IGEL Apps

All apps for IGEL OS 12 devices can be found on the IGEL App Portal https://app.igel.com/.

Difference between Apps Created by IGEL and Apps Created by IGEL Ready Partners

Detailed information on this topic can be found under Difference between Apps Created by IGEL and Apps Created by IGEL Ready Partners[1].

1. https://kb.igel.com/en/apps-created-by-igel-ready-partners/current/difference-between-apps-created-by-igel-and-apps-c

Amazon WorkSpaces Client



Amazon WorkSpaces is a cloud-native desktop virtualization, which is built on the AWS Cloud and used to provide Windows or Linux desktops.

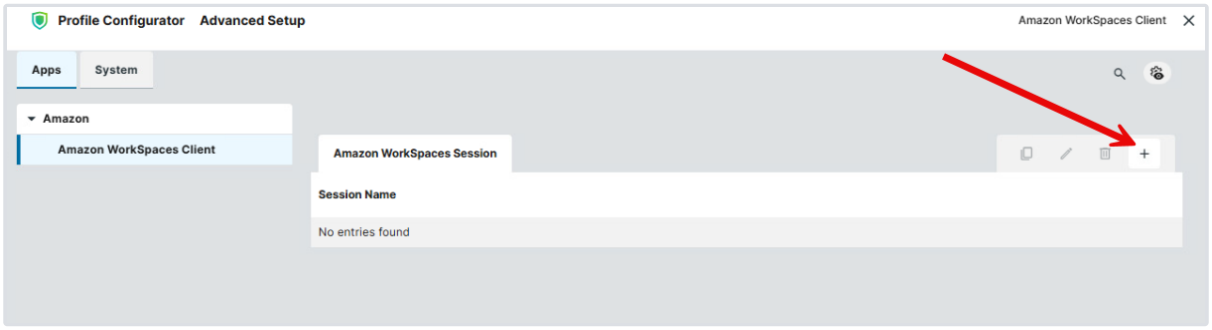
Using Amazon WorkSpaces Client, you can configure Amazon WorkSpaces sessions on IGEL OS. For details on how to import the app to your IGEL Universal Management Suite (UMS), see How to Import IGEL OS Apps from the IGEL App Portal[2].

Requirements

- An existing Amazon WorkSpaces account is required. To set up your account, visit https://aws.amazon.com/workspaces/.

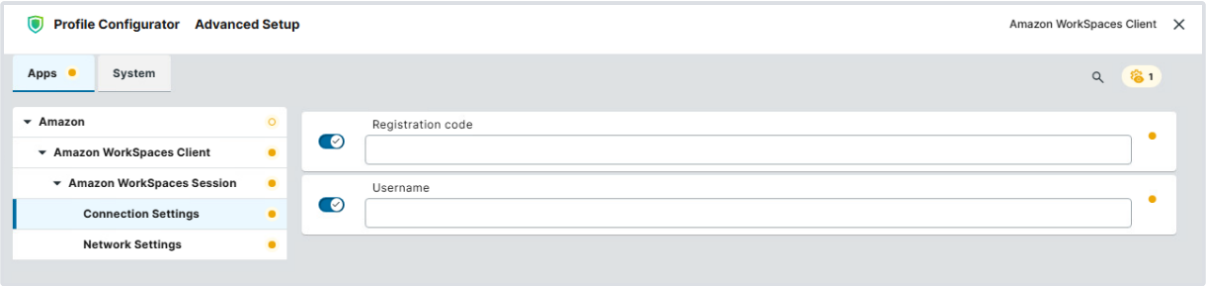
How to Configure Amazon WorkSpaces Client

1. In the IGEL UMS, create a profile configuring the Amazon WorkSpaces Client app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[3].
2. In the profile configurator, go to **Apps > Amazon > Amazon WorkSpaces Client** and click **+** to create a session:



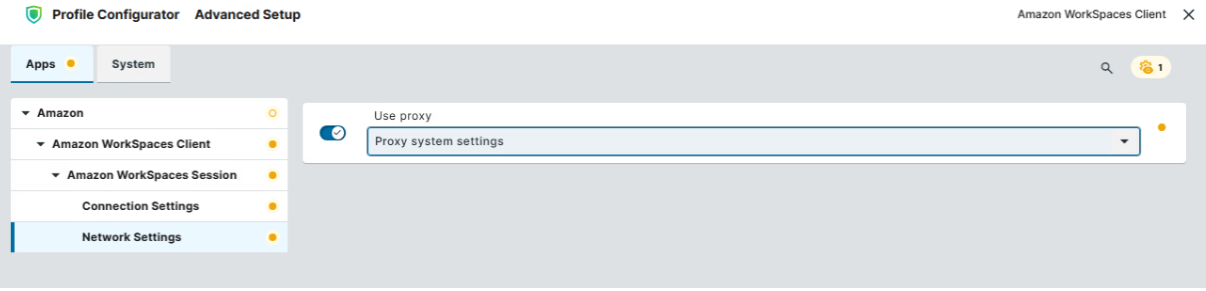
3. Configure the starting methods for the session. The starting methods parameters are described under Starting Methods for Apps[4].
4. Under **Apps > Amazon > Amazon WorkSpaces Client > [Session Name] > Connection Settings**, define the following settings:

2. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
3. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-
4. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps



Registration code
The WorkSpaces registration code which you got from Amazon
Username
Username used to log in to Amazon WorkSpaces

5. Under **Apps > Amazon > Amazon WorkSpaces Client > [Session Name] > Network Settings**, define the following settings:



Use proxy
Possible values:

- **No proxy**: No proxy is used.
- **Proxy system settings**: The proxy configured for the IGEL OS base system under **Network > Proxy**[5] is used. (Default)
- **Custom proxy settings**: The proxy settings configured in the following fields will be used.

  Proxy address
  Hostname or IP address of the proxy server
  Proxy port
  Port on which the proxy service is available

5. https://kb.igel.com/en/igel-os-base-system/current/proxy-configuration-in-igel-os-12

Chromium Browser



- Getting Started with the Chromium Browser in IGEL OS (see page 7)
- Configuration of the Chromium Browser in IGEL OS (see page 11)
- Troubleshooting: Cannot Download Outlook E-amail Attachments (see page 30)
- Troubleshooting: Cannot Log into MS Teams in Chromium Browser (see page 31)

Getting Started with the Chromium Browser in IGEL OS

This article describes how you can create a Chromium browser session and configure it on IGEL OS.

Changes as of Chromium Browser app version 142.0.7444.175:
The dependency on the apps "Chromium Multimedia Codec" and "libva for Chromium" was removed, as they are no longer required with IGEL OS Base System 12.7.2 or later.
Note: These components must be unassigned if they were previously added manually. If they were installed via Chromium Browser app, they will automatically be deleted during the Chromium Browser update.

Requirements

- Chromium browser app is imported to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[6].

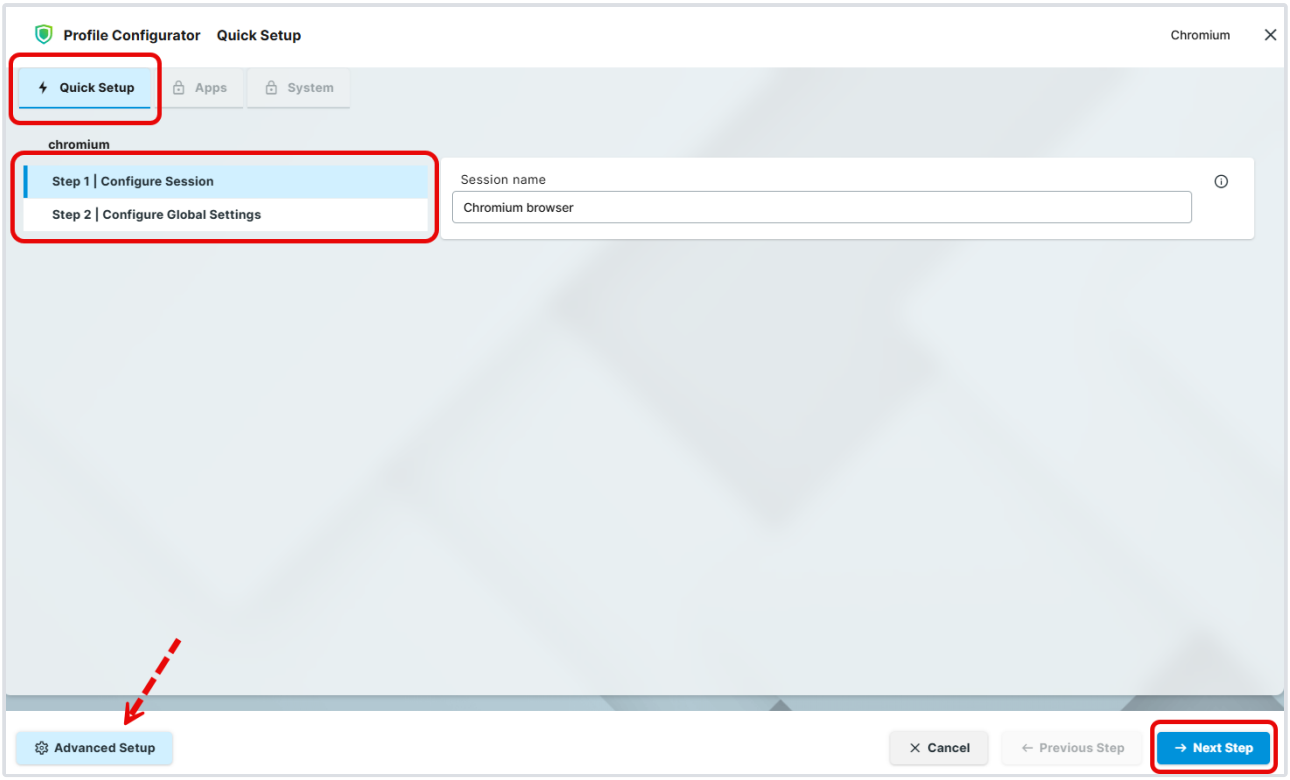
How to Create a Session

This app has Quick Setup mode available...

To quickly create a Chromium session and configure the basic settings, you can use Quick Setup mode when creating a profile configuring the app. For detailed information on profile creation and Quick Setup mode, see How to Create and Assign Profiles in the IGEL UMS Web App[7].

→ To display all available app settings, click **Advanced Setup**.

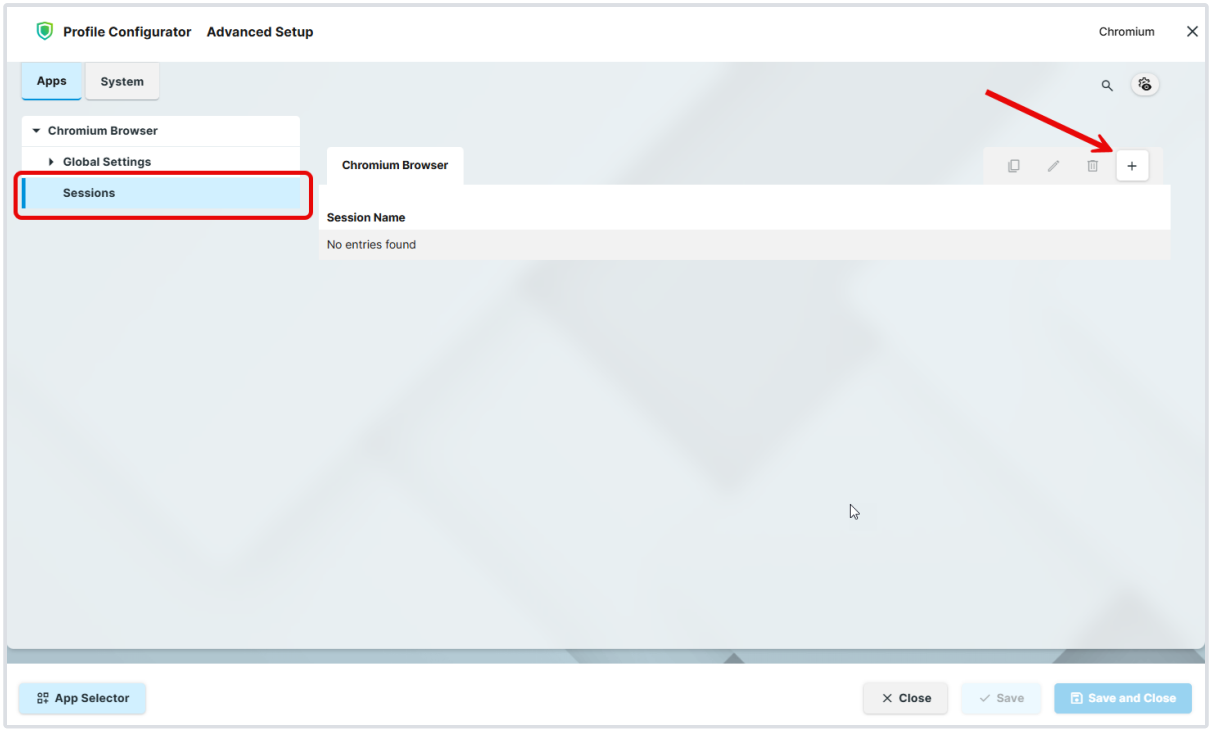
6. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
7. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



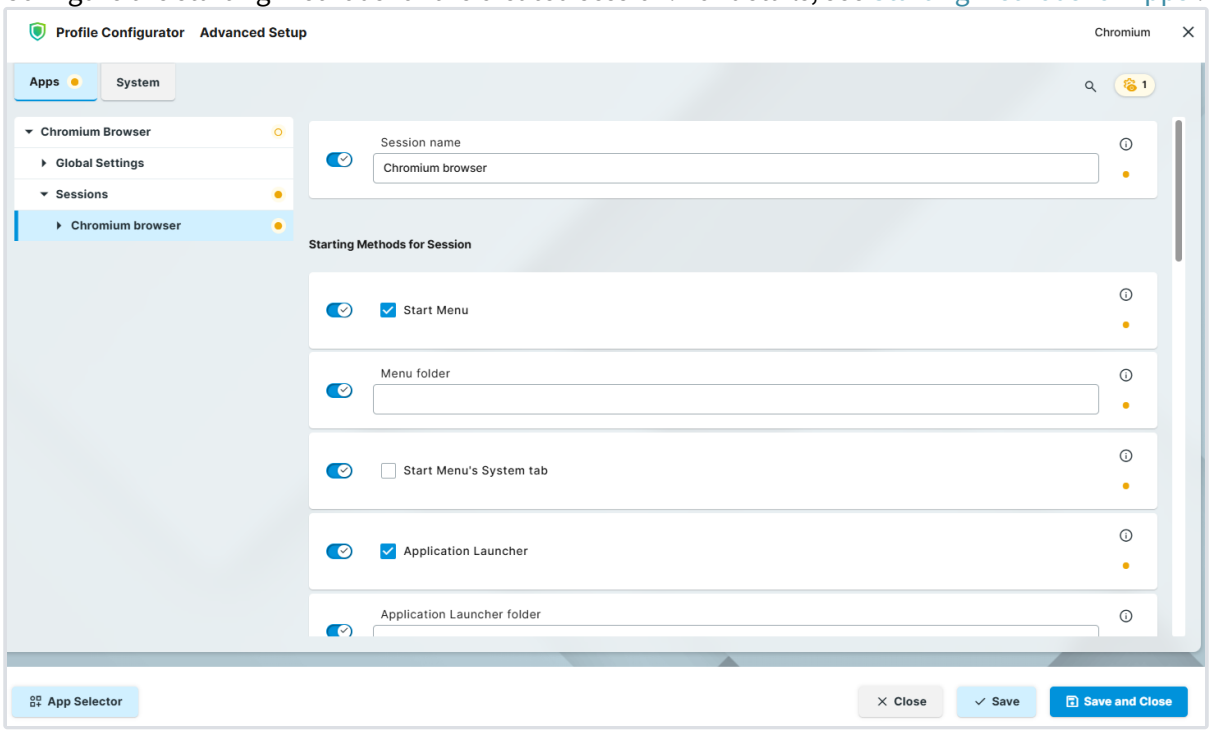
This is how you can create a Chromium browser session via the profile configurator using Advanced Setup mode with all settings available for configuration:

1. In the IGEL UMS, create a profile configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[8].
2. In the profile configurator, go to **Apps > Chromium Browser > Sessions** and click **+**.

8. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



3. Configure the starting methods for the created session. For details, see Starting Methods for Apps[9].



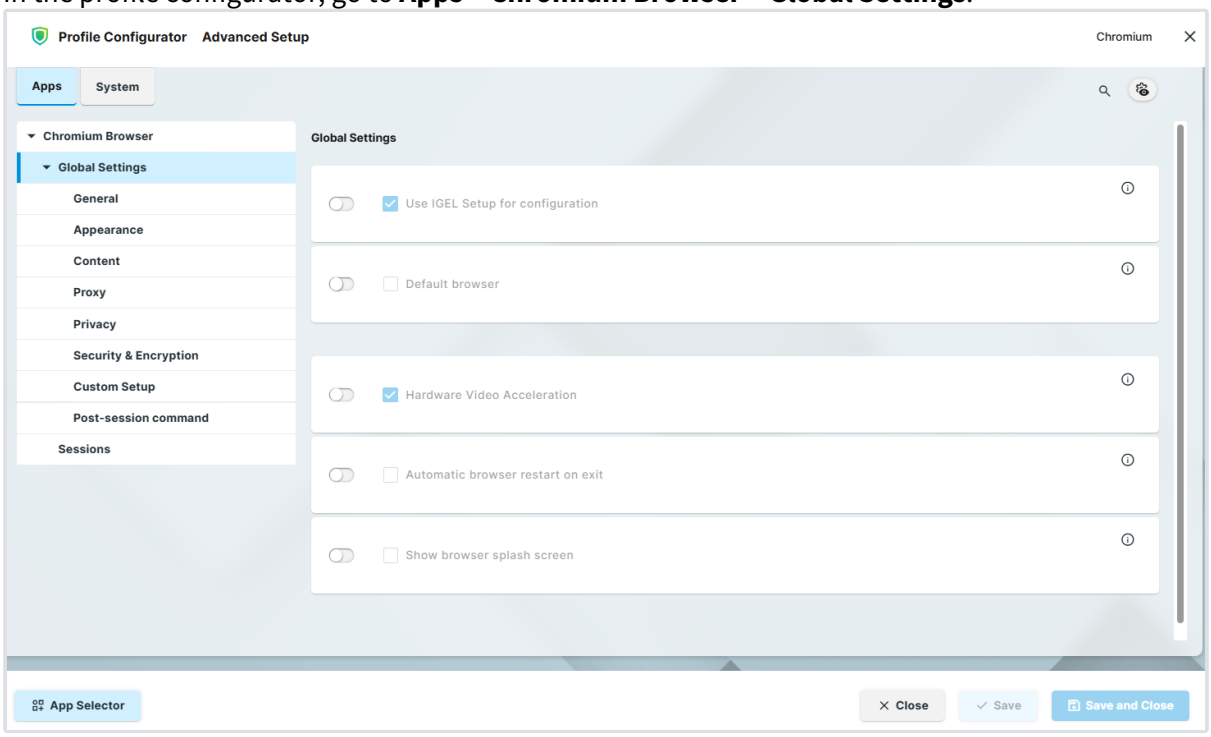
9. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

4. Edit the settings according to your needs. For details, see Configuration of the Chromium Browser in IGEL OS (see page 11).

Configuration of the Chromium Browser in IGEL OS

Configuring Global Settings

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings**.



2. Edit the settings according to your needs. The parameters are described in the following.

Use IGEL Setup for configuration

- ☑ The settings made in the IGEL Setup or the UMS configuration dialog will be effective. (Default)
- ☐ The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

Default Browser

> ⚠ **Importance of Setting a Default Browser Correctly**
> Please note the following:
> - If several browsers are installed and no browser is set as default, the browser whose name is last in alphabetical order is the default. Example: If Chromium, Edge, Firefox, and Island are installed and no default browser is set, Island will be the default browser.

- If several browsers are erroneously set as default, the browser from this selection whose name is last in alphabetical order will be the actual default.

- [x] Chromium is the default browser.
- [ ] Chromium is not the default browser. (Default)

Hardware Video Acceleration

- [x] Hardware video acceleration is enabled for the Chromium browser. (Default)
- [ ] Hardware video acceleration is disabled for the Chromium browser.

Automatic browser restart on exit

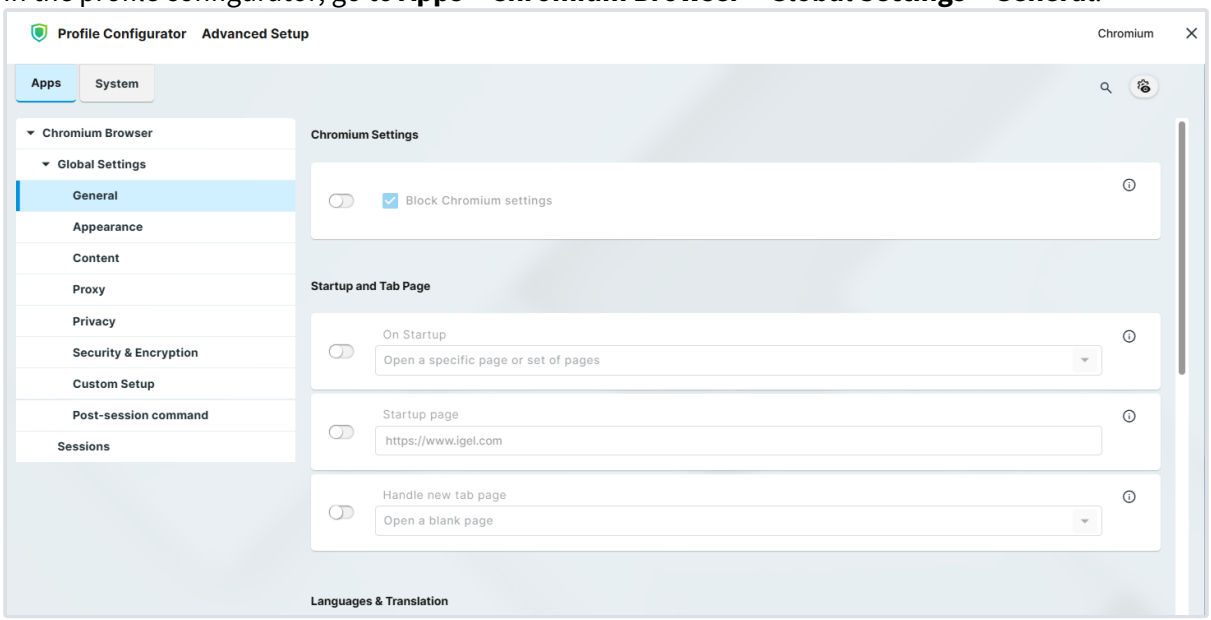
- [x] Chromium is restarted when the user closes it.
- [ ] Chromium is not restarted on exit. (Default)

Show browser splash screen

- [x] The Chromium splash screen is shown at the start.
- [ ] Chromium starts without a splash screen. (Default)

Configuring General Settings

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > General**.



2. Edit the settings according to your needs. The parameters are described in the following.

Block Chromium Settings

- ☑ The Chromium URL chrome://settings (see page 11) is blocked to prevent users from changing Chromium settings. (Default)
- ☐ The user can change Chromium settings via chrome://settings (see page 11).

On Startup

Specifies what is displayed on browser startup.

- **Open the New Tab page**
- **Open a specific page or set of pages**: The page or set of pages defined by **Startup page** is displayed. (Default)
- **Continue where you left off**

Startup page

This parameter is only shown when **On Startup** is set to **Open a specific page or set of pages**.

Specifies the page or set of pages to be shown when the user opens a new tab. This is effective only if **On Startup** is set to **Open a specific page or set of pages**. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". (Default: "https://www.igel.com")

Handle new tab page

Defines the content of a new tab.

Possible options:

- **Open a blank page**
- **Open a specific page**

Languages

One or more preferred languages for multilingual websites, given in the form of language abbreviations separated by commas. The languages should be given in the order of preference. Example: With "de, en, fr, it", the website will be shown in German, if available, otherwise in English, and so on.

Use spell check for

Defines the languages which should be spell-checked, separated by a comma. Example: With "de, en", a spell check is performed for German and English pages. If the field is left empty, the default language is spell-checked.

Integrated translation service of Chromium

- ☑ When a web page has a language that differs from your system language, Chromium will offer to translate the page. (Default)

Menu & interface language

The language into which Chromium menus and interface will be translated.

Possible values:

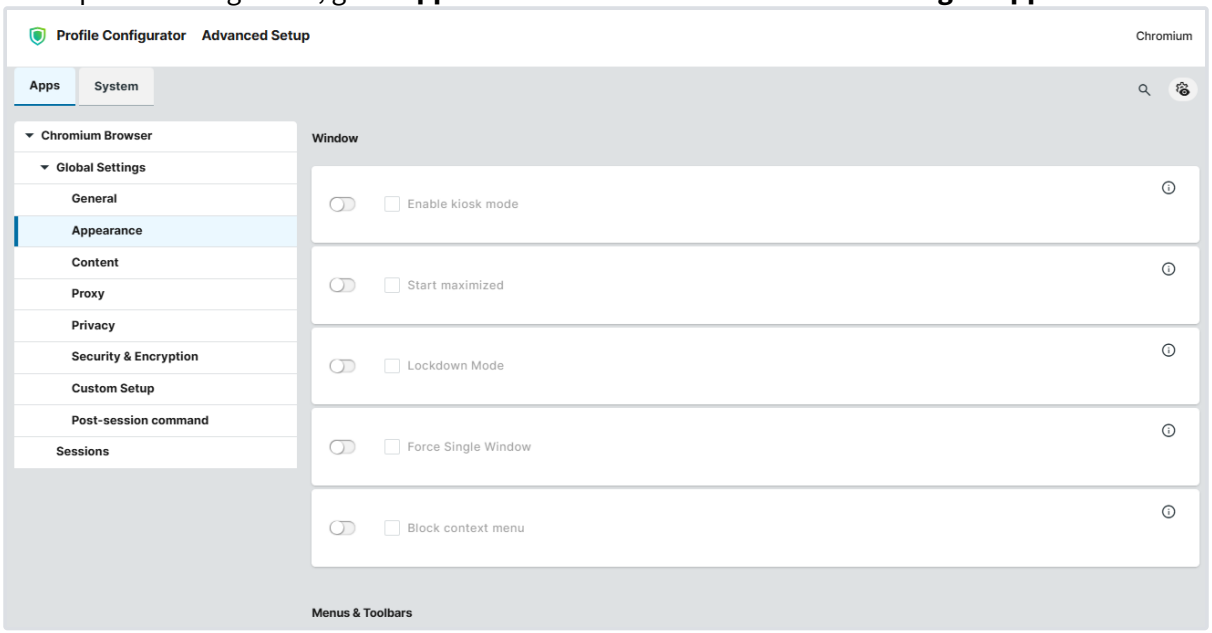
- **System default**: Sets the language you configured under **User Interface > Language > Language**. (Default)
- List of possible languages…

Autoplay

- ☑ Embedded audio and video content on a web page is played automatically when the page is loaded.
- ☐ Audio and video content is not played automatically. (Default)

Configuring the Browser Appearance

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Appearance**.



2. Edit the settings according to your needs. The parameters are described in the following.

Enable kiosk mode

- ☑ Chromium starts in kiosk mode.
- ☐ Chromium starts in normal mode. (Default)

Start maximized

- ☑ Chromium starts in a maximized window.
- ☐ Chromium starts in a window with a default size. (Default)

Lockdown mode

- ☑ The user will not be able to leave the main browser window. New tabs and windows are blocked. Note that browser windows that are not on the same Chromium profile can still be opened, which means you can open a Progressive Web App if Chromium is opened.
- ☐ The user can leave the main browser window. New tabs and windows can be opened. (Default)

Force single window

- ☑ Links are always opened in the same window / tab. New windows or tabs opened externally, e.g. via `Ctrl+N`, `Ctrl+T`, are not blocked.
- ☐ New tabs and windows are not redirected to the main window. (Default)

Block context menu

- ☑ The right-click context menu will be blocked.
- ☐ The right-click context menu will not be blocked. (Default)

Hide home button

- ☑ The home button will not be shown in the toolbar. (Default)
- ☐ The home button will be shown.

Hide bookmarks bar

- ☑ The bookmarks menu will not be shown in the menu bar. (Default)
- ☐ The bookmarks menu will be shown in the menu bar.

Font size

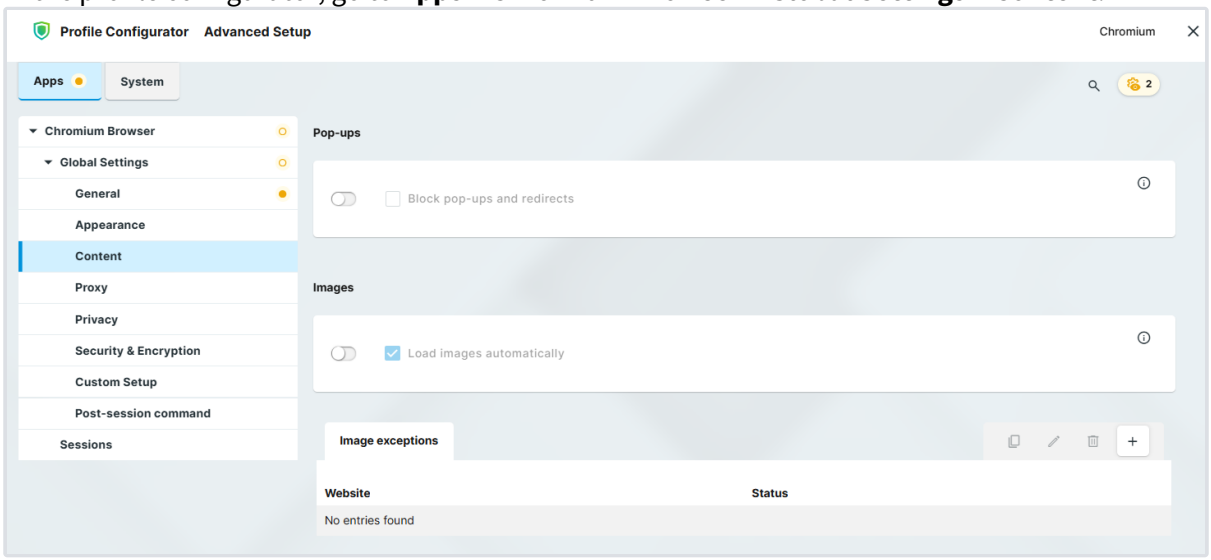
Changes the font size of the web content displayed in the browser window.

Possible options:

- **Very small**
- **Small**
- **Medium (recommended)** (Default)
- **Large**
- **Very large**

Configuring the Handling of Content: Pop-Ups, Images, and Downloads

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Content**.



2. Edit the settings according to your needs. The parameters are described in the following.

Block pop-ups and redirects

- ☑ Pop-up windows and redirects are blocked.
- ☐ Pop-up windows and redirects are allowed. (Default)

Pop-up exceptions

Add websites on which pop-up windows and redirects are not blocked.

Load images automatically

- ☑ Images from websites are loaded automatically. (Default)

Image exceptions

Add websites on which images are not loaded automatically.

Open PDFs externally

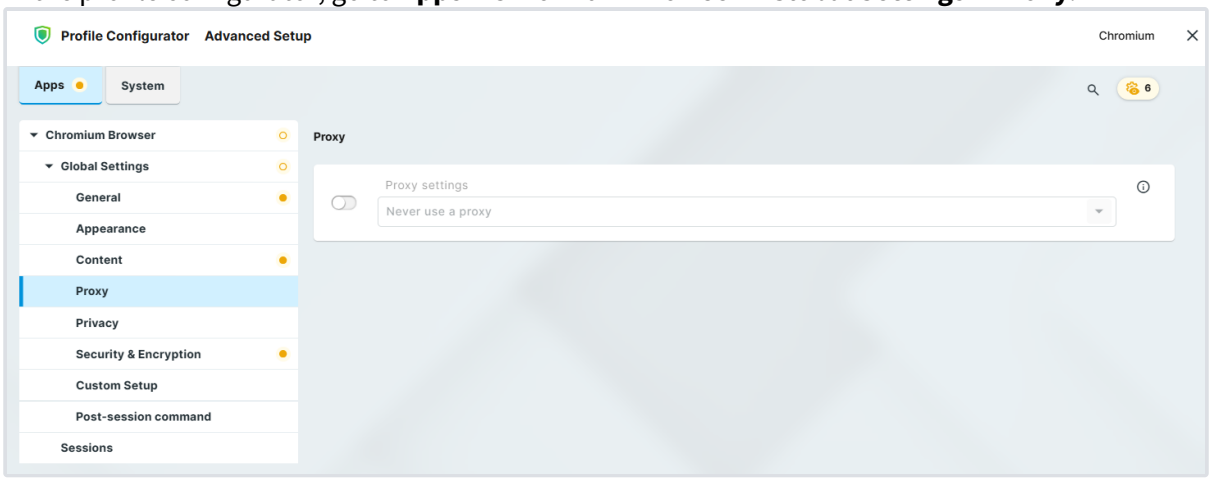
- ☑ PDFs are automatically opened externally, e.g. with Evince Document Viewer[10] if installed.

10. https://app.igel.com/evince/43.1.2+1

- [ ] PDFs are opened with the internal PDF viewer. (Default)

Configuring the Proxy Settings

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Proxy**.

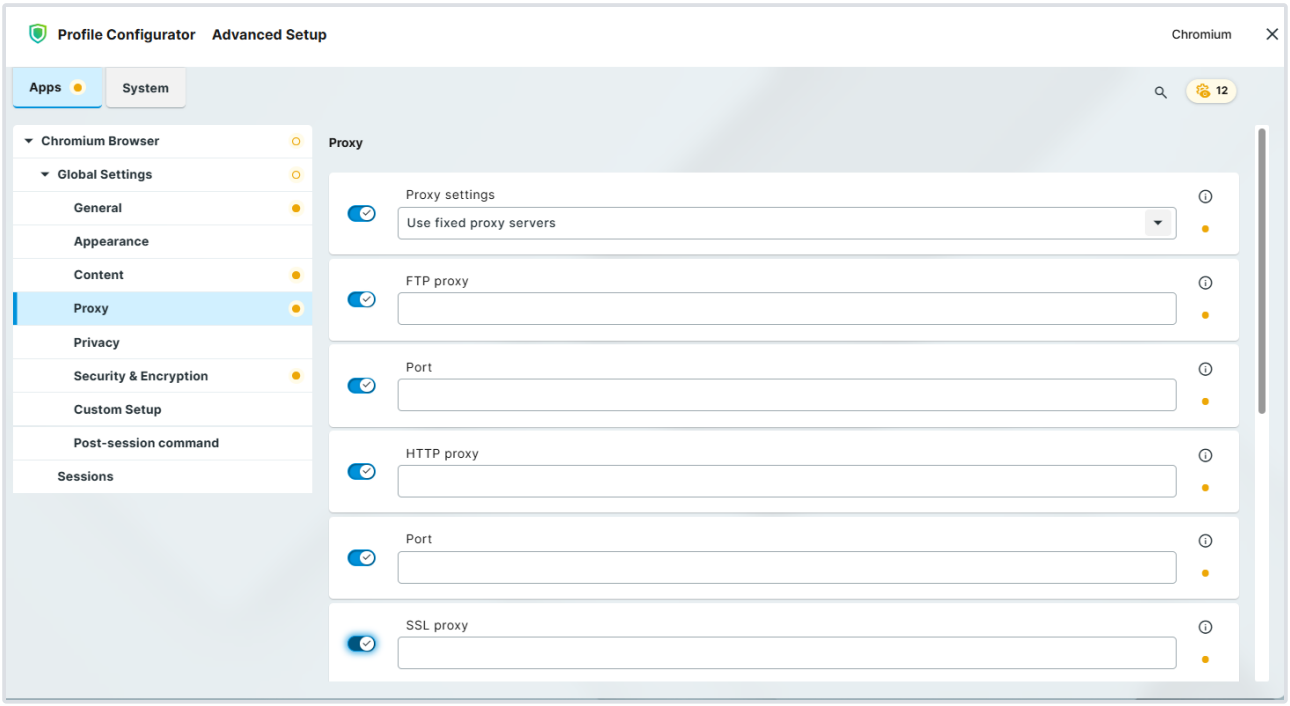


2. Select the proxy configuration according to your needs. The proxy configurations are described in the following.

Never use a proxy

With this proxy configuration, no proxy is used.

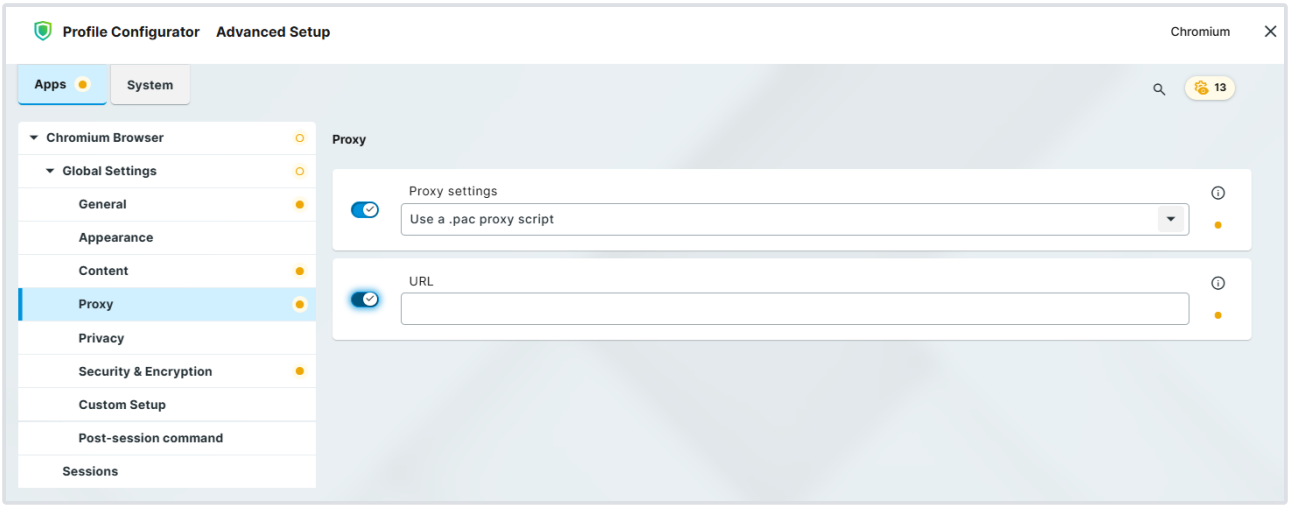
Use fixed proxy servers



The configuration data must be specified in the following fields.

- **FTP proxy**: URL of the proxy for FTP
- **Port**: Port of the proxy for FTP
- **HTTP proxy**: URL of the proxy for HTTP
- **Port**: Port of the proxy for HTTP
- **SSL proxy**: URL of the proxy for SSL
- **Port**: Port of the proxy for SSL
- **SOCKS host**: URL of the proxy for SOCKS
- **Port**: Port of the proxy for SOCKS
- **SOCKS protocol version**: Version of the SOCKS protocol used (default: SOCKS v5)
- **No proxy for**: List of URLs for which no proxy is to be used (default: "localhost, 127.0.0.1")

Use a .pac proxy script



With this proxy configuration, the PAC file (Proxy Auto Config) available under **URL** will be used.

- **URL**: URL of the proxy configuration file

Use system proxy settings

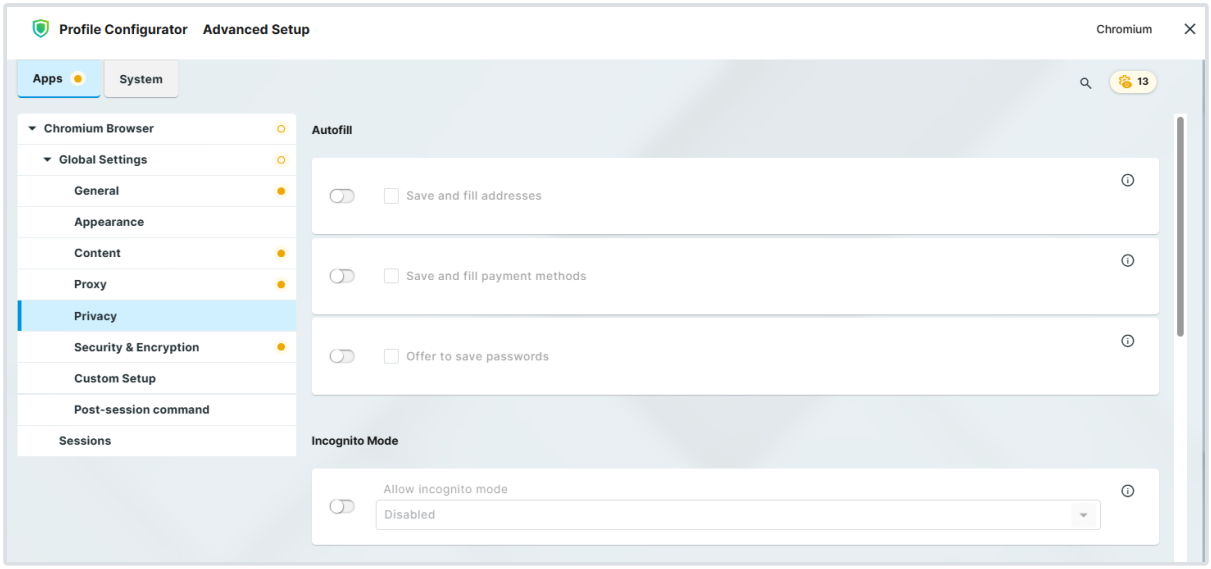
With this proxy configuration, the proxy configured under **Network > Proxy** will be used.

Auto detect proxy settings

With this proxy configuration, WPAD (Web Proxy Autodiscovery Protocol) will be used. The browser will determine the URL of the WPAD file `wpad.dat` automatically with the help of DNS.

Configuring the Privacy Settings

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Privacy**.



2. Edit the settings according to your needs. The parameters are described in the following.

Save and fill addresses

- ☑ Entries in forms and search bars will be retained after Chromium or the system restarts. Examples: Phone numbers, e-mail addresses, shipping addresses
- ☐ Entries in forms and search bars will be retained only for the duration of the session. (Default)

Save and fill payment methods

- ☑ Entries in payment forms will be retained after Chromium or the system restarts.
- ☐ Entries in payment forms will be retained only for the session duration. (Default)

Offer to save passwords

- ☑ Chromium offers to retain passwords after Chromium or the system restarts.
- ☐ Passwords entered will be retained only for the duration of the session. (Default)

Allow incognito mode

When the incognito mode is active, all data from private windows will be deleted after Chromium is closed.

Possible options:

- **Enabled**: The user can open browser windows in incognito mode.
- **Disabled**: The user cannot open browser windows in incognito mode. (Default)
- **Forced**: All browser windows started by the user are in incognito mode.

Enable "Do Not Track" feature

☑ Chromium will inform the website you are visiting that you do not wish to be tracked, i.e. you do not want your surfing history to be recorded. (Default)

The browser will use the `DNT` ("Do Not Track") field in the HTTP header for this purpose. Observing this setting is voluntary; from a technical point of view, websites can still record the surfing history even when `DNT` is set to 1.

Block third party cookies

☑ Third-party cookies are not accepted by Chromium. For details, see https://chromeenterprise.google/policies/#BlockThirdPartyCookies . (Default)

With some websites, the functionality might be limited if third-party cookies are blocked.

☐ Third-party cookies are accepted by Chromium.

Enable cookies allowlist for MS Teams

This parameter is visible if **Block third party cookies** is enabled.

☑ Enables the sites specified under **Cookies allowlist for MS Teams** to set cookies. Required to be able to sign in MS Teams. For more information, see Troubleshooting: Cannot Log into MS Teams in Chromium Browser (see page 31)

☐ The sites specified under **Cookies allowlist for MS Teams** are not enabled to set cookies. (Default)

Cookies allowlist for MS Teams

This parameter is visible if **Block third party cookies** is enabled.

Sets a list of URL patterns that specify sites which are allowed to set cookies.
Default value: `[*.]` microsoft.com[11] `;` `[*.]` microsoftonline.com[12] `;` `[*.]` teams.skype.com[13] `;` `[*.]` teams.microsoft.com[14] `;` `[*.]` sfbassets.com[15] `;` `[*.]` skypeforbusiness.com[16]

Autocomplete searches and URLs

11. http://microsoft.com
12. http://microsoftonline.com
13. http://teams.skype.com
14. http://teams.microsoft.com
15. http://sfbassets.com
16. http://skypeforbusiness.com

- [x] Cookies and searches are sent from the address bar and search box to your default search engine. Search recommendations are displayed when a user types in a search term in the search field. (Default)

Clear browsing data

- [x] Data created during the Chromium session will be deleted when Chromium is closed. What data are deleted is specified in the following options.
- [ ] Data created during the Chromium session will not be deleted when the browser is closed. (Default)

> All policies that are defined for Chromium are also valid for the progressive web apps (PWAs). Exception: **Clear browsing data** options starting from Chromium Browser app version 144.0.7559.96 BUILD 1.0. Before Chromium Browser app version 144.0.7559.96 BUILD 1.0: Though most PWAs have the **Clear data** setting, the **Clear browsing data** options configured for Chromium under **Chromium Browser > Global Settings > Privacy** still overrule every Chromium browser window, including PWAs (exception: MS Teams PWA).

Browsing and download history

This parameter is visible if **Clear browsing data** is enabled.

- [x] Addresses (URLs) of visited websites and the list of downloads will be deleted when Chromium is closed. (Default)

Cookies

This parameter is visible if **Clear browsing data** is enabled.

- [x] All cookies, not only third-party cookies, will be deleted when Chromium is closed. (Default)

Other site data

This parameter is visible if **Clear browsing data** is enabled.

- [x] Other site data will be deleted when Chromium is closed.
- [ ] Other site data will not be deleted when Chromium is closed. (Default)

Saved passwords

This parameter is visible if **Clear browsing data** is enabled.

- [x] Passwords that have been saved during the browser session will be deleted when Chromium is closed.
- [ ] Saved passwords entered will still be available when Chromium or the system is restarted. (Default)

Cache

This parameter is visible if **Clear browsing data** is enabled.

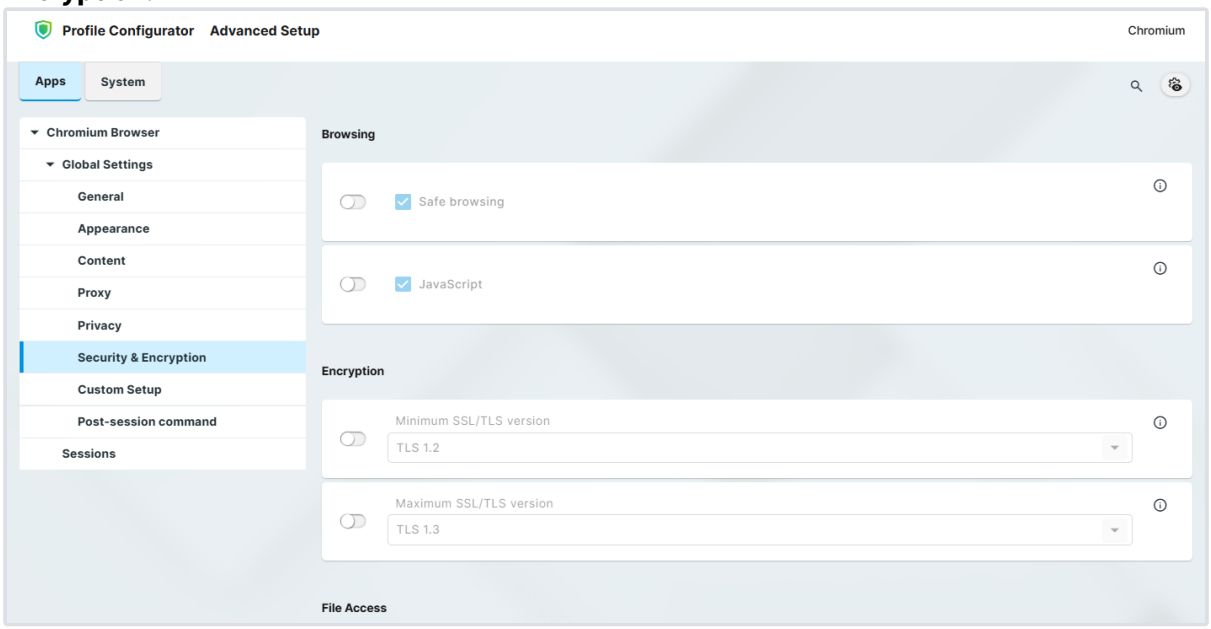
- ☑ The cache for temporarily saving web pages will be emptied when Chromium is closed.

Keep Cookies

Cookies define here will not to be removed if cookies are cleared.

Configuring Security and Encryption Settings

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Security & Encryption**.



2. Edit the settings according to your needs. The parameters are described in the following.

Safe browsing

- ☑ Chromium will check all web content, including e.g. images and scripts, against a continuously updated list of known phishing and malware websites. If Chromium finds suspicious content, you will be given a warning. (Default)
- ☐ Chromium will not check web content.

JavaScript

- ☑ JavaScript will be executed by Chromium. (Default)
- ☐ JavaScript is not executed.

Many websites use JavaScript for full functionality.

Minimum SSL/TLS version

This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.

Possible options:

- **TLS 1.2** (default)
- **TLS 1.3**

Maximum SSL/TLS version

This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.

Possible options:

- **TLS 1.2**
- **TLS 1.3** (default)

File access

- [x] Chromium can access local files on the endpoint device. Uploads are allowed.
- [ ] Local files cannot be accessed by Chromium. Uploads are not allowed. When the user tries to upload a file, a message informs the user that the access to local files is blocked. (Default)

Block Downloads

- [x] Downloads are not allowed. When the user tries to download a file, a message informs the user that downloads are blocked. Exceptions can be specified under **Download allowlist**. (Default)
- [ ] Downloads are allowed. The storage location is defined under **Handle downloads**.

Handle downloads
Possible options:

- **Downloads**: The file will be downloaded to `/userhome/Downloads`
- **Custom location**: The file will be downloaded to the directory specified with **Download path**. (Default)
- **Prompt for download location**: The user will be prompted to choose a download location.

Download Path

Defines the path files are downloaded to. Only effective when **Handle downloads** is set to **Custom location**. (Default: `/tmp`)

Download allowlist

The MIME types listed here are not blocked even when **Block downloads** is activated. If the file suffix matches with one of the entries in **Open file types automatically after downloading**, the file is opened immediately after download. The list entries are separated by semicolons ";". (Default: "application/x-ica; application/smil; application/nxs; application/x-java-jnlp-file; application/x-sapshortcut; application/x-virt-viewer; image/tiff")

Open file types automatically after downloading

Any file whose suffix is listed here will be opened immediately after downloading. The list entries are separated by semicolons ";". (Default: "ica; rpd; smi; smil; nxs; jnlp; vv; tif; tiff")

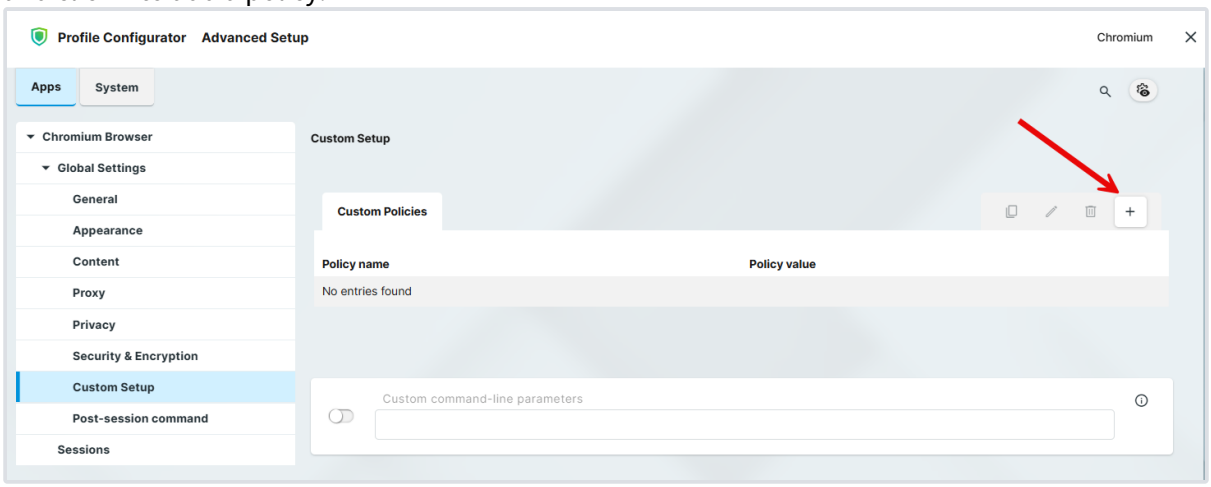
Configuring Custom Settings

You can add, edit, and remove policies for the Chromium sessions on your IGEL OS device. Please note that the custom settings always win over the IGEL Setup, i.e. if a policy is defined both here and in the Setup, but with different values, the value defined here is effective.

For a complete list of available policies, see https://chromeenterprise.google/policies/.

> Please note that the enterprise policy URL pattern format that is defined by Chrome is not fully supported by the IGEL Setup.

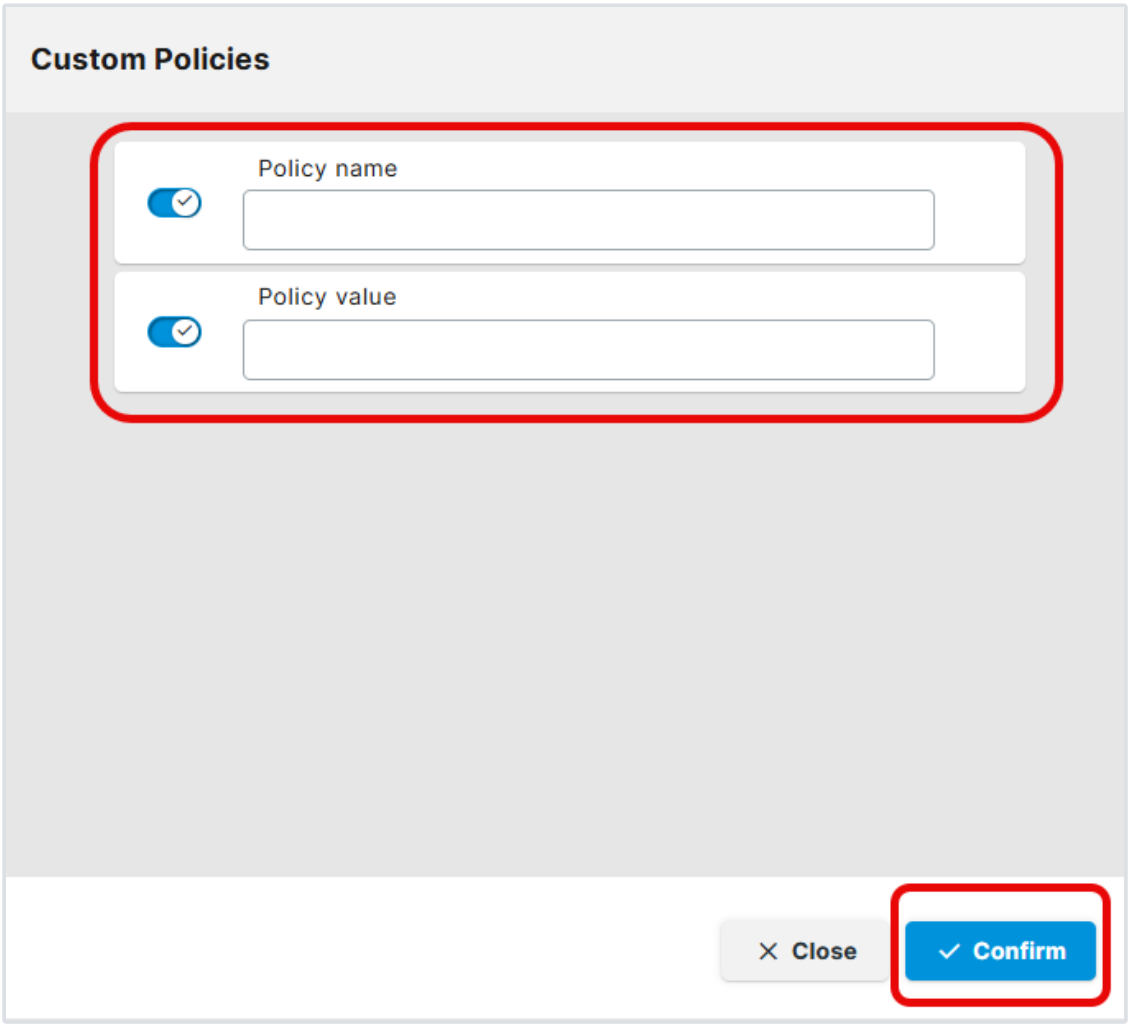
1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Custom Setup** and click **+** to add a policy.



2. Enter the Policy name. For possible policies, see https://chromeenterprise.google/policies/.

3. Enter the Policy value.

   The data format is described in https://chromeenterprise.google/policies/. Please note the following:
   - Use the correct data type (see the right column of the relevant policy description, e. g. https://chromeenterprise.google/policies/#URLBlocklist)
   - Use the Linux examples
   - Make sure to separate the policy name from the policy value; some of the examples in the Chrome documentation include the policy name accidentally, e. g. https://chromeenterprise.google/policies/#PrintingPaperSizeDefault

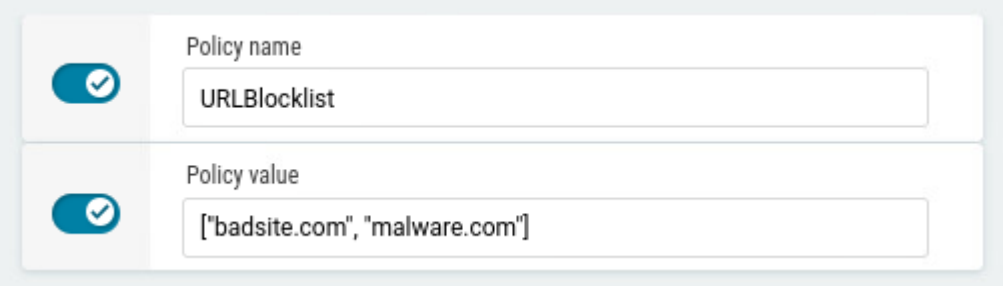


4. Click **Confirm** to create the policy.

URL Blocklist Example

If you want to block the websites badsite.com[17] and malware.com[18], define your policy as follows (see also https://chromeenterprise.google/policies/#URLBlocklist):

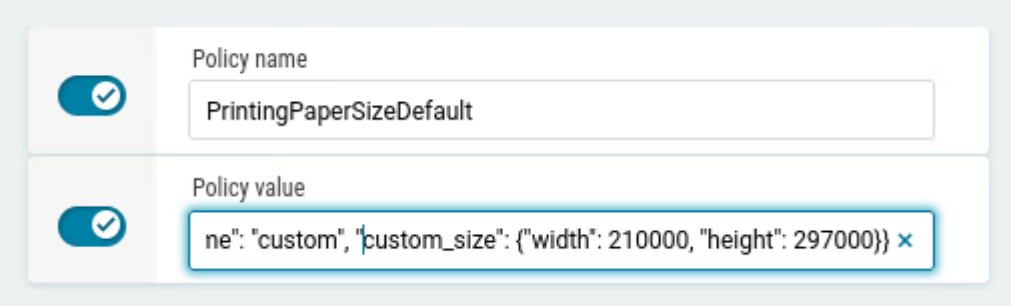
- **Policy name**: `URLBlocklist`
- **Policy value**: `["` badsite.com[19] `", "` malware.com[20] `"]`



Printing Paper Size Example

If you want to define a paper size for printing, define your policy as follows (see https://chromeenterprise.google/policies/#PrintingPaperSizeDefault):

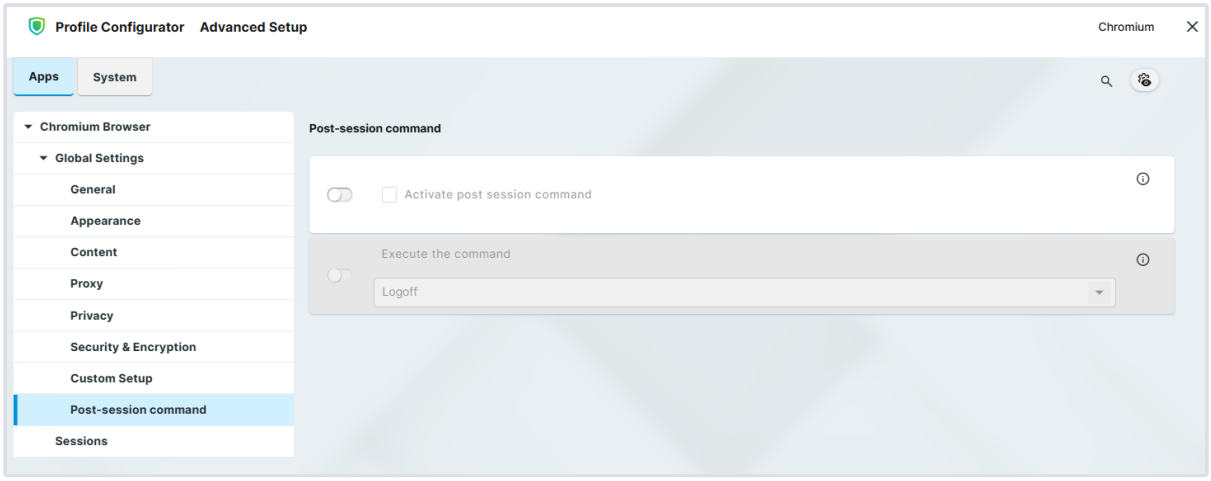
- **Policy name**: `PrintingPaperSizeDefault`
- **Policy value**: `{"name": "custom", "custom_size": {"width": 210000, "height": 297000}}`



Configuring a Post-session Command

1. In the profile configurator, go to **Apps > Chromium Browser > Global Settings > Post-session command**.

17. http://badsite.com/
18. http://malware.com/
19. http://badsite.com
20. http://malware.com



2. Edit the settings according to your needs. The parameters are described in the following.

Activate post session command

Allows to define an action that is performed when the last Chromium session is ended. For information on global post-session commands, see Post-session Custom Commands in IGEL OS 12[21].

- ☑ The post-session command specified under **Execute the command** will be executed.
- ☐ The post-session command specified under **Execute the command** will not be executed. (Default)

Execute the command

Action that is carried out after the end of the Chromium session(s).

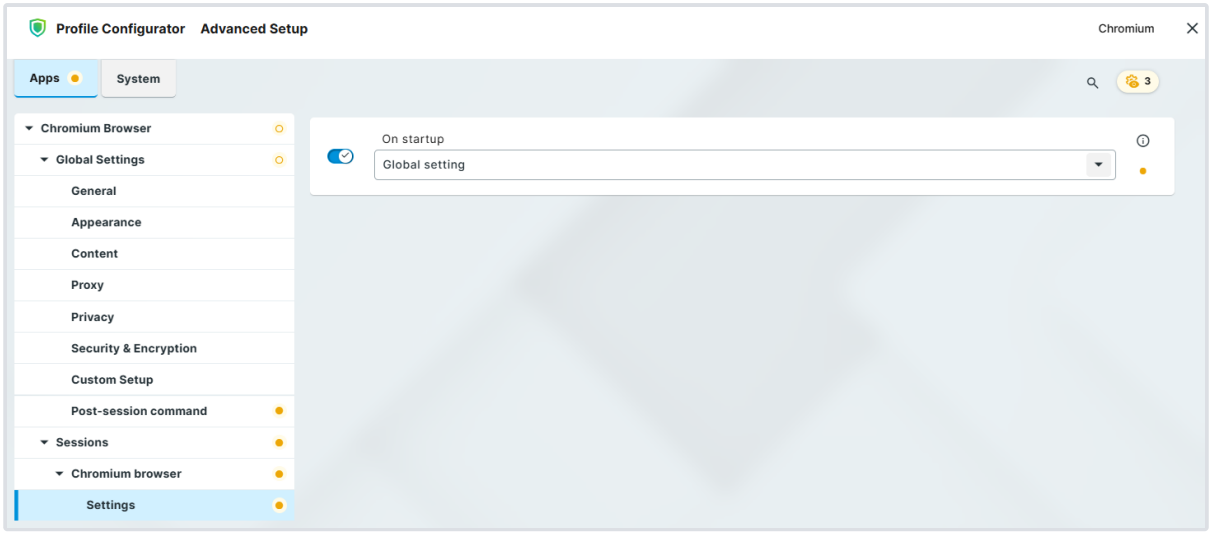
Possible values:

- **Logoff**: The user is automatically logged off; a login method must be defined for this purpose. Further information can be found under Logon Settings in IGEL OS 12[22]. (Default)
- **Shutdown**: The device will be shut down.
- **Enter custom command here**: Command to be executed.

Configuring the Settings for an Individual Session

1. In the profile configurator, go to **Apps > Chromium Browser > Sessions >** [session name] **> Settings**.

21. https://kb.igel.com/en/igel-os-base-system/current/post-session-custom-commands-in-igel-os-12
22. https://kb.igel.com/en/igel-os-base-system/current/logon-settings-in-igel-os-12



2. Edit the settings according to your needs. The parameters are described in the following.

On Startup

Specifies what is displayed on browser startup.

- **Global setting**: The global setting for browser startup is used. (Default)
- **Open the new tab page**: The new tab page is shown.
- **Open a specific page or set of pages**: The page or set of pages defined under **Startup page** is shown.

Startup page

This parameter is only shown when **On Startup** is set to **Open s specific page or set of pages**.

Specifies the page or set of pages to be shown when the user opens a new tab. This is effective only if **On Startup** is set to **Open a specific page or set of pages**. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". (Default: "https://www.igel.com")

Troubleshooting: Cannot Download Outlook E-amail Attachments

Problem

When trying to download an attachment from e-mails in Outlook in Chromium Browser, Chromium only downloads a file named with a uid.

Solution

Deactivate the dialog for accepting downloads by disabling the following registry key:

Parameter	**Enable IGEL Download Dialog**
Path	**System > Registry**
Registry	`chromiumglobal.app.enable_download_dialog`
Value	**enabled** (default) / **disabled**

Troubleshooting: Cannot Log into MS Teams in Chromium Browser

Problem

When you try to sign into Microsoft Teams in Chromium Browser, the site loops continuously, and you can't sign in.

For more information, see https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-sign-in/sign-in-loop#resolution.

Solution

For Microsoft Teams to work in Chromium Browser, it is required to allow the use of cookies. You can allow the use of all third party cookies in Chromium Browser by disabling the **Block third party cookies** parameter under **Apps > Chromium Browser > Chromium Browser Global > Privacy**.

To make the necessary cookie exception while keeping the blocking of third party cookies:

1. Enable the **Block third party cookies** parameter under **Apps > Chromium Browser > Chromium Browser Global > Privacy**.
   MS Teams specific parameters are shown to configure the exception.
2. Enable the **Enable Cookies Allowlist for MS Teams** parameter.
   The **Cookies Allowlist for MS Teams** becomes activated with the list of necessary URLs as default.
3. Save the changes.

Cisco Jabber VDI



- Getting Started with Cisco Jabber VDI (JVDI) on IGEL OS (see page 33)

Getting Started with Cisco Jabber VDI (JVDI) on IGEL OS

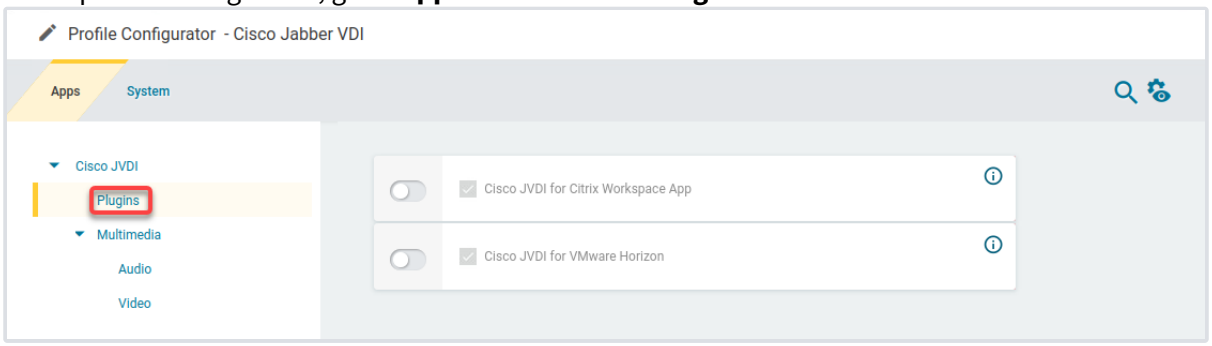
Installation

As Cisco Jabber VDI (JVDI) handles multimedia redirection but is not a standalone application, it cannot be used on its own. At least one of the following apps must be installed and configured as well:

- Citrix Workspace app
- Omnissa Horizon Client

Disabling or Enabling the Plugin

1. In the profile configurator, go to **Apps > Cisco JVDI > Plugins**.



2. Change the settings as required.

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

Cisco JVDI for Citrix Workspace App

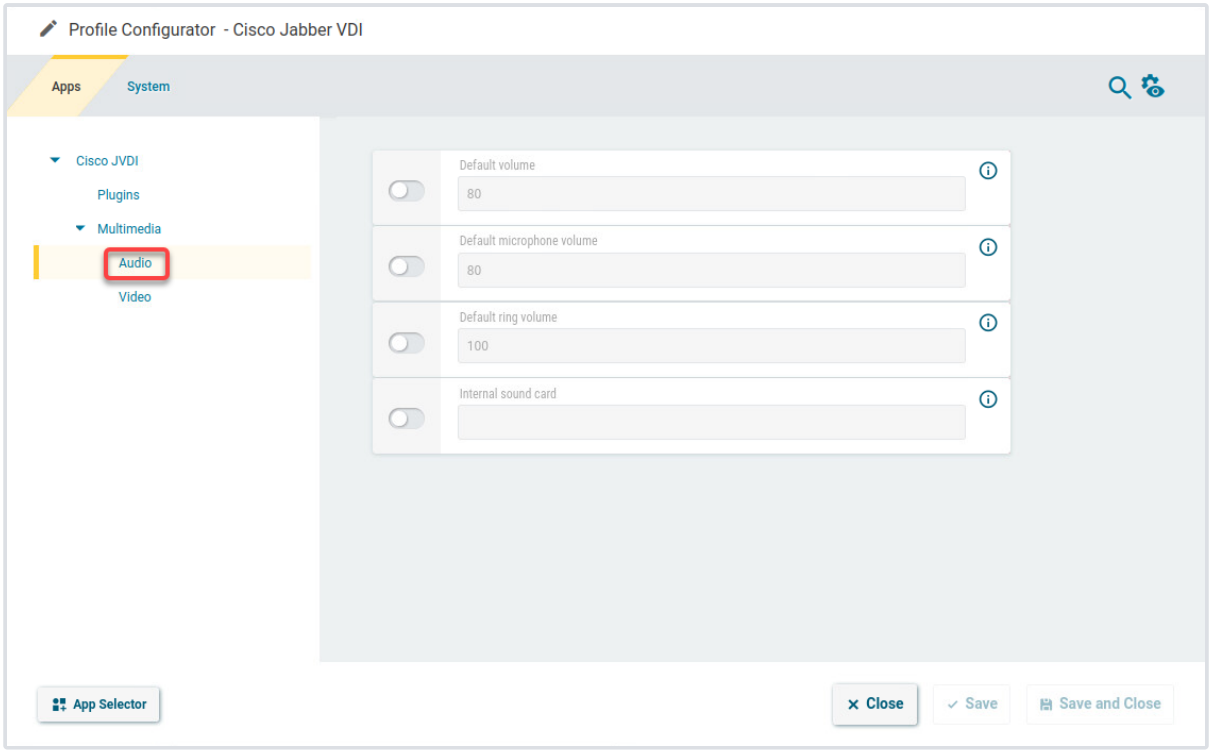
- ☑ The Cisco JVDI plugin is enabled in Citrix sessions. (Default)
- ☐ The Cisco JVDI plugin is disabled in Citrix sessions.

Cisco JVDI for VMware Horizon

- ☑ The Cisco JVDI plugin is enabled in Omnissa Horizon sessions. (Default)
- ☐ The Cisco JVDI plugin is disabled in Omnissa Horizon sessions.

Configuring Audio

1. In the profile configurator, go to **Apps > Cisco JVDI > Multimedia > Audio**.



2. Change the settings as required.

Default volume

The preset volume for the headphone in percent (default: 80). When a new device is plugged in, this value will be automatically assigned to all channels,

Default microphone volume

The preset volume for the microphone in percent. (Default: 80)

Default ring volume

The preset volume for the ringtone in percent. (Default: 100)

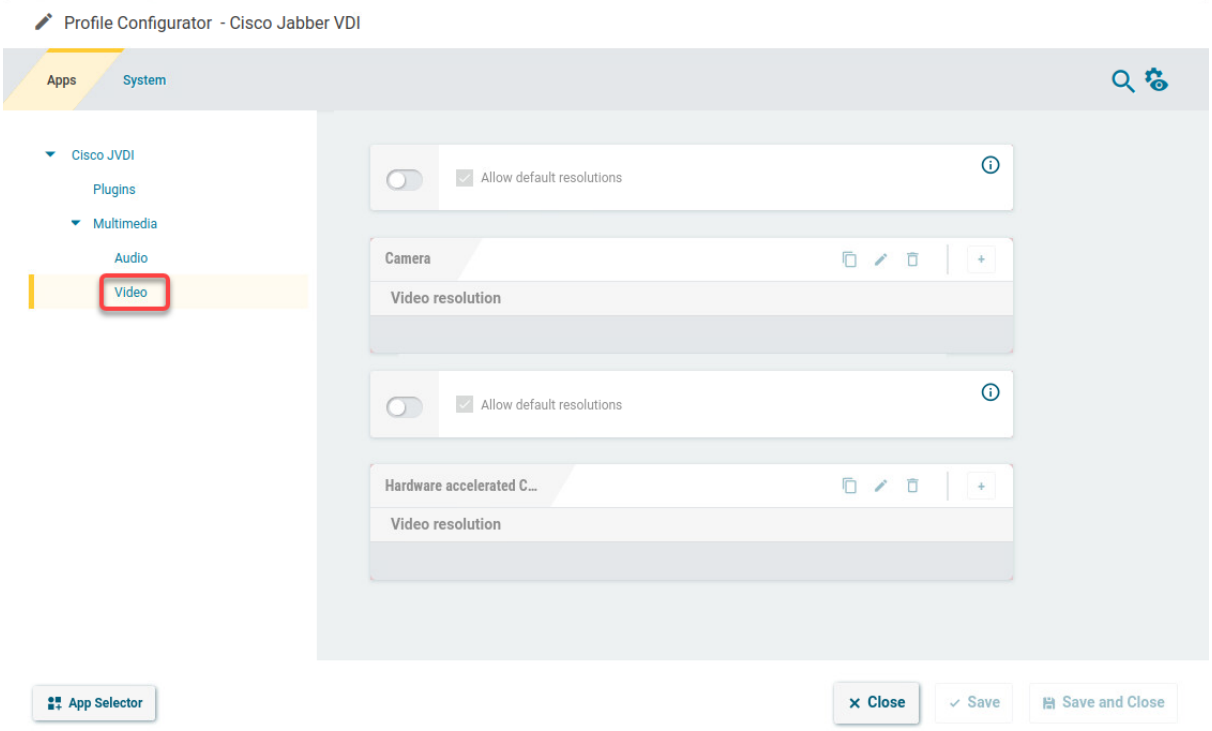
Internal sound card

Defines the sound card that is connected to the internal speaker; this will be used to play the ringtone. If you leave the field empty, the default sound card of the system is used.

Configuring Video

You can set the Cisco Jabber VDI Client to use the default resolutions of the camera or to use a user-defined set of resolutions. Separate configurations for cameras with and without hardware acceleration are possible.

1. In the profile configurator, go to **Apps > Cisco JVDI > Multimedia > Video**.

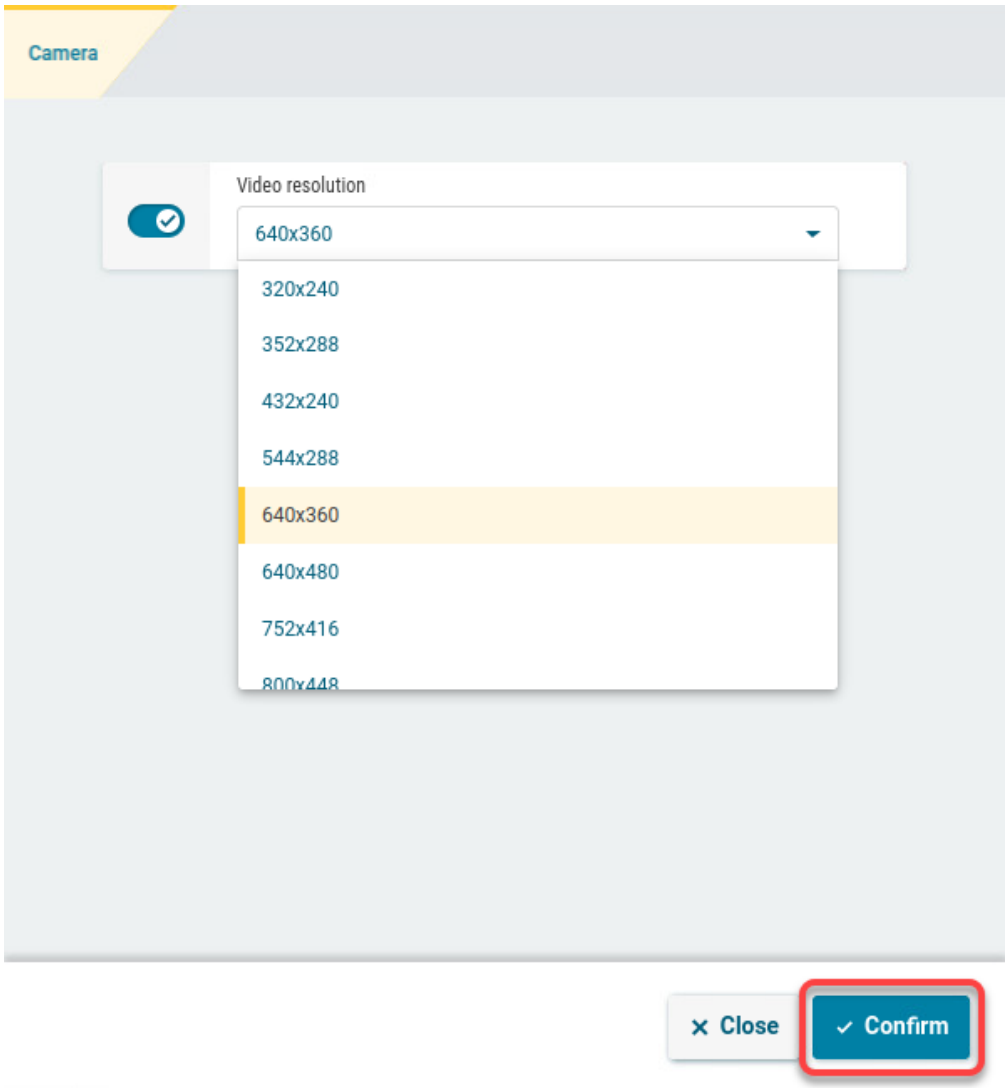


2. Change the settings as required.

Allow default resolutions

This setting is for cameras without hardware acceleration.

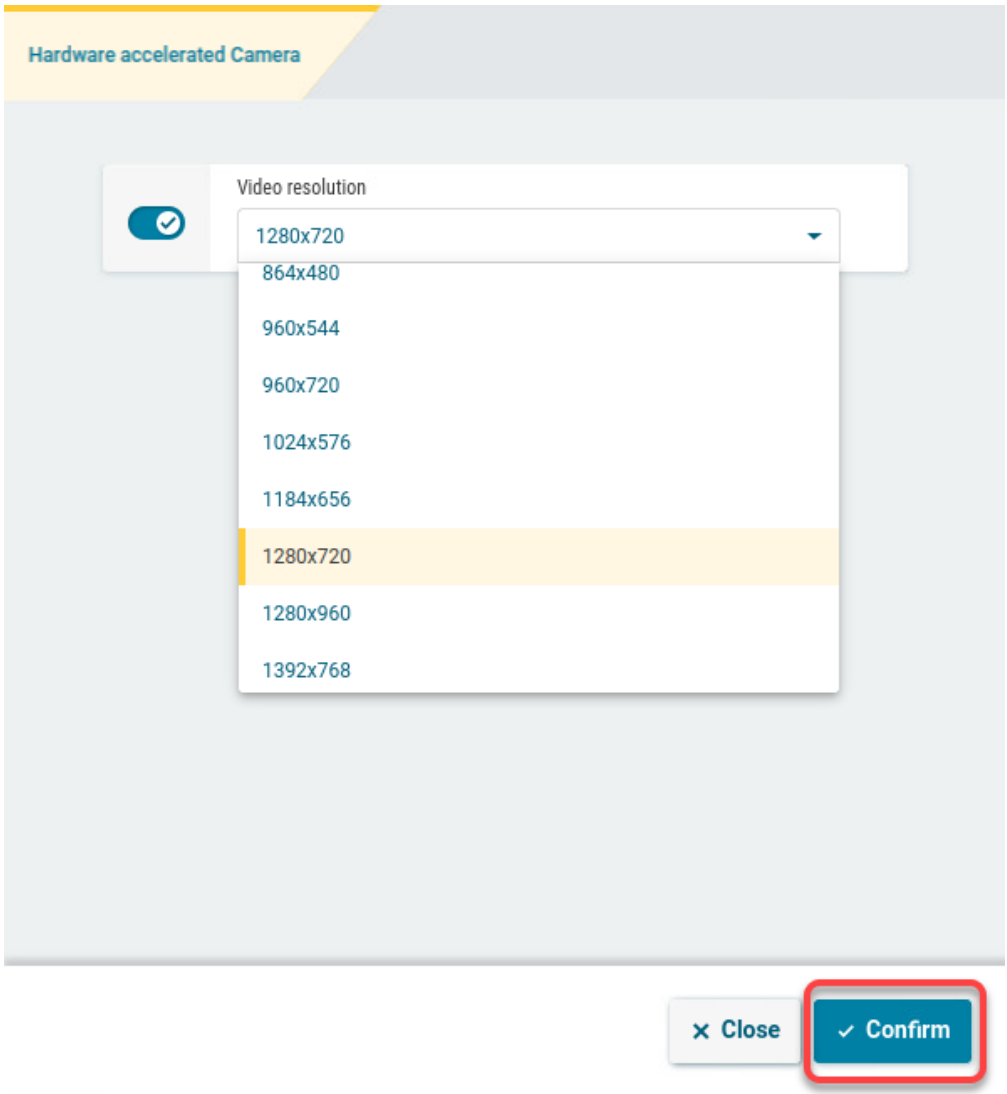
- ☑ The default resolutions of the camera are used. (Default)
- ☐ A user-defined set of resolutions is used. To add a resolution, click + in the **Camera** area and select the desired resolution.



Allow default resolutions

This setting is for cameras with hardware acceleration.

- ☑ The default resolutions of the camera are used.
- ☐ A user-defined set of resolutions is used. You can add a resolution by clicking + in the **Hardware Accelerated Camera** area and selecting the desired resolution.


Hardware accelerated Camera
Video resolution
1280x720
864x480
960x544
960x720
1024x576
1184x656
1280x720
1280x960
1392x768
Close
Confirm

Cisco Webex Meetings VDI



- Getting Started with Cisco Webex Meetings VDI on IGEL OS (see page 39)

Getting Started with Cisco Webex Meetings VDI on IGEL OS

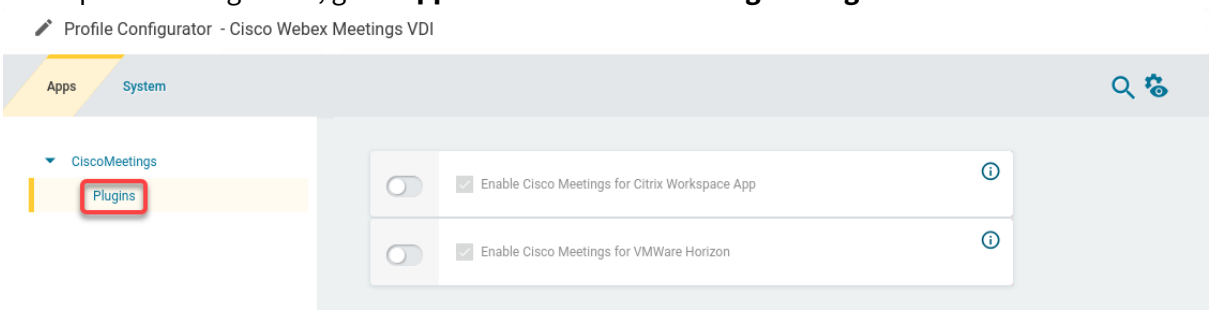
Installation

As Cisco Webex Meetings VDI handles multimedia redirection but is not a standalone application, it cannot be used on its own. At least one of the following apps must be installed and configured as well:

- Citrix Workspace app
- Omnissa Horizon Client

How to Disable or Enable the Plugin

1. In the profile configurator, go to **Apps > Cisco Webex Meetings > Plugins**.



2. Change the settings as required.

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

Enable Cisco Meetings for Citrix Workspace App

- ☑ The Cisco Webex Meetings VDI plugin is enabled in Citrix sessions. (Default)
- ☐ The Cisco Webex Meetings VDI plugin is disabled in Citrix sessions.

Enable Cisco Meetings for Omnissa Horizon

- ☑ The Cisco Webex Meetings VDI plugin is enabled in Omnissa Horizon sessions. (Default)
- ☐ The Cisco Webex Meetings VDI plugin is disabled in Omnissa Horizon sessions.

Cisco Webex VDI



- Getting Started with Cisco Webex VDI on IGEL OS (see page 41)

Getting Started with Cisco Webex VDI on IGEL OS

Dependencies

As Cisco Webex VDI handles multimedia redirection but is not a standalone application, it cannot be used on its own. At least one of the following apps must be installed and configured as well:

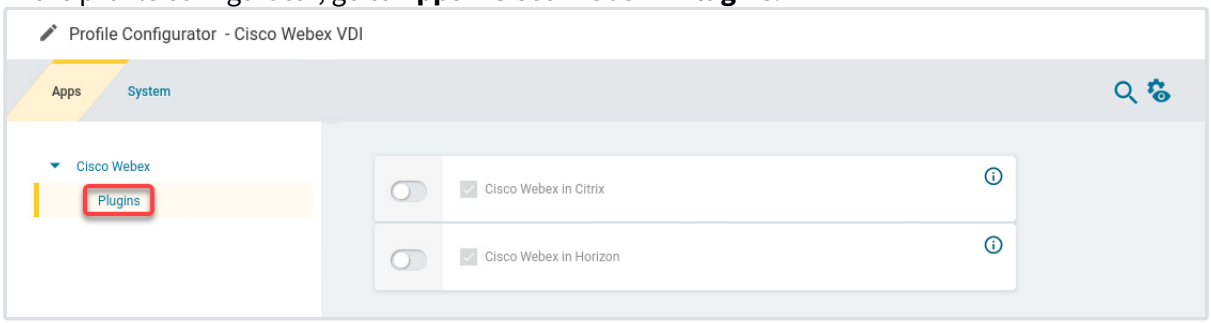
- Citrix Workspace app
- Omnissa Horizon Client

If your users want to make audio and video calls with Cisco Webex, the following app must be installed:

- Cisco Webex Meetings VDI

How to Disable or Enable the Plugin

1. In the profile configurator, go to **Apps > Cisco Webex > Plugins**.



2. Change the settings as required.

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

Cisco Webex in Citrix

- ☑ The Cisco Webex VDI plugin is enabled in Citrix sessions. (Default)
- ☐ The Cisco Webex VDI plugin is disabled in Citrix sessions.

Cisco Webex in Horizon

- ☑ The Cisco Webex VDI plugin is enabled in Horizon sessions. (Default)
- ☐ The Cisco Webex VDI plugin is disabled in Horizon sessions.

Citrix Workspace App



- Getting Started with the Citrix Workspace App on IGEL OS (see page 43)
- Configuration of the Citrix Workspace App on IGEL OS (see page 46)

Getting Started with the Citrix Workspace App on IGEL OS

Apps that Are Installed with the Citrix Workspace App

When the Citrix Workspace app is installed, the following apps are installed automatically:

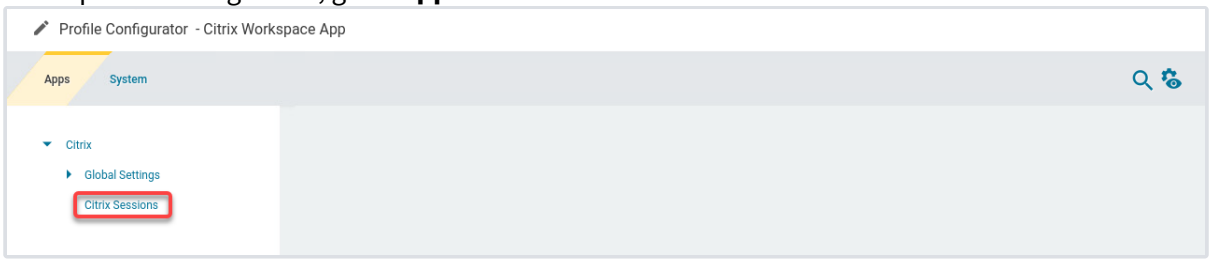
- Citrix Multimedia Codec

App Functionality and Setup

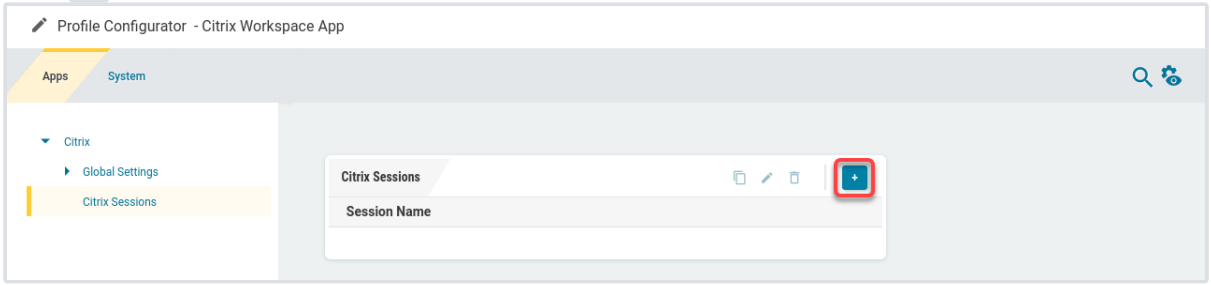
The functionality between IGEL OS 11 and IGEL OS 12 has changed fundamentally. While in IGEL OS 11 only one Storefront and SelfService session can be created, in IGEL OS 12 it is possible to create multiple sessions.

How to Create a Session

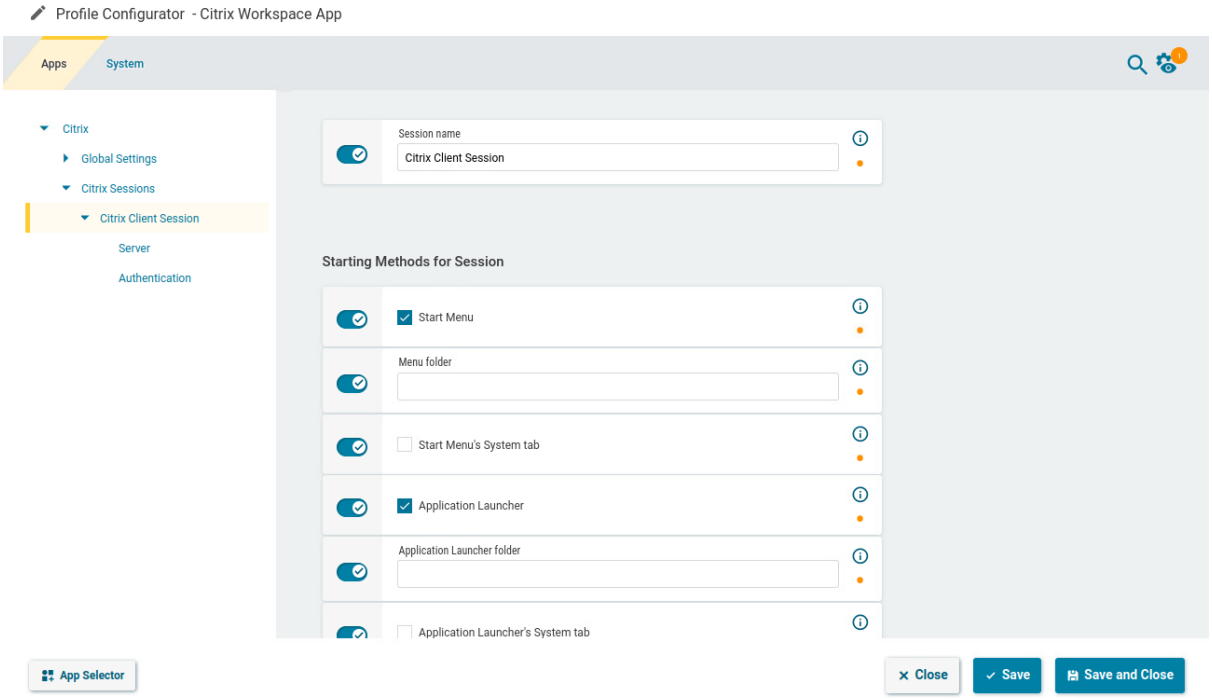
1. In the profile configurator, go to **Apps > Citrix > Citrix Sessions**.



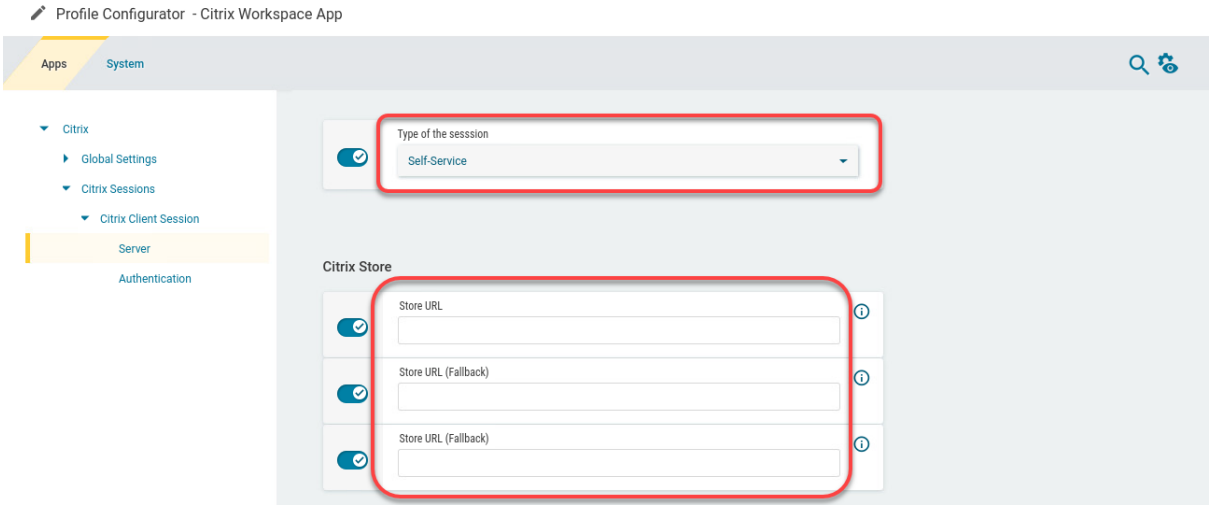
2. Click + .



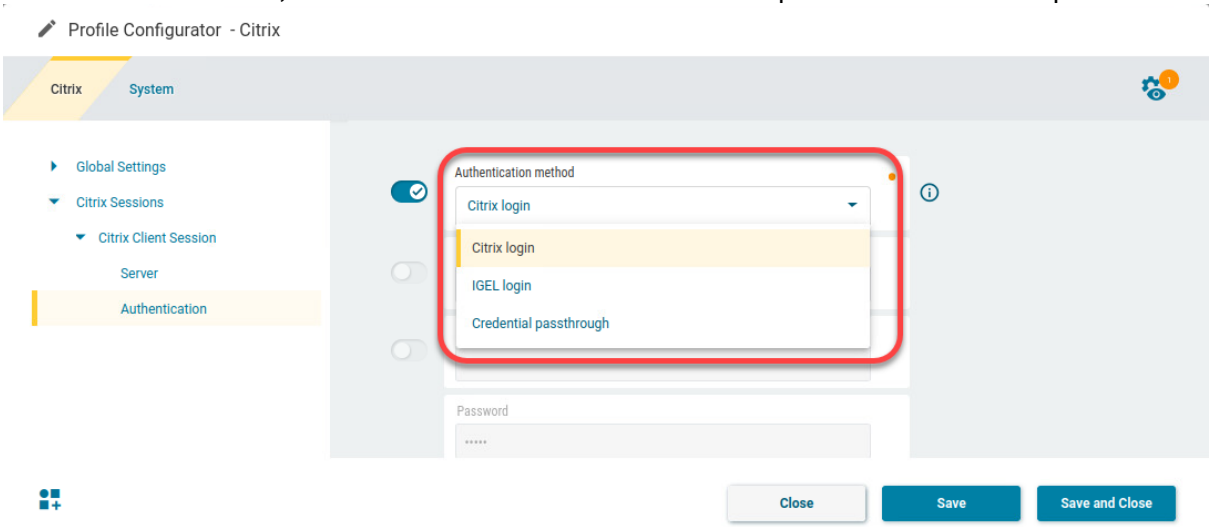
The session is created.



3. Under **Server**, choose the **Type of the session** and specify the server address under **Store URL**. You can specify up to three server addresses; the first available URL will be connected to.



4. Under **Authentication**, select the **Authentication method** and provide the data as required.



- **Citrix login**: The Citrix login dialog is used. (Default)

  > **Smartcard Authentication for Citrix Sessions in IGEL OS 12**
  > If the server offers smartcard authentication, it will be automatically used. No settings need to be made on the client side.

- **IGEL login**: The fields for **Username**, **Domain**, and **Password** become active. If all fields are filled in by the user, the login is performed automatically. If none or only a part of the fields are filled, the IGEL OS login dialog is presented to the user.

  > For this authentication method, HTTPBasic must be active on the server and on the client (default). This method is available only for Citrix on-premises, not for the Cloud solution. Also, on the **Server** page, HTTPS should be specified in the **Store URL** to ensure an encrypted connection.

- **Credential passthrough**: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.

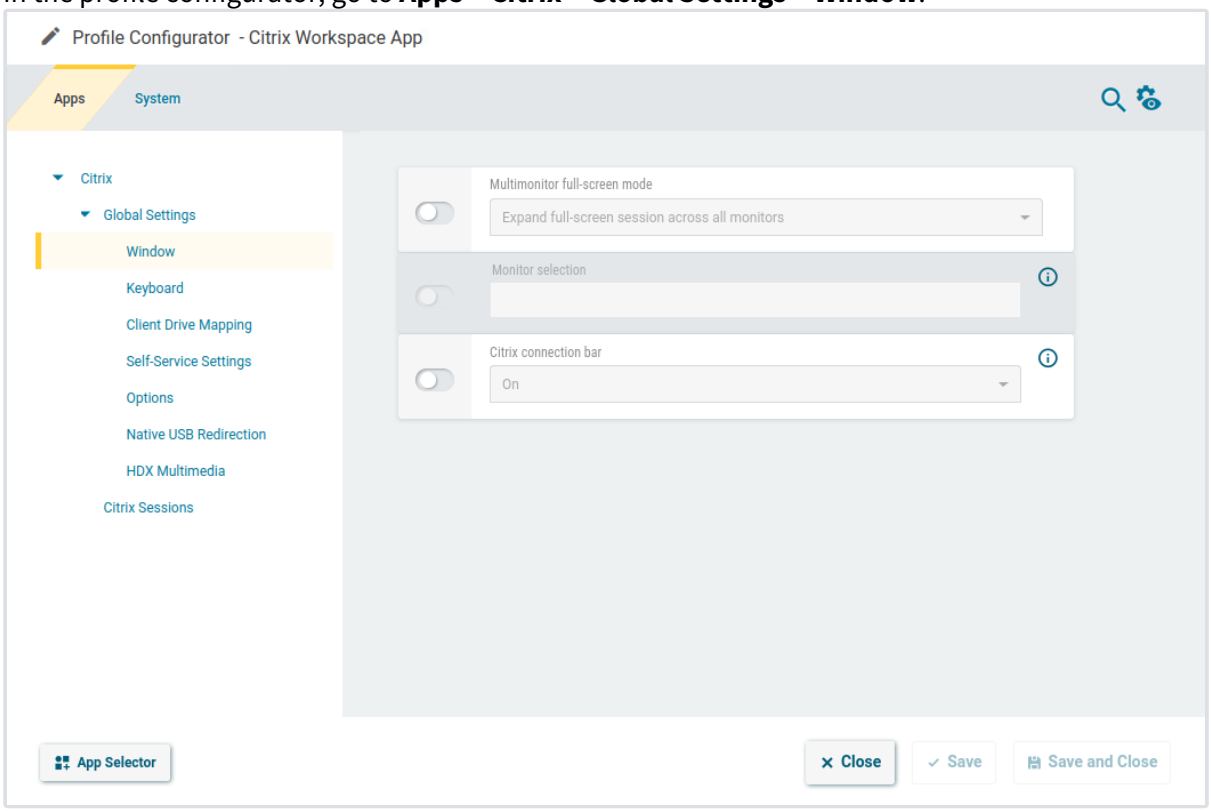
  > For this authentication method, HTTPBasic must be active on the server. This method is available only for Citrix on-premises, not for the Cloud solution. Also, on the **Server** page, HTTPS should be specified in the **Store URL** to ensure an encrypted connection.

5. Save the settings.

Configuration of the Citrix Workspace App on IGEL OS

Configuring the Session Window

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Window**.



2. Edit the settings according to your needs. The parameters are described in the following.

Multimonitor full-screen mode

- **Expand full-screen session across all monitors**: A full-screen session is expanded across all monitors. (Default)
- **Expand the session over a self-selected number of monitors**: Select this setting if you want to span the session across a certain number of monitors. Under **Monitor selection**, specify the relevant monitors, separated by numbers. You can use a short form to specify several subsequent monitors; for instance, "2,4" means that monitors 2, 3, and 4 are used.
- **1st monitor** ... **8th monitor**: The session is displayed on the specified monitor.

Monitor selection

This setting is available if you selected **Expand the session over a self-selected number of monitors** for **Multimonitor full-screen mode**.

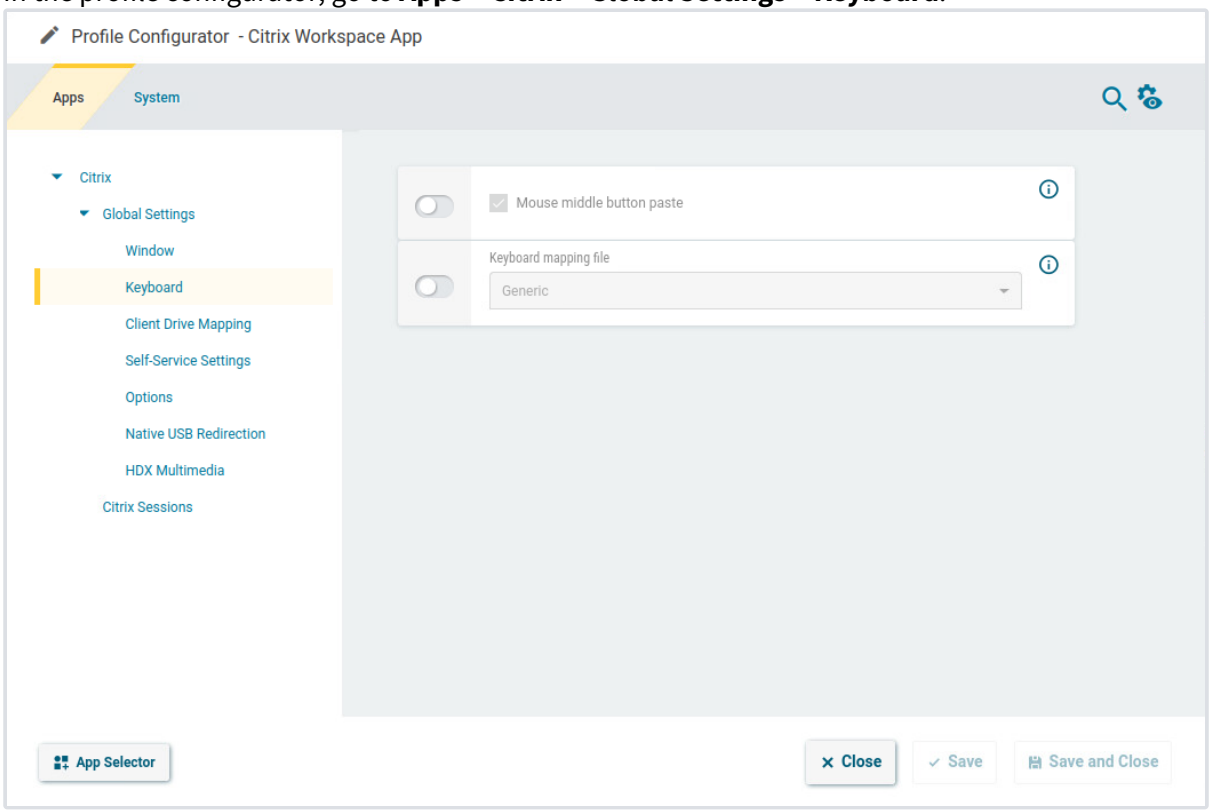
> **Example**
>
> Sample configuration: If you have 4 monitors and want to expand your session across monitors 2, 3, and 4 you have to insert `2,3,4` or `2,4`.

Citrix connection bar

- **On**: The pulldown menu "Desktop Viewer" by Citrix will be displayed. This applies to non-seamless sessions. (Default)
- **Off**: The pulldown menu is not displayed.

Configuring the Keyboard

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Keyboard**.



2. Edit the settings according to your needs. The parameters are described in the following.

Mouse middle button paste

☑ The middle button of the mouse can be used for pasting content in the Citrix session. (Default)

Keyboard mapping file

- **Generic**: The client sends language-independent scancodes to the server. (Default)
- **Linux**: The client sends language-specific scancodes to the server.
- **Automatic**: The mapping file provided by Citrix is used.

Alt + F1 ... Alt + F12

The hotkey mappings are available if **Keyboard mapping file** is set to **Linux** or **Automatic**.

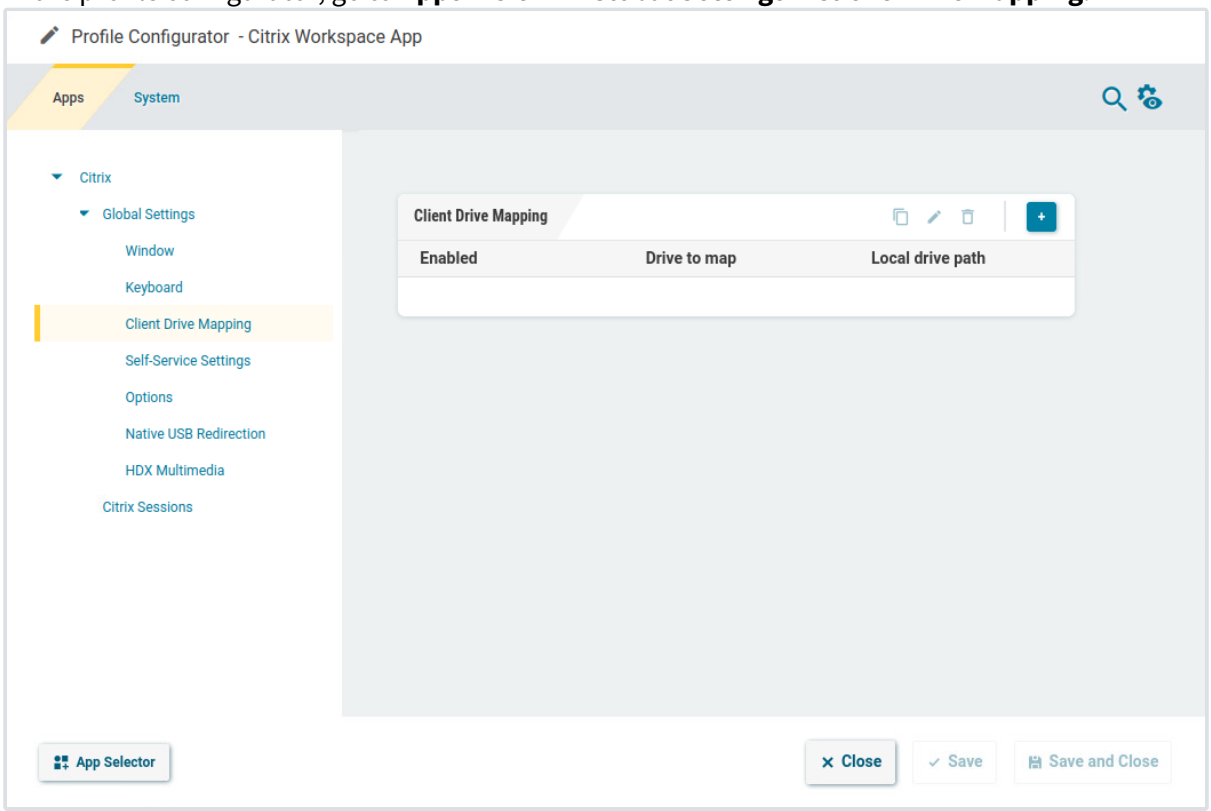
- **Hotkey character**: The function key to be sent when the relevant key combination [Alt] + [F<n>] is pressed
- **Hotkey modifier**: The modifier for the function key to be sent when the relevant key combination [Alt] + [F<n>] is pressed

Configuring the Client Drive Mapping

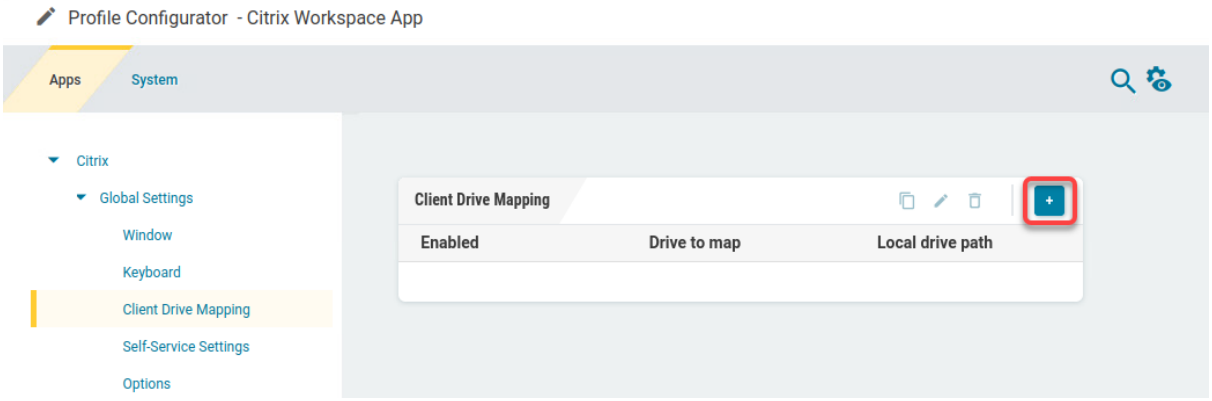
Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to your Citrix session.

You can specify which drives and paths are mapped during the logon. This applies to all Citrix sessions.

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Client Drive Mapping**.



2. To add a client drive mapping, click +.

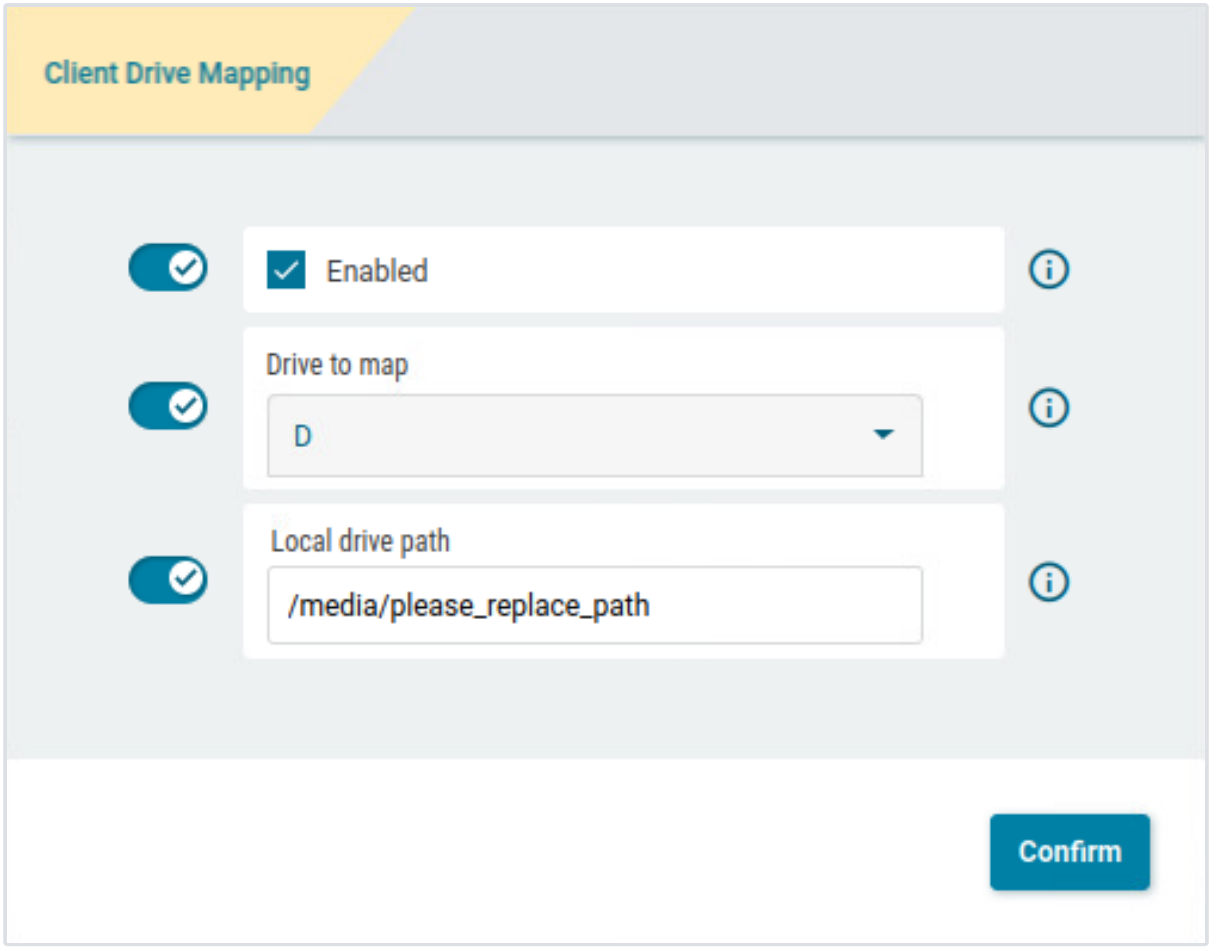


3. Edit the settings according to your needs and click **Confirm**:

- **Enabled**: Activate to make this drive available in Citrix sessions.
- **Drive to map**: Choose a DOS-style drive letter under which the drive will appear on the Citrix Server.

> If the drive letter you have selected is no longer available on the Citrix server, the specified directory or local drive will be given the next free letter during the logon.

- **Local drive path**: Enter a Unix path name of the local directory to which the mapping is to refer. If you map a locally connected device, use the pre-defined path names available in the drop-down field.



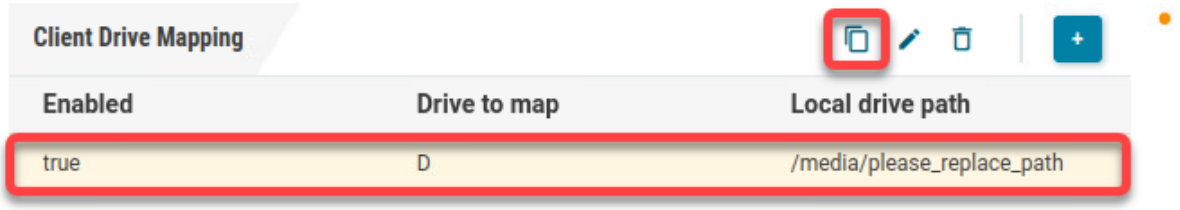
Local (USB) devices which are to be used for drive mapping purposes must first be set up as storage devices.

Before you unplug a hotplug storage device from the device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there is one or several possibilities to safely remove a hotplug storage device:

- Click on ⏏ in the task bar. The taskbar is not available in a fullscreen session.
- Click on in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session.
- Function **Devices > Storage Devices > Disk Removal** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Don't remove the device.**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

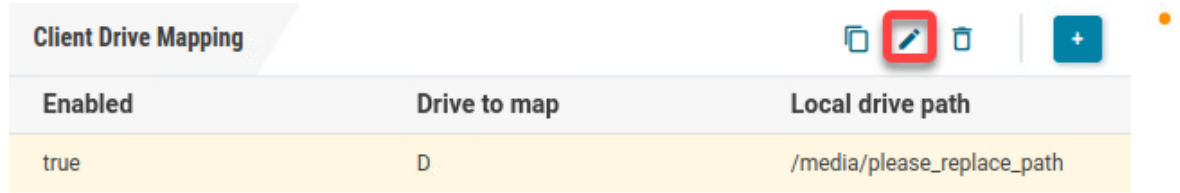
Adding Further Drive Mappings by Copying

To add further drive mappings, you can use an existing drive mapping by duplicating it. Select an existing drive mapping, click , and then edit the new drive mapping as desired.



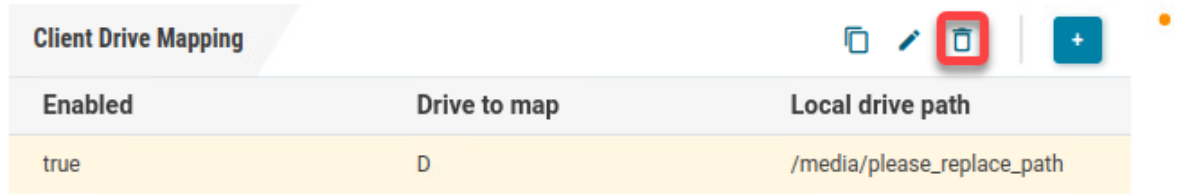
Editing a Drive Mapping

To edit a drive mapping, select the relevant drive mapping and click .



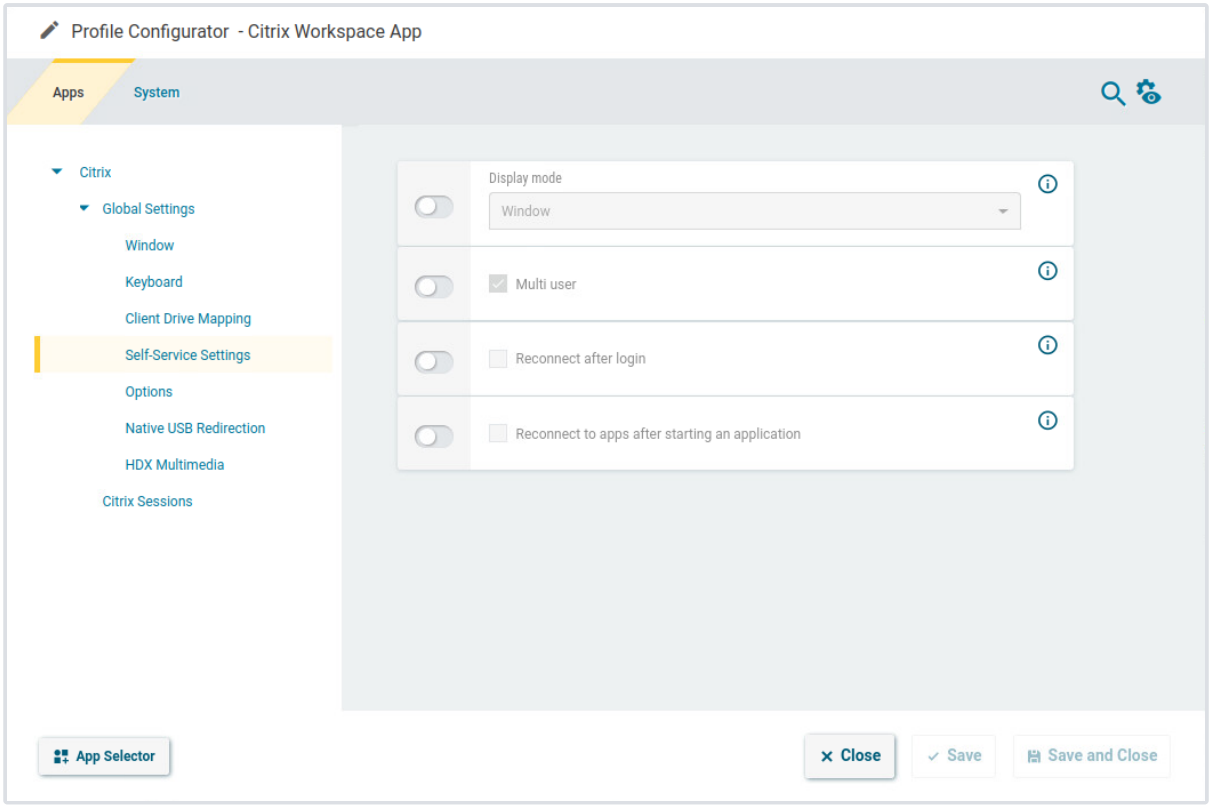
Deleting a Drive Mapping

To delete a drive mapping, select the relevant drive mapping and click .



Editing the Self-Service Settings

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Self-Service Settings**.



2. Edit the settings according to your needs. The parameters are described in the following.

Display mode

Display type for the Self-Service user interface

Possible values:

- **Window** (Default)
- **Full-screen**

> In full screen mode, the IGEL desktop will not be available.

Multi user

- ☑ The user data on the client will be deleted after logging off or terminating Self-Service. (Default)

Reconnect after login

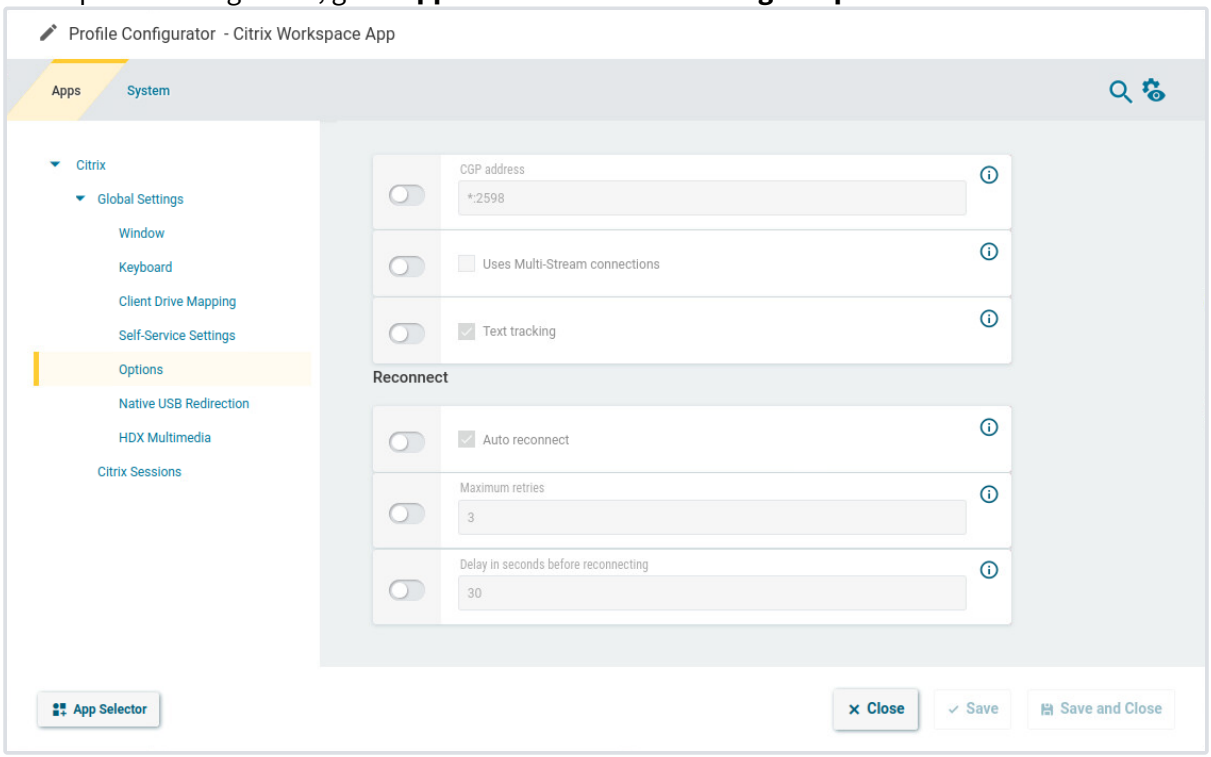
- ☑ The Self-Service user interface reconnects automatically to applications and desktops after being launched.
- ☐ The Self-Service user interface does not reconnect automatically. (Default)

Reconnect to apps after starting an application

- [x] The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
- [ ] The Self-Service user interface will not attempt to reconnect. (Default)

Configuring the Options

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Options**.



2. Edit the settings according to your needs. The parameters are described in the following.

CGP address

This is relevant if a CGP connection is used. Address and port for the CGP connection in the format `<address>.<port>`. If the same address as that for non-CGP connections is to be used, enter `*`. Default: *.2598

Uses multi-stream connections

- [x] The ICA virtual channels are divided into four separate ICA channels.
- [ ] The ICA virtual channels are not divided. (Default)

Text tracking

- Loss-free depiction of texts. Text is displayed sharper, especially if "Visual Quality" is set to Low/Medium. Recommended for office applications, but requires a higher bandwidth. (Default)

⚠ With a bad connection, this method can lead to missing text parts.

Auto reconnect

- Automatically attempt to reconnect if the connection to the Citrix server is lost. (Default)

Maximum retries

Relevant if **Auto reconnect** is activated. Specifies how often the client should retry to connect to the Citrix server. Default: 3

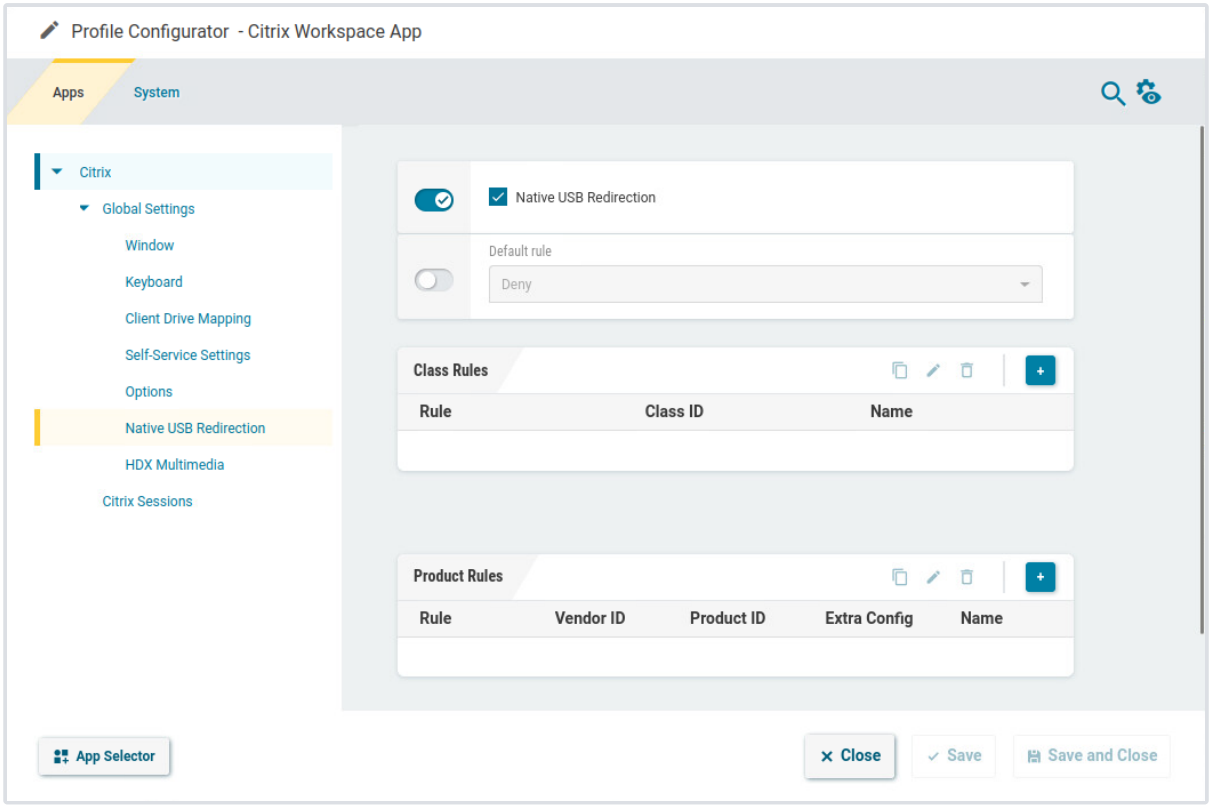
Delay in seconds before reconnecting

Relevant if **Auto reconnect** is activated. Time to wait for the network to recover before the client tries to reconnect. Default: 30

Configuring Native USB Redirection

USB devices can be permitted or prohibited during a Citrix session on the basis of rules. Sub-rules for specific devices or device classes are also possible.

1. In the profile configurator, go to **Apps > Citrix > Global Settings > Native USB Redirection**.



2. Edit the settings according to your needs. The parameters are described in the following.

Native USB redirection

- ☑ Native USB redirection is enabled globally.
- ☐ Native USB redirection is disabled. (Default)

Default rule

This rule will apply if no specific rule was configured for a class or a device.

> To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

- **Deny** (Default)
- **Allow**

Class Rules

Class rules apply to USB device classes and sub-classes.

To add a class rule:

In the **Class Rules** are, click +.



1. Set the criteria according to your needs:
   - **Rule**:
     - **Deny**: Devices of this class/subclass will not be redirected automatically.
     - **Allow**: When a device of this class/subclass is plugged in after the start of the session, it will be redirected. If you want an already plugged-in device to be redirected, unplug it and plug it in again.
     - **Connect**: A device of this class/subclass is redirected, regardless of whether it has been plugged in before or after the start of the session.
   - **Class ID**: Select the class to which this rule should apply.
   - **Subclass ID**: Select the subclass to which this rule should apply.
   - **Name**: Enter a name for this rule.

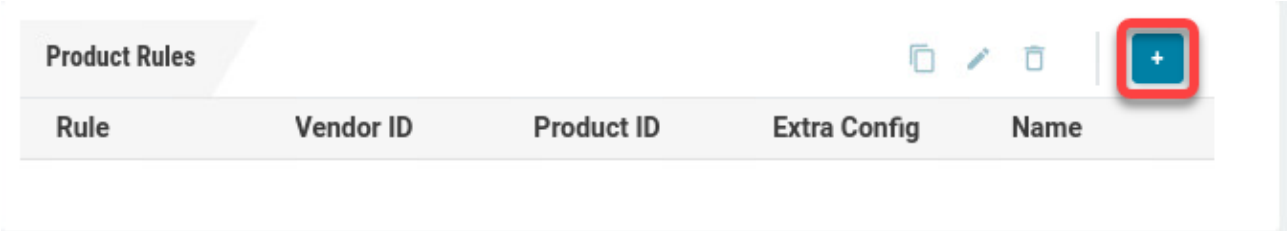
Product Rules

Product rules apply to individual USB devices.

> **Composite USB Redirection**
> You can configure composite USB redirection which is needed for multifunctional devices that use different interfaces. Examples of such composite USB devices are dictation microphones or Bloomberg keyboards which comprise a keyboard, fingerprint reader, an audio device, USB hub, etc.
> To redirect the entire composite device to the session, only **Vendor ID** (`vid`) and **Product ID** (`pid`) must be added.
> If you need to split the composite device and redirect only the child interfaces that use a generic USB channel, you must also add filter parameters `split` and `intf` under **Extra Config**. For more information on composite USB redirection and sample device rules, see https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#usb.

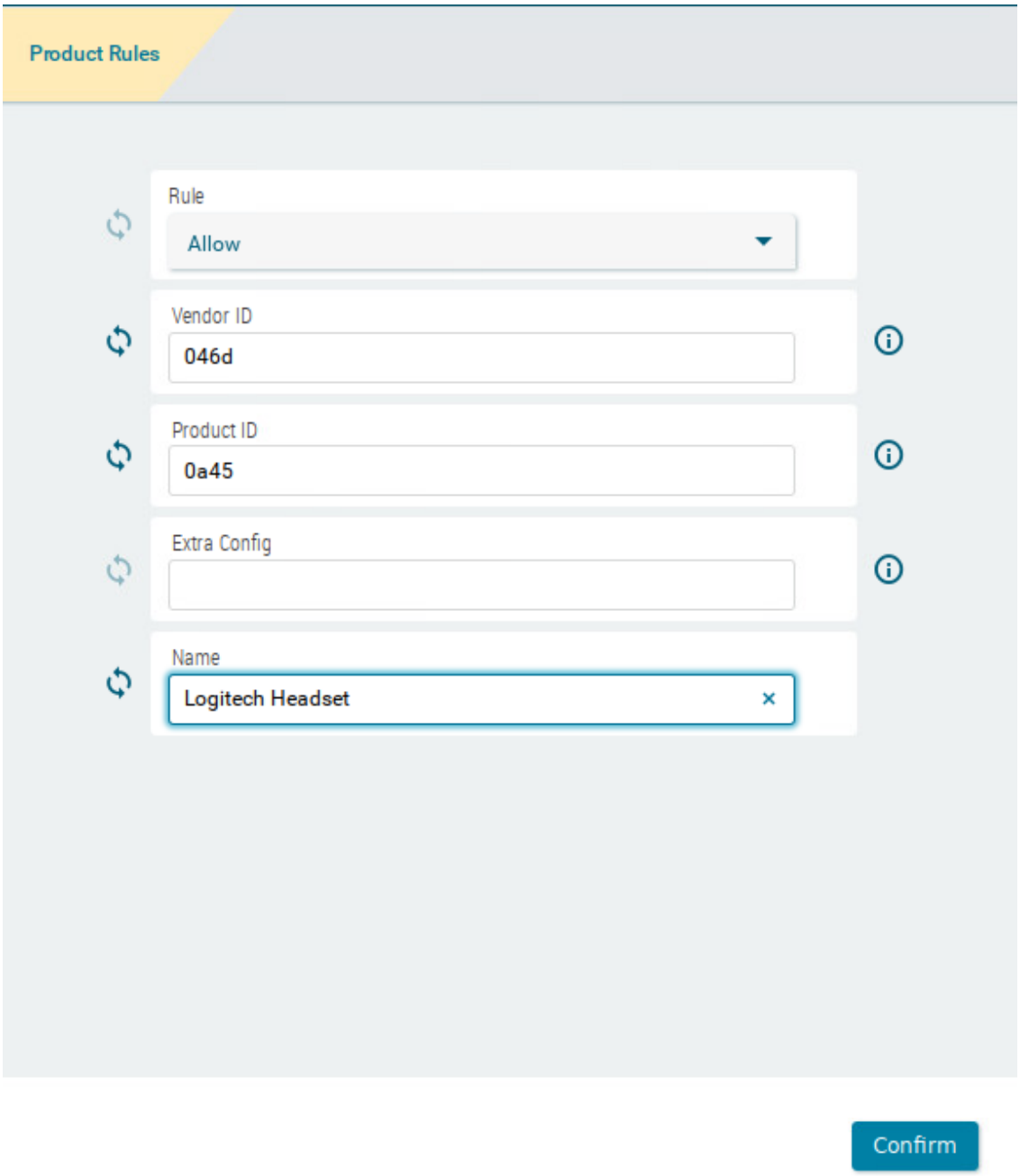
To add a product rule:

In the **Class Rules** are, click +.



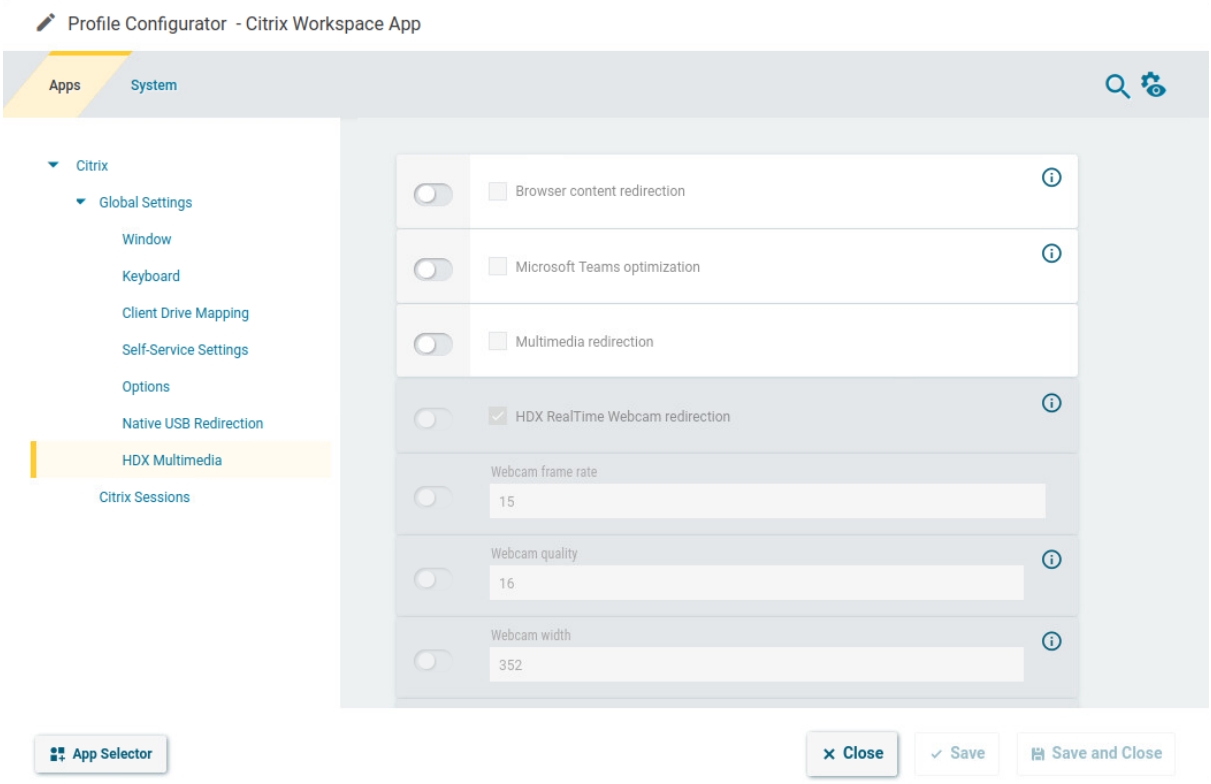
1. Set the criteria according to your needs:
   - **Rule**:

    - **Deny**: This device of this class/subclass will not be redirected automatically.
    - **Allow**: When this device is plugged in after the session start, it will be redirected. If you want an already plugged-in device to be redirected, unplug it and plug it in again.
    - **Connect**: This device is redirected, regardless of whether it has been plugged in before or after the session start.
- **Vendor ID**: Enter the hexadecimal value of the vendor id for the device to which this rule should apply.
- **Product ID**: Enter the hexadecimal value of the product id for the device to which this rule should apply.
- **Extra config**: If desired, enter configuration parameters for the device.
  Example:
  `CONNECT: vid=047F pid=C039 split=1 intf=03` (For composite USB devices: Allow HID device and connect automatically)
- **Name**: Enter a name for this rule.



Configuring the Settings for HDX Multimedia

1. In the profile configurator, go to **Apps > Citrix > Global Settings > HDX Multimedia**.



2. Edit the settings according to your needs. The parameters are described in the following.

Browser content redirection

- ☑ The browser content is redirected from the server to the device, e.g. to reduce the load on the server.
- ☐ Browser content redirection is disabled. (Default)

Microsoft Teams optimization

- ☑ A virtual channel for Microsoft Teams optimization is enabled.
- ☐ Microsoft Teams optimization is disabled. (Default)

Multimedia redirection

- ☑ Multimedia data is decoded on the device.
- ☐ Multimedia data is decoded on the server, (Default)

HDX RealTime webcam redirection

This setting is only available if **Multimedia redirection** is enabled.

- ☑ Webcam redirection with HDX RealTime support is enabled. (Default)

Webcam frame rate

This setting is only available if **Multimedia redirection** is enabled.

The frame rate requested from the webcam. Default: 15

Webcam quality

This setting is only available if **Multimedia redirection** is enabled.

The image quality requested from the webcam. Range: 1-63. Default: 16

Webcam width

This setting is only available if **Multimedia redirection** is enabled.

The image width requested from the webcam. Default: 352

Webcam height

This setting is only available if **Multimedia redirection** is enabled.

The image height requested from the webcam. Default: 288

HDX webcam delay time

This setting is only available if **Multimedia redirection** is enabled.

Time to wait before the webcam is opened, in milliseconds. Default: 2000

HDX Webcam delay type

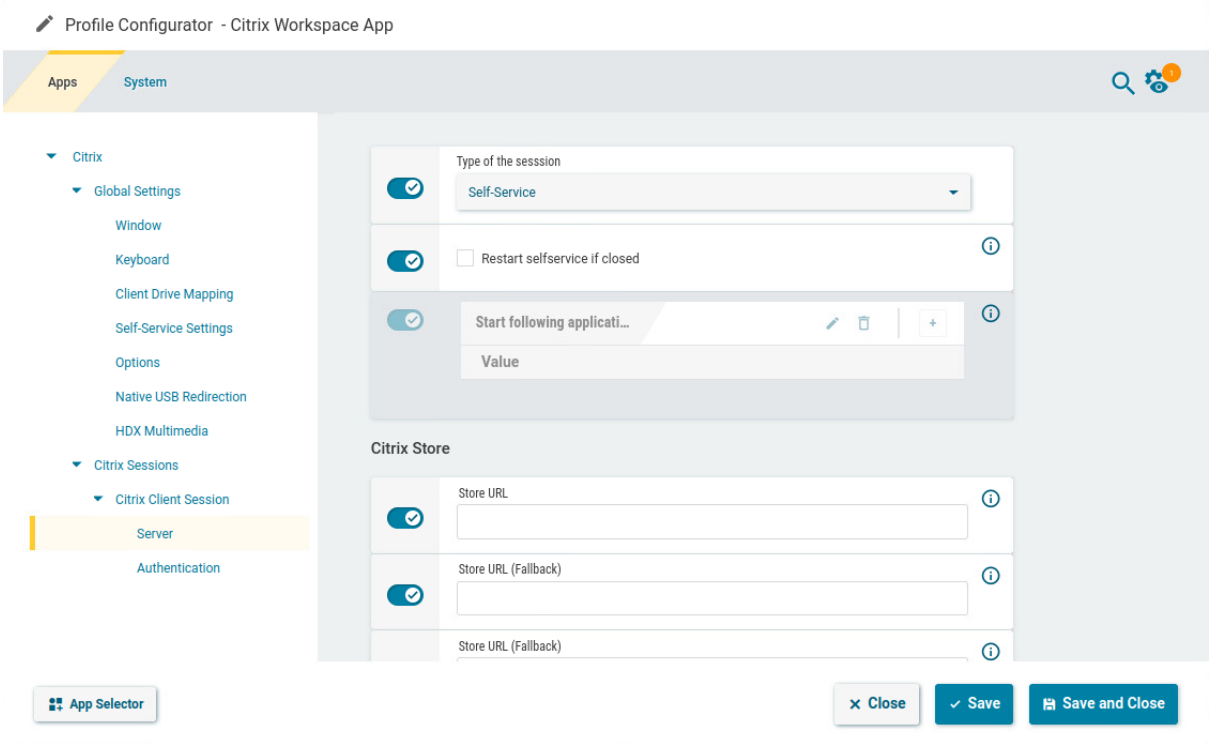
This setting is only available if **Multimedia redirection** is enabled.

Determines if and how the opening of the webcam should be delayed in a session.

- **0**: No delay
- **1**: If the time interval since the last closing of the webcam is less than the defined delay time (**HDX Webcam delay time**), the delay length is the remaining time. (Default)
- **2**: The delay time is as defined by **HDX Webcam delay time**.

Configuring the Server for an Individual Session

1. In the profile configurator, go to **Apps > Citrix > [session name] > Server**.



2. Edit the settings according to your needs. The parameters are described in the following.

Type of the session

Possible options:

- **Self-Service**
- **StoreFront**

Restart selfservice if closed

- ☑ Self-Service is restarted when the session is closed.
- ☐ Self-Service is not restarted.

Store URL

URL of the Citrix server.

Start following applicati...

This parameter is available if **Type of the session** is set to **StoreFront**.

- ☑ You can define a list of applications that are started automatically when the server connection is established. For each application, click + and enter the name of the application.

Store URL (Fallback)

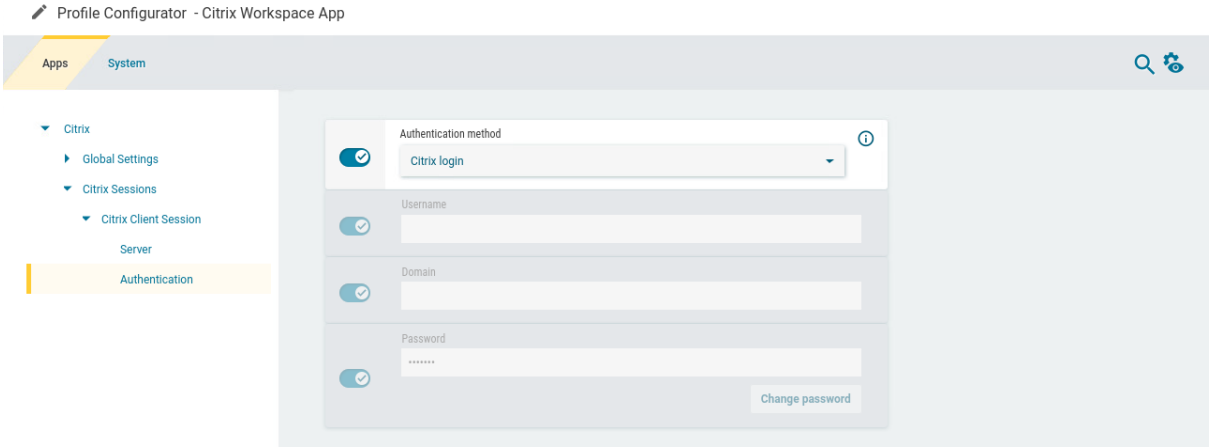
URL of the first fallback Citrix server.

Store URL (Fallback)

URL of the second fallback Citrix server.

Configuring the Authentication for an Individual Session

1. In the profile configurator, go to **Apps > Citrix > [session name] > Authentication**.



2. Edit the settings according to your needs. The parameters are described in the following.

Authentication method

- **Citrix login**: The Citrix login dialog is used. (Default)

> **Smartcard Authentication for Citrix Sessions in IGEL OS 12**
>
> If the server offers smartcard authentication, it will be automatically used. No settings need to be made on the client side.

- **IGEL login**: The fields **Username**, **Domain**, and **Password** become active. If all fields are filled in by the user, the login is performed automatically. If none or only a part of the fields are filled, the IGEL OS login dialog is presented to the user.

> To use this authentication method, make sure the following requirements are met:
> - HTTP basic authentication is enabled on the server and the endpoint device. The relevant registry parameter is **app.cwa.authman.protocols.httpbasic.enabled** (enabled by default). Web pages served via HTTPS will always be encrypted, regardless of this setting.
> - You are using Citrix on-premises; this method is not available for the cloud solution.
> - To ensure an encrypted connection, HTTPS should be specified in the **Store URL** on the **Server** page.

- **Credential passthrough**: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.

  To use this authentication method, make sure the following requirements are met:
  - HTTP basic authentication is enabled on the server.
  - You are using Citrix on-premises; this method is not available for the cloud solution.
  - To ensure an encrypted connection, HTTPS should be specified in the **Store URL** on the **Server** page.

Username

This setting is only available if the **Authentication method** is set to **IGEL login**.

Username for authentication via **IGEL login**.

Domain

This setting is only available if the **Authentication method** is set to **IGEL login**.

Domain for authentication via **IGEL login**.

Password

This setting is only available if the **Authentication method** is set to **IGEL login**.

Password for authentication via **IGEL login**.

CUPS printing app



- Getting Started with CUPS Printing on IGEL OS (see page 65)
- Configuration of CUPS Printing on IGEL OS (see page 67)

Getting Started with CUPS Printing on IGEL OS

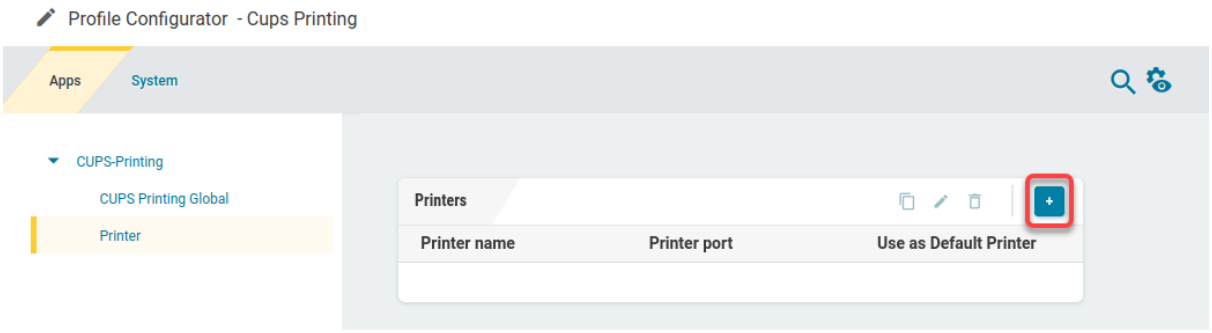
Printers cannot yet be detected automatically.

Because the endpoint device merely places incoming print jobs in a queue, you need to install the printer on the server. Note that you will need to be logged in as an administrator to the terminal to which the printer is connected.

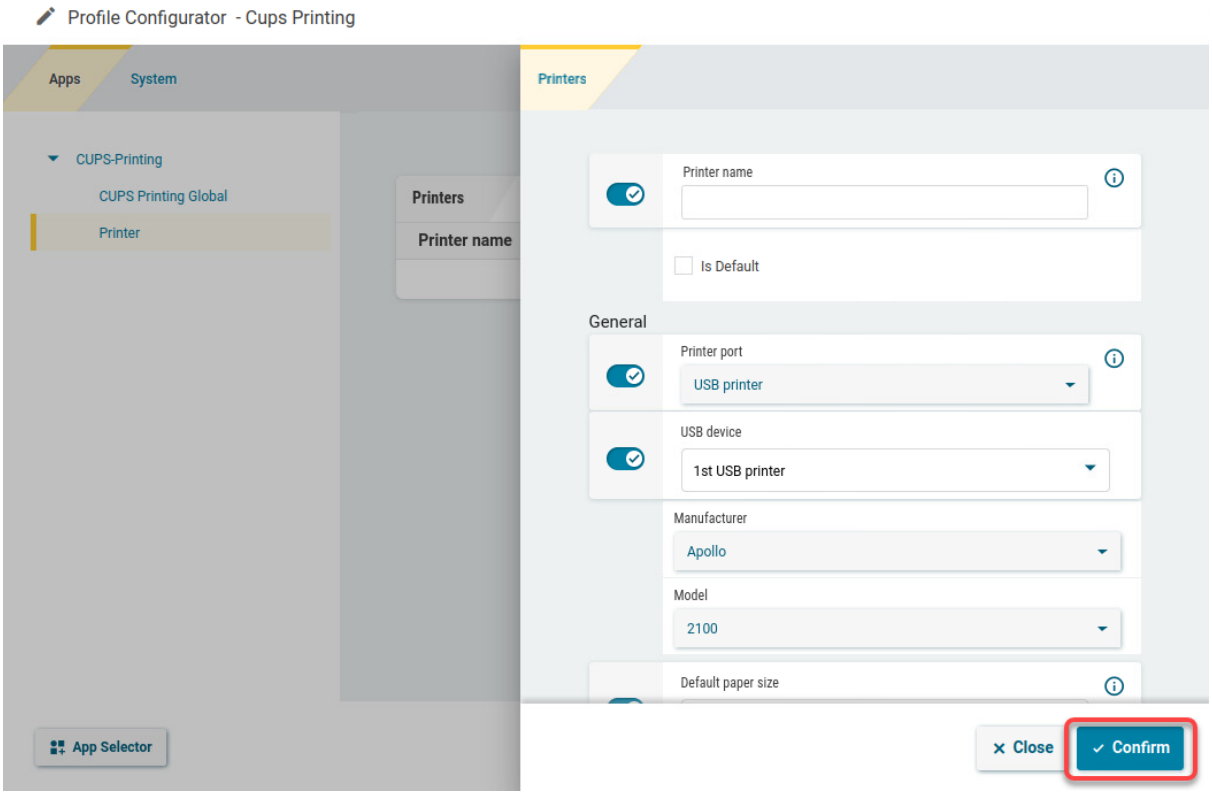
Settings made here apply to local printing (e.g. PDF, Chromium etc.) and to mapping a local printer into a session.

How to Set Up a Printer

1. In the profile configurator, go to **Apps > CUPS Printing > Printer** and click +.



2. Edit the settings according to your needs and then click **Confirm**.

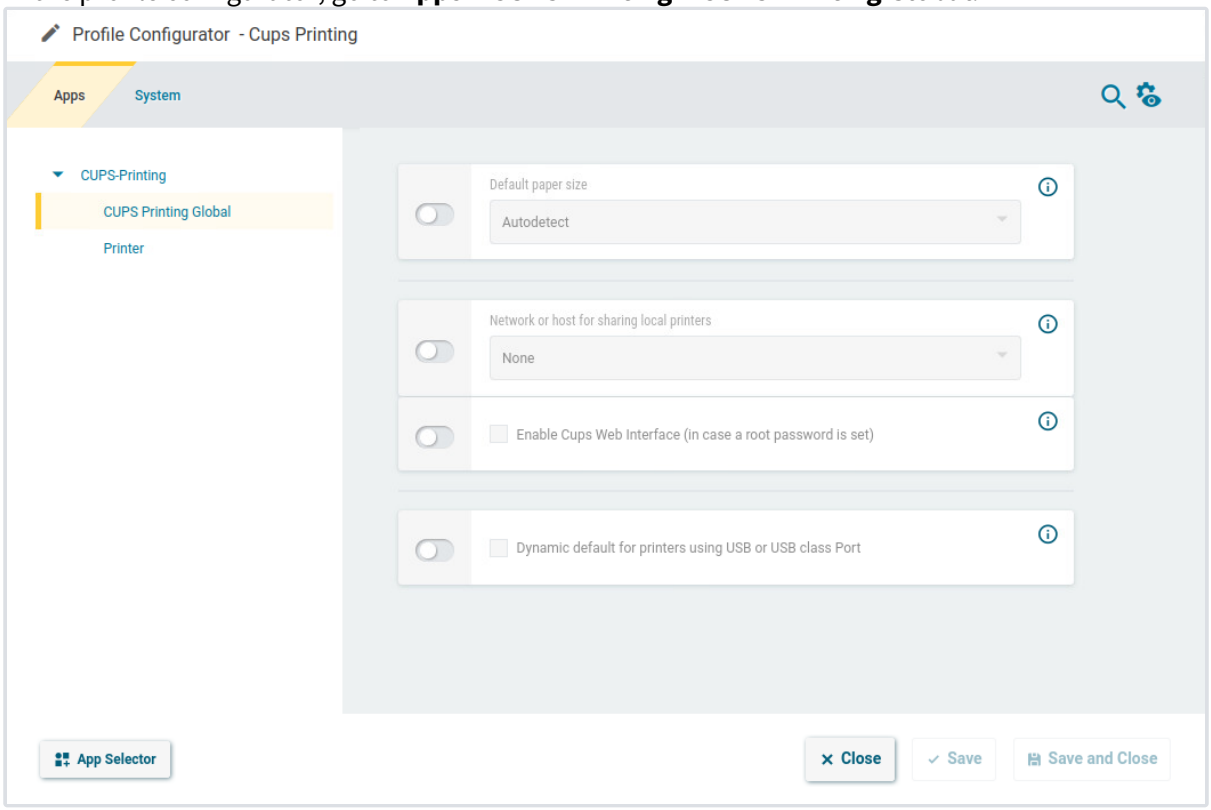


Configuration of CUPS Printing on IGEL OS

Configuring Global Printer Settings

The settings defined here are valid for all printers if not specified otherwise.

1. In the profile configurator, go to **Apps > CUPS Printing > CUPS Printing Global**.



2. Edit the settings according to your needs. The parameters are described in the following.

Default paper size

Set the printer-specific paper size that you would like to use as a default.

Possible values:

- **Autodetect** (default)
- **Letter**
- **Legal**
- **Executive**
- **A5**
- **A4**
- **A3**

Network or host for sharing local printers

Access to the printer is possible from this network or host.

Possible values:

- **None** (default)
- **Local network**: Allows printing on the local device from the local network.

> This can also be given in the form 192.0.2.* or 192.0.2.0/24 or *.domain.com or 192.0.2.1 or host.domain.auth.

- **Global**: Allows printing on the local device from the global network.

Enable CUPS Web Interface (in case a root password is set)

- [x] If you have set a root password under **Security > Password > Administrator**, you can enable the CUPS web interface on port 631. You can access it via the browser at http://localhost:631/
- [ ] The CUPS Web Interface is disabled. (Default)

Dynamic default for printers using USB or USB class port

If your users frequently change their workplace, e.g. in a mobile workplace scenario, they might often face the problem that the local printer is not the one that is set as the default printer and, as a result, this local printer may not be redirected to the remote session.

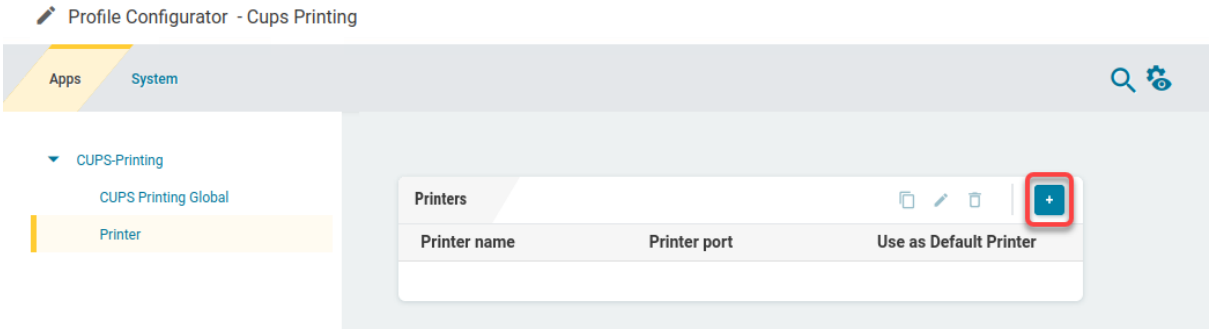
To save your users from dealing with default printer selection, you can configure IGEL OS to automatically set the currently connected printer as the default printer. This feature works with USB printers and USB class printers.

- [x] The currently connected USB printer or USB class printer will be automatically set as the default printer (no matter if any of the printers under **CUPS Printing > Printer** has already been selected manually as the default printer via **Is Default**). If several printers are connected at the same time, the last printer you plugged in will be automatically set as the default printer.
- [ ] The dynamic selection of the default printer is disabled. (Default)

> **Limitations**
> The method of the dynamic selection of the default printer is feasible if only one printer is connected at a time.
> Note: The default printer selection may change on a reboot of the endpoint device. This means: If two or more printers are connected to the endpoint device at the same time, the printer that was dynamically selected as the default printer before the reboot will NOT necessarily remain the default printer after the reboot.
> Best practice recommendations for the case when multiple USB printers are used can be found hier.

Configuring an Individual Printer

1. In the profile configurator, go to **Apps > CUPS Printing > Printer** and click + . If you want to edit an existing printer, select it and click ✎ .



2. Edit the settings according to your needs. The parameters are described in the following.

Printer name

The name by which this printer will be referred to. Maximum length: 127 characters. The printer's name must start with a letter. Allowed characters: Letters, digits, underscores; blank spaces are not allowed.

> The name of each printer must be unique.

Is default

☑ This printer is the default printer for all sessions. See also Dynamic Selection of the Default Printer on IGEL OS[23] (OS 11 article).

Printer port

Interface type for locally connected printers or the network protocol for network printers. For details, see Settings to Be Configured for Each Printer Port Type[24] (IGEL OS 11 article).

- **USB printer**
- **USB class printer**
- **TCP network printer**
- **IPP network printer**

> Depending on the chosen **Printer port** type, different parameters have to be configured.

23. https://kb.igel.com/en/igel-os/11.10.250/dynamic-selection-of-the-default-printer-on-igel-o
24. https://kb.igel.com/en/igel-os/11.10.250/settings-to-be-configured-for-each-printer-port-ty

If multiple USB printers are used at the same time, it is not recommended to use "2nd USB printer"/ "1st USB printer" (**Printer port**="USB printer") since the numbering depends on the timing the printer is registered on the endpoint and can be different on the next reboot. Instead, it is advisable to use one of the following methods:
USB Printer Class
The printer is assigned by matching patterns. This method is recommended if the endpoint device is to be configured completely with the UMS, preferably with a profile.

1. Open the relevant printer under **CUPS Printing > Printer**.
2. Set **Printer port** to "USB class printer" and edit the printer settings appropriately.
3. Optional: Set the printer as the default printer by enabling **Is Default**.

Manufacturer

List of possible printer manufacturers. When you select a manufacturer here, the relevant selection of models will be provided under **Model**.

A custom printer driver cannot yet be defined.

Model

List of possible models.

Default paper size

Set the printer-specific paper size that you would like to use as a default.
Possible values:

- **Letter**
- **Legal**
- **Executive**
- **A5**
- **A4**
- **A3**
- **System setting**: The global setting is used. (Default)

Share printer

- ☑ You can access the printer via the network if you have enabled the print server under **CUPS Printing > CUPS Printing Global > Network or host for sharing local printers**. (Default)

Map printer in Citrix sessions

- ☑ The printer is available in Citrix sessions. (Default)

Install the HP Color LaserJet 2800 Series PS driver on the server side to redirect the local printer to Citrix sessions, see https://support.citrix.com/article/CTX140208.

Map printer in AVD sessions

☑ The printer is available in AVD sessions. (Default)

CUPS printer redirection must also be activated under **AVD > AVD Sessions > [session name] > Printing**.

Printer driver

Windows driver name for the automatically created printer. Specify only if the Universal Printer Driver should not be used.

The name must not contain “;” or “:”.
Note that special characters, spaces, and case-sensitive characters are relevant when specifying a driver name.

FabulaTech Plugins



- Getting Started with FabulaTech Plugins on IGEL OS (see page 73)

Getting Started with FabulaTech Plugins on IGEL OS

Dependencies

FabulaTech Plugins is connecting FabulaTech products with different remote desktop clients. As it is not a standalone application, at least one of the following apps must be installed and configured as well:

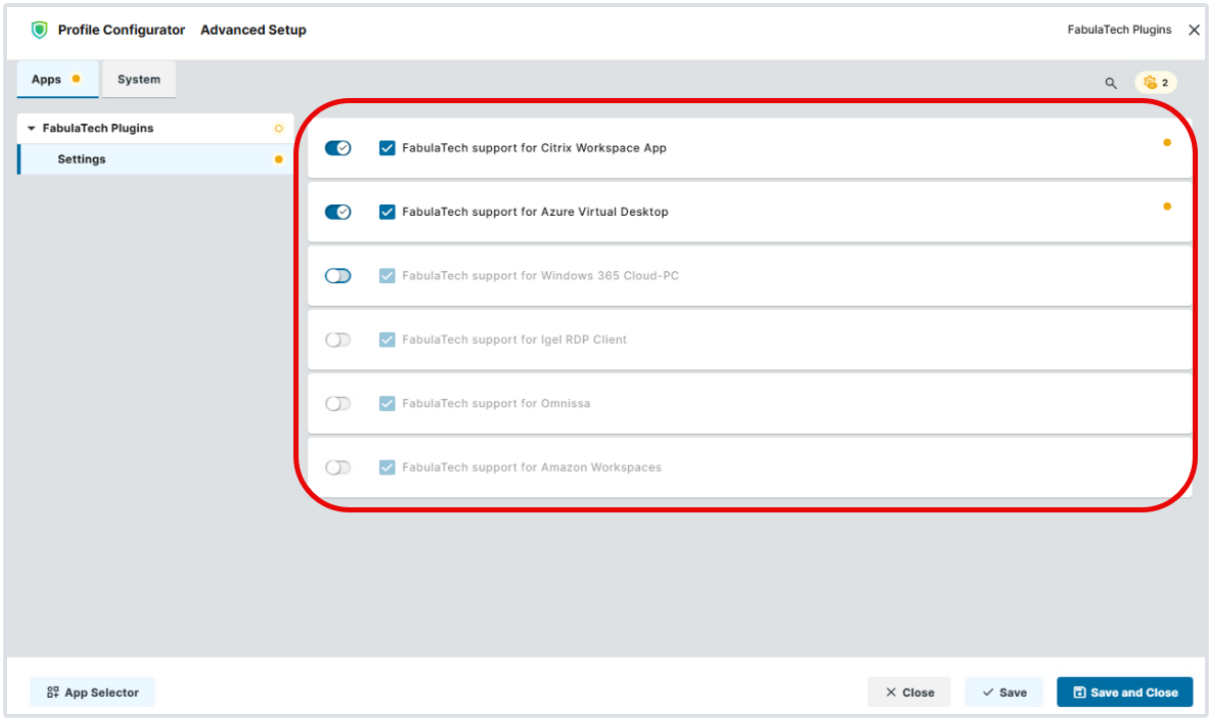
- FabulaTech USB for Remote Desktop
- FabulaTech Scanner for Remote Desktop
- FabulaTech Webcam for Remote Desktop

Important Notes

- For the Fabulatech USB Redirection, a server-side component is required. We recommend the USB for Remote Desktop IGEL Edition; see http://www.usb-over-network.com/partners/igel/ . For details on the configuration, see https://www.usb-over-network.com/partners/igel/usb-for-remote-desktop-docs.html . Please note that licenses must be purchased from Fabulatech to enable this functionality.
- Enable either native USB redirection or Fabulatech USB Redirection – not both together.
- Disable USB redirection if you use DriveLock.
- Ensure that no other hotplug storage device (USB memory stick) is connected before you enable Fabulatech USB redirection. Otherwise, the hotplug storage device is insecurely removed.
- Generally, Fabulatech USB Redirection might not be the ideal solution for each use case. For details, refer to the general device redirection recommendations of your terminal server or VDI vendor.

How to Disable or Enable the Plugin

1. In the profile configurator, go to **Apps > FabulaTech Plugins > Settings**.



2. Change the settings as required.

FabulaTech support for Citrix Workspace App

- ☑ The FabulaTech plugin is enabled in Citrix sessions. (Default)
- ☐ The FabulaTech plugin is disabled in Citrix sessions.

FabulaTech support for Azure Virtual Desktop

- ☑ The FabulaTech plugin is enabled in AVD sessions. (Default)
- ☐ The FabulaTech plugin is disabled in AVD sessions.

FabulaTech support for Windows 365 Cloud PC

- ☑ The FabulaTech plugin is enabled in IGEL Windows 365 sessions. (Default)
- ☐ The FabulaTech plugin is disabled in IGEL Windows 365 sessions.

FabulaTech support for IGEL RDP Client

- ☑ The FabulaTech plugin is enabled in IGEL RDP sessions. (Default)
- ☐ The FabulaTech plugin is disabled in IGEL RDP sessions.

FabulaTech support for Omnissa

- [x] The FabulaTech plugin is enabled in Omnissa Horizon sessions. (Default)
- [ ] The FabulaTech plugin is disabled in Omnissa Horizon sessions.

FabulaTech support for Amazon Workspaces

- [x] The FabulaTech plugin is enabled in Amazon Workspaces sessions. (Default)
- [ ] The FabulaTech plugin is disabled in Amazon Workspaces sessions.

FabulaTech Scanner for Remote Desktop



- Getting Started with FabulaTech Scanner for Remote Desktop OS (see page 77)

Getting Started with FabulaTech Scanner for Remote Desktop OS

More detailed information about the function can be found on the Fabulatech partner site: http://www.usb-over-network.com/partners/igel/.

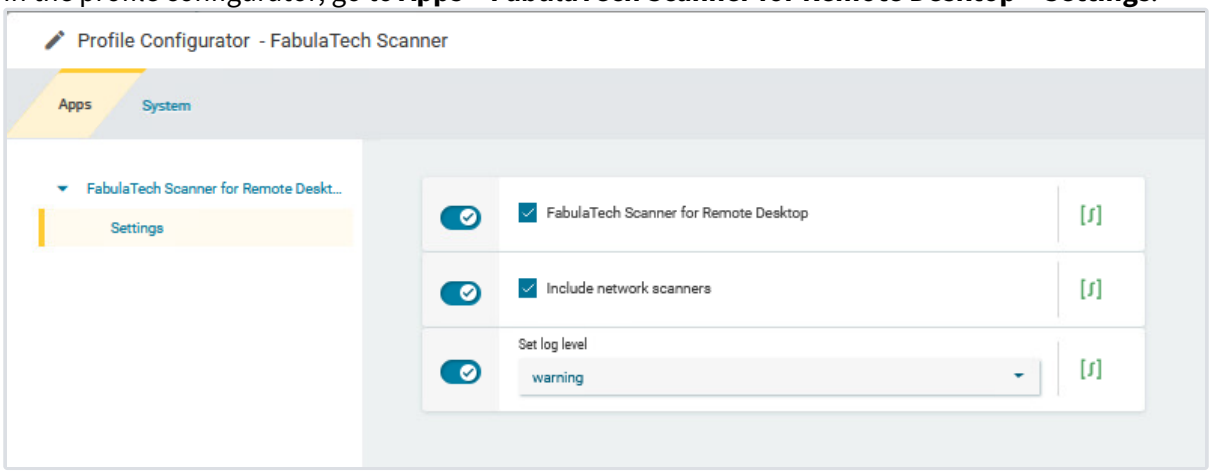
Dependencies

To use the FabulaTech Scanner redirection, the following apps must be installed and configured as well:

- FabulaTech Plugins. For configuration details, see Getting Started with FabulaTech Plugins on IGEL OS[25].

How to Disable or Enable the Scanner Redirection

1. In the profile configurator, go to **Apps > FabulaTech Scanner for Remote Desktop > Settings**.



2. Change the settings as required.

FabulaTech Scanner for Remote Desktop

- Fabulatech Scanner redirection is enabled for the sessions that are enabled in the FabulaTech Plugins app. (Default)
- Fabulatech Scanner redirection is disabled.

Include network scanners

- Scanners that are made available to the device through the network are also redirected. (Default)
- Network scanners are not redirected.

Set log level

25. https://kb.igel.com/en/igel-apps/current/getting-started-with-fabulatech-plugins-on-igel-os

Defines the degree of detail written into the log file.
Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

FabulaTech USB for Remote Desktop



- Getting Started with FabulaTech USB for Remote Desktop on IGEL OS (see page 80)

Getting Started with FabulaTech USB for Remote Desktop on IGEL OS

More detailed information about the function can be found on the Fabulatech partner site: http://www.usb-over-network.com/partners/igel/.

Dependencies

To use the FabulaTech USB redirection, the following apps must be installed and configured as well:

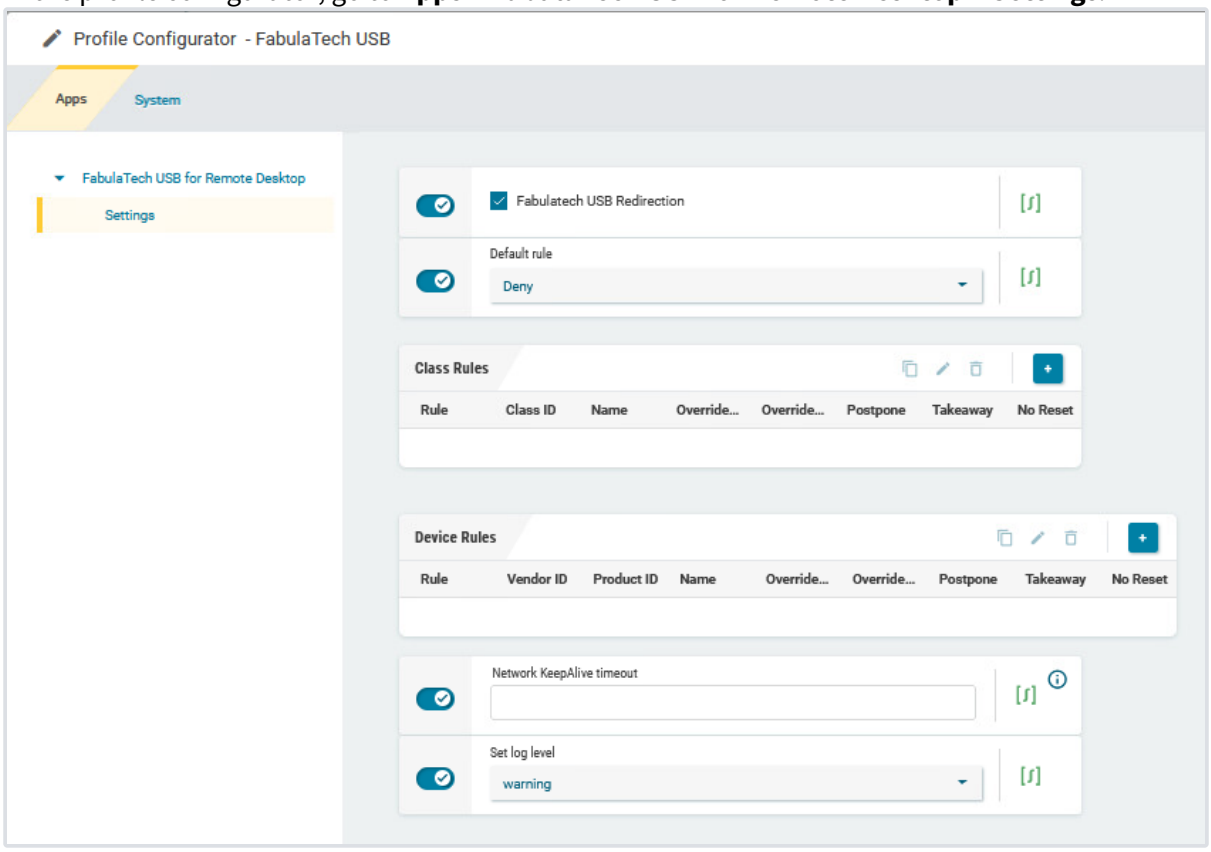
- FabulaTech Plugins. For configuration details, see Getting Started with FabulaTech Plugins on IGEL OS[26].

Possible Conflicts

The FabulaTech USB for Remote Desktop application conflicts with the IGEL Advanced Device Redirection USB application. You cannot use both applications at the same time.

How to Disable or Enable the USB Redirection

1. In the profile configurator, go to **Apps > FabulaTech USB for Remote Desktop > Settings**.



26. https://kb.igel.com/en/igel-apps/current/getting-started-with-fabulatech-plugins-on-igel-os

2. Change the settings as required.

FabulaTech USB Redirection

☑ Fabulatech USB redirection is enabled for the sessions that are enabled in the FabulaTech Plugins app. (Default)

☐ Fabulatech USB redirection is disabled.

Default rule

This rule will apply if no special rule was configured for a class or a device.

- **Deny**: Devices are only redirected if they have **Allow** rules configured under **Class Rules** or **Device Rules**. (Default)
- **Allow**: Devices are always redirected unless they have **Deny** rules configured under **Class Rules** or **Device Rules**.

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- Click + to create a new entry.
- Click 🗑 to remove the selected entry.
- Click ✎ to edit the selected entry.
- Click ⧉ to copy the selected entry.

Clicking + brings up the **Class Rules** dialog, where you can define the options described under Class Rules (see page 82).

Device Rules

A device rule applies to a specific device that is identified by its serial number.

To manage rules, proceed as follows:

- Click + to create a new entry.
- Click 🗑 to remove the selected entry.
- Click ✎ to edit the selected entry.
- Click ⧉ to copy the selected entry.

Clicking + brings up the **Device Rules** dialog, where you can define the options described under Device Rules (see page 86).

Network KeepAlive timeout

Interval in seconds between keep-alive messages sent to the server port to prevent the client-server link from being broken.

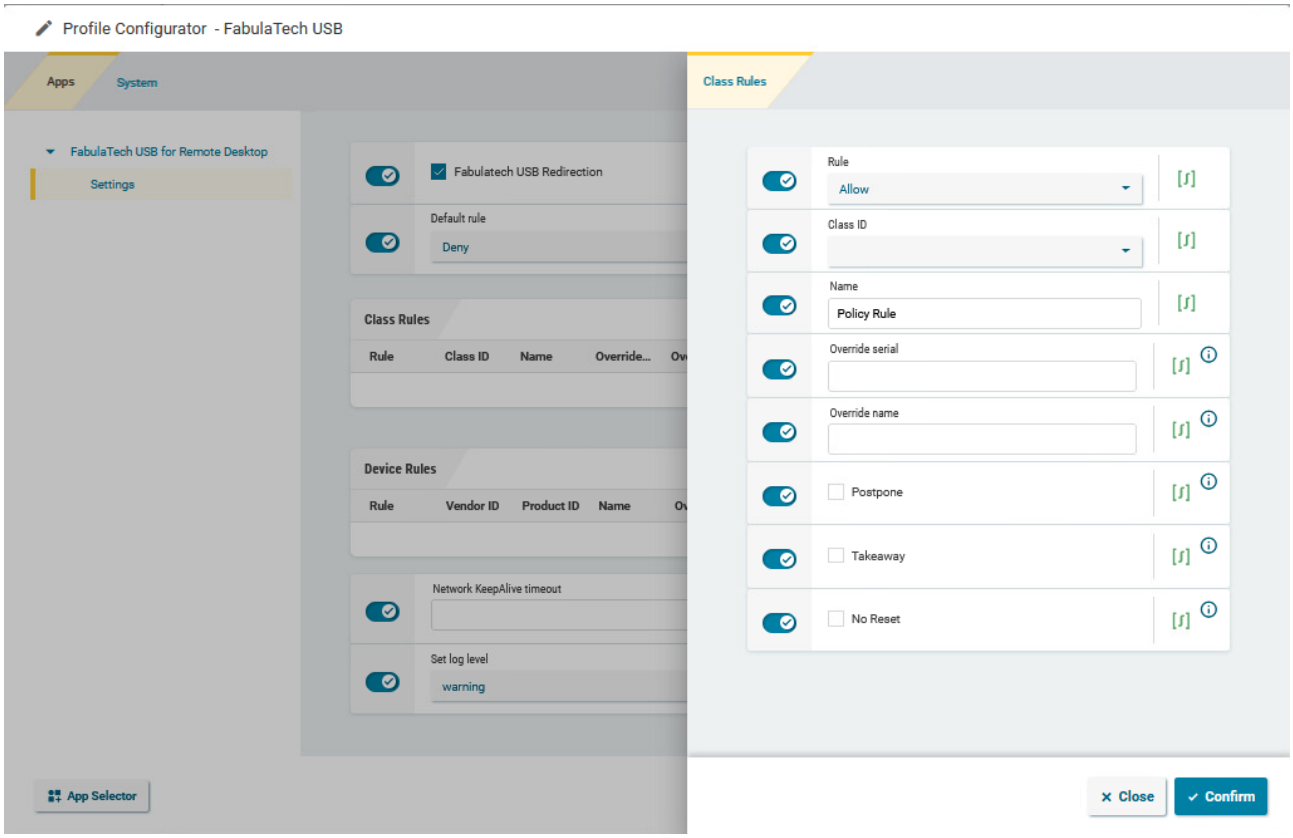
Set log level

Defines the degree of detail written into the log file.

Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

Class Rules



Rule

- **Allow**: Devices that have the properties defined here are redirected by the Fabulatech USB redirection. (Default)
- **Deny**: Devices that have the properties defined here are not redirected.

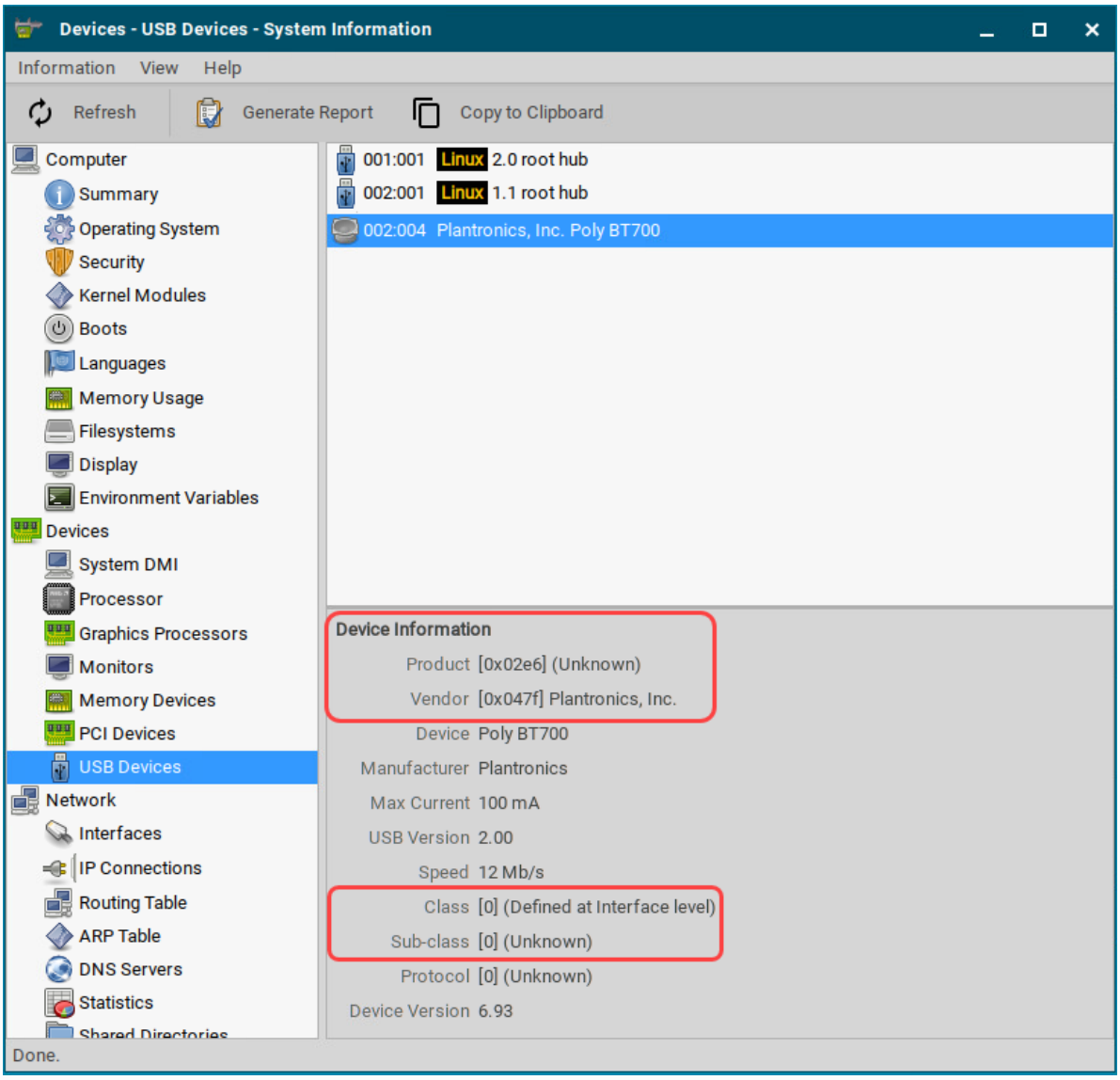
Class ID

Device class

Getting USB Device Information

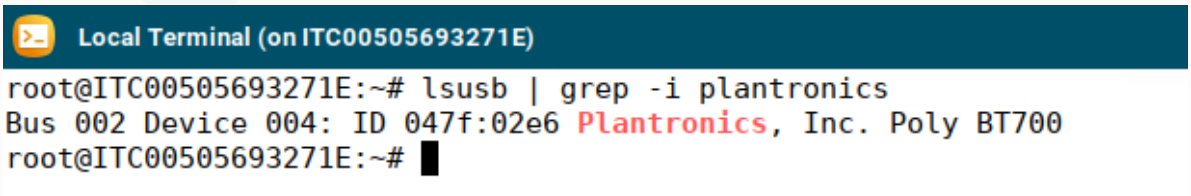
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see System Information[27].
System Information example:

27. https://kb.igel.com/en/igel-os-base-system/current/system-information



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

Example for `lsusb`:



Subclass ID

Subclass relating to the specified device class

Name

Free text entry

Override serial

Serial number that will appear in the session

Override name

Device name that will appear in the session

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts.
- ☐ The USB device is no longer shown immediately after the system is booted. (Default)

> This setting is only effective if the **Takeaway** parameter is enabled.

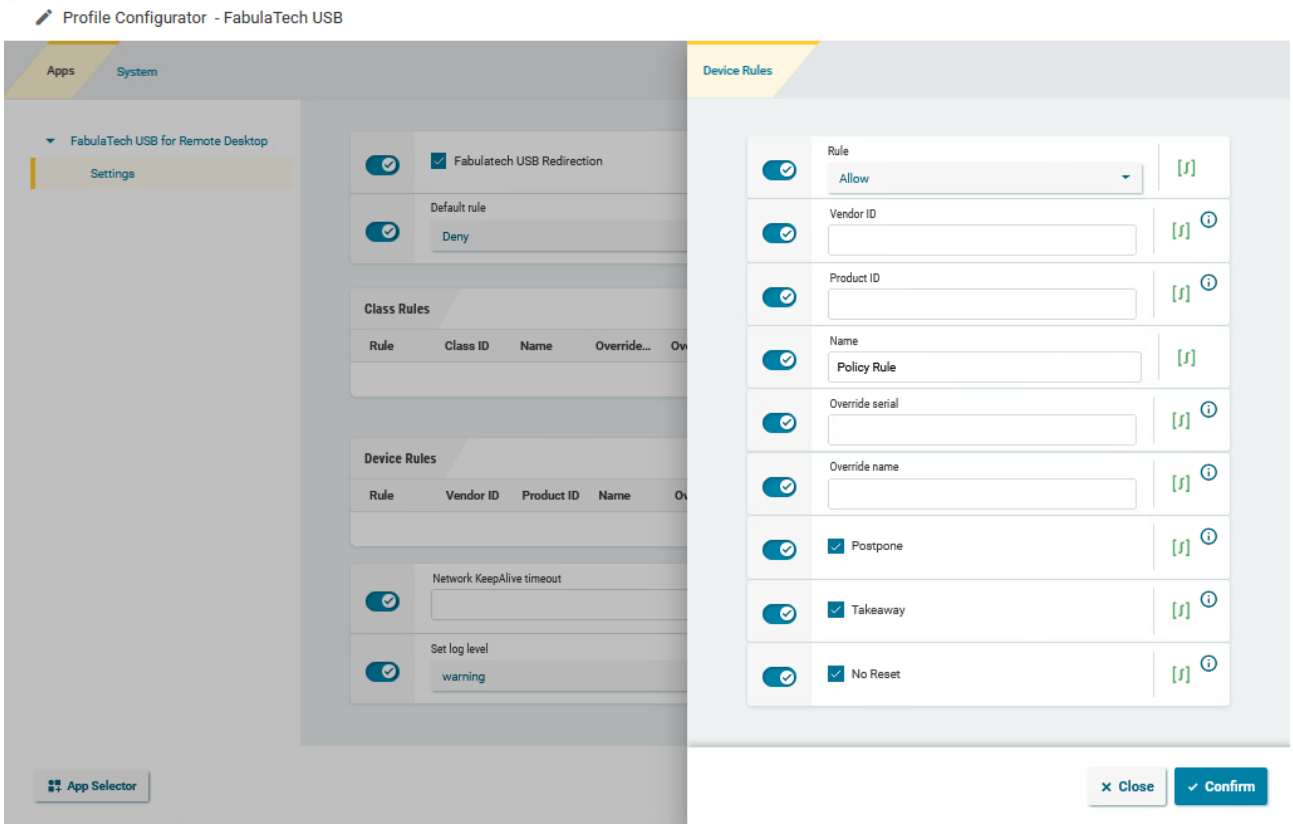
Takeaway

- ☑ The USB device may be removed from the system (endpoint device).
- ☐ The USB device may not be removed. (Default)

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated.
- ☐ The device will be reset after the connection with the session has been terminated. (Default)

Device Rules



Rule

- **Allow**: Devices that have the properties defined here are redirected by the Fabulatech USB redirection. (Default)
- **Deny**: Devices that have the properties defined here are not redirected.

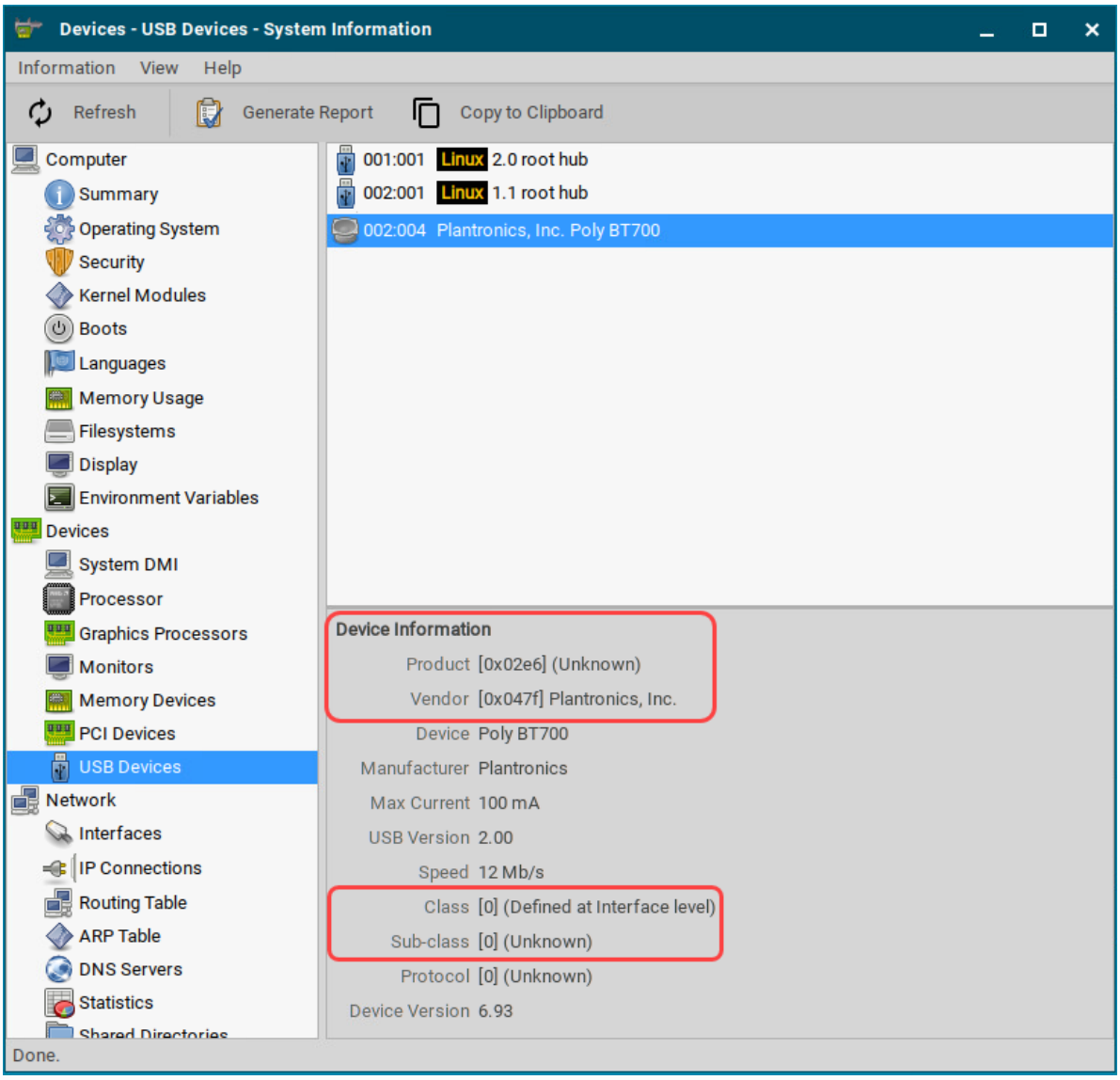
Vendor ID

Hexadecimal manufacturer number

Getting USB Device Information

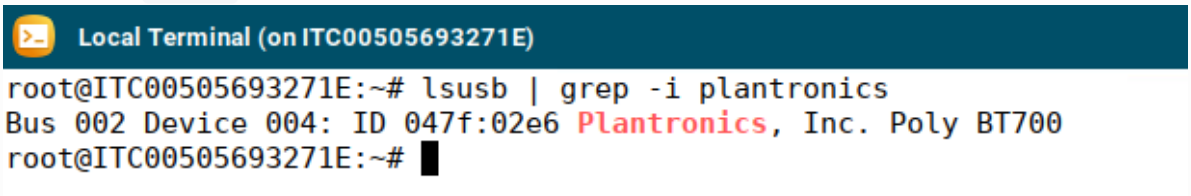
To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see System Information[28].
System Information example:

28. https://kb.igel.com/en/igel-os-base-system/current/system-information



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

Example for `lsusb`:



Product ID

Hexadecimal device number

Name

Free text entry

Override serial

Serial number that will appear in the session

Override name

Device name that will appear in the session

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts. (Default)
- ☐ The USB device is no longer shown immediately after the system is booted.

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- ☑ The USB device may be removed from the system (endpoint device). (Default)
- ☐ The USB device may not be removed.

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated. (Default)
- ☐ The device will be reset after the connection with the session has been terminated.

FabulaTech Webcam for Remote Desktop



- Getting Started with FabulaTech Webcam for Remote Desktop on IGEL OS (see page 90)

Getting Started with FabulaTech Webcam for Remote Desktop on IGEL OS

More detailed information about the function can be found on the Fabulatech partner site: http://www.usb-over-network.com/partners/igel/.

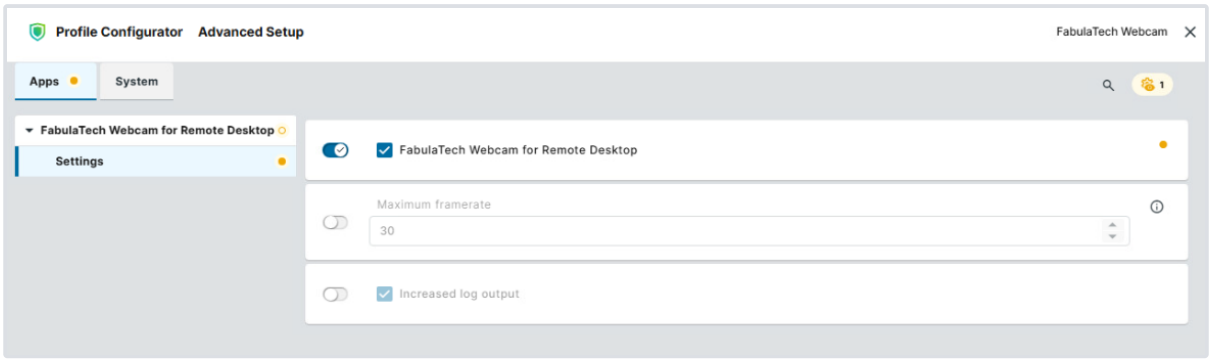
Dependencies

To use the FabulaTech Webcam redirection, the following apps must be installed and configured as well:

- FabulaTech Plugins. For configuration details, see Getting Started with FabulaTech Plugins on IGEL OS[29].

How to Disable or Enable the Webcam Redirection

1. In the profile configurator, go to **Apps > FabulaTech Webcam for Remote Desktop > Settings**.



2. Change the settings as required.

FabulaTech Webcam for Remote Desktop

- ☑ Fabulatech Webcam redirection is enabled for the sessions that are enabled in the FabulaTech Plugins app. (Default)
- ☐ Fabulatech Webcam redirection is disabled.

Maximum framerate

The maximum framerate can be defined on a 1-30 scale. (Default: 30)

Increased log output

29. https://kb.igel.com/en/igel-apps/current/getting-started-with-fabulatech-plugins-on-igel-os

- [x] The information written into the log file is increased. (Default)
- [ ] The information written into the log file is set to minimal.

HP BIOS Tools

With the HP BIOS Tools OS 12 app, you can manage and update the BIOS, BIOS settings, and BIOS password of supported Hewlett-Packard (HP) devices using the IGEL Universal Management Suite (UMS).

You can use profiles and specific device commands to handle any number of devices.

BIOS Updates at Your Own Risk
IGEL is offering and supporting the BIOS Update mechanism - BIOS updates are performed at your own risk!

The BIOS update mechanism is functional even with Secure Boot enabled and when a BIOS password is set.

Supported Devices

The HP BIOS Tools app is supported for the following HP models:

- t540
- Pro t550
- t640
- Elite t655
- t740
- Elite t755
- Elite mt645 G7 (HP BIOS Tools 2.0.0 or higher)
- Elite mt645 G8 (HP BIOS Tools 2.0.0 or higher)
- Pro mt440 G3 (HP BIOS Tools 2.0.0 or higher)
- Elite t660 (HP BIOS Tools 2.0.1 or higher)

Apps That Are Installed with HP BIOS Tools 2.0.0

When HP BIOS Tools 2.0.0 is installed, the following apps are also installed automatically:

- Optional Kernel Modules for IGEL OS 12 Systems (optional_kernel_modules)
- The Base System will be updated to IGEL OS Base System 12.5.0 if not already done

Requirements

- UMS 12.01 or higher
- Supported devices with IGEL OS Base System 12.01.100 or higher

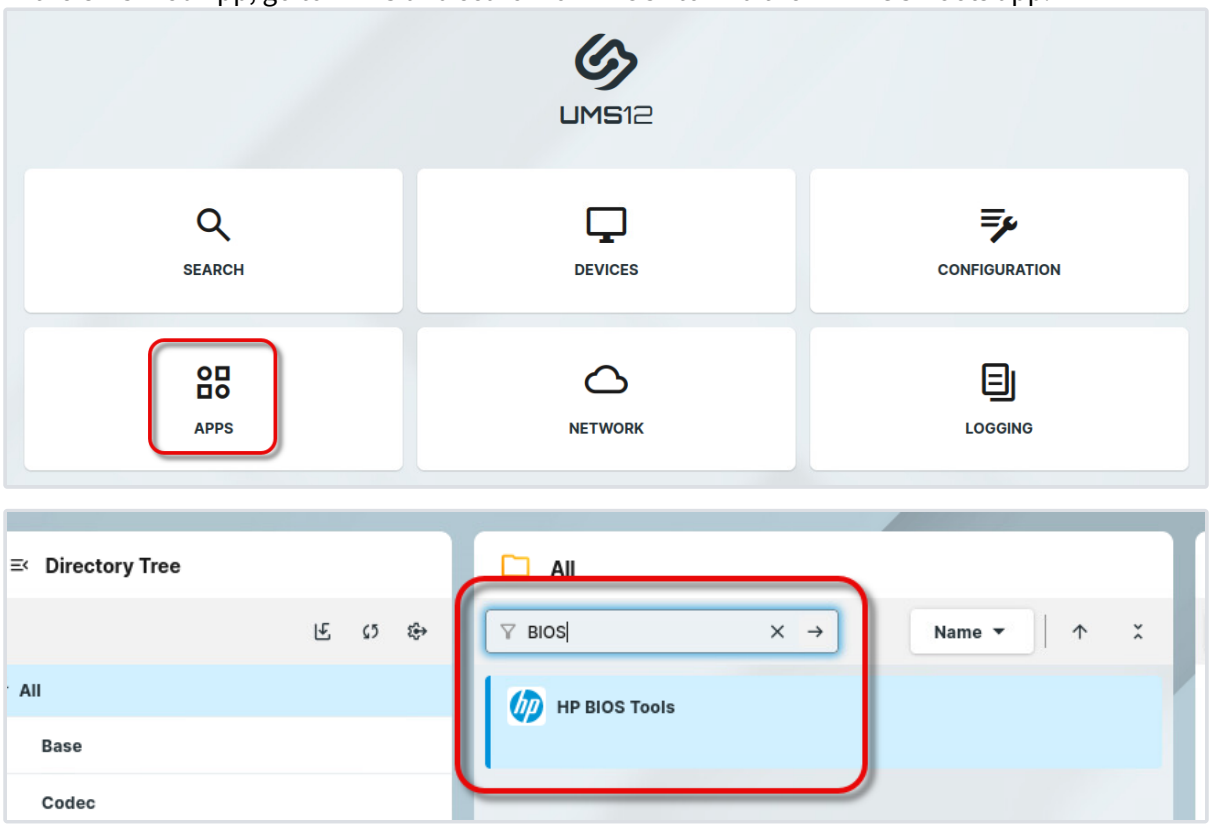
The IGEL OS Base System needs to be installed directly on the device. The HP BIOS Tools app is unsupported if the IGEL OS boots from a UD Pocket.

- A Windows machine for creating the password file

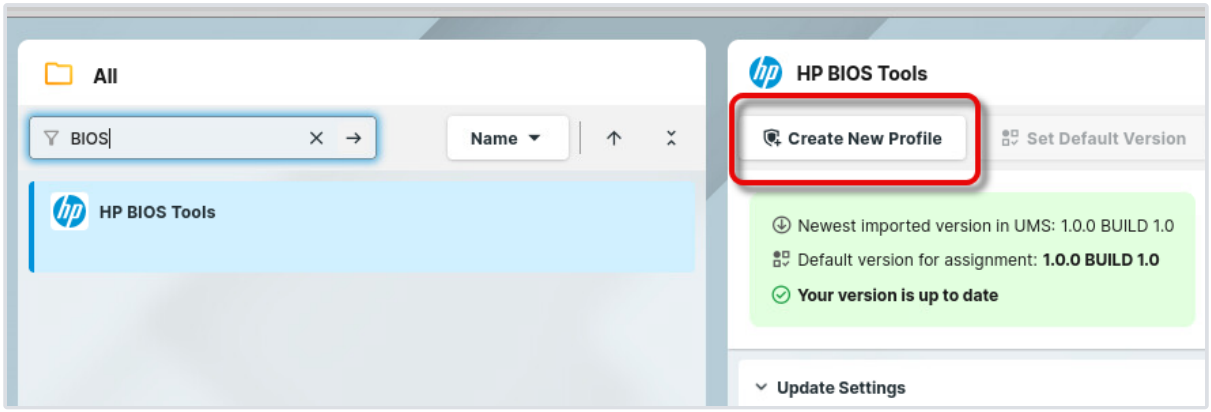
Creating a Profile

If you have not done so already, create a profile for your app.

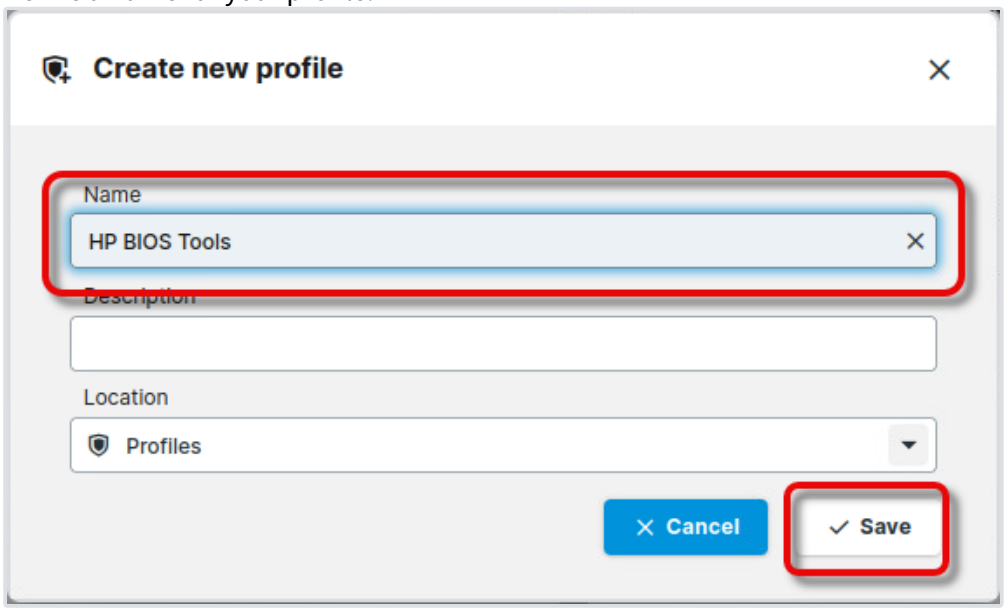
1. In the UMS Web App, go to **APPS** and search for “BIOS” to find the **HP BIOS Tools** app.



2. Click **Create New Profile**.



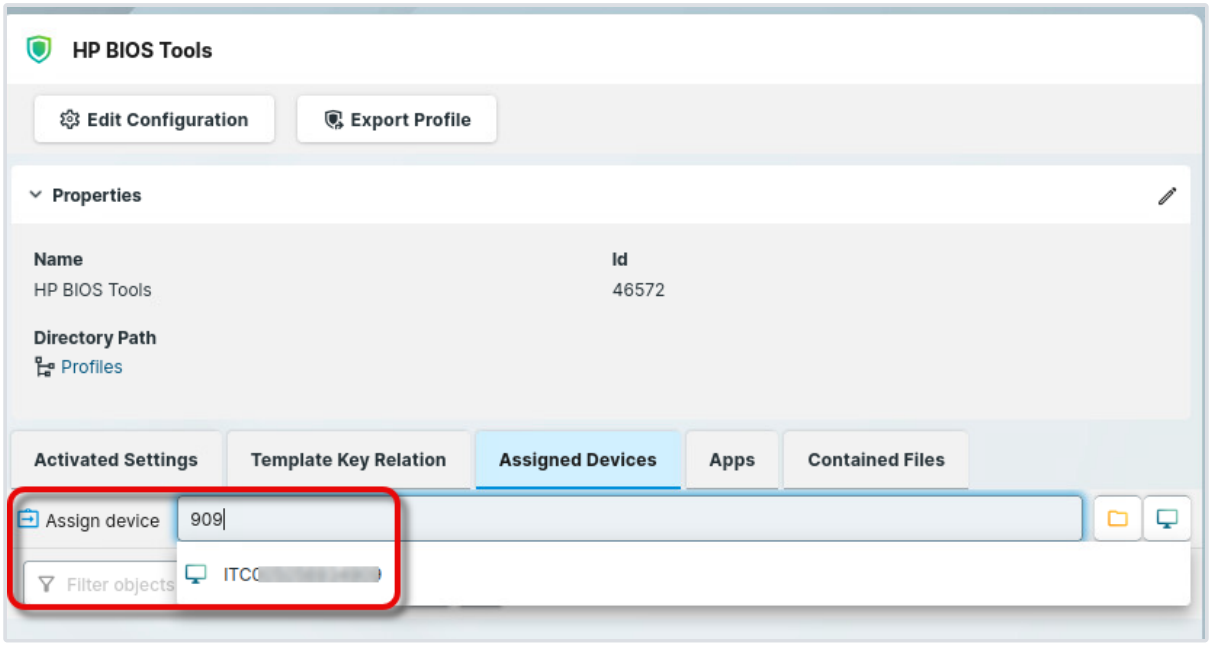
3. Define a name for your profile.



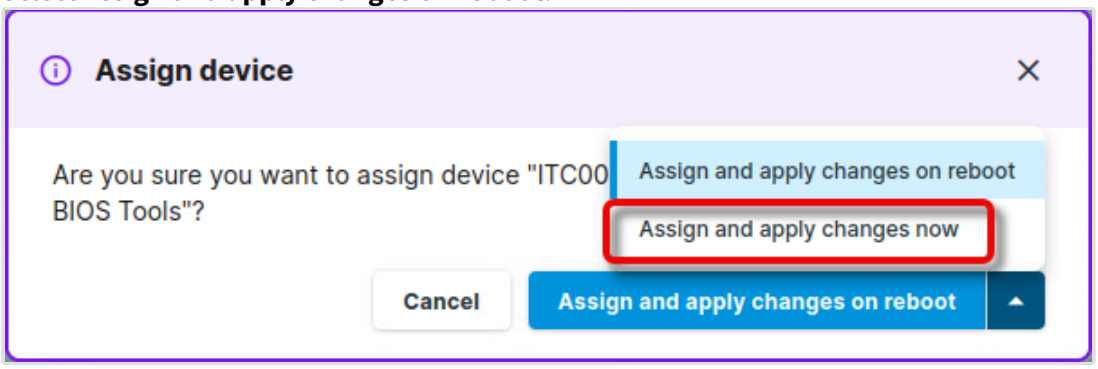
We will use this profile for every use case of the HP BIOS Tools app.

Assigning the Profile to Your Devices

1. In the field **Assign device**, enter the name of the device or device directory for which you want to use the HP BIOS Tools app.



2. Select **Assign and apply changes on reboot**.



Setting up the File Source

Since not only updating the BIOS but also its configuration is done using files, we need to set up a file source that is reachable by all devices.

The creation of the files is described in the relevant sections. The procedures described here are the same for all files in question, that is:

- BIOS update file
- BIOS settings file
- BIOS password file

Security Note

If you use password files, ensure the password file is not accessible longer than necessary.

Using an External Source (HTTP/HTTPS)

If you want to deploy the BIOS update file, the BIOS settings file, and the password file from an external source, you can set up an HTTP/HTTPS server.

You can secure the file access using a username and password. To achieve this, you must configure your devices to provide a username and password:

→ In your HP BIOS Tools profile, edit **Apps > HP BIOS Tools > Password** as follows:

- **Download username**: Username required for downloading
- **Download password**: Password required for downloading



Using a Local Storage Device (USB)

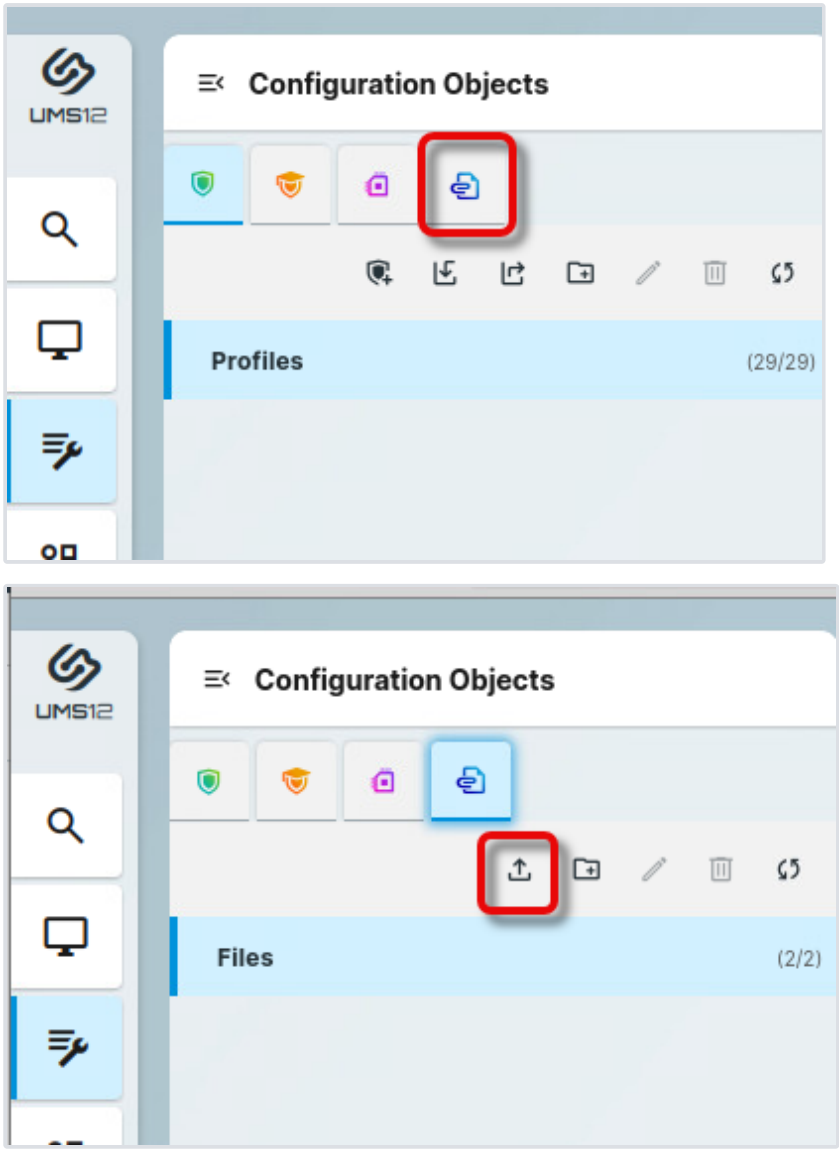
For more information on how to use a storage device with IGEL OS, see Storage Hotplug in IGEL OS 12[30].

Using UMS File Transfer

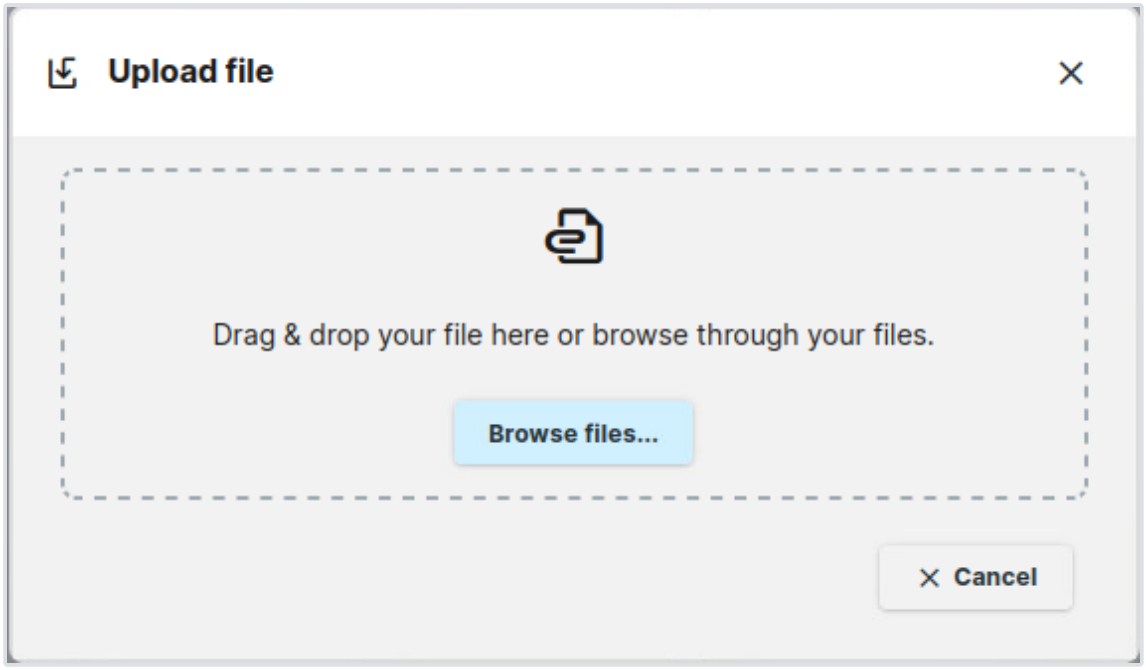
The following example shows how to use the UMS file transfer facility for file deployment. In this example, a BIOS update file is provided; the procedure is the same for settings and password files.

1. In the UMS Web App, go to **Configuration Objects**, select the icon for files, and then the icon for uploads.

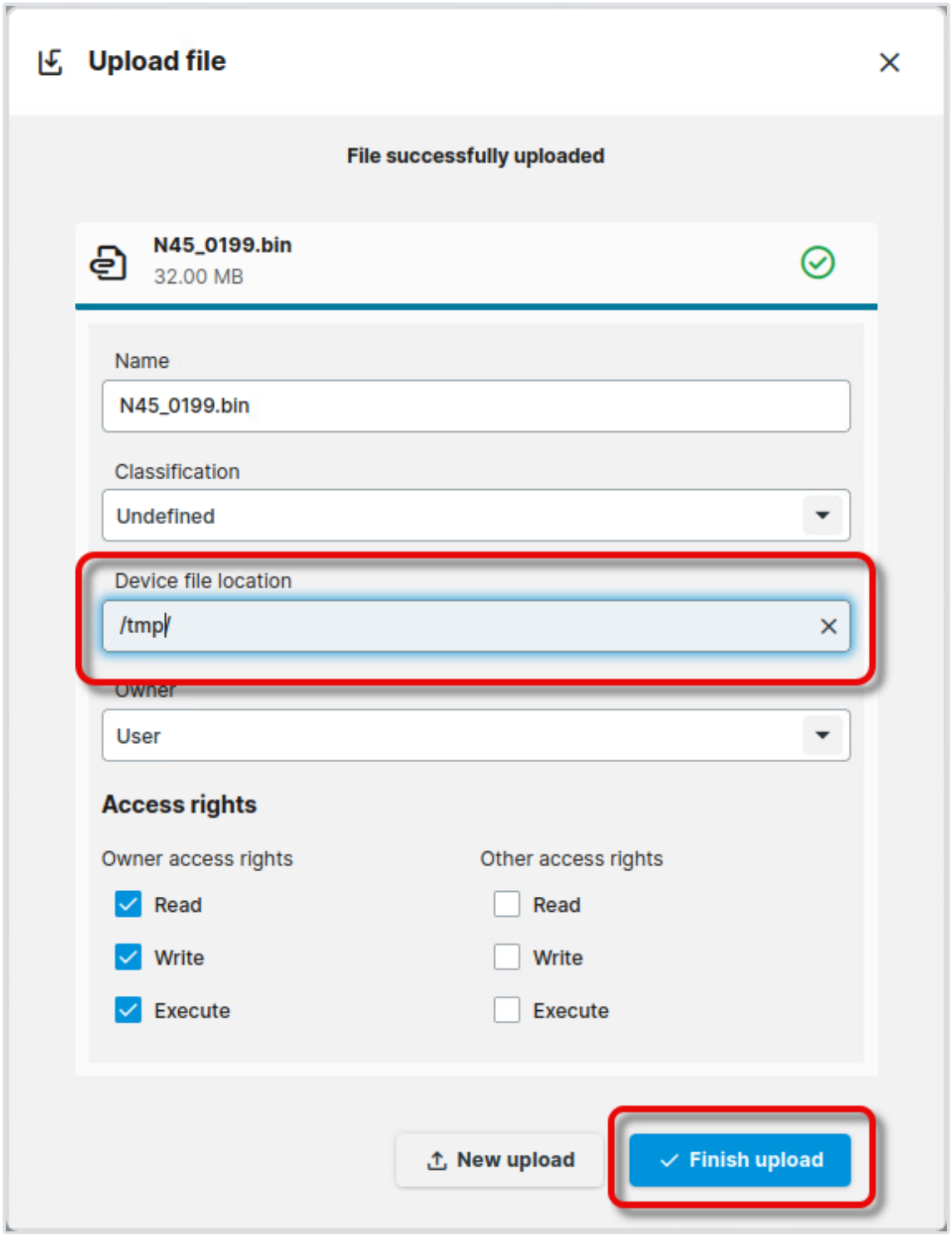
30. https://kb.igel.com/en/igel-os-base-system/12.6.1/storage-hotplug-in-igel-os-12



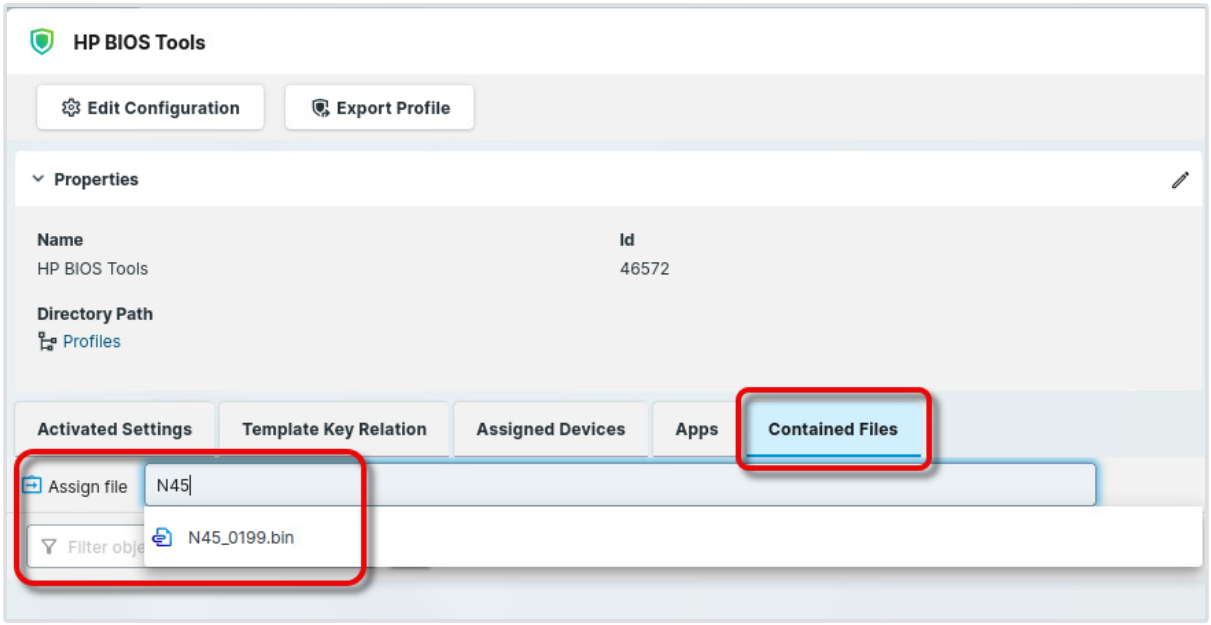
2. Choose the file on your system via drag & drop or via **Browse files...**.

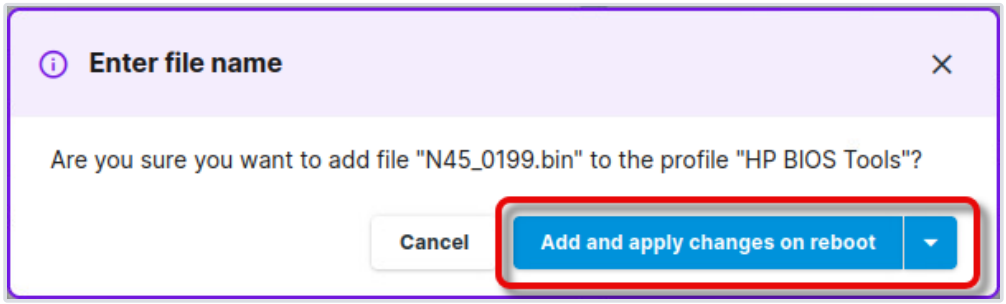


3. In the field **Device file location**, define the local path in which the file will be stored on the device, e.g. `/tmp/`. Afterward, click **Finish upload**.



4. Assign the file to your devices by assigning it to the profile we have created beforehand.



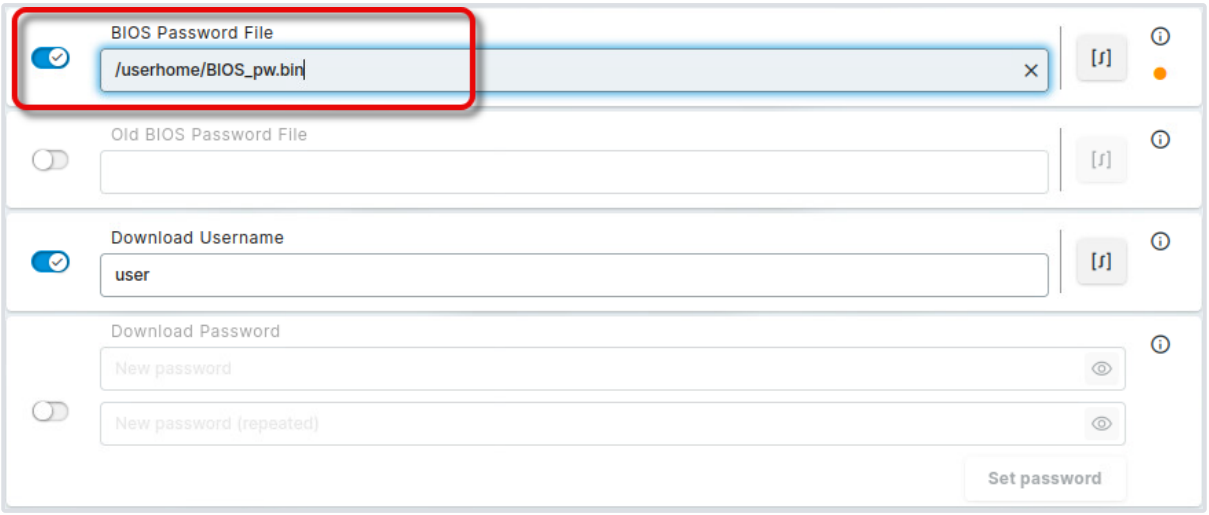


If Your BIOS is Password-Protected: Provide a BIOS Password File to Make Changes

If your BIOS is protected by a password, a valid password file must be provided to allow any kind of changes to the BIOS. For this purpose, you must create a password file and make it available to the device.

As a precondition, you must know the BIOS password of your devices, of course.

1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.htmland install it.
2. Create a password file with the known password and make it available as described under Setting up the File Source (see page 95).
3. In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Password** and enter the file path.



Updating the BIOS

⚠ Some target devices might power off instead of rebooting. This effect has been observed with the following models:

- Elite mt645 G7
- Elite mt645 G8

Getting the BIOS Update File from HP

1. Open https://support.hp.com/, select your device, click **Software, Drivers, and Firmware**, and follow the steps.
2. Download the file (example: `sp126570.exe`) and unzip it.
3. In the directories created by unzipping, look for a file with the ending `.bin`, for instance, `M44_0103.bin`, and store it in a location that is reachable from your UMS machine.

Making the BIOS Update File Available

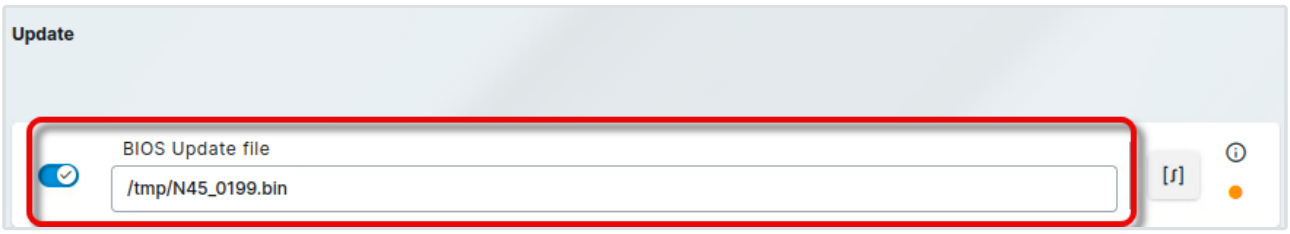
→ Make the BIOS update file available to your devices; see Setting up the File Source (see page 95).

Configuring the Devices for the BIOS Update

> ⚠ You can replace the current BIOS with a higher version, but not the same version. Therefore, restoring the original BIOS that had been installed on the device before is not possible.
> Moreover, it is not possible to downgrade the BIOS.

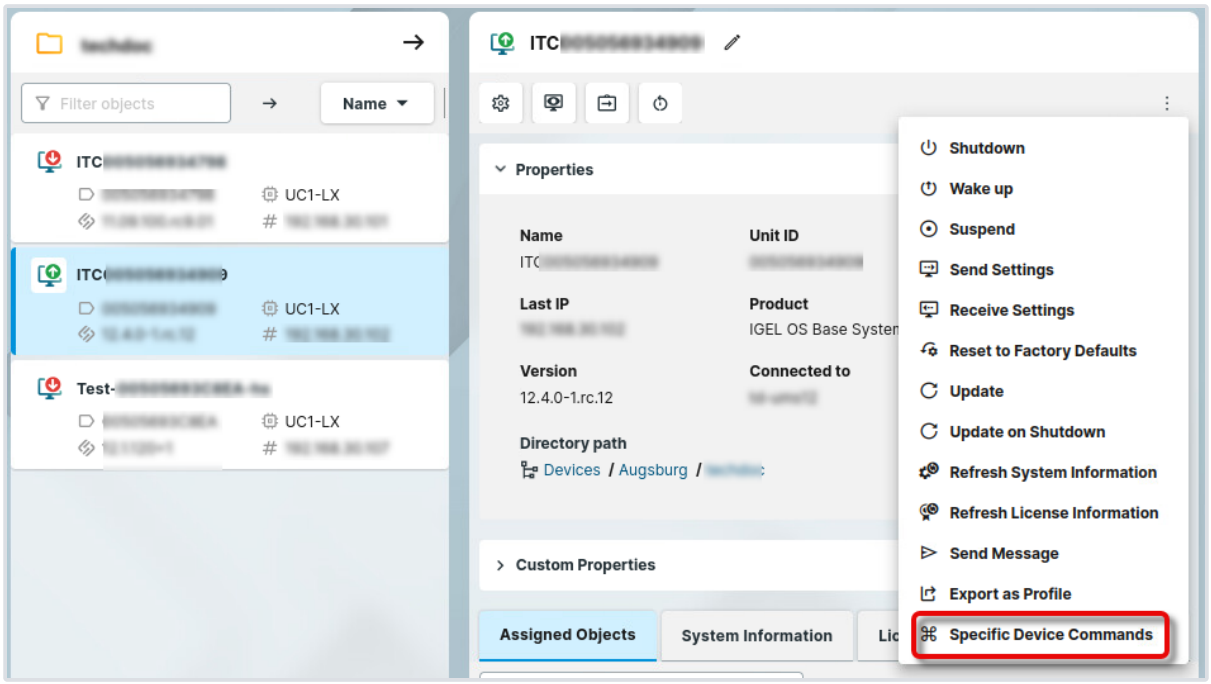
→ In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Update**, make the following edits, and save your settings.

- **BIOS update file**: Local path or URL of the BIOS update file

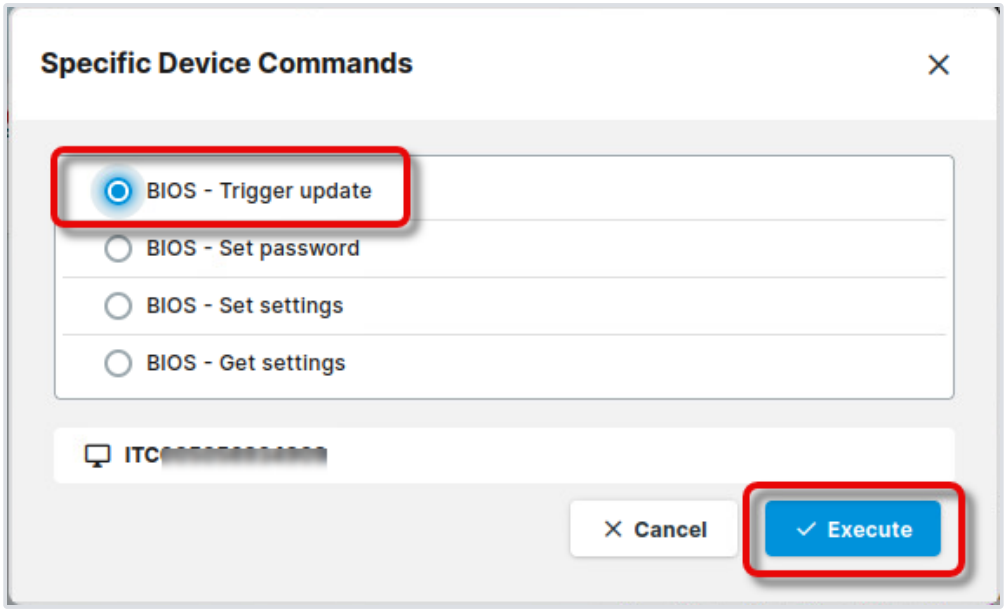


Triggering the BIOS Update

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.



2. Select **BIOS - Trigger update** and click **Execute**.



The target devices receive a reboot command; a corresponding message is displayed.

The timespan before the BIOS logo and the progress bar is shown might be significantly longer than usual. Please ensure that the device remains powered on until the update process is finished.

Changing the BIOS Settings

To change the BIOS settings of the device, a settings file needs to be transferred to the device with the setting updates in the correct syntax.
In the section below, we describe in detail the easiest way to do this, that is:

1. Getting the BIOS settings file from the device through scp. This way you get the correct base file.
2. Editing the transferred file.
3. Transferring the file back to the device or device directory. This way you can distribute the update in batches.

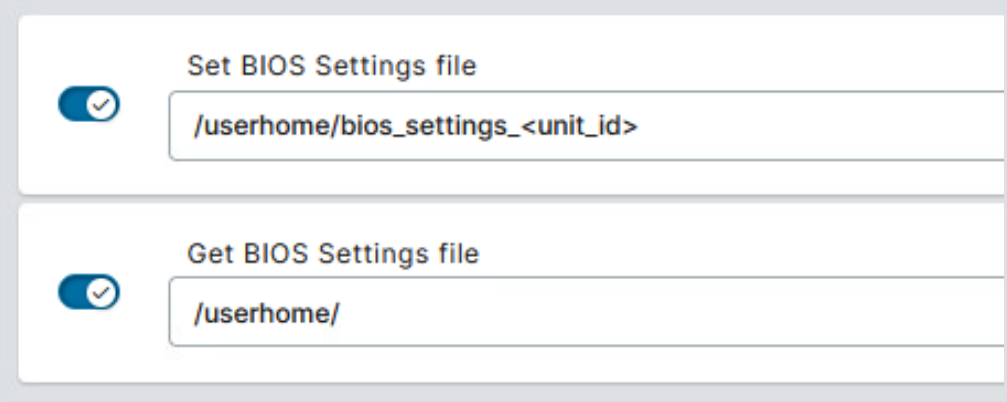
Defining the Paths for Exchanging the BIOS Settings Files

First, we will define a local directory path in which the HP BIOS Tools app will store the current BIOS settings as a file and a local directory path in which the edited settings file will be stored so the app can apply them to the device's BIOS.

→ In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Settings**, make the following edits, and save your settings.

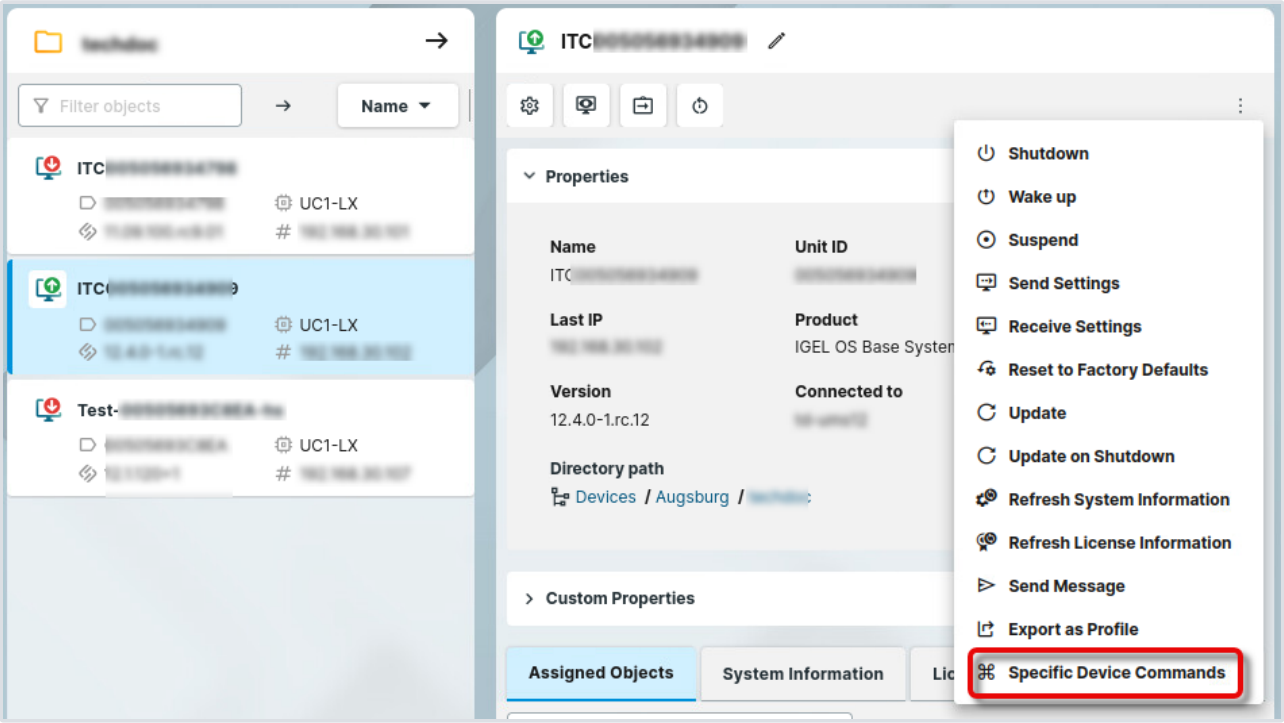
- **Set BIOS settings file**: Path to the file path.

- **Get BIOS settings file**: Path to the file folder with the current BIOS settings file. The filename will be `bios_settings_<unit_id>`

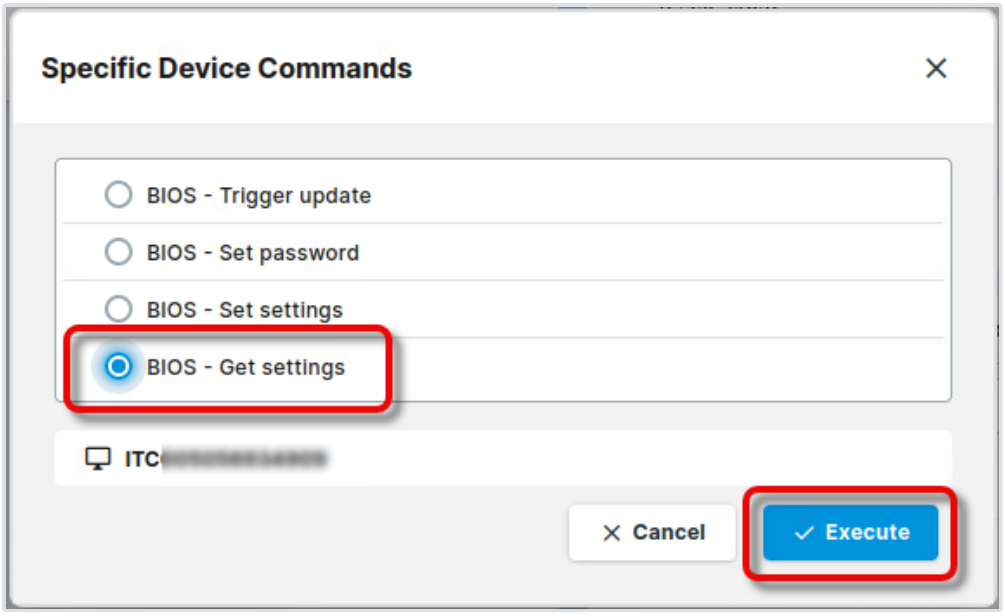


Generating the Current BIOS Settings File

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Commands**.



2. Select **BIOS - Get settings** and click **Execute**.



Transferring and Editing the BIOS Settings File

1. Enable SSH as described in https://kb.igel.com/en/igel-os-base-system/12.6.1/ssh-access-in-igel-os-12 .

2. Use scp from a linux or windows terminal:

```
scp username@remote:/path /localpath
```

- Depending on the SSH access configuration, `username` could be `root`, `ruser`, or `user`.
- `remote` is the IP address of the OS 12 device.
- `/path` it the path to the BIOS settings file on the OS 12 device
- `/localpath` is the path to where the file will be saved locally

3. Download and install the HP BIOS Configuration Utility. For information on the download source and the use of the utility, see https://ftp.ext.hp.com/pub/caps-softpaq/cmit/whitepapers/BIOS_Configuration_Utility_User_Guide.pdf.

4. Edit the configuration file as desired.

⚠ Regarding the configuration file, please note the following:
- It is recommended to use a text editor under Unix/Linux for editing. This ensures that the correct line feeds are used and that the characters are encoded correctly (UTF-8).

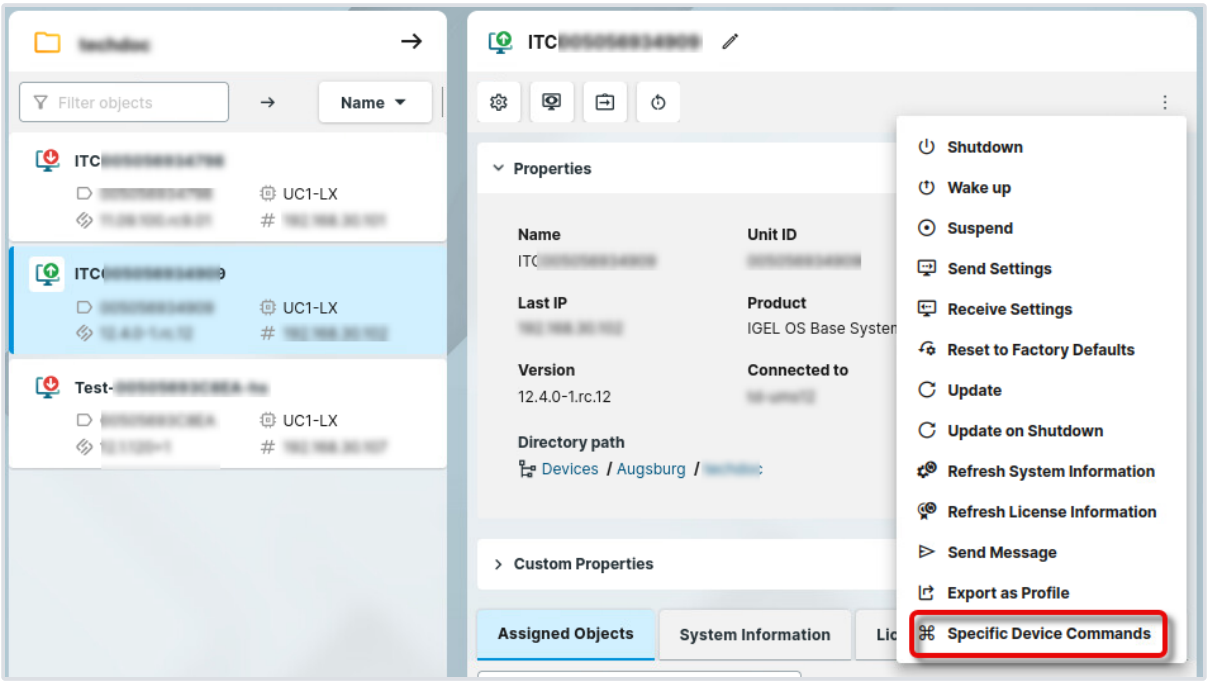
- Make sure that the BIOS settings file is formatted properly and that the REPSET format is respected. For further information, see https://ftp.ext.hp.com/pub/caps-softpaq/cmit/whitepapers/BIOS_Configuration_Utility_User_Guide.pdf

It is sufficient to specify only those BIOS setting you want to change so that your edited file contains snippets instead of all possible settings.

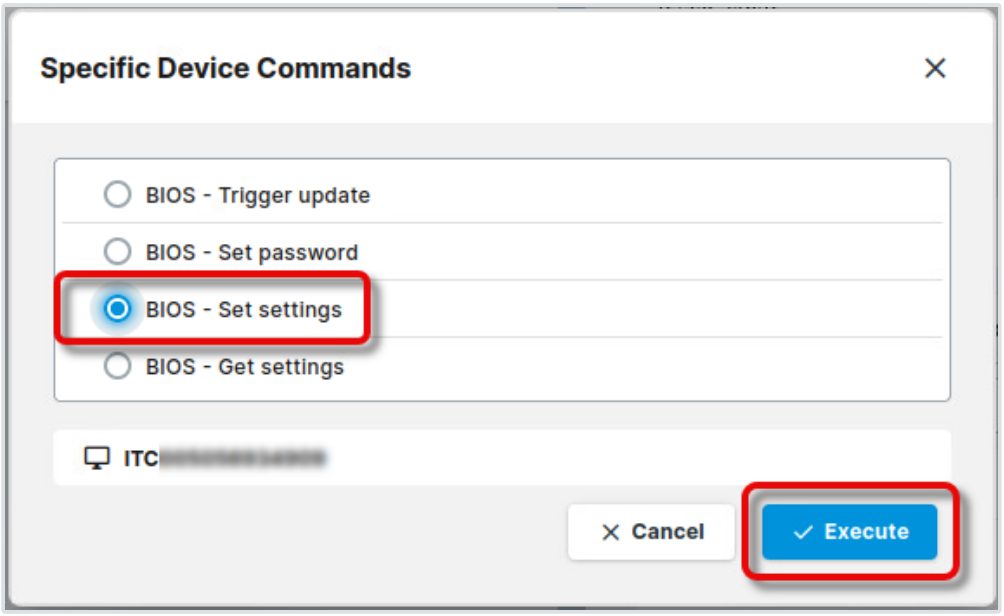
5. Save the settings file. Make the edited file available as described under Setting up the File Source (see page 92).

Deploying the Changed Settings on the Device

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.



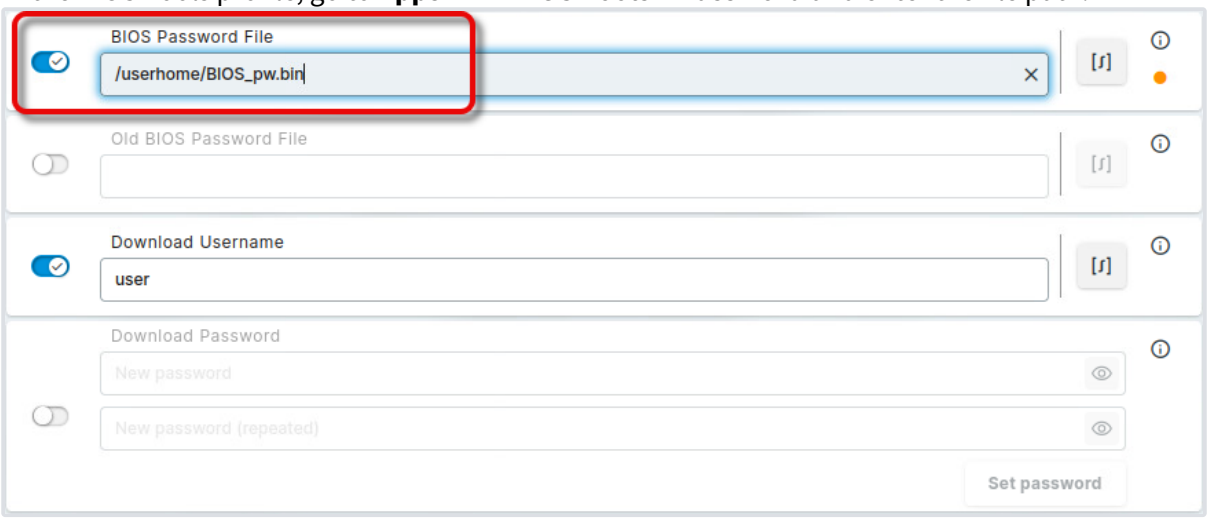
2. Select **BIOS - Set settings** and click **Execute**.



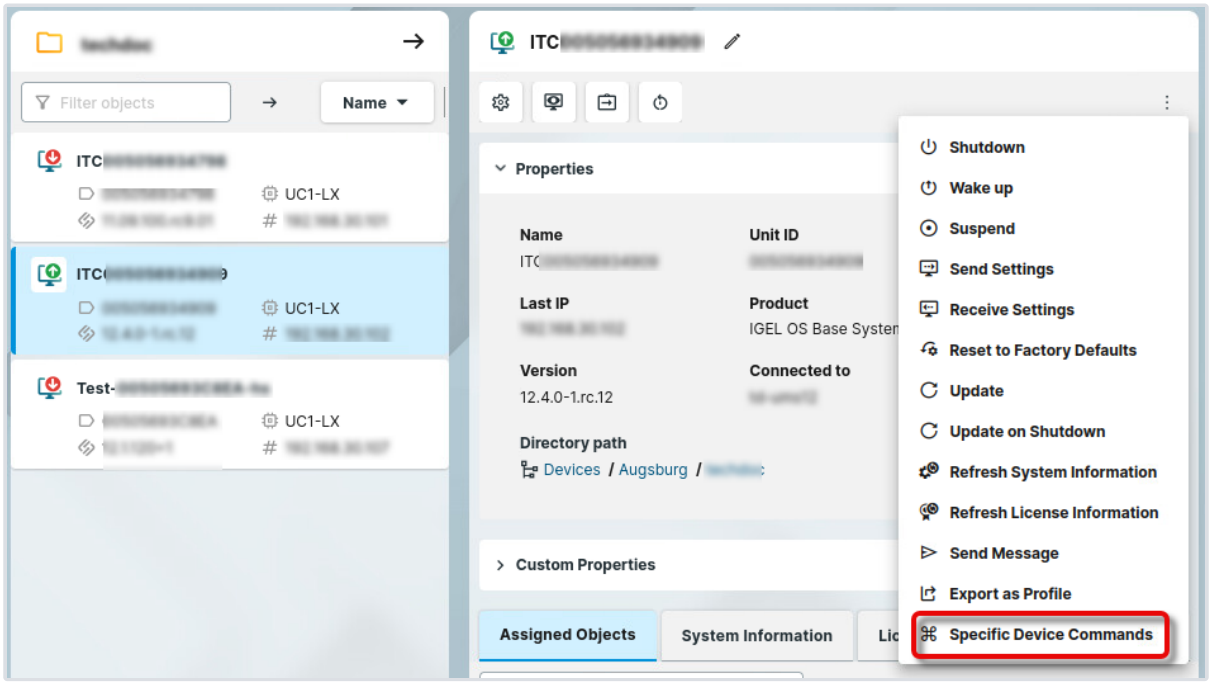
Setting a BIOS Password to Protect Your BIOS

If your BIOS is not protected by a password yet and you want to secure it with a BIOS password, proceed as follows.

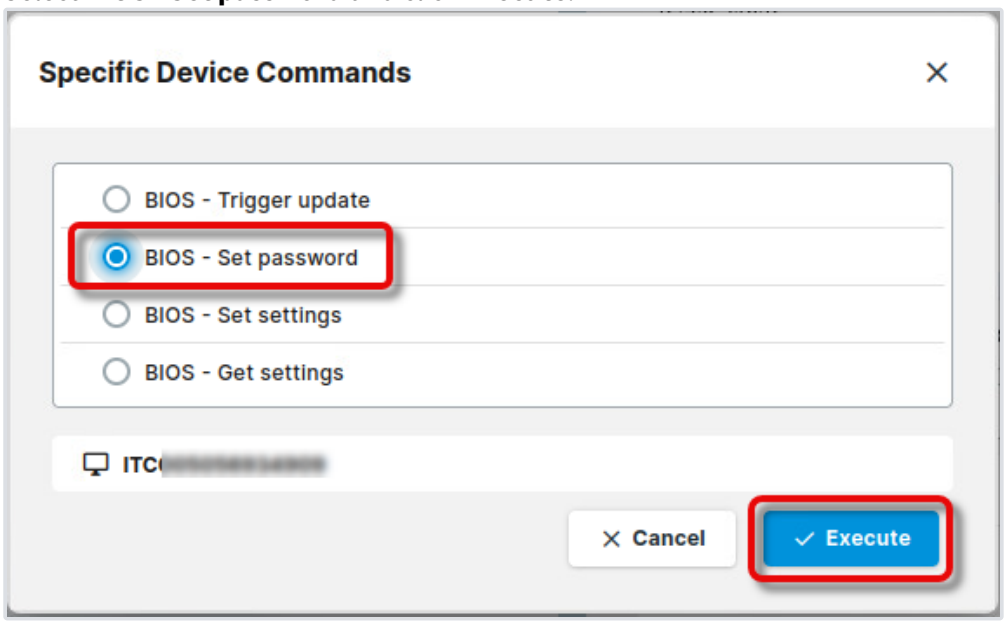
1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.
2. Create a password file with the new password and make it available as described under Setting up the File Source (see page 95).
3. In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Password** and enter the file path.



4. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Commands**.



5. Select **BIOS - Set password** and click **Execute**.



Changing the BIOS Password

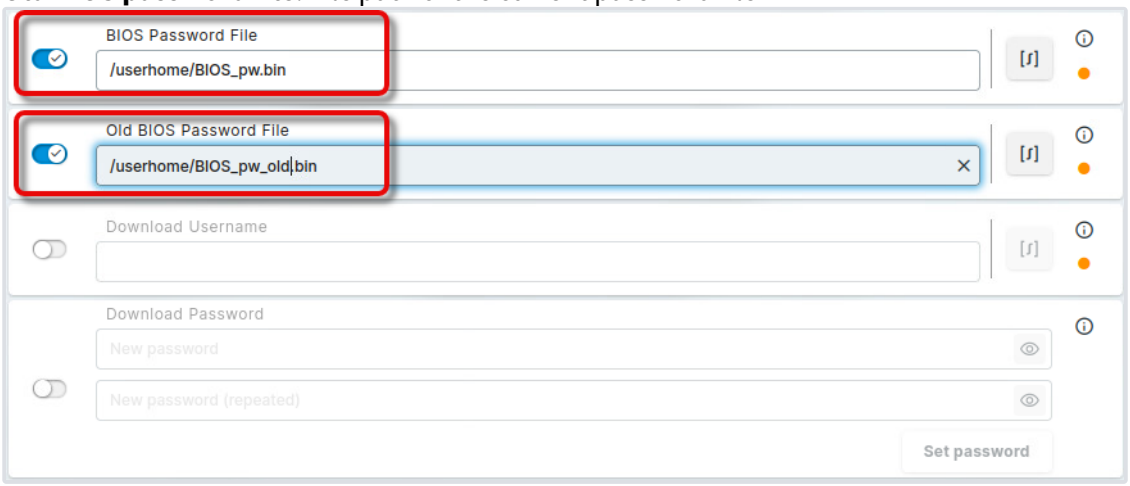
If your devices already have a BIOS password and you want to change it, proceed as follows.

1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

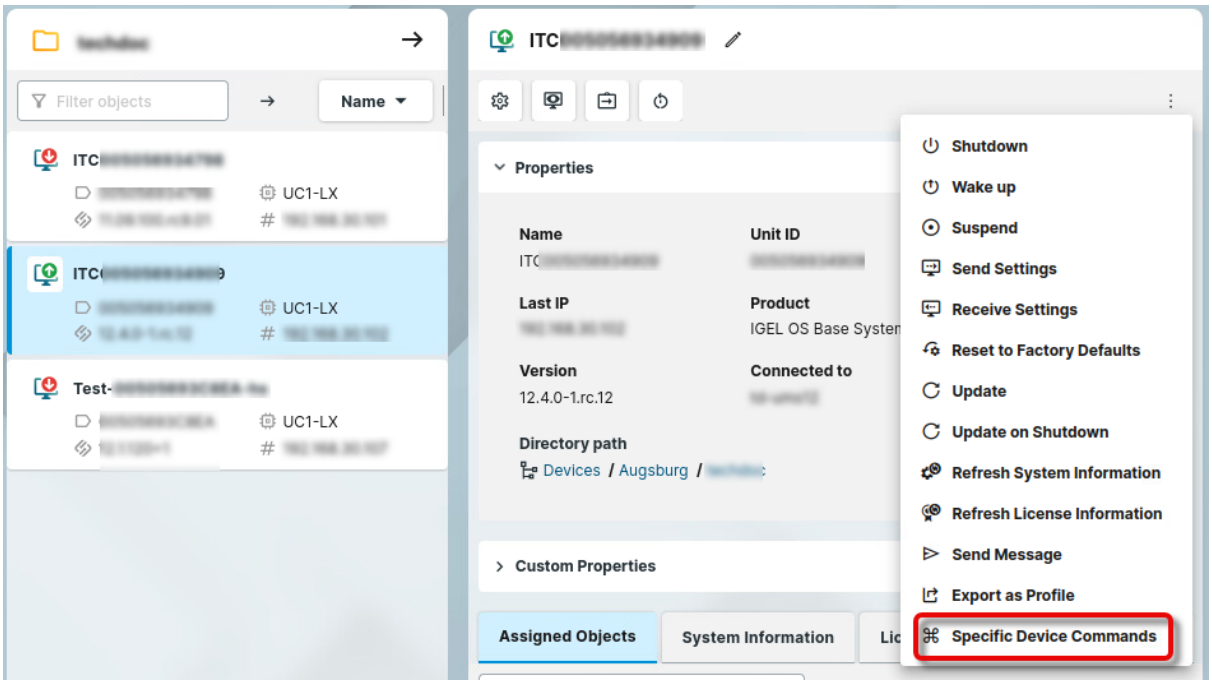
2. Create a password file with the current password and make it available as described under Setting up the File Source (see page 95).

3. Create a password file with the new password and make it available as described under Setting up the File Source (see page 95).

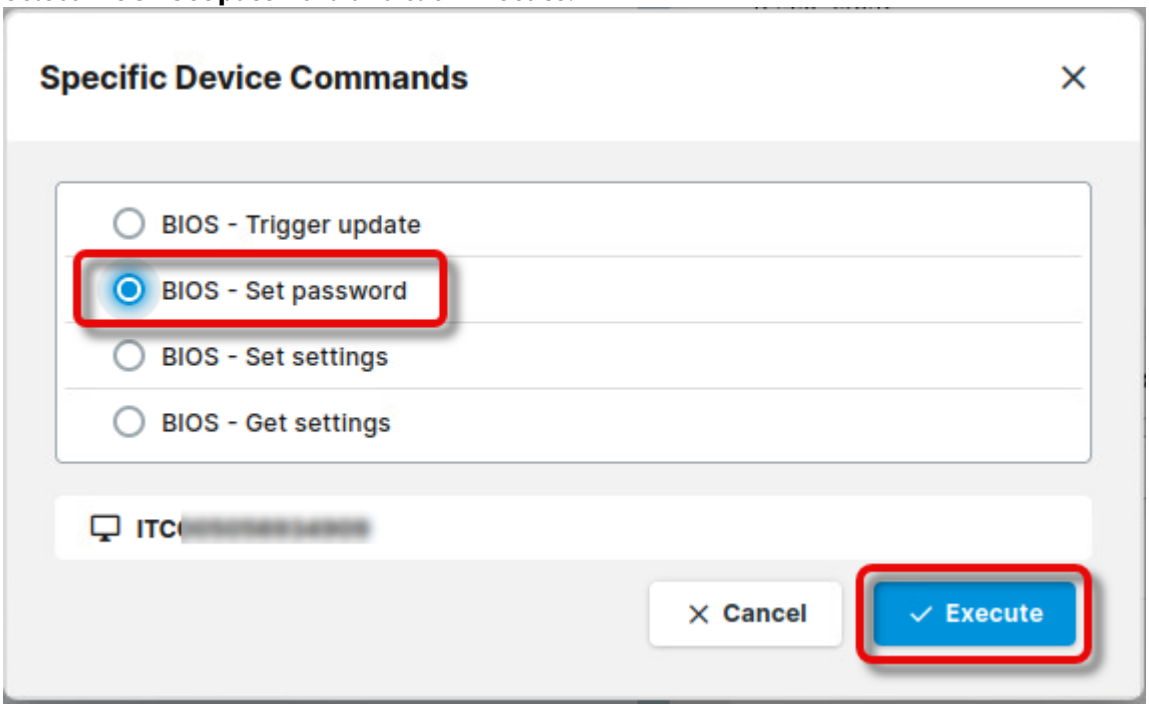
4. In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Password**, make the following edits, and save your settings.
   - **BIOS password file**: File path of the new password file
   - **Old BIOS password file**: File path of the current password file



5. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.



6. Select **BIOS - Set password** and click **Execute**.



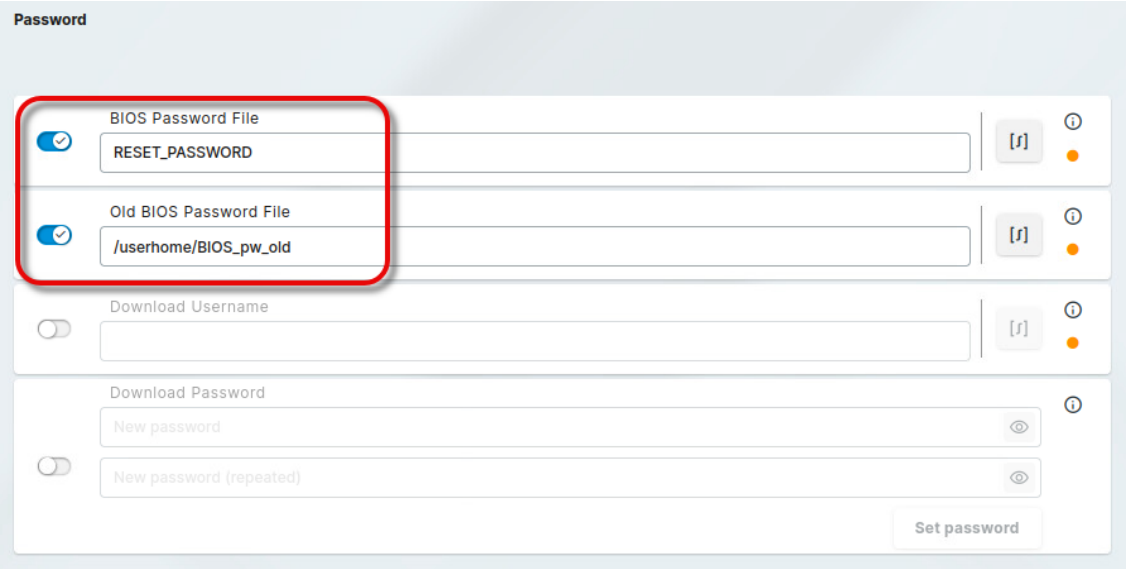
Resetting the BIOS Password (Removing Password Protection)

If your devices have a BIOS password and you want to reset it so that the BIOS will be accessible without a password, proceed as follows.

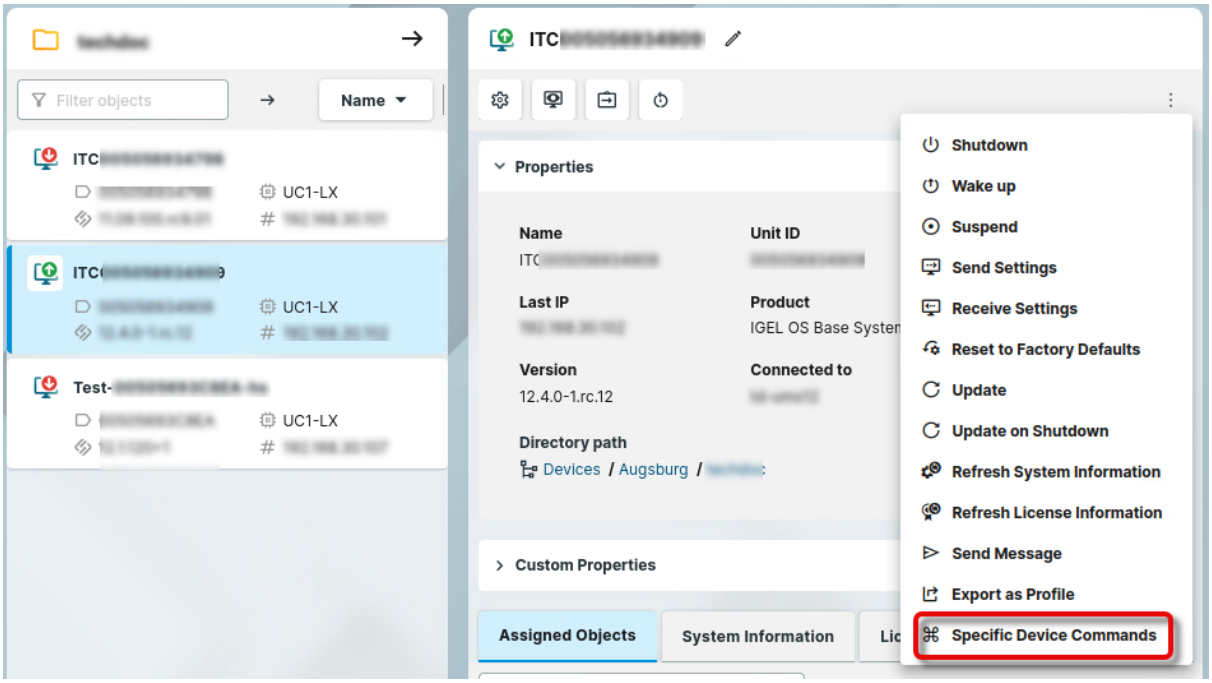
1. On a Windows machine, download the password tool from https://ftp.ext.hp.com/pub/caps-softpaq/cmit/HPQPswd.html and install it.

2. Create a password file with the old password and make it available as described under Setting up the File Source (see page 95).

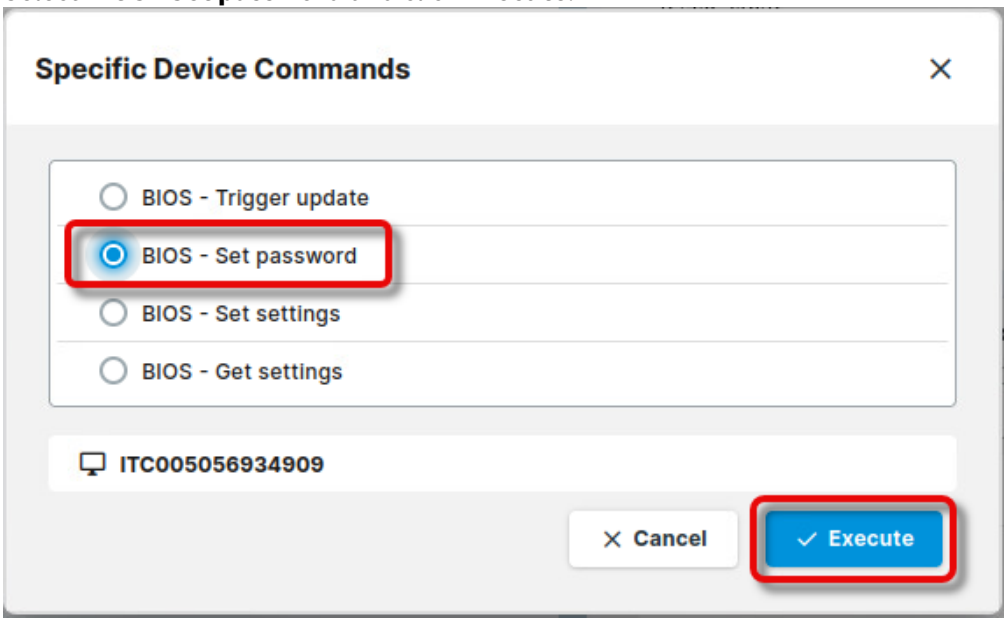
3. In the BIOS Tools profile, go to **Apps > HP BIOS Tools > Password**, make the following edits, and save your settings.
   - **BIOS password file**: Enter `RESET_PASSWORD`
   - **OLD BIOS password file**:



4. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Commands**.



5. Select **BIOS - Set password** and click **Execute**.



Command Line Interface (CLI) for the BIOS Tools

To test the BIOS update on a single device, you can use the command line tool as an alternative to the Specific Device Commands from the UMS.

As a prerequisite, the steps described under Setting up the File Source (see page 95) and the relevant settings in the profile must be completed.

When the command has been executed, a dialog informs you that a reboot is required. You can choose between two options:

- Perform the reboot and update right away
- Postpone the update to the next reboot

Usage

```
callBiosTools [OPTIONS] COMMAND [ARGS]...
```

Options

Option	Description
`--debug / --no-debug`	
`--info / --no-info`	
`--test / --no-test`	
`--help`	Show this message and exit

Commands

Command	Argument	Description
`password`		Set BIOS password
`settings`		Handle BIOS settings
	`-c, --configure`	Configure BIOS settings with a configuration file
	`-g, --get`	Get current BIOS settings
	`--help`	Show this message and exit
`update`		Handle BIOS update
	`-e, --enable`	Enable BIOS update. The update will be triggered after a reboot.
	`-d, --disable`	Disable BIOS update

Command	Argument	Description
	`-s, --show`	Show if BIOS update is enabled or not
	`--help`	Show this message and exit

IGEL Advanced Device Redirection Plugins

The IGEL Advanced Device Redirection (ADR) apps support the integration of endpoint devices with on premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- IGEL Windows 365 (Cloud PC)
- Citrix Workspace App
- Omnissa Horizon Client

IGEL ADR is not yet supported with the IGEL Remote Desktop (RDP) app
Support will be introduced in a future update of both the IGEL ADR app and the corresponding server-side component. As an interim solution, a server license is included with the purchase of IGEL ADR to enable device redirection in RDP sessions using FabulaTech redirection apps.

Requirements

IGEL Advanced Device Redirection Plugins is connecting IGEL Advanced Device Redirection apps with different remote desktop clients. As it is not a standalone application, at least one of the following apps must be installed and configured as well:

- IGEL Advanced Device Redirection Scanner
- IGEL Advanced Device Redirection Sound
- IGEL Advanced Device Redirection USB
- IGEL Advanced Device Redirection Webcam

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License . When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

How to Disable or Enable the Plugins

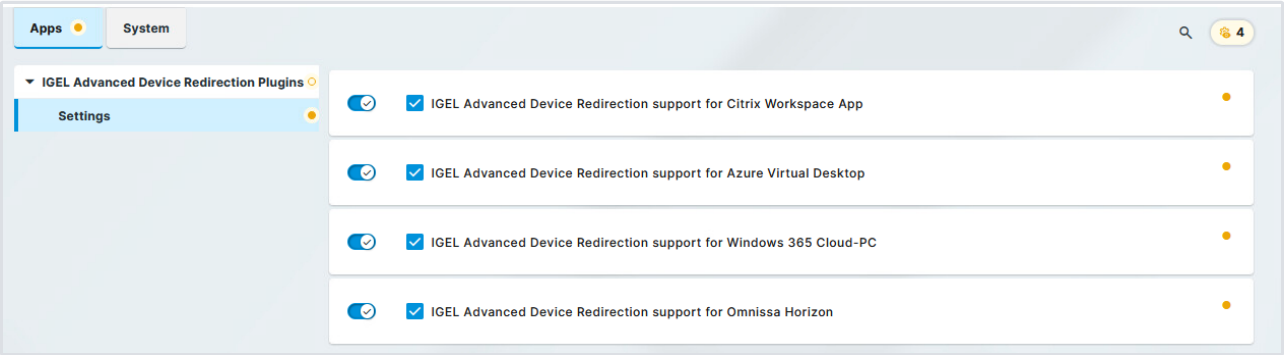
1. Import the IGEL Advanced Device Redirection Plugins app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[31].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[32].

31. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
32. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection Plugins > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



IGEL Advanced Device Redirection support for Citrix Workspace App

- ☑ The IGEL Advanced Device Redirection plugin is enabled in Citrix sessions. (Default)
- ☐ The IGEL Advanced Device Redirection plugin is disabled in Citrix sessions.

IGEL Advanced Device Redirection support for Azure Virtual Desktop

- ☑ The IGEL Advanced Device Redirection plugin is enabled in AVD sessions. (Default)
- ☐ The IGEL Advanced Device Redirection plugin is disabled in AVD sessions.

IGEL Advanced Device Redirection support for Windows 365 Cloud-PC

- ☑ The IGEL Advanced Device Redirection plugin is enabled in Windows 365 Cloud-PC sessions. (Default)
- ☐ The IGEL Advanced Device Redirection plugin is disabled in Windows 365 Cloud-PC sessions.

IGEL Advanced Device Redirection support for Omnissa Horizon

- ☑ The IGEL Advanced Device Redirection plugin is enabled in Omnissa Horizon sessions. (Default)
- ☐ The IGEL Advanced Device Redirection plugin is disabled in Omnissa Horizon sessions.

IGEL Advanced Device Redirection Scanner

The IGEL Advanced Device Redirection (ADR) apps support the integration of endpoint devices with on-premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- IGEL Windows 365 (Cloud PC)
- Citrix Workspace App
- Omnissa Horizon Client
- IGEL Remote Desktop (RDP) App

Starting from Version 1.3.0 BUILD 1.0, IGEL ADR Plugins supports the IGEL RDP app.

Requirements

To use the IGEL Advanced Device Redirection Scanner app, the following app must be installed and configured as well:

- IGEL Advanced Device Redirection Plugins[33]

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License. When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

Server Component Required

To use the IGEL Advanced Device Redirection apps, you need to have a server component in place. You can install the component both on Linux and Windows:

- Linux Server Component - Request the component here.[34]
- Windows Server Component (version 4.0.4) - Download the component here[35].

A benefit of using the IGEL Advanced Device Redirection is that the server component does not need to be licensed. Once the server recognizes the IGEL Advanced Device Redirection license, the full version is activated on the server side.

33. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-plugins
34. https://www.fabulatech.com/usb-for-remote-desktop-linux-server-request.html
35. https://igel-technology.sharefile.com/public/share/web-s52239ee5676545be961c5cfdef9d50ea

Possible Conflicts

The IGEL Advanced Device Redirection Scanner application conflicts with the FabulaTech Scanner for Remote Desktop application. You cannot use both applications at the same time.

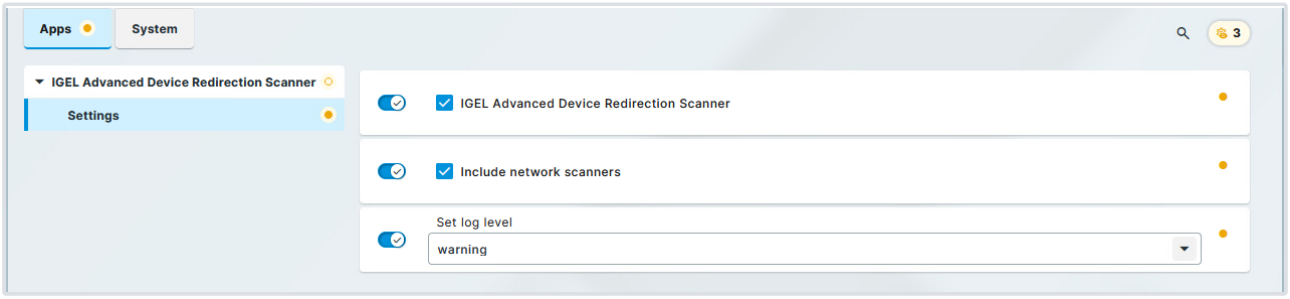
How to Configure Scanner Redirection

1. Import the IGEL Advanced Device Redirection Scanner app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[36].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[37].

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection Scanner > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



IGEL Advanced Device Redirection Scanner

IGEL Advanced Device Redirection Scanner is enabled for the sessions that are enabled in the IGEL Advanced Device Redirection Plugins app. (Default)

Include network scanners

Scanners that are made available to the device through the network are also redirected. (Default)

Set log level

Defines the degree of detail written into the log file.

36. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
37. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

IGEL Advanced Device Redirection Serialport

The IGEL Advanced Device Redirection apps support the integration of endpoint devices with on-premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- Citrix Workspace App
- Omnissa Horizon Client
- IGEL Remote Desktop (RDP) App

Starting from Version 1.3.0 BUILD 1.0, IGEL ADR Plugins supports the IGEL RDP app.
IGEL ADR Serialport is not supported with IGEL Windows 365 (Cloud PC).

Requirements

To use the IGEL Advanced Device Redirection Serialport app, the following app must be installed and configured as well:

- IGEL Advanced Device Redirection Plugins[38]

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License. When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

Server Component Required

To use the IGEL Advanced Device Redirection apps, you need to have a server component in place. You can install the component both on Linux and Windows:

- Linux Server Component - Request the component here.[39]
- Windows Server Component (version 4.0.4) - Download the component here[40].

A benefit of using the IGEL Advanced Device Redirection is that the server component does not need to be licensed. Once the server recognizes the IGEL Advanced Device Redirection license, the full version is activated on the server side.

38. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-plugins
39. https://www.fabulatech.com/usb-for-remote-desktop-linux-server-request.html
40. https://igel-technology.sharefile.com/share/view/s131eb3c73dbc4c27bb1bb2cdae495ae7

Possible Conflicts

The IGEL Advanced Device Redirection Serialport application conflicts with the FabulaTech Serial Port for Remote Desktop application. You cannot use both applications at the same time.

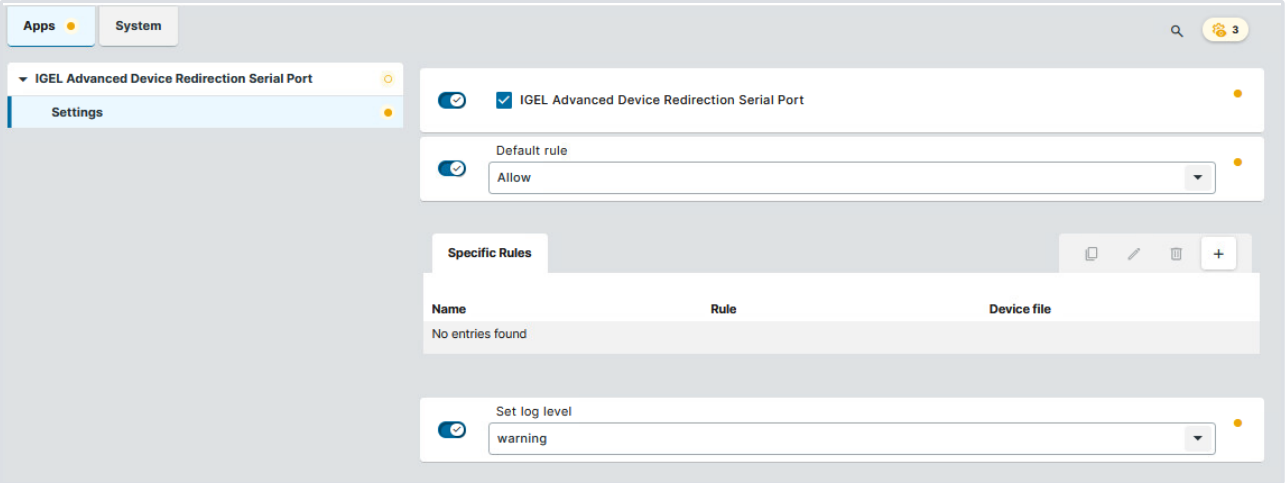
How to Configure Serialport Redirection

1. Import the IGEL Advanced Device Redirection Serialport app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[41].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[42].

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection Serial Port > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



IGEL Advanced Device Redirection Serial Port

IGEL Advanced Device Redirection Serial Port is enabled for the sessions that are enabled in the IGEL Advanced Device Redirection Plugins app. (Default)

Default rule

41. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
42. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

This rule will apply if no special rule was configured.

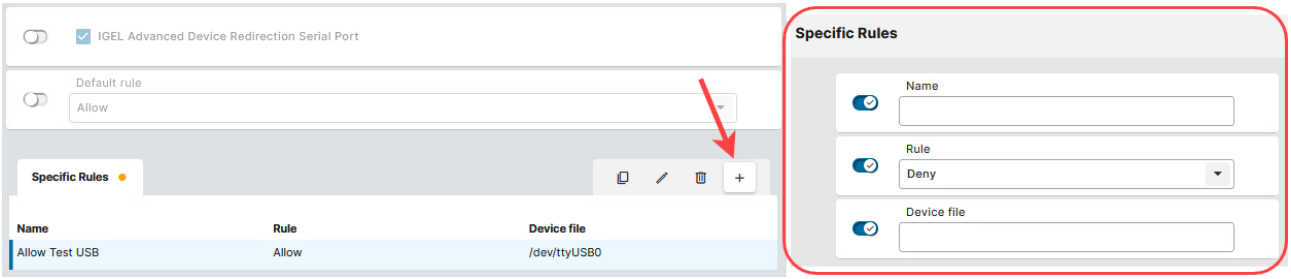
- **Deny**: Devices are only redirected if they have **Allow** rules configured under **Specific Rules**. (Default)
- **Allow**: Devices are always redirected unless they have **Deny** rules configured under **Specific Rules**.

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required serial ports.

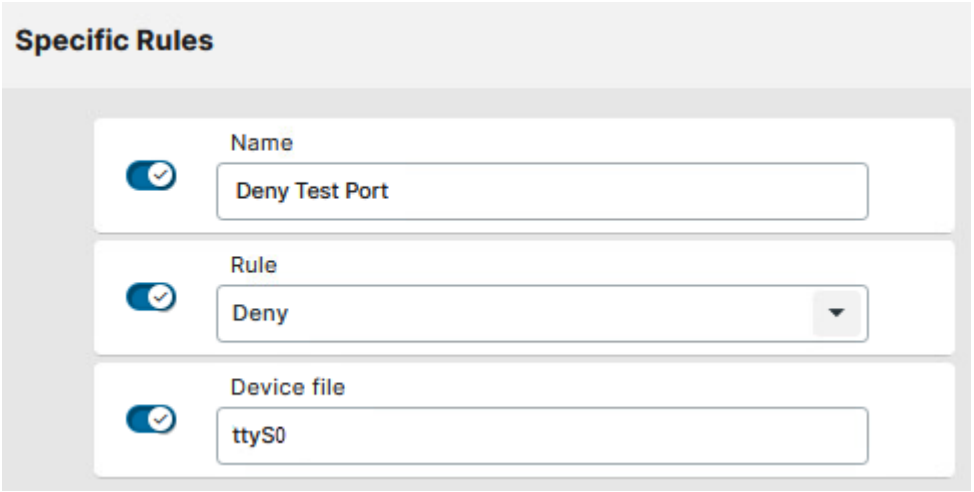
Specific Rules

Specific rules apply to specific devices only. Specific rules override **Default rule** configurations. This way, you can generally deny redirection and allow only for specific devices. You can also generally allow redirection but deny for specific devices.

- Click to bring up a dialog to configure a new rule.



Click for Specific Rules configuration options ...



Name

The name of the rule.

Rule

- **Deny**: Devices configured under **Device file** are never redirected. They are specifically denied, regardless of the global configuration under **Default rule**. (Default)
- **Allow**: Devices configured under **Device file** are always redirected. They are specifically allowed, regardless of the global configuration under **Default rule**.

Device file

A device file is the representation of a local serial port. Provide the device file without path.

For example, use `ttyUSB0` or `ttyS0` . Do not use `/dev/ttyUSB0` or `/dev/ttyS0` .

To manage the rules, you can:

- Click to edit the selected entry.
- Click to remove the selected entry.
- Click to copy the selected entry.

Set log level

Defines the degree of detail written into the log file.

Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

IGEL Advanced Device Redirection Sound

The IGEL Advanced Device Redirection apps support the integration of endpoint devices with on-premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- IGEL Windows 365 (Cloud PC)
- Citrix Workspace App
- Omnissa Horizon Client
- IGEL Remote Desktop (RDP) App

Starting from Version 1.3.0 BUILD 1.0, IGEL Advanced Device Redirection Plugins supports the IGEL Remote Desktop (RDP) app.

Requirements

To use the IGEL Advanced Device Redirection Sound app, the following app must be installed and configured as well:

- IGEL Advanced Device Redirection Plugins[43]

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License. When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

Server Component Required

To use the IGEL Advanced Device Redirection apps, you need to have a server component in place. You can install the component both on Linux and Windows:

- Linux Server Component - Request the component here.[44]
- Windows Server Component (version 4.2.12) - Download the component here[45].

A benefit of using the IGEL Advanced Device Redirection is that the server component does not need to be licensed. Once the server recognizes the IGEL Advanced Device Redirection license, the full version is activated on the server side.

43. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-plugins
44. https://www.fabulatech.com/usb-for-remote-desktop-linux-server-request.html
45. https://igel-technology.sharefile.com/public/share/web-s77f64c5eb9ce49ba84594fd7f7499f7a

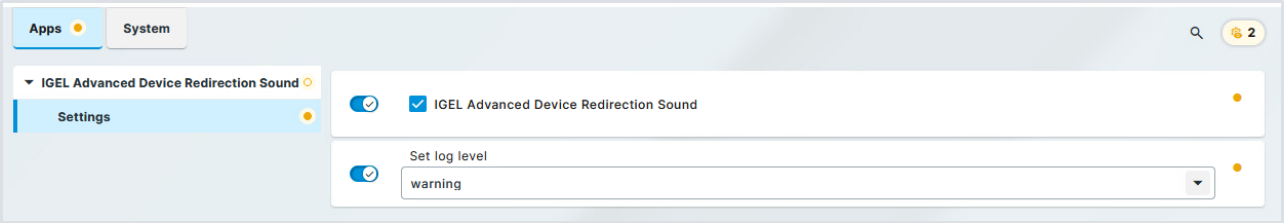
How to Configure the Sound Redirection

1. Import the IGEL Advanced Device Redirection Sound app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[46].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[47].

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection Sound > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



IGEL Advanced Device Redirection Sound

IGEL Advanced Device Redirection Sound is enabled for the sessions that are enabled in the IGEL Advanced Device Redirection Plugins app. (Default)

Set log level

Defines the degree of detail written into the log file.

Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

46. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
47. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

IGEL Advanced Device Redirection USB

The IGEL Advanced Device Redirection apps support the integration of endpoint devices with on-premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- IGEL Windows 365 (Cloud PC)
- Citrix Workspace App
- Omnissa Horizon Client
- IGEL Remote Desktop (RDP) App

Starting from Version 1.3.0 BUILD 1.0, IGEL Advanced Device Redirection Plugins supports the IGEL Remote Desktop (RDP) app.

Requirements

To use the IGEL Advanced Device Redirection USB app, the following app must be installed and configured as well:

- IGEL Advanced Device Redirection Plugins[48]

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License. When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

Server Component Required

To use the IGEL Advanced Device Redirection apps, you need to have a server component in place. You can install the component both on Linux and Windows:

- Linux Server Component - Request the component here.[49]
- Windows Server Component (version 6.3.10) - Download the component here[50].

A benefit of using the IGEL Advanced Device Redirection is that the server component does not need to be licensed. Once the server recognizes the IGEL Advanced Device Redirection license, the full version is activated on the server side.

48. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-plugins
49. https://www.fabulatech.com/usb-for-remote-desktop-linux-server-request.html
50. https://igel-technology.sharefile.com/share/view/s1ca6918acebb49618a6384bd86014070

Possible Conflicts

The IGEL Advanced Device Redirection USB application conflicts with the FabulaTech USB for Remote Desktop application. You cannot use both applications at the same time.

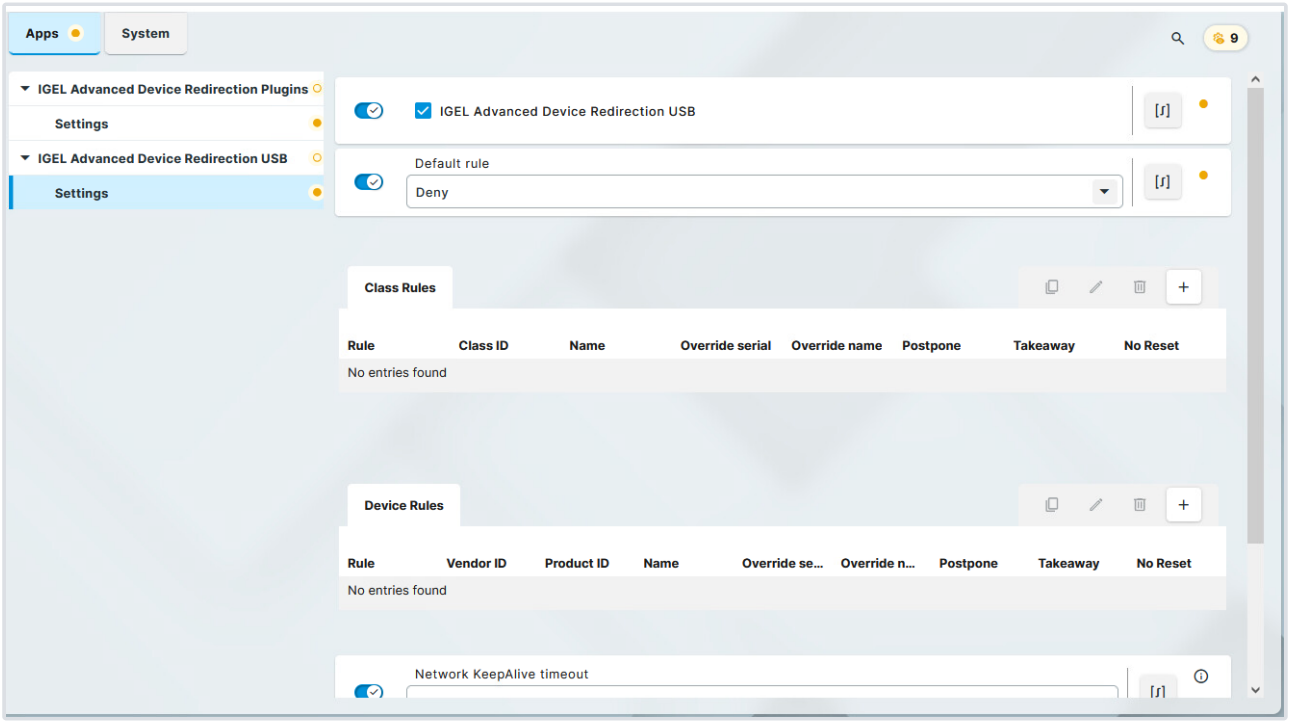
How to Configure the USB Redirection

1. Import the IGEL Advanced Device Redirection USB app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[51].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[52].

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection USB > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



51. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
52. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

IGEL Advanced Device Redirection USB

- ☑ IGEL Advanced Device Redirection USB is enabled for the sessions that are enabled in the IGEL Advanced Device Redirection Plugins app. (Default)
- ☐ IGEL Advanced Device Redirection USB redirection is disabled.

Default rule

This rule will apply if no special rule was configured for a class or a device.

- **Deny**: Devices are only redirected if they have **Allow** rules configured under **Class Rules** or **Device Rules**. (Default)
- **Allow**: Devices are always redirected unless they have **Deny** rules configured under **Class Rules** or **Device Rules**.

> To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Class Rules

Class rules apply to USB device classes and sub-classes.

To manage rules, proceed as follows:

- Click + to bring up the **Class Rules** dialog, where you can define a new rule with the options described under Class Rules (see page 129).
- Click to copy the selected entry.
- Click to edit the selected entry.
- Click to remove the selected entry.

Device Rules

Device rules are based on the vendor ID and product ID of USB devices.

To manage rules, proceed as follows:

- Click + to bring up the **Device Rules** dialog, where you can define a new rule with the options described under Device Rules (see page 133).
- Click to copy the selected entry.
- Click to edit the selected entry.
- Click to remove the selected entry.

Network KeepAlive timeout

Interval in seconds between keep-alive messages sent to the server port to prevent the client-server link from being broken.

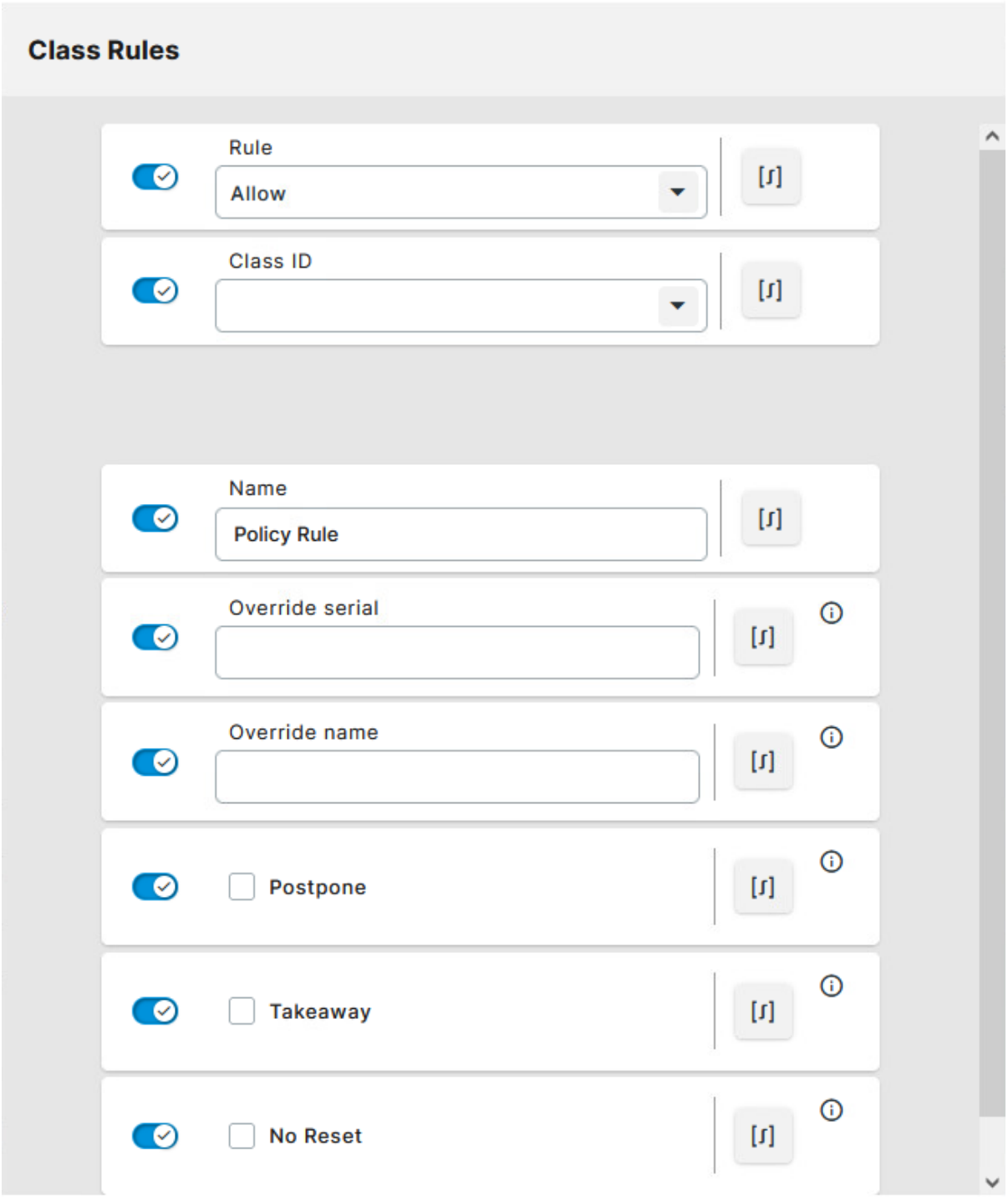
Set log level

Defines the degree of detail written into the log file.

Possible options:

- **Debug**
- **Info**
- **Warning** (Default)
- **Error**
- **None**

Class Rules



Rule

- **Allow**: Devices that have the properties defined here are redirected by the IGEL Advanced Device Redirection USB. (Default)

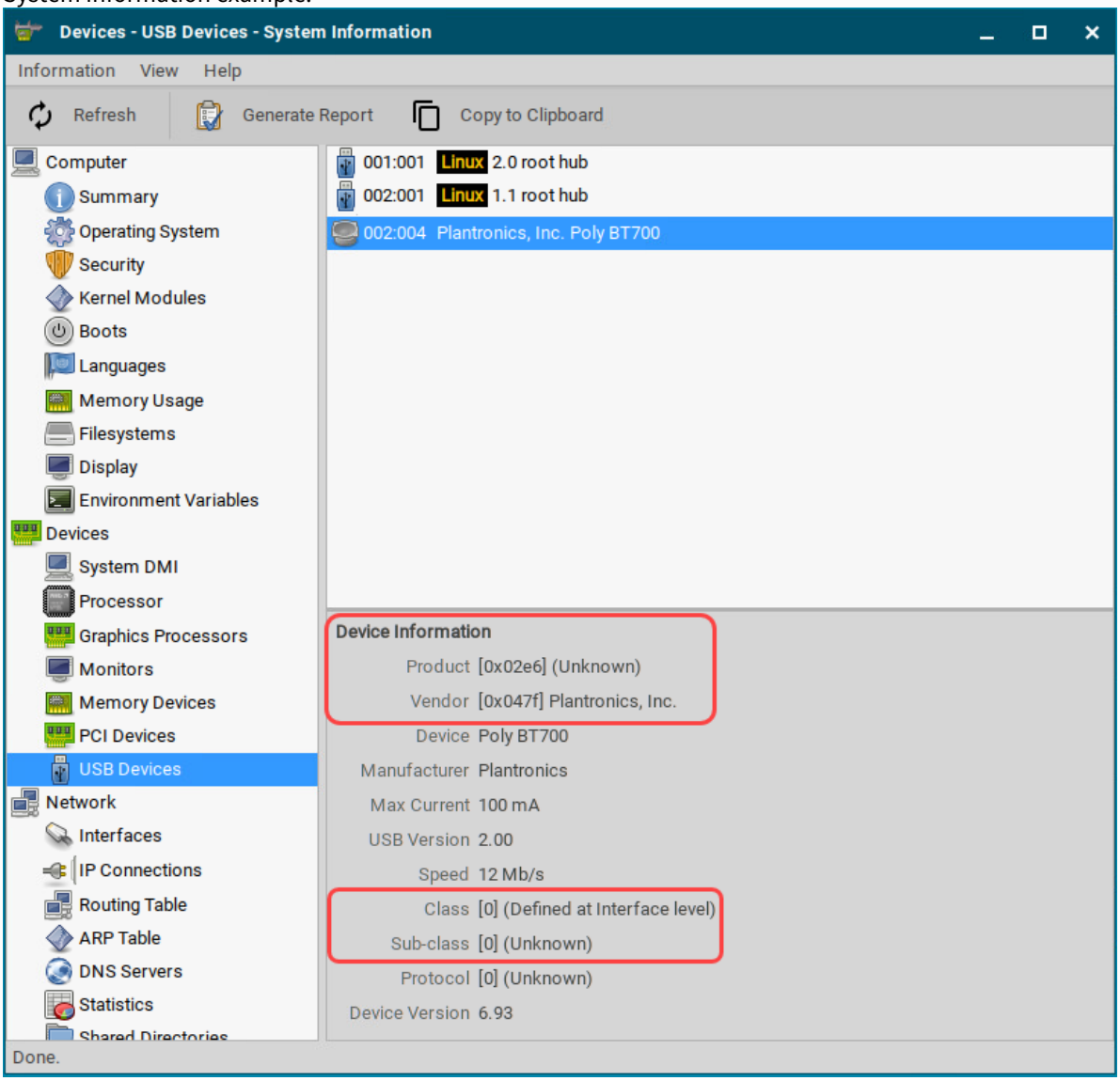
- **Deny**: Devices that have the properties defined here are not redirected.

Class ID

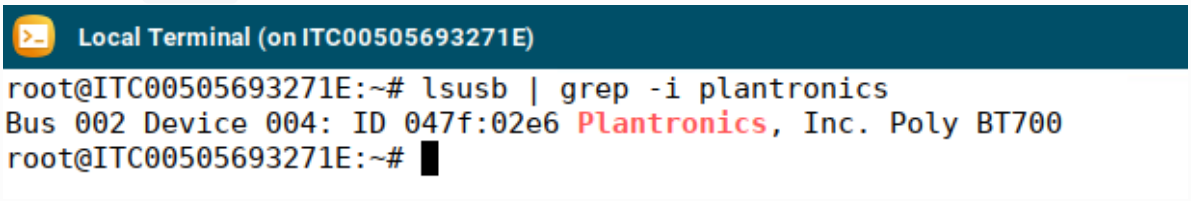
Determines the device class

Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool.
System Information example:



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



Subclass ID

Subclass of the device class

Name

Free text entry

Override serial

Serial number that will appear in the session

Override name

Device name that will appear in the session

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts.
- ☐ The USB device is no longer shown immediately after the system is booted. (Default)

ℹ This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

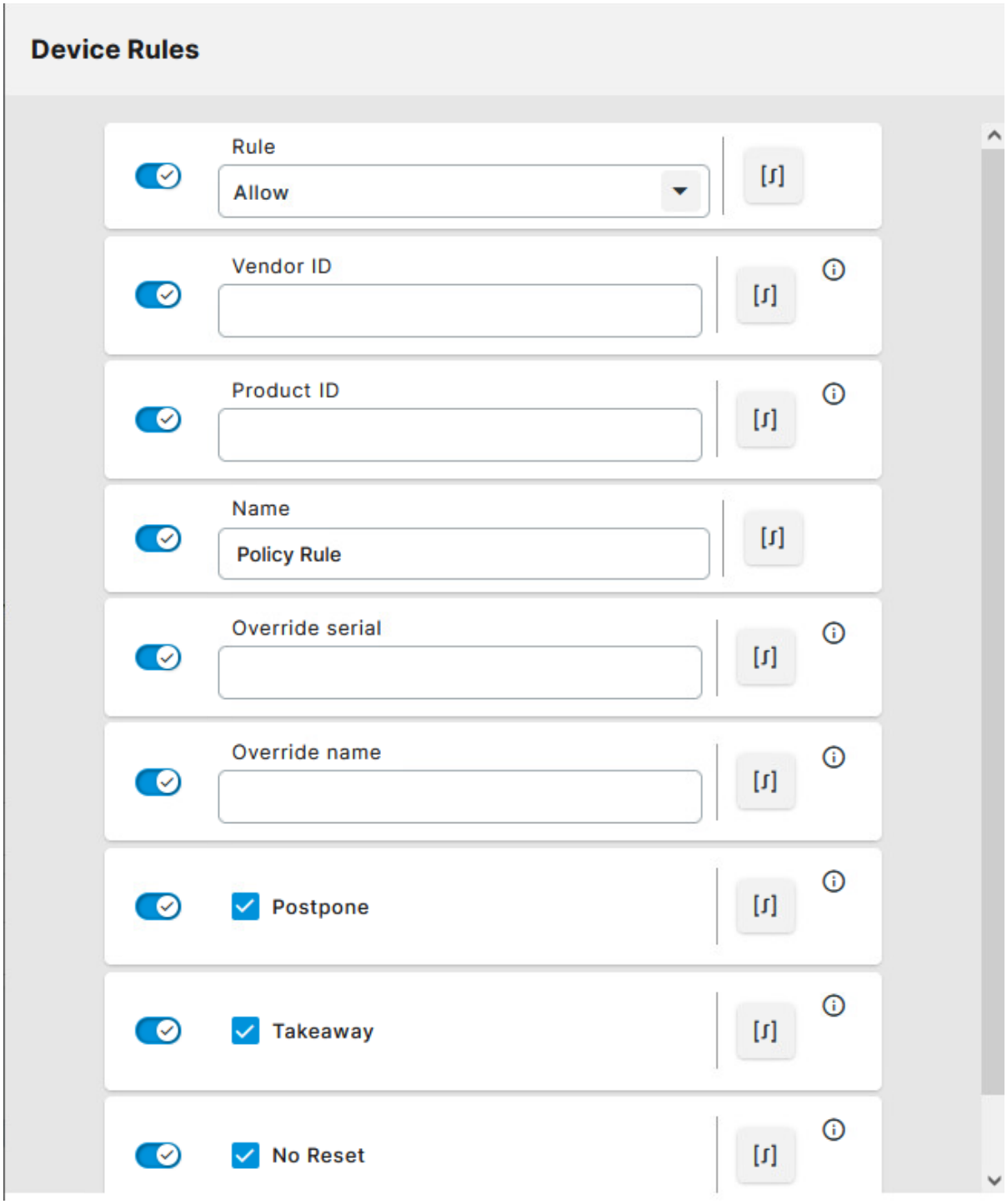
- ☑ The USB device may be removed from the system (endpoint device).
- ☐ The USB device may not be removed. (Default)

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated.

- [ ] The device will be reset after the connection with the session has been terminated. (Default)

Device Rules



Rule

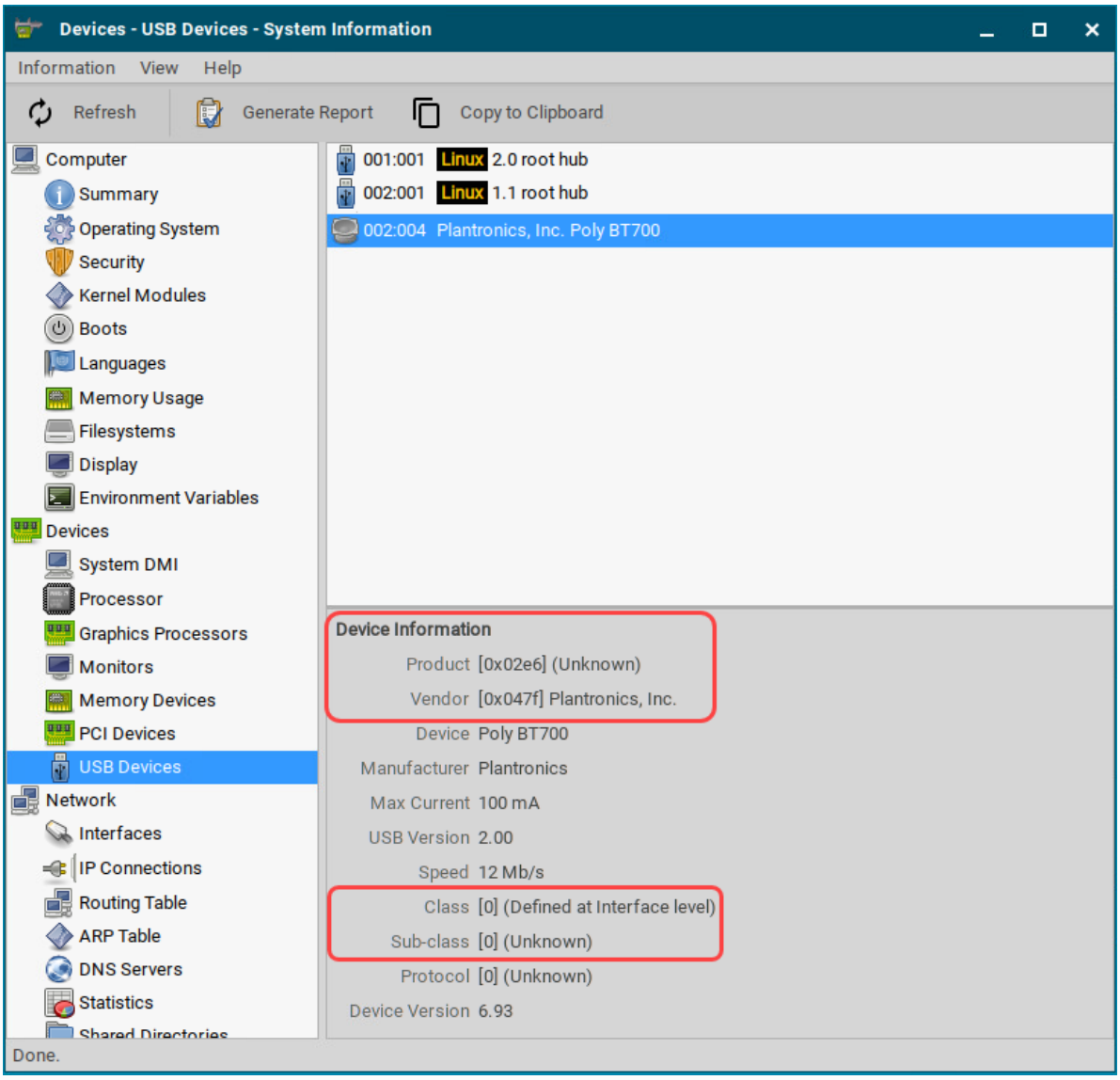
- **Allow**: Devices that have the properties defined here are redirected by the IGEL Advanced Device Redirection USB. (Default)
- **Deny**: Devices that have the properties defined here are not redirected.

Vendor ID

Hexadecimal manufacturer number

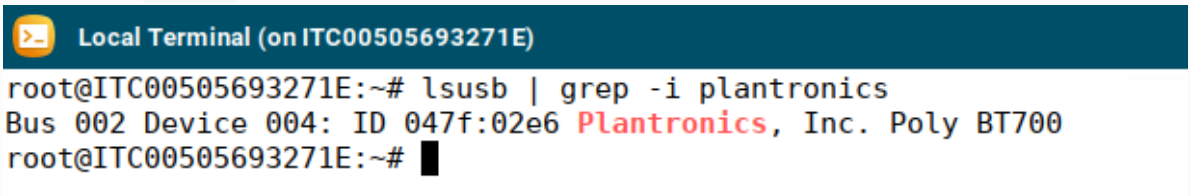
Getting USB Device Information

To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool.
System Information example:



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

Example for `lsusb`:



Product ID

Hexadecimal device number

Name

Free text entry

Override serial

Serial number that will appear in the session

Override name

Device name that will appear in the session

Postpone

- ☑ The USB device is only removed from the system (endpoint device) when the session starts. (Default)
- ☐ The USB device is no longer shown immediately after the system is booted.

> This setting is only effective if the **Takeaway** parameter is enabled.

Takeaway

- ☑ The USB device may be removed from the system (endpoint device). (Default)
- ☐ The USB device may not be removed.

No Reset

- ☑ The device will not be automatically reset after the connection with the session has been terminated. (Default)
- ☐ The device will be reset after the connection with the session has been terminated.

IGEL Advanced Device Redirection Webcam

The IGEL Advanced Device Redirection apps support the integration of endpoint devices with on-premises or cloud-hosted desktops in virtual workplace setups. You can use the app in configurations with:

- IGEL AVD (Azure Virtual Desktop)
- IGEL Windows 365 (Cloud PC)
- Citrix Workspace App
- Omnissa Horizon Client
- IGEL Remote Desktop (RDP) App

Starting from Version 1.3.0 BUILD 1.0, IGEL ADR Plugins supports the IGEL RDP app.

Requirements

To use the IGEL Advanced Device Redirection Webcam app, the following app must be installed and configured as well:

- IGEL Advanced Device Redirection Plugins[53]

License Required

To use the IGEL Advanced Device Redirection apps, you need to have an IGEL Advanced Device Redirection License applied to the OS 12 device. For details, see IGEL Advanced Device Redirection Add-On License. When IGEL Advanced Device Redirection apps are installed without the license, a license warning message is shown on the device.

Server Component Required

To use the IGEL Advanced Device Redirection apps, you need to have a server component in place. You can install the component both on Linux and Windows:

- Linux Server Component - Request the component here.[54]
- Windows Server Component (version 3.2) - Download the component here[55].

A benefit of using the IGEL Advanced Device Redirection is that the server component does not need to be licensed. Once the server recognizes the IGEL Advanced Device Redirection license, the full version is activated on the server side.

53. https://kb.igel.com/en/igel-apps/current/igel-advanced-device-redirection-plugins
54. https://www.fabulatech.com/usb-for-remote-desktop-linux-server-request.html
55. https://igel-technology.sharefile.com/public/share/web-sf925a586a6714a6a9a9d04f2ebb5c507

Possible Conflicts

The IGEL Advanced Device Redirection Webcam application conflicts with the FabulaTech Webcam for Remote Desktop application. You cannot use both applications at the same time.

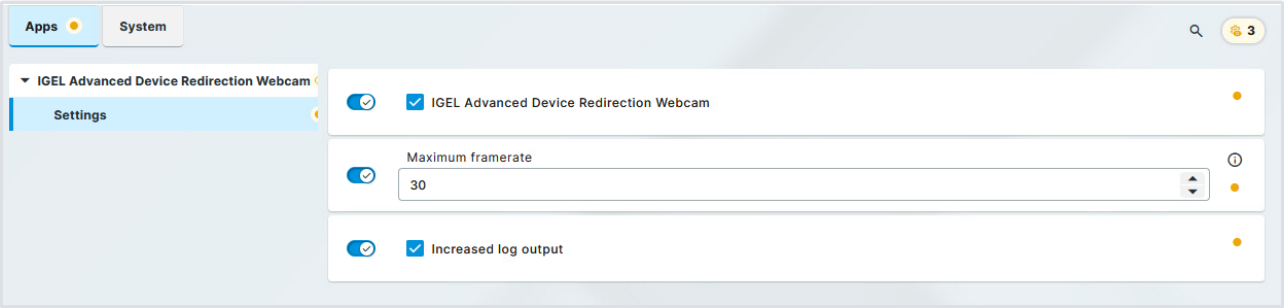
How to Configure the Webcam Redirection

1. Import the IGEL Advanced Device Redirection Webcam app to the IGEL UMS Web App. For details, see How to Import IGEL OS Apps from the IGEL App Portal[56].

2. Create a profile for the app in the IGEL UMS Web App. For details on profile configuration, see Create an OS 12 Profile via Apps[57].

3. In the profile configurator, go to **Apps > IGEL Advanced Device Redirection Webcam > Settings**.

4. Change the settings as required and assign the profile and the app to the IGEL OS 12 devices according to your app distribution workflow.



IGEL Advanced Device Redirection Webcam

IGEL Advanced Device Redirection Webcam is enabled for the sessions that are enabled in the IGEL Advanced Device Redirection Plugins app. (Default)

Maximum framerate

The maximum framerate can be defined on a 1-30 scale. (Default: 30)

Increased log output

56. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
57. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-#id-(12.07.110-en)HowtoCreateandAssignProfilesintheIGELUMSWebApp-Option2:CreateanOS12ProfileviaApps

- [x] The information written into the log file is increased. (Default)
- [ ] The information written into the log file is set to minimal.

IGEL Managed Hypervisor



- How To Create, Distribute, and Manage Virtual Machines with the IGEL Managed Hypervisor (IMH) (see page 141)
- Reconfiguring IGEL Managed Hypervisor (see page 175)

How To Create, Distribute, and Manage Virtual Machines with the IGEL Managed Hypervisor (IMH)

Synopsis

The workflow from setup to operation can be divided into four steps:

1. Create a golden virtual machine image on an IGEL OS 12 machine dedicated to this task (image creation machine)
2. Capture the golden image and upload it to a WebDAV repository
3. Configure the IGEL OS 12 endpoint devices on which the virtual machines will run
4. Remotely manage and configure the virtual machines on the target machines via the UMS Web App

Prerequisites

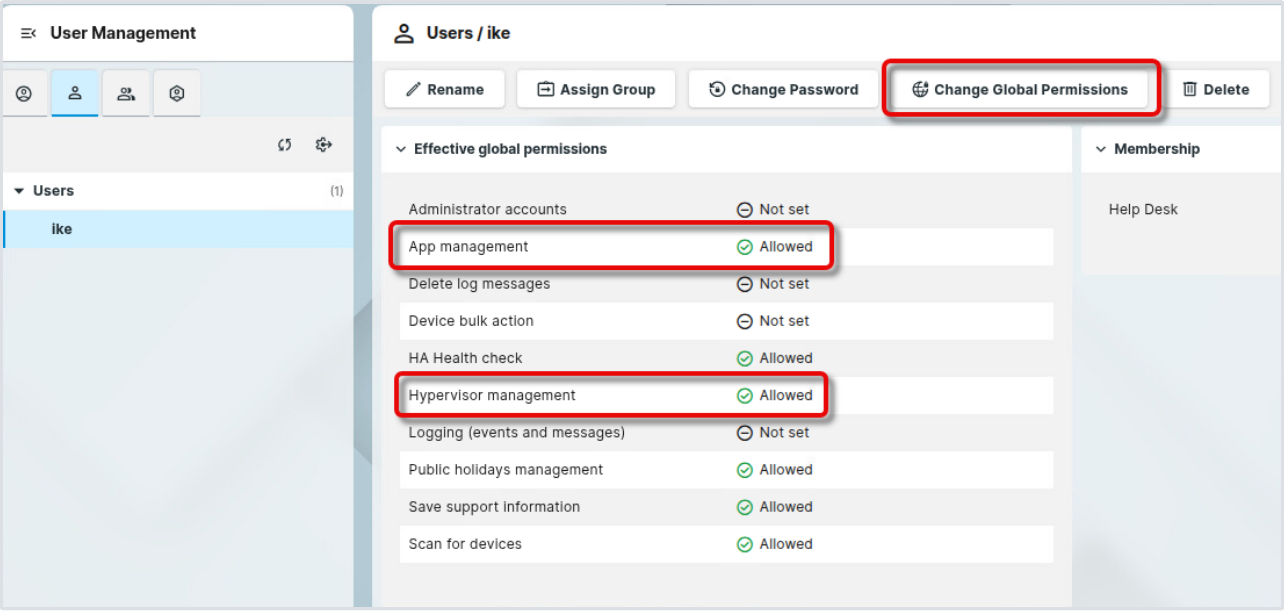
Hardware

- CPU
  - 64-bit capable
  - Dual Core or more
  - 1.5 GHz or more
  - CPU must be virtualization-enabled (Intel VT-x or AMD-V)
- RAM: 8 GB minimum, 16 GB recommended
- Storage
  - 128 GB or more; for virtual machines that run MS Windows 10 or MS Windows 11, the storage requirements may be higher
  - SSDs are strongly recommended

Environment / Infrastructure

UMS

- Your UMS version is 12.08.100 or higher
- Your UMS user has the following permissions (**User Management** area in the UMS Web App):
  - **App management**
  - **Hypervisor management**



- The image creation machine and all target machines are registered in the UMS
- The app IGEL Managed Hypervisor 1.0.0 BUILD 1.0 is registered in the UMS

ISO Source

- The image from which you want to create the Golden Image is available

WebDAV server

- Your WebDAV server is set to use basic authentication
- HTTPS should be used
- Two users are configured:
  - 1 user with read permissions
  - 1 user with write permissions
- The following servers can be used:
  - Apache
  - Nginx
  - Microsoft IIS; please note the following: Use the IIS manager to add the MIME type `application/x-lz4` as described here: Adding Static Content MIME Mappings[58]
  - If you want to roll out the VMs on about 15 or fewer devices, the built-in WebDAV server of the UMS might be sufficient.

58. https://learn.microsoft.com/en-us/iis/configuration/system.webserver/staticcontent/mimemap

IGEL OS Base System

- IGEL OS Base System 12.7.1 PR 1 or higher is installed on the image creation machine and all target machines

Licenses

- Your UMS has the IGEL Enterprise UMS license; for details, see IGEL OS Editions[59]
- The IGEL Managed Hypervisor Add-On License is deployed to the image creation machine and all target machines

Supported Operating Systems on Virtual Machines

The following operating systems can be used on virtual machines created and managed by the IGEL Managed Hypervisor:

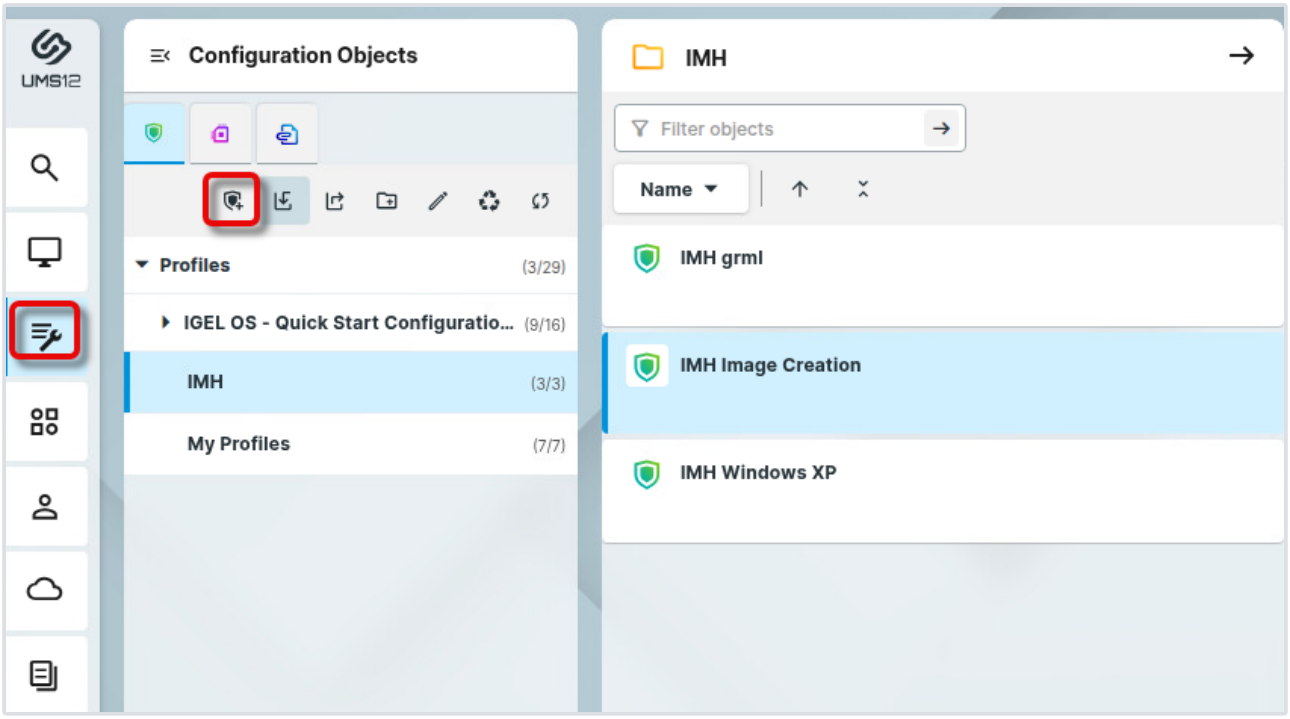
- Microsoft Windows XP
- Microsoft Windows 7
- Microsoft Windows Embedded Systems (WES) 7
- Microsoft Windows 10
- Microsoft Windows 10 IoT Core
- Microsoft Windows 11
- Microsoft Windows 11 IoT Core

Preparing the Image Creation Machine

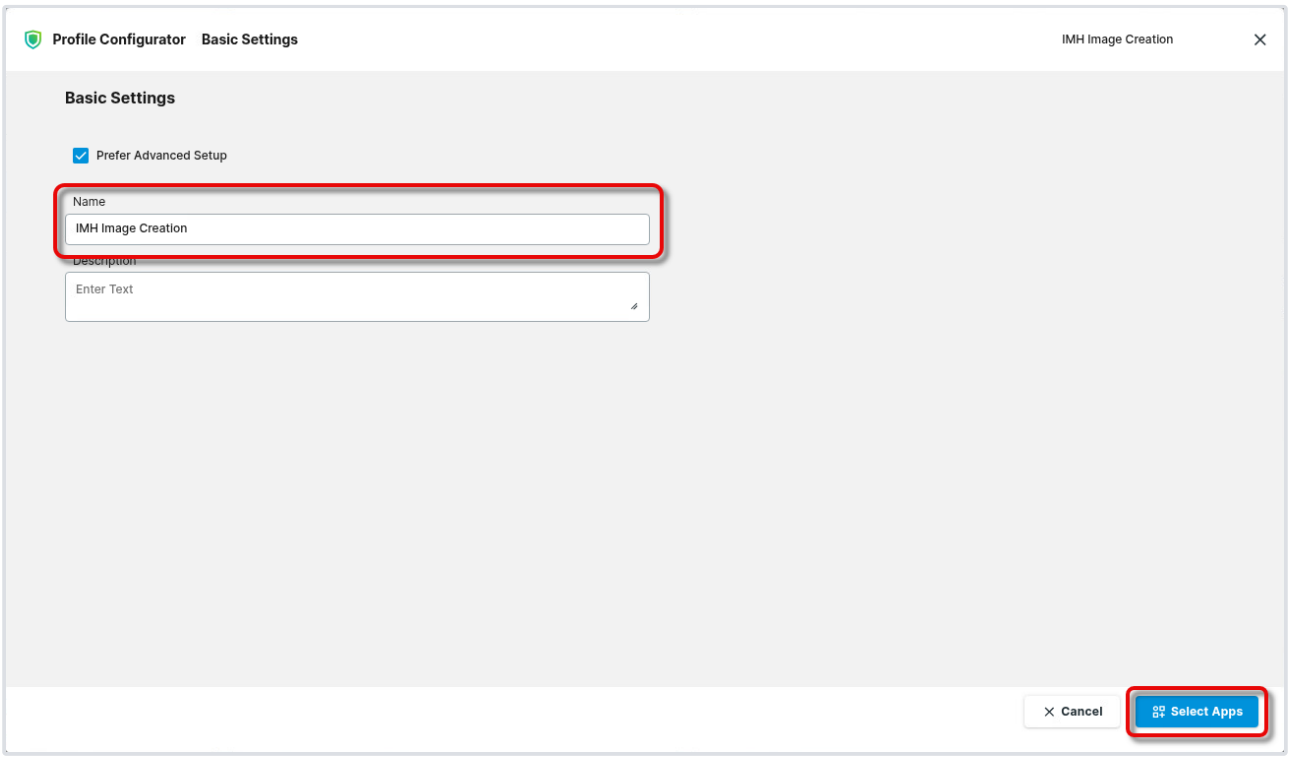
Creating a profile for the IGEL Managed Hypervisor App

1. Open the UMS Web Console, go to **Profiles**, and create a new profile.

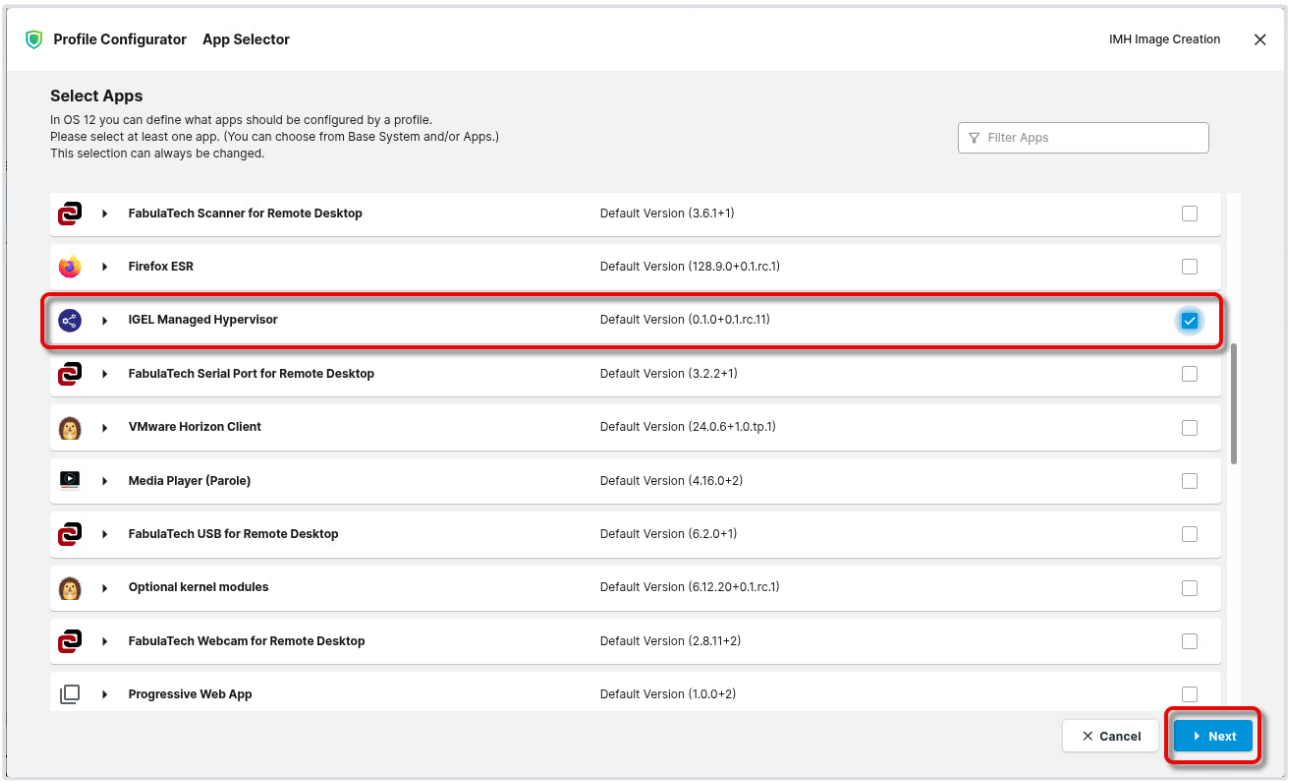
59. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions



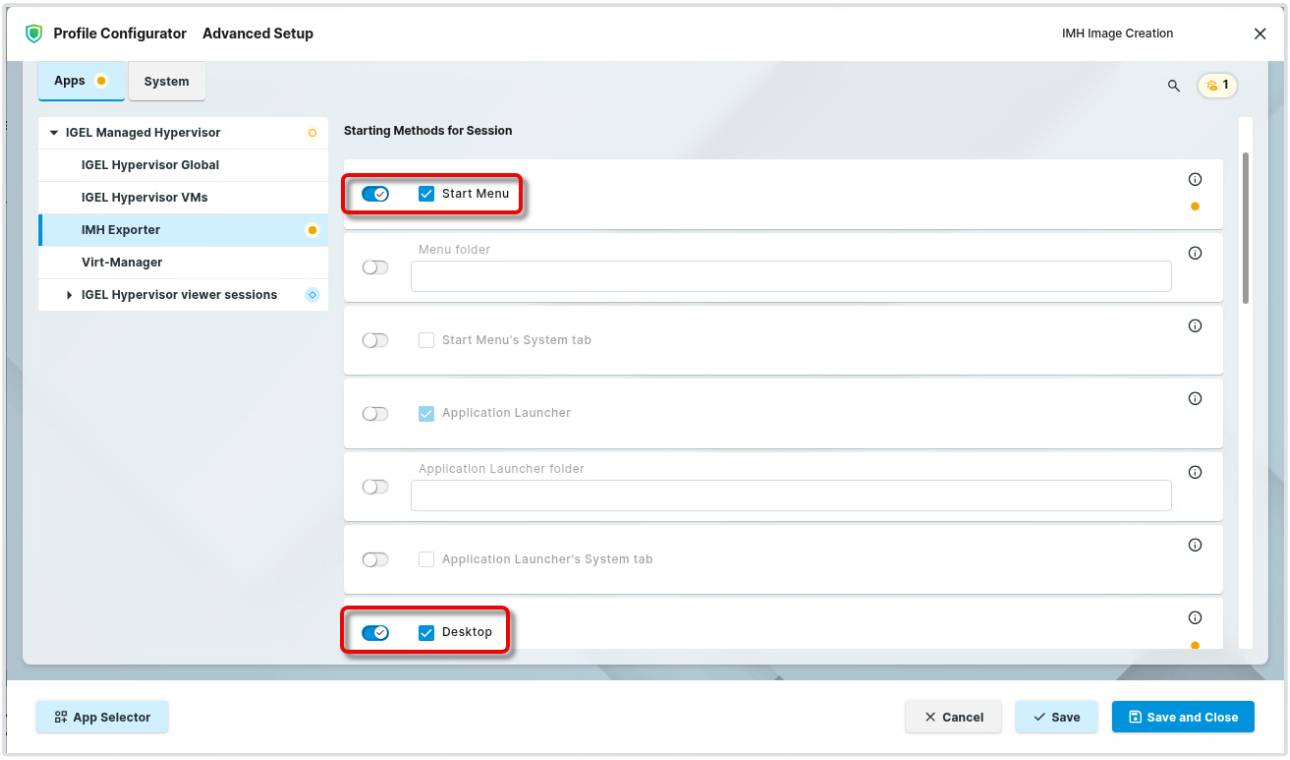
2. Provide a **Name** for the profile and click **Select Apps**.



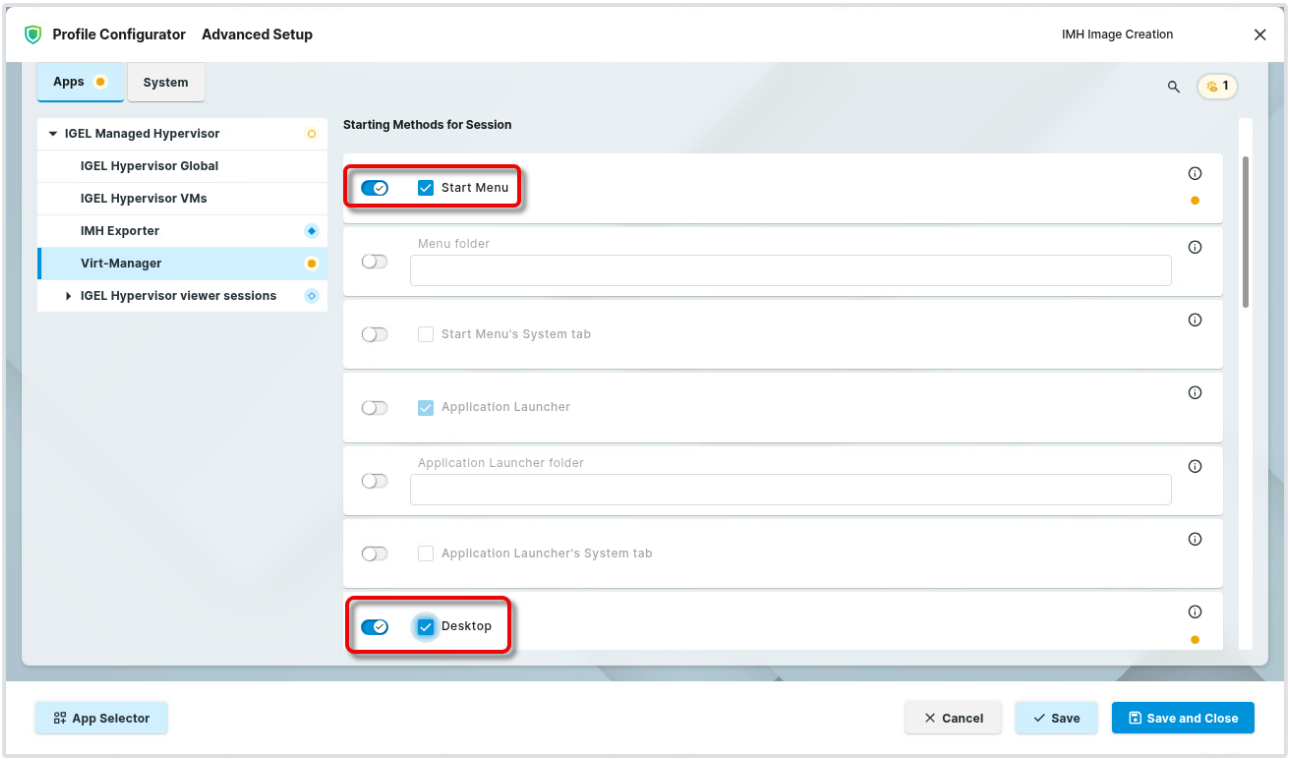
3. Select the app **IGEL Managed Hypervisor** and click **Next**.



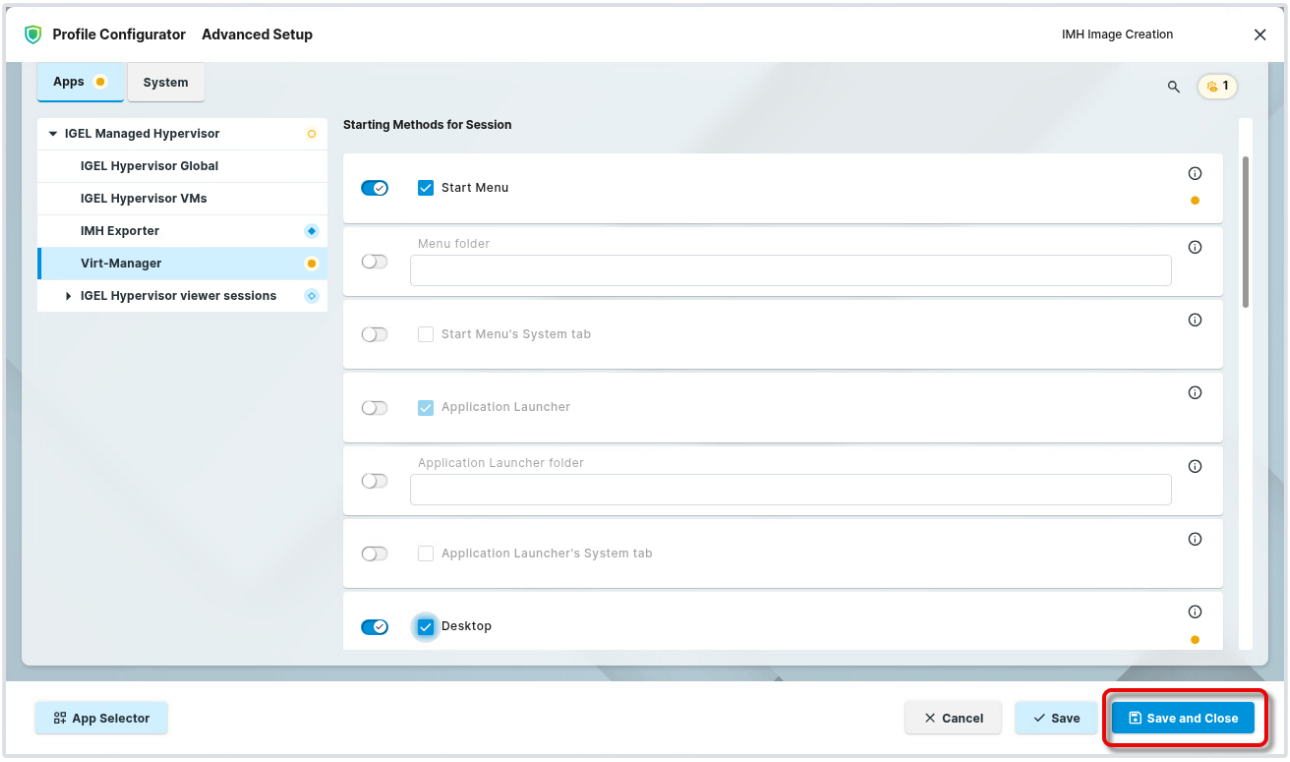
4. If you want to configure the start options for the IMH Exporter, go to **Apps > IGEL Managed Hypervisor > IMH Exporter** and add/remove starting methods. In our example, we add a starter to the start menu and to the desktop.



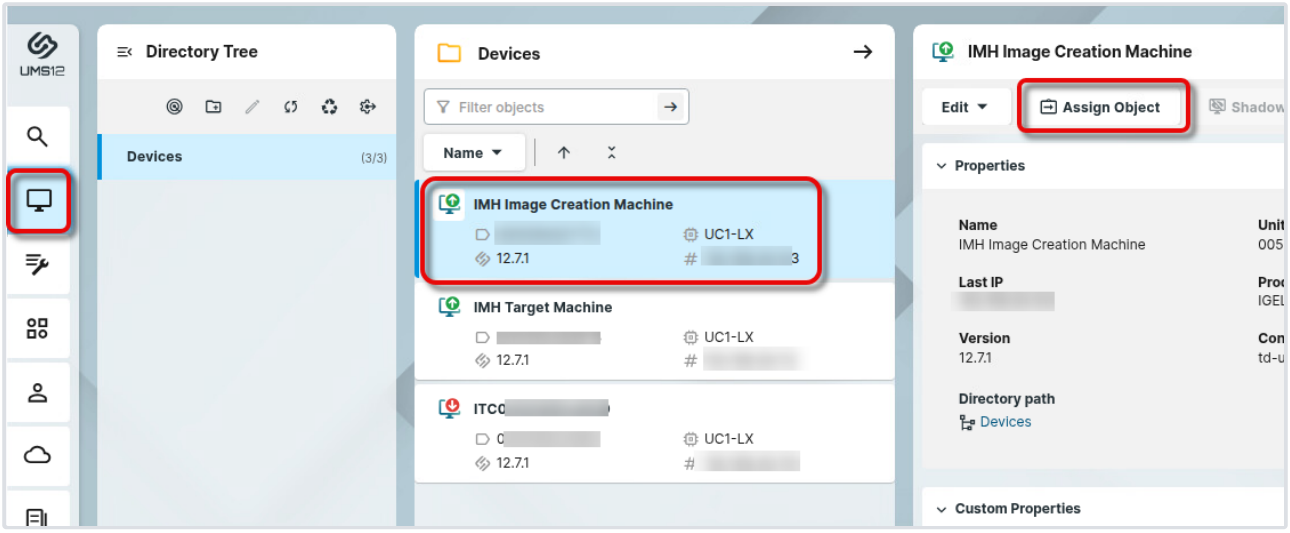
5. If you want to configure the start options for virt-manager, the actual tool for creating the virtual machine, go to **Apps > IGEL Managed Hypervisor > Virt-Manager** and add/remove starting methods. In our example, we add a starter to the start menu and to the desktop.



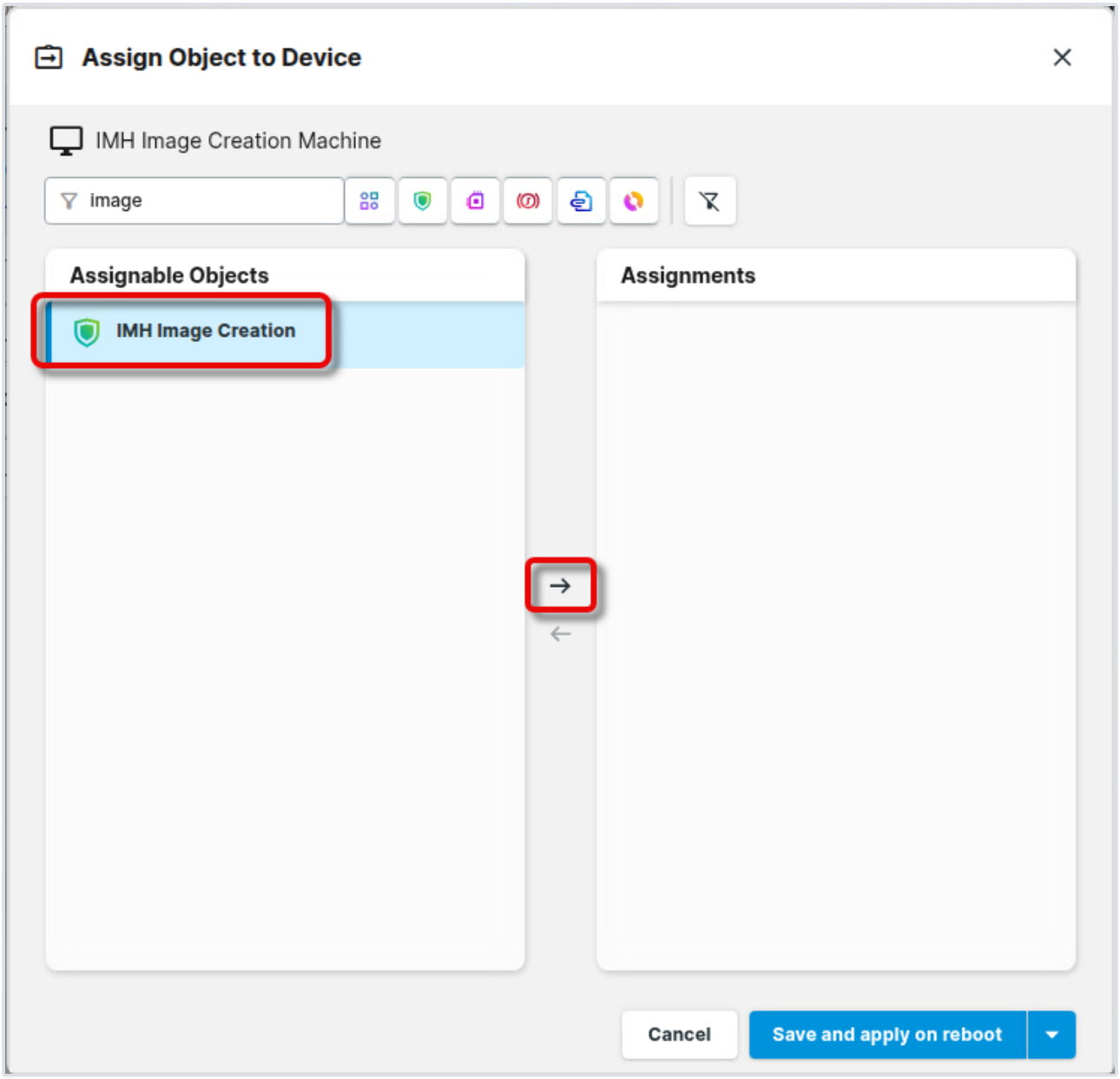
6. Click **Save and Close** to finish the profile.

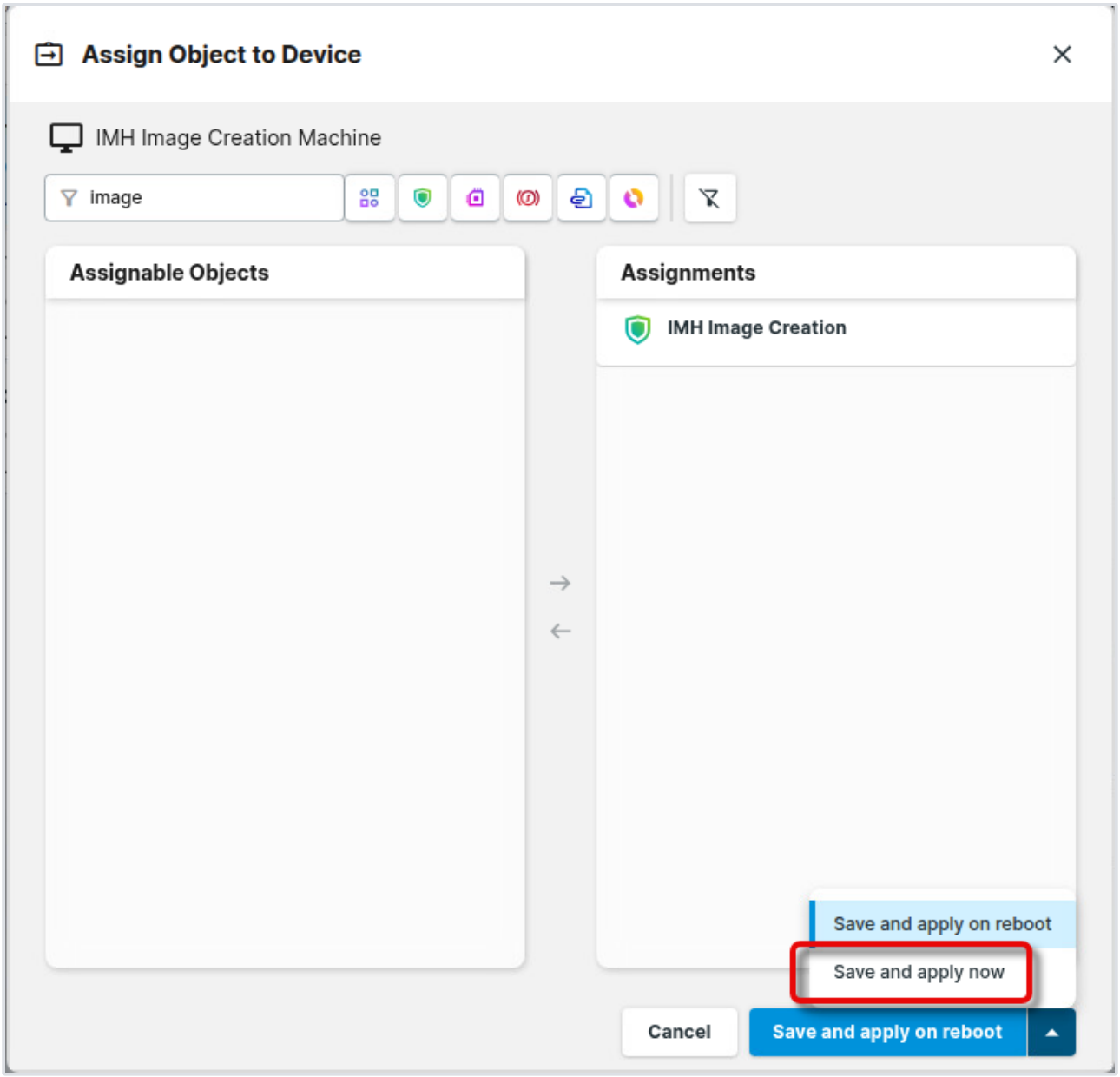


7. Go to **Devices**, select your image creation machine, and click **Assign Object**.



8. Find and select your profile and assign it to your device.


Assign Object to Device
IMH Image Creation Machine
image
Assignable Objects
IMH Image Creation
Assignments
Cancel
Save and apply on reboot



Providing the ISO File

We must ensure that the ISO file from which we will create the Golden Image is available to the image creation machine.

You can use the following methods to provide the ISO file:

- Local installation media (ISO image on a USB memory stick, network drive, or CD-ROM)
- Network installation

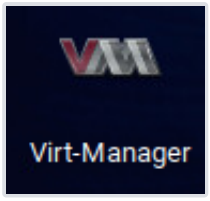
- Manual installation

In our example, we will use a local installation medium.

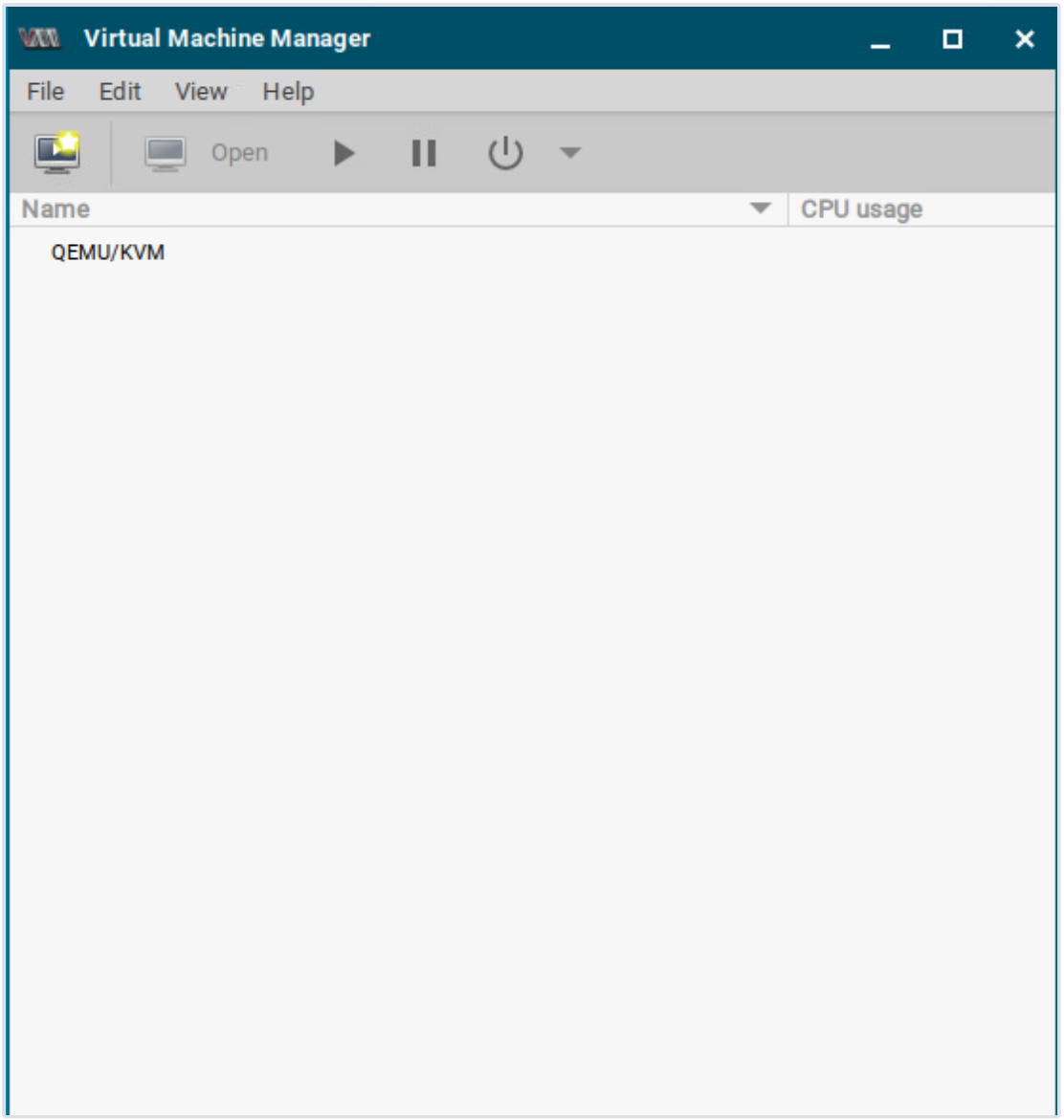
→ Ensure that the installation media is accessible for IGEL OS.

Creating Your Golden Image on the Image Creation Machine

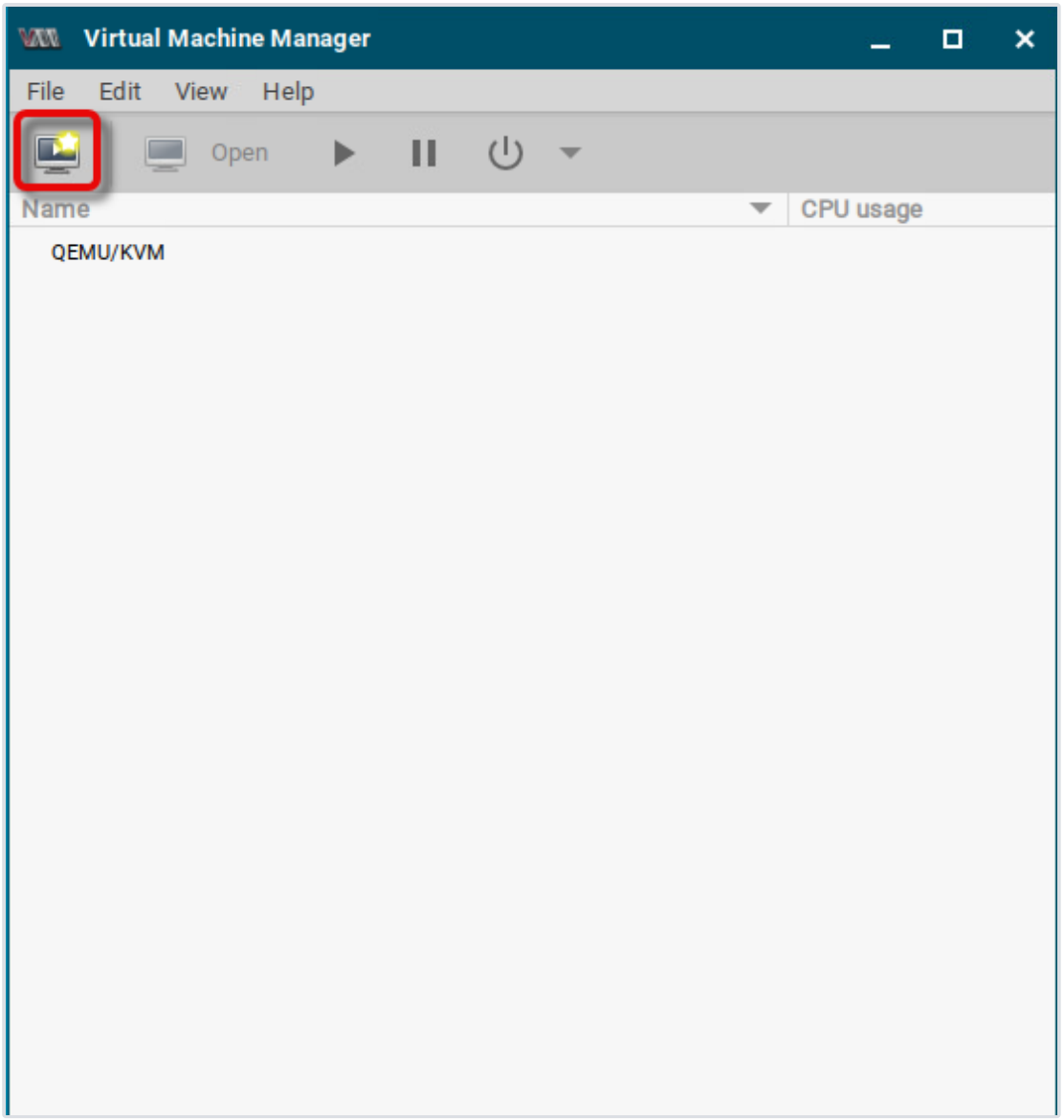
1. Click the virt-manager start icon. (In our example, we configured a start icon on the desktop.)



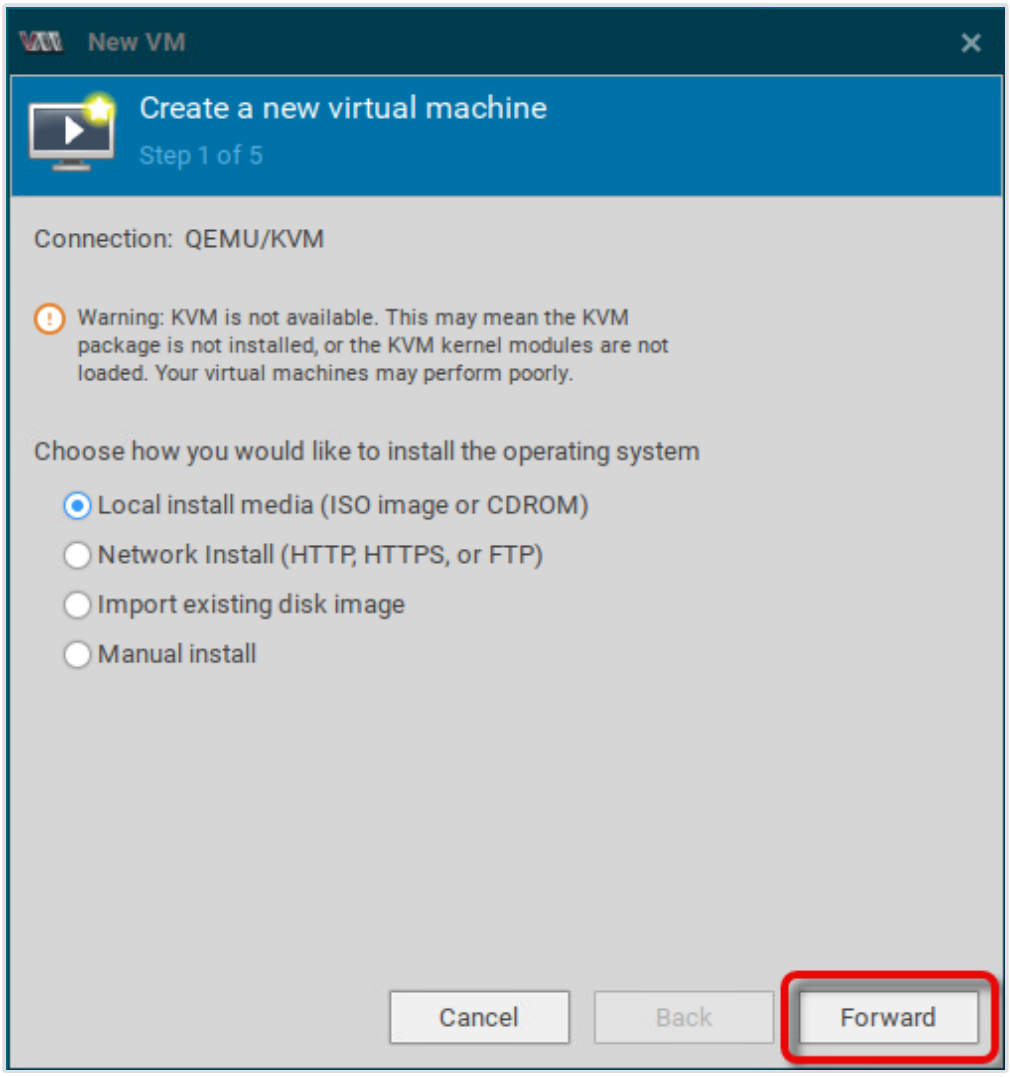
The **Virtual Machine Manager** appears.



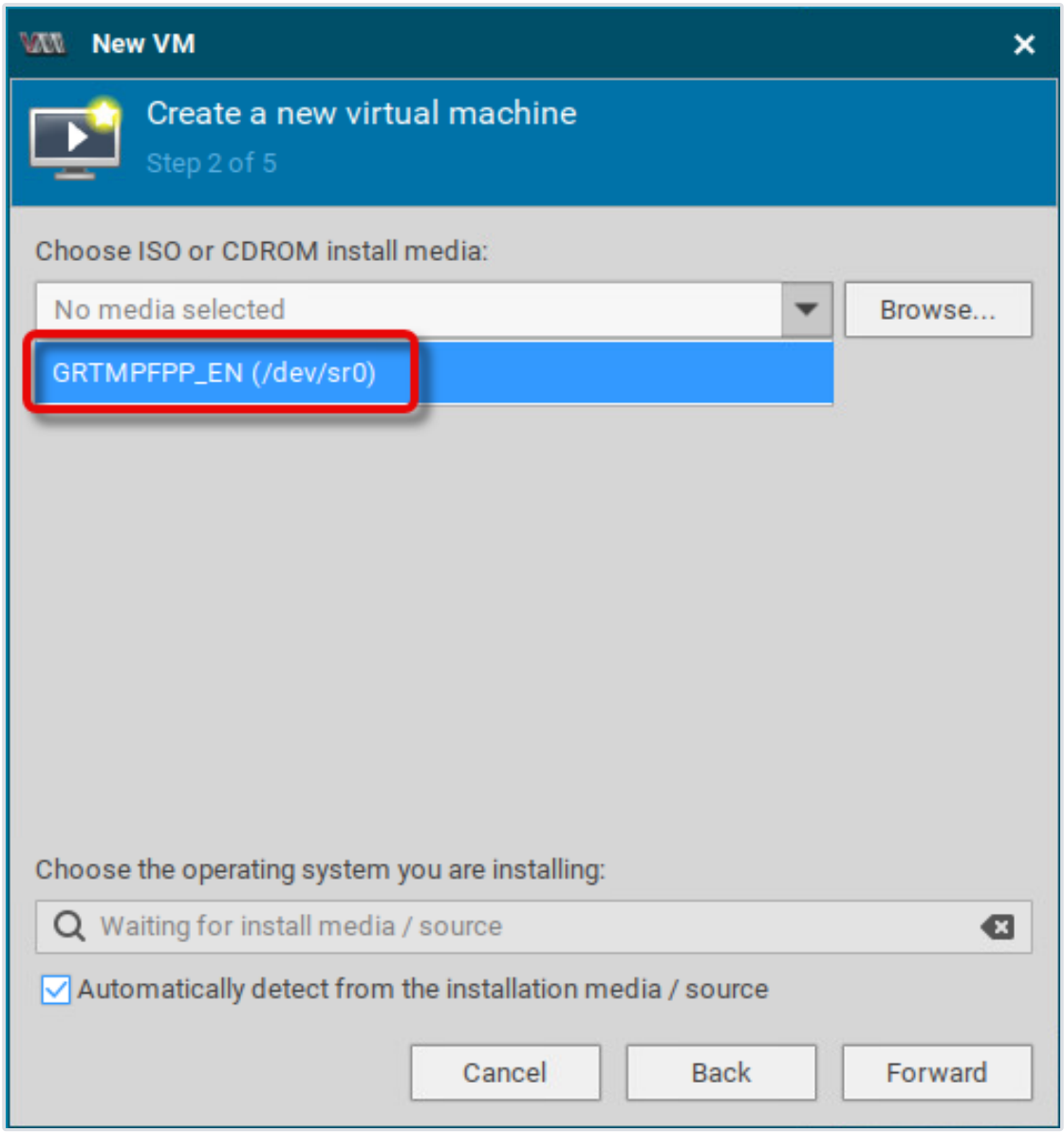
2. Click to create a new machine.

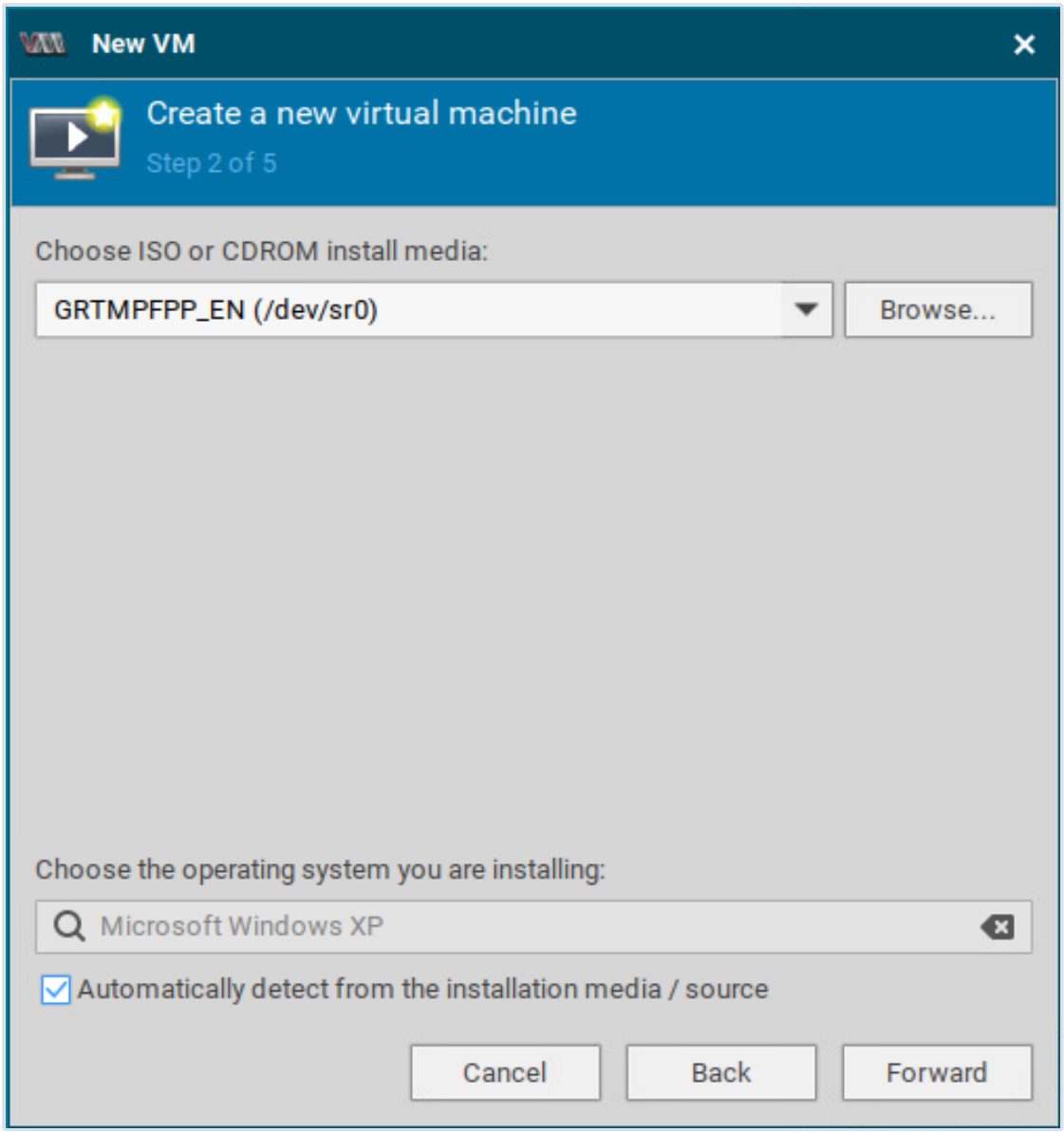


4. Select the source for the new virtual machine (in our example: **Local install media (ISO image or CDROM)**) and click **Forward**.

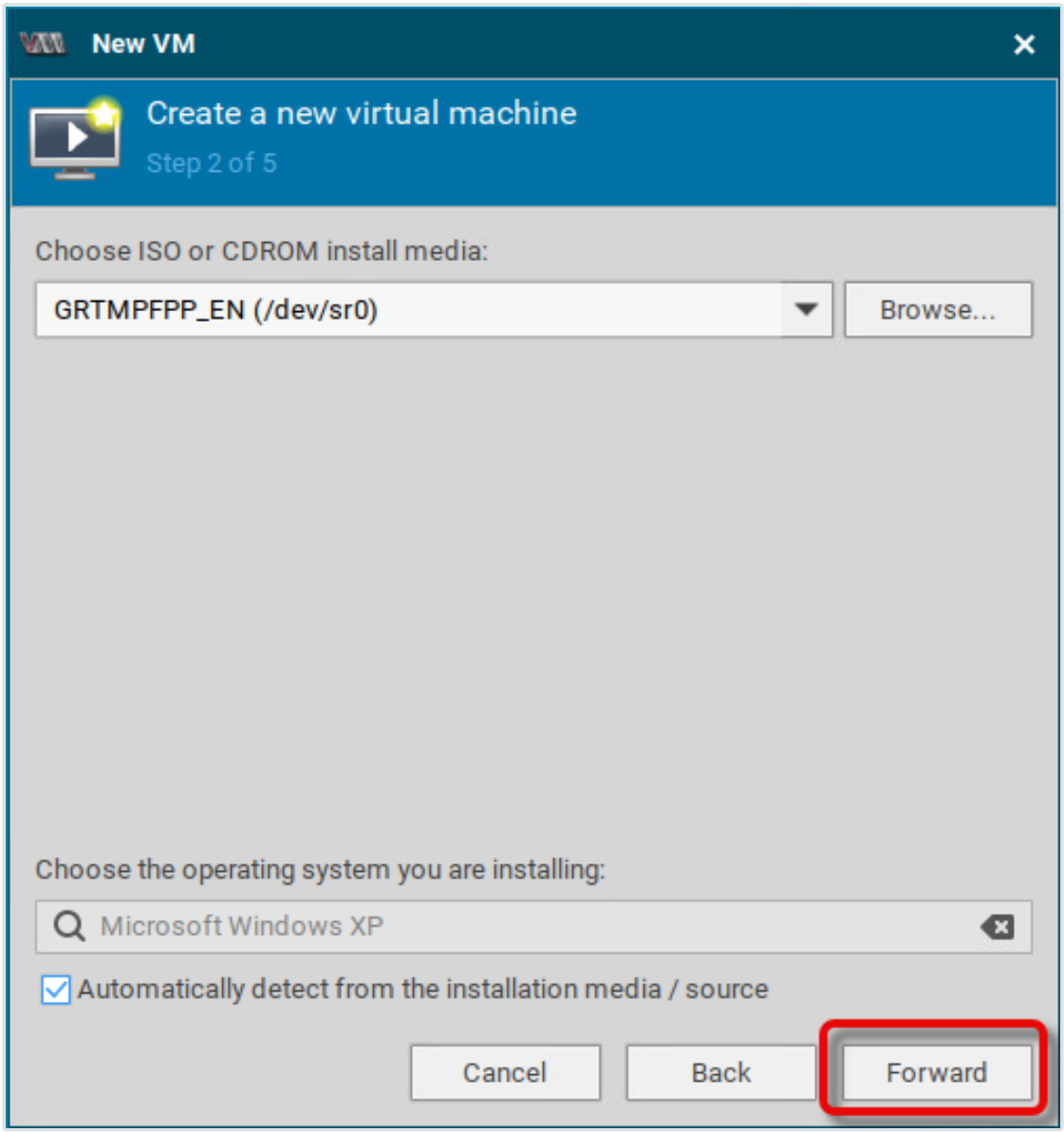


5. Select your installation media. **Browse...**

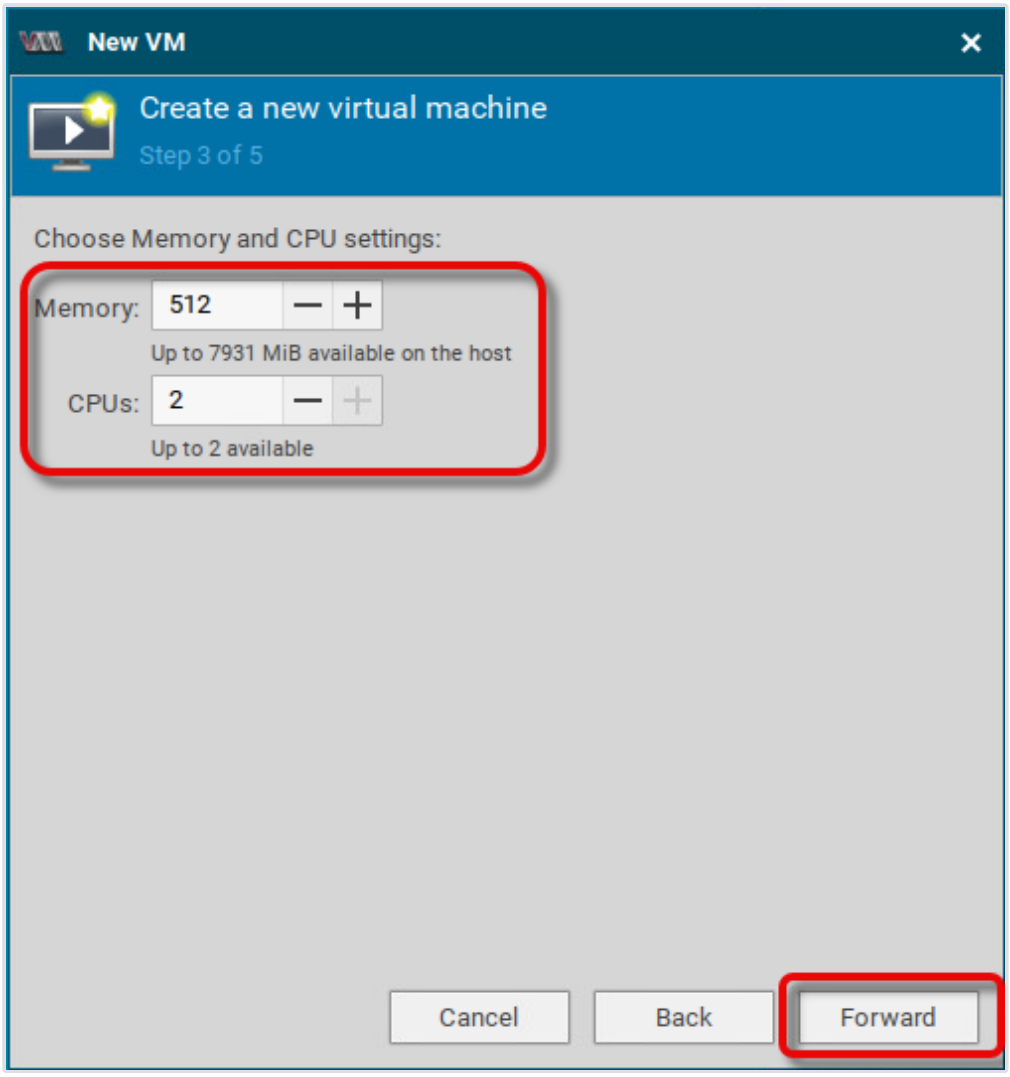

New VM
Create a new virtual machine
Step 2 of 5
Choose ISO or CDROM install media:
No media selected
Browse...
GRTMPFPP_EN (/dev/sr0)
Choose the operating system you are installing:
Waiting for install media / source
Automatically detect from the installation media / source
Cancel
Back
Forward



6. Click **Forward**.

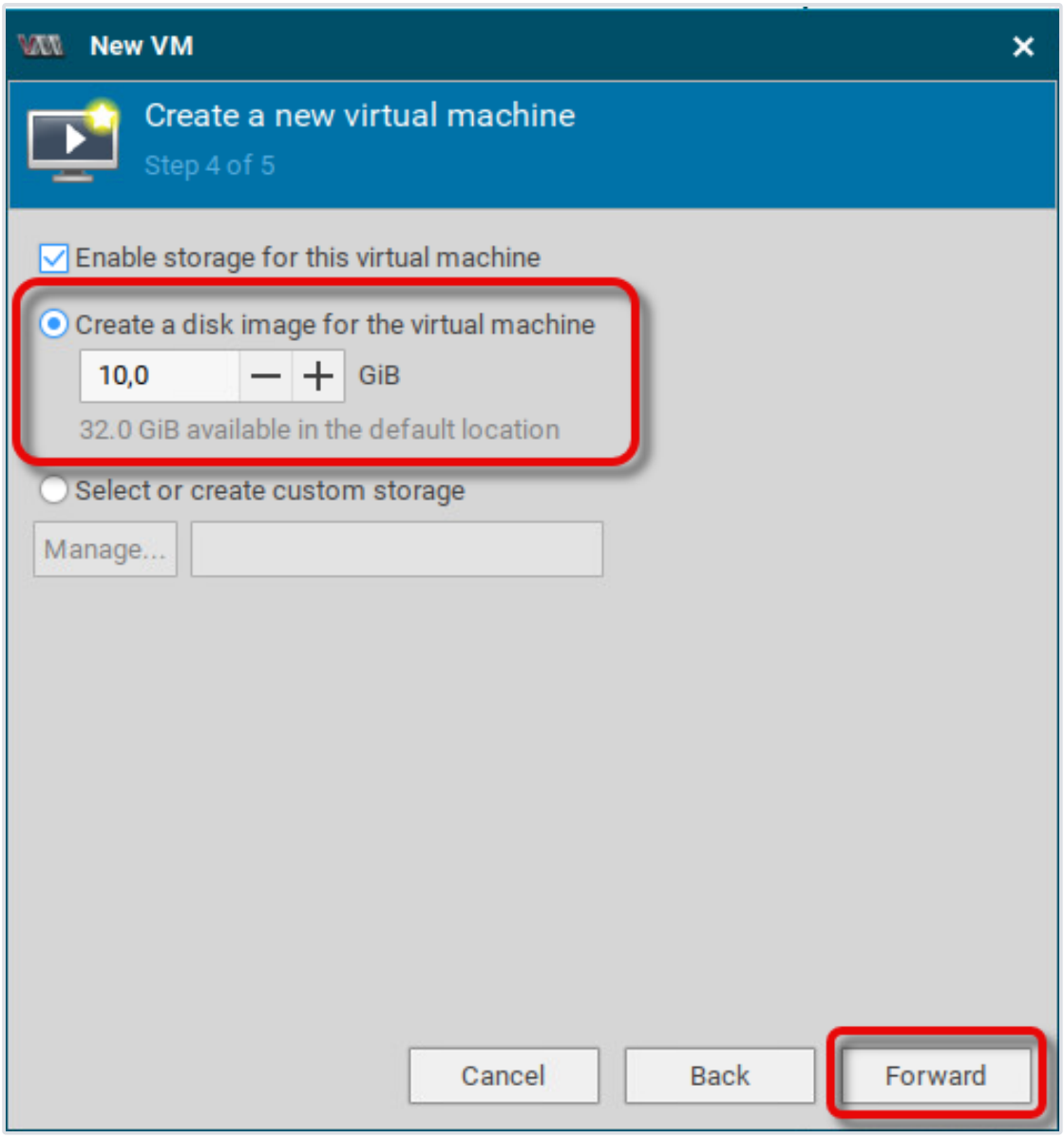


7. Choose the RAM size and the number of CPUs. Afterward, click **Forward**.

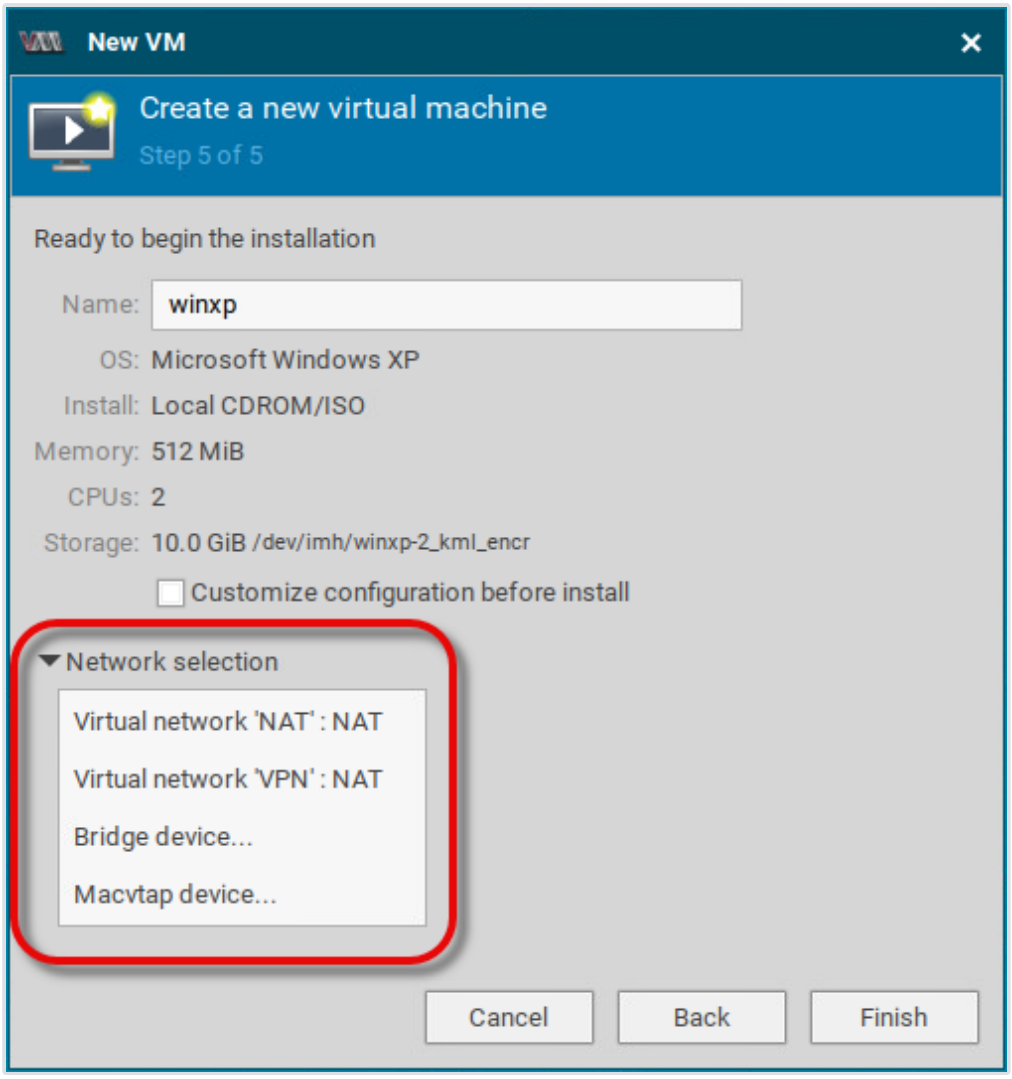


8. Review the size of the disk image that is to be created and click **Forward**.

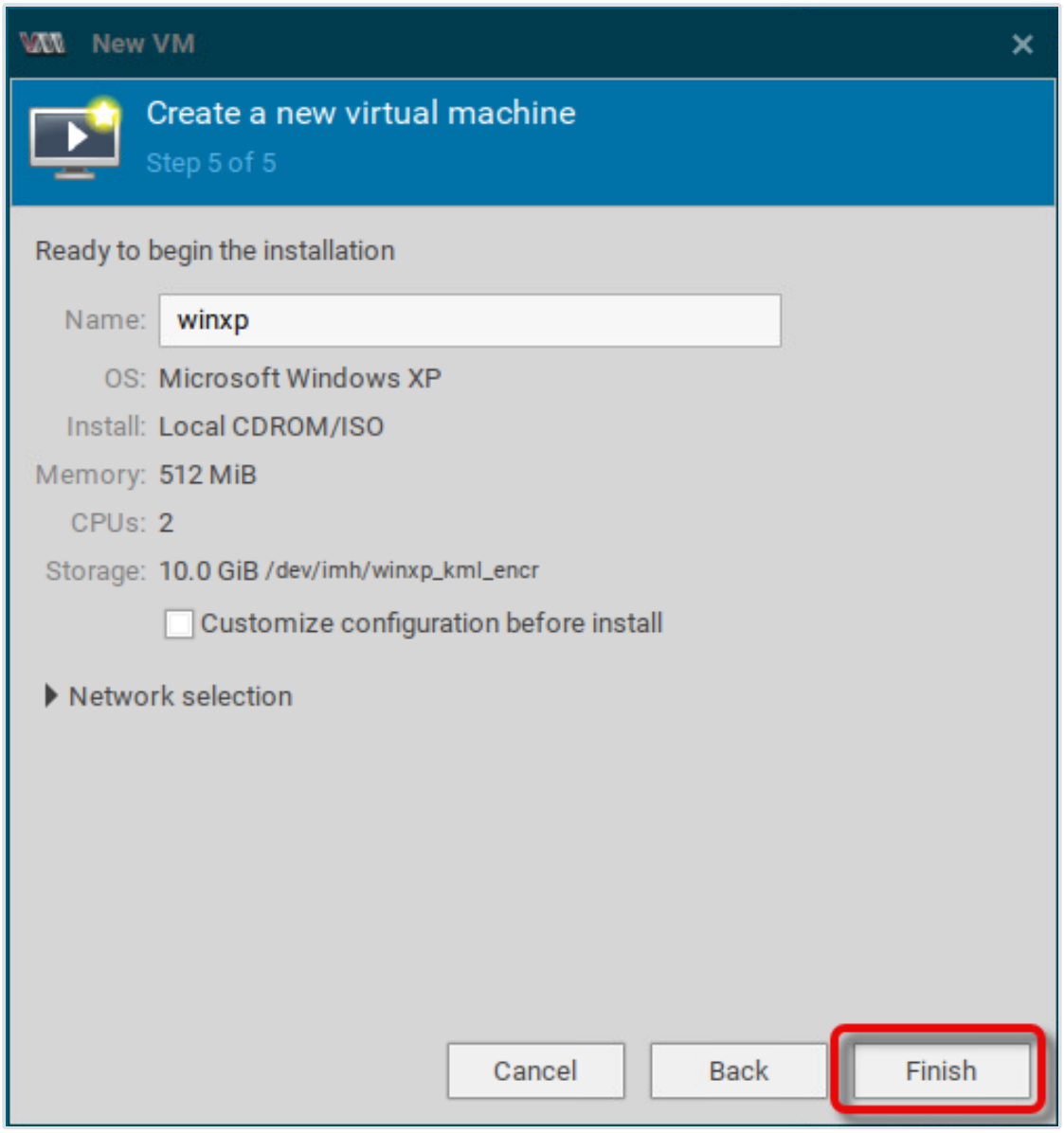
We do NOT recommend selecting or creating custom storage; this might interfere with the preconfigured storage provided by IGEL Managed Hypervisor.



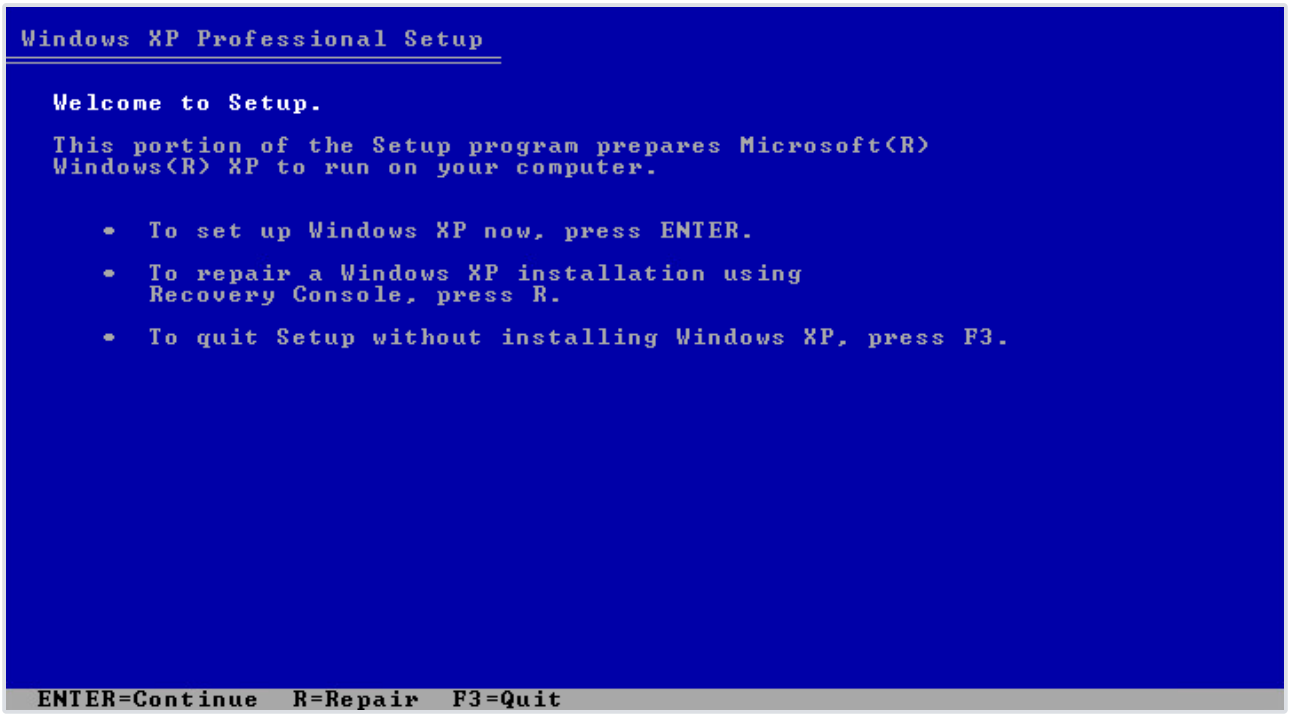
9. Select the network to be used by the virtual machine.



10. Review the settings and click **Finish**.



The installer provided by the ISO file starts (in our example: Microsoft Windows XP).



10. Follow the instructions to install your guest system; if required, modify it according to your needs.

Exporting Your VM Image to the WebDAV server

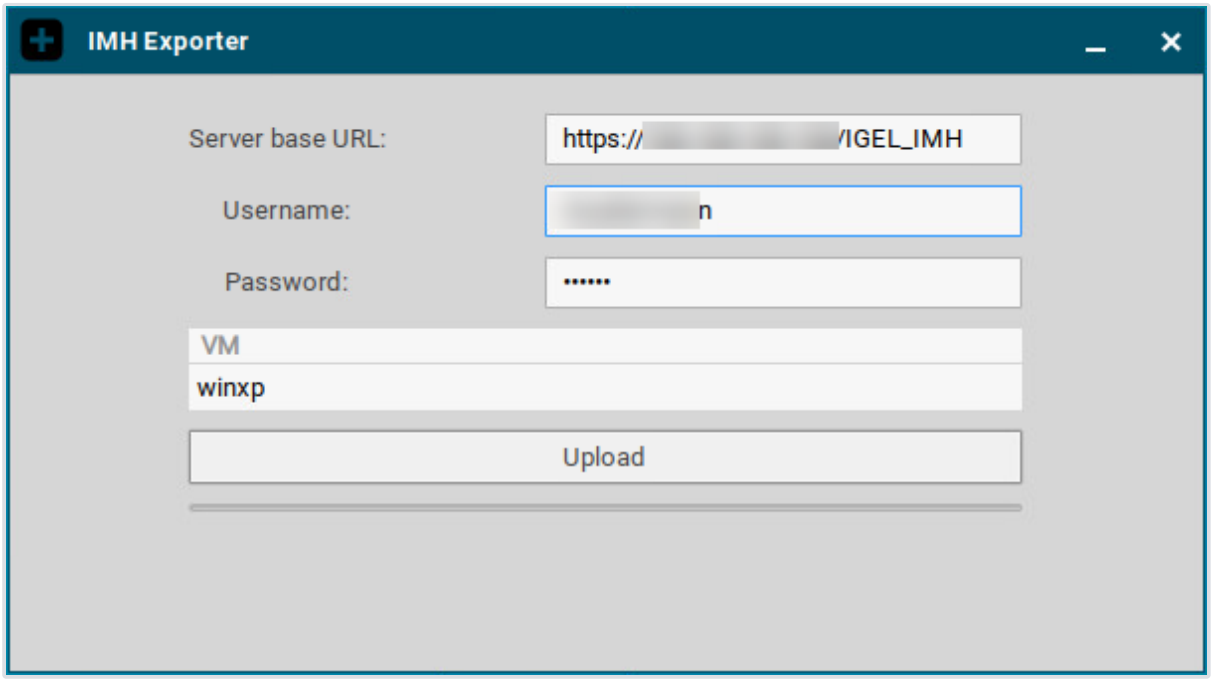
1. On the image creation machine, shut down the virtual machine.

2. Start the IMH Exporter by clicking on this icon:



3. Enter the required data:
   - **Server base URL**: The path to the directory on the WebDAV repository

- **Username**: The username for write access to the WebDAV repository
- **Password**: The password associated with the username. Please note that the password must not contain “@”.
- **VM**: Select the name of the image you have created.

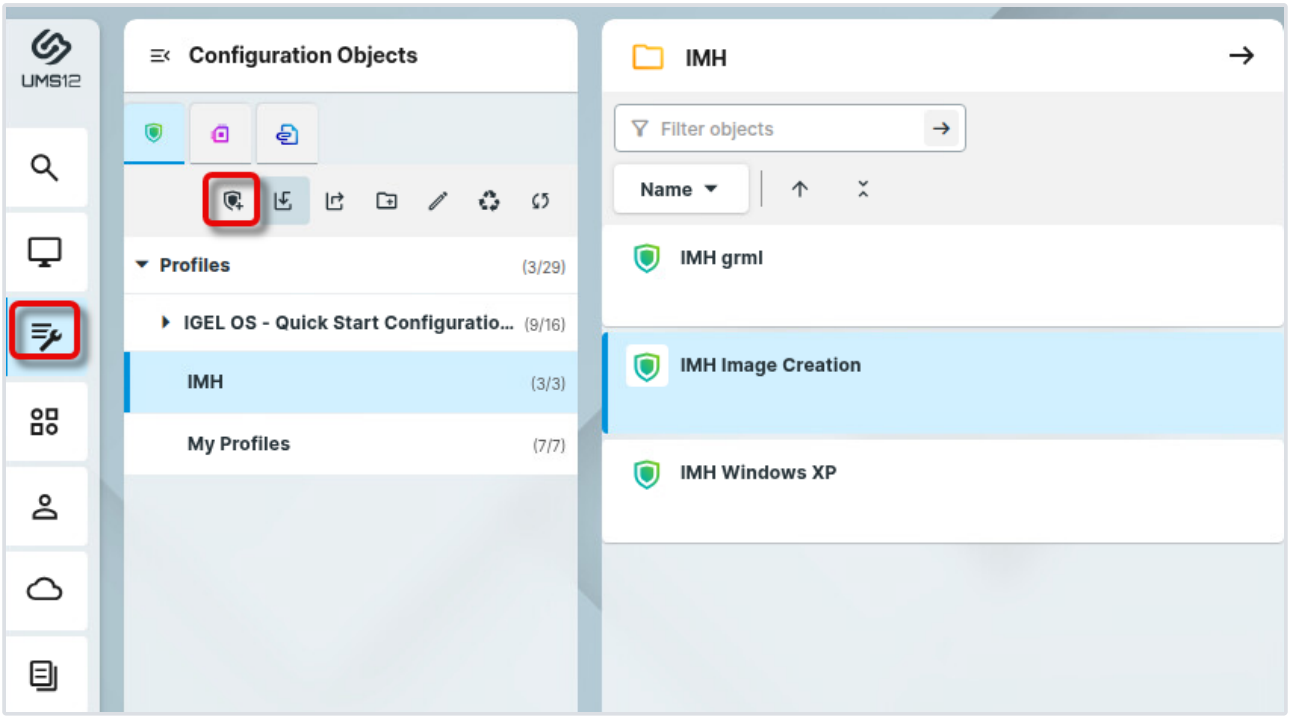


The following files are uploaded to the WebDAV repository:

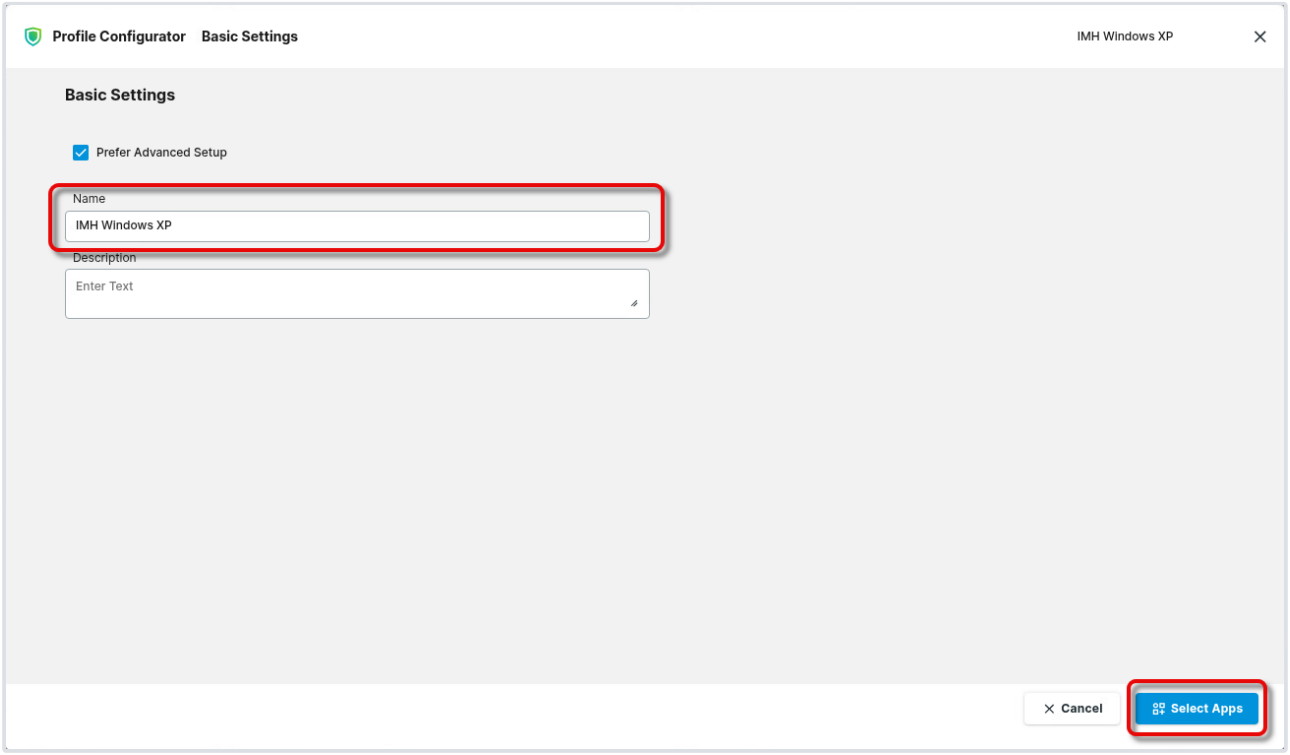
- `<Server base URL>/<domain>.xml` : An XML file that provides the size, URL, checksum, and compression method of the image file. Example: `https://123.123.123.123/IGEL_IMH/winxp.xml`
- `<Server base URL>/<domain>_d0.img.lz4:` The image file, compressed with lz4. Example: `https://123.123.123.123/IGEL_IMH/winxp_d0.img.lz4`

Distributing Your VM Image to the Target Machines

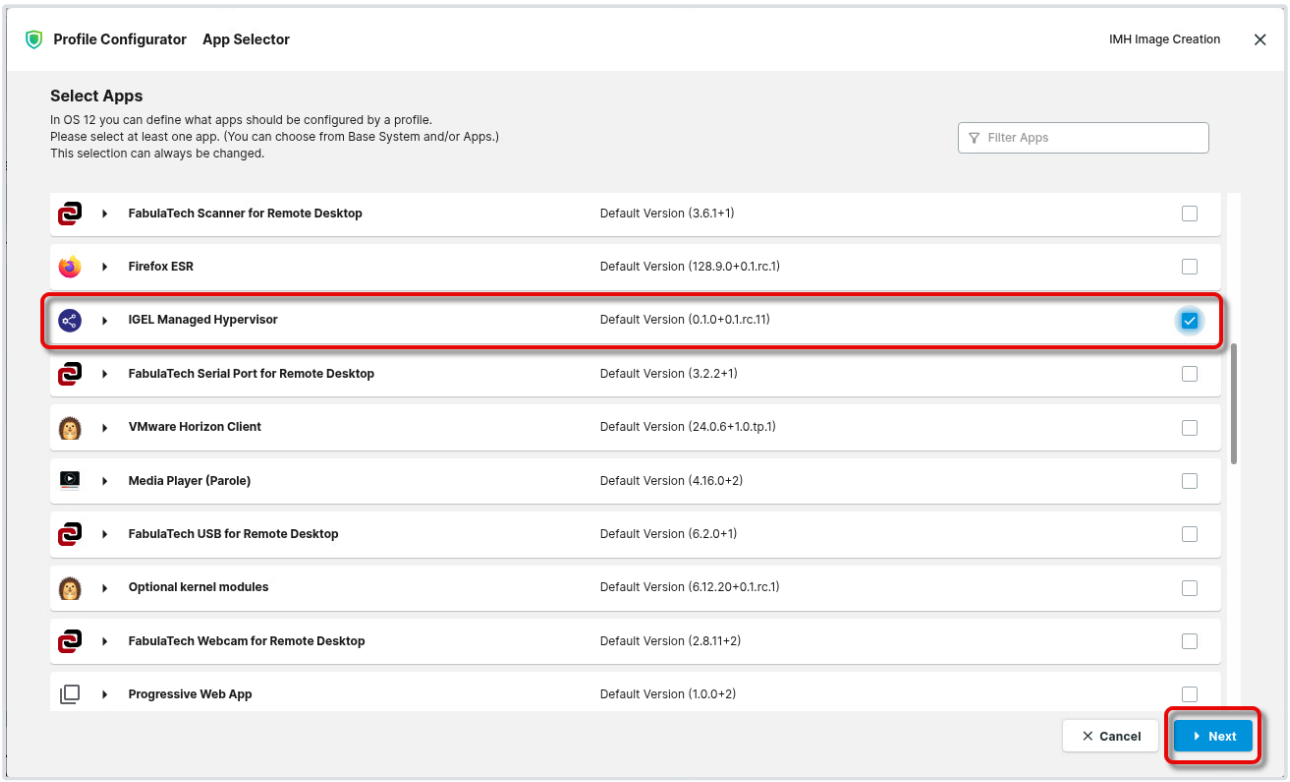
1. In the UMS Web Console, go to **Profiles**, and create a new profile.



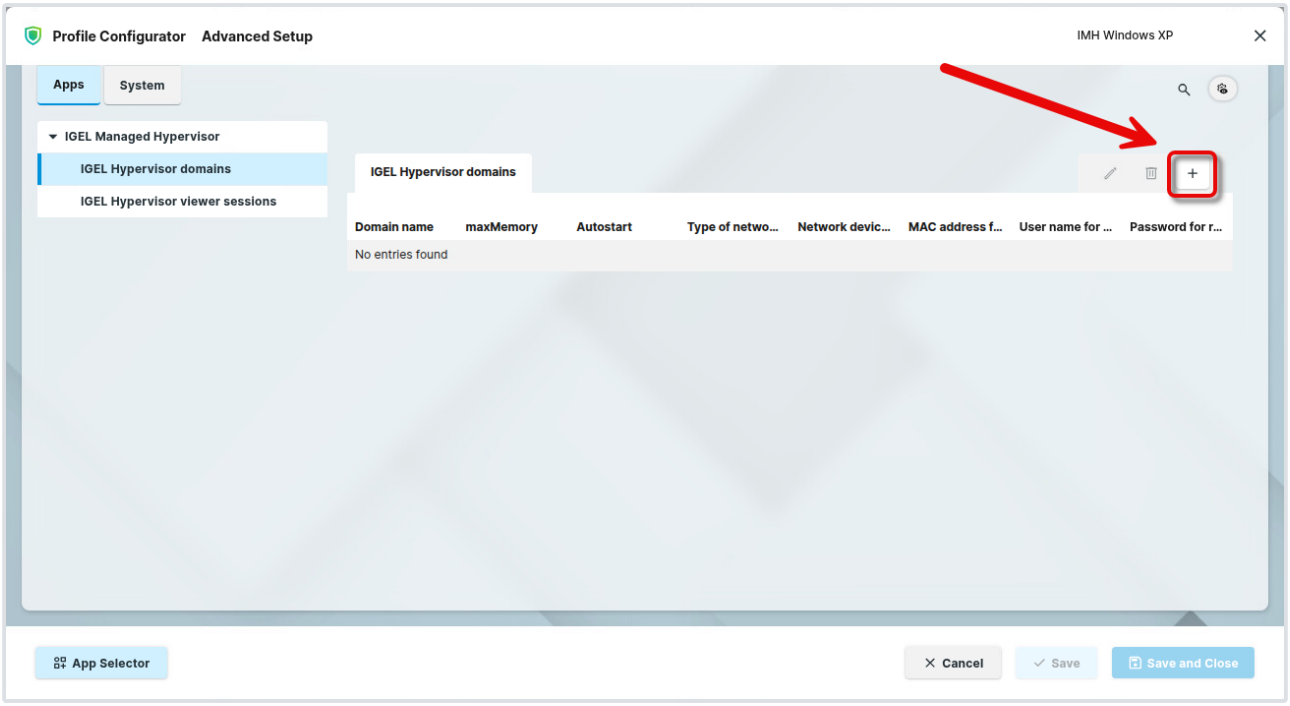
2. Provide a **Name** for the profile and click **Select Apps**.



3. Select the app **IGEL Managed Hypervisor** and click **Next**.



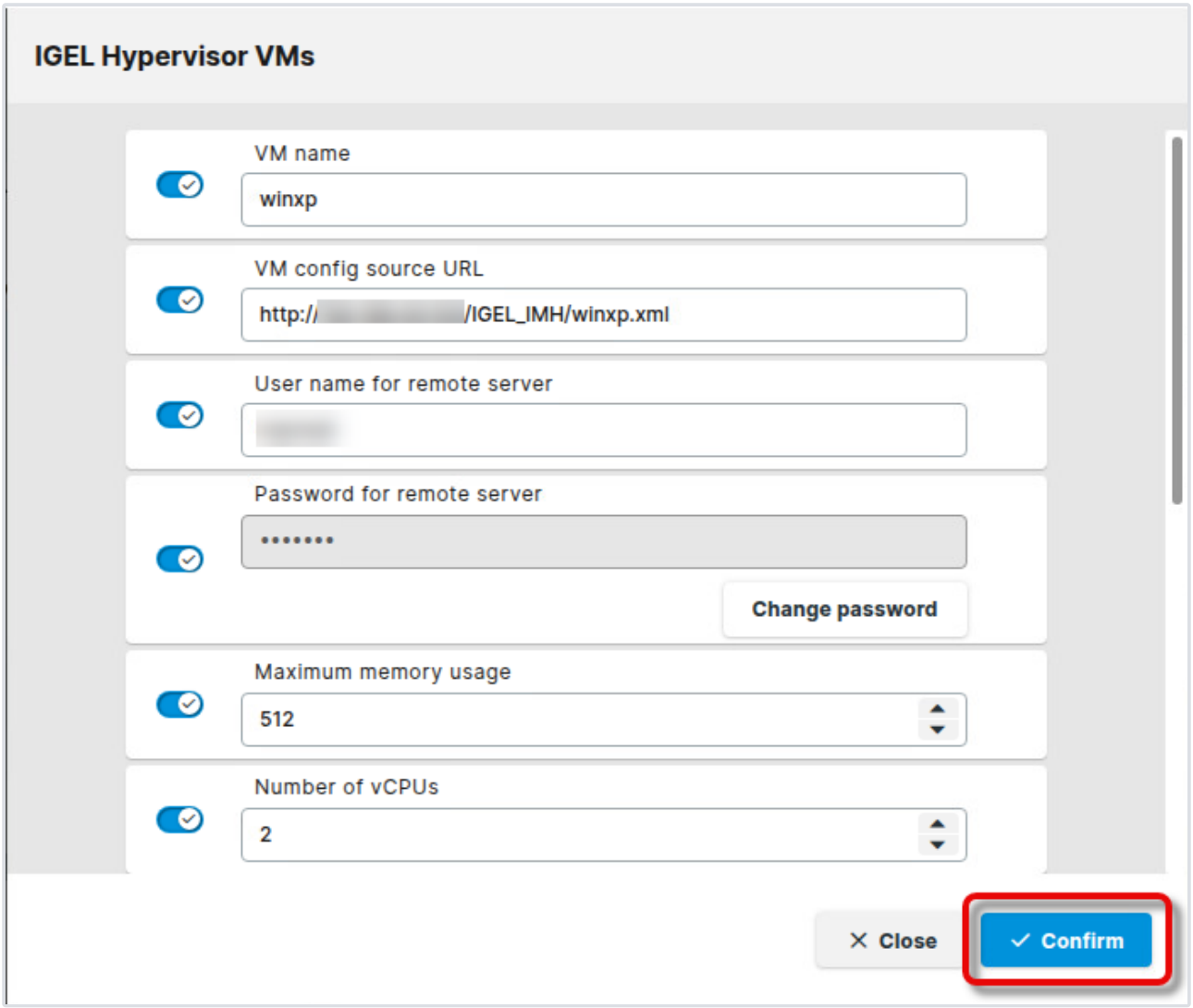
4. Go to **Apps > IGEL Managed Hypervisor > IGEL Hypervisor domains** and click **+** to add a new domain.



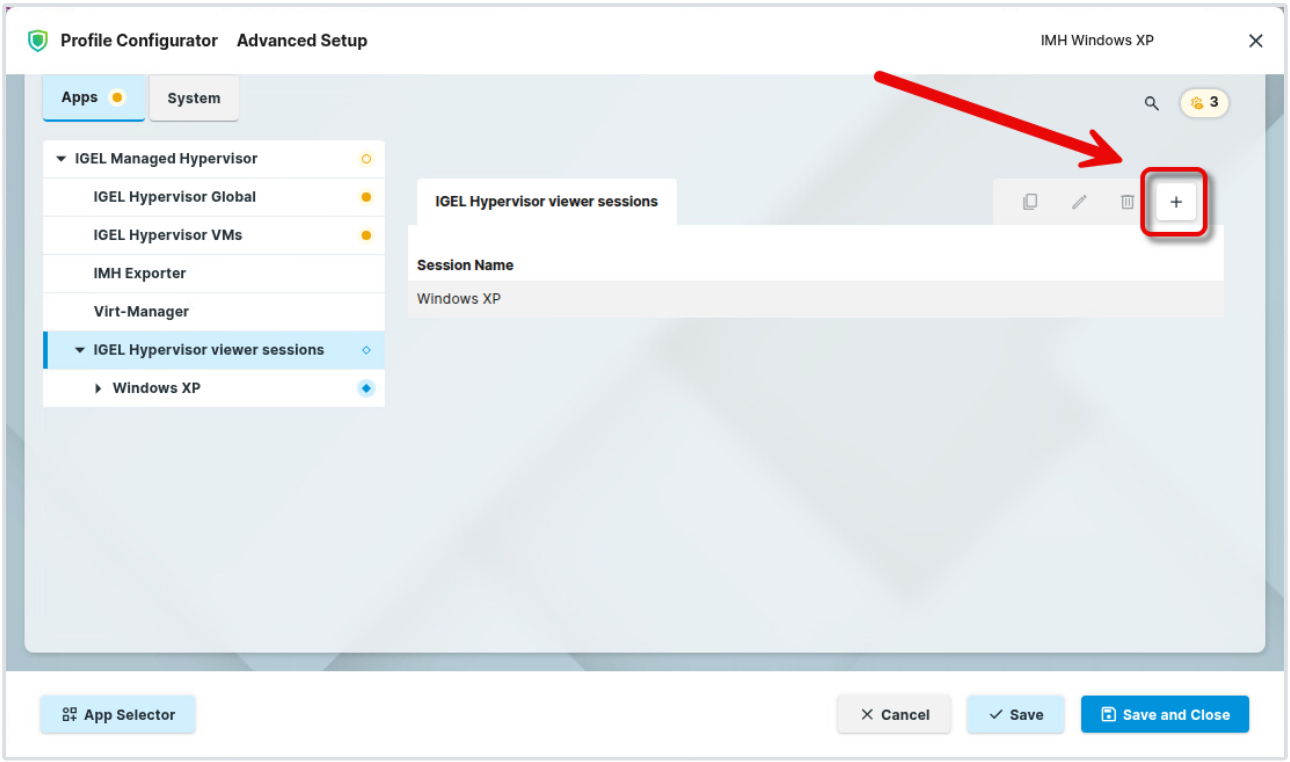
5. Edit the data according to your needs:

- **VM name**: The name of the virtual machine you have created
- **VM config source URL**: The URL of the XML file you have exported
- **User name for remote server**: The username for read access to the WebDAV repository
- **Password for remote server**: The password associated with the username
- **Maximum memory usage**: The maximum memory (RAM) used by the virtual machine
- **Number of vCPUs**: The number of virtual CPUs
- **Autostart**: When enabled, the virtual machine will be started automatically
- **Disk Image is immutable:** If enabled, changes in the virtual machine will be gone when it is restarted. If this is disabled (default), changes in the virtual machine will persist after a restart.
- **MAC address for virtual interface**: You can specify the MAC address of your virtual machine's network interface. This is useful if the software in your virtual machine is licensed for a specific MAC address.
- **Type of network for this VM**: The following networks are supported on the target machines:
  - **isolated**: The network interface is deactivated in the virtual machine.
  - **NAT**: Network Address Translation (NAT) is used; the host machine translates the internal IP address of the virtual machine to its own IP address.
  - **bridged**: The network device specified in **Network device used for this VM. Will be ignored for some pre-configured bridge devices** is used.
  - **hostonly**: The preconfigured hostonly bridge is used.
  - **macvtap**: The network device specified in **Network device used for this VM. Will be ignored for some pre-configured bridge devices** is used with the macvtap driver.

- **Network device used for this VM. Will be ignored for some pre-configured bridge devices**: Create a network interface by setting the Registry key **network.interfaces.ethernet.device<NUMBER>.bridge** (**System** tab **> Registry > network > interfaces > ethernet > device<NUMBER>.bridge** to **own**). Example: If the setting has been made for device0, the network interface will be `breth0`. Enter the resulting name in this field.

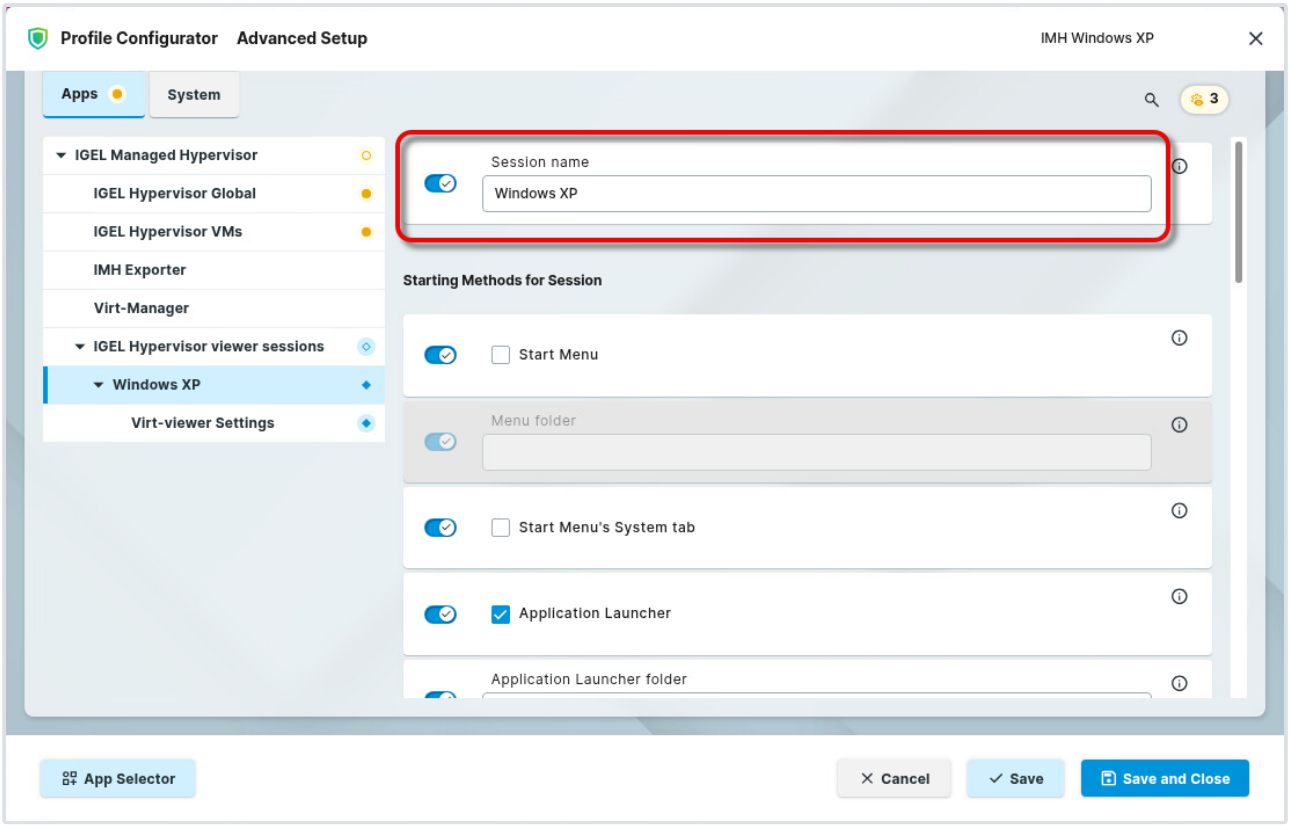


6. Go to **Apps > IGEL Managed Hypervisor > IGEL Hypervisor viewer sessions** and click **+** to add a new session.



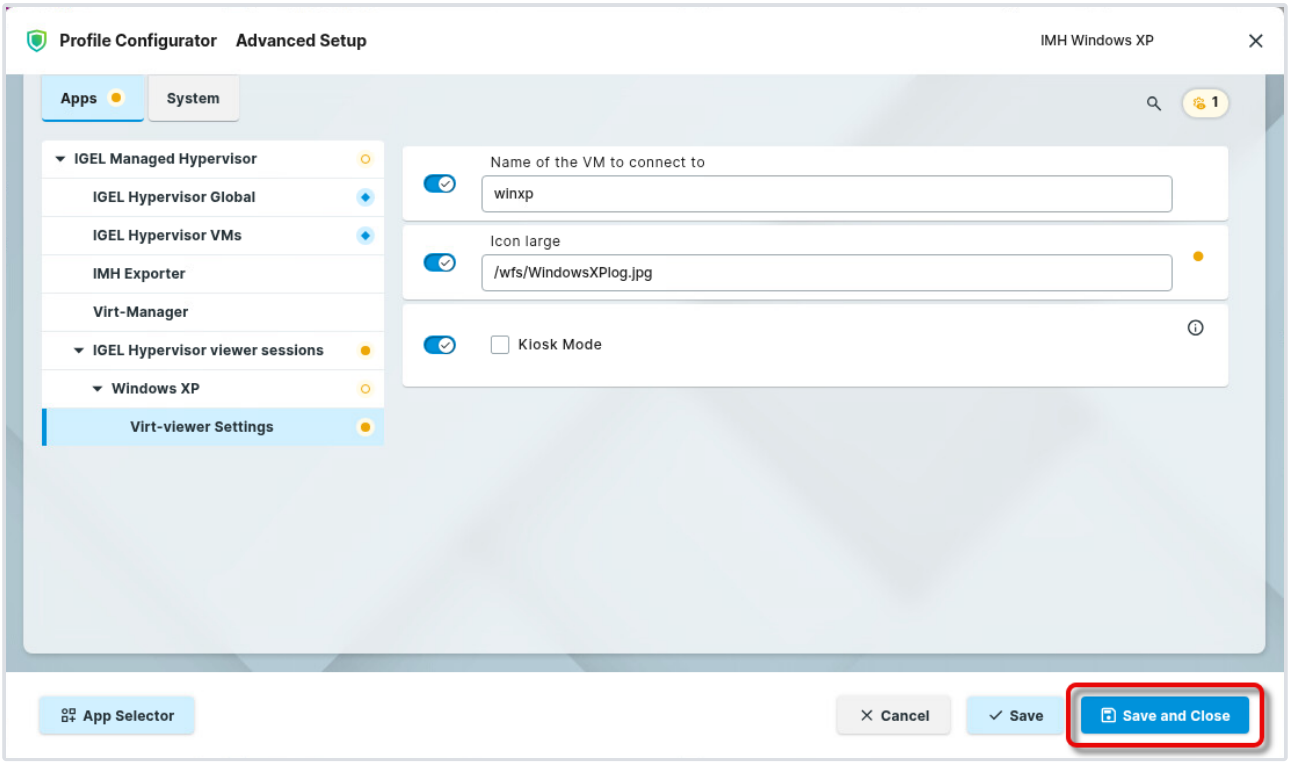
7. Enter a **Session name** and configure the start options according to your needs. For details on the start options, see Starting Methods for Apps[60] .

60. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

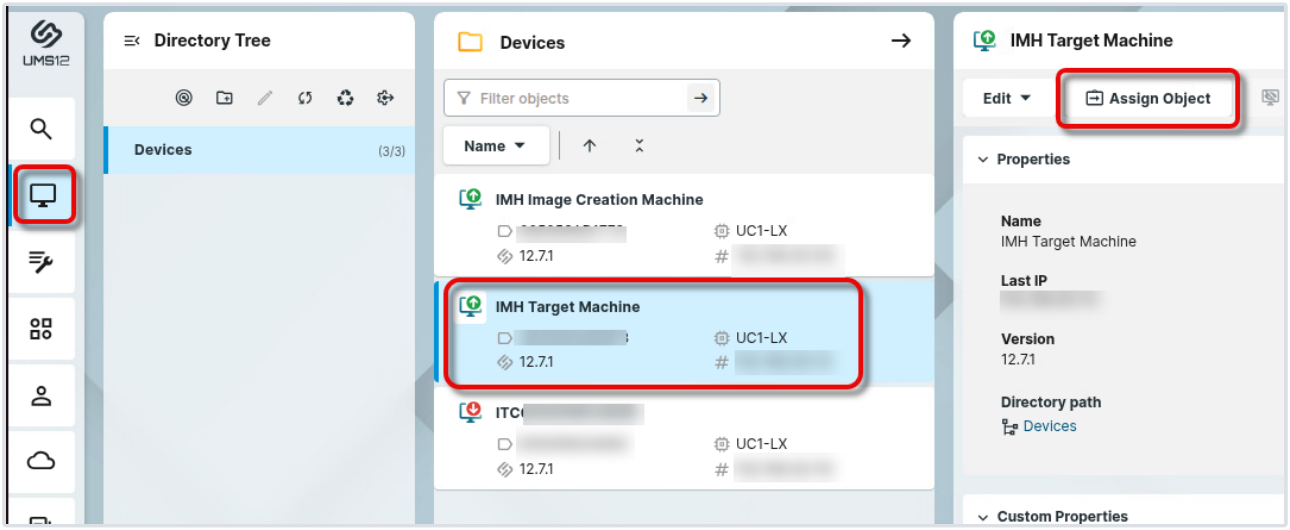


8. Go to **Apps > IGEL Managed Hypervisor > IGEL Hypervisor viewer sessions > [session name] > Virt-viewer Settings** and edit the data according to your needs:

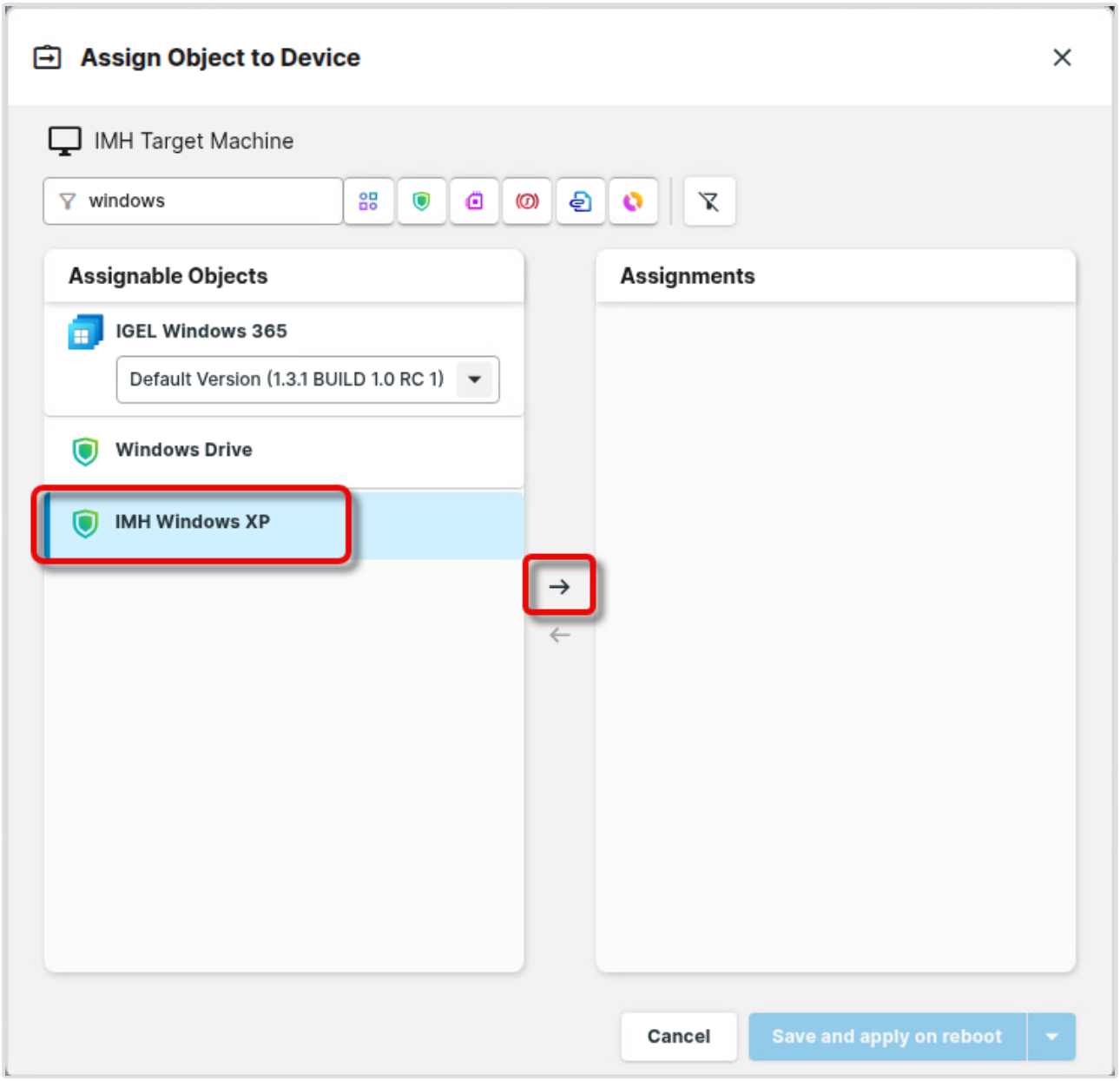
- **Name of the VM to connect to**: The name of the virtual machine you have created
- **Icon large**: By default, a generic icon will be used as the start icon. You can add the path to a custom icon
- **Kiosk Mode**: If enabled, the user views the virtual machine in full-screen mode with limited controls, allowing interaction only with the VM itself. The viewer automatically connects to the specified virtual machine on startup..

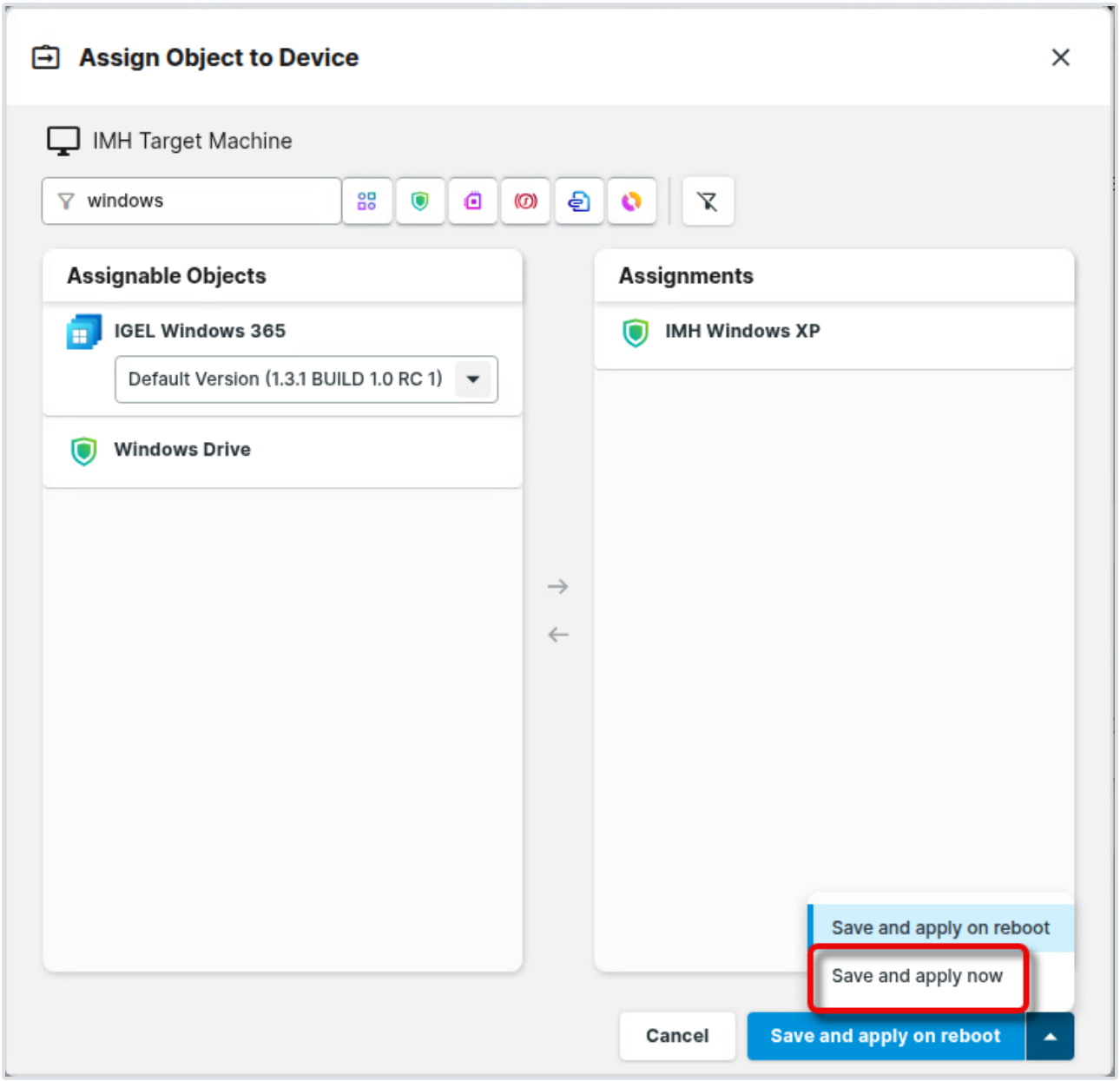


7. Go to **Devices**, select your target machine, and click **Assign Object**.



8. Find and select your profile and assign it to your device.

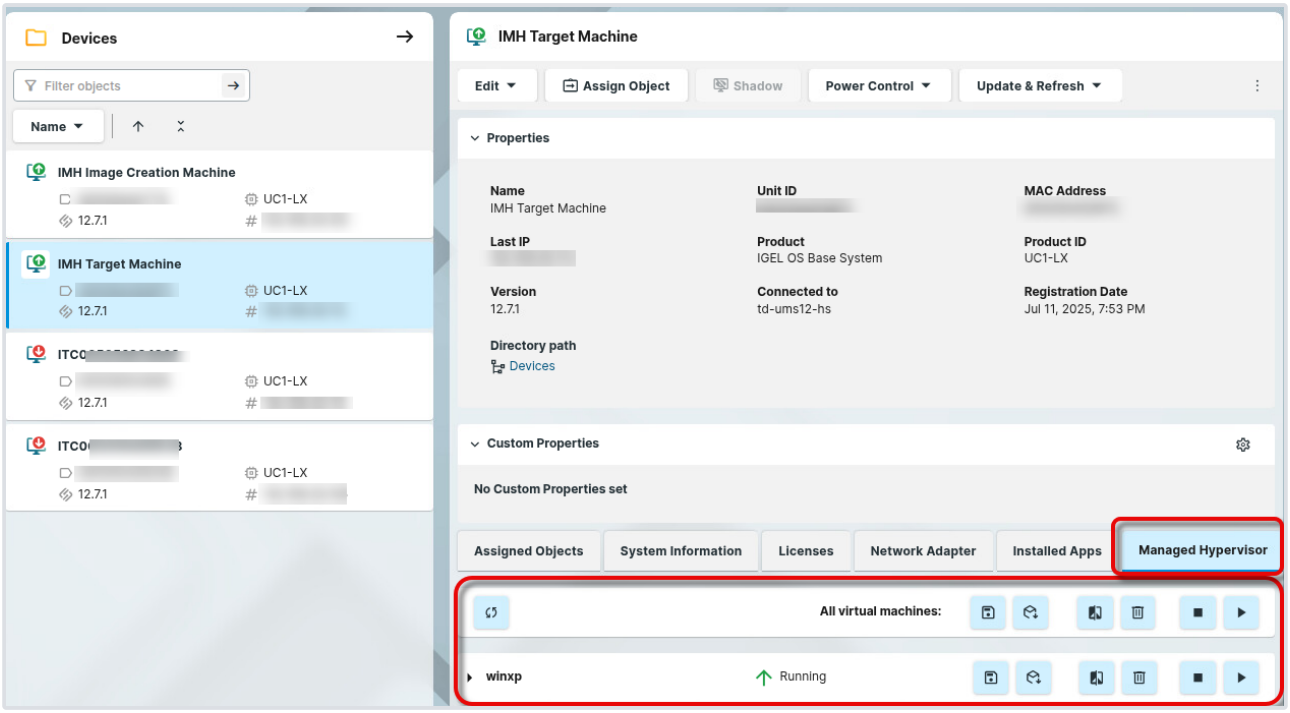

Assign Object to Device
IMH Target Machine
windows
Assignable Objects
IGEL Windows 365
Default Version (1.3.1 BUILD 1.0 RC 1)
Windows Drive
IMH Windows XP
Assignments
Cancel
Save and apply on reboot



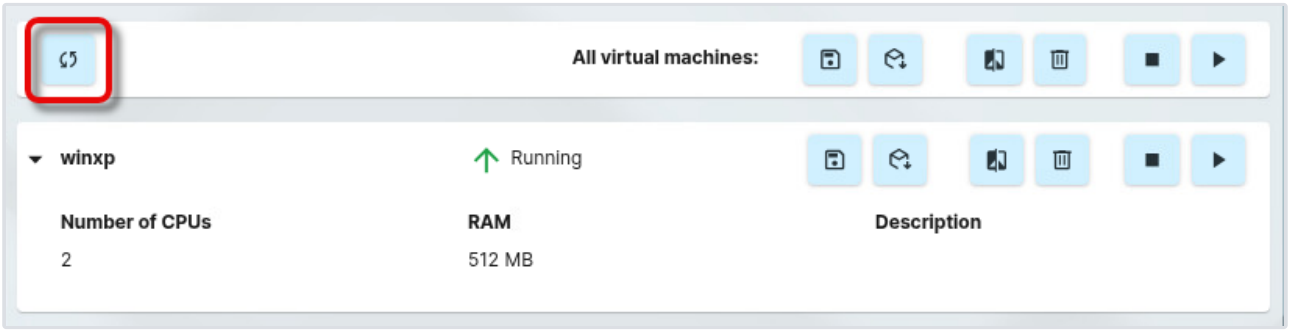
When the profile is applied, the device downloads and installs the IGEL Managed Hypervisor app. Afterward, it downloads the virtual machine from the WebDAV repository. You can now access, start, and stop the virtual machine via the start icon.

Managing the Virtual Machine via the Universal Management Suite (UMS)

When the target device has received the virtual machine and restarted, a new tab labeled **Managed Hypervisor** is added.



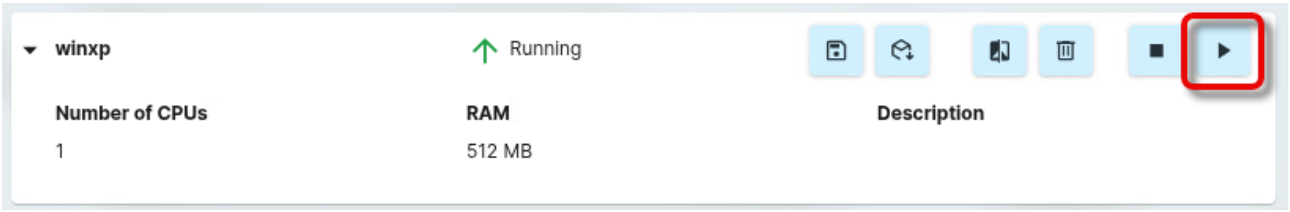
→ Click the refresh button to determine the current status of your virtual machines.



The available possibilities of managing virtual machines on endpoint devices are described below.

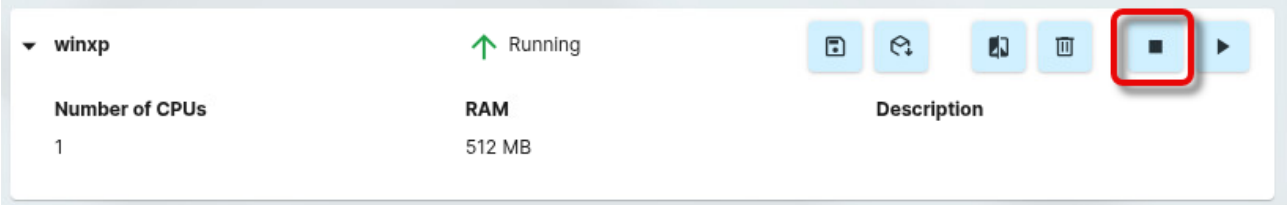
Starting a Virtual Machine

→ To start a virtual machine, click ▶.



Stopping a Virtual Machine

→ To stop a virtual machine, click ■ .

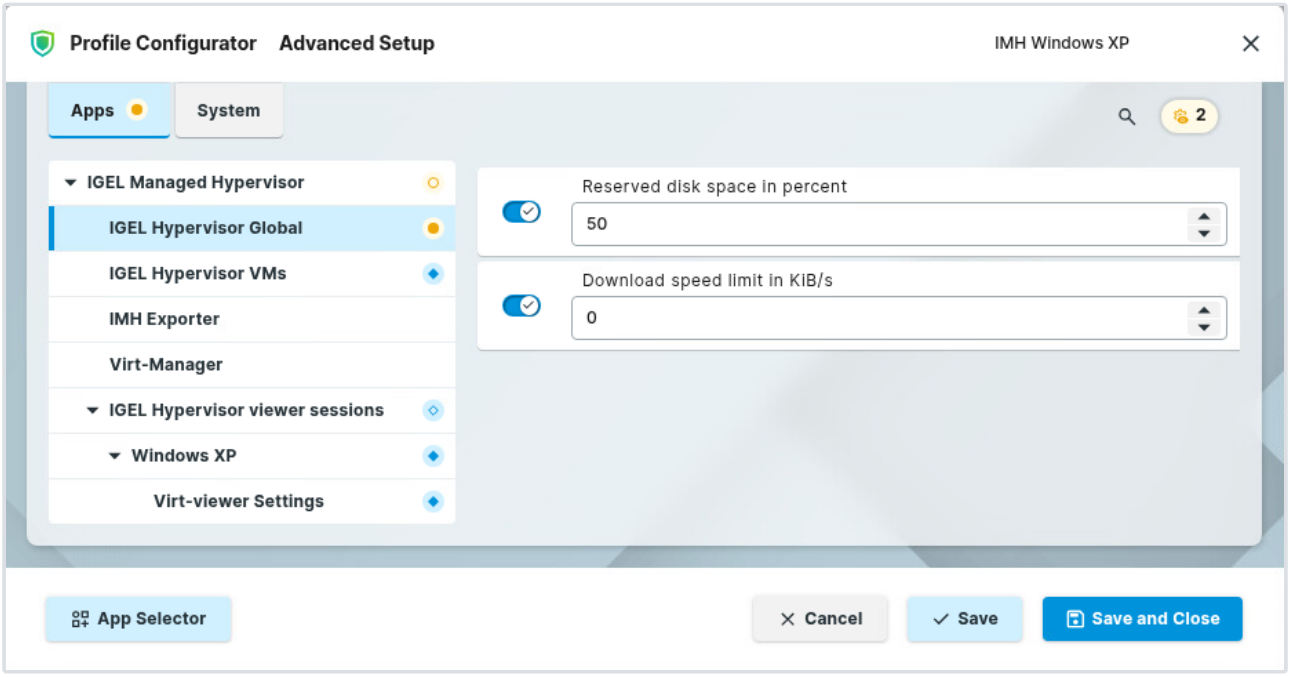


Reconfiguring IGEL Managed Hypervisor

Image Creation Machine

Configuring Reserved Disk Space and Download Speed

→ Open the **Apps** tab, go to **IGEL Managed Hypervisor > IGEL Hypervisor Global** and edit the settings according to your needs.



Reserved disk space in percent

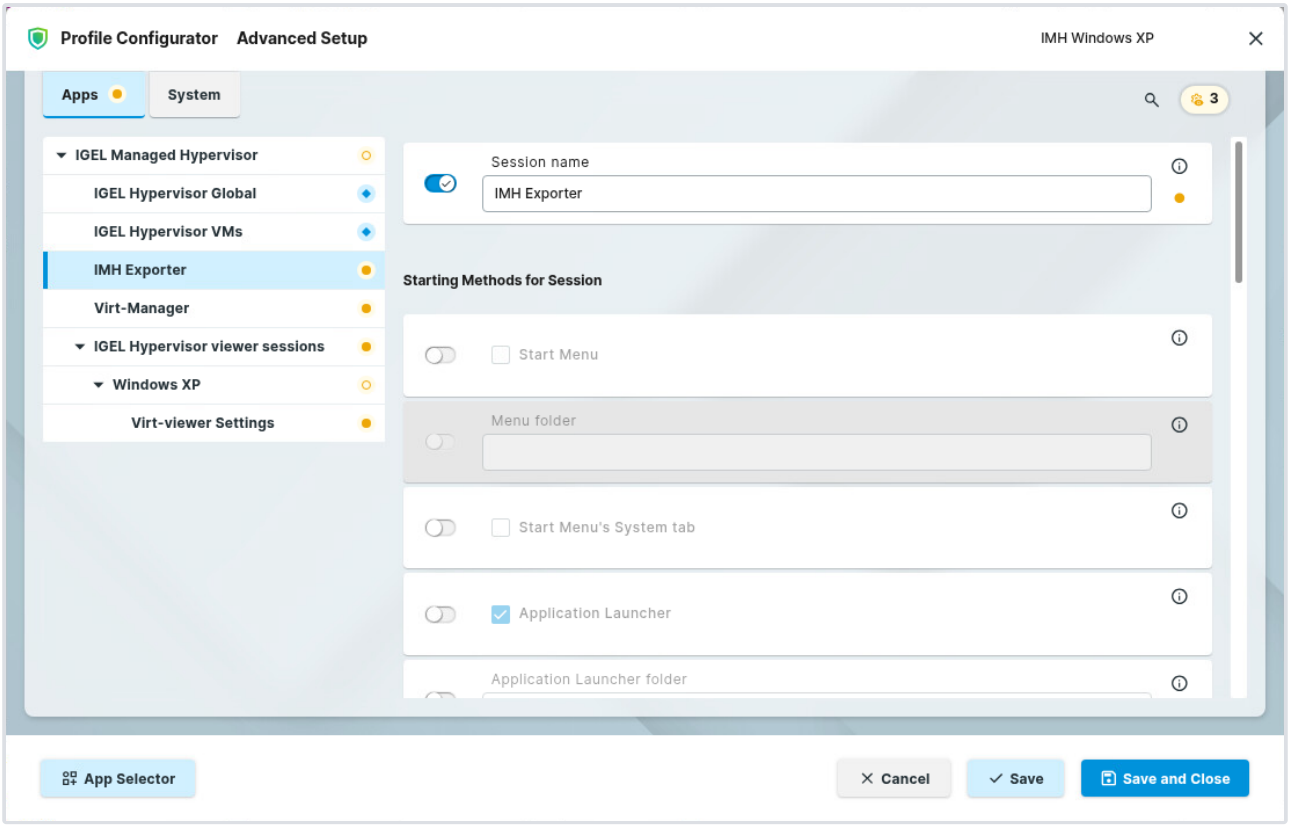
The proportion of the image creation machine's storage that is used for the virtual machine. Default: 50

Download speed limit in KiB/s

Speed limit for downloading the image file from the WebDAV server.

Configuring the Start Options for the IMH Exporter

→ Open the **Apps** tab, go to **IGEL Managed Hypervisor > IMS Exporter**, and edit the settings according to your needs.

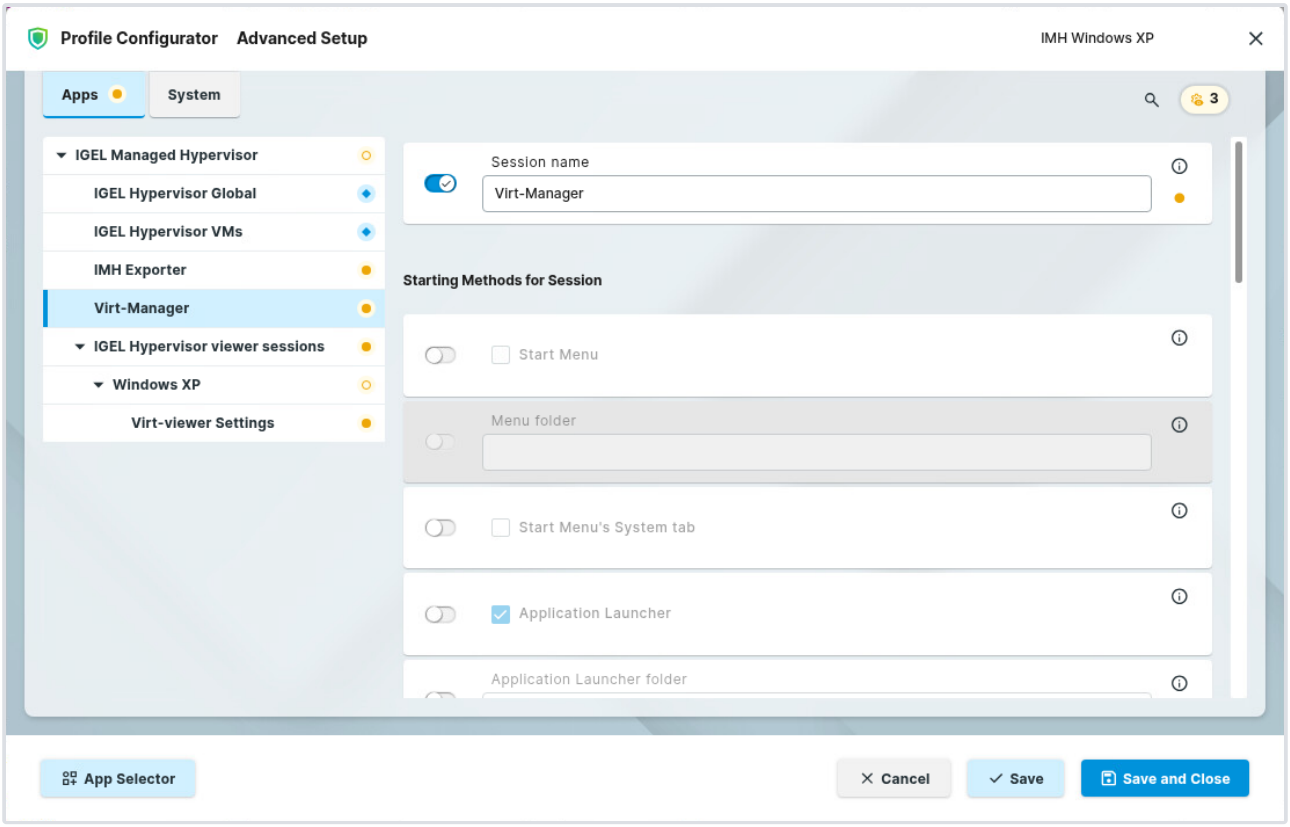


For detailed information on the start options, see Starting Methods for Apps[61].

Configuring the Start Options for the Virt-Manager

→ Open the **Apps** tab, go to **IGEL Managed Hypervisor > Virt-Manager**, and edit the settings according to your needs.

61. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps



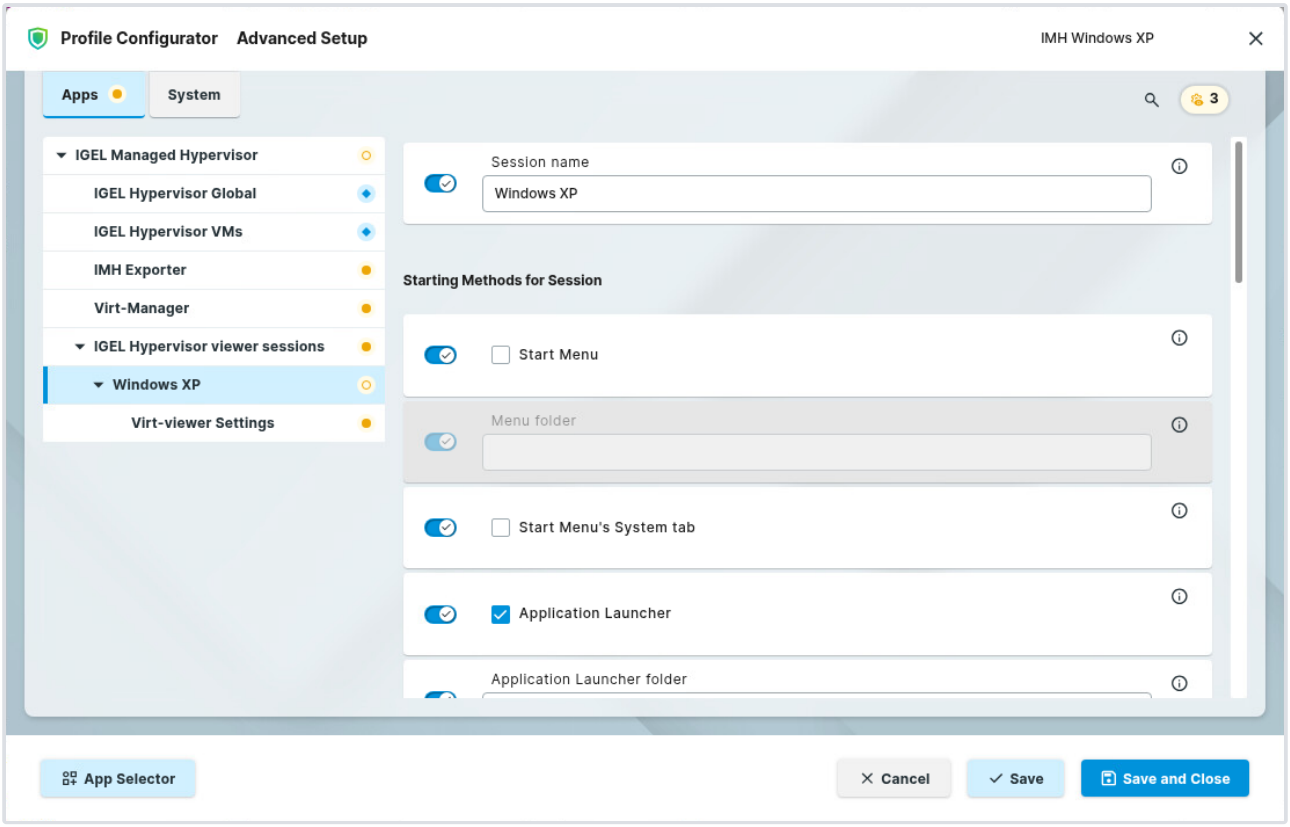
For detailed information on the start options, see Starting Methods for Apps[62].

Target Machines

Configuring the Start Options for the Virtual Machine

→ Open the **Apps** tab, go to **IGEL Managed Hypervisor > IGEL Hypervisor viewer sessions > [session name]**, and edit the settings according to your needs.

62. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

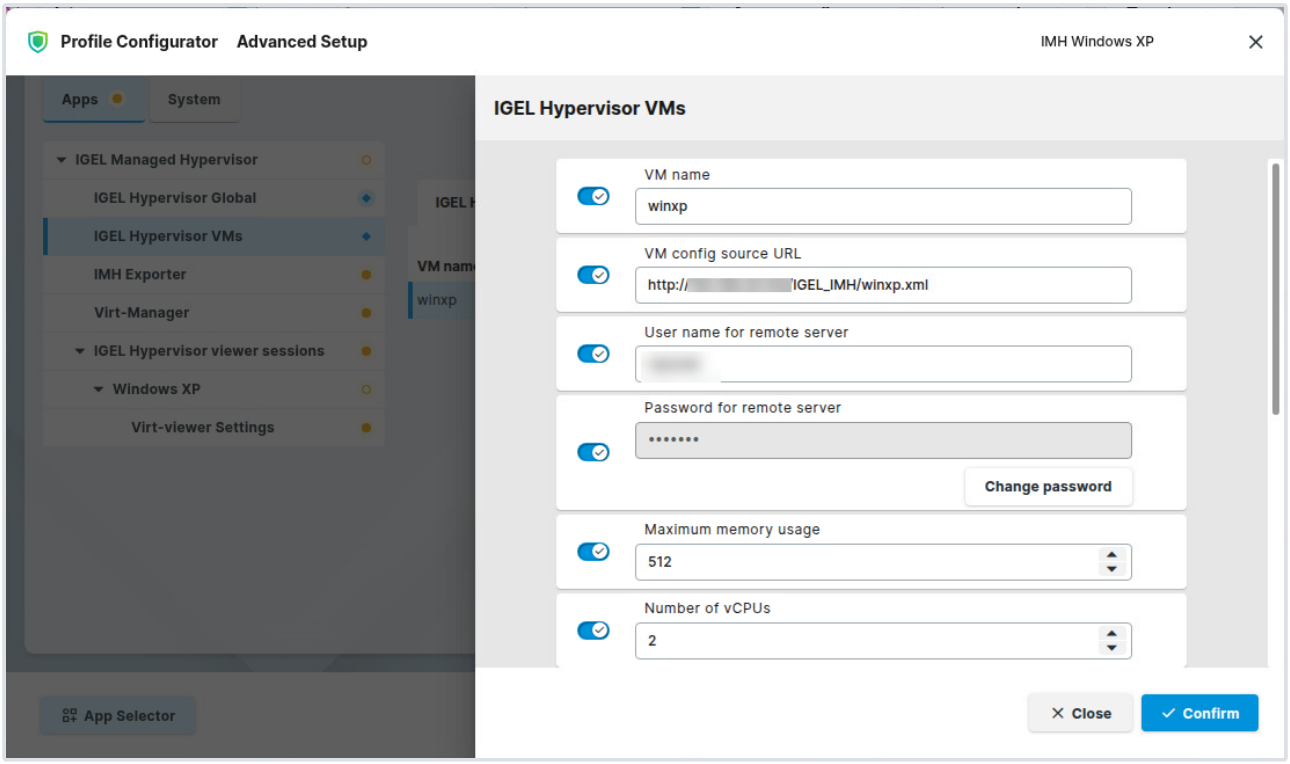


For detailed information on the start options, see Starting Methods for Apps[63].

Configuring the Virtual Machine

→ Open the **Apps** tab, go to **IGEL Managed Hypervisor > IGEL Hypervisor viewer sessions > [session name] > Virt-viewer Settings**, and edit the settings according to your needs.

63. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps



VM name

The name of the virtual machine you have created

VM config source URL

The URL of the XML file you have exported

User name for remote server

The username for read access to the WebDAV repository

Password for remote server

The password associated with the username

Maximum memory usage

The maximum memory (RAM) used by the virtual machine

Number of vCPUs

The number of virtual CPUs

Autostart

- ☑ The virtual machine will be started automatically.
- ☐ The virtual machine will only start if the user starts the session. (Default)

Disk Image is immutable

- ☑ Changes in the virtual machine will be gone when it is restarted.
- ☐ Changes in the virtual machine will persist after a restart. (Default)

MAC address for virtual interface

You can specify the MAC address of your virtual machine's network interface. This is useful if the software in your virtual machine is licensed for a specific MAC address.

Type of network for this VM

The following networks are supported on the target machines:

- **isolated**: The network interface is deactivated in the virtual machine.
- **NAT**: Network Address Translation (NAT) is used; the host machine translates the internal IP address of the virtual machine to its own IP address.
- **bridged**: The network device specified in **Network device used for this VM. Will be ignored for some pre-configured bridge devices** is used.
- **hostonly**: The preconfigured hostonly bridge is used.
- **macvtap**: The network device specified in **Network device used for this VM. Will be ignored for some pre-configured bridge devices** is used with the macvtap driver.

Network device used for this VM. Will be ignored for some pre-configured bridge devices

1. Create a network interface by setting the Registry key **network.interfaces.ethernet.device<NUMBER>.bridge** (**System** tab **> Registry > network > interfaces > ethernet > device<NUMBER>.bridge** to **own**). Example: If the setting has been made for device0, the network interface will be `breth0`.
2. Enter the resulting name in this field.

IGEL Secure Kiosk App

In the following article, you will learn how to configure the IGEL Secure Kiosk App. The app allows organizations to deliver web-based applications safely, using a hardened configuration with minimal user interaction and strong control for administrators.

With the IGEL Secure Kiosk App, any web page whitelisted by the administrator is opened in a fully locked-down, kiosk-like mode. There are no standard browser menus, no shortcuts, and no right-clicking possibilities. The browser is controlled by a fully customizable toolbar with buttons for navigation, printing, or custom commands. Strong control over the allowed websites and browser options makes the app ideal for public kiosks and secure enterprise terminals.

The IGEL Secure Kiosk app is always displayed in full-screen mode, even if multiple monitors are used.

To authenticate the app, you can provide a client certificate.

Requirements

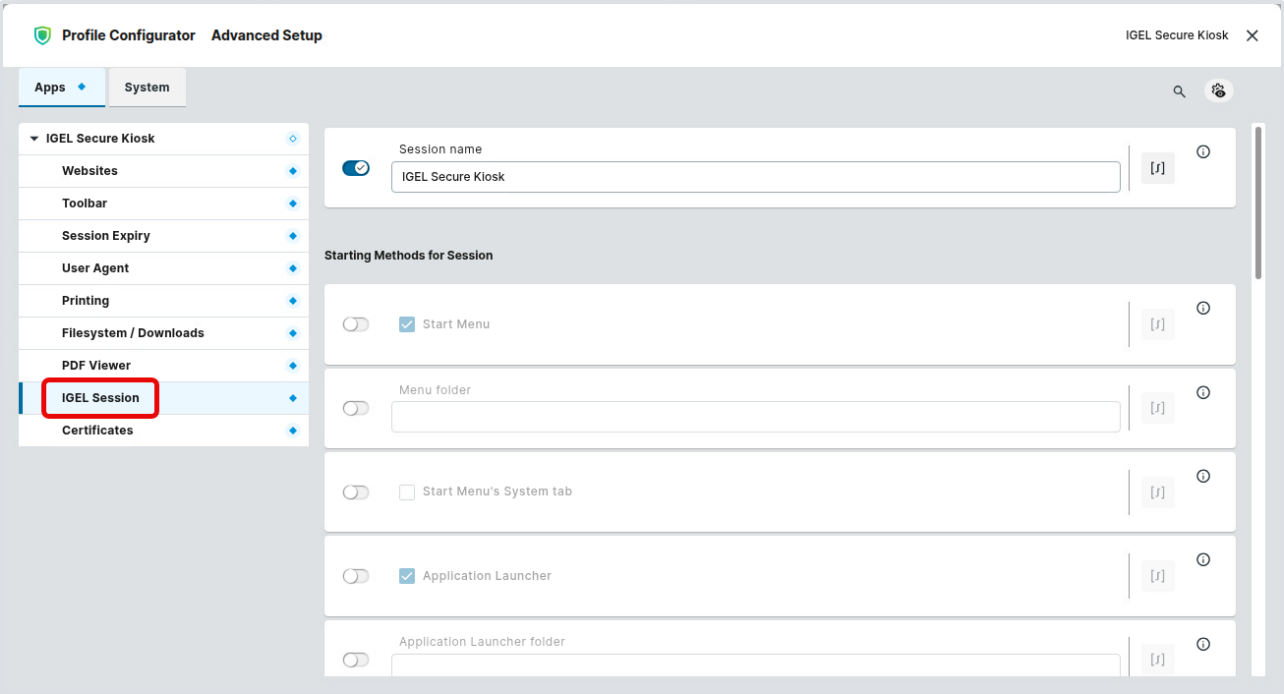
- IGEL OS Base System 12.7.4 or higher
- The IGEL Secure Kiosk app is imported to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[64].
- Highly recommended: Virtual console access should be disabled. Follow the instructions under Disabling Virtual Console Access[65] and reboot the device afterward.

How to Configure IGEL Secure Kiosk App

1. In the IGEL UMS, create a profile that configures the IGEL Secure Kiosk app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[66].

2. In the profile configurator, go to **Apps > IGEL Secure Kiosk > IGEL Sessions** and define the required **Session name** and starting methods for the app (e. g. **Autostart** as a typical use case). The starting methods are described under Starting Methods for Apps[67].

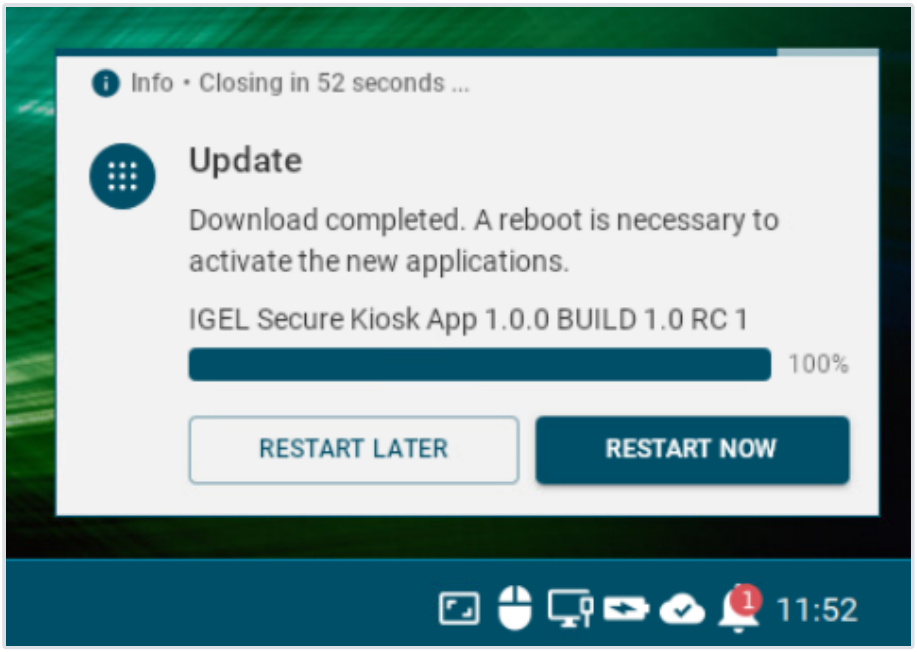
64. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
65. https://kb.igel.com/en/security-safety/current/disabling-virtual-console-access
66. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-
67. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps



3. Configure the settings described below.

4. Save the profile and assign it to the required devices. For details on profile assignment, see How to Create and Assign Profiles in the IGEL UMS Web App[68].
   The app will be downloaded and installed on the IGEL OS device.

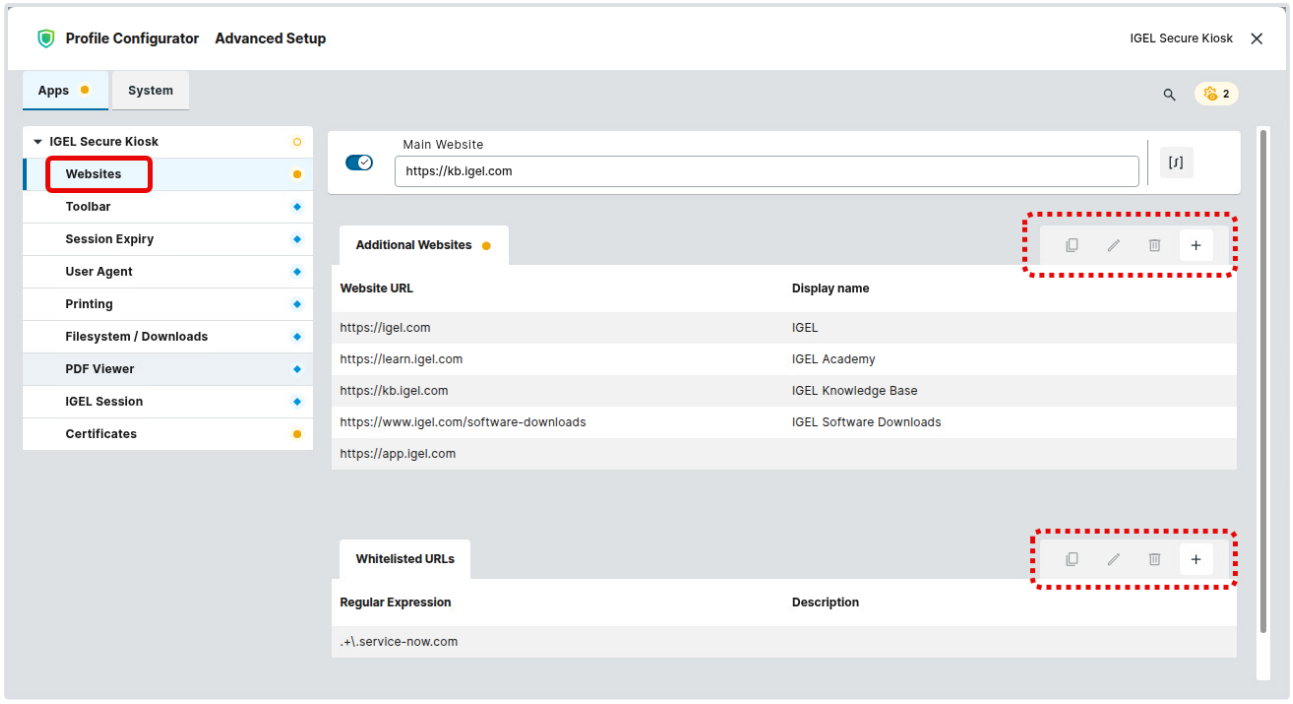
68. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



6. Reboot the device.

Configuring the Allowed Websites

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Websites**.



2. Configure the settings according to your requirements.

Main Website

URL of the website that should be opened initially.

Additional Websites

URLs of other websites that the end user is allowed to open. These websites will be opened when **Page Selector** is added as a toolbar element under **Apps > IGEL Secure Kiosk > Toolbar > Toolbar Items > Toolbar item type**.

To add a new entry:

1. Click +.
   The entry mask will be opened.



2. Specify **Website URL**.

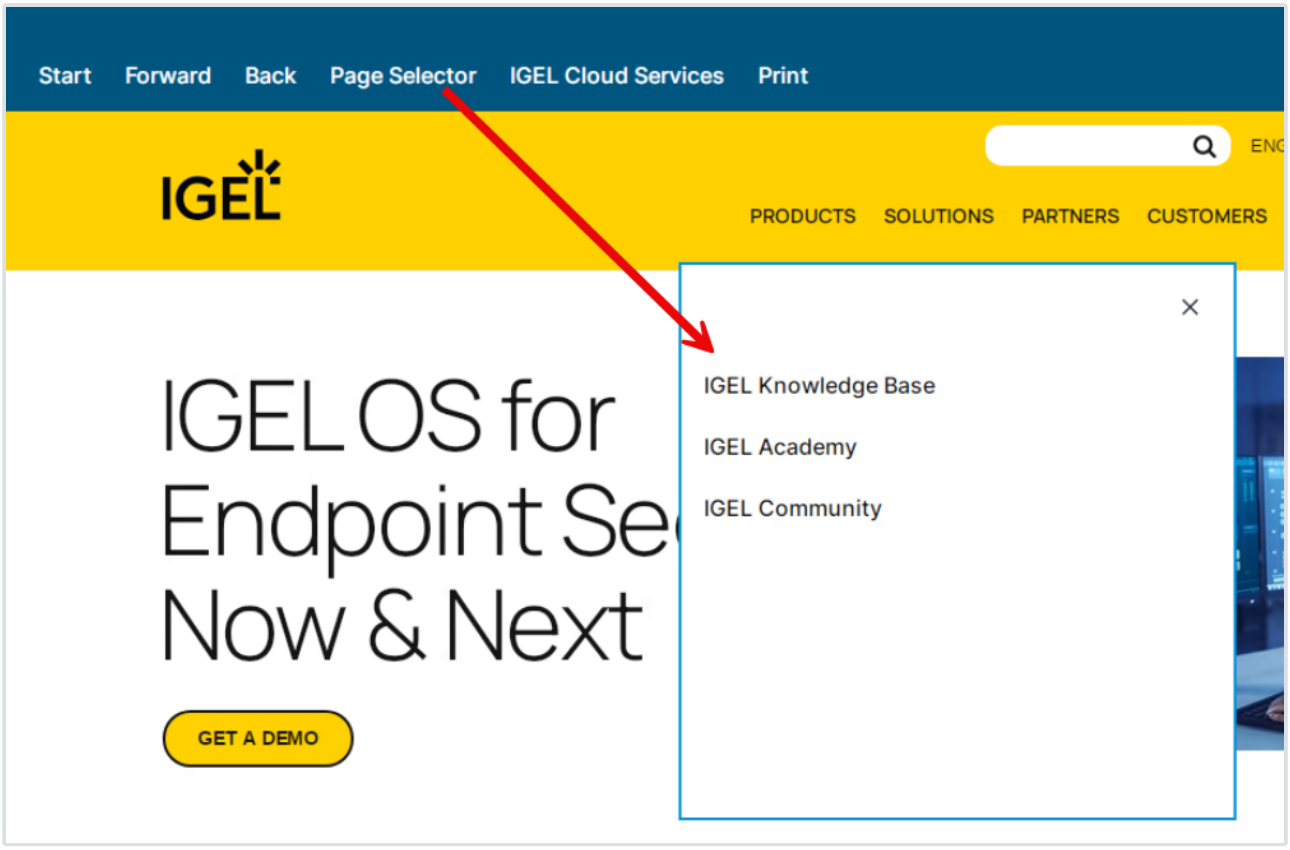
3. Specify **Display name**. If left empty, the **Website URL** will be displayed in the **Page Selector** (configured under **Apps > IGEL Secure Kiosk > Toolbar > Toolbar Items > Toolbar item type > Page Selector)**.

4. Click **Confirm** to save the settings.

To manage the list of additional allowed websites, proceed as follows:

- Click + to add a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Example of additionally allowed websites:

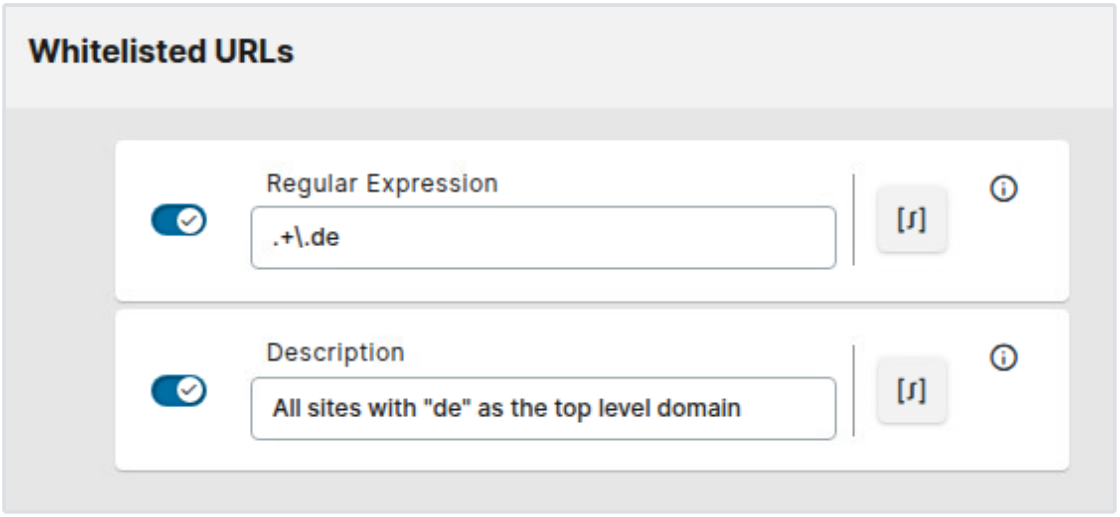


Whitelisted URLs

A list of domains, patterns, or concrete web addresses that are explicitly permitted to be accessed or processed by the system.

To add a new entry:

1. Click + and specify the following parameters:
   - **Regular Expression**: A pattern that represents the URLs you want to allow. The usual regular expressions can be used.
   - **Description**: A short text that describes the allowed URLs.



2. Click **Confirm** to save the settings.

To manage the list, proceed as follows:

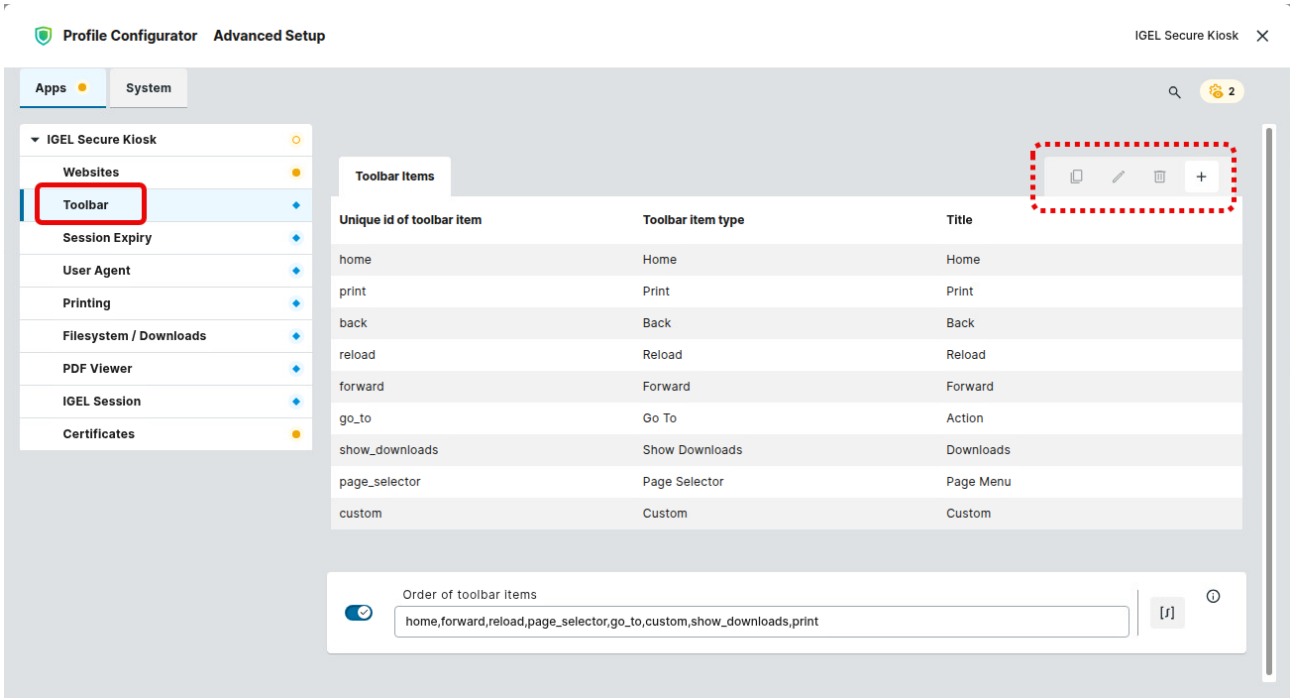
- Click + to add a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Configuring the Toolbar

You can populate the toolbar with GUI elements.

To configure the toolbar:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Toolbar**.



2. Configure the toolbar items and their order as described below.

To manage the toolbar items, proceed as follows:

- Click + to add a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

Home Button

This button loads the page defined under **Main Website**.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - “-”
  - “_”
- **Toolbar item type**: Select **Home**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.

- **Icon path** (optional): The file path to an icon for this toolbar item.

Reload Button

This button reloads the current page.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - "-"
  - "_"
- **Toolbar item type**: Select **Reload**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Back Button

This button loads the previous page in the page history, if applicable.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - "-"
  - "_"
- **Toolbar item type**: Select **Back**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Forward Button

This button loads the next page in the page history, if applicable.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - "-"
  - "_"
- **Toolbar item type**: Select **Forward**.

- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Print Button

This button prints the current page.

For details on printer configuration, see Configuring Printing (see page 195).

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - "-"
  - "_"
- **Toolbar item type**: Select **Forward**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Page Selector

This button adds a menu with the pages configured in **Websites > Additional Websites**.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide an identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - "-"
  - "_"
- **Toolbar item type**: Select **Page Selector**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Go To Button

This button can load a specific target URL, clear the browser cache, or execute a configurable command or script. Please note that a target URL must be defined for this type of toolbar item; if you need a button to clear the browser cache, or execute a configurable command or script without loading a target URL, check out the Custom Button (see page 191).

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - “-”
  - “_”
- **Toolbar item type**: Select **Page Selector**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.
- **Target URL**: The URL that will be loaded when the user clicks the button.
- **Clear browser data**: If enabled, the browser cache will be cleared when the user clicks the button.
- **Command to execute**: The command that will be executed when the user clicks the button. The full absolute path must be provided. Example for test purposes: `/usr/bin/notify-send ‘Message’ 'You are in the kiosk'`

Show Downloads Button

This button opens a list of files downloaded to the device.

For configuration details on downloads, see Configuring Downloads and Filesystem Access (see page 196).

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - “-”
  - “_”
- **Toolbar item type**: Select **Show Downloads**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

Custom Button

This button executes a configurable command or script.

→ Edit the parameters according to your needs:

- **Unique id of toolbar item**: Provide a unique identifier for this toolbar item. Allowed characters:
  - letters
  - numbers
  - “-”
  - “_”
- **Toolbar item type**: Select **Custom**.
- **Title**: Provide a title that contains at least one non-whitespace character.
- **Tooltip** (optional): A hint for the user that explains the function of this toolbar item.
- **Icon path** (optional): The file path to an icon for this toolbar item.

- **Clear browser data**: If enabled, the browser cache will be cleared when the user clicks the button.
- **Command to execute**: This command is executed when the user clicks the button. The full absolute path must be provided. Example for test purposes: `/usr/bin/notify-send 'Message' 'You are in the kiosk'`

Order of Toolbar Items

You can define the order of the toolbar items by creating a comma-separated list of their unique identifiers.

Example: `home,forward,reload,page_selector,go_to,custom,show_downloads,print`

Configuring the Session Expiry

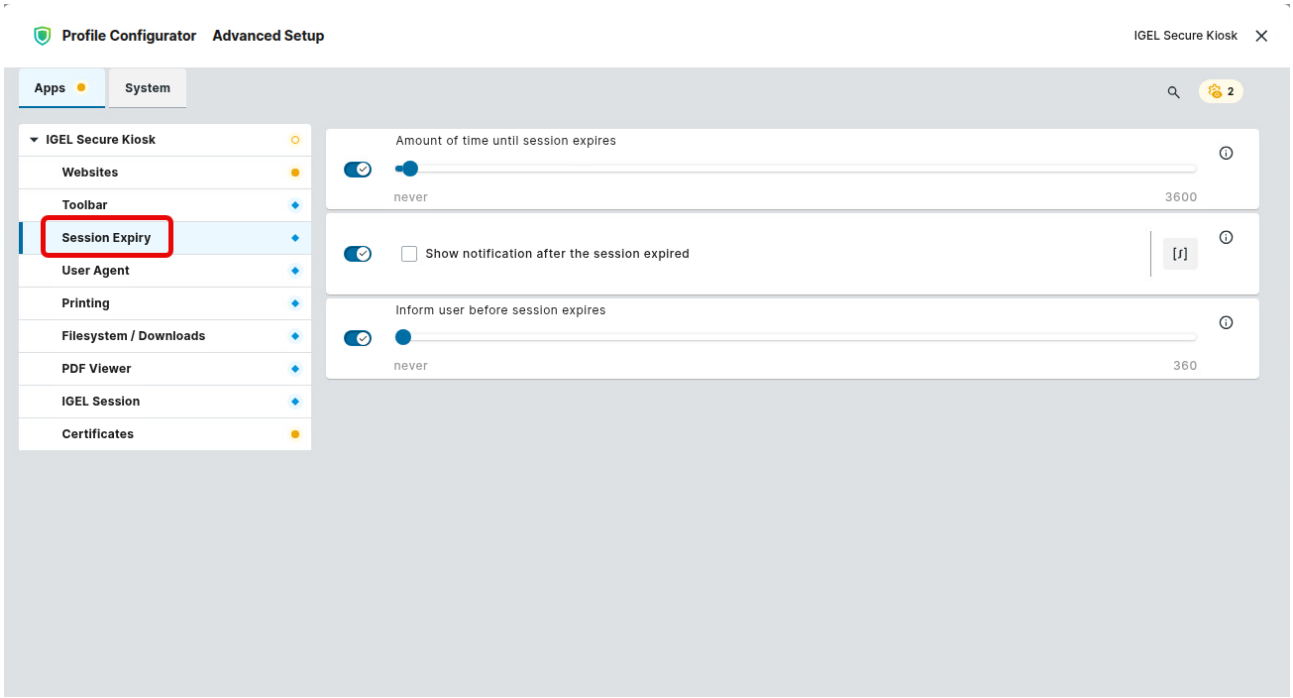
You can define if and when an IGEL Secure Kiosk App session expires, and if the user is notified.

When a session expires, the following happens:

- The browser returns to the start page (**Main Website**).
- The browser data is cleared.
- The download folder is cleared.

To configure the session expiry:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Session Expiry**.



2. Configure the details as described below.

Amount of time until session expires

Sets an idle timeout in seconds. When there has been no user interaction during the specified time, the IGEL Secure Kiosk session expires.

Value range: never (0) … 3600

Show notification after the session expired

☑ A notification is shown when the session has expired.

Inform user before session expires

Defines how many seconds before session expiry a notification is shown.

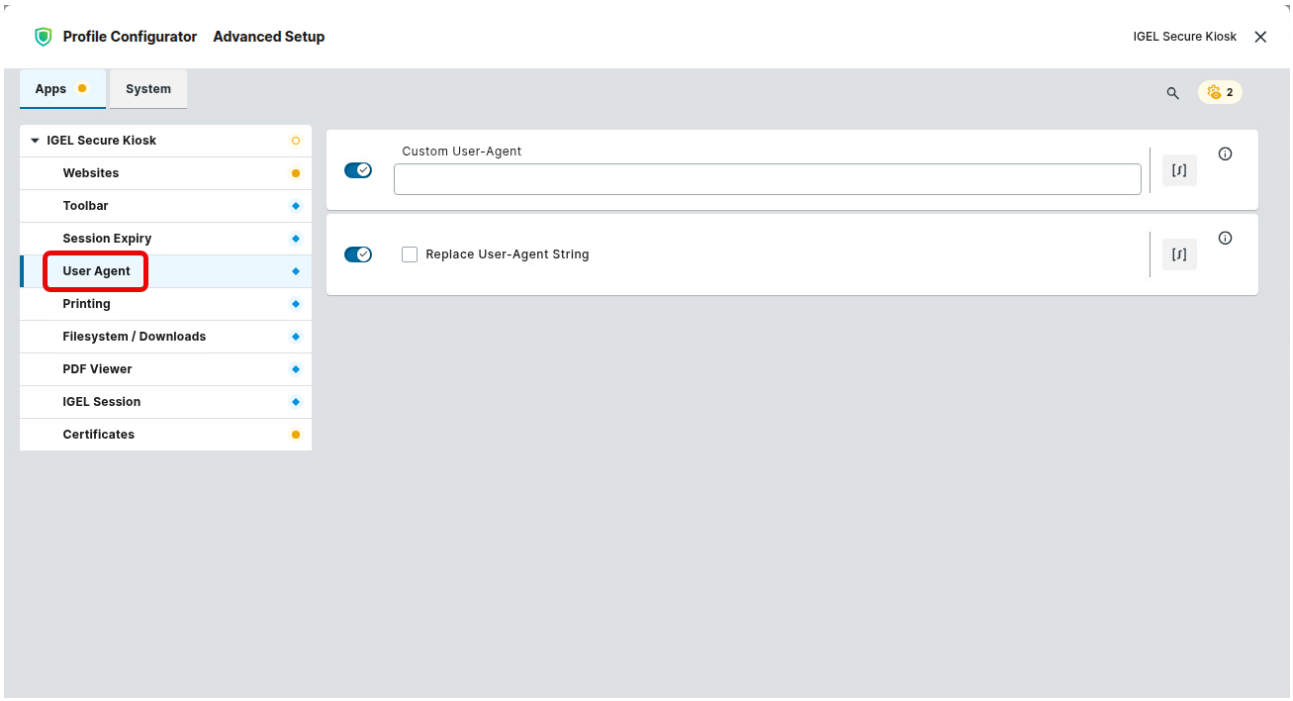
Value range: never … 360

Configuring the User Agent

You can edit the user-agent string that the app will send with its HTTP requests. You can choose between adding a custom user-agent string to the predefined user-agent string and replacing the predefined user-agent string with the custom user-agent string.

To configure the session expiry:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > User Agent**.



2. Configure the details as described below.

User Agent

You can edit the user-agent string that the app will send with its HTTP requests. Please note the requirements below.

- The user-agent string must have at least one PRODUCT.
- Each PRODUCT consists of a NAME, an optional VERSION, and zero or more optional COMMENTs.
- For the Name, the following characters are allowed: `!` / `#` / `$` / `%` / `&` / `'` / `*` / `+` / `-` / `.` / `^` / `_` / `` ` `` / `|` / `~` / DIGIT / ALPHA
- For the COMMENT, the following characters are allowed: `!` / `#` / `$` / `%` / `&` / `'` / `*` / `+` / `-` / `.` / `^` / `_` / `` ` `` / `|` / `~` / `=` / “ / DIGIT / ALPHA
- Examples of valid user-agent strings:
  - One product: `Mozilla`
  - One product with version: `Mozilla/5.0`
  - One product with version and comment: `Mozilla/5.0 (info=1)`
  - Several products: `Mozilla Gecko/1.0 MyBrowser/1234 (additional info)`

Replace User-Agent String

- ☐ The custom user-agent string is added to the predefined user-agent string. (Default)
- ☑ The custom user-agent string replaces the predefined user-agent string.

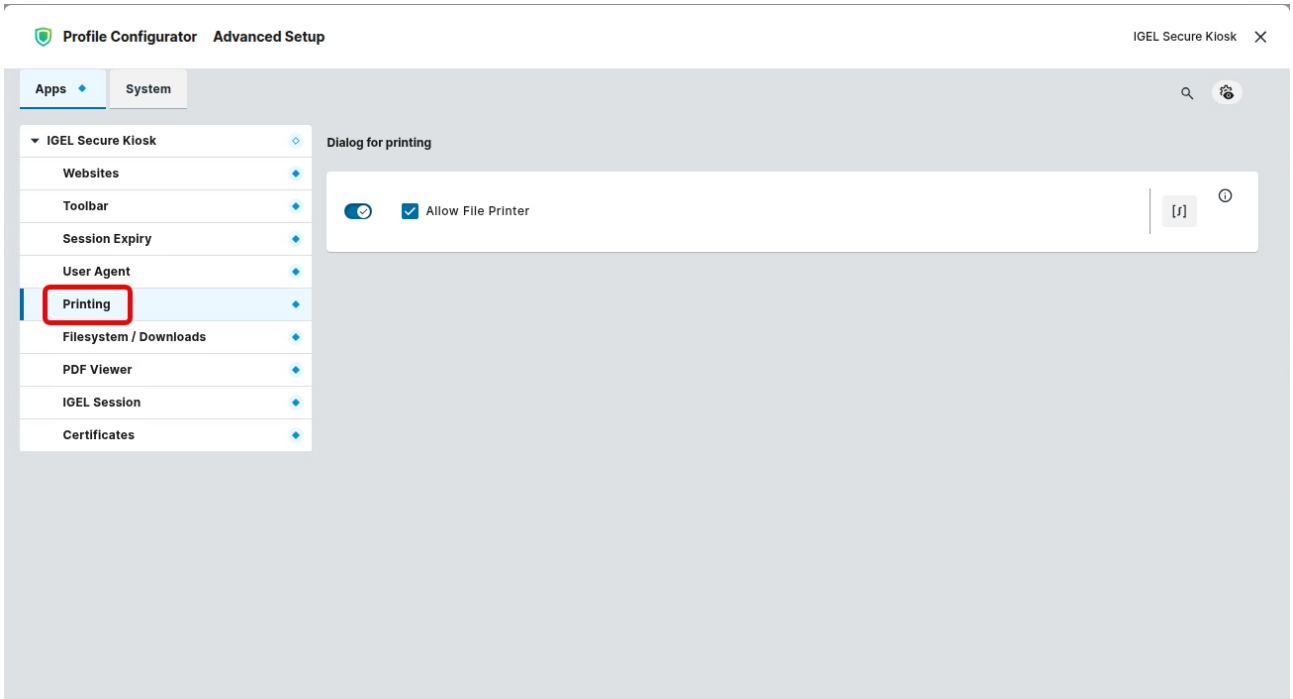
Configuring Printing

> For all printing functions except printing to a file, the **CUPS printing app** must be installed, and a printer must be set up. For details, see CUPS printing app[69].

You can select the printer to be used, enable or disable the printing dialog, and set printing parameters.

To configure printing:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Printing**.



69. https://kb.igel.com/en/igel-apps/current/cups-printing-app

2. Configure the details as described below.

Allow File Printer

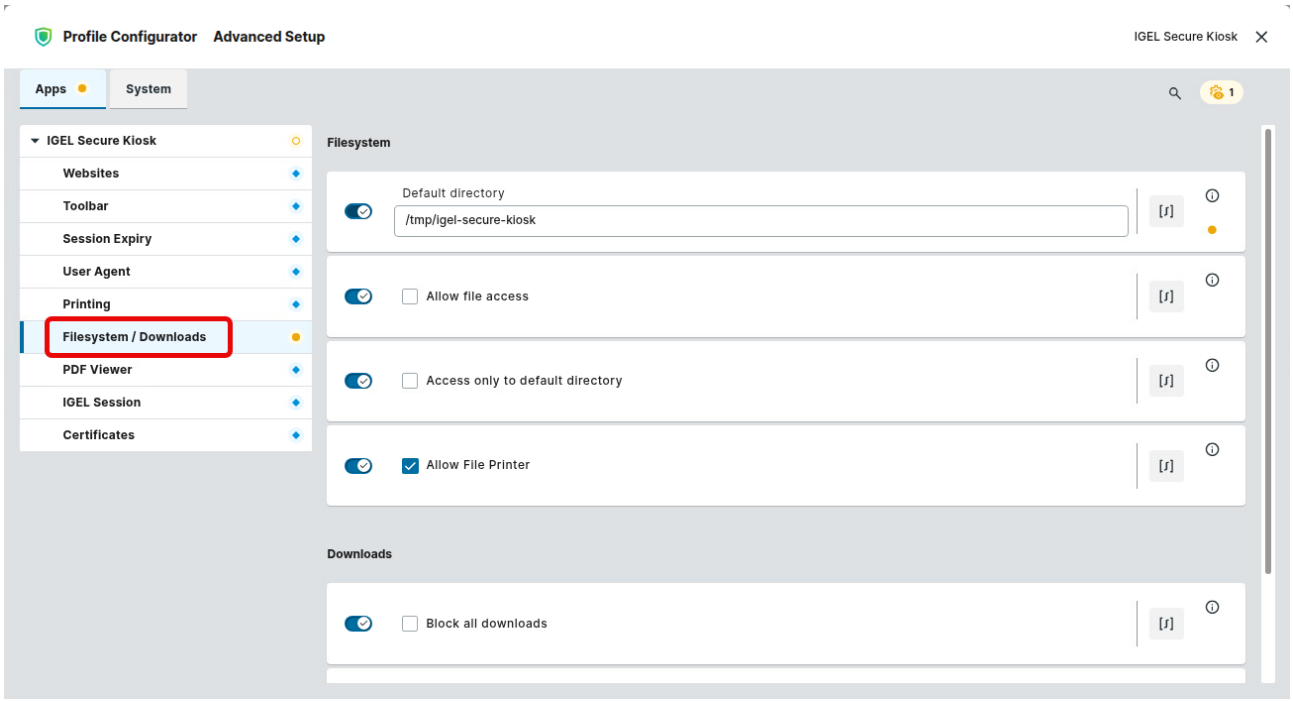
☑ The user can print to a PDF file. The user can view the file via the **Show Downloads** button.

Configuring Downloads and Filesystem Access

You can configure whether downloads and PDFs from a file print are allowed and where they are stored. Also, you can allow, restrict, or disallow user access to stored files.

To configure downloads:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Filesystem / Downloads**.



2. Configure the details as described below.

Default directory

The directory on the device's file system to which files are downloaded and PDF files are printed. This field must be filled in. Please note that only absolute paths are allowed. Default: `/tmp/igel-secure-kiosk`

Allow file access

To enable the user to upload files to a web page or to view local files with the PDF viewer, this option must be activated.

- [x] The user can see files on the device's file system.
- [ ] Files on the device's file system cannot be viewed. (Default)

Access only to default directory

When the user opens a web page with an upload button or a PDF document, the contents of the default directory are available in a file chooser. This parameter determines whether the file chooser allows the user to access other directories.

- [x] The user can only access files located in the default directory. (Default)
- [ ] The user can change to other directories.

Allow File Printer

- [x] The user can print to a PDF file. The user can view the file via the **Show Downloads** button.

Block all downloads

- [x] No files can be downloaded.
- [ ] All files that are specified under **Allowed file extensions for download** can be downloaded. (Default)

Allowed file extensions for download

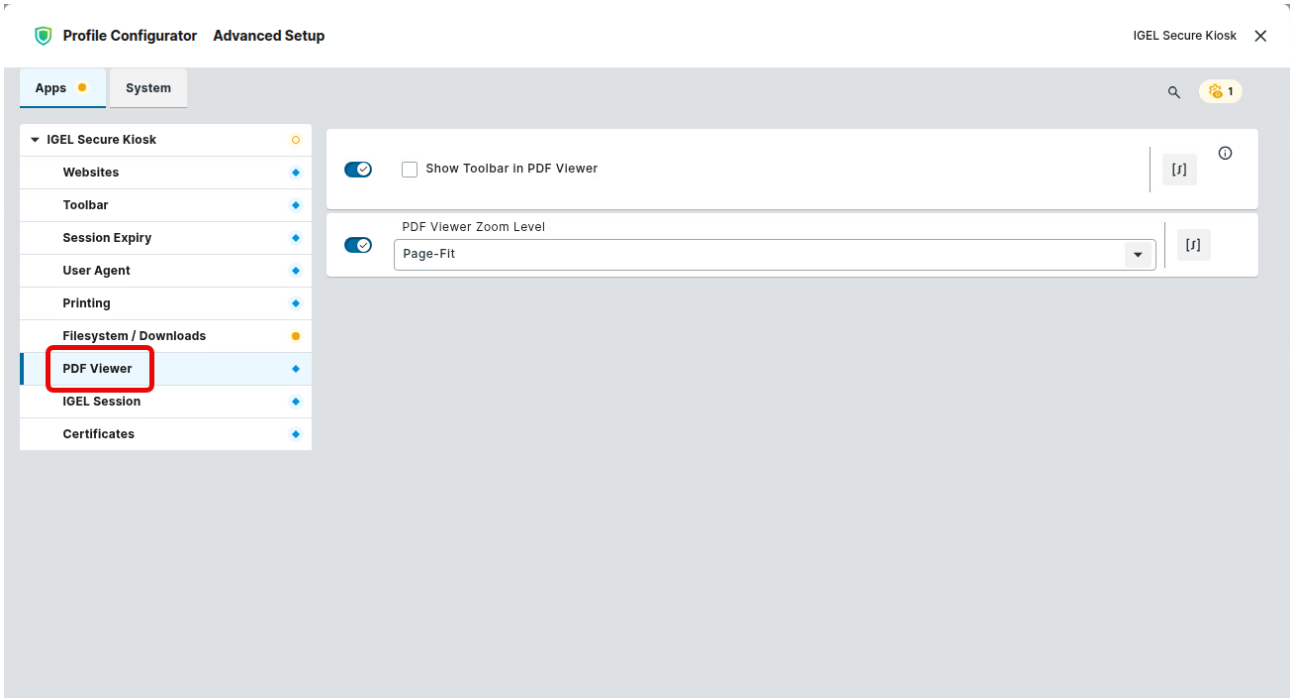
Enter a comma-separated list of allowed file extensions. Example: `.txt,.pdf,.zip`

Configuring the PDF Viewer

You can configure the appearance of the built-in PDF viewer.

To configure the PDF viewer:

1. In the profile configurator, go to **Apps > IGEL Secure Kiosk > PDF Viewer**.



2. Configure the details as described below.

Show Toolbar in PDF Viewer

With the toolbar, the user can adjust the display of pages, like zooming in and out.

- ☑ The toolbar of the PDF viewer is shown.
- ☐ The toolbar is hidden. (Default)

PDF Viewer Zoom Level

Defines the size in which a document is displayed.

Possible values:

- **Page-Fit**: The size is adjusted so that a complete page fits on the available space.

- **Page-Height**: The size is adjusted so that the page height matches the height of the available space.
- **Page-Width**: The size is adjusted so that the page width matches the width of the available space.
- **50%** … **200%**

Installing a Client Certificate

To authenticate the IGEL Secure Kiosk app with a server, you can install a client certificate on your device. Certificate files in the PKCS#12 format are supported.

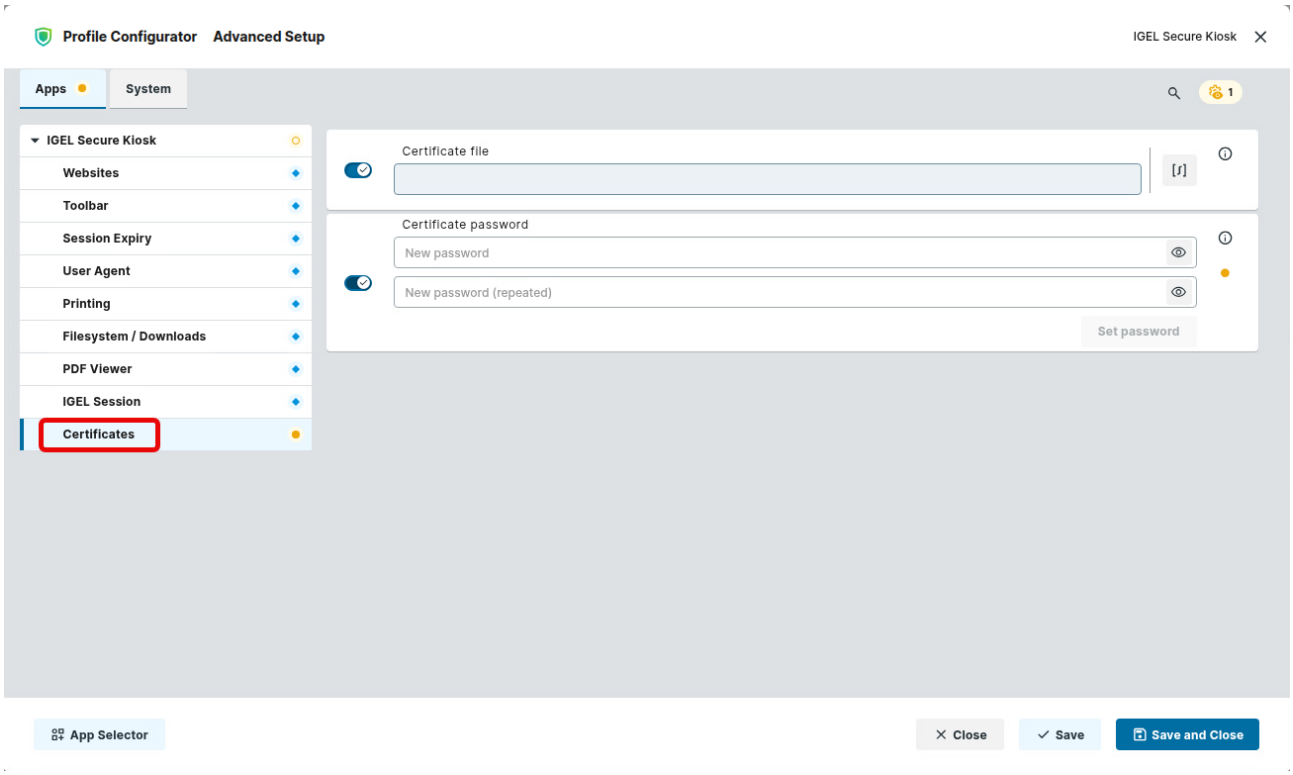
Ensure that the certificate file meets the following requirements:

- File extension: `.p12` or `.pfx`
- Compatible with SSL 3.0 or higher

To install a certificate:

1. Transfer the file to the devices using UMS file transfer. For this purpose, follow the instructions in Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices[70], using the following settings:
   - Set **Classification to Undefined**. This allows you to define the file path yourself.
   - Ensure the **Owner** has **Read**, **Write**, and **Execute** permissions.
   - Ensure the **Owner** is set to **User**.
2. In the profile configurator, go to **Apps > IGEL Secure Kiosk > Certificate**.

70. https://kb.igel.com/en/universal-management-suite/current/files-registering-files-on-the-igel-ums-server-and



3. Configure the details as described below.

Certificate file

Enter the file path you have specified for the file transfer in step 1.

Certificate password

The password for the certificate file.

IGEL Agent for Imprivata



- Introduction (see page 202)
- IGEL Agent for Imprivata (IAFI) Configuration Guide (see page 239)
- IGEL Agent for Imprivata (IAFI) Articles (see page 271)

Introduction

IGEL Agent for Imprivata (IAFI) Overview

IGEL has been an Imprivata technology partner since 2011. Our partnership has empowered tens of thousands of healthcare users globally to achieve secure, quick and easy access to clinical virtual applications and desktops using IGEL OS powered endpoints and the Imprivata ProveID Embedded (PIE) agent for Linux devices.

In September 2022, we expanded our partnership to develop a new ProveID Web agent that would deliver enhanced integrations, enable new workflows, and address evolving market and customer demands. A few examples of these market changes have been Windows 10 to 11 migrations, saving endpoint costs by repurposing existing devices and extending the life of their hardware, the adoption of Cloud delivered desktops or applications such as Microsoft Azure Virtual Desktop (AVD), and the rise of ransomware attacks and a desire for a more secure endpoint OS to help mitigate these threats.

Key Differences Between PIE and IAFI

The IGEL Agent for Imprivata (IAFI) is our implementation for various Imprivata Enterprise Access Management (formerly called OneSign and ConfirmID) related workflows. IAFI is available as an IGEL OS 12 application from the IGEL App Portal[71]. Some older OS 11 firmware versions have the agent but all the latest IAFI versions with updated features, enhancements and fixes are in the OS 12 app. Please see this for additional information: IAFI - IGEL System Requirements[72]

Appliance Mode vs. Non-Appliance Mode Agent

Since our initial integration with the Imprivata PIE Agent, it has only been available as a feature in the IGEL Appliance Mode (OS 11 and older versions). In Appliance Mode, PIE users are unable to access the local IGEL OS desktop and can only connect to virtualized desktops and apps supported by Imprivata. The list of supported features and workflows is maintained by Imprivata on their website which can be accessed here: Imprivata Enterprise Access Management - SSO Supported Components[73]. The IGEL KB for OS 11 and Imprivata can be accessed here: OS 11 and Imprivata Setup[74]

In contrast, due to high customer demand for options such as access to the IGEL local desktop and underlying OS features, the IAFI was created as a "**non-appliance mode**" option which by design, allowed full access (if needed) to the IGEL OS Desktop and new workflows previously unavailable with the PIE agent. During the initial IAFI development, OS 11 was the only available option for testing, and with a limited feature set, we chose to create a license to enable the use of the agent during the beta and customer early access phase. We also required a workflow review and use case validation before providing licenses for customer testing or production use.

While the IAFI initial feature set was limited, it has since grown and is maintained by IGEL in cooperation with Imprivata. You can review the current IAFI Feature Matrix here: IGEL Agent for Imprivata (IAFI) Feature Comparison Matrix[75]

71. https://app.igel.com/
72. https://kb.igel.com/en/igel-apps/current/iafi-igel-system-requirements
73. https://docs.imprivata.com/supported/content/topics/ossupportedcomponents.html#Endpoint2
74. https://kb.igel.com/en/igel-os/11.10.270/imprivata-1
75. https://kb.igel.com/en/igel-apps/current/igel-agent-for-imprivata-iafi-feature-matrix-compa

Summary of IGEL and Imprivata Agent Options for OS 11 and 12

Imprivata ProveID Embedded - PIE Agent	IGEL Agent for Imprivata
Built and maintained by Imprivata	Built and maintained by IGEL
IGEL OS 11: Appliance Mode only experience • No IGEL local desktop access or the ability to easily access other applications or utilities within the IGEL OS 11 firmware.	Non-Appliance Mode experience for OS 12 • Allows IGEL local desktop access
Uses the Imprivata ProveID Web API • Requires Imprivata VDA licensing • Imprivata and IGEL OS Version dependencies	Uses the Imprivata ProveID Web API • Requires Imprivata VDA licensing for some workflows • Backward compatible with older Imprivata versions (7.10 or higher)
The PIE Agent is downloaded from the Imprivata appliance and installed on IGEL OS 11 via an embedded bootloader.	OS 12 agent built as a separate application under the new OS 12 app delivery model.
Supported workflows, authentication devices, use cases, and roadmap developed by Imprivata. See the Imprivata Supported Configurations Guide[76] for more information.	Supported workflows, use cases, and roadmap developed by IGEL. See IGEL Agent for Imprivata Feature Matrix (see page 206) for further details.
Not supported for IGEL OS 12	OS 12 app available in the IGEL App Portal[77]

76. https://docs.imprivata.com/supported/content/topics/ossupportedcomponents.html
77. https://app.igel.com/

IAFI Workflow Configuration Options

Four IAFI configuration options are available based on the required Imprivata workflow used on the IGEL endpoint.

Follow Imprivata Policies and Workflows	Authentication Only (Auth Only)	Fast User Switching (FUS)	Kiosk Mode
Description	**Description**	**Description**	**Description**
• Requires VDA policy setup on the Imprivata appliance (user and computer) • Utilizes the VDA workflow policies like the PIE agent to automate the workflow • Does not use an IGEL preconfigured session like Authentication Only workflow • Supports (on-prem) Citrix, Horizon, or MS RDP only • Provides a chooser to display multiple apps or desktops if applicable	• Imprivata appliance is used to authenticate the user but does not use the VDA user/computer policies to automate the workflow. • IAFI securely retrieves user credentials from the Imprivata EAM appliance and authenticates the user into a local (IGEL) preconfigured session of a supported VDI client.	• Like the PIE agent, this utilizes the Imprivata Computer Policy FUS settings to automate the workflow. • Keeps a virtual app (Epic) hot while switching users on the endpoint	• In this mode, IAFI runs like a service to provide virtual channel support for Imprivata authentication devices • All other IAFI modes are disabled when kiosk mode is enabled.
IAFI Benefits	**IAFI Benefits**	**IAFI Benefits**	**IAFI Benefits**

Follow Imprivata Policies and Workflows	Authentication Only (Auth Only)	Fast User Switching (FUS)	Kiosk Mode
• Support for commonly used Imprivata VDA policy workflows but in an IGEL non-appliance mode option that allows access to the local IGEL desktop. • IGEL Resource Chooser for apps or desktops that support Citrix and Horizon. • Support to launch a preselected resource based on device location - override IGEL Resource Chooser	• Native integration with local IGEL virtualization apps • Support for commonly used roaming apps or desktop workflows • Required for Microsoft AVD / Windows 365 Cloud PC workflows • Can also be used with Citrix, Horizon, or Remote Desktop apps.	• Utilizes an IGEL app preconfigured session with a generic user account to launch the virtual app. • Can be used for Citrix, Horizon, Microsoft AVD, or RDSH sessions • Supports the same FUS computer policy options as the PIE agent • Supports the Imprivata Persistent App Workflow (requires VDA licenses for users).	• Supports virtual kiosks (Imprivata Type 2 agent) and Epic Only workflows • Can be used for Citrix, Horizon, Microsoft RDP, AVD, or Windows 365 Cloud PC's • Does not require USB redirection of supported Imprivata proximity card readers

IGEL Agent for Imprivata (IAFI) Feature Comparison Matrix

Updated: 20 Jan 2026

General Recommendations

- Use the latest IAFI OS 12 app version as it will contain the newest features, updates, and fixes.
  - You can access the latest IAFI version and release notes on the IGEL App Portal[78].
- IGEL OS 11 - as of November 2024, no new IAFI features have been included in OS 11. All new features are with OS 12 only.
- For Imprivata Windows or ProveID Embedded Agent (PIE), always refer to the latest Imprivata Enterprise Access Management - SSO Supported Components[79] Guide.

NOTE: For any blank features, please contact your IGEL account team to inquire about any future roadmap items.

Imprivata EAM General Features and Workflows

General Features and Workflows	Windows Agent	PIE Agent (OS 11 only)	IAFI OS12	IAFI Notes Please refer to the Configuring IAFI KB article[80]
Appliance Failover	✓	✓	✓	
Offline Mode	✓	✓		
Self-Service Password Reset (Legacy Agent Dialogs)	✓	✓	✓	For IAFI agents 1.1.1 and lower, use the Imprivata EAM 24.1 branch or older versions. If using the 24.2 branch, use hotfix 2 or higher

78. https://app.igel.com/
79. https://docs.imprivata.com/supported/content/topics/ossupportedcomponents.html
80. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringBasicSettings

Self-Service Password Reset Web App	✓	✓	✓	The new SSPR Web App experience was introduced in EAM 24.2. IAFI 1.2.0 and higher will use this new SSPR Web App experience and not the Agent Dialogs from prior IAFI versions.
Third-party Self-Service Password Reset	✓	✓	✓	Supported with IAFI 1.2.0 and higher
Non-OneSign User Workflow	✓	✓	✓	
Guest Login			✓	For IAFI 1.3.0 agents or higher
Spine Combined Workflow (NHS)	✓	✓		
Smartcard as Proximity Card Workflow	✓	✓		
Customization Objects (Computer Policy)	✓	✓	✓	
Multi-Monitor support	✓	✓	✓	Refer to this KB Article[81]
Default Domain Setting for Agent login	✓	✓	✓	
Configurable Setting for Lock Screen Toggle			✓	An optional hotkey that can be configured to toggle the IAFI full lock screen to a compact mode. The default setting is empty. Some example hotkeys: [Esc] or [Esc] + [i]
Entra ID Directory Users	✓		✓	
Enforce MFA for PIN Enrollment	✓	✓	✓	

81. https://kb.igel.com/en/igel-apps/current/how-to-enable-multiple-monitors-for-igel-agent-for

Primary Authentication Methods (Including Enrollment)

These additional Imprivata Licensed Options for Primary Authentication are NOT supported by IAFI

- Fingerprint Identification (one-to-many match) - Configuring Fingerprint Identification in Enterprise Access Management[82]
  - **NOTE: Fingerprint enrollments must occur with a Imprivata Windows agent. Enrolling Fingerprints via the Imprivata Virtual Channel from an IAFI endpoint is not yet supported.**
- Imprivata ID for Windows access - Imprivata ID for Windows Access[83]
- VASCO OTP token authentication - Managing OneSpan (VASCO) OTP Tokens[84]

Primary Authentication Methods	Windows Agent	PIE Agent OS 11 Only	IAFI OS 12	IAFI Notes
Password	✓	✓	✓	
Face recognition	✓			Imprivata Windows Agent feature only. Face Recognition Authentication[85]
Imprivata PIN (Device-bound Passkey)	✓			Imprivata Windows Agent feature only. Passwordless Authentication with Device-Bound Passkey[86]
Fingerprint Biometrics	✓	✓ NOTE: Authentication only, not enrollment	✓ NOTE: Authentication only, not enrollment	IAFI 1.4.0 and higher **Supported readers:** Imprivata IMP-1C UPEK ET700 / ET710

82. https://docs.imprivata.com/onesign/content/topics/onesign/authentication_management/configuringfingerprintid.html
83. https://docs.imprivata.com/onesign/content/topics/onesign/authentication_management/imprivataidforwindowsaccess.html
84. https://docs.imprivata.com/onesign/content/topics/onesign/authentication_management/managingvascodigipasstokens.html
85. https://docs.imprivata.com/onesign/content/topics/onesign/authentication_management/facialbiometric.html
86. https://docs.imprivata.com/onesign/content/topics/onesign/authentication_management/configuringfidoauth.html

Proximity Card	✓	✓	✓	**Supported Prox readers:** • rfIDeas readers / Imprivata branded models • HID Omnikey 5022 CL • MFR-75/75A
FIDO Security Key	✓	✓	✓	IAFI 1.3.0 and higher **Supported FIDO readers:** • rfIDeas readers / Imprivata branded FIDO models • HID Omnikey 5022 CL • MFR-75/75A
Smart Card using Active Directory Certificate	✓			
Smart Card using external certificate	✓			
Question and Answer	✓	✓		
Windows Hello for Business	✓			Windows Agent Only feature

Primary + Second Factor Authentication Workflows

IAFI supports the grace period settings for the Imprivata second factor in the user policy

Second-Factor Authentication Workflows	Windows Agent	PIE Agent (OS 11 only)	IAFI OS 12	IAFI Notes

Password + Imprivata ID	✓			PW + Imprivata ID is a Windows agent only feature. Additional Second factor policy options for password are not supported.
Fingerprint + Password	✓	✓	✓	IAFI 1.4.0 and higher
Fingerprint + Imprivata PIN	✓	✓	✓	IAFI 1.4.0 and higher
Proximity Card + Password	✓	✓	✓	
Proximity Card + Imprivata PIN	✓	✓	✓	
Proximity Card + Fingerprint	✓	✓	✓	IAFI 1.4.0 and higher
Proximity Card + Fingerprint or Password	✓	✓	✓	IAFI 1.5.0 and higher
Proximity Card + Fingerprint or Imprivata PIN	✓	✓	✓	IAFI 1.5.0 and higher
FIDO Security Key + Password	✓		✓	IAFI 1.3.0 and higher
FIDO Security Key + Imprivata PIN	✓		✓	IAFI 1.3.0 and higher
FIDO Security Key + Fingerprint	✓		✓	IAFI 1.4.0 and higher
FIDO Security Key + Fingerprint or Password	✓		✓	IAFI 1.5.0 and higher
FIDO Security Key + Fingerprint or Imprivata PIN	✓		✓	IAFI 1.5.0 and higher

Authentication / Reauthentication Methods via Imprivata Virtual Channel

This is to support Imprivata EAM (Confirm ID) reauthentication workflows for **EPCS and Clinical Workflows**

Authentication / Reauthentication Methods via Virtual Channel	Windows Agent	PIE Agent (OS 11 Only)	IAFI OS 12	IAFI Notes
Proximity Card	✓	✓	✓	
Smart Card	✓			
FIDO Security Key	✓			
Fingerprint Biometrics	✓	✓	✓	IAFI 1.5.1 and higher Older IAFI versions can use USB redirection of a Fingerprint reader.
Imprivata Hands Free Authentication	✓	✓		
Imprivata ID (Push Notification)	✓	✓	✓	IAFI 1.5.1 and higher

Walk-Away Security

This is for support of the Imprivata Computer Policy > Walk-Away Security settings.

Walk-Away Security	Windows Agent	PIE Agent (OS 11 only)	IAFI OS 12	IAFI Notes

Honors Lock Command (Hotkey in User Policy Challenges tab)	✓	✓	✓	With IAFI 1.5.0 and higher, we now support the full Imprivata Hotkey Glossary options. Older IAFI versions support these Hotkey combinations: • [SHIFT] + any other key [ESC] + any other key [HOME] + any other key [RIGHT] alone • Fn keys either alone or in combination with [SHIFT], [ESC] or [HOME] • Example: [F4] or [SHIFT]+[F4]
Fade to Lock Screensaver	✓	✓	✓	Black screensaver only - no fade to lock
Notification Balloon	✓	✓	✓	
Secure Walk-Away (via Imprivata BLE Dongle)	✓	✓		
Transparent Screen lock	✓			Imprivata Windows Agent Only feature

For the following workflow configurations, please refer to this IAFI KB Article - IAFI Profile Templates[87]

Microsoft Workflows

For OS 12, IGEL recommends using the latest IAFI version and the latest Microsoft app versions for AVD, Win 365 Cloud PC, or Remote Desktop
IAFI versions will specify the minimum required Microsoft companion app.

87. https://kb.igel.com/en/igel-apps/current/iafi-profile-templates

Microsoft Workflows	Windows Agent	PIE Agent (OS 11 only)	IAFI OS 12	IGEL Agent for Imprivata Configuration Mode				IAFI Notes
				Auth Only	Follow Policies	Kiosk	Fast User Switching	
AVD Desktops (Roaming)	✓		✓	✓				Manual or auto-launch
AVD Remote Apps (Roaming)			✓	✓				Manual or auto-launch
Win365 Cloud PCs Enterprise or Frontline (Roaming)			✓	✓				OS 12 only Manual or auto-launch
Virtual Kiosk for AVD/Win365 Cloud PC - (Non-Roaming)	✓ *(AVD only)*		✓			✓		Imprivata Type 2 agent installed on Windows virtual kiosk
RDS/Remote PC Desktops (Roaming)		✓	✓	✓	✓			Only one Remote PC desktop connection is supported in Follow Policies mode.
RDS Applications (Roaming)	✓	✓						
Virtual Kiosk for RDS/Remote PC Desktops (Non-Roaming)	✓		✓			✓		Imprivata Type 2 agent installed on Windows virtual kiosk

Virtual Kiosk for RDS Published Apps (Non-Roaming)	✓		✓			✓		

Citrix Workflows

For OS 12, IAFI has specific Citrix version requirements for these workflows.
NOTE: IAFI app versions will specify the minimum Citrix companion app.

Citrix Workflows	Windows Agent	PIE Agent (OS 11 only)	IAFI OS 12	IGEL Agent for Imprivata Configuration Mode				IAFI Notes
				Auth Only	Follow Policies	Kiosk	Fast User Switching	
Virtual Desktops (Roaming)	✓	✓	✓	✓	✓			Manual or auto-launch
Virtual Apps (Roaming)	✓	✓	✓	✓	✓			Manual or auto-launch
Virtual Kiosk for Citrix Desktops (Non-Roaming)	✓	✓	✓			✓		Imprivata Type 2 agent installed on virtual kiosk
Virtual Kiosk for Published Applications (Non-Roaming)						✓		Epic Only workflow with Type 3 agent on Microsoft Server OS

Citrix Connection Configuration Details (All IAFI configuration modes - Auth Only, Follow Policies, Kiosk, Fast User Switching):

- Storefront Authentication (Store and Storeweb)
  - HTTPS required
  - The Citrix Store must be configured with the following authentication methods to support connections from IAFI.
    - User name and Password
    - Domain pass-through
    - HTTP Basic
- When using IAFI in **Follow Policies and Fast User Switching (Persistent App workflow)**, the Imprivata VDA Citrix URL must be the Citrix Storeweb URL. The legacy PNAgent URL is not supported with IAFI.
  - ex: https://citrix.igeldemolab.org/Citrix/StoreWeb
- When using IAFI in **Auth Only or Kiosk Mode**, the Citrix Workspace App URL must be the Citrix Store URL
  - ex: https://citrix.igeldemolab.org/Citrix/Store

Troubleshooting Tip for Citrix Storefront connections

- If you see a double-prompt to reauthenticate after initially logging into the Citrix Workspace App (i.e. IAFI Auth Only mode), check to make sure the Trusted Domain information is consistent across the Citrix environment.
- IGEL recommends using the FQDN across all of the Citrix environment. The FQDN should also match the domain information that the Imprivata appliance is synching with against Active Directory.
  - ex: Trusted Domain = igeldemolab.org

Omnissa Horizon Workflows

For OS 12, IGEL recommends using the latest IAFI version and the latest Omnissa Horizon app version.
NOTE: IAFI app versions will specify the minimum Omnissa Horizon companion app.
** If using the Horizon NextGen v2 broker, only Workspace ONE is supported as the Horizon IdP. Please review the Omnissa Horizon documentation.

Horizon Workflows	Windows Agent	PIE Agent (OS 11 only)	IAFI OS 12	IGEL Agent for Imprivata Configuration Mode				IAFI Notes
				Auth Only	Follow Policies	Kiosk	Fast User Switching	
Virtual Desktops / on-prem (Roaming)	✓	✓	✓	✓	✓			Manual or auto-launch
Virtual Published Applications / on-prem (Roaming)	✓		✓	✓	✓			Manual or auto-launch
Virtual Desktops (Cloud)	✓		✓	✓				
Virtual Published Apps (Cloud)	✓		✓	✓		✓		
Horizon Cloud Entitlement On-Ramp Broker (Roaming Desktops or Apps)			✓	✓				Requires IAFI Auth Only mode

Horizon Cloud Entitlement On-Ramp Broker (Virtual Kiosk)						✓		
Horizon Cloud Service / v2 NextGen Broker**			✓	✓		✓		Desktops or apps and virtual kiosk with Imprivata Type 2 agent
Virtual Kiosk for Horizon Desktops (Non-Roaming)	✓	✓	✓			✓		Imprivata Type 2 agent installed on virtual kiosk
Virtual Kiosk for Horizon Apps (Non-Roaming)	✓		✓			✓		Epic Only workflow with Type 3 agent on Microsoft Server OS

Imprivata Requirements

Imprivata Enterprise Access Management (EAM) System Requirements

Components	Version	Notes
Imprivata Appliance	• On-prem or Azure deployed • G4 Appliances: 7.10 and higher • G3 Appliances: 7.6-7.10	IMPORTANT: Imprivata no longer supports the G3 appliance. IAFI can still work with the ProveID Web API running on G3 appliance versions, but customers should migrate to the G4 appliances for production use. Please refer to the Imprivata support site for a list of currently maintained versions.

Imprivata Licensing	REQUIRED:
	• Authentication Management (AM)
	• Single Sign-On (SSO)
	• Virtual Desktop Access (VDA)
	• ProveID Web API
	OPTIONAL:
	• Self Service Password Reset (SSPR)
		IMPORTANT:
		• Restricted API Access for ProveID Web API is not supported
		• VDA licensing is optional for these IAFI configurations:
		  • Kiosk mode (ex: Epic Only, Type 2 Virtual Kiosk)
		  • FUS mode (ex: Epic with IAFI full lock screen)

IAFI does not support these additional Imprivata licensed options for primary authentication:
- Fingerprint identification (one-to-many match)
- Imprivata ID for Windows access
- External ID token
- VASCO OTP token authentication

Further Details

- How to Deploy the Imprivata Appliance Certificate(s) to IGEL Devices (see page 219)
- How to Configure the Imprivata EAM Admin Console for ProveID Web API Access (see page 224)
- Proximity Card Allow List - Self Enrollment (see page 225)

How to Deploy the Imprivata Appliance Certificate(s) to IGEL Devices

IGEL supports the Imprivata appliance certificates in the Base64 encoded X.509 `.crt` or `.cer` format.

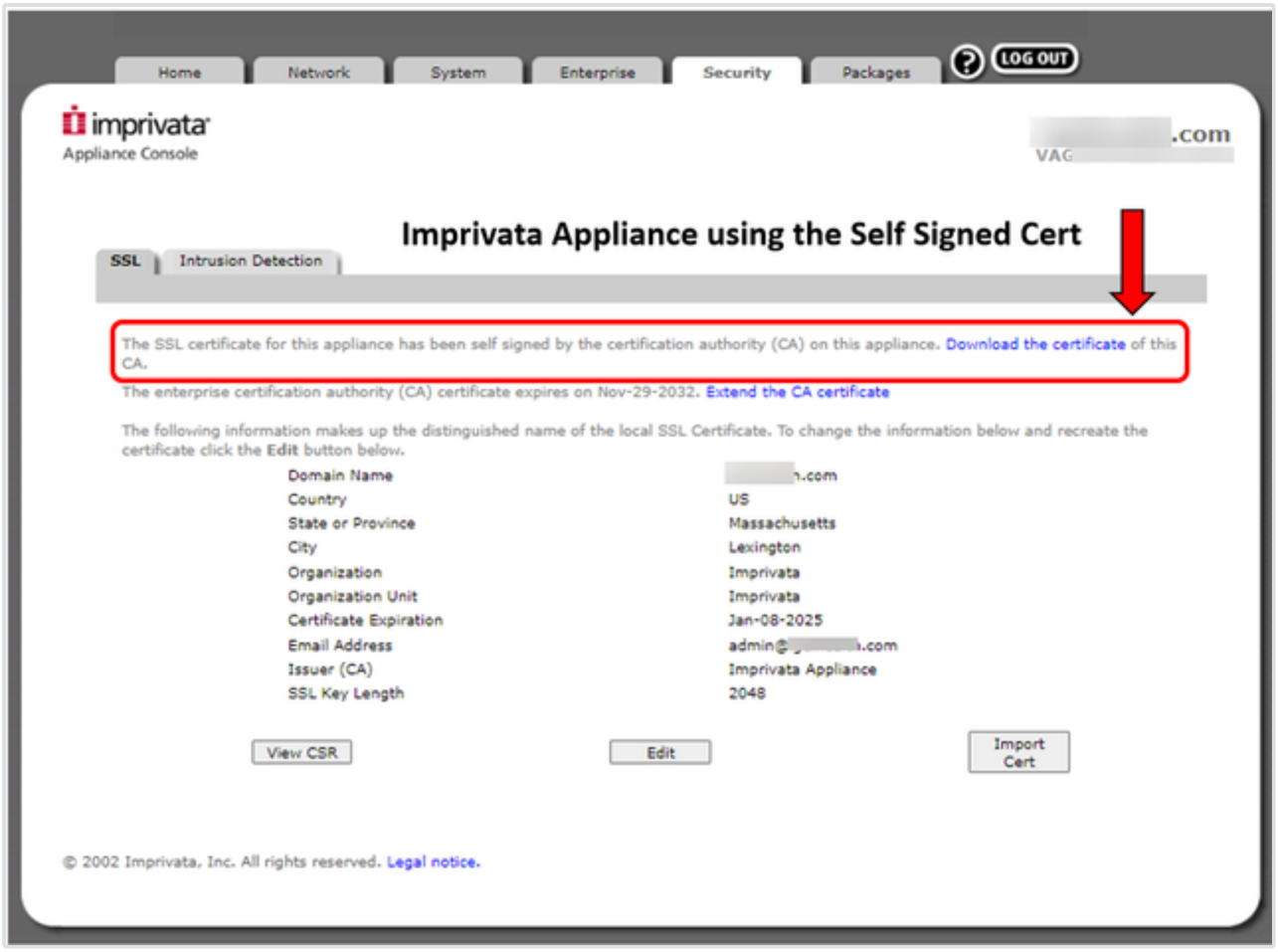
By default, Imprivata appliances use a self-signed certificate (`.crt` format) generated by the Imprivata root CA that is built into the appliance.

Customers can change the appliance certificate to one that is signed by a trusted root CA for either their network (e.g. Active Directory Domain Enterprise Root CA) or a publicly trusted CA like DigiCert. If this is the situation, you will need to export the root CA / subordinate CA / appliance certificate chain in Base64 X.509 `.crt` or `.cer` format and deploy the chain to all the devices via the UMS.

Using the Imprivata Root CA Certificate

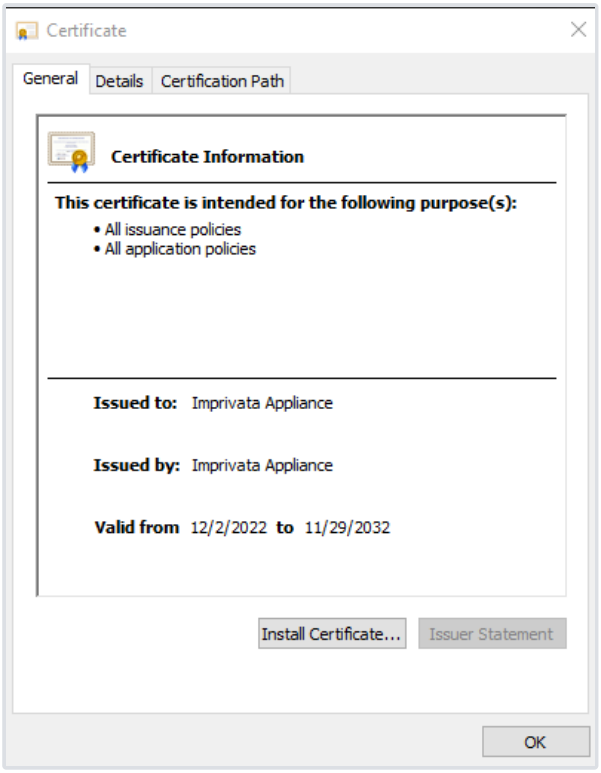
1. To confirm a customer is using the self-signed certificate, log into the Imprivata Appliance Console and go to the tab **Security.**
   (example appliance URL: https://fqdn-of-appliance:81)

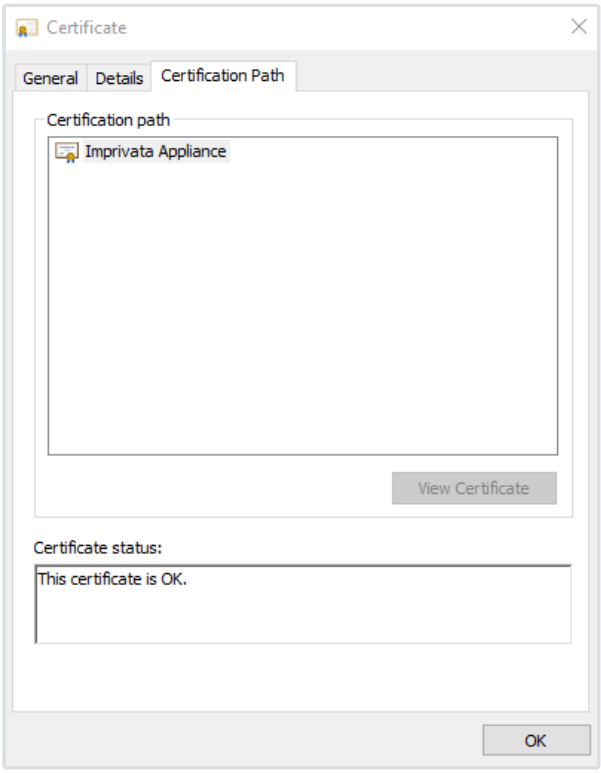
2. The following message will be shown:
   "**The SSL certificate for this appliance has been self signed by the certification authority (CA) on this appliance. Download the certificate of this CA.**"



3. Click **Download the certificate**.

4. The root certificate will be automatically downloaded as a file called `ssoCA.crt`.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: Imprivata Appliance
Issued by: Imprivata Appliance
Valid from 12/2/2022 to 11/29/2032
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certification path
Imprivata Appliance
View Certificate
Certificate status:
This certificate is OK.
OK

The Imprivata root CA certificate is the only one you need to deploy to the IGEL devices from the UMS Console as it will verify the trusted connection to the different appliances in the environment.

Using a Third-Party Root CA (e.g. Microsoft AD or Public CA)

In this situation, you will not be able to download the root CA from the Imprivata Appliance Console.

You will have to export the chain via a browser supported by the Imprivata Appliance Console (MS Edge or Chrome).

Export the certificate chain in `.crt` format (Base64 X.509).

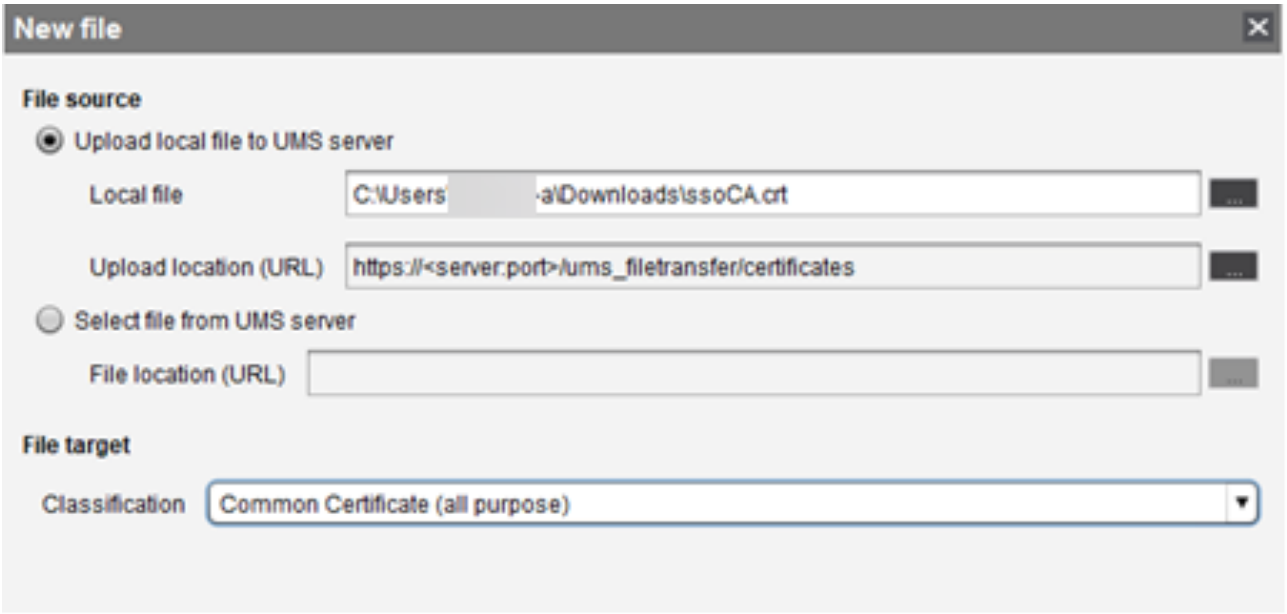
Deploying the Appliance Certificates

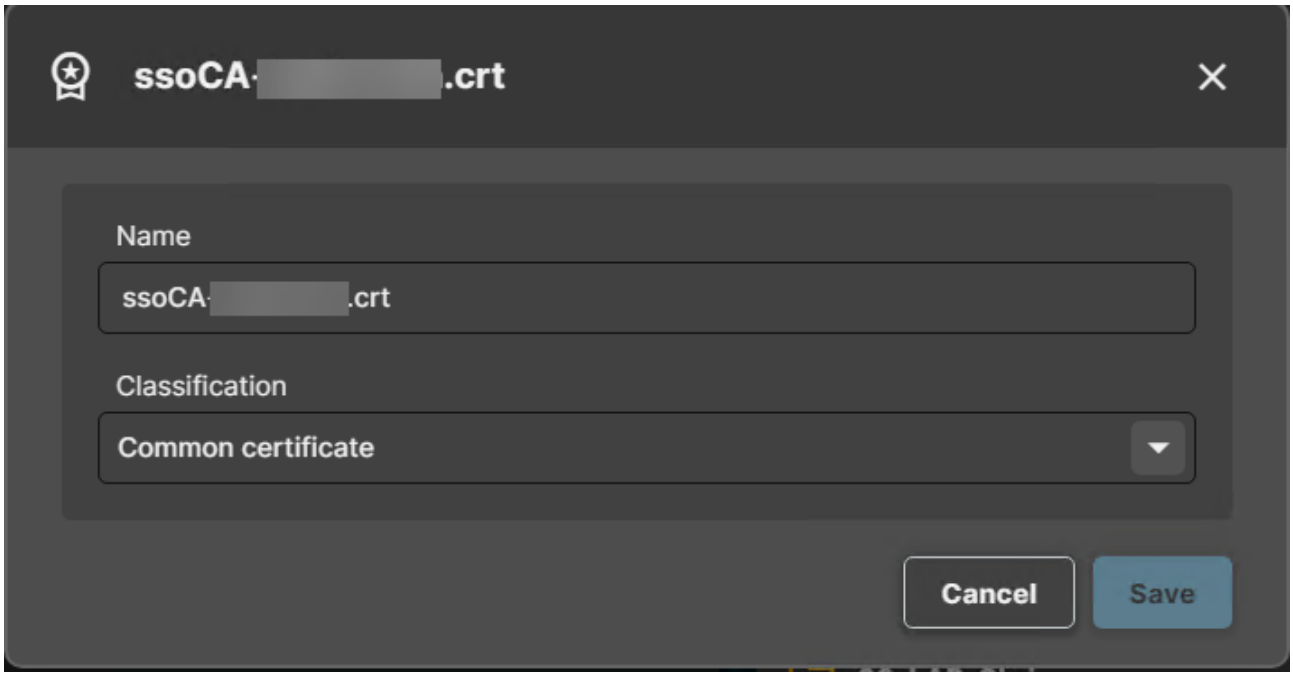
For how to deploy certificates via the UMS, see(11.10.210-en) Deploying Trusted Root Certificates in IGEL OS.

When uploading the Imprivata root CA certificate or third-party certificate(s) to UMS, you can choose either of two options for file classification:

- **Common certificate** (all-purpose) - this is the preferred choice
- **SSL certificate**

Examples of Imprivata Certificate for UMS Java or Web Console:





With either option, once the certificate is deployed to the device, it will automatically install in the `/wfs/ca-certs` directory which is where the IGEL Agent for Imprivata looks for the certificates. If needed, you can verify the certificate by opening a terminal window and running the following command; the exact command depends on the name of the certificate file:

```
cd /wfs/ca-certs; openssl verify ssoCA.crt
```

or

```
cd /wfs/ca-certs; openssl verify ssoCA.cer
```

How to Configure the Imprivata EAM Admin Console for ProveID Web API Access

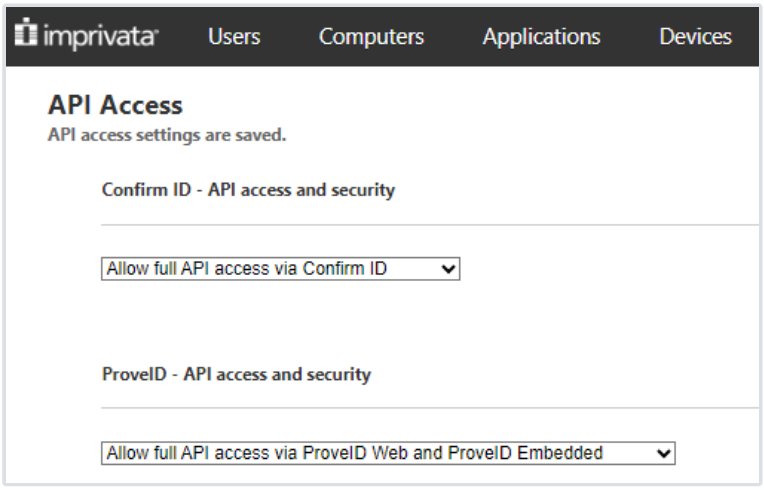
This is a required step to work with IGEL OS endpoints.

1. Open the Imprivata EAM Admin Console.

2. Log in as an administrator.

3. On the upper-right corner of the console, click the **gear icon > API Access.**

4. In the section **ProveID - API Access and Security**, select **Allow full API access via ProveID Web API and ProveID Embedded.**



Restricted API Access is not currently supported

5. Select the check box **IGEL OS**.

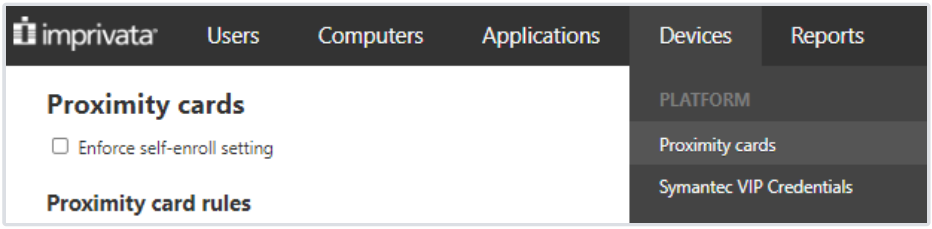
6. Click **Save**.

Proximity Card Allow List - Self Enrollment

If you want to use the IGEL Agent for Imprivata, **Enforce self-enroll setting** must be disabled.

1. Go to **Devices > Proximity cards.**

2. Disable **Enforce self-enroll setting.**



When you enable the proximity card allow list, you control what specific proximity cards users can self-enroll.

See **Imprivata KB article 23313** for an explanation of this setting.

With this option selected, users can only self-enroll a proximity card when all of the following criteria are fulfilled:

- The card is listed on the proximity cards page
- The assignment status is set to **Available**
- A checkmark appears in the column **Allow Self-enrollment**

If a user attempts to enroll a proximity card that does not appear on the allow list, an error message appears.

IAFI - IGEL System Requirements

Components	Version	Notes
IGEL UMS	UMS 12.x - latest version recommended	UMS 12.x supports both OS 11 and 12 devices and licenses.
IGEL OS	OS 12 OS 11 (specific versions)	The IAFI Agent's latest features will be in the OS 12 app and are included in specific OS 11 firmware versions as noted in the Feature Matrix. The IGEL Agent for Imprivata is available on the IGEL App Portal[88]. See IGEL Agent for Imprivata Feature Matrix Comparison[89] for more information.
IGEL Licensing	• IGEL Workspace Edition • IGEL Agent for Imprivata Workspace Edition add-on license As of November 1st, 2024, these are the new licensing requirements: • IGEL OS Editions | IGEL[90] • IGEL-Editions-Licensing-Info-Brief.pdf[91]	The IGEL Agent for Imprivata add-on license is part of the Smart Login Feature Pack included in the IGEL Healthcare Edition. The IGEL Healthcare Edition is subscription-based and tailored for mission-critical healthcare environments. It includes 24/7 Priority Plus technical support[92] with all the capabilities of the IGEL Enterprise Edition, and at no extra cost, the IGEL Smart Login Feature Pack, which supports Imprivata (and includes the IAFI licensed feature). ⚠ Imprivata workflow / use case validation is required before providing IAFI licenses for customer testing or production use. Please refer to the IGEL Agent for Imprivata Feature Matrix Comparison[93] for currently supported features and workflows.

88. https://app.igel.com/
89. https://kb.igel.com/en/igel-apps/current/igel-agent-for-imprivata-iafi-feature-matrix-compa
90. https://www.igel.com/licensing/
91. https://www.igel.com/wp-content/uploads/2024/10/IGEL-Editions-Licensing-Info-Brief.pdf
92. https://www.igel.com/support/
93. https://kb.igel.com/en/igel-apps/current/igel-agent-for-imprivata-iafi-feature-matrix-compa

What changed with IGEL OS 12?

IGEL OS 12 introduced a new architecture that was app-centric with the IGEL App Portal vs. monolithic firmware with all integrated apps included. This required changes to the app deployment methodology within the OS. As noted earlier, the initial IAFI integration was delivered in IGEL OS 11 firmware and later updated to support the new OS 12 architecture changes. Generally speaking, the delivery model was updated to be more app-centric for IGEL OS 12 and the other applications we integrate with such as Citrix, Horizon, or AVD. It was determined that the Imprivata PIE would not function on OS 12 without significant changes, and the collective decision was made to move customers over to IAFI as they upgrade to OS 12.

How to Enable IAFI Licenses in the IGEL License Portal (ILP)

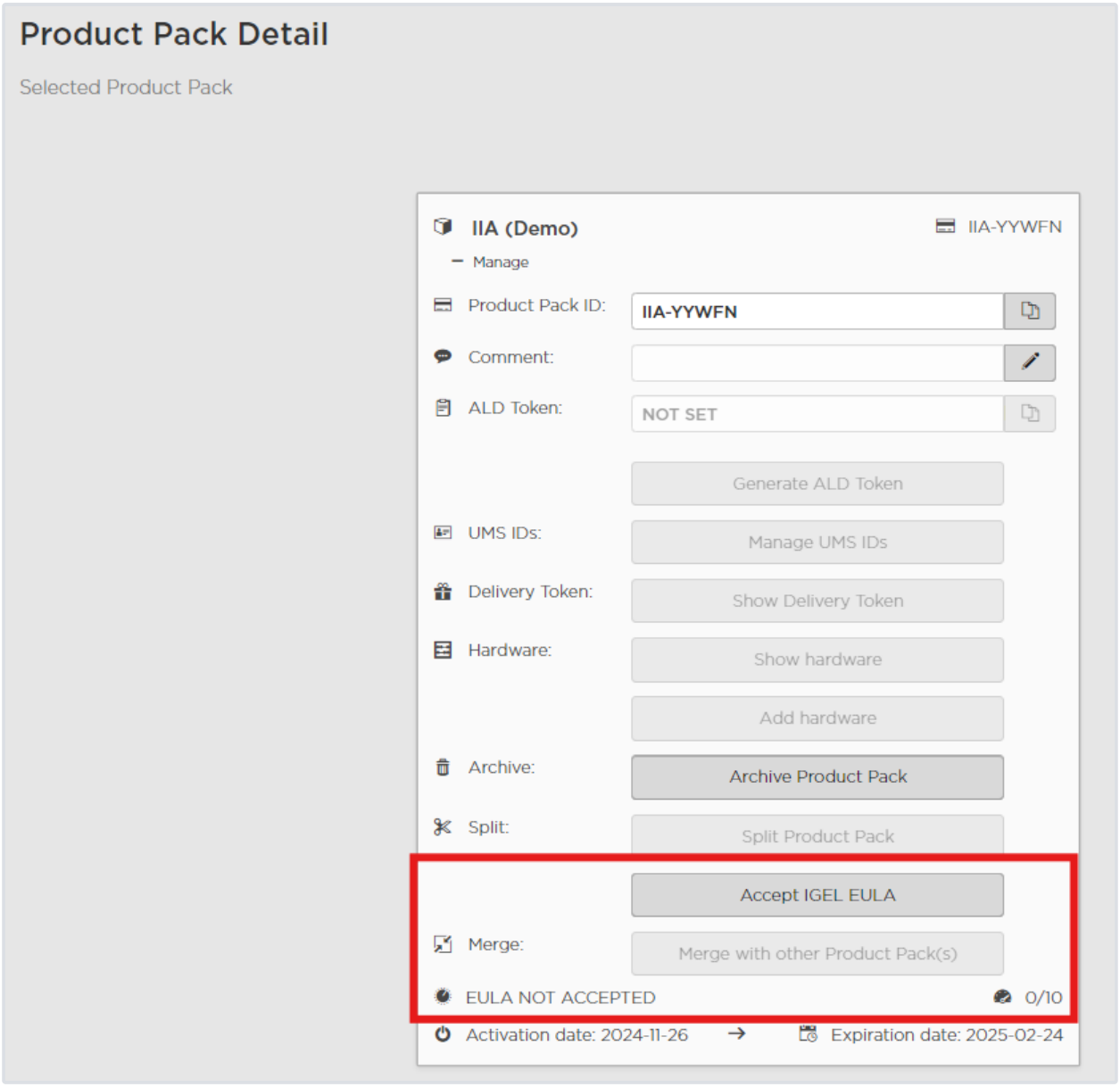
⚠ Within the IGEL License Portal, once the licenses are assigned, the **EULA must be accepted** and then the IAFI product pack will be available to assign to a UMS Server for Automatic License Deployment (ALD)[94].

Fetching the IAFI Product Pack from the ILP

1. Login into the IGEL License Portal and navigate to the IIA Product Pack.

2. Click the **Accept IGEL EULA** button

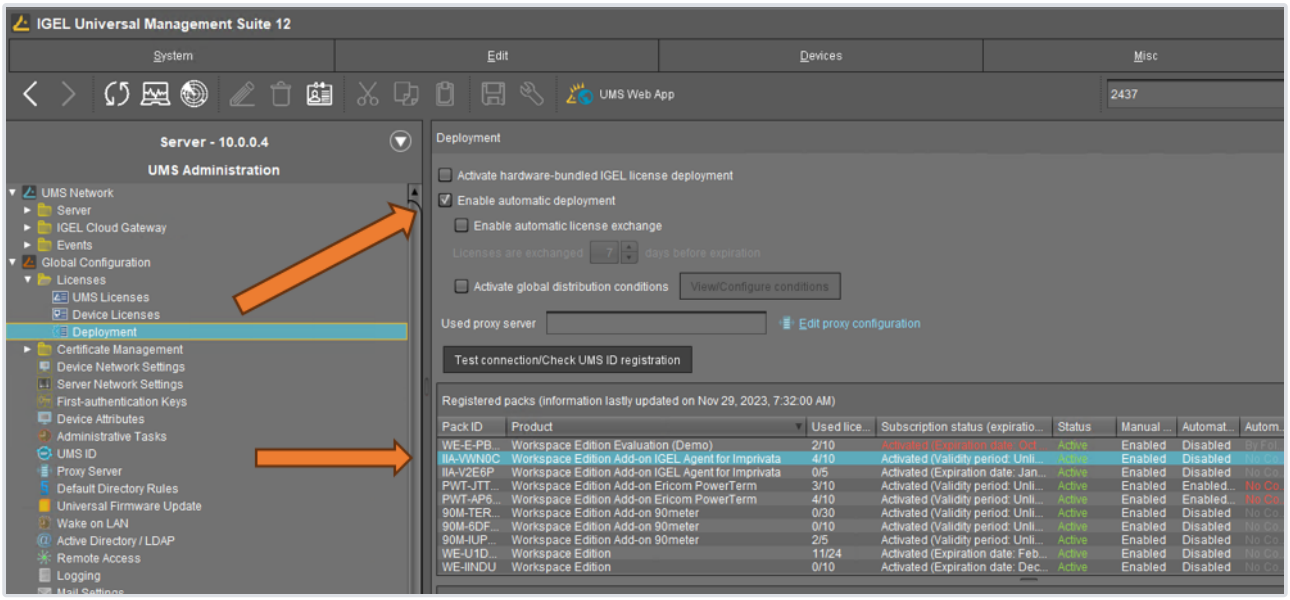
94. https://kb.igel.com/en/igel-subscription-and-more/current/setting-up-automatic-license-deployment-ald



Once the EULA is accepted, make sure to assign the IIA Product Pack to your IGEL UMS ID. This is done with **Manage UMS IDs**:.

Automatic License Deployment Using the IGEL Universal Management Suite (UMS)

UMS integrated with the IGEL License Portal showing IAFI Workspace Edition Add-on enabled for automatic deployment:



IGEL OS 12 device with Workspace Edition and Workspace Edition Add-on IGEL Agent for Imprivata licenses:



IAFI Terminology Glossary

Term	Definition	Additional Notes
IGEL Agent for Imprivata (IAFI)	The IGEL built ProveID Web API agent for Imprivata Enterprise Access Management (EAM) formerly called OneSign and Confirm ID.	• Non-appliance mode experience • OS11 agent built into firmware • OS 12 app available in the IGEL App Portal. Allows access to the IGEL desktop and flexible control over user experience and workflows. • Supports Microsoft AVD apps and desktops (single and multi-session), Windows 365 Cloud PC (Frontline edition also), RDP desktops, Citrix apps and desktops, and Horizon apps and desktop workflows. • Supports Fast User Switching (FUS) workflows with Citrix, Horizon, or Microsoft AVD • Supports Kiosk Mode workflows (Epic Only and Virtual Kiosk Type 2 agent) • Requires Imprivata VDA licensing for automated workflows • Requires IGEL Agent for Imprivata Workspace Edition add-on license
Imprivata ProveID Embedded (PIE) Agent	The Imprivata built Linux agent that is installed on the appliance and is downloaded and installed on an IGEL OS 11 device. This is version dependent on both IGEL OS and Imprivata versions.	• OS 11 Appliance Mode only experience • No IGEL local desktop access • Policies and workflows developed and supported by Imprivata • Requires Imprivata VDA licensing • Supports Citrix apps and desktops, VMware desktops, and Microsoft RDSH/RDP desktops • Supports Citrix Fast User Switching (FUS) workflows
IAFI Authentication Only	In this configuration, IAFI authenticates a user to the Imprivata appliance and then securely logs the user into a local preconfigured session for a supported application. Only one preconfigured session type is supported at a time (example: AVD).	• Roaming apps or desktop workflows only • Does not use the Imprivata VDA User or Computer Policy settings to drive the workflow • Required for Microsoft AVD / Windows 365 Cloud PC workflows • Can also be used for Citrix apps or desktops, Horizon apps or desktops, or Microsoft RDP desktops • Requires Imprivata VDA licensing

IAFI Follow Imprivata Policies	In this configuration, IAFI uses the Imprivata VDA user and computer policies to automate the workflow. This is similar to how the PIE agent works.	• Requires Imprivata VDA policy setup on the appliance (user and computer) • Supports the ability to launch a preselected resource based on location (example: bypassing a chooser if you want a specific desktop or app to be launched at that location). • Supports on-prem Citrix, Horizon, or Microsoft RDP

IAFI Fast User Switching (FUS)	Imprivata OneSign fast user switching (FUS) is used in shared workstation workflows to allow rapid switching between user identities at the desktop level and the application level. • For **desktop-level FUS**, the Windows-based shared workstation or virtual desktop kiosk is configured to automatically authenticate to Windows using generic credentials (i.e. kioskuser/ kioskpassword). Users authenticate to Imprivata OneSign (versus having to authenticate to Windows) to access the shared Windows desktop which greatly reduces the time to logon.	IAFI supports FUS in multiple modes: • Desktop-level FUS with a lock screen - aka Imprivata Multi-App Epic workflow • Application-level FUS - aka Imprivata Epic Only which maps to the IAFI Kiosk Mode configuration • Virtual Kiosk - Imprivata Type 2 agent - this maps to the IAFI Kiosk Mode configuration

	• For **application-level FUS**, an application, such as the EHR (ex: Epic), is configured to remain persistent (or “hot”) on a shared workstation. With a lock screen configured, during a desktop-level fast user switch, Imprivata OneSign logs the previous user out of the application and logs the new user in which greatly reduces the time to access the application since it is not restarted during the user change event. • **Application-level FUS** can also be configured to support virtualized applications delivered via technologies like Citrix, Horizon, or Microsoft AVD. An example of this would be the Imprivata Epic Only workflow	
IAFI Kiosk Mode	In this configuration, IAFI runs as a service with Imprivata virtual channel support for supported authentication devices. This does not require USB redirection of these devices into the remote session.	• Supported workflows are Imprivata Epic Only and Virtual Kiosks (Type 2 agent)
Imprivata Private Workstation Agent (Type 1)	A method of installing and configuring the Imprivata Windows agent to support private workstation workflows. Also see private workstations.	

Imprivata Shared Workstation Agent (Type 2)	A method of installing and configuring the Imprivata Windows agent to support shared workstation workflows. Also see shared workstations.	
Imprivata Citrix Server / Terminal Server Agent (Type 3)	A method of installing and configuring the Imprivata Windows agent to support shared Citrix (Citrix XenApp) servers or Microsoft Terminal Server servers.	
Private workstations	Private workstations are commonly used by a single user who requires access to one or more applications for a prolonged period of time. These workstations are typically found in private/physician offices, administration areas, and in specialty areas such as radiology.	
Shared workstations	Often called kiosks or public workstations, shared workstations are commonly used in areas where many different users require fast access to clinical applications for a limited period of time. These workstations are typically found in patient rooms, exam rooms, nursing stations, and physician documentation areas.	

Thin or zero client	A thin or zero client is an end user computing device that uses a lightweight version of Windows or a non-Windows operating system such as Linux to access virtualized applications and/or desktops.	
Virtual Desktop Infrastructure (VDI)	Virtual desktop infrastructure is a desktop virtualization approach in which a desktop operating system, typically Microsoft Windows, runs and is managed in a data center. The desktop image is delivered over a network to an endpoint device, which allows the user to interact with the OS and its applications as if they were running locally.	
Citrix DaaS	Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface. (Source: Citrix)	

Microsoft Azure Virtual Desktops (AVD)	Microsoft's VDI solution in their Azure cloud data centers, accessible through public internet or private network connections.	
Microsoft Azure Local (formerly Azure Stack HCI)	Microsoft offering that allows for customers to use on-prem datacenter hardware to access the AVD Windows Multi-Session OS.	
Microsoft Windows 365 Cloud PC	Microsoft's Desktop as a Service (DaaS) solution for business. Subcription-based offering for private workstations.	
Microsoft Windows 365 Cloud PC Frontline	Microsoft's Desktop as a Service (DaaS) offering for frontline workers (healthcare, public sector) that allows a 3-1 license model for a more cost effective solution.	

Omnissa Horizon	Formerly VMware Horizon, Omnissa Horizon is a desktop virtualization software platform that allows multiple users to access and run Microsoft Windows desktops and apps that are installed at a centralized location separate from the devices from which they are being accessed. Earlier versions were referred to as VMware View. Omnissa is a new company created from the sale of VMWare to Broadcom. Omnissa is the End User Computing products and services from the former VMWare.	
Virtual Desktop Infrastructure (VDI)	Traditional Virtual Desktop Infrastructure provisioned on-prem with the management plane consisting of distinct server based roles. Compute and Storage run on the tenant or hosting partner's datacenter	Example: Citrix desktop and application virtualization, Omnissa Horizon virtual desktops or RDSH apps, Microsoft RDSH
Cloud VDI	The evolution of traditional VDI where the virtualization management plane is delivered as a service. Elastic compute and storage are offered on consumption basis or through reservation based pricing. An evolutionary advancement in desktop virtualization.	Example: Microsoft Azure Virtual Desktop

Cloud PC	Fully managed, subscription-based model for a more consistent user experience similar to a physical PC. A great option for customers looking to outsource their VDI infrastructure.	Example: Microsoft 365 Cloud PC

IGEL Agent for Imprivata (IAFI) Configuration Guide

The IGEL Agent for Imprivata supports four configuration modes. There are general agent settings, virtual channel settings, and workflow configuration settings for the following:

- Follow Imprivata Policies and Workflows
- Authentication Only
- Fast User Switching
- Kiosk Mode

See the instructions below for how to enable the different settings and configuration modes.

- Configuration of the IGEL Agent for Imprivata on IGEL OS (see page 240)
- Primary Authentication Using Fingerprint (IAFI 1.4.0+) (see page 266)
- Resource Chooser Display Options (IAFI 1.5.0+) (see page 267)

Configuration of the IGEL Agent for Imprivata on IGEL OS

Before You Begin

- Review the Supported Features and Workflows: IGEL Agent for Imprivata (IAFI) Feature Comparison Matrix[95]
- Review the IAFI Workflow Configuration Options[96]
- Review the IAFI Terminology Glossary[97]

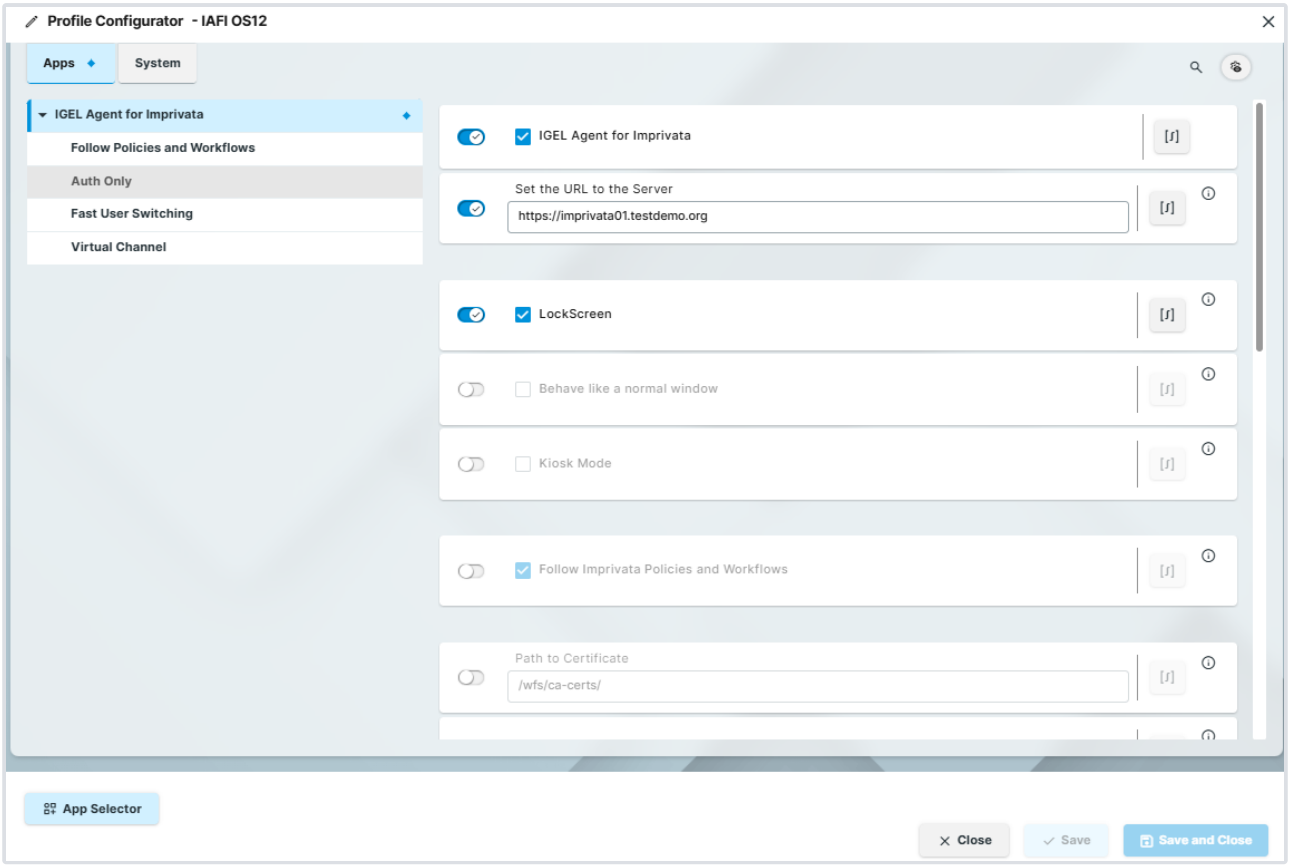
Requirements

- Review the Imprivata Requirements[98]
- Review the IAFI - IGEL System Requirements[99]
    - Add-on license that can be acquired via the request form at IGEL Agent for Imprivata[100]

Configuring Basic Settings

1. In the profile configurator, go to **Apps > IGEL Agent for Imprivata**.

95. https://kb.igel.com/en/igel-apps/current/igel-agent-for-imprivata-iafi-feature-matrix-compa
96. https://kb.igel.com/en/igel-apps/current/iafi-workflow-configuration-options
97. https://kb.igel.com/en/igel-apps/current/iafi-terminology-glossary
98. https://kb.igel.com/en/igel-apps/current/imprivata-requirements
99. https://kb.igel.com/en/igel-apps/current/iafi-igel-system-requirements
100. https://www.igel.com/imprivata-agent/



2. Edit the settings according to your needs. The parameters are described below according to how they appear in the profile configurator.

Some settings are only in the App registry and may be moved into the profile configurator in future releases.

IGEL Imprivata Agent

☑ The IGEL Agent for Imprivata is enabled.

☐ The IGEL Agent for Imprivata is disabled. (Default)

Registry	Value
`app.iia.enabled`	*False* (default), True

Set the URL to the server

Type in the URL address of the Imprivata Appliance. This needs to be the FQDN of at least one appliance.

For appliance failover with multiple appliances, separate the URL's using a semicolon " ; " and no spaces. Example: https://imprivata01.demolab.org;https://imprivata02.demolab.org;https://imprivata03.demolab.org
Related IAFI Configuration settings:

- **Path to Certificate**
- **Skip Certificate Verification**
- **Connection timeout**

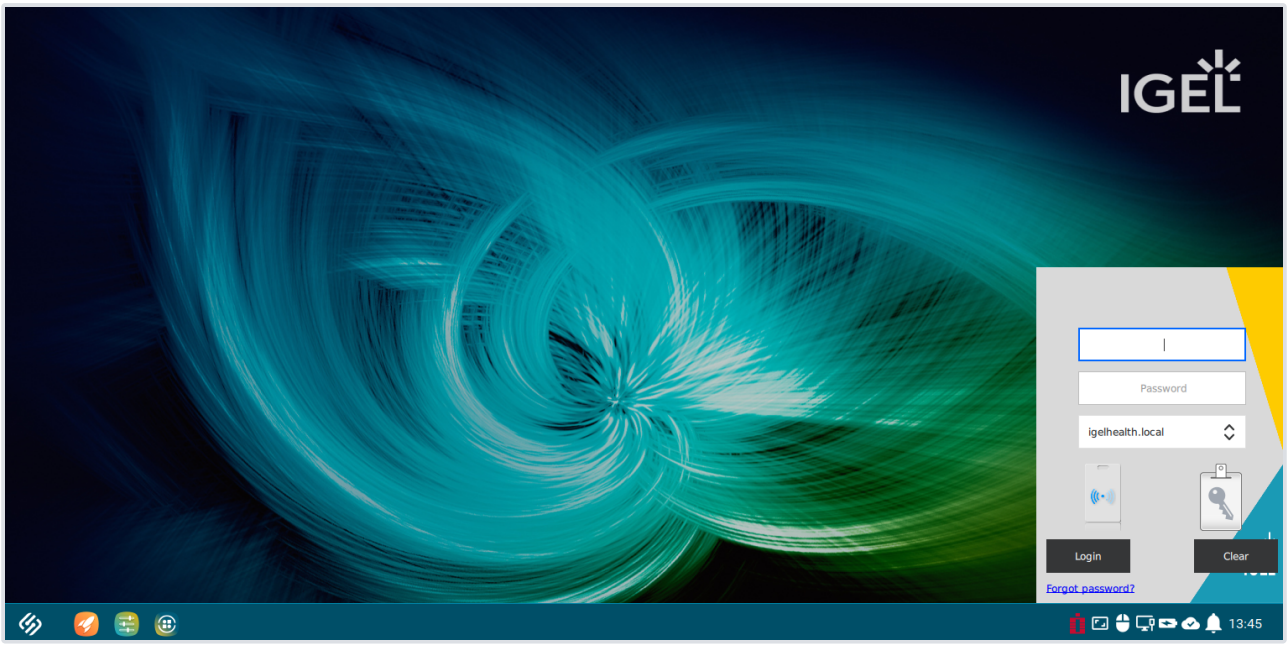
Registry	Value
`app.iia.server`	*Blank* (default)

LockScreen

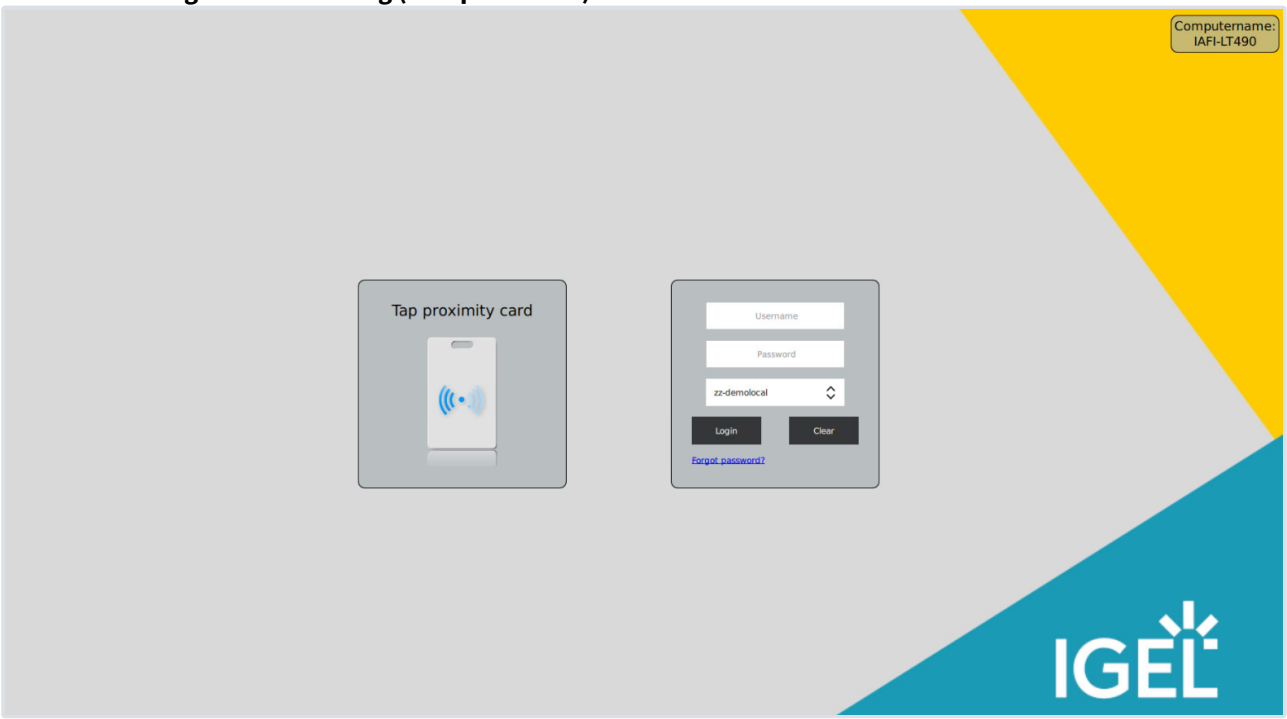
☑ When enabled, the agent will be in a full lock screen, similar to Appliance Mode in OS 11 with the Imprivata PIE agent. Only the Imprivata agent authentication dialogs and a background image are displayed. The IGEL desktop is not accessible.

☐ The Lockscreen is disabled. (Default)

In the default setting, the agent will start in a compact mode login in the bottom right corner of the screen with a portion of the IGEL desktop accessible.



1 IAFI default login screen setting (Compact Mode)

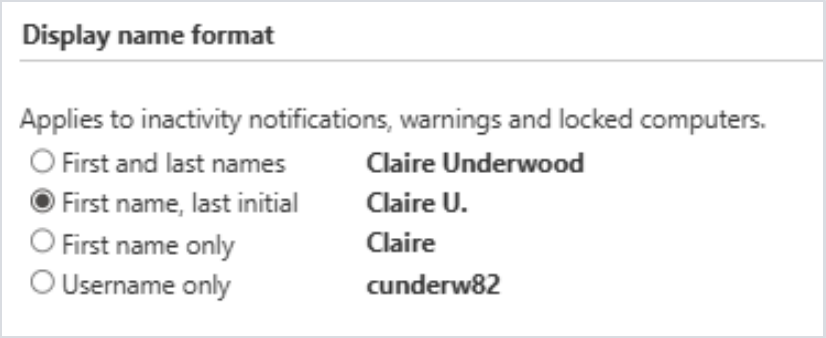


2 IAFI Lockscreen enabled (with the default background image)

Registry	Value
`app.iia.lockscreen`	*False* (default), True

Related IAFI Profile Configuration Lockscreen settings:

- **Choose the Background Image**
- **Show Computername on Lockscreen (**upper right corner of the screen**)**
- **Lockscreen Shortcut**
- **Show the username at the Lockscreen (**Registry Only**)**
  - This is related to an Imprivata Computer Policy setting: **General - Display name format**
  - You can change the format based on the policy options.
  - If you don't want to show the logged in user on the lock screen, disable this in the registry.



Registry	Value
`app.iia.show_username_on_lockscreen`	False, *True* (default)

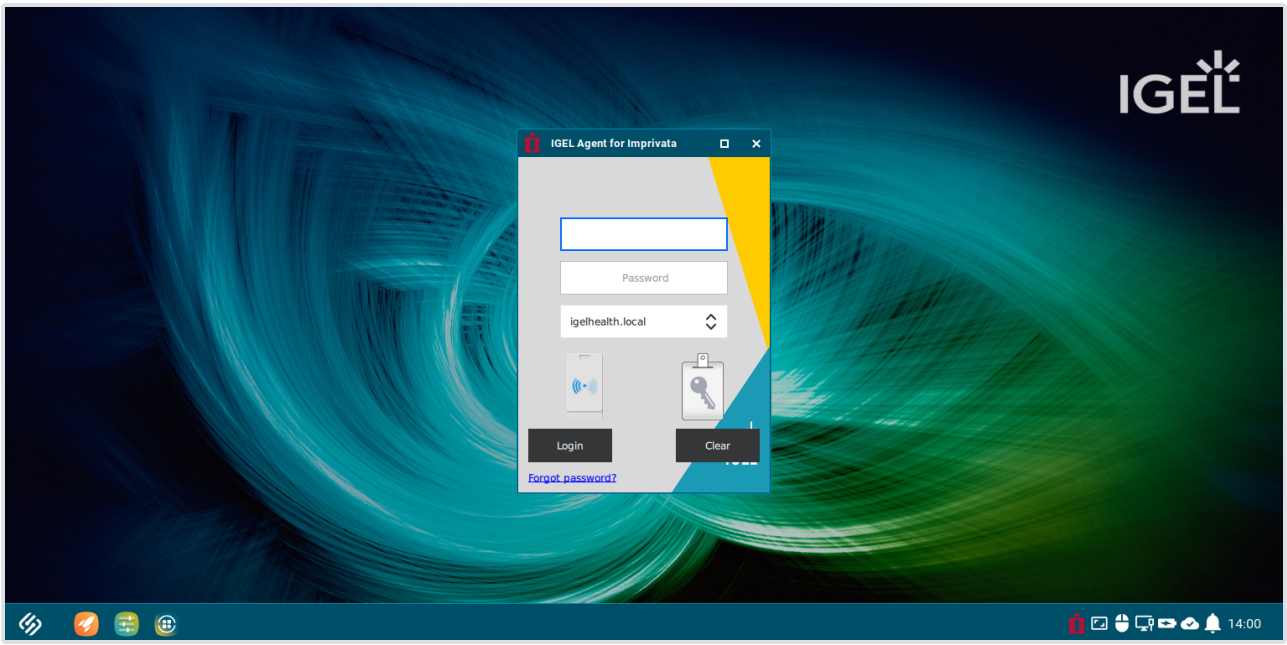
Behave like a normal window

☑ When enabled, this setting undocks the compact login screen from the IGEL taskbar and places it in the middle of the screen.

☐ Disabled (Default)

This feature is an option primarily for the **Follow Imprivata Policies and Workflows** configuration that will use the IAFI Resource Chooser. However, if you want the IAFI login to be in a Windows mode (not Fullscreen), you could also use this with the **Auth Only** configuration.

Registry	Value
`app.iia.windows_mode`	*False* (default), True



3 IAFI compact login in Windowed Mode

Enabling the Windowed mode setting will also impact the IAFI resource chooser (Apps or Desktops).

IAFI Compact Mode Login and Resource Chooser behavior:

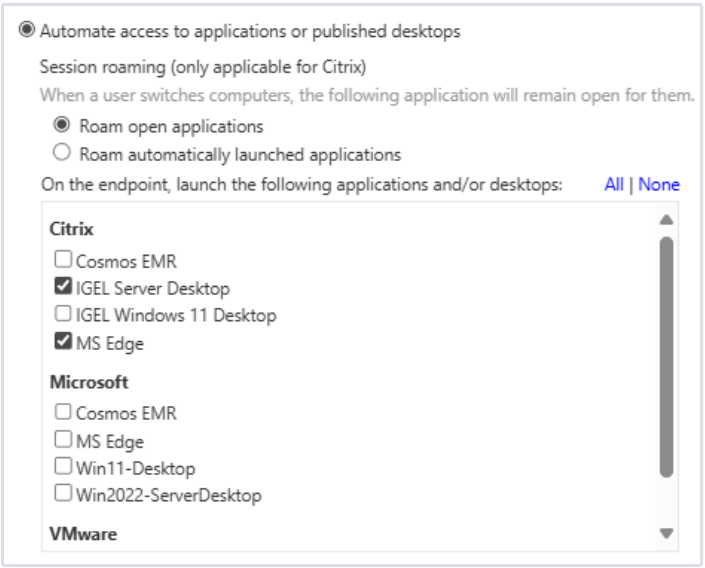
No Autolaunch of Imprivata VDA resources

- By default, if the Imprivata VDA User Policy for “Automate access to applications or published desktops” **does not have any resources set to autolaunch**, then the IAFI resource chooser will show in the middle of the screen after a user logs into the agent.
- The user will have to manually select the resources to launch.
- The chooser will be available for other resources to launch if necessary.
- The chooser **shows the logged in user**, a **search option to filter on resource names** and a **scroll bar** on the right side.



Autolaunch of Imprivata VDA resources

- If the Imprivata VDA policy is set to autolaunch any resources, then by default, the IAFI resource chooser will **NOT** appear after the user logs in.



- There is an IAFI registry setting that can change this behavior.

Changing the IAFI registry setting to keep the resource chooser available for Autolaunch workflows:

- Enabling this will keep the IAFI resource chooser available if the Imprivata VDA User Policy “Automate access to applications or published desktop” dictates autolaunching of resources (apps or desktops).

- After a resource is autolaunched, the user can go to the IAFI chooser to select other resources (apps or desktops) to manually launch.

Registry	Value
`app.iia.chooser_upon_restart`	*False* (default), True

Kiosk Mode

☑ When enabled, all other IAFI workflow modes (Auth Only, Follow Policies, FUS) are disabled and those settings do not apply.

☐ Disabled (Default)

NOTE: In Kiosk Mode, the agent runs as a service to provide virtual channel support for Imprivata authentication devices. Currently, this is Proximity Readers. Future IAFI versions will also support Fingerprint readers.

Kiosk Mode supports these common Imprivata workflows:

- Virtual kiosks (Imprivata Type 2 agent)
- Epic Only workflows
- Can be used for Citrix, Horizon, Microsoft RDP, AVD, or Windows 365 Cloud PC kiosk sessions
- Does not require USB redirection of supported Imprivata proximity card readers

Registry	Value
`app.iia.kiosk`	*False* (default), True

Follow Imprivata Policies and Workflows

This is the default configuration mode for IAFI. Generally speaking, this mode mimics the same workflows as the Imprivata PIE agent. When enabled, the Imprivata Virtual Desktop Access User and Computer policies that are defined on the Imprivata appliance will be applied such as the automatic startup of Citrix, Horizon or RDP sessions on login.

☑ Enabled (Default)

☐ Disabled

When disabled, the agent switches to **Auth Only** mode and the Imprivata appliance is only used as an identity provider. No further VDA policy automation will be evaluated or executed. Instead, the credentials that are passed on from the Imprivata appliance will be securely stuffed into the session that is defined under **Auth Only preconfigured session**. Auth Only mode can be used for connecting to AVD, Windows 365, Citrix or Horizon sessions.

Registry	Value
`app.iia.follow_policies`	False, *True* (default)

Path to certificate

☑ The default is set to: `/wfs/ca-certs/` and you do not have to specify the name of the certificate itself.

IAFI will look at certificates in that directory when they are deployed from the UMS server. Follow these guidelines for deploying the Imprivata appliance certificate(s) from UMS to the devices. How to Deploy the Imprivata Appliance Certificate(s) to IGEL Devices[101]

Registry	Value
`app.iia.path_to_certificate`	/wfs/ca-certs

Skip certificate verification

This can be used when you don't have the appliance certificate or the certificate chain deployed to the IGEL device. IGEL does not recommend enabling this setting for production use.

☑ When enabled, this skips appliance certificate verification and allows the agent to connect to the Imprivata appliance.

☐ Disabled (default)

Registry	Value
`app.iia.noverify`	*False* (default), True

Connection timeout

101. https://kb.igel.com/en/igel-apps/current/how-to-deploy-the-imprivata-appliance-certificate-

The timeout in seconds when the agent is connecting to the appliance.

> The default is 20 seconds but can be adjusted to a lower or higher number. IGEL does not recommend lowering this below 3 seconds.
> Related setting: **Set the URL to the server**
> If multiple appliances are listed, after the timeout setting is reached, the agent will contact the next appliance listed.

Registry	Value
`app.iia.connection_timeout`	20

Default entry of domain list

☑ When enabled, you can specify the name of a specific domain if more than one is configured in the Imprivata Appliance directories.

☐ Setting is blank and will use the domains provided by the appliance **in alphabetical order**. (Default)

Registry	Value
`app.iia.default_domain`	Blank

Choose the Background Image

IAFI has three options for the lockscreen background image.

- Default image (Default)
- Imprivata Appliance image (pulled from the Computer Policy - Customization settings)
- Custom Image deployed from the UMS Server to: `/wfs/`

> See this KB article for more information on customizing the background image.
> How to enable IAFI logon screen customizations[102]

Registry	Value
`app.iia.bgimage`	*default* (Default), appliance, custom

Hide agent window when idle

102. https://kb.igel.com/en/igel-apps/current/how-to-enable-iafi-logon-screen-customizations

☑ When enabled, this hides the agent compact dialog after a user logs in. You can click the agent icon in the IGEL system tray to display the popup window.

☐ The agent compact dialog will be displayed in the bottom right corner after a user logs in. (Default)

Registry	Value
`app.iia.hide_on_idle`	*False* (default), True

Lockscreen Shortcut

This shortcut setting allows you to toggle the lockscreen if you need to quickly access the IGEL desktop. It is disabled by default (blank).

> You can type a keyboard shortcut of your choosing. IGEL only supports two key combinations. Example shortcut keys are:
> - Esc
> - Esc, q
> - Alt, x

Registry	Value
`app.iia.lockscreen_shortcut`	Blank (default)

Query Email from App Moniker

> This is not a required setting but an option that can be used for IAFI Auth Only mode for Microsoft AVD or Windows 365 Cloud PCs. You would specify the name of the IGEL AVD app profile that is configured in the appliance "**application mapping**" section.

Registry	Value
`app.iia.query_moniker`	Blank (default)

Allow tap-over of running session

☑ Enabled (Default) - Another user can take over the device even when a user is still logged in. The session of the previous user will be disconnected, or the previous user will be logged off. (Default)

☐ Disabled - There is no possibility for another user to log in while a user is logged in.

> Related IAFI settings

- **Follow Policies and Workflows > Default on how to leave a follow policies session**
- **Auth Only > default on how to leave a AuthOnly session**
- **Auth Only > When an endpoint is locked**

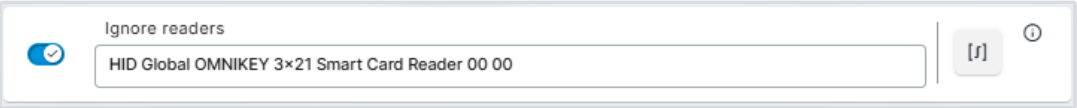
Registry	Value
`app.iia.allow_tapover`	*True* (default), False

Ignore readers

This is only needed when an embedded smartcard (PCSC) reader is built into the IGEL device (ex: thin client, laptop) or an external keyboard. The agent recognizes the PCSC reader and displays it as a proximity reader on the IAFI login screen even though you can't tap a badge.

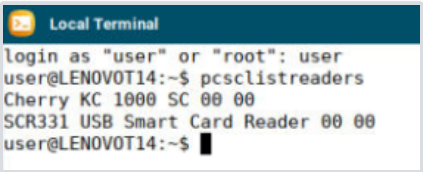
To ignore the PCSC reader:

- Enable the **Ignore readers** setting in the IAFI profile
- on the device, open a terminal, log in as user or root.
- At the command prompt, type: **pcsclistreaders**
- The output should display the name of the PCSC reader(s) and the slot numbers
  - For example, the output may look like this: **HID Global OMNIKEY 3x21 Smart Card Reader 00 00**
  - Copy the output and paste it into the "Ignore readers" field



NOTE: if there are multiple PCSC readers, they will be displayed as a list. You can add both readers separated by a semicolon (;)

- In this example, you see both a keyboard device and USB smartcard reader.



- To add both of these devices to the Ignore readers field, it would look like this:
  - **Cherry KC 1000 SC 00 00;SCR331 USB Smart Card Reader 00 00**

Registry	Value
`app.iia.ignore_readers`	Blank (default)

Logging Verbosity

There are three IAFI logging options to choose from:

- **info** (default)
- **debug**
- **error**

> See this IAFI Article for more information on enabling debug logging.
> How to Enable and Export IAFI Debug Logging for Troubleshooting[103]

Registry	Value
`app.iia.log_level`	*info* (default), debug, error

Configuring Follow Policies and Workflows

Default on how to leave a follow policies session

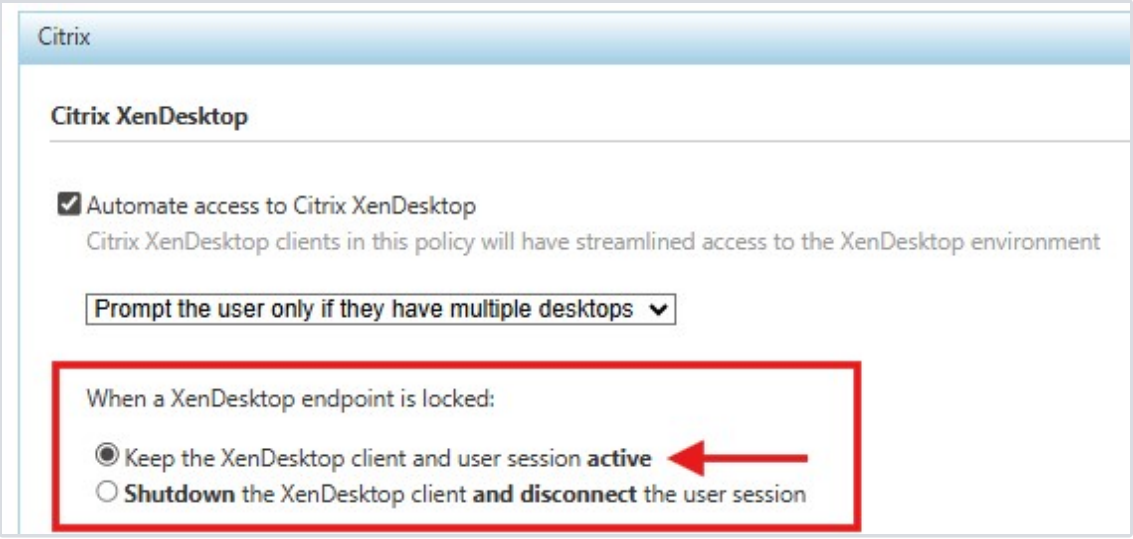
Defines the behavior of the IGEL Agent for Imprivata when users tap their cards to leave the session.

Possible options:

- **disconnect**: The user is disconnected from the session. (Default)
- **logoff**: The user is logged out of the session.

Registry	Value
`app.iia.exit_default.followvdi`	*disconnect* (Default), logoff

> Starting with IAFI 1.3.0 and higher, there is a new feature that supports the Imprivata VDA Computer Policy setting to keep a session active when the endpoint is locked as shown in this example.



103. https://kb.igel.com/en/igel-apps/current/how-to-enable-and-export-iafi-debug-logging-for-tr

IMPORTANT: In Follow Policies Mode, IAFI 1.3.0 and higher will honor this setting if it is enabled.

NetScaler COOKIEINSERT

Supports the Citrix NetScaler COOKIEINSERT Session Persistence method for Load Balanced sessions.

Session persistence maintains the connection between an endpoint and the Citrix Storefront after load balancing is performed. A common way to maintain session persistence is to use the endpoint source IP address. However, customers who use Network Address Translation (NAT) in front of a NetScaler load balancer cannot use this persistence method, because endpoints appear to have the same IP address at the load balancer.

Those customers must use the NetScaler COOKIEINSERT session persistence method. This method causes the NetScaler to insert a cookie into client requests, which the NetScaler uses to track the server to which the connection belongs.

See this Imprivata documentation article[104] for reference.

☑ enabled - Enter the COOKIEINSERT value from the NetScaler. Example: **IGELOS12**

☐ disabled (default)

Make sure that the cookie names are the same on the NetScaler and the IGEL endpoints.

Registry	Value
`app.iia.cookieinsert`	*Blank* (default)

Hide apps on the Citrix Chooser

☑ enabled (default)

☐ disabled

This setting filters out Citrix Apps in the IAFI Resource Chooser. Only Citrix desktops will be shown. When disabled, the IAFI Resource Chooser will display Desktops and Apps that a user is entitled to. **NOTE:** This setting is similar to how the Imprivata PIE agent Chooser works with XenDesktop VDA. Only Citrix desktop icons will appear if the user has multiple resources.

104. https://docs.imprivata.com/onesign/content/topics/imprivataplatform/vda/xendesktop/vdacitrixxendesktop.html?Highlight=COOKIEINSERT

Registry	Value
app.iia.hide_citrix_apps_on_chooser	*True* (default), False

Hide apps on the Horizon Chooser

☑ enabled (default)

☐ disabled

> This setting filters out Horizon Apps in the IAFI Resource Chooser. Only Horizon desktops will be shown. When disabled, the IAFI Resource Chooser will display Horizon Desktops and Apps that a user is entitled to. **NOTE:** This setting is similar to how the Imprivata PIE agent Chooser works with Omnissa Horizon VDA. Only Horizon desktop icons will appear if the user has multiple resources.

Registry	Value
app.iia.hide_horizon_apps_on_chooser	*True* (default), False

Launch a sole Horizon Desktop without prompting

☑ enabled (default)

☐ disabled

> For users that only have a single Horizon desktop entitlement, IAFI will launch that resource automatically when they log in. No IAFI resource chooser will appear.
> **NOTE:** This setting is similar to how the Imprivata PIE agent works with Horizon VDA for users with just a single desktop.

Registry	Value
app.iia.launch_sole_horizon_desktop	*True* (default), False

Preselect the Citrix resource if there are multiple

☐ enabled

☑ disabled (default)

Enter the name of the Citrix resource that should be started. Examples: "Calculator", "Notepad", “Windows 11”.

If this field is blank, and there are multiple Citrix resources, the IAFI Resource Chooser is shown to the user.

This is setting that can “bypass” the VDA Policy settings and automatically start a specific resource if required. A good use case is for a “Location Based Override” where in that specific area, you want to always launch a specific resource regardless of the VDA policy settings.

Registry	Value
`app.iia.preselect_resource.citrix`	*Blank* (default)

Preselect the Horizon resource if there are multiple

☐ enabled

☑ disabled (default)

Enter the name of the Horizon resource that should be started. Examples: "Calculator", "Notepad", “Windows 11”.

If this field is blank, and there are multiple Horizon resources, the IAFI Resource Chooser is shown to the user.

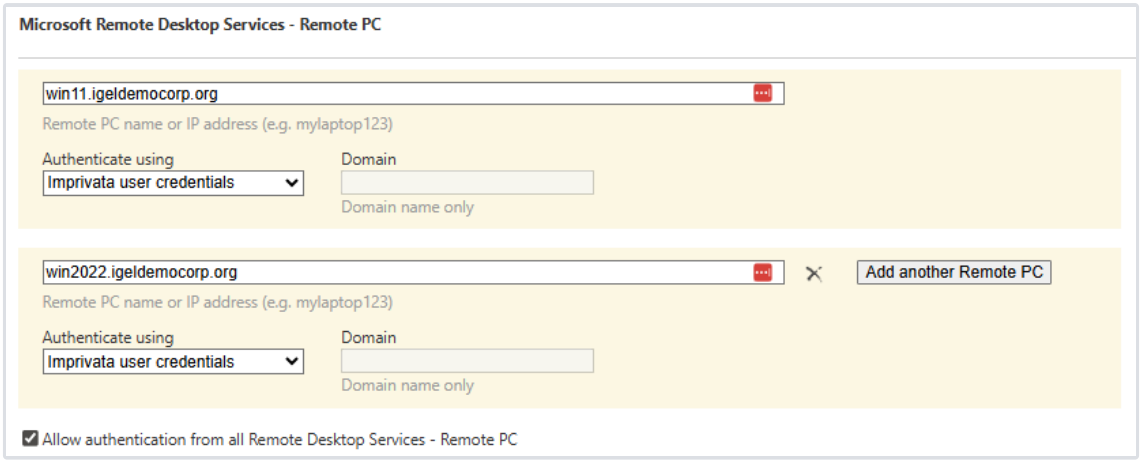
This is setting that can “bypass” the VDA Policy settings and automatically start a specific resource if required. A good use case is for a “Location Based Override” where in that specific area, you want to always launch a specific resource regardless of the VDA policy settings.

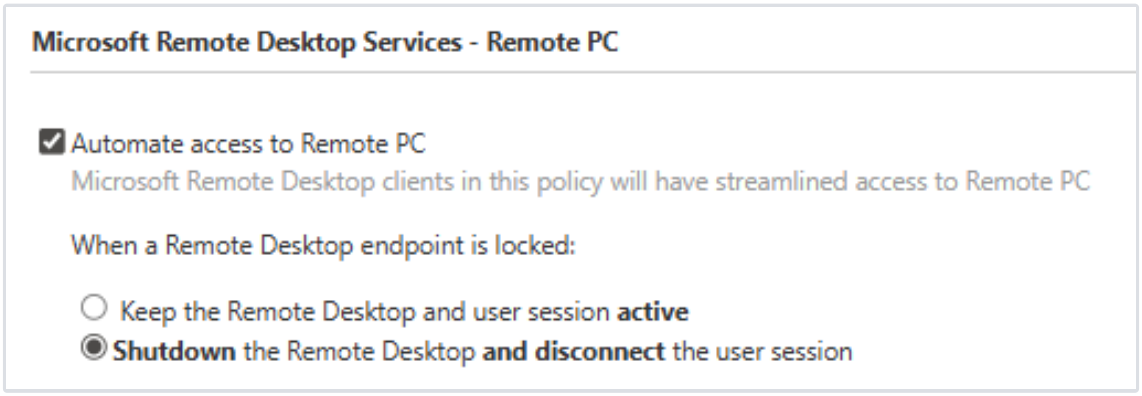
Registry	Value
`app.iia.preselect_resource.horizon`	*Blank* (default)

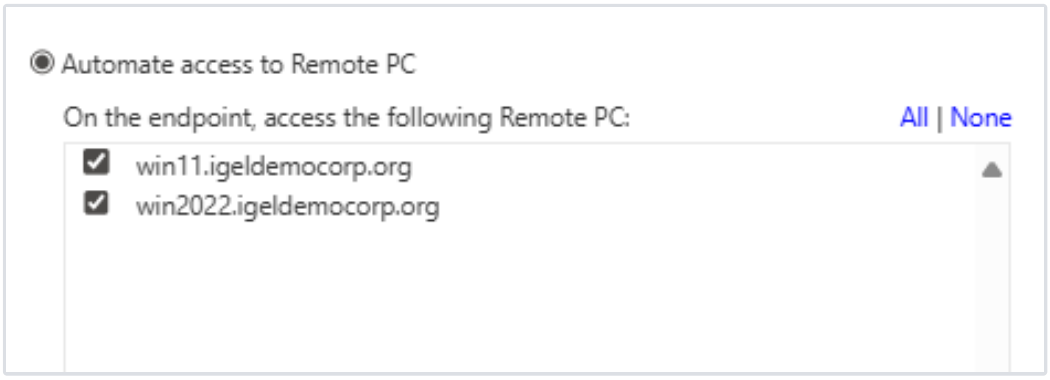
Preselect the Microsoft resource if there are multiple

IMPORTANT: This setting is not currently supported for Microsoft resources.

In Follow Policies and Workflows mode, IAFI only supports the Imprivata VDA policy for **Microsoft Remote Desktop Services - Remote PC** as seen below in the Imprivata Global VDA, Computer and User Policy settings.







IMPORTANT:

- If a user policy has more than one Remote PC enabled, IAFI will autolaunch the first one listed.
- In the example above, the first resource is win11.igeldemocorp.org[105]

105. http://win11.igeldemocorp.org

☐ enabled

☑ disabled (default)

Registry	Value
`app.iia.preselect_resource.microsoft`	*Blank* (default)

Configuring Auth Only

default on how to leave a AuthOnly session

Defines the behavior of the IGEL Agent for Imprivata when users tap their cards to leave the session.

Possible options:

- **disconnect**: The user is disconnected from the session.
- **logoff**: The user is logged out of the session. (Default)

Registry	Value
`app.iia.exit_default.authonly`	*logoff* (default), disconnect

When an endpoint is locked

> Starting with IAFI 1.3.0 and higher, there is a new feature for **Auth Only mode** to keep a session active (vs. disconnected or logged off) when the endpoint is locked. When enabled, this keeps the user session active if the endpoint is locked via Badge Tap, Hotkey or Walkaway Security.
> **IMPORTANT:** The IAFI Full Lockscreen should be enabled when using this setting in order to protect what is in use on the remote session (ex: virtual desktop with financial information or a patient record that requires privacy protection).

☐ Shutdown and disconnect the session (default)

☑ Keep the session active

Registry	Value
`app.iia.close_on_lock`	*Shutdown and disconnect the session* (default), Keep the session active

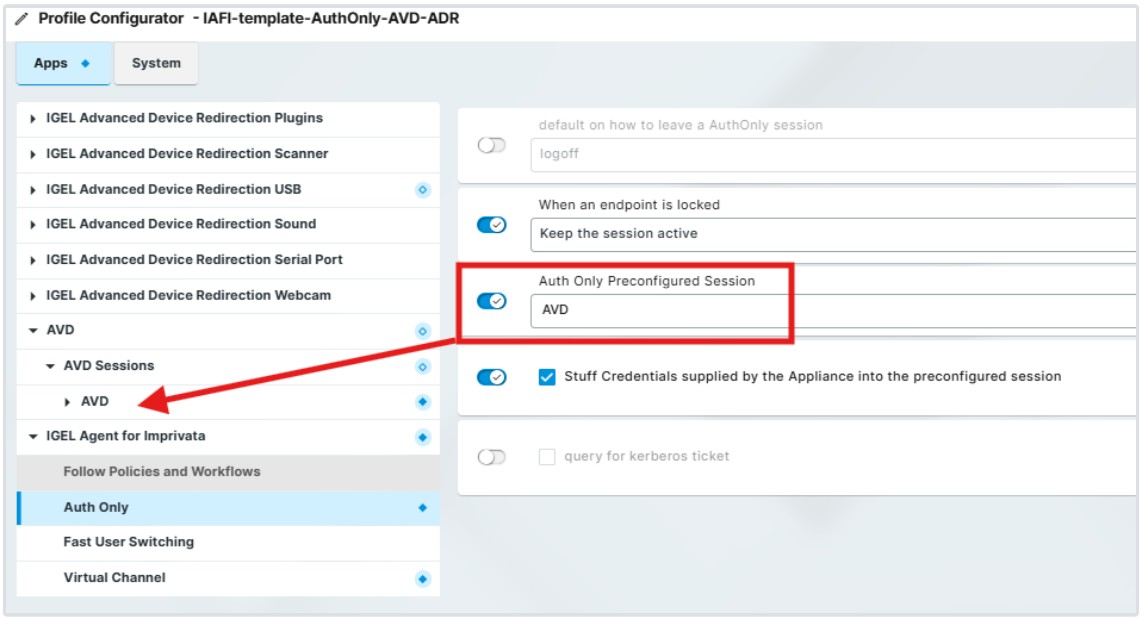
Auth Only Preconfigured Session

☐ enabled

☑ disabled (default)

This is a required setting.

IMPORTANT: Enter the name of the preconfigured session resource that is to be started when the user has logged in.



Supported Auth Only session types: AVD, Windows 365, Citrix, Horizon

Stuff credentials supplied by the appliance into the preconfigured session

☑ The credentials passed on from the Imprivata appliance will be stuffed into the session defined under **Auth only preconfigured session**. (Default)

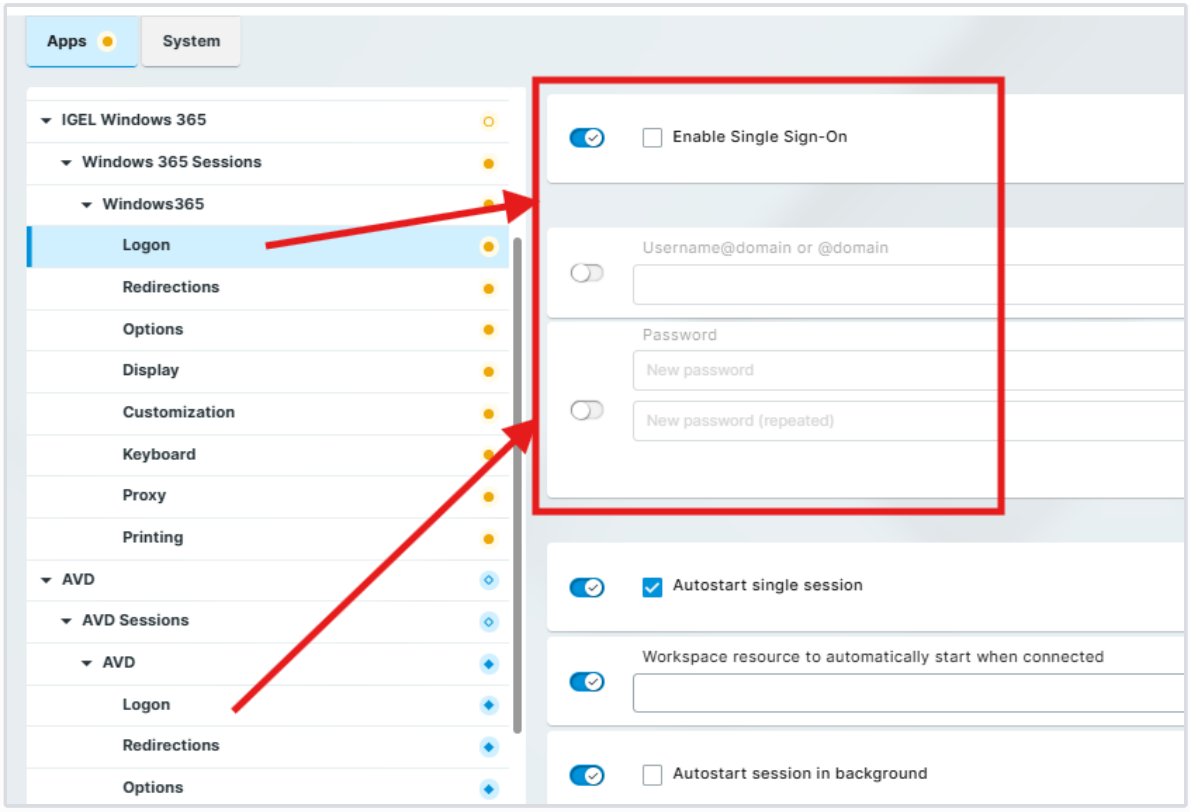
☐ The user will be prompted for the credentials by the session itself.

To make the credential stuffing possible, the credentials **must not be predefined** for the preconfigured session. Therefore set the relevant session credential parameters to inactive so that they are not controlled by the UMS profile.

Microsoft AVD or Windows 365

For an **AVD or Windows 365 session**, the settings should look like this:

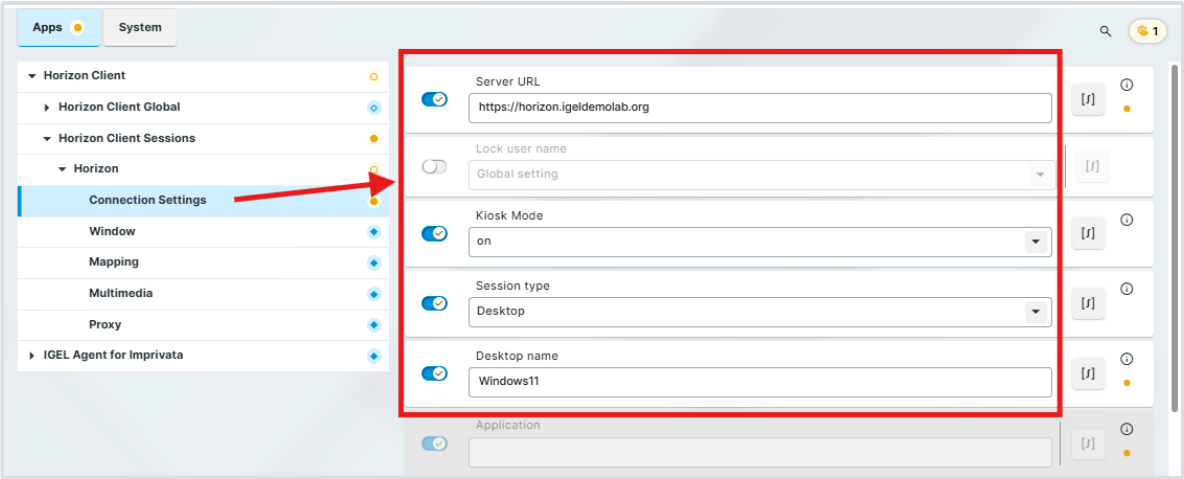
- **Apps > AVD > AVD Sessions > [session name] > Logon**:
- **Apps > IGEL Windows 365 > Windows 365 Sessions > [session name] > Logon**:
  - Disable the “Enable Single Sign-On” setting
  - Set the Username@domain or @domain and Password parameters to inactive



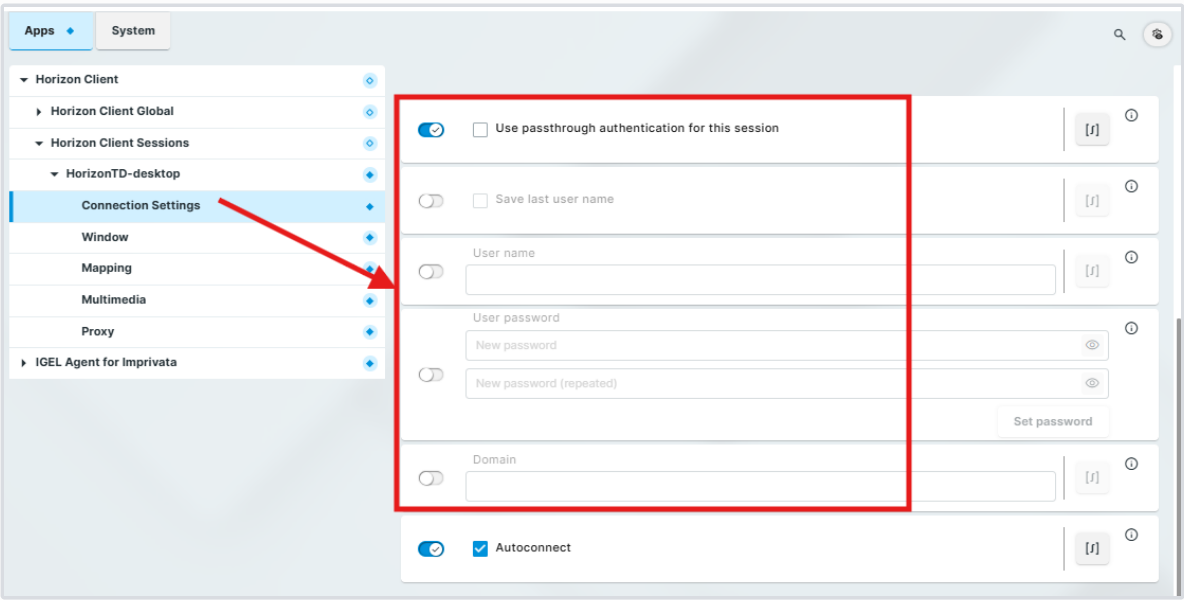
Omnissa Horizon

For a **Horizon Client Auth Only session**, the settings should look like this:

- **Apps > Horizon Client > Horizon Client Sessions > [session name] > Connection Settings**:
  - **Server URL**: Enter the FQDN of the Horizon server
    - ex: https://horizon.igeldemolab.org
  - **Lock user name**: Disable or set inactive
  - **Kiosk mode:** Enable and set to **'on'**
    - this setting uses a noninteractive mode for the Horizon Client so the user doesn't see a login prompt
  - **Session type** (you can only choose one session type)
    - Select **Desktop** (if connecting to a Horizon Desktop session)
      - **OPTIONAL: Desktop name**
        - If you want to auto launch a specific Horizon desktop, enter the name of the desktop
          - ex: Windows11
    - Select **Application** (if connecting to Horizon Applications)
      - **OPTIONAL: Application**
        - If you want to auto launch a specific Horizon application, enter the name of the app
          - ex: Outlook



- **Use passthrough authentication for this session:** Disable or set inactive
- **Save last user name:** Disable or set inactive
- Set inactive:
  - **User name**
  - **User password**
  - **Domain**
- **Autoconnect:** Enable
  - this will automatically launch the desktop or application resource specified in the Desktop or Application name setting

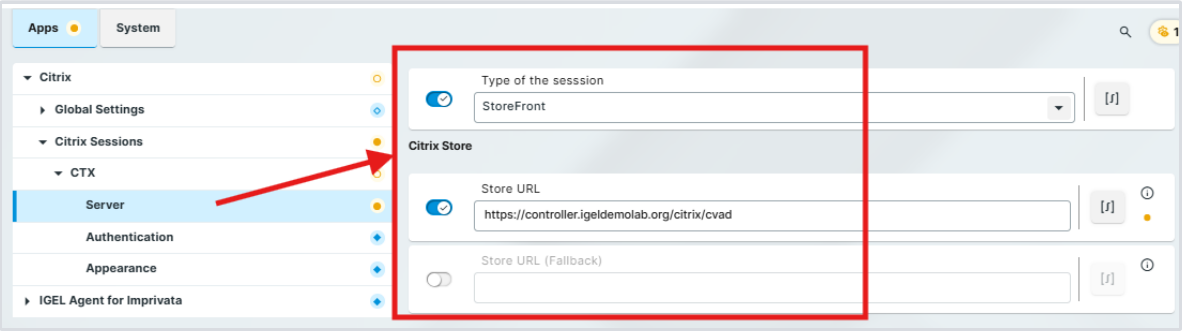


Citrix Workspace App

For a Citrix Workspace App Auth Only session, the settings under **Apps > Citrix > Citrix Sessions > [session name] > Server** should look like this:

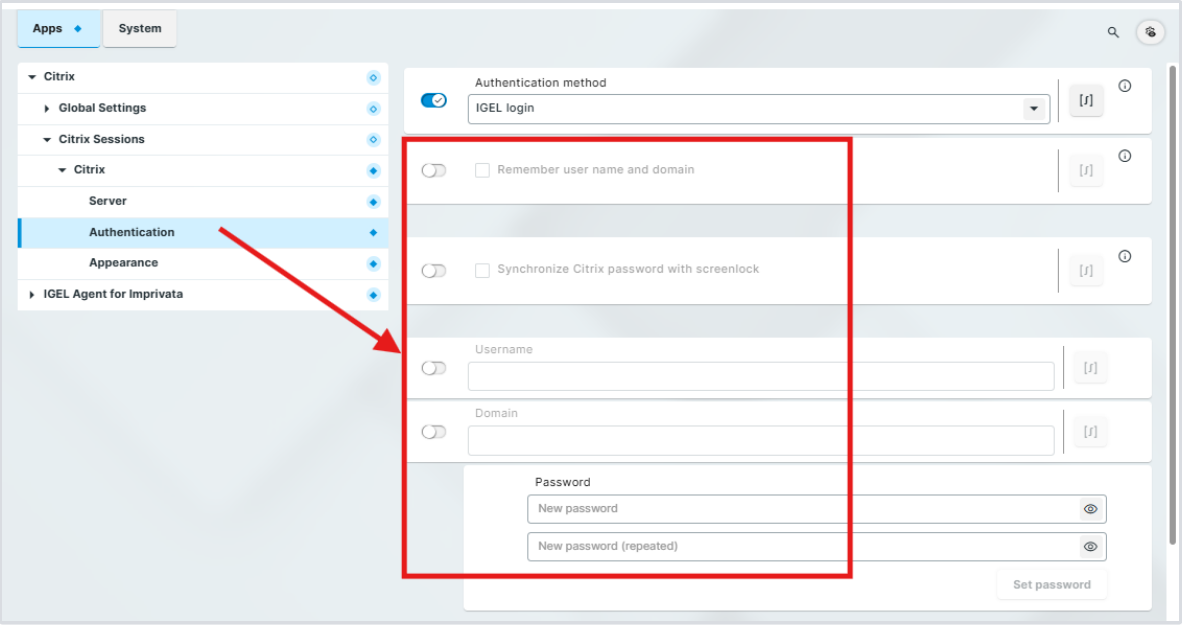
- **Type of the session:** Select **Storefront**
- **Citrix Store:** Enter the FQDN URL for the Citrix Store

- ex: https://controller.igeldemolab.org/citrix/cvad

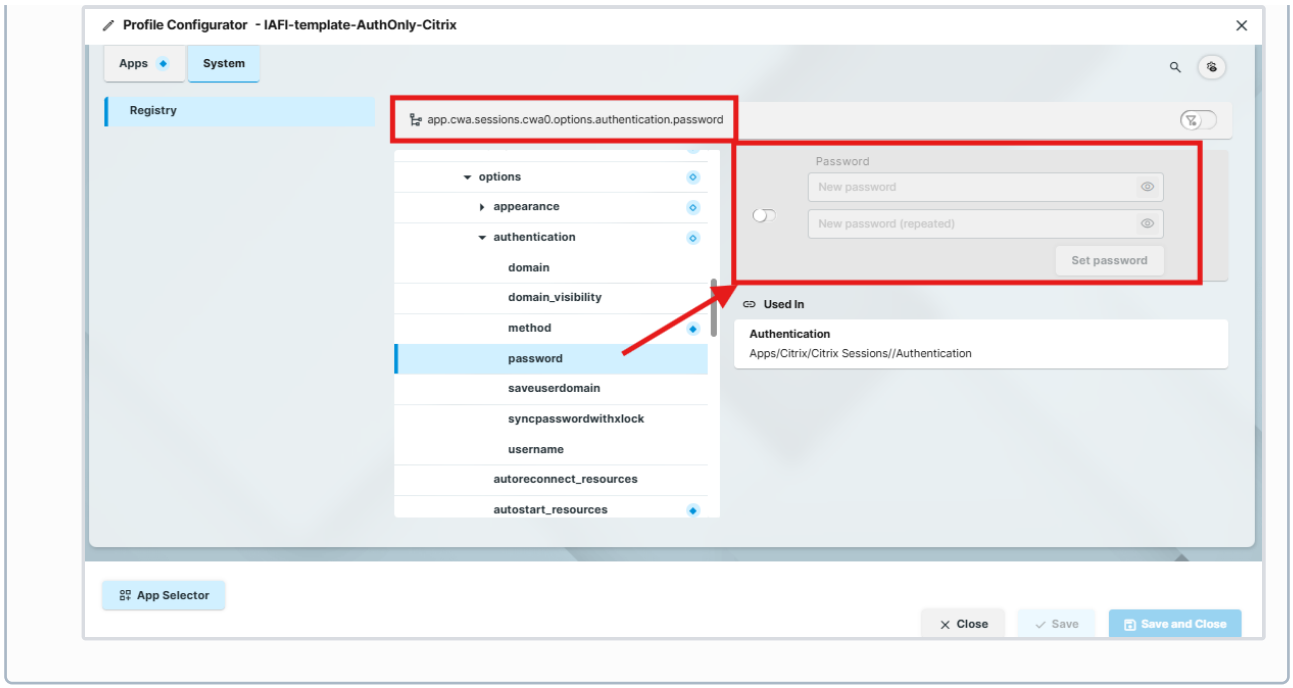


For a Citrix Client Auth Only session, the settings under **Apps > Citrix > Citrix Sessions > [session name] > Authentication** should look like this:

- **Authentication Method:** Set to **IGEL Login**
- **Remember user name and domain:** Disable or set to inactive
- **Synchronize Citrix password with screenlock:** Disable or set to inactive
- Set inactive:
  - **Username**
  - **Domain**
  - **Password**



IMPORTANT: For Citrix Auth Only, you have to disable the Password field in the application registry.



Query for Kerberos ticket

> ⚠ This is an experimental feature being investigated for future workflows. It is disabled by default. Generally, this option can be recommended for a Chromium session in an on-premises environment. When Azure Entra ID is used, this might result in a delay due to a timeout.

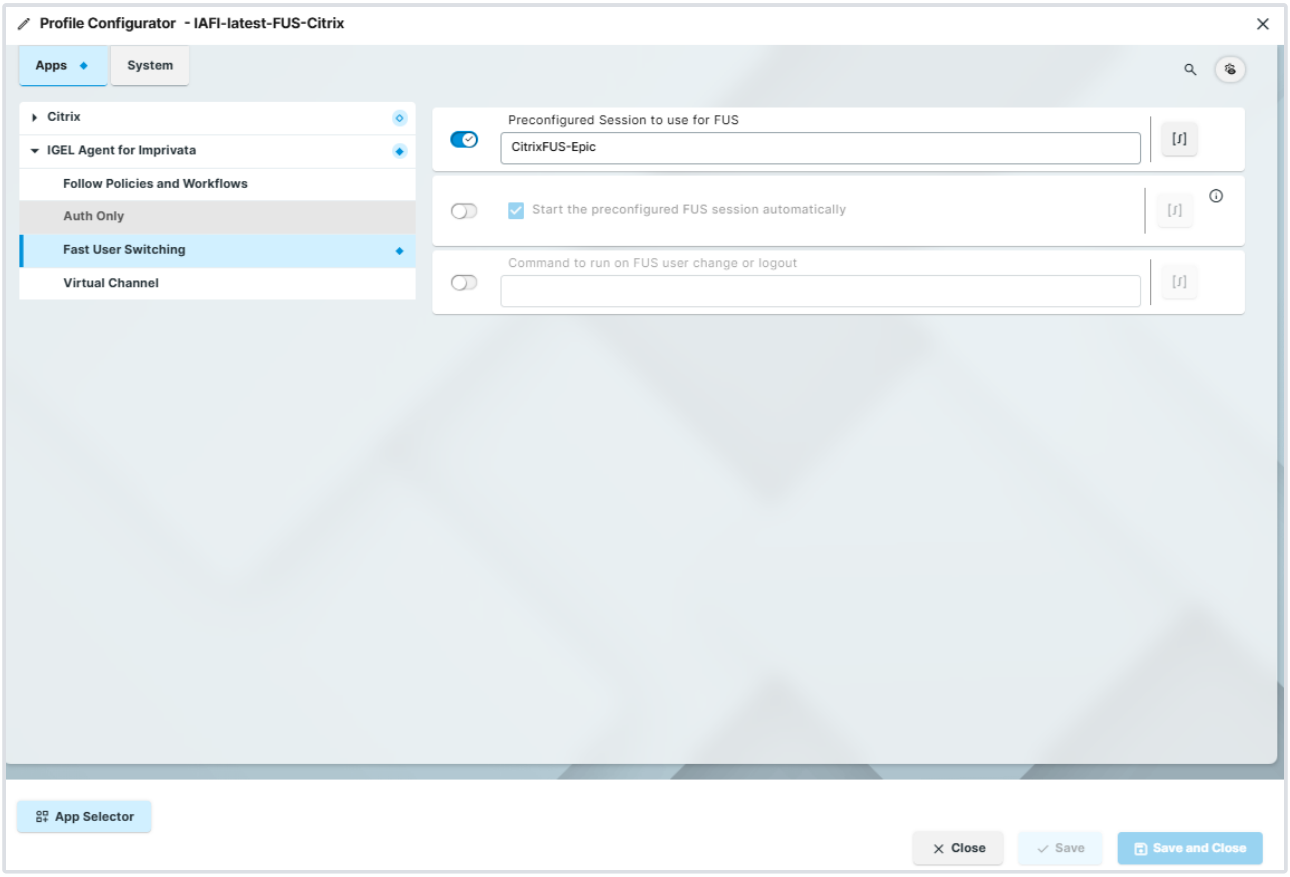
☑ After successful authentication with the IGEL Agent for Imprivata, the agent requests a ticket from the local Active Directory (AD).

☐ No Kerberos ticket will be requested. (default)

Configuring Fast User Switching (FUS)

> ℹ Starting with the IAFI 1.0.0 version, we changed the FUS configuration to support standalone IGEL sessions (ex: Citrix, Horizon, AVD).
> The FUS configuration is primarily for Imprivata Epic workflows with an IAFI lock screen used to obscure the session.

1. In the profile configurator, go to **Apps > IGEL Agent for Imprivata > Fast User Switching**.
2. Edit the settings according to the FUS workflow you are configuring. The parameters are described as follows:



Preconfigured Session to use for FUS

Enter the name of a preconfigured session.

> The preconfigured session would be for launching Epic or a Published Desktop. This session would be configured using generic credentials (ex: HOSTNAME).

Start the preconfigured FUS session automatically

☑ Enabled (Default)

☐ Disabled

> With this setting enabled, when IAFI starts, it will automatically launch the preconfigured session. Once the virtual channel is established between IAFI and the Imprivata agent on the remote session, IAFI will show an authentication dialog indicating the user can log in.
> Once the user logs into IAFI, their identity will be passed over the virtual channel to log the user into Epic

Command to run on FUS user change or logout

Enter a command that can be used to close a local application such as Chromium when a user logs out or during a user switch.

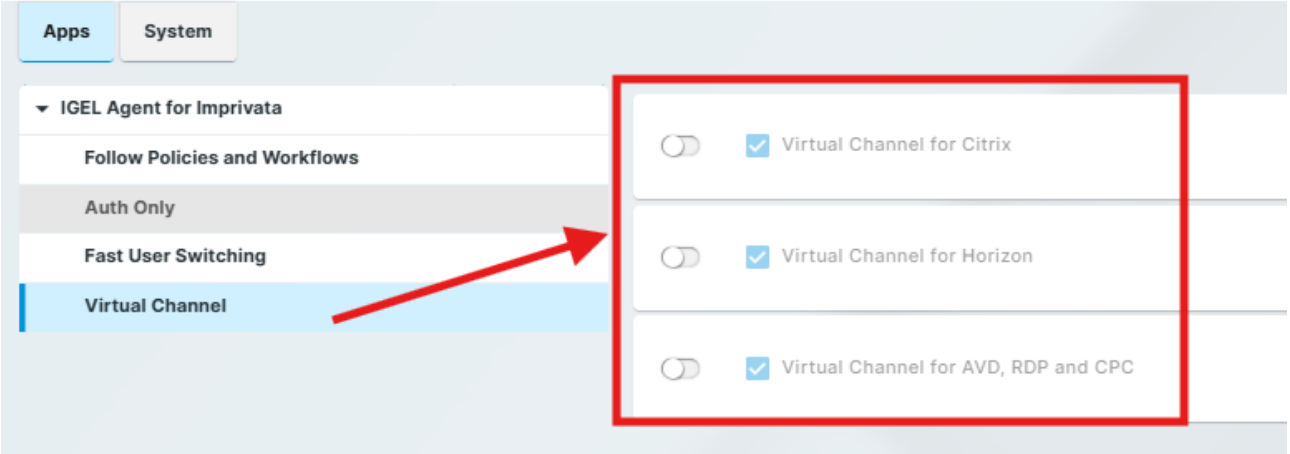
Configuring Virtual Channel

By default, all of the Imprivata Virtual Channel settings are enabled for the supported session types (Citrix, Horizon, Microsoft AVD, Windows 365 Cloud PC, RDP).

Supported protocols are ICA, RDP, Horizon Blast and PCoIP.

1. In the profile configurator, go to **Apps > IGEL Agent for Imprivata > Virtual Channel**.

2. Edit the settings according to your needs.



The parameters are described as follows:

Virtual Channel for Citrix

☑ Imprivata's virtual channel is used for the Citrix session. (Default)

☐ Imprivata's virtual channel is disabled for the Citrix session.

Virtual Channel for Horizon

☑ Imprivata's virtual channel is used for the Horizon session. (Default)

☐ Imprivata's virtual channel is disabled for the Horizon session.

Virtual Channel for AVD, RDP and CPC

☑ Imprivata's virtual channel is used for the AVD, RDP, or CPC session. (Default)

☐ Imprivata's virtual channel is disabled for the AVD, RDP, or CPC session.

Registry	Value
`app.iia.vc.avd`	Virtual Channel for AVD, RDP and CPC - *True* (default) / False
`app.iia.vc.citrix`	Virtual Channel for Citrix - *True* (default) / False
`app.iia.vc.horizon`	Virtual Channel for Horizon - *True* (default) / False

Primary Authentication Using Fingerprint (IAFI 1.4.0+)

Starting with the latest IAFI release, IGEL OS provides support for Imprivata fingerprint authentication over the Virtual Channel (VC). This enables organizations to offer a fast and secure biometric authentication flow similar to Imprivata PIE.

Supported Fingerprint Readers

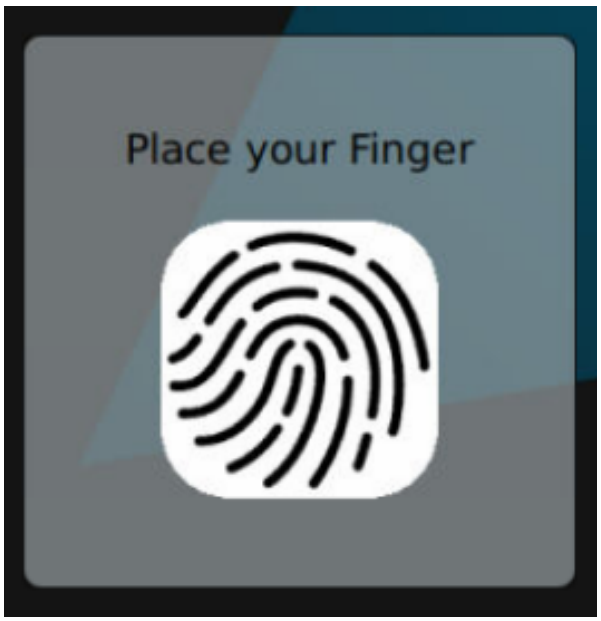
IAFI currently supports Imprivata EPCS-certified readers only. Devices of the following vendors are allowed:

- EIKON
- UPEK
- DIGITAL PERSONAS

Fingerprint Login Tile

IAFI adds a dedicated fingerprint authentication tile on the login screen, similar to the PIE agent.

This tile appears whenever fingerprint capability is enabled via policy:



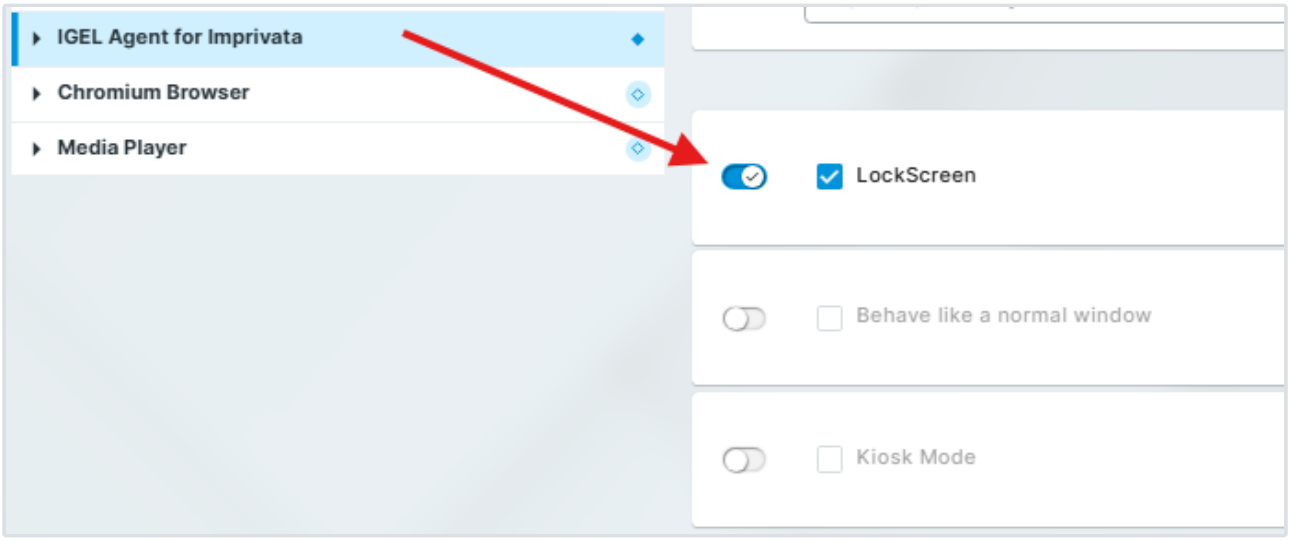
Virtual Channel Support (Fingerprint)

The Virtual Channel (VC) for fingerprint is implemented from IAFI 1.5.0.

Resource Chooser Display Options (IAFI 1.5.0+)

IAFI 1.5.0 introduces enhancements to the Follow Imprivata Policies and Workflows configuration[106]. Specifically, the **Resource Chooser** window, enabling a lock-screen (full-screen) mode identical to the PIE agent experience. This update addresses customer requirements around preventing access to the IGEL desktop before session launch.

→ To enable the full-screen chooser option, go to **Apps > IGEL Agent for Imprivata** and enable **LockScreen**.



Available Modes

Lock-Screen (Full-Screen) Mode

- This mirrors how the Imprivata PIE agent behaves when a user has multiple resources available (Desktops or Apps)
  - See this: Configuration of the IGEL Agent for Imprivata on IGEL OS[107]
- Blocks access to IGEL desktop
- The Resource Chooser shows only once after authentication
- Only displays in full screen if **no autostarted apps** are configured. This only applies if IAFI is in “follow policies” and the VDI is Citrix.

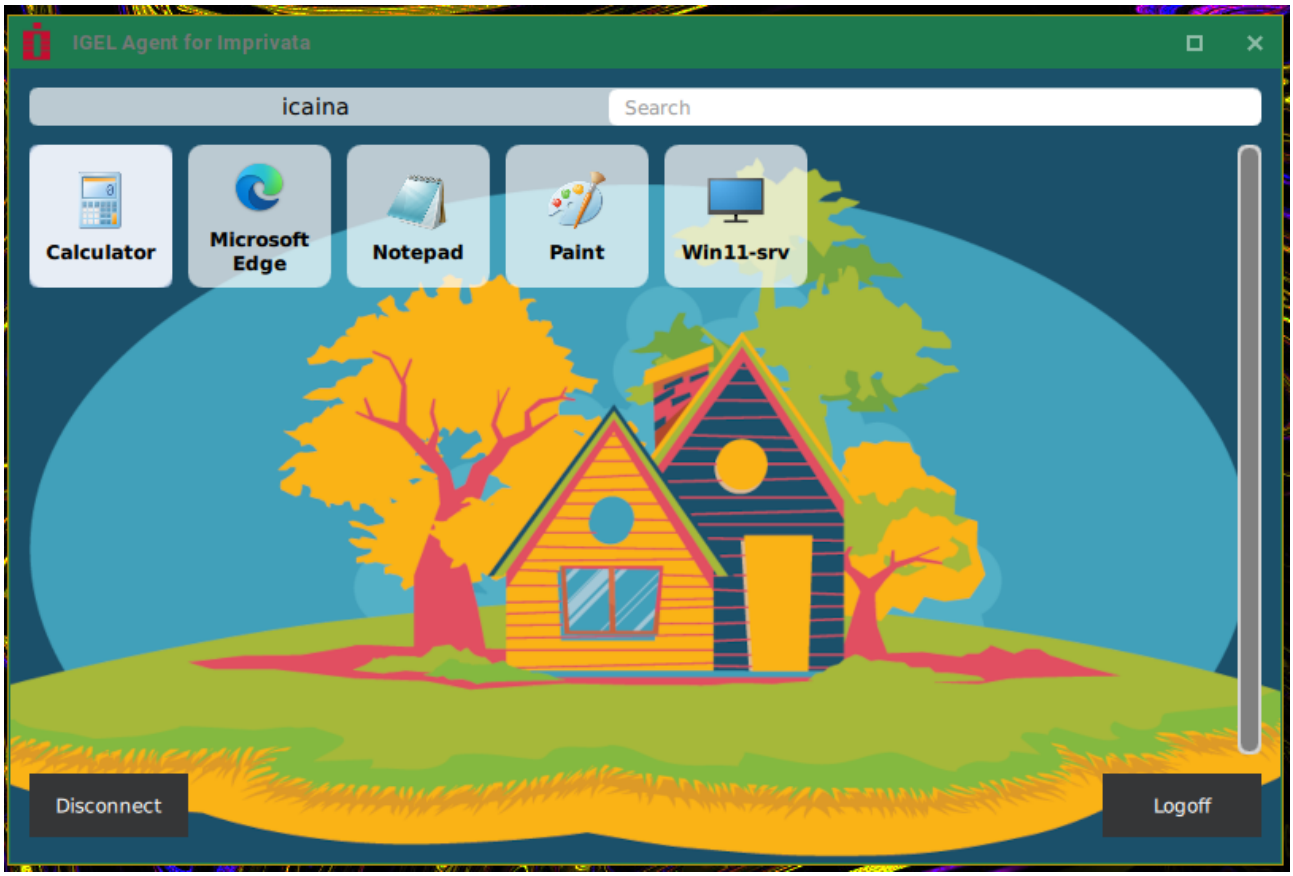
106. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringFollowPoliciesandWorkflows
107. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringFollowPoliciesandWorkflows



Windowed/Floating Mode

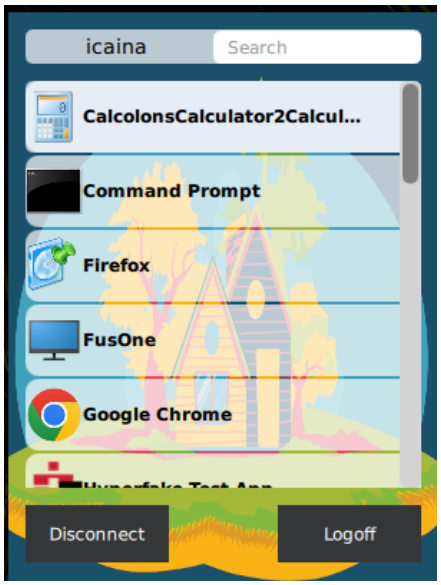
- This is the “Behave like a normal window” setting - see this: Configuration of the IGEL Agent for Imprivata on IGEL OS[108]
- If the Lockscreen is enabled, and Windowed mode is selected, once a user picks a resource to launch, the chooser will be available in the middle of the screen behind the resource launched.
- Can be used for secondary chooser appearances after login. This only applies if IAFI is in “follow policies” and the VDI is Citrix.

108. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringBasicSettings



Docked to IGEL Taskbar Mode

- This is the default chooser behavior if the Windowed Mode is not enabled.
- Traditional tray-style chooser showing the current logged in user, a search option and scroll bar.
- Can be used for secondary chooser appearances after login. This only applies if IAFI is in “follow policies” and the VDI is Citrix.


icaina
Search
CalcolonsCalculator2Calcul...
Command Prompt
Firefox
FusOne
Google Chrome
Disconnect
Logoff

IGEL Agent for Imprivata (IAFI) Articles

- Prevention/Troubleshooting: How to Prevent IAFI from Installing on IGEL OS 11 in Mixed Environments (see page 272)
- How to Enable and Export IAFI Debug Logging for Troubleshooting (see page 284)
- How to Enable Multiple Monitors for IGEL Agent for Imprivata (see page 294)
- How to Create a Profile to Restart the IGEL Agent for Imprivata (see page 297)
- Troubleshooting: Use the Card Reader's Former Configuration (see page 301)
- How to enable IAFI logon screen customizations (see page 302)
- IAFI Profile Templates (see page 306)
- How to use the IAFI Guest Login option (see page 317)

Prevention/Troubleshooting: How to Prevent IAFI from Installing on IGEL OS 11 in Mixed Environments

Background Information:

Prior to the release of IGEL OS 12, the earliest versions of the IGEL Agent for Imprivata were included in IGEL OS 11. Like with OS 12, the IAFI app still needed a license to enable the feature since we were still in an Early Access Program phase with a limited feature set. Starting in early 2024, all new IAFI features and fixes are within the OS 12 app, but due to the OS 11 architecture, the older version remains and could be activated if an IGEL Agent for Imprivata add-on license is installed.

What is the Risk?

After upgrading your licenses to Healthcare Plus and deploying the IAFI license broadly, some IGEL OS 11 devices might accept an IAFI license and then download and start the legacy Imprivata agent. If this is the case, the device will display unexpected Imprivata pop-ups.

This can be prevented by defining appropriate distribution conditions for the IGEL Agent for Imprivata license pack.

Environment

IGEL OS 11 and IGEL OS 12 devices are managed by the same Universal Management Suite (UMS)

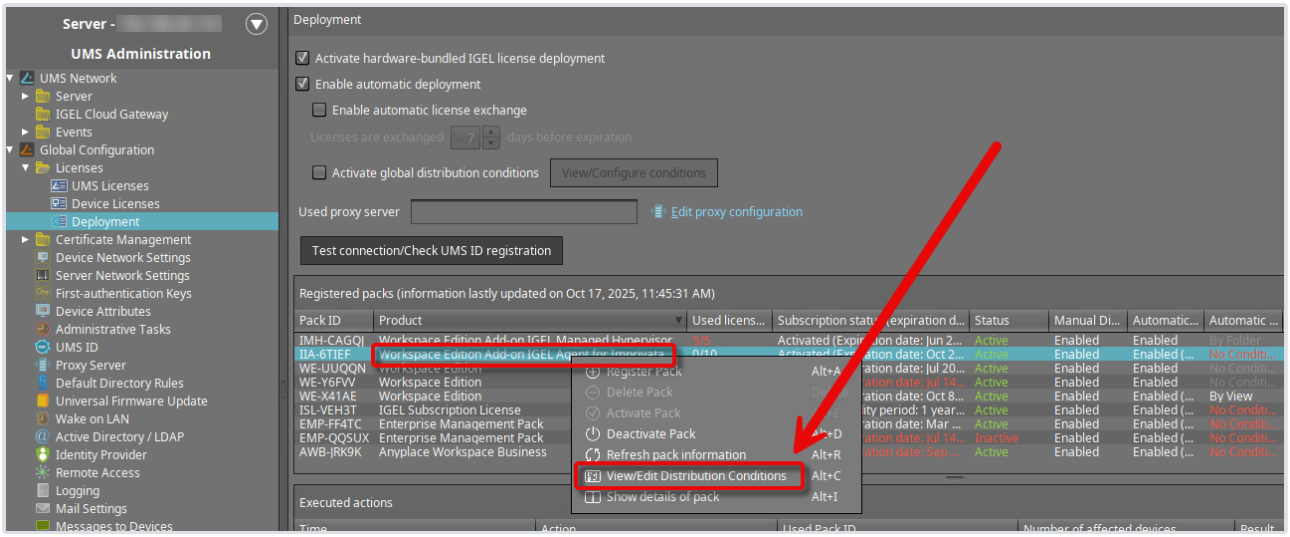
Preventing Unwanted License Assignment

To ensure that only selected devices get licenses from your IGEL Agent for Imprivata license pack, you can define appropriate distribution conditions. The license distribution conditions can be based on directories or on views.

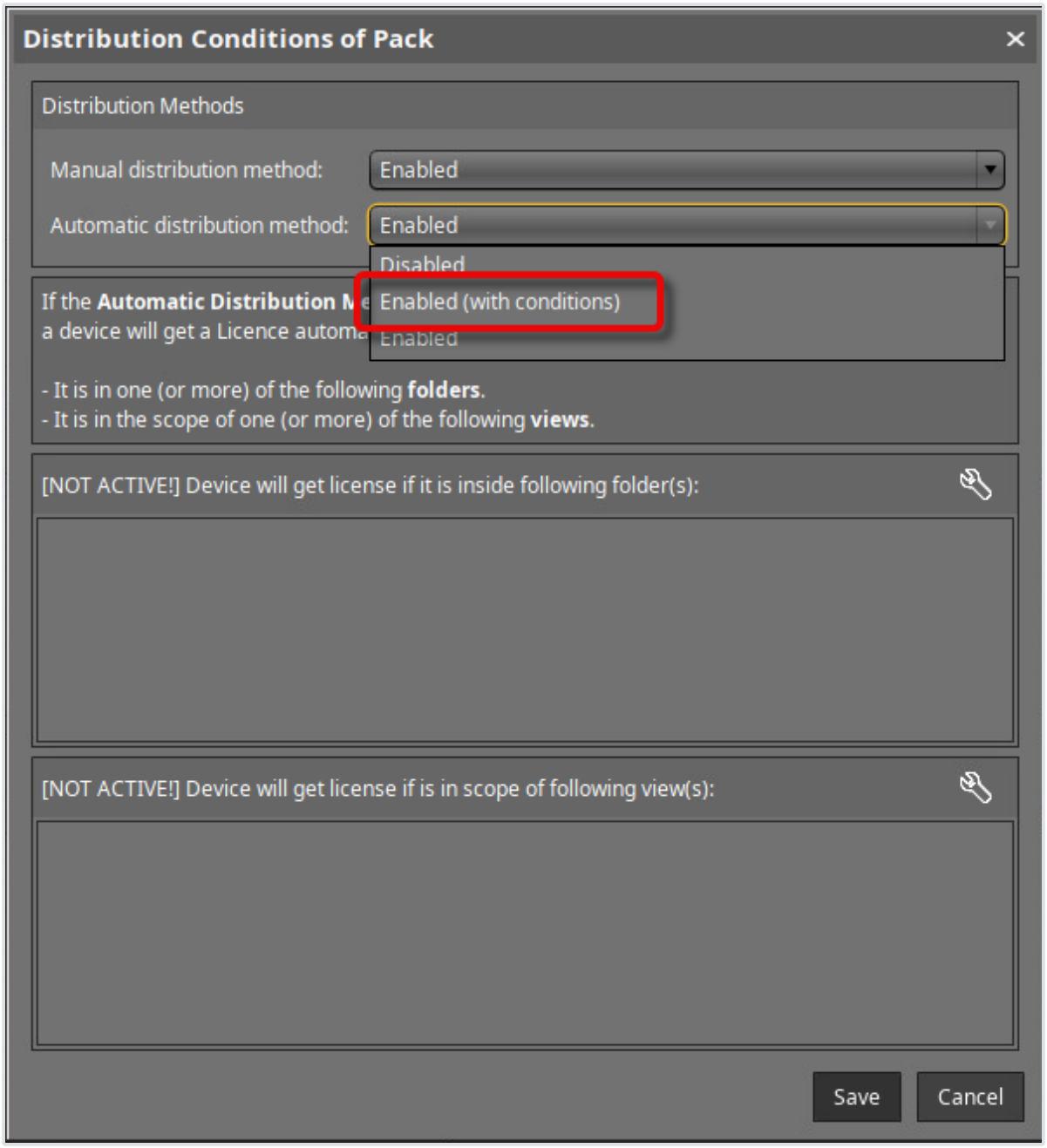
License Distribution Based on Directories

This method is feasible if all your devices are consistently separated by folders; that is, all devices that require an IGEL Agent for Imprivata licensing are located in folders that contain no IGEL OS 11 devices.

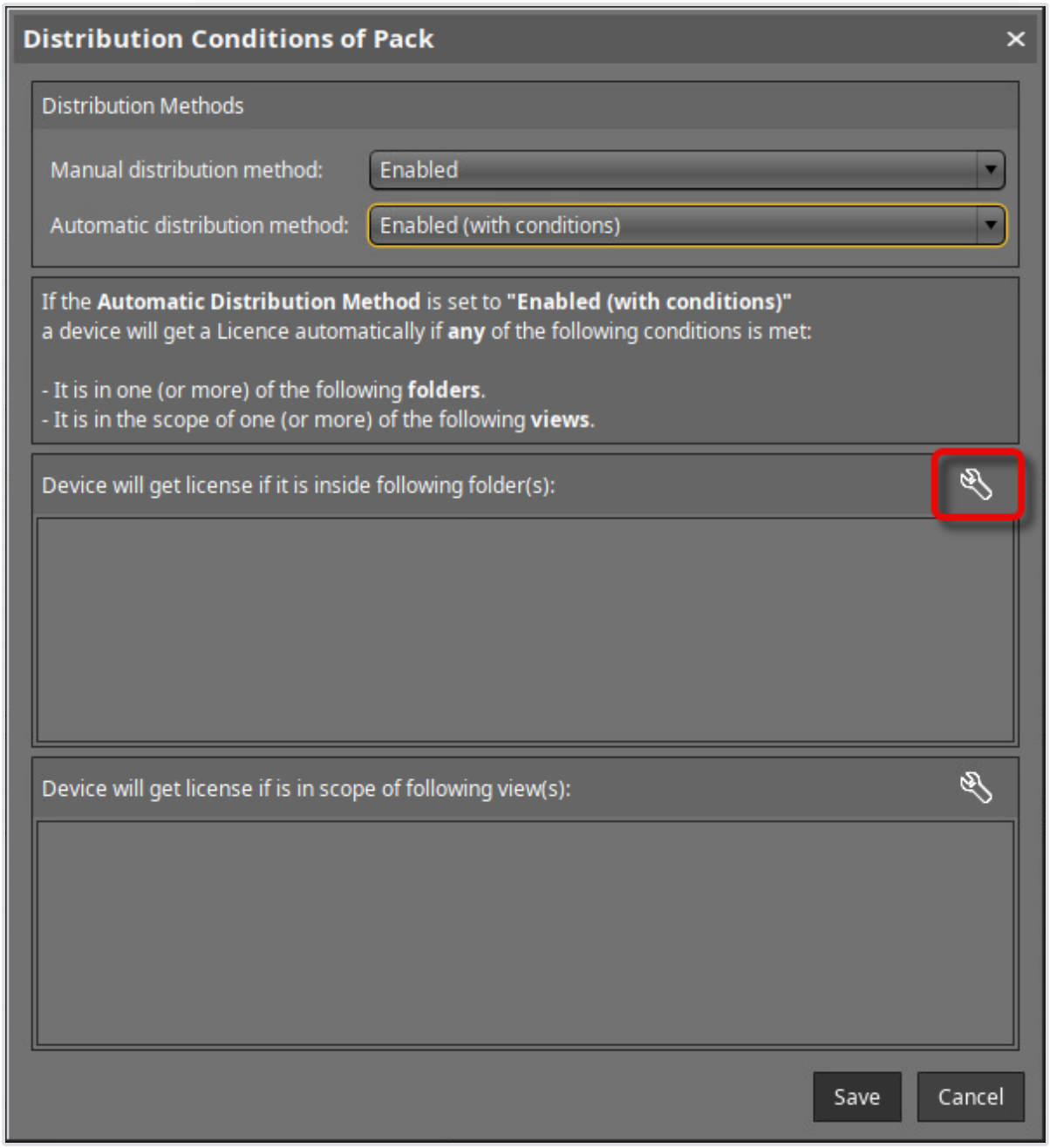
1. In the UMS Console, go to **UMS Administration > Global Configuration > Licenses > Deployment**, open the context menu for your IGEL Agent for Imprivata Product Pack, and select **View/Edit Distribution Conditions**.



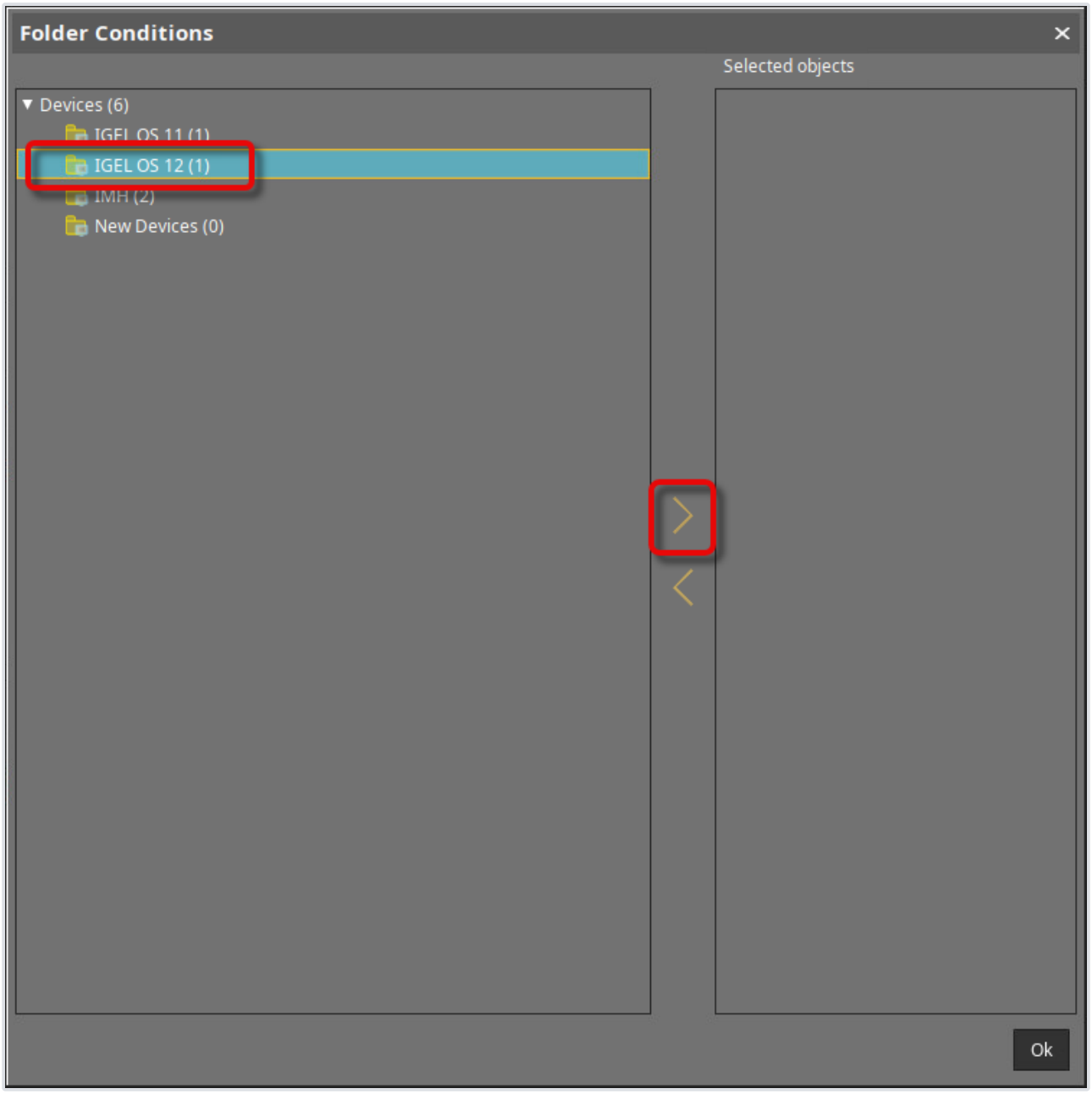
2. Set **Automatic distribution method** to **Enabled (with conditions)**.

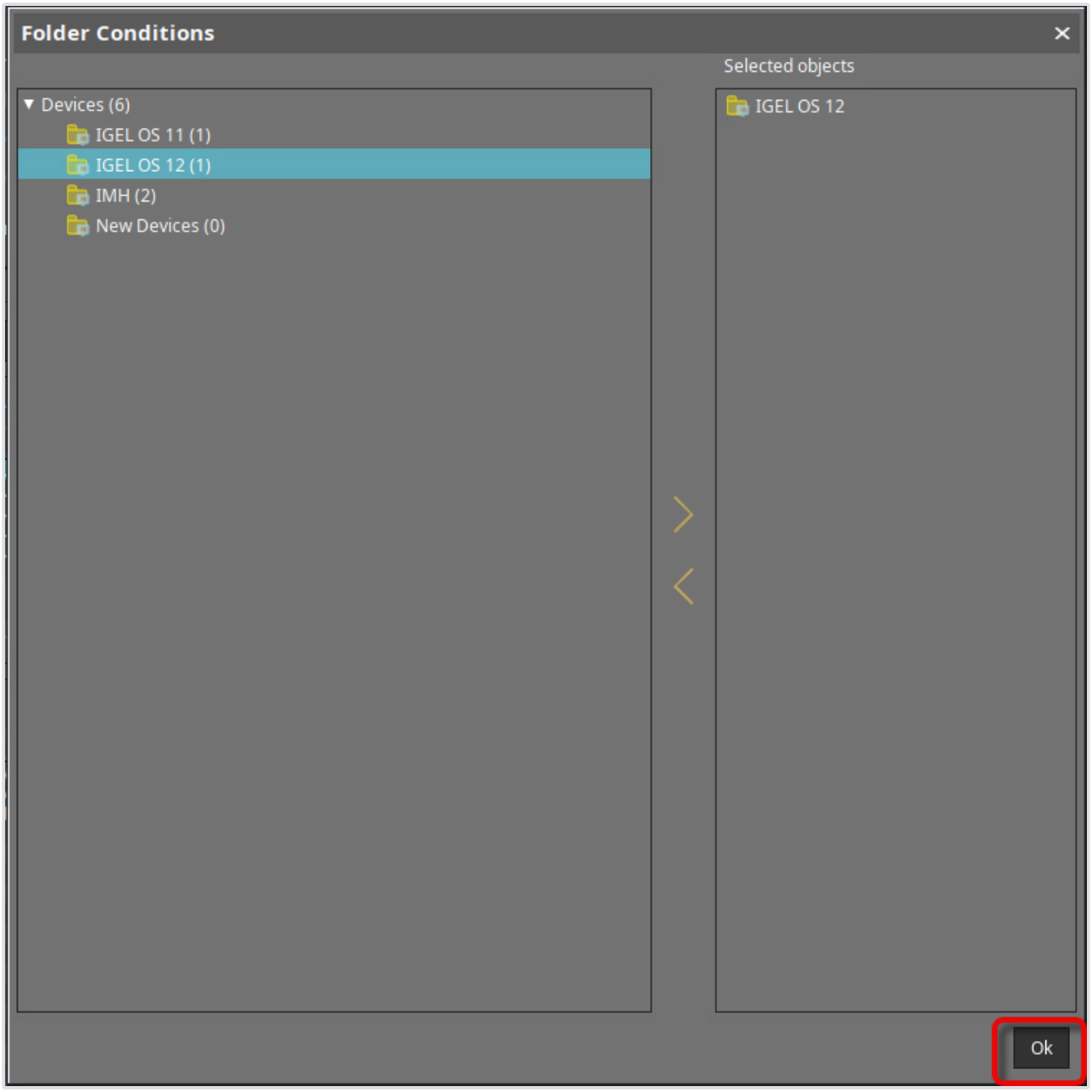


3. Click the wrench symbol next to **Device will get license if it is inside following folder(s)**.

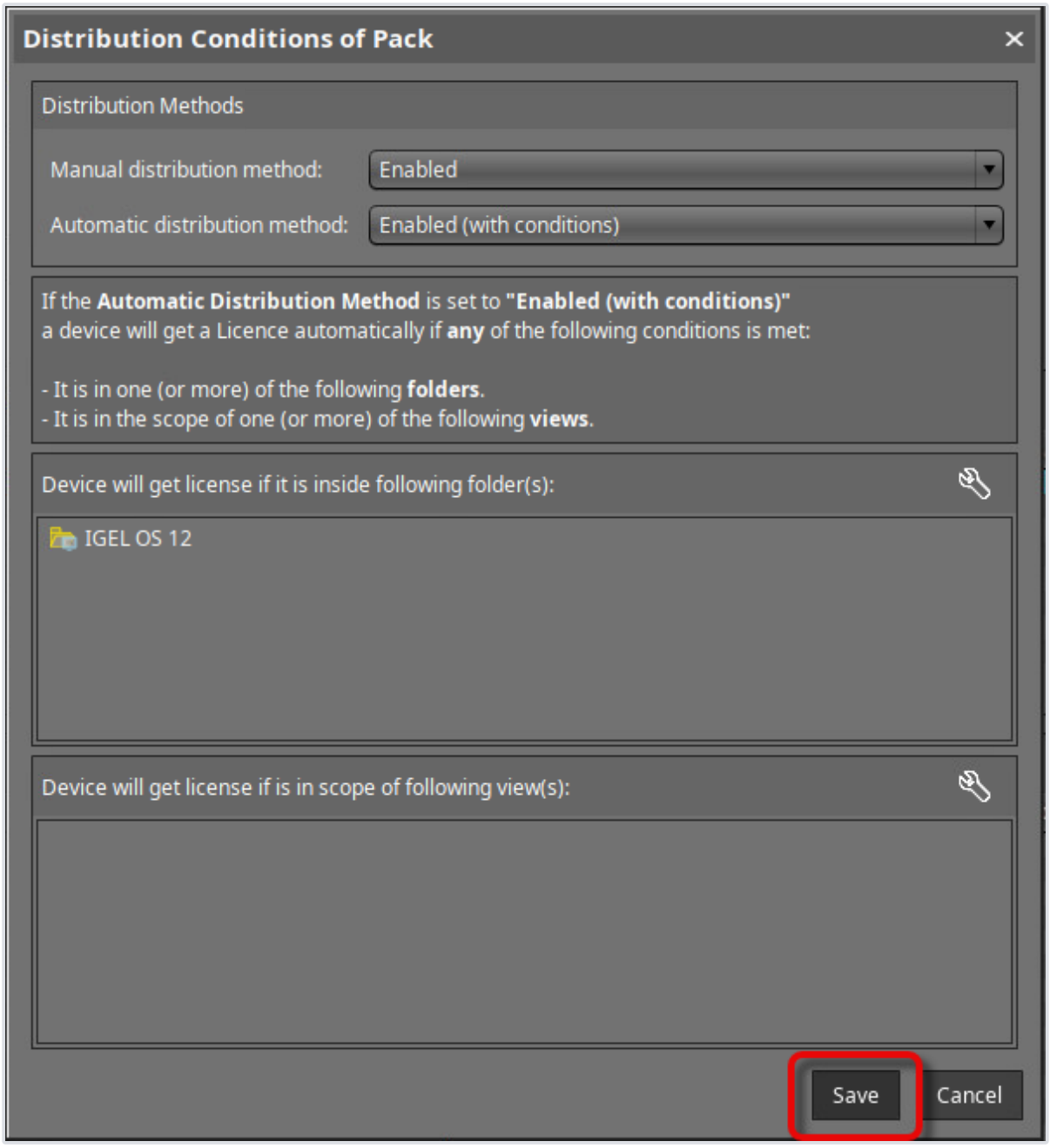


4. Select the folder(s) that contain the IGEL OS 12 devices that should receive a license.


Folder Conditions
Selected objects
Devices (6)
IGEL OS 11 (1)
IGEL OS 12 (1)
IMH (2)
New Devices (0)
Ok



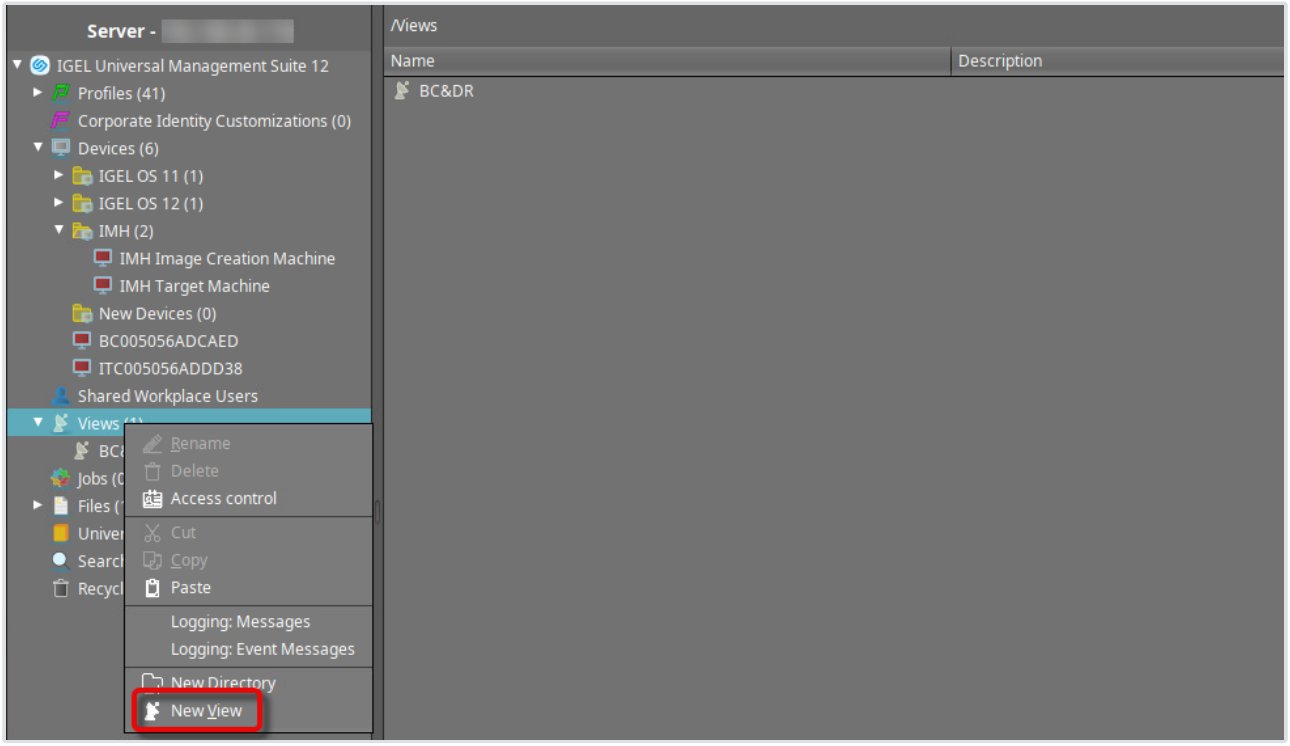
5. When your selection is completed, click **Save**.



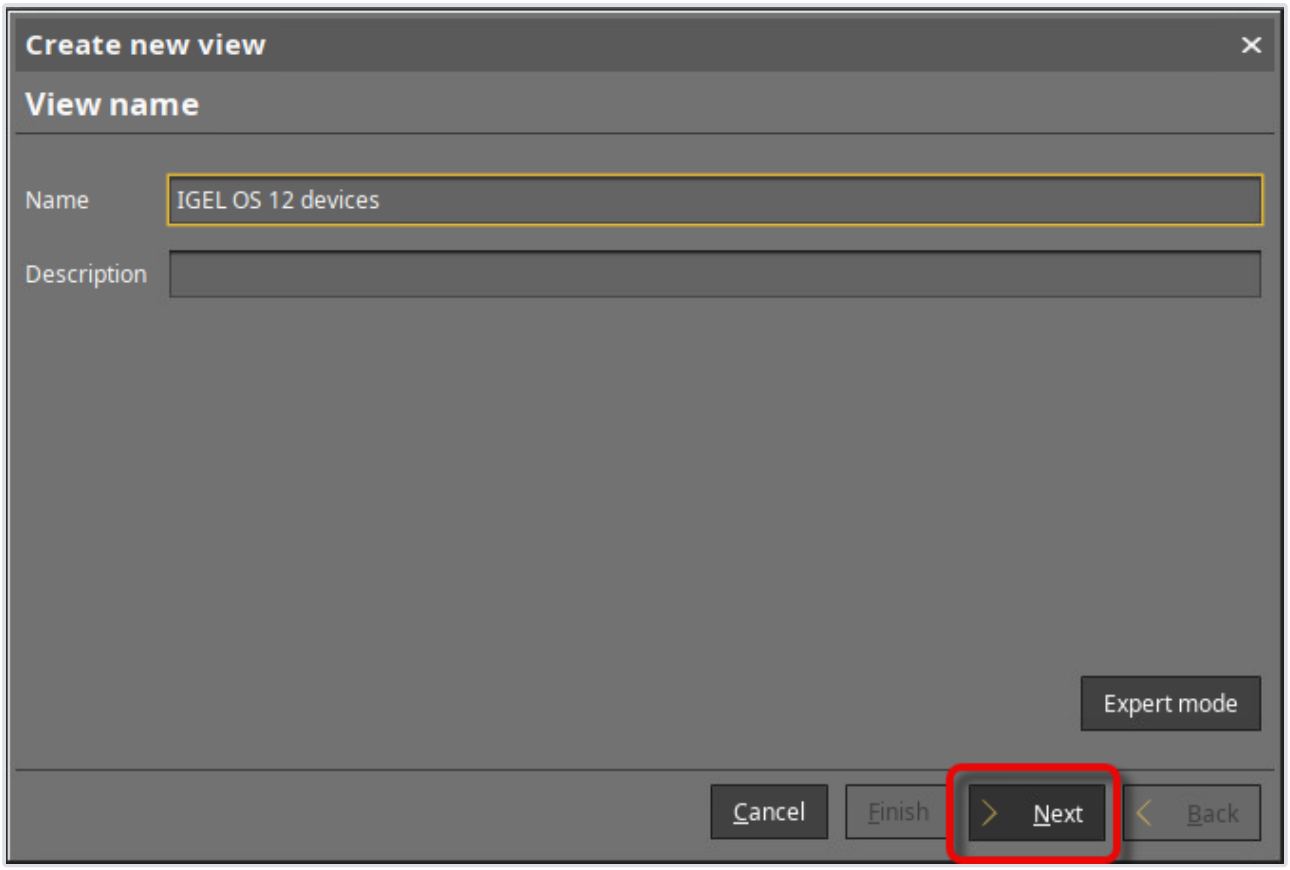
License Distribution Based on a View

This method is feasible if those devices that are to receive an IGEL Agent for Imprivata license and those that should not receive one are not separated by different directories.

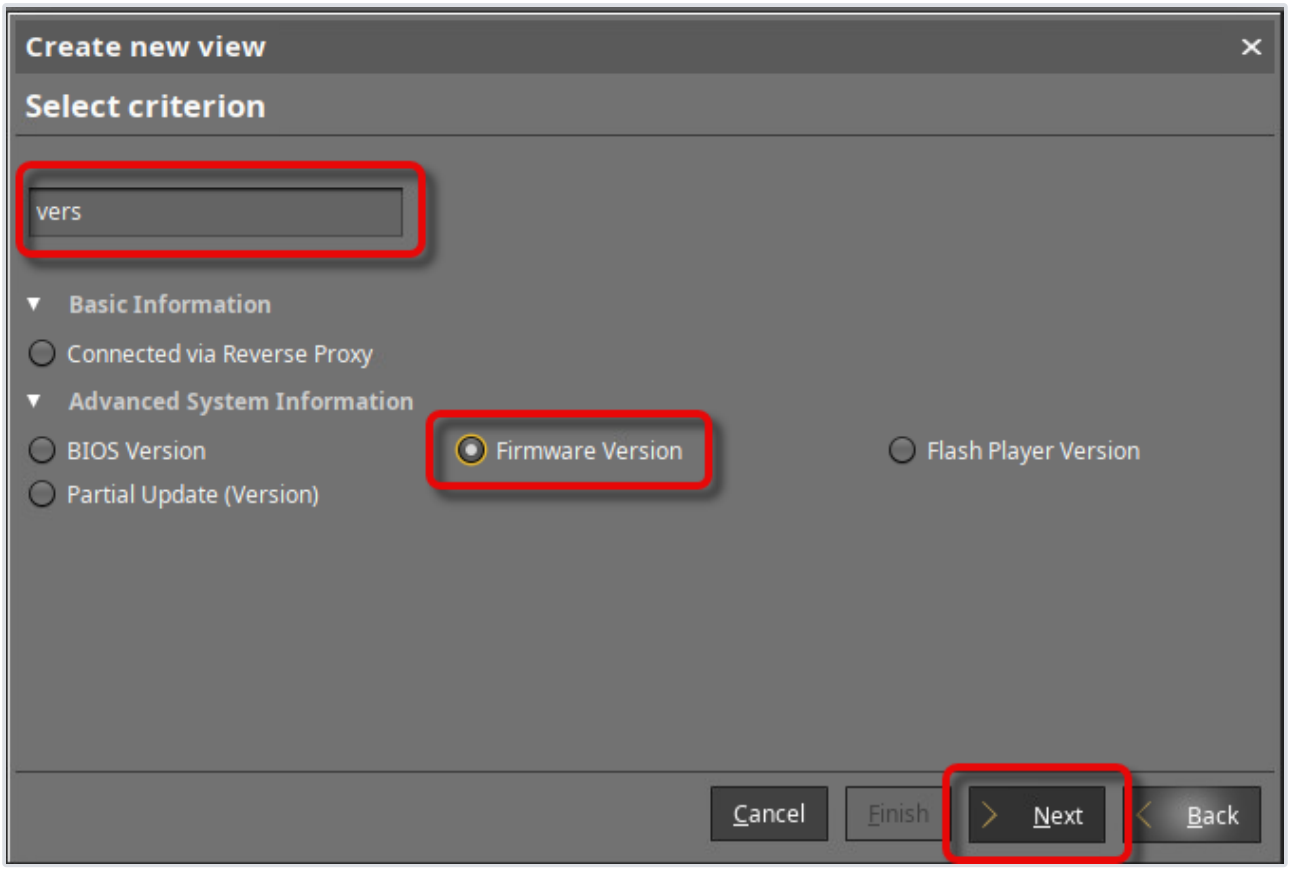
1. In the UMS Console, go to **Server - [host name or IP] > IGEL Universal Management Suite 12 > Views** and select **New View** in the context menu.



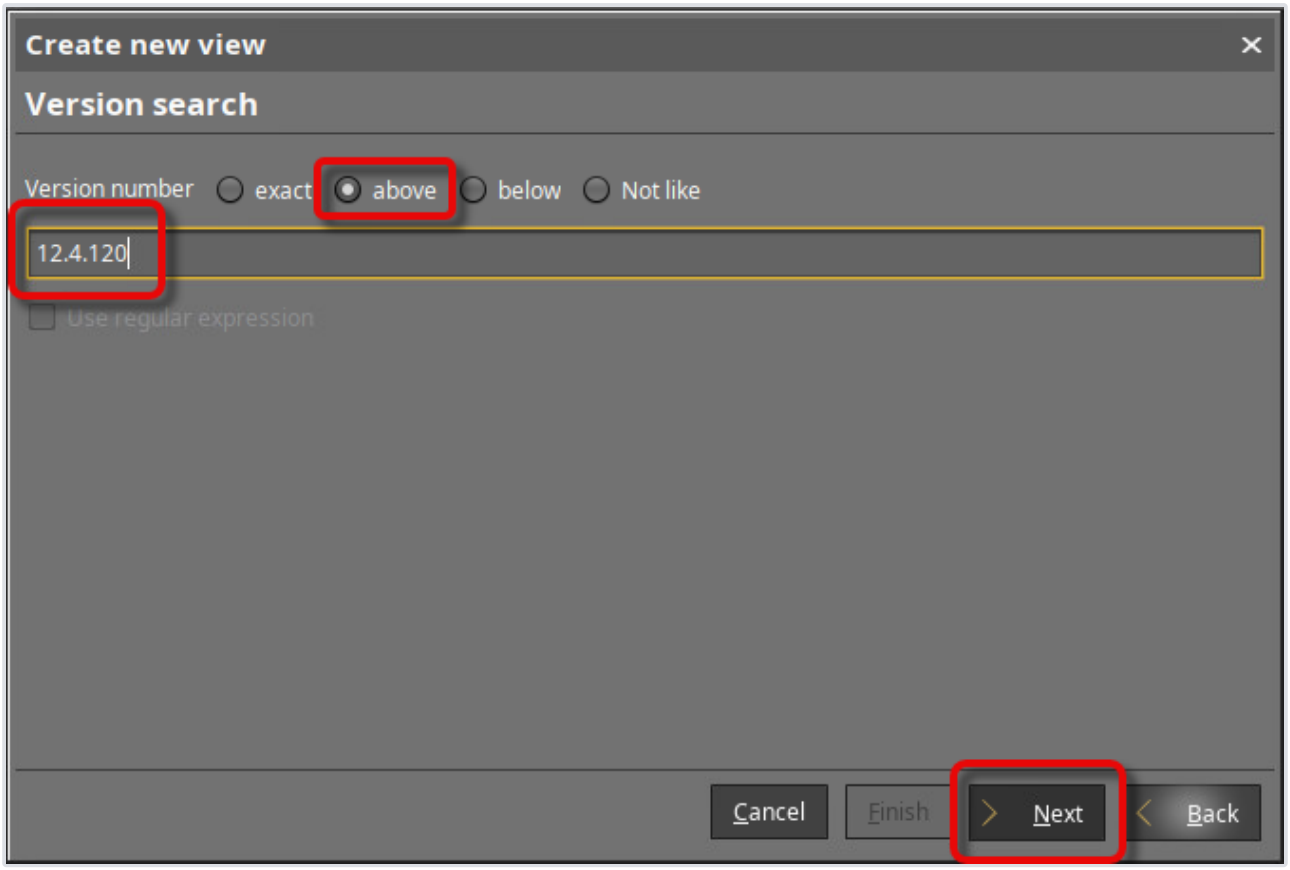
2. Enter a name, e. g. “IGEL OS 12 devices”, and click **Next**.



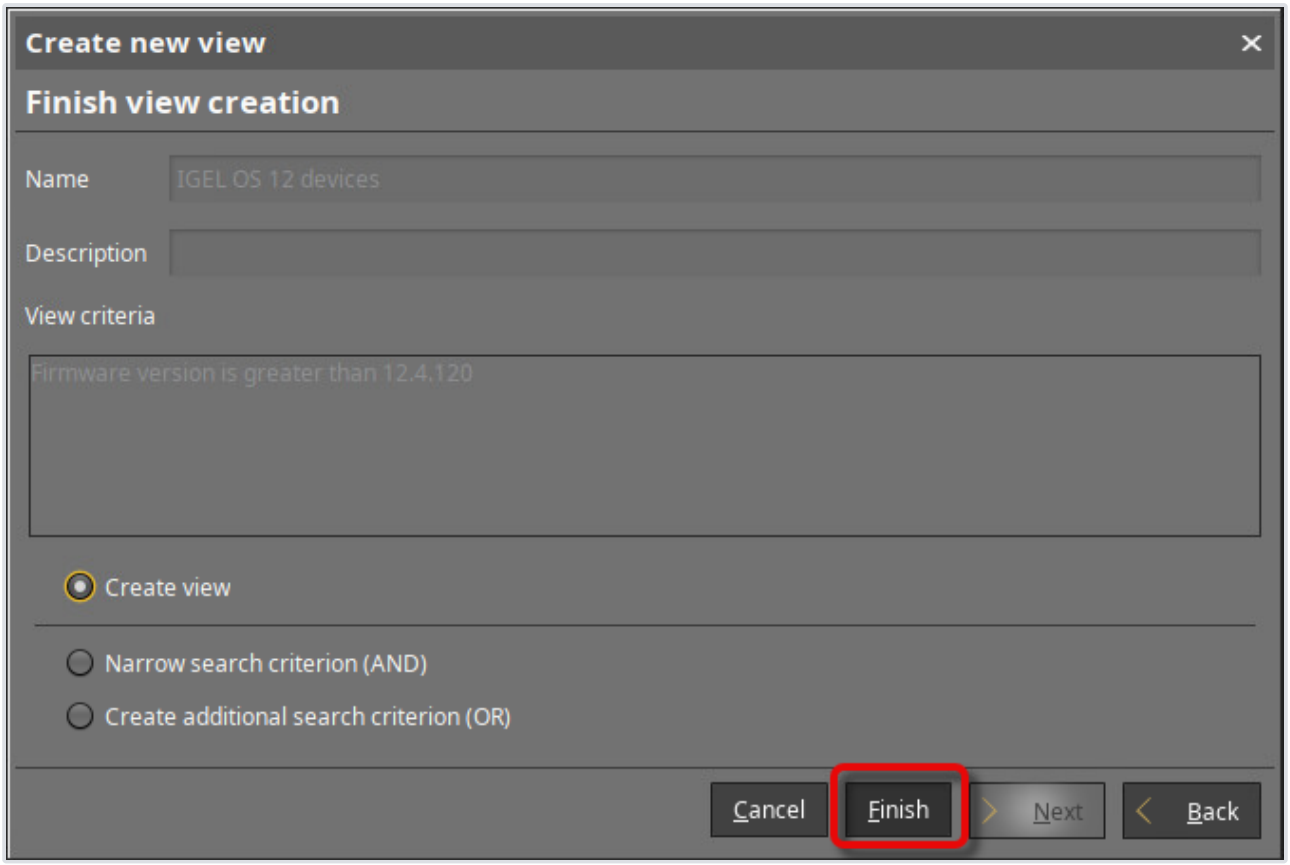
3. Enter “vers” in the filter window to reduce the displayed options, enable **Firmware Version** and click **Next**.



4. Under **Version number**, select above and enter “12.4.120” (example). With this value, devices with IGEL OS 12.5.100 or higher will get IGEL Agent for Imprivata licenses; this is the Base System version required by the IGEL Agent for Imprivata 1.4.2.



5. Click **Finish**.



The devices that are collected by this view are displayed.

How to Enable and Export IAFI Debug Logging for Troubleshooting

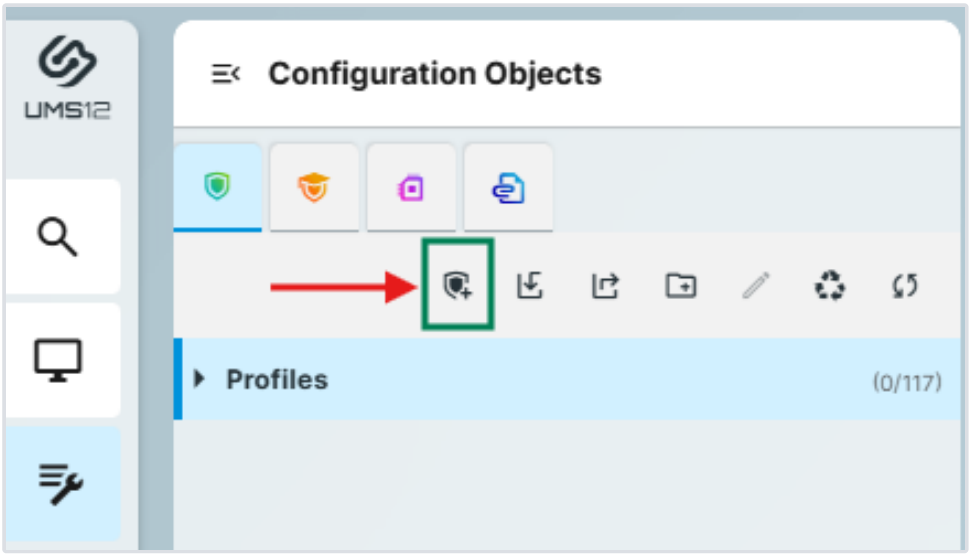
Creating a Profile to Enable the Advanced Logging Levels

Best Practices

- Create a separate profile for enabling IAFI debug logging when troubleshooting.
- Do not leave debug logging enabled for an extended period of time.
- Remove the debug profile when troubleshooting is no longer required.
- If you need additional OS level log files, refer to this KB article: Debugging / How to Collect and Send Device Log Files to IGEL Support[109]

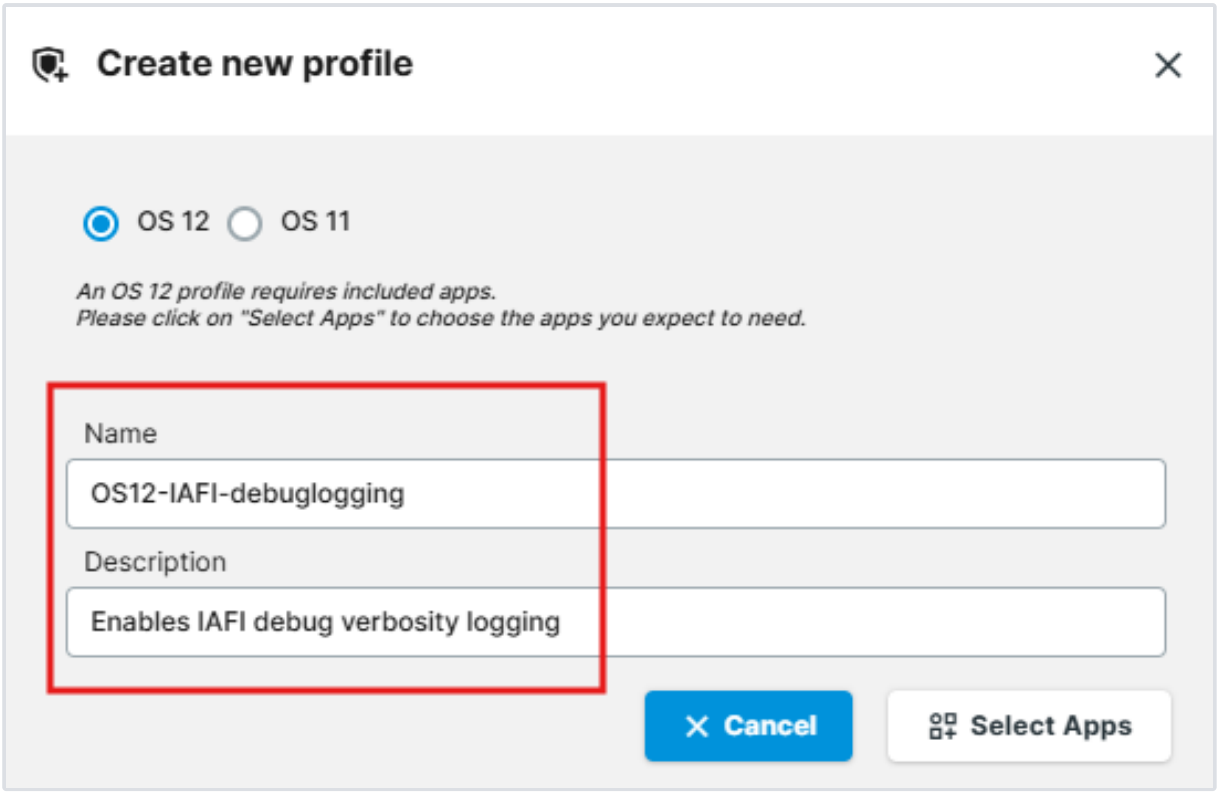
1. Open the UMS Web App and select **Configuration Objects** on the main menu or left side menu.

2. Click the icon to **Create new profile**.



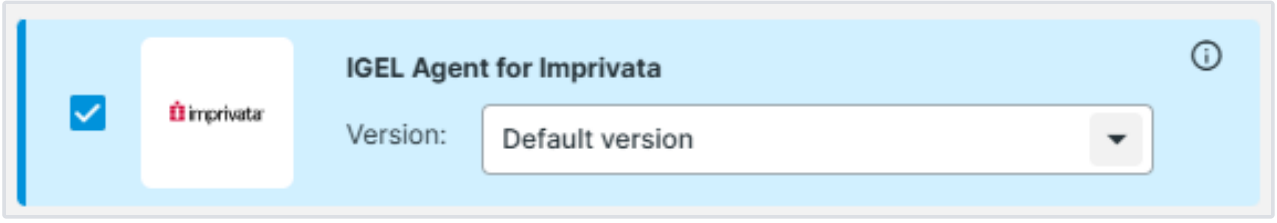
3. Give the OS 12 profile a name and easy description like the example shown here.

109. https://kb.igel.com/en/how-to-start-with-igel/current/debugging-how-to-collect-and-send-device-log-files



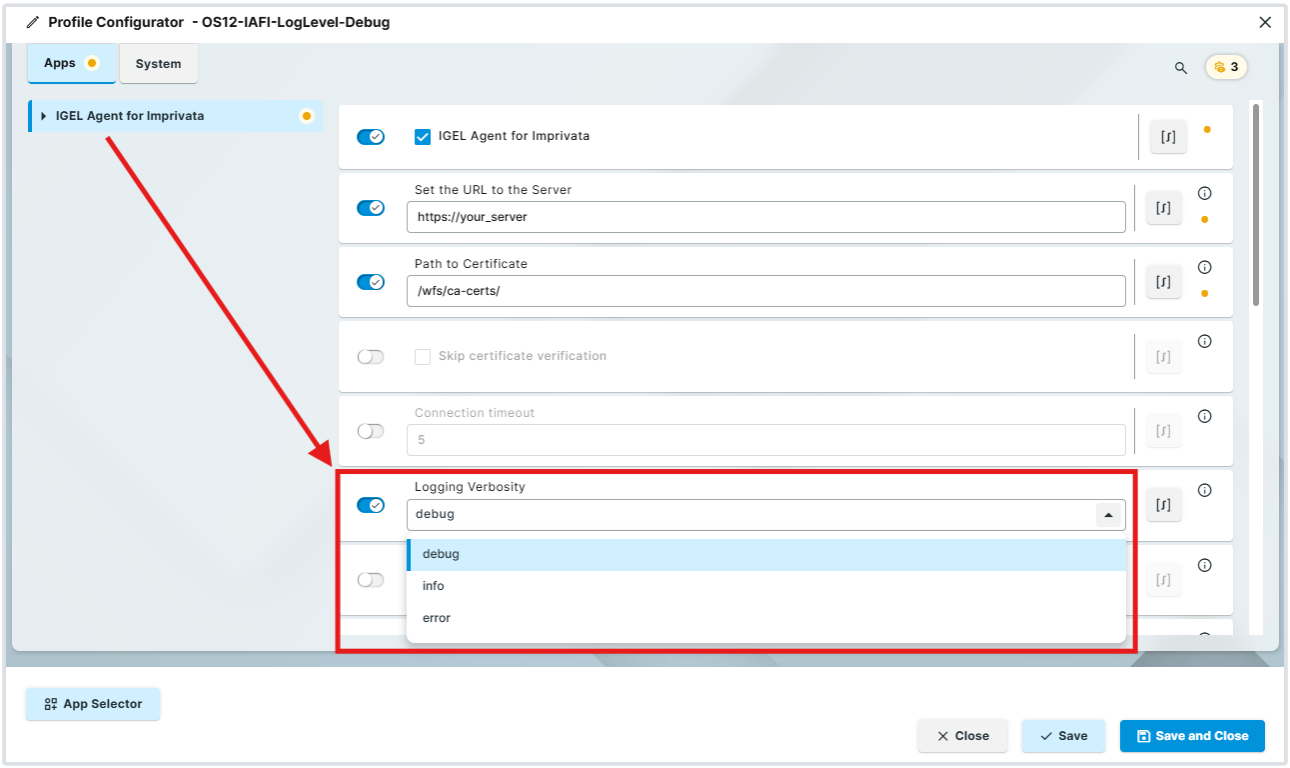
4. Click the **Select Apps** button and in the **App Selector**, pick the **IGEL Agent for Imprivata** as the app and click **Save**.

NOTE: In the app selector, if you have **Show Versions** enabled, you can leave it at **Default Version** or select a specific IAFI app version installed on the endpoint.



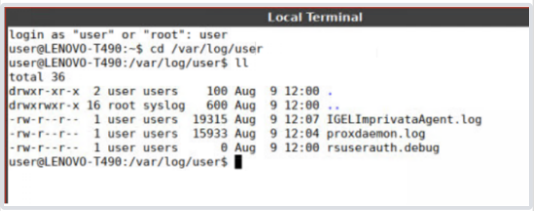
5. In the Profile Configurator, go to **Apps > IGEL Agent for Imprivata.**

6. Scroll down to the **Logging Verbosity** option and modify the settings to switch to **debug** or **error** log levels:



IMPORTANT: Do not leave debug or error logging on continuously. It should only be enabled for troubleshooting and removed when completed. Switch back to **info** logging for normal production use.

7. Save the profile and apply it to the device/folder as needed.

Log location	`/var/log/user` 	
Log Files	`IGELImprivataAgent.log` Main agent/appliance activity log	

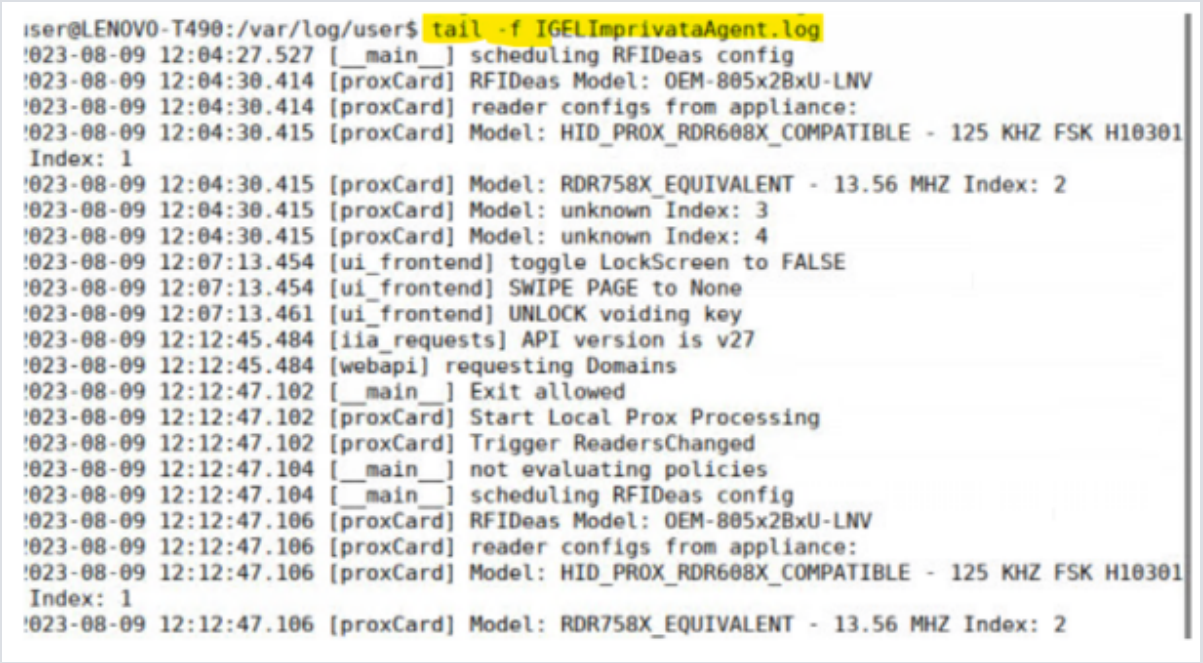
	`Proxdaemon.log` RFIdeas reader log. Will show activity with the prox reader	
	`IGELImprivataAgentERR.log` Only seen if an agent crash occurs	

Live Monitoring the Log Files While Troubleshooting

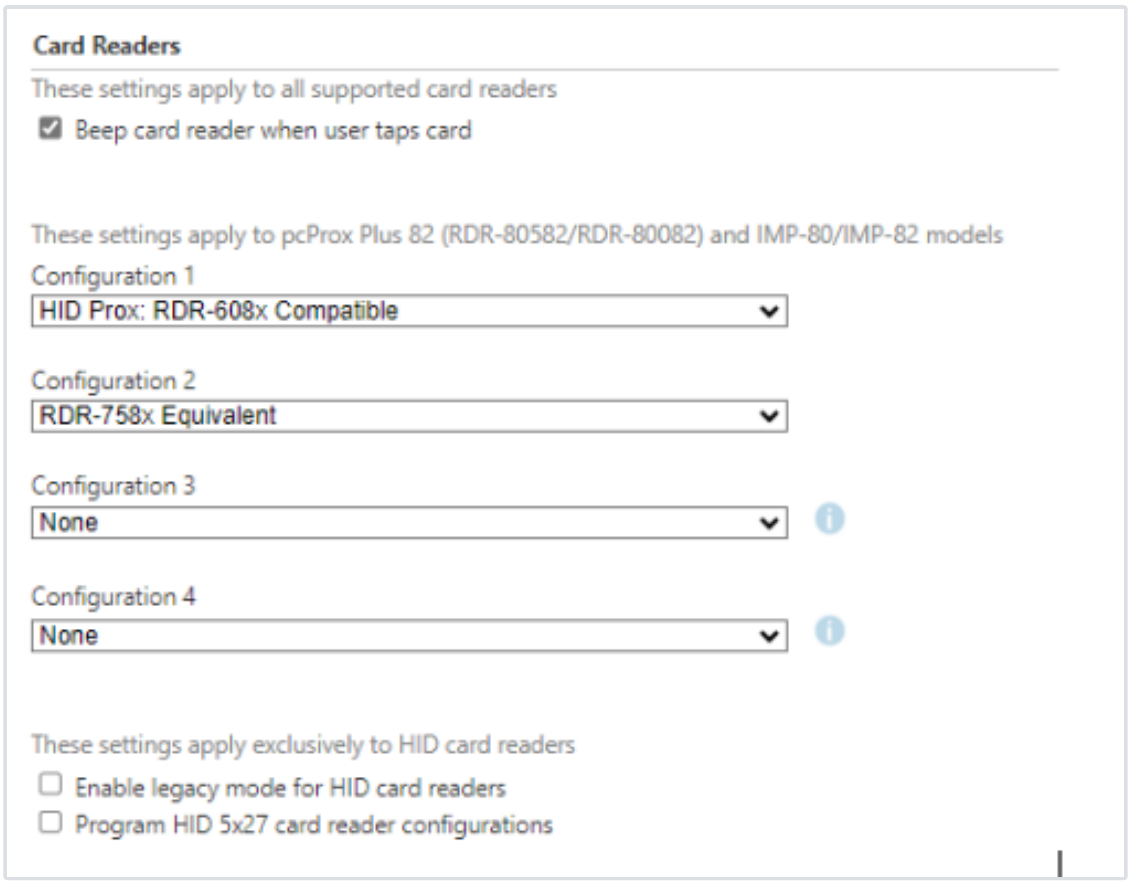
> This requires the log level to be in debug mode.

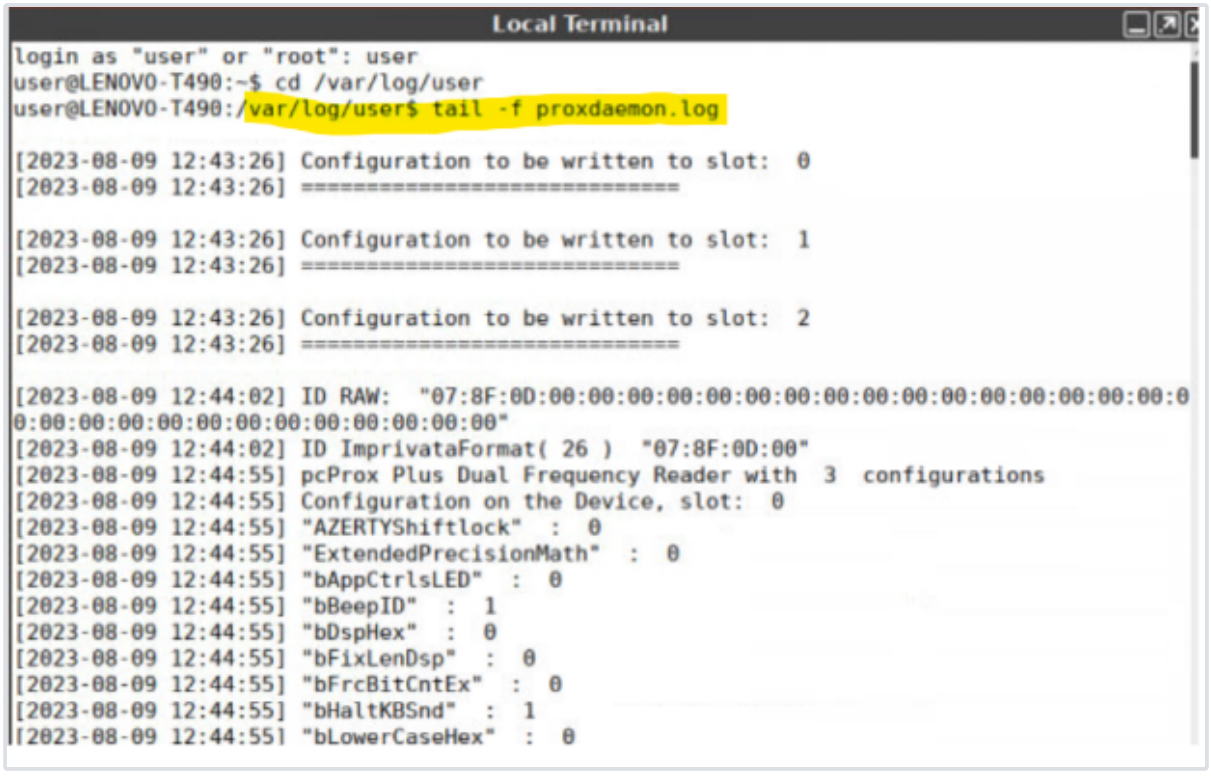
Tailing the Log Files

1. Create a profile for a local terminal or use a remote terminal session.
2. Open the terminal session and **change to the user context**.
3. If logged in as root, type `su user` to change to the user context.
4. At the command line, type `/var/log/user` and hit [Enter].
5. Type `ls` to see the contents of the directory.
   You should see the `IGELImprivataAgent.log` file.
6. Type `tail -f IGELImprivataAgent.log` and hit [Enter].
   You should see live activity in the log file as you authenticate or use the agent system tray icon menu options like **Sync**.



7. Optional: To monitor the RFIdeas proximity card daemon, type `tail -f proxdaemon.log` and hit [Enter].
   You should see information about the configuration assigned to the proximity reader from the **Imprivata Computer Policy – General Tab – Card Readers** section.


Card Readers
These settings apply to all supported card readers
Beep card reader when user taps card
These settings apply to pcProx Plus 82 (RDR-80582/RDR-80082) and IMP-80/IMP-82 models
Configuration 1
HID Prox: RDR-608x Compatible
Configuration 2
RDR-758x Equivalent
Configuration 3
None
Configuration 4
None
These settings apply exclusively to HID card readers
Enable legacy mode for HID card readers
Program HID 5x27 card reader configurations


Local Terminal
login as "user" or "root": user
user@LENOVO-T490:~$ cd /var/log/user
user@LENOVO-T490:/var/log/user$ tail -f proxdaemon.log
[2023-08-09 12:43:26] Configuration to be written to slot: 0
[2023-08-09 12:43:26] ==========
[2023-08-09 12:43:26] Configuration to be written to slot: 1
[2023-08-09 12:43:26] ==========
[2023-08-09 12:43:26] Configuration to be written to slot: 2
[2023-08-09 12:43:26] ==========
[2023-08-09 12:44:02] ID RAW: "07:8F:0D:00:00:00

How to Enable Debugging for VDI Session Types

It may be helpful to enable additional debug logging for the different IGEL OS apps when you need to open a support case. Follow these best practices to enable logging for these apps.

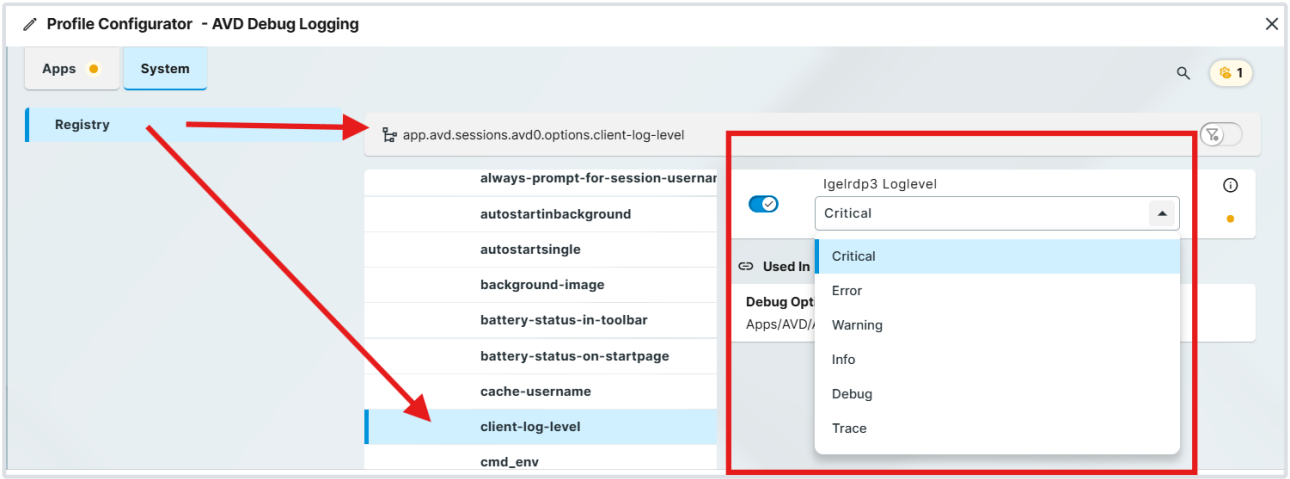
General Information

- Please also activate the debug logging of the base system in case of problems with apps.
- All parameters of apps are found in the registry under **app.[appname]** e.g., **app.cwa**. This also applies to the session parameters.
- The start scripts of apps are no longer located under `/config/sessions`, but under `/config/sessions/[appname]`.
- The setup sites of all apps can be found under **Apps**.

Microsoft AVD

- OS 12 registry parameter:
  - **app.avd.sessions.avd<x>.options.client-log-level** (**Critical**, **Error**, **Warning**, **Info**, **Debug**, **Trace**)

Template Profile
Download this profile and import into UMS as an example: AVD-debuglogging.ipm



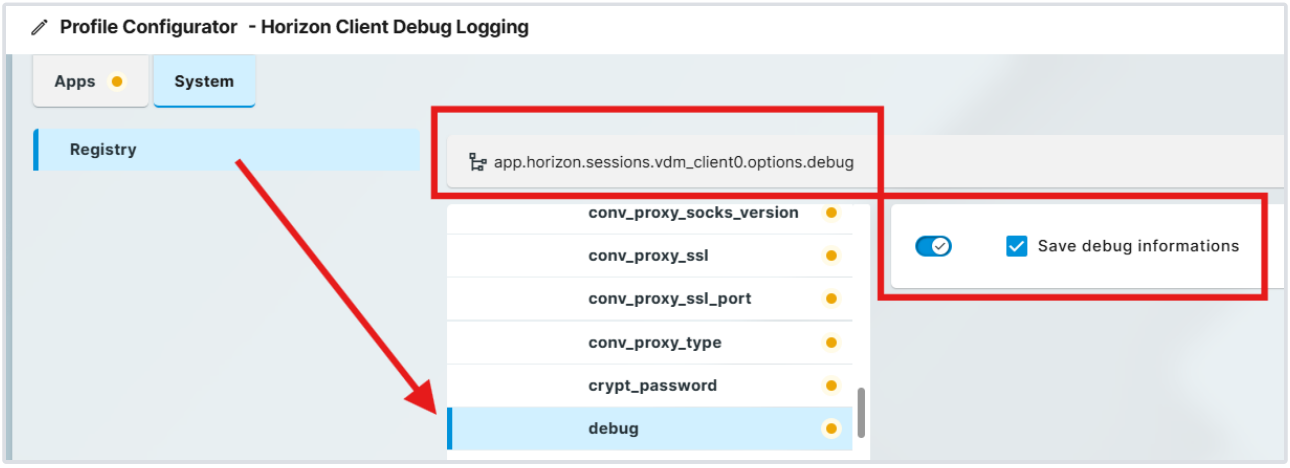
- Logfiles:
  - `/var/log/user`
- Collected with WUMS: **yes**

Omnissa Horizon Client

Dependencies: None

Template Profile
Download and import this profile into the UMS for an example: HorizonClient-debuglogging.ipm

- Parameter:
  - **app.horizon.vdm_client<x>.options.debug**

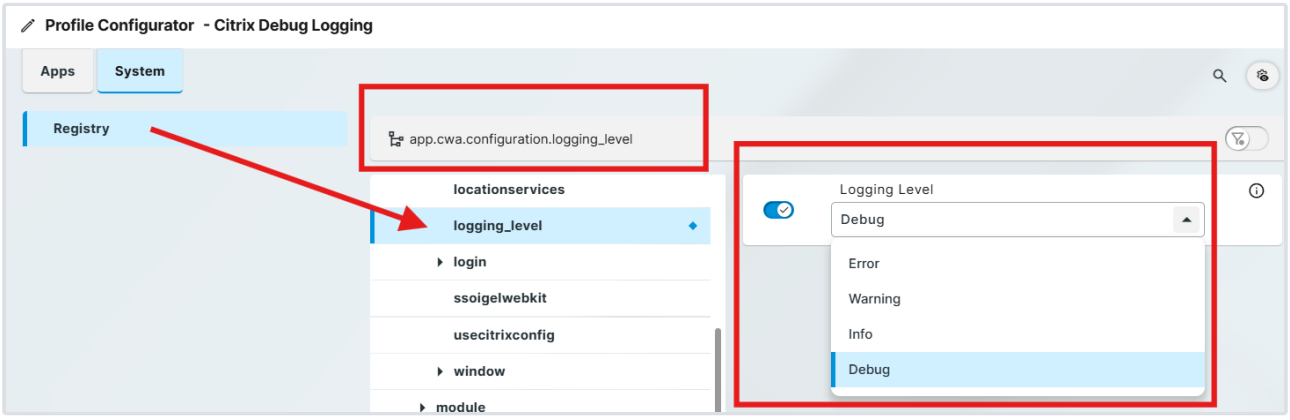


- Logfiles:
  - `/var/log/vmviewsess<x>.debug`
- Collected with WUMS: **yes**

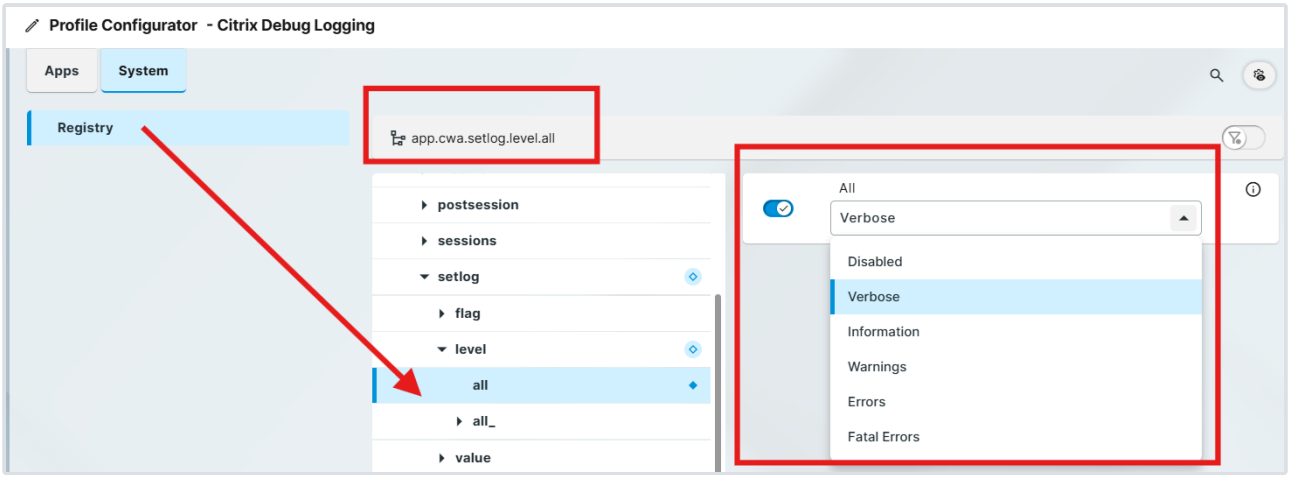
Citrix Workspace App

Template Profile
Download this profile and import it into the UMS as an example: CitrixWSA-debuglogging.ipm

Parameter: **app.cwa.configuration.logging_level** (**Error**, **Warning**, **Info**, **Debug**)



Parameter: **app.cwa.setlog.level.all** (**Disabled**, **Verbose**, **Information**, **Warnings**, **Errors**, **Fatal Errors**)


Profile Configurator - Citrix Debug Logging
Apps
System
Registry
app.cwa.setlog.level.all
postsession
sessions
setlog
flag
level
all
all_
value
All
Verbose
Disabled
Verbose
Information
Warnings
Errors
Fatal Errors

How to Enable Multiple Monitors for IGEL Agent for Imprivata

When enabled, the IGEL Agent for Imprivata (IAFI) lock screen officially supports two monitors.

- The resolution must be the same as well as the orientation (landscape).
- By default, when enabling two monitors, IGEL OS will automatically detect the resolution. If both monitors are the same, this is all you should need.

To enable multi-monitor support, create a profile as follows:

IGEL OS 12

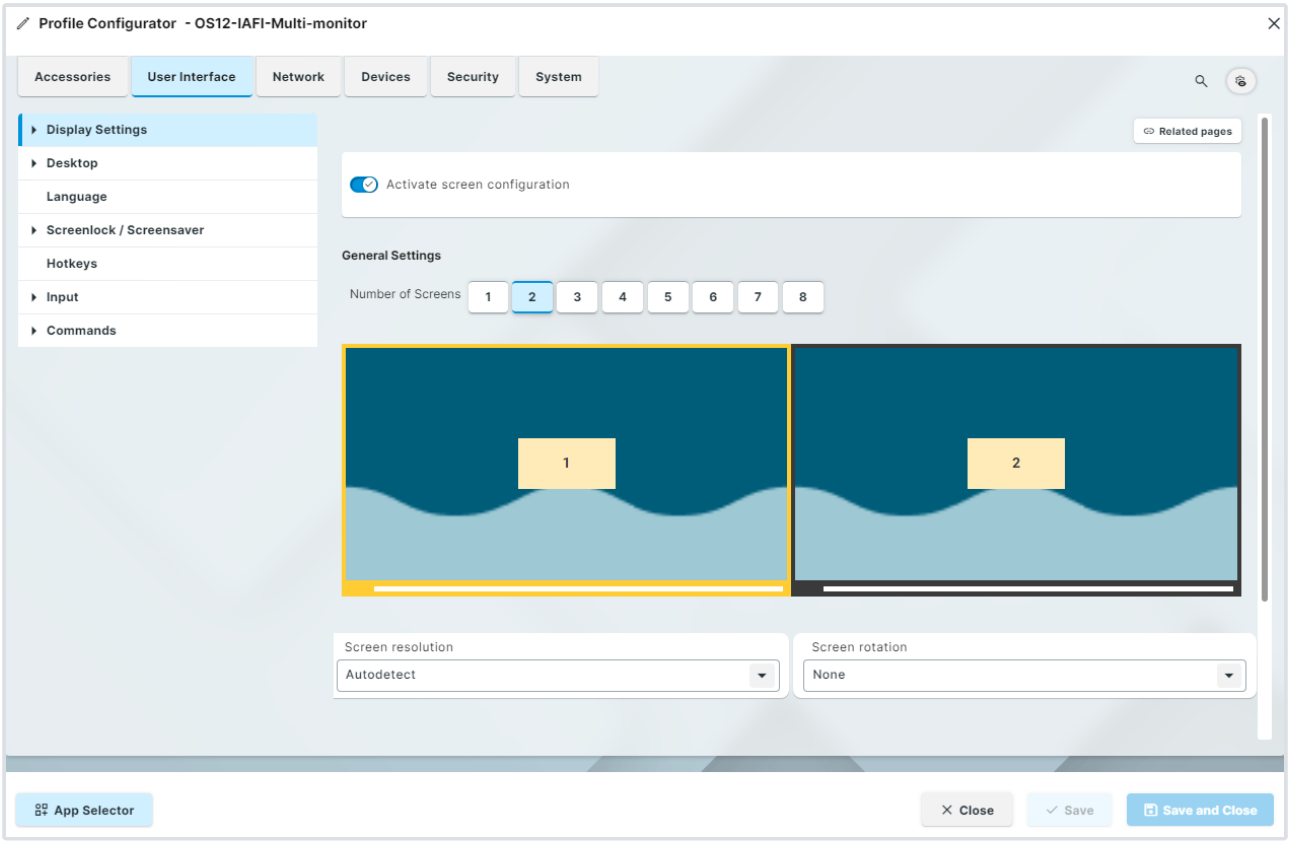
1. Within the **Configuration** area of the UMS web App, select the icon to create a new profile.
2. In the **Profile Configurator**, select **App Selector** and choose the **IGEL OS Base System**.
3. Go to **User Interface - Display Settings** and enable **Activate screen configuration**.
4. Under **General Settings – Number of Screens**, select **two (2)**.
5. For **Screen resolution**, select **Autodetect**.

> If the monitors are not the same, you may need to manually set the monitors to the same resolution.

6. For **Screen rotation**, select **None**.

> Only landscape orientation is supported.

7. Select the "**Save and close**" button and then assign the profile to the device directory where you want to apply the setting.



IGEL OS 11

1. Within the UMS Console, select the option to create a new profile.

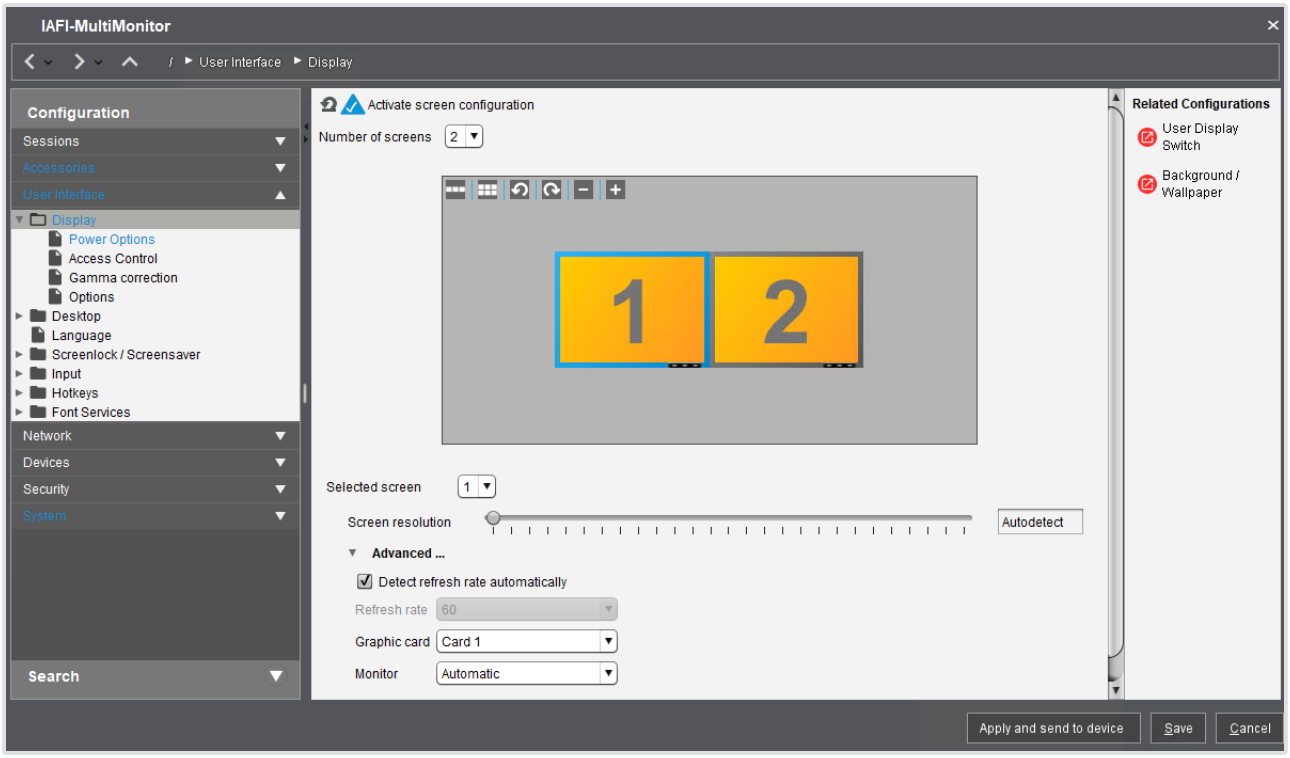
2. In the Profile Configurator, go to User Interface - Display – and enable Activate screen configuration.

3. **Number of Screens** should be **two (2)**.

4. For **Screen resolution**, select **Autodetect**.

5. For **Screen rotation**, orientation should be **landscape** only.

6. Select the **Save** button and then assign the profile to the device directory where you want to apply the setting.


IAFI-MultiMonitor
/ User Interface Display
Configuration
Sessions
Accessories
User Interface
Display
Power Options
Access Control
Gamma correction
Options
Desktop
Language
Screenlock / Screensaver
Input
Hotkeys
Font Services
Network
Devices
Security
System
Search
Activate screen configuration
Number of screens 2
1
2
Selected screen 1
Screen resolution
Autodetect
Advanced ...
Detect refresh rate automatically
Refresh rate 60
Graphic card Card 1
Monitor Automatic
Related Configurations
User Display Switch
Background / Wallpaper
Apply and send to device
Save
Cancel

How to Create a Profile to Restart the IGEL Agent for Imprivata

This profile allows for restarting the agent without a device reboot; it is highly recommended for production or testing purposes.

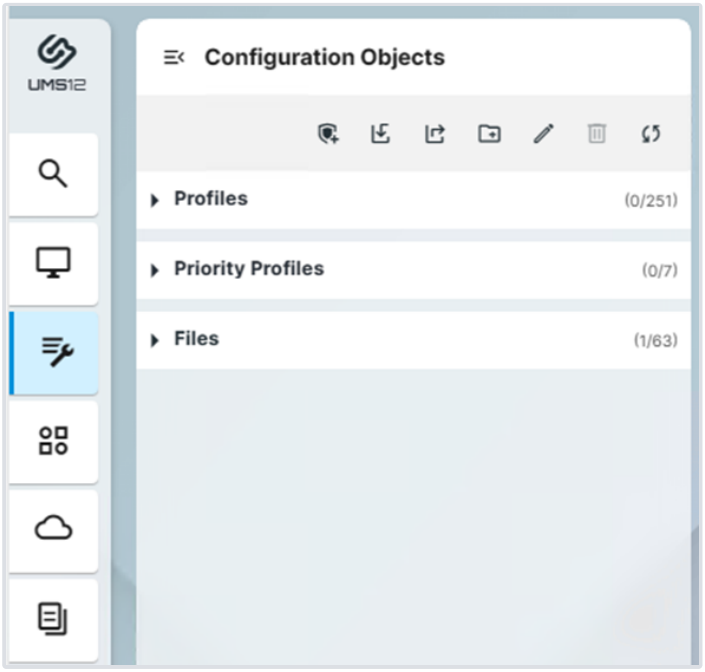
You have two options to use this profile in your environment:

- Download and import the profile here: OS12-IAFI-RestartAgent.ipm (based on OS 12.5.2 but can be used with older or newer OS 12 Base versions)
- Follow the instructions below to create the profile

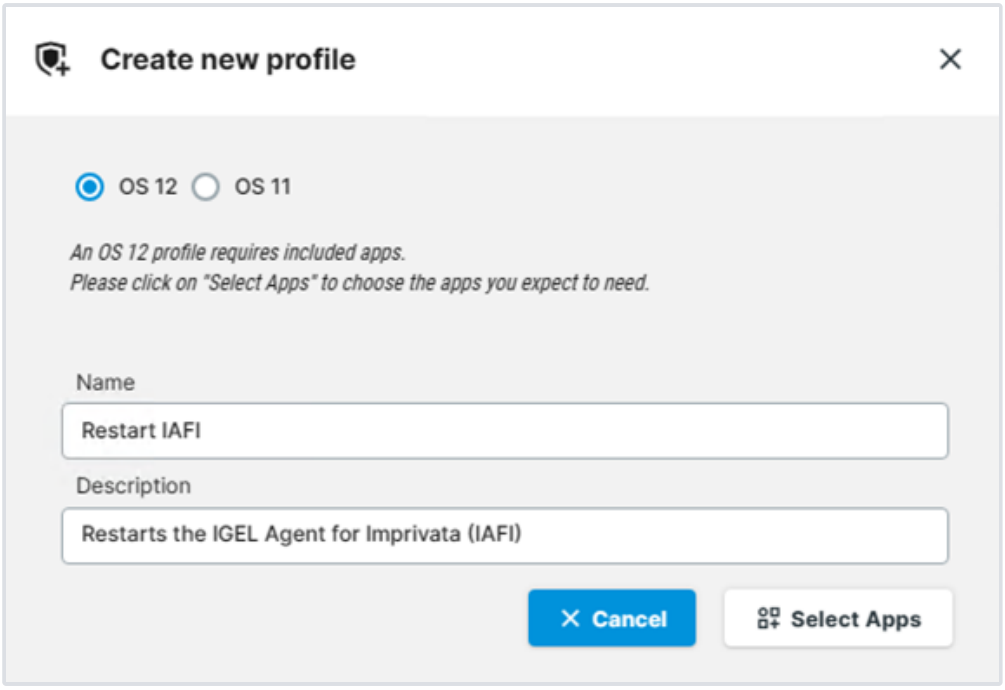
Creating the profile for OS 12

1. Open the **UMS Web App** and select **Configuration Objects** on the main menu or left side menu.

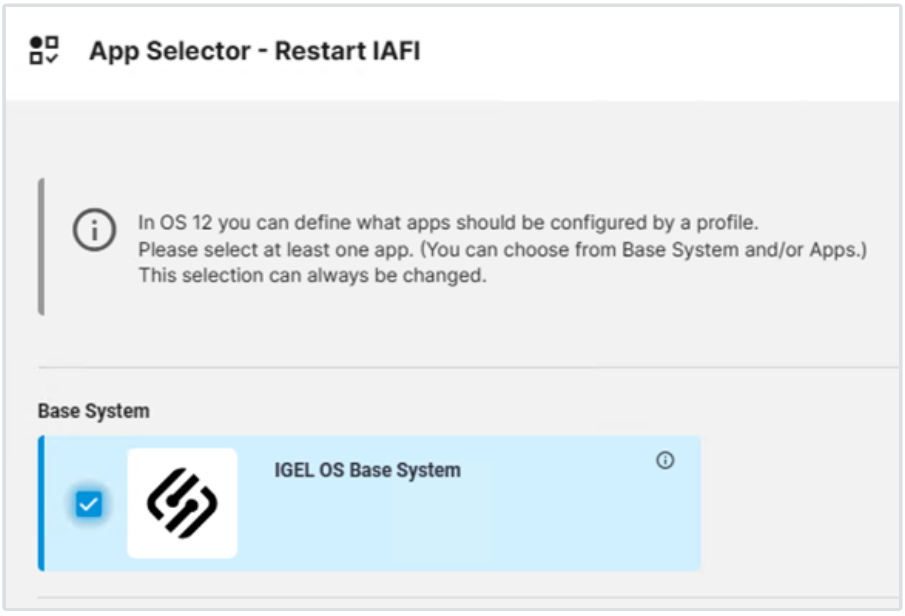
2. Click the icon to **Create new profile**.



3. Give the OS 12 profile a name and easy description like the example shown here.



4. Click the **Select Apps** button and in the **App Selector**, pick the **IGEL OS Base System** as the app and click **Save**.



5. Optional: Select **Show Versions** and you will see a list of app versions available. The minimum version should be 12.4.x, but we recommend using the **default version** which should be set in the Apps section of the UMS Web App.

6. Select the **System** tab and then **System Customization – Custom Application**, and then click the **+** icon to add an item.

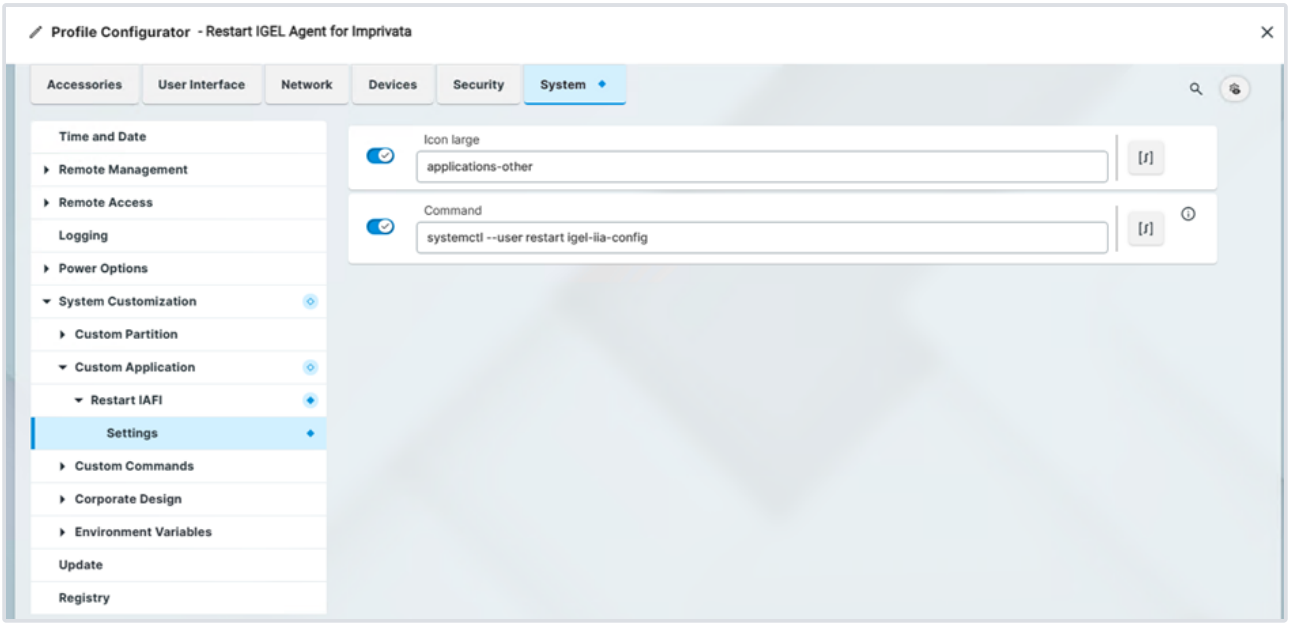
7. In **Session name**, provide a name such as **Restart IAFI**.

8. In the **Starting Methods for Session**, pick which options you want to enable/disable. One recommendation would be to select the **Desktop Context Menu** which would use the mouse click menu (right click to show a list of options).

9. On the left-hand menu, expand the name of the session (ex: Restart IAFI) and select **Settings**.

10. On the left-hand menu, expand the name of the session (ex: Restart IAFI) and select **Settings.**

11. In the **Command** field, type: `systemctl --user restart igel-iia-config`



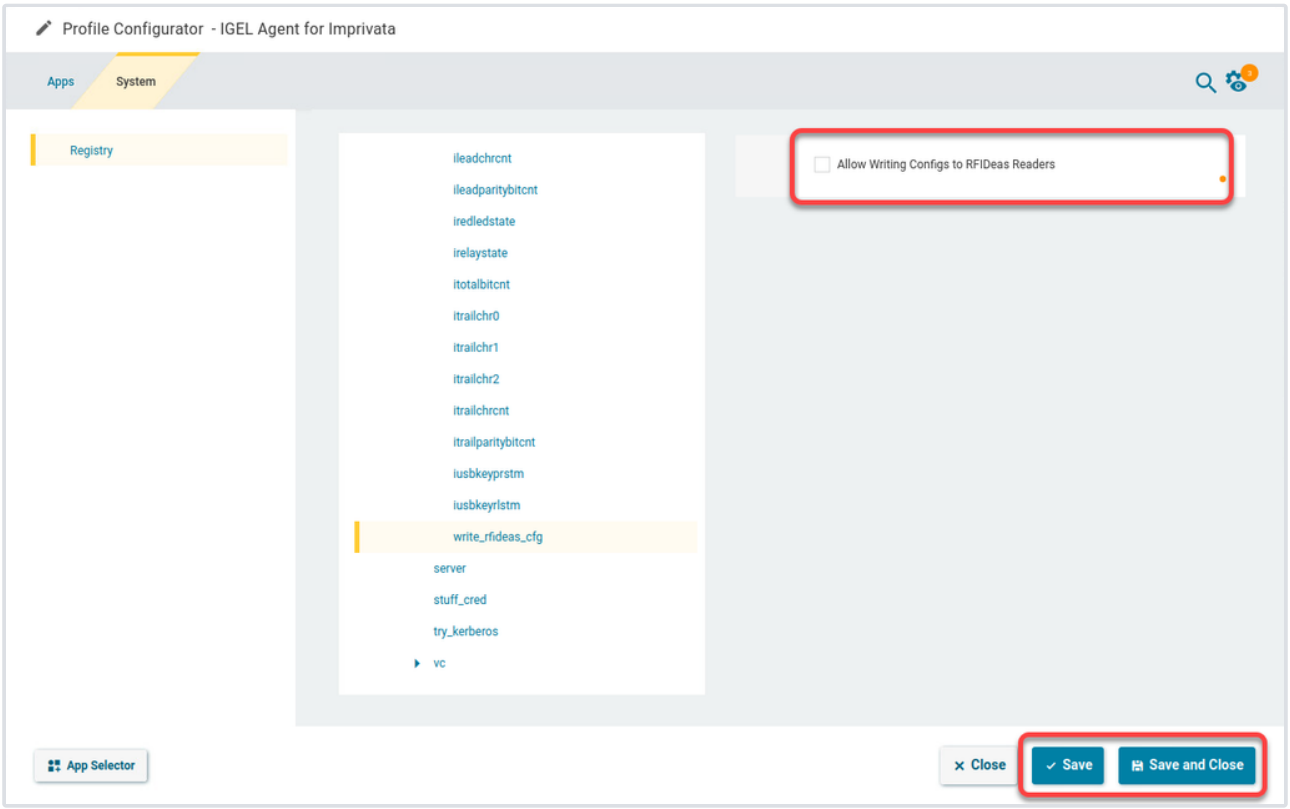
12. Select **Save and Close** and then deploy the profile to the Device Directory where your OS 12 devices reside.

Troubleshooting: Use the Card Reader's Former Configuration

By default, the card reader is configured by the IGEL Agent for Imprivata based on the settings in the Imprivata Computer Policy. Generally speaking, you should never have to change this setting. However, in case this configuration causes problems, you have the option to prevent the use of the IGEL Agent for Imprivata from configuring the card reader. Thus. the card reader's former configuration can be used.

To use the card reader's former configuration:

→ In the profile configurator, go to **Registry > app > iia > rfideas > write_rfideas_cfg**, deactivate **Allow writing configs to RFIDeas readers**, and save your settings.



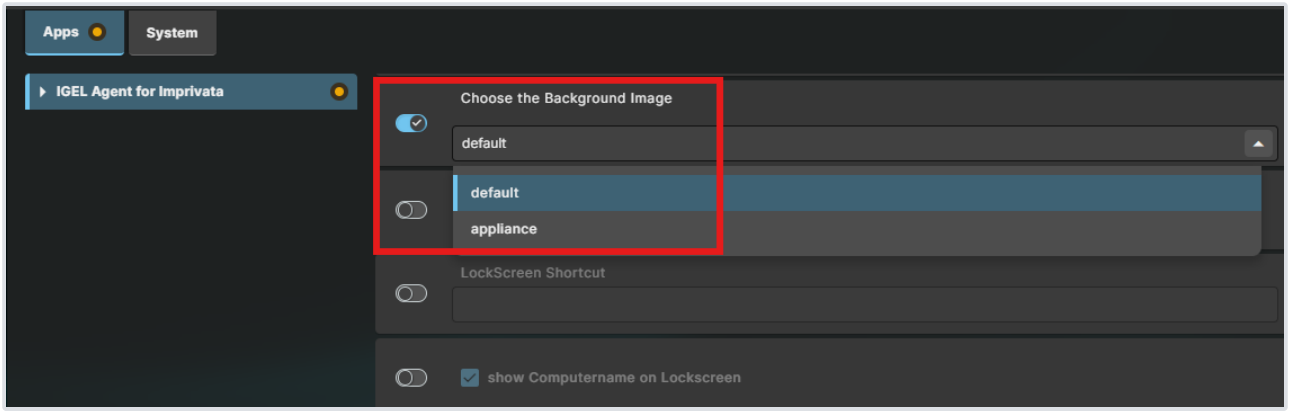
How to enable IAFI logon screen customizations

IAFI LockScreen Background Image Options

IAFI has three options for the lockscreen background image.

1. Default background image
2. Imprivata Appliance default image
3. Custom Image from the UMS Server

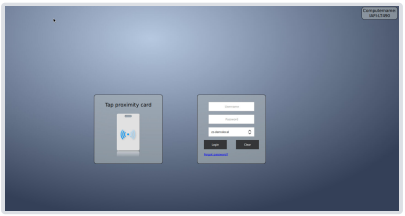
- IGEL OS 12 IAFI profile options for LockScreen background image



Default background image



Default Imprivata Appliance background image



Custom background image from the UMS



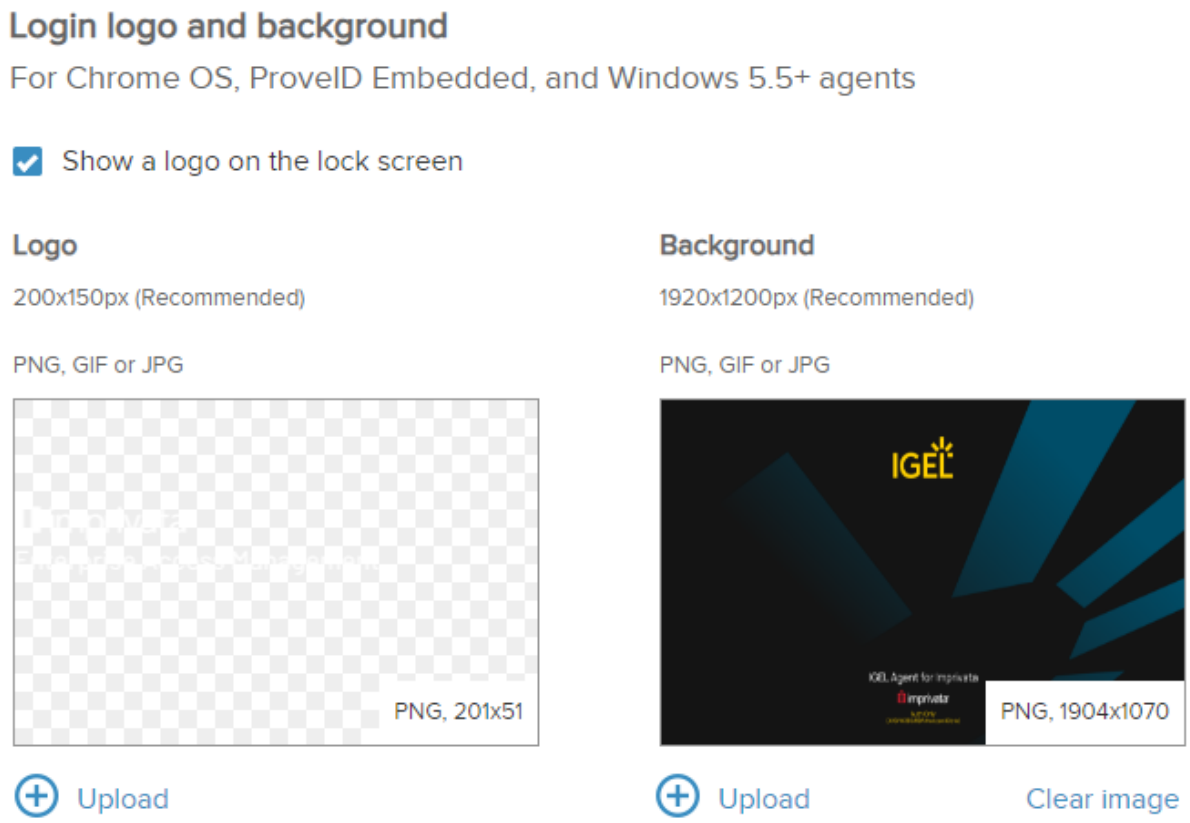
To customize the IAFI background image, you have two options:

1. The Imprivata Computer Policy - Customization setting
2. Custom image deployed from the UMS

Option 1: Imprivata Computer Policy - Customization

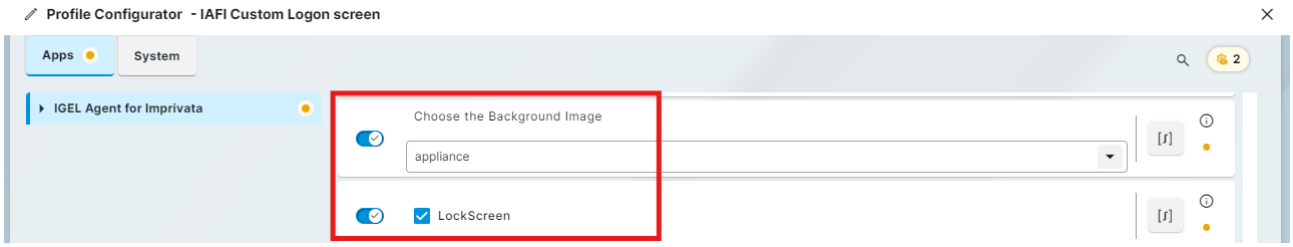
1. Log into the Imprivata Admin Console, navigate to **Computers - Computer Policies**
2. Edit a computer policy that is assigned to devices running IGEL Agent for Imprivata
3. Go to the Customization tab and scroll down to the **Login logo and background** section.

4. Upload a custom background image per the Imprivata recommended guidelines for size and format (PNG, GIF, JPG)



OS 12 - IAFI profile setting for custom wallpaper from the Imprivata appliance

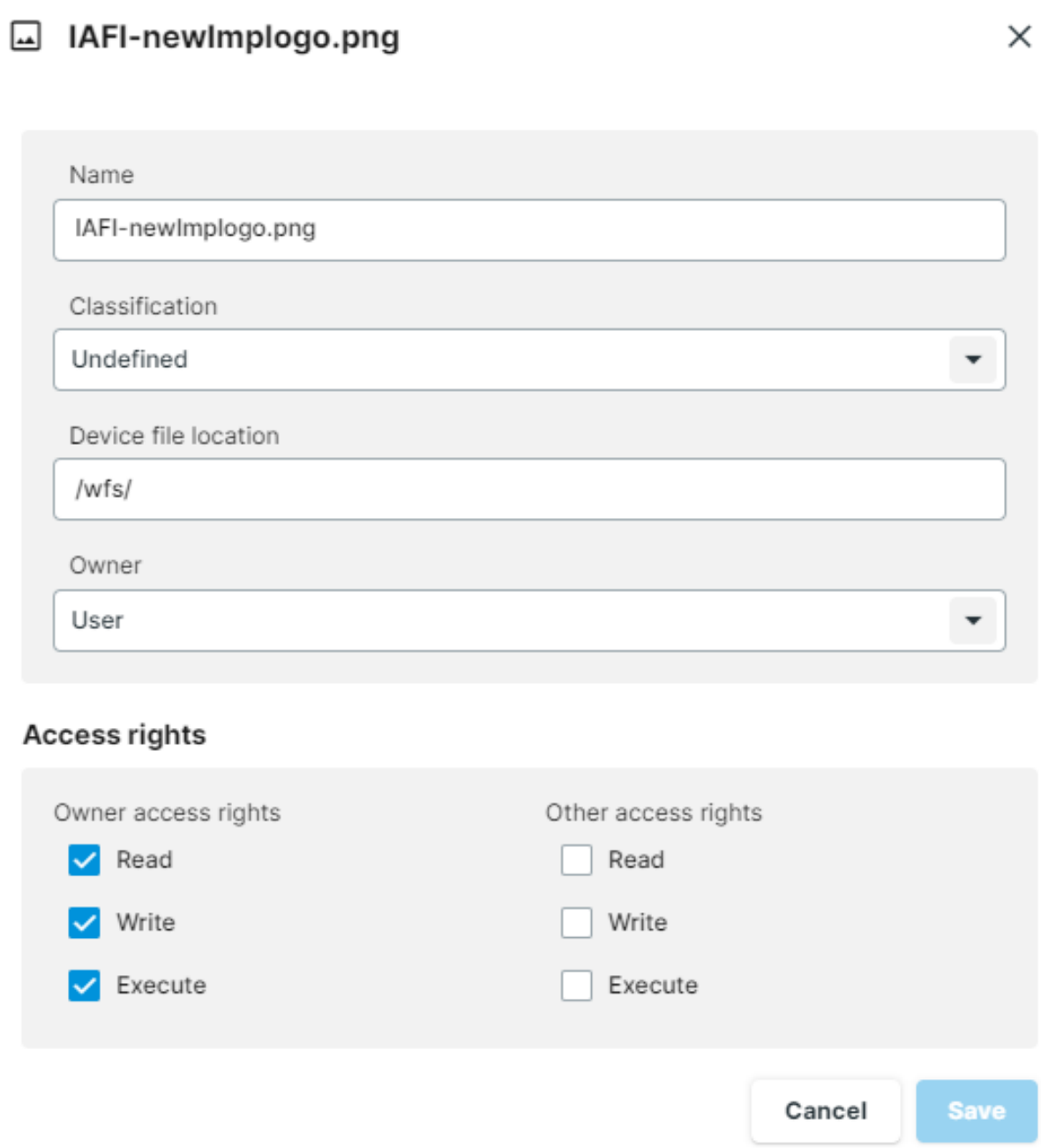
1. Open the IGEL Web UMS and edit an OS 12 profile with the IGEL Agent for Imprivata app.
2. In the IAFI general settings, scroll down to “Choose the Background Image”, click the drop-down menu and select **appliance**.



3. Enable the LockScreen setting.
4. Save the profile and apply the changes now or on next reboot.
5. When the agent restarts, you will see the custom wallpaper from the appliance.

Option 2: Custom image deployed from IGEL UMS

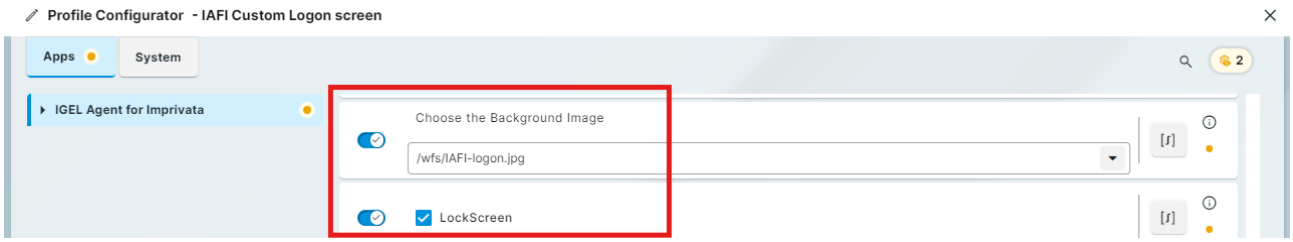
1. Log into the IGEL Web UMS and navigate to the **Configuration** section.
2. Upload an image file deployed as classification “Undefined”. The default settings should be fine.
    a. Owner = User
    b. Device file location = /wfs



3. Deploy the image file to the folder(s) where the devices reside.

OS 12 - IAFI profile setting for custom wallpaper from the Imprivata appliance

1. Edit an OS 12 profile with the IGEL Agent for Imprivata app.
2. In the IAFI general settings, scroll down to “Choose the Background Image”.
3. Where it says “Default”, type in the path to the image file you just deployed (ex: **/wfs/IAFI-logon.png**)
4. Enable the LockScreen setting.
5. Save the profile and apply the changes now or on next reboot.
6. When the agent restarts, you will see the custom wallpaper from the image deployed to the device.



IAFI Profile Templates

These profiles are available as templates for assisting with configuration of the different supported workflows.

Before You Begin:

Please refer to these additional articles:

- IAFI Workflow Configuration Options[110]
- Configuration of the IGEL Agent for Imprivata on IGEL OS[111]
- IGEL Agent for Imprivata (IAFI) Feature Comparison Matrix[112]
- IAFI Terminology Glossary[113]

Important:

- The profiles are set to use the “Default Version” of IAFI and any of the supported apps.
- You can modify them as necessary.
- Refer to this article for importing profiles: Exporting and Importing Profiles in the IGEL UMS Web App[114]
- For most of the workflow templates, you will have to fill in the details for your environment such as:
    - Imprivata Appliance URLs
    - Session connection information (ex: Server URL, generic user ID or passwords)
    - Lockscreen customizations (if applicable)

110. https://kb.igel.com/en/igel-apps/current/iafi-workflow-configuration-options
111. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i
112. https://kb.igel.com/en/igel-apps/current/igel-agent-for-imprivata-iafi-feature-matrix-compa
113. https://kb.igel.com/en/igel-apps/current/iafi-terminology-glossary
114. https://kb.igel.com/en/universal-management-suite/current/exporting-and-importing-profiles-in-the-igel-ums-w#id-(12.08.130-en)ExportingandImportingProfilesintheIGELUMSWebApp-ImportingProfiles

Imprivata Workflow Templates

Follow Policies and Workflows **This is for Roaming Sessions Only (Apps or Desktops)**	**Profile Template**	**Notes** **Please refer to this IAFI KB article for Follow Policies:** Configuration of the IGEL Agent for Imprivata on IGEL OS[115]
Virtual Desktops Only (Citrix, Horizon)		This configuration is for a workflow with just virtual desktops. If the user only has one, they will get automatically launched to that desktop. If the user has more than one, they will see the IAFI Chooser in Windowed Mode. **NOTE: This should be paired with the Citrix or Horizon Global best practice profiles further below.** **Citrix customers may need to enable the NetScaler COOKIEINSERT setting.**
Virtual Apps and Desktops (Citrix, Horizon)		This configuration is for a workflow with just virtual apps and desktops. The user will see the IAFI Chooser in Windowed Mode with a list of their resources. **NOTE: This should be paired with the Citrix or Horizon Global best practice profiles further below.** **Citrix customers may need to enable the NetScaler COOKIEINSERT setting.**
Microsoft Remote PC		Only supports Imprivata VDA for Microsoft Remote PC

115. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringFollowPoliciesandWorkflows

Auth Only	Profile Template	Notes **Refer to:** IAFI Configuration Guide - Auth Only[116]
Microsoft AVD		For AVD client settings, refer to: IGEL Azure Virtual Desktop[117]
Microsoft Windows 365		For Windows 365 client settings, refer to: IGEL Windows 365[118]
Microsoft RDP		This profile connects to a single Windows server. **NOTE: IAFI does not support connecting through RD Web / Gateway.**

116. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringAuthOnly
117. https://kb.igel.com/en/igel-apps/current/igel-azure-virtual-desktop
118. https://kb.igel.com/en/igel-apps/current/igel-windows-365

Auth Only	Profile Template	Notes **Refer to:** IAFI Configuration Guide - Auth Only
Citrix Workspace App		This is configured to automatically reconnect to “active or disconnected sessions” and to auto start a single published app or desktop after successful login. It does not have any auto launch of a specific app, but that could be configured if desired. For Citrix Workspace App settings, refer to: Citrix Workspace App[119]
Omnissa Horizon - Roaming Desktops		This is configured to auto launch a desktop after logging into the Horizon client. That can be modified if you’d like. For Horizon client settings, refer to: Omnissa Horizon Client[120]
Omnissa Horizon - Roaming Apps		This is configured to not auto launch any Horizon apps. The user will see the native Horizon chooser and can manually pick apps to start. The chooser will also remain available for other apps. Horizon will automatically reconnect disconnected apps or roam any of the users active or disconnected apps when they log in again. For Horizon client settings, refer to: Omnissa Horizon Client[121]

119. https://kb.igel.com/en/igel-apps/current/citrix-workspace-app
120. https://kb.igel.com/en/igel-apps/current/vmware-horizon-client
121. https://kb.igel.com/en/igel-apps/current/vmware-horizon-client

Kiosk Mode	Profile Template	Notes - see this: IAFI Workflow Configuration Options[122]
Citrix Virtual Kiosk **This is not an Imprivata VDA licensed workflow.**		Windows 11 Citrix Desktop OS with Imprivata Type 2 agent
Citrix Epic Only **This is not an Imprivata VDA licensed workflow.** • The Epic EHR (Epic) is delivered to the thin client via Citrix Virtual Apps application virtualization. Epic is the only application that is available on the thin client. This configuration is known as Epic Only mode. • The thin client establishes a Citrix session using generic user credentials. While Epic remains running under the generic user credentials, users authenticate to the Imprivata Connector for Epic Hyperdrive (Connector), and work under their credentials. • When the Connector detects a user switch, Imprivata Enterprise Access Management keeps Epic open, while switching the user that is logged in.		Connecting to a Windows Server with the Imprivata Type 3 agent. This config supports the Imprivata Epic Only workflow where a user will log directly into Epic using the Imprivata Windows Agent on the remote server. **BEST PRACTICE: Epic should be the only application launched from the preconfigured Citrix session. If other apps are opened from Citrix, this could break the Imprivata virtual channel and the workflow.** See this: Configuring Epic Only Virtual Kiosks for Citrix XenApp[123]
Horizon Virtual Kiosk **This is not an Imprivata VDA licensed workflow.**		Windows 11 Horizon Desktop OS with Imprivata Type 2 agent
Microsoft AVD Virtual Kiosk **This is not an Imprivata VDA licensed workflow.**		Windows 11 AVD Single Session with Imprivata Type 2 agent NOTE: This not a Win 11 Multi-Session or Windows Server.

122. https://kb.igel.com/en/igel-apps/current/iafi-workflow-configuration-options
123. https://docs.imprivata.com/onesign/content/topics/imprivataplatform/vda/fus/citrixxafusepiconly.html

Kiosk Mode	Profile Template	Notes - see this: IAFI Workflow Configuration Options
Microsoft RDP Virtual Kiosk **This is not an Imprivata VDA licensed workflow.**		Windows 11 RDP Desktop OS with Imprivata Type 2 agent

Fast User Switching (FUS)	Profile Template	Notes
Citrix Persistent App (Epic) **IMPORTANT: This is an Imprivata VDA licensed workflow.**		IAFI will be in full lockscreen mode and will automatically launch a preconfigured Citrix session for Epic using a generic account. Each Imprivata user that logs in and has VDA licensing assigned will get access to their own Citrix resources available in the IAFI chooser which is configured in Windowed Mode. For reference, please see this: Configuring Persistent Applications for Citrix XenApp with Manually Launched Applications[124]
Citrix Epic FUS **This is not an Imprivata VDA workflow like the Persistent App feature noted above.**		IAFI will be in full lockscreen mode and will automatically launch a preconfigured Citrix session for Epic using a generic account. Access to a local app like a browser is optional. IAFI also has a FUS feature to run a command script to close a local app on user logout or switch. **BEST PRACTICE: Epic should be the only application launched from the preconfigured Citrix session. If other apps are opened from Citrix, this could break the Imprivata virtual channel and the workflow.** **NOTE: This profile contains a post session command. If a user closes Epic, IGEL OS will logoff Citrix and the OS and return the user back to the IAFI lock screen. This will restart the preconfigured Epic session.**

124. https://docs.imprivata.com/onesign/content/topics/imprivataplatform/vda/xenapps/persistentapps.html

Fast User Switching (FUS)	Profile Template	Notes
Horizon Epic FUS **This is not an Imprivata VDA workflow like the Persistent App feature noted above.**		IAFI will be in full lockscreen mode and will automatically launch a preconfigured Horizon session for Epic using a generic account. Access to a local app like a browser is optional. IAFI also has a FUS feature to run a command script to close a local app on user logout or switch. **BEST PRACTICE: Epic should be the only application launched from the preconfigured Horizon session. If other apps are opened from Horizon, this could break the Imprivata virtual channel and the workflow.** **NOTE: This profile contains a post session command. If a user closes Epic, IGEL OS will logoff and bring the user back to the IAFI lock screen.**

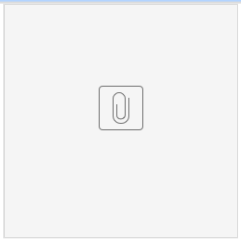
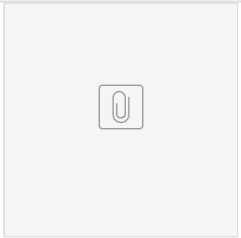
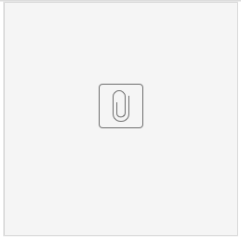
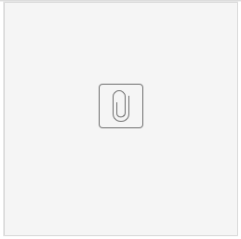
Debug Logging Templates:

Debug Profiles	Profile Template	Notes
		Start with the Base OS debug profile, then add IAFI debug and the client logging profile as needed (AVD, Citrix, Horizon) **See this:** How to Enable and Export IAFI Debug Logging for Troubleshooting[125]
OS 12 Base Debug, TCPDump		Enable Debug Logging for the Base OS. Remote Management Debug logging is disabled, and existing logs are deleted on boot.

125. https://kb.igel.com/en/igel-apps/current/how-to-enable-and-export-iafi-debug-logging-for-tr

Debug Profiles	Profile Template	Notes **Start with the Base OS debug profile, then add IAFI debug and the client logging profile as needed (AVD, Citrix, Horizon)** **See this:** How to Enable and Export IAFI Debug Logging for Troubleshooting
IAFI Debug Logging		Enables IAFI debug logging
AVD Debug Logging		Enables AVD debug logging
Citrix Debug Logging		Enables Citrix debug logging
Horizon Debug Logging		Enables Horizon debug logging

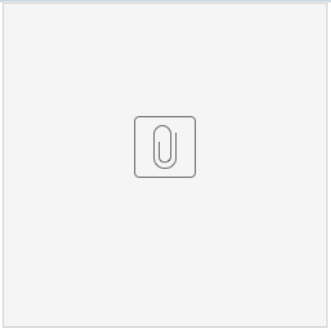
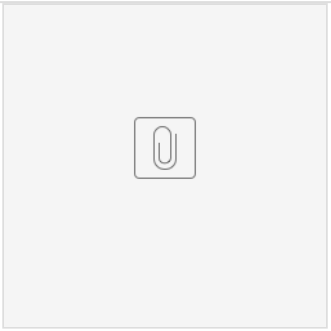
Non-workflow Templates:

Miscellaneous	Profile Template	Notes
IAFI Restart Agent		Custom App that restarts IAFI without rebooting IGEL OS. How to Create a Profile to Restart the IGEL Agent for Imprivata[126]
Ignore PCSC Readers		See the **Ignore Readers** setting in this article Configuration of the IGEL Agent for Imprivata on IGEL OS[127]
Base OS 12 - System Lockdown Settings		This profile applies some best practice security settings for locking down IGEL OS 12 to limit what end users have access to. This is common for shared workstations. For example: • Disable access to Setup, App Portal, Shutdown device
Base OS 12 - Disable Suspend (Power Management)		This profile controls Power Management settings and sets the System Suspend / Shutdown on Inactivity to Never. This also disables access to the Power Management Settings.

126. https://kb.igel.com/en/igel-apps/current/how-to-create-a-profile-to-restart-the-igel-agent-
127. https://kb.igel.com/en/igel-apps/current/configuration-of-the-igel-agent-for-imprivata-on-i#ConfigurationoftheIGELAgentforImprivataonIGELOS-ConfiguringBasicSettings

Miscellaneous	Profile Template	Notes
Logoff Desktop Icon		This puts a Logoff icon on the IGEL desktop. If IAFI gets into a bad state, this can be used to logoff the IGEL device without rebooting which will restart the IAFI app and return to a known good state.

Known Good Settings	Profile Template	Notes
Citrix Global		Best Practice Citrix Settings for: • Keyboard • Native USB Redirection • Client Drive Mapping • HDX Multimedia
Citrix Dictation		Best Practice Citrix Settings for: • USB Redirection for Dictation devices (ex: Power Mic III / IV and Philips Speechmike)
Horizon Global		Best Practice Horizon Settings for: • Server Options • Local Logon • Window • Multimedia • Unified Communications

Known Good Settings	Profile Template	Notes
Horizon Dictation		Best Practice Horizon Settings for: • USB Redirection for Dictation devices (ex: Power Mic III and IV, Philips Speechmike)
AVD Dictation with IGEL Advanced Redirection **NOTE: IGEL Advanced Redirection is a licensed add-on feature. See this for more information** IGEL Advanced Device Redirection Add-On License[128]		Best Practice AVD Settings with IGEL Advanced Redirection for: • USB Redirection for Dictation devices

128. https://kb.igel.com/en/igel-subscription-and-more/current/igel-advanced-device-redirection-add-on-license

How to use the IAFI Guest Login option

Requirements: IAFI 1.3.0 or higher

Description

The feature was added in IAFI 1.3.0 and extends the domain dropdown menu of the Imprivata login screen with additional menu items. These guest sessions can be used by **non-licensed Imprivata users** without authenticating to the Imprivata Appliance

Examples:

- Nursing students or part-time workers that need access to organization resources on the IGEL devices from a virtual desktop or website.
- Hospital Information Portal for patients to access
- Entertainment for patients

User experience:

- When the guest user selects their choice, they need to click the Login button and IAFI will automatically start the session.
- Once they are finished, they can close the session and IAFI will return to the lockscreen
- If a licensed Imprivata user needs to access the machine, they can “tap over” the guest user and the guest session will be closed and the next user can access their resources.

Configuration

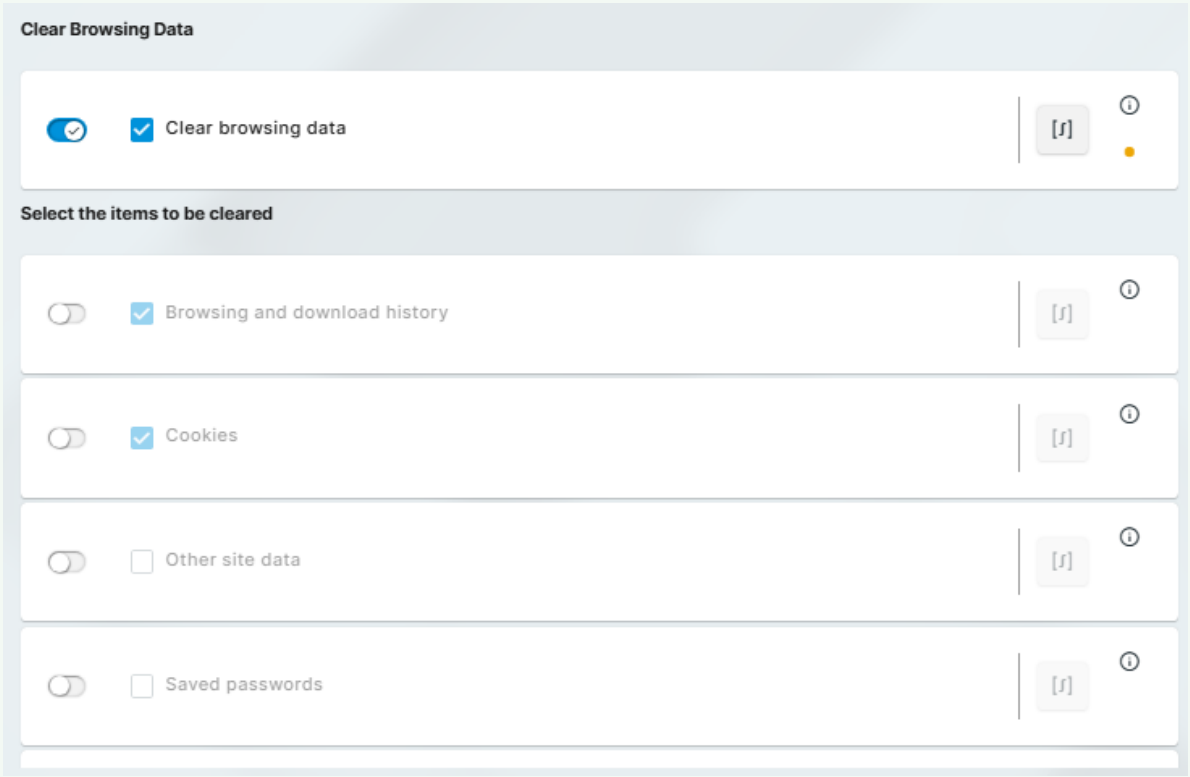
Step 1: In an OS 12 Web profile, create the guest session type(s) that you want to be available in the IAFI login screen

For each session type, make sure the corresponding OS 12 app is assigned and installed on the endpoint.

For this example, we will create four Guest Sessions

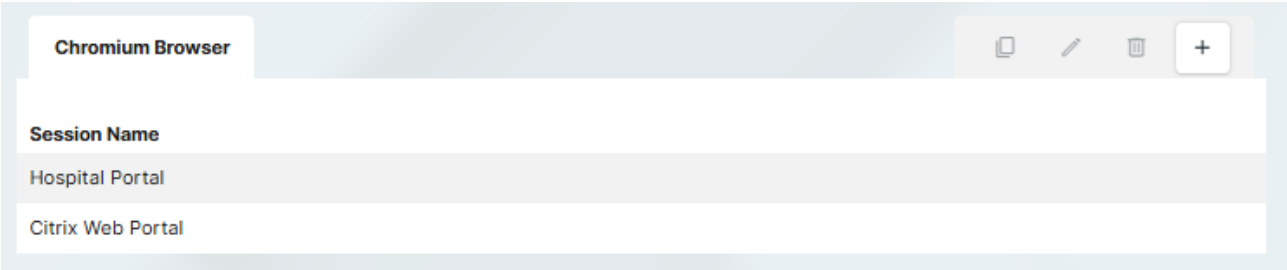
- AVD Guest - this will autostart the IGEL Microsoft AVD client and can be configured so the guest user has to manually log into the client to access their AVD resource(s)
- Citrix Web Portal - this will autostart a Chromium browser session and go to a Citrix Storefront login. The user can manually log in to access their Citrix resources.
- Hospital Portal - this will launch a Chromium browser and go to a hospital information portal
- Entertainment - this will launch a Media Player

Best Practice for browser sessions - in the Global settings, enable the option to **Clear Browsing Data** when the session is closed.

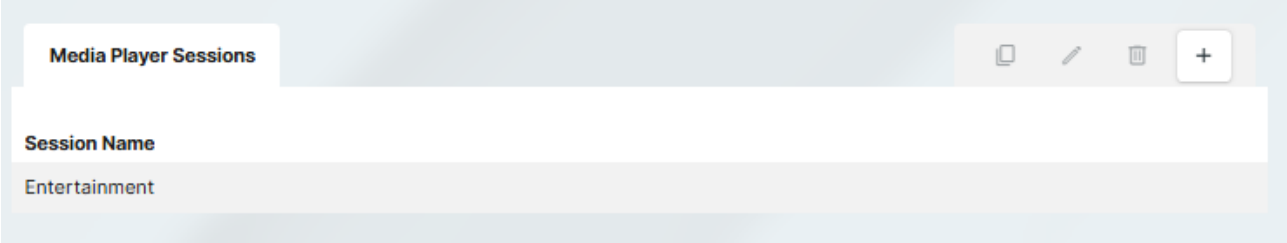


4 Setup/UMS profile: Apps > Chromium Browser > Global Settings > Privacy > Clear Browsing Data

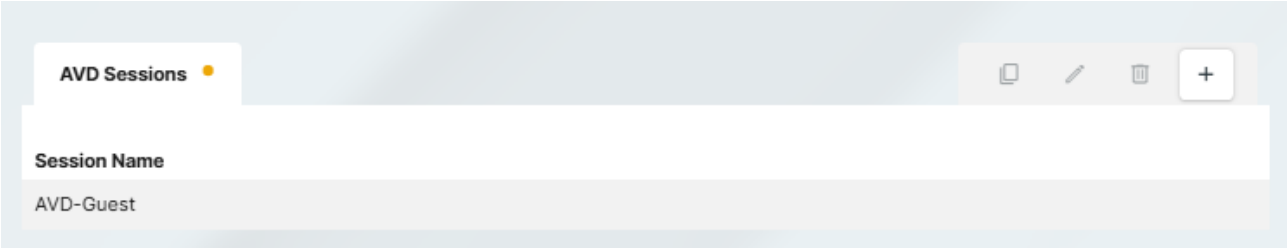
Setup/UMS profile



5 Setup/UMS profile: Apps > Chromium Browser > Sessions



6 Setup/UMS profile: Apps > Media Player > Media Player Sessions



7 Setup/UMS profile: Apps > AVD > AVD Sessions
Registry keys for Session Types

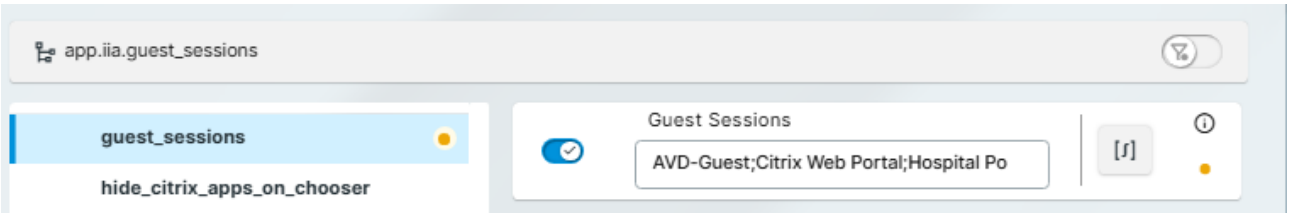
```
app.chromium.sessions.chromium0.name
Hospital Portal
```

```
app.chromium.sessions.chromium1.name
Citrix Web Portal
```

```
app.parole.sessions.parole0.name
Entertainment Channel
```

```
app.avd.sessions.avd0.name
AVD-Guest
```

Step 2: Go into the IAFI registry to add the names of the Guest Sessions you want to make available.



Registry key:

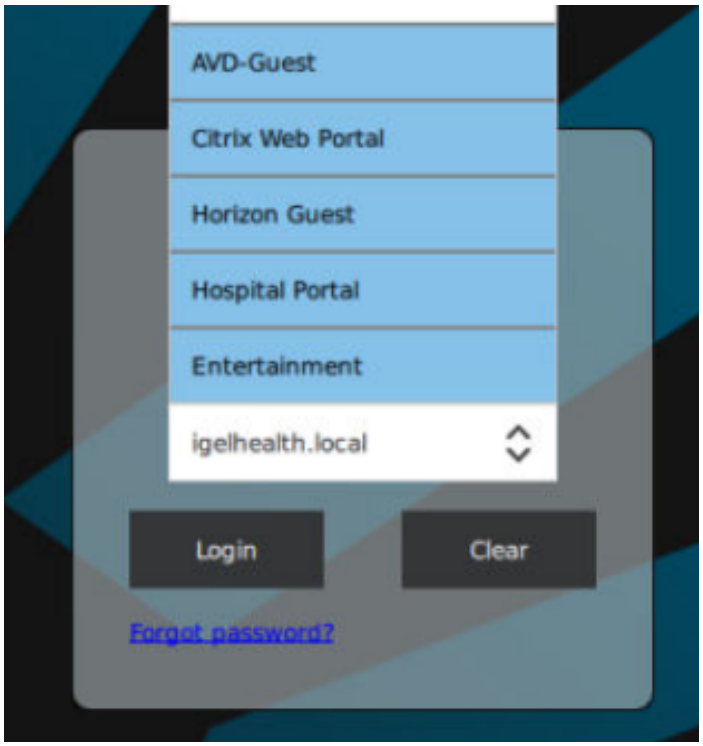
```
app.iia.guest_sessions
AVD Guest;Citrix Web Portal;Hospital Portal;Entertainment
```

The registry key can contain various entries separated by semicolons with no spaces.

The entries must refer to the exact name of the existing sessions.

Step 3: Save and apply the profile to the device

When the IAFI app restarts, you should now see the Guest Sessions available in the Domain drop down field.



Known Issue: Behavior with lock screen enabled

If lock screen and ‘keep session active’ option are enabled, the Windows session will stay active in the background if user taps out. In the case of opening a guest session, the Windows session in background was accessible for guest users. Expected behavior is that the previous user is signed off Windows session before guest application is started. We will implement a bug fix in IAFI 1.5.0.

Workaround: When using the Guest Login option, do not use the “keep session active” option in Imprivata VDA policy or in Auth Only mode.

IGEL for Windows



IGEL for Windows (formerly “IGEL Azure Virtual Desktop”) is a cloud-based desktop and app virtualization service that runs on the Azure cloud and lets users access Windows desktops and applications securely from IGEL OS devices.

Blogs about IGEL for Windows app can be found under One App. One Experience. Introducing IGEL for Windows.[129] and Introducing a new app from IGEL – IGEL for Windows app – The new app combining Windows 365 and Azure Virtual Desktop access – Built on the latest SDK code from Microsoft -Available now!![130]

IGEL Azure Virtual Desktop (AVD) app has been redesigned and renamed to “IGEL for Windows”. IGEL for Windows app combines AVD and Windows 365 CloudPC access in one app and can be downloaded on the IGEL App Portal[131].
Note the following:

- IGEL for Windows is fully compatible with IGEL AVD. This means that the existing AVD sessions and settings will still work and the UMS profiles created for IGEL AVD app will automatically apply to IGEL for Windows app. No app reselection in the existing UMS profiles for IGEL AVD is required.
- Registry keys remain unchanged and are still “**apps > avd**”.
- IGEL for Windows app replaces IGEL Windows 365 app. Therefore, if you are using IGEL Windows 365 app, it is necessary to import IGEL for Windows app to your IGEL UMS, create new profiles based on this app and assign them to your devices.

- How to Configure IGEL for Windows Session (see page 323)

For the previous version of documentation about IGEL AVD app, see

129. https://www.igel.com/blog/igel-for-windows-app/
130. https://virtualbrat.com/2026/03/31/introducing-igel-windows-app-the-new-app-combining-windows-365-and-azure-virtual-desktop-built-on-the-latest-sdk-code-from-microsoft/
131. https://app.igel.com/avd/1.4.0+1


IGEL Azure Virtual Desktop

How to Configure IGEL for Windows Session

This article describes how you can create an IGEL for Windows session and configure it on IGEL OS. IGEL for Windows was formerly IGEL Azure Virtual Desktop; for details, see IGEL for Windows[132].

Requirements

- IGEL OS 12.5 or higher
- IGEL for Windows app is imported to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[133].

Known Limitations

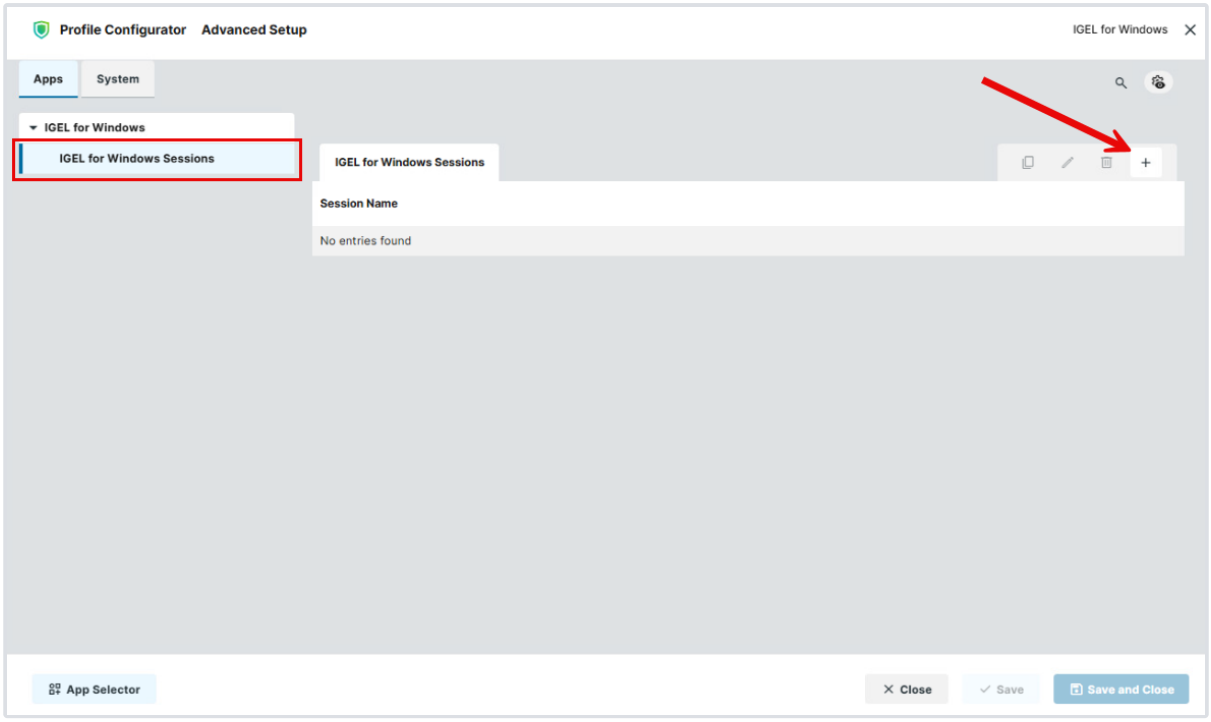
- The device must support SSE4.1 at least.

How to Create a Session

This is how you can create an IGEL for Windows session via the profile configurator:

1. In the IGEL UMS, create a profile configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[134].
2. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions** and click **+**.

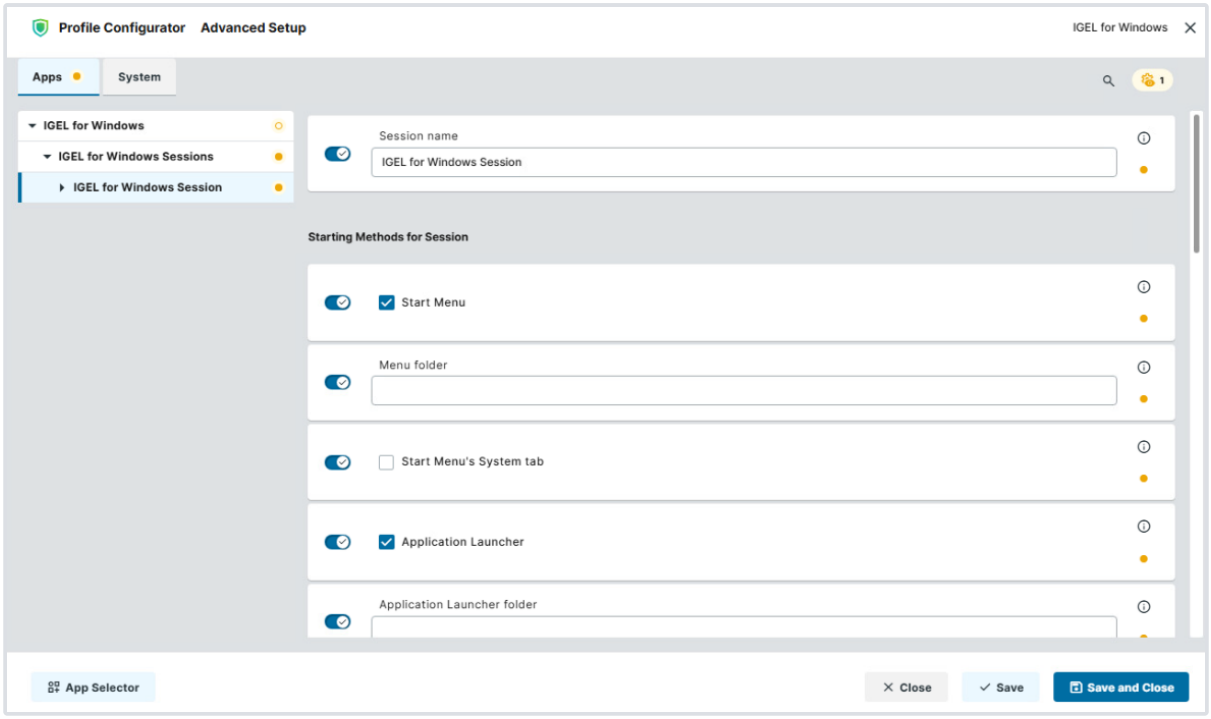
132. https://kb.igel.com/en/igel-apps/current/igel-azure-virtual-desktop
133. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
134. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



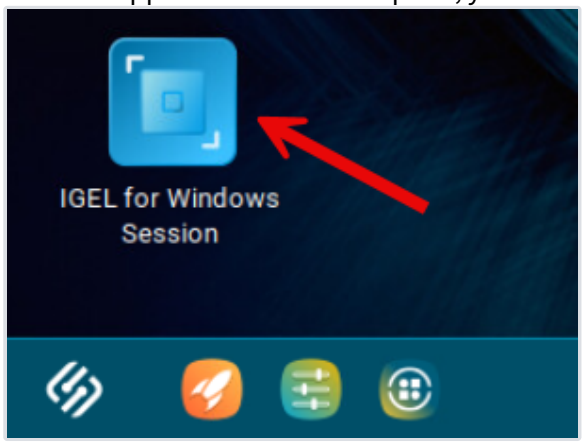
The session is created.

3. Configure the starting methods for the created session. For details, see Starting Methods for Apps[135].

135. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps



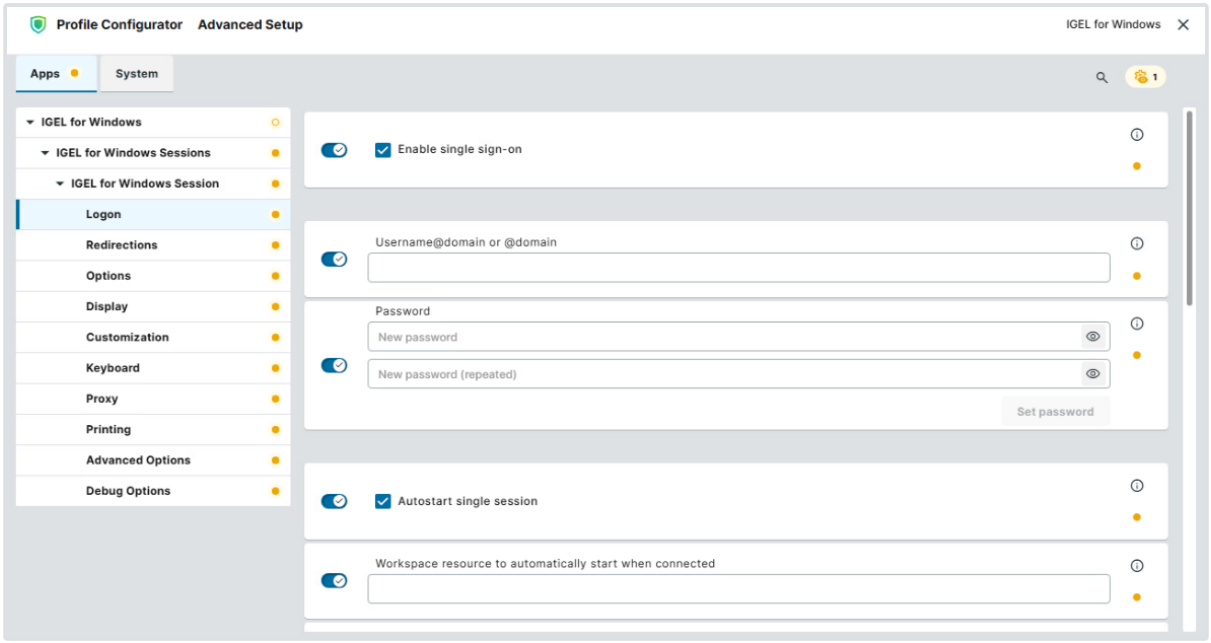
4. Edit the settings described below according to your needs.
5. Save the settings and assign the profile to the required devices / device directories. For details on profile assignment, see How to Create and Assign Profiles in the IGEL UMS Web App[136].
   After the app installation is complete, you can start the IGEL for Windows session:



Configuring the Logon

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Logon**.

136. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



2. Edit the settings according to your needs. The parameters are described below.

Enable single sign-on

- ☑ The user is automatically authenticated via the configured SSO and does not have to re-enter the credentials to log in to the remote Windows session. (Default)
  For how to configure SSO, see How to Configure Single Sign-On (SSO) on IGEL OS 12[137] and Single Sign-On in IGEL OS 12[138].
- ☐ Authentication via SSO is disabled.

Username@domain or @domain

The user name or a preset domain name that will be used for the automatic connection to the remote Windows session. The string after "@" is taken as a preset domain name.

Example:

`avd@your.domain.com` : To log in, the user does not need to enter the username and the domain name.

`@your.domain.com` : To log in, the user only needs to enter the username, e.g. `avd` . The preset domain – `your.domain.com` – will automatically be appended.

137. https://kb.igel.com/en/igel-os-base-system/current/how-to-configure-single-sign-on-sso-on-igel-os-12
138. https://kb.igel.com/en/igel-os-base-system/current/single-sign-on-in-igel-os-12

Overwriting the Preset Domain Name

Use the setting **Allow preset domain overwrite** to specify whether the user should be able to overwrite the preset domain, e.g. with `username@other-domain.com`.

If you define preset domain `@your.domain.com` under **Username@domain or @domain**, the setting **Show local login dialogue** must be set to “Auto” or “Always”.

Password

This password is used for the automatic connection to the remote Windows session. Click **Set password** to save the password.

Autostart single session

- [x] If there is only one published app or desktop session configured for the user, it will be started automatically upon successful authentication. (Default)
- [ ] The picker for resource selection is always displayed.

Workspace resource to automatically start when connected

Name of the specific published app or desktop session that is to be started automatically upon successful authentication.

Autostart session in background

- [x] A published app or desktop session that is started automatically is displayed in preview mode. The user must actively click on it to connect.
- [ ] A published app or desktop session that is started automatically is displayed in full-screen mode. (Default)

Resources to download

The following resource types will be shown for the user.

Possible values:

- **Desktop + Apps**
- **Desktops**
- **Apps**

Show local login dialog

Possible values:

- **Auto**: When a domain under **Username@domain or @domain** is preset like "@igel.com", the local login dialog will be shown automatically. (Default)
- **Always**: Before logging in via Entra ID, the local dialog for the user name and password will always be displayed.
- **Never**: The local dialog for the user name and password will never be displayed.

Example:



Hide the Microsoft Entra ID login

- ☑ Microsoft Entra ID login dialog will not be displayed.
- ☐ Microsoft Entra ID login dialog will be displayed. (Default)

Max. time the Microsoft Entra ID login will be hidden in milliseconds!

Specifies the waiting time in milliseconds, until Microsoft Entra ID login dialog is automatically shown to the user. This setting is active if **Hide the Microsoft Entra ID login** is enabled. (Default: 5000)

Remember previous username

Possible values:

- **Auto**: The same as **Enabled** (Default)
- **Enabled**: The previously entered username will be remembered and prefilled by the next login.
- **Disabled**: The previously entered username will not be remembered and used for the next login.

Allow preset domain overwrite

- The domain entered by the user is accepted.
- The domain entered by the user is replaced with the preset domain configured under **Username@domain or @domain**. (Default)

Always prompt for username and password upon session host connection

- The user will be forced to re-enter his username and password each time when connecting to the remote Windows session. Use this setting if the login credentials configured under **Username@domain or @domain** and **Password** should not be applied automatically.
- The user will not be forced to re-enter his username and password each time when connecting to the remote Windows session. (Default)

Always prompt for password upon session host connection

- The user will be forced to re-enter his password each time when connecting to the remote Windows session. Use this setting if the password set under **Password** should not be applied automatically.

On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result.

- The user will not be forced to re-enter his password each time when connecting to the remote Windows session. (Default)

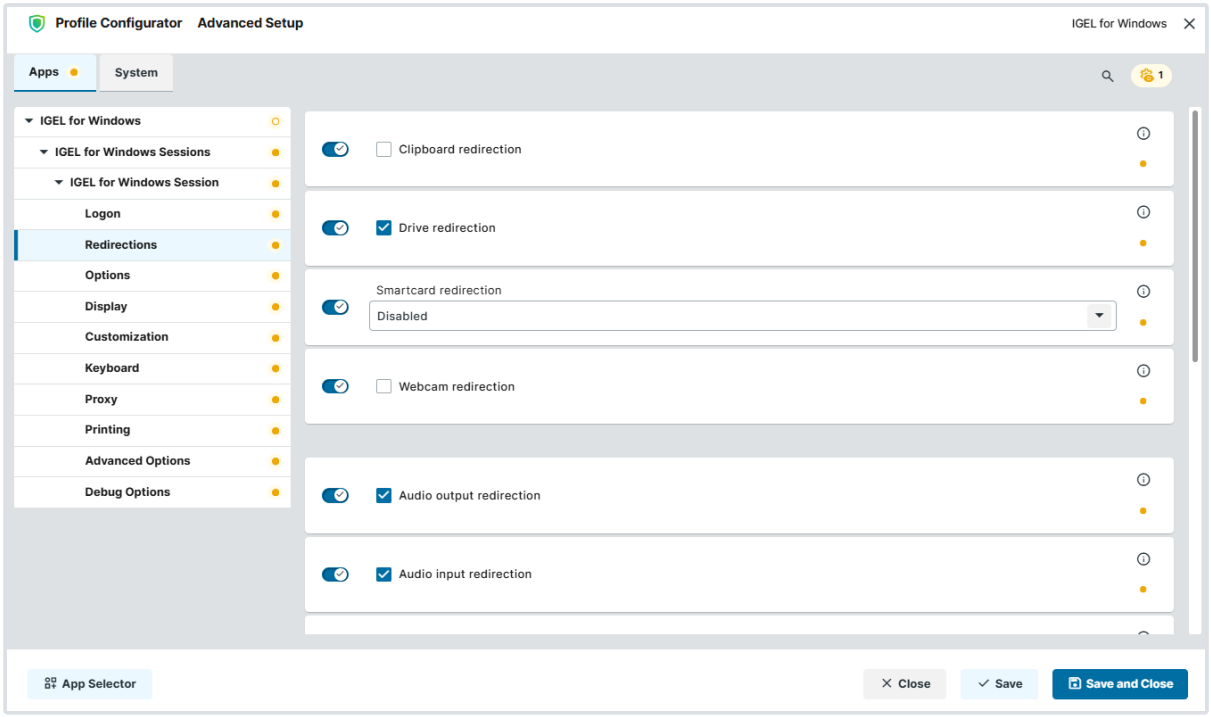
Deny empty passwords

Specifies if empty passwords can be used in the local login dialogue if it is enabled under **Show local login dialogue**.

- Empty passwords are forbidden. (Default)
- Empty passwords are allowed. Note, however, that empty passwords pose a security risk and should be avoided.

Editing the Redirections

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Redirections**.



2. Edit the settings according to your needs. The parameters are described in the following.

Clipboard redirection

- Text and images from the clipboard are shared between the IGEL for Windows session and the local client.
- Text and images from the clipboard cannot be shared between the IGEL for Windows session and the local client. (Default)

Drive redirection

- Redirection is bound to the `/media` folder, so that locally mounted storage devices, including USB sticks, are forwarded to the IGEL for Windows session. (Default)

Smartcard redirection

Possible values:

- **Disabled**: Smartcards are not forwarded to the remote Windows session. (Default)
- **Enabled**: Smartcards are forwarded from the local device to the remote Windows session. The Microsoft RdClientSDK implementation is used.
- **IGEL**: Smartcards are forwarded from the local device to the remote Windows session. A custom IGEL implementation is used. For details on the use of smartcards in IGEL OS, see How to Use Smart Card and Smart Key Authentication in IGEL OS 12[139].

Webcam redirection

- ☑ Local webcams are forwarded to the IGEL for Windows session.
- ☐ Local webcams are not forwarded to the IGEL for Windows session. (Default)

Audio output redirection

- ☑ The audio output is redirected between the IGEL for Windows session and the local client. (Default)

Audio input redirection

- ☑ The audio input (microphone) is redirected between the local client and the IGEL for Windows session. (Default)

AAC codec

- ☑ The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

H264 hardware acceleration

- ☑ H.264 hardware acceleration is activated and used to offload the decoding / encoding of H.264 video to a specialized hardware component. A compatible GPU on the endpoint device is required. (Default)
- ☐ H.264 hardware acceleration is not used. Disabling H.264 hardware acceleration may be considered if your hardware does not support it and/or you experience black screens, battery problems, app crashes or similar.

H264 hardware acceleration level

Possible values:

- **Video content**: H.264 hardware acceleration will only be used for the playback of videos.
- **Fullscreen**: H.264 hardware acceleration will be used for the complete desktop. (Default)

Serial port redirection

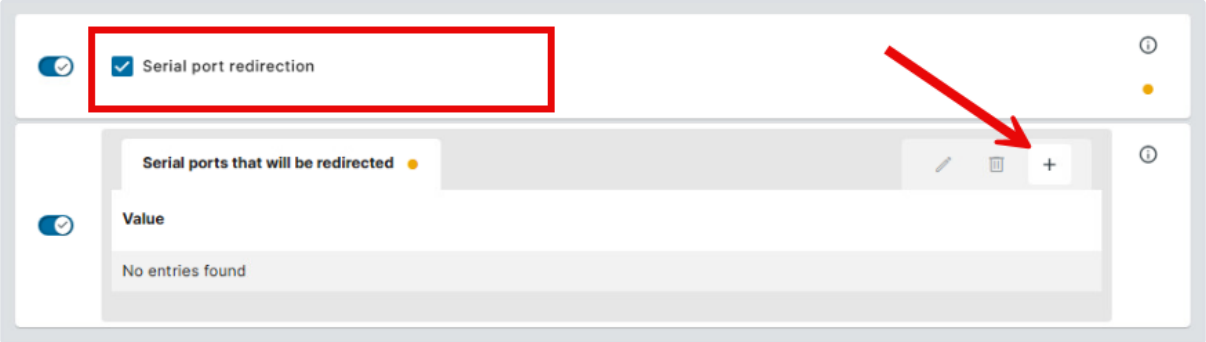
- ☑ Devices connected to the serial port(s) of the IGEL OS endpoint will be redirected to the remote session.
- ☐ Devices connected to the serial port(s) of the IGEL OS endpoint will not be forwarded to the remote session. (Default)

To add serial port redirection:

---

139. https://kb.igel.com/en/igel-os-base-system/current/how-to-use-smart-card-and-smart-key-authentication

1. Enable **Serial port redirection**.
2. Click **+** to define the serial port to be redirected.



3. Specify the port under **Serial ports that will be redirected**.

   Example:



How to Find the Serial (COM) Port Number

1. Open a terminal.
2. Run the following commands: `dmesg | grep tty` or `ls /dev/tty*`
3. Identify your device (commonly `/dev/ttyUSB0` or `/dev/ttyS0`).

4. Click **Confirm** to save the settings.

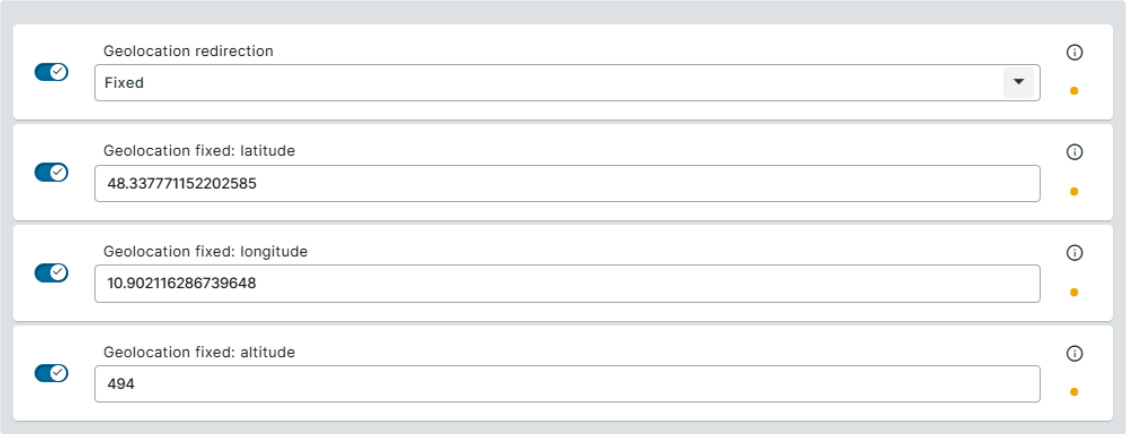
Geolocation redirection

Configures and enables location redirection on the local device. Note that it must also be configured on the server side, see e.g. Configure location redirection over the Remote Desktop Protocol[140].

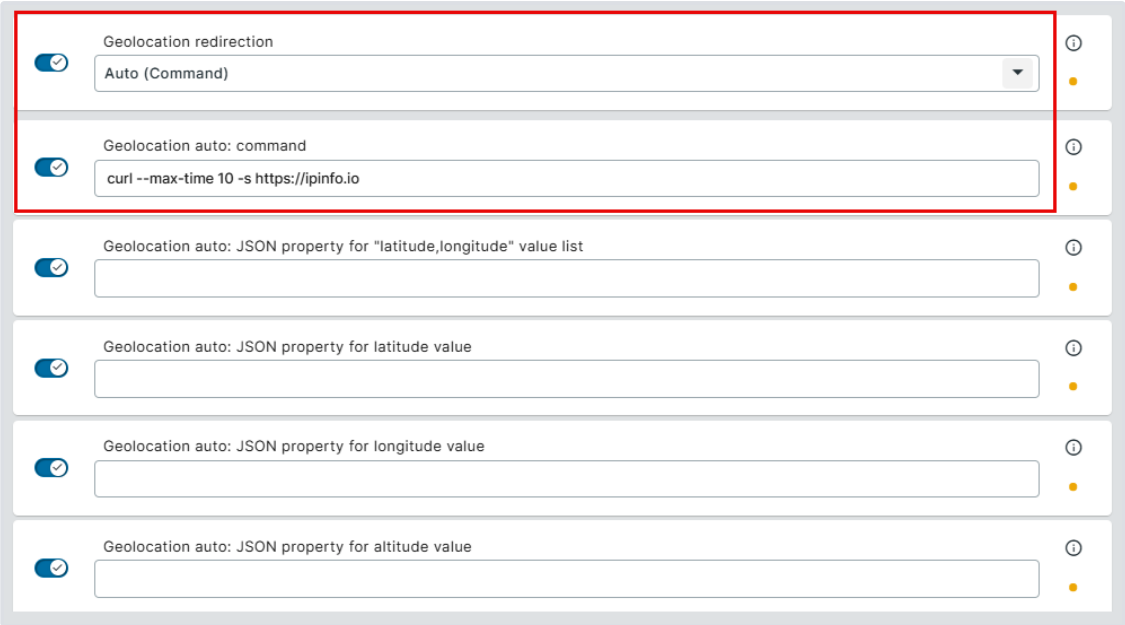
Possible values:

140. https://learn.microsoft.com/en-us/azure/virtual-desktop/redirection-configure-location?tabs=intune&pivots=azure-virtual-desktop

- **Off**: Geolocation information is not forwarded to the remote session. (Default)
- **Fixed**: Geolocation information is forwarded to the remote session. The location is manually defined as fixed geographic coordinates in the following fields:
  - **Geolocation fixed: latitude**: Fixed latitude value for the geolocation
  - **Geolocation fixed: longitude**: Fixed longitude value for the geolocation
  - **Geolocation fixed: altitude**: Fixed altitude value for the geolocation



- **Auto (Command)**: Geolocation information is forwarded to the remote session. To dynamically detect the current location, the custom command must be defined under **Geolocation auto: command**.
  - **Geolocation auto: command**: Shell command to be executed in order to dynamically detect the geolocation. The command needs to look up your public IP address.
    If you use the command `curl --max-time 10 -s https://ipinfo.io`, it is not necessary to define other settings.
    Note that `https://ipinfo.io` is a commercial service and requires a valid license. It is only an example service here.
    Example:



If you use your own command, note that the command must return a valid JSON response that contains the JSON property specified by the related setting below:

- **Geolocation auto: JSON property for "latitude,longitude" value list**: Name of the JSON property that contains the "latitude,longitude" value list

  Example: `loc`

  if the JSON file contains `"loc" : "48.337771152202585,10.902116286739648"`
- **Geolocation auto: JSON property for latitude value**: Name of the JSON property that contains the "latitude" value

  Example: `lat`

  if the JSON file contains `"lat" : "48.337771152202585"`
- **Geolocation auto: JSON property for longitude value**: Name of the JSON property that contains the "longitude" value

  Example: `long`

  if the JSON file contains `"long" : "10.902116286739648"`
- **Geolocation auto: JSON property for altitude value**: Name of the JSON property that contains the "altitude" value

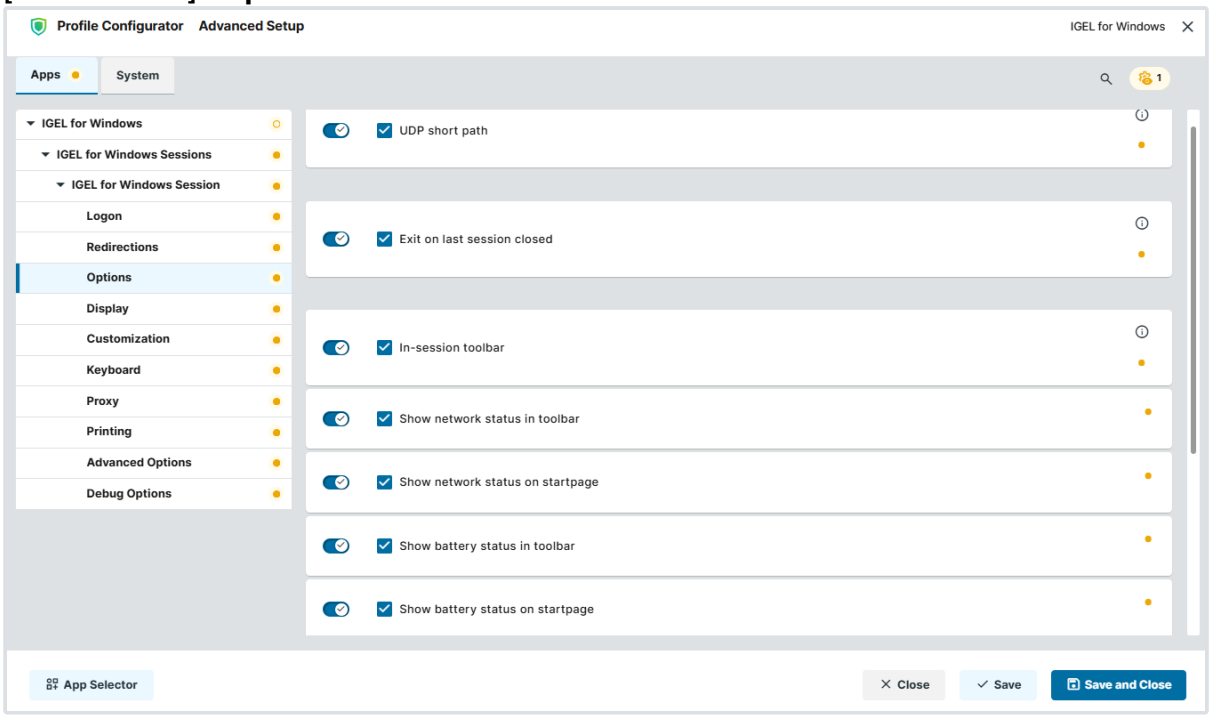
  Example: `alt`

  if the JSON file contains `"alt" : "494"`

For further information on geolocation redirection, see the blog IGEL for Windows app – for Windows 365 and AVD tech preview- New Feature – Geo Location Redirection – From now on your online ordered Pizzas will not end up at the Microsoft Azure Datacenters![141]

Editing the Options

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Options**.



2. Edit the settings according to your needs. The parameters are described below.

UDP short path

☑ RDP short path is activated. A direct UDP-based connection to the session host will be established. (Default)

Exit on last session closed

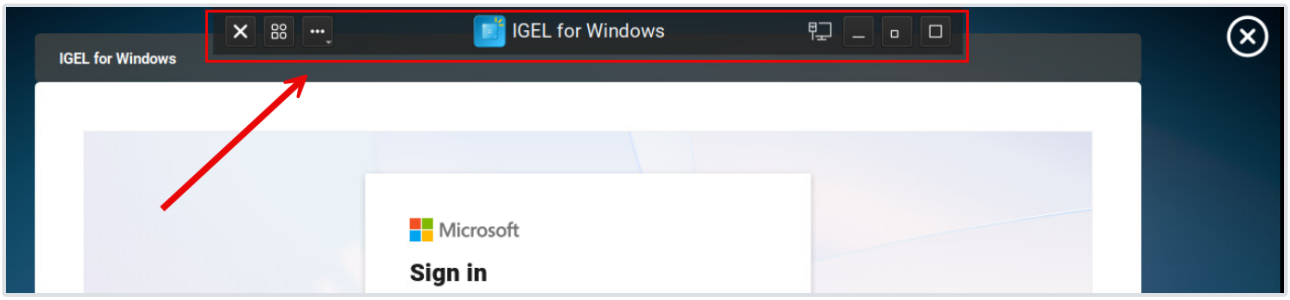
☑ When the last session window is closed, the entire IGEL for Windows client automatically closes. (Default)

In-session toolbar

141. https://virtualbrat.com/2026/03/31/igel-windows-app-new-feature-geo-location-redirection-from-now-on-your-online-ordered-pizzas-will-not-end-up-at-the-microsoft-azure-datacenters/

Allows you to minimize / maximize the session window, open Virtual Channel Statistics, view network and battery status if enabled, close the session.

- ☑ The in-session toolbar is activated and will be shown in the IGEL for Windows session as soon as you move the cursor to the top edge of the screen. (Default)



Show network status in toolbar

- ☑ The current network status of the IGEL OS device is displayed on the in-session toolbar. (Default)

Show network status on startpage

- ☑ The current network status of the IGEL OS device is displayed on the login window and in the resource picker. (Default)

Show battery status in toolbar

- ☑ The current status of the battery of the IGEL OS device is displayed on the in-session toolbar. (Default)

Show battery status on startpage

- ☑ The current status of the battery of the IGEL OS device is displayed on the login window and in the resource picker. (Default)

Custom session name

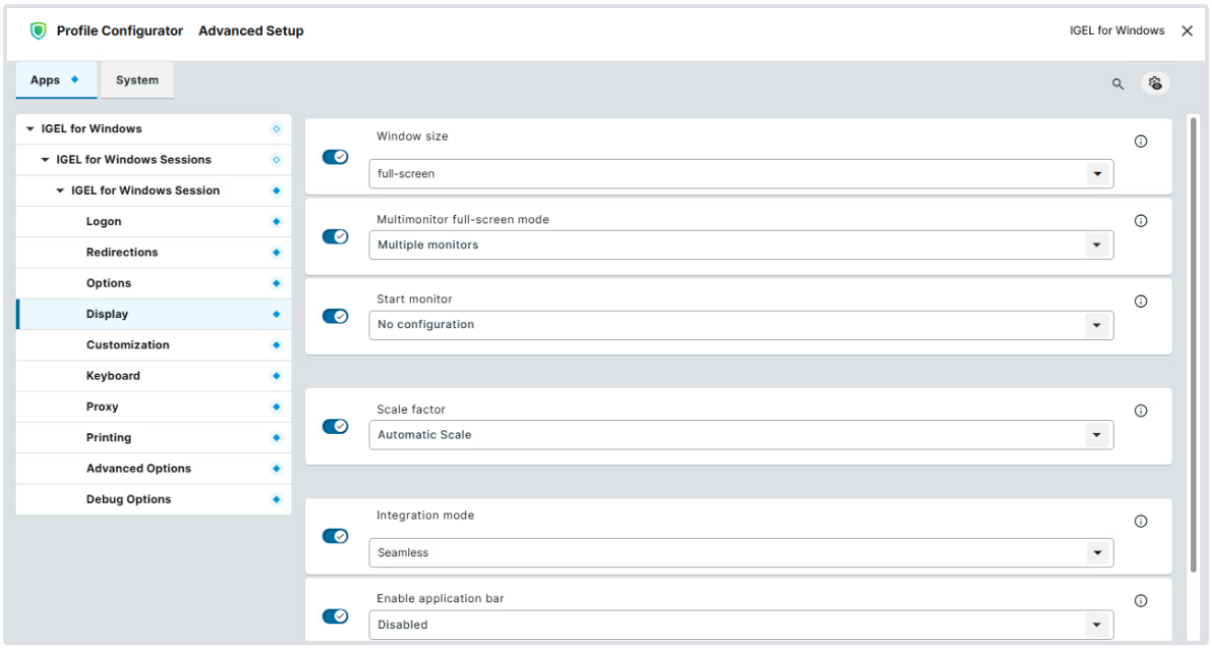
- ☑ The client name will not be “IGEL for Windows”, but will reflect the session name specified under **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Session name**.
- ☐ The client name will be “IGEL for Windows”. (Default)

Disconnect notification timeout

Time in seconds the notification window informing about the disconnection to the remote session is displayed. (Default: 5)

Configuring the Display

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Display**.



2. Edit the settings according to your needs. The parameters are described below.

Window size

Specifies the width and height of the window.

Possible options:

- **Full-screen**: The session is shown on the full screen. The device's taskbar is not visible. (Default)
- **Work area**: The session is shown on the full screen, minus the area needed by the device's taskbar.
- **[Numeric details]**: The session is shown in the selected resolution or on the selected percentage of the screen area.

Multimonitor full-screen mode

This setting is relevant if more than one monitor is connected to the terminal.

Possible options:

- **Single monitor**: Restricts the full-screen session to one monitor.
- **Multiple monitors**: Displays the full-screen session on multiple monitors. (Default)

- **Expand to all monitors**: Expands the full-screen session across all monitors.

Start monitor

Specifies the monitor on which the session is displayed.

Possible options:

- **No configuration**: The monitor is selected according to the current position of the mouse pointer. (Default)
- **1st monitor** ... **8th monitor**: The selected monitor is the start monitor.

Scale factor

Specifies the desktop scaling in percent.

Possible values:

- **Automatic scale**: The resolution set under **User Interface > Display > Options > Monitor DPI** is used for the session. (Default)
- Numeric details: The display is magnified by the factor given here.

Integration mode

Possible values:

- **Immersive**: Remote apps are displayed with one container window.
- **Seamless**: Remote apps are displayed with individual windows per app on the desktop. (Default)

Enable application bar

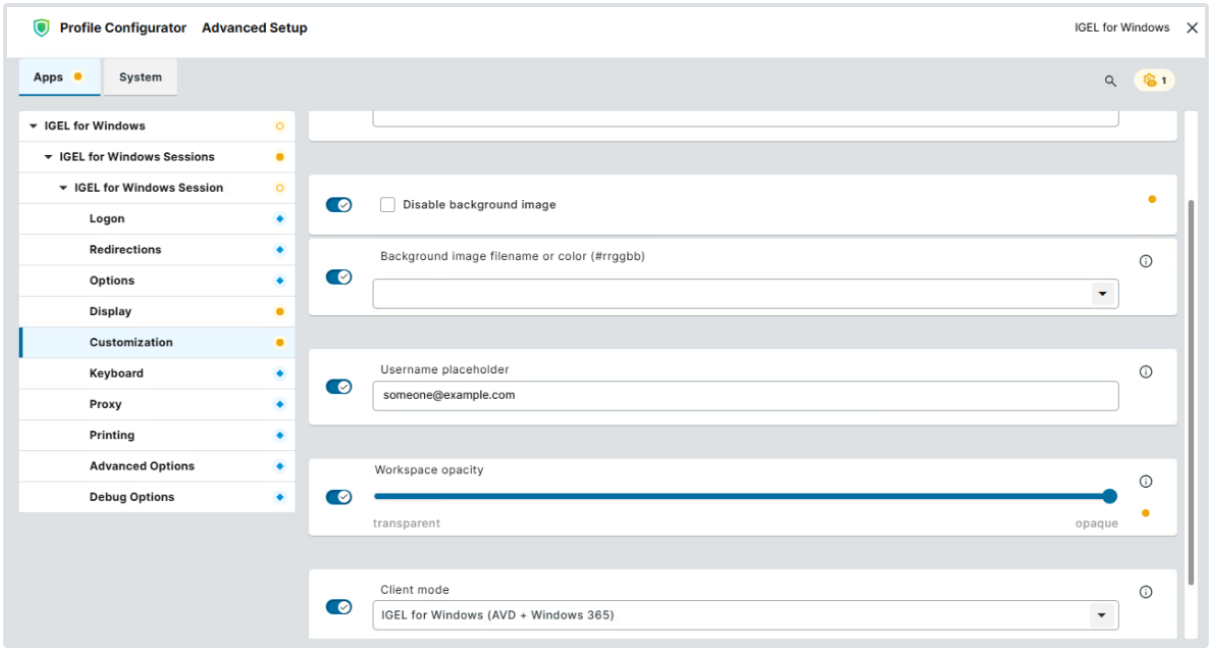
The application bar displays active sessions and provides a quick way to switch between them.

Possible values:

- **Auto**: When remote apps are started, the application bar is activated automatically. (Default)
- **Enabled**: The application bar is always activated.
- **Disabled**: The application bar is never shown.

Setting the Customization

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name]** > **Customization**.



2. Edit the settings according to your needs. The parameters are described below.

Disable company logo

- ☑ Custom company logo cannot be specified. IGEL company logo will not be displayed in the IGEL for Windows session.
- ☐ Company logo can be defined for the IGEL for Windows session under **Logo image filename**. If not defined, IGEL company logo will be displayed at the bottom of the IGEL for Windows session window. (Default)

Logo image filename

Name of the company logo file. The download source must be configured for the base system under **User Interface > Desktop > Background (1st Monitor) > Custom Wallpaper Server**, see Custom Wallpaper Server[142].

Disable background image

- ☑ Custom background image cannot be specified.
- ☐ Custom background image or custom color can be defined for the IGEL for Windows session under **Background image filename or color (#rrggbb)**. (Default)

Background image filename or color (#rrggbb)

Possible values:

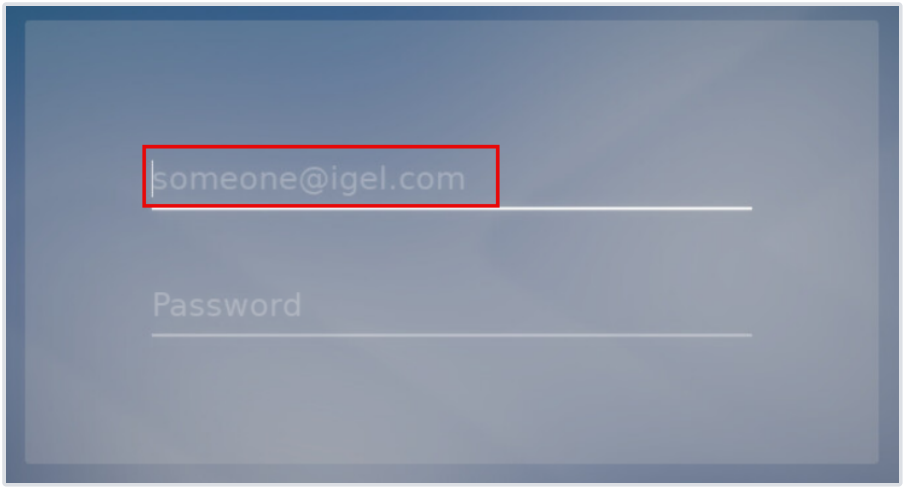
142. https://kb.igel.com/en/igel-os-base-system/current/custom-wallpaper-server

- **From Desktop Background**: Background defined under **User Interface > Desktop > Background (1st Monitor) > Wallpaper (1st monitor)** will be applied to the IGEL for Windows session.
- **[Color]**: Type the color code in the format `#rrggbb`.
- **[Background image filename]**: Name of the background image file. The download source must be configured for the base system under **User Interface > Desktop > Background (1st Monitor) > Custom Wallpaper Server**, see Custom Wallpaper Server[143].

Username placeholder

Text shown for the username field in the local login dialog. It should provide hints on what to input, e.g. `username@example.com`, `name@company.com` (Default: `someone@example.com`)

Example:



Workspace opacity

Defines the opacity of the workspace during the login and in the resource picker in the range between 0 (fully transparent) and 100 (fully opaque). (Default: 100)

Example:

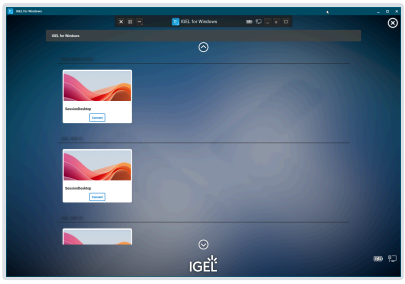
Workspace opacity set to “0” (fully transparent):

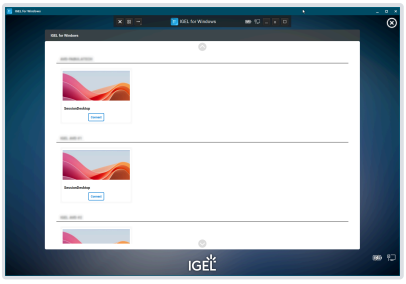
Workspace opacity set to “50”:



Workspace opacity set to “100” (fully opaque):

143. https://kb.igel.com/en/igel-os-base-system/current/custom-wallpaper-server





Client mode

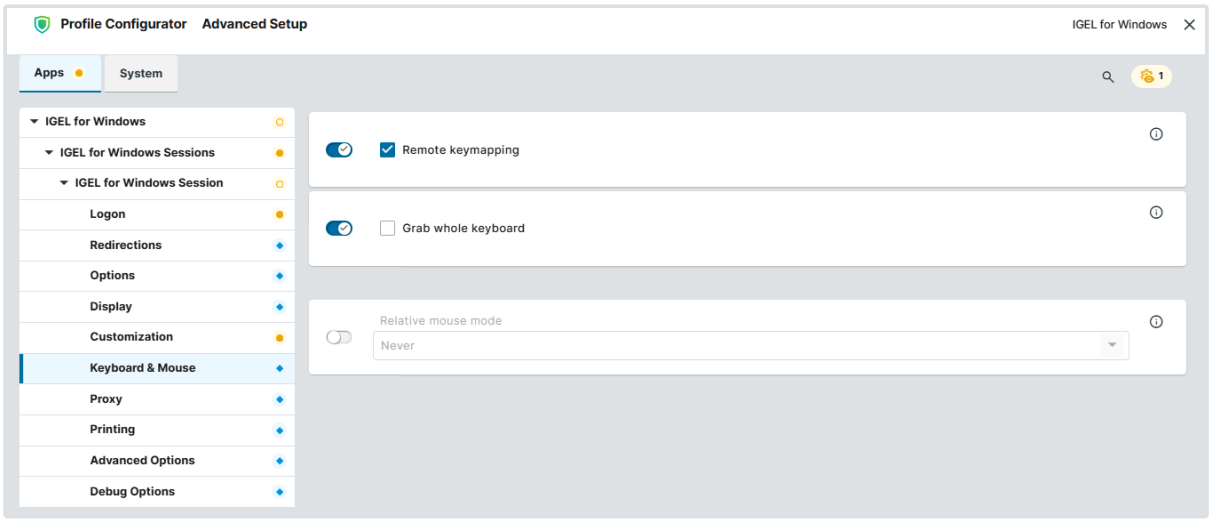
Defines user interface layout for the IGEL for Windows session.

Possible values:

- **IGEL for Windows (AVD + Windows 365)**: Fully supports AVD and Windows 365 sessions. (Default)
- **IGEL Azure Virtual Desktop (AVD)**: Legacy user interface mode that uses the previous layout of IGEL AVD app
- **IGEL Windows 365 (Cloud PC)**: Legacy user interface mode that uses the previous layout of IGEL Windows 365 app

Configuring Keyboard and Mouse

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name]** > **Keyboard & Mouse**.



2. Edit the settings according to your needs. The parameters are described below.

Remote keymapping

- [x] Sends keyboard events as Windows scan codes. This ensures that the remote session fully respects the client's keyboard layout and mapping. It can be required for certain input methods to function correctly. (Default)
- [ ] Sends keyboard events as Unicode characters.

Grab whole keyboard

- [x] All local hotkeys will be forwarded to the remote Windows session, and therefore they will not function locally. For information on hotkeys in IGEL OS, see e.g. Hotkeys[144].
- [ ] Local hotkeys will not be forwarded to the session. (Default)

Relative mouse mode

Allows the mouse to move beyond the borders of the screen. Relative mouse mode is typically used in 3D applications and video games. For further information, see the blog IGEL for Windows app – introducing Relative mouse support![145]

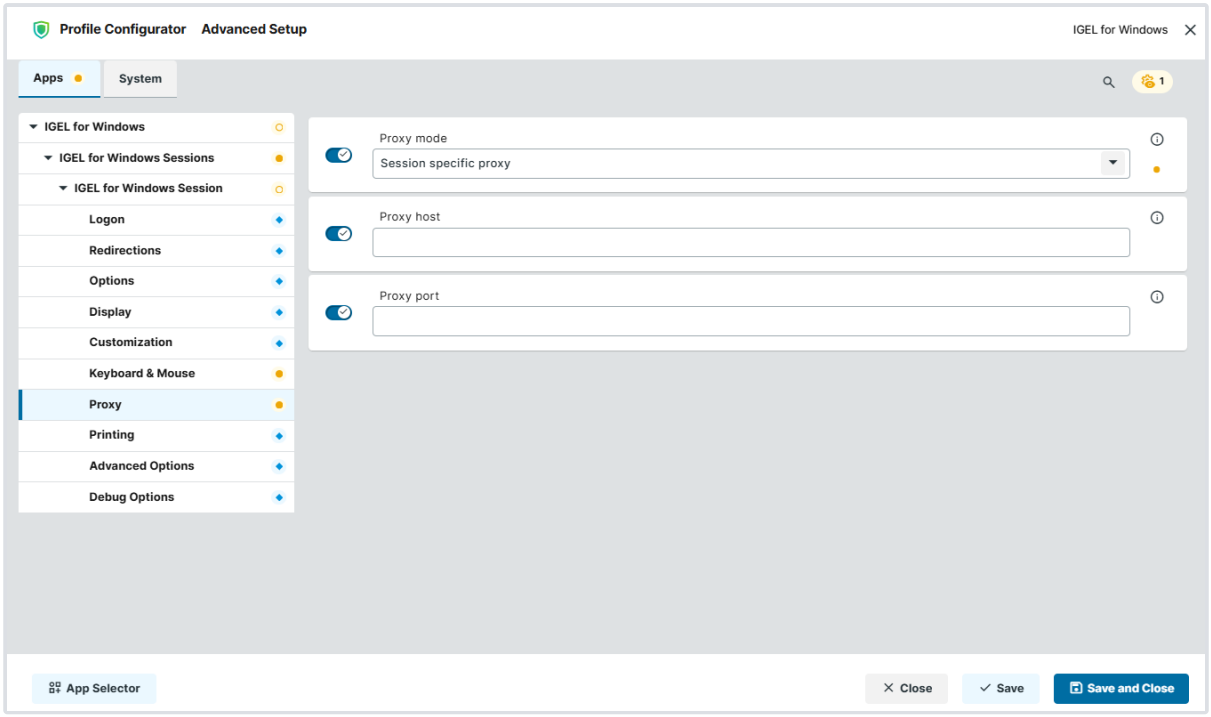
Possible values:

- **Never**: Relative mouse mode is disabled. (Default)
- **Auto**: The relative mouse mode is automatically activated when an application hides the mouse pointer. Note, however, there are applications in Windows that do not support relative mouse although they hide the mouse pointer. If you need to toggle relative mouse, press `Ctrl+Alt+M`.
- **Always**: Relative mouse mode is always active. If you need to toggle relative mouse, press `Ctrl+Alt+M`.

Configuring a Proxy

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Proxy**.

144. https://kb.igel.com/en/igel-os-base-system/current/hotkeys
145. https://virtualbrat.com/2026/03/31/igel-for-windows-app-introducing-relative-mouse-support/



2. Edit the settings according to your needs. The parameters are described below.

> **Proxy Configuration via a PAC File**
> If you want to use a PAC file, set **Proxy mode** to "Global proxy setting" and specify the **URL** of the PAC file under **Network > Proxy > System-wide proxy configuration > Automatic proxy configuration**.

Proxy mode

Specifies if a proxy should be used.

Possible options:

- **Off**: The use of a proxy is disabled. A direct connection to the Internet is used. (Default)
- **Global proxy setting**: The proxy configured under **Network > Proxy** is used.
- **Session specific proxy**: The proxy configuration specified under **Proxy host** and **Proxy port** is used.

The following fields are active if **Proxy mode** is set to **Session specific proxy**:

Proxy host

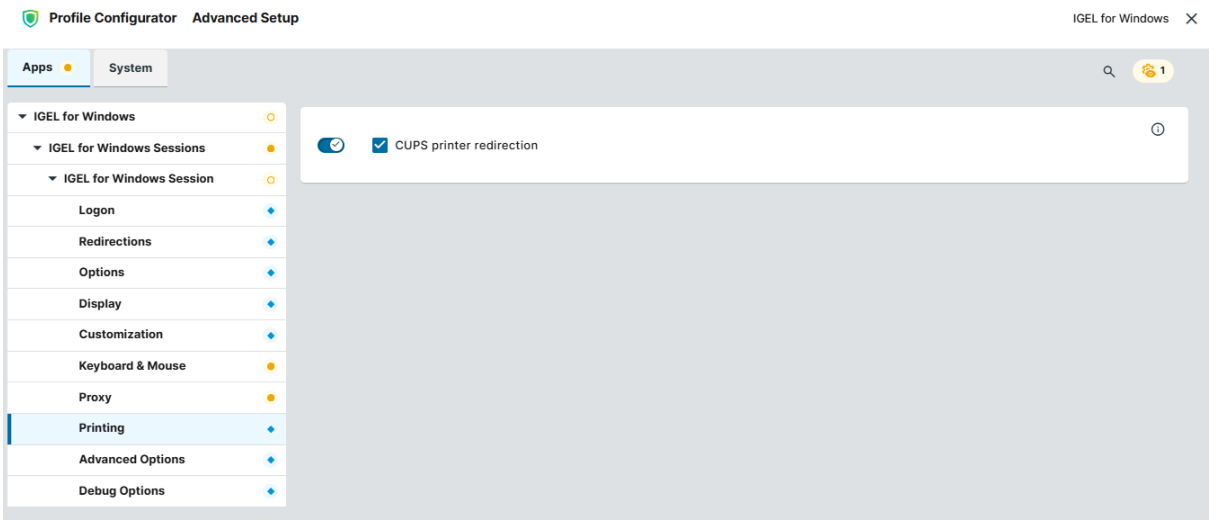
Hostname or IP address of the proxy server

Proxy port

Port on which the proxy service is available

Configuring Printing

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Printing**.



2. Edit the settings according to your needs. The parameters are described below.

CUPS printer redirection

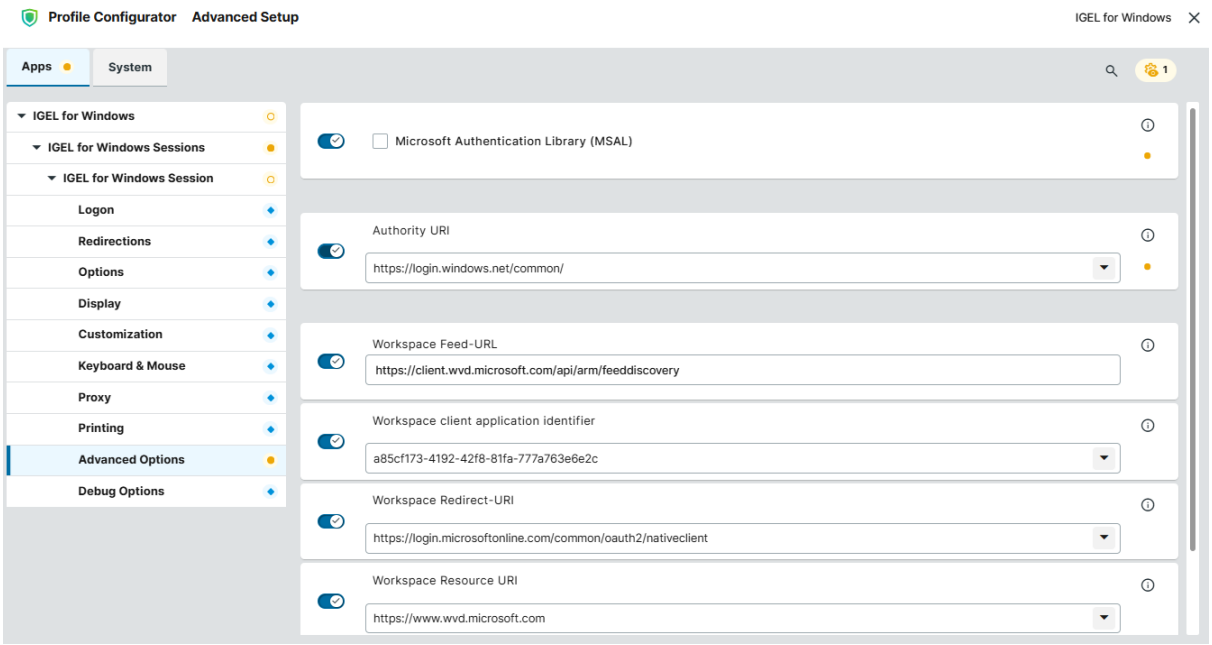
☑ CUPS printers are redirected to the remote session from the local endpoint. CUPS printers are configured under **CUPS Printing > Printer** and must be mapped into the session under **Use printer in RDP-based sessions**. (Default)

Set the printer driver name under **CUPS Printing > Printer > Driver to use in RDP-based sessions**:

- The default Windows driver name is "Microsoft PS Class Driver"; it is usually installed by default and works generically.
- In the case of a custom printer driver, make sure the driver is installed on the server side and enter the exact name of the driver.

Configuring Advanced Options

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Advanced Options**.



2. Edit the settings according to your needs. The parameters are described below.

Microsoft Authentication Library (MSAL)

☑ MSAL will be used for Microsoft Entra ID login. Currently, MSAL is used mainly for smartcard-based authentication, see e.g. How to Use Smart Card and Smart Key Authentication in IGEL OS 12[146].

⚠ If **Microsoft Authentication Library (MSAL)** is enabled, only predifined username is supported. Predefined passwords are not supported by MSAL.

☐ MSAL will not be used for Microsoft Entra ID login. (Default)

Authority URI

Authority URI (Uniform Resource Identifier) used for user login. It refers to the identity provider used for authentication. Usually, you need to modify it only if you have special Azure deployments like Azure GOV.

Possible values:

- **Auto:** If **Workspace Feed-URL** is customized, **Authority URI** will be discovered automatically.
- **https://login.windows.net/common/** (Default)
- **[custom value]**: Depends on your Azure environment.

Workspace Feed-URL

146. https://kb.igel.com/en/igel-os-base-system/current/how-to-use-smart-card-and-smart-key-authentication

Feed URL related to this workspace. This URL is used to sign in and access the assigned desktops and applications. Usually, you need to modify it only if you have special Azure deployments like Azure GOV. (Default: https://client.wvd.microsoft.com/api/arm/feeddiscovery)

Workspace client application identifier

Client application identifier related to this workspace

Possible values:

- **Auto**: If **Workspace Feed-URL** is customized, **workspace client application identifier** will be discovered automatically.
- **a85cf173-4192-42f8-81fa-777a763e6e2c** (Default)
- **[custom value]**: Depends on your Azure environment.

Workspace Redirect-URI

Redirection URI related to this workspace. This is the address where the Microsoft Entra authentication server sends the user after successful authentication.

Possible values:

- **Auto**: If **Workspace Feed-URL** is customized, **Workspace Redirect-URI** will be discovered automatically.
- **https://login.microsoftonline.com/common/oauth2/nativeclient** (Default)
- **[custom value]**: Depends on your Azure environment.

Workspace Resource URI

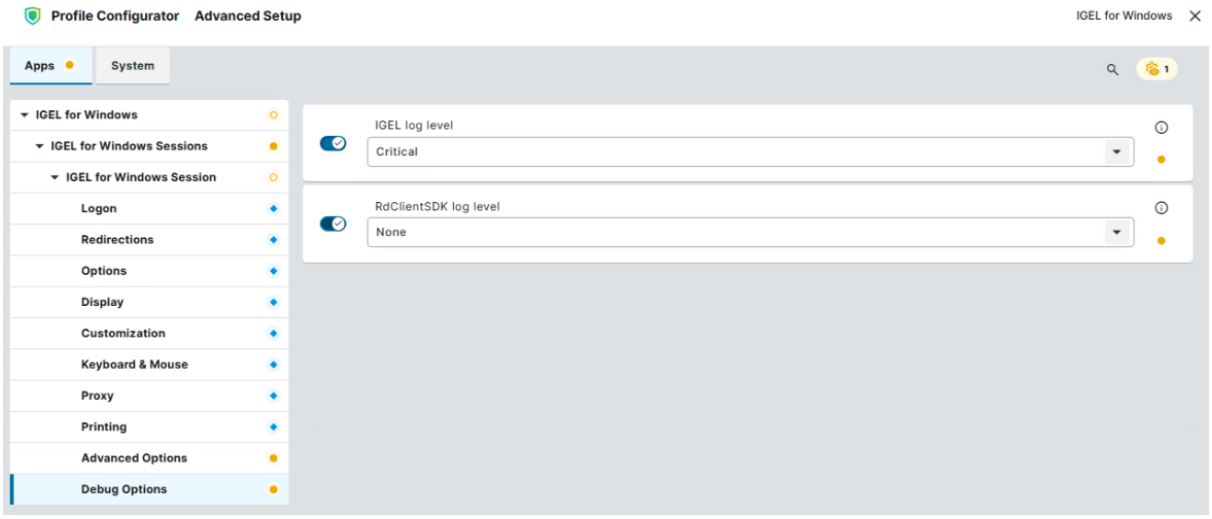
Resource URI related to this workspace.

Possible values:

- **Auto**: If **Workspace Feed-URL** is customized, **Workspace Resource URI** will be discovered automatically.
- **https://www.wvd.microsoft.com** (Default)
- **[custom value]**: Depends on your Azure environment.

Configuring Debug Options

1. In the profile configurator, go to **Apps > IGEL for Windows > IGEL for Windows Sessions > [session name] > Debug Options**.



2. Edit the settings according to your needs. The parameters are described below.

IGEL log level

Possible values:

- **Critical**: Logs severe system failures that require immediate attention. (Default)
- **Error**: Logs failures where something did not work as expected but the system may continue running.
- **Warning**: Logs potential issues or unusual situations that are not errors yet but could cause problems.
- **Info**: Logs general operational messages about normal system behavior.
- **Debug**: Logs detailed information useful for troubleshooting and development.
- **Trace**: Logs very fine-grained, step-by-step details of program execution for deep debugging.

RdClientSDK log level

Possible values:

- **None**: No logging is recorded, or only minimal essential events are captured. (Default)
- **Low**: Logs only basic, high-level information such as major events and errors.
- **Medium**: Includes more detailed operational data useful for general troubleshooting.
- **High**: Captures extensive, verbose details (including debug-level data) for in-depth diagnostics.

IGEL Digital Signage



- Configuring Digital Signage on IGEL OS (see page 349)

Configuring Digital Signage on IGEL OS

The IGEL Digital Signage App is a lean and secure digital signage solution that makes it possible to define the resolution and a URL for digital signage content.

For more information, see https://www.igel.com/secure-digital-signage-with-igel-os/ .

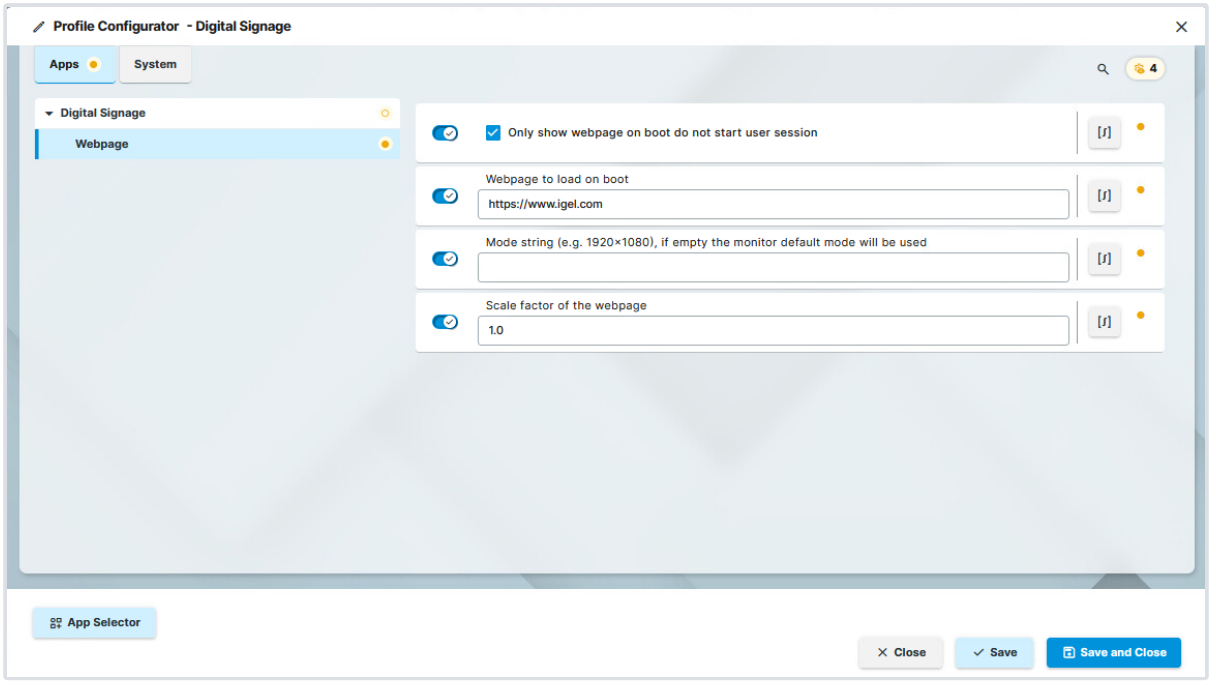
> When digital signage is installed and enabled on the device, the device runs in a kiosk-like digital signage mode. In this mode, all notification are closed immediately either by sending the default user action, or, if it is a notification with timeout, by sending the timeout action. For example, when the device is rebooted from the IGEL Universal Management Suite (UMS), the device reboots automatically, there is no confirmation needed.

Requirements

- **Hardware**: Digital signage has low hardware requirements, so you can use devices that fulfill the requirements outlined in Limited Device Support for Legacy Devices and Special Use Cases with IGEL OS 12. You can also use devices that fulfill the general hardware requirements.
- **Operating System**: IGEL OS 12 Base System running on the device.
- **Display setup**: The digital signage content can be displayed on a single monitor only.
- The device has access to the internet.
- The device is managed by IGEL Universal Management Suite (UMS).

Set up the IGEL Digital Signage App to Display a Webpage

1. Import the IGEL Digital Signage app to your IGEL UMS. For details on app import, see (12.06.110-en) How to Import IGEL OS Apps from the IGEL App Portal.
2. In the profile configurator, go to **Apps > Digital Signage > Webpage**.



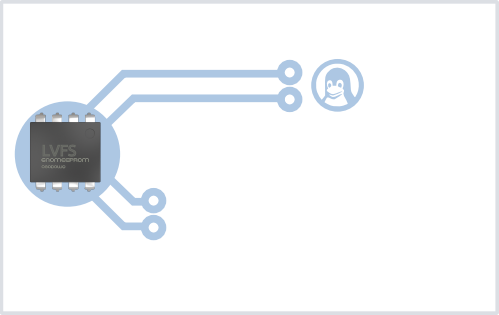
3. Configure the following before you assign the profile:
   Only show webpage on boot do not start user session
   ☑ The digital signage mode is enabled. The device boots directly into this mode, without showing the user session. (Default)

   Webpage to load on boot
   Provide the URL of the webpage you would like to display as digital signage. (Default: https://www.igel.com)

   Mode string (e.g.1920x1080), if empty, the monitor default mode will be used
   Provide the resolution of the digital signage display. If you leave this field empty, the monitor default mode will be used. (Default: empty)

   Scale factor of the webpage
   Set the scaling of the webpage. For example, 1.5 means the webpage will be zoomed to 150%. (Default: 1.0)
4. Save the configurations, and assign the app. For details on app assignment, see (12.06.110-en) How to Assign Apps to IGEL OS Devices via the UMS Web App .
   Once the app is assigned through the UMS, and the device is rebooted, it functions as a digital signage device.

LVFS BIOS Tools



The Linux Vendor Firmware Service (LVFS) BIOS Tools app offers BIOS tools to update the BIOS version. This app includes tools from the Linux Vendor Firmware Service - LF Projects LLC (https://lfprojects.org/policies/trademark-policy/). The Linux Vendor Firmware Service is a secure portal which allows hardware vendors to upload firmware updates.

This article serves as a guide for using the LVFS BIOS Tools app from configuration to debugging, including best practices.

BIOS Updates at Your Own Risk
IGEL is offering and supporting the LVFS BIOS Update mechanism - BIOS updates are performed at your own risk!

The LVFS BIOS update mechanism is functional even with Secure Boot enabled and when a BIOS password is set.

If the BIOS of your devices is distributed via the LVFS, you can update, downgrade, or reinstall it using the IGEL Universal Management Suite (UMS). As the procedures for reinstalling and downgrading the BIOS are analogous to the update procedure, we will use the term "update" in the following instructions.

Tip: Direct Download of Firmware from fwupd Repository
To download valid firmware updates on a given test device, run the following command on the test device:

```
fwupdmgr refresh --force
fwupdmgr get-updates --json > /tmp/updates.json
```

The `updates.json` file includes links to the `.CAB` files from `fwupd`. Use `wget` to download them.

Requirements

- UMS 12.01 or higher
- Device must support LVFS
- IGEL OS Base System 12.7.0 or higher must be installed on supported devices

⚠ The IGEL OS Base System needs to be installed directly on the device. The LVFS BIOS Tools app is unsupported if the IGEL OS boots from a UD Pocket.

Step 1: Configuring the App in the UMS Web App

Importing the App

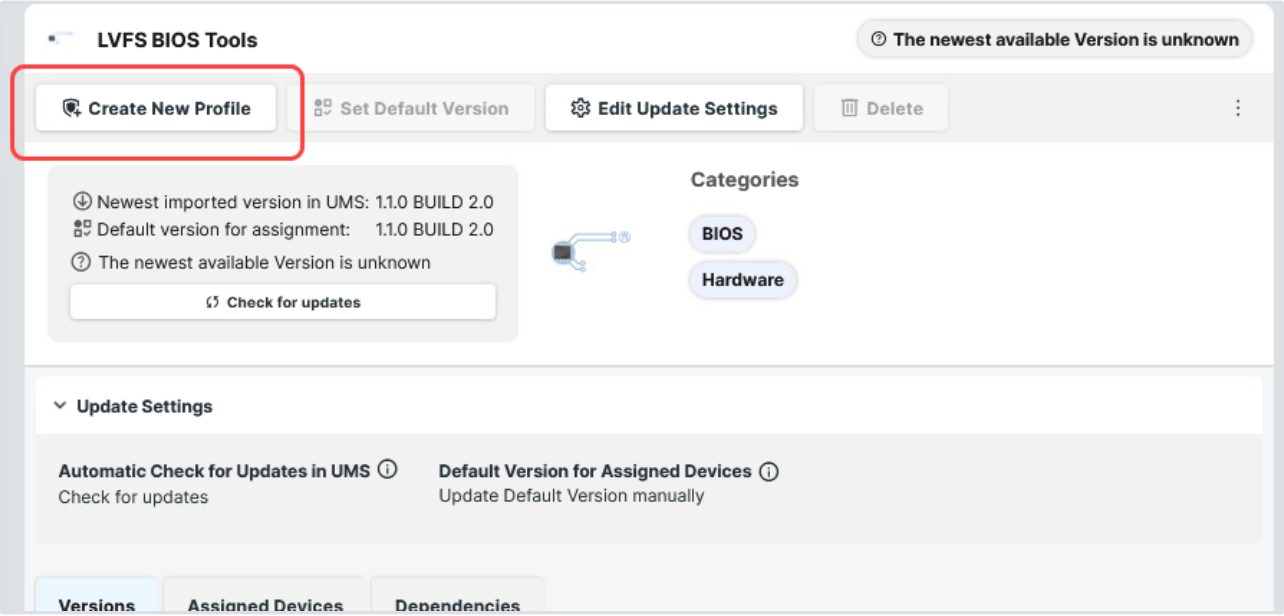
Import the LVFS BIOS Tools app into your UMS. For more information on how to do this, see (12.06.120-en) How to Import IGEL OS Apps from the IGEL App Portal or (12.06.120-en) How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access .

Creating a Profile

To distribute the app to the devices, create a profile:

1. In the UMS Web App, go to **Apps** and search for “BIOS” to find the **LVFS BIOS Tools** app.

2. Click **Create New Profile**.

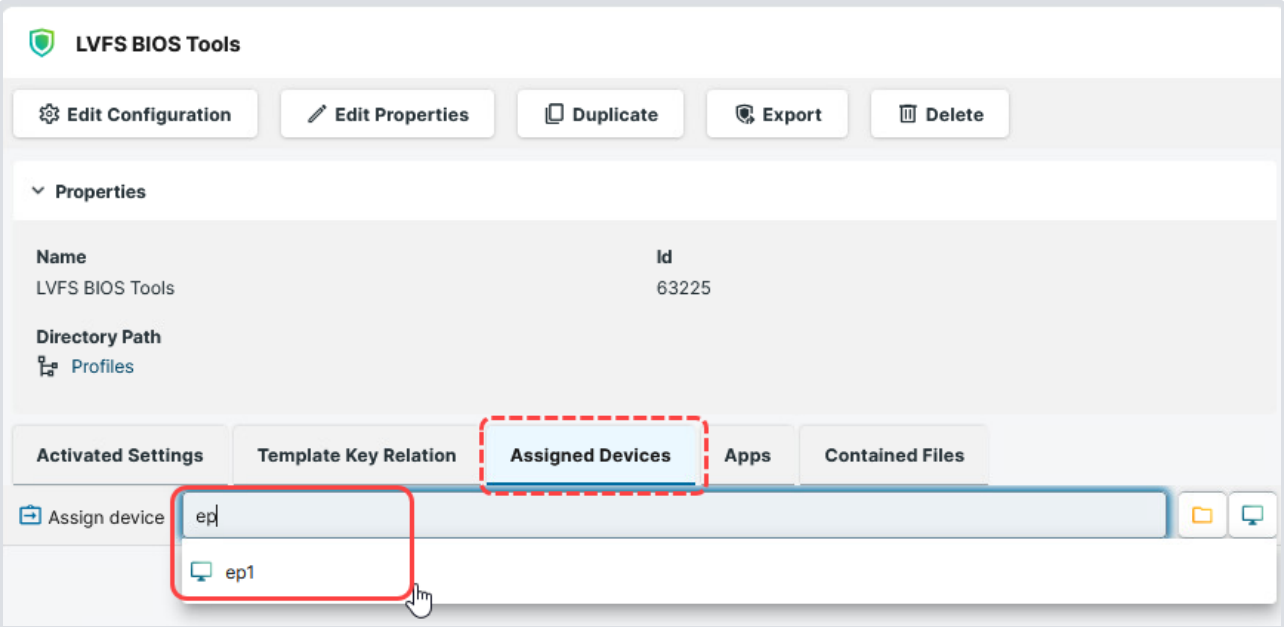


3. Define a name for your profile and save.

For more on profile creation, see (12.06.120-en) How to Create and Assign Profiles in the IGEL UMS Web App .

Assigning the Profile to Your Devices

1. In the field **Assign device**, enter the name of the device or device directory for which you want to use the LVFS BIOS Tools app.



2. Select **Assign and apply changes now.**

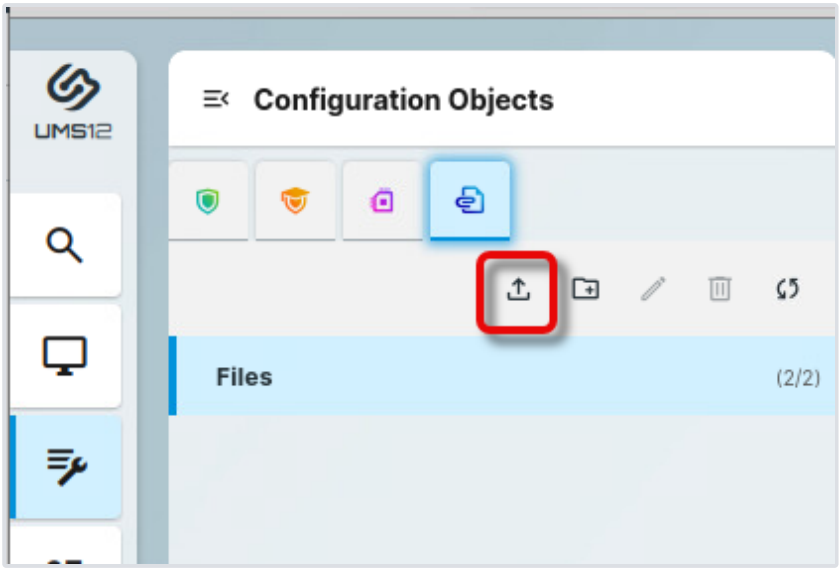
Step 2: Setting up the File Source

Look up the latest update file from https://fwupd.org/lvfs/devices/ and download it. If you want to use the UMS for file distribution, store it in a location that is reachable from the machine on which your UMS Server is running.

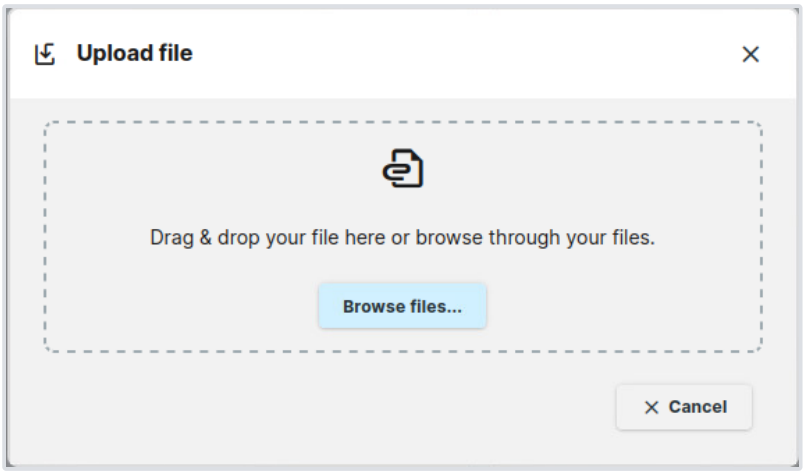
Using UMS File Transfer

The following example shows how to use the UMS file transfer facility for file deployment.

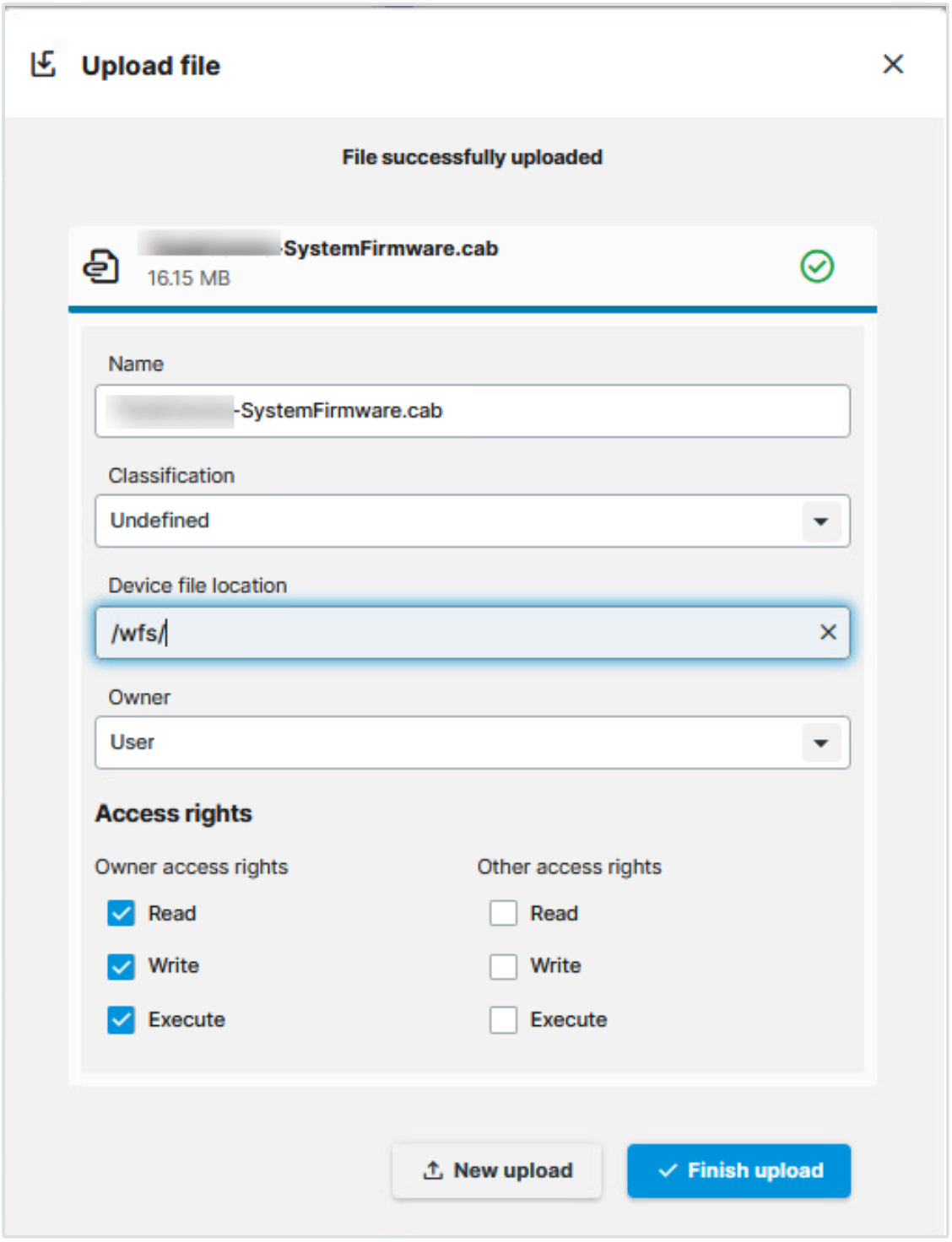
1. In the UMS Web App, go to **Configuration Objects**, select the icon for files, and then the icon for uploads.



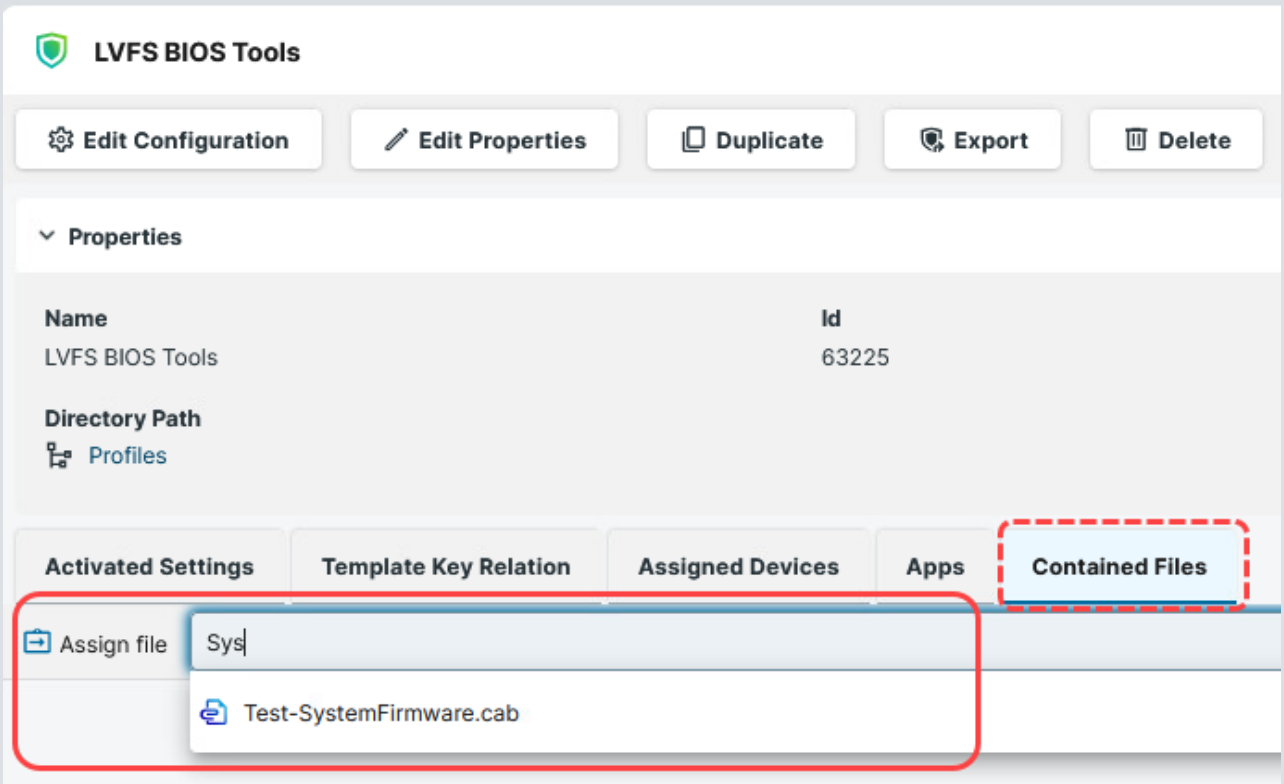
2. Choose the BIOS update file on your system via drag & drop or via **Browse files...**.



3. In the field **Device file location**, define the local path in which the file will be stored on the device, e.g. `/wfs/`. Afterward, click **Finish upload**.



4. Assign the file to your devices by assigning it to the profile we have created beforehand.



Step 3: Updating the BIOS

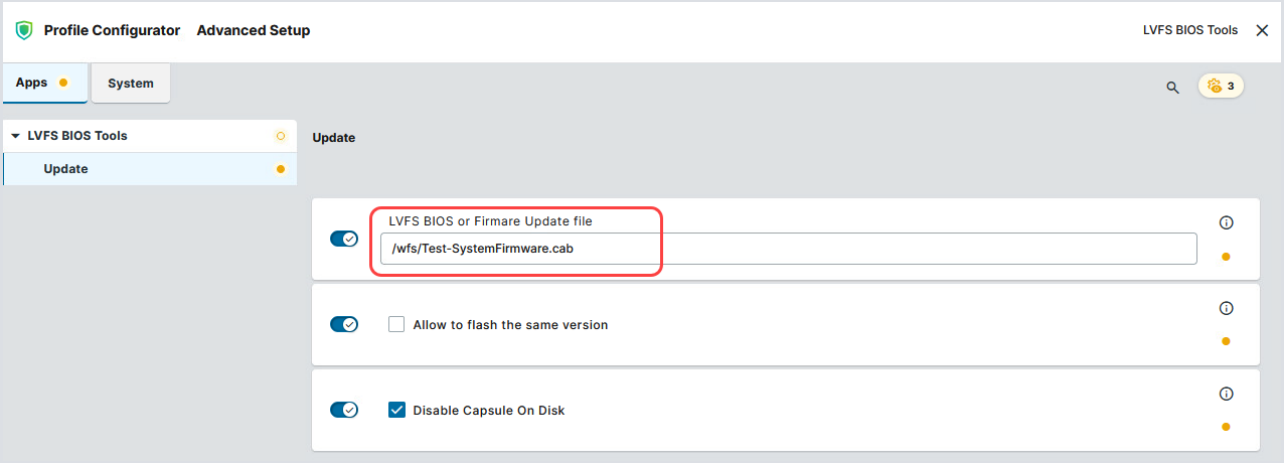
Configuring the Devices for the BIOS Update

Once the file is made available for the endpoint devices:

1. Open the previously configured LVFS BIOS Tools profile.

2. Go to **Apps > LVFS BIOS Tools > Update.**

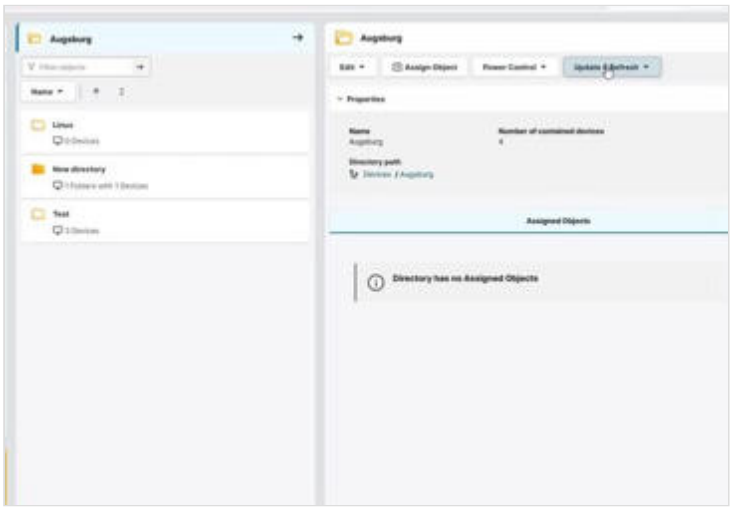
3. Under **LVFS BIOS or Firmware Update file** provide the local path of the BIOS update file with file extension. In our example: `/wfs/Test-SystemFirmware.cab`



⚠ You can reinstall the same BIOS/Firmware version that had already been installed on the device if you enable **Allow to flash the same version**.

Triggering the BIOS Update

1. In the UMS, select the relevant devices (or directory). In the actions menu, click **Update & Refresh > Specific Device Command.**



2. Select **BIOS - Trigger update** and click **Execute**.

The target devices receive a reboot command; a corresponding message is displayed.

The timespan before the BIOS logo and the progress bar is shown might be significantly longer than usual. Please ensure that the device remains powered on until the update process is finished.

If you trigger the command again via the UMS Web App, the lines are shown in red, showing that an update is already pending (as an error message).

Step 4: Checking Update Success

If you want to check whether the command reached the IGEL device, you can open a terminal or Secure Terminal and run: `journalctl -f` . You can check the BIOS version on the device with the command `dmidecode -t bios` as root.

Debugging

For most cases, the normal logging to journalctl should be good enough to identify any problems. The default loglevel is “INFO”.

→ To enable loglevel “DEBUG”, enable the registry key `app.lvfs_bios_tools.config.enable_debug`

Using the Command Line Interface (CLI)

For testing the BIOS update on a single device, you can use the command line tool as an alternative to a scheduled job from the UMS.

As a prerequisite, the steps described under Setting up the File Source and the relevant settings in the profile must be completed.

When the command has been executed, a dialog informs you that a reboot is required. You can choose between two options:

- Perform the reboot and update right away
- Postpone the update to the next reboot

Usage

```
lvfs-bios-tools [OPTIONS] COMMAND [ARGS]...
```

Options

Option / Contrary Option	Comment
`--debug / --no-debug`	Provide extensive information (verbose mode)
`--help`	Show the help text and exit

Commands

Command	Argument (Short / Long Form)	Comment
`update`		Handle BIOS update
	`-e --enable`	Trigger BIOS update. Will be triggered after reboot.
	`-d --disable`	Disable BIOS update
	`--help`	Show the help text and exit

Example

The following command performs a BIOS update and displays extensive information:

```
update --debug -e
```

IGEL Remote Desktop

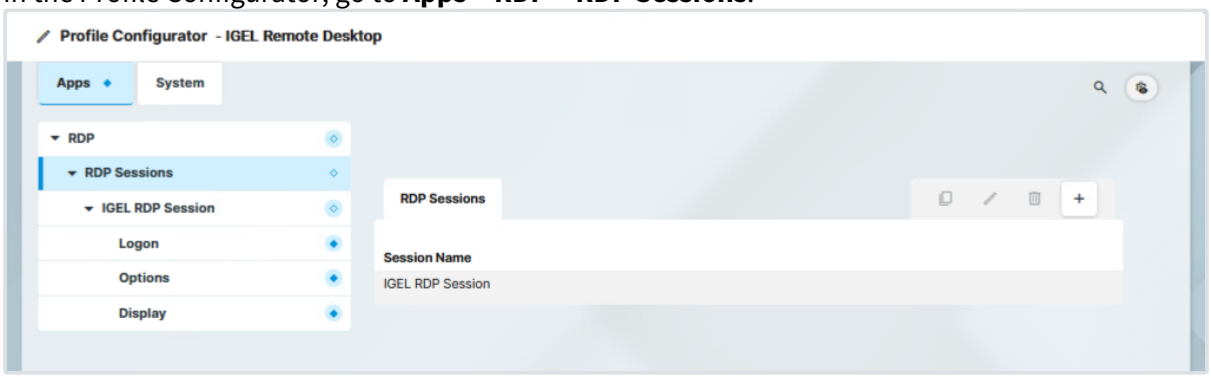


- Getting Started with IGEL Remote Desktop on IGEL OS (see page 361)
- Configuration of IGEL Remote Desktop on IGEL OS (see page 363)

Getting Started with IGEL Remote Desktop on IGEL OS

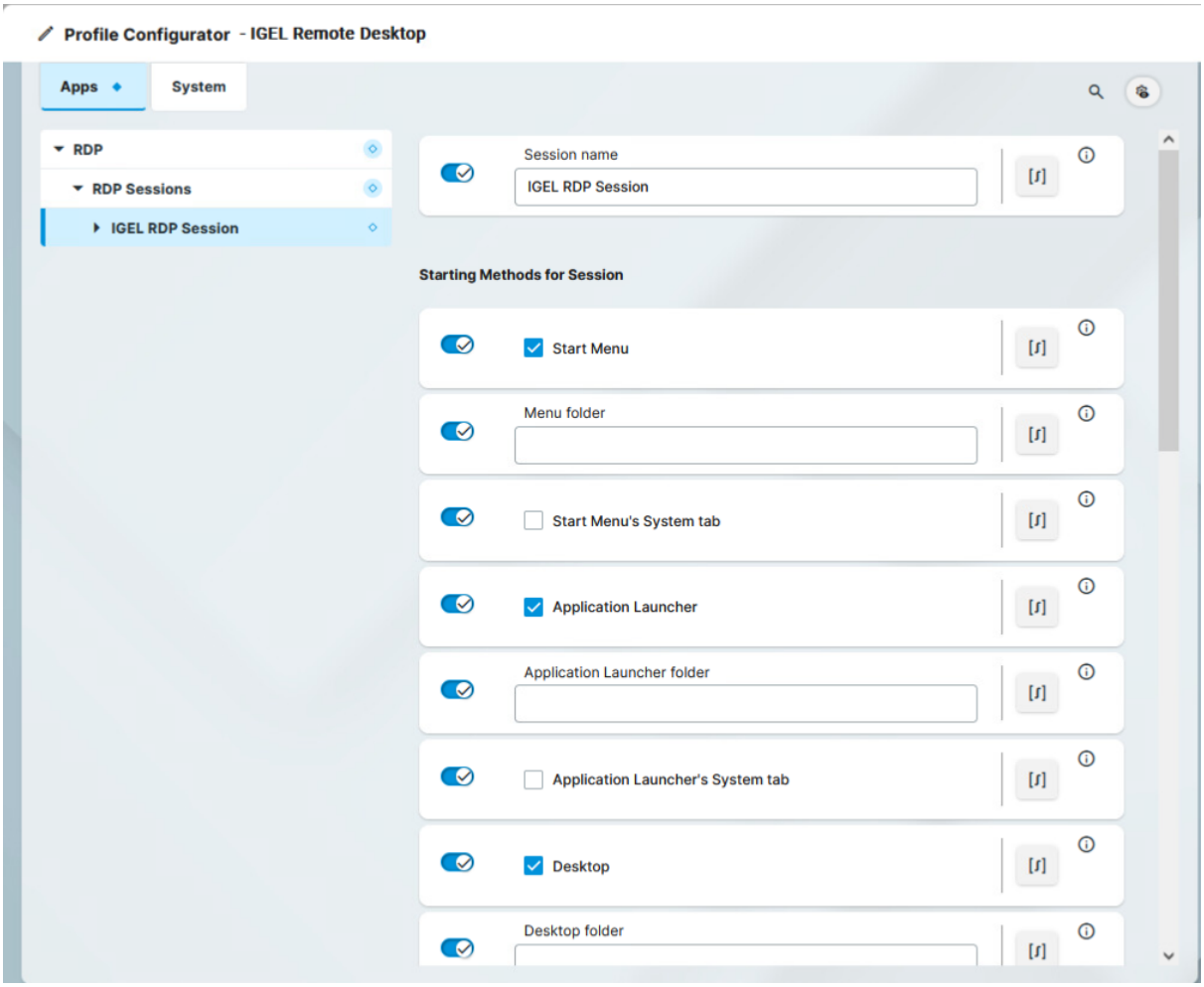
How to Create a Session

1. In the Profile Configurator, go to **Apps > RDP > RDP Sessions**.



2. Click + .
3. Define the starting methods for the session. The starting method parameters are described under Starting Methods for Apps[147].

147. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

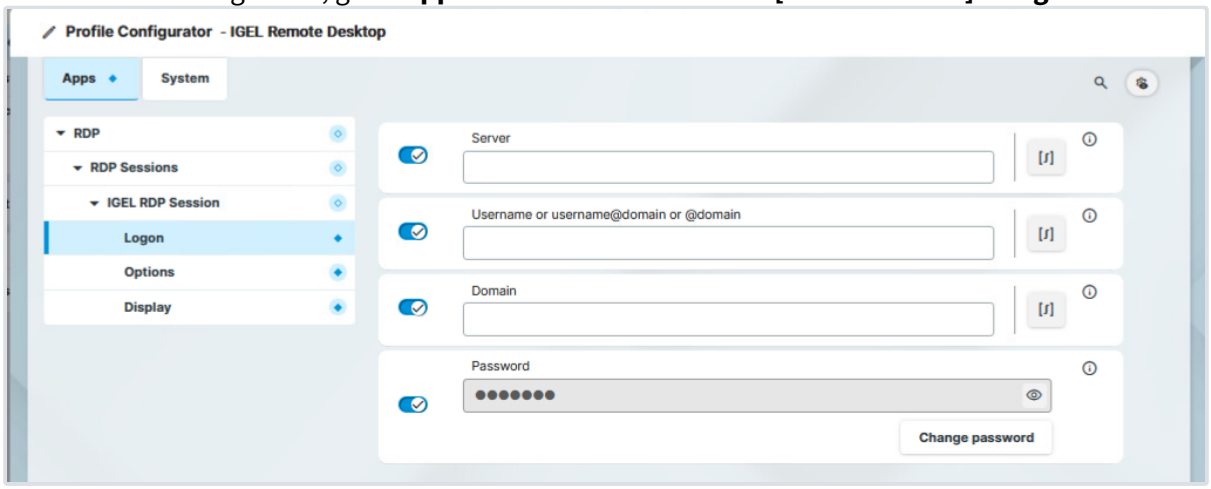


4. Save the settings.
   The session is created.
5. Configure the session according to your needs; for details, see Configuration of IGEL Remote Desktop on IGEL OS (see page 363)

Configuration of IGEL Remote Desktop on IGEL OS

Configuring the Logon

1. In the Profile Configurator, go to **Apps > RDP > RDP Sessions > [Session Name] > Logon**.



2. Edit the settings according to your needs. The parameters are described in the following.

Server

Name or IP address of the server

Username or username@domain or @domain

A username or a preset domain name used for automatic connection to the RDP session. The string after "@" is taken as a preset domain name.

Example:

user@your.domain.com[148]: To log in, the user does not need to enter the username and the domain name.

@your.domain.com[149]: To log in, the user only needs to enter the username. The preset domain – your.domain.com[150] – will automatically be appended.

Overwriting the Preset Domain Name

Use the following registry key to specify whether the user should be able to overwrite the preset domain, e.g. with username@other-domain.com[151]:

148. mailto:user@your.domain.com
149. http://your.domain.com
150. http://your.domain.com

Path	**System > Registry**
Registry	`sessions.rdp%.options.allow-preset-domain-overwrite`
Value	enabled / disabled (Default)
Note	If enabled: the domain entered by the user is accepted. If disabled: the domain entered by the user is replaced with the preset domain.

Domain

Windows domain

Password

The password used for the automatic connection to the RDP session.

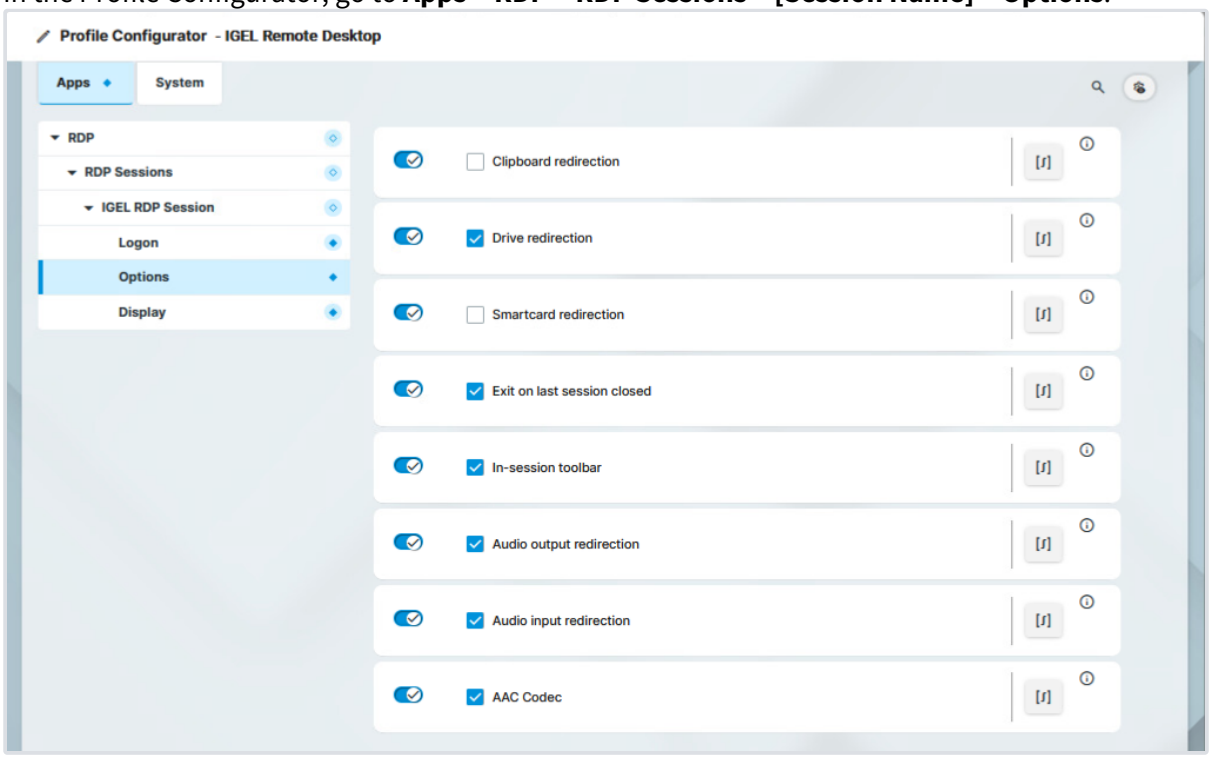
> **If the Login Credentials Should Not Be Applied Automatically**
>
> You can use the following registry key to always prompt for a user name and password or only for a password when connecting to an RDP session:

Path	**System > Registry**
Parameter	**Always prompt for username and password upon session host connection**
Registry	`sessions.rdp%.options.always-prompt-for-session-username-and-password`
Value	enabled / disabled (Default)
Path	**System > Registry**
Parameter	**Always prompt for password upon session host connection**
Registry	`sessions.rdp%.options.always-prompt-for-session-password`
Value	enabled / disabled (Default)
Note	On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result.

151. mailto:username@other-domain.com

Configuring the Options

1. In the Profile Configurator, go to **Apps > RDP > RDP Sessions > [Session Name] > Options**.



2. Edit the settings according to your needs. The parameters are described in the following.

Clipboard redirection

- ☑ Text and images from the clipboard are shared between the RDP session and the local client.
- ☐ Text and images from the clipboard are not shared between the RDP session and the local client. (Default)

Drive redirection

- ☑ Redirection is bound to the `/media` folder, so that locally mounted storage devices, including USB sticks, are forwarded to the RDP session. (Default)

Smartcard redirection

- ☑ Smartcards are forwarded to the RDP session.
- ☐ Smartcards are not forwarded to the RDP session. (Default)

Exit on last session closed

When the last session window is closed, the entire IGEL RDP Client automatically closes. (Default)

In-session toolbar

The in-session toolbar is enabled. (Default)

Audio output redirection

The audio output is redirected between the RDP session and the local client. (Default)

Audio input redirection

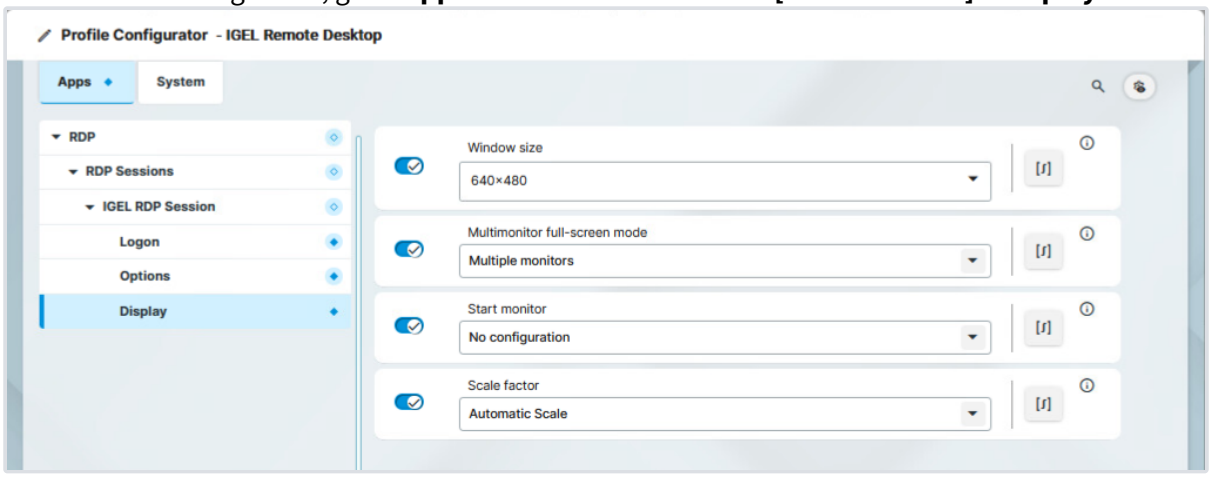
The audio input (microphone) is redirected between the local client and the RDP session. (Default)

AAC Codec

The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

Configuring the Display

1. In the Profile Configurator, go to **Apps > RDP > RDP Sessions > [Session Name] > Display**.



2. Edit the settings according to your needs. The parameters are described in the following.

Window size

Specifies the width and height of the window.
Possible options:

- **Full-screen**: The session is shown on the full screen. The device's taskbar is not visible. (Default)

- **Work area**: The session is shown on the full screen, minus the area needed by the device's taskbar.
- **Numeric details**: The session is shown in the selected resolution or on the selected percentage of the screen area.

Multimonitor full-screen mode

This setting is relevant if more than one monitor is connected to the terminal.
Possible options:

- **Single monitor**: Restricts the full-screen session to one monitor.
- **Multiple monitors**: Displays the full-screen session on multiple monitors. (Default)
- **Expand to all monitors**: Expands the full-screen session across all monitors.

Start monitor

Specifies the monitor on which the session is displayed.
Possible options:

- **No configuration**: The monitor is selected according to the current position of the mouse pointer. (Default)
- **1st-8th monitor**

Scale factor

Specifies the desktop scaling in percent.
Possible values:

- **Automatic scale**: The resolution set under **User Interface > Display Settings > DPI Options > Monitor-DPI** is used for the session. For details, see *IGEL OS Base System > IGEL OS Base System > Configuration of IGEL OS 12 Device Settings > User Interface > Display Settings > DPI Options*
- **Numeric details**: The display is magnified by the factor given here.

IGEL Windows 365



IGEL Windows 365 app is replaced by IGEL for Windows app. For details, see IGEL for Windows[152].
IGEL Windows 365 app will not receive any updates in the future; its last version is 1.3.7 BUILD 1.0.
Therefore, if you are using IGEL Windows 365 app, it is necessary to create new profiles based on IGEL for Windows app and assign them to the devices.

- Getting Started with IGEL Windows 365 on IGEL OS (see page 369)
- Configuration of IGEL Windows 365 on IGEL OS (see page 371)
- Troubleshooting: User Gets Prompt "Need admin approval" on IGEL Windows 365 Startup (see page 378)

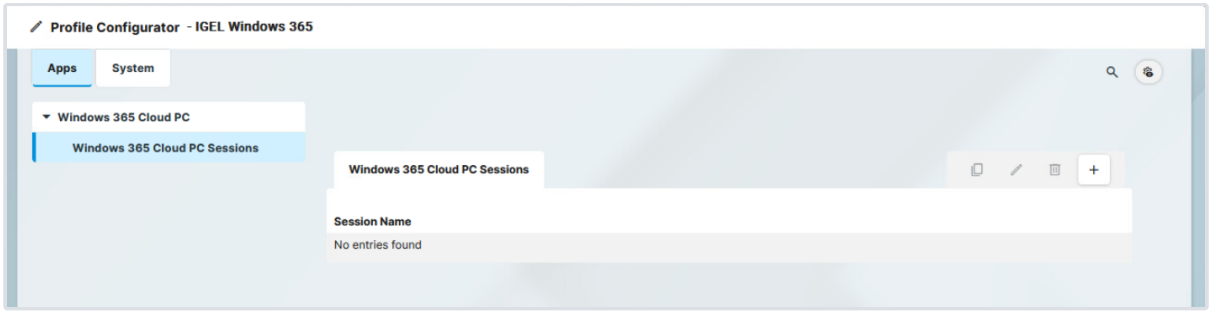
152. https://kb.igel.com/en/igel-apps/current/igel-azure-virtual-desktop

Getting Started with IGEL Windows 365 on IGEL OS

IGEL Windows 365 app is replaced by IGEL for Windows app. For details, see IGEL for Windows[153].
IGEL Windows 365 app will not receive any updates in the future; its last version is 1.3.7 BUILD 1.0.
Therefore, if you are using IGEL Windows 365 app, it is necessary to create new profiles based on IGEL for Windows app and assign them to the devices.

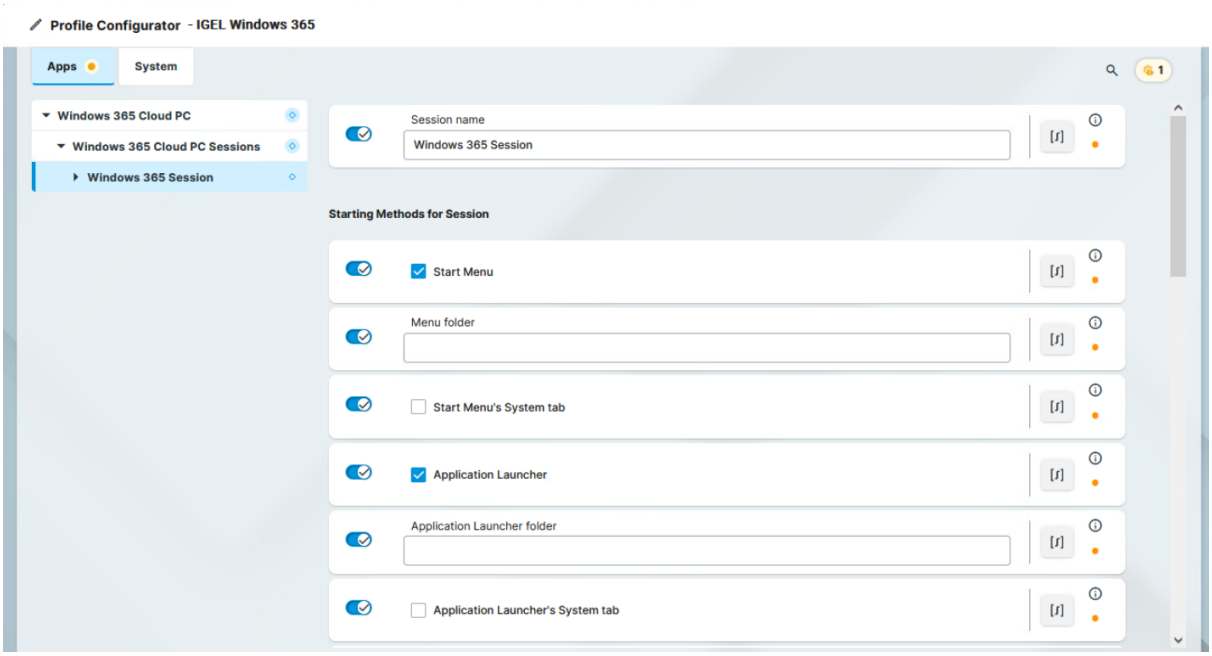
How to Create a Session

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions**.



2. Click + .
3. Define the starting methods for the session. The starting methods parameters are described under *IGEL OS Base System > IGEL OS Base System > Starting Methods for Apps*

153. https://kb.igel.com/en/igel-apps/current/igel-azure-virtual-desktop



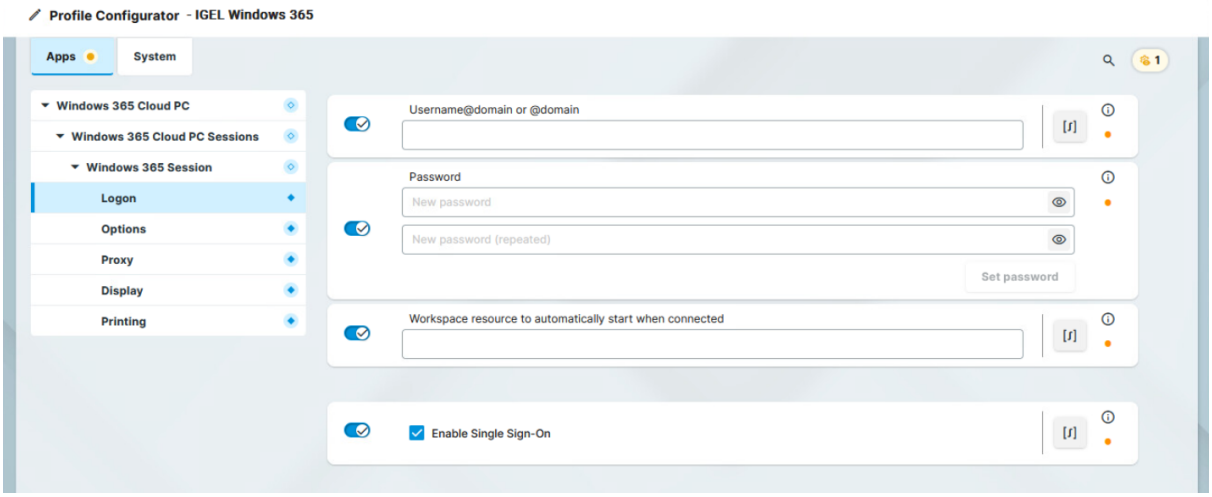
4. Save the settings.
   The session is created.
5. Configure the session according to your needs; for details, see Configuration of IGEL Windows 365 on IGEL OS (see page 371)

Configuration of IGEL Windows 365 on IGEL OS

> IGEL Windows 365 app is replaced by IGEL for Windows app. For details, see IGEL for Windows[154].
> IGEL Windows 365 app will not receive any updates in the future; its last version is 1.3.7 BUILD 1.0.
> Therefore, if you are using IGEL Windows 365 app, it is necessary to create new profiles based on IGEL for Windows app and assign them to the devices.

Configuring Logon

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions > [Session Name] > Logon**.



2. Edit the settings according to your needs. The parameters are described in the following.

Username@domain or @domain

A user name or a preset domain name used for the automatic connection to the Windows 365 session. The string after "@" is taken as a preset domain name.

Example:

windows@your.domain.com[155]: To log in, the user does not need to enter the username and the domain name.

@your.domain.com[156]: To log in, the user only needs to enter the username. The preset domain – your.domain.com[157] – will automatically be appended.

154. https://kb.igel.com/en/igel-apps/current/igel-azure-virtual-desktop
155. mailto:windows@your.domain.com
156. http://your.domain.com
157. http://your.domain.com

Overwriting the Preset Domain Name

Use the following registry key to specify whether the user should be able to overwrite the preset domain, e.g. with username@other-domain.com[158]:

Path	**System > Registry**
Registry	`sessions.cpc%.options.allow-preset-domain-overwrite`
Value	enabled / disabled (Default)
Note	If enabled: the domain entered by the user is accepted. If disabled: the domain entered by the user is replaced with the preset domain.

Password

The password used for the automatic connection to the Windows 365 session.

If the Login Credentials Should Not Be Applied Automatically for the Session Host Authentication

You can use the following registry key to always prompt for a user name and password or only for a password when connecting to an Windows 365 session:

Path	**System > Registry**
Parameter	**Always prompt for username and password upon session host connection**
Registry	`sessions.cpc%.options.always-prompt-for-session-username-and-password`
Value	enabled / disabled (Default)
Path	**System > Registry**
Parameter	**Always prompt for password upon session host connection**
Registry	`sessions.cpc%.options.always-prompt-for-session-password`
Value	enabled / disabled (Default)
Note	On the server side, you can enable the RDP group policy "Always prompt for password upon connection" to achieve the same result.

158. mailto:username@other-domain.com

Workspace resource automatically start when connected

Name of the resource that is to be started automatically when the Windows 365 session is launched. The name specified here must exactly match the name of the Windows 365 resource that has been assigned to the user.

> Only one resource can be started automatically; the automatic start of multiple resources is not supported.

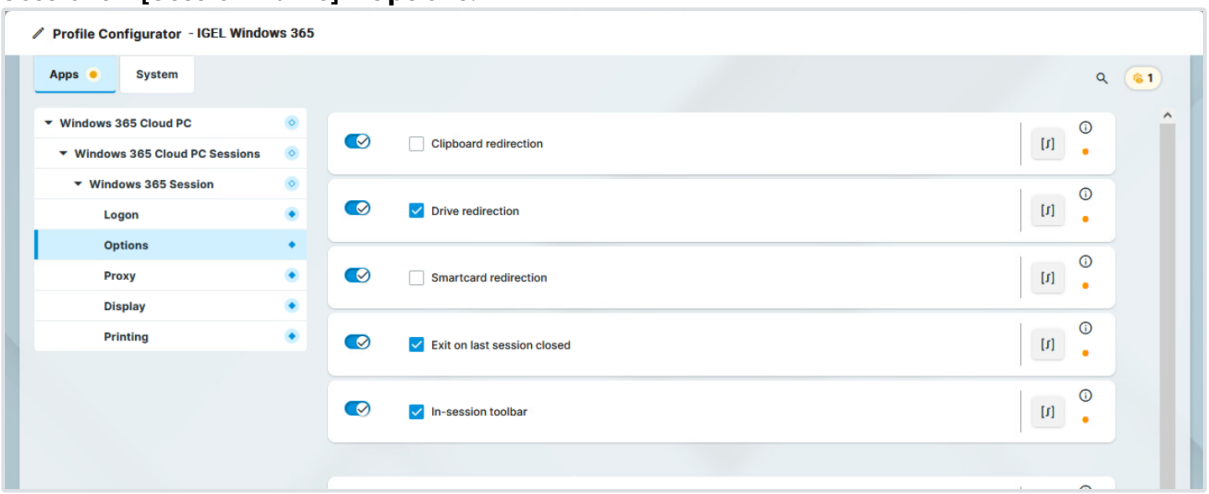
Enable Single Sign-On

- [x] Single sign-on (SSO) is activated. (Default)

After the Azure Active Directory authentication the user needs to authenticate to the session host as well, which is done automatically from what was used for the Azure Active Directory authentication.

Configuring the Options

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions > [Session Name] > Options**.



2. Edit the settings according to your needs. The parameters are described in the following.

Clipboard redirection

- [x] Text and images from the clipboard are shared between the Windows 365 session and the local client.
- [ ] Text and images from the clipboard are not shared between the Windows 365 session and the local client. (Default)

Drive redirection

- [x] Redirection is bound to the `/media` folder, so that locally mounted storage devices, including USB sticks, are forwarded to the Windows 365 session. (Default)

Smartcard redirection

- [x] Smartcards are forwarded to the Windows 365 session.
- [ ] Smartcards are not forwarded to the Windows 365 session. (Default)

Exit on last session closed

- [x] When the last session window is closed, the entire IGEL Windows 365 client automatically closes. (Default)

In-session toolbar

- [x] The in-session toolbar is enabled. (Default)

Audio output redirection

- [x] The audio output is redirected between the Windows 365 session and the local client. (Default)

Audio input redirection

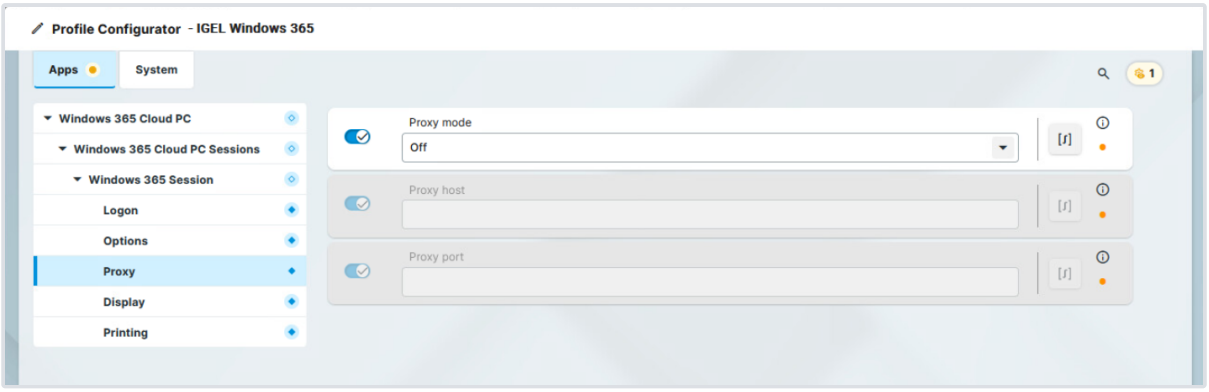
- [x] The audio input (microphone) is redirected between the local client and the Windows 365 session. (Default)

AAC Codec

- [x] The AAC (Advanced Audio Coding) codec used for support of audio output redirection is enabled. (Default)

Configuring the Proxy

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions > [Session Name] > Proxy**.



2. Edit the settings according to your needs. The parameters are described in the following.

Proxy mode

Specifies if a proxy should be used.
Possible options:

- **Off**: A proxy is disabled. The direct connection to the Internet is used. (Default)
- **Global proxy setting**: The proxy configured under **Network > Proxy** is used, see *IGEL OS Base System > IGEL OS Base System > Configuration of IGEL OS 12 Device Settings > Network Configuration in IGEL OS12 > Proxy Configuration in IGEL OS12*
- **Session specific proxy**: The proxy configuration specified under **Proxy host** and **Proxy port** is used.

Proxy host

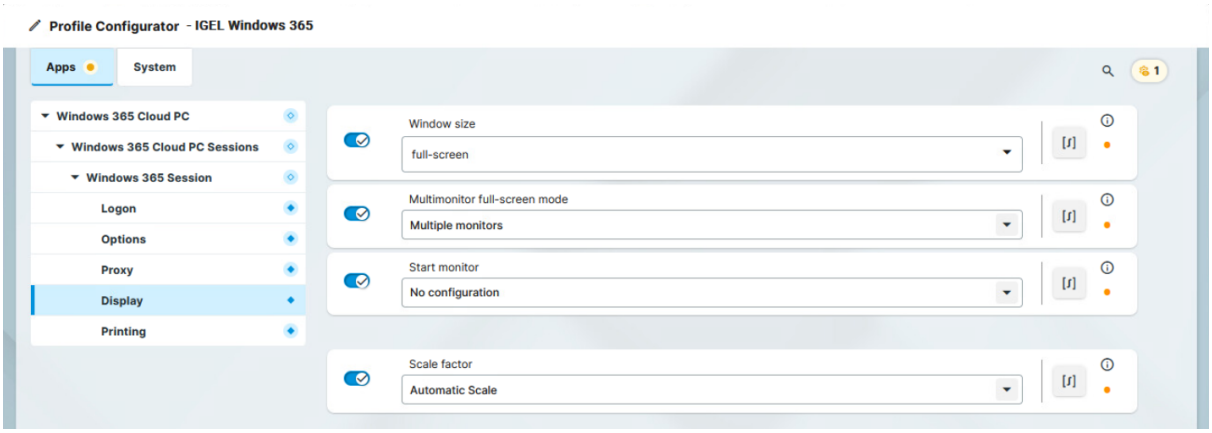
The hostname or IP address of the proxy server. Configurable if **Session specific proxy** is selected.

Proxy port

Port on which the proxy service is available. Configurable if **Session specific proxy** is selected.

Configuring the Display

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions > [Session Name] > Display**.



2. Edit the settings according to your needs. The parameters are described in the following.

Window size

Specifies the width and height of the window.
Possible options:

- **Full-screen**: The session is shown on the full screen. The device's taskbar is not visible. (Default)
- **Work area**: The session is shown on the full screen, minus the area needed by the device's taskbar.
- **Numeric details**: The session is shown in the selected resolution or on the selected percentage of the screen area.

Multimonitor full-screen mode

This setting is relevant if more than one monitor is connected to the terminal.
Possible options:

- **Single monitor**: Restricts the full-screen session to one monitor.
- **Multiple monitors**: Displays the full-screen session on multiple monitors. (Default)
- **Expand to all monitors**: Expands the full-screen session across all monitors.

Start monitor

Specifies the monitor on which the session is displayed.
Possible options:

- **No configuration**: The monitor is selected according to the current position of the mouse pointer. (Default)
- **1st-8th monitor**

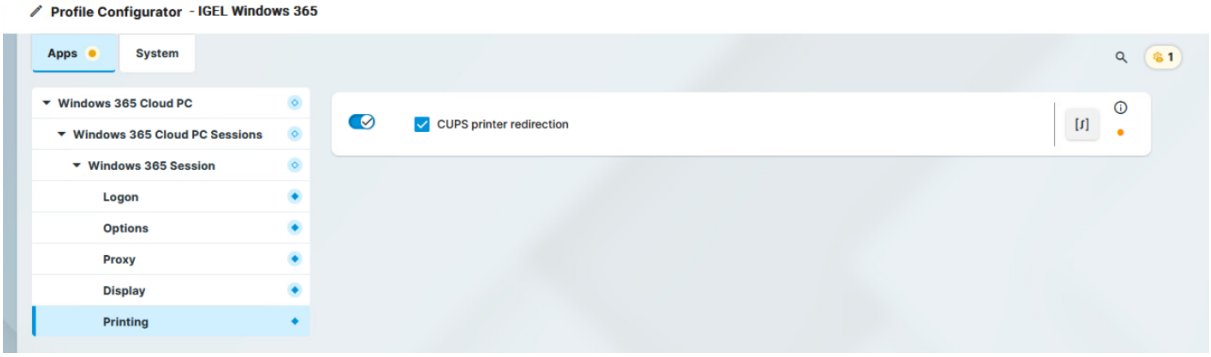
Scale factor

Specifies the desktop scaling in percent.
Possible values:

- **Automatic scale**: The resolution set under **User Interface > Display Settings > DPI Options > Monitor-DPI** is used for the session. For details, see *IGEL OS Base System > IGEL OS Base System > Configuration of IGEL OS 12 Device Settings > User Interface > Display Settings > DPI Options*
- **Numeric details**: The display is magnified by the factor given here.

Configuring Printing

1. In the Profile Configurator, go to **Apps > Windows 365 Cloud PC > Windows 365 Cloud PC Sessions > [Session Name] > Printing**.



2. Edit the settings according to your needs. The parameters are described in the following.

CUPS printer redirection

☑ CUPS printers are redirected to the Windows 365 session. (Default)

Troubleshooting: User Gets Prompt "Need admin approval" on IGEL Windows 365 Startup

Problem

The user enters the credentials to start a session with the IGEL Windows 365 app, but the session does not start. Instead, a prompt informs the user about missing permission to access resources in the organization.

This behavior is the same for all users in your organization because the underlying problem is tenant-wide.

Background

Your IGEL Windows 365 client app needs access to your organization's resources via the Microsoft Graph API. This enables the app to gather user information, like user pictures, and to control the virtual machine that hosts the session. For this purpose, admin consent must be granted in Microsoft Entra first. This involves providing the client ID, or app ID, of the IGEL Windows 365 app.

Solution

You must ensure that tenant-wide admin consent to the IGEL Windows 365 app is granted. Microsoft describes several methods; see Grant tenant-wide admin consent to an application[159].

For the IGEL Windows 365 app, the following two methods have been verified:

- If you are not a Microsoft Entra administrator, send an app ID consent request directly from the IGEL Windows 365 app to your Entra administrators (assuming your Entra is configured to allow this). The Entra administrators then need to review and consent to the app in Entra.
- If you are a Microsoft Entra admin with permission to consent apps, you can use this URL pattern: https://login.microsoftonline.com/{organization}/adminconsent?client_id=bcecda93-b0e7-48ce-ae4d-3263836332be
  Replace `{organization}` with your Microsoft Entra ID; note that `bcecda93-b0e7-48ce-ae4d-3263836332be` is the app ID of the IGEL Windows 365 app. For further details, see Construct the URL for granting tenant-wide admin consent[160].
  After a few minutes, the syncing should be done, and the app ID should be displayed.
  

159. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal#construct-the-url-for-granting-tenant-wide-admin-consent
160. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal#construct-the-url-for-granting-tenant-wide-admin-consent

Lenovo BIOS Tools



The Lenovo BIOS Tools app offers BIOS tools to update the BIOS version, BIOS settings, and BIOS password on supported Lenovo devices. This app includes tools from Lenovo Inc., and the Linux Vendor Firmware Service - LF Projects LLC (https://lfprojects.org/policies/trademark-policy/). The Linux Vendor Firmware Service is a secure portal which allows hardware vendors to upload firmware updates.

This article serves as a guide for using the Lenovo BIOS Tools app from configuration to debugging, including best practices.

BIOS Updates at Your Own Risk
IGEL is offering and supporting the LVFS BIOS Update mechanism - BIOS updates are performed at your own risk!

The LVFS BIOS update mechanism is functional even with Secure Boot enabled and when a BIOS password is set.

If the BIOS of your devices is distributed via the Linux Vendor Firmware Service (LVFS), you can update, downgrade, or reinstall it using the IGEL Universal Management Suite (UMS). As the procedures for reinstalling and downgrading the BIOS are analogous to the update procedure, we will use the term "update" in the following instructions.

Tip: Direct Download of Firmware from fwupd Repository
To download valid firmware updates on a given test device, run the following command on the test device:

```
fwupdmgr refresh --force
fwupdmgr get-updates --json > /tmp/updates.json
```

The `updates.json` file includes links to the `.CAB` files from `fwupd` , use `wget` to download.

Supported Devices

Currently supported Lenovo devices:

- ThinkCentre M70q Gen3
- ThinkCentre M70q Gen5
- ThinkCentre M75q Gen2
- ThinkCentre M75q Gen5
- ThinkCentre Neo50q Gen4
- ThinkPad L13 Gen4

- ThinkPad L13 Gen5
- ThinkPad L14 Gen4
- ThinkPad L14 Gen5
- ThinkPad L15 Gen4
- ThinkPad L16 Gen1

Requirements

- UMS 12.01 or higher
- Device supports LVFS
- Supported devices with IGEL OS Base System 12.7.0 or higher

> ⚠ The IGEL OS Base System needs to be installed directly on the device. The Lenovo BIOS Tools app is unsupported if the IGEL OS boots from a UD Pocket.

Configuring the App in the UMS Web App

Importing the App

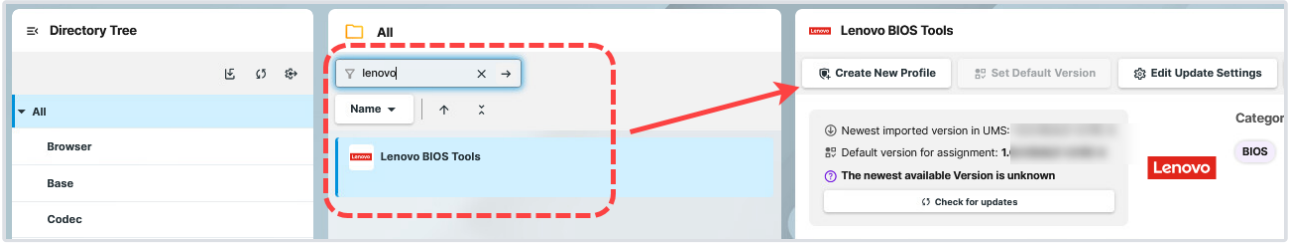
Import the Lenovo BIOS Tools app into your UMS. For more information on how to do this, see (12.06.120-en) How to Import IGEL OS Apps from the IGEL App Portal or (12.06.120-en) How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access .

Creating a Profile

To distribute the app to the devices, create a profile:

1. In the UMS Web App, go to **Apps** and search for “BIOS” to find the **Lenovo BIOS Tools** app.

2. Click **Create New Profile**.

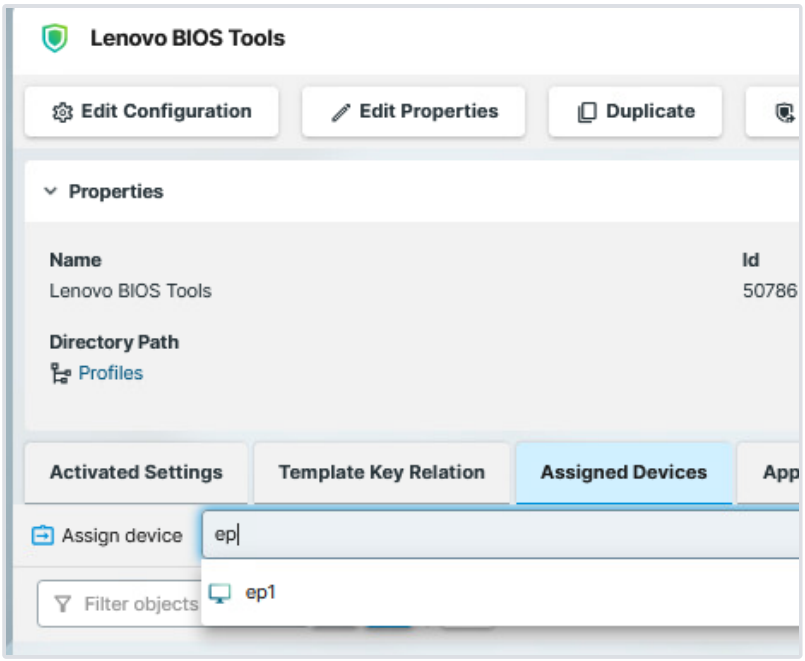


3. Define a name for your profile and save.

For more on profile creation, see (12.06.120-en) How to Create and Assign Profiles in the IGEL UMS Web App .

Assigning the Profile to Your Devices

1. In the field **Assign device**, enter the name of the device or device directory for which you want to use the Lenovo BIOS Tools app.



2. Select **Assign and apply changes now.**

Setting up the File Source

Since not only updating the BIOS but also its configuration is done using files, we need to set up a file source that is reachable by all devices.

The creation of the files is described in the relevant sections. The procedures described here are the same for all files in question, that is:

- BIOS update file
- BIOS settings file

Additional information

- Instead of a single `.CAB` file, it is possible to use a `.ZIP` file containing multiple `.CAB` files
  - There is no danger of flashing wrong firmware, the content of the `.CAB` file will be checked and has to match the system

- The `.CAB` file is not limited to BIOS updates: Any available firmware for a Lenovo device is supported:
  - EC (Embedded Controller) firmware update
  - Intel ME (Management Engine) firmware update
  - Docking station firmware update
  - NVMe drive firmware update
  - Secure Boot DBX update

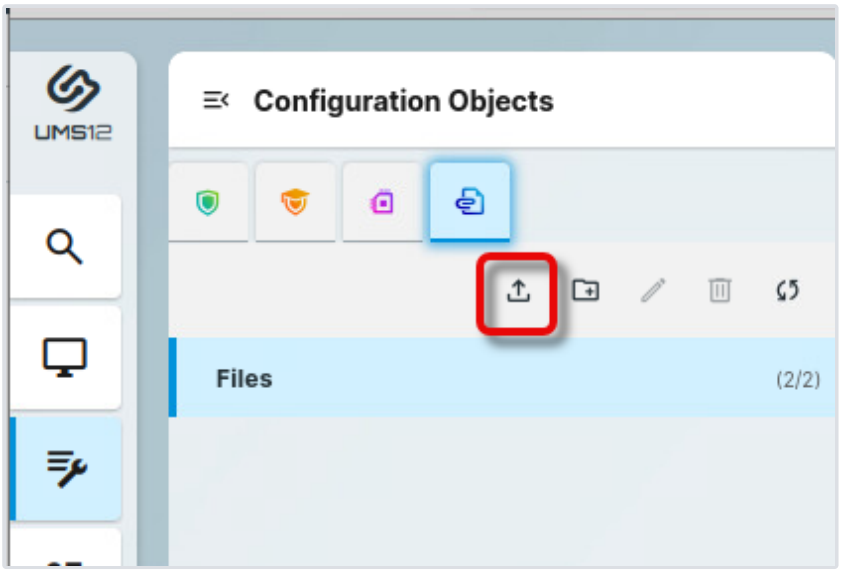
Getting the BIOS Update File from LVFS

→ Look up the latest update file from https://fwupd.org/ and download it. If you want to use the UMS for file distribution, store it in a location that is reachable from the machine on which your UMS Server is running.

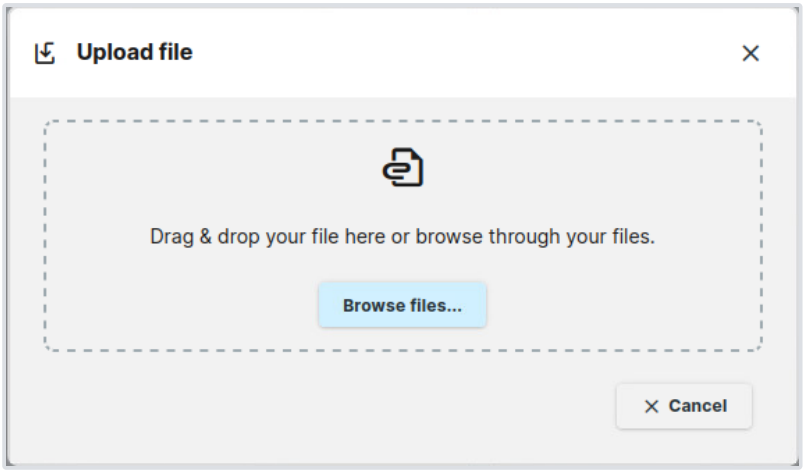
Using UMS File Transfer

The following example shows how to use the UMS file transfer facility for file deployment.

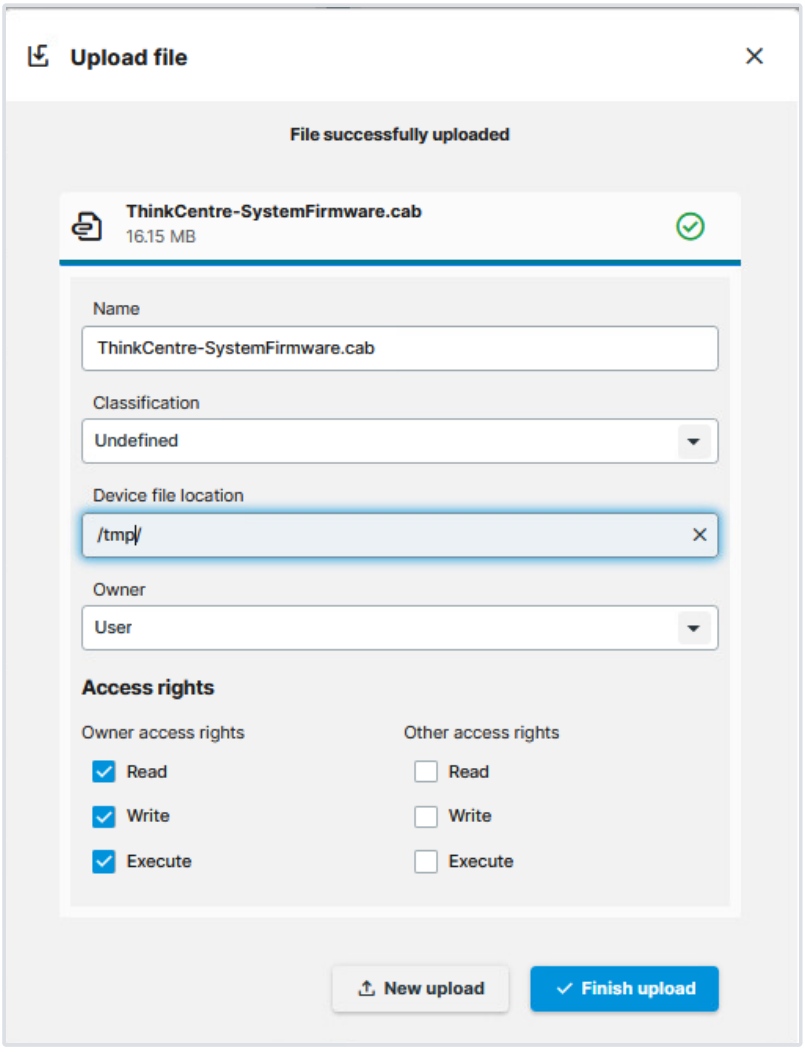
1. In the UMS Web App, go to **Configuration Objects**, select the icon for files, and then the icon for uploads.



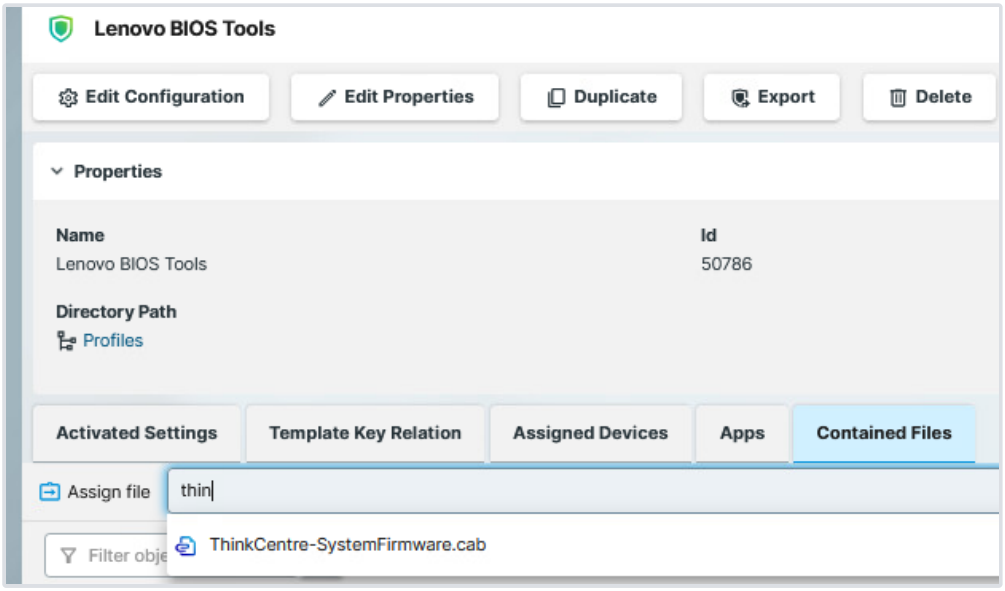
2. Choose the BIOS update file on your system via drag & drop or via **Browse files...**.



3. In the field **Device file location**, define the local path in which the file will be stored on the device, e.g. `/tmp/`. Afterward, click **Finish upload**.



4. Assign the file to your devices by assigning it to the profile we have created beforehand.



Updating the BIOS

Making the BIOS Update File Available

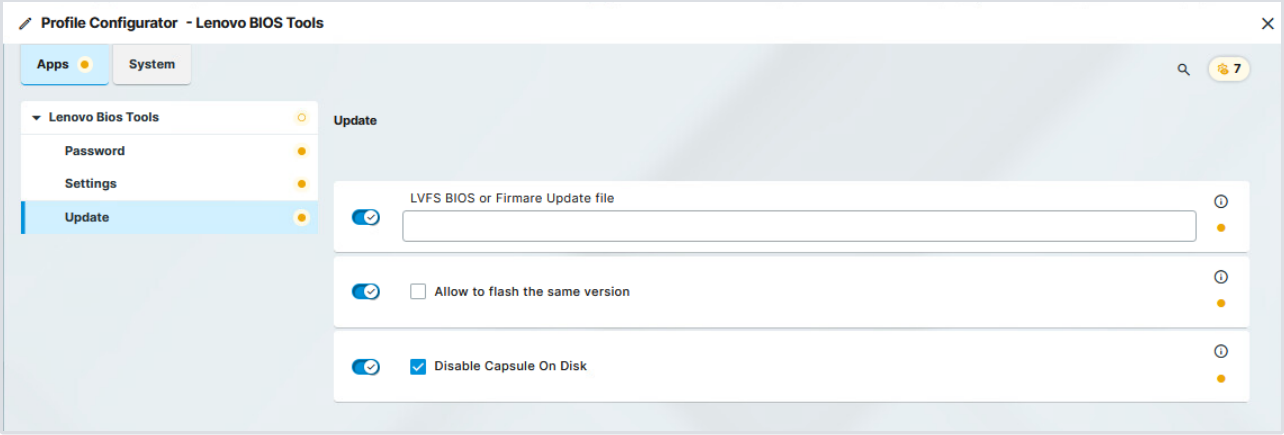
→ Make the BIOS update file available to your devices; see Setting up the File Source (see page 381).

Configuring the Devices for the BIOS Update

1. Open the previously configured Lenovo BIOS Tools profile.

2. Go to **Apps > Lenovo BIOS Tools > Update.**

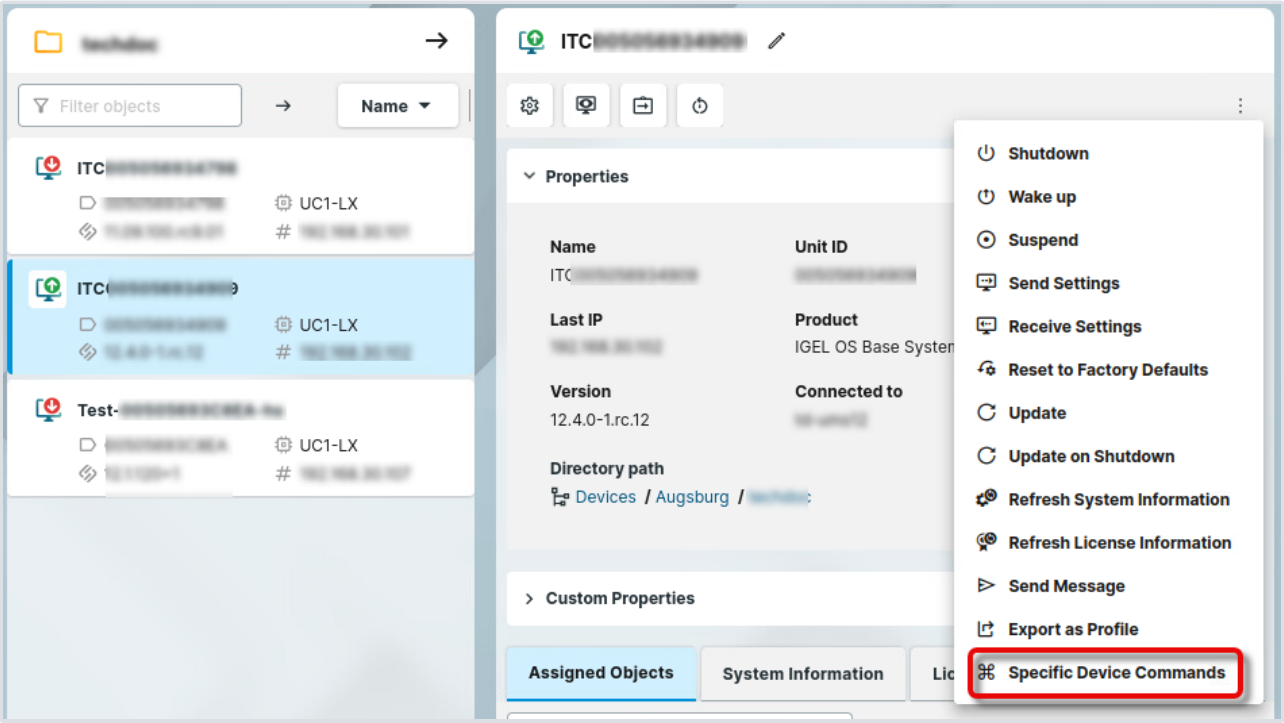
2. Under **LVFS BIOS or Firmware Update file** provide the local path of the BIOS update file.



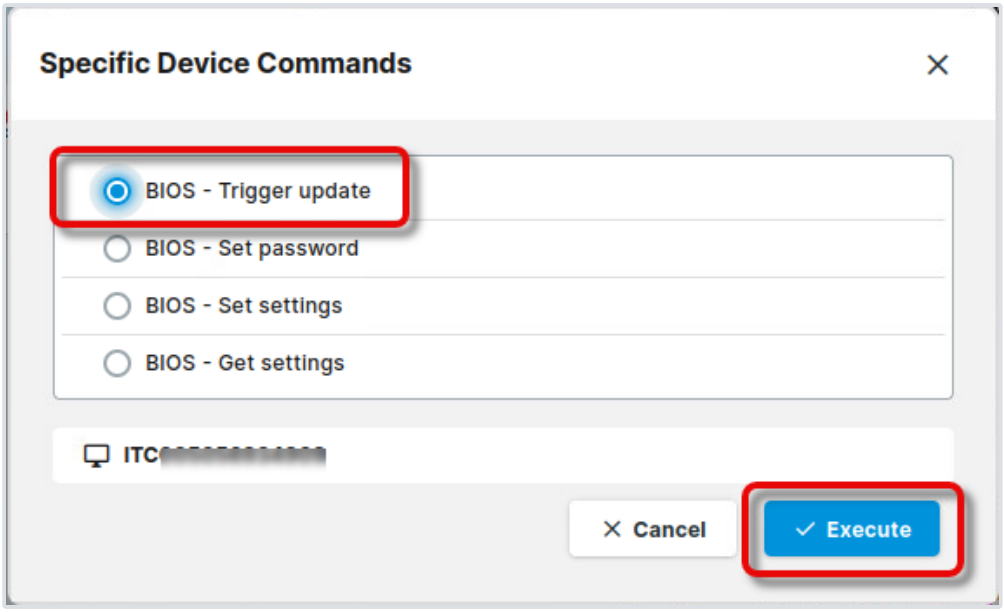
You can reinstall the same BIOS/Firmware version that had already been installed on the device if you enable **Allow to flash the same version**.

Triggering the BIOS Update

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**



2. Select **BIOS - Trigger update** and click **Execute**.



The target devices receive a reboot command; a corresponding message is displayed.

The timespan before the BIOS logo and the progress bar is shown might be significantly longer than usual. Please ensure that the device remains powered on until the update process is finished.

Changing the BIOS Settings

To change the BIOS settings a `set_settings.json` file needs to be transferred to the device with the setting updates in the correct syntax.
In the section below, we describe in detail the easiest way to do this, that is:

1. Getting the `get_settings.json` file from the device through scp. This way you get the correct syntax example.
2. Editing the transferred file with an editor of choice.
3. Transferring it back as `set_settings.json` to the device or device directory. This way you can distribute the update in batches.

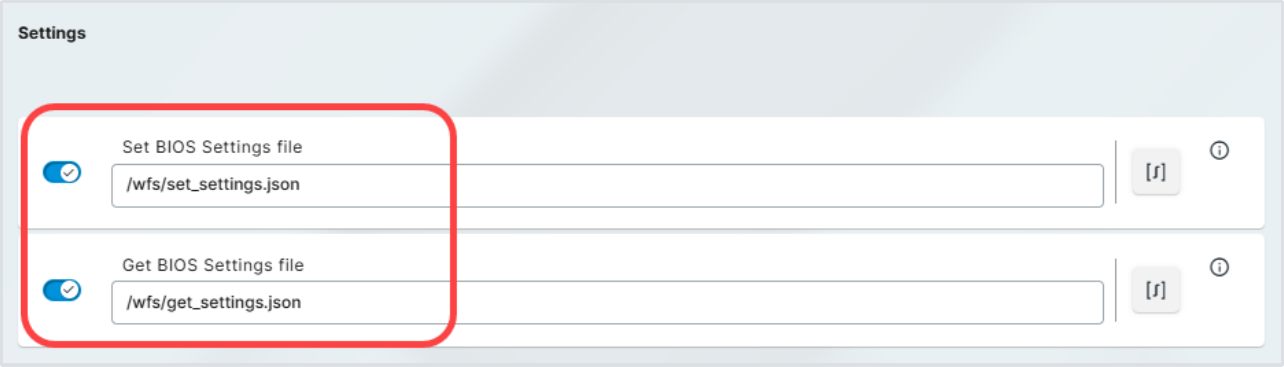
This is the recommended way to change BIOS settings, but not the only way. For example, you can also write the `set_settings.json` from scratch and transfer it using a USB pen drive.

Defining the Paths for Exchanging the BIOS Settings Files

First, we will define a local directory path in which the Lenovo BIOS Tools app will store the current BIOS settings as a file and a local directory path in which the edited settings file will be stored so the app can apply them to the device's BIOS.

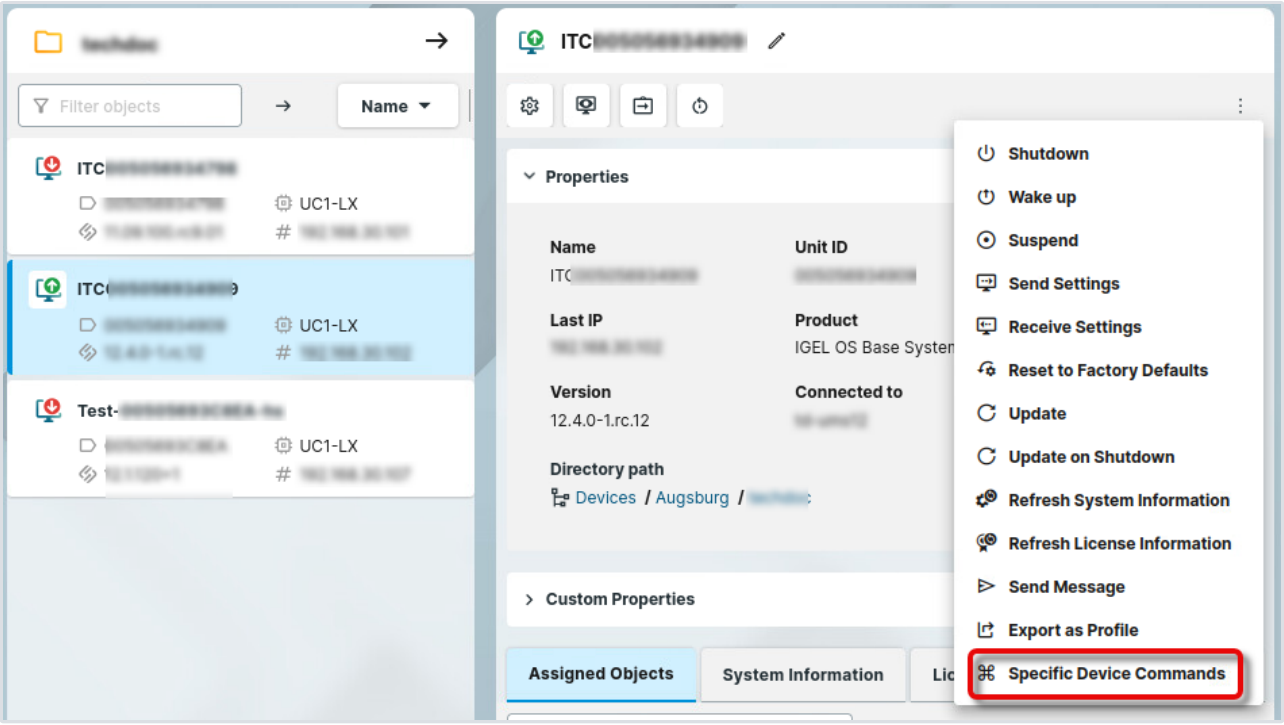
→ In the BIOS Tools profile, go to **Apps > Lenovo BIOS Tools > Settings**, make the following edits, and save your settings.

- **Set BIOS settings file**: Path where the file with the changed settings will be stored.
- **Get BIOS settings file**: Path to the file with the current settings. The path has to include the filename, for example: `/wfs/get_settings.json`

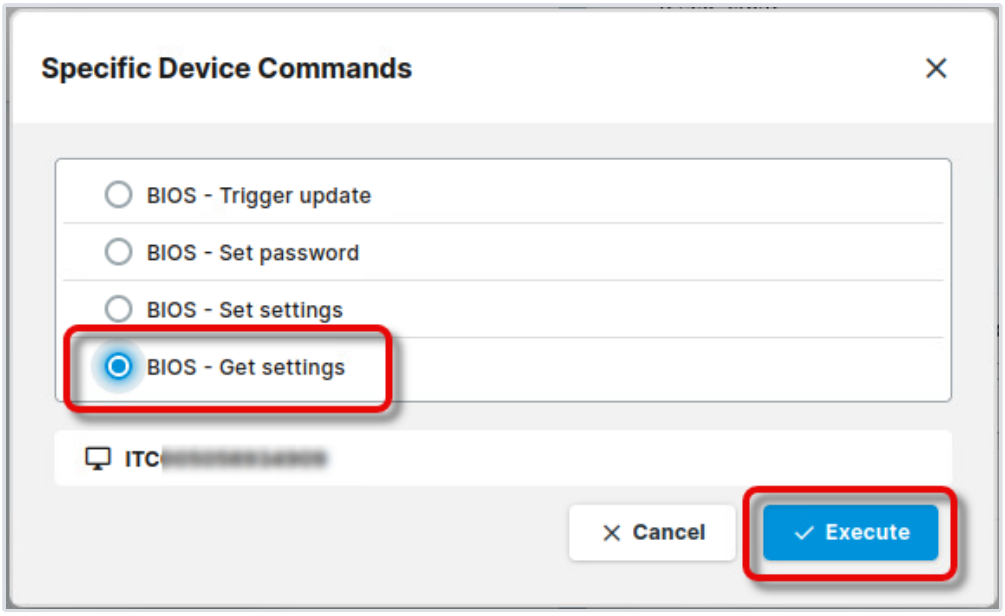


Generating the Current BIOS Settings File

1. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Commands**.



2. Select **BIOS - Get settings** and click **Execute**.



All BIOS settings will be listed in the saved `.json` file, including a list of possible values.

Transferring and Editing the BIOS Settings File

1. Enable SSH as described in SSH Access in IGEL OS 12[161] .

2. Use scp from a linux or windows terminal:

```
scp username@remote:/path /localpath
```

- Depending on the SSH access configuration, `username` could be `root` , `ruser` , or `user` .
- `remote` is the IP address of the OS 12 device.
- `/path` it the path to the `get_settings.json` on the OS 12 device
- `/localpath` is the path to where the file will be saved locally

3. Edit the configuration file as desired.

Limitations

- Some settings require that a BIOS supervisor password has been set.
- Some settings can only be changed from the BIOS menu (F1).

161. https://kb.igel.com/en/igel-os-base-system/12.6.1/ssh-access-in-igel-os-12

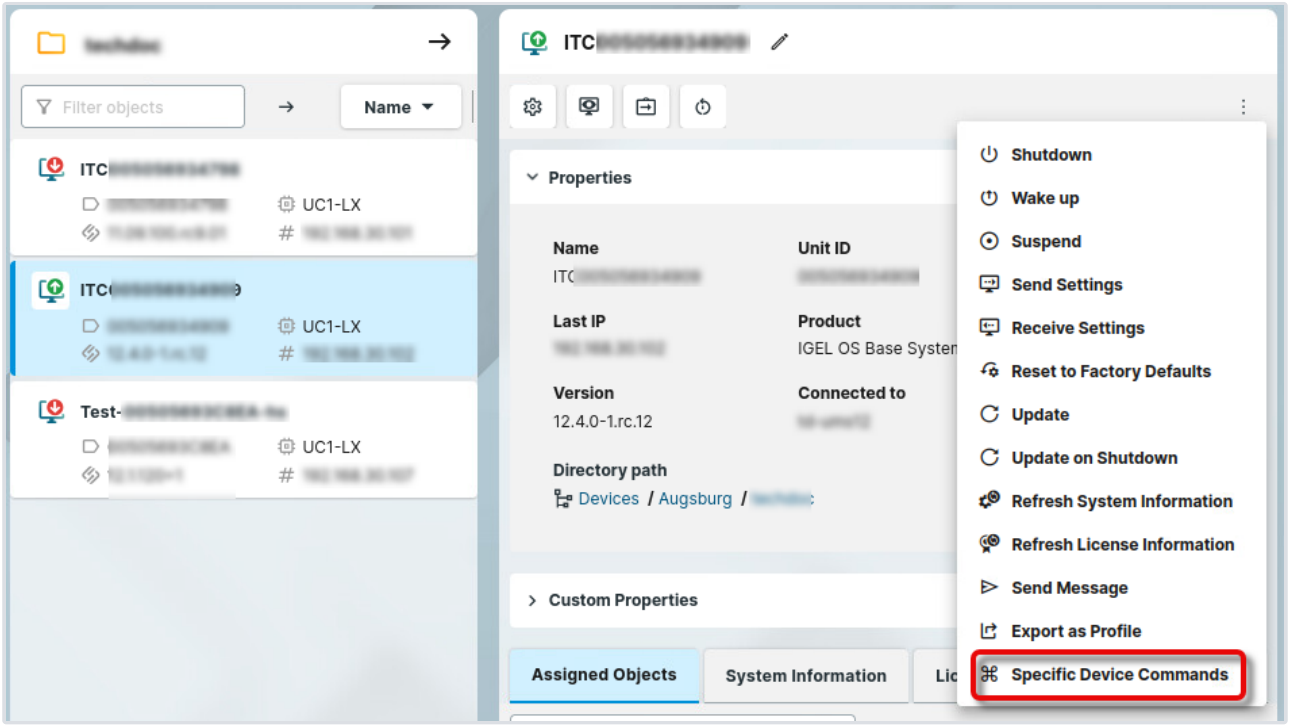
- For more details, check the Lenovo documentation: https://support.lenovo.com/manuals/um927324-thinklmi-lenovo-bios-setup-using-linux-wmi-deployment-guide-thinkpad

It is sufficient to specify only those BIOS setting you want to change so that your edited file contains snippets instead of all possible settings.

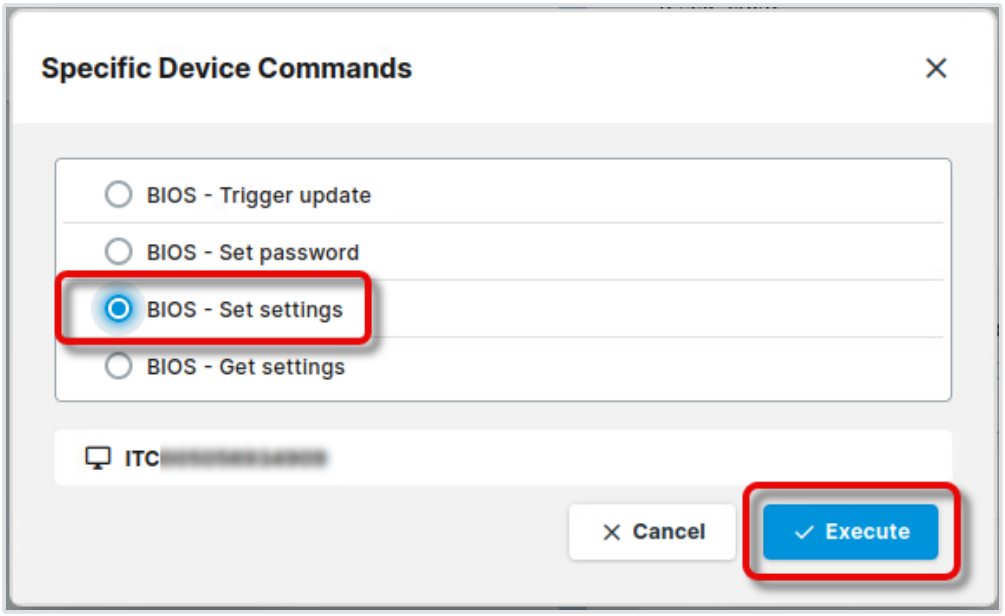
8. Save the settings file and make the edited file available as described under Setting up the File Source (see page 379).

Deploying the Changed Settings on the Device

1. In the UMS, select the relevant devices (or device directory), open the context menu, and select **Specific Device Command**.



2. Select **BIOS - Set settings** and click **Execute**.



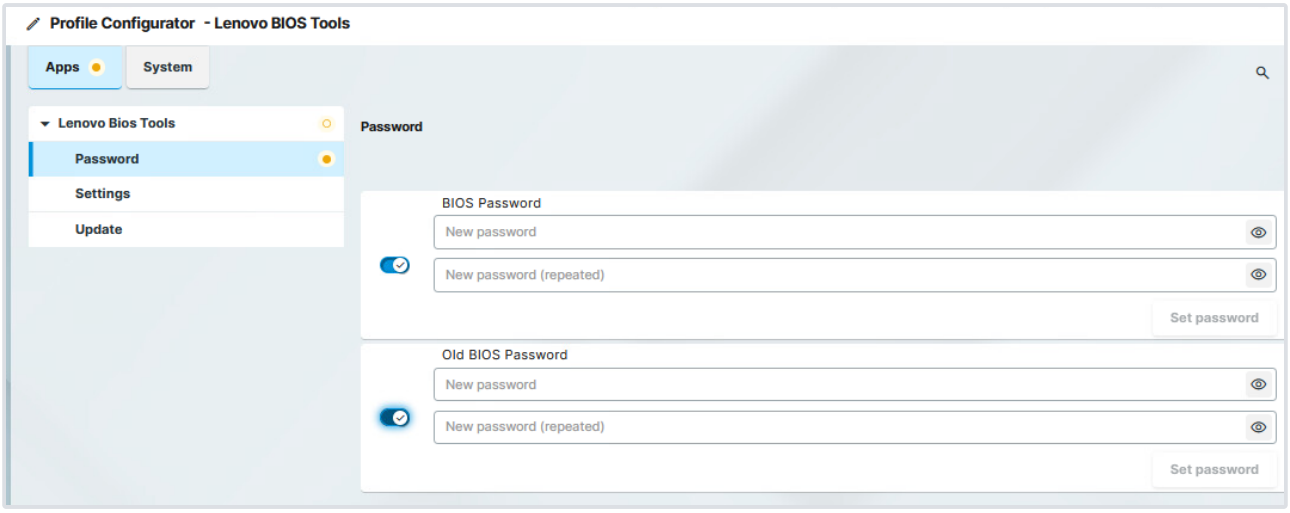
Setting a BIOS Password

Limitation

Lenovo does not support setting a new BIOS supervisor password if there is no old/current BIOS supervisor password.
Changing the BIOS password is possible, see below.

Changing the BIOS Password

1. In the BIOS Tools profile, go to **Apps > Lenovo Bios Tools > Password**.

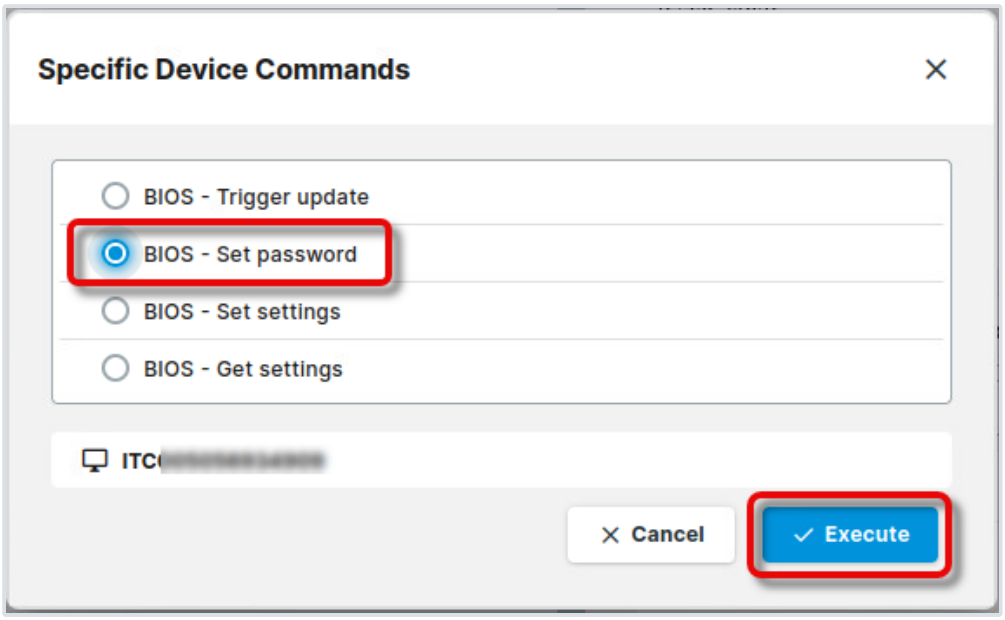


2. Enter the current BIOS supervisor password under **Old BIOS Password.**

3. Enter the new BIOS supervisor password under **BIOS Password.**

4. In the UMS, select the relevant devices (or directory), open the context menu, and select **Specific Device Command**.

5. Select **BIOS - Set password** and click **Execute**.



6. If the command is performed successfully, reboot the device.

Using the Command Line Interface (CLI)

For testing the BIOS update on a single device, you can use the command line tool as an alternative to a scheduled job from the UMS.

As a prerequisite, the steps described under Setting up the File Source and the relevant settings in the profile must be completed.

When the command has been executed, a dialog informs you that a reboot is required. You can choose between two options:

- Perform the reboot and update right away
- Postpone the update to the next reboot

Usage

```
lenovo-bios-tools [OPTIONS] COMMAND [ARGS]...
```

Options

Option / Contrary Option	Comment
`--debug / --no-debug`	Provide extensive information (verbose mode)
`--help`	Show the help text and exit

Commands

Command	Argument (Short / Long Form)	Comment
`update`		Handle BIOS update
	`-e --enable`	Trigger BIOS update. Will be triggered after reboot.
	`-d --disable`	Disable BIOS update
	`--help`	Show the help text and exit
`password`		Set BIOS password
`settings`		
	`-g --get`	Get current BIOS settings

Command	Argument (Short / Long Form)	Comment
	`-c --configure`	Configure BIOS settings

Example

The following command performs a BIOS update and displays extensive information:

```
update --debug -e
```

Debugging

For most cases, the normal logging to journalctl should be good enough to identify any problems. The default loglevel is “INFO”.

→ To enable loglevel “DEBUG”, enable the registry key `app.lenovo_bios_tools.config.enable_debug`

Microsoft Edge



- Getting Started with Microsoft Edge on IGEL OS (see page 395)
- Configuration of Microsoft Edge on IGEL OS (see page 398)

Getting Started with Microsoft Edge on IGEL OS

This article describes how you can create a Microsoft Edge browser session and configure it on IGEL OS.

For details on how to import the app to your IGEL Universal Management Suite (UMS), see How to Import IGEL OS Apps from the IGEL App Portal[162].

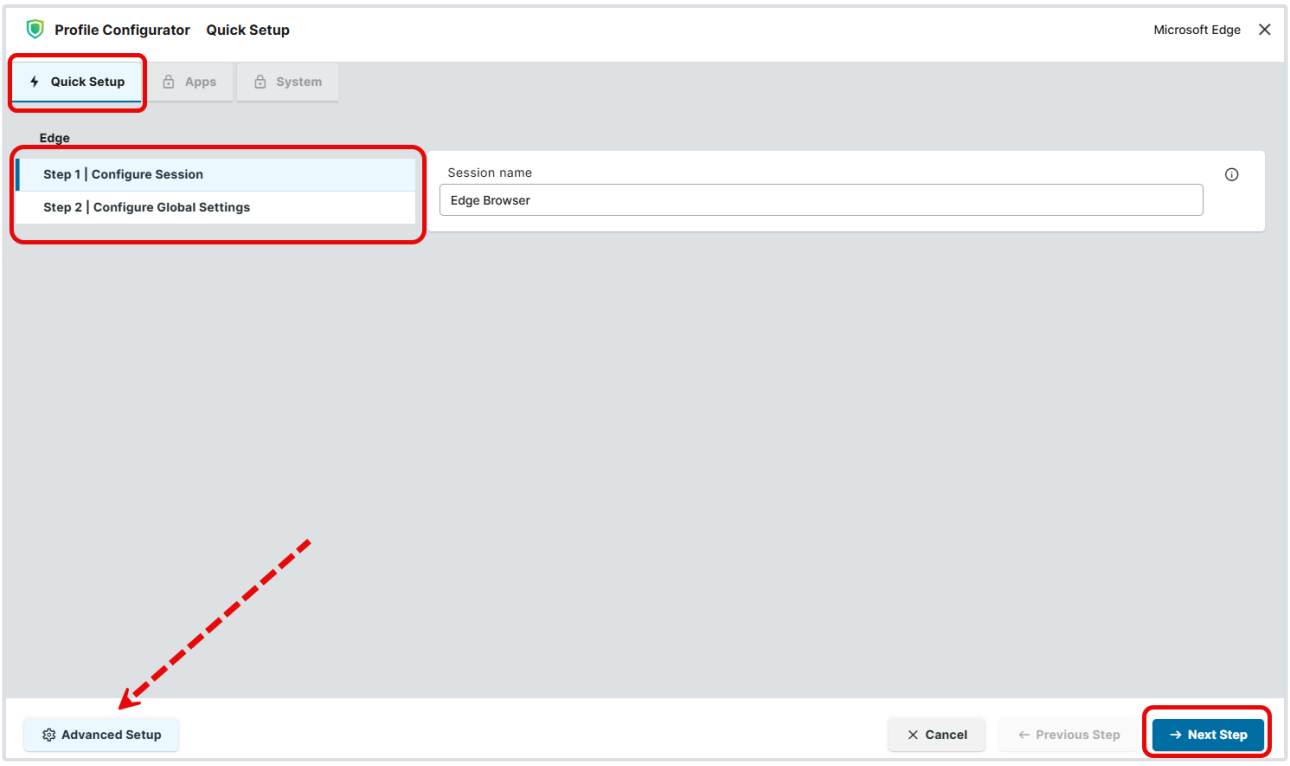
How to Create a Session

1. In the IGEL UMS, create a profile configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[163].

Quick Setup Mode (for a Quicker Profile Creation)

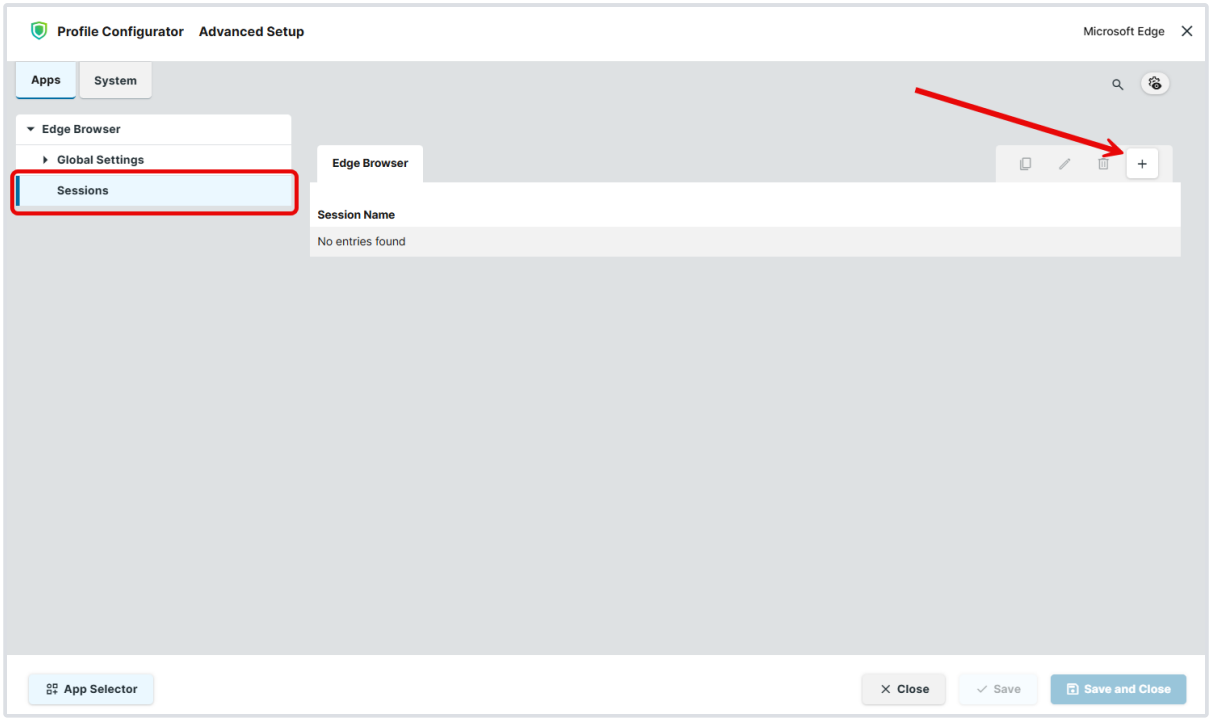
To quickly create an Edge session and configure the basic settings, you can use Quick Setup mode when creating a profile configuring the Microsoft Edge Browser app.

→ To display all available app settings, click **Advanced Setup**.

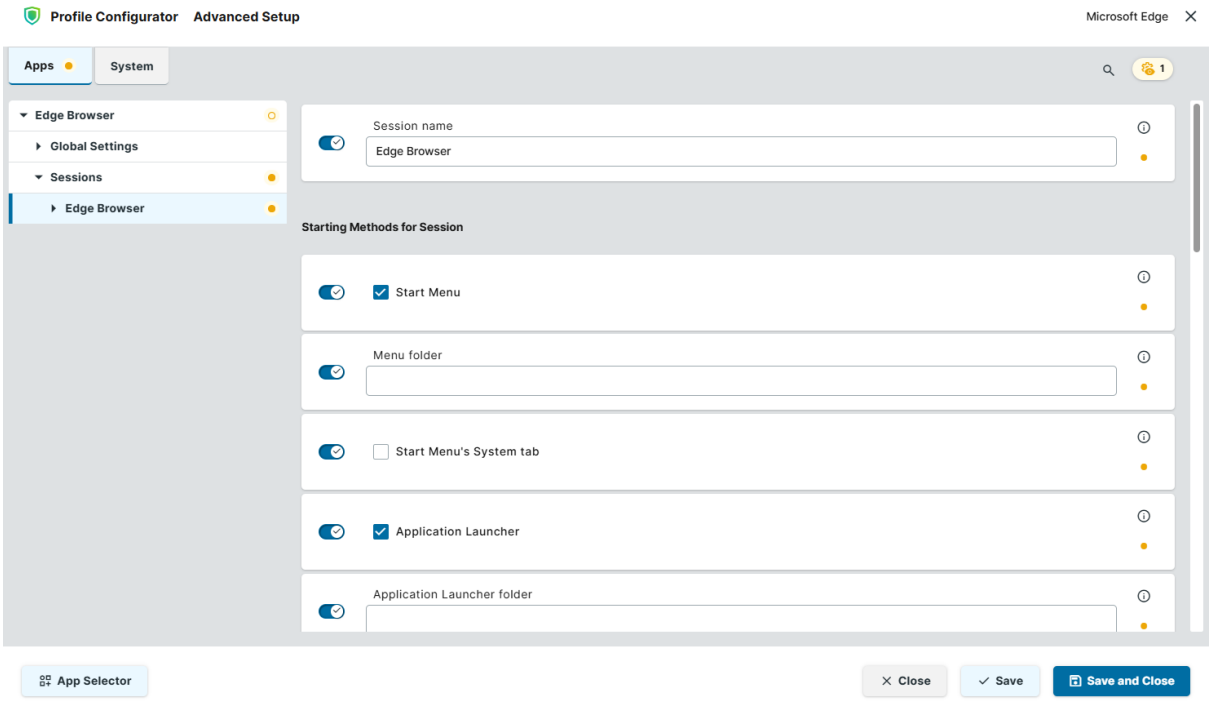


2. In the profile configurator, go to **Apps > Edge Browser > Sessions** and click +.

162. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
163. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



3. Configure the starting methods for the created session. For details, see Starting Methods for Apps[164].



164. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

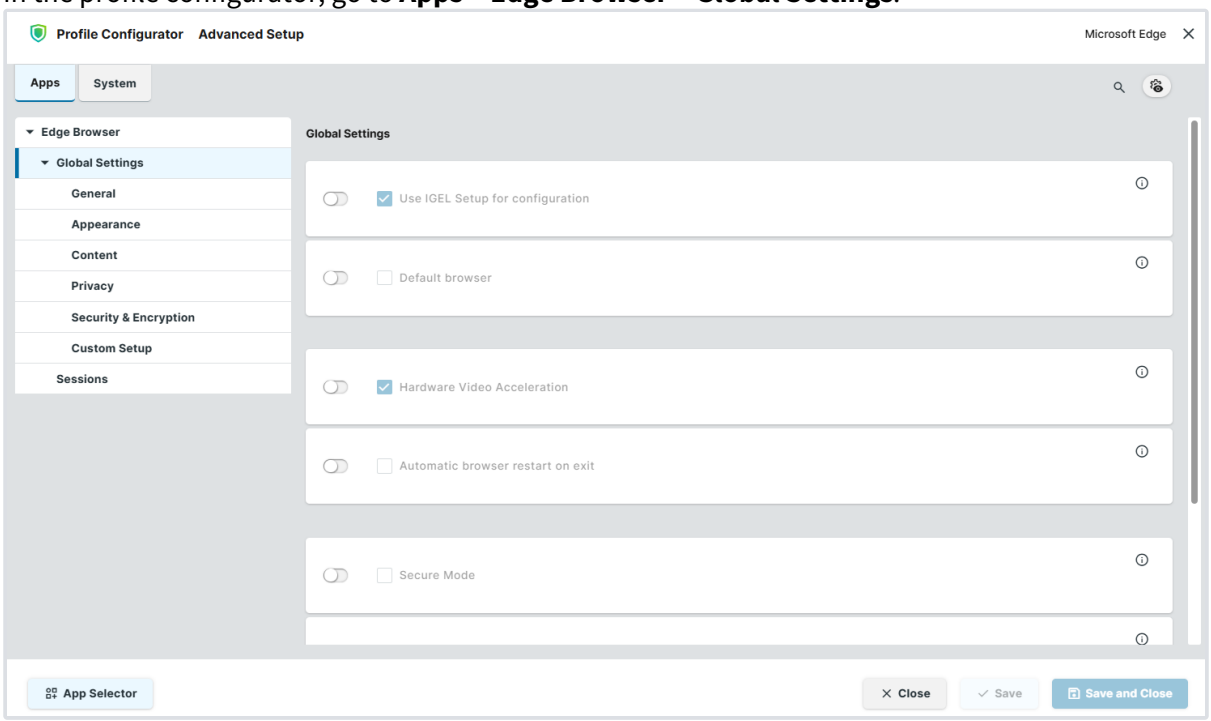
4. Edit the settings according to your needs. For details, see Configuration of Microsoft Edge on IGEL OS[165].

165. https://kb.igel.com/en/igel-apps/current/configuration-of-microsoft-edge-on-igel-os

Configuration of Microsoft Edge on IGEL OS

Configuring Global Settings

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings**.



2. Edit the settings according to your needs. The parameters are described in the following.

Use IGEL Setup for configuration

> While some changes will be applied instantly, others will only take effect after a browser restart.

- [x] The settings made in the IGEL Setup or the UMS configuration dialog will be effective. (Default)
- [ ] The settings made in the IGEL Setup or the UMS configuration dialog will not affect the behavior of Microsoft Edge.

> Custom policies are always effective, regardless of this setting.

Default Browser

Importance of Setting a Default Browser Correctly
Please note the following:

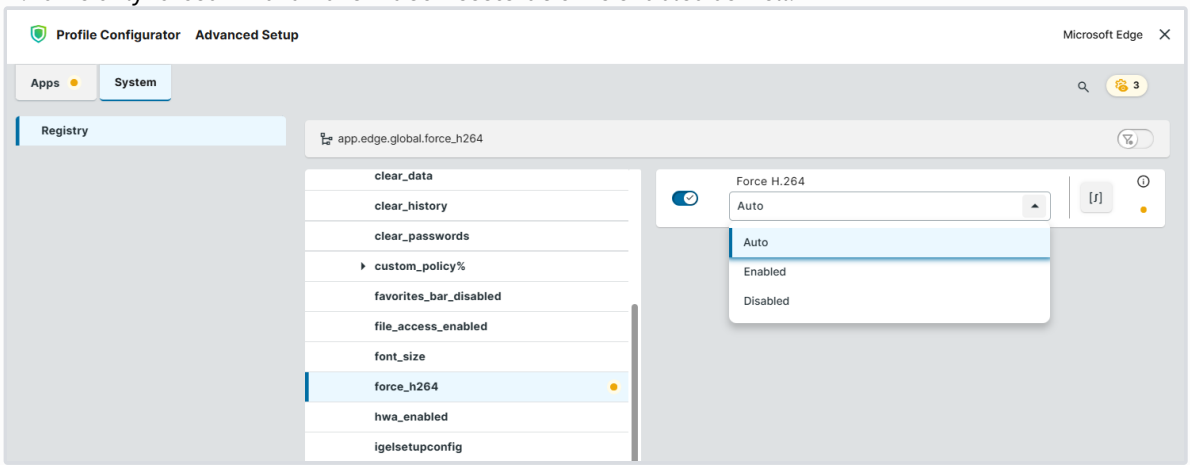
- If several browsers are installed and no browser is set as default, the browser whose name is last in alphabetical order is the default. Example: If Chromium, Edge, Firefox, and Island are installed and no default browser is set, Island will be the default browser.
- If several browsers are erroneously set as default, the browser from this selection whose name is last in alphabetical order will be the actual default.

- [x] Microsoft Edge is the default browser.
- [ ] Microsoft Edge is not the default browser. (Default)

Hardware Video Acceleration

- [x] Hardware video acceleration is enabled for the Microsoft Edge browser on Intel devices. (Default)
- [ ] Hardware video acceleration is disabled for the Microsoft Edge browser.

To improve video playback by preferring H.264 video, you can use the registry key **System > Registry > app.edge.global.force_h264**. This can reduce stuttering and CPU usage on some systems. If set to 'Auto', H.264 is only forced if **Hardware Video Acceleration** is enabled as well.



Automatic browser restart on exit

- [x] The browser is automatically restarted after all browser windows have been closed.
- [ ] The browser is not automatically restarted after closing the last browser window. (Default)

Secure Mode

This setting controls the parameters **Block Edge settings** and **Hide favorites bar**. You can still modify these parameters individually, no matter if **Secure mode** is enabled or disabled.

- ☑ Parameters **Block Edge settings** and **Hide favorites bar** will automatically be activated. Also, some security-related policies will be set.
- ☐ There are no restrictions concerning browser settings, the favorites bar, or security-related policies. (Default)

Block Edge settings

This setting is identical to **Block Edge Settings** under **Global Settings > General**.

- ☑ The user cannot change any settings for Microsoft Edge. (Default)
- ☐ The user can change settings for Microsoft Edge.

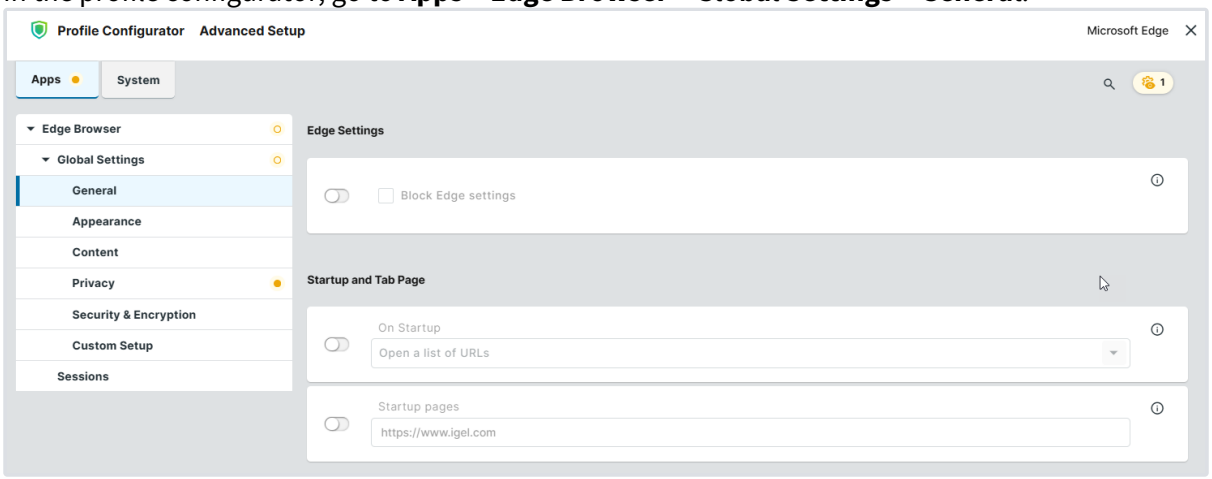
Hide favorites bar

This setting is identical to **Hide favorites bar** under **Global Settings > Appearance**.

- ☑ The favorites bar is hidden.
- ☐ The favorites bar is shown. (Default)

Configuring General Settings

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > General**.



2. Edit the settings according to your needs. The parameters are described in the following.

Block Edge settings

- ☑ The user cannot change any settings for Microsoft Edge.

- [ ] The user can change settings for Microsoft Edge. (Default)

On Startup

Defines what is displayed on browser startup.

Possible options:

- **Open a new tab**: The browser starts with an empty tab.
- **Open a list of URLs**: The page or set of pages defined by **Startup page** is displayed. (Default)
- **Restore the last session**

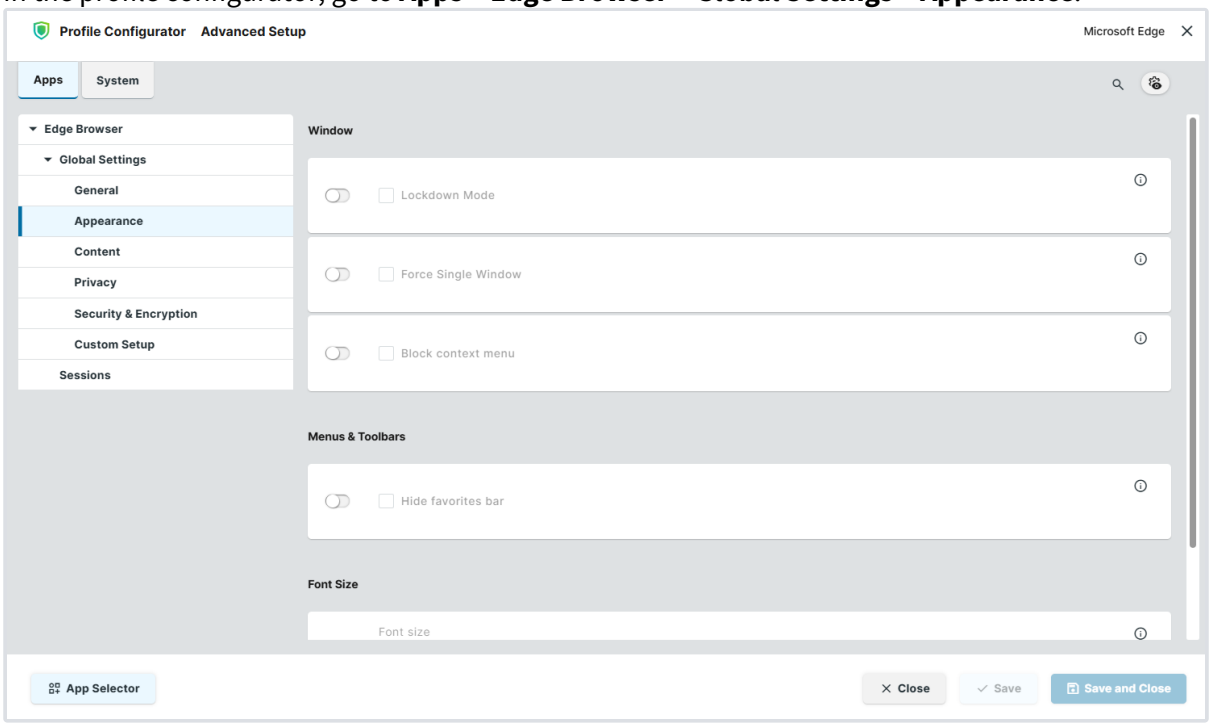
Startup pages

This parameter is only shown when **On Startup** is set to **Open a specific page or set of pages**.

Specifies the page or set of pages to be shown when the user opens a new tab. This is effective only if **On Startup** is set to **Open a specific page or set of pages**. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". (Default: "https://www.igel.com ")

Configuring the Browser Appearance

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > Appearance**.



2. Edit the settings according to your needs. The parameters are described in the following.

Lockdown mode

- ☑ The user will not be able to leave the main browser window. New tabs and windows are blocked.
- ☐ The user can leave the main browser window. New tabs and windows can be opened. (Default)

Force single window

- ☑ Links are always opened in the same window / tab. New windows or tabs opened externally, e.g. via `Ctrl+N`, `Ctrl+T`, are not blocked.
- ☐ New tabs and windows are not redirected to the main window. (Default)

Block context menu

- ☑ The right-click context menu will be blocked.
- ☐ The right-click context menu will not be blocked. (Default)

Hide favorites bar

- ☑ The favorites bar is hidden.
- ☐ The favorites bar is shown. (Default)

Font size

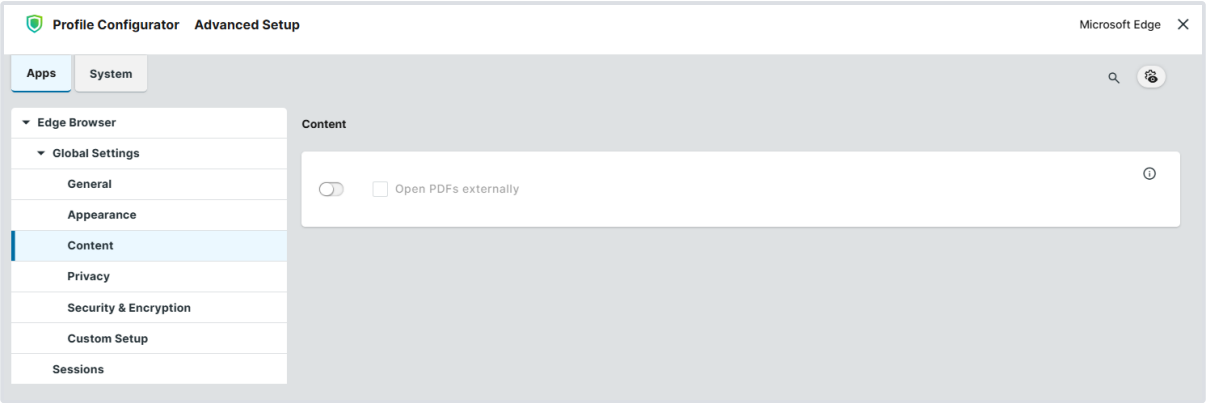
> This setting will only take effect after a restart.

Possible options:

- **Very small**
- **Small**
- **Medium (recommended)** (Default)
- **Large**
- **Very large**

Configuring Content Settings

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > Content**.



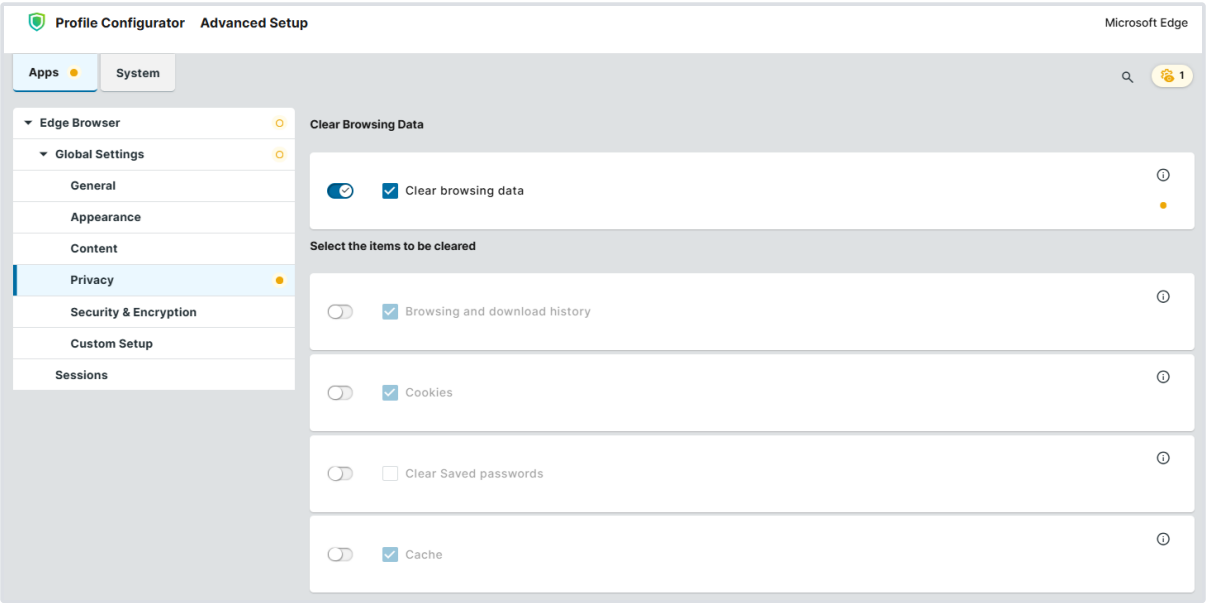
2. Edit the settings according to your needs. The parameters are described in the following.

Open PDFs externally

- [x] PDFs are automatically opened externally, e.g. with Evince Document Viewer[166] if installed.
- [ ] PDFs are opened with the internal PDF viewer. (Default)

Configuring Privacy Settings

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > Privacy**.



166. https://app.igel.com/evince/43.1.2+1

2. Edit the settings according to your needs. The parameters are described in the following.

Clear browsing data

- ☑ Data created during the Edge session will be deleted when the browser is closed. What data are deleted is specified in the following options.
- ☐ Data created during the Edge session will not be deleted when the browser is closed. (Default)

Browsing and download history

This parameter is visible if **Clear browsing data** is enabled.

- ☑ Addresses (URLs) of visited websites and the list of downloads will be deleted when Edge is closed. (Default)

Cookies

This parameter is visible if **Clear browsing data** is enabled.

- ☑ All cookies, not only third-party cookies, will be deleted when Edge is closed. (Default)

Saved passwords

This parameter is visible if **Clear browsing data** is enabled.

- ☑ Passwords that have been saved during the browser session will be deleted when Edge is closed.
- ☐ Saved passwords entered will still be available when Edge or the system is restarted. (Default)

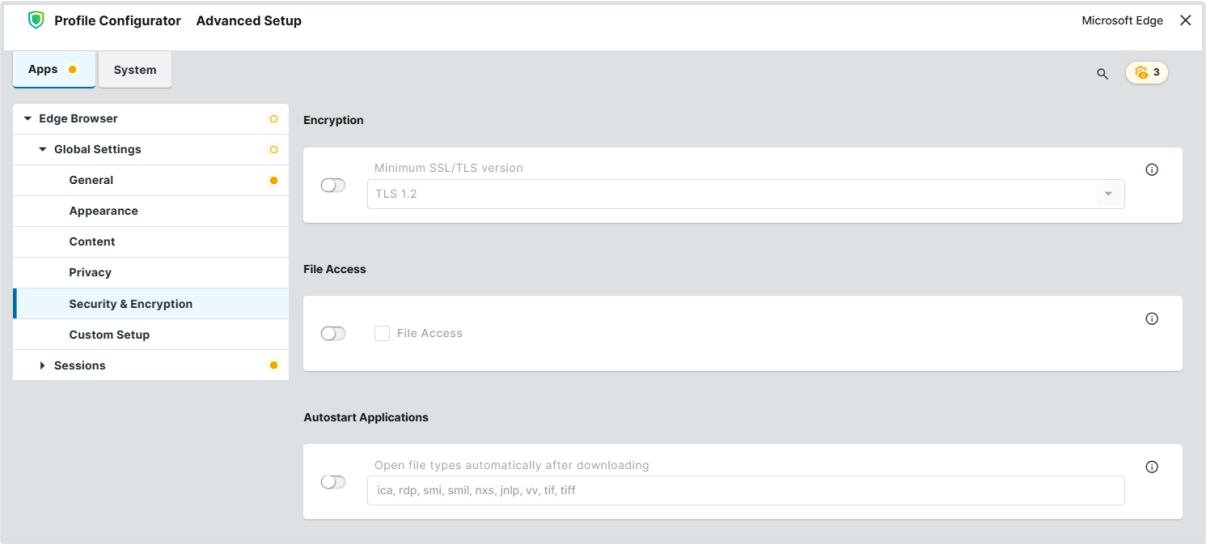
Cache

This parameter is visible if **Clear browsing data** is enabled.

- ☑ The cache for temporarily saving web pages will be emptied when Edge is closed.

Configuring Security and Encryption

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > Security & Encryption**.



2. Edit the settings according to your needs. The parameters are described in the following.

Minimum SSL/TLS version

Possible options:

- **TLS 1.2** (default)
- **TLS 1.3**

File access

- ☑ The browser can access local files on the endpoint device. Uploads are allowed.
- ☐ Local files cannot be accessed by the browser. Uploads are not allowed. When the user tries to upload a file, a message informs the user that the access to local files is blocked. (Default)

Open file types automatically after downloading

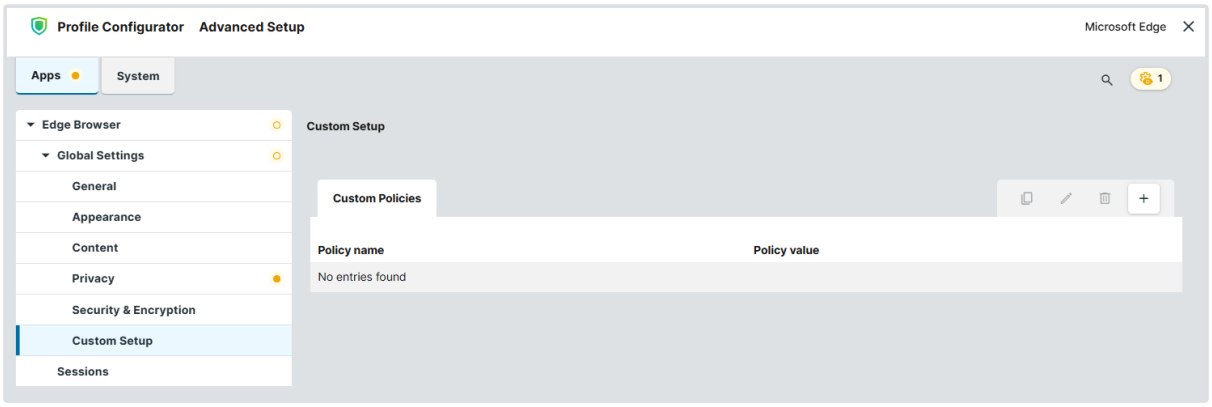
Any file whose suffix is listed here will be opened immediately after downloading. The list entries are separated by commas ",". (Default: "ica, rpd, smi, smil, nxs, jnlp, vv, tif, tiff")

Configuring Custom Policies

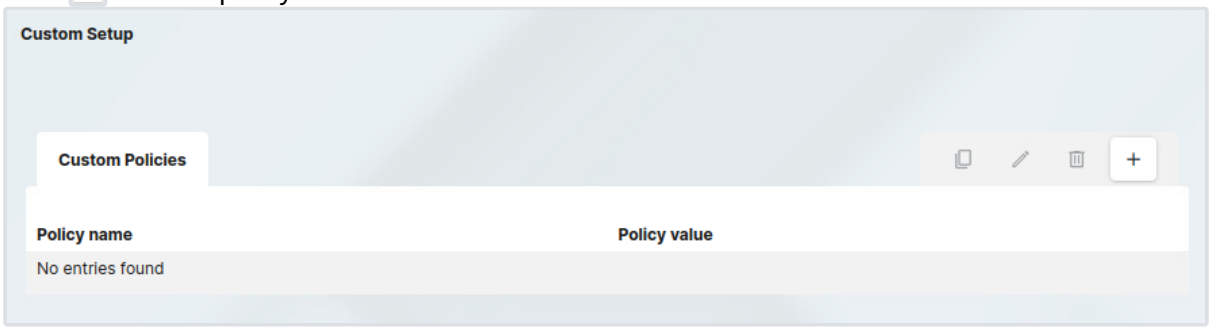
You can add, edit, and remove policies for the Edge sessions on your IGEL OS device. Please note that the custom settings always win over the IGEL Setup, i.e. if a policy is defined both here and in the Setup, but with different values, the value defined here is effective.

For a complete list of available policies, see https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies.

1. In the profile configurator, go to **Apps > Edge Browser > Global Settings > Custom Setup**.



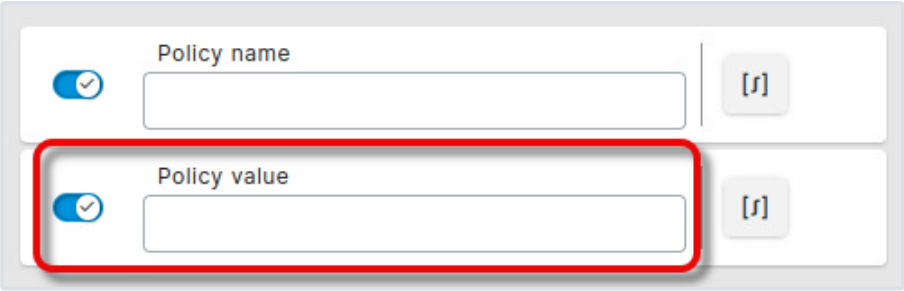
2. Click + to add a policy.



3. Enter the **Policy name**. For possible policies, see https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies



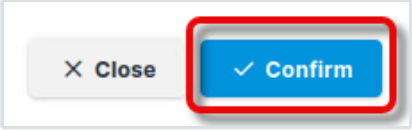
4. Enter the **Policy value**.



The data format is described in https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies. Please note the following:

- Use the correct data type (check out the example values)
- Make sure the desired policy is available in Microsoft Edge for Linux

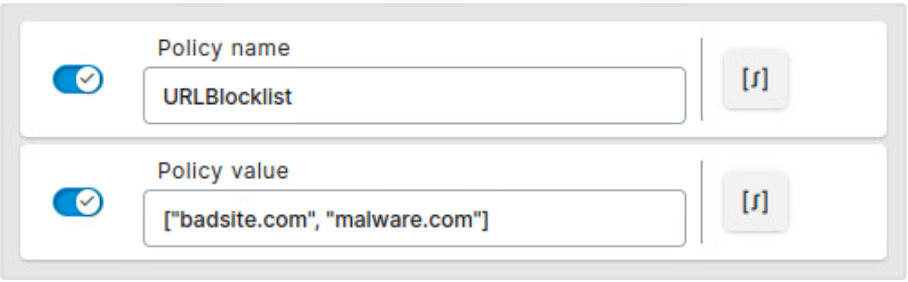
5. Click **Confirm** to create the policy.



URL Blocklist Example

If you want to block the websites badsite.com and malware.com, define your policy as follows (see also https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies#urlblocklist):

- **Policy name**: `URLBlocklist`
- **Policy value**: `["` badsite.com `", "` malware.com `"]`



Microsoft Intune



- Quick Start Guide: Onboarding with Microsoft Intune (see page 409)

You might also find the following IGEL Community article useful: HOWTO Microsoft Intune - IGEL Community Docs[167]
The content of this external guide is not covered by official support channels, and the IGEL Knowledge Base Team cannot guarantee its accuracy or completeness.

167. https://igel-community.github.io/IGEL-Docs-v02/Docs/HOWTO-Microsoft-Intune/

Quick Start Guide: Onboarding with Microsoft Intune

You might also find the following IGEL blog post useful: Microsoft Intune Agent for IGEL OS[168]
The content of this external guide is not covered by official support channels, and the IGEL Knowledge Base Team cannot guarantee its accuracy or completeness.

Requirements

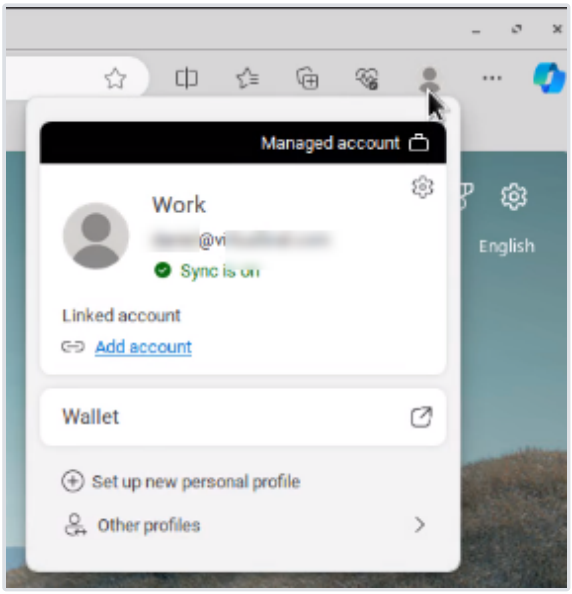
The following IGEL apps are installed on your device:

- The Microsoft Edge browser app is installed on your device
- You are logged in at the Microsoft Edge Browser with a managed account
- The Microsoft Intune app is installed on your device

Setting up the Intune App on Your Device

1. Start the Edge browser app on your device.

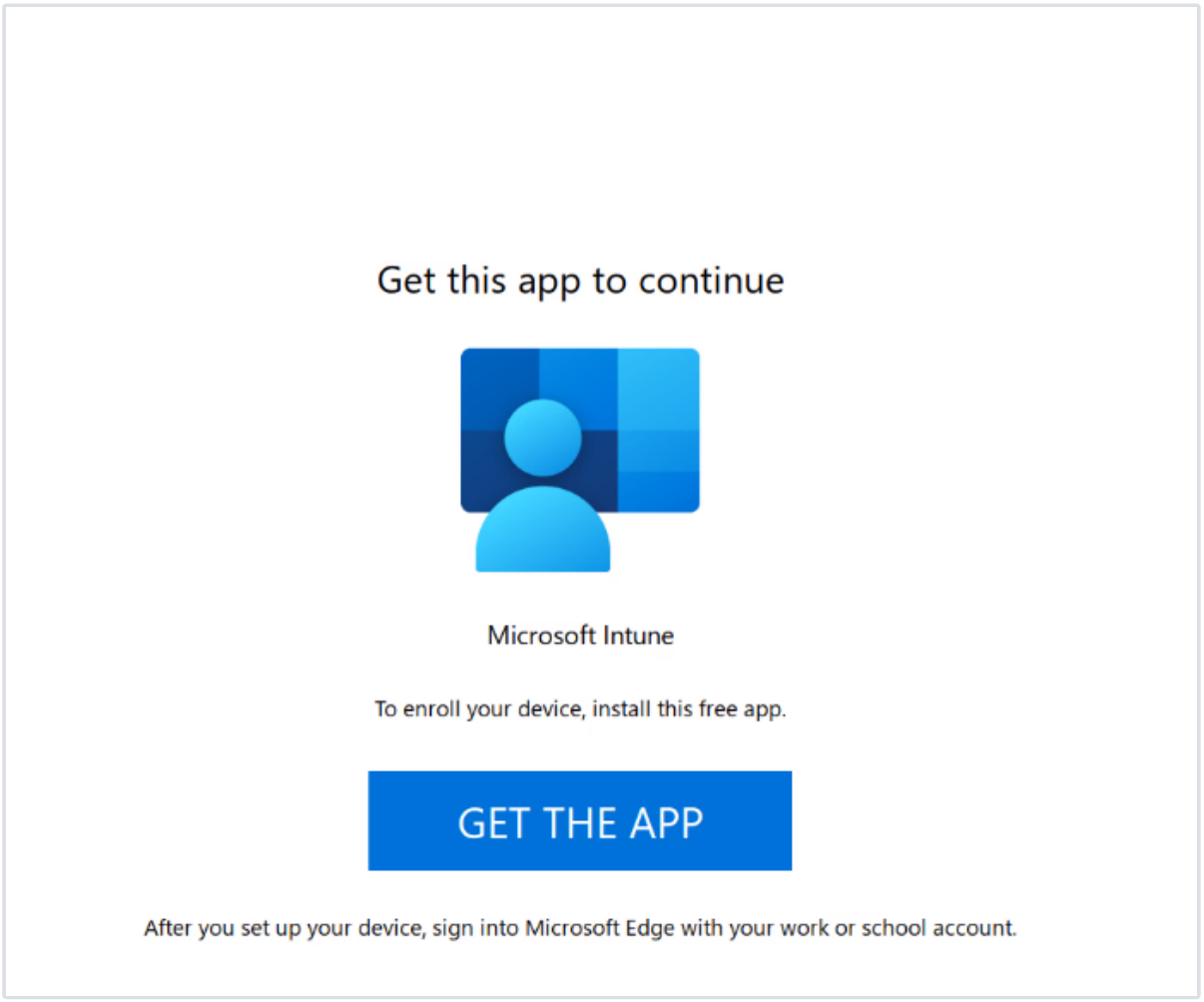
2. Verify you have a managed account.



3. With the Edge browser, go to `https://outlook.com/mail`
   You are redirected to the login page of your organisation.

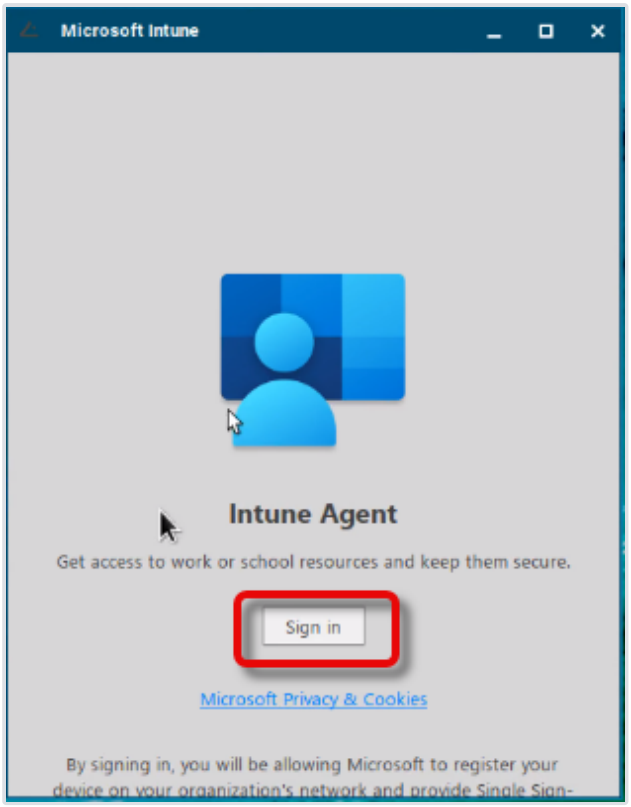
168. https://www.igel.com/blog/available-now-microsoft-intune-agent-for-igel-os/

4. Click **Continue**.
   You are taken to a page that requests you to install the Microsoft Intune app.

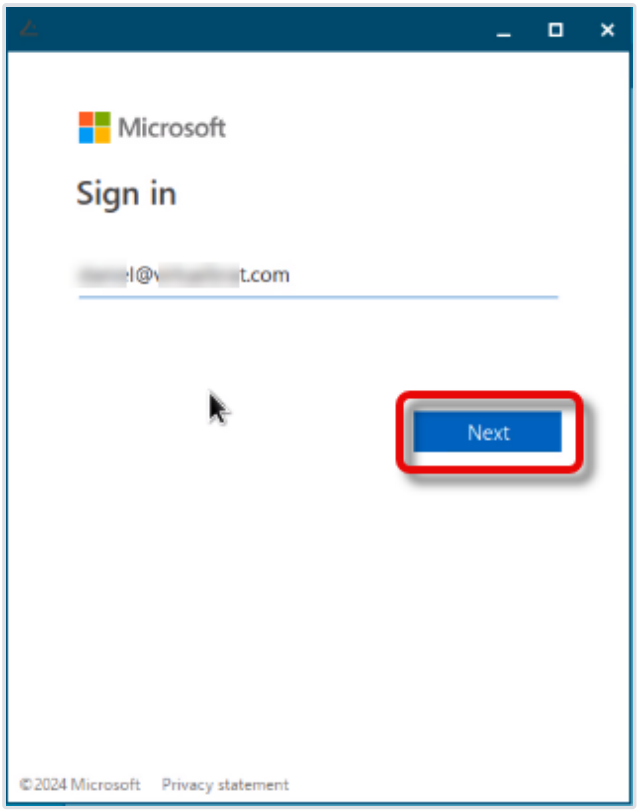


5. Start the Microsoft Intune app on your device.

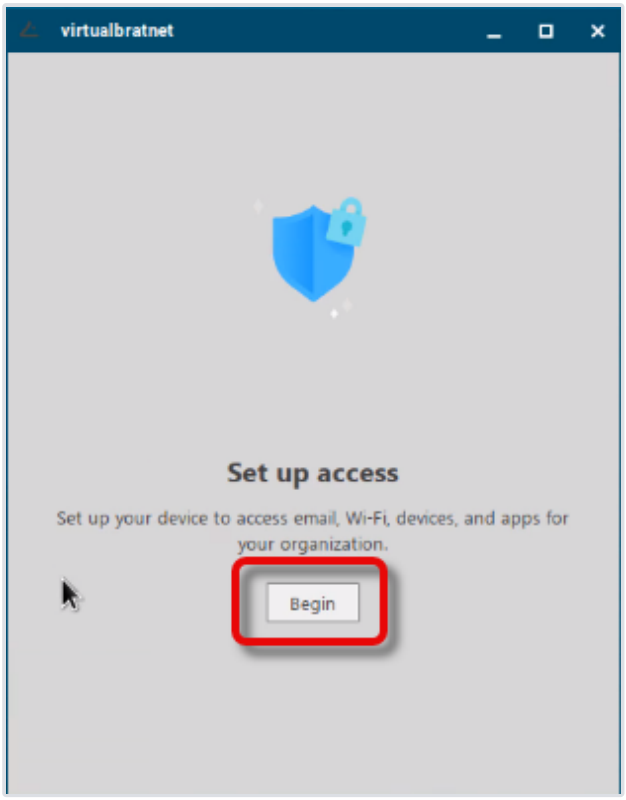
6. In the start dialog, click **Sign in**.



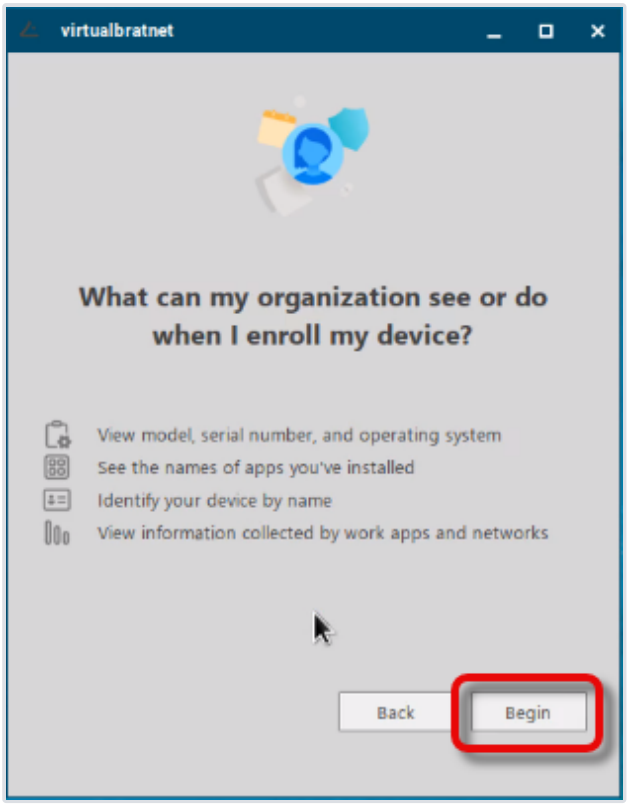
7. Enter the credentials for your organization.



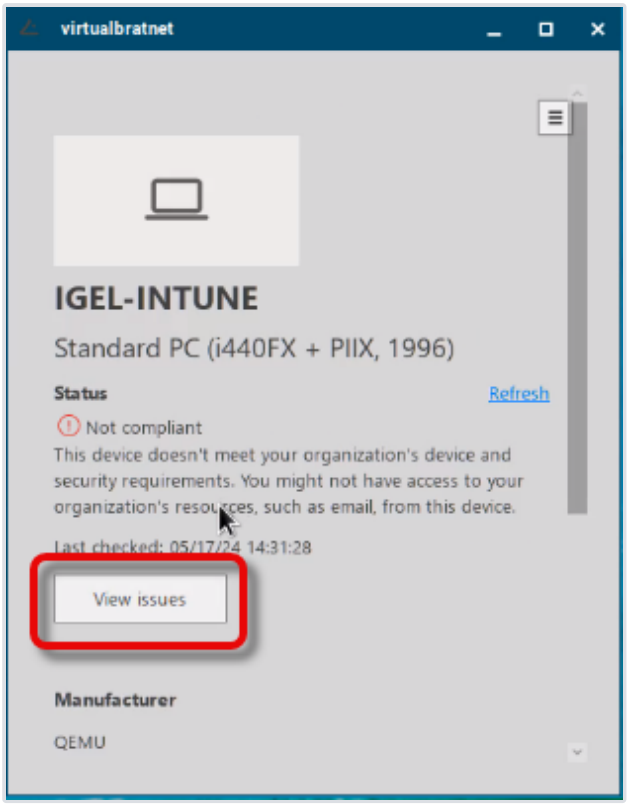
8. In the dialog **Set up access**, click **Begin**.



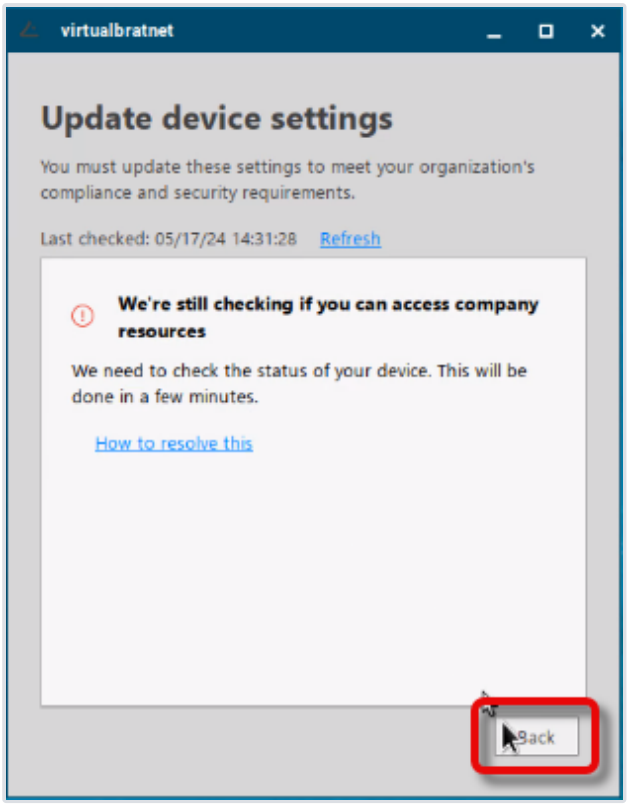
9. Review the information your device will expose to Microsoft Intune, and click **Begin**.

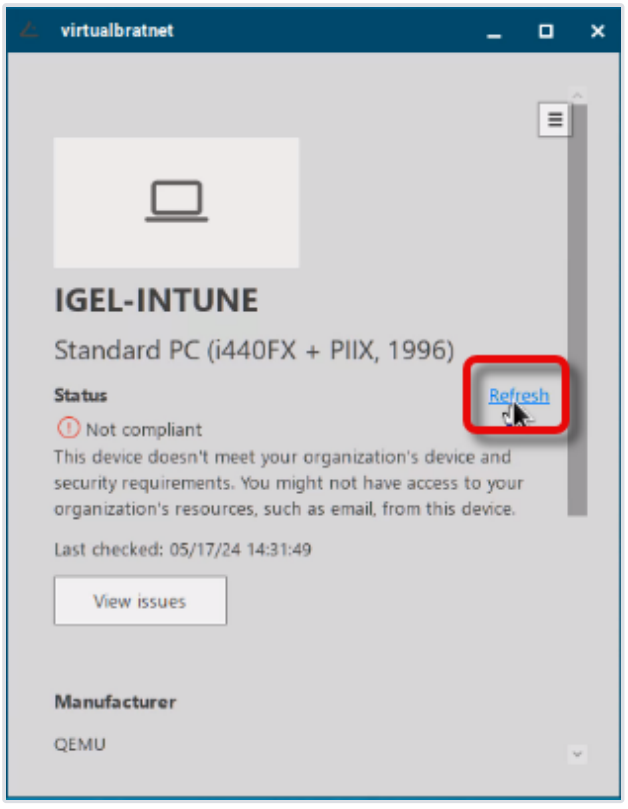


10. If the compliance check by Intune has a negative result, click **View issues**.

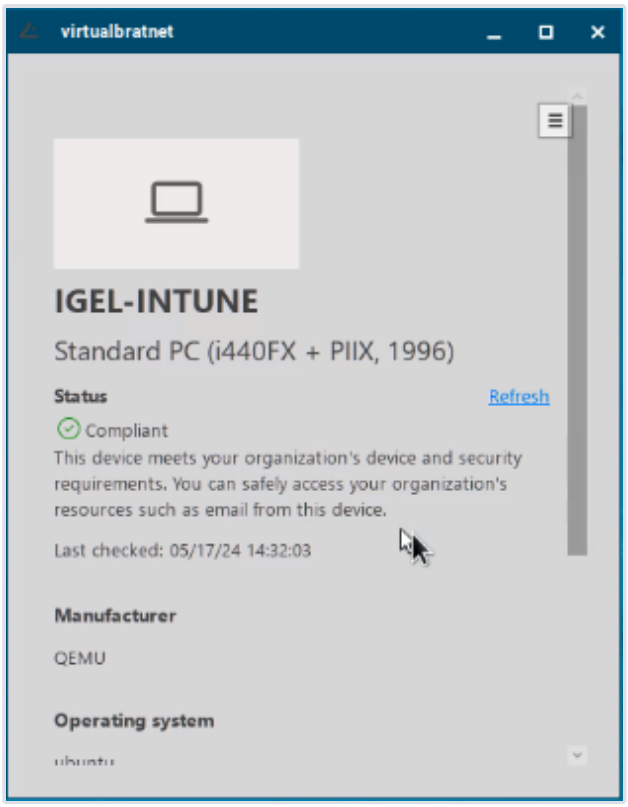


11. Review the information; if the check is still ongoing, click **Back**. and refresh the screen.


virtualbratnet
Update device settings
You must update these settings to meet your organization's compliance and security requirements.
Last checked: 05/17/24 14:31:28 Refresh
We're still checking if you can access company resources
We need to check the status of your device. This will be done in a few minutes.
How to resolve this
Back

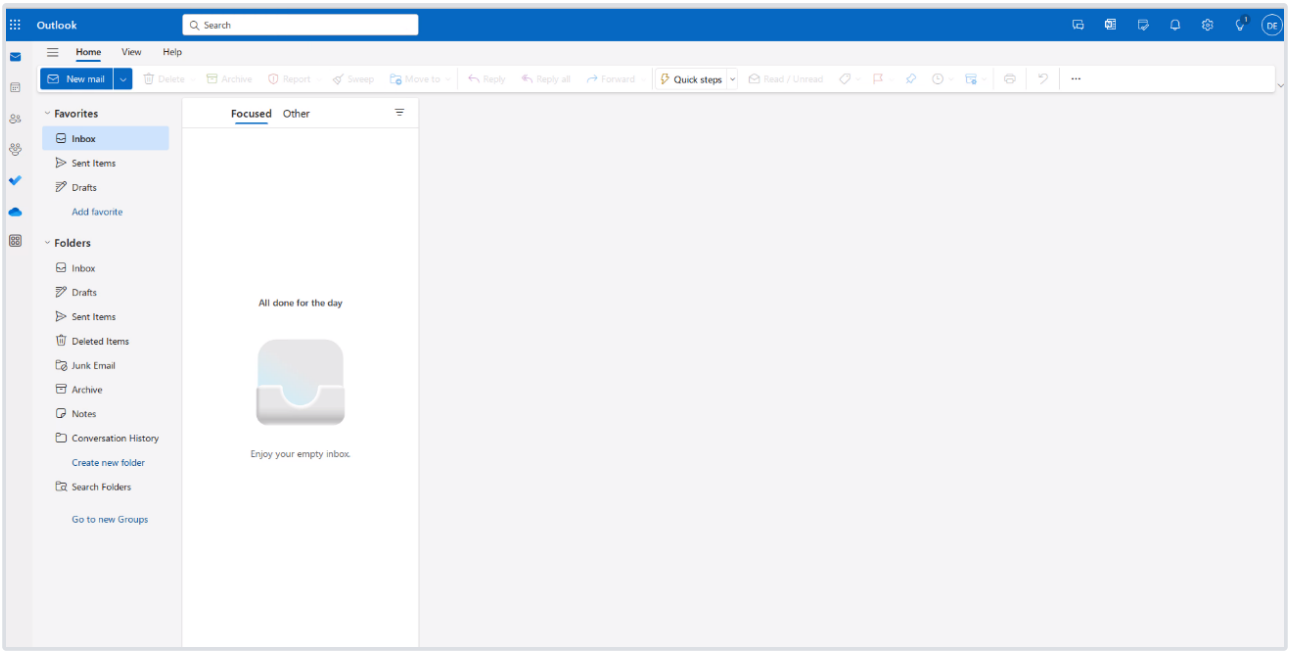

virtualbratnet
IGEL-INTUNE
Standard PC (i440FX + PIIX, 1996)
Status
Refresh
Not compliant
This device doesn't meet your organization's device and security requirements. You might not have access to your organization's resources, such as email, from this device.
Last checked: 05/17/24 14:31:49
View issues
Manufacturer
QEMU

If everything goes well, the device is eventually found to be compliant.



12. Open Microsoft Edge and go to Microsoft Outlook again.

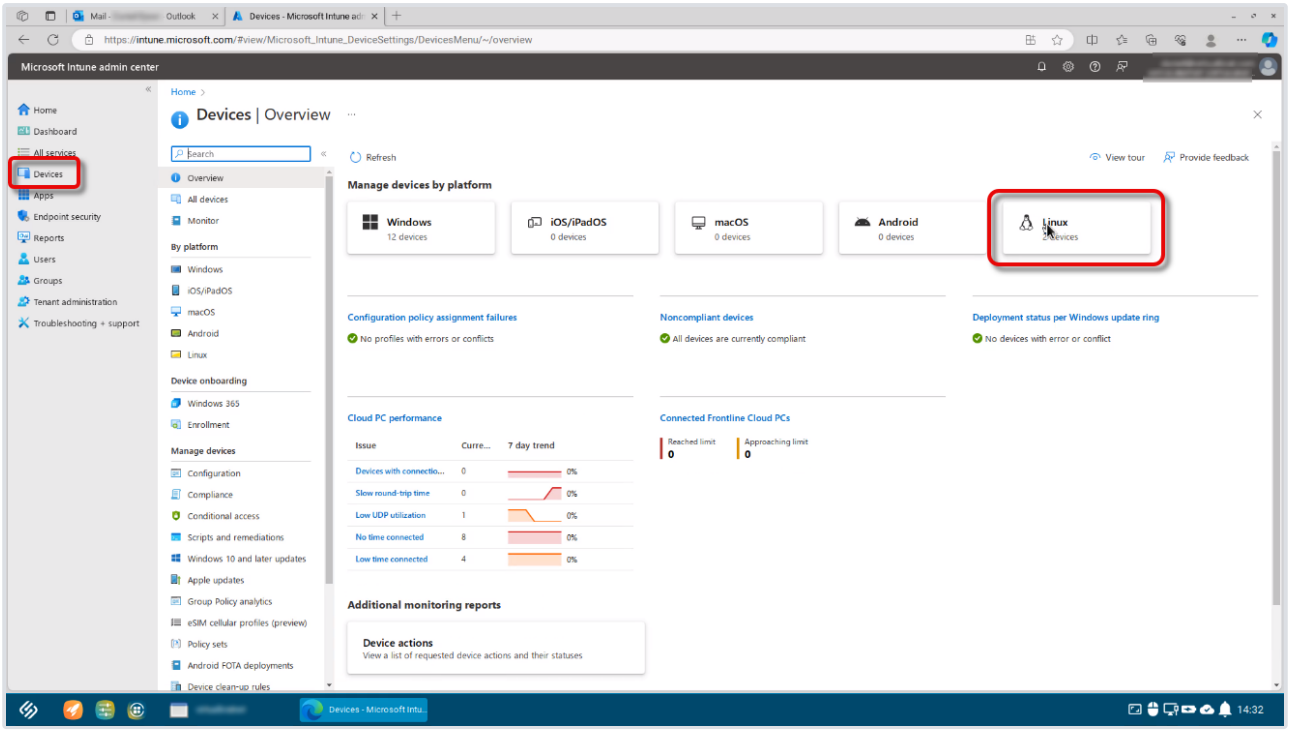
The browser content should look something like this:



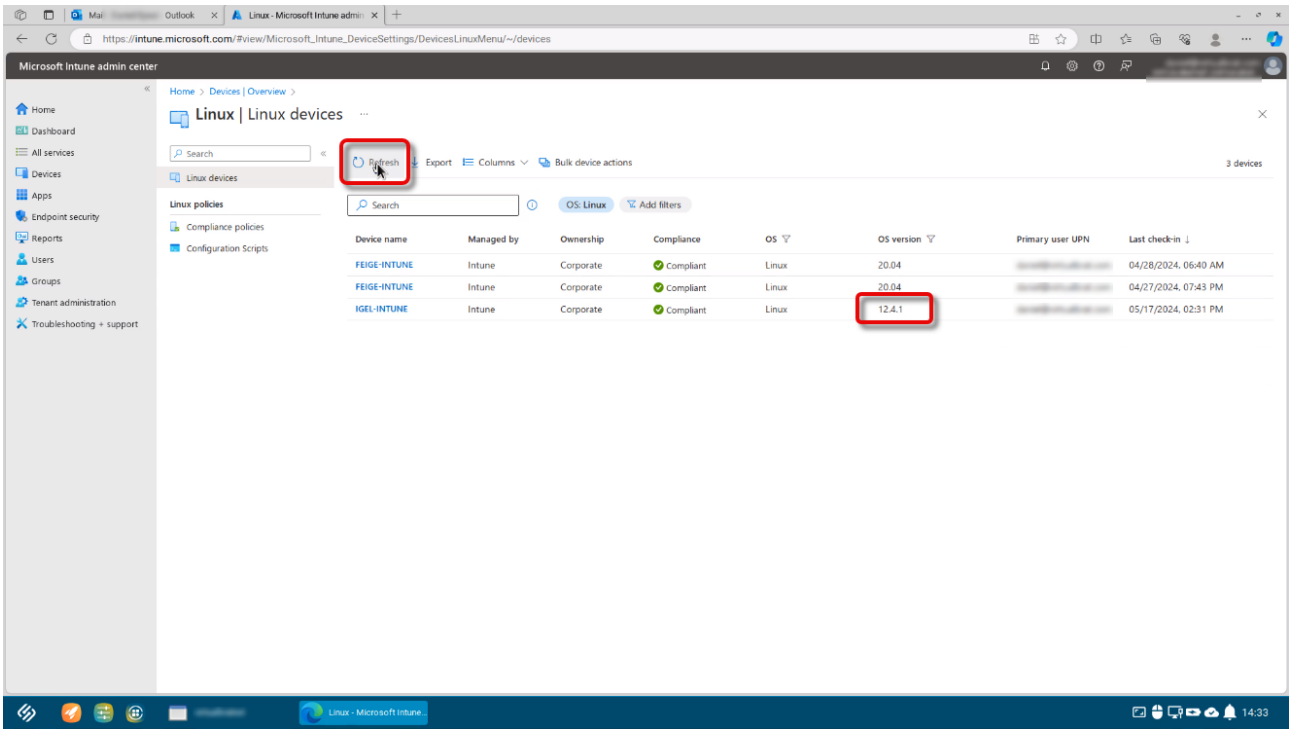
Getting Started with Device Administration with Microsoft Intune

1. Open Microsoft Edge and go to `https://intune.microsoft.com`

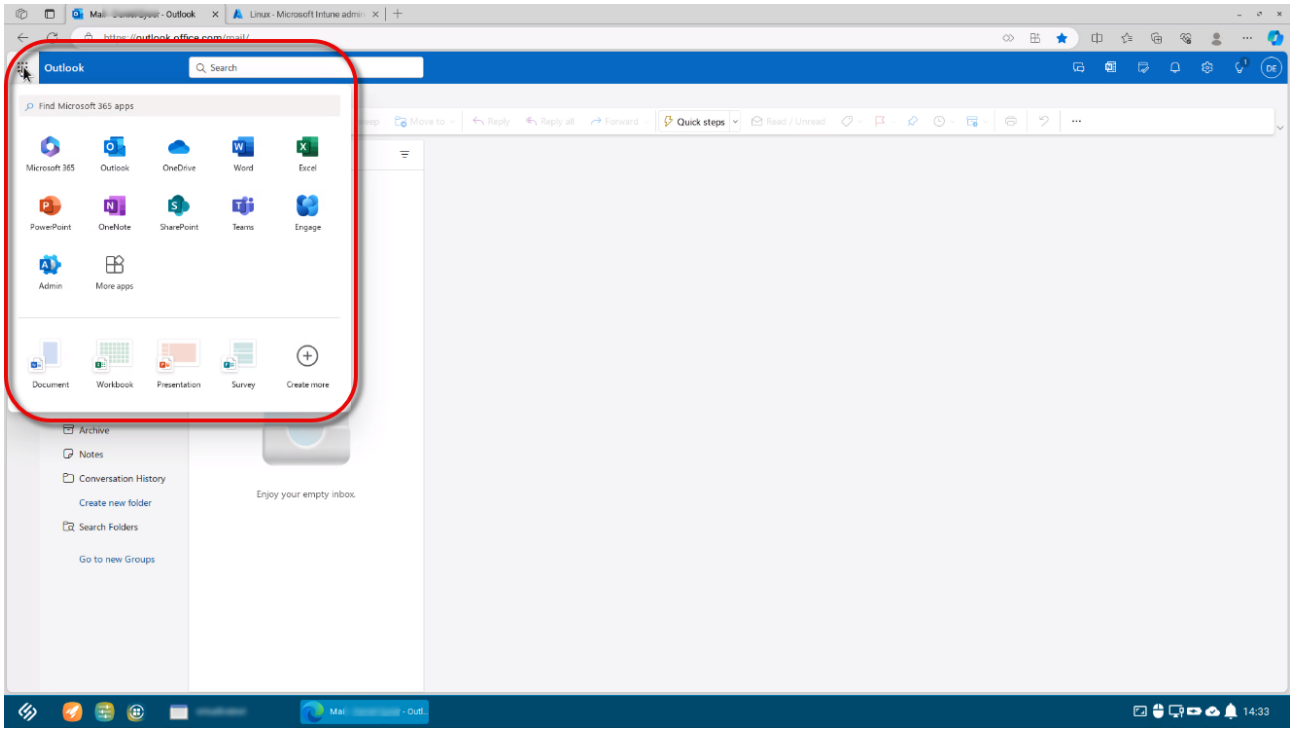
2. Go to **Devices** and then select **Linux**.



3. Check if your new device is displayed; if not, click **Refresh**. You can recognize it by the IGEL OS version number.



When your device has been integrated successfully with Microsoft Intune, you can use all the apps provided by Microsoft 365.



Media Player (Parole)

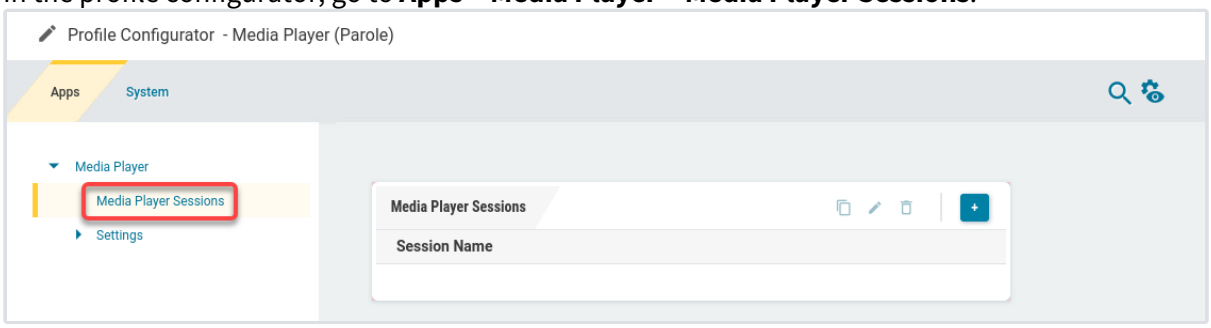


- Getting Started with the Media Player (Parole) on IGEL OS (see page 422)
- Configuring the Media Player (Parole) on IGEL OS (see page 424)
- Supported Formats and Codecs of the Media Player (Parole) Application in IGEL OS (see page 430)

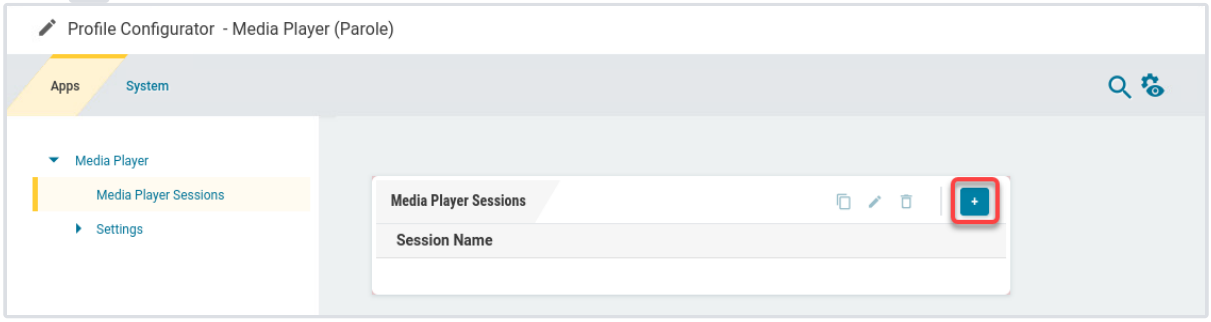
Getting Started with the Media Player (Parole) on IGEL OS

How to Create a Session

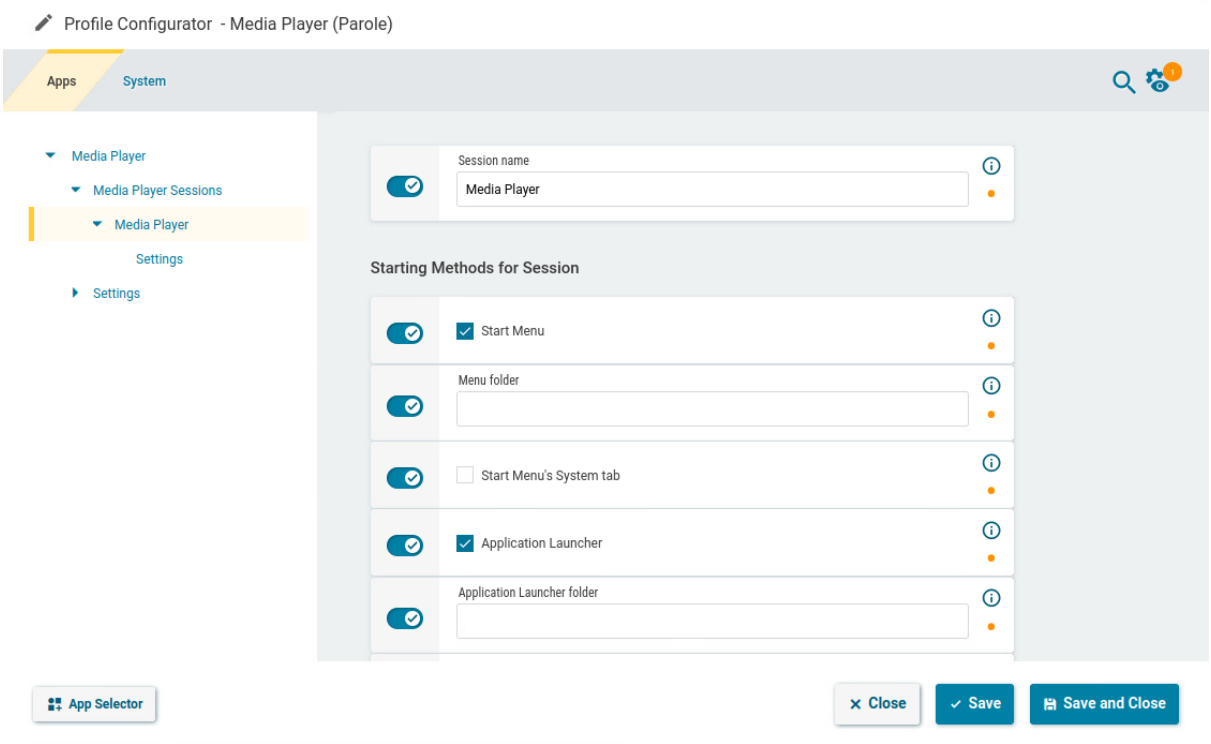
1. In the profile configurator, go to **Apps > Media Player > Media Player Sessions**.



2. Click + .



The session is created.

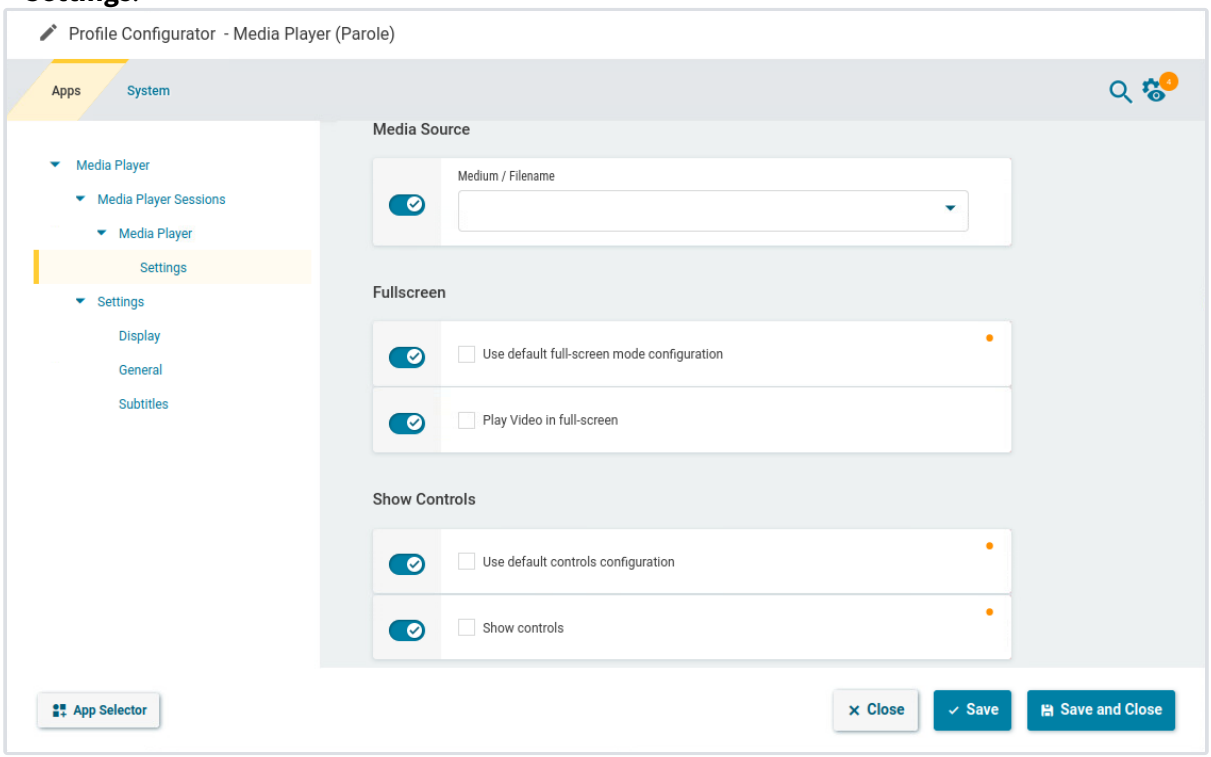


3. Edit the settings according to your needs; for details, see *IGEL Apps* > *Media Player (Parole)* > *Configuring the Media Player (Parole) on IGEL OS*

Configuring the Media Player (Parole) on IGEL OS

Configuring the Session-Specific Settings

1. In the profile configurator, go to **Apps > Media Player > Media Player Sessions > [session name] > Settings**.



2. Edit the settings according to your needs. The parameters are described in the following.

Medium / filename

Path to the audio data or video data that are to be played back when the media player session starts. This can be a local path or a URL.

Use default fullscreen mode configuration

- ☑ The global setting **Apps > Media Player > Settings > Display > Full-screen** will be used. (Default)
- ☐ The session-specific setting **Play video in full-screen** will be used.

Play video in full-screen

Only available if **Use default fullscreen mode configuration** is deactivated.

- ☑ The video will be shown in full-screen mode.
- ☐ The video will be shown in a standard window. (Default)

Use default controls configuration

- ☑ The global setting **Apps > Media Player > Settings > Display > Show controls** will be used. (Default)
- ☐ The session-specific setting **Show controls** will be used.

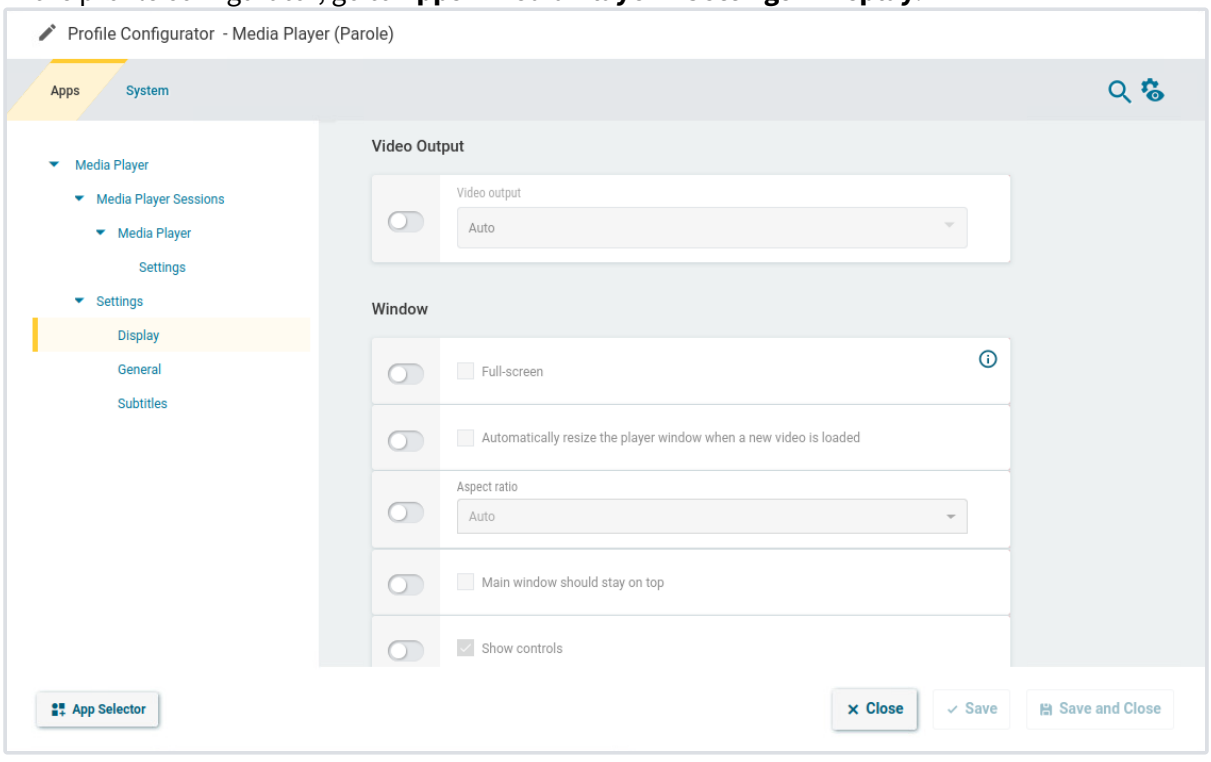
Show controls

Only available if **Use default controls configuration** is deactivated.

- ☑ The media player's controls will be shown. (Default)
- ☐ The media player's controls will not be shown; only the playback window is visible.

Configuring the Display (Global)

1. In the profile configurator, go to **Apps > Media Player > Settings > Display**.



2. Edit the settings according to your needs. The parameters are described in the following.

Video output

Specifies the video output method.

Possible options:

- **Auto**: The video output method will be set depending on availability. (Default)
  The other options will be queried in the given order: If available, hardware acceleration will be used. If hardware acceleration is not available but the X video extension is, the X video extension will be used.
- **Hardware accelerated**: Hardware acceleration will be used.
- **X video extension**: The images will be written to the graphics card memory using *shared memory*. Hardware acceleration will be used.
- **X Window System**: Video will be output via the X11 protocol. Hardware acceleration will not be used.

Full-screen

- ☑ The media player will be shown in full-screen mode.
- ☐ The media player will be shown in a standard window. (Default)

Automatically resize the player window when a new video is loaded

- ☑ The window size will adapt to the video being played.
- ☐ The window size will not change. (Default)

Aspect ratio

Aspect ratio for video playback

Possible values:

- **Auto**: The aspect ratio of the playback window will adapt to the video being played.
- **Square**
- **4:3 (TV)**
- **16:9 (widescreen)**
- **2.11:1 (DVB)**

Main window should stay on top

- ☑ The media player window will always remain in the foreground. Other windows cannot be placed on top of the media player window.
- ☐ The media player window will behave like a standard window. Other windows can be placed on top of the media player window. (Default)

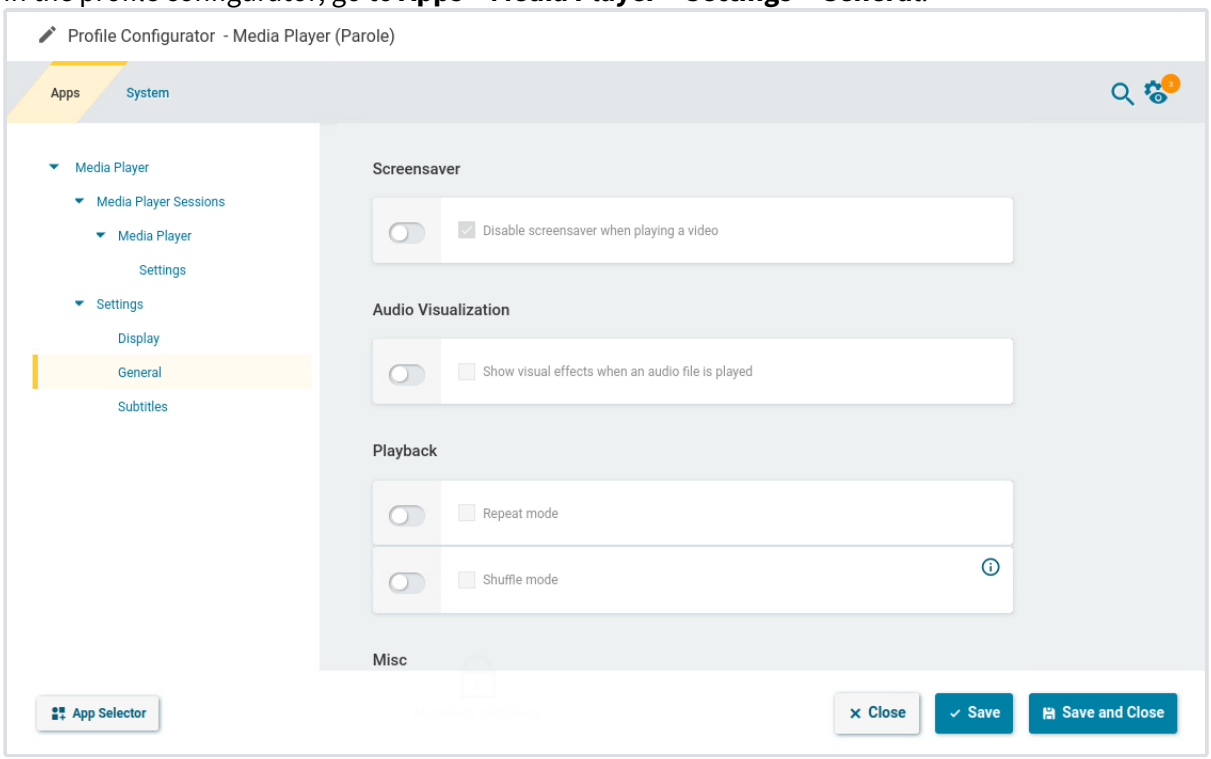
Show controls

- ☑ The media player's controls will be shown. (Default)

- [ ] The media player's controls will not be shown; only the playback window is visible.

Configuring General Playback Settings (Global)

1. In the profile configurator, go to **Apps > Media Player > Settings > General**.



2. Edit the settings according to your needs. The parameters are described in the following.

Disable screensaver when playing a video

- [x] As long as a video is played, the screensaver will not be started. (Default)
- [ ] The screensaver will start after the configured idle time, even when a video is played,

Show visual effects when an audio file is played

- [x] Visual effects will be shown when playing back audio data.
- [ ] No visual effects will be shown. (Default)

Repeat mode

- [x] The playlist will be repeated until the user stops the playback.
- [ ] The playlist will be played back once only. (Default)

Shuffle mode

- ☑ The playlist will be played back in random order.
- ☐ The playlist will be played back in the set order. (Default)

Network connection speed

Possible values:

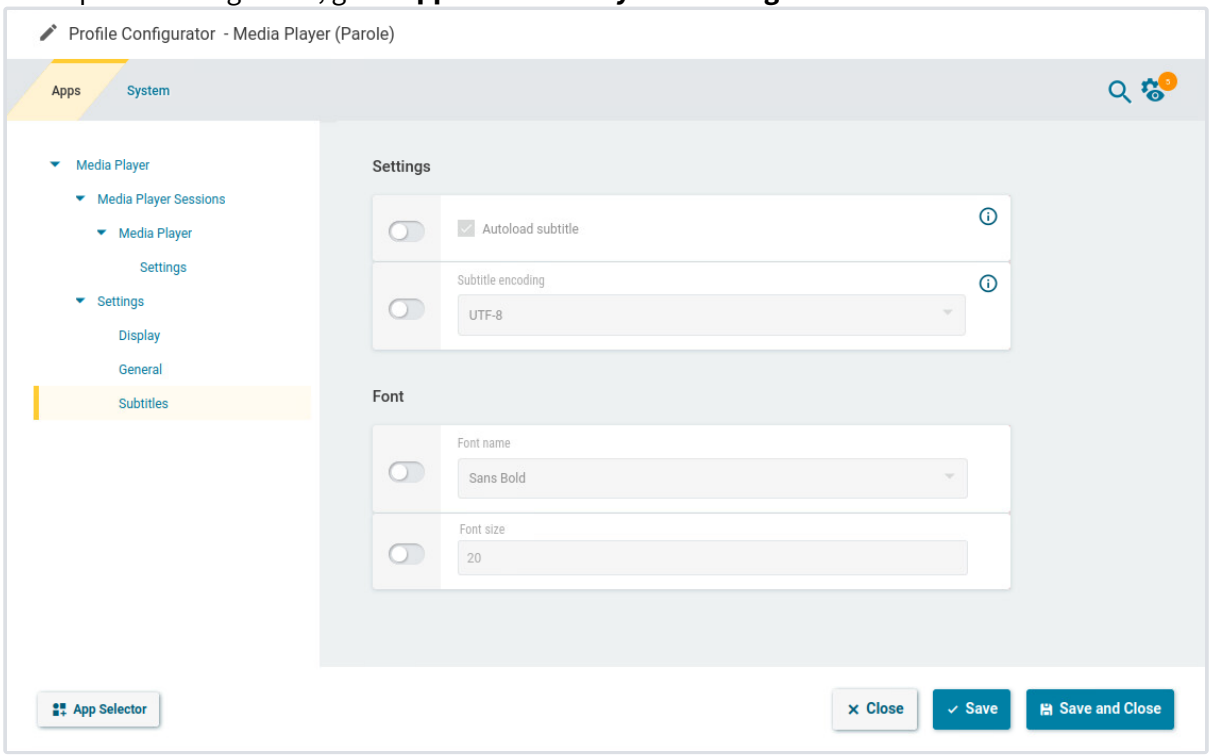
- **56 kBps modem/ISDN**
- **112 kBps dual ISDN/DSL**
- **256 kBps DSL/cable**
- **384 kBps DSL/cable**
- **512 kBps DSL/cable**
- **1.5 MBps T1/Intranet/LAN** (default)
- **Intranet/LAN**

Default location for the "Open..." dialogs

Defines the file location that is preset in the **Open...** dialog. Default: `/userhome`

Configuring the Subtitles

1. In the profile configurator, go to **Apps > Media Player > Settings > Subtitles**.



2. Edit the settings according to your needs. The parameters are described in the following.

Autoload subtitle

- ☑ Subtitles contained in the video will be shown. (Default)
- ☐ Subtitles contained in the video will only be shown if the user has enabled them via **Video > Subtitles**.

Subtitle encoding

Character coding for the subtitles. The value is set to UTF-8.

Font name

The font that is used for the subtitles.

Possible values:

- **Sans**
- **Sans Bold** (default)
- **Serif**
- **Serif Bold**

Font size

Size of the font that is used for the subtitles. (Default: 20)

Supported Formats and Codecs of the Media Player (Parole) Application in IGEL OS

The IGEL OS 12 Media Player application supports the following multimedia formats and codecs.

Supported Formats

- AVI
- MPEG
- ASF (restricted under Linux)
- WMA
- WMV (restricted under Linux)
- MP3
- OGG
- WAV
- FLAC

Supported Codecs

- MP3
- AAC
- WMA stereo
- WMV 7/8/9
- MPEG 1/2
- MPEG4
- H.264
- Ogg/Vorbis
- Ogg/Theora

Omnissa Workspace ONE Intelligent Hub



This article describes how you can enroll IGEL OS device with Omnissa Workspace ONE Intelligent Hub. Workspace ONE Intelligent Hub is a platform that allows you to unify device management, app management, etc. For more information, see https://www.omnissa.com/products/workspace-one-intelligent-hub/ and https://www.igel.com/blog/how-igel-and-omnissa-deliver-secure-and-efficient-user-desktop-and-application-solutions/.

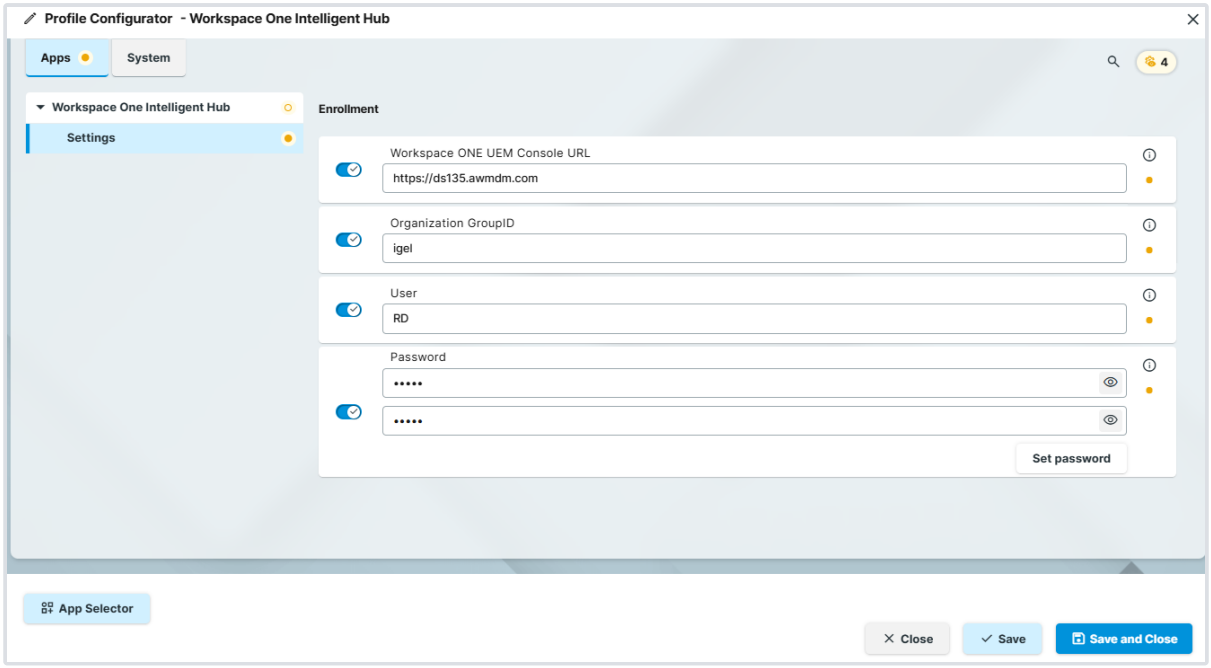
Requirements

- A user is created in your Workspace ONE Unified Endpoint Management (UEM) console.
- Workspace ONE Intelligent Hub app is imported to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[169].

How to Configure Workspace ONE Intelligent Hub to Enroll the IGEL OS Device

1. In the IGEL UMS, create a profile configuring Workspace ONE Intelligent Hub app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[170].
2. In the profile configurator, go to **Apps > Workspace One Intelligent Hub > Settings**.
3. Configure the following settings:

169. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
170. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



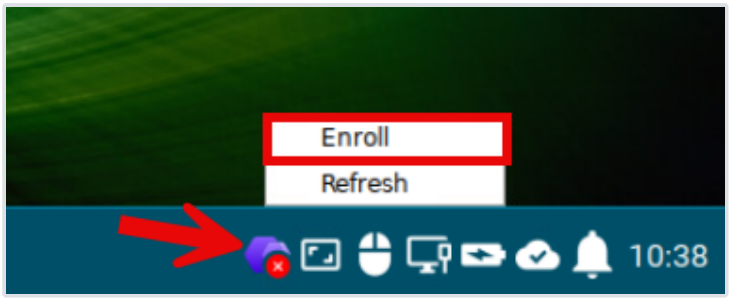
Workspace ONE UEM Console URL
The URL of your Workspace ONE UEM console to which the IGEL OS device has to be enrolled. This is usually not the URL of the UEM console itself but the device services URL. Example: `https://ds135.awmdm.com`

Organization GroupID
Organization GroupID created in the UEM console and to which the device must be enrolled. If left empty, the user will be requested to specify it in the enrollment dialog.

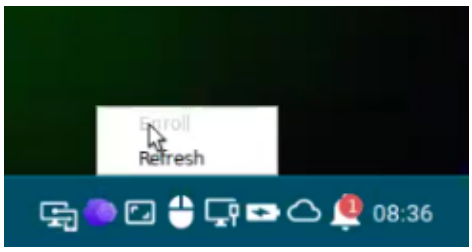
User
User name created in the UEM console. If left empty, the user will be requested to specify it in the enrollment dialog.

Password
Password for the user created in the UEM console. Repeat the password entry and click **Set password**. If left empty, the user will be requested to specify it in the enrollment dialog.

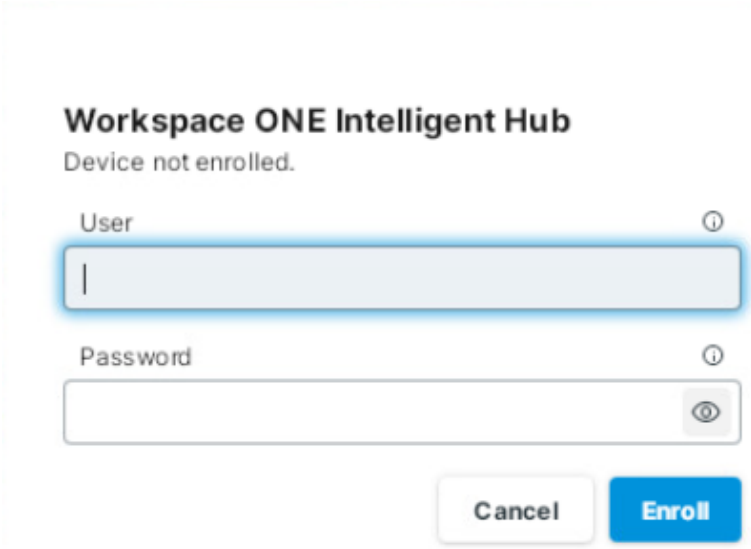
4. Assign the profile and, in case of the explicit app assignment, the app to the required devices.
5. After the app is installed on the device, navigate to the corresponding system tray icon and select **Enroll**.



The device will automatically be enrolled and the user will see the corresponding notification. As soon as the device is enrolled, the status will be updated and the **Enroll** option will be disabled:



If any of the above mentioned settings were not defined, the user has to specify them in the enrollment dialog first, e.g.



Device Unenrollment
To unenroll the device from the Workspace ONE Intelligent Hub, run the following command as root:
`ws1HubUtil unenroll`
For this purpose, you can use the terminal or configure a custom command (see (12.6.1-en) Custom CronJob/Systemd Timer in IGEL OS 12 or (12.6.1-en) Custom Commands in IGEL OS 12).

For more details, see https://docs.omnissa.com/de-DE/bundle/LinuxDeviceManagementVSaaS/page/Command-lineUtilitiesforWorkspaceONEIntelligentHubonLinux.html.
Note: After the unenrollment, it can take up to 1 minute to update the enrollment status automatically. Click **Refresh** in the system tray app to instantly update the status.

What is Currently Not Supported?

- Device details: Security options like encryption and firewall status detection. For more information on device details in the Workspace ONE UEM console, see Linux Device Details[171].
- Device details: Apps
- Device details: Custom configuration profiles, see https://docs.omnissa.com/de-DE/bundle/LinuxDeviceManagementVSaaS/page/LinuxProfiles.html
- Device details: Sensors
- Command-line utilities: `ws1HubUtil upgrade`

171. https://docs.omnissa.com/de-DE/bundle/LinuxDeviceManagementVSaaS/page/LinuxDeviceDetailsPage.html

Omnissa Horizon Client



For an overview of available features, see the vendor's article Horizon Client Feature Matrix for Horizon 8[172].

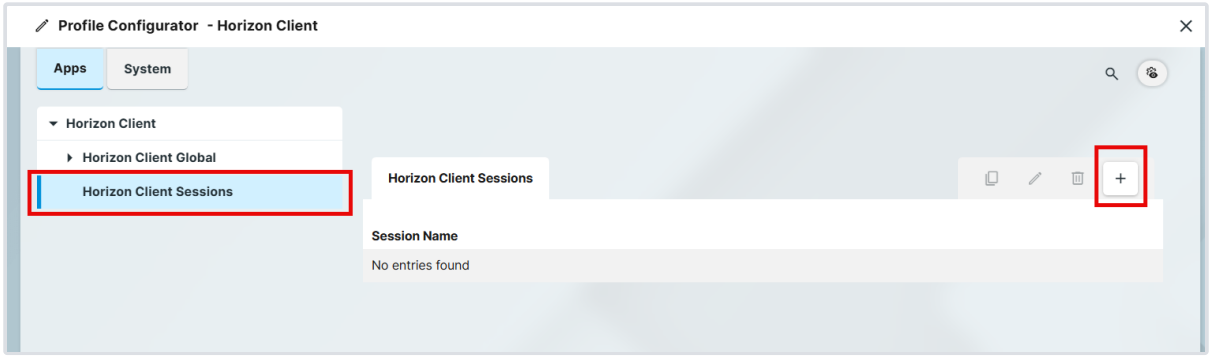
- Getting Started with the Omnissa Horizon Client on IGEL OS (see page 436)
- Configuring the Omnissa Horizon Client on IGEL OS (see page 438)
- Troubleshooting Topaz USB Not Passed through to Omnissa Horizon on IGEL OS (see page 469)

172. https://kb.omnissa.com/s/article/80386

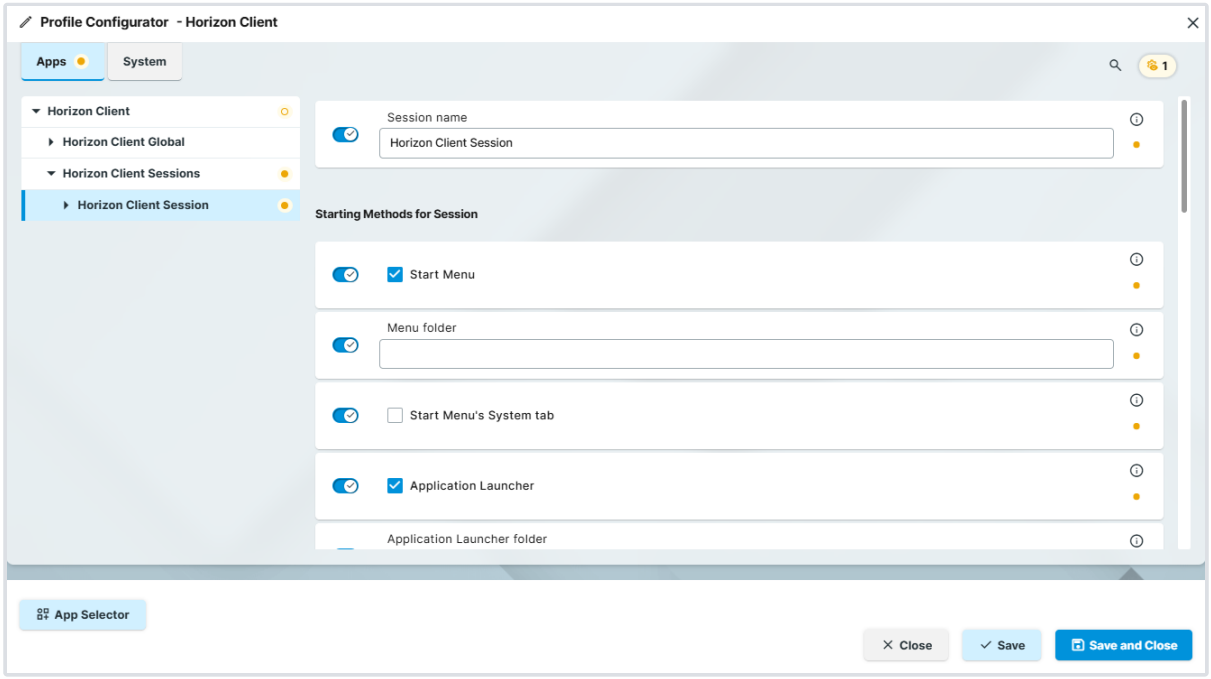
Getting Started with the Omnissa Horizon Client on IGEL OS

How to Create a Session

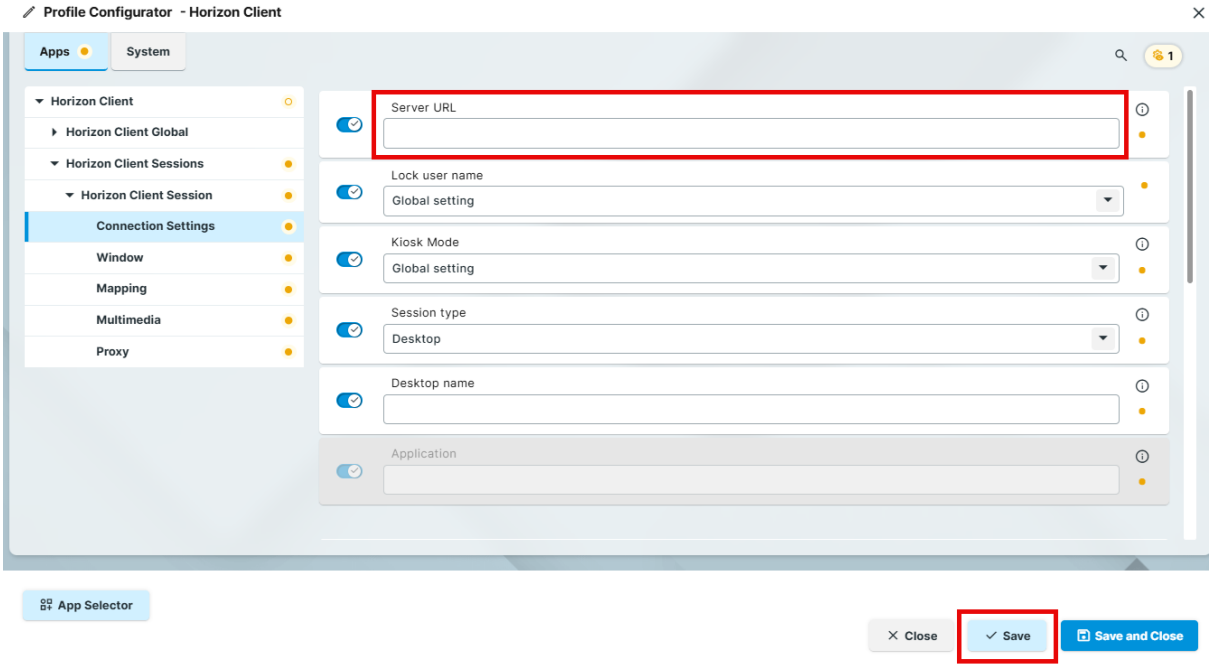
1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions** and click +.



The session is created.



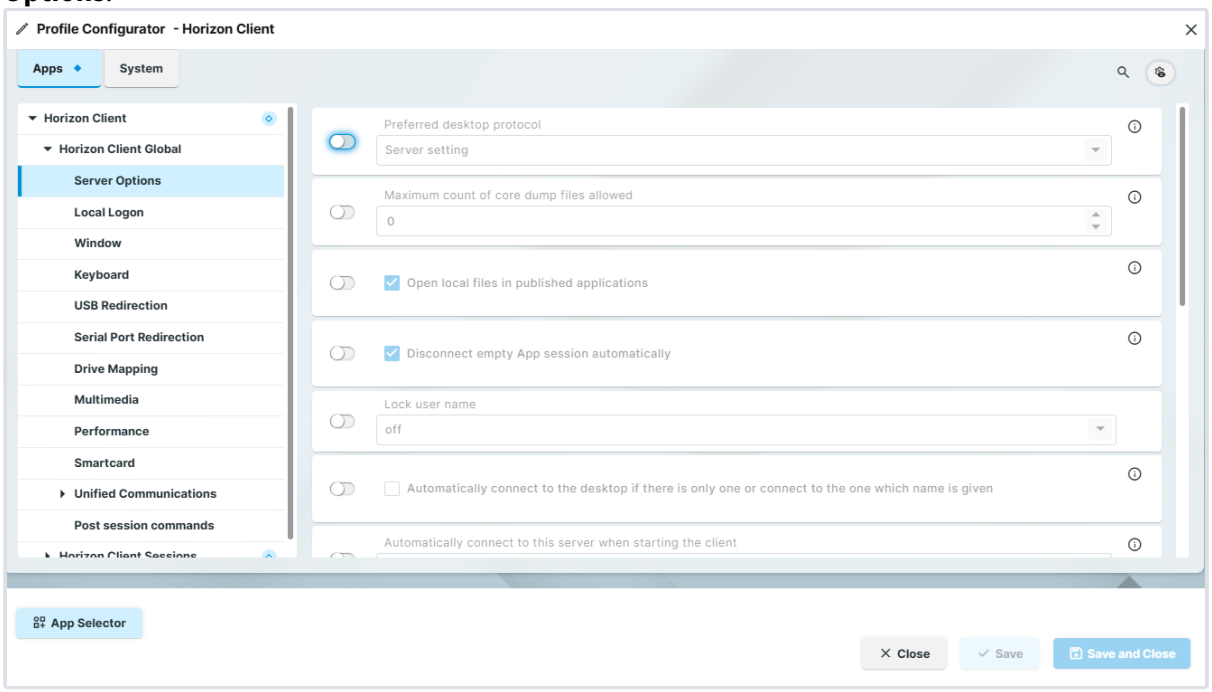
2. Under **Connection Settings**, specify the **Server URL** and then save the settings.


Profile Configurator - Horizon Client
Apps
System
Horizon Client
Horizon Client Global
Horizon Client Sessions
Horizon Client Session
Connection Settings
Window
Mapping
Multimedia
Proxy
Server URL
Lock user name
Global setting
Kiosk Mode
Global setting
Session type
Desktop
Desktop name
Application
App Selector
Close
Save
Save and Close

Configuring the Omnissa Horizon Client on IGEL OS

Configuring Server Options (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Server Options**.



2. Edit the settings according to your needs. The parameters are described in the following.

Preferred desktop protocol

The selected option is preferred by the client when negotiating the connection protocol. If the server does not accept the connection protocol preferred by the client, the connection protocol preferred by the server will be used.

Possible values:

- **Server setting**: The client does not provide the server details of a preferred connection protocol. The connection protocol preferred by the server is used. (Default)
- **PCoIP**: The client tells the server that it prefers PCoIP as the connection protocol.
- **Omnissa Blast**: The client tells the server that it prefers Omnissa Blast as the connection protocol.

Hardware video acceleration can be used for Omnissa Blast. Whether hardware video acceleration can be used or not is dependent on the device's hardware. If no hardware video acceleration is available, rendering will take place via software, without acceleration.

Maximum count of core dump files allowed

Specifies the maximum number of core dump files allowed for Horizon Client processes. (Default: 0)

Open local files in published applications

- [x] Users can open local files in Windows-based published applications directly from the local file system. (Default)
- [ ] Users cannot open local files in published applications.

Disconnect empty App session automatically

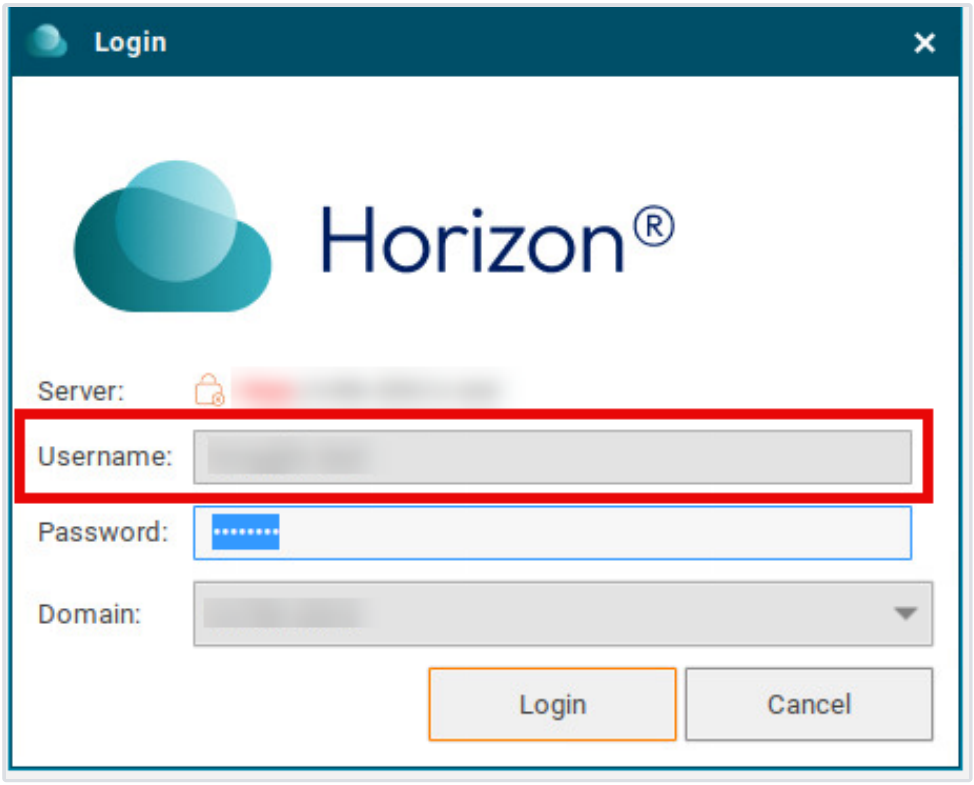
- [x] If the app session becomes empty because the user closes all applications, the session is automatically disconnected. (Default)
- [ ] If the app session becomes empty because the user closes all applications, the session remains open.

Lock user name

Locks the user name specified under **Apps > Horizon Client > Horizon Client Session > [session name] > Connection Settings > User name**.

Possible values:

- **on**: The user name will be locked and cannot be changed in the login window.
- **off**: The user name will not be locked in the login window. (Default)



Automatically connect to the desktop if there is only one or connect to the one which name is given

Automatically connects to the desktop if there is only one entitled desktop on the server or to the desktop specified under **Apps > Horizon Client > Horizon Client Session > [session name] > Connection Settings > Desktop name**.

- ☑ Automatic connection is allowed.
- ☐ Automatic connection is not allowed. (Default)

Automatically connect to this server when starting the client

Automatically connects to the specified server when Horizon Client is started.

Client behavior when all Sessions have been disconnected

Customizes the client behavior when all sessions are disconnected.

Possible values:

- **Unconfigured**: The setting is not configured. (Default)
- **Quit client**: The client will quit when all sessions are disconnected.
- **Logoff from server**: The client will log off from the server when all sessions are disconnected.
- **Keep current state**: The client will remain in its current state when all sessions are disconnected.

Auto-connect to remote desktop or published app in case there's only one of them

If there is only one entitled remote desktop or published application, the Horizon Client will automatically connect to that desktop or application after the user authenticates to the server.

- ☑ Automatic connection is allowed.
- ☐ Automatic connection is not allowed. (Default)

High Color Accuracy Mode

Enables H.264 encoding with high color accuracy in Omnissa Blast sessions. The Horizon Client uses high color accuracy only if the agent supports it.

> On mobile devices that are running on battery, this feature might reduce battery life and performance.

- ☑ High color accuracy is allowed.
- ☐ High color accuracy is not allowed. (Default)

Server certificate verification mode

Specifies what will happen if server certificate verification fails.

Possible values:

- **Reject if verification fails**
- **Warn if verification fails** (default)
- **Allow unverifiable connections**

Action to take in case there are running applications from previous sessions

Specifies the start behavior of an **application**-type session if applications from a previous session are still running. The session type is defined under **Apps > Horizon Client > Horizon Client Sessions > [Session Name] > Connection Settings > Session Type**.

Possible values:

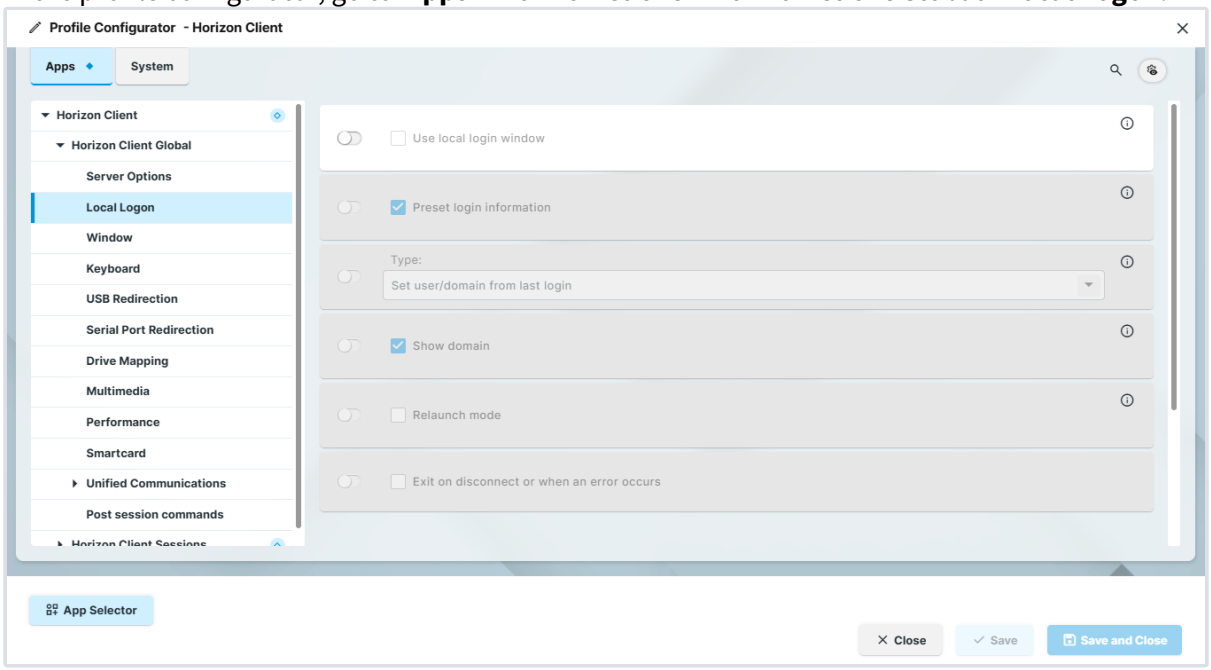
- **Ask to reconnect to open applications**: When the session starts, the user is asked whether they want to re-establish the connection. If the connection is reestablished, the applications running will be available. The applications will have the same status as when the connection was terminated. (Default)
- **Reconnect automatically to open applications**: The connection will be re-established automatically. The application running will be available. The application will have the same status as when the connection was terminated.
- **Do not ask to reconnect and do not reconnect**: The connection will not be re-established.

Kiosk mode

- ☑ Horizon client sessions are held in kiosk mode.
- ☐ Horizon client sessions are held in normal mode. (Default)

Configuring the Local Logon (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global> Local Logon**.



2. Edit the settings according to your needs. The parameters are described in the following.

Use local login window

- ☑ The local login window of the endpoint device will be used to log in to the server. If you use the local login window, you can prepopulate login information.
- ☐ The local login window will not be used. (Default)

Preset login information

Only available if **Use local login window** is enabled.

- ☑ Login information will appear automatically in the login window. With **Type**, you can specify the source of the login information. (Default)

Type

Only available if **Use local login window** is enabled.

- **Set user/domain from last login**: The login information from the last session will appear automatically in the login window. (Default)

- **Set user/domain from session setup**: Session-specific login information will appear automatically in the login window. The session-specific login information is described under **Connection Settings > [session name] > Connection Settings**.

Show domain

- ☑ The domain will be shown in the login window. (Default)

Relaunch mode

- ☑ The login window is shown in relaunch mode and cannot be closed.
- ☐ The login window is not shown in relaunch mode. (Default)

Exit on disconnect or when an error occurs

- ☑ The session will be ended completely when the connection is terminated.
- ☐ The connection overview will be shown when the connection is terminated. (Default)

Show domain

- ☑ The domain will be shown in the login window. (Default)

Relaunch mode

- ☑ The login window is shown in relaunch mode and cannot be closed.
- ☐ The login window is not shown in relaunch mode. (Default)

Exit on disconnect or when an error occurs

- ☑ The session will be ended completely when the connection is terminated.
- ☐ The connection overview will be shown when the connection is terminated. (Default)

Domain

Defines one or more domains under which the user can log in.

→ Click  to add a new domain.

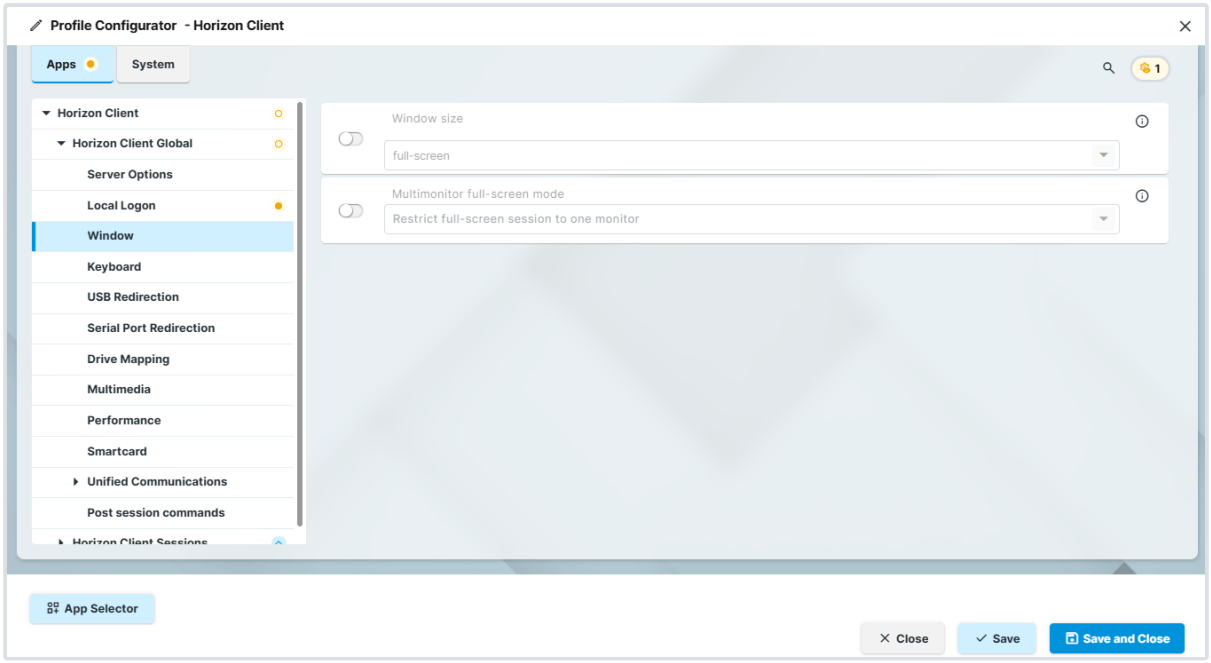
→ Click  to remove the selected domain.

→ Click  to edit the selected domain.

→ Click  to copy the selected domain.

Configuring the Window (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Window**.



2. Edit the settings according to your needs. The parameters are described in the following.

Window size

Specifies the width and height of the window.

Possible options:

- **full-screen**: The session is shown on the full screen. The device's taskbar is not visible. (Default)
- Numeric details, e.g. **1280x1024**: The session is shown in the selected resolution or on the selected percentage of the screen area.

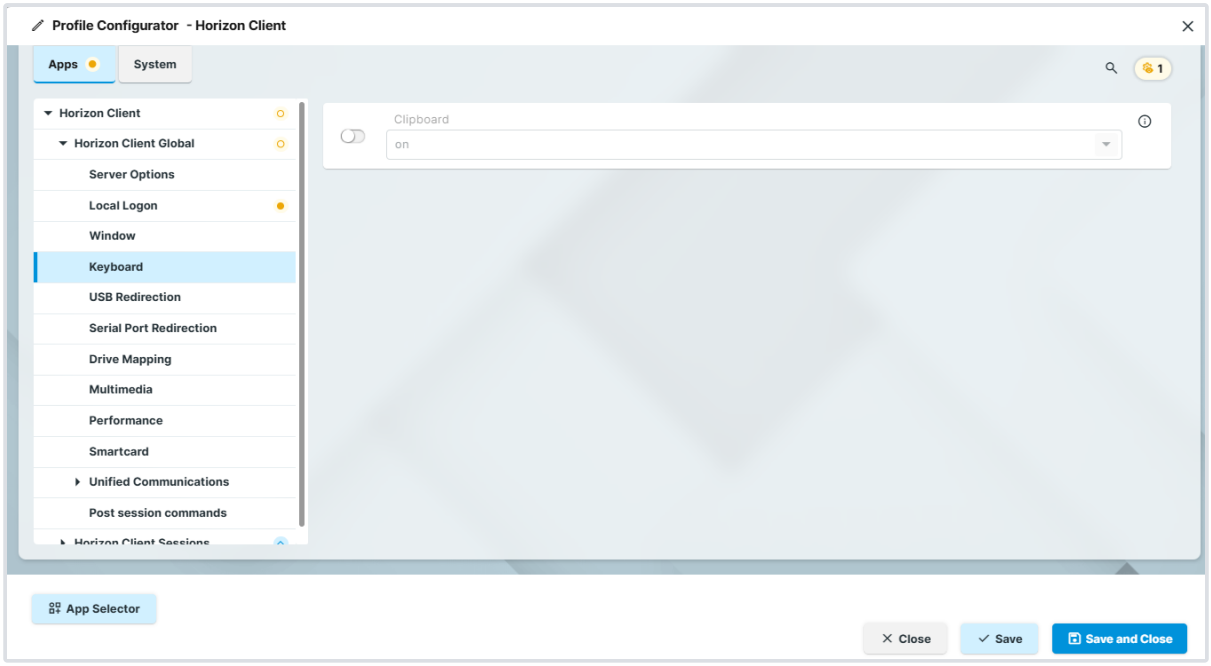
Multimonitor full-screen mode

Specifies how the session window is distributed across multiple screens.

- **Restrict full-screen session to one monitor** (Default)
- **Display full-screen session on all monitors**

Configuring the Keyboard Settings (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Keyboard**.



2. Edit the settings according to your needs. The parameters are described in the following.

Clipboard

Possible options:

- **on**: The clipboard of the device is redirected to the session.
- **off**: The clipboard is not redirected.

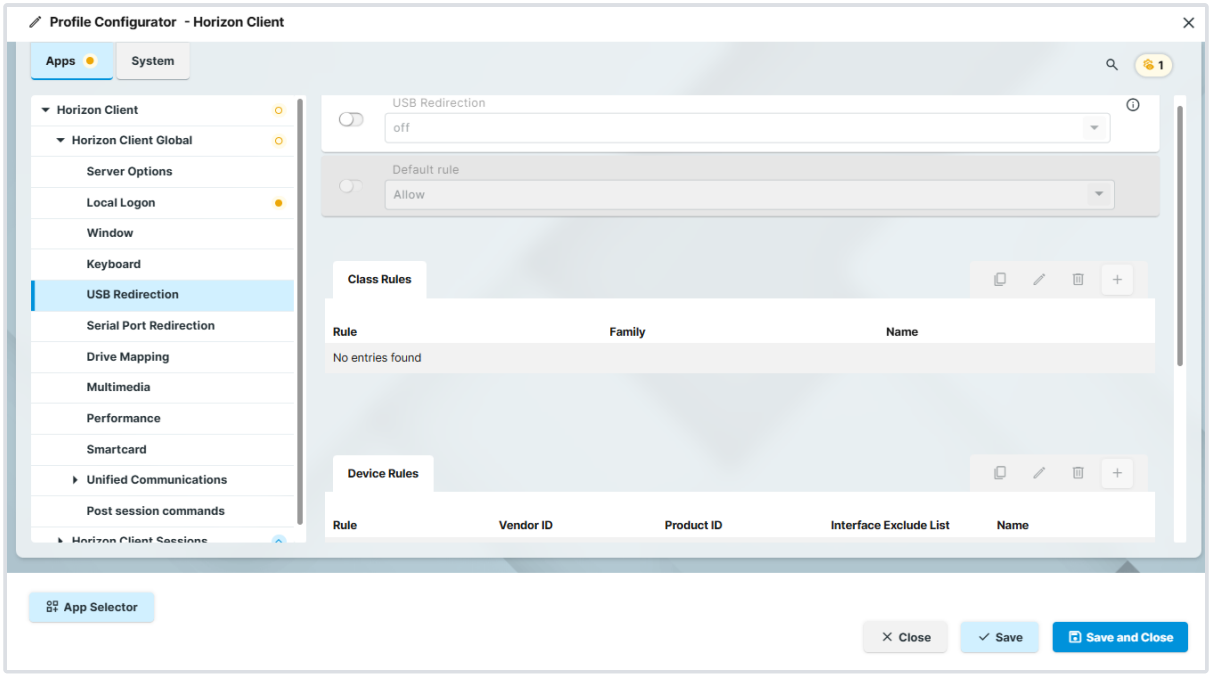
Configuring USB Redirection (Global)

You can enable and configure USB redirection for specific devices. A USB composite device can be split into its components (interfaces). Example: A USB dictation device that is split into the components loudspeaker, microphone, storage device/drive, and control buttons.

Ensure that the power supplied by the USB connection is adequate for the device.

If USB redirection is enabled, dynamic drive mapping should be disabled. Otherwise, USB redirection can cause a storage device to be removed from the drive mapping. This is the case if the **Automatically connect when inserted** option is enabled.

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > USB Redirection**.



2. Edit the settings according to your needs. The parameters are described in the following.

USB Redirection

- **on**: USB redirection is enabled,
- **off**: USB redirection is disabled (Default)

Default rule: This rule will apply if no special rule was configured for a class or a device.

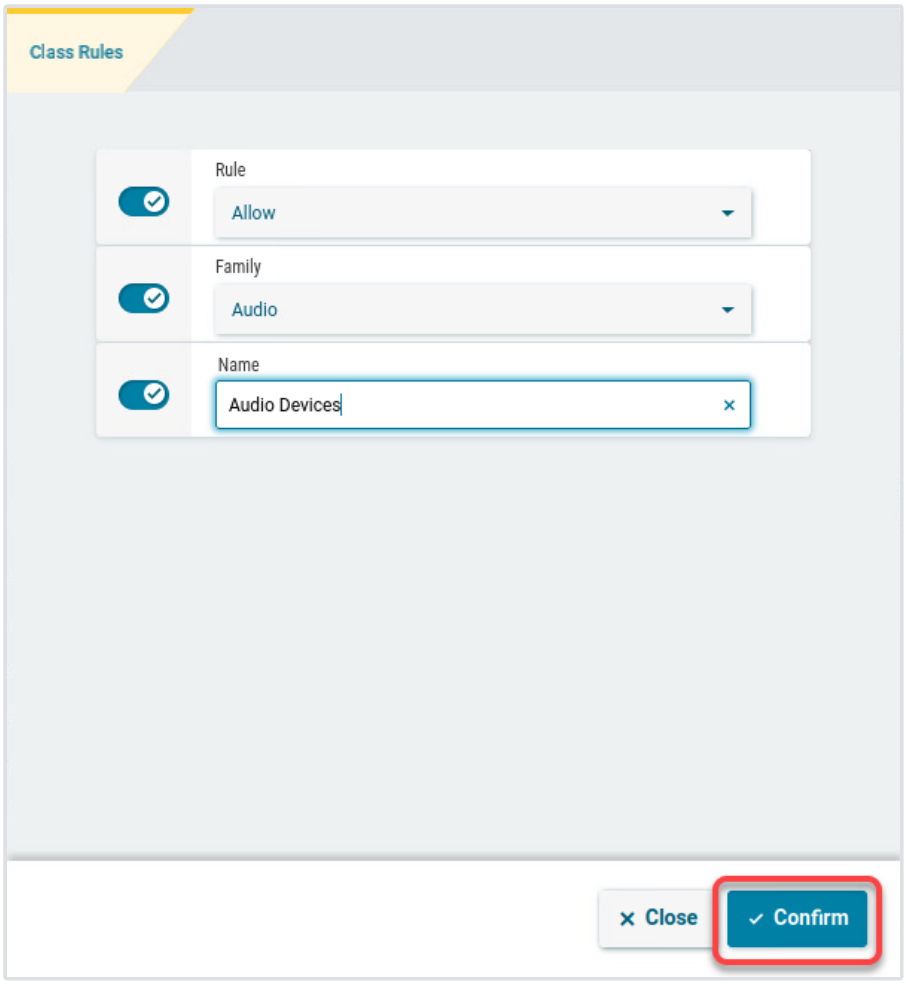
- **Allow**
- **Deny**

To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

Creating a Class Rule

1. To create a new rule, click + in the **Class Rules** area.
2. Choose a **Rule**. The rule specifies whether the use of the device class defined here is allowed or denied.
3. Under **Family**, select the class of device for which the rule should apply.
   Examples: **Audio**, **Printer**, **Smartcard**, **Storage Devices**.
4. Under **Name**, give a name for the rule.

5. Click on **Confirm**.



Creating a Device Rule

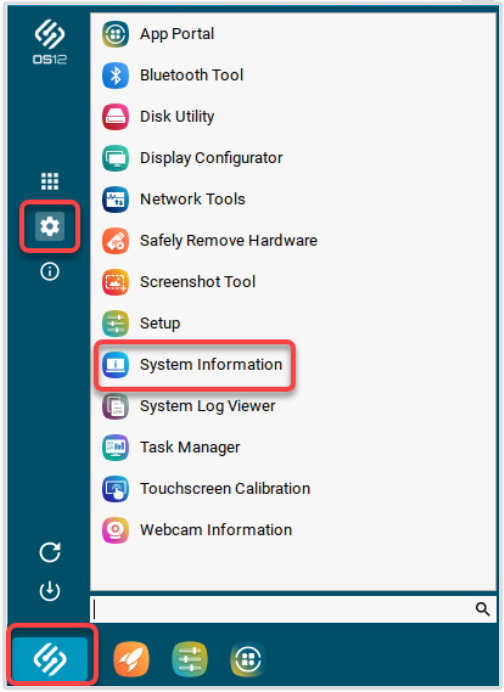
When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** must be given.

1. To create a new rule, click + in the **Device Rules** area.
2. Choose a **Rule**. The following rules are available:
   - **Deny**: The device will not be redirected via USB redirection.
   - **Allow**: The device will be redirected via USB redirection.
   - **Split**: A USB composite device will automatically be split into its individual components (interfaces).
   - **No auto-split**: A USB composite device will not be split.
3. Provide the **Vendor ID** of the device as a hexadecimal value.

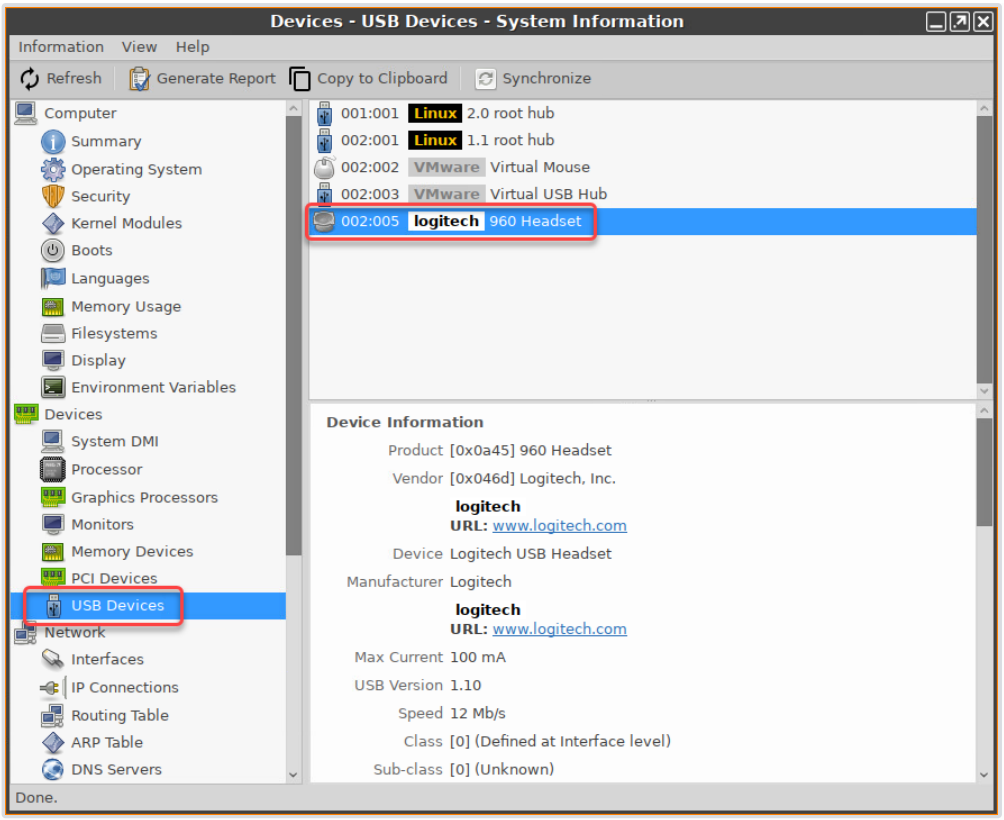
4. Provide the **Product ID** of the device as a hexadecimal value. The product ID can contain asterisks '*', each asterisk representing one hexadecimal digit. If the field is left empty, any product ID is matched.

Getting USB Device Information
To find out the **Class ID** , **Subclass ID** , **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool.

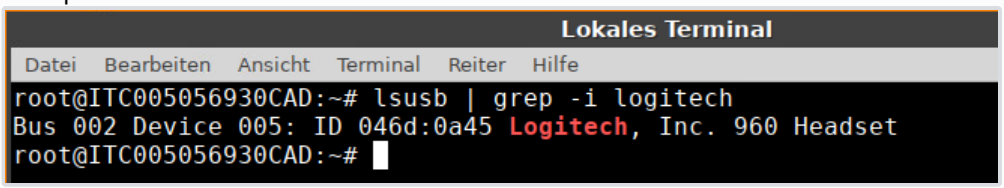
1. In the local Setup of the device, go to > > **System Information**.



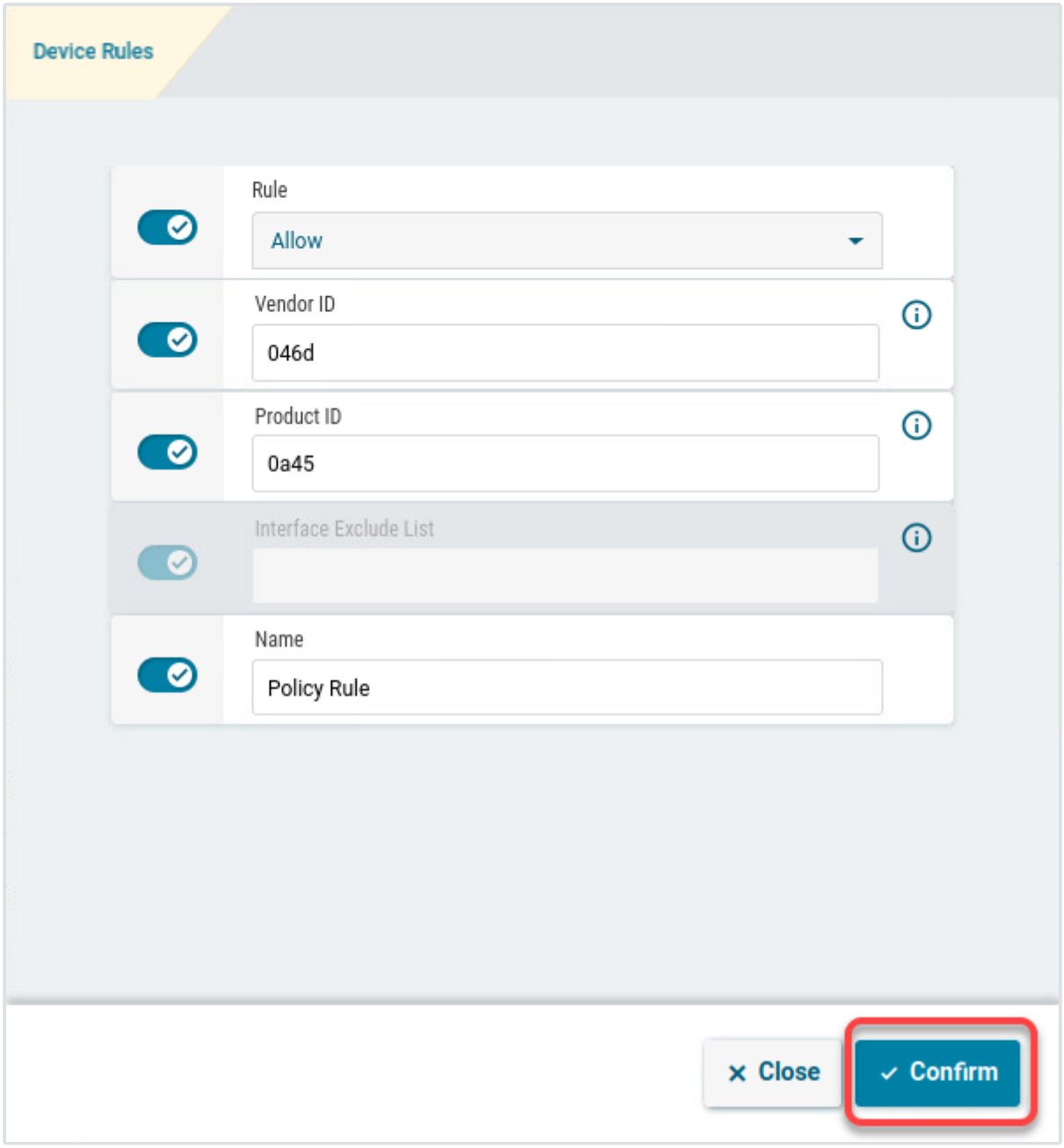
2. Select **USB Devices**.



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



5. Only for USB composite devices: Under **Interface Exclude List**, enter a list of interfaces that are to be excluded from USB redirection. The individual interfaces are separated by spaces. Example: "0 1".
6. Under **Name**, give a name for the rule.
7. Click on **Confirm**.



Automatically connect at startup

- ☑ USB devices that were inserted before the start of the session are available in the session. (Default)

Automatically connect when inserted

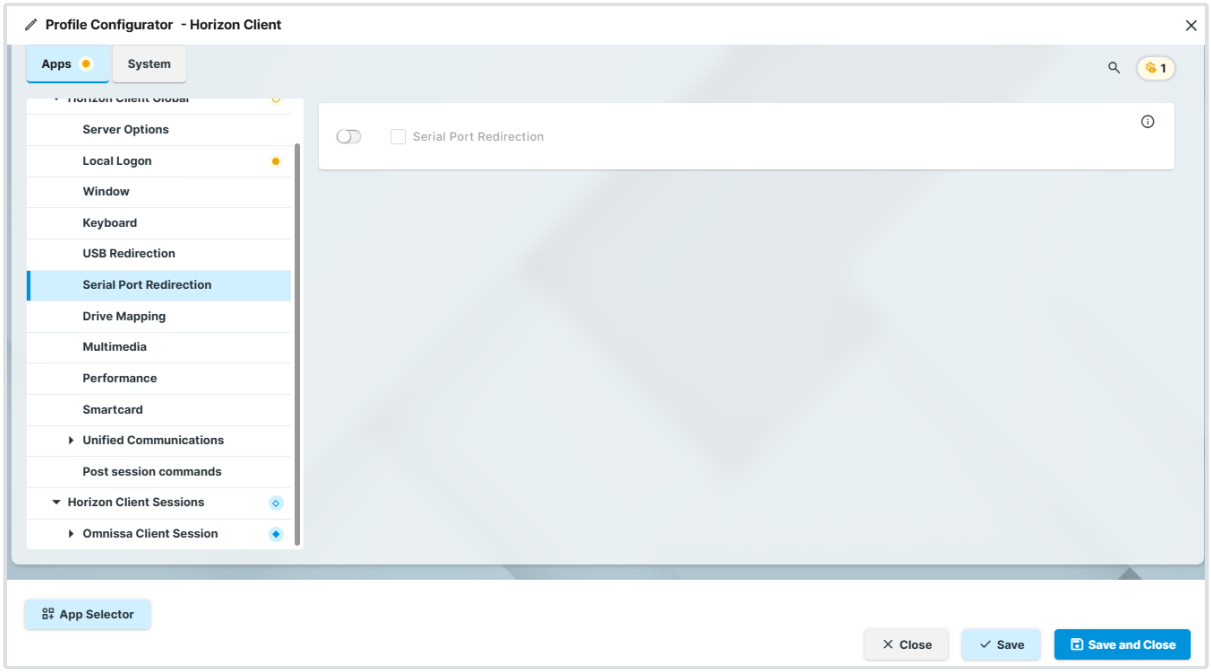
- ☑ USB devices that are inserted during the session are available in the session. (Default)

Automatic splitting of composite USB devices

- [x] A USB composite device will automatically be split into its individual components (interfaces). The class rules will be applied to these individual devices.
- [ ] The device will not be split into its components. (Default)

Configuring Serial Port Redirection (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Serial Port Redirection**.



2. Edit the settings according to your needs. The parameters are described in the following.

Serial Port Redirection

With the serial port redirection feature, you can redirect locally connected serial (`/dev/ttyS`) ports, such as built-in RS232 ports or USB-to-Serial adapters, to their RDS-hosted desktops.

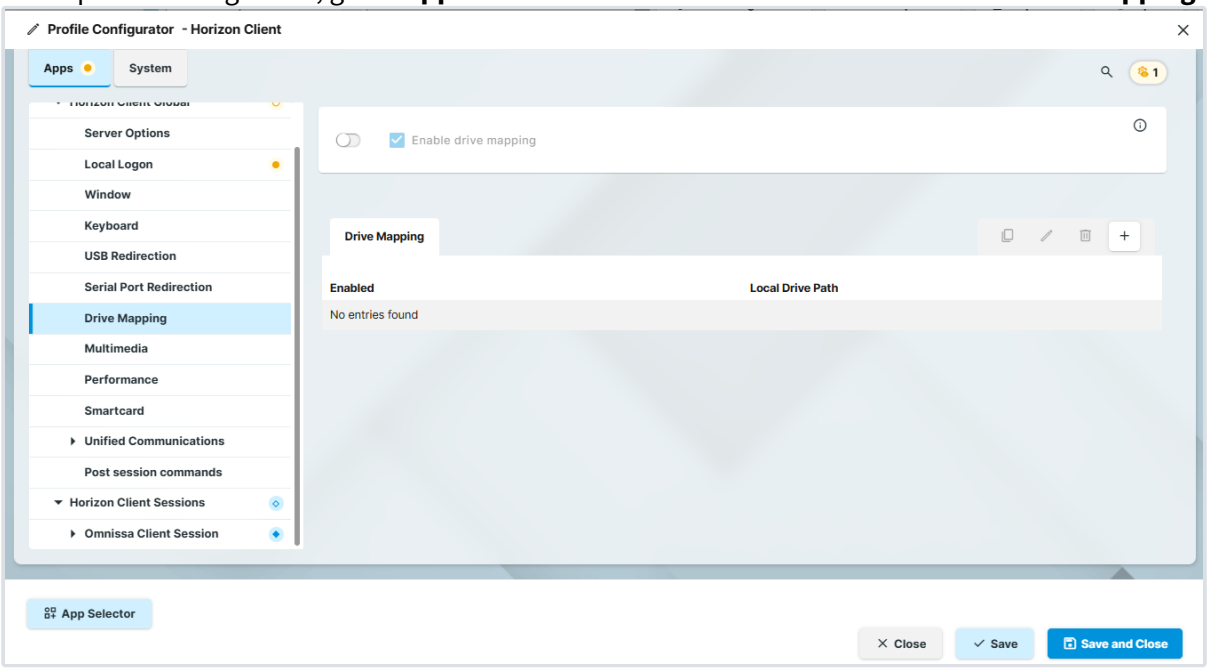
- **on**: The serial port is redirected.
- **off**: The serial port is not redirected. (Default)

Configuring Predefined Drive Mapping (Global)

You can make specific directories on USB storage devices available to your Horizon session. These directories will appear in the session, in addition to the drives that are mapped automatically (provided that **Devices > Storage Devices > Storage Hotplug > Enable dynamic client drive mapping** is enabled). Please note that **Devices > Storage Devices > Storage Hotplug > Enable dynamic client drive mapping** must be enabled to allow for predefined drive mapping.

You can define specific directories on a local drive that should be mapped.

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Drive Mapping**.



2. Edit the settings according to your needs. The parameters are described in the following.

Enable Drive Mapping

☑ Drive mapping is enabled. (Default)

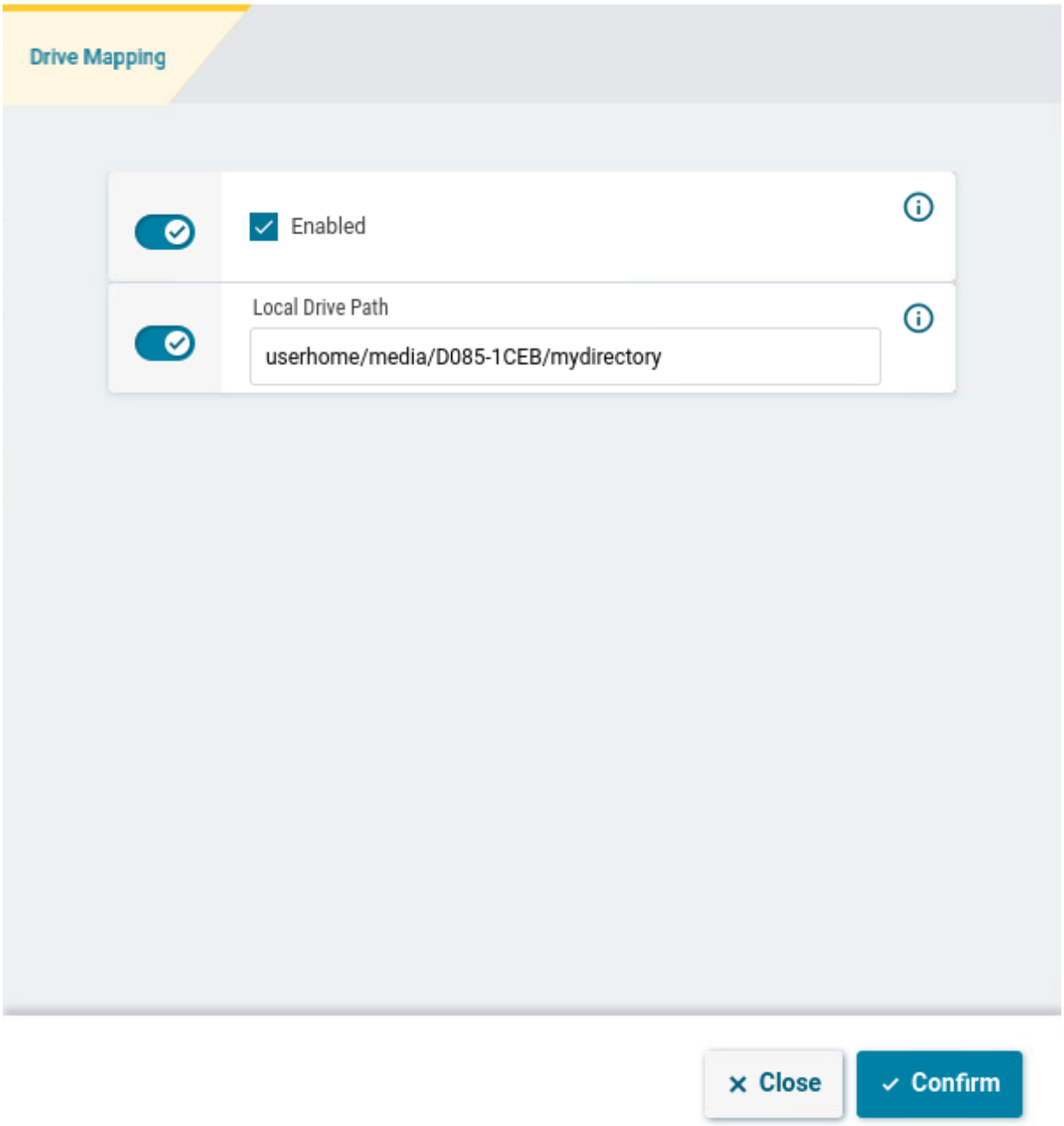
Before you unplug a hotplug storage device from the endpoint device, you must safely remove it. Otherwise, data on the hotplug storage device can be damaged. Depending on the configuration, there are one or several possibilities to safely remove a hotplug storage device:

- Click on ⏏ in the taskbar. The taskbar is not available in a fullscreen session.
- Click on ⏏ in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a fullscreen session.

- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Don't remove the device**, then the hotplug storage device must not be removed. First, exit the program concerned or close all files or directories that reside on the hotplug storage device.

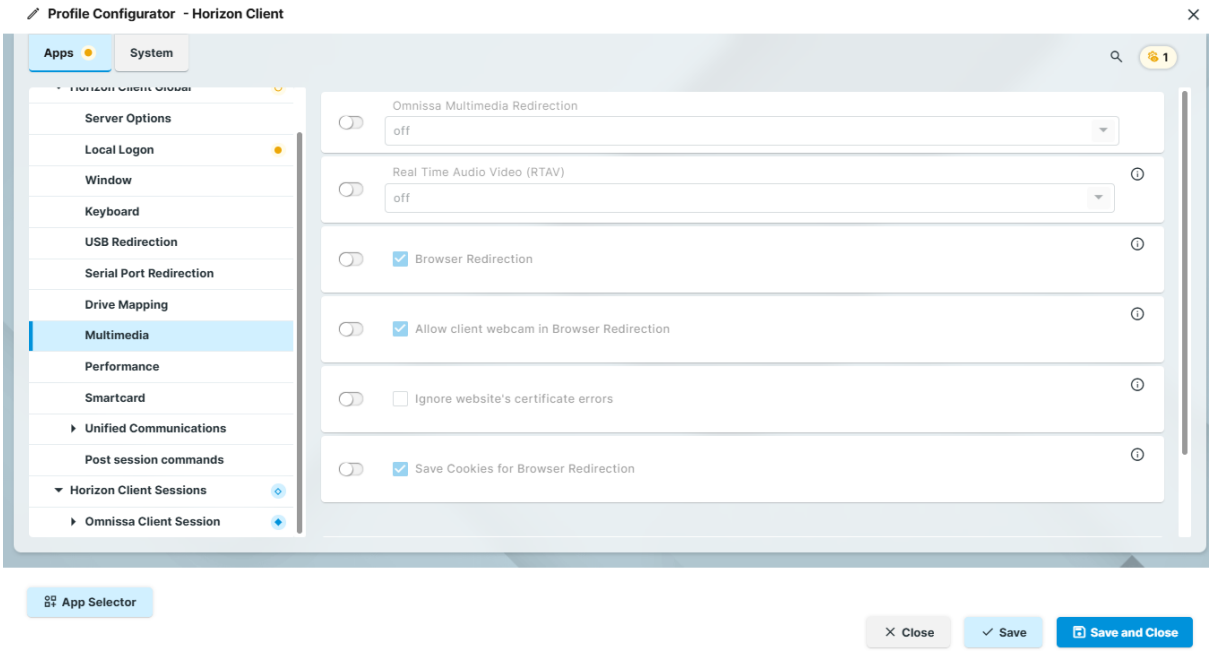
Maping a Specific Directory

1. Click **Add** to bring up the mapping window.
2. Click **Enabled** to enable the drive connection.
3. Provide the **Local Drive Path** of the local directory to which the mapping is to refer.



Configuring Multimedia (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Multimedia**.



2. Edit the settings according to your needs. The parameters are described in the following.

Omnissa Multimedia Redirection

Possible values:

- **off**: The server renders the multimedia data and sends the individual images to the client. (Default)
- **on**: The client renders the multimedia data supplied by the server.

Real Time Audio Video (RTAV)

Specifies the redirection of video data from the client USB webcam.

Possible values:

- **off**: The client does not forward the webcam data as video data. (Default)

With USB redirection, data from the webcam can be forwarded to the server even if RTAV is disabled.

- **on**: The client forwards the webcam data as video data.

Browser Redirection

☑ The rendering of the web page content is forwarded from the server to the local device, e.g. to reduce the load on the server. (Default)

Allow client webcam in Browser Redirection

- [x] Local webcam will be used in browser redirection. (Default)

Ignore website's certificate errors

- [x] Websites with certificate errors can be visited.
- [ ] Websites with certificate errors cannot be visited. (Default)

Save Cookies for Browser Redirection

- [x] Cookies will be saved. This allows the user to stay logged in on websites across remote sessions. (Default)

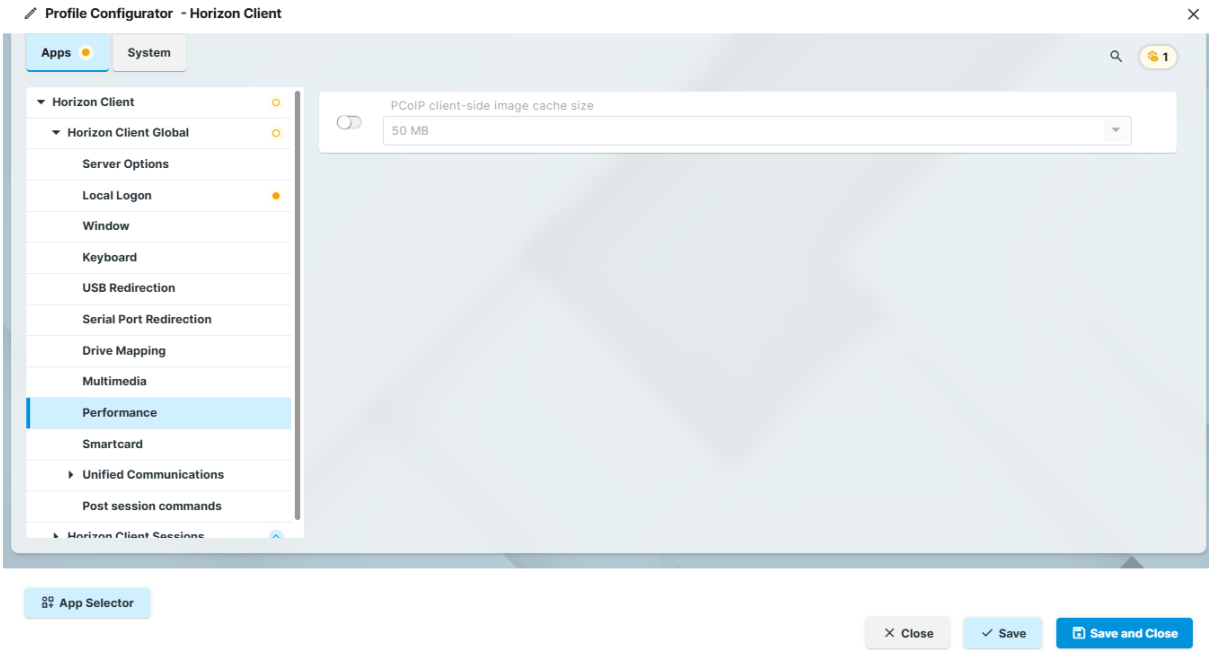
Select audio output devices

Possible values:

- **Default**: Audio is played back on the default audio output device attached to the endpoint. (Default)
- **All**: All the available audio output devices are redirected to the remote session. If you connect or remove a device during a remote session, the devices are updated dynamically during a remote session.
- **User selection**: Only the selected audio output device is redirected to the remote session. If you connect or remove a device during a remote session, the changes do not take effect in the remote session.

Configuring Performance Settings (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Performance**.



2. Edit the settings according to your needs. The parameters are described in the following.

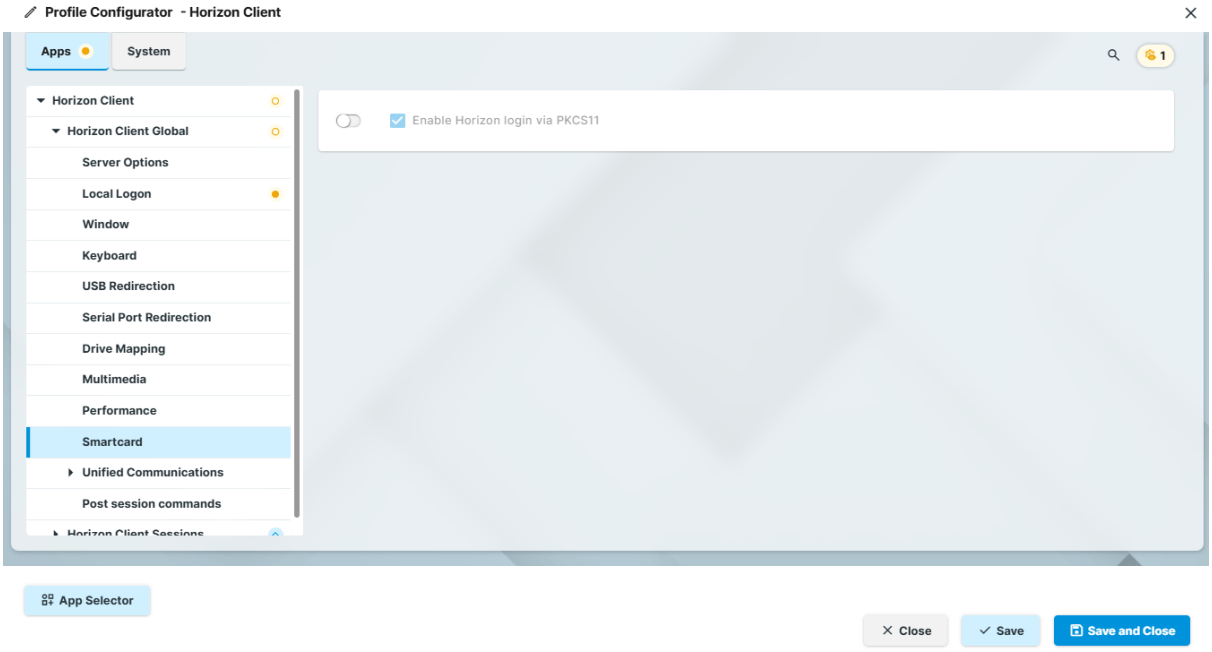
PCoIP client-side image cache size

Specifies the size of the cache for images. Caching parts of the display reduces the amount of data to be transferred. (Minimum: 50 MB; maximum: 300 MB; default: 50 MB)

Larger cache sizes of 250 MB or more should only be used if at least 2 GB RAM or more is available.

Configuring Smartcard Access (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Smartcard**.



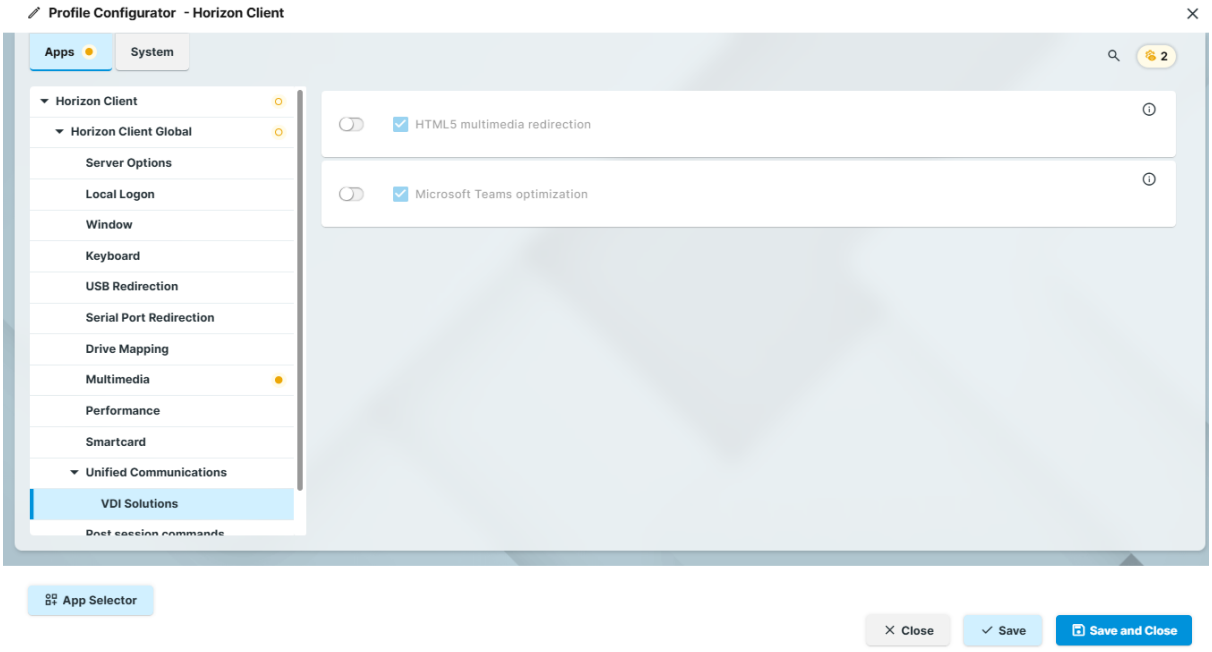
2. Edit the settings according to your needs. The parameters are described in the following.

Enable Horizon login via PKCS11

☑ The user can log in to a Horizon session via PKCS11. (Default)

Configuring HTML5 and Microsoft Teams Optimization (Global)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Unified Communications > VDI Solutions.**



2. Edit the settings according to your needs. The parameters are described in the following.

HTML5 multimedia redirection

> **Server and Browser Requirements**
> HTML5 multimedia redirection requires additional configuration on the server side.

☑ HTML5 multimedia content is redirected from a remote desktop to the endpoint devices. (Default)

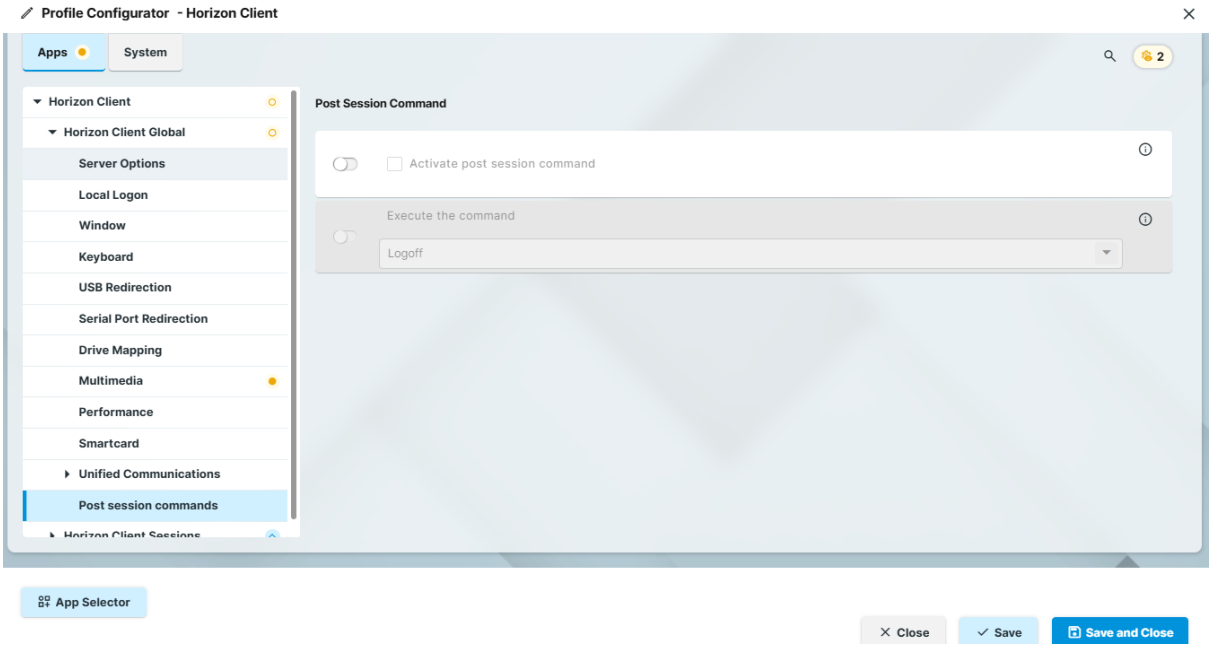
Microsoft Teams optimization

> **Server and Network Requirements**
> Microsoft Teams optimization requires additional configuration on the server side.

☑ The audio and video streams for Microsoft Teams are redirected to the endpoint devices. Audio and video data are not processed by the server. (Default)

Configuring Post-Session Commands

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Global > Post session commands**.



2. Edit the settings according to your needs. The parameters are described in the following.

Activate post session command

Allows to define an action that is performed when the last Horizon session is ended. For information on global post-session commands, see Post-session Custom Commands in IGEL OS 12[173].

- ☑ The post-session command specified under **Execute the command** will be executed.
- ☐ The post-session command specified under **Execute the command** will not be executed. (Default)

Execute the command

Action that is carried out after the end of the Horizon session(s).

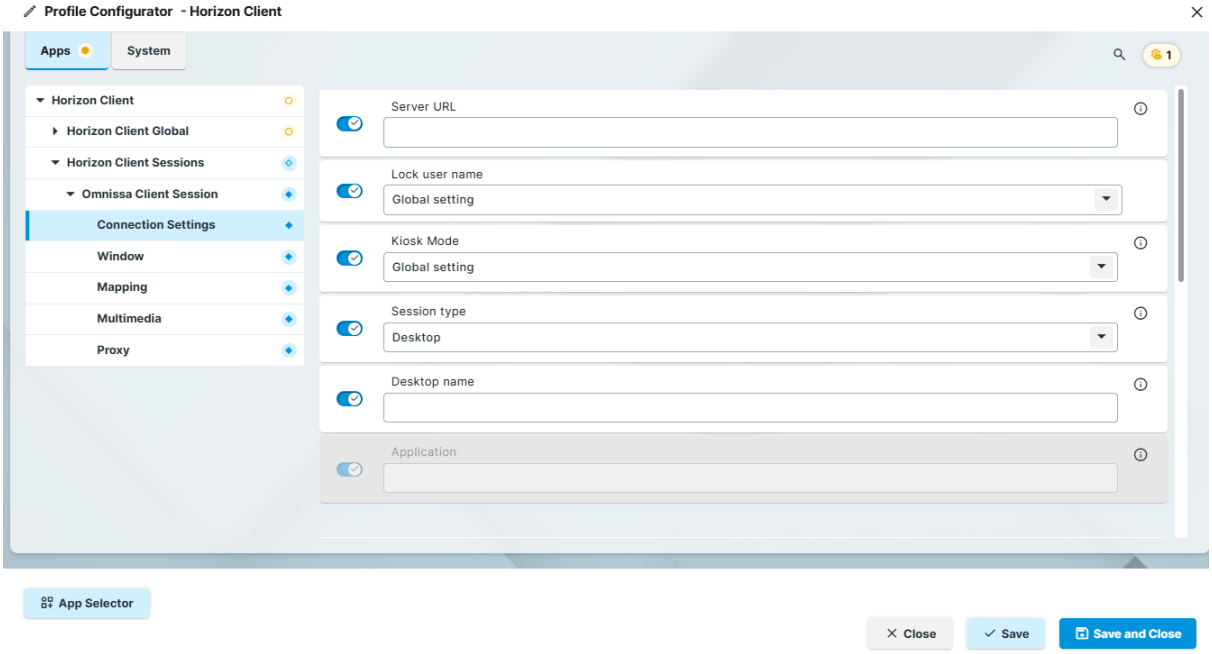
Possible values:

- **Logoff**: The user is automatically logged off; a login method must be defined for this purpose. Further information can be found under Logon Settings in IGEL OS 12[174]. (Default)
- **Shutdown**: The device will be shut down.
- **Enter custom command here**: Command to be executed.

173. https://kb.igel.com/en/igel-os-base-system/current/post-session-custom-commands-in-igel-os-12
174. https://kb.igel.com/en/igel-os-base-system/current/logon-settings-in-igel-os-12

Configuring the Connection Settings (Session Specific)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions > [session name] > Connections Settings**.



2. Edit the settings according to your needs. The parameters are described in the following.

Server URL

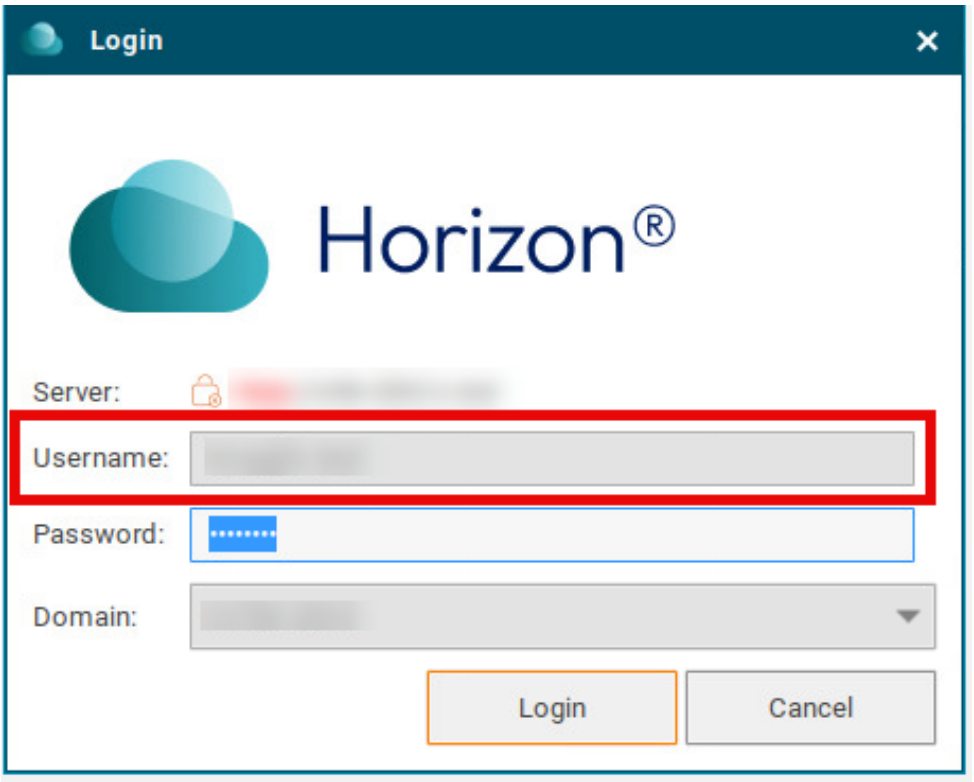
URL of the Horizon server.

Lock user name

Locks the user name specified under **Apps > Horizon Client > Horizon Client Session > [session name] > Connection Settings > User name**.

Possible values:

- **Global setting**: The setting from **Apps > Horizon Client > Horizon Client Global > Server Options > Lock user name** will be used. (Default)
- **on**: The user name will be locked and cannot be changed in the login window.
- **off**: The user name will not be locked in the login window.



Kiosk mode

- **Global setting**: The setting from **Apps > Horizon Client > Horizon Client Global > Server Options > Kiosk mode will be used**. (Default)
- **on**: The Horizon client is run in a non-interactive mode that is suitable for kiosk mode operation.
- **off**

Session type

Specifies whether the session contains a desktop or an individual application.

Possible values:

- **Desktop**: The session contains a desktop. (Default)
- **Application**: The session contains an individual application.

Desktop name

Specifies a name for the desktop. This option is available if **Session type** is set to “Desktop”.

Application

The name of the application that is launched during the session. This option is available if **Session type** is set to “Application”.

Use passthrough authentication for this session

- ☑ The username and password are temporarily saved and used for authentication purposes in this session.
- ☐ Passthrough authentication is not used. (Default)

Save last user name

- ☑ The login window will be prefilled with the last used user name.
- ☐ The last used user name will not be saved. (Default)

User name

User name when logging on to the Omnissa Horizon server

User password

Password when logging on to the Omnissa Horizon server

Domain

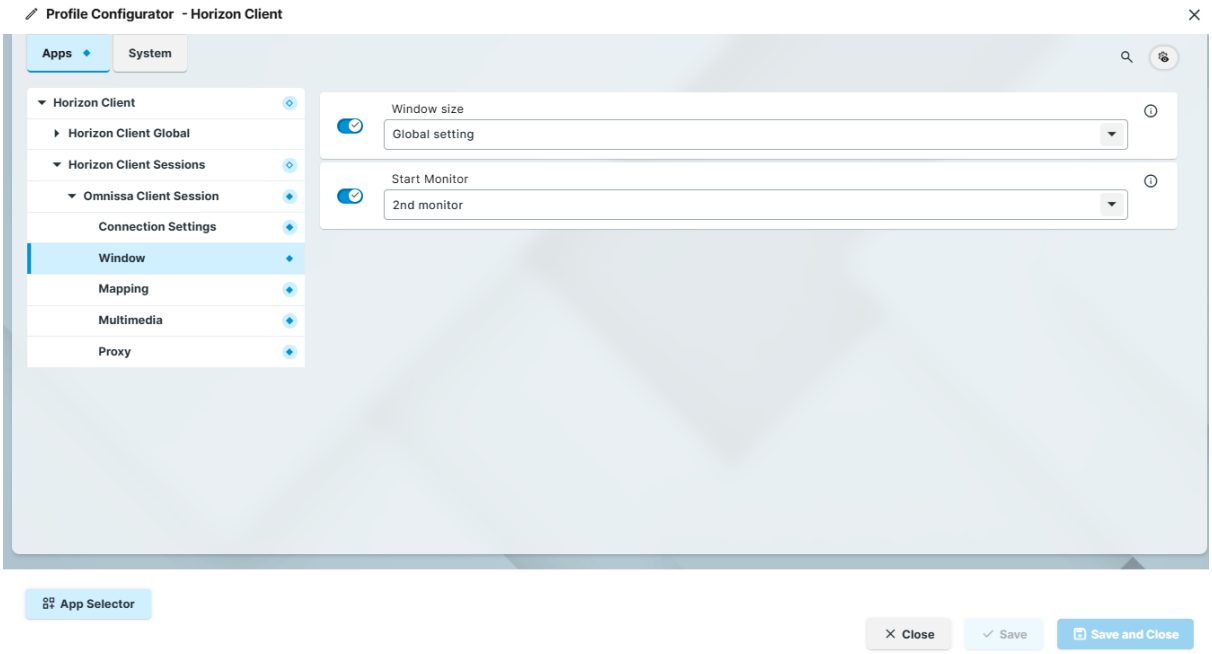
Domain when logging on to the Omnissa Horizon server

Autoconnect

- ☑ When the session starts, the connection to the desktop or application will automatically be established. For this to be possible, the name of the desktop or application must be defined.
- ☐ When the session starts, the overview will be shown. (Default)

Configuring the Window Settings (Session Specific)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions > [session name] > Window**.



2. Edit the settings according to your needs. The parameters are described in the following.

Window size

Specifies the width and height of the window.

Possible values:

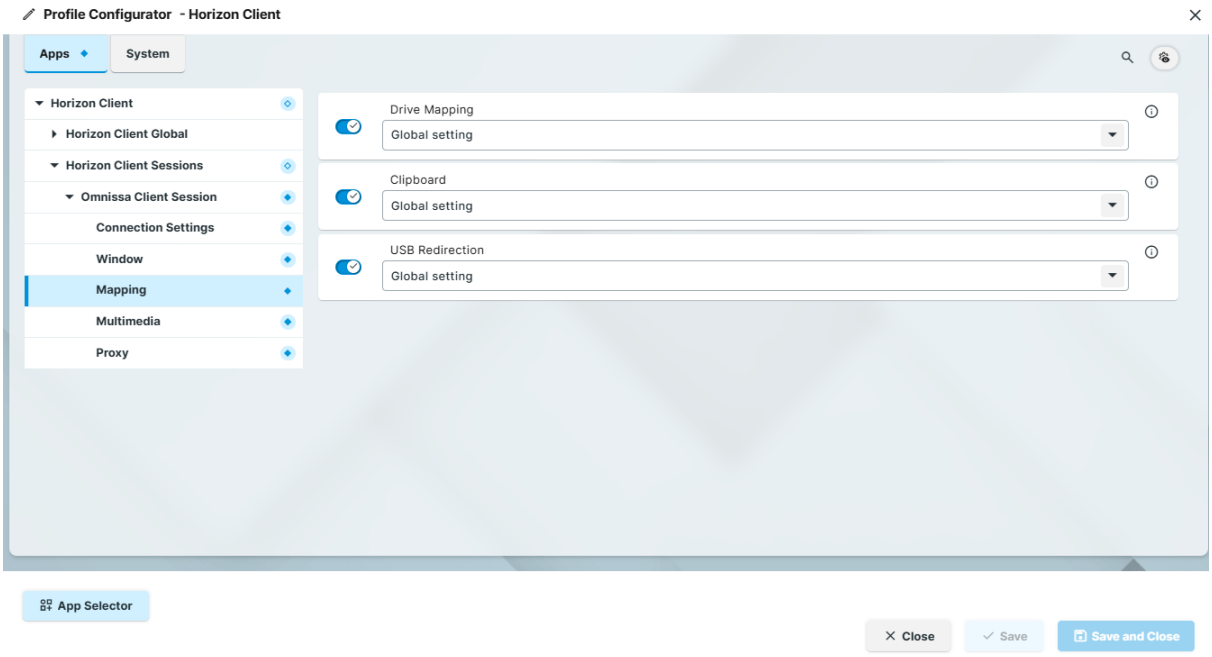
- **Global setting**: The window size is carried over from the global settings defined under **Apps > Horizon Client > Horizon Client Global > Window**. (Default)
- **full-screen**: The session is shown on the full screen.
- **user selection**
- Numeric details: The session is shown in the selected resolution or on the selected percentage of the screen area.

Start monitor

Specifies the monitor on which the session is shown.

Configuring Drive Mapping and USB Redirection (Session Specific)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions > [session name] > Mapping**.



2. Edit the settings according to your needs. The parameters are described in the following.

Drive Mapping

Possible options:

- **Global setting**: The setting **Apps > Horizon Client > Horizon Client Global > Drive Mapping > Enable drive mapping** will be used.
- **on**
- **off**

Clipboard

Possible options:

- **Global setting**: The setting **Apps > Horizon Client > Horizon Client Global > Keyboard > Clipboard** will be used.
- **on**
- **off**

USB Redirection

If the global setting **Apps > Horizon Client > Horizon Client Global > USB Redirection > USB Redirection** is disabled, USB redirection can not be enabled on a session-specific basis.

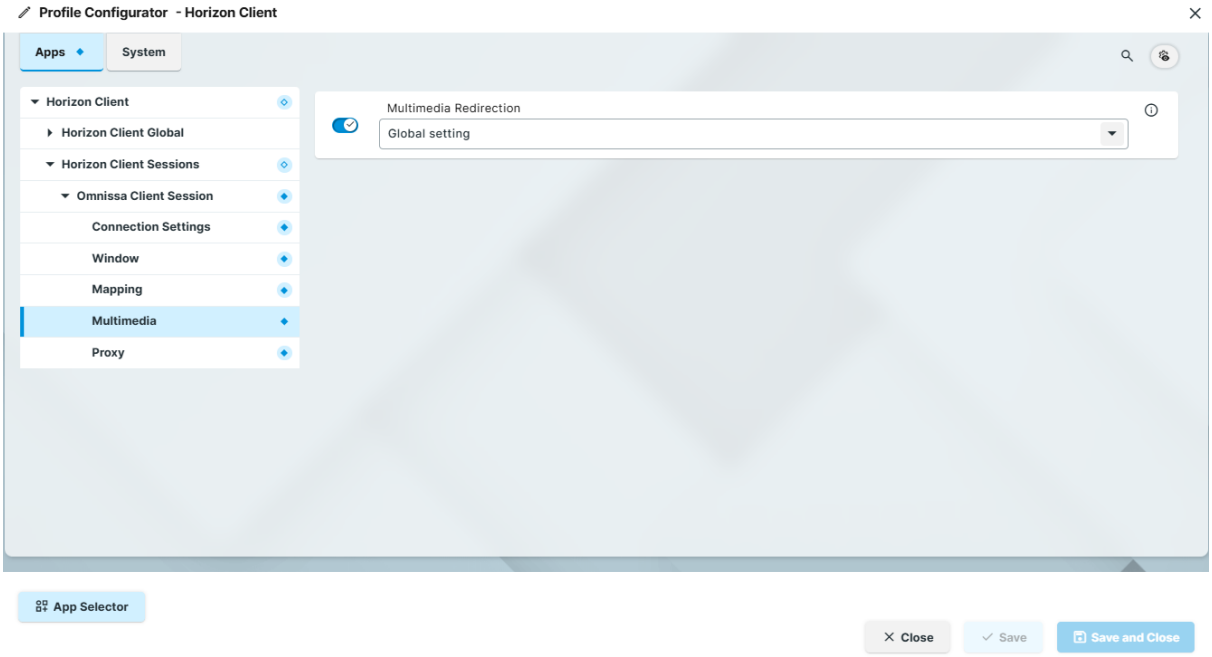
Possible options:

- **Global setting**: The setting **Apps > Horizon Client > Horizon Client Global > USB Redirection > USB Redirection** will be used.

- **off**

Configuring Multimedia Settings (Session Specific)

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions > [session name] > Multimedia**.



2. Edit the settings according to your needs. The parameters are described in the following.

Multimedia Redirection

If the global setting **Apps > Horizon Client > Horizon Client Global > Multimedia > Omnissa Multimedia Redirection** is disabled, multimedia redirection cannot be enabled on a session-specific basis.

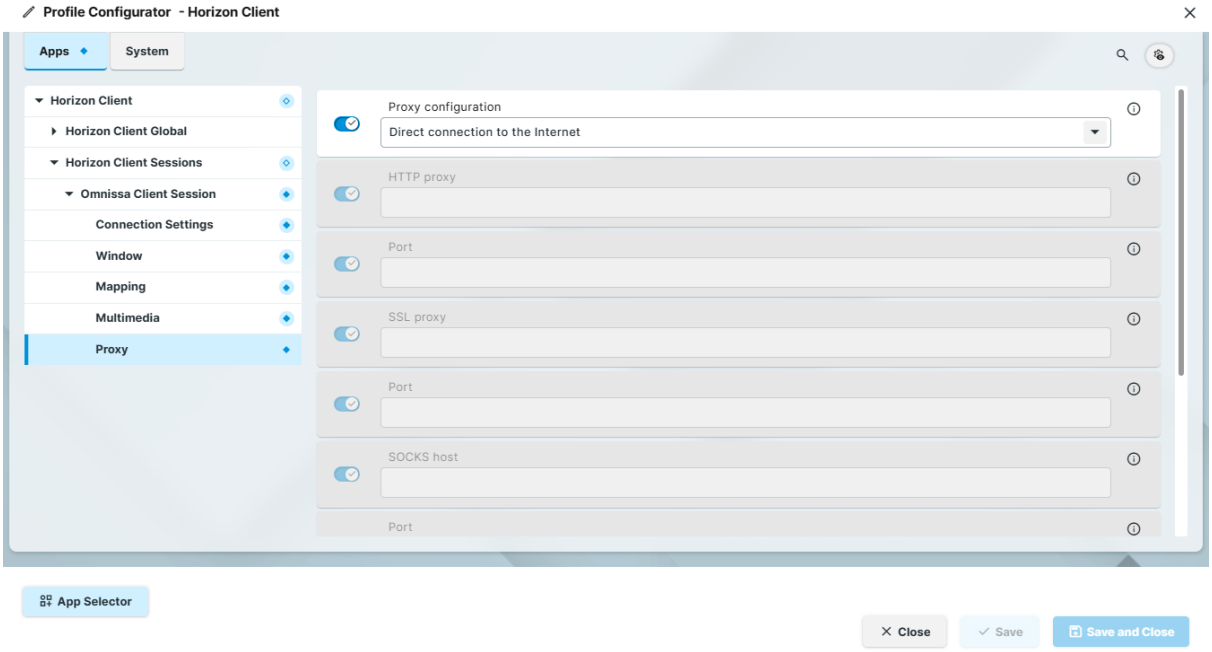
Possible options:

- **Global setting**: The setting **Apps > Horizon Client > Horizon Client Global > Multimedia > Omnissa Multimedia Redirection** will be used.
- **off**

Configuring Proxy Settings (Session Specific)

You can configure the use of a proxy for the connection between the client and server.

1. In the profile configurator, go to **Apps > Horizon Client > Horizon Client Sessions > [session name] > Proxy**.



2. Edit the settings according to your needs. The parameters are described in the following.

Proxy configuration

Possible options:

- **Direct connection to the Internet**: No proxy will be used. (Default)
- **Manual proxy configuration**: The proxy is configured with the following settings.
- **System-wide proxy configuration**: The proxy configured under **Network > Proxy** is configured. See https://kb.igel.com/en/igel-os-base-system/12.6.1/proxy-configuration-in-igel-os-12.

HTTP proxy

URL of the proxy for HTTP

Port

Port of the proxy for HTTP

SSL proxy

URL of the proxy for SSL

Port

Port of the proxy for SSL

SOCKS host

URL of the proxy for SOCKS

Port

Port of the proxy for SOCKS

SOCKS protocol version

Version of the SOCKS protocol used

Possible options:

- **SOCKS v4**
- **SOCKS v5** (Default)

No proxy for

List of URLs for which no proxy is to be used (separated by commas)

Troubleshooting Topaz USB Not Passed through to Omnissa Horizon on IGEL OS

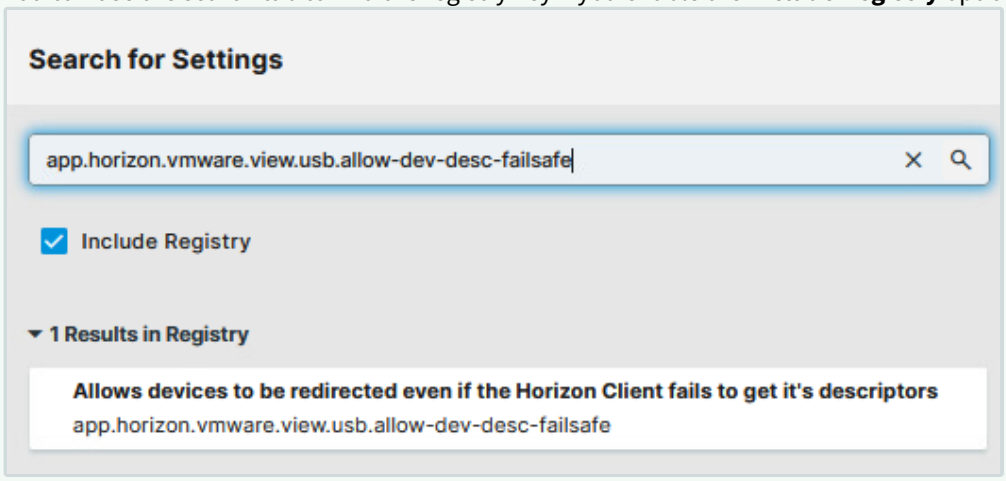
Problem

The Topaz USB device is not passing through to the Horizon VDI environment running on IGEL OS 12.

Solution

1. Enable the following setting in the system registry:
   `app.horizon.vmware.view.usb.allow-dev-desc-failsafe`

You can use the search tab to find the registry key if you enable the **Include Registry** option.



2. Apply the setting to the device.

3. Restart the session or restart the IGEL OS.

OpenConnect VPN

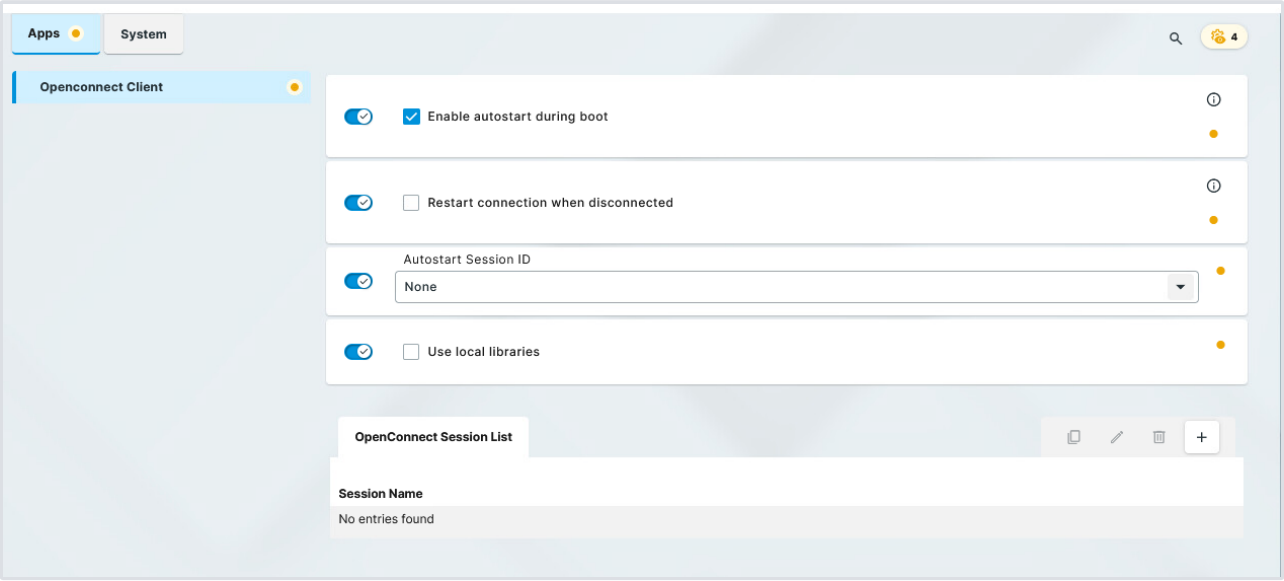


- Getting Started with OpenConnect VPN (see page 471)
- Configuration of OpenConnect VPN (see page 473)

Getting Started with OpenConnect VPN

The OpenConnect VPN app establishes a virtual private network using TLS encryption.

Global Configurations



Enable autostart during boot

The setting here overrides the settings under **Autostart configuration** in the OpenConnect session settings.

☑ Autostart is enabled.

☐ Autostart is disabled. (Default)

Restart connection when disconnected

☑ Reconnect automatically when a disconnect occurs.

☐ Do not reconnect automatically when a disconnect occurs. (Default)

Autostart session ID

Select a session name from the **OpenConnect Session List** that will be autostarted

Use local libraries

☑ Specific libraries are used by the OpenConnect app instead of the system-wide library. This allows for using TLS 1.2. For details, see https://www.infradead.org/openconnect/manual.html.

☐ The OpenConnect app utilizes the system's libraries. (Default)

How to Create a Session

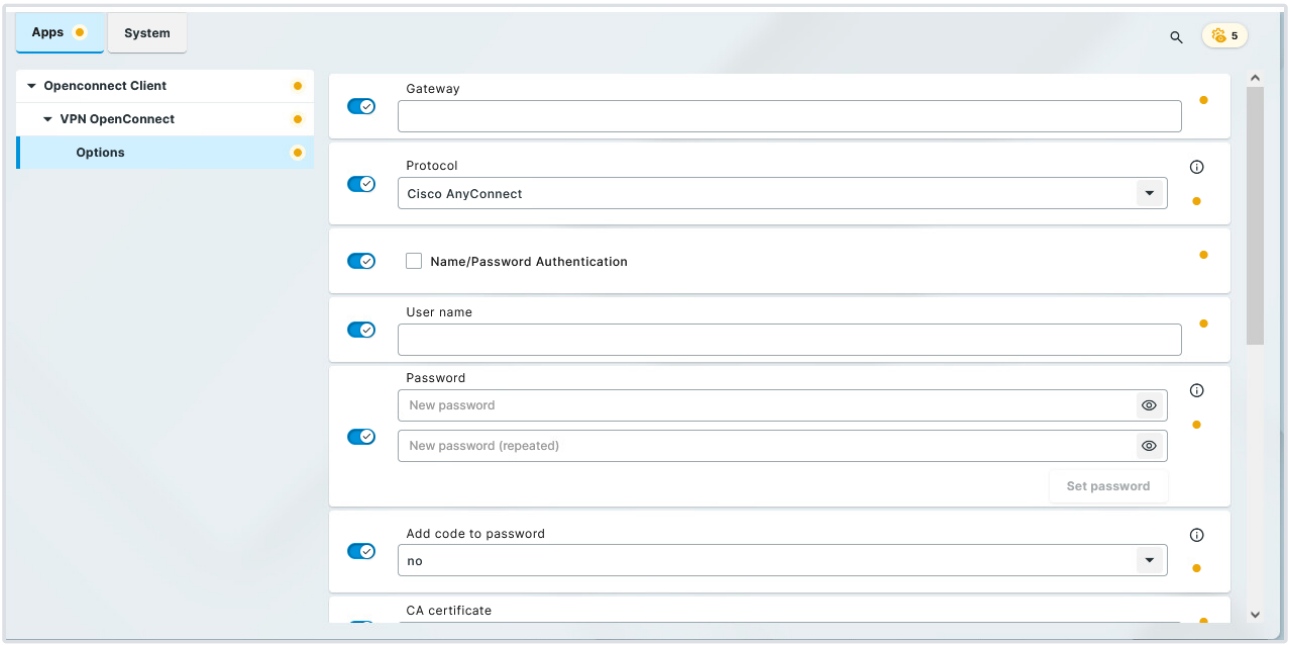
1. In the Profile Configurator, go to **Apps > OpenConnect Client**.
2. Click + under **OpenConnect Session List**.
3. Define the starting methods for the session. The starting methods parameters are described under Starting Methods for Apps[175] .
4. Save the settings.
   The session is created.
5. Configure the session according to your needs; for details, see Configuration of OpenConnect VPN (see page 473).

175. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps

Configuration of OpenConnect VPN

In this article you can find information on the configuration options for the OpenConnect VPN app.

Menu path: **Apps > OpenConnect Client> OpenConnect Session > Options**



Gateway

IP address, hostname or Fully Qualified Domain Name (FQDN) of the VPN gateway

Protocol

Defines the protocol used in the VPN connection

Possible options:

- Cisco AnyConnect (Default)
- Juniper Network
- Junos Pulse
- PAN GlobalProtect
- F5 BIG-IP
- Fortinet FortiGate
- Array Networks

Name/Password Authentication

☑️ User name and password are used for authentication.

☐ User name and password are not used for authentication. (Default)

User name

User name used for authentication

Password

Password used for authentication

Add code to password

An extra field is shown in the authentication dialog to provide the code for multi-factor authentication.

Possible options:

- **no**: No code is required for authentication
- **before**: The code has to be entered in the password field before the password
- **after**: The code has to be entered in the password field after the password
- **separate field**: A separate field is shown for entering the code. The Registry key **app.openconnect.settings.openconnect%.vpnopts.search_str_code** has to be set to the corresponding value.

CA Certificate

Path to the CA certificate

User Certificate

Path to the user certificate

Private Key

Path to the private key

Private Key password

Password of the private key

Server Certificate

Path to the server certificate

Extended parameters

These parameters are added to the parameter list. Ensure that you use unique and accurate parameter naming. Use `--` before each parameter.

Progressive Web App

- How to Set Up Standalone Microsoft PWAs on IGEL OS 12 (see page 477)
- Example: Microsoft Outlook as a Progressive Web App (PWA) on IGEL OS 12 (see page 482)
- Example: Google Maps as a Progressive Web App (PWA) on IGEL OS 12 (see page 483)

You might also find the following IGEL Community article useful: HOWTO Browsers - IGEL Community Docs[176]
The content of this external guide is not covered by official support channels, and the IGEL Knowledge Base Team cannot guarantee its accuracy or completeness.

176. https://igel-community.github.io/IGEL-Docs-v02/Docs/HOWTO-Browsers/#os-12-running-progressive-web-apps-pwa

How to Set Up Standalone Microsoft PWAs on IGEL OS 12

This article describes configuring Microsoft standalone progressive web apps (PWAs) on IGEL OS 12. In contrast to generic PWAs, standalone PWAs have predefined URLs and have their own Chromium Browser profile.

Basically, a PWA is a Chromium window with a specific profile in the so-called app mode. All policies that are defined for Chromium are also valid for the PWAs. Exception: **Clear browsing data** options configured for Chromium under **Chromium Browser > Global Settings > Privacy** starting from Chromium Browser app version 144.0.7559.96 BUILD 1.0.

The configuration procedure is similar for the following apps:

- Microsoft Excel PWA (used as an example in this article)
- Microsoft Outlook PWA
- Microsoft PowerPoint PWA
- Microsoft Word PWA

Requirements

- If the below apps have not been installed beforehand, they will automatically be installed during the app installation:
  - Progressive Web App
  - Chromium Browser
- To use the service, you may need to register an account with the service provider and to accept its terms of use.

Limitations

- Avoid configuring any installed standalone PWA as generic PWA because it can lead to unwanted behavior.
- Each standalone PWA has its own Chromium Browser profile and therefore, the user has to log in to each PWA.
- It is an expected behavior that links may be opened in a regular browser window/tab.

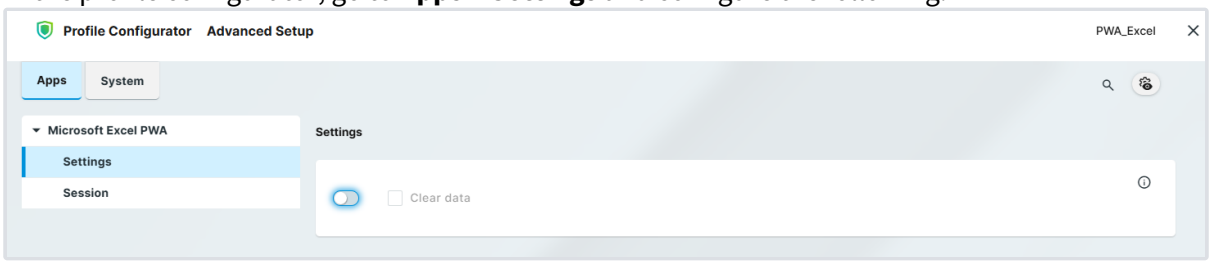
If you want to prevent switching between apps via Microsoft 365 App Launcher in the upper left corner, consider using the **Lockdown mode** setting under **Apps > Chromium Browser > Global Settings > Appearance**.

If you want to allow switching between apps via Microsoft 365 App Launcher in the upper left corner, but the newly opened app should be redirected to the main window, enable the following settings:

- **Apps > Chromium Browser > Global Settings > Appearance > Lockdown mode**
- **Apps > Chromium Browser > Global Settings > Appearance > Force single window**

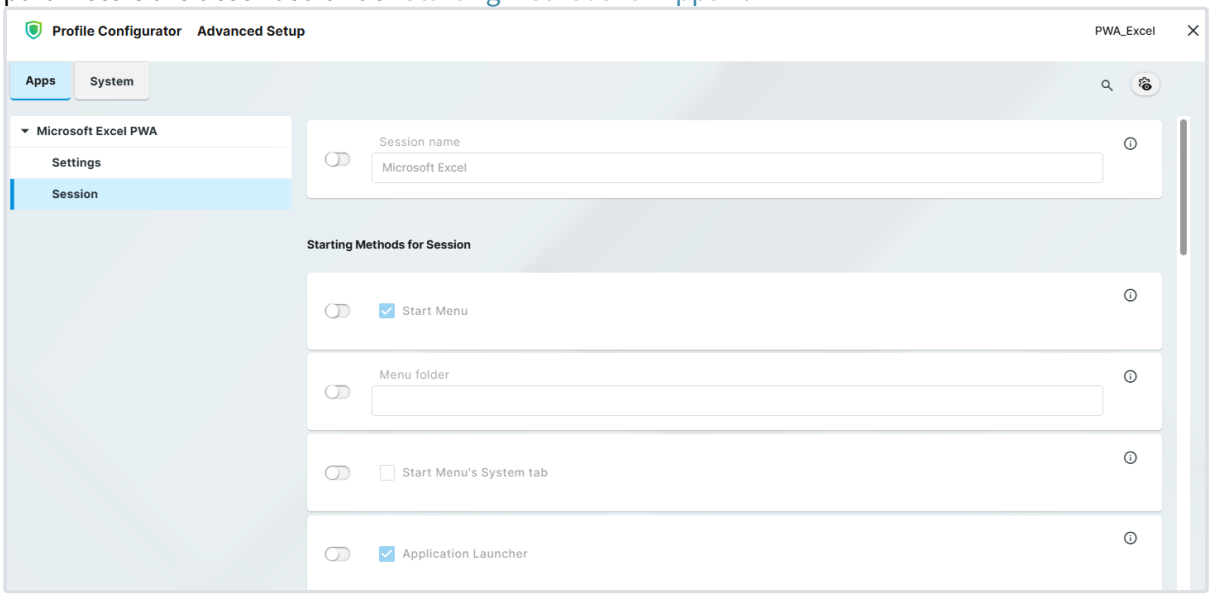
How to Configure Microsoft Excel PWA

1. Import the app to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[177].
2. In the IGEL UMS, create a profile configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[178].
3. In the profile configurator, go to **Apps > Settings** and configure the following:



Clear data
Removes all persistent data such as login credentials and Cookies each time the app is closed or the user logs out from the device.

4. Go to **Apps > Session** and configure the starting methods for the app. The starting methods parameters are described under Starting Methods for Apps[179].

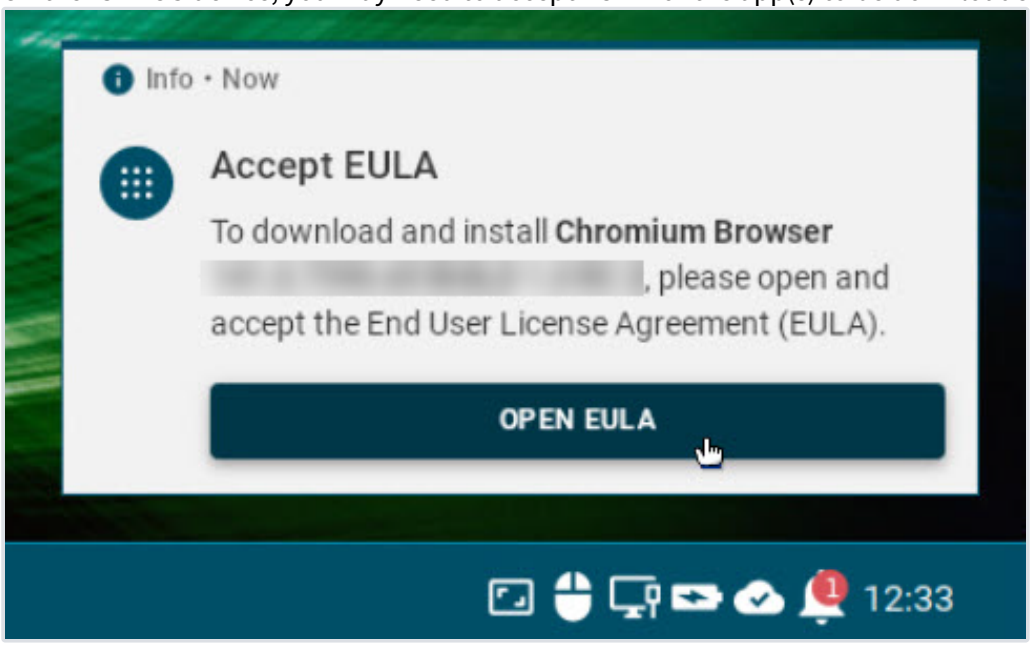


5. Save the profile and assign it to the required devices / device directories. For details on profile assignment, see How to Create and Assign Profiles in the IGEL UMS Web App[180].

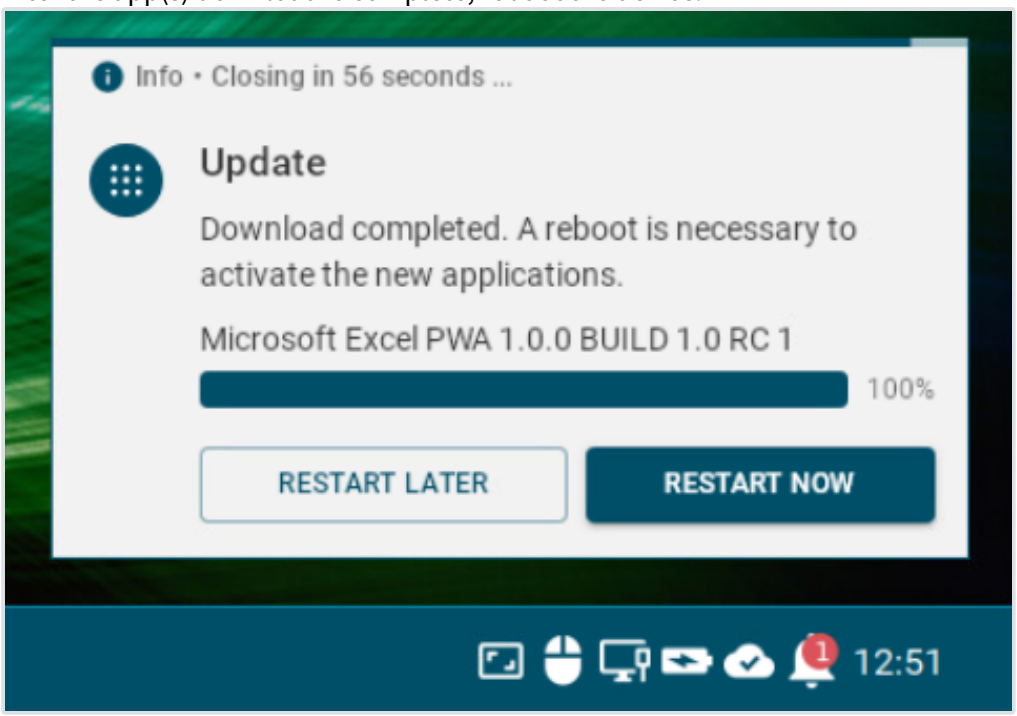
177. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
178. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-
179. https://kb.igel.com/en/igel-os-base-system/current/starting-methods-for-apps
180. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-

Completing the Installation

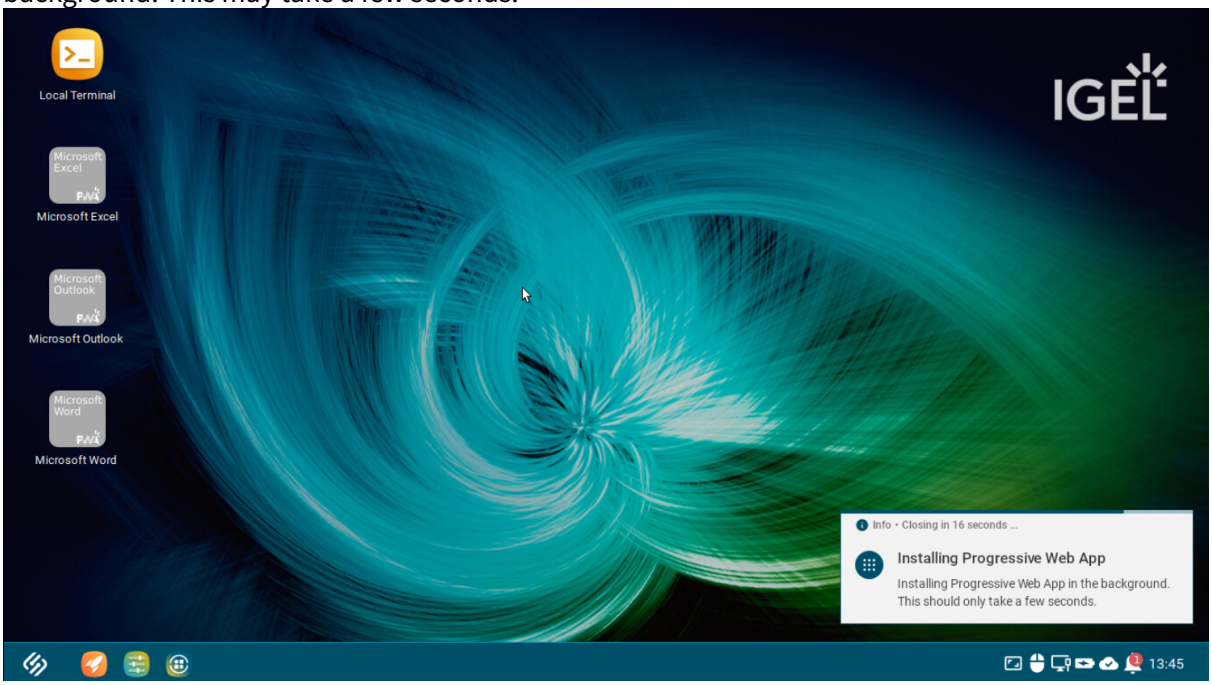
1. On the IGEL OS device, you may need to accept EULA for the app(s) to be downloaded.



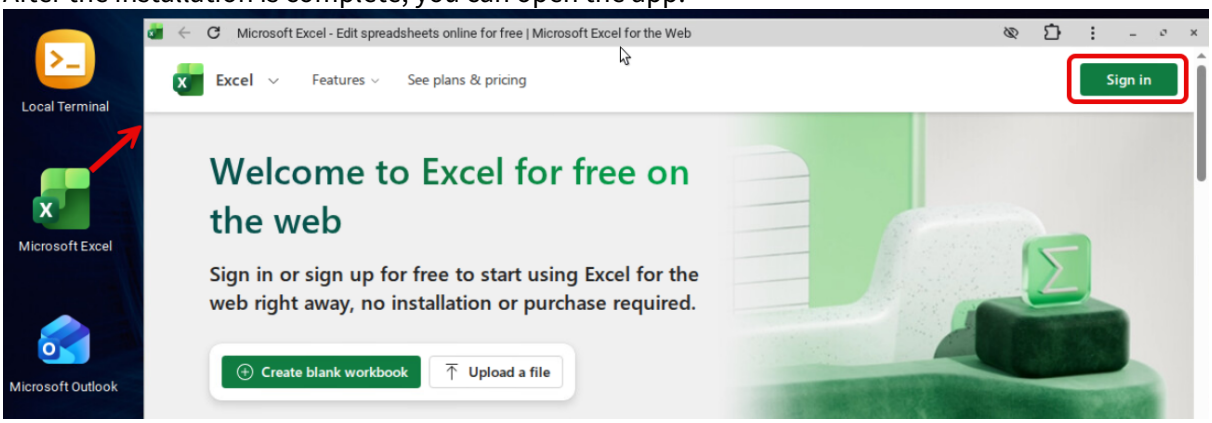
2. After the app(s) download is complete, reboot the device.



3. Log in to the device. If not logged in, the next step will not be started.
4. After the device is fully started, Progressive Web App will automatically be installed in the background. This may take a few seconds.



5. After the installation is complete, you can open the app.



If the app icon is not displayed correctly, some user action may be required to complete the installation:

1. Open the app and log in / accept the terms of use / etc.
2. Reboot the device afterwards.

If not all PWAs have been properly installed (e.g. required user actions have not yet been performed), the installation process of Progressive Web App will automatically start in the background after each reboot.

The installation process is finished as soon as no icon is grey.

Example: Microsoft Outlook as a Progressive Web App (PWA) on IGEL OS 12

This article is currently being updated. Please refer to How to Set Up Standalone Microsoft PWAs on IGEL OS 12[181] if you want to install Microsoft Outlook as a standalone PWA.
If you want to install an app as a generic PWA, see Example: Google Maps as a Progressive Web App (PWA) on IGEL OS 12[182].

181. https://kb.igel.com/en/igel-apps/current/how-to-set-up-standalone-microsoft-pwas-on-igel-os
182. https://kb.igel.com/en/igel-apps/current/example-google-maps-as-a-progressive-web-app-pwa-o

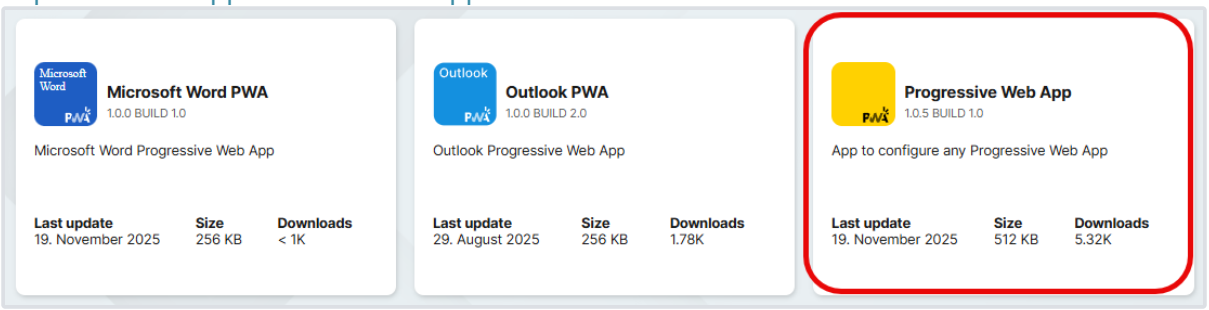
Example: Google Maps as a Progressive Web App (PWA) on IGEL OS 12

This article describes setting up a generic Progressive Web App (PWA) on IGEL OS 12. We will use Google Maps as an example; for other web apps, the procedure is similar.

Basically, a PWA is a Chromium window with a specific profile in the so-called app mode. All policies that are defined for Chromium are also valid for the PWAs. Exception: **Clear browsing data** options configured for Chromium under **Chromium Browser > Global Settings > Privacy** starting from Chromium Browser app version 144.0.7559.96 BUILD 1.0.

Prerequisites

- Device with IGEL OS 12
- The app "Progressive Web App" is imported to your UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[183].



- You know the **manifest_id** of your Progressive Web App. You can retrieve it by installing the PWA on any device, no matter which OS, by entering `chrome://web-app-internals` in the browser and scrolling to the entry **manifest_id** of the app in question. For this purpose, you can use Chrome, Chromium, Edge, or any other Chrome-based web browser; you may have to replace `chrome` with the actual browser name, e.g. `edge://web-app-internals`. Please note that Progressive Web Apps on IGEL OS always use Chromium.

Click for examples of the manifest_id...

183. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta





Limitations

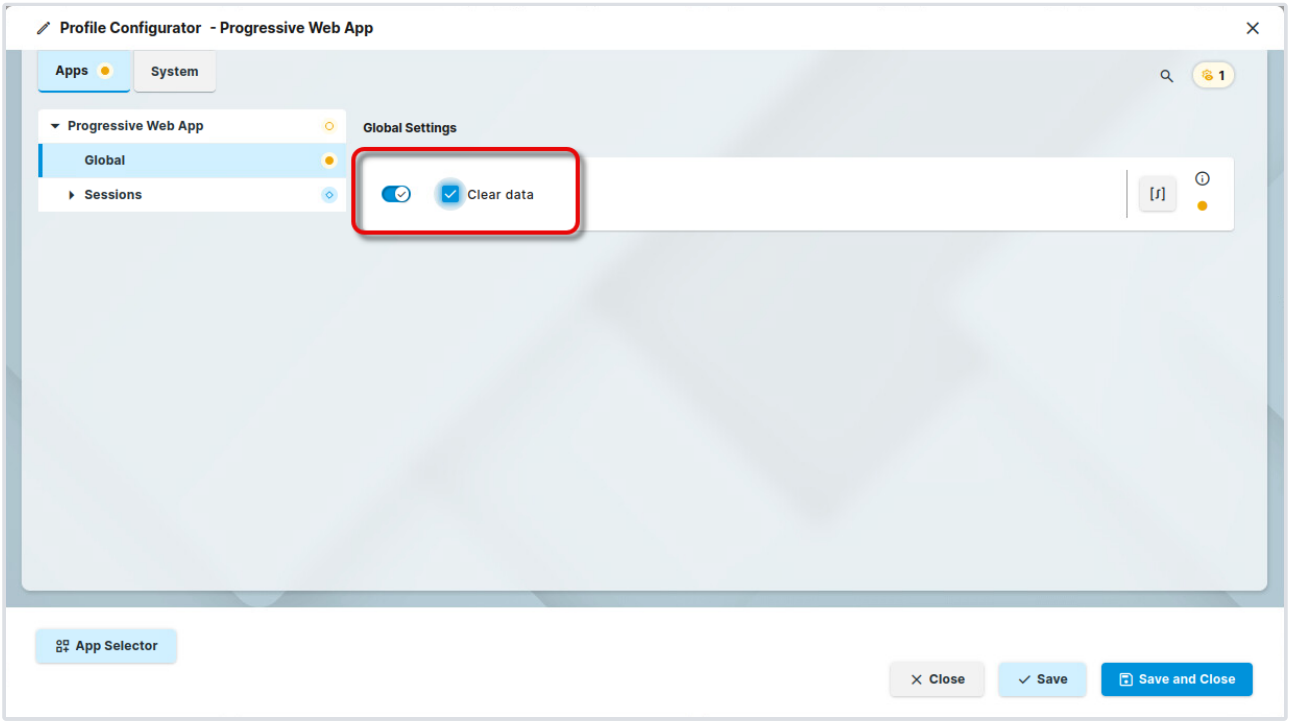
- Avoid configuring any installed standalone PWA as generic PWA because it can lead to unwanted behavior.
- If you have already apps installed as generic PWA, they will be shortly unavailable during the installation of a new generic PWA.

Global Setting for All Progressive Web Apps: Clear Data

You can define whether all profile-related data of a Progressive Web App (e.g. login credentials, cookies) should be removed each time the app is closed or the user logs out from the device or restarts it. This will influence all apps installed as a generic PWA.

→ In the profile configurator, go to **Apps > Progressive Web App > Global** and enable **Clear data**.

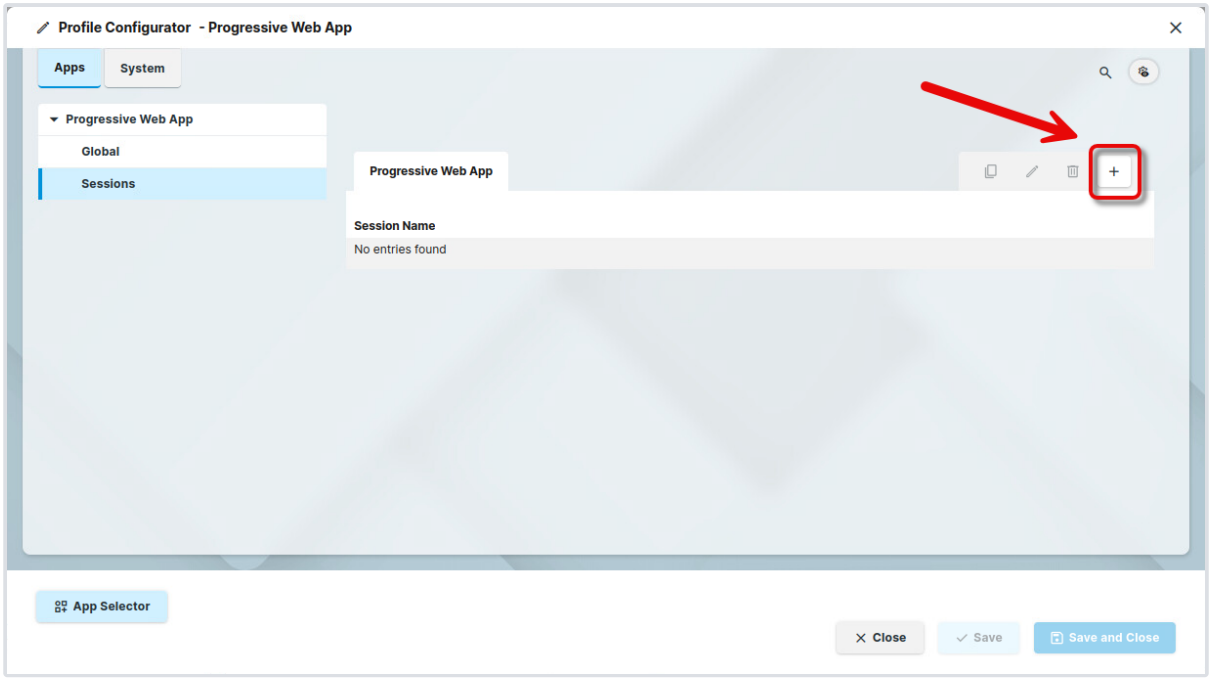
> ⚠ If you need to activate **Clear data** setting for the PWA app, it is recommended to enable it only after the app installation is complete (see the below instructions “Completing the Installation”). Otherwise, the app icon can be displayed incorrectly even after performing the required user actions and the device reboot. This is because the PWA requires user data (resulting from login, consent, accepting cookies etc.) to fully complete the installation and to correctly display the app icon.



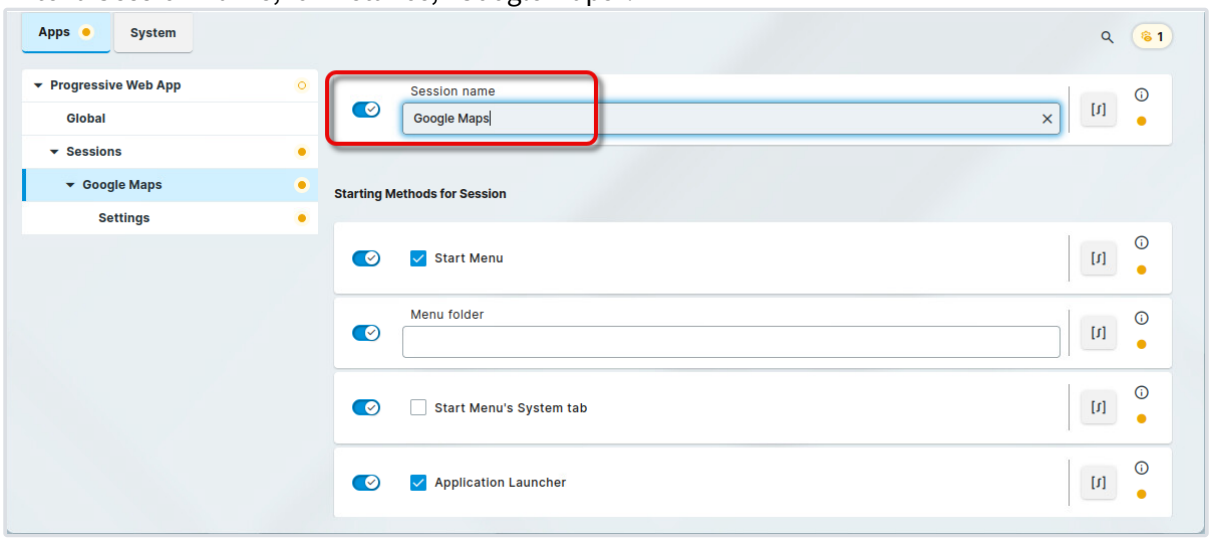
Creating a Session

1. In the IGEL UMS, create a profile configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[184].
2. In the profile configurator, go to **Apps > Progressive Web App > Sessions** and add a new session.

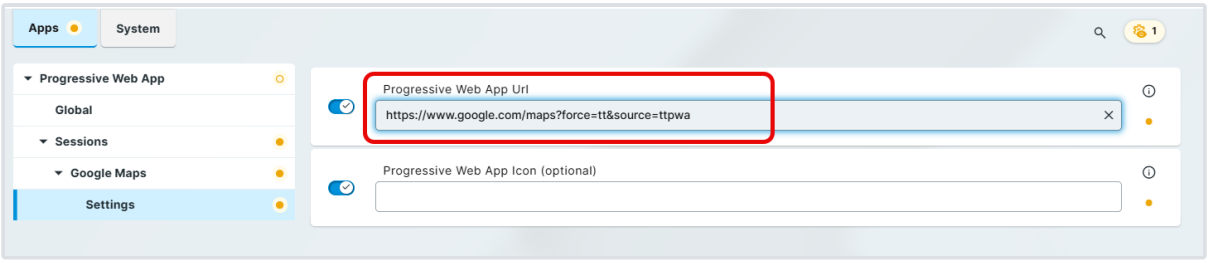
184. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-



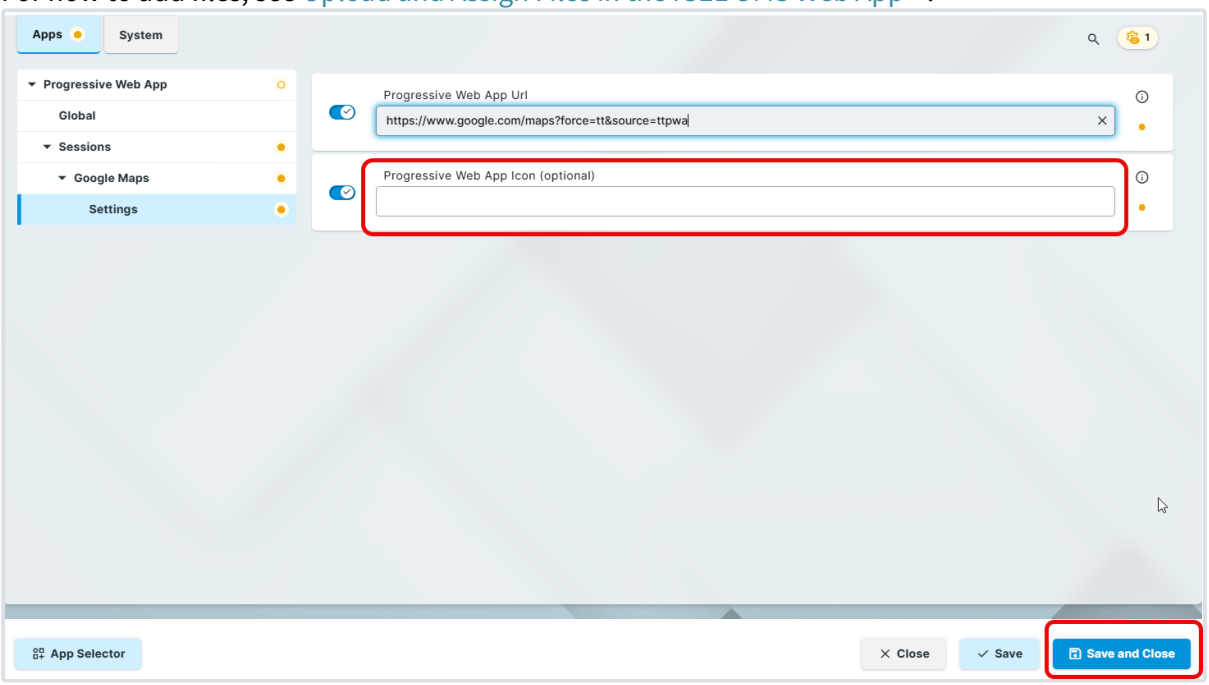
3. Enter a **Session name**, for instance, “Google Maps”.



4. Go to **Settings** and enter the **Progressive Web App Url**. This is the **manifest_id** you discovered via `chrome://web-app-internals`. For Google Maps, the correct value is `https://www.google.com/maps?force=tt&source=ttpwa`



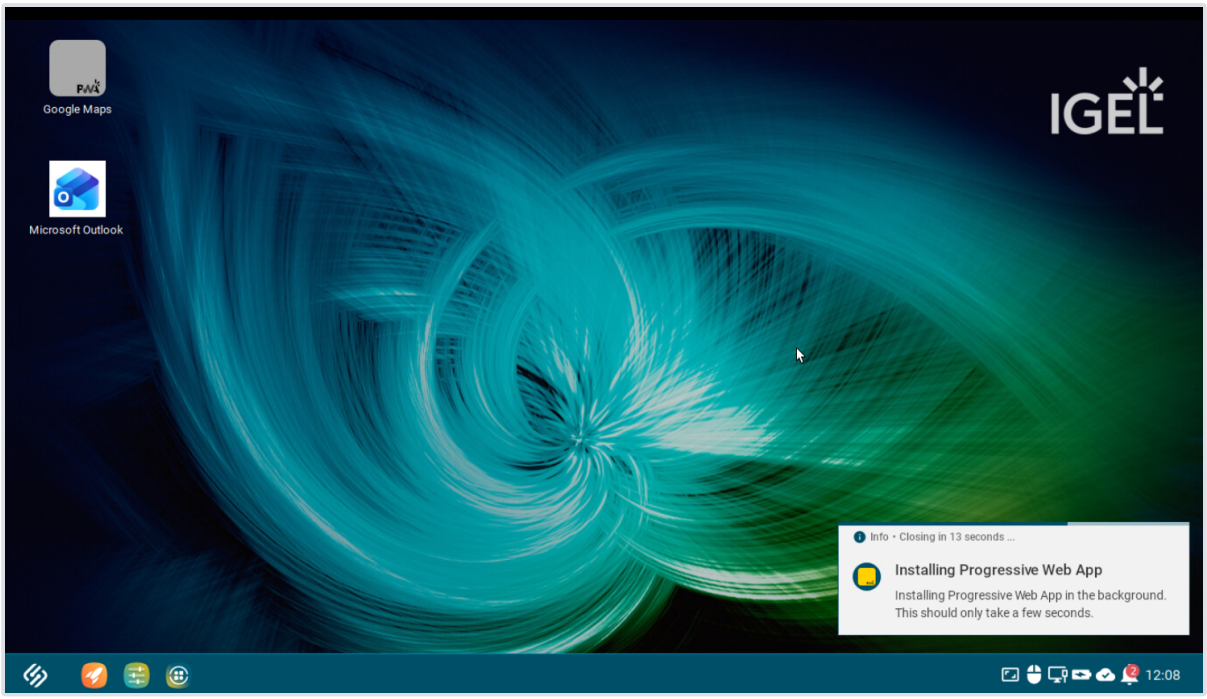
5. Optional: If you want to use an alternative icon, enter the path to the image file under **Progressive Web App Icon (optional)**. This will override any auto-detected icons coming from the PWA itself. For how to add files, see Upload and Assign Files in the IGEL UMS Web App[185].



6. Save the profile and assign it to the required devices / device directories. For details on profile assignment, see How to Create and Assign Profiles in the IGEL UMS Web App[186].

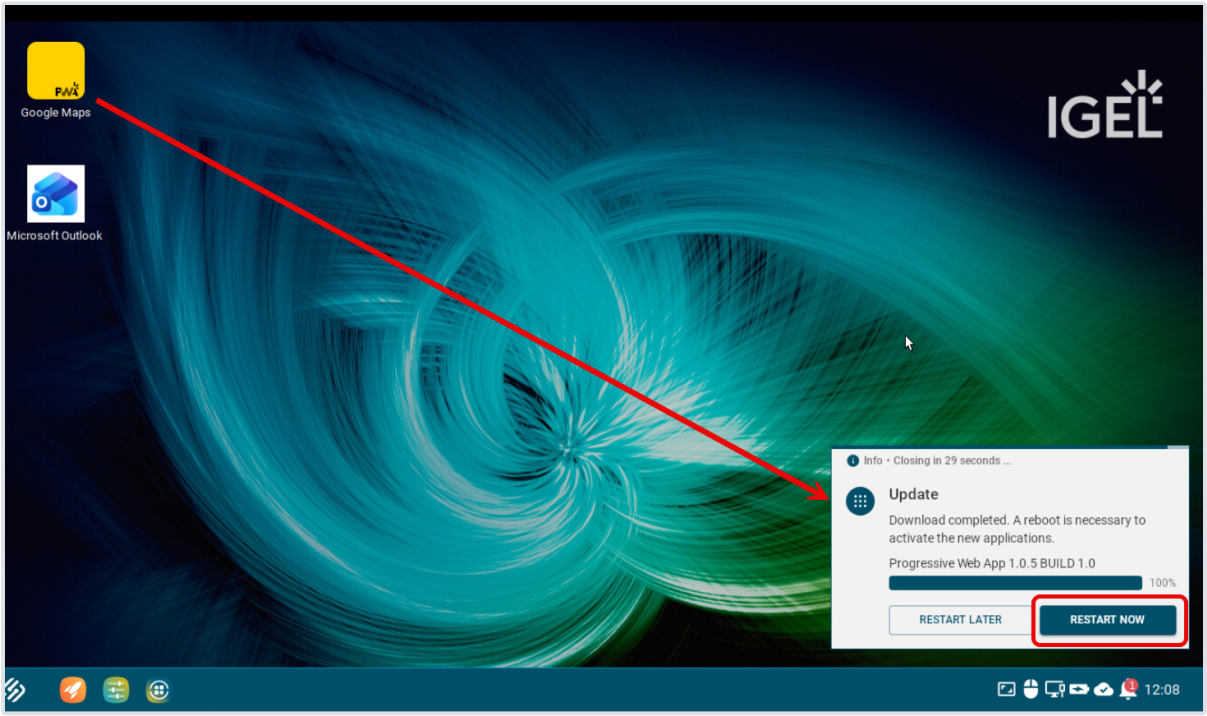
   On the device, a message window informs the user that the Progressive Web App is being installed. Note that the user has to be logged in to the device for this step.

185. https://kb.igel.com/en/universal-management-suite/current/upload-and-assign-files-in-the-igel-ums-web-app
186. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-

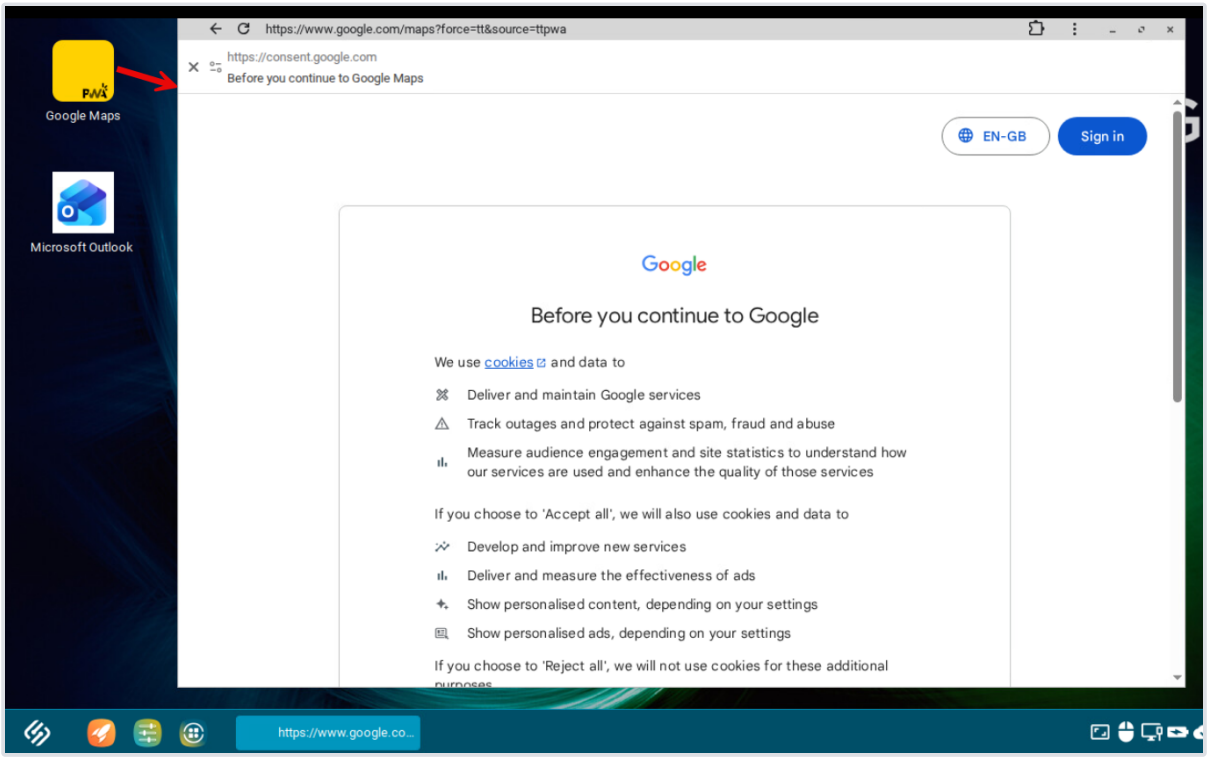


Completing the Installation

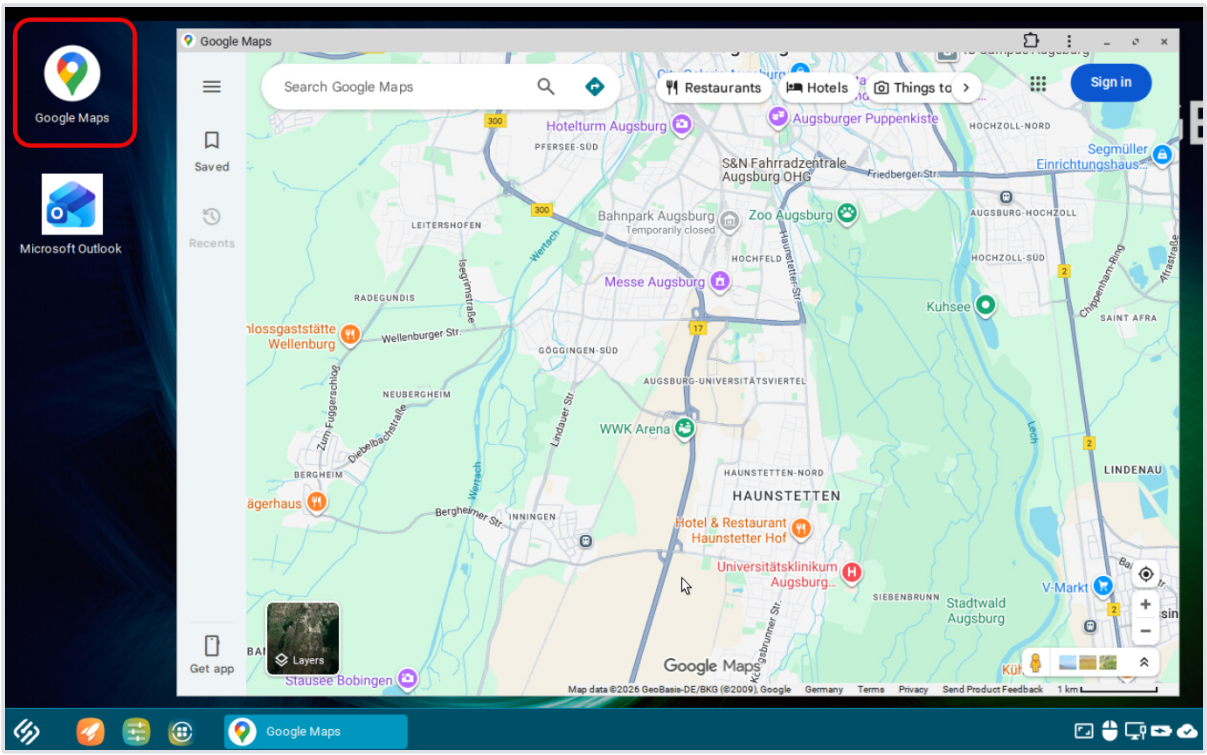
1. After the app download is complete, reboot the device.



2. To complete the installation so that the app icon is displayed correctly, some user action is required: Open the app and resolve the cookie consent dialog / accept the terms of use / log in / etc.
   For Google Maps app, resolving the cookie consent dialog is usually enough for completing the installation.



3. Reboot the device.
   The app icon is now displayed correctly. The app installation process is completed, and the app can be used.



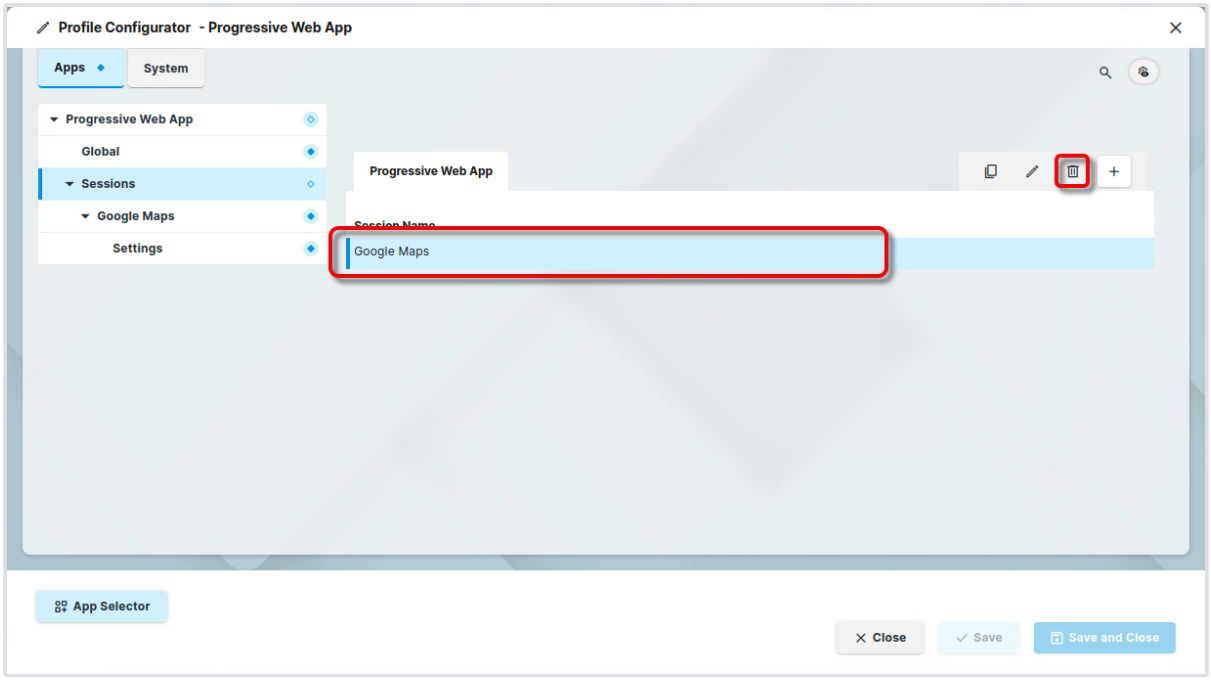
If not all PWAs have been properly installed (e.g. required user actions have not yet been performed), the installation process of Progressive Web App will automatically start in the background after each reboot. The installation process is finished as soon as no icon is grey.

Troubleshooting: Reinstalling the App if Something Went Wrong

If the Progressive Web App does not work as expected, e.g. the starter icon does not appear, it is recommended to reinstall it.

To reinstall a PWA:

1. Start the PWA (or any other PWA).
2. While the PWA window is open, remove the session.



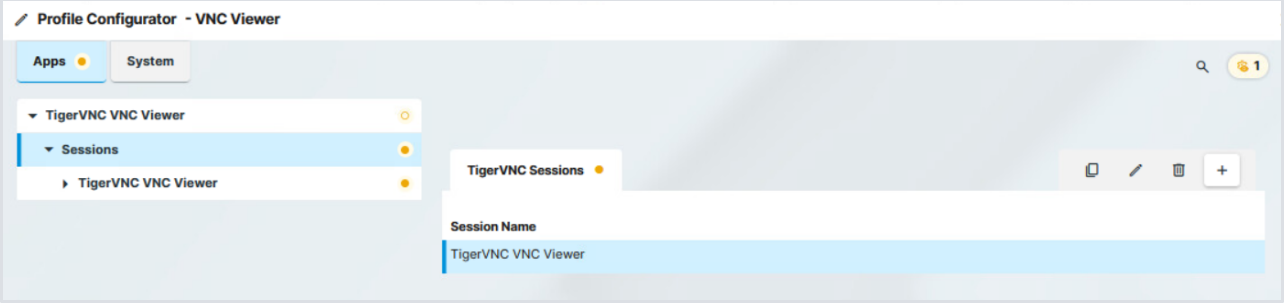
3. Wait for about 1 minute.
4. Install the PWA again as described above under “Creating a Session” and “Completing the Installation”.

TigerVNC VNC Viewer

With the TigerVNC VNC Viewer app, you can access the graphical user interface of a remote computer. In this article you can find how to create and configure the TigerVNC session.

How to Create a Session

1. In the profile configurator, go to **Apps > TigerVNC VNC Viewer > Sessions**.

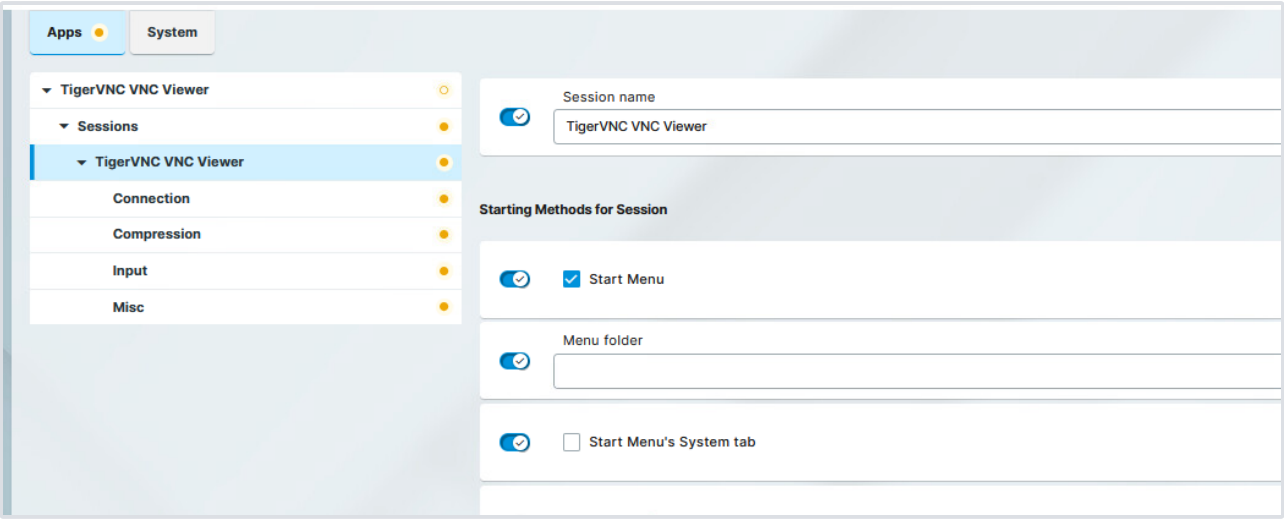


To manage the list of TigerVNC sessions:

- Cick to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

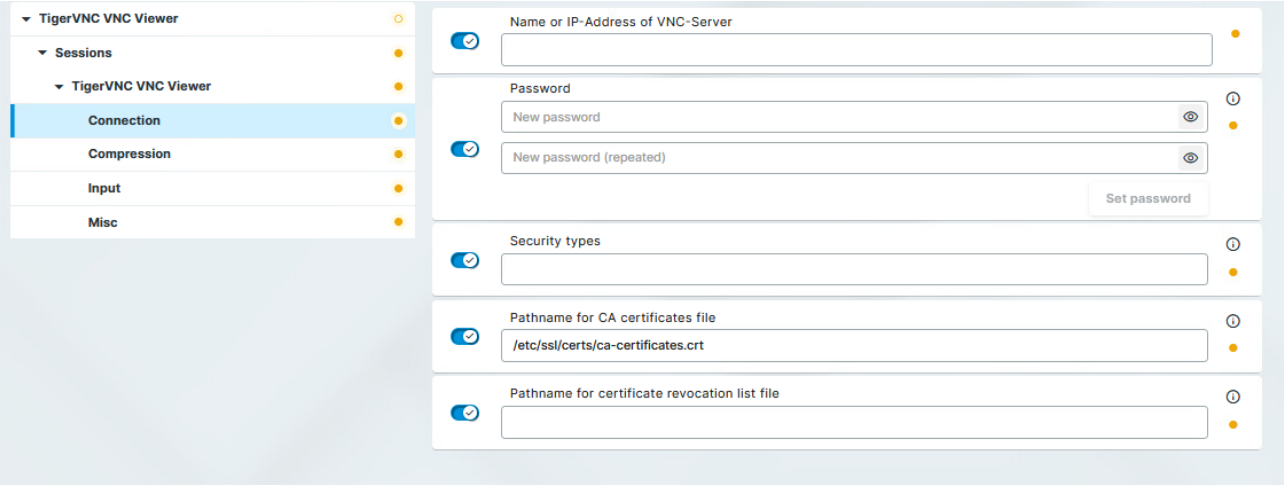
2. Click to create a new session.
   The new session is created. The starting methods for the session are described under Starting Methods for Apps[187] .

187. https://kb.igel.com/en/igel-os-base-system/12.6.1/starting-methods-for-apps



Configuring the TigerVNC session

Configuring the Connection



You have the following options to configure the VNC connection under **Apps > TigerVNC VNC Viewer > Sessions > Session name > Connection**:

Name or IP address of VNC server

Host name or IP address of the VNC server

Password

User password for logging on to the VNC server, if necessary

Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Security types

Comma separated list of VNC security types to use. Leave empty for default. (Default: TLSVnc, VncAuth)

Possible values:

- **X509Plain**
- **TLSPlain**
- **TLSVnc**
- **X509None**
- **TLSNone**
- **RA2**
- **RA2_256**
- **RA2ne_256**
- **VncAuth**
- **None**

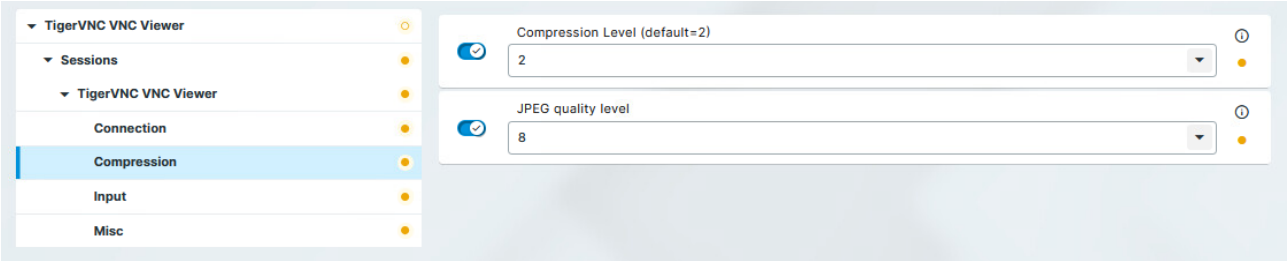
Pathname for CA certificates file

Used for X509* security types. File can contain one or more concatenated CA certificates in PEM format.

Pathname for certificate revocation list file

Used for X509* security types. File containing CRLs in PEM format.

Setting Compression



You have the following options to configure the compression for the TigerVNC session under **Apps > TigerVNC VNC Viewer > Sessions > Session name > Compression**:

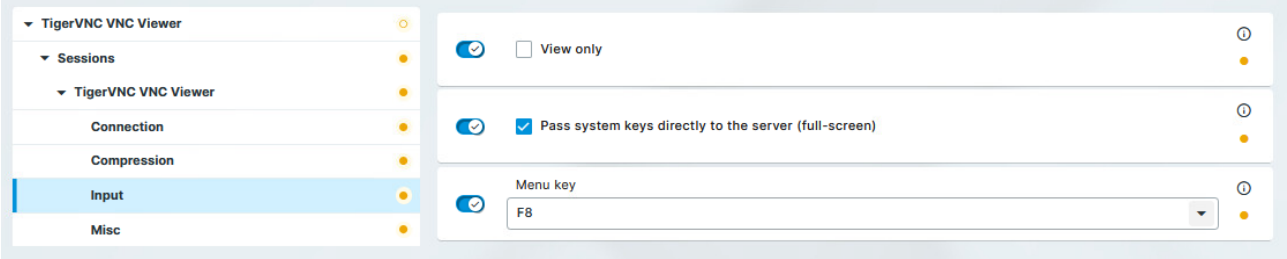
Compression level (default=2)

Allows you to select the compression level; 0 ist the lowest, 9 is the highest compression. (Default: 2)

JPEG quality level

Allows you to select the image quality. 1 means the highest compression and the lowest image quality, 9 means the lowest compression and the highest image quality. (Default: 8)

Configuring Input



You have the following options to configure the input for the TigerVNC session under **Apps > TigerVNC VNC Viewer > Sessions > Session name > Input**:

View only

- ☑ Mouse and keyboard inputs are not forwarded to the remote computer. You can only observe the remote computer.
- ☐ Mouse and keyboard inputs are forwarded to the remote computer. You can remote control the remote computer. (Default)

Pass system keys directly to the server (full-screen)

- ☑ You can use system key combinations in the TigerVNC session, e.g. [Alt] + [Tab]. (Default)
- ☐ System key combinations cannot be used in the TigerVNC session.

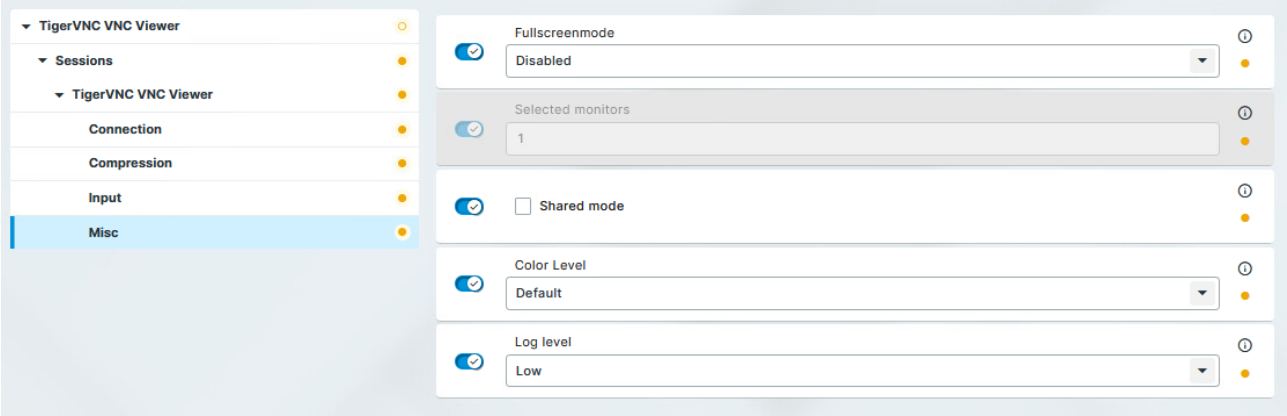
Menu key

Key which brings up the menu
Possible options:

- **F8** (Default)
- **F2 ... F12**
- **Pause**
- **Print**
- **Scroll_lock**
- **Escape**
- **Insert**
- **Delete**
- **Home**
- **Page_up**

- **Page_down**

Misc Settings



You have the following options to configure further settings for the TigerVNC session under **Apps > TigerVNC VNC Viewer > Sessions > Session name > Misc**:

Fullscreenmode

Which monitor to use when in full-screen mode.

Possible options:

- **Disabled**: The session is not shown in full-screen mode, the taskbar is visible. (Default)
- **Current**: The session will be shown in full-screen mode on the currently used monitor. The taskbar is not visible.
- **All monitors:** The session will be shown in full-screen mode on all monitors. The taskbar is not visible.
- **Selected:** The session will be shown in full-screen mode on selected monitors defined under **Selected monitors**. The taskbar is not visible.

Selected monitors

Enter the number of the monitor(s) you wish to use in full-screen mode. You can enter multiple numbers separated by comma, for example, if you would like to use monitor 1 and 3, enter: 1,3

Shared mode

- ☑ When starting a session, other users' sessions with the same server are not terminated. The sessions run alongside each other with equal status.
- ☐ If another user has a TigerVNC session with the same server, the other user's session will be terminated when the session is started. (Default)

Color Level

The color level used in TigerVNC VNC viewer sessions. If the session is running over a small bandwidth connection, the value can be configured to reduce the needed bandwidth.
Possible options:

- **Default**: The highest available color level is used. The TigerVNC VNC viewer automatically selects the level based on the speed of the connection. (Default)
- **Very Low (8 colors)**: The TigerVNC VNC viewer is forced to use the color level regardless of the speed of the connection.
- **Low (64 colors)**: The TigerVNC VNC viewer is forced to use the color level regardless of the speed of the connection.
- **Medium (256 colors)**: The TigerVNC VNC viewer is forced to use the color level regardless of the speed of the connection.

Log level

TigerVNC defines the log level between 0 and 100, with gradually increasing level of detail in the logs. You can configure the level of debug logging using the following options:

- **Quiet**: 0 level logging, without error logs
- **Low**: includes error logs
- **Middle**: includes detailed logs on top of error logs
- **High**: 100 level logging, including all details for debugging

Virtual Background and Blurring for Webcam



You can use the Virtual Background and Blurring for Webcam app to add background blur or a static background image to video calls in IGEL OS 12, even in Unified Communication apps that do not support this natively.

This article describes how to configure the Virtual Background and Blurring for Webcam app in IGEL OS 12.

Prerequisites

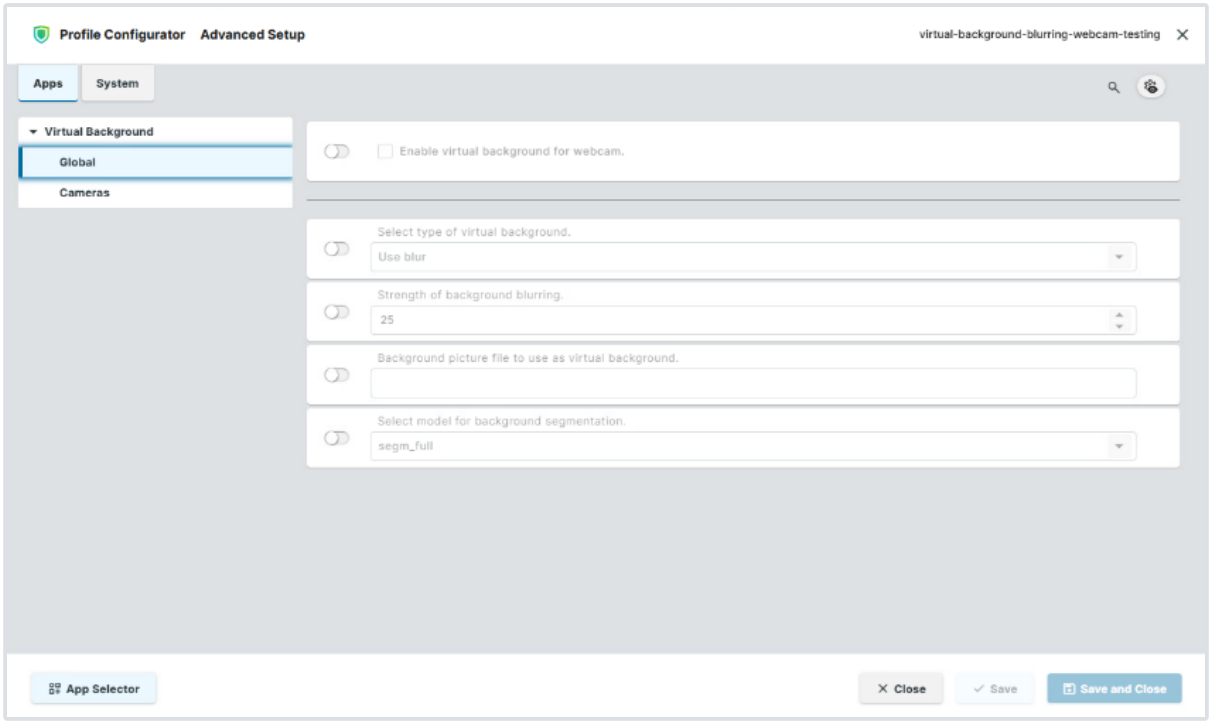
- The Virtual Background and Blurring for Webcam app is imported to your IGEL UMS. For details on app import, see How to Import IGEL OS Apps from the IGEL App Portal[188].

Configuring the Virtual Background and Blurring for Webcam

Global Settings

1. In the IGEL UMS Web App, create a profile for configuring the app. For details on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App[189].
2. In the profile configurator, go to **Apps > Virtual Background > Global**.

188. https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-porta
189. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-

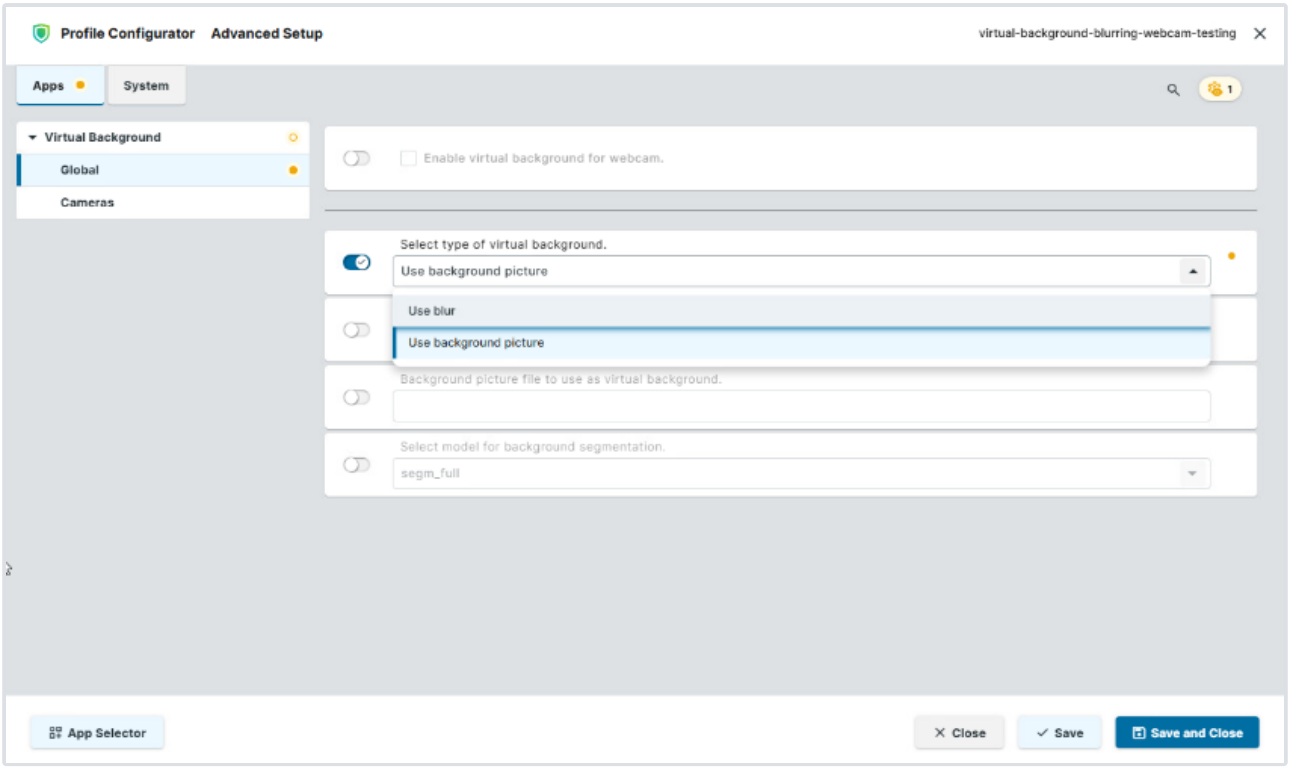


3. Edit the settings according to your needs. The following parameters are available:

Enable virtual background for webcam

- ☑ Enables the virtual background feature. A virtual webcam is created, and the app applies the configured background effect to the video stream before passing it to the Unified Communication client.
- ☐ The virtual background is disabled. (Default)

Select type of virtual background



Defines whether the background is blurred or replaced with a static image.

Possible values:

- **Use blur**: The app blurs the background behind the person. (Default)
- **Use background picture**: The app replaces the background with a static image. Specify the image file under **Background picture file to use as virtual background**.

Strength of background blurring

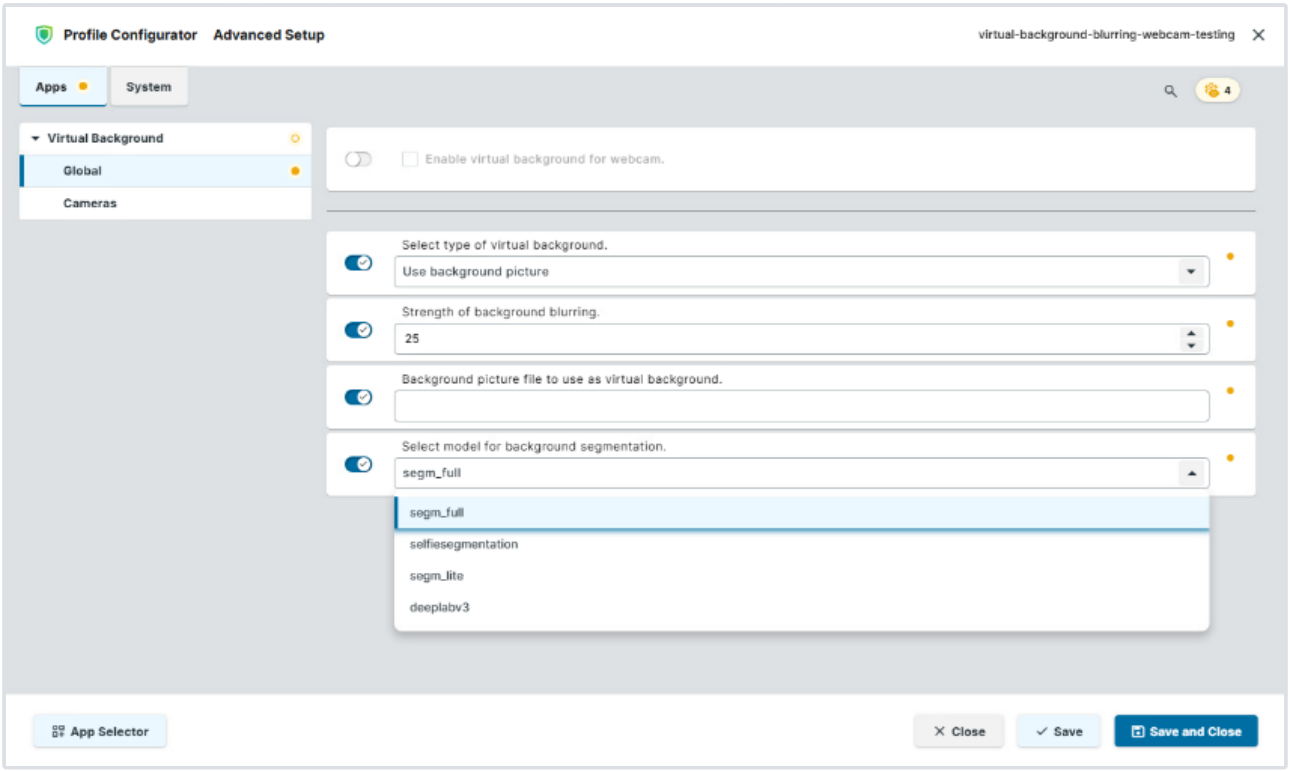
Sets the intensity of the blur effect. Only applies when **Select type of virtual background** is set to **Use blur**.

Range: 1 (minimal blurring) ... 100 (maximal blurring). (Default: 25)

Background picture file to use as virtual background

Path to the image file used as the replacement background. Only applies when **Select type of virtual background** is set to **Use background picture**.

Select model for background segmentation



The AI model that detects and separates the person from the background. Different models offer different trade-offs between accuracy and performance.

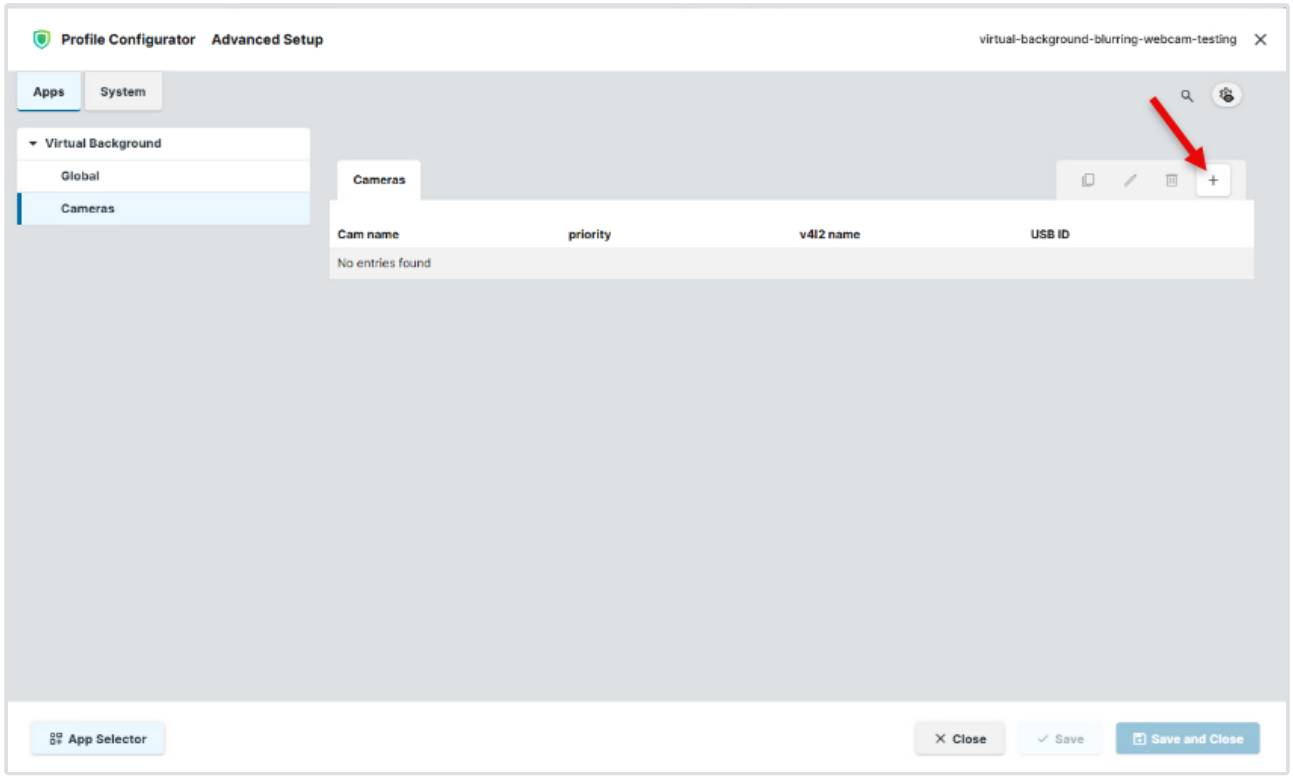
Possible values:

- **segm_full**: Full segmentation model with the highest accuracy. (Default)
- **selfiesegmentation**: Optimized for portrait/selfie scenarios.
- **segm_lite**: A lighter version of the full model, with reduced resource usage.
- **deeplabv3**: An alternative segmentation model.

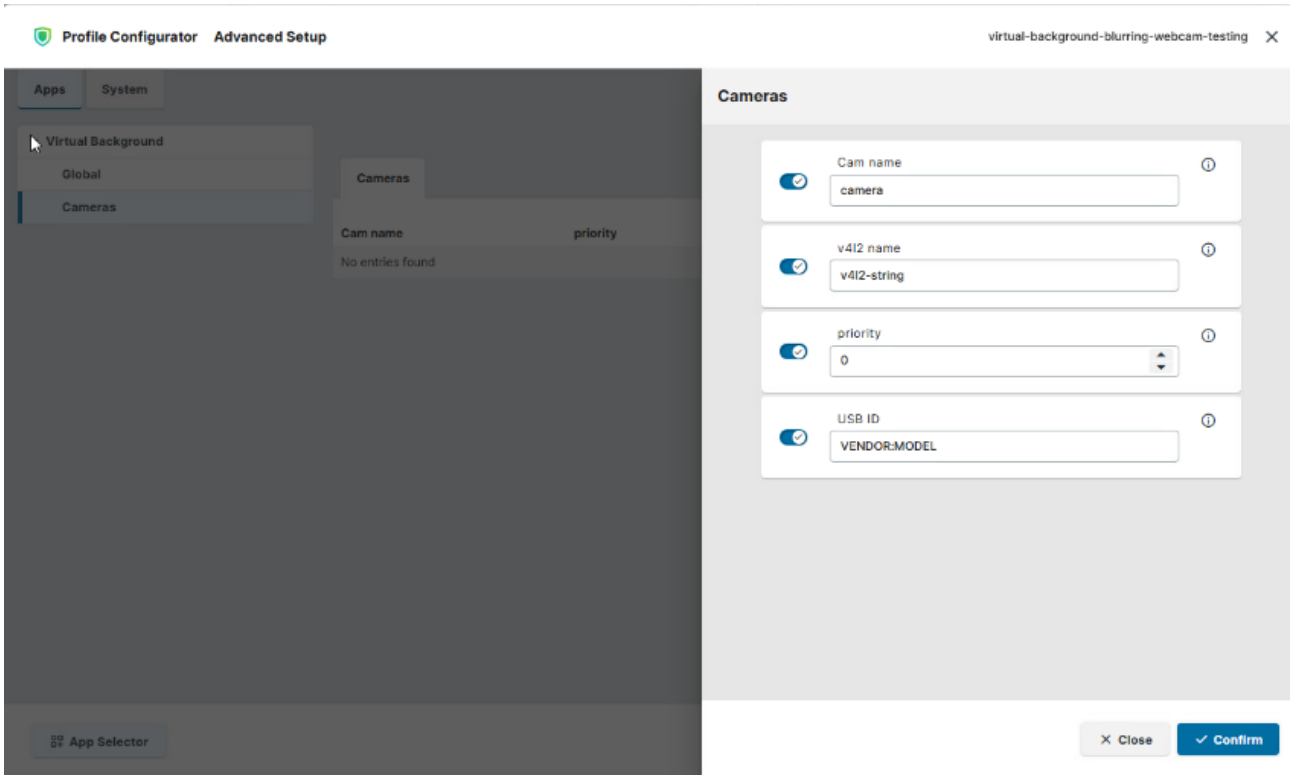
Camera Settings

Here you can define which physical webcam is used as the input source for the virtual webcam. You can add and prioritize multiple cameras.

1. In the profile configurator, go to **Apps > Virtual Background > Cameras**.
2. Click the **+** sign to add a camera entry.



The following fields are available when adding a camera entry:



Cam name

A descriptive name to identify the camera entry within the configuration. (Default: camera)

v4l2 name

The Video4Linux2 (v4l2) device name of the webcam to use. To retrieve the v4l2 name of a connected webcam, run the command `v4l2-ctl --list-devices` on the endpoint. (Default: v4l2-string)

priority

The priority of this camera entry relative to others in the list. Lower numbers indicate higher priority. If the camera with the highest priority is not available, the camera with the second highest priority is used as a fallback. (Default: 0)

USB ID

The USB vendor and product ID of the webcam, in the format `<VENDOR>:<MODEL>`. (Default: VENDOR:MODEL)

To retrieve this information, run the command `lsusb` on the endpoint and note the ID string after the `ID` field.

- Example: if the output of `lsusb` shows `Bus 001 Device 006: ID 045e:0810 Microsoft Corp. LifeCam HD-3000`, the string to enter is `045e:0810`.

Distributing the App

→ Save the profile and assign it to the required devices. For details on profile assignment, see How to Create and Assign Profiles in the IGEL UMS Web App[190].

190. https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums-

Zoom Media Plugins for VDI

- Getting Started with the Zoom Media Plugins for VDI on IGEL OS (see page 506)

Getting Started with the Zoom Media Plugins for VDI on IGEL OS

> **Zoom Media Plugins for VDI Version 5.13 Required for IGEL OS 12.01.100 or Higher**
>
> Make sure to select version 5.13 of the Zoom Media Plugins for VDI. Version 5.11 and 5.12 will not work with IGEL OS 12.01.100 or higher.

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

Installation

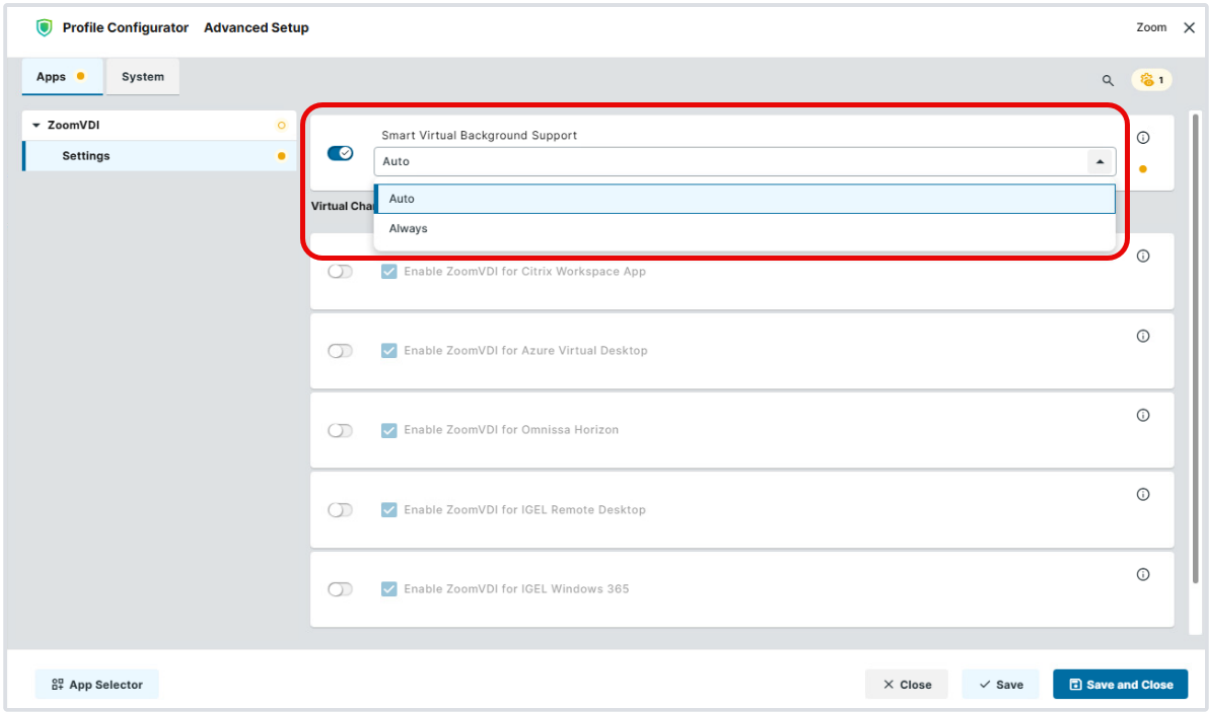
As the Zoom Media Plugin for VDI handles multimedia redirection but is not a standalone application, it cannot be used on its own. At least one of the following apps must be installed and configured as well:

- Citrix Workspace App
- IGEL Azure Virtual Desktop
- Omnissa Horizon Client
- IGEL Remote Desktop
- IGEL Windows 365

How to Configure the Smart Virtual Background

You can define whether the Smart Virtual Background feature can be activated by the user.

1. In the profile configurator, go to **Apps > ZoomVDI > Settings > Smart Virtual Background Support**.

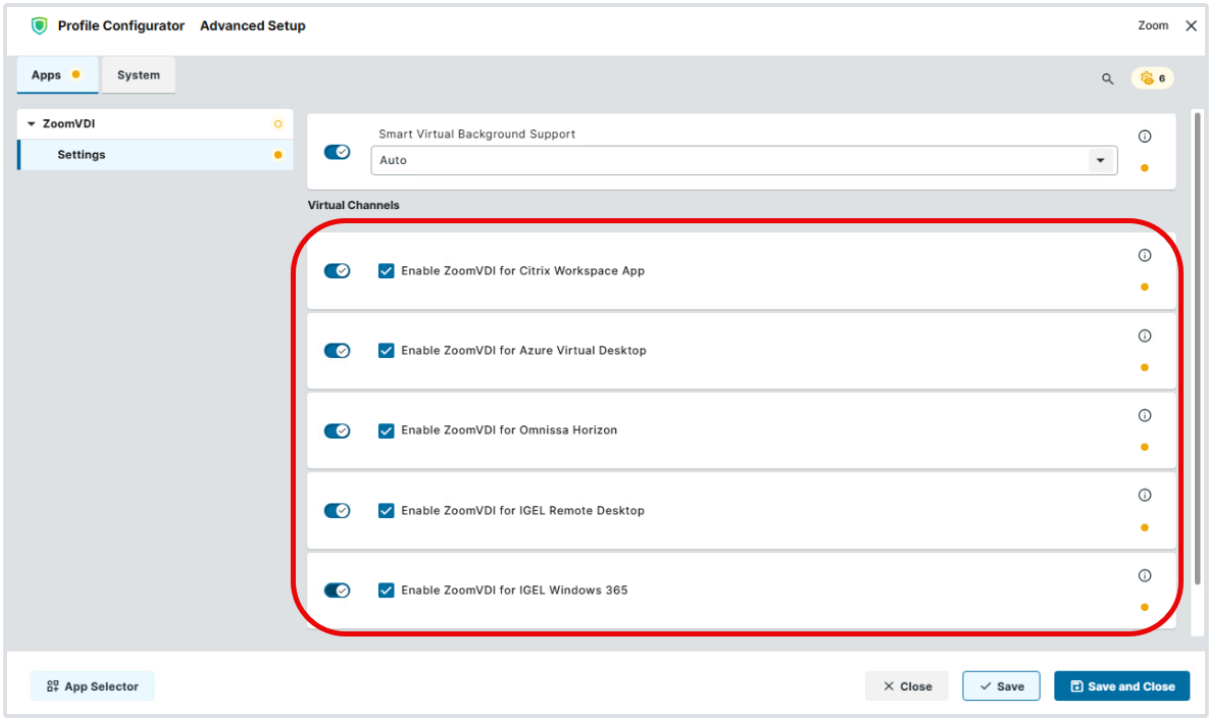


2. Select the desired option and save your changes.
   - **Auto**: The system checks whether the hardware supports the Smart Virtual Background feature. If this is the case, the feature can be activated. (Default)
   - **Always**: Smart Virtual Background can be activated irrespective of the hardware.

How to Disable Zoom Media Plugins for Specific Sessions

1. In the profile configurator, go to **Apps > ZoomVDI > Settings**.

2. Deactivate Zoom VDI for the sessions in question and save your settings.


Profile Configurator
Advanced Setup
Zoom
Apps
System
ZoomVDI
Settings
Smart Virtual Background Support
Auto
Virtual Channels
Enable ZoomVDI for Citrix Workspace App
Enable ZoomVDI for Azure Virtual Desktop
Enable ZoomVDI for Omnissa Horizon
Enable ZoomVDI for IGEL Remote Desktop
Enable ZoomVDI for IGEL Windows 365
App Selector
Close
Save
Save and Close