IGEL OS Base System

IGEL OS 12 is installed in the form of the IGEL OS Base System app.

Installation and Update

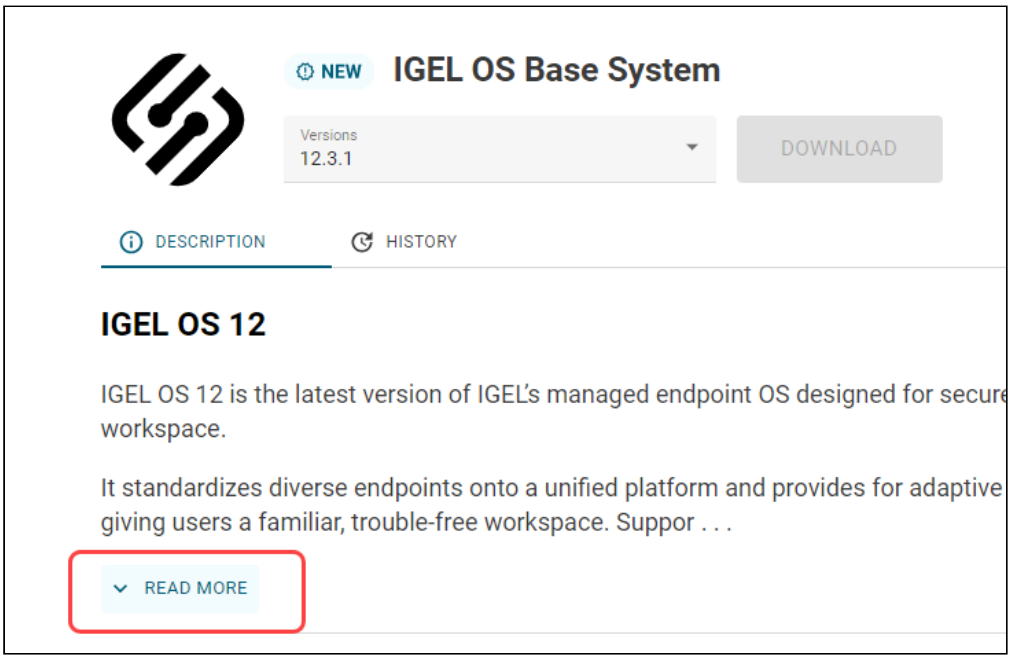
The Base System app can be installed on the devices through explicit app assignment in the IGEL Universal Management Suite (UMS) Web App. For more information on explicit app assignment, see IGEL UMS 12: Basic Configuration and How to Assign Apps to IGEL OS Devices via the UMS Web App.

You can find information on how to update the Base System app in IGEL UMS 12: App Update.

IGEL OS 12 Release Notes

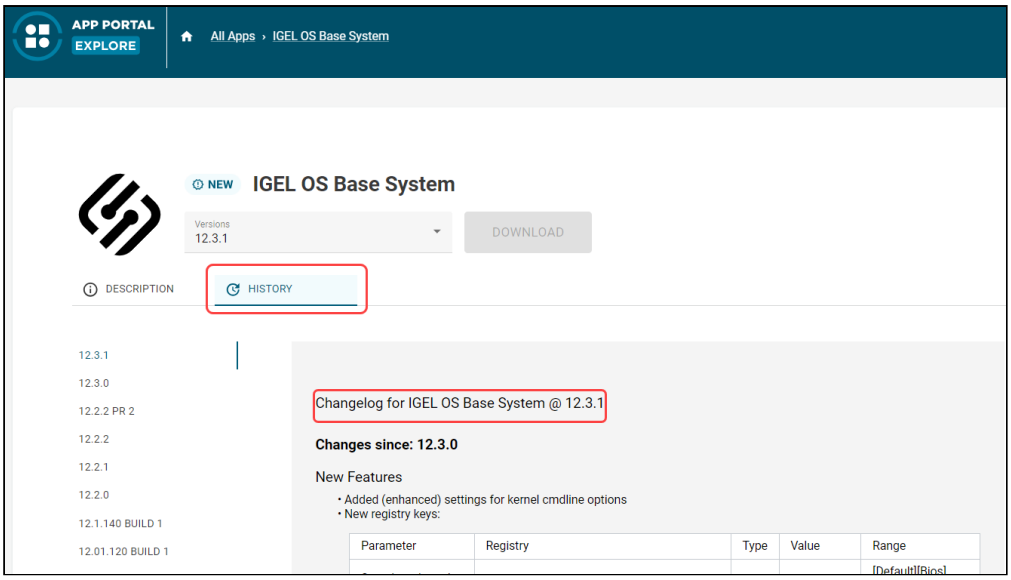
You can find information about the apps and app versions in the IGEL App Portal[1] in the **Description** and **History** tabs of the apps.

The component list of the IGEL OS Base System app can be found in the **Description** tab under **Read More**.



The changelog of the IGEL OS Base System app can be found in the **History** tab.

1 https://app.igel.com/#/



Knowledge Base Articles

- Partner Solutions (see page 4)
- Configuration of IGEL OS 12 Device Settings (see page 6)
- Tray Applications in IGEL OS 12 (see page 353)
- Starting Methods for Apps (see page 376)
- Boot Process (see page 380)
- How to Deploy IGEL OS 12 with IGEL OS Creator (OSC) (see page 385)
- How to Deploy IGEL OS 12 with PXE (see page 411)
- How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on (see page 422)
- How to Use IGEL OS 12 with UD Pocket (see page 443)
- Facilitated Switching between IdPs for Single-Sign On (SSO) In IGEL OS 12.2 (see page 448)
- Upgrading from IGEL OS 11 to IGEL OS 12 (see page 452)
- How to Customize the Unit ID Computation for IGEL OS Creator (OSC) (see page 453)
- How to Configure Single Sign-On (SSO) on IGEL OS 12 (see page 457)
- How to Mitigate Terrapin Vulnerability through Registry Parameter in IGEL OS (see page 496)

Partner Solutions

- Poly Headsets Supported by IGEL OS 12 (see page 5)

Poly Headsets Supported by IGEL OS 12

IGEL OS supports the following Poly (former Polycom/Plantronics) headsets; the headsets have been tested with Microsoft Teams in a Citrix session:

- Blackwire 5220
- Encorepro 320

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

Configuration of IGEL OS 12 Device Settings

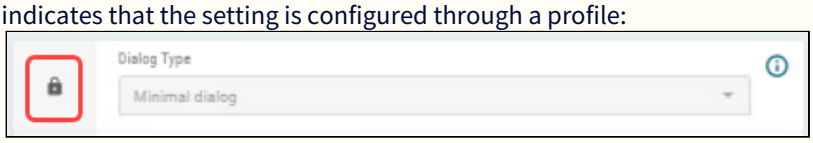
With the help of configurations, you can change the system and session settings of IGEL OS 12 devices both locally on the device and through the IGEL UMS Web App.

Configuration Options

You can use the following configuration methods:

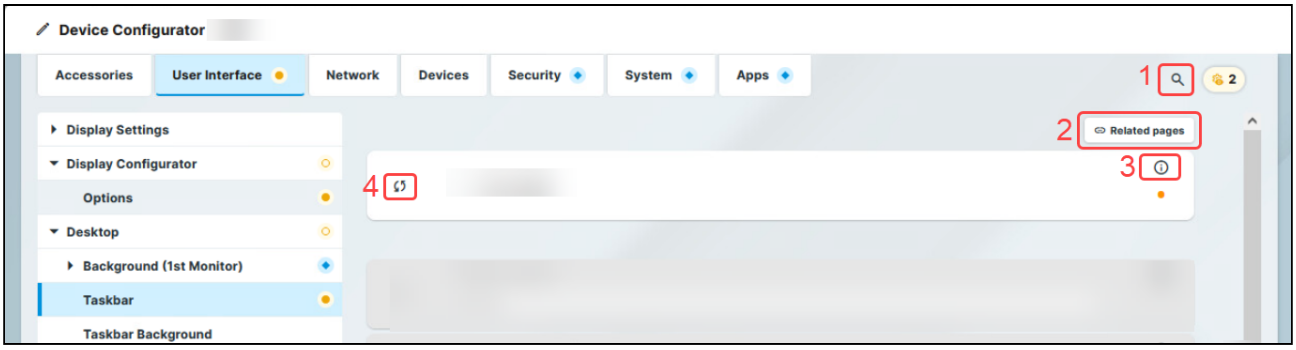
Configuration Method	Description	Opening Options
IGEL Setup	Configurations are made locally on the device. For more information, see IGEL Setup (see page 38).	• Starting methods defined under **Accessories > Setup** • Keyboard command [Ctrl] + [Alt] + [s] • Keyboard command [Ctrl] + [Alt] + [F2] in the Appliance Mode
Device Configurator	The Device Configurator can be opened from the **Devices** area of the UMS Web App. Configurations made here have the same effect as local configurations. For more information, see Devices - IGEL UMS Web App.	• Double clicking on the device name • Clicking the **Edit Configuration** button • Selecting **Edit Configuration** command in the context menu of the device
Profile Configurator	The Profile Configurator can be opened from the **Configuration** area of the UMS Web App. Configurations are made through activating parameters to be defined by the profile and then applying the profile to the device. For more information, see Configuration - IGEL UMS Web App.	• Double clicking on the profile name • Clicking the **Edit Configuration** button

⚠ Configurations applied through profiles take precedence and cannot be changed through other configuration methods. In other configuration methods, the parameter is grayed out and a lock symbol indicates that the setting is configured through a profile:



In the Device Configurator, hovering over the lock will display the name of the profile that defines the parameter.

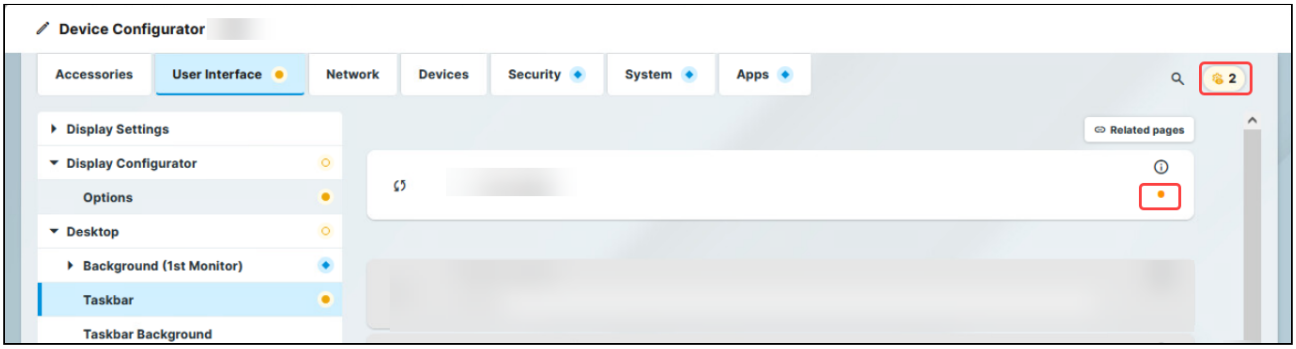
General GUI Elements of the Configurator Dialog



	GUI Element	Description
1	Search for Settings	Clicking the icon opens the **Search for Settings** tab. You can use free text to search for configuration pages and parameter fields. You can also search for registry keys by activating the toggle button for advanced search, and enabling the **Include Registry** option. Clicking on a search result displays the configuration page containing the result. The result is highlighted on the page. When a search result is clicked, the search menu remains displayed in the top right corner with the following navigation options: • arrows to go to the next or the previous search result • search icon to expand the search tab • X to close the search
2	Related Pages	Clicking the icon displays the **Related Pages** tab. The tab displays a list of pages that contain settings related to the settings on the current page.
3	Tooltip	Hovering over the icon displays information about the parameter.

	GUI Element	Description
4	Reset to default	Clicking the icon resets the parameter to the default value. In the Profile Configurator this icon is replaced by the parameter activator: . When you deactivate the parameter, the value will be automatically set back to the default value. For more on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App.

Adjustment Tracking in the Configurator Dialog



The adjustment tracker icon in the top right corner tracks the number of unsaved changes. Clicking the icon opens the **Unsaved adjustments** and the **All adjustments** tabs. The **Unsaved adjustments** tab displays a list of pages that contain unsaved changes. Clicking a page in the list opens the page. The unsaved changes are marked with an orange dot on the right side of the parameter. In the **All adjustments** tab, you find a list of pages that contain saved changes, grouped by tabs.

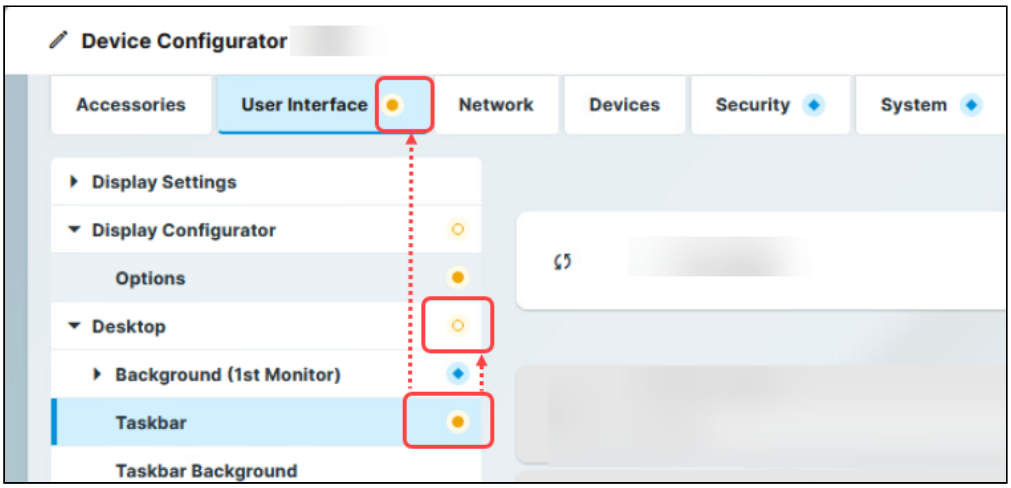
Navigation Tree Highlights

When using the configurator in the IGEL UMS Web App, your changes are marked with the following colored icons in the navigation tree for easier tracking.

	There is an unsaved change in one of the child pages.
	There is an unsaved change in the page. There is an unsaved change in the tab.
	There is a saved template key change in one of the child pages.

	There is a saved template key change in the page. There is a saved template key change in the tab.
	There is a saved change in one of the child pages.
	There is a saved change in the page. There is a saved change in the tab.

The icons marking the type and status of the change have a display priority, with unsaved changes having the highest priority and saved changes having the lowest.
For example, if there is a saved change on one child page and a unsaved change on another child page, the parent page and the tab will be marked for the unsaved change.



Saving Changes and Exiting the Configurator Dialog

You have the following options to save changes and close the configurator:

▶ Click **Save and Close** to save your changes and close the configurator.

▶ Click **Close** if you have not made any changes and would like to abort the configurator. If you have made changes, a confirmation dialog is displayed. In the dialog, you have the following options:

- Click **Discard** to close without saving the changes.
- Click **Save and Close** to save the changes before closing.
- Click **Cancel** to go back and see the list of unsaved changes.

▶ Click **Save** if you have finished configuring a setup area and would like to save your settings without closing the configurator.

Configurator Tabs

Configurations are grouped by function under the following tabs:

- Accessories (see page 11)
- User Interface (see page 48)
- Network (see page 132)
- Devices (see page 208)
- Security (see page 240)
- System (see page 276)

Accessories

In this chapter, you find information on the configuration of accessories in IGEL OS.

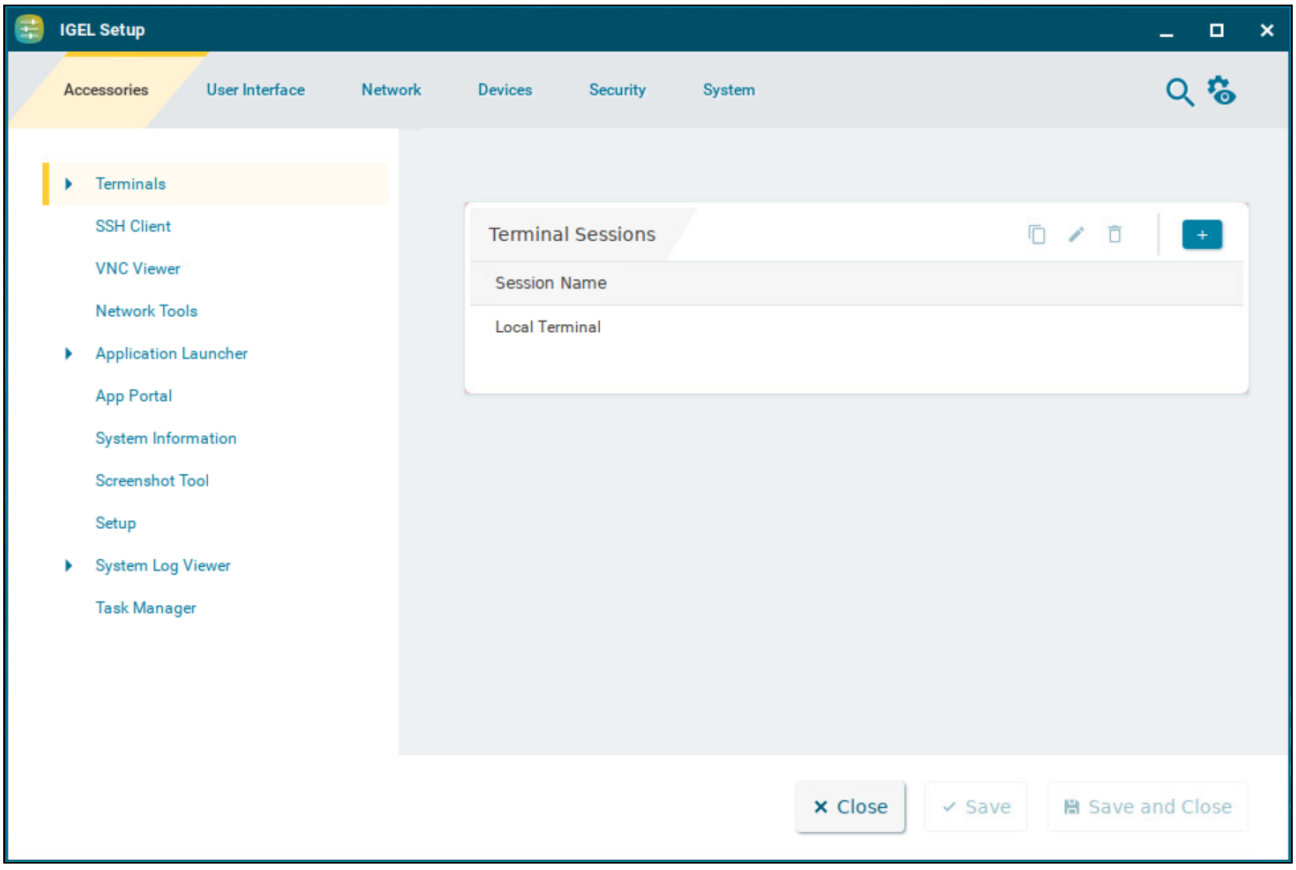
- Terminals (see page 12)
- SSH Client (see page 14)
- VNC Viewer (see page 16)
- Network Tools (see page 24)
- Application Launcher (see page 28)
- App Portal (see page 31)
- System Information (see page 32)
- Screenshot Tool (see page 35)
- Setup (see page 38)
- System Log Viewer (see page 40)
- Task Manager (see page 43)

Terminals

With a local terminal, you can execute local commands on your device. This article shows how to configure the starting methods for terminals, and how to use local terminals in IGEL OS.

> It is also possible to access a local shell without a terminal session: Alternatively, you can switch to the virtual terminals `tty11` and `tty12` by pressing [Ctrl]+[Alt]+[F11]or [Ctrl]+[Alt]+[F12]. Pressing [Ctrl]+[Alt]+[F1] takes you back to the user interface.

Menu path: **Accessories > Terminals**



Terminal Sessions

List of configured local terminal sessions

To manage the list of sessions, proceed as follows:

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

▶ Click to define the starting methods for the session.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using Local Terminal

To use the local terminal, proceed as follows:

1. Start the local terminal.
2. Log in as `user` or `root`.

   > ⚠ If **Use password** is enabled in the **Administrator** area under **Security > Password**, you need to enter the administrator password to access a local terminal as `root`.
   > If an administrator password is set, accessing a local terminal as `user` is only possible if the following two conditions are met:
   > - Access to local terminals has been activated for `user`. This is possible with the registry key `system.security.usershell` under **System > Registry**. The default setting of the registry key forbids terminal access for `user`.
   > - **Use password** is enabled in the **User** area under **Security > Password**.
   >
   > For accessing a local terminal as `user`, the user password has to be entered.
   > For more on password configuration, see Password (see page 245).

3. Enter the shell commands supported by IGEL OS.

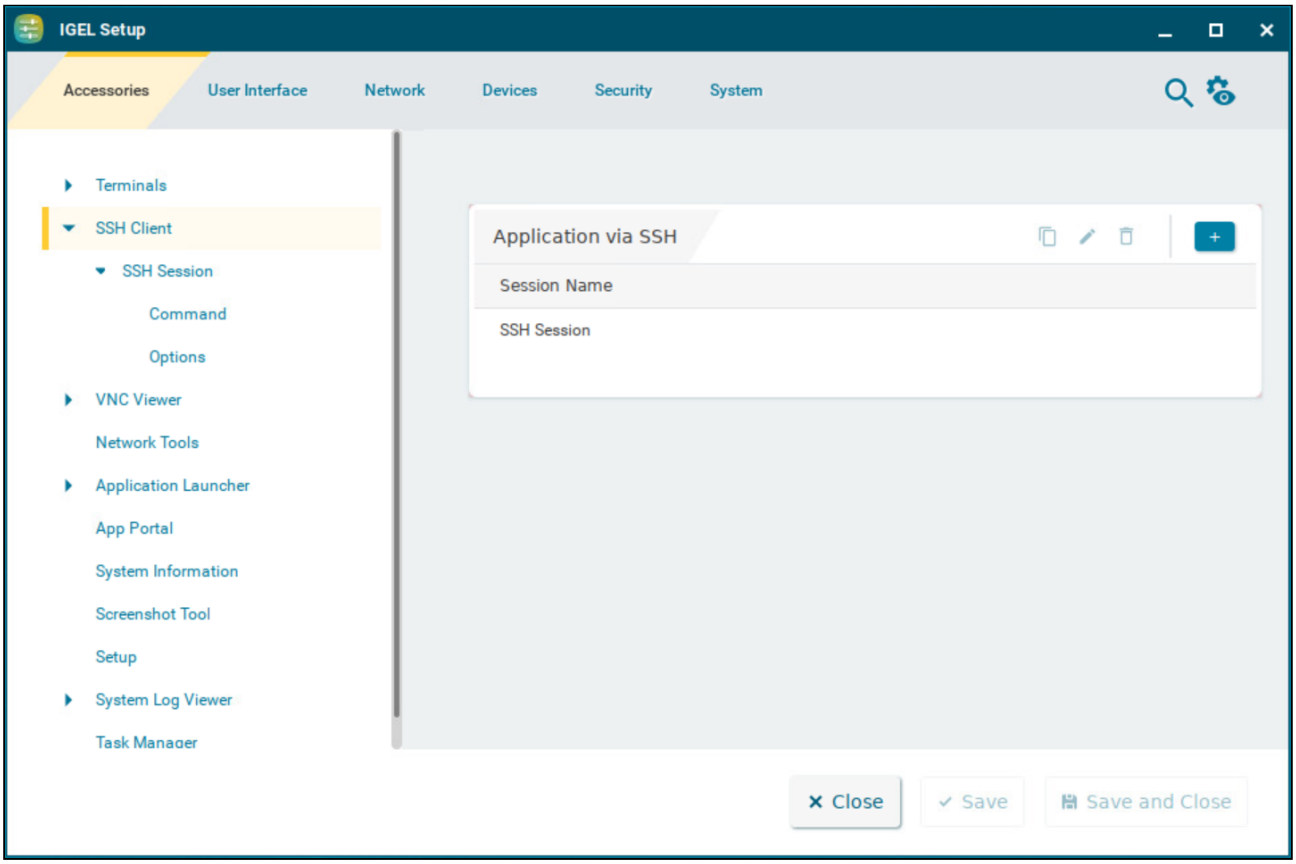
   > ⓘ For a collection of commands supported by IGEL OS, see the IGEL Community cheatsheet[2].

2 https://www.igelcommunity.com/post/igel-os-linux-commands-cheatsheet

SSH Client

You can launch applications on a remote computer via SSH (Secure Shell). The display is usually on the terminal; X11 connections can also be routed via SSH. This article shows how to configure SSH sessions in IGEL OS.

Menu path: **Accessories > SSH Client**



Application via SSH

To manage the list of SSH sessions, proceed as follows:

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

▶ Click to define the starting methods for the session.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Command

Menu path: **SSH Client > [Session Name] > Command**

Here, you can change the following settings:

Remote user name

User name under which the application runs on the remote computer. If left blank, user will be asked for it at session startup.

Remote Host

Host name or IP address of the remote computer.

Command Line

Command which is to be executed on the remote computer immediately after logging in.

Options

Menu path: **SSH Client > [Session Name] > Options**

Here, you can change the following settings:

Enable X11 connection forwarding

☑ X11 applications on the remote computer that are launched via the SSH session will be shown on your device. (Default)

☐ No X11 programs can be launched on the remote computer via the SSH session.

Enable compression

☑ The data will be compressed for transmission.

☐ The data will not be compressed for transmission. (Default)

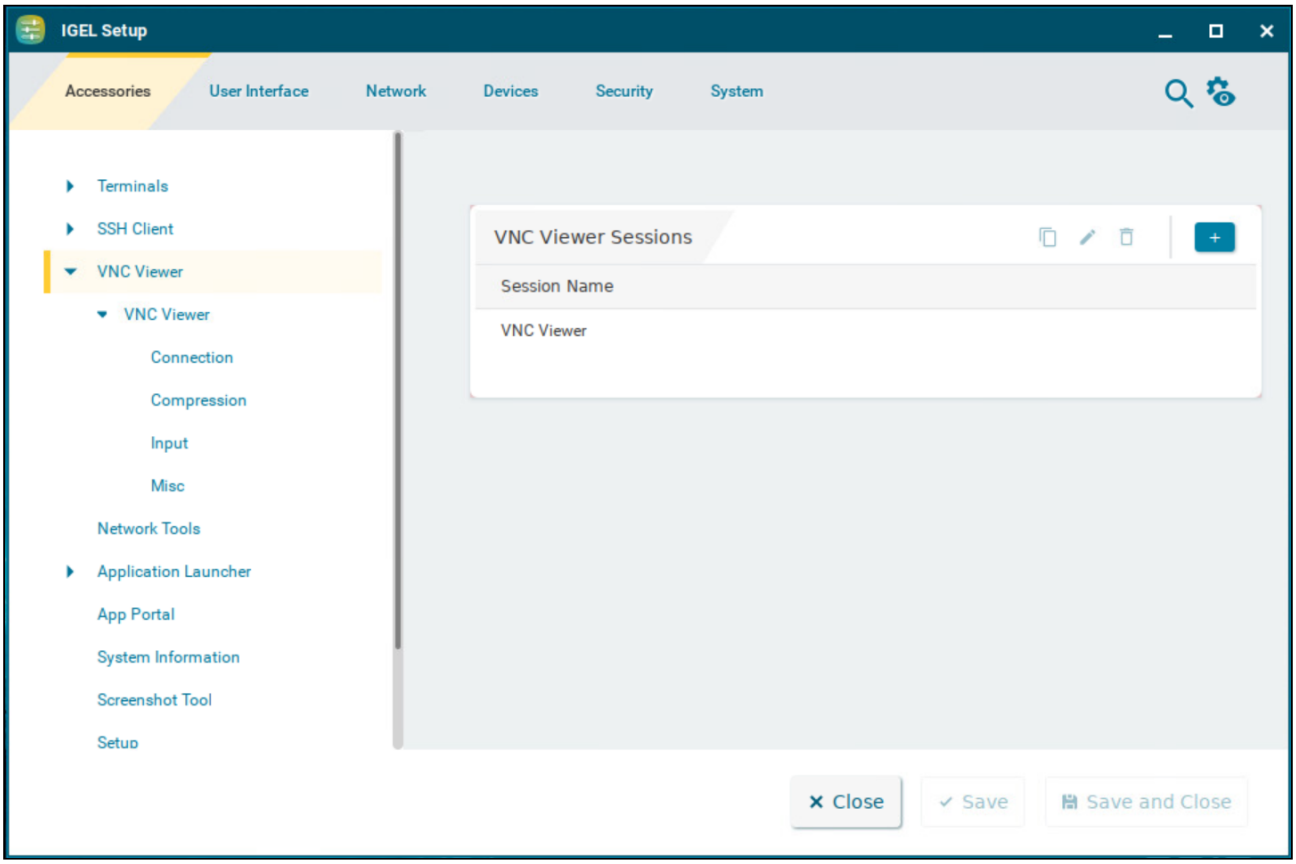
Port

SSH port. (Default: 22)

VNC Viewer

With the VNC viewer, you can access the graphical user interface of a remote computer. This article shows how to configure the starting methods for VNC viewer sessions in IGEL OS.

Menu path: **Accessories > VNC Viewer**



To manage the list of session, proceed as follows:

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

▶ Click to define the starting methods for the session.

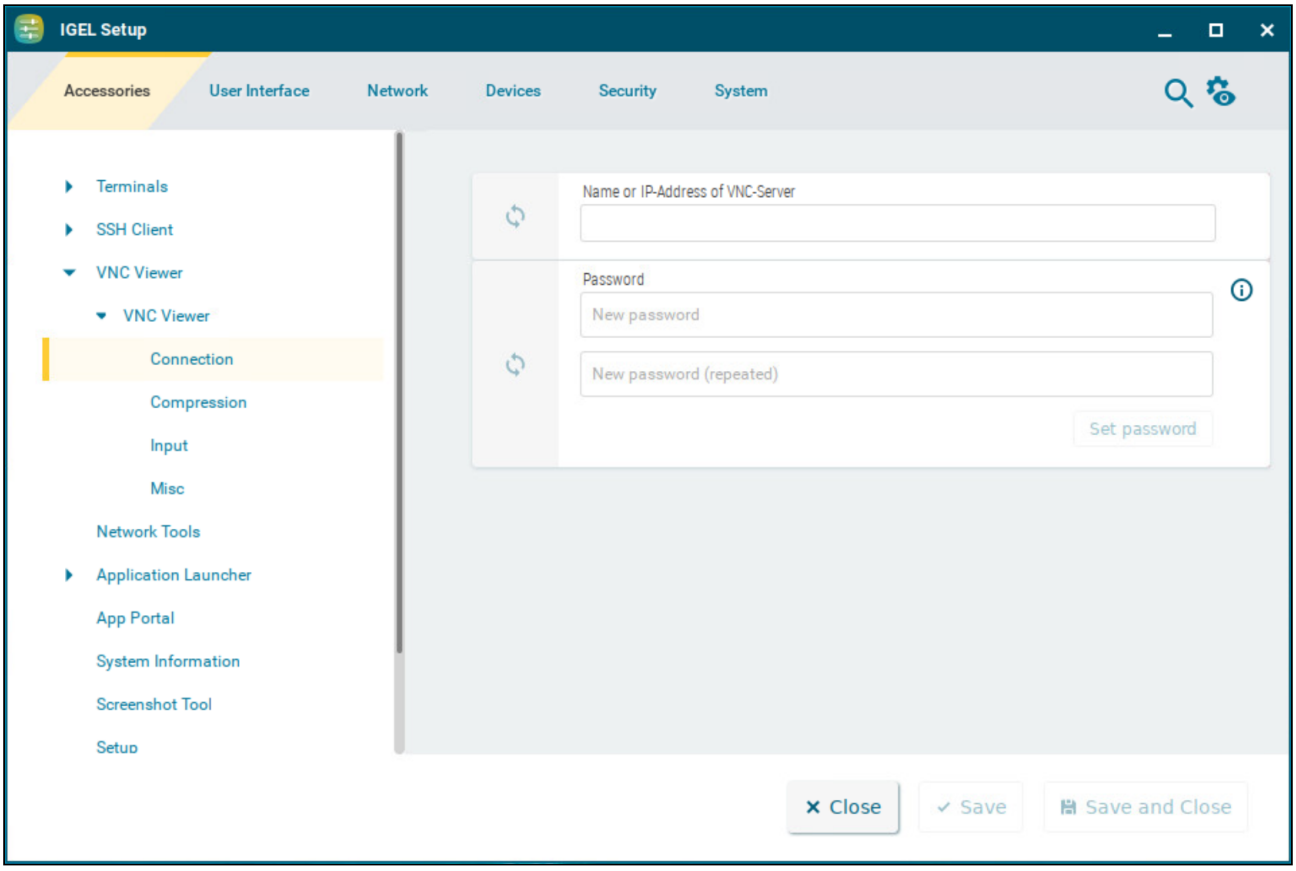
The starting methods parameters are described under Starting Methods for Apps (see page 376).

- Connection (see page 18)
- Compression (see page 19)
- Input (see page 20)
- Misc (see page 22)

Connection

This article shows how to configure the connection for VNC viewer sessions in IGEL OS.

Menu path: **Accessories > VNC Viewer > [Session Name] > Connection**



Name or IP address of VNC server

Host name or IP address of the VNC server

Password

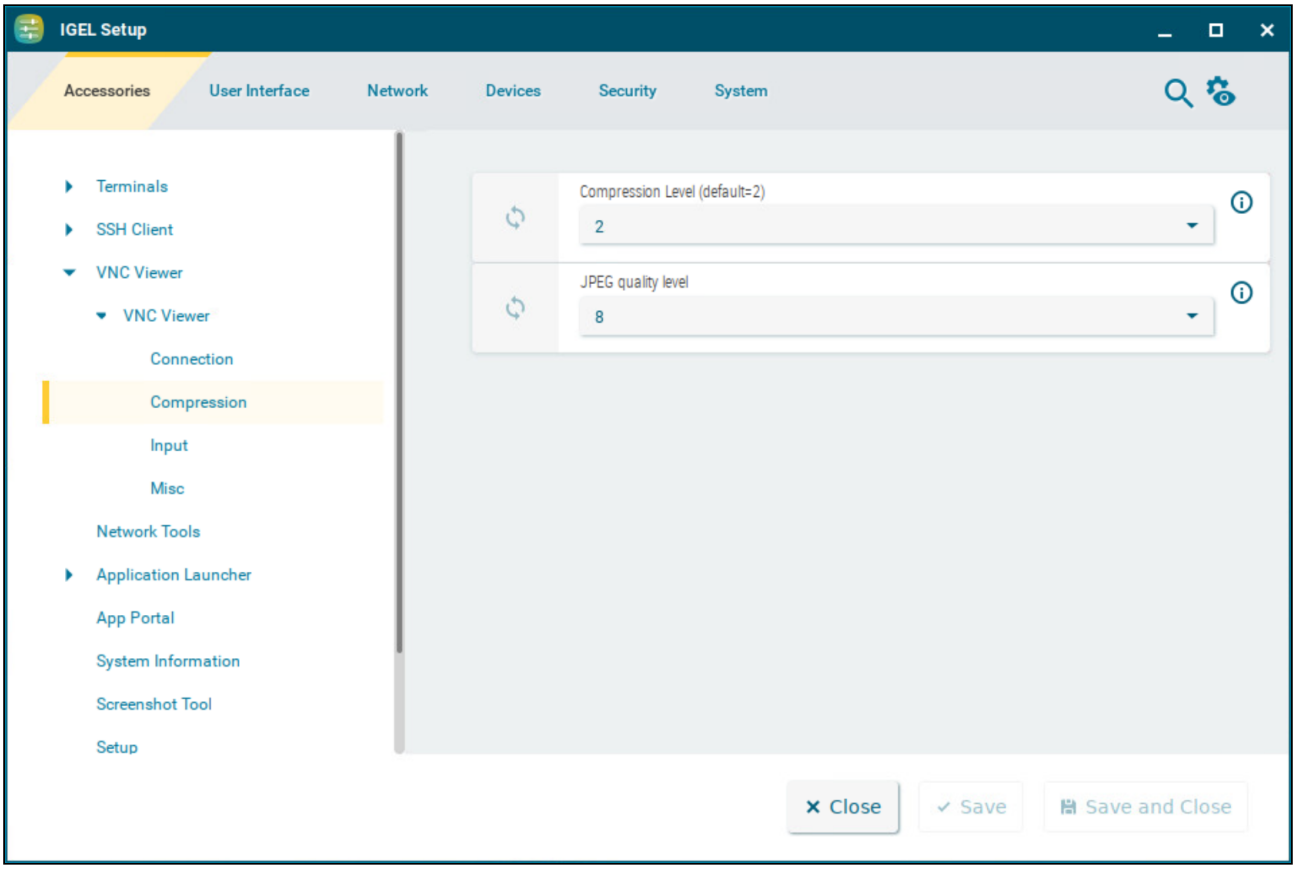
User password for logging on to the VNC server, if necessary

> Session passwords are stored with reversible encryption. Therefore, we strongly recommend not to store the session password on the endpoint device.

Compression

This article shows how to configure the compression for VNC viewer sessions in IGEL OS.

Menu path: **Accessories > VNC Viewer > [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)

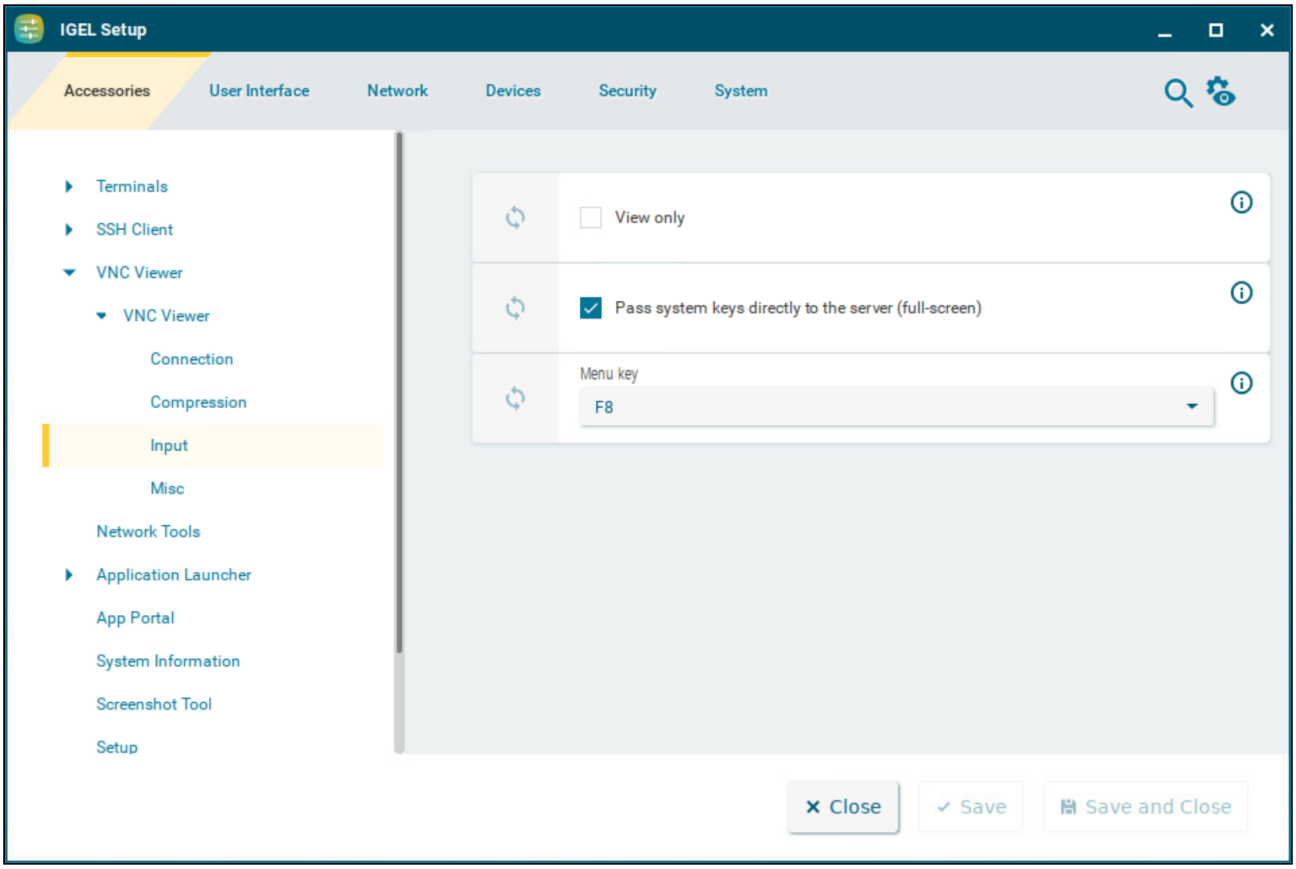
JPEG quality level

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)

Input

This article shows how to configure keyboard input for VNC viewer sessions in IGEL OS.

Menu path: **Accessories > VNC Viewer > [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 VNC session, e.g. [Alt] + [Tab]. (Default)

☐ System key combinations cannot be used in the VNC session.

Menu key

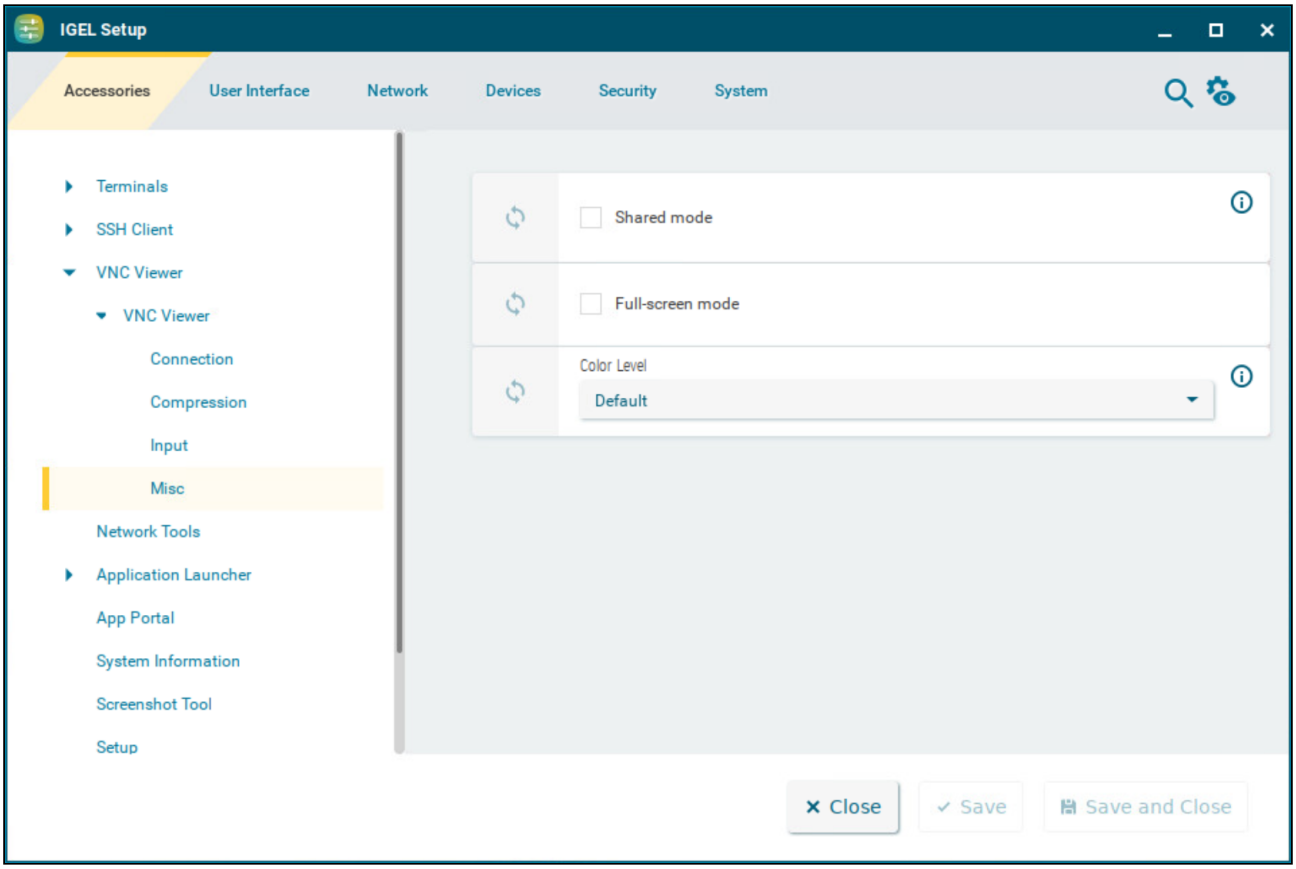
Key which brings up the menu
Possible options:

- **F8** (Default)
- **F2 ... F12**
- **Pause**
- **Print**
- **Scroll_lock**
- **Escape**
- **Insert**
- **Delete**
- **Home**
- **Page_up**
- **Page_down**

Misc

This article shows how to configure session modes and color level for VNC viewer sessions in IGEL OS.

Menu path: **Accessories > VNC Viewer > [Session Name] > Misc**



Shared mode

☑ When starting a session, other users' sessions with the same server are not terminated. The sessions run alongside each other with equal status.

☐ If another user has a VNC session with the same server, the other user's session will be terminated when the session is started. (Default)

Fullscreen mode

☑ The session will be shown in full-screen mode. The taskbar is not visible.

☐ The taskbar is visible. (Default)

Color Level

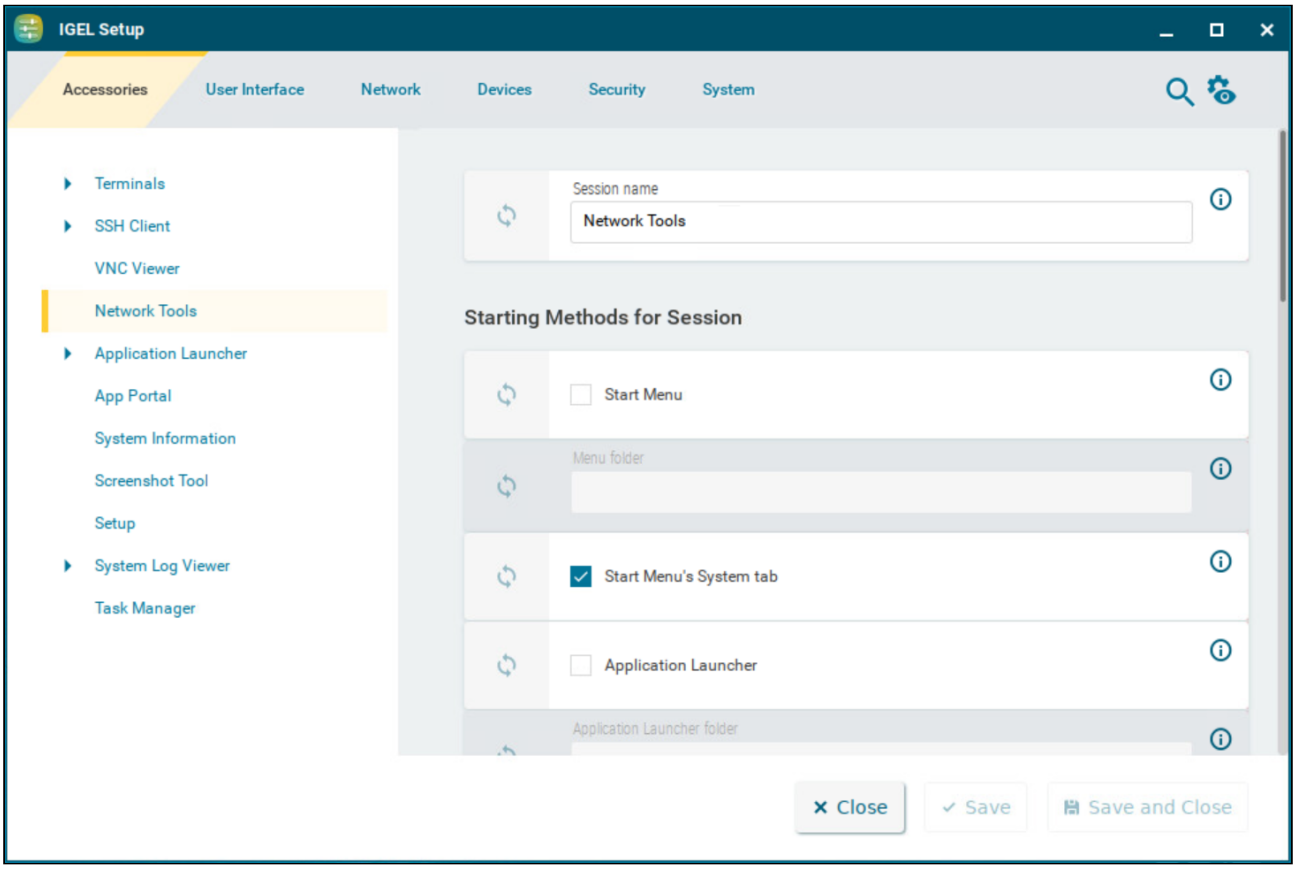
The color level used in VNC viewer sessions. If the session is running over a small bandwidth connection, the value can be configured to reduce the needed bandwidth.
Possible values:

- **Default**: The highest available color level is used. The VNC viewer automatically selects the level based on the speed of the connection. (Default)
- **Very Low (8 colors)**: The VNC viewer is forced to use the color level regardless of the speed of the connection.
- **Low (64 colors)**: The VNC viewer is forced to use the color level regardless of the speed of the connection.
- **Medium (256 colors)**: The VNC viewer is forced to use the color level regardless of the speed of the connection.

Network Tools

This article shows the starting methods configuration and the use of Network Tools in IGEL OS. The tool provides network analysis, for example, Ping, Netstat, Traceroute.

Menu path: **Accessories > Network Tools**



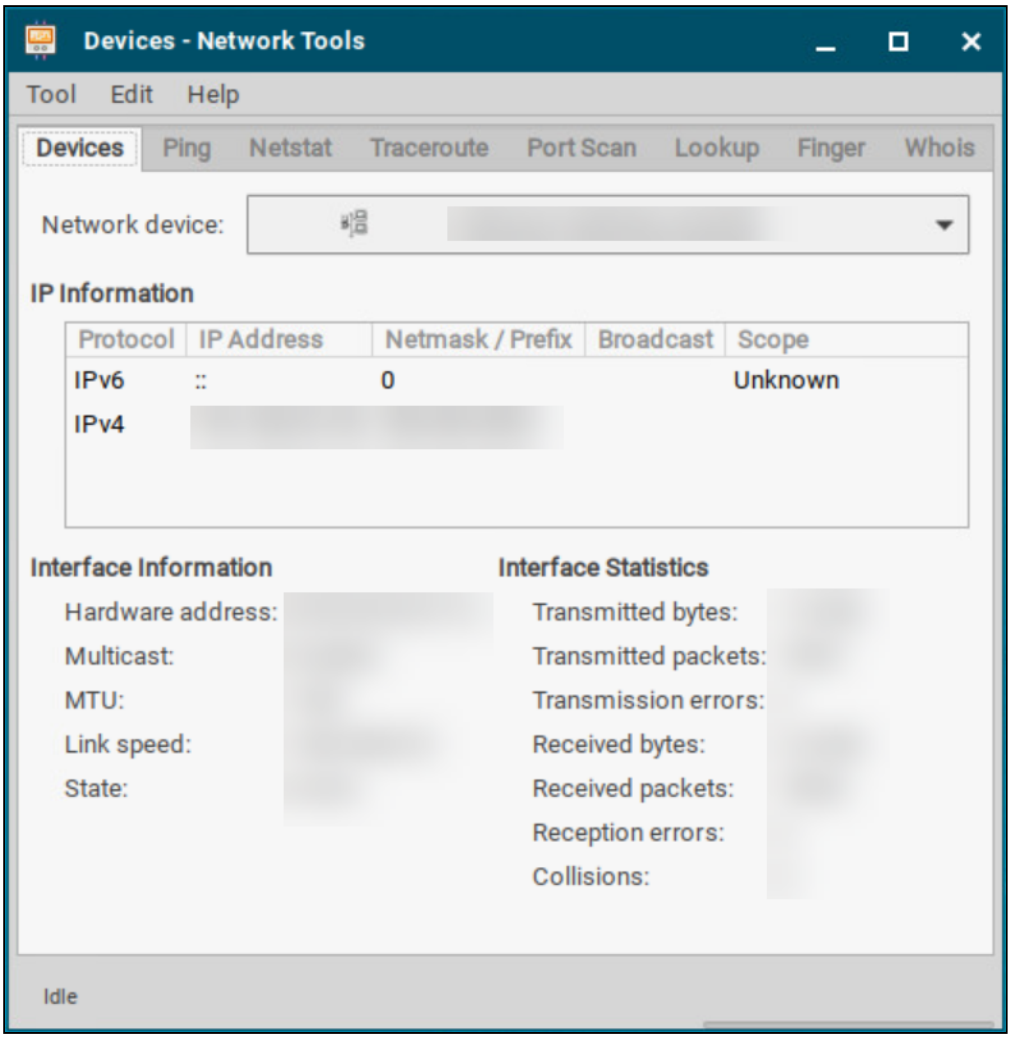
You can configure the starting methods for an easy access of the Network Tool.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

> Starting from OS version 12.3.1, **Password protection** is not configurable and administrator credentials are required to start Network Tools.

Using Network Tools

▶ Start **Network Tools**.



To obtain information regarding a network device available on your device, proceed as follows:

1. Switch to the **Devices** tab.
2. Under **Network device**, select the network device for which you would like to obtain information. The information regarding the selected network device will be shown.

To send a ping query to a device in your network, proceed as follows:

1. Switch to the **Ping** tab.

2. Under **Network address**, enter the IP address or the host name of the device to which you would like to send a ping query.

3. If necessary, add the number of ping queries under **Send**.

4. Click **Ping**.
   The set number of ping queries will be sent. The results will then be shown.

To obtain information regarding the network status of your device, proceed as follows:

1. Switch to the **Netstat** tab.

2. Select the desired information under **Display**:
   - **Routing Table Information**
   - **Active Network Services**
   - **Multicast Information**

3. Click **Netstat**.
   The desired information will be shown.

To identify the router via which an IP data packet from your device reaches a specific target computer, proceed as follows:

1. Switch to the **Traceroute** tab.

2. Under **Network address**, give the IP address of the target computer.

3. Click **Trace**.
   The device will send IP packets to the target computer at short intervals, each with a TTL (Time To Live, i.e. maximum number of hops) increased by 1.
   When the packet reaches the target computer, "reached” will be shown in the last line and no further packet will be sent.
   If no computer replies, "no reply" will be shown.

To obtain DNS information regarding an address on the Internet from your device, proceed as follows:

1. Switch to the **Lookup** tab.

2. Under **Network address**, give the IP address or the host name.

3. Under **Information type**, select which information is to be shown.
   The following information types are available:
   - **Default Information**
   - **Internet Address**
   - **Canonical Name**

- **CPU / OS Type**
- **Mailbox Exchange**
- **Mailbox Information**
- **Name Server**
- **Host name for Address**
- **Text Information**
- **Well Known Services**
- **Any / All information**

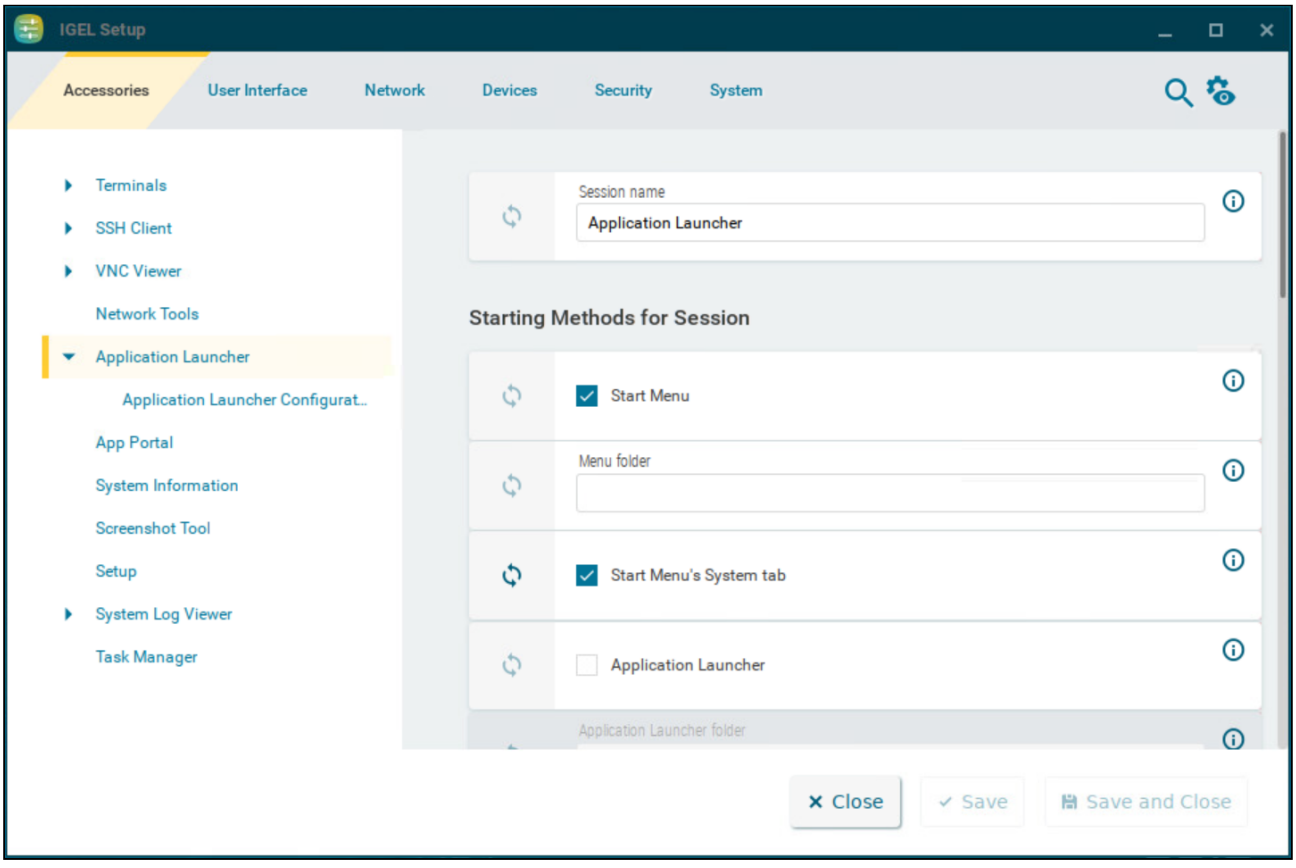
4. Click **Lookup**.
   The desired information will be shown.
   Further information regarding the DNS (Domain Name System) can be found on Wikipedia under Domain Name System[3].
   Detailed descriptions of the Domain Name concept can be found in RFC 1034[4] and in related RFCs.

3 https://en.wikipedia.org/wiki/Domain_Name_System
4 https://tools.ietf.org/html/rfc1034

Application Launcher

With the Application Launcher, you can launch predefined sessions, and device functions and tools. You are also given information regarding the device and the licenses used. This article shows how to configure the Application Launcher in IGEL OS.

Menu path: **Accessories > Application Launcher**

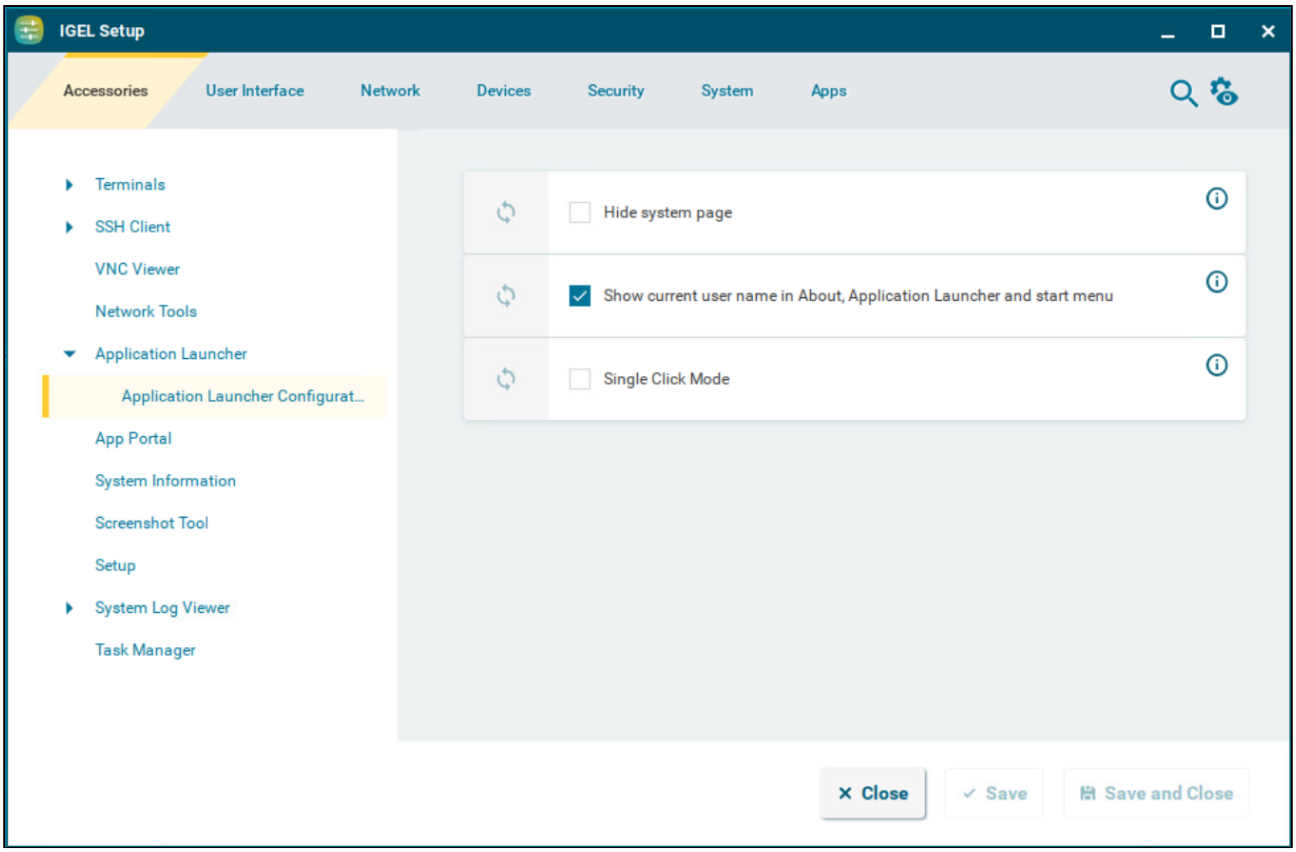


You can configure the starting methods for an easy access of the Application Launcher.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Application Launcher Configuration

Menu path: **Application Launcher > Application Launcher Configuration**



Hide system page

☑ The button for displaying the system tools (accessories) will not be shown.

☐ The button for displaying the system tools (accessories) will be shown. (Default)

Show current user name in About, Application Launcher and start menu

☑ The current user will be shown at the top edge of the relevant window. (Default)

☐ The current user will not be shown.

In order for user names to be recognized and passed on, you must configure two settings beforehand:

- Enable using Active Directory/Kerberos under **Security > Active Directory/Kerberos**. For details, see Active Directory/Kerberos (see page 264)
- Enable local logon under **Security > Logon > Active Directory/Kerberos**. For details, see Active Directory/Kerberos (see page 254)

Single click mode

☑ Sessions are started with a single-click. Recommended for users of touchscreen monitors.

☐ Sessions are started with a double-click. (Default)

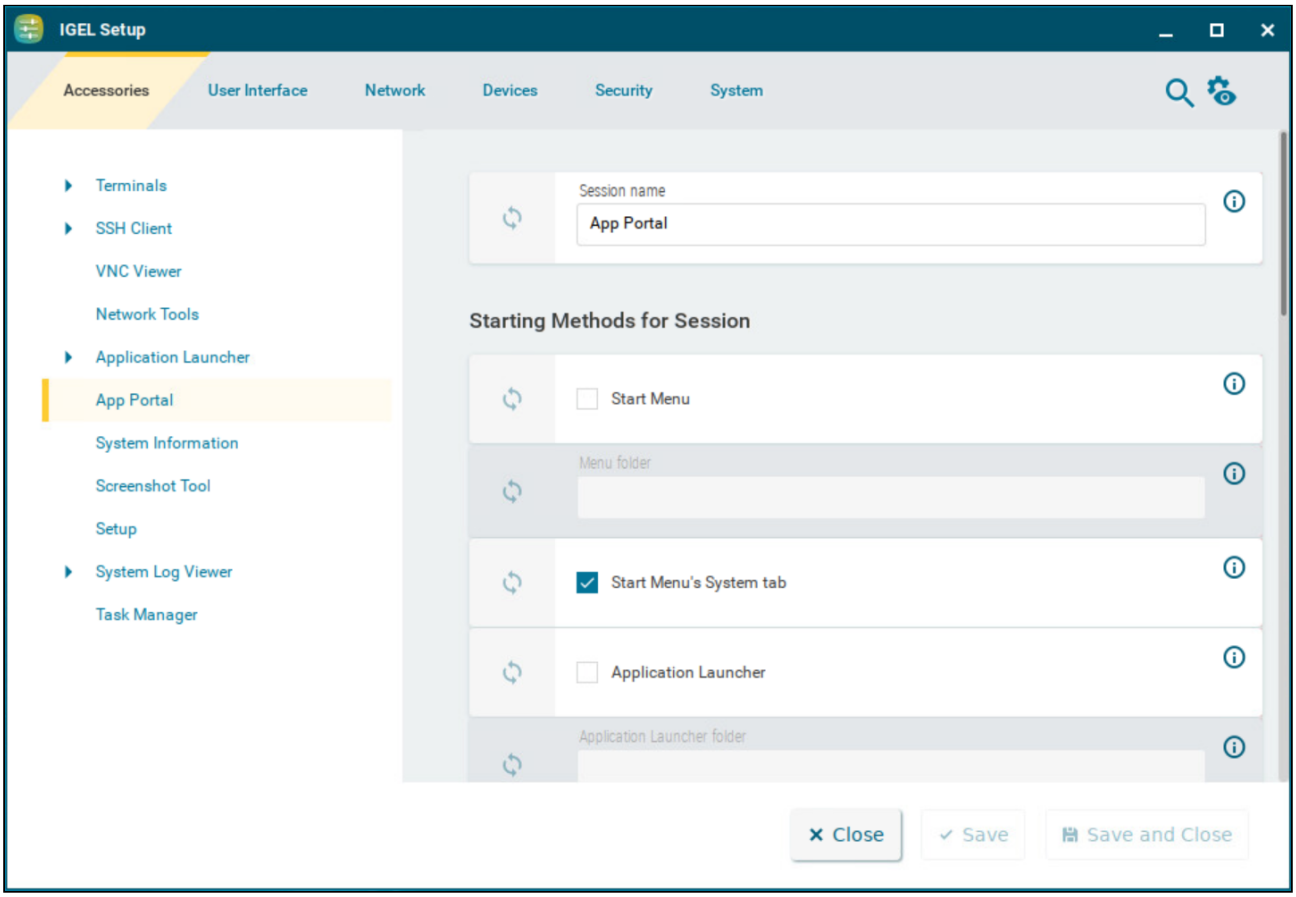
> You can hide the shutdown menu from the Application Launcher using the **Hide Shutdown menu button** option under **User Interface > Commands > Shutdown Menu > Quick Access**. For more information, see Commands (see page 129).

App Portal

This article shows how to configure the starting methods for the App Portal in IGEL OS.

> To use the IGEL App Portal locally on the device, verify first that **Permit local app installation** is enabled under **Security > Update**. (Default)
> For detailed information on how to use the App Portal, see Installing IGEL OS Apps Locally on the Device.

Menu path: **Accessories > App Portal**



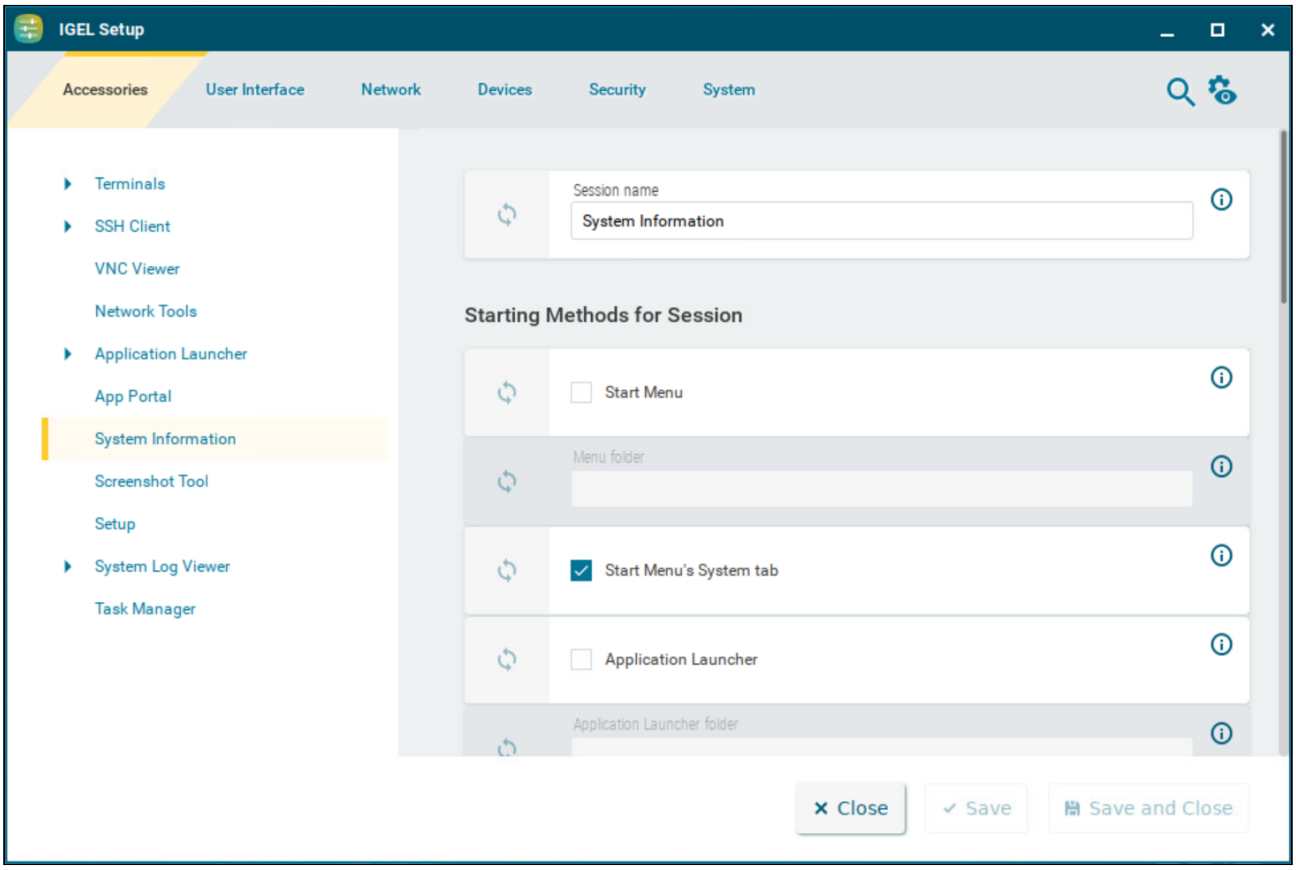
The starting methods parameters are described under Starting Methods for Apps (see page 376).

System Information

This article shows the starting methods configuration and the use of System Information in IGEL OS. Through System Information, you can obtain information regarding the operating system of your device, the installed system components, internal and connected hardware, and the network. You can also measure the performance of your device using various benchmarks.

> An administrator password is required by default to start **System Information** if **Use Password** is enabled under **Security > Password**. For details, see Password (see page 245).
> The password requirement can be changed through the **Password protection** option in the starting methods configuration.

Menu path: **Accessories > System Information**

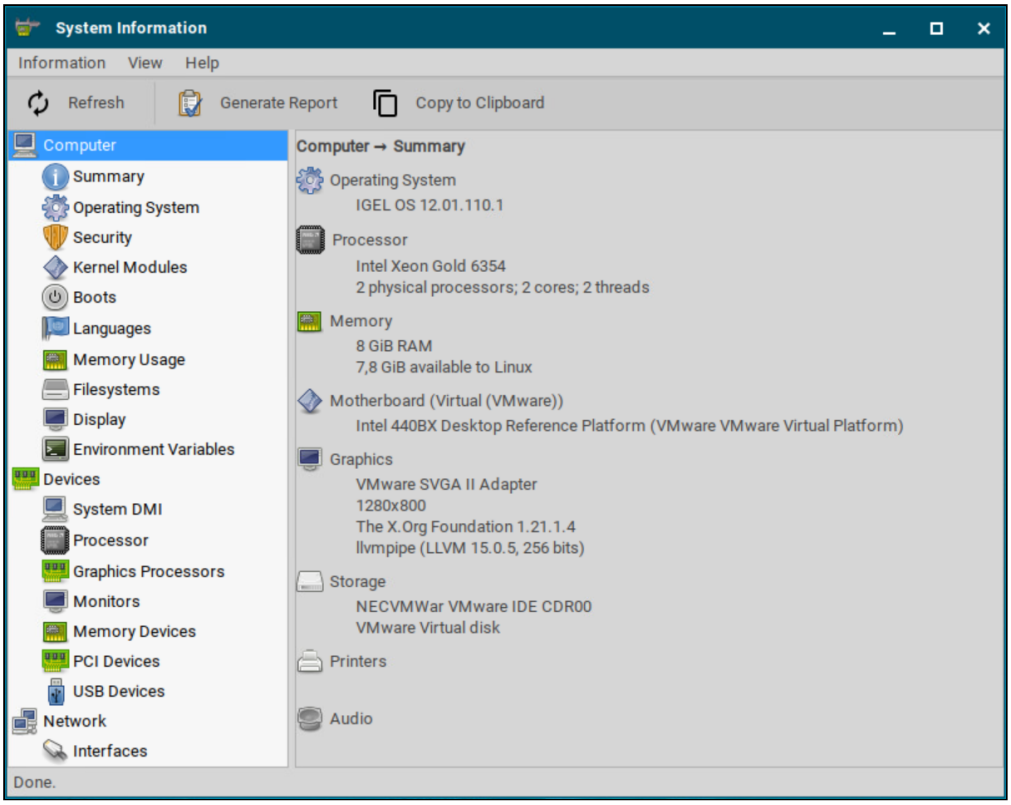


You can configure the starting methods for an easy access of the System Information.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using System Information

▶ Start **System Information**.

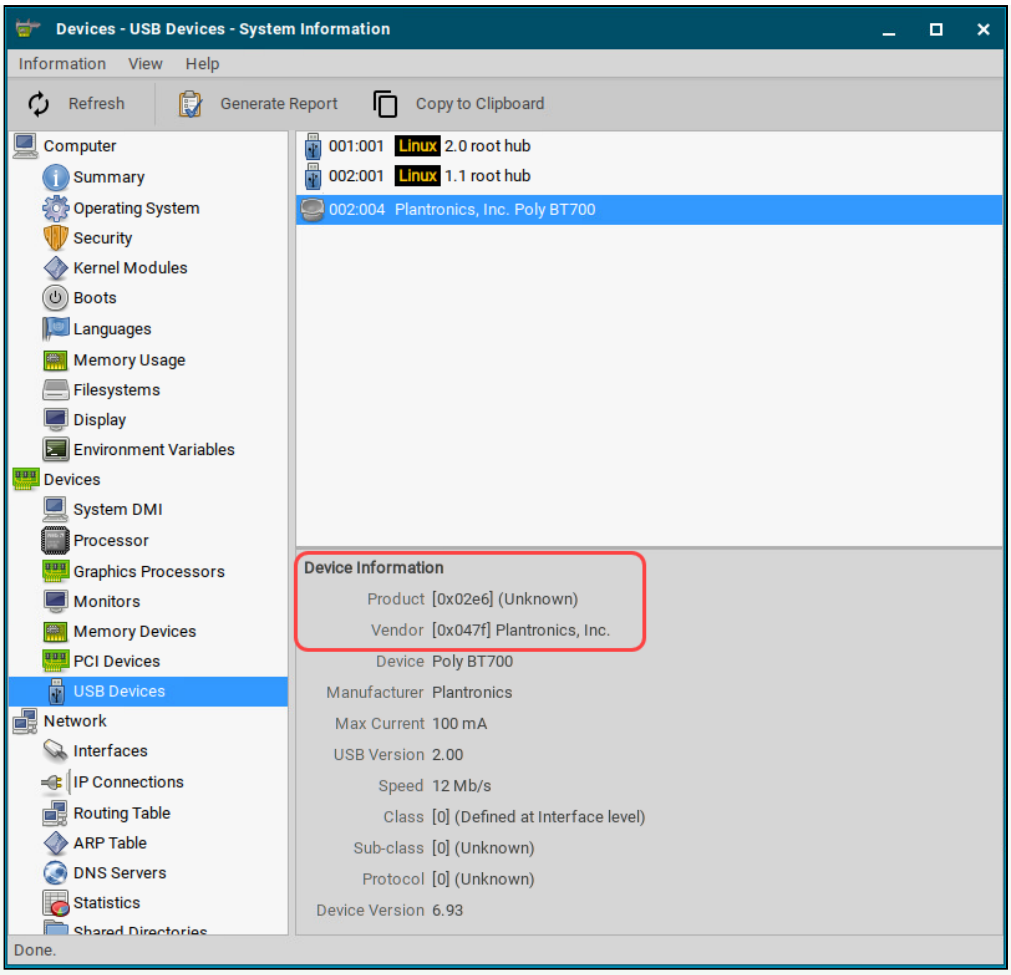


To obtain system information regarding a specific component of your IGEL OS device, proceed as follows:

1. Navigate to the desired area, e.g. **Computer > Operating System**.
   The information regarding the desired area will be shown.

2. To send the information shown, e.g. to the IGEL Support, click **Copy to Clipboard**.
   The information is on your clipboard. With **Paste** or [Ctrl] + [V], you can paste the information into an e-mail or a web form.

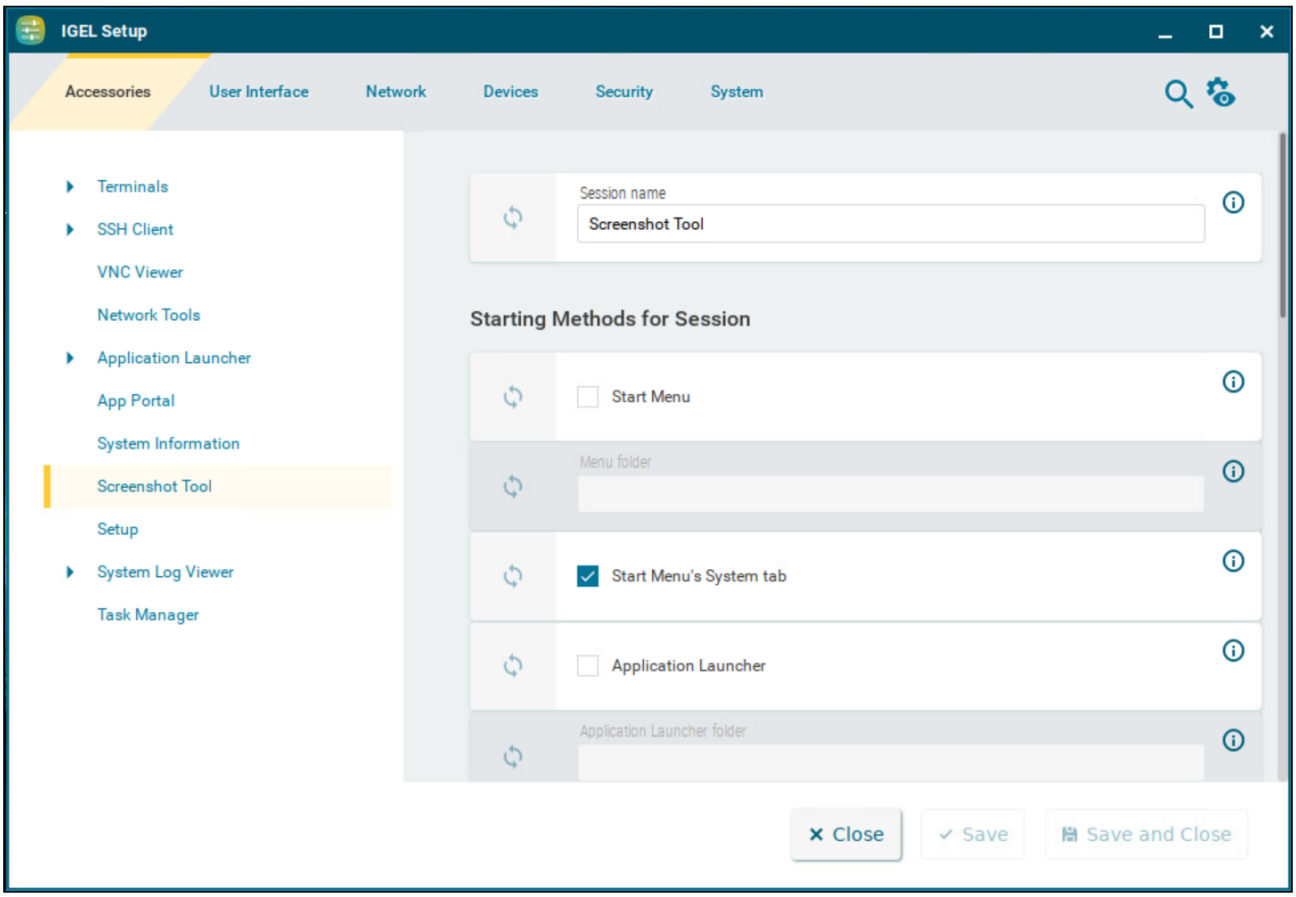
You can use the **System Information** function to find out the **Vendor ID** and **Product ID** of your connected hardware. They are required, for example, if you want to configure **Device Rules** under **Setup > Devices > USB Access Control**. For more information, see USB Access Control (see page 230).


Devices - USB Devices - System Information
Information
View
Help
Refresh
Generate Report
Copy to Clipboard
Computer
Summary
Operating System
Security
Kernel Modules
Boots
Languages
Memory Usage
Filesystems
Display
Environment Variables
Devices
System DMI
Processor
Graphics Processors
Monitors
Memory Devices
PCI Devices
USB Devices
Network
Interfaces
IP Connections
Routing Table
ARP Table
DNS Servers
Statistics
001:001 Linux 2.0 root hub
002:001 Linux 1.1 root hub
002:004 Plantronics, Inc. Poly BT700
Device Information
Product [0x02e6] (Unknown)
Vendor [0x047f] Plantronics, Inc.
Device Poly BT700
Manufacturer Plantronics
Max Current 100 mA
USB Version 2.00
Speed 12 Mb/s
Class [0] (Defined at Interface level)
Sub-class [0] (Unknown)
Protocol [0] (Unknown)
Device Version 6.93
Done.

Screenshot Tool

This article shows the starting methods configuration and the use of the Screenshot Tool in IGEL OS.

Menu path: **Accessories > Screenshot Tool**



You can configure the starting methods for an easy access of the System Information.

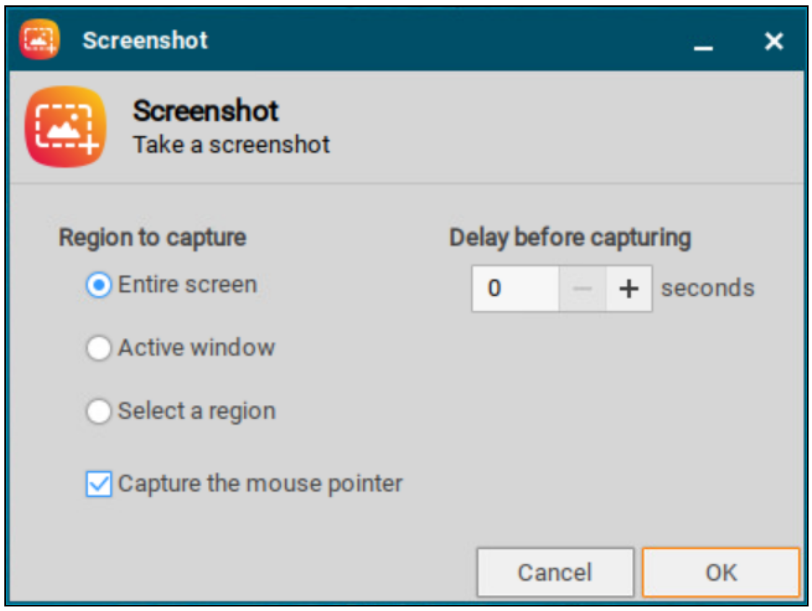
The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using Screenshot Tool

1. Start the **Screenshot Tool**.

> Hotkeys can be configured for using the Screenshot Tool under **User Interface > Hotkeys**. Hotkeys can be configured to take **Screenshot of active window** or **Screenshot of entire screen**. When using the hotkeys, the screenshot is taken without delay, and the mouse pointer is not captured. For more information on hotkey configuration, see Hotkeys (see page 99).

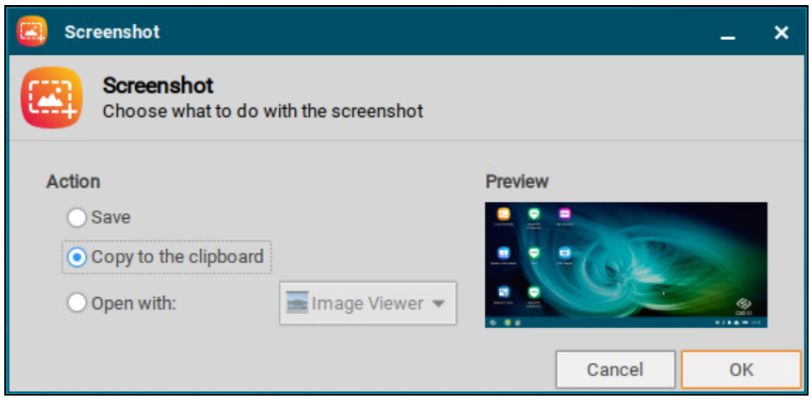
2. Select a **Region to capture** option. You have the following options:
   - **Entire screen**
     The entire screen content will be photographed.
   - **Active window**
     The window that is currently active will be photographed.
   - **Select a region**
     You can select a section of the screen using the mouse.



3. Set the **Capture the mouse pointer** option.
   ☑ The mouse pointer is visible on the screenshot.

4. Specify the **Delay before capturing** in seconds. The minimum value is 0.

5. Click **OK**.
   If you have enabled **Entire screen** or **Active window**, the screenshot will be taken after the **Delay before capturing** has elapsed.
   If you have enabled **Select a region**, you can select the desired part of the screen using the mouse. To do this, press and hold the left mouse button while dragging the mouse across the screen.

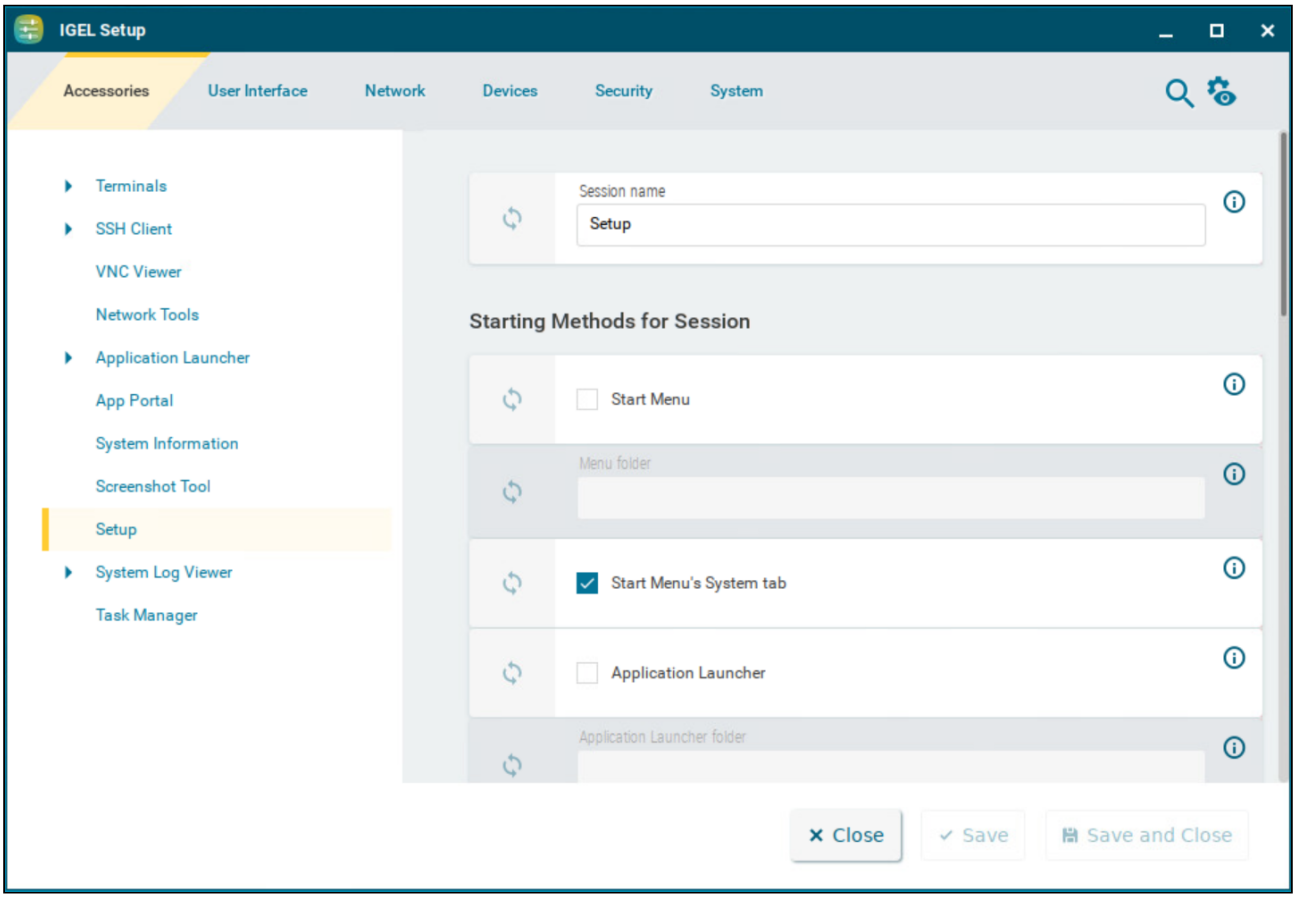


6. Specify how the screenshot is to be used.
   You have the following options:
   - **Save**
     If this option is enabled, the screenshot will be saved in PNG format via your device. You can save the screenshot locally, on a network drive or on a USB mass storage device.
   - **Copy to the clipboard**
     If this option is enabled, the screenshot will be available in the device's local cache.
   - **Open with**
     If this option is enabled, the screenshot will be opened in your device's image viewer.

Setup

With the IGEL Setup, you can configure your endpoint device. This article shows how to configure the starting methods for the IGEL Setup in IGEL OS.

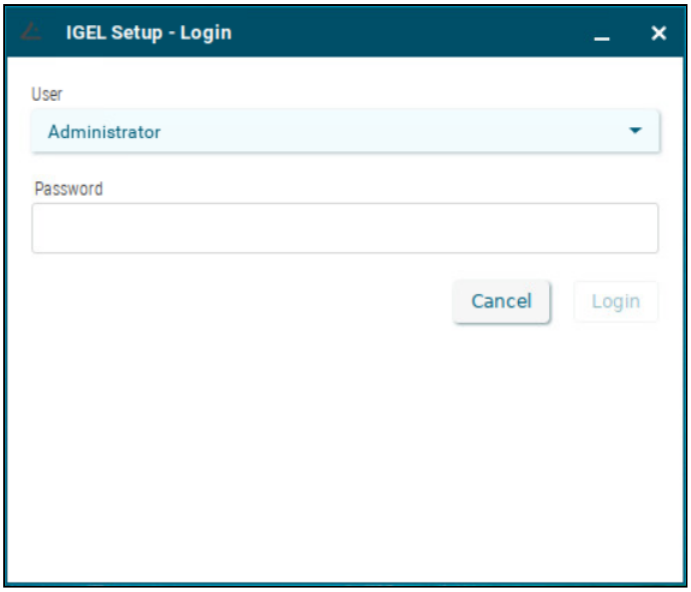
Menu path: **Accessories > Setup**



The starting methods parameters are described under Starting Methods for Apps (see page 376).

If you configure user types and passwords under **Security > Password**, a login window appears at the start of the IGEL Setup. For more information, see Password (see page 245).

> ⚠ If you do not configure the user types and passwords, the IGEL Setup can be opened without password protection.



▶ Select from the configured user types and provide the corresponding password.

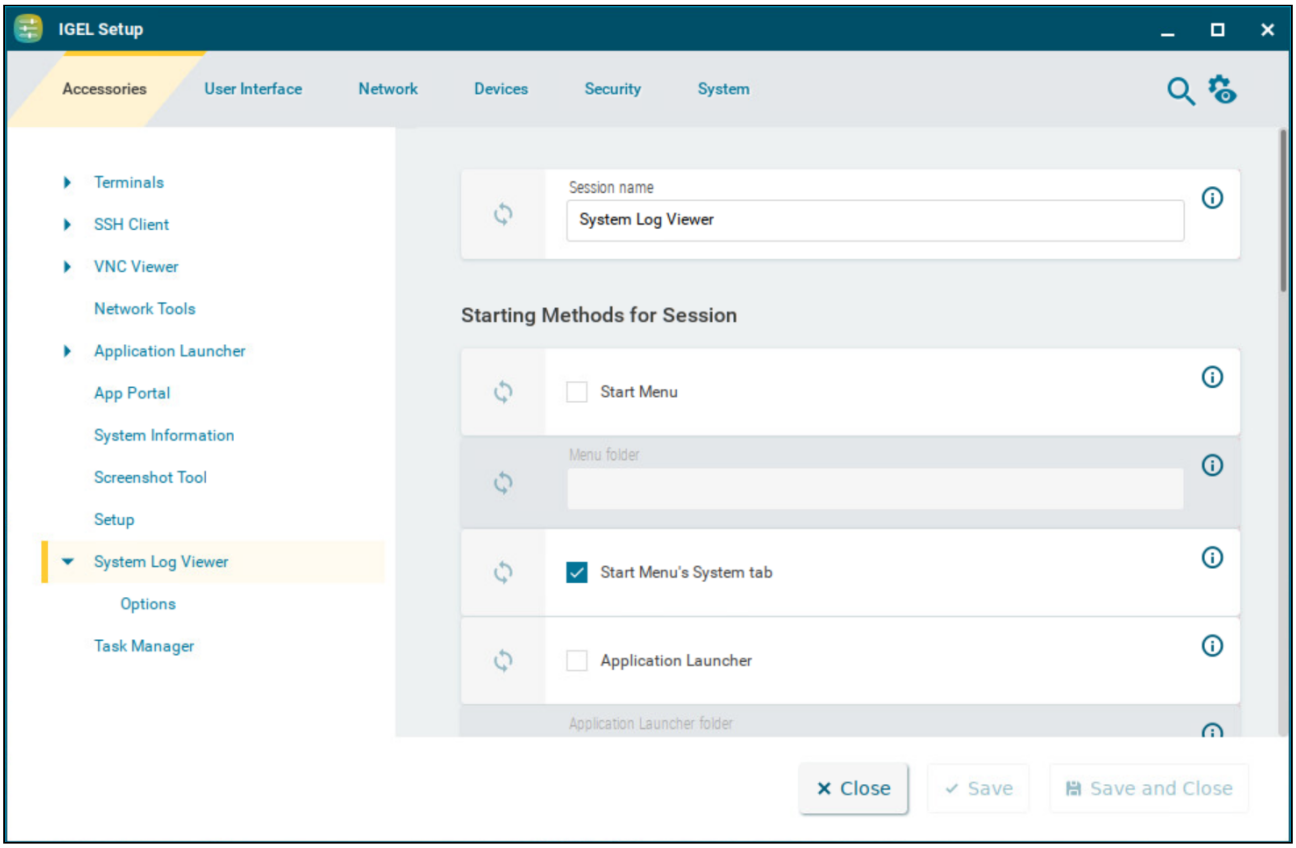
The following user types can be configured to access the IGEL Setup:

- Administrator
- Setup administrator
- Setup user

System Log Viewer

This article shows how to configure the System Log Viewer in IGEL OS. With this function, you can view your device's system logs.

Menu path: **Accessories > System Log Viewer**



You can configure the starting methods for an easy access of the System Log Viewer.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Options

Menu path: **Accessories > System Log Viewer > Options**

Here, you can add additional files to the files shown by default. The System Log Viewer shows the following files by default:

- `/config/Xserver/card0`
- `/config/Xserver/monitor-info`
- `/config/Xserver/xorg.conf-0`
- `/var/log/Xorg.0.log`
- `/var/log/auth.log`
- `/var/log/daemon.log`
- `/var/log/igfmount.log`
- `/var/log/kern.log`
- `/var/log/syslog`
- `/var/log/tcsetup.log`
- `/wfs/user/setup-assistant.log`

To add a further file to the display, proceed as follows:

1. Click .
2. In the **Add** dialog, enter the path and the file name of the desired file. Example: `/var/log/splash.debug`

   If you want to add several files, you can also use the asterisk *. Example: `/var/log/*.log` or `/var/log/*.txt`
3. Click **OK**.

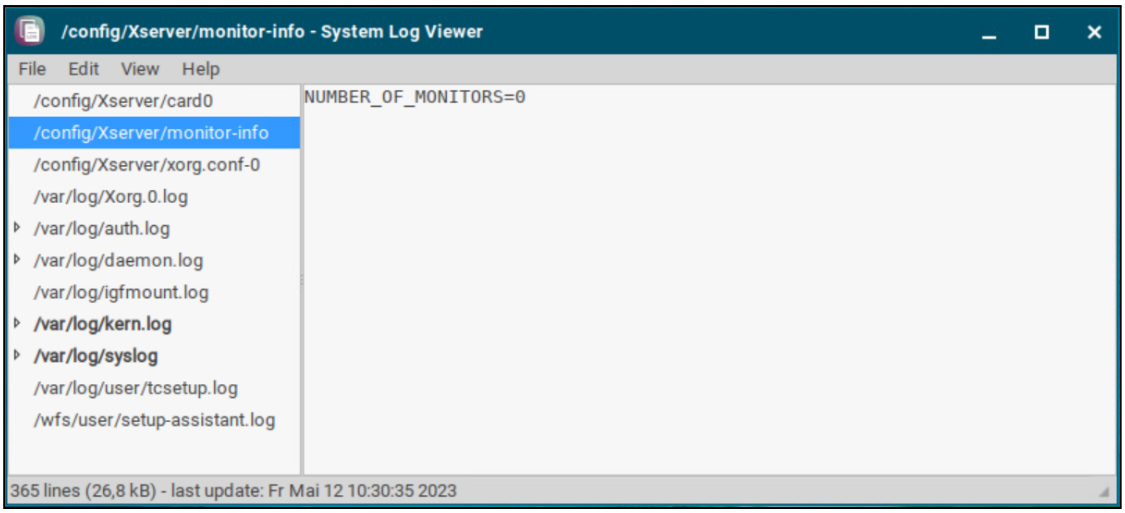
   When the System Log Viewer is started, the file that you have added will be shown.

   Known Issue

   The added file is only shown after the restart of the device. The configuration will be reworked in a future release.

Using System Log Viewer

▶ Start the **System Log Viewer**.



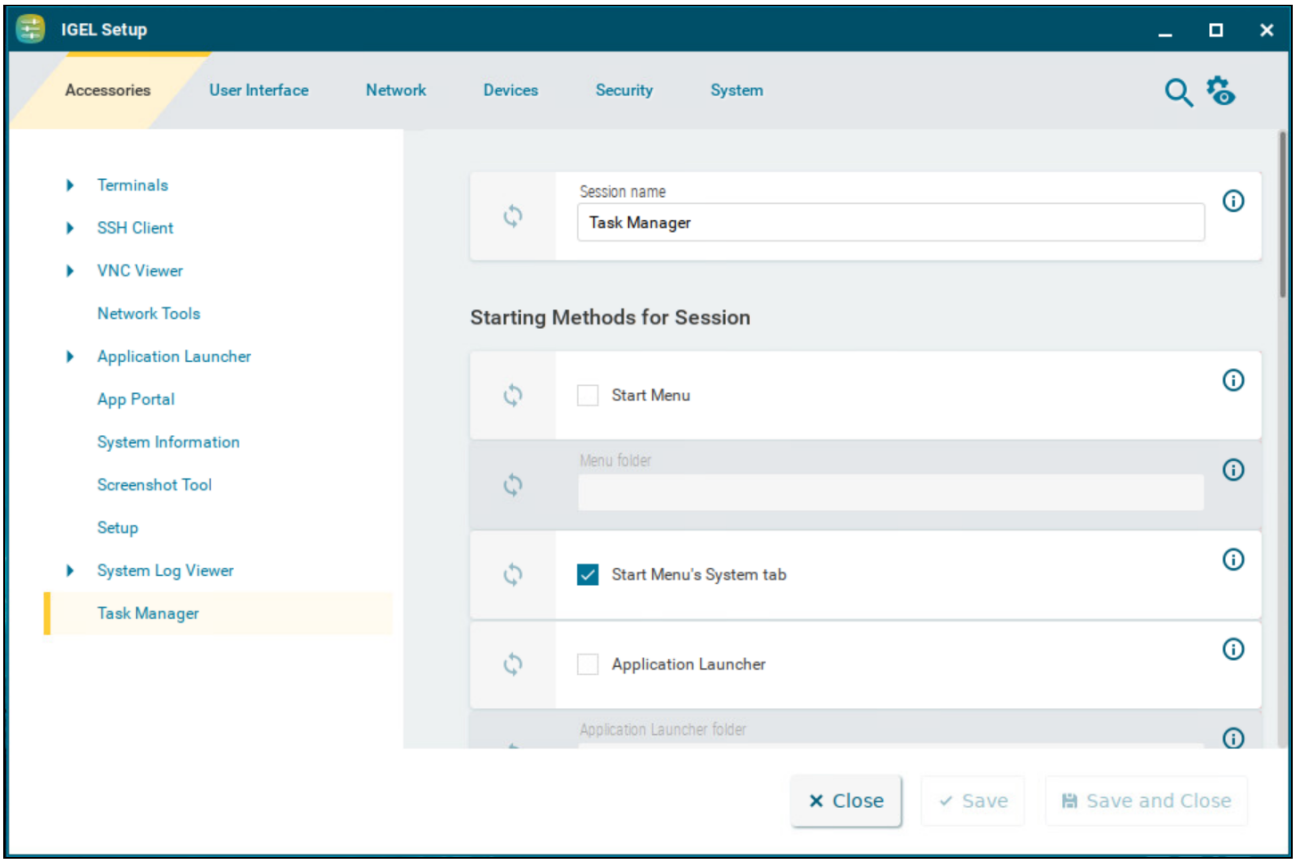
▶ In the left-hand column, select the file that you want to view.

The selected file will be shown in the right-hand column.

Task Manager

The Task Manager provides an overview of the applications and other processes running on the device. It can be used to pause, end, or change the priority of processes. This article shows the starting methods configuration and the use of the Task Manager in IGEL OS.

Menu path: **Accessories > Task Manager**



You can configure the starting methods for an easy access of the Task Manager.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using Task Manager

With the Task Manager, you can observe and influence applications and processes in the following ways:

- Determining device processor usage
- Determining device memory usage

- Determining processor usage by a specific application
- Determining memory usage by a specific application
- Pausing and continuing an application
- Closing an application
- Force closing an application
- Changing the priority of an application

▶ Start the **Task Manager**.

To determine the device's total processor usage:

▶ Read the percentage value under **CPU**.

To determine the devices's total memory usage:

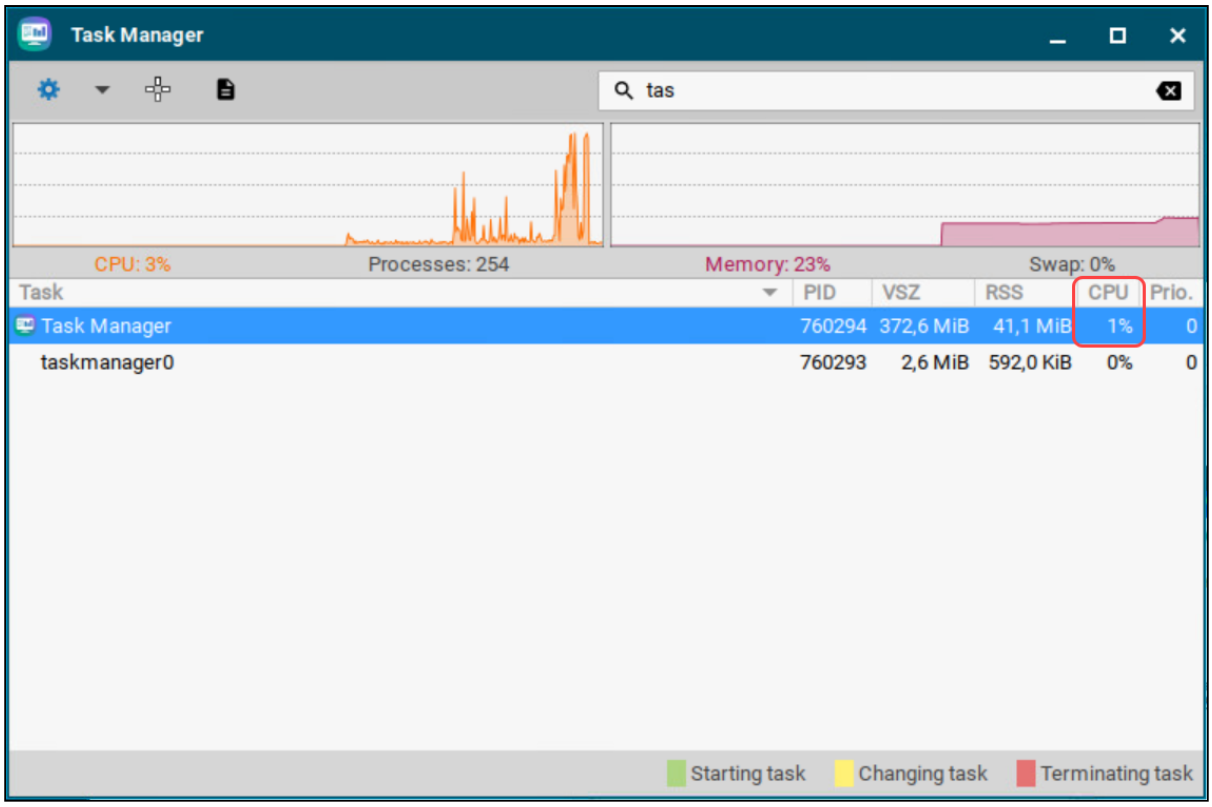
▶ Read the percentage value under **Memory**.

To calculate the value in bytes, click and enable **Show memory usage in bytes**.

To determine the extent to which a specific application contributes to processor usage, proceed as follows:

1. In the search window, enter the name of the application or part of the name.
   The Task Manager will now show only the relevant applications and processes.

2. Read the percentage value for the relevant application in the **CPU** column.

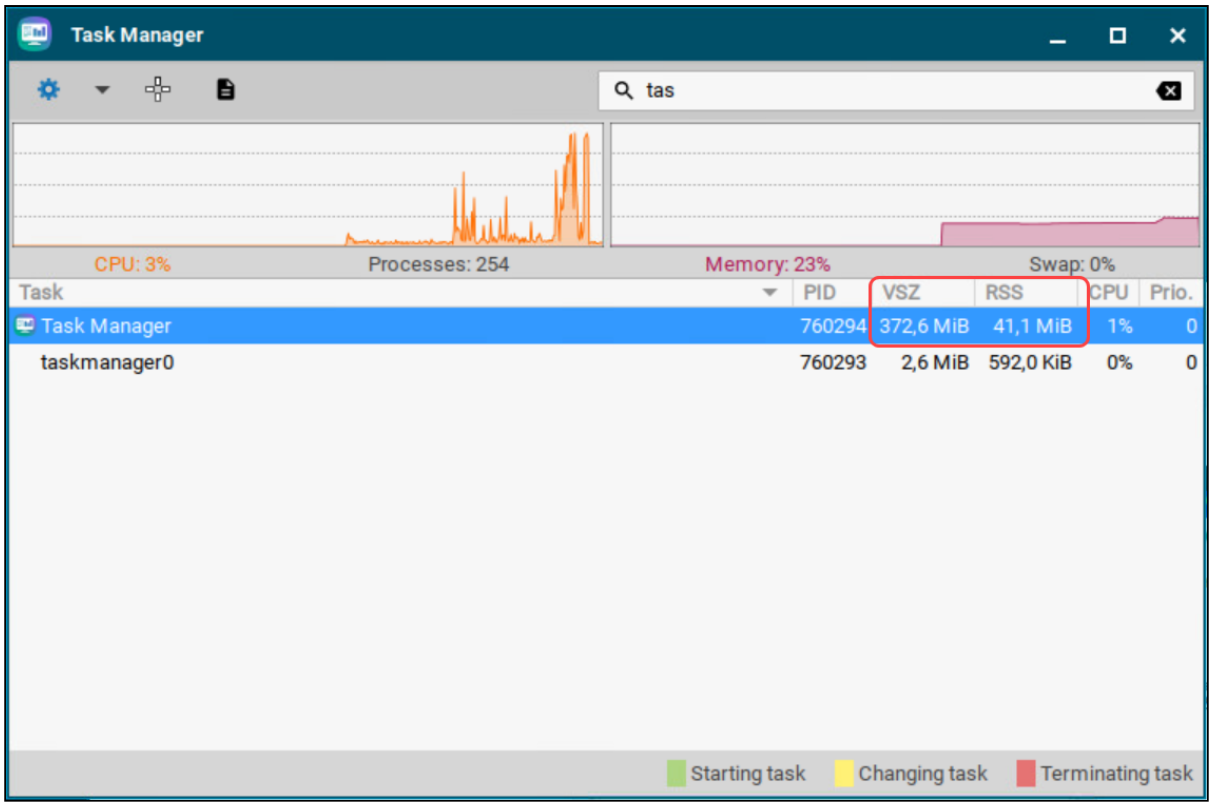


To determine the extent to which a specific application contributes to memory usage, proceed as follows:

1. Click next to and ensure that **Virtual Bytes** and **Private Bytes** are enabled.

2. In the search window, enter the name of the application or part of the name.
   The Task Manager will now show only the relevant applications and processes.

3. Read the values in the **VSZ** and **RSS** columns.
   The **VSZ** column shows how much memory is available for the application. The **RSS** column shows how much memory the application is currently using.



To pause an application, proceed as follows:

1. Highlight the application.

2. Open the application's context menu by right-clicking on it and select **Stop**.
   The application will be paused (Signal SIGSTOP). You can then continue the application.

To continue an application, proceed as follows:

1. Highlight the application.

2. Open the application's context menu by right-clicking on it and select **Continue**.
   The application will continue (Signal SIGCONT).

To close an application, proceed as follows:

1. Highlight the application.

2. Open the application's context menu by right-clicking on it and select **Terminate**.
   The application will close (Signal SIGTERM).

> In this case, the application is instructed to close by the operating system. If the application does not react to this instruction, you can force it to close with the **Kill** command.

To force an application to close, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Kill**.
   The application will be forced to close (Signal SIGKILL).

To change the priority of an application, proceed as follows:

1. Highlight the application.
2. Open the application's context menu by right-clicking on it and select **Priority**.
3. Select one of the following values for the priority:
   - **Very low** (nice value: 15)
   - **Low** (nice value: 5)
   - **Normal** (nice value: 0)
   - **High** (nice value: -5). This value can only be set by the administrator.
   - **Very high** (nice value: -15) This value can only be set by the administrator.

> As a normal user, you can only change the priority from a higher value to a lower value. Example: If you have changed the priority from **Normal** to **Low**, you can only then change it to **Very low** – you can no longer change it back to **Normal**. The administrator can increase the priority.

> The priority corresponds to the nice value. High values result in a low priority, while low values result in a high priority.

User Interface

In this chapter, you find information on the configuration of the user interface in IGEL OS.

- Display Settings (see page 49)
- Desktop (see page 59)
- Language (see page 85)
- Screenlock / Screensaver (see page 87)
- Hotkeys (see page 99)
- Input (see page 101)
- Commands (see page 129)

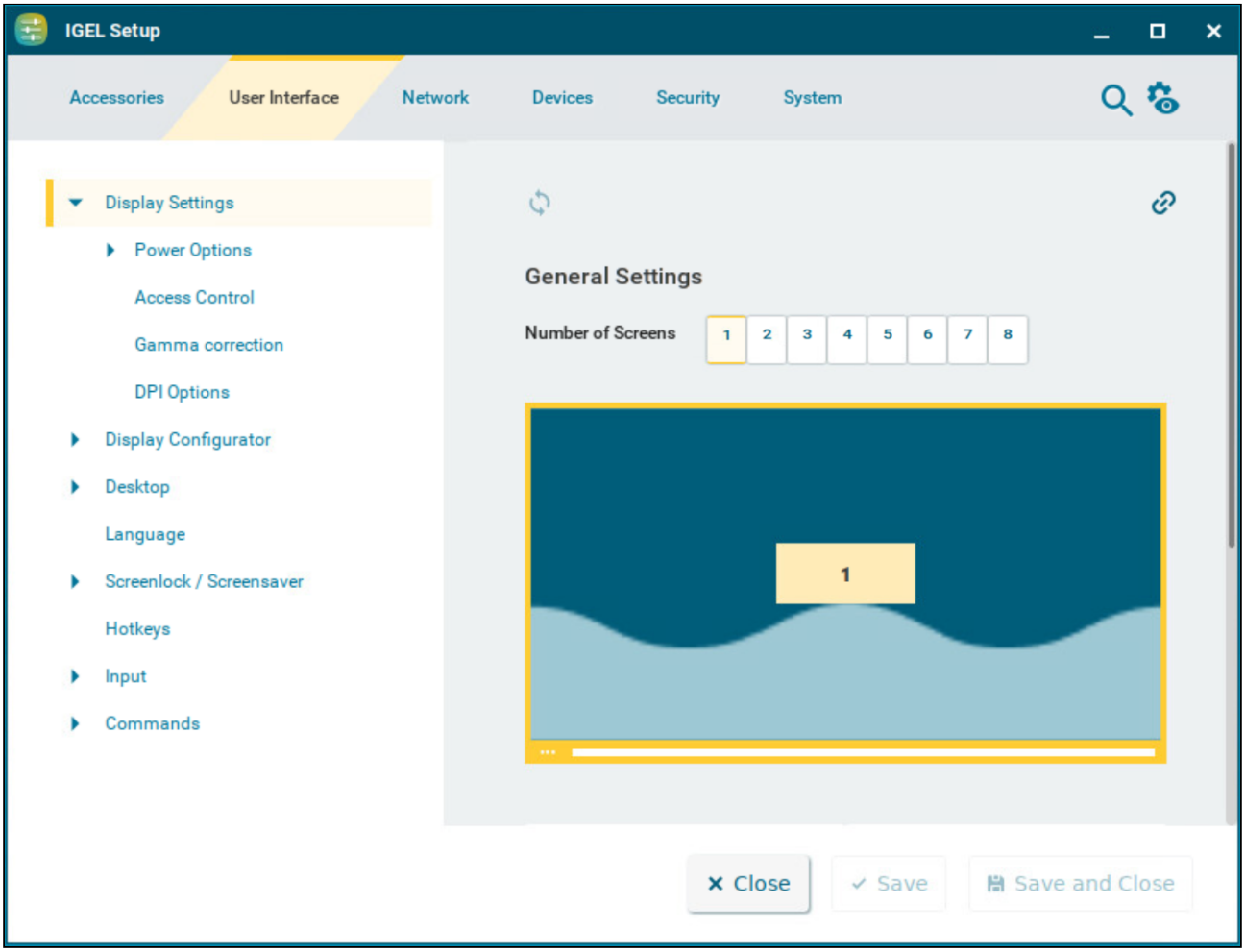
Display Settings

This article shows how to configure the display settings for the monitors in IGEL OS.

Take notice that a successful and correct display configuration depends, however, on many factors. For example, cables, current driver, BIOS settings, etc. can influence your screen configuration and, thus, have to be considered when setting up the monitor environment.

> You can also use the display tray app for display configurations. For more information, see Tray Applications in IGEL OS 12 (see page 353).

Menu path: **User Interface > Display Settings**



Always try the configuration locally before applying it to multiple devices via a profile: A faulty display configuration can cause your GUI to become unstable and lead to a black screen.
If you face a black screen problem because of the wrong display configuration, try one of the following recovery options:

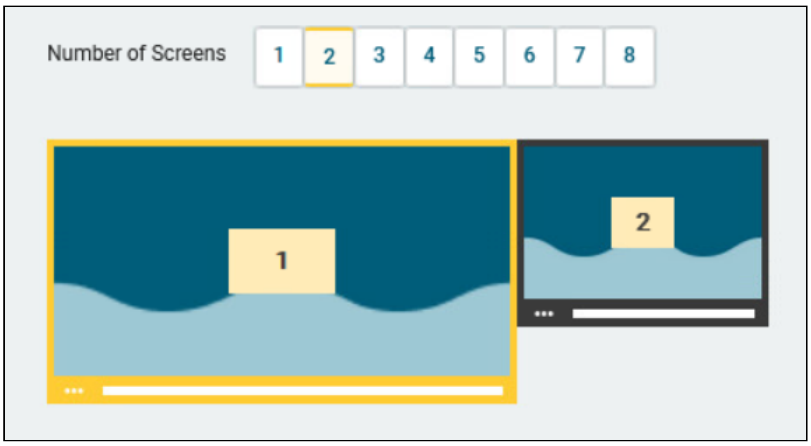
- In the UMS: Edit the display configuration via **Devices > [device name] > [device's context menu] > Edit Configuration** or via a new profile.
- In Web UMS: Edit the settings by clicking **Edit Configuration** in the Device Information of the device under **Devices > [device name]**.
- On the endpoint device: Restart the device and select **Emergency boot (setup only)** during the boot procedure. In the Setup, you can then change the display configuration.

General Settings

Number of screens

The number of monitors used can be selected by clicking the numbered buttons.

In a multimonitor configuration, every screen connected to the endpoint device can be configured independently after selecting the screen. The selected screen is highlighted with a yellow frame. The white bar at the bottom edge of the screen represents the physical orientation of the monitor. The position of the screens can be configured by drag&drop.



Screen resolution

The resolution can be selected from a drop-down menu. (Default: Autodetect)

You have the option of defining your own resolutions via the registry key `x.xserver0.custom_resolution`. In order for the values set there to take effect, the resolution must be set to **Autodetect**. The following parameters apply to the entry in the registry:

- `WxH` : W = width, H = height (example: 1920x1080)

- `WxH@R` : W = width, H = height, R = refresh rate (example: 1920x1080@60 or 1920x1200@59.8)

⚠ Be careful when changing resolutions manually. Excessively high resolutions can cause a black screen.

ⓘ For details of the display resolution supported by your IGEL device, please see the datasheet archive for legacy IGEL devices.
For detailed instructions on MST configuration for UD3 and UD7, see:
- UD3 Model M350C: Multistream Transport
- UD7 Model H860C: Multistream Transport (MST) / Monitor Daisy Chaining

Screen rotation

The rotation can be selected from a drop-down menu. (Default: None)

Advanced Settings for the Screen

Detect refresh rate automatically

☑ A refresh rate for the monitor is identified automatically. (Default)

☐ A refresh rate for the monitor is to be set manually.

Refresh rate

Number of individual images per second
Possible values:

- **30 ... 100** (Default: 60)

⚠ Be careful when changing the refresh rate manually since a faulty configuration can cause a black screen.

Graphic card

Graphic card assigned to the selected screen. A graphic card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphic cards manually.

ⓘ If **Automatic** is set for the **Monitor** and no configurable monitor is found for the selected graphic card, the next available monitor will be used by another graphic card.

Monitor

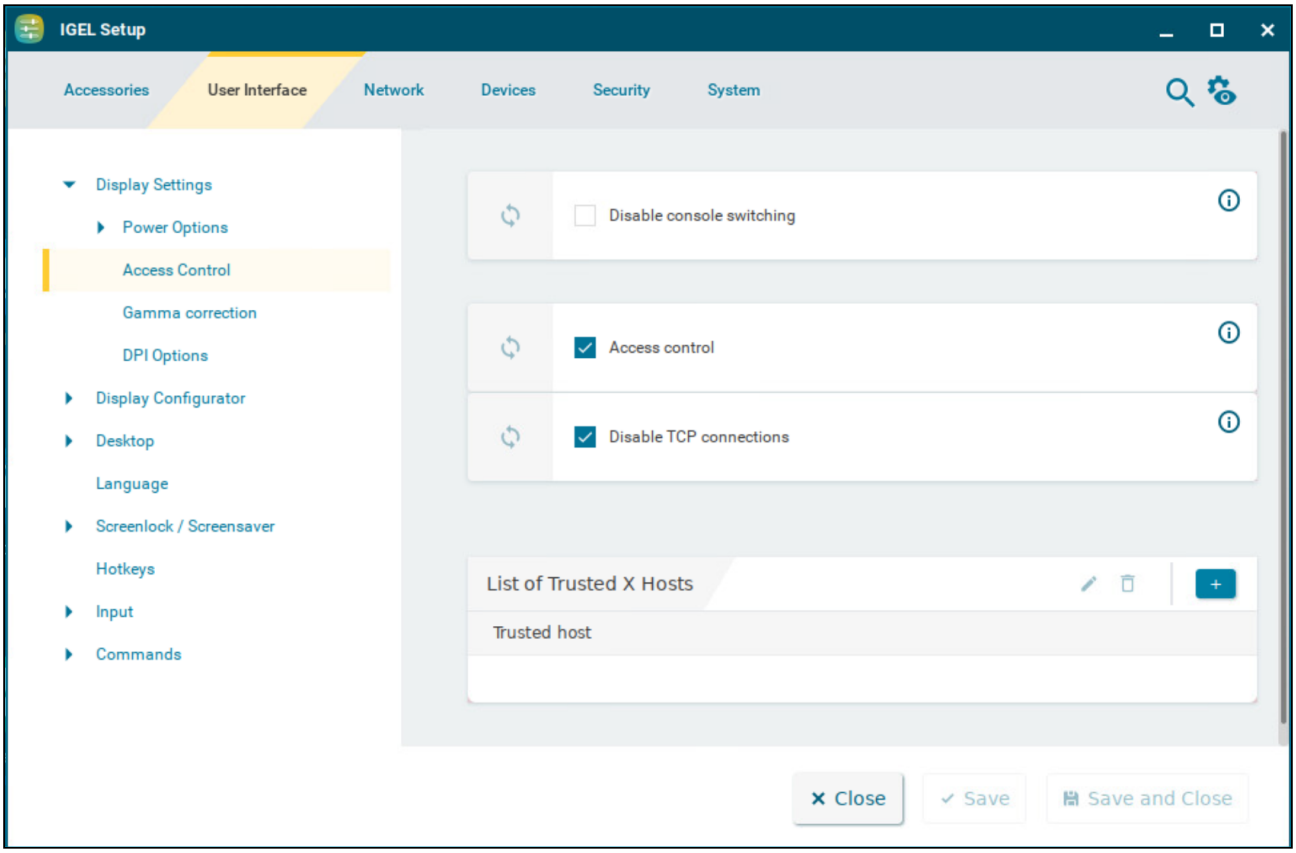
Connection type. (Default: Automatic)

- Access Control (see page 53)
- Gamma Correction (see page 55)
- DPI Options (see page 57)

Access Control

This article shows how to control access to the display in IGEL OS. Device access control is enabled by default.

Menu path: **User Interface > Display Settings > Access Control**



Disable console switching

☑ You can NOT switch to the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12].

☐ You can access the console using [Ctrl] + [Alt] + [F11] or [Ctrl] + [Alt] + [F12]. (Default)

Access control

☑ Access to this display from other computers will be controlled. (Default)

Disable TCP connections

☑ All TCP connections to the display are disabled. Only local applications are displayed. The xhost mechanism does not function. (Default)

> ⓘ This parameter is ignored if XDMCP is configured.

List of Trusted X Hosts

List of approved computers for console access

To manage the list:

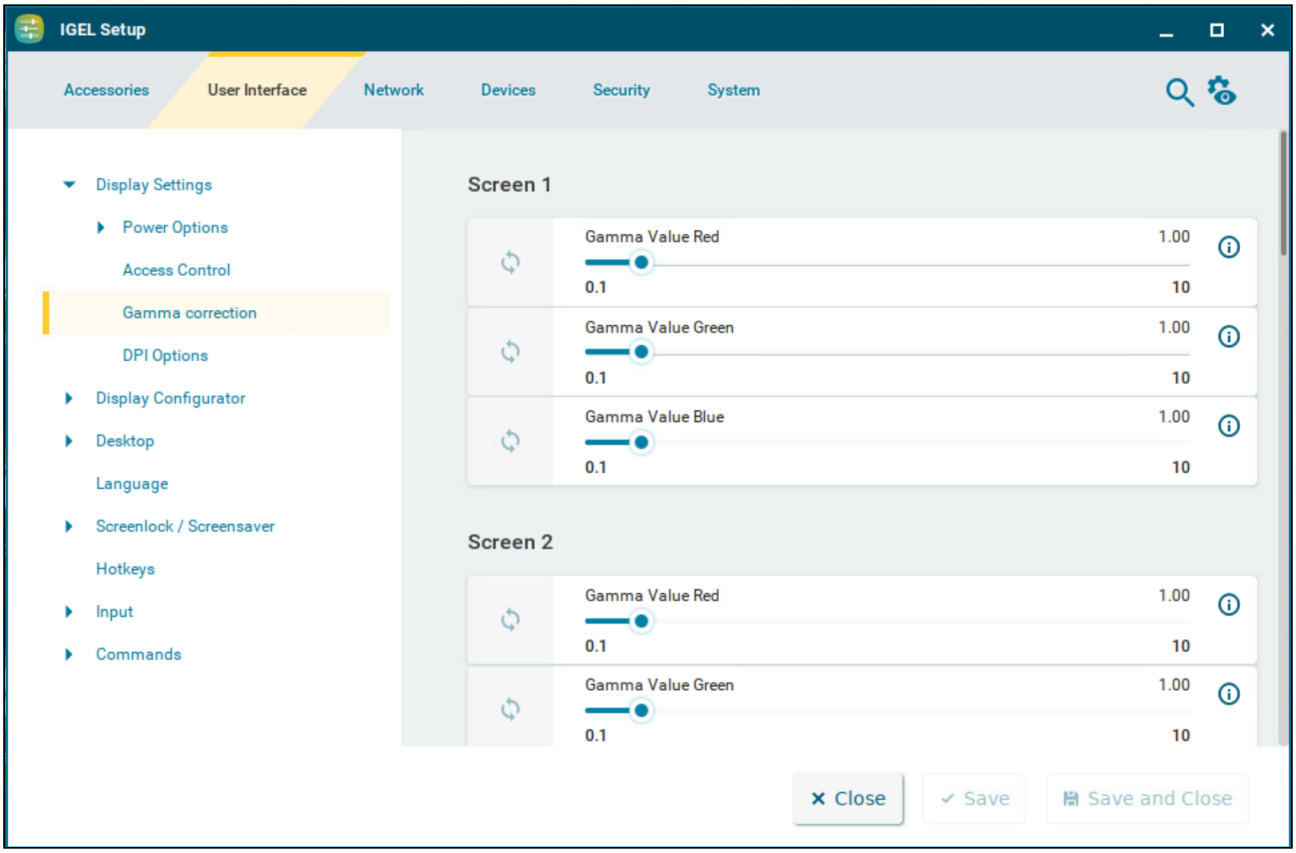
- Click to create a new entry.
- Click to remove the selected entry.
- Click to edit the selected entry.
- Click to copy the selected entry.

When adding the **Trusted host**, give the name of the remote host (not the IP address) you would like to add.

Gamma Correction

This article shows how to increase or decrease the various brightness ranges in order to adjust the display on your screen in IGEL OS.

Menu path: **User Interface > Display Settings > Gamma Correction**



You can change the gamma values for red, green and blue on each screen separately. The scale ranges from 0.10 (dark) to 10 (light) and is set to 1.00 by default.

Gamma Value Red

Changes the brightness curve for the red color portion.

Gamma Value Green

Changes the brightness curve for the green color portion.

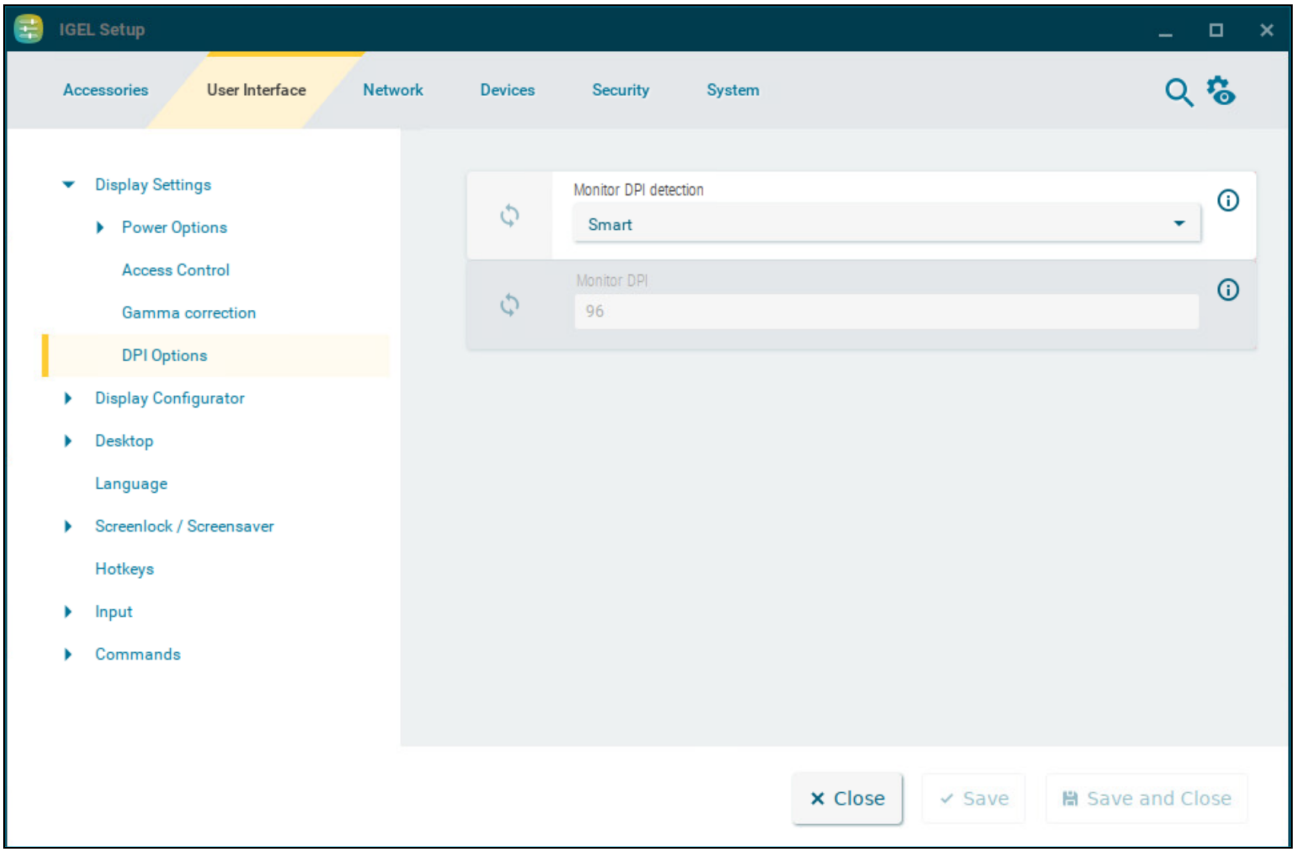
Gamma Value Blue

Changes the brightness curve for the blue color portion.

DPI Options

This article shows how to configure DPI values for the display in IGEL OS.

Menu path: **User Interface > Display Settings > DPI Options**



Monitor DPI detection

Defines how the DPI value should be determined.
Possible options:

- **Off**: The DPI value is defined by **Monitor DPI**. There is no automatic detection.
- **Smart** (Default):
  The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. The DPI value is set to either 96, 125, 150, 175, 200, 225, 250, 275 or 300, depending on which value is closest to the value calculated based on the monitor resolution.

- **Pixel-Precise**:
  The DPI value is defined automatically. With this setting, the user interface is readable also on monitors with very high resolutions, e.g. 4k monitors. The value calculated based on the monitor resolution is used directly.

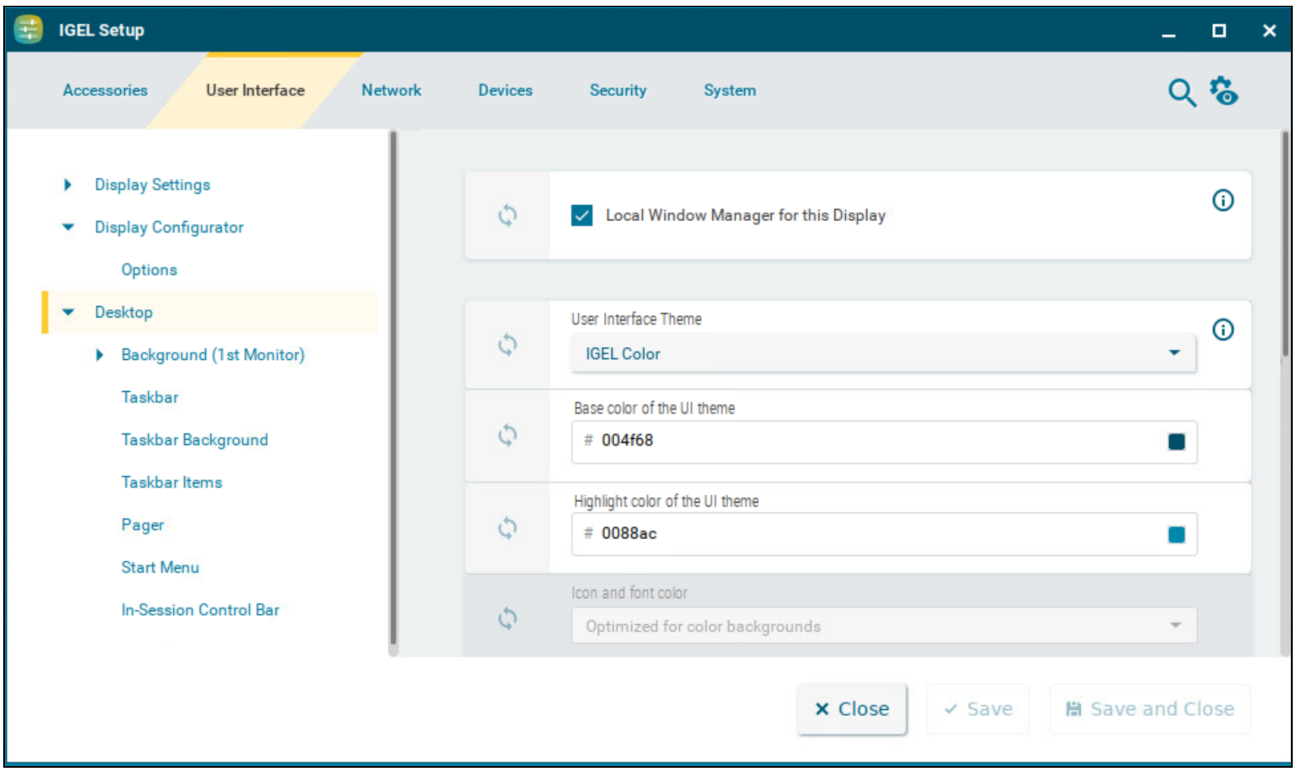
Monitor DPI

The DPI resolution (dots per inch) for your monitor. (Default: 96)
This parameter is only available if **Monitor DPI detection** is set to **Off**.

Desktop

This article shows how to configure general settings for the appearance of the desktop in IGEL OS.

Menu path: **User Interface > Desktop**



Local window manager for this display

☑ Enables local window management for the display. (Default)

User interface theme

You can either select one of our predefined color schemes or define a color scheme of your own.

- **IGEL color**: The color of dialog frames and the taskbar is blue, headings and icons are white, highlights are light blue.
- **IGEL dark**: The color of dialog frames and the taskbar is black, headings and icons are white, highlights are dark gray.
- **IGEL light**: The color of dialog frames and the taskbar is light gray, headings and icons are black, highlights are dark grey.

- **Custom colors**: Define your own color combinations below.
  - **Base color of the UI theme**: The color of dialog frames and the taskbar. Click the color preview square to open the color selector.
  - **Highlight color of the UI theme**: The color of highlights. Click the color preview square to open the color selector.
  - **Icon and font color**: The optimization can be selected based on custom colors.

Desktop icon size

The size of icons displayed on the desktop

Desktop icon font color

The font color for the labels associated with the desktop icons. Click the color preview square to open the color selector.

Monitor for desktop icons

If you use several monitors, select the one that is to display desktop icons.

- **All monitors**
- **Same as taskbar**
- **1st monitor**
- **2nd monitor**
- (other monitors if connected)

Single click mode

☑ Programs are opened with a single click. (Default)

Desktop Fonts

Default font

The font type of texts appearing on the taskbar and in the start menu. The following fonts are available to choose from:

- **RobotoRegular** (Default)
- **Sans**
- **Sans Bold**
- **Serif**
- **Serif Bold**

Default font size

The font size of texts appearing on the taskbar and in the start menu in pt (points).

Desktop icon font size

The font size of texts for desktop icons in pt (points).

Titlebar font

The font type of texts appering in titlebars. The following fonts are available to choose from:

- **RobotoBold** (Default)
- **Sans**
- **Sans bold**
- **Serif**
- **Serif Bold**

Titlebar font size

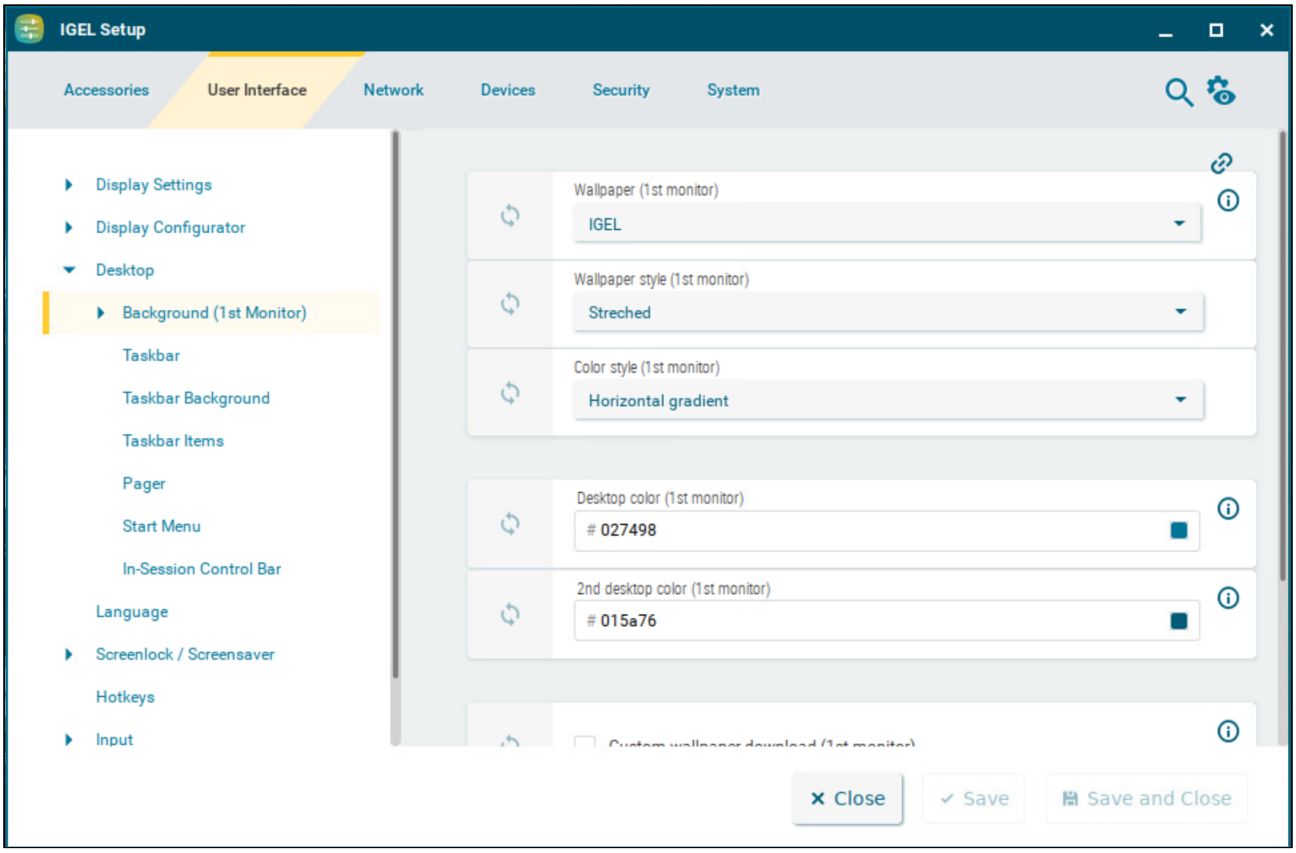
The font size of texts appearing in titlebars in pt (points).

- Background (1st Monitor) (see page 62)
- Taskbar (see page 67)
- Taskbar Background (see page 70)
- Taskbar Items in IGEL OS 12 (see page 72)
- Pager (see page 76)
- Start Menu (see page 81)
- In-Session Control Bar (see page 83)

Background (1st Monitor)

This article shows how to configure the desktop background in IGEL OS.

Menu path: **User Interface > Desktop > Background (1st Monitor)**



You can use predefined IGEL backgrounds, a fill color or a color gradient. You can also use a background image of your own.

> You can set up a separate background image for each monitor that is connected to the device.

Wallpaper

Provides a selection of predefined IGEL backgrounds:

- **Neutral**
- **Off**

- **IGEL** (Default)

Wallpaper style

Provides various design versions:

- **Auto**
- **Centered**
- **Tiled**
- **Stretched** (Default)
- **Scaled**
- **Zoomed**

Color style

Sets a fill color or a color gradient.

- **Solid color**
- **Horizontal gradient** (Default)
- **Vertical gradient**

Desktop color

The desktop color if **Wallpaper** is set to **Off**. Click the color preview square to open the color selector.

2nd desktop color

The second desktop color if **Wallpaper** is set to **Off** and a gradient **Color style** is selected. Click the color preview square to open the color selector.

Custom wallpaper download

☑ You can provide a user-specific background image on a download server. Specify the download server under **Desktop > Background > Custom Wallpaper Server**.

☐ Custom wallpaper is not used. (Default)

Custom wallpaper file

The name of the background image file

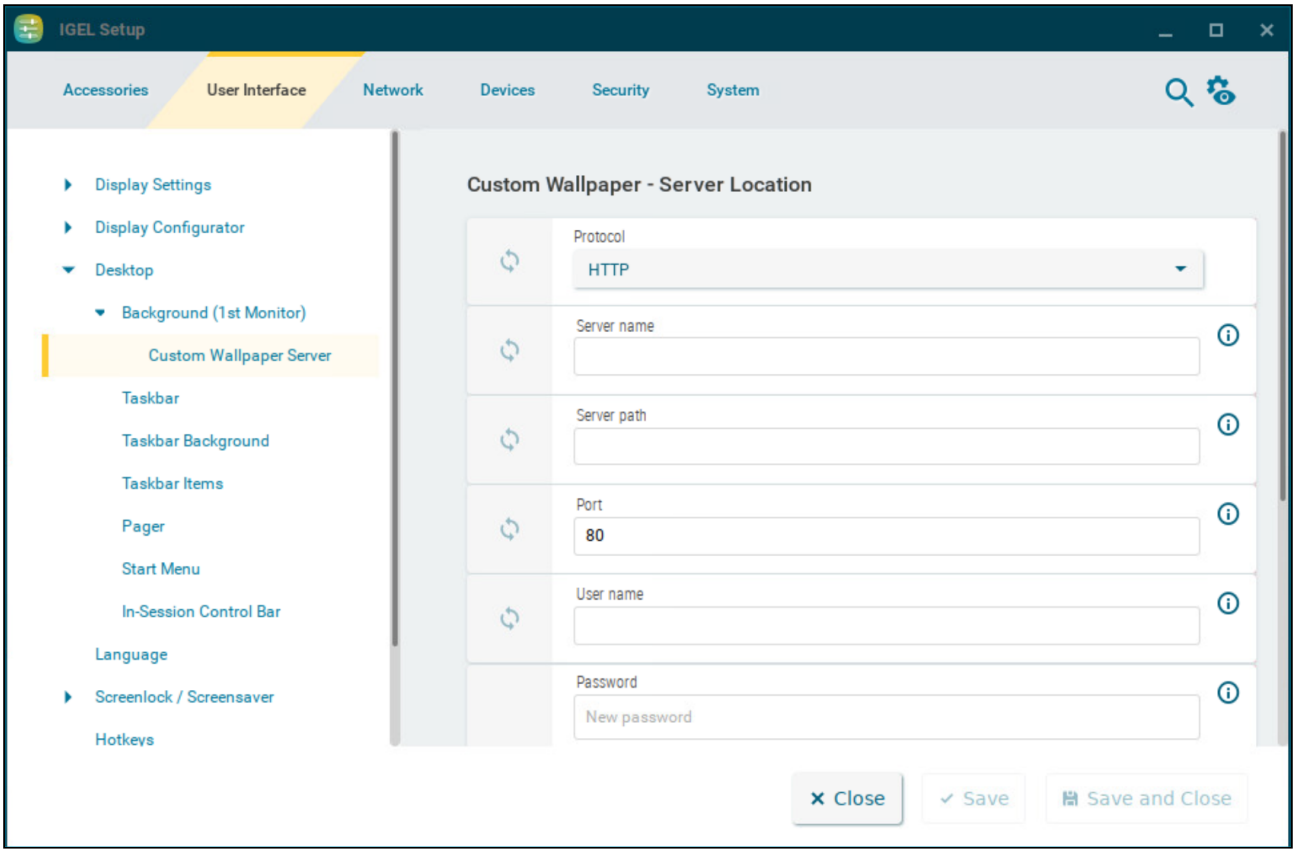
The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually through **Wallpaper update** under **Desktop > Background > Custom Wallpaper Server**. The download can also be launched from the IGEL Universal Management Suite (UMS) via the **Update desktop customization** command.

A user-specific boot image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an own background image and bootsplash. A total storage area of 25 MB is available for all user-specific images. For more information, see Firmware Customizations in the IGEL UMS.

Custom Wallpaper Server

This article shows how to configure the download server for your own background images in IGEL OS.

Menu path: **User Interface > Desktop > Background > Custom Wallpaper Server**



Protocol

Determines the protocol that is to be used. The following are available to choose from:

- **HTTP**: Download from a web server. (Default)
- **HTTPS**: Download from a TLS/SSL-secured web server
- **FTP**: Download from an FTP server
- **SecureFTP**: Download via SSH-secured FTP
- **FTPS**: Download from a TLS/SSL-secured FTP server
- **File**: The image file lies in the file system of the device, possibly as a shared NFS or Windows update. You can enter the location under **Local path**.

Local path

The path to the background image. The parameter is shown when **File** is selected as protocol.

Server name

Name or IP address of the server used

Server path

Directory in which you saved the background image

Port

Port used (Default: 80)

User name

Name of the user account on the server

Password

Password for this account

Wallpaper update

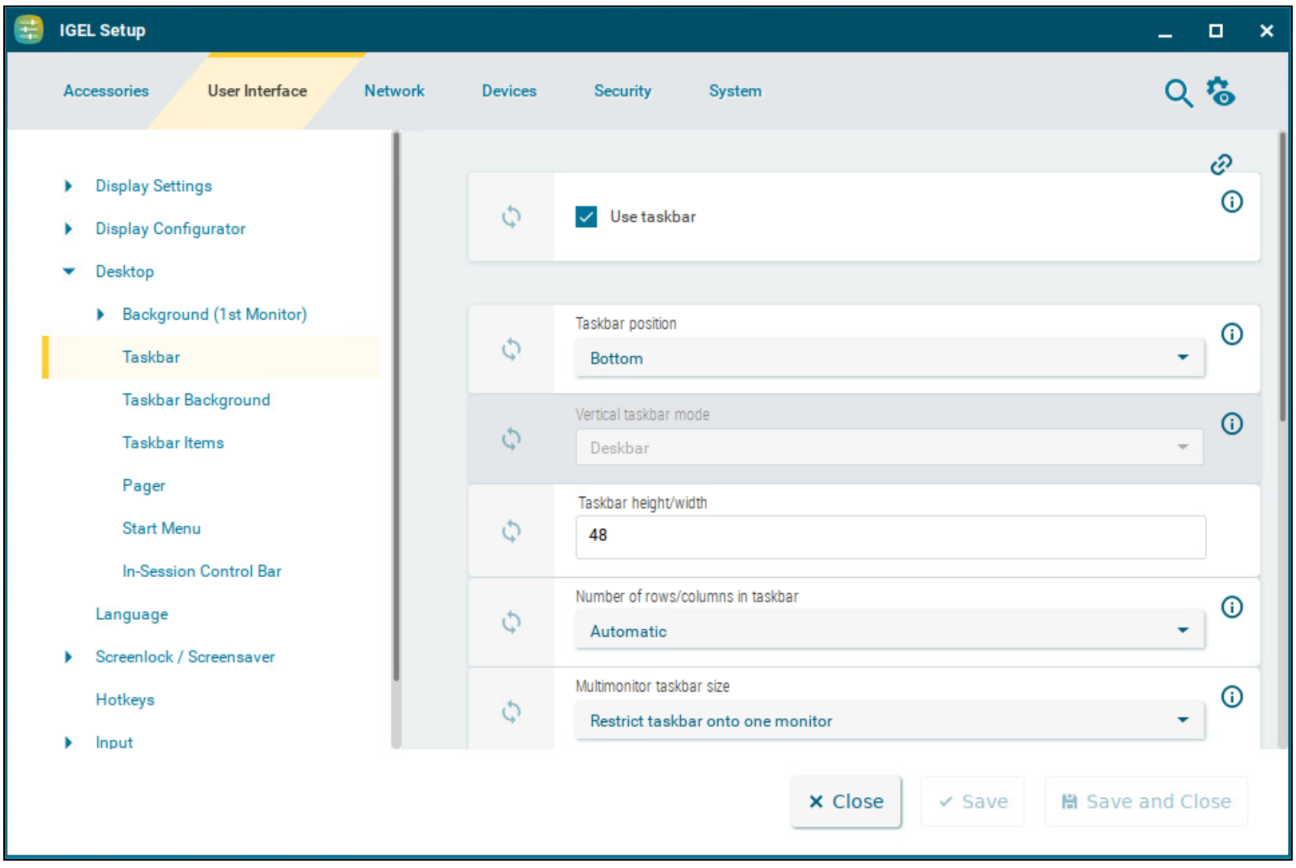
The button refreshes the background image when clicked.

Taskbar

This article shows how to enable and configure the taskbar in IGEL OS.

> Further settings can be found under **User Interface > Screenlock / Screensaver > Taskbar**. For detailed information on those settings, see Taskbar (see page 92).

Menu path: **User Interface > Desktop > Taskbar**



Use taskbar

☑ The taskbar is displayed and the setting options are available. (Default)

Taskbar position

Specifies the display position of the taskbar.
Possible values:

- **Bottom** (Default)
- **Top**
- **Left**
- **Right**

Vertical taskbar mode

Specifies how items are shown in the taskbar. This parameter is available if **Taskbar position** is set to **Left** or **Right**.
Possible values:

- **Vertical**: The session texts are rotated by 90°.
- **Deskbar**: The session texts are not shown. (Default)

Taskbar height/width

Specifies the size of the taskbar in pixels. This is the height of the taskbar if the position is top or bottom, and the width of the taskbar if the position is left or right. (Default: 48)

If **Maximum number of rows/columns in window button list** is set to **Automatic**, the window buttons as well as the icons in the Quick Start Panel will be shown in a number of rows depending on the height of the taskbar. The number of rows increases in increments of 55 pixels:

- 1 - 55 pixels: One row
- 56 - 110 pixels: Two rows
- 111 - 165 pixels: Three rows
- 166 - 220 pixels: Four rows
- 221 - 275 pixels: Five rows
- 276 or more pixels: Six rows

The **Maximum number of rows/columns in window button list** parameter is described under Taskbar Items in IGEL OS 12 (see page 72).

Number of rows/columns in taskbar

Specifies the number of rows for the Quick Start Panel. The following taskbar items can be broken down into a number of rows and columns: Icons in the Quick Start Panel, window buttons.
Possible values:

- **Automatic**: The number of rows for the Quick Start Panel depends on the height and width of the taskbar.
- **Numeric value**: The chosen value specifies the number of rows for the Quick Start Panel.

Multimonitor taskbar size

Specifies whether the taskbar is expanded onto several monitors or restricted to one monitor.
Possible values:

- **Restrict taskbar to one monitor**
- **Extend taskbar to all monitors**

Monitor

Specifies the screen on which the taskbar is shown. This parameter is available if **Multimonitor taskbar size** is set to **Restrict taskbar to one monitor**. (Default: 1st monitor)

Taskbar on top of all windows

☑ The taskbar is displayed on all screens, even in sessions with a full-screen window.

☐ The taskbar is not displayed in sessions with a full-screen window. (Default)

Taskbar auto hide

☑ The taskbar is hidden automatically and will only be shown if the mouse pointer is moved to the position of the taskbar at the edge of the screen.

☐ The taskbar is always displayed. (Default)

Auto hide behavior

Specifies when the taskbar is automatically hidden.
Possible values:

- **Intelligently**: The taskbar is shown as standard. The taskbar will be hidden if the space is needed by a window, e. g. a window in full-screen mode.
- **Always**: The taskbar is hidden as standard. The taskbar will be shown if the mouse pointer is moved to the edge of the screen.

Taskbar show delay

Time interval in milliseconds before the taskbar is shown. The mouse pointer must be at the edge of the screen constantly during this time interval. This setting is only effective if **Taskbar auto hide** is enabled. (Default: 600)

> With the show delay, you can prevent the taskbar for a full-screen session being covered by the device's taskbar. A show delay is necessary if the taskbar for the full-screen session is set to be shown automatically and both taskbars are positioned at the same screen edge. If no show delay is set and the user brings up the taskbar for the full-screen session, this will immediately be covered by the device's taskbar. During the show delay time interval, the user has time to move the mouse pointer away from the edge of the screen.

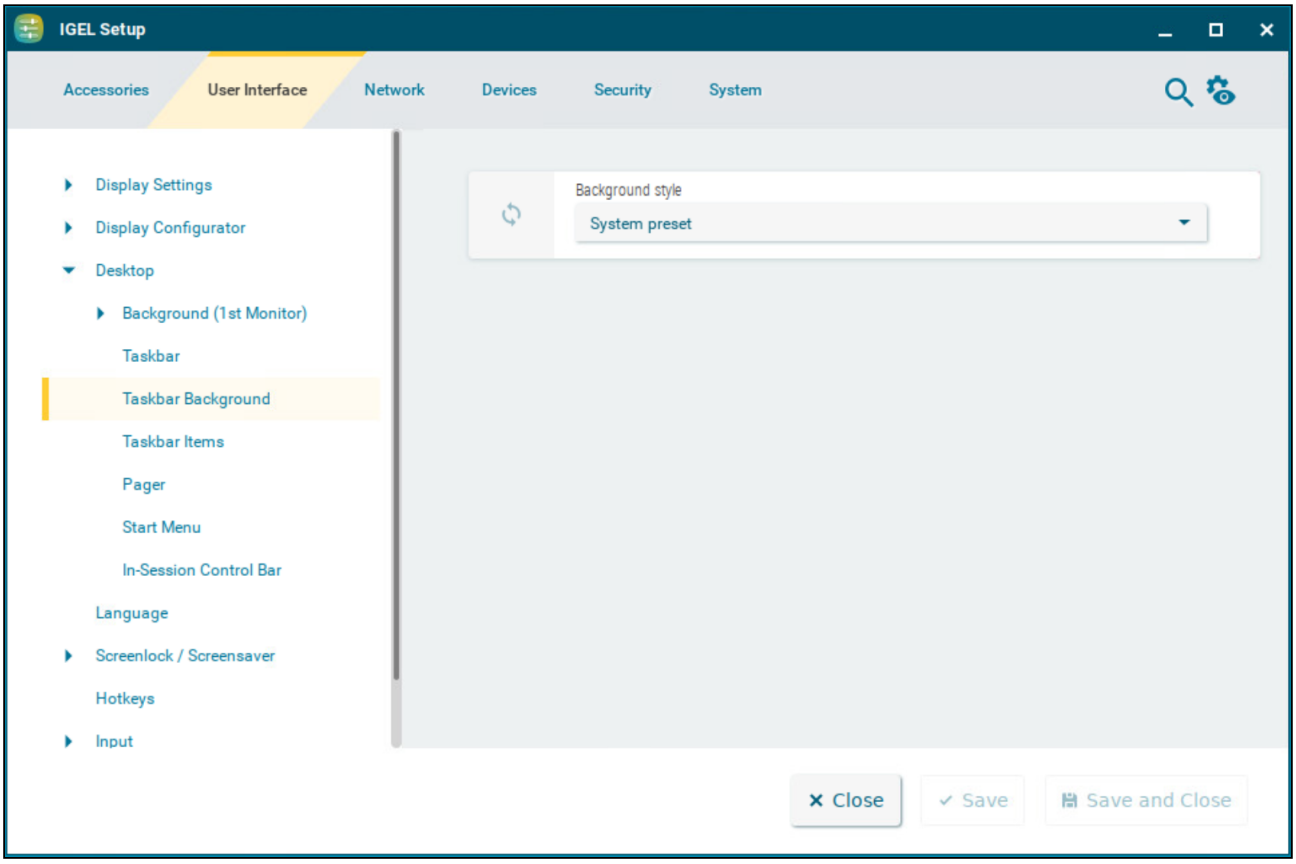
Taskbar hide delay

Time interval in milliseconds before the taskbar is hidden. This setting is only effective if **Taskbar auto hide** is enabled. (Default: 400)

Taskbar Background

This article shows how to configure the background style of the taskbar in IGEL OS.

Menu path: **User Interface > Desktop > Taskbar Background**



Background style
Possible values:

- **System preset** (Default)
- **Solid color**
- **Color gradient**
- **Background image**

Further settings depending on the style selection:

Taskbar color

The color for the taskbar. Click the color preview square to open the color selector.

2nd taskbar color

The 2nd color for the taskbar if you want to create gradient colors. Click the color preview square to open the color selector.

Reverse gradient

☑ The color gradient is reverse.

☐ The color gradient is normal. (Default)

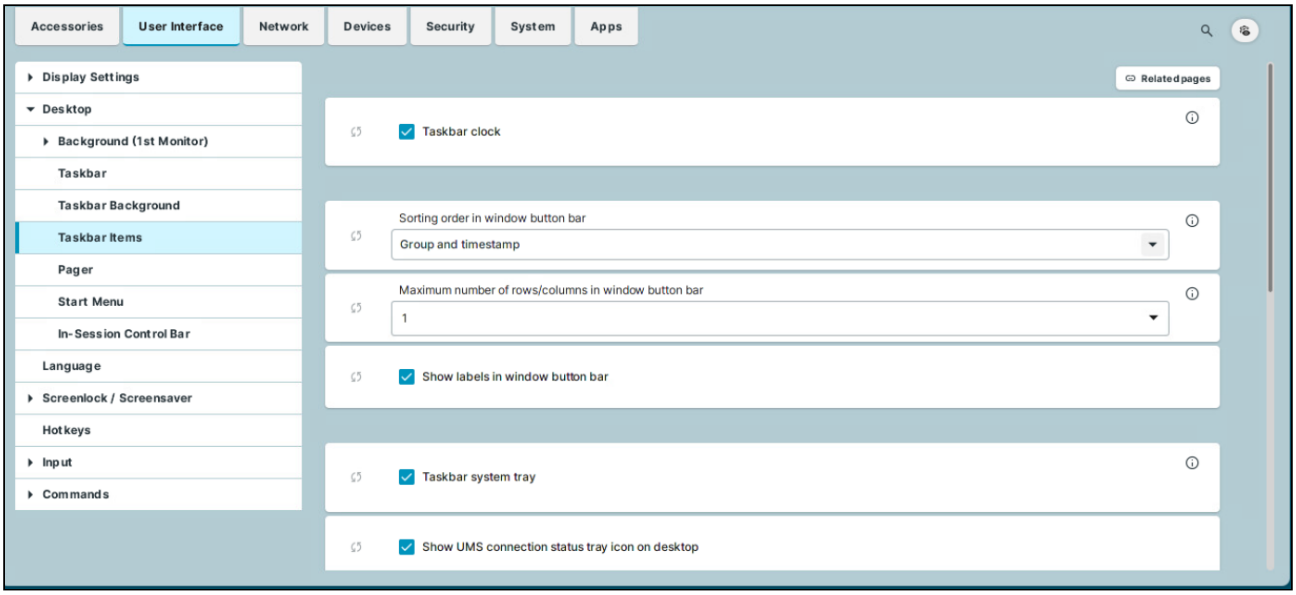
Background image path

Path to the background image

Taskbar Items in IGEL OS 12

This article shows how to configure taskbar items in IGEL OS.

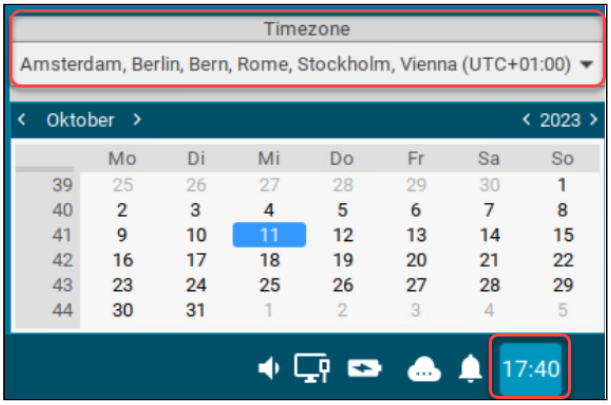
Menu path: **User Interface > Desktop > Taskbar Items**



Taskbar clock

☑ A clock is shown in the taskbar.

Clicking the taskbar clock displays the calendar and the **Timezone** dropdown menu. You can use the dropdown to set the timezone the device is located in. The dropdown menu is only accessible if the **System > Time and Date > Timezone systray settings** parameter is enabled. For details, see Time and Date (see page 277).



Sorting order in window button bar

Specifies the criteria according to which the window buttons are sorted.
Possible values:

- **Timestamp**: The window buttons are sorted in the chronological order in which the windows were opened.
- **Group and timestamp**: The window buttons are grouped according to the type of application. If, for example, a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted chronologically. (Default)
- **Window title**: The window buttons are sorted alphabetically.
- **Group and window title**: The window buttons are grouped according to type. If for example a number of setup applications are open, all associated window buttons will be arranged next to each other. Within the group, the window buttons are sorted alphabetically.
- **Drag'n'Drop**: You can order the buttons as you wish using drag and drop.

Maximum number of rows/columns in window button bar

Specifies the maximum number of rows available for window buttons.
Possible values:

- **Automatic**: The number of rows depends on the settings of the **Taskbar height/width** and **Number of rows/columns in taskbar** parameters under **User Interface > Desktop > Taskbar.** For details on the parameters, see Taskbar (see page 67).
- **Numeric values**: This value specifies the maximum number of rows. (Default: 1)

Show labels in window button bar

☑ The names of the ongoing sessions are displayed in the associated window buttons. (Default)

☐ Only the icons are displayed.

Taskbar system tray

☑ The system tray is shown in the taskbar. (Default)

> ⓘ The following parameters enable icons to access the system tray applications. For details on system tray apps, see Tray Applications in IGEL OS 12 (see page 353).
> The parameters for the desktop and the parameters for the locksreen are independent from each other. You need to enable / disable the icons for both use cases separately. You can enable taskbar items for the lockscreen under **User Interface > Desktop > Screenlock / Screensaver > Taskbar**. For more information, see Taskbar (see page 92).

Show UMS connection status tray icon on desktop

☑ The current status of the Universal management Suite (UMS) connection is shown in the system tray. For example, with the icon for connected. Clicking the icon displays information about the connected UMS server. (Default)

Show battery tray icon on desktop

☑ The current status of the battery is shown in the system tray. For example, with the icon . Hover over the icon to see information on the charge. Clicking the icon displays the battery tray app. (Default)

Show ethernet connection status tray icon on desktop

☑ The current status of the LAN network connection is shown in the system tray. For example, with the icon for connected. Clicking the icon displays the LAN tray app. (Default)

Show wifi connection status tray icon on desktop

☑ The current status of the Wi-Fi network connection is shown in the system tray. For example, with the icon . Clicking the icon displays the Wi-Fi tray app. (Default)

Show mobile-broadband connection status tray icon on desktop

☑ The current status of the mobile network connection is shown in the system tray. For example, with the icon or . Clicking the icon displays the mobile broadband tray app. (Default)

Show input settings tray icon on desktop

☑ If a mouse is detected, the icon is shown in the system tray. If a touchpad is detected, or both a mouse and a touchpad are detected, the icon is shown. Clicking the icon displays the mouse & touchpad tray app. (Default)

Show display tray icon on desktop

☑ The current display configuration icon is shown in the system tray. For example, with the icon. Clicking the icon displays the display tray app. (Default)

Show audio tray icon on desktop

☑ The and icons are shown in the system tray. Clicking the icon displays the sound tray app. (Default)

Size of icons in system tray

Specifies the size of system tray icons (volume, network connection etc.). You can select a pre-defined value or enter a numeric value.
Predefined values:

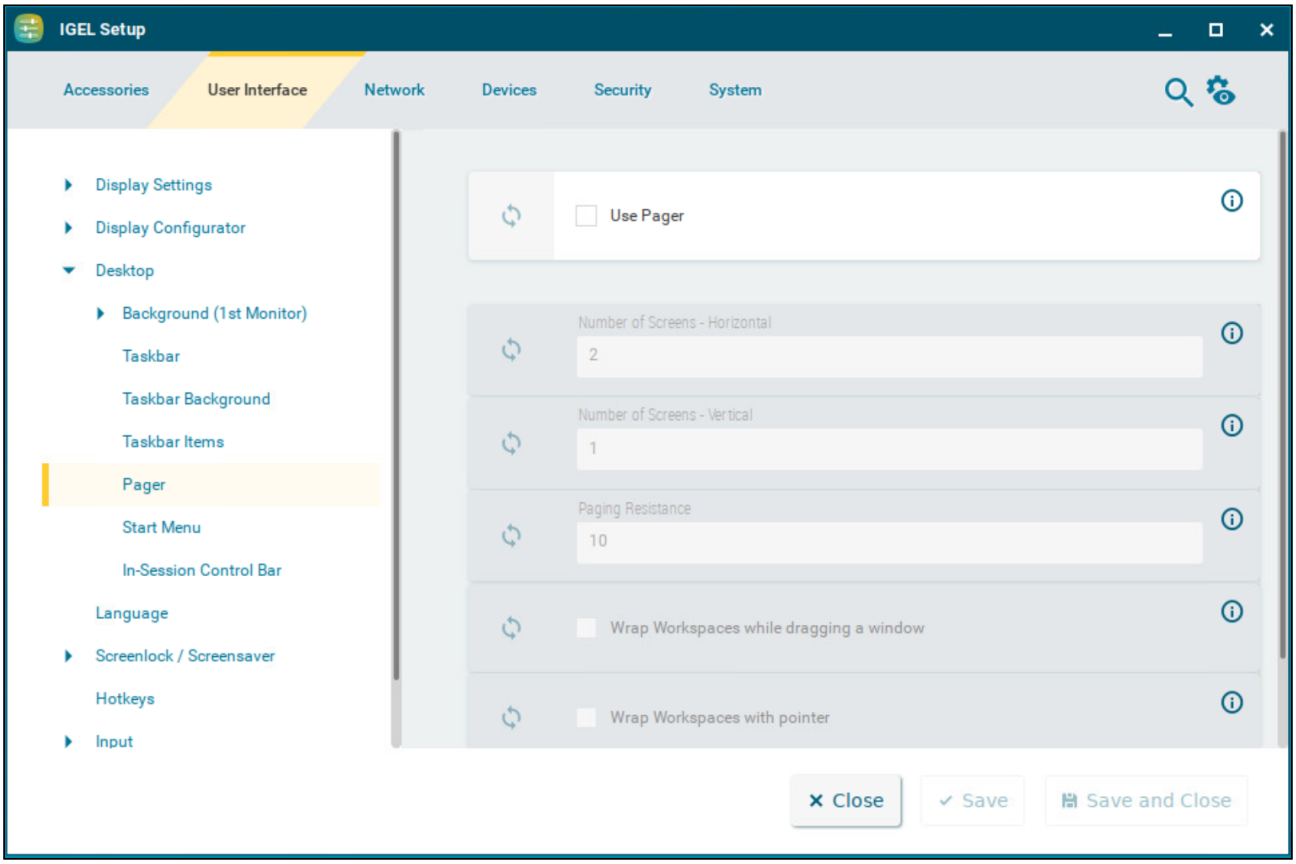
- **Automatic**: The size is adjusted to the height and width of the taskbar.
- **Small**: 20 pixels (Default)
- **Medium**: 40 pixels
- **Large**: 60 pixels

Pager

You can use the Pager tool to enable the use of multiple virtual desktops and organize your IGEL OS desktop. The Pager allows you to divide one desktop into several virtual workspaces. This article shows how to configure and use the Pager tool in IGEL OS. For details on how to use the pager, see the below section Using Pager (see page 77).

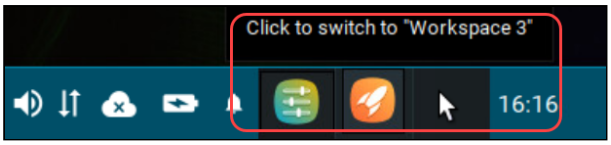
> ⚠ Make sure you have enabled **User Interface > Desktop > Taskbar > Taskbar on top of all windows** before using the Pager. For more information on the setting, see Taskbar (see page 67).

Menu path: **User Interface > Desktop > Pager**



Use pager

☑ The Pager is enabled. You can configure up to 25 virtual desktops. The Pager will be displayed on the right of the taskbar:



☐ The Pager is disabled. (Default)

Number of screens - Horizontal

Specifies how many workspaces will be shown next to each other. (Default: 2)

Number of screens - Vertical

Specifies how many workspaces will be shown above each other. (Default: 1)

> **Known Issue**
>
> The vertical value is implemented as horizontal and all the screens are shown next to each other. The configuration will be reworked in a future release.

Paging resistance

Specifies how many pixels the cursor needs to be moved over the edge of the screen before it triggers a switch of the desktop. (Default: 10)

You only need to use this setting if you enable at least one of the following options – **Wrap workspaces while dragging a window** or **Wrap workspaces with pointer**.

Wrap workspaces while dragging a window

☑ The desktop is switched as soon as a window is dragged out of view.

☐ The desktop is not switched when a window is dragged out of view. (Default)

Wrap workspaces with pointer

☑ The desktop is switched as soon as the mouse reaches the edge of the screen.

☐ The desktop is not switched when the mouse reaches the edge of the screen. (Default)

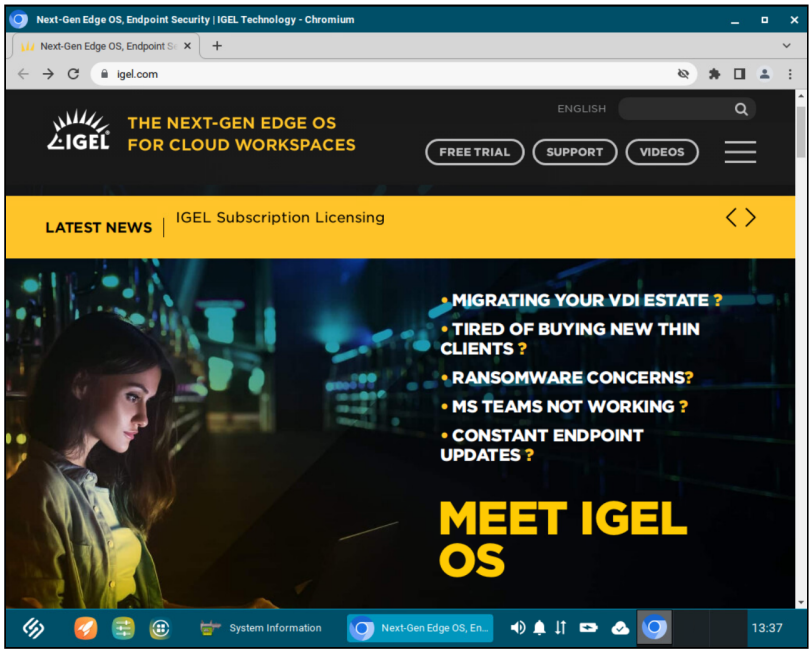
Using Pager

The Pager makes switching between multiple full-screen applications easier. Instead of minimizing/maximizing sessions or switching between them using key combinations, you simply click on the desired workspace using the mouse. When you switch back, the virtual desktop is displayed exactly as before (unless you restarted the system or changed the language in the IGEL Setup).

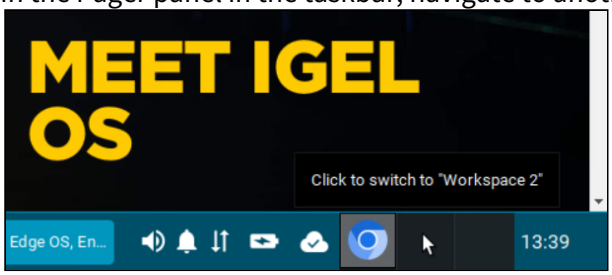
> The Pager can only be used in non-appliance mode.

To use multiple workspaces:

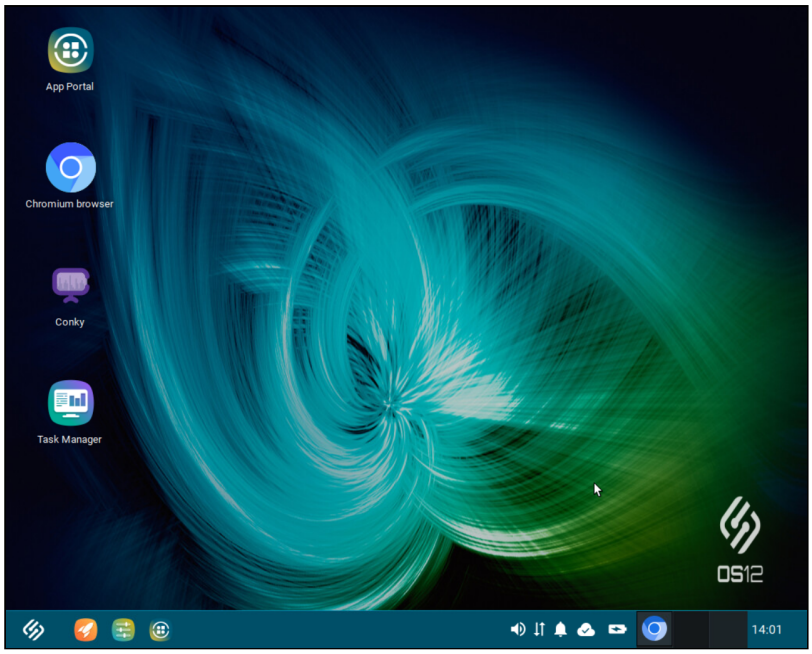
1. Launch the desired sessions/applications on your device, e.g. Chromium browser and System Information.



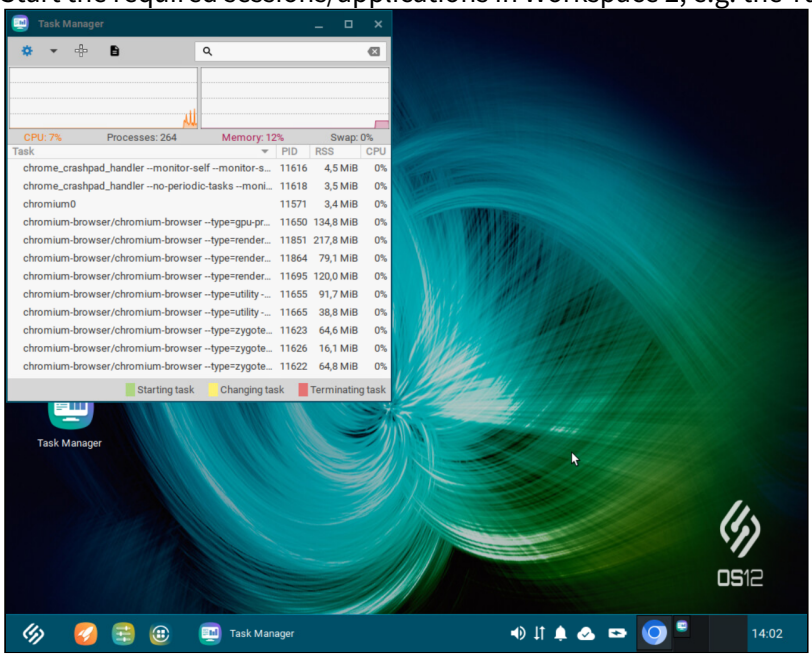
2. In the Pager panel in the taskbar, navigate to another workspace, e.g. Workspace 2, and click it.



   In Workspace 2, you will see the empty desktop, without opened sessions/applications.



3. Start the required sessions/applications in Workspace 2, e.g. the Task Manager.



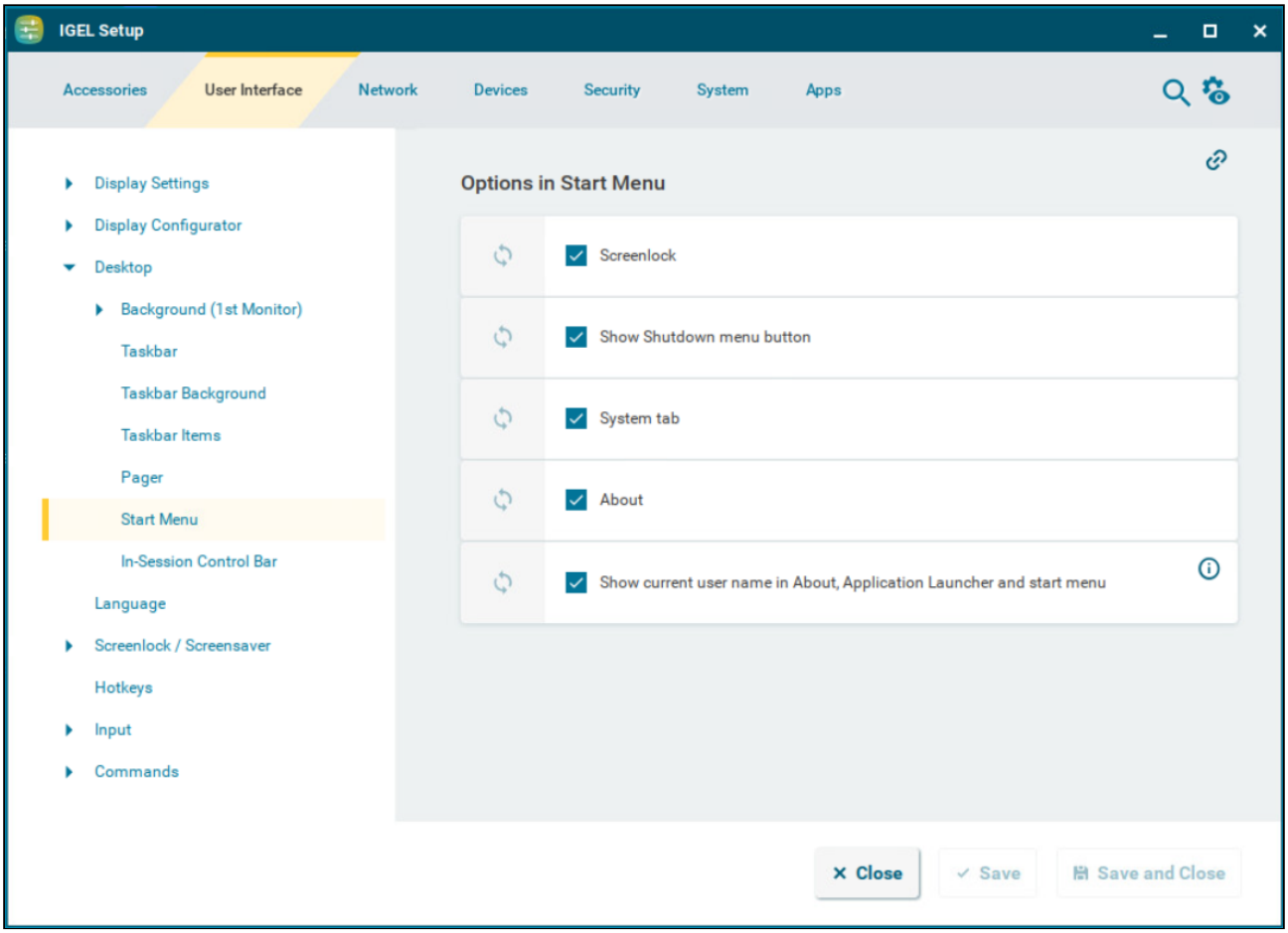
4. When you need to switch back to the Chromium browser and System Information, simply select the corresponding workspace (in this example, Workspace 1) in the Pager panel in the taskbar. Your desktop will be displayed exactly as before switching to Workspace 2.

Tip
You can use drag & drop to rearrange the sessions/applications between the workspaces. Click and hold the application/session symbol in the taskbar and drag it to the desired workspace in the Pager panel.

Start Menu

This article shows how to configure the desktop start menu in IGEL OS.

Menu path: **User Interface > Desktop > Start Menu**



The following options, which are all enabled by default, can be configured to be shown in the start menu:

- **Screenlock**

☑ The icon is shown. (Default)

ⓘ For the icon to be displayed, the following parameters need to be enabled:

- at least one login method under **Security > Logon**. For more information, see Logon.
- the **Require password to unlock (screenlock)** option under **User Interface > Screenlock / Screensaver > Options**. For more information, see Options.

- **Show Shutdown menu button**

☑ The icon is shown. (Default)

- **System tab**

☑ The icon is shown. (Default)

- **About**

☑ The icon is shown. (Default)

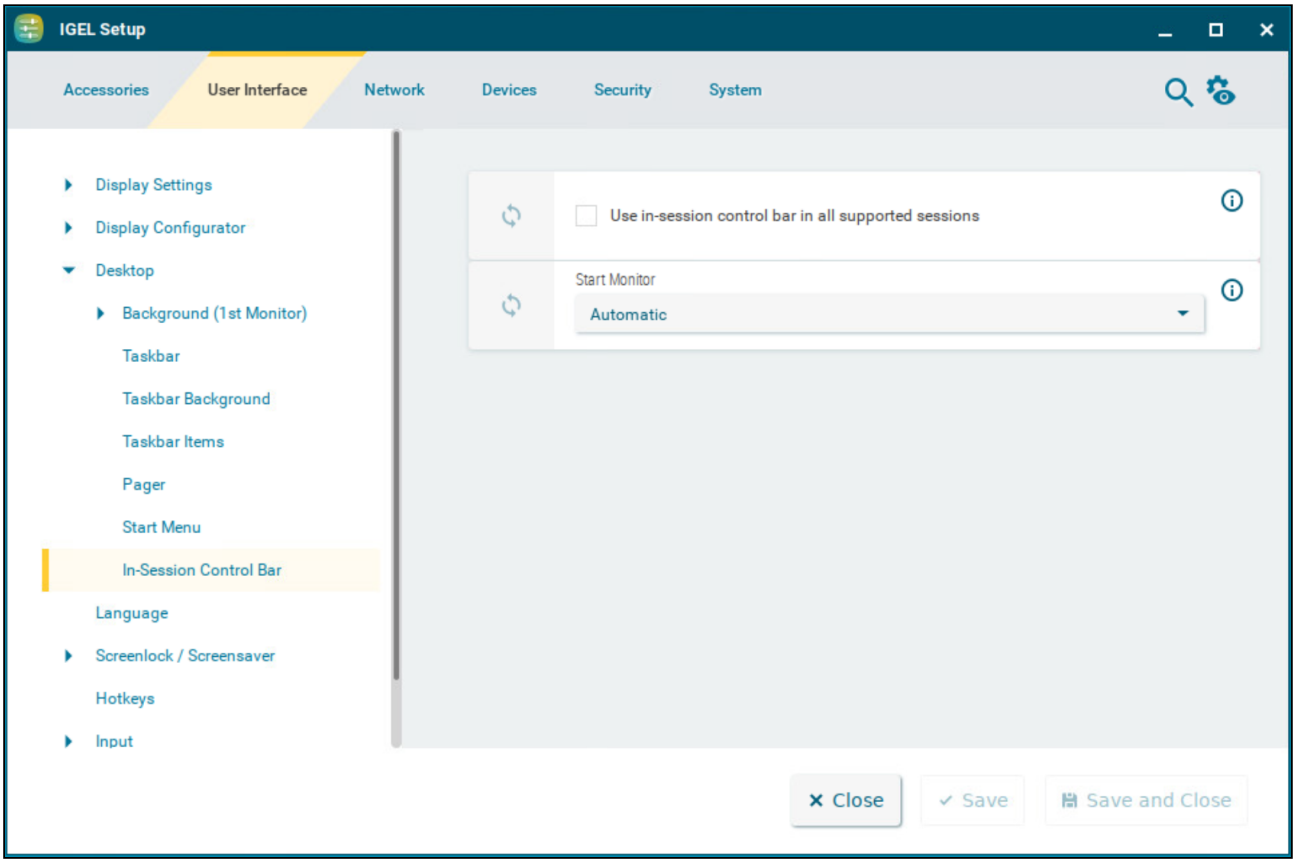
- **Show current user name in About, Application Launcher and start menu**

In order for user names to be recognized and passed on, you must configure two settings beforehand:
- Enable using Active Directory/Kerberos under **Security > Active Directory/ Kerberos**. For details, see Active Directory/Kerberos (see page 264)
- Enable local logon under **Security > Logon > Active Directory/Kerberos**. For details, see Active Directory/Kerberos (see page 254)

In-Session Control Bar

This article shows how to configure the control bar for full-screen sessions in IGEL OS.

Menu path: **User Interface > Desktop > In-Session Control Bar**



In a full-screen session, the in-session control bar allows you

- to eject a USB drive.
- to start the wireless manager (only available in Appliance Mode).
- to minimize the session view (not available in Appliance Mode).
- to end the session.

Use in-session control bar in all supported sessions

☑ The in-session control bar is shown. Depending on the configuration, the in-session control bar will be permanently visible or will be shown as soon as you move the cursor to the top edge of the screen.

☐ In-session control bar is not used. (Default)

> The in-session control bar is available for the following session types:
> - **Citrix** - see Citrix Workspace App
> - **ThinLinc**

Start Monitor

The monitor on which to start the session window.

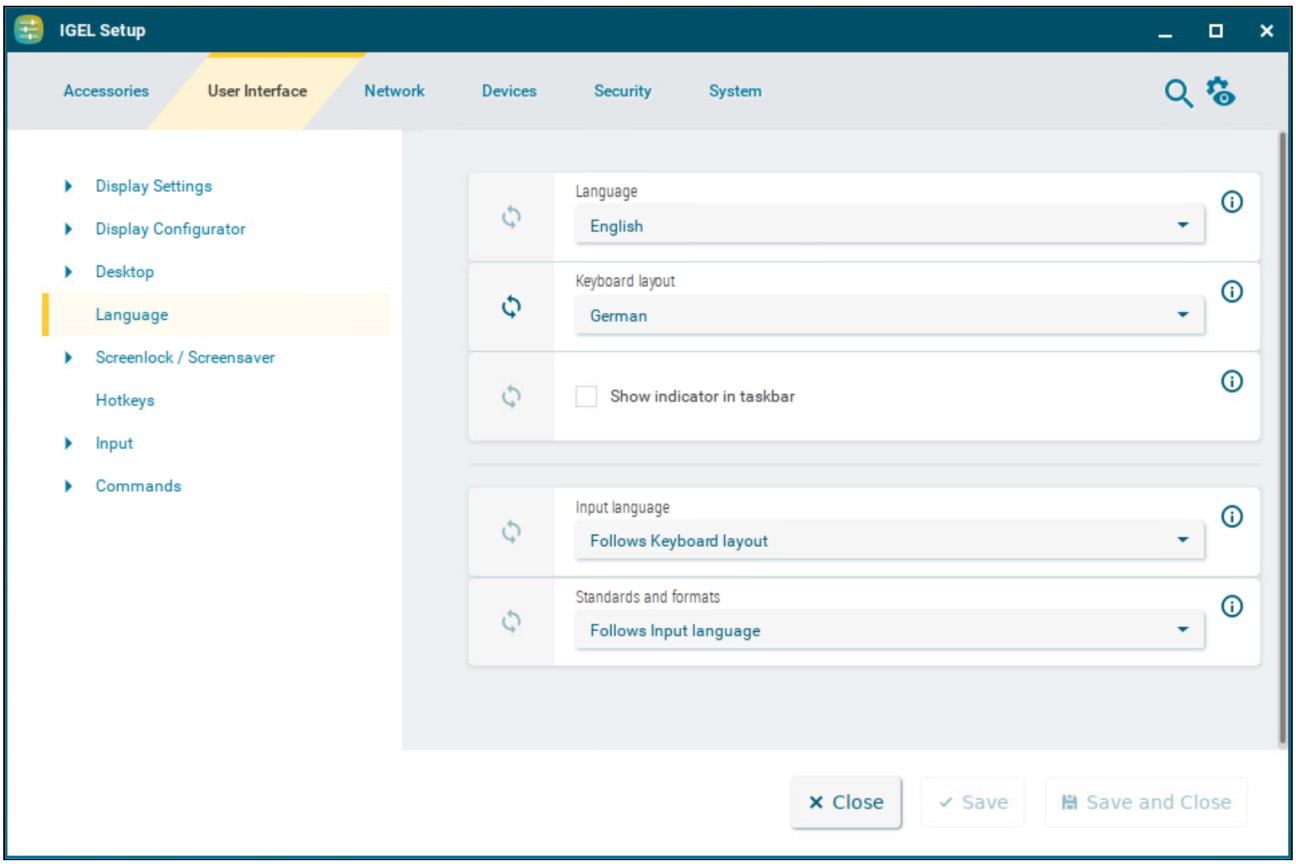
Using In-Session Control Bar

- To eject a USB device, click .
- To start the wireless manager in Appliance Mode, click .
- To minimize the session view, click . (Not available in Appliance Mode.)
- To end the session, click .
- To make the in-session control bar permanently visible, click .

Language

This article shows how to configure the country-specific language settings in IGEL OS.

Menu path: **User Interface > Language**



Language

The language of the user interface.

Keyboard layout

When the language is changed for the first time, the keyboard layout is automatically set to the same language.

Show indicator in taskbar

☑ Shows a country abbreviation for the keyboard layout in the taskbar.

☐ No indicator is shown. (Default)

Input language

The default setting is geared to the selected keyboard layout.

Standards and formats

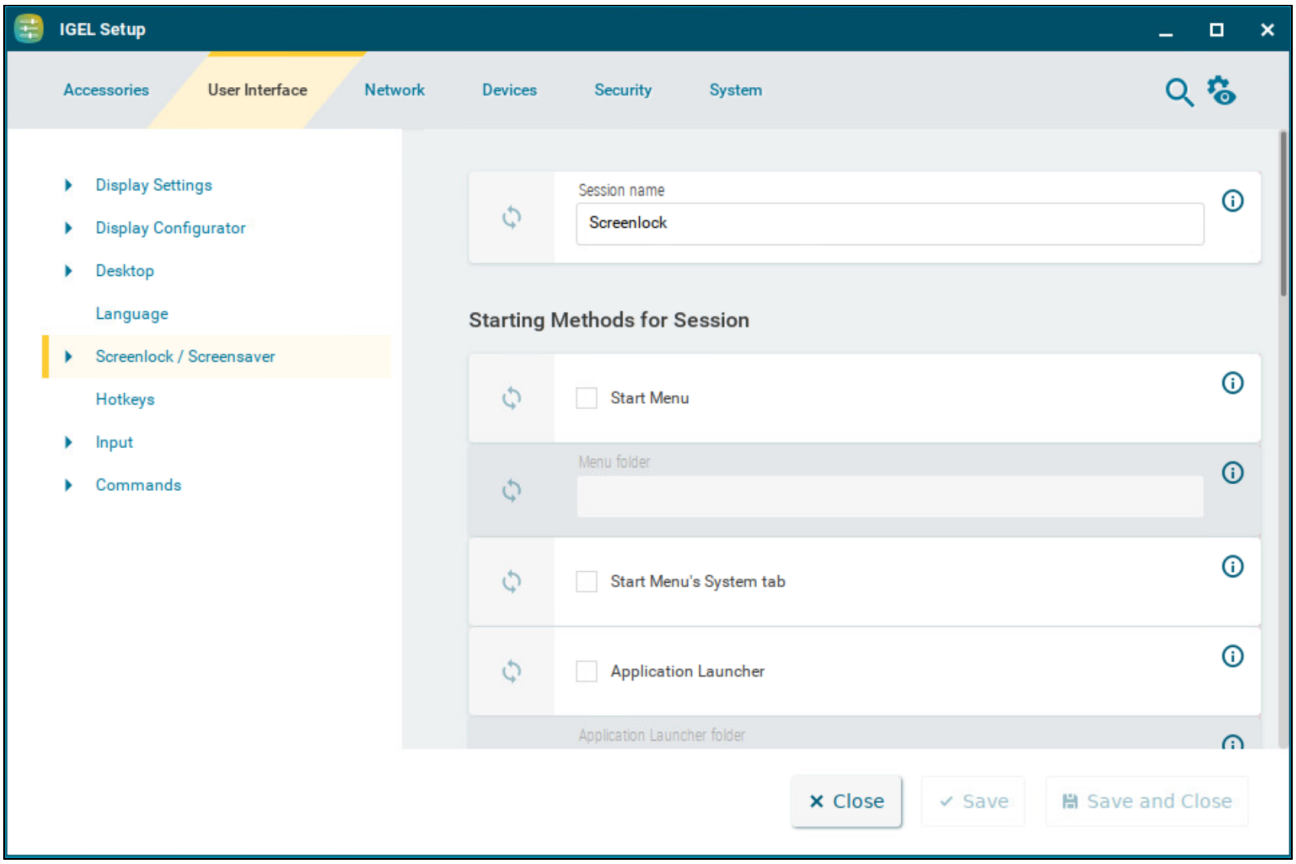
Sets the country-specific standards and formats, e.g. time and currency. The default setting is geared to the selected input language.

Screenlock / Screensaver

This article shows how to configure the starting methods for the screenlock and screensaver in IGEL OS.

> The automatic activation of the screensaver separate from the screenlock can be configured under **Screenlock / Screensaver > Options**. For details, see Options (see page 89).
> The look of the taskbar on the locked screen can be configured under **Screenlock / Screensaver > Taskbar**. For details, see Taskbar (see page 92).

Menu path: **User Interface > Desktop > Screenlock / Screensaver**



You can configure the screenlock and screensaver to be activated via icons in the Quick Start Panel and on the desktop or via hotkey.

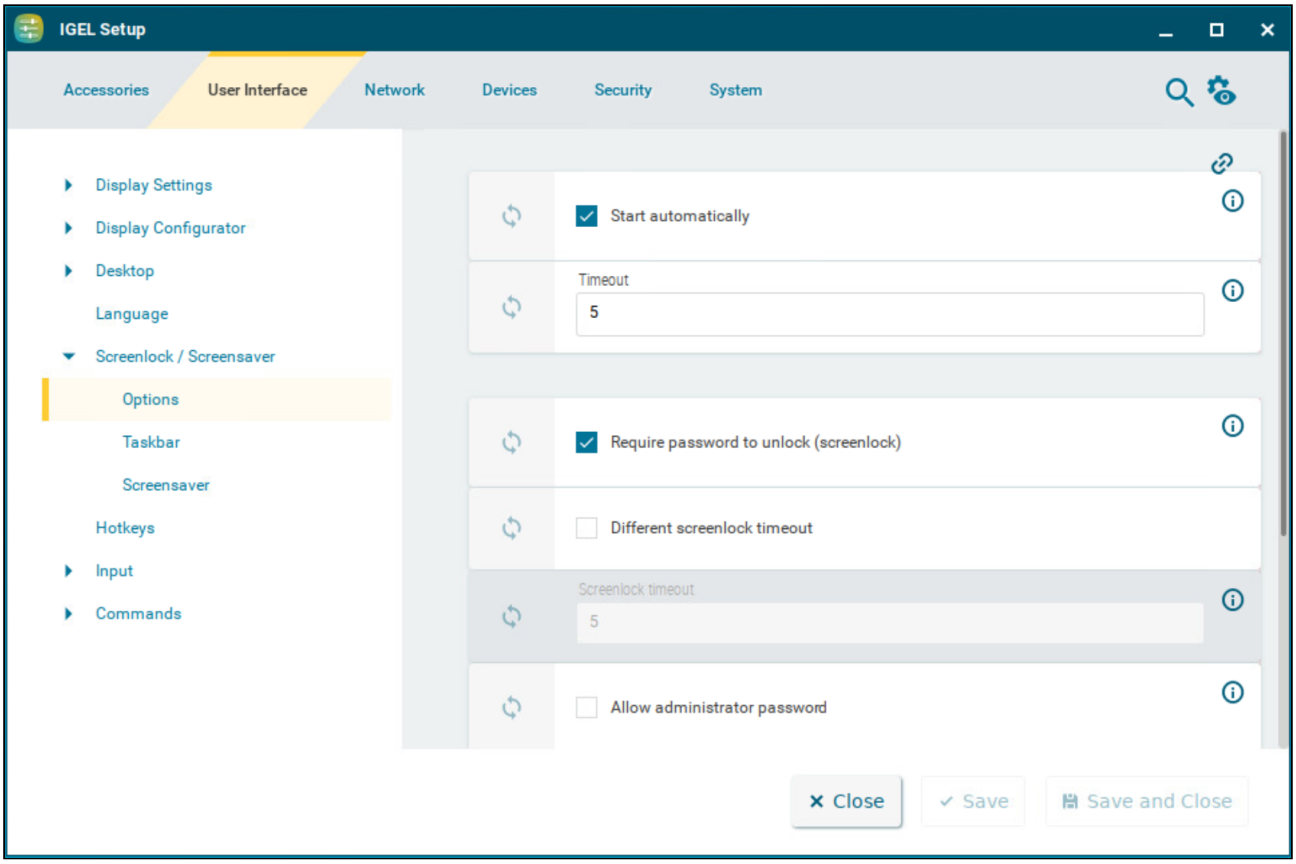
The starting methods parameters are described under Starting Methods for Apps (see page 376).

- Options (see page 89)
- Taskbar (see page 92)
- Screensaver (see page 96)

Options

This article shows how to configure the setting options for the screenlock and the screensaver in IGEL OS.

Menu path: **User Interface > Screenlock / Screensaver > Options**



Start automatically

☑ The screenlock and screensaver starts automatically if there is no activity on the device within the **Timeout** period. Depending on the configurations under **Require password to unlock (screenlock)** and **Allow administrator password**, the screen can be unlocked with the local user/administrator password. (Default)

Timeout

Period of time in minutes before the screenlock and the screensaver starts. (Default: 5)

Require password to unlock (screenlock)

☑ If a user is logged in, the same authentication is required to unlock the screen. For example, if the user is logged in via Active Directory (AD), the AD credentials are used to unlock the screen. For more information, see Active Directory/Kerberos (see page 254). The authentication methods can be configured under **Security > Logon**. For more information, see Logon (see page 250). (Default)

☐ The screen can be unlocked without authentication.

Different screenlock timeout

☑ You can specify a time limit for the screenlock to activate separately from the screensaver.

☐ The same time limit will be used for the screenlock and the screensaver. This means that after the set time the screen will be locked and then the screensaver will appear. (Default)

Screenlock timeout

Period of time in minutes before the screenlock starts. (Default: 5)

Allow administrator password

☑ Access is allowed for the user and the administrator. The screen can also be unlocked by the administrator password, if the administrator password is configured. For more information, see Password (see page 245).

☐ Access is allowed for the user only. (Default)

Countdown duration in seconds

Countdown time after which the screenlock is initiated. If the value is 0, the screen is locked without a countdown. (Default: 0)

The appearance of the digits for the countdown is specified together with the settings for the clock display under **Screenlock / Screensaver > Screensaver**. The following parameters are relevant for the countdown:

- **Clock display monitor**
- **Show seconds**
- **Horizontal clock position**
- **Vertical clock position**
- **Clock background color**
- **Clock foreground color**

For detailed information, see Screensaver (see page 96).

Countdown visual effect

While the countdown is running, a current screenshot is displayed in the background. This parameter determines the visual effect that the screenshot will be displayed with.
Possible options:

- **Dark screenshot**
- **Gray screenshot**

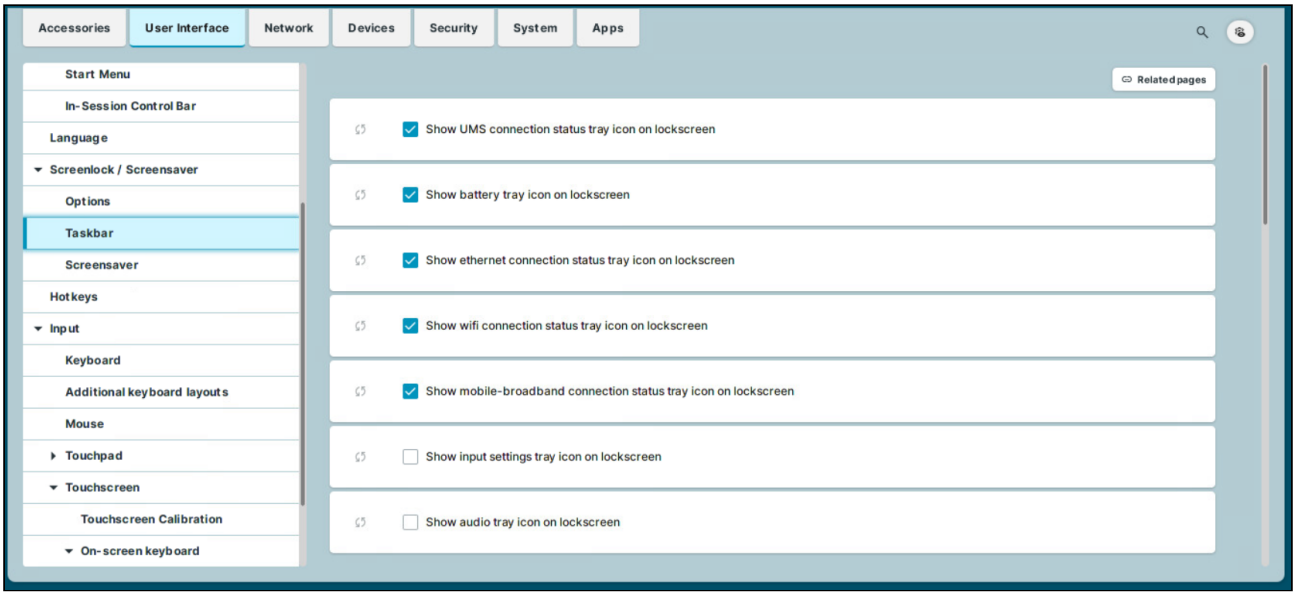
Countdown background image

Path and file name of an image file, which is displayed in the background while the countdown is running. This background image is displayed instead of the screenshot, if the path and file name are valid; if the field is empty, the screenshot is displayed. Supported file formats: JPEG, PNG, GIF. Example: `/images/image.jpg`

Taskbar

This article shows how to configure the taskbar for the login dialog and for when the screen is locked in IGEL OS.

Menu path: **User Interface > Desktop > Screenlock / Screensaver > Taskbar**



You can use the following parameters to enable / disable access to tray apps when the screen is locked. The parameters for the desktop (that can be found under **User Interface > Desktop > Taskbar Items**) and the parameters for the lockscreen are independent from each other. You need to enable / disable the icons for both use cases separately. For more information, see Tray Applications in IGEL OS 12 (see page 353) and Taskbar Items in IGEL OS 12 (see page 72).

Show UMS connection status tray icon on lockscreen

☑ When the screen is locked, the current status of the Universal management Suite (UMS) connection is shown in the system tray. For example, with the icon for connected. Clicking the icon displays information about the connected UMS server. (Default)

Show battery tray icon on lockscreen

☑ When the screen is locked, the current status of the battery is shown in the system tray. For example, with the icon . Hover over the icon to see information on the charge. Clicking the icon displays the battery tray app. (Default)

Show ethernet connection status tray icon on lockscreen

☑ The current status of the LAN network connection is shown in the system tray. For example, with the icon for connected. Clicking the icon displays the LAN tray app. (Default)

Show wifi connection status tray icon on lockscreen

☑ The current status of the Wi-Fi network connection is shown in the system tray. For example, with the icon . Clicking the icon displays the Wi-Fi tray app. (Default)

Show mobile-broadband connection status tray icon on lockscreen

☑ The current status of the network connection is shown in the system tray. For example, with the icon or . Clicking the icon displays the mobile broadband tray app. (Default)

Show input settings tray icon on lockscreen

☑ If a mouse is detected, the icon is shown in the system tray. If a touchpad is detected, or both a mouse and a touchpad are detected, the icon is shown. Clicking the icon displays the mouse & touchpad tray app.

☐ The icon is not shown when the screen is locked. (Default)

Show audio tray icon on lockscreen

☑ The and icons are shown in the system tray. Clicking the icon displays the sound tray app.

☐ The icon is not shown when the screen is locked. (Default)

Taskbar Settings for the Login Dialog

Show taskbar in login screen

☑ A taskbar is shown in the login screen. (Default)

Show clock

☑ A clock is shown in the taskbar in the login screen. (Default)

Show keyboard layout switcher

☑ A keyboard layout switcher is shown in the taskbar in the login screen. (Default)

Show on-screen keyboard button

☑ A button to start an on-screen keyboard is shown in the taskbar in the login screen.

☐ The button is not shown. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is started automatically with the login screen.

☐ The on-screen keyboard is not started automatically. (Default)

Show reboot button

☑ The reboot button is shown in the taskbar in the login screen.

☐ The button is not shown. (Default)

Show shutdown button

☑ The shutdown button is shown in the taskbar in the login screen. (Default)

Taskbar Settings When the Screenlock Is Active

Show taskbar in screenlock

☑ A taskbar is shown when the screen is locked. (Default)

Show clock

☑ A clock is shown in the taskbar when the screen is locked. (Default)

Show keyboard layout switcher

☑ A keyboard layout switcher is shown in the taskbar when the screen is locked. (Default)

Show on-screen keyboard button

☑ A button to start an on-screen keyboard is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is started automatically when the screen is locked.

☐ The on-screen keyboard is not started automatically. (Default)

Show reboot button

☑ The reboot button is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Show shutdown button

☑ The shutdown button is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Show logoff button

☑ The logoff button is shown in the taskbar when the screen is locked.

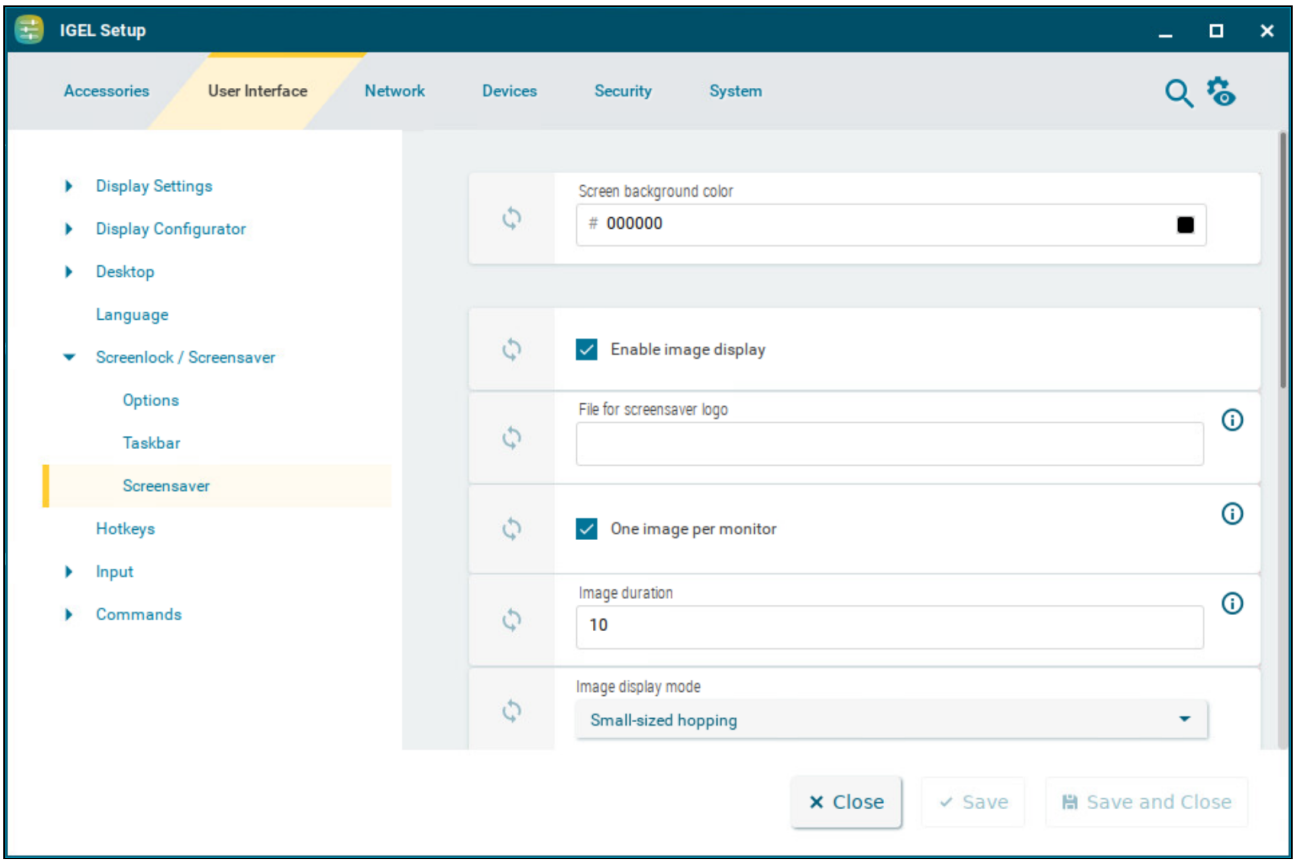
☐ The button is not shown. (Default)

Screensaver

This article shows how to configure the screensaver in IGEL OS.

You can configure the activation of the screensaver under **Screenlock / Screensaver > Options**. For details, see Options (see page 89).

Menu path: **User Interface > Desktop > Screenlock / Screensaver > Screensaver**



Screen background color

Color palette for determining the background color of the screen in screensaver mode. Click the color preview square to open the color selector.

Enable image display

☑ An image will be shown as the screensaver. (Default)

File for screensaver logo

Complete path for an individual image file or directory that contains an unlimited number of images. If no path is given, the IGEL logo will be used.

> If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The display time for the images can be configured under **Image duration**.

One image per monitor

☑ If a number of monitors are used, a different image will be shown on each one. (Default)

☐ Images will be distributed over the monitors.

Image duration

Time in seconds until the image is changed. (Default: 10)

Image display mode

Type of display. The following are available to choose from:

- **Small-sized hopping**: Small images are shown in changing positions. (Default)
- **Medium-sized hopping**: Larger images are shown in changing positions.
- **Full-screen center cut-out**: The images are shown in full-screen size. However, they may be clipped.
- **Full-screen letterbox**: The images are shown as large as possible in relation to the screen size.

Clock display monitor

Selects the monitor on which the clock is to be shown. The following are available to choose from:

- **None** (Default)
- **All**
- **Display [1-8]**

Show seconds

☑ Time is shown with seconds in digital format.

☐ Time is shown without seconds in digital format. (Default)

Clock display size

The following sizes are available to choose from:

- **Tiny**
- **Small**

- **Medium**
- **Large**
- **Huge**

Horizontal clock position

The following screen positions are available to choose from:

- **Left**
- **Center**
- **Right**

Vertical clock position

The following screen positions are available to choose from:

- **Top**
- **Center**
- **Bottom**

Clock background color

Color palette for determining the background color of the clock. Click the color preview square to open the color selector.

Clock background opacity percentage

The opacity of the clock background. (Default: 75)

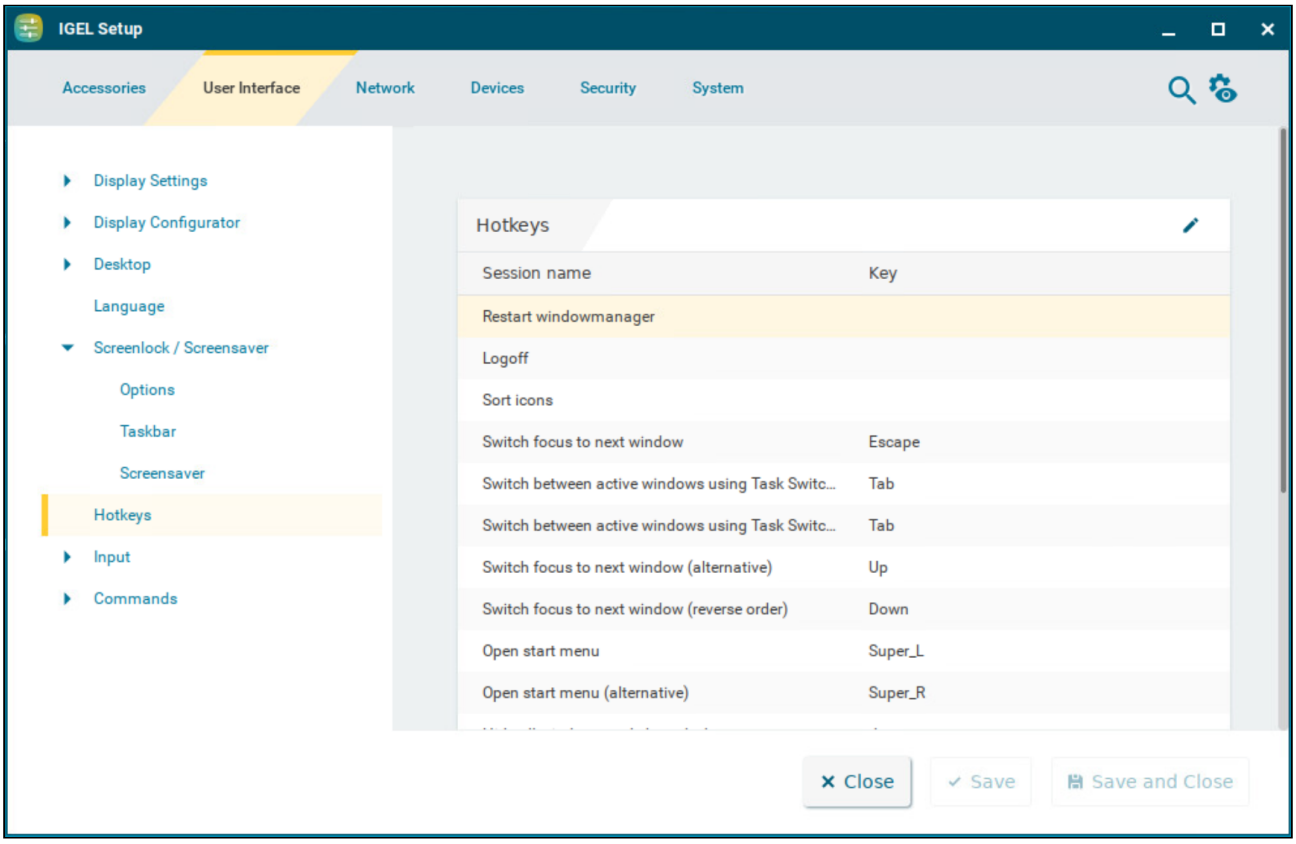
Clock foreground color

Color palette for determining the color of the numbers displayed. Click the color preview square to open the color selector.

Hotkeys

Hotkeys configured for frequently used operations make it easier to use the device. A hotkey is a combination of one or more modifiers and an alphanumeric key. This article shows how to configure hotkeys in IGEL OS.

Menu path: **User Interface > Hotkeys**



Editing Hotkeys

You can enable or disable hotkeys and change the keys used:

1. Click to edit the hotkey of the selected operation.
2. Use the **Hotkey** option to enable the hotkey.

3. Select a predefined **Modifier**.
   A modifier is a key symbol or key combination. These are the pre-defined modifiers and the associated key symbols:
   - **None**: No modifier is used
   - **Shift**: ⇧
   - **Ctrl**: [Ctrl]
   - **Win**:
     > When this keyboard key is used as a modifier, it is represented as Win; when it is used as a key, it is represented as `Super_L`.
   - **Alt**: [Alt]

   Key combinations are formed as follows with `|`:
   - **Ctrl|Alt**: [Ctrl] + [Alt]
4. Enter a **Key** that is to be used as the hotkey to start the operation.
   > To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`
5. Click **Confirm**.

Input

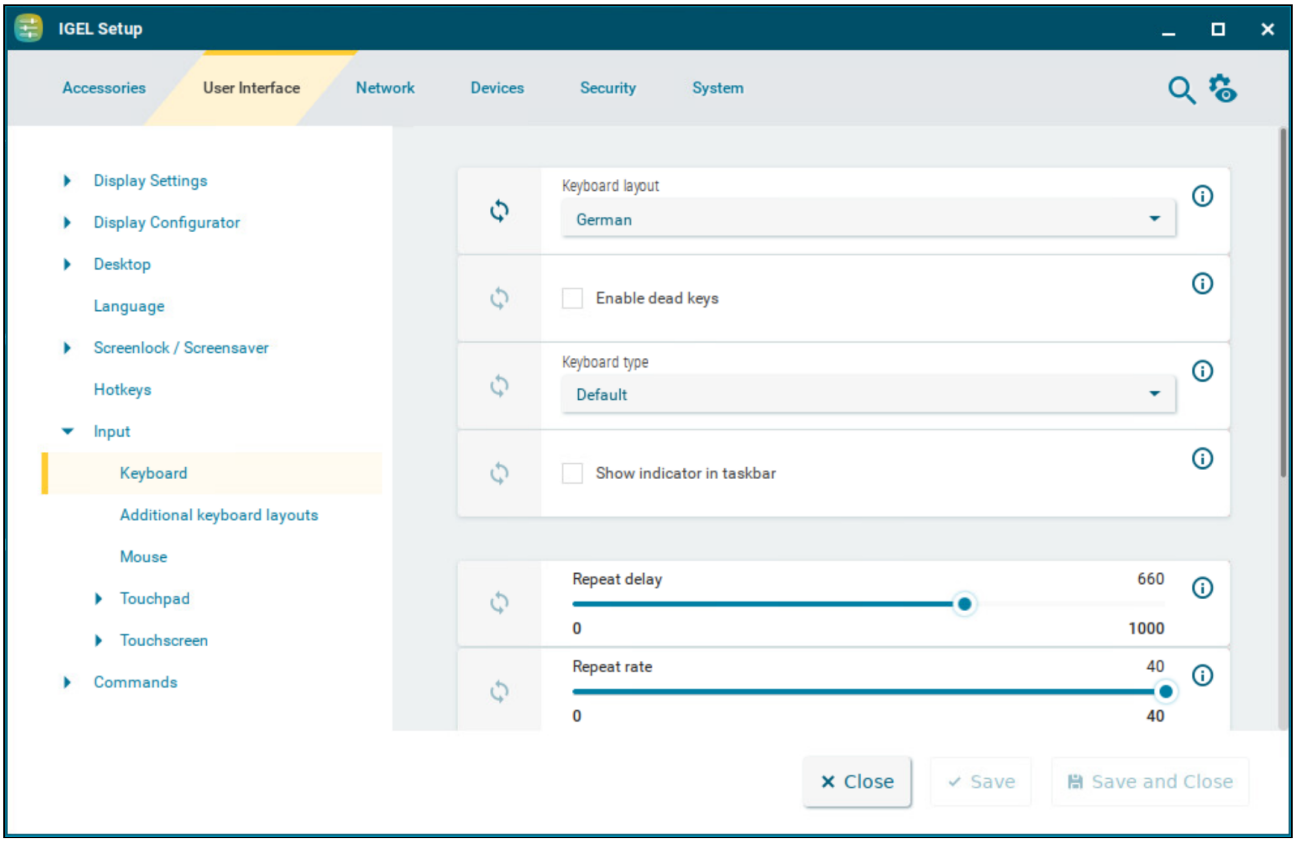
The following input devices can be configured in IGEL OS.

- Keyboard (see page 102)
- Additional Keyboard Layouts (see page 104)
- Mouse (see page 107)
- Touchpad (see page 111)
- Touchscreen (see page 120)

Keyboard

This article shows how to configure the keyboard settings in IGEL OS.

Menu path: **User Interface > Input > Keyboard**



Keyboard layout

Specify the keyboard layout. The selected layout applies to all parts of the system including emulations, window sessions and X applications.

Enable dead keys

☑ Dead keys can be used to enter special characters.

☐ Dead keys cannot be used to enter special characters. (Default)

Keyboard type

Specifies the keyboard type.
Possible values:

- **Default**: Automatically selects the keyboard type according to the computer type (Macbook, Chromebook or PC105 for all others).
- **Standard PC keyboard (105 keys)**
- **IBM keyboard (122 keys)**
- **Trimodal keyboard**
- **Sun Type 6 keyboard**
- **Chromebook**
- **Macbook**
- **Macbook international**
- **Thinkpad**

Show indicator in taskbar

☑ Shows the language code for the keyboard in the taskbar.

☐ Hides the language code for the keyboard in the taskbar. (Default)

Repeat delay

Determines the delay (in milliseconds) before automatic repetition begins. (Default: 660)

Repeat rate

Determines the number of times a character repeats per second. (Default: 40)

Test

Free-text area to test the repeat settings.

Start with NumLock on

☑ NumLock will be enabled automatically during the boot process. (Default)

Secure keyboard input with Cherry SECURE BOARD

☑ A secure keyboard input mode will be enabled for the connected Cherry SECURE BOARD. In this mode, keyboard traffic between the keyboard and the endpoint is transmitted over a TLS 1.3 encrypted connection. The standard keyboard channel will be locked, which means that keyboard input devices without the secure mode will be blocked; see https://www.cherry-world.com/cherry-secure-board-1-0.html.

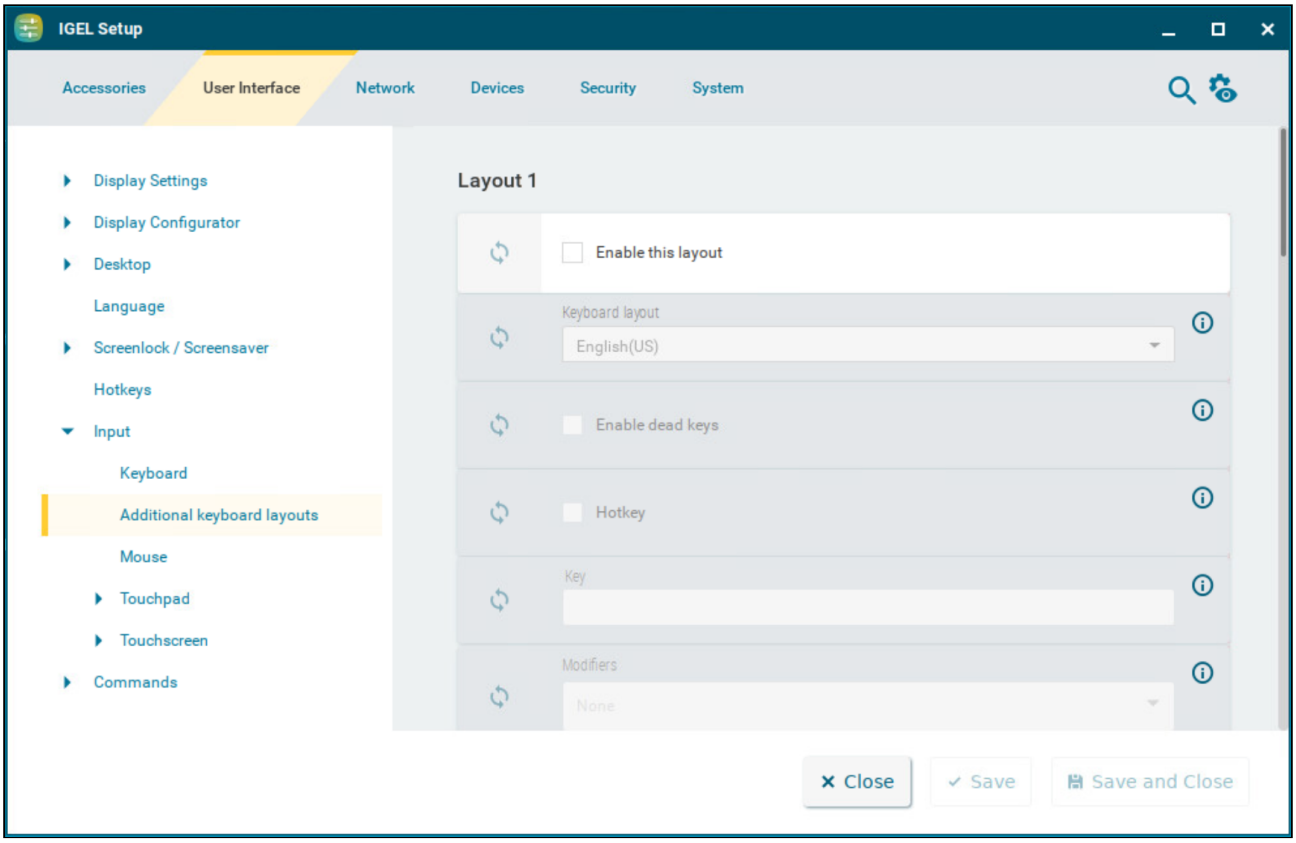
☐ The secure keyboard input mode is disabled. (Default)

Additional Keyboard Layouts

This article shows how to configure additional keyboard layouts in IGEL OS.

For information on how to configure an on-screen keyboard, see On-screen Keyboard (see page 124).

Menu path: **User Interface > Input > Additional Keyboard Layouts**



Layout [1-3]

Enable this layout

☑ Keyboard layout is enabled and can be defined.

☐ Keyboard layout is disabled. (Default)

Keyboard layout

Selects the language for the keyboard layout.

Enable dead keys

Enable this function if the keyboard used supports dead keys for special characters.

Hotkey

☑ A hotkey can be used to switch to this keyboard.

☐ The hotkey is disabled. (Default)

Key

Key for the hotkey

Modifiers

Additional modifier for the hotkey

Hotkey for Default Keyboard Layout

Activate hotkey to switch to the default keyboard layout

☑ A hotkey can be used to take you back to the default keyboard layout. This is useful when a number of keyboard layouts are configured.

☐ The hotkey is disabled. (Default)

Hotkey

Key for the hotkey

Modifiers

Additional modifier for the hotkey

Hotkey for Next Keyboard Layout

Activate hotkey to switch between a number of keyboard layouts

☑ A hotkey which switches to the next keyboard layout can be used. This is useful when a number of keyboard layouts are configured.

☐ The hotkey is disabled. (Default)

Hotkey

Key for the hotkey

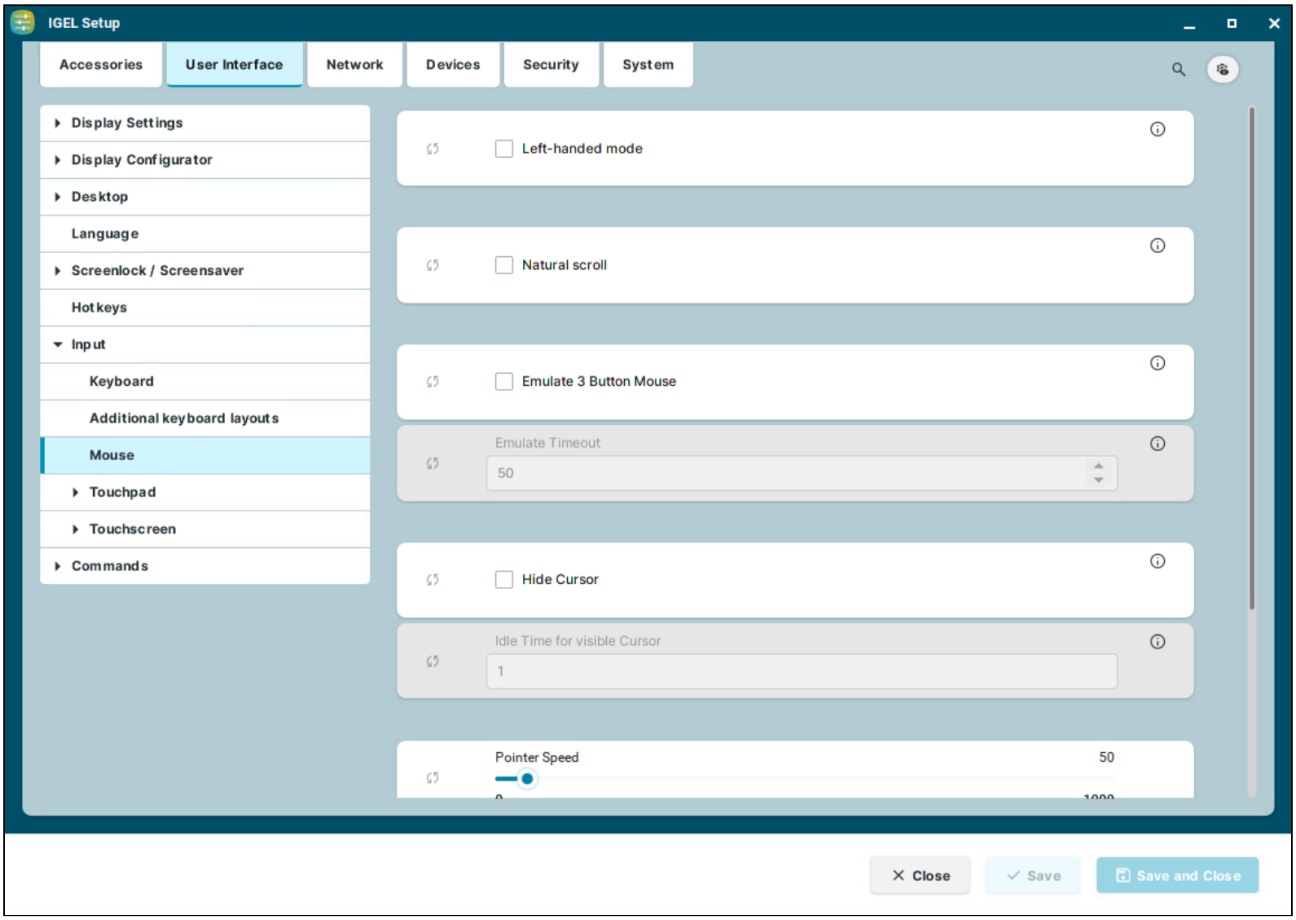
Modifiers

Additional modifier for the hotkey

Mouse

This article shows the mouse settings that you can configure in IGEL OS 12.

Menu path: **User Interface > Input > Mouse**



Left-handed mode

☑ The mouse is in left-handed mode.

☐ The mouse is in right-handed mode. (Default)

Natural scroll

☑ When scrolling with the mouse wheel, the screen content moves in reverse to the wheel movement. If you scroll the wheel down, the screen moves upwards and vice-versa.

☐ When scrolling with the mouse wheel, the screen content moves synchronously to the wheel movement. If you scroll the wheel down, the screen moves downwards and vice-versa. (Default)

Emulate 3 button mouse

☑ Enables emulation of the third (middle) mouse button for mice with only two physical buttons. This third button is emulated by pressing both buttons at the same time. The **Emulate timeout** determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.

☐ Disables emulation of the third (middle) mouse button for mice with only two physical buttons. (Default)

Emulate timeout

Determines how long (in milliseconds) the driver waits before deciding whether two buttons were pressed at the same time.

Hide cursor

☑ The mouse pointer will be hidden after the defined time limit.

☐ The mouse pointer is never hidden. (Default)

Idle time for visible cursor

The period after which the pointer is hidden.

Pointer speed

Determines the mouse resolution in counts per inch.

Double click interval

Changes the maximum interval in milliseconds between two consecutive mouse clicks which are to be recognized as a double-click. The smaller the interval, the faster the consecutive clicks need to happen, to be recognized as a double click.

Double click distance

Changes the maximum distance in pixels between two clicks which are to be recognized as a double-click. The object under the second click is double-clicked.

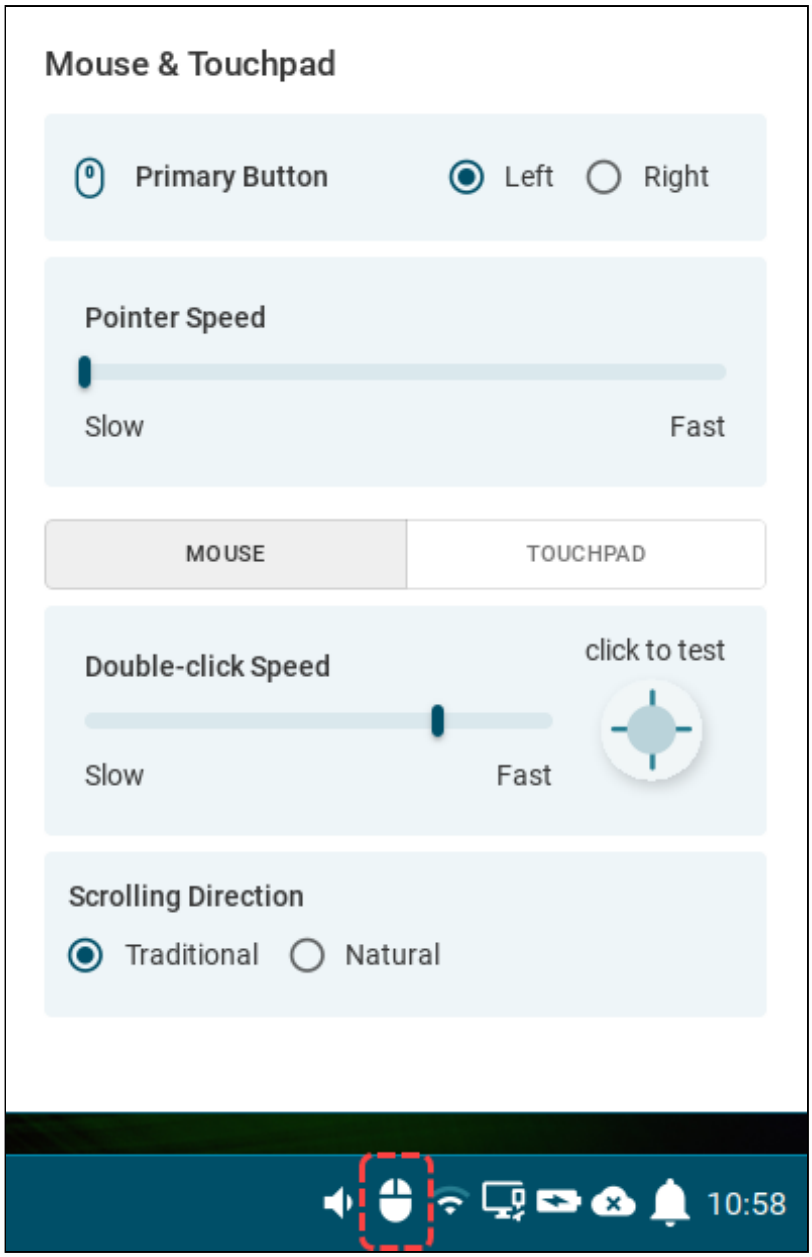
ⓘ If the **Show input settings tray icon on desktop** option is enabled under **User Interface > Desktop > Taskbar Items**, and a mouse is detected, you can use the Mouse & Touchpad tray app to quickly configure the following mouse settings:

- **Primary Button**
  Sets the primary button both for mouse and touchpad. In IGEL Setup, you can configure this through **Left-handed mode**.

- **Pointer Speed**
  Sets the speed of the pointer both for mouse and touchpad. In IGEL Setup, you can configure this through **Pointer speed**.

- **Double-click Speed**
  Sets how fast two consecutive mouse clicks need to happen to be recognized as a double-click. You can test this with the **click to test** area. In IGEL Setup, you can configure this through **Double click interval**. The smaller the interval, the faster the consecutive clicks need to happen, to be recognized as a double click.

- **Scrolling Direction**
  Sets the direction of the screen movement when scrolling with the mouse. In IGEL Setup, you can configure this through **Natural scroll**.

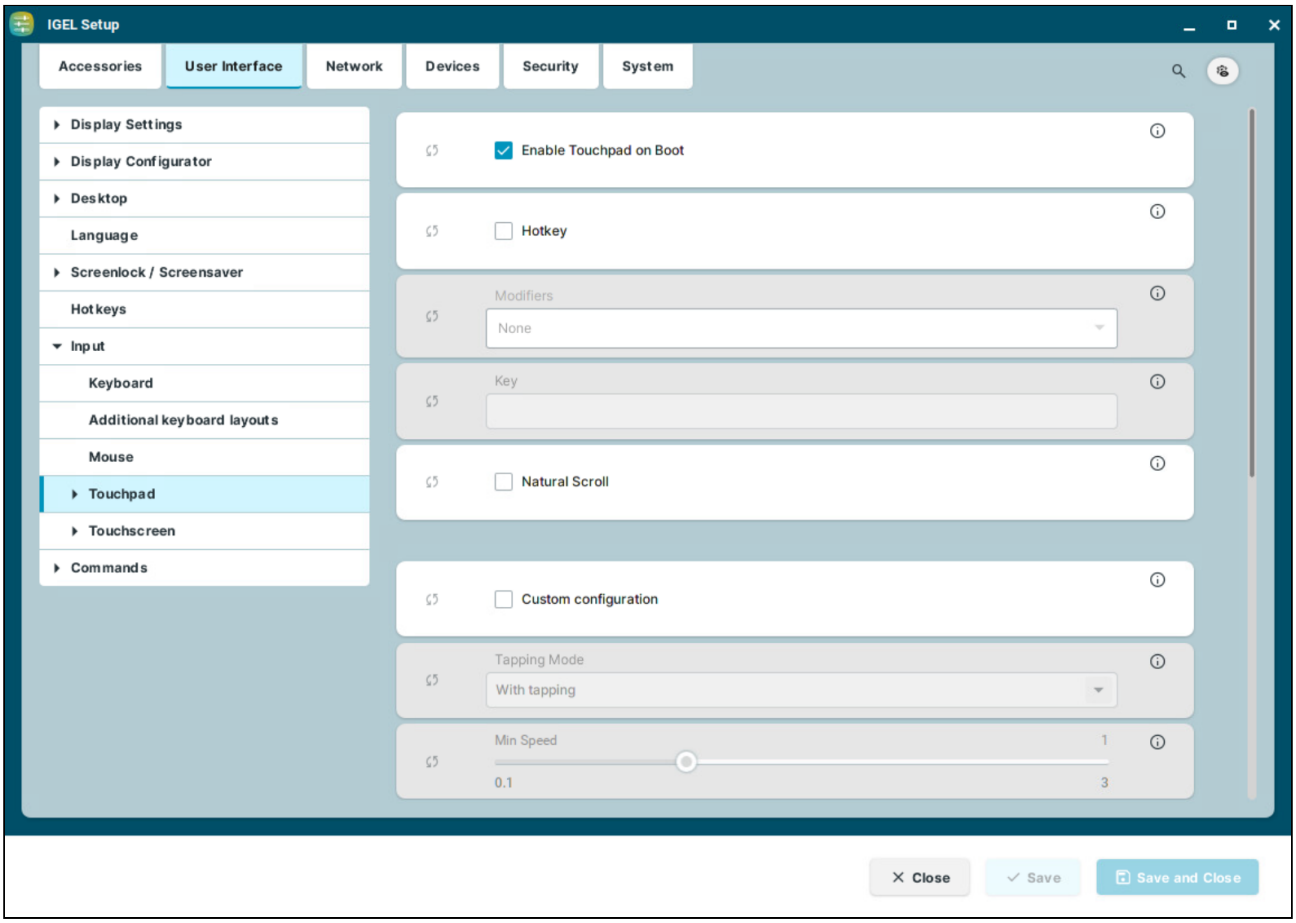

Mouse & Touchpad
Primary Button
Left
Right
Pointer Speed
Slow
Fast
MOUSE
TOUCHPAD
Double-click Speed
click to test
Slow
Fast
Scrolling Direction
Traditional
Natural
10:58

Touchpad

This article shows the touchpad settings that you can configure in IGEL OS 12.

> The actual settings depend on the hardware supported by the particular touchpad.

Menu path: **User Interface > Input > Touchpad**



Enable touchpad on boot

☑ The touchpad is enabled on boot. This can be overridden by the hotkey configured below. (Default)

Hotkey

☑ Each time you press the hotkey, you activate or deactivate the touchpad.

☐ No hotkey can be used to activate or deactivate the touchpad. (Default)

Modifiers

Modifiers for the hotkey

Key

Key for the hotkey

Natural Scroll

☑ When scrolling through the touchpad, the screen content moves synchronously to the fingers' movement. If you move your fingers down, the screen moves downwards and vice-versa.

☐ When scrolling through the touchpad, the screen content moves in reverse to the fingers' movement. If you move your fingers down, the screen moves upwards and vice-versa. (Default)

Custom configuration

☑ Further touchpad settings can be configured according to your needs.

☐ No custom configuration can be made. (Default)

Tapping mode

Switches the tapping mode on or off.
Possible values:

- **With tapping** (Default)
- **Without tapping**

Min speed

Minimum speed of the pointer in seconds. (Default: 1.00)

Max speed

Maximum speed of the pointer in seconds. (Default: 1.75)

Acceleration

Acceleration from the minimum to the maximum speed in seconds. (Default: 0.01)

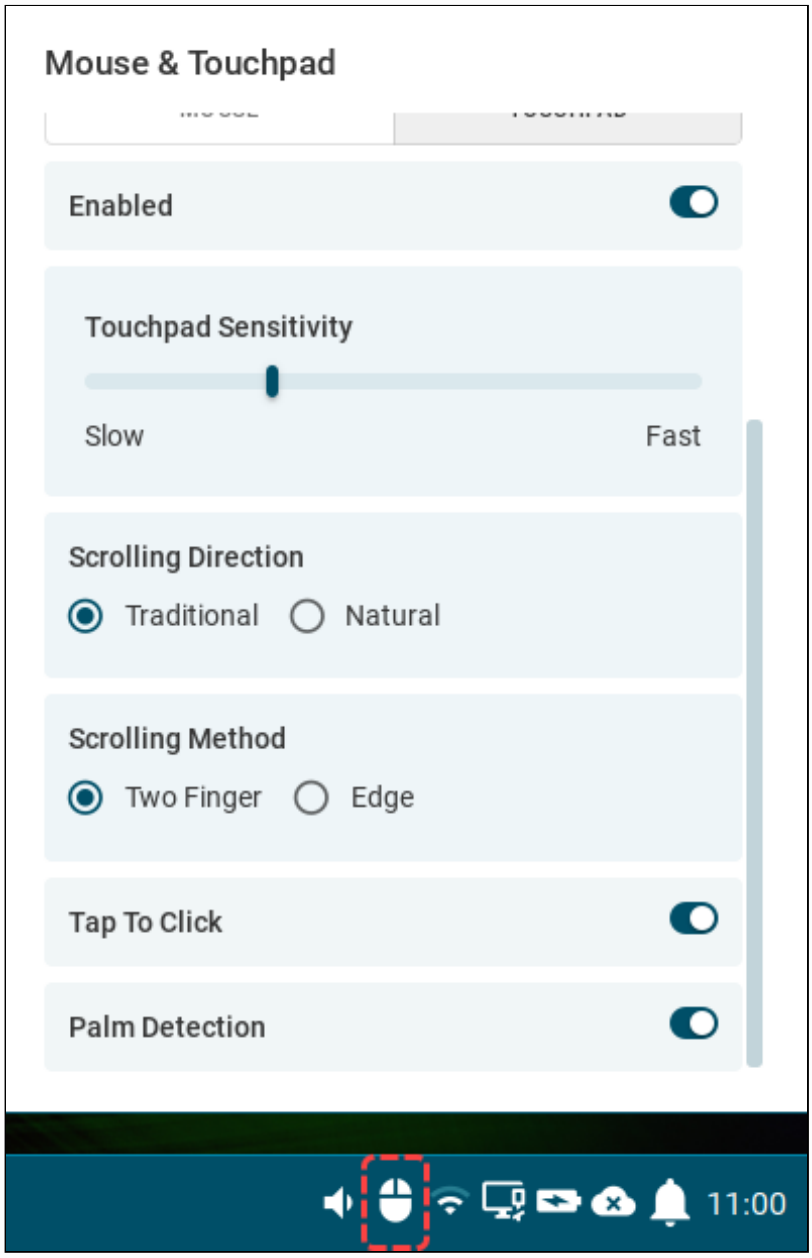
With some touchpads, you can assign mouse actions to tapping the corners of the touchpad. The action can be configured for each corner to trigger a right, left, or middle mouse click.

- **Top left action** (Default: No action)
- **Top right action** (Default: Middle mouse button)
- **Bottom left action** (Default: No action)
- **Bottom right action** (Default: Right mouse button)

If the **Show input settings tray icon on desktop** option is enabled under **User Interface > Desktop > Taskbar Items**, and a touchpad is detected, you can use the Mouse & Touchpad tray app to quickly configure the following touchpad settings:

- **Primary Button**
  Sets the primary button both for mouse and touchpad. In IGEL Setup, you can configure this through **Left-handed mode** under **User Interface > Input > Mouse**.
- **Pointer Speed**
  Sets the speed of the pointer both for mouse and touchpad. In IGEL Setup, you can configure this through **Pointer speed** under **User Interface > Input > Mouse**.
- **Enabled**
  The toggle buttons enables/disables the touchpad.
- **Touchpad Sensitivity**
  Sets how sensitive the touchpad is to the touch. In IGEL Setup, you can configure this through **Min speed**, **Max speed**, and **Acceleration**. If you have those values custom configured, it is advised not to change the slider in the tray app, as it will reset the levels in the IGEL Setup.
- **Scrolling Direction**
  Sets the direction of the screen movement when scrolling with the touchpad. In IGEL Setup, you can configure this through **Natural scroll**.
- **Scrolling Method**
  Sets the type of finer movement to be detected as scrolling. In IGEL Setup, you can configure this through **Two finger vertical scroll** and **Two finger horizontal scroll** under **User Interface > Input > Touchpad > Scrolling**.
- **Tap to Click**
  The toggle switch enables/disables clicking with a tap on the touchpad. In IGEL Setup, you can configure this through **Tapping mode**.
- **Palm Detection**

The toggle switch enables/disables palm detection. When enabled, it avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device. In IGEL Setup, you can configure this through **Palm detect** under **User Interface > Input > Touchpad > Advanced**.



- Scrolling (see page 116)

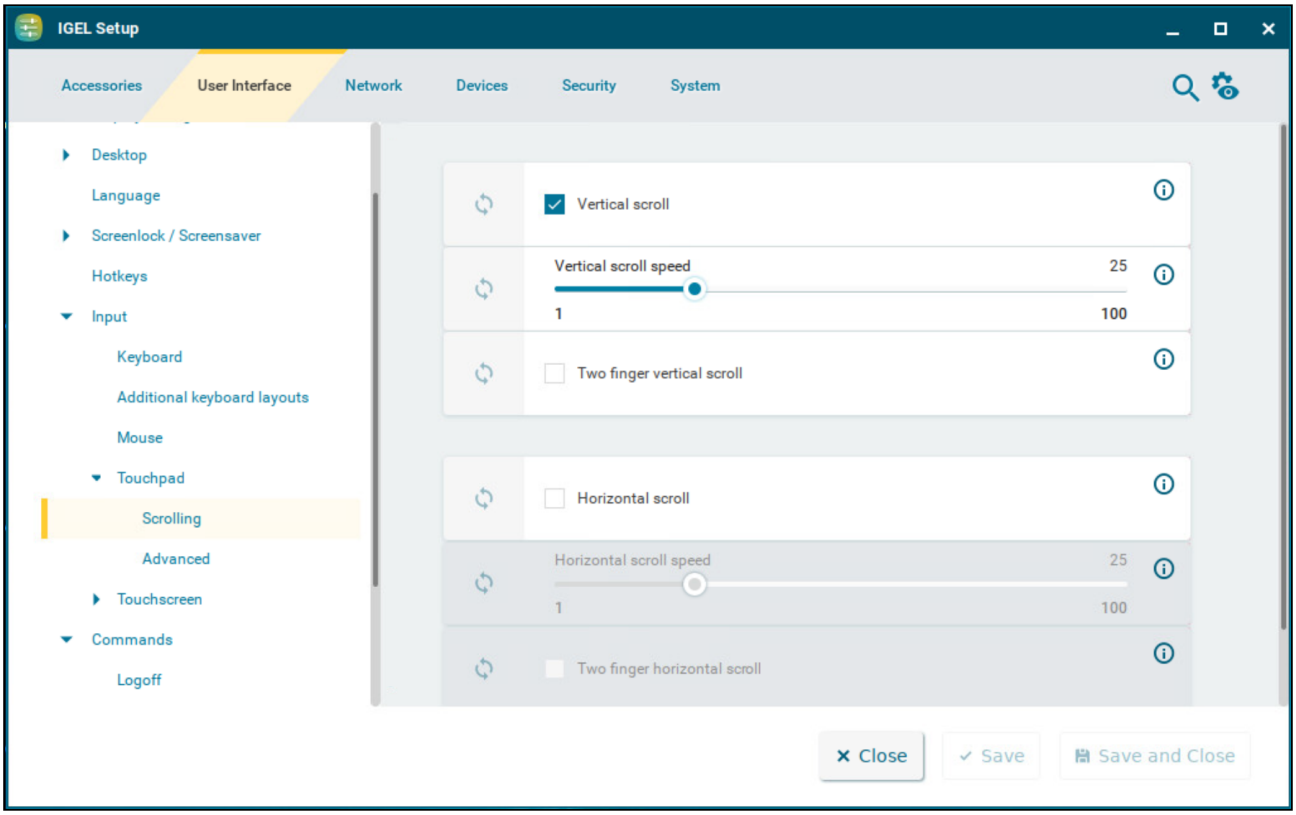
- Advanced (see page 118)

Scrolling

This article shows how to configure the scrolling with the touchpad in IGEL OS.

> In order to configure scrolling, **Custom configuration** needs to be enabled under **User Interface > Input > Touchpad**.

Menu path: **User Interface > Input > Touchpad > Scrolling**



Vertical scroll

☑ The right edge of the touchpad will be used as a vertical scrollbar. The vertical scroll speed can be set. (Default)

☐ The right edge is not enabled as a scrollbar.

Vertical scroll speed

The distance from which scrolling is recognized when moving the finger in a vertical direction. (Default: 25)

Two finger vertical scroll

☑ Two-finger scrolling is enabled for vertical scrolling.

☐ Two-finger scrolling is disabled. (Default)

Horizontal scroll

☑ The bottom edge of the touchpad will be used as a horizontal scrollbar. The horizontal scroll speed can be set.

☐ The bottom edge is not enabled as a scrollbar. (Default)

Horizontal scroll speed

The distance from which scrolling is recognized when moving the finger in a horizontal direction. (Default: 25)

Two finger horizontal scroll

☑ Two-finger scrolling is enabled for horizontal scrolling.

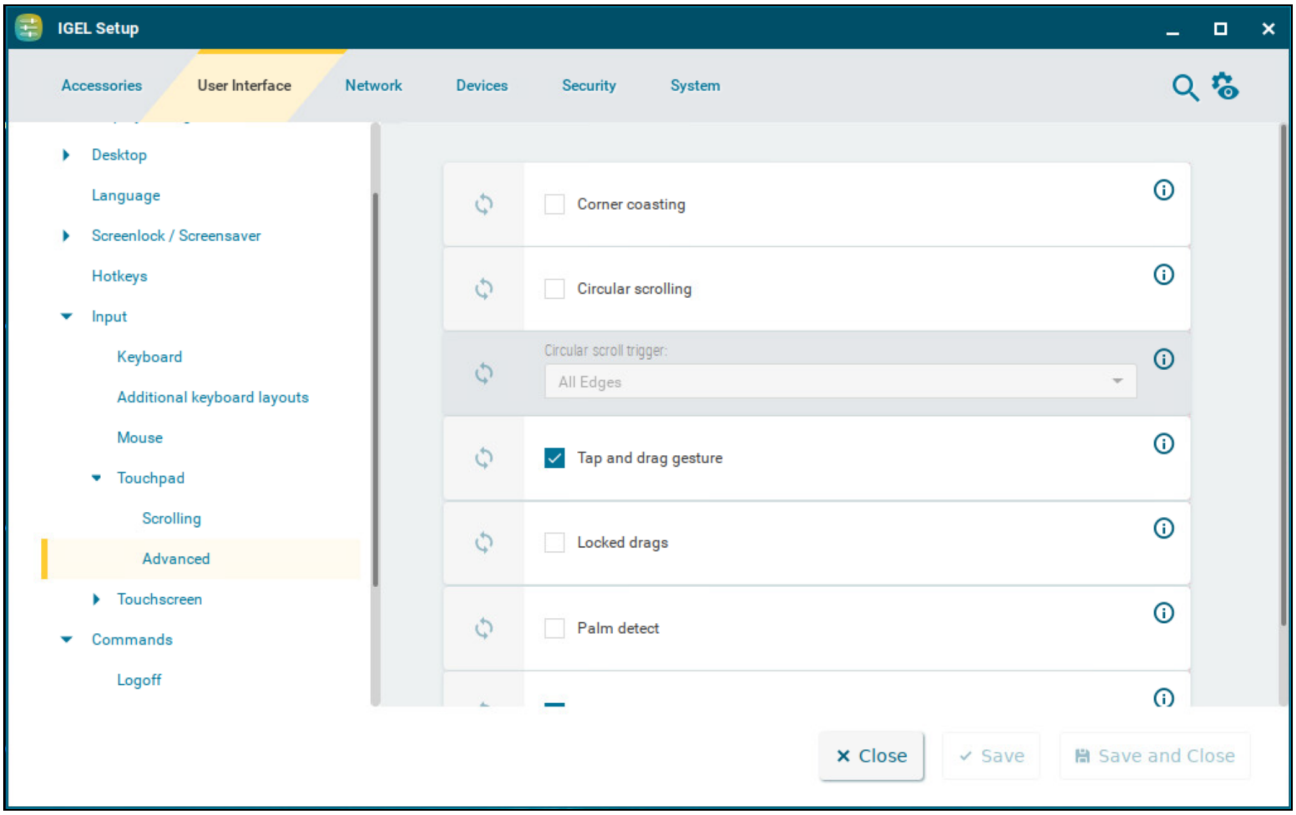
☐ Two-finger scrolling is disabled. (Default)

Advanced

This article shows how to configure advanced settings of the touchpad in IGEL OS.

> In order to configure advanced settings, **Custom configuration** needs to be enabled under **User Interface > Input > Touchpad**.

Menu path: **User Interface > Input > Touchpad > Advanced**



Corner coasting

☑ You can continue scrolling if your finger reaches the corner when scrolling vertically or horizontally along the touchpad edges. The scrolling continues while the finger stays in the corner.

☐ The scrolling stops as soon as the reaches the corner. (Default)

Circular scrolling

☑ You can scroll in a circle. In the selection menu, you can specify where to begint the circular scrolling.

☐ Circular scrolling is disabled. (Default)

Circular scroll trigger

Trigger region of the touchpad to start circular scrolling.
Possible values:

- **All edges** (Default)
- **Top edge**
- **Top right corner**
- **Right edge**
- **Bottom right corner**
- **Bottom edge**
- **Bottom left corner**
- **Left edge**
- **Top left corner**

Tap and drag gesture

☑ You can move items by tapping them and then touching again and dragging them by moving the finger on the touchpad. (Default)

Locked drags

☑ The tap and drag gesture ends only after an additional tap.

☐ The tap and drag gesture ends when you release the finger. (Default)

Palm detect

☑ Avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device.

☐ Palm detection is disabled. (Default)

ClickPad

☑ ClickPads are permitted. These are touchpads with so-called integrated soft buttons on which physical clicks are possible.

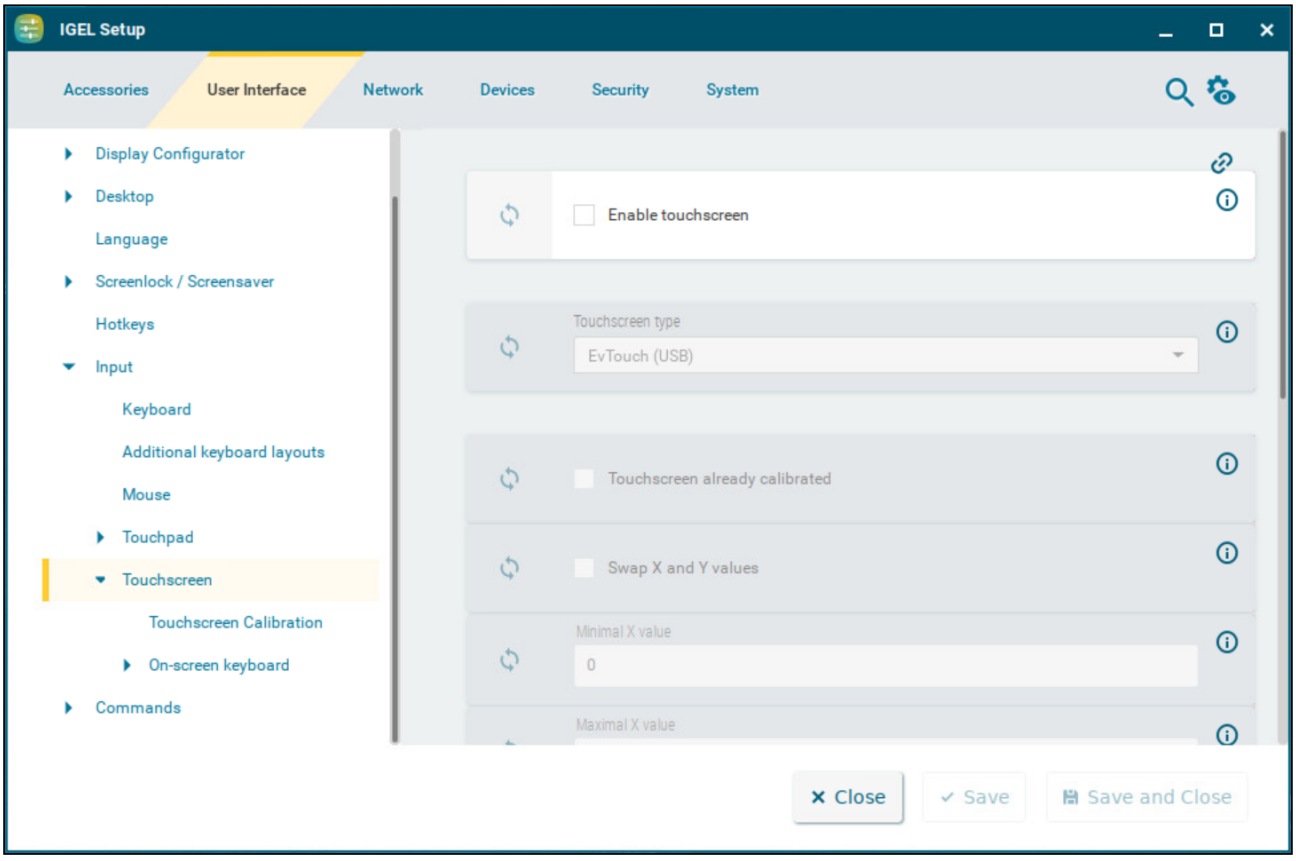
Touchscreen

This article shows how to configure the touchscreen connected to your endpoint device in IGEL OS. To ensure that you can open the setup and navigate within it, the initial configuration should take place with a mouse and keyboard connected.

For information on how to calibrate the touchscreen, see Touchscreen Calibration (see page 123).

For information on how to configure an on-screen keyboard, see On-screen Keyboard (see page 124).

Menu path: **User Interface > Input > Touchscreen**



Enable touchscreen

☑ The touchscreen is enabled.

☐ The touchscreen is disabled. (Default)

Touchscreen type

Selects the touchscreen driver which is to be used.
Possible options:

- **EvTouch (USB)** (Default)
- **eGalax**
- **Elo Multitouch (USB)**
- **Elo Singletouch (USB)**
- **TSharc**

Touchscreen already calibrated

If you enable the touchscreen function, the touchscreen must be calibrated before use.

☑ Calibration starts automatically after each system boot. (Default)

☐ Calibration does not start automatically after each system boot.

Swap X and Y values

☑ X values are interpreted as Y values and Y values as X values. Enable this option if the mouse pointer moves vertically when you move your finger in a horizontal direction. Enable if the touchscreen is used rotated by 90°.

☐ X and Y values are not swapped. (Default)

Minimal X value / Minimal Y value

These values are determined by the calibration tool. However, you can also change them manually. (Default: 0)

Maximal X value / Maximal Y value

These values are determined by the calibration tool. However, you can also change them manually. (Default: 4000)

Emulate right button

☑ A right-click is generated by touching the screen for the period of time defined under **Right button timeout**.

☐ Touching the screen for a long time does not generate a right-click. (Default)

Right button timeout

Time (in milliseconds) after which a right-click is generated. (Default: 1000)

Multimonitor

Graphic card

Graphics card assigned to the selected touchscreen. A graphics card can have more outputs than are actually used. In order to ensure transparency, you may need to assign the graphics cards manually.

If **Automatic** is set for the **Touchscreen monitor** and no configurable monitor is found for the selected graphics card, the next available monitor will be used by another graphics card.

Touchscreen monitor

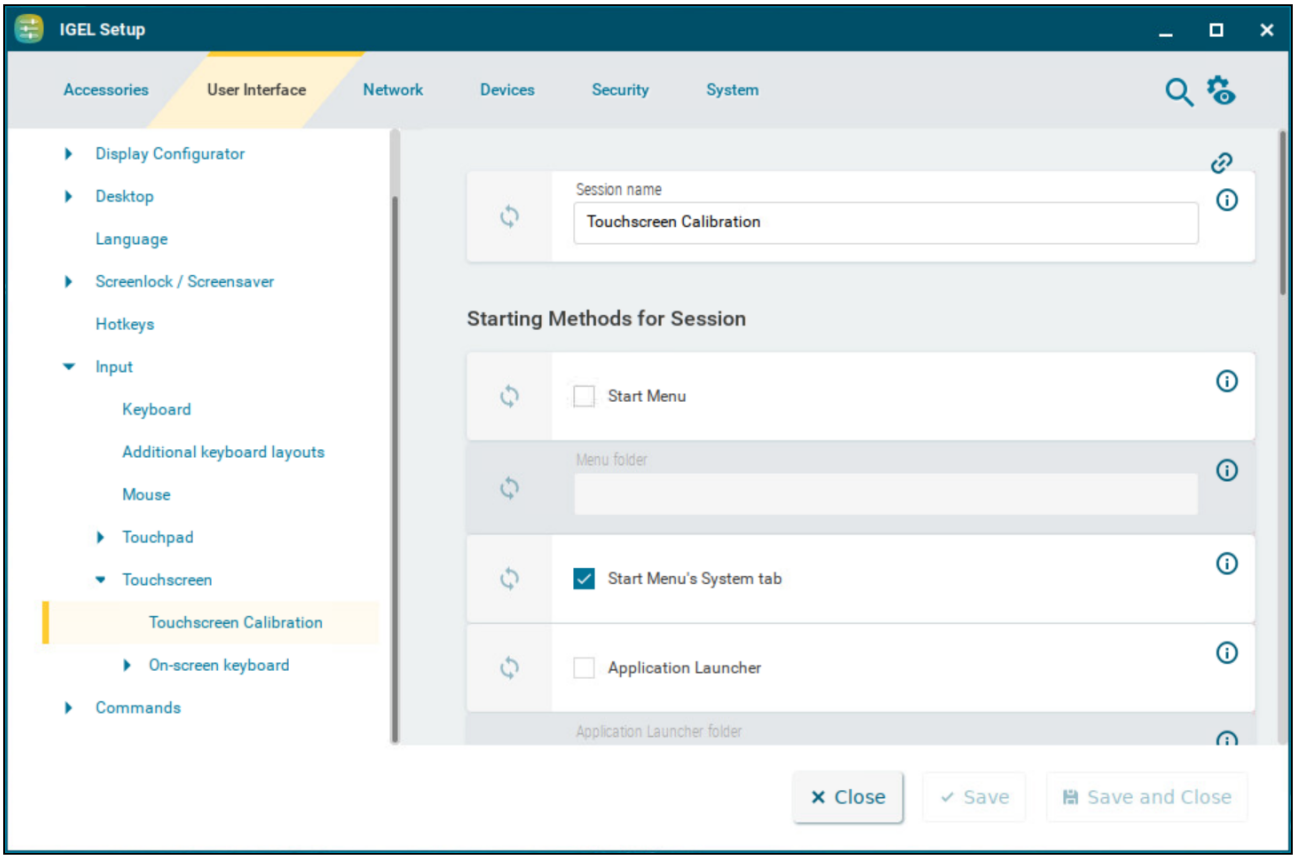
Assigns a monitor connection to the touchscreen. Example: **DisplayPort**. (Default: Automatic)

- Touchscreen Calibration (see page 123)
- On-screen Keyboard (see page 124)

Touchscreen Calibration

This article shows the starting options for the touchscreen calibration tool in IGEL OS.

Menu path: **User Interface > Input > Touchscreen > Touchscreen Calibration**

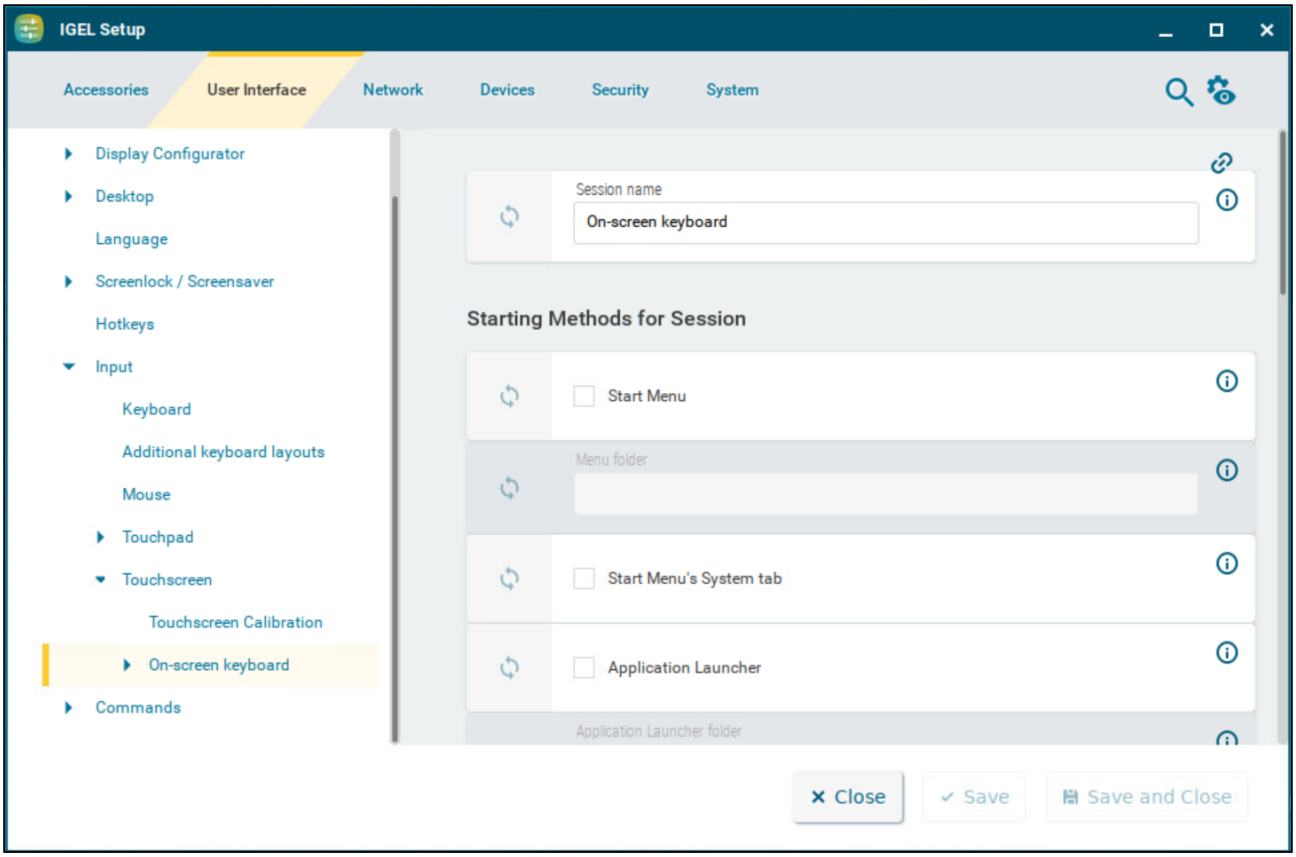


The starting methods parameters are described under Starting Methods for Apps (see page 376).

On-screen Keyboard

This article shows how to configure the starting methods for an on-screen keyboard in IGEL OS.

Menu path: **User Interface > Input > Touchscreen > On-screen keyboard**



The starting methods parameters are described under Starting Methods for Apps (see page 376).

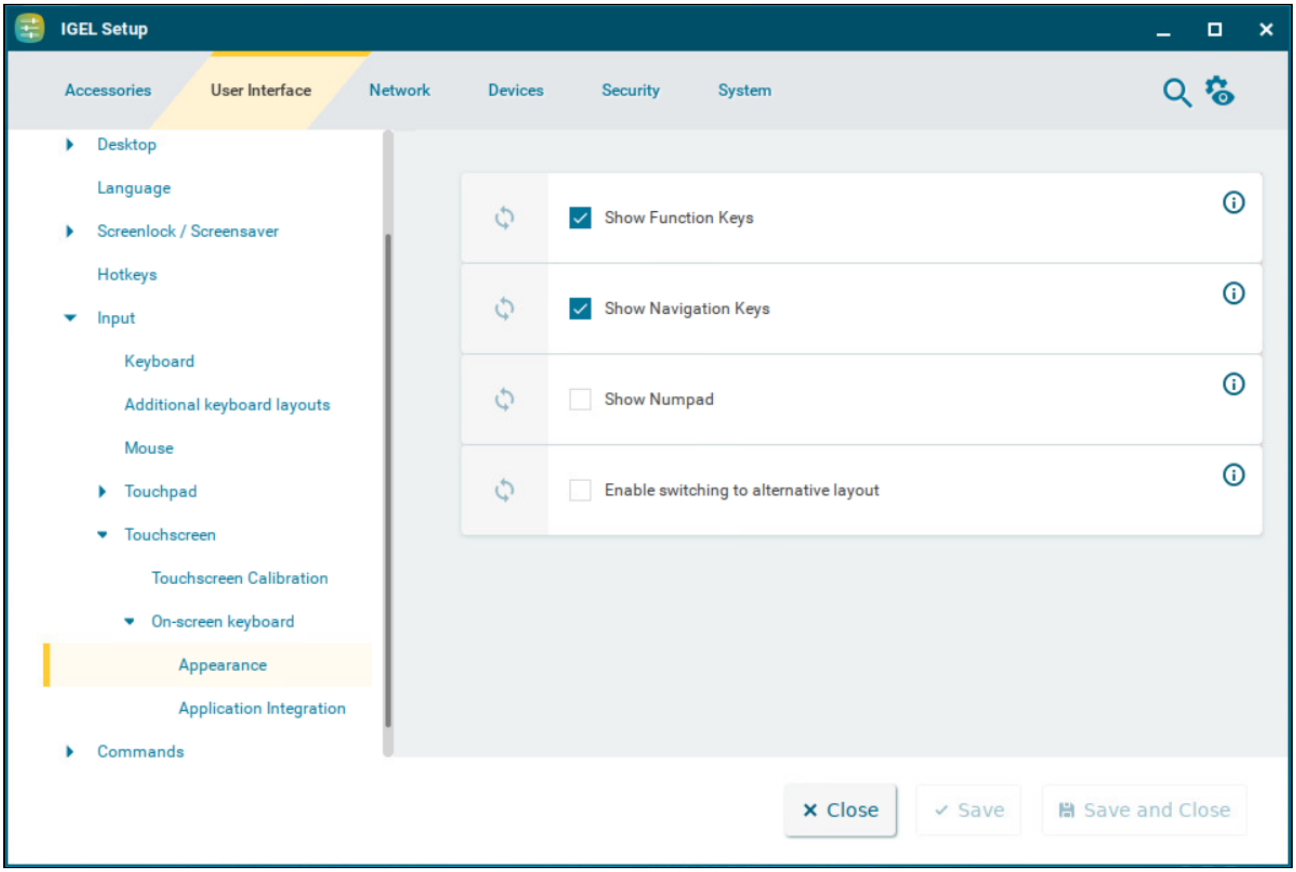
- Appearance (see page 125)
- Application Integration (see page 127)

Appearance

This article shows how to configure the appearance of the on-screen keyboard in IGEL OS.

> The layout for the normal keyboard is used for the on-screen keyboard.

Menu path: **User Interface > Input > Touchscreen > On-screen keyboard > Appearance**



Show function keys

☑ The on-screen keyboard features the function keys [F1] ... [F12]. (Default)

Show navigation keys

☑ The on-screen keyboard features the arrow keys for navigating on the screen. (Default)

Show Numpad

☑ The on-screen keyboard features the number block.

☐ The on-screen keyboard does not feature the number block. (Default)

Enable switching to alternative layout

☑ The on-screen keyboard has an additional key by which the user can toggle between the normal layout and a reduced layout. The reduced layout resembles the numpad, with the following differences:

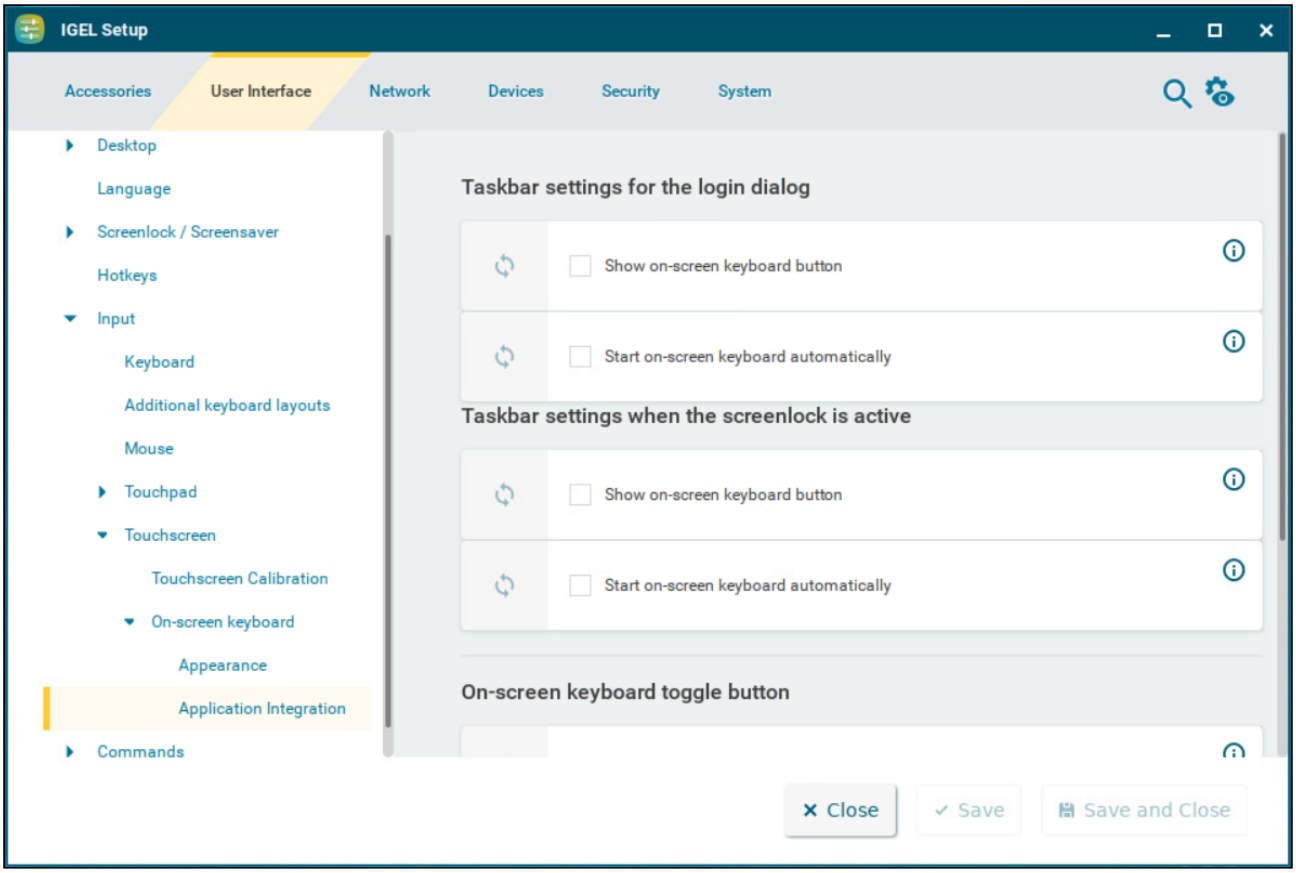
- Additional backspace key [←]
- Additional tab key [⇆]
- Additional space key [ ]
- Additional escape key [Esc]
- Return key [⏎] instead of [Enter] key

☐ Switching to the reduced layout is not possible. (Default)

Application Integration

This article shows how to configure the integration of the on-screen keyboard in IGEL OS.

Menu path: **User Interface > Input > Touchscreen > On-screen keyboard > Application Integration**



Taskbar Settings for the Login Dialog

These settings are relevant if a login is necessary in order to use the device. This applies to all logon methods that are possible with the device.

Show on-screen keyboard button

☑ A button for launching the on-screen keyboard is shown during the login dialog.

☐ The on-screen keyboard cannot be launched during the login dialog. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is shown during the login dialog and can be used for input.

☐ The on-screen keyboard is not shown during the login dialog. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

Taskbar Settings When the Screenlock Is Active

Show on-screen keyboard button

☑ A button for launching the on-screen keyboard is shown when the screen is locked.

☐ The on-screen keyboard cannot be launched when the screen is locked. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is shown when the screen is locked.

☐ The on-screen keyboard is not shown when the screen is locked. However, it can be launched via a button if **Show on-screen keyboard button** is enabled. (Default)

On-Screen Keyboard Toggle Button

Show button

☑ A button for switching the on-screen keyboard on and off is shown on the desktop.

☐ The toggle button is not shown. (Default)

Button size

The size of the toggle button. A size between 40 and 80 pixels can be chosen. (Default: 60px)

Automatically show on-screen keyboard when text field is selected

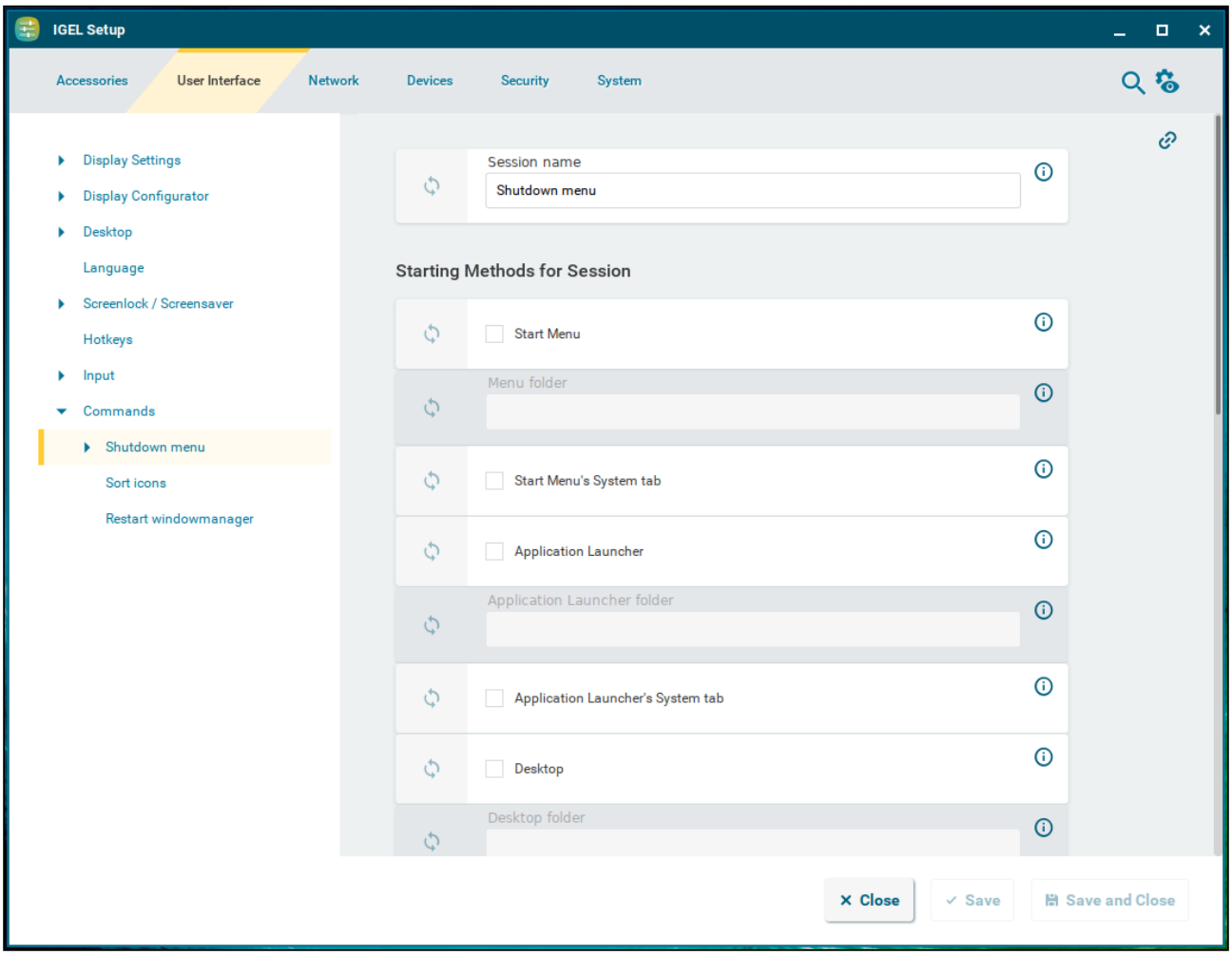
☑ The on-screen keyboard is shown automatically when an input field is selected.

☐ The on-screen keyboard is not shown automatically. (Default)

Commands

This article shows how to set up system command sessions in IGEL OS.

Menu path: **User Interface > Commands > Shutdown menu / Sort icons / Restart windowmanager**



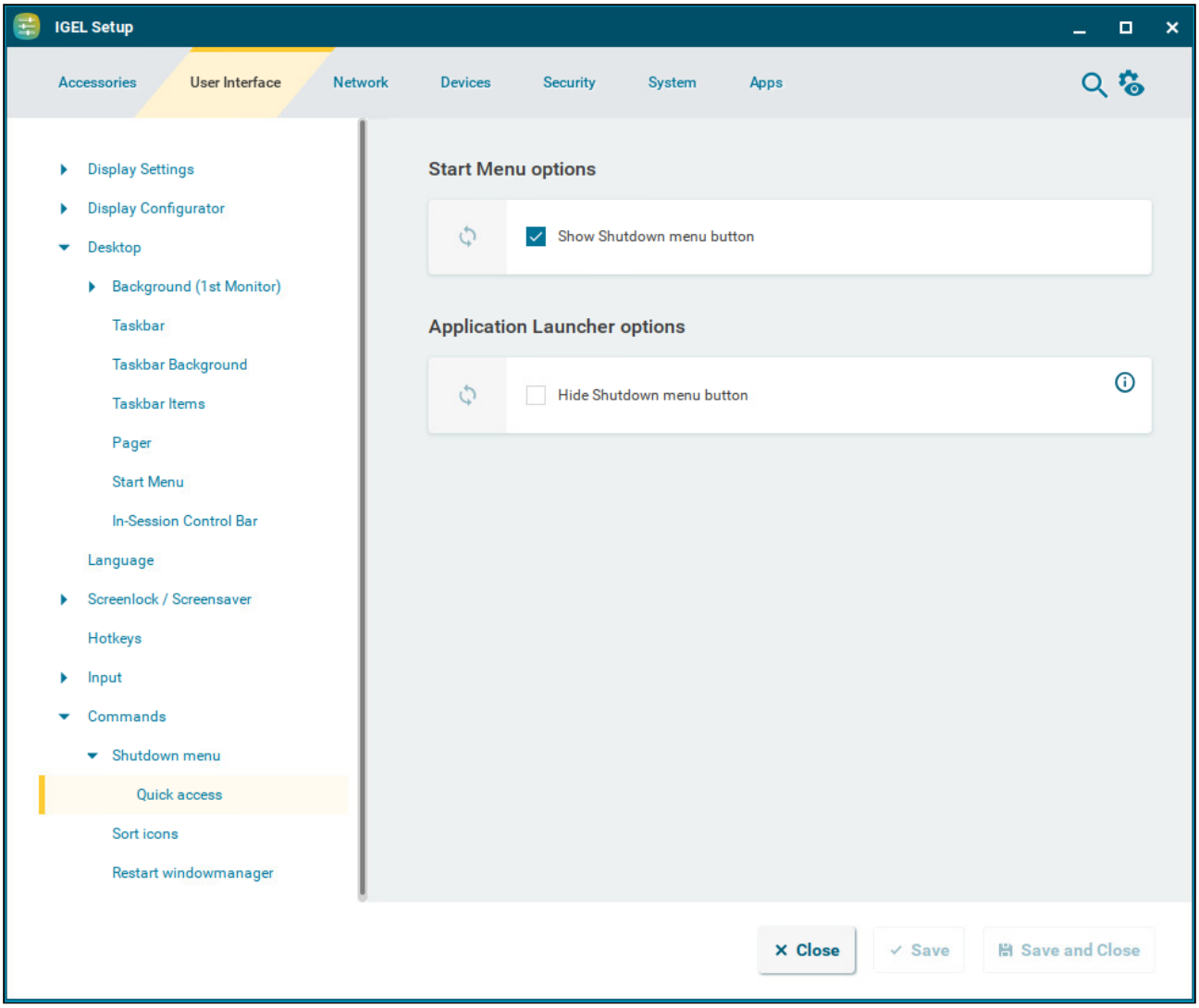
System commands can be made accessible to the user through configuring them as sessions:

- **Shutdown menu**: Opens the shutdown menu. You can configure the shutdown menu under **System > Power Options > Shutdown**. For more information, see Shutdown (see page 304).
- **Sort icons**: Sorts the symbols on the desktop so that they form a block.
- **Restart windowmanager**: Restarts the device's user interface.

The starting methods parameters are described under Starting Methods for Apps (see page 376).

Quick Access

Menu path: **User Interface > Commands > Shutdown Menu > Quick Access**



Here, you can configure the quick access to the shutdown menu from the start menu and the Application Launcher.

Show Shutdown menu button

☑ The icon is shown in the start menu. (Default)

Hide Shutdown menu button

☑ The icon is shown in the Application Launcher.

☐The icon is not shown in the Application Launcher. (Default)

Network

In this chapter, you find information on network configuration in IGEL OS.

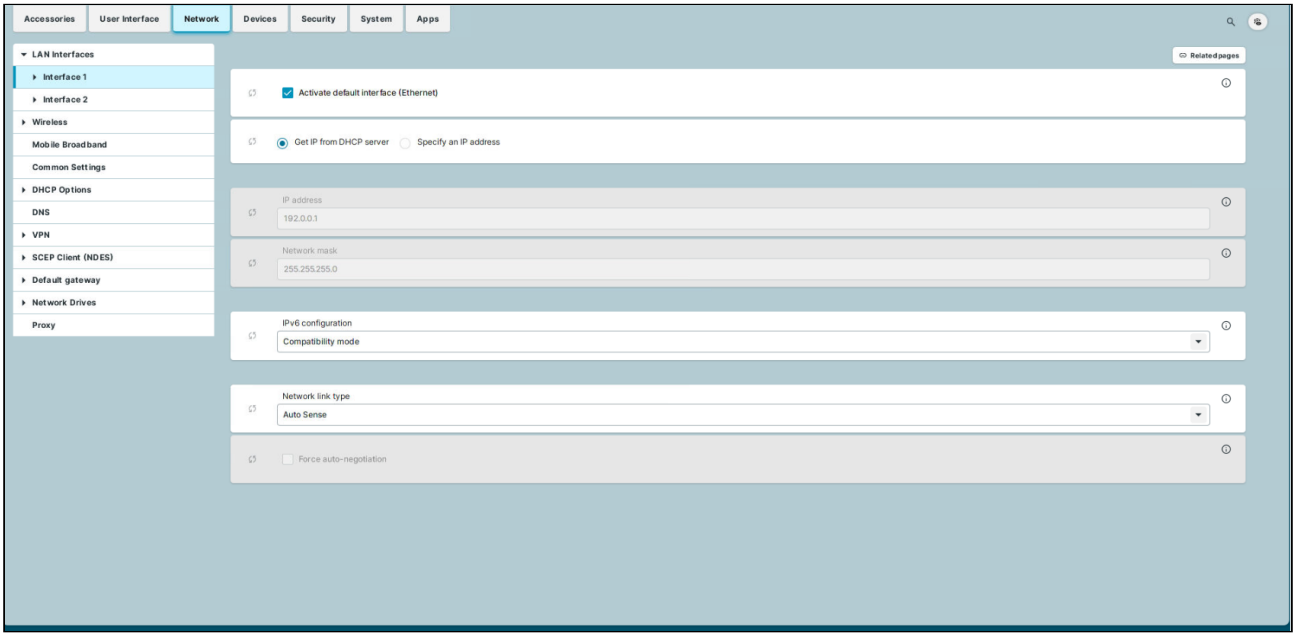
- LAN Interfaces in IGEL OS 12 (see page 133)
- Wireless (see page 142)
- Mobile Broadband in IGEL OS 12 (see page 153)
- Common Settings of the Network in IGEL OS 12 (see page 156)
- DHCP Options (see page 158)
- DNS (see page 162)
- VPN (see page 164)
- SCEP Client (NDES) (see page 186)
- Default Gateway (see page 194)
- Network Drives (see page 198)
- Proxy (see page 205)

LAN Interfaces in IGEL OS 12

This article shows how to configure LAN interfaces in IGEL OS.

> You can use the LAN tray app for quick ethernet network configurations. For details, see Tray Applications in IGEL OS 12 (see page 353).

Menu path: **Network > LAN Interfaces > [Interface]**



> **Predictable Network Interface Names (PNINs)**
> The names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[5]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.
>
> - As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.

5 https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
    - Tcpdump
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance by clicking **Add Instance**. To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate default interface (Ethernet)

☑ The interface is enabled. (Default)

☐ The interface is disabled.

Get IP from DHCP server

☑ The IP address of the client will be obtained automatically using DHCP. (Default)

DHCP options can be specified under **Network > DHCP Options > Standard Options**. For more information, see DHCP Options (see page 158).

Specify an IP address

The IP address and the network mask are entered manually.

IP address

IP address of the device

Network mask

Network mask of the device

IPv6 configuration

- **Compatibility mode**: Behavior of earlier firmware versions. (Default)

- **Disabled**: IPv6 completely disabled
- **Automatic**: IPv6 auto configuration based on router advertisements (can include DHCPv6). For further information, see RFC 4861.[6]
- **DHCPv6**: IPv6 configuration using DHCPv6 if router advertisements are not available. This is mentioned in RFC 4862 Section 5.5.2.[7]

Network link type

- **Auto sense** (Default)
- **1000 Mbps Full Duplex**
- **100 Mbps Full Duplex**
- **100 Mbps Half Duplex**
- **10 Mbps Full Duplex**
- **10 Mbps Half Duplex**

Force auto-negotiation

☑ The half-/full-duplex problems can be avoided for switches that expect the auto-negotiation flag for fixed bandwidths.

☐ Auto-negotiation is not forced. (Default)

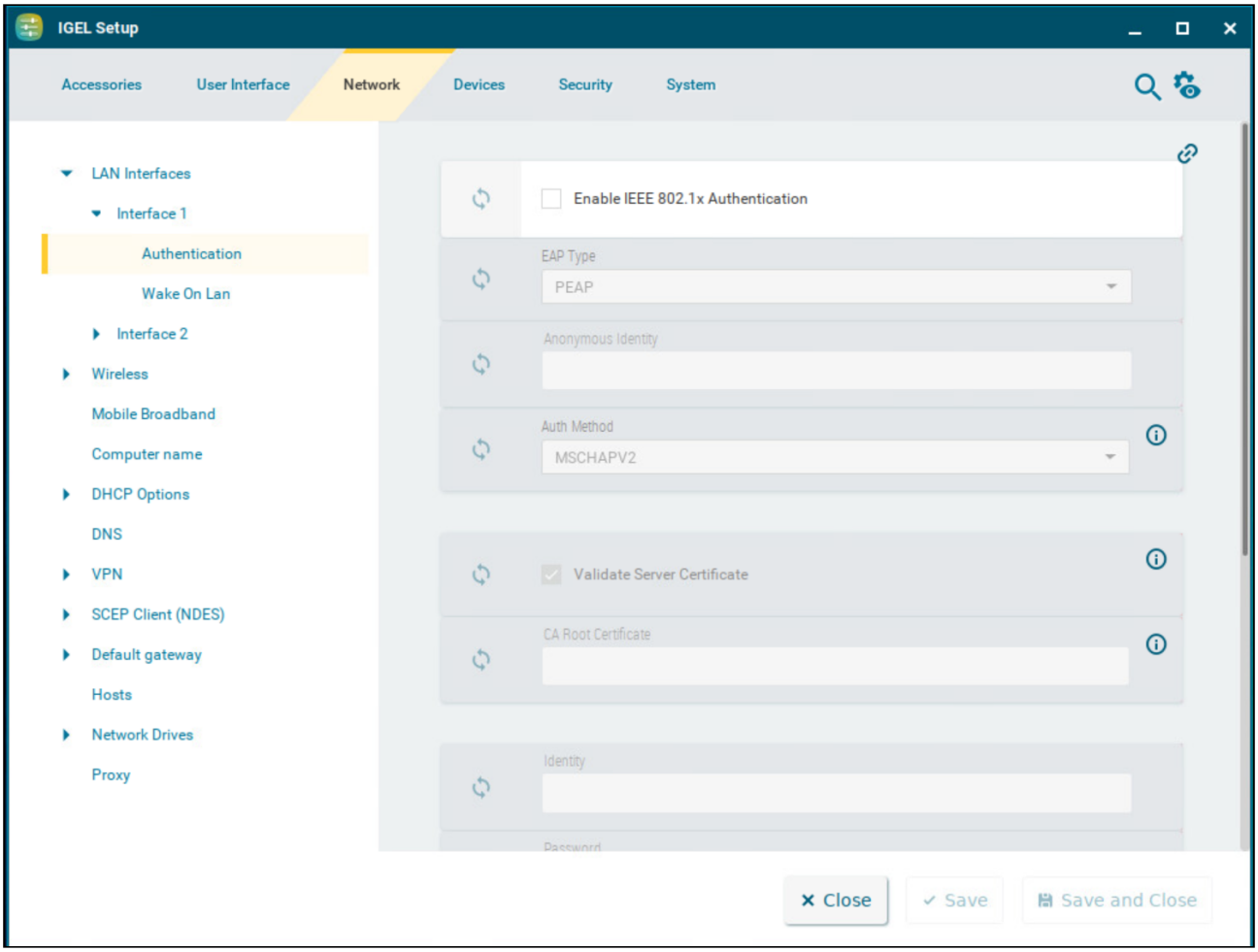
- Authentication (see page 136)
- Wake On LAN (see page 140)

6 https://tools.ietf.org/html/rfc4861
7 https://tools.ietf.org/html/rfc4862#section-5.5.2

Authentication

This article shows how to enable and configure network port authentication in IGEL OS.

Menu path: **Network > LAN Interfaces > [Interface] > Authentication**



Enable IEEE-802.1x authentication

☑ Network port authentication is enabled.

☐ Network port authentication is disabled. (Default)

If you enable authentication, further options become available:

EAP type

The type of the authentication procedure:

- **PEAP**: Protected Extensible Authentication Protocol (Default)
- **TLS**: Transport Layer Security with client certificate
- **TTLS**: Tunneled Transport Layer Security
- **FAST**: Flexible Authentication via Secure Tunneling

Anonymous identity

This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP Types**, except for **TLS**.

Auth method

The following authentication methods are available:

- **MSCHAPV2**: Microsoft Challenge Handshake Authentication Protocol (Default)
- **TLS**: Transport Layer Security with client certificate
- **GTC**: Generic Token Card
- **MD5**: MD5-Challenge
- **PAP**: Password Authentication Protocol

Validate server certificate

☑ The server's certificate is checked cryptographically. (Default)

CA root certificate

The path to the CA root certificate file. This can be in PEM or DER format.

Identity

User name for RADIUS

Password

Password for network access

> ⓘ If you leave the **Identity** and **Password** fields empty, an entry mask for authentication purposes will be shown. However, this does not apply to the methods with a client certificate (TLS and PEAP-TLS) where these details are mandatory.

The following settings are relevant if you have selected **TLS** as **EAP Type**:

Manage certificates with SCEP (NDES)

☑ Client certificates will automatically be managed with SCEP. For more information, see SCEP Client (NDES) (see page 186).

☐ Client certificates will not be managed with SCEP. (Default)

Client certificate

Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

> If a private key in the PKCS#12 (PFX) format is used, leave this field empty.

Private key

Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PKCS#12 (PFX) format. The **Private key password** may be required for access.

Identity

User name for network access

Private key password

Password for the **Private key** for the client certificate

The following setting is relevant if you have selected **FAST** as **EAP Type**:

Automatic PAC provisioning

Specifies how the PAC (Protected Access Credential) is delivered to the client.
Possible options:

- **Disabled**: PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- **Unauthenticated**: An anonymous tunnel will be used for PAC provisioning.
- **Authenticated**: An authenticated tunnel will be used for PAC provisioning.
- **Unrestricted**: Both authenticated and unauthenticated PAC provisioning is allowed. PAC files are automatically created after the first successful authentication. (Default)

> PAC files are stored in `/wfs/eap_fast_pacs/`.
> PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

In tests with `hostapd`, it has been necessary to disable TLS 1.2. To do that, enter the following command for **System > Registry > network.interfaces.ethernet.device0.ieee8021x.phase1_direct**: `tls_disable_tlsv1_2=1`
To add further device registry keys, go to **System > Registry > network.interfaces.ethernet.device%** and click **Add Instance.**

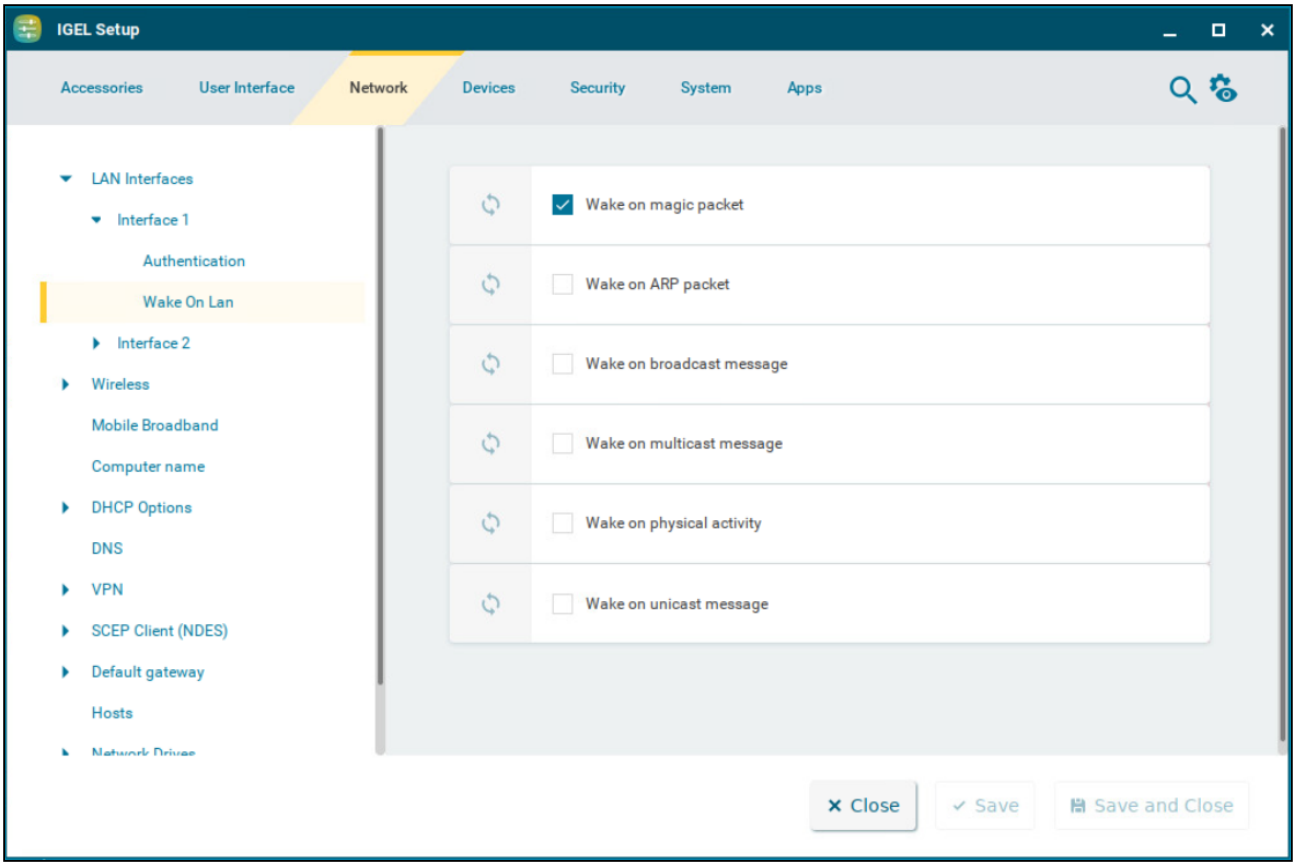
Wake On LAN

With Wake-on-Lan (WoL), you can switch on devices over the network. This article shows how to configure the packets or messages with which the endpoint device can be started in IGEL OS.

For further information on the WoL functionality of the Universal Management Suite (UMS), see Wake on LAN.

> **IGEL OS 12.3.2 or higher: WOL Setting in BIOS is Detected on Supported Lenovo Devices:**
>
> On Lenovo devices that are supported by IGEL OS 12, the system can detect whether WoL is enabled in the BIOS or not. If the system detects that WoL is disabled in the BIOS, all WoL described on this configuration page is disabled.
> You can enable or disable the WoL detection with **System > Registry > network > interfaces > respect_bios_wol_setting** (registry key `network.interfaces.respect_bios_wol_setting`).

Menu path: **Network > LAN Interfaces > [Interface] > Wake On LAN**



Wake on magic packet

☑ The device can be started with a Wake-on-LAN magic packet. (Default)

Wake on ARP packet

☑ The device can be started with a Wake on ARP packet.

☐ The device cannot be started with a Wake on ARP packet. (Default)

Wake on broadcast message

☑ The device can be started with a Wake on broadcast message.

☐ The device cannot be started with a Wake on broadcast message. (Default)

Wake on multicast message

☑ The device can be started with a Wake on multicast message.

☐ The device cannot be started with a Wake on multicast message. (Default)

Wake on physical activity

☑ The device can be started with a physical activity.

☐ The device cannot be started with a physical activity. (Default)

Wake on unicast message

☑ The device can be started with a Wake on unicast message.

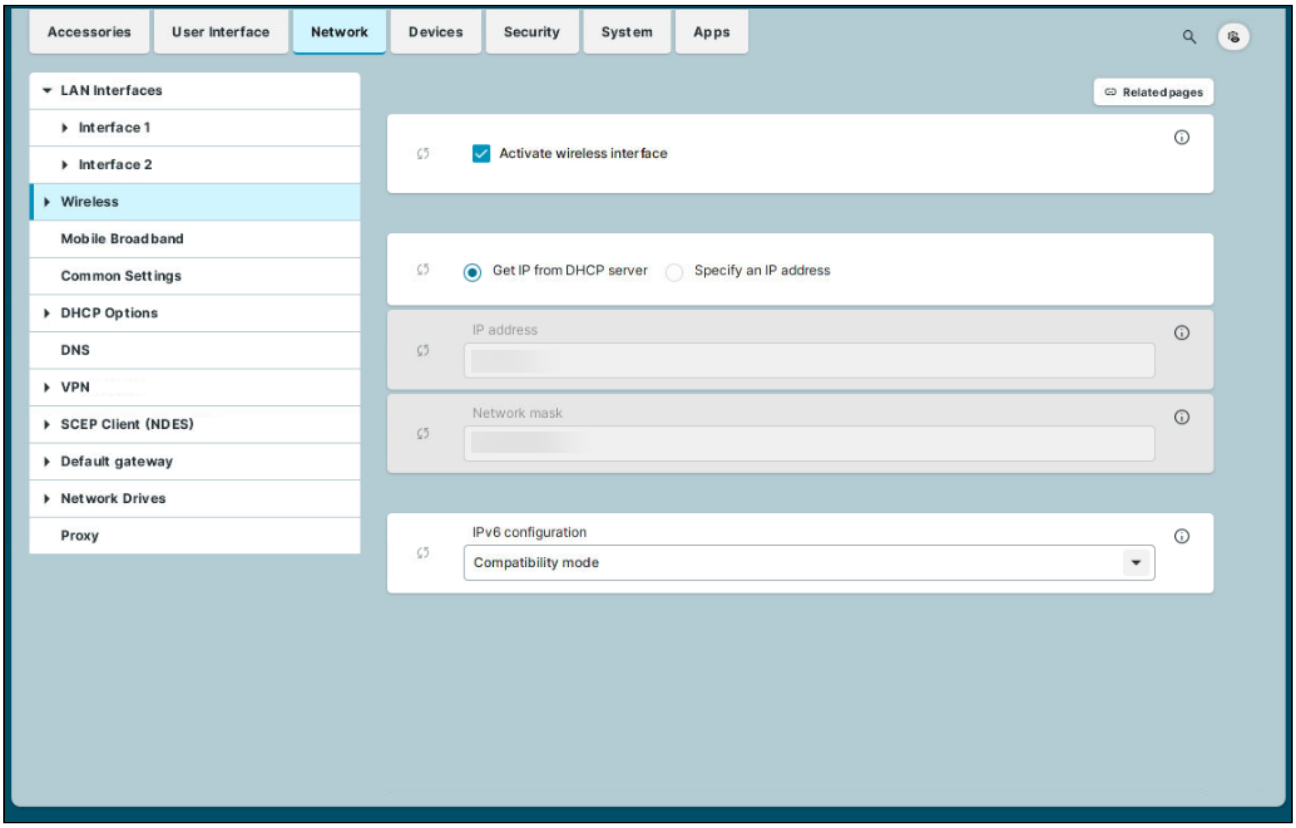
☐ The device cannot be started with a Wake on unicast message. (Default)

Wireless

This article shows how to configure wireless connections in IGEL OS.

> You can use the **Automatic switch of network connection** parameter under **Network > Common Settings** to set the behaviour of switching between LAN, Wi-Fi, and WWAN networks. For details, see Common Settings of the Network in IGEL OS 12 (see page 156).

Menu path: **Network > Wireless**



You can find details of compatible wireless hardware in the IGEL Linux 3rd Party Hardware Database[8].

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

Predictable Network Interface Names (PNINs)
The names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[9]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

- As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance by clicking **Add Instance**. To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

Activate wireless interface

☑ The wireless interface is enabled. (Default)

☐ The wireless interface is disabled.

Get IP from DHCP server

The IP address of the endpoint device will be obtained automatically using DHCP. (Default)

DHCP options can be specified under **Network > DHCP Options**. For details on the configuration, see DHCP Options (see page 158).

Specify IP address

The IP address and the network mask are entered manually.

IP address

9 https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

IP address of the endpoint device

Network mask

Network mask of the endpoint device

IPv6 configuration:

- **Compatibility mode**: Behavior of earlier firmware versions. (Default)
- **Disabled**: IPv6 is completely disabled.
- **Automatic**: IPv6 auto-configuration is based on router advertisements (can include DHCPv6). You will find further information in RFC 4861[10].
- **DHCPv6**: IPv6 configuration using DHCPv6 if router advertisements are not available. You will find further information in RFC 4862 Section 5.5.2[11].

Enable Wi-Fi automatic switch

☑ Wi-Fi is turned on automatically when a wired LAN connection is disconnected and Wi-Fi is turned off automatically when a wired LAN connection is established.

☐ Wi-Fi is not turned on automatically when a wired LAN connection is disconnected and Wi-Fi is not turned off automatically when a wired LAN connection is established. (Default)

If the toggle button in the Wi-Fi tray app is used for turning the Wi-Fi on or off, the Wi-Fi automatic switch gets disabled until the reboot of the device. On reboot, the previously configured setting will be restored. For details, see Tray Applications in IGEL OS 12 (see page 353).

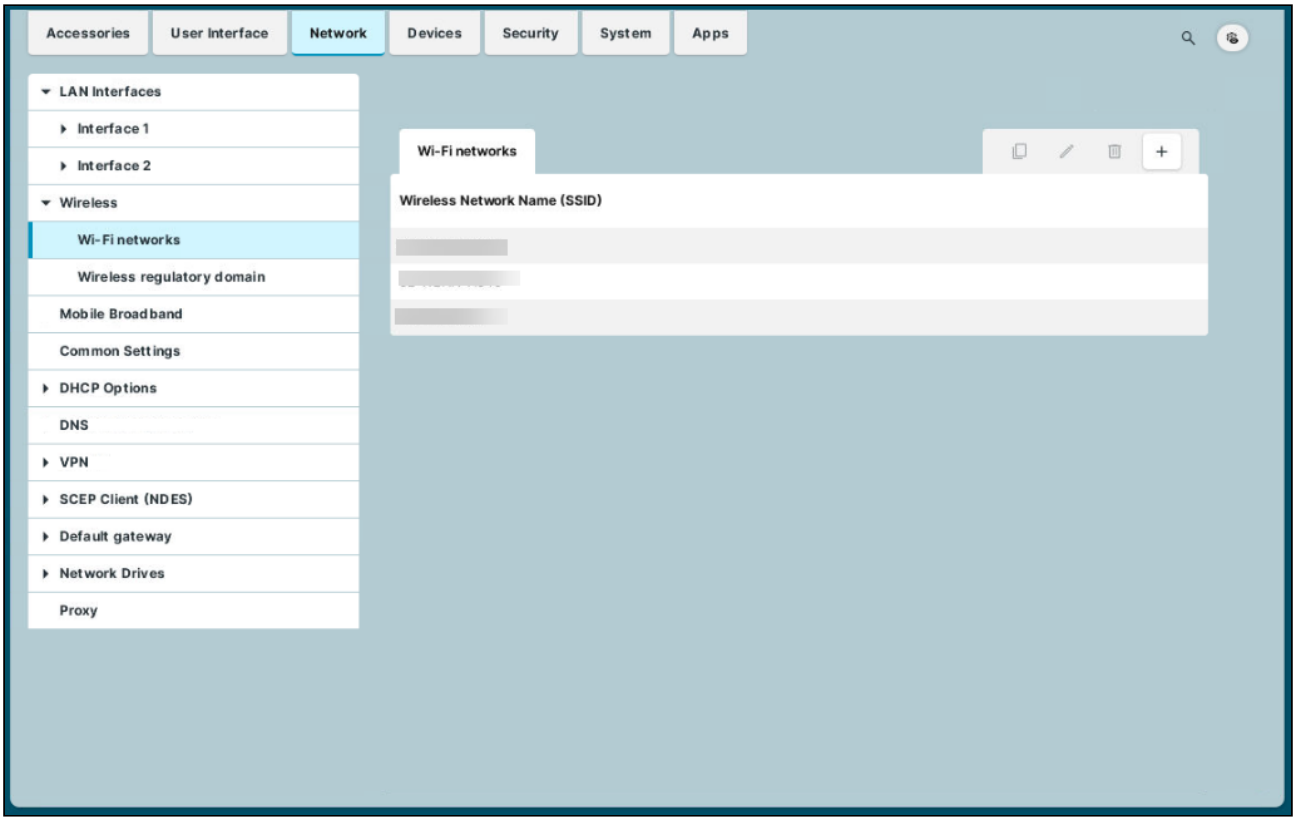
- Wi-Fi Networks (see page 145)
- Wireless Regulatory Domain (see page 151)

10 https://tools.ietf.org/html/rfc4861
11 https://tools.ietf.org/html/rfc4862#section-5.5.2

Wi-Fi Networks

This article shows how to configure wireless network connections in IGEL OS. All the wireless network connections configured for the device are shown in the list, including connections configured through the UMS or the Wi-Fi tray app. For more information on the tray app, see Tray Applications in IGEL OS 12 (see page 353).

Menu path: **Network > Wireless > Wi-Fi Networks**

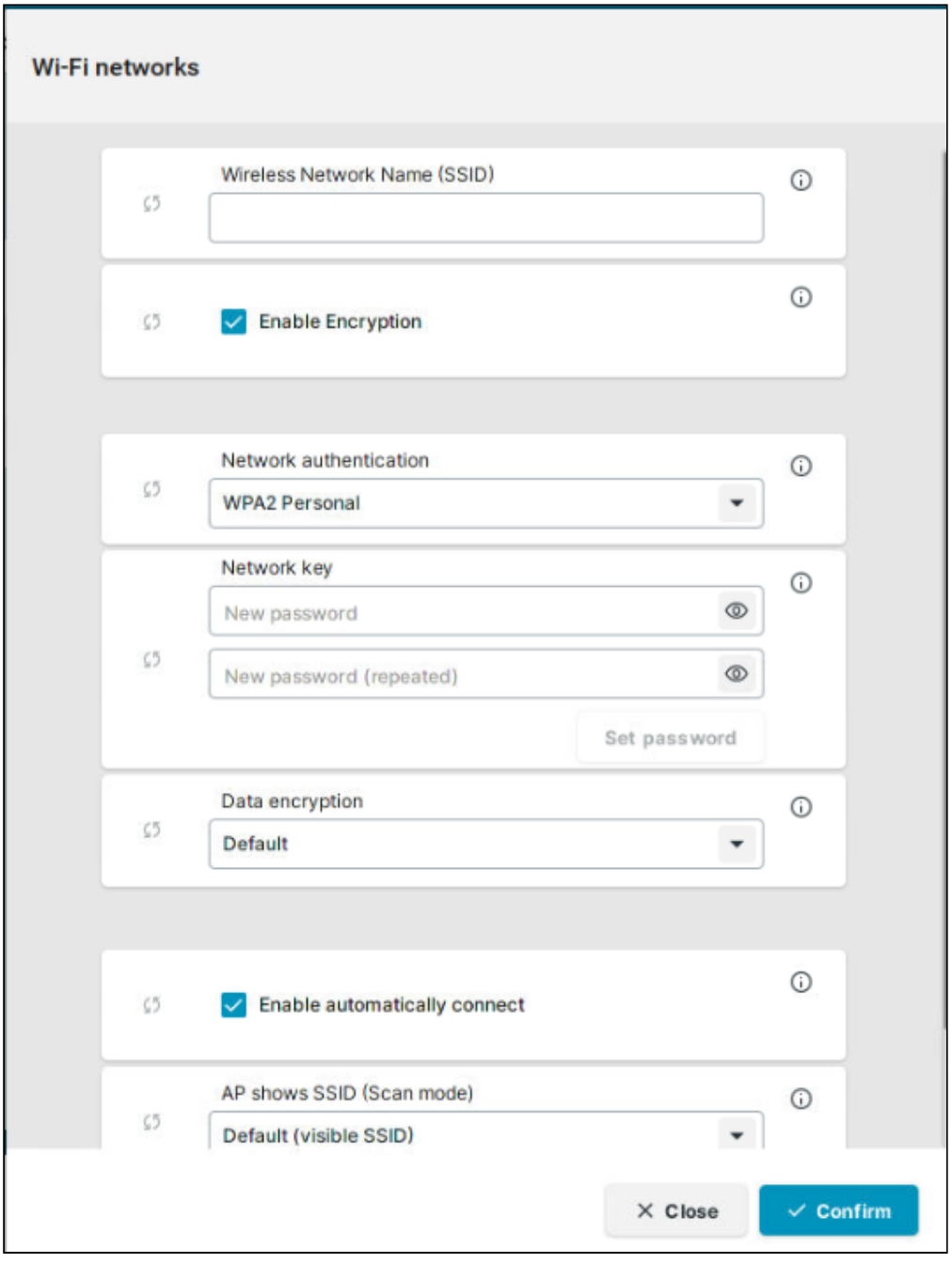


To edit the Wi-Fi networks list, proceed as follows:

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

Clicking + brings up the **Add** dialogue, where you can define the settings of the wireless network.

Wi-Fi Networks Settings



Wireless network name (SSID)

Name of the wireless network (SSID)

Enable encryption

▶ Encrypted connection is used. (Default)

Network authentication

You can configure the following network authentication methods.

- **WPA Personal**: Wi-Fi Protected Access Pre-Shared Key (WPA / IEEE 802.11i/D3.0)
- **WPA2 Personal**: Wi-Fi Protected Access Pre-Shared Key (WPA2 / IEEE 802.11i/RSN) (Default)
- **WPA3 Personal**: Wi-Fi Protected Access SAE (Simultaneous Authentication of Equals)
- **WPA Enterprise**: Wi-Fi Protected Access with 802.1X authentication (WPA / IEEE 802.11i/D3.0)
- **WPA2 Enterprise**: Wi-Fi Protected Access with 802.1X authentication (WPA2/IEEE 802.11i/RSN)

Depending on the selection, you can configure the corresponding parameters below.

- For **WPA/WPA2/WPA3 Personal** encryption, see WPA/WPA2/WPA3 Personal (see page 147).
- For **WPA/WPA2 Enterprise** encryption, see WPA/WPA2 Enterprise (see page 148).

WPA/WPA2/WPA3 Personal Encryption

Network key

WPA network key/passphrase as set at the access point. This is either an ASCII character string with a length of 8...63 or exactly 64 hexadecimal digits.

Data encryption

- **Default**: The default value depends on which network authentication method is selected. For WPA, TKIP is the default. For WPA2, AES (CCMP) is the default. (Default)
- **TKIP**: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- **AES (CCMP)**: AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- **AES (CCMP) + TKIP**: One of two encryption methods is selected by the access point.
- **Automatic**: The access point can choose the encryption method freely – nothing is stipulated.

AP scan mode

Scan mode for access points.

- **Default** (Default)
- **Broadcast**: Alternative for access points which allow the SSID broadcast
- **No broadcast**: Alternative for access points which refuse the SSID broadcast (hidden access points)

Enable automatically connect

▶ Automatic connection to the access point is enabled. (Default)

WPA/WPA2 Enterprise Encryption

Data encryption

- **Default**: The default value depends on which network authentication method is selected - TKIP for WPA, AES (CCMP) for WPA2. (Default)
- **TKIP**: Temporal Key Integrity Protocol (IEEE 802.11i/D7.0)
- **AES (CCMP)**: AES in Counter mode with CBC-MAC (RFC 3610, IEEE 802.11i/D7.0)
- **AES (CCMP) + TKIP**: One of two encryption methods is selected by the access point.
- **Automatic**: The access point can choose the encryption method freely – nothing is stipulated.

AP scan mode

Scan mode for access points

- **Default** (Default)
- **Broadcast**: Alternative for access points which allow the SSID broadcast
- **No broadcast**: Alternative for access points which refuse the SSID broadcast (hidden access points)

EAP type

- **PEAP**: Protected Extensible Authentication Protocol
- **TLS**: Transport Layer Security with client certificate
- **TTLS**: Tunneled Transport Layer Security
- **FAST**: Flexible Authentication via Secure Tunneling

Anonymous identity

This identity is sent by authentication instead of the actual **Identity**. This prevents the disclosure of the actual identity of the user. The anonymous identity is relevant for any of the above-mentioned **EAP Types**, except for **TLS**.

Auth method

Method for authentication that is available for the selected EAP type.
Possible options:

- **MSCHAPv2**: Microsoft Challenge Handshake Authentication Protocol (Default)
- **TLS**: Transport Layer Security with client certificate
- **GTC**: Generic Token Card
- **MD5**: MD5-Challenge
- **PAP**: Password Authentication Protocol

Validate server certificate

☑ The endpoint device validates the authenticity of the authentication server against the certificate file. This certificate file is stored under the path defined by **CA root certificate**.

☐ The authenticity of the authentication server is not validated.

CA root certificate

Path and file name of the file that contains the certificates with which the authentication server authenticates itself.

Identity

User name that is stored at the authentication server

Password

Password relevant to the user name

The following settings are relevant if you have selected **TLS** as **EAP type**:

Manage certificates with SCEP (NDES)

☑ Client certificates will automatically be managed with SCEP. For more information on SCEP configuration, see SCEP Client (NDES) (see page 186).

☐ Client certificates will not be managed with SCEP. (Default)

Client certificate

Path to the file with the certificate for client authentication in the PEM (base64) or DER format.

> ⓘ If a private key in the PKCS#12 (PFX) format is used, leave this field empty.

Private key

Path to the file with the private key for the client certificate. The file can be in the PEM (base64), DER, or PKCS#12 (PFX) format. The **Private key password** may be required for access.

Identity

User name for network access

Private key password

Password for the **Private key** for the client certificate

The following setting is relevant if you have selected **FAST** as **EAP type**:

Automatic PAC provisioning

Specifies how the PAC (Protected Access Credential) is delivered to the client.

Possible options:

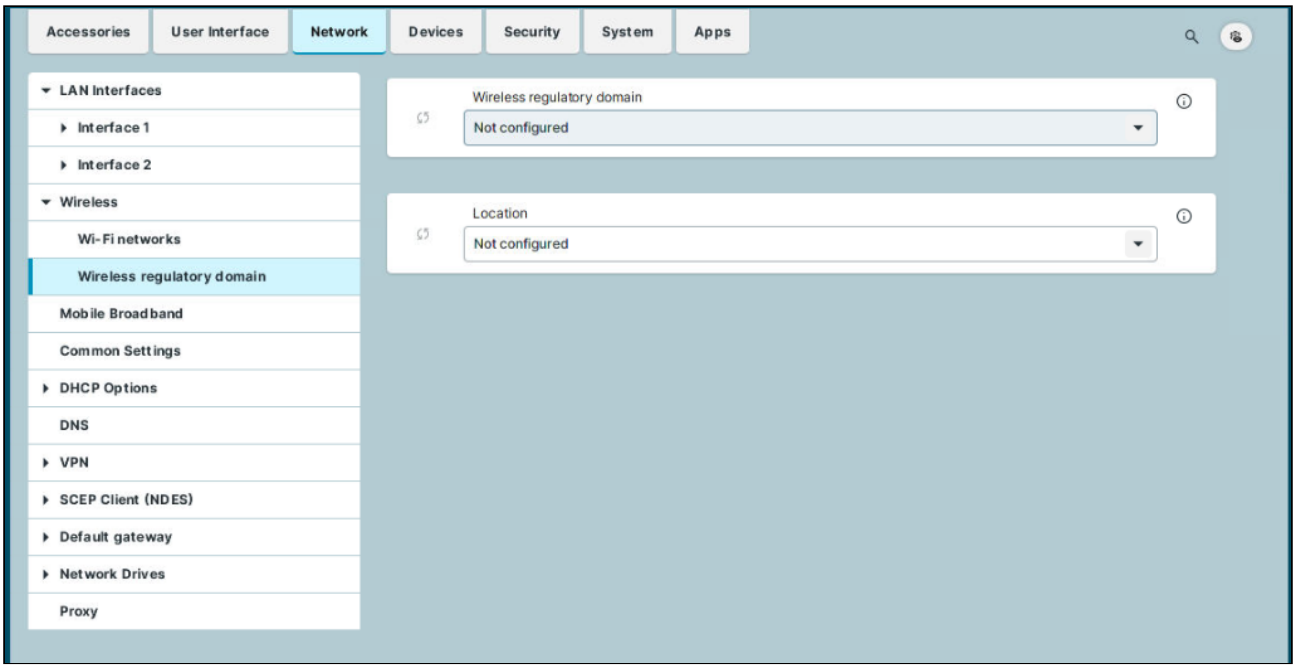
- **Disabled**: PAC files have to be transferred to the device manually, e.g. via UMS file transfer.
- **Unauthenticated**: An anonymous tunnel will be used for PAC provisioning.
- **Authenticated**: An authenticated tunnel will be used for PAC provisioning.
- **Unrestricted**: Both authenticated and unauthenticated PAC provisioning is allowed. PAC files are automatically created after the first successful authentication. (Default)

PAC files are stored in `/wfs/eap_fast_pacs/`.
PAC file names are automatically derived from the **Identity**, but are coded. In the case of the manual PAC provisioning, you can determine the PAC file names with the following script: `/bin/gen_pac_filename.sh`

Wireless Regulatory Domain

This article shows how to set the location of the device in IGEL OS.

Menu path: **Network > Wireless > Wireless Regulatory Domain**



Wireless regulatory domain

Select the area in which the device is located.

- **Not configured** (Default)
- **Africa**
- **Arctic**
- **Asia**
- **Australia**
- **Europe**
- **North America**
- **South America**
- **World**

Location

Select the country in which the device is located. The available options are based on the selected area.

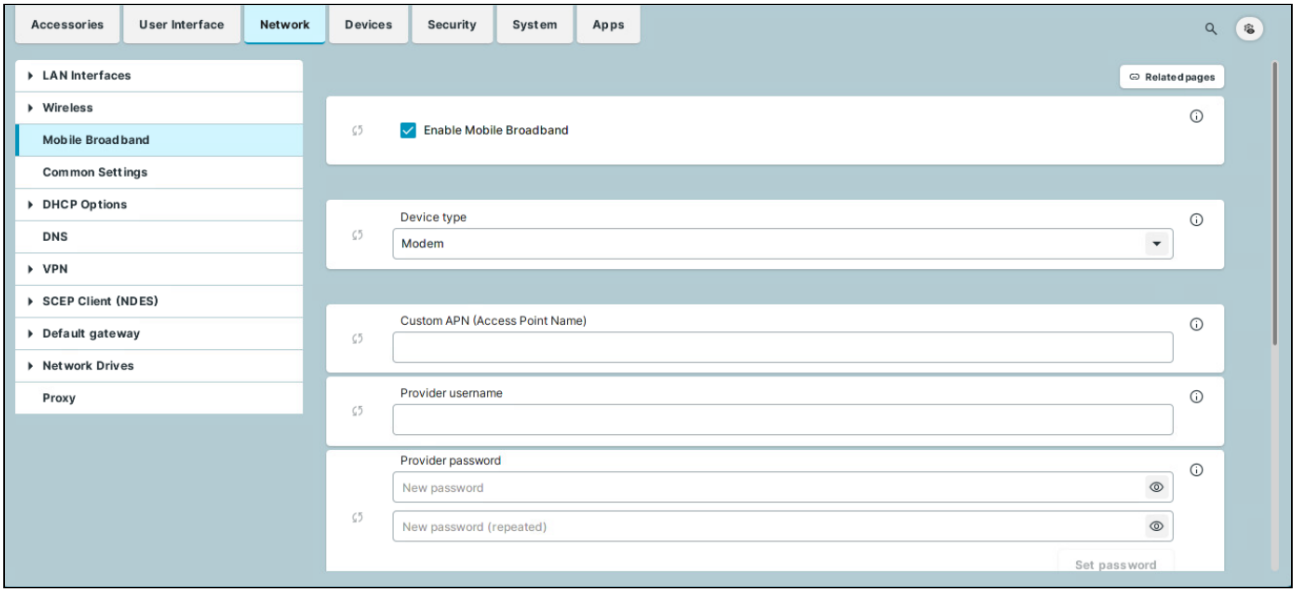
- **Not configured** (Default)
- **World**
- **Albania**
- **Armenia**
  [...]
- **Cyprus**

Mobile Broadband in IGEL OS 12

This article shows how to configure a modem or a surf stick in IGEL OS 12.

> You can also use the Mobile Broadband Tray App for quick configurations. For details, see Tray Applications in IGEL OS 12 (see page 353).

Menu path: **Network > Mobile Broadband**



> Ensure that data traffic is adequately secured. You can do this in the following ways:
> - Use a private APN.
> - Use OpenVPN and block traffic that would circumvent VPN with firewall rules.

If the surf stick is inserted and has been configured, the network connection will be established after the endpoint device boots. It can take between a few seconds and around 1 minute to establish a connection. The network connection will remain in place until the surf stick is removed or the endpoint device is put on standby or shut down.

The status of the network connection is shown in the system tray:

- The network connection is established; the endpoint device is online. This symbol is shown if **Modem** is selected as the device type:

If **Router** is selected as the device type, the corresponding symbol for a LAN connection is shown: .

- The network connection was interrupted; the endpoint device is offline. This symbol is shown if **Modem** is selected as the device type:

If **Router** is selected as the device type, the corresponding symbol for a LAN connection is shown: .

You can change the following settings:

Enable Mobile Broadband

☑ The mobile broadband network can be used if a supported modem is connected. (Default)

☐ The mobile broadband network cannot be used.

Device type

The type of the connected device.
Possible options:

- **Modem**: The device will be operated as a modem. The access data can be changed with the parameters **number**, **user name**, **password**, **APN**, **network ID** and **PIN**. (Default)
- **Router**: The device will be operated as a router. The device must be configured in advance in such a way that it is ready for use when it is inserted.

ⓘ Select the **Router** device type if you use a device from Huawei in the HiLink mode; example: Huawei E3372.

When Modem is Selected as Device Type

Custom APN (Access Point Name)

APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.

Provider username

User name for your network connection. If you do not know the user name, ask your mobile communications operator for it.

Provider password

Password for your network connection. If you do not know the password, ask your mobile communications operator for it.

Enable automatically connect

☑ The mobile internet connection is established automatically. (Default)

Allow changing the SIM-PIN in the tray application

☑ The PIN of the SIM-card can be changed in the tray application. (Default)

Allow changing the request for the SIM-PIN after boot inside the tray application

☑ The request for the PIN after booting can be enabled/disabled in the tray application. (Default)

Roaming

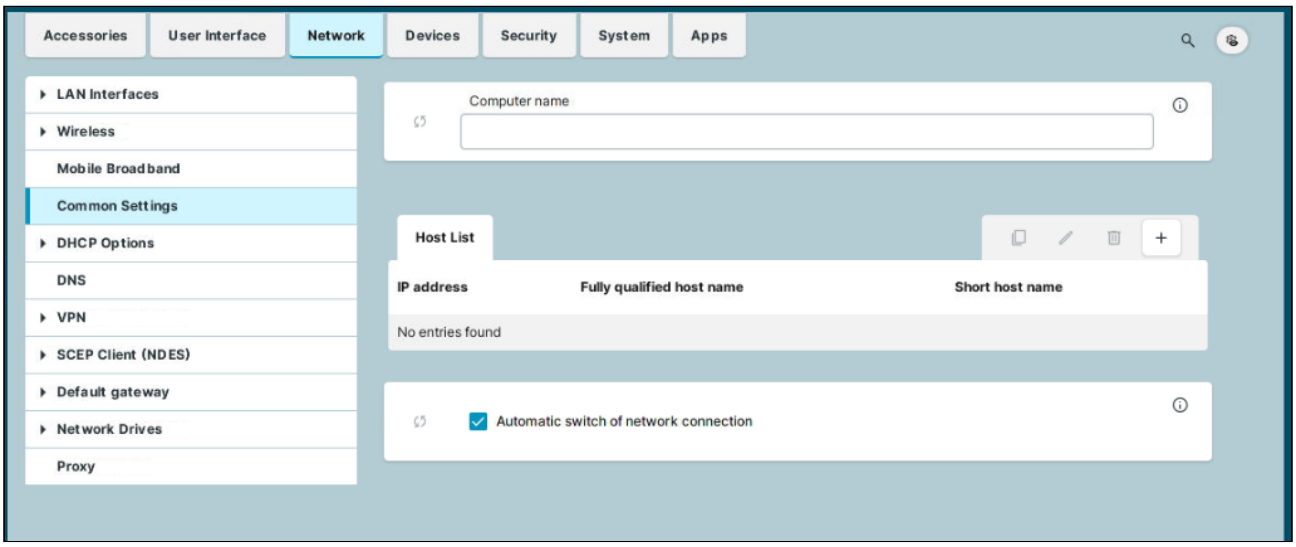
☑ The WWAN modem is allowed to connect to roaming networks. (Default)

☐ The WWAN modem can only connect to home networks.

Common Settings of the Network in IGEL OS 12

This article shows how to configure common network settings in IGEL OS 12.

Menu path: **Network > Common Settings**



Computer name

Local name of the device. If the field is empty, the default name is used. The default name is combined of '`ITC`' and the MAC address of the device.

For more information on naming configuration in Endpoint Management (UMS), see Renaming IGEL OS Devices.

Host List

List of configured hosts. If no Domain Name Service (DNS) is used, you can specify a list with computers in order to allow translation between the fully qualified host name, the short host name and the IP address.

To manage the list of computers, proceed as follows:

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

Clicking brings up the **Add** dialogue, where you can define the following settings:

- **IP address**
  IP address of the host you would like to add.
- **Fully qualified host name**
  Host name along with the domain, e.g. `mail.example.com`
- **Short host name**
  E.g. `mail`

Automatic switch of network connection

☑ The network connections (LAN, Wi-Fi, WWAN) are turned on and off automatically based on availability. (Default)

The automation is based on the following order of priorities:

1. LAN
2. Wi-Fi
3. Mobile broadband

Actions of the automation:

1. When a LAN connection is available, Wi-Fi and mobile broadband connections get disabled. The toggles in the the mobile broadband tray App and Wi-Fi tray app get disabled, so you cannot overwrite the setting there.
2. When a LAN connection is not available, the Wi-Fi connection is enabled automatically, and mobile broadband remains disabled. You can use the toggle in the Wi-Fi tray app to enable/disable Wi-Fi. When the network type is disabled through the toggle, the setting is saved persistently over boot.
3. When there are no available LAN and Wi-Fi connections, mobile broadband gets enabled. You can use the toggle in the mobile broadband tray app to enable/disable Wi-Fi. When the network type is disabled through the toggle, the setting is saved persistently over boot.

For more on network tray apps, see Tray Applications in IGEL OS 12 (see page 353).

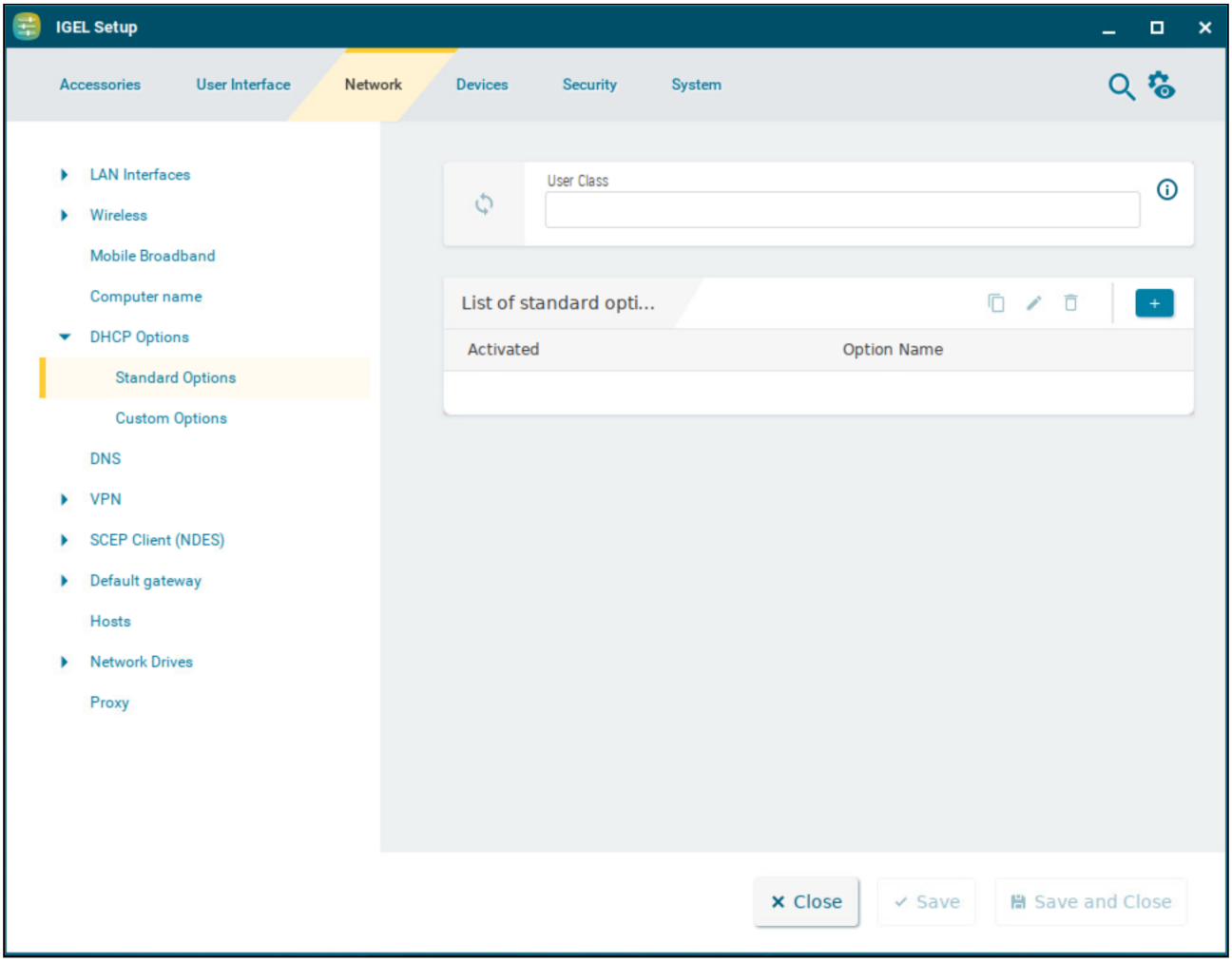
☐ The network connections are not turned on and off automatically. The toggles can be used in the mobile broadband tray app and Wi-Fi tray app to manage connections.

DHCP Options

This article shows how to configure standard and custom DHCP options with which the client can request information from the DHCP server in IGEL OS.

Standard Options

Menu path: **Network > DHCP Options > Standard Options**



User class

A freely definable character string which can serve as a criterion for allocating specific settings for the DHCP server.

List of standard options

Options with which the client can request information from the DHCP server.

You will find information regarding the various DHCP options in RFC 2132 DHCP Options and BOOTP Vendor Extensions[12].

To manage the list of options, 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 **Add** dialogue, where you can define the following settings:

Activated

☑ The option is enabled. (Default)

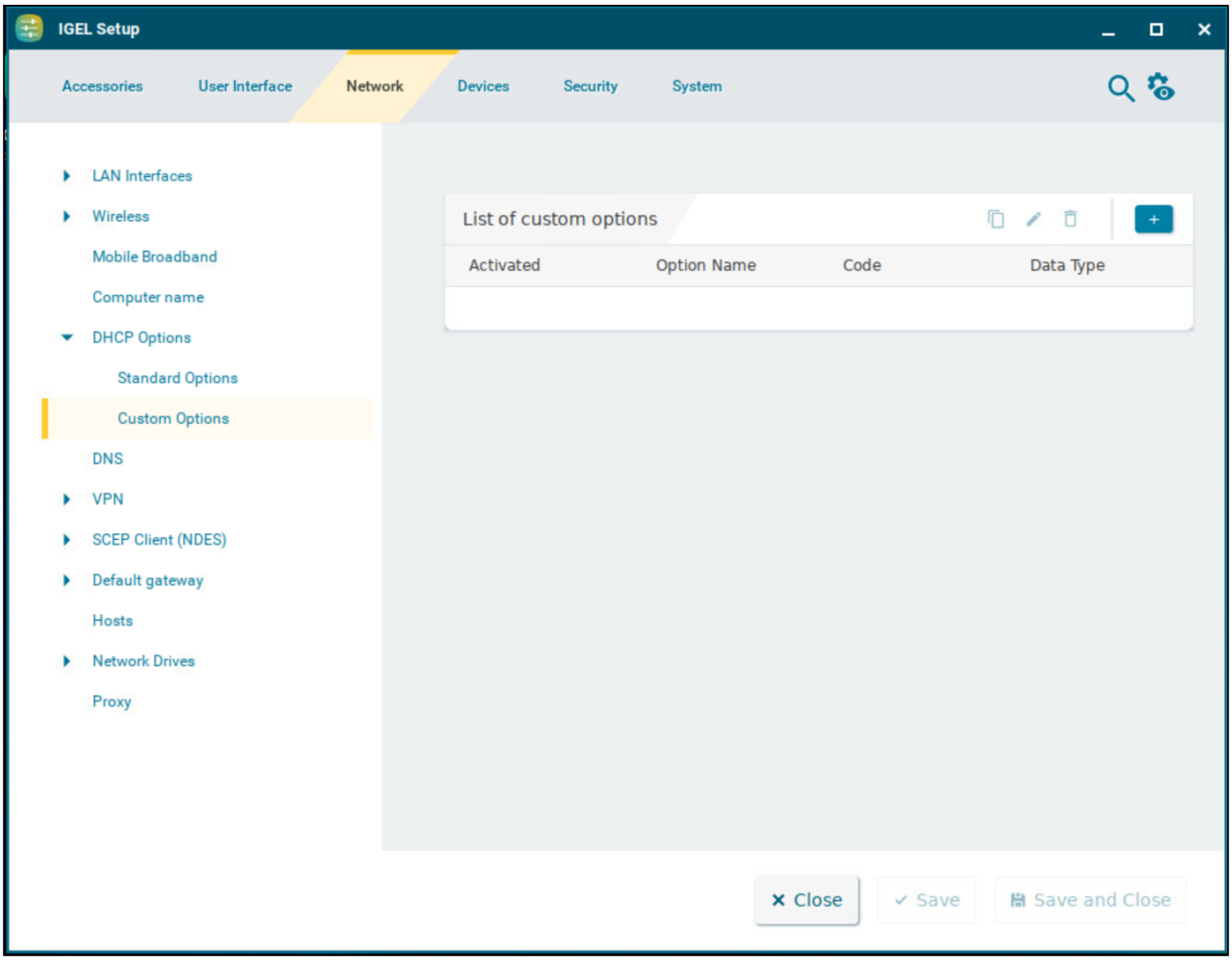
Option name

The name of the option. Select from the list of predefined names.

Custom Options

Menu path: **Network > DHCP Options > Custom Options**

12 https://tools.ietf.org/html/rfc2132



For more information regarding these options, see the manual for your DHCP server or your network components.

To manage the list of options, 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 **Add** dialogue, where you can define the following settings:

Activated

☑ The option is enabled. (Default)

Option name

The name of the option. Add a prefix of your own in order to prevent a conflict with the default DHCP options. Example of the syntax: `[YourPrefix]-[OptionName]`. English letters, numbers and the special character "-" are allowed.

Code

A number that is used by the DHCP server and DHCP client to reference an option. A number between 80 and 254 can be chosen. (Default: 80)

Data type

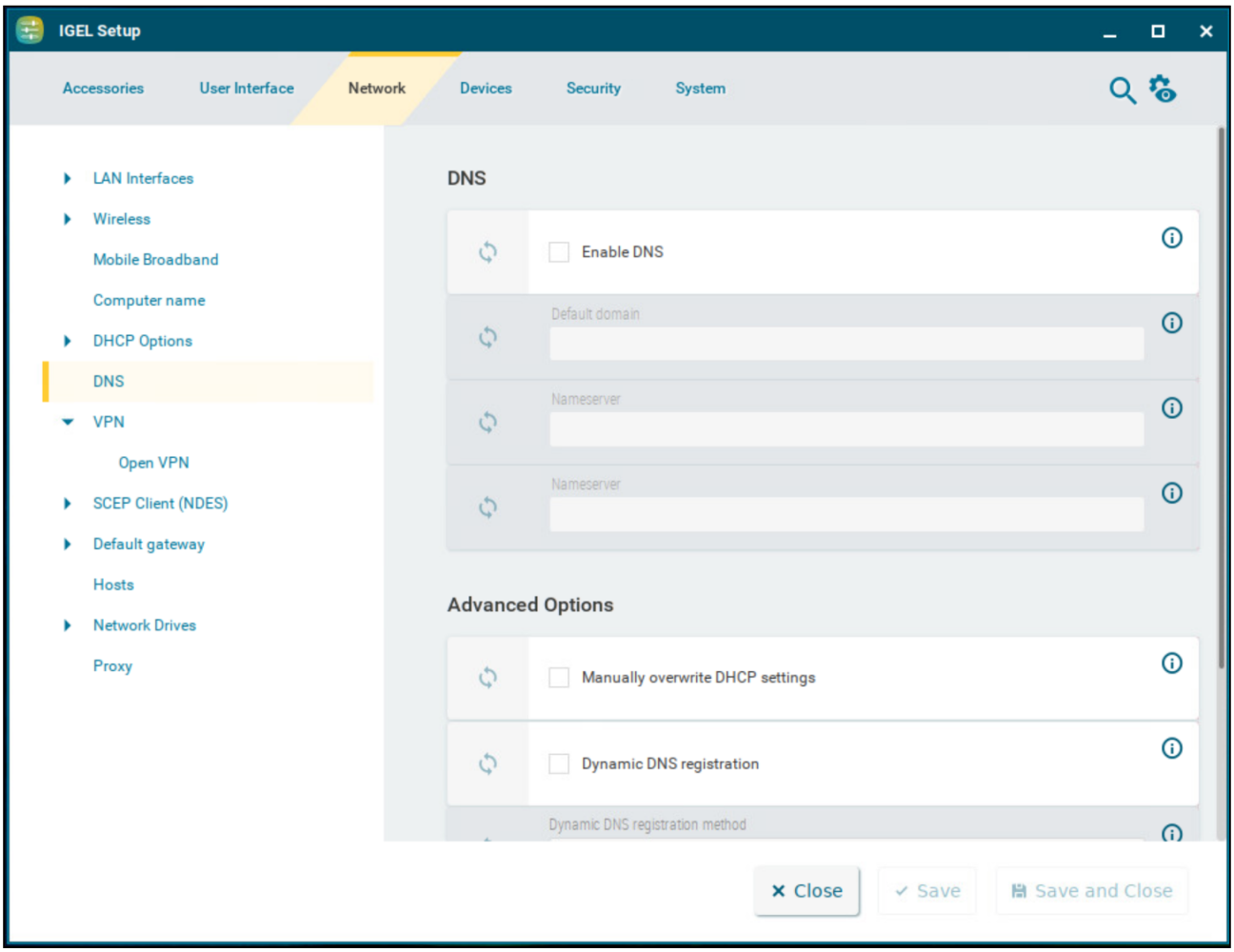
Type of option.
Possible values:

- **Boolean**
- **Integer 8**
- **Integer 16**
- **Integer 32**
- **Signed integer 8**
- **Signed integer 16**
- **Signed integer 32**
- **Unsigned integer 8**
- **Unsigned integer 16**
- **Unsigned integer 32**
- **IP address**
- **Text** (Default)
- **String**

DNS

This article shows how to configure DNS settings in IGEL OS.

Menu path: **Network > DNS**



Enable DNS

☑ The manual DNS configuration will be used.

☐ The DNS configuration will be carried out by DHCP or BOOTP. (Default)

Default domain

Usually the name of the local network.

Nameserver

IP address of the nameserver to be used.

Nameserver

IP address of an alternative nameserver.

Manually overwrite DHCP settings

☑ The default route, the domain name, and the DNS server will be overwritten by manual entries.

☐ Manual entries will not overwrite DHCP settings. (Default)

Dynamic DNS registration

☑ The terminal name will be registered dynamically via the DNS or DHCP server.

☐ The terminal name will not be registered dynamically. (Default)

Dynamic DNS registration method

- **DHCP**: Updates the terminal name through DHCP option 81. (Default)
- **DNS**: Sends updates to the DNS server in accordance with RFC 2136.

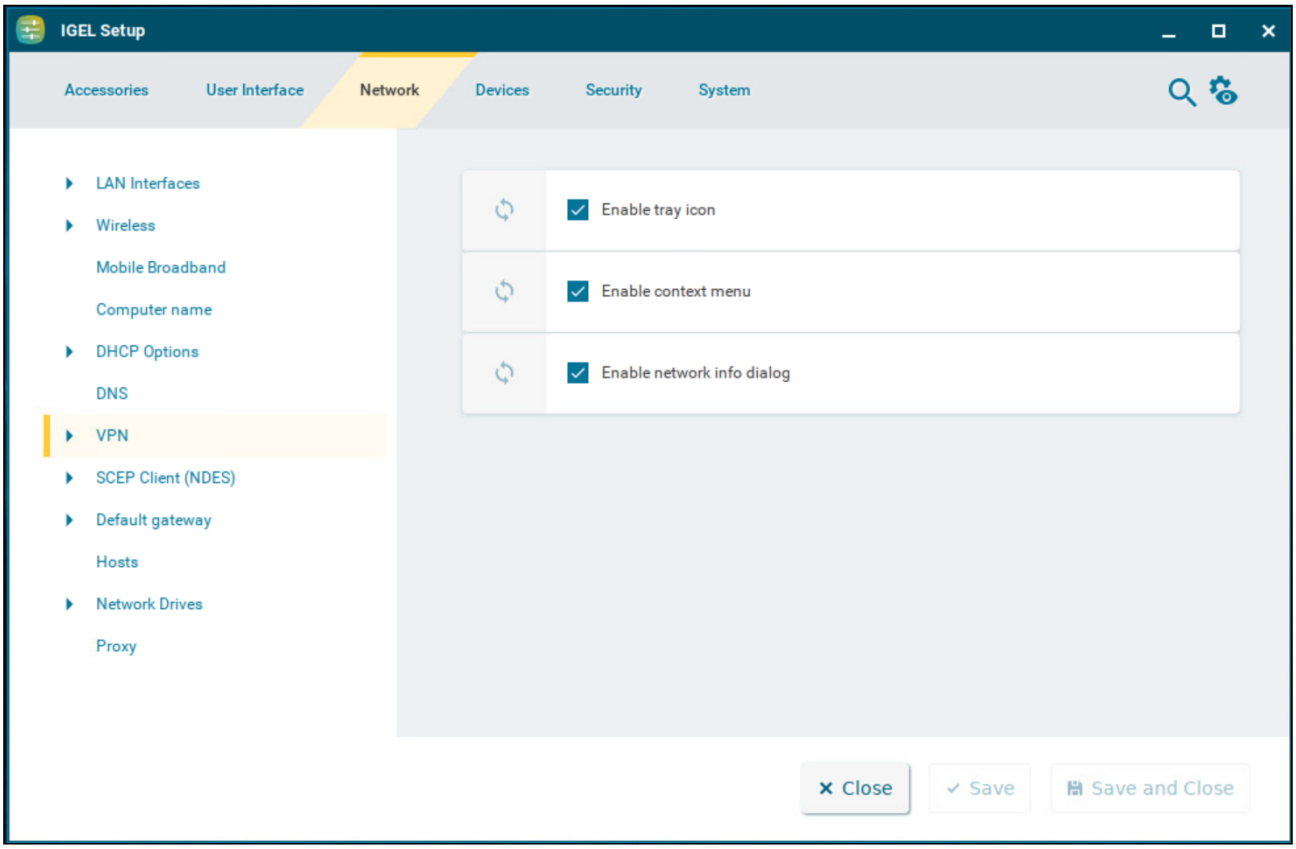
TSIG key file for additional DNS authentication

Path to the private key if TSIG-based DDNS registration is used.

VPN

Remote users securely access company networks via virtual private network (VPN) protocols. This article shows how to configure the tray icon, the context menu, and the dialog window for VPN in IGEL OS.

Menu path: **Network > VPN**



Enable tray icon

☑ A tray icon for the network interface will be shown. (Default)

Enable context menu

☑ A context menu will be shown when you click on the tray icon. (Default)

Enable network info dialog

☑ A dialog window with information regarding the network connection will be shown when you click on the context menu. (Default)

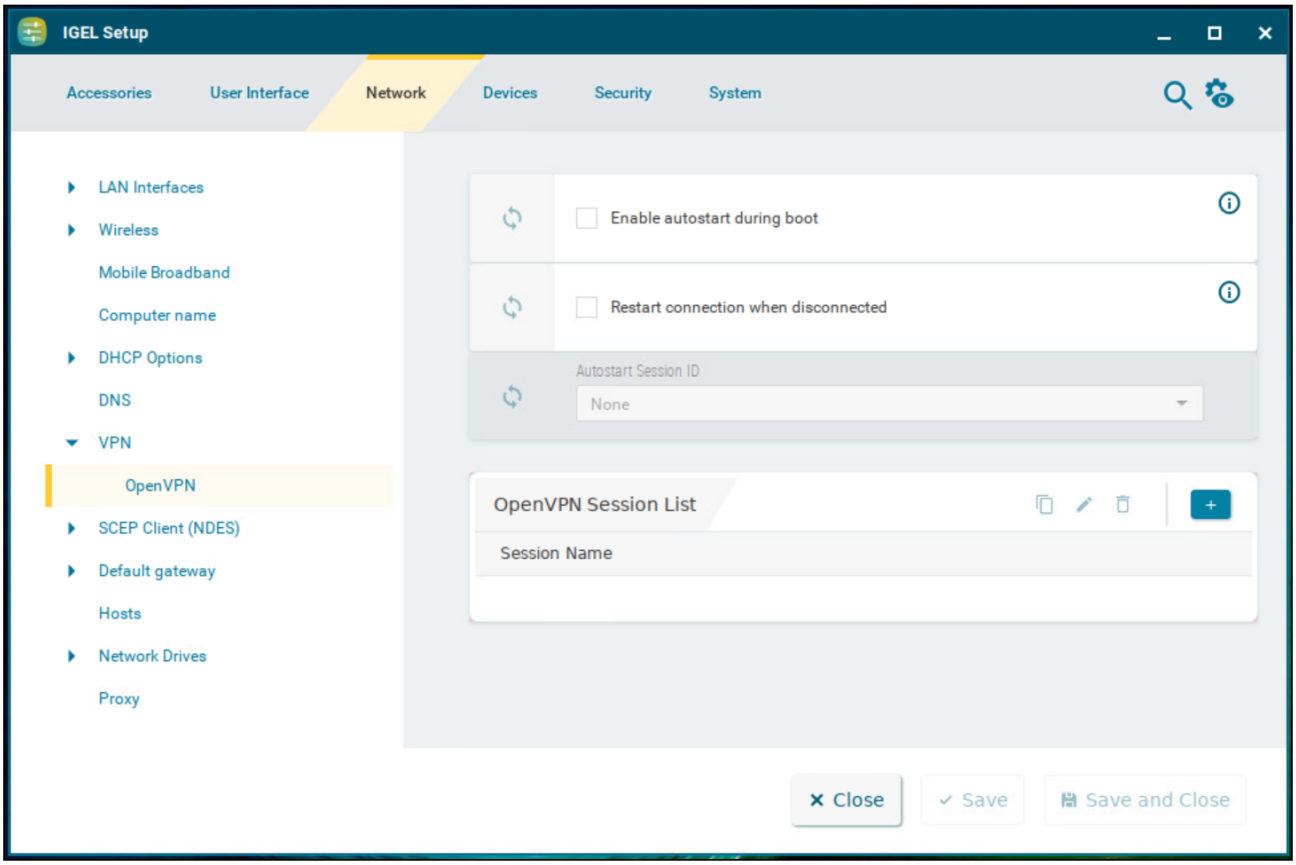
- OpenVPN (see page 166)

OpenVPN

The OpenVPN client puts in place a virtual private network using TLS encryption and requires OpenVPN 2.x as a VPN server. This article shows how to configure OpenVPN connection in IGEL OS.

> If problems occur with OpenVPN, read the `/var/log/syslog` file with the System Log Viewer. For more information, see System Log Viewer (see page 40).

Menu path: **Network > VPN > OpenVPN**



Enable autostart during boot

☑ Autostart will be enabled for the session selected under **Autostart session ID**.

☐ Autostart is disabled. (Default)

Restart connection when disconnected

☑ The connection is restarted automatically when a disconnect occurs.

☐ The connection is not restarted automatically when a disconnect occurs. (Default)

Autostart session ID

Select the desired session from the list of OpenVPN sessions to enable this connection to be established during the boot procedure.

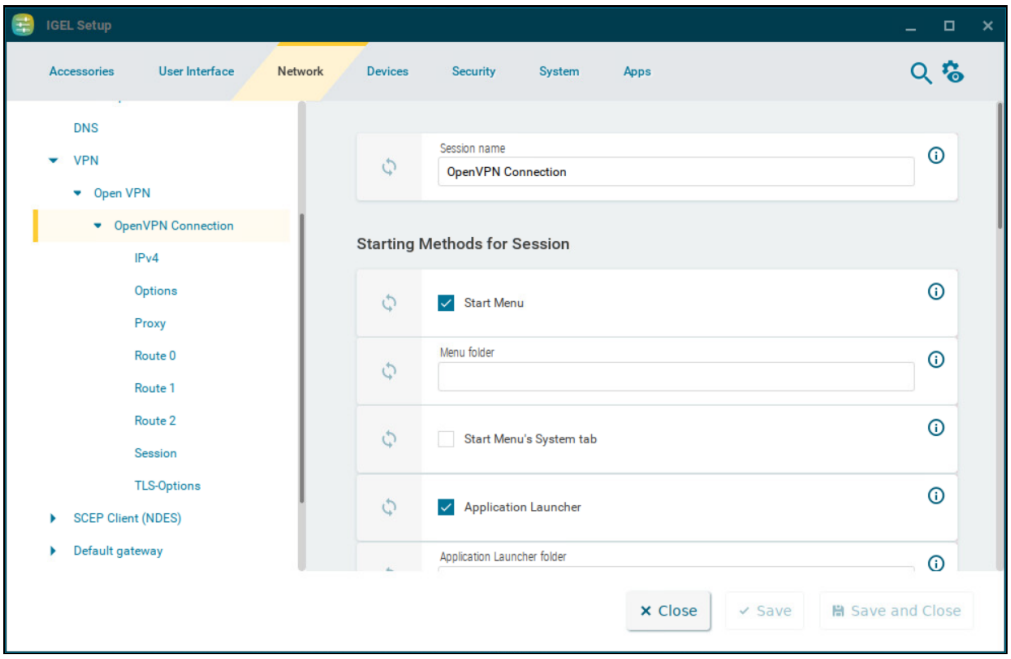
To manage the list of OpenVPN sessions, proceed as follows:

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

Clicking opens the configuration pages for the OpenVPN session.

OpenVPN Session Configuration

Menu path: **Network > VPN > OpenVPN > [OpenVPN Session Name]**



Session name: Name for the session.

> The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Menu folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher

☑ The session can be launched with the Application Launcher.

Application Launcher folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Desktop folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Quick start panel

☑ The session can be launched with the quick start panel.

Password protection

Specifies which password will be requested when launching the session.

Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user password is requested when launching the session.

⚠ **Password protection** only works if the selected password is configured under **Security > Password**. Without the password configuration, the session will launch without requesting a password. For more information, see Password (see page 245).

Hotkey Configuration

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers

A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

> ⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

  > ⓘ When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key

Key for the hotkey

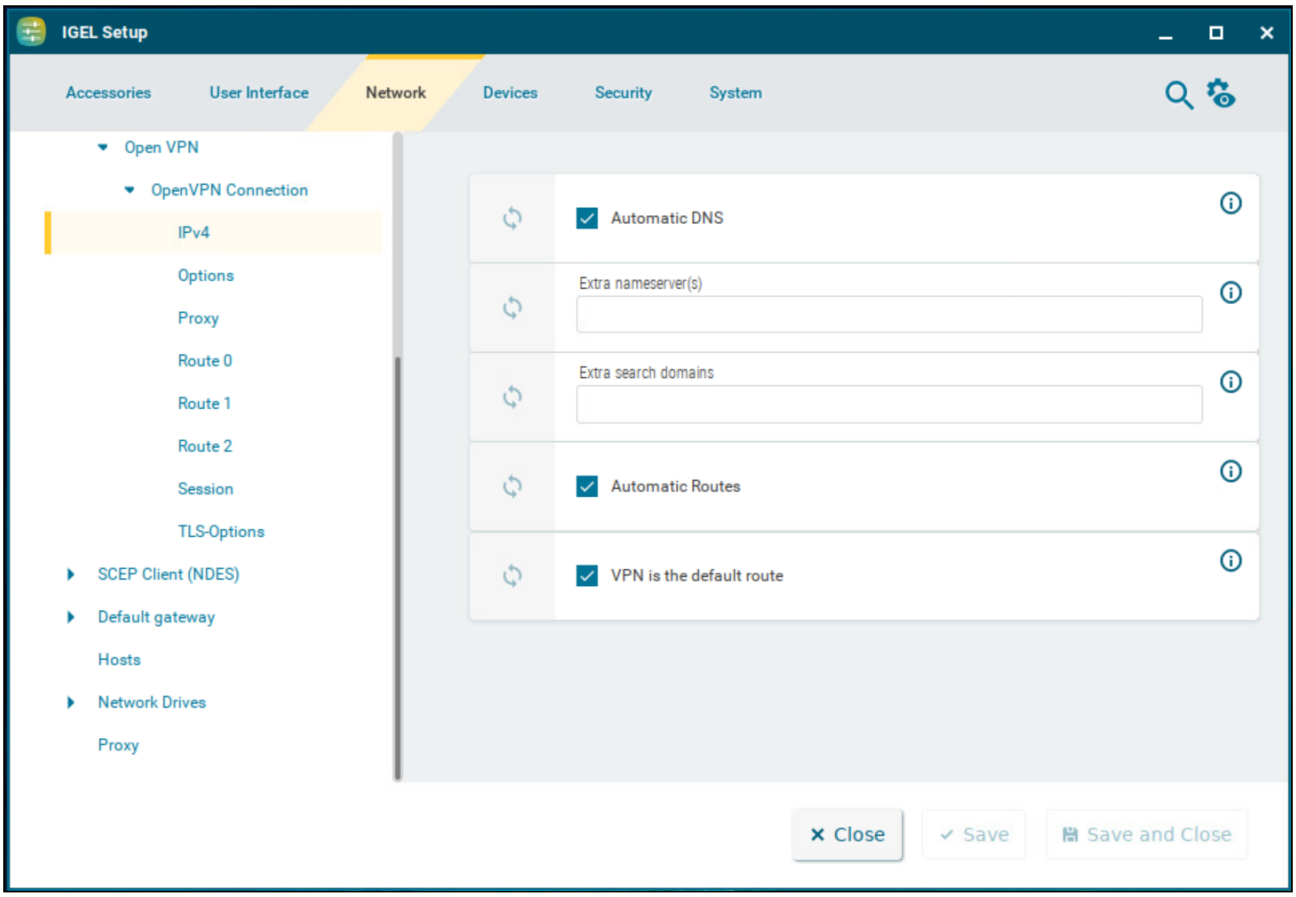
> ⓘ To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

- IPv4 (see page 171)
- Options (see page 173)
- Proxy (see page 176)
- Route (see page 178)
- Session (see page 180)
- TLS-Options (see page 184)

IPv4

This article shows how to configure DNS and routing settings for OpenVPN connections in IGEL OS. By default, OpenVPN uses the server's DNS and routing settings.

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > IPv4**



Automatic DNS

☑ The nameserver(s) will be carried over by the OpenVPN server. (Default)

☐ The nameserver(s) specified under **Extra nameserver(s)** will be used.

Extra nameserver(s)

One or more nameservers, IP addresses separated by commas.

Extra search domains

One or more search domains, separated by commas.

Automatic routes

☑ The routing table will be carried over by the OpenVPN server. (Default)

☐ Extra routes will be configured.

VPN is the default route

☑ All the traffic is routed through the VPN by default. (Default)

☐ Extra routes will be configured.

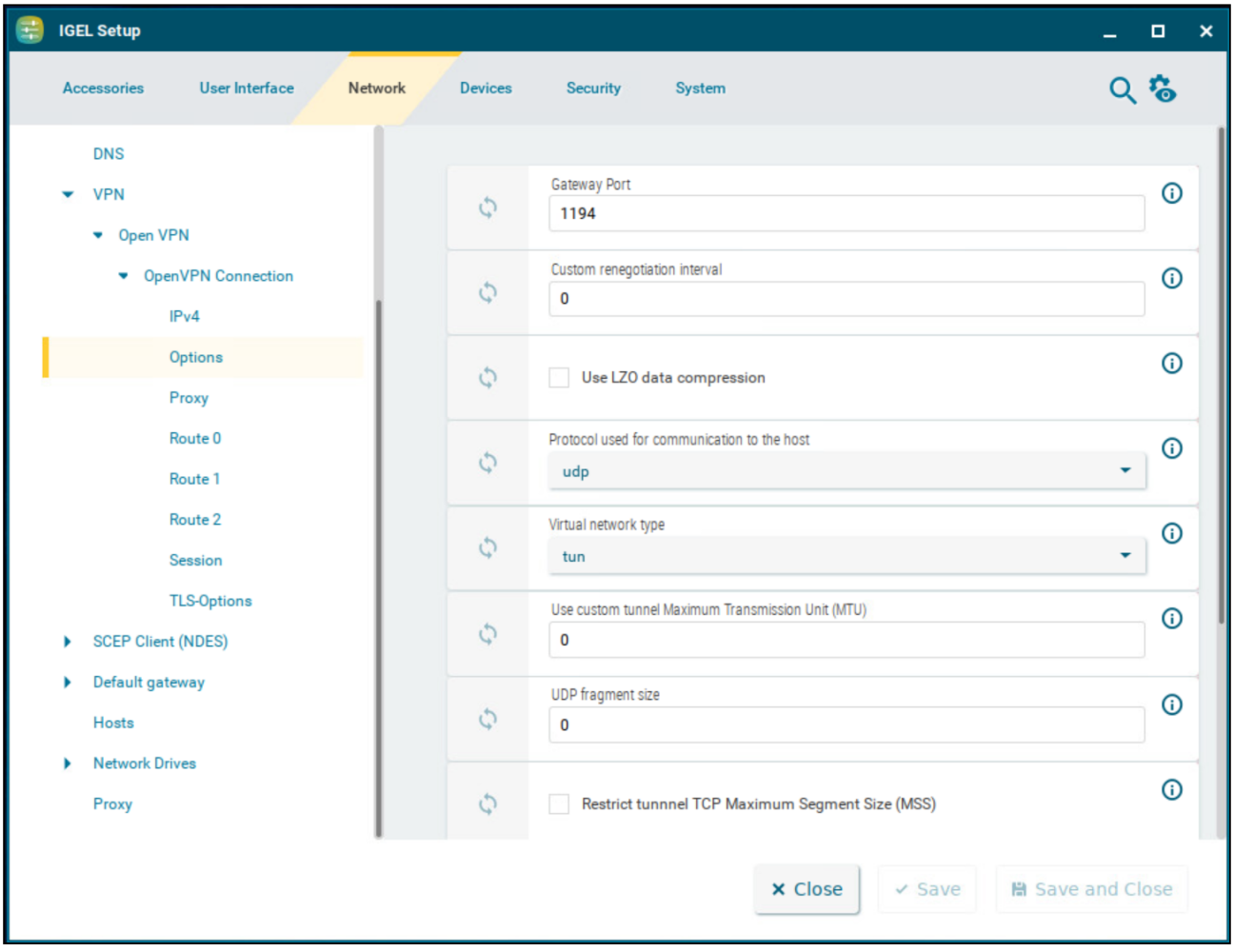
For details on extra route configuration, see Route (see page 178).

Options

This article shows how to configure the options for the OpenVPN client in IGEL OS in order to ensure interaction with the server.

> Further information regarding the options can be found in the OpenVPN documentation[13] which is maintained by the OpenVPN project.

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > Options**



13 https://openvpn.net/index.php/open-source/documentation.html

Gateway port

Local gateway port. (Default: 1194)

Custom renegotiation interval

Renegotiate data channel key after given number of seconds. (Default: 0)

Use LZO data compression

☑ The client will use LZO compression. Necessary if the server uses compression.

☐ The client will not use LZO compression. (Default)

ⓘ If establishing a tunnel fails, try again with **Use LZO data compression** enabled.

⚠ The **--comp-lzo** option is considered deprecated from OpenVPN v2.4 and should not be used any more. For more information, see https://community.openvpn.net/openvpn/wiki/DeprecatedOptions#Option:--comp-lzoStatus:Pendingremoval.

Protocol used for communication to the host

- **UDP**: UDP will be used. (Default)
- **TCP-client**: TCP will be used.

ⓘ If you use a proxy, select **TCP-client**.

Virtual network type

- **TUN**: Routing will be used. (Default)
- **TAP**: Bridging will be used.

Use custom tunnel Maximum Transmission Unit (MTU)

The MTU of the TUN device will be used as a given value. The MTU of the interface will be derived from it.

UDP fragment size

Allow internal data fragmenting up to this size in bytes. Leave this field empty to keep the default value.

Restrict tunnel TCP Maximum Segment Size (MSS)

☑ The TCP segment size (MSS) of the tunnel will be restricted.

☐ The TCP segment size (MSS) will not be restricted. (Default)

Randomize remote hosts

☑ The remote gateways will be ordered randomly as a simple type of load balancing.

☐ The remote computers will not be ordered randomly. (Default)

Cipher

Encryption algorithm for data packets. (Default: BF-CBC - Blowfish in the Cipher Block Chaining Mode)

HMAC authentication

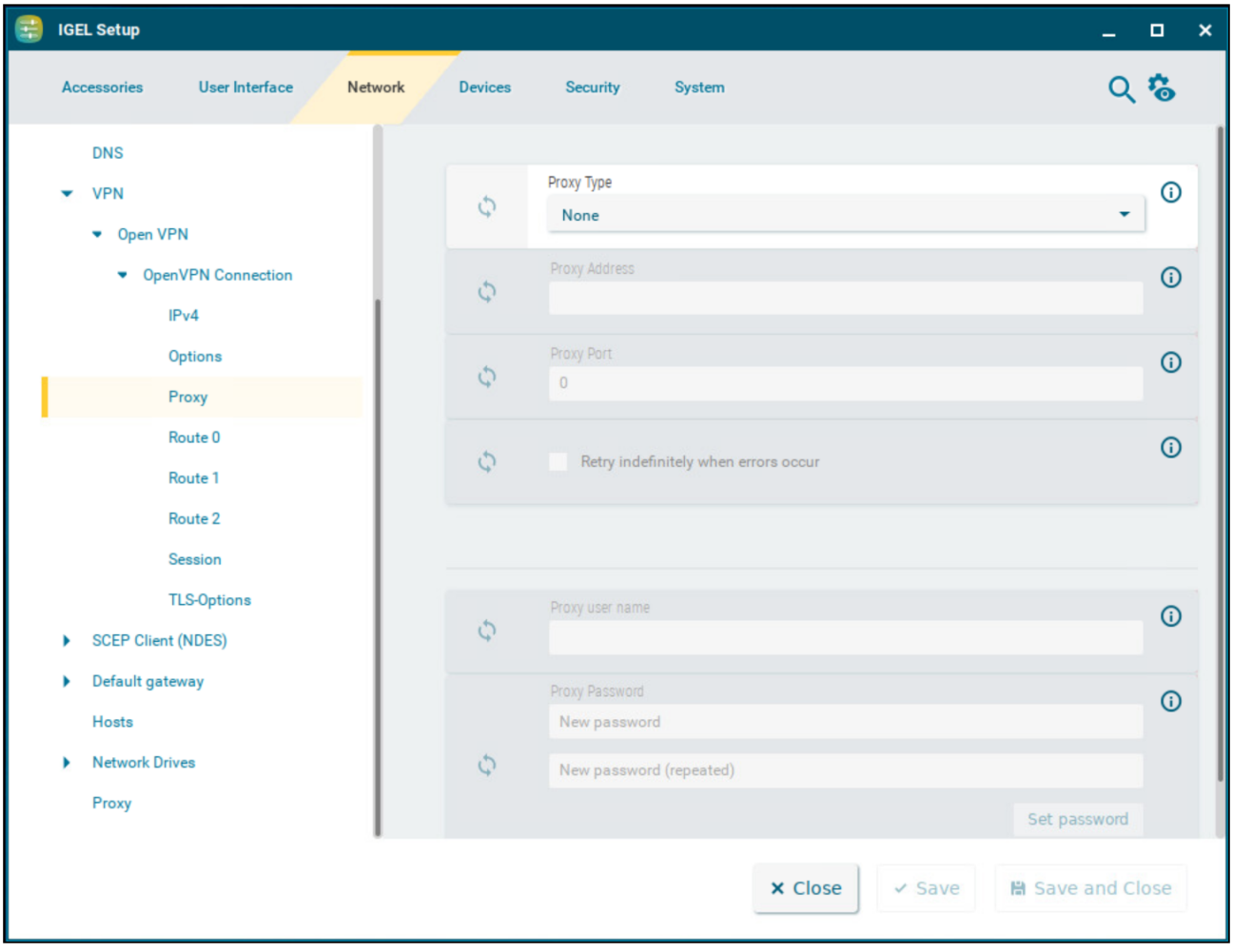
Hashing algorithm for packet authentication (Default: SHA1)

Proxy

This article shows how to set up an optional proxy server for the VPN connection in IGEL OS.

> If you use a proxy, set the **Communication protocol to the host** as **tcp-client** under **OpenVPN > [OpenVPN Connection] > Options**. For detailed information on options settings, see Options (see page 173).

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy**



Proxy type

- **None**: Direct connection to the Internet. (Default)

- **HTTP**: HTTP proxy will be used.
- **SOCKS**: SOCKS proxy will be used.

Proxy address

Name or IP address of the proxy server

Proxy port

Port on which the proxy service is available

Retry indefinitely when errors occur

☑ In the event of errors, repeated attempts to establish a connection via proxy will be made.

☐ No further attempts to establish a connection will be made. (Default)

The following credentials are for the **HTTP** proxy type:

Proxy user name

User name for the proxy server

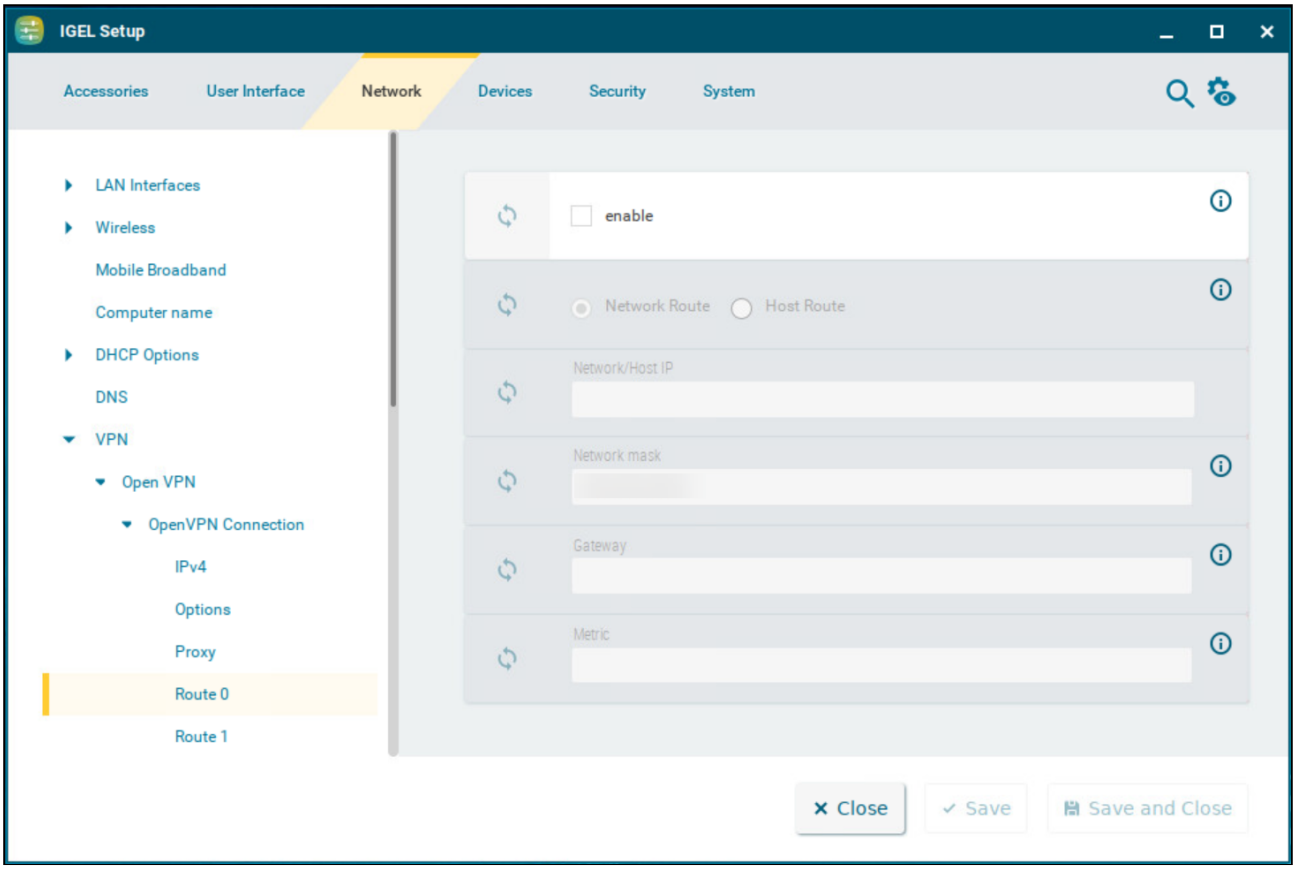
Proxy password

Password for the proxy server

Route

This article shows how to configure extra routes for the network in IGEL OS.

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > Route [0,1,2]**



Enable

☑ This route is enabled.

☐ This route is not enabled. (Default)

Network route / Host route

- **Network route**: The routing relates to a (sub) network. (Default)
- **Host route**: The routing relates to the address of a computer.

Network/Host IP

The address of the network (for a network route) or the IP address or the name of the host (for a host route).

Network mask

Mask for the desired IP range, e.g. 255.255.255.0

Gateway

Gateway that routes the packets to the target network.

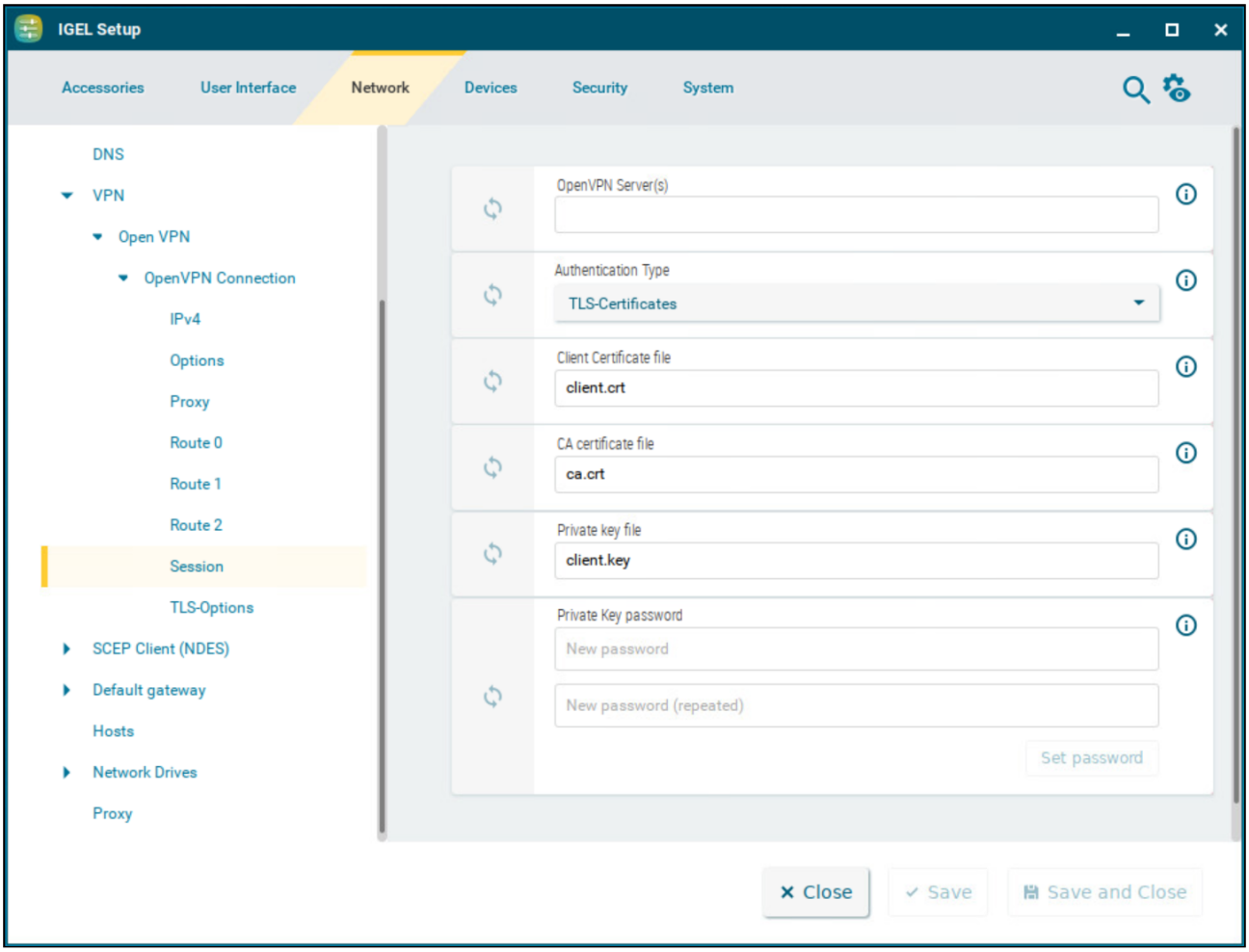
Metric

The numerical quality assessment for routing decisions, 0 is the best value.

Session

This article shows how to configure the authentication of the Open VPN session in IGEL OS.

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > Session**



OpenVPN server(s)

Name or public IP address of the OpenVPN server. You can enter multiple values separated by commas.

Authentication type

- **TLS-Certificates**: Authentication with user certificate and private key.
- **Name/Password**: Authentication with user name and password.

- **Name/Password with TLS-Certificates**: Combines name/password with user certificate.
- **Static Key**: Authentication with a private key. No PKI infrastructure is needed for this.

TLS Certificates Authentication Type

> Persistent storage of files is possible in the folder `/wfs` resp. subfolders of `/wfs` only.
> Files stored under other paths will be lost when the device is rebooted.

Client certificate file

File with the client certificate. Enter a path relative to `/wfs/OpenVPN`.

CA certificate file

File with the CA certificate. Enter a path relative to `/wfs/OpenVPN`.

Private key file

File with the private key. Enter a path relative to `/wfs/OpenVPN`.

Private key password

Password in case one is set for the private key.

> If you have a PKCS#12 file which contains the client certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

Name/Password Authentication Type

User name

User name - if you leave this field empty, the user will be asked for it when establishing a connection.

Password required

☑ The user must enter a password. (Default)

Password

Password - if you leave this field empty, the user will be asked for it when establishing a connection.

CA certificate file

File with the CA certificate. Enter a path relative to `/wfs/OpenVPN`.

Name/Password with TLS-Certificates Authentication Type

User name

User name - if you leave this field empty, the user will be asked for it when establishing a connection.

Password required

☑ The user must enter a password. (Default)

Password

Password - if you leave this field empty, the user will be asked for it when establishing a connection.

Client certificate file

File with the user certificate. Enter a path relative to `/wfs/OpenVPN`.

CA certificate file

File with the CA certificate. Enter a path relative to `/wfs/OpenVPN`.

Private key file

File with the private key. Enter a path relative to `/wfs/OpenVPN`.

Private key password

Password in case one is set for the private key.

> ⓘ If you have a PKCS#12 file which contains the user certificate, CA certificate and private key, always enter its name in the three file fields. The advantage lies in the fact that only a single file needs to be distributed.

Static Key Authentication Type

Private key file

File with the static key. Enter a path relative to `/wfs/OpenVPN`.

Key Direction

- **None**: No key direction. (Default)

- **0**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **1**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.

Remote IP address

The VPN IP address of the server

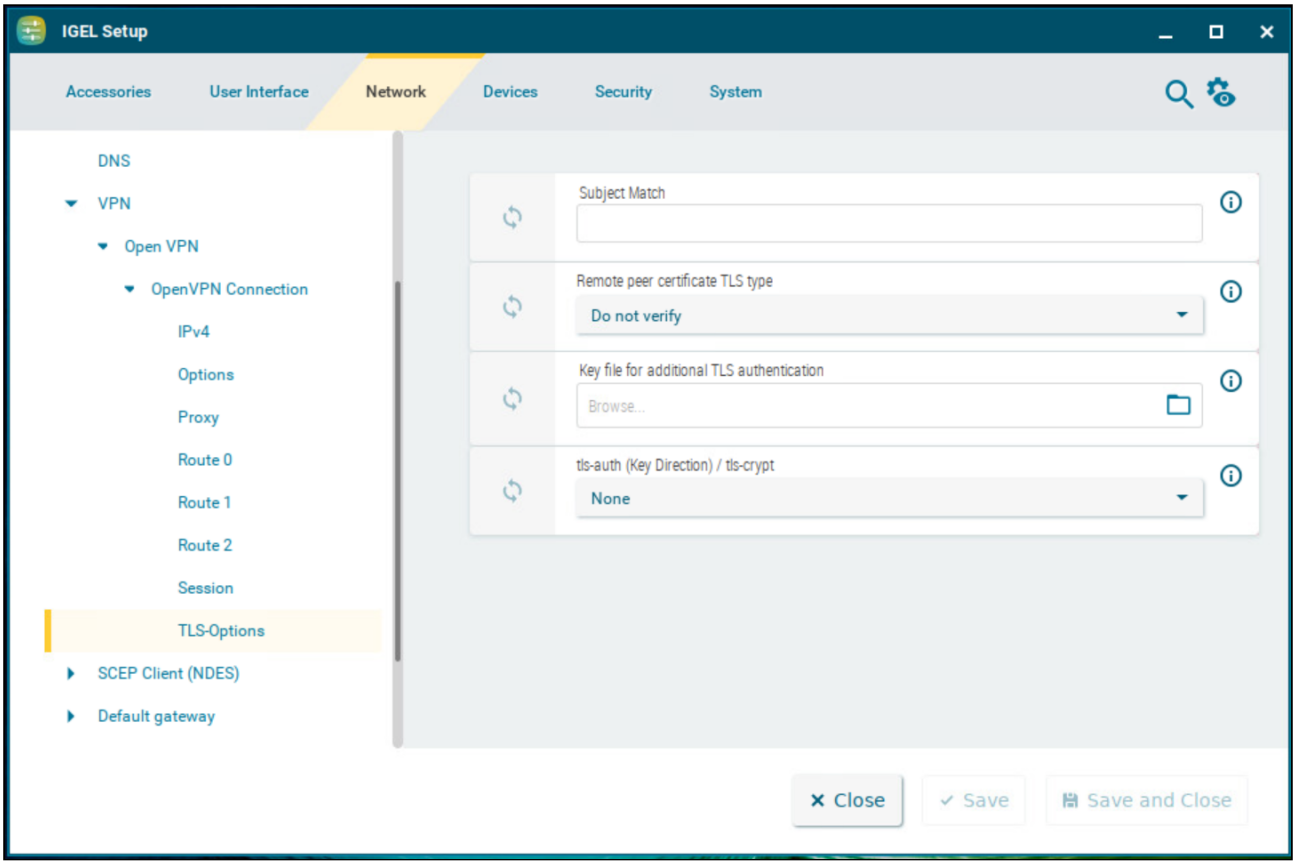
Local IP address

The VPN IP address of the client

TLS-Options

Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL). It is a standard consisting of several protocols that can transmit encrypted data between authenticated communication partners over potentially insecure IP networks such as the Internet. This article shows how to configure TLS options for the OpenVPN protocol in IGEL OS.

Menu path: **Network > VPN > OpenVPN > [OpenVPN Connection] > TLS-Options**



Subject match

The Subject Match accept/reject the server connection based on a custom test of the server certificate's embedded X509 subject details. The formatting of these fields changed into a more standardized format: **C=** `US` **, L=** `Somewhere` **, CN=** `JohnDoe` **, emailAddress=** `john@example.com` **.**

For more information, see the Reference manual for OpenVPN 2.6[14].

14 https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6//

Remote peer certificate TLS type

Require that peer certificate was signed with an explicit key usage and extended key usage based on RFC3280 TLS rules.

This is a useful security option for clients, to ensure that the host they connect to is a designated server. Or the other way around; for a server to verify that only hosts with a client certificate can connect.

- **Do not verify**: No remote certificate check. (Default)
- **Check for server certificate**: The **--remote-cert-tls server** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Server Authentication"**.
- **Check for client certificate**: The **--remote-cert-tls client** option is equivalent to **--remote-cert-ku --remote-cert-eku "TLS Web Client Authentication"**.

This is an important security precaution to protect against a man-in-the-middle attack, where an authorized client attempts to connect to another client by impersonating the server. The attack is easily prevented by having clients verify the server certificate using any one of **--remote-cert-tls, --verify-x509-name,** or **--tls-verify.**

Key file for additional TLS authentication

As the path enter relative to `/wfs/OpenVPN` or select using the file selection. This adds an additional HMAC legitimization level above the TLS control channel in order to prevent DDOS attacks.

tls-auth (Key Direction) / tls-crypt

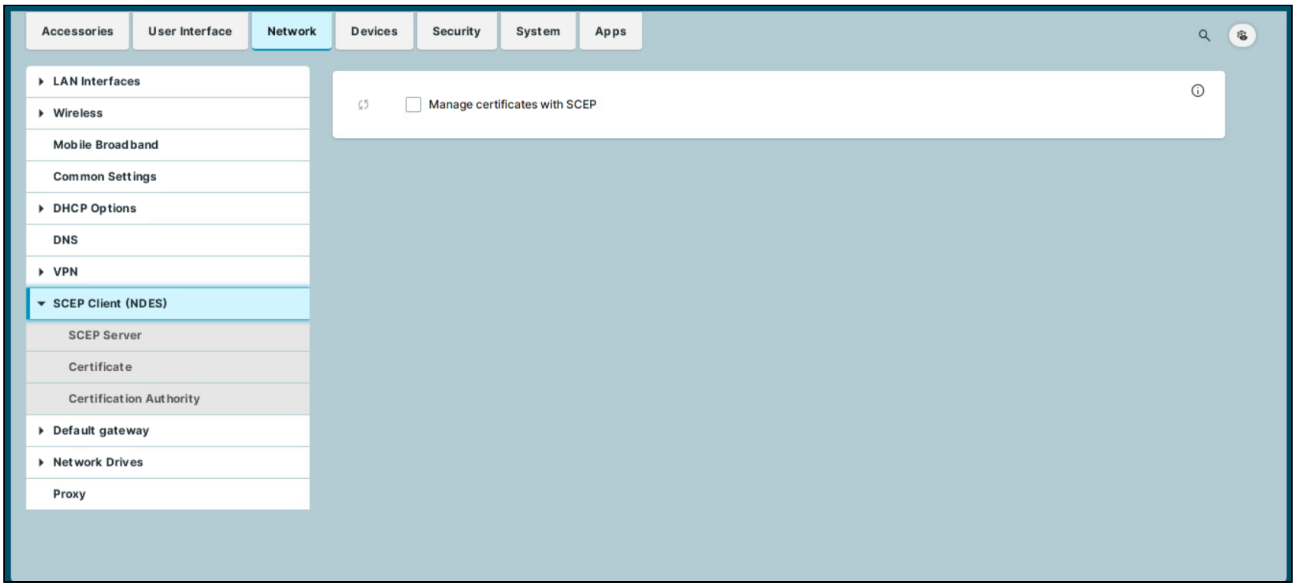
- **None**: No key direction. (Default)
- **tls-auth 0**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-auth 1**: If the default option is not used, one side of the connection should use Direction 0 and the other Direction 1.
- **tls-crypt**: In contrast to tls-auth, setting a key direction is not required. Use this option if the version of the OpenVPN server is 2.4 or higher. For more information on tls-crypt, see Reference manual for OpenVPN 2.6[15].

15 https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6//

SCEP Client (NDES)

SCEP allows the automatic provision of client certificates via an SCEP server and a certification authority. This type of certificate is automatically renewed before it expires and can be used for purposes such as network authentication (e.g. IEEE 802.1x). This article shows how to configure SCEP certificate management in IGEL OS.

Menu path: **Network > SCEP Client (NDES)**



Manage certificates with SCEP

☑ Certificate management via SCEP Client (NDES) is enabled.

☐ Certificate management via SCEP Client (NDES) is not enabled. (Default)

A Microsoft Windows Server (MSCEP, NDES) for example can serve as a queried counterpart (SCEP server and certification body). More information can be found at Microsoft, e.g. in the following Technet article: Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)[16].

- SCEP Server (see page 188)
- Certificate (see page 190)

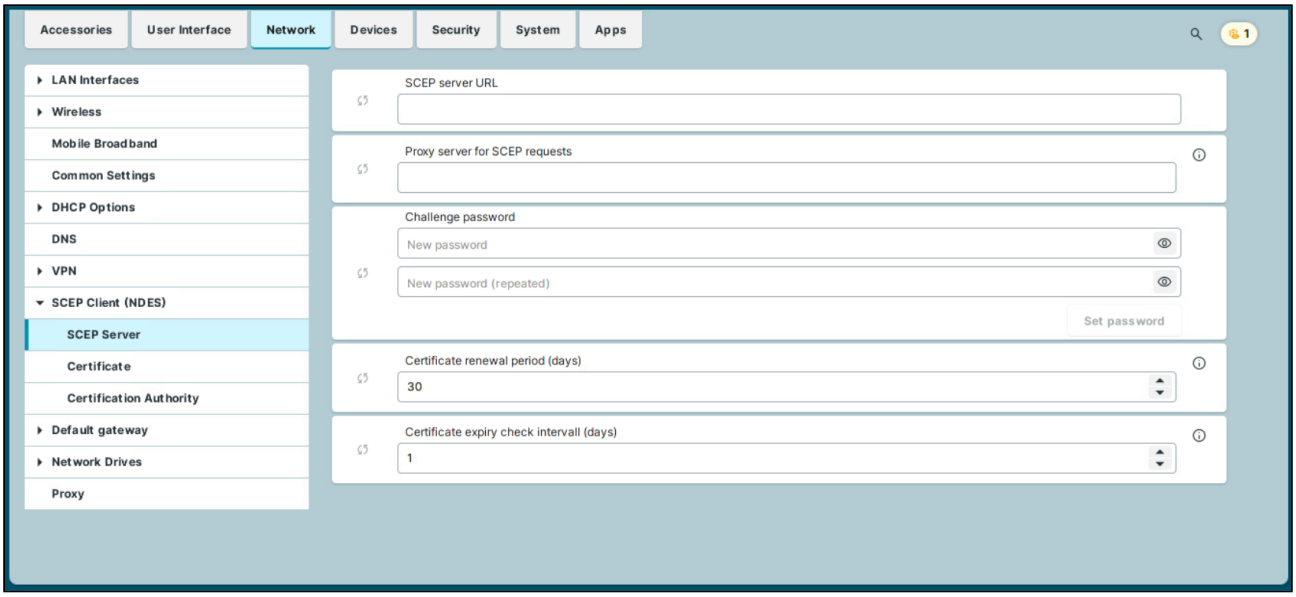
16 http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

- Certification Authority (see page 193)

SCEP Server

This article describes the settings required for a SCEP server in IGEL OS.

Menu path: **Network > SCEP Client (NDES) > SCEP Server**



Because of the need to enter a fingerprint (CA root certificate) and the **Challenge password** (SCEP server), the configuration process is somewhat complicated. Ideally, it should be set up in the UMS as a profile and distributed to the devices. For more information, see How to Create and Assign Profiles in the IGEL UMS Web App.
At the same time, the certificate cannot yet be used for communication purposes.

SCEP server URL

Address of the SCEP server.
Examples:

- `http://myserver.mydomain.com/certsrv/mscep/mscep.dll` (Windows Server 2019)
- `http://myserver.mydomain.com/certsrv/mscep` (before Windows Server 2019)

Proxy server for SCEP requests

Proxy server in the format `host:port`. If this field is empty, no proxy will be used.

Challenge password

Password for queries

Certificate renewal period (days)

Time interval before certificate expiry after which the certificate renewal procedure is started. (Default: 30)

Certificate expiry check interval (days)

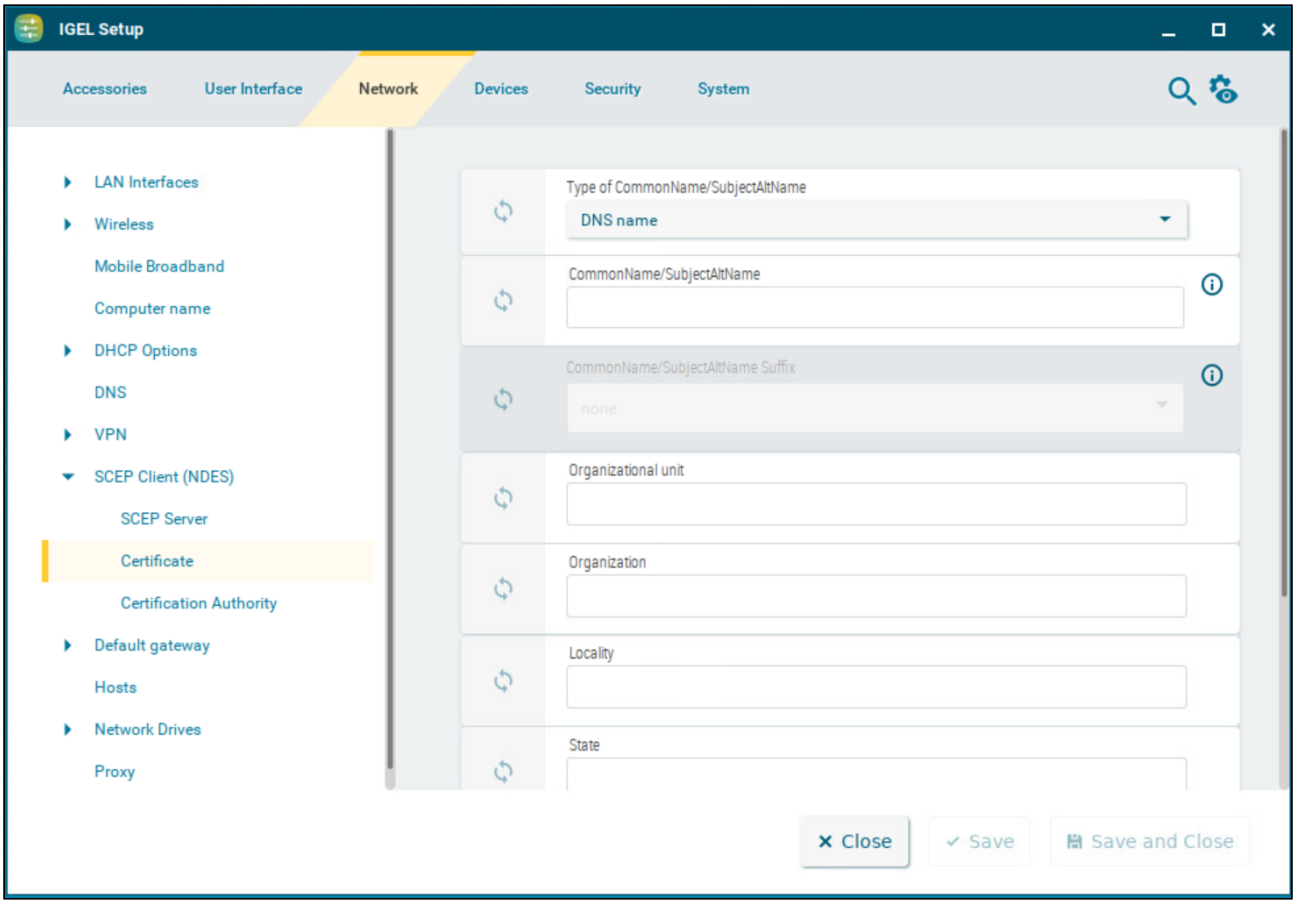
Specifies how often the certificate is checked against its expiry date. (Default: 1)

> As an example, a certificate is valid until 31.12. of a year. If the period for renewal is set to 10 days, a new certificate will be requested for the first time on 21.12. of the same year.

Certificate

This article shows how to specify the basic data for the certificate to be issued by the certification body for SCEP in IGEL OS.

Menu path: **Network > SCEP Client (NDES) > Certificate**



Type of CommonName/SubjectAltName

The characteristic for linking the certificate to the device.

- **IP address**: The IP address of the device.
- **DNS name**: The DNS name of the device. (Default)
- **IP address (auto)**: The IP address of the device (inserted automatically).
- **DNS name (auto)**: The DNS name of the device (inserted automatically).
- **Email address**: An email address.

- **DNS name as UPN (auto)**

> If the client automatically obtains its network name, **DNS name (auto)** is a good type for the client certificate.

CommonName/SubjectAltName

The parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address**, **DNS name**, or **Email address**. Give a designation which matches the **Type of CommonName/SubjectAltName**.

CommonName/SubjectAltName Suffix

The parameter is available if **Type of CommonName/SubjectAltName** is set to **IP address (auto)**, **DNS name (auto)**, or **DNS name as UPN (auto)**. Specifies a suffix that will be added to CommonName/SubjectAltName. Possible values:

- **None**: No suffix will be added.
- **Dot + DNS domain (auto)**: The system's current DNS domain name separated with a dot will be added. Example: `.igel.local`
- Free text entry: The manually entered suffix will be added. Take notice that the percent symbol "%" is used for introducing the escape sequence, and thus the following replacements take place automatically:
  - `%D` is replaced by the system's DNS domain name at the time the certificate signing request (CSR) is created. Example: `@%D` will be changed into `@igel.de` if the system's current DNS domain name is `igel.de`.
  - `%%` will be replaced by `%`. Example: `A%%B` will be changed into `A%B`.
  - Other combinations with `%` are currently discarded. Example: `A%BC` will be changed into `AC`.

  > If you have to specify the suffix manually, make sure you enter the separator.

Organizational unit

Stipulated by the certification authority

Organization

A freely definable designation for the organization to which the client belongs

Locality

Details regarding the device’s locality. Example: "Augsburg".

State

Details regarding the device’s locality. Example: "Bayern".

Country

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

RSA key length (bits)

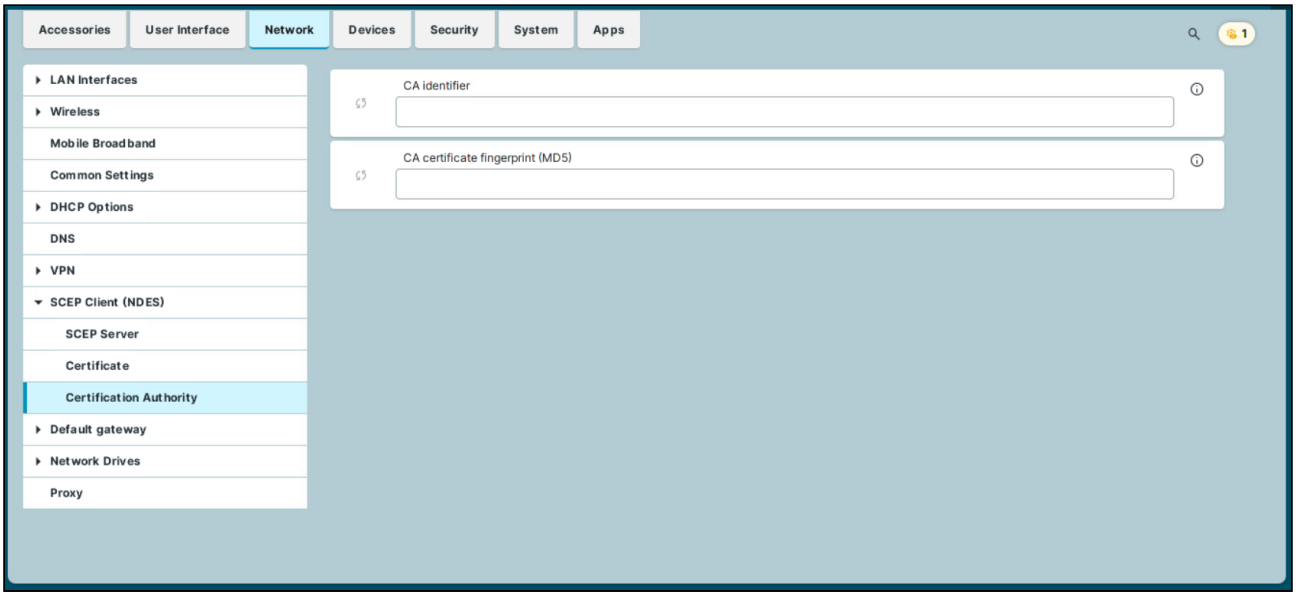
Defines the key length (one suited to the certification authority) for the certificate that is to be issued.
Possible values:

- **1024**
- **2048**
- **4096**

Certification Authority

This article shows how to configure the details of the certification authority in IGEL OS.

Menu path: **Network > SCEP Client (NDES) > Certification Authority**



The details for the following fields can be obtained from the certification authority:

CA identifier

Name of Certification Authority

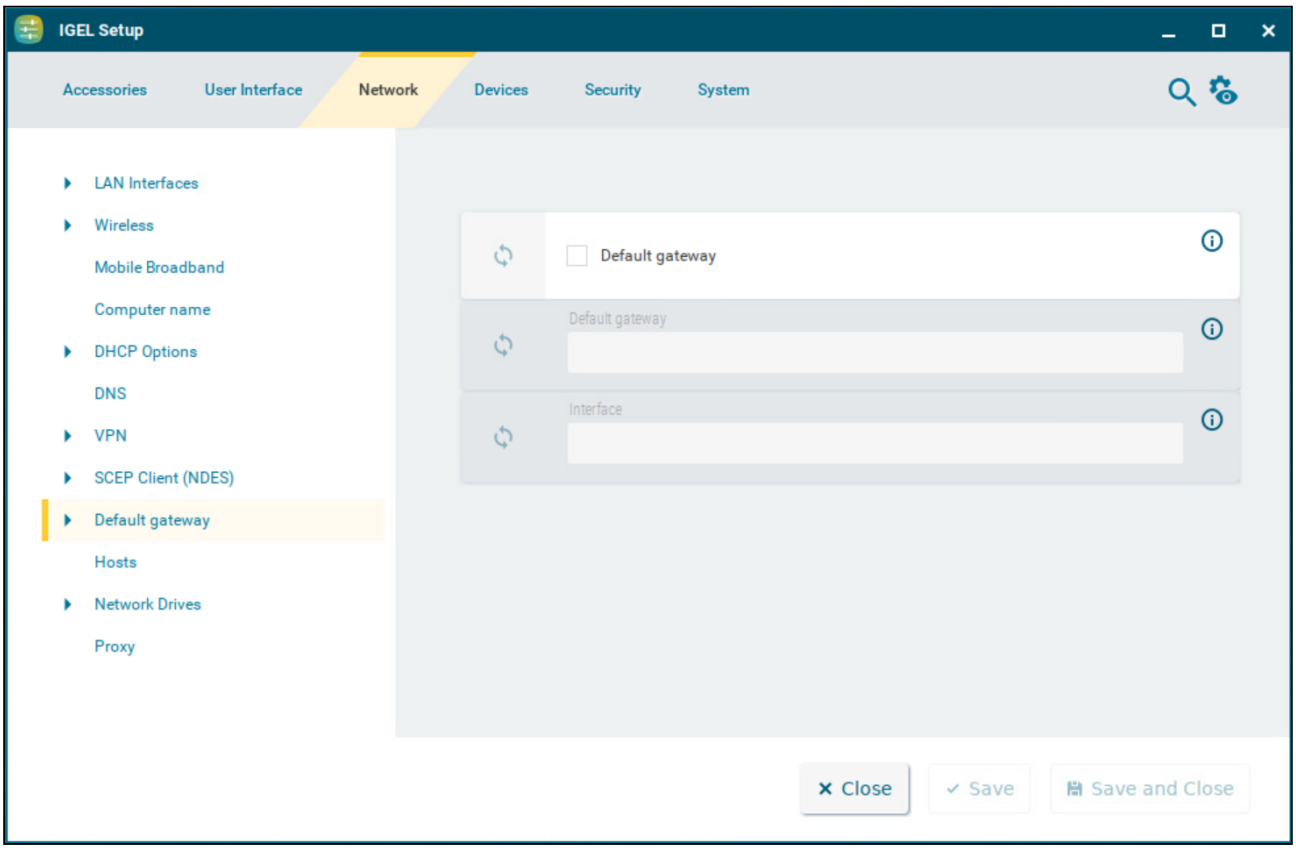
CA certificate fingerprint (MD5)

MD5 fingerprint of the root certificate

Default Gateway

This article shows how to configure the default gateway in IGEL OS.

Menu path: **Network > Default Gateway**



Default gateway

☑ Routing is enabled.

☐ Routing is disabled. (Default)

Default gateway

Gateway that routes the packets to the target network

Interface

The network interface via which the route is to run

Predictable Network Interface Names (PNINs)
The names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see Predictable Network Interface Names[17]. This ensures the stability of interface names on reboot and generally improves the reliability of associating configurations with interfaces.

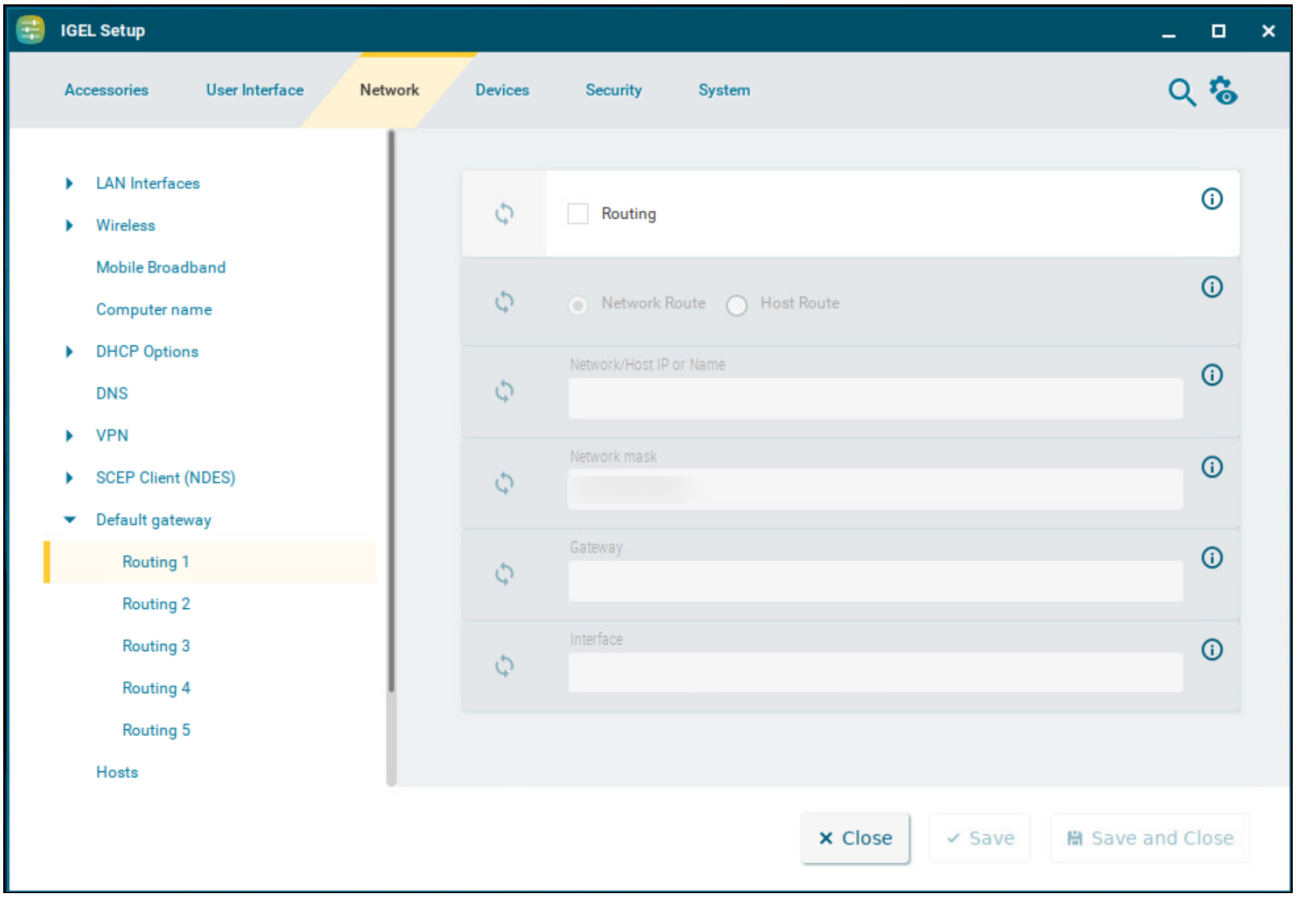
- As "`eth0`", "`eth1`", and "`wlan0`" have been replaced by PNINs, configurations or custom scripts that include the old names of Ethernet and WLAN interfaces, e.g. `eth0`, `eth2`, `wlan0`, have to be adjusted.
  The following already existing configurations do NOT require manual adjustment since old names `eth0`, `eth1`, etc. will internally be replaced by the correct PNINs automatically:
  - Tcpdump
- To view the PNINs and the order of the configured interfaces, you can use the following commands. The default interface is always listed first, the second interface is listed second, etc.
  Ethernet (LAN): `cat /config/net/en-interfaces`
  WLAN: `cat /config/net/wl-interfaces`
  (Note: Only the first wireless interface (former `wlan0`) is supported. All other wireless interfaces will be ignored.)
- If you need to configure more than two Ethernet interfaces, go to **System > Registry > network.interfaces.ethernet.device%** and add an instance by clicking **Add Instance**. To explicitly assign a configuration instance to a certain interface, enter the corresponding PNIN for the registry key **network.interfaces.ethernet.device%.ifname**.

17 https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/

Routing

This article shows how to configure routing in IGEL OS.

Menu path: **Network > Default gateway > Routing [1-5]**



Routing

☑ This route is enabled.

☐ This route is disabled. (Default)

Network route / Host route

Type of route.

- **Network route**: The routing relates to a (sub) network. (Default)
- **Host route**: The routing relates to the address of a computer.

Network/Host IP or Name

The address of the network (for a network route) or the IP address or the name of the host (for a host route).

Network mask

Mask for the desired IP range, e.g. 255.255.255.0

Gateway

Gateway that routes the packets to the target network

Interface

The network interface via which the route is to run

Network Drives

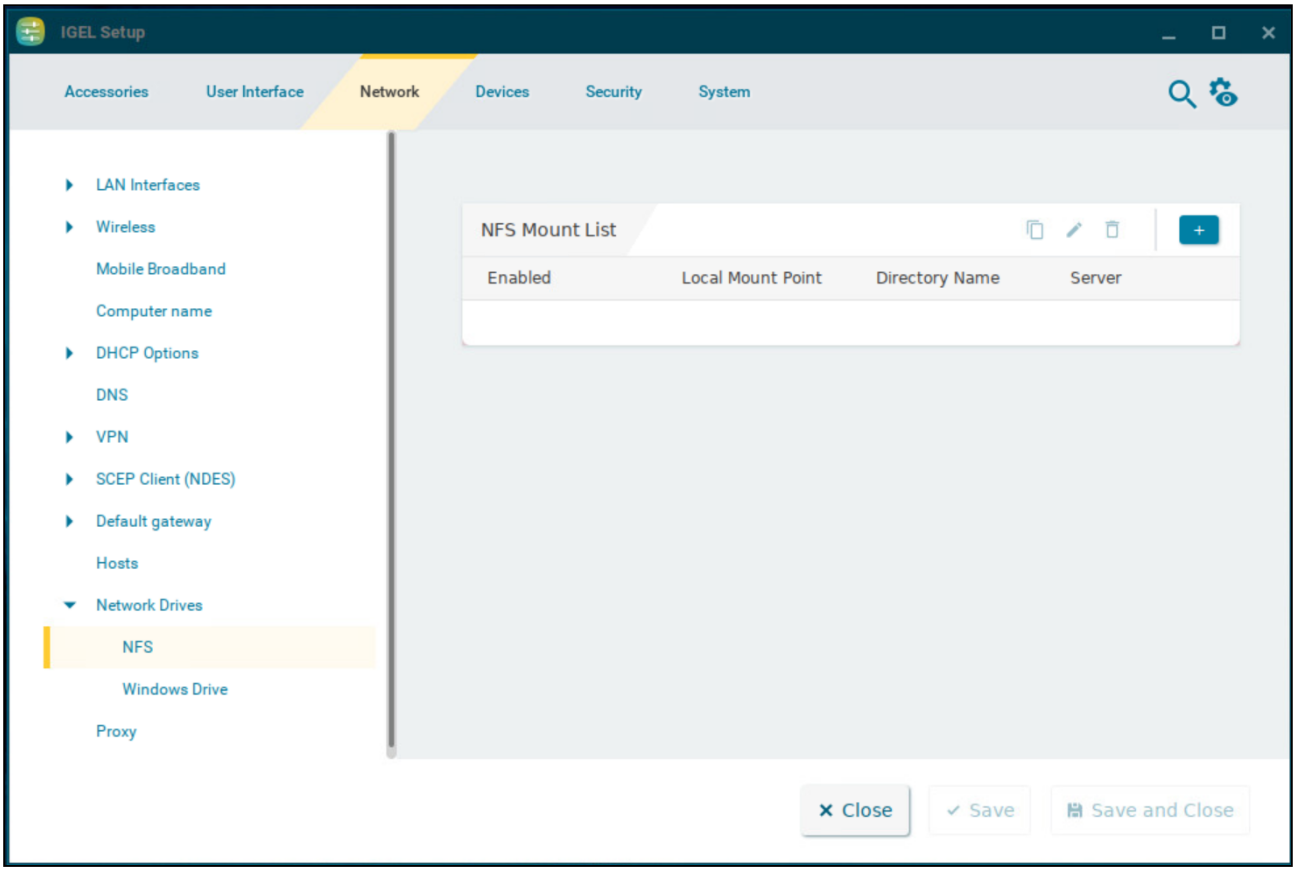
The following network drives can be configured in IGEL OS.

- NFS (see page 199)
- Windows Drive (see page 202)

NFS

This article shows how to integrate network drives using the Network File System (NFS) in IGEL OS.

Menu path: **Network > Network Drives > NFS**



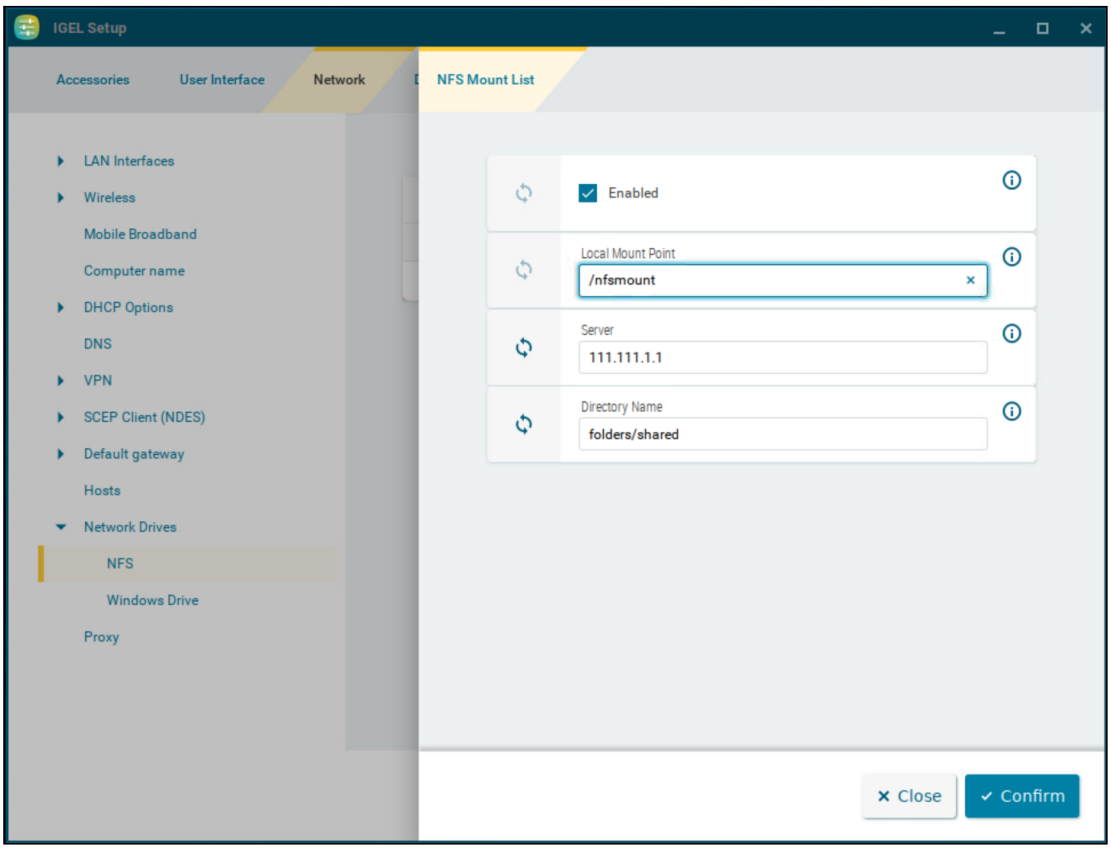
NFS Mount List

List of integrated network drives

To manage the network drives, proceed as follows:

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

Clicking + brings up the **Add** dialogue, where you can define the following settings:



Enabled

☑ The network drive will be integrated. (Default)

Local mount point

The local directory under which the server directory is to be visible. (Default: `/nfsmount`)

> In both the **Local mount point** and **Directory name** only `/` (Linux/Unix-style forward slash) is permitted as a path separator.

Server

NFS server that exports the directory.

> For **Server**, you can provide an IP address, a hostname or a Fully-Qualified Domain Name (FQDN).

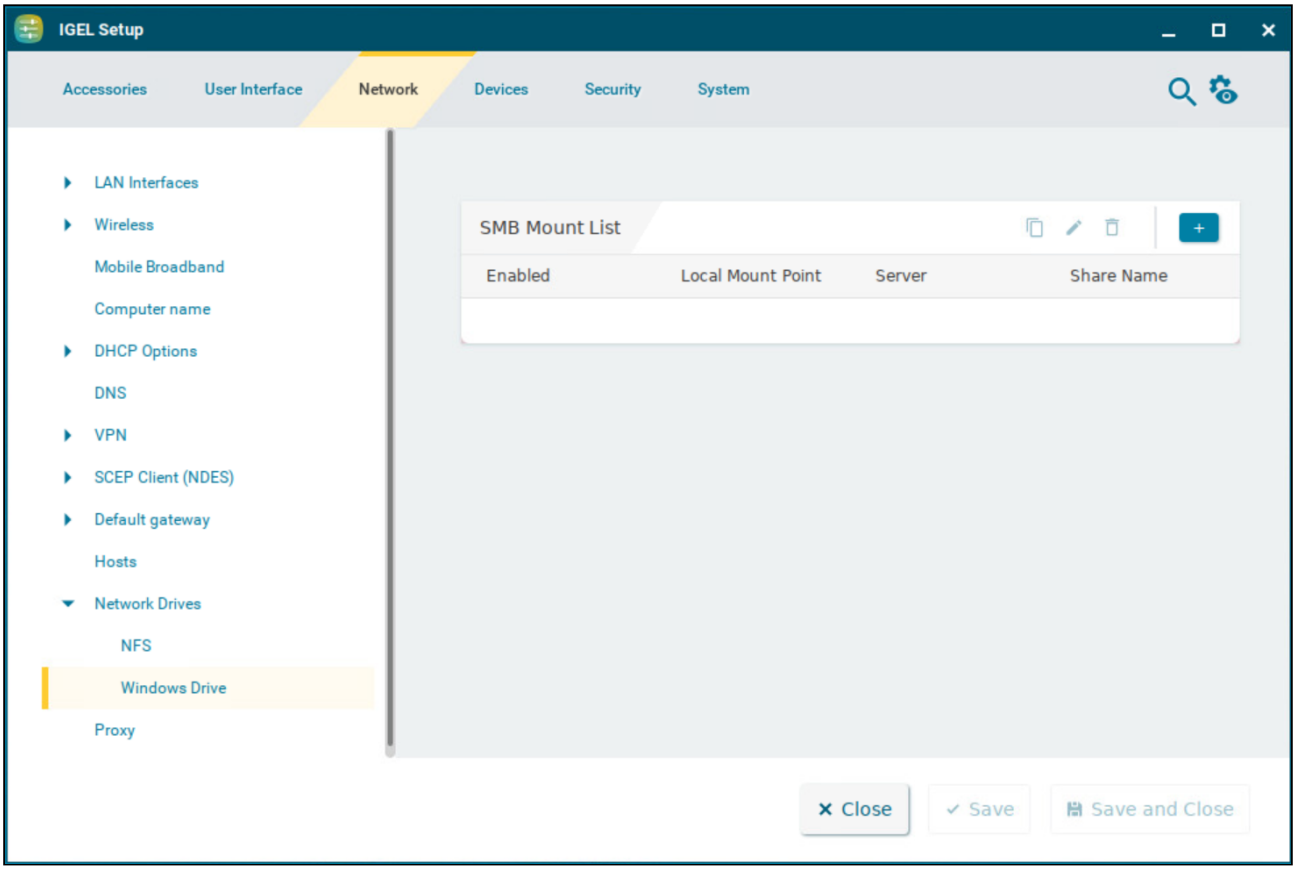
Directory name

Path under which the NFS server exports the directory.

Windows Drive

This article shows how to integrate network drives shared by Windows as well as those from Linux/Unix servers via the SMB protocol (Samba) in IGEL OS.

Menu path: **Network > Network Drives > Windows Drive**



SMB Mount List

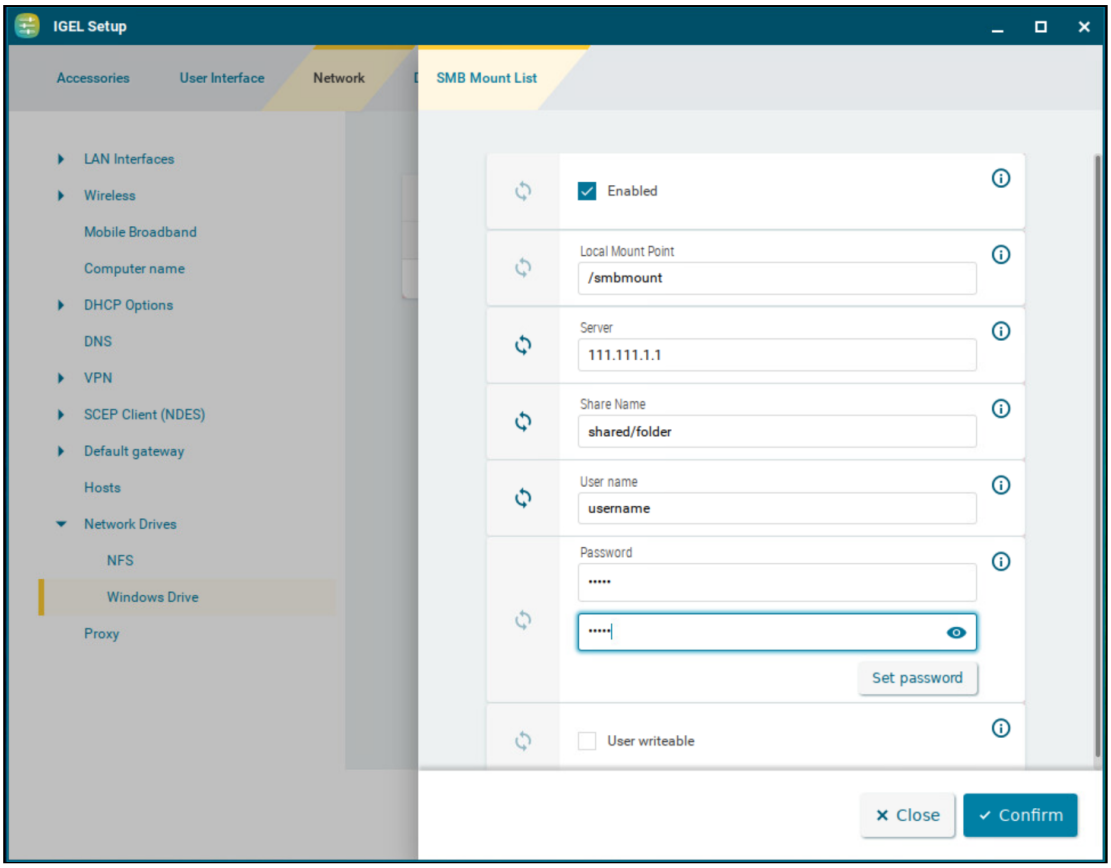
List of integrated network drives shared through SMB

To manage the list of drives, proceed as follows:

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

- Click to copy the selected entry.

Clicking + brings up the **Add** dialogue, where you can define the following settings:



Enabled

☑ The network drive will be integrated. (Default)

Local mount point

The local directory under which the server directory is to be visible. (Default: `/smbmount`)

> For **Local mount point**, only `/` (Linux/Unix-style forward slash) can be used as a path separator. Note that if you enter, for example, `\smbmount` as a moint point, a directory called `\smbmount` will be created, because `\` is a legal character in Linux directory names. For **Share name**, however, `/` (Linux/Unix-style forward slash) or `\` (Windows-style backward slash) can be used as a path separator.

Server

The IP address, Fully-Qualified Domain Name (FQDN) or NetBIOS name of the server

> If a NetBios name is provided for **Server**, make sure it is not preceded by slashes, e.g. `\\myComputer` (wrong) vs. `myComputer` (correct).

Share name

Path name as exported by the Windows or Unix Samba host

User name

User name for your user account on the Windows or Unix Samba host

Password

Password for your user account on the Windows or Unix Samba host

User writable

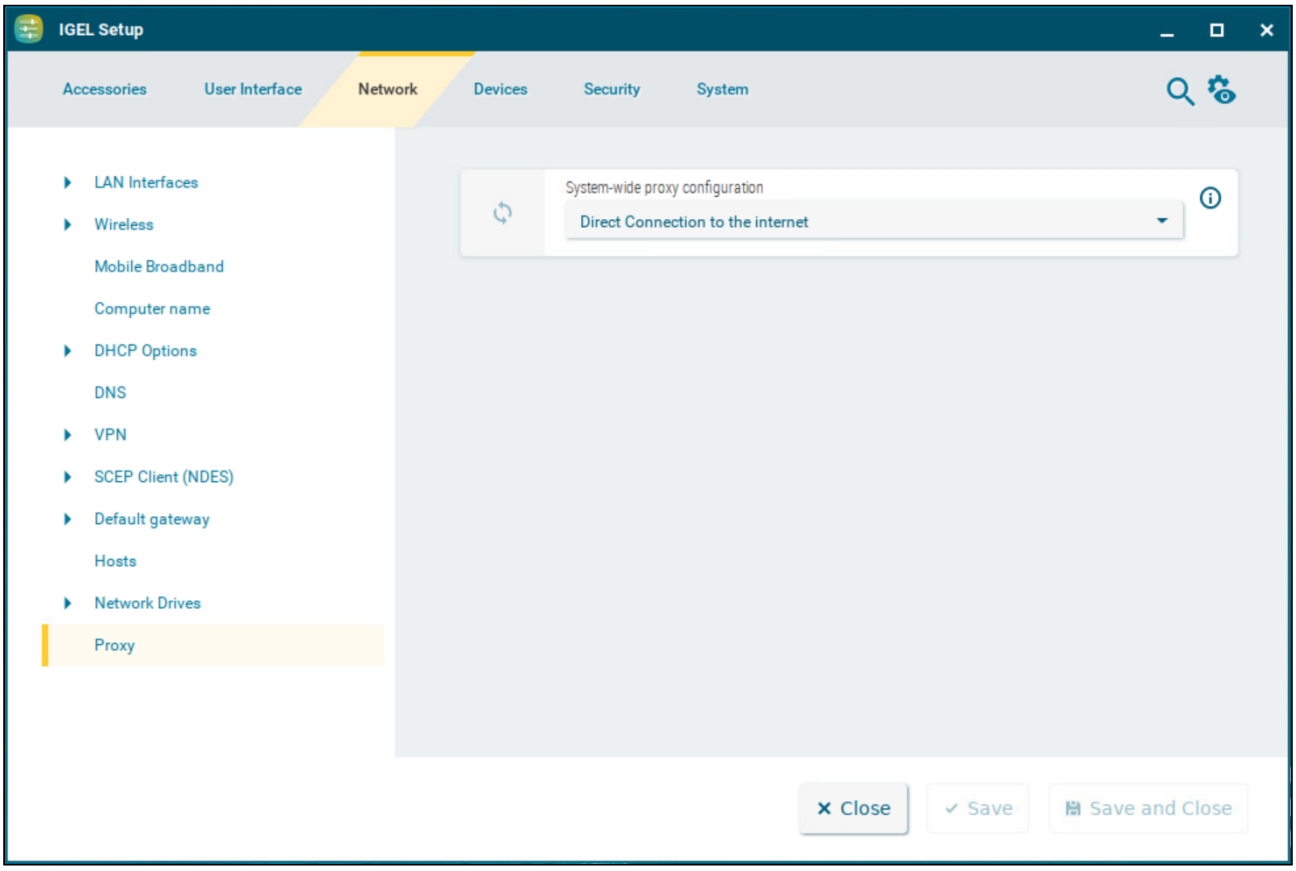
☑ The user can not only read but also write directory contents. Otherwise, only the local root user is able to do this.

☐ The user can only read directory contents. (Default)

Proxy

This article shows how to select the communication protocols for which a system-wide proxy server is to be used in IGEL OS.

Menu path: **Network > Proxy**



System-wide proxy configuration

Possible options:

- **Direct connection to the Internet**

  The endpoint device is directly connected to the Internet. No proxy is used. (Default)

- **Manual proxy configuration**

  You can configure one or more proxies in the fields from **FTP proxy** up to **SOCKS protocol version**, see Manual Proxy (see page 206).

- **Automatic proxy configuration**

  The proxy settings are dynamically retrieved via a PAC file (Proxy Auto Config) that you specify under **URL**, see Automatic Proxy (see page 207). For more information on PAC, see e.g. https://en.wikipedia.org/wiki/Proxy_auto-config.

Manual Proxy Configuration

FTP proxy / **Port**

FTP proxy server and port

HTTP proxy / **Port**

HTTP proxy server and port

SSL proxy / **Port**

SSL proxy server and port

SOCKS host / **Port**

Socks proxy server and port

SOCKS protocol version

Selects the SOCKS protocol version. (Default: SOCKS v5)

No proxy for

List of computers to which the endpoint device is to connect directly, separated by commas.
(Default: localhost,127.0.0.1)

Proxy realm for browser

Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

Use passthrough authentication

☑ The temporarily saved login information (user name and password) will be used to log in to the proxy server.

☐ The login information entered under **User name** and **Password** will be used to log in to the proxy server. (Default)

User name

User name for the proxy login

Password

Password for the proxy login

Enable client-side NTLM authenticating proxy

☑ Client-side proxy is enabled. It stands between the application and the corporate proxy, adding NTLM authentication at the corporate proxy. The credentials specified on this Setup page are used. (Default)

Listening port

Port for client-side proxy

Automatic Proxy Configuration

URL

URL of the PAC file for automatic proxy configuration

No Proxy for

List of computers to which the endpoint device is to connect directly, separated by commas.
(Default: localhost,127.0.0.1)

Proxy realm for browser

Area in which the browser authenticates itself for the proxy. Together with the user name and password, this information is necessary for authentication.

Use passthrough authentication

☑ The temporarily saved login information (user name and password) will be used to log in to the proxy server.

☐ The login information entered under **User name** and **Password** will be used to log in to the proxy server. (Default)

User name

User name for the proxy login

Password

Password for the proxy login

Devices

In this chapter, you find information on the configuration of devices in IGEL OS.

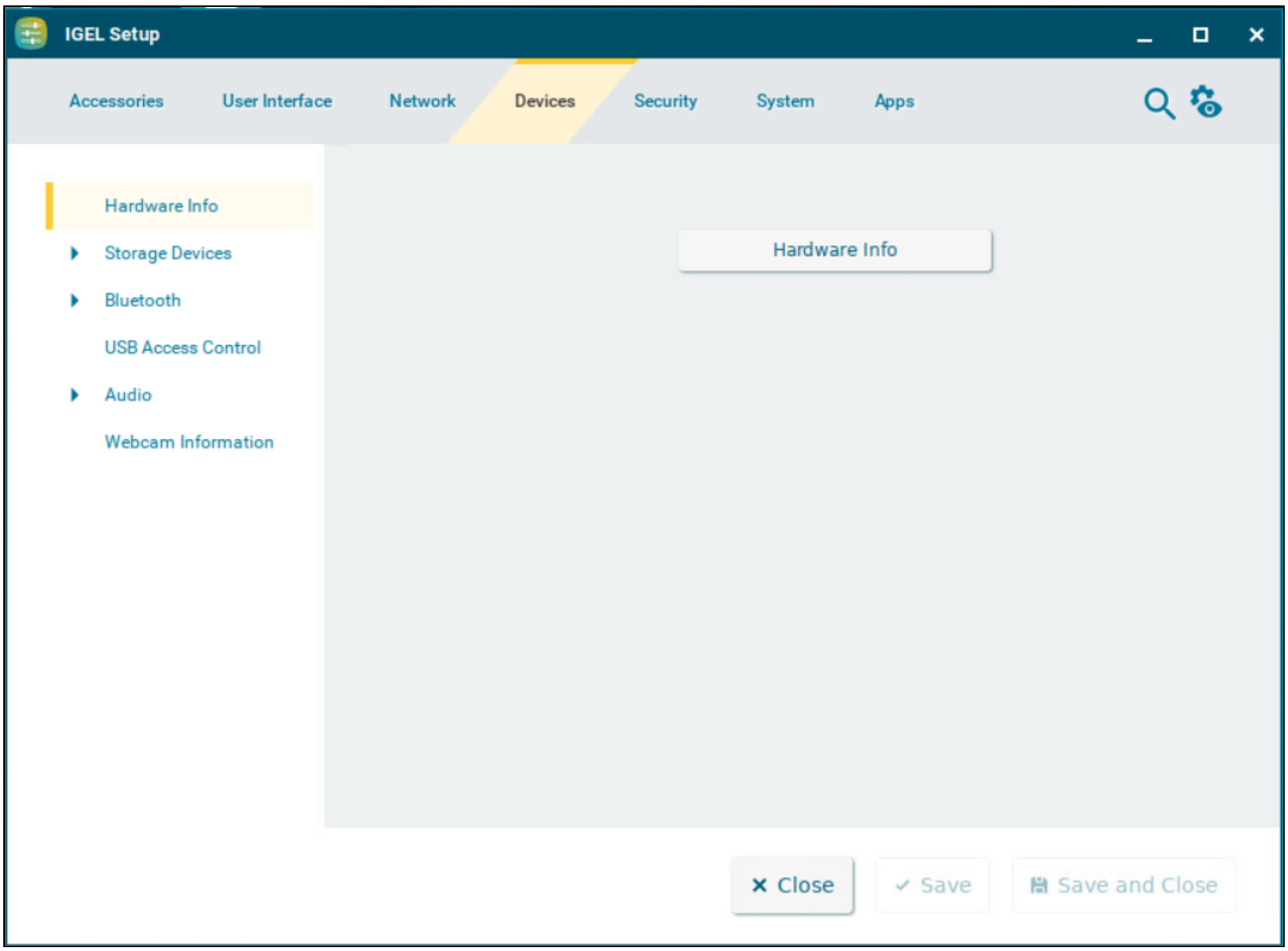
- Hardware Info (see page 209)
- Storage Devices (see page 211)
- Bluetooth (see page 223)
- USB Access Control (see page 230)
- Audio in IGEL OS 12 (see page 235)
- Webcam Information (see page 238)

Hardware Info

The **Hardware info** button provides quick access to information about the endpoint device and the connected devices.

> The page is only available locally on the device in the IGEL Setup. In order to access the page from the UMS, you need to shadow the device. For detailed information on shadowing, see Shadow (see page 287) and Shadowing - Observe IGEL OS Desktop via VNC.

Menu path: **Devices > Hardware Info**



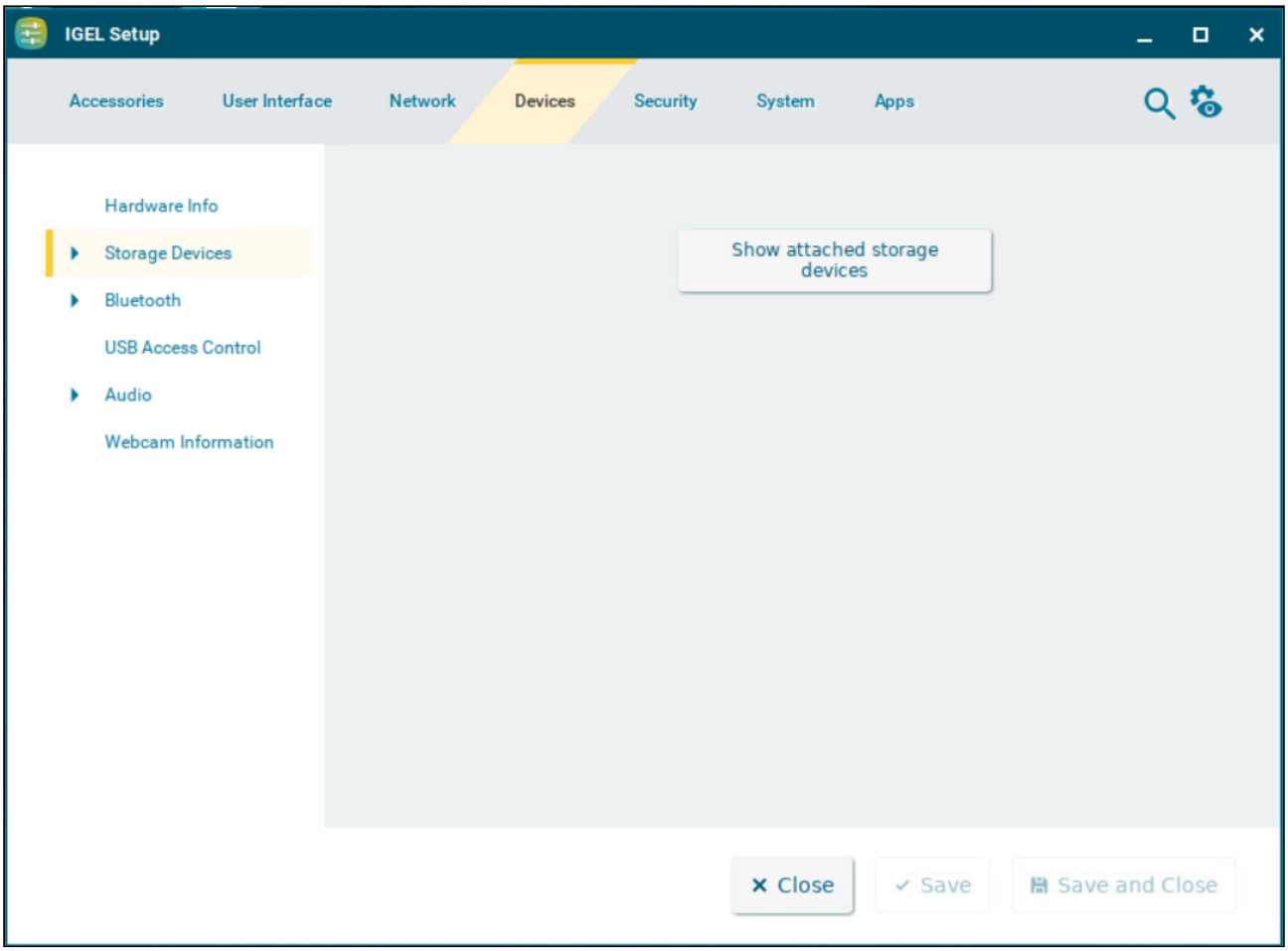
▶ Click **Hardware info** to view information on the used hardware in the **System Information** dialog.
For more information on the dialog, see System Information (see page 32).

Storage Devices

The **Show attached storage devices** button provides quick access to information about registered storage devices.

> The page is only available locally on the device in the IGEL Setup. In order to access the page from the UMS, you need to shadow the device. For detailed information on shadowing, see Shadow (see page 287) and Shadowing - Observe IGEL OS Desktop via VNC.

Menu path: **Devices > Storage Devices**



▶ Click **Show attached storage devices** to view a list of registered storage devices in the **Disk Utility** dialog. For more information on the dialog, see Disk Utility (see page 218).

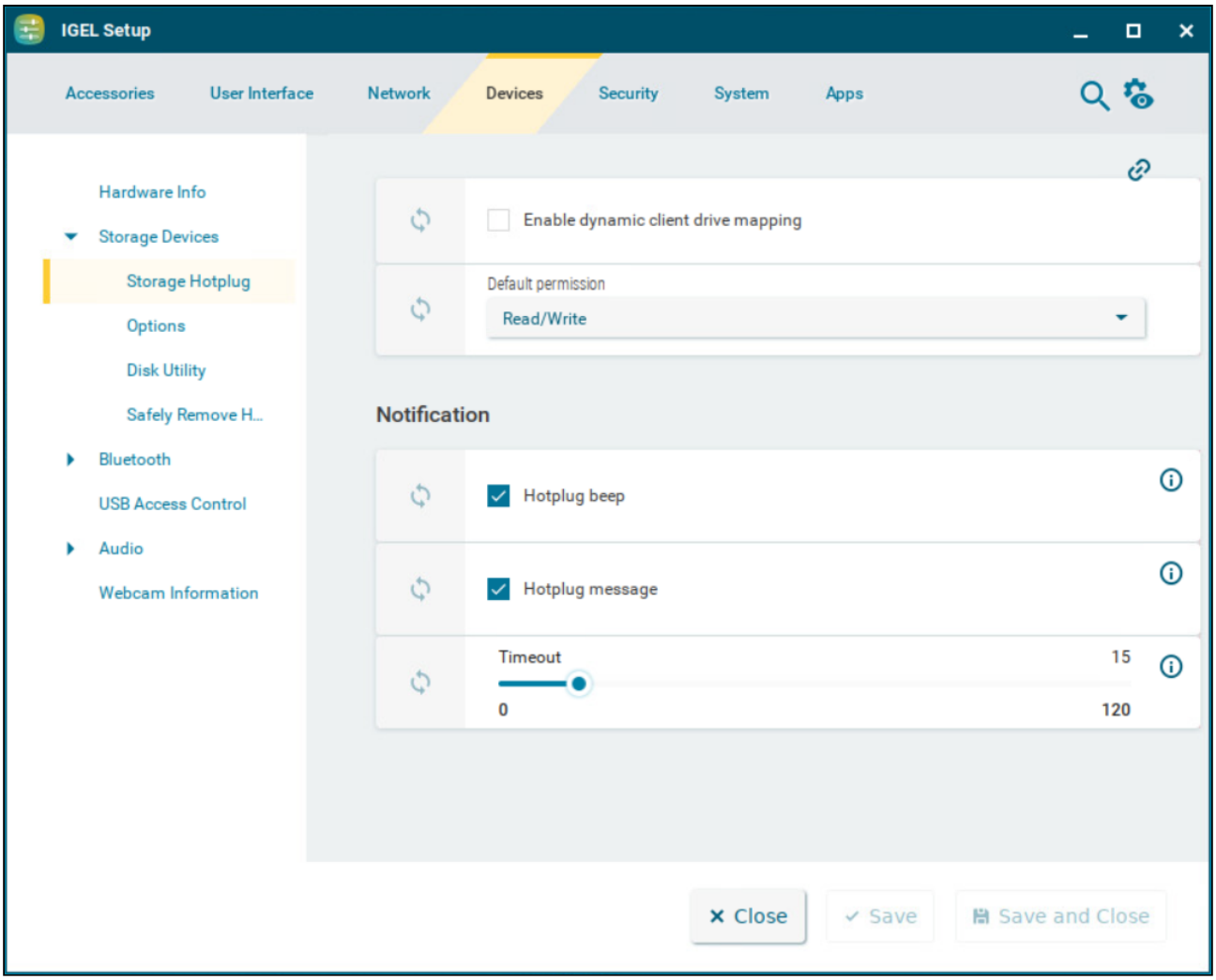
- Storage Hotplug (see page 213)
- Options (see page 216)
- Disk Utility (see page 218)
- Safely Remove Hardware (see page 221)

Storage Hotplug

This article shows how to set up the connection of hotplug storage devices to the device in IGEL OS. These can be, for example, USB mass storage devices or MMC card readers.

> For related settings options of the Citrix Workspace App, see Configuration of the Citrix Workspace App on IGEL OS.
> For related settings in the Devices area, see USB Access Control (see page 230) and Safely Remove Hardware (see page 221).

Menu path: **Devices > Storage Devices > Storage Hotplug**



The following file systems are officially supported:

ext2, ext3, ext4	Standard Linux file systems
squashfs	a packed read-only file system
vfat	supports all FAT variants
exFAT	supports exFAT (found on SDXC SD-cards)
ISO 9660	CDROM/DVD file systems
udf	CDROM/DVD file systems
ntfs	supported with ntfs-3g (Fuse)

Enable dynamic client drive mapping

Defines the creation of drives in ICA sessions, RDP sessions or Horizon sessions. The mounting of hotplug storage devices to the local file system is not influenced by this parameter.

☑ Drives are created automatically in a session when a hotplug storage device is connected to the device. When the device is removed, the corresponding drive is removed automatically.

☐ Drives are not created automatically in a session when a hotplug storage device is connected to the device.

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 several ways to safely remove a hotplug storage device:

- Click in the task bar. The taskbar can be made available in a full-screen session by enabling **Taskbar on top of all windows** under **User Interface > Desktop > Taskbar**. For more information, see Taskbar (see page 67).
- Click in the in-session control bar. Depending on the configuration, the in-session control bar may be available in a full-screen session. For further information, see In-Session Control Bar (see page 83).
- Use the **Safely Remove Hardware** function. The function can be configured under **Devices > Storage Devices > Safely Remove Hardware**. For more information, see Safely Remove Hardware (see page 221).

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.

Default permission

Default access rights for hotplug storage devices.
Possible values:

- **Read only**
- **Read/Write** (Default)

Notification

Hotplug beep

☑ A signal tone will be heard when connecting and disconnecting hotplug storage devices. (Default)

Hotplug message

☑ Hotplug messages will be shown when connecting and disconnecting hotplug storage devices. (Default)

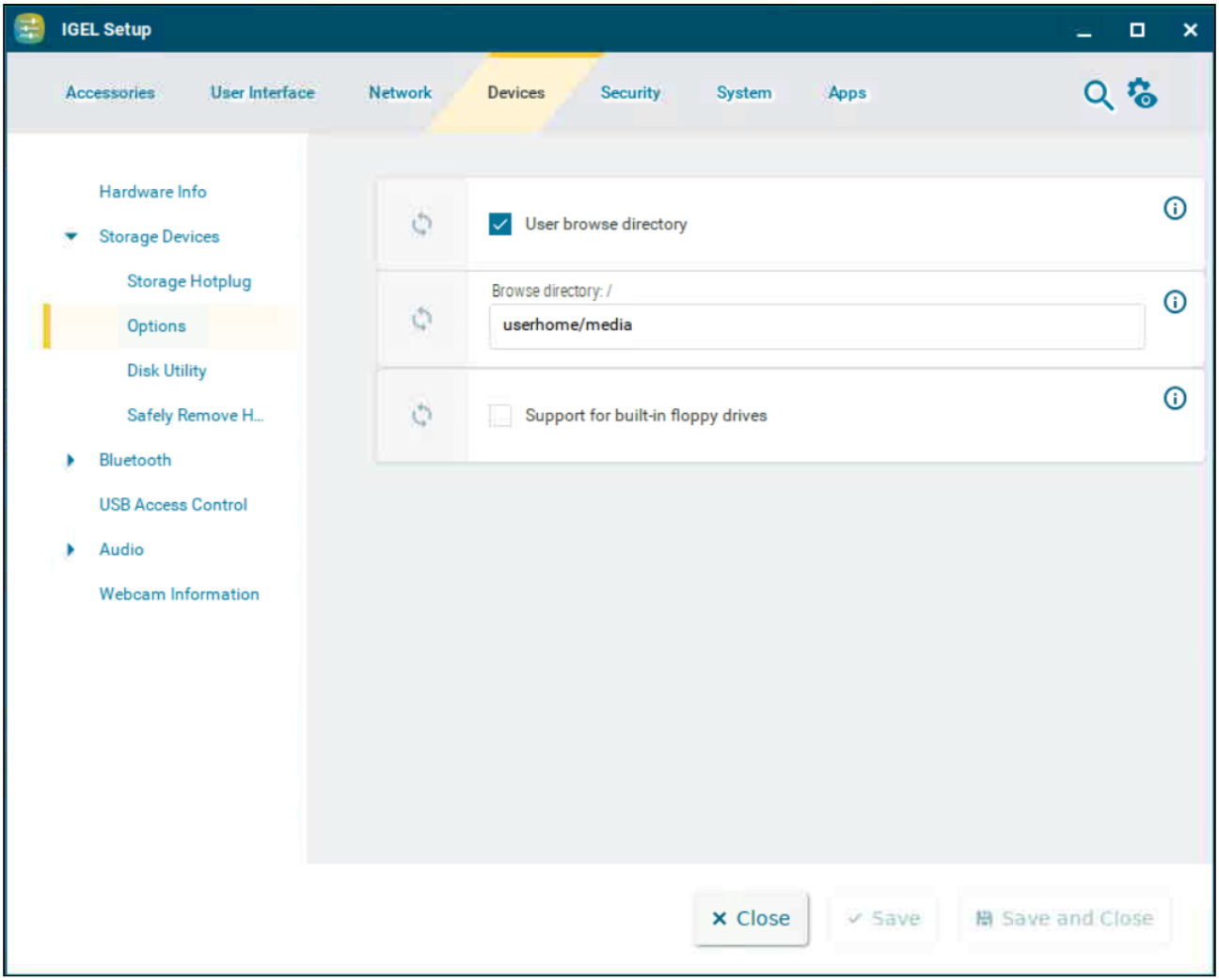
Timeout

Period of time in seconds after which the window with the hotplug messages is hidden. If the parameter is set to **No timeout**, the window will be shown until it is closed manually. (Default: 15)

Options

This article shows how to specify a directory in which external storage devices are accessible to the user in IGEL OS. The devices are always mounted in the `/media` directory.

Menu path: **Devices > Storage Devices > Options**



User browse directory

☑ The directory defined under **Browse directory: /** is linked to the `/media` directory. (Default)

Browse directory: /

Local directory in which the devices can be found. (Default: `userhome/media`)

Support for built-in floppy drives

☑ Built-in disk drives are active.

☐ Built-in disk drives are disabled. (Default)

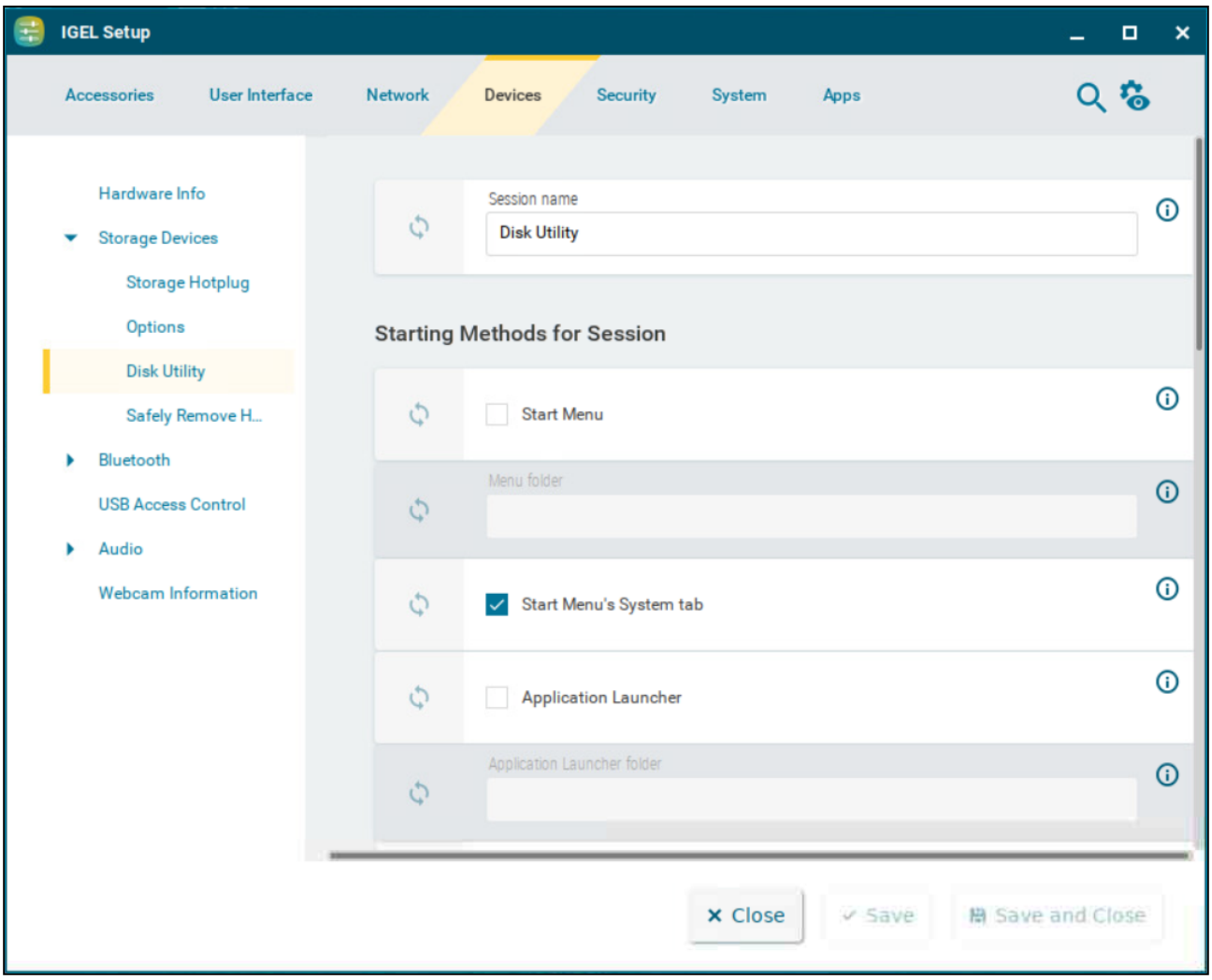
> This option is only valid for drives which are not connected via USB.

Disk Utility

With the Disk Utility function, you can obtain information regarding the hotplug storage devices connected to your endpoint device in IGEL OS. You can also use the function to safely remove hotplug storage devices.

> The Disk Utility function can only be started if the automatic mounting of hotplug storage devices is enabled through the **Enable dynamic client drive mapping** option under **Devices > Storage Devices > Storage Hotplug**.

Menu path: **Devices > Storage Devices > Disk Utility**

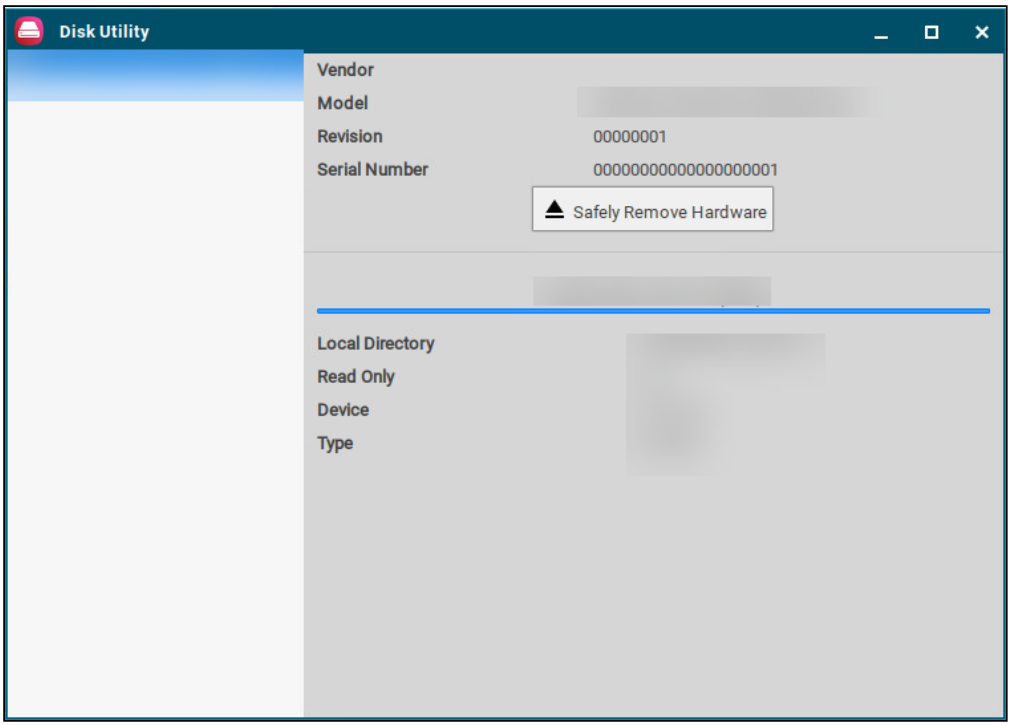


The starting methods parameters are described under Starting Methods for Apps (see page 376).

> If the **Disk utility in eject menu** option is enabled under **Devices > Storage Devices > Safely Remove Hardware**, the Disk Utility can also be started from the context menu of the eject icon in the taskbar.

Using Disk Utility

▶ Start **Disk Utility**.



To obtain information regarding a hotplug storage device connected to your endpoint device:

▶ Select the hotplug storage device in the left-hand column.
The information regarding the hotplug storage device is shown in the right-hand column.

To remove a hotplug storage device safely:

▶ Click **Safely Remove Hardware** in the right-hand column.
The hotplug storage device is disconnected from the endpoint device. Once it has been disconnected, the storage device can be removed from the device.

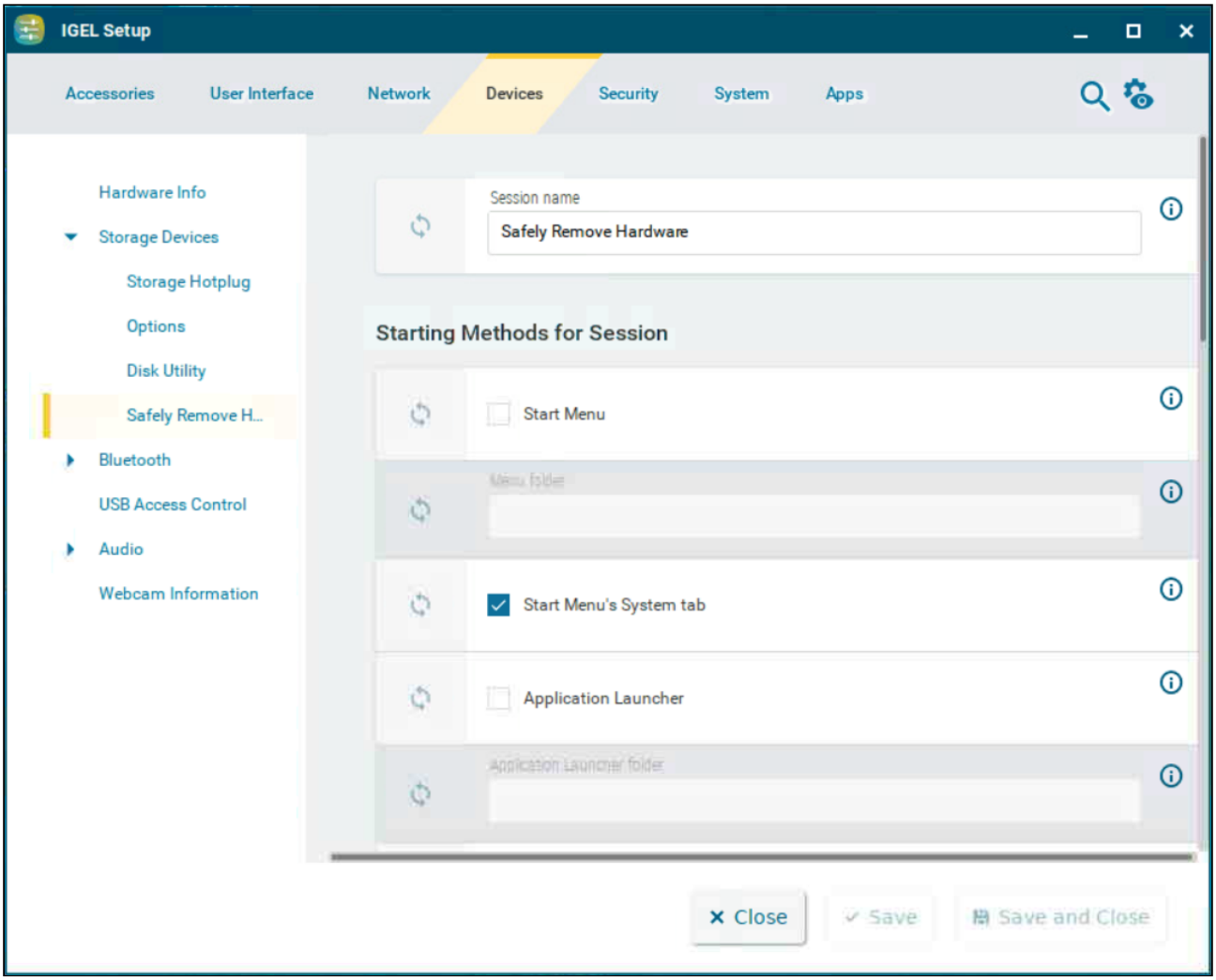
> If the **Hotplug beep** option is enabled under **Devices > Storage Devices > Storage Hotplug**, a signal tone will signal that the device has been disconnected successfully.

If the **Hotplug message** option is enabled under **Devices > Storage Devices > Storage Hotplug**, a message window will signal that the device has been disconnected successfully.
For more information, see Storage Hotplug (see page 213).

Safely Remove Hardware

With the Safely Remove Hardware function, you can remove a hotplug storage device connected to your endpoint device safely, without the risk of losing data. This article shows how to configure the starting methods for the function in IGEL OS.

Menu path: **Devices > Storage Devices > Safely Remove Hardware**



The starting methods parameters are described under Starting Methods for Apps (see page 376).

Disk utility in eject menu

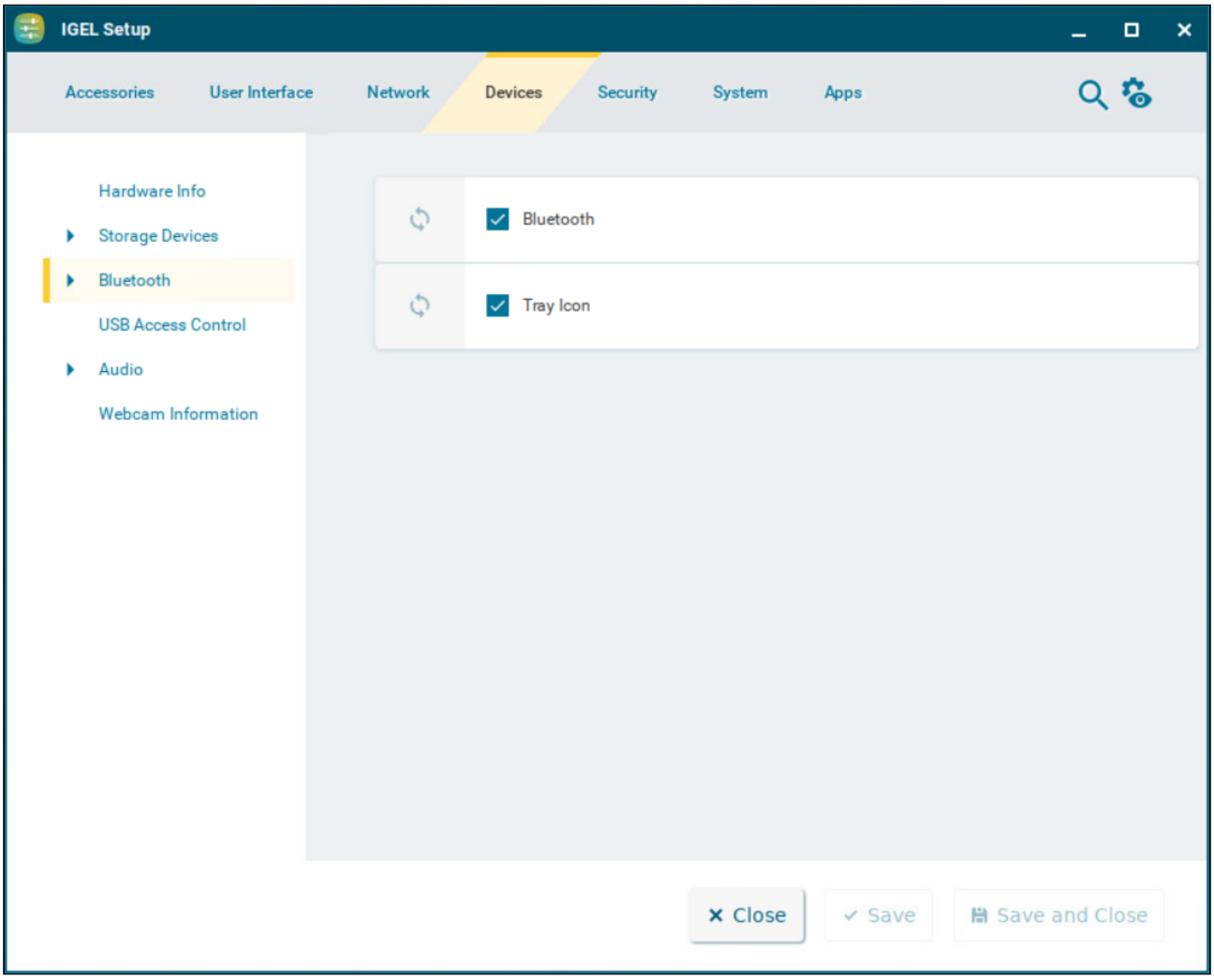
☑ The **Disk Utility** can be started from the context menu of the eject icon in the taskbar. (Default)

To start the function, click on and select **Disk Utility**. For more information on using the function, see Disk Utility (see page 218).

Bluetooth

This article shows how to set up a Bluetooth service in IGEL OS. For details on the settings options for Bluetooth devices, see Bluetooth Tool (see page 225).

Menu path: **Devices > Bluetooth**



Bluetooth

☑ The Bluetooth service is active. The **Bluetooth Tool** can be used. (Default)

Tray icon

☑ A Bluetooth icon will be shown in the system tray. You can launch the **Bluetooth Tool** by double-clicking on the Bluetooth icon. Right-clicking on the Bluetooth icon will bring up an overview as to which Bluetooth devices are connected to the endpoint device and you can enable or disable Bluetooth. (Default)

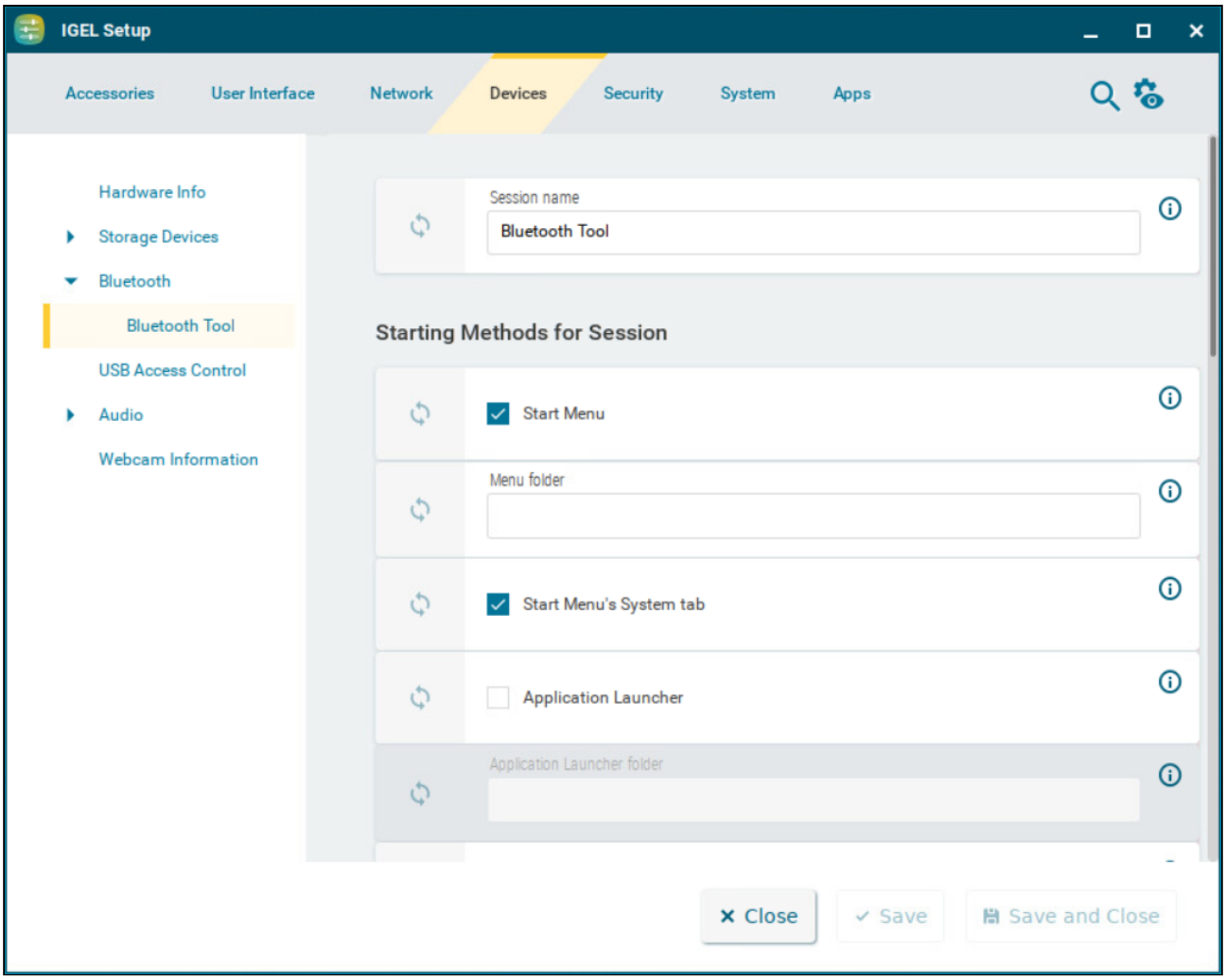
Bluetooth Tool

With the **Bluetooth Tool**, you can connect Bluetooth devices, e.g. a keyboard, a mouse, or a headset, to your endpoint device in IGEL OS.

> In order to be able to use Bluetooth, it must be enabled under **Devices > Bluetooth**.

> If your endpoint device does not support Bluetooth, it is necessary to connect a Bluetooth USB adapter to it.

Menu path: **Devices > Bluetooth > Bluetooth Tool**



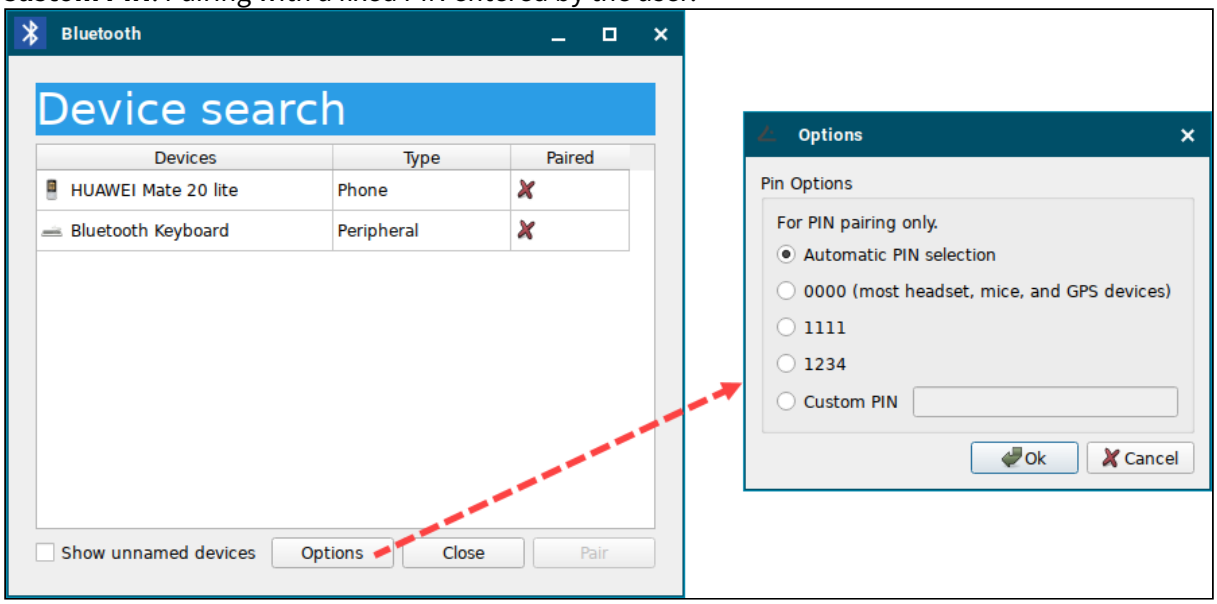
The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using Bluetooth Tool

The **Bluetooth Tool** supports the following coupling methods, i.e. the mutual authentication of the Bluetooth device and endpoint device:

- **Automatic PIN selection**: Pairing with automatic PIN allocation
- **0000**, **1111**, **1234**: Pairing with a fixed PIN (for most headsets, mice, or GPS devices)

- **Custom PIN**: Pairing with a fixed PIN entered by the user.



In addition, Bluetooth devices that do not require pairing are also supported.

Connecting a Bluetooth Device with Automatic PIN Selection

1. Ensure that the coupling mode is enabled on the Bluetooth device.
2. Start the **Bluetooth Tool**.
   The **Device search** dialog will be shown.
3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
   After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.
4. Select the desired Bluetooth device.
5. Under **Options**, enable **Automatic PIN selection**.
6. Click **Pair**.
7. A PIN will be shown in the dialog on your endpoint device.
   - If the PIN is identical to the PIN shown on your Bluetooth device, confirm the coupling.
   - If a Bluetooth device requires the manual entering of a PIN (e.g. keyboard), type in the PIN shown in the dialog.
     In a few seconds, the status of the connection will be shown.

Connecting a Bluetooth Device with a Fixed PIN

1. Ensure that the coupling mode is enabled on the Bluetooth device.

2. Start the **Bluetooth Tool**.
   The **Device search** dialog will be shown.

3. Enable **Show unnamed devices** if you want to include unnamed Bluetooth devices in the search list.
   After a few seconds, the Bluetooth devices found by the endpoint device will be displayed.

4. Select the desired Bluetooth device.

5. Under **Options**, select one of the specified PINs or enable **Custom PIN** and enter the PIN for the Bluetooth device. You will find this PIN in the documentation for your Bluetooth device.

6. Click **Pair**.
   In a few seconds, the status of the connection will be shown.

Canceling Coupling to a Bluetooth Device

1. Start the **Bluetooth Tool**.
   The connected Bluetooth device will be shown in the **Device search** dialog.

2. Highlight the connected Bluetooth device and click **Unpair**.
   The status of the connection will be shown.

Enabling Support for Devices That Do Not Require Coupling

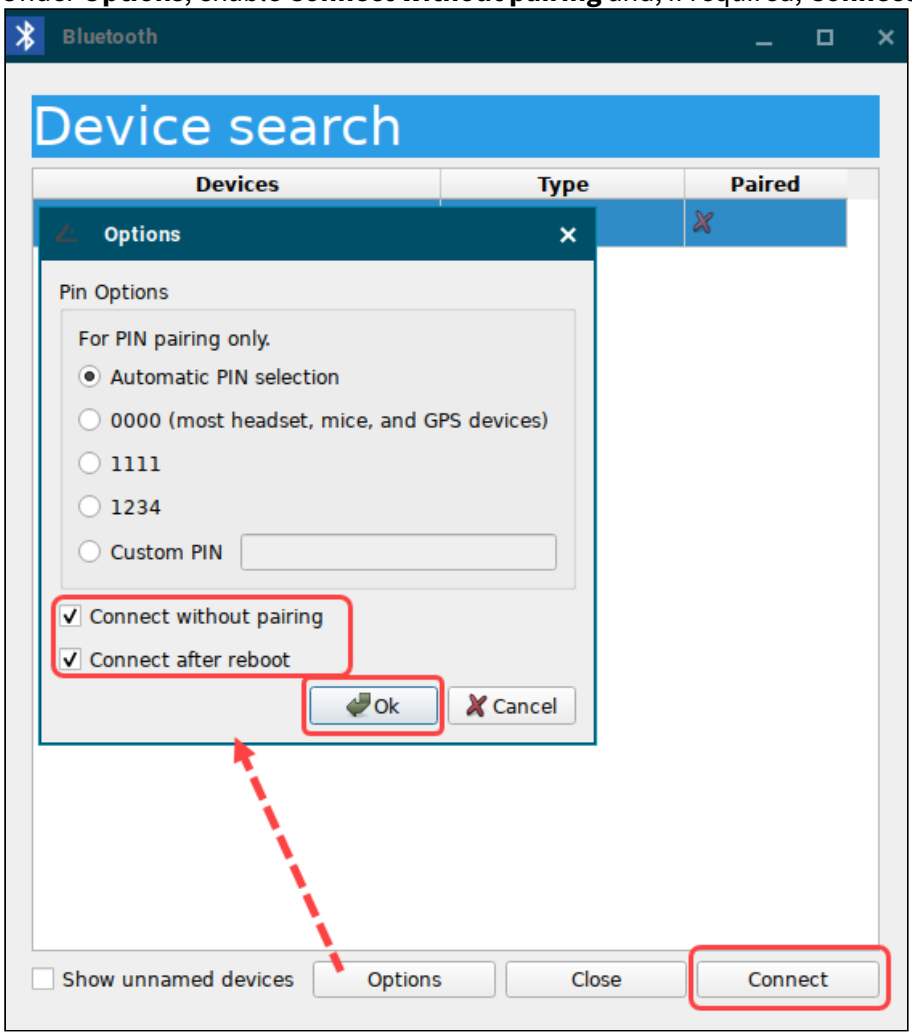
1. In the Setup or the configuration dialog of the UMS, go to **System > Registry > devices > bluetooth > connect_only** and activate **Connect devices without pairing** (registry key: `devices.bluetooth.connect_only`).

2. Save the changes.

3. Start the **Bluetooth Tool**.
   The **Device search** dialog will be shown.

4. Highlight the desired Bluetooth device.

5. Under **Options**, enable **Connect without pairing** and, if required, **Connect after reboot**.



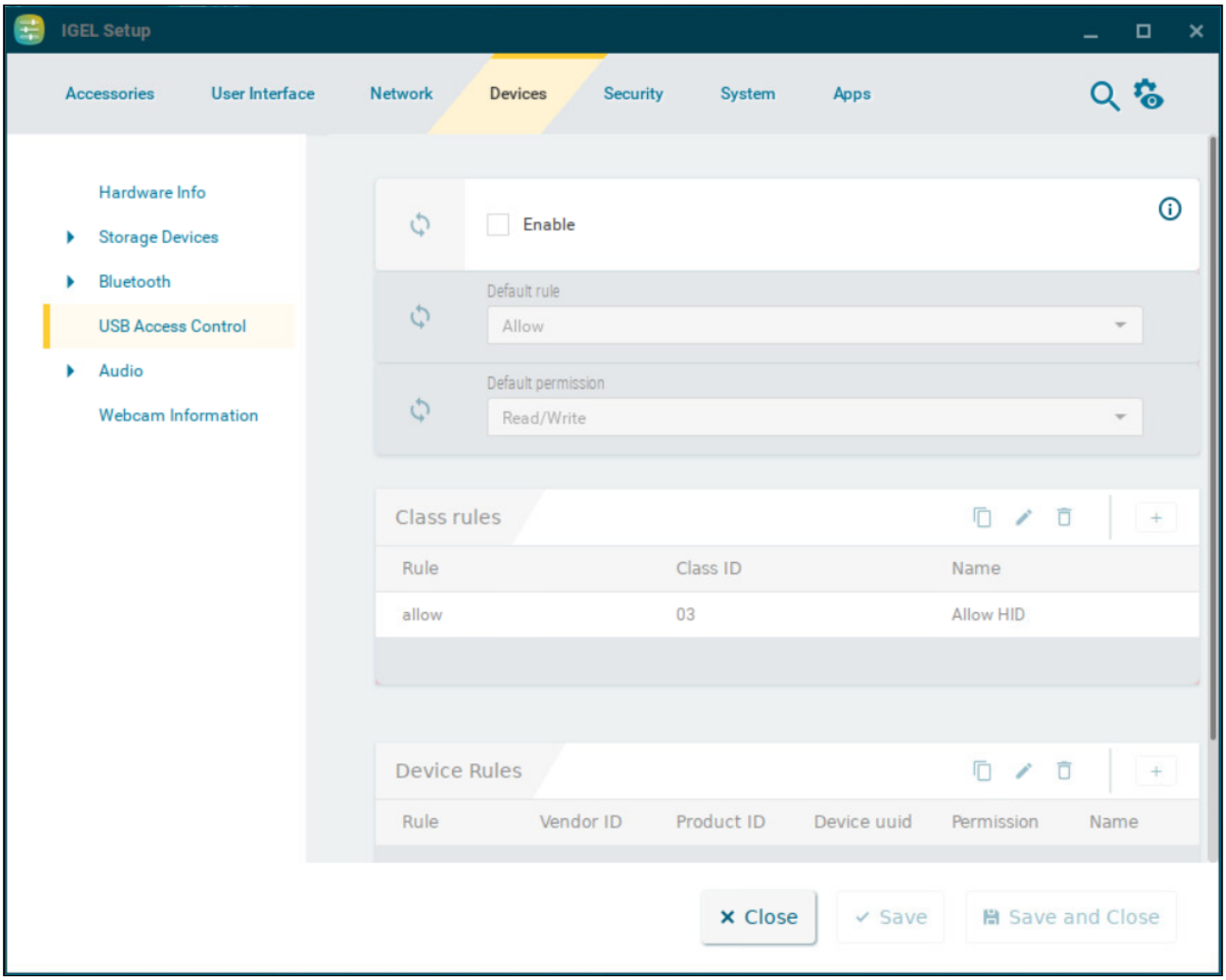
6. Click **Connect**.

> Some devices do not connect automatically after the reboot. To fix that, you can use the following command in a script:
> `bluetoothctl connect <device-ID>`
> The return value tells you if the device is connected (0) or not (1).

USB Access Control

This article shows how to control USB access to the endpoint device in IGEL OS. You can allow or prohibit the use of USB devices on your endpoint. Specific rules for individual devices or device classes are possible.

Menu path: **Devices > USB Access Control**



Enable

☑ USB access control is enabled and the following settings can be configured.

☐ USB access control is inactive. (Default)

⚠ The activation of **USB Access Control** and setting the **Default rule** to **Deny** will block the use of USB devices locally and in the session and, thus, might disable devices needed for the users. Therefore, activate the USB access control only if your security policy requires that. In this case, set **Default rule** to **Deny** and configure **Allow** rules for the required USB devices and USB device classes.
It is recommended to make settings for **USB Access Control** as the last step in the device configuration. Before activating the USB access control, check that all your other settings for printers, Unified Communication, USB redirections, mapping settings for USB devices are working as expected.
Note that the USB access control is completely separate than USB redirection for remote sessions.
Take also notice that the feature does not disable a USB port physically, i.e. power delivery will still work.

Default rule

Specifies whether the use of USB devices is allowed or prohibited.

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

Default permission

Default access rights for USB devices.

- **Read Only**
- **Read/Write** (Default)

Class Rules

Class rules apply to USB device classes. To manage the list of class rules:

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

Clicking brings up the **Add** dialogue, where you can define the following settings:

- **Rule**

  Specifies whether the use of the device class defined here is allowed or prohibited.

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

- **Class ID**

  Device class for which the rule should apply. (Examples: **Audio**, **Printers**, **Mass Storage**).

- **Name**

  Name of the rule

Device Rules

Device rules apply to specific USB devices. To manage the list of device rules:

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

Clicking brings up the **Add** dialogue, where you can define the following settings:

- **Rule**

  Specifies whether the use of the device defined here is allowed or prohibited.

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

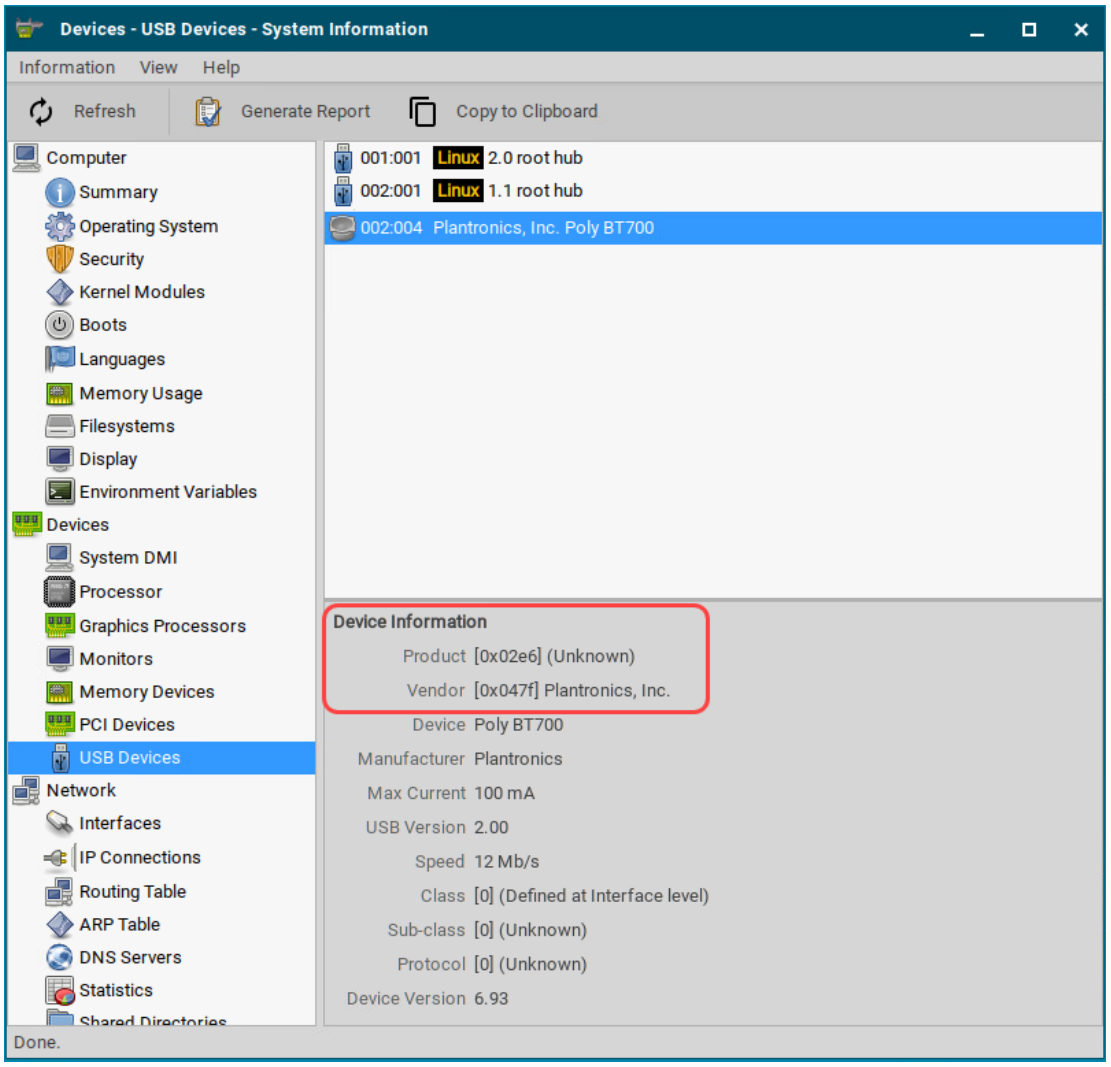
- **Vendor ID**

  Hexadecimal ID of the device manufacturer

- **Product ID**

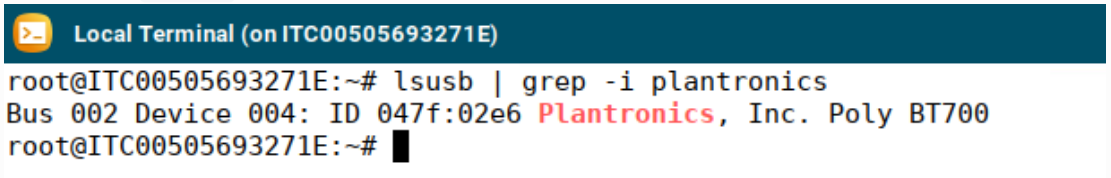
  Hexadecimal ID of the device

> **Getting USB Device Information**
>
> To find out the **Class ID**, **Subclass ID**, **Vendor ID** and **Product ID** of the connected USB device, you can use the **System Information** tool. For further information, see System Information (see page 32).
> System Information example:



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

Example for `lsusb`:



- **Device UUID**

Universal Unique Identifier (UUID) of the device

- **Permission**

Authorizations for access to the device
Possible values:

- **Global setting**: The default setting for hotplug storage devices is used; see the **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**. For more information, see Storage Hotplug (see page 213).
- **Read only**
- **Read/Write**

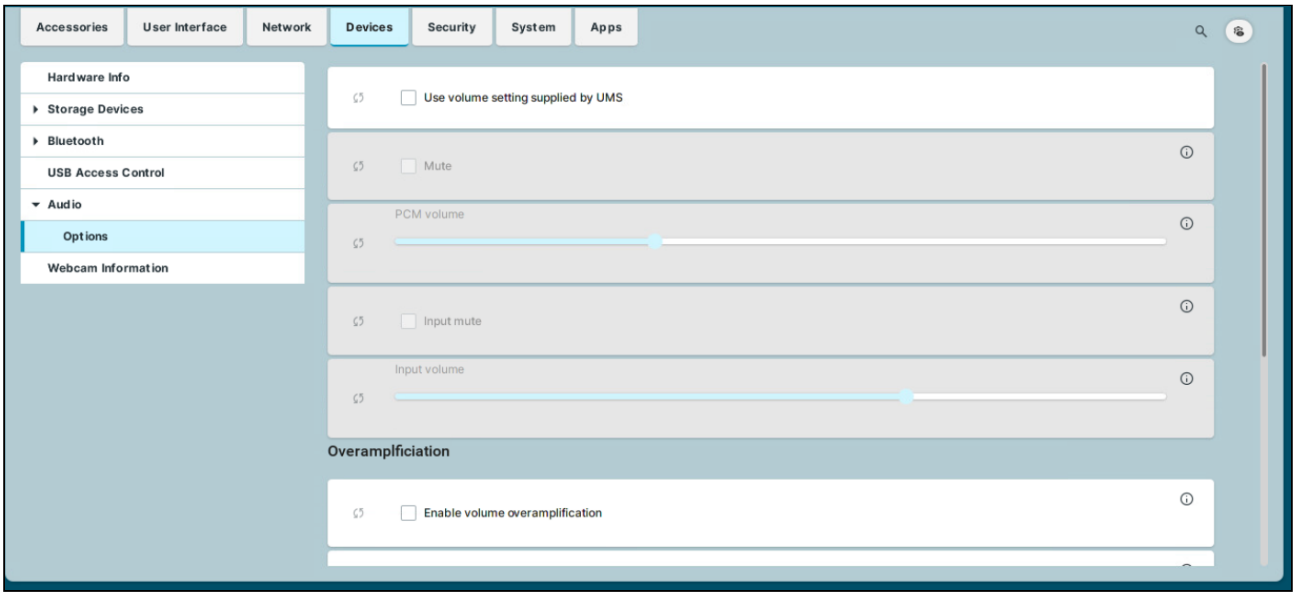
- **Name**

Name of the rule

Audio in IGEL OS 12

This article shows how to configure presets for the audio system in IGEL OS. The settings can also be changed using the Sound Tray App. For details, see Tray Applications in IGEL OS 12 (see page 353).

Menu path: **Devices > Audio > Options**



Use volume setting supplied by UMS

☑ The settings for the below parameters **Mute**, **PCM volume**, **Input mute**, and **Input volume** are restored after each system restart. The settings set in **Sound Preferences** or in the taskbar will only remain until system restart.

☐ The settings set in **Sound Preferences** or in the taskbar will be restored after system restart. (Default)

Mute

☑ Audio playback is muted.

☐ Audio playback is on. (Default)

PCM volume

Preset volume in percent. (Default: 50)

Input mute

☑ The audio input is muted. Sounds from a microphone that are recorded are not transferred to the endpoint device.

☐ The audio input is switched on. Sounds from a microphone that are recorded can be transferred to the endpoint device. (Default)

Input volume

Volume of recorded sounds at the audio input device in percent. (Default: 100)

Overamplification

Enable volume overamplification

☑ Allows to set the volume up to 150%.

☐ The volume cannot be overamplified. (Default)

Enable input volume overamplification

☑ Allows to set the input volume up to 150%.

☐ The input volume cannot be overamplified. (Default)

Default Sound Output

Default audio output

Name of the output port
Possible options:

- **Automatic**: The audio output is automatically assigned to a device. Not connected ports will be ignored. The following order applies here:
  1. USB devices
  2. PCI devices; this also includes the HDMI interface.
  3. Internal speaker
- **HDMI / DisplayPort**
- **Speakers**
- **Headphones**

Default Sound Input

Default audio input

Name of the input port
Possible options:

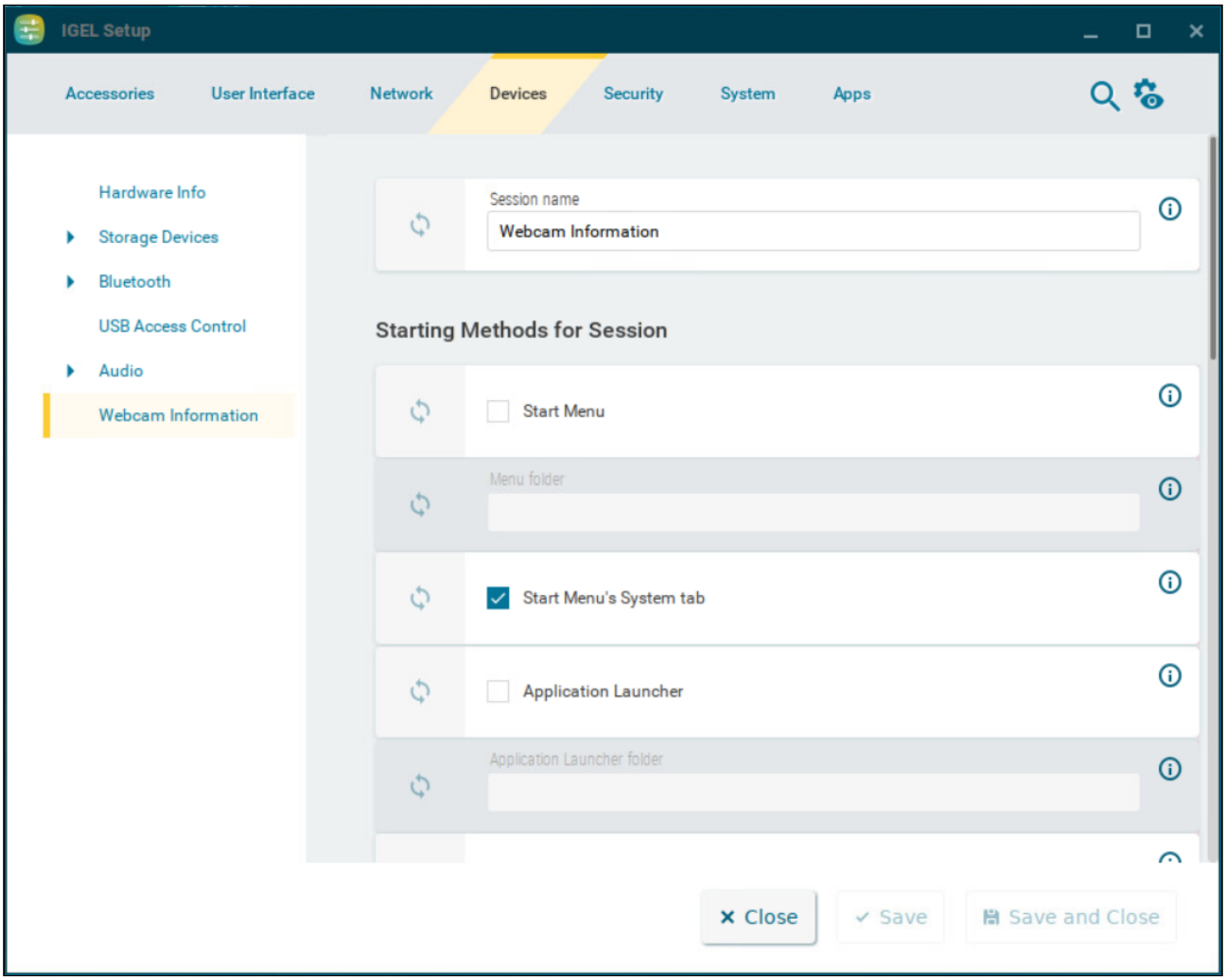
- **Automatic**: The audio input is automatically assigned to a device. Not connected ports will be ignored. The following order applies here:
  1. USB devices
  2. PCI devices

- **Microphone**
- **Headset microphone**

Webcam Information

With the Webcam Information function, you can check and change the settings for a connected webcam in IGEL OS. You can configure the width, height and frame rate values for the connected webcam.

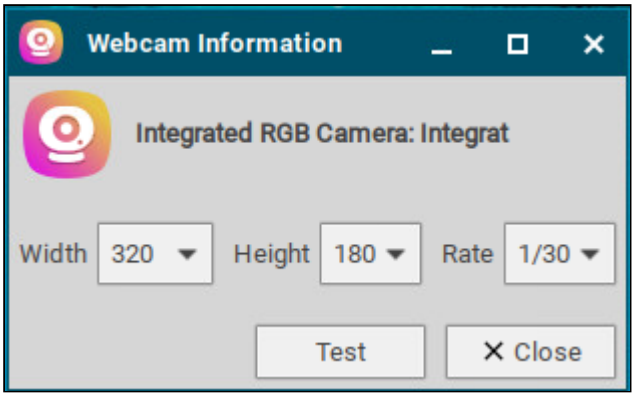
Menu path: **Devices > Webcam Information**



The starting methods parameters are described under Starting Methods for Apps (see page 376).

Using Webcam Information

To determine and change the values for width, height and frame rate, proceed as follows:



1. Start the **Webcam Information** function.
2. The following values will be shown:
   - **Width**: Width of the image in pixels
   - **Height**: Height of the image in pixels
   - **Rate**: Frame rate in fps (frames per second: individual images per second).
     Example: **1/30** means 30 individual images per second.
3. Click on one of the fields to change the value. The supported values will be shown in the process.
4. Click **Test**.
   The video image generated by the webcam with the current settings will be shown.

In order to check whether the webcam is functioning in a session (e.g. redirected via Citrix HDX Webcam Redirection), open https://www.onlinemictest.com/webcam-test/ in your browser within the session.

Alternatively, you can determine the values supported by the webcam in the local terminal with the command `webcam-info -l`.

Security

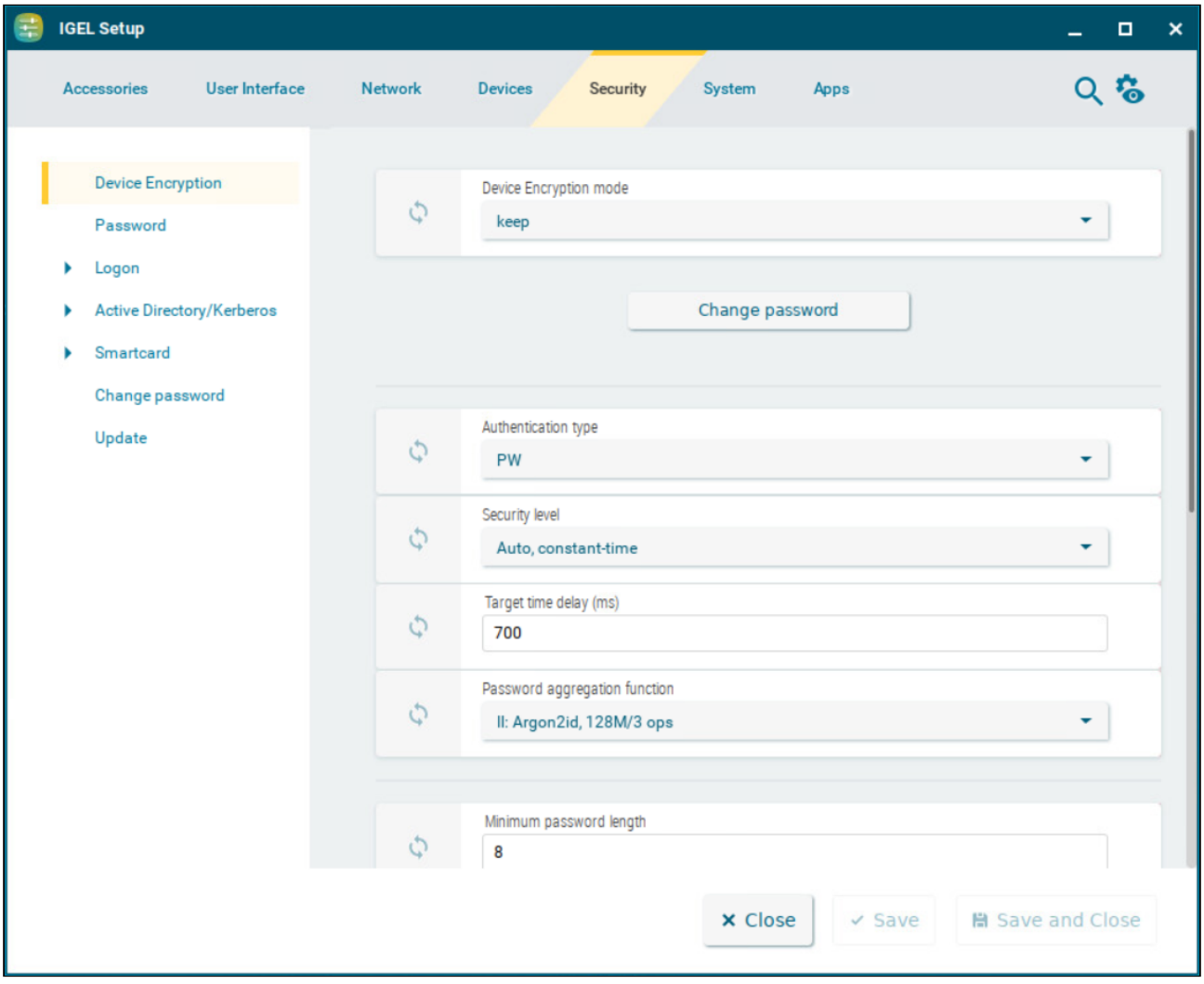
In this chapter, you find information on security configuration in IGEL OS.

- Device Encryption (see page 241)
- Password (see page 245)
- Logon (see page 250)
- Active Directory/Kerberos (see page 264)
- Smartcard Services (see page 270)
- Change Password (see page 273)
- Update (see page 275)

Device Encryption

If you want to strengthen the security of your endpoint device, you can deploy strong device encryption that is derived from a user password. The encryption is applied to all partitions that can contain user data, e.g. browser history or Custom Partitions.

Menu path: **Security > Device Encryption**



Device encryption mode

Possible options:

- **Keep**: The default encryption scheme is maintained. If a password has been set, it will remain unchanged. (Default)
- **Activate**: The device will be re-encrypted using strong encryption methods when the user enters the password for the first time. It is strongly recommended to enforce the use of a strong password; see Minimum password length (see page 243) and the subsequent password settings. The re-encryption may take about 10 to 60 seconds; the duration depends on the hardware performance and the size of the Custom Partition.
- **Deactivate**: The device will be re-encrypted back to the default device encryption scheme on the next boot. The re-encryption may take about 10 to 60 seconds.

  ⚠ If you want to switch back to the default device encryption, you must have the password. If the password gets lost, you must reinstall IGEL OS on the device, for example, using the OS Creator. For detailed instruction, see Installing the Base System via IGEL OS Creator (OSC).

Change password

Only applicable if device encryption is activated. Click the button to change the password for device encryption.

Authentication type

⚠ **Devices That Support TPM PCR**

TPM PCR is only supported by the following devices:
- HP T640
- IGEL UD 3 (M350C with Bios version V:3.D.13A-05232022 or higher)
- IGEL UD 7 (H860C with Bios version 3.6.13A-05202022 or higher)

If **TPM PCR** is selected on a device that does not support it, the authentication type falls back to **PW** (password authentication).
If **TPM PCR+PIN** is selected on a device that does not support it, the authentication type falls back to **TPM+PIN**.

Possible options:

- **PW**: Password authentication.
- **TPM+PIN**
- **TPM PCR**
- **TPM PCR+PIN**

Security level

Possible options:

- **Auto, constant-time**: The password aggregation function that fits best with the defined **Target time delay (ms)** is selected and the manual selection under **Password aggregation function** is ignored. (Default)
- **Auto, at least level**: The security level will be at least as high as the value selected by **Password aggregation function**; if the **Target time delay (ms)** allows for a higher security level, the higher security level will be used.

- **Manual**: The **Password aggregation function** can be set manually, irrespective of the delay time specified by **Target time delay (ms)**.

Target time delay (ms)

Maximum time that should be consumed by the password aggregation function. This delay is effective when the user enters the device encryption password on boot or changes the device encryption password. (Default: 700)

Password aggregation function

Security level of the encryption.
Possible options:

- **I: Argon2id, 8M/7 ops**
- **II: Argon2id, 128M/3 ops** (Default)
- **III: Argon2id, 256M/3 ops**
- **IV: Argon2id, 512M/3 ops**
- **V: Argon2id, 1024M/4 ops**
- **VI: Argon2id, 128M/4 ops**

Minimum password length

Minimum number of characters the password must be composed of. (Default: 8)

Unwanted strings in password (comma separated)

Comma-separated list of strings that must not be in the password

The password must contain

Defines how many of the subsequent minimum requirements (minimum amount of lower case letters, etc.) must be fulfilled.
Possible options:

- **All** (Default)
- **2 of**
- **3 of**

Minimum amount of lower case letters

Defines at least how many lower case letters must be in the password.

Minimum amount of upper case letters

Defines at least how many upper case letters must be in the password.

Minimum amount of numbers

Defines at least how many numbers must be in the password.

Minimum amount of special characters

Defines at least how many special characters must be in the password.

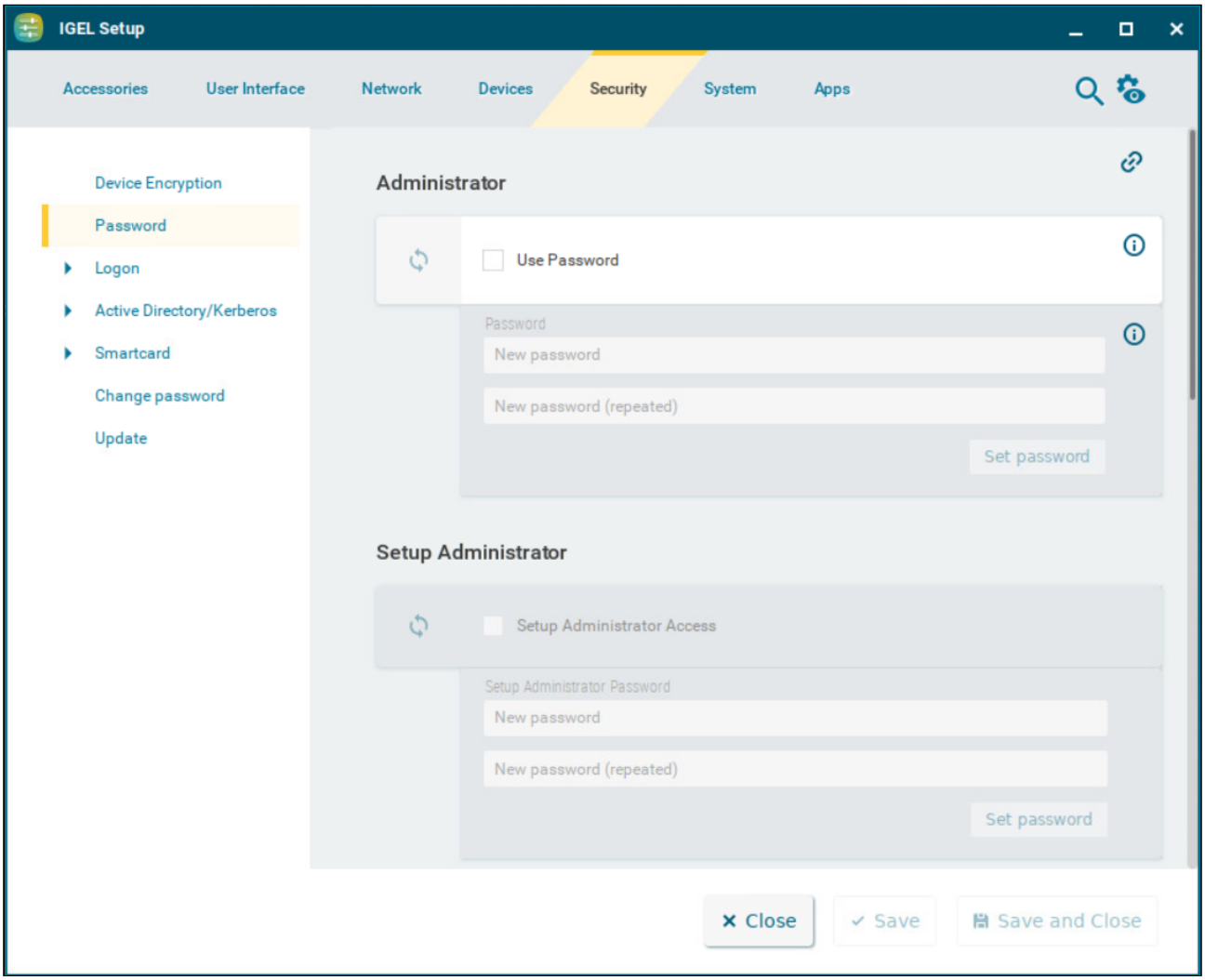
Special characters allowed

Lists all the non-alphanumerical characters without separators that are allowed in the password.

Password

The following article provides details on the user types and their roles in IGEL OS. You can configure passwords for the user types to protect your endpoint devices against unwanted changes.

Menu path: **Security > Password**



IGEL Setup Password Protection

Configure the administrator password to create the password protection for the IGEL Setup. You can also configure the setup administrator and the setup user to allow additional access to the IGEL Setup. For more information, see Setup (see page 38).

> The assignment of the administrator password is a prerequisite for all other rights assignments. Even if the administrator wants to leave the administration of the IGEL Setup to the setup administrator, the administrator password must be set.

> If you do not configure any password, the IGEL Setup can be opened without password protection.

User Rights

The user types have the following access rights:

- **Administrator**: If configured, the administrator password protects the following critical actions/areas from unauthorized access:
  - IGEL Setup
  - Reset to factory defaults boot mode. (For more information, see Boot Menu (see page 381).)
  - Accessing the local terminal as `root`. (For more information, see Terminals (see page 12).)
  - Virtual console access. (For more information, see Access Control (see page 53).)
  - sessions, for which **Administrator** is set under **Password protection**. (For more information, see Starting Methods for Apps (see page 376).)

  If configured, the administrator can access the following with a password:
  - Unlocking the screenlock. (For more information, see Options (see page 89).)
  - Secure Shell (SSH). (For more information, see SSH Access (see page 284).)

- **Setup administrator** : If configured, the setup administrator can access the following with a password:
  - IGEL Setup

- **Setup user** : If configured, the setup user can access the following with a password:
  - IGEL Setup
  - sessions, for which **Setup user** is set under **Password protection**. (For more information, see Starting Methods for Apps (see page 376).)

- **User** : If configured, the user can access the following with a password:
  - the terminal session as `user`. (For more information, see Terminals (see page 12).)
  - sessions, for which **User** is set under **Password protection**. (For more information, see Starting Methods for Apps (see page 376).)

> You can also use the **User** password for starting the screenlock: **User Interface > Screenlock / Screensaver > Starting Methods for Session > Password protection**. For details, see Screenlock / Screensaver (see page 87).
>
> However, note the following:
> The **User** is not the same as the local user configured under **Security > Logon > Local User**. For unlocking the screenlock, the local user password (not the user password) is used. For details, see Local User and Options (see page 89).

- **User account for remote access**: If configured, the `ruser` can access the device via Secure Shell (SSH). (For more information, see SSH Access (see page 284).)

Administrator

Use password

☑ Administrator password protection is enabled and further user types can be configured. The password is set by clicking **Set password**.

☐ Administrator access is granted without password protection. No password can be configured for the user (`user`), the setup user, and the setup administrator. (Default)

Change password

Click the button to set a new password.

> **Effects on local terminal access**
>
> Setting an administrator password has the following effects on the access to local terminals:
> - For logging in as `root`, the administrator password must be entered.
> - Logging in as `user` is no longer possible by default. However, you can allow access for `user` by making the following settings:
>   - Enable the registry key `system.security.usershell` (Default: Disabled).
>   - Set a user password.
>
> For logging in as `user`, the user password will have to be entered.

Setup Administrator

Setup administrator access

This option is only available if an administrator password is set.

☑ The setup administrator can access the IGEL Setup with a password. The password is set by clicking **Set password**.

☐ The setup administrator cannot access the IGEL Setup. (Default)

Change password

Click the button to set a new password.

Setup User

Setup user access

This option is only available if an administrator password is set.

☑ Setup user password protection is enabled. The password is set by clicking **Set password**.

☐ The setup user cannot access the IGEL Setup. Sessions, for which **Setup user** is set under **Password protection** will not have password protection. (Default)

Change password

Click the button to set a new password.

User

Use password

This option is only available if an administrator password is set.

☑ User password protection is enabled. The password is set by clicking **Set password**.

☐ If an administrator password is set, the user (`user`) cannot log in to the device via the local terminal. Sessions, for which **User** is set under **Password protection** will not have password protection. (Default)

Change password

Click the button to set a new password.

User Account for Remote Access

Enable login

☑ The remote user (`ruser`) can log in to the device via SSH. (Default)

☐ Logging in via SSH is not possible.

For further SSH access settings, see SSH Access (see page 284).

Use password

☑ A password is needed to log in via SSH. The password is set by clicking **Set password**.

☐ No password is needed to log in via SSH. (Default)

Change password

Click the button to set a new password.

Logon

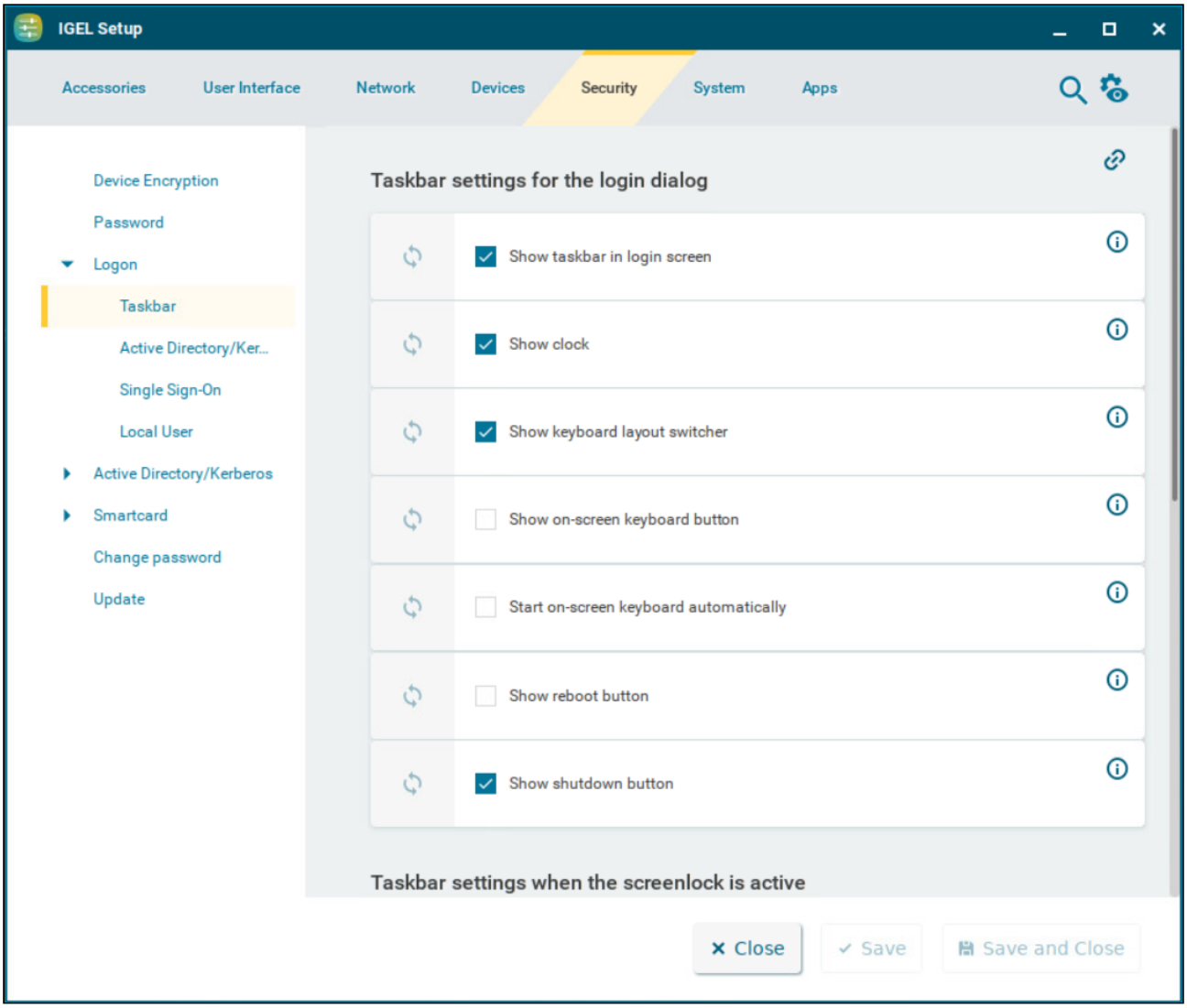
The following logon settings are available in IGEL OS.

- Taskbar (see page 251)
- Active Directory/Kerberos (see page 254)
- Single Sign-On in IGEL OS 12 (see page 256)
- Local User (see page 260)
- Guest - Passwordless Access to IGEL OS (see page 262)

Taskbar

This article shows how to configure the taskbar for the login dialog and for when the screen is locked in IGEL OS.

Menu path: **Security > Logon > Taskbar**



Taskbar Settings for the Login Dialog

Show taskbar in login screen

☑ A taskbar is shown in the login screen. (Default)

Show clock

☑ A clock is shown in the taskbar in the login screen. (Default)

Show keyboard layout switcher

☑ A keyboard layout switcher is shown in the taskbar in the login screen. (Default)

Show on-screen keyboard button

☑ A button to start an on-screen keyboard is shown in the taskbar in the login screen.

☐ The button is not shown. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is started automatically with the login screen.

☐ The on-screen keyboard is not started automatically. (Default)

Show reboot button

☑ Reboot button is shown in the taskbar in the login screen.

☐ The button is not shown. (Default)

Show shutdown button

☑ Shutdown button is shown in the taskbar in the login screen. (Default)

Taskbar Settings When the Screenlock Is Active

Show taskbar in screenlock

☑ A taskbar is shown when the screen is locked. (Default)

Show clock

☑ A clock is shown in the taskbar when the screen is locked. (Default)

Show keyboard layout switcher

☑ A keyboard layout switcher is shown in the taskbar when the screen is locked. (Default)

Show on-screen keyboard button

☑ A button to start an on-screen keyboard is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Start on-screen keyboard automatically

☑ The on-screen keyboard is started automatically when the screen is locked.

☐ The on-screen keyboard is not started automatically. (Default)

Show reboot button

☑ Reboot button is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Show shutdown button

☑ Shutdown button is shown in the taskbar when the screen is locked.

☐ The button is not shown. (Default)

Show logoff button

☑ Logoff button is shown in the taskbar when the screen is locked.

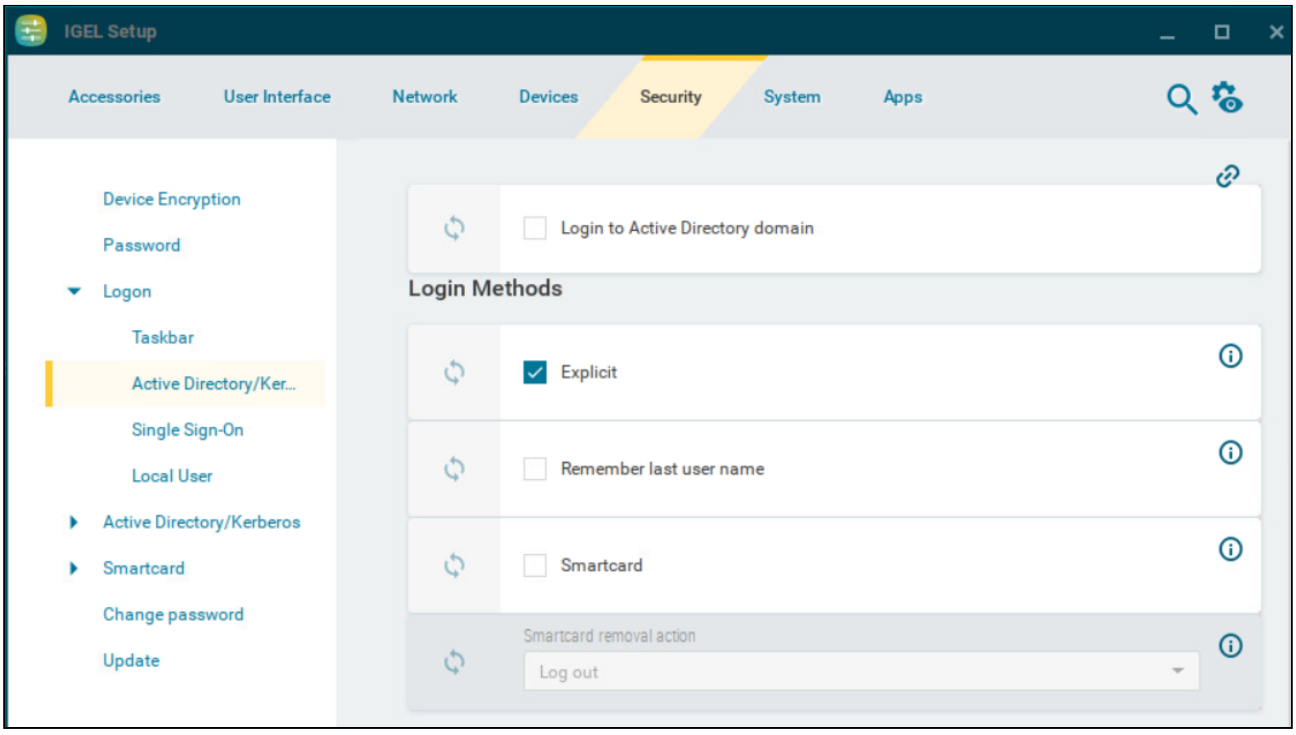
☐ The button is not shown. (Default)

Active Directory/Kerberos

This article shows how to enable local login to the device via the Kerberos protocol in IGEL OS.

> Active Directory/Kerberos must be configured as a prerequisite, see Active Directory/Kerberos (see page 264).

Menu path: **Security > Logon > Active Directory/Kerberos**



> The login can be used for single sign-on in a number of session types (ICA, RDP).

Login to Active Directory domain

☑ You can log in to the device via Active Directory.

☐ You cannot log in to the device via Active Directory. (Default)

Login Methods

Explicit

☑ You can log in with a user name and password. (Default)

☐ You cannot log in with a user name and password. If logging in with a smartcard is set up, you can log in with a smartcard.

Remember last user name

☑ The login dialog will be pre-populated with the last user name that logged on. **Explicit** must be enabled for this.

☐ The login dialog will not be pre-populated. (Default)

Smartcard

☑ You can log in using a smartcard.

☐ You cannot log in using a smartcard. (Default)

Smartcard removal action

Specifies what action is performed when the smartcard via which the user is logged in is removed.
Possible actions:

- **Log out**: The user is logged out from the device. (Default)
- **Lock device**: The screen is locked.

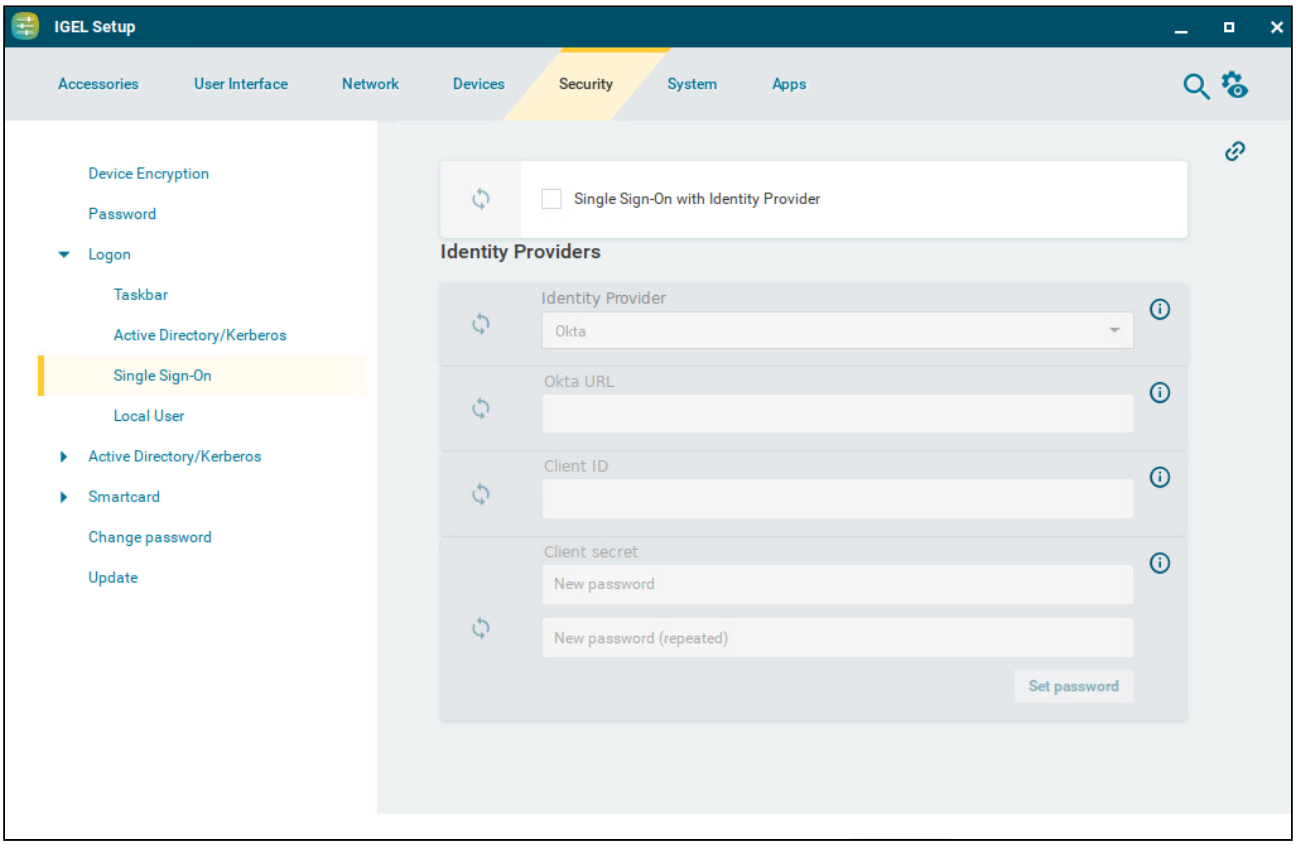
If the login method is configured and the **Allow system logoff** option is enabled under **System > Power Options > Shutdown**, the user can log off the device through the shutdown menu. For information on how to access the shutdown menu, see Commands (see page 129). For information on how to configure the shutdown menu, see Shutdown (see page 304).

Single Sign-On in IGEL OS 12

Single Sign-On (SSO) is an authentication method that can be used via a cloud-based identity provider (IdP) to access the local device and apps. This article describes the options used for configuring SSO in IGEL OS.

See How to Configure Single Sign-On (SSO) on IGEL OS 12 (see page 457) for a detailed description of the entire SSO configuration process.

Menu path: **Security > Logon > Single Sign-On**



Single Sign-On with identity provider

☑ SSO is used as the authentication method.

> To have a fallback option if something goes wrong with SSO, e.g. a network failure, it is recommended to configure local login in addition under **Security > Logon > Local User**. For more information, see Local User (see page 260).

☐ SSO is not used. (Default)

Identity provider

The identity provider used for the SSO configuration.
Possible options:

- **Azure AD**: Use Microsoft Entra ID as IdP
- **Okta**
- **OpenID Connect**
- **Ping Identity | PingOne**
- **VMware Workspace ONE Access**

Identity Provider Is Set to "Azure AD"

Azure AD Tenant Name/ID

The value you have obtained as **Directory (tenant) ID** in the Microsoft Entra ID Portal.

Application (client) ID

The value you have obtained as **Application (client) ID** in the Microsoft Entra ID Portal.

Client secret

The client secret that was created in the Microsoft Entra ID Portal.

> If the login method is configured and the **Allow system logoff** option is enabled under **System > Power Options > Shutdown**, the user can log off the device through the shutdown menu. For information on how to access the shutdown menu, see Commands (see page 129). For information on how to configure the shutdown menu, see Shutdown (see page 304).

Identity Provider Is Set to "Okta"

Okta URL

The URL of the Okta identity provider.

Client ID

The client ID that was created in Okta.

Client secret

This is a value created by the identity provider. The value can be copied from the Identity Provider Admin Console.

Identity Provider Is Set to "OpenID Connect"

This option can be used for various identity providers that support OpenID Connect.

Issuer URL

The URL at the identity provider's site where the OpenID configuration document for your application can be found. This is the part of the path that precedes `/.well-known/openid-configuration`

Client ID

The client ID that is registered in your identity provider.

Client secret

The client secret that has been created by your identity provider.

Identity Provider Is Set to "Ping Identity | PingOne"

PingOne issuer URL

The URL at the Ping Identity / PingOne site where the OpenID configuration document for your application can be found. This is the part of the path that precedes `/.well-known/openid-configuration`

Client ID

The client ID that is registered in Ping Identity / PingOne for your application.

Client secret

The client secret that has been created in Ping Identity / PingOne for your application.

Identity Provider Is Set to "VMware Workspace ONE Access"

Workspace ONE Access issuer URL

The URL at the Workspace ONE Access site where the OpenID configuration document for your client can be found. This is the part of the path that precedes `/.well-known/openid-configuration`

Client ID

The client ID that is registered in Workspace ONE Access for your client.

Client secret

The client secret that has been created in Workspace ONE Access for your client.

Automatic Desktop Login

As an alternative to the interactive desktop login, predefined user credentials can automatically be provided to the IdP on startup. The credentials are stored securely on the endpoint device.

- In this version of IGEL OS, only login via username and password is supported; multi-factor authentication (MFA) is not supported.
- Please be aware that after the automatic desktop login, a fully unlocked desktop session will run on your endpoint device. This feature should only be used for use cases where no interactive login is possible. It is good practice to restrict this user's access to only the relevant components and data that are necessary for the specific use case.

Automatic login is available for the following IdPs:

- Okta
- Microsoft Entra ID (formerly known as Microsoft Azure AD)
- Ping Identity | PingOne
- VMware Workspace ONE Access

Automatically perform login

☑ After startup, the endpoint device performs the login automatically using the **Username for autologin** and the **Password for autologin**.

Username for autologin

The name of a user known to the IdP used.

Password for autologin

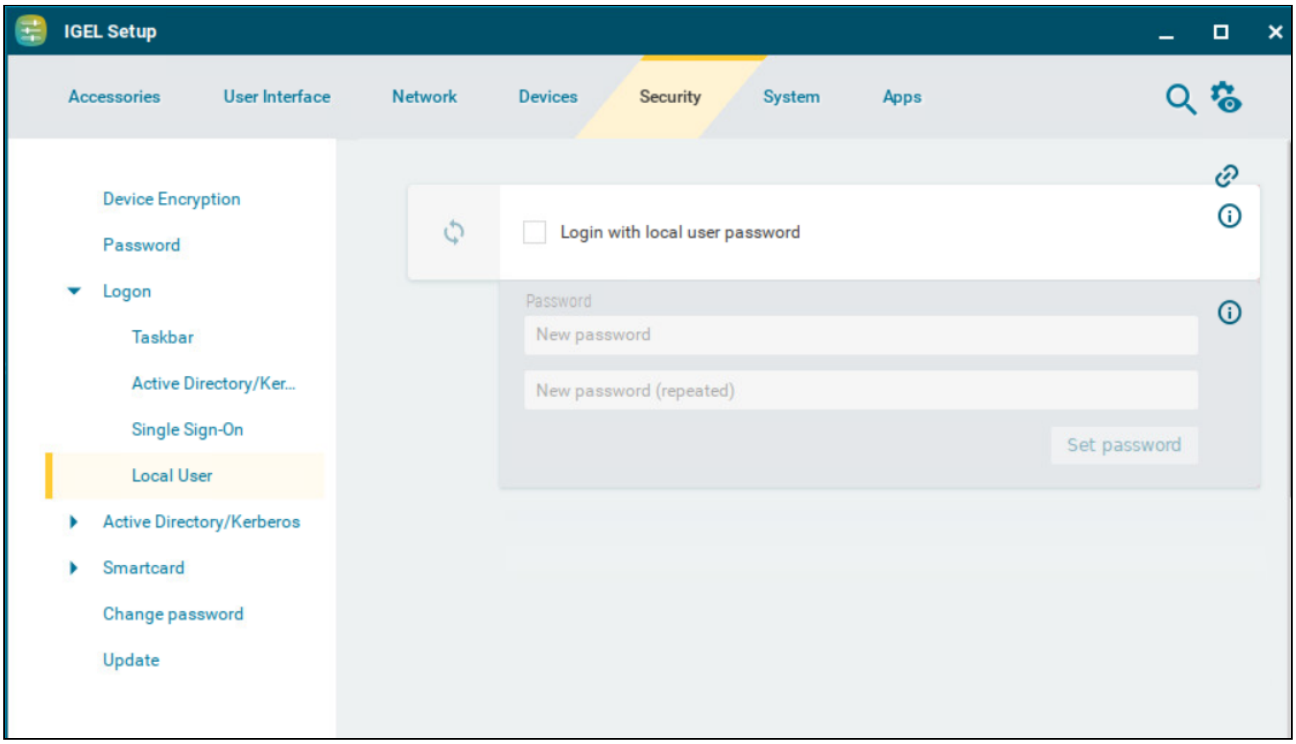
The password of the user provided in **Username for autologin**.

Local User

This article shows how to configure the local login authentication in IGEL OS.

> If several login methods are enabled, the login method can be selected on the login screen.

Menu path: **Security > Logon > Local User**



Login with local user password

☑ Upon the start of the device, a login screen is shown and authentication with a local user password is required. The password specified under **Password** is deployed to log in.

☐ No authentication is required upon device startup. (Default)

Password

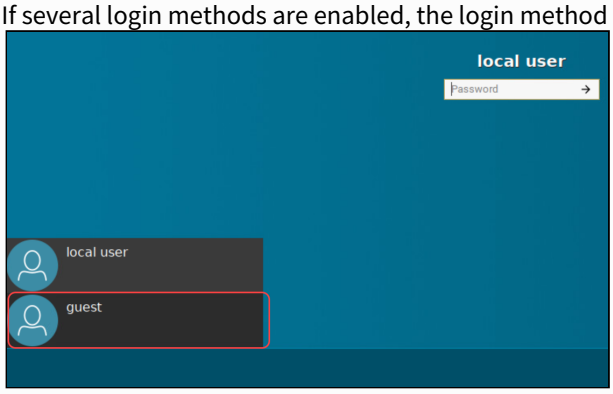
The password deployed to log in. This password is also required for unlocking the screen if the **Require password to unlock (screenlock)** option is enabled under **User Interface > Screenlock / Screensaver > Options**. For more information, see Options (see page 89).

If the login method is configured and the **Allow system logoff** option is enabled under **System > Power Options > Shutdown**, the user can log off the device through the shutdown menu. For information on how to access the shutdown menu, see Commands (see page 129). For information on how to configure the shutdown menu, see Shutdown (see page 304).

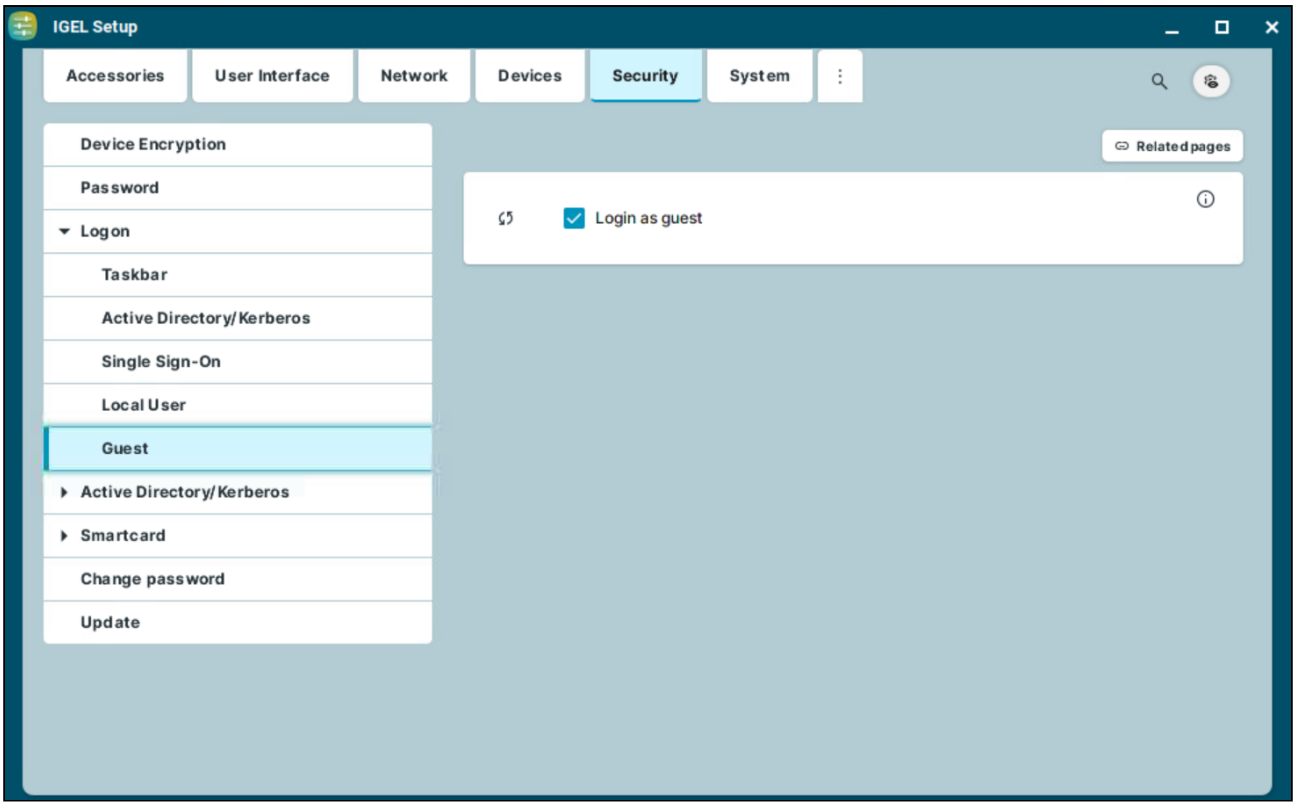
Guest - Passwordless Access to IGEL OS

This article shows how to configure a passwordless guest user with limited access to applications in IGEL OS.

If several login methods are enabled, the login method can be selected on the login screen:



Menu path: **Security > Logon > Guest**



Login as guest

☑ Pre-configured sessions can be accessed without a password through the guest user.

☐ The guest user is disabled. (Default)

Configuring Access for the Guest User

Each session can be made available for the normal user, the guest user, or both through the Registry parameters:

- **sessions.<instance>.login_method**
- **app.<app-name>.sessions.<instance>.login_method**

By default, all the sessions are available for the normal user only.

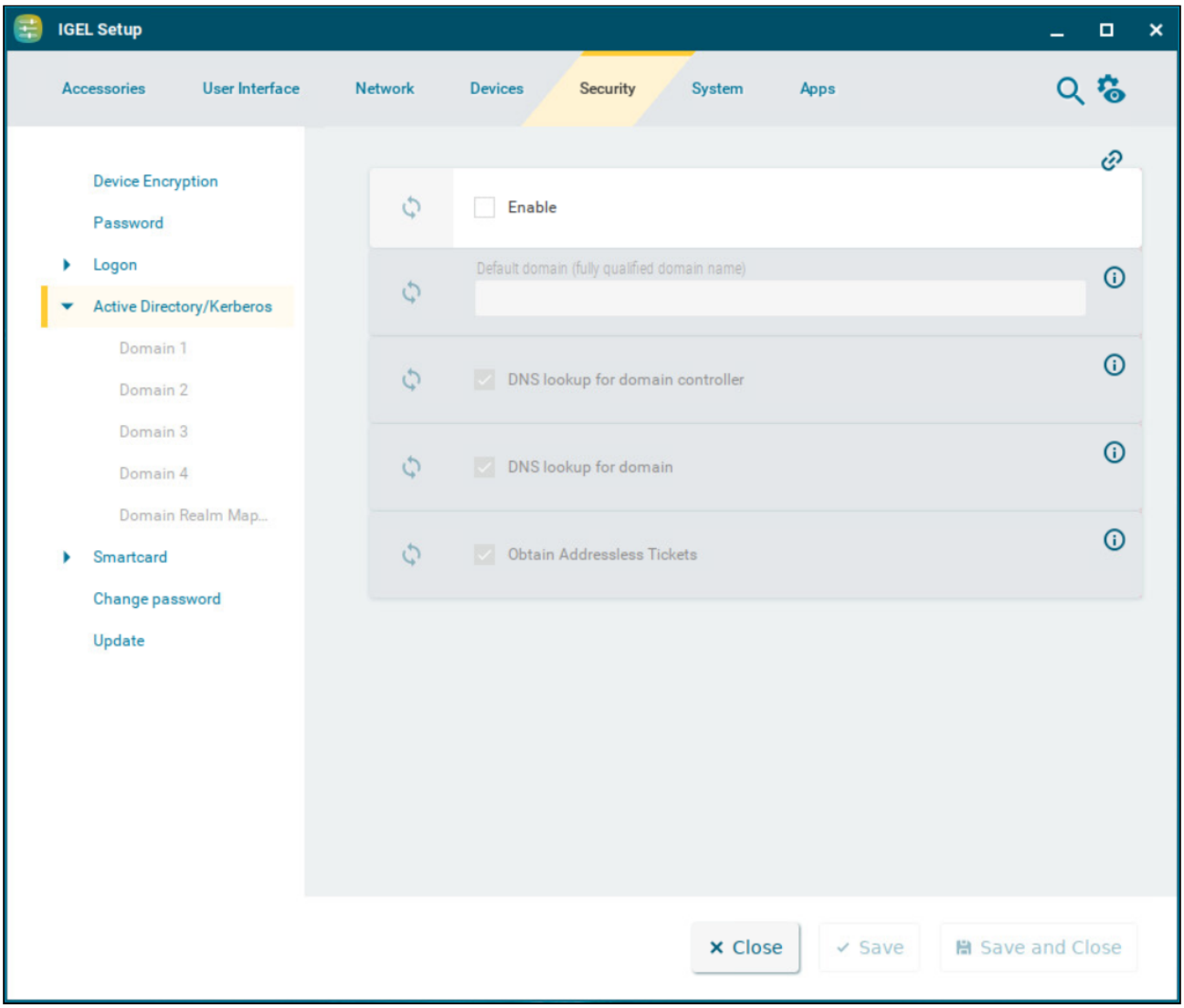
▶ To configure access for passwordless guest login, choose applications which should be available in a guest session by setting the above parameters to **Guest** or **All**.

On command-line use `nodelist sessions` to get a currently defined list of sessions.

Active Directory/Kerberos

This article shows how to configure the options for Active Directory with Kerberos in IGEL OS.

Menu path: **Security > Active Directory/Kerberos**



Enable

☑ The Kerberos basic configuration will be carried out.

☐ The Kerberos basic configuration will not be carried out. (Default)

Default domain (fully qualified domain name)

This value must match the Windows domain on which the logon is to take place. The value must be entered in upper case letters. e.g. `EXAMPLE.COM` .

DNS lookup for domain controller

☑ In order to find the Key Distribution Centers (KDCs, domain controllers) and other servers for a realm, if they are not explicitly indicated, DNS SRV records are used. (Default)

☐ The KDCs entered under **Security > Active Directory/Kerberos > Domain 1** ... **Domain 4** will be used.

DNS lookup for domain

☑ In order to determine the Kerberos realm of a host, DNS TXT records are used. (Default)

☐ The details under **Setup > Security > Active Directory/Kerberos > Domain Realm Mapping** are used.

Obtain Addressless Tickets

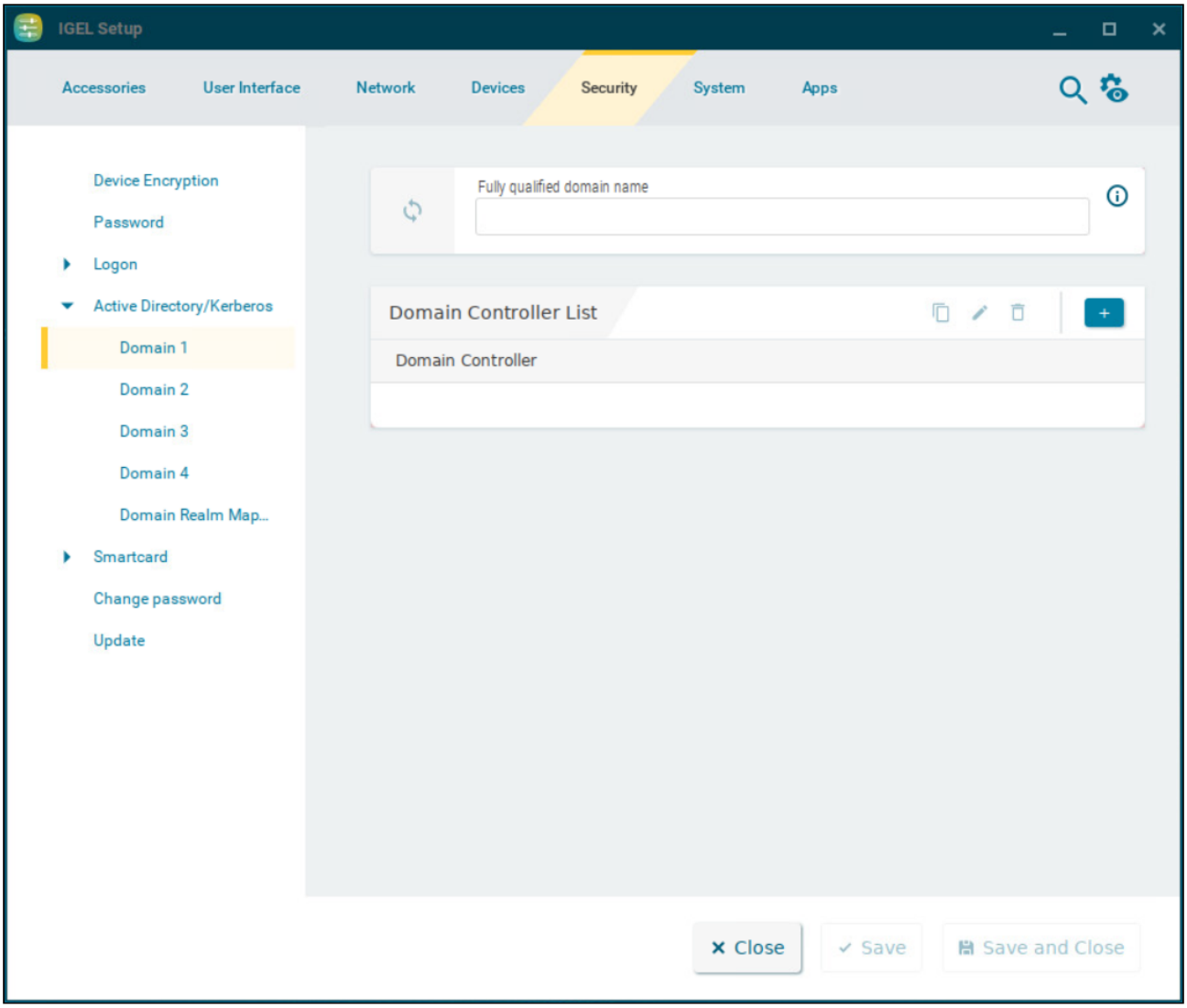
☑ The first Kerberos ticket is addressless. This may be necessary if the client is located behind an Network Address Translation (NAT) device. (Default)

- Domain (see page 266)
- Domain Realm Mapping (see page 268)

Domain

This article shows how to configure domains for the Active Directory/Kerberos configuration in IGEL OS. Up to four domains can be configured.

Menu path: **Security > Active Directory/Kerberos > Domain [1-4]**



Fully qualified domain name

Name of the domain

Domain Controller List

To manage the list of domain controllers:

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

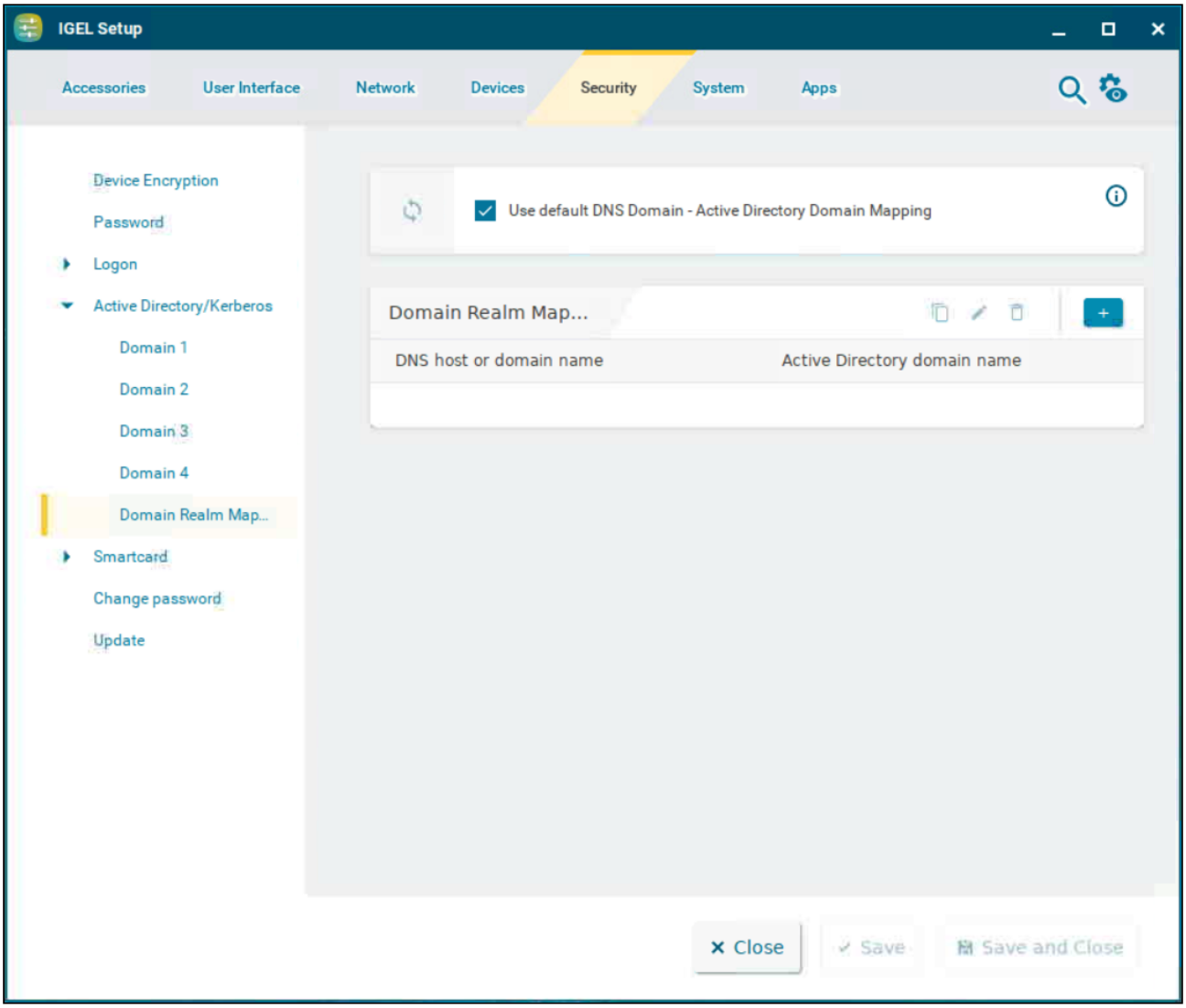
To configure a domain, proceed as follows:

1. Under **Fully qualified domain name**, give the name of the domain (Kerberos realm).
2. Click to create a new entry.
3. Under **Domain Controller**, give the name or IP address of the domain controller (Kerberos Key Distribution Center). A port number can be added to the host name; the port name must be preceded by a colon.
4. Click **Confirm**.
   The domain controller will be added to the **Domain Controller List**.

Domain Realm Mapping

With domain realm assignment, a host name is translated into the corresponding Kerberos realm name. This article shows how to configure domain realm mapping in IGEL OS.

Menu path: **Security > Active Directory/Kerberos > Domain Realm Mapping**



Use default DNS domain - Active Directory domain mapping

☑ The DNS name and Active Directory domain name match. (Default)

☐ DNS name and Active Directory domain name assignments must be set up.

Domain Realm Mapping

To manage the list of realm mappings:

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

To set up a DNS name to Active Directory domain name assignment proceed as follows:

1. Click to create a new entry.
   The Add dialog is displayed.
2. Under **DNS host or domain name**, enter the lower case FQDN name of a host or a domain that is to be assigned to an Active Directory domain name. Example: `.example.com`
3. Under **Active Directory domain name**, enter the Active Directory domain name that is to be assigned to the host name.
4. Click **Confirm**.
   The data entered will be added to the **Domain Realm Mapping** list.

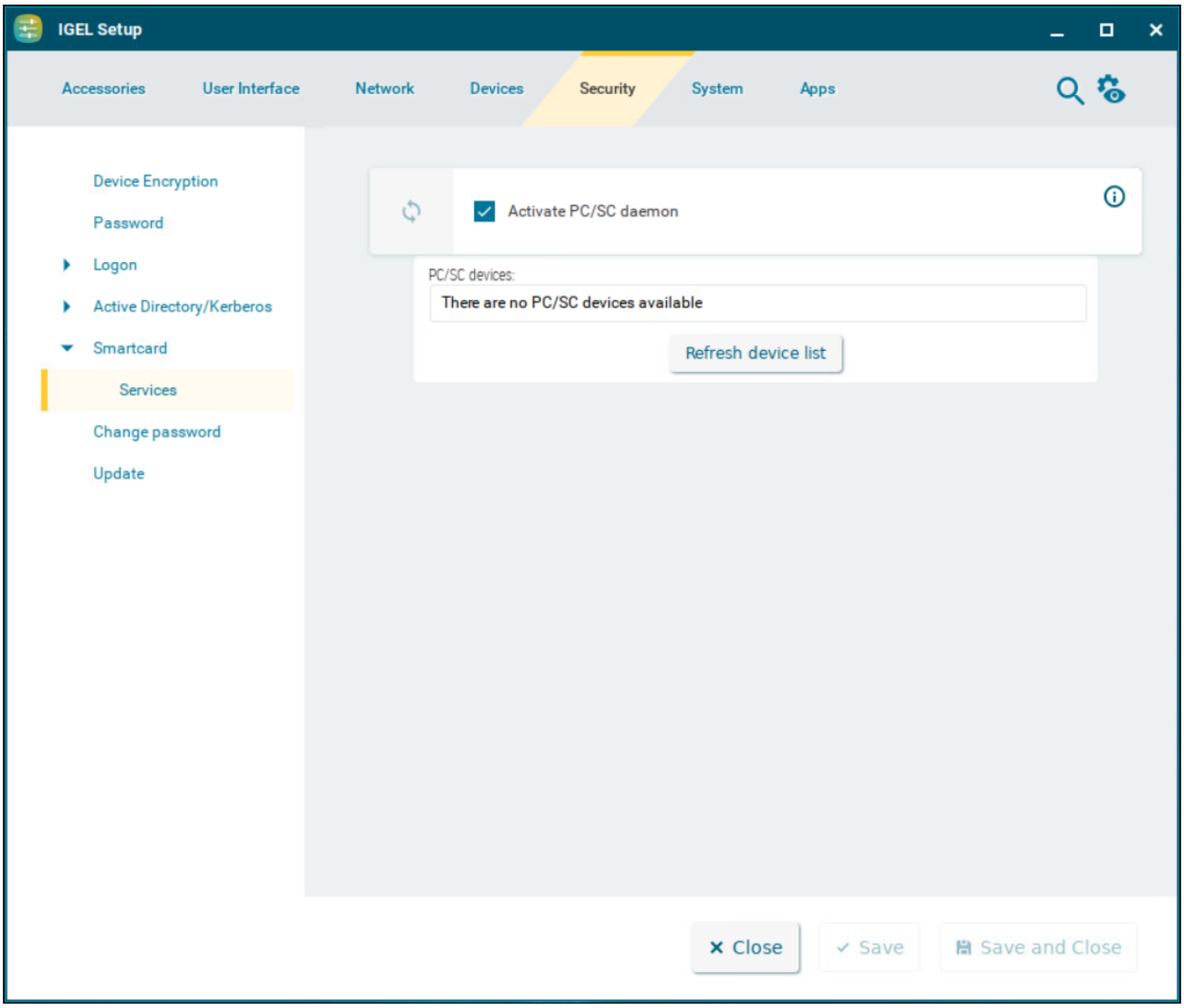
Smartcard Services

Smartcard services need to be configured in order to use smartcard readers. This article shows the settings options of smartcard services in IGEL OS.

You will find a list of supported smartcard readers in the IGEL Hardware Database[18].

Menu path: **Security > Smartcard > Services**

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



Activate PC/SC daemon

The PC/SC daemon enables the smartcard reader to connect to the device, so that the smartcard is available to an application. This can be a server-side application where data is forwarded via an RDP or ICA connection or a local application, e.g. the browser.

☑ The PC/SC service is enabled. The card reader is available for applications. (Default)

☐ The PC/SC service is disabled. The card reader is not available.

PC/SC devices

List of smartcard readers currently connected to the device. Internal smartcard readers and a variety of USB smartcard readers are supported.

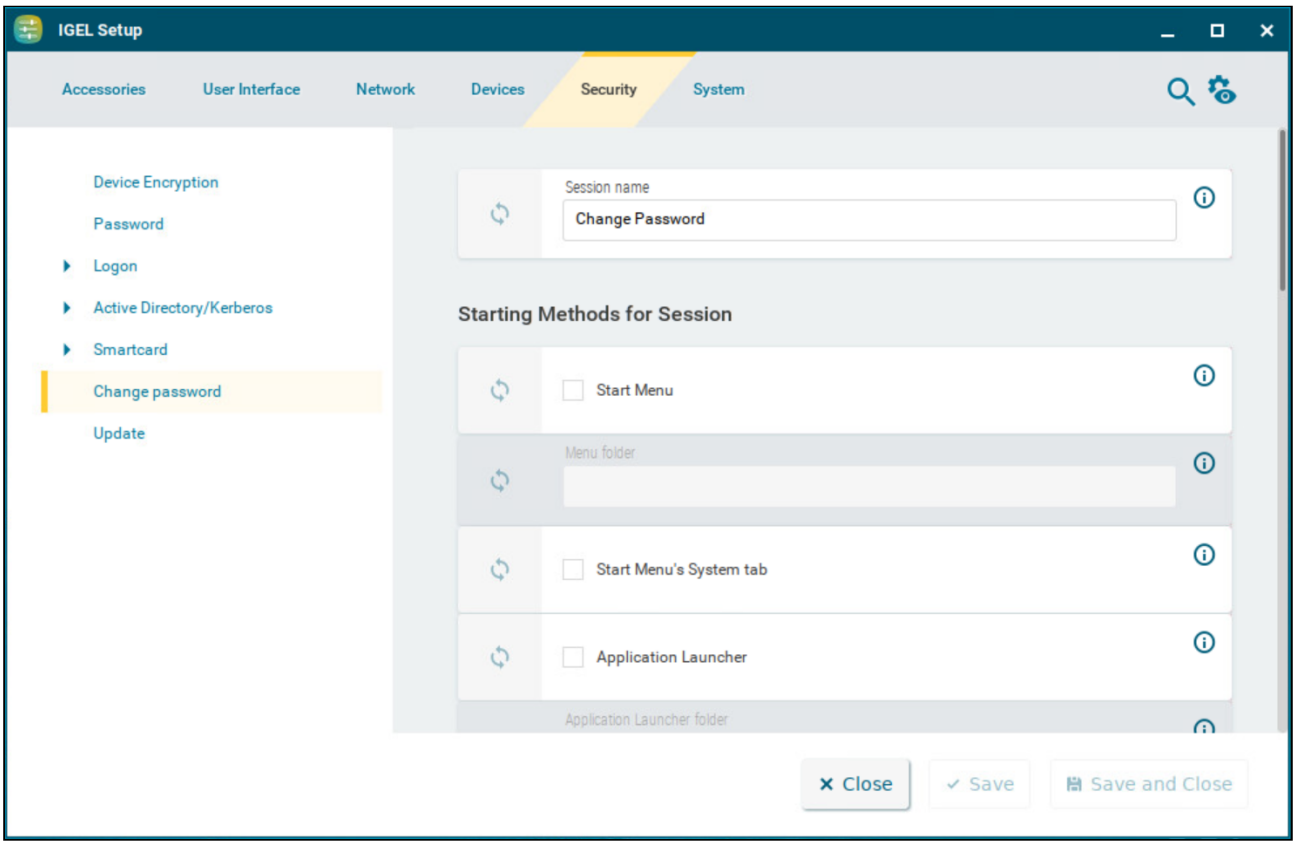
Refresh device list

Click the button to refresh the list of available PS/SC devices.

Change Password

This article shows how to set up and use the Change Password function in IGEL OS.

Menu path: **Security > Change Password**



With this function, the user can change the password or PIN for the login method he used for his current session, provided one of the following login methods was used:

- Active Directory with username and password
- Active Directory with third-party smartcard
- Local user password

The starting methods parameters are described under Starting Methods for Apps (see page 376).

> If autostart is enabled in the starting methods, the **Change Password** function is presented after login.

When a password change is required, a dialog informing the user is presented after login. When the user clicks the password change button in this dialog, the **Change Password** function starts automatically.

Using Change Password

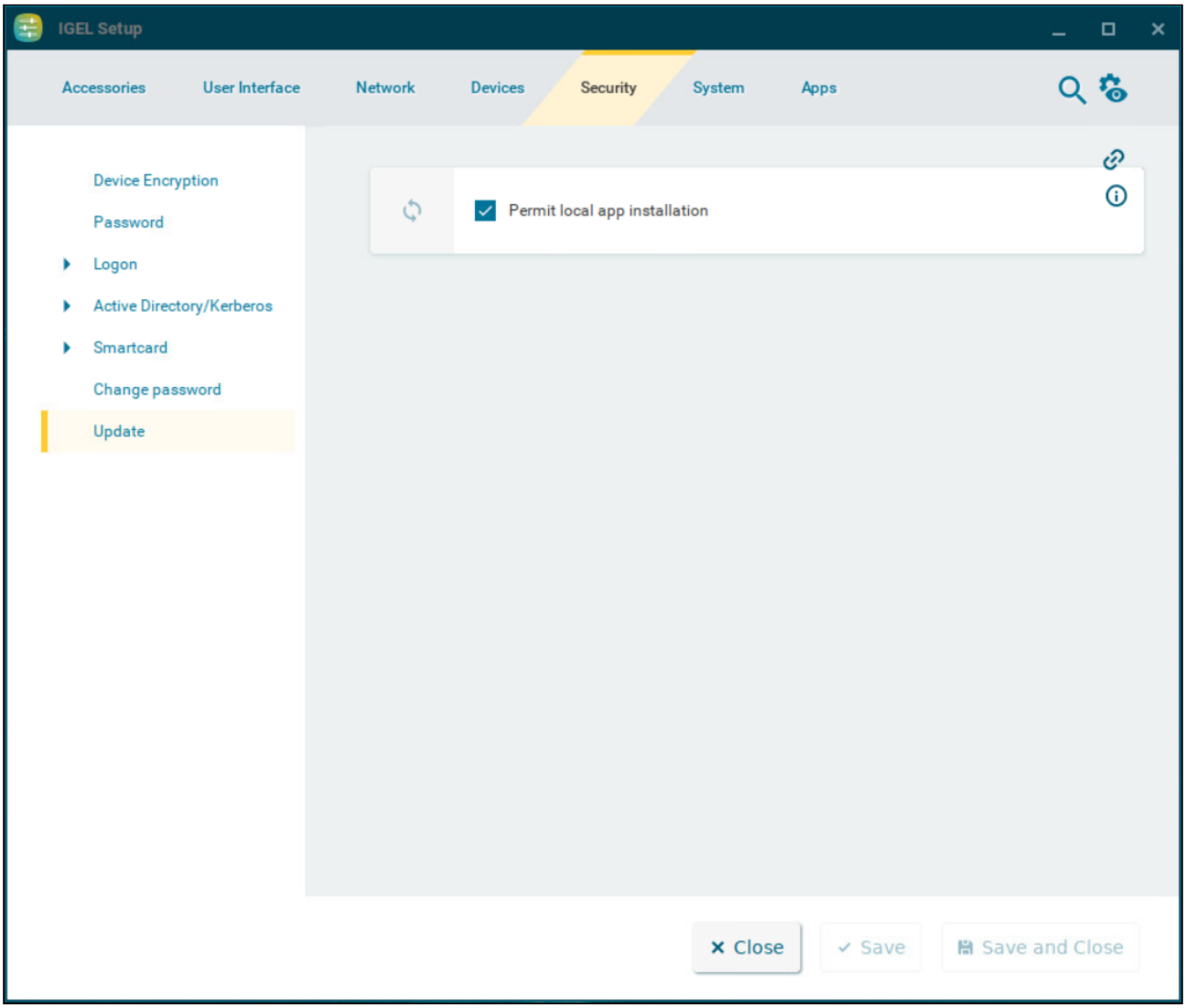
To change your password for your current login method, proceed as follows:

1. Start the **Change Password** function.
2. Enter the changed password or PIN in the dialog. The dialog differs according to the login method that is currently used.
3. Click **OK**.
   The password is changed.

Update

This article shows how to enable local app installation in IGEL OS. For more information on local app installation, see Installing IGEL OS Apps Locally on the Device. For more information on app updates, see Update (see page 347).

Menu path: **Security > Update**



Permit local app installation

☑ Enables the local app portal and the installation of apps by the user. (Default)

System

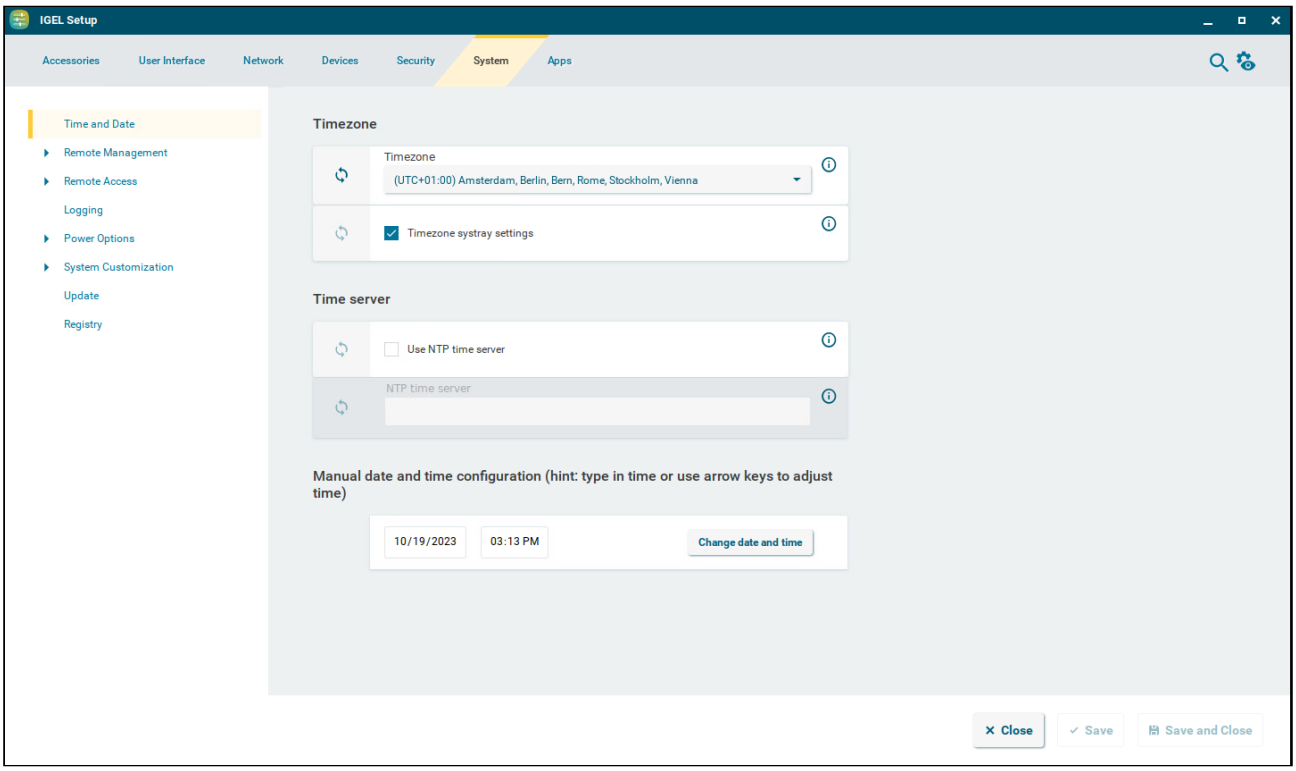
In this chapter, you find information on system configuration in IGEL OS.

- Time and Date (see page 277)
- Remote Management (see page 279)
- Remote Access (see page 283)
- Logging (see page 292)
- Power Options (see page 296)
- System Customization (see page 307)
- Update (see page 347)
- Registry in IGEL OS 12 (see page 350)

Time and Date

This article shows the time and date settings options in IGEL OS.

Menu path: **System > Time and Date**

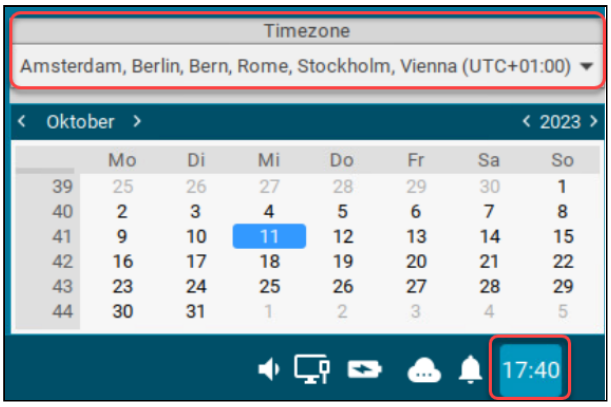


Timezone

Sets the timezone the device is located in.

Timezone systray settings

☑ You can set the timezone by clicking on the taskbar clock and selecting from the **Timezone** dropdown menu. The taskbar clock can be activated under **User Interface > Desktop > Taskbar Items**. (Default)



☐ The **Timezone** dropdown menu is not available through the taskbar clock.

Use NTP time server

☑ The system clock is set via Network Time Protocol (NTP) during boot.

☐ The system clock is not set via NTP. (Default)

NTP time server

IP address or name of the NTP time server. If you would like to enter a list of NTP time servers for redundancy purposes, separate the names / IP addresses by spaces.

Manual Date and Time Configuration

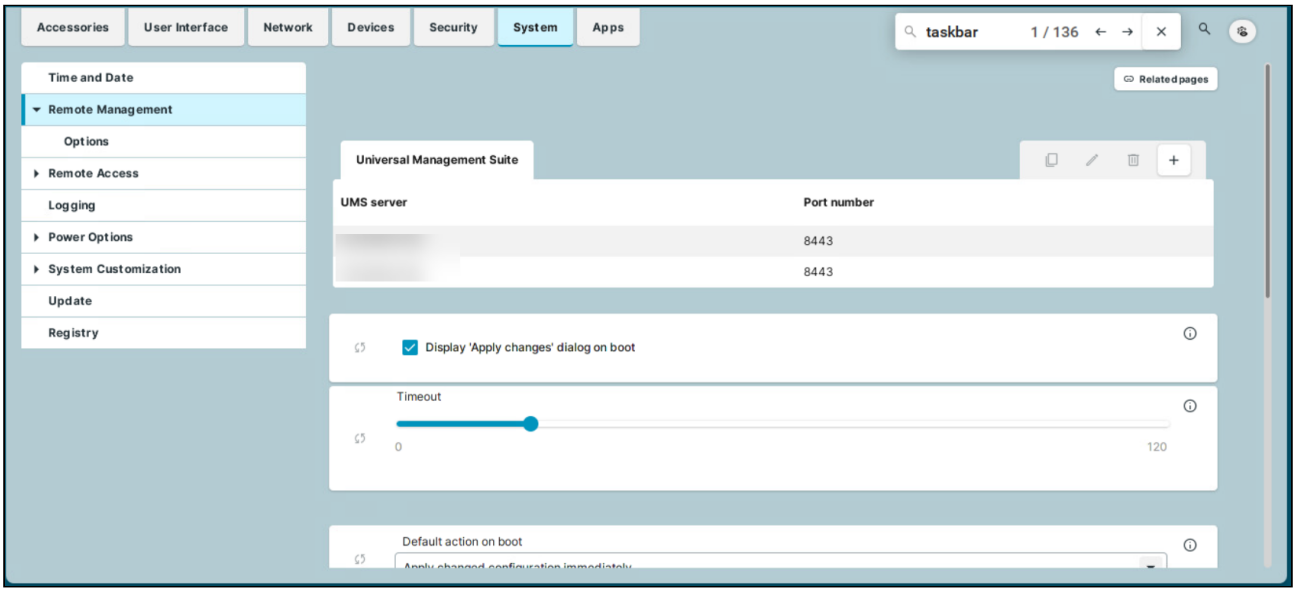
Carries over the time and date and sets the hardware clock. Once the date and time is set, click **Change date and time** to save the change.

You can set the date by selecting from the calendar, or using the arrow keys to adjust the date.
You can set the time by typing it in, or using the arrow keys to adjust the time.

Remote Management

In IGEL OS, endpoint devices are managed using the Universal Management Suite (UMS). This article shows the settings related to the remote management, for example, the configuration of UMS servers and user information dialogs on UMS updates. For more information on the UMS, see Universal Management Suite (UMS).

Menu path: **System > Remote Management**



Universal Management Suite

If the device is registered on a **UMS Server**, its IP address / hostname and **Port number** will be shown in the list.

> The list can contain more than one UMS instance. If the device cannot contact a UMS Server under the hostname `igelrmserver`, and the DHCP option 244 is not set, the device will go through the entries in the list until it can contact a UMS Server successfully.

To manage the list of servers:

- 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 **Add** dialogue, where you can define the following settings:

- **UMS server**
  Name or IP of the UMS Server
- **Port number**
  Port number of the UMS Server (Default: 8443)

Display “Apply changes” dialog on boot

If new settings were made in the UMS, the device may receive them during the boot procedure.

☑ During the boot procedure, the **Apply changes** dialog is displayed and the user can decide whether the new settings are applied immediately. If the user does not allow them to be applied immediately, they will automatically be applied next time the system is restarted. (Default)

☐ The **Apply changes** dialog will not be shown. The new settings will be applied or ignored depending on the setting under **Default action on boot**.

Timeout

Number of seconds for which the **Apply changes** dialog is shown. If the timeout is exceeded, the received settings will automatically be applied. (Default: 20)
Setting the value to 0 disables the timeout, and the dialog is shown until the user clicks a button.

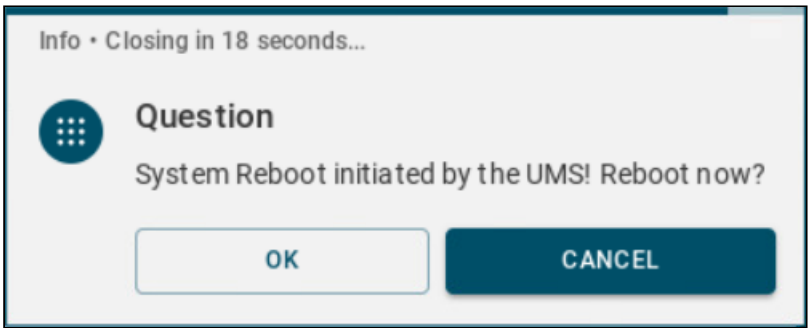
Default action on boot

Configure the action that is to be performed if the dialog exceeds the timeout or if the timeout is disabled.
Possible values:

- **Apply changed configuration immediately**: New settings will take effect immediately, and programs that are running may be restarted. (Default)
- **Ignore changed configuration**: New settings will not be applied. The new configuration will be saved on the device, and applied the next time a new configuration is applied.

Prompt user on UMS actions

☑ The user is informed through a message window when UMS actions are performed on the device. (Default)



☐ The user is not informed when UMS actions are performed on the device.

Timeout

Number of seconds for which the UMS actions information dialog is shown. If the timeout is exceeded, the received settings will automatically be applied. (Default: 20)
Setting the value to 0 disables the timeout, and the dialog is shown until the user clicks on a button.

Log message severity

Select the severity level above which device errors are to be transferred to the UMS. Messages with a lower severity are suppressed.
Possible options:

- **off** (Default)
- **error**
- **warn**
- **info**
- **debug**

Show UMS connection status tray icon on desktop

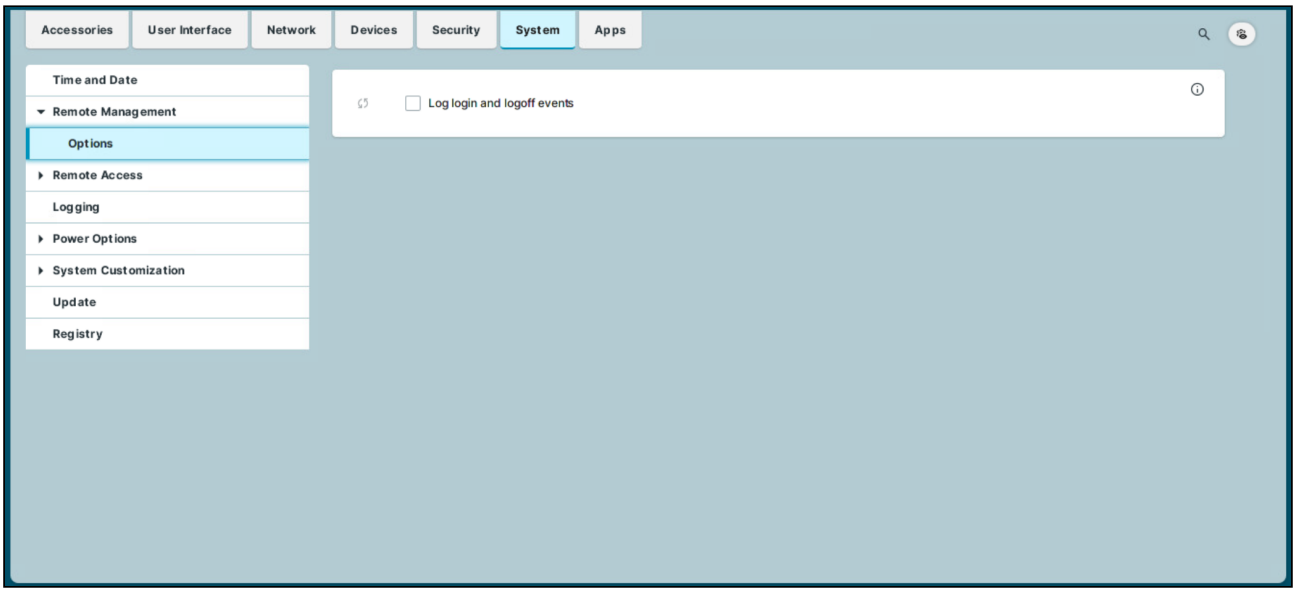
The icon is displayed in the taskbar, showing the status of the UMS connection. Clicking the icon displays information about the connected UMS server.

Options of Remote Management in IGEL OS 12

This article shows how to enable the logging of remote management events in IGEL OS.

> The logged events can be found both in the UMS Console and the UMS Web App. For more information, see View Device Information in the IGEL UMS and Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App.

Menu path: **System > Remote Management > Options**



Log login and logoff events

☑ Details of logon and logoff events of the following logon types are sent to the UMS:

- Active Directory/Kerberos
- Single Sign-On
- Local User
- Guest User

> Events are only logged if the **Enable user logon history** parameter is enabled in the UMS Console, under **UMS Administration > Global Configuration > Misc Settings.** For more information, see Misc Settings.

☐ Logon and logoff events are not sent to the UMS. (Default)

Remote Access

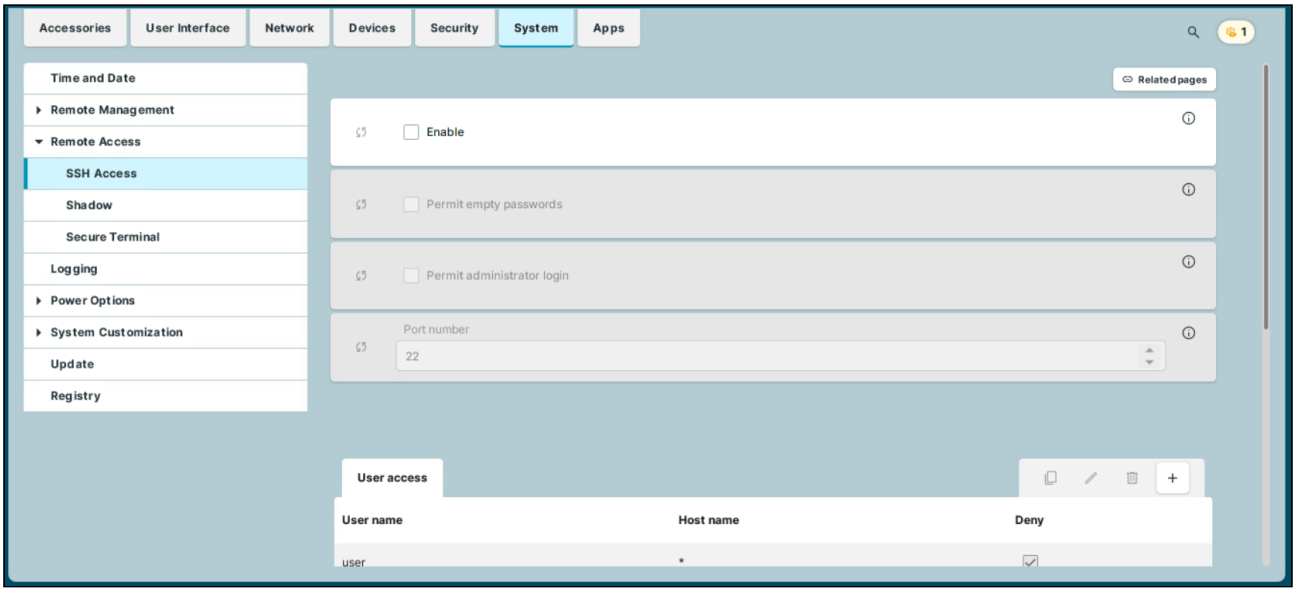
To support remote management, the following remote access options can be configured for the device.

- SSH Access (see page 284)
- Shadow (see page 287)
- Secure Terminal (see page 290)

SSH Access

This article shows how to configure Secure Shell (SSH) access to the device in IGEL OS.

Menu path: **System > Remote Access > SSH Access**



Enable

☑ The SSH service is enabled.

☐ The SSH service is disabled. (Default)

If SSH access is enabled, you can configure the following:

Permit empty passwords

☑ Logging on without a password is allowed.

☐ Logging on without a password is not allowed. (Default)

Permit administrator logon

☑ Logging on as an administrator is allowed.

☐ Logging on as an administrator is not allowed. (Default)

Port number

Port number for SSH. (Default: 22)

User Access

List of configured users.

> Unlike **root** and **user**, the **ruser** is not intended for real SSH sessions, but only for starting X applications that are listed below under **Applications Access for Remote User "ruser"**.

To manage the list:

- **User name**

  Permitted user

- **Hostname**

  Name of the host from which SSH access takes place (example: `xterm.igel.de`)

- **Deny**

  ☑ Access is denied.

  ☐ Access is allowed. (Default)

> For `ruser` a password has to be assigned under **Security > Password**. The names `root` and `user` work also without passwords. For more information, see Password (see page 245).

Permit X11 forwarding

☑ X11 forwarding is enabled.

☐ X11 forwarding is disabled. (Default)

Applications Access for Remote User "ruser"

The `ruser` is not intended for real SSH sessions, but only for starting X applications configured below. By default these are `localshell` and `/config/sessions/setup0`.

> If you try to log on to the device as **ruser** via SSH, then you will never be able to connect. The connection will be closed immediately without anything happening. In this case you must add the parameter "-X" and the program to be started in the session call, like in this example:

```
ssh -X ruser@192.168.10.203 localshell
```

To manage the list:

- 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 **Add** dialogue, where you can define the following settings:

- **Command line**

  Command that is allowed or prohibited for the remote user

- **Enable application**

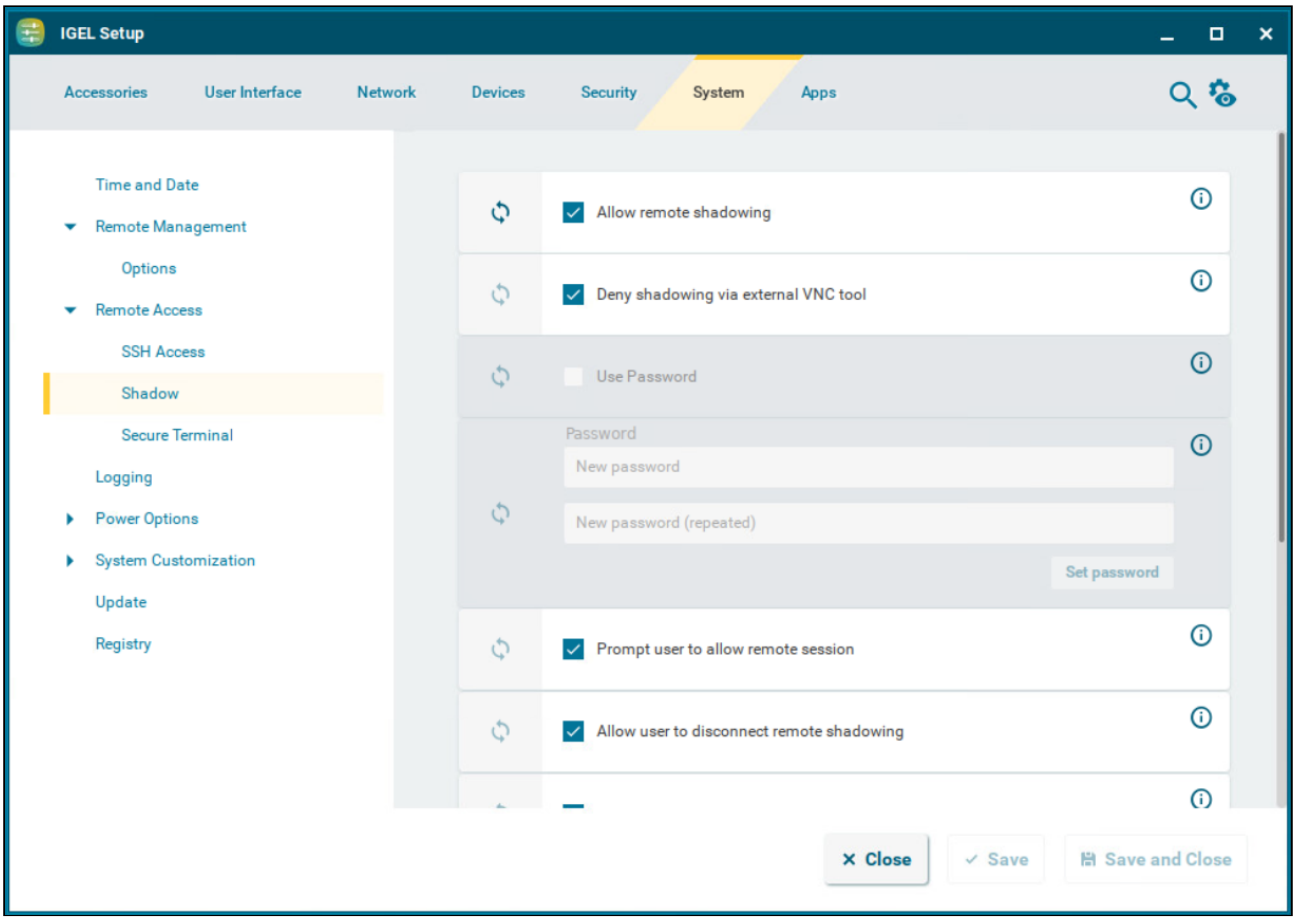
  ☑ The application given under **Command line** may be executed by the remote user. (Default)

  ☐ The application given under **Command line** may not be executed by the remote user.

Shadow

IGEL OS offers the ability to observe the endpoint device via shadowing through the IGEL Virtual Network Computing (VNC) Viewer in the Universal Management Suite (UMS) or another VNC client (e.g. TightVNC), see Shadowing - Observe IGEL OS Desktop via VNC. The shadowing of IGEL OS 12 devices through the UMS is always via Unified Protocol, i.e. communication is always encrypted. This article shows the settings for configuring the VNC access to your devices.

Menu path: **System > Remote Access > Shadow**



Allow remote shadowing

☑ Desktop content can be accessed by remote computers with VNC software.

☐ VNC shadowing is not allowed. (Default)

If **Allow remote shadowing** is activated, you can change the following settings:

Deny shadowing via external VNC tool

☑ The device can only be shadowed via the UMS. Shadowing of the device by an external VNC viewer is not possible. (Default)

☐ The device can be shadowed by an external VNC viewer, not only the UMS.

Use password

☑ The remote user is authenticated with a password before shadowing.

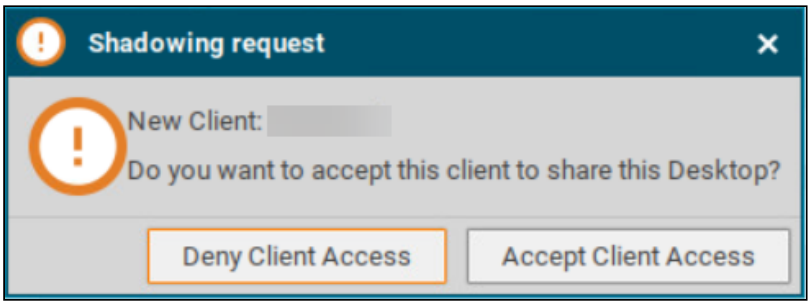
☐ The remote user is not authenticated for shadowing. (Default)

Password

Password for the VNC connection

Prompt user to allow remote session

☑ The local user will be asked for permission before shadowing. (Default)



In a number of countries, for example, Germany, unannounced shadowing is prohibited by law. Do not disable this option if you are in one of these countries!

Allow user to disconnect remote shadowing

☑ A **Disconnect** button with which the user can terminate the VNC connection is shown. (Default)

Allow input from remote

☑ The remote user can make entries using the keyboard and mouse as if they were the local user. (Default)

Scale frame buffer

☑ The screen content of the shadowed device is reduced or enlarged by the **Scale factor** before being transferred.

☐ The screen content is transferred in the original size. (Default)

Scale factor

Factor by which the screen content of the shadowed device is enlarged or reduced. Values under 1 reduce the content. (Default: 1.0)

Position of the indicator

Defines the position of the popup notification about being shadowed.
Possible options:

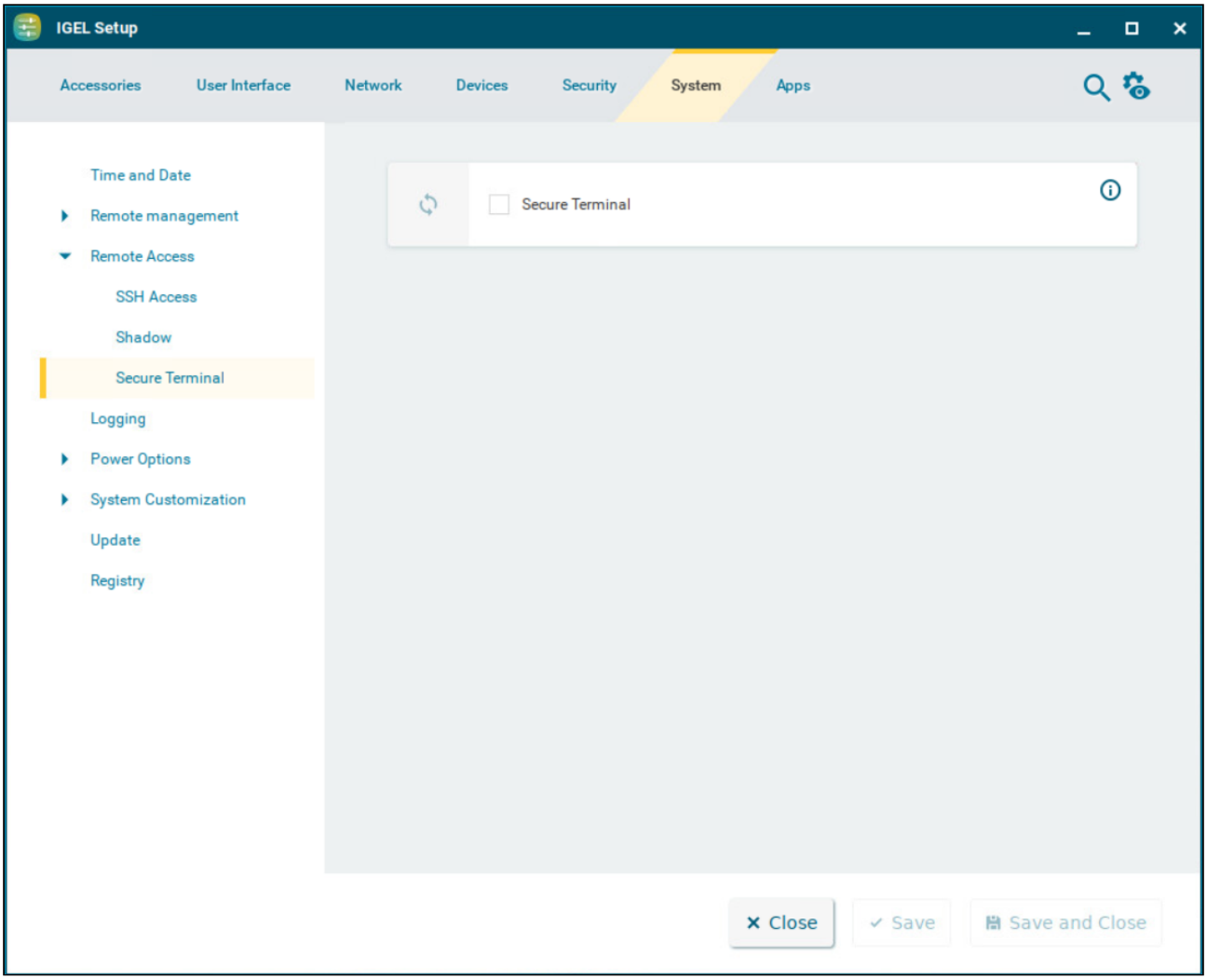
- **Top right**
- **Top left**
- **Bottom left**
- **Bottom right** (Default)

ⓘ Further parameters for the VNC server on the device are accessible under **System > Registry > network.vncserver**.

Secure Terminal

This article shows how to enable or disable the secure terminal connection on the endpoint device in IGEL OS.

Menu path: **System > Remote Access > Secure Terminal**



Secure Terminal

☑ Secure terminal connection is enabled between the device and the Universal Management Suite (UMS).

☐ Secure terminal connection is disabled between the device and the UMS. (Default)

For information on how to use the secure terminal from the UMS, see Configuring the Secure Terminal and Using the Secure Terminal.

You can enable secure terminal connection for all registered devices by activating the **Enable secure terminal globally** option under **UMS Console > UMS Administration > Global Configuration > Remote Access**.
For more information, see Remote Access.

For a list of IGEL specific commands collected by the IGEL Community, see Cheatsheet-IGELCommunity[19].

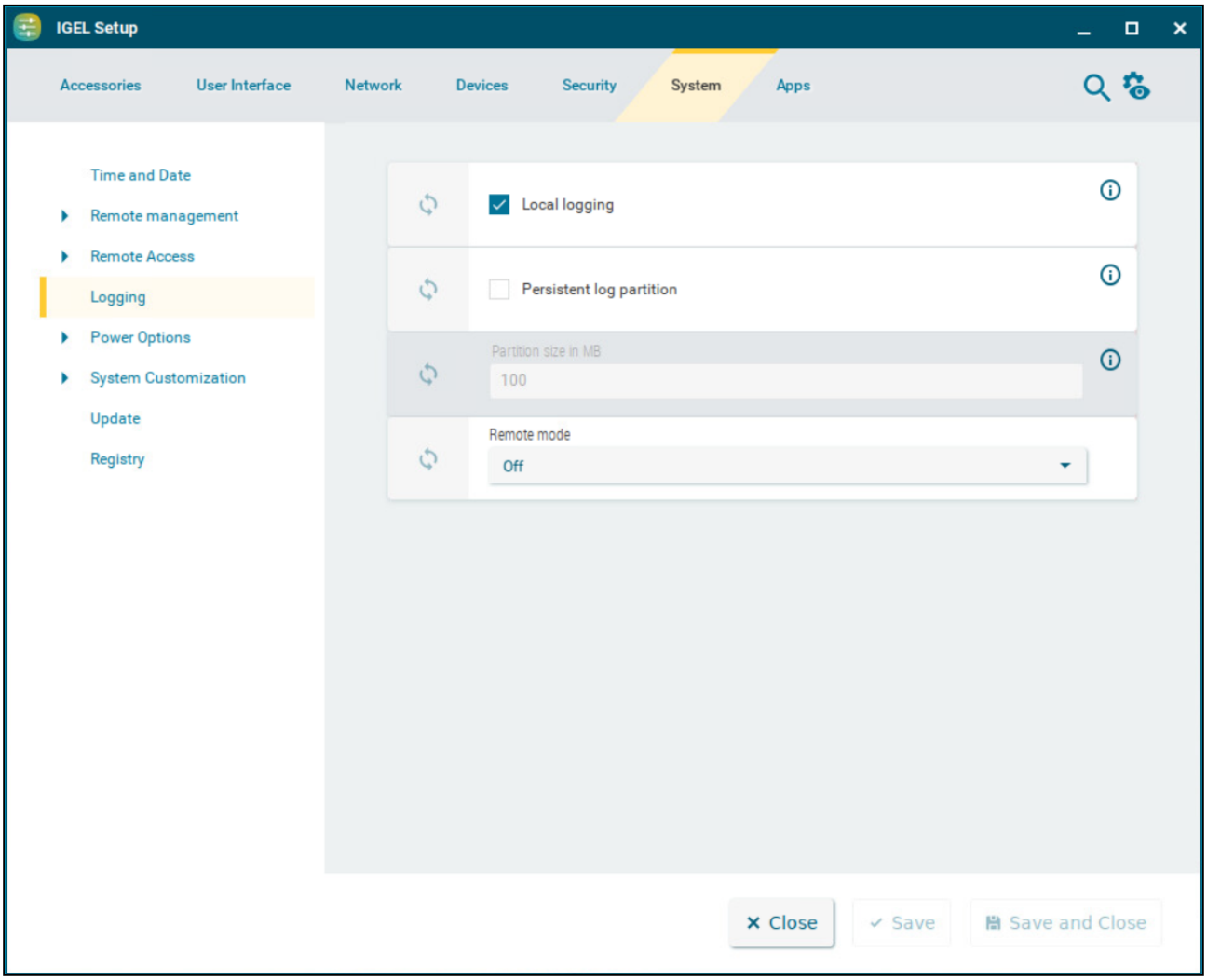
19 https://igel-community.github.io/IGEL-Docs-v02/Docs/Cheatsheet-IGELCommunity/

Logging

This article shows the options to configure local and remote logging for the device in IGEL OS.

> You can use the System Log Viewer to access system logs. For more information, see System Log Viewer (see page 40).

Menu path: **System > Logging**



Local logging

☑ The log messages are stored locally in `/var/log`. The format is human-readable. Log rotation is applied.

☐ The log messages are not stored locally.

Persistent log partition

This parameter is effective if **Local logging** is activated.

☑ The log messages are stored in a persistent partition on the device. This partition is encrypted.

☐ The log messages are stored in temporary files that are deleted on reboot.

Partition size in MB

Size of the persistent log partition

Remote mode

Possible options:

- **Server**: The device receives log messages from a remote client.
- **Client**: The device sends its log messages to a remote server.
- **Off**: The device does not send or receive any log messages. (Default)

Remote Mode Switched to Server

You can configure the device to act as a syslog server. Other clients can send log files to this server; you can create a separate server configuration for each client.

Template for log file storage

Pattern from which the file path for storing the received log messages is created. For example, in `/var/log/%HOSTNAME%/messages`. `%HOSTNAME%` is the name of the sender which is configured under **Name**.

To manage the **Server** list:

- 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 **Add** dialogue, where you can define the following settings:

- **Local port**

  Port on which the local server listens for log messages

- **Transport protocol**

  Protocol to be used for the transmission of log messages
  Possible options:

  - **TCP** (Default)
  - **UDP**

- **Name**

  Hostname of the sender (optional). This is useful for filtering the log messages based on the clients that have sent them.

- **Local address**

  Optional parameter; on multihomed machines (i. e. machines with multiple addresses), this specifies to which local address rsyslog is bound. If no address is specified it defaults to `0.0.0.0`, so that rsyslog listens on every network interface. For more information, see the official documentation at https://www.rsyslog.com/doc/v8-stable/configuration/modules/imtcp.html.

Remote Mode Switched to Client

You can configure one or more clients, e.g. one server for kernel messages and another server for authentication messages.

To manage the **Clients** list:

- 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 **Add** dialogue, where you can define the following settings:

- **Remote address**

  IP address or hostname of the remote server

- **Remote port**

  Port on which the server listens for log messages

- **Transport protocol**

Protocol to be used for the transmission of log messages
Possible options:

- **TCP** (Default)
- **UDP**

- **Syslog facility**

Type of program for which log messages are created. (Default: Any)

- **Syslog level**

Severity level of the event. (Default: Any)

- **Syslog style template**

Format in which the messages are sent
Possible options:

- **RSYSLOG_TraditionalForwardFormat** (Default)
- **RSYSLOG_ForwardFormat**
- **RSYSLOG_SyslogProtocol23Format**
- **RSYSLOG_StdJSONFmt**

- **TLS enabled**

☑ TLS encryption for the transmission of log messages is enabled.

☐ Transmitted log messages are not encrypted. (Default)

- **CA certificate**

Path to the local CA root certificate file in PEM format which is used to verify the authenticity of the X.509 certificate of your log collector and analyzer. If the UMS is used to transfer the certificate file to devices, the same path and file name as in the UMS must be entered. Example: `/wfs/ca-certs/ca.pem`
For more information, see Logging and Log Evaluation.

Power Options

The following power option configurations are available in IGEL OS.

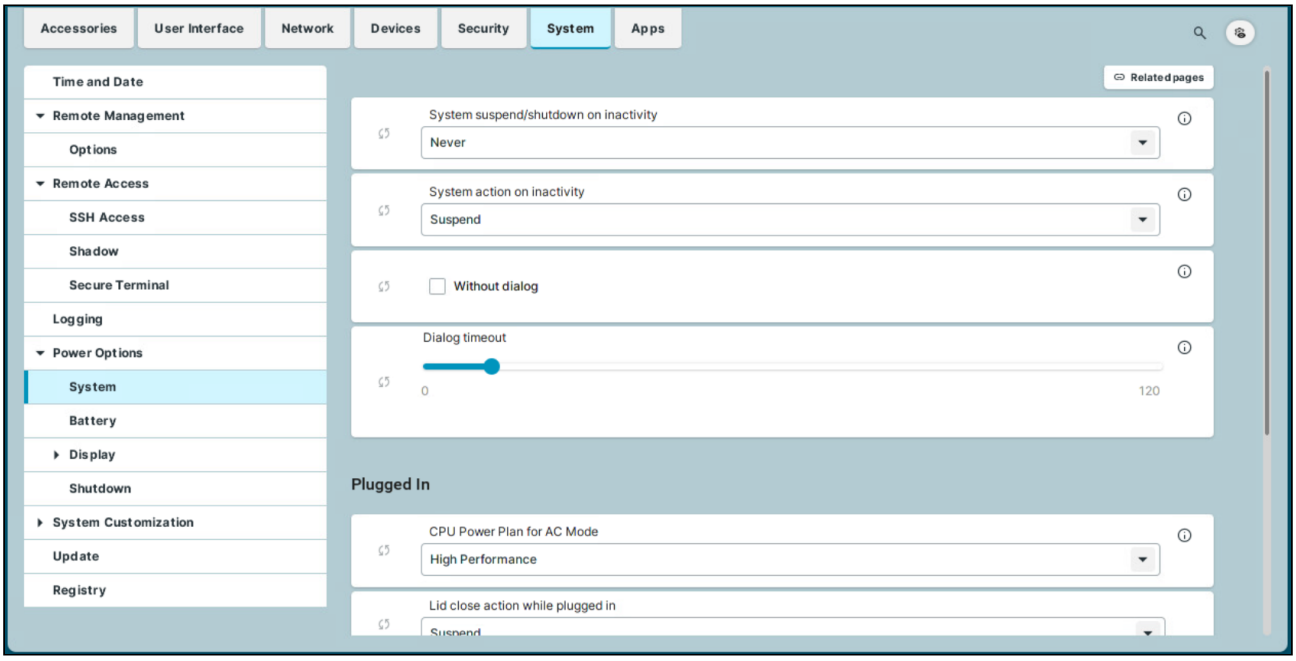
- System Power Options in IGEL OS 12 (see page 297)
- Battery (see page 300)
- Display (see page 302)
- Shutdown (see page 304)

System Power Options in IGEL OS 12

This article shows how to configure settings for energy saving on your IGEL OS device. You can configure the behavior after a time of inactivity and the CPU power plan.

> **Display of Energy Star Logo on Selected HP Endpoint Devices**
>
> With selected Hewlett-Packard (HP) endpoint devices, the Energy Star certification mark is displayed on this Setup page.

Menu path: **System > Power Options > System**



System suspend/shutdown on inactivity

Specify how long the user can be inactive before the system switches to standby mode or shuts down, depending on the **System action on inactivity** setting.
Possible values:

- **Never** (Default)
- **After 1 minute**
- **...**
- **After 24 hours**

System action on inactivity

Possible options:

- **Suspend**: The system is set to standby mode after the timeout defined under **System suspend/shutdown on inactivity**. (Default)
- **Shutdown**: The system is shut down after the timeout defined under **System suspend/shutdown on inactivity**.

Without dialog

☑ The user is not asked if the system is to be set to standby mode.

☐ The dialog asking for user confirmation is shown. (Default)

Dialog timeout

Time in seconds, for which the dialog is to be displayed. (Default: 10 seconds)

Plugged In

CPU power plan for AC mode

The CPU power plan (CPU Governor) used in AC mode
Possible options:

- **High performance**: Full performance with maximum processor speed. (Default)
- **Balanced**: Slower regulation of performance in a balanced manner according to the demands of programs.
- **Power saver**: Lowest processor speed

> ⓘ You can also use the battery tray app to set the CPU power plan for the current mode in use (AC or battery). For details, see Battery (see page 300).

Lid close action while plugged in

The action that is performed when the lid of the device gets closed.

Possible options:

- **Suspend**: When the lid gets closed, the device goes into suspend mode and applications are closed. When the lid is opened again, the device starts, connections are restarted, and re-login is required. Applications have to be started manually. (Default)

  > ⓘ The suspend action is only performed if there are no external displays connected and activated. When an external display is connected and activated, the internal display is turned off, and if the internal display was the primary display, a new primary display is assigned.

- **Turn off display**: When the lid gets closed, the internal display is turned off.

On Battery

CPU power plan for battery mode

The CPU power plan (CPU Governor) used in battery mode
Possible options:

- **High performance**: Full performance with maximum processor speed
- **Balanced**: Regulation of performance in a balanced manner according to the demands of programs. (Default)
- **Power saver**: Lowest processor speed

> You can also use the battery tray app to set the CPU power plan for the current mode in use (AC or battery). For details, see Battery (see page 300).

Lid close action while not plugged in

The action that is performed when the lid of the device gets closed.

Possible options:

- **Suspend**: When the lid gets closed, the device goes into suspend mode and applications are closed. When the lid is opened again, the device starts, connections are restarted, and re-login is required. Applications have to be started manually. (Default)

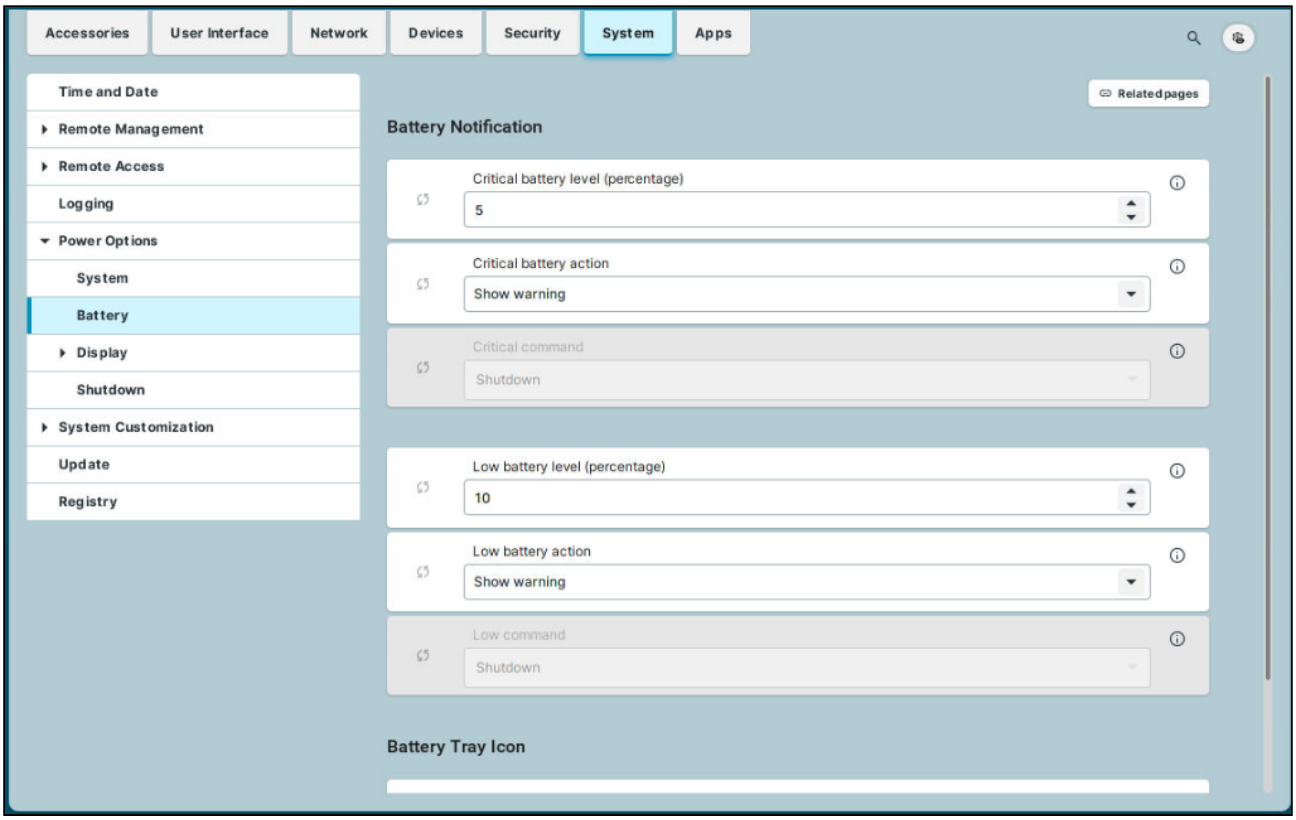
  > The suspend action is only performed if there are no external displays connected and enabled. When an external display is connected and activated, the internal display is turned off, and if the internal display was the primary display, a new primary display is assigned.

- **Turn off display**: When the lid gets closed, the internal display is turned off.

Battery

This article shows battery settings options in IGEL OS.

Menu path: **System > Power Options > Battery**



Battery Notification

Critical battery level (percentage)

Percentage of remaining battery charge deemed critical. (Default: 5)

Critical battery action

Action to be taken in the event of a critical charge level
Possible options:

- **Do nothing**
- **Show warning** (Default)

- **Run command**
- **Run command in terminal**

Critical command

Command that is executed when a critical charge level is reached. (Default: Shutdown)

Low battery level (percentage)

Percentage of remaining battery charge deemed low. (Default: 10)

Low battery action

Action to be taken in the event of a low charge level
Possible options:

- **Do nothing**
- **Show warning** (Default)
- **Run command**
- **Run command in terminal**

Low command

Command that is executed when a low charge level is reached. (Default: Shutdown)

Battery Tray Icon

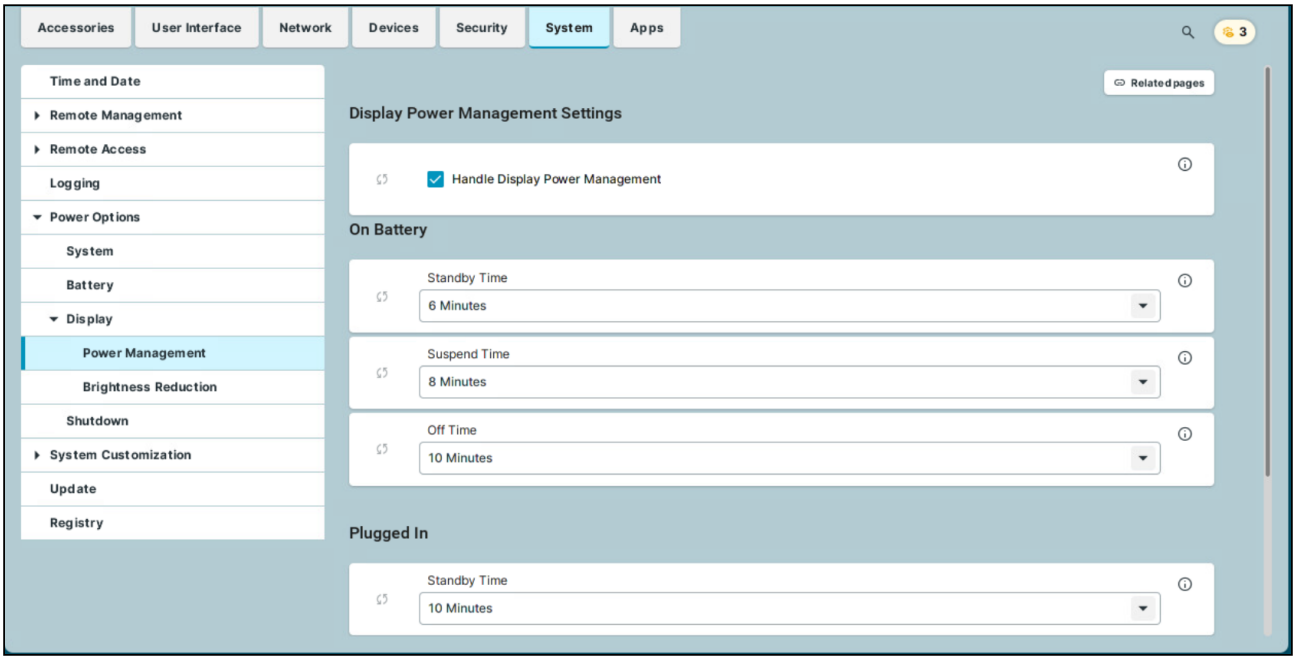
Show battery tray icon on desktop

☑ The battery icon is shown in the taskbar. The icon is dynamic and represents the state of the battery charge. For example, is displayed when the battery is charging. Hover over the icon to see information on the charge. Clicking the icon displays the battery tray app. For more information on the battery tray app, see Tray Applications in IGEL OS 12 (see page 353). (Default)

Display

This article shows how to configure energy-saving stages in IGEL OS.

Menu path: **System > Power Options > Display > Power Management / Brightness Reduction**



Power Management

Handle display power management

☑ The DPMS energy saving functions are enabled. (Default)

> The screen must support Display Power Management Signaling (DPMS).

On Battery / Plugged In

You can select time frames after which energy-saving modes get activated. The time frames are configured separately for **On Battery** and **Plugged In** use of the device. When **Never** is selected, the energy-saving mode is disabled.
The following energy-saving modes can be configured:

- **Standby Time**
  After this time frame the device goes to standby mode.

- **Suspend Time**
  After this time frame the device goes to sleep mode.
- **Off Time**
  After this time frame the device turns off.

Brightness Reduction

If a device is switched on but not used for some time, energy can also be saved by brightness reduction. The values of the reduction are configured separately for **On Battery** and **Plugged In** use of the device.

On Battery / Plugged In

On inactivity reduce to

The percent value to which the brightness is reduced after a period of inactivity.

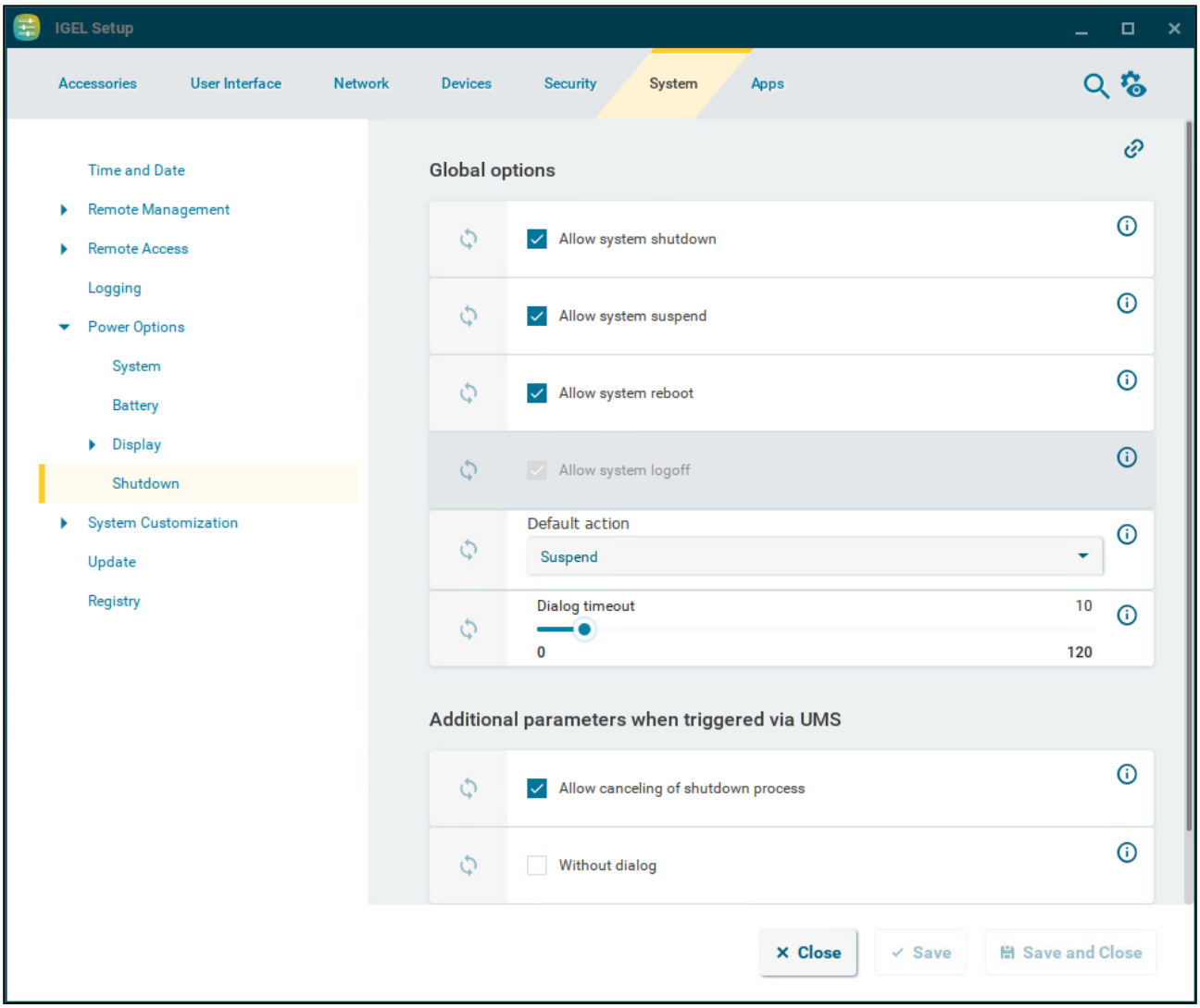
Reduce after

The period of inactivity after which brightness is reduced. You can set the period between 10-120 seconds. Setting the value to 9 deactivates the reduction.

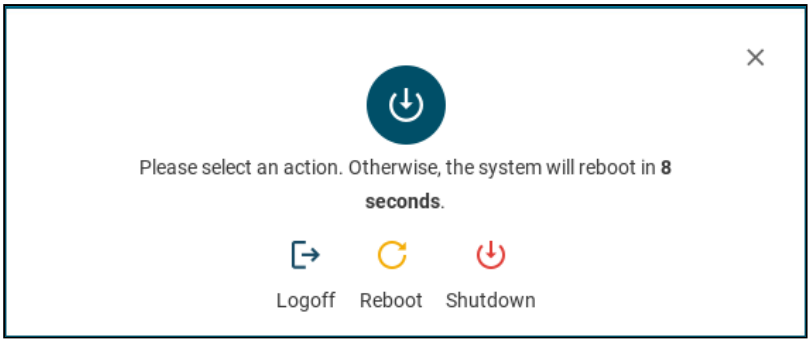
Shutdown

This article shows the options to configure the behavior of shutdown menu in IGEL OS. The shutdown menu button can be displayed in the start menu and in the Application Launcher. For more information, see Start Menu (see page 81). You can also configure the shutdown menu as a command session and configure various starting methods. For more information, see Commands (see page 129).

Menu path: **System > Power Options > Shutdown**



By default, when the user clicks the shutdown button, an information dialog is displayed. The user can select from the enabled actions or cancel the procedure by closing the window by clicking X or by pressing [Esc].



Global Options

Allow system shutdown

☑ The user can shut down the device. The **Shutdown** button is shown in the info dialog. (Default)

☐ The user cannot shut down the device. The **Shutdown** button is not shown in the info dialog.

Allow system suspend

☑ The user can suspend the device. The **Suspend** button is shown in the info dialog. (Default)

☐ The user cannot suspend the device. The **Suspend** button is not shown in the info dialog.

Allow system reboot

☑ The user can reboot the device. The **Reboot** button is shown in the info dialog. (Default)

☐ The user cannot reboot the device. The **Reboot** button is not shown in the info dialog.

Allow system logoff

☑ The user can log off the device, if the user is logged in. The **Logoff** button is shown in the info dialog. (Default)

☐ The user cannot log off the device. The **Logoff** button is not shown in the info dialog.

> To configure the option, at least one login method needs to be enabled under **Security > Logon**. For more information, see Logon (see page 250).

Default action

The action that is carried out if the timeout defined under **Dialog timeout** expires.
Possible options:

- **Shutdown**
- **Suspend** (Default)
- **Reboot**

- **Logoff**
- **Cancel**

Dialog timeout

Time (in seconds) after which the info dialog will close and the action specified under **Default action** will be carried out. If the value is set to 0, the dialog will be shown until the user selects one of the possible actions. (Default: 10)

Additional Parameters When Triggered via UMS

> **Known Issue**
>
> For OS version 12.2.0, the parameters of the **Additional Parameters When Triggered via UMS** are not effective. The parameters will be reworked in a future release.

Allow canceling of shutdown process

☑ The user can cancel the shutdown procedures initiated from the UMS by clicking the **Cancel** button in the info dialog. (Default)

☐ The user cannot cancel the procedures.

> For the manual cancellation to work, the following parameters need to be configured:
> - **Without dialog** needs to be disabled.
> - **Prompt user on UMS actions** under **System > Remote Management** needs to be enabled. For details, see Remote Management (see page 279).

Without dialog

☑ The info dialog is not shown. The shutdown procedures initiated from the UMS are carried out without notification.

☐ The info dialog is shown. (Default)

System Customization

You can use the following configuration to customize your IGEL OS.

- Custom Partition (see page 308)
- Custom Application (see page 314)
- Custom Commands (see page 318)
- Corporate Design (see page 326)
- Environment Variables (see page 341)

Custom Partition

In IGEL OS, a custom data partition is available for use as required. A download/update function that loads data from a server and, where appropriate, updates them can be set up for this custom storage area.

Menu path: **System > System Customization > Custom Partition**

⚠ The IGEL Support Team offers support for the deployment of Custom Partitions. However, it is not possible to offer support for any third-party software that is installed on a Custom Partition.

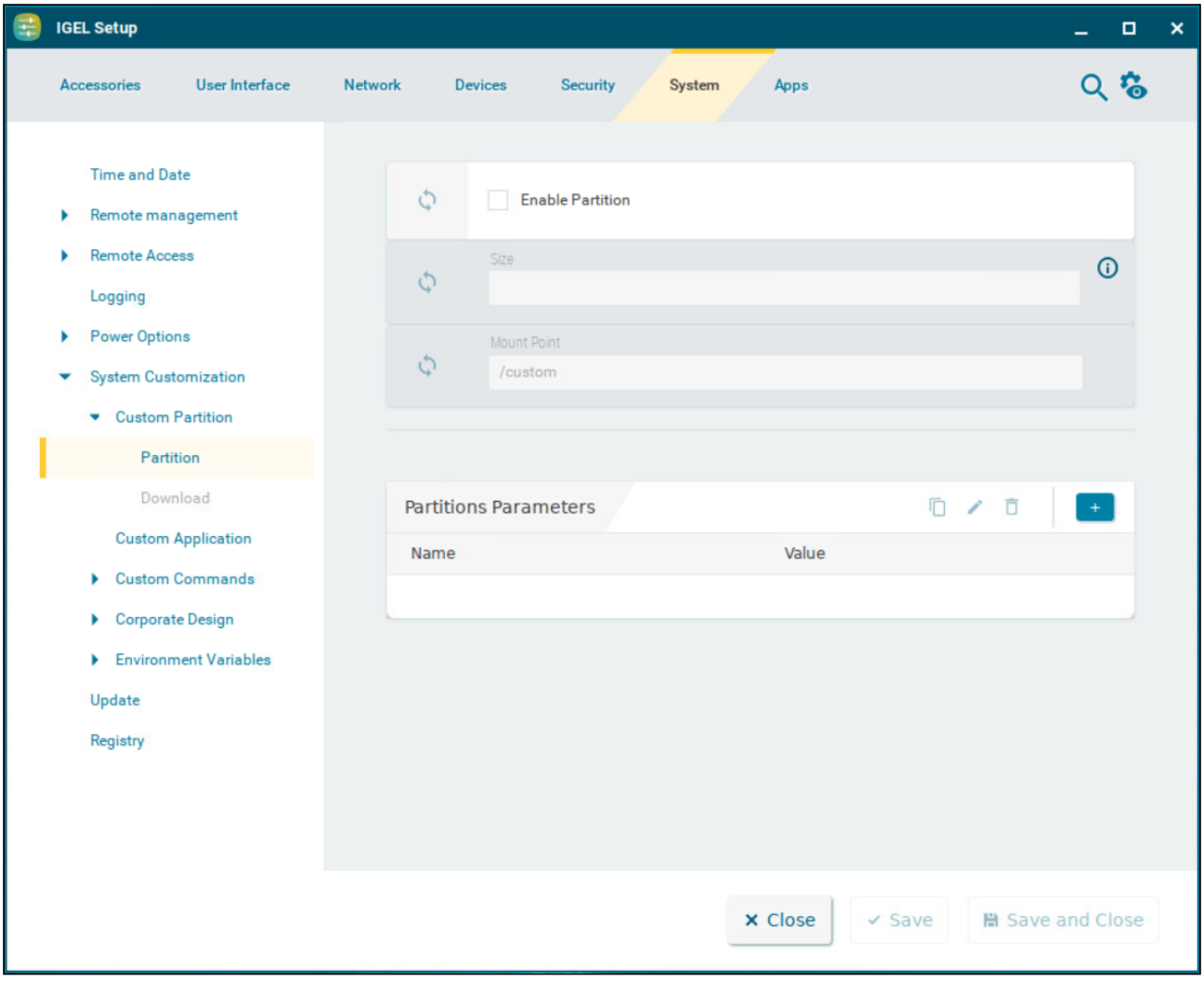
If the device is reset to the default settings (factory reset), the custom partition and all data stored on it will be deleted.

- Partition (see page 309)
- Download (see page 311)

Partition

This article shows how to configure options to use a custom partition of your own in IGEL OS.

Menu path: **System > System Customization > Custom Partition > Partition**



Enable partition

☑ The use of custom partitions is enabled.

☐ Custom partitions cannot be used. (Default)

Size

Size of the partition in bytes. The number can be followed by a multiplicative ending, without a space in between.
Example: "100K" stands for 100 Kibibytes, that is, 100 * 1024 bytes.
The following multiplicative endings are possible:

- k for Kilobytes
- K for Kibibytes (number * 1024)
- m for Megabytes
- M for Mebibytes (number * 1024 * 1024)
- g for Gigabytes
- G for Gibibytes (number * 1024 * 1024 * 1024)

Sensible values are for example "100K" (for 100 KiB = 100 * 1024 bytes) or "100M" (for 100 MiB = 100 * 1024 * 1024 bytes). The size of the partition should be set to at least 100 KiB. However, no more than 300 MiB should be reserved for the customer-specific partition (based on the 1 GB standard CF used in IGEL Linux thin clients). This is because subsequent firmware updates may require more storage space than the current version.

Mount point

Path on which the partition is to be mounted. (Default: `/custom`)

Partitions Parameters

You can enter name value pairs which are passed on to the custom partition for further processing.
To manage the list:

- 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 **Add** dialogue, where you can define the following settings:

- **Name**

  Name of the parameter

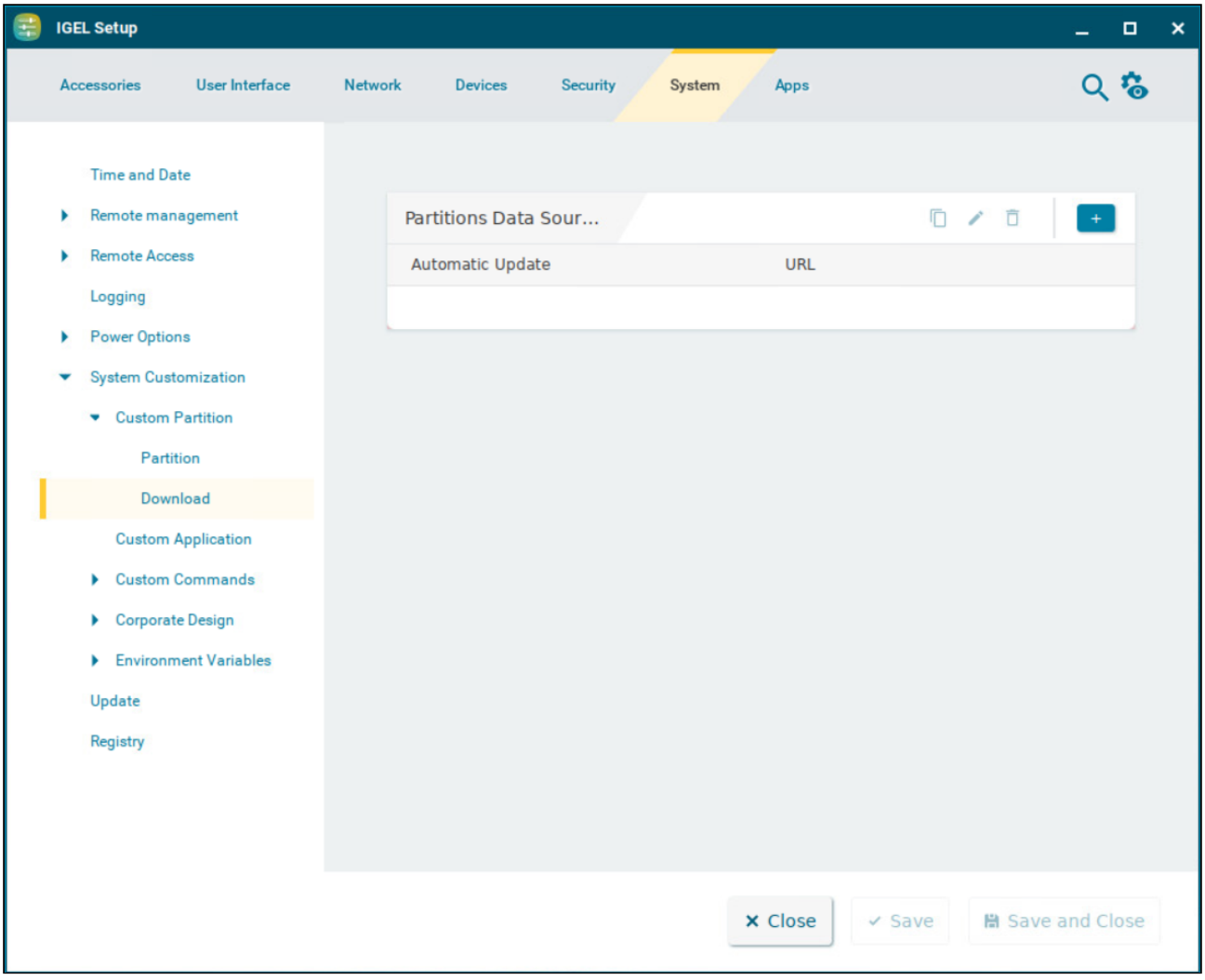
- **Value**

  Value of the parameter

Download

This article shows how to set up data sources for the custom partitions in IGEL OS.

Menu path: **System > System Customization > Custom Partition > Download**



Partitions Data Sources

In order to load data onto the custom partition, at least one partition data source must be set up here.

To manage the list, proceed as follows:

- Click + to create a new entry.

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

Clicking brings up the **Add** dialogue, where you can define the following settings:

- **Automatic update**
  ☑ The contents from this source will be updated automatically.
  ☐ The contents from this source will not be updated automatically. (Default)
- **URL**

  URL of the web server

- **User name**

  User name for access to the web server

- **Password**

  Password for access to the web server. Click **Set password** to save the password. Click **Change password** to change the password.

- **Initial action**

  Action which is performed after mounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be launched.

- **Final action**

  Action which is performed before unmounting the partition (program or script with absolute path). For example, a program downloaded to the partition can be ended.

The transfer protocols are the same as the ones for updating the firmware, e.g. HTTP and HTTPS. An `INF` file which in turn references a tar archive zipped using bzip2 must be referenced as the target.
The structure of the INF file is as follows:

`[INFO], [PART]`	Header information
`file="test.tar.bz2"`	File name of the compressed tar archive
`version="1"`	Version number - a higher version results in an update if Update automatically is enabled.

The files to be transferred must therefore be zipped in a tar archive which is then compressed using bzip2. This file is referenced in the INF file which is the target of the URL.

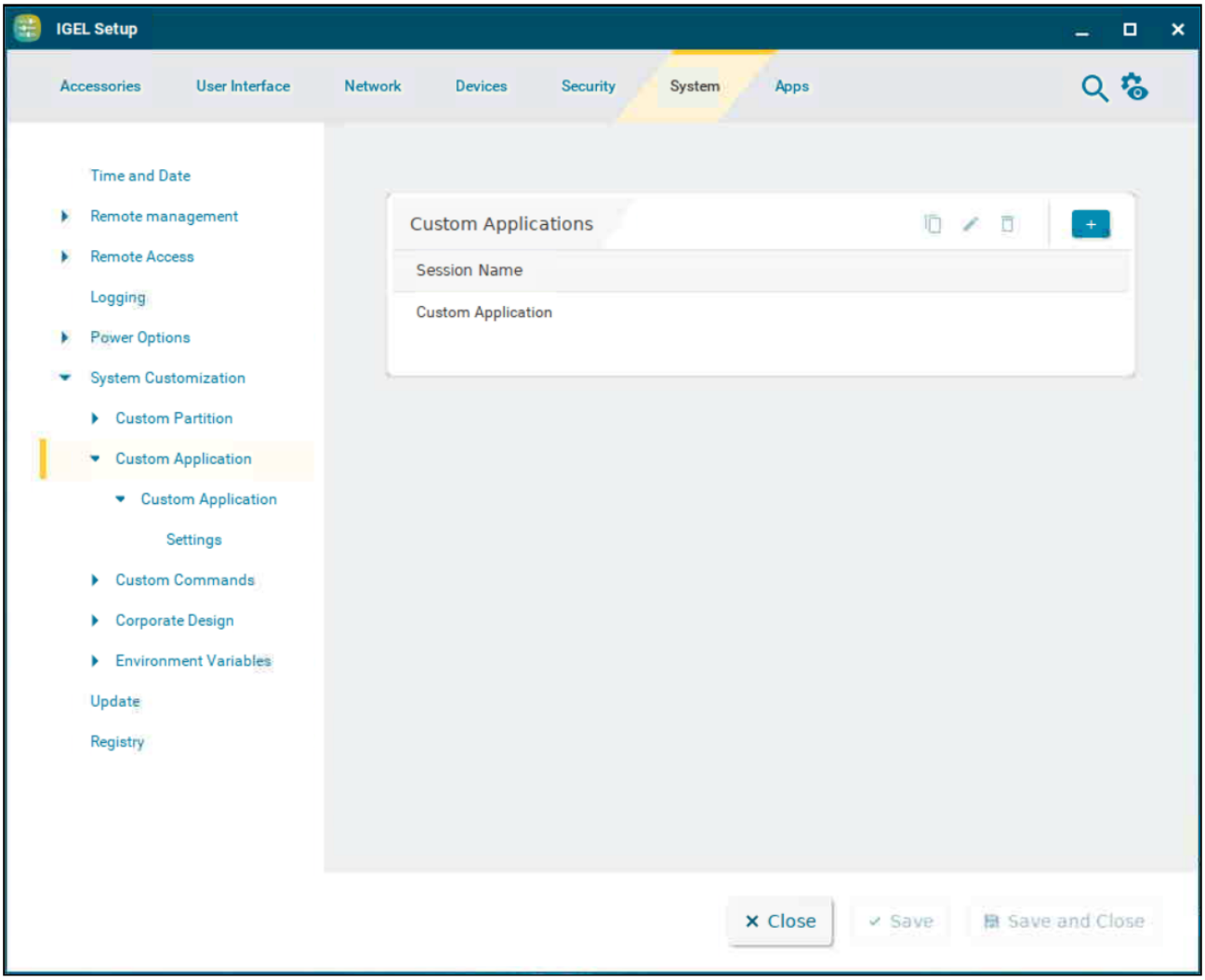
The tar archive can be created under Windows, e.g. with the open source program 7-Zip (www.7-zip.de[20]). This program also allows `bzip2` compression. Under Linux, tar and bz2 files can be created using onboard resources.
The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The `Version` parameter in the `INF` file must be increased for this purpose.

20 http://www.7-zip.de/

Custom Application

You can configure the starting options for an application that was loaded onto a customer partition once it is defined as a custom application. To do this, give the command to call up the application under **System Customization > Custom Application > Settings**. For more information, see Settings (see page 316).

Menu path: **System > System Customization > Custom Application**

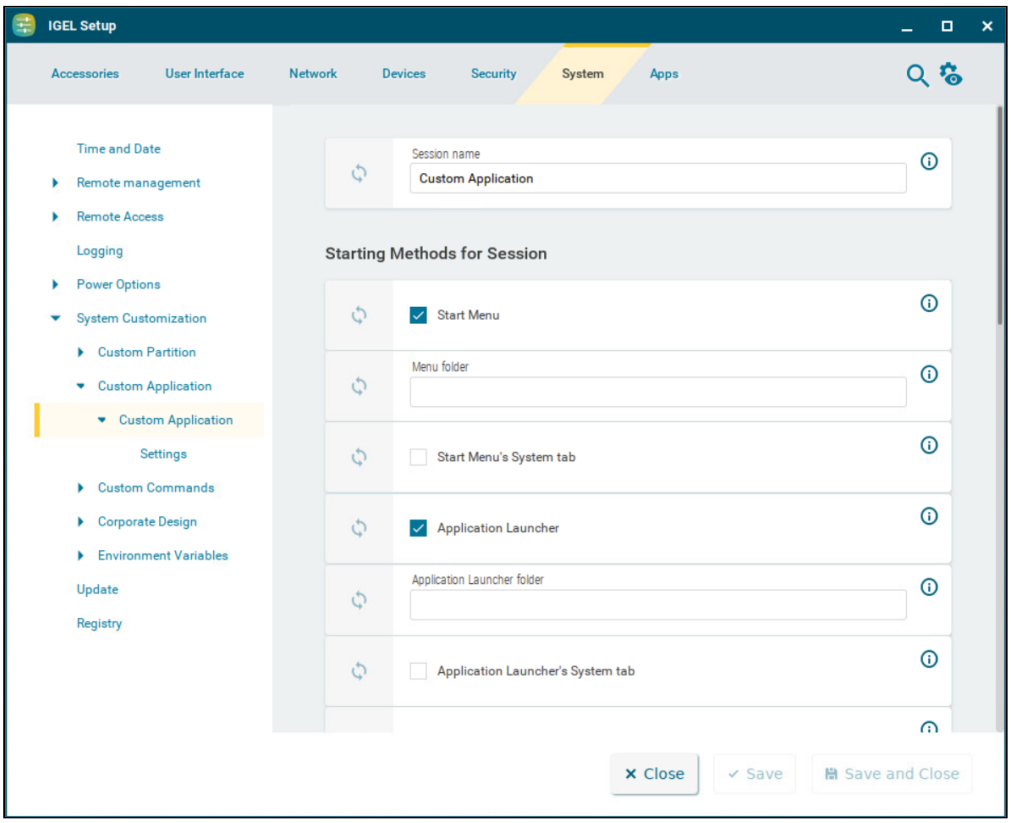


Custom Applications

To manage the list of custom applications:

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

▶ Click + to define the starting options for the custom application.

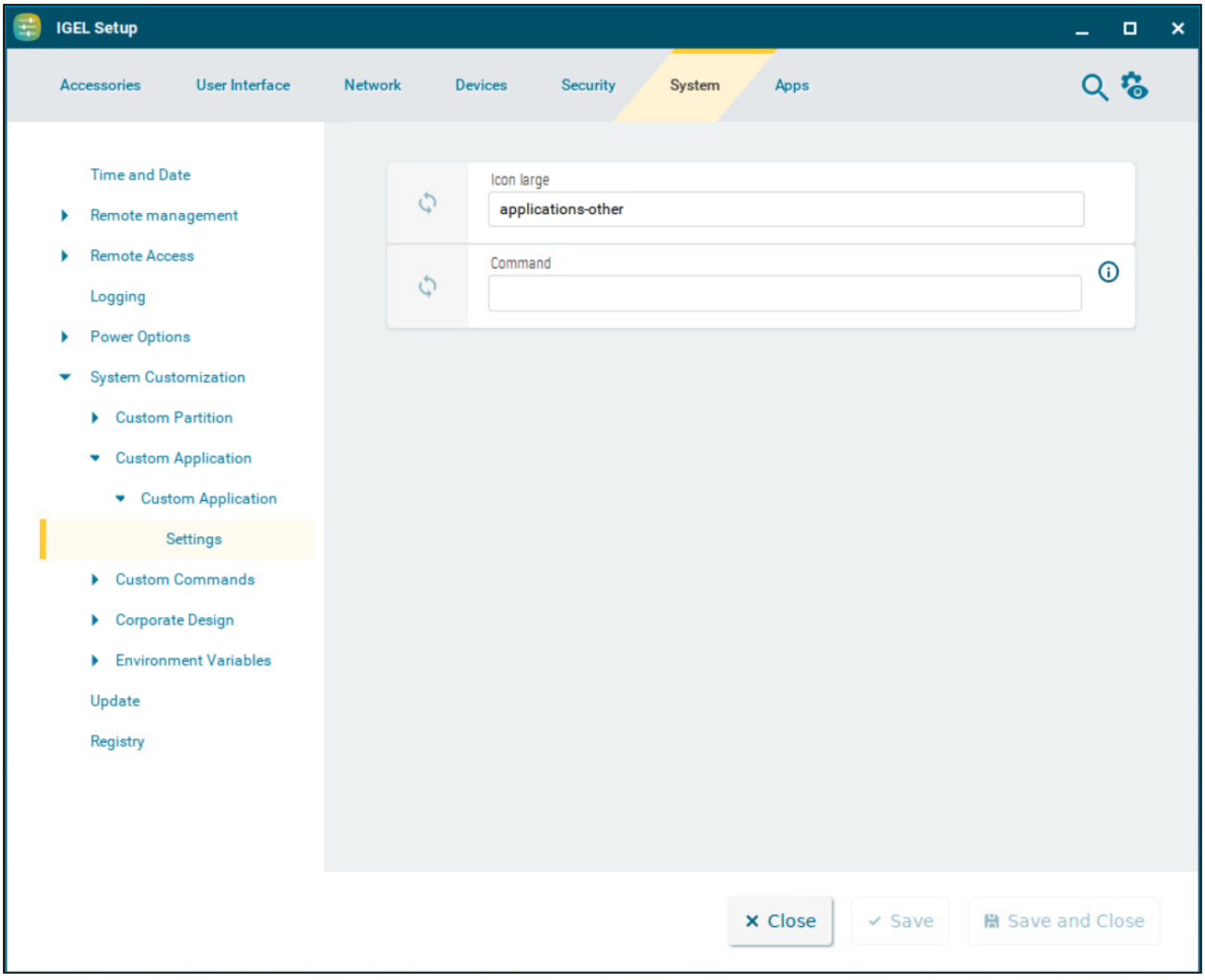


The starting methods parameters are described under Starting Methods for Apps (see page 376).

Settings

This article shows how to define a command for calling up an application in IGEL OS.

Menu path: **System > System Customization> Custom Application > [Custom Application Name] > Settings**



Icon large

Select an icon provided. (Default: applications-other)

> Only the desktop icon of a session is customizable. The taskbar icon of a session cannot be customized and will remain the default icon. Complete customization is not possible.

Command

Give the name and path of the application. (Example: `/usr/bin/gpicview`)

Custom Commands

Custom commands are executed at specific points of the system startup process. You can use environment variables in your custom commands. For more information on environment variables, see Environment Variables (see page 341).

> ⚠ The content of custom scripts used in the custom command fields cannot be supported by IGEL. Therefore, you may be requested to remove custom scripts as part of the troubleshooting/support process.

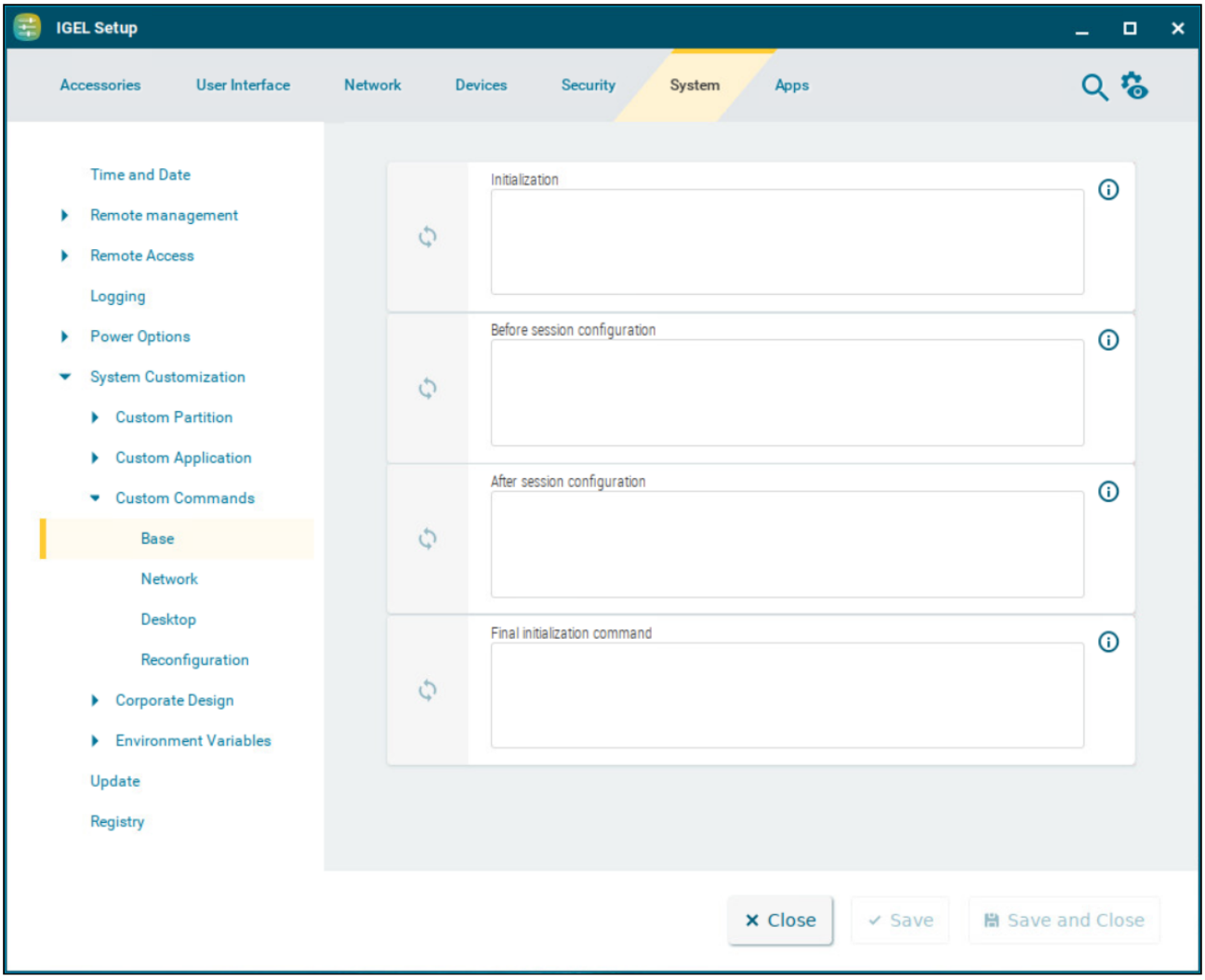
You can define custom commands for the following startup processes:

- Base (see page 319)
- Desktop (see page 321)
- Network (see page 323)
- Reconfiguration (see page 325)

Base

The commands defined here are executed at the specific execution times during the boot process.

Menu path: **System > System Customization > Custom Commands > Base**



You can define commands for the following execution times:

Initialization

The command is executed during boot, at the beginning of initialization. At this point:

- Not all drivers are loaded, not all devices are available

- Network scripts are not launched, network is not available
- Partitions are available, except for *firefox profile, scim data, ncp data, custom partition*

Before session configuration

The command is executed during boot, before the session configuration. At this point:

- Not all drivers are loaded, not all devices are available
- Network scripts are not launched, network is not available
- Partitions are available, except for *firefox profile, scim data, ncp data, custom partition*
- Sessions are not configured

After session configuration

The command is executed during boot, after the session configuration. At this point:

- All drivers are loaded, all devices are available
- Network is available
- Partitions are available, except for *custom partition*
- System daemons are not launched (CUPS, ThinPrint etc.)
- Sessions are configured
- UMS settings are retrieved but not yet effective

Final initialization command

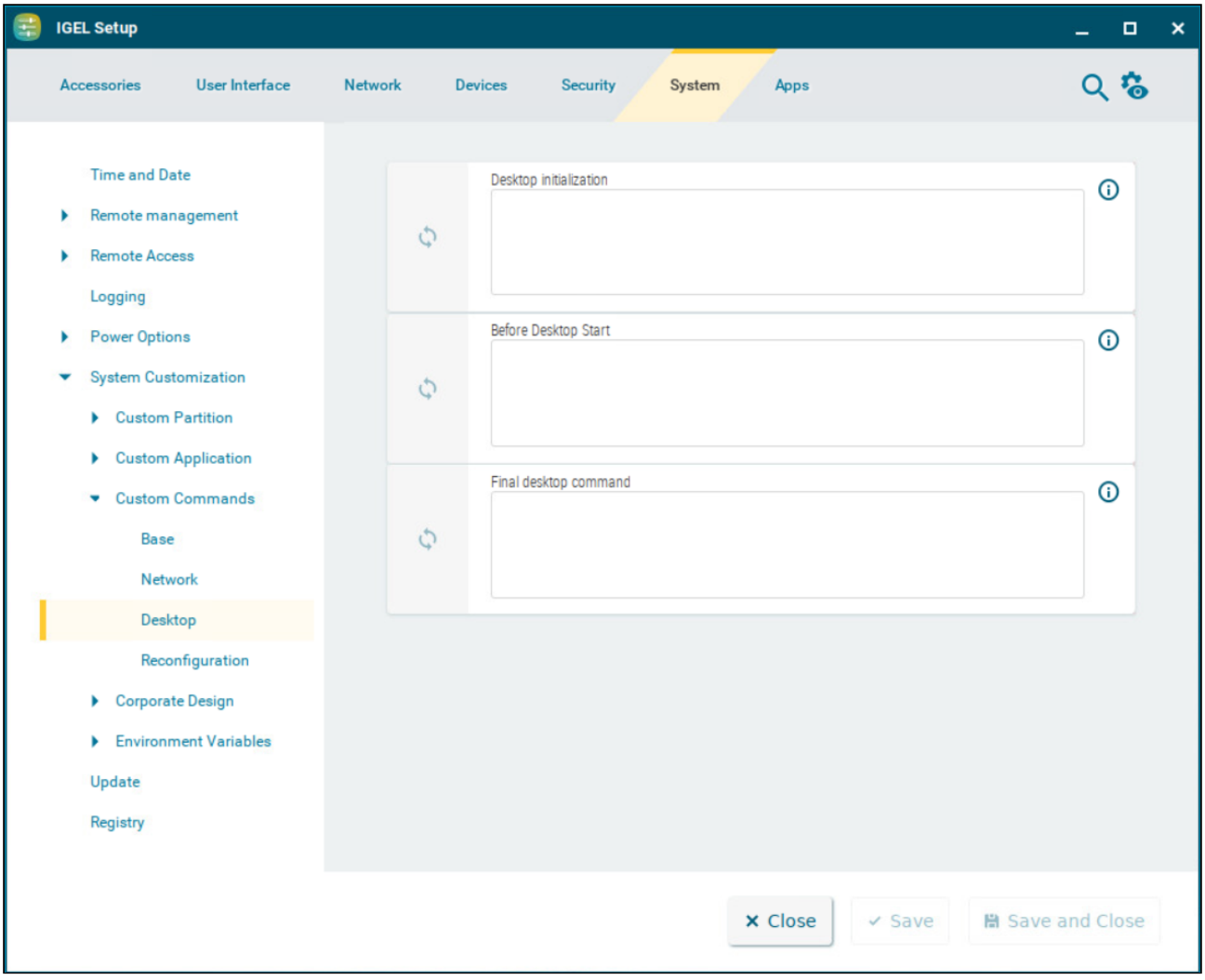
The command is executed during boot, after the initialization. At this point:

- All partitions are available
- All system daemons are launched
- UMS settings are effective

Desktop

The commands defined here are executed at the specific execution times when the X server is launched.

Menu path: **System > System Customization > Custom Commands > Desktop**



You can define commands for the following execution times:

Desktop initialization

The command is executed during the boot process, before the X server is started. At this point:

- Desktop environment is configured but not launched

- User is not logged on (Kerberos, smartcard etc.)

Before desktop start

The command is executed before the windowmanager and the autostart sessions are started. At this point:

- Desktop environment is launched
- Message service is launched
- Session D-Bus is launched
- User is not logged on (Kerberos, smartcard etc.)

Final desktop command

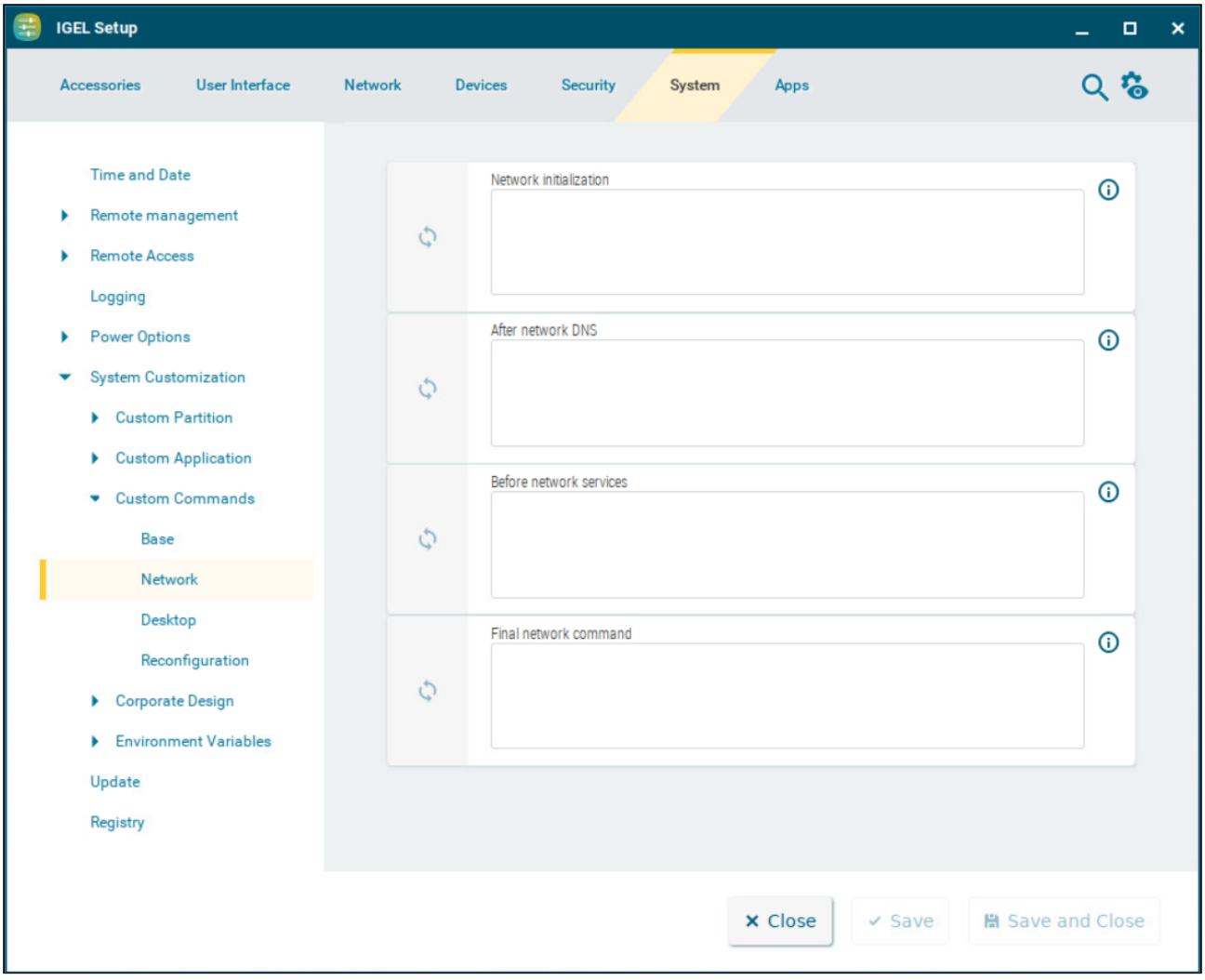
The command is executed after each user logon and desktop restart. At this point:

- User is logged on (Kerberos, smartcard etc.)
- User desktop is launched

Network

You can define commands for network-related execution times.

Menu path: **System > System Customization > Custom Commands > Network**



You can define commands for the following execution times:

Network initialization

The command is executed at the beginning of the network configuration.

The commands in the below fields are executed each time the relevant network interface starts.
The `INTERFACE` environment variable contains the name of the network interface started.

After network DNS

The command is executed after each change in the IP address or host name / after each DNS configuration. At this point:

- IP address / name server settings are used (e.g. via DHCP)

Before network services

The command is executed before network services are started. At this point:

- IP address / name server settings are used
- VPN is connected (if VPN autostart was enabled in the setup)
- No network / host routing settings used

Final network command

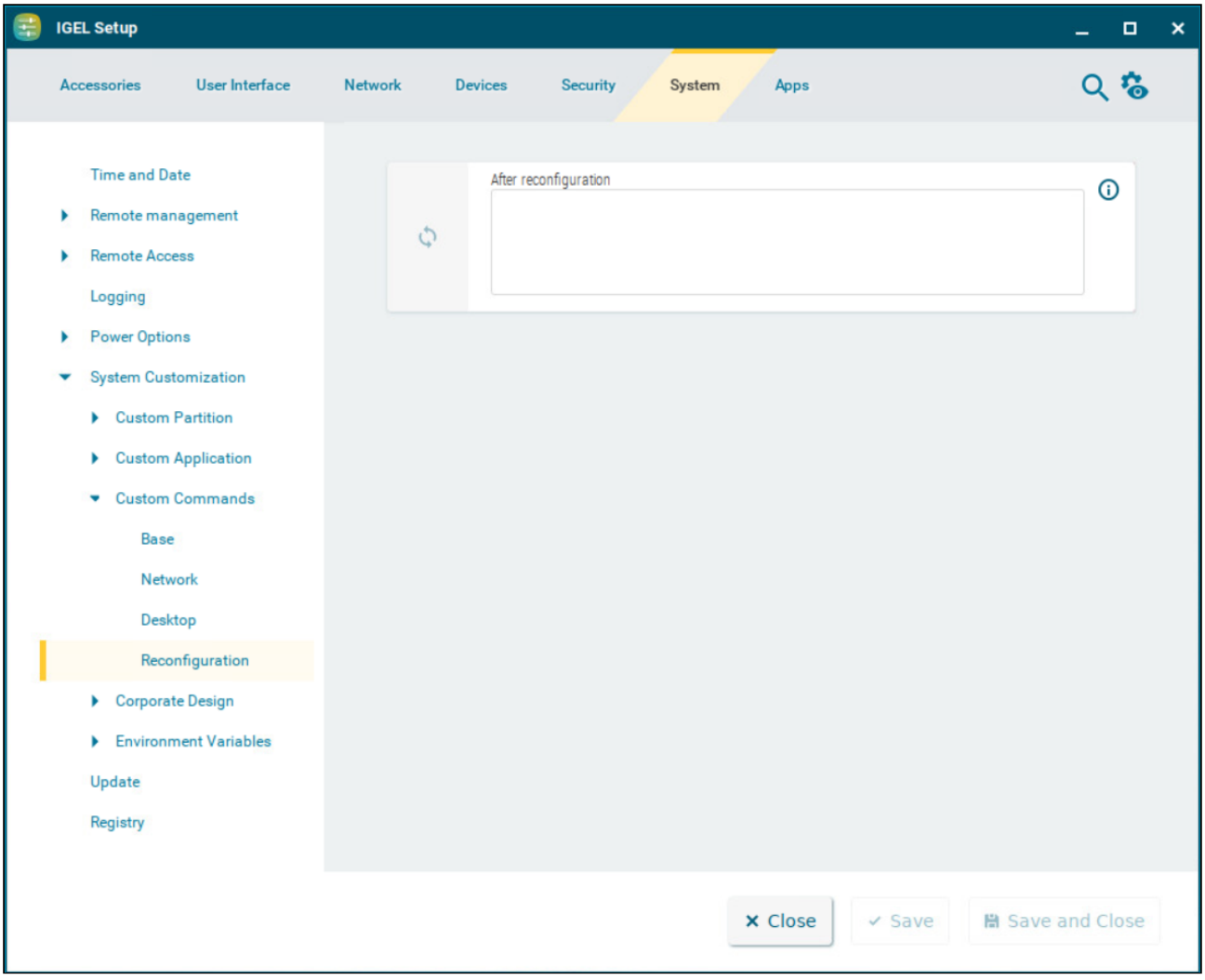
The command is executed after network configuration is finished. At this point:

- Network / host routing settings are used
- NFS and SMB drives are available
- System time is synchronized with the time server
- UMS settings are retrieved but not effective yet

Reconfiguration

The command defined here is executed after settings relating to the local setup or the UMS have been changed.

Menu path: **System > System Customization > Custom Commands > Reconfiguration**



After reconfiguration

The command is executed after an effective change in the endpoint device settings (local setup, UMS).

Corporate Design

In this area, you can configure settings allowing you to adapt the user interface to your needs.

Use the settings on the following pages to create your design:

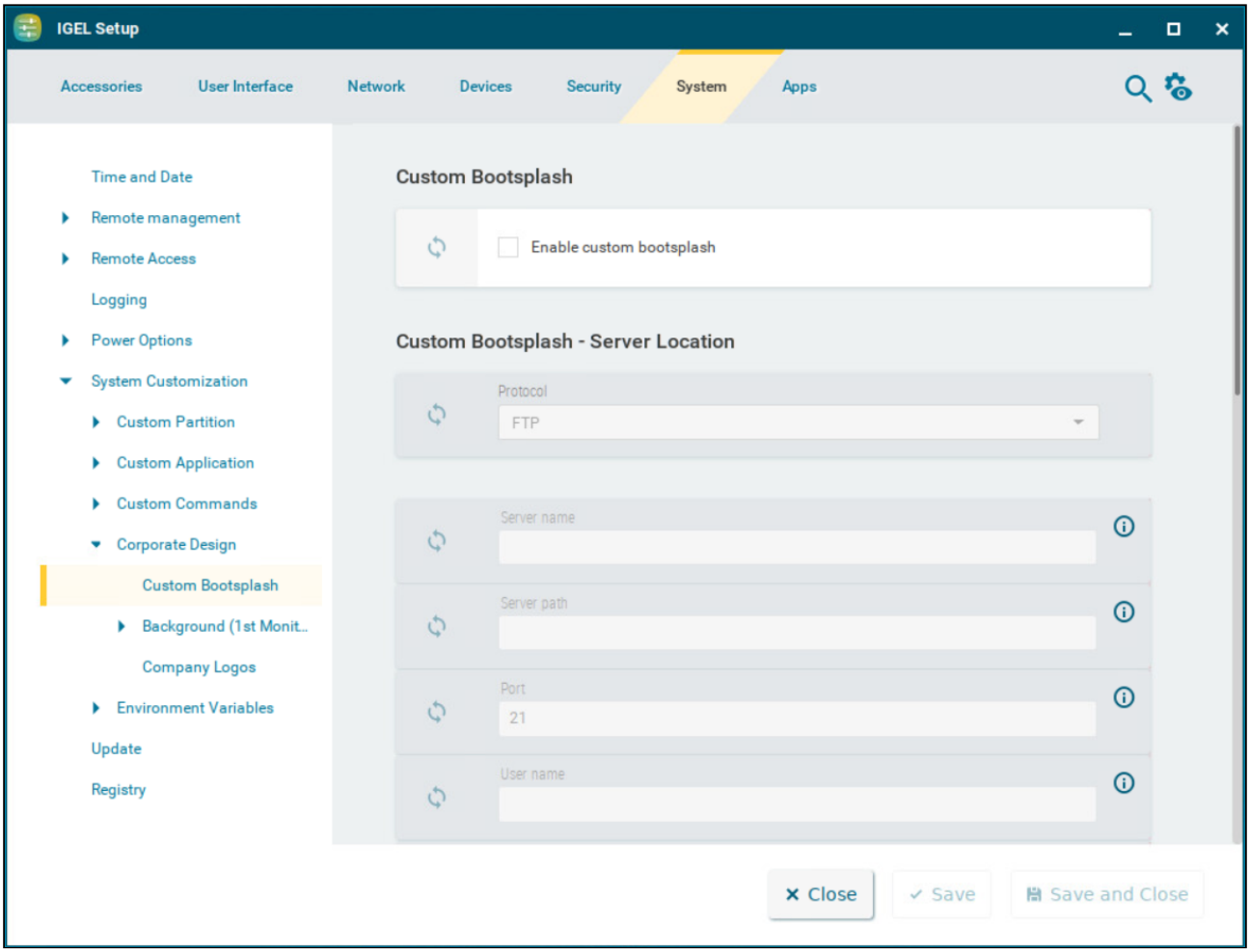
- Custom Bootsplash (see page 327)
- Background (1st Monitor) (see page 330)
- Company Logos (see page 338)

Custom Bootsplash

With a bootsplash, you can show your company logo or a specific image during the booting procedure. The bootsplash will be shown instead of the console messages. You need to provide an image file for your custom bootsplash on a download server.

> The file types JPG, JPEG, BMP, PNG, SVG, GIF, and TIFF can be used for a bootsplash. A total storage area of 25 MB is available for all user-specific images. The image is 800 x 600 pixels in size (aspect ratio remains unchanged). It can be positioned vertically and horizontally.

Menu path: **System > System Configuration > Corporate Design > Custom Bootsplash**



Custom Bootsplash

Enable custom bootsplash

☑ A custom bootsplash can be configured.

☐ No custom bootsplash is configured. (Default)

Custom Bootsplash - Server Location

Protocol

Access method for the image
Possible options:

- **HTTP**: Download from a web server
- **HTTPS**: Download from a TLS/SSL-secured web server
- **FTP**: Download from an FTP server. (Default)
- **Secure FTP**: Download via SSH-secured FTP
- **FTPS**: Download from a TLS/SSL-secured FTP server
- **FILE**: The image file lies in the file system of the device, possibly as a shared NFS or Windows update. You can enter the location under **Local path**.

Local path

The path to the background image. The parameter is shown when **FILE** is selected as protocol.

Server name

Name or IP address of the server

Server path

Path to the directory with the image file on the server

Port

Port of the server on which the service is provided. The field is populated by protocol specific default values.

User name

User name on the server

Password

Password for the user account on the server

Custom Bootsplash - Settings

Custom bootsplash file

Filename of the custom image

Custom bootsplash style

- **Original** (Default)
- **Stretched**
- **Scaled**
- **Zoomed**

Background color

The background color of the bootsplash. Click the color preview square to open the color selector.

Horizontal position of the bootsplash image

The following applies: 0 = left-justified, 50 = centered, 100 = right-justified. (Default: 50)

Vertical position of the bootsplash image

The following applies: 0 = aligned on top, 50 = centered, 100 = aligned on bottom. (Default: 50)

Size of progress indicator

Valid range is 72-256. (Default: 72)

Horizontal position of the progress indicator

The following applies: 0 = left-justified, 50 = centered, 100 = right-justified. (Default: 90)

Vertical position of the progress indicator

The following applies: 0 = aligned on top, 50 = centered, 100 = aligned on bottom. (Default: 90)

Bootsplash update

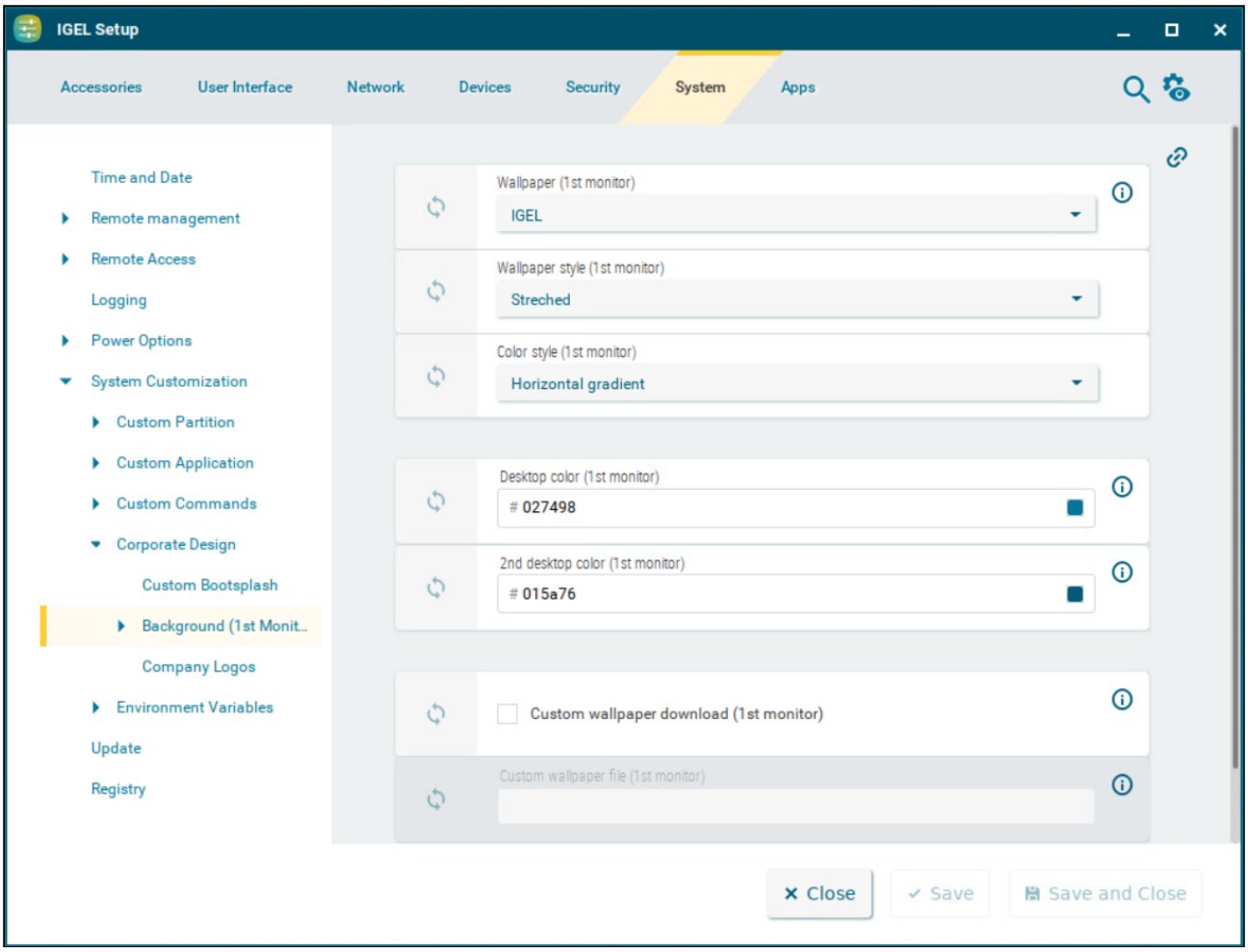
When clicked the user-specific bootsplash is downloaded from the given server.

> If you change the image file or even just one of the settings for an existing bootsplash, be sure to click **Bootsplash update** in order to regenerate the system files used.

Background (1st Monitor)

This article shows how to configure the desktop background for a corporate design in IGEL OS. You can use predefined IGEL backgrounds, a fill color/color gradient, or a background image of your own. You can set up different background images for each monitor connected to the device.

Menu path: **System > System Customization > Corporate Design > Background (1st Monitor)**



Wallpaper

Provides a selection of predefined IGEL backgrounds.
Possible options:

- **Neutral**
- **Off**

- **IGEL** (default)

Wallpaper style

Provides various design versions.
Possible options:

- **Auto**
- **Centered**
- **Tiled**
- **Stretched** (Default)
- **Scaled**
- **Zoomed**

Color style

Sets a fill color or a color gradient.
Possible options:

- **Solid color**
- **Horizontal gradient** (Default)
- **Vertical gradient**

Desktop color

The desktop color if **Wallpaper** is set to **Off**. Click the color preview square to open the color selector.

2nd desktop color

The second desktop color if **Wallpaper** is set to **Off** and a gradient **Color style** is selected. Click the color preview square to open the color selector.

Custom wallpaper download

☑ You can provide a user-specific background image on a download server. Specify the download server under **System > System Customization > Corporate Design > Background > Custom Wallpaper Server**.

☐ Custom wallpaper is not used. (Default)

Custom wallpaper file

The name of the background image file

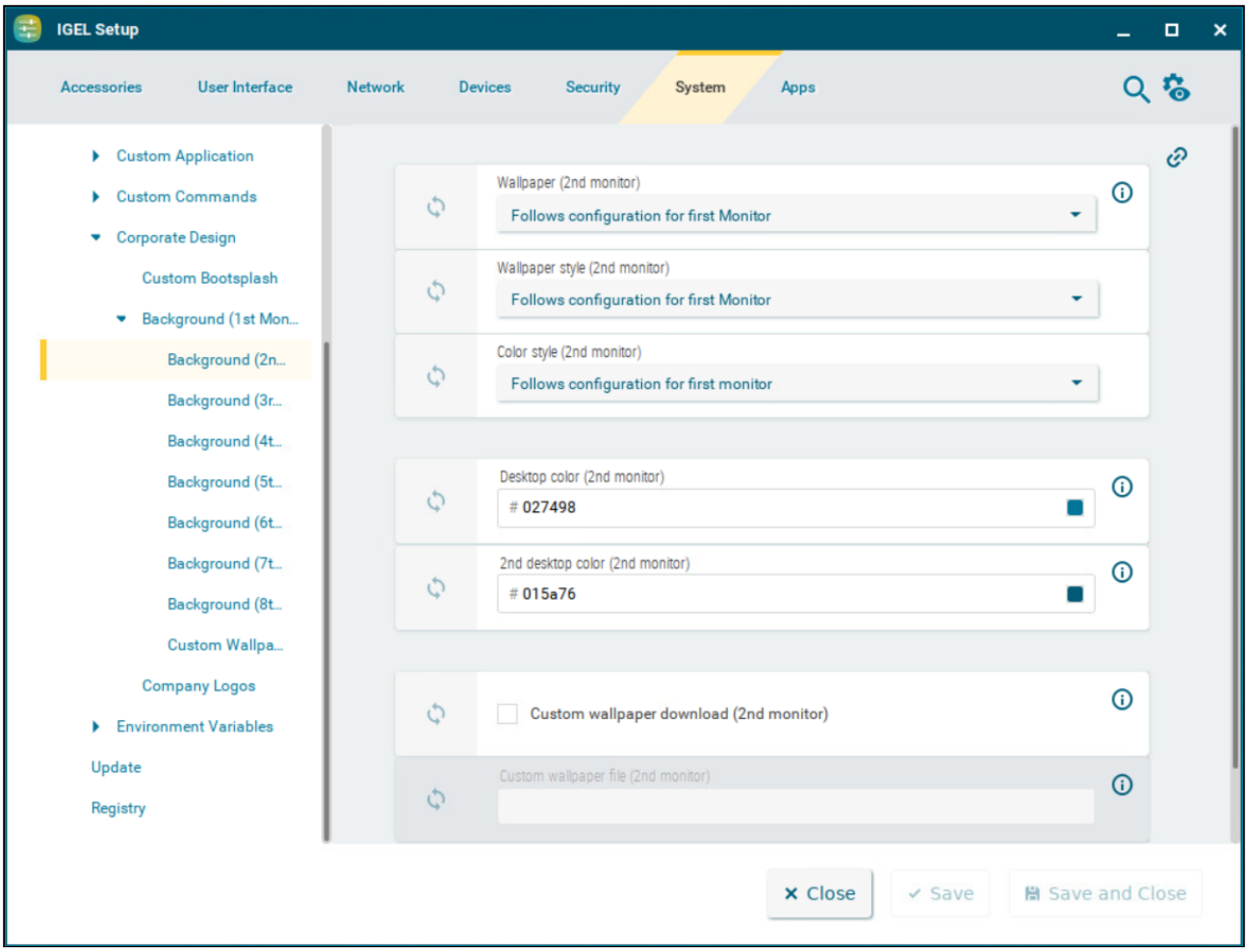
The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually by clicking **Wallpaper update** under **System > System Customization > Corporate Design > Background > Custom Wallpaper Server**. The download can also be launched from the IGEL Universal Management Suite (UMS) via the **Update desktop customization** command.

A user-specific image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an own background image and bootsplash. A total storage area of 25 MB is available for all user-specific images. For more information, see Firmware Customizations in the IGEL UMS.

Background (2nd-8th Monitor)

This article shows how to configure the desktop background of further monitors in multi-monitor environments in IGEL OS.

Menu path: **System > System Customization > Corporate Design > Background (2nd-8th Monitor)**



You can use predefined IGEL backgrounds, a fill color or a color gradient. You can also use a background image of your own.

> You can set up a separate background image for each monitor that is connected to the device.

Wallpaper

Provides a selection of predefined IGEL backgrounds.
Possible options:

- **Follows configuration for first monitor** (Default)
- **Neutral**
- **Off**
- **IGEL**

Wallpaper style

Provides various design versions.
Possible options:

- **Follows configuration for first monitor** (Default)
- **Auto**
- **Centered**
- **Tiled**
- **Stretched**
- **Scaled**
- **Zoomed**

Color style

Sets a fill color or a color gradient.
Possible options:

- **Follows configuration for first monitor** (default)
- **Solid color**
- **Horizontal gradient**
- **Vertical gradient**

Desktop color

The desktop color if **Wallpaper** is set to **Off**. Click the color preview square to open the color selector.

2nd desktop color

The second desktop color if **Wallpaper** is set to **Off**. Click the color preview square to open the color selector.

Custom wallpaper download

☑ You can provide a user-specific background image on a download server. Specify the download server under **System > System Customization > Corporate Design > Background > Custom Wallpaper Server**.

☐ Custom wallpaper is not used. (Default)

Custom wallpaper file

The name of the background image file

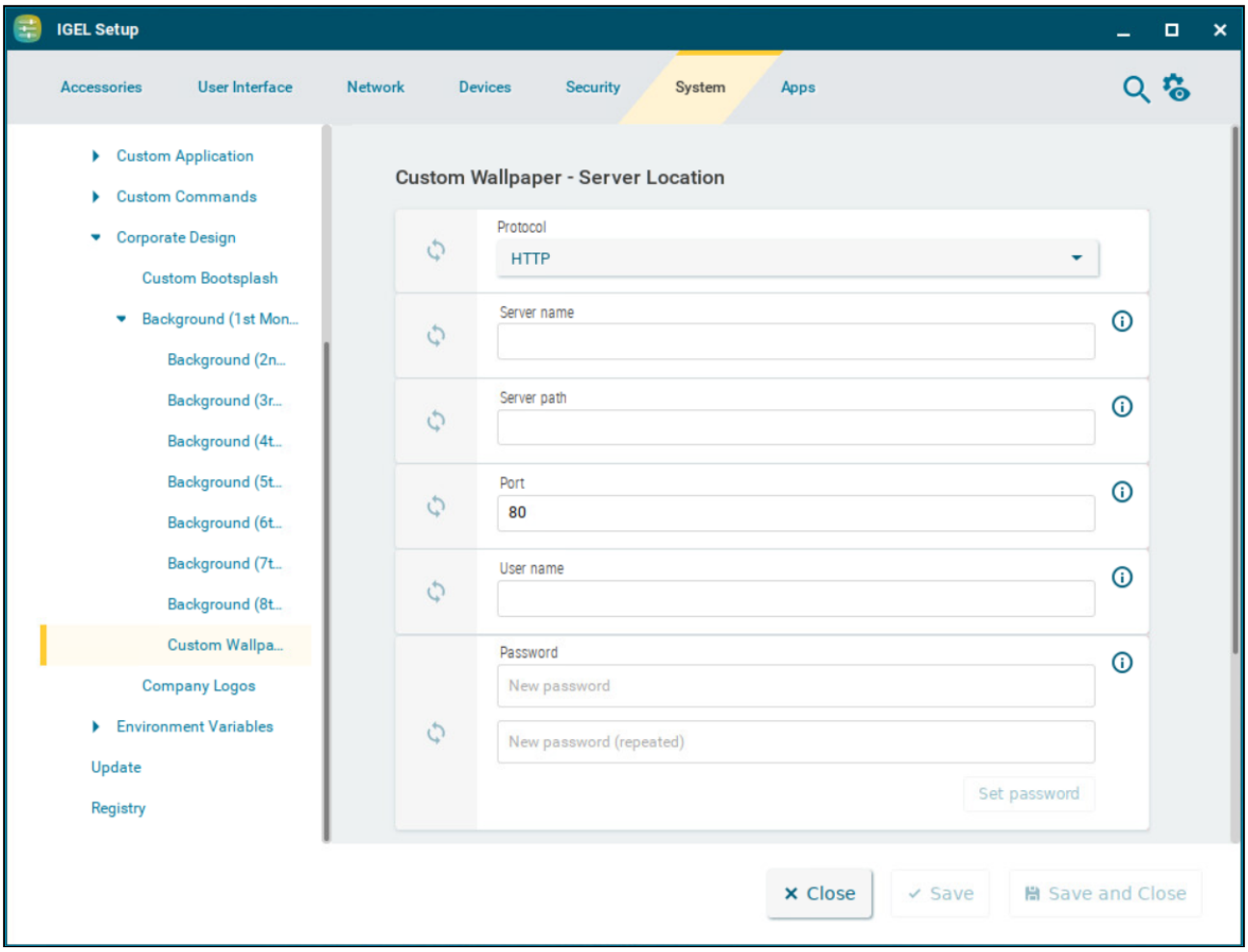
The user-specific background image will be downloaded from the specified server if the function was enabled and if requested manually by clicking **Wallpaper update** under **System > System Customization > Corporate Design > Background > Custom Wallpaper Server**. The download can also be launched from the IGEL Universal Management Suite (UMS) via the **Update desktop customization** command.

> A user-specific image can be provided on a download server. The file types BMP, JPG, GIF, TIF, PNG and SVG are supported for an own background image and bootsplash. A total storage area of 25 MB is available for all user-specific images. For more information, see Firmwareanpassungen in der IGEL UMS.

Custom Wallpaper Server

This article shows how to configure the download server for your own background images in IGEL OS.

Menu path: **System > System Customization > Corporate Design > Background (1st Monitor) > Custom Wallpaper Server**



Protocol

Access method for the image
Possible options:

- **HTTP**: Download from a web server. (Default)
- **HTTPS**: Download from a TLS/SSL-secured web server
- **FTP**: Download from an FTP server

- **Secure FTP**: Download via SSH-secured FTP
- **FTPS**: Download from a TLS/SSL-secured FTP server
- **FILE**: The image file lies in the file system of the device, possibly as a shared NFS or Windows update. You can enter the location under **Local path**.

Local path

The path to the background image. The parameter is shown when **FILE** is selected as protocol.

Server name

Name or IP address of the server used

Server path

Directory in which you saved the background image

Port

Port of the server on which the service is provided. The field is populated by protocol specific default values.

User name

Name of the user account on the server

Password

Password for this account

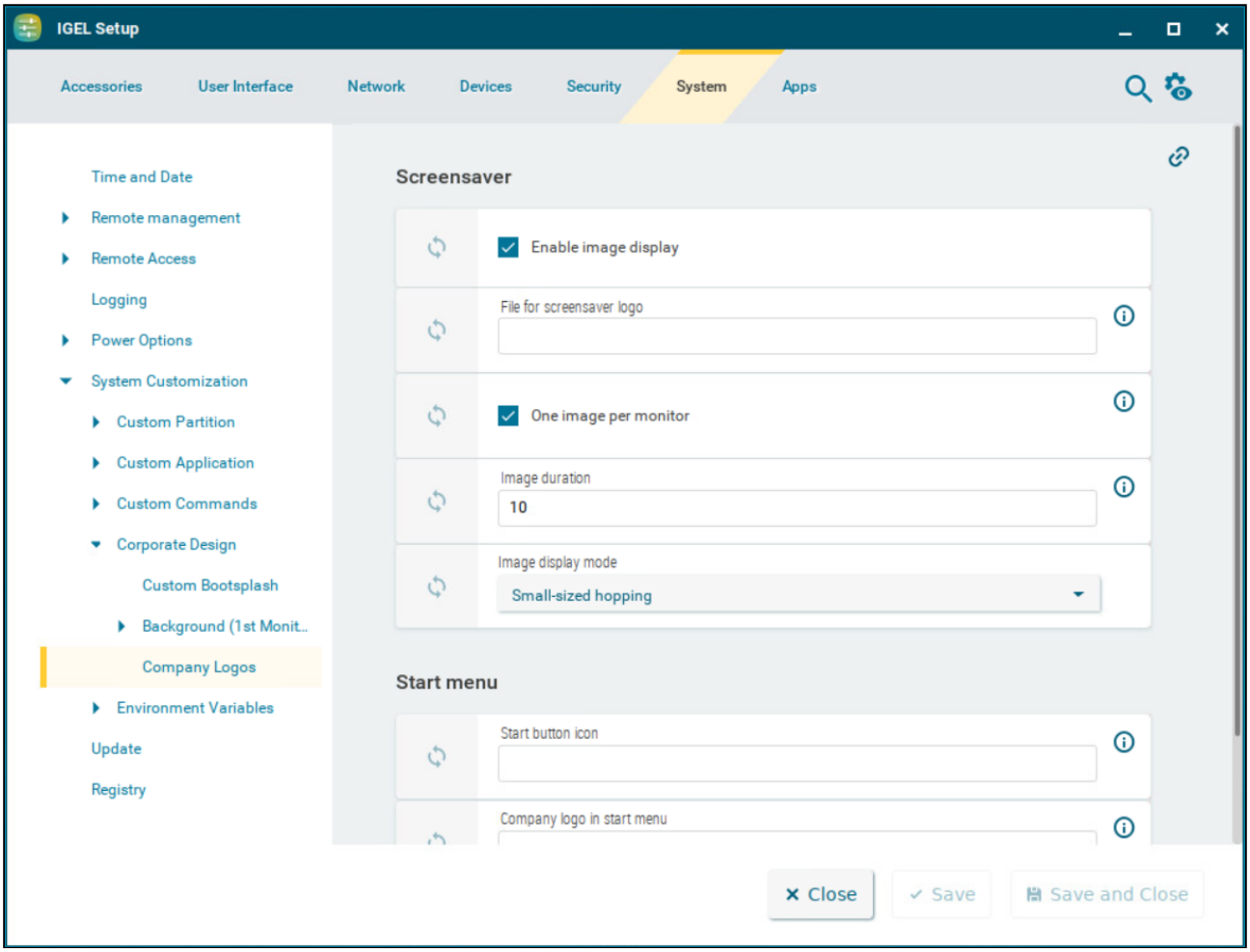
Wallpaper update

The button refreshes the background image when clicked.

Company Logos

You can configure the device to show your company logo in the screensaver and in the start menu.

Menu path: **System > Firmware Customization > Corporate Design > Company Logos**



Screensaver

Enable image display

☑ The image defined below will be shown as the screensaver. (Default)

File for screen saver logo

Complete path for an image file or a directory that contains a number of image files.

If you enter a folder instead of a single image file as the source, all images in the folder will be displayed as a slide show. The **image display time** for the images can be configured. If you do not specify a file of your own, the *IGEL* logo will be used.

One image per monitor

☑ The image will be shown on each individual monitor rather than one image across all monitors. (Default)

Image duration

Time in seconds until the image changes. (Default: 10)

Image display mode

Defines how the image is displayed
Possible options:

- **Small-sized hopping**: small image that jumps across the screen. (Default)
- **Medium-sized hopping**: larger image that jumps across the screen
- **Full screen center cut out**: Image is displayed across whole screen, edges can be cut off.
- **Full screen letterbox**: Complete image is shown. A black edge may be visible depending on the format.

Start menu

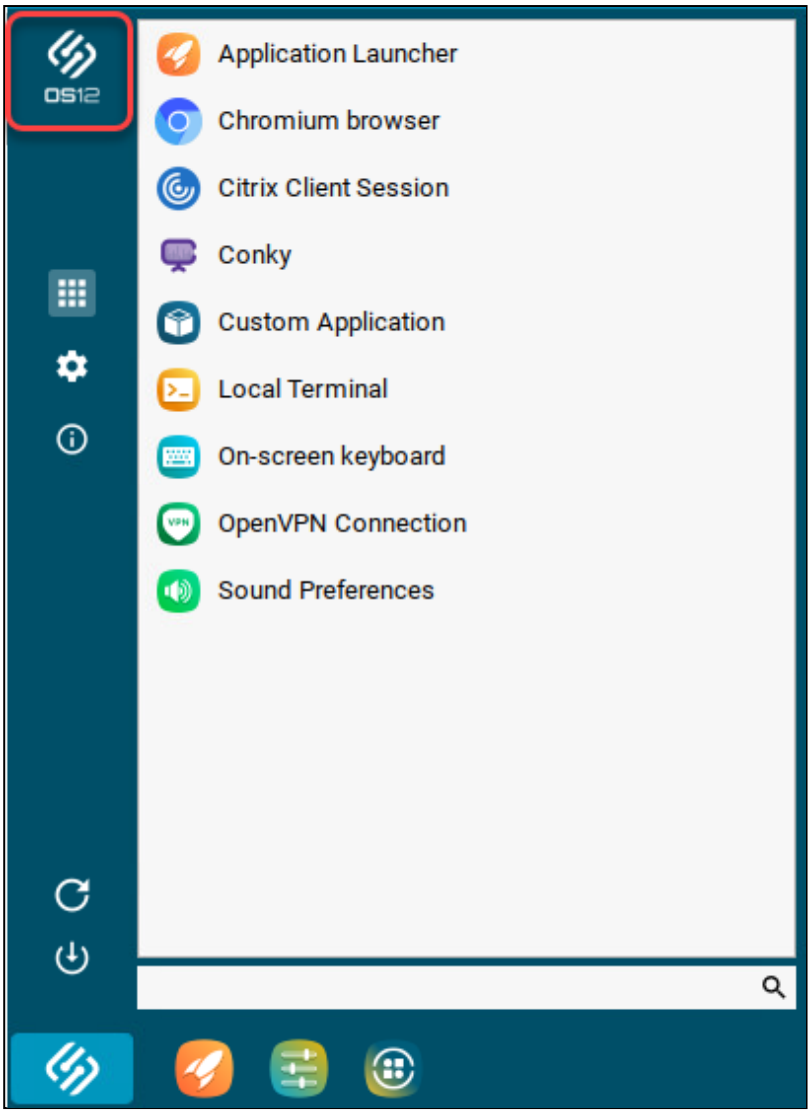
Start button icon

File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels

Company logo in start menu

File name with full path to show your company logo in the top of the start menu window. Size: 64x64 pixels

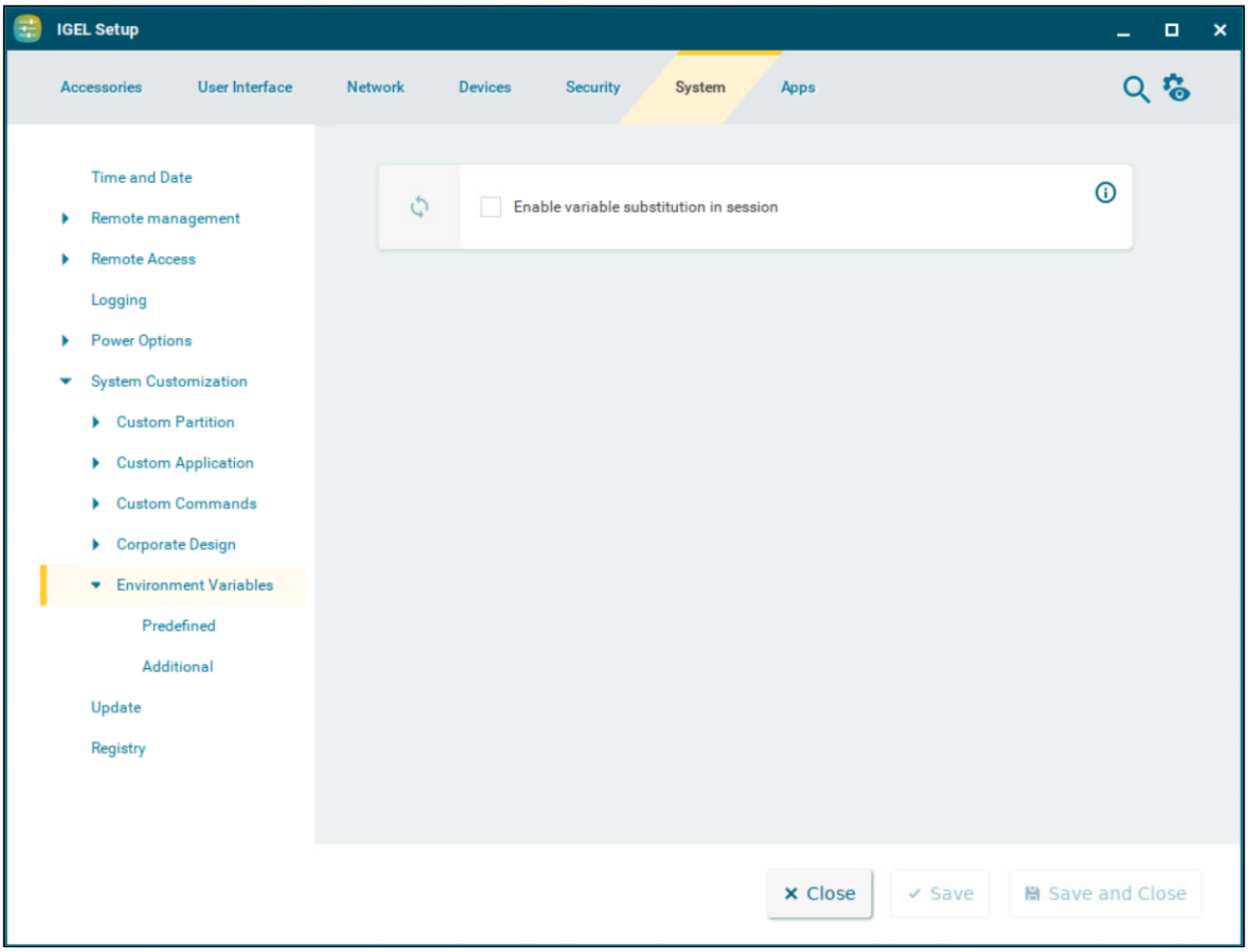
In order to see the company logo in the start menu window, you must set the start menu type to **Advanced**. You can do this under **User Interface > Desktop > Start Menu**. For more information, see Start Menu (see page 81).


OS12
Application Launcher
Chromium browser
Citrix Client Session
Conky
Custom Application
Local Terminal
On-screen keyboard
OpenVPN Connection
Sound Preferences

Environment Variables

Environment variables allow you to use dynamic parameter values for a number of session types, e.g. so as not to have to enter ICA or RDP servers for every session. Predefined variables can also be allocated and distributed via the IGEL UMS. Additional variables can only be used locally on the device and may be overwritten by a UMS configuration.

Menu path: **System > System Customization > Environment Variables**



Enable variable substitution in session

☑ The use of variables in sessions such as ICA and RDP is enabled. If specific parameters contain a `$`, shell substitution will be carried out.

☐ The use of variables in sessions is not enabled. (Default)

You can use environment variables in custom commands. For more information on these, see Custom Commands (see page 318).

In addition, the following session parameters can be updated through variables:

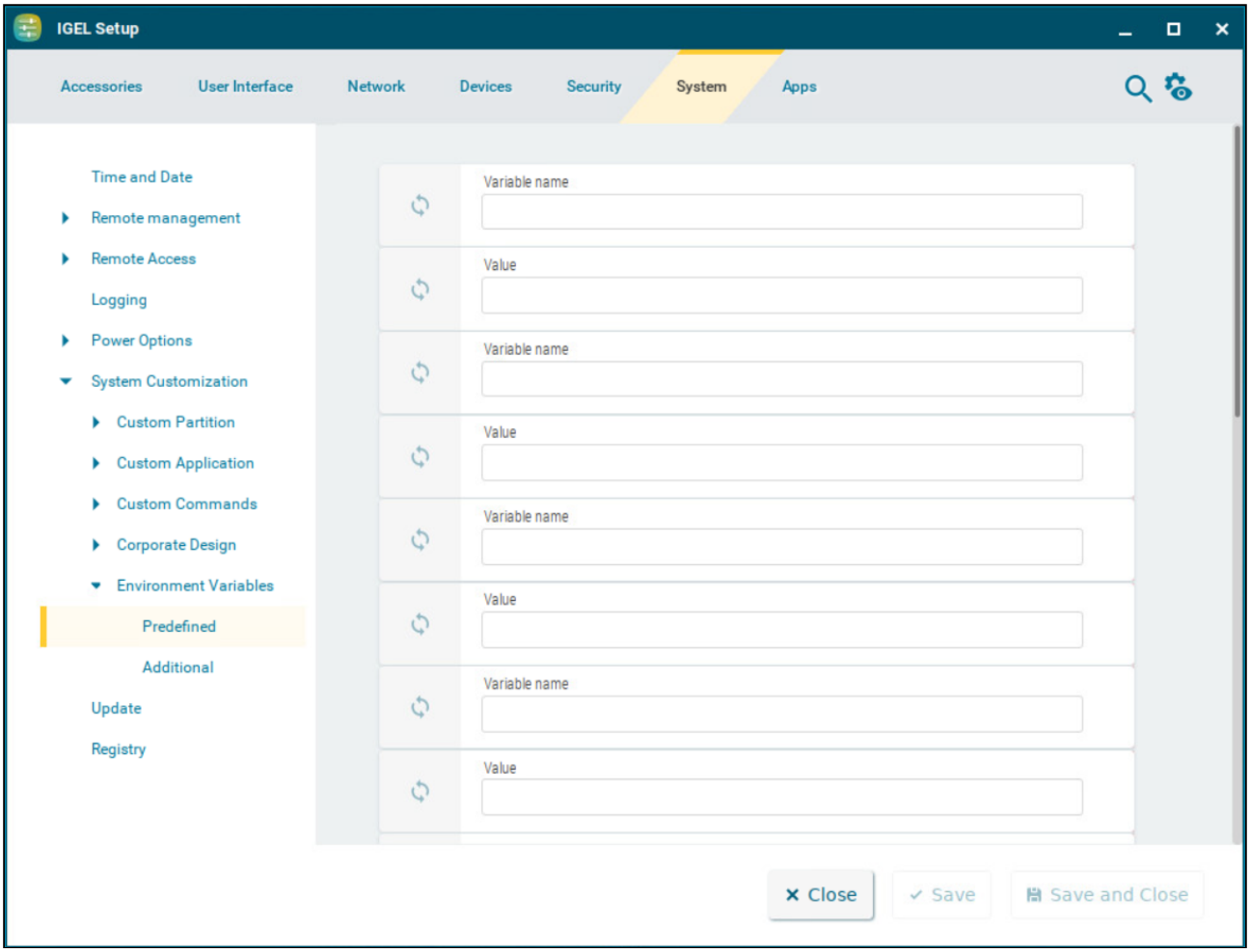
- Legacy ICA sessions: Citrix Server or published application
- Legacy ICA sessions: User
- RDP session: Server
- RDP session: User

- Predefined (see page 343)
- Additional (see page 345)

Predefined

This article shows the options to configure predefined environment variables in IGEL OS.

Menu path: **System > System Customization > Environment Variables > Predefined**



Variable name

Name for the variable

Value

Value for the variable

Using Environment Variables in Sessions

To use environment variables in sessions, proceed as follows:

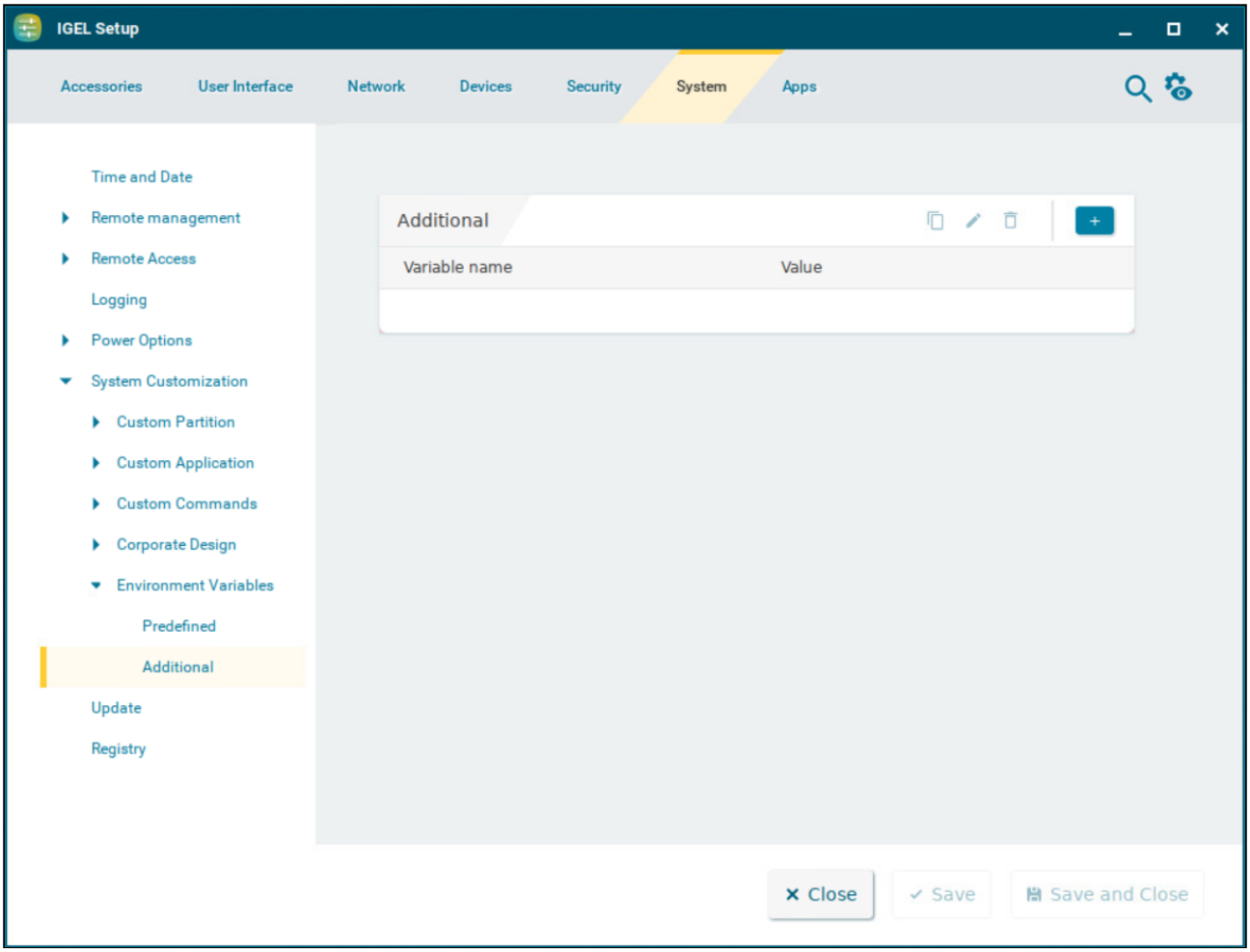
1. Enable environment variables under **System > System Customization > Environment Variables > Enable variable substitution in session**.
2. Define the variable name and content, e.g.
   - **Variable name**: `SERVERNAME`
   - **Value**: `testServer`
3. Enter the variable name in the parameter field of the session with the $ symbol before it.
   Example: `$SERVERNAME`

   > In the case of RDP and ICA sessions, the value is entered in the session file after saving. With XenApp, the setting is not implemented until a session starts and is running.

Additional

This article shows how to define other environment variables in addition to the predefined ones.

Menu path: **System > System Customization > Environment Variables > Additional**



To manage the list of **Additional** variables:

- 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 **Add** dialogue, where you can define the following settings:

- **Variable name**

  Name for the variable

- **Value**

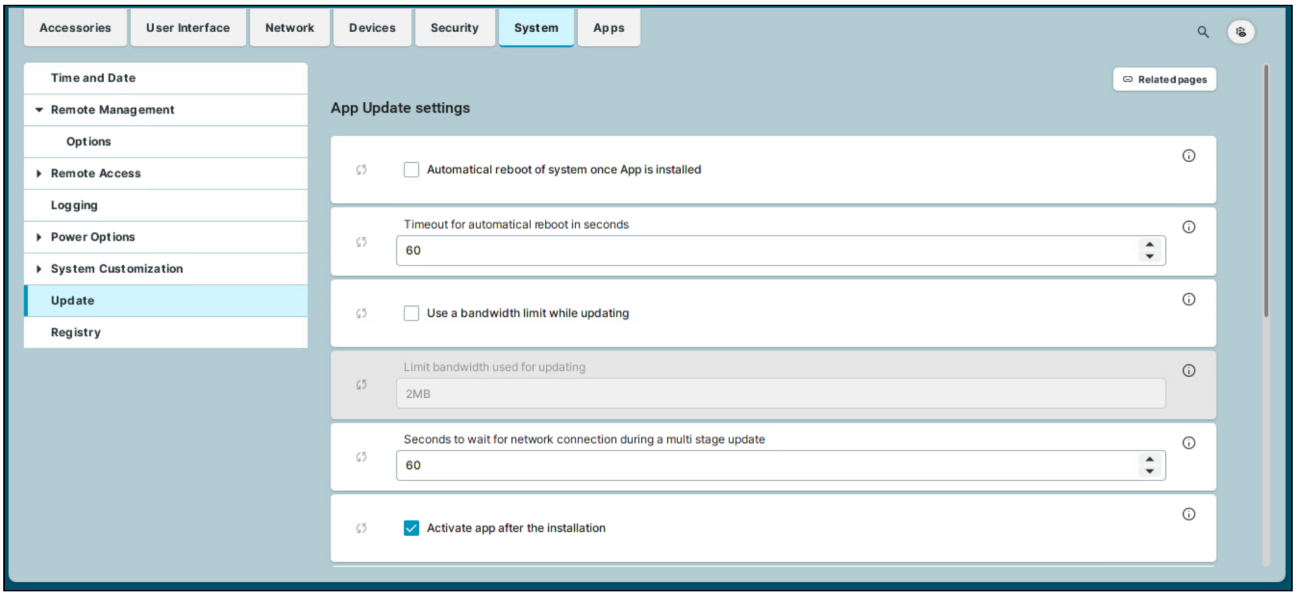
  Value for the variable

Update

This article shows how to configure app update settings in IGEL OS.

Apps can only be installed by the user if **Permit local app installation** is enabled under **Security > Update**. For more information, see Installing IGEL OS Apps Locally on the Device.

Menu path: **System > Update**



Automatic reboot of system once app is installed

☑ After app installation, the device reboots automatically. The user cannot postpone the reboot.

☐ After app installation, there is no automatic reboot. The user decides when to reboot. (Default)

Timeout for automatical reboot in seconds

Time period between the app installation and the reboot. (Default: 60)

Use a bandwidth limit while updating

☑ Limits bandwidth usage during the downloading of updates to the value set under **Limit bandwidth used for updating**.

☐ Bandwidth usage is not limited during the downloading of updates. (Default)

Limit bandwidth used for updating

The value to which the bandwidth is limited during the downloading of updates. You can give the value with KB, MB, or GB as the quantifier. If no quantifier is given, the value is in megabytes. (Default: 2MB)

Seconds to wait for network connection during a multi stage update

A multi stage update is cancelled if no network connection can be established during this period. (Default: 60)

Activate app after the installation

☑ Apps are directly activated after installation, no separate action is needed from the UMS Web App. (Default)

☐ Apps are activated through a separate action from the UMS Web App.

Check for and download updates for non pinned apps on boot

This option helps keep the apps on the device up-to-date by checking for updates on each boot. This is potentially security-relevant

Non-pinned apps are all apps that are not assigned to a device via the UMS, regardless of whether the assignment was made via a profile or directly. This applies to apps that are dependencies of other apps, for instance. Example: The app **Citrix Multimedia Codec** is a dependency for the **Citrix Workspace App**.

☑ On each boot, the device checks for updates of non-pinned apps. If updates are found, they are installed on the device. (Default)

☐ Updates of non-pinned apps are not checked automatically.

Check for and download updates for non pinned apps on given calendar time, use the crontab syntax to specify the calendar time

This option helps keep the apps on the device up-to-date by checking for updates periodically. To define the period, use the crontab syntax.

> **Consider Network Load**
>
> It is recommended to take into account the network load that occurs when a large number of devices download the updated apps. If required, use the settings **Use a bandwidth limit while updating** and **Limit bandwidth used for updating**.

Non-pinned apps are all apps that are not assigned to a device via the UMS, regardless of whether the assignment was made via a profile or directly. This applies to apps that are dependencies of other apps, for instance. Example: The app **Citrix Multimedia Codec** is a dependency for the **Citrix Workspace App**.

If the defined checking time has been missed because the device has no network or cannot reach the UMS or the IGEL App Portal, the update check is queued until the connection is available again. If the defined checking time has been missed because the device has been powered off, the update check will not be queued.

Possible values: Crontab syntax; if the field is empty, no update check will be performed. For details on the crontab syntax, see https://man7.org/linux/man-pages/man5/crontab.5.html or check out the interactive tool at https://crontab.guru/.

Repositories

Prioritized list of repositories used for app updates

To manage the list:

- 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 **Add** dialogue, where you can define the following settings:

- **Certificate**

  The certificate used for authentication

- **Priority**

  The number defines the priority of the repository, where a larger number means a higher priority. The priority determines the order the device tries to connect to download apps. It will try to connect to the repository with the highest priority, and if that is not available, it will fall back to the next one.

  Numbers are accepted from 0 to 4294967295.

- **Repository URL**

  The URL of the repository

Use only repositories deployed by the UMS

☑ The device can only download apps from repositories for which the UMS acts as an update proxy.

☐ The device can download apps from all the configured repositories. (Default)

⚠ The parameter requires UMS 12.04.110 or later. (Release planned for end of May 2024.)

Registry in IGEL OS 12

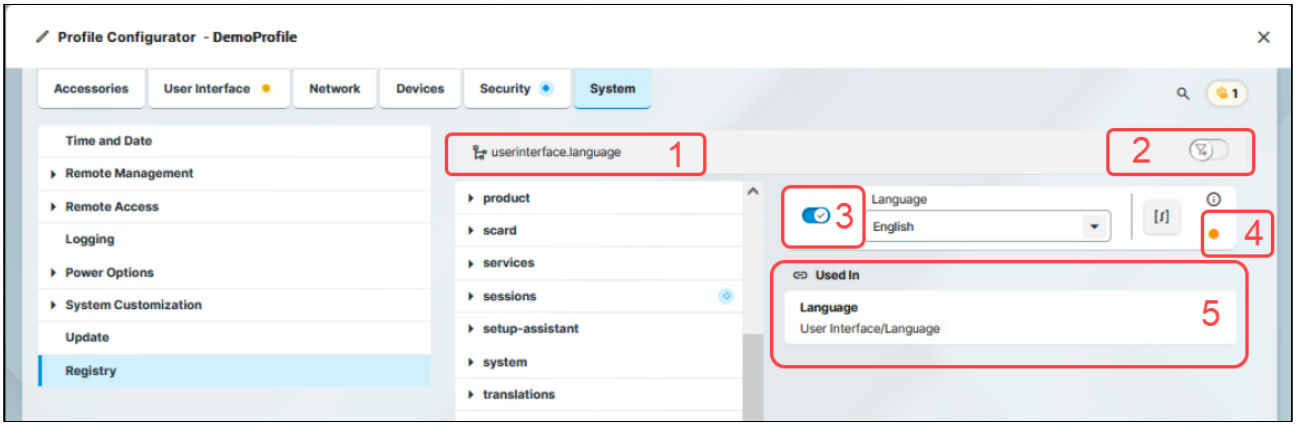
In the registry, you can change almost any firmware parameter, including parameters not shown in the GUI. You will find information on the individual items in the tooltips.

Menu Path: **System > Registry**

> Changes to the registry should only be made by experienced administrators. Incorrect parameter settings can easily destroy the configuration and cause the system to crash. In cases like these, the only way to restore the functionality is to reset the device to the factory defaults!

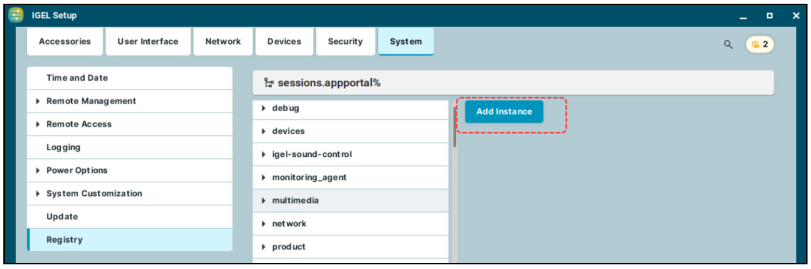
Registry User Interface

The registry shares most of the GUI elements with the rest of the configuration dialog. For details, see Configuration of IGEL OS 12 Device Settings (see page 6).

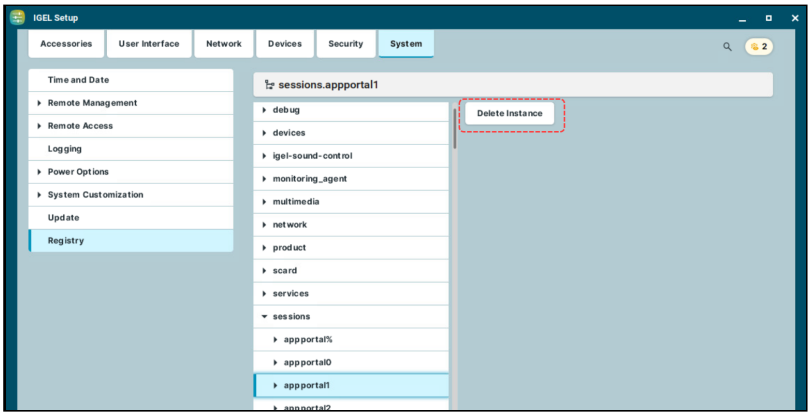


1	You can use the breadcrumbs to track your navigation within the registry.
2	In the Profile Configurator, you can use the toggle button to only see parameters activated by the parameter activator (3) in the registry.
3	In the Profile Configurator, you can use the parameter activator to activate registry parameters. When you deactivate the parameter, the value will be automatically set back to the default value. For more on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App.
4	Your changes are marked with indicators on the right side of the parameter. For more on change indicators, see Configuration of IGEL OS 12 Device Settings (see page 6).
5	Under **Used In**, you can find the list of configuration pages where the parameter is used. Click on the page link to jump to the page.

Add instance
Adds instances to the registry. This is possible with parameters that have a percent sign as their last character, e.g. `nfymount%`. The new instances are numbered consecutively: `nfymount1`, `nfymount2` etc.

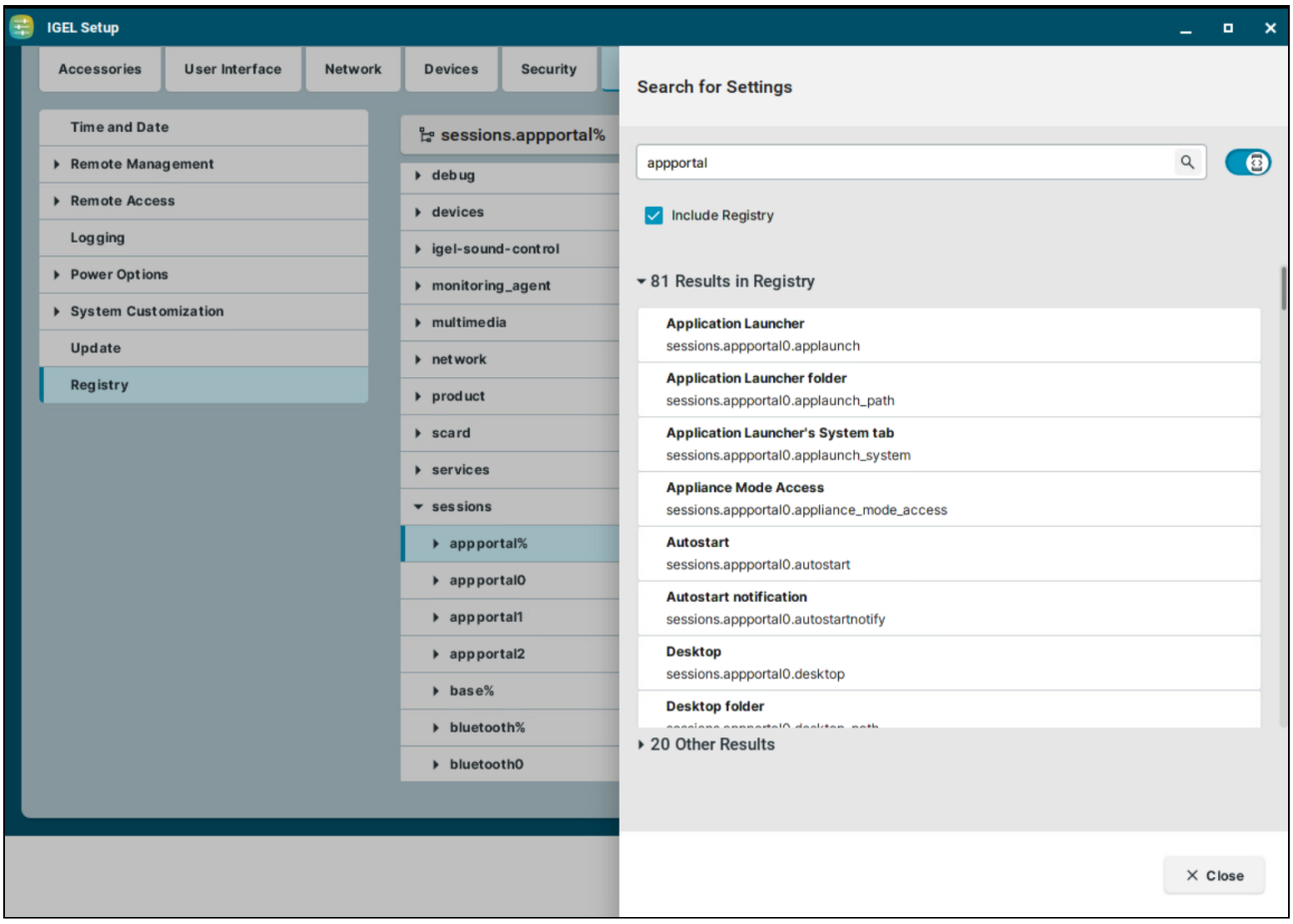


Delete instance
Deletes a previously added instance.



Search in the Registry

You can use the advanced search to search for registry parameters.



To search for parameters in the registry:

1. Enable advanced search using the toggle button.

2. Activate **Include Registry**.

3. Start typing in the search field.
   The search results list automatically refreshes as you type.

4. Click on a search result to display the registry page. The result is highlighted on the page.
   When a search result is clicked, the search menu remains displayed in the top right corner with the following navigation options:
   - arrows to go to the next or the previous search result
   - search icon to expand the search tab
   - X to close the search

Tray Applications in IGEL OS 12

This article describes the tray applications available in IGEL OS 12. You can open the tray apps by clicking the icons in the system tray.

The icons change dynamically to represent the current setup or status. If you hover over the icons, tooltips are displayed with further information.

> By default, the system tray and all the tray apps are available. You can configure the system tray and the tray apps under **User Interface > Desktop > Taskbar Items**. For details, see Taskbar Items in IGEL OS 12 (see page 72).
> The access to tray apps on lockscreen is configured separately under **User Interface > Desktop > Screenlock / Screensaver > Taskbar**. For details, see Taskbar (see page 92).

The following tray apps are described in detail:

Sound Tray App (see page 354)

Display Tray App (see page 355)

Mouse & Touchpad Tray App (see page 362)

Mobile Broadband Tray App (see page 365)

Wi-Fi Tray App (see page 369)

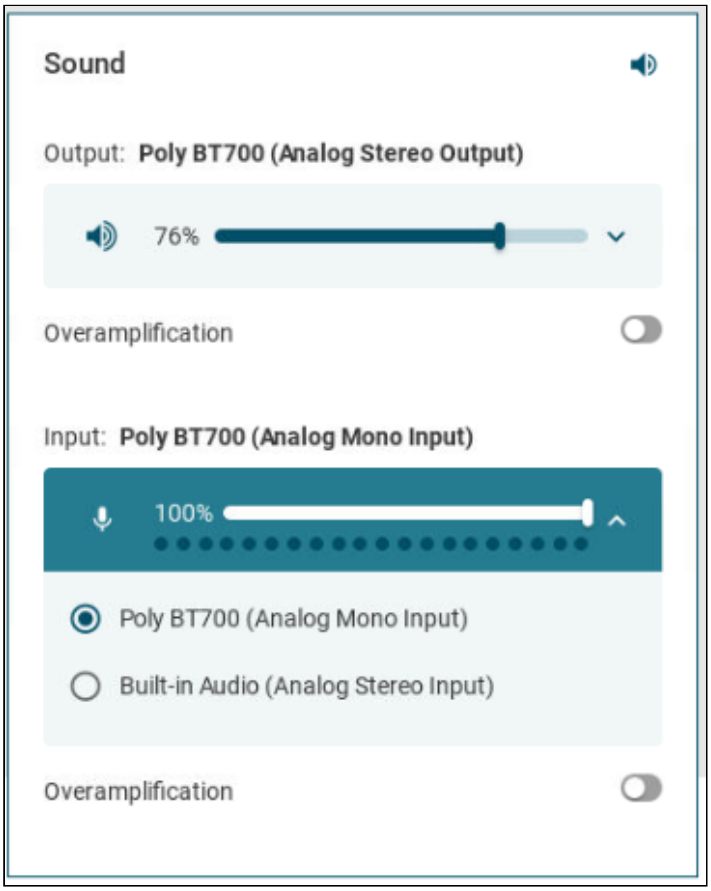
LAN Tray App (see page 372)

Battery Tray App (see page 374)

UMS Tray App (see page 374)

Sound Tray App

- Open the sound tray app by clicking the icon or the icon. When the devices are muted the icons change accordingly to and .



You can do the following in the tray app:

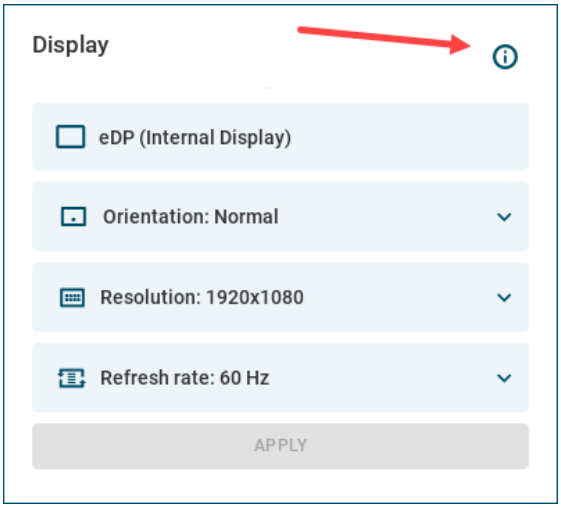
- Use the dropdown menu to select which output/input device is to be used.
- Set the volume for the selected output/input device.
- Enable/disable overamplification. If the overamplification parameters are set under Devices > Audio > Options (see page 235), you cannot change the setting from the tray app.
- Use the **Mute All** button to mute all the output devices.

Display Tray App

▶ Open the display tray app by clicking the tray icon . The icon is dynamic in multi monitor environments and represents the configured **Multiple Display Mode**.

The basic window opens with different content for single display and multiple display setups.

Basic Window - Single Display



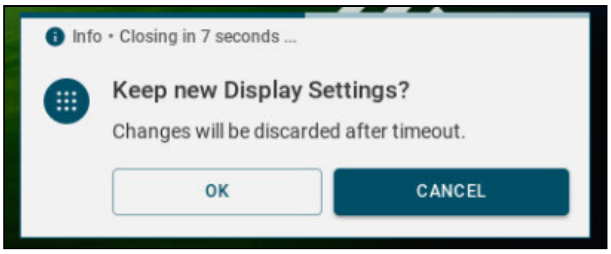
Here, you have the following options:

More...

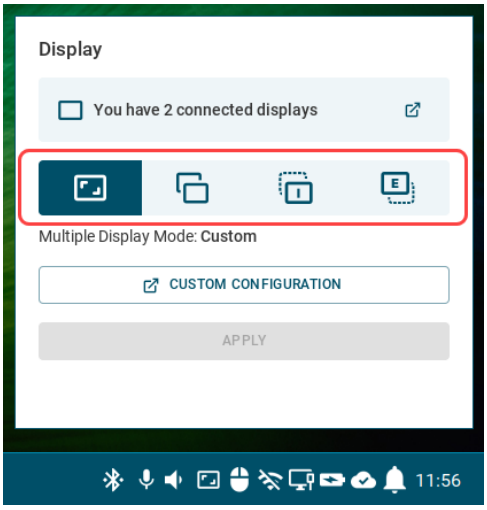
▶ Click the info icon to display device information.

▶ Set **Orientation**, **Resolution** and **Refresh rate** for the single display.

After clicking **Apply**, you need to confirm keeping the changes in a dialog. After the timeout, settings revert to the previous configuration.



Basic Window - Multiple Display



Here, you have the following options:

More...

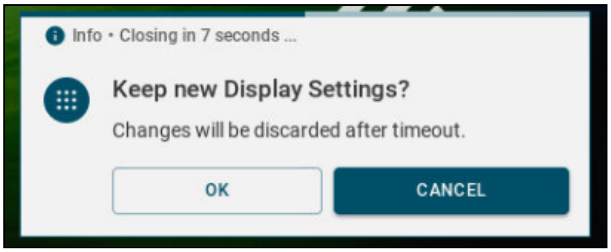
▶ Click the **You have X connected displays** or the **Custom Configuration** button to open the display configuration window.

> Display information is always available in the display configuration window, but configuration is only possible if **Custom** display mode is applied.

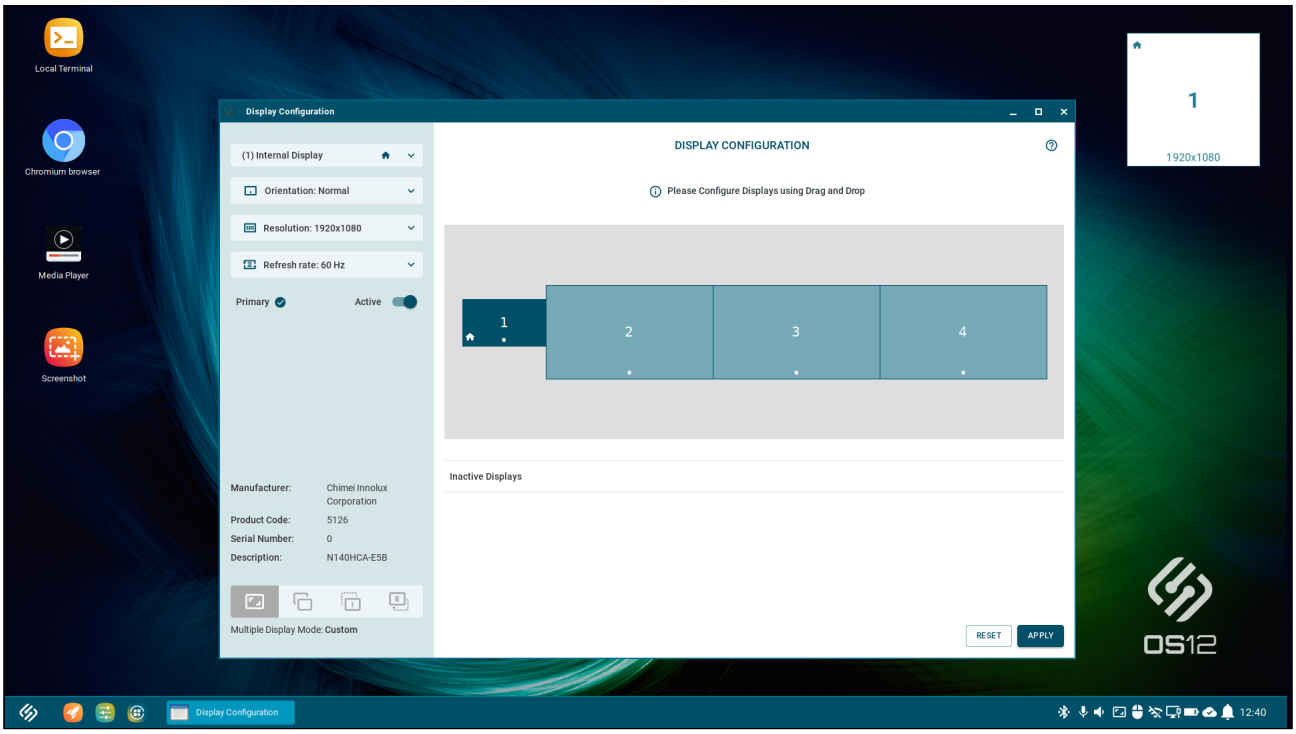
▶ Select the **Multiple Display Mode**:

- **Custom**
  You can configure your displays in the display configuration window.
- **Mirror**
  The content is mirrored to all displays.
- **Internal only**
  The internal display will become the primary display. External displays get deactivated.
- **External only**
  One of the external display will become the primary display. The internal display gets deactivated.

After clicking **Apply**, you need to confirm keeping the changes in a dialog. After the timeout, settings revert to the previous configuration.



Display Configuration Window



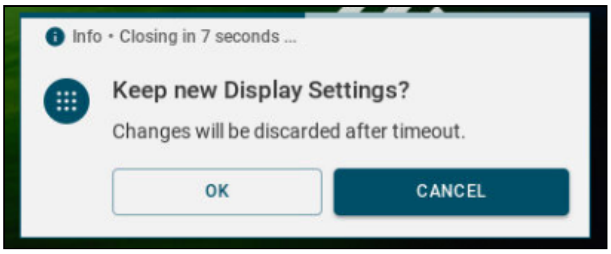
> Display information is always available in the display configuration window, but configuration is only possible if **Custom** display mode is applied in the basic window. You can see the selected mode in the bottom left corner.

Here, you have the following options:

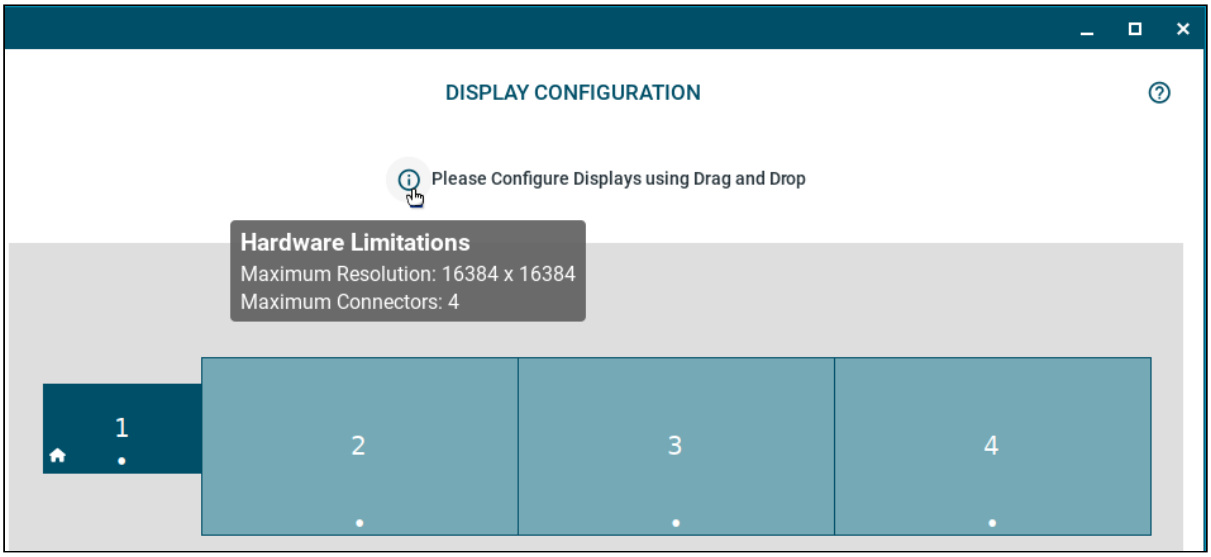
More...

- You can click **Reset** to restore the last saved configurations.

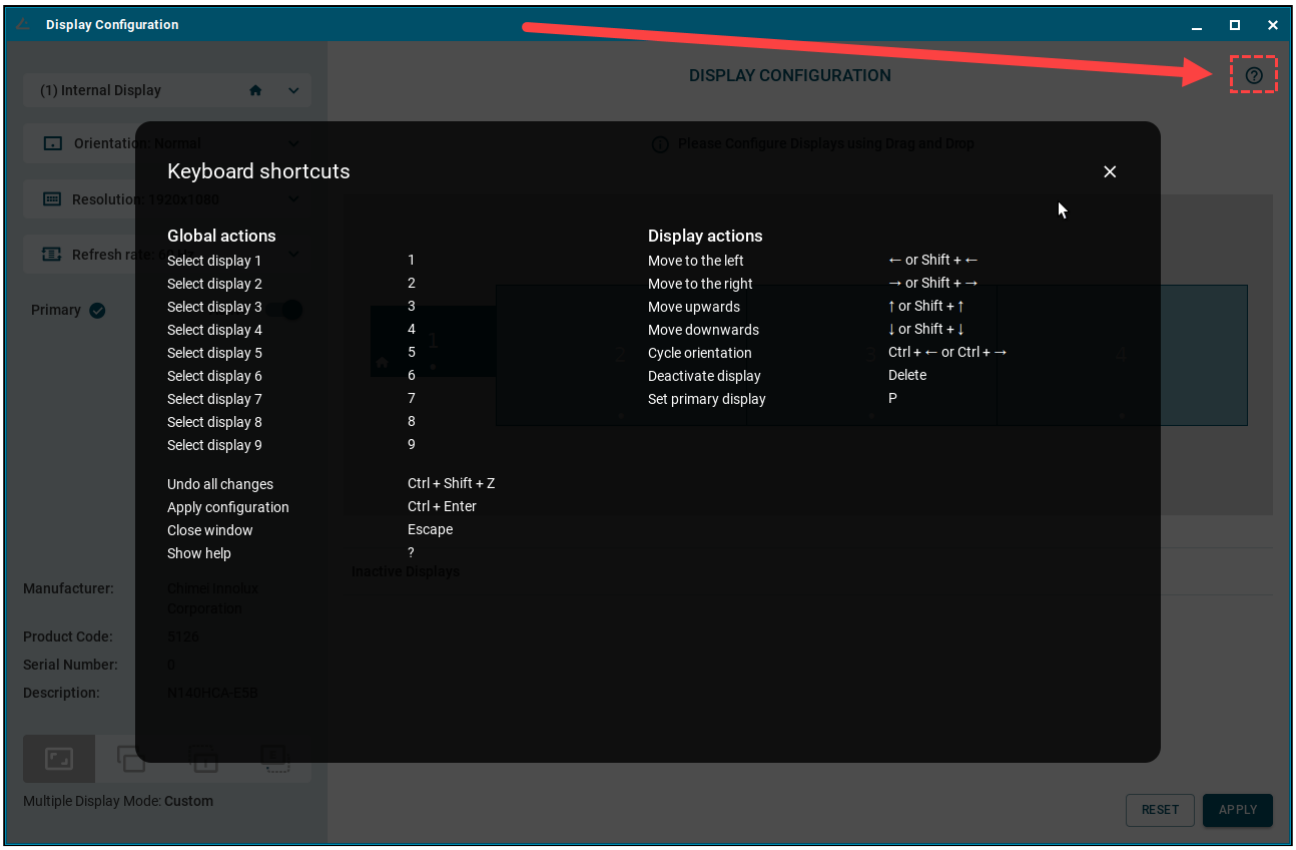
After clicking **Apply**, you need to confirm keeping the changes in a dialog. After the timeout, settings revert to the previous configuration.



▶ You can click the info icon to display information on **Hardware Limitations** for the device. This information is needed for the configuration, because you cannot create display layouts which exceed the given maximum resolution or number of connected displays.



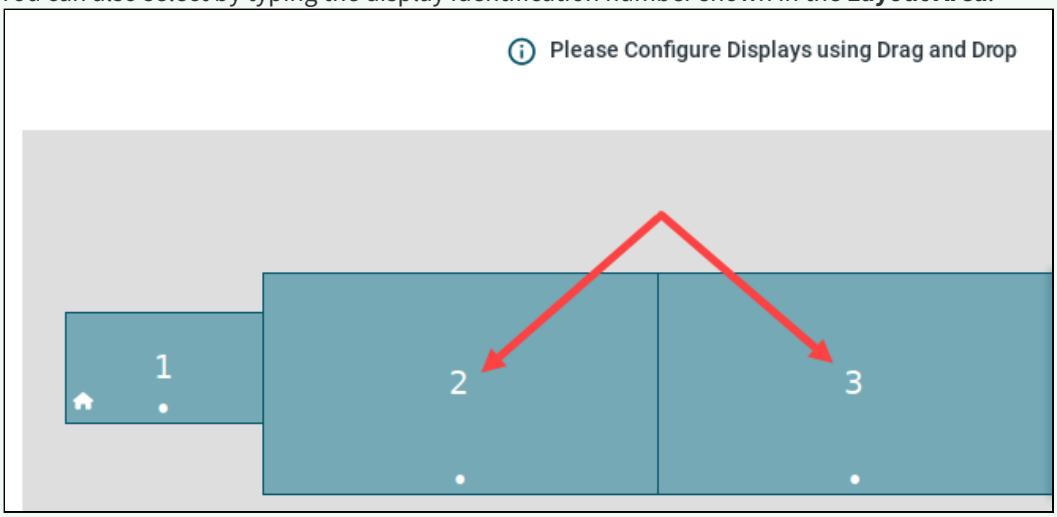
▶ Click the question mark icon to display the **Keyboard shortcuts** that you can use for display configuration.



Left Hand Panel

▶ Select a display from the dropdown at the top, or by clicking the display in the **Layout Area**, to configure the display and to see the details of the selected display at the bottom of the panel.

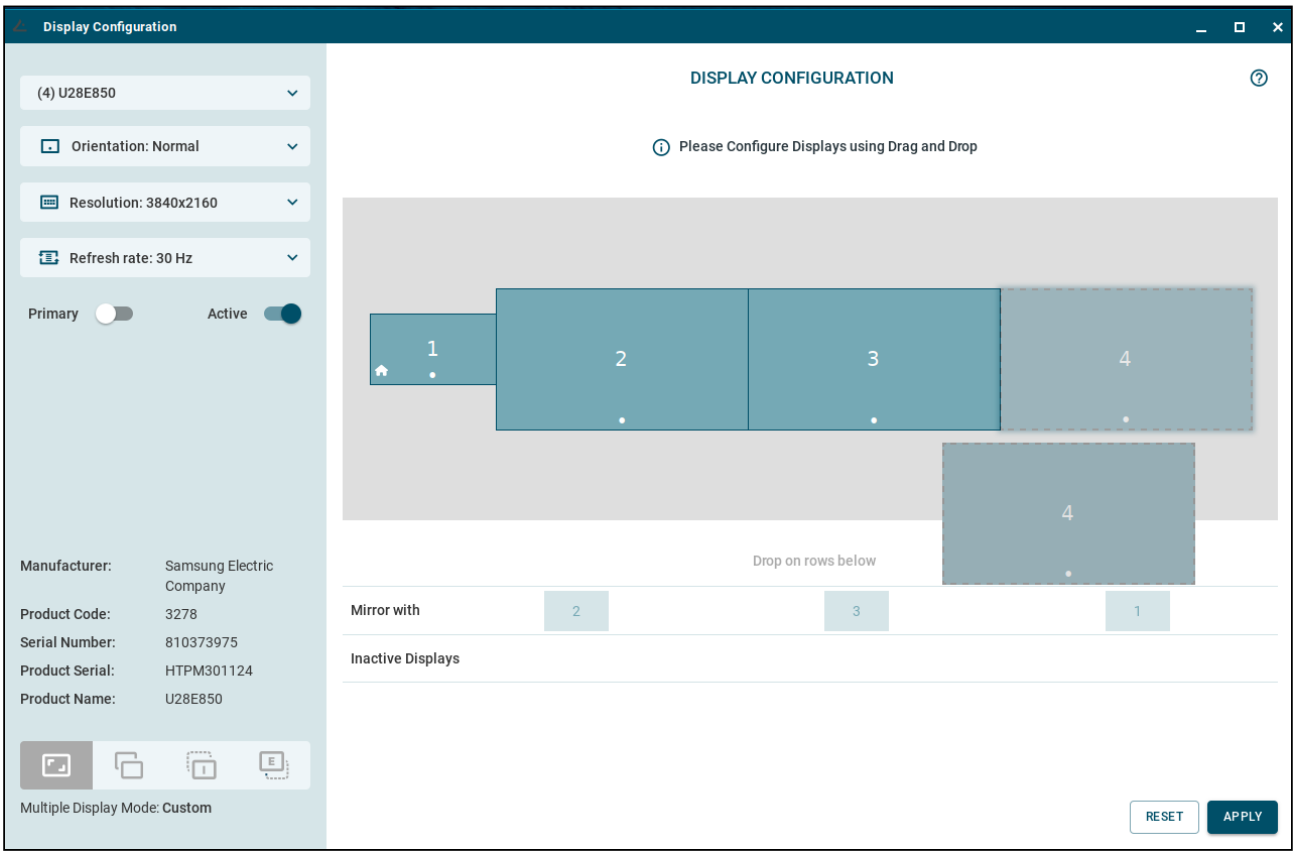
You can also select by typing the display identification number shown in the **Layout Area**.



You can use the parameters to configure the following:

- **Orientation**
- **Resolution**
- **Refresh rate**
- **Primary** toggle
  Activate if you would like to make the selected display the primary display. The primary display is marked with a house icon. Only one display can be primary; if a display is marked as primary, the existing primary becomes non-primary.
- **Active** toggle
  Use the toggle to activate/deactivate the selected display. You cannot deactivate all the displays, at least one display must remain active.

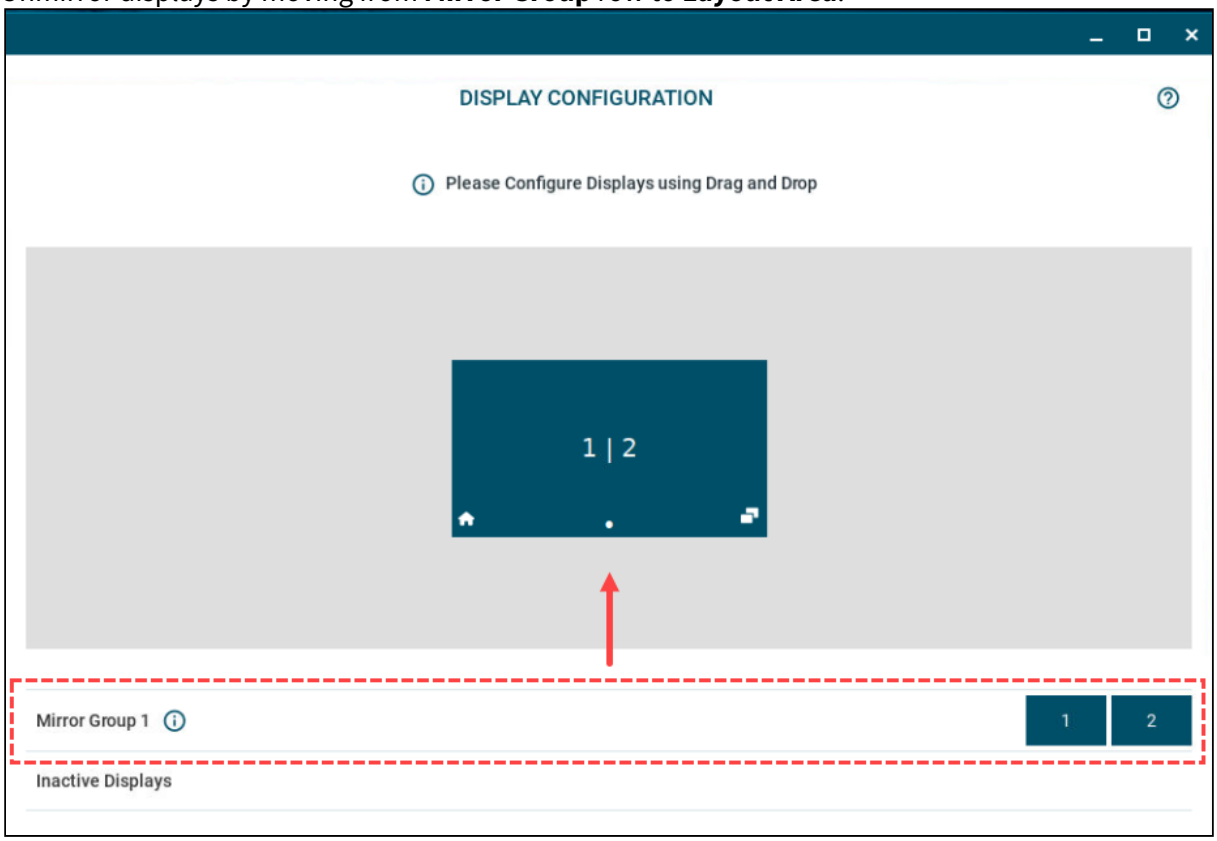
Drag and Drop Panel



Here you can:

- Select a display by clicking on it.
- Edit the layout of the displays by drag and drop.
- Deactivate displays by moving them to the **Inactive Displays** row.
- Activate displays by moving from **Inactive Displays** to the **Layout Area**.
- Create mirror groups by moving displays together in the **Mirror with** row.

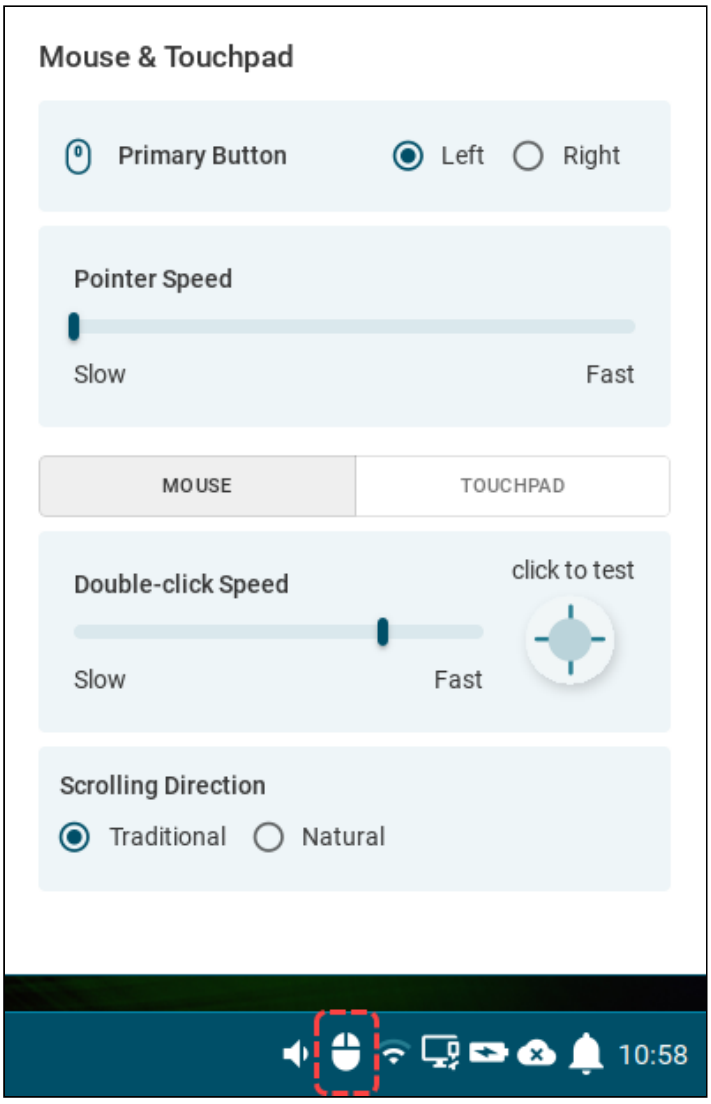
- Unmirror displays by moving from **Mirror Group** row to **Layout Area**.



Mouse & Touchpad Tray App

▶ Open the tray app by clicking the tray icon. The icon is dynamic and represents the detected device. If a mouse is detected, the icon is shown. If a touchpad is detected, or both a mouse and a touchpad are detected, the icon is shown.

Configuring the Mouse in the Mouse & Touchpad Tray App



You can use the mouse & touchpad tray app to configure the following mouse settings for the detected device:

More...

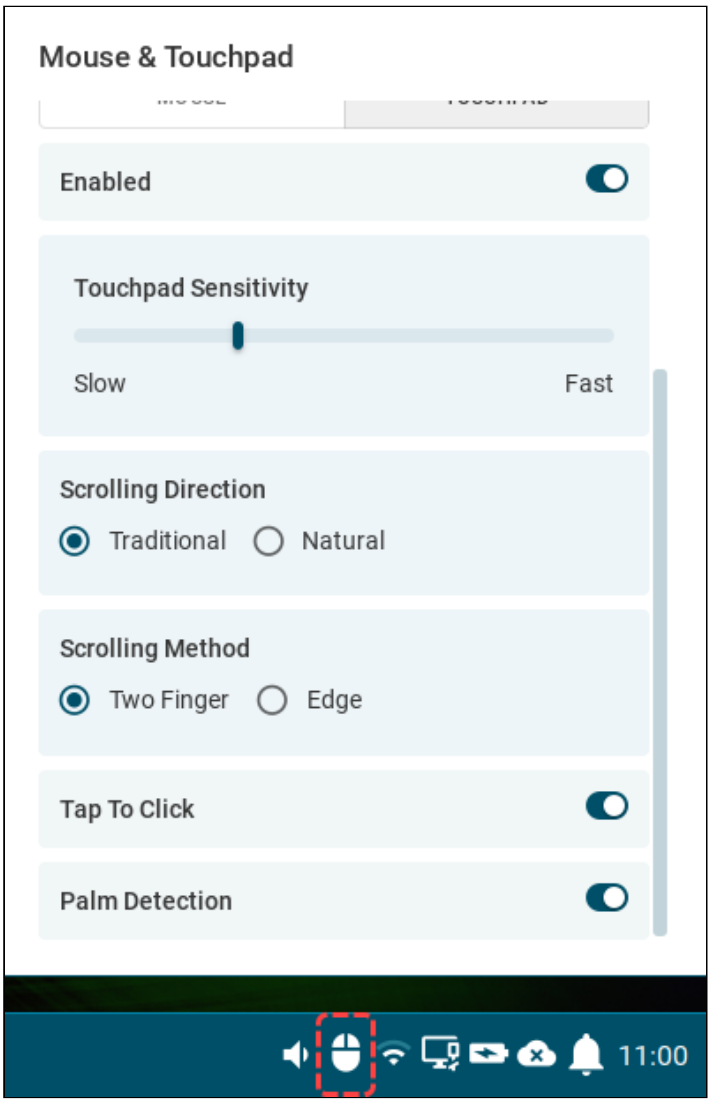
- **Primary Button**
  Sets the primary button both for mouse and touchpad. In IGEL Setup, you can configure this through **Left-handed mode**.

- **Pointer Speed**
  Sets the speed of the pointer both for mouse and touchpad. In IGEL Setup, you can configure this through **Pointer speed**.

- **Double-click Speed**
  Sets how fast two consecutive mouse clicks need to happen to be recognized as a double-click. You can test this with the **click to test** area. In IGEL Setup, you can configure this through **Double click interval**. The smaller the interval, the faster the consecutive clicks need to happen to be recognized as a double click.

- **Scrolling Direction**
  Sets the direction of the screen movement when scrolling with the mouse. In IGEL Setup, you can configure this through **Natural scroll.**

Configuring the Touchpad in the Mouse & Touchpad Tray App



You can use the mouse & touchpad tray app to configure the following touchpad settings for the detected device:

More...

- **Primary Button**
  Sets the primary button both for mouse and touchpad. In IGEL Setup, you can configure this through **Left-handed mode** under **User Interface > Input > Mouse**.

- **Pointer Speed**
  Sets the speed of the pointer both for mouse and touchpad. In IGEL Setup, you can configure this through **Pointer speed** under **User Interface > Input > Mouse**.

- **Enabled**
  The toggle buttons enables/disables the touchpad.

- **Touchpad Sensitivity**
  Sets how sensitive the touchpad is to the touch. In IGEL Setup, you can configure this through **Min speed**, **Max speed**, and **Acceleration**. If you have those values custom configured, it is advised not to change the slider in the tray app, as it will reset the levels in the IGEL Setup.

- **Scrolling Direction**
  Sets the direction of the screen movement when scrolling with the touchpad. In IGEL Setup, you can configure this through **Natural scroll**.

- **Scrolling Method**
  Sets the type of finer movement to be detected as scrolling. In IGEL Setup, you can configure this through **Two finger vertical scroll** and **Two finger horizontal scroll** under **User Interface > Input > Touchpad > Scrolling**.

- **Tap to Click**
  The toggle switch enables/disables clicking with a tap on the touchpad. In IGEL Setup, you can configure this through **Tapping mode**.

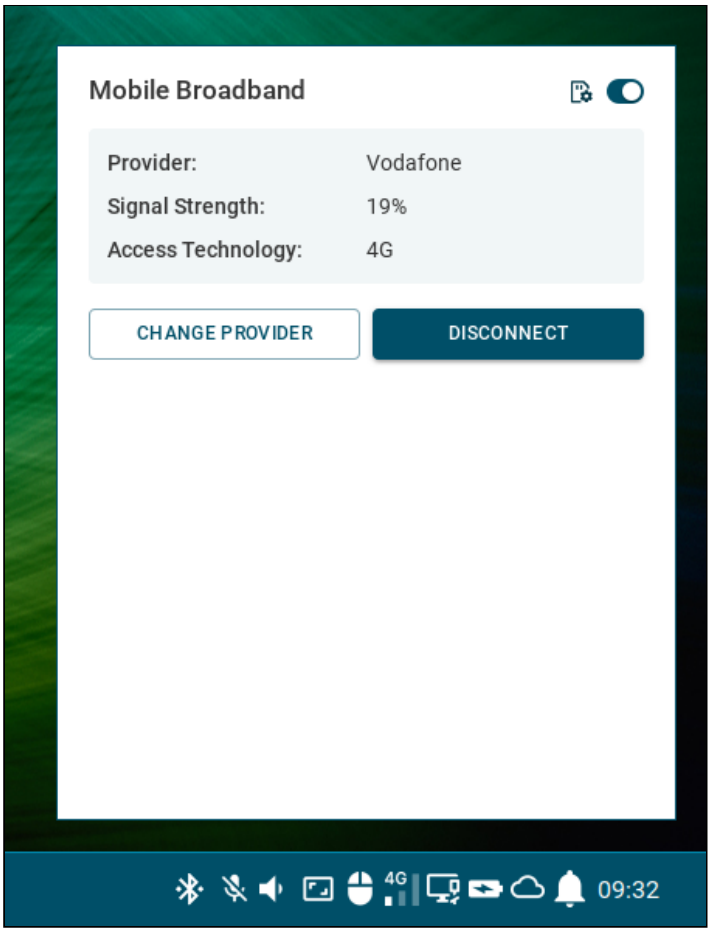
- **Palm Detection**
  The toggle switch enables/disables palm detection. When enabled, it avoids triggering a function accidentally with the palm of your hand. The function must be supported by the device. In IGEL Setup, you can configure this through **Palm detect** under **User Interface > Input > Touchpad > Advanced**.

Mobile Broadband Tray App

▶ Open the tray app by clicking the mobile broadband tray icon. The tray icon is dynamic and represents the state of the connection:

MBB Connection Status	Taskbar Icon
Connected	
No connection	
SIM locked	

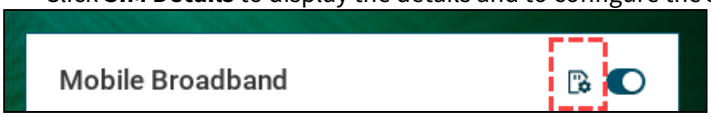
The mobile broadband tray app displays details about the WWAN network connection, like the network **Provider** and the **Signal Strength**, and provides an option to easily connect / disconnect and configure networks.



▶ Use the toggle to switch the WWAN connection off and on.

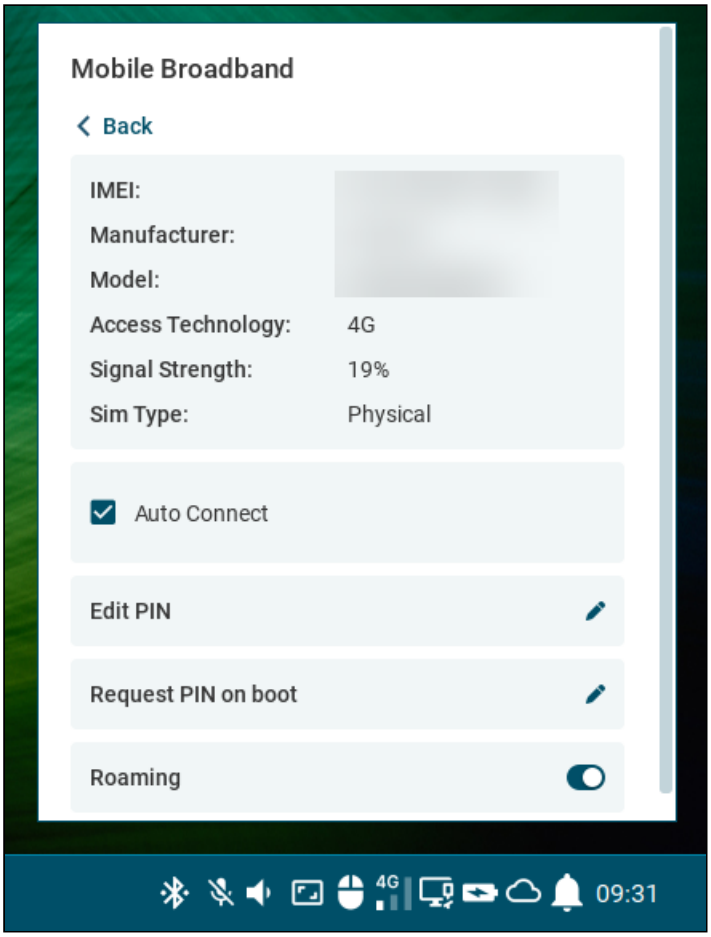
If the **Automatic switch of network connection** parameter is enabled under **Network > Common Settings**, the toggle can be disabled. For more information, see Common Settings (see page 156).

▶ Click **SIM Details** to display the details and to configure the settings that are enabled for the tray app.



More...

You can set which configurations are available in the tray up under **Network > Mobile Broadband**. For details, see Mobile Broadband in IGEL OS 12 (see page 153).



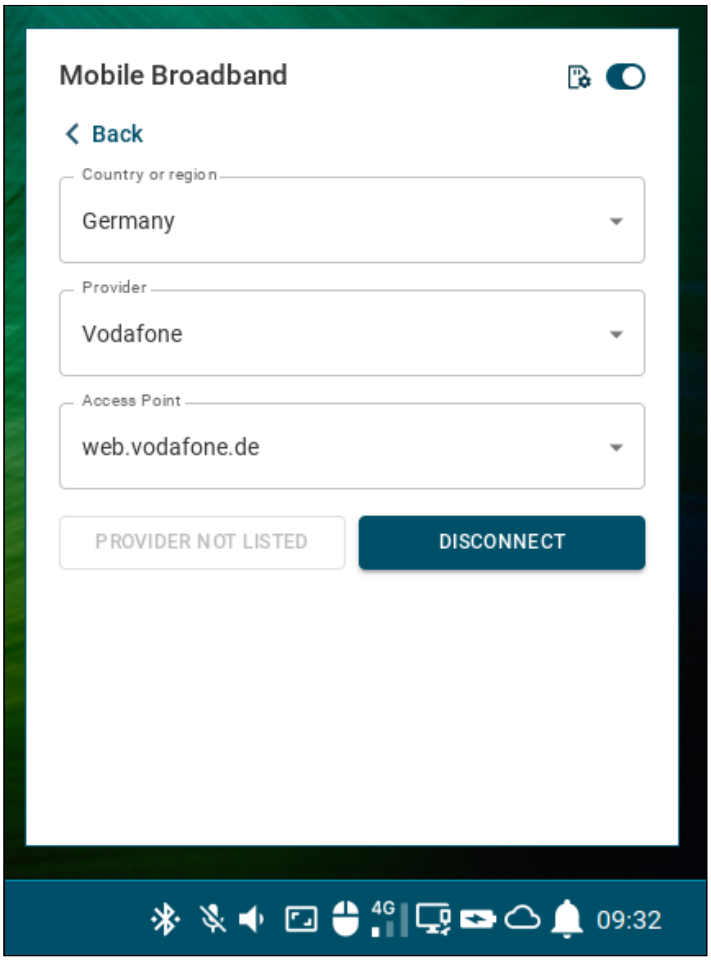
You can configure the following:

- **Auto Connect**
  ☑ The mobile internet connection is established automatically. (Default)
- **Edit PIN**
  Change the PIN of the SIM card.

- **Request PIN on boot**
  Set if PIN needs to be provided at startup.
- **Roaming**
  Use the toggle to enable/disable the connection to roaming networks.

▶ Click **Change Provider** to edit the network provider information:

More...



You can configure the following:

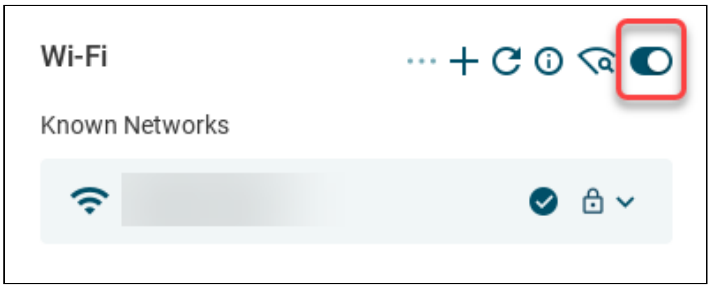
- **Country or region**
  Country or region of the service provider.
- **Provider**
  Your mobile network connection provider.
- **Access Point**
  APN (Access Point Name) for your network connection. If you do not know the APN, ask your mobile communications operator for it.

Wi-Fi Tray App

▶ Open the Wi-Fi tray app by clicking the Wi-Fi tray icon. The icon is dynamic and represents the state of the connection.

The Wi-Fi tray app opens. Using the icons at the top of the window, you can:

▶ Use the toggle switch of the Wi-Fi tray app to turn Wi-Fi off and on.



▶ Add a hidden network.

▶ Scan for Wi-Fi networks to refresh the list of available networks.

▶ Check the details of the connected network.

▶ Switch between the **Known Networks** list and the **Available Networks** list.

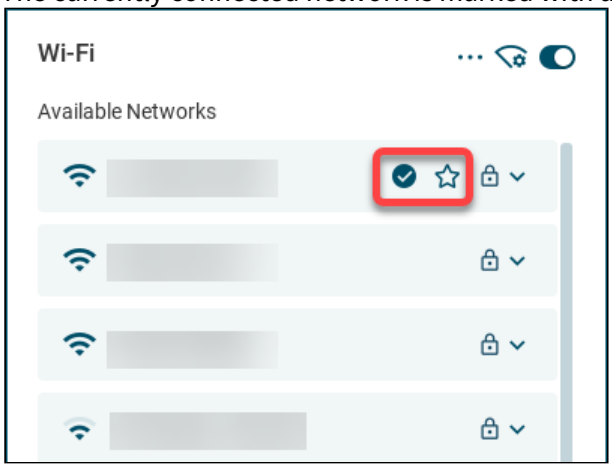
If the **Automatic switch of network connection** parameter is enabled under **Network > Common Settings**, the toggle can get disabled. For more information, see Common Settings (see page 156).

Connect to Available Wi-Fi Networks

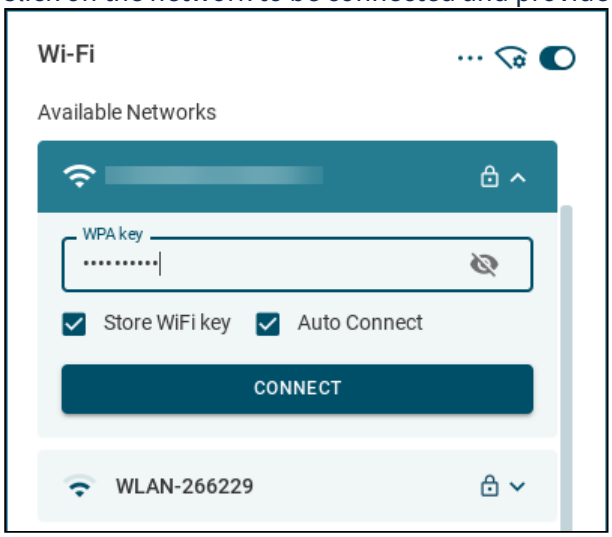
To connect to a network, do the following:

More...

1. Switch to the **Available Networks** list or use the **Scan Wifi** icon to refresh the list.
   - The list of networks is sorted according to their signal strength.
   - Previously configured networks are marked with a star icon. They are listed in the Known Networks List.
   - The currently connected network is marked with a tick icon.



2. Click on the network to be connected and provide the network key.



You can enable the **Store WiFi key** and **Auto Connect** parameters according to your needs.

3. Click **Connect**.
   The Wi-Fi tray icon changes to show the active connection.
   The configured network is listed in the **Known Networks** list.
   The configured connections get listed in the IGEL Setup under **Network > Wireless > Wi-Fi Networks**. For more information, see Wi-Fi Networks (see page 145).

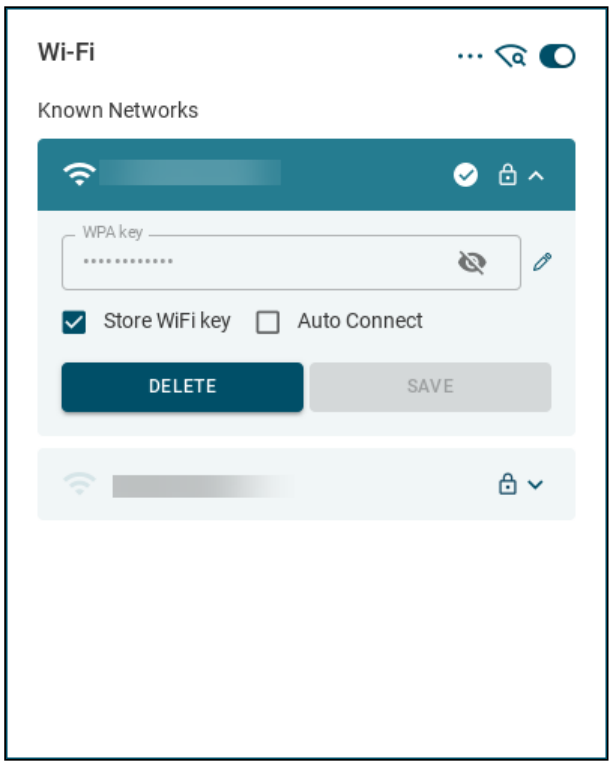
4. To disconnect from the connected network, click on the network and click **Disconnect**.

Edit and Delete Known Networks

If you want to edit or delete a network, do the following:

More...

1. Switch to the **Known Networks** list.



2. Click on the network to be edited or deleted.
   You can enable the **Store WiFi key** and **Auto Connect** parameters according to your needs.

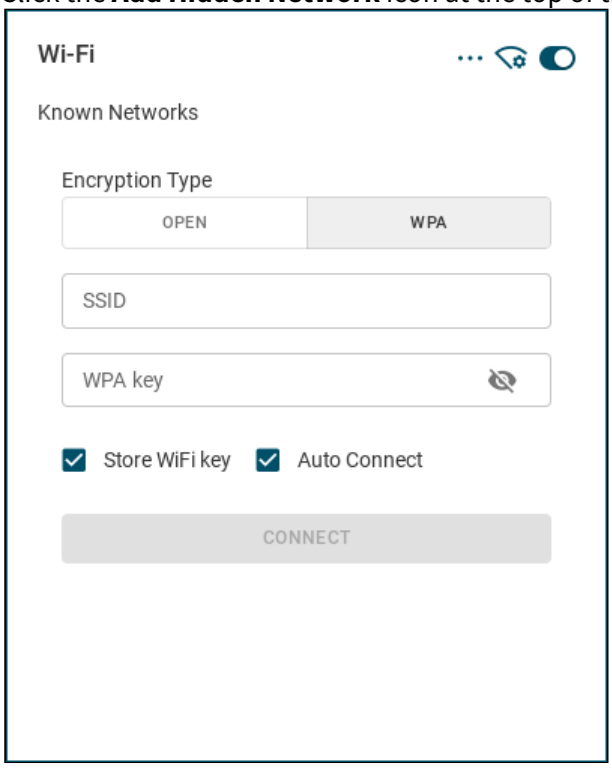
3. Click **Save** to save the changed configuration or click **Delete** to remove the network from the list.

Connect to Hidden Networks

If you want to connect to a hidden network, do the following:

More...

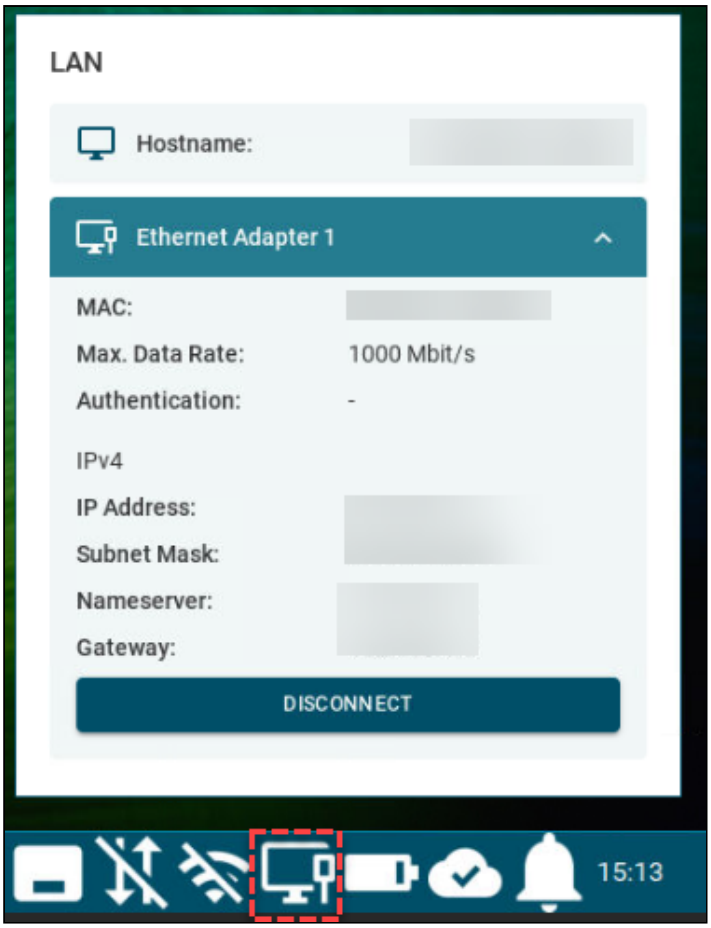
1. Switch to the **Known Networks** list.
2. Click the **Add Hidden Network** icon at the top of the window.



3. Set the **Encryption Type**, provide the SSID and the network key.
4. Click **Connect**.
   The Wi-Fi tray icon changes to show the active connection.
   The configured network is listed in the **Available Networks** list and in the **Known Networks** list.
   The configured connections get listed in the IGEL Setup under **Network > Wireless > Wi-Fi Networks**. For more information, see Wi-Fi Networks (see page 145).
5. To disconnect from the connected network, click on the network in the **Available Networks** list and click **Disconnect**.

LAN Tray App

▶ Open the LAN tray app by clicking the LAN tray icon. The app displays details about the LAN network connection and provides an option to easily connect to and disconnect from LAN networks.



The tray icon is dynamic and represents the state of the connection as described below.

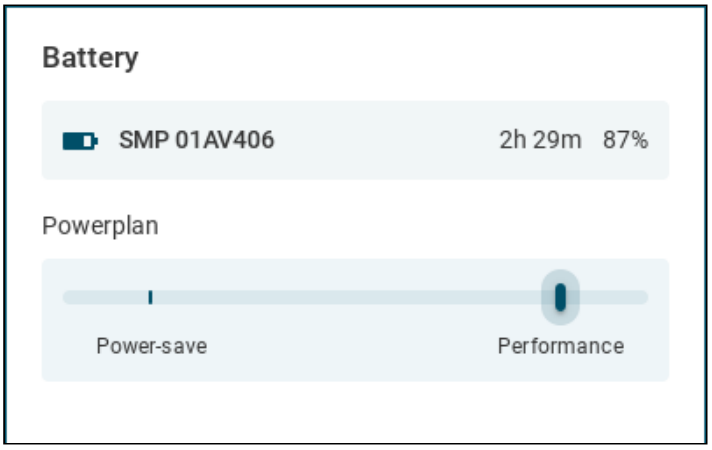
More ...

LAN Status	Taskbar Icon
Connected	
No connection	
Connected, but no internet	
Connecting	
Disconnected by user	

LAN Status	Taskbar Icon
Connection error	

Battery Tray App

▶ Open the tray app by clicking the battery tray icon. The icon is dynamic and represents the state of the battery charge. is displayed when the battery is charging and when it is discharging.



The battery tray app shows information for all available batteries, including multiple internal batteries and batteries of connected bluetooth devices. You can set the CPU power plan regulation under **Powerplan**.

> ⓘ The CPU power plan is set for the current mode in use (AC or Battery). The CPU power plan can be set for all modes under **System > Power Options > System**. For the description of the power plans, see System Power Options in IGEL OS 12 (see page 297).

UMS Tray App

▶ Open the UMS tray app by clicking the UMS tray icon. The icon is dynamic and represents the state of the connection as described below. The tray app also displays basic information of the connected Universal Management Suite (UMS), like **IP** address and **Hostname**.

UMS Connection Status	Taskbar Icon
Connected	

UMS Connection Status	Taskbar Icon
Connecting	
Disconnected	
Unmanaged	

Starting Methods for Apps

For all sessions that can be started by the user, a selection of starting methods is provided.

Session name: Name for the session.

The session name must not contain any of these characters: `\ / : * ? “ < > | [ ] { } ( )`

Starting Methods for Session

Start menu

☑ The session can be launched from the start menu.

Menu folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the start menu and in the desktop context menu.

Start menu's system tab

☑ The session can be launched with the start menu's system tab.

Application Launcher

☑ The session can be launched with the Application Launcher.

Application Launcher folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used in the Application Launcher.

Desktop

☑ The session can be launched with a program launcher on the desktop.

Desktop folder

If you specify a folder name or a path comprising a number of folder names separated by "/", a menu path will be created for the session. The menu path will be used for the program launcher on the desktop.

Desktop context menu

☑ The session can be launched with the desktop context menu.

Quick start panel

☑ The session can be launched with the quick start panel.

Password protection

Specifies which password will be requested when launching the session.

Possible values:

- **None**: No password is requested when launching the session.
- **Administrator**: The administrator password is requested when launching the session.
- **User**: The user password is requested when launching the session.
- **Setup user**: The setup user password is requested when launching the session.

⚠ **Password protection** only works if the selected password is configured under **Security > Password**. Without the password configuration, the session will launch without requesting a password. For more information, see Password (see page 245).

Hotkey Configuration

Hotkey

☑ The session can be started with a hotkey. A hotkey consists of one or more **modifiers** and a **key**.

Modifiers

A modifier or a combination of several modifiers for the hotkey. You can select a set key symbol/combination or your own key symbol/combination. A key symbol is a defined chain of characters, e.g. `Ctrl`.

⚠ Do not use [AltGr] as a modifier (represented as `Mod5`). Otherwise, the key that is configured as a hotkey with AltGr cannot be used as a regular key anymore. Example: If you configure [AltGr] + [E] as a hotkey, it is impossible to enter an "e".

These are the pre-defined modifiers and the associated key symbols:

- (No modifier) = `None`
- ⇧ = `Shift`
- [Ctrl] = `Ctrl`
- ⊞ = `Mod4`

> When this keyboard key is used as a modifier, it is represented as `Mod4`; when it is used as a key, it is represented as `Super_L`.

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + = `Ctrl|Super_L`

Key

Key for the hotkey

> To enter a key that does not have a visible character, e. g. the [Tab] key, open a terminal, log on as `user` and enter `xev -event keyboard`. Press the key to be used for the hotkey. The text in brackets that begins with `keysym` contains the key symbol for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Autostart Configuration

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be relaunched automatically after the termination.

Autostart delay

Waiting time in seconds between the complete startup of the desktop and the automatic session launch.

Autostart notification

This parameter is available if **Autostart** is activated and **Autostart delay** is set to a value greater than zero.

☑ For the duration defined by **Autostart delay**, a dialog is shown which allows the user to start the session immediately or cancel the automatic session start.

☐ No dialog is shown; the session is started automatically after the timespan specified with **Autostart delay**.

Autostart requires network

☑ If no network is available at system startup, the session is not started. A message is shown. As soon as the network is available, the session is started automatically.

☐ The session is started automatically, even when no network is available.

Boot Process

The following stages of the boot process are important from a configuration perspective:

1. Second stage loader, the loading of the kernel
   - You can access the Boot Menu in this stage. For details, see Boot Menu (see page 381).
   - You can set up Base Custom Commands with specific execution times. For details, see Base (see page 319).

2. Network Integration
   - After the kernel has loaded, network configurations are applied. Depending on the settings of the endpoint device, there are three possible ways of integrating the endpoint device into the network environment:
     - **DHCP**
     - **BOOTP**
     - **Manually configured IP address**

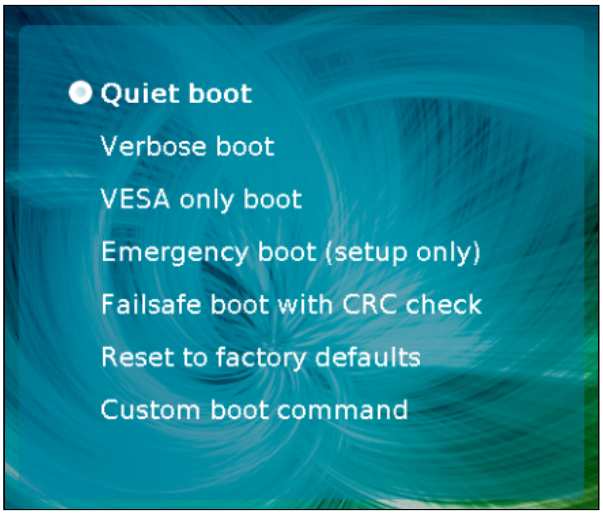
     > The network interface can be stopped and restarted on the Linux Console (accessible via [Ctrl]+[Alt]+[F11]) with this command: `/etc/init.d/network stop` `/etc/init.d/network start`

3. Starting the X server and the local windowmanager
   - You can set up Desktop Custom Commands for the stages of the X server launch. For details, see Desktop (see page 321).

Boot Menu

During the boot process, a boot menu is available on request. Through this menu, you can start boot modes for troubleshooting. There are modes to access system parameters, or to reset the device to the factory defaults if the device is configured incorrectly or if you experience problems when booting.

▶ During the boot process, press the [Esc] key repeatedly in rapid succession in the second stage loader, when the `loading kernel` message is shown on the screen.
The boot menu is displayed with the available boot modes:



Using the arrow keys, navigate to one of the boot modes and press the [Enter] key to start the process. You can start the following boot modes:

- Quiet boot (see page 381): Normal startup. (Default)
- Verbose boot (see page 382): Start with system messages and an interactive root shell
- VESA only boot (see page 382): Basic graphic boot
- Emergency boot (setup only) (see page 382): Only the **Setup** window is available
- Failsafe boot with CRC check (see page 383): Start with an integrity check of the operating system
- Reset to factory defaults (see page 383): Reset the client to factory defaults
- Custom boot command (see page 383): Boot with configurable command line options

Quiet Boot

Quiet boot is the default boot mode. It is the normal startup mode. In this mode, all kernel messages are disabled and the graphical user interface is started.

Verbose Boot

Unlike in **Quiet boot** mode, the kernel messages are shown in **Verbose boot** mode. The boot process also pauses before the graphics system and the user session start.

This gives you an opportunity to open a root shell and interactively execute debugging commands (for example, `ifconfig`).

> Only use the root shell if you have adequate knowledge of Linux or if you are instructed to do so by the IGEL Helpdesk and are given appropriate guidance. Incorrect use can destroy the operating system.

To execute debugging commands:

1. Select **Verbose boot** from the boot menu.
2. Wait until the boot messages stop at `Reached target IGEL Network Online`.
3. Open a virtual console with one of the key combinations:
   - [Ctrl] + [Alt] + [F11]
   - [Ctrl] + [Alt] + [F12]
4. Log in by pressing [Return] and enter the root password if necessary.
5. Go through the desired individual commands.
6. Now enter the following command to continue the normal boot process: `systemctl default`
   The graphical user session starts.

VESA Only Boot

Use this boot mode if normal boot has graphic issues, for example, if the device has limited Graphical Processor Unit (GPU) support. This mode is not manufacturer specific. In this mode resolution and multimonitor mode and performance might be limited.

Emergency Boot (Setup Only)

In the **Emergency boot** mode, the device is started without network drivers and with a resolution of 640 x 480 - 60 Hz. After the boot process, the **Setup** window is opened automatically.

This mode is useful, for example, if you have selected an excessively high screen resolution or a wrong mouse type and these settings can no longer be changed in the normal setup. Unlike with a reset, the setup opens with the actual settings.

▶ Once you are done with the changes, close the setup window to reboot the device.

Failsafe Boot with CRC Check

During a **Failsafe boot**, a check of the file system is carried out first. Then, the **Verbose boot** is started.

This mode is helpful if you no longer have a bootable system after a firmware update. The **Failsafe boot** checks where the problem is. If need be, an old version will be booted and you will need to repeat the firmware update.

Reset to Factory Defaults

If you select **Reset to factory defaults**, all personal settings on the device (including your password and the sessions you have configured) will be lost.

Before the procedure is carried out, a warning message is displayed. If the device is protected by an administrator password, you will be prompted to enter this password.

If you know the password:

1. Confirm the warning message.
2. Enter the password. You have three attempts.

If you do not know the password:

1. Confirm the warning message.
2. When you are prompted to enter the password, press the [Enter] key three times.
3. Press [c].
   The Terminal Key is displayed.
4. Contact us using license@igel.com[21].
5. Enter the Terminal Key that is shown, the firmware version, and your contact details.
   IGEL will send you a Reset to Factory Defaults Key that is specific to your device. To ensure that the process is as straightforward and yet as secure as possible, each key is valid for just one device.

You can also reset your device to factory defaults through the UMS Web App. In this case, the device will be removed from the UMS and you will have to register your device with the UMS again. For details, see Resetting a Device to Factory Defaults via the IGEL UMS Web App.

Custom Boot Command

In the **Custom boot command** mode, preconfigured options are placed on the kernel command line. This allows you, for example, to investigate and rectify problems with specific hardware components.

21 mailto:license@igel.com

The **Custom boot command** is merely a temporary solution – it is not an everyday booting method. It must therefore be selected manually in the boot menu.

To configure the options for the **Custom boot command**, proceed as follows:

1. Open a local terminal and log in as `root`.
2. Enter the following command to bring up the current options:
   ```
   bootreg get /dev/igfdisk boot_cmd
   ```
3. Save your desired options with the following command:
   ```
   bootreg set /dev/igfdisk boot_cmd "<Your Options>"
   ```
4. Check the options that you have entered:
   ```
   bootreg get /dev/igfdisk boot_cmd
   ```

   If you would like to delete options for the Custom boot command, leave an empty string of characters in their place: `bootreg set /dev/igfdisk boot_cmd ""`

IGEL Tech Video

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

https://www.youtube.com/watch?v=bpfWNIR6eUE

In the video, IGEL OS11 is used for demonstration.

How to Deploy IGEL OS 12 with IGEL OS Creator (OSC)

With the IGEL OS Creator (OSC), you can install IGEL OS 12 on any supporting device. Moreover, you can use the IGEL OS Creator to recover a broken installation of IGEL OS that cannot boot anymore.

> Installing the IGEL OS operating system via OSC destroys all data on the target device's mass storage device (hard disk, flash memory, SSD).

Devices Supported by IGEL OS 12

For a detailed list, see Devices Supported by IGEL OS 12.

Licensing

For information on licensing, see Essential IGEL Licensing FAQ.

Create USB Installation Medium

Windows

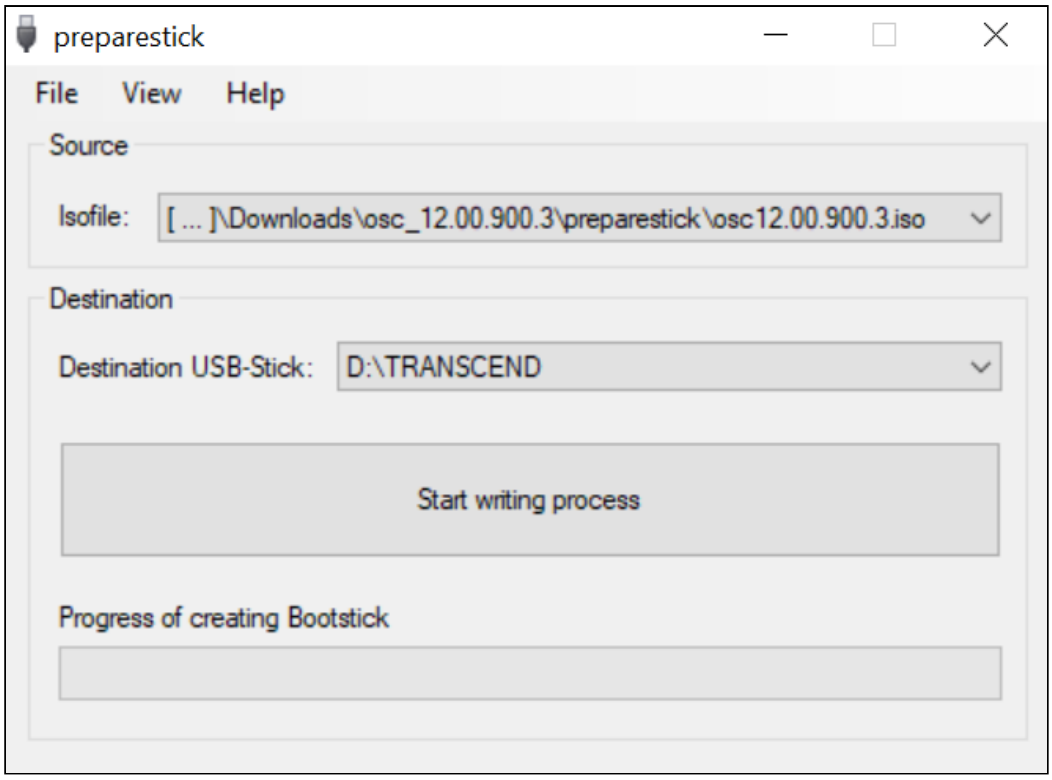
1. Download the ZIP archive for OS Creator from the IGEL Download Server[22]:
   - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).

2. Unzip the contents into a local directory.

3. Connect a USB memory stick with at least 4 GB capacity to the computer.
   All existing data on the USB memory stick will be destroyed.

4. Double-click the `preparestick.exe` file from the unzipped directory.
   If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.

22 https://www.igel.com/software-downloads/cosmos/



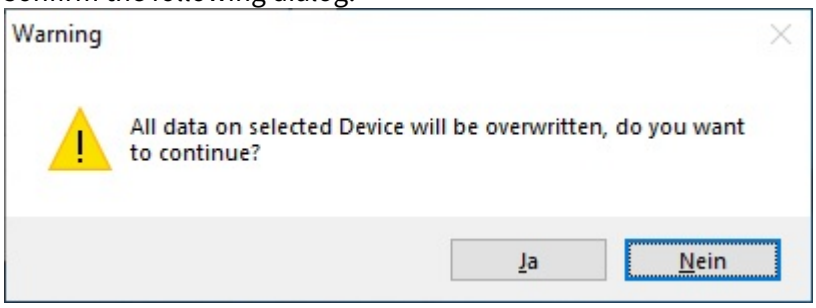
The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

5. Under **Isofile**, select the appropriate ISO file, e.g. `osc12.01.110.iso`

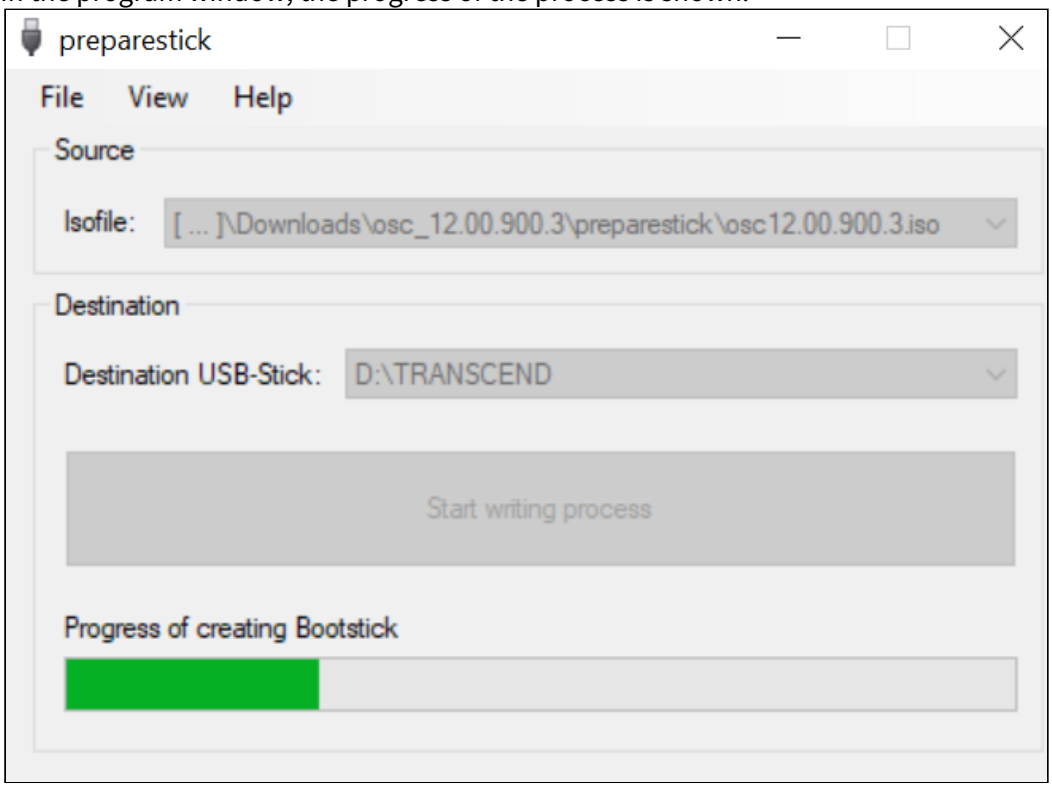
6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.
   It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.
   Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List**.

7. Click **Start writing process**.

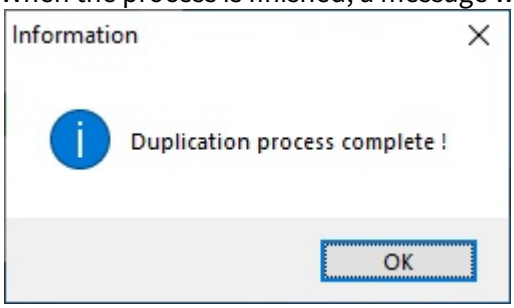
8. Confirm the following dialog:



In the program window, the progress of the process is shown.



When the process is finished, a message window is displayed.



9. Close the message window and the program.

10. After about 3 seconds, remove the USB memory stick.

> If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

The USB memory stick for OSC installation is ready for use.

Linux

1. Download the ZIP archive for OS Creator from the IGEL Download Server[23]:
   - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).

2. Unzip the contents into a local directory.

3. From this directory, you will need the ISO file (e.g. `osc12.01.110.iso` or `osc12.01.110_legacy.iso`) to create a bootable medium.

4. Connect a USB memory stick with at least 4 GB capacity to the computer.

   > All existing data on the USB memory stick will be destroyed.

5. Open a terminal emulator and enter the command `dmesg` to determine the device name of the USB memory stick.
   Example output:

```
[...]
[19514.742229] scsi 3:0:0:0: Direct-Access JetFlash Transcend 8GB 1100 PQ: 0 ANSI: 6
[19514.742805] sd 3:0:0:0: Attached scsi generic sg1 type 0
[19514.744688] sd 3:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/7.35 GiB)
[19514.745370] sd 3:0:0:0: [sdb] Write Protect is off
[19514.745376] sd 3:0:0:0: [sdb] Mode Sense: 43 (0) 00 00 00
[19514.746040] sd 3:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[19514.752438] sdb: sdb1
```

23 https://www.igel.com/software-downloads/cosmos/

In this example, the device name searched for is `/dev/sdb`.

> Ensure that you have determined the correct device name. Use of the `dd` command in the next step can destroy your operating system if you use the wrong device name.

6. The following command writes the installation data to the USB memory stick:
   `dd if=osc12.01.110.iso of=/dev/sdX bs=1M oflag=direct`
   Replace `sdX` with the device name of the USB memory stick that you have determined.
   When the `dd` command has terminated, you can see the terminal emulator input prompt again.

7. Wait for about 3 seconds after the `dd` command has terminated, and remove the USB memory stick.

   > If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

   The USB memory stick for OSC installation is ready for use.

Create DVD Installation Medium

The ISO file in the installation directory for OSC is a so-called hybrid image. It can not only be copied onto USB storage devices but can also be used to create a bootable DVD.

Burn ISO Image (Windows)

1. In Explorer, open the directory that contains the ISO file.
2. Right-click on the ISO file.
3. Select **Burn disc image**.

Burn ISO Image (Linux)

Under Linux, various burning programs with a graphical user interface or for the command line are available.

The Ubuntu Wiki[24] explains how to burn an ISO image onto a DVD using a number of programs.

24 https://help.ubuntu.com/community/BurningIsoHowto#Burning_from_Ubuntu

Boot Settings

OSC works on systems with BIOS and UEFI.

Your system must support booting from USB storage media or DVD. This may already be enabled, or you may have to enable it yourself.

> IGEL OS 12 supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS. For instructions on how to check whether Secure Boot has been properly enabled, ee Verifying that Secure Boot is Enabled .
> For UEFI Secure Boot on devices manufactured by IGEL, see UEFI Secure Boot Enabling Guides.

> If IGEL OS fails to boot in UEFI mode, try it in legacy/BIOS mode. IGEL OS will then be installed in legacy/BIOS mode.

> For older devices or if you haven't been able to boot the installer at all, use the legacy installer under https://www.igel.com/software-downloads/workspace-edition/ **> OS 11 > OS CREATOR > LEGACY**.

General Hints on Changing the Boot Settings

The required key presses for this may vary from vendor to vendor. However, here are some hints:

▶ While the device is booting, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access a list of boot devices and select your USB installation medium.

▶ If the above does not work, access the BIOS settings via pressing [Del], [F1], or [F2] during boot, activate booting from USB storage media and/or change the boot order.

▶ See the BIOS/UEFI documentation for your system for details of how to boot from USB storage media.

Changing the Boot Settings of Devices Manufactured by IGEL

> If the USB installation medium is not found, though the USB boot is enabled, try the following:
> - Reconnect the USB installation medium and reboot the endpoint device.
> - Use another USB port.

UD7 (H860C)

1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.

4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the installation procedure.

UD3 (M350C)

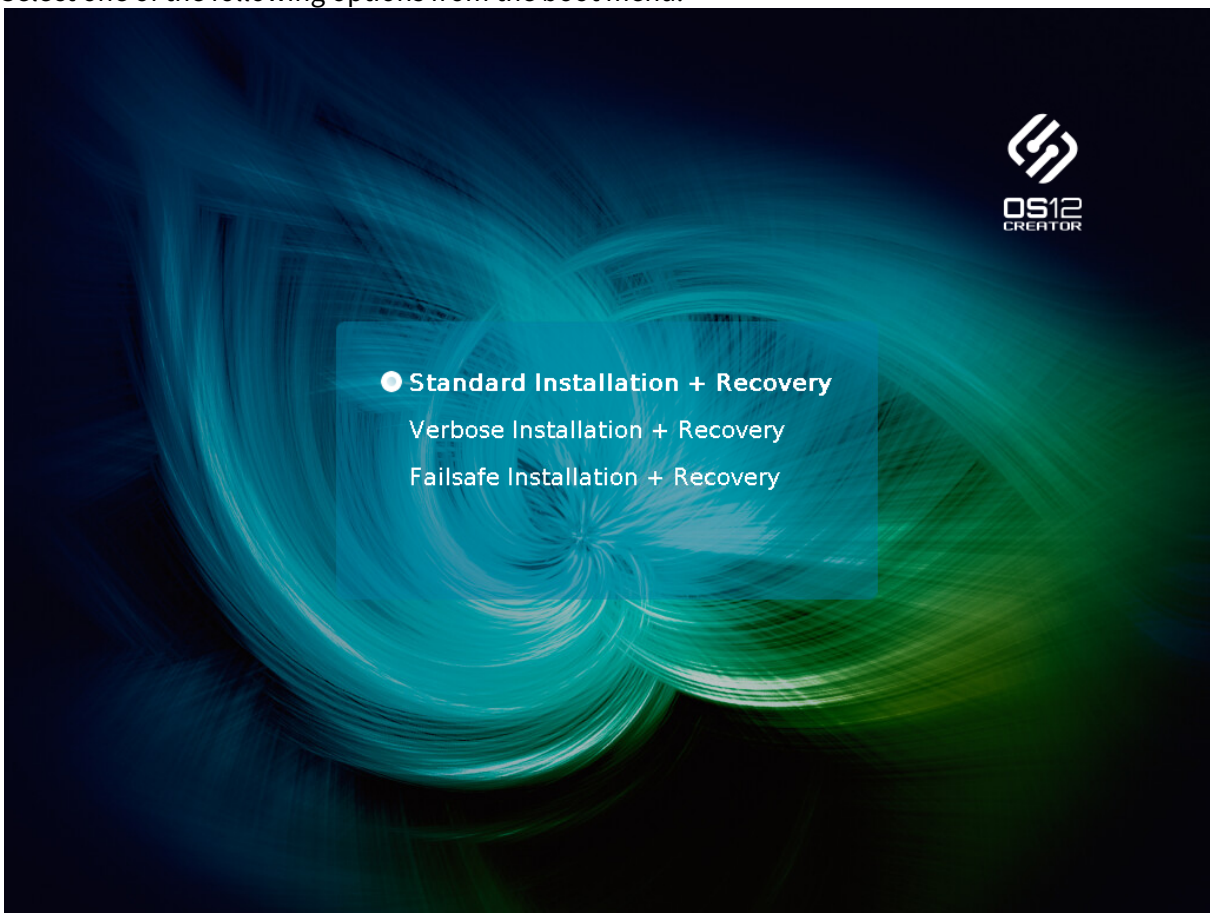
1. Power up the device while pressing the [Del] button repeatedly in rapid succession.
2. If a password prompt is shown, enter the BIOS password.
3. Select **Setup Utility**.
4. Select the **Boot** tab.
5. Set **USB Boot** to **<ENABLED>**.
6. Save the settings and exit.
7. Connect the USB stick to the device.
8. Reboot the device while pressing the [Del] button repeatedly in rapid succession.
9. Select **Boot Manager**.
10. Select the USB stick as the boot medium and press **Enter**.
11. You can continue with the installation procedure.

Installation Procedure

The installation will overwrite all existing data on the target drive.

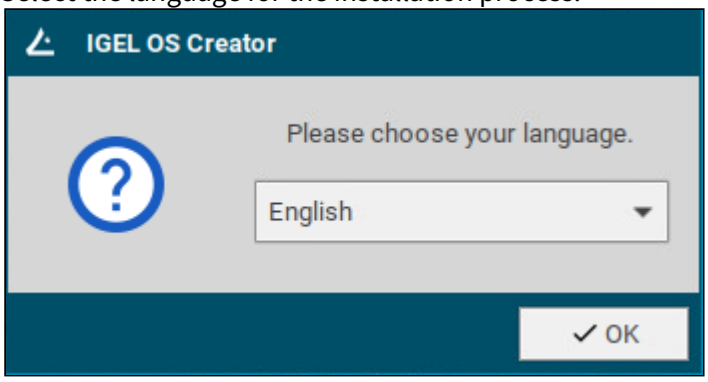
1. Connect the prepared USB memory stick to the target device and switch the target device on. General information on how you can boot from the stick can be found under Boot Settings.

2. Select one of the following options from the boot menu:

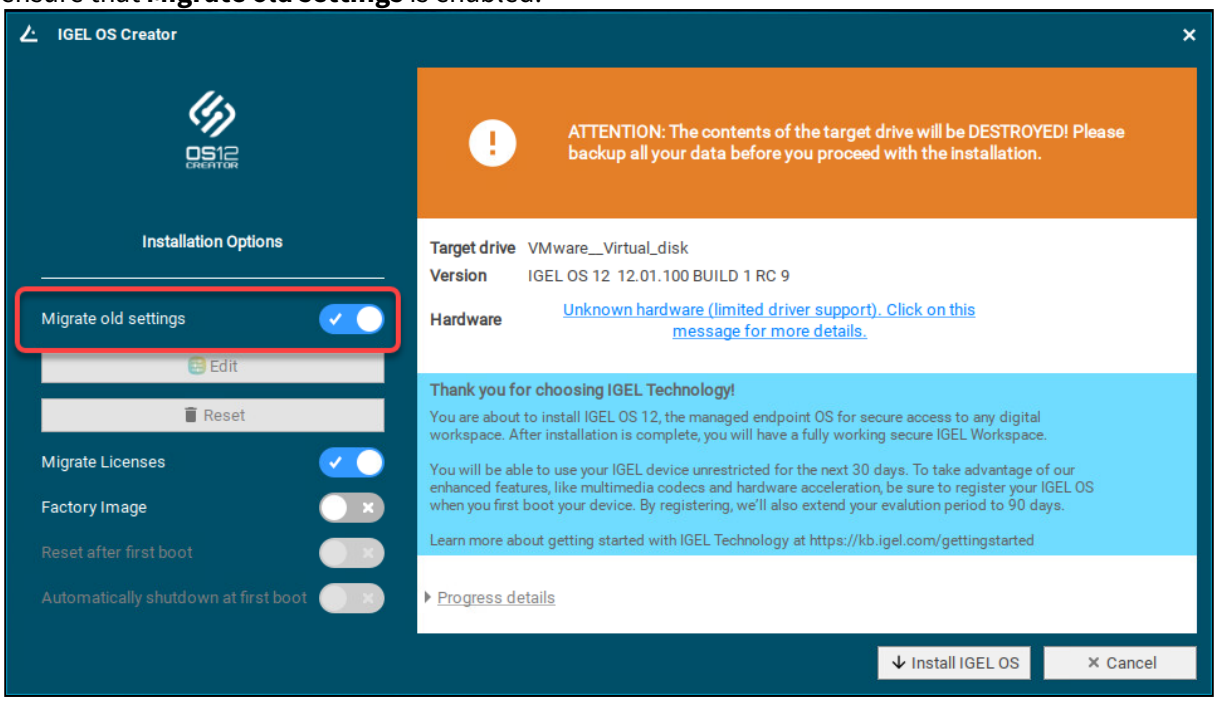


   - **Standard Installation + Recovery**: Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
   - **Verbose Installation + Recovery**: Boots the system from the USB memory stick and shows the Linux boot messages in the process.
   - **Failsafe Installation + Recovery**: Fallback mode; to be used if the graphical boot screen cannot be displayed.
   - **Memory Test**: Memory test, only available in legacy/BIOS mode. This option does not carry out an installation.

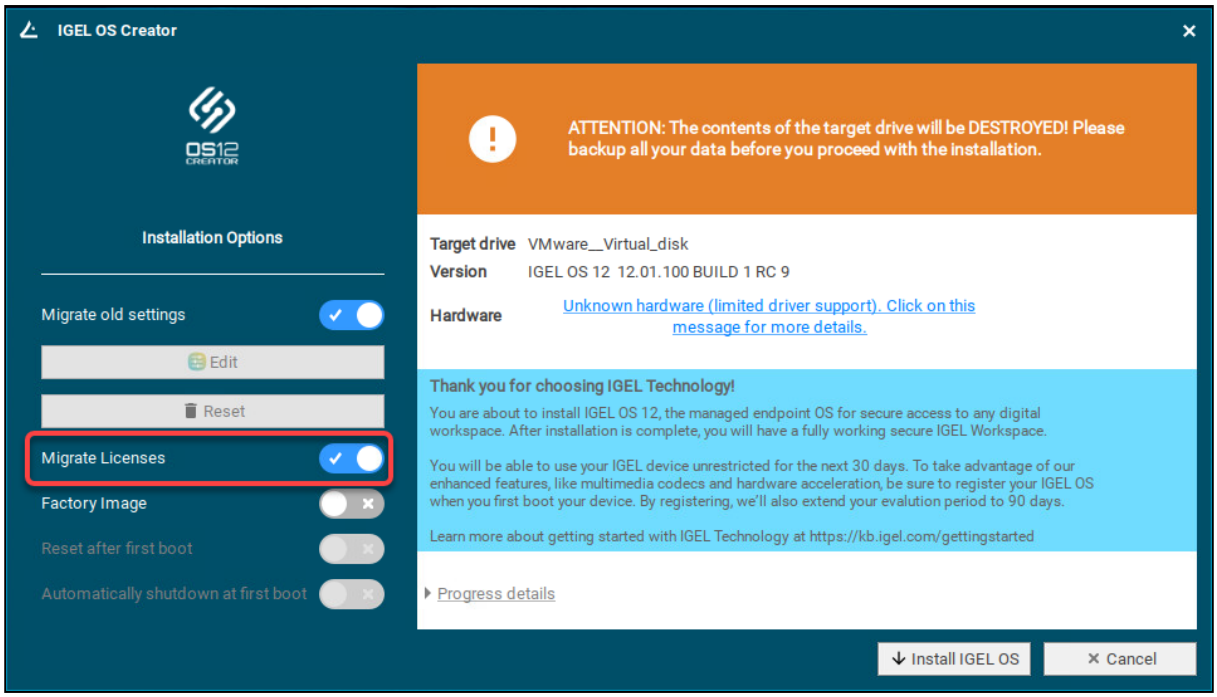
3. Select the language for the installation process.



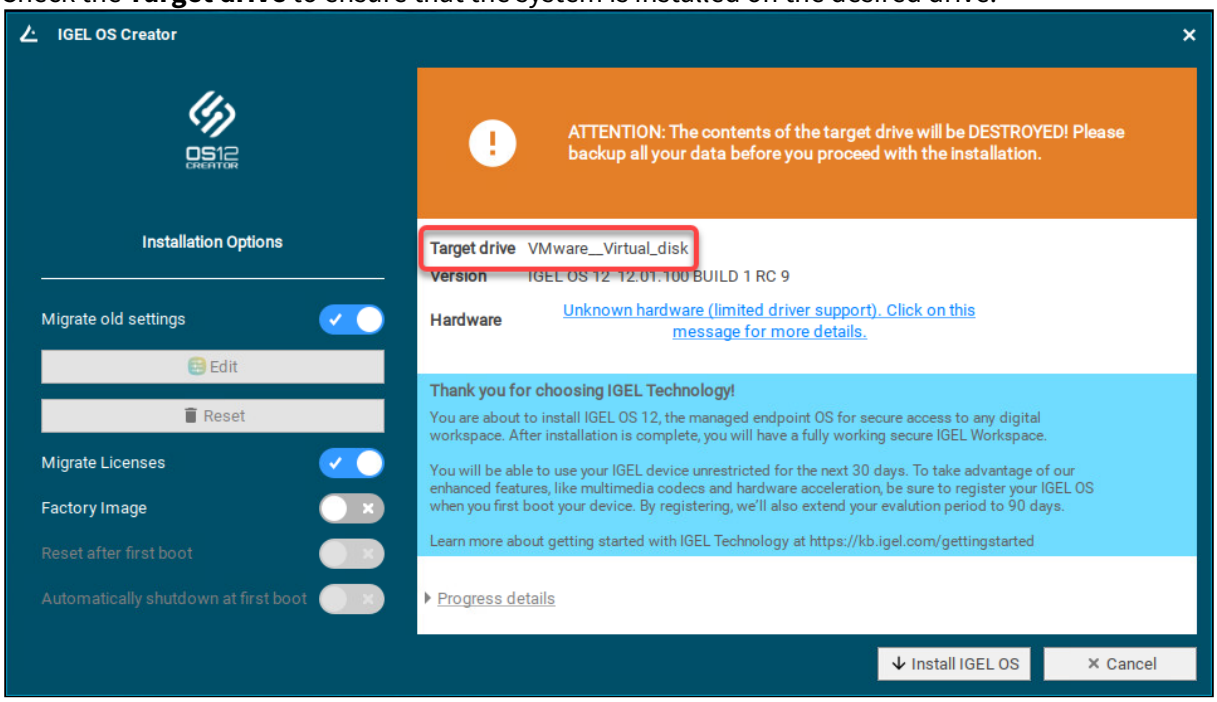
4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



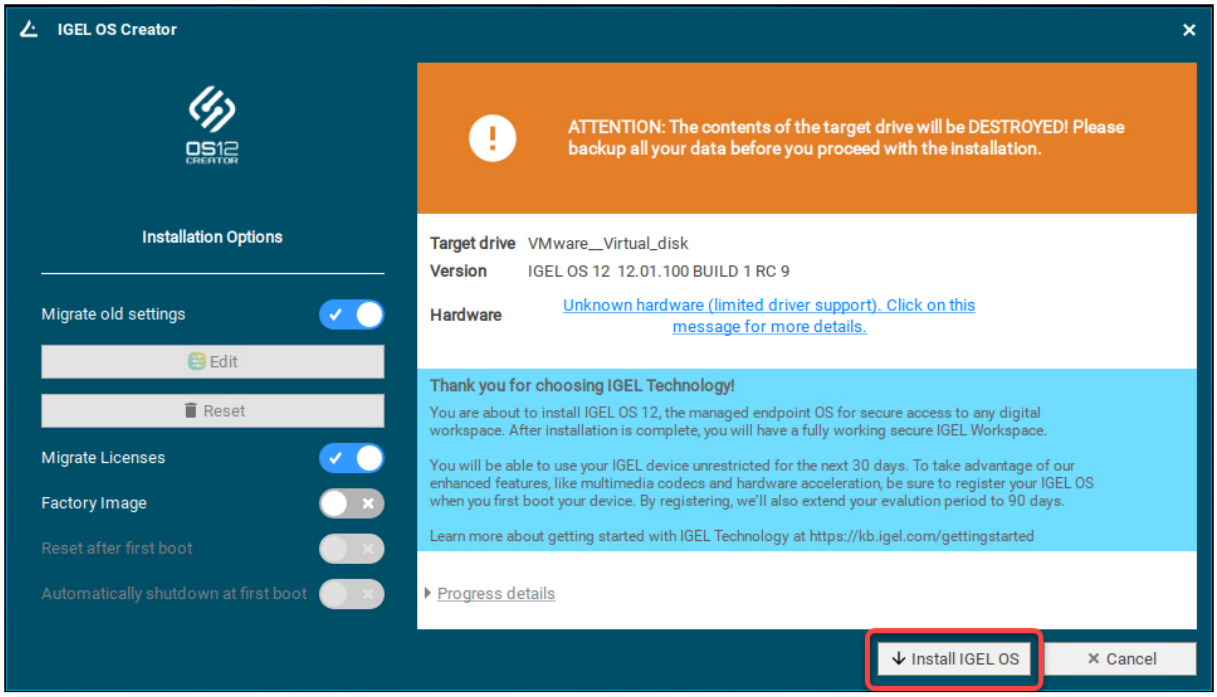
5. If one of the following is the case, make sure that **Migrate licenses** is enabled:
   - Your device has been operating with IGEL OS 11 before and you want to preserve the device's IGEL OS 11 licenses because you want to test IGEL OS 12 and downgrade to IGEL OS 11 afterward
   - Your device has been operating with IGEL OS 12 before and you want to keep the licenses on the device



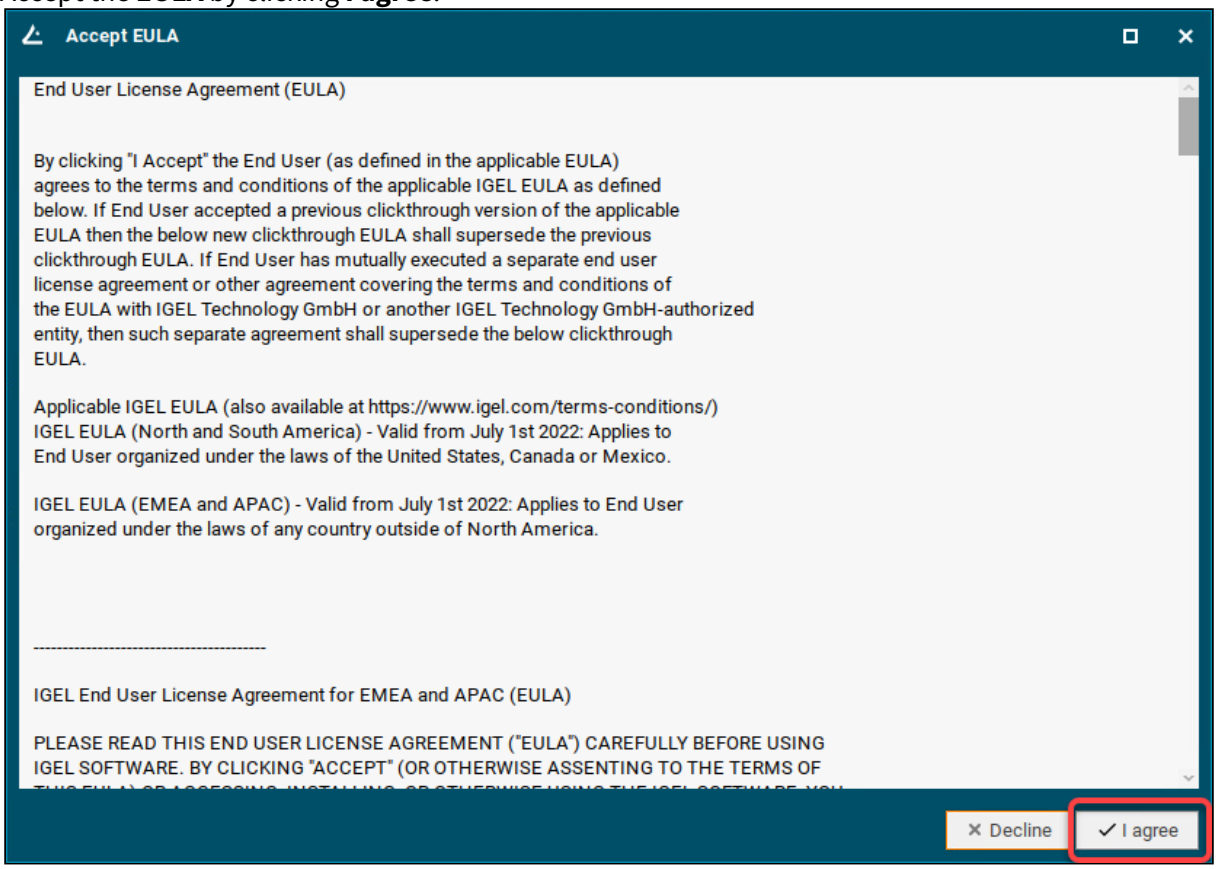
6. Check the **Target drive** to ensure that the system is installed on the desired drive.



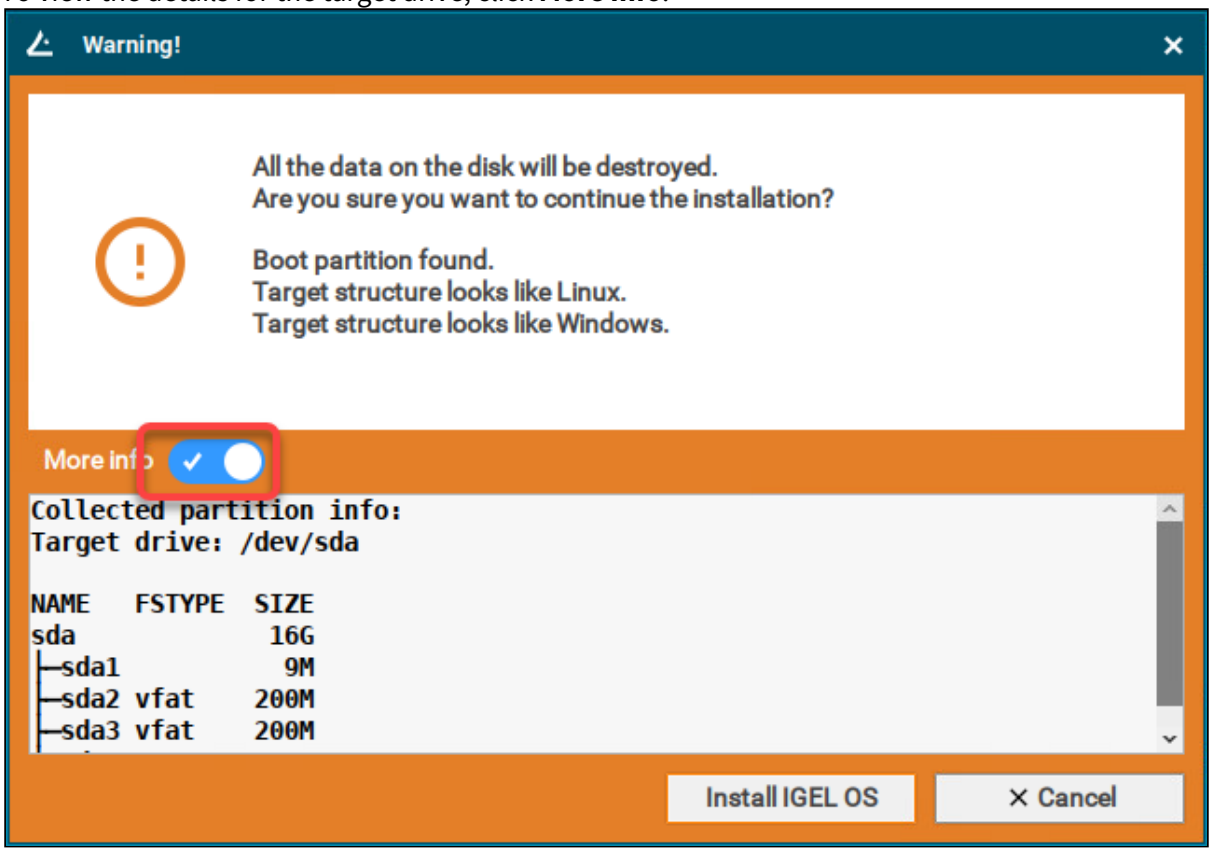
7. Click **Install IGEL OS**.



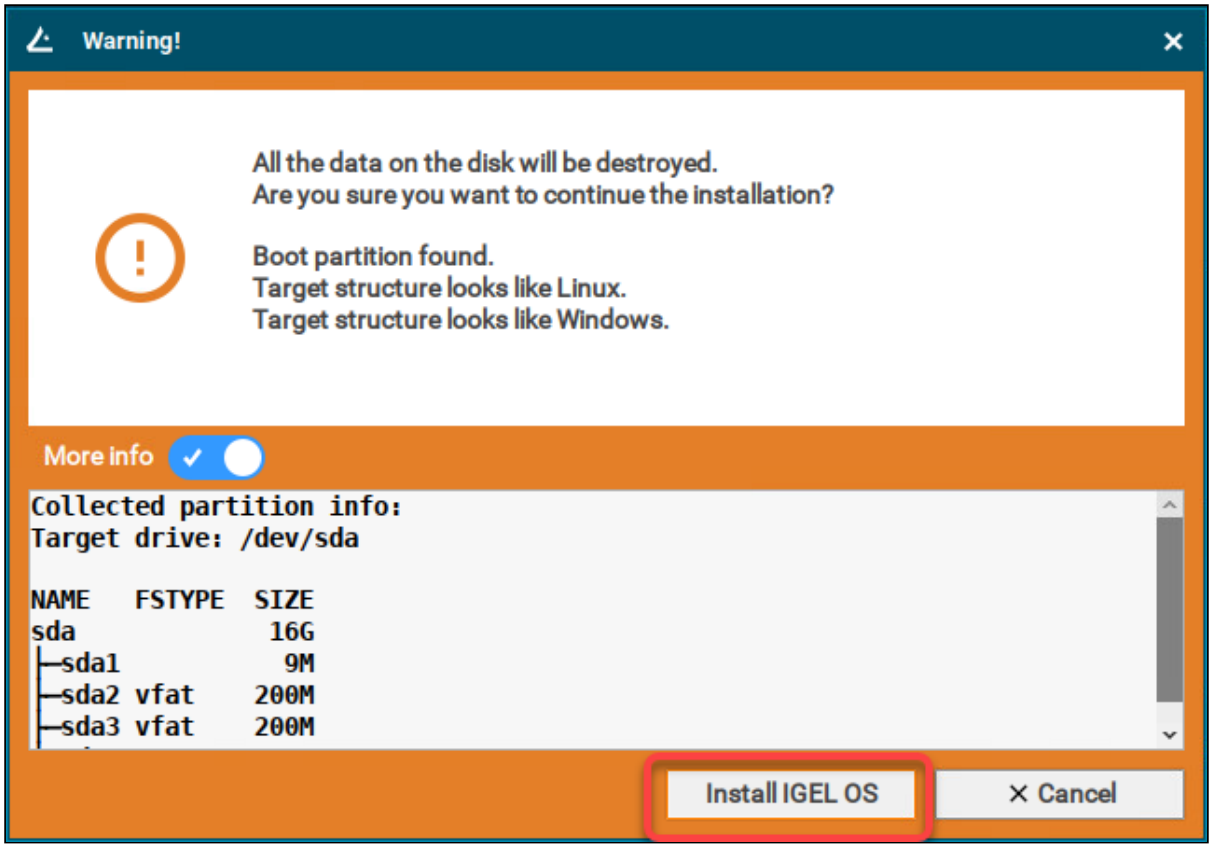
8. Accept the **EULA** by clicking **I agree**.



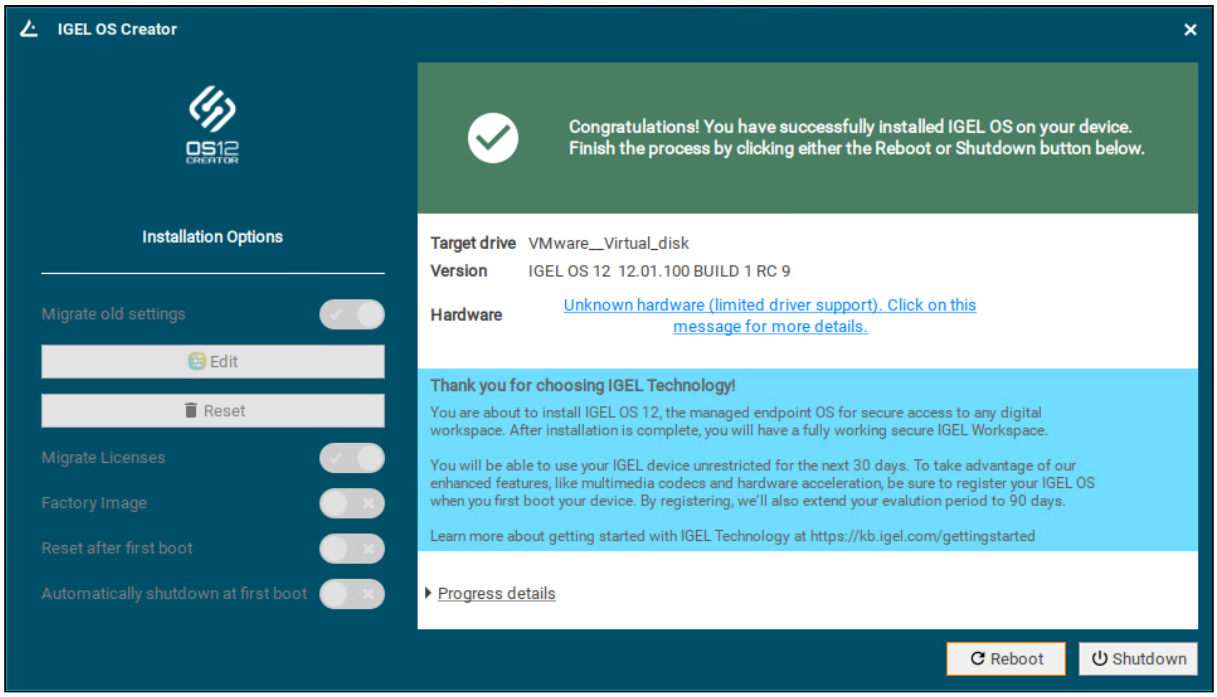
9. To view the details for the target drive, click **More Info**.



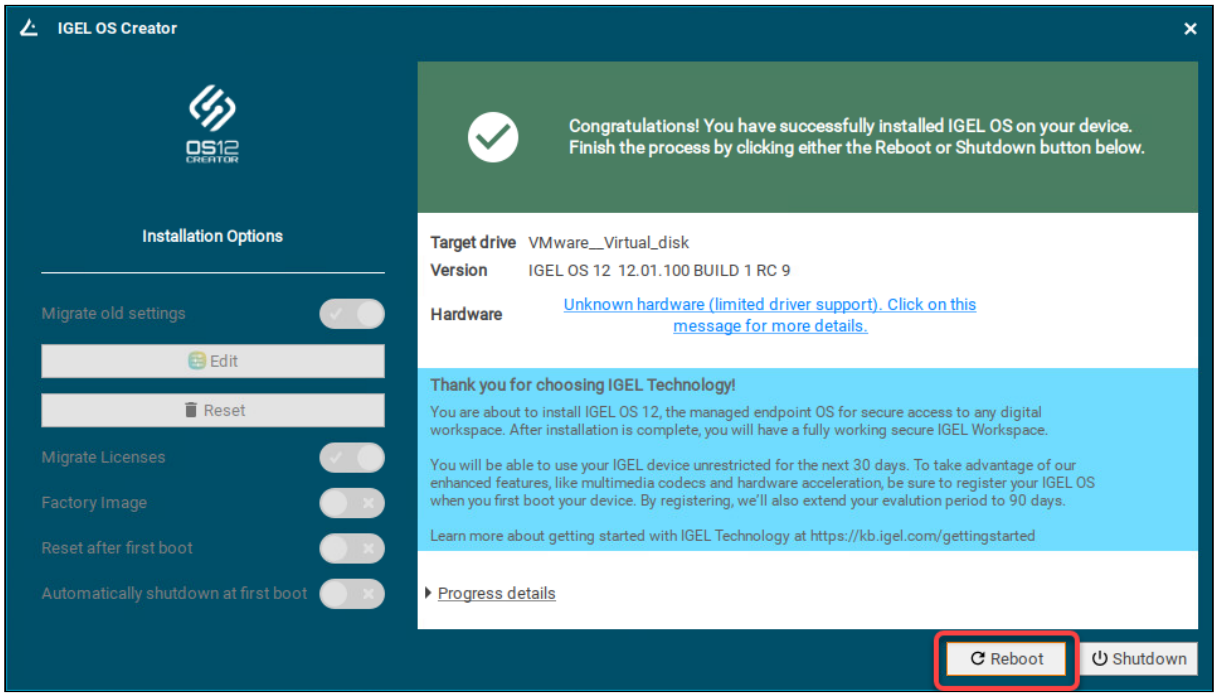
10. Click **Install IGEL OS**.



The installation program will install IGEL OS 12 on the target drive. If you see the success message, the installation is complete.

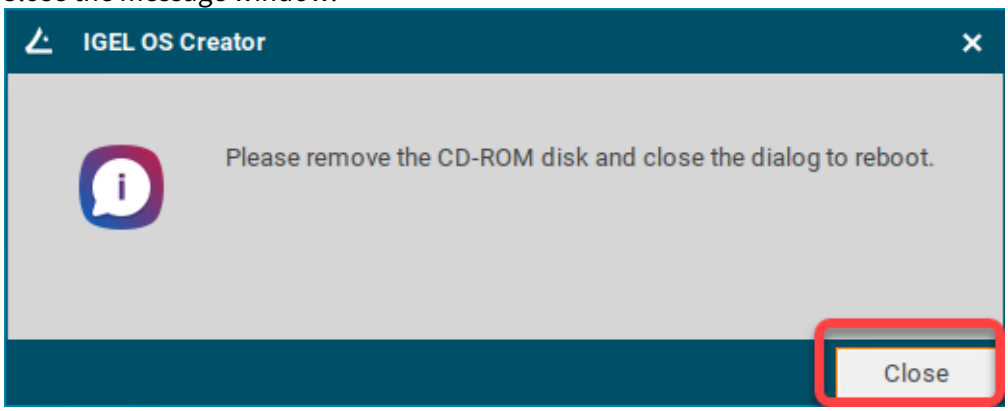


11. Click **Reboot**.



12. Remove the USB memory stick.

13. Close the message window.



The system will shut down and then boot IGEL OS 12.
The device is ready for onboarding; for details, see Onboarding.

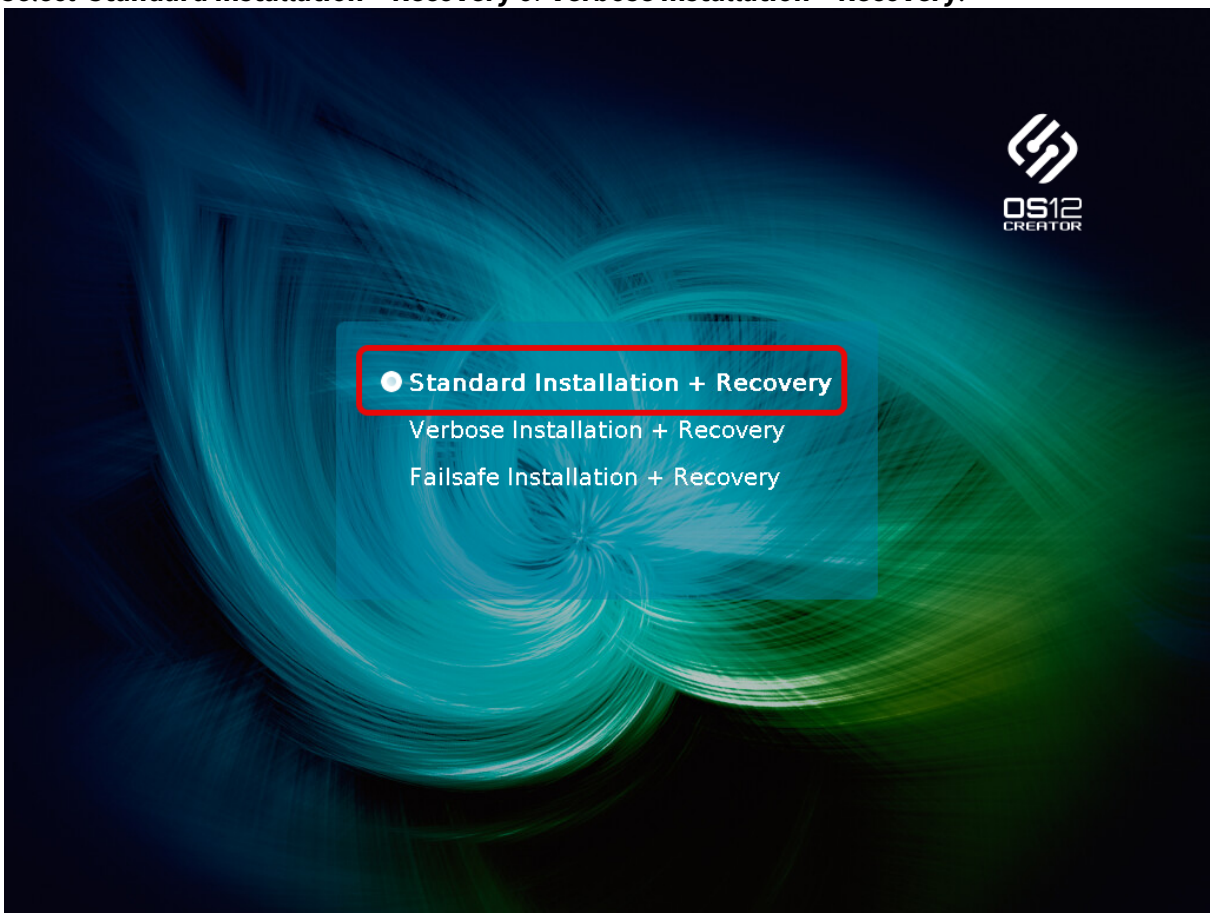
Installation Procedure for Factory Images

The installation will overwrite all existing data on the target drive.

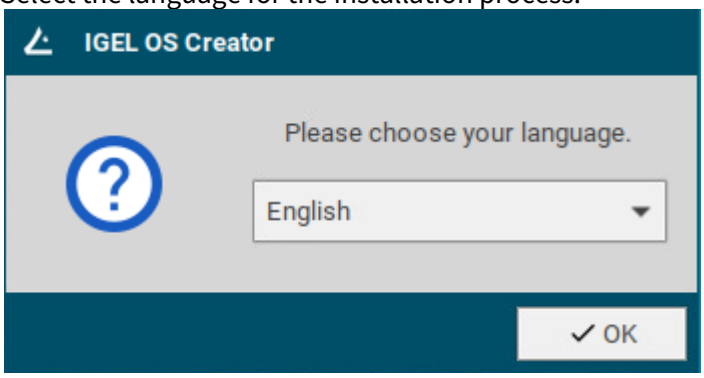
Preparing the Image

1. Connect the prepared USB memory stick to the target device and switch on the target device.

2. Select **Standard Installation + Recovery** or **Verbose Installation + Recovery**.

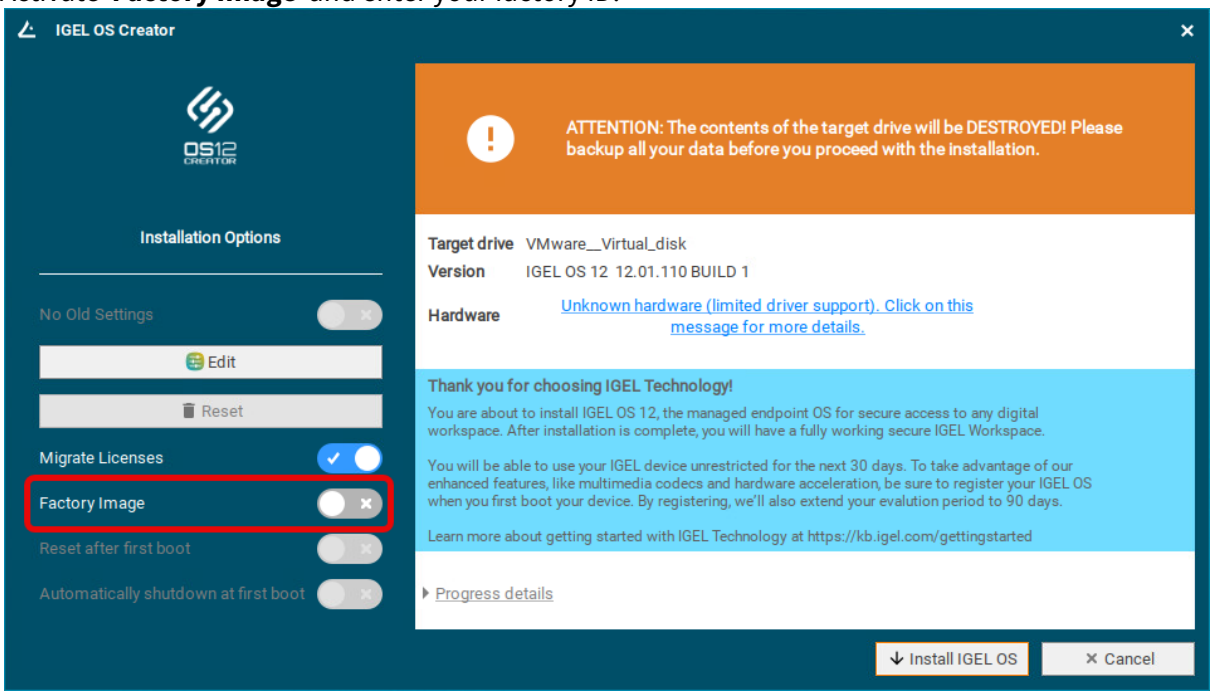


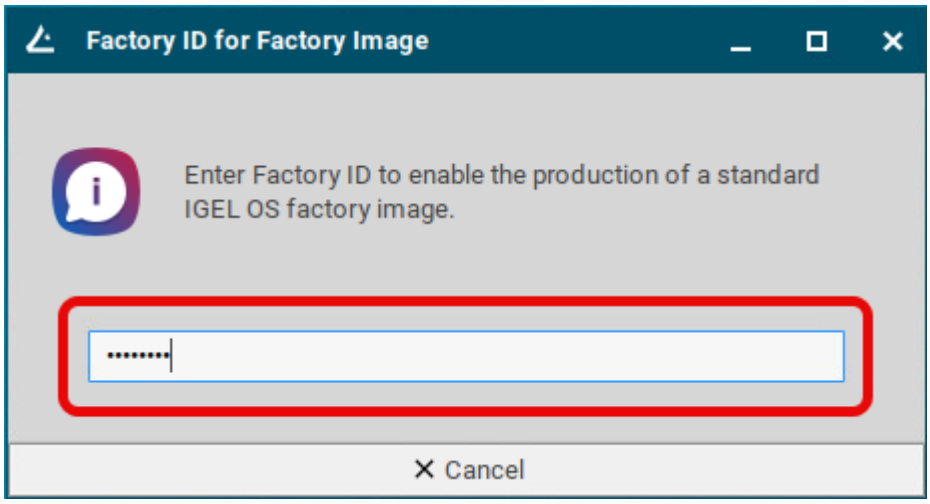
3. Select the language for the installation process.



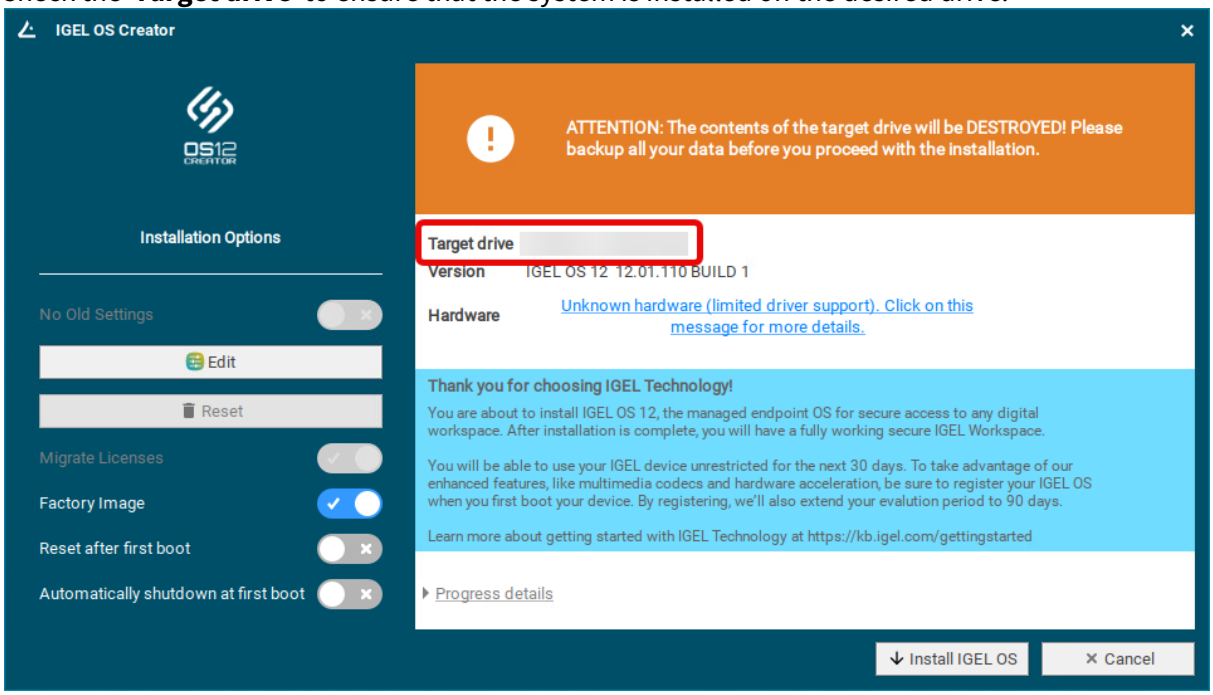
The installation program **IGEL OS Creator** opens. Here, you can configure settings for the installation process and start it.

4. Activate **Factory Image** and enter your factory ID.

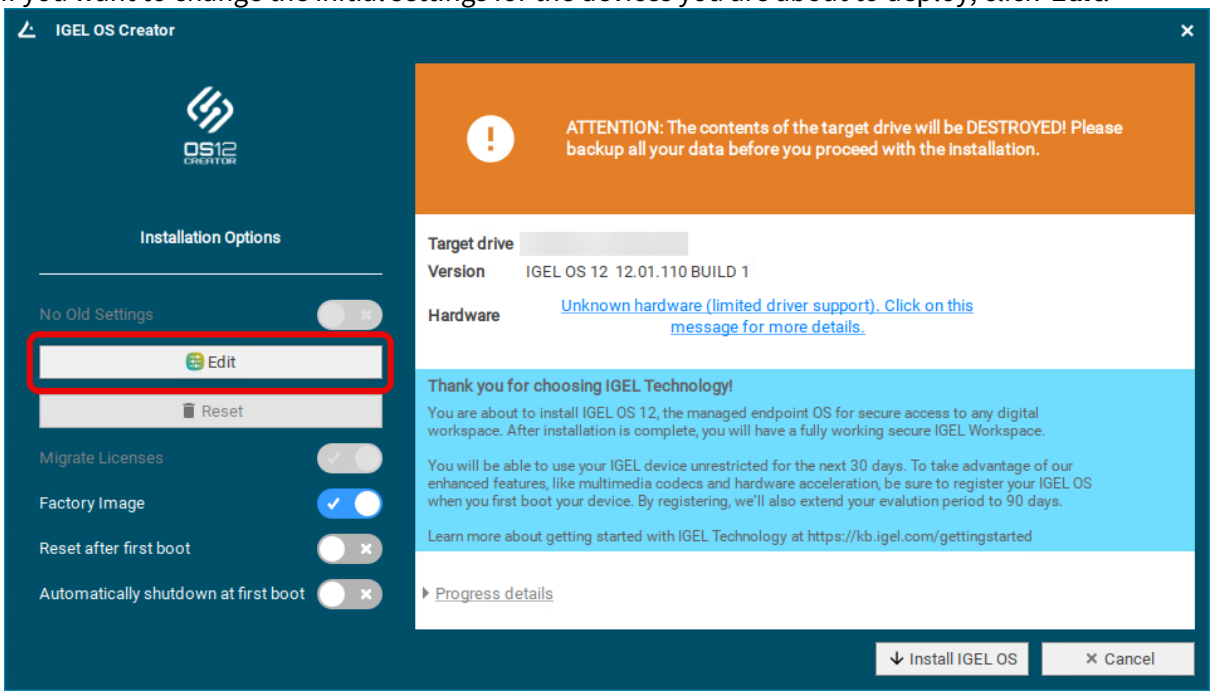




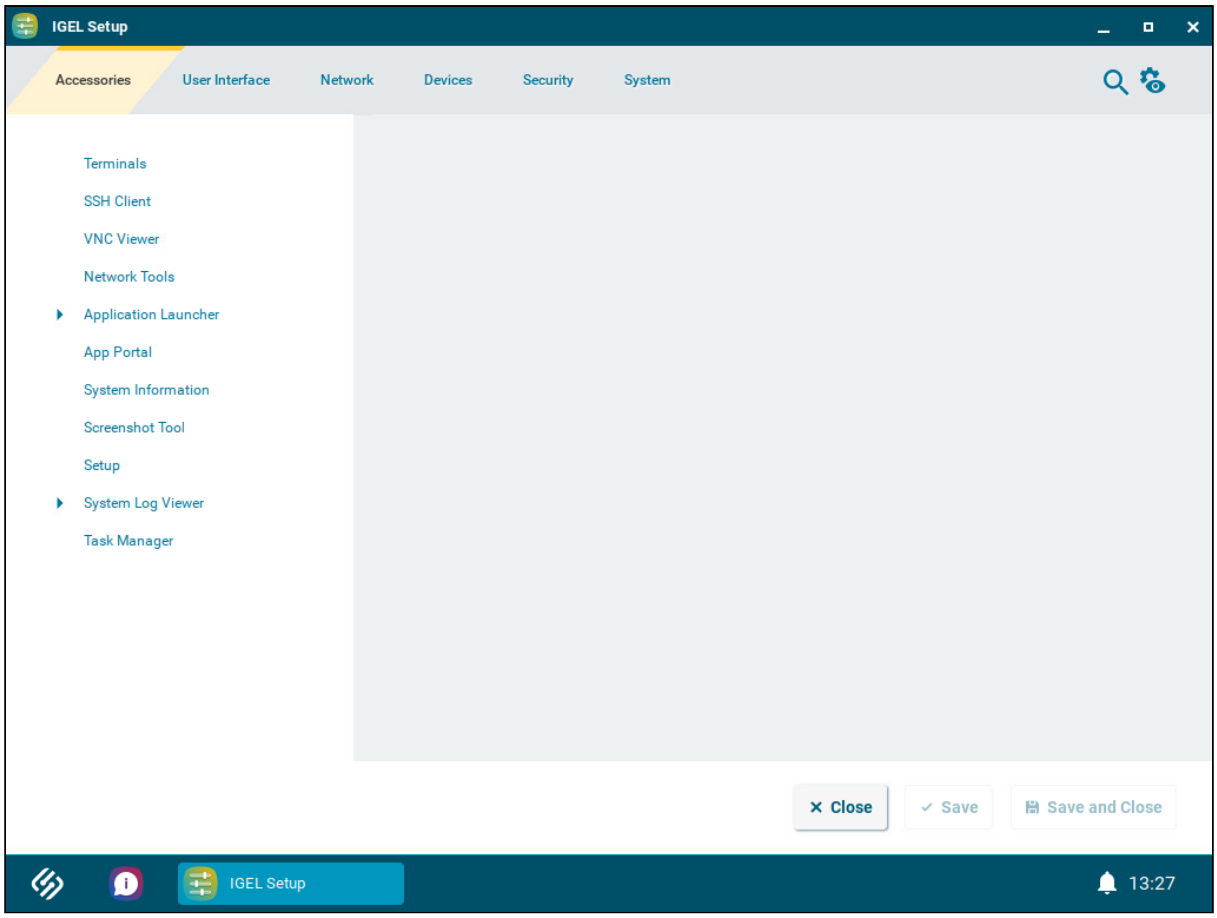
5. Check the **Target drive** to ensure that the system is installed on the desired drive.



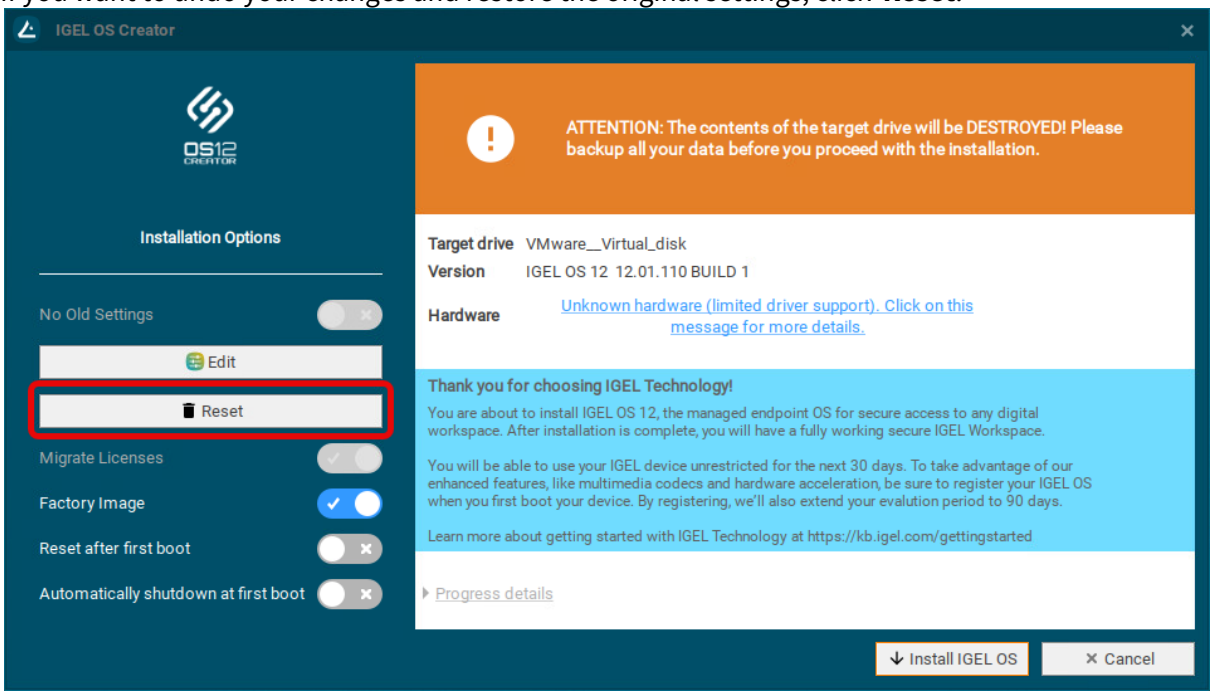
6. If you want to change the initial settings for the devices you are about to deploy, click **Edit**.



The IGEL Setup opens, enabling you to change the settings in the same way as with a regular IGEL OS installation. The changes are stored on the USB memory stick from which the IGEL OS Creator (OSC) is executed. For details about the settings, see Configuration of IGEL OS 12 Device Settings (see page 6).

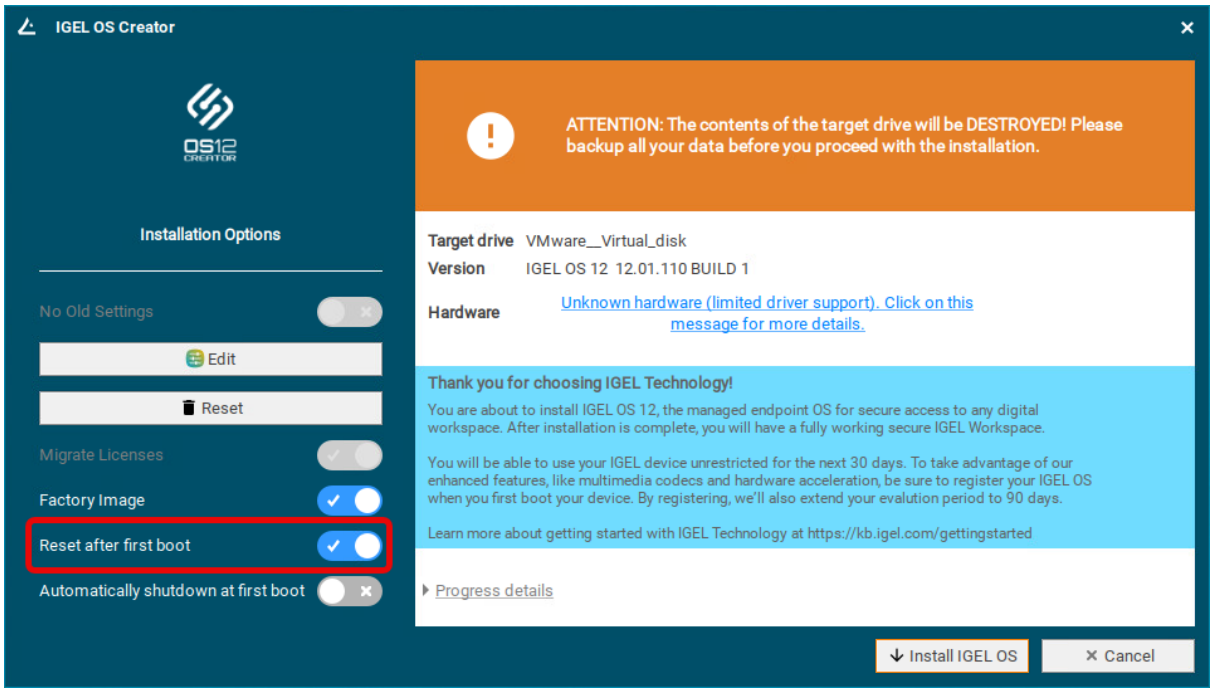

IGEL Setup
Accessories
User Interface
Network
Devices
Security
System
Terminals
SSH Client
VNC Viewer
Network Tools
Application Launcher
App Portal
System Information
Screenshot Tool
Setup
System Log Viewer
Task Manager
Close
Save
Save and Close
IGEL Setup
13:27

7. If you want to undo your changes and restore the original settings, click **Reset**.

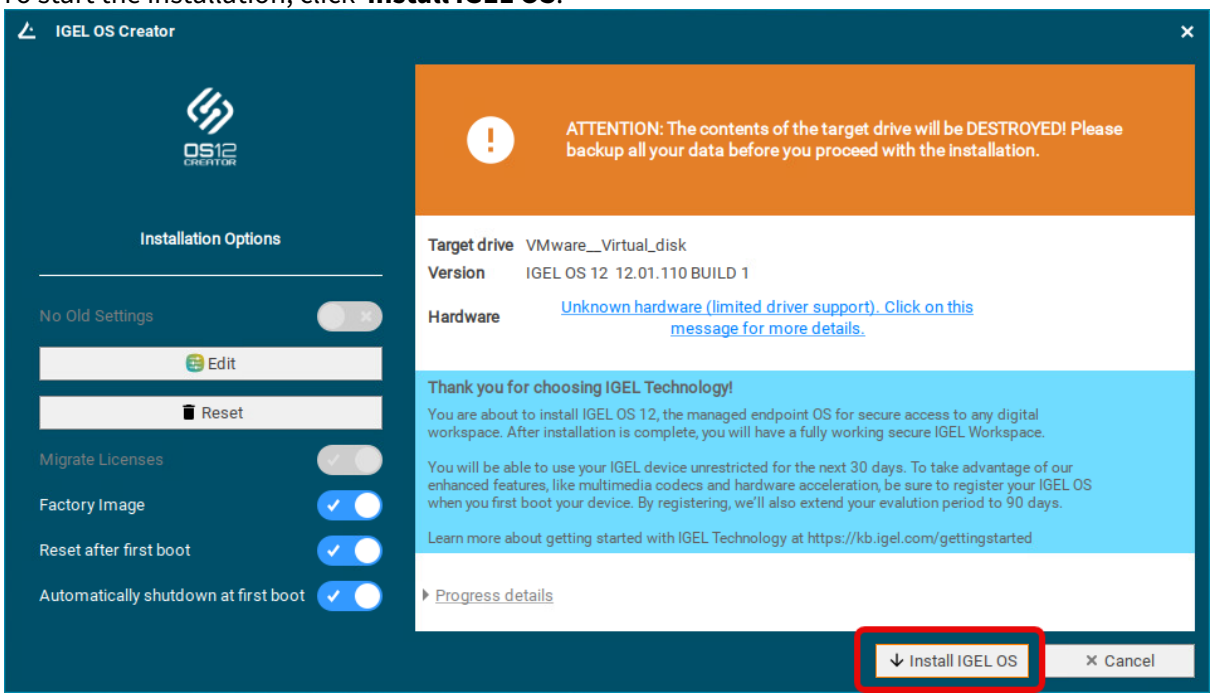


8. If you want to perform a functional test on each device, enable **Reset after first boot**. The test procedure is described under Unit Testing (see page 409).

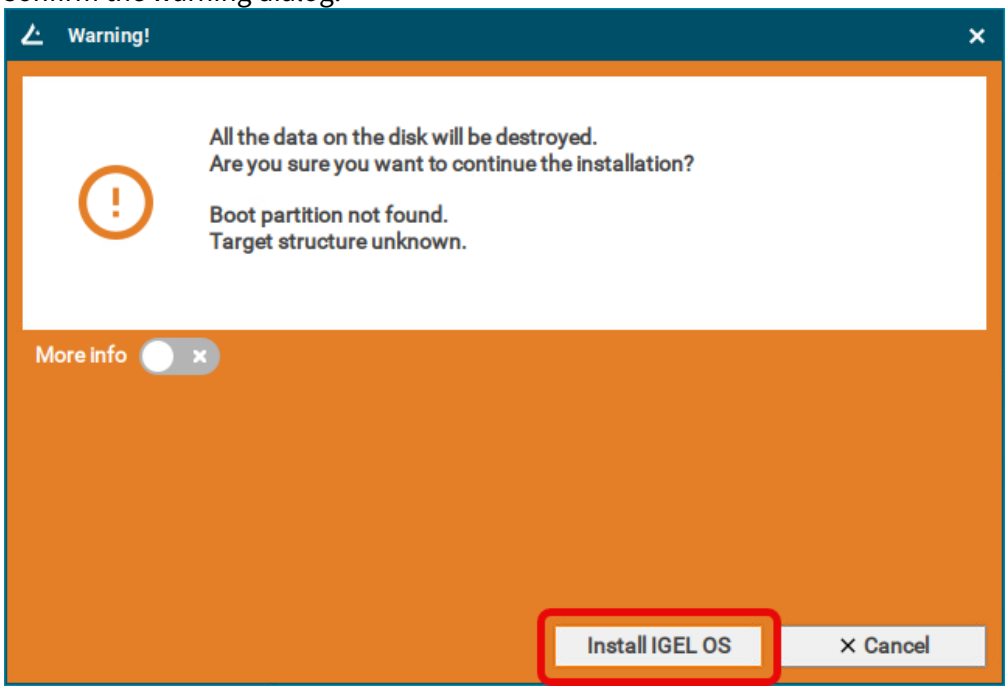
> **Important Note**
>
> If **Reset after first boot** is activated on your factory preload image, the first boot of your devices MUST take place BEFORE shipment to end customers!



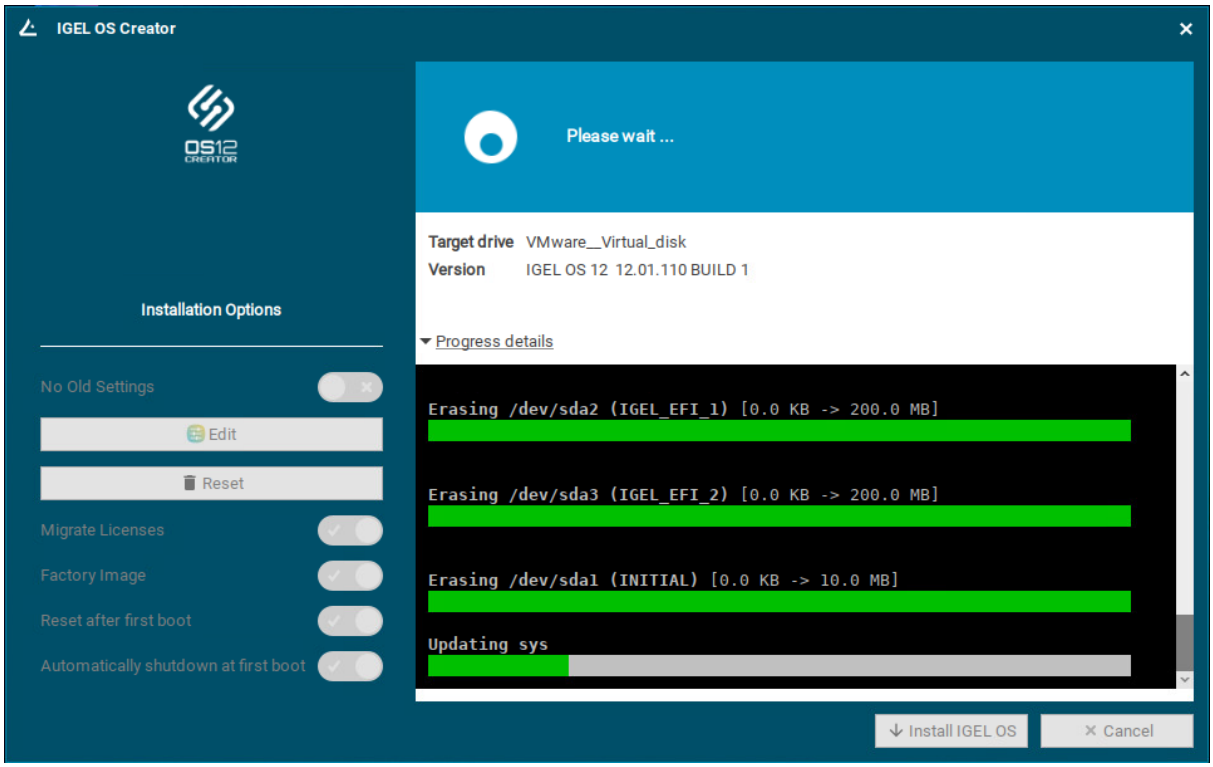
9. To start the installation, click **Install IGEL OS**.



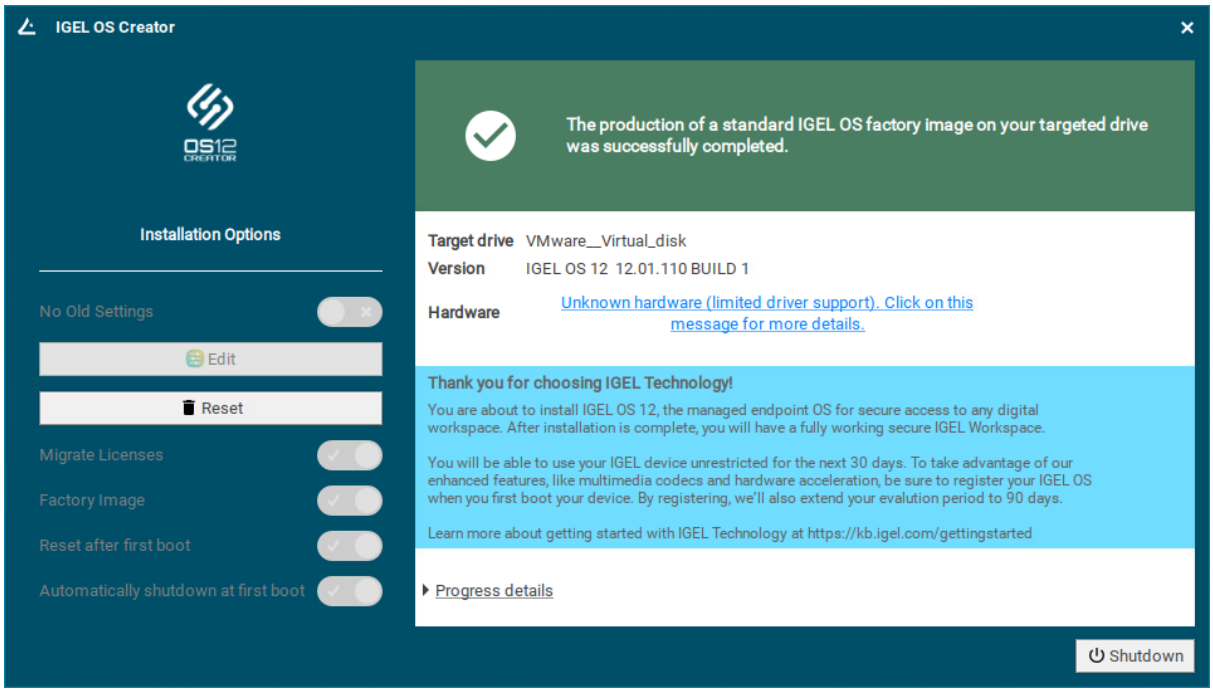
10. Confirm the warning dialog.



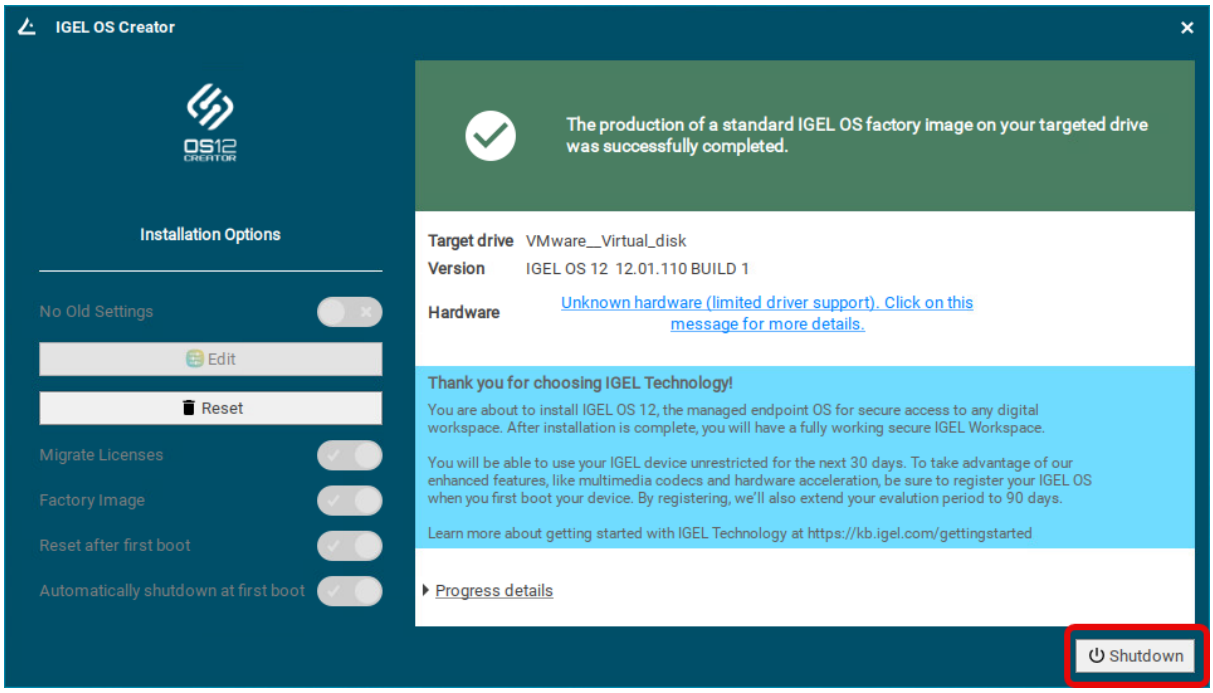
The installation of IGEL OS 12 starts.



The installation program will set up IGEL OS 11 on the target drive. If you see the success message, the installation is complete.



11. Click **Shutdown**.



12. Read out the image from your device to deploy it on the units.

> **DO NOT BOOT THE EXACT FACTORY IMAGE INTENDED FOR DEPLOYMENT ON YOUR DEVICES! ALL DEVICES TO WHICH THIS IMAGE HAS BEEN DEPLOYED WOULD SHARE ONE AND THE SAME UNIT ID. AS A RESULT, YOUR DEVICES WOULD BE PRACTICALLY UNUSABLE.**
> If you want to test the factory image before its deployment, transfer it to your target medium first and then boot the image on the machine on which you created it, or any other test machine. The important thing is that the factory image that will be mass-deployed to your units has not been booted before.

> **64 GiB Maximum Image Size**
>
> The maximum size of the image created by the IGEL OS Creator (OSC) is 64 GiB. Therefore, only the first 64 GiB of your storage medium is needed. If your devices have larger storage, this will allow for faster deployment.

13. To ensure the integrity of the image, you should create checksums of the original image and the deployed images and then compare them. For details, see IGEL Third-party Endpoint Partner: Image Checkums .

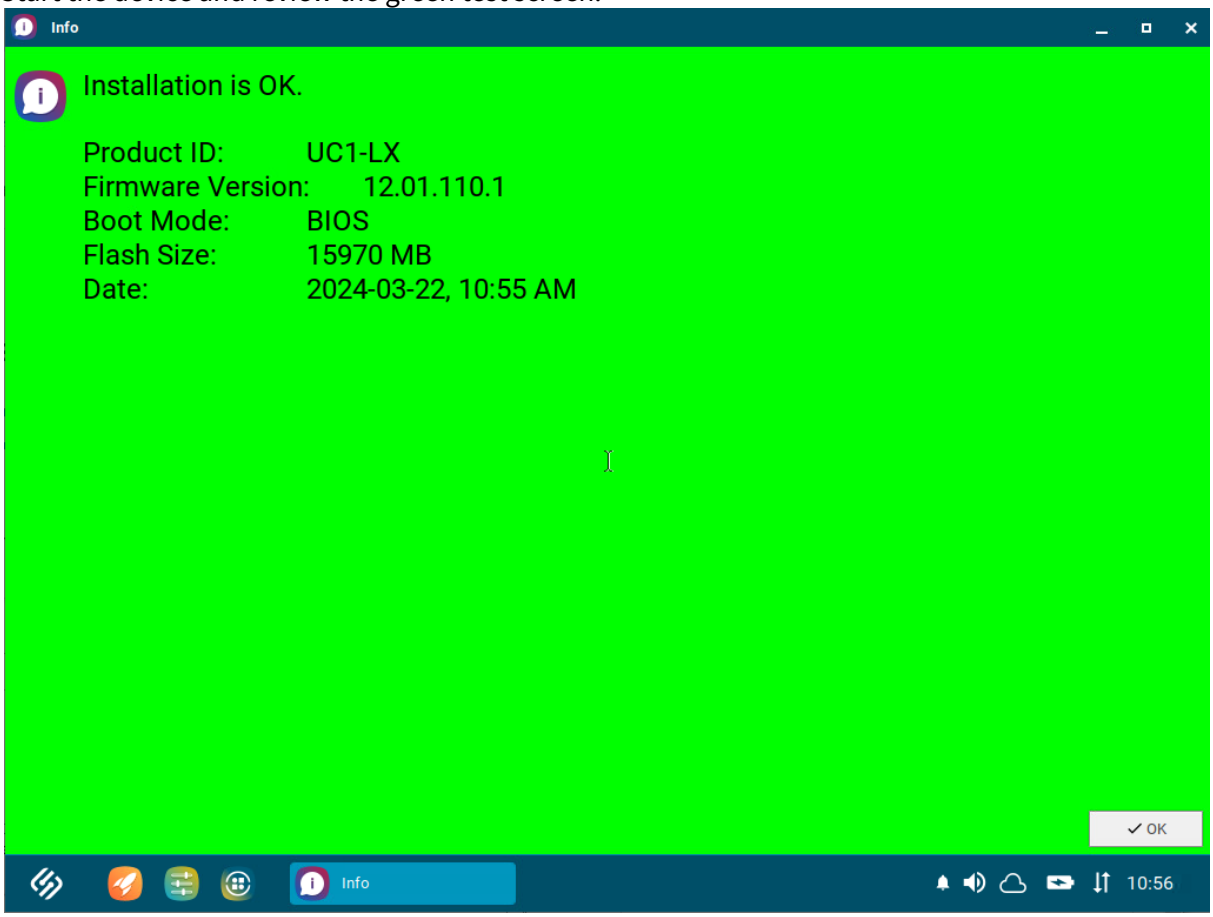
14. Proceed as appropriate:
    - If **Reset after first boot** is inactive, you can deploy the images on the units and roll them out straight away. The deployment should include a comparison of the checksums.
    - If **Reset after first boot** has been activated, deploy the images on the units and continue with Unit Testing (see page 409). (see page 0)

Unit Testing

Perform the following procedure on the original device and every unit on which the image has been deployed.

> **Important Note**
>
> The first boot test MUST take place with each unit BEFORE it is rolled out. (Otherwise, the device would present the green test screen on the first boot instead of the IGEL Setup Assistant.)

1. Start the device and review the green test screen.



2. Click **OK**.
   You can access IGEL OS in a regular way and perform your tests.

3. Shut the device down.
   The device is ready for roll-out.

How to Deploy IGEL OS 12 with PXE

> **Internet Access Required**
>
> In contrast to a typical PXE environment, the installation of IGEL OS 12 requires Internet access because the endpoint devices must be able to reach the IGEL App Portal.

Prerequisites

- Your devices meet the requirements for IGEL OS 12. For further information, see Devices Supported by IGEL OS 12.
- Your devices are able to boot via the network
- Your devices are in a network with Internet access
- A DHCP Server is available in your network

Retrieving the Required Files from the OSC ZIP File

1. Open a web browser, go to https://www.igel.com/software-downloads/cosmos/, and select the folder **OS 12 BASE SYSTEM IMAGE FOR PXE**.

2. Download the ZIP file (e.g. `osc_12.2.1_pxe.zip`) and extract it.
   We will distribute the required files to their appropriate locations later on.

Setting up the DHCP Server

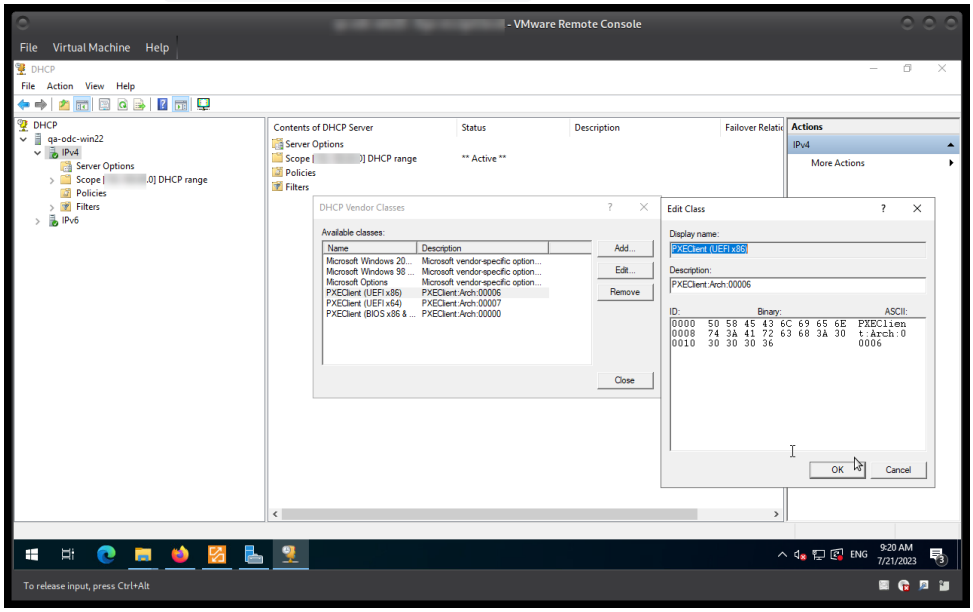
When the devices are powered on, they need to be directed to the TFTP server that provides the low-level files required for booting. This is done by the DHCP server. In our example, we use a Microsoft Windows DHCP server; other DHCP can be used as well.

In the following, we will create three vendor classes, two for UEFI and one for BIOS.

1. On your Windows server, go to **DHCP** and right-click on **IPv4**.

2. Define each vendor class as follows:
   a. In the **DHCP Vendor Classes** dialog, click **Add**.
   b. Enter the data according to the vendor class you are creating:
      i. Vendor class for UEFI on an x86 architecture:
         - **Display name**: `PXEClient (UEFI x86)`
         - **Description**: `PXEClient:Arch:00006`
      ii. Vendor class for UEFI on an x64 architecture:
         - **Display name**: `PXEClient (UEFI x64)`
         - **Description**: `PXEClient:Arch:00007`
      iii. Vendor class for BIOS on x86 and x64 architectures:

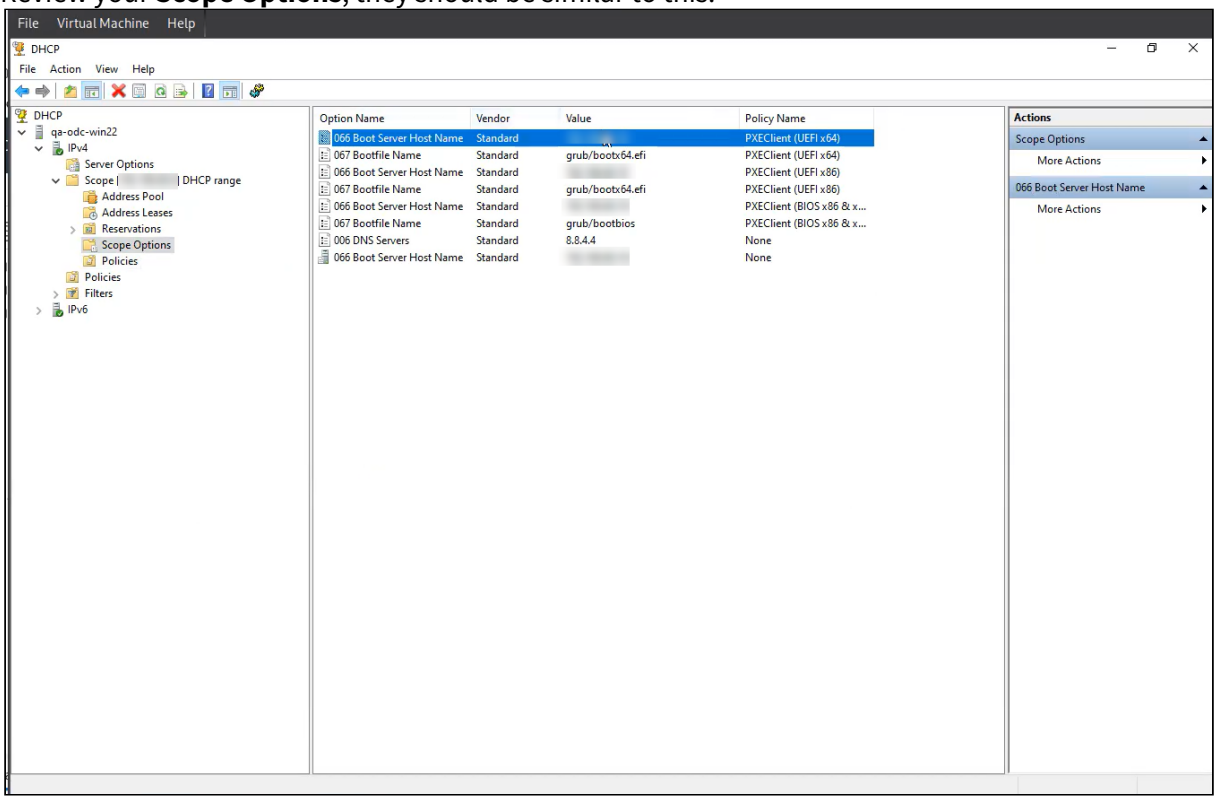
- **Display name**: `PXEClient (BIOS x86 & x64)`
- **Description**: `PXEClient:Arch:00000`



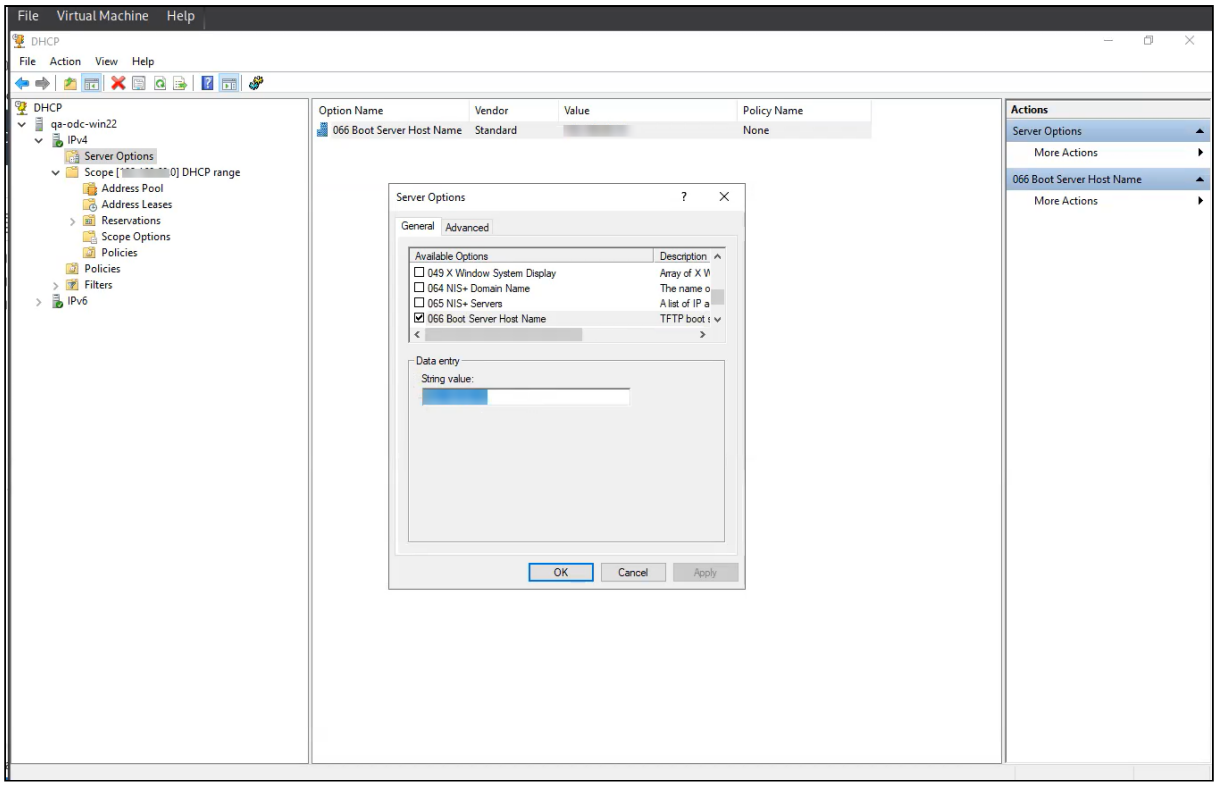
3. Perform the following steps for each vendor class you have created:
   a. Right-click **Scope ([IP address]) DHCP range > Policies** and select **New Policy** from the context menu.
   b. At **Policy Name**, enter the name exactly as you did for the vendor classes, i.e, once `PXEClient (UEFI x86)`, once, `PXEClient (UEFI x64)`, and once `PXEClient (x86 & x64)`.
   c. Click **Next**.
   d. In the **Configure Conditions for the policy** screen, click **Add**.
   e. In the **Add/Edit Condition** dialog, click the drop-down menu **Value:**.
   f. Select the appropriate vendor class.
   g. Activate **Append wildcard**. click **Add** and then **OK**.
   h. Click **Next**,
   i. Answer the question **Do you want to configure an IP address range for the policy?** with **No** and click **Next**.
   j. Activate option **060** and edit it, according to the policy you are at:
      - For `PXEClient (UEFI x86)`, enter `PXEClient`.
      - For `PXEClient (UEFI x64)`, enter `PXEClient`.
      - For `PXEClient (BIOS x86 & x64)`, leave the option empty.
   k. Activate option **066** and enter the Fully Qualified Domain Name (FQDN) or the IP address of your TFTP server.
   l. Activate option **067** and enter the path to the appropriate .efi file on your TFTP server. For example, this might be `grub/bootx64.efi` for the `PXEClient (UEFI x64)`

vendor class if you are using GRUB as the bootloader.

4. Review your **Scope Options**; they should be similar to this:



5. Go to **Server Options**, add option **066**, and enter the Fully Qualified Domain Name (FQDN) or the IP address of your TFTP server.

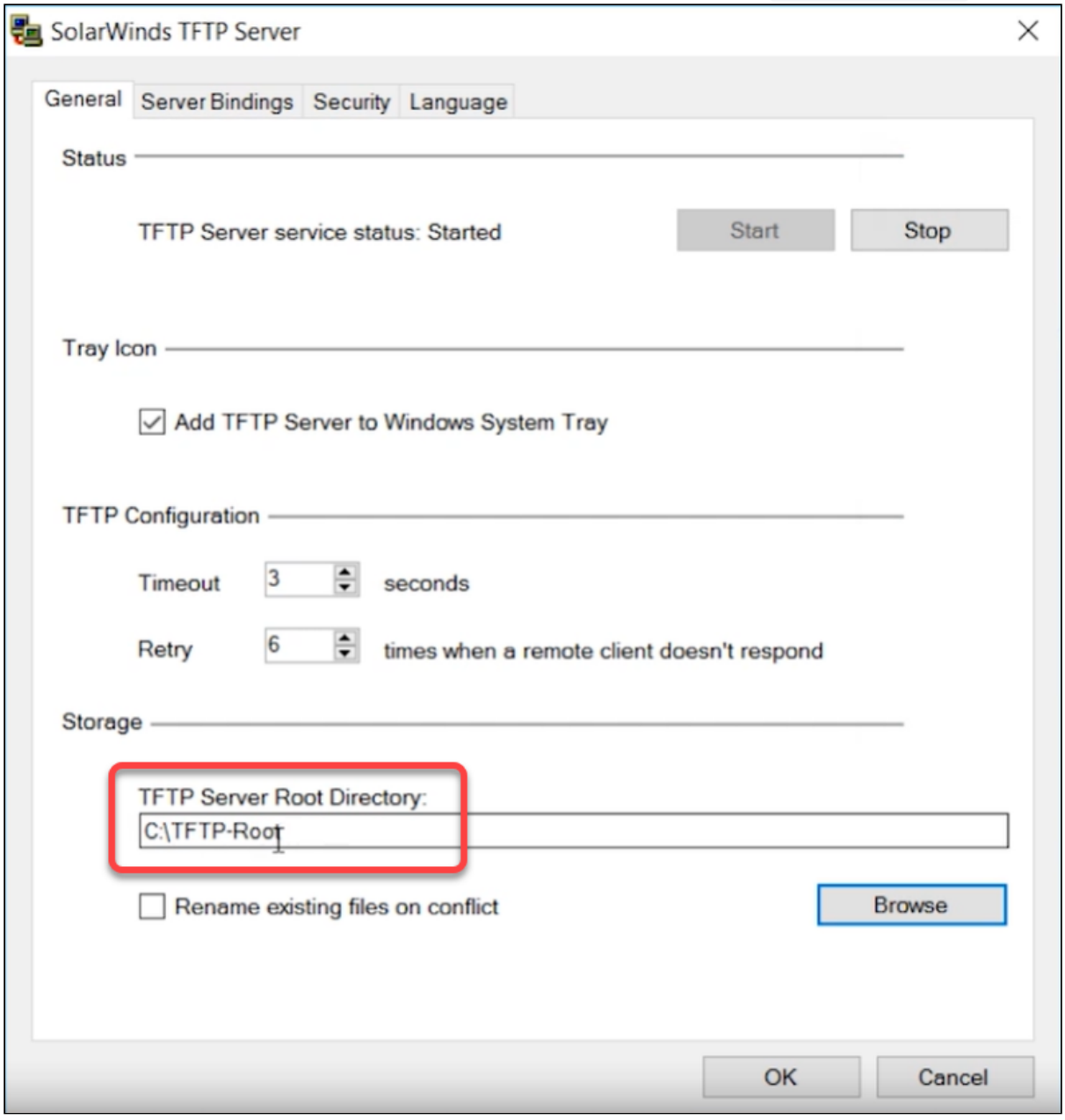


Deploying the TFTP Server

In this step, we deploy that TFTP server that provides the bootloader and a minimal OS that will load the higher-level components of IGEL OS.

1. Install a TFTP server, e.g. SolarWinds. see https://www.solarwinds.com/de/free-tools/free-tftp-server

2. Specify the directory in which the PXE boot files will be stored, typically `C:\TFTP-Root`



3. Copy the directories and files from the `tftp/` directory of your OSC ZIP file to the TFTP root directory, in our example `C:\TFTP-Root`. The directory structure must be preserved.
   The most important contents are:
   - GRUB Bootloader for 64-bit EFI systems
   - GRUB Bootloader for i386/BIOS systems
   - Configuration file for GRUB Bootloader

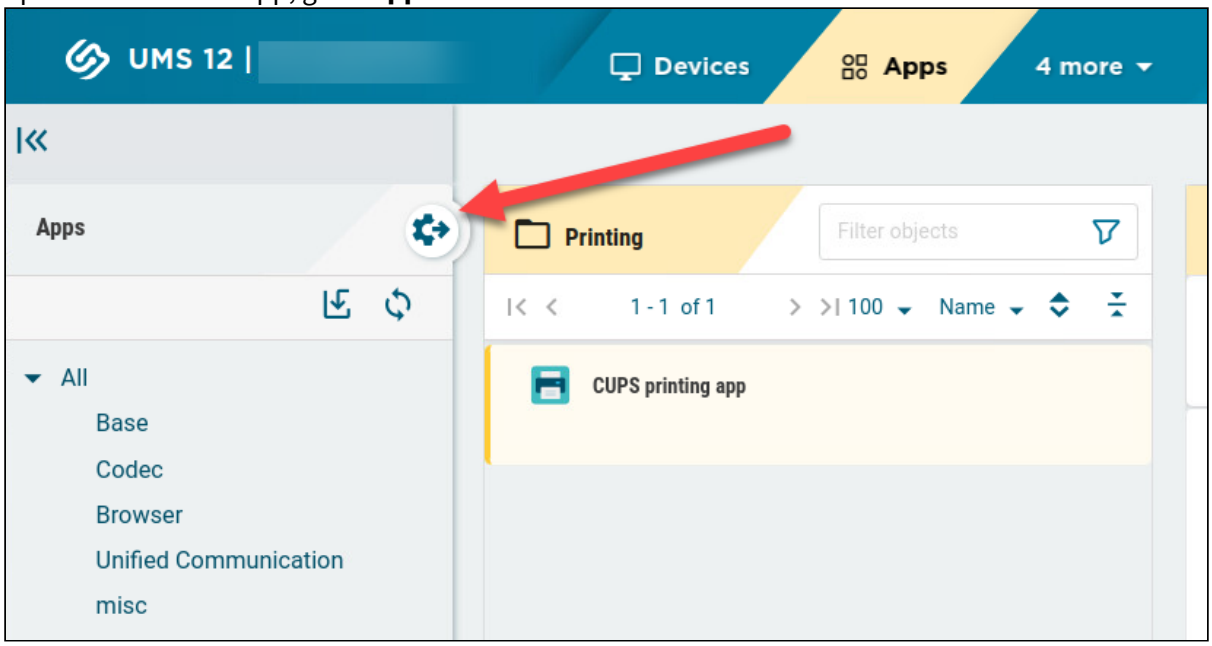
Providing the PXE Configuration File (pxe-config.json)

The file `pxe-config` is used at an early stage of the boot process and will be provided by the TFTP server. It specifies the download paths for specific necessary files, an authentication token for connecting with the IGEL App Portal, and the version of the Base System that is to be installed.

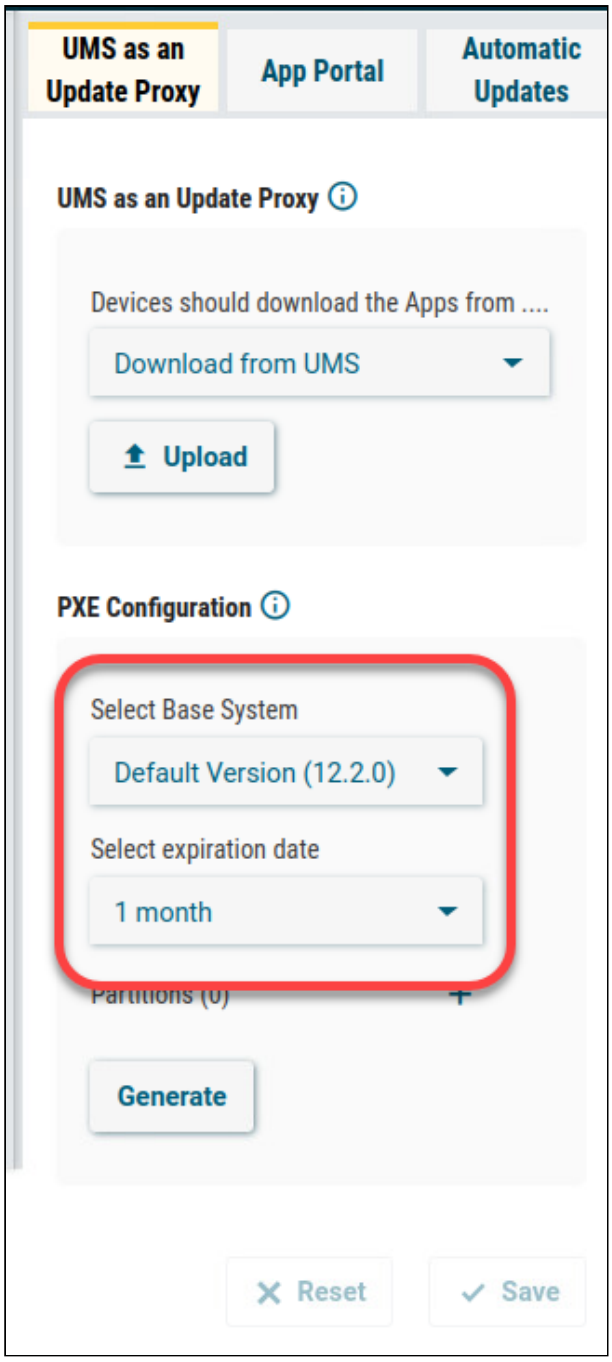
First, we retrieve the file from the UMS, then we edit it to adapt it to our environment. Afterward, we put it into the appropriate directory on the TFTP server.

Retrieving the File from the UMS

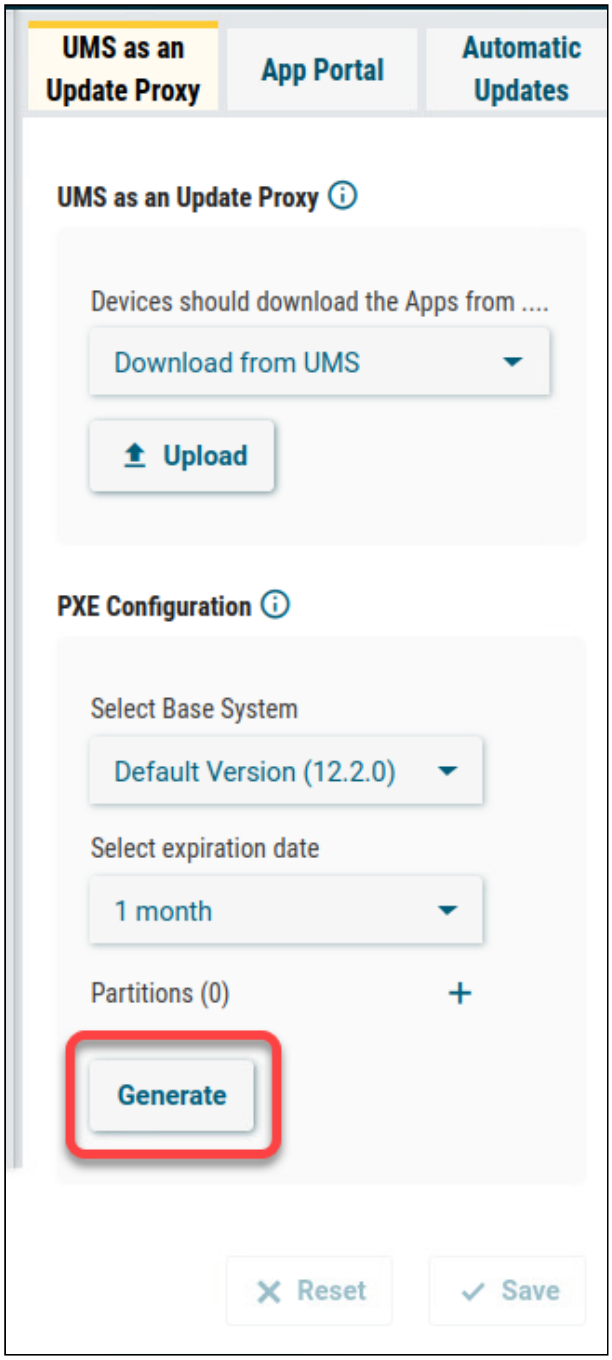
1. Open the UMS Web App, go to **Apps** and click the icon.



2. In the area **PXE Configuration**, select the version of the IGEL OS Base System you want to install and the validity period for the authentication token that enables access to the App Portal.


UMS as an Update Proxy
App Portal
Automatic Updates
UMS as an Update Proxy
Devices should download the Apps from ....
Download from UMS
Upload
PXE Configuration
Select Base System
Default Version (12.2.0)
Select expiration date
1 month
Partitions (0)
Generate
Reset
Save

3. Click **Generate**.



The file `pxe-config.json` is downloaded by your browser.

Editing the "pxe-config.json" FIle

1. In the OSC ZIP file (example: `osc_12.2.1_pxe.zip`), check out the contents of the `webserver/` directory. We will create a reference for each file in step 2.
   Example:
   `osc.bspl`
   `osc.nvgfx`
   `osc.sys`
2. Edit `pxe-config.json` as follows:
   - `"osc"/"partitions"`: Enter a list of the URLs of the files to be downloaded from your web server. The format is `http://<WEB SERVER ADDRESS>/<PATH>/<FILENAME>`
   - `"apps"/"version"`: Ensure that the desired version of IGEL OS is specified.
     Example:

```
{
    "osc": {
        "partitions": [
            "http://igel-pxe-weberver/osc.bspl",
            "http://igel-pxe-weberver/osc.nvgfx",
            "http://igel-pxe-weberver/osc.sys"
        ]
    },
    "appdata": {
        "app_portal": "https://app.igel.com/api/",
        "auth_token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJmaW5nZXJwcmludCI6IjQ2Njc
E4NkMyMTk4Njg3MUIzMEUwMzU3NUQ5Q0NFRTQzNUJGRkU3M0IxQjYxRkMiLCJib2R5Ijp7InVt
c0lkIjoiVU1TL
UNMVVNURVItLTQ0MDMxLTE2ODgxMzQzNTY4NDEtMi0wIn0sInR5cGUiOiJ1bXMiLCJleHAiOjE
3MDA0ODAxMDgs
ImlhdCI6MTY5NzgwMTcwOH0.p-03tX5Zoesud95cpZBJuBCJU77fGzd17J3i1cbCIvhdIAB8D6
CmAdN6kFQ-9Qn
q35SmhyN8f8Jyn63AZEhmiAKPYVGNu1OgVxN-oIU3SBTE74JlU0W26kQuYNEa-WqyAh4BGm-
dJ2qnyqH7_5L08F
DFalJChN8v7DlZ5MVA_G9IWNQ6d87cM13dNFbuH4gK9z6lvKKI2s9Mfr2WQcu5qxBi3HhR-
f3M45zCMyUfm95Tu
eON48tAyfLPbxlqBUjm2FREJN89dqoZpo-obfcLQ85od6bFyotnK-MDm27-
BQvSlOpRujki2wMMYHz1vBeEJJfN
l78aGha5wRDpvrffrOgd_vY4Taicd8hwETcAmI9ihksOHO4gj6GIYZ1dBTbSGBMdooBkB4T5nK
trSX3IOkKCm79-
x_c9gfRNKS-5ox8fvYPIVTK42gHBkQvpgJ5c0G2PqpFCiA8wSBU1bx6bgJdNpQQA1WhadKjOjM
ICp49pf5PPrfA
```

```
zvDzRpXxzQ43HpA86r2Jd59KSOi7QuW7Jb0D2WvjaoCSUFvXhaB-
UTsey61DKJJH73xqXbOoA5bdon123m8eTVK
wUJRTL6By41wG6nHnQ0dCYg8noucCg_rOCPBxVfvAhgxzwxllWNgQbGBWtG9Iw1qZIpEuvJa3u
x3YxJE5flMsXm
qDtpsyRURBQ0E2RTc3Qzg4RDI5Mjfzzhbs",
        "apps": [
            {
                "name": "base_system",
                "version": "12.2.1"
            }
        ]
    }
}
```


Proving the PXE Configuration File (pxe-config.json) via the TFTP Server

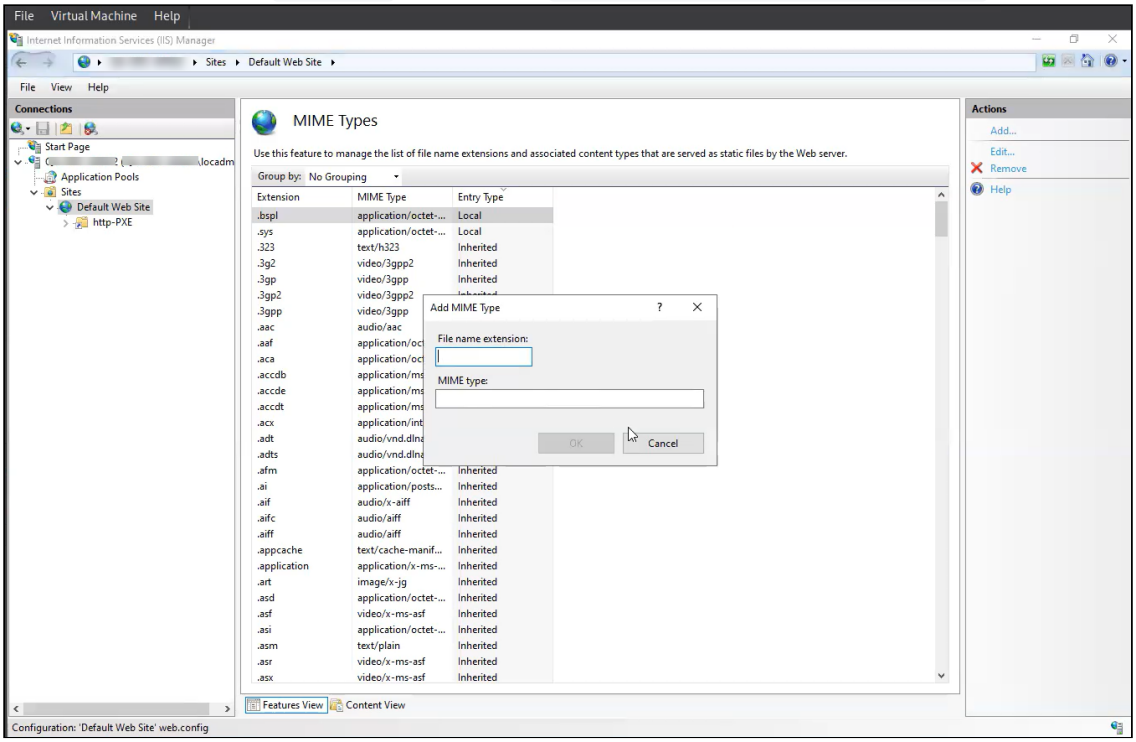
▶ Copy `pxe-config.json` to `<TFTP ROOT>/images/`. Example file path: `C:\TFTP-Root\images\pxe-config.json`

Configuring the Web Server (IIS)

For installing the components of IGEL OS 12, we need a web server. In our example, we will use the Microsoft Internet Information Server (IIS).

1. If IIS is not already available on your Windows server, install it.
2. Add the file name extensions and the corresponding MIME types for all file types that are present in the `webserver/` directory of the OSC ZIP file. In our example:
   - **File name extension** `.bspl` ; **MIME type** `application/octet stream`
   - **File name extension**: `.sys` ; **MIME type** `application/octet stream`

- **File name extension**: `.nvgfx` ; **MIME type** `application/octet stream`



3. Specify a directory in which the required files will be stored, in our example `C:\HTTP-Root`

4. Copy all files from the `webserver/` directory of the OSC ZIP file into the directory on the web server that has been defined in the section `"osc"/"partitions"` of your `pxe-config.json` (see Editing the "pxe-config.json" File (see page 419)). In our example, the directory is `C:\HTTP-Root` and the files are `osc.bspl` , `osc.nvgfx` , and `osc.sys` . The files may vary depending on the version of your OSC ZIP file.

> **Web Server Check**
>
> We recommend checking the URLs for these files in a web browser to ensure the download is functional.

Installing IGEL OS via PXE

▶ Start the devices in your PXE environment.

If everything has been set up correctly, your devices boot into IGEL OS 12.

How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on

IGEL OS 12 SCCM Add-on facilitates deploying IGEL OS via Microsoft SCCM. The package contains IGEL OS Base System as a dd image that will be booted using a Windows PE boot file customized for this purpose.

Optionally, you can use a different version of IGEL OS Base System, add certificates and license files, and compress the image file; for details, see Alternative Deployment (see page 438). Moreover, you can choose whether you want to deploy the IGEL OS dd image together with the Windows PE boot image as one single file or separately via a network share.

With the installation of IGEL OS SCCM Add-on, a customized Windows PE image and a task sequence for deploying IGEL OS are created, and the IGEL OS Image Manager is installed.

This article is based on version 2.2.0 of IGEL OS 12 SCCM Add-on; the supplied version of IGEL OS Base System is 12.3.1. For details on this version, see the Readme_2.2.0.txt.

Prerequisites

- Microsoft Endpoint Configuration Manager (see https://docs.microsoft.com/en-us/mem/configmgr/)

  > The solution presented here has been developed and tested with the current version of Microsoft Endpoint Configuration Manager (status 01/2024). For details on the versioning of Microsoft Endpoint Configuration Manager, see https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/changes/whats-new-incremental-versions.

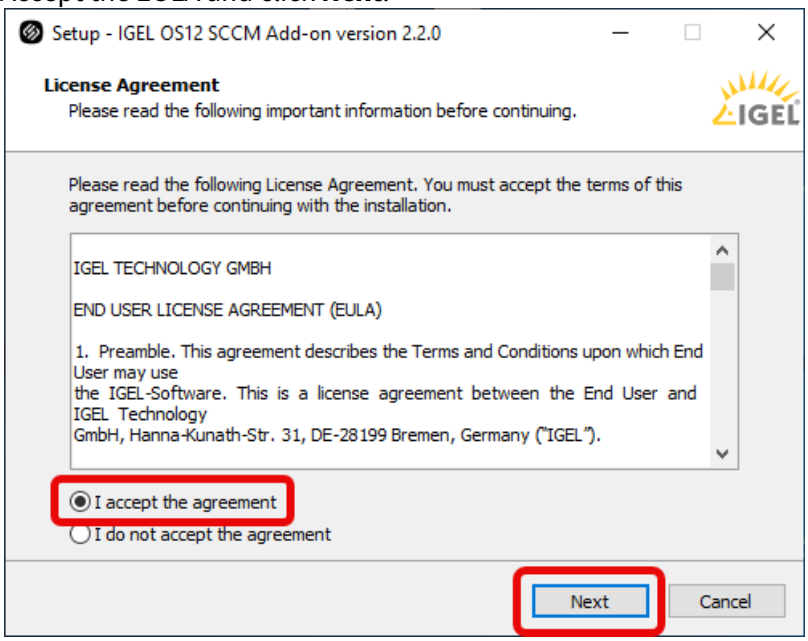
- Configured PXE environment for OS deployment; all target devices must be in a network where they are available either from the main site server or a distribution point. (For further information, see https://docs.microsoft.com/en-us/mem/configmgr/osd/plan-design/infrastructure-requirements-for-operating-system-deployment)
- All target devices have a minimum of 4 GB RAM.
- On the host on which Microsoft Endpoint Configuration Manager is running, Microsoft Power Shell Script execution must be allowed, at least for signed scripts (the Powershell scripts that come with IGEL OS SCCM Add-on are signed by IGEL).

Installing IGEL OS SCCM Add-On

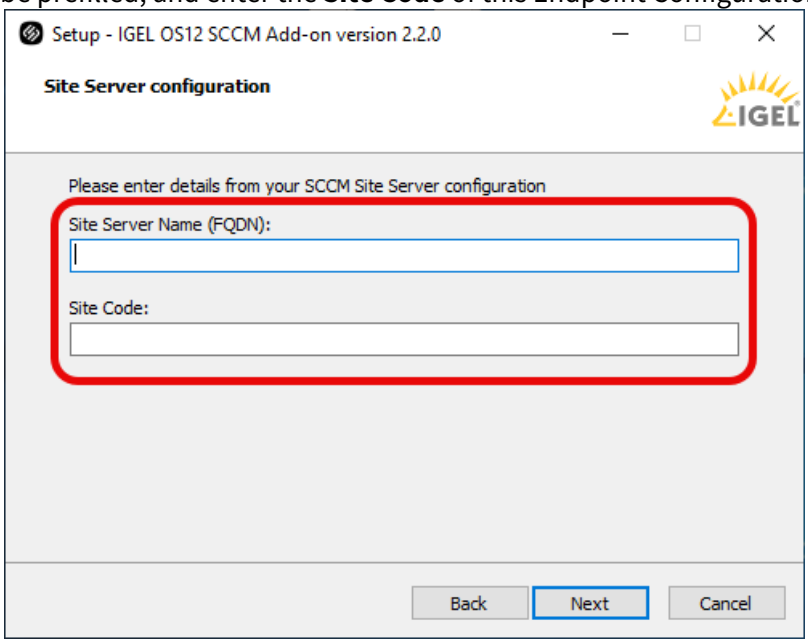
1. Go to https://www.igel.com/software-downloads/cosmos/ **> OS 12 Base System Deployment Tool for SCCM** and download the executable file to the host on which Microsoft Endpoint Configuration Manager is running.

2. Start the executable file.

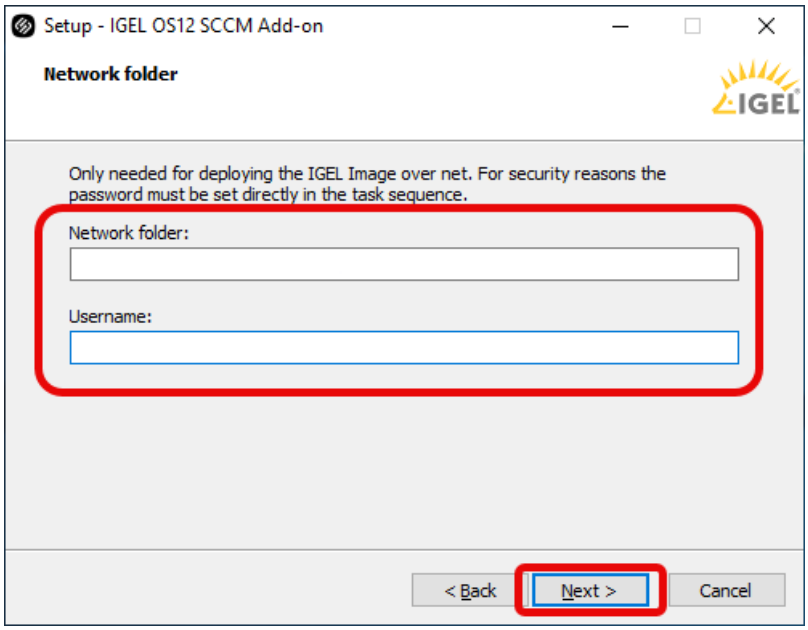
3. Accept the EULA and click **Next**.



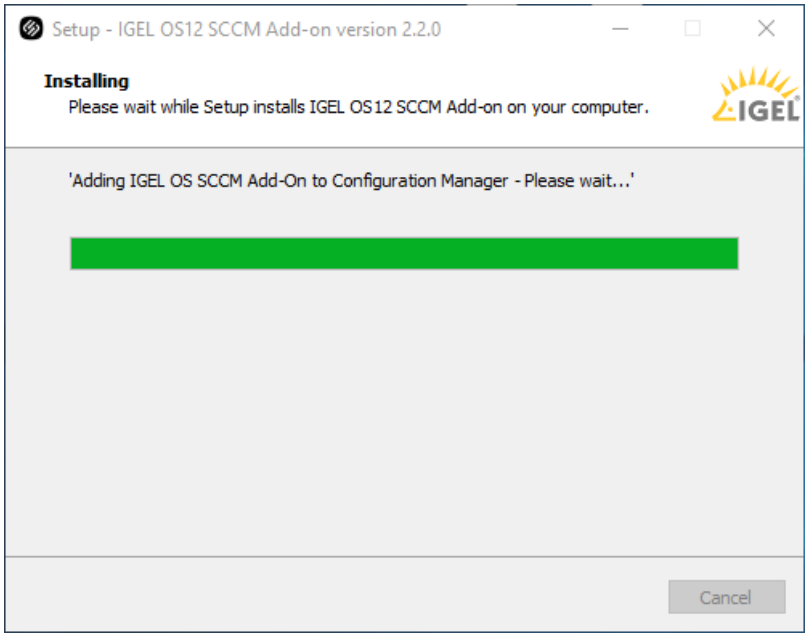
4. On the **Site Server configuration** page, review the field **Site Server Name (FQDN)**, which should be prefilled, and enter the **Site Code** of this Endpoint Configuration Manager site. Then, click **Next**.



5. If you plan to deploy the IGEL OS image separately via a network share, i.e., not embedded in the boot file, enter the shared **Network folder** containing the IGEL OS image and the corresponding **Username**. Then, click **Next**.

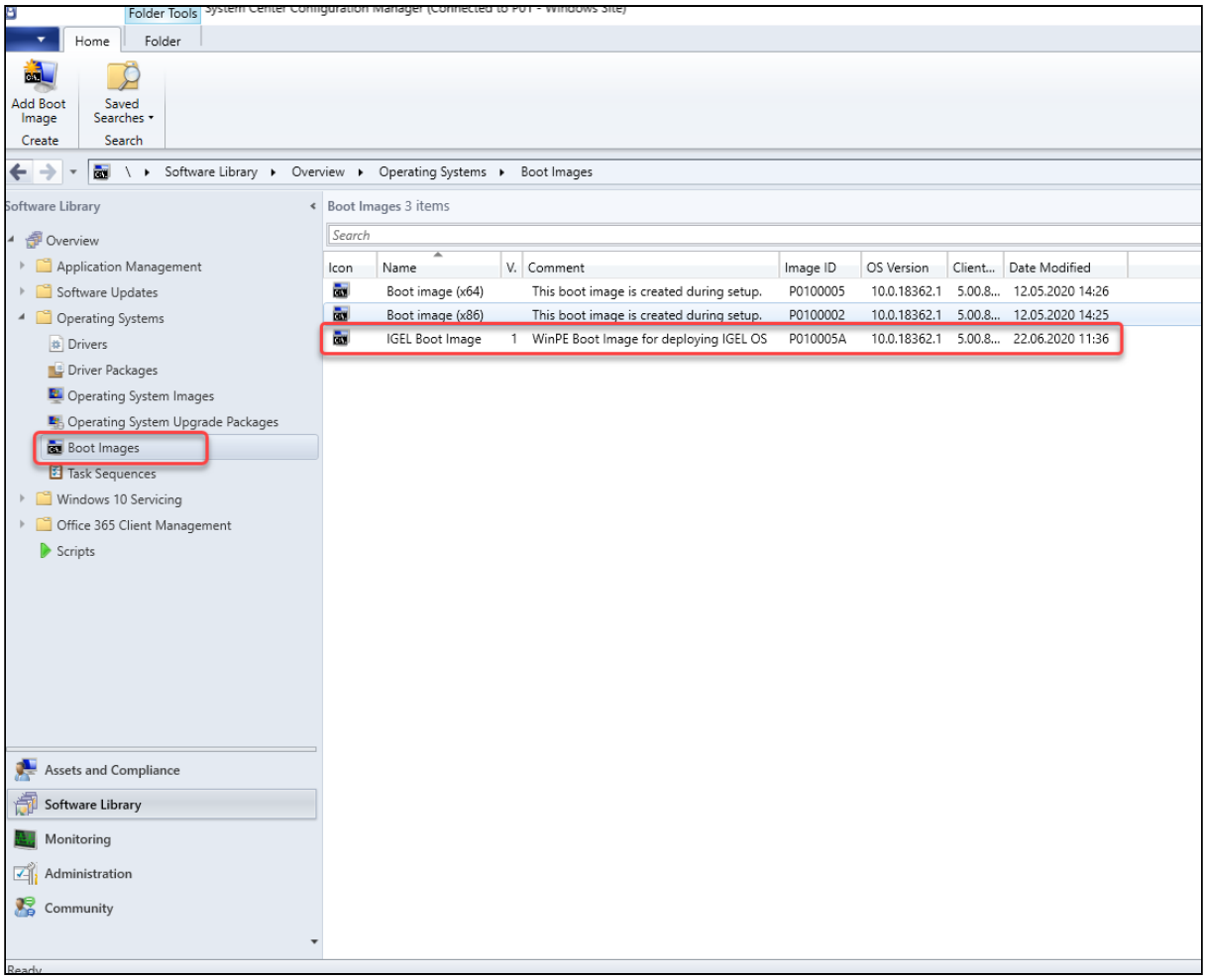


The installation of IGEL OS SCCM Add-on starts.

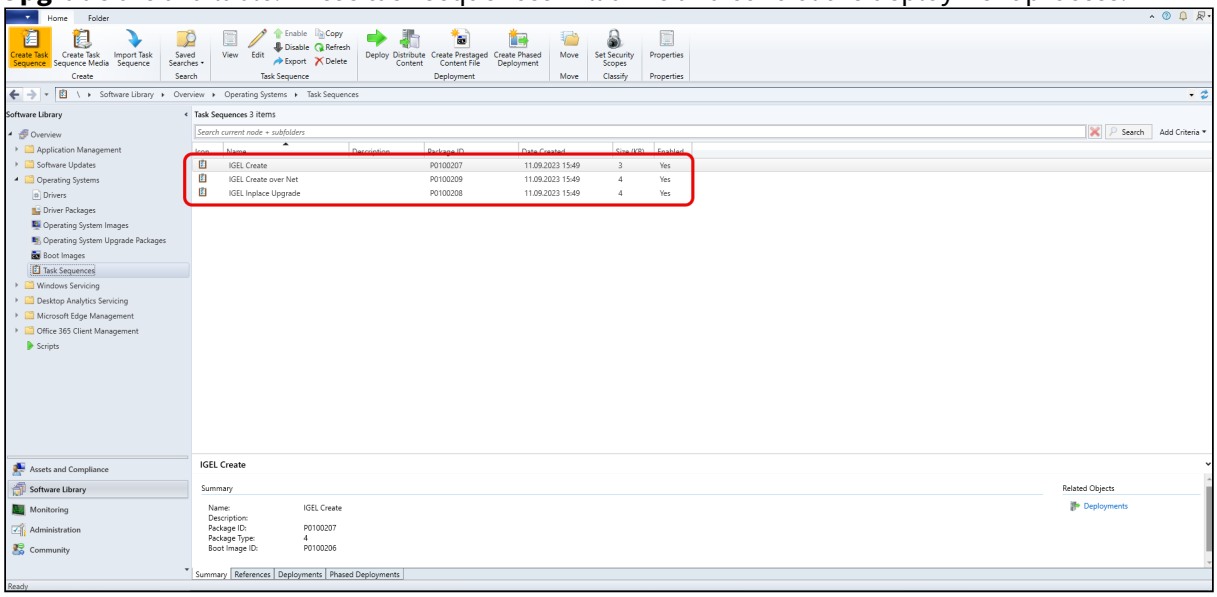


Verifying the Installation

1. Under Software Library, select **Operating Systems > Boot Images** and check if the **IGEL Boot Image** (WIM) is available.


Folder Tools
Home
Folder
Add Boot Image
Create
Saved Searches
Search
Software Library
Overview
Operating Systems
Boot Images
Boot Images 3 items
Search
Icon
Name
V.
Comment
Image ID
OS Version
Client...
Date Modified
Boot image (x64)
This boot image is created during setup.
P0100005
10.0.18362.1
5.00.8...
12.05.2020 14:26
Boot image (x86)
This boot image is created during setup.
P0100002
10.0.18362.1
5.00.8...
12.05.2020 14:25
IGEL Boot Image
1
WinPE Boot Image for deploying IGEL OS
P010005A
10.0.18362.1
5.00.8...
22.06.2020 11:36
Application Management
Software Updates
Drivers
Driver Packages
Operating System Images
Operating System Upgrade Packages
Task Sequences
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Monitoring
Administration
Community
Ready

2. Go to **Task Sequences** and check if **IGEL Create** , **IGEL Create over Net**, and **IGEL Inplace Upgrade** are available. These task sequences will drive and control the deployment process.



Provisioning IGEL OS via a PXE Boot Environment

The task sequences provided by IGEL OS SCCM Add-on will deploy IGEL OS to a device collection via a PXE boot environment. The task sequence will be executed after the device has booted into the IGEL Boot Image (`igel.wim`).

You can choose between the following task sequences:

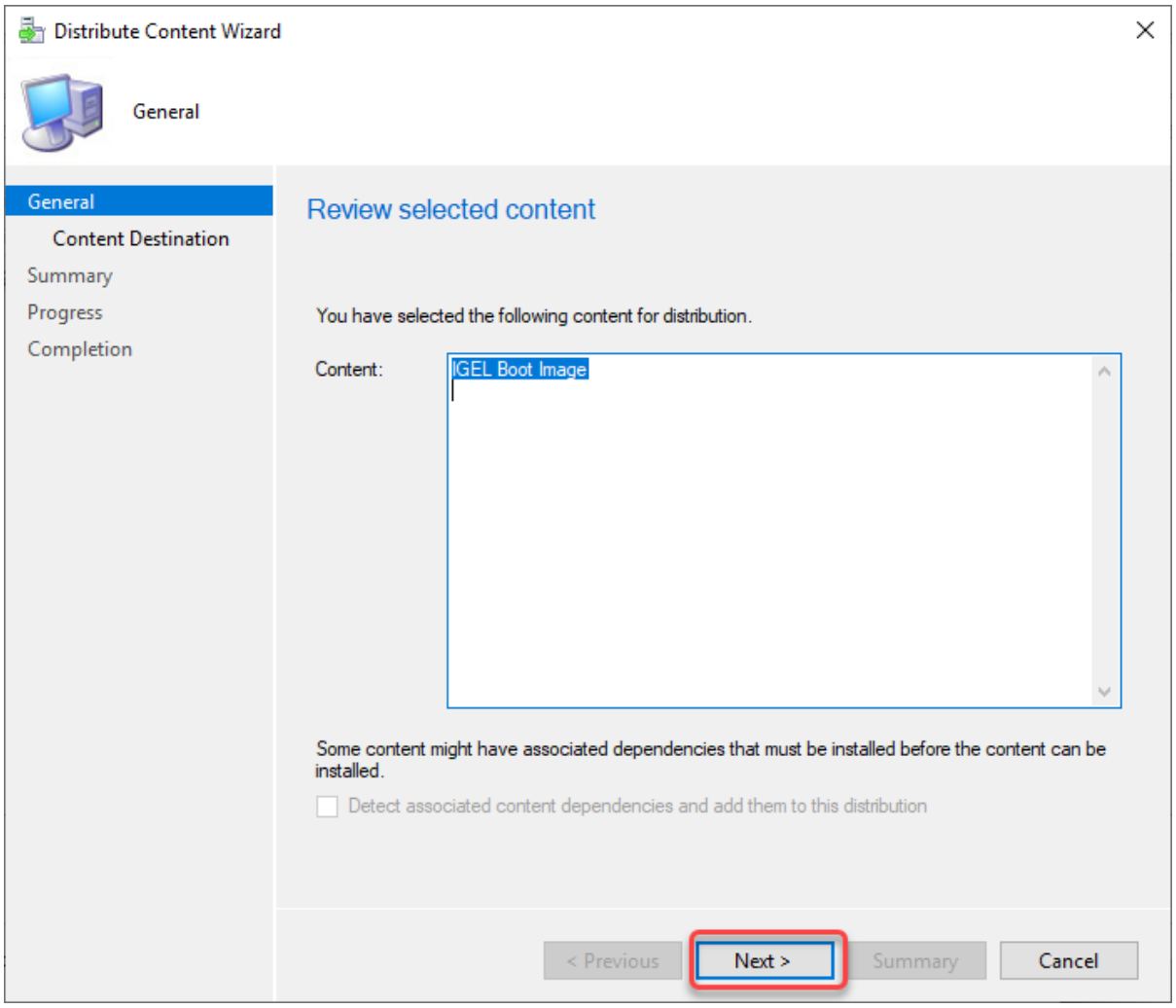
- **IGEL Create**: The IGEL OS image (`minimal.bin`) is built into the IGEL Boot Image (`igel.wim`)
- **IGEL Create over Net**: IGEL OS image (`minimal.bin`) is provided separately via a network share

To deploy the PXE boot environment:

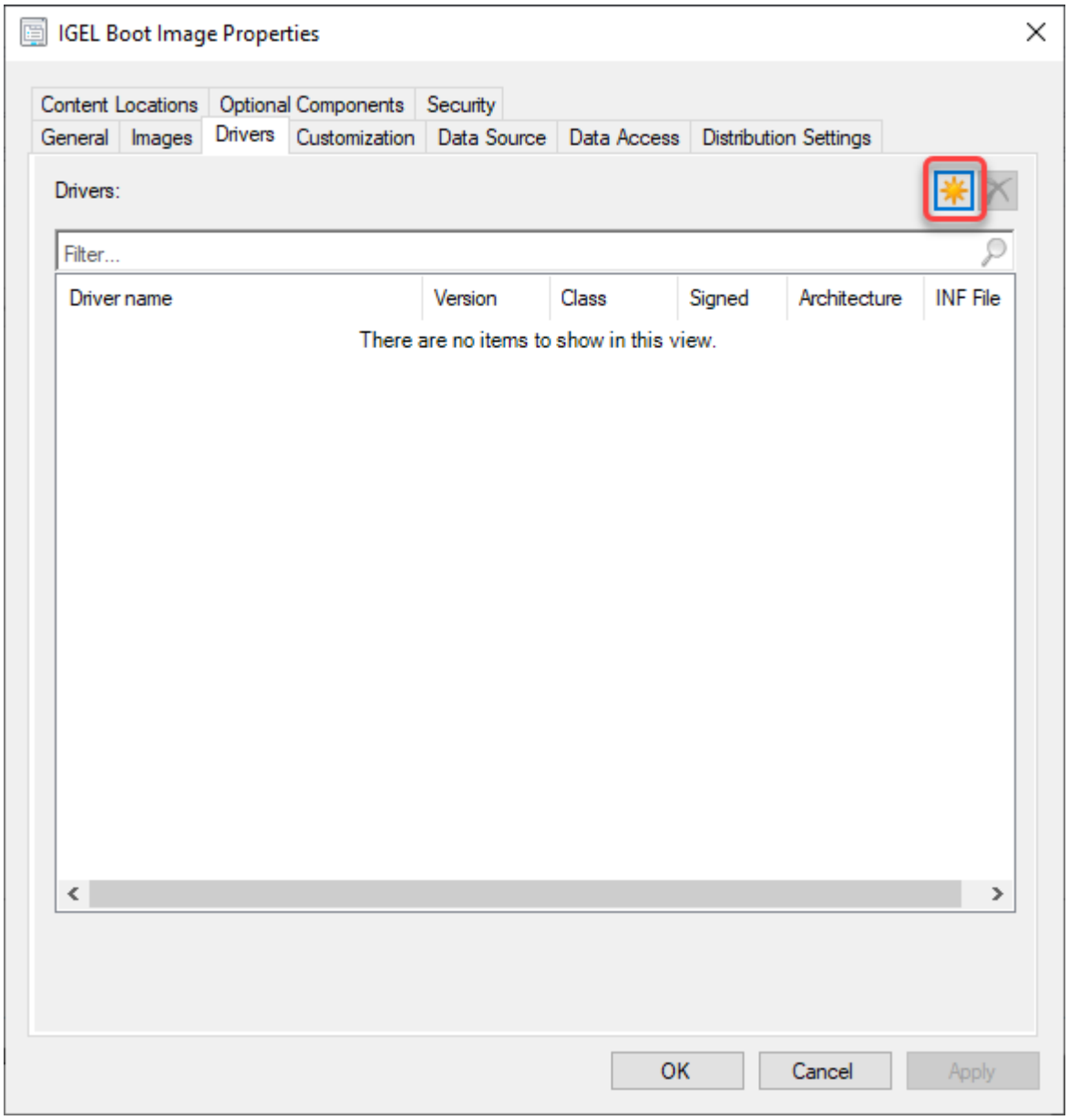
1. Check if you need to define your own custom device collection to allocate your target devices or if you can use one of the preconfigured collections.

2. Under **Software Library**, select **Operating Systems > Boot Images**. Open the context menu for **IGEL Boot Image** and select **Distribute content**.

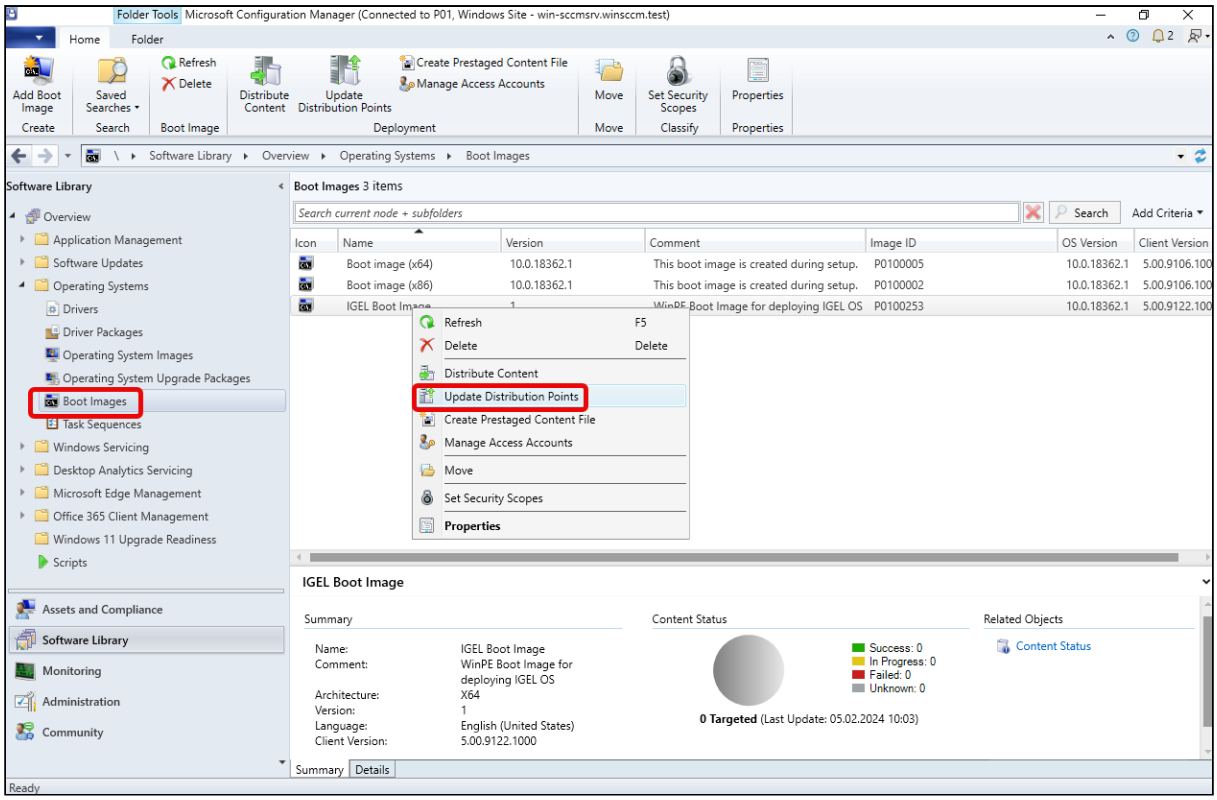
3. Open the **Distribute Content Wizard** and check if **IGEL Boot Image** is shown in the **Content** area. Afterward, continue with the wizard.

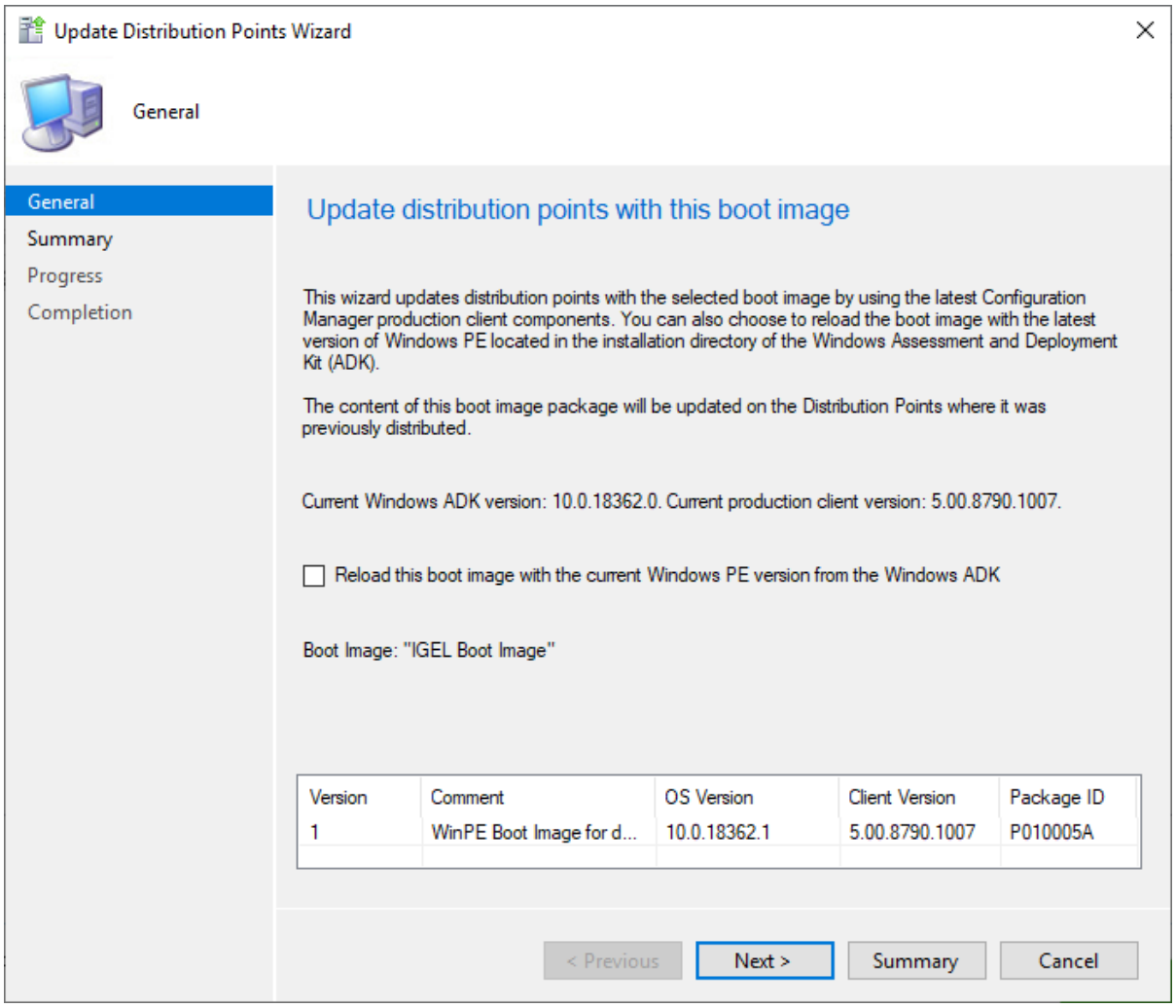


4. If your device requires a specific network driver: Select **Operating Systems > Boot Images**, Open the context menu for **IGEL Boot Image**, and select **Properties**. Then, select the **Drivers** tab and add the driver.

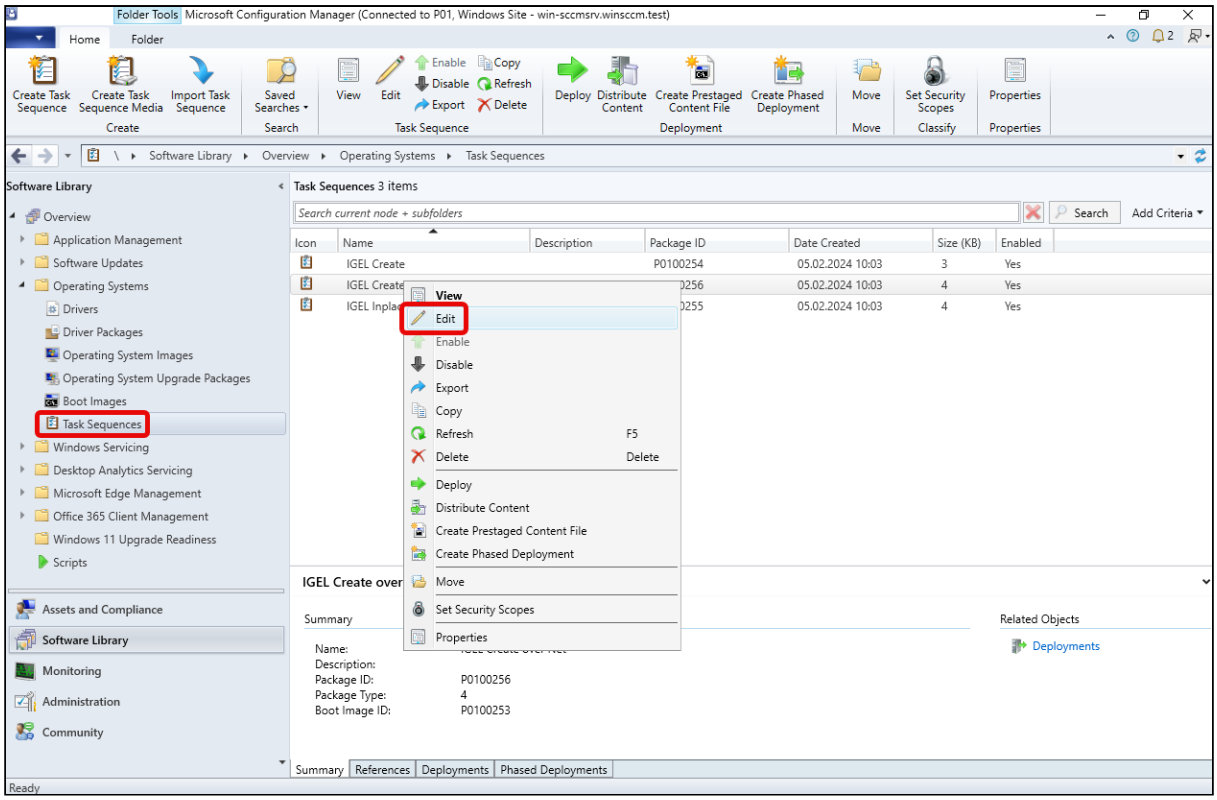


5. Select **Operating Systems > Boot Images**, Open the context menu for **IGEL Boot Image** and select **Update distribution points**.


Folder Tools Microsoft Configuration Manager (Connected to P01, Windows Site - win-sccmsrv.winsccm.test)
Home
Folder
Add Boot Image
Saved Searches
Refresh
Delete
Distribute Content
Update Distribution Points
Create Prestaged Content File
Manage Access Accounts
Move
Set Security Scopes
Properties
Create
Search
Boot Image
Deployment
Move
Classify
Properties
Software Library
Overview
Application Management
Software Updates
Operating Systems
Drivers
Driver Packages
Operating System Images
Operating System Upgrade Packages
Boot Images
Task Sequences
Windows Servicing
Desktop Analytics Servicing
Microsoft Edge Management
Office 365 Client Management
Windows 11 Upgrade Readiness
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
Community
Boot Images 3 items
Search current node + subfolders
Search
Add Criteria
Icon
Name
Version
Comment
Image ID
OS Version
Client Version
Boot image (x64)
10.0.18362.1
This boot image is created during setup.
P0100005
10.0.18362.1
Boot image (x86)
10.0.18362.1
This boot image is created during setup.
P0100002
10.0.18362.1
IGEL Boot Image
WinPE Boot Image for deploying IGEL OS
P0100253
10.0.18362.1
Refresh F5
Delete Delete
Distribute Content
Update Distribution Points
Create Prestaged Content File
Manage Access Accounts
Move
Set Security Scopes
Properties
IGEL Boot Image
Summary
Name: IGEL Boot Image
Comment: WinPE Boot Image for deploying IGEL OS
Architecture: X64
Version: 1
Language: English (United States)
Client Version: 5.00.9122.1000
Content Status
Success: 0
In Progress: 0
Failed: 0
Unknown: 0
0 Targeted (Last Update: 05.02.2024 10:03)
Related Objects
Content Status
Summary
Details
Ready

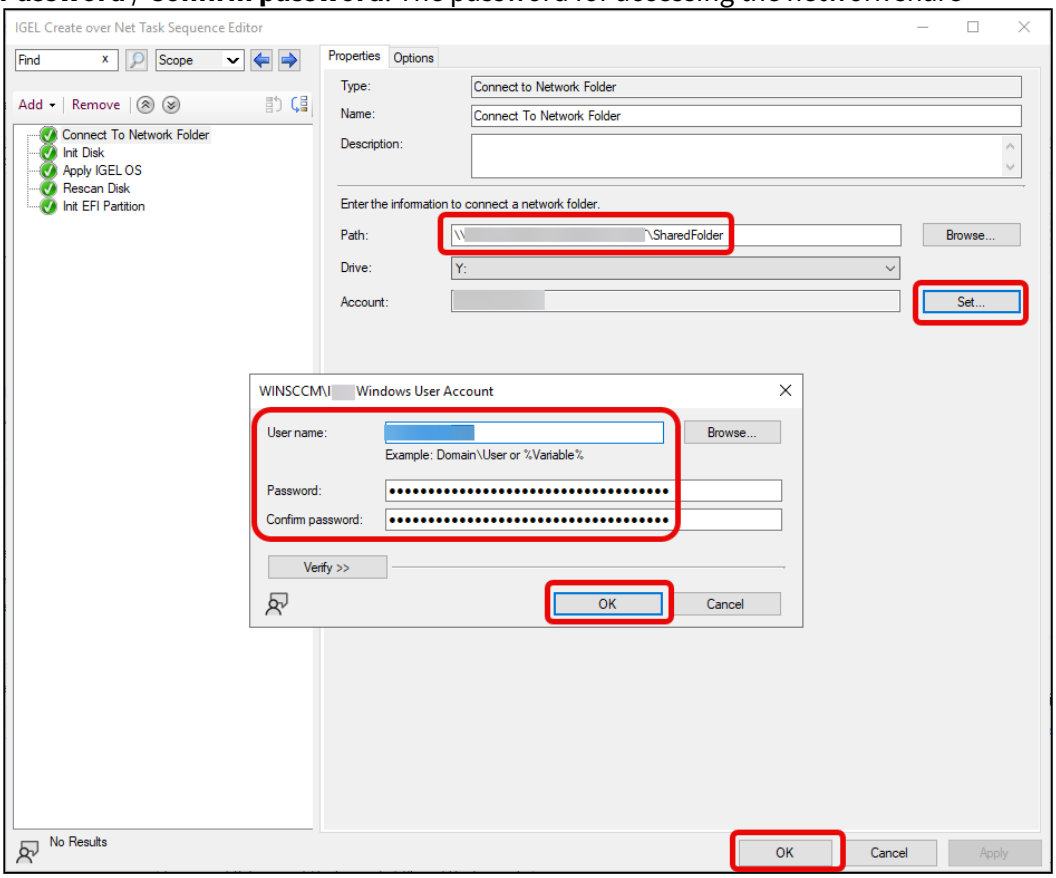


6. If you want to deploy the IGEL OS image separately via a network share: Select **Operating Systems > Task Sequences**, open the context menu for **IGEL Create over Net**, and then select **Edit**. Otherwise, continue with step 8.

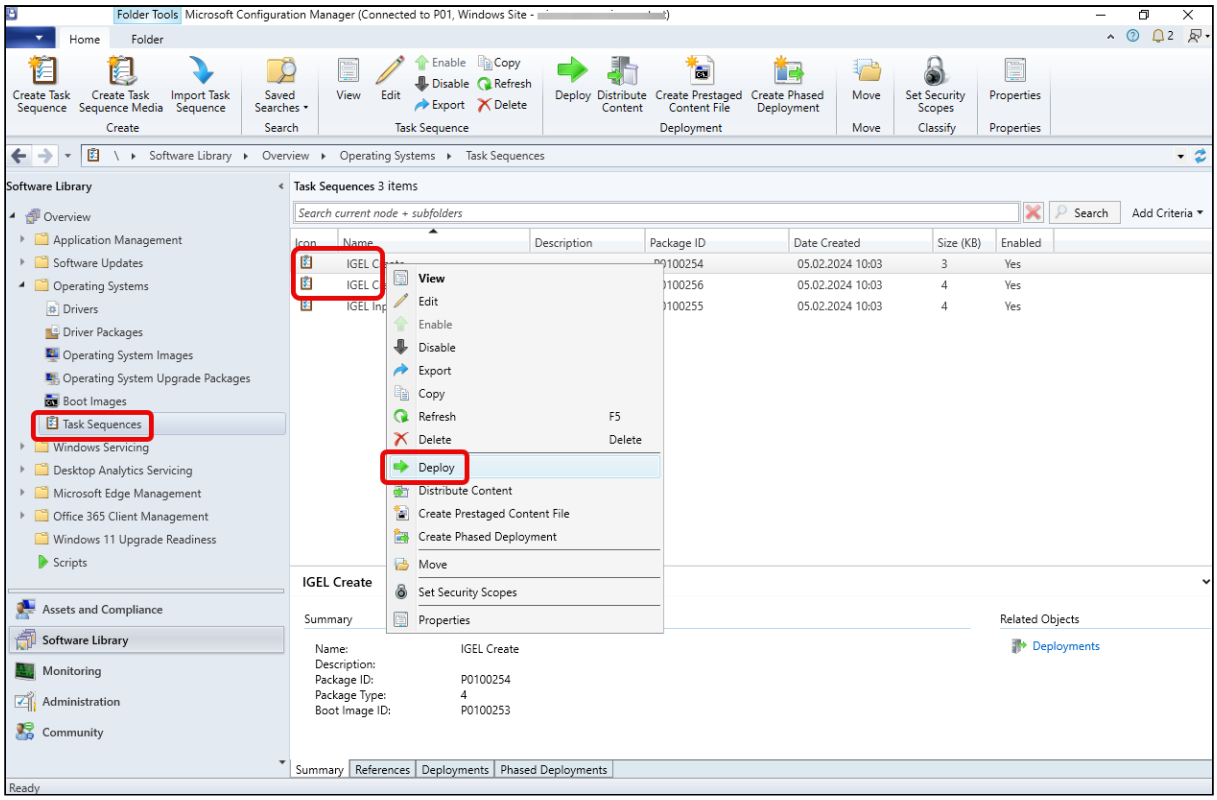


7. If you want to deploy the IGEL OS image separately via a network share (continued): Edit the settings for the task **Connect to Network Folder** as follows:
    - **Path**: Enter the path to the network share you want to use for distributing the IGEL OS image.
    - **Account**: Click **Set** to open the account data dialog and enter the required data:
        - **User name**: The username for accessing the network share, in the format DOMAIN\user

- **Password** / **Confirm password**: The password for accessing the network share

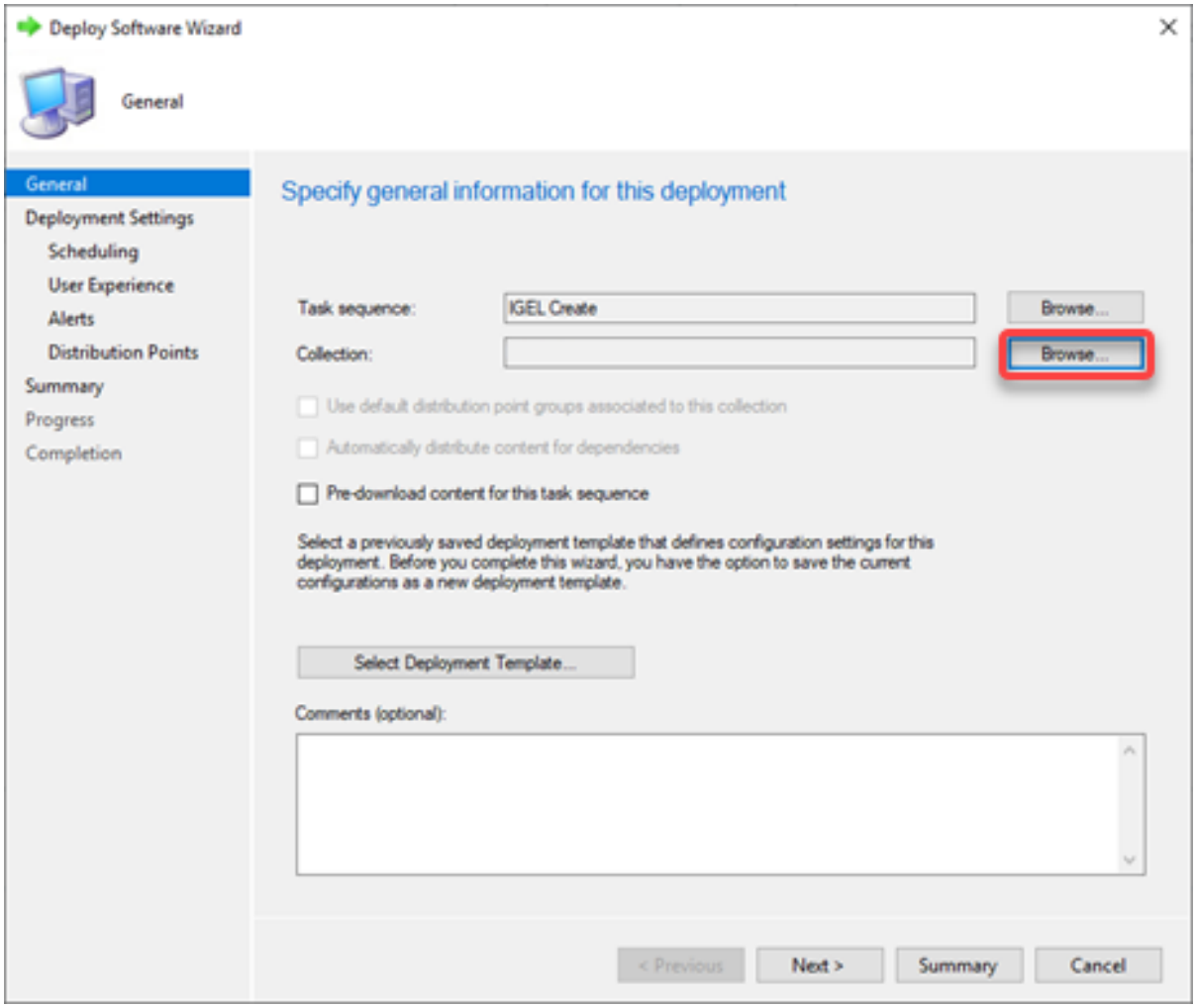


8. Select **Operating Systems > Task Sequences**, open the context menu for **IGEL Create** or **IGEL Create over Net**, and then select **Deploy**.



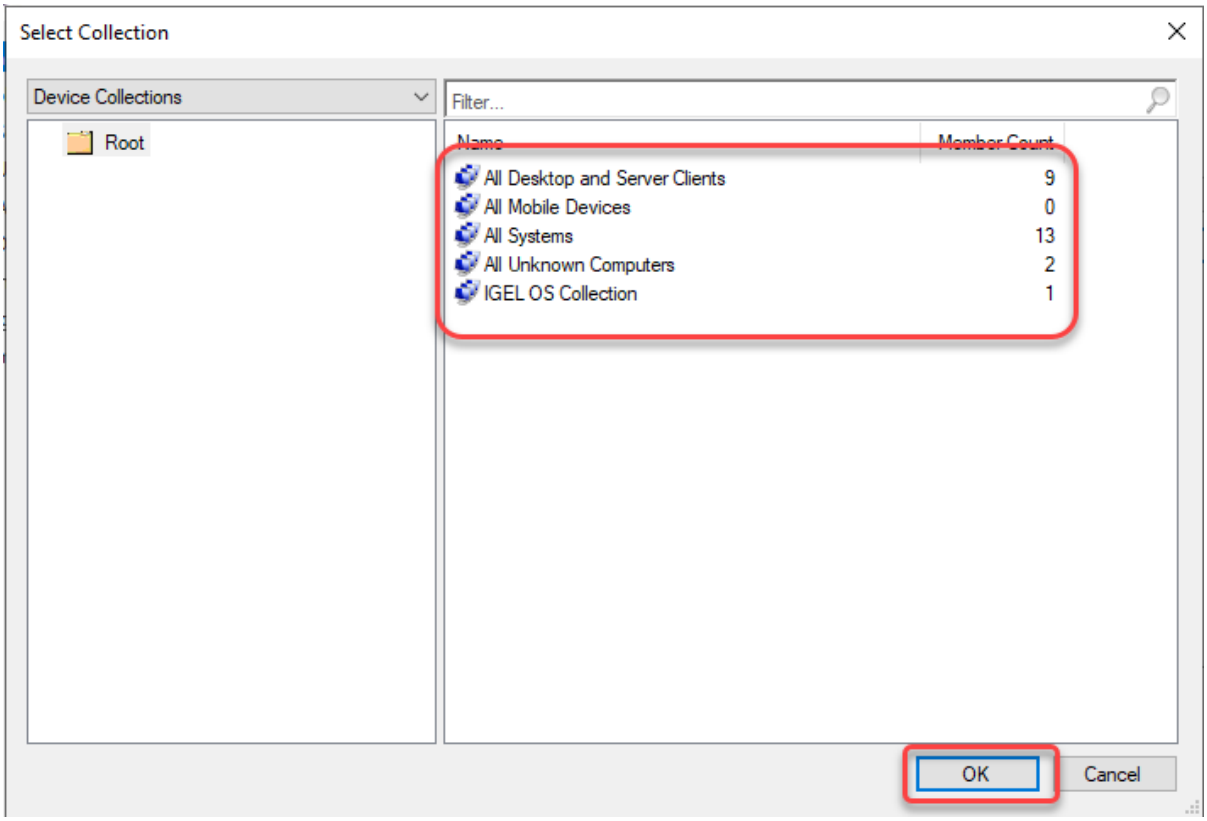
The **Deploy Software Wizard** opens.

9. Click the **Browse** button next to **Collection:**.



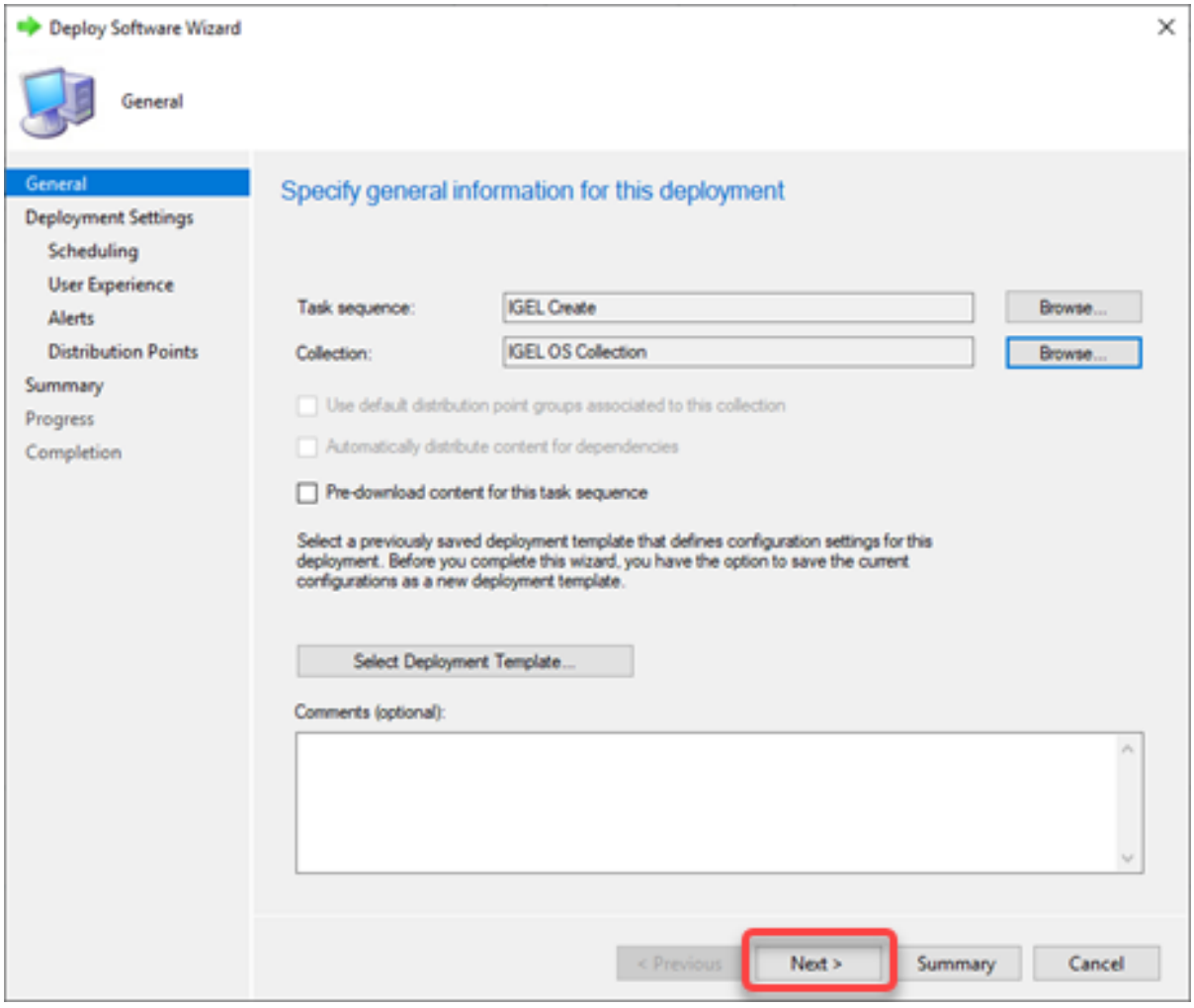
The **Select Collection** dialog opens.

10. From the list of collections, select the collection that contains your target devices and click **OK**.

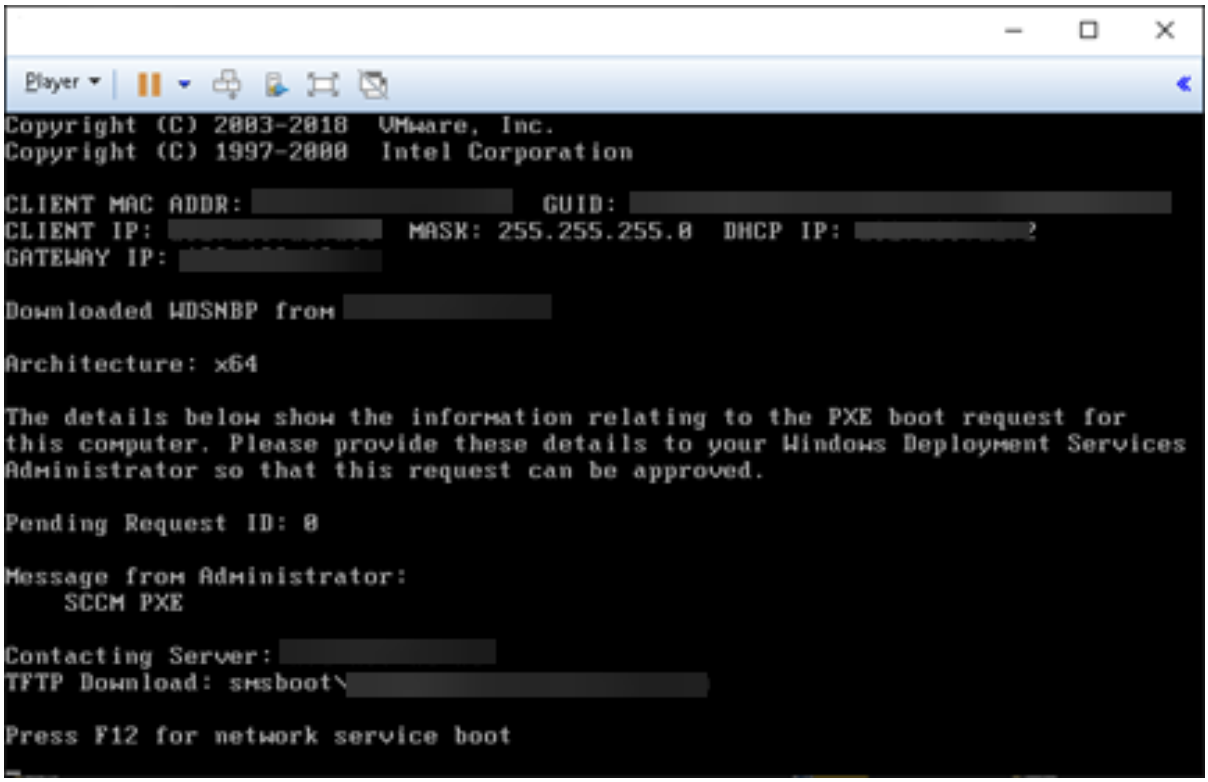


In our example, a user-created collection named **IGEL OS Collection** is selected.

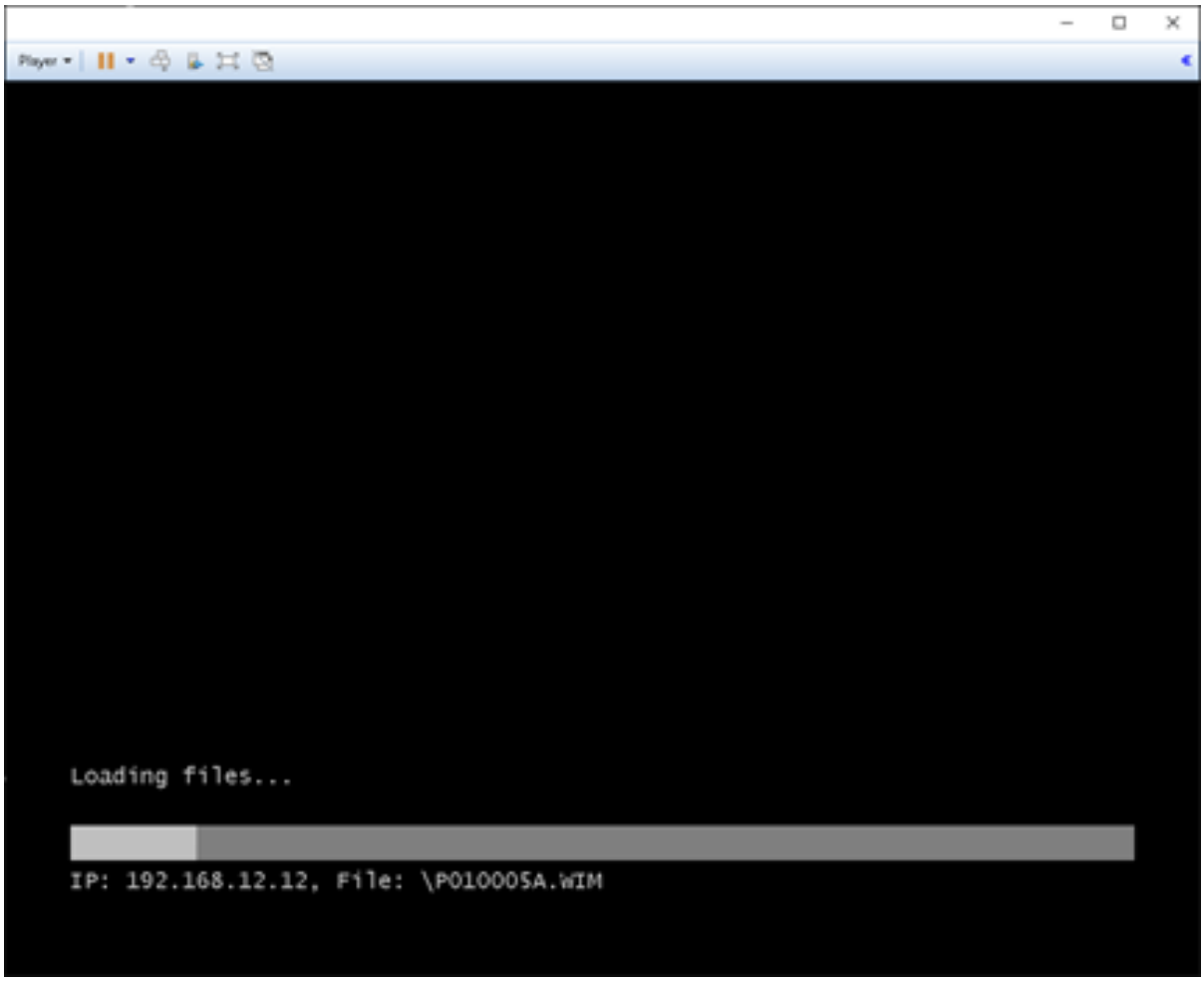
11. Click **Next** to continue with the wizard.



All target devices receive the PXE boot request that triggers them to boot the IGEL Boot Image.



The target devices load the IGEL Boot Image (WIM).



Alternative Deployment

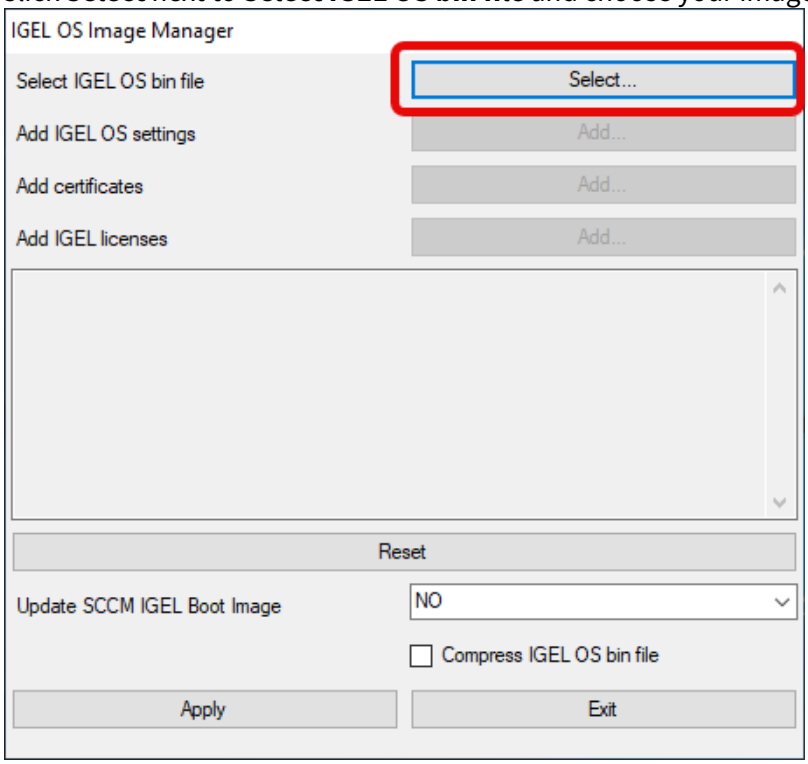
You can deploy a different IGEL OS image as an alternative to the image that comes with IGEL OS SCCM Add-on. The current main version is available from igel.com[25]. Optionally, you can add pre-configured settings, certificates, and license files to the image. In addition, you can compress the image to reduce the network load during distribution; please note that this increases the processing effort on the endpoint's side because the image needs to be decompressed.

1. Open a web browser, go to https://www.igel.com/software-downloads/cosmos/ **> OS 12 Base System Deployment Tool for SCCM**, download the current IGEL OS file, and unzip it.
   The IGEL OS image is ready for deployment.

2. Start the IGEL OS Image Manager by clicking on the desktop icon.

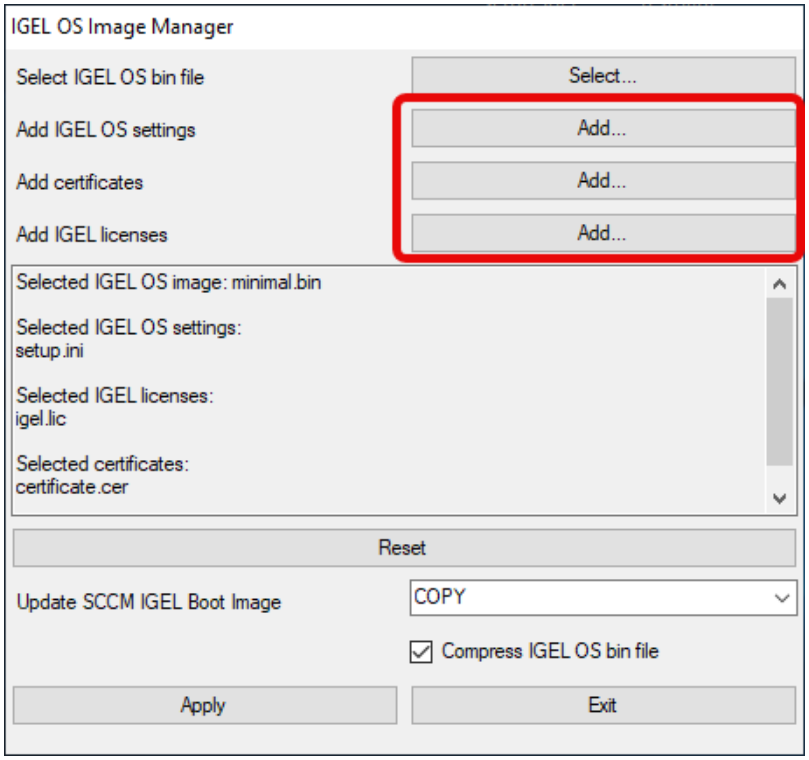
25 http://igel.com

3. Click **Select** next to **Select IGEL OS bin file** and choose your image file.

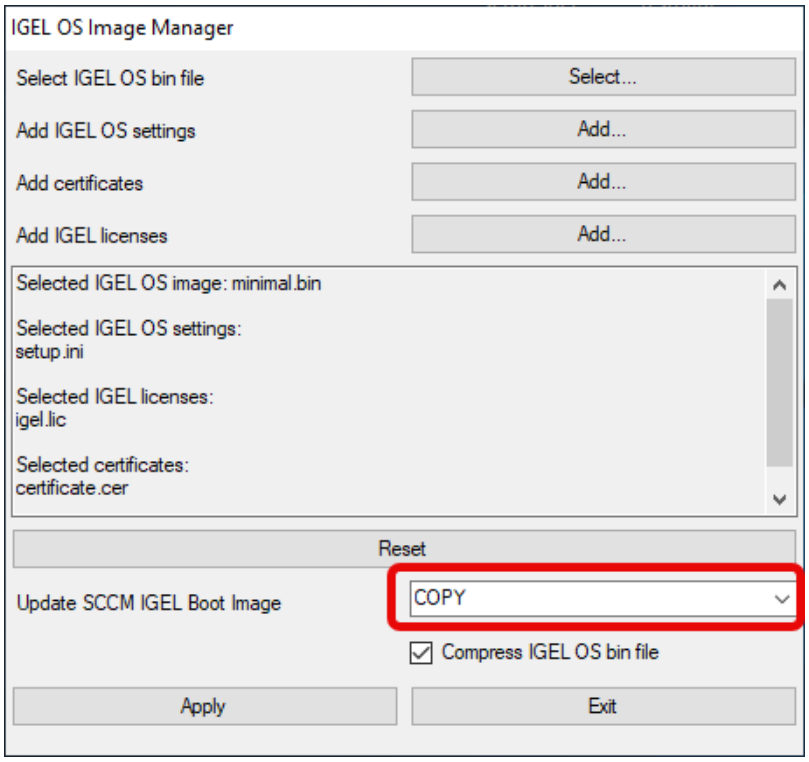


4. If you want to add settings, certificates, or license files, click **Add** next to the relevant item and choose the relevant files.
    - **Add IGEL OS settings**: The settings for IGEL OS. These settings can also be configured via the local Setup, the UMS device configurator, or a UMS profile.
    - **Add certificate**: Certificate files

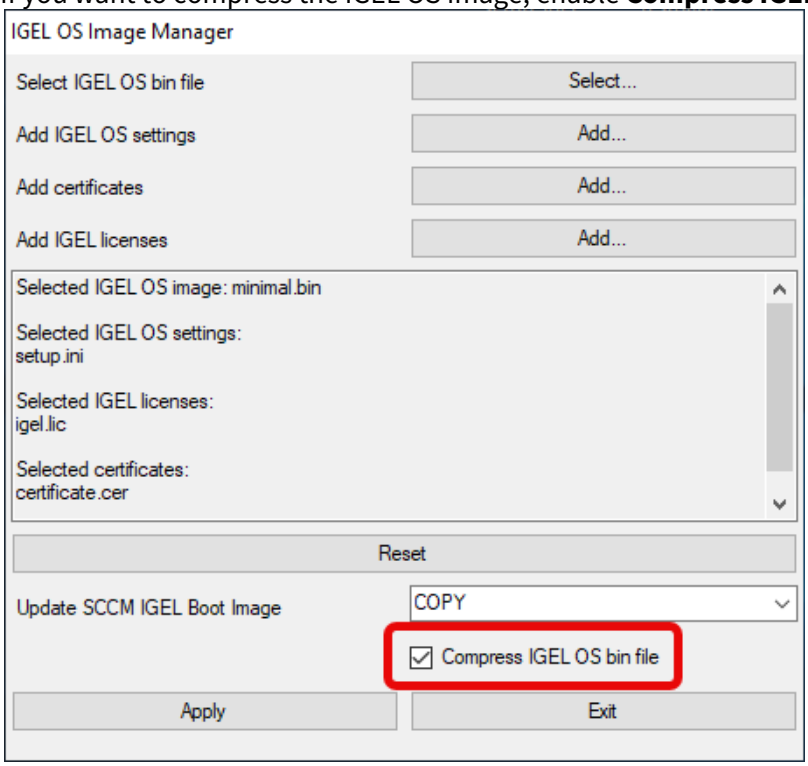
- **Add IGEL licenses**: License files



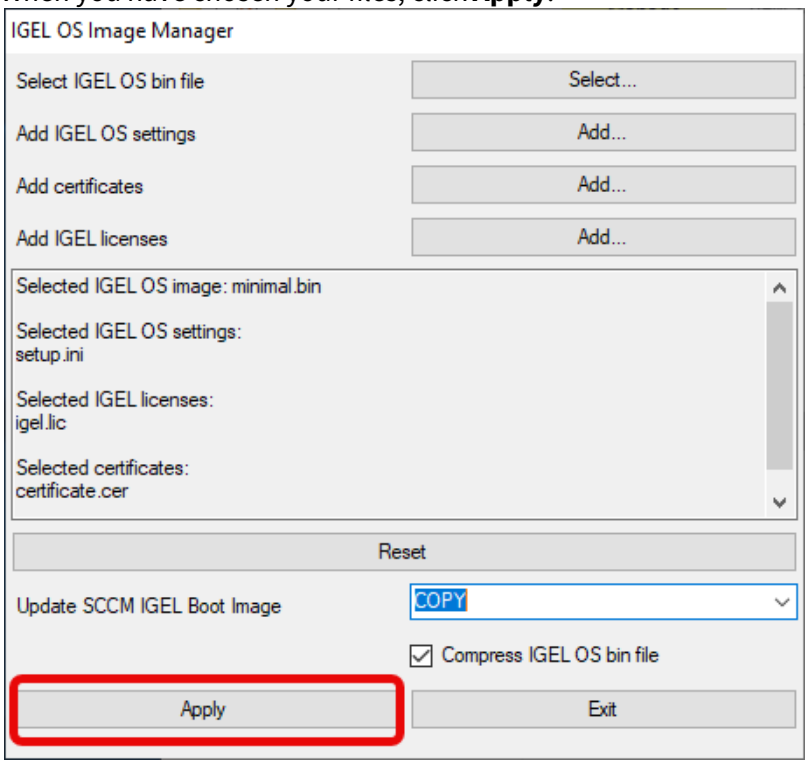
5. Set **Update SCCM IGEL Boot Image** according to your deployment method:
   - **NO**: Select this option if you want to modify only the IGEL OS image, but not the IGEL OS boot image (Windows PE).
   - **COPY**: Select this option if you want to deploy the IGEL OS image together with the basic Windows PE boot image. The Windows PE boot image and the IGEL OS image will be baked into one file which is distributed by the Microsoft Endpoint Configuration Manager.
   - **DELETE**: Select this option if you want to deploy the IGEL OS image separately via a network share. Only the basic Windows PE boot image will be distributed by the Microsoft Endpoint Configuration Manager; at a later stage, the devices will fetch the IGEL OS image from the network share.



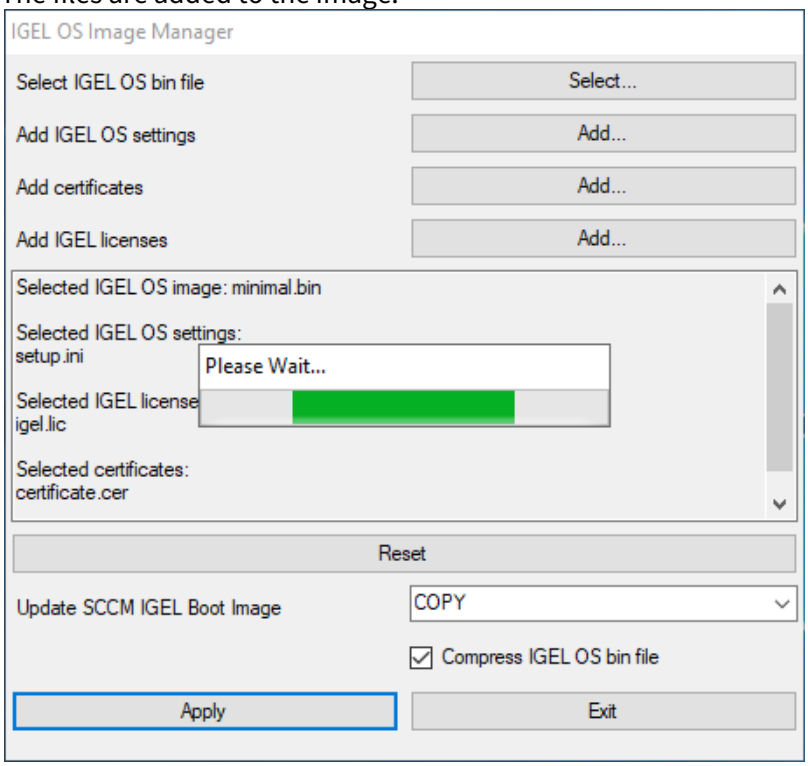
6. If you want to compress the IGEL OS image, enable **Compress IGEL OS bin file**.



7. When you have chosen your files, click **Apply**.



The files are added to the image.



How to Use IGEL OS 12 with UD Pocket

UD Pocket boots IGEL OS on your computer. However, it does not make any changes to the operating system already installed on the device's storage – UD Pocket runs entirely from the USB stick.

To facilitate booting your UD Pocket, you can use the IGEL UD Pocket Starter. The IGEL UD Pocket Starter creates a boot option for the UD Pocket so that there is no need to change the boot settings manually. You can install the IGEL UD Pocket Starter easily on an endpoint device running Microsoft Windows 10 or 11 - provided Microsoft BitLocker is not active on the device. When you uninstall the IGEL UD Pocket Starter, it is removed without any trace on the device.

UD Pocket, like all IGEL operating systems, can be managed centrally using the IGEL Universal Management Suite (UMS). UD Pocket uses IGEL OS, which is described in detail under Configuration of IGEL OS 12 Device Settings (see page 6).

UD Pocket has a partition that contains this manual and is readable under Windows. The manual describes setting up and starting UD Pocket on your computer.

> These instructions apply to UD Pocket and UD Pocket2.

Requirements

To use UD Pocket, your computer must meet the following requirements:

- USB 3.0 or 2.0 port from which the computer can boot
- Capability of booting from USB storage media
- Ethernet or wireless adapter. For a detailed list of supported graphics and network chips, see the IGEL Linux 3rd Party Hardware Database[26].
- The device is supported by IGEL OS; for details, see Devices Supported by IGEL OS 12.

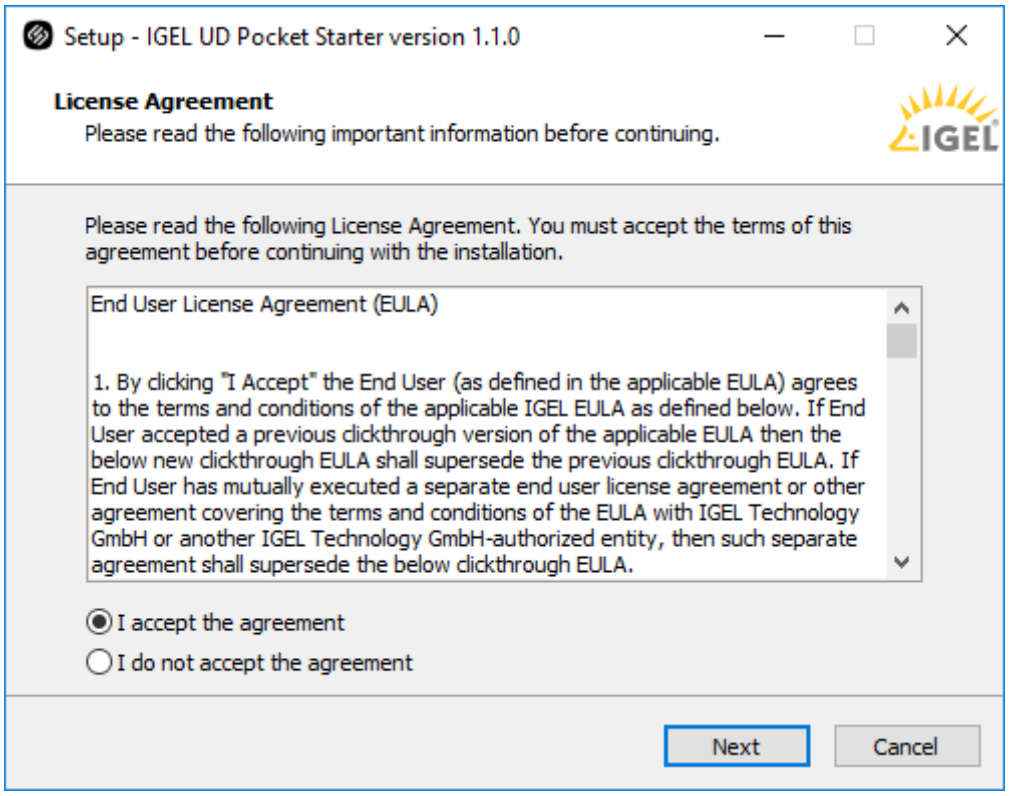
If you want to use the IGEL UD Pocket Starter, the following requirements apply:

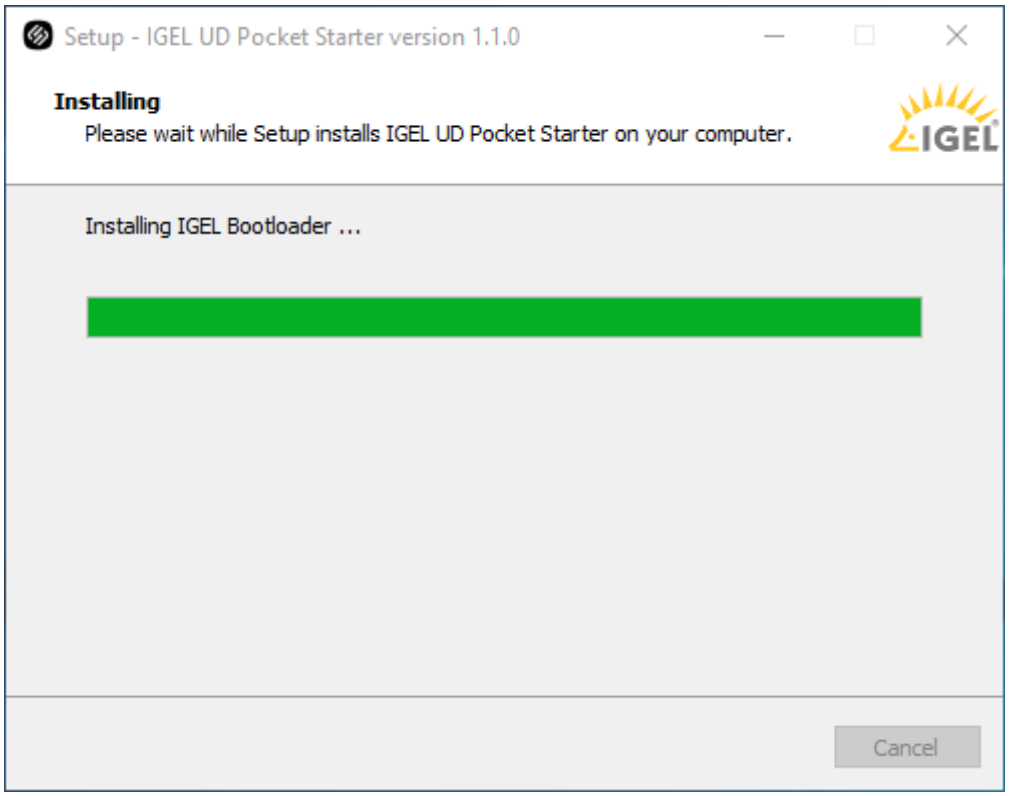
- Microsoft Windows 10 or 11 is installed on the endpoint device.
- The device has EFI BIOS
- Microsoft BitLocker is deactivated

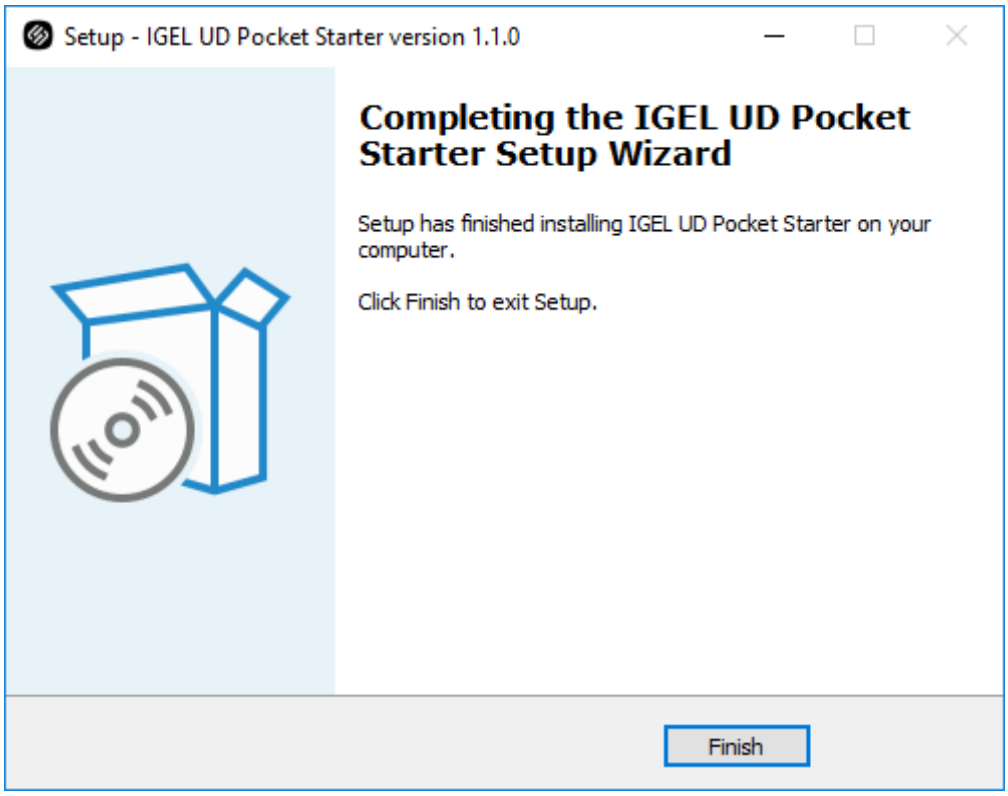
Installing the IGEL UD Pocket Starter

1. Download `setup-igel-udp_starter_<VERSION_NUMBER>.exe` from https://www.igel.com/software-downloads/
2. Copy the file to your endpoint device, double-click it, and follow the instructions of the IGEL UD Pocket Starter Setup Wizard.

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


Setup - IGEL UD Pocket Starter version 1.1.0
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
End User License Agreement (EULA)
1. By clicking "I Accept" the End User (as defined in the applicable EULA) agrees to the terms and conditions of the applicable IGEL EULA as defined below. If End User accepted a previous clickthrough version of the applicable EULA then the below new clickthrough EULA shall supersede the previous clickthrough EULA. If End User has mutually executed a separate end user license agreement or other agreement covering the terms and conditions of the EULA with IGEL Technology GmbH or another IGEL Technology GmbH-authorized entity, then such separate agreement shall supersede the below clickthrough EULA.
I accept the agreement
I do not accept the agreement
Next
Cancel

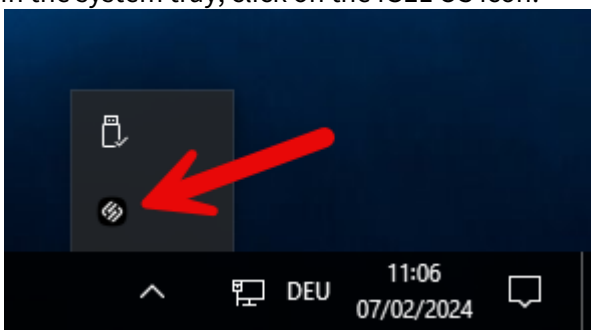

Setup - IGEL UD Pocket Starter version 1.1.0
Installing
Please wait while Setup installs IGEL UD Pocket Starter on your computer.
Installing IGEL Bootloader ...
Cancel



Configuring the Boot Order

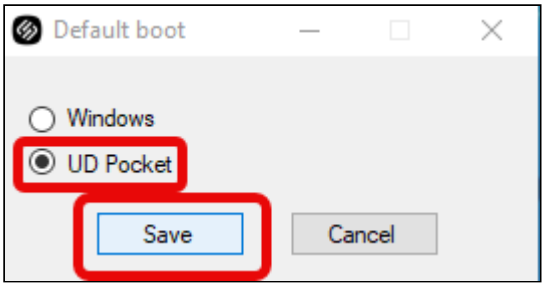
You can define which operating system is booted by default, i.e. if the user does not make a selection in the boot menu.

1. In the system tray, click on the IGEL OS icon.



2. Choose the desired default operating system and click **Save**.
   - **Windows**: Windows is booted by default, even if a UD Pocket is plugged into the device.

- **UD Pocket**: IGEL OS is booted from the UD Pocket, provided it is plugged in.



Starting Your IGEL UD Pocket (With IGEL UD Pocket Starter Installed)

1. Plug the UD Pocket into a free USB slot of your device.
2. Turn on your device; if the device is already switched on, restart it.
   Your device boots into IGEL OS, provided you have chosen this option when configuring the boot order (see page 445).

Starting Your IGEL UD Pocket (Without IGEL UD Pocket Starter)

Booting from Your UD Pocket

1. Plug the UD Pocket into a free USB slot of your device.
2. Turn on your device; if the device is already switched on, restart it.
3. If a boot menu is presented that contains **IGEL UD Pocket** as an option, select this option. If not, proceed with Customizing the Boot Settings (see page 446).

Customizing the Boot Settings

Booting from USB storage media may already be enabled on your device, or you may have to enable it yourself. The required key presses for this may vary from vendor to vendor. However, here are some hints:

▶ While the device is booting, try pressing [F12] (in general), [F10] (Intel devices), or [F9] (Hewlett-Packard devices) to access a list of boot devices and select **IGEL UD Pocket**.

▶ If the above does not work, access the BIOS settings via pressing [Del], [F1], or [F2] during boot, activate booting from USB storage media, and/or change the boot order.

▶ See the BIOS/UEFI documentation for your system for details on how to boot from USB storage media.

IGEL OS supports UEFI Secure Boot. Refer to the manual of your device's manufacturer to learn whether your device supports Secure Boot and how to enable it. Enabling Secure Boot often consists of two steps. First, the boot mode has to be changed to UEFI Boot in the BIOS; after that, Secure Boot can be activated, also in the BIOS. How to check whether Secure Boot has been properly enabled, you can learn under Verifying that Secure Boot is Enabled.

If UD Pocket fails to boot in UEFI mode, try it in legacy/BIOS mode. If this does not help, try another endpoint device to verify that the UD Pocket is functional and/or check for BIOS updates for your endpoint device and the latest IGEL OS updates.

Do not remove the UD Pocket from the computer until you have shut down the IGEL OS contained on it. Otherwise, you can damage the operating system on UD Pocket and lose your settings as well as data on other removable media.

After the First Boot-Up

To get started with your IGEL OS 12 device, see Onboarding IGEL OS 12 Devices.

IGEL Tech Video

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

https://www.youtube.com/watch?v=iURhgESsn6k

Facilitated Switching between IdPs for Single-Sign On (SSO) In IGEL OS 12.2

Overview

Switching between Okta and Microsoft Entra ID has been facilitated with IGEL OS 12.2.

With IGEL OS 12.01, the behavior of the SSO configuration was as follows: When you wanted to switch the IdP between Okta and Microsoft Entra ID, you had to delete and re-enter the public client identifier and the secret every time. This goes back to the fact that these values were not stored as separate parameters on the device.

With IGEL OS 12.2 or higher, the SSO configuration has been optimized. The public client identifiers and the secrets are now handled separately for Okta and Microsoft Entra ID. To benefit from this improvement, the profile must be based on IGEL OS 12.2.

Automatic Update Results in Broken SSO

If your devices have been updated because **Auto-update Default Version to newest version** is active (see Configuring Update Settings for Individual IGEL OS Apps), and the SSO settings are still defined by a profile for IGEL Base System 12.01, SSO will not function anymore. In this case, you must immediately create an appropriate profile for IGEL OS Base System 12.2, as described in this article.

Important Measures for Devices that Retain Base System 12.01

If some of your devices are to keep IGEL OS Base System 12.01, ensure the following:

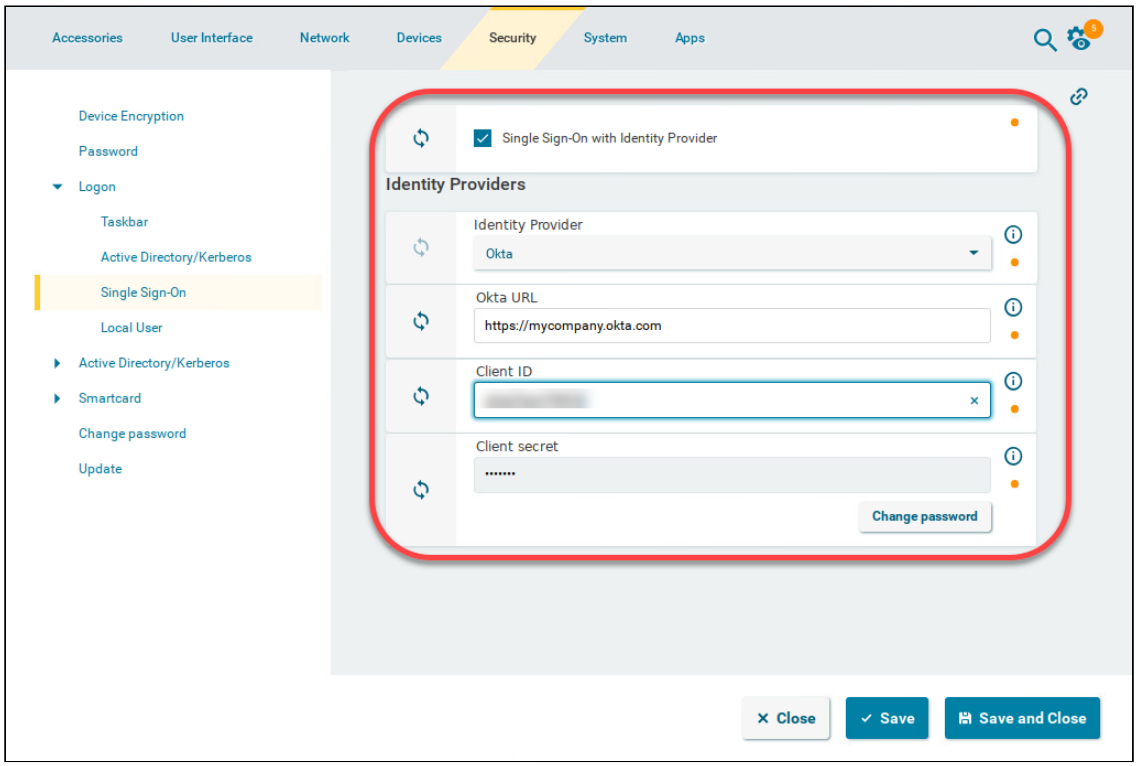
- The current SSO profile is set to version 12.01.x of the IGEL OS Base System, not to the default version. This is done by setting the **App Selector** to version **12.01**.x explicitly. If the base system version remains set to the default version, and the default version is then set to 12.2 or higher, the settings will be lost when the profile is saved.
- The current SSO profile (based on IGEL OS Base System 12.01) remains assigned to those devices.

Setting Up a New Profile for Easy IdP Switching

1. In the UMS Web App, create a new profile for the IGEL OS Base System based on version 12.2. This can be done by setting the profile's **App Selector** to version **12.2.0** explicitly or by setting the base system's default version to 12.2 and the profile's **App Selector** to **Default version**.

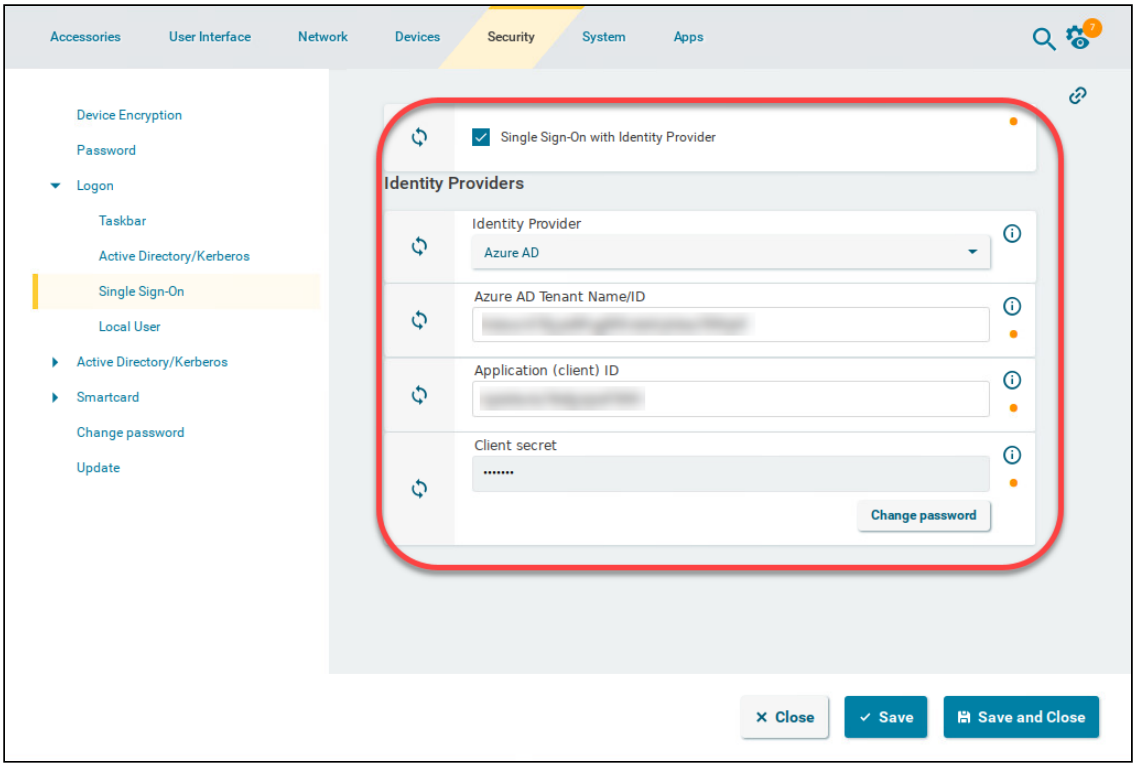
2. For your Okta configuration, go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Okta**.
   - Provide the **Okta URL** for your user. This is the Okta organization URL. Example: "https://mycompany.okta.com"

- Provide the **Client ID**. This is the client ID that was created in Okta.
- Provide the **Client secret**.



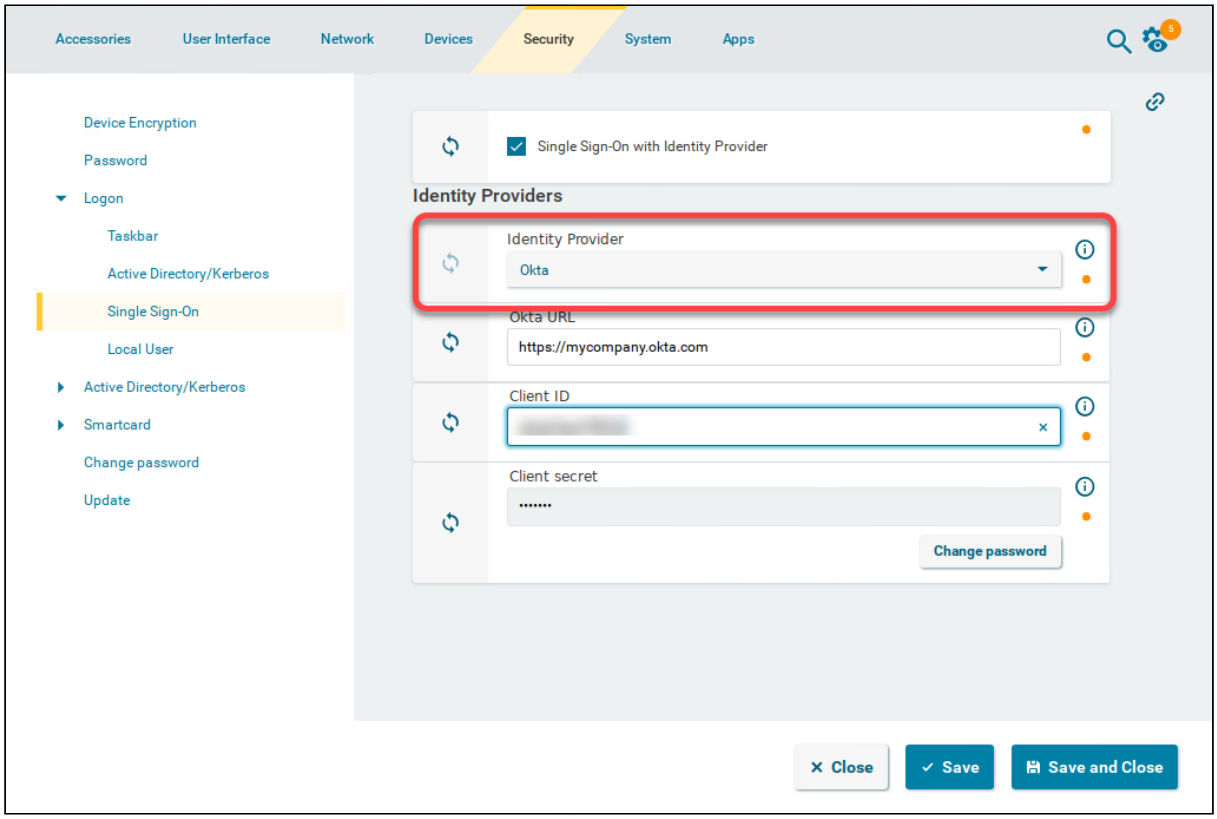
3. For your Microsoft Entra configuration, go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Azure ID**.
   - Enter the **Azure AD Tenant Name/ID**. This is the value you have obtained as **Directory (tenant) ID** in the Microsoft Entra Portal.
   - Set the appropriate **Application (client) ID**. This is the value you have obtained as **Application (client) ID** in your Microsoft Entra ID Portal.
   - Enter the **Client secret**.

   ⚠ The secret for Microsoft Entra ID can only be viewed once. If you have not stored it, you need to generate a new one.



4. Assign this profile to all relevant devices.

5. If you want to switch between Okta and Microsoft Entra ID, simply select the appropriate **Identity Provider**:



Upgrading from IGEL OS 11 to IGEL OS 12

For instructions on upgrading endpoint devices from IGEL OS 11.09 to IGEL OS 12 via the Universal Management Suite (UMS), see Upgrading (Migration) from IGEL OS 11 to IGEL OS 12.

How to Customize the Unit ID Computation for IGEL OS Creator (OSC)

In Which Cases Should I Change the Computation of the Unit ID?

Every IGEL OS device has a unit ID which must be unique and persistent. This is crucial for the administration and licensing of the device. For devices with a permanently installed IGEL OS (not UD Pocket), the unit ID is derived from the MAC address of a network interface.

The unit ID is computed on the first boot after IGEL OS has been successfully installed by IGEL OS Creator (OSC). In almost all cases, the default algorithm for computing the unit ID will choose the appropriate MAC address. However, in the rare case that the MAC address chosen by the default algorithm is not the ideal one for your requirements, e.g. if the chosen network device is not used later on, you can define custom rules. To apply your custom rules, you must write them to a file within the IGEL OS Creator (OSC).

> **Changing the Unit ID of a Registered Device**
>
> When the unit ID of a device that is registered with the UMS is changed, the registration is broken. In this case, you must re-register the device, e.g. by scanning.

Requirements

- Bootable USB memory stick with IGEL OS Creator (OSC) 12.2.2 or higher. If you haven't got this software already, download it from https://www.igel.com/software-downloads/cosmos/.
- A Linux machine; the examples in this article are based on IGEL OS.

What Is the Default for Computing the Unit ID?

The default algorithm for choosing the MAC address for unit ID computation is as follows:

1. If a network interface exists that matches a license already installed on the device, discard all other network interfaces.
2. Discard network interfaces that do not have the highest subsystem priority. The subsystem priorities are (from highest to lowest): PCI, SDIO, USB, others.
3. Discard wireless network interfaces if a wired interface exists.
4. From the remaining network interfaces, use the one that is first in lexicographical order.

Which Computation Rules Are Available?

The following list contains all available rules for unit ID computation. Please note that if several network interfaces meet the criteria, the first one in the lexicographic order is selected unless the rule `reverse_order` is applied.

- `prefer_pci` : If a network interface connected via the PCI subsystem exists, discard all interfaces connected via other subsystems.

- `prefer_sdio` : If a network interface connected via the SDIO subsystem exists, discard all interfaces connected via other subsystems.
- `prefer_usb` : If a network interface connected via USB subsystem exists, discard all interfaces connected via other subsystems.
- `prefer_wired` : If a wired network interface exists, discard all wireless interfaces.
- `prefer_wireless` : If a wireless network interface exists, discard all wired interfaces.
- `ignore_licensed` : Do not take into account whether an interface is licensed or not. (In contrast to the default behavior where network interfaces that match the device's license are given preference.)
- `reverse_order` : If more than one equivalent network interface is found, use the last one in the lexicographical order instead of the first one,

Creating a Custom Set of Rules

To achieve a specific computation of the unit ID, you can combine several rules.

Example

The set of rules `prefer_wireless, ignore_licensed, reverse_order` leads to the following behavior:

1. `prefer_wireless` : If a wireless network card is connected, all wired network cards are discarded.
2. `ignore_licensed` : If there are several wireless network cards and one of them matches the device's license, this does not count as a reason to use it for unit ID computation.
3. `reverse_order` : As the licensing criterion does not count, the position of a network device's name in the lexicographic order is the next criterion. By default, the first device in lexicographic order would be selected, but `reverse_order` defines that the last device is selected.

Applying the Set of Rules to Your OSC (IGEL OS)

In the following description, we use IGEL OS. On other Linux variants, the procedure may differ; in particular, mounting the memory stick may require `sudo` .

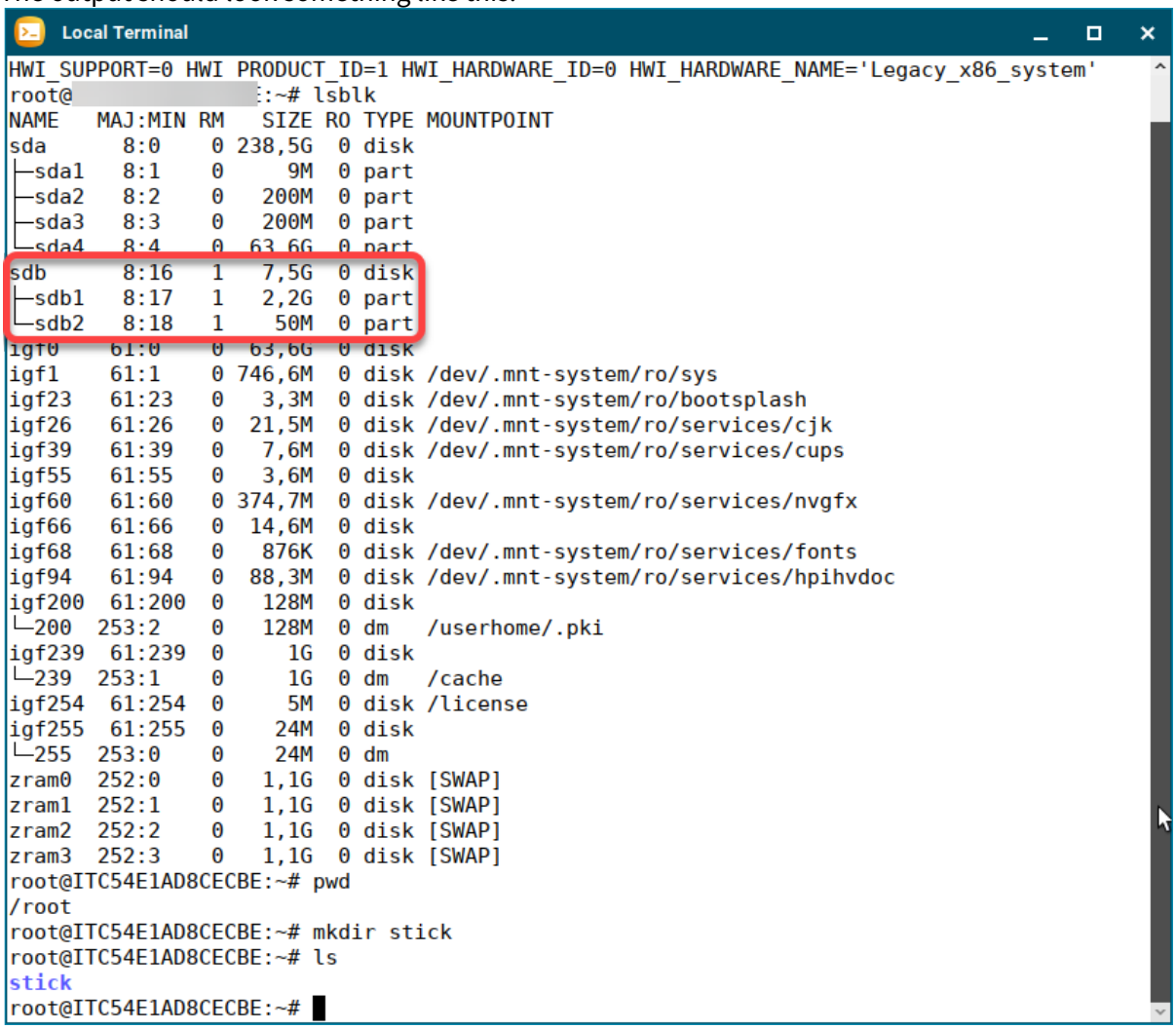
1. Plug the USB memory stick with IGEL OSC on it into your device.
2. Open a terminal on the device and log in as root. For details on configuring a terminal on IGEL OS, see Terminals (see page 12).
3. Create a directory to which the memory stick will be mounted, e.g. `stick/`

```
mkdir stick
```

4. Determine the device name of the memory stick with `lsblk`

```
lsblk
```

The output should look something like this:

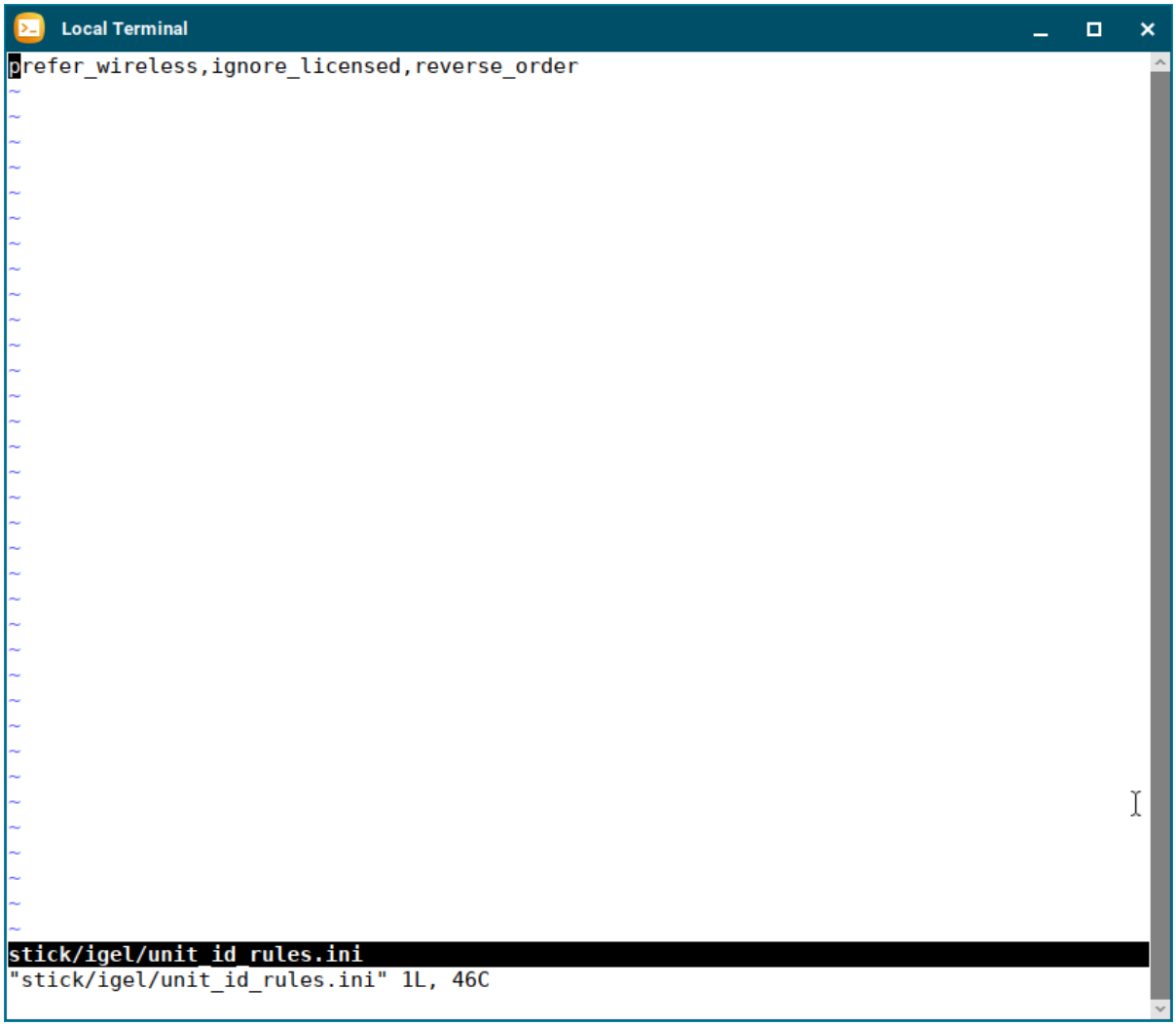


5. When you have determined which of the listed devices is your memory stick, mount the second partition to the `stick/` directory. In our example, this is `sdb2`.

```
mount /dev/sdb2 stick/
```

6. Use your favorite text editor, e.g. `vi`, to create your `unit_id_rules.ini` file.

```
vi stick/igel/unit_id_rules.ini
```



7. Unmount the partition.

```
umount stick
```

Now you can use the modified OSC on your memory stick to install IGEL OS on your devices.

How to Configure Single Sign-On (SSO) on IGEL OS 12

With IGEL OS 12, you can use Single Sign-On (SSO) via a cloud-based identity provider (IdP) to access the local device and apps.

The following identity providers are supported:

- Okta
- Microsoft Entra ID (formerly known as Microsoft Azure AD)
- Ping Identity | PingOne
- VMware Workspace ONE Access

Generally, IGEL OS 12 supports OpenID Connect authentication. For IdPs that adhere closely to this standard, there is a good chance that they can be used with IGEL OS 12.

Generally, you can edit the IGEL OS 12 device configuration as follows:

- via the IGEL UMS Web App:
  - **Configuration > Create new profile** (You select one or several apps that will be configured by the profile. If the IGEL OS base system app is selected, all other apps are shown under the tab "Apps"; if not, each app is displayed as a separate tab)
  - **Apps > [name of the app] > Create new profile** (used to quickly configure a profile for the selected app. It is also possible to add other apps that will be configured by this profile)
  - **Devices > [name of the device] > Edit Configuration** (shows all installed apps. Apps are displayed under the tab "Apps")
- via IGEL Setup locally on the device (shows all installed apps. Apps are displayed under the tab "Apps")

The best practice to configure your devices is via profiles. For details on how to create profiles, see Creating a Profile.

Apps and Utilities for IGEL OS 12 That Support SSO with Microsoft Entra ID

- IGEL Azure Virtual Desktop Client (AVD)
- Zoom client (SSO via Chromium)
- Web apps, e. g. Office 365 (SSO via Chromium)
- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with Okta

- Web apps, e. g. Okta portal (SSO via Chromium)

- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with Ping Identity / PingOne

- Web apps (SSO via Chromium)
- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with VMware Workspace ONE Access

- VMware Horizon (if Chromium is used for authentication)
- Web apps (SSO via Chromium)
- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with Other IdPs

- Web apps (SSO via Chromium)
- Device login
- Screenlock

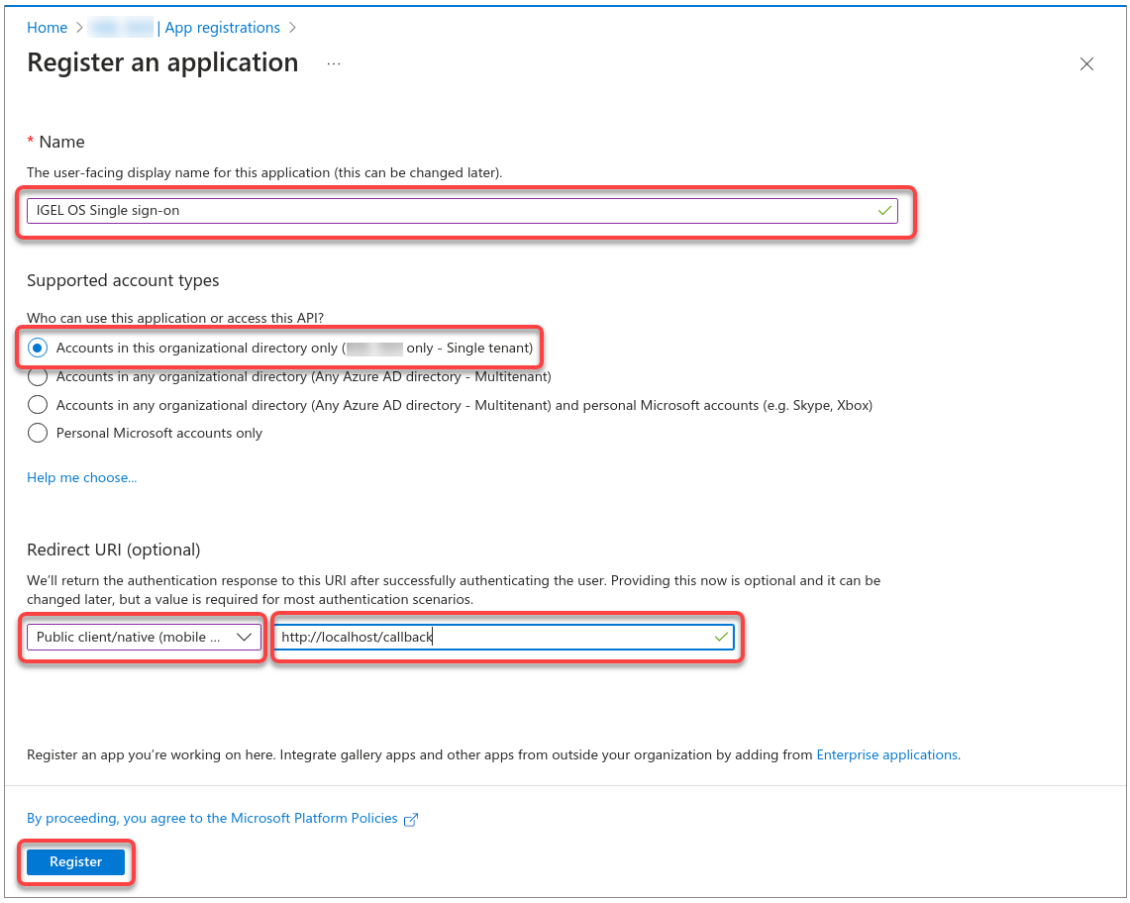
Setting up SSO with Microsoft Entra ID

To enable SSO with Entra ID on IGEL OS 12 devices, an Entra application must be registered first. Then, you can configure IGEL OS 12 to use this application for authentication; the Entra application is referenced via its Public Client Identifier.

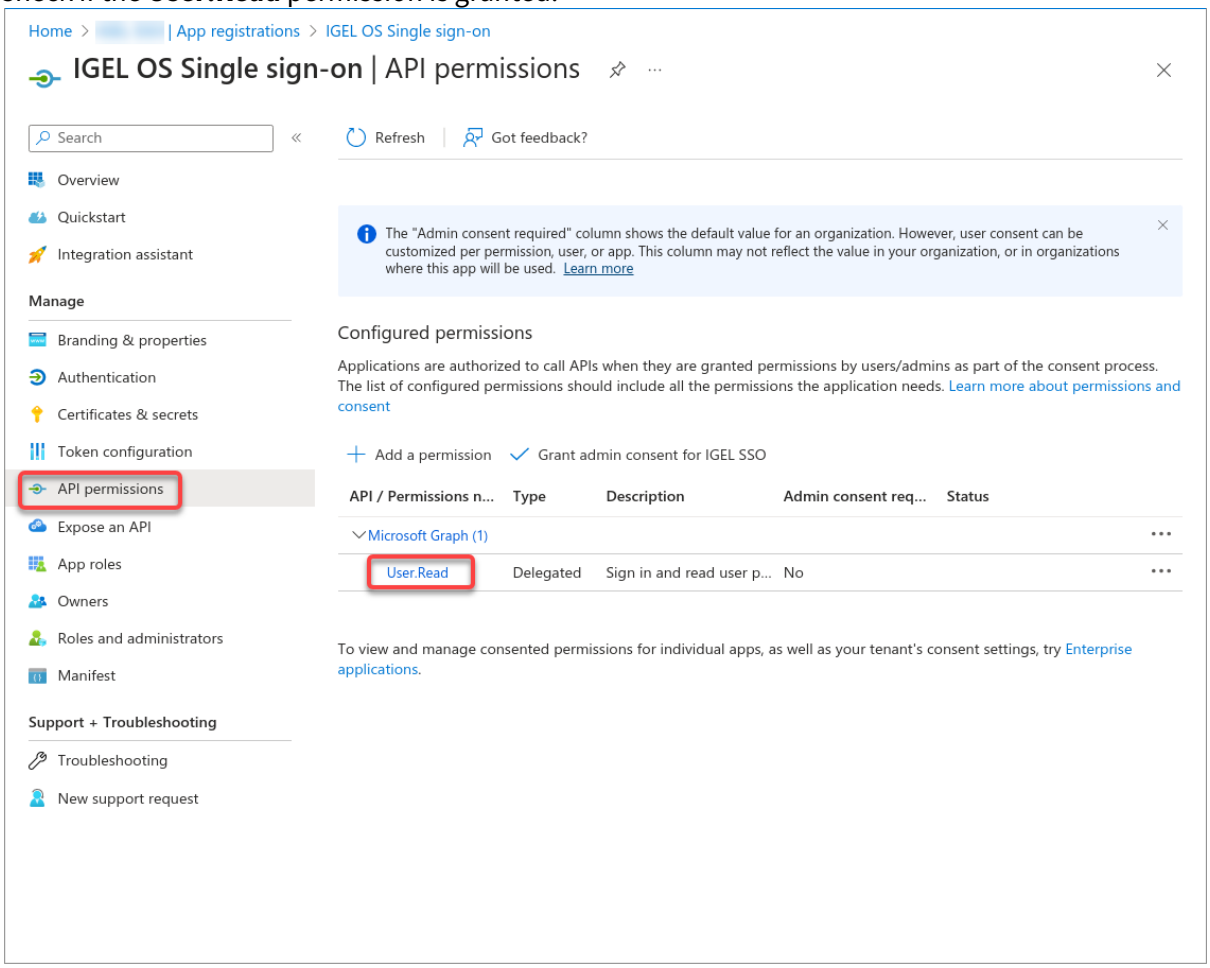
Registering an Entra Application

1. In your Entra AD Portal, go to **App registrations > New registration**.

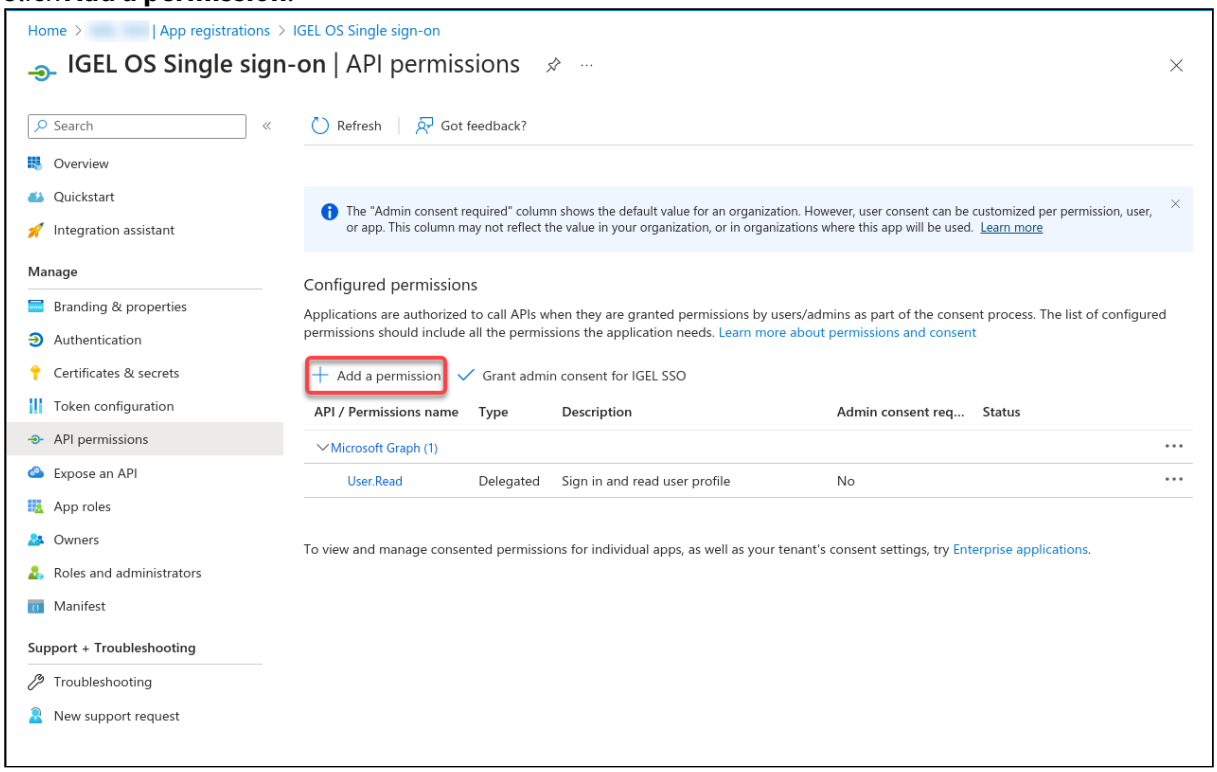
2. Edit the data as follows and then click **Register**:
    - Add a proper name for the application. Note that this name will be visible to the user once during the consent process for granting permissions. In our example, "IGEL OS Single sign-on" is used as the name.
    - Select the option **Accounts in this organizational directory only ([name of your organization's AD Portal] only - Single tenant)**.
    - Under **Redirect URI (optional)**, select the option **Public client/native (mobile & desktop)** and enter "http://localhost/callback" as the URI.


Home > | App registrations >
Register an application
* Name
The user-facing display name for this application (this can be changed later).
IGEL OS Single sign-on
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft accounts only
Help me choose...
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Public client/native (mobile ...
http://localhost/callback
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.
By proceeding, you agree to the Microsoft Platform Policies
Register

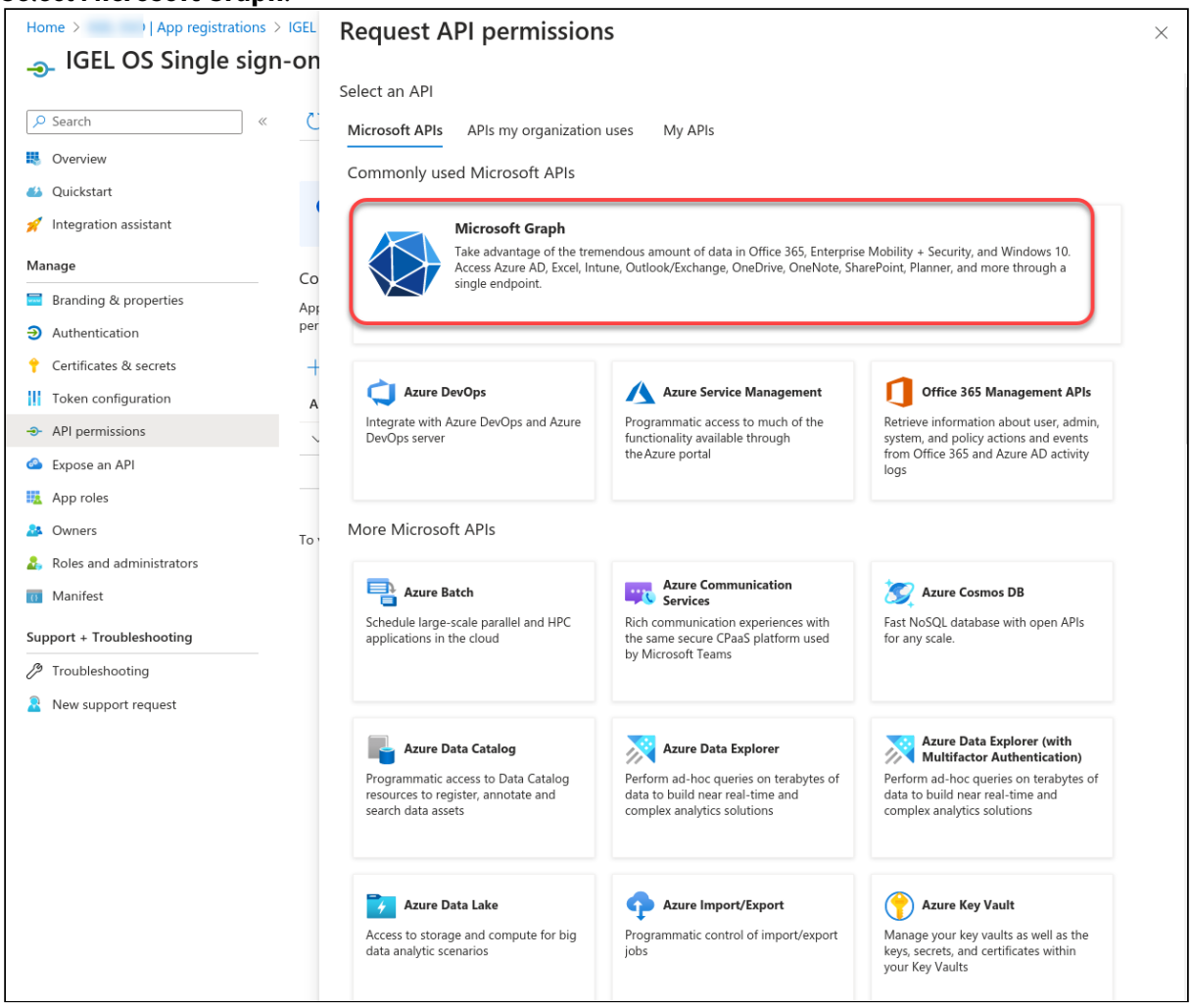
3. Check if the **User.Read** permission is granted.



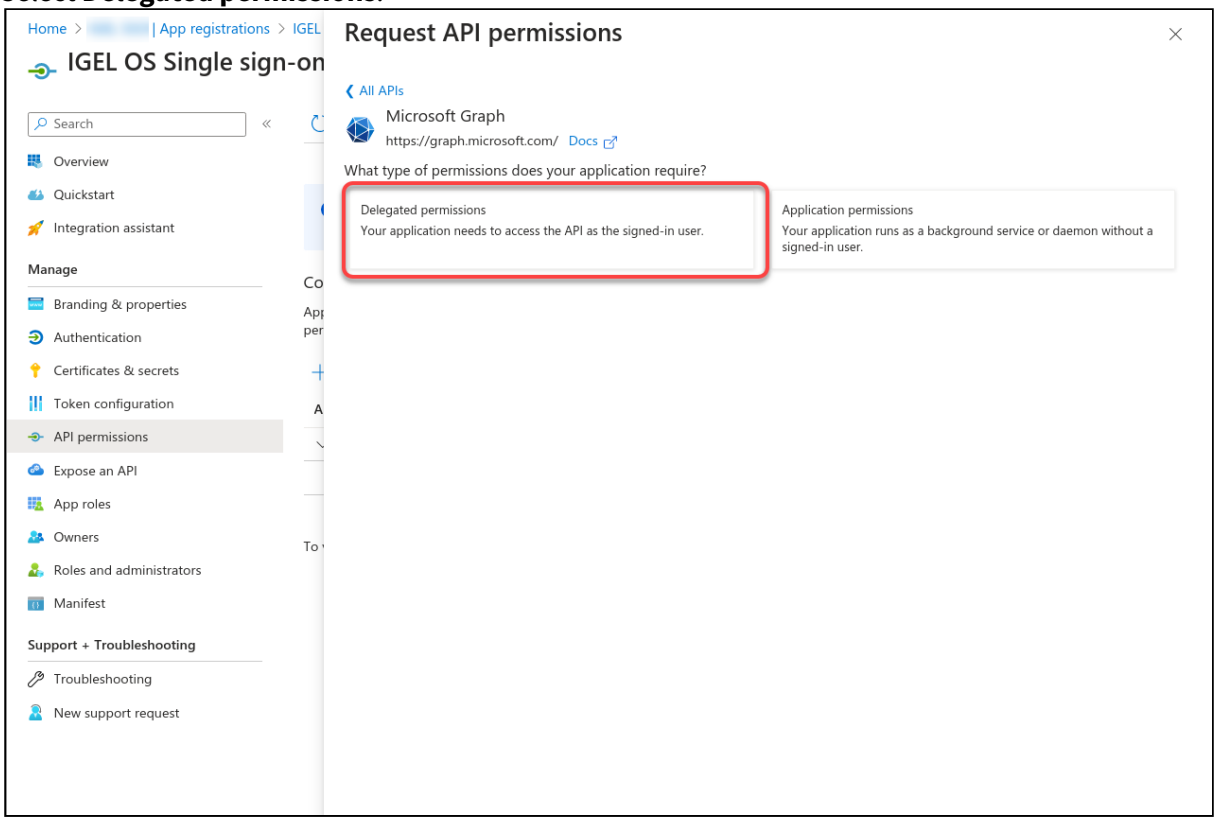
4. Click **Add a permission**.



5. Select **Microsoft Graph**.

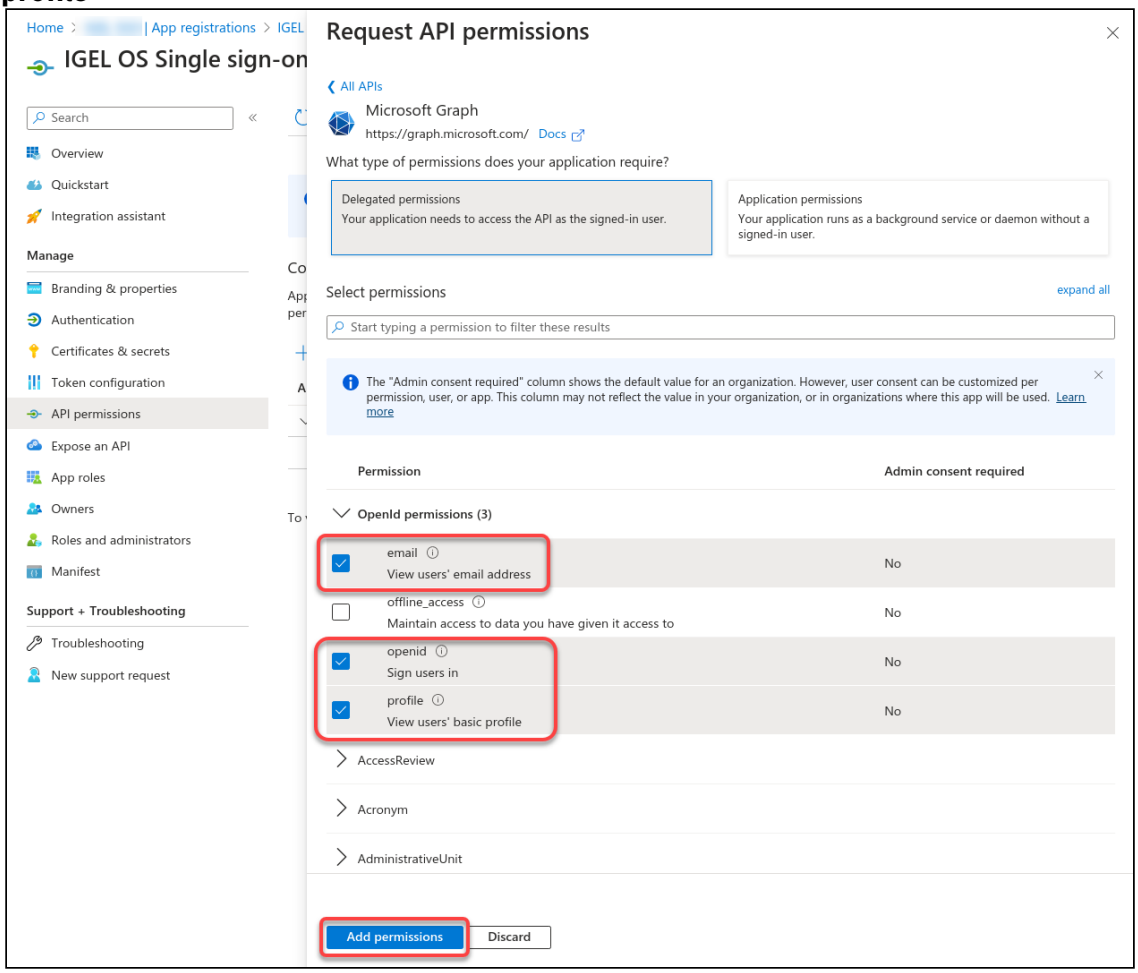


6. Select **Delegated permissions**.

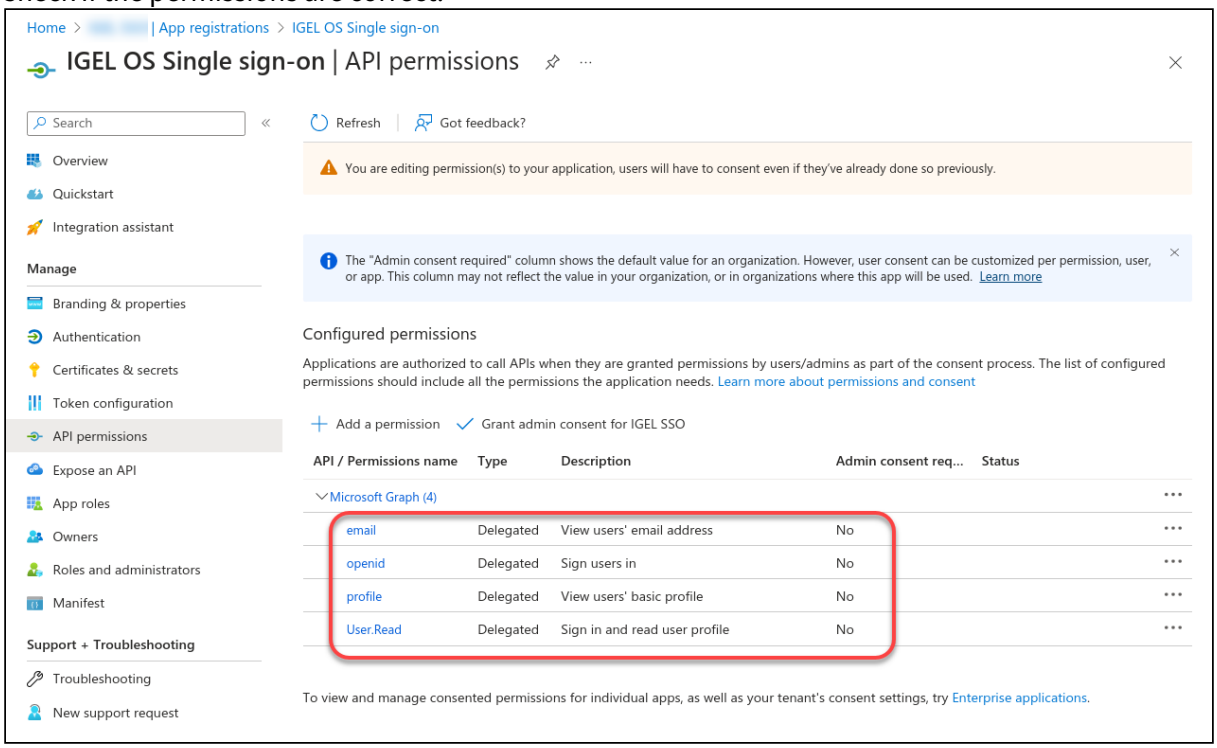


7. Enable the following permissions and then click **Add permissions**:
   - **email**
   - **openid**

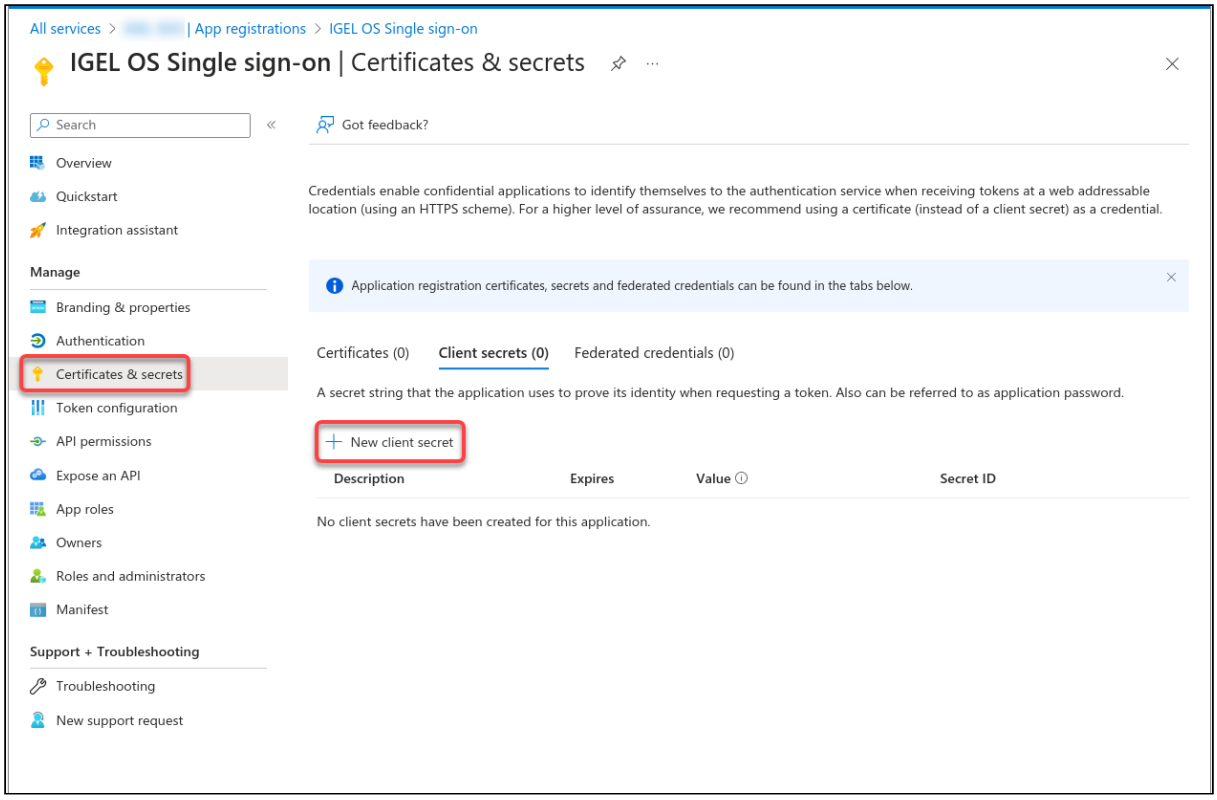
- **profile**


Home > | App registrations > IGEL
IGEL OS Single sign-on
Search
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Request API permissions
All APIs
Microsoft Graph
https://graph.microsoft.com/ Docs
What type of permissions does your application require?
Delegated permissions
Your application needs to access the API as the signed-in user.
Application permissions
Your application runs as a background service or daemon without a signed-in user.
Select permissions
expand all
Start typing a permission to filter these results
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more
Permission
Admin consent required
OpenId permissions (3)
email
View users' email address
No
offline_access
Maintain access to data you have given it access to
No
openid
Sign users in
No
profile
View users' basic profile
No
AccessReview
Acronym
AdministrativeUnit
Add permissions
Discard

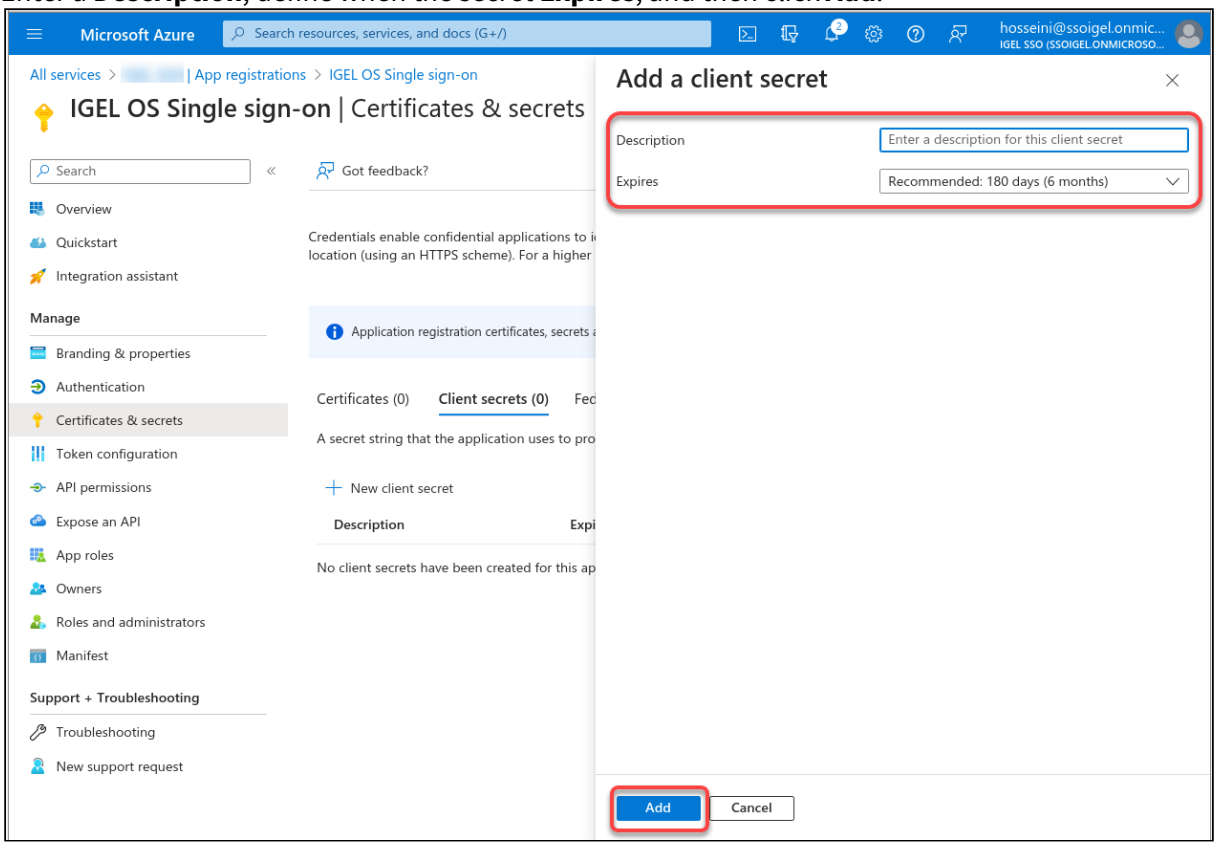
8. Check if the permissions are correct.



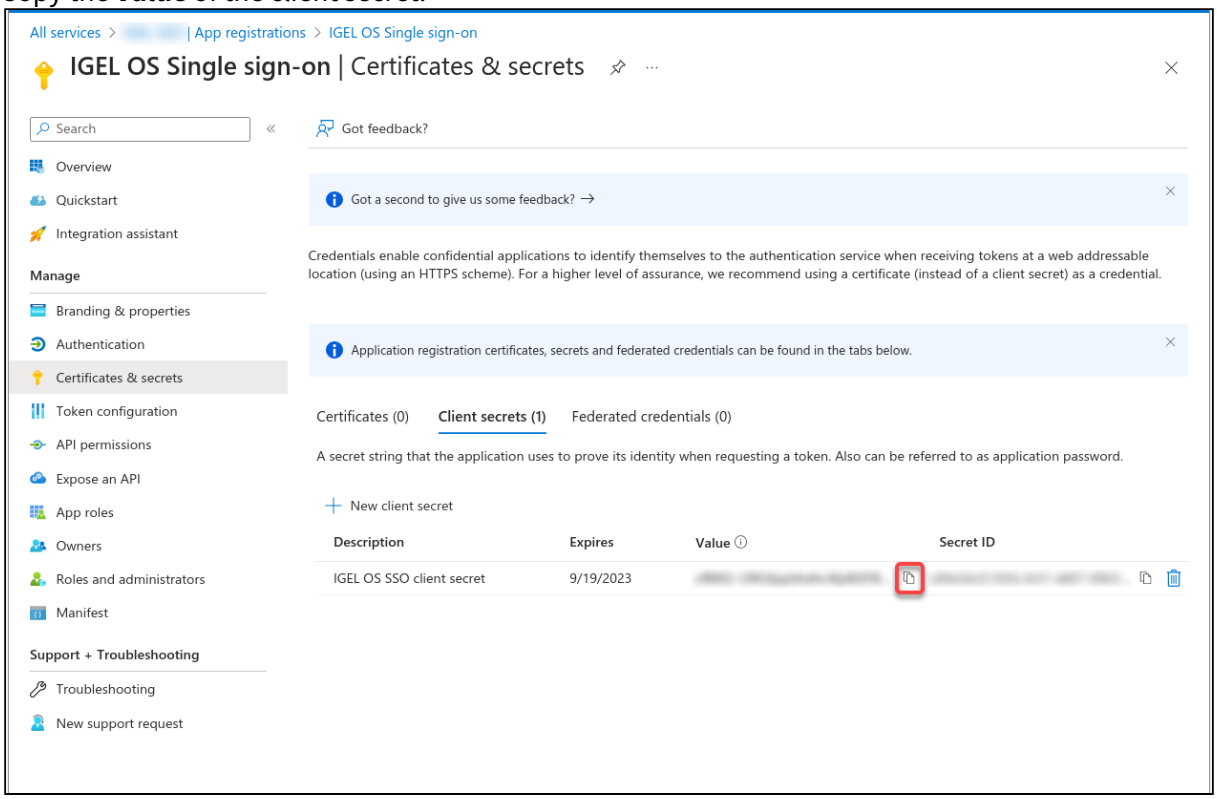
9. Go to **Certificates & secrets** and click **New client secret**.



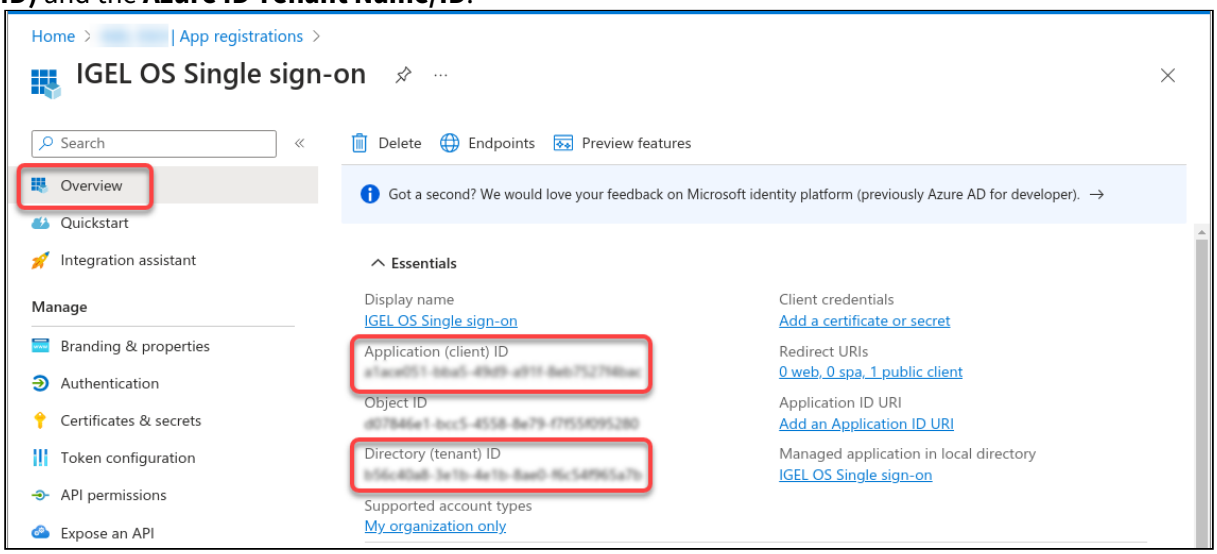
10. Enter a **Description**, define when the secret **Expires**, and then click **Add**.



11. Copy the **Value** of the client secret.

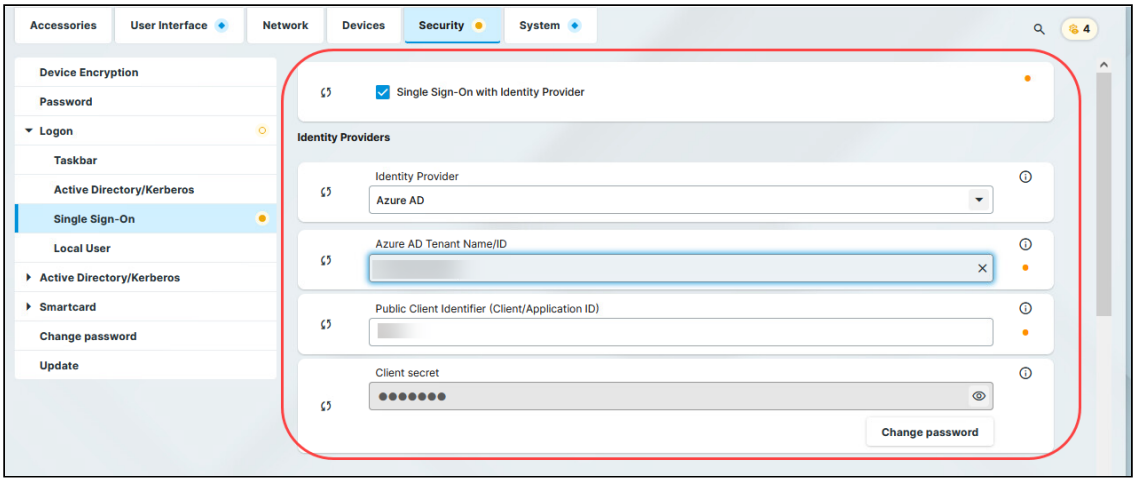


12. Go to **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**. In the IGEL OS configuration, these values will be used as the **Public client identifier (client/application ID)** and the **Azure ID Tenant Name/ID**.



Configuring IGEL OS for SSO with Entra ID

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Azure ID**.
   - Enter the **Azure AD Tenant Name/ID**. This is the value you have obtained as **Directory (tenant) ID** in Azure AD Portal.
   - Set the appropriate **Application (client) ID**. You have obtained this value as **Application (client) ID** in your Azure AD Portal.
   - Enter the **Client secret**.



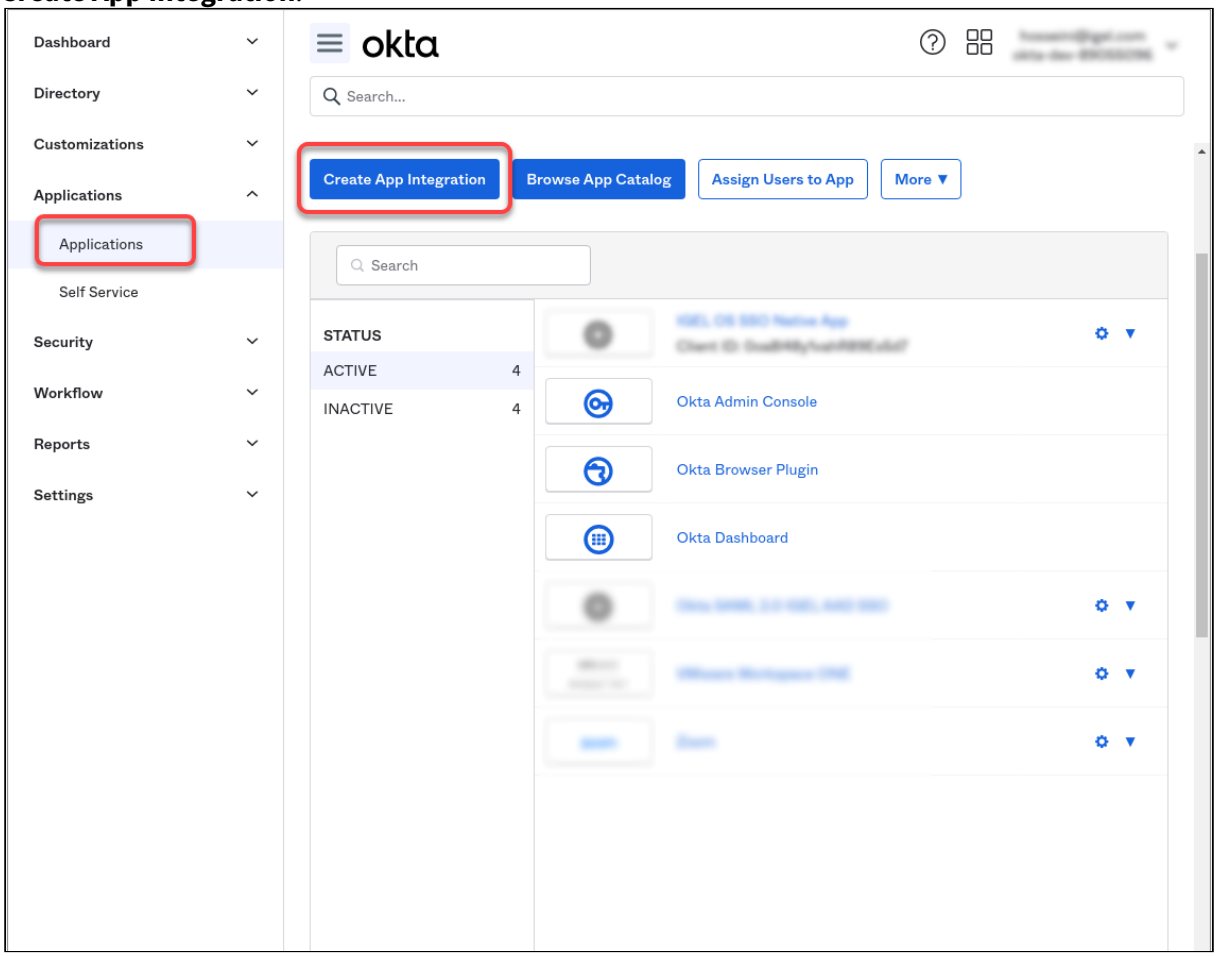
2. If you want to use an automatic desktop login with predefined credentials that are stored securely on your endpoint device:
   - Enable **Automatically perform login**.
   - Under **Username for autologin**, enter a user's name known to your IdP.
   - Under **Password for autologin**, enter the enter the corresponding password.

3. Click **Save** or **Save and close**.
   The desktop of the device is terminated. The login screen is displayed.
   You can now use the apps and utilities for IGEL OS 12 that support SSO with Entra AD (see page 457).
   For details on importing apps from the IGEL App Portal and installing them on IGEL OS devices, see IGEL UMS 12: Basic Configuration and Assignment of Apps and Profiles.
   All methods of multi-factor authentication are available except the hardware token.

Configuring SSO with Okta

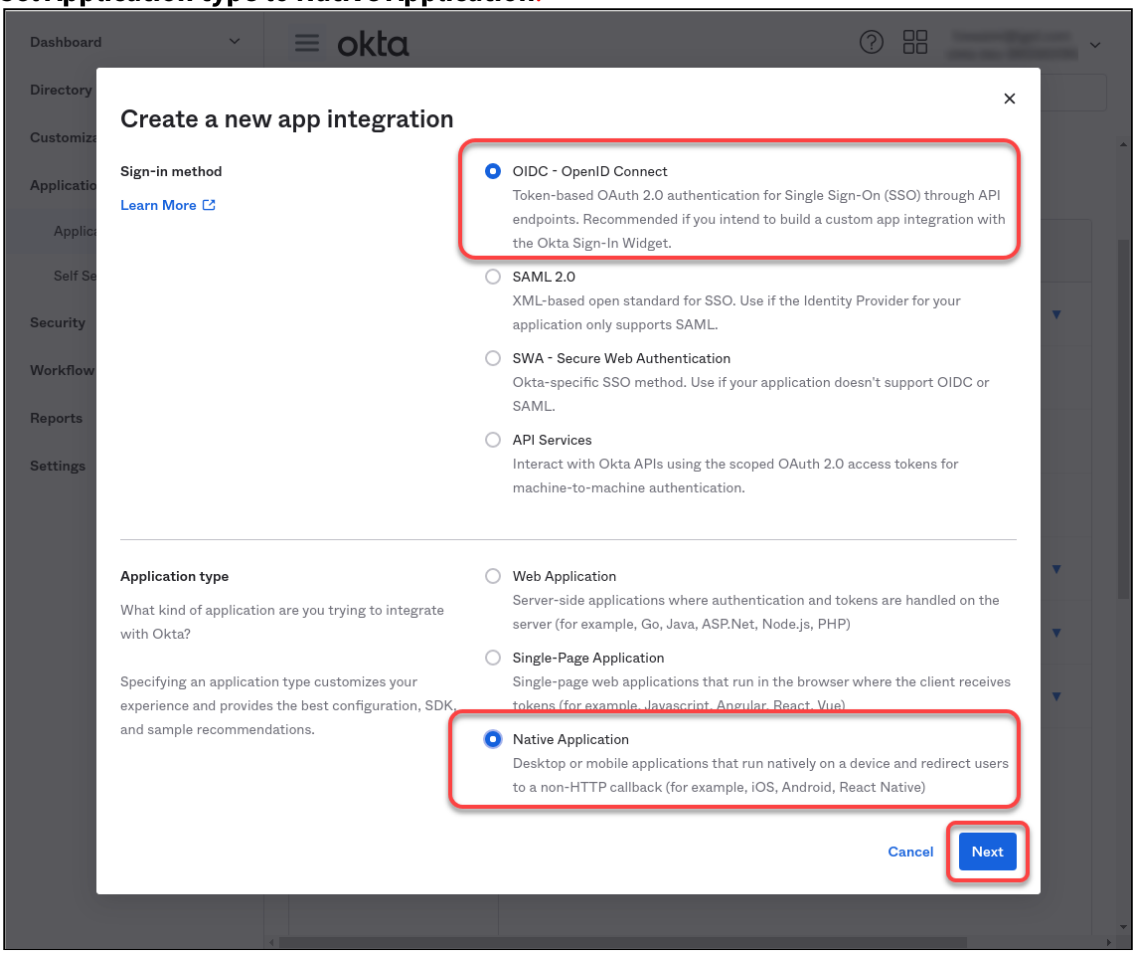
Registering an Application in Okta

1. Log in to Okta with your admin account, and from the **Applications** menu, select **Applications > Create App Integration**.



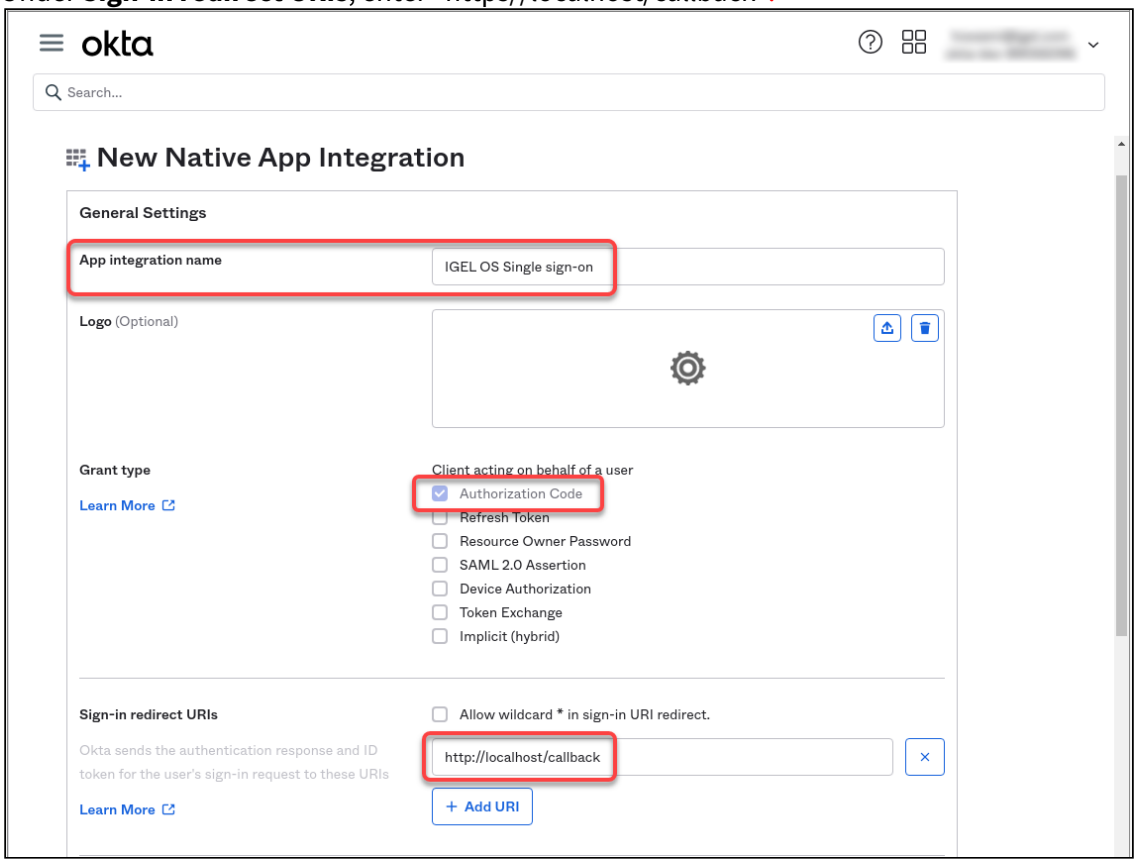
2. Edit the settings as follows and then click **Next**.
   - Set **Sign-in method** to **OIDC - OpenID Connect**.

- Set **Application type** to **Native Application**.



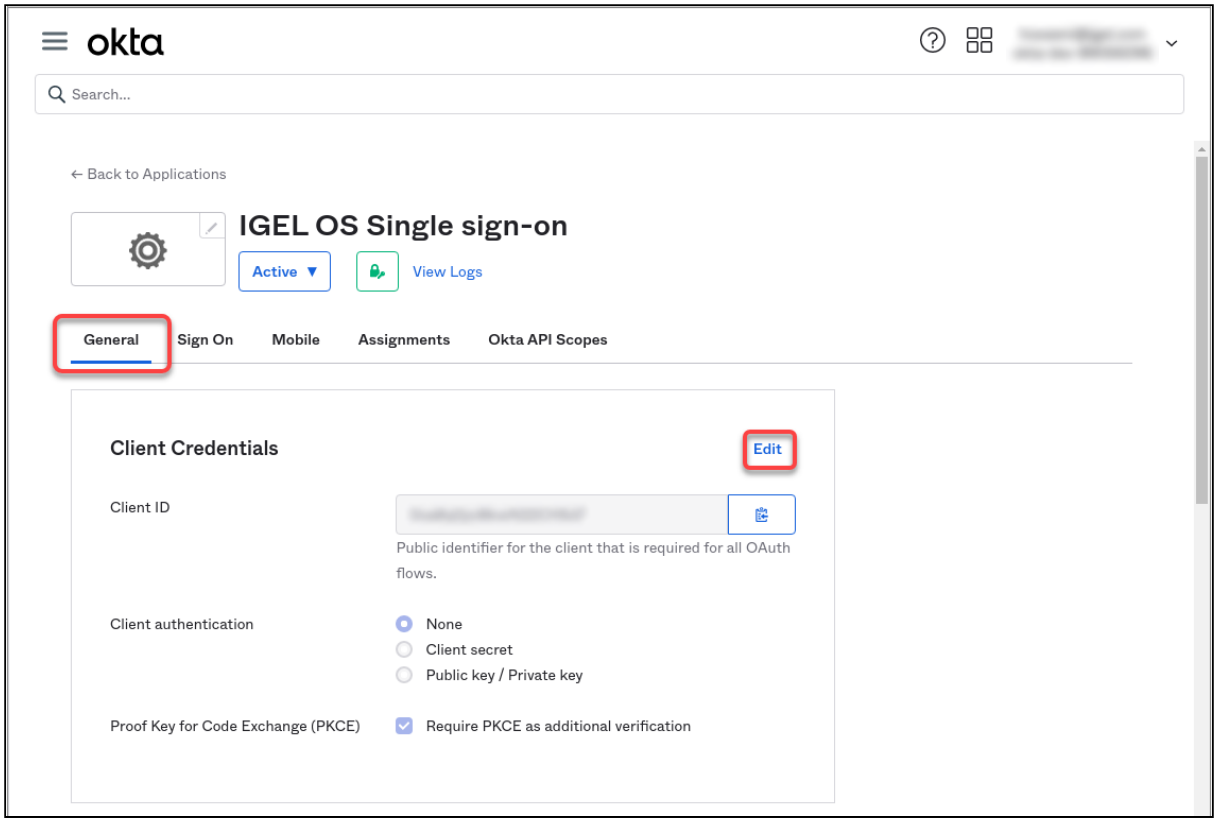
3. Edit the settings as follows and then click **Save**.
   - Under **App integration name**, enter a name for your application, e.g. "IGEL OS Single sign-on".
   - Make sure that as the **Grant type**, the option **Authorization Code** is selected.

- Under **Sign-in redirect URIs**, enter "https//localhost/callback".

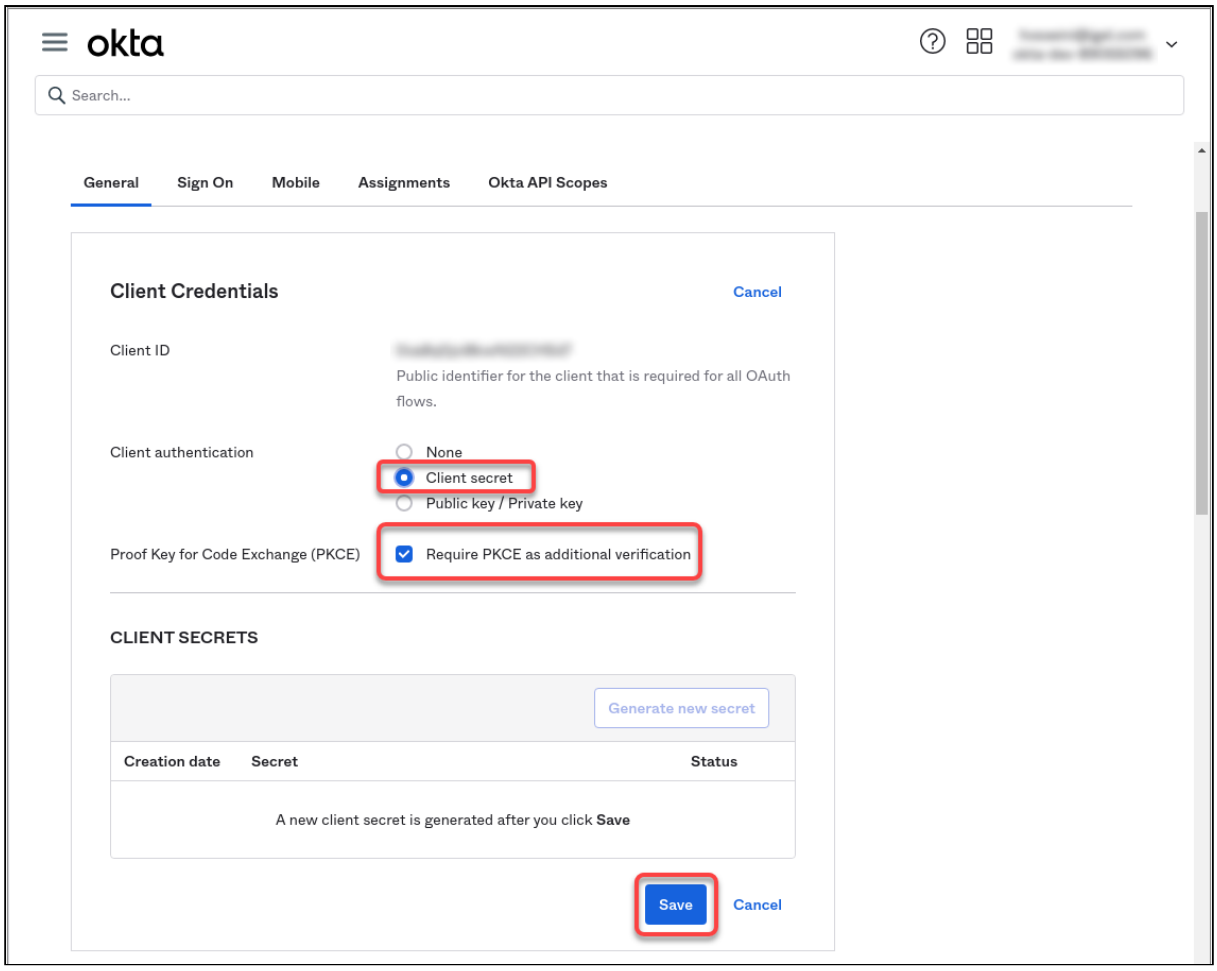


The app integration is created.

4. Select the **General** tab and then click **Edit**.

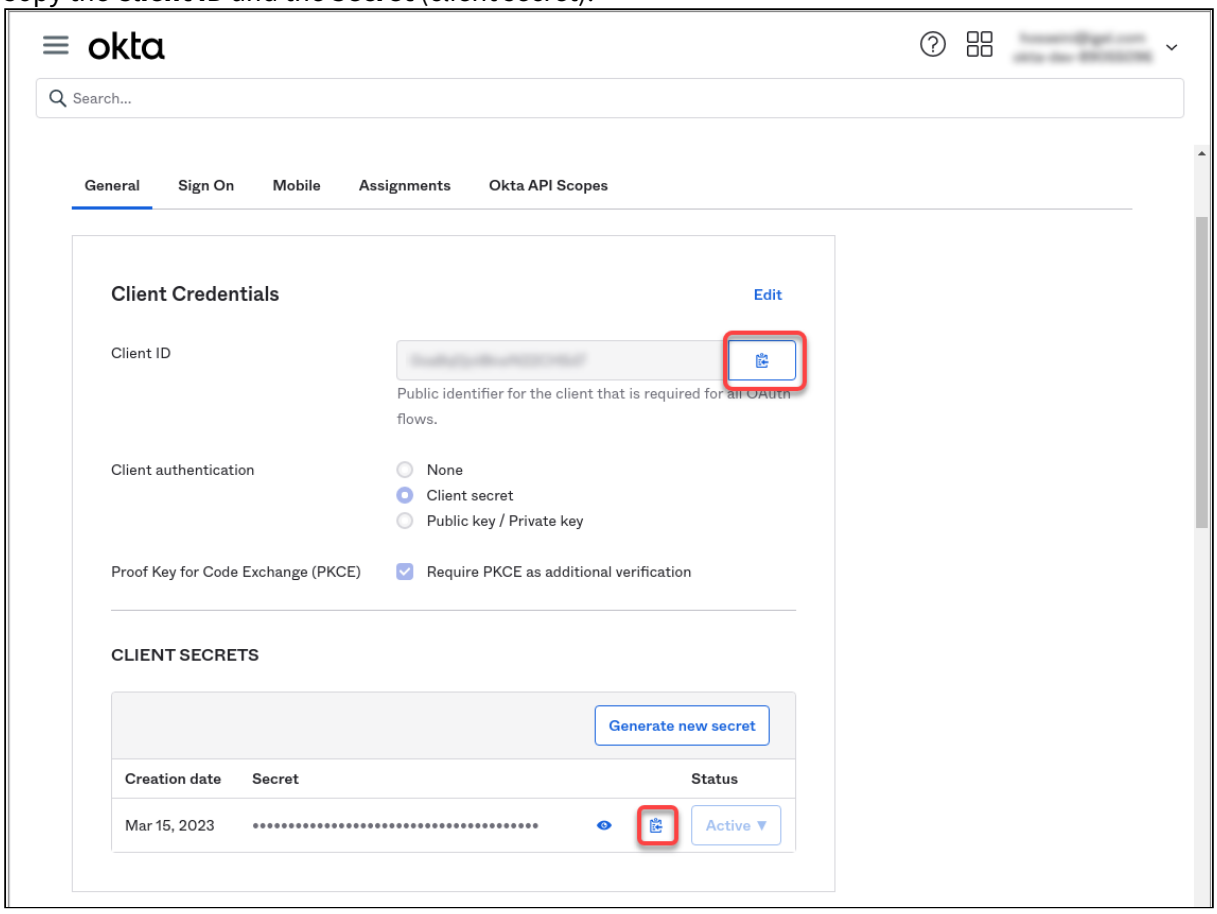


5. Under **Client authentication**, select **Client secret** and make sure that under **Proof Key for Code Exchange (PKCE)**, **Require PKCE as additional verification** is enabled. Afterward, click **Save**.



The client secret will be created.

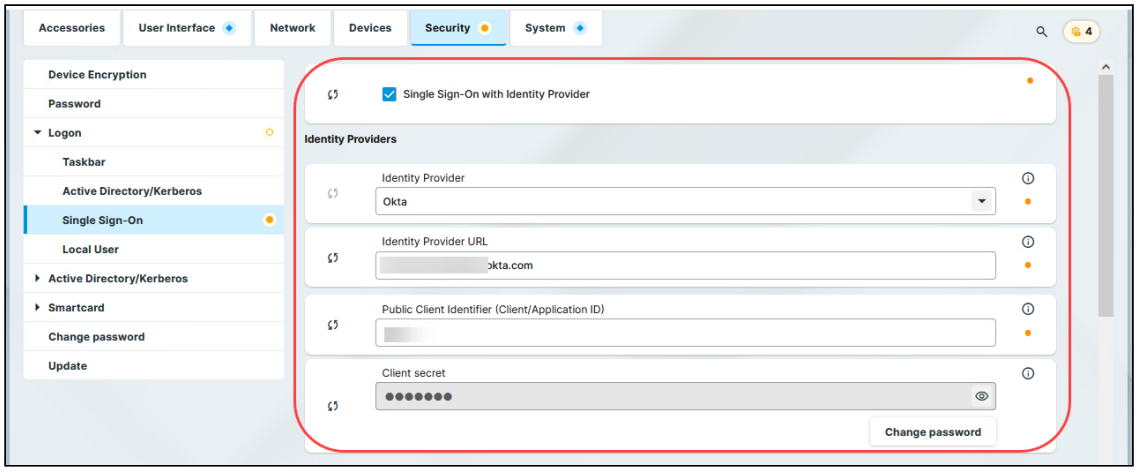
6. Copy the **Client ID** and the **Secret** (client secret).



Configuring IGEL OS for SSO with Okta

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Okta**.
   - Provide the **Okta URL** for your user. This is the Okta organization URL. Example: "https://mycompany.okta.com/"
   - Provide the **Client ID**. This is the client ID that was created in Okta.

- Provide the **Client secret**.

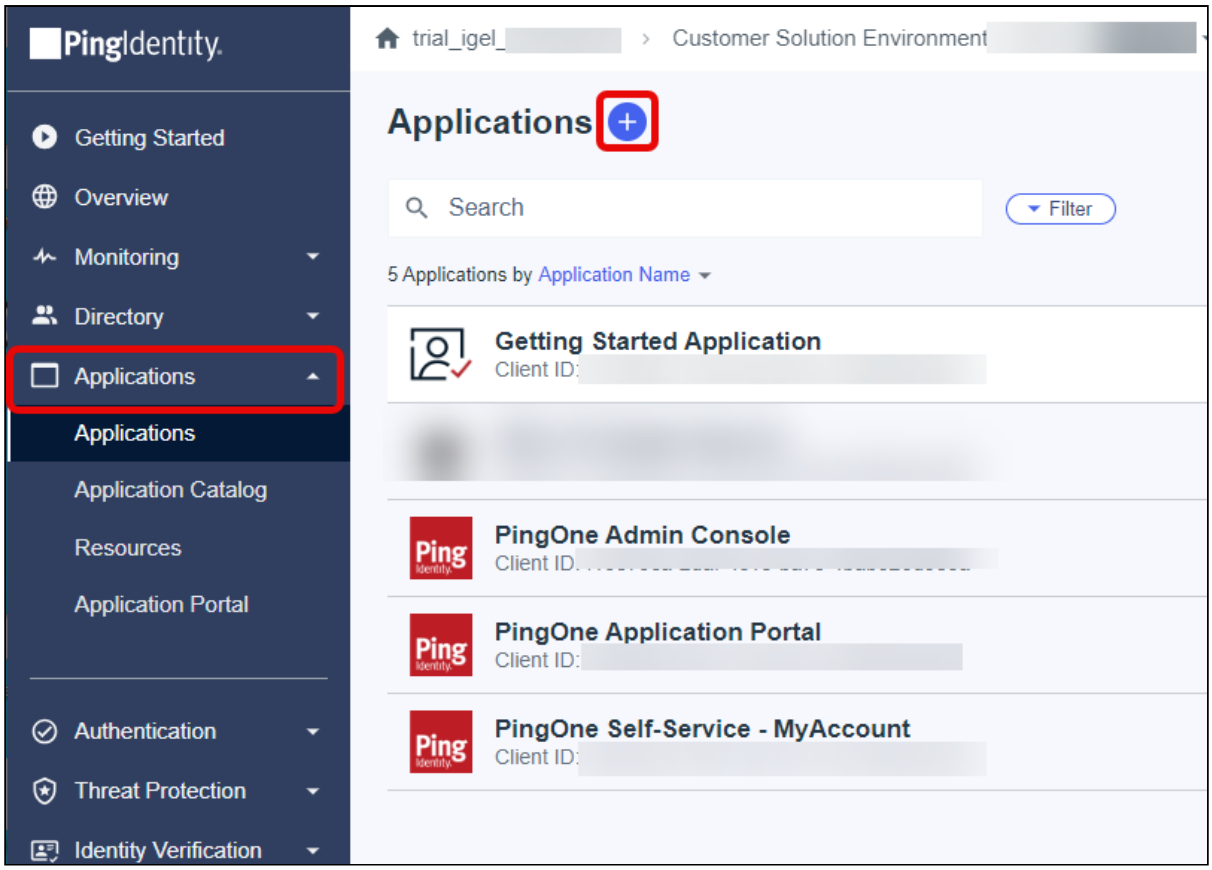


2. If you want to use an automatic desktop login with predefined credentials that are stored securely on your endpoint device:
   - Enable **Automatically perform login**.
   - Under **Username for autologin**, enter a user's name known to your IdP.
   - Under **Password for autologin**, enter the enter the corresponding password.
3. Click **Save** or **Save and close**.
   The desktop of the device is terminated after the profile is applied. The login screen is displayed.
   You can now use the apps and utilities for IGEL OS 12 that support SSO with Okta (see page 457).
   If you want to use multi-factor authentication, you can configure this in the Okta console. The available methods are Google Authenticator, E-Mail, and Okta Verify.

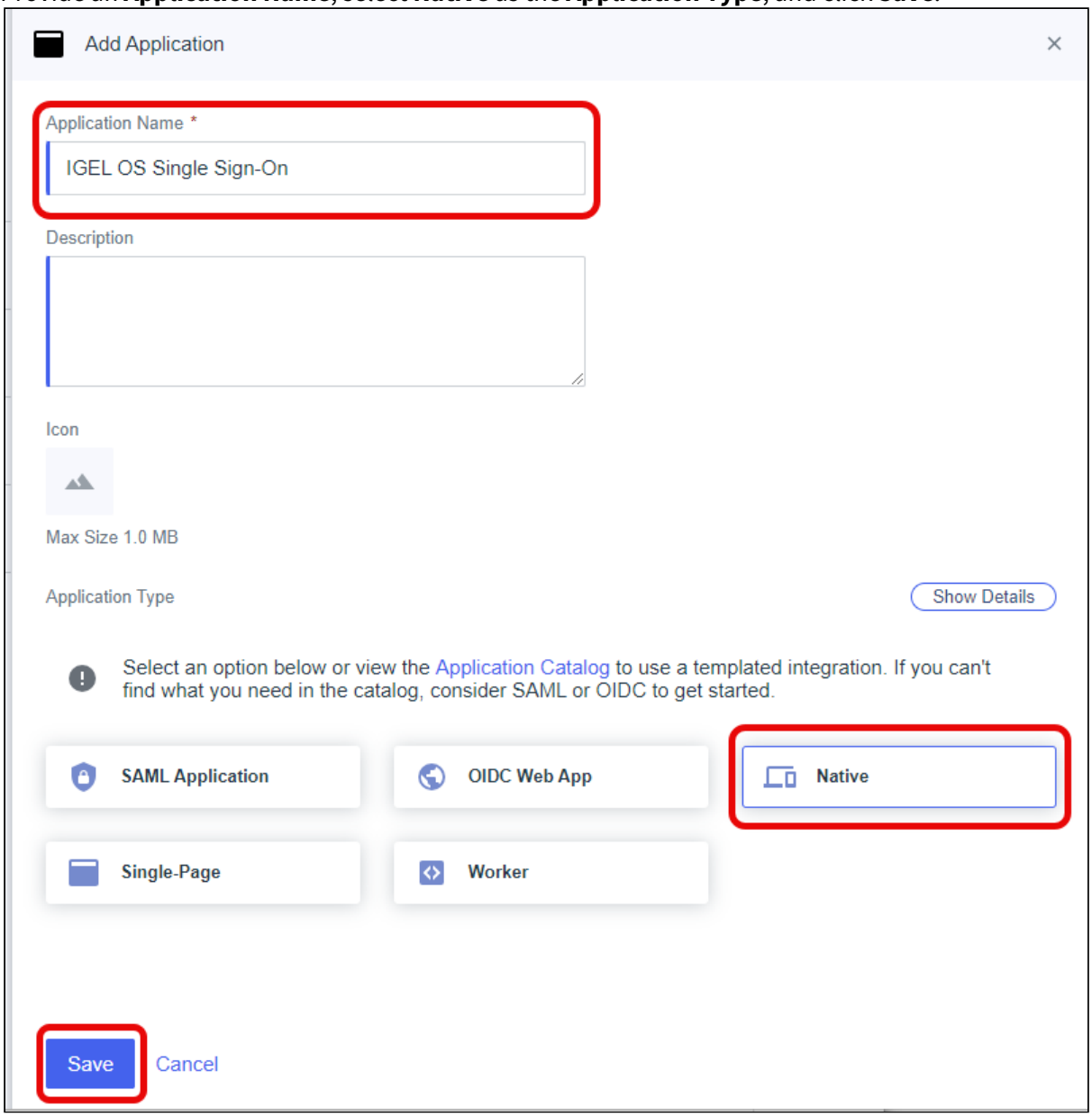
Setting up SSO with Ping Identity / PingOne

Setting up Your Application

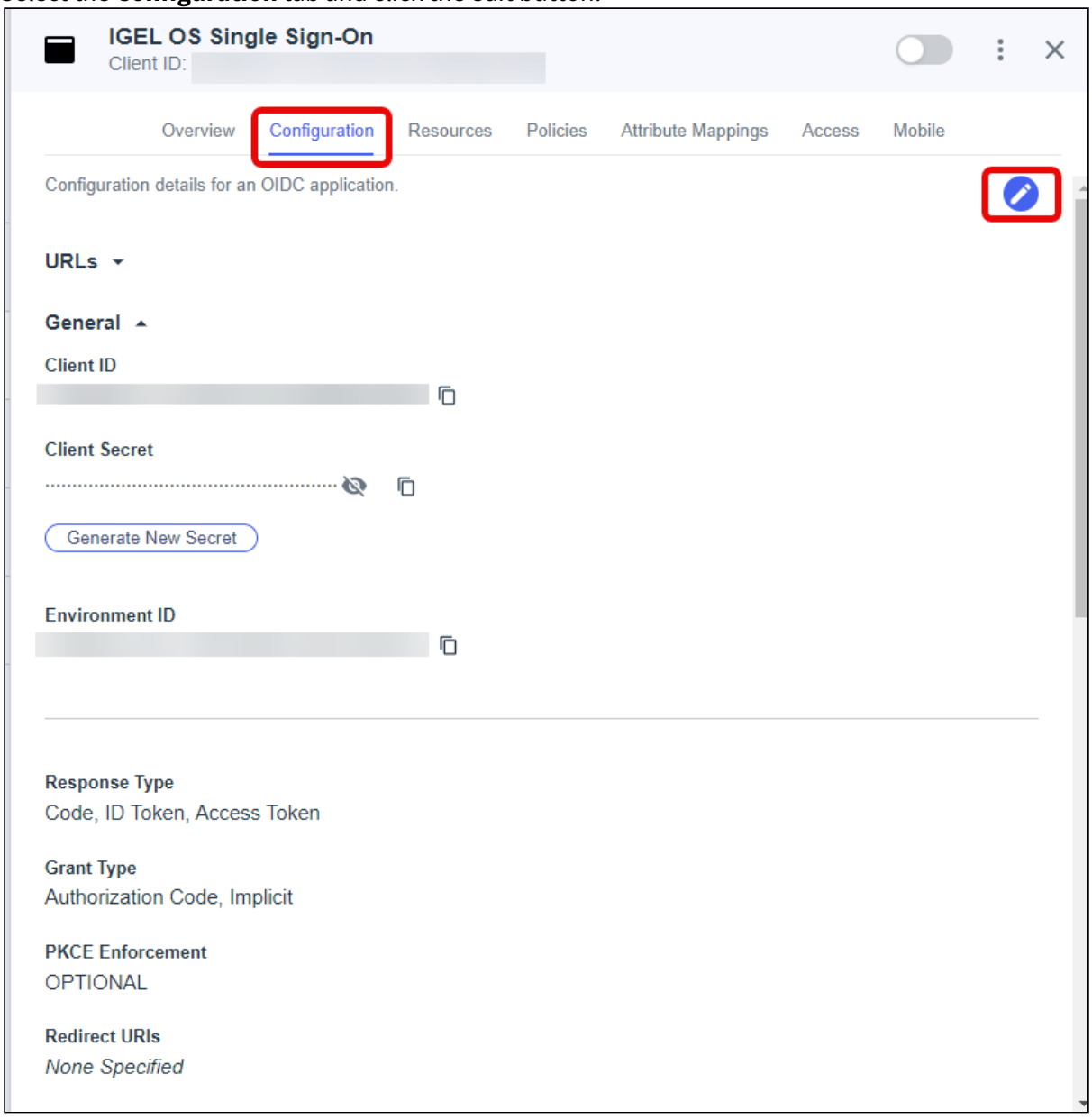
1. Log in to your PingIdentity account, go to **Applications**, and click the add symbol to create a new application.


PingIdentity.
trial_igel_
Customer Solution Environment
Getting Started
Overview
Monitoring
Directory
Applications
Applications
Application Catalog
Resources
Application Portal
Authentication
Threat Protection
Identity Verification
Applications
Search
Filter
5 Applications by Application Name
Getting Started Application
Client ID:
PingOne Admin Console
Client ID:
PingOne Application Portal
Client ID:
PingOne Self-Service - MyAccount
Client ID:

2. Provide an **Application Name**, select **Native** as the **Application Type**, and click **Save**.

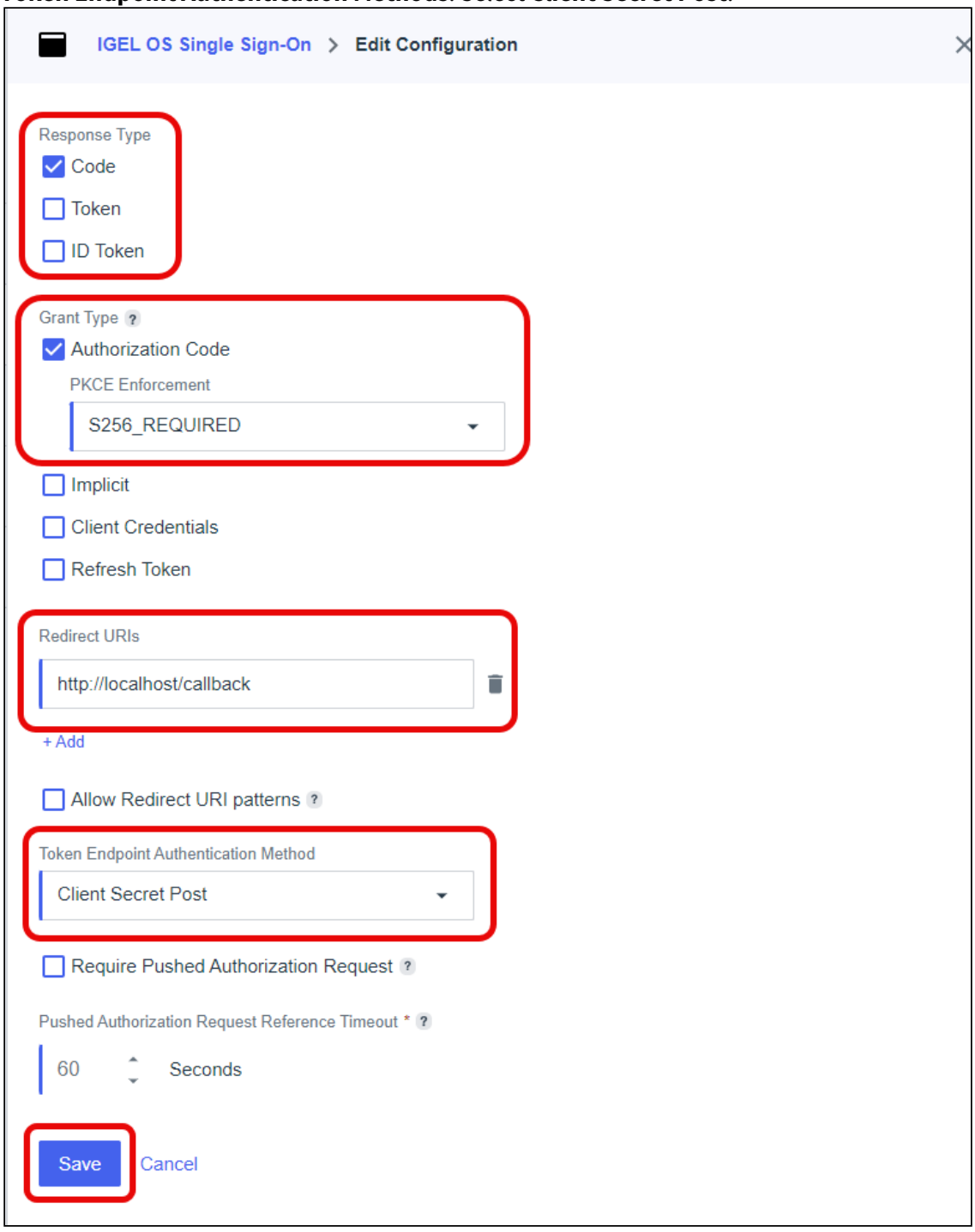


3. Select the **Configuration** tab and click the edit button.

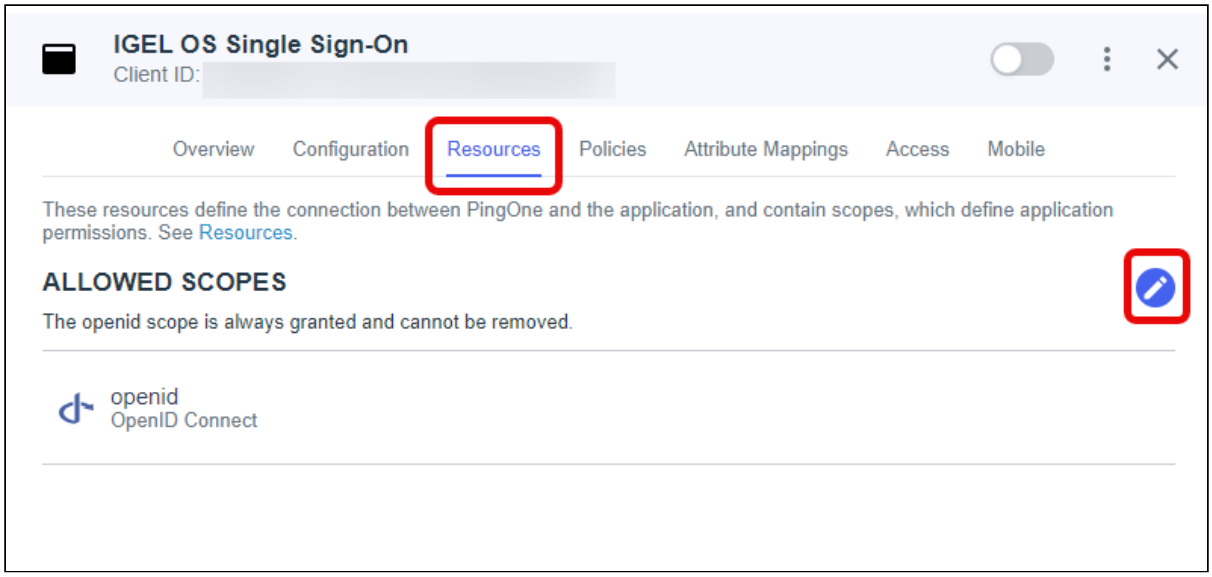


4. Edit the configuration as described below and click **Save**.
   - **Response Type**: Select **Code**.
   - **Grant Type**: Select **Authorization Code** and set **PKCE Enforcement** to **S256_REQUIRED**.
   - **Redirect URIs**: Enter `http://localhost/callback`

- **Token Endpoint Authentication Methods**: Select **Client Secret Post**.

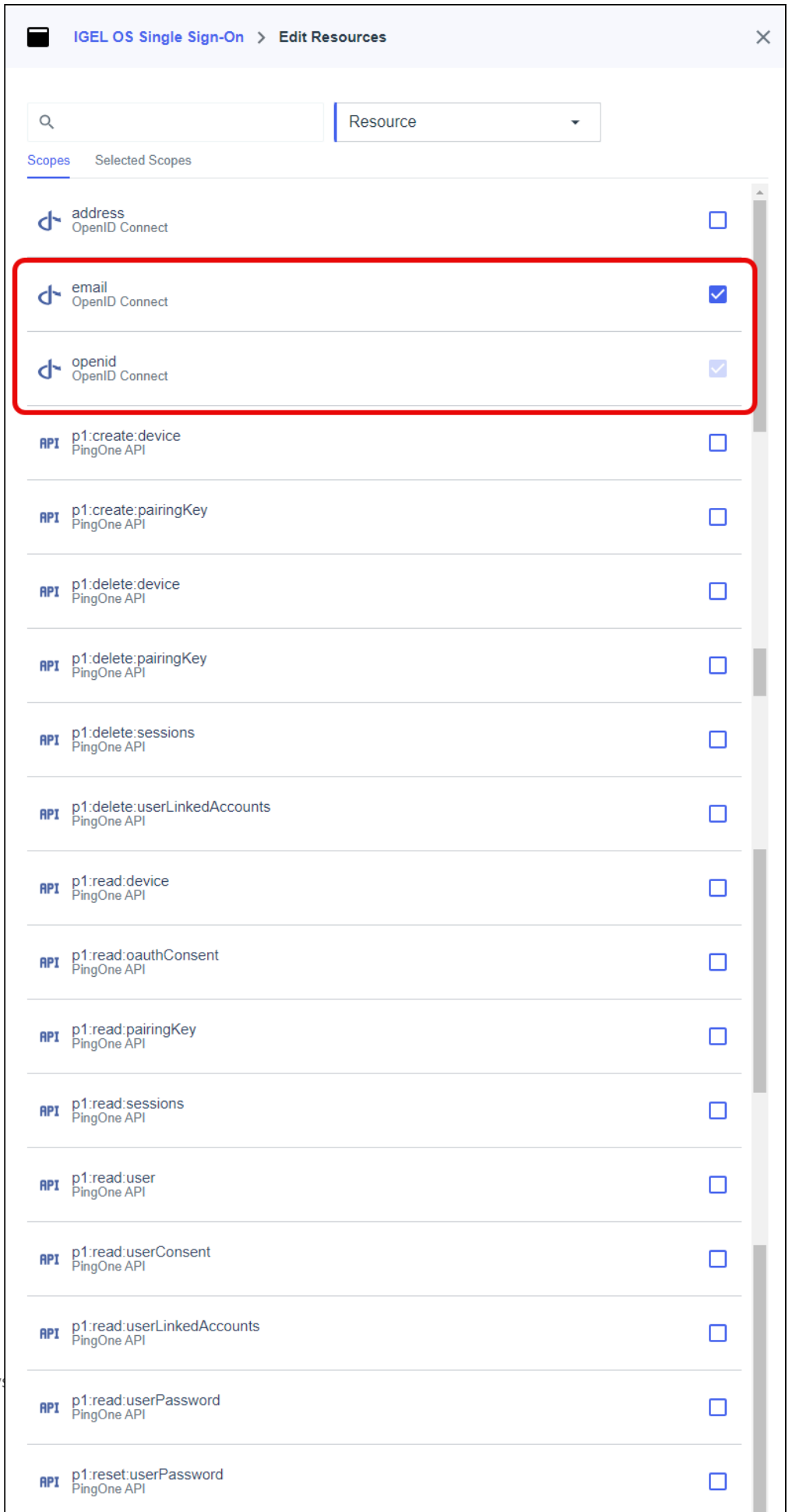


5. Select the **Resources** tab and click the edit button.

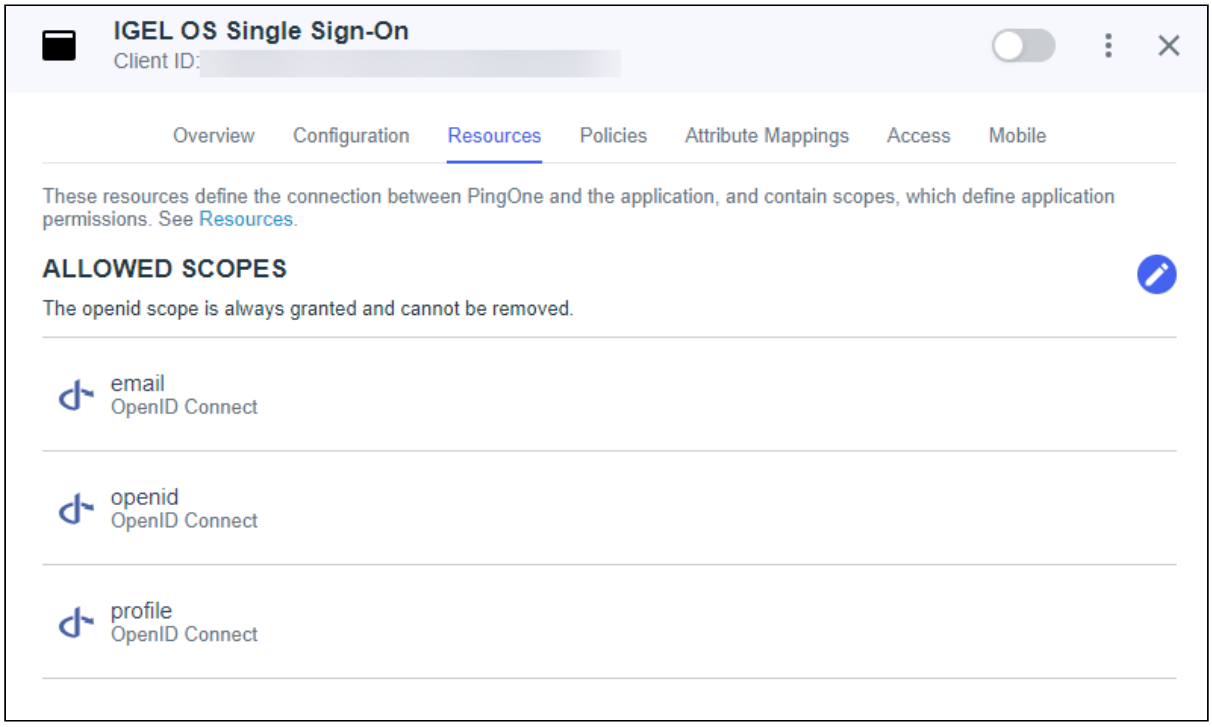


6. Ensure that the following resource scopes are activated and click **Save**.
   - **email**
   - **openid**

- **profile**


IGEL OS Single Sign-On > Edit Resources
Resource
Scopes
Selected Scopes
address
OpenID Connect
email
OpenID Connect
openid
OpenID Connect
p1:create:device
PingOne API
p1:create:pairingKey
PingOne API
p1:delete:device
PingOne API
p1:delete:pairingKey
PingOne API
p1:delete:sessions
PingOne API
p1:delete:userLinkedAccounts
PingOne API
p1:read:device
PingOne API
p1:read:oauthConsent
PingOne API
p1:read:pairingKey
PingOne API
p1:read:sessions
PingOne API
p1:read:user
PingOne API
p1:read:userConsent
PingOne API
p1:read:userLinkedAccounts
PingOne API
p1:read:userPassword
PingOne API
p1:reset:userPassword
PingOne API

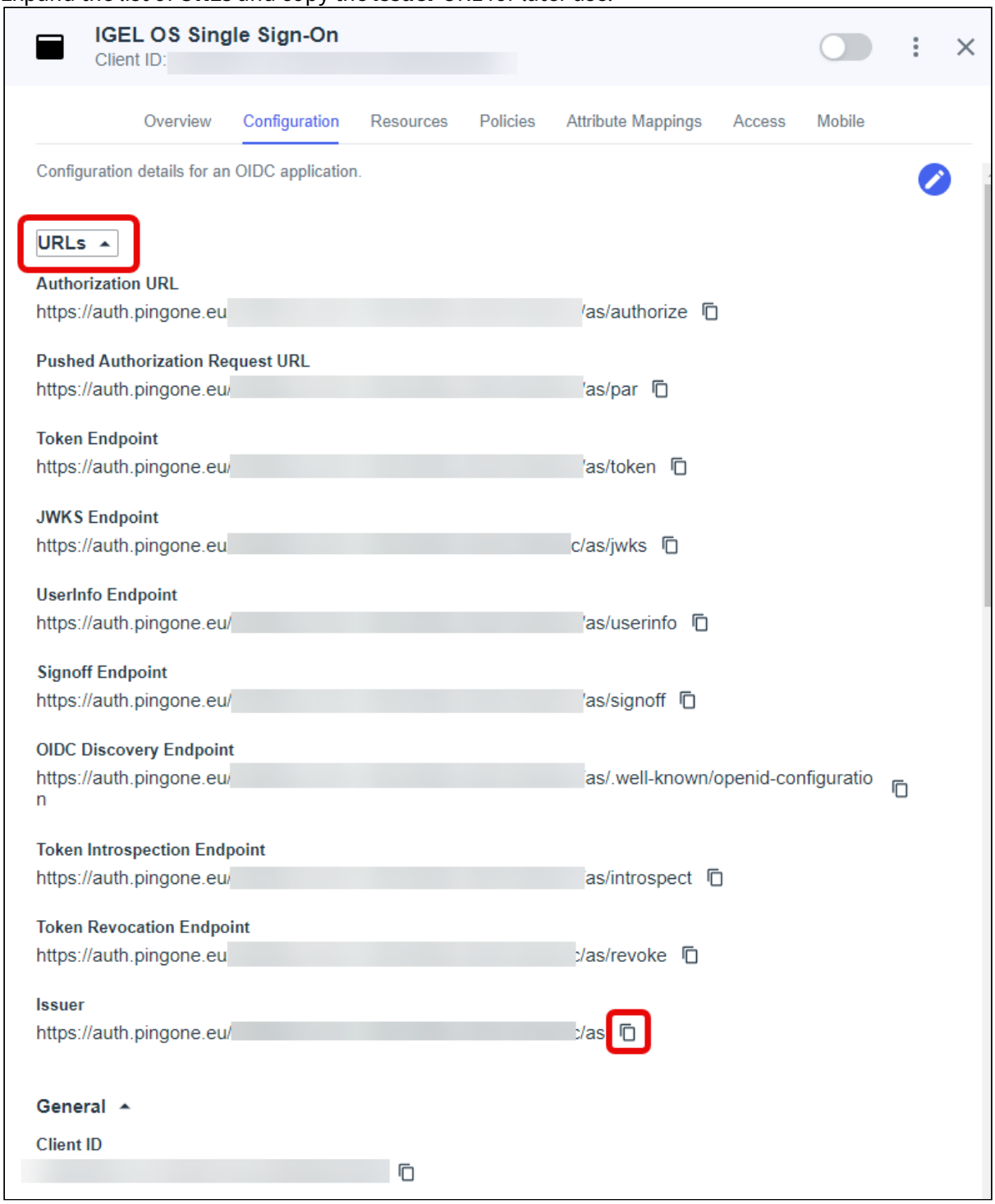
7. Review the list of **ALLOWED SCOPES**.



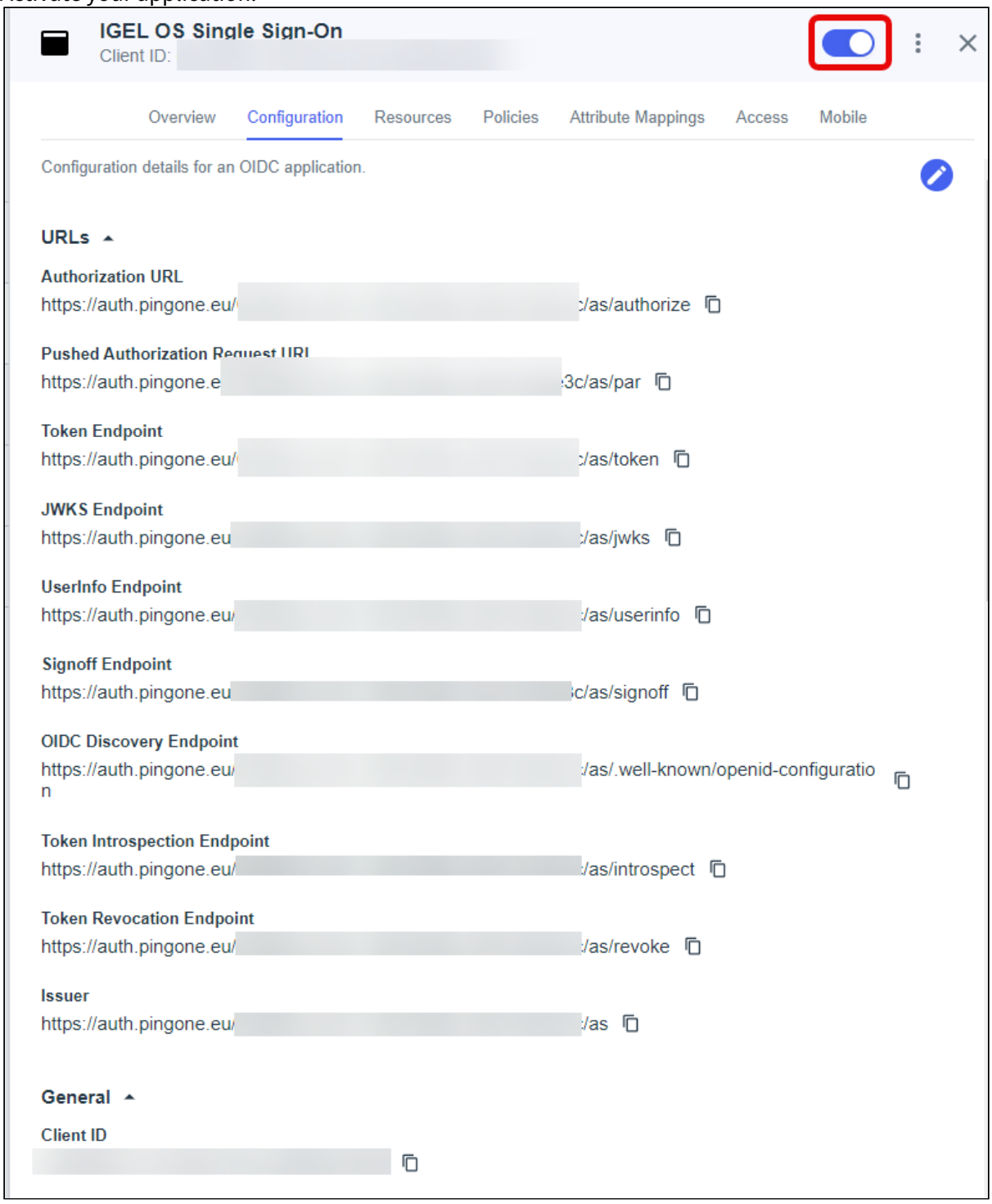
8. Select the Configuration tab and copy the following data for later use:
   - **Client ID**

- **Client Secret**

9. Expand the list of **URLs** and copy the **Issuer** URL for later use.

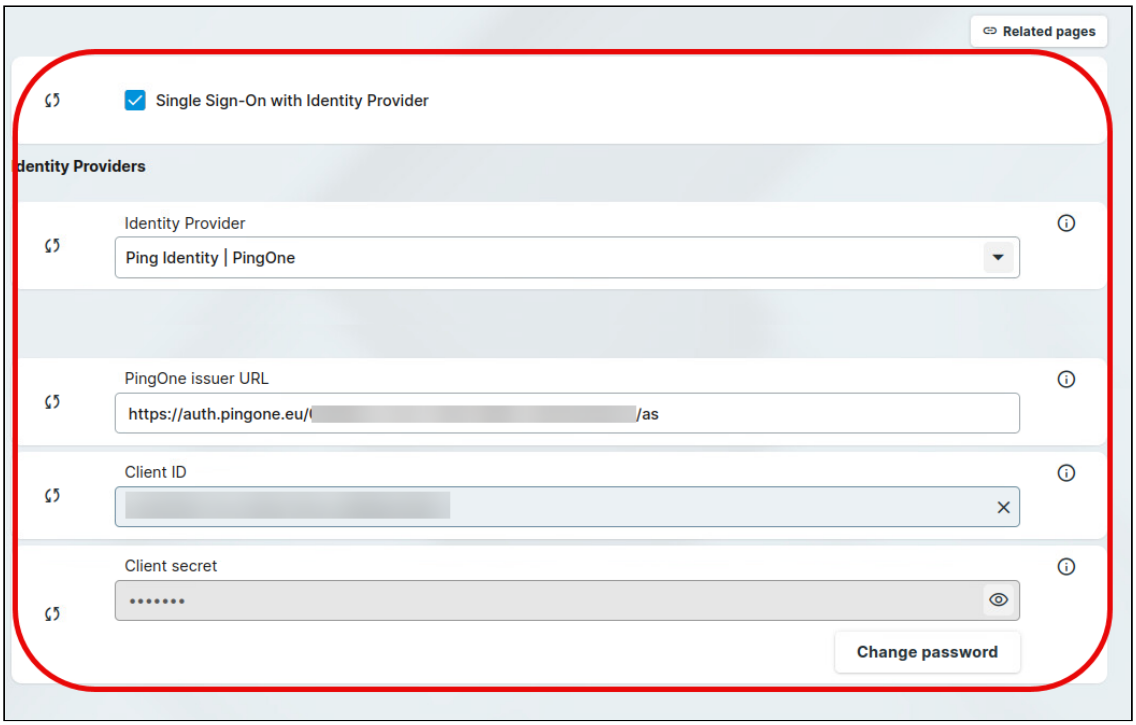


10. Activate your application.



Configuring IGEL OS for SSO with Ping Identity / PingOne

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Ping Identity | PingOne**.
   - Provide the **PingOne issuer URL** for your user. This is the **Issuer** URL provided in the Ping Identity configuration portal. Example: `https://auth.pingone.eu/0815abc-xyz123456/as`
   - Provide the **Client ID**. This is the client ID that was created in Ping Identity.
   - Provide the **Client secret**.

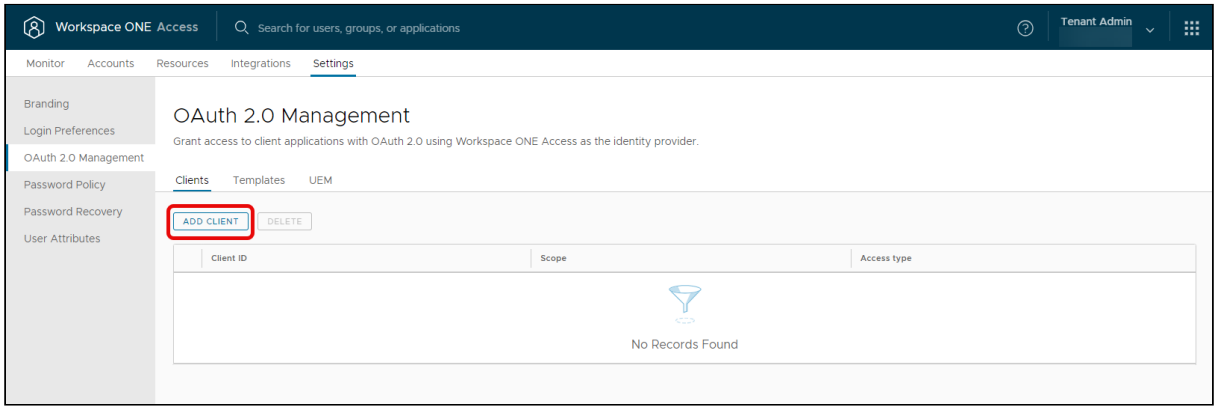


2. If you want to use an automatic desktop login with predefined credentials that are stored securely on your endpoint device:
   - Enable **Automatically perform login**.
   - Under **Username for autologin**, enter a user's name known to your IdP.
   - Under **Password for autologin**, enter the enter the corresponding password.
3. Click **Save** or **Save and close**.
   The desktop of the device is terminated after the profile is applied. The login screen is displayed. You can now use the apps and utilities for IGEL OS 12 that support SSO with Ping Identity / PingOne (see page 458).
   If you want to use multi-factor authentication, you can configure this in the Ping Identity console.

Setting up SSO with VMware Workspace ONE Access

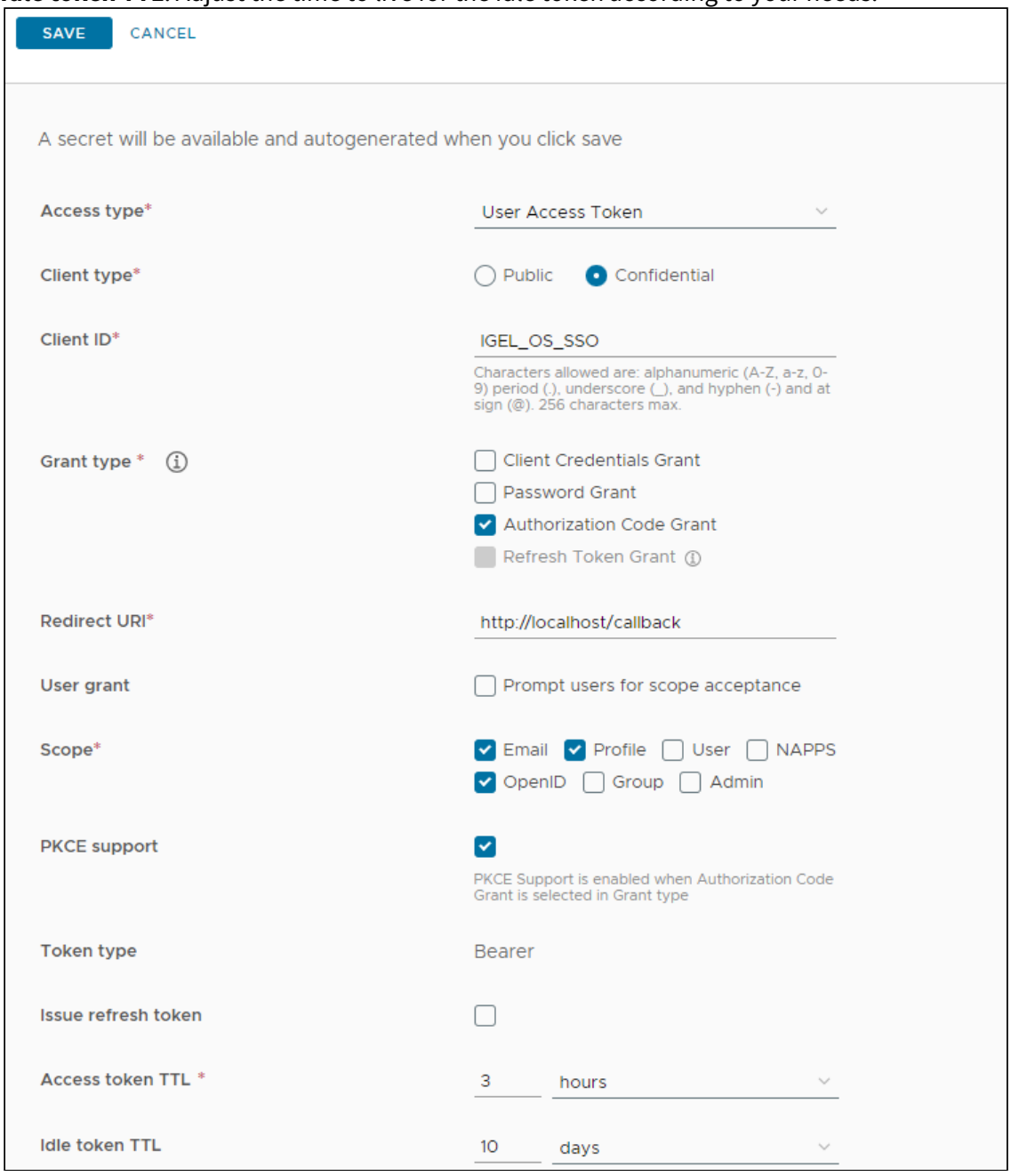
Registering an Application in VMware Workspace ONE Access

1. In the VMware Workspace ONE Access console, go to **Settings > OAuth 2.0 Management** and click **Add client**.



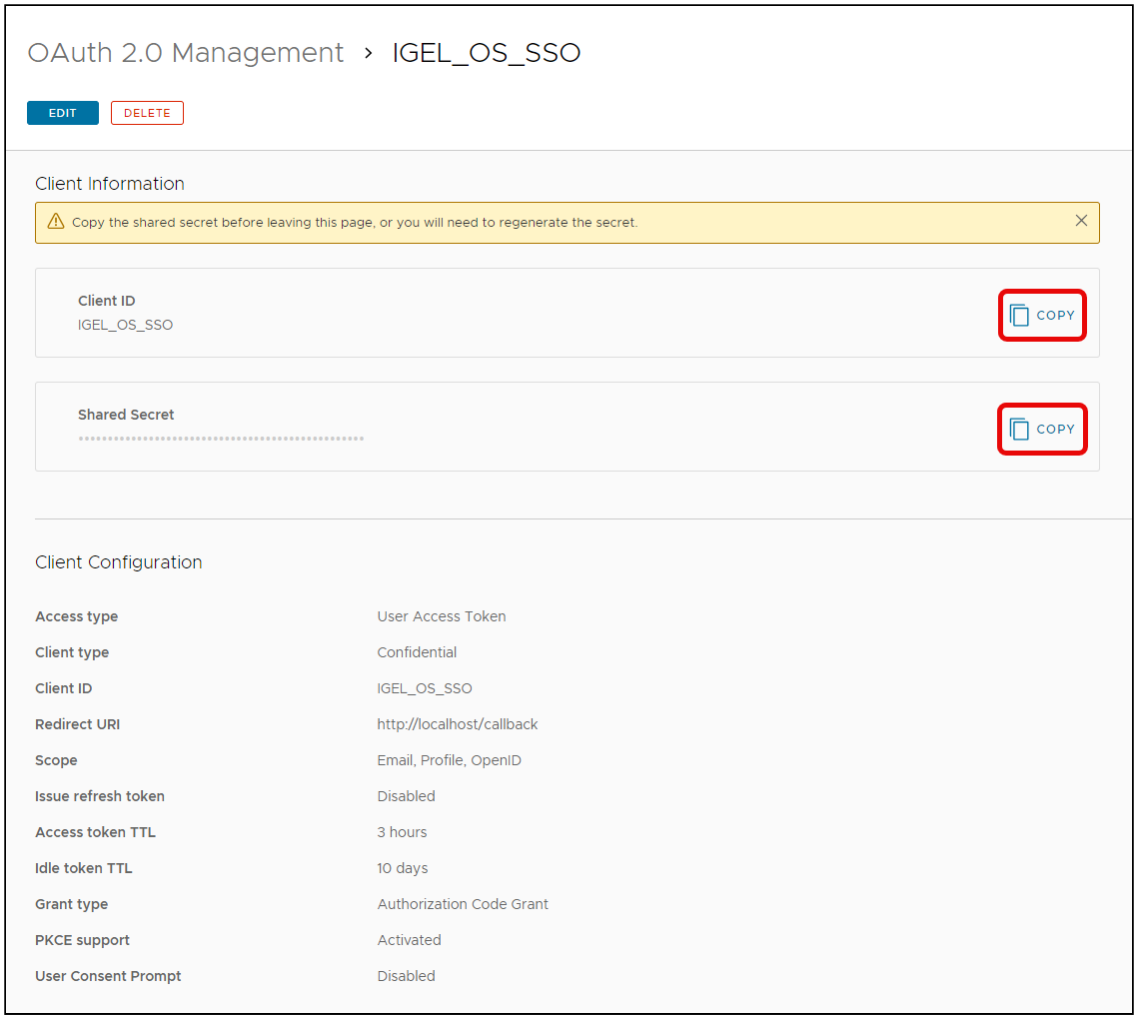
2. Set up the client as follows and finally click **Save**.
   - **Access type**: Select **User Access Token**.
   - **Client type**: Select **Confidential**.
   - **Client ID**: Enter a client ID that suits your needs; respect the allowed characters.
     Example: `IGEL_OS_SSO`
   - **Grant type**: Enable **Authorization Code Grant**.
   - **Redirect URI**: Enter `http://localhost/callback`
   - **User grant**: Disable **Prompt users for scope acceptance**.
   - Scope: Edit the settings as follows:
     - **Email**: Enabled
     - **Profile**: Enabled
     - **User**: Disabled
     - **NAPPS**: Disabled
     - **OpenID**: Enabled
     - **Group**: Disabled
     - **Admin**: Disabled
   - **PKCE support**: This option is enabled because **Authorization Code Grant** is selected as the **Grant type**.
   - **Issue refresh token**: Enable or disable this option according to your needs.
   - **Access token TTL**: Adjust the time to live for the authorization token according to your needs.

- **Idle token TTL**: Adjust the time to live for the idle token according to your needs.



3. Review the settings and copy the following data for later use:
   - **Client ID**

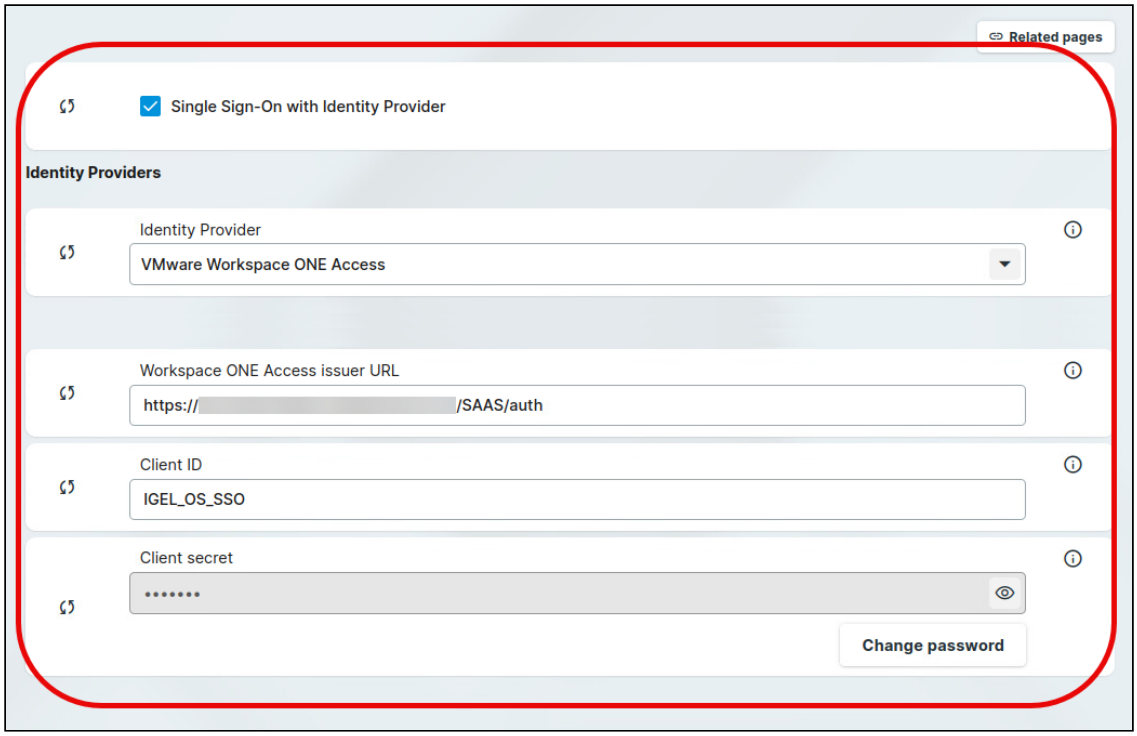
- **Shared Secret**



Configuring IGEL OS for SSO with VMware Workspace ONE Access

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **VMware Workspace ONE Access**.
   - Provide the **Workspace ONE Access issuer URL** for your user. Pattern: `https://<YOUR WORKSPACE ONE ACCESS URL>/SAAS/auth`
   - Provide the **Client ID**. This is the client ID that was created in VMware Workspace ONE Access.

- Provide the **Client secret**.



2. If you want to use an automatic desktop login with predefined credentials that are stored securely on your endpoint device:
   - Enable **Automatically perform login**.
   - Under **Username for autologin**, enter a user's name known to your IdP.
   - Under **Password for autologin**, enter the enter the corresponding password.
3. Click **Save** or **Save and close**.
   The desktop of the device is terminated after the profile is applied. The login screen is displayed.
   You can now use the apps and utilities for IGEL OS 12 that Support SSO with VMware Workspace ONE Access (see page 458).
   If you want to use multi-factor authentication, you can configure this in the VMware Workspace ONE Access portal.

Configuring SSO with Other IdPs That Use OpenID Connect

For setting up your application or client, the exact procedure depends on the exact OpenID Connect solution you are using. Therefore, the settings in the IdP console can only be described generically.

Setting up Your Application / Client

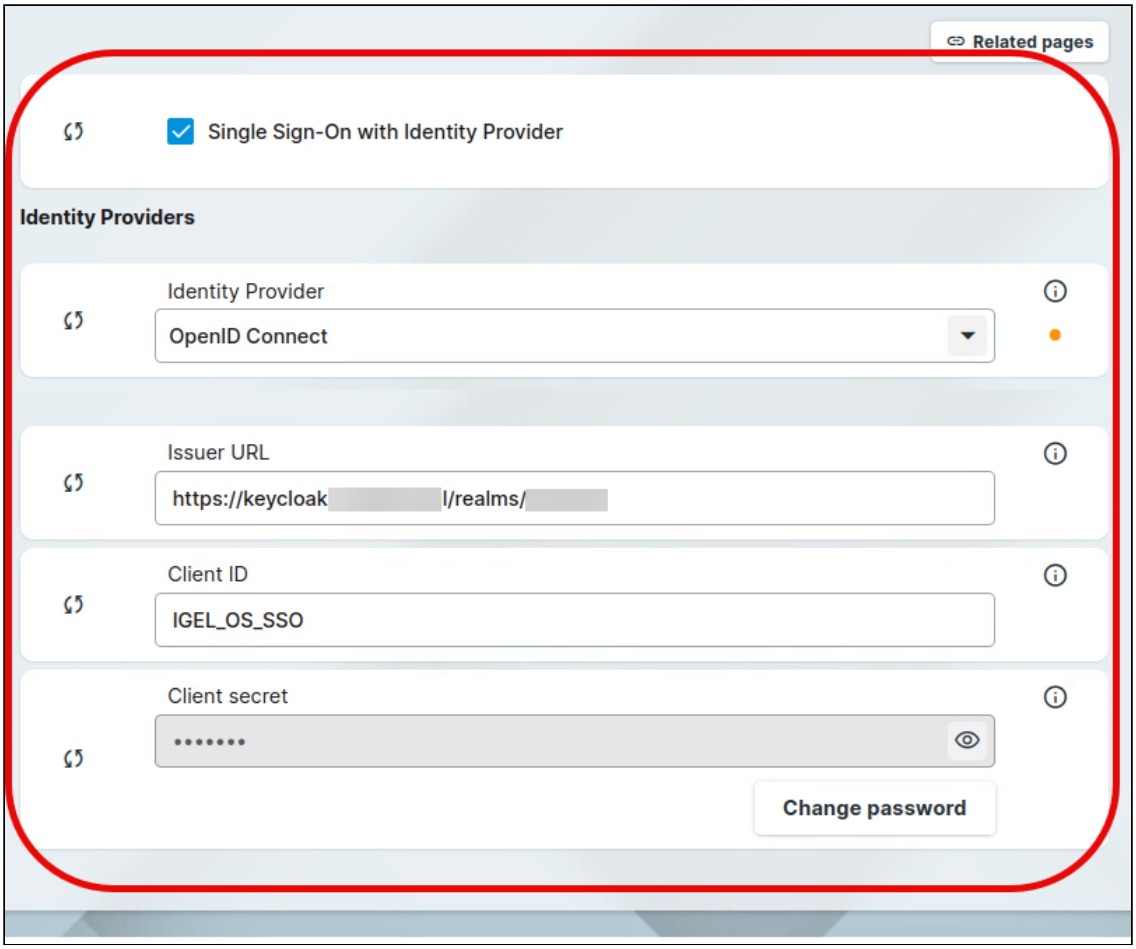
In your IdP console, edit the parameters as follows (the exact parameter names will probably deviate):

Parameter	Values
Response type	code
Scopes	openid, profile, email
Redirect URI	`http://localhost/callback`
Code challenge method	S256
Response mode	fragment
Client authentication	client_secret_post

Configuring IGEL OS for SSO with Generic OpenID Connect

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **OpenID Connect**.
   - Provide the **Issuer URL** for your user. This is the **Issuer** URL provided in the IdP console. Example for Keycloak: `https://keycloak.yourcompany.com/realms/yourrealm`
   - Provide the **Client ID**. This is the client ID that was created in the IdP console.

- Provide the **Client secret**.



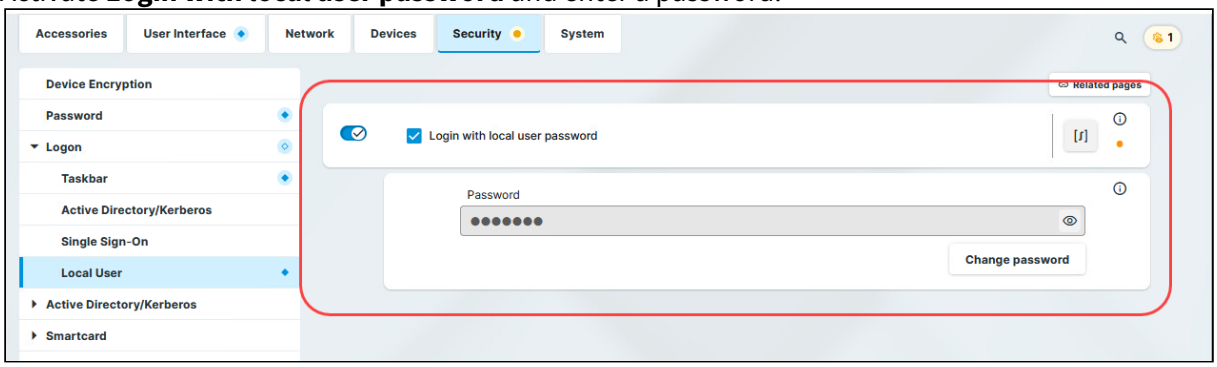
2. Click **Save** or **Save and close**.
   The desktop of the device is terminated. The login screen is displayed.
   You can now use the apps and utilities for IGEL OS 12 that support SSO with OpenID Connect (generic) (see page 458).
   For details on importing apps from the IGEL App Portal and installing them on IGEL OS devices, see IGEL UMS 12: Basic Configuration and Assignment of Apps and Profiles.
   For supported multi-factor authentication methods, check the documentation of your IdP.

Enabling Local Login (Optional)

To have a fallback option if something goes wrong with SSO, e.g. a network failure, it is recommended to configure local login in addition.

1. Open the profile configurator and go to **Security > Logon > Local user**.

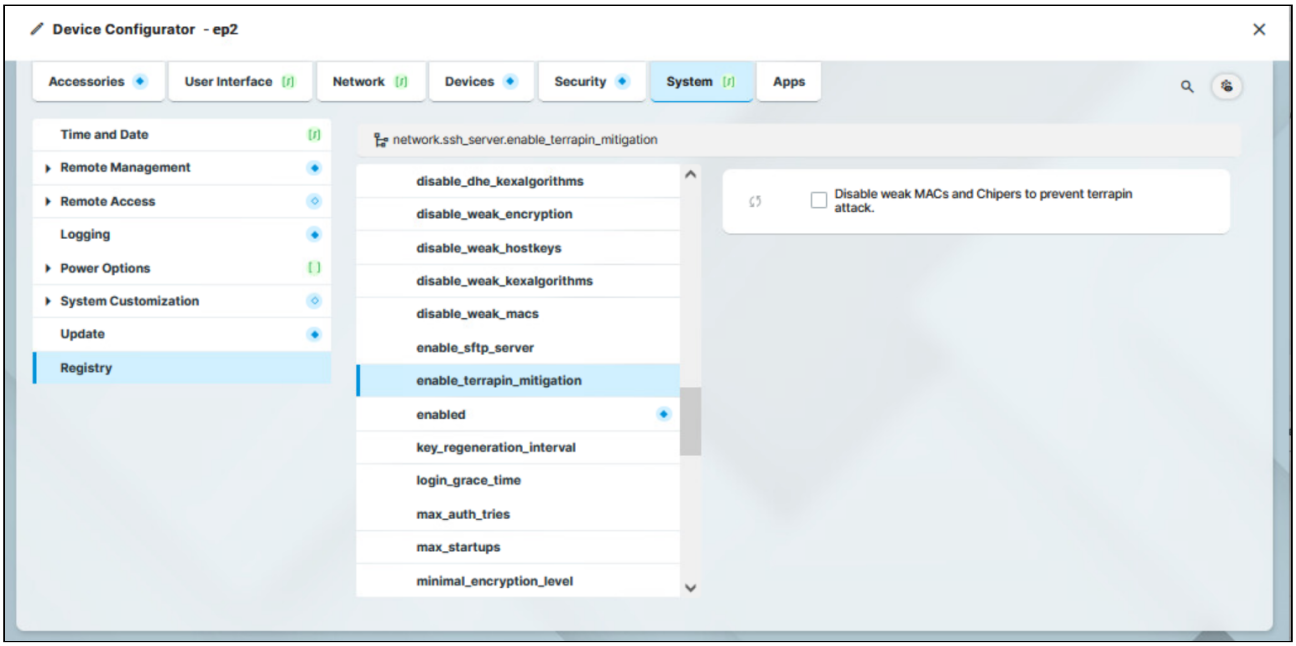
2. Activate **Login with local user password** and enter a password.



How to Mitigate Terrapin Vulnerability through Registry Parameter in IGEL OS

To mitigate ISN 2023-39: SSH Terrapin Vulnerability, you can enable a registry parameter that will disable weak MACs and Chipers to prevent terrapin attacks. For more information on terrapin attacks and the related CVE-2023-48795, see https://terrapin-attack.com/ and https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-48795.

> If you use OpenSSH 9.6p1 both on the client and server there is no need to use this registry parameter. IGEL OS versions 12.3.1 or higher use the latest OpenSSH 9.6p1. When you use this version or newer on the peer, they will automatically use the new "strict KEX" protocol extension.



To enable Terrapin mitigation through the registry parameter:

1. In configuration, go to **System > Registry > network > ssh_server > enable_terrapin_mitigation**.
2. Enable the parameter.
3. Click **Save** or **Save and Close** to save the change.

   The following options vulnerable to Terrapin attack are disabled:

   - the ChaCha20-Poly1305 cipher
   - all -cbc ciphers

- all -ctr ciphers
- all -etm@openssh.com macs