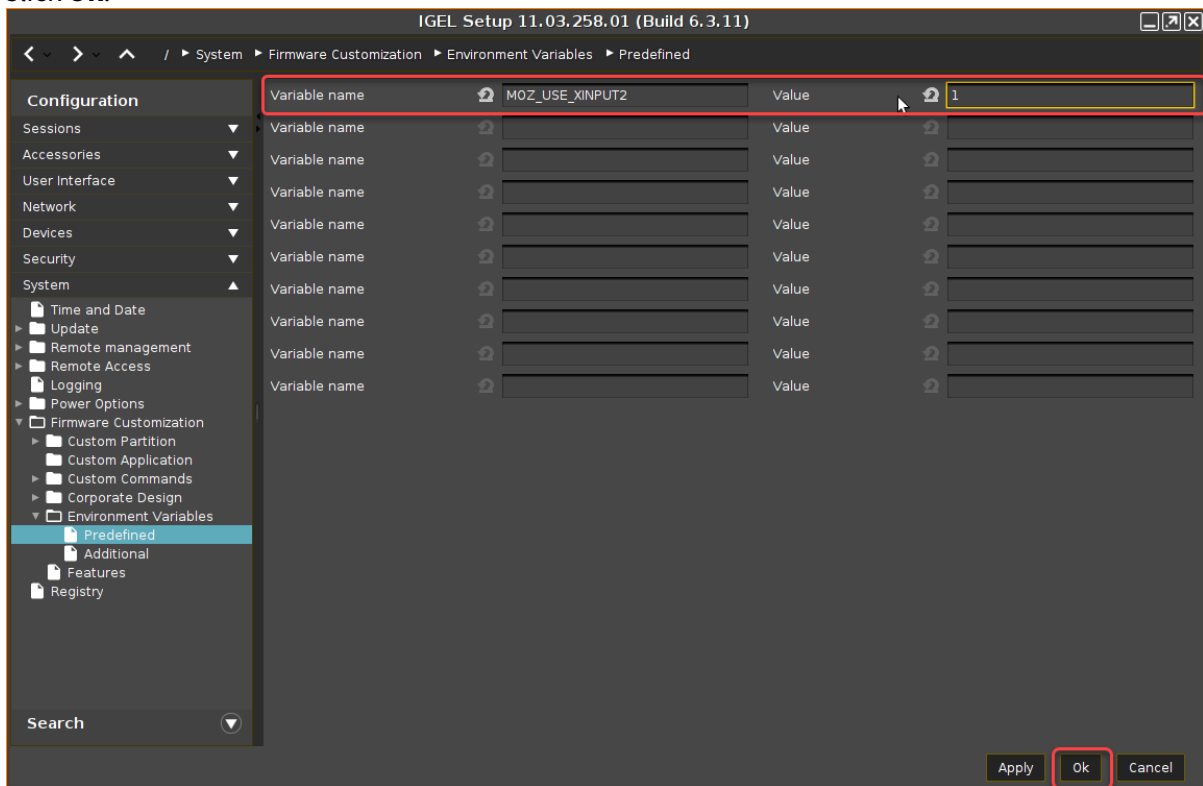
5. Reboot the device.
6. To check if multitouch is working, open the Firefox browser and go to https://www.paulirish.com/demo/multi.

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 S*etup.

You will find information regarding the configuration parameters for Firefox in the MozillaZine Knowledge Base under Firefox About:config entries[10].

1. In **Setup**, go to **Sessions > Browser > Browser Global > Advanced**.
2. In the **Custom preferences** area, click on **Add**.
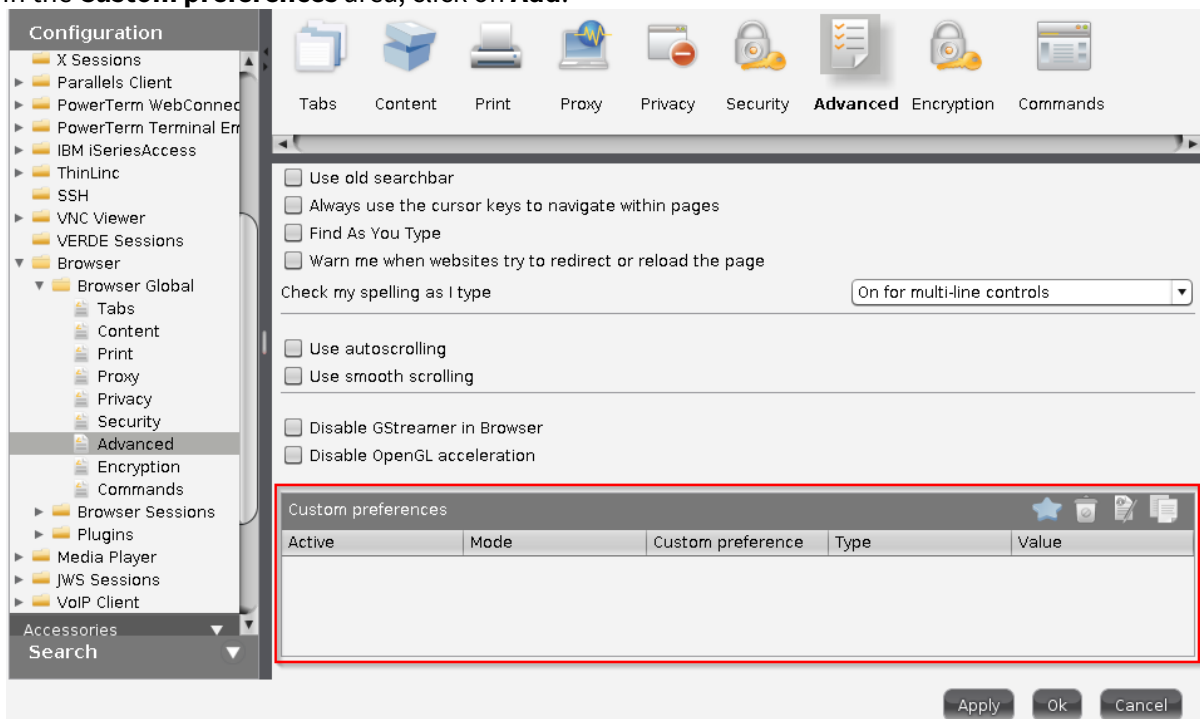
3. Using the **Active** option, specify whether the configuration parameter is to be active.
4. Specify the **Mode** of the configuration parameter - for many cases **pref** will do.
5. Under **Custom preference**, give the name of the configuration parameter. Example:

   `ui.textSelectBackground`

6. Specify the **Type** of the configuration parameter.
   Possible values:

---

10 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.
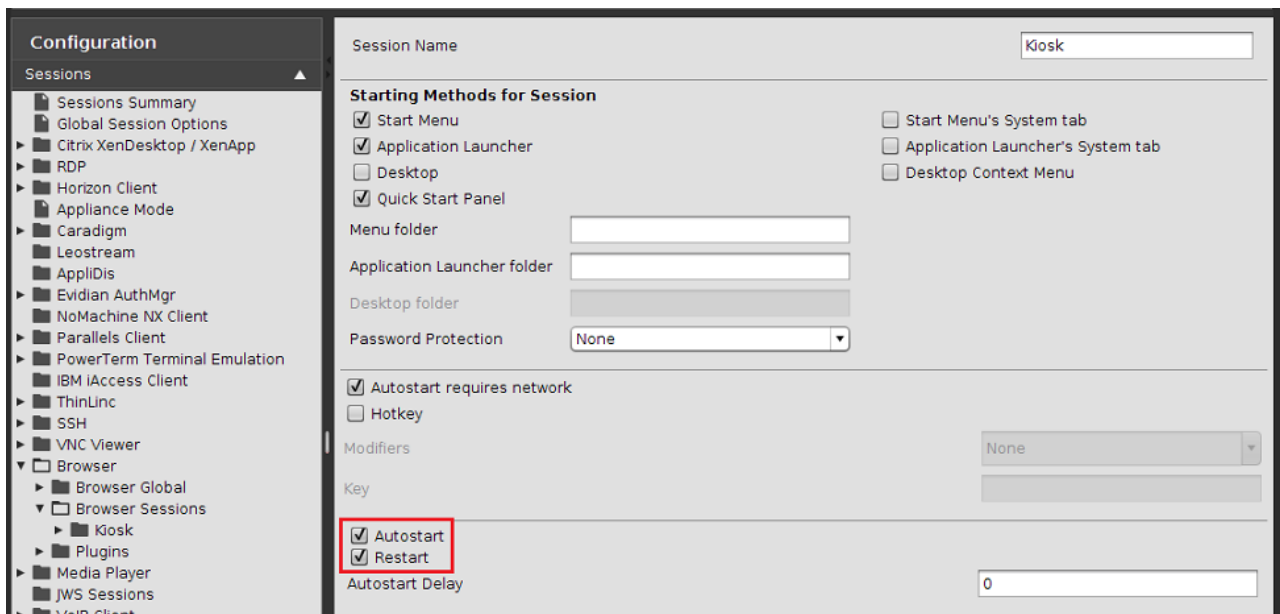
Use the Browser in Kiosk Mode

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]

▶ Activate **Autostart**.

▶ Activate **Restart**.

IGEL

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings
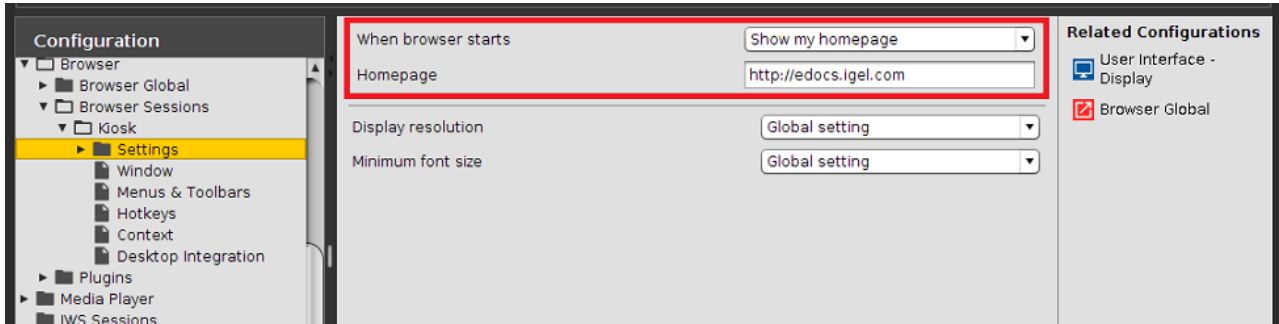
▶ Set **When browser starts** to **Show my home page**.

▶ Set **Home Page** to the desired home page.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Tabs
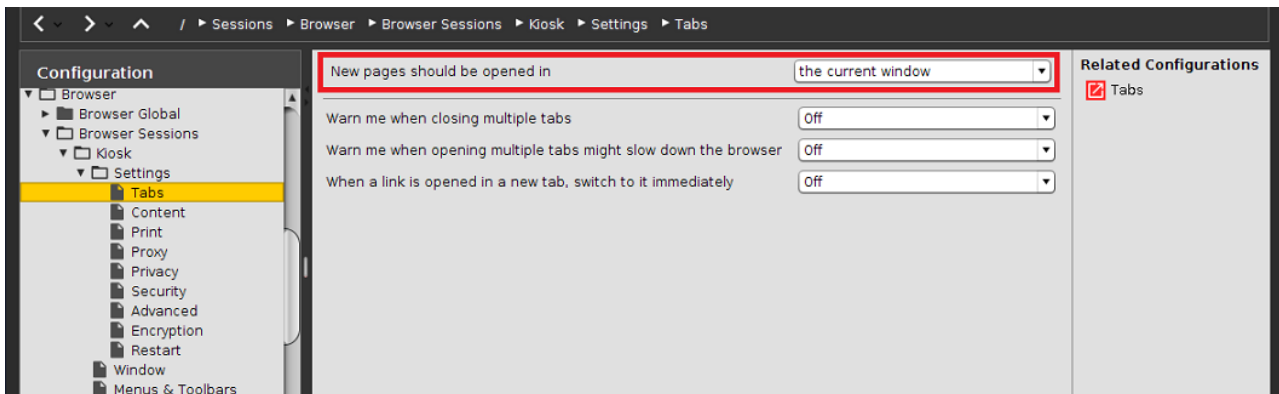
▶ Set **New pages should be opened in** to **the current window** or to **a new tab**.

Settings in Setup > Sessions > Browser Sessions > [Session Name] > Settings > Content
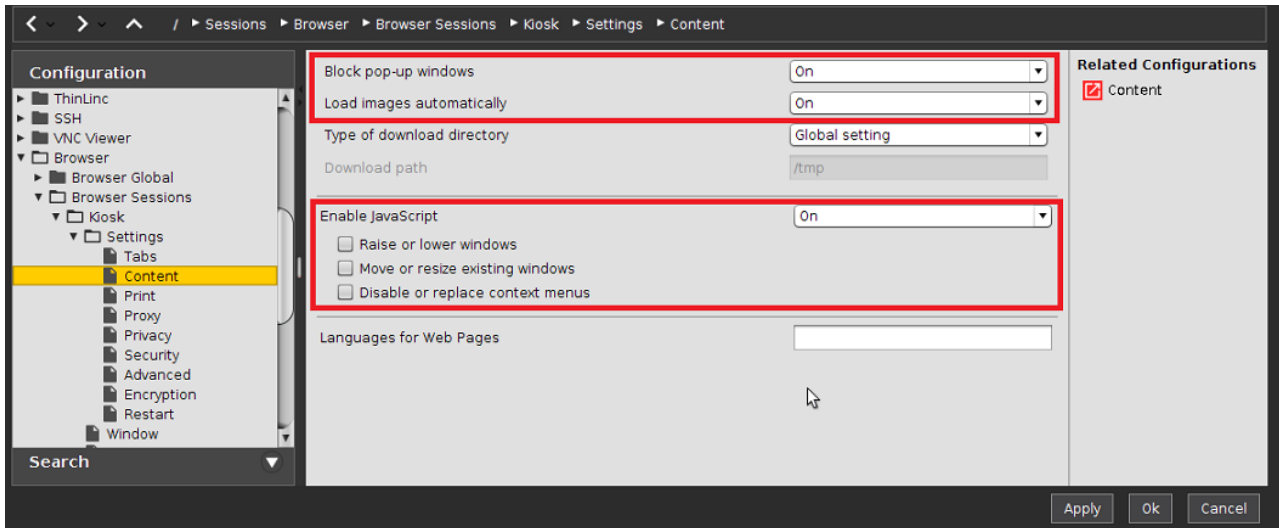
▶ If applicable, activate **Block pop-up windows**.

▶ 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
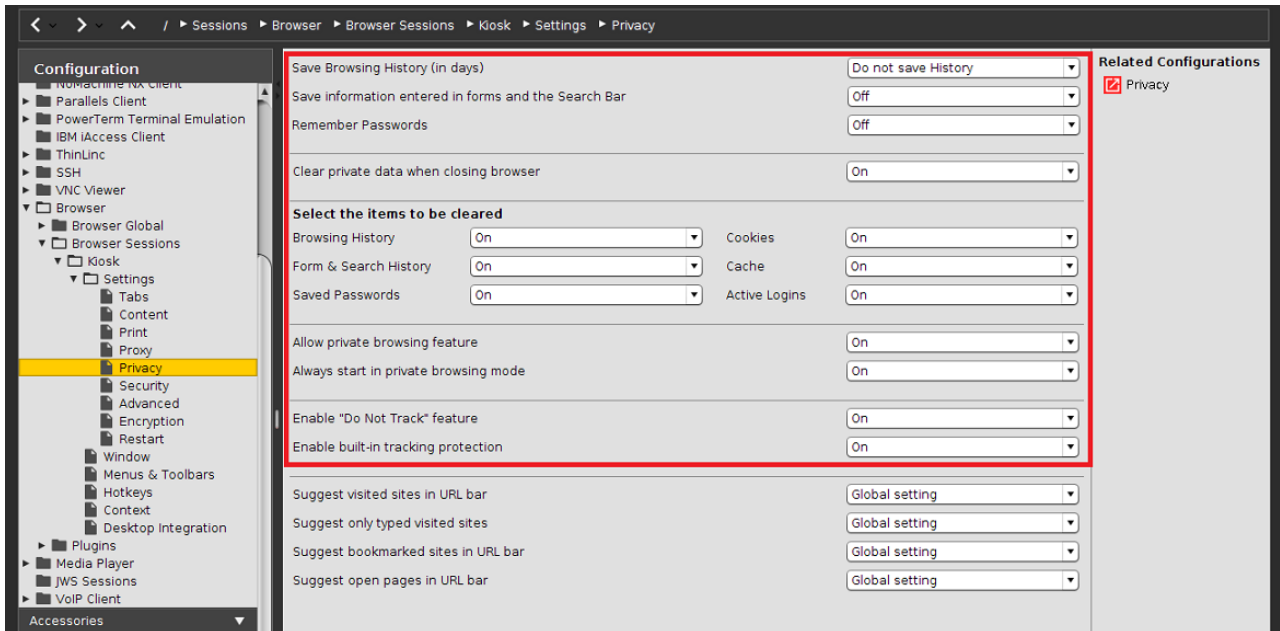
▶ Set **Save Browsing History (in days)** to **Do not save History**.

▶ 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
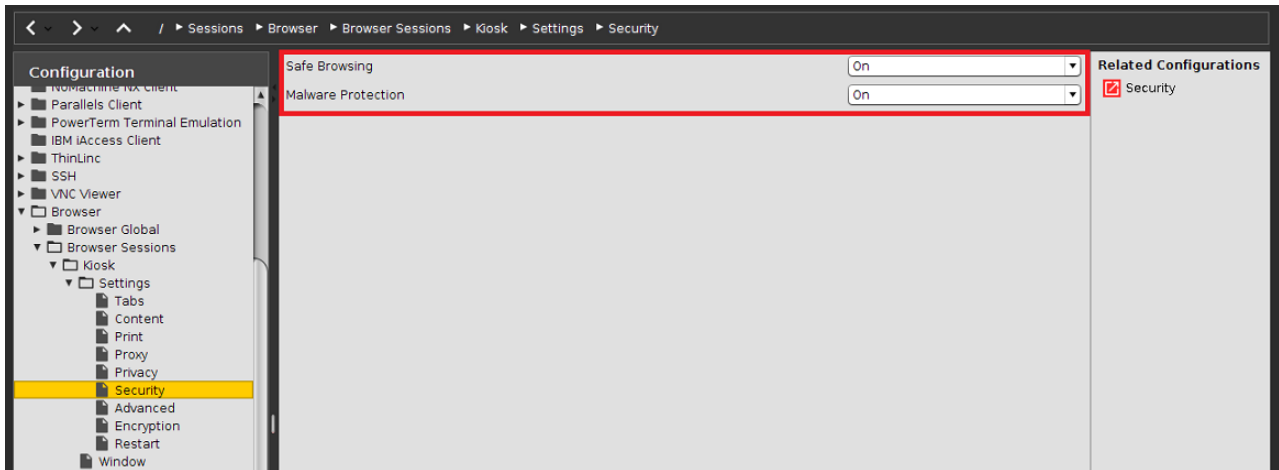
▶ To enable phishing protection, activate **Safe Browsing**.

▶ To enable protection against malicious downloads, activate **Malware Protection**.

Settings in Setup > Browser Sessions > [Session Name] > Settings > Restart
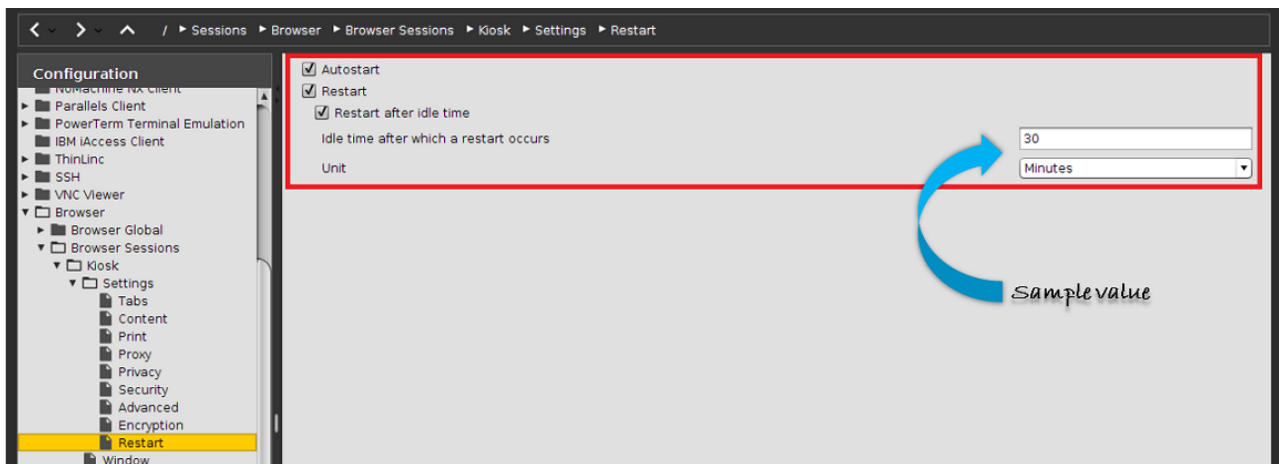
▶ Activate **Restart**. The browser will restart automatically if a user closes the browser window.

▶ 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
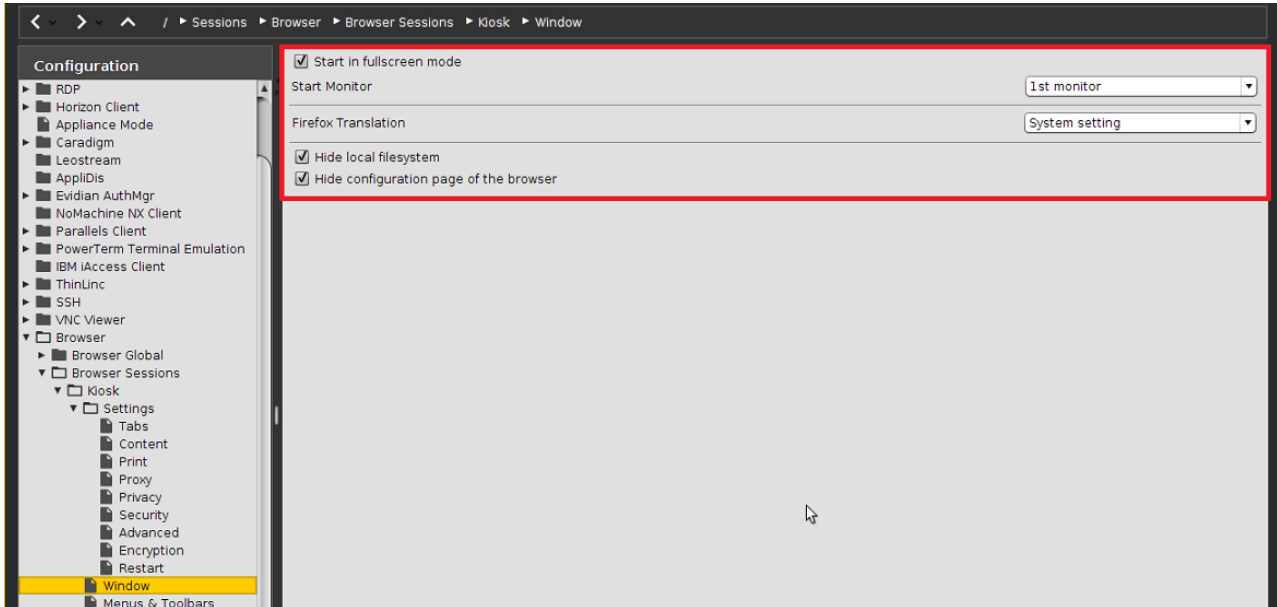
▶ If the browser shall run in fullscreen mode, activate **Start in Fullscreen Mode**.

▶ 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
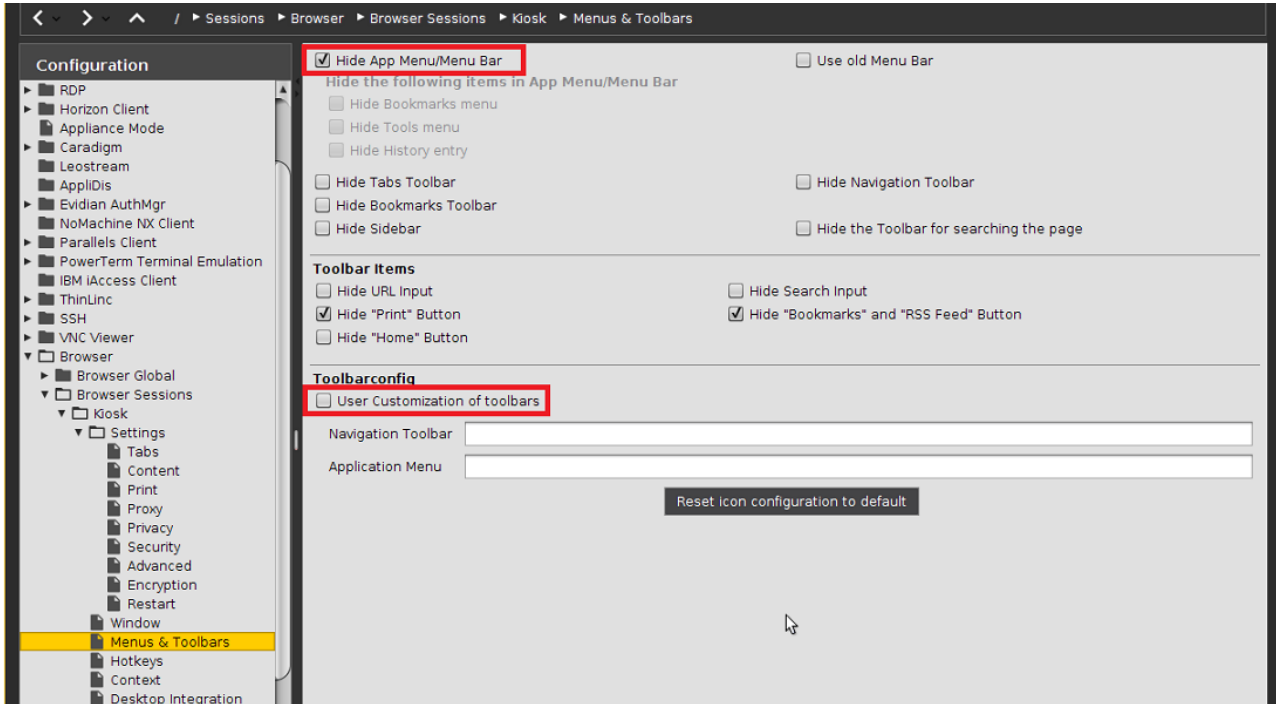
▶ Activate **Hide App Menu/Menu Bar**.

▶ 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 135).

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 135).

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`

IGEL

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.

Some PDFs are not opened by Firefox

Symptom

When opening some PDFs from the Internet, the Mozilla Firefox browser opens a new window or tab, but fails to display the PDF contents.

Problem

This can be due to a malfunction of the mozplugger Firefox component.

Solution

Disable mozplugger. Firefox will download the PDF document and open it with a local application (*IGEL Linux* 5.07.100 or newer):

1. Go to **System > Registry** in *IGEL Setup*.
2. Use **Search Parameter ...** to find the parameter
   `browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so`.
3. Check **Completely disable mozplugger**.
4. Confirm the setting with **Apply** or **OK**.
5. Restart Firefox.
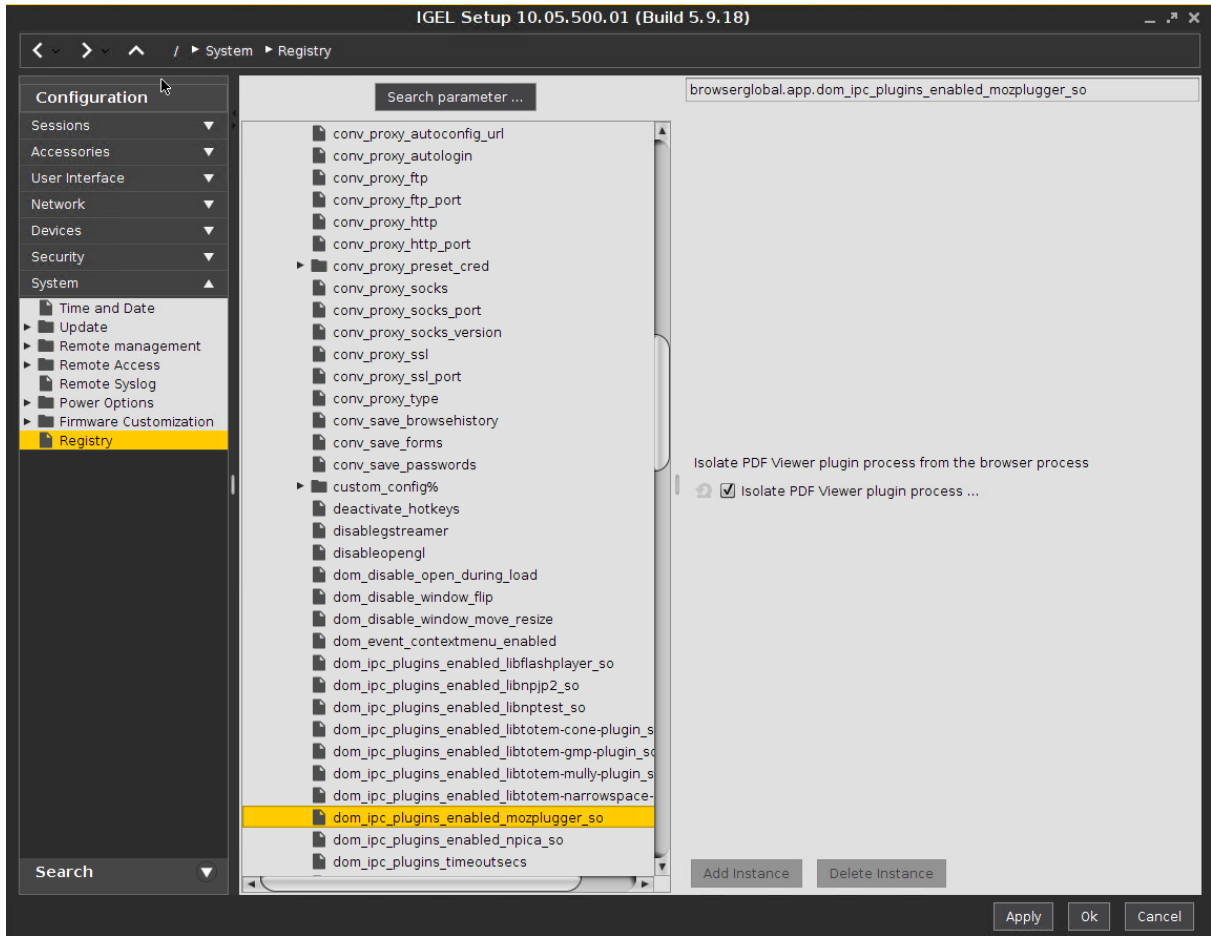
IGEL

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

IGEL

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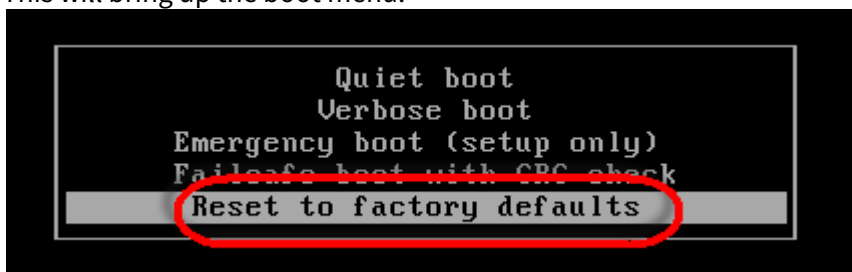
2. Choose **Reset to factory defaults** and press [Enter].
   The following will be displayed:

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[11] 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.

---

11 mailto:license@igel.com

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

IGEL

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[12]. 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.

---

12 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*.
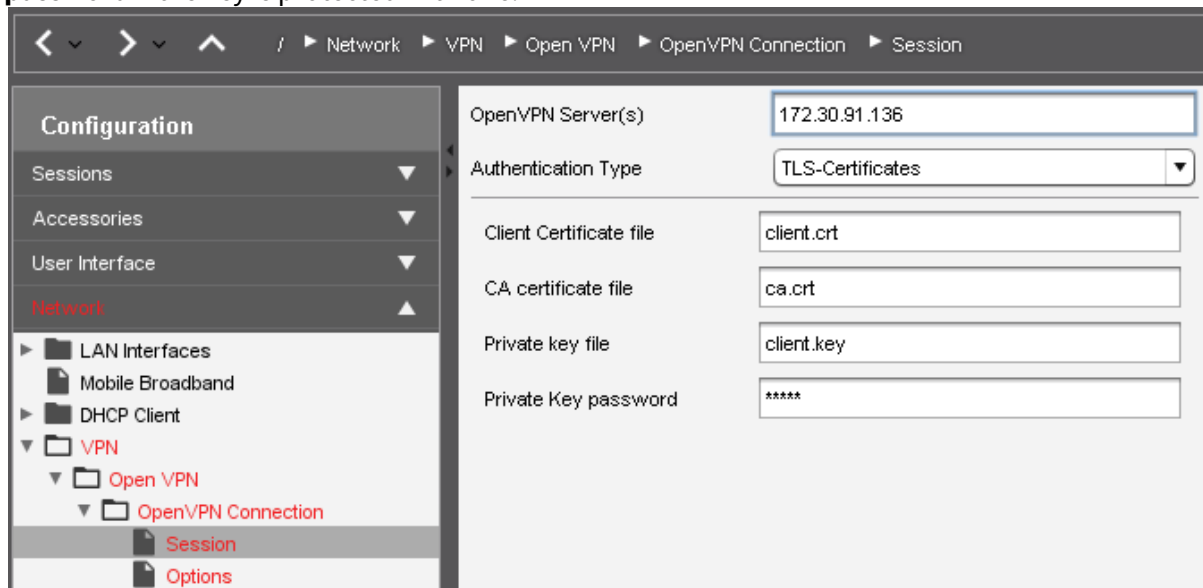
Prerequisites

- 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 168)".

Authenticating with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **TLS-Certificates** as the **Authentication Type.**
4. Select the client certificate as the **Client Certificate file**.
5. Select the root certficate of the CA as the **Certificate Authority (CA) file** .
6. Select the client's private key as the **Private Key file**. Enter the passphrase in **Private Key password** if the key is protected with one.
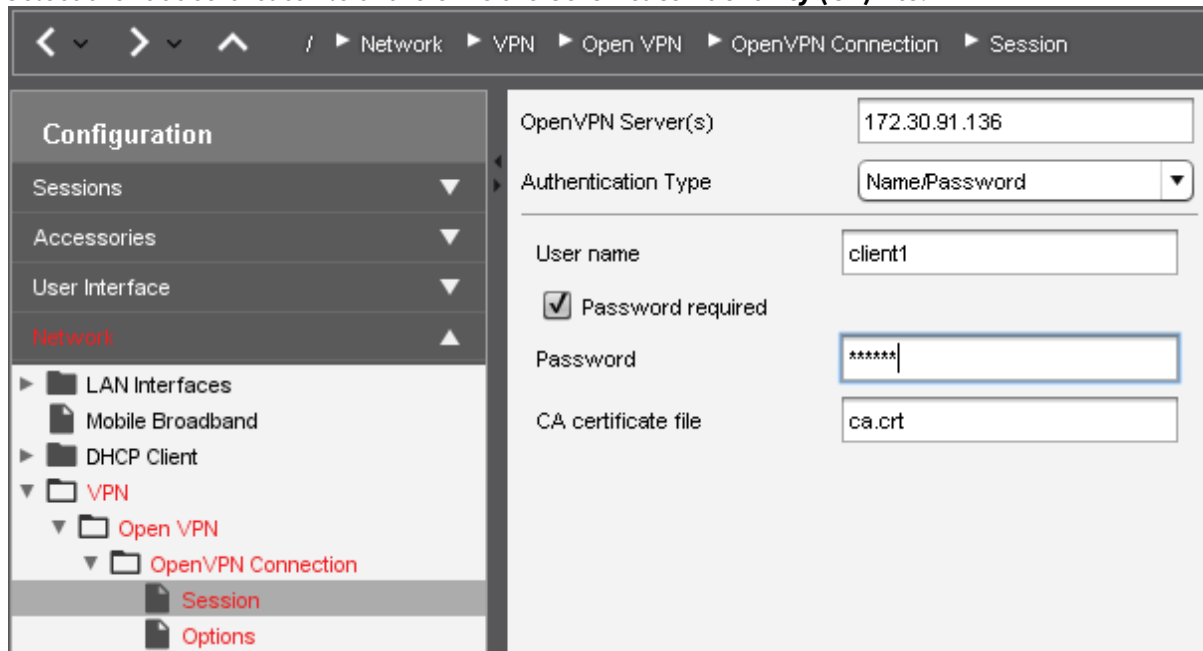
7. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

> ⓘ If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

Authenticating with Name/Password

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password** as the **Authentication Type.**
4. Enter the **Username.** If you leave this field blank the user will be prompted for the Username when connecting.
5. Check **Password required.**
6. Enter the **Password.** If you leave this field blank the user will be prompted for the password when connecting.
7. Select the root certficate file of the CAAs the **Certificate Authority (CA) file**.

8. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

Authenticating with Name/Password with TLS Certificates

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Name/Password with TLS-Certificates** as the **Authentication Type**.
4. Enter the **Username.** If you leave this field blank the user will be prompted for the username when connecting.
5. Check **Password required.**
6. Enter the **Password.** If you leave this field blank the user will be prompted for the password when connecting.
7. Select the client certificate as the **Client Certificate file**.
8. Select the root certficate of the CA as the **Certificate Authority (CA) file**.
9. Select the client's private key as the **Private Keyfile**. Enter the passphrase in **Private Key password** if the key is protected with one.

10. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

> ⓘ If a PKCS12 file is available, which includes the client certificate, the certificate authority and the private key, then you just need to enter the PKCS12 file name in the three corresponding fields. The advantage is that you only have to roll out one single file instead of three different files.

Authenticating with Static Key

1. Go to **Network > VPN > OpenVPN** and create a new connection.
2. In the **Session** section for the new connection, enter the name or public IP address of the **OpenVPN Server**.
3. Select **Static Key** as the **Authentication Type**.
4. Select the static key file as the **Private Key**.
5. Select **None** as the **Key Direction**.
6. Enter the server's VPN IP address as **Remote IP Address**.
7. Enter your client's VPN IP address as **Local IP Address**.
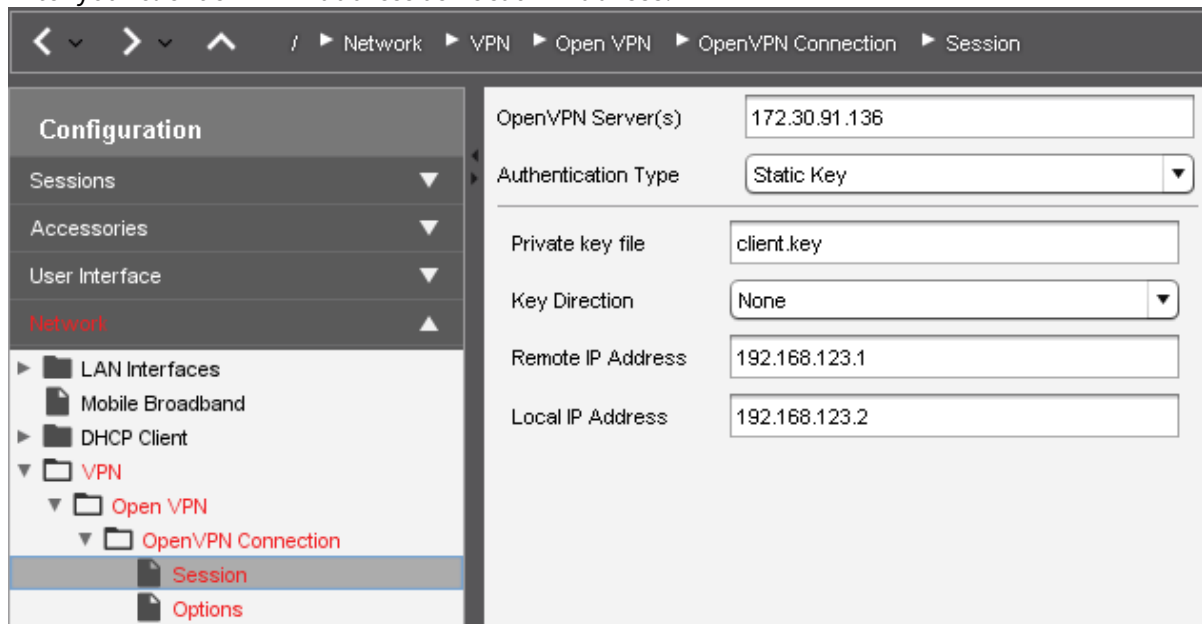
8. Click an icon for the newly created session (e.g. in the Start Menu) to initiate the connection.

Options and TLS Options

Options

Under **Network > VPN > OpenVPN > [Session Name] > Options**, you can set various options for the OpenVPN client. Usually, you can leave the default settings as they are. If the server uses compression, enable **Use LZO data compression**.

> ⓘ 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 157) 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.

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[13] and
- the OpenVPN manual page[14]

maintained by the *OpenVPN* project.

---

13 https://openvpn.net/index.php/open-source/documentation/howto.html
14 https://openvpn.net/community-resources/reference-manual-for-openvpn-2-0/
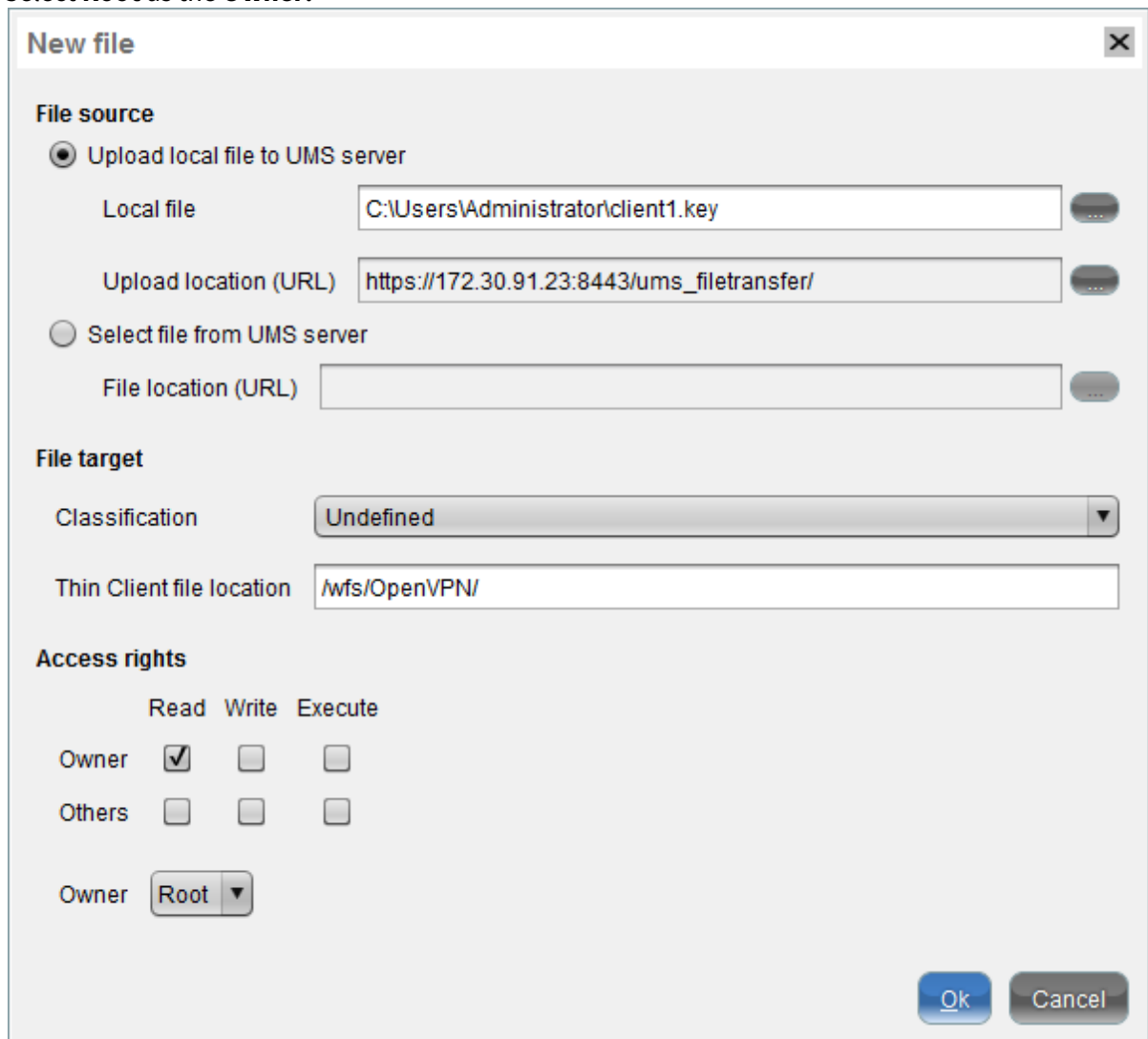
Securely Distributing Keys and Certificates for OpenVPN

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.**

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.

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.
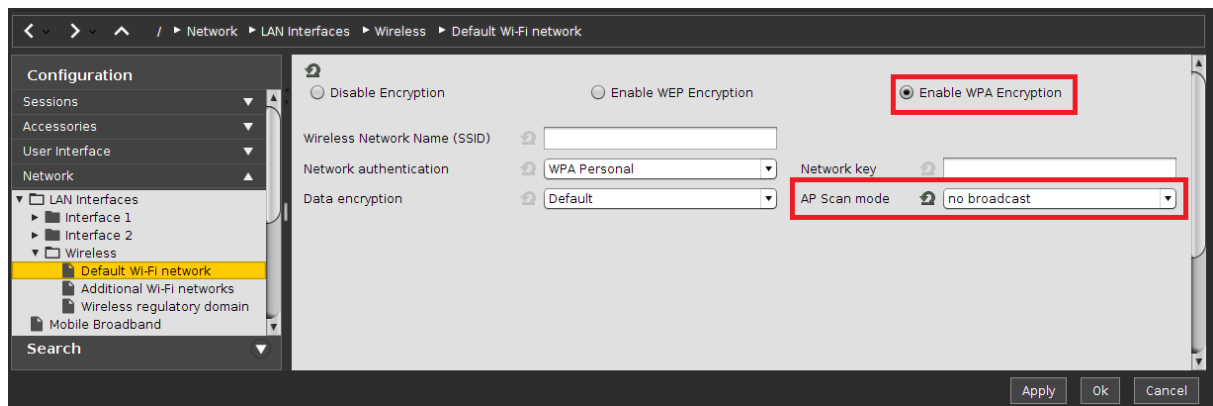
Improving WiFi Connectivity

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 171).

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.

IGEL

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) .

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
- Configuring the Network Interface

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 280).
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 280).

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:**
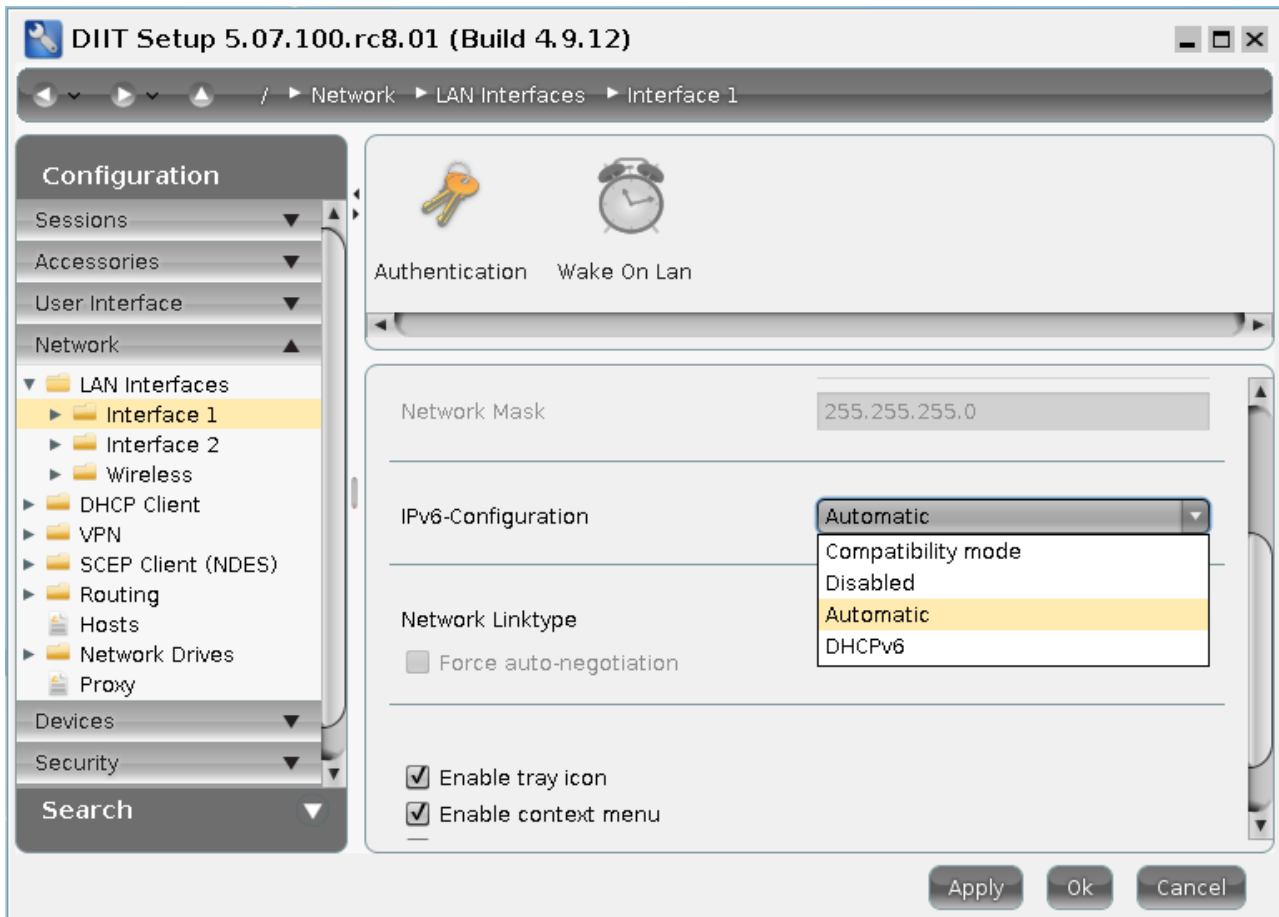
The following configurations are available:

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.

> (i) 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 506).

- Debuglog Partition (see page 188)
- Syslog (see page 190)
- Tcpdump (see page 191)
- Netlog (see page 194)

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 / <u>disabled</u>
Enables the debuglog partition.		

IGEL Setup > System > Registry		
> Size of debuglog partition in MiB	debug.tools.log_partition_size	50 ... 500 / <u>100</u>

⚠ 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/ <u>false</u>
IGEL Setup > System > Registry		
> Number of Rotate Files	debug.tools.syslog0.num_rotate_files	<u>2</u> ... 9
Number of files to be kept while rotating.		
IGEL Setup > System > Registry		
> Logfile rotate size in MiB	debug.tools.syslog0.rotate_size	<u>2,</u> 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 194) 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[15].

IGEL Setup > Registry		
> Resolve addresses/ports to names	`debug.tools.tcpdump[0-3].address_resolution`	enabled / <u>disabled</u>
IGEL Setup > Registry		
> Compression Method	`debug.tools.tcpdump[0-3].compression`	<u>lzop</u>, 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 / <u>eth0</u>
IGEL Setup > Registry		
> Number of Rotate Files	`debug.tools.tcpdump[0-3].num_rotate_files`	<u>3</u> … 10
Number of files to be kept while rotating.		
IGEL Setup > Registry		

---

15 http://www.tcpdump.org

> Only Log Package Headers	`debug.tools.tcpdump[0-3].only_headers`	enabled / <u>disabled</u>
IGEL Setup > Registry		
> **Enable promisc tcpdump logging**	`debug.tools.tcpdump[0-3].promisc`	enabled / <u>disabled</u>
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`	<u>10</u>, 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`	<u>0</u> / 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 / <u>disabled</u>
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)[16] manpage.

---

[16] 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 / <u>disabled</u>
IGEL Setup > Registry		
> period between netlog logs in s	debug.tools.netlog.period	<u>1</u>, 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 / <u>false</u>
	By default Ethtool logging is included in Netlog logging. However, you can disable it here.		
	IGEL Setup > Registry		
	> Log only if ethtool output changes	debug.tools.netlog.ethtool.log_on_changes _only	<u>true</u> / false
	Log only if ethtool output changes (on bootup there will always be at least one log entry)		
	IGEL Setup > Registry		
	> Number of Rotate Files	debug.tools.netlog.ethtool.num_rotate_files	<u>2</u> ... 4
	Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines)		
	IGEL Setup > Registry		
	> Logfile rotate size in MiB	debug.tools.netlog.ethtool.rotate_size	<u>2</u>, 4, 6
	Rotate when the size of the uncompressed file reaches this size in MiB.		

Ifconfig

Ifconfig

Apart from configuring network devices, ifconfig also gives diagnostic information such as RX bytes, TX bytes and dropped packets.

IGEL Setup >		
> Disable ifconfig logging	debug.tools.netlog.ifconfig.disabled	true / <u>false</u>
By default Ifconfig logging is included in Netlog logging. However, you can disable it here.		

IGEL Setup >		
> Log only if ifconfig output changes	debug.tools.netlog.ifconfig.log_on_changes_only	no,<u>error_counter</u>,all
no: log on every netlog run **error_counter**: log only if an error counter or the address changes **all**: log on every change of ifconfig output		
IGEL Setup >		
> Number of Rotate files	debug.tools.netlog.ifconfig.num_rotate_files	<u>2</u> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.ifconfig.rotate_size	<u>2</u>, 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup >		
> Trigger tcpdump log	debug.tools.netlog.ifconfig.trigger_tcpdump_save	true / <u>false</u>
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.		

Netstat

Netstat displays a variety of network statistics for the local machine.

> Disable netstat logging	debug.tools.netlog.netstat.disabled	true / <u>false</u>	
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	<u>2</u> ... 4	
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).			
>Logfile rotate size in MiB	debug.tools.netlog.netstat.rotate_size	<u>2</u>, 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	<u>net_error_changes</u>, 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 / <u>false</u>

IGEL Setup >		
> Log only if ping fails	debug.tools.netlog.ping_host[0-9].log_only_on_error	true / <u>false</u>
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	<u>2</u> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.ping_host0.rotate_size	<u>2</u> ... 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	<u>2</u> ... 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	<u>1</u>, 5, 10, 30, 60, 120
Time between pings in seconds.		

IGEL Setup >		
> Type of ping	debug.tools.netlog.ping_host0.type	<u>icmp</u>, http request, https request
	• **icmp**: use normal `ping` command • **http request**: send an http request (fails if no `HTTP/*.* * OK` answer is received) • **https request**: send an https request (fails if no `CONNECTED` is returned by openssl)	

Socket Status (ss)

Socket Status (ss)

IGEL Setup >		
> Disable socket status Logging	debug.tools.netlog.socket_status.disabled	true / <u>false</u>
By default socket_status logging is included in Netlog logging. However, you can disable it here.		
IGEL Setup >		
> Number of Rotate Files	debug.tools.netlog.socket_status.num_rotate _files	true / <u>false</u>
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
IGEL Setup >		
> Logfile rotate size in MiB	debug.tools.netlog.socket_status.rotate_size	true / <u>false</u>
Rotate when the size of the uncompressed file reaches this size in MiB.		
IGEL Setup >		
> Log only if triggered	debug.tools.netlog.socket_status.trigger_log	<u>ping_errors</u>, no_trigger
ping_errors: log only if ping test fails **no_trigger**: log on every netlog run		

IGEL

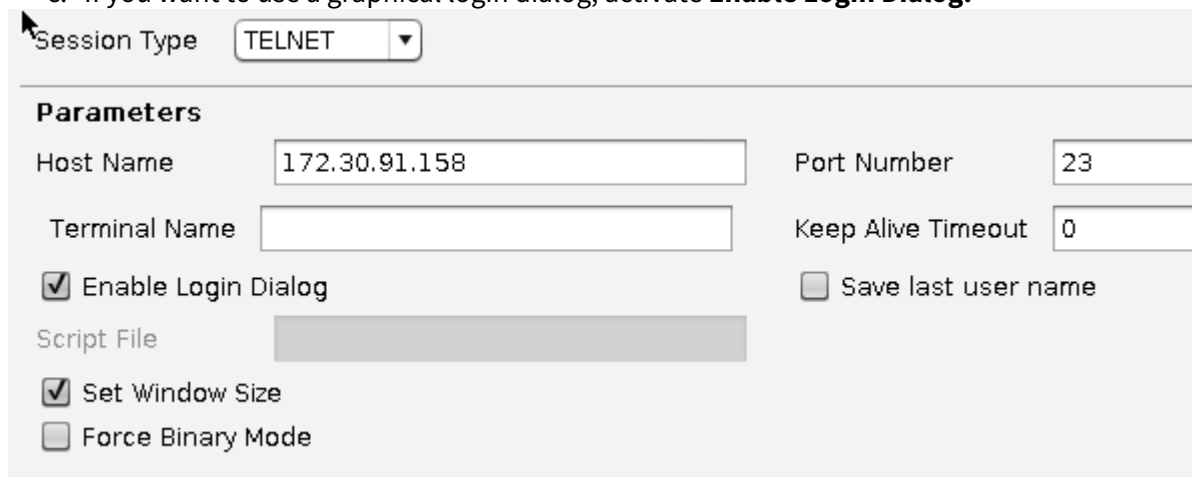# Making a Telnet Connection from IGEL Linux

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.**

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.

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
   - <u>2.0</u>
   - 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**.

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 209)
- Password-Protecting Sessions and Accessories (see page 210)
- Using Screenlock (see page 211)
- Do Not Save Session Passwords (see page 212)
- Setting a UEFI Password (see page 213)
- Using Two-Factor Authentication (2FA) (see page 214)

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 236).

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 209)) 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 214).

IGEL logo

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 313)
    - Citrix Legacy ICA Sessions (see page 317)
    - Citrix Legacy ICA Sessions with Local Logon Window (see page 318)
    - Citrix Storefront (see page 319)
    - Citrix Xen Desktop Appliance Mode (see page 324)
    - RDP Sessions (see page 321)
    - Horizon Sessions (see page 322)
    - Web browser (see page 323)
- (Kerberos) Passthrough Authentication (see page 522)

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[17].

> ⓘ 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.

---

17 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 210).

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
- Citrix XenDesktop
- 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 214) 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 210).

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 210).

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 and JWS

Rationale

Java is a powerful programming language that can harm your data and system. Disabling the Java plugin in the web browser and Java Web Start (JWS) protects you against execution of Java programs from the Web.

Instructions

By default, both the Java plugin in the web browser and Java Web Start are activated. Here is how to deactivate them:

1. In the IGEL Setup, go to **System > Registry**
2. Go to the registry key `java.deployment.webjava_enabled`.
3. Uncheck **Enable Java content in the browser**.
4. Click **Apply**.
5. Reboot the device.

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 490).
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 (see page 213) 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.

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.

IGEL

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[18].
5. Optionally, assign a Master Profile[19] 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.

---

18 http://edocs.igel.com/index.htm#9531.htm
19 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**.

IGEL

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 239)
- Disabling Bluetooth (see page 240)

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 Linux with Keys

IGEL Linux has a built-in *OpenSSH* server which can be activated and configured via the setup application. It lets you connect securely to the client over the network in order to issue commands or transfer files. While authentication can be done with a username-password combination, using a private-public key pair can increase convenience and/or security. This document describes how to generate and distribute the keys required.

- Generating the SSH Key Pair (see page 243)
- Distributing the Public Key with UMS (see page 245)
- Configuring SSH Access on the Device (see page 247)

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[20].

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.

---

20 http://blakesmith.me/2010/02/08/understanding-public-key-private-key-concepts.html

> ⚠️ This increases convenience because you will be able to log in without entering the passphrase. However, it weakens security: The private key file will be unprotected if it gets into the hands of an attacker.

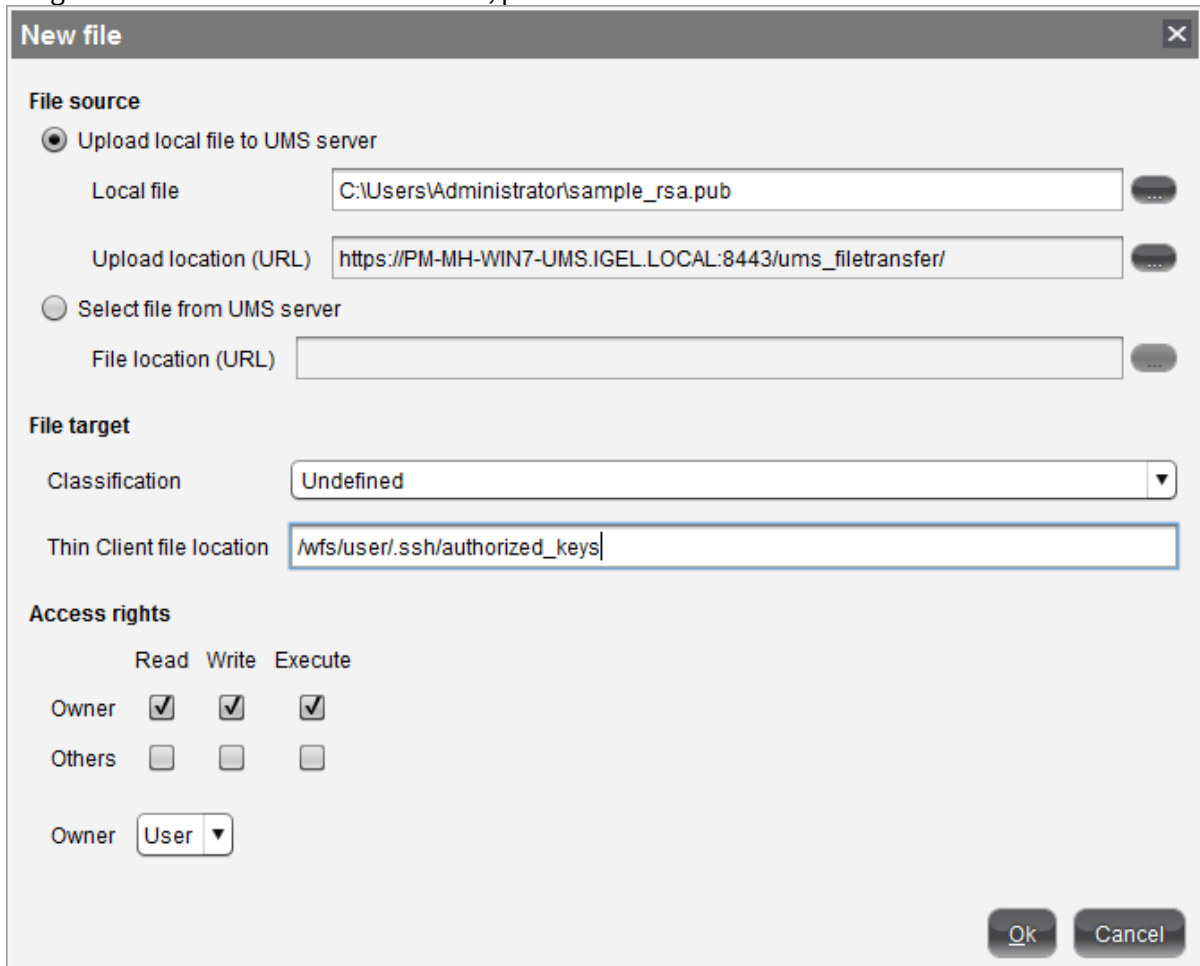Two files have been generated (default names):

- `id_rsa` - the private key file
- `id_rsa.pub` - the public key file

Distributing the Public Key with UMS

1. In *UMS Console*, right-click on **Files** in the navigation tree.
2. Select **New File.**
3. Upload the public key file (`*.pub`) as a **Local File**.

> ⬥ Make sure that you do not upload the private key file by mistake.

4. Set the **Classification** to **Undefined.**
5. Specify the **Thin Client file location** as `/wfs/user/.ssh/authorized_keys`
6. Leave the **Access rights** as **Read, Write, Execute.**
7. Leave the **Owner** as **User.**
8. Assign the file to the desired thin clients, profiles or directories.

ⓘ If you wish to authorize more keys for SSH connections to thin clients, prepare an
`authorized_keys` file containing all the public keys. Simply append them using a text
editor.

Configuring SSH Access on the Device

1. Go to **System > Remote Access > SSH Access** in the IGEL Setup or a profile.
2. Check **Enable.**
3. Optionally, if `user` has an empty password, check **Permit empty passwords.**
4. Set **Deny** to **No** in the **User access** entry for **user**.

> ⓘ This configuration gives the remote user full shell access as if they were the local user on the client.

Now you can connect to the device from the administrator's machine with the following command:

```
ssh user@[client name or IP address]
```

Depending on whether you set a passphrase for the key, you may have to enter it or not.

Secure Terminal (Telnet with TLS/SSL)

IGEL Linux version 5.11.100 or newer and IGEL Linux version 10.01.100 or newer allow terminal access via UMS with transport encryption. In analogy to secure shadowing (see page 249), 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 subject to the following requirements being met:

- IGEL Universal Desktop Linux or IGEL Universal Desktop OS 2, *Version 5.03.190* and newer or *Version 10.01.100* and newer or IGEL Universal Desktop Windows Embedded Standard 7 from *Version 3.09.100.*
- IGEL Universal Management Suite from *Version 4.07.100* onwards.
- The client is registered on the UMS server.
- The client can communicate with 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 client) 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 client) 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 > Shadowing > Secure Shadowing**), 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 does the console call 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 client configuration for all devices that support this function: **UMS Administration > Global Configuration > Remote Access > Activate Global Secure VNC**.

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.
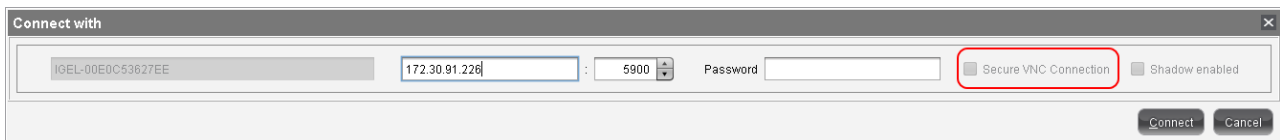
When a VNC connection has been established, the symbol in the connection tab indicates secure shadowing:
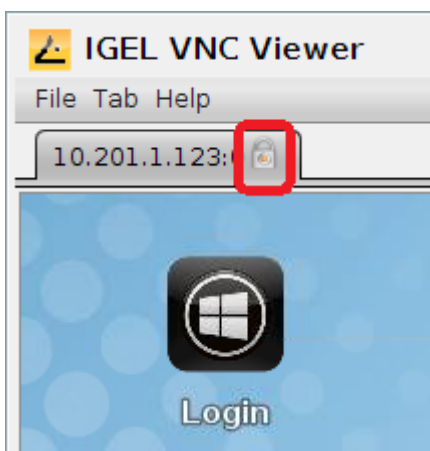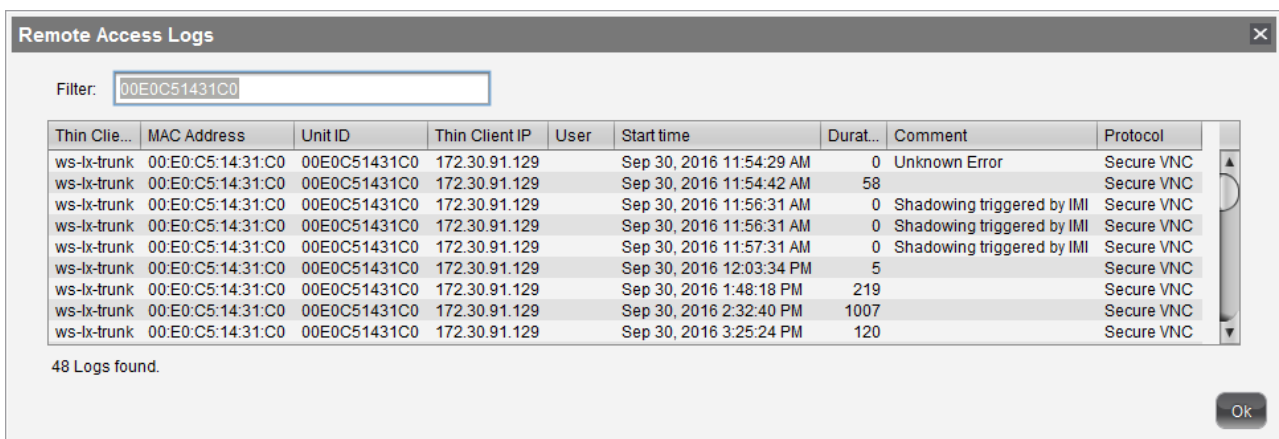
VNC Logging

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.

Ok

▶ To sort the list (e.g. according to user names), click on the relevant column header or filter the content shown by making entries in the **Filter** field.

Cherry eGK Channel Substitution

As of firmware version 10.05.100, the Cherry eGK Channel is no longer available. In the Igel Universal Desktop Firmware, Linux V5, the VirtualChannel for Cherry eGK devices is still included parallel to the Cherry USB2LAN Proxy. If you want to continue using the G87-1504/ST-1503 as before, with firmware version 10.05.100 and higher you have to activate the proxy. All settings are automatically applied and run through the connector in the network.
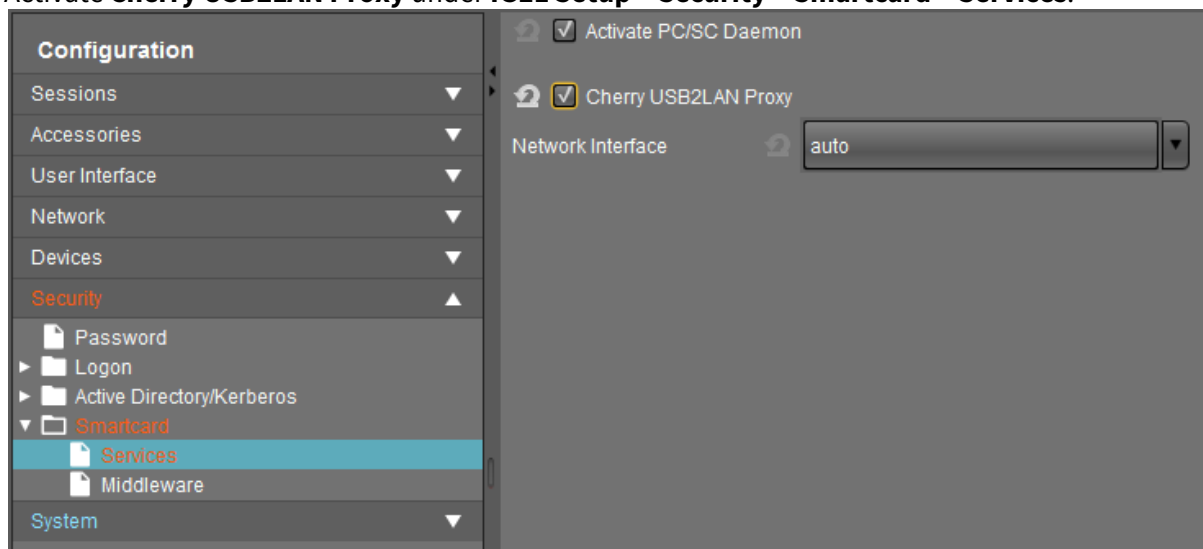
Using the G87-1504/ST-1503 with firmware version 10.05.100 and higher:

- Activate the proxy - this can also be done from the backend.

> ⓘ
> - Cherry USB2LAN Proxy (Under Smartcard) (see screenshot)
> - IGEL device, valid for Cherry devices G87-1505, G87-1504/ST-1503 to USB

For IGEL Lx v5 and OS10:

- Activate **Cherry USB2LAN Proxy** under **IGEL Setup > Security > Smartcard > Services**.

For IGEL Lx v5:

- Disable **Cherry Channel 0** and **Cherry Channel 1** under **IGEL Setup > Sessions > RDP > RDP Global > Mapping > Device Support**.

- Do not activate smartcard.
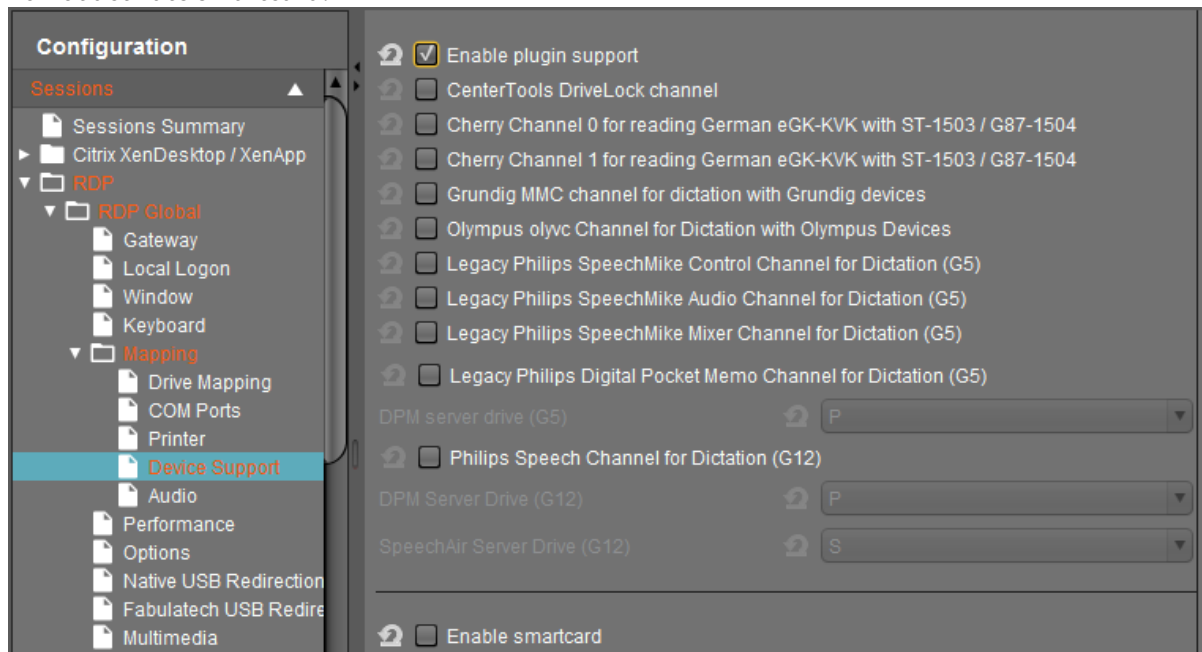
Install the Cherry eGK KVK software on the server. See https://www.cherry.de/files/software/Cherry-eGK-KVK_Software_33.zip

Install the Cherry Linux software on the device.

- In the CT-API configuration the G87-1504/ST-1503 can be configured as network device.
- Link to Doku Client Server Integration: https://www.cherry.de/files/manual/64410063-01_USBLANProxyClientServerUndCitrix.pdf
- Link to the software architecture documentation:: https://www.cherry.de/files/manual/Cherry-eGK-KVK_Sofware-Architektur_Windows-20130927-v04.pdf

> ⓘ The VirtualChannel was replaced due to the following difficulties and the future application of the telematics infrastructure (see also gematik anforderung lan)
> - Independent of Citrix version (no need to check compatibility anymore)
> - Independent of the server version (2008, 2012...), if the connection runs via RDP

Single Sign-on for the Browser Proxy

Using a proxy to handle a browser's internet traffic provides additional security and control. However, if the proxy is password-authenticated, the user has to enter their credentials, which adds some inconvenience.

With IGEL Linux *version 5.08* or newer and IGEL Linux *version 10.01.100* or newer, you can avoid this inconvenience by using the passthrough feature. As a prerequisite, user logon must be carried out via Kerberos.
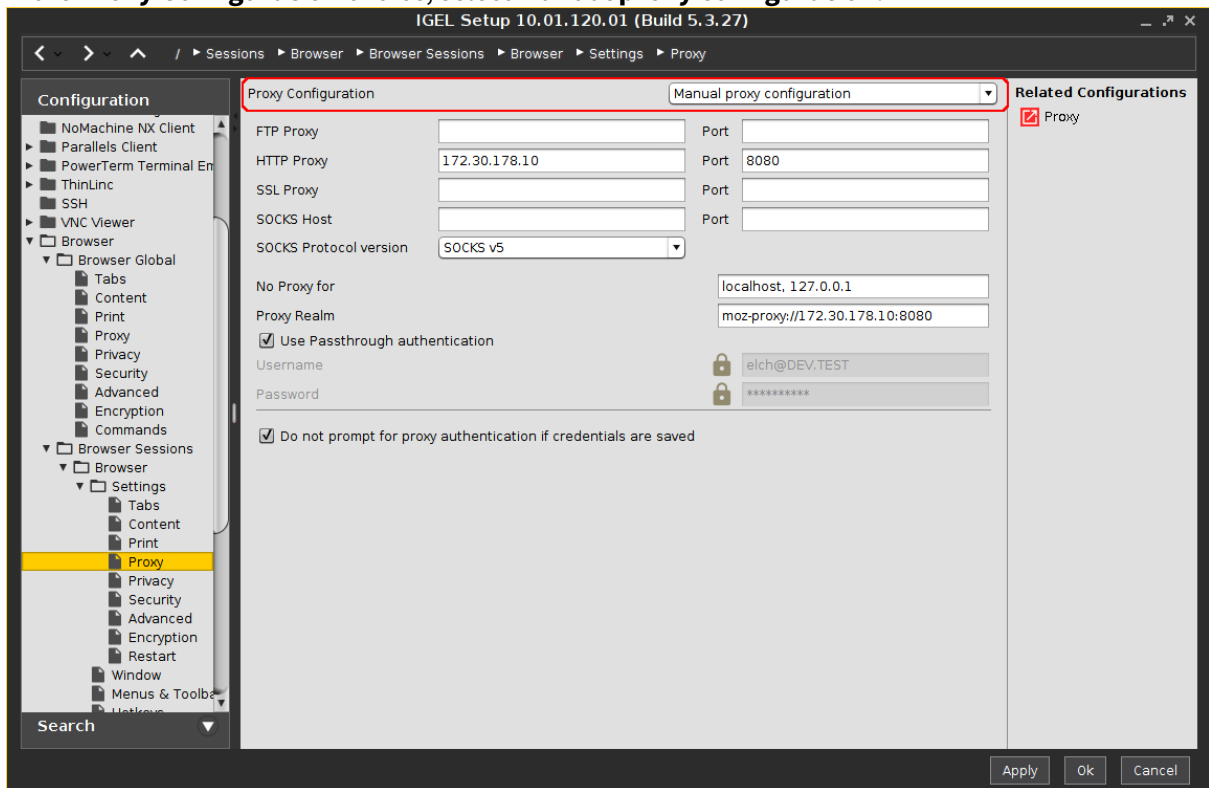
To enable single sign-on for the browser proxy:

1. Open the Setup and go to **Security > Logon > Active Directory/Kerberos**.
2. Activate **Login to Active Directory/Kerberos**.
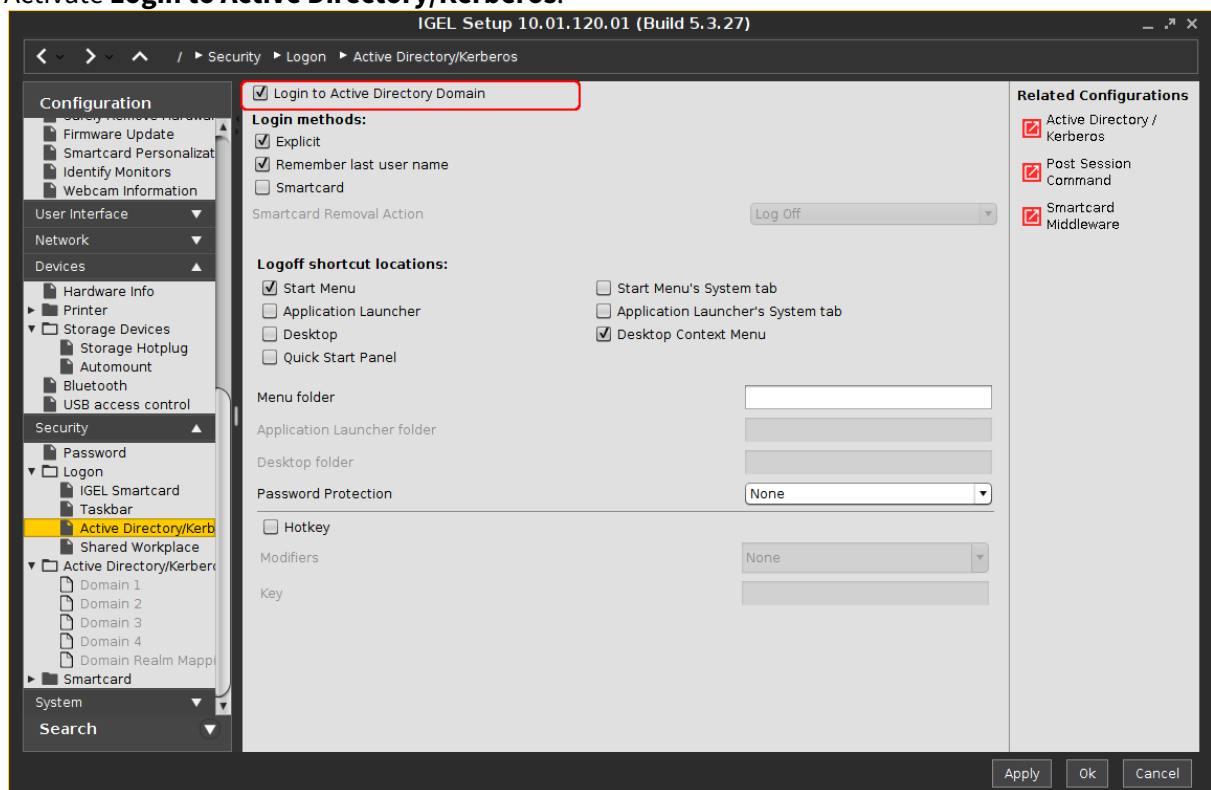
3. Go to **Sessions > Browser > Browser Sessions >** [name of the browser session] **> Settings > Proxy**.

4. In the **Proxy Configuration** choice, select **Manual proxy configuration**.

5. For an HTTP proxy, define the following settings:
   - **HTTP proxy**: IP address or hostname of the proxy to be used
   - **Port**: Port of the proxy for HTTP
   - **No proxy for**: IP addresses or hostnames of servers that can be accesses directly
   - **Proxy realm**: Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

> ⓘ The **Proxy realm** field is internally pre-populated with the value `moz-proxy://[HTTP Proxy]:[Port]`. If the field is empty, this value will be used when authenticating the browser. If the proxy expects another unknown value for the proxy realm, you can determine this as follows: Leave the **User name** and **Password** fields empty and launch the browser. The dialog window which appears will contain the correct value for the **Proxy realm** field:

In the

example above, the value for the **Proxy realm** field is as follows: `moz-proxy://172.30.178.10:8080`

- **Use passthrough authentication**: Must be enabled to allow single sign-on for the browser proxy.
- **Do not prompt for proxy authentication if credentials are saved**: Must be enabled to enable seamless single sign on for the browser proxy; suppresses the **Authentication Required** dialog.
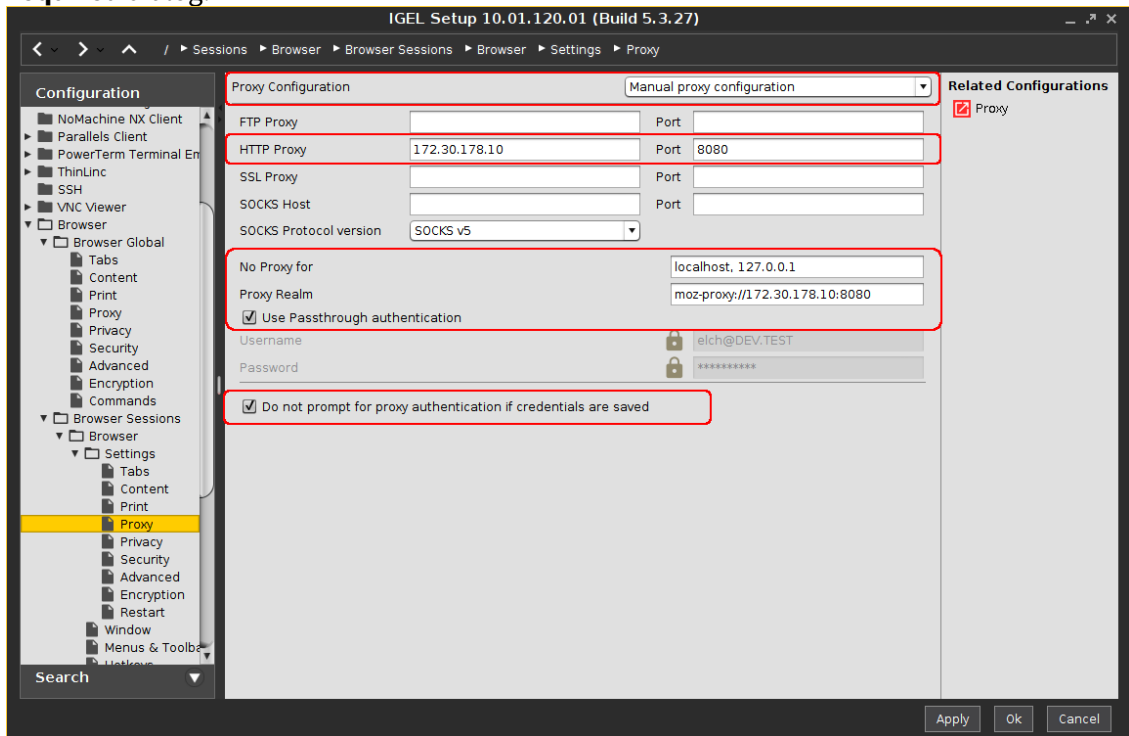
The next time the user logs in to the device, the browser proxy is ready to use.

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**.

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:
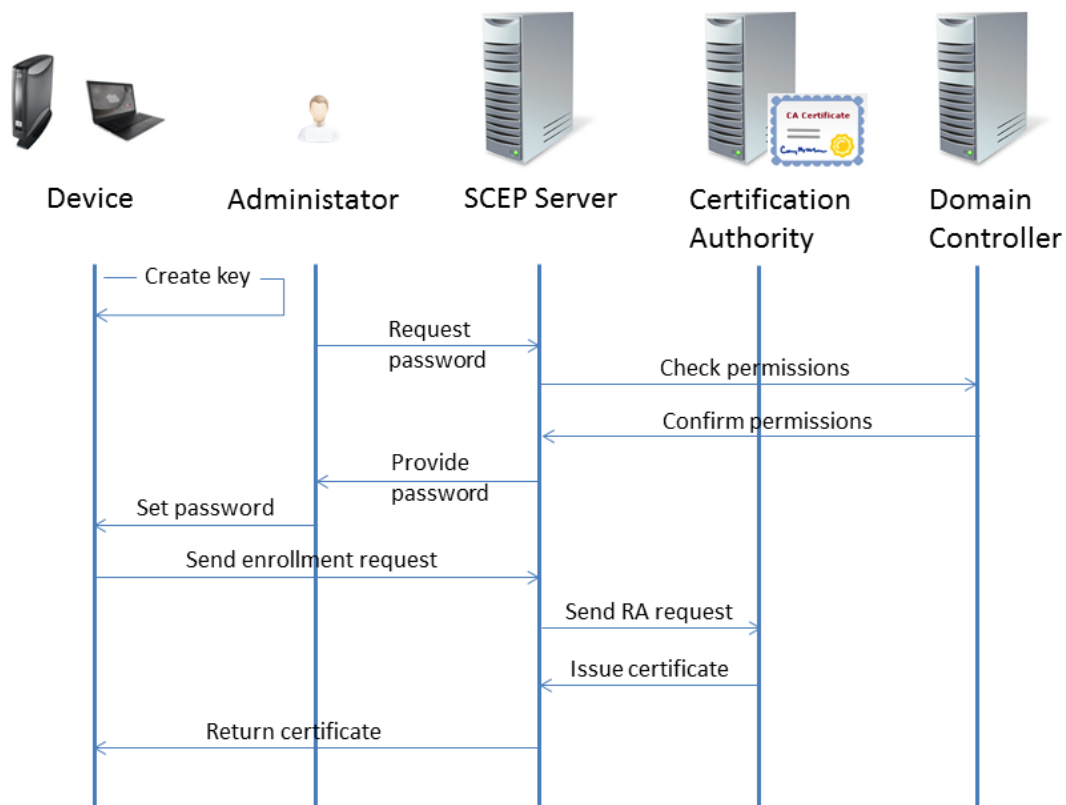
1. The device creates an RSA public-private key pair.
2. The administrator requests a challenge password from the SCEP service (e. g. NDES).

> ⓘ 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 .

> (i) 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 .
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 Linux device is carried out as follows:

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**.

IGEL
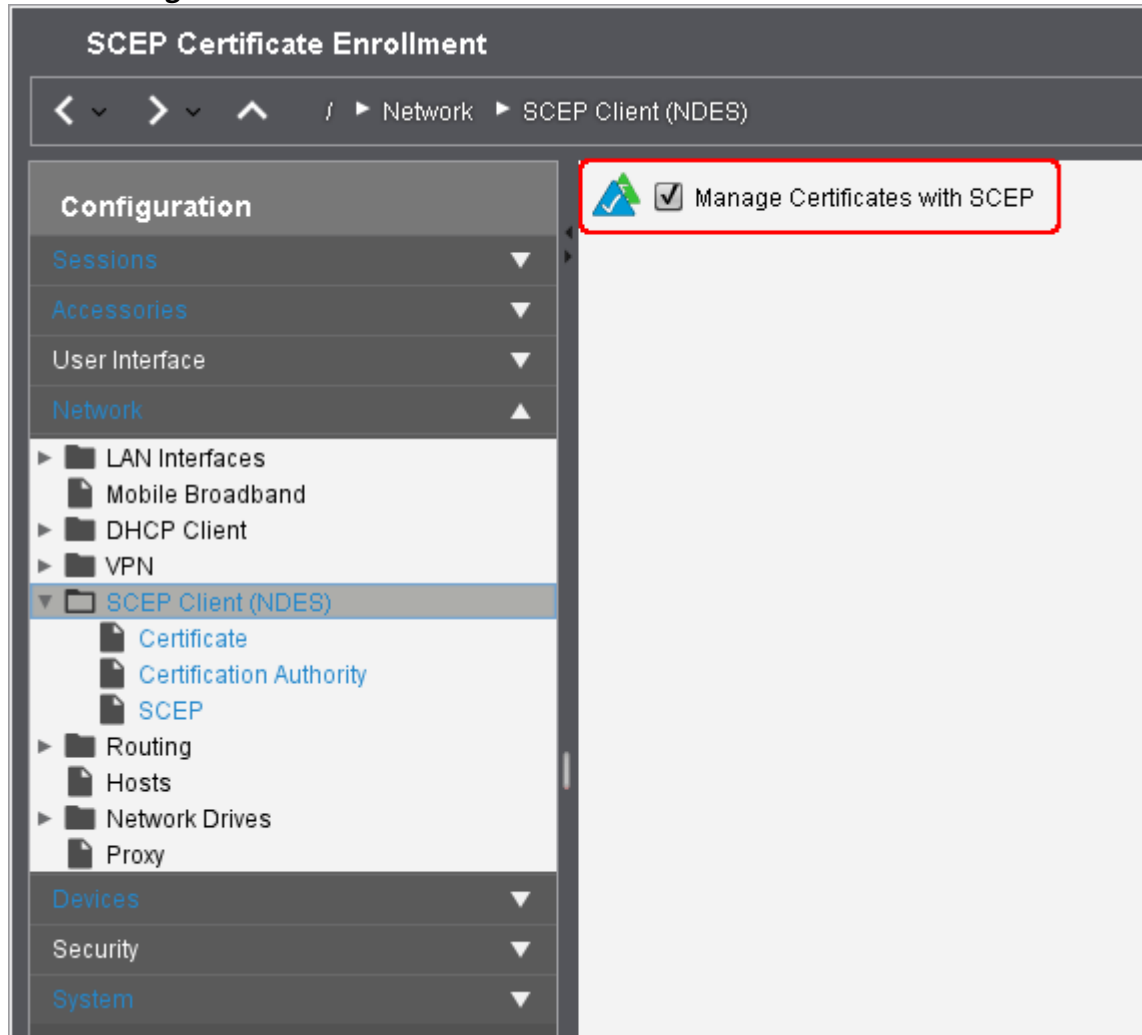
Entering the Data for the Certificate Signing Request (CSR)

▶ Go to **Network > SCEP Client (NDES) > Certificate** and enter the following data:

Type of CommonName/SubjectAltName: The characteristic for linking the certificate to the thin client.

- IP address: The IP address of the thin client.
- DNS name: The DNS name of the thin client.
- IP address (auto): The IP address of the thin client (inserted automatically).
- DNS name (auto): The DNS name of the thin client (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 thin 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 thin client's locality. Example: "Augsburg".

State: Details regarding the thin client's locality. Example: "Bayern".

Country: Two-digit ISO 3166-1 country code. Example: "DE".

RSA key length (bits): Select a key length (one suited to the certification authority) for the certificate that is to be issued.
Possible values:

- "1024"
- "2048"
- "4096"

ⓘ The RSA key length specified here must not be lower than the minimum key length configured on the server.

Defining the Certification Authority (CA)

1. Go to **Network > SCEP Client (NDES) > Certification Authority**.
2. Enter the details for the certification authority (CA):
   - **CA Identifier**: FQDN (fully qualified domain name) of the CA
   - **CA Certificate Fingerprint (MD5)**: Fingerprint of the CA certificate in the form
     `01:02:03:04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10`

> ⓘ You can get the fingerprint from your NDES server: `https://<NDES Servername>/`
> `certsrv/mscep_admin`
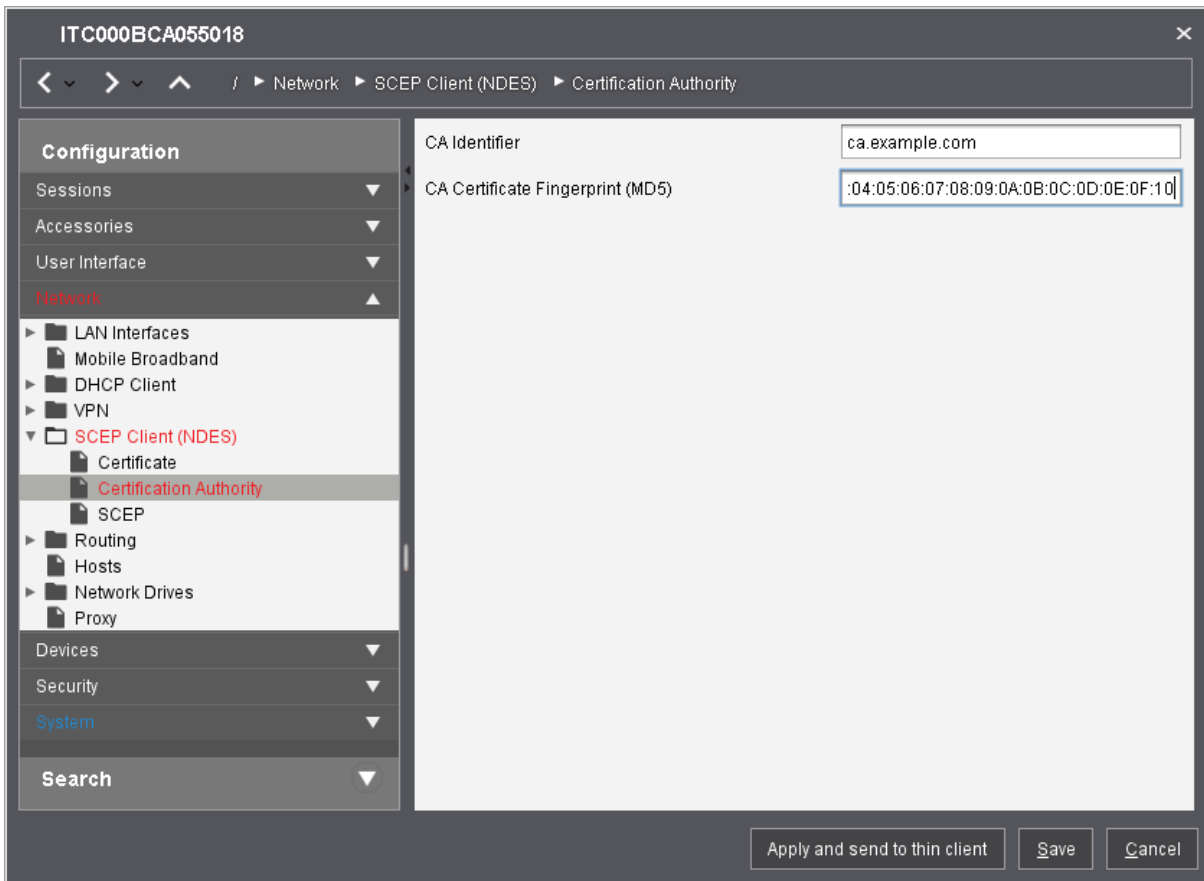
If the CA certificate fingerprint is specified, the client will use it to check the integrity of the CA certificate it receives from the SCEP server.

Providing the SCEP Server Data

1. Go to **Network > SCEP Client (NDES) > SCEP**.
2. Enter the following data:
   - **SCEP server URL**: URL by which the SCEP client communicates with the SCEP server.

   > ⓘ HTTPS is not supported; however, all security critical data that are transferred between the SCEP client and other components are encrypted.

   - **Proxy server for SCEP requests** (optional): IP address or host name of the proxy server that is used for the communication between the device and the SCEP server. If a web application firewall is used instead of a proxy, its IP address or host name of the proxy server must be entered here.
   - **Challenge password**: Password that the SCEP client must present to the SCEP server in its request (CSR).

   > ⓘ On a Microsoft NDES server, you can retrieve the password by default under `https:///certsrv/mscep_admin`.

   > ⚠ By default, the password on a Microsoft NDES server is valid for 1 hour and can be used only once. In order to use the password on numerous devices, additional settings must be made on the NDES server. For information, see the section "Password and Password Cache" on https://social.technet.microsoft.com[21].

   - **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.

---

[21] https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx

IGEL

Applying the Profile to the Thin Clients

1. Select all thin clients in the structure tree.
2. In the **Assigned objects** area, click ⊕.
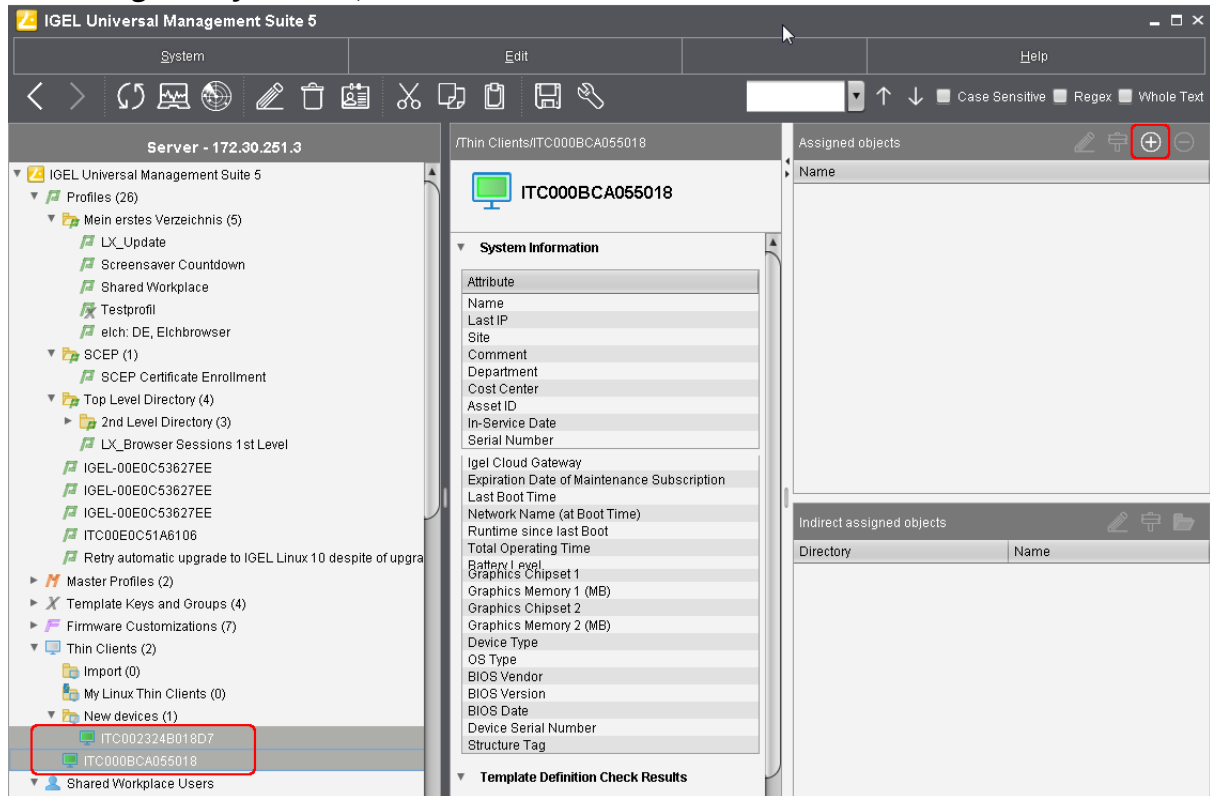
3. In the **Select assignable objects** dialog, select the relevant profile and click ⟩ to assign it.
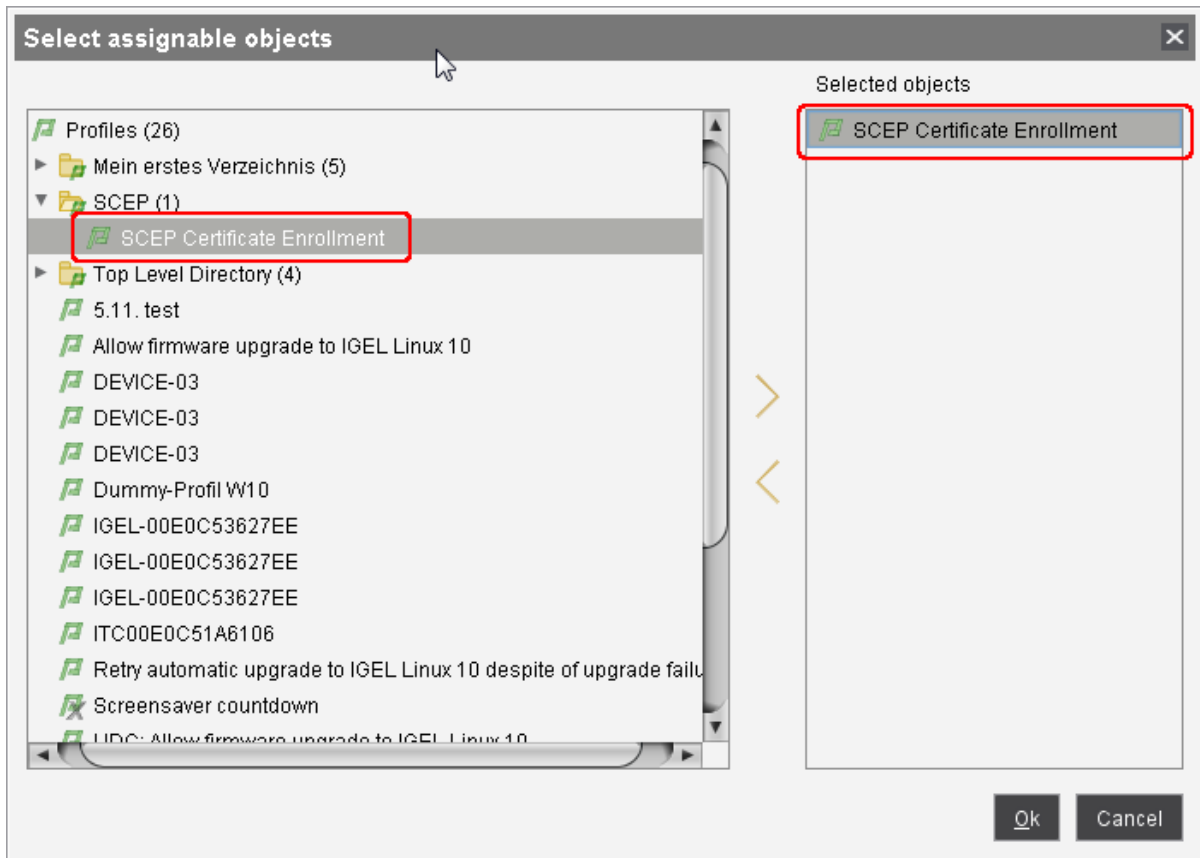
4. Click **Ok**.

5. In the **Update time** dialog, select **Now** and click **Ok**.
   The client performs the actions as described in Client Enrollment Details .

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 276)

IGEL
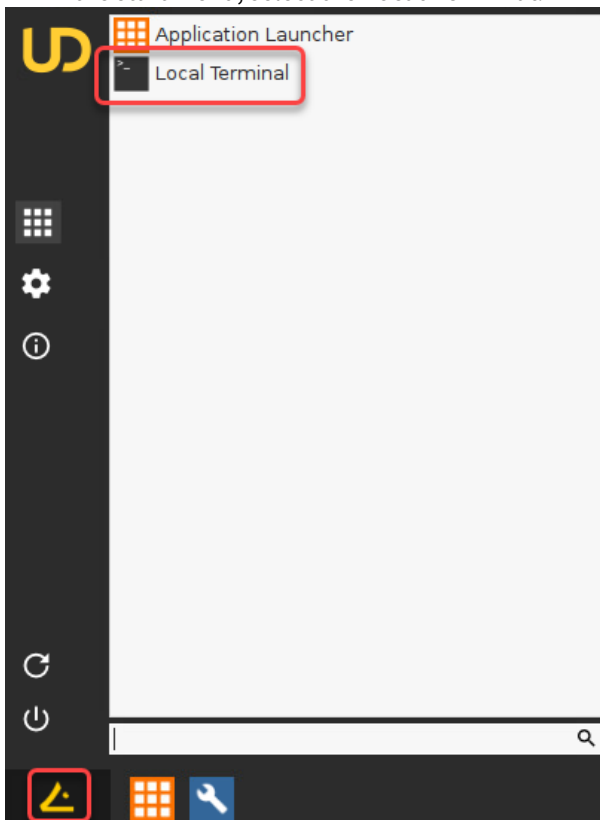
Diagnostics

Preliminary: Tools

System Log Viewer

▶ In the start menu, select the system icon and then **System Log Viewer** to open the system log viewer.
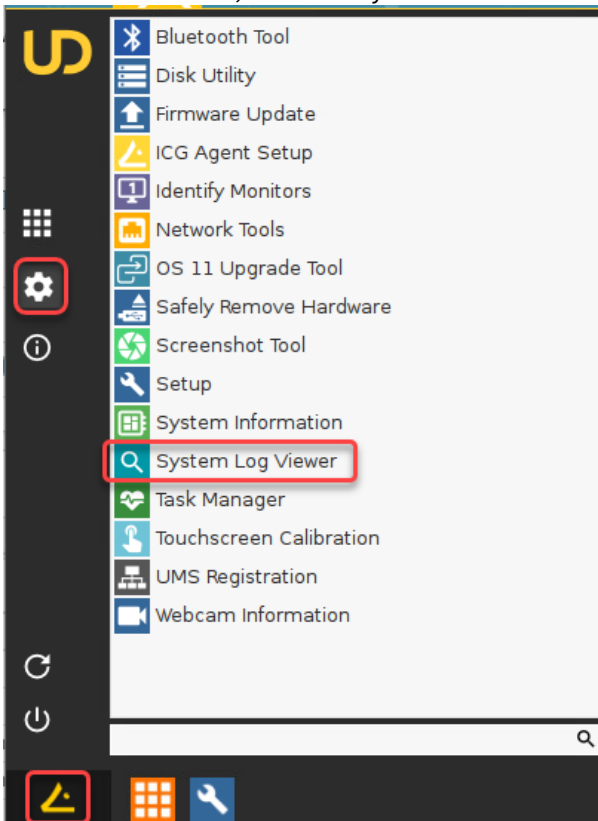
For more information on starting, using, and configuring the system log viewer, see the System Log Viewer chapter of the IGEL OS Manual.

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 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[22]. They are named `[version]_CA-certificates.txt` - for example, the list for IGEL OS version 10.03.100[23].

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-----
MIIDwzCCAkOgAwIBAgIQa64BW7UVO6dG
MRQwEgYKCZImiZPyLGQBGRYEdGVzdDETI
            ...
3iNjPszgHJs9LmHM9mmy5q29z8B0GZUJl
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

22 http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX/V10/
23 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
- Installing Certificates Manually

IGEL

Deploying Certificates via UMS

We recommend using the Universal Management Suite when you need to deploy certificates to a several thin clients.

Step 1: Loading certificate in the UMS

1. Open the **UMS console**.
2. Right-click **Files**.
3. Choose **New file** to open the **New file** dialog.
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**.
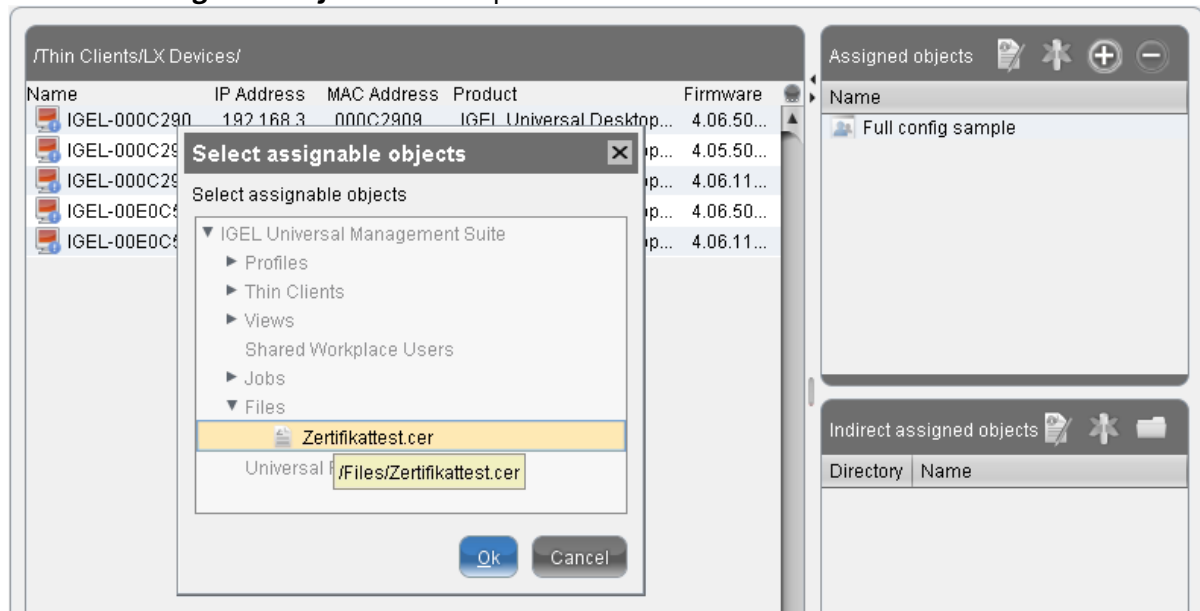7. Confirm with **OK**.
   Your certificate is now listed in the **Files** window.

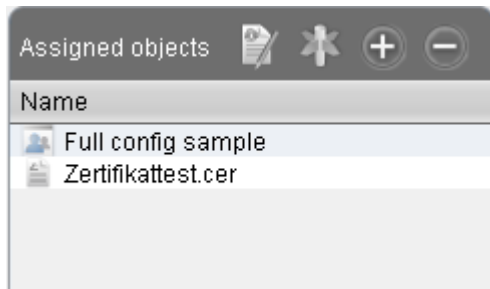### Step 2: Assigning certificates to thin clients

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.

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**.

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**.
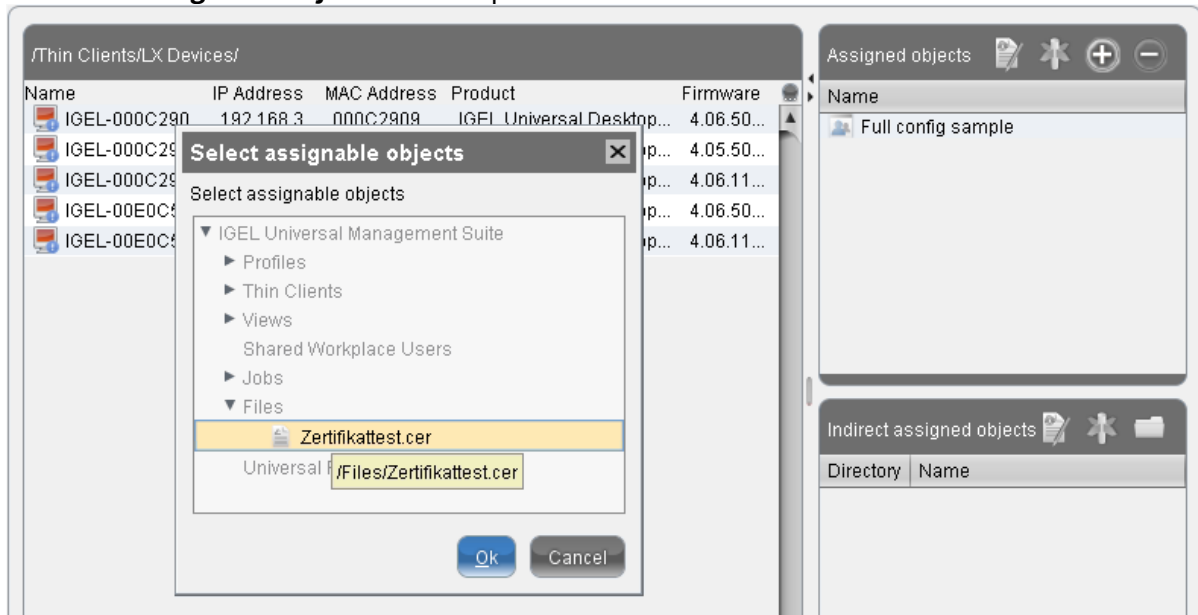7. Confirm with **OK**.
   Your certificate is now listed in the **Files** window.

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.

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**.
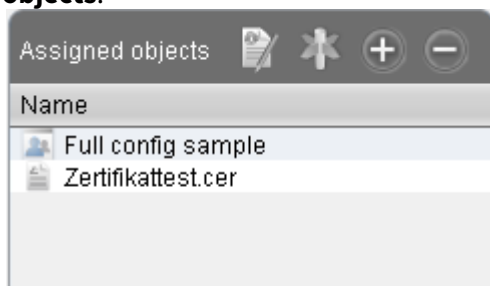
Installing Certificates Manually

Use the **Firefox Certificate Manager** in order to install web browser certificates; see Installing Web Browser Certificates .

For Java Runtime Environment certificates, use the **Java Manager** from the IGEL Setup; see Installing JRE Certificates .

Also a USB flash drive can be used for the manual import.

IGEL

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.
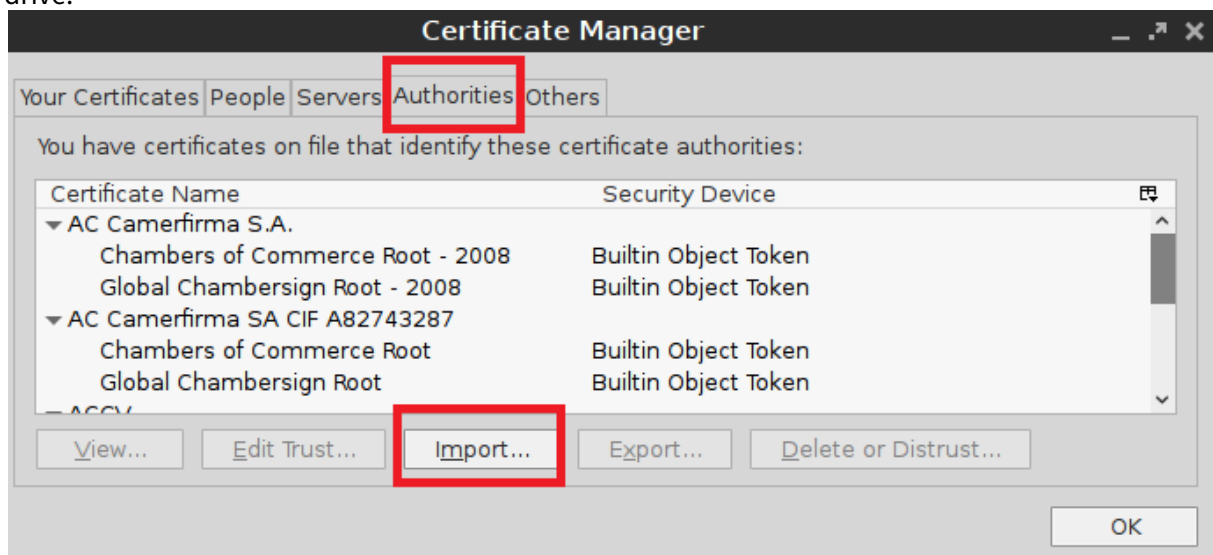
IGEL

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**.
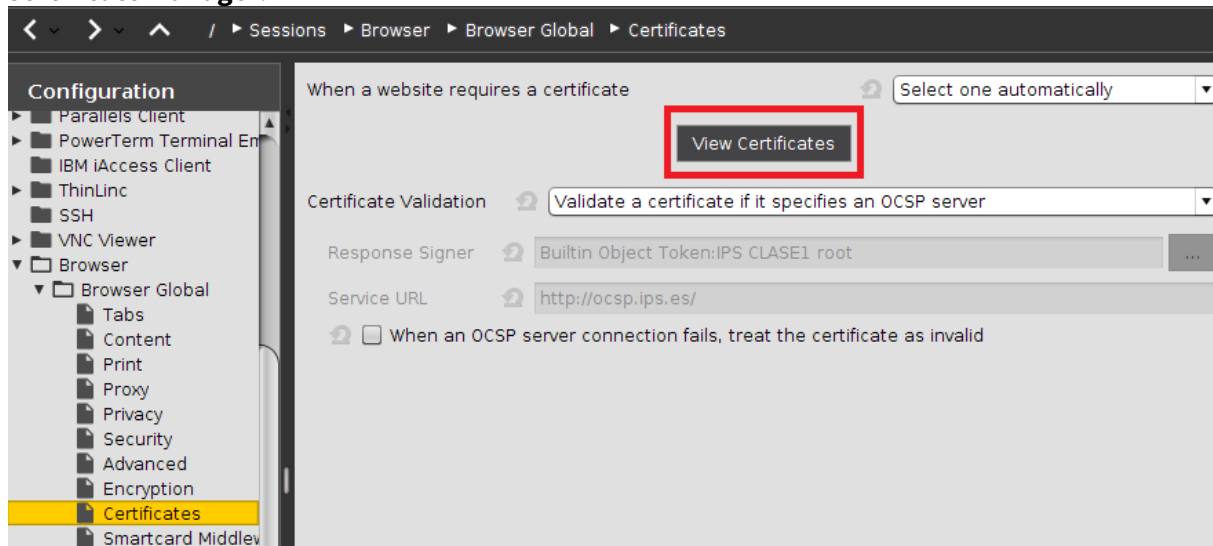
3. Click **Import...** in the **Authorities** tab to import a new certificate from a directory or a USB flash drive.


ⓘ   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.
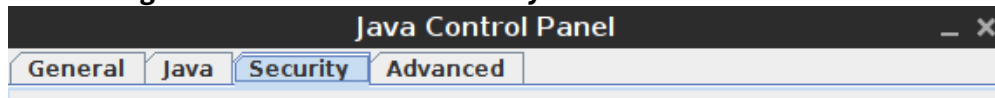
6. Choose **Signer CA** under **Certificate type**.
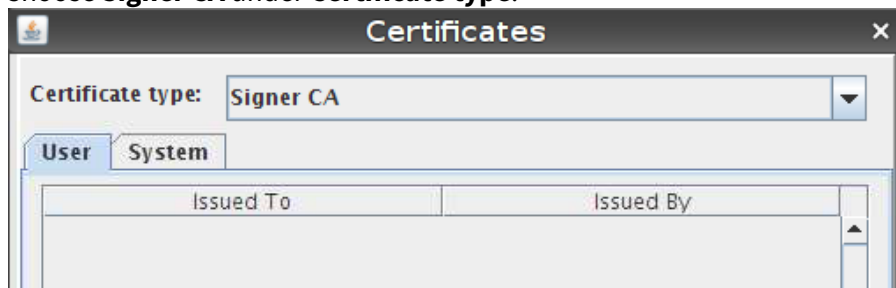
7. Import the certificate.

> ⓘ 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 10.05:

Certificate name	Expiry date	File in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	`ACCVRAIZ1.crt`
ACEDICOM Root	Apr 13 16:24:22 2028 GMT	`ACEDICOM_Root.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`
AddTrust Class 1 CA Root	May 30 10:38:31 2020 GMT	`AddTrust_Low-Value_Services_Root.crt`
AddTrust Public CA Root	May 30 10:41:50 2020 GMT	`AddTrust_Public_Services_Root.crt`
AddTrust Qualified CA Root	May 30 10:44:50 2020 GMT	`AddTrust_Qualified_Certificates_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`

Certificate name	Expiry date	File in /etc/ssl/certs
Amazon Root CA 2	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_2.crt`
Amazon Root CA 3	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_3.crt`
Amazon Root CA 4	May 26 00:00:00 2040 GMT	`Amazon_Root_CA_4.crt`
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	`Atos_TrustedRoot_2011.crt`
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	`Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt`
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	`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 R1	Jul 19 09:06:56 2042 GMT	`CA_Disig_Root_R1.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`
CNNIC ROOT	Apr 16 07:09:14 2027 GMT	`CNNIC_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`

Certificate name	Expiry date	File in /etc/ssl/certs
Chambers of Commerce Root	Sep 30 16:13:44 2037 GMT	`Camerfirma_Chambers_of_Commerce_Root.crt`
Global Chambersign Root	Sep 30 16:14:18 2037 GMT	`Camerfirma_Global_Chambersign_Root.crt`
Certigna	Jun 29 15:13:05 2027 GMT	`Certigna.crt`
Certinomis - Autorité Racine	Sep 17 08:28:59 2028 GMT	`Certinomis_-_Autorité_Racine.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`
Certum CA	Jun 11 10:46:39 2027 GMT	`Certum_Root_CA.crt`
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	`Certum_Trusted_Network_CA.crt`
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	`Certum_Trusted_Network_CA_2.crt`
Chambers of Commerce Root - 2008	Jul 31 12:29:50 2038 GMT	`Chambers_of_Commerce_Root_-_2008.crt`
China Internet Network Information Center EV Certificates Root	Aug 31 07:11:25 2030 GMT	`China_Internet_Network_Information_Center_EV_Certificates_Root.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_AAA_Services_root.crt`
Secure Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_Secure_Services_root.crt`
Trusted Certificate Services	Dec 31 23:59:59 2028 GMT	`Comodo_Trusted_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 ACES CA X6	Nov 20 21:19:58 2017 GMT	`DST_ACES_CA_X6.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 Assured ID Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Assured_ID_Root_CA.crt`
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G2.crt`
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Assured_ID_Root_G3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_Global_Root_CA.crt`
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G2.crt`
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	`DigiCert_Global_Root_G3.crt`
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	`DigiCert_High_Assurance_EV_Root_CA.crt`
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	`DigiCert_Trusted_Root_G4.crt`
E-Tugra Certification Authority	Mar 3 12:09:48 2023 GMT	`E-Tugra_Certification_Authority.crt`
EC-ACC	Jan 7 22:59:59 2031 GMT	`EC-ACC.crt`
EE Certification Centre Root CA	Dec 17 23:59:59 2030 GMT	`EE_Certification_Centre_Root_CA.crt`
Entrust.net[24] Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	`Entrust.net_Premium_2048_Secure_Server_CA.crt`
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	`Entrust_Root_Certification_Authority.crt`
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	`Entrust_Root_Certification_Authority_-_EC1.crt`
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	`Entrust_Root_Certification_Authority_-_G2.crt`

---

24 http://Entrust.net

Certificate name	Expiry date	File in /etc/ssl/certs
GeoTrust Global CA	May 21 04:00:00 2022 GMT	`GeoTrust_Global_CA.crt`
GeoTrust Global CA 2	Mar 4 05:00:00 2019 GMT	`GeoTrust_Global_CA_2.crt`
GeoTrust Primary Certification Authority	Jul 16 23:59:59 2036 GMT	`GeoTrust_Primary_Certification_Authority.crt`
GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	`GeoTrust_Primary_Certification_Authority_-_G2.crt`
GeoTrust Primary Certification Authority - G3	Dec 1 23:59:59 2037 GMT	`GeoTrust_Primary_Certification_Authority_-_G3.crt`
GeoTrust Universal CA	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA.crt`
GeoTrust Universal CA 2	Mar 4 05:00:00 2029 GMT	`GeoTrust_Universal_CA_2.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R4.crt`
GlobalSign	Jan 19 03:14:07 2038 GMT	`GlobalSign_ECC_Root_CA_-_R5.crt`
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	`GlobalSign_Root_CA.crt`
GlobalSign	Dec 15 08:00:00 2021 GMT	`GlobalSign_Root_CA_-_R2.crt`
GlobalSign	Mar 18 10:00:00 2029 GMT	`GlobalSign_Root_CA_-_R3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
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[25]	Dec 13 08:27:25 2037 GMT	`Izenpe.com`[26]`.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`
Autoridad de Certificacion Raiz del Estado Venezolano	Dec 25 23:59:59 2020 GMT	`PSCProcert.crt`
QuoVadis Root Certification Authority	Mar 17 18:33:33 2021 GMT	`QuoVadis_Root_CA.crt`

---

25 http://Izenpe.com
26 http://Izenpe.com

Certificate name	Expiry date	File in /etc/ssl/certs
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	`QuoVadis_Root_CA_1_G3.crt`
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	`QuoVadis_Root_CA_2.crt`
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	`QuoVadis_Root_CA_2_G3.crt`
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	`QuoVadis_Root_CA_3.crt`
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	`QuoVadis_Root_CA_3_G3.crt`
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 EV RootCA1	Jun 6 02:12:32 2037 GMT	`Security_Communication_EV_RootCA1.crt`
Security Communication RootCA2	May 29 05:00:39 2029 GMT	`Security_Communication_RootCA2.crt`
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	`Security_Communication_Root_CA.crt`
Sonera Class2 CA	Apr 6 07:29:40 2021 GMT	`Sonera_Class_2_Root_CA.crt`
Staat der Nederlanden EV Root CA	Dec 8 11:10:28 2022 GMT	`Staat_der_Nederlanden_EV_Root_CA.crt`
Staat der Nederlanden Root CA - G2	Mar 25 11:03:10 2020 GMT	`Staat_der_Nederlanden_Root_CA_-_G2.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
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`
Swisscom Root CA 1	Aug 18 22:06:20 2025 GMT	`Swisscom_Root_CA_1.crt`
Swisscom Root CA 2	Jun 25 07:38:14 2031 GMT	`Swisscom_Root_CA_2.crt`
Swisscom Root EV CA 2	Jun 25 08:45:08 2031 GMT	`Swisscom_Root_EV_CA_2.crt`
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_2.crt`
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	`T-TeleSec_GlobalRoot_Class_3.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	`TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt`
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Dec 22 18:37:19 2017 GMT	`TURKTRUST_Certificate_Services_Provider_Root_2007.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`
Trustis FPS Root CA	Jan 21 11:36:54 2024 GMT	`Trustis_FPS_Root_CA.crt`
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3	Aug 21 11:37:07 2017 GMT	`TÜBİTAK_UEKAE_Kök_Sertifika_Hizmet_Sağlayıcısı_-_Sürüm_3.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`
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	`USERTrust_RSA_Certification_Authority.crt`

Certificate name	Expiry date	File in /etc/ssl/certs
UTN-USERFirst-Hardware	Jul 9 18:19:22 2019 GMT	`UTN_USERFirst_Hardware_Root_CA.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".
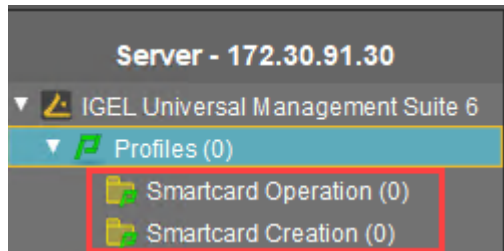
Folder "Smartcard Operation"

In this folder, you create a new profile "Smartcard Login":

1. Right-click the folder "Smartcard Operation".
2. Choose **New Profile**.
3. Enter a **Profile Name**, e.g. "Smartcard Login".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enable **Login with IGEL smartcard**.
6. Enter your **Company key**.
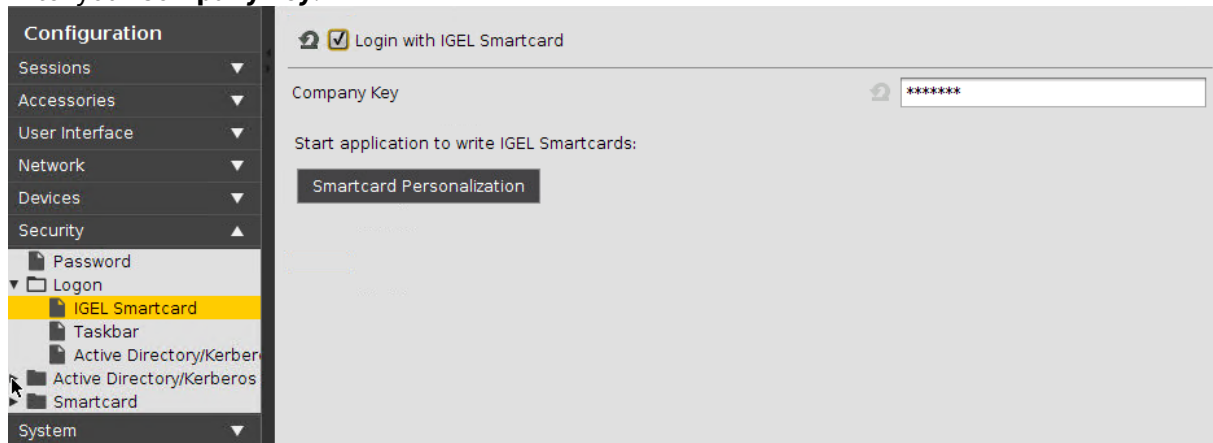
> ⓘ Later on, this profile will be applied to all devices where the authentication process shall work only with a smartcard.
> This way, the device will receive:
> - the company key and
> - the information that the authentication is only possible with the smartcard.

> ⓘ The company key is a private key shared between devices and smartcards. It should be chosen similarly to a good password. If the smartcard does not hold the same company key as the device, authentication will not be possible. Remember this company key because you will need later to write exactly the same key to the smartcard.

Folder "Smartcard Creation"

In this folder, you create a new profile "Smartcard Key":

1. Right-click the folder "Smartcard Creation".
2. Choose **New Profile**.
3. Enter a profile name, e.g. "Smartcard Key".
4. Click **Security > Logon > IGEL Smartcard**.
5. Enter the same **Company key** as in the profile "Smartcard Login".

Another additional folder is useful:

▶ Create the subfolder "Get settings from" under "Smartcard Creation".
In this folder, you create the profile with the session information you want to write to the smartcard.
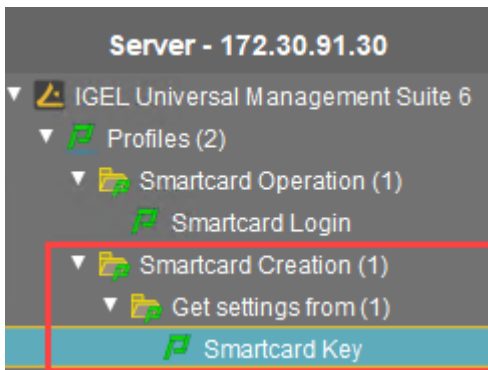
> ⓘ You need this additional folder because the assignment of active profiles from the UMS to the IGEL smartcard can cause problems (firmware version < 5.06.100). Later on, you will copy the folder locally to your device.

Writing the IGEL Smartcard

Assigning the Profile "Smartcard Creation" to the Device

1. Prepare one device which has a smartcard reader/writer.
2. Integrate this device in the UMS and put it into the folder "Smartcard Creation".
   Now the device automatically receives the company key from the profile. It will be used when writing the smartcard.

Ensuring That the Profile Assignment Was Successful

1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.
   You should now see a disabled field **Company key** with a lock symbol.
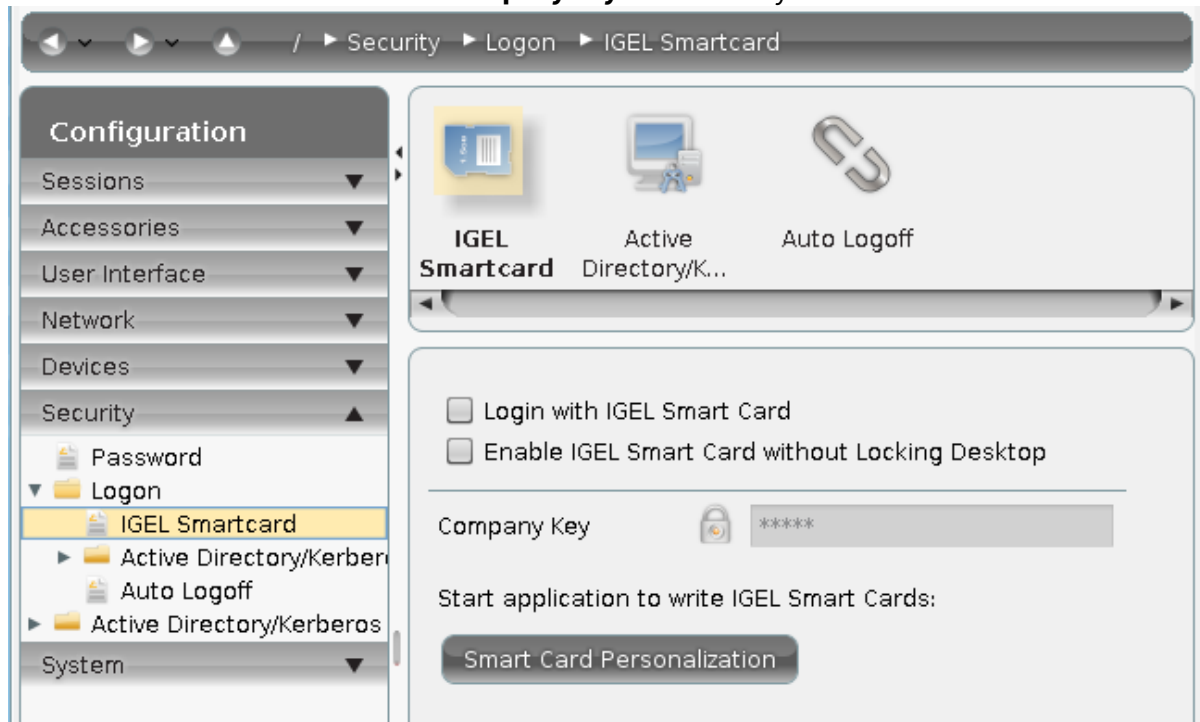
Writing the Profiles to the Smartcard

1. Open the folder "Smartcard Creation" in the UMS.
2. Right-click your device.
3. Choose **Take over settings from...** to copy the profile settings to the device.
   The dialog **Copy settings from...** opens.
4. Choose your profile from the folder "Smartcard Creation" > "Get settings from".
5. Enable **Overwrite Sessions**.
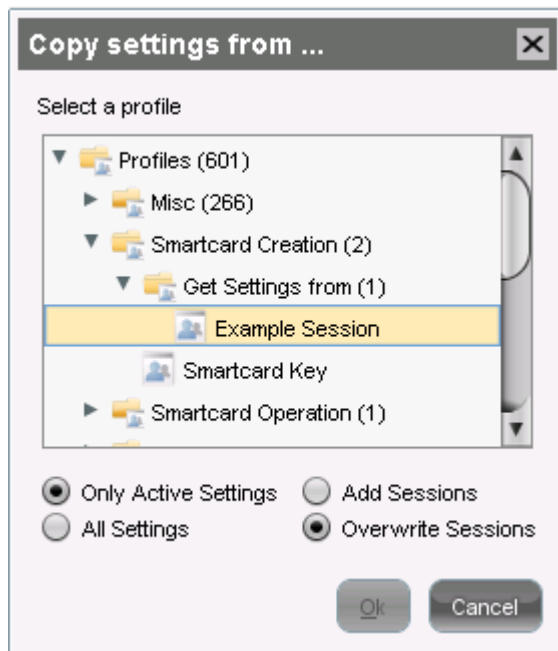
6. Click **OK** to copy the profile with the settings and the company key to the device.

Writing the Smartcard

1. Open the local setup of your device.
2. Click **Security > Logon > IGEL Smartcard**.
3. Click **Smartcard personalization**.
   The **Smartcard personalization** dialog opens.
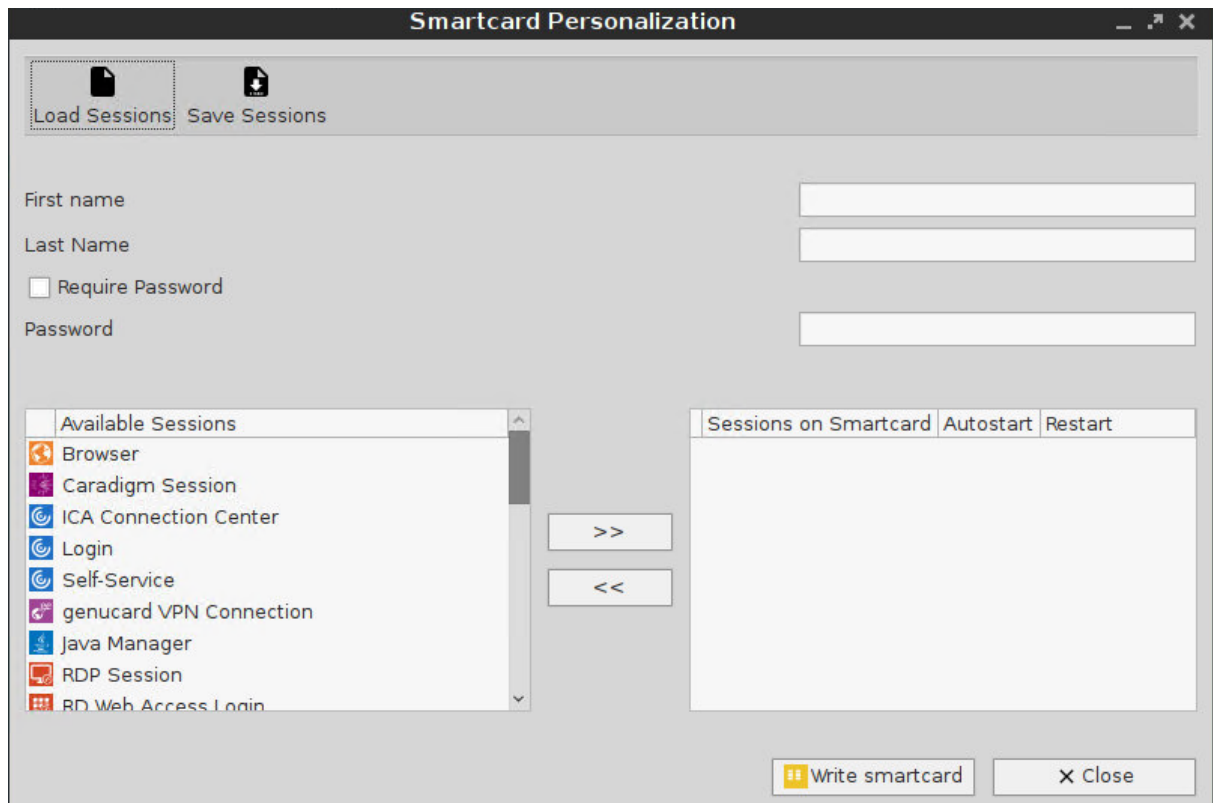
4. Enter the **First name** and the **Last name** of the smartcard holder that should appear at the login prompt.
5. Activate **Require password** and specify the **Password** if a password has to be required for the smartcard login.
6. Select the local sessions you want to write to the smartcard.

> ⓘ Use the arrow buttons to add a session to the smartcard session list.

7. Activate **Autostart** for a session in the smartcard list if it should be automatically started at login. Check **Restart** if desired.

> ⓘ The configuration of the sessions can be saved and reloaded at a later time.

8. Click **Write smartcard** to start the writing process with the defined settings.
9. Confirm the security question with **Yes**.
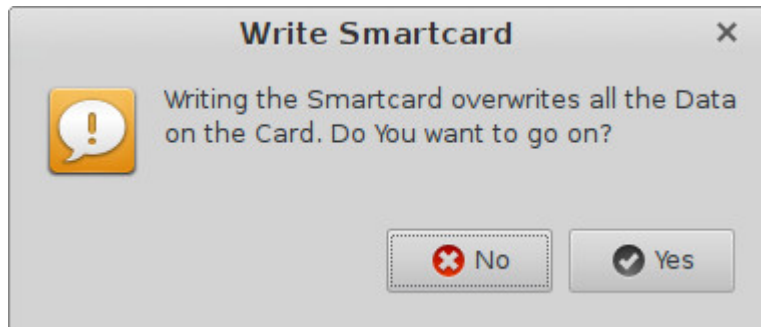
The notice **Smartcard successfully written** appears.
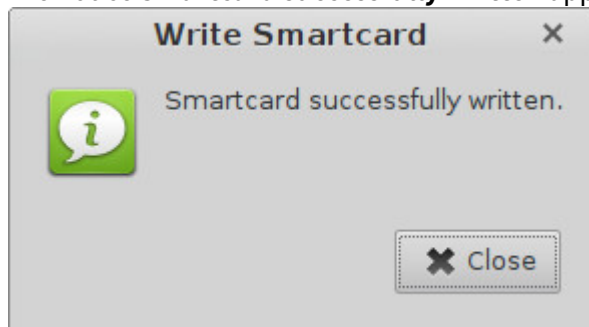
Testing the New IGEL Smartcard

1. Go to the UMS.
2. Register a new device in the UMS and put it in the folder "Smartcard Operation".
   The device gets the company key and the profile information that authentication is only possible with the IGEL smartcard.
3. Restart the device.
   The **Insert Smartcard...** dialog opens.
4. Insert the IGEL smartcard into your device and verify the selected configuration.

IGEL

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[27] 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	✓	✓

---

27 https://www.igel.com/linux-3rd-party-hardware-database/
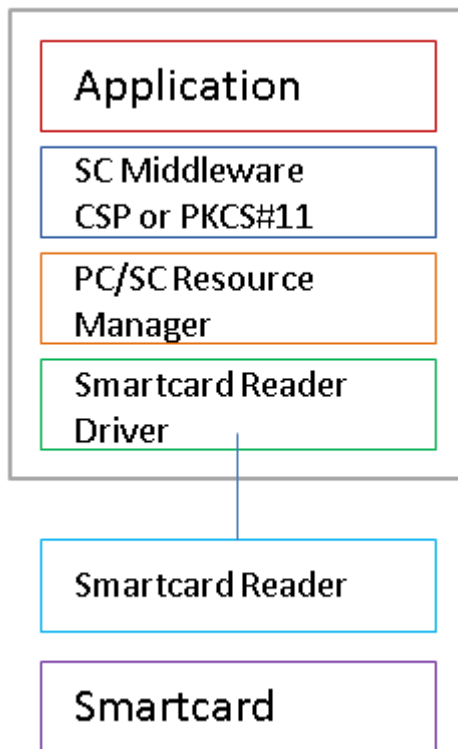
Some of the smartcard authentication methods require s*martcard middleware* to be installed on the endpoint device. The following modules are available:

- *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 378).

- Active Directory Logon with Smartcard (see page 316)
- Citrix Legacy ICA Sessions (see page 317)
- Citrix Legacy ICA Sessions with Local Logon Window (see page 318)
- Citrix StoreFront (see page 319)
- RDP Sessions (see page 321)
- Horizon Sessions (see page 322)
- Smartcard Authentication in Browser (see page 323)

- **Citrix XenDesktop Appliance Mode**

Active Directory Logon with Smartcard

See the how-to Passthrough Authentication .

IGEL

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**.
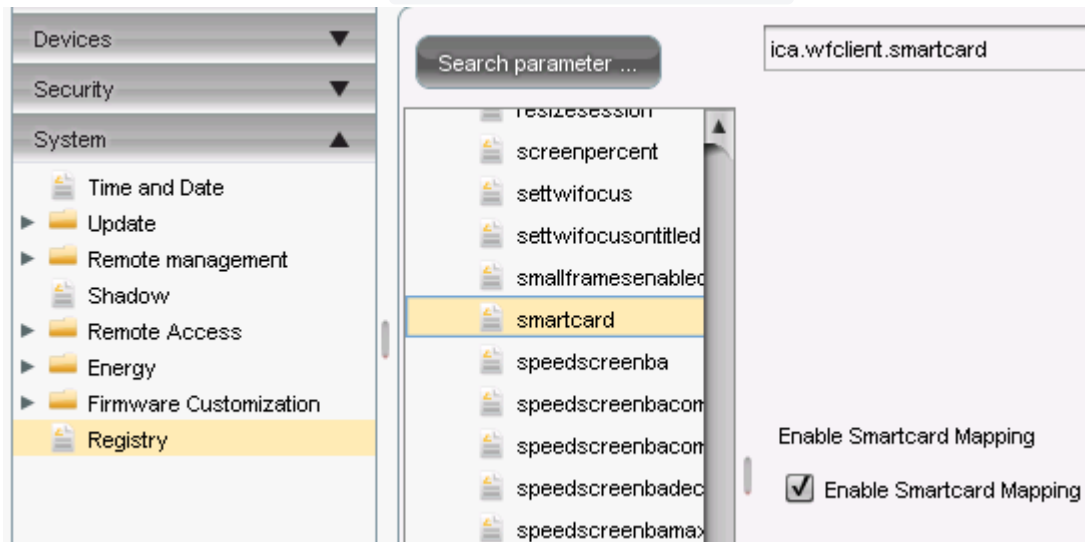
ⓘ Both settings are active by default!

IGEL

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 (see page 317), the following settings are necessary:

▶ Check **Use local login window** and **Smartcard logon** under **Sessions > Citrix > Citrix Global > Legacy ICA Login**.
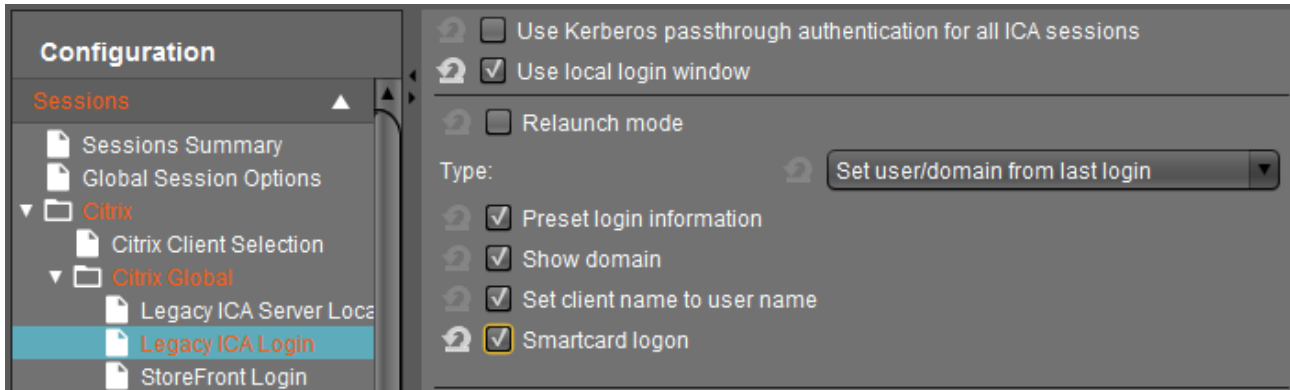
▶ Select the appropriate PKCS#11 module for the smartcard under **Security > Smartcard > Middleware**.

- 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 the CoolKey Cryptographic Library (see page 378).

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 thin client - see Deploying Trusted Root Certificates (see page 280), Certificate Type **SSL Certificate**.

1. Choose **StoreFront** as **Citrix server type** under **Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront/Web Interface > Server**.
2. Specify the **Server Location**.
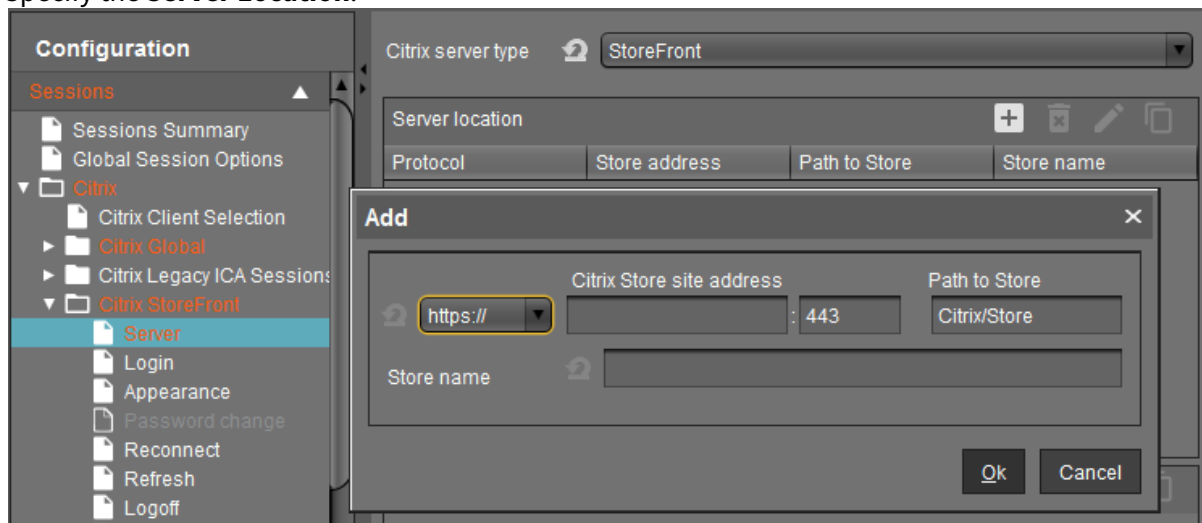
3. Choose **Smartcard authentication** as **Authentication type** under **Sessions > Citrix XenDesktop/XenApp > Citrix StoreFront/Web Interface > Login**.
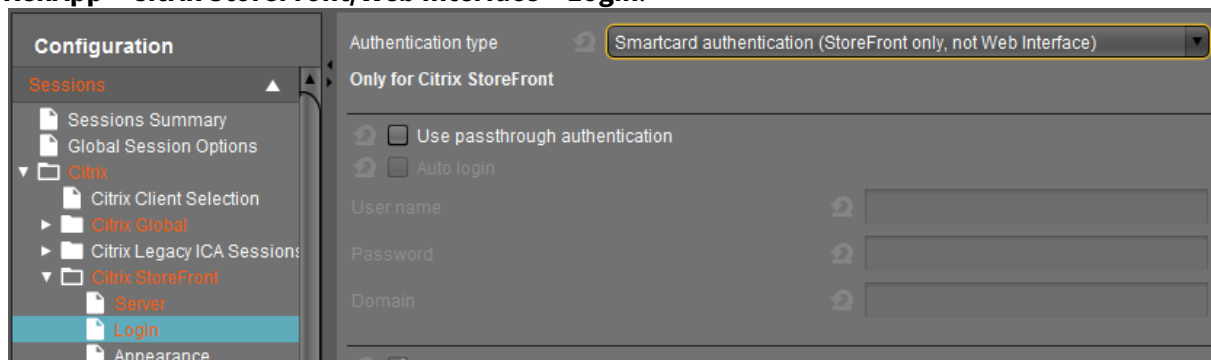
> ⓘ When used in combination with **Active Directory Logon** the enabled **Use Passthrough authentication** activates single sign-on with smartcard.

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 378).

IGEL

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**.

IGEL
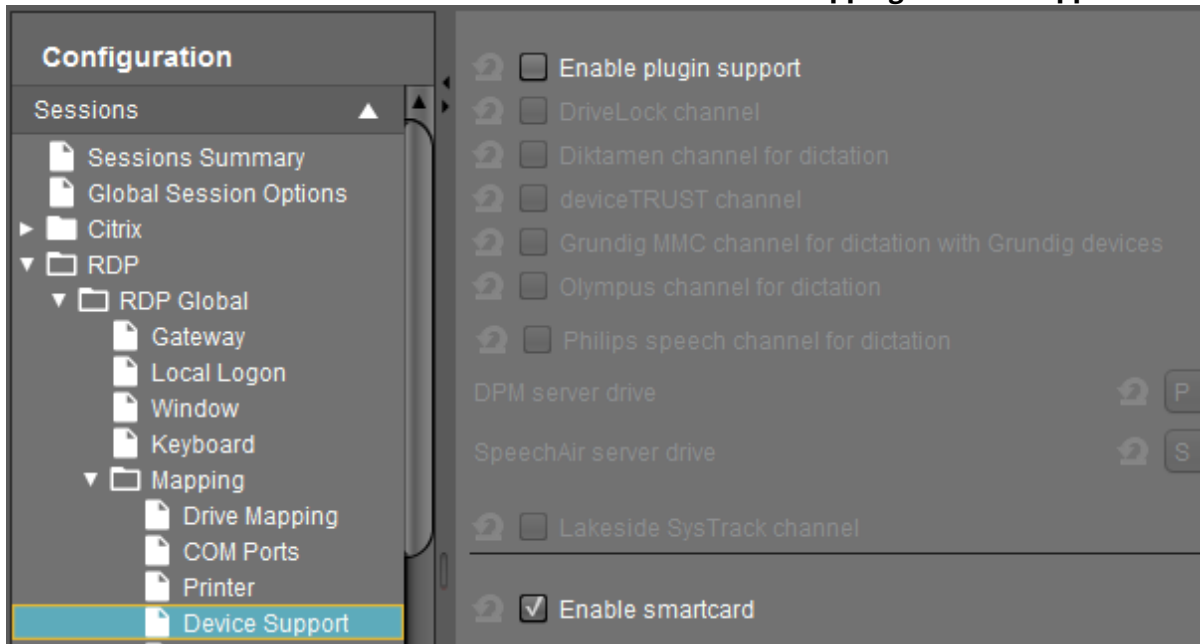
Horizon Sessions

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 280), 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 378).

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 280), 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 378).

Citrix XenDesktop Appliance Mode

First configure the Smartcard authentication as described in Smartcard Authentication in Browser (see page 323).

Additionally:

1. Activate **Enable Citrix Virtual Desktop** under **Sessions > Appliance Mode**.
2. Enter the **Virtual Desktop delivery server URL**.
3. Enable **Smartcard Login**.
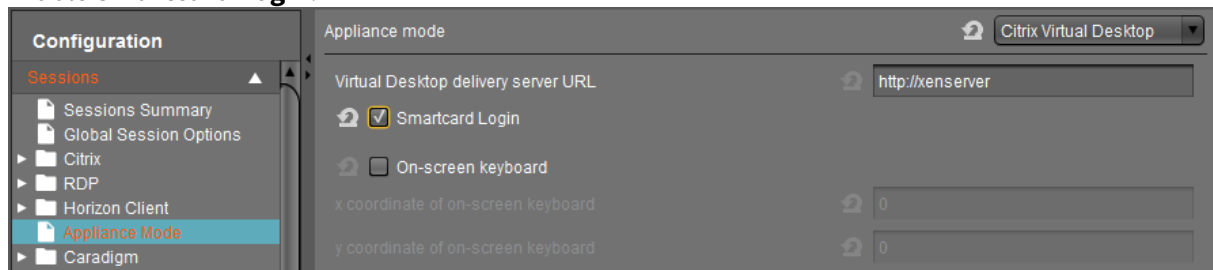
Desktop and Display

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])
```

IGEL

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**.
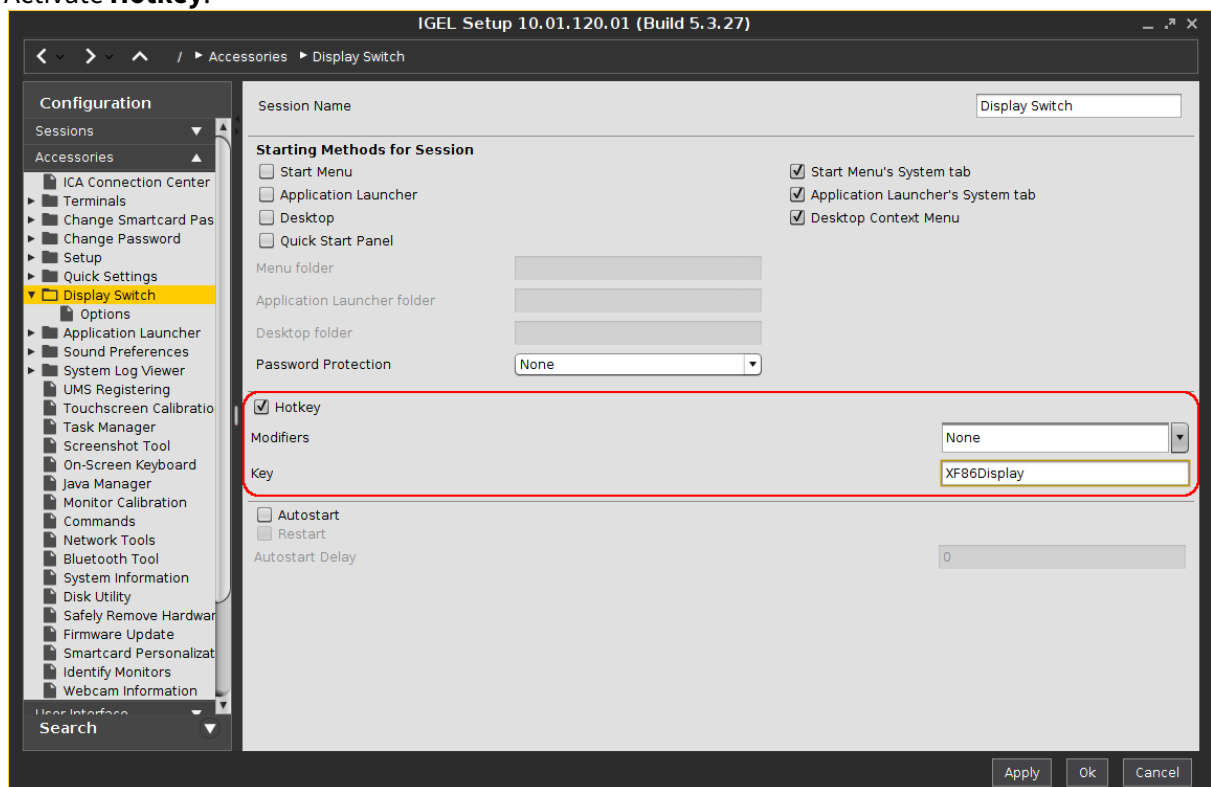
By default, [Fn]+[F7] (`XF86Display`) is defined as the hotkey for starting the display switch. You can change the hotkey by selecting or entering different keys in **Modifiers** and **Key**.

> ⓘ 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**.
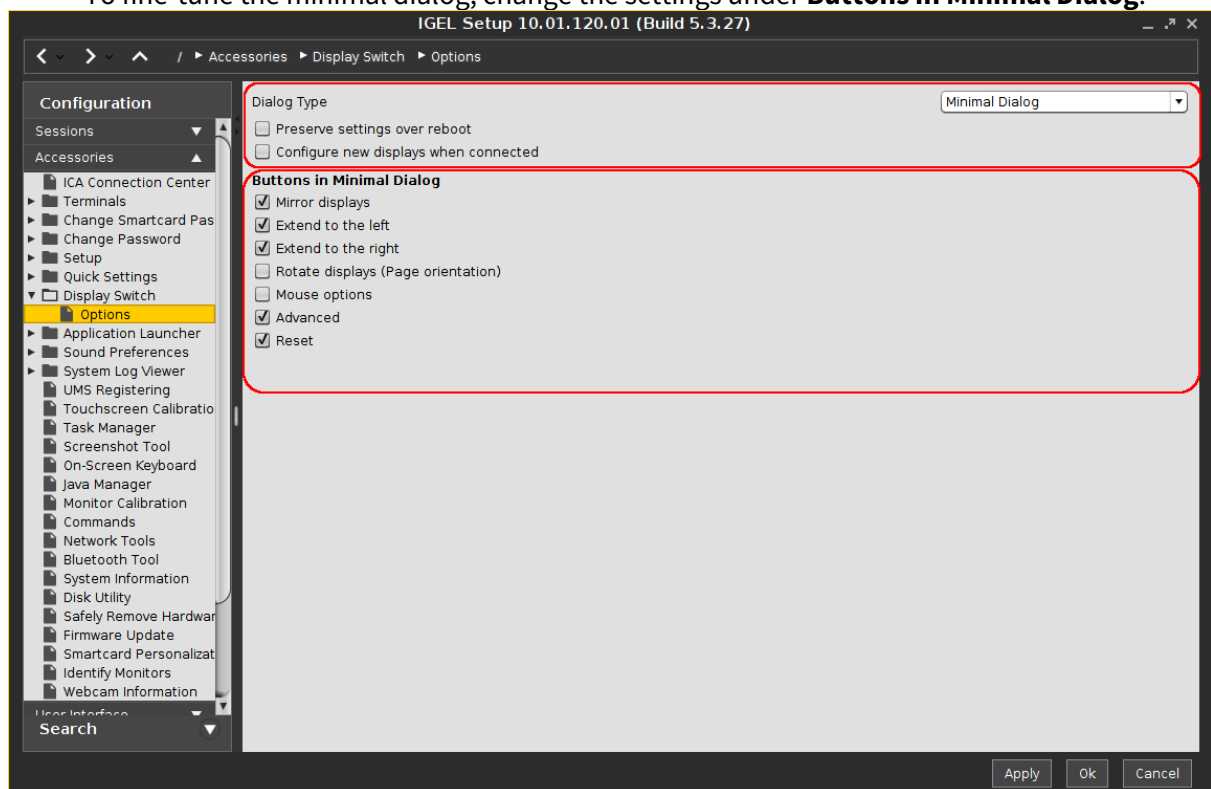
Use the Display Switch

The minimal dialog will look similar to this; details depend on your specific setup:

IGEL
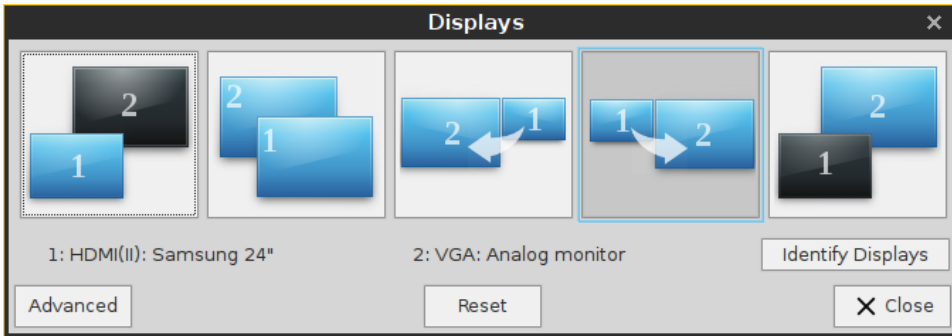
Button	Function
Identify Displays	Starts the monitor detection.
	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the right.
	Extends the display area to the screen on the left

	Uses only display 2.

For more information, see the manual chapter Using Display Switch.
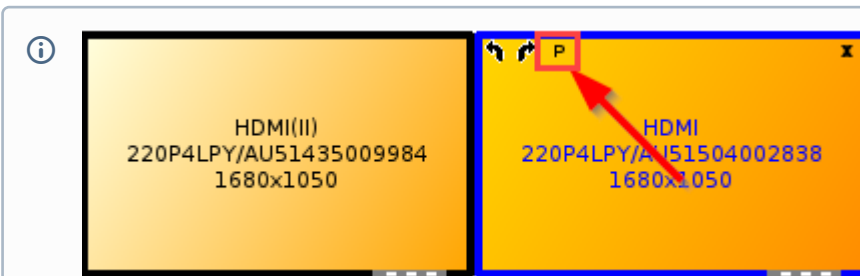
The **P** marks the **primary Display.**

IGEL

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 332)
- Manual Configuration (see page 334)
- Additional Settings (see page 336)
- Auto Switch Monitor Configuration for Laptops (see page 341)

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.

> (i) 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[28] for supported graphic cards.

---

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

IGEL

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**.
   A yellow and a white rectangle for the primary and secondary screens will be shown:
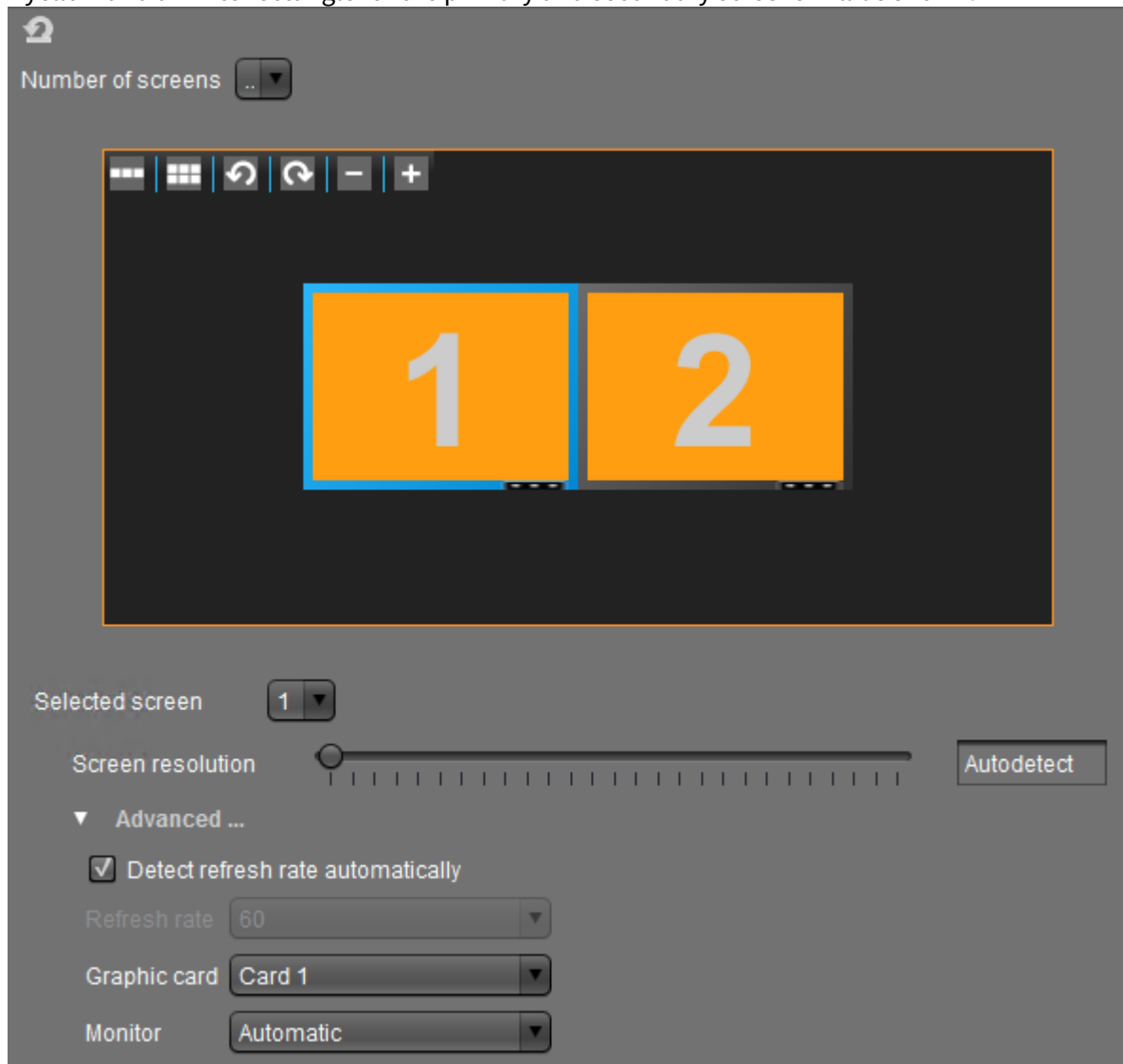
Autodetect Resolution: The operating system reads out the EDID (Extended Display Identification Data) of the monitors through DDC (Display Data Channel). With these data, the correct resolution for the monitors can be recognized and set.
Automatic Monitor: Automatic assignment of the screen to the graphic connector (monitor).

3. Drag and drop the rectangles to position the screens.
   By default, the primary screen is the one where the taskbar is situated.

> ⓘ If the **Autodetect** resolution is not available check the **DDC Option** under **User interface > Display > Options**. The **DDC Option** must be enabled (default setting).

Manual Configuration

During automatic configuration, the following problems can sometimes arise:

- One of the screens remains black.
- There is the same display on all screens.

In this case, you can set the screens manually:

1. Go to **User Interface > Display** in the structure tree.
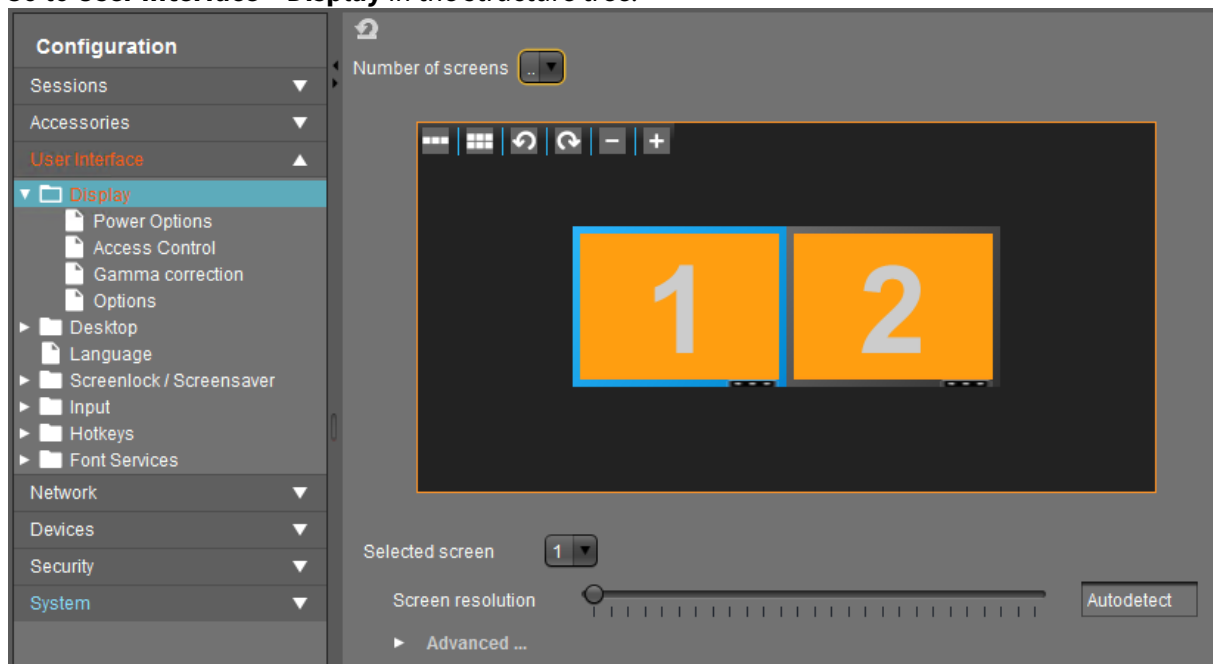
2. Select a screen number under **Selected screen**.
3. Specify the resolution manually under **Resolution**.

> ⓘ 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 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 **Identify monitors** 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:

IGEL
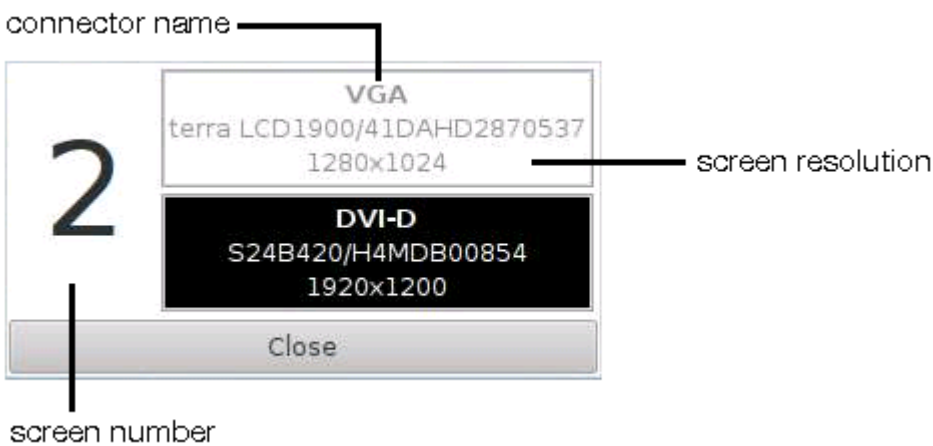
Additional Settings

A number of useful tips are provided below:

- Rotating a Screen (Pivot)
- Setting Different Backgrounds
- Useful Window Settings

Rotating a Screen (Pivot)

1. Click on a monitor field.
2. Select ⟲ **(Rotates the selected screen counterclockwise)** or ⟳ (Rotates the selected screen clockwise).

> ⓘ Two screens with autodetected resolutions are automatically aligned to the top.

▶ **Alignment**: If you enter the correct resolution, you can see the real size of the screens and you will be able to align them the way you want.

> ⓘ The individual screen areas must however be in contact with each other at one edge and corner, and cannot overlap.

Setting Different Backgrounds

You can easily set different backgrounds for your screens.

▶ Click **User Interface > Desktop > Background** in the structure tree of the setup.
There is a configuration page for each screen.
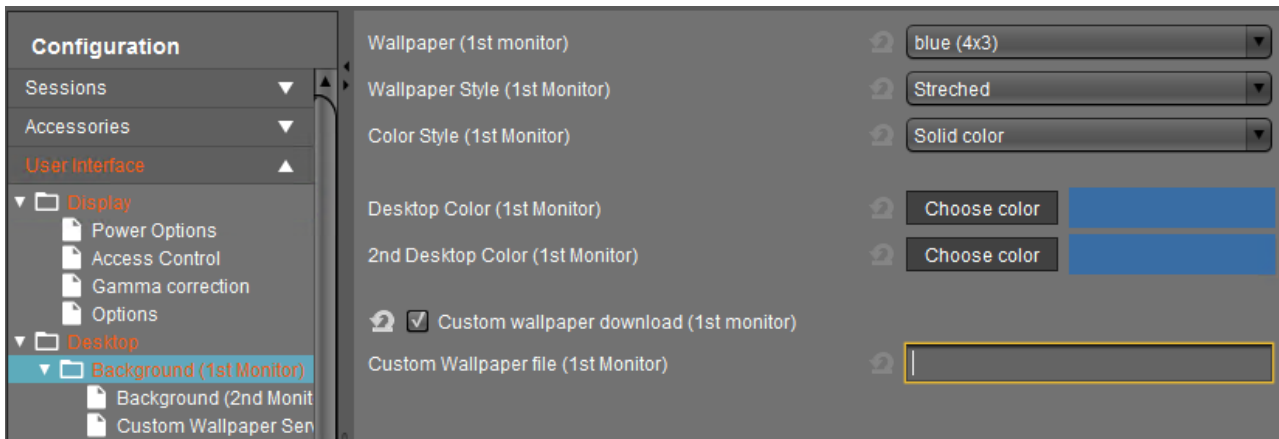
▶ Select the wallpaper and define the style.

ⓘ You may also upload your own **Custom Wallpaper**, e.g. a background with your corporate design. See Creating Your Own Wallpaper (see page 388).

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**.
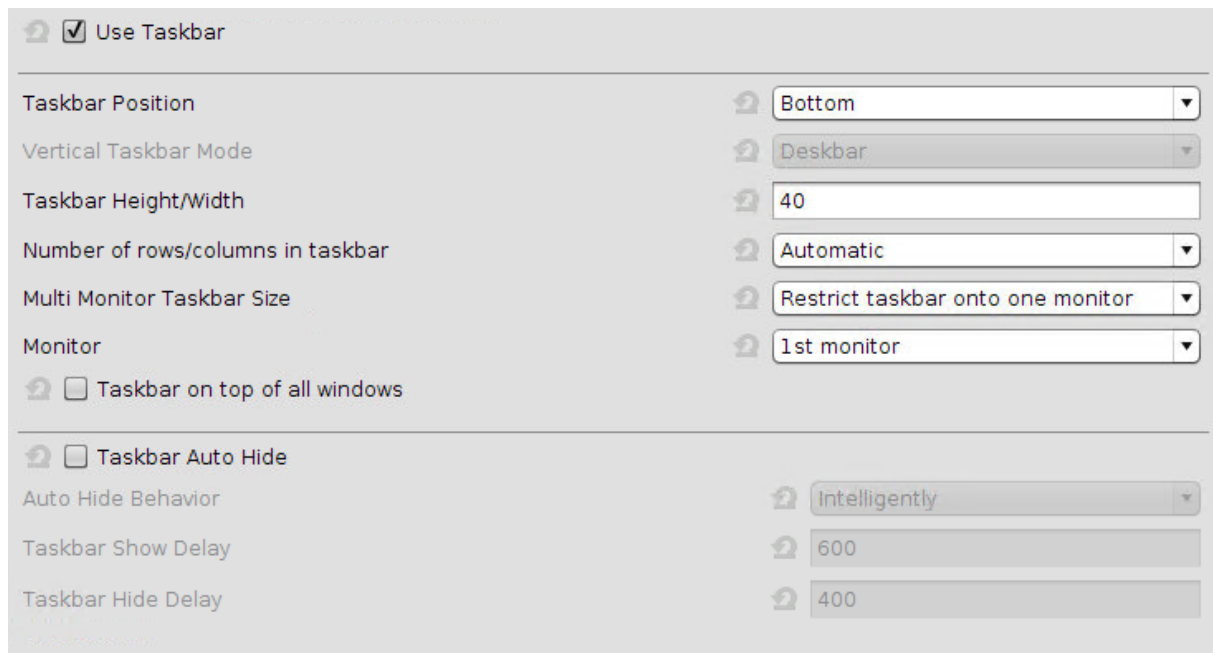
Setting the Multimonitor Full-screen Mode

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 Laptops

This ist one example of how to configurate auto switch monitor for Laptops

1. Connect the Hardware and close/open lid
2. Open the Display Switch Utility
3. You can Drag & Drop the Displays for your intended configuration.
   The display will snap adjacent to others.
4. If a display should not be used, it can be dragged to the **disabled** area on the top right - the screen will be reactivated when it is dragged back to the active area.
5. To show the same content on multiple displays, one display should be dragged onto an other active screen.
   The interface will show **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.
   You can configure advanced functionality (e. g. panning, scalling and resolutions) in drop-down boxes (hidden in a drawer on the right side)
   - Klick the **>** button on the right edge.
8. Go in IGEL Setup under **Accessories > Display Switch > Options.**
9. Enable **Preserve settings over reboot** and **Smart display configuration.** (Default: disabled)
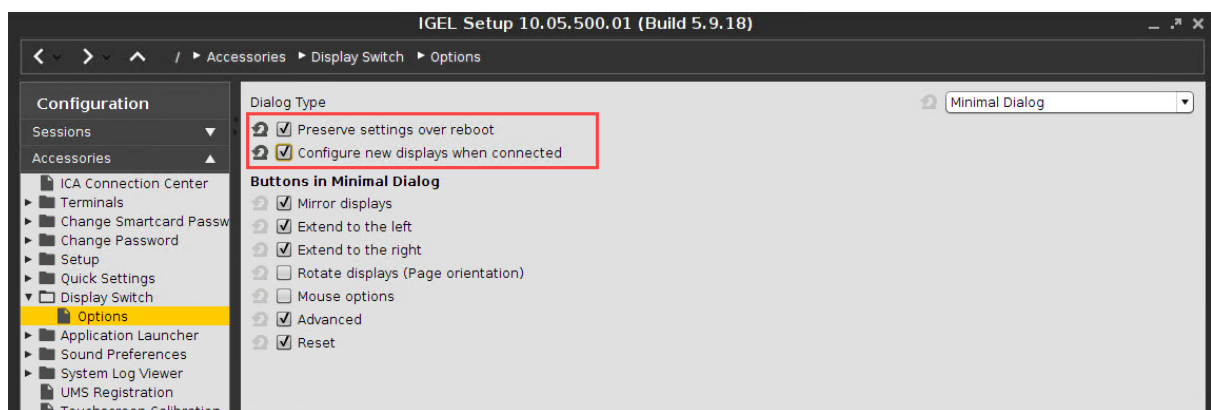
10. The IGEL Display Switch utility is now used for NVIDIA graphic devices as well.

Configuration of the display setting for Notebook lid handling

You can configure the lid handling of a notebook so that the notebook goes into standby mode by closing the lid, regardless of whether the notebook is plugged in or not.

Settings of the Standby Mode

If you want your notebook to go into standby mode by closing the lid, while your notebook is plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > ac**

2. Set **Lid close action while plugged in** to **Suspend** (Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting

If you want your notebook to go into standby mode by closing the lid, while your notebook isn't plugged in, you have to do following setting:

1. Go under **IGEL Setup** to **System > Registry > system > actions > lid > battery**
2. Set **Lid close action while not plugged in** to **Suspend** (Default: Turn off display)
3. Click **Apply** or **Ok** to save the setting

ⓘ If you want that the notebook **turn off display** after closing the lid, it makes sense to set the following setting to switch off the notebook internally:
   1. Go under **IGEL Setup** to **System > Registry > sessions > user_display0 > options > lid_events.**
   2. Enable **React on lid open and close event.**
   3. Click **Apply** or **Ok** to save the setting.

IGEL

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**

IGEL

Overcoming the Restrictions of a Full-Screen Session with the in-Session Control Bar

Running a session in full-screen mode gives you the advantage that the complete real estate of your monitor is at the disposal of that session. However, you might still want to eject a hotplug drive, or to minimize or end the current session. The solution provided by IGEL Linux is called **in-session control bar**.

Activating the in-session control bar:

1. Open the Setup and go to **User Interface > Desktop > In-Session Control Bar**.
2. Activate **Use in-session control bar in all supported sessions** if you want to have an in-session control bar in all session types for which it is supported. If you want to have an in-session control bar only in sessions of certain types, activate the appropriate options, e.g. **Control bar for RDP sessions**.
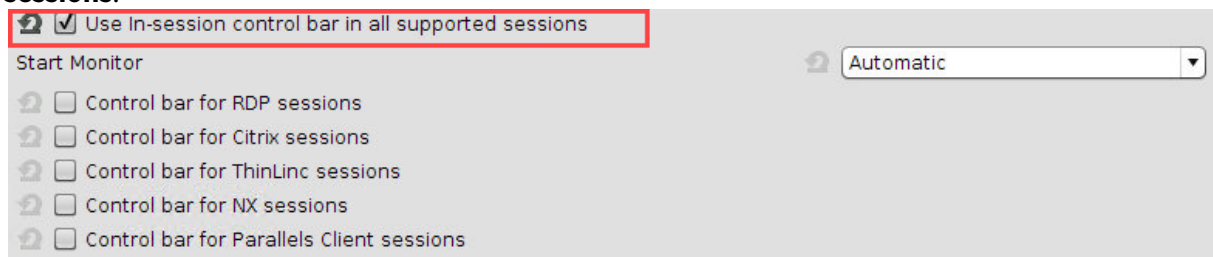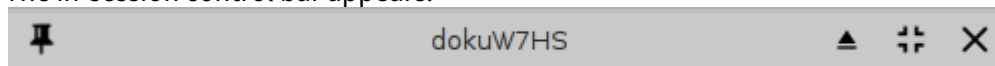

3. In the **Start Monitor** choice, select the display on which you want the in-session control bar to appear. If unsure, leave it at **Automatic**.
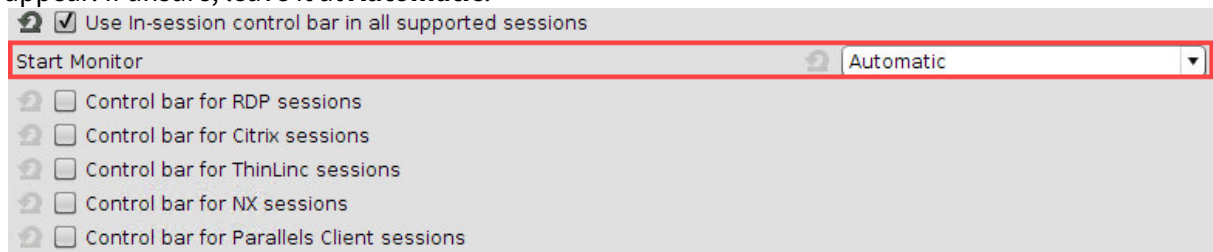

4. Click **Apply** or **Ok**.

Using the in-session control bar:

1. Move the mouse to the upper edge of the desktop.
   The in-session control bar appears.

2. To perform the desired action, click the appropriate icon:
   - To eject a USB device, click ⏏ .

- To minimize the session view, click ⸬ .
- To end the session, click ✕ .
- To make the in-session control bar visible permanently, click ⚲ .

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[29] apply.

---

29 https://www.igel.com/terms-conditions/

IGEL

Customizing

IGEL

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.

IGEL

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`.

IGEL

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.

IGEL

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.
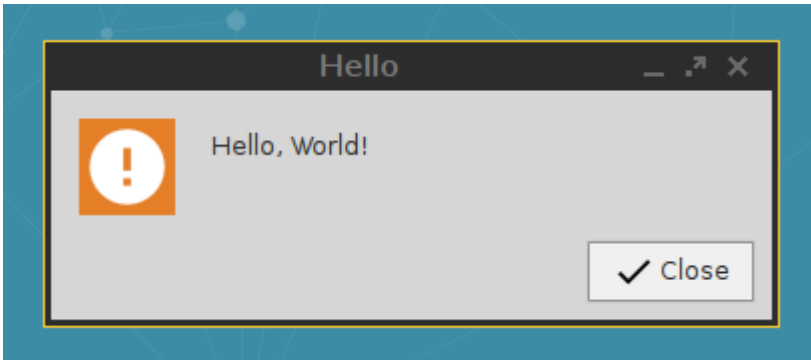
1. Log into **Local Terminal** as `root`.

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.

IGEL

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.
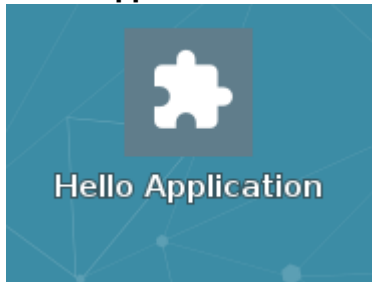
8. Double-click the icon.
   The message window should open.

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.

> (i) 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:

IGEL
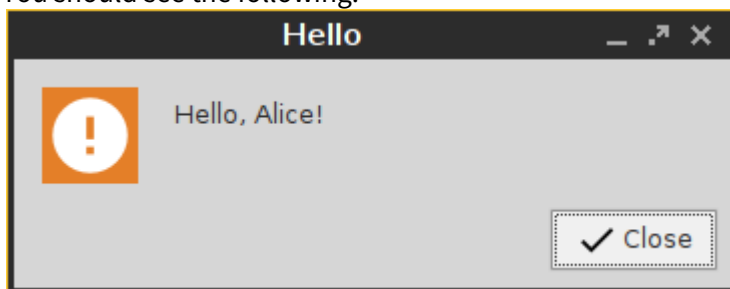
Packaging a Simple Custom Partition

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:
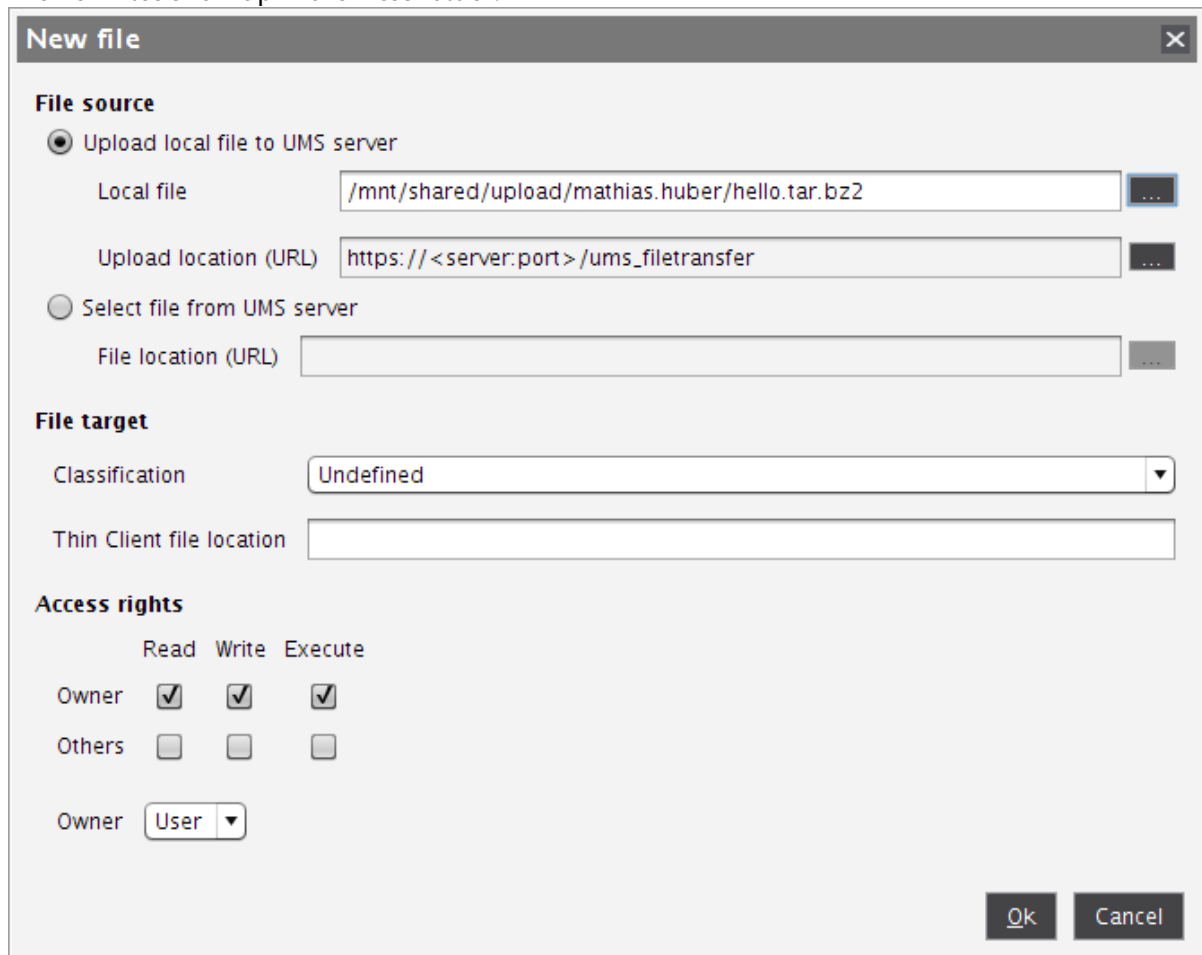
- **[INFO]**: Mandatory string
- **[PART]**: Mandatory string
- **file**: The filename of the `*.tar.bz2` archive
- **version**: The version of the contents, consisting of the vendor version (let's say this is hello 1.0) and the IGEL package version (the first package we produced of the software), joined 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

IGEL

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.

IGEL

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.
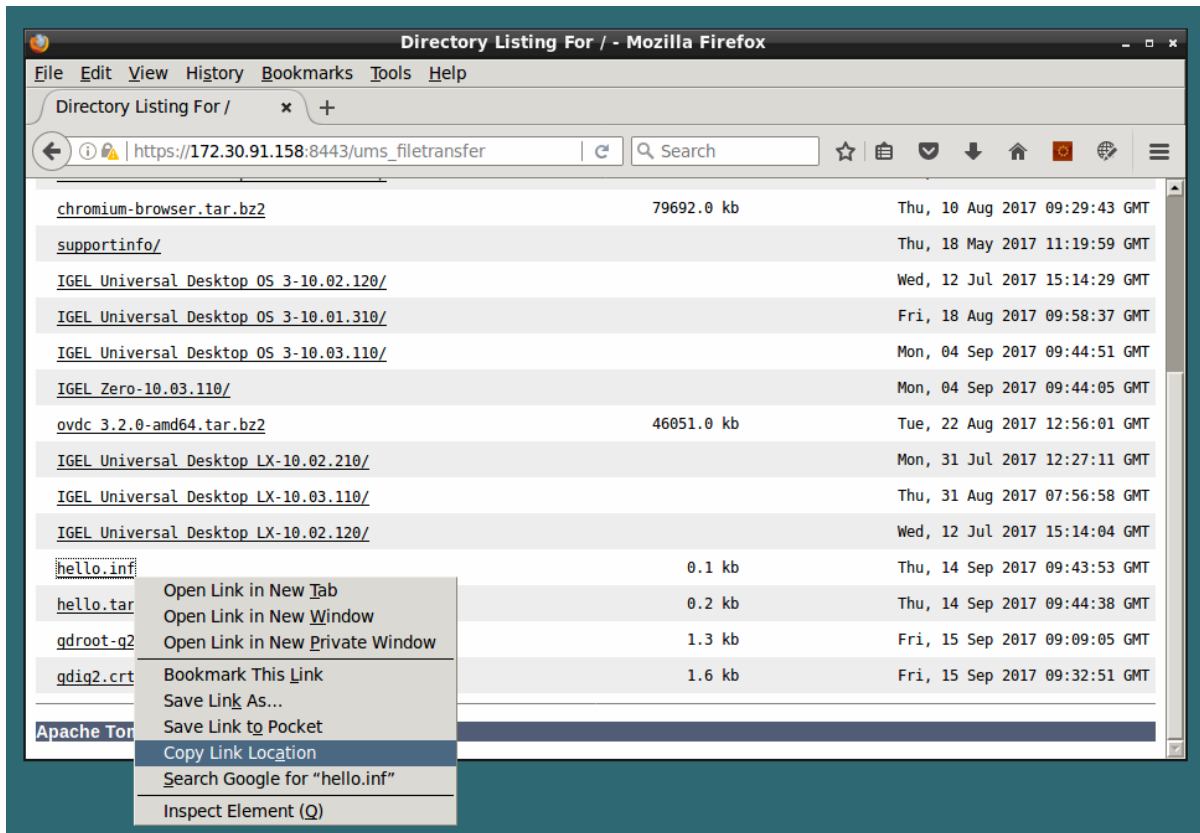
4. Right-click the `hello.inf` entry and select **Copy Link Location**.

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 .

IGEL

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.

_____

IGEL

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.[30]

---

[30] http://edocs.igel.com/11105.htm

IGEL

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] [Reset]
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.

IGEL

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.

IGEL

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   [Search] [Reset]
   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

IGEL

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`

IGEL

Providing Libffmpeg

To obtain Libffmpeg, repeat the process for obtaining Libatomic (see page 371). 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.
> - ...

IGEL

Chromium Starts Successfully

Now you are ready to give running Chromium another try. It does not like to be started by `root` , because it is much safer to run it as the non-privileged `user` .

1. Log into **Local Terminal** as `user` .
2. Change into the `/custom/chromium-browser` directory.
3. Enter the following command:
   `./usr/lib/chromium-browser/chromium-browser`
   Chromium starts for the first time. Congratulations, you now have working Chromium installation.
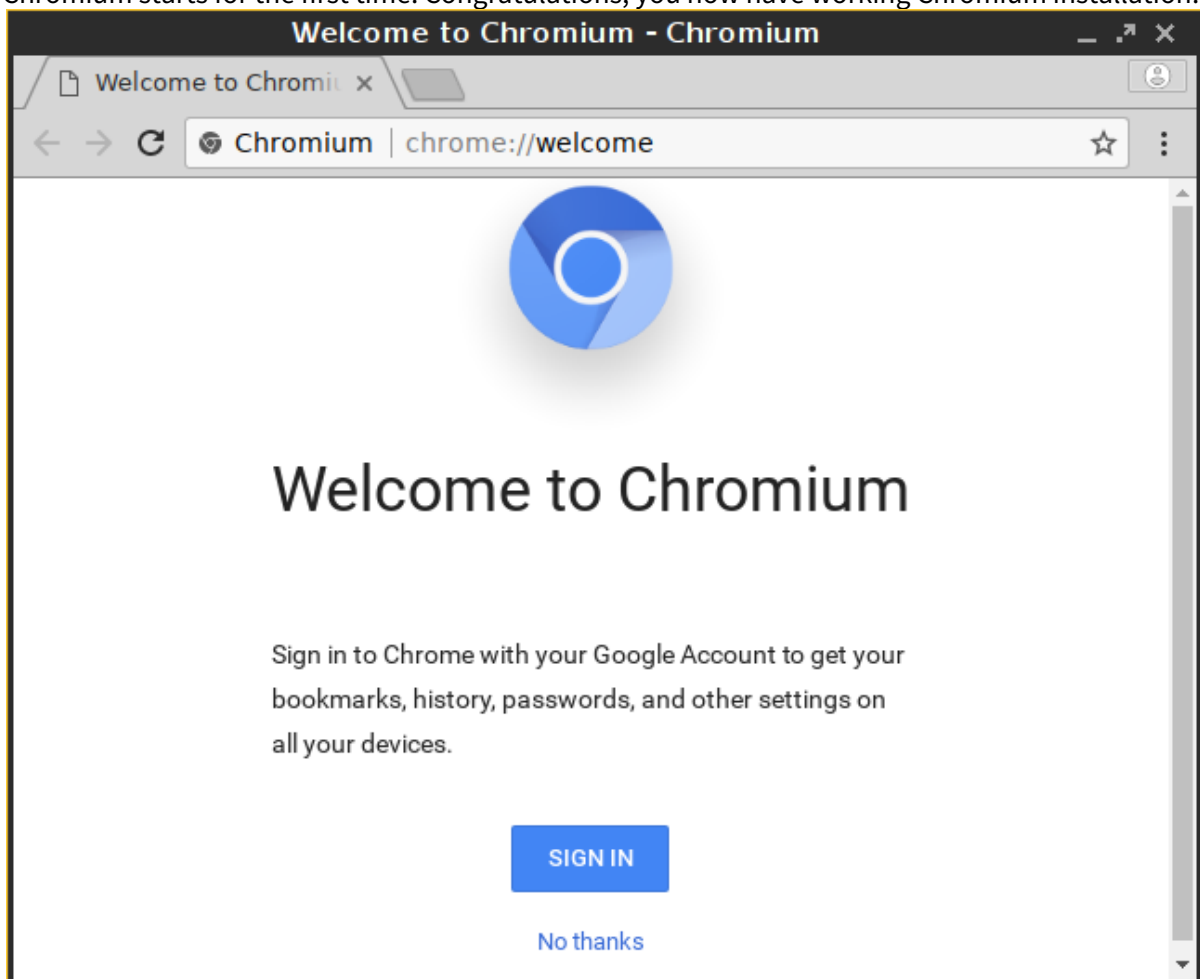
The next step will package the Custom Partition so it can be deployed to any number of thin clients from UMS:

Packaging the Custom Application

Now that the hardest part of creating the Custom Partition is done, package the CP for UMS. You are already familiar with most of the steps from earlier in this tutorial.

1. Compress the CP Contents (see page 357) into `chromium-browser.tar.bz2`
2. Upload the compressed file to UMS as a new **File**.
3. Write the *.inf Metadata File (see page 358) 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 360) 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 353) with the **Command** set to:

   `/custom/chromium-browser/usr/lib/chromium-browser/chromium-browser`
7. Assign the CP to a new thin client in order to test everything.

Advanced

Here are some advanced topics for you to try after you have completed this tutorial.
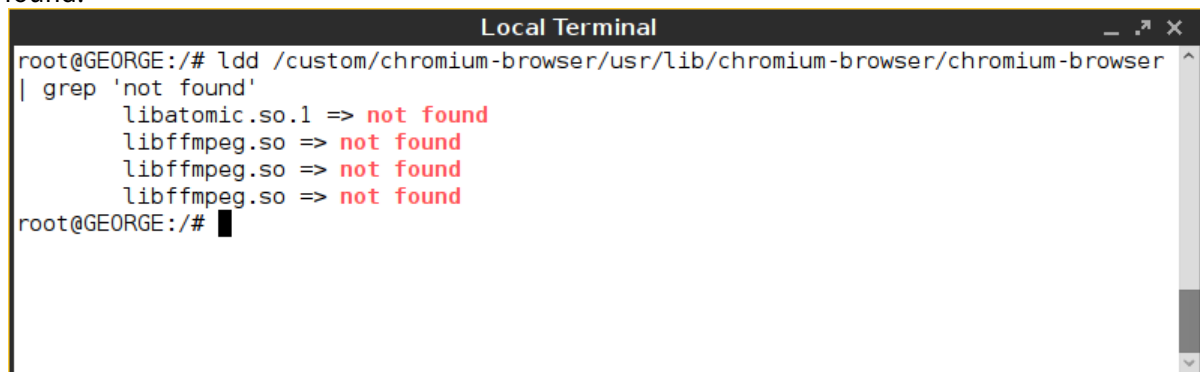
Using ldd to Find Required Libraries

Using the `ldd` command is another way of determining the libraries that a binary requires.

1. Log into **Local Terminal** as `root`.

2. Find out which file the main binary of the Custom Partition is. It is usually found in `bin/`, `usr/bin/` or `usr/lib/` and is named similar to the application name.

3. Run the following command:

   ```
   ldd /custom/[name]/[binary] | grep 'not found'
   ```

   This command line contains a filter, so that it will only show you those libraries that could not be found.

Auto-updating Custom Partitions

The Custom Partition mechanism in IGEL OS can update the Custom Partition contents automatically when a newer version is available on UMS. To activate it, follow these steps:

1. In Setup, go to **System > Firmware Customization > Custom Partition > 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.

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 348).
>
> 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`

IGEL

Adding an Icon for Browsing Removable Storage

Symptom

There is no obvious way of viewing files from removable media locally on the thin client.

Problem

You want to view files from removable media locally on the thin client.

Solution

Create a custom application that opens the contents of removable media in the **File Manager**.

1. Go to **System > Firmware Customization > Custom Application** in **Setup**.
2. Click the star symbol to create a new **Custom Application**.
3. Enter a name, e.g. *Removable Media*, and choose desktop integration options for the application.
4. Enter `folder` as the **Icon name** and `thunar` as the **Command** in the **Settings** dialog:
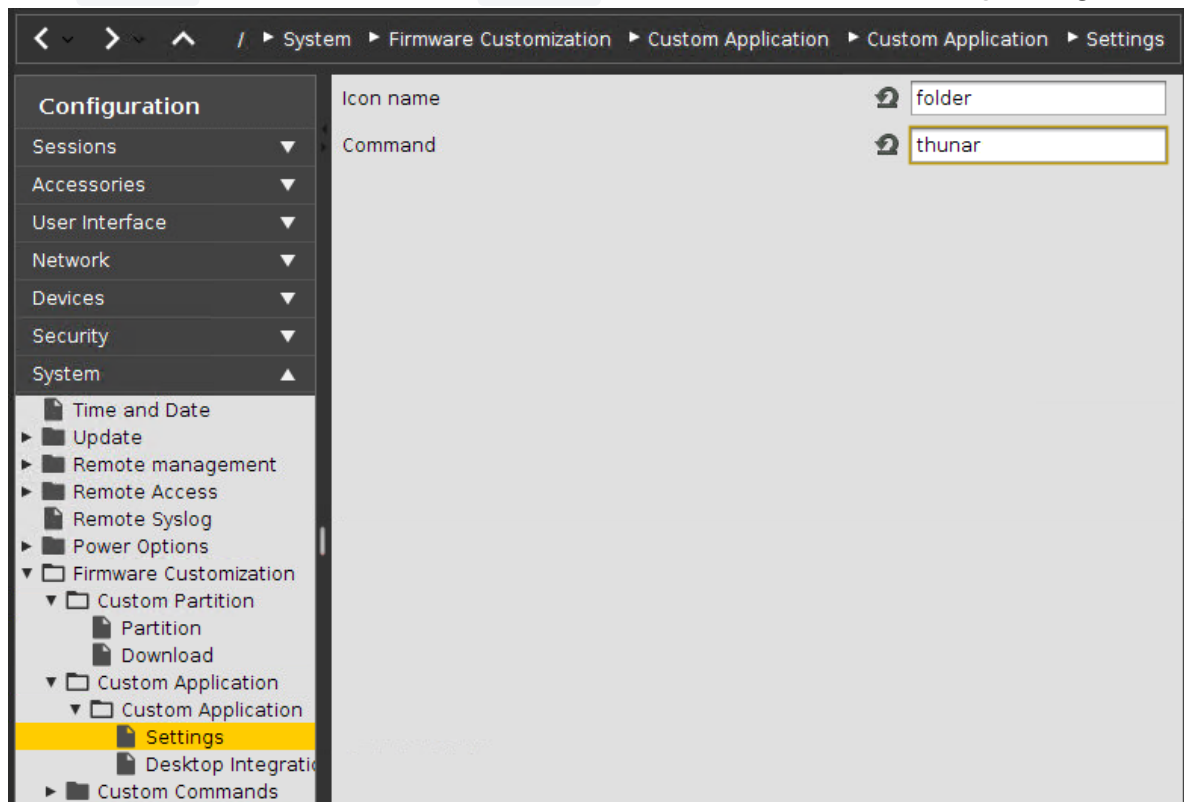
5. Save the settings.

6. Insert a removable medium such as a USB stick into the thin client.
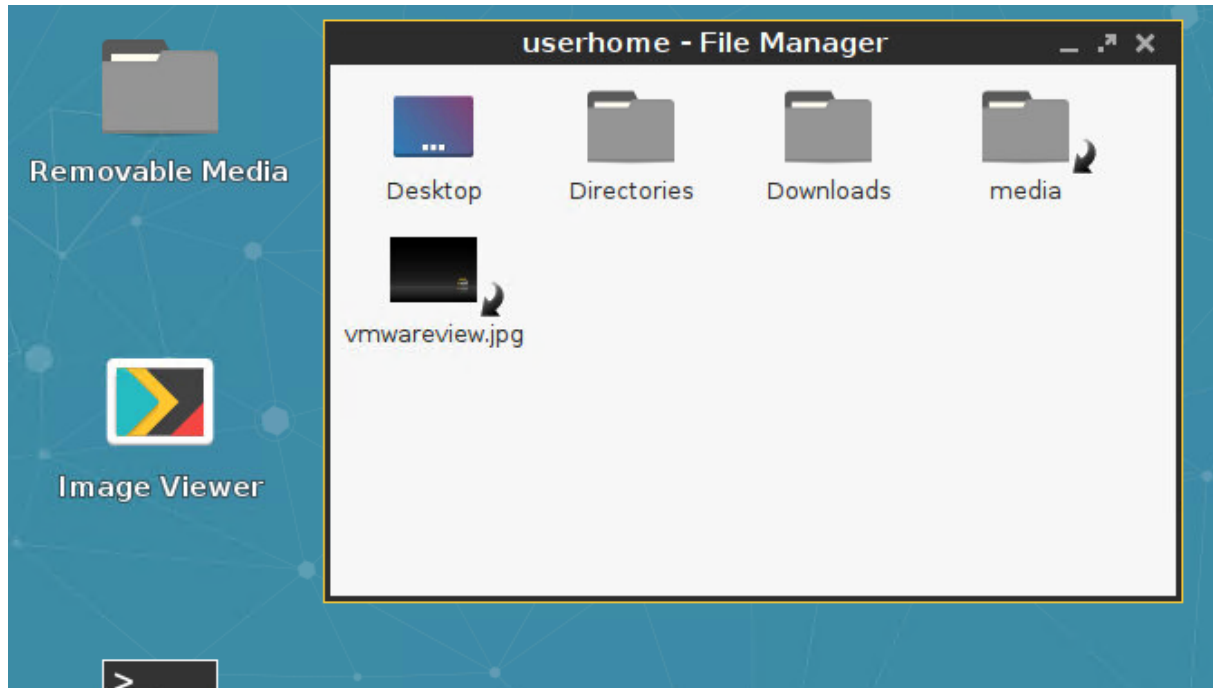
7. Click the new **Removable Media** icon. This opens **File Manager** and lets you browse the contents.
   Clicking a file will open it in the application configured by the MIME type handler (as of IGEL LINUX
   5.06.100, see FAQ (see page 426)).

Adding an Icon for the Image Viewer

Symptom

You want to view images locally on the thin client.

Problem

The image viewer contained in *IGEL Linux* as from version 5.06.100 on has no desktop icon or menu entry.

Solution

Create a custom application that opens the Image Viewer.

1. Go to **System > Firmware Customization > Custom Application** in Setup.
2. Click ⊞ to create a new **Custom Application**.
3. Enter a name, e.g. *Image Viewer*, and choose desktop integration options for the application.
4. Go to **Image Viewer > Settings**:
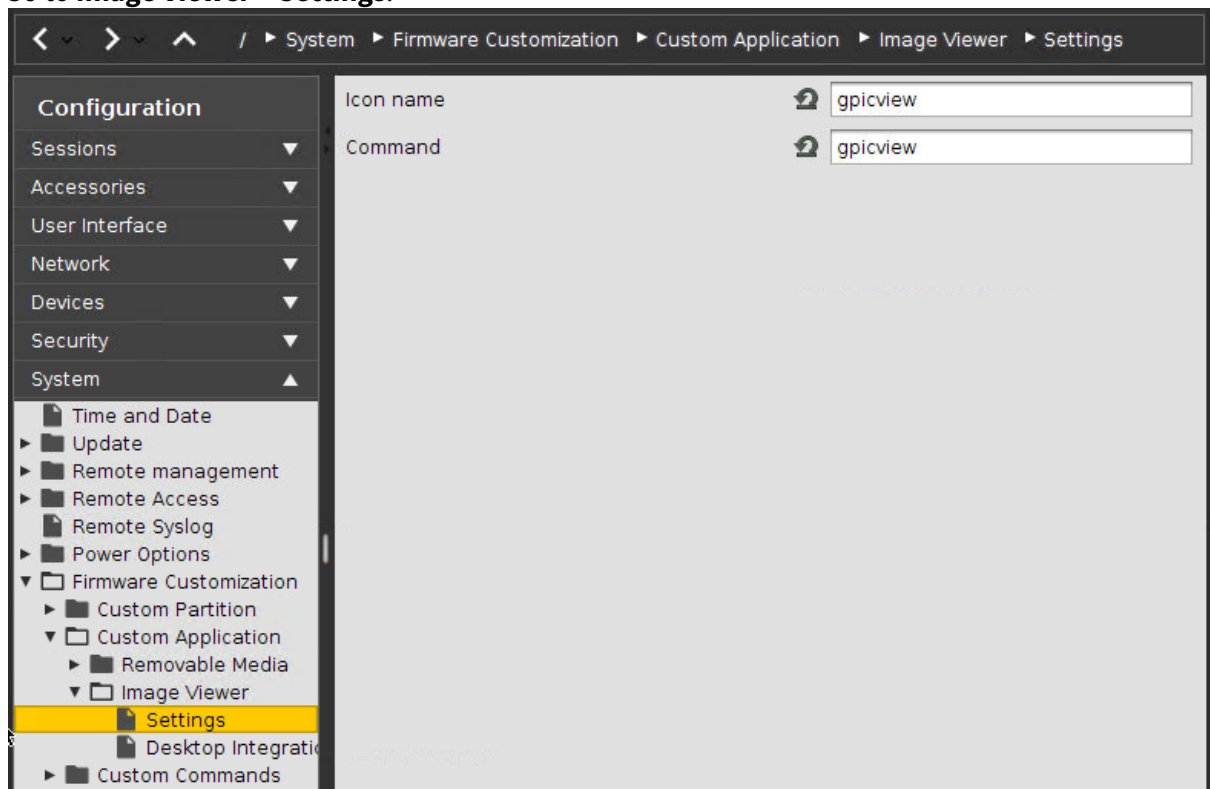
5. Enter `gpicview` as both the **Icon name** and the **Command** in the **Settings** dialog.
6. Save the settings.

7. Click the newly created icon for **Image Viewer**.
8. The **Image Viewer** opens.
9. Click the **Open File** symbol to open a file.
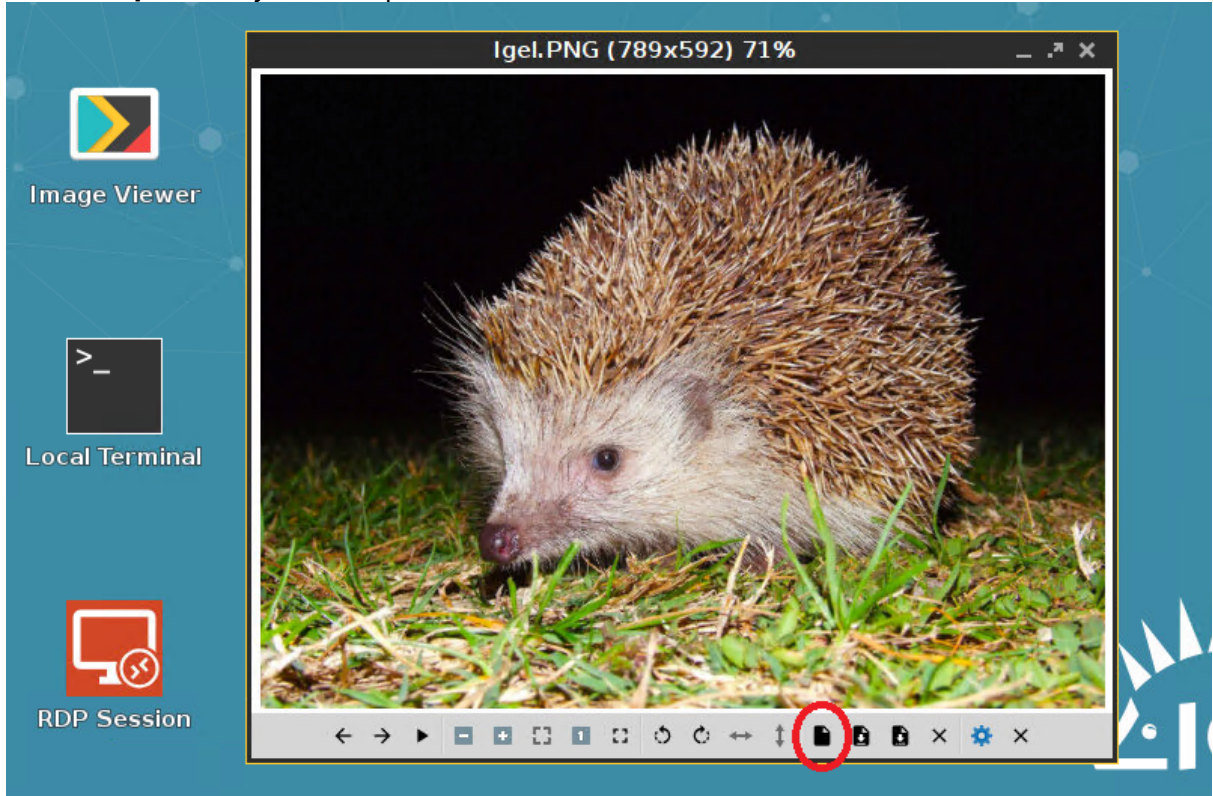
IGEL

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 389). See also Firmware Customizations and Create Firmware Customization in the UMS Reference Manual.

For information on customizing IGEL OS desktops via a profile, see:

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

IGEL

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
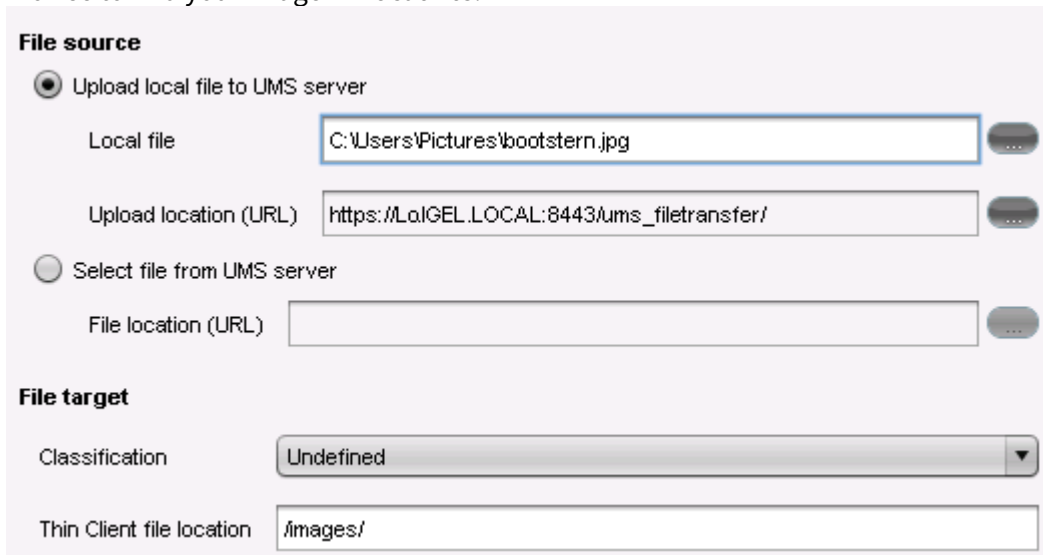- Creating a Profile

Uploading a Picture

Upload your image files to the UMS server, then assign them to the relevant profile and also to your devices.

You can choose between the following formats for your pictures : **BMP, JPG, GIF, TIF, PNG** and **SVG**. Ensure that the name of your image file has no blanks, otherwise the file will not be accepted. **25 MB** of free storage space are available for your pictures.

Upload your files:

1. Click **New file** on the context menu of the **Files** directory in the tree.
2. Browse to find your image in **Local file**.

3. Browse to select a picture directory in **Upload location (URL)**.
   Since UMS version 5 you can use as upload location only /ums-filetransfer/ and its subdirectories.
4. Enter a **Thin Client file location** directory for the target device.
   If you enter a directory which does not yet exist, it will be created automatically. If you do not enter a specific directory, the image will be put in the root directory.
5. Click **OK**.
   Your image will be listed in the list of **Files**.
6. Assign the image to your devices by dragging and dropping them or by adding them under **Assigned objects**.

> ⓘ If you put more than one image in the **Thin Client file location** directory, all images will be alternately shown by the screensaver (see page 394), one after the other.
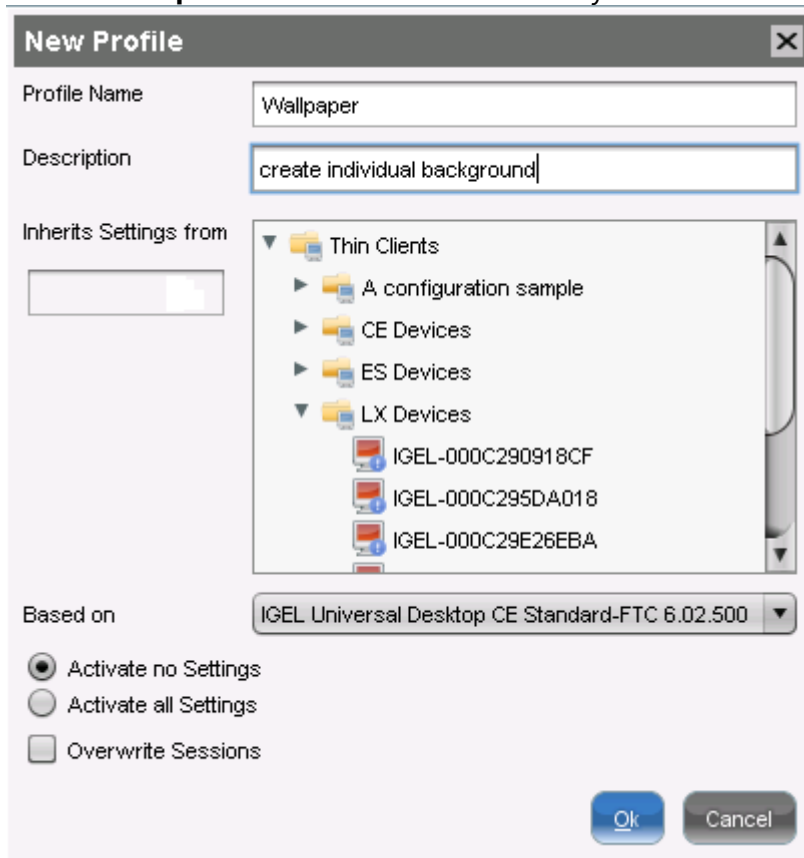
IGEL

Creating a Profile

You have already uploaded your image file .

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**.

4. Click **OK**.

Creating Your Own Wallpaper

There are two ways how to create an own wallpaper:

- Via a Firmware Customization (see page 389)
- Via a Profile (see page 390)

With a Firmware Customization, setting up your own wallpaper is much easier than with a profile.

IGEL

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.
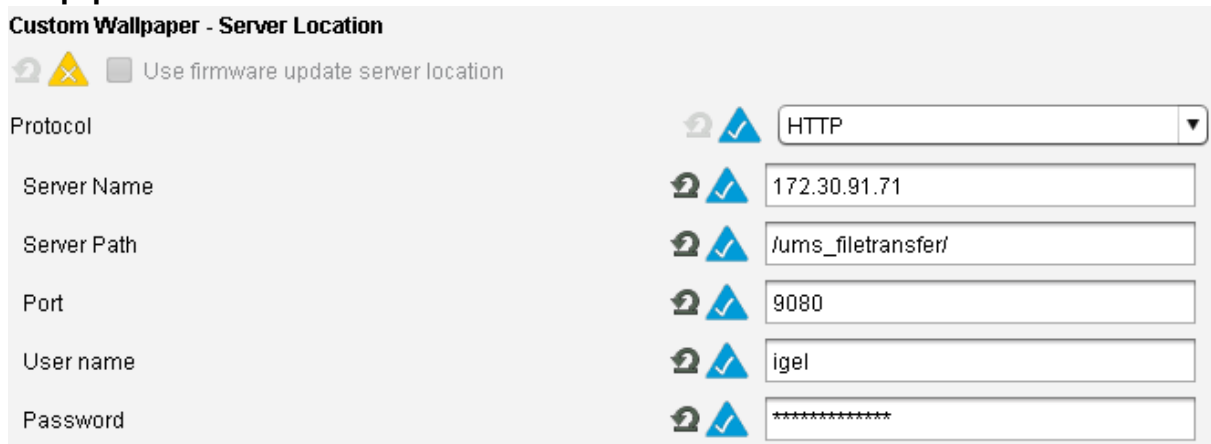8. Click **Finish** to save your new firmware customization.

IGEL

Creating Your Own Wallpaper via a Profile

You have already uploaded your wallpaper picture; see Uploading a Picture (see page 386).

1. Create a profile and name it, for example, **Wallpaper**; see Creating a Profile (see page 387).
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 386).
2. Create a new profile named **Bootlogo**; seeCreating a Profile (see page 387).
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

IGEL

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**.

IGEL

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 386).

   ⓘ 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 387).
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 395)
   - Setting a Timeout for Autostart (see page 396)
   - Assigning the Custom Logo (see page 397)
   - Assigning the Custom Clock (see page 398)
4. Assign the profile to your devices by dragging and dropping them or by adding them under **Assigned objects**.

IGEL

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.

IGEL

Setting a Timeout for Autostart

1. Click **User Interface > Screenlock / Screensaver > Options**.
2. Enable **Start automatically**.
3. Enter a number of minutes for **Timeout**.

> (i) 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 386).

   > ⓘ 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.

IGEL

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.

IGEL

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 the start menu with a company logo, you first have to set the **Start Menu Type** to "Advanced" under **User Interface > Desktop > Start Menu**.
> If you set the **Start Menu Type** to "Auto" and the device has a clock frequency of 1 GHz, the system will select the "Advanced" type.
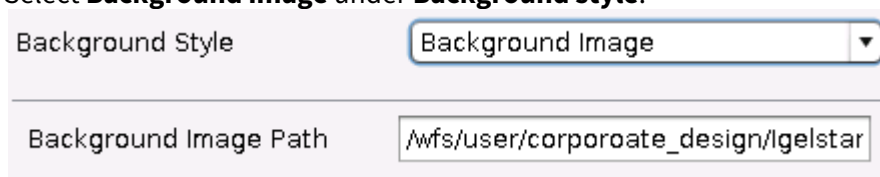
To assign your own icons via UMS:

1. Upload your logos to the UMS Server. For details, see Uploading a Picture .
2. Create a new profile. For details, see Creating a Profile .
   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.

IGEL

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 386).
2. Create a new profile, see Creating a Profile (see page 387).
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**.

IGEL

Customizing Desktop Icons

> (i) 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.

> (i) We recommend at least a resolution of 64x64.

- SVG - no resolutions because SVG contains freely scalable vector graphics.

> (i) 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**.

   > (i) For technical reasons, some registry keys do not match the session's name. For example, RDP sessions are found under the key `winconnect[0-...]`.

3. Enter under **Icon name** the absolute path to your custom icon as shown in the sample picture below.
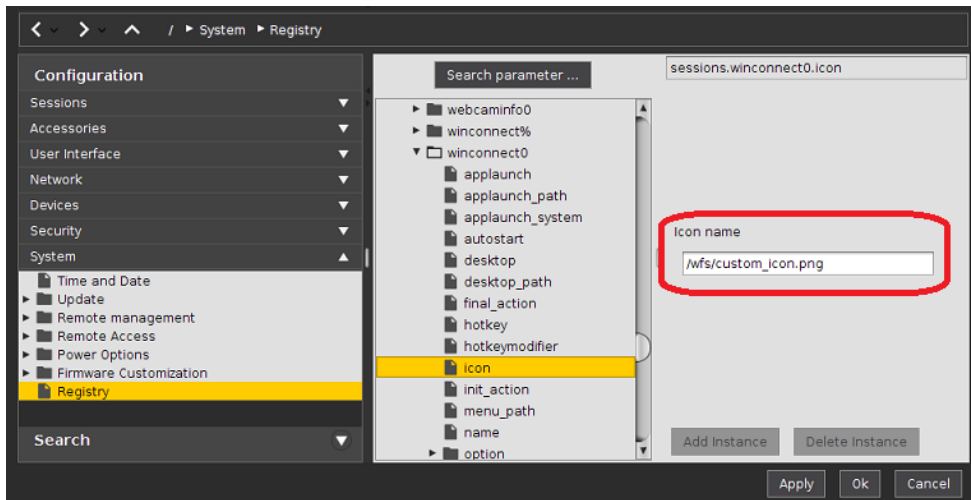
4. Click **Ok** to save the changes.

IGEL

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 403)
- Defining the Countdown's Appearance (see page 405)

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 407)
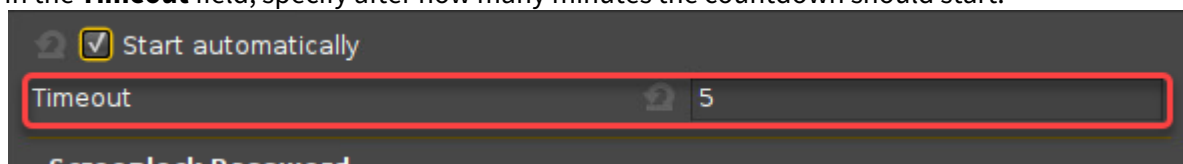

Defining the Countdown's Behavior

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**.

3. In the **Timeout** field, specify after how many minutes the countdown should start.
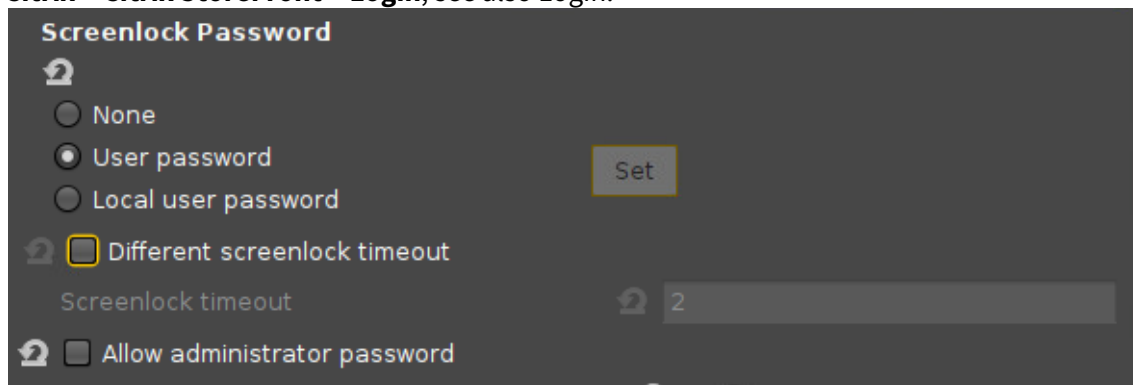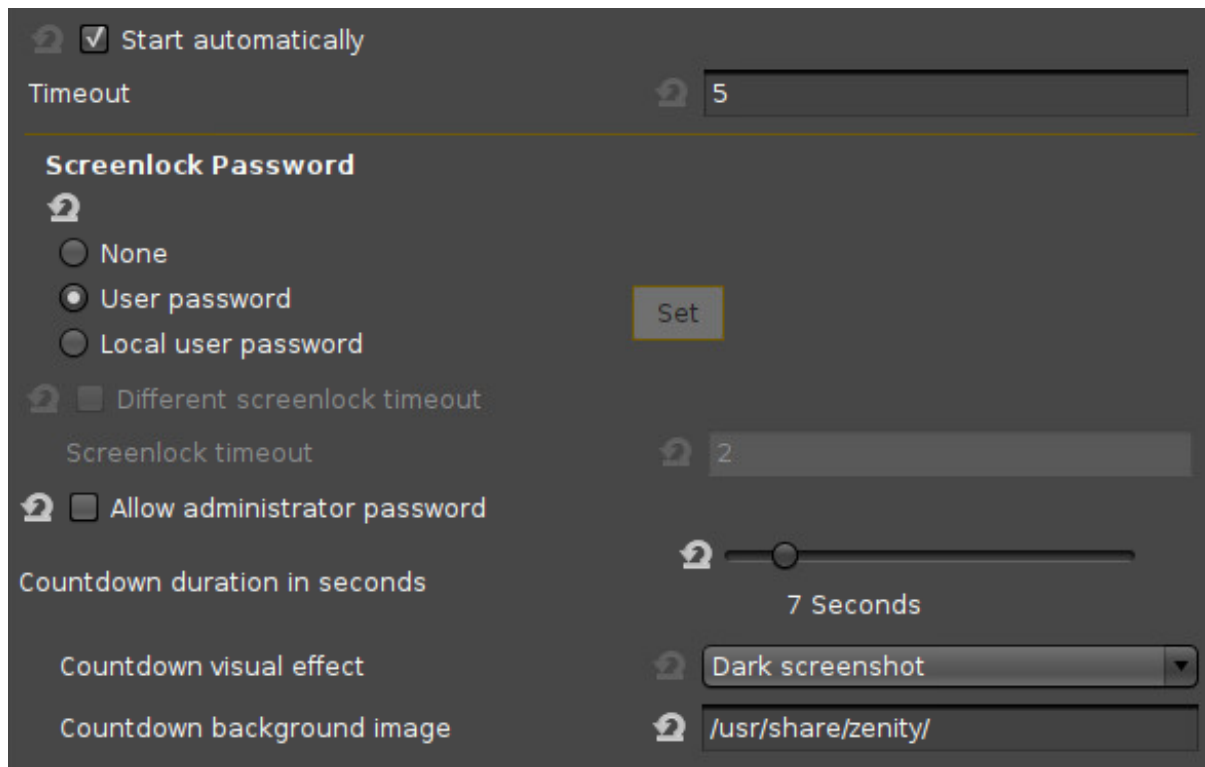
4. Select the password to be used to unlock the screen:
     • **None**: The user can unlock the screen without a password. Please note that the countdown will not be started when this option is selected!
     • **User password**: The user must enter the user password to unlock the screen. If you are using Microsoft Active Directory (AD) resp. Kerberos for authentication, which is highly recommended, the user's AD/Kerberos password will be used here. For details, see Active Directory/Kerberos. If you are not using AD/Kerberos, the user password is configured in **Security > Password** under **User**. Please note that the password should not, at any rate, be set via a UMS profile, otherwise all affected devices would have the same password!
     • **Local user password**: The user must enter a special screen lock password to unlock the screen; click **Set** to define this password. Please note that the password should not, at any rate, be set via a UMS profile, otherwise all affected devices would have the same password! This password is also used for **Security > Logon > Local User > Login with local user password**; see Local User (see page 403).
     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.
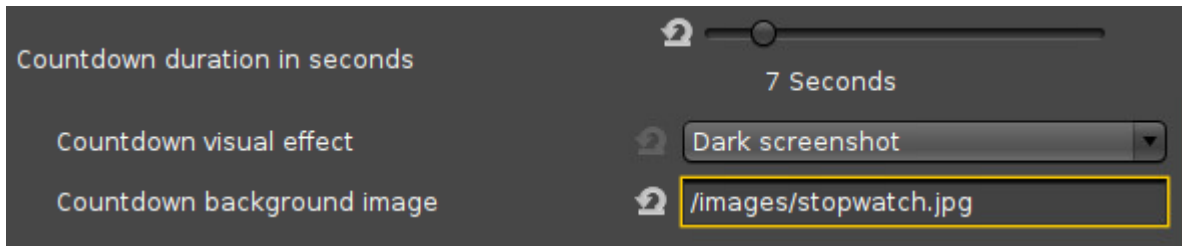

5. Set the **Countdown duration in seconds**. The range is from 1 to 60.
   Configuration example:

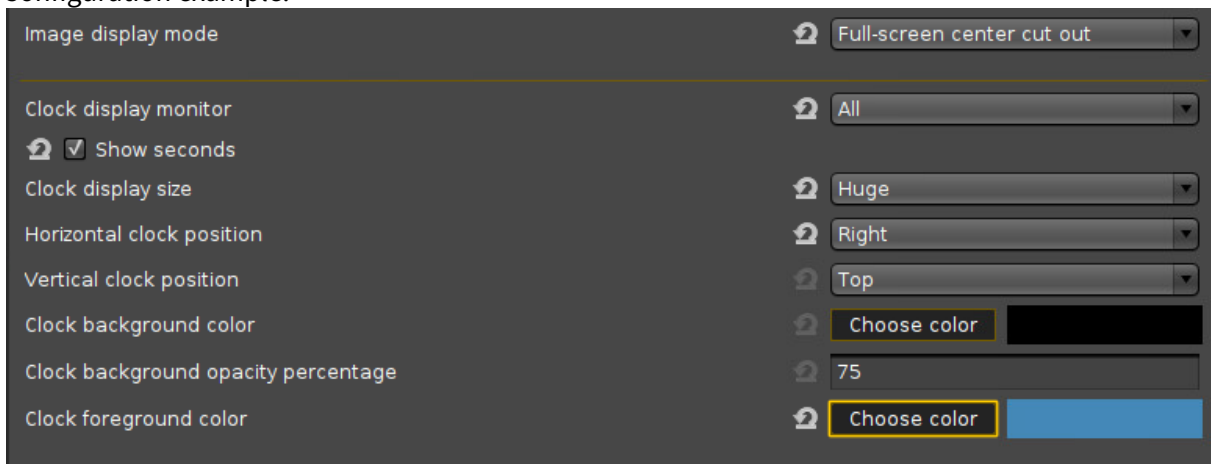6. Apply the settings to your devices or to your profile.

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 386).
   Configuration example with custom image:

4. Go to **User Interface > Screenlock / Screensaver > Screensaver**.

5. Customize the countdown's appearance using the following parameters; these parameters define the appearance of both the screensaver's clock and the countdown. For further information, see Screensaver.
    - **Image display mode**: Position and scaling for the background image
    - **Clock display monitor**: Select the monitor(s) on which the countdown is to be shown.
    - **Show seconds**: Define whether the seconds should be displayed on the clock.
    - **Clock display size**: Size of the countdown digits
    - **Horizontal clock position**: Horizontal position of the countdown digits
    - **Vertical clock position**: Vertical position of the countdown digits
    - **Clock background color**: Color of the countdown background area. The countdown background area is a rectangle with rounded corners.
    - **Clock background opacity percentage**: Set the opacity for the clock's background area (defined by **Clock background color**),
    - **Clock foreground color**: Color of the countdown digits

Configuration example:

6. Apply the settings to your devices or to your profile.
Here is an example of the countdown with a custom image:

Configuring a Conditional Countdown and Command

In our example, a Citrix session is running (e.g. in appliance mode), and the endpoint device has been idle for a while. After the timeout, the system checks whether a Citrix session is running; this is to prevent the session from running unattended. The Citrix session is detected, so the countdown kicks in. The user does not interact with the device, so the countdown is not stopped. When the countdown has reached 0, the system kills the Citrix client; the user is logged off.

In the following, we will first specify the command that determines whether the countdown should be started. Then, we will specify the command that is executed when the countdown has reached 0.

Command That Determines the Condition under Which the Countdown Should Be Started

> ⚠ This command only makes sense in combination with a command that is to be executed after the countdown is done; see .

1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown_condition_cmd**
(`sessions.xlock0.options.countdown_condition_cmd`).

2. Enter the command in the field **Countdown condition command**. The user that issues the commands is `user` . If no command is defined here, the countdown will be started. Examples: `pgrep wfica` (returns 0 if a Citrix session is present), `pgrep igelrdp2`
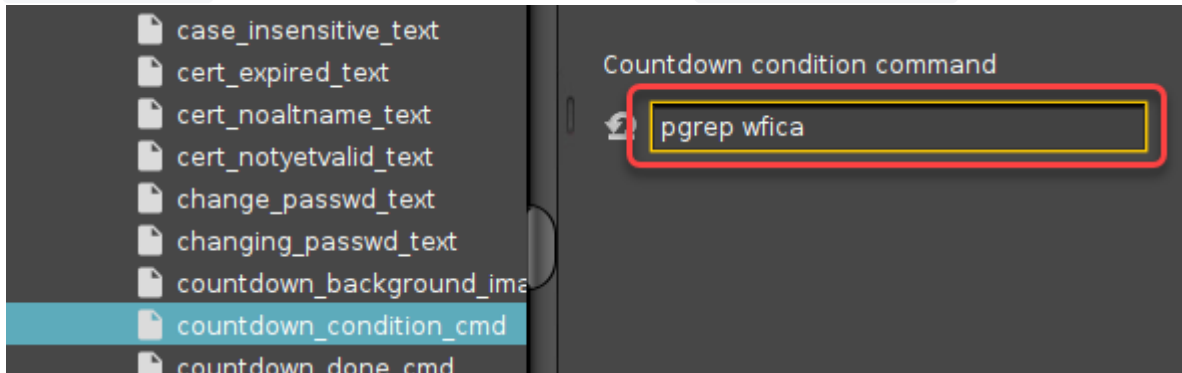


3. Click **Apply** or **Ok**.
   If the command returns 0, the countdown is started. When the countdown has reached 0, the command specified with **System > Registry > sessions > xlock0 > options > countdown_done_cmd** is executed (see Command to Be Executed after the Countdown (see page 408)).
   If the command returns a non-zero value, the countdown is not started. A command that is configured for execution after the countdown will therefore not be executed. The screen lock or screensaver will be started.

## Command to Be Executed after the Countdown

1. In the Setup, go to **System > Registry** and open the registry key **sessions > xlock0 > options > countdown_done_cmd** (`sessions.xlock0.options.countdown_done_cmd`).

2. Enter the command in the field **Countdown done command**. The user that issues the commands is `user` . Examples: `killall wfica` (terminates the Citrix ICA client), `logoff`

> ⓘ The command is executed synchronously before the countdown goes away. If the command doesn't terminate quickly, it must be sent to the background by appending " & ".
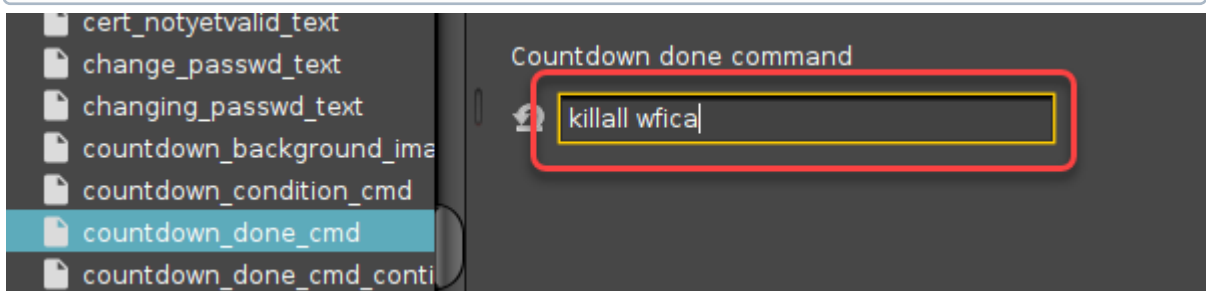
3. (Optional) If you want to enforce the start of the screensaver after the **Countdown done command** has been executed, open the registry key **sessions > xlock0 > options > countdown_done_cmd_continue**

(`sessions.xlock0.options.countdown_done_cmd_continue`) and enable **Continue screensaver after countdown done command**.

> ⓘ Some applications stop the screensaver when they get restarted, so this does not always have the desired effect.
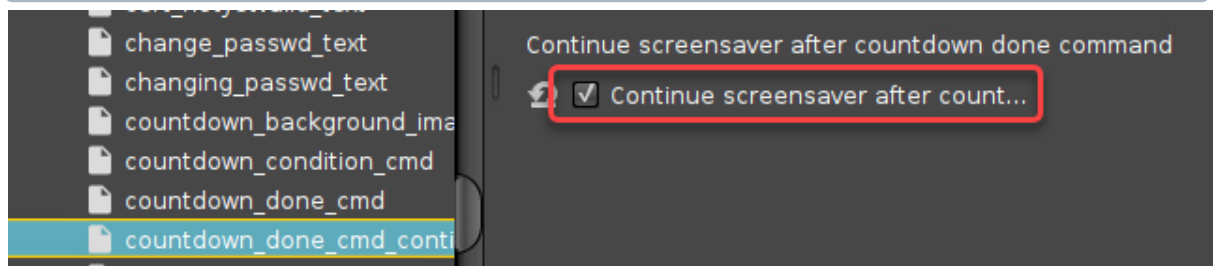
4. Click **Apply** or **Ok**.

IGEL

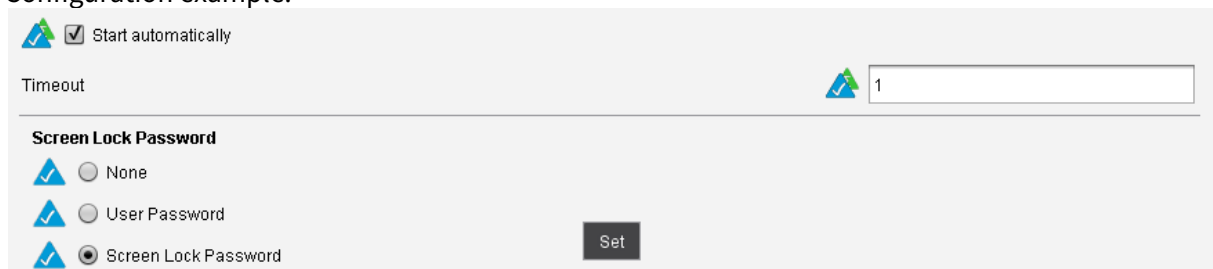# How to Set Up a Countdown in the IGEL OS

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:

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 386).
Configuration example with custom image:

Countdown duration in seconds		10
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:
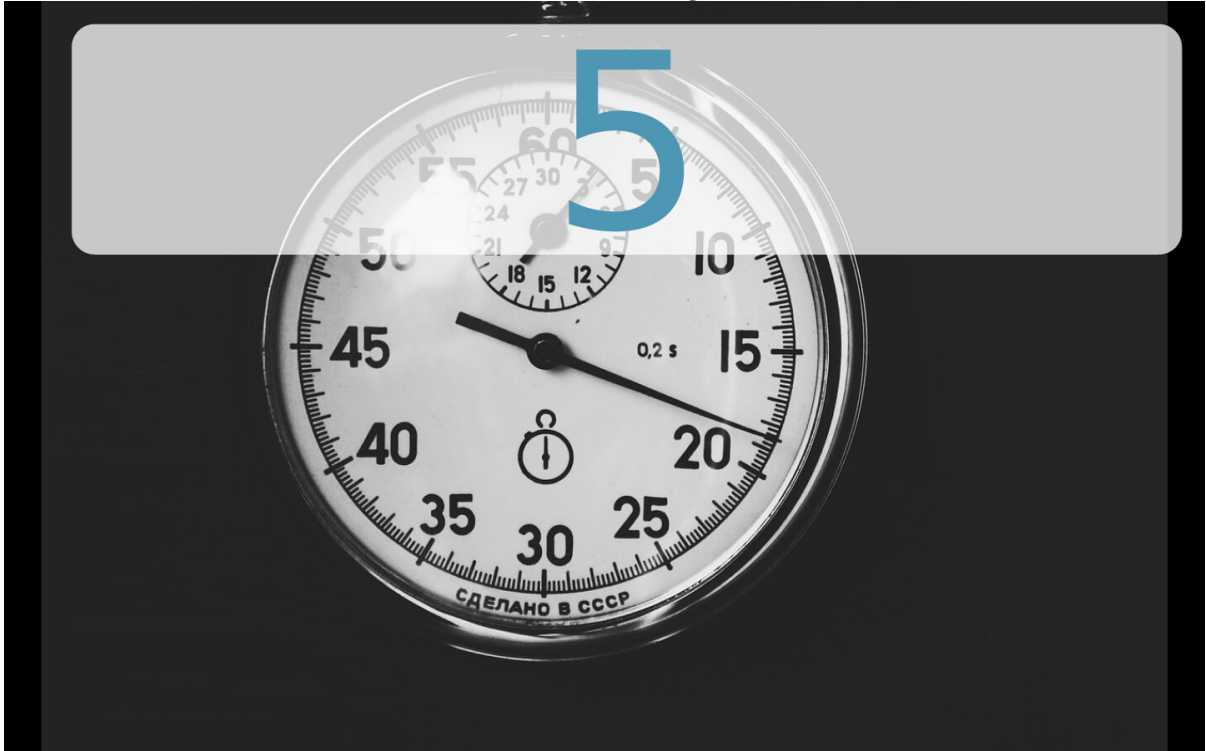
Configuring a Conditional Countdown and Command

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:
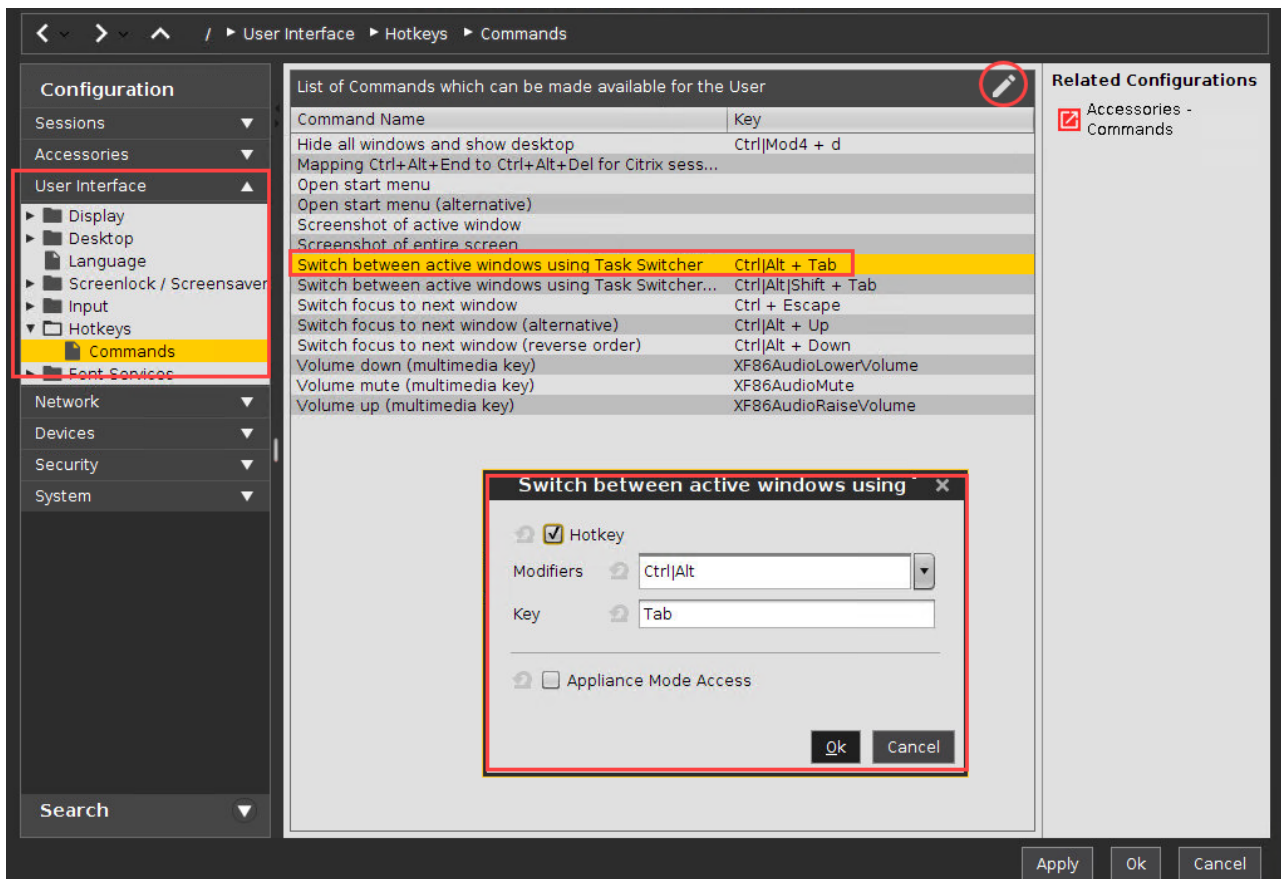
1. Open the setup and go to **User Interface > Hotkeys > Commands**.
2. Select **Switch between active windows using Task Switcher**.
3. Click on **Modify**.
   A dialog window is opened.
4. Enable **Hotkey**, if not already enabled.
5. Select a modifier key or a combination of modifier keys under **Modifiers**.
6. Enter a **Key**.

> ⓘ If you want to enter a key that has no visible character assigned, e. g. the [Tab] key, open a terminal, logon as user and enter `xev -event keyboard`. Press the key designated for the hotkey. The text in brackets starting with `keysym` will contain the desired string for the **Key** field; example: `Tab` in `(keysym 0xff09, Tab)`

7. Click on **Ok**.
8. Click on **Apply** or **Ok**.
   The hotkey is ready for use.

The following example shows how to define a hotkey to lock the screen:
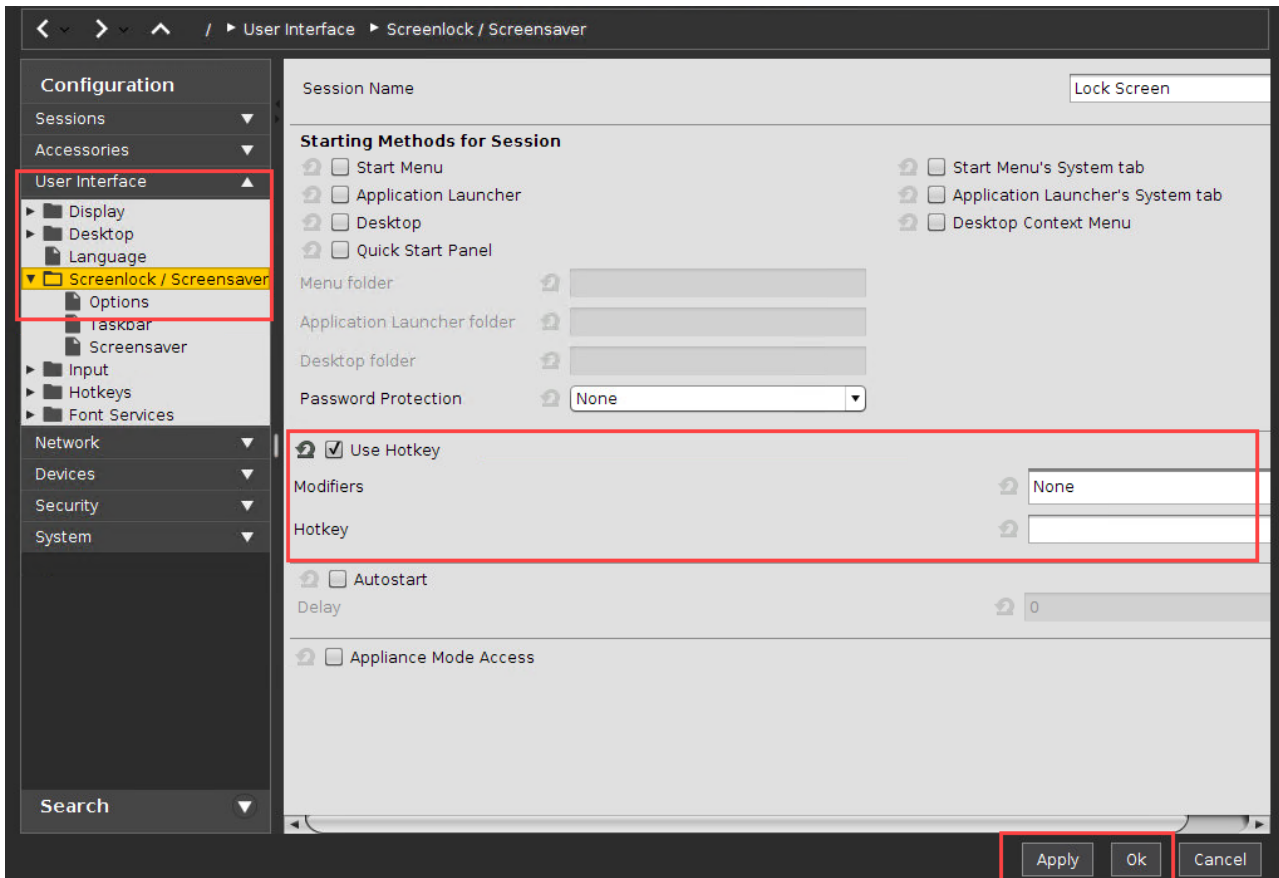
1. Open the setup and go to **User Interface > Screenlock/Screensaver**.
2. Enable **Hotkey**.
3. Select a modifier key or a combination of modifier keys under **Modifiers**.
4. Enter a **Key**.
5. Click on **Apply** or **Ok**.
   The hotkey is ready for use.

IGEL

Suspend to RAM - Wake Up by USB Mouse

You can wake up your device by mouse click or key press.

> (i) 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[31].

   > ⓘ 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!

---

31 https://sourceforge.net/projects/screenshot/?source=directory

IGEL

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**

IGEL

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.

IGEL

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 .

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;

IGEL

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.

IGEL

Devices

IGEL

Monitor

IGEL

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 434)
- eGalax (see page 438)
- Elo Multitouch (USB) (see page 440)
- Elo Singletouch (USB) (see page 442)
- TSHARC (USB) (see page 444)

IGEL

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 / <u>disabled</u>

- **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 / <u>disabled</u>

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 / <u>disabled</u>

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: <u>1000 msec</u>

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`.

IGEL

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 / <u>disabled</u>

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: <u>1000 msec</u>

Multimonitor

Multimonitor configuration is not supported.

IGEL

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 / <u>disabled</u>

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 / <u>disabled</u>

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: <u>1000 msec</u>

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 / <u>disabled</u>

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`.

IGEL

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 / <u>disabled</u>

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: <u>1000 msec</u>

Multimonitor

Multimonitor configuration is not supported.

IGEL

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**.

IGEL

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 >**
    `sessions.user_display%.options.disable_hotplug`
  - Set it to **DP_Disconnect_Only**.

IGEL

No Sound When Using a DisplayPort Monitor

Symptom

You do not hear any sound from your *IGEL UD5* or *UD6* device. You are using a monitor connected via DisplayPort.

Problem

Some DisplayPort monitors misleadingly report support for display audio although they do not have loudspeakers. Therefore *IGEL Linux* will try to play back audio via the monitor.

Solution

1. Right-click on the loudspeaker icon in the panel and open **Sound Preferences**.
2. In the **Output** tab select **Speakers / Built-in Audio**.
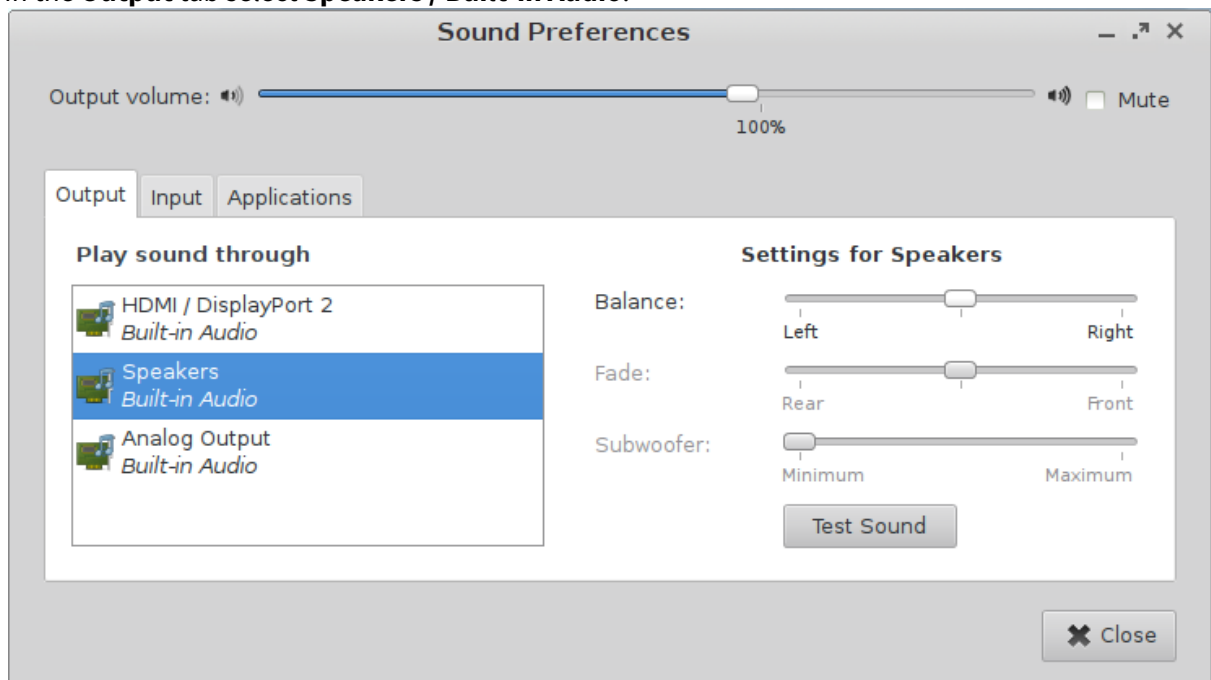
3. Click **Test Sound** to test the new setting. Check if you hear a voice saying "Front Left" and "Front Right" on the device speakers.

Speaker Testing for Speakers

Front Left

Test

Front Right

Test

100%

Settings for Speakers

Left

Rear

Minimum

Test Sound

Close

IGEL
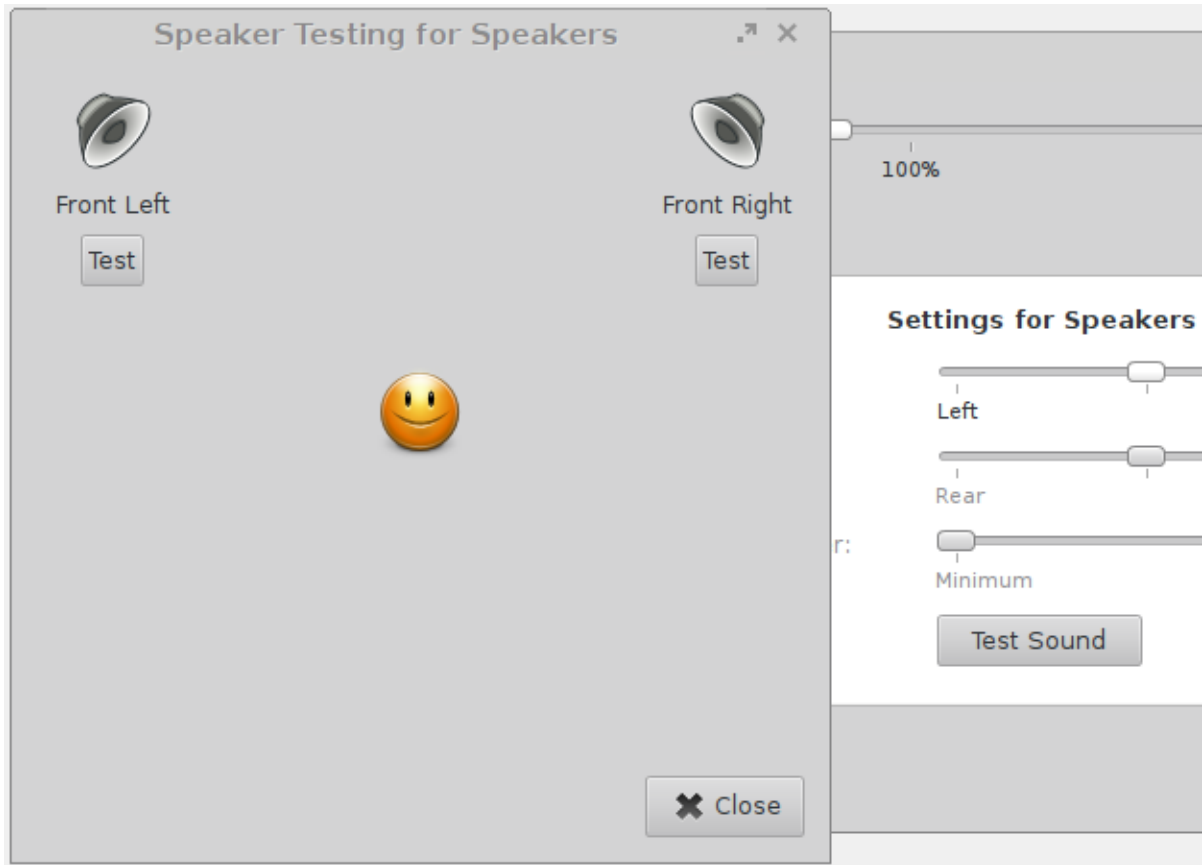
Connecting Three DVI Monitors to UD7 with Passive DisplayPort Adapters

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.

IGEL

Webcam Information

If you are running a device with *IGEL Linux* version *5.3.100* or higher, you can configure and test a webcam using a built-in tool. This tool is called **Webcam Information**.

▶ To configure a starter for **Webcam Information**, open the IGEL Setup and go to **Accessories > Webcam Information**.

To determine and change the width, height, and frame rate of your webcam:

1. Start the **Webcam Information** tool.
   The following values are shown:
   - **Width**: Width of the image in pixels
   - **Height**: Height of the image in pixels
   - **Rate**: Frame rate in fps (frames per second). Example: **1/30** means 30 single images per second.
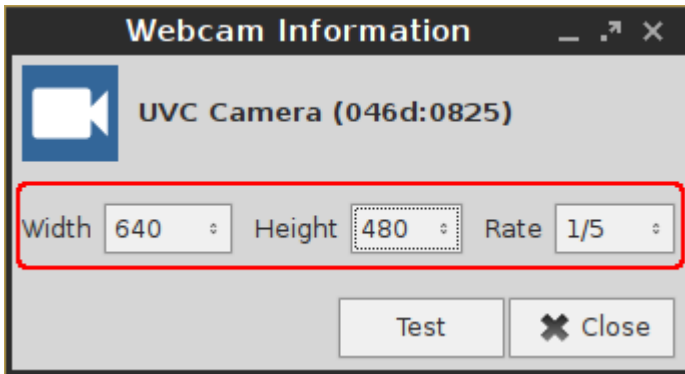
2. Click on on one of the fields to change the value. In doing so, the supported values are shown.
3. Click **Test**.
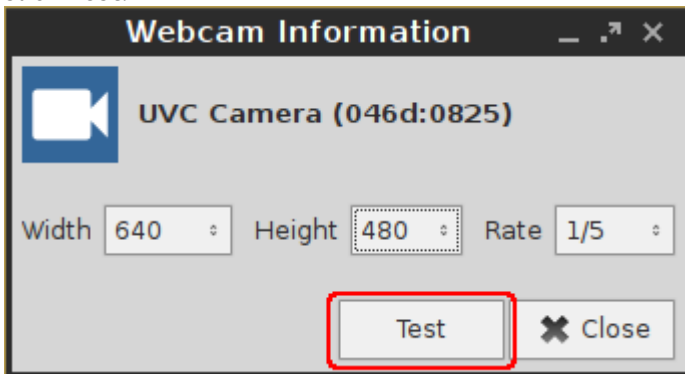
The video image generated with the current settings is shown.
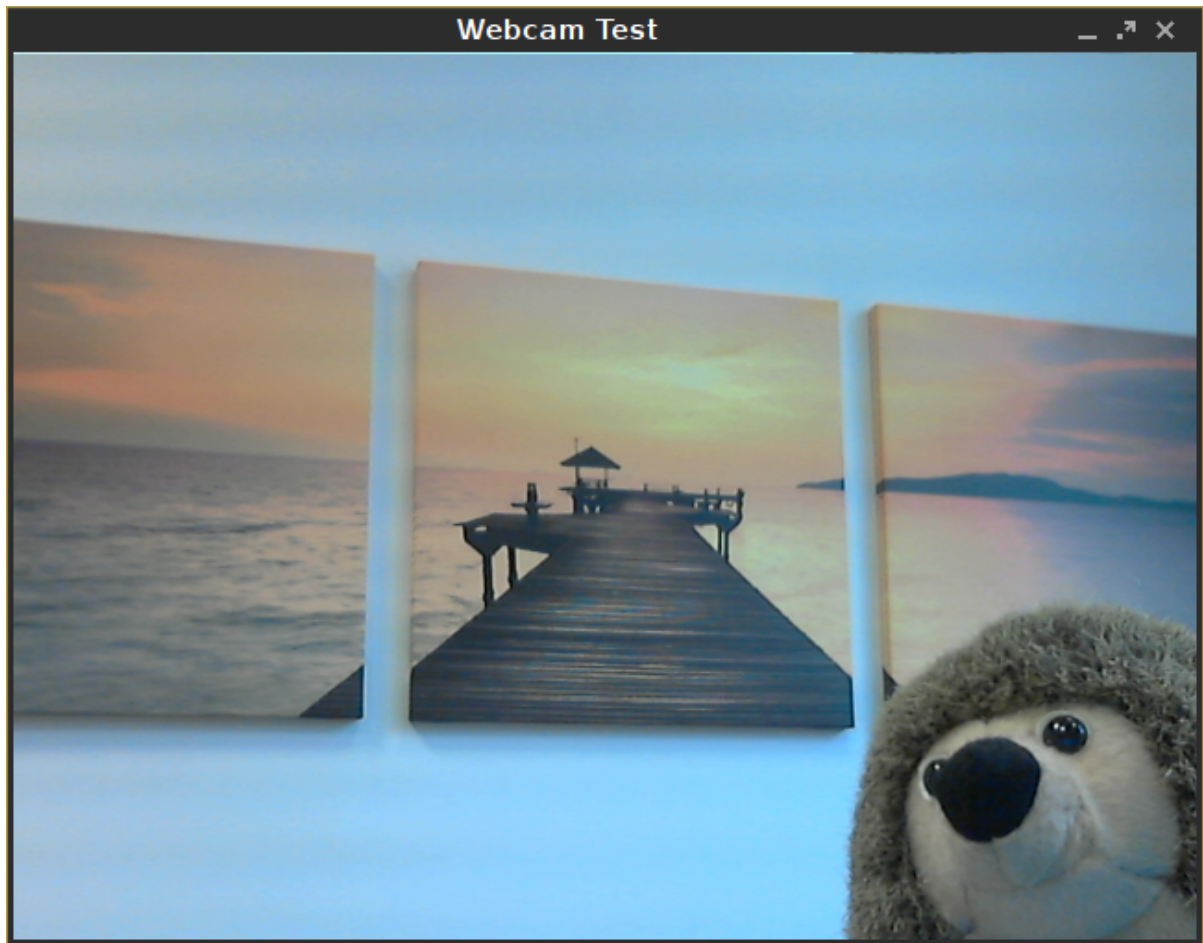
To check if the webcam is working in a session (e.g. via Citrix HDX webcam redirection), open a browser in the session and go to https://www.onlinemictest.com/webcam-test/.

Bluetooth Tool

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.
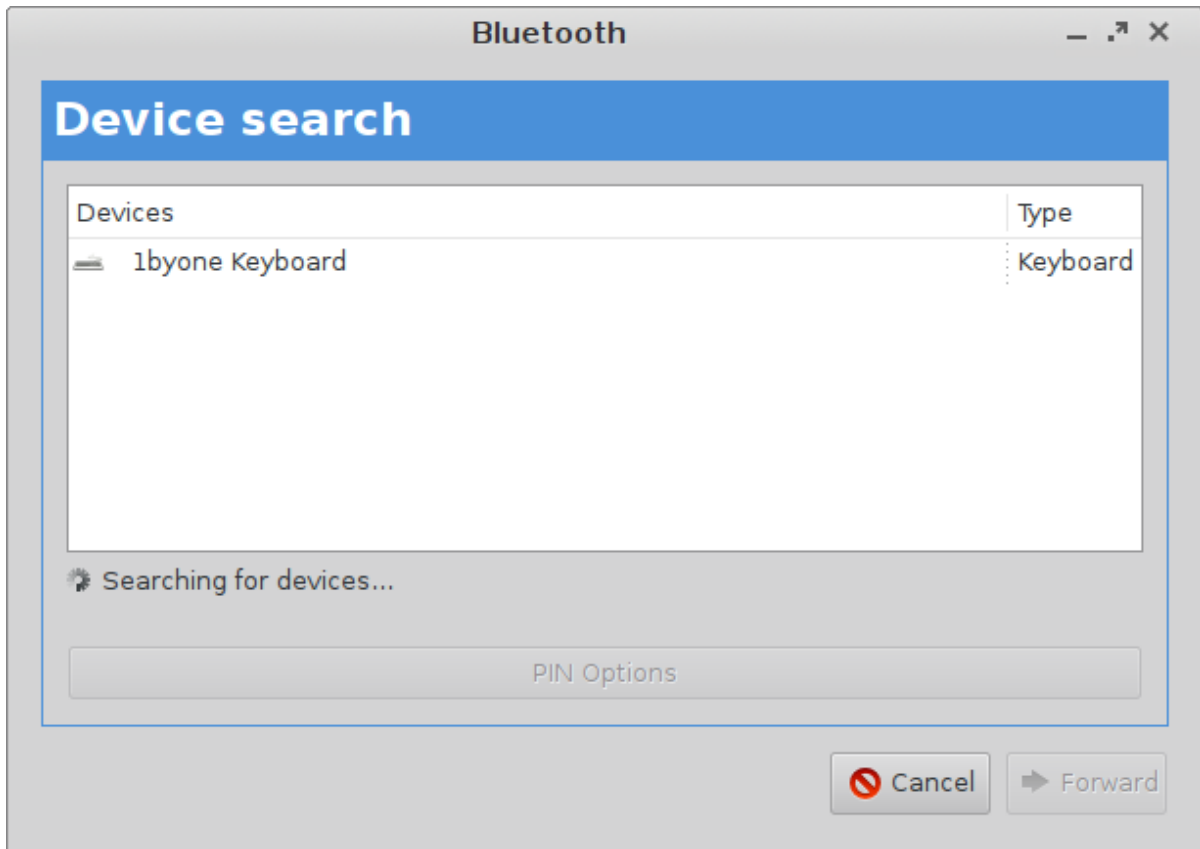
3. Highlight the desired Bluetooth device and click on **Forward**.
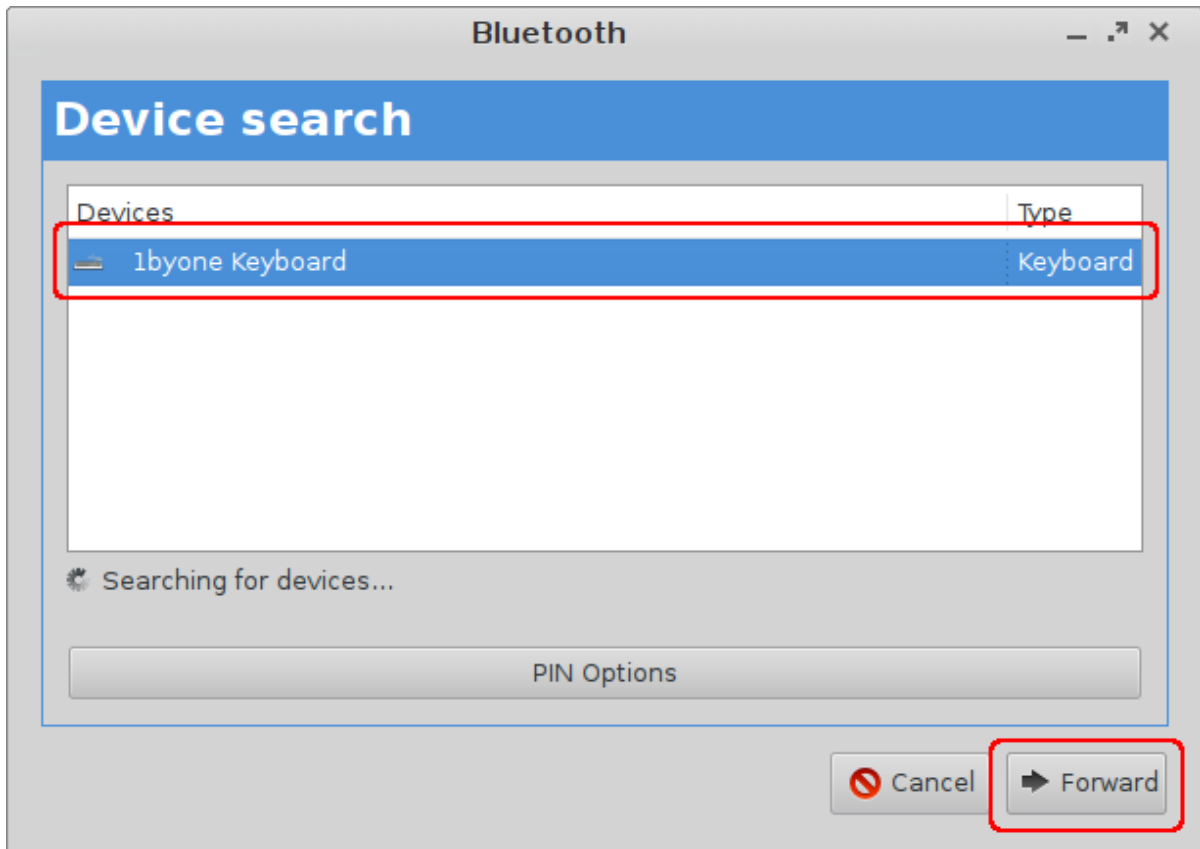
A PIN will be shown on the **Device setup** dialog.

Bluetooth

Device setup

Please enter the following PIN on '1byone Keyboard' and press Enter on the keyboard.

162319⏎

◄ Back   Ⓧ Cancel
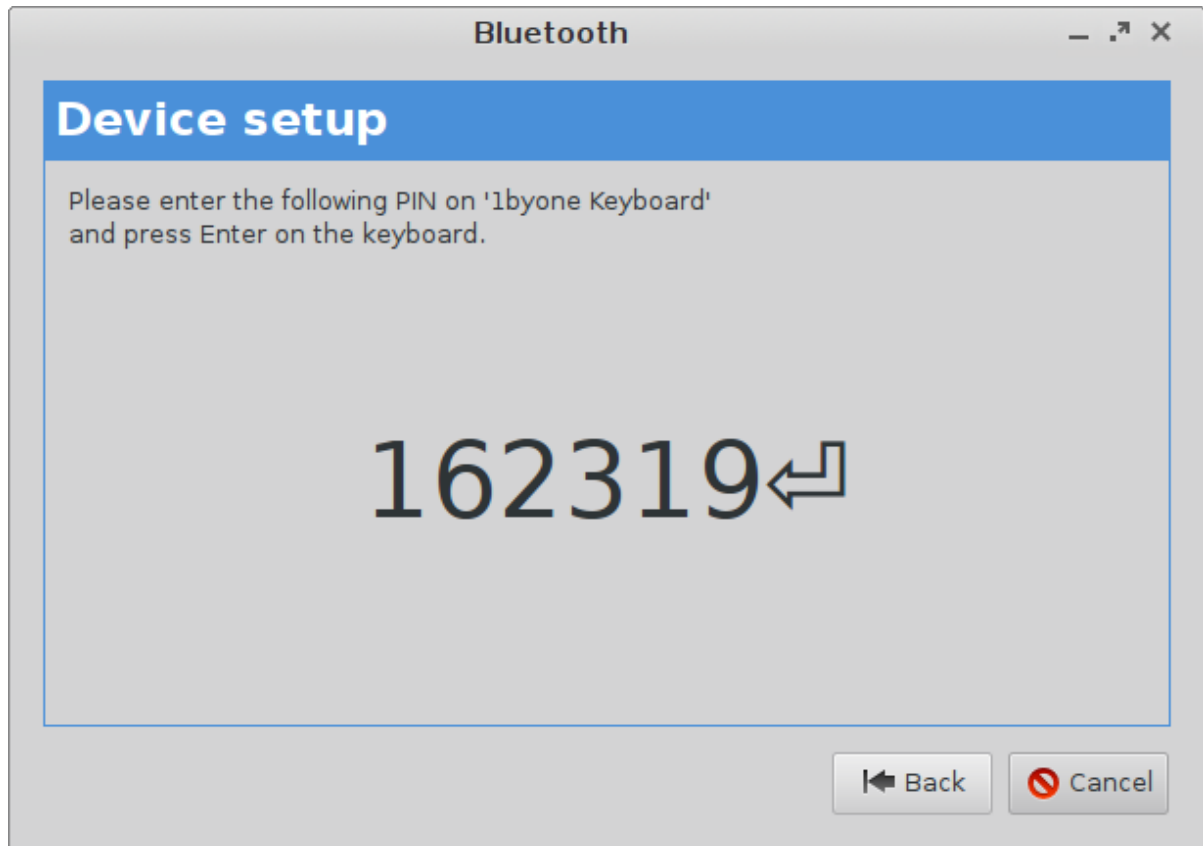
4. Enter the PIN into your Bluetooth device.
   If everything went well, the status of the connection will be shown.

Bluetooth

Setup summary

Successfully set up new device '1byone Keyboard'.

Back   Close
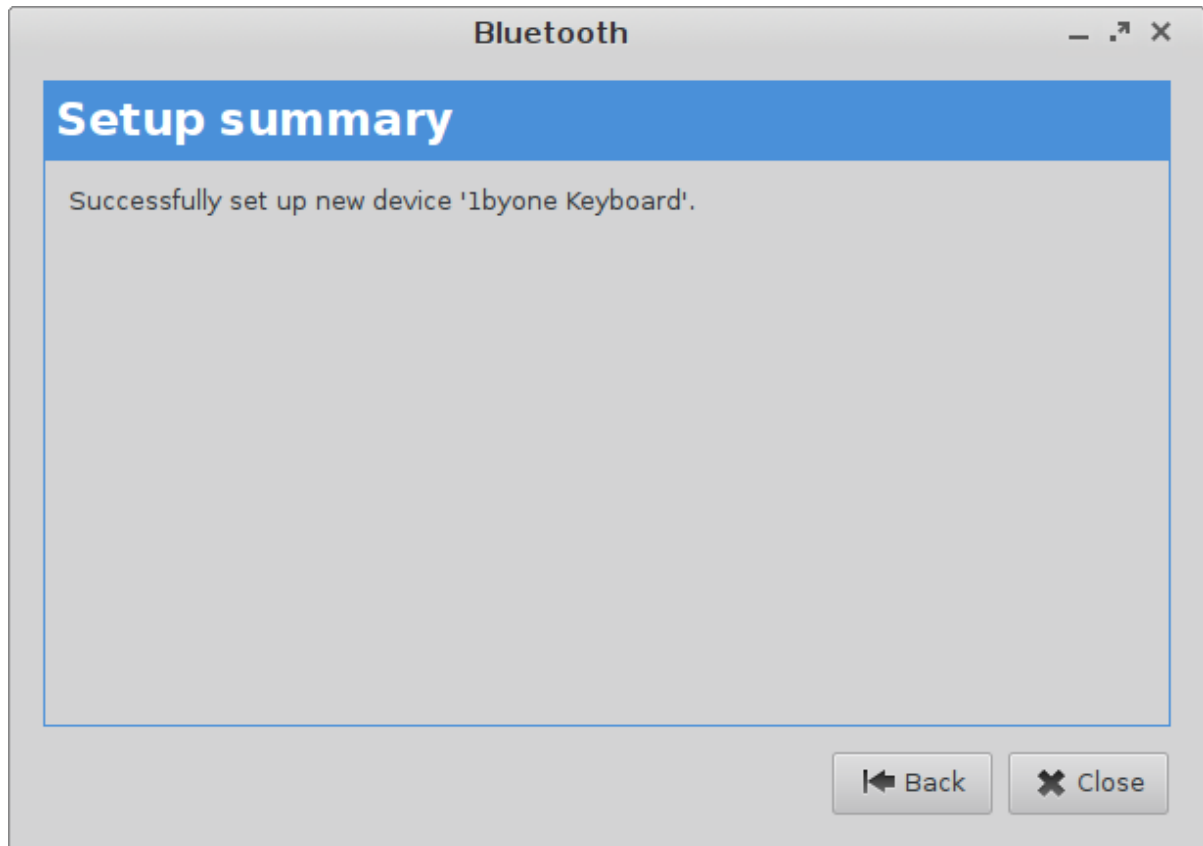
5. Click on **Close**.

   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.

IGEL

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.

IGEL

Using a Kofax / Wacom Signature Pad

You can use a Kofax / Wacom signature pad in Citrix sessions using the Kofax SPVC signature pad channel. The Virtual Serial Sign Pad method is no longer supported.

On the Device

1. Connect the signature pad to one of the device's USB ports.
2. Go to **Sessions > Citrix > Citrix Global > Mapping > Device Support**.
3. Enable **Kofax SPVC signature pad channel**.
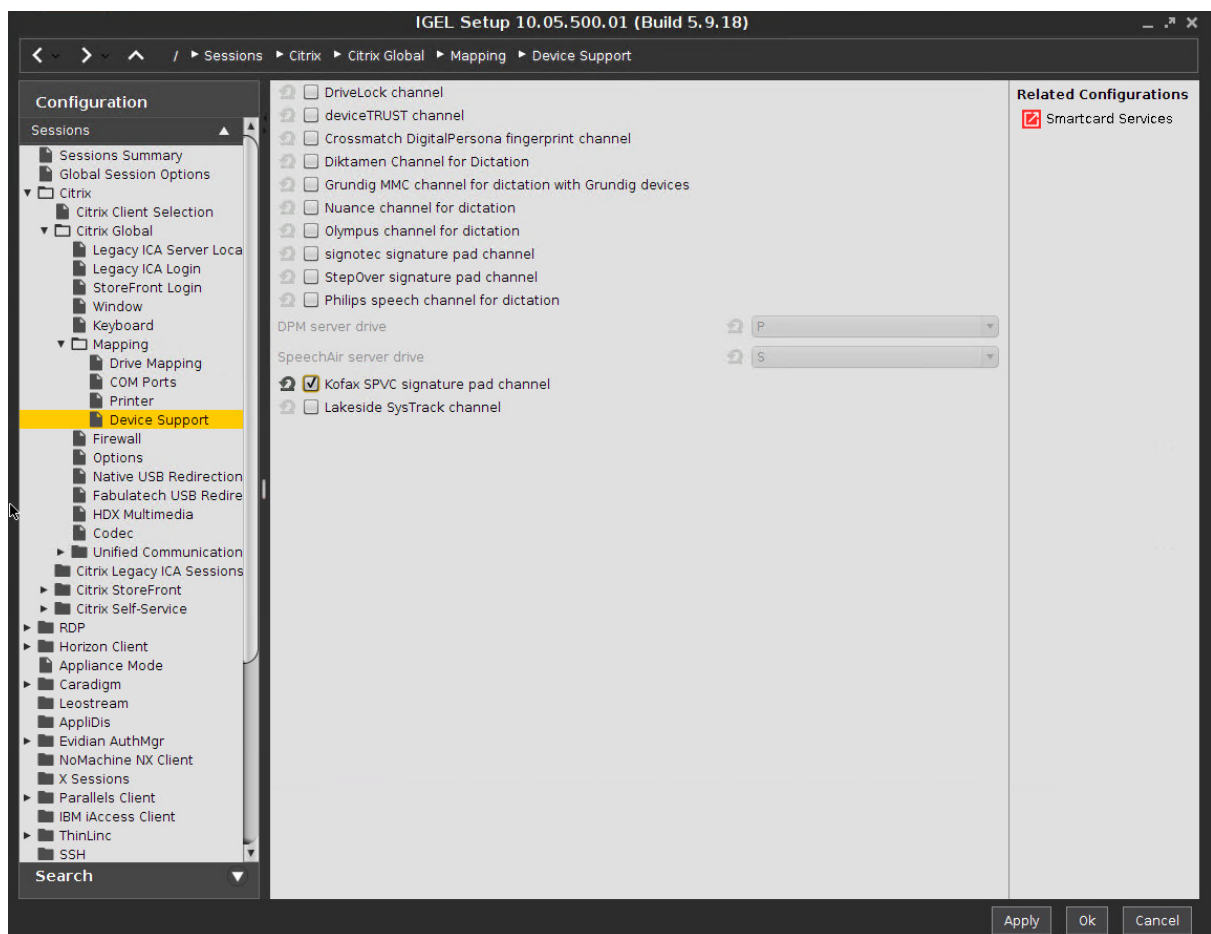
On the VDI Server (Windows)

▶ Install the required software from Kofax / Wacom.

The driver contained in this software will listen for signature pads on a virtual channel. Applications such as SignDoc will be able to use the signature pad.

IGEL

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:

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.

IGEL

With StepOver TCP Client

On the Device

▶ Connect the signature pad to one of the device's USB ports.

▶ Go to **User Interface > Input > Signature Pad** in IGEL Setup.

▶ Enable **StepOver TCP Client**.

▶ Modify **Listening TCP Port** if needed. (Default: 8888)
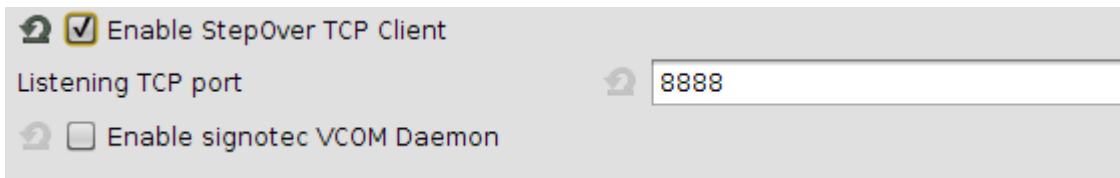
> ⓘ You can check whether the **StepOver TCP Client** is running on the device by entering the following in a local terminal: `ps waux | grep sotcp`. The result should contain an `sotcp` process.

On the VDI Server (Windows)

▶ Locate the `sodc.exe` program on the server. It is the part of StepOver eSignature Office and can be found in `[Your Program Files Directory]\StepOver\eSignatureOffice [version]\driver\`.

▶ If you are using a non-standard TCP port, change it in the `config.ini` file located in the same directory.
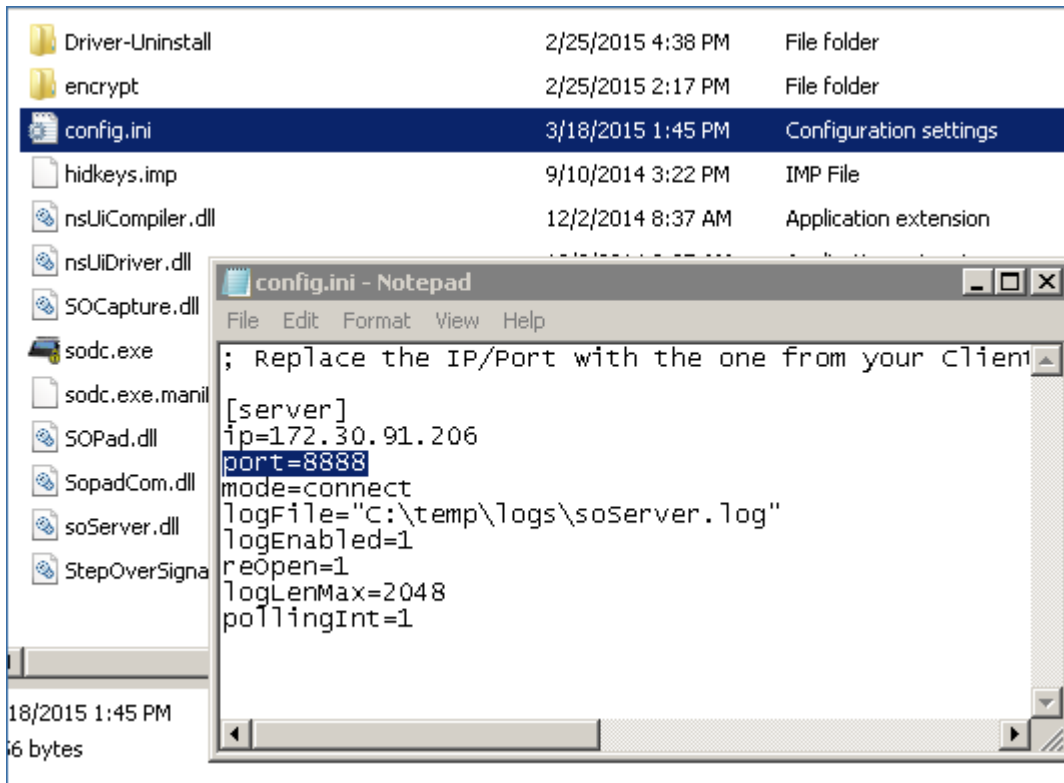
▶ Execute `sodc.exe` . The **StepOver Pad Test** window will open. Use its buttons to search and select your signature pad and try writing into the provided field.
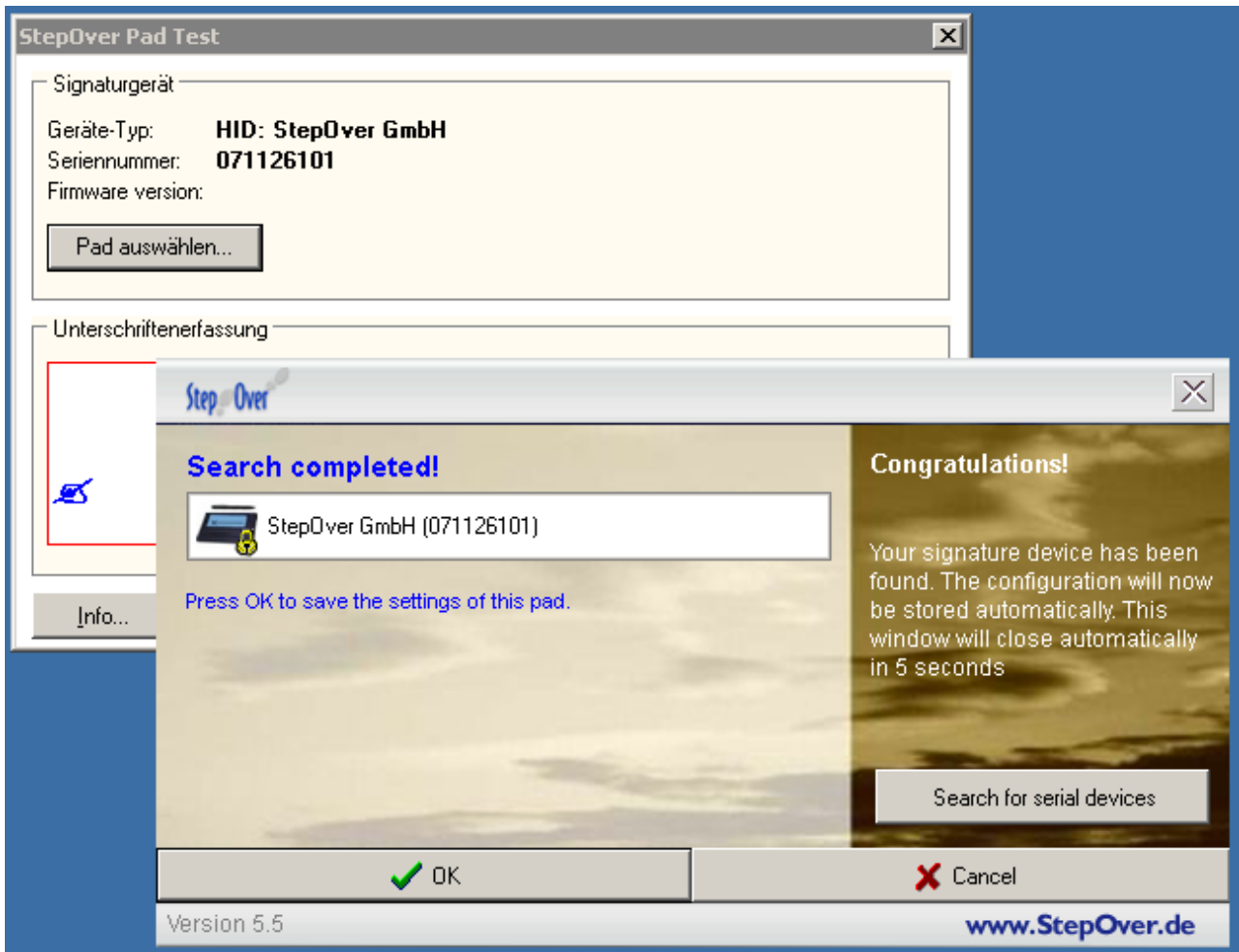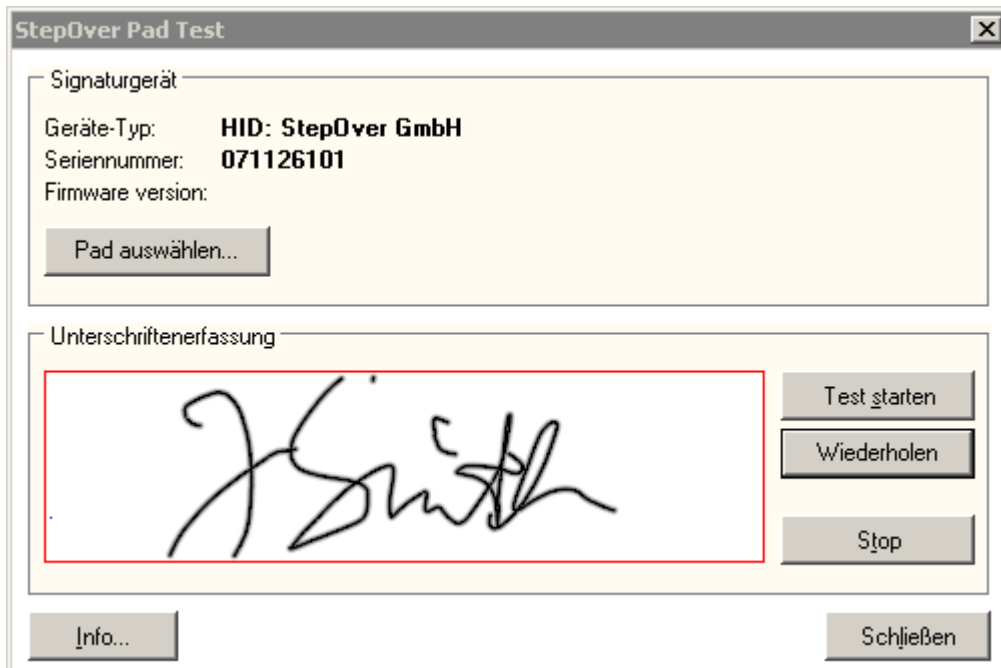
The status LED of the pad will turn to green when the connection is successful. The signature pad is now ready to be used with enabled applications such as StepOver eSignature Office.

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

Keywords: elektronische Gesundheitskarte, Krankenversicherungskarte, Heilberufsausweis

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

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 ⊕.

1. 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**:
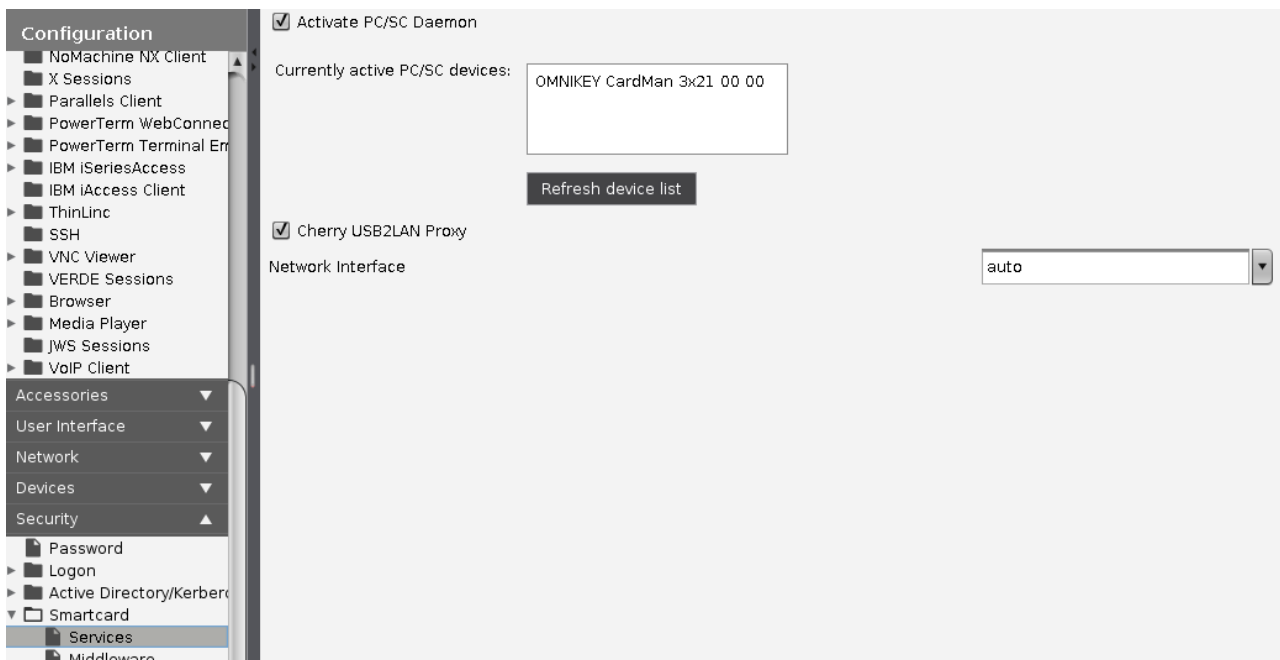
Configuring the server

1. Install the eGK-KVK software by *Cherry*.
   See also http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf
2. Start the program *CT-API configuration*.
3. Select port number 1 for the ST-2052.
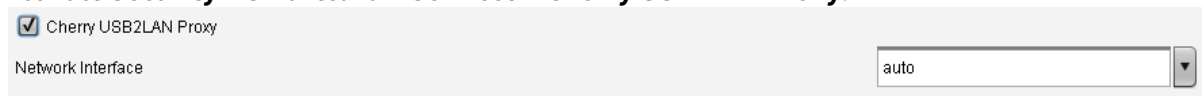
Cherry ST-1503 und G87-1504 (USB)

Functionality	
USB ID:	046a:0080 for ST-1503
	046a:0081 for G87-1504
Software:	Cherry eHealth eGK/KVK software
Client/server connection:	SICCT via LAN provided by the Cherry USB2LAN proxy

Cherry USB2LAN proxy: Makes Cherry electronic health card devices available in the network via SICCT. The communication between card reader and server takes place independently of the VDI connections.

Configuring the Thin Client for Using the Cherry USB2LAN Proxy

1. Activate **Security > Smartcard > Services > Cherry USB2LAN Proxy**:

Configuring the Server for the Cherry USB2LAN Proxy

1. Install the eGK-KVK software by Cherry.
2. Configuration according to chapter 6 in http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf.

Orga 910/920 M

Functionality	
USB ID:	0780:1202
Software:	CT-API by Orga
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP
2. Select **Enable Com Port Mapping**:
3. Click ⊕.
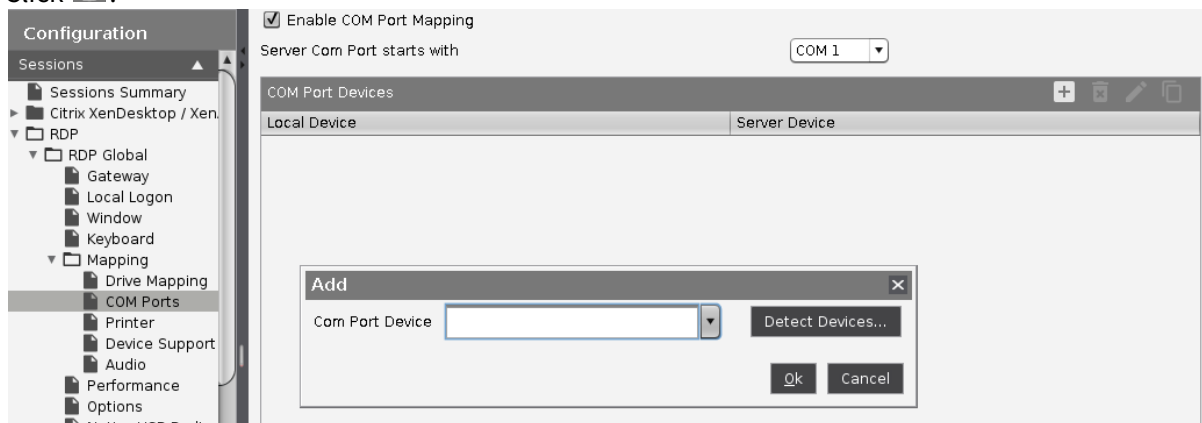
4. Select USB COM 1 as a new COM port device (/dev/ttyUSB0).

Configuring the server

1. Download the appropriate driver for *Orga 910/920 M* from the download page:
   http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx[32]
2. Install the driver.

---

32 https://ingenico.de/healthcare/downloads

Orga 6041 L eGK eHealth-BC S

Functionality	
USB ID:	0780:1302
Software:	CT-API by Orga
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click ⊕.
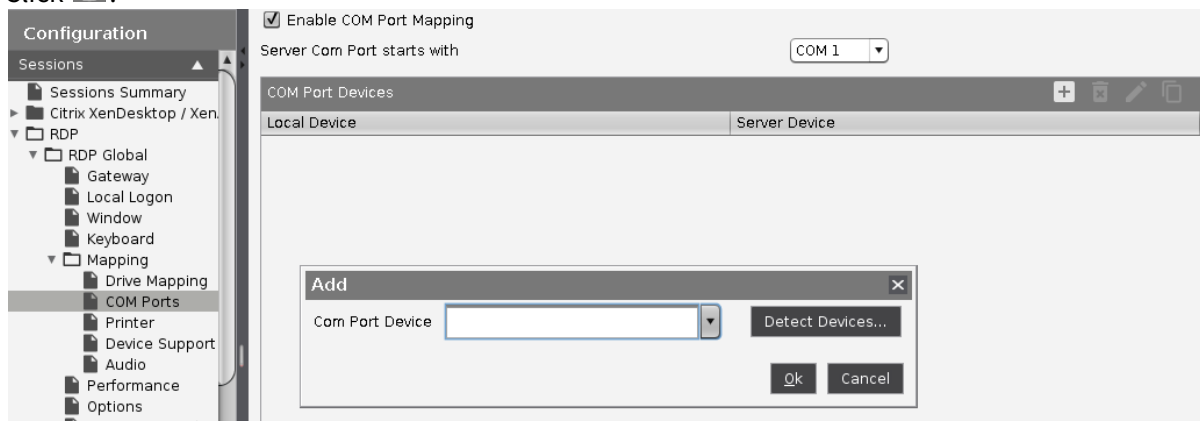
4. Select USB COM 1 as a new COM port device (`/dev/ttyUSB0`).

Configuring the server

1. Download the appropriate driver for *Orga 6041 L eGK eHealth-BC S* from the download page:
   http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx[33]
2. Install the driver.

---

33 https://ingenico.de/healthcare/downloads

celectronic CARD STAR / medic2

Connecting the reader

▶ Connect the reader to the COM port of the thin client.

ⓘ The reader must be set to host/PC serial interface.

Functionality	
Software:	CT-API by celectronic
Device/server connection:	COM port mapping

Configuring the device

In IGEL Setup, add the COM port device to which the keyboard is connected:

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
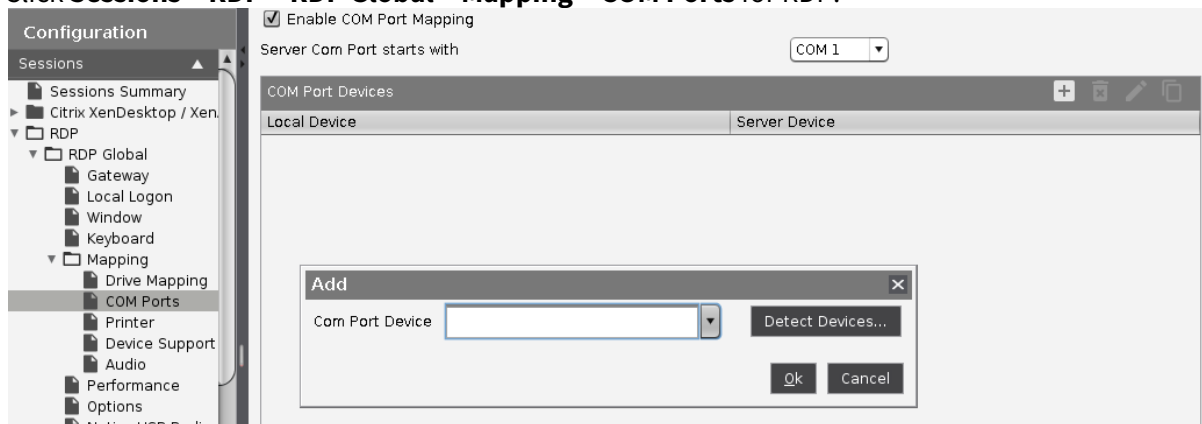
2. Click ⊕ .
3. Select a **COM port device** (COM1, COM2,...).

Configuring the server

1. Download the appropriate driver for *celectronic CARD STAR /medic2* from the download page: https://www.ccv.eu/de/
2. Install the driver.

celectronic CARD STAR/ memo3

Functionality	
USB ID:	152a:8180
Software:	CT-API by celectronic
Device/server connection:	COM port mapping

Configuring the device

1. Click **Sessions > RDP > RDP Global > Mapping > COM Ports** for RDP.
2. Select **Enable Com Port Mapping**:
3. Click ⊕.
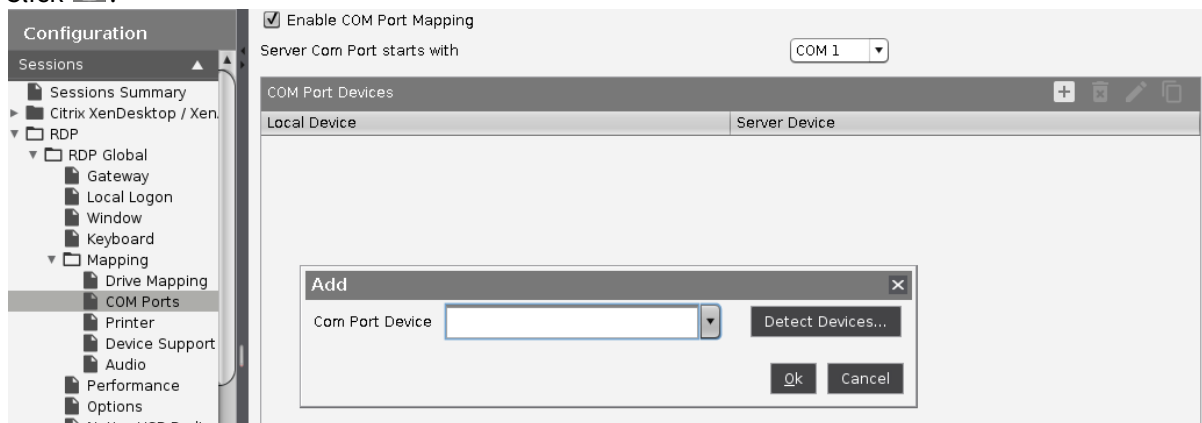
4. Select USB COM 1 as a new COM port device (`/dev/ttyUSB0`).

Configuring the server

1. Download the appropriate driver for *celectronic CARD STAR memo3* from the download page: https://www.ccv.eu/[34]
2. Install the driver.

IGEL

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.

_____

IGEL

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 .

Disabling Mobile Device Access

Disabling Mobile Device Access

▶ In the context menu of the tray icon, click **Quit**.
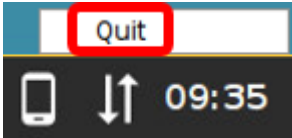
Mapping a Mobile Device for a Session

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 475).
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.

IGĖL

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 480).
   You can remove the mobile device securely; see Safely Removing the Mobile Device (see page 482).

Accessing the Mobile Device USB Window from a Session

Non-Fullscreen Session

▶ Click ▯ to open the **Mobile Device Access USB** window.
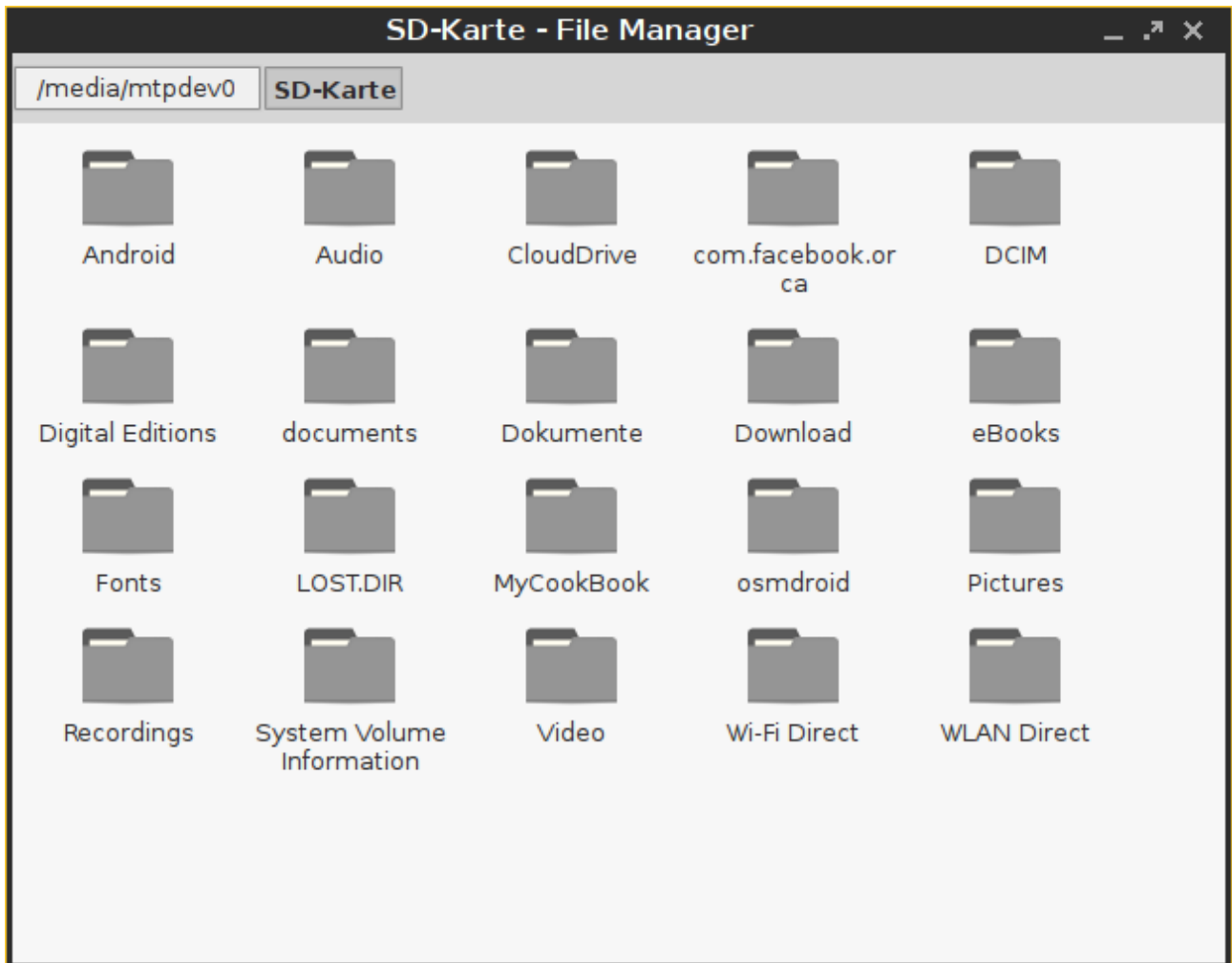The **Mobile Device Access USB** window appears.
You can view the directories and files on your mobile device or safely remove the device; see Safely Removing the Mobile Device (see page 482).

Fullscreen Session

In a session that is running in fullscreen mode or appliance in a fullscreen session, you can use the in-session control bar to open the **Mobile Device Access USB** window.

1. Move the mouse pointer to the upper edge of the screen.
   The in-session control bar appears.
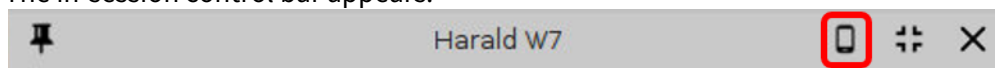
2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

Appliance Mode Session

In a session that is running in appliance mode, you can use the in-session control bar to open the **Mobile Device Access USB** window.

1. Move the mouse pointer to the upper edge of the screen.
   The in-session control bar appears.
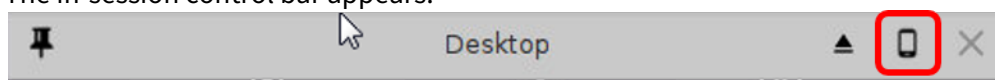
2. Click the smartphone symbol.
   The **Mobile Device Access USB** window appears.
   You can view the directories and files on your mobile device or safely remove the device.

Viewing the Files and Directories Locally

▶ Select **View** in the context menu.
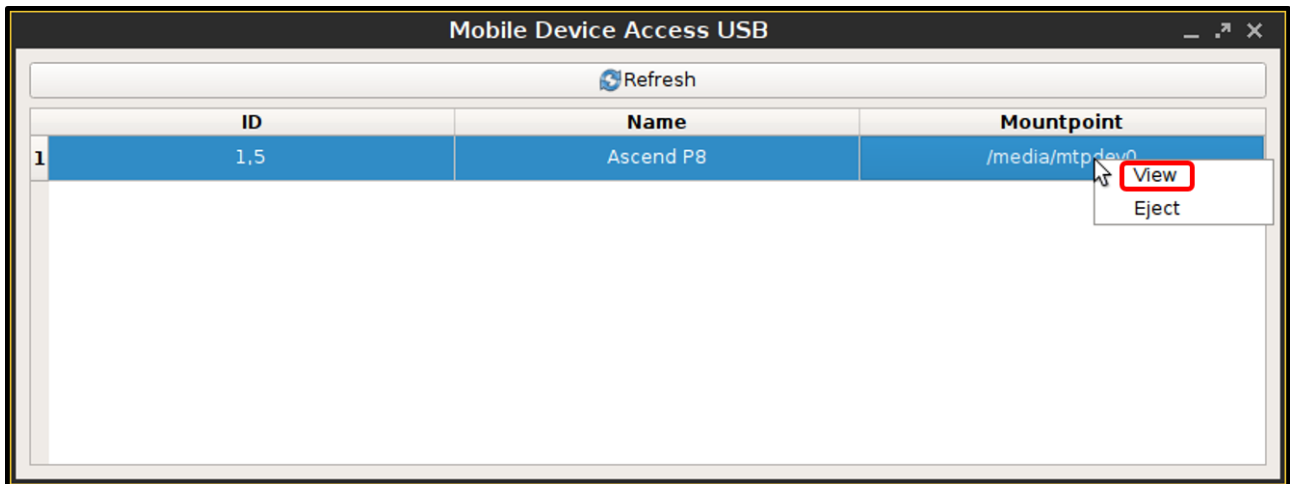
The directories on your smartphone are displayed. Access is read-only, i. e. you can only view the directories and files.

SD-Karte - File Manager

/media/mtpdev0 | **SD-Karte**

Android	Audio	CloudDrive	com.facebook.orca	DCIM
Digital Editions	documents	Dokumente	Download	eBooks
Fonts	LOST.DIR	MyCookBook	osmdroid	Pictures
Recordings	System Volume Information	Video	Wi-Fi Direct	WLAN Direct

Safely Removing the Mobile Device

▶ Click **Eject** in the context menu for the device in question.

Swapping Function of Mouse Buttons (e.g. When Using an Evoluent Mouse)

The assignment of mouse buttons for *Evoluent Mouse* 3 changed between firmware versions 5.04.130 and 5.05.100.

Problem

Users have become used to the assignment as it was up to version 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 B 2. 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 C 1.

IGEL

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).

IGEL

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 486). If you are lucky, this will do it. If not, continue with the extended procedure (see page 487).

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 487) 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.

IGEL

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 Linux version 10.04.100, SATA devices are also supported.

Problem

How to integrate DriveLock solution with IGEL Linux 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 XenDesktop / XenApp > HDX / ICA Global > Mapping > Drive Mapping**, change the settings as follows:
   - Enable **Activate Drive Mapping**.
3. In **Sessions > Citrix XenDesktop / XenApp > HDX / ICA Global > Mapping > Device Support**, change the settings as follows:
   - Activate **DriveLock channel**.

IGEL

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.

IGEL

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

> ℹ️ 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:
>
>
>
> Alternatively, you can use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal.
> Example for `lsusb`:
>
>
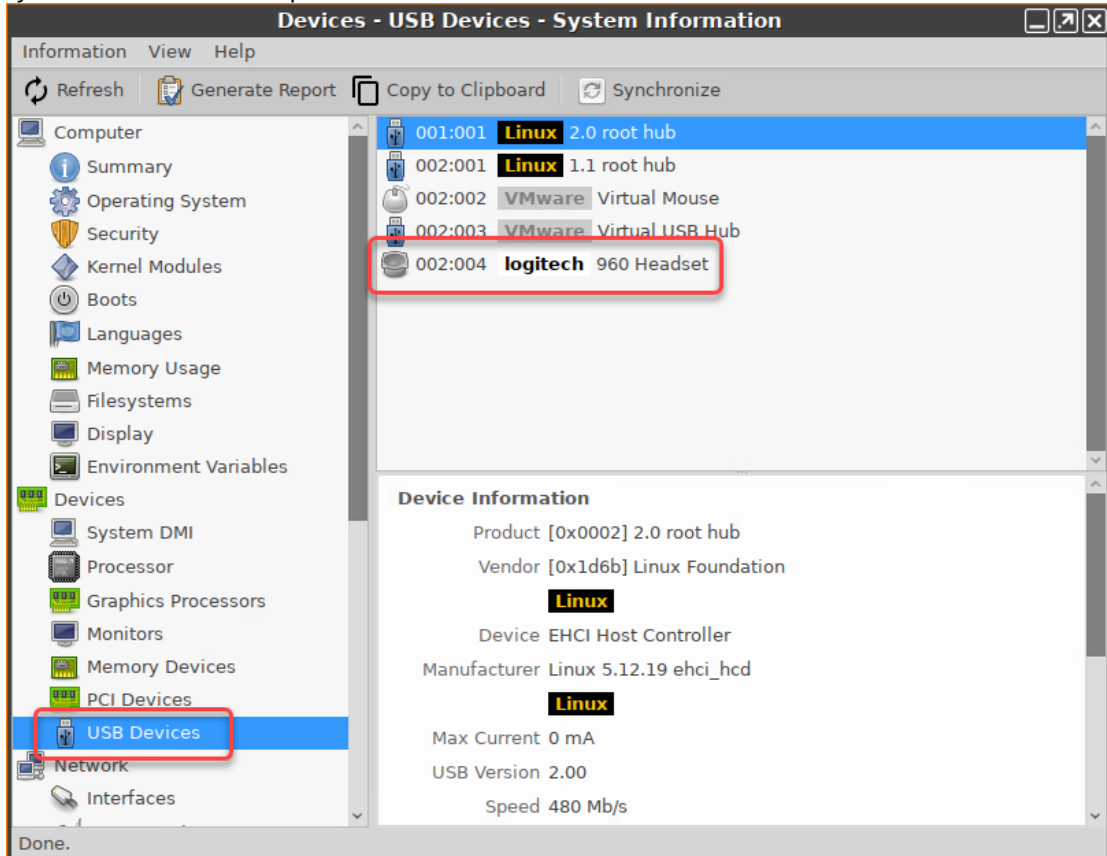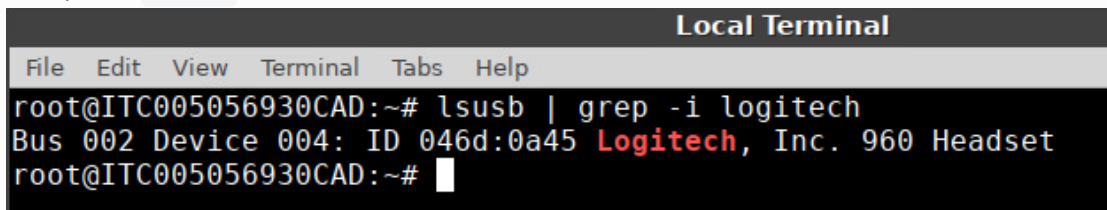
5. Give the **Device UUID** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.
   Possible values:
   - Global setting: The default setting for hotplug storage devices is used; see **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.

- Read only
- Read/Write

7. Under **Name**, give a name for the rule.
8. Click **OK**.
9. Save the changes.
   The rule is active.

Example

- The set rule prohibits the use of USB devices on the device.
- A class rule allows the use of all entry devices (HID = Human Interface Devices).
- A device rule allows the use of the USB storage device with the UUID 67FC-FDC6.
- The use of all other USB devices, for example, storage devices or printers, is prohibited.

Issues with USB IDs in USB Devices Rules

Symptom

USB Device Rules you configured do not take effect.

Problem

The **System Information** tool in IGEL OS up to version 11.04.100 omits leading zeros in USB vendor and product IDs. These are shown only three hexadecimal digits long.
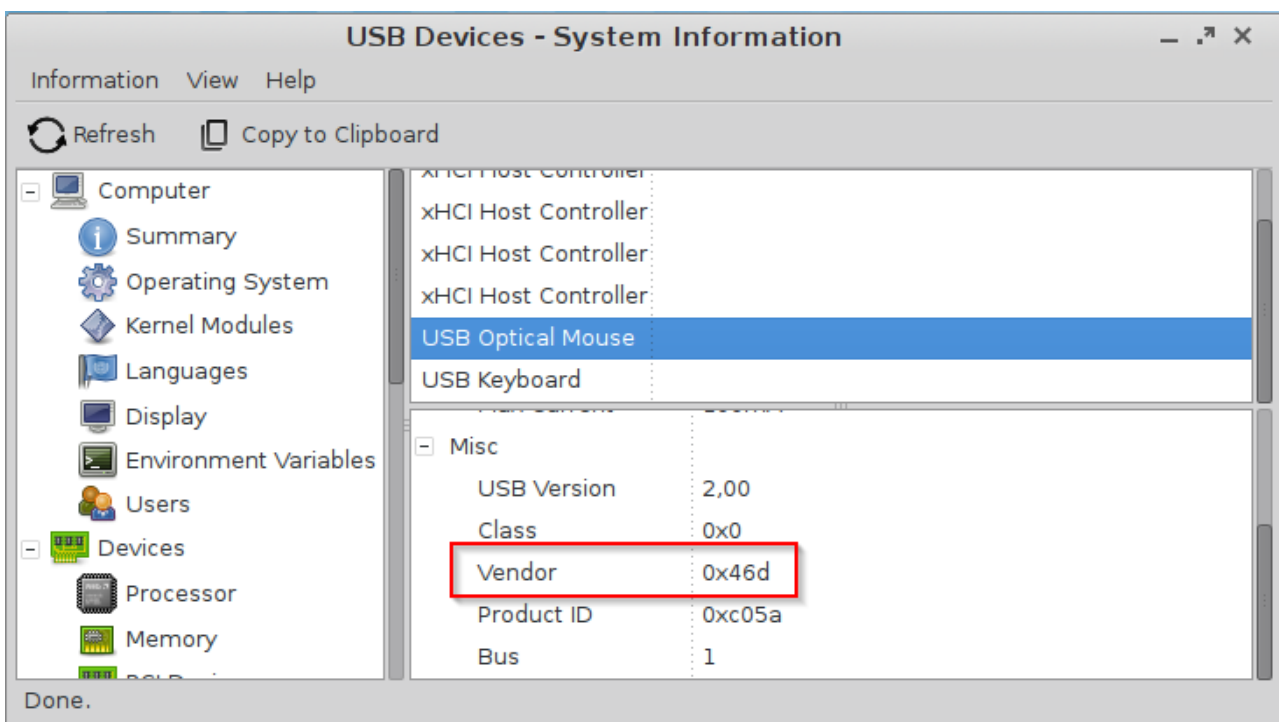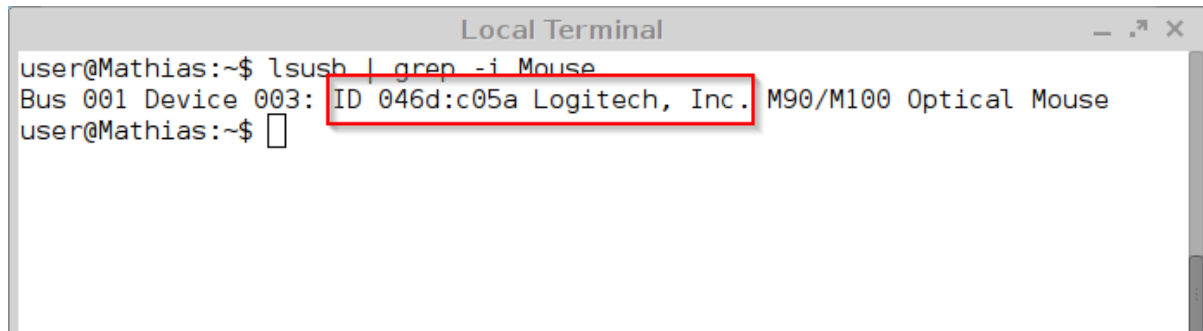
Solution

If you see three-digit USB IDs in **System Information**, use the `lsusb` command:

1. Open **Local Terminal**.
2. Enter the `lsusb` command.
3. Look for the device in question, possibly using `grep` to search in the `lsusb` output:

   `lsusb | grep -i [search term]`

4. Use the four-digit IDs that `lsusb` reports.

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 ICA 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 tab **Mapping in sessions**.
8. Enable **Map Printer in ICA Sessions** or **Map Printer in RDP Sessions**.
9. Enable 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 XenDesktop/XenApp > HDX / ICA Global > Mapping > Printer > Enable 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
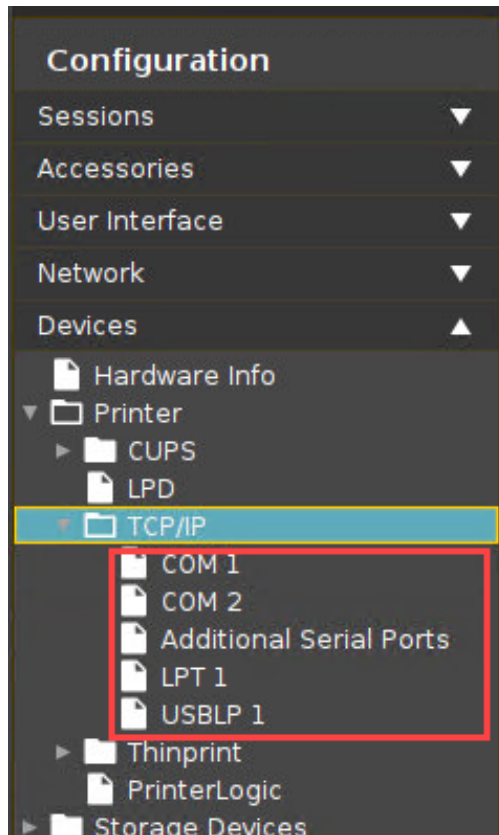
3. Enable **Activate TCP/IP Printer on this Port.**
   Enter the **TCP/IP port number** on which the print server service is listening. (Windows default: 9100)
   Poll Criterion and **Poll Frequency** must only be adjusted if required by the environment.
4. Click **Apply** or **Ok** to save the settings.
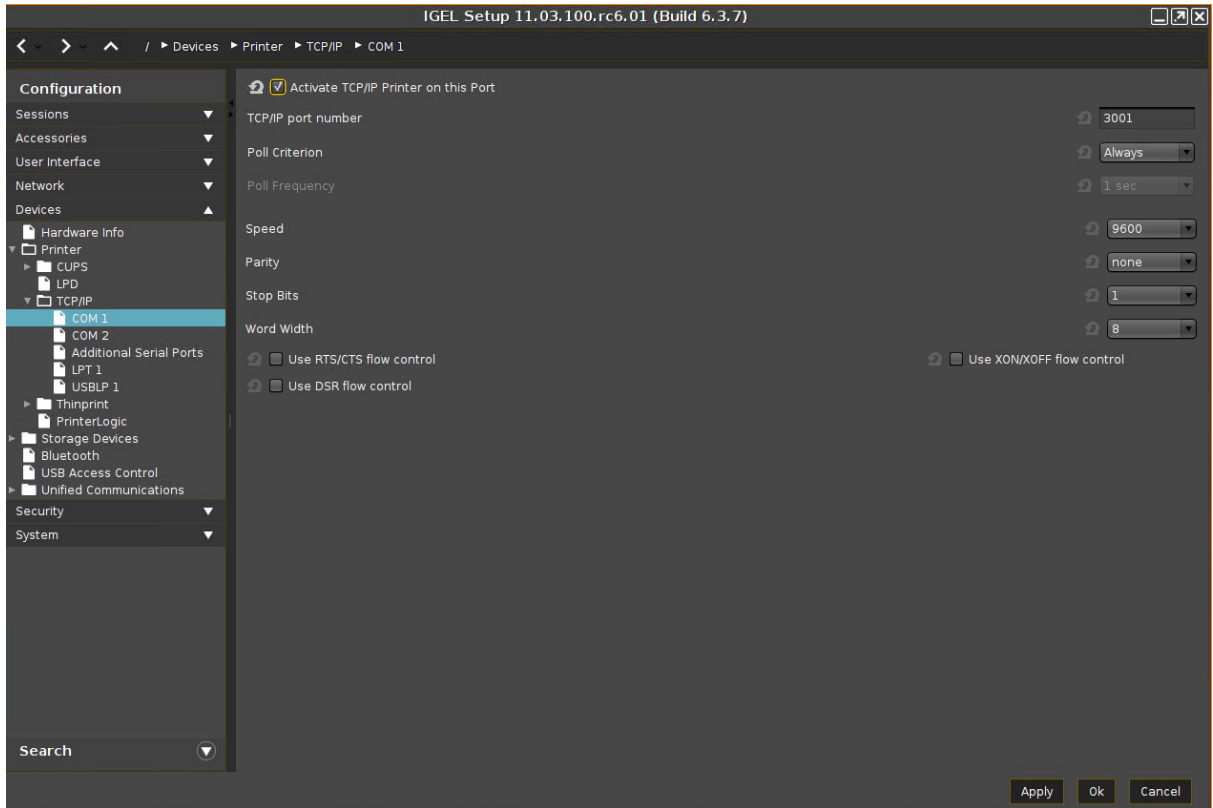
The printer can be installed and used by other systems like a regular network printer.

IGEL

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

IGEL

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

IGEL

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[35].

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] + `c` (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.

---

35 https://mrchromebox.tech

Miscellaneous

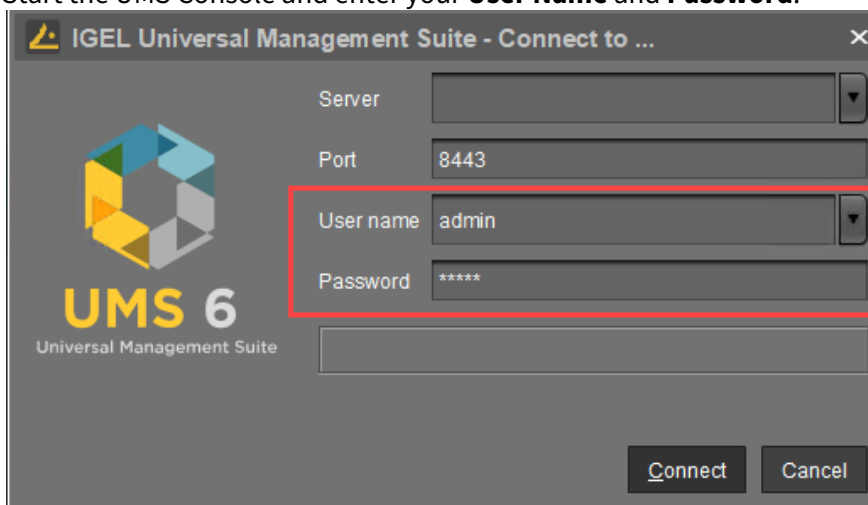# Sending Device Log Files to IGEL Support

When the IGEL support team asks you to provide your device's log files, follow the instructions below.

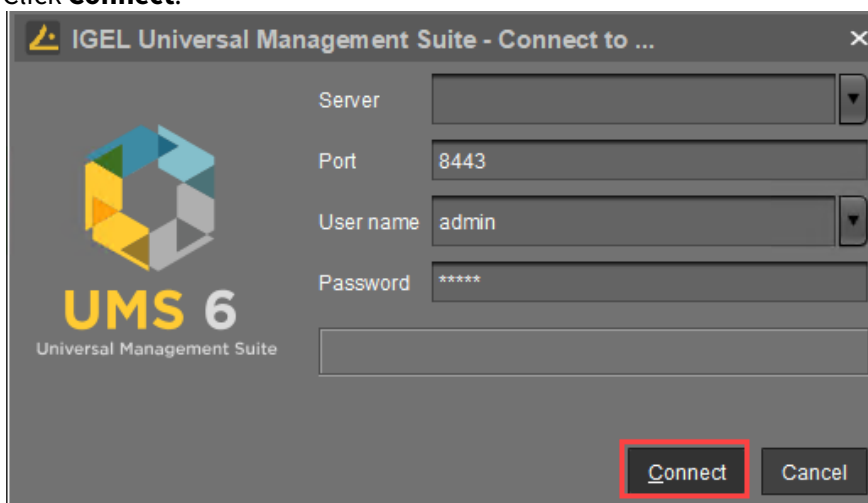There are two opportunities to send log files to the support team:

With UMS

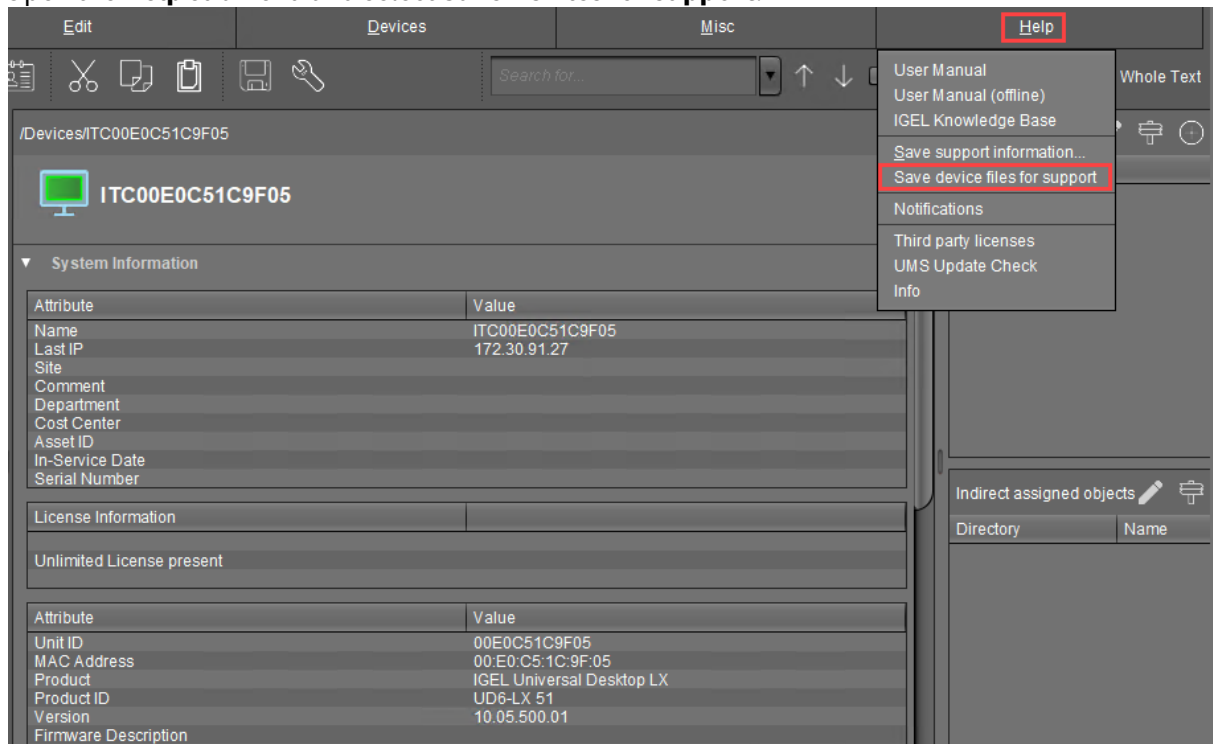1. Start the UMS Console and enter your **User Name** and **Password**.
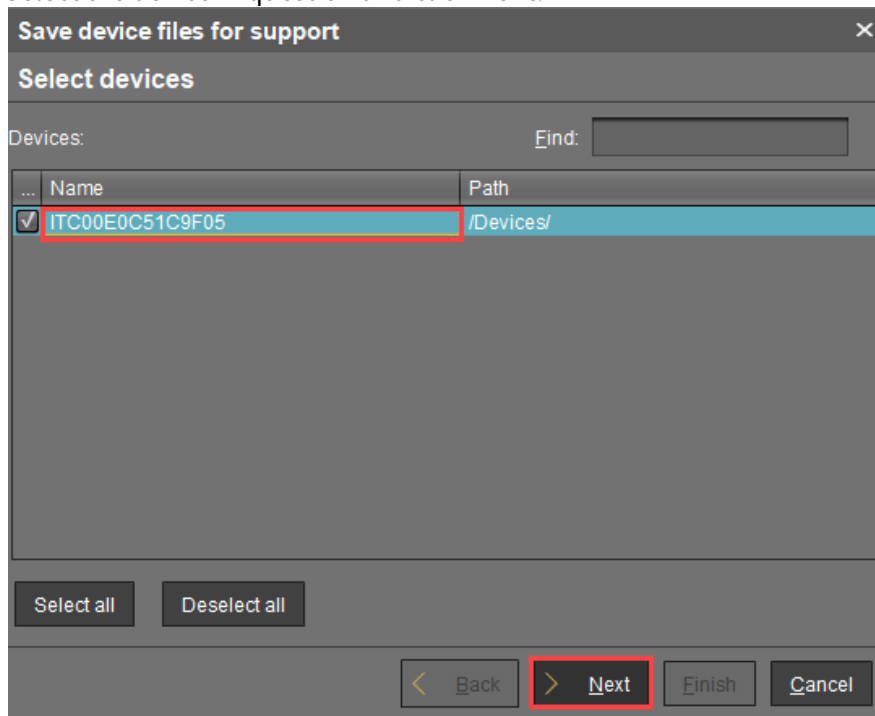

2. Click **Connect**.

   The UMS Console window opens.

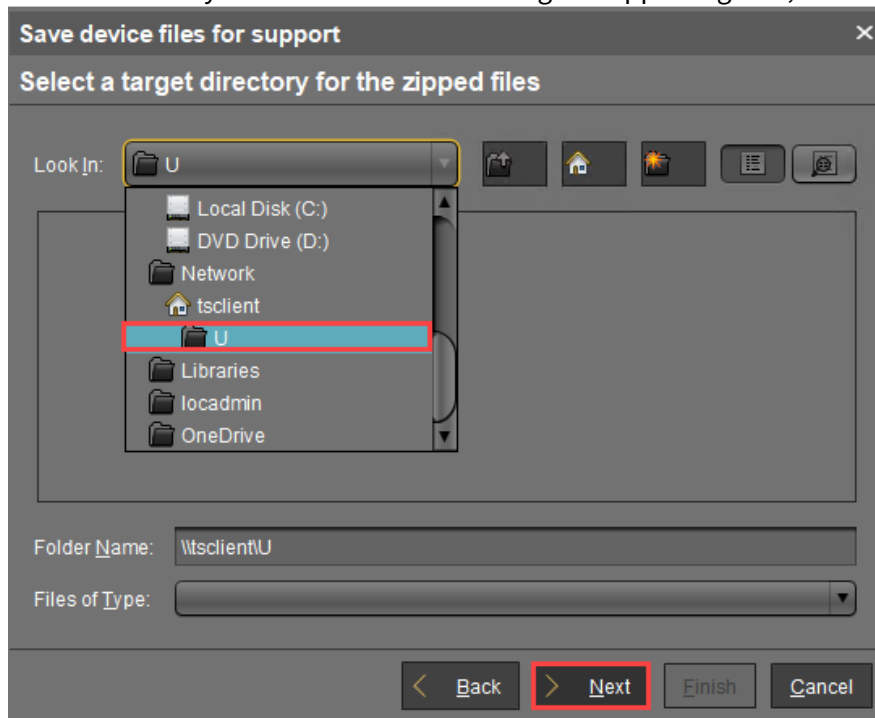3. Open the **Help** submenu and select **Save TC files for support**.

The dialog **Save TC files for support** opens.
4. Select the device in question and click **Next**.

The dialog **Select a target directory for the zipped files** opens.

5. Select a directory which is suitable for saving the zipped log files, and click **Next**.
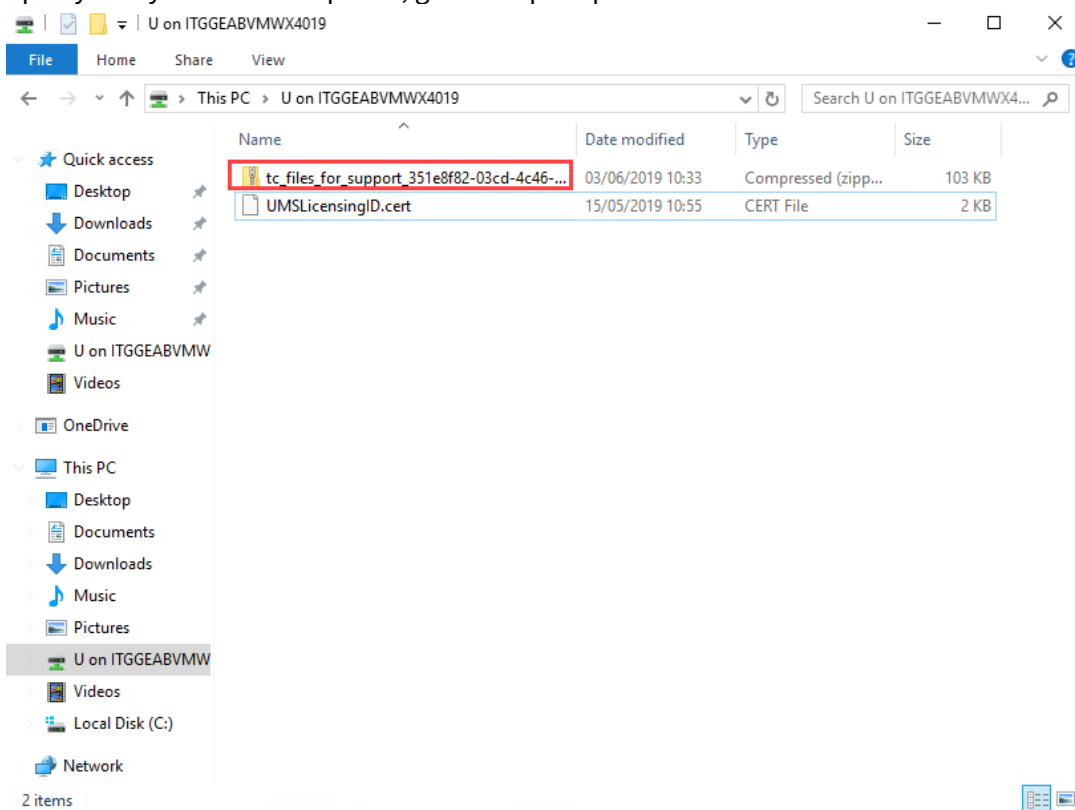

A confirmation dialog shows the path and file name under which the log files are stored.

> (i) Depending on your system, you can copy the path using [Ctl] + [C] and paste it into the File Explorer's address bar.
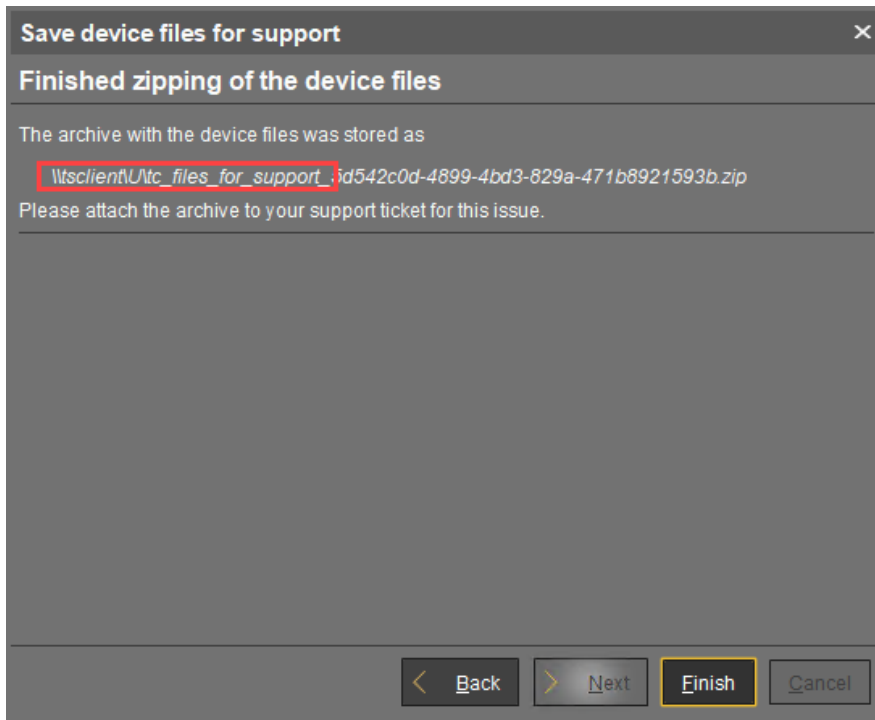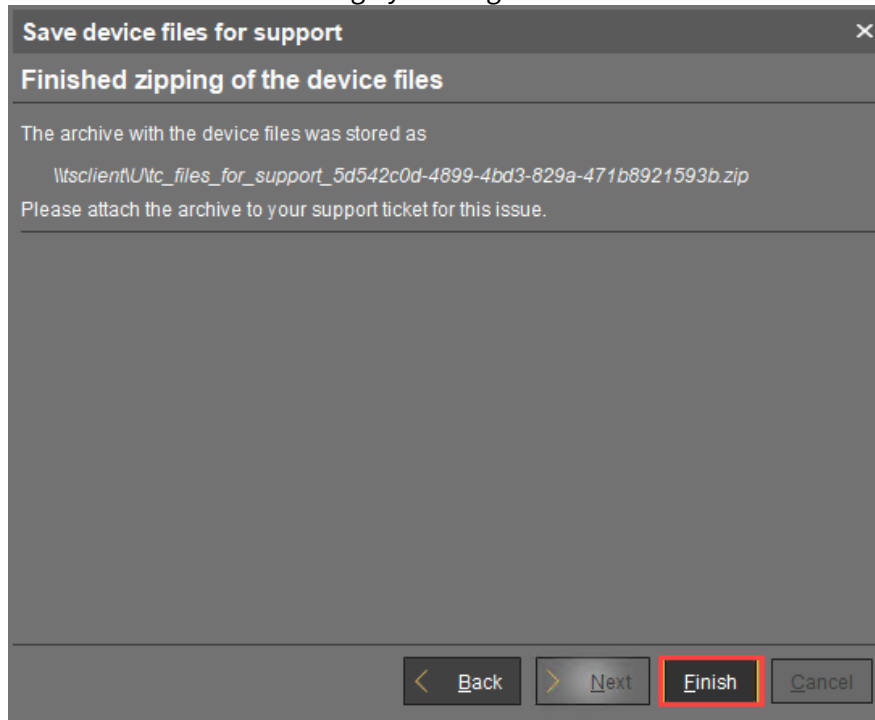
6. Open your system's File Explorer, go to the path portion of the file location.

7. Send the ZIP file to the IGEL support team.

8. Close the confirmation dialog by clicking **Finish**.

ⓘ The above procedure collects only those logs that have been written since the last system start. To allow persistent logs, you can configure a dedicated partition for debug logs. For more information, also on adding additional logs, see Extended Logging With Syslog, Tcpdump and Netlog (see page 187).

Without UMS

When the UMS is not accessible or there is an issue with network connectivity, you can still extract system logs from a device and send them to support. You will need a USB stick, preferably formatted to NTFS format, to transfer the logs to.

Setting Up the Device

1. In the IGEL Setup, go to **Devices > Storage Devices > Storage Hotplug** and enable **Storage Hotplug**.
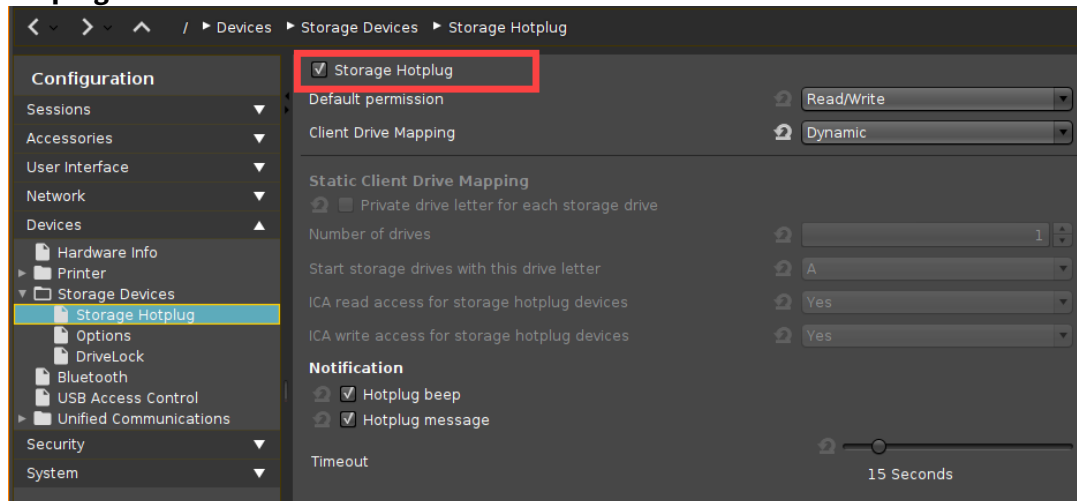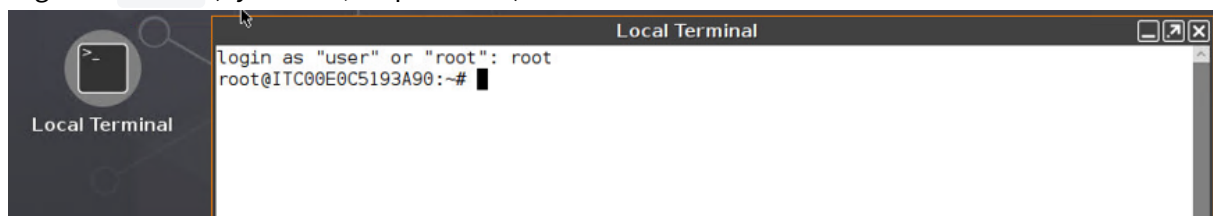

2. Under **Accessories > Terminals**, click ⊞ to create a terminal session.
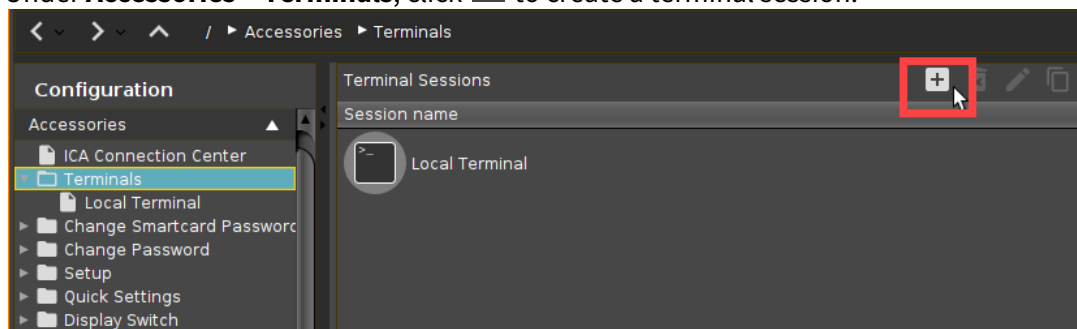
Identifying the USB Stick

1. Plug the USB stick into the IGEL OS device and start the terminal session.
2. Log in as `root` (by default, no password).

3. Enter the following commands:

`cd /userhome/media`

`ls -l`

4. Note the name of the USB stick:

Writing the Log File

1. In the terminal, run the command `cd /userhome/media/[Name of your USB stick]`.

   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`.

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.

IGEL

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 .
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\`

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.
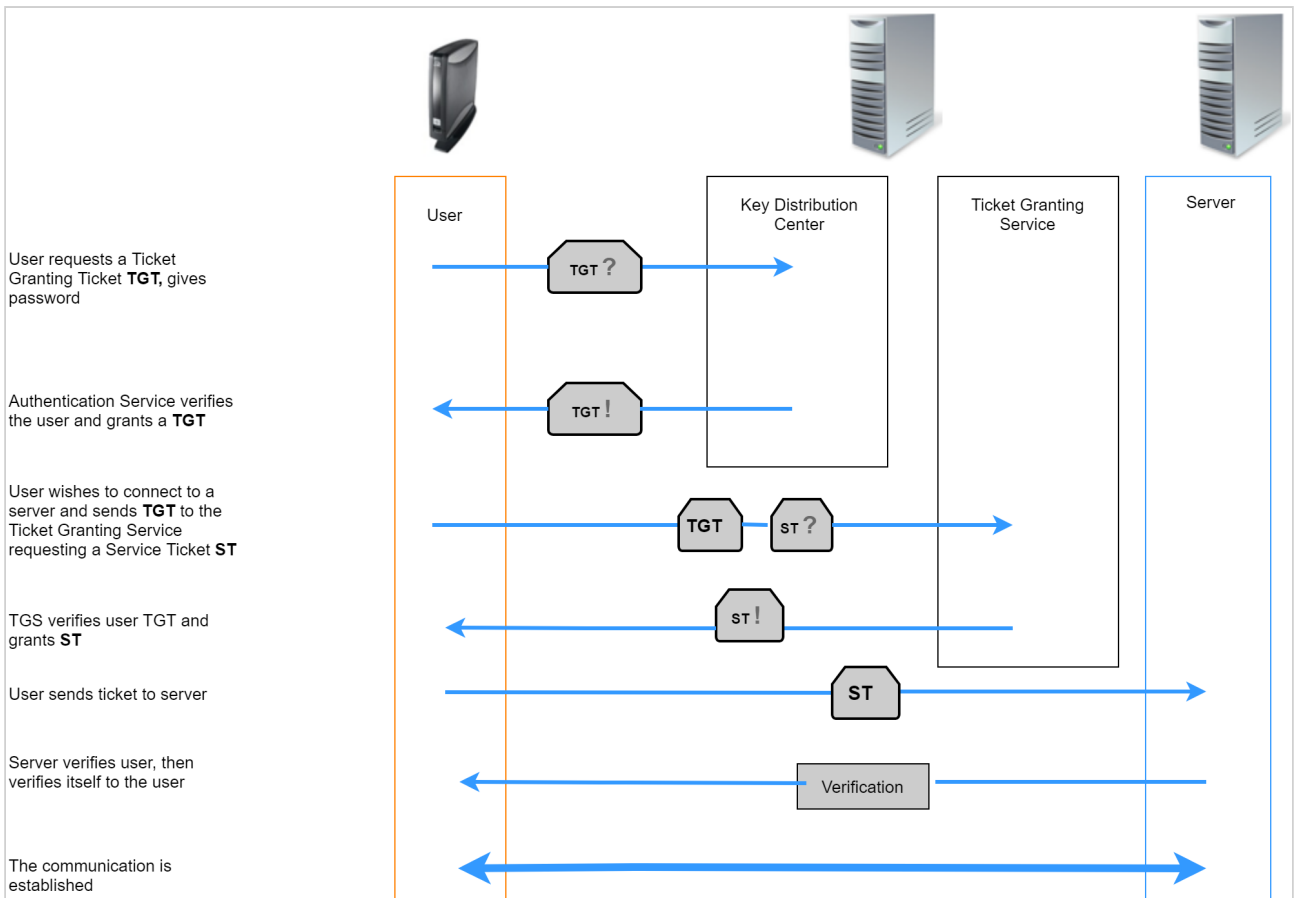
To enable passthrough authentication you have to make certain settings:

1. Modify certain basic settings which are necessary to fulfill the conditions for Kerberos passthrough authentication. (see page 517)
2. Enable passthrough authentication in the relevant session. (see page 524)

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 518)
- Configure the domain. (see page 519)
- Activate login to the Active Directory domain. (see page 521)

> ⓘ When activating the **Smartcard** login method, some additional configuration may be necessary (see page 522).

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.

IGEL

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 under **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.
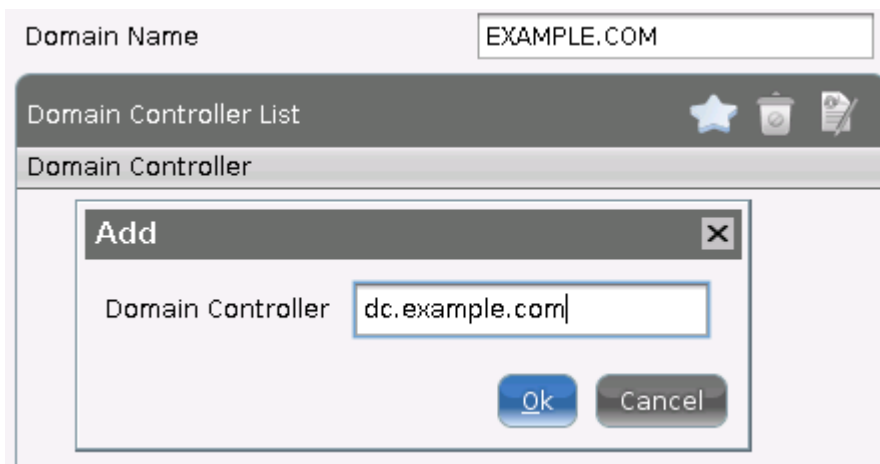
1. Click **Security > Active Directory/Kerberos > Domain Realm Mapping** to define the mapping between *Active Directory* domain names and DNS names.
2. Activate **Use default DNS Domain - Active Directory Domain Mapping**.

ⓘ If both names match, i.e. if a host in the domain `EXAMPLE.COM` has the DNS name `host.example.com`, nothing needs to be done here and the default setting is sufficient. Otherwise an appropriate entry in the **Domain Realm Mapping** list has to be created.

IGEL

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 **Logoff shortcut locations**, specify where a log-off button will appear.

IGEL

Smartcard

For using the **Smartcard** login method, some additional configuration is necessary:

1. Under **Security > Login > Active Directory/Kerberos**, activate **Smartcard**.
2. Under **Smartcard removal action**, define what should happen when the smartcard is removed:
    - **Log off**: Performs a disconnect or log off of running sessions, removes all user related data from the thin client and prepares the thin client for the next user login.
    - **Lock Thin Client**: Locks the screen during sessions. Only the user who is already logged in can unlock the thin client 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 > Custom PKCS#11 module**.

> ⓘ 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 thin client. Either the root certificate is one of the public trusted certificate authorities or it must be deployed to the thin client, see Deploying Trusted Root Certificates .

> ⓘ 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

IGEL

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:

IGEL

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**.

IGEL

Citrix StoreFront/Web Interface

1. Go to **Sessions > Citrix XenDesktop / XenApp > Citrix StoreFront/Web Interface > Login**.
2. Select the **Authentication type**:
   - **Kerberos Passthrough authentication (Web Interface only, not StoreFront)**: This will only work with Web Interface, not with StoreFront.
   - **Password authentication**: To enable passthrough this option must be selected, and **Use Passthrough authentication** must be activated.
   - **Smartcard authentication**: 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**

IGEL

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**.

IGEL

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.
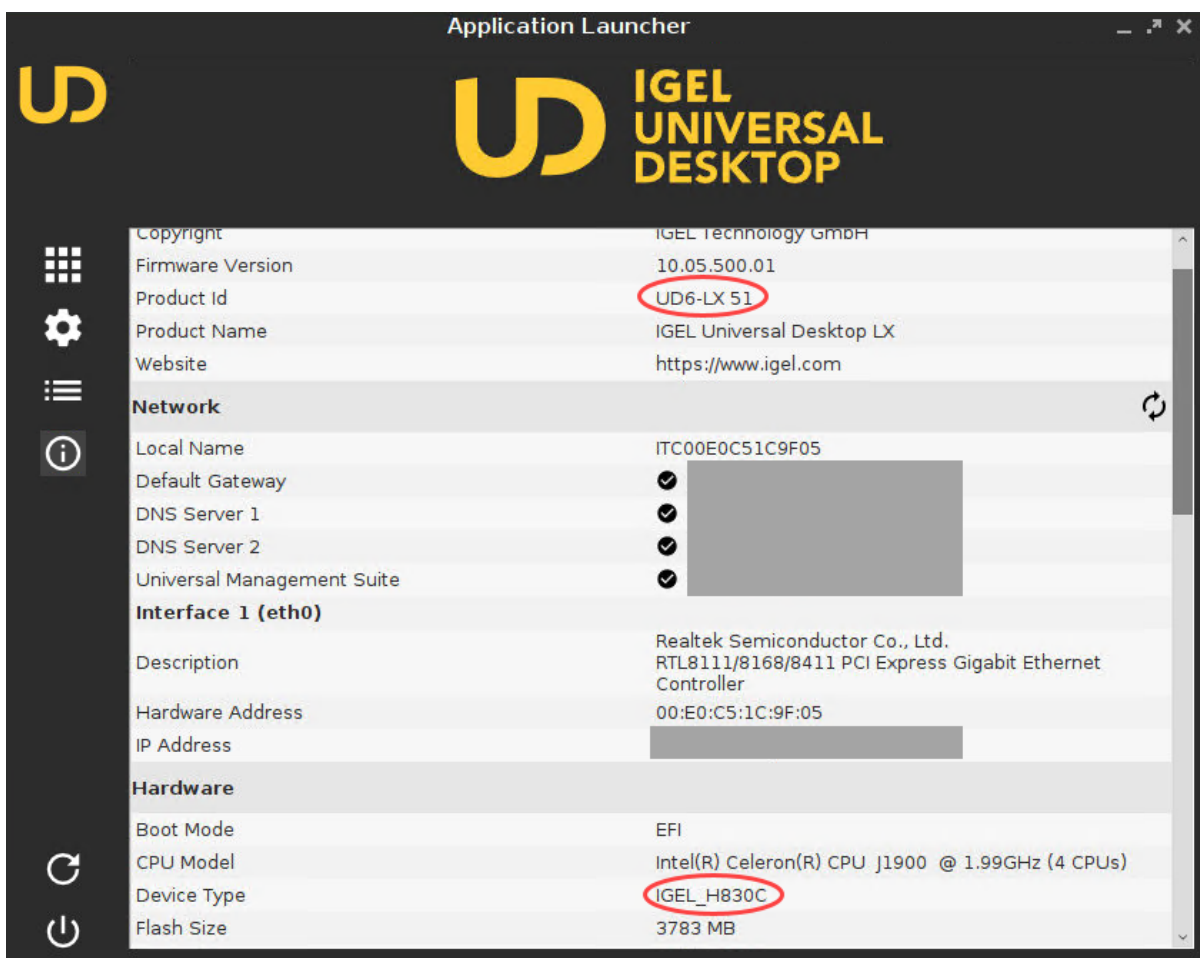
Hardware Video Acceleration on IGEL OS

Question

Does my hardware with IGEL OS offer video acceleration?

Answer

Open **Application Launcher > About** to look up your product ID and device type:

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	✓	✓	

IGEL

> ⓘ 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:
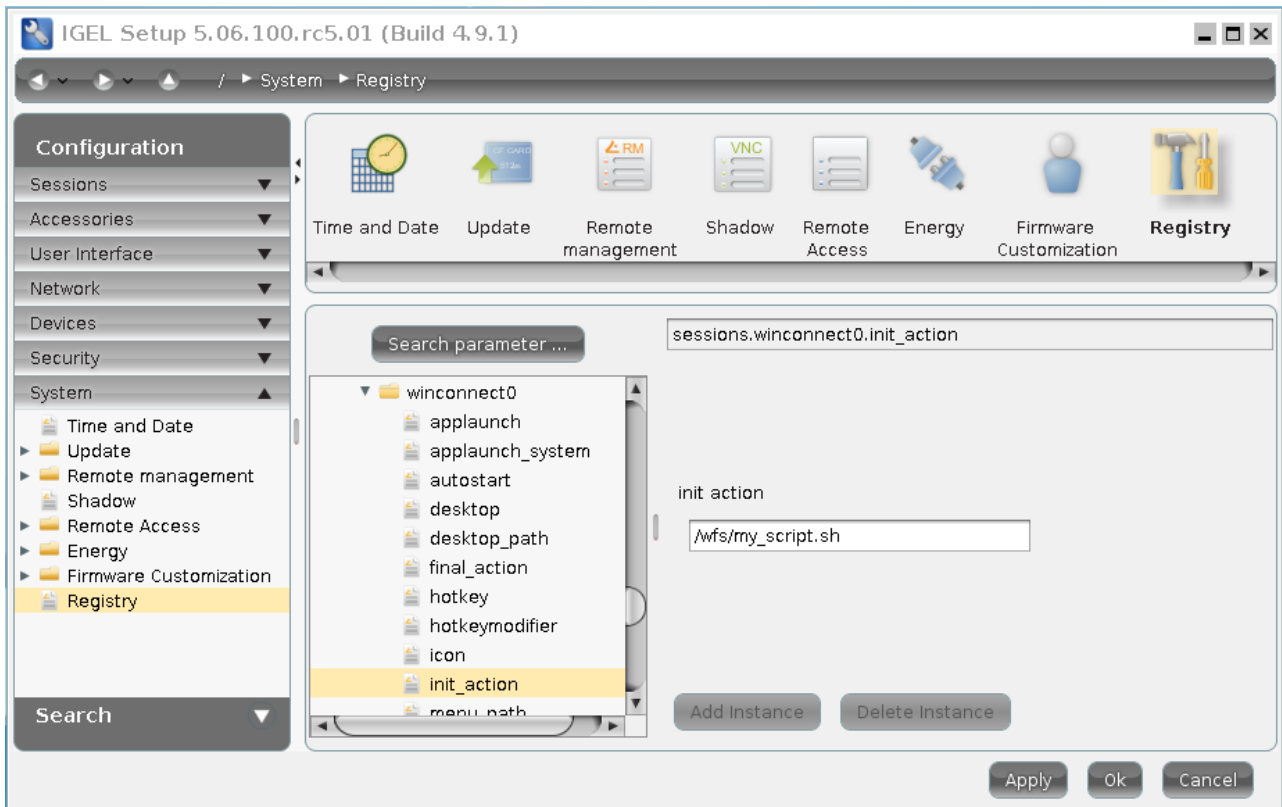
ⓘ The Registry keys for newly created sessions only appear after a restart of **Setup**.

ⓘ 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.

IGEL

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

IGEL

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.

IGEL

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.
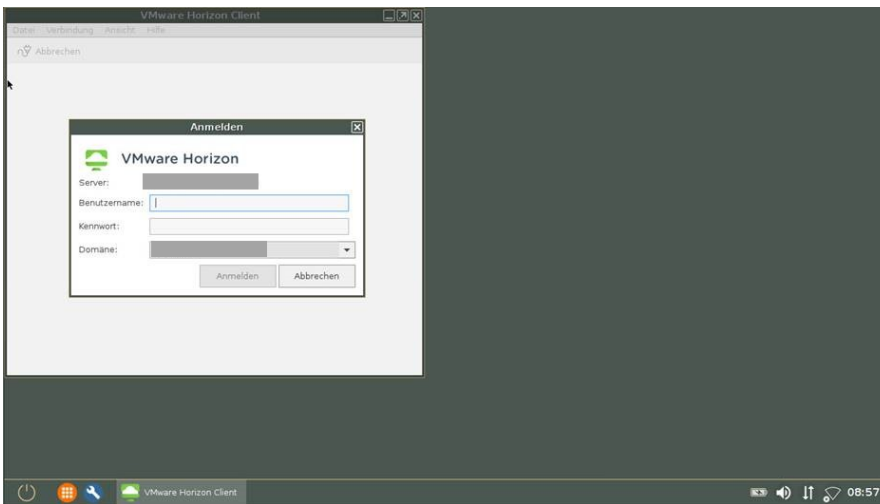
Solution

To start the IGEL Setup within the appliance mode, press hotkey [Ctrl+Alt+F2].

IGEL

An Application Window Cannot Be Repositioned

Symptom

Some application windows, e.g. VMware Horizon windows, are placed at startup in the upper left corner instead of being displayed in the middle. In case of frameless applications, the window cannot then be moved and may conceal the icons.

Problem

Either the screen is too small or the selected resolution is too low.

Solution

1. Go to **System > Registry**.
2. Select the registry key `windowmanager.wm0.variables.placement_ratio`.
3. Specify a higher percentage value under **Maximum window size for which the preferred placement should apply**. This entry refers to the total work area.

> ⓘ The preferred placement is defined with the registry
> key `windowmanager.wm0.variables.placement_mode`.
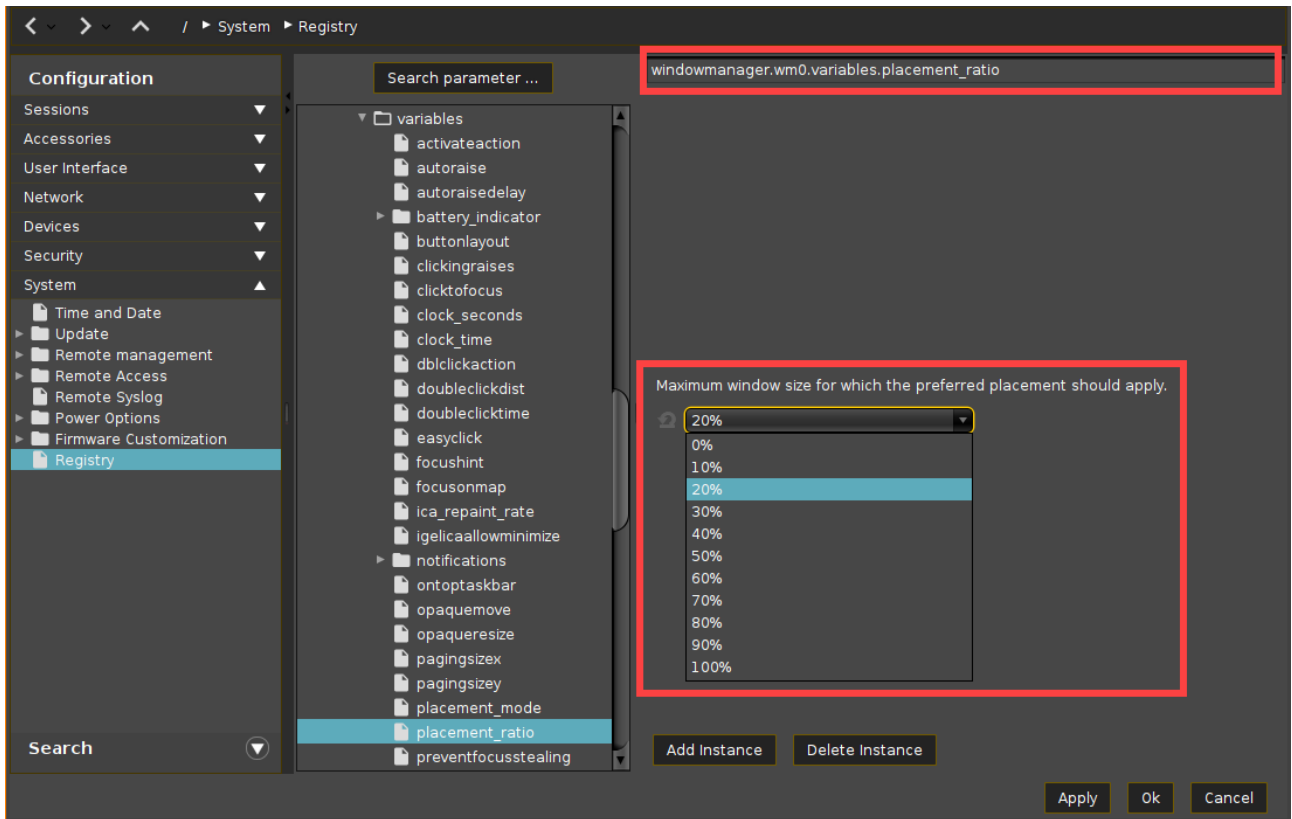
Example

Session: VMware Horizon Client
Screen resolution: 1366x768
Value for **Maximum window size for which the preferred placement should apply**: at least 40%

IGEL

Updating IGEL UMD: Error "not compatible with System5"

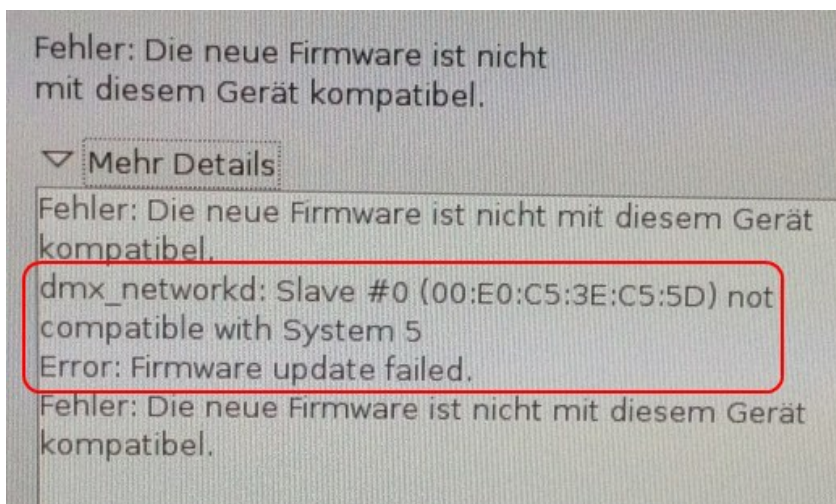### Symptom

Universal Multi Display firmware (IGEL UMD) can't be updated to version 4.13.100.

Error Message:

```
Firmware not compatible.
dmx_networkd: Slave #0 (MAC) not compatible with System5
```


Solution

Delete file `/tmp/NOT_SYS_5_COMPATIBLE` from UMD master client and update again without rebooting.

IGEL

IGEL Linux Features that Require the Multimedia Codec Pack

Some features in IGEL Linux 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 530) is available.

Here is an overview of the affected IGEL setup pages and parameters:

Use Case	Setup Page	Parameter	Feature
Citrix Session	**Sessions > Citrix XenDesktop/XenApp > HDX/ ICA Global > HDX Multimedia**	**Enable Multimedia Redirection**	Redirection of H.264, WMV, MPEG-1, MPEG-2, MPEG-4 ASP (DivX, Xvid) videos, WMA and MP3 audio
	Sessions > Citrix XenDesktop/XenApp > HDX/ ICA Global > Codec	**Graphical Codec**	Citrix H.264 deep compression codec support
	Sessions > Citrix XenDesktop/XenApp > HDX/ ICA Global > HDX Multimedia	**Enable HDX Realtime Media Engine**	Skype for Business H.264 with HDX Realtime Media Engine (RTME)

Use Case	Setup Page	Parameter	Feature
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**	**Enable 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	**Enable VMware 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