



Citrix Workspace App

- [Getting Started with the Citrix Workspace App on IGEL OS \(see page 3\)](#)
- [Configuration of the Citrix Workspace App on IGEL OS \(see page 6\)](#)

Getting Started with the Citrix Workspace App on IGEL OS

Apps that Are Installed with the Citrix Workspace App

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

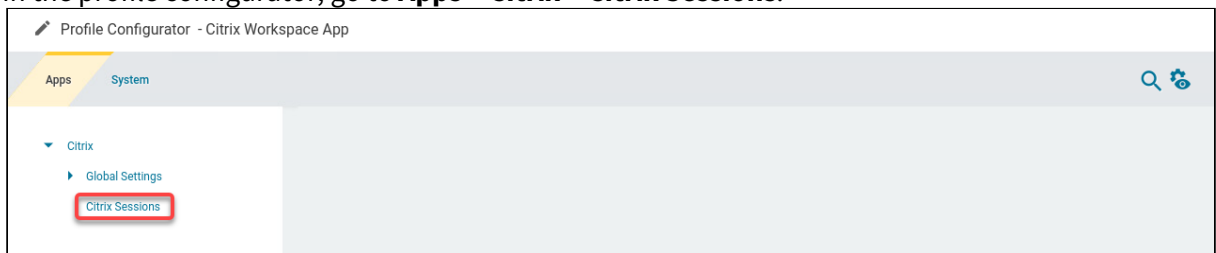
- Citrix Multimedia Codec

App Functionality and Setup

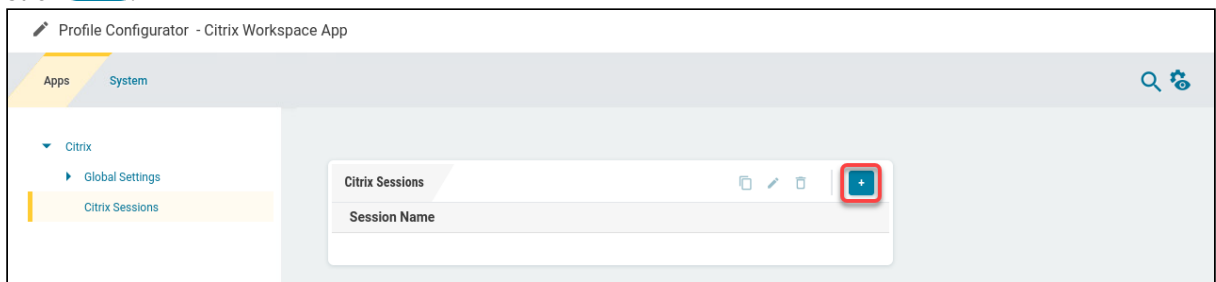
The functionality between IGEL OS 11 and IGEL OS 12 has changed fundamentally. While in IGEL OS 11 only one Storefront and SelfService session can be created, in IGEL OS 12 it is possible to create multiple sessions.

How to Create a Session

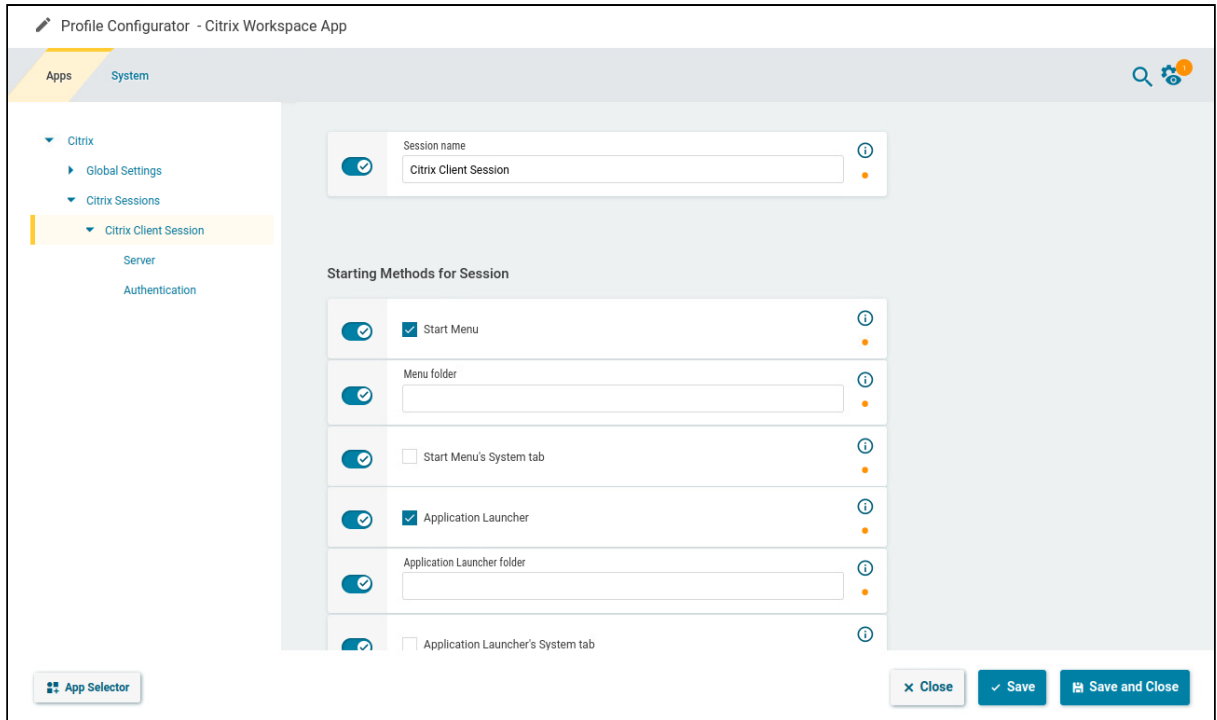
1. In the profile configurator, go to **Apps > Citrix > Citrix Sessions**.



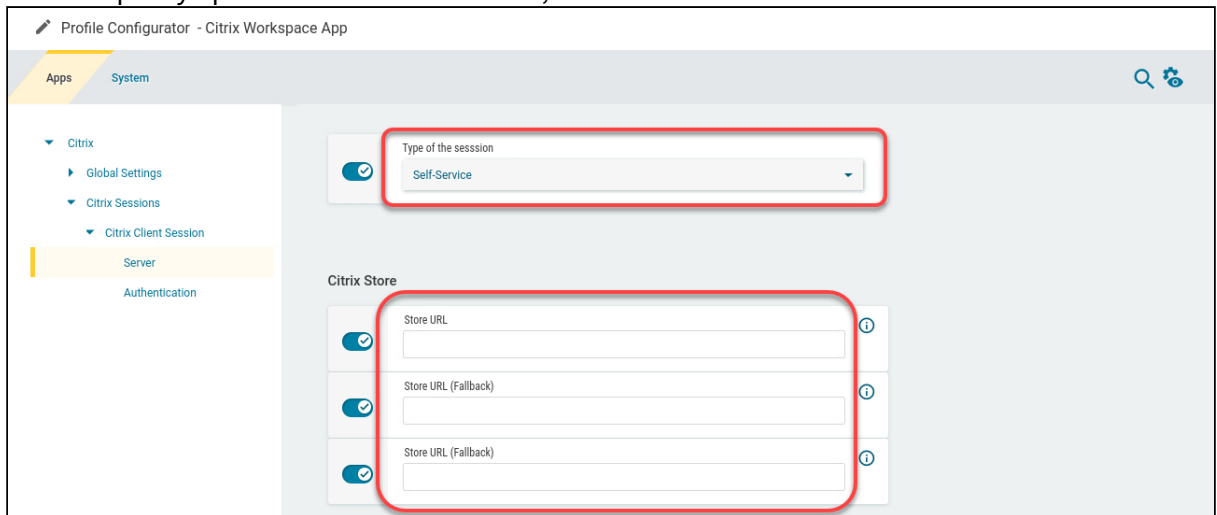
2. Click .



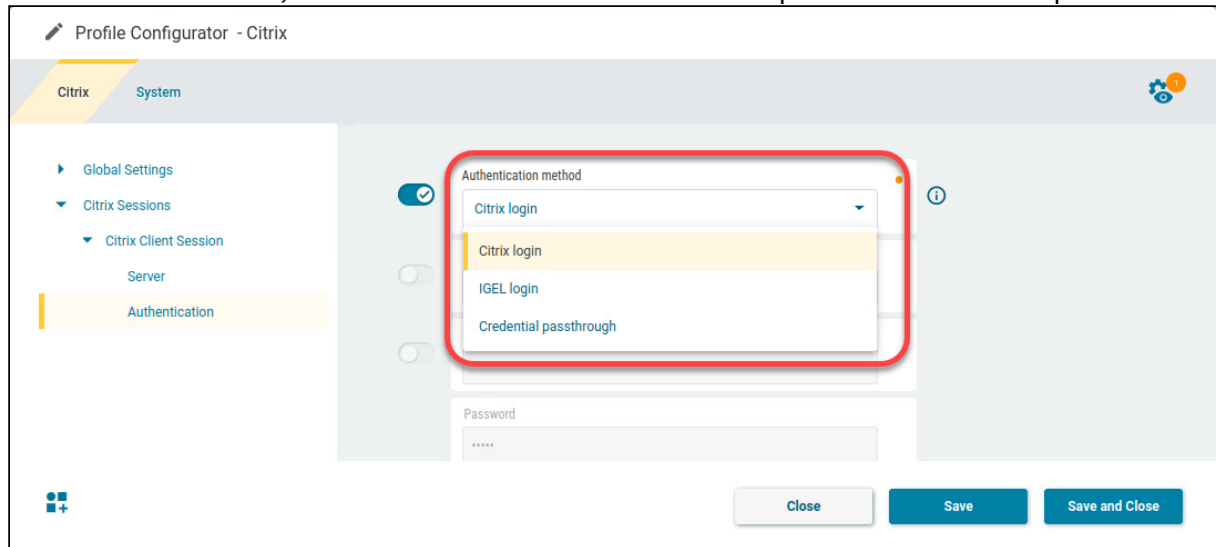
The session is created.



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



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



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

Smartcard Authentication for Citrix Sessions in IGEL OS 12

If the server offers smartcard authentication, it will be automatically used. No settings need to be made on the client side.

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

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

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

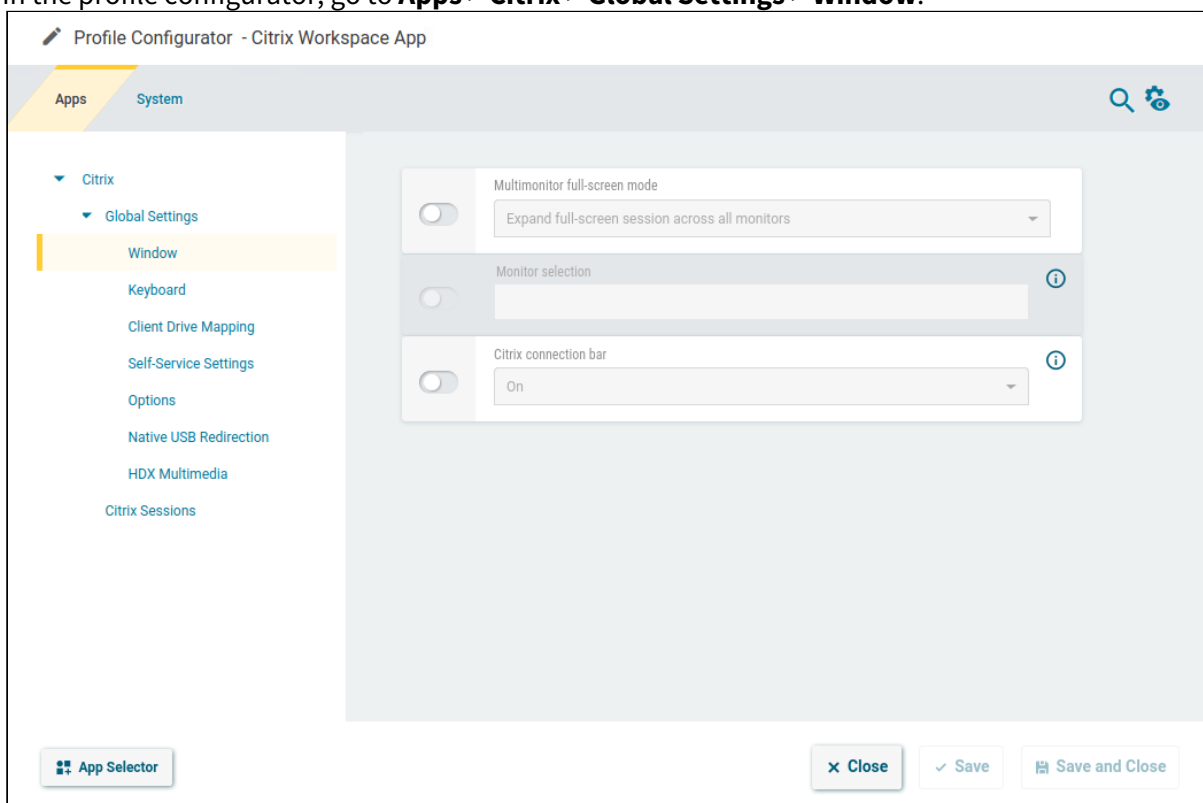
For this authentication method, HTTPBasic must be active on the server. This method is available only for Citrix on-premises, not for the Cloud solution. Also, on the **Server** page, HTTPS should be specified in the **Store URL** to ensure an encrypted connection.

5. Save the settings.

Configuration of the Citrix Workspace App on IGEL OS

Configuring the Session Window

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



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

Multimonitor full-screen mode

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

Monitor selection

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

Example

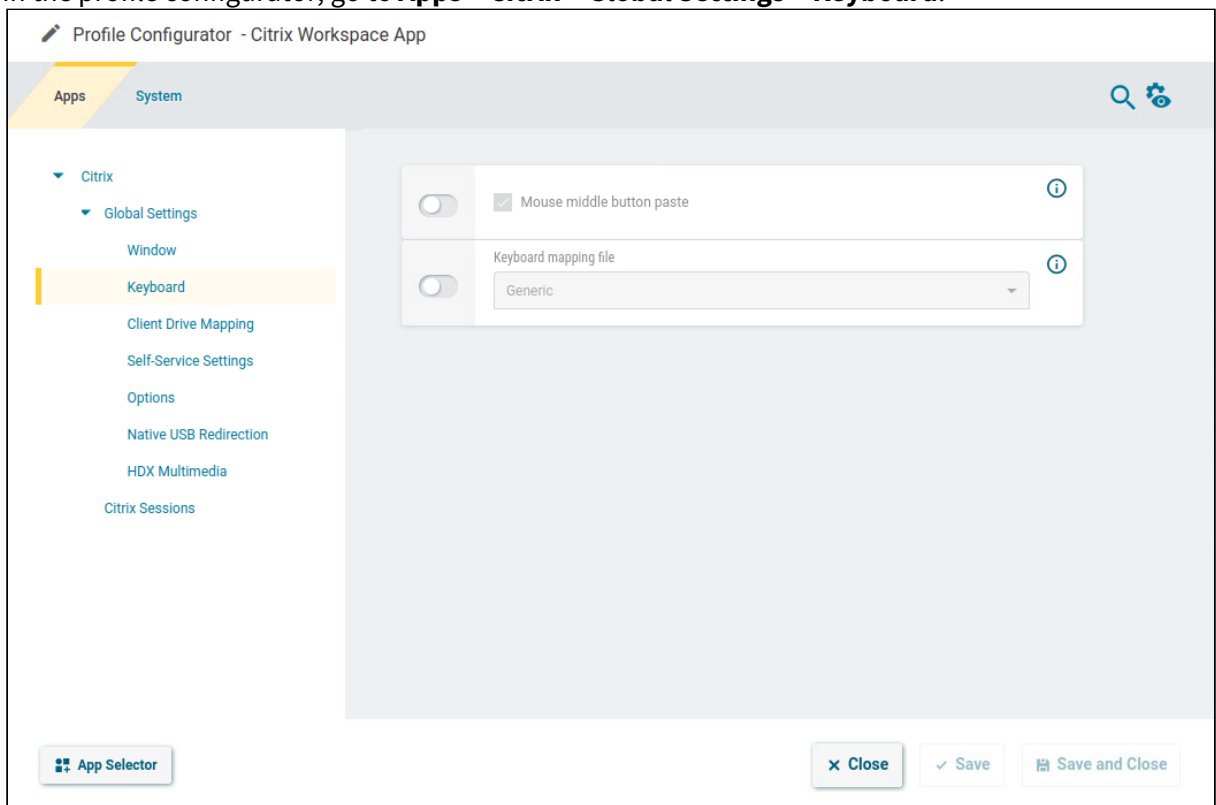
Sample configuration: If you have 4 monitors and want to expand your session across monitors 2, 3, and 4 you have to insert 2, 3, 4 or 2, 4 .

Citrix connection bar

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

Configuring the Keyboard

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



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

Mouse middle button paste

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

Keyboard mapping file

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

Alt + F1 ... Alt + F12

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

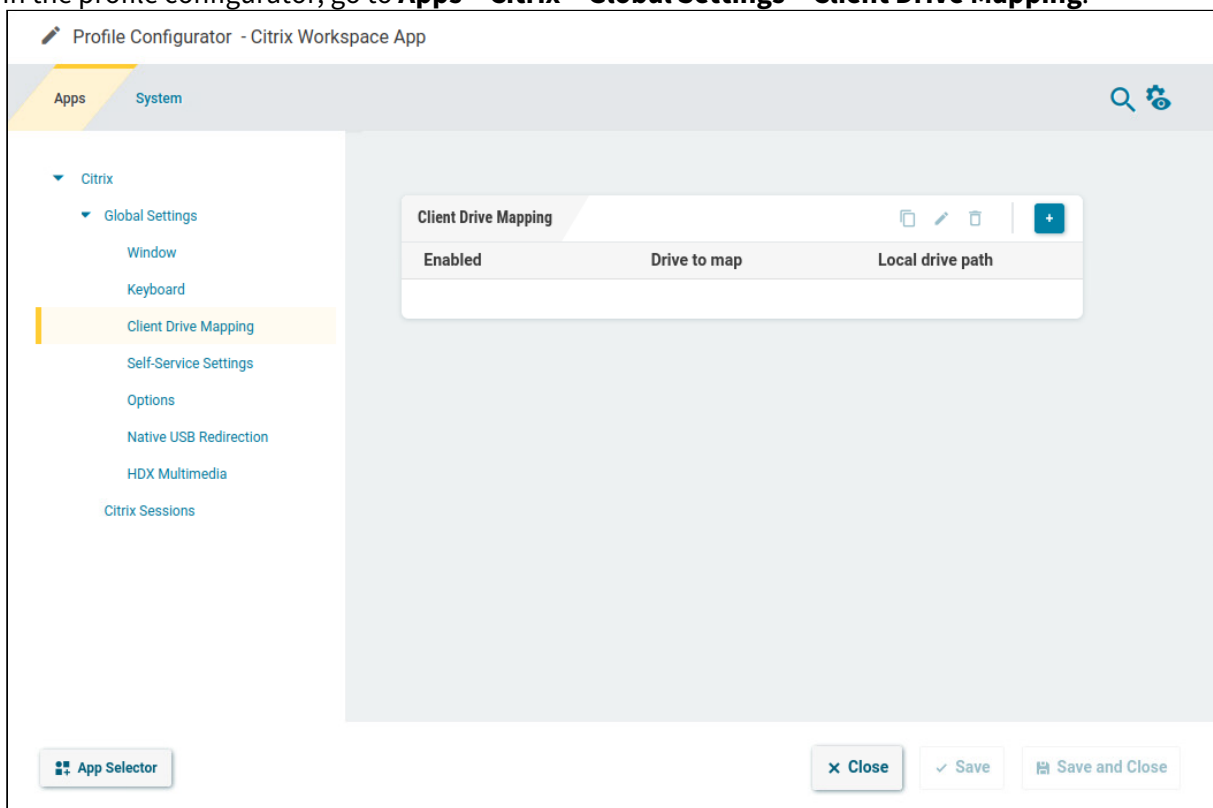
- **Hotkey character:** The function key to be sent when the relevant key combination [Alt] + [F<n>] is pressed
- **Hotkey modifier:** The modifier for the function key to be sent when the relevant key combination [Alt] + [F<n>] is pressed

Configuring the Client Drive Mapping

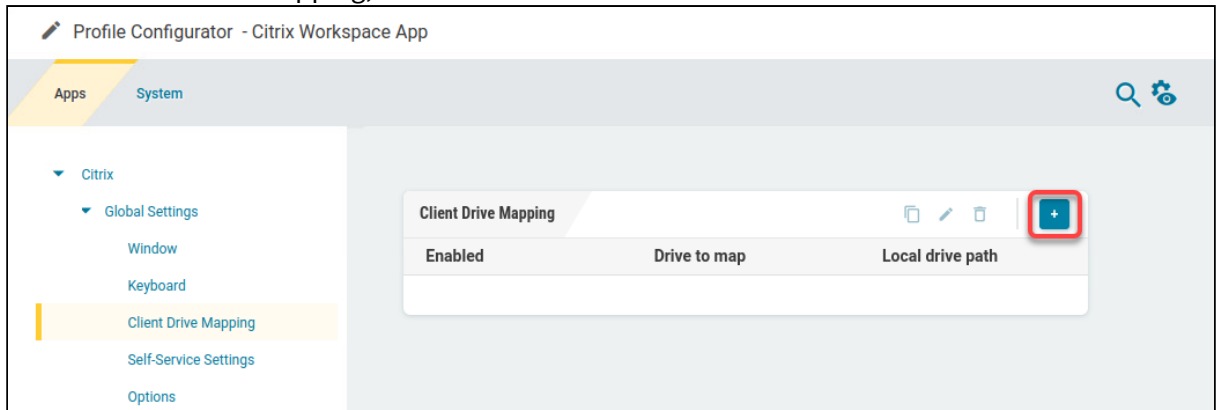
Through drive mapping, each directory mounted on the device (including CD-ROMs and disk drives) is made available to your Citrix session.

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

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




2. To add a client drive mapping, click .

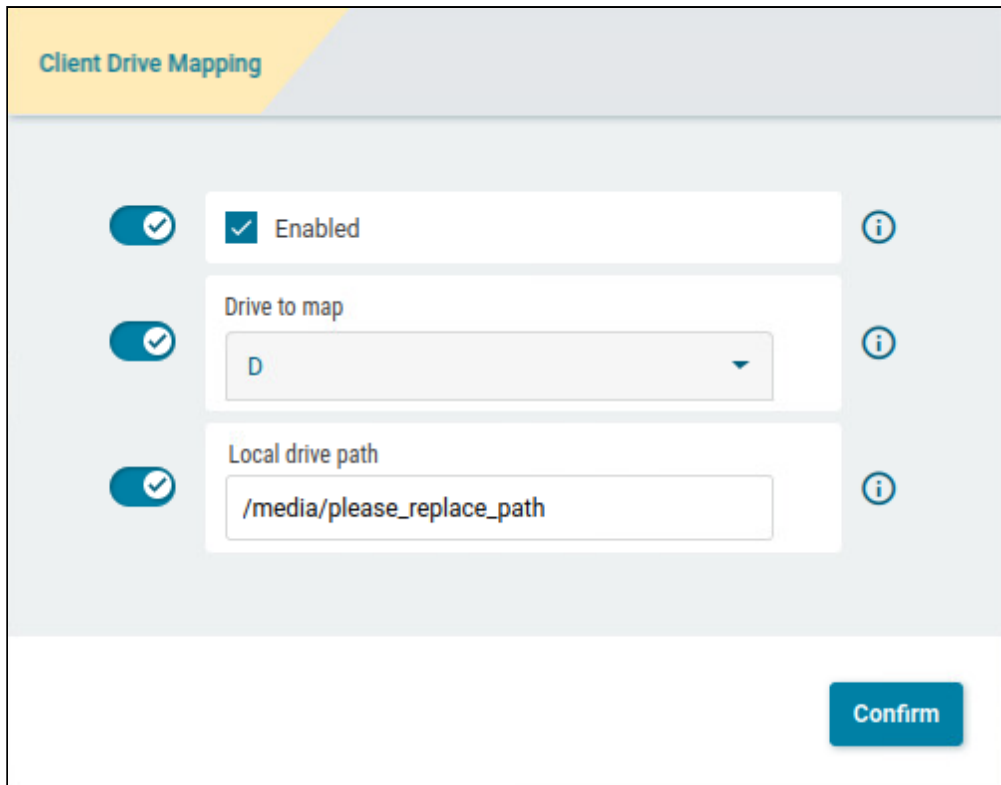


3. Edit the settings according to your needs and click **Confirm**:



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

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


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

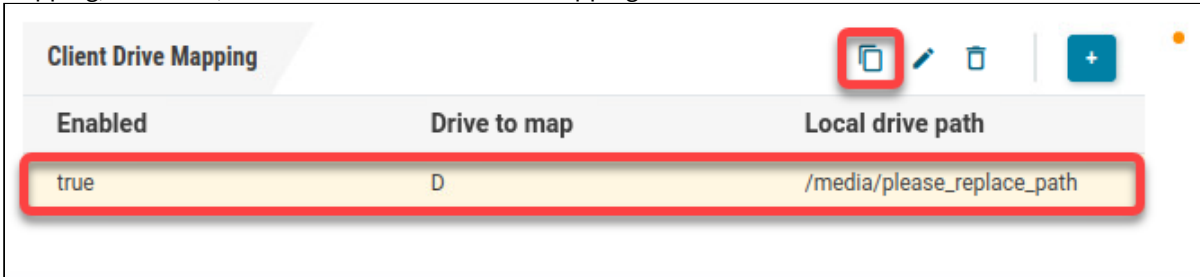


i Local (USB) devices which are to be used for drive mapping purposes must first be set up as storage devices.


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

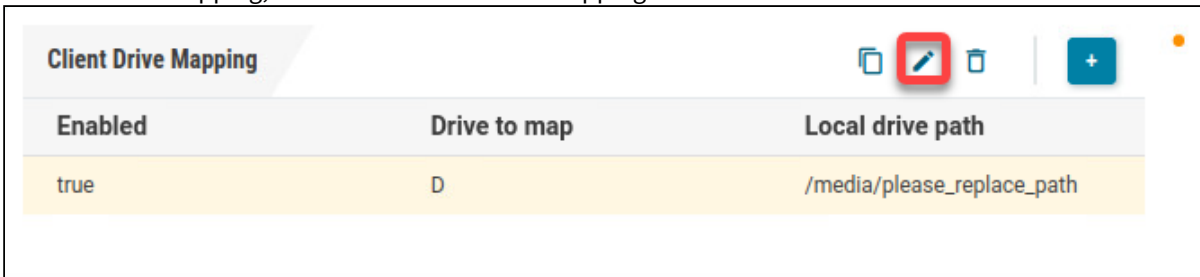
Adding Further Drive Mappings by Copying

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




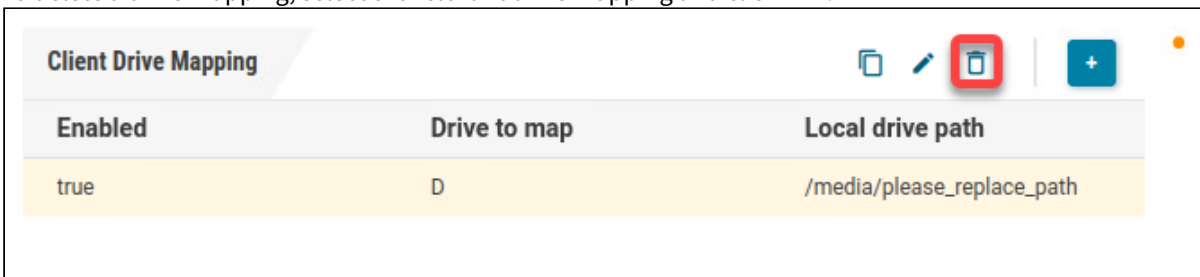
Editing a Drive Mapping

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



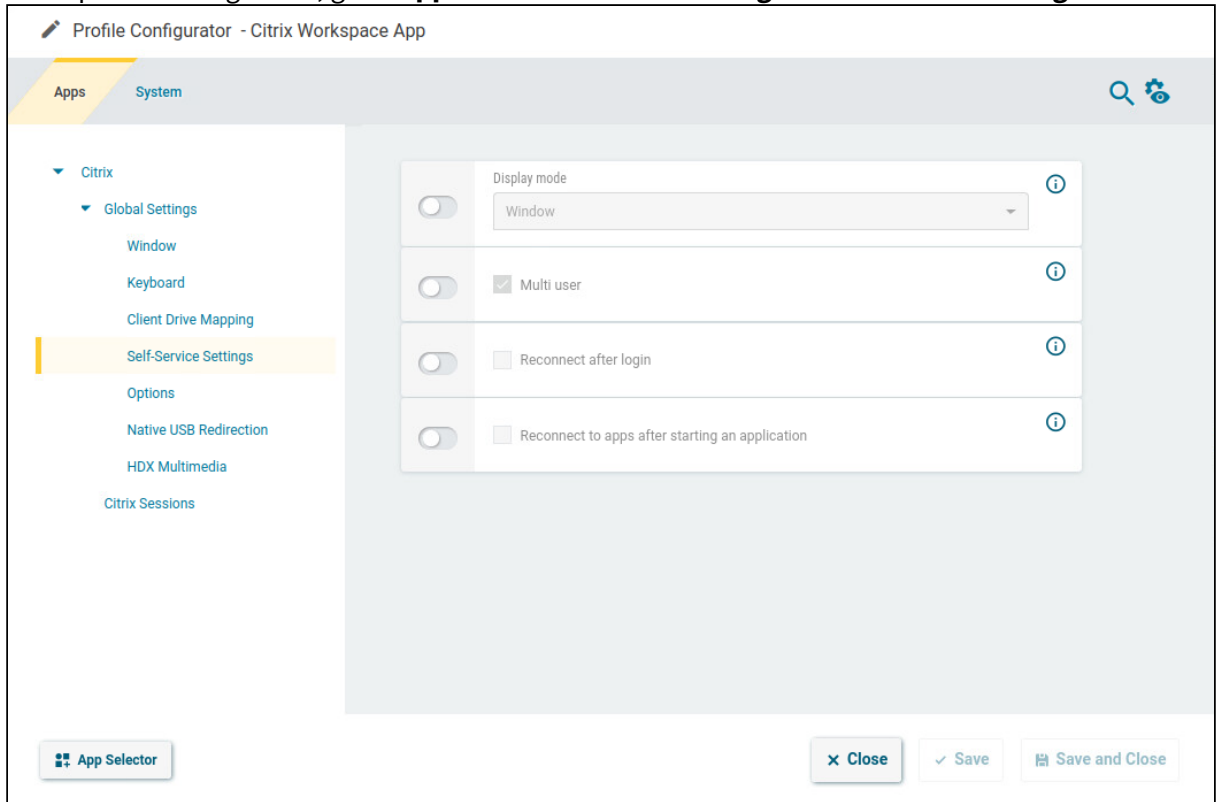
Deleting a Drive Mapping

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



Editing the Self-Service Settings

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



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

Display mode

Display type for the Self-Service user interface

Possible values:

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

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

Multi user

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

Reconnect after login

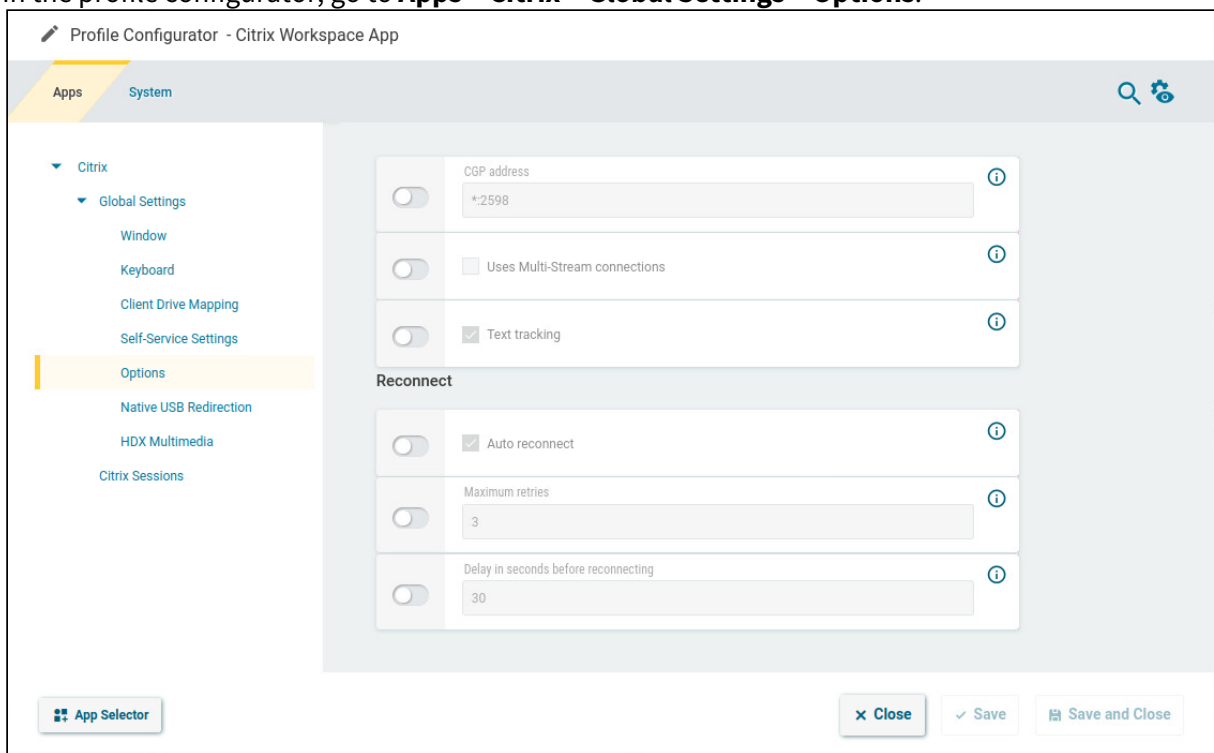
- The Self-Service user interface reconnects automatically to applications and desktops after being launched.
- The Self-Service user interface does not reconnect automatically. (Default)

Reconnect to apps after starting an application

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

Configuring the Options

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



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

CGP address

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


Uses multi-stream connections

- The ICA virtual channels are divided into four separate ICA channels.

The ICA virtual channels are not divided. (Default)

Text tracking

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

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

Auto reconnect

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

Maximum retries

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

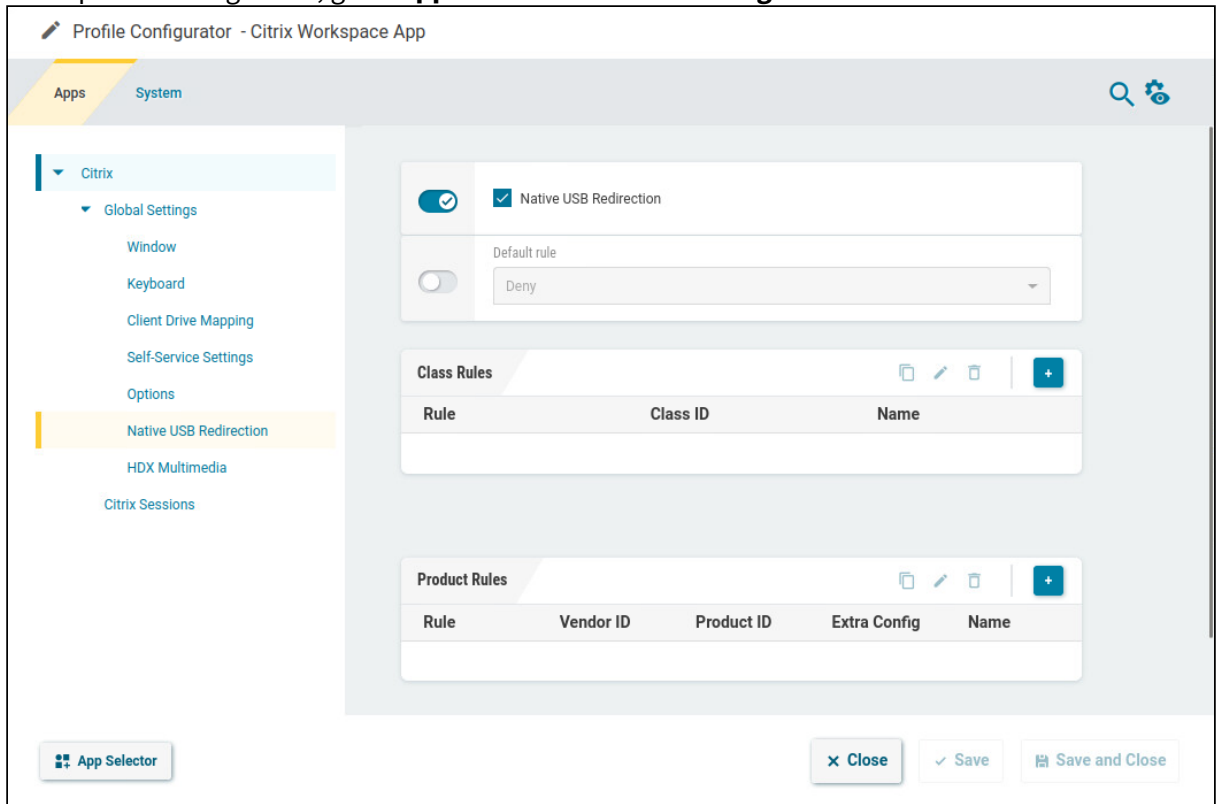
Delay in seconds before reconnecting

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

Configuring Native USB Redirection

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

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



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

Native USB redirection

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

Default rule

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

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

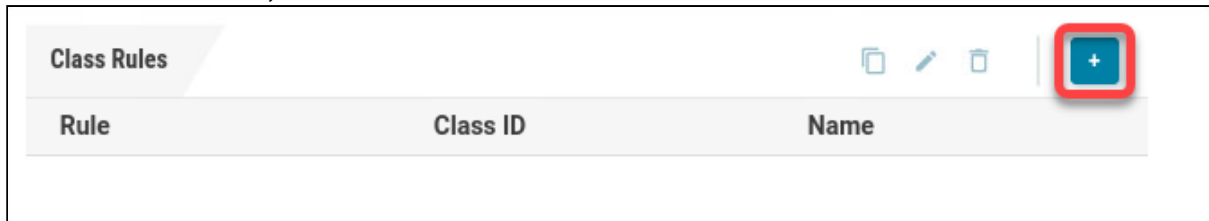
- **Deny** (Default)
- **Allow**

Class Rules

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

To add a class rule:

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




2. Set the criteria according to your needs:

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

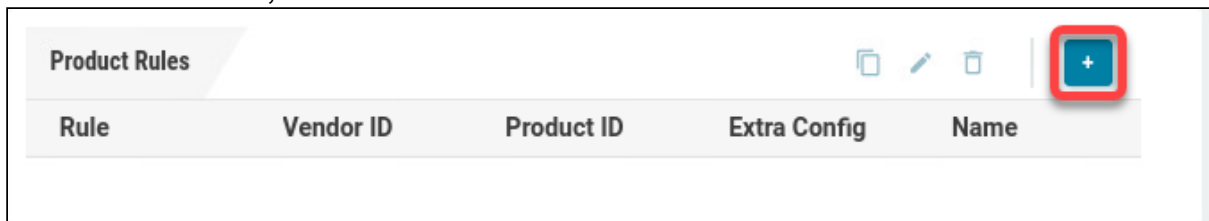
Product Rules

Product rules apply to individual USB devices.

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

To add a product rule:

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





2. Set the criteria according to your needs:

- **Rule:**
 - **Deny:** This device of this class/subclass will not be redirected automatically.
 - **Allow:** When this device is plugged in after the session start, it will be redirected. If you want an already plugged-in device to be redirected, unplug it and plug it in again.
 - **Connect:** This device is redirected, regardless of whether it has been plugged in before or after the session start.
- **Vendor ID:** Enter the hexadecimal value of the vendor id for the device to which this rule should apply.
- **Product ID:** Enter the hexadecimal value of the product id for the device to which this rule should apply.
- **Extra config:** If desired, enter configuration parameters for the device.

Example:

```
CONNECT: vid=047F pid=C039 split=1 intf=03 (For composite USB devices:  
Allow HID device and connect automatically)
```

- **Name:** Enter a name for this rule.

Product Rules

Rule: Allow

Vendor ID: 046d

Product ID: 0a45

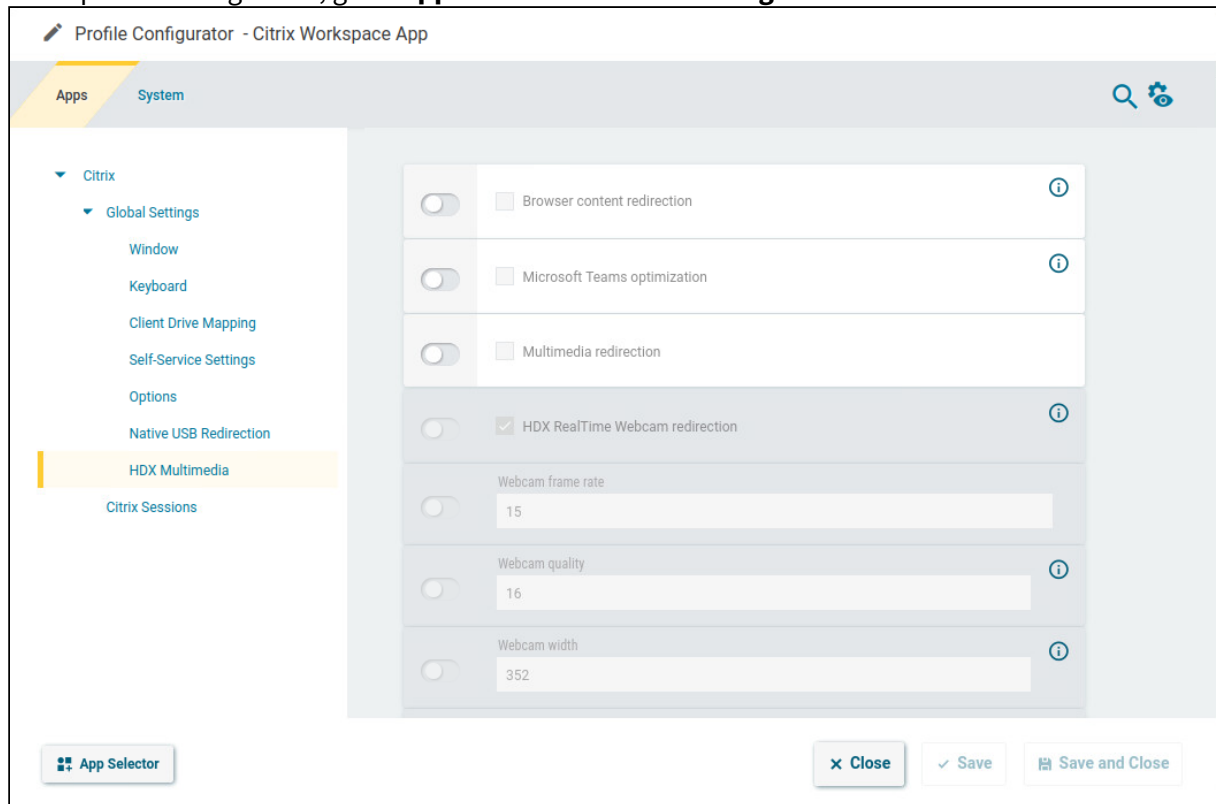
Extra Config:

Name: Logitech Headset

Confirm

Configuring the Settings for HDX Multimedia

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



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

Browser content redirection

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

Microsoft Teams optimization

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

Multimedia redirection

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

HDX RealTime webcam redirection

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

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

Webcam frame rate

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

The frame rate requested from the webcam. Default: 15

Webcam quality

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

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

Webcam width

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

The image width requested from the webcam. Default: 352

Webcam height

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

The image height requested from the webcam. Default: 288

HDX webcam delay time

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

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

HDX Webcam delay type

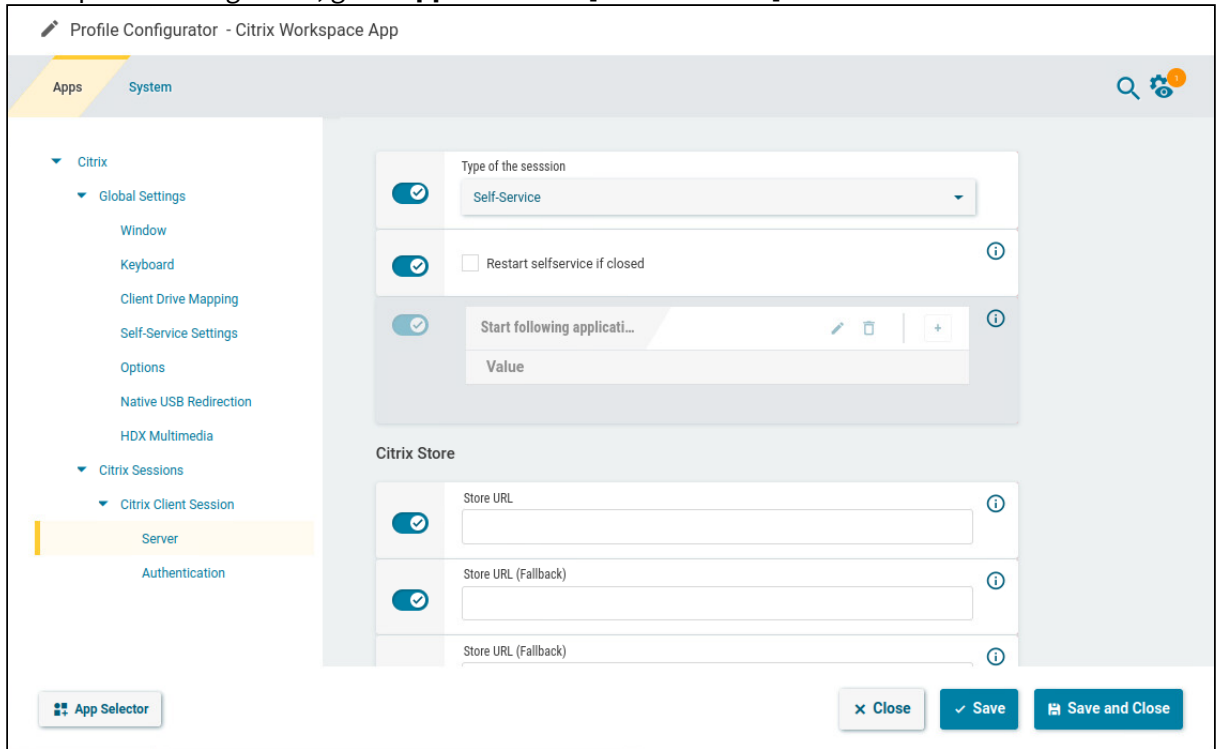
This setting is only available if **Multimedia redirection** is enabled.

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

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

Configuring the Server for an Individual Session

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



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

Type of the session

Possible options:

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

Restart selfservice if closed

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


Store URL

URL of the Citrix server.

Start following applicati...

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

You can define a list of applications that are started automatically when the server connection is established.

For each application, click  and enter the name of the application.

Store URL (Fallback)

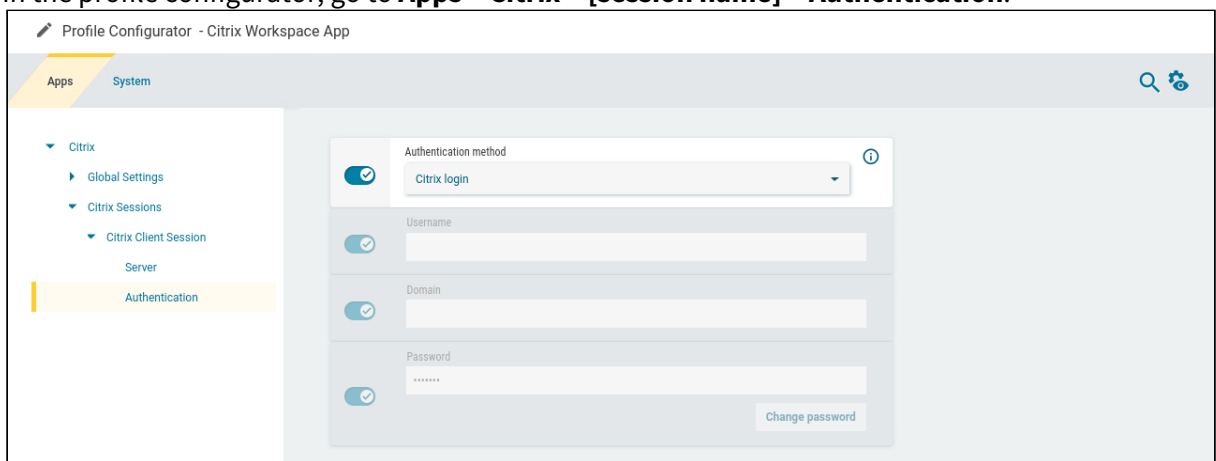
URL of the first fallback Citrix server.

Store URL (Fallback)

URL of the second fallback Citrix server.

Configuring the Authentication for an Individual Session


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



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

Authentication method

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

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

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



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

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

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

Username

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

Username for authentication via **IGEL login**.

Domain

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

Domain for authentication via **IGEL login**.

Password

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

Password for authentication via **IGEL login**.