



IGEL OS Base System



- Partner Solutions(see page 3)
- Configuration of IGEL OS 12 Device Settings(see page 5)
- Starting Methods for Apps(see page 373)
- Boot Process(see page 376)
- How to Deploy IGEL OS 12 with PXE(see page 381)
- How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on(see page 392)
- How to Use IGEL OS 12 with UD Pocket(see page 413)
- Facilitated Switching between IdPs for Single-Sign On (SSO) In IGEL OS 12.2(see page 418)
- Upgrading from IGEL OS 11 to IGEL OS 12(see page 422)
- How to Customize the Unit ID Computation for IGEL OS Creator (OSC)(see page 423)
- How to Configure Single Sign-On (SSO) on IGEL OS 12(see page 427)



Partner Solutions

- Poly Headsets Supported by IGEL OS 12(see page 4)



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



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:

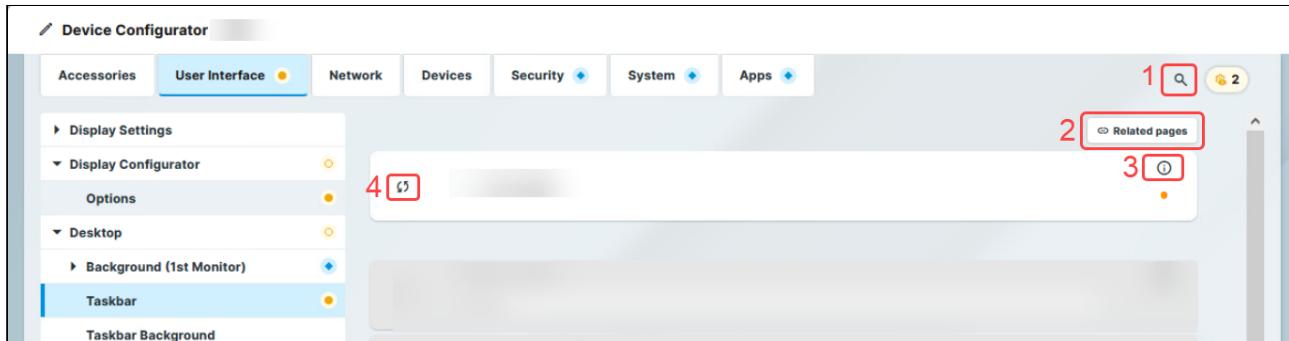
Configuration Method	Description	Opening Options
IGEL Setup	<p>Configurations are made locally on the device.</p> <p>For more information, see IGEL Setup (see page 37).</p>	<ul style="list-style-type: none"> Starting methods defined under Accessories > Setup Keyboard command [Ctrl] + [Alt] + [s] Keyboard command [Ctrl] + [Alt] + [F2] in the Appliance Mode
Device Configurator	<p>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.</p> <p>For more information, see Devices - IGEL UMS Web App.</p>	<ul style="list-style-type: none"> Double clicking on the device name Clicking the Edit Configuration button Selecting Edit Configuration command in the context menu of the device
Profile Configurator	<p>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.</p> <p>For more information, see Configuration - IGEL UMS Web App.</p>	<ul style="list-style-type: none"> 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:





General GUI Elements of the Configurator Dialog



	GUI Element	Description
1	Search for Settings	<p>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.</p> <p>Clicking on a search result displays the configuration page containing the result. The result is highlighted on the page.</p> <p>When a search result is clicked, the search menu remains displayed in the top right corner with the following navigation options:</p> <ul style="list-style-type: none"> • 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.
4	Reset to default	Clicking the icon resets the parameter to the default value.



	GUI Element	Description
		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 **Unused adjustments** and the **All adjustments** tabs. The **Unused 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.

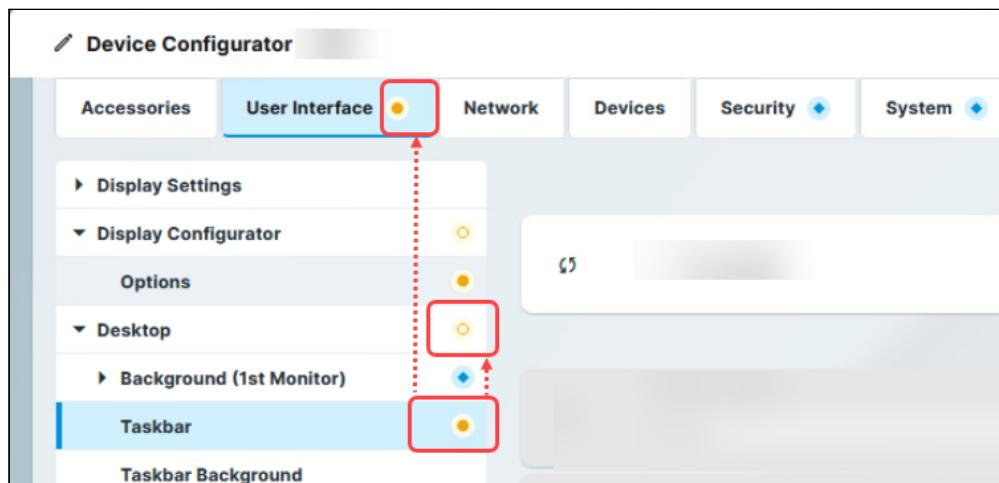
	There is an unsaved change in one of the child pages.
	There is an unsaved change in the page. There is an unsaved change in the tab.
	There is a saved template key change in one of the child pages.
	There is a saved template key change in the page. There is a saved template key change in the tab.



	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 10)
- [User Interface](#)(see page 47)
- [Network](#)(see page 143)
- [Devices](#)(see page 229)
- [Security](#)(see page 262)
- [System](#)(see page 293)



Accessories

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

- [Terminals](#)(see page 11)
- [SSH Client](#)(see page 13)
- [VNC Viewer](#)(see page 15)
- [Network Tools](#)(see page 23)
- [Application Launcher](#)(see page 27)
- [App Portal](#)(see page 30)
- [System Information](#)(see page 31)
- [Screenshot Tool](#)(see page 34)
- [Setup](#)(see page 37)
- [System Log Viewer](#)(see page 39)
- [Task Manager](#)(see page 42)



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.

- i** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected and highlighted in yellow), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of accessories: Terminals (selected and expanded), SSH Client, VNC Viewer, Network Tools, Application Launcher (expanded), App Portal, System Information, Screenshot Tool, Setup, System Log Viewer (expanded), and Task Manager. The main content area is titled "Terminal Sessions". It shows a table with one row: "Session Name" (Local Terminal). At the bottom right of the content area are buttons for "Close", "Save", and "Save and Close".

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 373).

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 267).

3. Enter the shell commands supported by IGEL OS.

i For a collection of commands supported by IGEL OS, see the [IGEL Community cheatsheet](#)¹.

¹ <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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top menu bar has tabs: Accessories (which is selected and highlighted in yellow), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of accessories: Terminals, SSH Client (selected and expanded), VNC Viewer, Application Launcher, App Portal, System Information, Screenshot Tool, Setup, System Log Viewer, and Task Manager. The main content area is titled "Application via SSH". It has a table with two columns: "Session Name" and "SSH Session". There is one entry in the table: "SSH Session". At the bottom of the content area are buttons for "Close", "Save", and "Save and Close".

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 373).

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected and highlighted in yellow), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Terminals, SSH Client, VNC Viewer (selected and expanded), Connection, Compression, Input, Misc, Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, and Setup. The main content area is titled "VNC Viewer Sessions". It shows a table with one row: "Session Name" (containing "VNC Viewer"). Below the table are four icons with labels: a plus sign for creating a new entry, a trash can for removing, a pencil for editing, and a copy symbol for copying. At the bottom are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

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 373).

- [Connection](#)(see page 17)
- [Compression](#)(see page 18)
- [Input](#)(see page 19)
- [Misc](#)(see page 21)



Connection

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Terminals, SSH Client, VNC Viewer (expanded), VNC Viewer (selected), Connection, Compression, Input, Misc, Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, and Setup. The main content area is titled "Name or IP-Address of VNC-Server" and contains three input fields: "Name or IP-Address of VNC-Server" (with a refresh icon), "Password" (with a "New password" field and an info icon), and "New password (repeated)". Below these is a "Set password" button. At the bottom of the content area are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view: Terminal, SSH Client, VNC Viewer (selected), VNC Viewer (Connection, Compression, Input, Misc), Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, and Setup. The main content area shows two configuration fields: "Compression Level (default=2)" with a dropdown menu showing "2" and an info icon, and "JPEG quality level" with a dropdown menu showing "8" and an info icon. At the bottom are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

The screenshot shows the "Compression" tab selected under the "VNC Viewer" section of the left sidebar. The main panel displays two configuration options: "Compression Level (default=2)" set to 2, and "JPEG quality level" set to 8. The "Save" button at the bottom is highlighted with a checkmark.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Terminals, SSH Client, VNC Viewer (selected), Connection, Compression, Input (selected), Misc, Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, and Setup. The main content area shows configuration options for the selected "Input" category under "VNC Viewer". There are three sections: 1) "View only" with an unchecked checkbox. 2) "Pass system keys directly to the server (full-screen)" with a checked checkbox. 3) "Menu key" with a dropdown menu set to "F8". At the bottom are buttons for Close, Save, and Save and Close.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. There are also search and settings icons. The left sidebar has a tree view: Terminal, SSH Client, VNC Viewer (selected), VNC Viewer (Connection, Compression, Input, Misc), Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, and Setup. The main content area shows "Shared mode" (unchecked), "Full-screen mode" (unchecked), and a "Color Level" dropdown set to "Default". At the bottom are "Close", "Save" (with a checkmark), and "Save and Close" buttons.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top menu bar has tabs: Accessories (which is selected and highlighted in yellow), User Interface, Network, Devices, Security, and System. On the right side of the menu bar are a search icon and a settings gear icon. The main left pane is a sidebar with a tree view of tools: Terminals, SSH Client, VNC Viewer, Network Tools (which is selected and highlighted in orange), Application Launcher, App Portal, System Information, Screenshot Tool, Setup, System Log Viewer, and Task Manager. The main right pane shows a "Session name" field with "Network Tools" entered. Below it is a section titled "Starting Methods for Session" with four items: "Start Menu" (unchecked), "Menu folder" (empty), "Start Menu's System tab" (checked), and "Application Launcher" (unchecked). At the bottom are three buttons: "Close", "Save", and "Save and Close".

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 373).

- ⓘ 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**.

A screenshot of the "Devices - Network Tools" application window. The window has a dark blue header bar with the title "Devices - Network Tools" and standard window controls. Below the header is a menu bar with "Tool", "Edit", and "Help". A tab bar below the menu includes "Devices" (which is selected and highlighted in blue), "Ping", "Netstat", "Traceroute", "Port Scan", "Lookup", "Finger", and "Whois".

The main content area is divided into sections:

- IP Information:** A table showing network protocol details.

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv6	::	0		Unknown
IPv4	[Redacted]			
- Interface Information:** A list of hardware parameters.
 - Hardware address: [Redacted]
 - Multicast: [Redacted]
 - MTU: [Redacted]
 - Link speed: [Redacted]
 - State: [Redacted]
- Interface Statistics:** A list of network statistics.
 - Transmitted bytes: [Redacted]
 - Transmitted packets: [Redacted]
 - Transmission errors: [Redacted]
 - Received bytes: [Redacted]
 - Received packets: [Redacted]
 - Reception errors: [Redacted]
 - Collisions: [Redacted]

At the bottom left of the main content area, the word "Idle" is displayed.

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](#)².

Detailed descriptions of the Domain Name concept can be found in [RFC 1034](#)³ and in related RFCs.

² https://en.wikipedia.org/wiki/Domain_Name_System

³ <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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. To the right of the tabs are a search icon and a settings gear icon. The left sidebar contains a tree view of accessories: Terminals, SSH Client, VNC Viewer, Network Tools, Application Launcher (selected and expanded), App Portal, System Information, Screenshot Tool, Setup, System Log Viewer, and Task Manager. The main content area is titled "Starting Methods for Session". It shows four configuration items with checkboxes:

- Start Menu: checked
- Menu folder: empty input field
- Start Menu's System tab: checked
- Application Launcher: empty input field

At the bottom are buttons for Close, Save, and Save and Close.

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 373).

Application Launcher Configuration

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



The screenshot shows the IGEL Setup application interface. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System, and Apps. On the right of the top bar are search and settings icons. The left sidebar has a tree view with "Application Launcher" expanded, showing "Application Launcher Configuration" as the selected item. Other items in the sidebar include Terminals, SSH Client, VNC Viewer, Network Tools, System Log Viewer, and Task Manager. The main content area contains three configuration items in a grid:

	<input type="checkbox"/> Hide system page	
	<input checked="" type="checkbox"/> Show current user name in About, Application Launcher and start menu	
	<input type="checkbox"/> Single Click Mode	

At the bottom right of the main content area are buttons: "Close", "Save", and "Save and Close".

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 282)
 - Enable local logon under **Security > Logon > Active Directory/Kerberos**. For details, see [Active Directory/Kerberos](#)(see page 275)



Single click mode

- Sessions are started with a single-click. Recommended for users of touchscreen monitors.
- Sessions are started with a double-click. (Default)

- i** 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 140).



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. On the far right of the top bar are a search icon and a settings gear icon. The left sidebar contains a tree view of configuration categories: Terminals, SSH Client, VNC Viewer, Network Tools, Application Launcher (which is expanded and has "App Portal" selected), System Information, Screenshot Tool, Setup, System Log Viewer, and Task Manager. The main content area is titled "Starting Methods for Session" and shows a list of methods for the "App Portal" session. Each method has a circular refresh icon to its left. The methods are: "Start Menu" (unchecked), "Menu folder" (empty), "Start Menu's System tab" (checked), and "Application Launcher" (unchecked). At the bottom right of the content area are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

Method	Status
Start Menu	<input type="checkbox"/>
Menu folder	
Start Menu's System tab	<input checked="" type="checkbox"/>
Application Launcher	<input type="checkbox"/>

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).



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 267).
The password requirement can be changed through the **Password protection** option in the starting methods configuration.

Menu path: **Accessories > System Information**

The screenshot shows the 'IGEL Setup' application window with the 'Accessories' tab selected. On the left sidebar, 'System Information' is highlighted. The main panel displays session settings for 'System Information'. It includes a 'Session name' field set to 'System Information' and a 'Starting Methods for Session' section. This section lists four methods: 'Start Menu' (unchecked), 'Menu folder' (unchecked), 'Start Menu's System tab' (checked), and 'Application Launcher' (unchecked). At the bottom are 'Close', 'Save', and 'Save and Close' buttons.

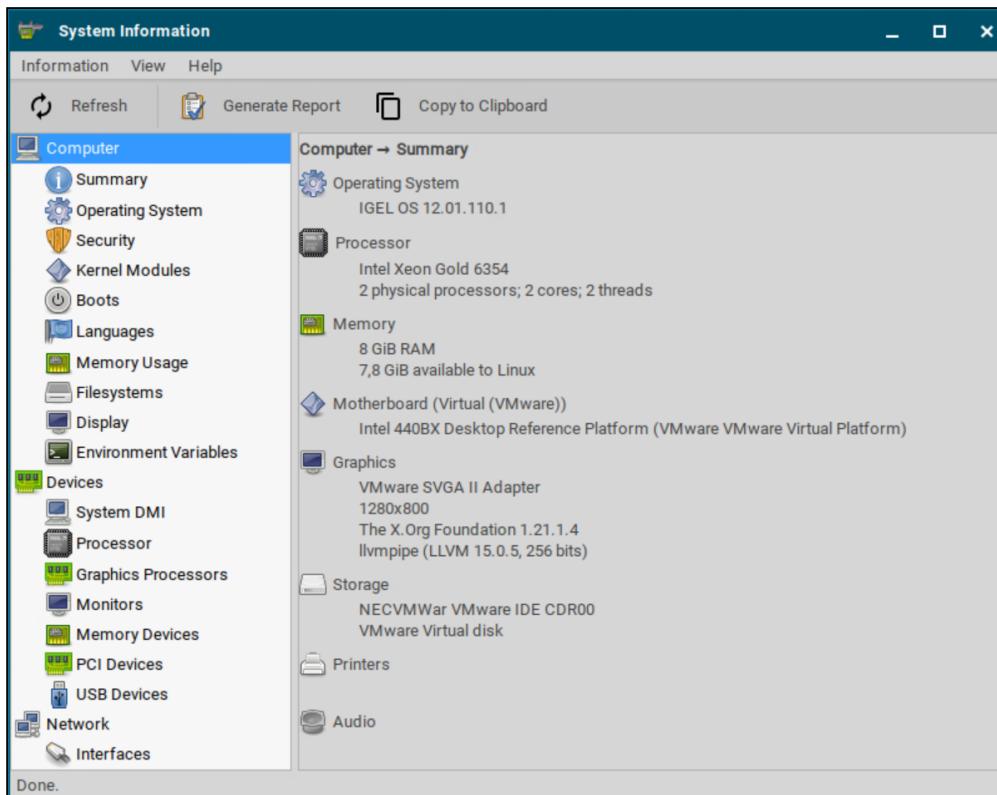
You can configure the starting methods for an easy access of the System Information.

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).



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 249).

Configuration of IGEL OS 12 Device Settings

A screenshot of the "Devices - USB Devices - System Information" window in the IGEL OS interface. The left sidebar shows navigation categories like Computer, Devices (selected), Network, and USB Devices (also selected). The main pane lists USB devices: 001:001 [Linux] 2.0 root hub, 002:001 [Linux] 1.1 root hub, and 002:004 Plantronics, Inc. Poly BT700. The last item is highlighted with a blue selection bar. A red box highlights the "Device Information" section for the selected device, which contains the following details:

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



Screenshot Tool

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

Menu path: **Accessories > Screenshot Tool**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories (which is selected), User Interface, Network, Devices, Security, and System. There are also search and settings icons. The left sidebar has a tree view with categories like Terminals, SSH Client, VNC Viewer, Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool (which is selected and highlighted in yellow), Setup, System Log Viewer, and Task Manager. The main right panel shows a "Session name" field with "Screenshot Tool" entered. Below it is a section titled "Starting Methods for Session" with five entries: "Start Menu" (unchecked), "Menu folder" (empty), "Start Menu's System tab" (checked), "Application Launcher" (unchecked), and "Application Launcher folder" (empty). At the bottom are "Close", "Save", and "Save and Close" buttons.

Starting Method	Status	Description
Start Menu	<input type="checkbox"/>	
Menu folder		
Start Menu's System tab	<input checked="" type="checkbox"/>	
Application Launcher	<input type="checkbox"/>	
Application Launcher folder		

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 373).

Using Screenshot Tool

1. Start the **Screenshot Tool**.

- i** 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 111).

2. Select a **Region to capture** option. You have the following options:

- **Entire screen**

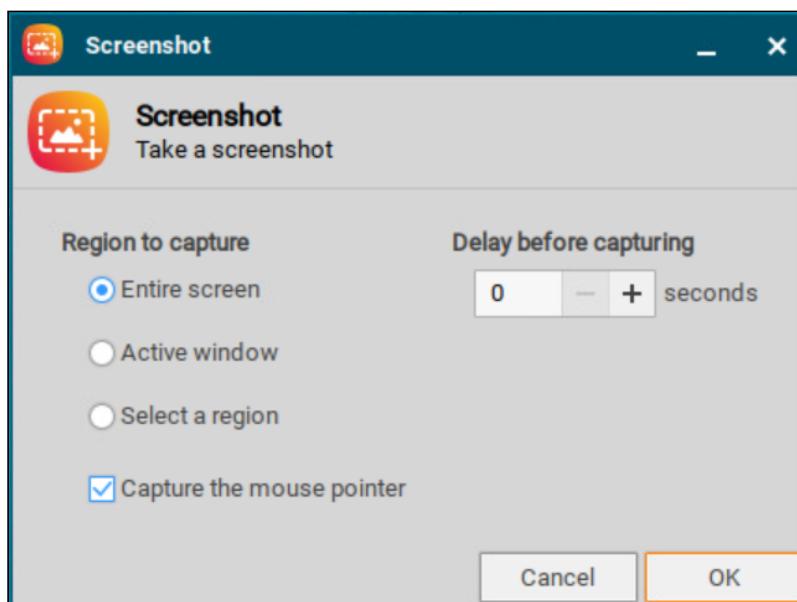
The entire screen content will be photographed.

- **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.

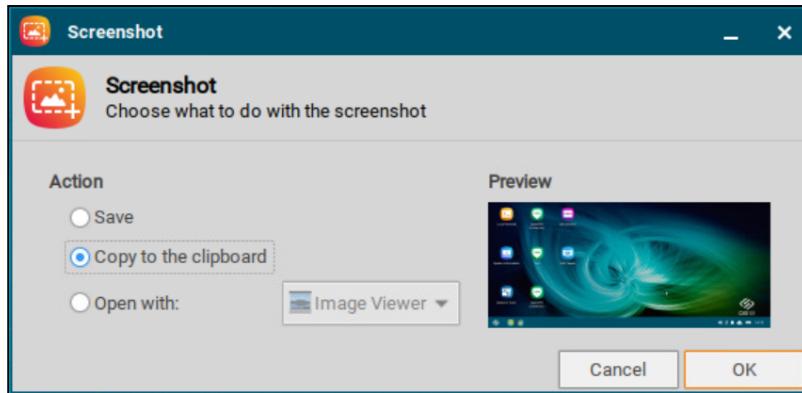
The mouse pointer is visible on the screenshot.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top menu bar has tabs: Accessories (which is selected and highlighted in yellow), User Interface, Network, Devices, Security, and System. On the far right of the menu bar are a search icon and a settings gear icon. The left sidebar contains a list of tools: Terminals, SSH Client, VNC Viewer, Network Tools, Application Launcher, App Portal, System Information, Screenshot Tool, Setup (which is selected and highlighted in yellow), System Log Viewer, and Task Manager. The main content area is titled "Starting Methods for Session". It shows a list of methods with checkboxes:

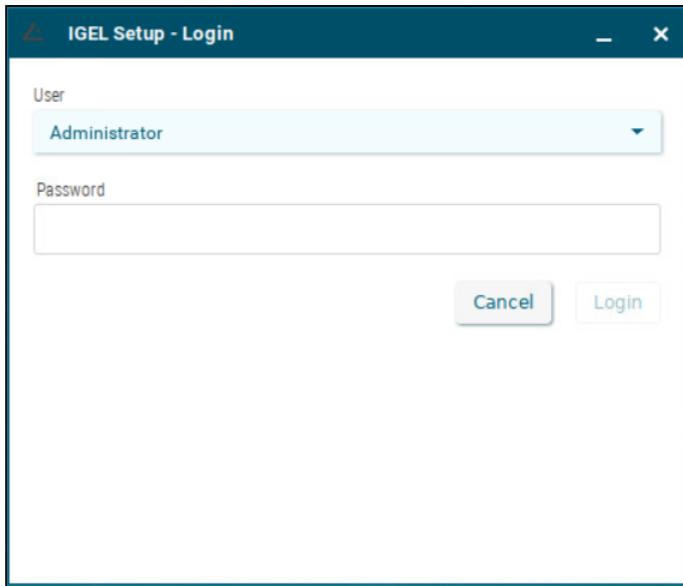
- Start Menu (unchecked)
- Menu folder (unchecked)
- Start Menu's System tab (checked)
- Application Launcher (unchecked)

At the bottom of the main content area are three buttons: "Close", "Save", and "Save and Close".

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

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 267).

- ⚠** 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:

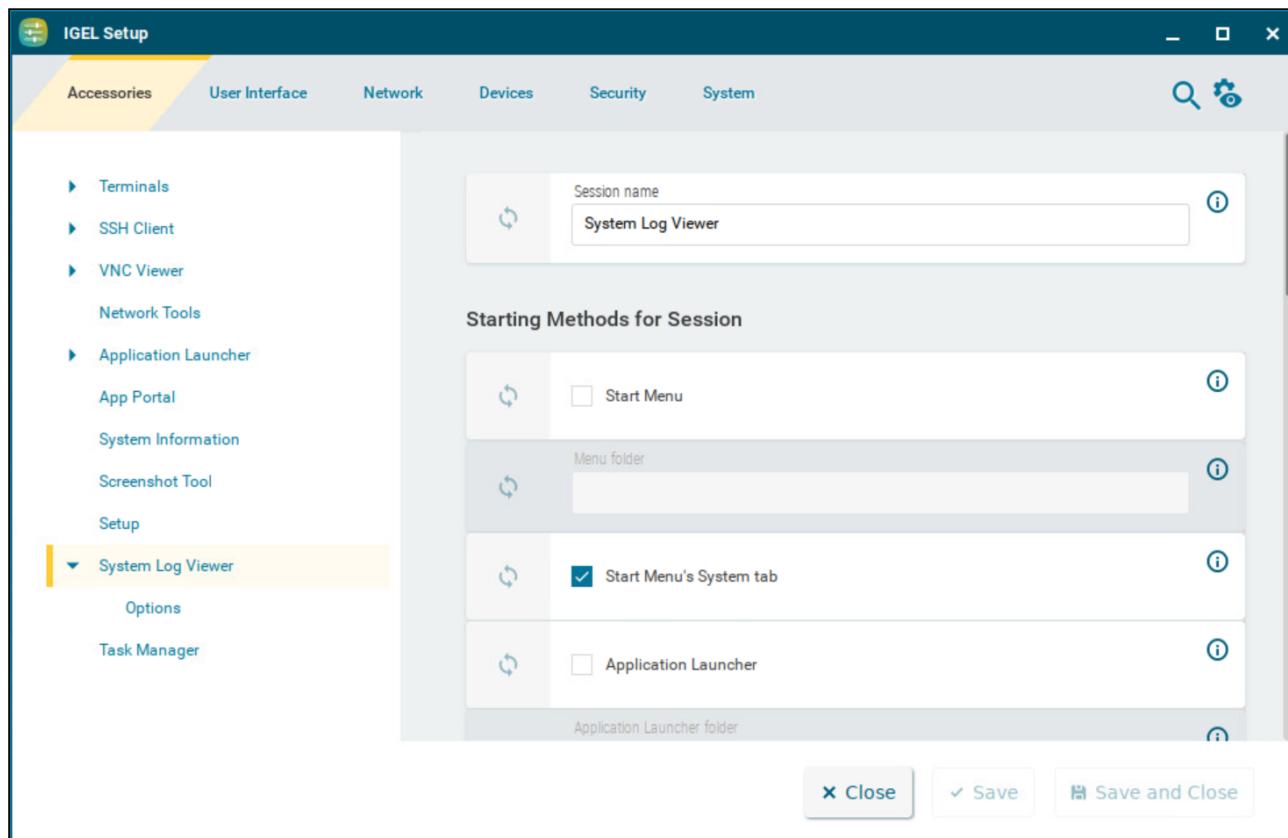
- Administrator
- Setup administrator
- Setup user



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 373).

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**.

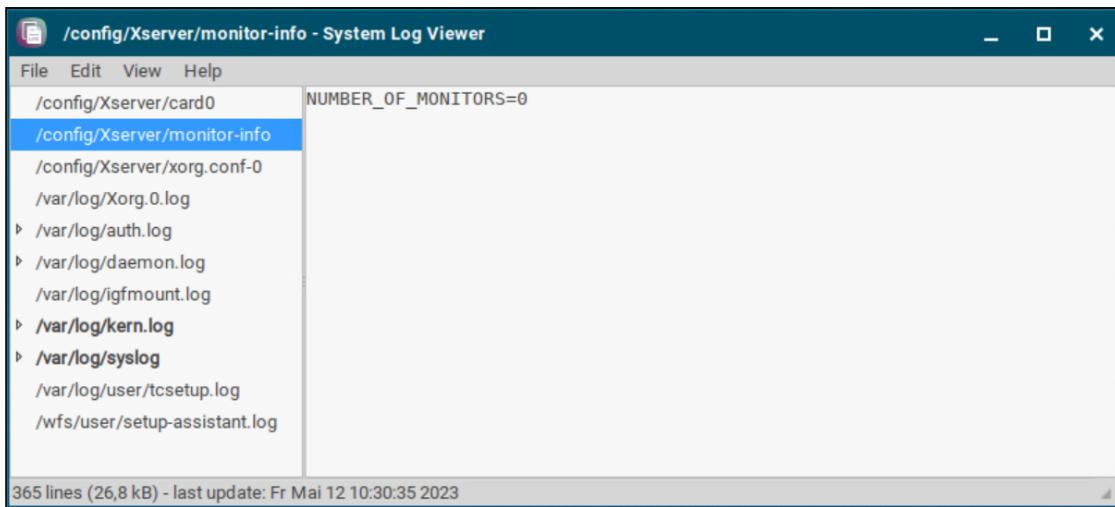
When the System Log Viewer is started, the file that you have added will be shown.

Known Issue

For OS version 12.02.x, 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**.



A screenshot of the "System Log Viewer" application window. The title bar reads "/config/Xserver/monitor-info - System Log Viewer". The menu bar includes File, Edit, View, and Help. The left-hand column is a tree view of log files:

- /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/user/tcsetup.log
- /wfs/user/setup-assistant.log

The right-hand column displays the content of the selected file: "NUMBER_OF_MONITORS=0". At the bottom of the window, a status bar shows "365 lines (26,8 kB) - last update: Fr Mai 12 10:30:35 2023".

- ▶ 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**

 A screenshot of the IGEL Setup application window. The left sidebar shows a tree view with categories like Accessories, User Interface, Network, Devices, Security, and System. Under Accessories, 'Task Manager' is selected and highlighted with a yellow bar at the bottom. The main right panel has a title 'Starting Methods for Session'. It contains four items with checkboxes:

- 'Start Menu' with an unchecked checkbox.
- 'Menu folder' with an unchecked checkbox.
- 'Start Menu's System tab' with a checked checkbox.
- 'Application Launcher' with an unchecked checkbox.

 Below these items is a section labeled 'Application Launcher folder'. At the bottom of the panel are three buttons: 'Close', 'Save', and 'Save and Close'.

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 373).

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**.



CPU: 3%

Processes: 248

Memory: 18%

Swap: 0%

To determine the device's total memory usage:

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



CPU: 3%

Processes: 248

Memory: 18%

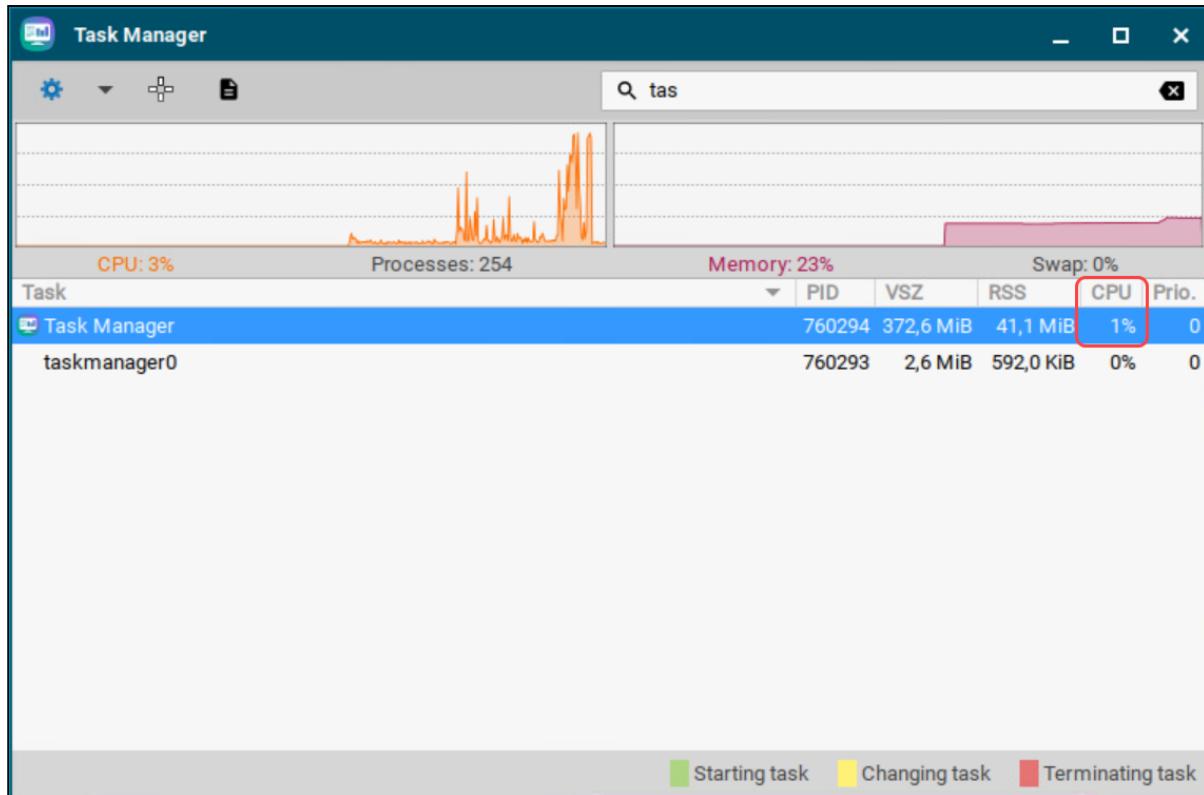
Swap: 0%



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

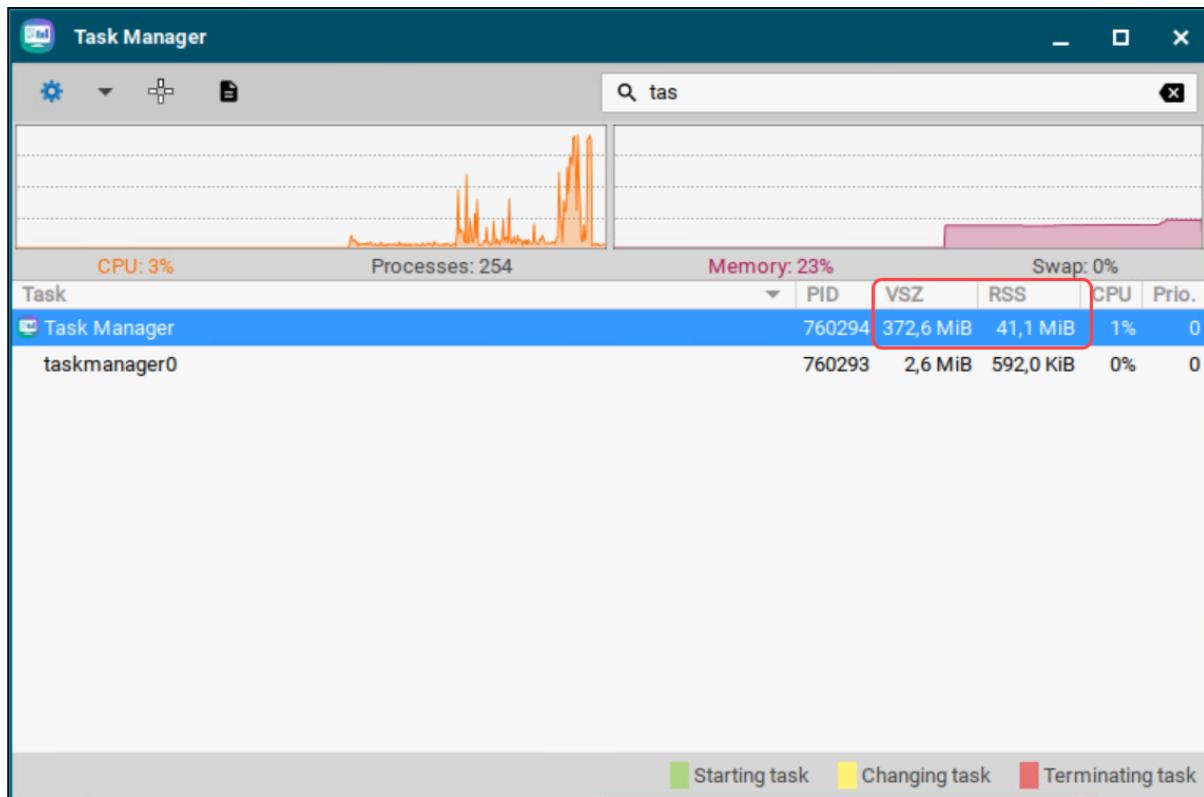
To determine the extent to which a specific application contributes to processor usage, proceed as follows:

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).



- i** 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.

- i** 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.
- i** 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 48)
- [Display Configurator](#)(see page 60)
- [Desktop](#)(see page 74)
- [Language](#)(see page 98)
- [Screenlock / Screensaver](#)(see page 100)
- [Hotkeys](#)(see page 111)
- [Input](#)(see page 113)
- [Commands](#)(see page 140)



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.

- ⓘ For information on how to use the Display Configurator for quick display configuration, see [Display Configurator](#)(see page 60).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Settings (selected and highlighted in orange), Power Options, Access Control, Gamma correction, DPI Options, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input, and Commands. The main content area is titled "General Settings" and shows a "Number of Screens" section with a row of buttons numbered 1 through 8. The button for "1" is highlighted with a yellow border. Below this is a large preview window showing a single monitor setup with a central window labeled "1". At the bottom of the window are three buttons: "Close", "Save", and "Save and Close".



⚠ 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:

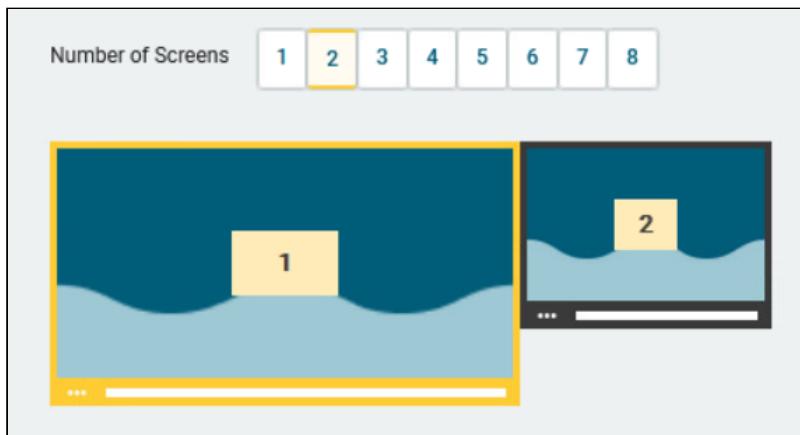
- In the UMS: Edit the display configuration via **Devices > [device name] > [device's context menu] > Edit Configuration** or via a new profile.
- In Web UMS: Edit the settings by clicking **Edit Configuration** in the Device Information of the device under **Devices > [device name]**.
- On the endpoint 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)

- i** 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.

i 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.

i 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)

- [Power Options](#)(see page 51)
- [Access Control](#)(see page 54)
- [Gamma Correction](#)(see page 56)
- [DPI Options](#)(see page 58)



Power Options

This article shows how to configure energy-saving stages in IGEL OS.

Power Management

Menu path: **Display Settings > Power Options > Power Management**

A screenshot of the IGEL Setup application window. The left sidebar shows a tree view with categories like Accessories, User Interface, Network, Devices, Security, and System. Under Display Settings, the Power Options category is expanded, and its subcategory Power Management is selected. The main panel is titled "Display Power Management Settings". It contains a section for "On Battery" with three dropdown menus for Standby Time (6 Minutes), Suspend Time (8 Minutes), and Off Time (10 Minutes). Below this is a section for "Plugged In" with a dropdown menu for Standby Time. At the bottom are buttons for Close, Save, and Save and Close.

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

Menu path: **Display Settings > Power Options > Brightness Reduction**

Setting	On Battery	Plugged In
On inactivity reduce to	20	80
Reduce after	9	9

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.



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are a search icon and a gear icon. The left sidebar has a tree view with categories like Display Settings, Power Options, Access Control (which is selected and highlighted in orange), Gamma correction, DPI Options, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input, and Commands. The main content area shows three configuration items: "Disable console switching" (unchecked), "Access control" (checked), and "Disable TCP connections" (checked). Below these is a section titled "List of Trusted X Hosts" with a table header "Trusted host" and an empty table body. At the bottom are buttons for "Close", "Save", and "Save and Close".

List of Trusted X Hosts	
Trusted host	

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Settings (expanded), Power Options, Access Control, Gamma correction (selected and highlighted in yellow), DPI Options, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input, and Commands. The main content area is divided into two sections: "Screen 1" and "Screen 2". Each section contains three sliders for "Gamma Value Red", "Gamma Value Green", and "Gamma Value Blue". Each slider has a current value (e.g., 1.00 for Red), a scale from 0.1 to 10, and an information icon (i). At the bottom right of the content area are buttons for "Close", "Save", and "Save and Close".

Screen	Color	Value	Scale Range
Screen 1	Red	1.00	0.1 to 10
	Green	1.00	0.1 to 10
	Blue	1.00	0.1 to 10
Screen 2	Red	1.00	0.1 to 10
	Green	1.00	0.1 to 10
	Blue	1.00	0.1 to 10

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Display Settings, Power Options, Access Control, Gamma correction, and so on. Under "Display Settings", "DPI Options" is selected and highlighted with a yellow bar. The main content area shows two configuration options: "Monitor DPI detection" set to "Smart" (with a dropdown arrow) and "Monitor DPI" set to "96" (with a dropdown arrow). At the bottom are buttons for "Close", "Save" (with a checkmark icon), and "Save and Close".

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**.



Display Configurator

With the Display Configurator, you can configure the display on several screens. This article shows how to configure the starting methods for the Display Configurator in IGEL OS.

- ⓘ For details on how to use the function, see [Using Display Configurator](#)(see page 70).
For details on how to configure the function, see [Options](#)(see page 62).

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

The screenshot shows the 'User Interface' tab selected in the top navigation bar of the 'IGEL Setup' application. Under the 'Display Settings' section, the 'Display Configurator' option is highlighted. On the right, a configuration dialog is open for the 'Display Configurator' session. It shows the session name 'Display Configurator' and a list of 'Starting Methods for Session'. The 'Start Menu's System tab' method is checked. At the bottom, there are 'Close', 'Save', and 'Save and Close' buttons.

You can configure the starting methods for easy access to the Display Configurator.

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

- [Options](#)(see page 62)
- [Minimal Dialog](#)(see page 65)
- [Advanced Dialog](#)(see page 67)



- Using Display Configurator(see page 70)



Options

This article shows how to configure the details of the Display Configurator function in IGEL OS.

Menu path: **User Interface > Display Configurator > Options**

Setting	Value
Dialog Type	Minimal dialog
Smart display configuration	<input checked="" type="checkbox"/>
Preserve settings over reboot	<input checked="" type="checkbox"/>
Configure new displays when connected	<input type="checkbox"/>
Mirror displays	<input checked="" type="checkbox"/>
Extend to the left	<input type="checkbox"/>

Dialog type

Defines the opening dialog of the Display Configurator.

Possible values:

- **Minimal dialog:** The Display Configurator starts with the minimal dialog.
- **Advanced dialog:** The Display Configurator starts with the advanced dialog.

Smart display configuration

Configurations of the displays will be saved and automatically re-applied when the same displays are re-connected. (Default)

Display configurations will not be saved.



Preserve settings over reboot

- The display settings will be preserved over a reboot. (Default)
- The display settings will be reset to the default settings in the event of a reboot.

Configure new displays when connected

- The Display Configurator starts as soon as new screens are connected.
- The Display Configurator does not start automatically when new screens are connected. (Default)

Options in Minimal Dialog

Mirror displays

- The option to mirror the displays is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

Extend to the left

- The **Extend to the left** option is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

Extend to the right

- The **Extend to the right** option is shown in the minimal dialog. (Default)
- The option is not shown in the minimal dialog.

Rotate displays (Page orientation)

- The **Rotate displays (Page orientation)** option is shown in the minimal dialog.
- The option is not shown in the minimal dialog. (Default)

Mouse options

- Options to quickly change the mouse configurations are shown in the minimal dialog. (Default)
- The mouse settings are not shown.

Advanced

- The **Advanced** button is shown in the minimal dialog. With this button, you can switch to the advanced dialog. (Default)
- The **Advanced** button is not shown.



Reset

- The **Reset** button is shown in the minimal dialog. With this button, you can restore the default settings. (Default)
- The **Reset** button is not shown.

Timeout for confirmation dialog

Specifies a timeout for the confirmation dialog.

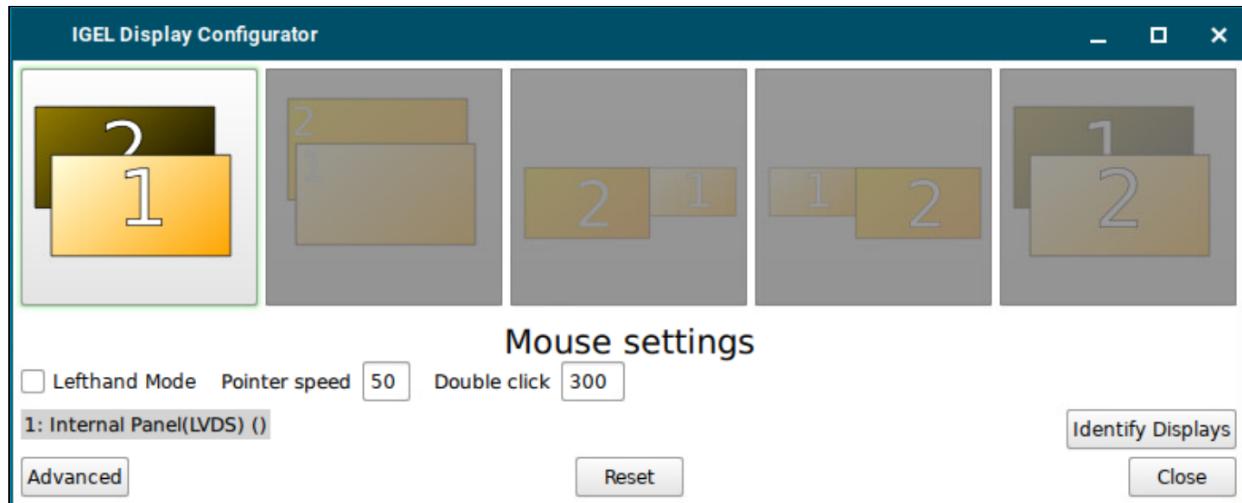
The value can be set between 0-120 seconds. (Default: 10 seconds)



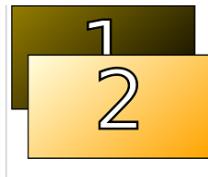
Minimal Dialog

This article shows the functions of the minimal dialog of the IGEL Display Configurator dialog. For details on how to use the function, see [Using Display Configurator](#)(see page 70).

If the Display Configurator starts with the advanced dialog, you can access the minimal dialog by clicking **Simple**.



Selection	Function
	Uses only display 1.
	Shows the same content on all screens, i.e. clone mode or mirroring.
	Extends the display area to the screen on the left
	Extends the display area to the screen on the right.
	Uses only display 2.



Identify displays

Starts the monitor detection.

Advanced

Switches to advanced mode of display configuration.

Reset

Restores the default settings.

Close

Closes the dialog.

Mouse Settings

- ⓘ The following parameter must be activated for the configuration of mouse settings:
• **User Interface > Display Configurator > Options > Mouse options** (disabled by default)

Lefthand Mode

- Lefthand mode is active.
 Righthand mode is active. (Default)

Pointer speed

Value for the mouse speed in percentage between 1 (slow) and 100 (fast). (Default: 50)

Double click

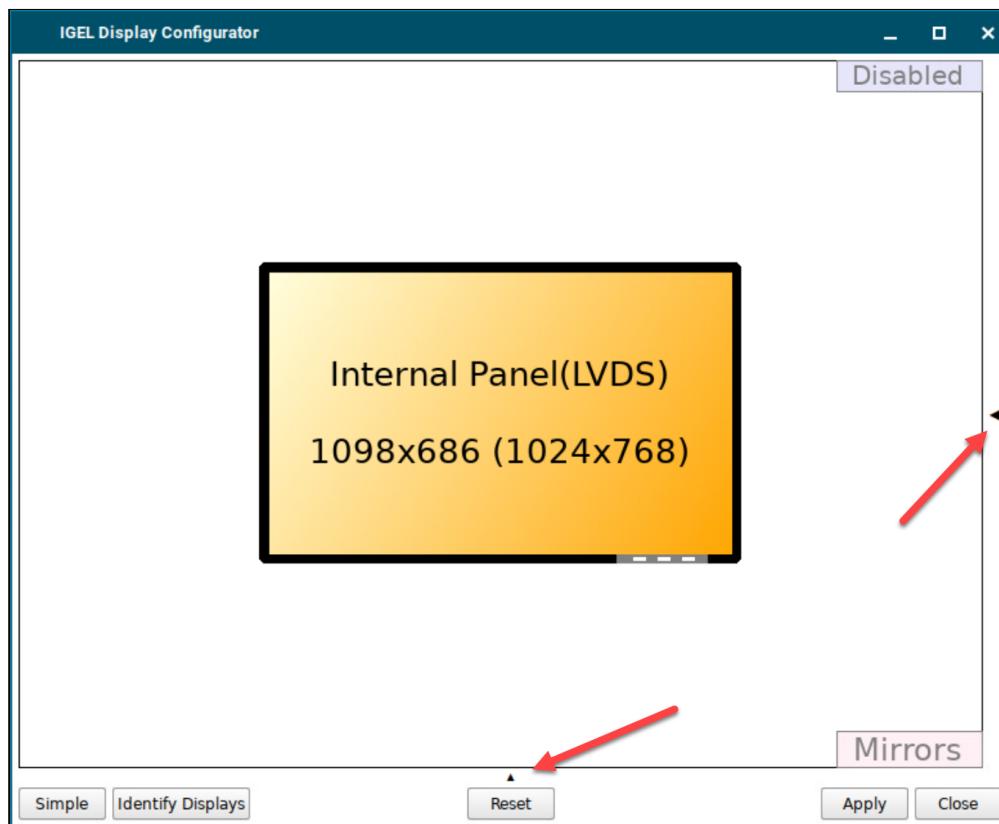
Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click. (Default: 300)



Advanced Dialog

This article shows the functions of the advanced dialog of the IGEL Display Configurator. For details on how to use the function, see [Using Display Configurator](#).

If the Display Configurator starts with the minimal dialog, you can access the advanced dialog by clicking **Advanced**.



Advanced Settings

Advanced settings (pan/scale/resolution) can be configured in a collapsible area on the right side of the window.

- ▶ Click the arrow on the right side of the window, to enlarge the advanced settings area.

The display selector at the top defines the display for which the following settings are configured:

Use this display

- Enables the display.
- Disables the display.



Index

Gives the display an order number.

Rotation

Rotates the display.

Possible values:

- **None** (Default)
- **Left**
- **Inverted**
- **Right**

Resolution

The resolution of the display can be selected. (Default: Automatic)

Refresh rate

The refresh rate of the display can be selected. The available values depend on the selected resolution. (Default: Automatic)

Panning

Sets up a virtual screen that is larger than your physical screen. It will look like an enlarged screen. By moving the mouse to the edge of the screen, hidden parts become visible. (Default: None)

Reflection

Transforms the display as if being reflected by a mirror.

Possible values:

- **None** (Default)
- **Horizontal**
- **Vertical**
- **Horizontal and Vertical**

Scale from

A software variant of the resolution. This can be useful if you need a resolution that is not available on the hardware. (Default: None)

Mouse Settings

(i) The following parameter must be activated for the configuration of mouse settings:



- **User Interface > Display Configurator > Options > Mouse options** (disabled by default)

Mouse settings can be configured in a collapsible area on the bottom of the window.

- ▶ Click the arrow on the bottom of the window, to enlarge the mouse settings area.

Lefthand mode

- Lefthand mode is active.
 Righthand mode is active. (Default)

Pointer speed

Value for the mouse speed in percentage between 1 (slow) and 100 (fast). (Default: 50)

Double click

Maximum interval in milliseconds between two mouse clicks to still be recognized as a double-click. (Default: 300)

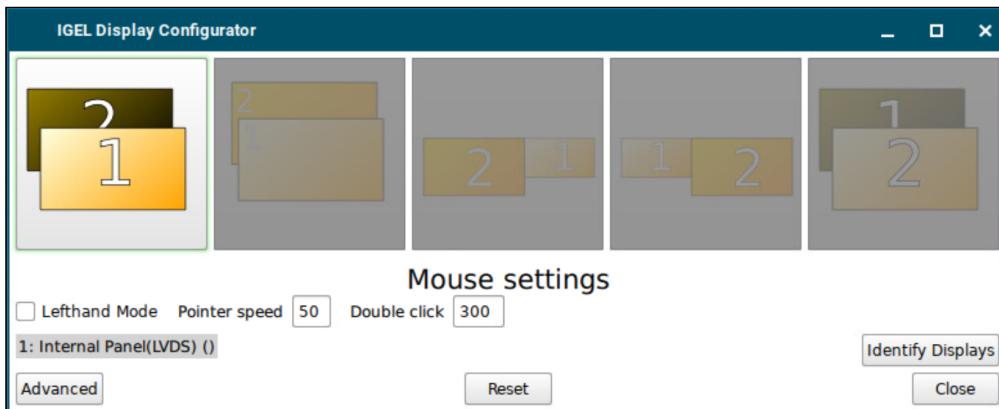


Using Display Configurator

This article shows how to use the Display Configurator in IGEL OS.

- ⓘ To save the configured settings, the following parameters need to be enabled:
 - **User Interface > Display Configurator > Options > Smart display configuration**
(enabled by default)
 - **User Interface > Display Configurator > Options > Preserve settings over reboot**
(enabled by default)

-
- ▶ Start the **Display Configurator**. The starting options are described under [Display Configurator](#)(see page 60).



It is possible to use several different profiles in the Display Configurator. The profiles are automatically selected at runtime depending on the currently connected monitors. A profile is created when the current monitor layout, or the current resolution is configured via Display Configurator. The profile is automatically assigned to the currently connected monitors and recognizes the manufacturer, model by plug, and, if available, the status of the laptop cover. When the screen configuration changes (by hot (un)plugging), the system will automatically switch to the profile.

Identify Displays

- ▶ Click **Identify Displays** to start screen detection.
The names and properties of the screens will be detected. The connection, the assigned number (**1** = main screen) and the name will be shown on each screen. Example: **1: DVI-D(II): Samsung 24"**

Define Main Screen

1. If necessary, switch to the advanced dialog by clicking **Advanced**.



2. Select the screen that you wish to define as the main screen under the advanced settings.

3. Set the **Index** to 1.

The display is now marked as the main screen.

Split Display over Several Screens

You have various options for using several screens. In the dialog, the connection, the assigned number (**1** = main screen) and the name is shown for each screen. (Example: **1: DVI-D(II): Samsung 24"**)

The procedure with the minimal dialog:

1. If necessary, switch to the minimal dialog by clicking **Simple**.

2. Select according to your needs:

- To show the same content on all screens (Shadow screens), select .
- If you would like to expand the display to all screens and the other screens are to the left of the main screen, select .
- If you would like to expand the display to all screens and the other screens are to the right of the main screen, select .

The procedure with the advanced dialog:

1. If necessary, switch to the advanced dialog by clicking **Advanced**.

2. Use drag-and-drop to move the displays to the desired configuration.

- Move the displays to the desired layout. They will snap together when they touch each other at the edge.
- If you no longer need a monitor, drag it to the upper right corner to the **Disabled** area to disable it.
- To display the same content on multiple displays, drag them one on top the other. **Mirror \<other>** will be displayed. The mirroring monitor is displayed in the lower right corner.

3. Click **Apply** to set the current status. Click **Yes** in the confirmation window to save the configuration permanently and associate it with the profile.

Rotate Displays (Page Orientation)

i The following parameter must be activated for the configuration:

- **Setup > User Interface > Display Configurator > Options > Rotate displays (Page orientation)** (disabled by default)



1. If necessary, switch to the advanced dialog by clicking **Advanced**.



2. To rotate the display counterclockwise, click on . To rotate the display clockwise, click on .
3. Click **Apply** to set the current status. Click **Yes** in the confirmation window to save the configuration permanently and associate it with the profile.

Change Mouse Settings

- i** The following parameter must be activated for the configuration of mouse settings:
- **Setup > User Interface > Display Configurator > Options > Mouse options** (disabled by default)

1. If necessary, switch to the minimal dialog by clicking **Simple**.
2. To adjust the mouse for left-handed users, enable the **Lefthanded Mode**.
3. To adjust the speed of the mouse pointer, change the value under **Pointer speed**. The higher the value, the further the mouse pointer will move when the mouse is moved.
4. To change the time interval within which two consecutive mouse clicks are recognized as a double-click, change the number of milliseconds under **Double click interval**.

Zoom Display (Screen Magnifying Glass)

You can magnify the screen content. The effect is the same as with the screen magnifying glass in Microsoft Windows: All text and graphics are magnified by the same factor; this results in a virtual display area which is bigger than the monitor's available display area. The user therefore sees a magnified section of the entire screen; the section can be moved by moving the mouse to the edge of the screen.

To activate the function:

1. If necessary, switch to the advanced dialog by clicking **Advanced**.
2. Under **Panning**, set the desired value. Example: **3860x2160**
3. Under **Resolution**, set a low value. This value simulates the actual resolution of the screen. Example: **1280x800**
4. Click **Apply**.
The screen content will be magnified. The magnification factor results from the ratio of the virtual resolution and the simulated actual resolution.



- ⓘ If the same content is displayed on a number of screens (Shadow screens), all screens will show the same section. However, you can set a different magnification level for each of the screens.

Change Refresh Rate

- ⓘ This is only possible if a resolution has been selected. The respective resolutions can be different. A refresh rate of 60 Hz is usually suitable for standard screens.

1. If necessary, switch to the advanced dialog with **Advanced**.
2. Under **Refresh rate**, set the desired value.

Restore Default Settings

- ▶ Click **Reset** to restore the default settings.



Desktop

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

Menu path: **User Interface > Desktop**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface" (which is highlighted in yellow), "Network", "Devices", "Security", and "System". Below the tabs is a search bar and a settings gear icon. The left sidebar contains a tree view with categories like "Display Settings", "Display Configurator", "Options", "Desktop" (which is expanded to show "Background (1st Monitor)", "Taskbar", "Taskbar Background", "Taskbar Items", "Pager", "Start Menu", and "In-Session Control Bar"). The main right panel shows configuration options for the desktop theme. It includes a checkbox for "Local Window Manager for this Display" (checked), a dropdown for "User Interface Theme" set to "IGEL Color", and color swatches for "Base color of the UI theme" (#004f68) and "Highlight color of the UI theme" (#0088ac). At the bottom are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

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 appearing 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 77)
- [Taskbar](#)(see page 81)
- [Taskbar Background](#)(see page 84)
- [Taskbar Items](#)(see page 86)
- [Pager](#)(see page 89)
- [Start Menu](#)(see page 94)
- [In-Session Control Bar](#)(see page 96)



Background (1st Monitor)

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Settings, Display Configurator, Desktop (which is expanded to show Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager, Start Menu, In-Session Control Bar, Language, Screenlock / Screensaver, Hotkeys, and Input). The main content area shows the "Background (1st Monitor)" configuration. It includes three dropdown menus: "Wallpaper (1st monitor)" set to "IGEL", "Wallpaper style (1st monitor)" set to "Stretched", and "Color style (1st monitor)" set to "Horizontal gradient". Below these are two color swatches: "Desktop color (1st monitor)" in "#027498" and "2nd desktop color (1st monitor)" in "#015a76". At the bottom are "Close", "Save", and "Save and Close" buttons. A small checkbox for "Custom wallpaper download (1st monitor)" is also present.

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

i 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.

- i** 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**

The screenshot shows the 'Custom Wallpaper - Server Location' configuration dialog in the IGEL Setup application. The dialog has the following fields:

- Protocol:** HTTP
- Server name:** (empty)
- Server path:** (empty)
- Port:** 80
- User name:** (empty)
- Password:** New password

At the bottom of the dialog are three buttons: **Close**, **Save**, and **Save and Close**.

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 105).

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

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface" (which is highlighted in yellow), "Network", "Devices", "Security", and "System". On the far right of the header are icons for search, refresh, and settings. The left sidebar contains a tree view of configuration categories: "Display Settings", "Display Configurator", "Desktop" (expanded to show "Background (1st Monitor)", "Taskbar" which is selected and highlighted in orange, "Taskbar Background", "Taskbar Items", "Pager", "Start Menu", "In-Session Control Bar", "Language", "Screenlock / Screensaver", "Hotkeys", and "Input". The main content area on the right is titled "Taskbar" and contains several configuration options with "refresh" and "info" icons: "Use taskbar" (checkbox checked), "Taskbar position" (dropdown set to "Bottom"), "Vertical taskbar mode" (dropdown set to "Desobar"), "Taskbar height/width" (text input set to "48"), "Number of rows/columns in taskbar" (dropdown set to "Automatic"), and "Multimonitor taskbar size" (dropdown set to "Restrict taskbar onto one monitor"). At the bottom are buttons for "Close", "Save", and "Save and Close".

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](#)(see page 86).

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)

- i** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are a search icon and a settings gear icon. The left sidebar contains a tree view of configuration categories: Display Settings, Display Configurator, Desktop (expanded to show Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager, Start Menu, In-Session Control Bar, Language, Screenlock / Screensaver, Hotkeys, Input). The "Taskbar Background" item is selected and highlighted with a yellow background. The main content area shows a "Background style" section with a "System preset" dropdown menu. At the bottom right are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

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

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

i Further taskbar settings can be found under:

- **User Interface > Desktop > Taskbar.** For more information, see [Taskbar\(see page 81\)](#).
- **User Interface > Input > Keyboard.** For more information, see [Keyboard\(see page 114\)](#).
- **User Interface > Input > Touchscreen > On-screen keyboard > Application Integration.** For more information, see [Application Integration\(see page 138\)](#).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Display Settings, Display Configurator, Desktop, Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items (which is selected and highlighted in orange), Pager, Start Menu, In-Session Control Bar, Language, Screenlock / Screensaver, Hotkeys, and Input. The main content area shows configuration options for Taskbar Items. It includes sections for "Taskbar clock" (with a checked checkbox), "Sorting order in window button bar" (set to "Group and timestamp"), "Maximum number of rows/columns in window button bar" (set to 1), "Show labels in window button bar" (with a checked checkbox), and "Taskbar system tray" (with a checked checkbox). At the bottom are "Close", "Save", and "Save and Close" buttons.

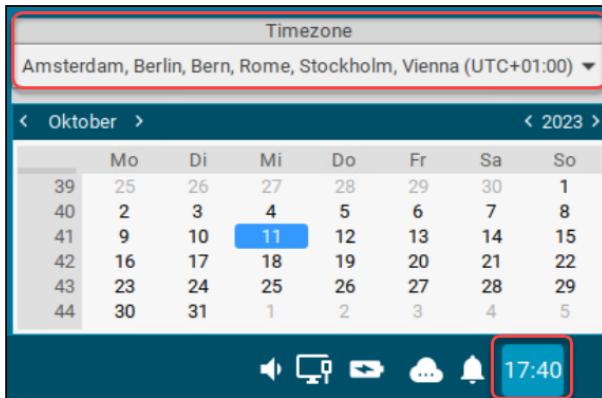
The screenshot shows the "Taskbar Items" section of the "User Interface > Desktop" configuration. It includes settings for the taskbar clock, window button bar sorting, maximum rows/columns, labels, and the taskbar system tray.

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 294).



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 81).
- **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)

Show UMS connection status tray icon on desktop



The icon is shown in the system tray. (Default)

Show battery tray icon on desktop



The icon is shown in the system tray. (Default)

Show ethernet connection status tray icon on desktop



The icon is shown in the system tray. (Default)

Show wifi connection status tray icon on desktop



The icon is shown in the system tray. (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

Show input settings tray icon on desktop



The icon is shown in the system tray. (Default)



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 90).

- ⚠** 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 81).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view of configuration categories: Display Settings, Display Configurator, Desktop (expanded), Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager (which is selected and highlighted in orange), Start Menu, In-Session Control Bar, Language, Screenlock / Screensaver, Hotkeys, and Input. The main content area shows configuration for the Pager. It includes a "Use Pager" checkbox (unchecked) and three input fields: "Number of Screens - Horizontal" (set to 2), "Number of Screens - Vertical" (set to 1), and "Paging Resistance" (set to 10). There are also two checkboxes: "Wrap Workspaces while dragging a window" and "Wrap Workspaces with pointer", both of which are unchecked. At the bottom are buttons for "Close", "Save", and "Save and Close".

IGEL Setup

Accessories User Interface Network Devices Security System

Display Settings

Display Configurator

Desktop

- Background (1st Monitor)
- Taskbar
- Taskbar Background
- Taskbar Items
- Pager**
- Start Menu
- In-Session Control Bar
- Language
- Screenlock / Screensaver
- Hotkeys
- Input

Use Pager

Number of Screens - Horizontal: 2

Number of Screens - Vertical: 1

Paging Resistance: 10

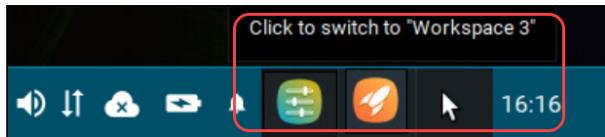
Wrap Workspaces while dragging a window

Wrap Workspaces with pointer

Close Save Save and Close

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

For OS version 12.2.x, 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

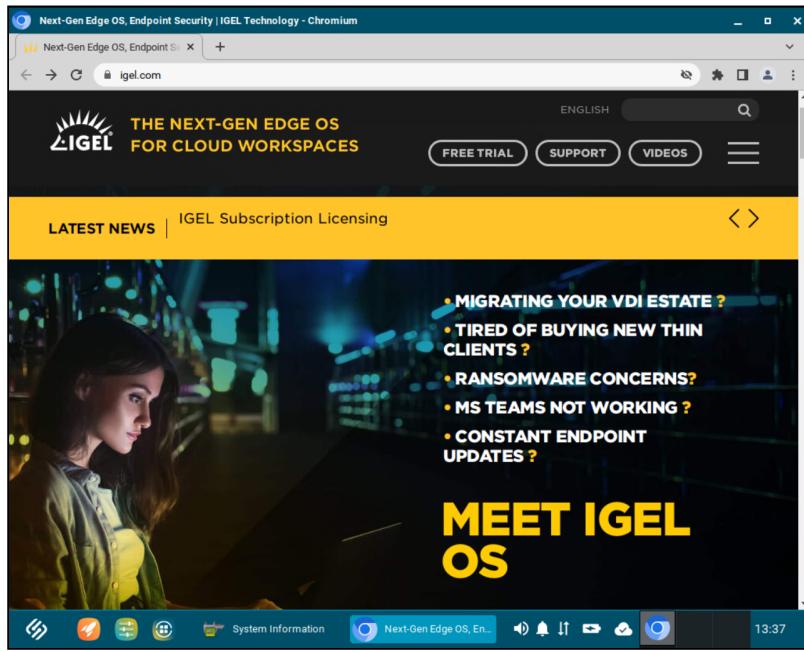
The Pager makes switching between multiple full-screen applications easier. Instead of minimizing/maximizing sessions or switching between them using key combinations, you simply click on the desired workspace using the mouse. When you switch back, the virtual desktop is displayed exactly as before (unless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



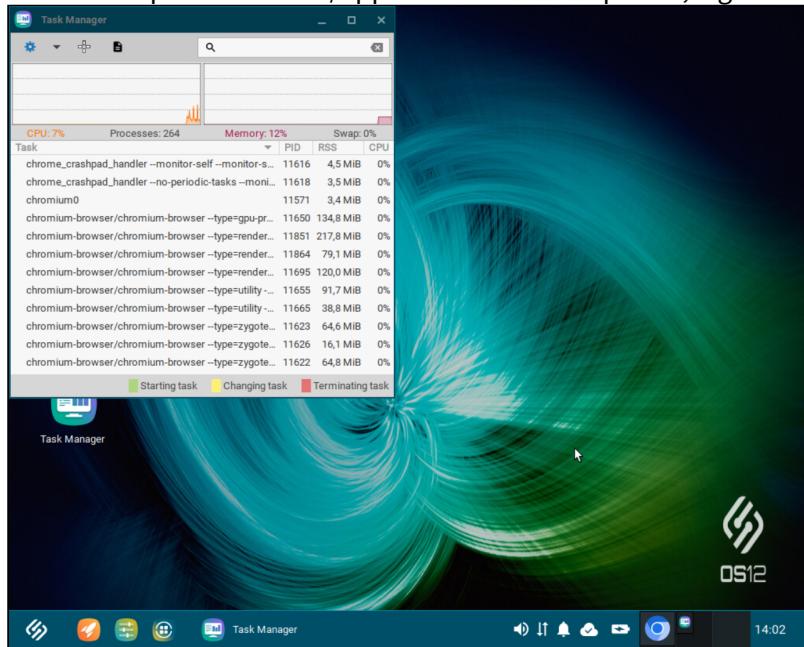
2. In the Pager panel in the taskbar, navigate to another workspace, e.g. Workspace 2, and click it.



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, System, and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Settings, Display Configurator, Desktop (with sub-options: Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager, Start Menu, In-Session Control Bar, Language), Screenlock / Screensaver (with sub-options: Hotkeys, Input, Commands). The "Start Menu" option is selected and highlighted with a yellow bar at the bottom of the sidebar. The main content area is titled "Options in Start Menu" and lists five configuration items, each with a circular refresh icon and a checked checkbox: "Screenlock" (checked), "Show Shutdown menu button" (checked), "System tab" (checked), "About" (checked), and "Show current user name in About, Application Launcher and start menu" (checked). At the bottom right of the content area are three buttons: "Close" (with an X icon), "Save" (with a checkmark icon), and "Save and Close" (with a checkmark and a save icon).

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)

- i** 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\(see page 282\)](#)
 - Enable local logon under **Security > Logon > Active Directory/Kerberos**. For details, see [Active Directory/Kerberos\(see page 275\)](#)



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Settings, Display Configurator, Desktop (expanded to show Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager, Start Menu, and In-Session Control Bar, which is selected and highlighted in orange), Language, Screenlock / Screensaver, Hotkeys, and Input. The main content area shows two configuration items: "Use in-session control bar in all supported sessions" (with a checked checkbox) and "Start Monitor" (set to "Automatic"). At the bottom are "Close", "Save" (with a checkmark), and "Save and Close" buttons.

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**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface" (which is highlighted in yellow), "Network", "Devices", "Security", and "System". To the right of the tabs are search and settings icons. The left sidebar contains a tree view with categories like "Display Settings", "Display Configurator", "Desktop", "Language" (which is selected and highlighted in orange), "Screenlock / Screensaver", "Hotkeys", "Input", and "Commands". The main content area displays language configuration options:

- Language: English
- Keyboard layout: German
- Show indicator in taskbar:
- Input language: Follows Keyboard layout
- Standards and formats: Follows Input language

At the bottom right are buttons for "Close", "Save", and "Save and Close".

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\(see page 102\)](#).
- ⓘ The look of the taskbar on the locked screen can be configured under **Screenlock / Screensaver > Taskbar**. For details, see [Taskbar\(see page 105\)](#).

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

The screenshot shows the 'User Interface' tab selected in the top navigation bar. The 'Screenlock / Screensaver' option is highlighted in the left sidebar. The main panel displays session settings, including a session name field set to 'Screenlock'. Below this, a section titled 'Starting Methods for Session' lists several options, each with a refresh icon and an info icon:

- Start Menu
- Start Menu's System tab
- Application Launcher

At the bottom right of the panel are three buttons: 'Close', 'Save', and 'Save and Close'.

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\(see page 373\)](#).

- [Options\(see page 102\)](#)



- Taskbar(see page 105)
- Screensaver(see page 108)



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar has a tree view with categories like Display Settings, Display Configurator, Desktop, Language, and Screenlock / Screensaver. Under Screenlock / Screensaver, "Options" is selected and highlighted in yellow. Other items in this list include Taskbar, Screensaver, Hotkeys, Input, and Commands. The main content area shows three configuration groups. The first group has a checked checkbox for "Start automatically" and a "Timeout" input field set to "5". The second group has a checked checkbox for "Require password to unlock (screenlock)" and an unchecked checkbox for "Different screenlock timeout", with a "Screenlock timeout" input field also set to "5". The third group has an unchecked checkbox for "Allow administrator password". At the bottom right are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

<input checked="" type="checkbox"/>	Start automatically
<input type="text" value="5"/>	Timeout
<input checked="" type="checkbox"/>	Require password to unlock (screenlock)
<input type="checkbox"/>	Different screenlock timeout
<input type="text" value="5"/>	Screenlock timeout
<input type="checkbox"/>	Allow administrator password

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 275). The authentication methods can be configured under **Security > Logon**. For more information, see [Logon](#)(see page 271). (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 267).
- 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)

- i** 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 108).

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories: Display Settings, Display Configurator, Desktop, Language, Screenlock / Screensaver (which is expanded), Options, Taskbar (which is selected and highlighted in yellow), Screensaver, Hotkeys, Input, and Commands. The main content area is titled "Taskbar settings for the login dialog". It contains a table with six rows, each with a refresh icon and a checkbox. The first five rows have checked boxes, while the last one is unchecked. To the right of each row is an information icon. At the bottom of the content area are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

	<input checked="" type="checkbox"/> Show taskbar in login screen	
	<input checked="" type="checkbox"/> Show clock	
	<input checked="" type="checkbox"/> Show keyboard layout switcher	
	<input type="checkbox"/> Show on-screen keyboard button	
	<input type="checkbox"/> Start on-screen keyboard automatically	
	<input type="checkbox"/> Show reboot button	

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)

- i** There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, the icons appear automatically if **Enable tray icon** is activated under:
- **Network > LAN Interfaces > Interface 1 / Interface 2 / Wireless**
 - **Network > Mobile Broadband**
 - **Network > VPN**

The network connection icons in the login dialog and on the locked screen serve for information purposes only and thus are inactive on clicking, except for the Wi-Fi icon.

The Wi-Fi icon invokes a dialog for turning Wi-Fi on/off, or the Wireless Manager in case it is activated under **Network > LAN Interfaces > Wireless**. For more information, see [Switching the Wi-Fi Connection Off or On\(see page 167\)](#) and [Wireless Manager\(see page 165\)](#).



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 102).

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

A screenshot of the IGEL Setup application window titled "IGEL Setup". The left sidebar shows navigation categories: Accessories, User Interface (selected), Network, Devices, Security, and System. Under "User Interface", the "Screensaver" option is highlighted. The main panel displays screensaver settings:

- Screen background color: Hex code #000000, with a color preview square and a color selector icon.
- Enable image display: A checked checkbox with an info icon.
- File for screensaver logo: An empty text input field with an info icon.
- One image per monitor: A checked checkbox with an info icon.
- Image duration: A text input field containing the value "10" with an info icon.
- Image display mode: A dropdown menu set to "Small-sized hopping" with an info icon.

At the bottom are three buttons: "Close", "Save", and "Save and Close".

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.

- i** 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**

 A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and refresh icons. The left sidebar has sections: Display Settings, Display Configurator, Desktop, Language (with a dropdown menu for Screenlock / Screensaver, Options, Taskbar, and Screensaver), and Hotkeys (which is also selected and highlighted in yellow). Under Hotkeys, there are sub-options: Input and Commands. The main content area is titled "Hotkeys" and contains a table with columns "Session name" and "Key". The table lists various hotkey definitions. At the bottom of the content area are three buttons: "Close", "Save", and "Save and Close".

Session name	Key
Restart windowmanager	
Logoff	
Sort icons	
Switch focus to next window	Escape
Switch between active windows using Task Switc...	Tab
Switch between active windows using Task Switc...	Tab
Switch focus to next window (alternative)	Up
Switch focus to next window (reverse order)	Down
Open start menu	Super_L
Open start menu (alternative)	Super_R

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 114)
- [Additional Keyboard Layouts](#)(see page 116)
- [Mouse](#)(see page 119)
- [Touchpad](#)(see page 123)
- [Touchscreen](#)(see page 131)



Keyboard

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are a search icon and a gear icon. The left sidebar has a tree view with categories: Display Settings, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded), Keyboard (selected and highlighted in orange), Additional keyboard layouts, Mouse, Touchpad, Touchscreen, and Commands. The main content area shows keyboard configuration options. At the top, there's a dropdown for "Keyboard layout" set to "German". Below it is a checkbox for "Enable dead keys" which is checked. Under "Keyboard type", it says "Default". There's also a checkbox for "Show indicator in taskbar" which is unchecked. At the bottom of the main content area are two sliders: "Repeat delay" (set to 660) and "Repeat rate" (set to 40). At the very bottom are three buttons: "Close", "Save", and "Save and Close".

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 135).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are a search icon and a settings gear icon. The left sidebar has a tree view with categories: Display Settings, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded), Keyboard (selected), Additional keyboard layouts (selected and highlighted in orange), Mouse, Touchpad, Touchscreen, and Commands. The main content area is titled "Layout 1". It contains five sections: "Enable this layout" (with a checked checkbox), "Keyboard layout" (set to English(US)), "Enable dead keys" (unchecked), "Hotkey" (empty field), and "Modifiers" (set to None). At the bottom are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

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**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The "User Interface" tab is selected. On the left, a sidebar menu is open under the "Input" section, with "Mouse" selected. The main pane displays various mouse configuration options. These include:

- Left-handed mode:** A checkbox labeled "Left-handed mode" with an information icon.
- Natural scroll:** A checkbox labeled "Natural scroll" with an information icon.
- Emulate 3 Button Mouse:** A checkbox labeled "Emulate 3 Button Mouse" with an information icon.
- Emulate Timeout:** A numeric input field set to "50" with up and down arrows.
- Hide Cursor:** A checkbox labeled "Hide Cursor" with an information icon.
- Idle Time for visible Cursor:** A numeric input field set to "1" with up and down arrows.
- Pointer Speed:** A slider control with a scale from 0 to 1000, currently set to 50.

At the bottom right of the main pane are three buttons: "Close", "Save", and "Save and Close".

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.

- i** 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**

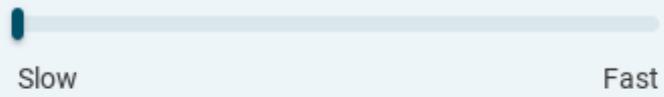
Sets the direction of the screen movement when scrolling with the mouse. In IGEL Setup, you can configure this through **Natural scroll**.



Mouse & Touchpad

Primary Button Left Right

Pointer Speed



MOUSE

TOUCHPAD

Double-click Speed

click to test

Slow

Fast



Scrolling Direction

Traditional Natural





Touchpad

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

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in blue), Network, Devices, Security, and System. Below the tabs is a search bar and a refresh button. The left sidebar contains a tree view of configuration categories: Display Settings, Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded), Keyboard, Additional keyboard layouts, Mouse, Touchpad (selected and highlighted in blue), Touchscreen, and Commands. The main content area shows settings for the selected "Touchpad" category. There are several configuration items with checkboxes and dropdown menus: "Enable Touchpad on Boot" (checked), "Hotkey" (unchecked), "Modifiers" (set to "None"), "Key" (empty input field), "Natural Scroll" (unchecked), "Custom configuration" (unchecked), "Tapping Mode" (set to "With tapping"), and "Min Speed" (a slider set between 0.1 and 1). At the bottom right are buttons for "Close", "Save", and "Save and Close".

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**.

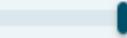
- **Palm Detection**

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**.



Mouse & Touchpad

Enabled

Touchpad Sensitivity  A horizontal slider with a blue dot indicating the current setting, positioned between the labels "Slow" and "Fast".

Slow Fast

Scrolling Direction Traditional Natural

Scrolling Method Two Finger Edge

Tap To Click

Palm Detection

A dark blue taskbar at the bottom of the screen showing several icons: a speaker, a circular progress bar with a red outline, a signal strength icon, a monitor icon, a mail icon, a cloud icon, and a bell icon. The time "11:00" is also displayed on the right side of the taskbar.

- Scrolling(see page 127)
- Advanced(see page 129)



Scrolling

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

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are a search icon and a gear icon. The left sidebar has a tree view with categories like Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded to show Keyboard, Additional keyboard layouts, Mouse), Touchpad (selected, expanded to show Scrolling, Advanced), Touchscreen, Commands, and Logoff. The main content area shows settings for the selected "Scrolling" category under "Touchpad". It includes three sections: 1) Vertical scroll (checkbox checked, slider at 25), 2) Two finger vertical scroll (checkbox unchecked), and 3) Horizontal scroll (checkbox unchecked). Below these are sections for Horizontal scroll speed (slider at 25) and Two finger horizontal scroll (checkbox unchecked). At the bottom right are buttons for Close, Save, and Save and Close.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are a search icon and a gear icon. The left sidebar has a tree view with categories: Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded), Keyboard, Additional keyboard layouts, Mouse, Touchpad (expanded), Scrolling (selected), Advanced (highlighted in orange), Touchscreen, Commands, and Logoff. The main content area shows scrollable lists of touchpad features. Under "Advanced", there are two sections: "Circular scroll trigger:" with a dropdown menu set to "All Edges", and a list of checkboxes. The checkboxes are: "Corner coasting" (unchecked), "Circular scrolling" (unchecked), "Tap and drag gesture" (checked), "Locked drags" (unchecked), and "Palm detect" (unchecked). At the bottom right of the content area are three buttons: "Close", "Save", and "Save and Close".

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 begin 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 134).

For information on how to configure an on-screen keyboard, see [On-screen Keyboard](#)(see page 135).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (which is expanded to show Keyboard, Additional keyboard layouts, Mouse, Touchpad, and Touchscreen), Touchscreen Calibration, On-screen keyboard, and Commands. The "Touchscreen" item under "Input" is currently selected and highlighted in orange. The main content area shows several configuration options: "Enable touchscreen" (with a checked checkbox), "Touchscreen type" set to "EvTouch (USB)" (with a dropdown menu), "Touchscreen already calibrated" (with an unchecked checkbox), "Swap X and Y values" (with an unchecked checkbox), "Minimal X value" set to "0" (with an input field), and "Maximal X value" (which is not visible in the screenshot). At the bottom are three buttons: "Close", "Save", and "Save and Close".

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 134)
- [On-screen Keyboard](#)(see page 135)



Touchscreen Calibration

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar contains a tree view of configuration categories: Display Configurator, Desktop (with Language), Screenlock / Screensaver (with Hotkeys), Input (expanded to show Keyboard, Additional keyboard layouts, Mouse, Touchpad, Touchscreen, and On-screen keyboard), Commands, and a section for Starting Methods for Session. The "Touchscreen Calibration" option under Input is currently selected and highlighted with a yellow background. In the main panel, there is a "Session name" field containing "Touchscreen Calibration". Below it is a section titled "Starting Methods for Session" with four items: "Start Menu" (unchecked), "Menu folder" (unchecked), "Start Menu's System tab" (checked), and "Application Launcher" (unchecked). At the bottom of the main panel are three buttons: "Close", "Save", and "Save and Close".

The screenshot shows the "User Interface" tab selected in the top navigation bar. The left sidebar lists various input-related configurations. The "Touchscreen" section is expanded, and "Touchscreen Calibration" is selected, indicated by a yellow highlight. In the main pane, a session name "Touchscreen Calibration" is entered, and the "Starting Methods for Session" section shows the "Start Menu's System tab" option is checked.

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view of settings: Display Configurator, Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded), Keyboard, Additional keyboard layouts, Mouse, Touchpad, Touchscreen (expanded), Touchscreen Calibration, On-screen keyboard (selected and highlighted in yellow), and Commands. The main content area shows a "Session name" field with "On-screen keyboard" entered. Below it is a section titled "Starting Methods for Session" with four items: "Start Menu" (unchecked), "Menu folder" (unchecked), "Start Menu's System tab" (unchecked), and "Application Launcher" (unchecked). At the bottom are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

- [Appearance](#)(see page 136)
- [Application Integration](#)(see page 138)



Appearance

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

- (i) The layout for the normal keyboard is used for the on-screen keyboard.

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view of settings: Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded to show Keyboard, Additional keyboard layouts, Mouse, Touchpad, and Touchscreen), Touchscreen Calibration, On-screen keyboard (expanded to show Appearance, Application Integration), and Commands. The "Appearance" option under "On-screen keyboard" is selected and highlighted in yellow. The main content area shows four configuration options with checkboxes:

	<input checked="" type="checkbox"/> Show Function Keys	
	<input checked="" type="checkbox"/> Show Navigation Keys	
	<input type="checkbox"/> Show Numpad	
	<input type="checkbox"/> Enable switching to alternative layout	

At the bottom right are buttons for Close, Save, and Save and Close.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface (which is selected and highlighted in yellow), Network, Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Desktop, Language, Screenlock / Screensaver, Hotkeys, Input (expanded to show Keyboard, Additional keyboard layouts, Mouse, Touchpad, and Touchscreen), Touchscreen Calibration, On-screen keyboard (expanded to show Appearance and Application Integration), and Commands. The "Application Integration" item under On-screen keyboard is currently selected and highlighted in blue. The main content area shows "Taskbar settings for the login dialog" with two options: "Show on-screen keyboard button" (unchecked) and "Start on-screen keyboard automatically" (unchecked). Below that is "Taskbar settings when the screenlock is active" with similar two options. At the bottom is "On-screen keyboard toggle button" with a small preview image. At the bottom right are three buttons: "Close" (with a red X), "Save" (with a checkmark), and "Save and Close" (with a checkmark and a circular arrow).

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**

The screenshot shows the 'IGEL Setup' application window with the 'User Interface' tab selected. In the left sidebar, under the 'Commands' category, 'Shutdown menu' is highlighted. The main panel displays a session configuration for 'Shutdown menu'. It includes a 'Session name' field and a list of 'Starting Methods for Session' with checkboxes for 'Start Menu', 'Menu folder', 'Start Menu's System tab', 'Application Launcher', 'Application Launcher's System tab', 'Desktop', and 'Desktop folder'. At the bottom are 'Close', 'Save', and 'Save and Close' buttons.

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 324).
- **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 373).



Quick Access

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

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface" (which is selected and highlighted in yellow), "Network", "Devices", "Security", "System", and "Apps", along with search and settings icons. The left sidebar contains a tree view of configuration categories: Accessories (Display Settings, Display Configurator), Desktop (Background (1st Monitor), Taskbar, Taskbar Background, Taskbar Items, Pager, Start Menu, In-Session Control Bar), Language, Screenlock / Screensaver (Hotkeys, Input), Commands (Shutdown menu, Quick access, Sort icons, Restart windowmanager). The "Shutdown menu" node is expanded, and "Quick access" is selected, indicated by a yellow highlight bar. The main content area shows two sections: "Start Menu options" with a checked checkbox for "Show Shutdown menu button" and "Application Launcher options" with an unchecked checkbox for "Hide Shutdown menu button". At the bottom are buttons for "Close", "Save", and "Save and Close".

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](#)(see page 144)
- [Wireless](#)(see page 154)
- [Mobile Broadband](#)(see page 173)
- [Computer Name](#)(see page 176)
- [DHCP Options](#)(see page 177)
- [DNS](#)(see page 181)
- [VPN](#)(see page 183)
- [SCEP Client \(NDES\)](#)(see page 205)
- [Default Gateway](#)(see page 213)
- [Hosts](#)(see page 217)
- [Network Drives](#)(see page 219)
- [Proxy](#)(see page 226)



LAN Interfaces

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

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

The screenshot shows the 'IGEL Setup' application window with the 'Network' tab selected. Under the 'LAN Interfaces' section, 'Interface 1' is currently selected. The configuration options include:

- Activate default interface (Ethernet)**: A checked checkbox.
- Get IP from DHCP server** and **Specify an IP address**: Two radio button options, with 'Get IP from DHCP server' selected.
- IP address** and **Network mask**: Input fields for network configuration.
- IPv6 configuration**: A dropdown menu set to **Compatibility mode**.
- Network link type**: A dropdown menu set to **Auto Sense**.
- Force auto-negotiation**: An unchecked checkbox.

At the bottom right are three buttons: **Close**, **Save**, and **Save and Close**.

(i) Predictable Network Interface Names (PNINs)

The names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)⁴. 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.

⁴ <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 177).

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](#).⁵
- **DHCPv6:** IPv6 configuration using DHCPv6 if router advertisements are not available.
This is mentioned in [RFC 4862 Section 5.5.2](#).⁶

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)

LAN Tray App

Based on the status of the LAN connection, one of the following icons is shown in the taskbar. Clicking the icon opens the LAN tray app. The app displays details about the network connection and provides an option to quickly connect to and disconnect from LAN networks.

Taskbar Icon	LAN Status
	Connected
	No connection
	Connected, but no internet
	Connecting
	Disconnected by user
	Connection error

⁵ <https://tools.ietf.org/html/rfc4861>

⁶ <https://tools.ietf.org/html/rfc4862#section-5.5.2>



- [Authentication](#)(see page 148)
- [Wake On LAN](#)(see page 152)



Authentication

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

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces (selected), Interface 1 (selected), Authentication (highlighted in orange), Wake On Lan, Interface 2, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main content area shows the "Authentication" configuration for Interface 1. It includes fields for: "Enable IEEE 802.1x Authentication" (checkbox), "EAP Type" (dropdown set to PEAP), "Anonymous Identity" (text input field), "Auth Method" (dropdown set to MSCHAPV2), "Validate Server Certificate" (checkbox checked), "CA Root Certificate" (text input field), and "Identity" (text input field). At the bottom are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

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

- i** 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 205).

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.

i 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)

i 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`

i 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_tls1_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](#).

(i) 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**

The screenshot shows the IGEL Setup interface with the Network tab selected. In the left sidebar, under LAN Interfaces, the 'Wake On Lan' option is highlighted. The main pane displays a list of wake-on options, each with a circular refresh icon and a checkbox. The 'Wake on magic packet' checkbox is checked, while the others are unchecked. At the bottom right are buttons for Close, Save, and Save and Close.

Wake On Option	Status
Wake on magic packet	<input checked="" type="checkbox"/>
Wake on ARP packet	<input type="checkbox"/>
Wake on broadcast message	<input type="checkbox"/>
Wake on multicast message	<input type="checkbox"/>
Wake on physical activity	<input type="checkbox"/>
Wake on unicast message	<input type="checkbox"/>

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.

- ⓘ If you have to frequently switch between LAN and WLAN networks, it is useful to activate **Enable Wi-Fi automatic switch**.
For the Wi-Fi tray icon to be displayed, **Show wifi connection status tray icon on desktop** needs to be enabled under **User Interface > Desktop > Taskbar Items**. For details, see [Taskbar Items\(see page 86\)](#).

Menu path: **Network > Wireless**

The screenshot shows the 'IGEL Setup' application window with the 'Network' tab selected. On the left, a sidebar lists network-related settings: LAN Interfaces, Wireless (which is currently selected and highlighted in yellow), Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main panel contains several configuration fields:

- Activate wireless interface:** A checkbox labeled with a refresh icon and a checked state.
- IP Configuration:** A section with two radio button options: "Get IP from DHCP server" (selected) and "Specify an IP address". Below these are fields for "IP address" and "Network mask", each with a refresh icon and an information icon.
- IPv6 configuration:** A dropdown menu set to "Compatibility mode".
- Enable Wi-Fi automatic switch:** A checkbox labeled with a refresh icon and an unchecked state.

At the bottom right of the main panel are three buttons: "Close" (with an X icon), "Save" (with a checkmark icon), and "Save and Close" (with a disk icon).



You can find details of compatible wireless hardware in the [IGEL Linux 3rd Party Hardware Database](#)⁷.

(i) Predictable Network Interface Names (PNINs)

The names of Ethernet and WLAN interfaces are predictable network interface names (PNINs), see [Predictable Network Interface Names](#)⁸. 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 177).

Specify IP address

The IP address and the network mask are entered manually.

⁷ <https://www.igel.com/linux-3rd-party-hardware-database/>

⁸ <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/>



IP address

IP address of the endpoint device

Network mask

Network mask of the endpoint device

IPv6 configuration:

- **Compatibility mode:** Behavior of earlier firmware versions. (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](#)⁹.
- **DHCPv6:** IPv6 configuration using DHCPv6 if router advertisements are not available.
You will find further information in [RFC 4862 Section 5.5.2](#)¹⁰.

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)

- i** 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 more information on the toggle button, see [Switching the Wi-Fi Connection Off or On](#)(see page 167).

-
- [Wi-Fi Networks](#)(see page 157)
 - [Wireless Regulatory Domain](#)(see page 163)
 - [Wireless Manager](#)(see page 165)
 - [Switching the Wi-Fi Connection Off or On](#)(see page 167)
 - [Wi-Fi Tray App](#)(see page 169)

⁹ <https://tools.ietf.org/html/rfc4861>

¹⁰ <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 [Wi-Fi Tray App](#)(see page 169).

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

A screenshot of the IGEL Setup software interface. The window title is "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface", "Network" (which is highlighted in yellow), "Devices", "Security", "System", and "Apps", along with search and settings icons. The left sidebar contains a tree view of network configuration options: LAN Interfaces, Wireless (selected, expanded), Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxv. The main content area is titled "Wi-Fi networks" and displays a table with one row: "Wireless Network Name (SSID)" set to "User-defined". Below the table are four icons: a blue square with a white plus sign (+) for creating a new entry, a blue square with a white minus sign (-) for removing the selected entry, a blue square with a white pencil for editing the selected entry, and a blue square with a white copy symbol for copying the selected entry. At the bottom right are buttons for "Close", "Save", and "Save and Close".

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 159).
- For **WPA/WPA2 Enterprise** encryption, see [WPA/WPA2 Enterprise](#)(see page 159).

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 205).
- 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**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for "Accessories", "User Interface", "Network" (which is highlighted in yellow), "Devices", "Security", "System", and "Apps", along with search and settings icons. The left sidebar contains a tree view with categories like LAN Interfaces, Wireless (with sub-options for Wi-Fi networks and Wireless regulatory domain), Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main right panel shows two configuration items: "Wireless regulatory domain" (status: Not configured) and "Location" (status: Not configured). At the bottom are buttons for "Close", "Save", and "Save and Close".

The "Wireless regulatory domain" section is currently selected, indicated by a yellow background and a yellow border around its input field.

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**



Wireless Manager

The Wireless Manager tool allows the user to connect quickly to available wireless networks. This article shows how to use the Wireless Manager in IGEL OS.

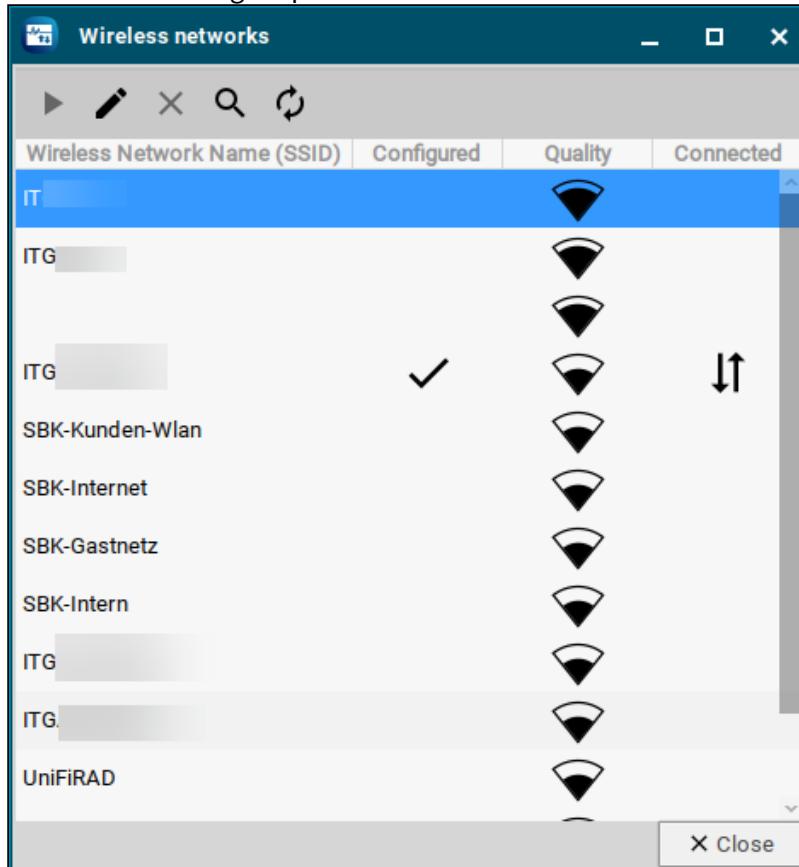
- i** The Wireless Manager is only available from the Wi-Fi tray icon in the login screen or the locked screen. Once the screen is unlocked and the user is logged in, the Wi-Fi tray app can be used for the same purpose. For the description of the tray app, see [Wi-Fi Tray App\(see page 169\)](#).

This is how you can use the Wireless Manager:

1. To bring up the Wireless Manager, click the tray icon for wireless:



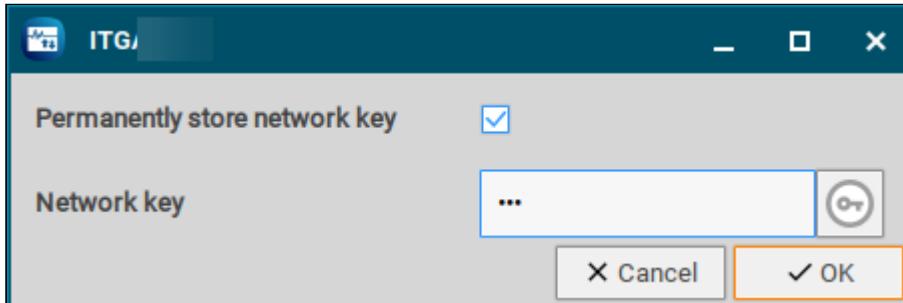
The Wireless Manager opens.





2. Search for available networks.
 - The list of active networks is sorted according to the quality of their signal strength.
 - Previously configured connections are flagged with a tick in the **Configured** column.
 - The connection currently active is likewise flagged with a symbol under **Connected**.

3. Double-click on a network in the list in order to open the entry mask.
You can either **permanently store** the login information or enter it each time you establish a connection to this network.



i Click on the key symbol in order to display the key phrase while you are typing.

4. Click on the **Connect network** button in order to establish the previously configured connection:
The tray icon will change to show the connection quality.
Hidden networks appear in the Wireless Manager with the network name empty or can be defined using the **Search for network** button.
In order to connect to a previously unknown hidden network, you must first enter the SSID before the access data are retrieved:

i If you have configured the available connections, you will no longer need the Wireless Manager in order to establish a connection.

In the context menu for the tray icon, all available networks are listed and can be brought up from here.

5. The IGEL Setup shows all connections configured for the device under **Network > Wireless > Wi-Fi Networks**. For more information, see [Wi-Fi Networks](#)(see page 157).

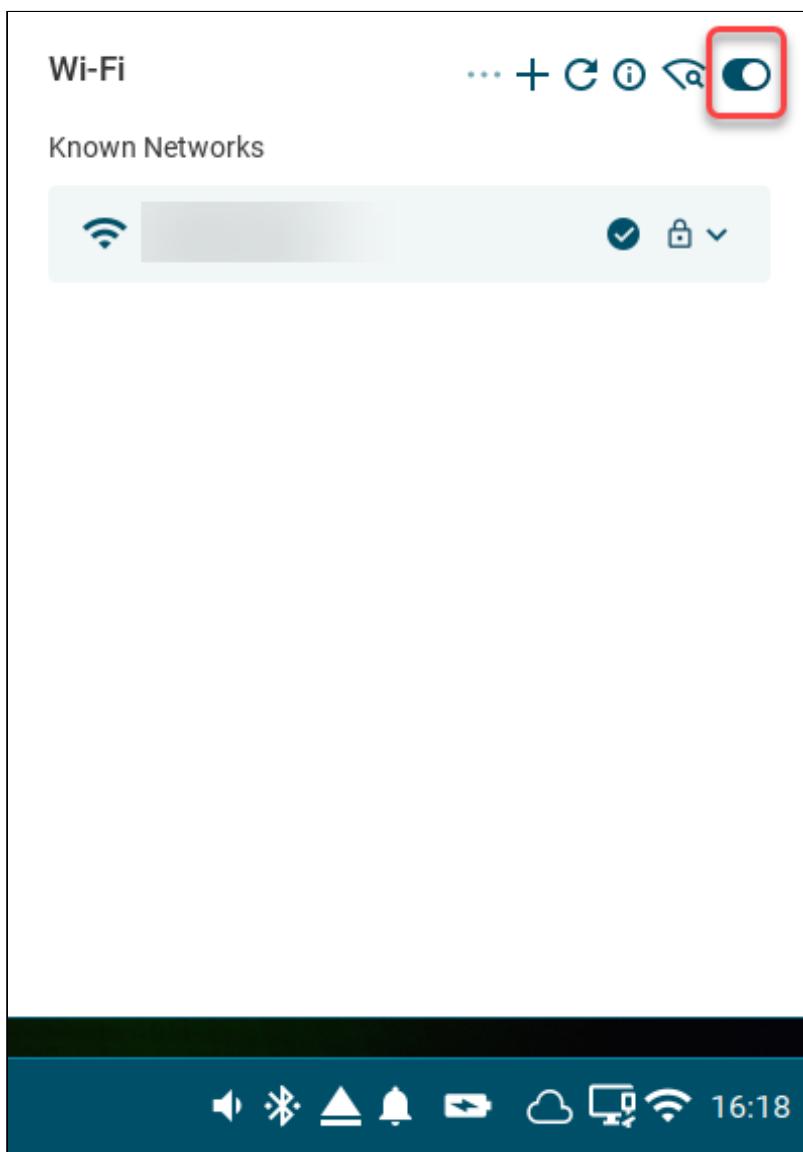


Switching the Wi-Fi Connection Off or On

This article shows how to turn Wi-Fi off or on in IGEL OS. The switch works differently if you are logged in and if the login dialog is displayed or the screen is locked.

Turning Wi-Fi Off or On If You Are Logged In

- ▶ Use the toggle switch of the Wi-Fi tray app to turn Wi-Fi off and on.





- ⓘ Once the toggle switch is used, the **Enable Wi-Fi automatic switch** option under **Network > Wireless** becomes disabled until the reboot of the device. On reboot, the previously configured setting will be restored. For more information, see [Wireless](#)(see page 154).

Turning Wi-Fi Off or On In the Login Dialog or the Locked screen

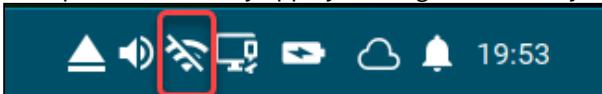
- ▶ To turn Wi-Fi off, click the tray icon  and select **OK** in the **Turn Wi-Fi off** dialog.
- ▶ To turn Wi-Fi on, click  and select **OK** in the **Turn Wi-Fi on** dialog.



Wi-Fi Tray App

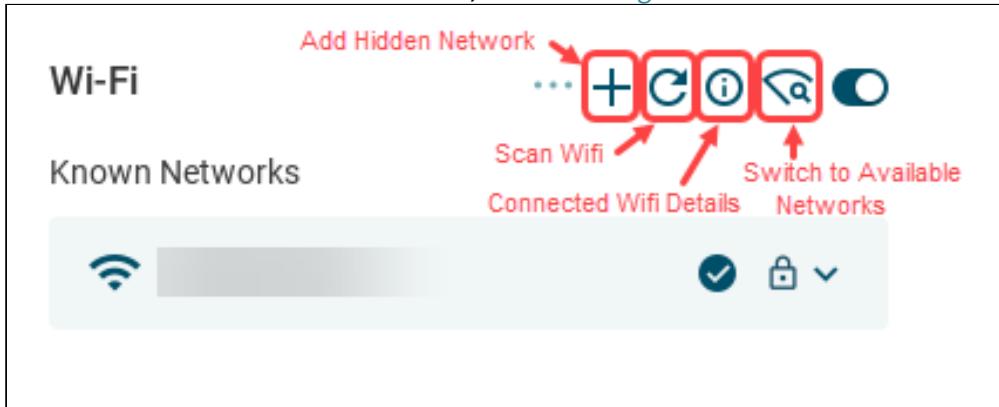
The Wi-Fi tray app allows the user to connect quickly to available wireless networks. This article shows how to establish a Wi-Fi connection using the Wi-Fi tray app in IGEL OS.

- Open the Wi-Fi tray app by clicking the Wi-Fi tray icon:



The Wi-Fi tray app opens. Using the icons at the top of the window, you can:

- 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.
- Switch the Wi-Fi on and off. For details, see [Switching the Wi-Fi Connection Off or On](#)(see page 167).

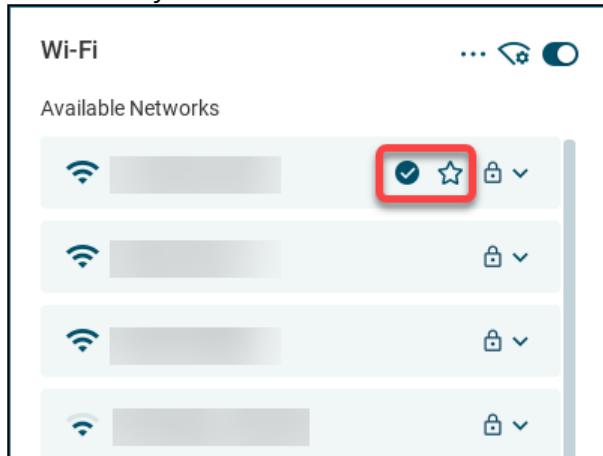


Connect to Available Wi-Fi Networks

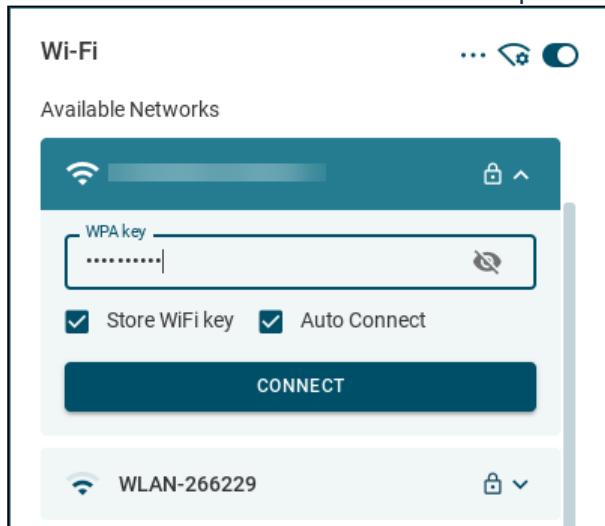
1. Switch to the **Available Networks** list or use the **Scan WiFi** icon to refresh the list.
 - The list of networks is sorted according to the quality of their signal strength.
 - Previously configured networks are marked with a star icon. They are listed in the Known Networks List.



- The currently connected network is marked with a tick icon.



- 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.

- 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 157).

- To disconnect from the connected network, click on the network and click **Disconnect**.



Edit and Delete Known Networks

1. Switch to the **Known Networks** list.

A screenshot of the "Known Networks" section of the IGEL OS device settings. At the top, there's a header with a Wi-Fi icon, three dots, a search icon, and a toggle switch. Below the header, it says "Known Networks". There's a list of networks. The first network is highlighted with a blue bar at the top. It shows a Wi-Fi icon, the network name (partially obscured), a lock icon, and a dropdown arrow. Below this, there's a "WPA key" field containing "*****" with a copy/paste icon and a pencil edit icon. Underneath the key field are two checkboxes: "Store WiFi key" (checked) and "Auto Connect" (unchecked). At the bottom of this card are "DELETE" and "SAVE" buttons. Below this card, another network entry is partially visible with a lock icon and a dropdown arrow.

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

1. Switch to the **Known Networks** list.



2. Click the **Add Hidden Network** icon at the top of the window.

A screenshot of a Wi-Fi configuration window titled "Wi-Fi". At the top right are three icons: a gear, a refresh, and a power switch. Below the title is a section for "Known Networks". Under "Encryption Type", there are two radio buttons: "OPEN" (selected) and "WPA". Below these are fields for "SSID" and "WPA key", each with a "copy" icon. At the bottom are two checked checkboxes: "Store WiFi key" and "Auto Connect", followed by a large "CONNECT" button.

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 157).

5. To disconnect from the connected network, click on the network in the **Available Networks** list and click **Disconnect**.



Mobile Broadband

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

Menu path: **Network > Mobile Broadband**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. Below the tabs is a search bar and a settings gear icon. On the left is a sidebar with the following items: LAN Interfaces, Wireless, Mobile Broadband (which is selected and highlighted in orange), Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main right panel shows configuration fields for "Mobile Broadband": "Enable Mobile Broadband" (checkbox), "Device type" (dropdown set to "Modem"), "Number" (text input field), "User name" (text input field), "Password" (text input field), "New password" (text input field), "New password (repeated)" (text input field), and "APN" (text input field). At the bottom are buttons for "Close", "Save", and "Save and Close".

The screenshot shows the "Mobile Broadband" configuration page. It includes fields for enabling mobile broadband, selecting a device type (Modem), and entering connection details like APN and user credentials. The "Save and Close" button is visible at the bottom.

- ⚠ 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.
 The mobile broadband network cannot be used. (Default)

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.

Number

Access number for your network connection. If you do not know the access number, ask your mobile communications operator for it.



User name

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

Password

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

APN

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

Network ID

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

PIN

PIN for the SIM card used.

Enable tray icon

The current status of the network connection is shown with the symbol or . (Default)

Enable context menu

If you click on or , a context menu can be opened. (Default)

Enable network info dialog

Via the context menu, you can bring up detailed information regarding the network connection. (Default)

Enable mobile broadband configuration dialog

Via the context menu, you can open a configuration dialog in order to change the access data.

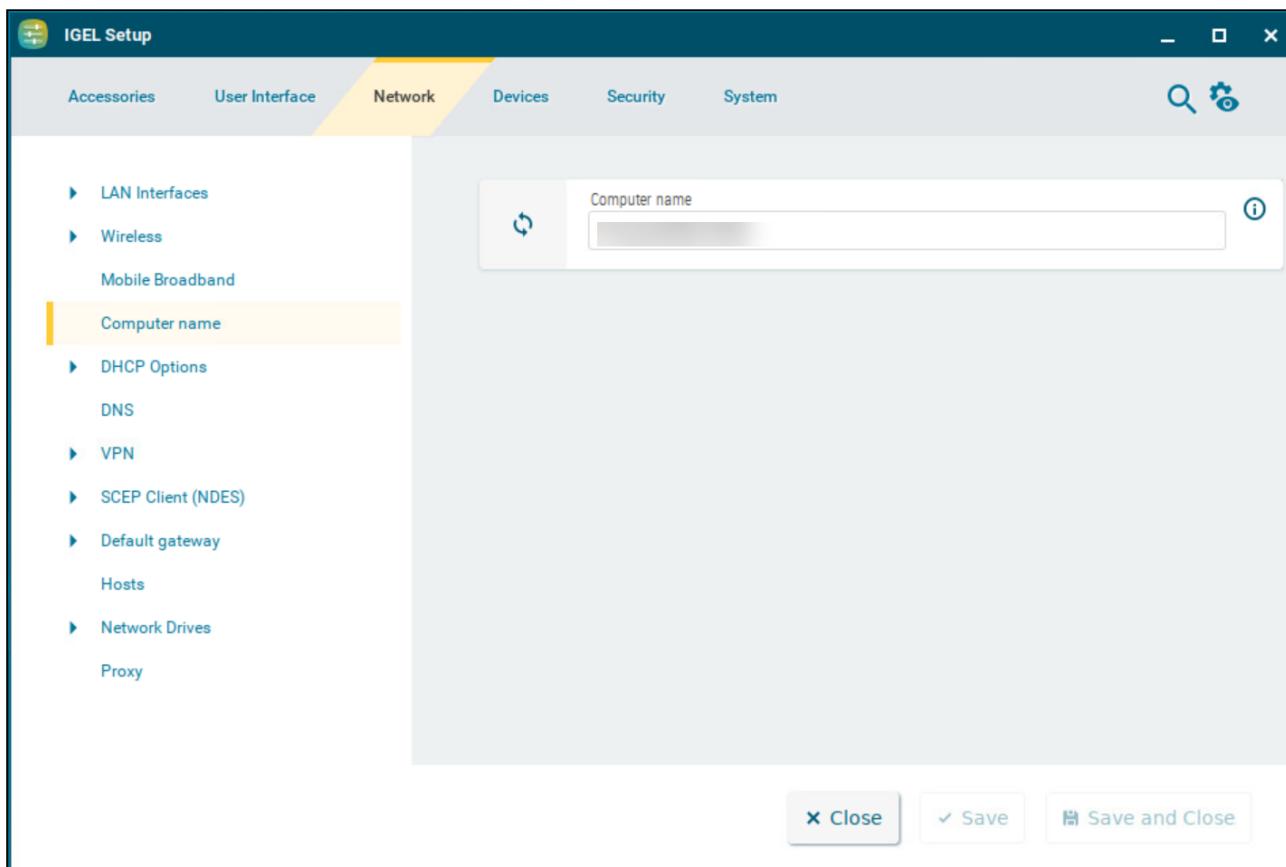
The configuration dialog cannot be opened. (Default)



Computer Name

This article shows how to configure the local name of the device in IGEL OS.

Menu path: **Network > Computer name**



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.



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options (which is expanded to show Standard Options and Custom Options), DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main content area is titled "List of standard opti...". It has two columns: "Activated" and "Option Name". There is a header row with icons for refresh, search, edit, delete, and add. At the bottom of the content area are buttons for "Close", "Save", and "Save and Close".

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](#)¹¹.

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**

¹¹ <https://tools.ietf.org/html/rfc2132>



A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The main content area on the left shows a tree view of network configuration options: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options (expanded to show Standard Options and Custom Options), DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The "Custom Options" tab under DHCP Options is currently selected. On the right, there is a table titled "List of custom options" with four columns: Activated, Option Name, Code, and Data Type. Below the table are four buttons: "Close", "Save", "Save and Close", and a plus sign icon for adding new entries. The "Save and Close" button is highlighted with a blue border.

i 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**

A screenshot of the IGEL Setup software interface. The window title is "IGEL Setup". The top navigation bar includes "Accessories", "User Interface", "Network" (which is highlighted in yellow), "Devices", "Security", and "System". Below the navigation bar is a search bar and a gear icon. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS (which is selected and highlighted in orange), VPN (with Open VPN), SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main content area is titled "DNS". It contains several configuration fields with "refresh" icons: "Enable DNS" (unchecked), "Default domain" (empty input field), "Nameserver" (empty input field), and another "Nameserver" (empty input field). Below this is a section titled "Advanced Options" with two more fields: "Manually overwrite DHCP settings" (unchecked) and "Dynamic DNS registration" (unchecked). At the bottom right are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

The screenshot shows the "DNS" configuration page in the IGEL Setup application. The "Network" tab is active. On the left, the "DNS" option under "DHCP Options" is selected. The main pane displays fields for enabling DNS, setting a default domain, and specifying nameservers. Advanced options like manual DHCP overwrite and dynamic DNS registration are also shown. Buttons at the bottom allow saving changes.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar is a tree view with nodes like LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN (which is selected and highlighted in yellow), SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main right panel contains three configuration items, each with a circular refresh icon and a checked checkbox: "Enable tray icon", "Enable context menu", and "Enable network info dialog". At the bottom right of the panel are buttons for "Close", "Save", and "Save and Close".

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 185)



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.

- i** 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 39).

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

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is selected and highlighted in yellow), Devices, Security, and System. On the far right of the top bar are a magnifying glass icon for search and a gear icon for settings. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN (expanded to show OpenVPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy). The main content area shows configuration for the selected "OpenVPN" session. It includes two checkboxes: "Enable autostart during boot" and "Restart connection when disconnected", both currently unchecked. Below these is a dropdown menu labeled "Autostart Session ID" set to "None". At the bottom of this section is a "Session Name" input field which is empty. To the right of the main configuration area is a "Session List" panel titled "OpenVPN Session List" with a table header "Session Name". There are three buttons at the bottom right of the configuration area: "Close", "Save", and "Save and Close".

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]**

The screenshot shows the 'IGEL Setup' application interface. The top navigation bar includes 'Accessories', 'User Interface', 'Network' (which is highlighted in yellow), 'Devices', 'Security', 'System', and 'Apps'. A search bar and a gear icon are also present. The left sidebar has sections for 'DNS', 'VPN' (which is expanded to show 'Open VPN' and 'OpenVPN Connection'), 'IPv4', 'Options', 'Proxy', 'Route 0', 'Route 1', 'Route 2', 'Session', 'TLS-Options', 'SCEP Client (NDES)', and 'Default gateway'. The main panel shows a 'Session name' field containing 'OpenVPN Connection'. Below it is a section titled 'Starting Methods for Session' with four entries: 'Start Menu' (checked), 'Menu folder' (unchecked), 'Start Menu's System tab' (unchecked), and 'Application Launcher' (checked). At the bottom are three buttons: 'Close', 'Save', and 'Save and Close'.



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 267).

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`
- = `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 + Windows` = `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 190)
 - [Options](#)(see page 192)
 - [Proxy](#)(see page 195)
 - [Route](#)(see page 197)
 - [Session](#)(see page 199)
 - [TLS-Options](#)(see page 203)



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**

A screenshot of the IGEL Setup software interface. The top navigation bar includes tabs for Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network configurations: Open VPN (selected), OpenVPN Connection (selected), IPv4 (selected), Options, Proxy, Route 0, Route 1, Route 2, Session, TLS-Options, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main content area displays several configuration options for the selected IPv4 profile. These include: Automatic DNS (checked), Extra nameserver(s) (empty input field), Extra search domains (empty input field), Automatic Routes (checked), and VPN is the default route (checked). Each option has an information icon (i) to its right. At the bottom of the window are buttons for Close, Save, and Save and Close.

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\(see page 197\)](#).



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](#)¹² which is maintained by the OpenVPN project.

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

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network (which is selected), Devices, Security, and System, along with search and settings icons. The left sidebar contains a tree view of network configurations: DNS, VPN (selected), Open VPN (selected), OpenVPN Connection (selected), IPv4, Options (highlighted in yellow), Proxy, Route 0, Route 1, Route 2, Session, TLS-Options, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main right panel displays configuration options for the selected "Options" under "OpenVPN Connection":

- Gateway Port: 1194
- Custom renegotiation interval: 0
- Use LZO data compression
- Protocol used for communication to the host: udp
- Virtual network type: tun
- Use custom tunnel Maximum Transmission Unit (MTU): 0
- UDP fragment size: 0
- Restrict tunnel TCP Maximum Segment Size (MSS)

At the bottom are buttons for Close, Save, and Save and Close.

Gateway port

¹² <https://openvpn.net/index.php/open-source/documentation.html>



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)

i 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.

i 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 192).

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

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network (which is selected and highlighted in yellow), Devices, Security, and System. Below the tabs is a search bar and a settings gear icon. The left sidebar contains a tree view of network configurations: DNS, VPN (selected), Open VPN (selected), OpenVPN Connection (selected), IPv4, Options, and Proxy (highlighted with a yellow bar). Other items like Route 0, Route 1, Route 2, Session, TLS-Options, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and another Proxy entry are also listed. The main right panel displays proxy settings for the selected "Proxy" configuration. It includes fields for "Proxy Type" (set to "None"), "Proxy Address" (empty), "Proxy Port" (set to 0), and a checkbox for "Retry indefinitely when errors occur" (unchecked). Below this is a section for "Proxy user name" (empty), "Proxy Password" (set to "New password"), and "New password (repeated)" (empty). At the bottom are buttons for "Close", "Save", and "Save and Close".

The screenshot shows the "Proxy" configuration screen in the "Network > VPN > OpenVPN > [OpenVPN Connection] > Proxy" section. The "Proxy Type" dropdown is set to "None". The "Proxy Address" and "Proxy Port" fields are empty. The "Proxy user name", "Proxy Password", and "New password (repeated)" fields are also empty. The "Set password" button is visible. At the bottom are "Close", "Save", and "Save and Close" buttons.

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]**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is selected and highlighted in yellow), Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN (selected and expanded), Open VPN (selected and expanded), OpenVPN Connection (selected and expanded), IPv4, Options, Proxy, Route 0 (highlighted in orange), and Route 1. The main content area shows configuration for "Route 0": an "enable" checkbox (unchecked), a radio button for "Network Route" (selected), a "Network/Host IP" input field, a "Network mask" input field, a "Gateway" input field, and a "Metric" input field. At the bottom are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is selected and highlighted in yellow), Devices, Security, and System. On the far right of the top bar are search and settings icons. The left sidebar contains a tree view of configuration categories: DNS, VPN (expanded), Open VPN (expanded), OpenVPN Connection (selected and highlighted in yellow), IPv4, Options, Proxy, Route 0, Route 1, Route 2, Session (highlighted in orange), TLS-Options, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy. The main right panel shows the "Session" configuration settings for an OpenVPN connection. It includes fields for "OpenVPN Server(s)" (empty), "Authentication Type" set to "TLS-Certificates", "Client Certificate file" set to "client.crt", "CA certificate file" set to "ca.crt", "Private key file" set to "client.key", "Private Key password" set to "New password", and "New password (repeated)". There is also a "Set password" button. At the bottom right of the main panel are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

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

- i** 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.

- i** 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.

- i** 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**

The screenshot shows the IGEL Setup interface with the Network tab selected. On the left, the navigation tree is expanded to show the path: DNS > VPN > Open VPN > OpenVPN Connection > TLS-Options. The main panel displays four configuration fields:

- Subject Match:** An empty text input field.
- Remote peer certificate TLS type:** A dropdown menu set to "Do not verify".
- Key file for additional TLS authentication:** A "Browse..." button to select a file.
- tls-auth (Key Direction) / tls-crypt:** A dropdown menu set to "None".

At the bottom right are three buttons: "Close", "Save", and "Save and Close".

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](#)¹³.

Remote peer certificate TLS type

¹³ <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/>



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"`.

i 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](#)¹⁴.

¹⁴ <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)**

A screenshot of the IGEL Setup software interface. The window title is "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES) (which is selected and highlighted in orange), Default gateway, Hosts, Network Drives, and Proxy. The main content area on the right shows a configuration panel for "Manage certificates with SCEP". It includes a checkbox labeled "Manage certificates with SCEP" which is checked. There is also an information icon (i) next to the checkbox. At the bottom right of the content area are three buttons: "Close", "Save", and "Save and Close".

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 \(AD CS\)](#)¹⁵.

¹⁵ <http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx>



- [SCEP Server](#)(see page 207)
- [Certificate](#)(see page 209)
- [Certification Authority](#)(see page 212)



SCEP Server

This article describes the settings required for a SCEP server in IGEL OS.

Menu path: **Network > SCEP Client (NDES) > SCEP Server**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is selected and highlighted in yellow), Devices, Security, and System. On the far right of the top bar are a search icon and a gear icon. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES) (which is expanded and has "SCEP Server" selected), Certificate, Certification Authority, Default gateway, Hosts, Network Drives, and Proxy. The main content area is titled "SCEP Server". It contains several configuration fields with placeholder text and "i" information icons: "SCEP server URL" (placeholder: "http://scepserver.com"), "Proxy server for SCEP requests" (placeholder: "http://proxyserver.com"), "Challenge password" (placeholder: "New password"), "New password (repeated)" (placeholder: "New password (repeated)"), "Certificate renewal period (days)" (placeholder: "30"), and "Certificate expiry check interval (days)" (placeholder: "1"). At the bottom are three buttons: "Close", "Save", and "Save and Close".

SCEP server URL

Proxy server for SCEP requests

Challenge password

New password

New password (repeated)

Certificate renewal period (days)

Certificate expiry check interval (days)

- i** 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)

- i** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar has a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES) (which is expanded to show "SCEP Server", "Certificate" which is selected and highlighted in orange, and "Certification Authority"), Default gateway, Hosts, Network Drives, and Proxy. The main panel on the right is titled "Type of CommonName/SubjectAltName" and has a dropdown menu set to "DNS name". It contains fields for "CommonName/SubjectAltName" (with an info icon), "CommonName/SubjectAltName Suffix" (set to "none"), "Organizational unit" (empty), "Organization" (empty), "Locality" (empty), and "State" (empty). At the bottom are buttons for "Close", "Save", and "Save and Close".

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)**



- i** 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 `A C`.

- i** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES) (which is expanded to show SCEP Server, Certificate, and Certification Authority), Default gateway, Hosts, and Network Drives. The "Certification Authority" item under "SCEP Client (NDES)" is selected and highlighted with a yellow background. The main content area on the right has two input fields: "CA identifier" with a placeholder "CA identifier" and an info icon, and "CA certificate fingerprint (MD5)" with a placeholder "CA certificate fingerprint (MD5)" and an info icon. At the bottom are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway (which is selected and highlighted in yellow), Hosts, Network Drives, and Proxy. The main content area shows the "Default gateway" configuration. It has three fields: "Default gateway" with a checkbox (unchecked) and an info icon; "Default gateway" with a text input field and an info icon; and "Interface" with a text input field and an info icon. At the bottom are "Close", "Save" (with a checkmark), and "Save and Close" buttons.

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](#)¹⁶. 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**.

¹⁶ <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]**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway (which is expanded to show Routing 1, Routing 2, Routing 3, Routing 4, Routing 5, and Hosts), and Hosts. The main panel shows the "Routing" configuration for "Routing 1". It includes fields for "Network/Host IP or Name", "Network mask", "Gateway", and "Interface", each with a refresh icon. There are also radio buttons for "Network Route" and "Host Route". At the bottom are buttons for "Close", "Save", and "Save and Close".

The screenshot shows the "Routing" configuration for "Routing 1". The "Network/Host IP or Name" field is empty. The "Network mask" field is also empty. The "Gateway" field is empty. The "Interface" field is empty. The "Network Route" radio button is selected. The "Host Route" radio button is not selected. There are three information icons (i) next to each of the four input fields.

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



Hosts

This article shows how to configure hosts in IGEL OS. 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.

Menu path: **Network > Hosts**

A screenshot of the IGEL Setup software interface. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts (which is selected and highlighted in orange), Network Drives, and Proxy. The main content area is titled "Host List" and contains a table with columns: IP address, Fully qualified host name, and Short host name. There are three rows in the table, but they are completely blank. Below the table are three buttons: "Close", "Save", and "Save and Close".

Host List

List of configured hosts

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`



Network Drives

The following network drives can be configured in IGEL OS.

- [NFS](#)(see page 220)
- [Windows Drive](#)(see page 223)



NFS

This article shows how to integrate network drives using the Network File System (NFS) in IGEL OS.

Menu path: **Network > Network Drives > NFS**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network configuration options: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives (which is expanded to show NFS, Windows Drive, and Proxy), and a plus sign icon. The main content area is titled "NFS Mount List". It features a table with columns: Enabled, Local Mount Point, Directory Name, and Server. Below the table are four buttons: Close, Save, and Save and Close. The "NFS" entry under Network Drives is currently selected.

NFS Mount List

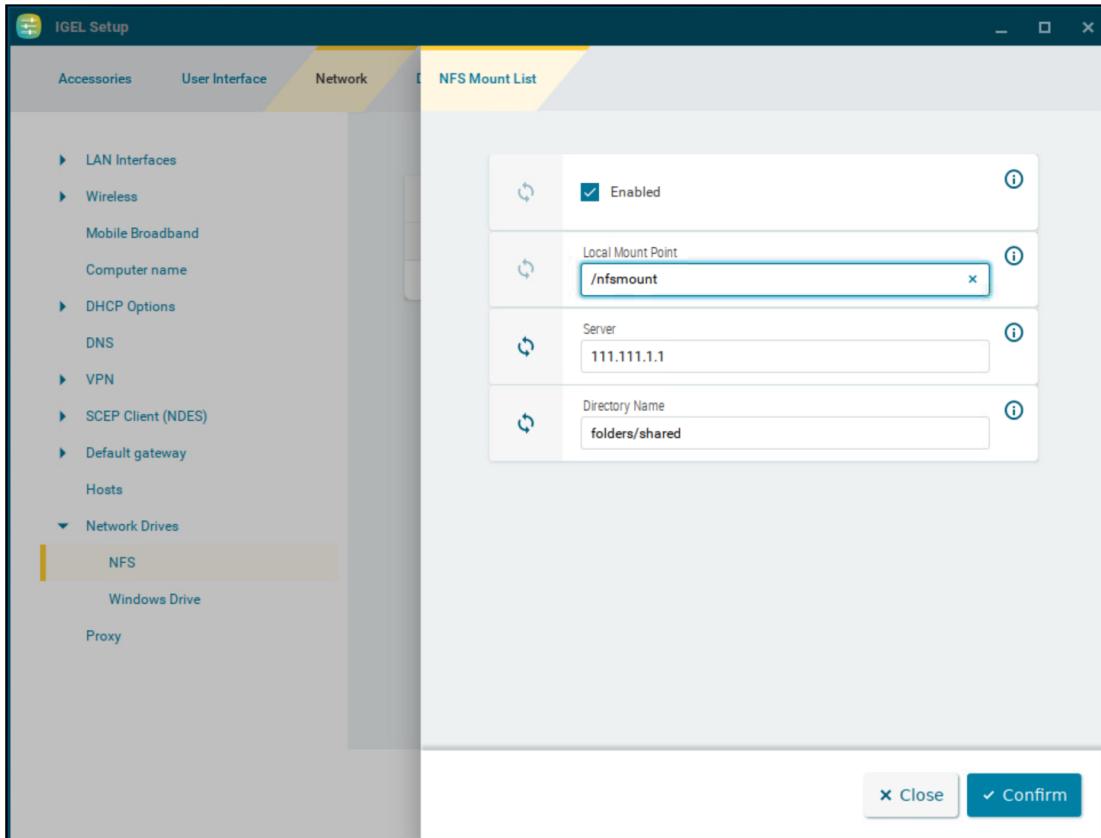
List of integrated network drives

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives (which is expanded to show NFS, Windows Drive, and Proxy), and a plus sign icon. The main content area is titled "SMB Mount List". It has a table with columns: Enabled, Local Mount Point, Server, and Share Name. There are four buttons at the bottom right: "Close", "Save", and "Save and Close".

Enabled	Local Mount Point	Server	Share Name

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:

The screenshot shows the 'SMB Mount List' dialog within the 'IGEL Setup' application. The left sidebar lists various setup categories. The 'Windows Drive' option under 'Network Drives' is selected, highlighted with a yellow bar. The main dialog contains fields for 'Enabled' (checked), 'Local Mount Point' (/smbmount), 'Server' (111.111.1.1), 'Share Name' (shared/folder), 'User name' (username), and 'Password'. A 'Set password' button is present. At the bottom are 'Close' and 'Confirm' buttons.

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 mount 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**

A screenshot of the IGEL Setup application window. The title bar says 'IGEL Setup'. The top navigation bar has tabs: Accessories, User Interface, Network (which is highlighted in yellow), Devices, Security, and System. Below the tabs is a search bar with a magnifying glass icon and a gear icon. On the left, there's a sidebar with a tree view of network settings: LAN Interfaces, Wireless, Mobile Broadband, Computer name, DHCP Options, DNS, VPN, SCEP Client (NDES), Default gateway, Hosts, Network Drives, and Proxy (which is highlighted with a yellow bar). In the main pane, there's a message box with a circular loading icon that says 'System-wide proxy configuration' and 'Direct Connection to the internet'. At the bottom right are three buttons: 'Close', 'Save', and 'Save and Close'.

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 227).

- **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 228). 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 230)
- [Storage Devices](#)(see page 231)
- [Bluetooth](#)(see page 243)
- [USB Access Control](#)(see page 249)
- [Audio](#)(see page 254)
- [Webcam Information](#)(see page 260)

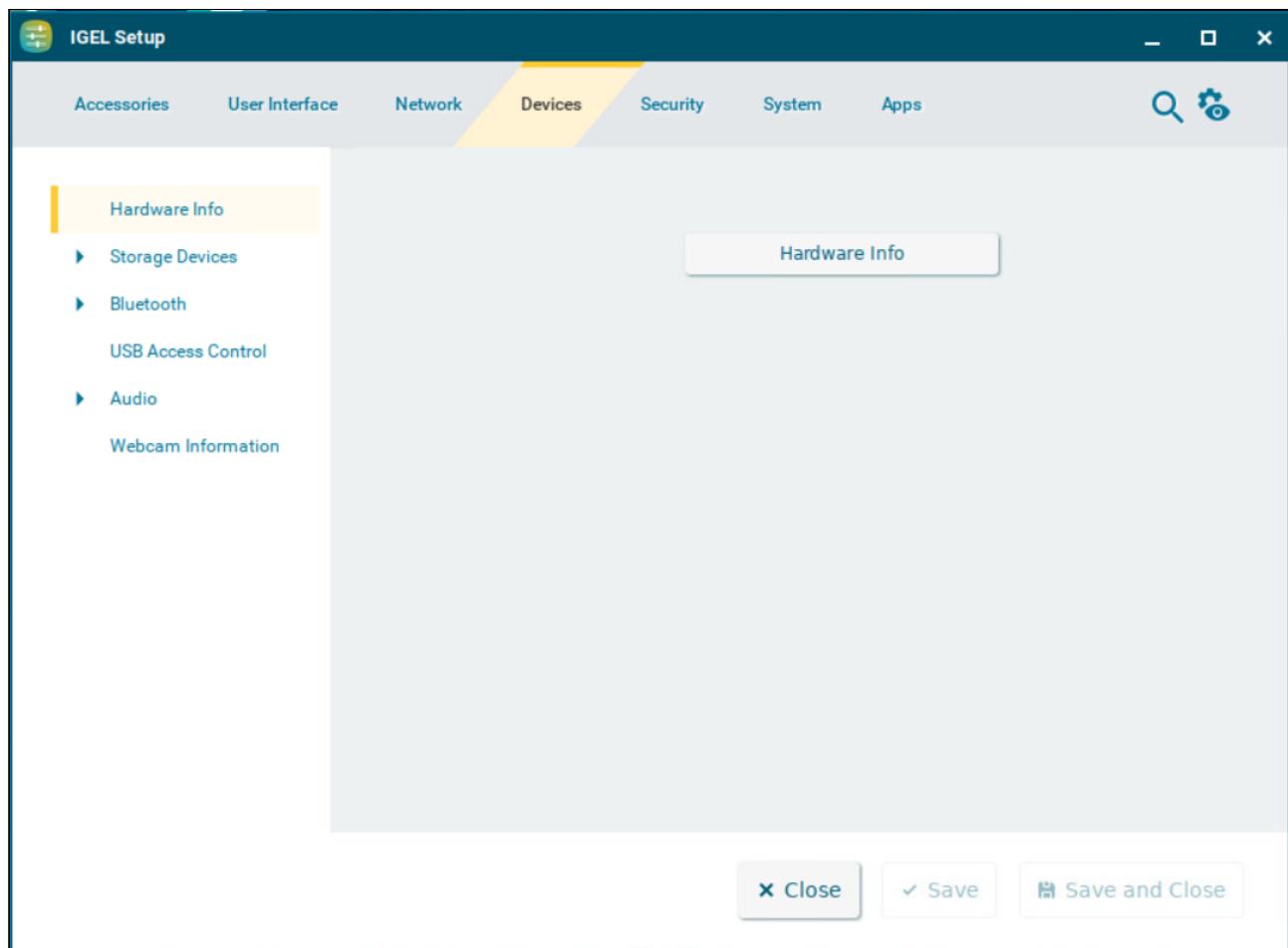


Hardware Info

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\(see page 305\)](#) 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\(see page 31\)](#).

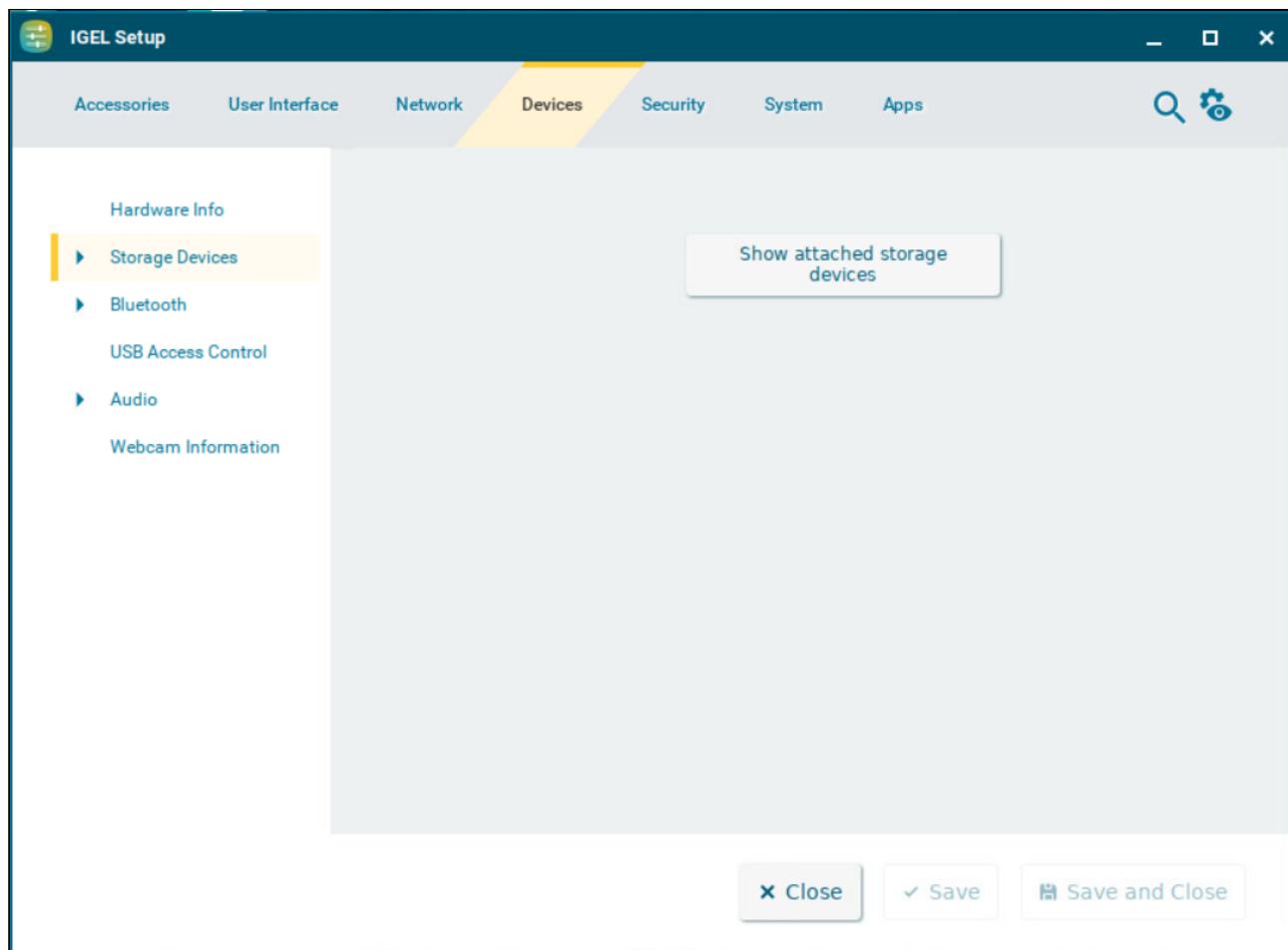


Storage Devices

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 305) 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 238).



- Storage Hotplug(see page 233)
- Options(see page 236)
- Disk Utility(see page 238)
- Safely Remove Hardware(see page 241)



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 249) and [Safely Remove Hardware](#)(see page 241).

Menu path: **Devices > Storage Devices > Storage Hotplug**

The screenshot shows the 'IGEL Setup' application window with the 'Devices' tab selected. On the left, a sidebar menu includes 'Hardware Info', 'Storage Devices' (which is expanded to show 'Storage Hotplug', 'Options', 'Disk Utility', and 'Safely Remove H...'), 'Bluetooth', 'USB Access Control', 'Audio', and 'Webcam Information'. The main panel displays 'Storage Hotplug' settings. It has two sections: 'Default permission' (set to 'Read/Write') and 'Notification' (which includes 'Hotplug beep' (checked), 'Hotplug message' (checked), and a 'Timeout' slider set to 15). At the bottom are buttons for 'Close', 'Save', and 'Save and Close'.



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 81).
- 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 96).
- 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 241).

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a gear icon. The left sidebar has a tree view with categories like Hardware Info, Storage Devices (expanded), Storage Hotplug (selected), Options (highlighted in orange), Disk Utility, Safely Remove H..., Bluetooth, USB Access Control, Audio, and Webcam Information. The main content area shows a configuration panel for "Storage Devices Options". It contains three items: 1) "User browse directory" with a checked checkbox and an info icon. 2) "Browse directory: / userhome/media" with an info icon. 3) "Support for built-in floppy drives" with an unchecked checkbox and an info icon. At the bottom are buttons for "Close", "Save", and "Save and Close".

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)

i 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.

- Info** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a gear icon. The left sidebar has a tree view with categories like Hardware Info, Storage Devices (expanded), Storage Hotplug, Options (expanded), Disk Utility (selected and highlighted in orange), Safely Remove H..., Bluetooth, USB Access Control, Audio, and Webcam Information. The main content area shows a "Session name" field with "Disk Utility" entered. Below it is a section titled "Starting Methods for Session" with five options: "Start Menu" (unchecked), "Menu folder" (unchecked), "Start Menu's System tab" (checked), "Application Launcher" (unchecked), and "Application Launcher folder" (unchecked). At the bottom are buttons for "Close", "Save", and "Save and Close".

Session name
Disk Utility

Starting Methods for Session

- Start Menu
- Menu folder
- Start Menu's System tab
- Application Launcher
- Application Launcher folder

Close **Save** **Save and Close**

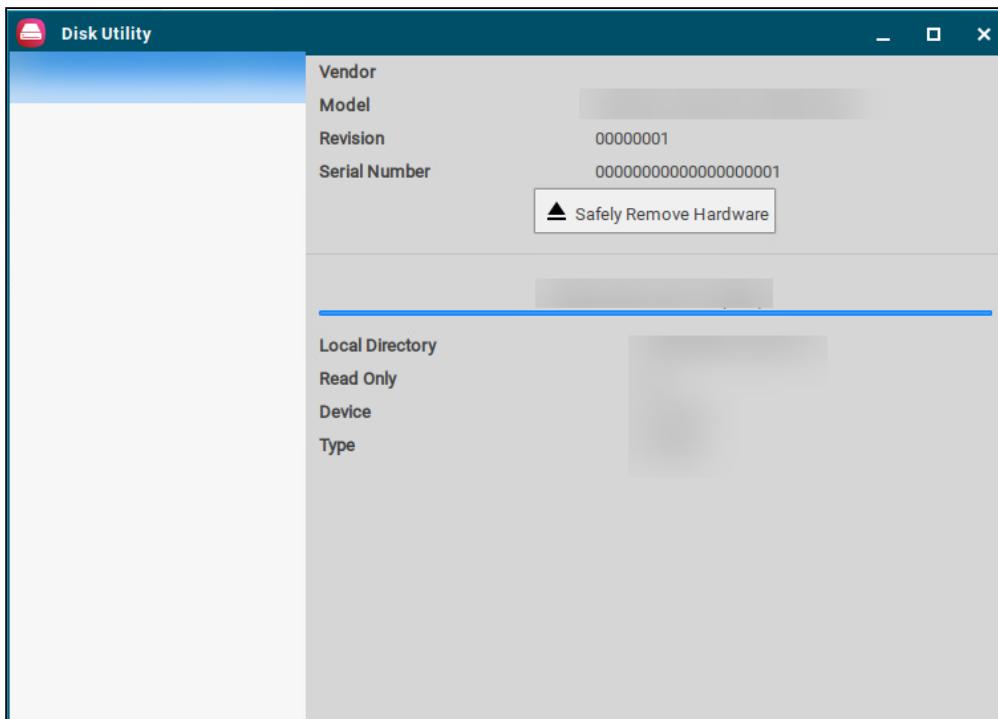


The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

- ⓘ 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 toolbar.

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 233).



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**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices (which is selected), Security, System, and Apps, along with search and settings icons. On the left, a sidebar lists categories like Hardware Info, Storage Devices (expanded to show Storage Hotplug, Options, Disk Utility, and Safely Remove H...), Bluetooth, USB Access Control, Audio, and Webcam Information. The main content area shows a "Session name" field containing "Safely Remove Hardware". Below it, a section titled "Starting Methods for Session" lists five options: Start Menu (unchecked), Start Menu's System tab (checked), Application Launcher (unchecked), and Application Launcher folder (unchecked). Each option has an "info" icon next to it. At the bottom are buttons for Close, Save, and Save and Close.

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

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 238).



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 245).

Menu path: **Devices > Bluetooth**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a gear icon. The left sidebar under "Hardware Info" has the following items: Storage Devices, Bluetooth (which is selected and highlighted in orange), USB Access Control, Audio, and Webcam Information. The main content area shows two configuration items in a list: "Bluetooth" with a checked checkbox and "Tray Icon" with a checked checkbox. At the bottom of the window are three buttons: "Close", "Save", and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a settings gear icon. On the left, there's a sidebar with sections: Hardware Info, Storage Devices, Bluetooth (with "Bluetooth Tool" selected and highlighted in yellow), USB Access Control, Audio, and Webcam Information. The main content area shows a "Session name" field with "Bluetooth Tool" entered. Below it is a section titled "Starting Methods for Session" with five entries, each with a refresh icon and a checkbox:

- Start Menu (checkbox checked)
- Menu folder (checkbox unchecked)
- Start Menu's System tab (checkbox checked)
- Application Launcher (checkbox unchecked)
- Application Launcher folder (checkbox unchecked)

At the bottom are three buttons: "Close" (with an X icon), "Save" (with a checkmark icon), and "Save and Close" (with both icons).

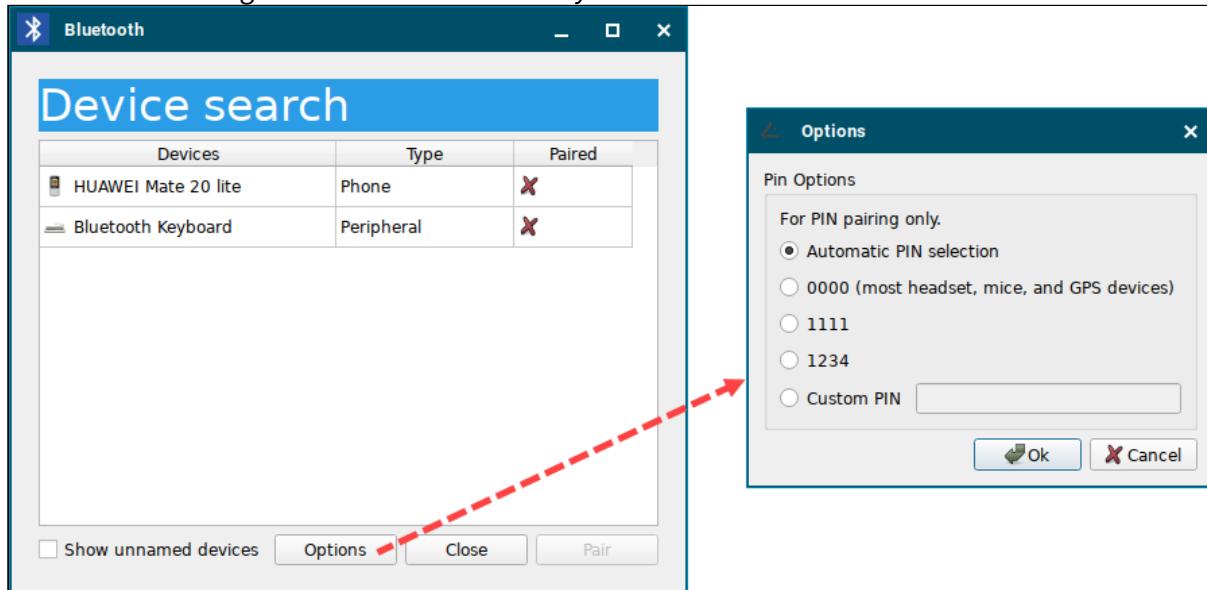


The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

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.

Cancelling 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**.

i 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a settings gear icon. The left sidebar has a tree view with categories: Hardware Info, Storage Devices, Bluetooth, USB Access Control (which is selected and highlighted in orange), Audio, and Webcam Information. The main content area shows three sections: 1) "Enable" status with a checkbox (unchecked) and a refresh button. 2) "Default rule" dropdown set to "Allow" with a refresh button. 3) "Default permission" dropdown set to "Read/Write" with a refresh button. Below these are two tables: "Class rules" and "Device Rules". The "Class rules" table has one entry: Rule "allow", Class ID "03", and Name "Allow HID". The "Device Rules" table is currently empty. At the bottom are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".

Rule	Class ID	Name
allow	03	Allow HID

Rule	Vendor ID	Product ID	Device uuid	Permission	Name

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\(see page 31\)](#).

System Information example:



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
- Shared Directories

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 2.0
Speed 12 Mb/s
Class [0] (Defined at Interface level)
Sub-class [0] (Unknown)
Protocol [0] (Unknown)
Device Version 6.93

Done.

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

Example for `lsusb`:

Local Terminal (on ITC00505693271E)

```
root@ITC00505693271E:~# lsusb | grep -i plantronics
Bus 002 Device 004: ID 047f:02e6 Plantronics, Inc. Poly BT700
root@ITC00505693271E:~#
```

• 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 233).
 - **Read only**
 - **Read/Write**
- **Name**

Name of the rule



Audio

The audio settings of the device can be configured through the following.

- Options(see page 255)
- Sound Preferences(see page 258)



Options

This article shows how to configure presets for the audio system in IGEL OS. The settings can be changed at any time with the Sound Preferences function. For details, see [Sound Preferences\(see page 258\)](#).

Menu path: **Devices > Audio > Options**

Show volume control in taskbar

- The  icon is shown in the taskbar. When you click the icon, the volume control is shown. When you right-click the icon, you can select **Sound preferences** to start the sound Sound Preferences function. (Default)
- The  icon is not shown. You can only use the **Sound Preferences** function to change the volume.

Remote volume settings

- The settings for the 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)

Default Sound Output

Port name

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**

Device name

Name of the output device. Select the device for audio output from a list of available devices. If the device is not present at the moment, you can type in its name.

Examples:

- Built-in Audio Analog Stereo
- Microsoft LifeChat LX-3000



Default Sound Input

Port name

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**

Device name

Name of the input device. Select the device for audio input from a list of available devices. If the device is not present at the moment, you can type in its name.

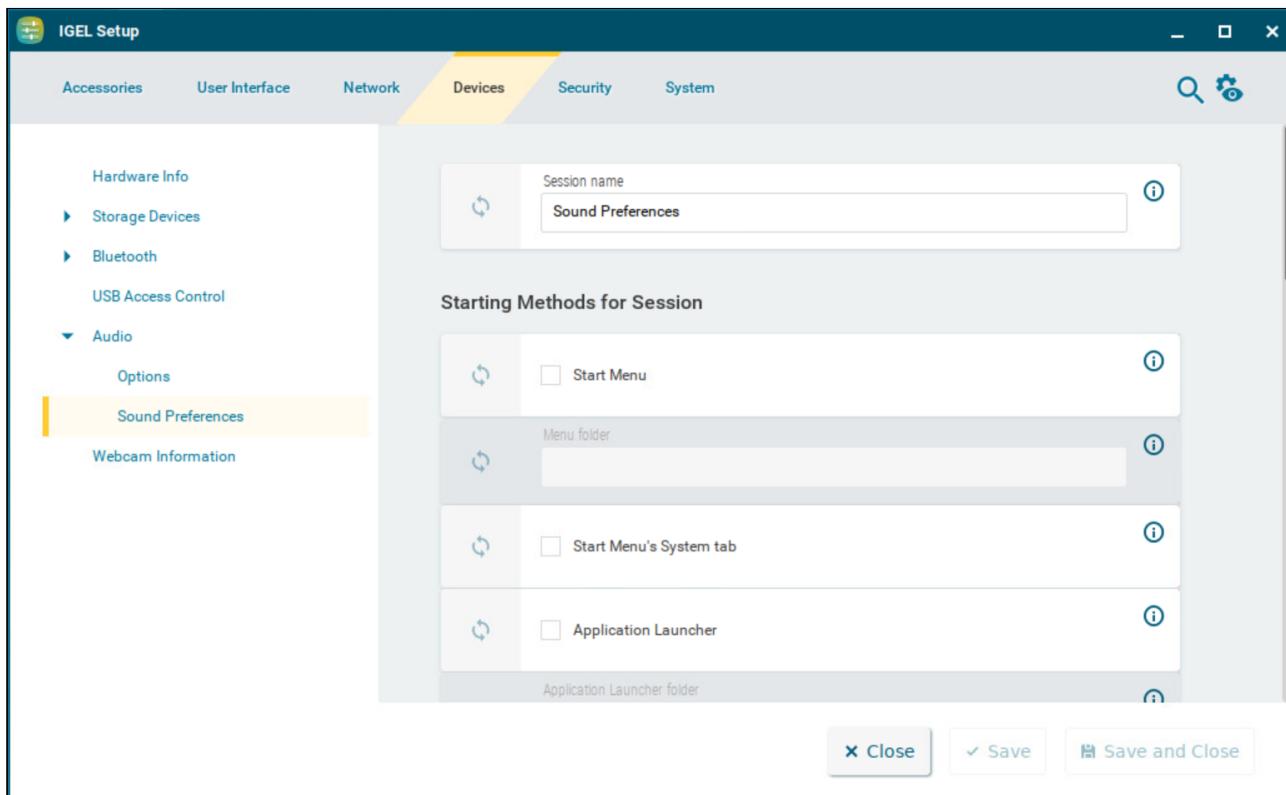
Example: Microsoft LifeChat LX-3000



Sound Preferences

This article shows the starting methods and the use of **Sound Preferences** in IGEL OS. With this function, you can configure your device's audio settings.

Menu path: **Devices > Audio > Sound Preferences**

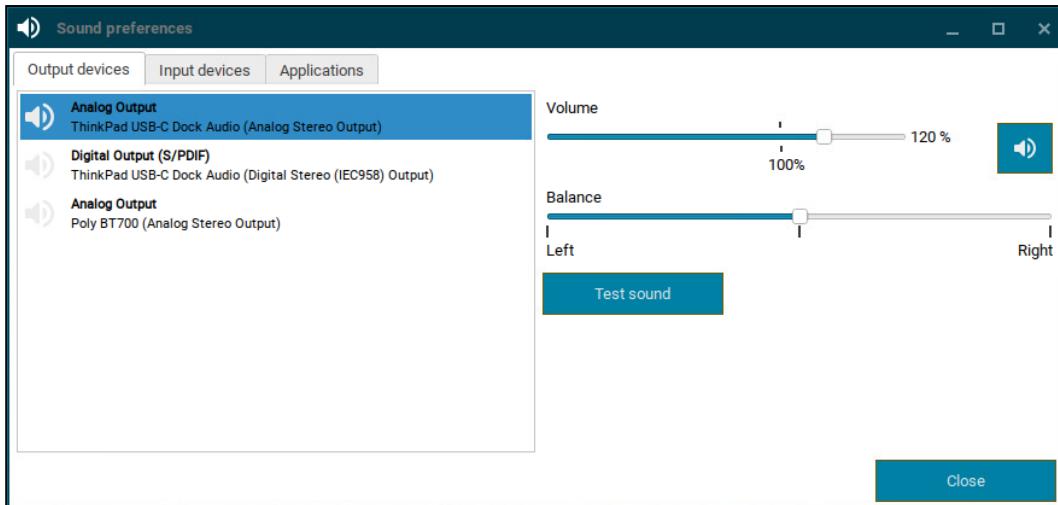


The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

- ⓘ If the **Show volume control in taskbar** option is enabled under **Devices > Audio > Options**, you can also start the function by right-clicking the icon in the taskbar and selecting **Sound preferences**. For details on the preset options for the audio system, see [Options](#)(see page 255).

Using Sound Preferences

- ▶ Start the **Sound Preferences** function.



To select and configure the device for playback, proceed as follows:

1. Navigate to the **Output devices** tab.
2. Select the device which is to be used for playback from the list of available devices.
3. If necessary, adjust the **Volume** and **Balance** settings. Optionally, you can test the configuration by clicking **Test sound**.

To select and configure the device for recording, proceed as follows:

1. Navigate to the **Input devices** tab.
2. Select the device which is to be used for recording from the list of available devices.
3. Adjust the **Volume** if necessary.

To change the playback volume for specific applications, proceed as follows:

1. Navigate to the **Applications** tab.
2. Adjust the volume control for the relevant application.



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.

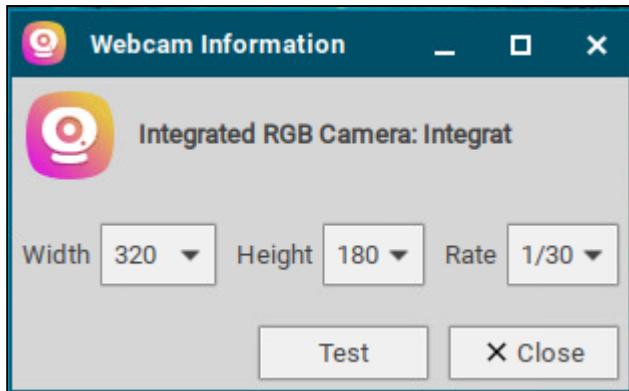
Menu path: **Devices > Webcam Information**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices (which is highlighted in yellow), Security, System, and Apps. To the right of the tabs are a search icon and a gear icon. The left sidebar has a tree view with categories: Hardware Info, Storage Devices, Bluetooth, USB Access Control, Audio, and Webcam Information (which is selected and highlighted in orange). The main content area shows a "Session name" field with "Webcam Information" and a "Starting Methods for Session" section. This section lists five methods with checkboxes: "Start Menu" (unchecked), "Menu folder" (unchecked), "Start Menu's System tab" (checked), "Application Launcher" (unchecked), and "Application Launcher folder" (unchecked). At the bottom are buttons for "Close", "Save", and "Save and Close".

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).

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 263)
- [Password](#)(see page 267)
- [Logon](#)(see page 271)
- [Active Directory/Kerberos](#)(see page 282)
- [Smartcard Services](#)(see page 288)
- [Change Password](#)(see page 290)
- [Update](#)(see page 292)



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**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps, along with search and settings icons. On the left, a sidebar menu lists "Device Encryption" (selected and highlighted in orange), "Password", "Logon", "Active Directory/Kerberos", "Smartcard", "Change password", and "Update". The main content area displays configuration options for "Device Encryption mode" set to "keep", "Authentication type" set to "PW", "Security level" set to "Auto, constant-time", "Target time delay (ms)" set to "700", "Password aggregation function" set to "H: Argon2id, 128M/3 ops", and "Minimum password length" set to "8". At the bottom right are buttons for "Close", "Save", and "Save and Close".

Device Encryption mode
keep

Change password

Authentication type
PW

Security level
Auto, constant-time

Target time delay (ms)
700

Password aggregation function
H: Argon2id, 128M/3 ops

Minimum password length
8

Close Save Save and Close

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 265) 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-alphanumeric 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are a search icon and a settings gear icon. On the left, there's a sidebar with "Device Encryption" and several sub-options: "Password" (which is selected and highlighted in orange), "Logon", "Active Directory/Kerberos", "Smartcard", "Change password", and "Update". The main content area has two sections: "Administrator" and "Setup Administrator". Both sections have a "Use Password" checkbox. Under "Administrator", there are fields for "New password" and "New password (repeated)". Under "Setup Administrator", there are also fields for "New password" and "New password (repeated)". At the bottom are three buttons: "Close", "Save", and "Save and Close".

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 37).



- i** 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\(see page 377\)](#).)
 - Accessing the local terminal as `root`. (For more information, see [Terminals\(see page 11\)](#).)
 - Virtual console access. (For more information, see [Access Control\(see page 54\)](#).)
 - sessions, for which **Administrator** is set under **Password protection**. (For more information, see [Starting Methods for Apps\(see page 373\)](#).)

If configured, the administrator can access the following with a password:

- **Unlocking the screenlock.** (For more information, see [Options\(see page 102\)](#).)
- **Secure Shell (SSH).** (For more information, see [SSH Access\(see page 302\)](#).)
- **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\(see page 373\)](#).)
- **User :** If configured, the user can access the following with a password:
 - the terminal session as `user`. (For more information, see [Terminals\(see page 11\)](#).)
 - sessions, for which **User** is set under **Password protection**. (For more information, see [Starting Methods for Apps\(see page 373\)](#).)

i 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\(see page 100\)](#).

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 102).

- **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 302).)

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 302).

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 272)
- Active Directory/Kerberos(see page 275)
- Single Sign-On(see page 277)
- Local User(see page 280)



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Device Encryption, Password, Logon (which is expanded to show Logon, Taskbar, Active Directory/Kerberos, Smartcard, Change password, and Update), Single Sign-On, Local User, and Active Directory/Kerberos. The "Taskbar" item under Logon is selected and highlighted with a yellow background. The main content area is titled "Taskbar settings for the login dialog". It contains a list of checkboxes with descriptions and info icons. The checked items are: "Show taskbar in login screen", "Show clock", "Show keyboard layout switcher", and "Show shutdown button". The unchecked items are: "Show on-screen keyboard button", "Start on-screen keyboard automatically", and "Show reboot button". At the bottom of this section is a subtitle "Taskbar settings when the screenlock is active". At the very bottom of the window are buttons for "Close", "Save", and "Save and Close".

Setting	Status	Description
Show taskbar in login screen	<input checked="" type="checkbox"/>	Show taskbar in login screen
Show clock	<input checked="" type="checkbox"/>	Show clock
Show keyboard layout switcher	<input checked="" type="checkbox"/>	Show keyboard layout switcher
Show on-screen keyboard button	<input type="checkbox"/>	Show on-screen keyboard button
Start on-screen keyboard automatically	<input type="checkbox"/>	Start on-screen keyboard automatically
Show reboot button	<input type="checkbox"/>	Show reboot button
Show shutdown button	<input checked="" type="checkbox"/>	Show shutdown button

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)

i There is no separate option for enabling/disabling network connection icons in the login dialog and/or on the locked screen. With **Show taskbar in login screen** and **Show taskbar in screenlock** enabled, the icons appear automatically if **Enable tray icon** is activated under:

- **Network > LAN Interfaces > Interface 1 / Interface 2 / Wireless**
- **Network > Mobile Broadband**
- **Network > VPN**

The network connection icons in the login dialog and on the locked screen serve for information purposes only and thus are inactive on clicking, except for the Wi-Fi icon.

The Wi-Fi icon invokes a dialog for turning Wi-Fi on/off, or the Wireless Manager in case it is activated under **Network > LAN Interfaces > Wireless**. For more information, see [Switching the Wi-Fi Connection Off or On](#)(see page 167) and [Wireless Manager](#)(see page 165).



Active Directory/Kerberos

This article shows how to enable local login to the device via the Kerberos protocol in IGEL OS.

- i** Active Directory/Kerberos must be configured as a prerequisite, see [Active Directory/Kerberos\(see page 282\)](#).

Menu path: **Security > Logon > Active Directory/Kerberos**

A screenshot of the IGEL Setup software interface. The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. Below the navigation bar is a search and settings icon. On the left, a sidebar menu lists: Device Encryption, Password, Logon (with sub-options: Taskbar, Active Directory/Kerberos, Single Sign-On, Local User), Active Directory/Kerberos (with a plus sign indicating expandable sub-options), Smartcard, Change password, and Update. The main content area is titled "Login Methods". It contains five entries, each with a refresh icon: "Login to Active Directory domain" (checkbox is empty), "Explicit" (checkbox is checked), "Remember last user name" (checkbox is empty), "Smartcard" (checkbox is empty), and "Smartcard removal action" (dropdown menu set to "Log out").

Method	Status	Action
Login to Active Directory domain	<input type="checkbox"/>	
Explicit	<input checked="" type="checkbox"/>	
Remember last user name	<input type="checkbox"/>	
Smartcard	<input type="checkbox"/>	
Smartcard removal action	Log out	

- i** 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.

- i** 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 140). For information on how to configure the shutdown menu, see [Shutdown](#)(see page 324).



Single Sign-On

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.

- i For a detailed description of the entire SSO configuration process, see [Configuring Single Sign-On \(SSO\)](#).

Menu path: **Security > Logon > Single Sign-On**

The screenshot shows the IGEL Setup application window. The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. Below the tabs is a search and settings icon. The left sidebar has a tree view with sections like Device Encryption, Password, Logon (with Taskbar, Active Directory/Kerberos, Single Sign-On selected, and Local User), Active Directory/Kerberos, Smartcard, Change password, and Update. The main content area is titled 'Identity Providers' and contains fields for Identity Provider (set to Okta), Okta URL, Client ID, Client secret, and New password (repeated). A 'Set password' button is at the bottom right of the form.

Single Sign-On with identity provider

- SSO is used as the authentication method.

- i 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 280).



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.

- i** 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 140). For information on how to configure the shutdown menu, see [Shutdown](#)(see page 324).

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.



Local User

This article shows how to configure the local login authentication in IGEL OS. [Commands\(see page 140\)](#)

- i If several login methods are enabled, the login method can be selected on the login screen.

Menu path: **Security > Logon > Local User**

The screenshot shows the IGEL Setup interface with the following details:

- Top Navigation Bar:** Accessories, User Interface, Network, Devices, **Security** (highlighted in yellow), System, Apps.
- Left Sidebar:** Device Encryption, Password, Logon (expanded), Taskbar, Active Directory/Ker..., Single Sign-On, **Local User** (selected and highlighted in orange), Active Directory/Kerberos, Smartcard, Change password, Update.
- Right Main Area:**
 - Login with local user password:** A checkbox labeled "Login with local user password" is checked. To its right are three input fields: "Password", "New password", and "New password (repeated)". Below these is a "Set password" button.
 - A small circular icon with a question mark and an exclamation mark is located to the right of the password fields.

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\(see page 102\)](#).



- ⓘ 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 140). For information on how to configure the shutdown menu, see [Shutdown](#)(see page 324).



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are search and filter icons. The left sidebar contains a tree view of configuration categories: Device Encryption, Password, Logon, Active Directory/Kerberos (which is expanded to show Domain 1, Domain 2, Domain 3, Domain 4, and Domain Realm Map...), Smartcard, Change password, and Update. The main content area is titled "Active Directory/Kerberos" and contains the following configuration options:

- Enable: A checkbox labeled "Enable" with a refresh icon to its left. It is currently unchecked.
- Default domain (fully qualified domain name): An input field with a refresh icon to its left, currently empty.
- DNS lookup for domain controller: A checkbox labeled "DNS lookup for domain controller" with a refresh icon to its left. It is checked.
- DNS lookup for domain: A checkbox labeled "DNS lookup for domain" with a refresh icon to its left. It is checked.
- Obtain Addressless Tickets: A checkbox labeled "Obtain Addressless Tickets" with a refresh icon to its left. It is checked.

At the bottom of the window are three buttons: "Close", "Save", and "Save and Close".

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 a Network Address Translation (NAT) device. (Default)

-
- [Domain\(see page 284\)](#)
 - [Domain Realm Mapping\(see page 286\)](#)



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]**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are a search icon and a settings gear icon. On the left is a sidebar with a tree view of configuration options: Device Encryption, Password, Logon, Active Directory/Kerberos (which is expanded, showing Domain 1, Domain 2, Domain 3, Domain 4, and Domain Realm Map...), Smartcard, Change password, and Update. The main content area has a "Fully qualified domain name" input field with a refresh button and an information icon. Below it is a "Domain Controller List" table with a header row "Domain Controller" and a single data row "Domain Controller". At the bottom are buttons for Close, Save, and Save and Close.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are a search icon and a settings gear icon. The left sidebar contains a tree view with nodes: Device Encryption, Password, Logon, Active Directory/Kerberos (expanded), Domain 1, Domain 2, Domain 3, Domain 4, Domain Realm Map... (selected and highlighted in yellow), Smartcard, Change password, and Update. The main content area is titled "Domain Realm Map..." and contains a table with two columns: "DNS host or domain name" and "Active Directory domain name". There is one row in the table with the values "DNS host or domain name" and "Active Directory domain name". Below the table are icons for edit, delete, and add. At the bottom of the content area are buttons for "Close", "Save", and "Save and Close".

DNS host or domain name	Active Directory domain name
DNS host or domain name	Active Directory domain name

Use default DNS domain - Active Directory domain mapping

- The DNS name and Active Directory domain name match. (Default)
 DNS name and Active Directory domain name assignments must be set up.



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 Database¹⁷](#).

Menu path: **Security > Smartcard > Services**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The window has a dark header bar with the title and standard window controls. Below the header is a navigation menu with tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are a search icon and a gear icon. The main content area has a sidebar on the left containing links: Device Encryption, Password, Logon, Active Directory/Kerberos, Smartcard (with "Services" selected), Change password, and Update. The main panel displays a configuration section for "Smartcard Services". It includes a "Activate PC/SC daemon" checkbox which is checked. Below it is a message: "PC/SC devices: There are no PC/SC devices available" and a "Refresh device list" button. At the bottom of the main panel are three buttons: "Close", "Save", and "Save and Close".

¹⁷ <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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), and System. To the right of the tabs are search and settings icons. The left sidebar contains a tree view with categories like Device Encryption, Password, Logon, Active Directory/Kerberos, Smartcard, Change password (which is selected and highlighted in orange), and Update. The main panel shows a "Session name" field with "Change Password" entered. Below it is a section titled "Starting Methods for Session" with four items: "Start Menu" (unchecked), "Menu folder" (empty), "Start Menu's System tab" (unchecked), and "Application Launcher" (unchecked). At the bottom are "Close", "Save", and "Save and Close" buttons.

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 373).

i 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 367).

Menu path: **Security > Update**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. To the right of the tabs are a search icon and a settings gear icon. The left sidebar contains a tree view with nodes: Device Encryption, Password, Logon, Active Directory/Kerberos, Smartcard, Change password, and Update (which is selected and highlighted with a yellow bar). The main content area shows a "Permit local app installation" section with a checkbox labeled "Permit local app installation" which is checked. Below the checkbox are "Close", "Save", and "Save and Close" buttons.

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 294)
- [Remote Management](#)(see page 296)
- [Remote Access](#)(see page 301)
- [Logging](#)(see page 310)
- [Power Options](#)(see page 314)
- [System Customization](#)(see page 327)
- [Update](#)(see page 367)
- [Registry in IGEL OS 12](#)(see page 370)



Time and Date

This article shows the time and date settings options in IGEL OS.

Menu path: **System > Time and Date**

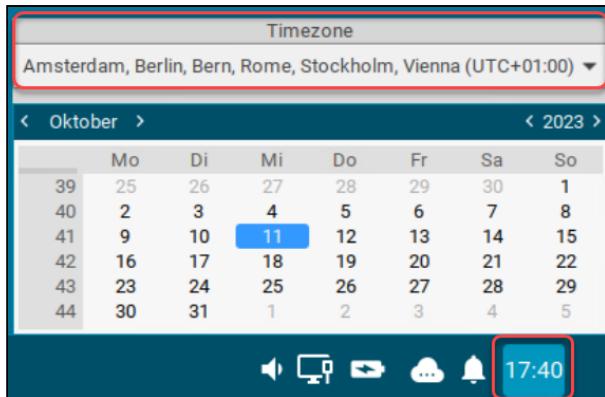
A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search bar with a magnifying glass icon and a refresh button. On the left, a sidebar menu is open under the "Time and Date" section, which is also highlighted in yellow. The sidebar contains links for Remote Management, Remote Access, Logging, Power Options, System Customization, Update, and Registry. The main content area is titled "Timezone" and shows a dropdown menu set to "(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna". Below this is a checkbox labeled "Timezone systray settings" which is checked. The next section is "Time server", which includes a checkbox "Use NTP time server" (unchecked) and a field for "NTP time server" containing an empty IP address field. At the bottom, there's a note about manual date and time configuration with fields for "10/19/2023" and "03:13 PM", and a "Change date and time" button. At the very bottom right are three buttons: "Close", "Save", and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has sections: Time and Date, Remote management (which is expanded and highlighted with a yellow bar), Remote Access, Logging, Power Options, System Customization, Update, and Registry. The main content area shows "Universal Management..." with a table of UMS server configurations. Below that are several configuration options with checkboxes and sliders: "Display 'Apply changes' dialog on boot" (checked), "Timeout" (set to 20), "Default action on boot" (set to "Apply changed configuration immediately"), and "Prompt user on UMS actions" (checked). At the bottom are "Close", "Save", and "Save and Close" buttons.

UMS server	Port number
192.168.30.109	8443
192.168.30.109	8443

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.



- i 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.

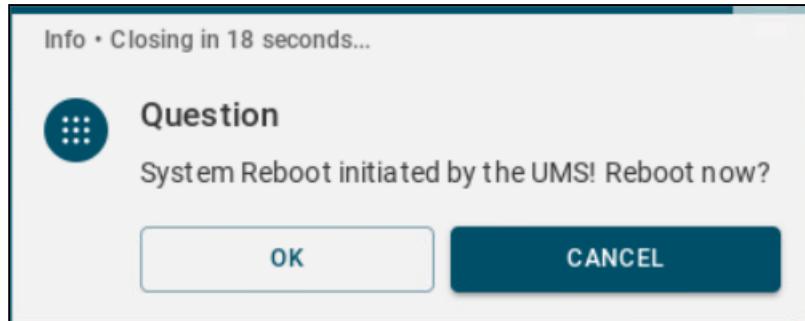
Possible values:

- **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.

Structure tag

You can define a structure tag in order to sort the device into a directory in accordance with the UMS directory rules. For further information on the use of structure tags, see Using Structure Tags.

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

This article shows how to enable the logging of remote management events in IGEL OS.

- ⓘ The event logs for the endpoint device can be found in the UMS console under **System > Logging**. For more information, see User Logs.

Menu path: **System > Remote Management > Options**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The window has a dark header bar with the title and standard window controls. Below the header is a navigation bar with tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are a search icon and a gear icon. The main content area has a sidebar on the left containing a tree view of configuration categories: Time and Date, Remote management (which is expanded, showing Options, Remote Access, Logging, Power Options, System Customization, Update, and Registry), and several collapsed categories like Advanced, General, and Network. On the right side of the main area, there is a configuration panel for "Log login and logoff events". It contains a checkbox labeled "Log login and logoff events" which is currently unchecked. There is also a small circular icon with an "i" symbol. At the bottom of the window are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

Log login and logoff events



- If a user logs on or off via Citrix or Kerberos, details of this event are sent to the UMS and can be used there, e.g. to process support queries. Logoffs from the Shared Workplace are also logged (logons take place via the UMS anyway).

(i) For this option to work, the **Activate event logging** option must be enabled in **UMS Console > UMS Administration > Globale Configuration > Logging**. For more information, see **Logging**.

- Logon and logoff events are not relayed. (Default)



Remote Access

To support remote management, the following remote access options can be configured for the device.

- [SSH Access](#)(see page 302)
- [Shadow](#)(see page 305)
- [Secure Terminal](#)(see page 308)



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote management, Remote Access (with SSH Access selected and highlighted in yellow), Shadow, Secure Terminal, Logging, Power Options, System Customization, Update, and Registry. The main content area shows configuration for SSH Access. It includes: a "Enable" checkbox (unchecked), a "Permit empty passwords" checkbox (unchecked), a "Permit administrator login" checkbox (unchecked), a "Port number" input field set to "22", a "User access" table with two entries (user and ruser), and a "Permit X11 forwarding" checkbox (unchecked). At the bottom are "Close", "Save", and "Save and Close" buttons.

User name	Host name	Deny
user	*	true
ruser	*	false

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

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:

- **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)

- i** 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 267).



Permit X11 forwarding

- X11 forwarding is enabled.
- X11 forwarding is disabled. (Default)

Applications Access for Remote User “ruser”

List of commands with availability configurations for the `ruser`

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). 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**

A screenshot of the IGEL Setup application interface. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote Management (expanded, showing Options), Remote Access (expanded, showing SSH Access, Shadow, Secure Terminal, Logging, Power Options, System Customization, Update, Registry). The "Shadow" option under Remote Access is selected and highlighted with a yellow background. The main content area shows several configuration items with checkboxes:

- Allow remote shadowing (checked)
- Deny shadowing via external VNC tool (checked)
- Use Password (unchecked)
- >Password: New password (text input field)
- New password (repeated) (text input field)
- Set password (button)
- Prompt user to allow remote session (checked)
- Allow user to disconnect remote shadowing (checked)

At the bottom are three buttons: Close, Save, and Save and Close.

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

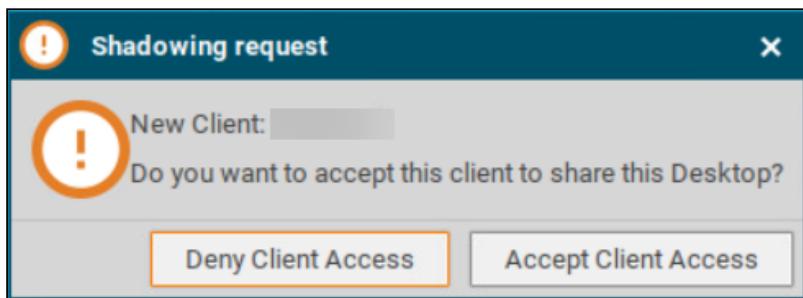
- The remote user is authenticated with a password before shadowing.
- The remote user is not authenticated for shadowing. (Default)

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)

i 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Time and Date, Remote management, Remote Access (expanded), SSH Access, Shadow, Secure Terminal (selected and highlighted with a yellow bar), Logging, Power Options, System Customization, Update, and Registry. The main content area shows a "Secure Terminal" section with a checkbox labeled "Secure Terminal" which is unchecked. There is also a small circular icon with a dot and a question mark icon. At the bottom right of the content area are "Close", "Save", and "Save and Close" buttons.

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](#)¹⁸.

¹⁸ <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.

- i** You can use the System Log Viewer to access system logs. For more information, see [System Log Viewer](#)(see page 39).

Menu path: **System > Logging**

A screenshot of the IGEL Setup application interface. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view with categories: Time and Date, Remote management, Remote Access, Logging (which is selected and highlighted in yellow), Power Options, System Customization, Update, and Registry. The main content area shows configuration options for the selected "Logging" category. There are four sections: 1) "Local logging" with a checked checkbox and an info icon. 2) "Persistent log partition" with an unchecked checkbox and an info icon. 3) "Partition size in MB" with a text input field containing "100" and an info icon. 4) "Remote mode" with a dropdown menu showing "Off". At the bottom are buttons for "Close", "Save" (with a checkmark), and "Save and Close".

Local logging	<input checked="" type="checkbox"/>	
Persistent log partition	<input type="checkbox"/>	
Partition size in MB	100	
Remote mode	Off	

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](#)(see page 315)
- [Battery](#)(see page 318)
- [Display](#)(see page 321)
- [Shutdown](#)(see page 324)



System

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search bar with a magnifying glass icon and a gear icon. On the left is a sidebar with a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options (expanded), System (selected), Battery, Display, Shutdown, System Customization, Update, and Registry. The main content area shows the "System" tab of the Power Options configuration. It includes the following settings:

- System suspend/shutdown on inactivity: Set to "Never".
- System action on inactivity: Set to "Suspend".
- A checkbox labeled "Without dialog" is unchecked.
- A slider for "Dialog timeout" is set to 10, with a range from 0 to 120.
- CPU power plan for battery mode: Set to "Balanced (recommended)".
- CPU Power Plan for AC Mode: Set to "High Performance".

At the bottom are three buttons: "Close", "Save" (with a checkmark), and "Save and Close".



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)

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

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



- ⓘ The CPU power plan can also be set using the battery tray app. For details, see [Battery](#)(see page 318).



Battery

This article shows battery settings options in IGEL OS.

Menu path: **System > Power Options > Battery**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories: Time and Date, Remote management, Remote Access, Logging, Power Options (expanded), System (expanded), Battery (selected and highlighted in orange), Display, Shutdown, System Customization, Update, and Registry. The main content area is titled "Battery Notification". It contains two sections: "Critical battery level (percentage)" set to 5, "Critical battery action" set to "Show warning", and "Critical command" set to "Shutdown". Below this is another section for "Low battery level (percentage)" set to 10, "Low battery action" set to "Show warning", and "Low command" set to "Shutdown". At the bottom of the content area is a section titled "Battery Tray Icon". At the very bottom are three buttons: "Close", "Save", and "Save and Close".

Battery Notification

Critical battery level (percentage)

Percentage of remaining battery charge deemed critical. (Default: 5)

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. (Default)
 The battery icon is not shown.



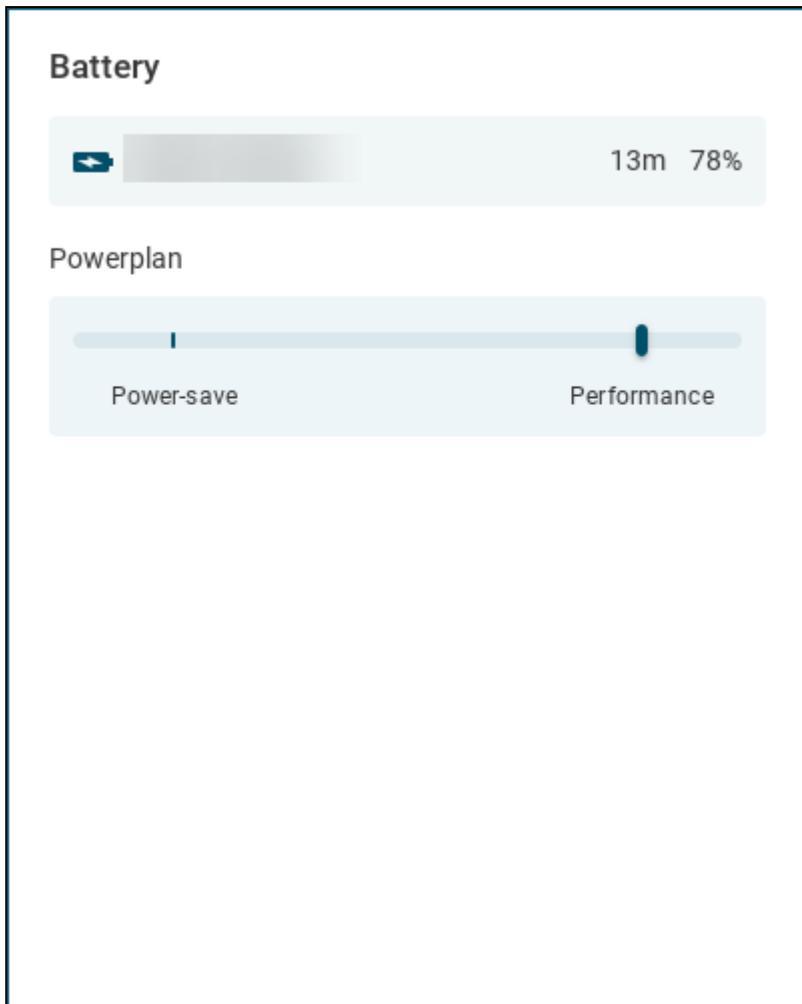
The icon is dynamic and represents the state of the battery charge. For example,  is displayed when the battery is charging.

Battery Tray App

The battery tray app shows information for all available batteries, including multiple internal batteries and batteries of connected bluetooth devices.



Hovering over the battery tray icon displays information on the charge level. Clicking the icon displays the battery tray app with details on the battery status and the option for setting the CPU power plan regulation.



- i** 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](#)(see page 315).



Display

This article shows how to configure energy-saving stages in IGEL OS.

- ⓘ Naturally, all stages are gone through only if the X-Server does not receive any new entries during the configured time period.

Power Management

Menu path: **System > Power Options > Display > Power Management**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search bar and a refresh icon. On the left, there's a sidebar with categories like Time and Date, Remote management, Remote Access, Logging, Power Options (which is expanded to show System, Battery, Display, Power Management, Brightness Reduction, and Shutdown), System Customization (with Update and Registry), and Registry. The main content area is titled "Display Power Management Settings". It contains a section for "On Battery" with three dropdowns: Standby Time (6 Minutes), Suspend Time (8 Minutes), and Off Time (10 Minutes). Below that is a section for "Plugged In" with three dropdowns: Standby Time (10 Minutes), Suspend Time (12 Minutes), and Off Time (disabled). At the bottom are buttons for Close, Save, and Save and Close.



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

Menu path: **System > Power Options > Display > Brightness Reduction**



Brightness Reduction

On Battery

On inactivity reduce to: 20

Reduce after: 9

Plugged In

On inactivity reduce to: 80

Reduce after: 9

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\(see page 94\)](#). You can also configure the shutdown menu as a command session and configure various starting methods. For more information, see [Commands\(see page 140\)](#).

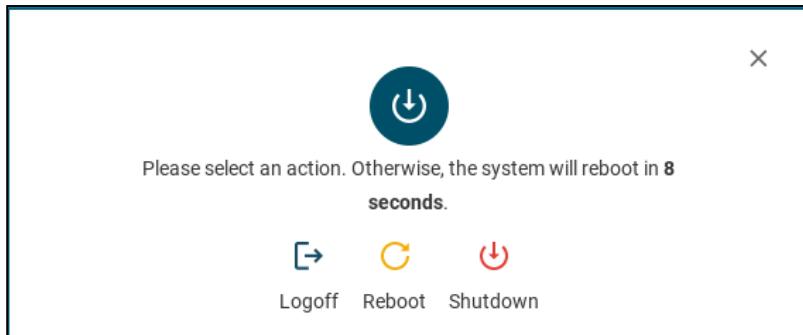
Menu path: **System > Power Options > Shutdown**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security, System, and Apps, with the System tab currently selected. On the left, a sidebar lists categories like Time and Date, Remote Management, Remote Access, Logging, Power Options (which is expanded to show System, Battery, Display, and Shutdown), System Customization, Update, and Registry. The "Shutdown" option under Power Options is highlighted with a yellow background. The main content area is titled "Global options" and contains four checkboxes: "Allow system shutdown" (checked), "Allow system suspend" (checked), "Allow system reboot" (checked), and "Allow system logoff" (checked). Below this is a "Default action" dropdown set to "Suspend" and a "Dialog timeout" slider set to 10. Under "Additional parameters when triggered via UMS", there are two checkboxes: "Allow canceling of shutdown process" (checked) and "Without dialog" (unchecked). At the bottom are three buttons: "Close", "Save", and "Save and Close".

Global options	
	<input checked="" type="checkbox"/> Allow system shutdown
	<input checked="" type="checkbox"/> Allow system suspend
	<input checked="" type="checkbox"/> Allow system reboot
	<input checked="" type="checkbox"/> Allow system logoff
Default action	
	Suspend
Dialog timeout	
	10
	0

Additional parameters when triggered via UMS	
	<input checked="" type="checkbox"/> Allow canceling of shutdown process
	<input type="checkbox"/> Without dialog

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.

i To configure the option, at least one login method needs to be enabled under **Security > Logon**. For more information, see [Logon](#)(see page 271).

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 296).

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 328)
- [Custom Application](#)(see page 334)
- [Custom Commands](#)(see page 338)
- [Corporate Design](#)(see page 346)
- [Environment Variables](#)(see page 361)



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 329)
- [Download](#)(see page 331)



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded), Custom Partition (selected and expanded), Partition (selected), Download, Custom Application, Custom Commands, Corporate Design, Environment Variables, Update, and Registry. The main content area shows configuration for a custom partition. It includes fields for "Enable Partition" (checkbox), "Size" (text input field), and "Mount Point" (text input field containing "/custom"). Below this is a table titled "Partitions Parameters" with columns "Name" and "Value". At the bottom are buttons for "Close", "Save", and "Save and Close".

Name	Value

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)

i Sensible values are for example "100K" (for $100 \text{ KiB} = 100 * 1024$ bytes) or "100M" (for $100 \text{ MiB} = 100 * 1024 * 1024$ 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Partition, Download, Custom Application, Custom Commands, Corporate Design, Environment Variables), Update, and Registry. The main content area is titled "Partitions Data Sour..." and shows a table with one row. The table has columns for "Automatic Update" and "URL". There are icons for edit, delete, and add (+) next to the URL column. At the bottom of the content area are buttons for Close, Save, and Save and Close.

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.de¹⁹). This program also allows **bzip2** compression. Under Linux, tar and bz2 files can be created using onboard resources.

¹⁹ <http://www.7-zip.de/>



The procedure makes it possible to replace the file(s) on the server with a new version which the thin client loads the next time it is booted. The `Version` parameter in the `INF` file must be increased for this purpose.



Custom Application

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 336).

Menu path: **System > System Customization > Custom Application**

A screenshot of the IGEL Setup software interface. The window title is "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. There are also search and filter icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition and Custom Application), Update, and Registry. The "Custom Application" node under System Customization is selected. The main content area shows a "Custom Applications" table with one entry: "Session Name" (Custom Application) and "Custom Application" (under the "Session Name" column). A blue "+" button is located at the top right of the table. At the bottom of the window are buttons for Close, Save, and Save and Close.

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.

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search bar with a magnifying glass icon and a gear icon. On the left is a sidebar with a tree view of settings: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (with Custom Partition, Custom Application, and another Custom Application node under it), Settings, Custom Commands, Corporate Design, Environment Variables, Update, and Registry. The "Custom Application" node under System Customization is expanded, and its "Settings" node is also expanded. The main content area shows a session named "Custom Application" with a "Session name" field containing "Custom Application". Below this is a section titled "Starting Methods for Session" with several items:

- Start Menu (checkbox checked)
- Menu folder (text input field)
- Start Menu's System tab (checkbox)
- Application Launcher (checkbox checked)
- Application Launcher folder (text input field)
- Application Launcher's System tab (checkbox)

At the bottom are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

Starting Method	Setting	Status
Start Menu	checkbox	checked
Application Launcher	checkbox	checked

The starting methods parameters are described under [Starting Methods for Apps](#)(see page 373).



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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration options: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Custom Application (expanded to show Custom Application), Settings (selected and highlighted in yellow), Custom Commands, Corporate Design, Environment Variables), Update, and Registry. The main content area shows two input fields: "Icon large" with a placeholder "applications-other" and "Command" with an empty field. At the bottom are buttons for Close, Save, and Save and Close.

Icon large

Select an icon provided. (Default: applications-other)

- i** 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 361).

You can define custom commands for the following startup processes:

- [Base](#)(see page 339)
- [Desktop](#)(see page 341)
- [Network](#)(see page 343)
- [Reconfiguration](#)(see page 345)



Base

The commands defined here are executed at the specific execution times during the boot process.

Menu path: **System > System Customization > Custom Commands > Base**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Custom Application, and Custom Commands), Base (selected and highlighted in orange), Network, Desktop, Reconfiguration, Corporate Design, Environment Variables, Update, and Registry. The main content area shows four execution times with empty text input fields: "Initialization", "Before session configuration", "After session configuration", and "Final initialization command". Each time entry has a blue circular refresh icon to its left and an information icon (i) to its right. At the bottom right of the content area are three buttons: "Close", "Save", and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Custom Application, and Custom Commands), Base, Network, Desktop (which is selected and highlighted in yellow), Reconfiguration (expanded to show Corporate Design and Environment Variables), Update, and Registry. The main content area shows three sections: "Desktop initialization" (with a refresh icon), "Before Desktop Start" (with a refresh icon), and "Final desktop command" (with a refresh icon). Each section has an "info" icon (a blue circle with an "i") in the top right corner. At the bottom right of the content area are buttons for "Close", "Save", and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. There are also search and settings icons. The left sidebar has a tree view with categories like Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (with sub-options like Custom Partition, Custom Application, and Custom Commands), Base, Network (which is selected and highlighted in orange), Desktop, Reconfiguration, Corporate Design, Environment Variables, Update, and Registry. The main panel shows four execution times for custom commands: "Network initialization" (with a preview window), "After network DNS", "Before network services", and "Final network command". Each time has a small circular refresh icon next to it. At the bottom right are buttons for Close, Save, and Save and Close.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. There are also search and settings icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded), Custom Partition, Custom Application, Custom Commands (expanded), Base, Network, Desktop, Reconfiguration (selected and highlighted in yellow), Corporate Design, Environment Variables, Update, and Registry. The main content area has a header "After reconfiguration" with a refresh icon and an info icon. Below it is a large empty rectangular box. At the bottom right of the content area are three buttons: "Close", "Save", and "Save and Close".

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 347)
- [Background \(1st Monitor\)](#)(see page 350)
- [Company Logos](#)(see page 358)



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.

- i** 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar contains a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (with sub-options like Custom Partition, Custom Application, Custom Commands), Corporate Design (with sub-options like Custom Bootsplash, Background (1st Monitor), Company Logos, Environment Variables), Update, and Registry. The "Custom Bootsplash" option under Corporate Design is currently selected and highlighted in yellow. The main content area is titled "Custom Bootsplash". It contains a "Custom Bootsplash" section with a "Enable custom bootsplash" checkbox and a "Custom Bootsplash - Server Location" section. In the "Server Location" section, the "Protocol" dropdown is set to "FTP". Below it are four input fields: "Server name", "Server path", "Port" (set to 21), and "User name". Each input field has a small circular info icon to its right. At the bottom of the main content area are three buttons: "Close", "Save", and "Save and Close".

Custom Bootsplash

Custom Bootsplash - Server Location

Protocol: FTP

Server name:

Server path:

Port: 21

User name:

Close Save Save and Close



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.

- i** 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)**

The screenshot shows the 'IGEL Setup' application interface. The top navigation bar includes 'Accessories', 'User Interface', 'Network', 'Devices', 'Security', 'System' (which is highlighted in yellow), and 'Apps'. The search and settings icons are also present. The left sidebar has a tree view with 'Time and Date', 'Remote management', 'Remote Access', 'Logging', 'Power Options', 'System Customization' (expanded to show 'Custom Partition', 'Custom Application', 'Custom Commands', 'Corporate Design', 'Custom Bootsplash', and 'Background (1st Monitor)...'), 'Company Logos', 'Environment Variables', 'Update', and 'Registry'. The main content area is titled 'Background (1st Monitor)'. It contains several configuration fields with preview icons and dropdown menus:

- Wallpaper (1st monitor):** Set to 'IGEL'.
- Wallpaper style (1st monitor):** Set to 'Stretched'.
- Color style (1st monitor):** Set to 'Horizontal gradient'.
- Desktop color (1st monitor):** Hex code '# 027498'.
- 2nd desktop color (1st monitor):** Hex code '# 015a76'.
- Custom wallpaper download (1st monitor):** An unchecked checkbox.
- Custom wallpaper file (1st monitor):** An empty input field.

At the bottom right are buttons for 'Close', 'Save', and 'Save and Close'.

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)**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search bar and a settings gear icon. The left sidebar contains a tree view of configuration categories: Custom Application, Custom Commands, Corporate Design (expanded), Custom Bootsplash, Background (1st Monitor) (expanded), Background (2nd Monitor) (selected and highlighted in yellow), Background (3rd Monitor), Background (4th Monitor), Background (5th Monitor), Background (6th Monitor), Background (7th Monitor), Background (8th Monitor), Custom Wallpapers, Company Logos, Environment Variables (expanded), Update, and Registry. The main content area shows settings for the second monitor: "Wallpaper (2nd monitor)" dropdown set to "Follows configuration for first Monitor"; "Wallpaper style (2nd monitor)" dropdown set to "Follows configuration for first Monitor"; "Color style (2nd monitor)" dropdown set to "Follows configuration for first monitor"; "Desktop color (2nd monitor)" input field with hex code "#027498" and a color swatch; "2nd desktop color (2nd monitor)" input field with hex code "#015a76" and a color swatch; a checkbox for "Custom wallpaper download (2nd monitor)" which is unchecked; and a "Custom wallpaper file (2nd monitor)" input field with a browse button. At the bottom are "Close", "Save", and "Save and Close" buttons.

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

- i 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**

A screenshot of the IGEL Setup application window. The title bar says 'IGEL Setup'. The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search icon and a gear icon. The left sidebar contains a tree view of settings: Custom Application, Custom Commands, Corporate Design (selected), Custom Bootsplash, Background (1st Mon... (selected), Background (2n...), Background (3r...), Background (4t...), Background (5t...), Background (6t...), Background (7t...), Background (8t...), Custom Wallpa... (highlighted in orange), Company Logos, Environment Variables, Update, and Registry. The main content area is titled 'Custom Wallpaper - Server Location'. It contains fields for Protocol (set to HTTP), Server name, Server path, Port (set to 80), User name, Password (set to New password), and New password (repeated). There is a 'Set password' button. At the bottom are 'Close', 'Save', and 'Save and Close' buttons.

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view of configuration categories: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Custom Application, Custom Commands), Corporate Design (expanded to show Custom Bootsplash, Background (1st Monit...), and Company Logos (which is selected and highlighted in orange)), Environment Variables, Update, and Registry. The main content area is divided into two sections: "Screensaver" and "Start menu". The "Screensaver" section contains settings for enabling image display, selecting a file for the screensaver logo, choosing one image per monitor, setting the image duration to 10 seconds, and selecting the image display mode as "Small-sized hopping". The "Start menu" section contains settings for the start button icon and for displaying a company logo in the start menu. At the bottom right are buttons for Close, Save, and Save and Close.

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.



- i** 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

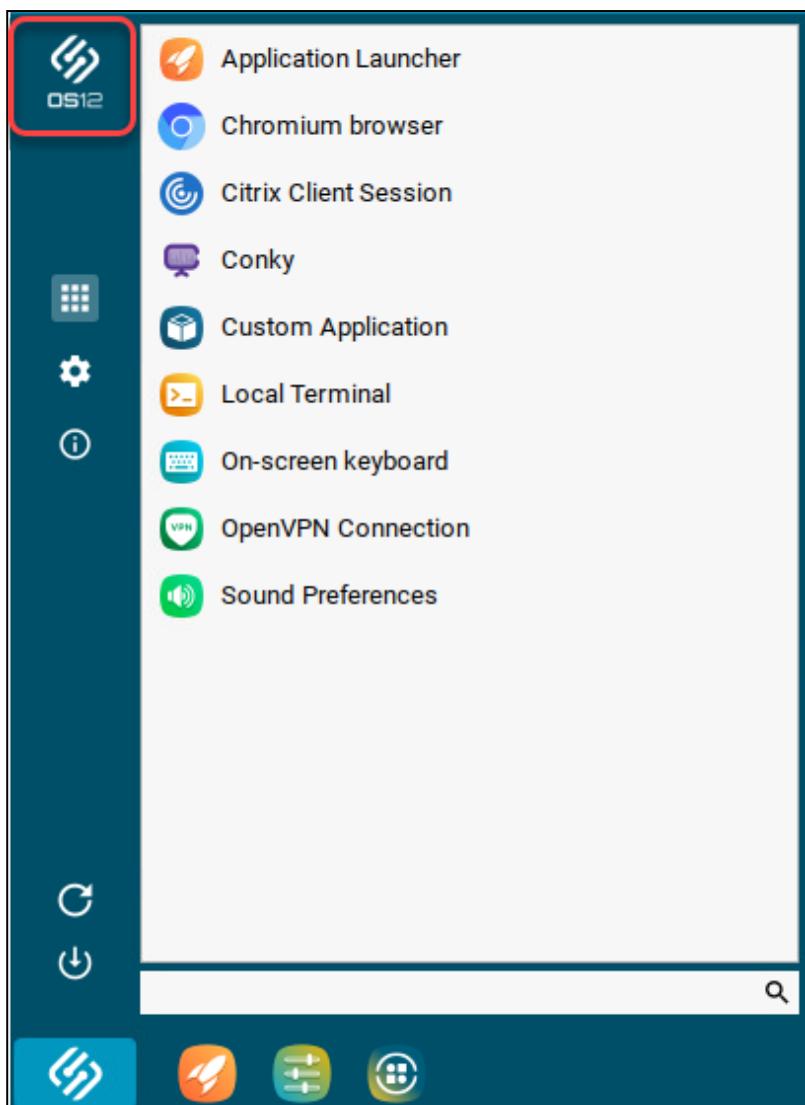
File name with full path to select your logo as the icon for the start menu in the taskbar. Size: 32x32 pixels



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

- i** 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 94).





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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view of settings: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded), Custom Partition, Custom Application, Custom Commands, Corporate Design, Environment Variables (also expanded). Under Environment Variables, there are sections for Predefined and Additional. At the bottom of the sidebar are Update and Registry buttons. The main content area shows a "Enable variable substitution in session" checkbox with a tooltip. At the bottom right are Close, Save, and Save and Close buttons.

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 338).

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 363)
 - [Additional](#)(see page 365)



Predefined

This article shows the options to configure predefined environment variables in IGEL OS.

Menu path: **System > System Customization > Environment Variables > Predefined**

A screenshot of the IGEL Setup application window titled "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. Below the tabs is a search and settings icon. The left sidebar contains a tree view with categories like Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (expanded to show Custom Partition, Custom Application, Custom Commands, Corporate Design), Environment Variables (expanded to show Predefined and Additional), Update, and Registry. The main content area displays a table with two columns: "Variable name" and "Value". There are four rows in the table, each with a refresh icon next to it. At the bottom right are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

Variable name	Value

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

i 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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. The left sidebar has a tree view with categories like Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization (with sub-options like Custom Partition, Custom Application, Custom Commands, Corporate Design), Environment Variables (which is expanded), Predefined, and a selected category named "Additional". Below the sidebar are buttons for Update and Registry. The main content area is titled "Additional" and contains a table with two columns: "Variable name" and "Value". There are four icons above the table: a delete icon, an edit icon, a copy icon, and a plus sign icon. At the bottom of the content area are three buttons: "Close", "Save" (with a checkmark icon), and "Save and Close".

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**

A screenshot of the IGEL Setup application window. The title bar says "IGEL Setup". The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security, System (which is highlighted in yellow), and Apps. To the right of the tabs are search and settings icons. On the left, there's a sidebar with sections: Time and Date, Remote management, Remote Access, Logging, Power Options, System Customization, Update (which is selected and highlighted in orange), and Registry. The main content area is titled "App Update settings". It contains several configuration items with checkboxes and input fields:

- Automatical reboot of system once App is installed (checkbox, unchecked)
- Timeout for automatical reboot in seconds (input field, value: 60)
- Use a bandwidth limit while updating (checkbox, unchecked)
- Limit bandwidth used for updating (input field, value: 2MB)
- Seconds to wait for network connection during a multi stage update (input field, value: 60)
- Activate app after the installation (checkbox, checked)

Below this is a "Repositories" section with a table:

Repository URL	Priority	Actions
		Remove Edit Add

At the bottom are three buttons: "Close", "Save", and "Save and Close".

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. Numbers are accepted from 0 to 4294967295.

- **Repository URL**

The URL of the repository



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!

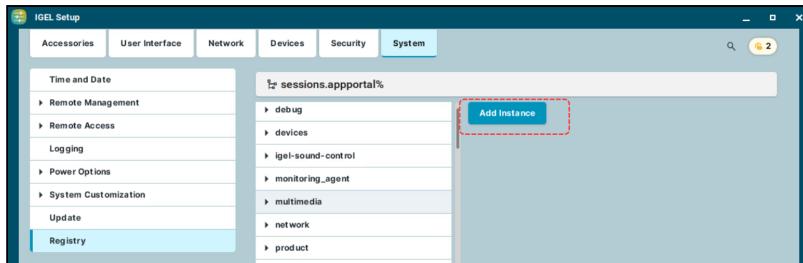
Registry User Interface

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 5).

- 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 The unsaved changes are marked with an orange dot on the right side of the parameter.

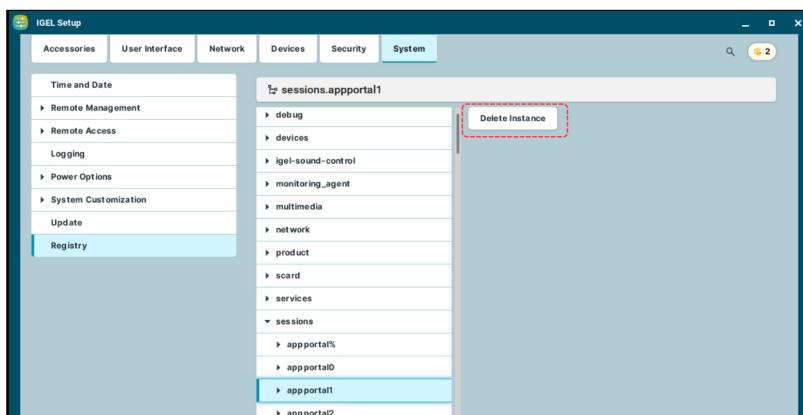
Add instance

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



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 267).

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 + Windows` = `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\(see page 377\)](#).
 - You can set up Base Custom Commands with specific execution times. For details, see [Base\(see page 339\)](#).
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**
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\(see page 341\)](#).

i The network interface can be stopped and restarted on the Linux Console (accessible via [Ctrl]+[Alt]+[F11]) with this command: `/etc/init.d/network stop /etc/init.d/network start`

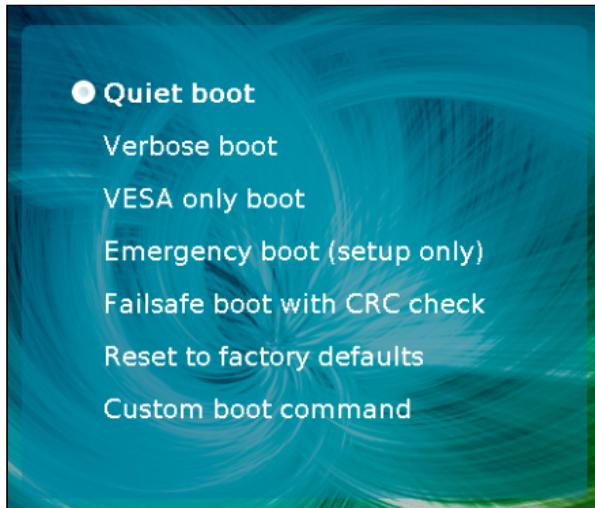


Boot Menu

During the boot 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 377): Normal startup. (Default)
- [Verbose boot](#)(see page 378): Start with system messages and an interactive root shell
- [VESA only boot](#)(see page 378): Basic graphic boot
- [Emergency boot \(setup only\)](#)(see page 378): Only the **Setup** window is available
- [Failsafe boot with CRC check](#)(see page 379): Start with an integrity check of the operating system
- [Reset to factory defaults](#)(see page 379): Reset the client to factory defaults
- [Custom boot command](#)(see page 379): 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.com²⁰.
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.

²⁰ <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 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

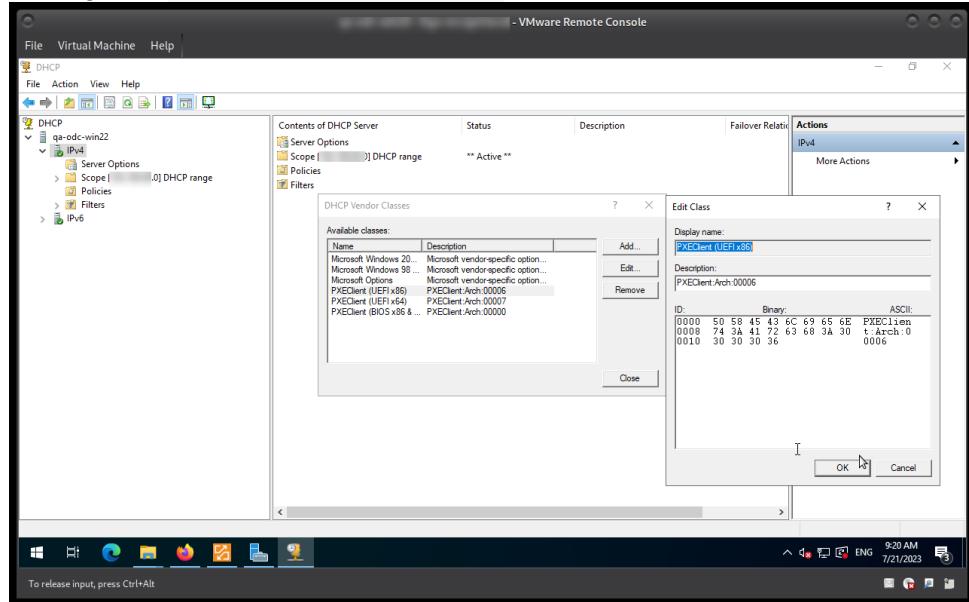
When the devices are powered on, they need to be directed to the TFTP server that provides the low-level files required for booting. This is done by the DHCP server. In our example, we use a Microsoft Windows DHCP server; other DHCP can be used as well.

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



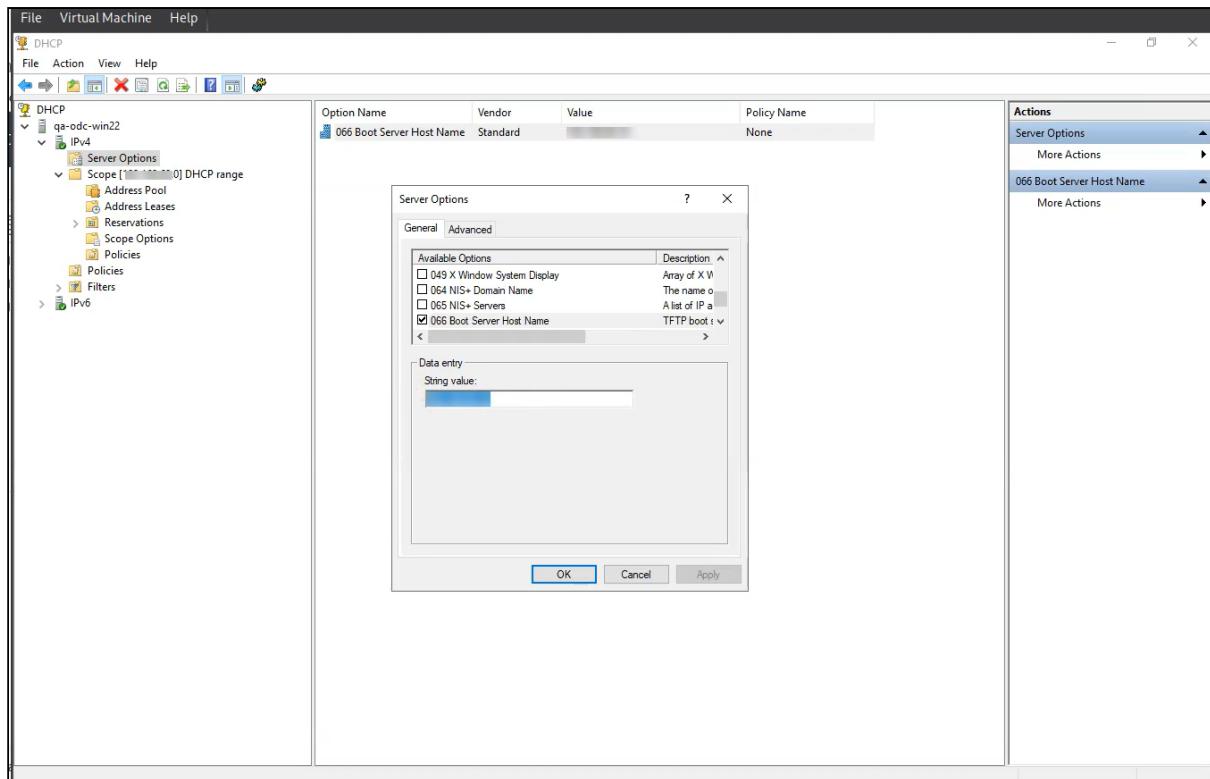
3. Perform the following steps for each vendor class you have created:

- 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:A screenshot of a Windows-based DHCP management tool. The left pane shows a tree view of a DHCP scope named 'qa-odc-win22'. Under 'Server Options' > 'Scope Options', there are several options listed. The right pane is a table showing detailed settings for these options. The table has columns for 'Option Name', 'Vendor', 'Value', and 'Policy Name'. One row is highlighted with a blue background, showing '066 Boot Server Host Name' with a value of 'grub/bootx64.efi' and a policy name of 'PXECClient (UEFI x64)'.

Option Name	Vendor	Value	Policy Name
066 Boot Server Host Name	Standard	grub/bootx64.efi	PXECClient (UEFI x64)
067 Bootfile Name	Standard	grub/bootx64.efi	PXECClient (UEFI x64)
066 Boot Server Host Name	Standard	grub/bootx64.efi	PXECClient (UEFI x86)
067 Bootfile Name	Standard	grub/bootx64.efi	PXECClient (UEFI x86)
066 Boot Server Host Name	Standard	grub/bootbios	PXECClient (BIOS x86 & x...
006 DNS Servers	Standard	8.8.4.4	None
066 Boot Server Host Name	Standard		None

5. Go to **Server Options**, add option **066**, and enter the Fully Qualified Domain Name (FQDN) or the IP address of your TFTP server.



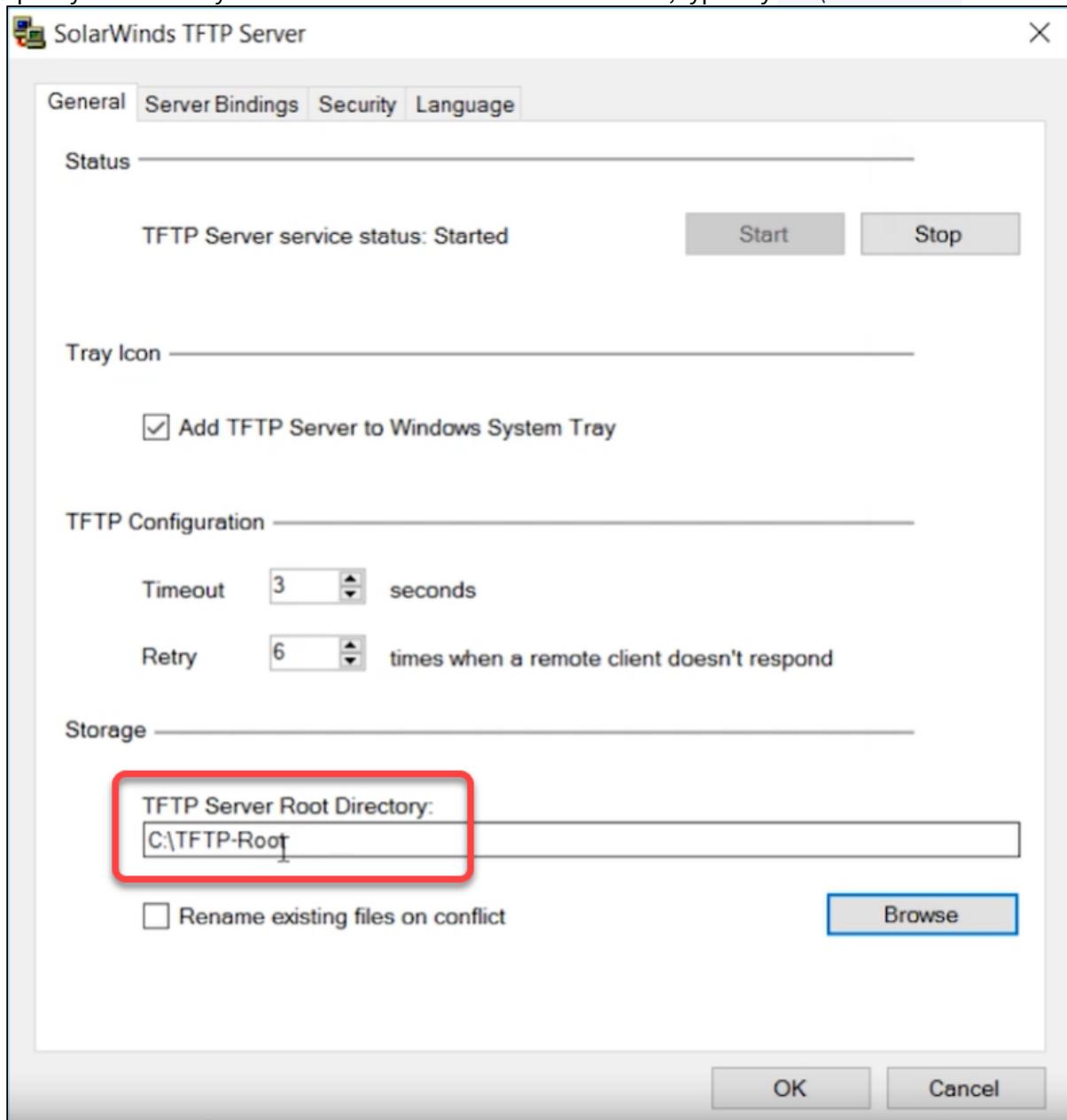
Deploying the TFTP Server

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.

A screenshot of the UMS 12 web interface. The top navigation bar has tabs for 'Devices', 'Apps' (which is highlighted in yellow), and '4 more'. On the left, there's a sidebar with a 'Apps' button and a gear icon. Below the sidebar, there's a dropdown menu for 'All' categories: 'Base', 'Codec', 'Browser', 'Unified Communication', and 'misc'. The main content area shows a folder named 'Printing' with one item: 'CUPS printing app'. A red arrow points to the gear icon in the sidebar.

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 i

Devices should download the Apps from

Download from UMS ▼

Upload

PXE Configuration i

Select Base System

Default Version (12.2.0) ▼

Select expiration date

1 month ▼

Partitions (0) +

Generate

X Reset ✓ Save

The "Select Base System" and "Select expiration date" sections are highlighted with a red rounded rectangle.



3. Click **Generate**.

A screenshot of a web-based configuration interface for UMS as an Update Proxy. At the top, there are three tabs: "UMS as an Update Proxy" (selected), "App Portal", and "Automatic Updates".

Under "UMS as an Update Proxy", there is a note: "Devices should download the Apps from" followed by a dropdown menu set to "Download from UMS". Below this is a blue "Upload" button.

Under "PXE Configuration", there are fields for "Select Base System" (set to "Default Version (12.2.0)") and "Select expiration date" (set to "1 month").

A section for "Partitions (0)" has a "+" button and a "Generate" button, which is highlighted with a red rectangular box.

At the bottom are "Reset" and "Save" buttons.

The file `pxe-config.json` is downloaded by your browser.

Editing the "pxe-config.json" File

- 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-webever/osc.bspl",
            "http://igel-pxe-webever/osc.nvgfx",
            "http://igel-pxe-webever/osc.sys"
        ]
    },
    "appdata": {
        "app_portal": "https://app.igel.com/api/",
        "auth_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJmaW5nZXJwcmludCI6IjQ2NjcE4NkMyMTk4Njg3MUIzMEUwMzU3NUQ5Q0NFRTQzNUJGRkU3M0IxQjYxRkMiLCJib2R5Ijp7InVt
c0lkIjoiVU1TL
UNMVVNURVIltQ0MDMxLTE20DgxMzQzNTY4NDEtMi0wIn0sInR5cGUi0iJ1bXMiLCJleHAI0jE
3MDA0ODAxMDgs
ImIhdCI6MTY5NzgwMTcwOH0.p-03tX5Zoesud95cpZBJuBCJU77fGzd17J3i1cbCIvhdiAB8D6
CmAdN6kFQ-9Qn
q35SmhyN8f8Jyn63AZEhmiAKPYVGNu10gVxN-oIU3SBTE74JlU0W26kQuYNEa-WqyAh4BGm-
dJ2qnyqh7_5L08F
DFalJChn8v7DlZ5MVA_G9IWQN6d87cM13dNFbuH4gK9z6lvKKI2s9Mfr2WQcu5qxBi3HhR-
f3M45zCMyUfm95Tu
eON48tAyfLPbx1qBUjm2FREJN89dqoZpo-obfcLQ85od6bFyotnK-MDm27-
BQvSl0pRujki2wMMYHz1vBeEJJfn
l78aGha5wRDpvrfcr0gd_vY4Taicd8hwETcAmI9ihks0H04gj6GIYZ1dBtbSGBMdooBkB4T5nK
trSX3IOkKCm79-
x_c9gfRNKS-5ox8fvYPIVTk42gHBkQvpgJ5c0G2PqpFCiA8wSBU1bx6bgJdNpQQA1WhadKj0jM
ICp49pf5PPPrfA
zvDzRpXxzQ43HpA86r2Jd59KS0i7QuW7Jb0D2WvjaoCSUFvXhaB-
UTsey61DKJJH73xqXb0oA5bdon123m8eTVK
wUJRTL6By41wG6nHnQ0dCYg8noucCg_r0CPBxVfvAhgxzwllWNgQbGBWtG9Iw1qZIpEuvJa3u
x3YxE5flMsXm
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`

The screenshot shows the IIS Manager interface with the 'Default Web Site' selected in the left navigation pane. The main area displays the 'MIME Types' configuration, which lists various file extensions and their associated MIME types. A modal dialog box is overlaid on the page, titled 'Add MIME Type', asking for a 'File name extension:' and a 'MIME type:'.

Extension	MIME Type	Entry Type
.bspl	application/octet-stream	Local
.sys	application/octet-stream	Inherited
.323	text/h323	Inherited
.3g2	video/3gpp2	Inherited
.3gp	video/3gpp	Inherited
.3gp2	video/3gpp2	Inherited
.3gpp	video/3gpp	Inherited
.aac	audio/aac	Inherited
.aaf	application/ocf+xml	Inherited
.aca	application/aca	Inherited
.accdb	application/msexcel	Inherited
.accde	application/msaccess	Inherited
.accdt	application/msonline	Inherited
.acx	application/internetprotocolsoap	Inherited
.adt	audio/vnd.dlna.adts	Inherited
.adts	audio/vnd.dlna.adts	Inherited
.afm	application/octet-stream	Inherited
.ai	application/postscript	Inherited
.aif	audio/x-aiff	Inherited
.aifc	audio/aiff	Inherited
.aiff	audio/aiff	Inherited
.appcache	text/cache-manifest	Inherited
.application	application/x-ms-application	Inherited
.art	image/x-jg	Inherited
.asd	application/octet-stream	Inherited
.asf	video/x-ms-asf	Inherited
.asi	application/octet-stream	Inherited
.asm	text/plain	Inherited
.asr	video/x-ms-asf	Inherited
.asx	video/x-ms-asf	Inherited



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 388)). 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 408). 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/>)

i 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>.

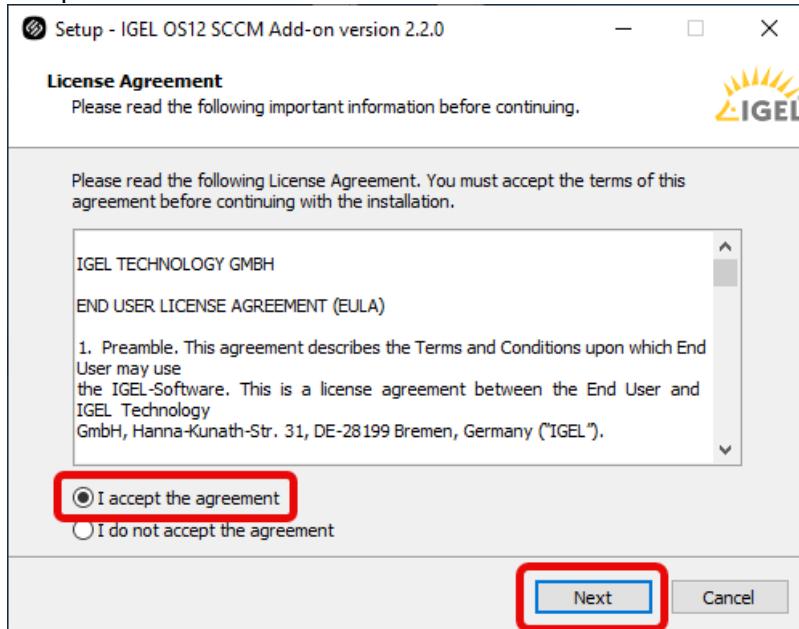
- Configured PXE environment for OS deployment; all target devices must be in a network where they are available either from the main site server or a distribution point. (For further information, see <https://docs.microsoft.com/en-us/mem/configmgr/osd/plan-design/infrastructure-requirements-for-operating-system-deployment>)
- 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

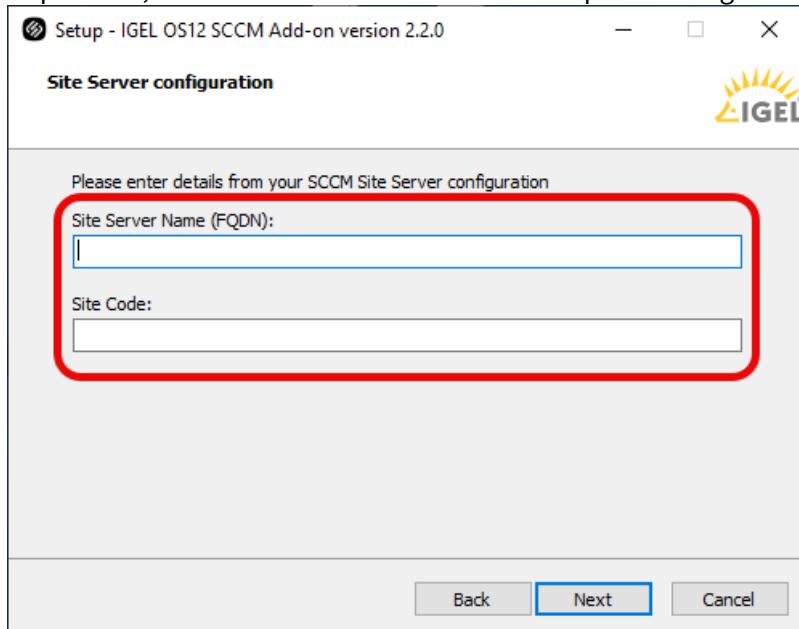
1. Go to <https://www.igel.com/software-downloads/cosmos/> > **OS 12 Base System Deployment Tool for SCCM** and download the executable file to the host on which Microsoft Endpoint Configuration Manager is running.
2. Start the executable file.



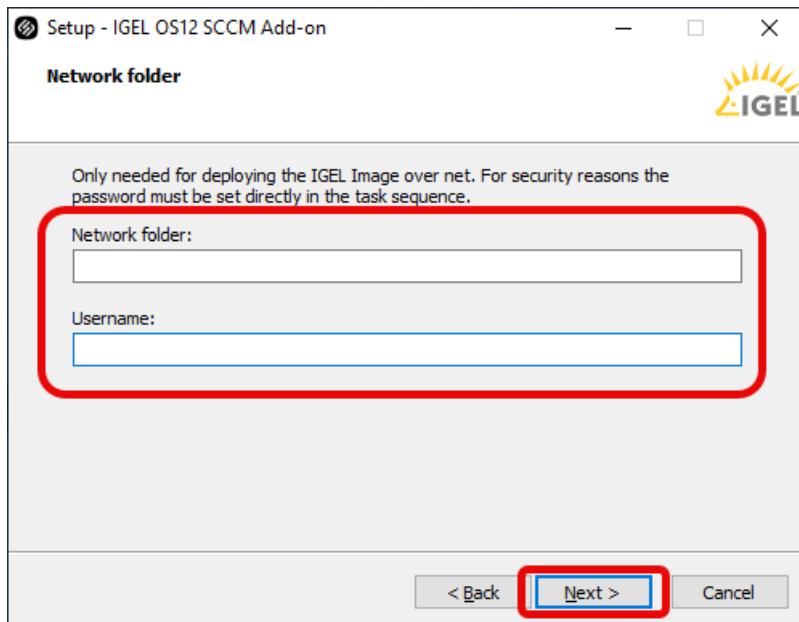
3. Accept the EULA and click **Next**.



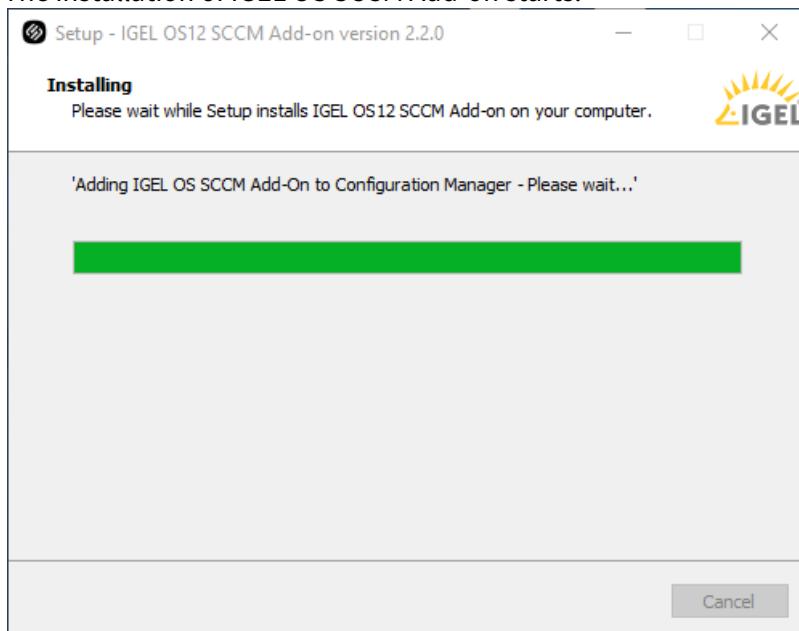
4. On the **Site Server configuration** page, review the field **Site Server Name (FQDN)**, which should be prefilled, and enter the **Site Code** of this Endpoint Configuration Manager site. Then, click **Next**.



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.

How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on

A screenshot of the System Center Configuration Manager (SCCM) interface. The title bar reads "System Center Configuration Manager (Connected to POU - Windows Site)". The left navigation pane shows "Software Library" with "Boot Images" selected. The main content area displays a table titled "Boot Images 3 items".

Icon	Name	V.	Comment	Image ID	OS Version	Client...	Date Modified
Boot image (x64)	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)	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	IGEL Boot Image	1	WinPE Boot Image for deploying IGEL OS	P010005A	10.0.18362.1	5.00.8...	22.06.2020 11:36

The "IGEL Boot Image" row is highlighted with a red box. The "Boot Images" folder in the navigation pane is also highlighted with a red box.



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.

Name	Description	Package ID	Date Created	Size (KB)	Enabled
IGEL Create		P0100207	11.09.2023 15:49	3	Yes
IGEL Create over Net		P0100209	11.09.2023 15:49	4	Yes
IGEL Inplace Upgrade		P0100208	11.09.2023 15:49	4	Yes

Provisioning IGEL OS via a PXE Boot Environment

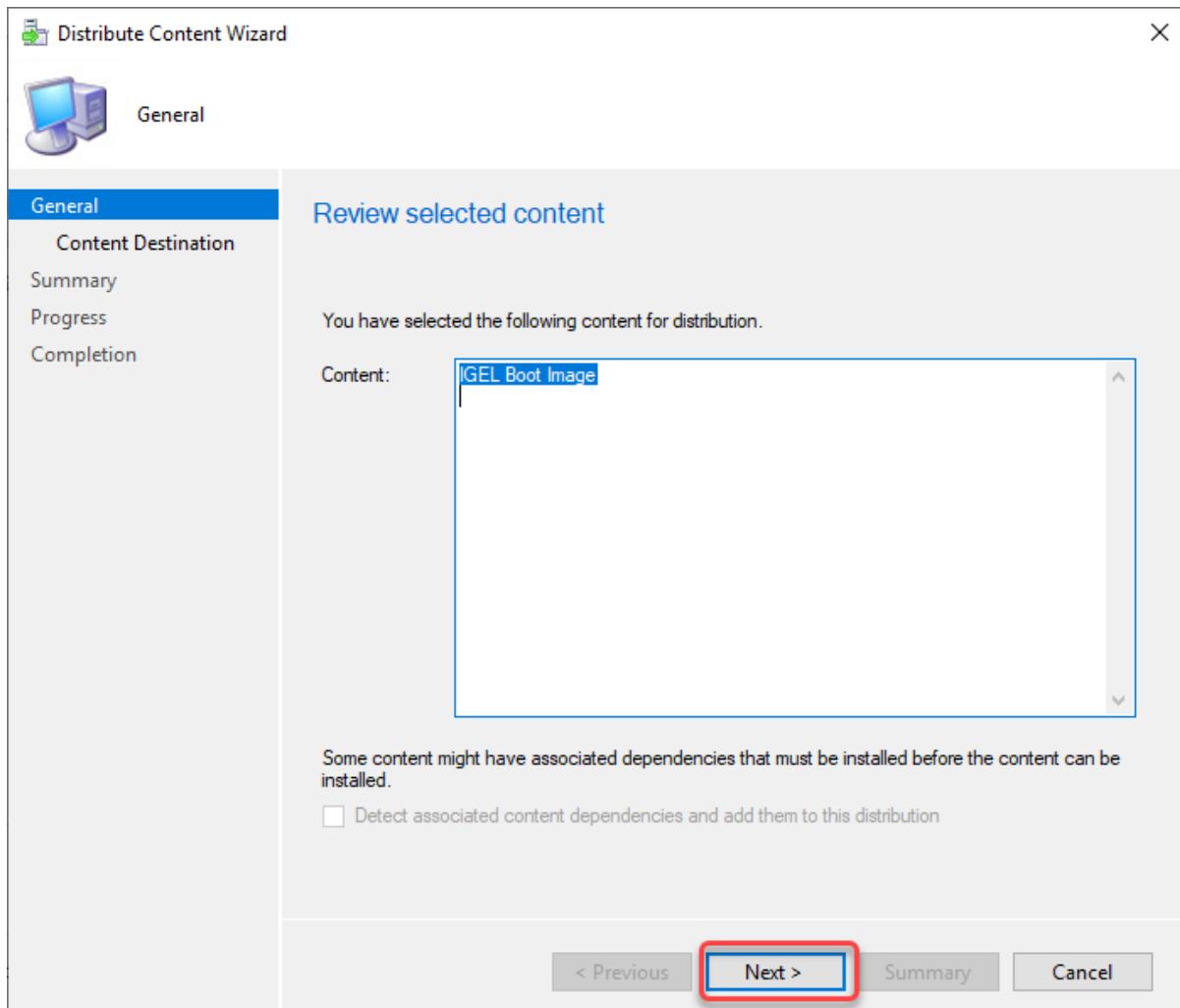
The task sequences provided by IGEL OS SCCM Add-on will deploy IGEL OS to a device collection via a PXE boot environment. The task sequence will be executed after the device has booted into the IGEL Boot Image (`igel.wim`).

You can choose between the following task sequences:

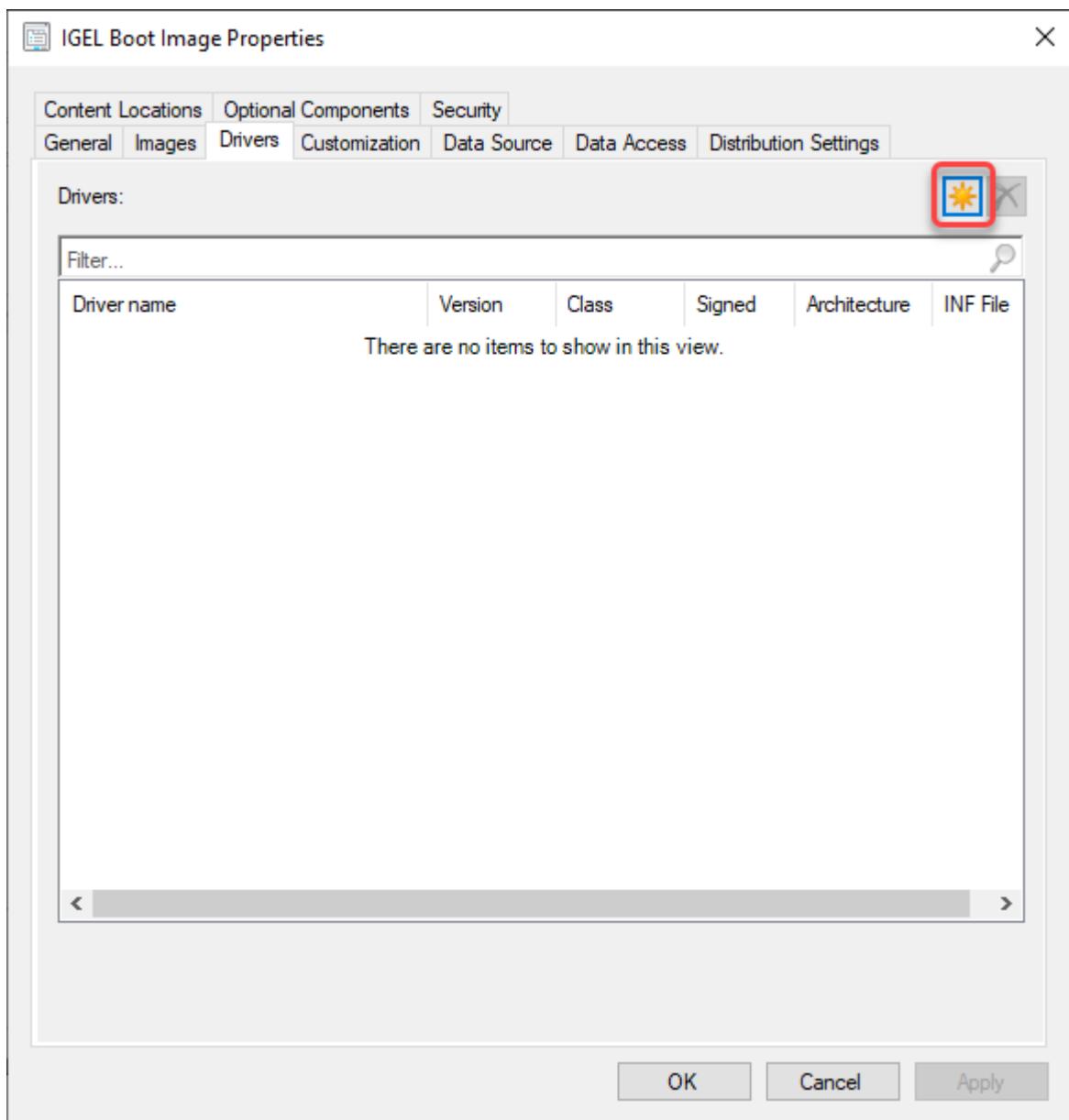
- **IGEL Create**: The IGEL OS image (`minimal.bin`) is built into the IGEL Boot Image (`igel.wim`)
- **IGEL Create over Net**: IGEL OS image (`minimal.bin`) is provided separately via a network share

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**.

How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on



The screenshot shows the Microsoft Configuration Manager interface. The left navigation pane is titled 'Software Library' and includes sections for Overview, Application Management, Software Updates, Operating Systems (with sub-options like Drivers, Driver Packages, Operating System Images, and Operating System Upgrade Packages), Task Sequences, Windows Servicing, Desktop Analytics Servicing, Microsoft Edge Management, Office 365 Client Management, Windows 11 Upgrade Readiness, and Scripts. The 'Boot Images' option under Operating Systems is highlighted with a red box. The main content area shows a table titled 'Boot Images 3 items' with columns for Icon, Name, Version, Comment, Image ID, OS Version, and Client Version. Three items are listed: 'Boot image (x64)' (Version 10.0.18362.1), 'Boot image (x86)' (Version 10.0.18362.1), and 'IGEL Boot Image' (Version 1, Comment: 'WinPE Boot Image for deploying IGEL OS'). A context menu is open over the 'IGEL Boot Image' row, with the 'Update Distribution Points' option highlighted with a red box. Below the table, a summary for the 'IGEL Boot Image' is shown, including fields for Name, Comment, Architecture, Version, Language, and Client Version. The 'Content Status' section indicates '0 Targeted' (Last Update: 05.02.2024 10:03). A 'Related Objects' section shows a link to 'Content Status'.



Update Distribution Points Wizard

General

General

Summary

Progress

Completion

Update distribution points with this boot image

This wizard updates distribution points with the selected boot image by using the latest Configuration Manager production client components. You can also choose to reload the boot image with the latest version of Windows PE located in the installation directory of the Windows Assessment and Deployment Kit (ADK).

The content of this boot image package will be updated on the Distribution Points where it was previously distributed.

Current Windows ADK version: 10.0.18362.0. Current production client version: 5.00.8790.1007.

Reload this boot image with the current Windows PE version from the Windows ADK

Boot Image: "IGEL Boot Image"

Version	Comment	OS Version	Client Version	Package ID
1	WinPE Boot Image for d...	10.0.18362.1	5.00.8790.1007	P010005A

< Previous Next > Summary Cancel

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.

How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on

A screenshot of the Microsoft Configuration Manager interface. The title bar reads "Microsoft Configuration Manager (Connected to P01, Windows Site - win-sccmsrv.winsccm.test)". The ribbon menu has "Home" selected. The main pane shows a "Task Sequences 3 items" list with three entries: "IGEL Create", "IGEL Create over network share", and "IGEL Install". The entry "IGEL Create" is selected, and its properties are displayed in the details pane below. A context menu is open over the selected item, with the "Edit" option highlighted by a red box. The details pane shows the following summary:

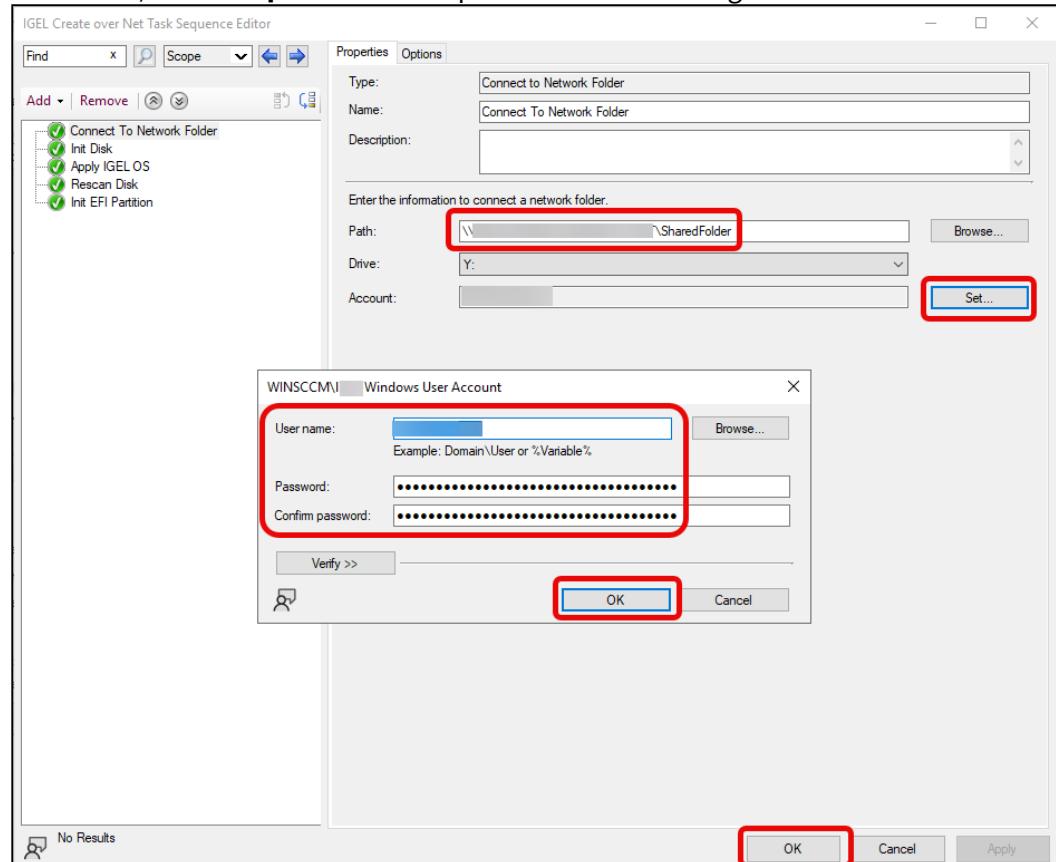
Name:	P0100256
Description:	
Package ID:	4
Package Type:	
Boot Image ID:	P0100253

Related Objects: Deployments

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**.

How to Deploy IGEL OS 12 with IGEL OS 12 SCCM Add-on

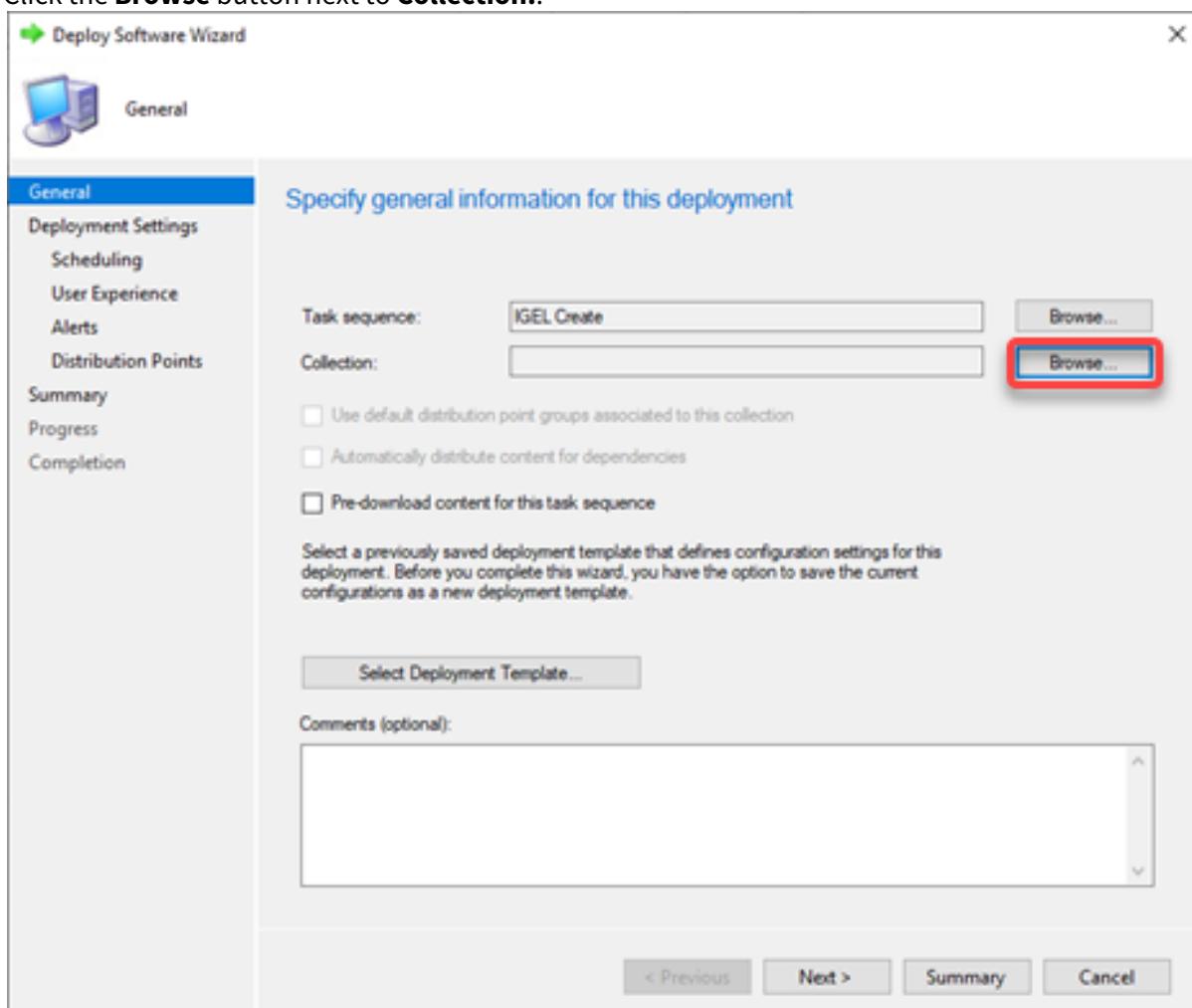
A screenshot of the Microsoft Configuration Manager interface. The left navigation pane shows "Software Library" with "Task Sequences" selected. The main area displays a table titled "Task Sequences 3 items" with three entries: "IGEL Create" (Package ID: P0100254), "IGEL Create" (Package ID: P0100256), and "IGEL Inc." (Package ID: P0100255). The "IGEL Create" entry from February 5th is selected. A context menu is open over this entry, with the "Deploy" option highlighted and surrounded by a red box. Other options in the menu include View, Edit, Enable, Disable, Export, Copy, Refresh, Delete, Distribute Content, Create Prestaged Content File, Create Phased Deployment, Move, Set Security Scopes, and Properties. Below the table, a "Summary" section provides details for the selected item: Name: IGEL Create, Description: , Package ID: P0100254, Package Type: 4, Boot Image ID: P0100253. A "Related Objects" section shows a link to "Deployments".

Icon	Name	Description	Package ID	Date Created	Size (KB)	Enabled
IGEL Create	IGEL Create		P0100254	05.02.2024 10:03	3	Yes
IGEL Create	IGEL Create		P0100256	05.02.2024 10:03	4	Yes
IGEL Inc.	IGEL Inc.		P0100255	05.02.2024 10:03	4	Yes

The **Deploy Software Wizard** opens.

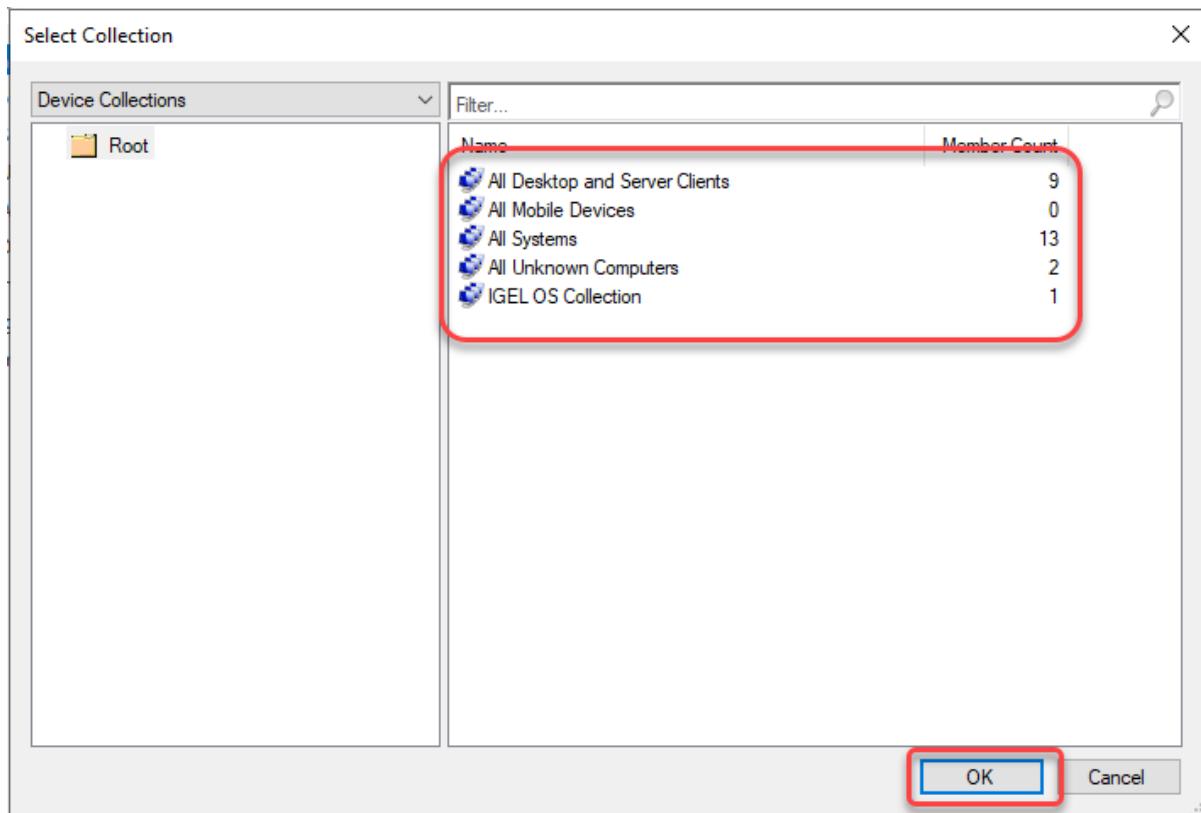


9. Click the **Browse** button next to **Collection**:



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.

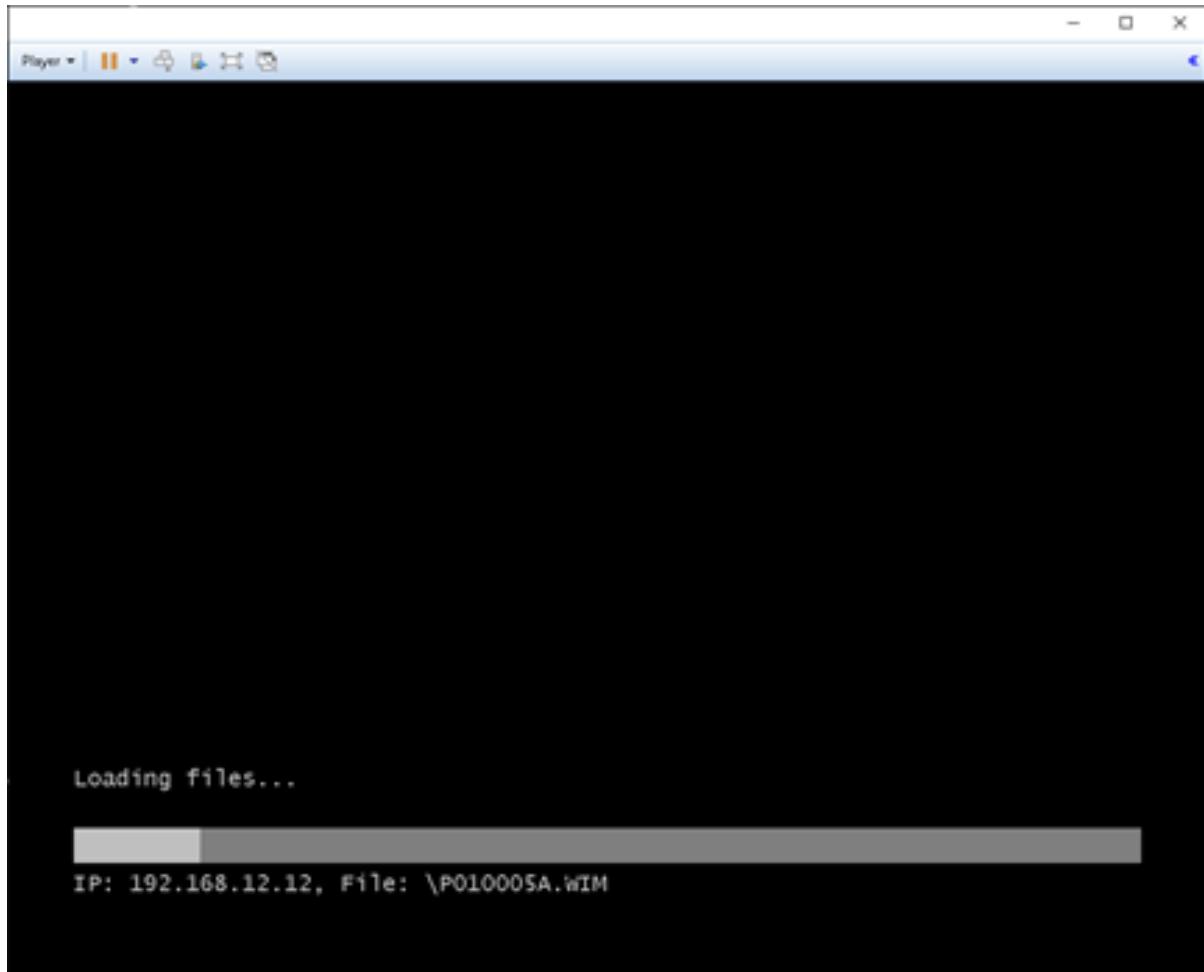
The screenshot shows the 'Deploy Software Wizard' window with the title 'General'. On the left is a navigation pane with tabs: General (selected), Deployment Settings, Scheduling, User Experience, Alerts, Distribution Points, Summary, Progress, and Completion. The main area is titled 'Specify general information for this deployment'. It contains fields for 'Task sequence' (set to 'IGEL Create') and 'Collection' (set to 'IGEL OS Collection'). Below these are three checkboxes: 'Use default distribution point groups associated to this collection', 'Automatically distribute content for dependencies', and 'Pre-download content for this task sequence'. A note below the checkboxes says: 'Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard, you have the option to save the current configurations as a new deployment template.' At the bottom are buttons for 'Select Deployment Template...', 'Comments (optional)', and a footer with buttons for '< Previous', 'Next >' (which is highlighted with a red box), 'Summary', and 'Cancel'.

All target devices receive the PXE boot request that triggers them to boot the IGEL Boot Image.

A screenshot of a terminal window titled "Player". The window displays a series of deployment logs. At the top, it shows copyright information for VMware (1983-2018) and Intel (1997-2008). Below that, network configuration details are listed: CLIENT MAC ADDR, GUID, CLIENT IP (255.255.255.0), MASK (255.255.255.0), and DHCP IP. The log continues with GATEWAY IP, a message about downloading WDSNBP from a server, and noting the architecture as x64. It then provides instructions for administrators regarding PXE boot requests. Further down, it shows pending request ID (8), a message from the administrator (SCCM PXE), and details about contacting a server and performing a TFTP download. Finally, it prompts the user to press F12 for network service boot.

```
Copyright (C) 1983-2018 VMware, Inc.  
Copyright (C) 1997-2008 Intel Corporation  
  
CLIENT MAC ADDR: [REDACTED] GUID: [REDACTED]  
CLIENT IP: [REDACTED] MASK: 255.255.255.0 DHCP IP: [REDACTED]  
GATEWAY IP: [REDACTED]  
  
Downloaded WDSNBP from [REDACTED]  
  
Architecture: x64  
  
The details below show the information relating to the PXE boot request for  
this computer. Please provide these details to your Windows Deployment Services  
Administrator so that this request can be approved.  
  
Pending Request ID: 8  
  
Message from Administrator:  
SCCM PXE  
  
Contacting Server: [REDACTED]  
TFTP Download: smsboot [REDACTED]  
  
Press F12 for network service boot
```

The target devices load the IGEL Boot Image (WIM).



Alternative Deployment

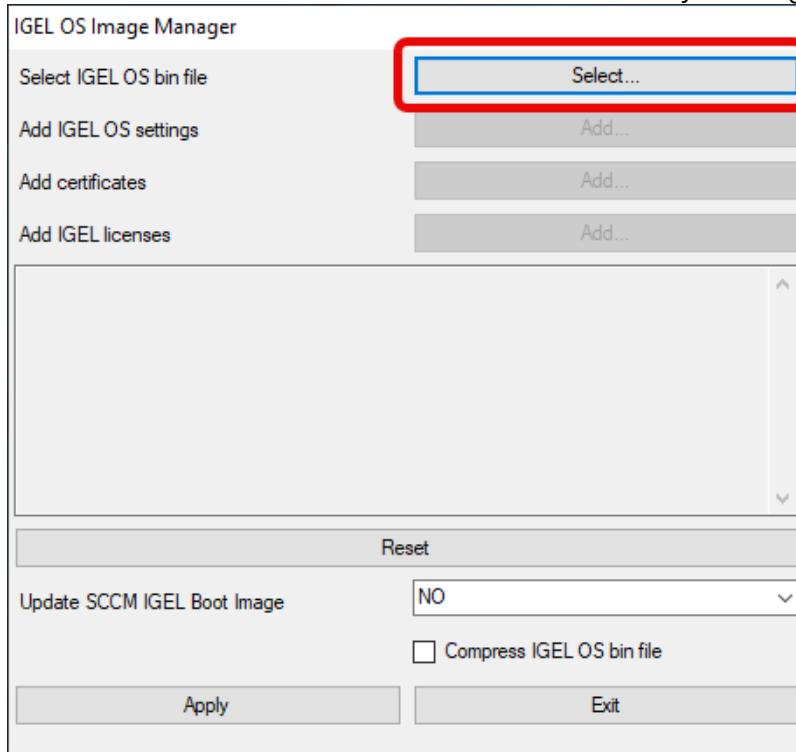
You can deploy a different IGEL OS image as an alternative to the image that comes with IGEL OS SCCM Add-on. The current main version is available from igel.com²¹. Optionally, you can add pre-configured settings, certificates, and license files to the image. In addition, you can compress the image to 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.

²¹ <http://igel.com>



3. Click **Select** next to **Select IGEL OS bin file** and choose your image file.

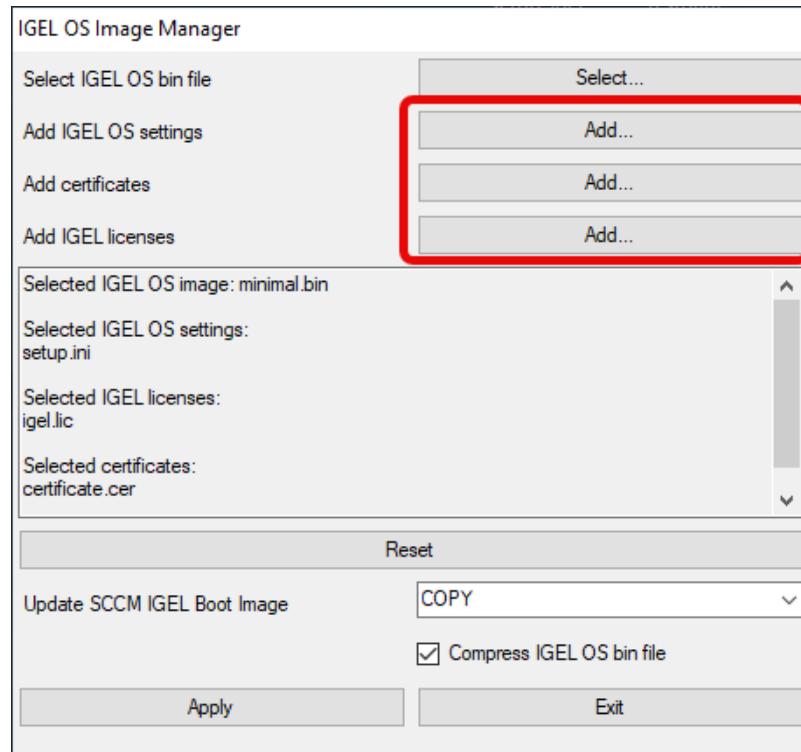


4. If you want to add settings, certificates, or license files, click **Add** next to the relevant item and choose the relevant files.

- **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

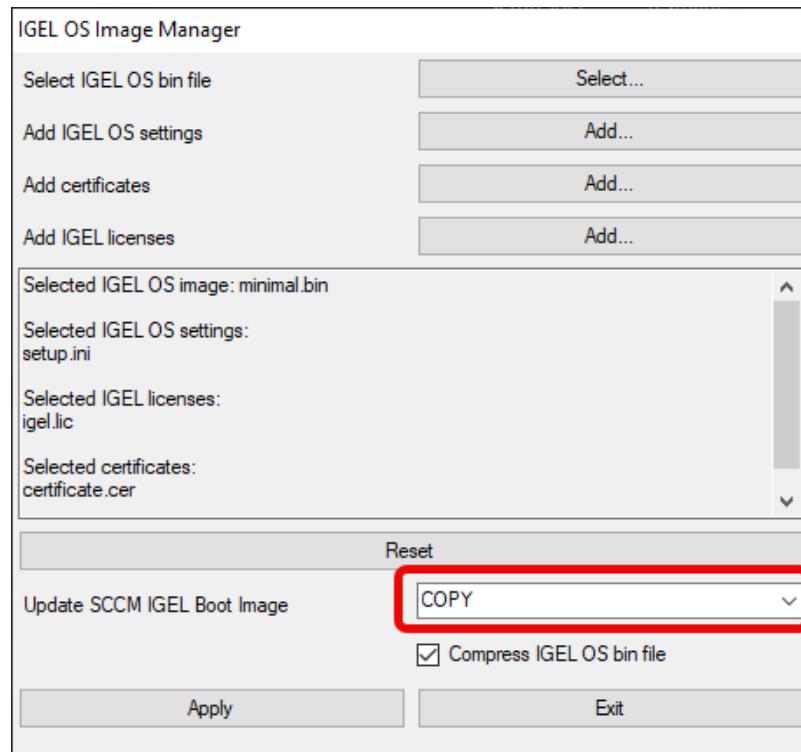


- **Add IGEL licenses:** License files

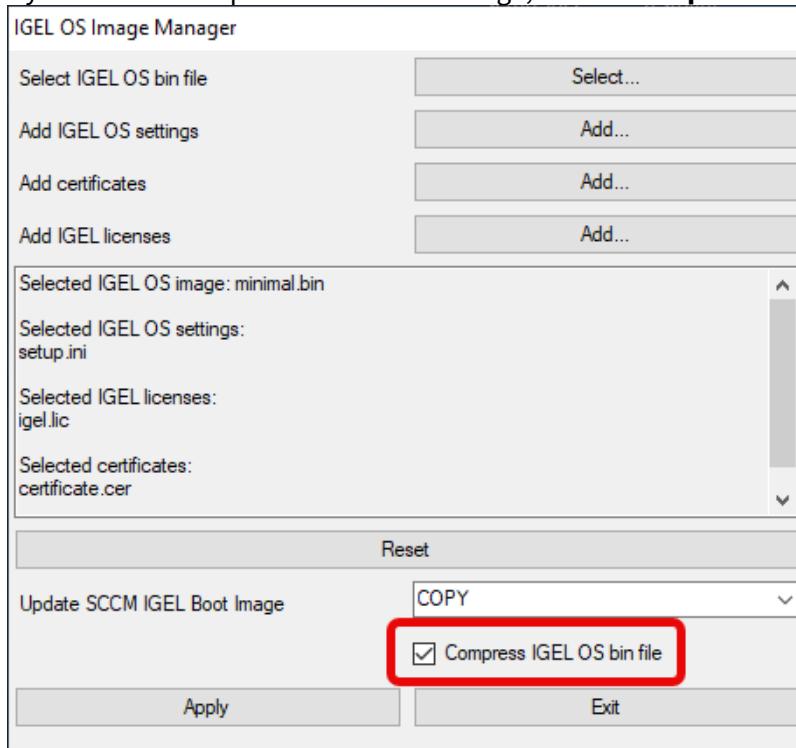


5. Set **Update SCCM IGEL Boot Image** according to your deployment method:

- **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**.A screenshot of the IGEL OS Image Manager application window. The interface includes sections for selecting IGEL OS bin file, adding settings, certificates, and licenses. Below these are lists of selected files: 'Selected IGEL OS image: minimal.bin', 'Selected IGEL OS settings: setup.ini', 'Selected IGEL licenses: igel.lic', and 'Selected certificates: certificate.cer'. At the bottom, there are buttons for 'Reset', 'Update SCCM IGEL Boot Image' (set to 'COPY'), a checked checkbox for 'Compress IGEL OS bin file', and two main action buttons: 'Apply' (which is highlighted with a red box) and 'Exit'.

The files are added to the image.

A screenshot of the IGEL OS Image Manager application window, similar to the previous one but showing the process of adding files. The 'Selected IGEL OS settings' section shows 'setup.ini' with a status message 'Please Wait...'. The 'Selected IGEL license' section shows 'igel.lic' with a green progress bar indicating the addition process. The rest of the interface is identical to the first screenshot, with the 'Apply' button highlighted by a blue border.



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 5).

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](#)²².
- 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.

²² <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

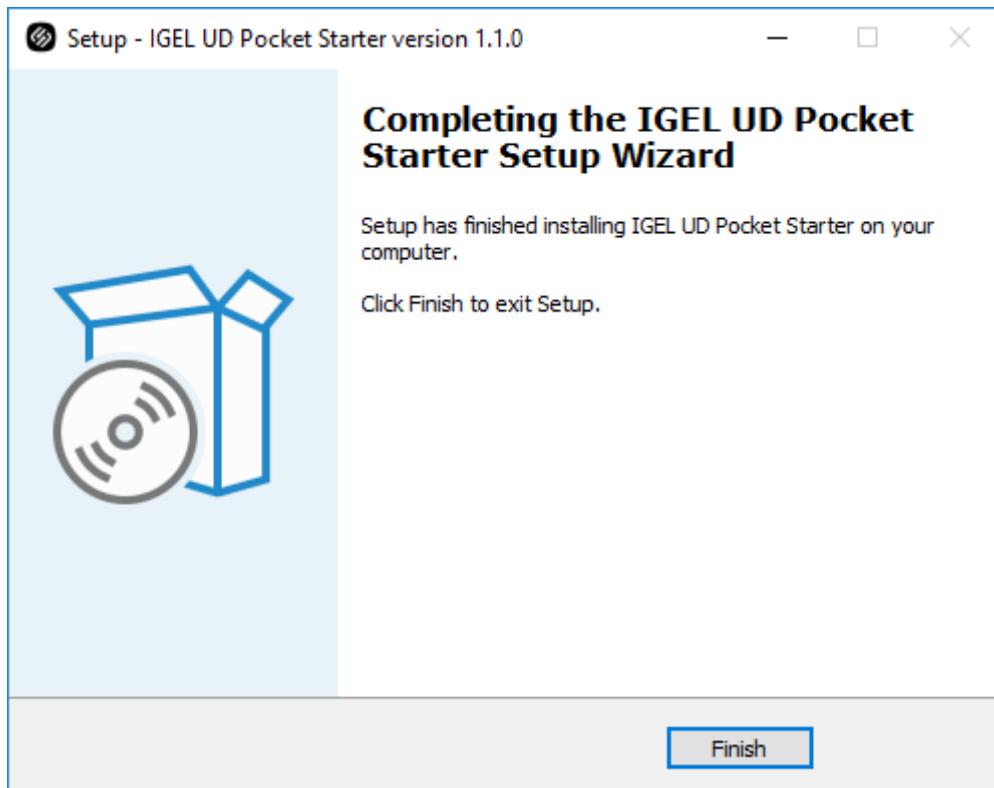
Setup - IGEL UD Pocket Starter version 1.1.0

Installing

Please wait while Setup installs IGEL UD Pocket Starter on your computer.

Installing IGEL Bootloader ...

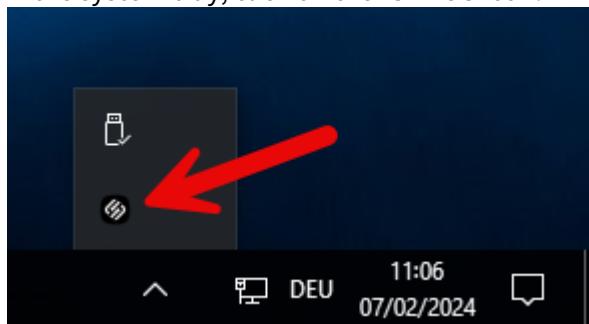
Cancel



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.

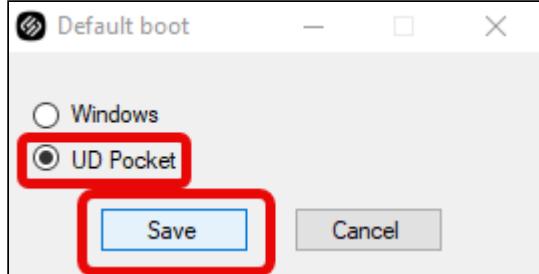


2. Choose the desired default operating system and click **Save**.

- **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 415).

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 416).

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**.

The screenshot shows the 'Single Sign-On with Identity Provider' configuration dialog. The 'Identity Providers' section is highlighted with a red box. It contains the following fields:

- Identity Provider: Okta
- Okta URL: https://mycompany.okta.com
- Client ID: (redacted)
- Client secret: (redacted)

Buttons at the bottom include 'Close', 'Save', and 'Save and Close'.

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 AD**.
- 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.



The screenshot shows the IGEL OS web interface with the 'Security' tab selected. On the left, a sidebar menu under 'Logon' includes options like 'Device Encryption', 'Password', 'Logon' (with 'Taskbar' and 'Active Directory/Kerberos' collapsed), 'Single Sign-On' (which is expanded and highlighted in yellow), 'Local User', 'Active Directory/Kerberos', 'Smartcard', 'Change password', and 'Update'. A red box highlights the 'Identity Providers' configuration dialog. This dialog has a title bar with a checkmark and the text 'Single Sign-On with Identity Provider'. It contains four input fields: 'Identity Provider' set to 'Azure AD', 'Azure AD Tenant Name/ID' (redacted), 'Application (client) ID' (redacted), and 'Client secret' (redacted). Below these fields is a 'Change password' button. At the bottom of the dialog are three buttons: 'Close', 'Save', and 'Save and Close'.

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**:

A screenshot of the IGEL OS Settings interface. The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (highlighted in yellow), System, and Apps. Below the navigation is a search bar and a gear icon. The main content area has a sidebar with sections like Device Encryption, Password, Logon (Taskbar, Active Directory/Kerberos, Single Sign-On, Local User), Active Directory/Kerberos, Smartcard, Change password, and Update. The Single Sign-On section is currently selected. A large central panel titled "Identity Providers" contains fields for "Identity Provider" (set to Okta), "Okta URL" (https://mycompany.okta.com), "Client ID" (redacted), and "Client secret" (redacted). A "Change password" button is also present. A red box highlights the "Identity Provider" dropdown. At the bottom are "Close", "Save", and "Save and Close" buttons.

Device Encryption

Password

Logon

- Taskbar
- Active Directory/Kerberos
- Single Sign-On
- Local User

Active Directory/Kerberos

Smartcard

Change password

Update

Identity Providers

Identity Provider

Okta

Okta URL

https://mycompany.okta.com

Client ID

Client secret

Change password

Close

Save

Save and Close



Upgrading from IGEL OS 11 to IGEL OS 12

For instructions on how to upgrade endpoint devices from IGEL OS 11.09.100 to IGEL OS 11 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\(see page 11\)](#).
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:



```

HWI_SUPPORT=0 HWI_PRODUCT_ID=1 HWI_HARDWARE_ID=0 HWI_HARDWARE_NAME='Legacy_x86_system'
root@ITC54E1AD8CECBE:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda     8:0    0 238,5G  0 disk
└─sda1  8:1    0   9M  0 part
└─sda2  8:2    0 200M  0 part
└─sda3  8:3    0 200M  0 part
└─sda4  8:4    0 63,6G  0 part
sdb     8:16   1  7,5G  0 disk
└─sdb1  8:17   1  2,2G  0 part
└─sdb2  8:18   1   50M  0 part
igf0    61:0    0 63,6G  0 disk
igf1    61:1    0 746,6M 0 disk /dev/.mnt-system/ro/sys
igf23   61:23   0   3,3M 0 disk /dev/.mnt-system/ro/bootsplash
igf26   61:26   0 21,5M 0 disk /dev/.mnt-system/ro/services/cjk
igf39   61:39   0   7,6M 0 disk /dev/.mnt-system/ro/services/cups
igf55   61:55   0   3,6M 0 disk
igf60   61:60   0 374,7M 0 disk /dev/.mnt-system/ro/services/nvgfx
igf66   61:66   0 14,6M 0 disk
igf68   61:68   0  876K 0 disk /dev/.mnt-system/ro/services/fonts
igf94   61:94   0 88,3M 0 disk /dev/.mnt-system/ro/services/hpihvdoc
igf200  61:200  0 128M 0 disk
└─200   253:2  0 128M 0 dm  /userhome/.pki
igf239  61:239 0   1G 0 disk
└─239   253:1  0   1G 0 dm  /cache
igf254  61:254 0   5M 0 disk /license
igf255  61:255 0  24M 0 disk
└─255   253:0  0  24M 0 dm
zram0  252:0  0  1,1G 0 disk [SWAP]
zram1  252:1  0  1,1G 0 disk [SWAP]
zram2  252:2  0  1,1G 0 disk [SWAP]
zram3  252:3  0  1,1G 0 disk [SWAP]
root@ITC54E1AD8CECBE:~# pwd
/root
root@ITC54E1AD8CECBE:~# mkdir stick
root@ITC54E1AD8CECBE:~# ls
stick
root@ITC54E1AD8CECBE:~#

```

- 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/
```

- Use your favorite text editor, e.g. `vi`, to create your `unit_id_rules.ini` file.

```
vi stick/igel/unit_id_rules.ini
```

A screenshot of a "Local Terminal" window. The window title is "Local Terminal". The terminal content shows the command "prefer_wireless,ignore_licensed,reverse_order" being typed. After the command is entered, the terminal displays the creation of a file: "stick/igel/unit_id_rules.ini" and its size: "1L, 46C".

```
prefer_wireless,ignore_licensed,reverse_order
stick/igel/unit_id_rules.ini
"stick/igel/unit_id_rules.ini" 1L, 46C
```

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 Azure AD
- OpenID Connect
- Ping Identity | PingOne
- VMware Workspace ONE Access

ⓘ 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 Azure AD

- 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 OpenID Connect (Generic)

Generic OpenID Connect is supported by IGEL OS 12.3 or higher.

- Web apps (SSO via Chromium)
- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with Ping Identity / PingOne

Ping Identity / PingOne is supported by IGEL OS 12.3 or higher.

- Web apps (SSO via Chromium)
- Device login
- Screenlock

Apps and Utilities for IGEL OS 12 That Support SSO with VMware Workspace ONE Access

VMware Workspace ONE Access is supported by IGEL OS 12.3 or higher.

- VMware Horizon (if Chromium is used for authentication)
- Web apps (SSO via Chromium)
- Device login
- Screenlock

Setting up SSO with Azure AD

To enable SSO with Azure ID on IGEL OS 12 devices, an Azure application must be registered first. Then, you can configure IGEL OS 12 to use this application for authentication; the Azure application is referenced via its Public Client Identifier.

Registering an Azure Application

1. In your Azure 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 ... X

* Name
The user-facing display name for this application (this can be changed later).
 ✓

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.
 ✓

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.

The screenshot shows the Microsoft Azure portal interface for managing API permissions. The left sidebar lists various management options like Overview, Quickstart, Integration assistant, and API permissions, with 'API permissions' selected and highlighted by a red box. The main content area displays the 'Configured permissions' section for the 'Microsoft Graph (1)' API. A specific permission, 'User.Read', is highlighted with a red box. The table below provides details about this permission:

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)	Delegated	Sign in and read user p...	No	...
User.Read	Delegated	Sign in and read user p...	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

**4. Click Add a permission.**

The screenshot shows the Microsoft Azure portal interface for managing API permissions. The left sidebar has a 'Manage' section with various options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (which is selected and highlighted in grey), Expose an API, App roles, Owners, Roles and administrators, and Manifest. Below that is a 'Support + Troubleshooting' section with Troubleshooting and New support request. The main content area is titled 'IGEL OS Single sign-on | API permissions'. It includes a search bar, refresh button, and feedback link. A note says '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.' A red box highlights the '+ Add a permission' button. Below it is a table with one row for 'Microsoft Graph (1)'. The table columns are API / Permissions name, Type, Description, Admin consent req..., and Status. The row shows 'User.Read', 'Delegated', 'Sign in and read user profile', 'No', and three vertical dots. A note at the bottom says 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.'

API / Permissions name	Type	Description	Admin consent req...	Status
User.Read	Delegated	Sign in and read user profile	No	...



5. Select Microsoft Graph.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps Integrate with Azure DevOps and Azure DevOps server

Azure Service Management Programmatic access to much of the functionality available through the Azure portal

Office 365 Management APIs Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

More Microsoft APIs

Azure Batch Schedule large-scale parallel and HPC applications in the cloud

Azure Communication Services Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Cosmos DB Fast NoSQL database with open APIs for any scale

Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake Access to storage and compute for big data analytic scenarios

Azure Import/Export Programmatic control of import/export jobs

Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults



6. Select **Delegated permissions**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with navigation links like Home, Overview, Quickstart, Integration assistant, Manage (with sub-options: Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions), and Support + Troubleshooting. The 'API permissions' link under 'Manage' is highlighted with a red box. In the main content area, a dialog titled 'Request API permissions' is open for the 'IGEL OS Single sign-on' app. It shows the 'Microsoft Graph' API selected from a list of 'All APIs'. The 'Delegated permissions' section is highlighted with a red box and contains the text: 'Your application needs to access the API as the signed-in user.' To the right, the 'Application permissions' section is visible with the note: 'Your application runs as a background service or daemon without a signed-in user.'

7. Enable the following permissions and then click **Add permissions**:

- **email**
- **openid**

How to Configure Single Sign-On (SSO) on IGEL OS 12



• profile

The screenshot shows the 'Request API permissions' dialog in the Microsoft Azure portal. The left sidebar shows the 'IGEL OS Single sign-on' app registration with the 'API permissions' section selected. The main area displays the 'Request API permissions' dialog for the 'Microsoft Graph' API. The 'Delegated permissions' section is selected, showing three permissions: 'email', 'openid', and 'profile'. The 'email' and 'profile' checkboxes are checked and highlighted with red boxes. The 'Add permissions' button at the bottom is also highlighted with a red box.

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

Start typing a permission to filter these results

Permission Admin consent required

OpenId permissions (3)

Permission	Admin consent required
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

Add permissions Discard



8. Check if the permissions are correct.

Screenshot of the Microsoft Azure portal showing the API permissions for the "IGEL OS Single sign-on" application. The "API permissions" section is selected in the left sidebar. A red box highlights the "User.Read" permission row in the table below.

API / Permissions name	Type	Description	Admin consent req...	Status
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...



9. Go to **Certificates & secrets** and click **New client secret**.

The screenshot shows the Microsoft Azure portal interface for managing application registrations. The URL in the address bar is `All services > [redacted] | App registrations > IGEL OS Single sign-on`. The main title is **IGEL OS Single sign-on | Certificates & secrets**. On the left, there's a sidebar with various management options like Overview, Quickstart, Integration assistant, etc., and a specific section for **Certificates & secrets**, which is highlighted with a red box. In the center, there are three tabs: **Certificates (0)**, **Client secrets (0)** (which is currently selected), and **Federated credentials (0)**. Below the tabs, it says, "A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password." A red box highlights the **+ New client secret** button. At the bottom, there's a table header with columns: **Description**, **Expires**, **Value ⓘ**, and **Secret ID**. A note below the table states, "No client secrets have been created for this application."



10. Enter a **Description**, define when the secret **Expires**, and then click **Add**.

The screenshot shows the Microsoft Azure portal interface for managing app registrations. The left sidebar shows navigation options like Overview, Quickstart, Integration assistant, Manage (with sub-options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest), and Support + Troubleshooting. The main content area is titled 'IGEL OS Single sign-on | Certificates & secrets'. It displays a message about credentials enabling confidential applications to interact with external locations via HTTPS. Below this, there are tabs for Certificates (0), Client secrets (0), and Federation (0). Under 'Client secrets (0)', it says 'A secret string that the application uses to prove its identity'. A 'New client secret' button is available. On the right, a modal window titled 'Add a client secret' is open. It has two input fields: 'Description' (with placeholder 'Enter a description for this client secret') and 'Expires' (set to 'Recommended: 180 days (6 months)'). At the bottom of the modal are 'Add' and 'Cancel' buttons, with the 'Add' button being highlighted with a red box.



11. Copy the **Value of the client secret.**

The screenshot shows the 'Certificates & secrets' tab selected in the left sidebar. Under 'Client secrets (1)', there is one entry for 'IGEL OS SSO client secret'. The 'Value' field is highlighted with a red box. The 'Secret ID' field is also visible.

Description	Expires	Value	Secret ID
IGEL OS SSO client secret	9/19/2023	[Redacted Value]	[Redacted Secret ID]

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**.**

The screenshot shows the 'Overview' tab selected in the left sidebar. The 'Essentials' section displays the following information:

- Display name: **IGEL OS Single sign-on**
- Client credentials: [Add a certificate or secret](#)
- Redirect URLs: **0 web, 0 spa, 1 public client**
- Application ID URI: [Add an Application ID URI](#)
- Managed application in local directory: **IGEL OS Single sign-on**

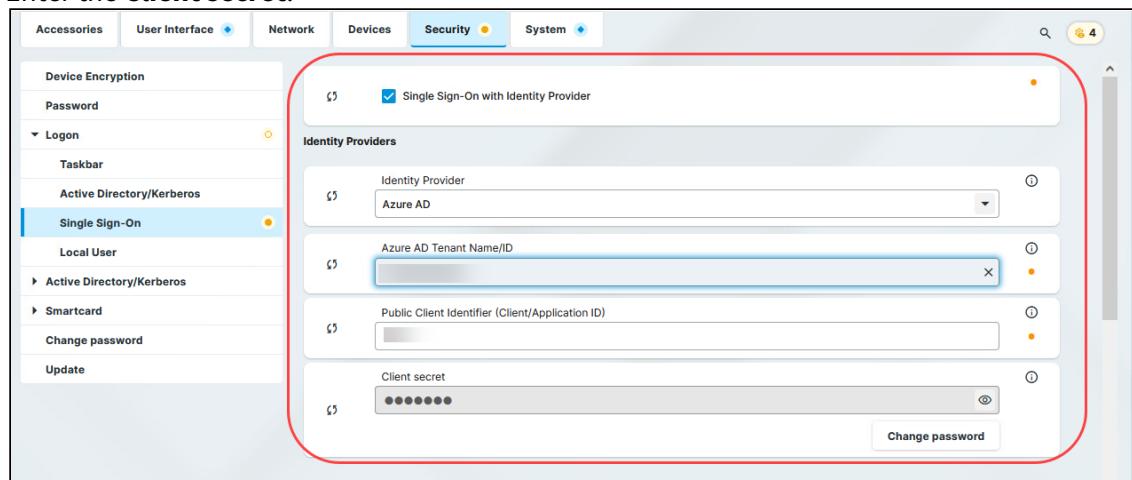
Two specific fields are highlighted with red boxes:

- Application (client) ID**: `af6a0051-00a0-49d9-ad91-8e67527946ec`
- Directory (tenant) ID**: `b04c40d3-3e10-4e10-8d01-8c54f965a70`



Configuring IGEL OS for SSO with Azure 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 AD**.
 - 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. 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 Azure AD](#)(see page 427).

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**.

A screenshot of the Okta Applications page. On the left, there's a sidebar with categories like Dashboard, Directory, Customizations, Applications (which is expanded and has 'Applications' highlighted with a red box), Self Service, Security, Workflow, Reports, and Settings. At the top right, there's a search bar and several buttons: 'Create App Integration' (highlighted with a red box), 'Browse App Catalog', 'Assign Users to App', and 'More'. Below these buttons is a table titled 'STATUS' with two rows: 'ACTIVE' (4 entries) and 'INACTIVE' (4 entries). Each row lists an application name, its icon, and a settings gear icon. The applications listed are: 'IGEL OS 12 Native App' (Client ID: 9ad9167cfa1f991c0d7), 'Okta Admin Console', 'Okta Browser Plugin', and 'Okta Dashboard'.

STATUS	Count
ACTIVE	4
INACTIVE	4

2. Edit the settings as follows and then click **Next**.
 - Set **Sign-in method** to **OIDC - OpenID Connect**.



- Set **Application type** to **Native Application**.

The screenshot shows the 'Create a new app integration' dialog in the Okta interface. The 'Sign-in method' section is visible, with 'OIDC - OpenID Connect' selected. The 'Application type' section is also visible, with 'Native Application' selected. Both sections have red boxes around them, and the 'Next' button at the bottom right is also highlighted with a red box.

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 screenshot shows the Okta configuration interface for a new native app integration. The 'App integration name' field is set to 'IGEL OS Single sign-on'. Under 'Grant type', 'Authorization Code' is selected. In the 'Sign-in redirect URIs' section, the URL 'http://localhost/callback' is entered. Both fields are highlighted with red boxes.

General Settings

App integration name: IGEL OS Single sign-on

Logo (Optional)

Grant type

Client acting on behalf of a user

- Authorization Code
- Refresh Token
- Resource Owner Password
- SAML 2.0 Assertion
- Device Authorization
- Token Exchange
- Implicit (hybrid)

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Allow wildcard * in sign-in URI redirect.

http://localhost/callback

+ Add URI

The app integration is created.



4. Select the **General** tab and then click **Edit**.

A screenshot of the Okta application configuration interface. At the top, there's a search bar and navigation links for 'Back to Applications', 'IGEL OS Single sign-on' (which is active, indicated by a blue background), 'Active', and 'View Logs'. Below this is a tabs menu with 'General' (highlighted with a red box and underlined), 'Sign On', 'Mobile', 'Assignments', and 'Okta API Scopes'. The main content area is titled 'Client Credentials' and contains fields for 'Client ID' (with an 'Edit' button highlighted with a red box) and 'Client authentication' (with radio buttons for 'None', 'Client secret', and 'Public key / Private key', where 'Client secret' is selected). There's also a checkbox for 'Proof Key for Code Exchange (PKCE)' which is checked, and another for 'Require PKCE as additional verification' which is also checked. A note below the Client ID field states: 'Public identifier for the client that is required for all OAuth flows.'

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**.

A screenshot of the Okta Client Credentials configuration page. The page has a header with tabs: General (selected), Sign On, Mobile, Assignments, and Okta API Scopes. Below the tabs is a section titled "Client Credentials" with a "Cancel" button. Under "Client ID", there is a placeholder value. Under "Client authentication", the "Client secret" radio button is selected. A checkbox for "Require PKCE as additional verification" is checked and highlighted with a red box. Below this is a "CLIENT SECRETS" section with a "Generate new secret" button. A table shows a single client secret entry with columns: Creation date, Secret, and Status. A note says "A new client secret is generated after you click Save". At the bottom are "Save" and "Cancel" buttons, with the "Save" button also highlighted with a red box.

Client ID: [REDACTED]
Client authentication:
 None
 Client secret
 Public key / Private key
Proof Key for Code Exchange (PKCE)
 Require PKCE as additional verification

CLIENT SECRETS

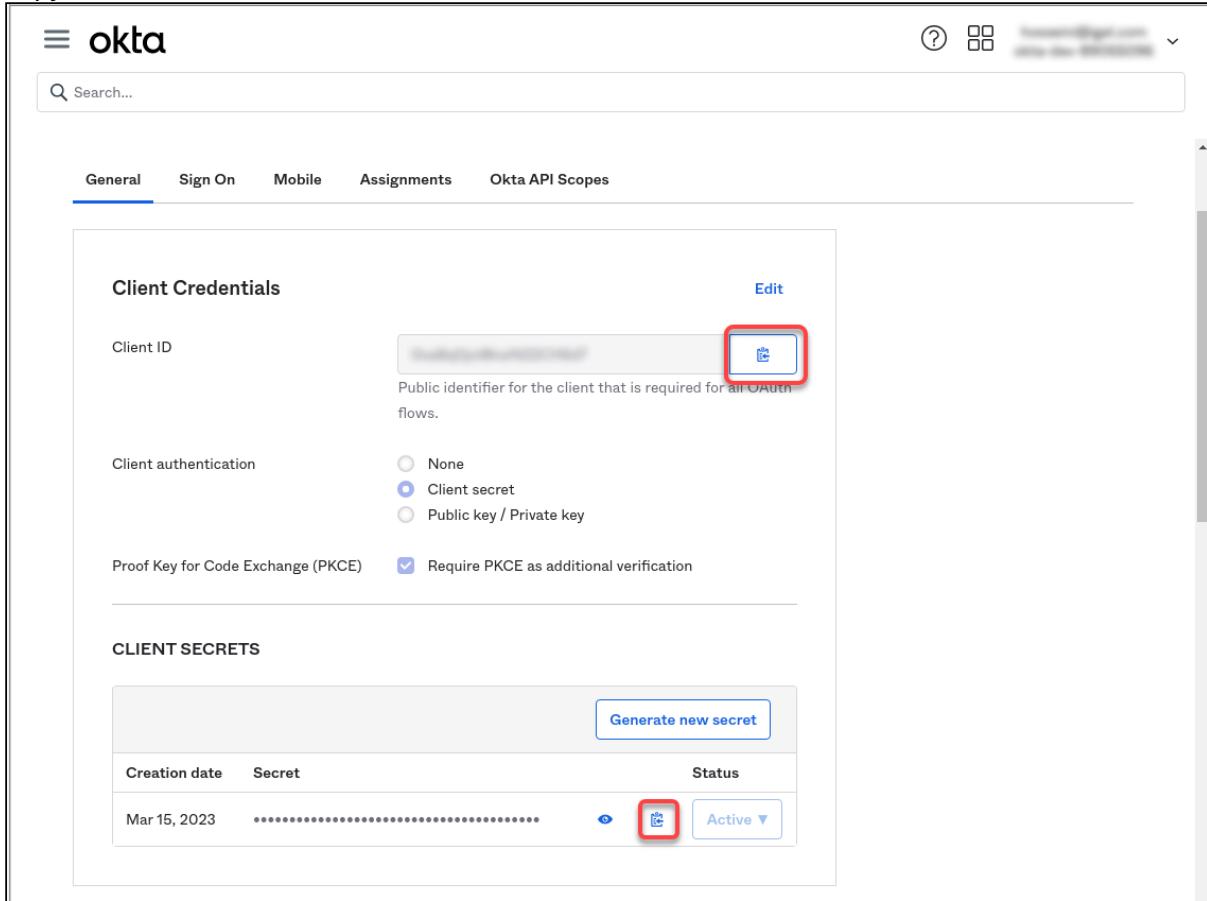
Creation date	Secret	Status
A new client secret is generated after you click Save		

Save **Cancel**

The client secret will be created.



6. Copy the **Client ID** and the **Secret** (client secret).



The screenshot shows the Okta client configuration page. The 'General' tab is selected. In the 'Client Credentials' section, the 'Client ID' field is highlighted with a red box. Below it, the 'Client authentication' section shows 'Client secret' selected. In the 'CLIENT SECRETS' section, a table lists a single secret entry. The 'Secret' column for this entry is also highlighted with a red box. The table has columns for 'Creation date', 'Secret', and 'Status'. The status is 'Active' with a dropdown arrow.

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. 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 427). 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.

Configuring SSO with Generic OpenID Connect

Generic OpenID Connect is supported by IGEL OS 12.3 or higher.

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	<code>http://localhost/callback</code>
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/realm/yourrealm>
 - Provide the **Client ID**. This is the client ID that was created in the IdP console.
 - Provide the **Client secret**.

A screenshot of the IGEL OS configuration interface, specifically the "Single Sign-On" section. A large red oval highlights the entire form. At the top, there is a checked checkbox labeled "Single Sign-On with Identity Provider". Below it, under "Identity Providers", there is a dropdown menu set to "OpenID Connect". The next section contains fields for "Issuer URL" (with a value of "https://keycloak.../realms/..."), "Client ID" (with a value of "IGEL_OS_SSO"), and "Client secret" (with a value of "....."). A "Change password" button is located at the bottom right of this section. In the top right corner of the interface, there is a "Related pages" link.

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 428).

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.



Setting up SSO with Ping Identity / PingOne

Ping Identity / PingOne is supported by IGEL OS 12.3 or higher.

Setting up Your Application

1. Log in to your PingIdentity account, go to **Applications**, and click the add symbol to create a new application.

A screenshot of the PingIdentity web interface. On the left is a dark sidebar with various navigation options like 'Getting Started', 'Overview', 'Monitoring', 'Directory', 'Applications' (which is highlighted with a red box), 'Application Catalog', 'Resources', and 'Application Portal'. Below these are sections for 'Authentication', 'Threat Protection', and 'Identity Verification'. The main content area has a header 'trial_igel_ > Customer Solution Environment'. It shows a list titled 'Applications' with a blue '+' button. Below it is a search bar and a 'Filter' button. The list contains four items:

- Getting Started Application** (Client ID: [redacted])
- PingOne Admin Console** (Client ID: [redacted])
- PingOne Application Portal** (Client ID: [redacted])
- PingOne Self-Service - MyAccount** (Client ID: [redacted])



2. Provide an **Application Name**, select **Native** as the **Application Type**, and click **Save**.

Add Application

Application Name *
IGEL OS Single Sign-On

Description

Icon

Max Size 1.0 MB

Application Type [Show Details](#)

SAML Application **OIDC Web App** **Native** **Single-Page** **Worker**

Save [Cancel](#)

The form is a modal window titled "Add Application". It has fields for "Application Name" (containing "IGEL OS Single Sign-On"), "Description" (empty), "Icon" (placeholder image), and "Max Size 1.0 MB". Under "Application Type", there are five options: "SAML Application", "OIDC Web App", "Native" (which is highlighted with a red box), "Single-Page", and "Worker". At the bottom are "Save" and "Cancel" buttons, with "Save" also highlighted with a red box.



3. Select the **Configuration** tab and click the edit button.

The screenshot shows the 'IGEL OS Single Sign-On' configuration interface. The 'Configuration' tab is selected and highlighted with a red box. A red box also highlights the edit button (a pencil icon) in the top right corner of the main content area. The configuration details for an OIDC application are displayed, including fields for Client ID, Client Secret (with a 'Generate New Secret' button), Environment ID, Response Type (Code, ID Token, Access Token), Grant Type (Authorization Code, Implicit), PKCE Enforcement (OPTIONAL), and Redirect URIs (None Specified).

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**.

IGEL OS Single Sign-On > Edit Configuration

Response Type

Code
 Token
 ID Token

Grant Type ?

Authorization Code
PKCE Enforcement
S256_REQUIRED

Implicit
 Client Credentials
 Refresh Token

Redirect URIs

http://localhost/callback

+ Add

Allow Redirect URI patterns ?

Token Endpoint Authentication Method

Client Secret Post

Require Pushed Authorization Request ?

Pushed Authorization Request Reference Timeout * ?

60 Seconds

Save Cancel



5. Select the **Resources** tab and click the edit button.

A screenshot of a web-based configuration interface for IGEL OS Single Sign-On. At the top, there's a header with the title "IGEL OS Single Sign-On" and a "Client ID" input field. To the right of the title are a toggle switch, three vertical dots, and a close button (X). Below the header is a navigation bar with tabs: Overview, Configuration, Resources (which is highlighted with a red box), Policies, Attribute Mappings, Access, and Mobile. A descriptive text below the tabs states: "These resources define the connection between PingOne and the application, and contain scopes, which define application permissions. See [Resources](#)". Under the heading "ALLOWED SCOPES", it says "The openid scope is always granted and cannot be removed." and shows a list with a single item: "openid" (with a blue icon) and "OpenID Connect". On the far right of this section is a red-bordered edit button icon (a pencil inside a square).

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	<input type="checkbox"/>
email	OpenID Connect	<input checked="" type="checkbox"/>
openid	OpenID Connect	<input checked="" type="checkbox"/>
p1:create:device	PingOne API	<input type="checkbox"/>
p1:create:pairingKey	PingOne API	<input type="checkbox"/>
p1:delete:device	PingOne API	<input type="checkbox"/>
p1:delete:pairingKey	PingOne API	<input type="checkbox"/>
p1:delete:sessions	PingOne API	<input type="checkbox"/>
p1:delete:userLinkedAccounts	PingOne API	<input type="checkbox"/>
p1:read:device	PingOne API	<input type="checkbox"/>
p1:read:oauthConsent	PingOne API	<input type="checkbox"/>
p1:read:pairingKey	PingOne API	<input type="checkbox"/>
p1:read:sessions	PingOne API	<input type="checkbox"/>
p1:read:user	PingOne API	<input type="checkbox"/>
p1:read:userConsent	PingOne API	<input type="checkbox"/>
p1:read:userLinkedAccounts	PingOne API	<input type="checkbox"/>
p1:read:userPassword	PingOne API	<input type="checkbox"/>
p1:reset:userPassword	PingOne API	<input type="checkbox"/>



7. Review the list of **ALLOWED SCOPES**.

A screenshot of a web-based application interface titled "IGEL OS Single Sign-On". At the top, there is a header bar with a "Client ID" input field, a toggle switch, and three icons. Below the header, a navigation bar includes tabs for "Overview", "Configuration", "Resources" (which is underlined in blue), "Policies", "Attribute Mappings", "Access", and "Mobile". A note below the tabs states: "These resources define the connection between PingOne and the application, and contain scopes, which define application permissions. See [Resources](#)". Under the heading "ALLOWED SCOPES", it says: "The openid scope is always granted and cannot be removed." There are three listed items, each with a small blue icon and the text "OpenID Connect":

- email
- openid
- profile

A blue edit icon is located at the top right of the "ALLOWED SCOPES" section.

8. Select the Configuration tab and copy the following data for later use:

- **Client ID**



• Client Secret

The screenshot shows the "IGEL OS Single Sign-On" configuration interface. The "Configuration" tab is selected. In the "General" section, two fields have red boxes drawn around their clear (trash can) buttons: "Client ID" and "Client Secret". A blue pencil icon is visible in the top right corner of the main content area.

IGEL OS Single Sign-On

Client ID

Overview Configuration Resources Policies Attribute Mappings Access Mobile

Configuration details for an OIDC application.

URLs ▾

General ▾

Client ID

Client Secret

Generate New Secret

Environment ID

9. Expand the list of **URLs** and copy the **Issuer** URL for later use.

The screenshot shows the 'Configuration' tab of the IGEL OS Single Sign-On application. The 'URLs' section is expanded, displaying various OAuth 2.0 and OpenID Connect endpoints. The 'Issuer' URL is highlighted with a red box. The 'Client ID' field is also partially visible at the bottom.

Endpoint	Value
Authorization URL	https://auth.pingone.eu/as/authorize
Pushed Authorization Request URL	https://auth.pingone.eu/as/par
Token Endpoint	https://auth.pingone.eu/as/token
JWKS Endpoint	https://auth.pingone.eu/c/as/jwks
Userinfo Endpoint	https://auth.pingone.eu/as/userinfo
Signoff Endpoint	https://auth.pingone.eu/as/signoff
OIDC Discovery Endpoint	https://auth.pingone.eu/as/.well-known/openid-configuration
Token Introspection Endpoint	https://auth.pingone.eu/as/introspect
Token Revocation Endpoint	https://auth.pingone.eu/c/as/revoke
Issuer	https://auth.pingone.eu/as



10. Activate your application.

IGEL OS Single Sign-On

Client ID: [REDACTED]

Overview Configuration Resources Policies Attribute Mappings Access Mobile

Configuration details for an OIDC application.

URLs ▾

Authorization URL: https://auth.pingone.eu/[REDACTED]/as/authorize

Pushed Authorization Request URI: https://auth.pingone.eu/[REDACTED]3c/as/par

Token Endpoint: https://auth.pingone.eu/[REDACTED]/as/token

JWKS Endpoint: https://auth.pingone.eu/[REDACTED]/as/jwks

Userinfo Endpoint: https://auth.pingone.eu/[REDACTED]/as/userinfo

Signoff Endpoint: https://auth.pingone.eu/[REDACTED]ic/as/signoff

OIDC Discovery Endpoint: https://auth.pingone.eu/[REDACTED]/as/.well-known/openid-configuration

Token Introspection Endpoint: https://auth.pingone.eu/[REDACTED]/as/introspect

Token Revocation Endpoint: https://auth.pingone.eu/[REDACTED]/as/revoke

Issuer: https://auth.pingone.eu/[REDACTED]/as

General ▾

Client ID: [REDACTED]



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**.

The screenshot shows the 'Single Sign-On with Identity Provider' configuration page. A red circle highlights the entire form area. The page has a header with a 'Related pages' link. Below it, there's a section for 'Identity Providers' with a dropdown menu set to 'Ping Identity | PingOne'. The main configuration area contains fields for 'PingOne issuer URL' (set to 'https://auth.pingone.eu/0815abc-xyz123456/as'), 'Client ID' (redacted), and 'Client secret' (redacted). A 'Change password' button is located at the bottom right of this section.

2. 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 428).

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

VMware Workspace ONE Access is supported by IGEL OS 12.3 or higher.



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**.

A screenshot of the VMware Workspace ONE Access web interface. The top navigation bar shows "Workspace ONE Access" and "Tenant Admin". The left sidebar has sections for "Branding", "Login Preferences", "OAuth 2.0 Management" (which is selected and highlighted in blue), "Password Policy", "Password Recovery", and "User Attributes". The main content area is titled "OAuth 2.0 Management" with the sub-instruction "Grant access to client applications with OAuth 2.0 using Workspace ONE Access as the identity provider." Below this are tabs for "Clients", "Templates", and "UEM". A prominent red box highlights the "ADD CLIENT" button, which is located in a row with "DELETE" and other buttons. The main table below has columns for "Client ID", "Scope", and "Access type". A search bar at the top of the table says "Search for users, groups, or applications".

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.

SAVE
CANCEL

A secret will be available and autogenerated when you click save

Access type*	User Access Token
<hr/>	
Client type*	<input type="radio"/> Public <input checked="" type="radio"/> Confidential
<hr/>	
Client ID*	IGEL_OS_SSO
<small>Characters allowed are: alphanumeric (A-Z, a-z, 0-9) period (.), underscore (_), and hyphen (-) and at sign (@). 256 characters max.</small>	
<hr/>	
Grant type * <small>(i)</small>	<input type="checkbox"/> Client Credentials Grant <input type="checkbox"/> Password Grant <input checked="" type="checkbox"/> Authorization Code Grant <input type="checkbox"/> Refresh Token Grant <small>(i)</small>
<hr/>	
Redirect URI*	http://localhost/callback
<hr/>	
User grant	<input type="checkbox"/> Prompt users for scope acceptance
<hr/>	
Scope*	<input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Profile <input type="checkbox"/> User <input type="checkbox"/> NAPPS <input checked="" type="checkbox"/> OpenID <input type="checkbox"/> Group <input type="checkbox"/> Admin
<hr/>	
PKCE support	<input checked="" type="checkbox"/>
<small>PKCE Support is enabled when Authorization Code Grant is selected in Grant type</small>	
<hr/>	
Token type	Bearer
<hr/>	
Issue refresh token	<input type="checkbox"/>
<hr/>	
Access token TTL *	3 hours
<hr/>	
Idle token TTL	10 days

3. Review the settings and copy the following data for later use:

- **Client ID**



- **Shared Secret**

OAuth 2.0 Management > IGEL_OS_SSO

EDIT **DELETE**

Client Information

⚠ Copy the shared secret before leaving this page, or you will need to regenerate the secret.

Client ID	IGEL_OS_SSO	COPY
Shared Secret	COPY

Client Configuration

Access type	User Access Token
Client type	Confidential
Client ID	IGEL_OS_SSO
Redirect URI	http://localhost/callback
Scope	Email, Profile, OpenID
Issue refresh token	Disabled
Access token TTL	3 hours
Idle token TTL	10 days
Grant type	Authorization Code Grant
PKCE support	Activated
User Consent Prompt	Disabled

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**.

The screenshot shows the 'Single Sign-On with Identity Provider' configuration screen. It includes fields for 'Identity Provider' (set to 'VMware Workspace ONE Access'), 'Workspace ONE Access issuer URL' (set to 'https://.../SAAS/auth'), 'Client ID' (set to 'IGEL_OS_SSO'), and 'Client secret' (containing '*****'). A red box highlights the 'Client secret' field.

2. 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 428).

If you want to use multi-factor authentication, you can configure this in the VMware Workspace ONE Access portal.

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.

The screenshot shows the IGEL OS 12 Settings interface. The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), and System. A search bar and a notification icon (1) are also present. The main content area is titled "Device Encryption" and contains sections for Password, Logon, Taskbar, Active Directory/Kerberos, and Single Sign-On. Under Single Sign-On, the "Local User" option is selected. A red box highlights the "Login with local user password" checkbox, which is checked, and a password field containing "*****". A "Change password" button is located below the password field.