IGEL OS(RPI4)

IGEL OS(RPI4) Articles

Devices

How to Configure USB Access Control

You can allow and prohibit the use of USB devices on your device. Specific rules for individual devices or device classes are possible.

Enable USB Access Control

1. Open the Setup and go to **Devices > USB Access Control**.
2. Enable the option **Enable**.
3. Select the **Default Rule**. The default rule specifies whether the use of USB devices is generally allowed or prohibited.

   > ✓ **Tip**
   >
   > It is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.

4. Create one or more rules for classes of devices or individual devices.

Create a Class Rule

1. To create a new rule, click ⊞ in the **Class Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device class defined here is allowed or prohibited.
3. Under **Class ID**, select the class of device for which the rule should apply. Examples: **Audio**, **Printer**, **Mass Storage**.
4. Under **Name**, give a name for the rule.
5. Click **OK**.
6. Save the changes.
   The rule is active.

Create a Device Rule

> ⓘ When a rule is defined, at least one of the properties **Vendor ID** or **Product ID** or **UUID** must be given.

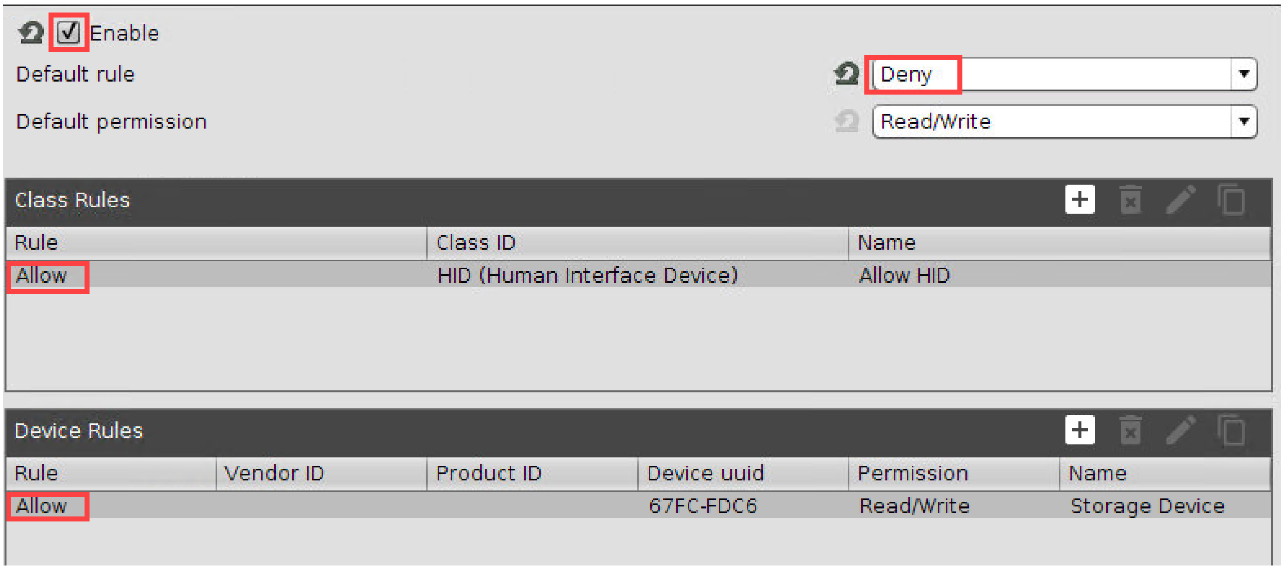
1. To create a new rule, click ⊞ in the **Device Rules** area.
2. Choose a **rule**. The rule specifies whether use of the device defined here is allowed or prohibited.
3. Give the **Vendor ID** of the device as a hexadecimal value.
4. Give the **Product ID** of the device as a hexadecimal value.
   ⊞
5. Give the **Device UUID** (Universal Unique Identifier) of the device.
6. Specify **Permissions** for the device.
   Possible values:
   - Global setting: The default setting for hotplug storage devices is used; see **Default permission** parameter under **Devices > Storage Devices > Storage Hotplug**.

- Read only
- Read/Write

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

Example

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



☑ Enable

Default rule: Deny

Default permission: Read/Write

Class Rules

Rule	Class ID	Name
Allow	HID (Human Interface Device)	Allow HID

Device Rules

Rule	Vendor ID	Product ID	Device uuid	Permission	Name
Allow			67FC-FDC6	Read/Write	Storage Device

Audio

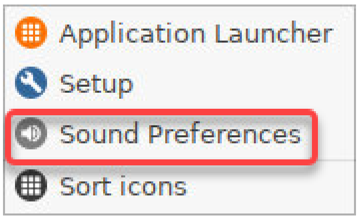
Configuring Audio on the NComputing RX420/440(IGEL)

Overview

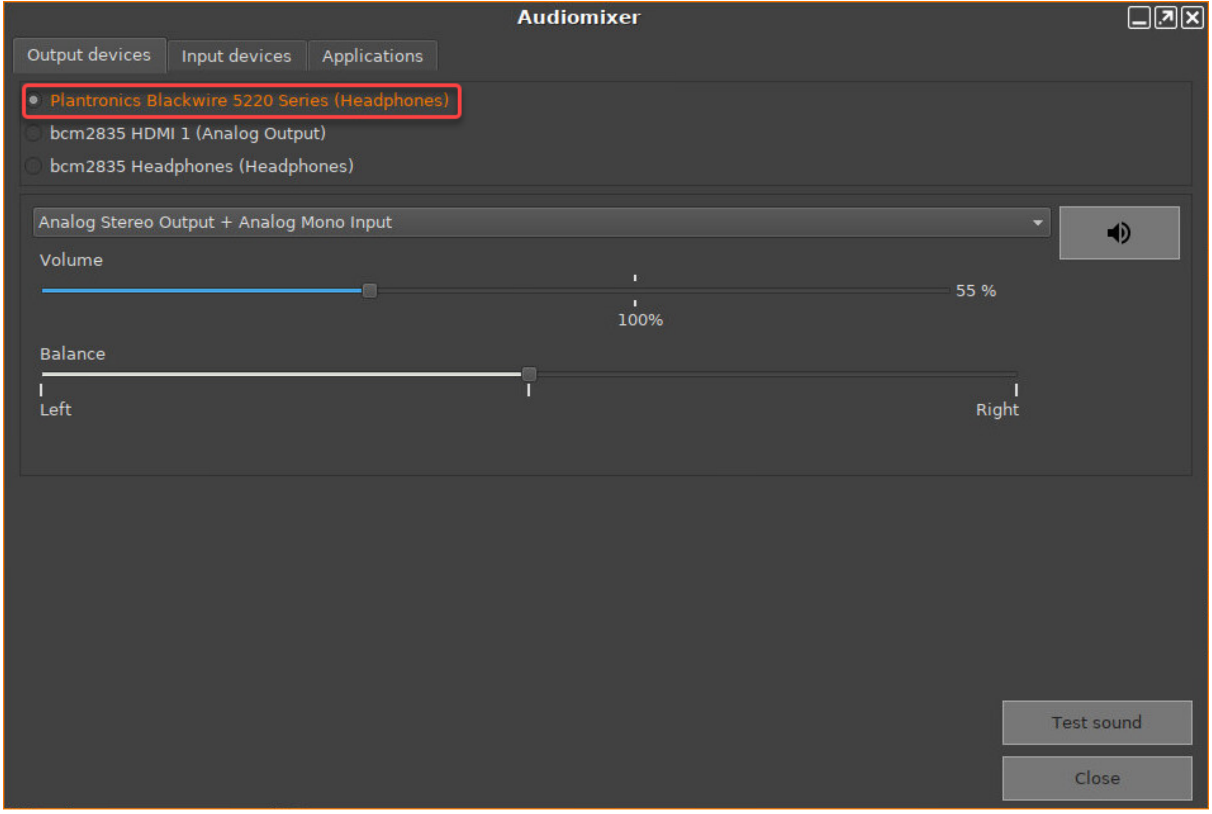
The NComputing RX420(IGEL) supports digital audio via USB and HDMI and analog audio via a 3.5mm jack. The user can select a device using the audiomixer.

Selecting a USB Headset on the Endpoint

1. Open the audiomixer, e.g. by right-clicking on the desktop and selecting **Sound Preferences** from the context menu. For further starting methods, see Sound Preferences(see page 8).



2. In the **Audiomixer** dialog, select the desired device. If in doubt about the device naming, see How Do My Audio Devices Appear in the Audiomixer?(see page 11).

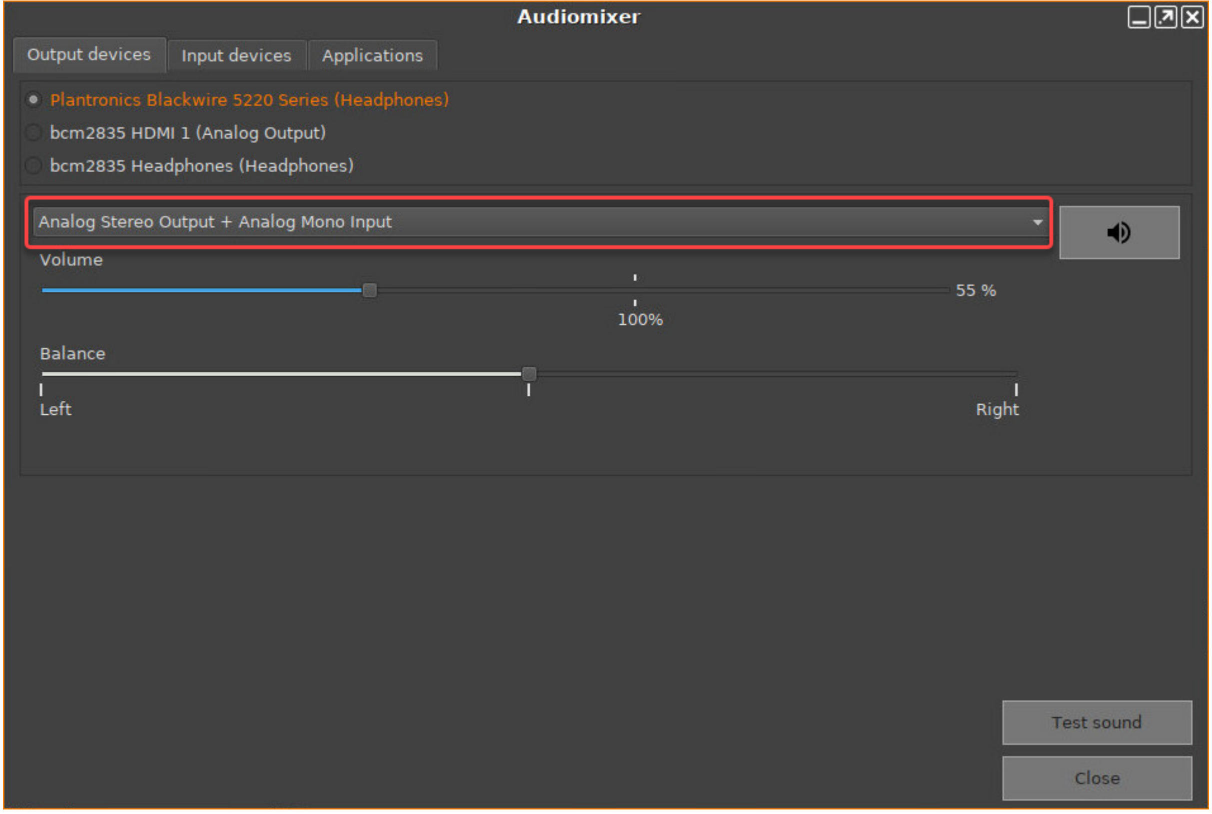


● Plantronics Blackwire 5220 Series (Headphones)
○ bcm2835 HDMI 1 (Analog Output)
○ bcm2835 Headphones (Headphones)

Analog Stereo Output + Analog Mono Input

Volume 55 %

3. Check if the appropriate profile is selected. For a headset, this should be **Analog Stereo Output + Analog Mono Input**.



Audiomixer

● Plantronics Blackwire 5220 Series (Headphones)

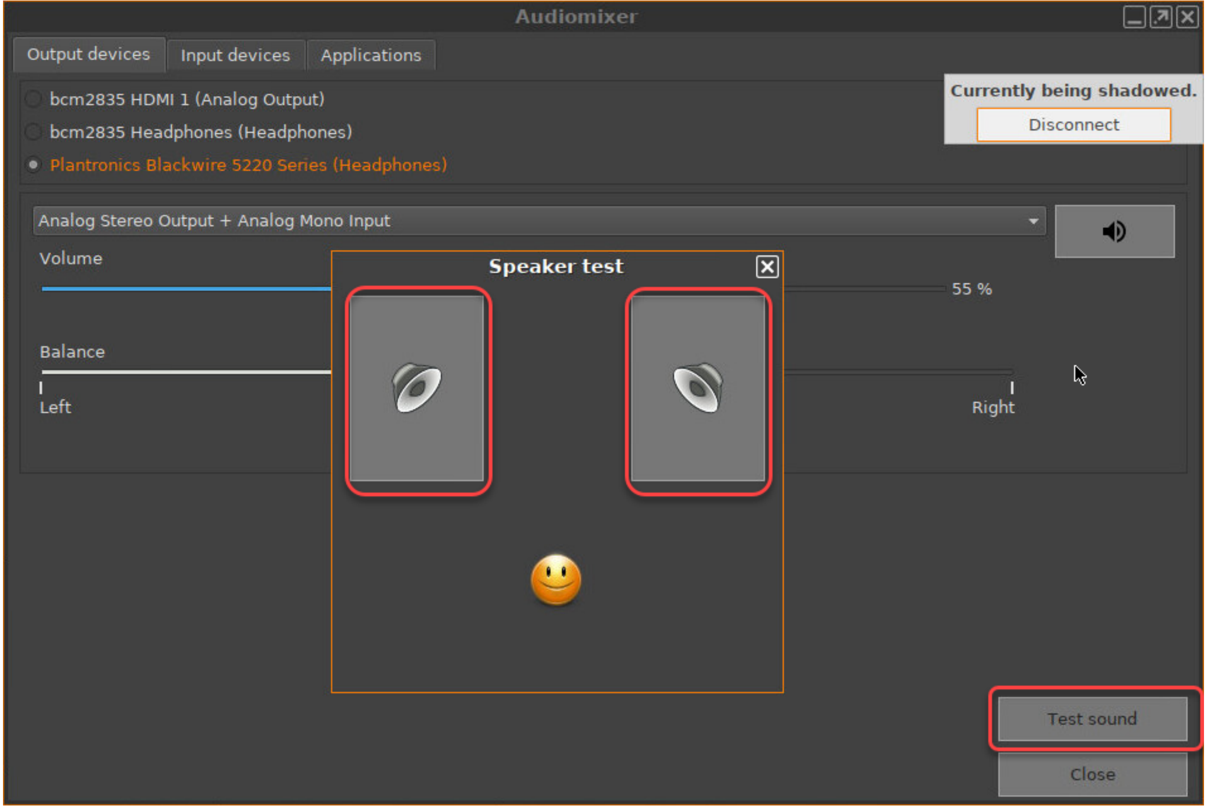
○ bcm2835 HDMI 1 (Analog Output)

○ bcm2835 Headphones (Headphones)

Analog Stereo Output + Analog Mono Input

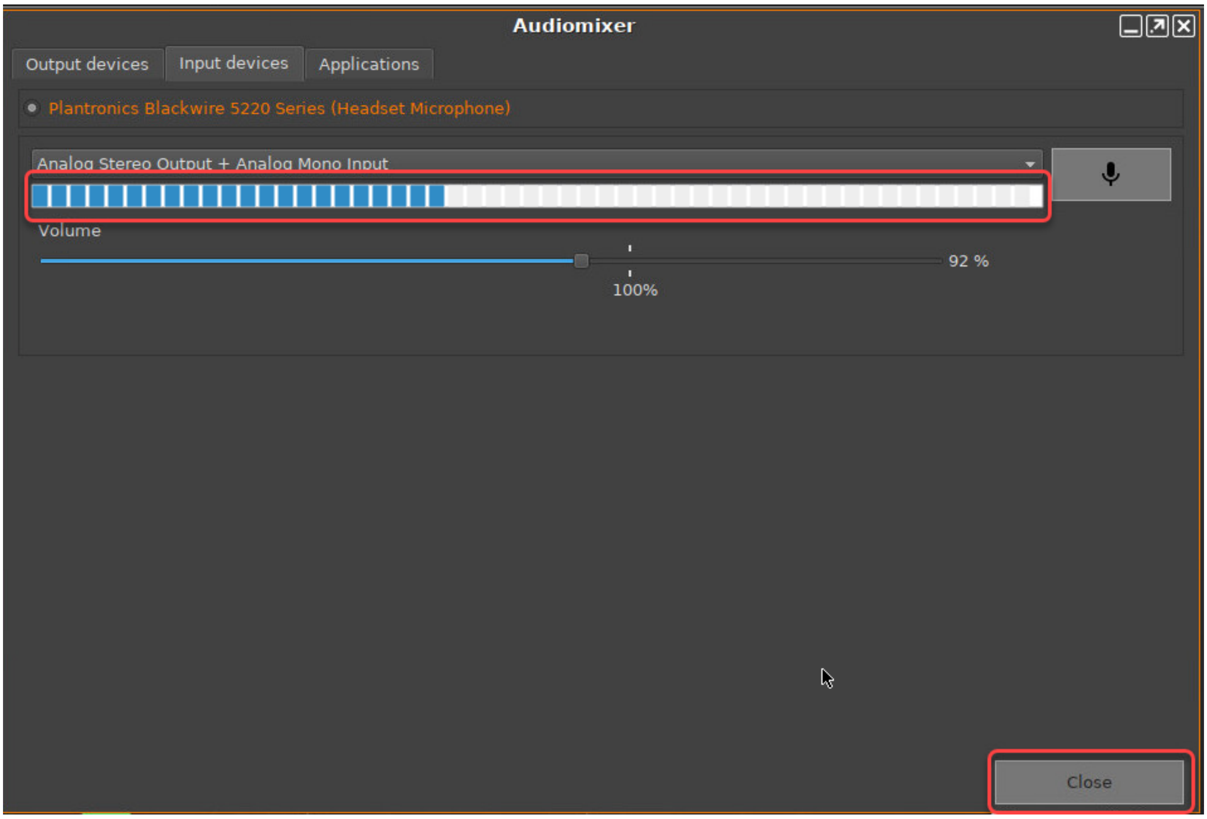
Volume: 55 %

4. To make sure that the audio output is working, click **Test sound** and then click the speaker symbols. You should hear a test sound on your headset.


Audiomixer
Output devices
Input devices
Applications
Currently being shadowed.
Disconnect
○ bcm2835 HDMI 1 (Analog Output)
○ bcm2835 Headphones (Headphones)
● Plantronics Blackwire 5220 Series (Headphones)
Analog Stereo Output + Analog Mono Input
Volume
55 %
Balance
Left
Right
Speaker test
Test sound
Close

5. To make sure that the audio input is working, click the **Input devices** tab and speak into your headset's microphone. If the VU meter is reacting, the sound input is working correctly, and you

can click **Close**.



Audiomixer
Output devices
Input devices
Applications
Plantronics Blackwire 5220 Series (Headset Microphone)
Analog Stereo Output + Analog Mono Input
Volume
92 %
100%
Close

How Do My Audio Devices Appear in the Audiomixer?

Output Devices

Name in Audiomixer	Physical Audio Output
[Device name] (Headphones) Example: **Plantronics Blackwire 5220 Series (Headphones)**	USB
bcm2835 HDMI 1 (Analog Output)	HDMI
bcm2835 Headphones	3.5mm audio jack

Input Devices

Name in Audiomixer	Physical Audio Input
[Device name] (Headset Microphone) Example: **Plantronics Blackwire 5220 Series (Headset Microphone)**	USB

Desktop and Display

Showing and Hiding the On-Screen Software Keyboard Automatically

You can configure the on-screen software keyboard to appear or disappear automatically when an input box is selected or deselected (e. g. Firefox or screenlock).

Showing Automatically

With the following setting, a software keyboard will be shown automatically when an input box is focused.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autoshow** (parameter: `userinterface.softkeyboard.autoshow`).
2. Enable **Automatically show on-screen keyboard when text field is selected**.

Hiding Automatically

With the following setting, the software keyboard will be hidden automatically when an input box is not focused anymore.

1. In the Setup, go to **Registry > userinterface > softkeyboard > autohide** (parameter: `userinterface.softkeyboard.autohide`)
2. Enable **Automatically hide on-screen keyboard when text field is deselected**.

If there are any problems, e. g. the keyboard does not hide automatically, you have to disable **Automatically hide on-screen keyboard when text field is deselected** and make sure that the following Setup parameters have been enabled:

- **Accessories > On-Screen Keyboard > Autostart**
- **Accessories > On-Screen Keyboard > Restart**

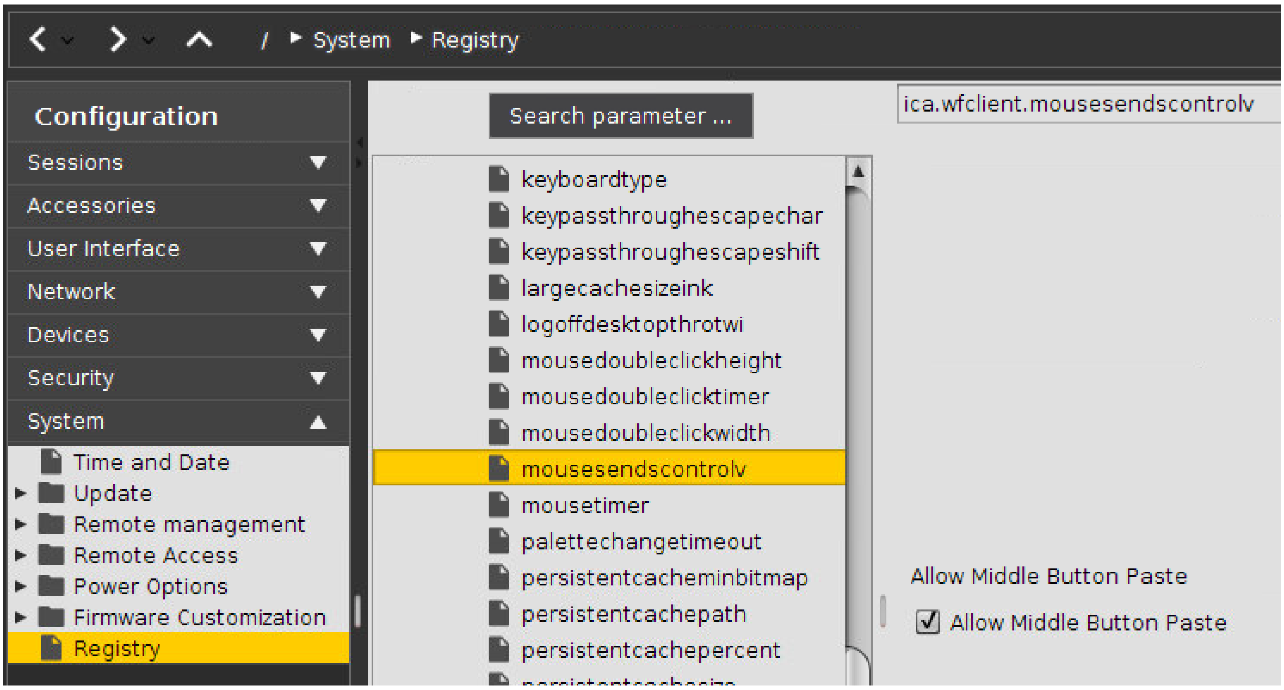
Citrix

Changing Middle Mouse Button Function for Citrix Session and Local Firefox Browser

Middle mouse button cannot be used for smooth scrolling within applications like *Excel* or *Internet Explorer* within a Citrix session or with the local *Firefox* browser.

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

▶ Open IGEL registry in local client setup or UMS.



ica.wfclient.mousesendscontrolv

Allow Middle Button Paste

☑ Allow Middle Button Paste

▶ For Citrix sessions change:

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

▶ For local Firefox browser change:

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

More information on the Firefox parameters can be found at

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

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

The changes will take effect after rebooting the thin client.

Configuring Citrix Workspace Hub

Overview

Feature in Beta Status (Experimental)

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

With Citrix Workspace Hub, you can log in to a Citrix session via a mobile device app and then run this session on any endpoint device that provides Citrix Workspace Hub (hot-desking).

Initially, the Citrix Workspace Hub application must be started on the endpoint device. The Citrix Workspace Hub application displays a launcher screen with a QR code that identifies the endpoint device and signals that the endpoint device is available. On the mobile device app, the user authenticates himself for a Citrix session (session roaming) or has a Citrix session that is already running (session casting). To connect with the endpoint device of choice, the user takes a photo of the QR code. When the mobile device app has recognized the QR code, it connects to the relevant endpoint device via Wi-Fi, and the Citrix session is started on the endpoint device (session roaming) or handed over to the endpoint device (session casting).

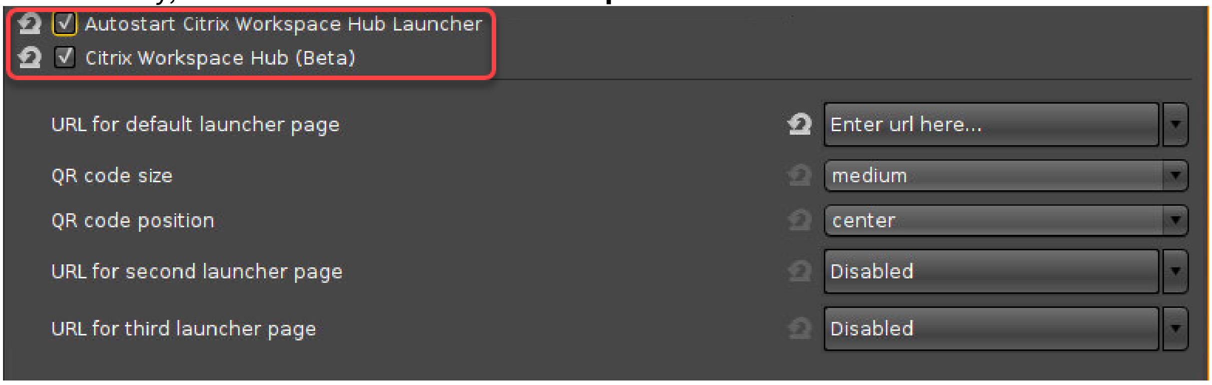
Environment

For a detailed list of prerequisites, see https://docs.citrix.com/en-us/citrix-ready-workspace-hub/system-requirements.html

- Endpoint device with IGEL OS(RPI4)
- Mobile device with Citrix Workspace
- Mobile device and endpoint device are on the same Wi-Fi network
- Wi-Fi network is an open IPv4 network (no ports blocked)
- If the launcher page is a page on the Internet, the endpoint device must have Internet access.

Instructions

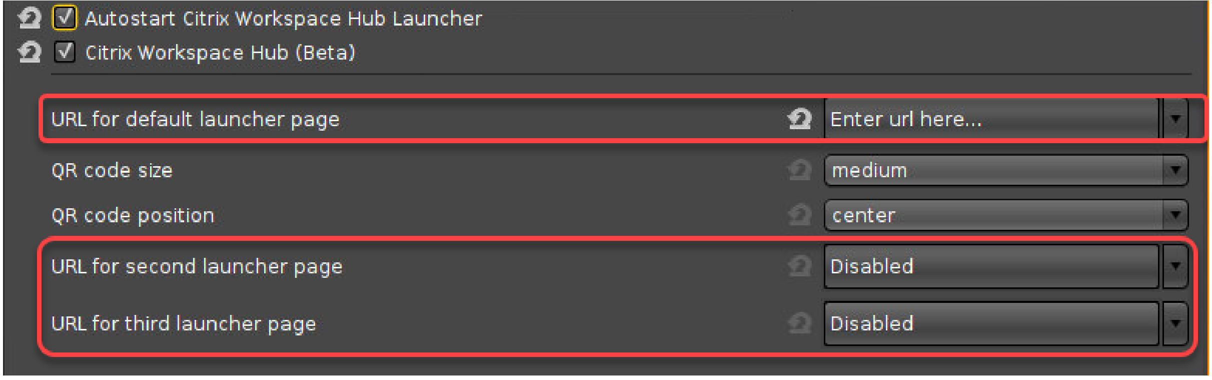
1. Open the Setup and go to **Sessions > Citrix > Citrix Workspace Hub > Options**.
2. Activate **Citrix Workspace Hub (Beta)**. If you do not want Citrix Workspace Hub to start automatically, deactivate **Autostart Citrix Workspace Hub Launcher**.



☑ Autostart Citrix Workspace Hub Launcher
☑ Citrix Workspace Hub (Beta)

URL for default launcher page: Enter url here...
QR code size: medium
QR code position: center
URL for second launcher page: Disabled
URL for third launcher page: Disabled

3. To configure the background of the launcher screen that contains the QR code, define one or more launcher pages. For details, see Options(see page 121), **URL for default launcher page**, **URL for second launcher page**, and **URL for third launcher page**.



☑ Autostart Citrix Workspace Hub Launcher

☑ Citrix Workspace Hub (Beta)

URL for default launcher page: Enter url here...

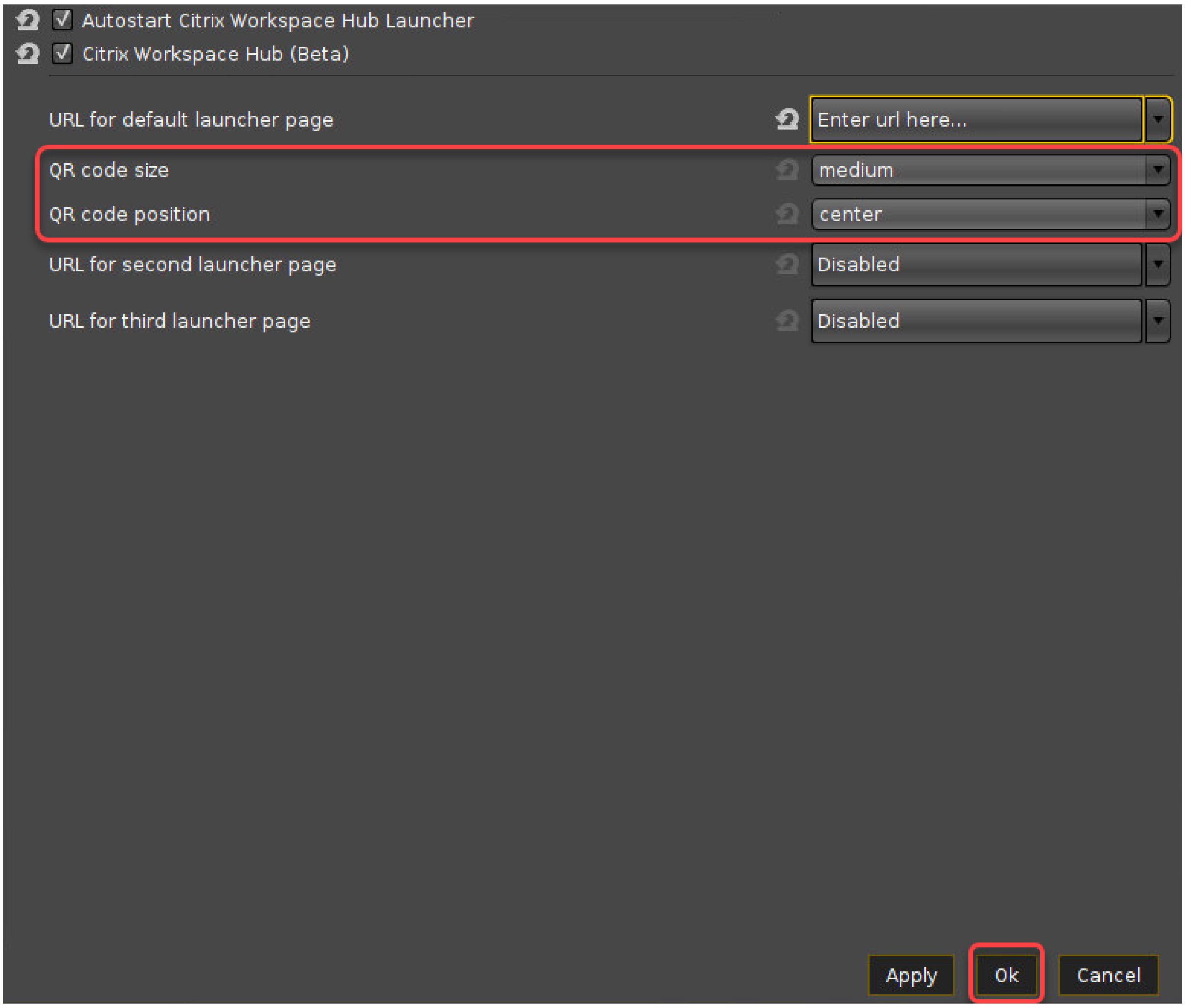
QR code size: medium

QR code position: center

URL for second launcher page: Disabled

URL for third launcher page: Disabled

4. To configure the display of the QR code, set **QR code size** and **QR code position** accordingly, and confirm with **Ok**.



☑ Autostart Citrix Workspace Hub Launcher

☑ Citrix Workspace Hub (Beta)

URL for default launcher page: Enter url here...

QR code size: medium

QR code position: center

URL for second launcher page: Disabled

URL for third launcher page: Disabled

How to Connect a SpaceMouse with a Citrix Session

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

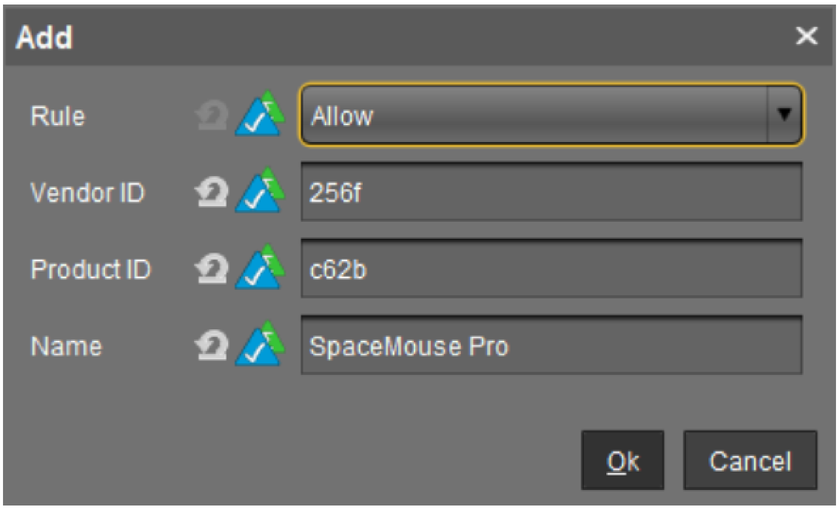
> Always use a SpaceMouse only as an additional, i.e. second, mouse.

> To prevent the SpaceMouse from interfering with the IGEL graphical user interface, use the following registry parameter:

IGEL Setup	**System > Registry**
Parameter	Deactivates 3Dconnexion/Logitech SpaceMouse products as a standard mouse
Registry Key	`userinterface.mouse.spacemouse.x11_ignore`
Value	enabled/disabled
Info	"enabled" means that the SpaceMouse is passed through to the session and ignored by the local GUI. "disabled" means that the SpaceMouse is also used for the local GUI.

To configure the SpaceMouse for Citrix sessions:

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Activate the checkbox **Native USB Redirection**.
3. Set the **Default rule** to **Deny**.
4. Add a device exception rule as in the following screenshot with the **Vendor ID** and **Product ID** of your specific SpaceMouse:
   SpaceMouse products included (VID, PID, Vendor, Product)
   - 0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT
   - 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman
   - 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic
   - 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000
   - 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse
   - 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse
   - 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse
   - 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse
   - 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks
   - 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse
   - 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro
   - 0x256F; *; 3Dconnexion; SpaceMouse



Add

Rule: Allow

Vendor ID: 256f

Product ID: c62b

Name: SpaceMouse Pro

5. Save the settings.

Now, the SpaceMouse is ready for use.

To achieve that the mouse behaves as usual in CAD programs, change the configuration as follows:

1. Go to **IGEL Setup > System > Registry > ica.wfclient.mousesendscontrolv**.
2. Set the parameter to **disable**.

Wireless Mouse Keyboard Set Logitech k520 Freezes in Citrix Session

⚠ **Solution Based on Experience from the Field**

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

Issue

Wireless Mouse Keyboard Set Logitech k520 freezes in Citrix XenDesktop session.

Environment

- IGEL OS 11
- UMS 6.01 and higher

Description

If the Wireless Mouse Keyboard's infrared signal is disturbed, it freezes.

Solution

This particular device uses infrared dongle. BT devices should work fine as a workaround and we suggest using those. Citrix discourages the use of the IR dongles.

How to Configure Citrix Native USB Redirection

Native USB Redirection redirects most popular USB devices to the Citrix session. To use this feature, you must have at least **XenDesktop 7.6** installed. In addition, the guidelines for USB redirection must be defined. More information can be found on the following pages

- Citrix Generic USB Redirection Configuration Guide[1]
- Generic USB redirection and client drive considerations[2]

The following types of USB device are **not** supported by default for use in a **Citrix Virtual Apps** and **Desktops** session:

- Bluetooth dongles
- Integrated NICs
- USB hubs

The following types of device are supported directly in a **Citrix Virtual Apps** and **Desktops** session, and so do not use USB support:

- Keyboards
- Mice
- Smart cards
- Headsets
- Webcams

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

1. In Setup, go to **Sessions > Citrix > Citrix Global > Native USB Redirection**.
2. Enable **Native USB Redirection**.
3. Set the **Default rule** to **Deny** or **Allow**:
   - **Allow**: All devices that are allowed by default are redirected.
   - **Deny**: No device is redirected.

   > **Tip**
   >
   > To secure your endpoint, it is generally recommended to set **Default rule** to **Deny** and to configure **Allow** rules only for the required USB devices and USB device classes.
4. To customize the USB redirection, you can create classes or device rules to redirect e.g. Bloomberg keyboards or 3D Spacemouse.

> To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool (**Accessories > System Information**).

> For a device exception rule, use the SpaceMouse Guide.
> For more information about USB redirection rules at the client, see the documentation of the respective receiver.

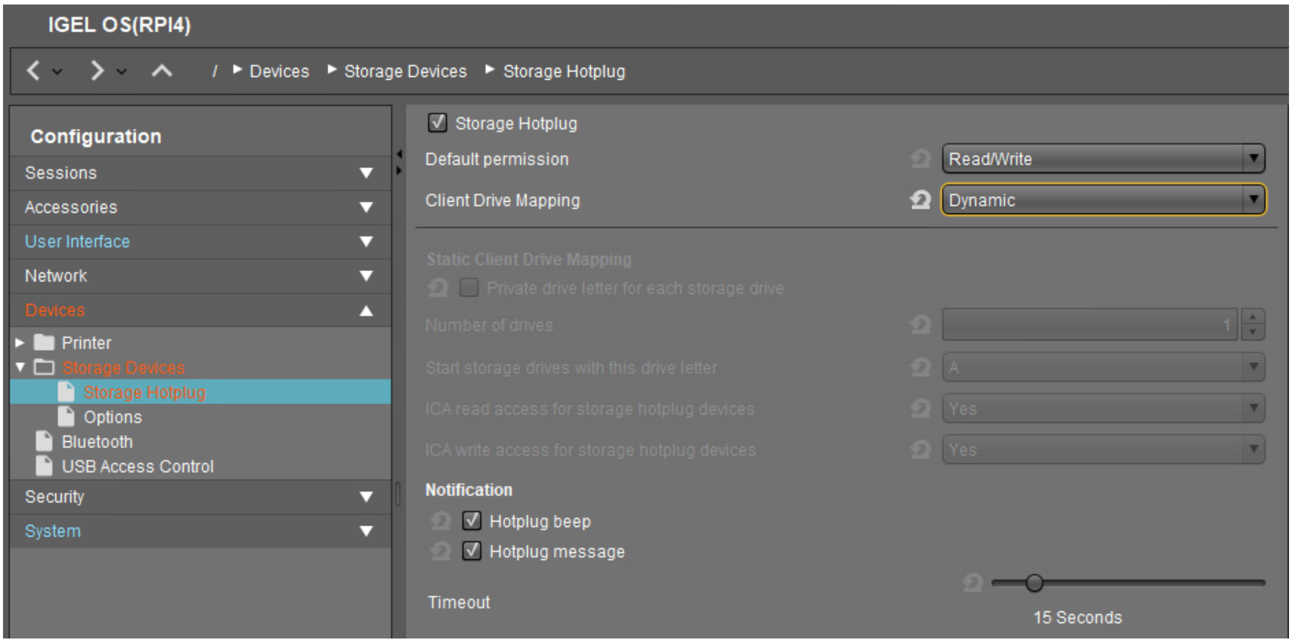
[1] https://support.citrix.com/article/CTX137939
[2] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/general-content-redirection/usb.html

Mapping USB Storage Media into Citrix Sessions

How to configure USB storage mapping so that users can access USB storage media within Citrix sessions?

The mapping of USB storage devices is possible for "USB mass storage class" devices.

Basic Configuration of the Client



☑ Storage Hotplug

Default permission: Read/Write

Client Drive Mapping: Dynamic

Static Client Drive Mapping

□ Private drive letter for each storage drive

Number of drives: 1

Start storage drives with this drive letter: A

ICA read access for storage hotplug devices: Yes

ICA write access for storage hotplug devices: Yes

Notification

☑ Hotplug beep

☑ Hotplug message

Timeout: 15 Seconds

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

▶ Activate **Devices > Storage Devices > Storage Hotplug > Client drive mapping > Dynamic**. This option activates dynamic client drive mapping. It automatically recognizes new storage media as they are connected to the endpoint device. The endpoint device beeps and shows a notification while it mounts the new device. The storage devices automatically become usable on the endpoint device and in Citrix ICA Sessions.

Mounted devices need to be unmounted before they are removed to ensure data integrity. This can be done via the **Disk Utility / Disk Removal** tool (for activation, see **Accessorries**) or a tray icon.

Additional Parameters to Check

▶ The following parameters are set by default, thus storage mapping will work, but maybe for some reason you have changed these and need to adjust them to allow the storage mapping:

Sessions > Citrix > Citrix Global > Mapping > Drive Mapping > Drive mapping (set checkmark)

Sessions > Citrix > Citrix Global > Native USB Redirection > Native USB redirection (remove checkmark)

Devices > USB access control > Enable (remove checkmark)

Assigning a Drive Letter within the Session (Optional)

▶ In case you not only want to see the drive in the session as e.g. "A on IGEL-123456789", but want to address the drive with a real drive letter within the session, you may run one of these commands:

```
subst T: \\tsclient\t
```

or

```
net use T: \\tsclient\t
```

In this example, "T on IGEL-123456789" is assigned to drive letter T: within the session. You may also assign the mapped drive to another drive letter than is used in its name.

Configuration on the Server Side

On the server side, e.g. with Windows Server 2008R2, a user in the group "Users" with access to the terminal server will have the mapping default. This is true for a newly installed server. But the mapping can be prevented by changing the policies:

ⓘ **Do not allow drive redirection** specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format [driveletter] on [computername]. You can use this setting to override this behavior." Source: https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx

Citrix StoreFront

Prerequisites:

- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates in IGEL OS)

Connecting via **StoreFront**:

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

Citrix Self-Service

Prerequisites:

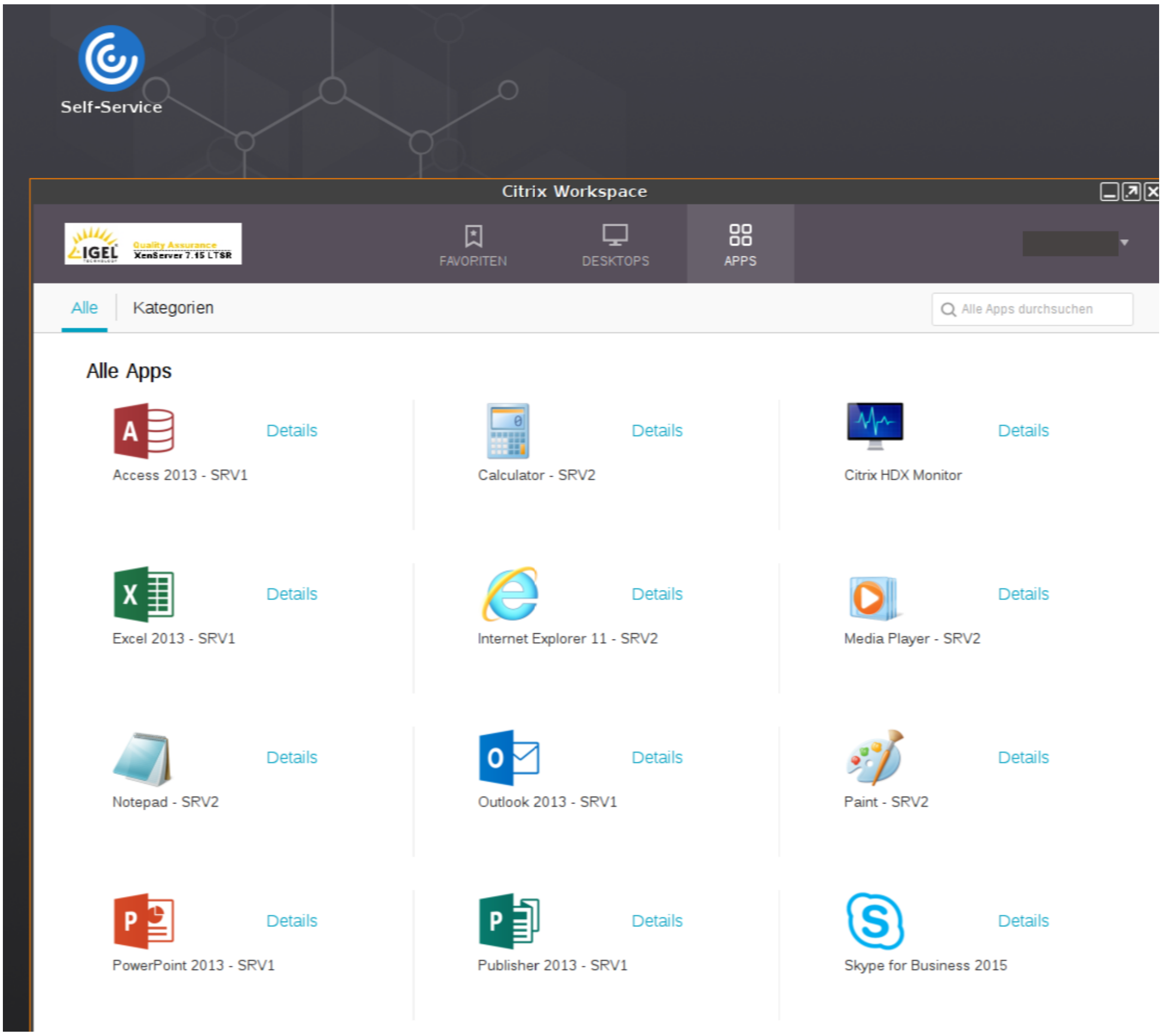
- Trust root certificate in directory /wfs/ca-certs (see Deploying Trusted Root Certificates in IGEL OS)

Connecting via **StoreFront**:

1. Click **Sessions** in the configuration tree of the IGEL setup.
2. Click **Citrix > Citrix Self-Service > Server**.
3. Enter the **Server**, the **Path to Store** and the **Store name** of the services sites.
4. Confirm with **OK**.
5. Click **Citrix Self-Service > Desktop Integration**.
6. Enter "Citrix Self-Service" under **Login Session Name**.
7. Choose **Desktop** as the starting method.
8. Click **OK** to save the changes.
   Setup closes.
9. Doubleclick the Citrix icon on the desktop.
   The login window opens.
10. Enter the credentials of a user in the login window.
    The published application icons of the Citrix farm will appear in the Self-Service UI.
11. Doubleclick an application icon to start the program.

Using Citrix Self-Service

1. Start **Citrix Self-Service** e.g. with desktop icon.
2. Log on to the server.
3. Add published applications to the list (**+**-button on the left).
4. Click a published application to start.
5. Use the search bar to find a published application.
6. Use the user's menu to change preferences, server etc.



- Configure Full-Screen Mode(see page 27)

Configure Full-Screen Mode

Use following parameter in your Custom Command script to activate the full-screen mode for *Citrix Self-Service*:

▶
```
$ICADIR/storebrowse -c FullscreenMode=[0/1/2]
```

With following options:

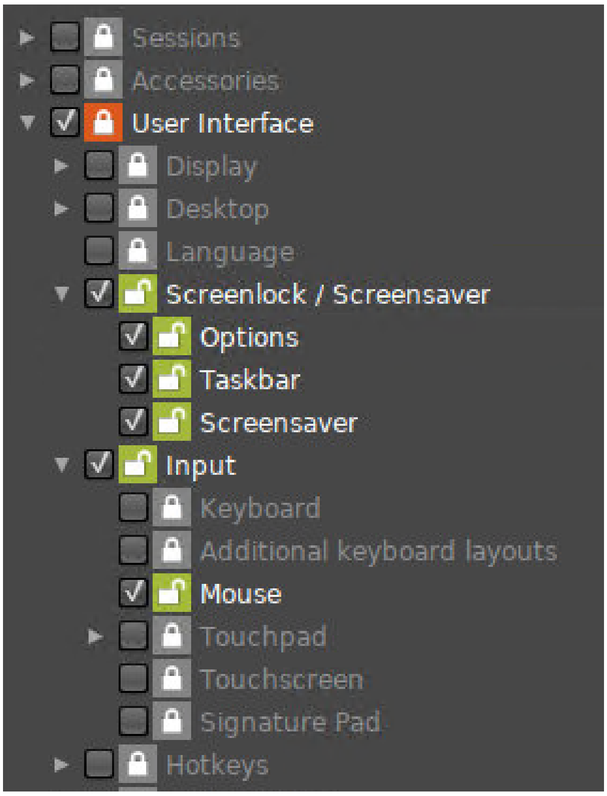
- `0` = The window is not displayed full-screen
- `1` = The window is displayed full-screen
- `2` = The window is displayed maximized and undecorated, which does not mask the desktop environment's taskbar

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

Usually, the user should not have full access to the thin client's setup. However, it may prove useful to enable users to quickly change certain settings by themselves, without even needing a password. Typical examples are settings for keyboard, mouse, or screen. This can be done using the **Quick Settings**.

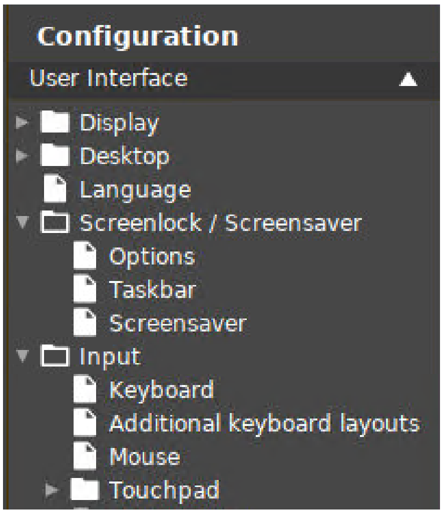
Here is how to select setup pages for quick setup:

1. Open the setup and go to **Accessories** > **Quick Settings** > **Setup User Permissions**.
2. Select the setup pages to which the user should have access, e. g. **User Interface > Input > Mouse**, or **Screenlock / Screensaver**.



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

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



Quick settings set permissions for setup screens. If you want to set permissions for individual parameters, you can use UMS profiles. For more information, see Profiles.

Login Failed because of the Expired AD Password

Problem

When you try to log in to a native **Citrix Storefront** session, you get the error message "Login Failed!" because your Active Directory password expired.
You are unable to change your password, because the local login does not provide an option for that.

> ⓘ Before you follow these instructions, check that the ports are open, maybe you can fix the problem by that:
>
> - Login to Client -> Port: 88
> - Change password -> Port: 464
>
> Here you find an overview of ports of the domain controller: Required Ports to Communicate with Domain Controller[3]

Solution

Enable **Active Directory/Kerberos** authentication for the **Storefront** session. The next time you try to log in to IGEL OS, you will be prompted to change your expired password.

Changing an Expired Active Directory Password

> When using sessions with passthrough authentication, it is essential that you lock your device's screen when leaving it unattended.

Enabling Active Directory/Kerberos Authentication for Storefront Sessions

1. In IGEL setup, go to **Security > Login > Active Directory/Kerberos**.
2. Enable **Login to Active Directory domain**.
3. Go to **Security > Active Directory/Kerberos**.
4. Activate **Enable**.
5. Fill in the **Default domain (fully qualified domain name)**.
6. Go to **Sessions > Citrix > Citrix Storefront > Login**.
7. Enable **Use passthrough authentication**.
8. Click **Apply** or **Ok**.

> ⓘ Please note that the client must now be locked locally and no longer in the session to prevent another person from entering the session via the passthrough without specifying the password.

[3] https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS

Enabling Screenlock

1. In the IGEL setup go to **User Interface > Screenlock / Screensaver**.
2. Enable **Use hotkey**.
3. Under **Modifiers** select `Win`.
4. Under **Hotkey** enter "L".
5. Got to **User Interface > Screenlock / Screensaver > Options**.
6. Enable **User password**.

So the "Win + L" hotkey locks the IGEL client instead of the session desktop.

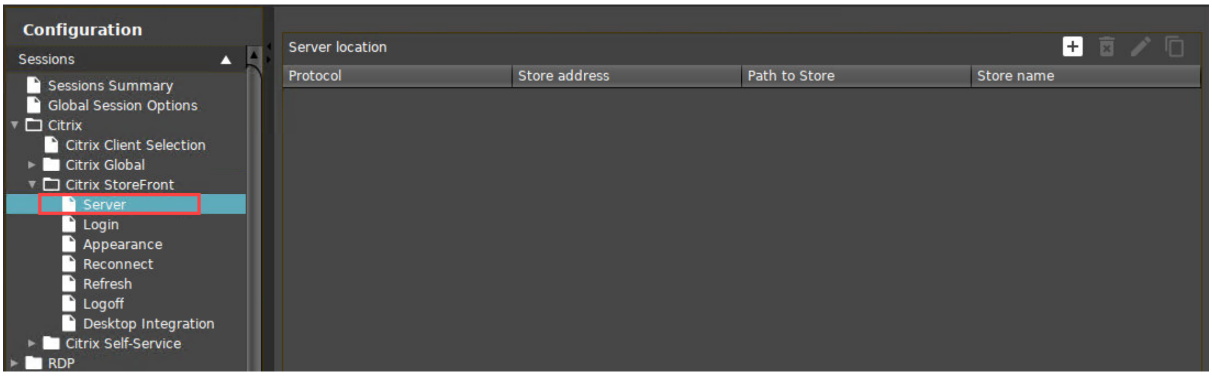
The AD password must be entered to activate the IGEL clients.

Configuring Auto Logon for Citrix Virtual Desktops

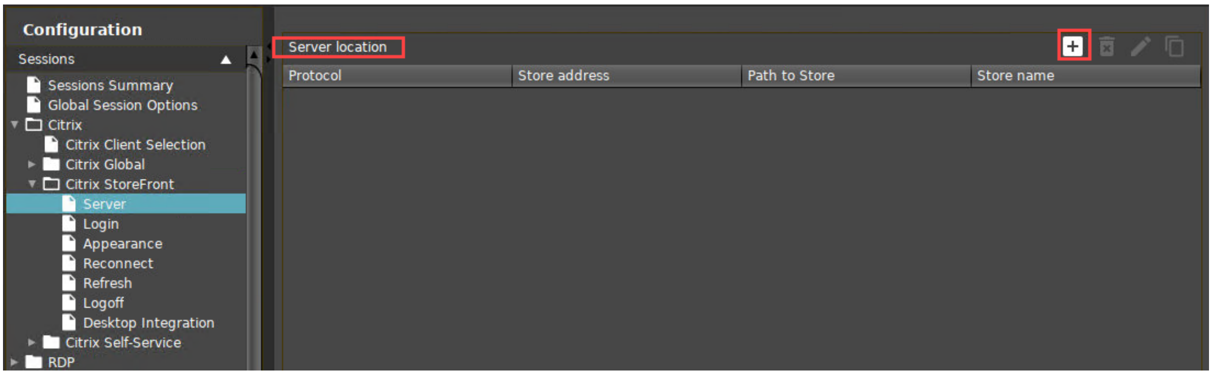
This how-to describes how to configure Auto Logon for Citrix Virtual Desktops.

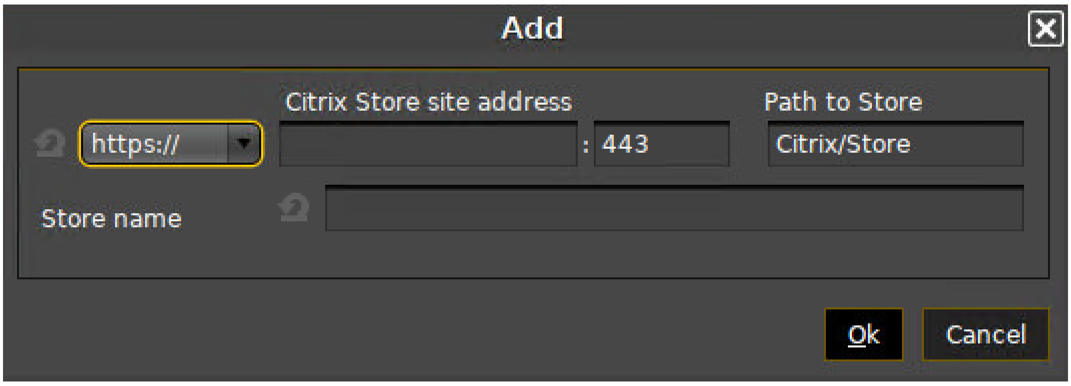
Steps

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



2. Add your **Server Location**.

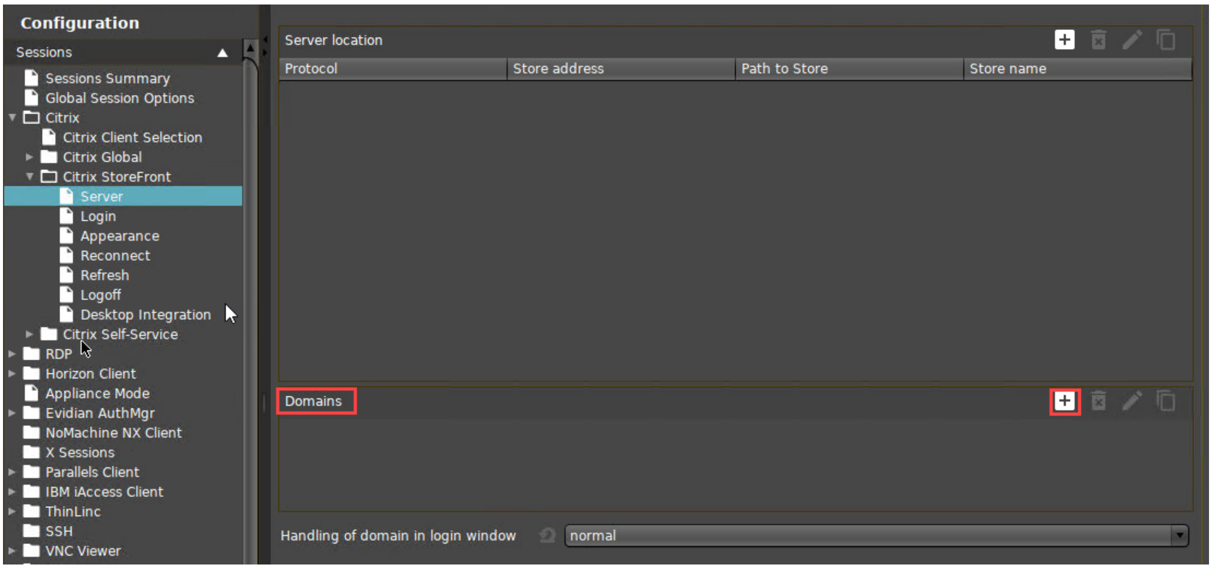




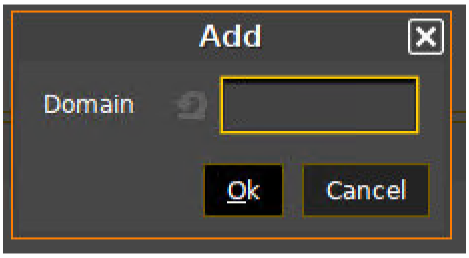
https:// | Citrix Store site address: | : 443 | Path to Store: Citrix/Store

Store name:

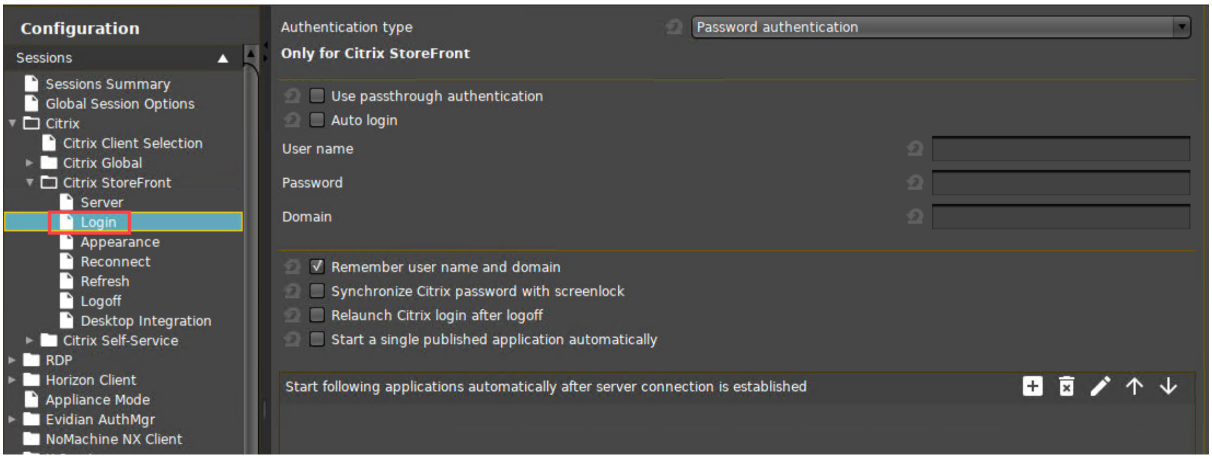
3. Add your Active Directory domain to **Domains**, making sure that you use its Fully Qualified Domain Name (FQDN).



Handling of domain in login window: normal



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



Authentication type: Password authentication

Only for Citrix StoreFront

- □ Use passthrough authentication
- □ Auto login

User name

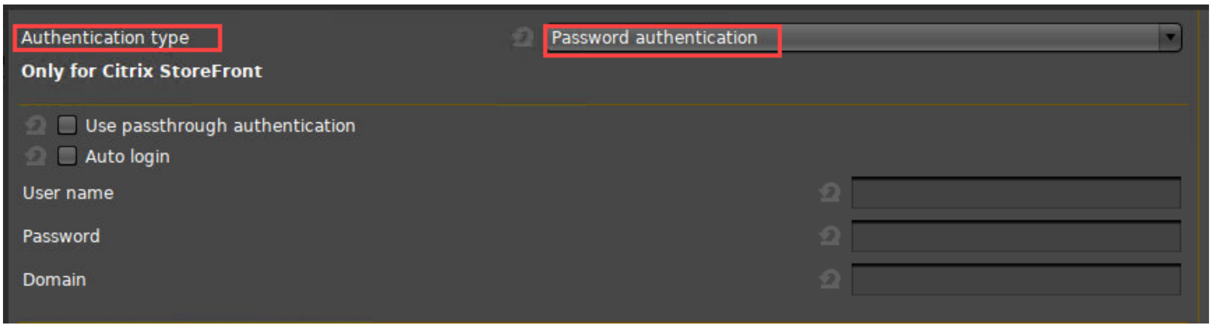
Password

Domain

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

Start following applications automatically after server connection is established

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

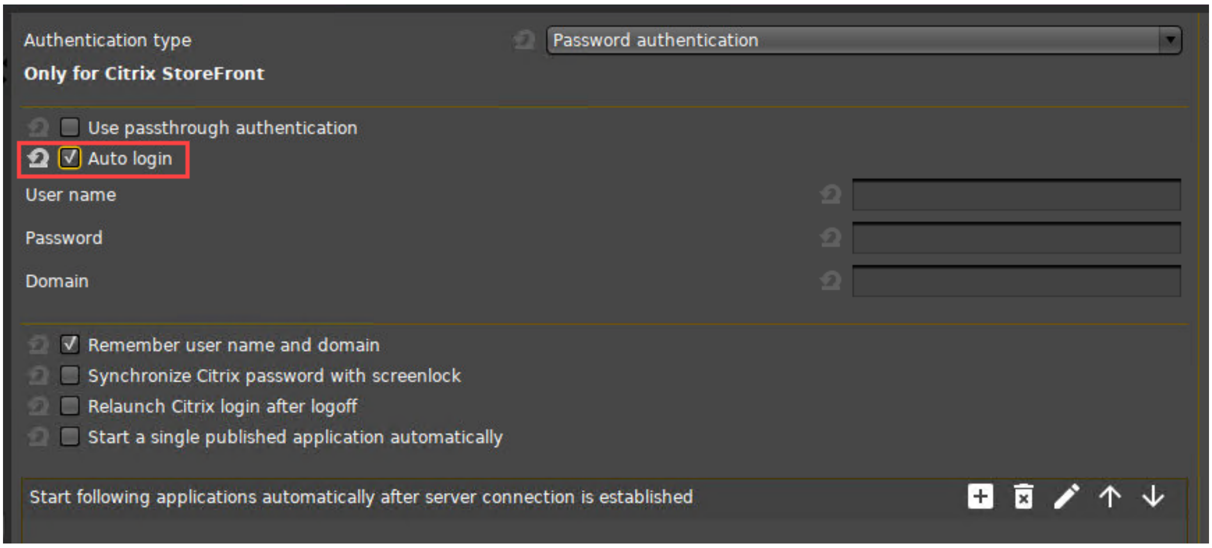


Authentication type: Password authentication

Only for Citrix StoreFront

☐ Use passthrough authentication
☐ Auto login
User name
Password
Domain

6. Activate **Auto Login**.



Authentication type: Password authentication

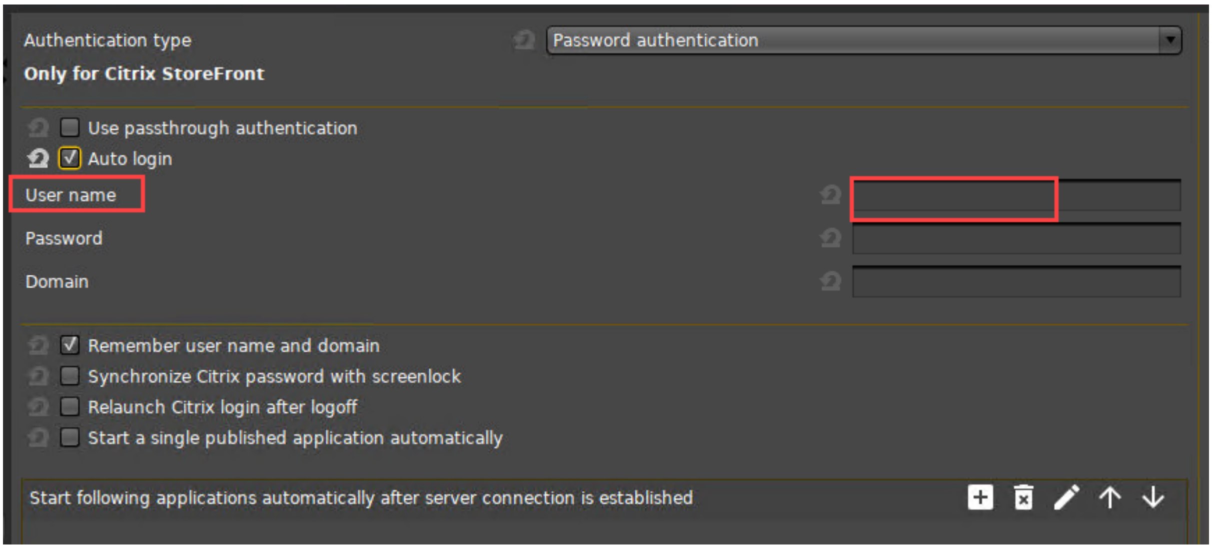
Only for Citrix StoreFront

☐ Use passthrough authentication
☑ Auto login
User name
Password
Domain

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

Start following applications automatically after server connection is established

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



Authentication type: Password authentication

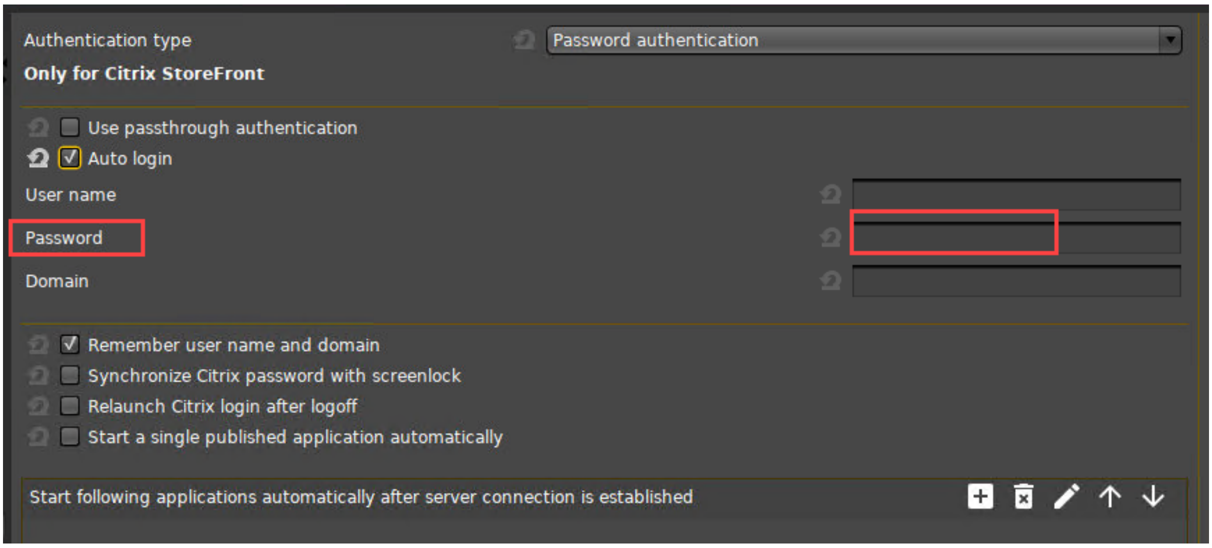
Only for Citrix StoreFront

☐ Use passthrough authentication
☑ Auto login
User name
Password
Domain

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

Start following applications automatically after server connection is established

8. Set the **Password**.



Authentication type: Password authentication

Only for Citrix StoreFront

□ Use passthrough authentication

☑ Auto login

User name

Password

Domain

☑ Remember user name and domain

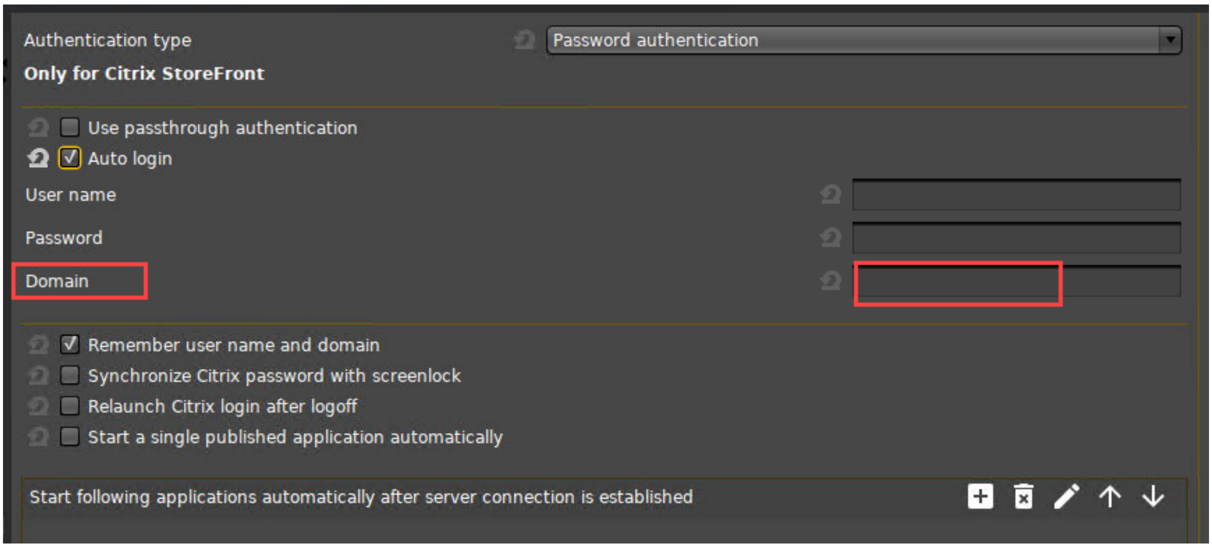
□ Synchronize Citrix password with screenlock

□ Relaunch Citrix login after logoff

□ Start a single published application automatically

Start following applications automatically after server connection is established

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



Authentication type: Password authentication

Only for Citrix StoreFront

□ Use passthrough authentication

☑ Auto login

User name

Password

Domain

☑ Remember user name and domain

□ Synchronize Citrix password with screenlock

□ Relaunch Citrix login after logoff

□ Start a single published application automatically

Start following applications automatically after server connection is established

Citrix: Freeze at Logout

Symptom

A user tries to log out from a Citrix session but the session does not respond.

Example: Once you connect to a Citrix session, everything works. After having reconnected and disconnected several times, you log out. The window freezes while the logout screen is shown.

Solution

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

OR

▶ Try to use another Citrix Receiver version: **Sessions > Citrix > Citrix Client Selection > Citrix client version**.

OR

▶ Troubleshoot the issue with your Citrix infrastructure to discover why the session is not closing when the `wfica` process makes the call for disconnection.

Workaround

As a less recommended alternative, you can configure a hotkey to force a logout in such situations. Note, however, that this workaround can cause issues with hung sessions on the Citrix servers.

To configure a logout hotkey:

1. In IGEL Setup, go to **System > Firmware Customization > Custom Application**.
2. Click ⊞ to create a new **Custom Application** and name it e.g. "Kill Citrix Sessions".
3. Disable all **Starting Methods** for this session.
4. Enable **Hotkey**.
5. Choose e.g. `Ctrl|Alt` as **Modifiers** and define `C` (for "Citrix) as **Key**.
6. Go to **System > Firmware Customization > Custom Application > Kill Citrix Sessions > Settings**.
7. Enter an **Icon name**.
8. Enter `/tmp/kill_citrix` as **Command**.
9. Go to **System > Firmware Customization > Custom Commands > Desktop**.
10. In the field **Desktop initialization** enter following command in one line:
    ```
    echo -e "#! /bin/bash\n\nps -eo comm,pid | grep ^wfica | while read c p tail; do echo \$p; done | xargs -r kill -TERM" >/tmp/kill_citrix; chmod 755 /tmp/kill_citrix
    ```
11. Click **Apply** and reboot the device.

To configure the hotkey for a group of devices, you can alternatively create a profile or use this one: profile_KillCitrixSessionsViaHotkey.xml(see page 36).

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

Workaround for Citrix Receiver X Error

Problem

When starting Citrix XenApp you get the following Citrix Receiver errors on your IGEL OS devices:

```
The X Request 55.0 caused error: "9: BadDrawable (invalid Pixmap or Window parameter)"
```

```
The X Request 60.0 caused error: "13: BadGC (invalid GC parameter)".
```

Environment

- Citrix XenApp 7.15
- Citrix Receiver e.g. 13.2, 13.3, 13.7, 13.8

Solution

Two parameters have to be activated in IGEL Setup:

1. Go to **System > Registry > ica > forceignorexerrors**.
2. Activate **Suppress X error message boxes**.
3. Go to **System > Registry > ica > wfclient > ignorexerrors**.
4. Activate **IgnoreXErrors** and pass the parameters: `55.0/9, 60.0/13`

See also the corresponding entry in the Citrix forum[4].

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

System

Rescue, Reset and Boot Options

Symptom/Problem

Your device does not boot properly, or you need to reset it to factory defaults without using the UMS.

Environment

- NComputing RX420(IGEL) with IGEL OS 11.01.111(RPI4) or higher
- NComputing RX440(IGEL) with IGEL OS 11.01.111(RPI4) or higher

Solution

You can use the following device buttons and key combinations:

Key Combination	**Function**
[Power button] (short press)	Normal boot
[Power button] (long press)	Emergency setup
[Ctrl] + [Space] (press and hold until the system boots)	Reset to factory defaults
[Ctrl] + [V] (press and hold until the system boots)	Verbose boot
[Esc] (press and hold until the system boots)	Go to the boot menu

IGEL OS(RPI4) Automatic Update Service for Device Evaluation

Overview

The automatic update service checks for available firmware updates periodically; if a firmware update is available, the user is prompted to start the update. The firmware is provided by IGEL via a download server that is known by the automatic update service. Alternatively, you can use a download server of your own.

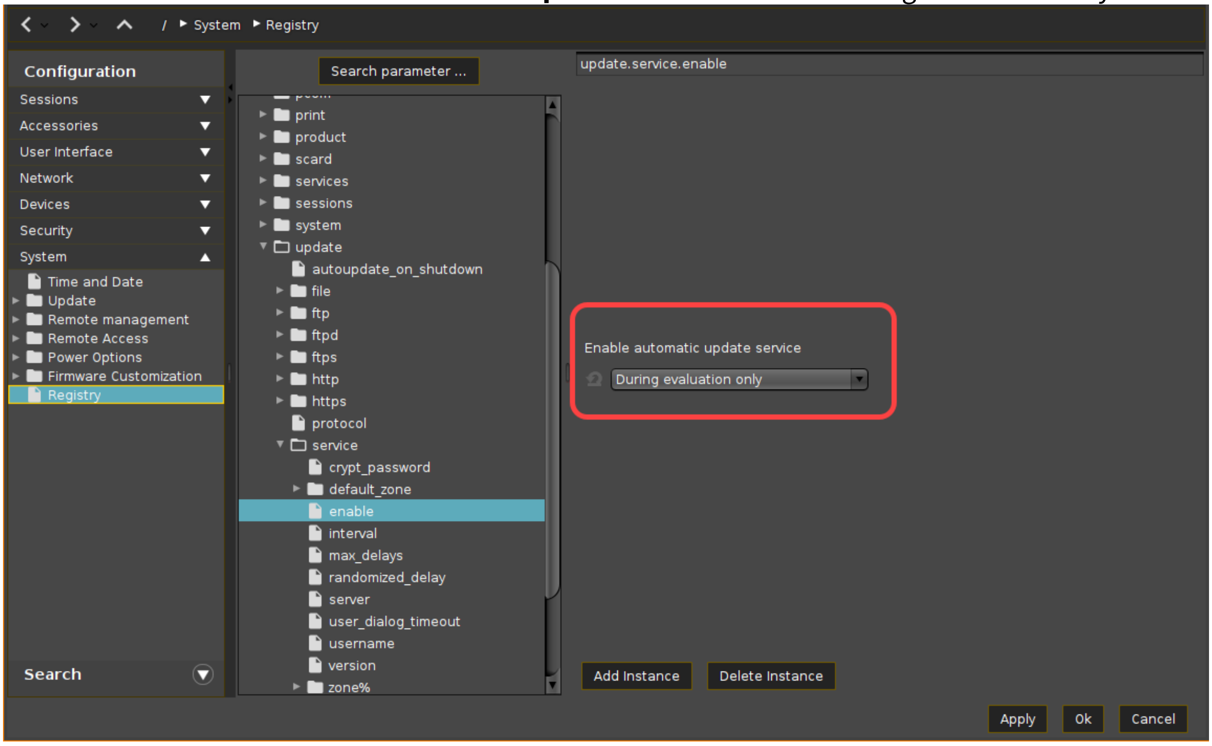
> ⓘ The automatic update service is by default available for devices with an evaluation license; when the device receives a Workspace Edition license, the service is deactivated.

Environment

- IGEL OS(RPI4) 11.02.110 or higher

Configuring the Automatic Update Service

1. In the UMS configuration dialog or the local Setup, go to **System > Registry > update > service > enable** and ensure that **Enable automatic update service** is set to "During evaluation only".



update.service.enable

Enable automatic update service: During evaluation only

2. Set the following parameters according to your requirements:

- **crypt_password**: If you want to use an update server of your own and it requires authentication, enter the password for this server here. If no authentication is required, leave the field empty.
- **default_zone > server**: Do NOT change this field, even if you want to use your own update server.
- **interval**: Time interval in hours in which the device should check for firmware updates during runtime. When the value is 0, the device only checks on boot.
- **max_delays**: Maximal times the user can postpone an update. Example: When this value is set to 9, the user can postpone the update 9 times before the update will be forced. When the value is 0, the update will be forced immediately.
- **randomized_delay**: Delay time in minutes that is added to the interval to avoid an excessive amount of requests to the server at the same time.
- **server**: If you want to use an update server of your own, enter its address here. If the field is empty, the public update server provided by IGEL will be used.
- **user_dialog_timeout**: Timeout in seconds before the user dialog is closed and the update is started. When set to 0, the dialog remains open until the user closes it.
- **username**: If you want to use an update server of your own and it requires authentication, enter the username for this server here. If no authentication is required, leave the field empty.
- **version**: Name of the update server directory with the firmware to which the device should be updated. Example: "latest", "11.02.120", "igelos_rpi_11.02.130". If the field is left empty and IGEL public update server is in use, the latest version will be used.

3. Click **Apply** or **Ok** to confirm your settings.

YouTube Video Not Playing / Issues With Web Content

Symptom

Videos on YouTube won't play, or other web content is not displayed as expected.

Environment

- IGEL OS(RPI4) on devices with no battery-backed real-time clock

Problem

Certificate issues arise because of incorrect time and date settings. Devices without a battery-backed real-time clock lose the current time and date when they are powered off.

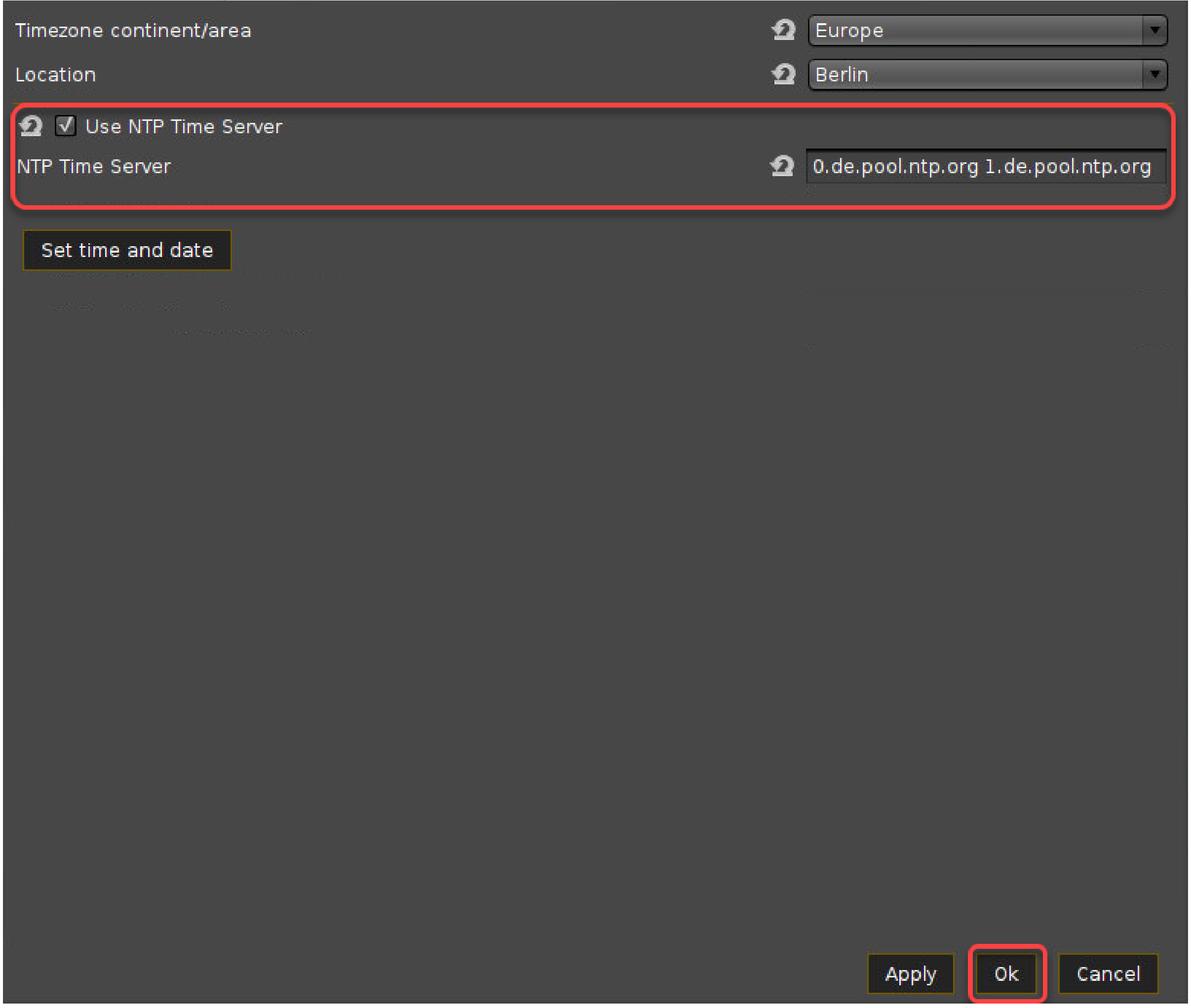
Solution

1. In the Setup or UMS configuration dialog, go to **System > Time and Date**.

   ✓ It is recommended to use a profile. For details, see Profiles.

2. Edit the following settings:
   - **Use NTP time server**: Activate this option.
   - **NTP time server**: Define one or more NTP time servers. To define multiple NTP time servers, separate them by spaces. Example: `0.de.pool.ntp.org 1.de.pool.ntp.org`

3. Confirm the settings with **Ok**.



Timezone continent/area: Europe

Location: Berlin

☑ Use NTP Time Server

NTP Time Server: 0.de.pool.ntp.org 1.de.pool.ntp.org

IGEL OS(RPI4) Reference Manual

For supported devices, see Devices Supported by IGEL OS 11(RPI4).

✓ **Getting Started**

To get started, see IGEL OS(RPI4) for NComputing RX420(IGEL) - STEP-BY-STEP GETTING STARTED GUIDE[5]

[5] http://files.igelcommunity.com/igel/igel%20os-rpi4-for-ncomputing-rx420-getting-started-guide.pdf

Important Information for IGEL OS(RPI4) 11.02.110 Release

IGEL OS(RPI4) release version **11.02.110** has been **removed** from the IGEL download server www.igel.com/software-downloads/workspace-edition/[6] and from the UMS > Universal Firmware Update.

Reason: In some cases, **when there are problems with the network consistency (or power) while the update is running, the device may enter a state where the update fails and the device is no longer usable**.

Unfortunately, there is no way to manually fix this directly on the device via USB options or similar. **As a solution, IGEL offers IGEL OS(RPI4) version 11.02.120** which handles interruptions and inconsistencies in the network during updates.

[6] https://www.igel.com/software-downloads/workspace-edition/

IGEL Workspace Edition

The firmware included with every IGEL Workspace product is multifunctional and contains a wide range of protocols allowing access to server-based services.

Management software: Universal Management Suite

For optimum management of your IGEL devices, the IGEL Universal Management Suite (UMS) is available on our download page[7].

> ⓘ With the IGEL Universal Management Suite, you can configure devices in the same way as in the devices' local setup.

- Supported Formats and Codecs(see page 47)

[7] https://www.igel.com/software-downloads/igel-universal-management-suite/

Supported Formats and Codecs

As supplied, IGEL OS 11 supports the following multimedia formats and codecs:

- Ogg/Vorbis
- Ogg/Theora
- WAV
- FLAC
- Multimedia Codec Pack (MMCP); enabled by the Workspace Edition, see IGEL Software License Overview
  The MMCP includes the following codecs:

Supported Formats	Supported Codecs
AVI	MP3
MPEG	AAC
ASF (restricted under Linux)	WMA stereo
WMA	WMV 7/8/9
WMV (restricted under Linux)	MPEG 1/2
MP3	MPEG4
OGG	H.264

ⓘ AC3 is not licensed.

Devices Supported by IGEL OS 11(RPI4)

Core Requirements

- CPU with 64-bit support
- CPU speed: ≥ 1 GHz
- Memory (RAM): ≥ 2 GB

NComputing

Name	Memory (RAM)	Storage	Processor	Supported from IGEL OS(RPI4) Version	Datasheet
RX420(IGEL)	2 GB	16 GB internal Micro SD card	Broadcom BCM2711	11.01.100	RX420_440-IGEL.pdf
RX440(IGEL)	4 GB	16 GB internal Micro SD card	Broadcom BCM2711	11.01.111	

Bluetooth Assistant

A Bluetooth Assistant starts before the actual Setup Assistant. This tests whether a USB mouse and/or a USB keyboard are available. If not, it searches for unconnected Bluetooth devices and helps you connect them.

The assistant starts with a window in which a timeout expires for a few seconds. During this time you can still cancel the wizard.

On the following setup pages you can make settings related to Bluetooth:

Bluetooth Tool:

Path: **Accessories > Bluetooth Tool**

Here you define the start options for the **Bluetooth Tool** session.

USB Access Control:

Path: **Devices > USB Access Control**

If you have USB access control enabled, you should make sure that you explicitly allow the connection to your Bluetooth devices via a class rule or device rule.

Bluetooth

Path: **Devices > Bluetooth**

Bluetooth must be activated here so that you can work with Bluetooth devices.

If you activate **Tray Icon**, you can start the Bluetooth tool via an icon in the system bar.

> ⓘ If you want to disable the Bluetooth Assistant in general, put the file `.igel_skip_bt-autopairing` in the directory `/wfs/user/`
> The assistant will be skipped.

Setup Assistant

Overview

When you start an unconfigured device, you will be welcomed by the **Setup Assistant**. This assistant takes you through the most important initial configuration steps.

> The Setup Assistant starts automatically after booting IGEL OS if all of the following requirements are met:
> - The device is not yet configured.
> - No IP address for the Universal Management Suite (UMS) was transferred using the DHCP option 224.
> - No UMS can be accessed under the DNS name `igelrmserver`.

Buttons

Next: Go to the next configuration step

Skip: This button is shown if the current configuration step can be omitted. If you click on **Skip**, nothing will change during the configuration step. If the configuration is edited, the button will switch to **Next**.

Back: Go back to the previous step

Cancel: Exit the setup assistant without saving changes to the configuration. Changes to the time and date will however remain effective.

Language

Language: Select the language for the user interface.

Keyboard Layout

Keyboard layout: Select the keyboard layout. The selected layout applies for all parts of the system including emulations, window sessions and X11 applications.

Time Zone Continent/Area

Timezone continent/area: Select the continent/area for your location.
Possible values:

- General: Under **Location**, you can select a GMT time zone.
- Africa ... Pacific: Under **Location**, you can select a city for the selected continent/area.

Location: Select your location or time zone.

ⓘ Location: Summer time adjustment is taken into account here. Example: If you select "Berlin", the device will switch between summer time and normal time in accordance with the German adjustment rules. Time zone: The GMT time zones specify by how many hours the time zone for a particular location differs from the Greenwich time zone. The preceding symbol is used in accordance with the POSIX format. Examples: For New York City, select "GMT+5" which means "5 hours west of Greenwich". For Moscow, select "GMT-3" which means "3 hours east of Greenwich".

Time and Date

Date: Select the current date.

Time: Set the current local time.

Use NTP Time Server

☑ The device uses the NTP time server that is entered in the field. You can specify multiple NTP time servers separated by spaces. Example: `0.de.pool.ntp.org 1.de.pool.ntp.org`

⚠ **NTP Server Highly Recommended**

Raspberry Pi-based devices like NComputing RX420(IGEL) have no battery-backed real-time clock. After a power outage, the system time will reset to the build time of the IGEL OS firmware. If the time and date are not correct, certificate issues may arise, which causes problems with websites, for instance.
Therefore, it is highly recommended to specify an NTP server. When an NTP server is configured, the system is always provided with the correct time and date.
To configure an NTP server via a UMS profile, edit **Use NTP time server** and **NTP time server** under **System > Time and Date**. For details on profiles, see Using Profiles.

Next: Sets the system clock according to what is entered above.

Mobile Broadband

In the basic mode (default), you can make the following settings:

Country: The country of your provider.

Provider: Provider (the possible options depend on what you choose for **Country**)

APN/Plan: APN/Plan (the possible options depend on what you choose for **Provider**)

For more configuration options, click the **Expert Mode** button.

In the expert mode, you can make the following settings:

- **Enabled**: Determines if the settings made in the expert mode are used. (Default: Enabled)
- **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.
- **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.
- **PIN**: PIN for the SIM card used.

Wireless

This configuration step is available if a WLAN adapter was found when starting the device. The device will search for available WLAN access points as soon as the configuration step is opened. The WLAN access points found will be listed. You can then connect to your desired WLAN access point.

> ⓘ If you carry out the WLAN configuration and exit the Setup Assistant by selecting **Finish**, the connection will be saved and WLAN will be permanently enabled. If you skip this configuration step or cancel the configuration, WLAN will not be permanently enabled.

Wireless regulatory domain: In the first selection menu, select the world region (example: **Europe**) in which you are situated and in the second one the country (example: **United Kingdom**).

⟳: Searches again for WLAN access points.

🔍: Opens a dialog which allows you to enter the WLAN name (SSID) of a hidden WLAN access point.

(Name of a WLAN access point in the list): Click on your desired WLAN access point and enter your access data in the dialog.

Once the connection is established, the ⇅ symbol will be shown in the **Connected** column.

Connectivity

This page is shown if for any reason no network connectivity is available.

Follow the instructions on the screen.

Local Logon

This step is optional. You can configure a local user password later under **Security > Logon > Local User**.

Login with screenlock password: A login screen is shown upon the start of the device, and a screenlock password set under **Password** is used to log in.

Password: Enter the desired password. The checker shown below assesses the strength of the password.

Password (repeated): Repeat the password.

Activate Your IGEL OS

In this step, you select the method for licensing the device.

If the device has no license yet, the following options are available:

- **Install license via UMS/ICG**
- **Manual license deployment**
- **Register for demo license**

If the device already has a license, the following options are available:

- **Keep using the current license**: You can continue with **Next**.
- **Manual license update**: The procedure is the same as that for **Manual license deployment**.

The options are described in detail further below.

Install License via UMS/ICG

The device will request a license from the UMS. If the device is outside the company network, the IGEL Cloud Gateway (ICG) will be used for connecting the device to the UMS. In this case, ICG access must be set up; see ICG Agent Setup(see page 61).

Manual License Deployment

You can deploy a license via HTTP download from a specific URL, via FTP, or from a USB memory stick.

To deploy a license from a URL:

1. Enter the complete URL of the license file in the text field, including the protocol.
2. Click **Install**.

To deploy a license via FTP:

1. Click **FTP**.
2. Define the access data for you FTP server:
   - **Host/Port**: URL of the FTP server on which the license file is located
   - **User**: User for accessing the FTP server
   - **Password**: Password associated with the **User**
3. Click **Browse**.
4. In the dialog, go to the license file and select it.
5. Click **Install**.

To deploy a license from a USB memory stick.

1. Click **File**.
2. Connect the USB flash drive that contains the license to the device.
3. Under **Storage Device**, select the USB flash drive that contains the license.
4. Click **Browse**.
5. In the dialog, go to the license file, select it and click **Open**.
6. Click **Install**.

Register for Demo License

With this evaluation license, all features of IGEL OS 11 are available for a fixed period. This period starts when the device has received the demo license.

> ⓘ For a demo license, you must accept the EULA to continue with setting up and using your device.

1. Make your choice as required and fill in all fields.
2. Activate the checkbox near **I agree to the terms + conditions and privacy policy**.
3. Click **ACTIVATE YOUR OS 11**.
   Your device fetches a demo license from IGEL.

Troubleshooting: Proxy Configuration

If you get an error at this stage of the wizard, you may need to configure a proxy.

1. Click **Proxy configuration** in the upper right of the wizard to get to the proxy configuration dialog.
2. Edit the proxy settings as required:
   - **Use proxy server**: Activate this if a proxy is required.
   - **HTTP Proxy**: Address of the HTTP proxy
   - **Port**: Port of the HTTP proxy
   - **SSL Proxy**: Address of the SSL proxy
   - **Port**: Port of the SSL Proxy
   - **SOCKS Host**: Address of the SOCKS Host
   - **Port**: Port of the SOCKS host
   - **User name**: User name for authentication
   - **Password**: Password for authentication

   > ⓘ **User name** and **Password** are the credentials for all proxy types configurable here (HTTP, SSL and SOCKS).

ICG Agent Setup

If your system administrator has given you access data for IGEL Cloud Gateway, you can connect the device to the gateway here.

You will find instructions for this under Using ICG Agent Setup(see page 61).

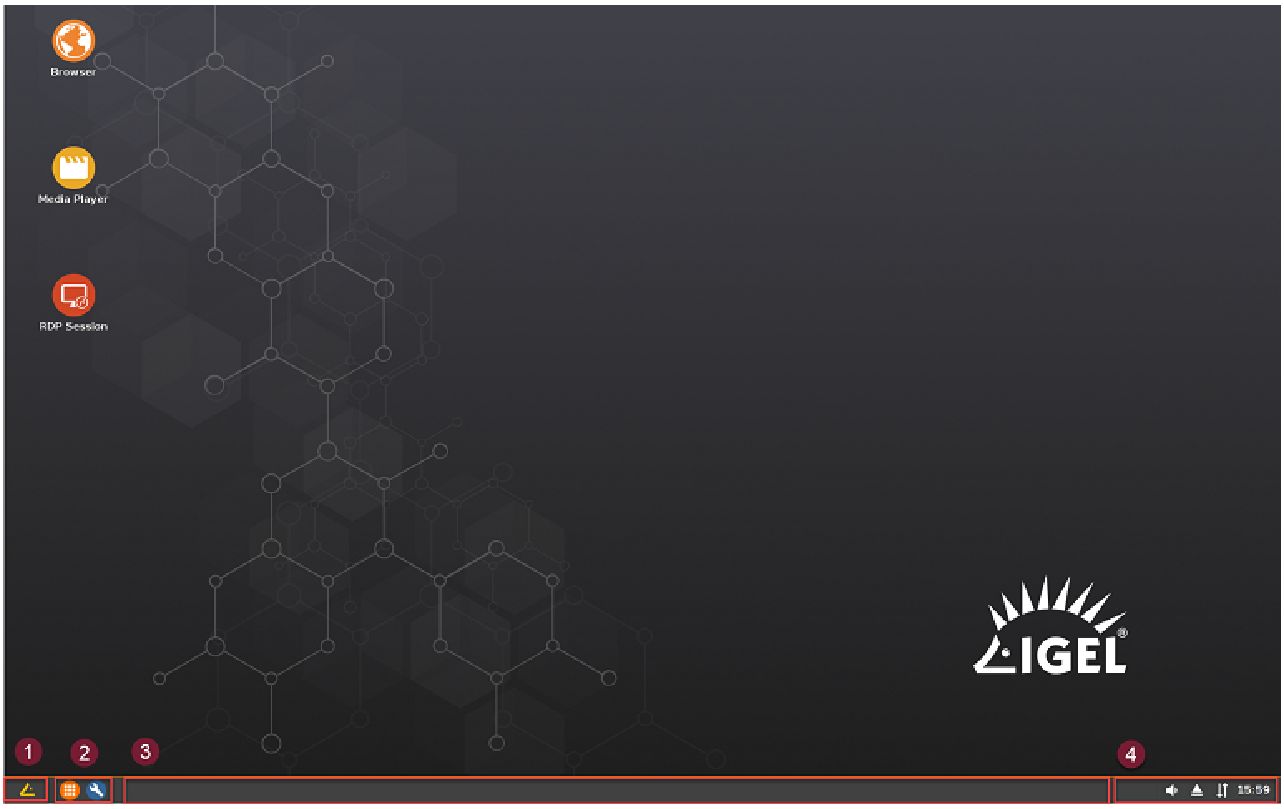
Otherwise, do not touch this page and click on **Skip** or **Next**.

Finish

Finish: Saves all settings and closes the Setup Assistant. If you have changed the language, the X11 graphics system will restart; the screen will go black for a short time. If you have a UD Pocket Demo, a restart is required to finish the activation.

The IGEL OS Desktop

You can operate the device via the taskbar and the *IGEL* menu.



The following items can be found in the taskbar at the bottom of the screen:

1			Opens the *IGEL* menu.
2	Quick Start Panel		
		▦	Application Launcher: Opens a dialog window with start symbols for sessions.
		🔧	Setup: Opens the *IGEL* setup.

		🌐 🎬 🖥	Symbol for sessions: Launches a session.
3	Window bar		
		Window buttons	Allows you to switch between open windows.
4	System tray		
		⚙	CPU power plan: Changes the power saving settings.
		🔈	Volume control
		⏏	Allows you to remove a USB stick safely
		⇅	Local network connection
		09:14	Time / date

The *IGEL* menu offers the following areas and functions:

- **Sessions**: Allows you to launch sessions
- **System**: Allows you to launch system programs
- **About**: Shows all relevant system information
- **Search window**: Allows you to find sessions and functions in the start menu
- ⏻ Allows you to shut down the device
- ↻ Allows you to restart the device

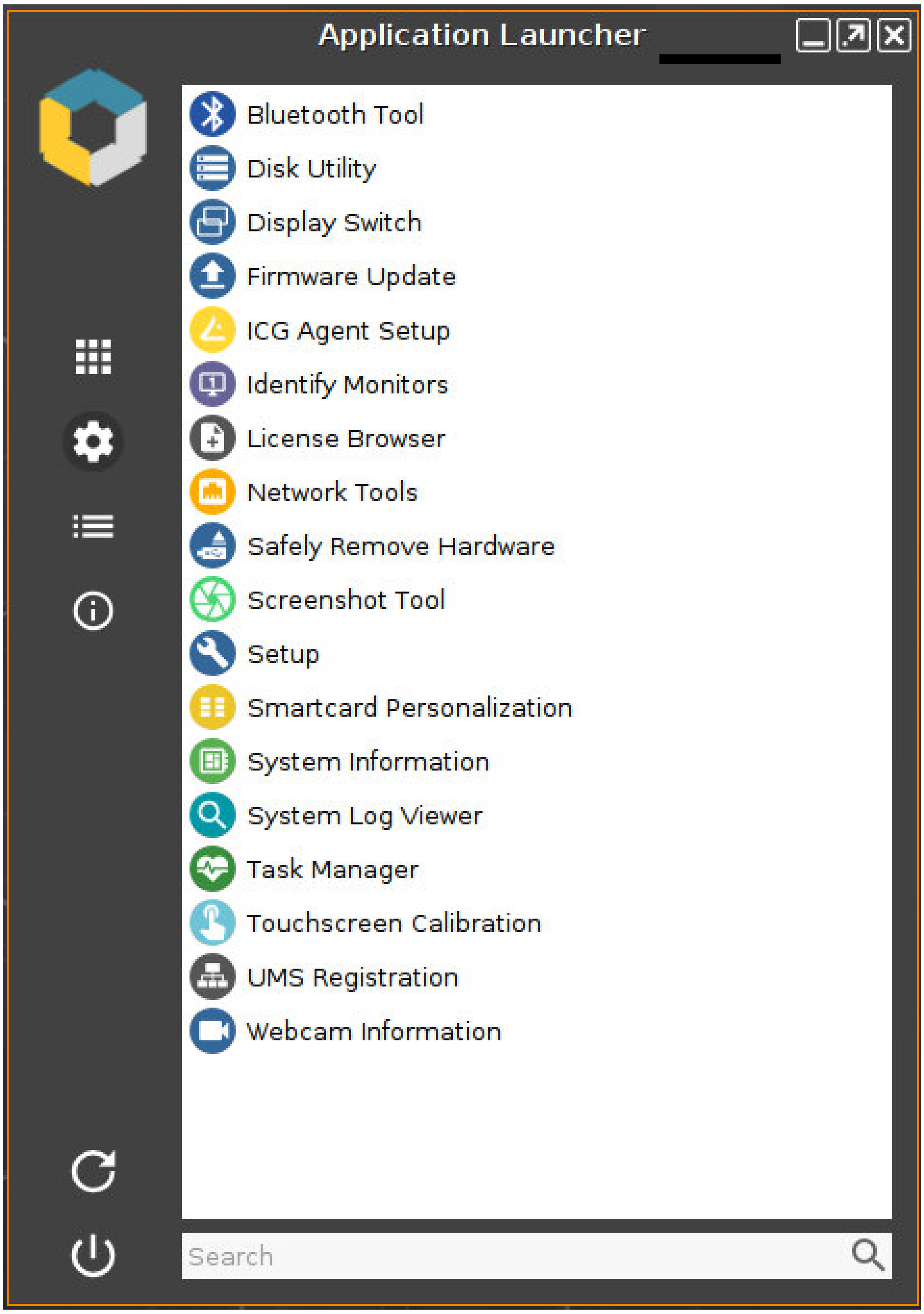
- Application Launcher(see page 66)
- Sessions(see page 68)
- System(see page 69)
- License(see page 70)

- About Window(see page 71)
- Restart and Shutdown(see page 72)

Application Launcher

To launch the **Application Launcher**, proceed as follows:

- Click on ▦ in the Quick Start Panel or in the start menu.



Application Launcher

- Bluetooth Tool
- Disk Utility
- Display Switch
- Firmware Update
- ICG Agent Setup
- Identify Monitors
- License Browser
- Network Tools
- Safely Remove Hardware
- Screenshot Tool
- Setup
- Smartcard Personalization
- System Information
- System Log Viewer
- Task Manager
- Touchscreen Calibration
- UMS Registration
- Webcam Information

Search

The sub-areas of the Launcher provide access to:

▦	Listing of the sessions(see page 68) that have been set up
⚙	Listing of the most important tools(see page 69)
☰	License declarations(see page 70) for the components used
ⓘ	The About Window(see page 71) with information about the system
↻	Restart
⏻	Shut down
🔍	Search field for fast access to the components

You will find information regarding the configuration here Application Launcher(see page 66).

Sessions

All sessions created are shown in a list of applications if they are enabled for the main session page.

▶ To open an application, double-click on it or click on ▶ **Run**.
Alternatively, you can launch sessions via icons on the desktop, in the quick launch bar or from the Start menu and context menu.
Applications can also be launched automatically and a key combination (hotkey) can be defined.
It is also possible, to build a file structure for the sessions in the application launcher. Therefor, in the setup page **Desktop Integration** of the relevant application you have to define a folder in the application launcher.

ⓘ The available options for launching a session can be defined under **Desktop Integration** in the session configuration.

System

Under **System** ⚙, you can execute various tools including the firmware updating tool with the pre-set update information.

The following tools are available:

- **Identify Monitors**: Shows the screen's number and manufacturer details.
- **Screenshot Tool**: Takes photos of the screen content.
- **Bluetooth Tool**: Starts the Bluetooth tool.
- **Firmware Update**: Carries out the update with the settings made during the setup.
- **Safely Remove Hardware**: Removes external storage devices without a risk of losing data.
- **Disk Utility**: Shows information regarding connected USB drives.
- **Network Tools**: Provides detailed information on the network connection and offers a number of problem analysis tools such as ping or traceroute.
- **Setup**: Launches the IGEL Setup.
- **System Information**: Shows information regarding hardware, the network and connected devices.
- **System Log Viewer**: Shows system log files "live" and allows you to add your own logs.
- **Task Manager**: Manages all processes.
- **Touchscreen Calibration**: Allows a connected touchscreen monitor to be calibrated.
- **UMS Registration**: Logs the device on to a UMS server (access data for the server are required).
- **Webcam Information**: Shows data relating to a connected webcam and allows the camera to be tested.

License

Under **License** ☰ you will find the following:

- The licenses for the components used in the UD system
- Information on the provision of source code, e.g. under GPL

About Window

In the **About** window, accessible via the ⓘ icon, you will find the following data:

- **Product**: Information regarding the installed firmware
  - Copyright
  - Firmware Version
  - Product ID
  - Product Name
  - Website
- **Network**: Computer name, hardware address and IP address of the device
  - Local Name
  - Standard Gateway (only with valid network connection)
  - DNS Server (only with valid network connection)
  - Universal Management Suite
- **Interface** [number name]:
  - Description
  - Hardware Address
  - IP Address

> If the network status changes, the details will automatically be updated. To force an update, click on ⟳.

- **Hardware**:
  - Boot Mode
  - CPU Model
  - Device Type
  - Flash Size
  - Graphic Chipset
  - Memory Size
  - Total Operating Time
  - Unid ID (equal to MAC address (UD, UDC) or serial number (UD Pocket))
- **Licensed Features**: List with all firmware features for which a license is available

> You can copy individual entries via the context menu (right mouse button).

Restart and Shutdown

Within the **Application Launcher** you will find two buttons for ↻ **rebooting** or ⏻ **shutting down** the device. Both actions can be disabled for the user and will then be available to the administrator only.

You can change the default action when shutting down the device using the button on the screen or the on/off button on the device itself in the setup under **System > Power Options > Shutdown**.

Setup

With the help of the setup, you can change the system configuration and session settings.

ⓘ Any changes you have made in the UMS take precedence and may no longer be able to be changed. A lock symbol before a setting indicates that it cannot be changed.

Starting the Setup

You can open the setup in the following ways:

- Double-click 🔧 in the **Application Launcher**
- or click on **Run**.
- Double-click 🔧 on the desktop (if available based on the settings).
- Select 🔧 **Setup** in the desktop context menu (if available based on the settings).
- Select **System >** 🔧 **Setup** in the start menu.
- Click on 🔧 in the Quick Start Panel.
- Launch the setup using the keyboard command [Ctrl]+[Alt]+[s], or
  in the Appliance Mode using [Ctrl]+[Alt]+[F2].

> ⓘ You can configure how the setup can be launched under **Accessories**. The options described above as well as combinations thereof are available.

End the Setup

In order to end the setup again, you have the following options:

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

▶ Click on **Cancel** if you have not made any changes and would like to abort the setup.

▶ Click on **OK** to save your changes and exit the setup.

Quick Setup

As administrator, you prepare the setup for the user. If you want to give the user the option of defining their own settings in certain areas of the setup, you can prepare a quick setup. A quick setup is a slimmed-down version of the setup. It only displays areas the user is allowed to change.

To create a quick setup session, proceed as follows:

1. Enable the password for the administrator in IGEL Setup under **Security > Password**.

   > ⓘ If users are to be allowed to edit parts of the setup only with a password, enable the password for the setup user too.

2. Under **Accessories > Quick Settings**, define the name and options for calling up the quick setup.

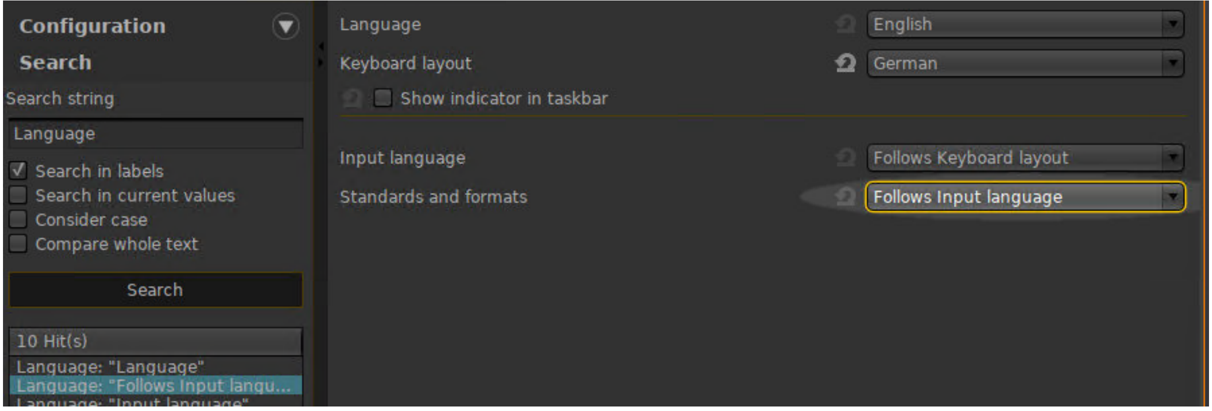
   > ⓘ You can set up a hotkey to start quick setup in appliance mode.

3. Under **Accessories > Quick Settings > Setup User Permissions**, enable those areas to which the user is to have access.

Setup Search

The **Search** function enables you to find parameter fields or parameter values within the setup.

1. To start a **search**, click on the button below the tree structure.
2. Enter the text to be searched for and the search details.
3. Select one of the hits.
4. Click on **Show result** and you will be taken to the relevant setup page.
   The parameter or value found will be highlighted as shown below.



Search string: Language

☑ Search in labels
□ Search in current values
□ Consider case
□ Compare whole text

10 Hit(s)
Language: "Language"
Language: "Follows Input langu...
Language: "Input language"

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

Sessions

Menu path: **Sessions > Sessions Summary**

In this area, you will find an overview of all available sessions.

Add: Adds a session from the selection of available session types.

Filter: Filters sessions shown in the list according to the string of characters entered.

- Copy Session(see page 79)
- Global Session Options(see page 80)
- Citrix(see page 81)
- SSH Session(see page 125)
- Chromium Browser Global(see page 133)
- Chromium Sessions(see page 147)

Copy Session

You can copy a session in the setup. The copy of the session has all the properties of the original session and is located in the same folder as the original session.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. In the **[Session Type] Sessions** area, click ⧉. Alternative: Open the context menu of the session by right-click and select **Copy**.
   A copy of the session will be created.

Global Session Options

Menu path: **Setup > Sessions > Global Session Options**

- **Network notification on session start**: If when launching sessions no network is available, a notification will be shown.
  ☑ Network notification is enabled (default)
  □ Network notification is disabled
- **Notification delay**: Time in seconds after which the notification is shown. (default: 15)
  Possible values:
  - 1 ... 120 seconds
- **Delay session start at boot time to apply new UMS settings**: If new settings were made in the UMS, the device may receive them during the boot procedure.
  ☑ The session start will be delayed until the settings have been transferred or the time limit has been exceeded.
- **Timeout**: Delay in seconds. (default: 10)
  Possible values:
  - 1 ... 120 seconds

Citrix

Menu path: **Setup > Sessions > Citrix**

Citrix Client Selection

Menu path: **Sessions > Citrix > Citrix Client Selection**

Citrix client version: Selects the Citrix client version to be used for Citrix sessions. For the included Citrix client versions, see the "Component Versions" section in the IGEL OS(RPI4) Release Notes(see page 152).

ⓘ After changing the **Citrix client version**, check the settings under:

- **Citrix > Citrix StoreFront > Server**
- **Citrix > Citrix StoreFront > Login**

Citrix Global

Menu path: **Sessions > Citrix > Citrix Global**

This section describes global Citrix settings which apply for all Citrix sessions. Most of these settings can be either carried over or overwritten in the individual sessions.

> ⓘ Please note that a number of configuration options depend on the version of the Citrix Receiver selected.

If there are problems with the logging in to a Citrix Storefront session because of the expired password, see Login Failed because of the Expired AD Password.

StoreFront Login

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**

In this area, you can define session-specific login options.

Authentication type: Depending on the Citrix client version, the following types are available:

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

ⓘ If you have set an authentication type with smartcard, select the type of card on the Smartcard (1)(see page 84) page.

Additional options include the following:

Use passthrough authentication

☑ Cached login data are used for listing and starting applications.

☐ No passthrough authentication (default)

Auto login

☑ Uses the login data preset on this page when connecting to the server.

☐ Do not log on automatically (default)

User name: Can only be filled in with password authentication

Password: Can only be filled in with password authentication

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

Domain: Can only be filled in with password authentication

Remember username and domain:

☑ Saves the user name and domain from the last login. (default)

☐ The user name and domain will not be saved.

Synchronize Citrix password with screen lock:

☑ Synchronizes the screen lock password with that of the Citrix application.

☐ No synchronization (default)

Relaunch Citrix login after logout:

☑ Automatically shows the login dialog again after logging off.

☐ Does not start the login procedure again. (default)

Start a single published application automatically: This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.
☑ The published application is started when the user has logged in.
☐ The published application is not started on login. (default)

Start following applications automatically after server connection is established: A list of applications to be started in the session.
To edit the list, proceed as follows:

- Click on ⊞ to create a new entry. In the Add dialog, give the name of the application.

ⓘ You can also enter part of the name followed by an asterisk (*).

- Click on ☒ to remove the selected entry.
- Click on

  Error rendering macro 'include'

  com.atlassian.renderer.v2.macro.MacroException: No page title provided.

  to move the entry upwards.
- Click on

  Error rendering macro 'include'

  com.atlassian.renderer.v2.macro.MacroException: No page title provided.

  to move the entry downwards.

ⓘ After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

Window

Menu path: **Setup > Sessions > Citrix > Citrix Global > Window**

Under **Window**, you can configure the following settings:

Multimonitor full-screen mode:

- Restrict full-screen session to one monitor
- Expand full-screen session across all monitors
- Expand the session over a self-selected number of monitors

> ⓘ Select this setting if you do not want to span the session across all monitors, but only across a certain number of monitors. Under **Monitor selection**, specify the relevant monitors.

StoreFront start monitor: This setting is available if you selected **Restrict full-screen session to one monitor** for **Multimonitor full-screen mode**.

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

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

Embed systray icons into window manager taskbar: Specifies if an application icon is shown in the local taskbar.

- On
- Off

Citrix connection bar

- Off: Disabled (Default)
- On: Shows a control bar for minimizing and closing a Citrix full-screen session.
- Factory default is "*": The Citrix connection bar is enabled or disabled by the server.

Screen Pinning

You can run multiple Citrix desktop sessions simultaneously on different monitors. In this section, you assign one or more monitors to each session.

If a desktop session is not assigned to monitors, the default settings in the general section of this Setup page apply to it.

> ⚠ This feature works only with desktop sessions; published applications cannot be controlled.

Error rendering macro 'include'

com.atlassian.renderer.v2.macro.MacroException: No page title provided.

For each Citrix desktop session, click

Error rendering macro 'include'

com.atlassian.renderer.v2.macro.MacroException: No page title provided.

to configure a corresponding monitor setup. The following parameters must be set:

Citrix session name: Name of the desktop session as displayed in the browser, desktop, or Self-Service. The session name is provided by the server. The wildcards "*" (any number of any characters) and "?" (any single character) can be used.

Example

With three desktop sessions that are named "Desktop2019", "DesktopW10", and "DesktopD10", you can assign settings like so, for instance:
"Desktop*": The settings are assigned to all three desktops.
"Desktop?10": The settings are assigned to "DesktopW10" and "DesktopD10".
"DesktopW10": The settings are assigned to "DesktopW10".

Multimonitor full-screen mode: Defines how the desktop sessions are distributed over the monitors. For the arrangement of the monitors and their numbering, go to **User Interface > Display**.

Possible options:

- Restrict full-screen session to one monitor: The desktop session is displayed on the monitor that is selected under **Desktop session start monitor**.
- Expand full-screen session across all monitors: The desktop session uses all monitors.
- Expand the session over a self-selected number of monitors: The monitors can be selected with **Monitor selection**.

Desktop session start monitor: The desktop session is displayed on the selected monitor.

Monitor selection: Selects one or several monitors on which this desktop session is to be displayed. This setting is available if you selected **Expand the session over a self-selected number of monitors**.

Example

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

Keyboard

Menu path: **Setup > Sessions > Citrix > Citrix Global > Keyboard**

On the **Keyboard** page, you can define alternative key combinations for hotkeys commonly used during ICA sessions. In *Windows* for example, the key combination [Alt]+[F4] closes the current window. This key combination works in ICA sessions too. All key combinations with [Alt] which are not used by the *X Window Manager* function in the familiar way during an ICA session.

The following settings can be configured:

Keyboard layout

- default: The local keyboard setting will be used in ICA too.
- Other Countries

Input language:

- default: The local keyboard setting will be used in ICA too.
- Other Countries

Mapping Ctrl+Alt+End to Ctrl+Alt+Del for Citrix sessions

☑ The user can use the combination [Ctrl]+[Alt]+[End]to change the password instead of [Ctrl]+[Alt]+[Del]when the corresponding prompt message appears.

☐ No mapping (default)

Keyboard mapping file: You can choose between two alternatives.

- generic: Sends language-independent scancodes from the keyboard to the computer.
- Linux: Sends language-specific scancodes.

Mouse middle button paste: Enables the copy/paste function of the middle mouse button.

The key alternatives are restricted to [Ctrl]+[Shift]+[Key] by default. However, you can change the settings by clicking on the Hotkey Modifier drop-down field and/or hotkey symbol for the relevant key combination.

- Possible keys: [F1] – [F12] , [Plus], [Minus], [Tab]
- Possible modifiers: [Shift], [Ctrl], [Alt], [Alt]+[Ctrl], [Alt]+[Shift], [Ctrl]+[Shift]
- **Toggle SpeedScreen**: Key combination for switching *SpeedScreen* (client reacts immediately to keyboard inputs or mouse clicks) on and off alternately.

Mapping

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping**

Locally connected devices such as printers or USB storage devices can be made available in ICA sessions.

- Drive Mapping (Citrix)(see page 90)
- COM Ports(see page 92)
- Printer(see page 93)
- Device Support(see page 94)

Drive Mapping (Citrix)

Menu path: **Setup > Sessions > Citrix > Citrix Global> Mapping > Drive Mapping**

Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to you during *ICA* sessions on *Citrix* servers.

In this area, you can specify which drives and paths are mapped during the logon. This applies for all *ICA* sessions.

- **Drive mapping**:
  ☑ *Citrix* servers can access the device's local drives. (default)

To manage the **Drive Mapping** list, proceed as follows:

▶ Click on ⊞ to create a new entry.

▶ Click on ⊠ to remove the selected entry.

▶ Click on ✎ to edit the selected entry.

▶ Click on ⧉ to copy the selected entry.

ⓘ Local (USB) devices which are to be used for drive mapping purposes must first be set up as storage devices(see page 90).

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

- Click on ⏏ in the task bar. The taskbar is not available in a fullscreen session.
- Function **Accessories > Safely Remove Hardware** with further starting possibilities; amongst other things, a hotkey can be defined here.
  If the following warning is displayed: **Volume(s) still in use. Dont' 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.

Add Drive Mapping

- **Enable**:
  ☑ The drive will be made available in the session.
- **Drive to map**: DOS-style drive letters on the Citrix Server.

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

- **Local drive path**: Unix path name of the local directory to which the mapping is to refer.

> ⓘ If you map a locally connected device, use the pre-defined path names available in the drop-down field.

- **Read access**
  Possible options:
  - yes
  - no
  - ask user: The read access right is queried when each ICA session is accessed for the first time.
- **Write access**
  Possible options:
  - yes
  - no
  - ask user: The write access right is queried when each ICA session is accessed for the first time.

COM Ports

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > COM Ports**

- **COM port mapping**
  ☑ Enables the mapping of serial devices connected to the device to the serial interfaces of the Citrix server. (Default)

To manage the list of **COM port devices**, 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.

Add

- **COM port device**: Allows you to select from all serial and USB interfaces on the device.
  Possible values:
  - "COM 1"
  - "COM 2"
  - "COM 3"
  - "COM 4"
  - "USB COM 1"
  - "USB COM 2"
  - "USB COM 3"
  - "USB COM 4"
- **Detect Devices...**: Opens a dialog allowing you to select the device file. 3 device files are available for each device; the **Description** column shows the type of device file:
  - (GENERIC) [device designation]: Generic type. The name of the device file ends in a consecutive number which depends on the boot procedure or the order of insertion. Example: `/dev/ttyUSB0`
  - (BY PORT) [device designation]: According to USB port. The device file is in the `/dev/usbserial/` directory. The name of the device file ends in the number of the USB port that the device is plugged into. Example: `/dev/usbserial/ttyUSB_P12`
  - (BY USBID) [device designation]: According to USB ID. The device file is in the `/dev/usbserial/` directory. The name of the device file ends as follows: `_V[Vendor ID]_P[Product ID]` . Example: `/dev/usbserial/ttyUSB_V067b_P2303`
  - (Virtual) [device designation]: Virtual device; used for signature pads for example. Example: `/dev/ttyVST0`

> ⓘ If your device has an additional multiport PCI card, more than 2 connections may be available.

Printer

Menu path: **Setup > Sessions > Citrix > Citrix Global > Mapping > Printer**

You can set up a printer for ICA sessions here.

Client printer mapping: With this function, the locally connected device printer is made available for your ICA sessions, provided that it was not disabled on the server side.

Set another default printer:

☑ Allows you to specify a default printer for the client which differs from the one defined in the printer setup.

□ Do not set another default printer. (default)

Default printer: Print queues used on the device to specify the default printer for the session. `lp` is the locally configured default printer.

Default printer driver: Windows driver name for the printer which is automatically set up. Enter one of the universal drivers or your own driver name here.
Possible values:

- Metaframe XP PS Universal Driver
- Metaframe XP PCL5c Universal Driver
- Metaframe XP PCL4 Universal Driver
- Citrix PCL4 Universal Driver (old)
- User entry

ⓘ See also https://support.citrix.com/article/CTX140208.

ⓘ The printers must be set up on the **Devices > Printers > CUPS > Printer** page and must be enabled there for mapping in ICA sessions.

Because the device merely places incoming print jobs in a queue, you need to install the printer on the server.

Device Support

Menu path: **Sessions > Citrix > Citrix Global > Mapping > Device Support**

Philips speech channel for dictation

☑ A virtual channel for communication with Philips dictation devices is enabled.

☐ No virtual channel for communication with Philips dictation devices is enabled. (Default)

DPM server drive: Via this drive, the Philips PocketMemo dictation device makes the voice recordings available to the server. (Default: P)

> ⓘ The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter, see **Devices > Storage Devices > Storage Hotplug** and **Sessions > Citrix > Citrix Global > Mapping > Drive Mapping**.

SpeechAir server drive: Via this drive, the Philips SpeechAir dictation device makes the voice recordings available to the server. (Default: S)

> ⓘ The dictation device is automatically assigned to the selected drive letter. Ensure that no other Hotplug storage device is assigned to this drive letter, see **Devices > Storage Devices > Storage Hotplug** and **Sessions > Citrix > Citrix Global > Mapping > Drive Mapping**.

Firewall

Menu path: **Setup > Sessions > Citrix > Citrix Global > Firewall**

In this area, you can configure the following firewall settings:

- **Alternative address**:
  ☑ Allows you to use a proxy or Secure Gateway server as an alternative address for connections via a firewall.
  □ Do not use an alternative address (default)

  > ⓘ After enabling the alternative address, add the server to the address list under **Sessions > Citrix > Citrix Global > Legacy ICA Server Location**.

SOCKS / Secure Proxy

- **Proxy type**
  - None (Direct Connection)
  - SOCKS: A proxy that uses the SOCKS protocol
  - Secure (HTTPS): An HTTP proxy with TLS/SSL encryption.
- **Proxy server**: Name or IP address of the proxy server
- **Proxy port**: TCP port of the proxy server (default: 1080)

Secure Gateway (relay mode)

- **Secure gateway address**: If you would like to use a Citrix Secure Gateway in relay mode, you must give the full DNS name – the IP address is not sufficient in this case.
- **Port**: TCP port of the gateway (default: 443)

Options

Menu path: **Sessions > Citrix > Citrix Global > Options**

In this area, you can set up additional options to optimize the system's general behavior and its performance.

Use server redraw

☑ The Citrix server is responsible for refreshing the screen content.

☐ Do not use server redraw. (Default)

Disable Windows alert sounds

☑ Switches off the Windows warning sounds.

☐ The warning sounds remain enabled. (Default)

Backing store

☑ The X Server temporarily stores hidden window content.

☐ Window content is not stored. (Default)

Deferred screen update mode

☑ Enables delayed updates from the local video buffer on the screen. The local video buffer is used if the seamless Windows mode or HDX latency reduction is used.

☐ No delayed update. (Default)

Cache size in kB: (default: 1024)

Minimum bitmap size in bytes: The minimum size of the bitmap files that are to be stored in the cache. (Default: 1024)

Persistent cache path: The directory where the files are to be stored locally. (Default: $ICAROOT/cache)

> Do not make the cache too big otherwise you run the risk of the device having too little storage space for its own system and other applications. You may have no alternative but to equip your device with additional RAM.

Scrolling control: Depending on the speed of your network or the response time of your server, there may be a delay between you letting go of the mouse button on a scroll bar and the scrolling actually stopping (e.g. when using Excel). Changing this value may help. (Default: 100)

Audio bandwidth limit in StoreFront sessions

- High
- Medium
- Low

> Higher quality requires more network and computing resources.

Auto reconnect

☑ Automatically attempt to reconnect if connection is terminated. (Default)

☐ Do not attempt to reconnect.

Maximum retries: (default: 3)

Delay in seconds before reconnecting: (default: 30)

Allow Kerberos passthrough authentication in StoreFront sessions

☑ Kerberos passthrough authentication is allowed. (Default)

□ Kerberos passthrough authentication is not allowed.

ⓘ This point concerns Citrix XenApp in Version 6.5 and older.

CGP address

- Use server address
- Text input
- disabled

Multistream sessions

☑ Support multistream ICA.

□ Do not support multistream ICA. (Default)

HDX Adaptive Transport over EDT
Possible options:

- UDP with fallback to TCP
- TCP Only - UDP disabled
- UDP without fallback to TCP

Native USB Redirection

Menu path: **Sessions > Citrix > Citrix Global > Native USB Redirection**

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

Native USB redirection

☑ Native USB redirection is enabled globally.

> ⓘ Disable USB redirection if you use DriveLock.

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

- Deny
- Allow

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

Class Rules

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

To manage rules, proceed as follows:

- ▶ Click ⊞ to create a new entry.
- ▶ Click ☒ to remove the selected entry.
- ▶ Click ✎ to edit the selected entry.
- ▶ Click ⧉ to copy the selected entry.

Add class rule:

Rule:

- Allow
- Deny

Class ID: Selection list

Sub-class ID: Selection list

Name: Free text entry

Device Rules

Device rules apply to specific USB devices.

Add device rule:

Rule:

- Allow
- Deny

Vendor ID: Hexadecimal manufacturer number

Product ID: Hexadecimal device number

ⓘ To find out the **Vendor ID** and **Product ID** of the connected USB device, use the command `lsusb` (or `lsusb | grep -i [search term]`) in the terminal. You can also use the **System Information** tool (**Accessories > System Information**).

Name: Free text entry

HDX Multimedia

Menu path: **Sessions > Citrix > Citrix Global > HDX Multimedia**

HDX multimedia redirection improves the playback of audio and video content during a Citrix session.

Multimedia redirection

☑ Multimedia data are sent to the device and decoded there.

□ Multimedia data are decoded on the server.

HDX RealTime Webcam redirection

☑ Redirection is enabled.

□ Redirection is disabled.

Automatic HDX webcam configuration

☑ The endpoint device detects the characteristics of the webcam and derives 6 different quality levels from these characteristics. The user can choose a quality level with the **Resolution grade** parameter.

□ The webcam must be configured manually using **HDX Webcam frame rate** and the subsequent parameters. For information on how to determine the capabilities of the webcam, see Using Webcam Information(see page 100).

Resolution grade
Possible options:

- "Very low"
- "Low"
- "Normal"
- "High"
- "Very high"
- "Best"

HDX Webcam frame rate: The frame rate that is requested from the webcam

HDX Webcam quality: The image quality requested from the webcam. Range: 1-63

HDX Webcam width: The image width requested from the webcam

HDX Webcam height: The image height requested from the webcam

HDX Webcam delay time: Time to wait before the webcam is opened, in milliseconds

HDX Webcam delay type
Possible options:

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

Browser content redirection

☑ The browser content is redirected from the server to the device, e.g. to relieve the load on the server.

□ Browser content redirection is disabled.

Codec

Menu path: **Setup > Sessions > Citrix > Citrix Global > Codec**

- **Graphical codec**: Decoding method for the transferred screen content
  - Automatic: Automatically selects the appropriate codec according to the performance of the hardware.
  - H.264 Deep Compression Codec:
    - High image quality is possible, with lower network load
    - Without available hardware acceleration it is very CPU intensive.

    > At the Citrix Server following policies must be set:
    > - **Use video codec for compression** must be enabled.
    > - **For the entire screen**: Text tracking should be enabled if bandwidth is not a problem to increase readability in Office applications
    > - **For actively changing regions**: Citrix Receiver 13.6+ required, otherwise JPEG fallback will be loaded
    > - **Use video codec when preferred**: If **For actively changing regions** is selected by Citrix, a Citrix receiver 13.6+ must be activated, otherwise JPEG fallback is loaded.
  - JPEG:
    - High image quality possible, with high network load
    - Moderate CPU load

Additional parameters for H.264 Deep Compression Codec

These parameters are relevant if **Automatic** or **H.264 Deep Compression Codec** is selected.

- **Accelerated H.264 Deep Compression Codec**
  ☑ Enables hardware-accelerated decoding with H.264, which reduces CPU load.
  □ Uses the software implementation of H.264 and results in a greater CPU load. (default)

Following options are available in combination with H.264 Deep Compression Codec:

- **Text tracking**:
  ☑ Loss-free depiction of texts (default)
  Text is displayed sharper, especially if "Visual Quality" is set to Low/Medium. Recommended for office applications, but requires a higher available bandwidth. With bad connection and EDT over UDP it can lead to missing text parts.
- **Small frames feature**:
  ☑ Pixel-perfect depiction of lines etc. (default)
  This feature allows efficient processing when only a small part of the screen changes over time (for example, when a cursor flashes on an otherwise stable background).

Additional parameters for JPEG

These parameters are relevant if **JPEG** is selected.

- **JPEG direct-to-screen decoding**

☑ Decodes image tiles directly without using a bitmap cache.
☐ No JPEG direct-to-screen decoding (default)

- **JPEG batch decoding**
  ☑ Enables batch processing and delayed XSync. (default)

Citrix StoreFront

Menu path: **Sessions > Citrix > Citrix StoreFront**

Most of the settings were already configured under Citrix Global.

- Server(see page 104)
- Login(see page 105)
- Appearance(see page 107)
- Reconnect(see page 108)
- Refresh(see page 110)
- Logoff(see page 111)
- Desktop Integration(see page 113)

Server

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront** > **Server**

- **Server location:** You can set up up to 5 Citrix master browsers per domain. If the first browser is not available, the second will be queried and so on. Please note that multiple farms can be searched. You can therefore specify addresses for a number of server farms.
- To manage the list, proceed as follows:
  - Click on ⊞ to create a new entry.
  - Click on ☒ to remove the selected entry.
  - Click on ✎ to edit the selected entry.
  - Click on ⧉ to copy the selected entry.

Add

- **Protocol**:
  - https://
- **Citrix Store site address**: Server name or IP address of the server
- **Port**: Network port on which the service is available (default: 443)
- **Path to Store**: (default: Citrix/Store)
- **Store name**: Name of the Citrix store

Domains

- To manage the list of **domains**, proceed as follows:
  - Click on ⊞ to create a new entry.
  - Click on ☒ to remove the selected entry.
  - Click on ✎ to edit the selected entry.
  - Click on ⧉ to copy the selected entry.

Handling of domain in login window:

- normal
- locked
- hidden

Login

Menu path: **Sessions > Citrix > Citrix StoreFront > Login**

In this area, you can define session-specific login options.

Authentication type: Depending on the Citrix client version, the following types are available:

- Password authentication: Suitable for on-premises connections; connections via Citrix NetScaler or to a cloud environment may cause problems.
- Kerberos passthrough authentication: Uses local login data for listing and launching applications. The option enables single sign-on if login with AD/Kerberos is configured on the device.
- Smartcard authentication (StoreFront only, not Web Interface)
- Citrix authentication mechanism (instead of IGEL), Smartcard disabled
- Citrix authentication mechanism (instead of IGEL), Smartcard enabled

ⓘ If you have set an authentication type with smartcard, select the type of card on the Smartcard (1)(see page 105) page.

Additional options include the following:

Use passthrough authentication

☑ Cached login data are used for listing and starting applications.

☐ No passthrough authentication (default)

Auto login

☑ Uses the login data preset on this page when connecting to the server.

☐ Do not log on automatically (default)

User name: Can only be filled in with password authentication

Password: Can only be filled in with password authentication

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

Domain: Can only be filled in with password authentication

Remember username and domain:

☑ Saves the user name and domain from the last login. (default)

☐ The user name and domain will not be saved.

Synchronize Citrix password with screen lock:

☑ Synchronizes the screen lock password with that of the Citrix application.

☐ No synchronization (default)

Relaunch Citrix login after logout:

☑ Automatically shows the login dialog again after logging off.

☐ Does not start the login procedure again. (default)

Start a single published application automatically: This parameter is relevant if exactly 1 published application is provided for the user whose login is configured here.
☑ The published application is started when the user has logged in.
☐ The published application is not started on login. (default)

Start following applications automatically after server connection is established: A list of applications to be started in the session.
To edit the list, proceed as follows:

- Click on ⊞ to create a new entry. In the Add dialog, give the name of the application.

> ⓘ You can also enter part of the name followed by an asterisk (*).

- Click on ☒ to remove the selected entry.
- Click on

  Error rendering macro 'include'

  com.atlassian.renderer.v2.macro.MacroException: No page title provided.

  to move the entry upwards.
- Click on

  Error rendering macro 'include'

  com.atlassian.renderer.v2.macro.MacroException: No page title provided.

  to move the entry downwards.

> ⓘ After a successful login, the associated desktop icon for each available application will be placed on the device desktop. All applications whose name matches one of the names given in the **Start following applications automatically after server connection is established** area will then be launched.

Appearance

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Appearance**

- **Show applications in the start menu**
  ☑ Applications will appear in the start menu (default)
  □ Applications will not appear in the start menu
- **Show in the start menu**
  - All: All Citrix applications will be shown in the start menu.
  - Follow server settings
- **Resize icons for the start menu**
  ☑ The size of icons for the start menu will automatically be adjusted. (default)

  > ⓘ Automatic scaling can prolong the logon procedure.

- **Apply display filter to start menu entries**
  ☑ Only the applications selected in the display filter will be shown in the start menu.
  □ Do not use display filter (default)
- **Show applications in the Application Launcher**
  ☑ Applications will be shown in the Application Launcher. (default)
- **Apply display filter to Application Launcher entries**
  ☑ Only the applications selected in the display filter will be shown in the Application Launcher.
  □ Do not use display filter (default)
- **Show applications on desktop**
  ☑ The applications will be shown on the desktop. (default)
- **Keep folder structure on desktop**
  ☑ The Citrix sessions are shown in their directory structure on the desktop.
  □ The directory structure is not shown. (default)
- **Show desktop shortcuts**
  - All: All Citrix applications will be shown in the Desktop Launcher.
  - Follow server settings
- **Apply display filter to desktop icons**
  ☑ Desktop icons are created only for the applications selected in the display filter (see below). (default)
- **Display filter: Show only the following applications**. In the **Add** dialog, enter the name of the application that is to be shown on the desktop.
  To manage the list, proceed as follows:
  - Click on ⊞ to create a new entry.
  - Click on 🗑 to remove the selected entry.
  - Click on ✎ to edit the selected entry.
- **Enable following applications in quick start panel**: In the **Add** dialog, enter the name of the application that is to be shown in the quick start panel.

Reconnect

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Reconnect**

- **Automatic reconnection at logon**
  ☑ Connection will take place when logging on.
  □ Do not reconnect (default)
- **Connect to**
  Possible values:
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Automatic reconnection from menu/desktop**
  ☑ Reconnect
  □ Do not reconnect (default)
- **Connect to**
  Possible values
  - Active and terminated sessions
  - Terminated sessions only
  - Ask user
- **Reconnect session name**: Session name (default: Reconnect)

Starting Methods for Sessions

- **Start menu**: If this option is enabled, the session can be launched from the start menu.
- **Application Launcher**: If this option is enabled, the session can be launched with the Application Launcher.
- **Desktop**: If this option is enabled, the session can be launched with a program launcher on the desktop.
- **Quick start panel**: If this option is enabled, the session can be launched with the quick start panel.
- **Start menu's system icon**: If this option is enabled, the session can be launched with the start menu's system icon.
- **Application Launcher's system icon**: If this option is enabled, the session can be launched with the Application Launcher's system icon.
- **Desktop context menu**: If this option is enabled, the session can be launched with the desktop context 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.
- **Path in the Application Launcher**: 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 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.
- **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's password is requested when launching the session.
- **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`. Here, you will find the available modifiers and the associated key symbols:
    - (No modifier) = `None`
    - ⇧ = `Shift`
    - [Ctrl] = `Ctrl`
    - ⊞ = `Super_L`
    - [Alt] = `Alt`

  Key combinations are formed as follows with `|`:
    - Ctrl + ⊞ = `Ctrl|Super_L`
- **Key**: Key for the hotkey

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

Refresh

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Refresh**

- **Refresh Session Name:** (default: Update)

Starting Methods for Session

- **Start menu**
  ☑ The session can be started with the start menu. (default)
- **Application Launcher**
  ☑ The session can be started with the Application Launcher. (default)
- **Desktop**:
  ☑ The session can be started with a program starter on the desktop. (default)
- **Quick start panel**
  ☑ The session can be started with the quick start panel. (default)
- **Start menu's system icon**
  ☑ The session can be started with the start menu's system icon.
  □ The session cannot be started with the start menu's system icon. (default)
- **Application Launcher's system icon**
  ☑ The session can be started with the Application Launcher's system icon.
  □ The session cannot be started with the Application Launcher's system icon. (default)
- **Desktop context menu**
  ☑ The session can be started with the desktop context menu. (default)
- **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.
- **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.
- **Password protection**: Specifies which password will be requested when launching the session. (default: disabled)
  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's password is requested when launching the session.
- **Hotkey**: Specifies a hotkey consisting of modifiers and a key which can be used to launch the session. (default: disabled)
  - **Modifiers**: One or two modifiers for the hotkey
  - **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 in 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 character string for the **Key** field. Example: `Tab` in `(keysym 0xff09, Tab)`

Logoff

Menu path: **Setup > Sessions > Citrix > Citrix StoreFront > Logoff**

- **Logoff session name:** Session name (default: Logoff)

Starting Methods for Session

- **Session name**: Name for the session

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

- **Start menu**:
  ☑ The session can be started with the start menu. (Default)
  □ The session cannot be found in the start menu.
- **Application Launcher**:
  ☑ The session can be started with the Application Launcher. (Default)
  □ The session cannot be found in the Application Launcher.
- **Desktop**:
  ☑ The session can be started with a program starter on the desktop. (Default)
  □ The session does not have a program starter on the desktop.
- **Quick start panel**:
  ☑ The session can be started with the quick start panel.
  □ The session cannot be found in the quick start panel. (Default)
- **Start menu's system icon**:
  ☑ The session can be started with the start menu’s system icon.
  □ The session cannot be found in the start menu’s system icon. (Default)
- **Application Launcher's system icon**:
  ☑ The session can be started with the Application Launcher’s system icon.
  □ The session cannot be found in the Application Launcher’s system icon. (Default)
- **Desktop context menu**:
  ☑ The session can be started with the desktop context menu.
  □ The session cannot be found in the desktop context menu. (Default)
- **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.
- **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.
- **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's password is requested when launching the session.

- **Hotkey**: A hotkey with which the session can be started is defined. It consists of modifiers and a key.
- **Modifiers**: One or two modifiers for the hotkey:
  - `None`
  - ⇧ = `Shift`
  - [Ctrl] `= Ctrl`
  - ⊞ = `Super_L`
  - [Alt] = `Alt`

  Modifiers can be combined by using the pipe character `|:`
  - [Ctrl]+ ⊞ = `Ctrl|Super_L`
- **Key**: Key for the hotkey

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

Desktop Integration

Menu path: **Sessions > Citrix > Citrix StoreFront> Desktop Integration**

Login session name: Session name.

> 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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

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.

Citrix Self-Service

Menu path: **Sessions > Citrix > Citrix Self-Service**

The Citrix Self-Service interface allows access to Citrix Virtual Desktops and Apps via Self-Service UI.

Server

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server**

To manage the list, proceed as follows:

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

Server: Web Interface

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))
- **Path to config.xml file:** (default: Citrix/PNAgent/config.xml)
- **Store Name**: Name for the store

Server: StroreFront

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))
- **Path to the store** (default: Citrix/Store)
- **Store Name**: Name for the store

Server: StoreFront Legacy Mode

Add:

- **Protocol**:
  - http://
  - https://
- **Server**: Name or IP address of the server
- **Server port**: Port on which the service is available (default: 80 (http), 443 (https))
- **Path to the config.xml file** (default: Citrix/Store/PNAgent/config.xml)
- **Store Name**: Name for the store

Options

Menu path: **Setup > Sessions > Citrix > Citrix Self-Service > Server > Options**

- **Display mode**: Display type for the Self-Service user interface
  Possible values:
  - Window
  - Full screen

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

- **Multi user**
  ☑ The user data on the client will be deleted after logging off or terminating Self-Service. (default)
- **Reconnect after logon**:
  ☑ The Self-Service user interface reconnects automatically to applications and desktops after being launched.
  □ The Self-Service user interface does not reconnect automatically.
- **Reconnect to apps after starting an application**:
  ☑ The Self-Service user interface will attempt to reconnect to ongoing sessions if an application is launched or the store is reloaded.
  □ The Self-Service user interface will not attempt to reconnect. (default)

Desktop Integration

Self-Service session: Name for the Self-Service session. (Default: Self-Service)

> 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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

  Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

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.

Citrix Workspace Hub

Menu path: **Sessions > Citrix > Citrix Workspace Hub**

⚠ **Feature in Beta Status (Experimental)**

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

When your IGEL OS(RPI4) device is configured as a Citrix Ready Workspace Hub, you can use it for session roaming, session casting, and screen casting.

- Options(see page 121)
- Desktop Integration(see page 123)

Options

Menu path: **Sessions > Citrix > Citrix Workspace Hub > Options**

⚠ **Feature in Beta Status (Experimental)**

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

Autostart Citrix Workspace Hub Launcher

☑ The Citrix Workspace Hub Launcher is started automatically on system start.

☐ The Citrix Workspace Hub Launcher is not started automatically.

Citrix Workspace Hub (Beta)

☑ The Citrix Workspace Hub is enabled. When enabled, **Autostart Citrix Workspace Hub Launcher** is enabled as well but can be disabled separately.

URL for default launcher page

ⓘ The user can switch between the default launcher page, the second launcher page, and the third launcher page by clicking an arrow on the screen border.

- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- https://myworkprod0.cloud.com : Citrix launcher page; requires Internet access
- https://www.igel.com: IGEL homepage; requires Internet access
- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

QR code size

Possible options:

- small
- medium
- large

QR code position

Possible options:

- top left
- top right
- bottom left
- bottom right
- center: Exactly in the middle, both horizontally and vertically

URL for second launcher page

Possible options:

- Disabled: This page cannot be selected.
- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- https://myworkprod0.cloud.com: Citrix launcher page; requires Internet access
- https://www.igel.com: IGEL homepage; requires Internet access

- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

URL for third launcher page

Possible options:

- Disabled: This page cannot be selected.
- Default launcher page: System default launcher page; IGEL OS(RPI4) default background
- https://myworkprod0.cloud.com: Citrix launcher page; requires Internet access
- https://www.igel.com: IGEL homepage; requires Internet access
- Enter url here...: Custom URL of the launcher page of your choice; requires Internet access if external

Desktop Integration

⚠ **Feature in Beta Status (Experimental)**

In this version of IGEL OS(RPI4), the integration of Citrix Workspace Hub is in beta status (experimental).

Citrix Workspace Hub Session: Name for the Citrix Workspace Hub 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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

  Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart Citrix Workspace Hub Launcher

☑ Citrix Workspace Hub Launcher will be launched automatically when the device boots.

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.

SSH Session

Menu path: **Sessions > SSH > [Session Name]**

You can launch applications on a remote computer via SSH (Secure Shell). The display is usually on the terminal; X11 connections too can be routed via SSH.

▶ Click on ⊞ **Add** to create an SSH session.

In the following area, you can configure desktop integration for the SSH session.

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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted 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.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively.

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

- Command(see page 128)
- Options(see page 129)
- Desktop Integration(see page 130)

Command

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

Remote user name: User name under which the application runs on the remote computer If you do not give a name, you will be asked when the session starts.

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: **Sessions > SSH > [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.

Port: SSH port. (Default: 22)

Desktop Integration

Menu path: **Sessions > SSH > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the SSH session.

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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

  Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

Restart

☑ The session will be restarted 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.

Appliance mode access: Determines whether the session can be started in appliance mode. By default, appliance mode implies that one session is running on the device exclusively.

☑ The session can be started in appliance mode. The following starting methods can be used in appliance mode:

- **Desktop** (desktop icon; not in appliance mode **XDMCP for this Display**)
- **Desktop Context Menu** (not in appliance mode **XDMCP for this Display**)
- **Application Launcher** (includes **Application Launcher's system tab**; not in appliance mode **XDMCP for this Display**)
- **Hotkey**
- **Autostart** (not in appliance mode **XDMCP for this Display**)

☐ The session cannot be started in appliance mode.

Chromium Browser Global

Menu path: **Sessions > Chromium Browser > Chromium Browser Global**

Here, you can change settings that will be valid for all Chromium sessions.

Use IGEL Setup for configuration

☑ The settings made in the IGEL Setup or the UMS configuration dialog will be effective.

□ The settings made in the IGEL Setup or the UMS configuration dialog will not have any effect on the behavior of Chromium.

H.264 decoding

☑ Hardware acceleration will be used for H.264 decoding.

□ Hardware acceleration will not be used.

Automatic browser restart on exit

☑ Chromium is restarted when the user closes it.

□ Chromium is not restarted on exit.

Show browser splash screen

☑ The Chromium splash screen is shown on start.

□ Chromium starts without a splash screen.

General

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > General**

In this area, you can change the following settings:

On startup: Specifies what pages are shown when Chromium is launched.
Possible options:

- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.
- "Continue where you left off": All tabs from the last session are reopened.

Startup page: Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Open a specific page or set of pages" is chosen under **On startup.**

New tab page setting: Specifies the page that is shown when a new tab is opened.
Possible options:

- "Open a blank page"
- "Open a specific page": The page defined under **New tab page location** is shown.

New tab page location: Specifies the page that is shown when the user opens a new tab. This is effective only if **New tab page setting** is set to "Open a specific page".

Font size: Specifies the font size for web content.
Possible options:

- "Very small"
- "Small"
- "Medium (recommended)"
- "Large"
- "Very large"

Content

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Content**

Block pop-ups and redirects

☑ Pop-up windows and redirects are blocked.

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

Load images automatically

☑ Images from websites are loaded automatically.

Exceptions...: Add websites on which images are not loaded automatically.

Type of download directory
Possible options:

- "Custom location": The user will be prompted for a location to download a file.
- "userhome": Files will be downloaded to `/userhome/Downloads`.

Location: Defines the path files are downloaded to. Only effective when **Type of download directory** is set to "Custom location".

JavaScript

☑ JavaScript is enabled.

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

Integrated translation service of Chromium

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

Autoplay

☑ Embedded audio and video content on a web page is played automatically when the page is loaded.

☐ Audio and video content is not played automatically.

Proxy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Proxy**

In this area, you can change the proxy configuration.

To change the proxy configuration, proceed as follows:

1. In the **Proxy Configuration** menu, select the type of proxy configuration.
   The following proxy configurations are available:
   - "Never use a proxy"
   - "Use fixed proxy servers"
   - "Use a .pac proxy script"
   - "Use system proxy settings"
   - "Auto detect proxy settings"
2. Enter the necessary configuration data for the selected proxy configuration.

"Never use a proxy"

With this proxy configuration, no proxy is used.

"Use fixed proxy servers"

The configuration data must be specified in the following fields.

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

"Use a .pac proxy script"

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

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

"Use system proxy settings"

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

"Auto detect proxy settings"

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

Privacy

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Privacy**

Autofill addresses and more

☑ Entries in forms and search bars will be retained after Chromium restarts.

☐ Entries in forms and search bars will be retained only for the duration of the session.

Autofill payments

☑ Entries in payment forms will be retained after Chromium restarts.

☐ Entries in payment forms will be retained only for the duration of the session.

Autofill passwords

☑ Passwords entered will be retained after Chromium restarts.

☐ Passwords entered will be retained only for the duration of the session.

Clear browsing data

☑ Data entered will be deleted when Chromium is closed. What data are deleted is specified in the following options.

☐ Data entered will not be deleted when the browser is closed.

Browsing & download history

☑ Addresses (URLs) of visited websites and the list of downloads will be deleted when Chromium is closed.

Saved passwords

☑ Passwords entered will be deleted when Chromium is closed.

Cookies

☑ Cookies will be deleted when Chromium is closed.

Cache

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

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

Possible options:

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

Incognito mode

☑ Chromium is started in incognito mode.

☐ Chromium is started in normal browsing mode.

Enable "Do Not Track" feature

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

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

Block third party cookies

☑ Cookies from third parties are blocked.

□ Cookies from third parties are allowed.

Enable search suggestions

☑ Suggestions will be shown while an address is being typed in the address bar. The suggestions will be based on previously visited websites which are stored in the history.

Security

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Security**

In this area, you can define settings for preventing phishing and malware.

Enable phishing and malware protection

☑ The browser will check each address entered as to whether it can be found in the blacklist of fraudulent websites that use phishing. If this is the case, you will be given a warning.

□ The browser will not check whether an address is on the blacklist of fraudulent websites.

File access

☑ Chromium can access local files on the endpoint device. Downloads and uploads are allowed. Before a file is downloaded, a confirmation dialog is shown.

□ Local files cannot be accessed by Chromium. Neither downloads nor uploads are allowed. When the user tries to download a file, a message informs the user that downloads are blocked.

Encryption

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Encryption**

In this area, you can define the settings for encryption methods.

Minimum SSL/TLS version: This protocol will be used to establish a secure connection if no higher protocol is available. Higher protocols are preferred.
Possible options:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

Maximum SSL/TLS version: This protocol is requested when negotiating the connection. If this protocol is not available, the next lowest protocol will be requested.
Possible options:

- TLS 1.2
- TLS 1.3

Menus & Toolbars

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Menus & Toolbars**

In this area, you can change the browser’s menus and toolbars.

Hide home button

☑ The home button will not be shown.

□ The home button will be shown.

Hide bookmarks toolbar

☑ The bookmarks menu will not be shown in the menu bar.

□ The bookmarks menu will be shown in the menu bar.

Window

Menu path: **Sessions > Chromium Browser > Chromium Global > Window**

In this area, you can define the window settings for a Chromium session.

Enable kiosk mode

☑ Chromium starts in kiosk mode.

☐ Chromium starts in normal mode.

Start maximized

☑ Chromium starts in a maximized window.

☐ Chromium starts in a window with default size.

Chromium translation: Changes the default language when Chromium offers to translate a web page.

Block Chromium settings

☑ The settings menu of Chromium can not be accessed by the user.

☐ The user can access the settings menu.

Custom Setup

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup**

- Policies(see page 144)
- Custom Command Line Options(see page 145)

Policies

Menu path: **Sessions > Chromium Browser > Chromium Browser Global >Custom Setup > Policies**

Here, you can define policies for Chromium. For further information, see https://chromium.googlesource.com/chromium/src/+/master/docs/enterprise/add_new_policy.md.

- Click on ⊞ **Add** to create a policy.

Policy name: Name of the policy

Policy value: Value of the policy

Custom Command Line Options

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Custom Setup > Custom Command Line Options**

Here, you can define command-line parameters that are passed to Chromium on startup. The syntax is exactly the same as if Chromium would be started from a terminal.

Custom command-line parameters: One or more command-line parameters. Multiple parameters are separated by whitespace.

Example:

```
--proxy-server="socks://localhost:8080" --incognito
```

Smartcard Middleware

Menu path: **Sessions > Chromium Browser > Chromium Browser Global > Smartcard Middleware**

In this area, you can activate or deactivate smartcard middleware that is to be used for encryption.

Coolkey security device

☑ Coolkey will be used for encryption.

☐ Coolkey will be not used for encryption.

OpenSC security device

☑ OpenSC will be used for encryption.

☐ OpenSC will not be used for encryption.

Use a custom security device

☑ The PKCS#11 module stored under the **Path to the library** is used.

☐ The custom security device will not be used for encryption.

Name of the security device: Name of the custom security device that uses the library specified under **Path to the library**

Path to the library: Path to the custom PKCS#11 module

> ⚠ In case of the installation of a custom PKCS#11 library, the file(s) must be placed on the endpoint device either via UMS file transfer or via Custom Partition (**System > Firmware Customization > Custom Partition**).
> The use of the `/wfs` folder is NOT recommended because of its space limit.

Chromium Sessions

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name]**

In this area, you can configure desktop integration for the Chromium session.

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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

  Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

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**.

- Settings(see page 149)
- Desktop Integration(see page 150)

Settings

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Settings**

In this area, you can change the following settings:

On startup: Specifies what pages are shown when Chromium is launched.
Possible options:

- "Global setting"
- "Open the new tab page"
- "Open a specific page or set of pages": The page or set of pages specified under **Startup page** are opened.

Startup page: Specifies the URL of the start page. You can specify a set of start pages by separating the URLs of the start pages with a vertical dash "|". This setting is active only when "Show my home page" is chosen under **On startup.**

Desktop Integration

Menu path: **Sessions > Chromium Browser > Chromium Sessions > [Session Name] > Desktop Integration**

In this area, you can configure desktop integration for the Chromium session.

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.

Application Launcher

☑ The session can be launched with the Application Launcher.

Desktop

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

Quick start panel

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

Start menu's system tab

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

Application Launcher's system tab

☑ The session can be launched with the Application Launcher's system tab.

Desktop context menu

☑ The session can be launched with the desktop context 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.

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 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.

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's password is requested when launching the session.

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`. Here, you will find the available modifiers and the associated key symbols:

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

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

- [Alt] = `Alt`

  Key combinations are formed as follows with `|`:

- Ctrl + ⊞ = `Ctrl|Super_L`

Key: Key for the hotkey

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

Autostart

☑ The session will be launched automatically when the device boots.

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**.

IGEL OS(RPI4) Release Notes

Notes for Release IGEL OS(RPI4) 11.02.120

Software:	IGEL OS(RPI4) Version	11.02.120
Release Date:	2022-12-13	
Release Notes:	Version	RN-1102120-1
Last update:	2022-12-12	

Supported Devices IGEL OS(RPI4) 11.02.120

- UC3-RPI4 NComputing RX420/RX440

Component Versions IGEL OS(RPI4) 11.02.120

Clients

Product	**Version**
Chromium	104.0.5112.101-igel1660893911
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace App	21.04.0.11
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.7
Zulu JRE	8.0.345-1

Dictation

Philips Speech driver	12.9.2

Smartcard

PKCS#11 Library OpenSC	0.20.0-4igel38
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.8-1igel1655196158

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	9.0p1-1igel1650701678
OpenSSH Server	9.0p1-1igel1650701678
Bluetooth Stack (bluez)	5.64-0igel1647863644
MESA OpenGL Stack	22.1.5-1igel1659869061

VDPAU Library Version	1.5-1igel1646992192
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Synaptics	1.9.1-2+b1igel1647004160
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.15.56 #1
Xorg X11 Server	21.1.3igel1652689124
CUPS Printing Daemon	2.2.7-1ubuntu2.9igel1654064309
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel1650560118
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.20.3-2igel1655908747
WebKit2Gtk	2.36.6-1igel1660197492
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6+b1igel1649775315
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622

Services

Service Partitions	**Size**	**Services**
Java SE Runtime Environment	47.2M	Java SE Runtime Environment
Citrix ICA	89.2M	Citrix Workspace app Citrix StoreFront Citrix Workspace Hub

Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	3.0M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration
Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	98.0M	Local Browser (Chromium)
Limited Support Features	256.0K	Mobile Device Access USB (Limited support) Limited Support Features
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

Resolved Issues IGEL OS(RPI4) 11.02.120

Base System

- Fixed issue with the **update not working** if user partition is wrong or not present.

Notes for Release IGEL OS(RPI4) 11.02.110

⚠ **Important Information for Release IGEL OS(RPI4) 11.02.110**
IGEL OS(RPI4) release version **11.02.110** has been **removed** from the IGEL download server www.igel.com/software-downloads/workspace-edition/[8] and from the UMS > Universal Firmware Update.
Reason: In some cases, **when there are problems with the network consistency (or power) while the update is running, the device may enter a state where the update fails and the device is no longer usable**.
Unfortunately, there is no way to manually fix this directly on the device via USB options or similar. **As a solution, IGEL offers IGEL OS(RPI4) version 11.02.120** which handles interruptions and inconsistencies in the network during updates.

Software:	IGEL OS(RPI4) Version	11.02.110
Release Date:	2022-10-07	
Release Notes:	Version	RN-1102110-1
Last update:	2022-10-06	

[8] https://www.igel.com/software-downloads/workspace-edition/

Supported Devices IGEL OS(RPI4) 11.02.110

- UC3-RPI4 NComputing RX420/RX440

Component Versions IGEL OS(RPI4) 11.02.110

Clients

Product	**Version**
Chromium	104.0.5112.101-igel1660893911
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace App	21.04.0.11
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.7
Zulu JRE	8.0.345-1

Dictation

Philips Speech driver	12.9.2

Smartcard

PKCS#11 Library OpenSC	0.20.0-4igel38
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.9.8-1igel1655196158

System Components

OpenSSL	1.0.2n-1ubuntu5.10
OpenSSL	1.1.1-1ubuntu2.1~18.04.20
OpenSSH Client	9.0p1-1igel1650701678
OpenSSH Server	9.0p1-1igel1650701678
Bluetooth Stack (bluez)	5.64-0igel1647863644
MESA OpenGL Stack	22.1.5-1igel1659869061

VDPAU Library Version	1.5-1igel1646992192
Graphics Driver FBDEV	0.5.0-2igel1644486279
Graphics Driver VESA	2.5.0-1+b1igel1647004096
Input Driver Evdev	2.10.6-2+b1igel1647004239
Input Driver Synaptics	1.9.1-2+b1igel1647004160
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.15.56 #1
Xorg X11 Server	21.1.3igel1652689124
CUPS Printing Daemon	2.2.7-1ubuntu2.9igel1654064309
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel1650560118
XFCE4 Window Manager	4.14.5-1~18.04igel1643191202
ISC DHCP Client	4.3.5-3ubuntu7.3
NetworkManager	1.32.12-0ubuntu1igel1641211455
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.20.3-2igel1655908747
WebKit2Gtk	2.36.6-1igel1660197492
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.20-1igel1660111560
Mobile Device Access USB (imobile)	1.3.0-6+b1igel1649775315
Mobile Device Access USB (gphoto)	2.5.29-1igel1653377622

Services

Service Partitions	**Size**	**Services**
Java SE Runtime Environment	47.2M	Java SE Runtime Environment
Citrix ICA	89.2M	Citrix Workspace app Citrix StoreFront Citrix Workspace Hub

Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	3.0M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration
Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	98.0M	Local Browser (Chromium)
Limited Support Features	256.0K	Mobile Device Access USB (Limited support) Limited Support Features
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

Security Fixes IGEL OS(RPI4) 11.02.110

Chromium

- Fixed chromium-browser security issues:
  More...

  CVE-2022-2296, CVE-2022-2295,
  CVE-2022-2294, CVE-2022-2165, CVE-2022-2164, CVE-2022-2163, CVE-2022-2162, CVE-2022-2161, CVE-2022-2160, CVE-2022-2158, CVE-2022-2157, CVE-2022-2156, CVE-2022-2011, CVE-2022-2010, CVE-2022-2008, CVE-2022-2007, CVE-2022-2011, CVE-2022-2010, CVE-2022-2008, CVE-2022-2007, CVE-2022-1876, CVE-2022-1875, CVE-2022-1874, CVE-2022-1873, CVE-2022-1872, CVE-2022-1871, CVE-2022-1870, CVE-2022-1869, CVE-2022-1868, CVE-2022-1867, CVE-2022-1866, CVE-2022-1865, CVE-2022-1864, CVE-2022-1863, CVE-2022-1862, CVE-2022-1861, CVE-2022-1860, CVE-2022-1859, CVE-2022-1858, CVE-2022-1857, CVE-2022-1856, CVE-2022-1855, CVE-2022-1854, CVE-2022-1853, CVE-2022-1641, CVE-2022-1640, CVE-2022-1639, CVE-2022-1638, CVE-2022-1637, CVE-2022-1636, CVE-2022-1635, CVE-2022-1634, CVE-2022-1633, CVE-2022-1501, CVE-2022-1500, CVE-2022-1499, CVE-2022-1498, CVE-2022-1497, CVE-2022-1496, CVE-2022-1495, CVE-2022-1494, CVE-2022-1493, CVE-2022-1492, CVE-2022-1491, CVE-2022-1490, CVE-2022-1489, CVE-2022-1488, CVE-2022-1487, CVE-2022-1486, CVE-2022-1485, CVE-2022-1484, CVE-2022-1483, CVE-2022-1482, CVE-2022-1481, CVE-2022-1480, CVE-2022-1479, CVE-2022-1478, CVE-2022-1477, CVE-2022-1364, CVE-2022-1314, CVE-2022-1313, CVE-2022-1312, CVE-2022-1311, CVE-2022-1310, CVE-2022-1309, CVE-2022-1308, CVE-2022-1307, CVE-2022-1306, CVE-2022-1305, CVE-2022-1232, CVE-2022-1146, CVE-2022-1145, CVE-2022-1144, CVE-2022-1143, CVE-2022-1142, CVE-2022-1141, CVE-2022-1139, CVE-2022-1138, CVE-2022-1137, CVE-2022-1136, CVE-2022-1135, CVE-2022-1134, CVE-2022-1133, CVE-2022-1132, CVE-2022-1131, CVE-2022-1130, CVE-2022-1129, CVE-2022-1128, CVE-2022-1127, CVE-2022-1125, CVE-2022-1096, CVE-2022-0980, CVE-2022-0979, CVE-2022-0978, CVE-2022-0977, CVE-2022-0976, CVE-2022-0975, CVE-2022-0974, CVE-2022-0973, CVE-2022-0972, CVE-2022-0971, CVE-2022-0809, CVE-2022-0808, CVE-2022-0807, CVE-2022-0806, CVE-2022-0805, CVE-2022-0804, CVE-2022-0803, CVE-2022-0802, CVE-2022-0801, CVE-2022-0800, CVE-2022-0799, CVE-2022-0798, CVE-2022-0797, CVE-2022-0796, CVE-2022-0795, CVE-2022-0794, CVE-2022-0793, CVE-2022-0792, CVE-2022-0791, CVE-2022-0790, CVE-2022-0789, CVE-2022-0610, CVE-2022-0609, CVE-2022-0608, CVE-2022-0607, CVE-2022-0606, CVE-2022-0605, CVE-2022-0604, CVE-2022-0603, CVE-2022-0470, CVE-2022-0469, CVE-2022-0468, CVE-2022-0467, CVE-2022-0466, CVE-2022-0465, CVE-2022-0464, CVE-2022-0463, CVE-2022-0462, CVE-2022-0461, CVE-2022-0460, CVE-2022-0459, CVE-2022-0458, CVE-2022-0457, CVE-2022-0456, CVE-2022-0455, CVE-2022-0454, CVE-2022-0453, CVE-2022-0452, CVE-2022-0311, CVE-2022-0310, CVE-2022-0309, CVE-2022-0308, CVE-2022-0307, CVE-2022-0306, CVE-2022-0305, CVE-2022-0304, CVE-2022-0303, CVE-2022-0302, CVE-2022-0301, CVE-2022-0300, CVE-2022-0298, CVE-2022-0297, CVE-2022-0296, CVE-2022-0295, CVE-2022-0294, CVE-2022-0293, CVE-2022-0292, CVE-2022-0291, CVE-2022-0290, CVE-2022-0289, CVE-2022-0120, CVE-2022-0118, CVE-2022-0117, CVE-2022-0116, CVE-2022-0115, CVE-2022-0114, CVE-2022-0113, CVE-2022-0112, CVE-2022-0111, CVE-2022-0110, CVE-2022-0109, CVE-2022-0108, CVE-2022-0107, CVE-2022-0106, CVE-2022-0105, CVE-2022-0104,

CVE-2022-0103, CVE-2022-0102, CVE-2022-0101, CVE-2022-0100, CVE-2022-0099, CVE-2022-0098, CVE-2022-0097, CVE-2022-0096, CVE-2021-4102, CVE-2021-4101, CVE-2021-4100, CVE-2021-4099, CVE-2021-4098, CVE-2021-4068, CVE-2021-4067, CVE-2021-4066, CVE-2021-4065, CVE-2021-4064, CVE-2021-4063, CVE-2021-4062, CVE-2021-4061, CVE-2021-4059, CVE-2021-4058, CVE-2021-4057, CVE-2021-4056, CVE-2021-4055, CVE-2021-4054, CVE-2021-4053, CVE-2021-4052, CVE-2021-38022, CVE-2021-38021, CVE-2021-38020, CVE-2021-38019, CVE-2021-38018, CVE-2021-38017, CVE-2021-38016, CVE-2021-38015, CVE-2021-38014, CVE-2021-38013, CVE-2021-38012, CVE-2021-38011, CVE-2021-38010, CVE-2021-38009, CVE-2021-38008, CVE-2021-38007, CVE-2021-38006, CVE-2021-38005, CVE-2021-38003, CVE-2021-38002, CVE-2021-38001, CVE-2021-38000, CVE-2021-37999, CVE-2021-37998, CVE-2021-37997, CVE-2021-37996, CVE-2021-37995, CVE-2021-37994, CVE-2021-37993, CVE-2021-37992, CVE-2021-37991, CVE-2021-37990, CVE-2021-37989, CVE-2021-37988, CVE-2021-37987, CVE-2021-37986, CVE-2021-37985, CVE-2021-37984, CVE-2021-37983, CVE-2021-37982, CVE-2021-37981, CVE-2021-37980, CVE-2021-37979, CVE-2021-37978, CVE-2021-37977, CVE-2021-37976, CVE-2021-37975, CVE-2021-37974, CVE-2021-37973, CVE-2021-37972, CVE-2021-37971, CVE-2021-37970, CVE-2021-37969, CVE-2021-37968, CVE-2021-37967, CVE-2021-37966, CVE-2021-37965, CVE-2021-37964, CVE-2021-37963, CVE-2021-37962, CVE-2021-37961, CVE-2021-37960, CVE-2021-37959, CVE-2021-37958, CVE-2021-37957, CVE-2021-37956, CVE-2021-30633, CVE-2021-30632, CVE-2021-30631, CVE-2021-30630, CVE-2021-30629, CVE-2021-30628, CVE-2021-30627, CVE-2021-30626, CVE-2021-30625, CVE-2021-30624, CVE-2021-30623, CVE-2021-30622, CVE-2021-30621, CVE-2021-30620, CVE-2021-30619, CVE-2021-30618, CVE-2021-30617, CVE-2021-30616, CVE-2021-30615, CVE-2021-30614, CVE-2021-30613, CVE-2021-30612, CVE-2021-30611, CVE-2021-30610, CVE-2021-30609, CVE-2021-30608, CVE-2021-30607, CVE-2021-30606, CVE-2021-30604, CVE-2021-30603, CVE-2021-30602, CVE-2021-30601, CVE-2021-30600, CVE-2021-30599, CVE-2021-30598, CVE-2021-30597, CVE-2021-30596, CVE-2021-30594, CVE-2021-30593, CVE-2021-30592, CVE-2021-30591, CVE-2021-30590, CVE-2021-30589, CVE-2021-30588, CVE-2021-30587, CVE-2021-30586, CVE-2021-30585, CVE-2021-30584, CVE-2021-30583, CVE-2021-30582, CVE-2021-30581, CVE-2021-30580, CVE-2021-30579, CVE-2021-30578, CVE-2021-30577, CVE-2021-30576, CVE-2021-30575, CVE-2021-30574, CVE-2021-30573, CVE-2021-30572, CVE-2021-30571, CVE-2021-30569, CVE-2021-30568, CVE-2021-30567, CVE-2021-30566, CVE-2021-30565, CVE-2021-30564, CVE-2021-30563, CVE-2021-30562, CVE-2021-30561, CVE-2021-30560, CVE-2021-30559, CVE-2021-30557, CVE-2021-30556, CVE-2021-30555, CVE-2021-30554, CVE-2021-30553, CVE-2021-30552, CVE-2021-30551, CVE-2021-30550, CVE-2021-30549, CVE-2021-30548, CVE-2021-30547, CVE-2021-30546, CVE-2021-30545, CVE-2021-30544, CVE-2021-30541, CVE-2021-30540, CVE-2021-30539, CVE-2021-30538, CVE-2021-30537, CVE-2021-30536, CVE-2021-30535, CVE-2021-30534, CVE-2021-30533, CVE-2021-30532, CVE-2021-30531, CVE-2021-30530, CVE-2021-30529, CVE-2021-30528, CVE-2021-30527, CVE-2021-30526, CVE-2021-30525, CVE-2021-30524, CVE-2021-30523, CVE-2021-30522, CVE-2021-30521, CVE-2021-30520, CVE-2021-30519, CVE-2021-30518, CVE-2021-30517, CVE-2021-30516, CVE-2021-30515, CVE-2021-30514, CVE-2021-30513, CVE-2021-30512, CVE-2021-30511, CVE-2021-30510, CVE-2021-30509, CVE-2021-30508, CVE-2021-30507, CVE-2021-30506, CVE-2021-21233, CVE-2021-21232, CVE-2021-21231, CVE-2021-21230, CVE-2021-21229, CVE-2021-21228, CVE-2021-21227, CVE-2021-21226, CVE-2021-21225, CVE-2021-21224, CVE-2021-21223, CVE-2021-21222, CVE-2021-21221, CVE-2021-21220, CVE-2021-21219, CVE-2021-21218, CVE-2021-21217, CVE-2021-21216, CVE-2021-21215, CVE-2021-21214, CVE-2021-21213, CVE-2021-21212, CVE-2021-21211, CVE-2021-21210, CVE-2021-21209, CVE-2021-21208, CVE-2021-21207, CVE-2021-21206, CVE-2021-21205, CVE-2021-21204, CVE-2021-21203, CVE-2021-21202, CVE-2021-21201, CVE-2021-21199, CVE-2021-21198, CVE-2021-21197, CVE-2021-21196, CVE-2021-21195, CVE-2021-21194, CVE-2021-21193, CVE-2021-21192, CVE-2021-21191, CVE-2021-21190, CVE-2021-21189, CVE-2021-21188, CVE-2021-21187, CVE-2021-21186, CVE-2021-21185, CVE-2021-21184, CVE-2021-21183, CVE-2021-21182, CVE-2021-21181, CVE-2021-21180, CVE-2021-21179, CVE-2021-21178, CVE-2021-21177, CVE-2021-21176, CVE-2021-21175, CVE-2021-21174, CVE-2021-21173, CVE-2021-21172, CVE-2021-21171, CVE-2021-21170, CVE-2021-21169, CVE-2021-21168, CVE-2021-21167, CVE-2021-21166, CVE-2021-21165, CVE-2021-21164, CVE-2021-21163, CVE-2021-21162, CVE-2021-21161, CVE-2021-21160, CVE-2021-21159, CVE-2021-21157, CVE-2021-21156, CVE-2021-21155, CVE-2021-21154, CVE-2021-21153, CVE-2021-21152, CVE-2021-21151, CVE-2021-21150, CVE-2021-21149, CVE-2021-21148, CVE-2021-21147, CVE-2021-21146, CVE-2021-21145, CVE-2021-21144, CVE-2021-21143, CVE-2021-21142, CVE-2021-21141, CVE-2021-21140, CVE-2021-21139, CVE-2021-21138, CVE-2021-21137, CVE-2021-21136, CVE-2021-21135, CVE-2021-21134, CVE-2021-21133, CVE-2021-21132, CVE-2021-21131, CVE-2021-21130, CVE-2021-21129, CVE-2021-21128, CVE-2021-21127, CVE-2021-21126, CVE-2021-21125, CVE-2021-21124, CVE-2021-21123, CVE-2021-21122, CVE-2021-21121, CVE-2021-21120, CVE-2021-21119, CVE-2021-21118, CVE-2021-21117, CVE-2021-21116, CVE-2021-21115, CVE-2021-21114, CVE-2021-21113, CVE-2021-21112, CVE-2021-21111, CVE-2021-21110, CVE-2021-21109, CVE-2021-21108, CVE-2021-21107, CVE-2021-21106, CVE-2020-27844, CVE-2020-16044, CVE-2020-16043, CVE-2020-16036, CVE-2020-16035, CVE-2020-16034, CVE-2020-16033, CVE-2020-16032, CVE-2020-16031, CVE-2020-16030, CVE-2020-16029, CVE-2020-16028, CVE-2020-16027, CVE-2020-16026, CVE-2020-16025, CVE-2020-16024, CVE-2020-16023, CVE-2020-16022, CVE-2020-16021, CVE-2020-16020, CVE-2020-16019, CVE-2020-16018, CVE-2020-16017, CVE-2020-16015, CVE-2020-16014, CVE-2020-16013, CVE-2020-16012, CVE-2020-15995, and CVE-2019-8075

- Fixed chromium-browser security issues:
  More...

  CVE-2022-2852, CVE-2022-2854, CVE-2022-2855, CVE-2022-2857, CVE-2022-2858, CVE-2022-2853, CVE-2022-2856, CVE-2022-2859, CVE-2022-2860, CVE-2022-2861, CVE-2022-2624, CVE-2022-2623, CVE-2022-2622, CVE-2022-2621, CVE-2022-2620, CVE-2022-2619, CVE-2022-2618, CVE-2022-2617, CVE-2022-2616, CVE-2022-2615, CVE-2022-2614, CVE-2022-2613, CVE-2022-2612, CVE-2022-2611, CVE-2022-2610, CVE-2022-2609, CVE-2022-2608, CVE-2022-2607, CVE-2022-2606, CVE-2022-2605, CVE-2022-2604, CVE-2022-2603, CVE-2022-2481, CVE-2022-2480, CVE-2022-2479, CVE-2022-2478, CVE-2022-2477, and CVE-2022-2163

- Updated **Chromium** browser to **version 104.0.5112.101**

Base System

- Fixed **curl** security issue CVE-2022-35252.
- Fixed **dbus** security issues CVE-2020-12049 and CVE-2020-35512.
- Fixed **nss** security issues CVE-2022-34480, CVE-2022-22747, CVE-2020-25648, CVE-2021-43527, CVE-2020-12403.
- Fixed **shadow** security issue CVE-2018-7169.
- Fixed **policykit-1** security issue CVE-2021-4034.
- Fixed **vim** security issues:
  More...

  CVE-2021-4069, CVE-2021-4019, CVE-2021-3984, CVE-2021-3928, CVE-2021-3927, CVE-2021-3903, CVE-2021-3796, CVE-2021-3778, and CVE-2019-20807
- Fixed **glib-networking** security issue CVE-2020-13645.
- Fixed **aspell** security issue CVE-2019-25051.
- Fixed **avahi** security issue CVE-2021-3468.
- Fixed **bind9** security issues:
  More...

  CVE-2021-25220, CVE-2021-25219, CVE-2021-25216, CVE-2021-25215, CVE-2021-25214, CVE-2020-8625, CVE-2020-8624, CVE-2020-8623, CVE-2020-8622, CVE-2020-8617, and CVE-2020-8616
- Fixed **brotli** security issue CVE-2020-8927.
- Fixed **libcaca** security issues CVE-2021-3410, CVE-2021-30499, and CVE-2021-30498.
- Fixed **libexif** security issues:
  More...

  CVE-2020-13114, CVE-2020-13113, CVE-2020-13112, CVE-2020-0452, CVE-2020-0198, CVE-2020-0182, and CVE-2020-0093
- Fixed **expat** security issues:
  More...

  CVE-2022-25315, CVE-2022-25314, CVE-2022-25313, CVE-2022-25236, CVE-2022-25235, CVE-2022-23990, CVE-2022-23852, CVE-2022-22827, CVE-2022-22826, CVE-2022-22825, CVE-2022-22824, CVE-2022-22823, CVE-2022-22822, CVE-2021-46143, and CVE-2021-45960
- Fixed **freetype** security issues CVE-2022-31782, CVE-2022-27406, CVE-2022-27405, CVE-2022-27404, and CVE-2020-15999.
- Fixed **libgd2** security issues CVE-2021-40145, CVE-2021-38115, and CVE-2017-6363.
- Fixed **glib2.0** security issue CVE-2021-3800.
- Fixed **ghostscript** security issues:
  More...

CVE-2021-45949, CVE-2021-45944, CVE-2020-8112, CVE-2020-6851, CVE-2020-27845, CVE-2020-27843, CVE-2020-27842, CVE-2020-27841, CVE-2020-27824, CVE-2020-27814, and CVE-2018-5727

- Fixed **krb5** security issue CVE-2020-28196.
- Fixed **nettle** security issues CVE-2021-3580, CVE-2021-20305, and CVE-2018-16869.
- Fixed **icu** security issue CVE-2020-21913.
- Fixed **webkit2gtk** security issues:
  More...

  CVE-2022-32816, CVE-2022-32792, CVE-2022-26710, CVE-2022-2294, CVE-2022-22677, CVE-2022-22662, CVE-2022-30294, CVE-2022-30293, CVE-2022-26719, CVE-2022-26717, CVE-2022-26716, CVE-2022-26709, CVE-2022-26700, CVE-2022-22620, CVE-2022-22592, CVE-2022-22590, CVE-2022-22589, CVE-2021-45483, CVE-2021-45482, CVE-2021-45481, CVE-2021-30984, CVE-2021-30954, CVE-2021-30953, CVE-2021-30952, CVE-2021-30951, CVE-2021-30936, CVE-2021-30934, CVE-2021-30897, CVE-2021-30890, CVE-2021-30889, CVE-2021-30888, CVE-2021-30887, CVE-2021-30884, CVE-2021-30836, CVE-2021-30823, CVE-2021-30818, CVE-2021-30809, CVE-2021-30858, CVE-2021-30799, CVE-2021-30797, CVE-2021-30795, CVE-2021-30758, CVE-2021-30749, CVE-2021-30744, CVE-2021-30734, CVE-2021-30720, CVE-2021-30689, CVE-2021-30665, CVE-2021-30663, CVE-2021-21779, CVE-2021-21775, CVE-2021-1871, CVE-2021-1870, CVE-2021-1844, CVE-2021-1801, CVE-2021-1799, CVE-2021-1789, CVE-2021-1788, CVE-2021-1765, CVE-2020-9983, CVE-2020-9952, CVE-2020-9951, CVE-2020-9948, CVE-2020-29623, CVE-2020-27918, CVE-2020-13753, CVE-2020-13558

- Fixed **json-c** security issue CVE-2020-12762.
- Fixed **bash** security issue CVE-2019-18276.
- Fixed **openldap** security issues:
  More...

  CVE-2022-29155, CVE-2021-27212, CVE-2020-36230, CVE-2020-36229, CVE-2020-36228, CVE-2020-36227, CVE-2020-36226, CVE-2020-36225, CVE-2020-36224, CVE-2020-36223, CVE-2020-36222, and CVE-2020-36221

- Fixed **ldb** security issues CVE-2021-20277 and CVE-2020-27840.
- Fixed **ldns** security issues CVE-2020-19861 and CVE-2020-19860.
- Fixed **lz4** security issue CVE-2021-3520.
- Fixed **p11-kit** security issues CVE-2020-29363, CVE-2020-29362, and CVE-2020-29361.
- Fixed **perl** security issues CVE-2020-12723, CVE-2020-10878 and CVE-2020-10543.
- Fixed **poppler** security issues CVE-2020-27778, CVE-2019-9959, CVE-2019-10871, and CVE-2018-21009.
- Fixed **libproxy** security issues CVE-2020-26154 and CVE-2020-25219.
- Fixed **python2.7** security issues:
  More...

  CVE-2015-20107, CVE-2022-0391, CVE-2021-4189, CVE-2021-3177, CVE-2020-26116, CVE-2019-9674, CVE-2019-20907, and CVE-2019-17514

- Fixed **python3.6** security issues:

More...

CVE-2015-20107, CVE-2022-0391, CVE-2021-4189, CVE-2021-3737, CVE-2021-3733, CVE-2021-3426, CVE-2021-3177, CVE-2020-27619, CVE-2020-26116, CVE-2020-14422, CVE-2019-9674, CVE-2019-20907, and CVE-2019-17514

- Fixed **qpdf** security issues CVE-2021-36978 and CVE-2018-18020.
- Fixed **qtbase-opensource-src** security issues CVE-2021-38593 and CVE-2020-17507.
- Fixed **qtsvg-opensource-src** security issues CVE-2021-45930, CVE-2021-3481, and CVE-2018-19869.
- Fixed **librsvg** security issue CVE-2019-20446.
- Fixed **cyrus-sasl2** security issue CVE-2022-24407.
- Fixed **samba** security issues:
  More...

  CVE-2021-44142, CVE-2021-3671, CVE-2021-20254, CVE-2020-25722, CVE-2020-25717, CVE-2020-14383, CVE-2020-14323, CVE-2020-14318, and CVE-2016-2124

- Fixed **speex** security issue CVE-2020-23903.
- Fixed **sqlite3** security issues CVE-2021-36690, CVE-2020-13632, CVE-2020-13630, CVE-2020-13434, and CVE-2018-8740.
- Fixed **libssh** security issue CVE-2020-16135.
- Fixed **openssl1.0** security issues:
  More...

  CVE-2022-2068, CVE-2022-1292, CVE-2022-0778, CVE-2021-3712, CVE-2021-23841, CVE-2021-23840, and CVE-2020-1971

- Fixed **openssl** security issues:
  More...

  CVE-2022-2097, CVE-2022-2068, CVE-2022-1292, CVE-2022-0778, CVE-2021-3712, CVE-2021-3711, CVE-2021-3449, CVE-2021-23841, CVE-2021-23840, and CVE-2020-1971

- Fixed **tiff** security issues:
  More...

  CVE-2022-0891, CVE-2022-0865, CVE-2022-0562, CVE-2022-0561, CVE-2020-35522, CVE-2020-35524, and CVE-2020-35523

- Fixed **libwebp** security issues:
  More...

  CVE-2020-36332, CVE-2020-36331, CVE-2020-36330, CVE-2020-36329, CVE-2020-36328, CVE-2018-25014, CVE-2018-25013, CVE-2018-25012, CVE-2018-25011, CVE-2018-25010, and CVE-2018-25009

- Fixed **libx11** security issues CVE-2021-31535, CVE-2020-14363, and CVE-2020-14344.
- Fixed **zlib** security issues CVE-2022-37434 and CVE-2018-25032.
- Fixed **dnsmasq** security issues:
  More...

CVE-2021-3448, CVE-2020-25687, CVE-2020-25686, CVE-2020-25685, CVE-2020-25684, CVE-2020-25683, CVE-2020-25682, CVE-2020-25681, and CVE-2019-14834

- Fixed **iproute2** security issue CVE-2019-20795.
- Fixed **isc-dhcp** security issue CVE-2021-25217.
- Fixed **ntp** security issue CVE-2019-8936.
- Fixed **openvpn** security issues CVE-2022-0547, CVE-2020-15078, and CVE-2020-11810.
- Fixed **python-cryptography** security issue CVE-2020-25659.
- Fixed **lxml** security issues CVE-2021-43818, CVE-2021-28957, and CVE-2020-27783.
- Fixed **paramiko** security issue CVE-2022-24302.
- Fixed **pillow** security issues:
  More...

  CVE-2022-22817, CVE-2022-22816, CVE-2022-22815, CVE-2021-34552, CVE-2021-28678, CVE-2021-28677, CVE-2021-28676, CVE-2021-28675, CVE-2021-27923, CVE-2021-27922, CVE-2021-27921, CVE-2021-2792, CVE-2021-25293, CVE-2021-25292, CVE-2021-25290, CVE-2021-25288, CVE-2021-25287, CVE-2021-23437, CVE-2020-35655, and CVE-2020-35653.

- Fixed **busybox** security issues:
  More...

  CVE-2021-42386, CVE-2021-42385, CVE-2021-42384, CVE-2021-42382, CVE-2021-42381, CVE-2021-42380, CVE-2021-42379, CVE-2021-42378, CVE-2021-42374, CVE-2021-423, CVE-2021-28831, and CVE-2018-1000500

- Fixed **util-linux** security issue CVE-2018-7738.
- Fixed **tar security** issues CVE-2021-20193, CVE-2019-9923, and CVE-2018-20482.
- Fixed **blueman** security issue CVE-2020-15238.
- Fixed **bluez** security issues CVE-2021-41229, CVE-2020-0556, and CVE-2017-1000250.
- Fixed **systemd** security issues CVE-2021-3997, CVE-2021-33910, and CVE-2020-13529.
- Fixed **util-linux** security issues CVE-2021-3996, CVE-2021-3995, and CVE-2018-7738.
- Fixed **udisks2** security issue CVE-2018-17336.
- Fixed **heimdal** security issue CVE-2021-3671.
- Fixed **curl** security issues:
  More...

  CVE-2022-30115, CVE-2022-27782, CVE-2022-27781, CVE-2022-27780, CVE-2022-27779, CVE-2022-27778, CVE-2022-27776, CVE-2022-27775, CVE-2022-27774, CVE-2022-22576, CVE-2021-22947, CVE-2021-22946, CVE-2021-22945, CVE-2021-22924, CVE-2021-22901, CVE-2021-22898, CVE-2021-22897, CVE-2021-22890, CVE-2021-22876, CVE-2020-8286, CVE-2020-8285, CVE-2020-8284, CVE-2020-8231, CVE-2020-8177, and CVE-2020-8169

- Fixed **libgcrypt20** security issues CVE-2021-40528, CVE-2021-33560 and CVE-2019-13627.
- Fixed **pulseaudio** security issue CVE-2020-16123.
- Fixed **libsdl2** security issue CVE-2019-13616.
- Fixed **libsndfile** security issue CVE-2021-3246.
- Fixed **libssh2** security issue CVE-2019-17498.
- Fixed **libvncserver** security issues:

More...

CVE-2020-14405, CVE-2020-14404, CVE-2020-14403, CVE-2020-14402, CVE-2020-14401, CVE-2020-14400, CVE-2020-14399, CVE-2020-14398, CVE-2020-14397, CVE-2020-14396, CVE-2019-20840, CVE-2019-20839, CVE-2019-15690, CVE-2019-15681, CVE-2018-7225, CVE-2018-6307, CVE-2018-21247, CVE-2018-20750, CVE-2018-20749, CVE-2018-20748, CVE-2018-20024, CVE-2018-20023, CVE-2018-20022, CVE-2018-20021, CVE-2018-20020, CVE-2018-20019, CVE-2018-15127, and CVE-2018-15126

- Fixed **wpa** security issues CVE-2021-0326 and CVE-2020-12695.
- Fixed **ntfs-3g** security issues:
  More...

  CVE-2022-30789, CVE-2022-30788, CVE-2022-30787, CVE-2022-30786, CVE-2022-30785, CVE-2022-30784, CVE-2022-30783, CVE-2021-46790, CVE-2021-39263, CVE-2021-39262, CVE-2021-39261, CVE-2021-39260, CVE-2021-39259, CVE-2021-39258, CVE-2021-39257, CVE-2021-39256, CVE-2021-39255, CVE-2021-39254, CVE-2021-39253, CVE-2021-39252, CVE-2021-39251, CVE-2021-35269, CVE-2021-35268, CVE-2021-35267, CVE-2021-35266, CVE-2021-33289, CVE-2021-33287, CVE-2021-33286, and CVE-2021-33285
- Fixed **unzip** security issues CVE-2022-0530, CVE-2022-0529, and CVE-2019-13232.
- Fixed **libx11** security issues CVE-2021-31535, CVE-2020-14344, CVE-2018-14600, CVE-2018-14599, and CVE-2018-14598.
- Fixed **x11vnc** security issue CVE-2020-29074.
- Fixed **xorg-server** security issues CVE-2021-4011, CVE-2021-4010, CVE-2021-4009, CVE-2021-4008, and CVE-2021-3472.
- Fixed **xterm** security issue CVE-2021-27135.
- Fixed **elfutils** security issues:
  More...

  CVE-2019-7665, CVE-2019-7664, CVE-2019-7150, CVE-2019-7149, CVE-2019-7148, CVE-2019-7146, CVE-2018-18521, CVE-2018-18520, CVE-2018-18310, CVE-2018-16403, CVE-2018-16402, and CVE-2018-16062.
- Fixed **fribidi** security issues CVE-2022-25310, CVE-2022-25309, and CVE-2022-25308.
- Fixed **xz-utils** security issue CVE-2022-1271.
- Fixed **openssh** security issues CVE-2021-41617, CVE-2021-28041, CVE-2019-6111, CVE-2019-6109, CVE-2018-20685, and CVE-2018-15473.
- Fixed **tcpdump** security issues CVE-2020-8037 and CVE-2018-16301.
- Fixed **gettext** security issue CVE-2018-18751.
- Fixed **gzip** security issue CVE-2022-1271.
- Fixed **gst-plugins-good1.0** security issues CVE-2021-3498 and CVE-2021-3497.
- Fixed **openjpeg2** security issues:
  More...

  CVE-2018-6616, CVE-2018-5785, CVE-2018-5727, CVE-2018-21010, CVE-2018-20847, CVE-2018-18088, CVE-2018-14423 and CVE-2017-17480
- Fixed **nfs-utils** security issue CVE-2019-3689.
- Fixed **expat** security issues:

More...

CVE-2022-25315, CVE-2022-25314, CVE-2022-25313, CVE-2022-25236, CVE-2022-25235, CVE-2022-23990, CVE-2022-23852, CVE-2022-22827, CVE-2022-22826, CVE-2022-22825, CVE-2022-22824, CVE-2022-22823, CVE-2022-22822, CVE-2021-46143, CVE-2021-45960, CVE-2019-15903, CVE-2018-20843, and CVE-2013-0340

- Fixed **flac** security issues CVE-2021-0561, CVE-2020-0499, and CVE-2017-6888.
- Fixed **taglib** security issue CVE-2018-11439.
- Fixed **libvorbis** security issues CVE-2018-5146, CVE-2018-10393, CVE-2018-10392, CVE-2017-14633, CVE-2017-14632, and CVE-2017-14160.
- Fixed **wavpack** security issues:
  More...

  CVE-2021-44269, CVE-2020-35738, CVE-2019-11498, CVE-2019-1010319, CVE-2019-1010317, CVE-2018-7254, CVE-2018-7253, CVE-2018-6767, CVE-2018-19841, CVE-2018-19840, CVE-2018-10540, CVE-2018-10539, CVE-2018-10538, CVE-2018-10537, and CVE-2018-10536.

- Fixed **libxml2** security issues:
  More...

  CVE-2022-29824, CVE-2022-23308, CVE-2021-3541, CVE-2021-3537, CVE-2021-3518, CVE-2021-3517, CVE-2021-3516, CVE-2020-7595, CVE-2020-24977, CVE-2019-20388, CVE-2019-19956, CVE-2018-9251, CVE-2018-14567, CVE-2018-14404, CVE-2017-18258, CVE-2017-16932, CVE-2016-9318, and CVE-2017-8872

- Fixed **cifs-utils** security issues CVE-2022-29869, CVE-2022-27239, CVE-2021-20208, and CVE-2020-14342.
- Fixed **libinput** security issue CVE-2020-1215.
- Fixed **network-manager** security issue CVE-2021-20297.
- Fixed **ghostscript** security issue CVE-2019-25059.
- Fixed **libsdl1.2** security issue CVE-2021-33657.
- Fixed **libsepol** security issues CVE-2021-36087, CVE-2021-36086, CVE-2021-36085, and CVE-2021-36084.
- Fixed **dnsmasq** security issue CVE-2022-0934.
- Fixed **pcre3** security issues CVE-2020-14155 and CVE-2019-20838.
- Fixed **cups** security issues CVE-2022-26691, CVE-2020-10001, and CVE-2019-8842.
- Fixed **libtirpc** security issue CVE-2021-46828.
- Fixed **gnutls28** security issues CVE-2022-2509 and CVE-2021-4209.
- Fixed **net-snmp** security issues:
  More...

  CVE-2022-24810, CVE-2022-24809, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806, CVE-2022-24805, and CVE-2022-248

- Fixed **zulu8-ca** security issues CVE-2022-34169, CVE-2022-25647, CVE-2022-21541, and CVE-2022-21540.

Known Issues IGEL OS(RPI4) 11.02.110

Citrix

- **Adding smartcard readers while the session is ongoing** does not work. The reader is visible, but cannot be used due to permanently unknown reader status.
- Citrix Workspace Hub **CitrixCasting** is **limited to 1920x1200 FullHD** resolution.
- **Limitations** while running Citrix sessions **with hardware accelerated H.264 codec**:
  - Notifications are not visible.
  - UMS enhanced messages are not visible.
  - In-Session or Citrix toolbar is not visible.
  - Window switching between local windows is not possible.
  - The maximum supported resolution is 2 x 1920x1200 FullHD. There are display corruptions with higher resolutions.
  - Rotated screens are not supported.
  - Seamless Windows are not supported.
  - The Citrix session is not visible via Shadowing.
  - **Workaround**: Disable hardware accelerated H.264 codec:

IGEL Setup	**Sessions > Citrix > Citrix Global > Codec**
Parameter	Accelerated H.264 Deep Compression Codec
Registry	`ica.hw-accelerated-h264-codec`
Value	enabled / disabled

  - Citrix **Kerberos passthrough authentication** is not supported.
  - **Citrix Multimedia Redirection** does not work reliably.

Network

- **Wake on Lan** is currently not supported on this platform.

Chromium

- If watching a Live stream, there is a **memory leak in Chromium so the session will freeze** at some point.
- If **a startup page** is **set while Chromium Browser is running**, it **will not be applied**. In that case, a **reboot** is **required**.

X11 System

- It is **not possible to hotplug monitors while system is running**. Monitors must be already connected before turning on the device.

Audio

- **HDMI audio output** is only supported **on 1st HDMI connector**.

New Features IGEL OS(RPI4) 11.02.110

Chromium

- Added "**Block third-party cookies**" as a parameter in the registry, see Privacy(see page 137).

IGEL Setup	**Sessions > Chromium Browser > Chromium Browser Global > Privacy**
Parameter	Block third party cookies
Registry	`chromiumglobal.app.block_third_party_cookies`
Type	bool
Value	enabled / disabled

Network

- Updated **NetworkManager** to version **1.32.12**

Smartcard

- Updated **Resource Manager PC/SC Lite** to version **1.9.8-1igel1655196158**

Base System

- Added support for custom bootsplash configurable at **IGEL Setup > System > Firmware Customization > Corporate Design > Custom Bootsplash**.
- **Post-session command**: Added **multi-session support**. It is now possible to define additional session types which will all be covered by the post-session command mechanism.
- Updated **kernel** to version **5.15.56**.
- Added **ZRAM swap**.
- Updated **IGEL EULA** to version of **1st July 2022**.
- Changed **Auto Update** feature configuration at registry `update.service.**` .
  The **Auto Update feature** is **enabled by default when the device is evaluated and has no IGEL Workspace license installed**. See IGEL OS(RPI4) Automatic Update Service for Device Evaluation(see page 40).

Parameter	Enable automatic update service
Registry	`update.service.enable`
Range	[During evaluation only] [On] [Off]

- Updated **OpenSSH** to version **9.0p1-1**

- Updated **Bluetooth Stack (bluez)** to version **5.64-0**
- Updated **Mesa OpenGL** to version **22.1.5**
- Updated **XFCE4 Window Manager** to version **4.14.5**
- Updated **WebKit2Gtk** to version **2.36.6-1**
- Updated **Zulu JRE** to version **8.0.345-1**
- Updated **Mobile Device Access libraries**:
  - **libmtp9** to version **1.1.20-1**
  - **libimobiledevice6** to version **1.3.0-6**
  - **libgphoto2** to version **2.5.29**

X Server

- Updated **X server** to version **21.1.3**

Audio

- Updated sound preferences dialog to current version.

Multimedia

- Updated **omxplayer** to version **20190723+gitf543a0d-1+bullseye**
- Updated **ffmpeg multimedia library** to version **4.3.4-0+deb11u1+rpt3.**
- Updated **GStreamer 1.x** to version **1.20.3**

TC Setup (Java)

- Updated **TC Setup** to version **6.10.3**.

Resolved Issues IGEL OS(RPI4) 11.02.110

Citrix

- Improved **dialog for Citrix farm selection**.
- Fixed **Connection Center** showing wrong entries.
- Improved **Workspace Hub** session **startup**
- The **NSAP virtual channel** is **loaded correctl**y and works as expected.

Chromium

- Fixed a bug where **browser certificates** were **lost after reboot** if the UMS was not reachable.
- Fixed bug where Chromium browser was **not clearing browsing history properly**.
- Fixed a bug for Chromium settings where **parent settings did not influence the child settings**.
- Removed option **On Startup->Continue where you left off** for Chromium sessions. This feature only works globally.
- '**Automatic browser restart on exit**' no longer needs a reboot to be deactivated.

Base System

- Fixed issue with **update fails if bandwidth to update server is low**.
- Fixed issue with **time** is **not set before starter license is issued if NTP time server was configured in Setup Assistant**.

Window Manager

- **Desktop Icon Font Color** will **now** be **previewed correctly** in the setup.

Misc

- Fixed a bug **in system messages** where **lines were cut off**.

Notes for Release 11.01.120

Software:	IGEL OS(RPI4) Version	11.01.120
Release Date:	2021-07-14	
Release Notes:	Version	RN-1101120-1
Last update:	2021-07-14	

Supported Devices 11.01.120

- UC3-RPI4 NComputing RX420/RX440

Component Versions 11.01.120

Clients

Product	**Version**
Chromium (experimental)	86.0.4240.197-rpt1
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace App	21.04.0.11
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2

Dictation

Philips Speech driver	12.9.2

Smartcard

PKCS#11 Library OpenSC	0.20.0-3igel37
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14

System Components

OpenSSL	1.0.2n-1ubuntu5.4
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth Stack (bluez)	5.52-1igel6
MESA OpenGL Stack	20.2.3-1igel128

VDPAU Library Version	1.4-1igel1003
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-1igel1011
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.9.3-v8~IGEL #1
Xorg X11 Server	1.20.8-2igel1055
CUPS Printing Daemon	2.2.7-1ubuntu2.8igel32
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel12
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.18.0-1ubuntu5igel92
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.18.1-1igel272
WebKit2Gtk	2.28.4-0ubuntu0.18.04.1
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-3igel5

Services

Service Partitions	**Size**	**Services**
Java SE Runtime Environment	129.5M	Java SE Runtime Environment
Citrix ICA	89.2M	Citrix Workspace app Citrix StoreFront Citrix Workspace Hub

Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	2.8M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration
Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	127.5M	Local Browser (Chromium)
Limited Support Features	256.0K	Mobile Device Access USB (Limited support) Limited Support Features
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

Security Fixes 11.01.120

Base system

- Fixed **user logoff** when the device is switched into **system suspend**.

Known Issues 11.01.120

Citrix

- **Adding smartcard readers** while the session is ongoing does not work. The reader is visible, but cannot be used due to permanently unknown reader status.
- **Citrix Workspace Hub** CitrixCasting is **limited to 1920x1200** FullHD resolution.
- **Limitations** while running Citrix sessions **with** hardware-accelerated **H.264 codec**:
  - Notifications are not visible.
  - UMS enhanced messages are not visible.
  - In-session or Citrix toolbar is not visible.
  - Window switching between local windows is not possible.
  - The maximum supported resolution is 2 x 1920x1200 FullHD. There are display corruptions with higher resolutions.
  - Rotated screens are not supported.
  - Seamless windows are not supported.
  - The Citrix session is not visible via shadowing.
- Workaround: **Disable hardware-accelerated H.264 codec**:

IGEL Setup	**Sessions > Citrix > Citrix Global > Codec**
Parameter	Accelerated H.264 Deep Compression Codec
Registry	`ica.hw-accelerated-h264-codec`
Value	enabled / disabled

- Citrix **Kerberos passthrough authentication** is not supported.

Network

- Wake on LAN is currently not supported on this platform.

Base system

- **Custom bootsplash** configuration is not supported.

X11 system

- It is not possible to **hotplug monitors while the system is running**. Monitors must be already connected before turning on the device.

New Features 11.01.120

Citrix

- Integrated **Citrix Workspace app 21.04**. Available versions: 20.06, 20.10, 21.04 (default)
- Improvements:
  - Faster startup of **ctxusbd**
  - More options with **ctxlogd** (`ica.logging.setlog.level.**`)
  - **Paste screencopy** into Citrix session
- New registry keys:
  - Added a registry key for enabling **screen pinning or multimonitor support** with native Workspace app.
    More...

Parameter	Enhanced experience for multimonitor scenario
Registry	`ica.authman.screenpinenabled`
Value	on / off

  - Added a registry key to enable **DNS cache**.
    More...

Parameter	Enable DNS Cache
Registry	`ica.authman.dnscacheenabled`
Value	on / off

- Fixed Issue: **mic** and **webcam** devices can be **redirected** using **Browser Content Redirection**.
  More...

Parameter	Enables mic and webcam redirection using BCR
Registry	`ica.allregions.cefenablemediadevices`
Value	[Factory default is "**"] [False] [True]

Resolved Issues 11.01.120

Citrix

- Fixed **Connection Center** showing wrong entries.
- The **NSAP virtual channel** is loaded correctly and works as expected.

Base system

- Fixed **post-session commands**.

Remote Management

- Bug fix related to **viewing asset information on UMS**.
  Please note the Asset Inventory Tracker requires a valid license from the IGEL Enterprise Management Pack (EMP). For more information, please check the IGEL Knowledge Base page: View Asset Information.

Notes for Release 11.01.111

Software:	IGEL OS(RPI4) Version	11.01.111
Release Date:	2021-04-08	
Release Notes:	Version	RN-1101111-1
Last update:	2021-04-08	

Supported Devices 11.01.111

- UC3-RPI4 NComputing RX420/RX440

Component Versions 11.01.111

Clients

Product	**Version**
Chromium (experimental)	86.0.4240.197-rpt1
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2

Dictation

Philips Speech driver	12.9.2

Smartcard

PKCS#11 Library OpenSC	0.20.0-3igel37
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14

System Components

OpenSSL	1.0.2n-1ubuntu5.4
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth Stack (bluez)	5.52-1igel6
MESA OpenGL Stack	20.2.3-1igel128
VDPAU Library Version	1.4-1igel1003

Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-1igel1011
Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.9.3-v8~IGEL #1
Xorg X11 Server	1.20.8-2igel1055
CUPS Printing Daemon	2.2.7-1ubuntu2.8igel32
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel12
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.18.0-1ubuntu5igel92
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.18.1-1igel272
WebKit2Gtk	2.28.4-0ubuntu0.18.04.1
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-3igel5

Services

Service Partitions	**Size**	**Services**
Java SE Runtime Environment	129.5M	Java SE Runtime Environment
Citrix ICA	59.2M	Citrix Workspace Hub Citrix Workspace app Citrix StoreFront

Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	2.8M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration
Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	127.5M	Local Browser (Chromium)
Limited Support Features	256.0K	Limited Support Features Mobile Device Access USB (Limited support)
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

Known Issues 11.01.111

Citrix

- **Adding smartcard readers** while the session is ongoing does not work. The reader is visible, but cannot be used due to permanently unknown reader status.
- **Citrix Workspace Hub** CitrixCasting is **limited to 1920x1200** FullHD resolution.
- **Limitations** while running Citrix sessions **with** hardware-accelerated **H.264 codec**:
  - Notifications are not visible.
  - UMS enhanced messages are not visible.
  - In-session or Citrix toolbar is not visible.
  - Window switching between local windows is not possible.
  - The maximum supported resolution is 2 x 1920x1200 FullHD. There are display corruptions with higher resolutions.
  - Rotated screens are not supported.
  - The Citrix session is not visible via shadowing.
- Workaround: **Disable hardware-accelerated H.264 codec**:

IGEL Setup	**Sessions > Citrix > Citrix Global > Codec**
Parameter	Accelerated H.264 Deep Compression Codec
Registry	`ica.hw-accelerated-h264-codec`
Value	enabled / disabled

- Citrix **Kerberos passthrough authentication** is not supported.

Network

- Wake on Lan is currently not supported on this platform.

Base system

- **Custom bootsplash** configuration is not supported.
- **Post-session commands** are not supported in this release.

X11 system

- It is not possible to **hotplug monitors while the system is running**. Monitors must be already connected before turning on the device.

New Features 11.01.111

Chromium

- Added "**Block third party cookies"** as a parameter **in the registry**.

Base system

- Added support for the **NComputing RX440(IGEL)** device.

Driver

- Added **Philips Speech driver 12.9.2 for dictation** via Citrix.
  More...

Setup	**Sessions > Citrix > Citrix Global >Mapping > Device Support**
Parameter	Philips speech channel for dictation
Registry	`ica.module.virtualdriver.philipsspeech.enable`
Value	false / true

Setup	**Sessions > Citrix > Citrix Global >Mapping > Device Support**
Parameter	DPM server drive
Registry	`devices.philipsspeech.dpm_drive`
Value	p (default)

Setup	**Sessions > Citrix > Citrix Global >Mapping > Device Support**
Parameter	SpeechAir server drive
Registry	`devices.philipsspeech.speechair_drive`
Value	S (default)

Resolved Issues 11.01.111

Chromium

- Fixed a bug where **browser certificates were lost after reboot if UMS was not reachable**
- Fixed bug where Chromium browser was **not clearing browsing history properly**
- Fixed a bug for Chromium settings where **parent settings did not influence the child settings**

Misc

- Fixed a bug in **system messages where lines were cut off**

Notes for Release 11.01.110

Software:	IGEL OS(RPI4) Version	11.01.110
Release Date:	2021-02-18	
Release Notes:	Version	RN-1101110-1
Last update:	2021-02-24	

Supported Devices 11.01.110

- NComputing RX420 (UC3-RPI4)

Component Versions 11.01.110

Clients

Product	Version
Chromium	86.0.4240.197-rpt1
Citrix Workspace App	20.06.0.15
Citrix Workspace App	20.10.0.6
Citrix Workspace Hub	19.11.100.297
Open VPN	2.4.4-2ubuntu1.3
Zulu JRE	8.48.0.51-2

Smartcard

PKCS#11 Library OpenSC	0.20.0-3igel37
Reader Driver ACS CCID	1.1.6-1igel2
Reader Driver MUSCLE CCID	1.4.31-1igel10
Reader Driver REINER SCT cyberJack	3.99.5final.sp13igel15
Resource Manager PC/SC Lite	1.8.26-3igel14

System Components

OpenSSL	1.0.2n-1ubuntu5.4
OpenSSL	1.1.1-1ubuntu2.1~18.04.6
OpenSSH Client	7.6p1-4ubuntu0.3
OpenSSH Server	7.6p1-4ubuntu0.3
Bluetooth Stack (bluez)	5.52-1igel6
MESA OpenGL Stack	20.2.3-1igel128
VDPAU Library Version	1.4-1igel1003
Graphics Driver FBDEV	0.5.0-1igel1012
Graphics Driver VESA	2.4.0-1igel1010
Input Driver Evdev	2.10.6-1igel1011

Input Driver Synaptics	1.9.1-1ubuntu1igel1009
Input Driver Wacom	0.36.1-0ubuntu2igel1017
Kernel	Linux version 5.9.3-v8~IGEL #1
Xorg X11 Server	1.20.8-2igel1055
CUPS Printing Daemon	2.2.7-1ubuntu2.8igel32
Lightdm Graphical Login Manager	1.26.0-0ubuntu1igel12
XFCE4 Window Manager	4.14.2-1~18.04igel1595331607
ISC DHCP Client	4.3.5-3ubuntu7.1
NetworkManager	1.18.0-1ubuntu5igel92
ModemManager	1.10.0-1~ubuntu18.04.2
GStreamer 1.x	1.18.1-1igel272
WebKit2Gtk	2.28.4-0ubuntu0.18.04.1
Python2	2.7.17
Python3	3.6.9

Features with Limited IGEL Support

Mobile Device Access USB (MTP)	1.1.17-3igel5
Mobile Device Access USB (imobile)	1.2.1~git20191129.9f79242-1+b1igel8
Mobile Device Access USB (gphoto)	2.5.25-3igel5

Services

Service Partitions	**Size**	**Services**
Java SE Runtime Environment	129.5M	Java SE Runtime Environment
Citrix ICA	59.2M	Citrix Workspace Hub Citrix Workspace app Citrix StoreFront
Internet Printing Protocol (CUPS)	21.8M	Printing (Internet printing protocol CUPS)
Multimedia Codecs	2.8M	Multimedia Codecs
Hardware Video Acceleration	256.0K	Hardware Video Acceleration

Extra Fonts	1.0M	Extra Font Package
Local browser (Chromium)	127.5M	Local Browser (Chromium)
Limited Support Features	256.0K	Limited Support Features Mobile Device Access USB (Limited support)
Mobile Device Access USB	512.0K	Mobile Device Access USB (Limited support)

Known Issues 11.01.110

Citrix

- **Adding smartcard readers during the session** does not work. The reader is visible, but cannot be used due to permanently unknown reader status.
- **Kerberos passthrough authentication** is not supported.
- **Citrix Workspace Hub** CitrixCasting is **limited to 1920x1200** FullHD resolution.
- **Limitations** while running Citrix sessions **with enabled hardware acceleration** (H.264):
  - Notifications are not visible.
  - UMS enhanced messages are not visible.
  - In-session or Citrix toolbar is not visible.
  - Toggle between local windows is not possible.
  - The maximum supported resolution is 2 x 1920x1200 FullHD. There are display corruptions with higher resolutions.
  - Rotated screens are not supported.
  - The Citrix session is not visible via shadowing.
- Workaround: **Disable hardware-accelerated H.264 codec**:

IGEL Setup	**Sessions > Citrix > Citrix Global > Codec**
Parameter	Accelerated H.264 Deep Compression Codec
Registry	`ica.hw-accelerated-h264-codec`
Value	enabled / disabled

Base system

- **Custom bootsplash** configuration is not supported.

X11 system

- It is not possible to **hotplug monitors while the system is running**. Monitors must be already connected when boot.

Network

- Wake on Lan is currently not supported on this platform.

New Features 11.01.110

Hardware

- Added support for **Raspberry Pi revision 1.4**
- Reworked **naming for audio outputs**

Citrix

- Integrated **Citrix Workspace Hub 19.11** and **WSH Chrome 0.0.3**
- Added option to **enable Workspace Hub**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	Citrix Workspace Hub (Beta)
Registry	`ica.workspacehub.enable`
Value	disabled / enabled

- Added **a "friendly name" configuration** for the Workspace Hub device. The **empty string** as a default will be **replaced by the hostname** of the device:

Parameter	Friendly name for Workspace Hub device
Registry	`ica.workspacehub.friendlyname`
Value	(empty string, default)

- Added **autostart** of **WSH Chrome Launcher**. If enabled, using TC Setup Workspace Hub is also activated.

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	Autostart Citrix Workspace Hub Launcher
Registry	`sessions.workspacehub0.autostart`
Value	disabled / enabled

- Added **default launcher page URL**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	URL for default launcher page
Registry	`sessions.workspacehub0.launcher.page1.url`
Value	Default launcher page/"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Added **flag to activate a QR code** at the launcher page/s:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	Display QR code

Registry	`sessions.workspacehub0.launcher.page1.qrcode`
Value	enabled / disabled

- Added hint to **size the QR code**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	QR code size
Registry	`sessions.workspacehub0.launcher.page1.qrcodesize`
Value	small / medium / large

- Added hint to **position the QR code**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	QR code position
Registry	`sessions.workspacehub0.launcher.page1.qrcodeposition`
Value	top left / top right / bottom left / bottom right / center

- Added **URL** for a **second launcher page**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	URL for a second launcher page
Registry	`sessions.workspacehub0.launcher.page2.url`
Value	Disabled /Default launcher page/"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Added URL for a **third launcher page**:

IGEL Setup	**Sessions > Citrix > Citrix Workspace Hub > Options**
Parameter	URL for a third launcher page
Registry	`sessions.workspacehub0.launcher.page3.url`
Value	Disabled/Default launcher page/"https://myworkprod0.cloud.com"/"https://www.igel.com"/"Enter url here..."

- Integrated **Citrix Workspace app 20.10**
  The performance of the Citrix Workspace app was improved and a more detailed logging was implemented.
- New feature added with this release: **multiple audio devices could be mapped** inside the sessions.

Parameter	Multiple Audio Device support

Registry	`ica.module.vdcamversion4support`
Value	disabled / enabled

- Integrated **centralized Citrix logging** in IGEL OS, so only one parameter is needed to activate logging.

Parameter	Enable logging for Citrix sessions
Registry	`ica.logging.debug`
Value	off / on

- Since Workspace app 20.09, the tool **setlog** is **used to configure the logging**.
  For this purpose, parameters are provided in the registry **ica.logging.setlog**, but usually nothing needs to be changed.
- Added automatic configuration of the **Citrix webcam redirection in ICA** sessions.

IGEL Setup	**Sessions > Citrix > Citrix Global > HDX Multimedia**
Parameter	Automatic HDX webcam configuration
Registry	`ica.igel_hdxwebcam.enabled`
Value	disabled / enabled
Parameter	Resolution grade
Registry	`ica.igel_hdxwebcam.quality`
Range	[Very low] [Low] [Normal] [High] [Very high] [Best]
Parameter	Minimal frame rate
Registry	`ica.igel_hdxwebcam.framerate`
Value	20

- Added configuration for **H264 encoding in the Citrix webcam redirection**:

Parameter	HDX Webcam H264 encoding
Registry	`ica.wfclient.hdxh264inputenabled`
Value	disabled / enabled

- Added configuration for **native H264 encoding provided by webcam** and used in the Citrix webcam redirection. This parameter **requires** the **ica.wfclient.hdxh264inputenabled** to be set to "**true**".

Parameter	HDX Webcam H264 native
Registry	`ica.wfclient.hdxh264enablenative`
Value	disabled / enabled

Chromium

- Updated **Chromium** to version **86.0.4240.197-rpt1**. **Hardware-accelerated video decoding** is **disabled by defaul**t now.

Firmware update

- Added support for the **IGEL automatic update service**.

Registry	`update.service.enable`
Value	enabled / disabled

Boot

- Boot mode selection during power on:
  - Hold **power button** for '**Emergency boot (setup only)**'
  - Press hotkey '**Ctrl + Space**' for '**Reset to defaults**'
  - Press hotkey '**Ctrl + V**' for '**Verbose boot**'

Resolved Issues 11.01.110

Citrix

- On Citrix sessions with **H.264 HW-Acceleration** (default), **TransparentKeypassThrough=Remote** at `AllRegions.ini` is enabled to ensure **all window manager keypress events are directed** to the Citrix session.
- Added new parameter **AckDelayThresh**: Max time (in milliseconds) between sending "resource free" message if any resources free. Default=350

Parameter	AckDelayThresh
Registry	`ica.module.AckDelayThresh`
Type	Integer
Value	350

- Added new parameter **AudioBufferSizeMilliseconds**: Audio buffer size, in ms. Default=200 ms

Parameter	AudioBufferSizeMilliseconds
Registry	`ica.module.AudioBufferSizeMilliseconds`
Type	Integer
Value	200

- Added new parameter **AudioLatencyControlEnabled**: Enables latency control. Default=False

Parameter	AudioLatencyControlEnabled
Registry	`ica.module.AudioLatencyControlEnabled`
Type	Boolean
Value	false / true

- Added new parameter **AudioMaxLatency**: Sets the maximum latency (in ms) before trying to discard audio data. Default=300 ms

Parameter	AudioMaxLatency
Registry	`ica.module.AudioMaxLatency`
Type	Integer
Value	300

- Added new parameter **AudioLatencyCorrectionInterval**: Defines how often to correct the latency (in ms). Default=300 ms

Parameter	AudioLatencyCorrectionInterval
Registry	`ica.module.AudioLatencyCorrectionInterval`
Type	Integer

Value	300

- Added new parameter **AudioTempLatencyBoost**: Sets the higher latency band (in ms) above the lower **PlaybackDelayThresh** band. Default=300 ms

Parameter	AudioTempLatencyBoost
Registry	`ica.module.AudioTempLatencyBoost`
Type	Integer
Value	300

- Added new parameter **CommandAckThresh**: Number of free client command buffers causing a "resource free" message to be sent to the server. Default=10

Parameter	CommandAckThresh
Registry	`ica.module.CommandAckThresh`
Type	Integer
Value	10

- Added new parameter **DataAckThresh**: Number of free client data buffers causing a "resource free" message to be sent to the server. Default=10

Parameter	DataAckThresh
Registry	`ica.module.DataAckThresh`
Type	Integer
Value	10

- Added new parameter **MaxDataBufferSize**: Maximum size of each data buffer. Default=2048 bytes

Parameter	MaxDataBufferSize
Registry	`ica.module.MaxDataBufferSize`
Type	Integer
Value	2048

- Added new parameter **NumCommandBuffers**: Number of client buffers to use for audio commands. Default=64

Parameter	NumCommandBuffers
Registry	`ica.module.NumCommandBuffers`
Type	Integer
Value	64

- Added new parameter **PlaybackDelayThresh**: Delay (in ms) between being asked to start audio playback and actually starting audio playback in order to build up a backlog of sound. Default=150

Parameter	PlaybackDelayThresh
Registry	`ica.module.PlaybackDelayThresh`
Type	Integer
Value	150