PeakOS/RepurpOS V16.5.39
User Guide

Document and Version Control			
Version	Created by	Date	Authorized & checked
1.0	Jason Hudson	17/09/2024	K. Greenway
2.0	Jason Hudson	03/10/2024	K. Greenway
3.0	Jason Hudson	20/05/2025	K. Greenway
4.0	Jason Hudson	06/08/2025	K. Greenway

About This Guide

Thank you for choosing from the 10ZiG Technology series of Thin Clients which are designed for an array of different users in many different office environments. They feature a powerful, yet simple and affordable solution to virtual desktop computing in a fashionable and sleek design.

In this User Guide, you will find everything you need to quickly begin using your new device. Please be sure to verify with your network administrator that your network is prepared for the configuration of your new device.

Declaration of Conformity

It is hereby declared that this device is in conformity with the essential requirements, and other relevant provisions of the CE and the FCC.

CE Mark Warning

This is a class B device, in a domestic or office environment. This product may cause radio interference; in which case the user may be required to take adequate measures.

Waste Electrical and Electronic Equipment (WEEE) Warning

To potentially avoid adverse effects on the environment, and human health, as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed out wheeled bin symbol. Do **NOT** dispose of WEEE as unsorted municipal waste as municipalities must collect WEEE separately.

ABOUT THIS GUIDE **2**

GETTING STARTED **7**

Packing List *7*
Initial Hardware Setup *7*

SUPPORT **8**

ID CODE 9

INTRODUCTION **10**

10ZIG'S PEAKOS AND REPURPOS 10
PEAKOS 10
REPURPOS 10

INITIAL SETUP **11**

EULA 11

ACCESS TO THE CONTROL PANEL **12**

THE FLEXIBLE PEAKOS DESKTOP **13**

SETTING ALTERNATIVE DESKTOP MODES IN CONTROL PANEL **14**

APPEARANCE 14
WALLPAPER/BACKGROUND 14
Theme *15*
Screensaver *15*
ADVANCED 16
Terminal Modality *16*
Modality : Full Desktop *17*
Modality : Portal Mode. *17*
Modality : Kiosk Mode (Single application) *18*
Modality : NOS-O, NOS-C and NOS-M *19*
Saving Display Changes *19*
NOS-O – Omnissa Horizon Client Login *NOS-C – Citrix Client login* *19*
NOS-M – Microsoft Remote Desktop Client login *19*
Importing your own Wallpaper and Launchpad Desktop Images *20*
Setting the PKOS Thin Client to "Enable Install from USB" 20
Setting the Wallpaper using a local USB key 20
Examples of Full Desktop and NOS-O Modality after Setting the Wallpaper using a local USB key 21
Setting the NOS Launchpad Desktop using a local USB key 22
Using 10ZiG Manager to import images and deploy them to your Thin Clients 23

NOS FOR OMNISSA NOS-O **27**

GENERAL 27
LOGOFF ACTION 29

Login 30
RTAV(Real Time Audio and Video) Camera Settings 33
Blast Extreme Settings 34
PCoIP 36
Proxy 37
Plugins 38
Advanced 39
Saving your settings 43
Editing your connection settings 43
Omnissa Horizon Connection Examples 44

NOS for Citrix NOS-C 47

General 47
Workspace 49
WebAPI/PNAgent 51
Login 54
Logoff Action 56
Proxy 57
Reconnection 58
Teams Optimization 59
Advanced 60
Saving your settings 63
Editing your connection settings 63
Citrix Connection Examples 64

NOS for Microsoft NOS-M 66

Azure Virtual Desktop and Windows 365 Cloud PC(AVD/W365) 66
General 66
AVD/W365 68
Login 70
Example of Cached login details 71
Logoff Action 72
Resources 73
Advanced 74
Direct RDP 76
Login 77
Logoff Action 80
Display 81
Resources 82
Programs 84
Experience 85
RD Gateway 87
Advanced 89

RDWeb webfeed 91
RDWeb *92*
Login *94*
Logoff Action *97*
Display *98*
Resources *99*
Programs *101*
Experience *102*
RD Gateway *104*
Advanced *106*
Saving your settings 108
Editing your connection settings 108
Azure Virtual Desktop – Connection setting examples 109

CONTROL PANEL SETTINGS **111**

Applications 112
Connection Manager *112*
Creating a New Connection using the Connection Manager 113
Saving your settings 114
Editing your Connection settings 114
Startup options for your Connections in Kiosk Mode 115
Deleting your Connection settings 115
Citrix Logger *116*
ICA Global Settings *117*
The example below shows editing of the "wfclient.ini". *117*
Imprivata *118*
New Connection *119*
Hardware 120
Display *120*
Dual Monitors 121
Power Saving (DPMS) 122
Keyboard *123*
Layout 123
Keyboard – Typing Settings 124
Mouse *125*
Network *126*
Wireless Network Connection (Additional Hardware Opt.) 127
Printers *130*
Configuring Local USB Printer 130
Configuring a Network Printer 133
Smart Card Service *136*
Sound *137*
Touch Screen *138*
USB Devices *139*
System 141

Auto Shutdown *141*
Certificates *142*
Importing Certificates 142
Importing a Certificate from a USB storage device 143
Importing a Certificate from the 10ZiG Manager Web Console 144
Time & Date *147*
SECURE AGENT 148
Desktop *149*
Event Logger *150*
General 150
System Events Security Events 150
Performance Events Network Events 151
Valid Keywords for the Format String. 151
Examples of Security Events being triggered 151
Complete list of Event IDs 152
System Logs *153*
Collecting Logs via a USB storage device 153
Collecting Logs via the 10ZiG Manager Web Console 154
Network File System *155*
Power *156*
RPOS License *157*
Security settings *158*
System 158
Control Panel Options inside Security Settings 160
Authentication 161
System Information *163*
Information 163
Packages 163
Advanced 164
Factory Default message 164
Console Screen 164
BIOS 165
VNC Service *166*
VPN Client *167*
SideBar/TaskBar *169*

Getting Started

Packing List

The following components are included in the package:

- Thin Client Device
- Stand
- 12v DC Power Adapter with Cord

Optional equipment that may be included:

- USB Wheel Mouse
- USB to PS2 Adapter
- SVGA to DVI Adapter
- Monitor Mount Kit (may include optional video cable)
- SVGA and DVI splitter cable
- Wireless Network Adapter and Antenna
- Quick Installation Guide & Management Software CD

Check this list before installation to ensure that you have received each item ordered. If you are missing any items, please contact technical support.

Initial Hardware Setup

To setup the device for initial use :

- Attach the Stand (if desired)
- Connect a Keyboard, Monitor and Mouse
- Connect to a Network and a Power Source

Support

If you require support for your Linux-based Thin Client, please contact your region's nearest Technical Support Center. While 10ZiG Technology does provide technical support for its Linux-based Thin Clients, it does not provide support for the Linux operating system or application components that are obtained from the open source community and that may be included as part of the software image installed.

10ZiG Technology, Inc.

Headquarters USA (North America)

2043 W. Lone Cactus Drive
Phoenix, AZ 85027

Phone 866-865-5250

support@10zig.com

sales@10zig.com

www.10zig.com

Headquarters UK (EMEA)

10ZiG Technology Limited

7 Highcliffe Road
Leicester
LE5 1TY
UK

Phone +44 (0)116 2148661

support@10zig.eu

sales@10zig.eu

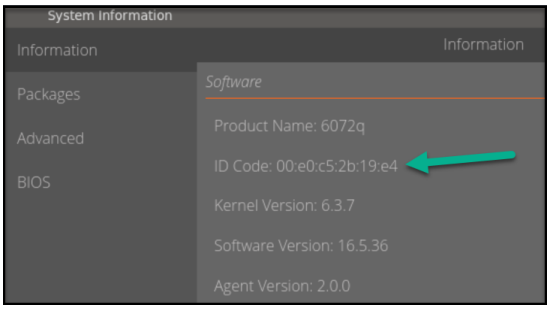
www.10zig.eu

For more information, FAQs, and helpful hints, please browse to
https://www.10zig.com/resources/support_faq

ID Code

Each Thin Client has a unique **ID CODE:** which is the **MAC address** of the unit. The sticker with this information may be found either on the side, bottom, near the video output port or on a slide out tab on the back of the unit, depending on which model you have. Please have this number available when contacting 10ZiG Technology's Technical Support for assistance. You can also find this number against the Thin Client in the 10ZiG Manager Web Console or inside the Control Panel and System Information of the Thin Client OS, as shown by the arrows in the pictures below.

Control Panel – System Information



The Device's Information Sticker

Introduction

This guide provides the user with instructions for the hardware configuration of the Linux-based Thin Client and explains the various utilities used to accomplish these tasks. Typically, a Thin Client is configured locally and then used as a template to configure other units. These saved configuration templates can then be pushed out to additional Thin Clients using the optional "10ZiG Manager", which can be found at http://www.10zig.com/manager.

10ZiG's PeakOS and RepurpOS

The PeakOS and RepurpOS operating systems are the same platform under the hood and run the same software version, with just a few minor differences.

PeakOS

This is 10ZiG's Linux-based fully featured Thin Client operating system running on 10ZiG hardware.

RepurpOS

If you're running this Linux-based operating system on non-10ZiG 3rd party hardware, then this goes by the name of RepurpOS and needs licensing to unlock full functionality as outlined below.

- Firmware Updates are not available, either locally to the device via a USB drive, or remotely via "10ZiG Manager". A software support subscription registered (PAID) license is required to gain access to these features.

- Technical support is not available and requires a Software Support subscription registered (PAID) license to gain access.

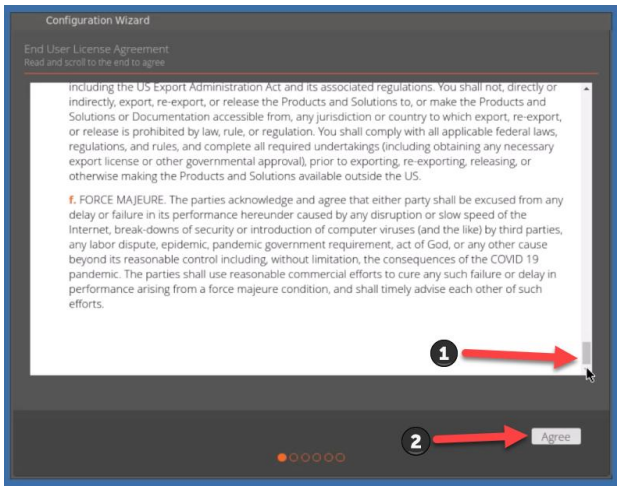
If you need further information on how to license your RepurpOS operating system on non-10ZiG 3rd party hardware, get in touch with your local 10ZiG representative and they will be more than happy to assist you with this

Initial Setup

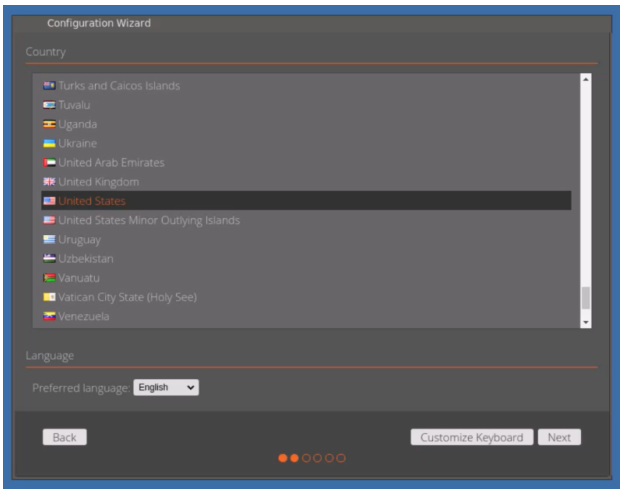
Upon Initial boot up you will be taken to the first of several “Configuration Wizard” screens, where you’ll be prompted to accept the “End User License Agreement” (EULA), select your country, keyboard settings, time zone, and set the time and date.

To accept the EULA, read and scroll down to the bottom of the agreement (1) and click “Agree” (2)

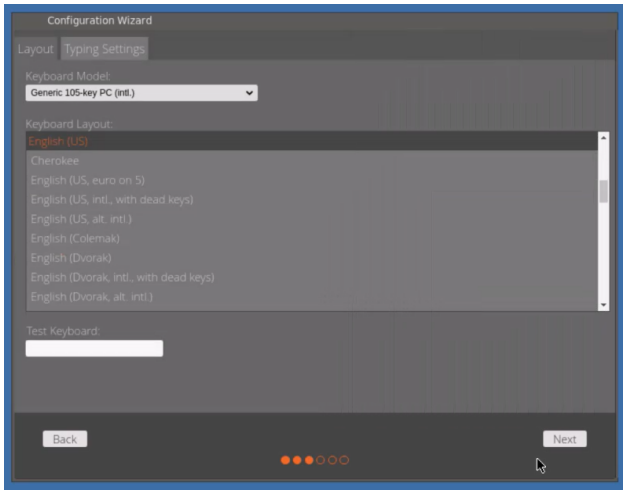
EULA



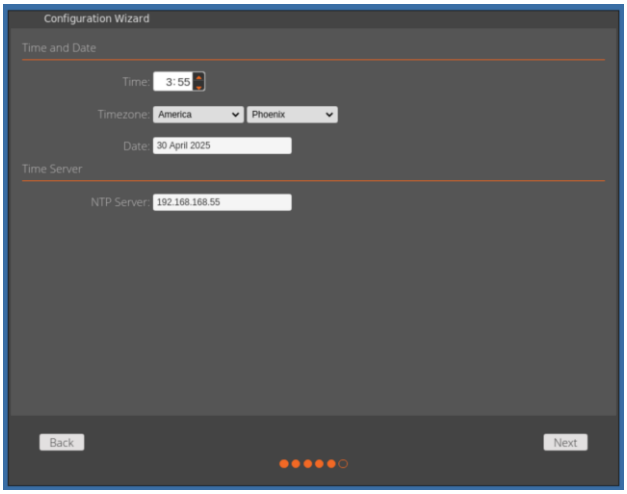
Country and Language settings



Keyboard settings



Time and Date settings



Access to the Control Panel

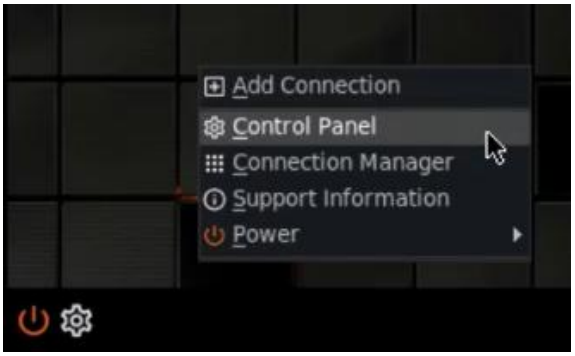
The Control Panel is where you'll carry out most of the configuration of your Thin Client and can be launched using several different methods as shown below. Just look out for the "Gear" icon.

On the taskbar

Click the "Gears" icon in the bottom left corner of the taskbar, when running in "Full Desktop" mode.

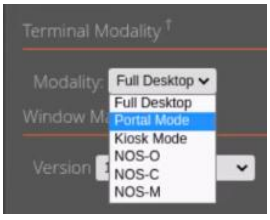
On the Desktop

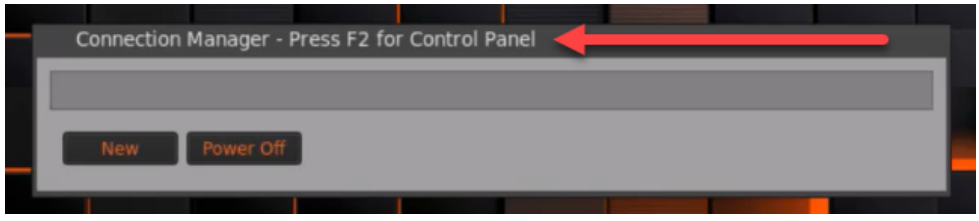
Right click anywhere on the desktop or taskbar when running in "Full Desktop" mode.



In Terminal Modality called "Portal Mode" – "F2" Key

If you're running your desktop in "Portal Mode", then inside the "Connection Manager", use the "F2" key to enter the Control Panel.





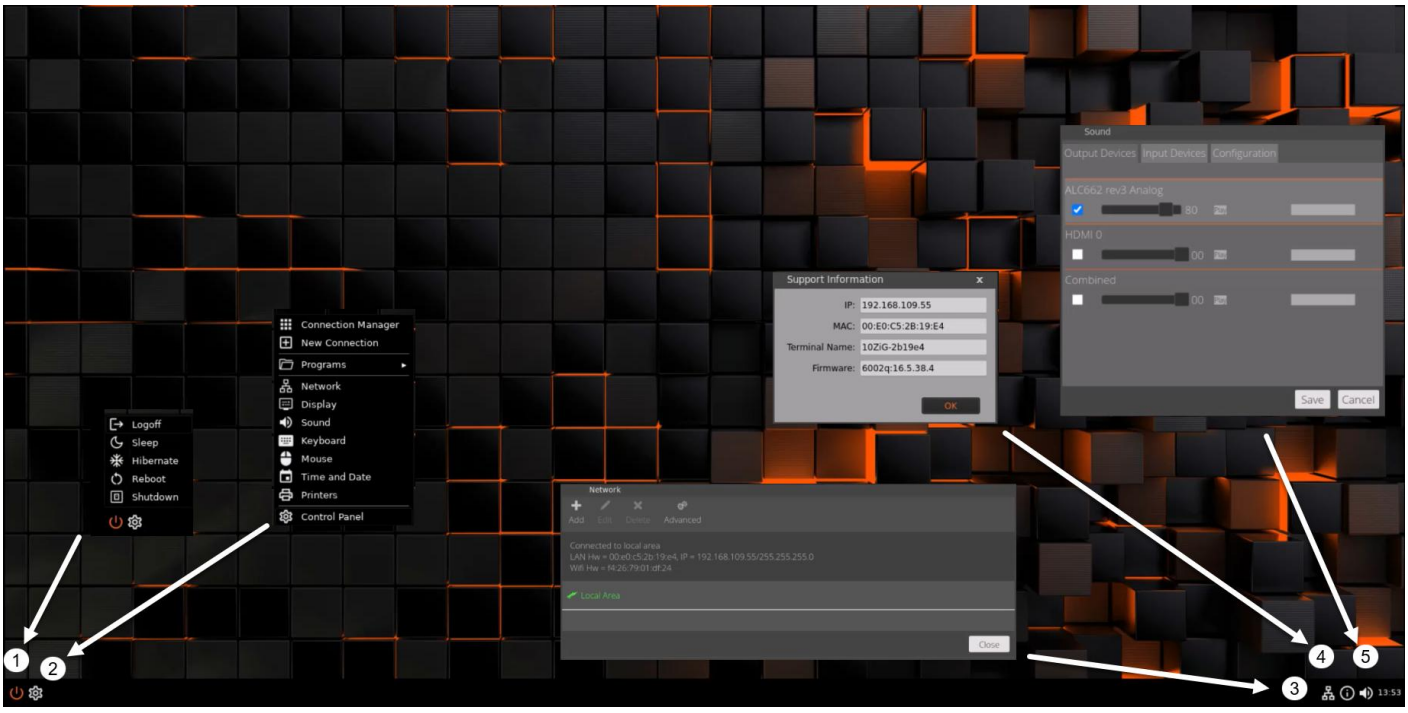
The Flexible PeakOS Desktop

You can completely customize the whole look and feel of the PeakOS desktop environment and configure the Thin Client to run in full desktop mode, Portal Mode, Kiosk, and even transform the device to run as a 10ZiG NOS Zero Client.

We're mentioning these "Desktop" options now, as they form the basis of your user's working environment and serve as a starting point for customization. Your organization might have a set standard for the desktop configuration. It might want to run in single app kiosk mode for example to only run a single application at startup to create a more secure environment to both manage and work with.

Note: We'll show sample screens that may include "Connection" icons, whilst we talk about "Desktop" modes, but we'll cover "Connection" types in more detail further on in this guide.

Once you have completed the initial setup you'll see the default desktop displayed below. We've highlighted areas on here that are useful for first time navigation just to get you started.

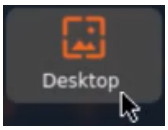


1. Shutdown, Reboot, Hibernate, Sleep and Logoff options.
2. Control Panel, Quick Items, Programs and Connections.
3. Network Settings.
4. Support Information.
5. Sound Configuration Applet.

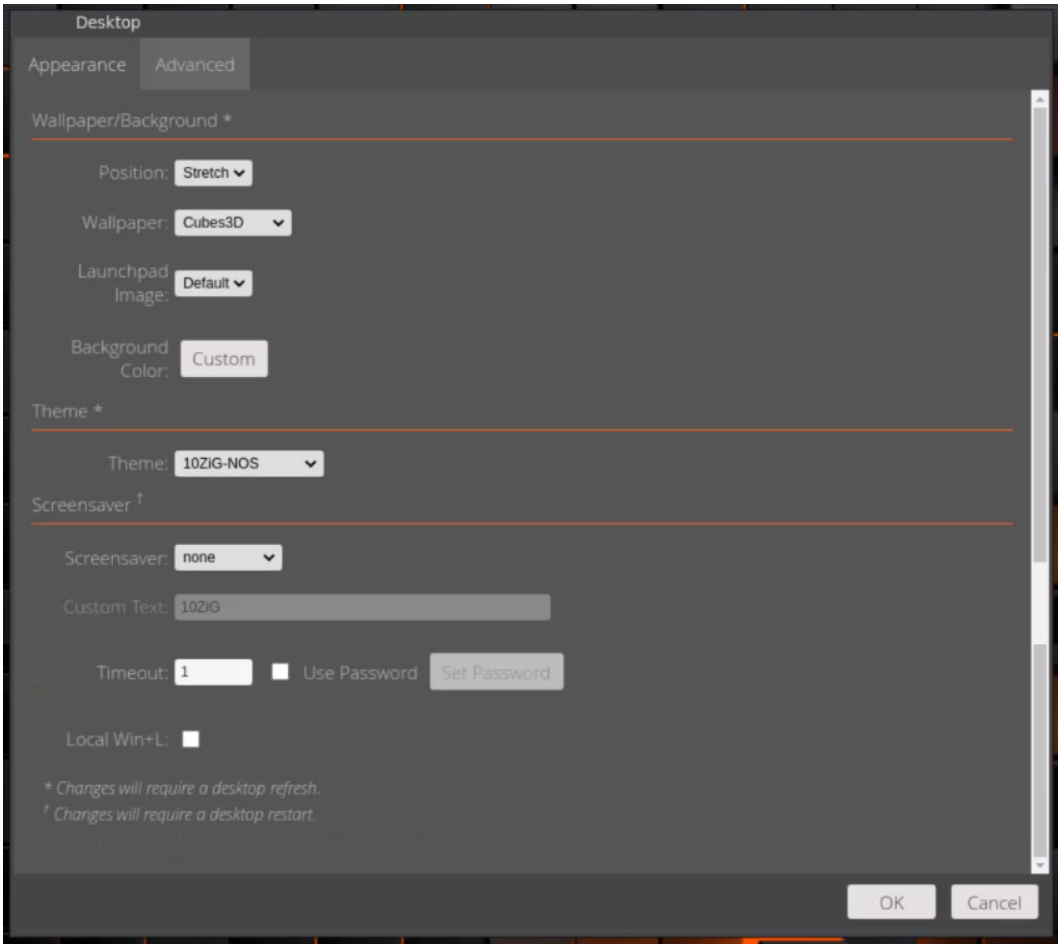
Setting Alternative Desktop Modes in Control Panel

We'll cover the Control Panel and its components in greater detail in the next sections but first let's explore the "Desktop" modes available to us inside PeakOS.

Open the Control Panel using the one of the methods mentioned in "Access to the Control Panel" earlier and click on the icon named "Desktop" under the "System" section heading and you will see the following screen displayed with the "Appearance" tab highlighted.



Appearance



Wallpaper/Background

- **Position**: Available options are "Center", "Stretch" and "Tile". "Center" will place the image in the center of the screen. "Stretch" will take a single background image, as seen in "Center" and stretch it to fill the entire screen. "Tile" will take a single background image, as seen in "Center" and replicate the image to fit the background.

- **Wallpaper**: This drop down menu lets you choose from a selection of different images or just leave the option as the default “Cubes3D”. If you want to use your own images for a different look and feel, such as you own company branding, then you can apply these in several different ways. Click this link to navigate to the end of this chapter, where we’ll explain how to do this using a local USB key, and 10ZiG Manager to deploy Configs or Templates.

- **Launchpad Image**: Just as explained in the “Wallpaper” definition above, if you have any of your own images that you’d like to apply to your Thin Clients, you can use the methods described at the end of this chapter. Click this link to find out how.

- **Background Color**: Click the “Custom” button and then select the specific color for the background, using the “Color Picker” dialog box. Alternatively, you can key in the RGB colors or the HEX value. Click “OK” to save the colour. See below.

Note: To take advantage of using a “Background Color”, you must make sure that “Wallpaper” drop down is set to “none” before you click “OK” to save the “Desktop” changes.

Theme

- **Theme**: The default is “10ZiG-NOS” to resemble look and feel of the “NOS” Zero Client theme. Other possible options are “LookXP-WXPBlue”, “LookXP-BOS”, “10ZiG-pkos” and “10ZiG-Classic”.

Screensaver

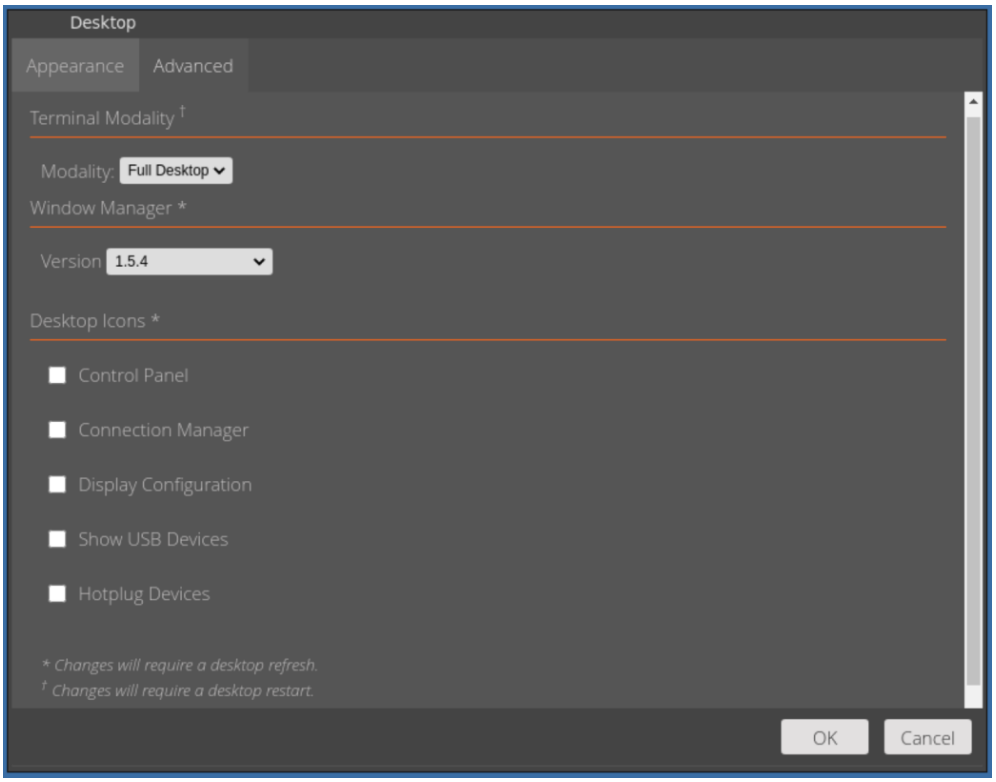
- **Screensaver**: By default, the screensaver is set to “none”. There are many screensavers to choose from in the drop down menu. If you select the screensaver called “gltext” from the drop down, then you can type in your own message in the “**Custom Text**” field, and this will be displayed when the screensaver is launched.

- **Timeout**: The number of minutes of keyboard or mouse inactivity before the screensaver is launched. The default time is set to 1 minute of inactivity.

- **Use Password**: Ticking this box for the first time will allow you to specify a password against changing the screensaver options in future. If you wish to change the password or remove password functionality from the screensaver options, then you must click the “Set Password” button and provide the existing password to gain access.

- **Local Win+L**: This is used to block sending the key combination to the remote desktop, if you’re running in PKOS/RPOS full desktop mode and requires the use of LDAP and your user’s AD credentials. Ask a 10ZiG Technical representative for more information on using this feature.

Advanced



Terminal Modality

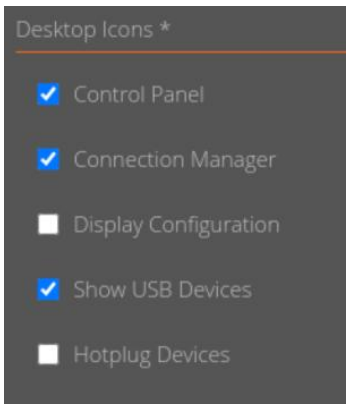
Modality: This “Desktop” feature is one of the most important as it defines the look, feel and overall mode of operation of your Thin Clients. Some of these modes will give you greater operational control from a user perspective and others will give your users the flexibility to add and manage their own app content, based on what is currently available in PeakOS. These modes are described below.

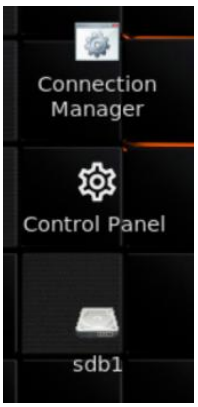
Three of these modes are dedicated to running your Thin Client just like a Zero Client with 10ZiG’s NOS-O(Omnissa), NOS-C(Citrix) and NOS-M(Microsoft Remote Desktop) and will be explained later on in this guide.

Modality : Full Desktop

This is the default mode that PeakOS installs with and gives you access to and “Start Menu” and taskbar. It also allows you to create your VDI/DaaS, browser and various other connections to the desktop.

If you’re running the desktop in “Full” mode, you have the option of including additional desktop icons. Here is a sample screen of desktop icons “Control Panel”, “Connection Manager” and “USB Devices”. Note the sda1 is our plugged in USB device.





Modality : Portal Mode.

This mode allows you to run your connections from within a single terminal style window. All your connections are created and contained inside the “Connection Manager” window. Access to the “Control Panel” is available by pressing the “F2” function key whilst you’re in this mode. Below is a sample screen of the Portal Mode session “Connection Manager” window with some example connection types.

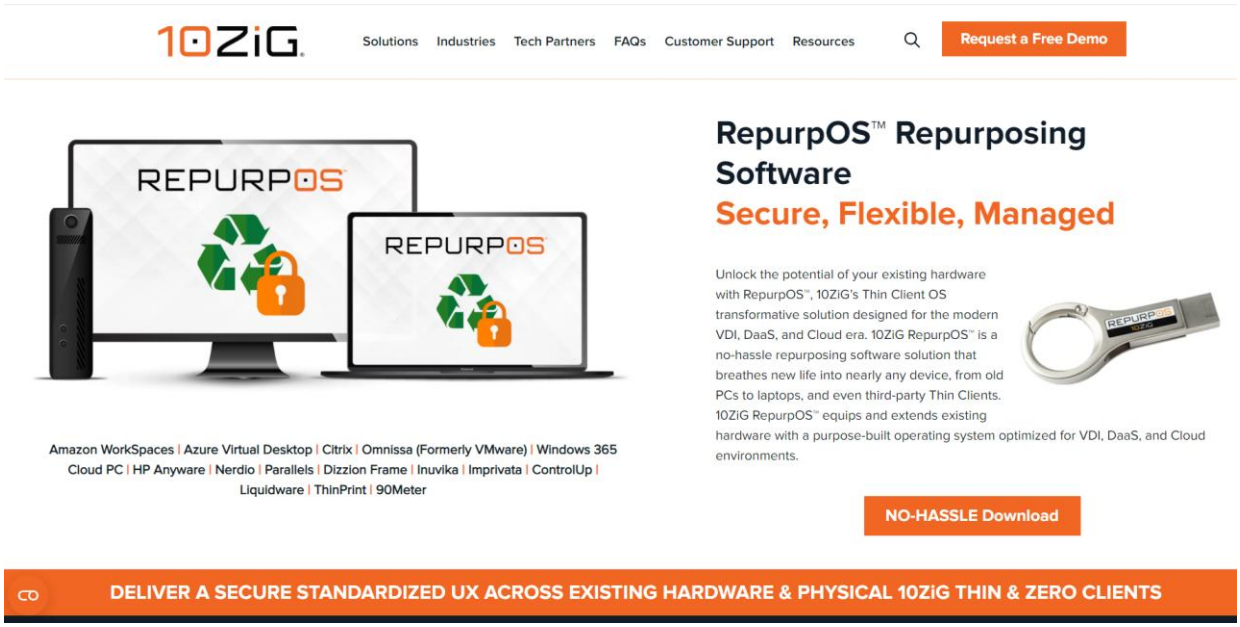
Modality : Kiosk Mode (Single application)

This mode allows you to launch a single application at startup, restricting access to all other desktop functionality and is the best option for securing your Thin Client.

This mode is ideal for running your Thin Clients in locations such as schools, libraries, airports, and hotel lobbies, where they can be left unattended for public use.

For example, you might want to run a browser that itself runs in Kiosk mode, without any navigation buttons or address bar, launches a default URL and relaunches itself if end users close the browser window or restart the Thin Client.

Below is a sample screen running a single browser window, itself in “Kiosk” mode as described above.

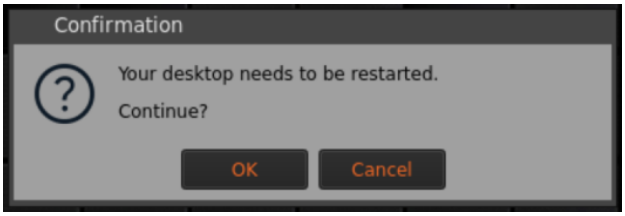


Modality : NOS-O, NOS-C and NOS-M

These modes allow you to run your Thin Client as a dedicated NOS-O, NOS-C or NOS-M device, running the respective Linux VDI/DaaS clients as a “Launchpad”, as mentioned earlier.

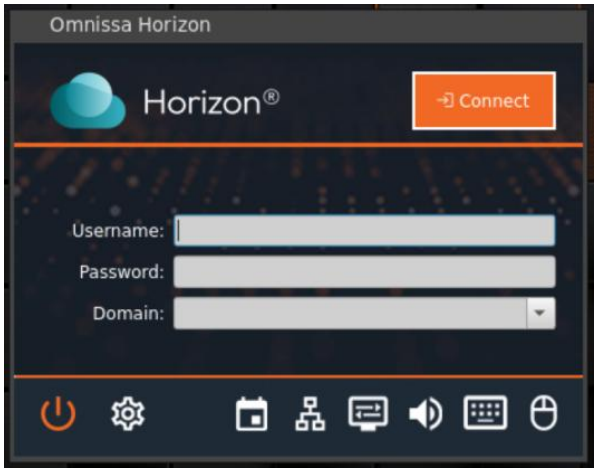
Saving Display Changes

Once you’re happy with the display changes, click “OK” and you might need to accept the “desktop needs to be restarted” dialog as shown below, for the desktop changes to take place.

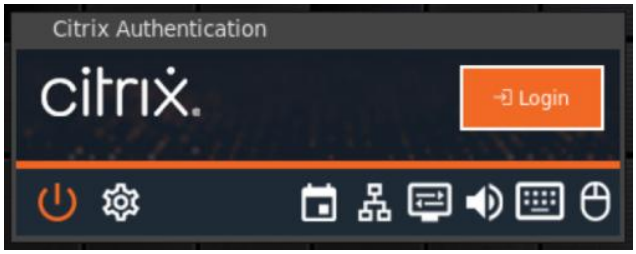


Below are example of NOS-O, NOS-C and NOS-M desktop “Launchpad” login boxes once you have changed the modality to the required NOS flavor.

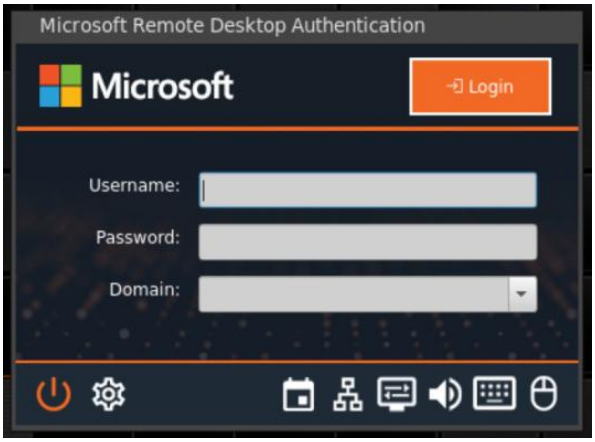
NOS-O – Omnissa Horizon Client Login



NOS-C – Citrix Client login



NOS-M – Microsoft Remote Desktop Client login



Importing your own Wallpaper and Launchpad Desktop Images

Importing your own “Wallpaper” or “Launchpad Desktop” images can be done in several ways. You can either use images supplied on a USB key, or using 10ZiG Manager to import these into your device configs or templates, that can then be deployed back to your thin clients. These methods are outlined below.

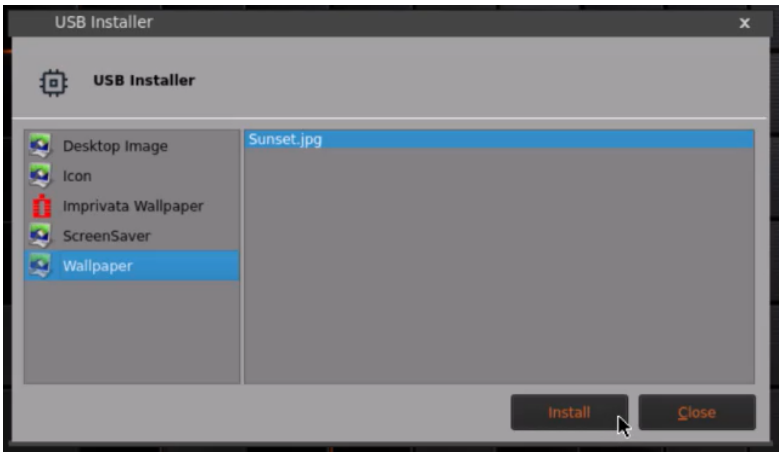
Setting the PKOS Thin Client to “Enable Install from USB”

Before you can import any image related content locally from a USB key, you first need to “Enable Install from USB”. To do this, you need to go into the “Control Panel” and click “Security Settings”. Tick the box named “Enable Install from USB” and click “SAVE”. See below.

Once you have done this, insert the USB that contains the image you want to set as the “Wallpaper” or “Launchpad Desktop” and the “USB Installer” dialog will automatically appear.

Setting the Wallpaper using a local USB key

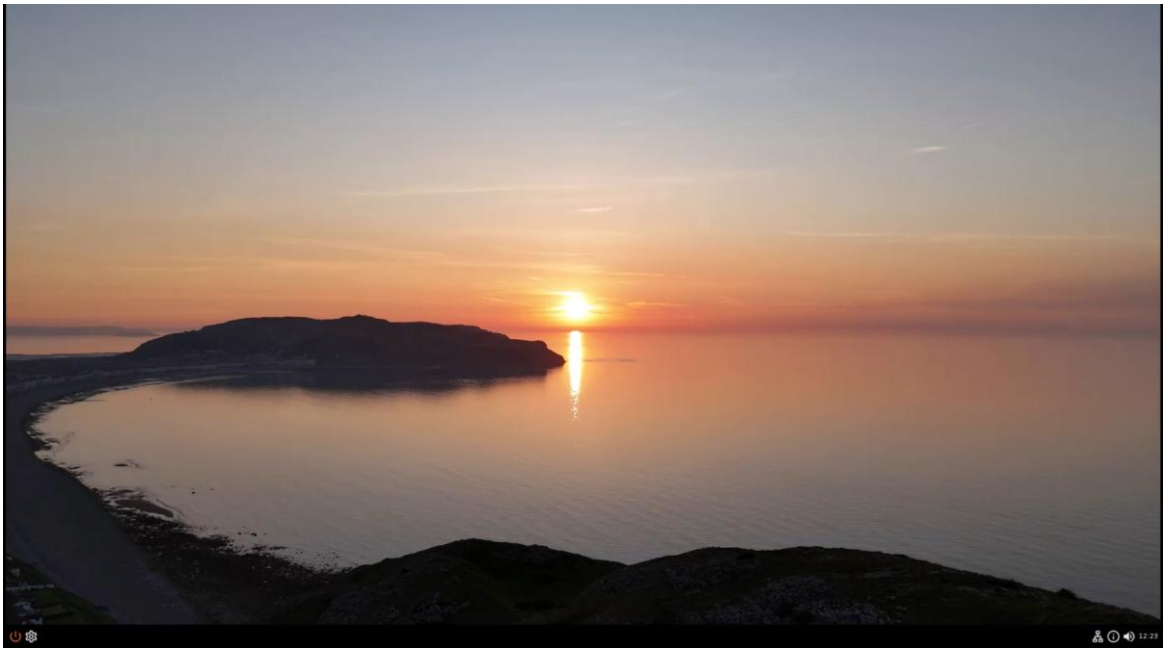
We have an image called “Sunset.jpg” on the USB key. So, to set this as the “Wallpaper”, just click and highlight the filename “Sunset.jpg”, highlight the “Wallpaper” item in the left menu and then click “Install”. Close the Control Panel once you have done this.



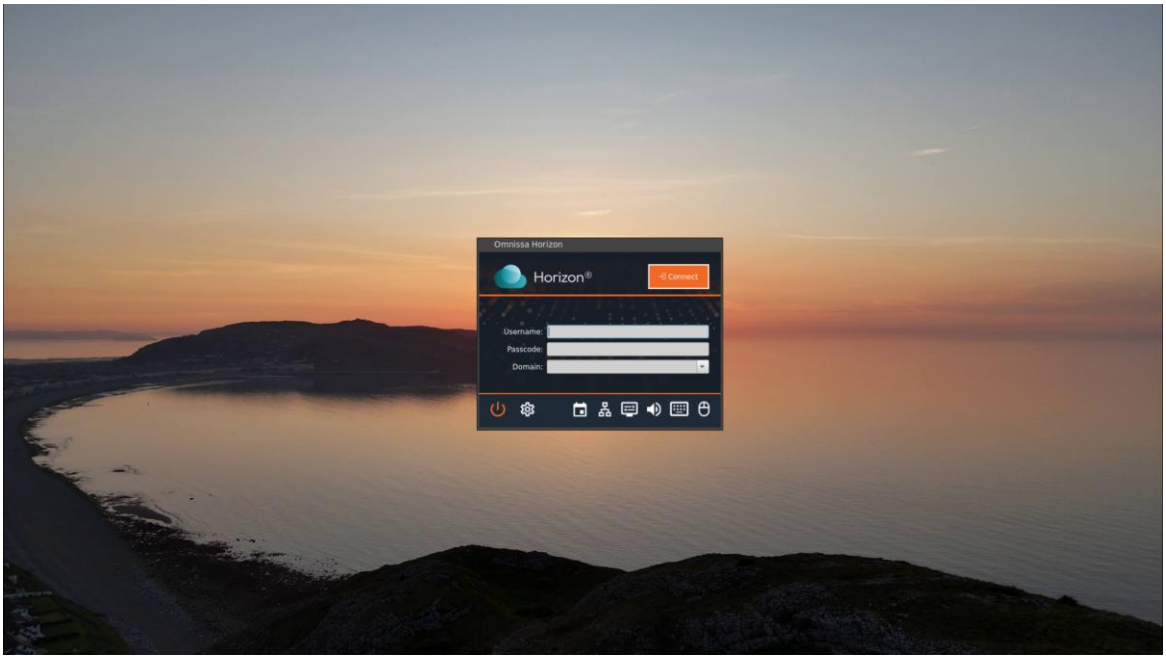
Examples of Full Desktop and NOS-O Modality after Setting the Wallpaper using a local USB key

Here are 2 examples of the new “Sunset” wallpaper that we just added, one in Full Desktop and one in a NOS-O modality.

Full Desktop



NOS-O Modality

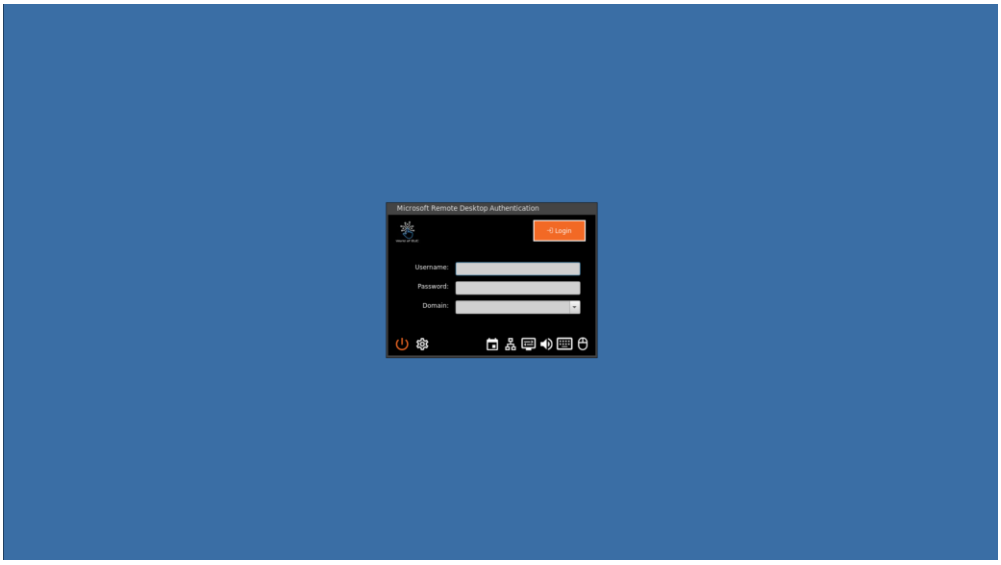


Setting the NOS Launchpad Desktop using a local USB key

This time, we'll import an image that will be used to set the "Launchpad Desktop" as seen using the NOS Modalities. This image needs to be a specific size and needs to be a resolution of 400x320, so that it fits just inside the Launchpad neatly.

We have an image on the USB key called "WorldOfEUC.jpg", so we just insert the USB key with that image on and this time select the "Desktop Image" menu option, click to highlight the "WorldOfEUC.jpg" and then click "Install". Close the "USB Installer" dialog.

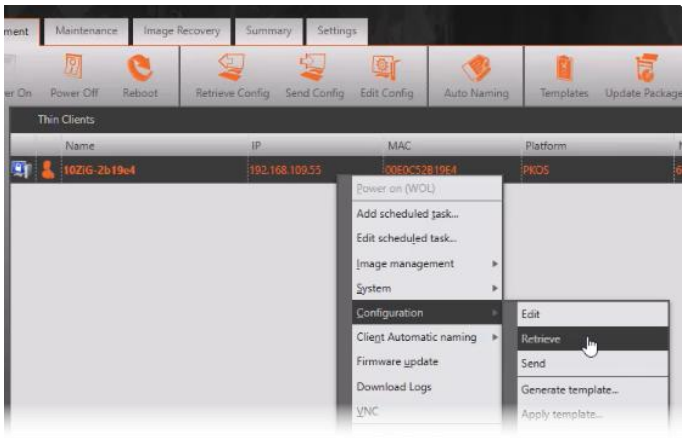
For this example, we have set the desktop to a blue color, so the "Launchpad" stands out. See below.

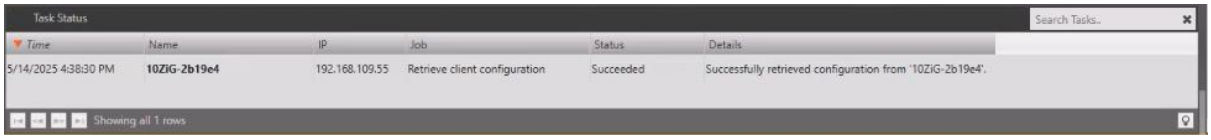


Using 10ZiG Manager to import images and deploy them to your Thin Clients

This time, we'll import the same 2 images into 10ZiG Manager and inject them into the thin client's retrieved config. Then we'll save the new config and "push" it down to the client again, setting both the "Wallpaper" and "Launchpad Desktop" at the same time.

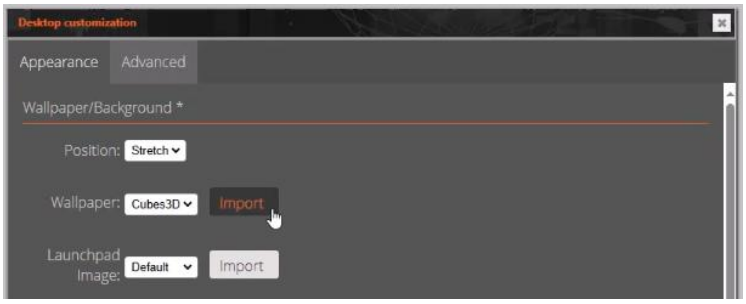
1. Inside 10ZiG Manager, right click on the thin client and then select, "Configuration" and then "Retrieve" .You will see the progress I the "Task Status" below.



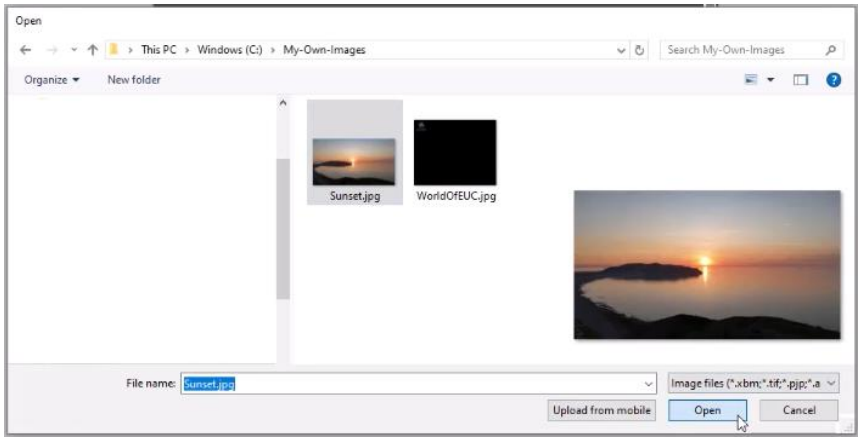


2. Next, right click the client again and select "Configuration" and then "Edit", and you should see the configuration dialog box displayed.

3. Double click on the “Desktop” applet and the “Desktop” dialog box will be displayed.
4. Next, click the “Wallpaper” Import button.

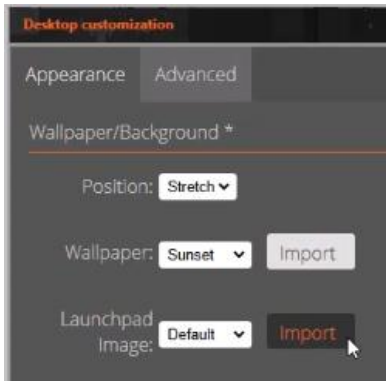


5. In the file dialog, find and highlight the “Sunset.jpg” image and click open.

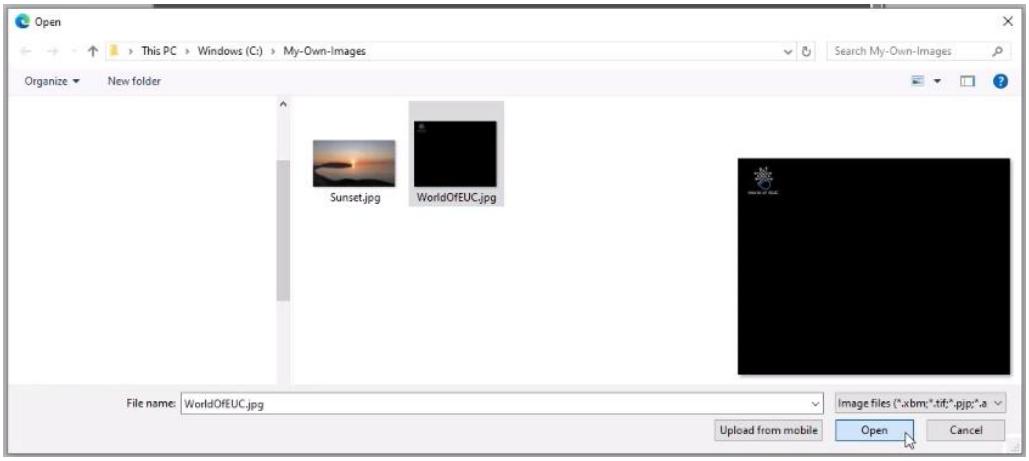


6. Next, answer “Yes” when asked if you want to import the image file.

7. Next, click the “Launchpad Image” Import button.

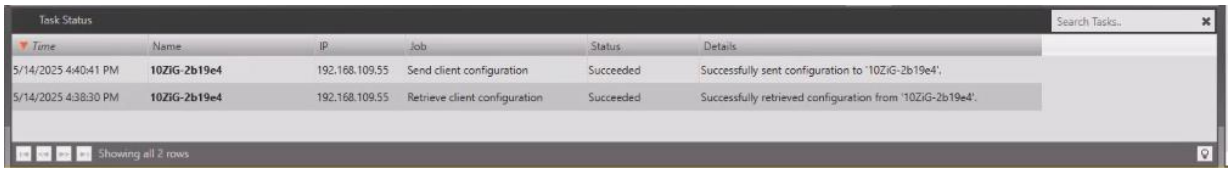


8. In the file dialog, find and highlight the “WorldOfEUC.jpg” image and click open.

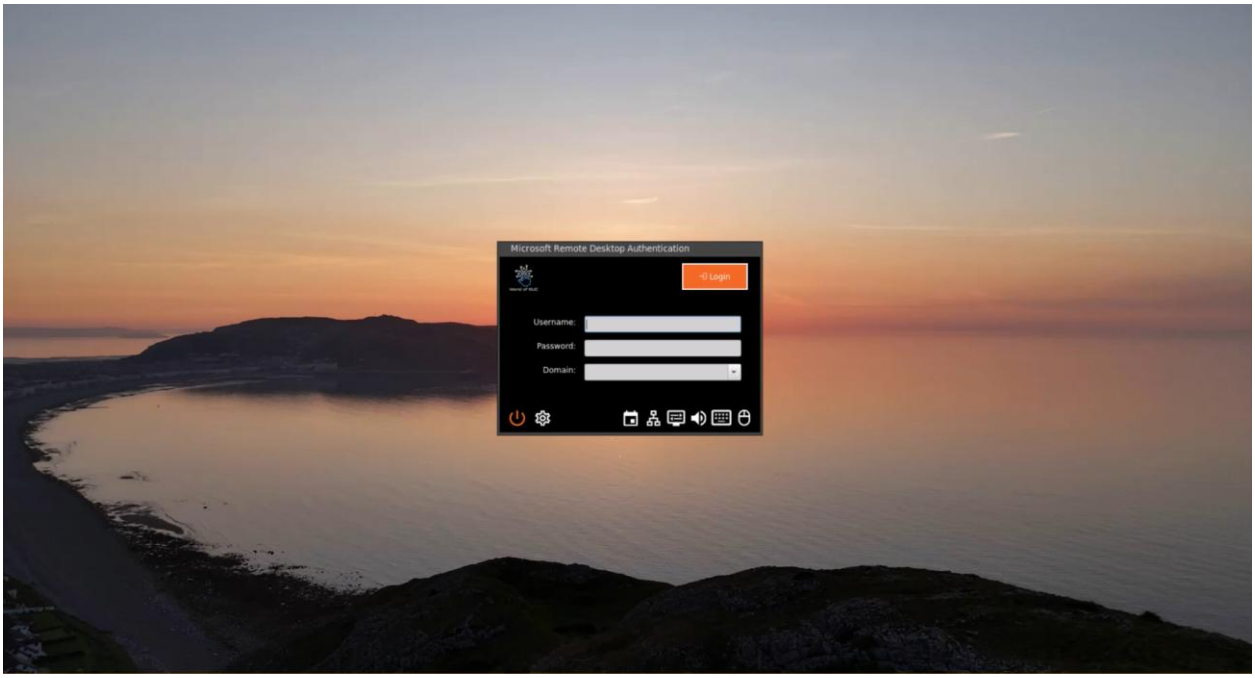


9. Next, answer “Yes” when asked if you want to import the image file again.

10. Click “OK” and then “OK” once more to save the changes.
11. When you’re asked if you want to “send the configuration now”, click “Yes”. You will see the configuration was send back to the client successfully.



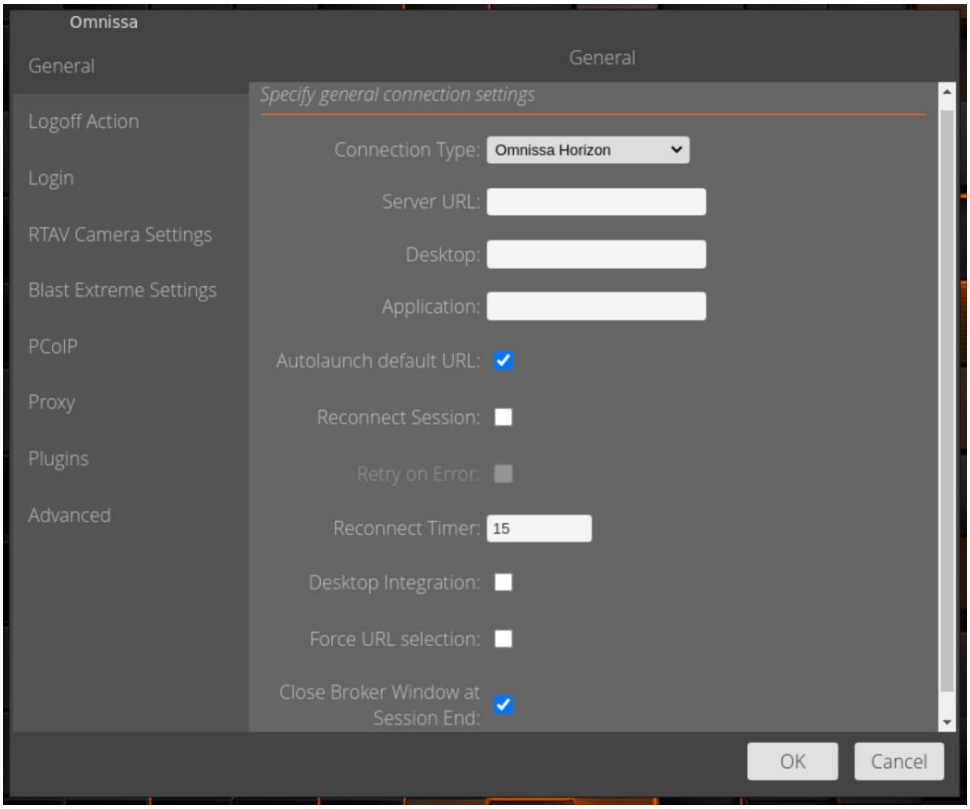
12. If we take a look at the 10ZiG Thin Client desktop, following the configuration send, you can see that we have the “Sunset” wallpaper with the “WorldOfEUC” launchpad displayed. We set this with a NOS-M modality just so you can see both in action.



NOS for Omnissa NOS-O

General

After the initial setup you will be taken to the “Omnissa Horizon Settings” screen, where you can begin to configure your Horizon connections.



- **Connection type**: The type of connection you wish to set up, either an “Omnissa Horizon” or “Omnissa Workspace One”, that can be selected in the drop-down list. Contact your system administrators for information on which is applicable to you.
- **Server URL**: Network address for your Omnissa server environment.
- **Desktop**: The name of the published Omnissa desktop you would like to connect to by default.
- **Application**: The name of the published Omnissa applications you would like to connect to by default.
- **Autolaunch Default URL:** Default URL can be specified in the Server Address Box. Disabling this will present the user with the choice of URL to select. You can have multiple URL’s for different Omnissa environments separated by a comma in the server address field.

- **Reconnect Session**: Enable this for automatic reconnection when a session is disconnected. If this is ticked then you have the option to tick the “Retry on Error” option, that will attempt reconnection if errors are detected during the Horizon connection.

- **Reconnect Timer**: The interval you would like the session attempt to reconnect (in seconds).

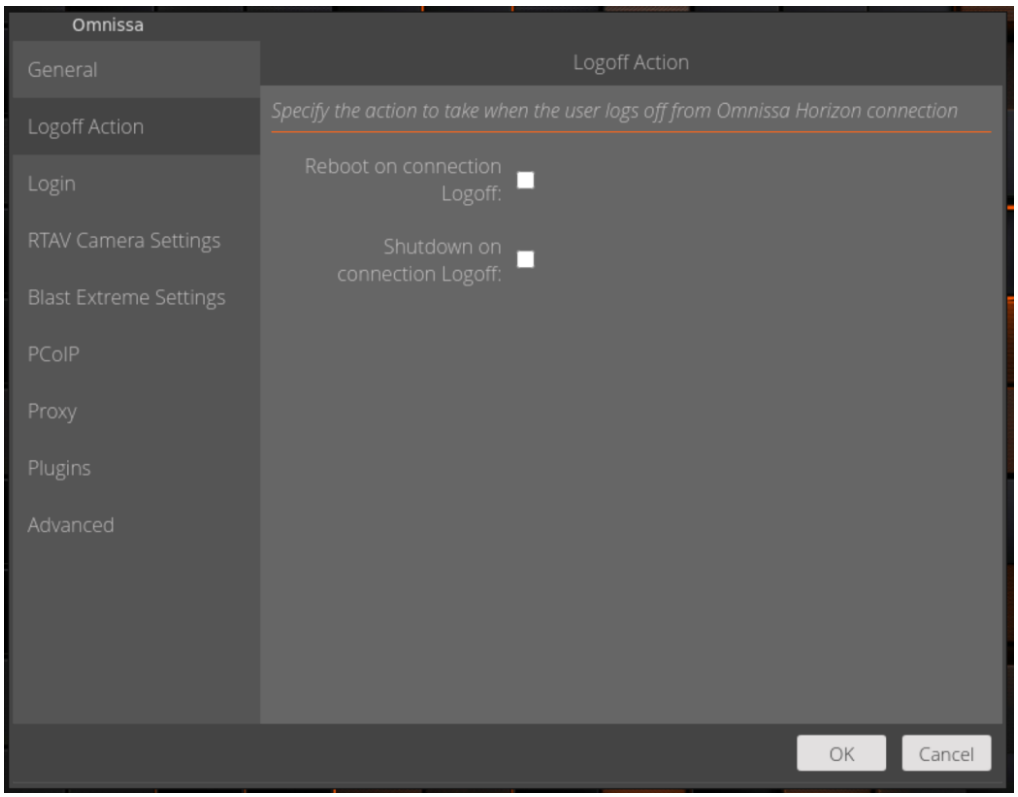
- **Desktop Integration**: Enabling this, separates Omnissa’s message prompts that usually display as a banner within the Horizon client, to a local dialog box instead. This can be useful when users are prone to entering wrong credentials – the horizon client will re-prompt for an incorrect password but usually grays out the username. With this enabled, instead you get a local dialog box that shows the status of unknown username or password and brings you back to the NOS launchpad.

- **Force URL selection**: When multiple server addresses are defined in the Server URL field (comma separated), the default behavior is to use the first URL listed. To force users to select which server to connect to, enable this option.

- **Close Broker Window at Session End**: On session logoff or password error/expiry, the Omnissa Client is closed automatically where this option is enabled.

Logoff Action

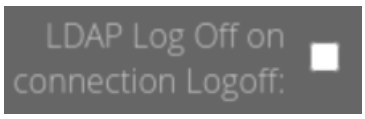
Allows you to control the behavior of the NOS-O client, following disconnect and logoff from a Horizon remote session.



- **Reboot on connection Logoff**: This will shut down and reboot the Thin Client, following logoff.

- **Shutdown on connection Logoff**: This will physically power off the Thin Client, following logoff.

  Note: If you're running your connection in "Full Desktop" mode, then you will see the LDAP Log Off on Connection Logoff field as shown below. This will allow you to logoff the "Full Desktop" if the remote desktop is logged off.



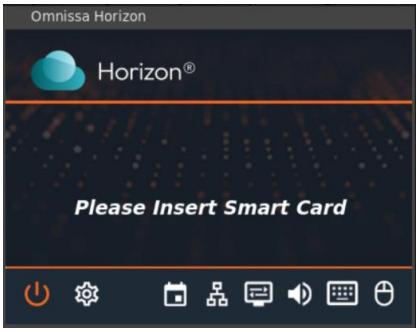
Login

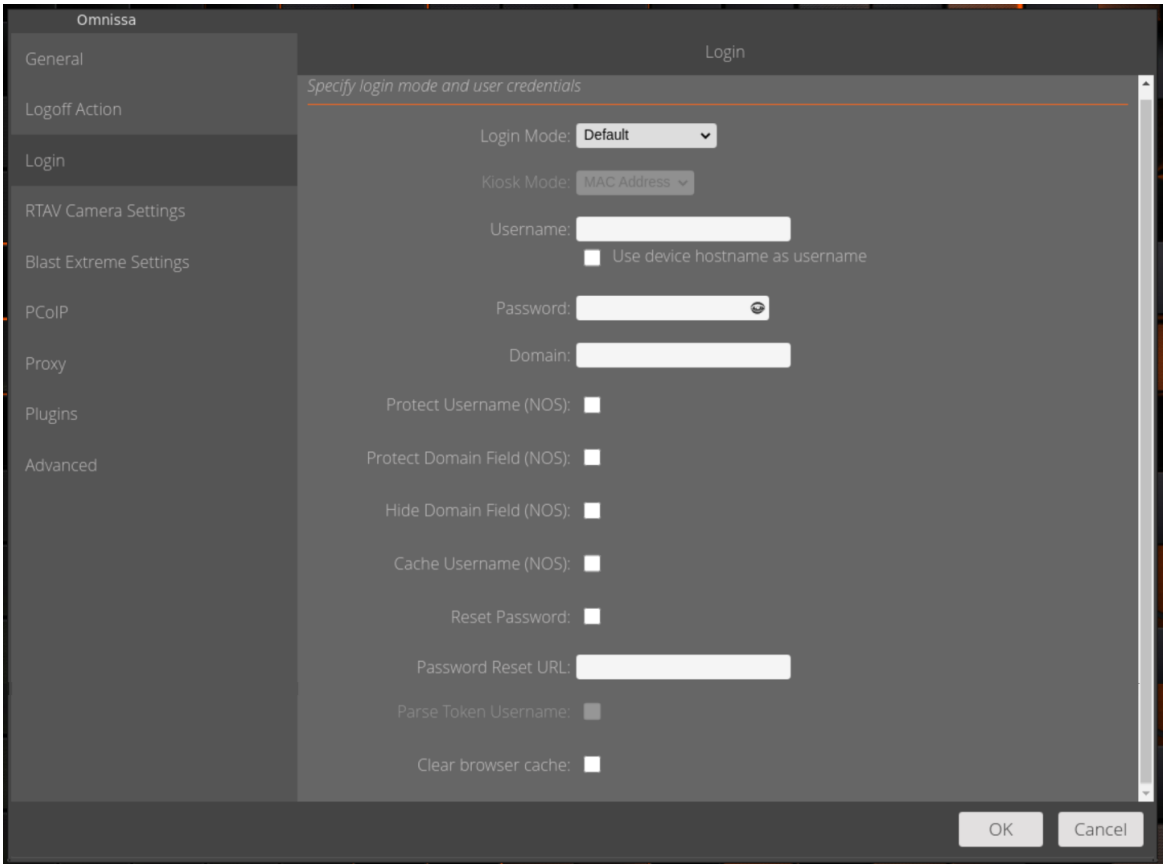
In this section of Omnissa Horizon Settings, you have the ability to fully customize the way that you want your users to login to their specific Omnissa environment that we configured earlier.

- **Login Mode**: There are several ways that you can configure the NOS-O client when it comes to logging in to your Horizon sessions. These are :-

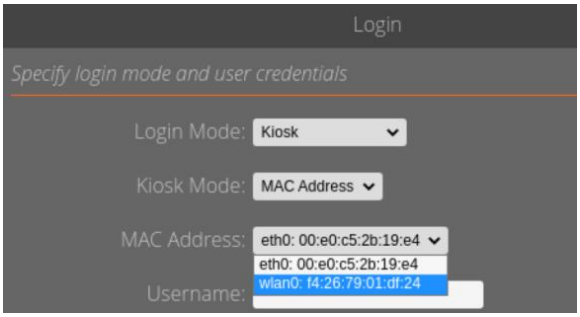
  Default, Anonymous, Kiosk, Smart Card Login, 2-Factor and SAML(Security Assertion Markup Language).

  Choosing Smart Card Login will present your users with a login screen that asks for a smart card as shown below.





- **Kiosk Mode**: If you have selected “Login Mode” to be “Kiosk”, then you will be able to select the Kiosk Mode to use the MAC address as your logging in user. If you have more than one NIC(Network Interface Card) installed in your device, then you have the ability to choose which device is your login username. See below as an example.



- **Use device hostname as username**: If you tick this box, then the device hostname will be used as the username to login with. If you already have a username in the “Username” field, then this will be greyed out and not used as the username.

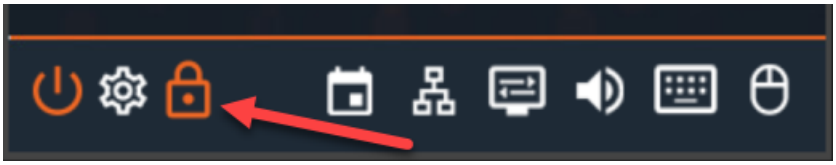
- **Protect Username**: If you have selected “Login Mode” to be “SCLogin” for smart card use, the username will be greyed out at the connect screen.

- **Protect Domain Field**: Ticking this option will disable editing of the DOMAIN field on the main login screen.

- **Hide Domain Field**: Ticking this option will hide the DOMAIN field on the main login screen.

- **Cache Username**: Enabling this, will ensure that the last logged on user is remembered for next login.

- **Reset Password and Password Reset URL**: If you tick this box and type in the address of a password reset URL in the box below it, this will be made available as a “keylock” clickable link on the login box, as pointed to by the red arrow in the image below.



Most URLs will work here, as it launches a browser and can fulfill other use cases.

- **Parse Token Username**: Where 2-Factor mode is selected under Omnissa settings and 'Parse Token Username' option is enabled, the following should be transmitted at point of login.

  Horizon-view --serverURL='horizonservername' -q --userName='username' --passcode='password'

  Note: The following commands are used in place of a 'Default' login. The usage in this scenario of --userName vs --tokenUserName causes the Horizon client to cache the username field, so that the user is only required to enter their username once during login. Where as in scenario #1, the user is required to enter the username twice.

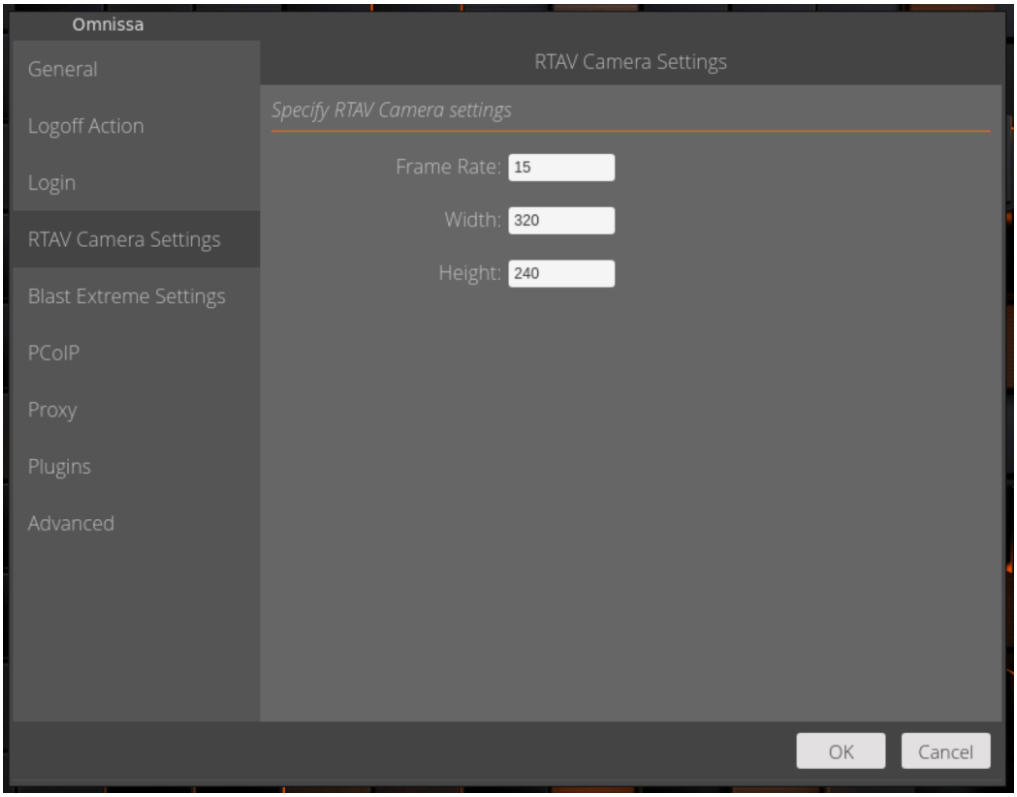
  --passcode replaces –password as used in 'Default' login scenario.

- **Clear browser cache**: This prevents caching of details in password reset browser window.

Note: If you're running your connection in "Full Desktop" mode, then you will see an additional "Login Mode" of LDAP Credentials. This will allow you to use your network domain credentials to log in.

RTAV(Real Time Audio and Video) Camera Settings

In this section of Omnissa Horizon Settings, you have the ability to customize and set thresholds for the Video being passed from the 10ZiG Thin Client to the remote Omnissa VDI desktop.

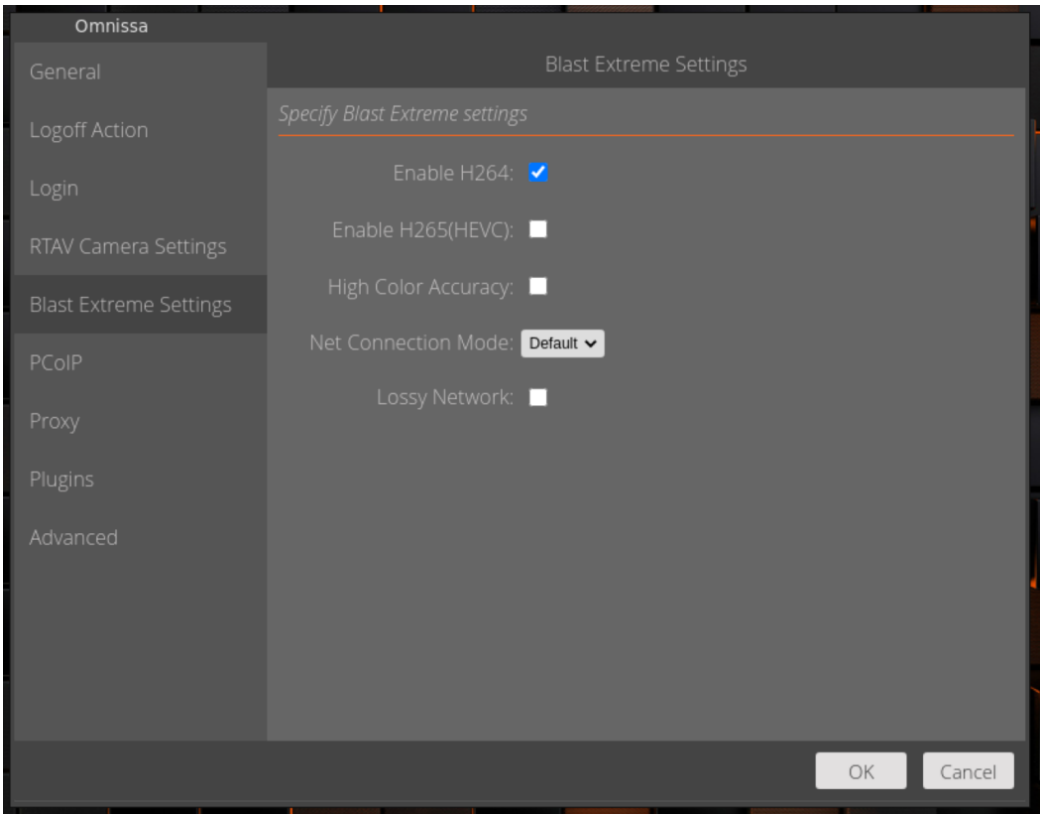


- **Frame Rate**: The number of frames per second that RTAV will transmit to the virtual desktop. The example above shows the client transmitting video at a rate of 15 frames per second (FPS). RTAV is an Omnissa virtual channel for transmitting Audio/Video. This allows you to control the Frame rate for the video feed. Omnissa only supports a maximum of 25 FPS, and it is limited to what the webcam can actually offer, as well as the endpoint and what the resolution of the webcam is set to.

- **Width and Height**: Changing these settings will determine the quality of the video being transmitted to the virtual Omnissa desktop.

Blast Extreme Settings

In this section you have the ability to customize options for the Blast Extreme display protocol. This enables you to tweak the protocol to take best advantage of your user's operating environment, especially where network conditions are less than favorable.



- **Enable H264**: This is set by default and should ideally be left as enabled, as it's an industry standard in video compression, and delivers a quality video compression that's more than adequate for most use cases.

- **Enable H265(HEVC)**: If your infrastructure has limitations regarding bandwidth but requires a more improved, lossless video stream, then consider switching this on, as it has higher compression rates without visible deterioration of video quality.

  Note: that this option requires the appropriate NVIDIA hardware on the server side and equivalent client side (6048qv/6148v). Consult NVIDIA documentation for further information.

- **High Color Accuracy**: If your users require certain text and images to be delivered with greater clarity, then they can switch HCA on.

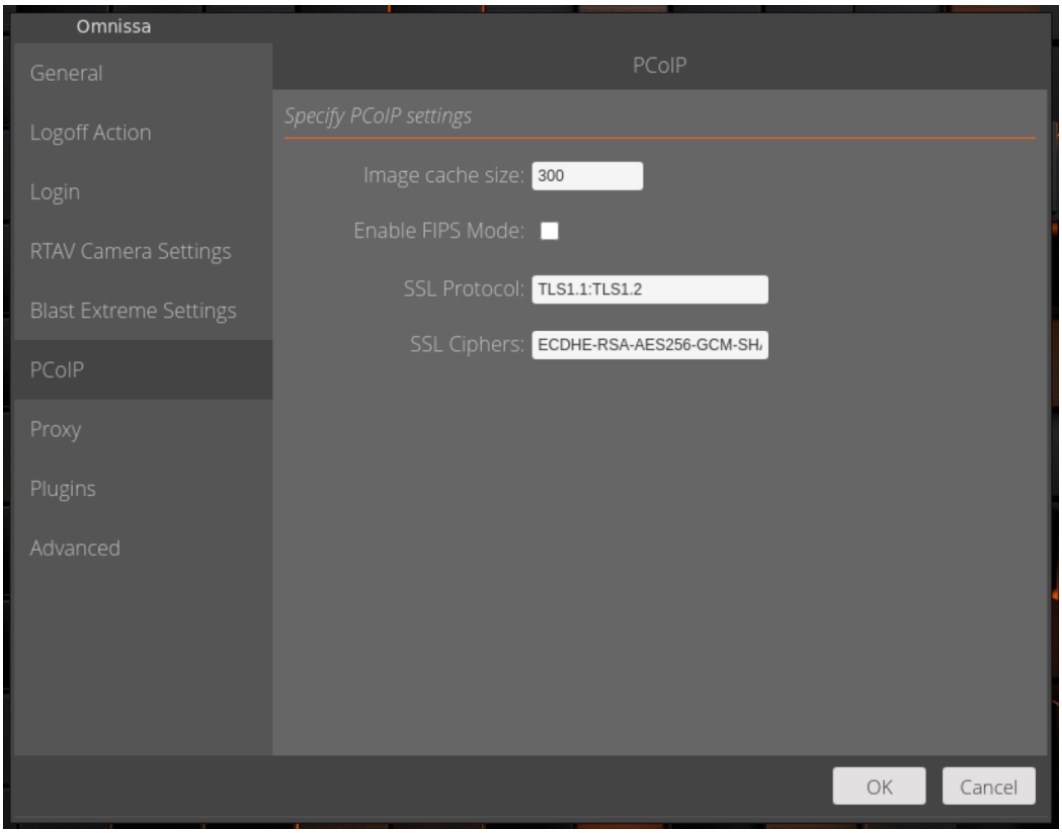
  Note: This option is decoded via CPU and hardware decoding not supported. This is generally not recommended on lower powered hardware. The 6048qv or more powerful hardware is required as a minimum.

- **Net Connection Mode**: Unless you require a specific mode for a particular use case, leave this as default, as Blast Extreme will then determine the best mode for efficient and accurate delivery of data.

- **Lossy Network**: Enable this feature when packet loss on the network is 20% or greater.

PCoIP

In this section you have the ability to customize options for the PCoIP display protocol.



- **Image cache size**: PCoIP client-side image caching stores image content on the client to avoid retransmission. This feature is enabled by default to reduce bandwidth usage. Physical system memory should be taken into consideration when changing this setting.

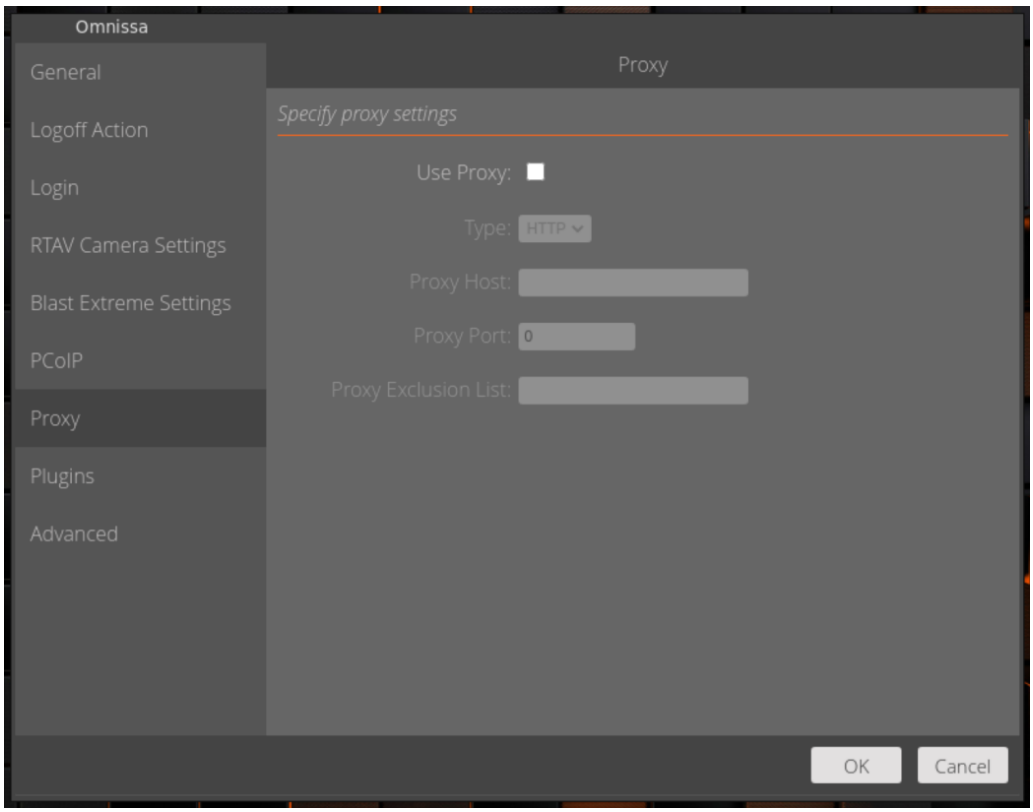
- **Enable FIPS Mode**: You can enable FIPS (Federal Information Processing Standard) Compatible mode so that the client uses FIPS-compliant cryptographic algorithms when communicating with remote desktops.

- **SSL Protocol**: Use this to set the SSL protocols to be used by the PCoIP connection. The defaults are TLS1.1 and TLS1.2

- **SSL Ciphers**: Use this to modify the list of SSL ciphers that you want to include in your secure SSL connection strings for authentication.

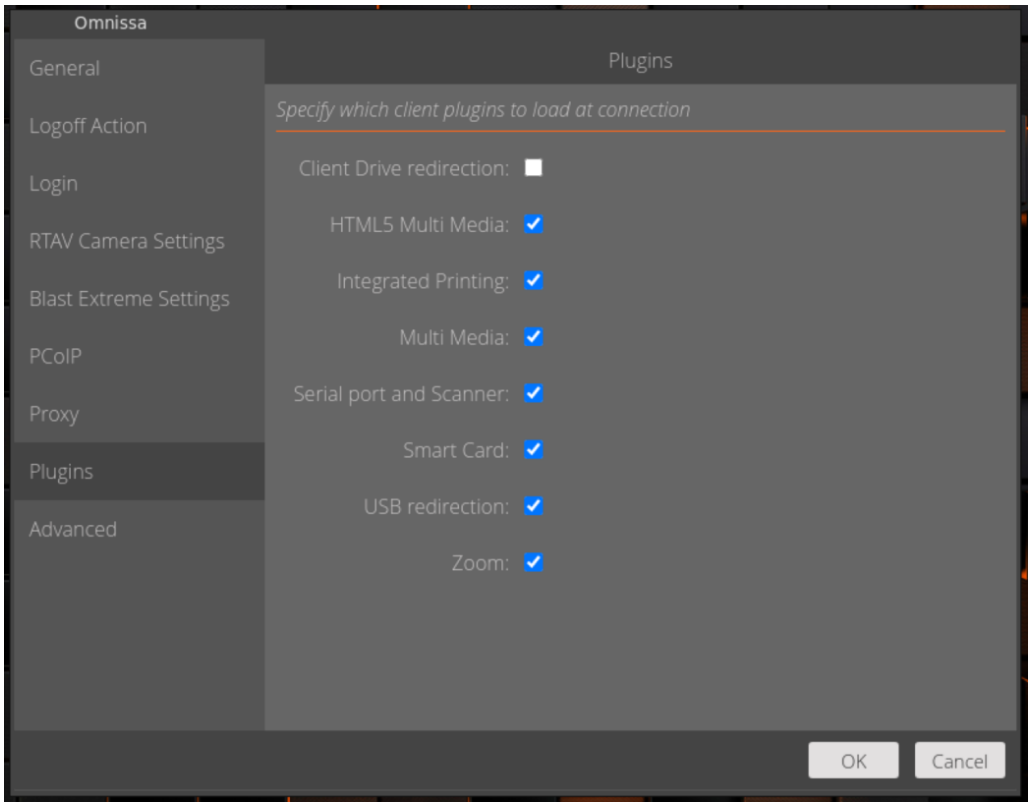
Proxy

If your network is set to use a Proxy, here is where you will type in the connection information.



- **Use Proxy:** Enables Proxy connection.
- **Type:** Defaults to HTTP
- **Proxy Host:** Type in the proxy host IP or hostname.
- **Proxy Port:** Assign port number.
- **Proxy Exclusion List:** If you have multiple sites or addresses that you wish to bypass the proxy, then type them in here and use a comma to separate the list of exclusions.

Plugins

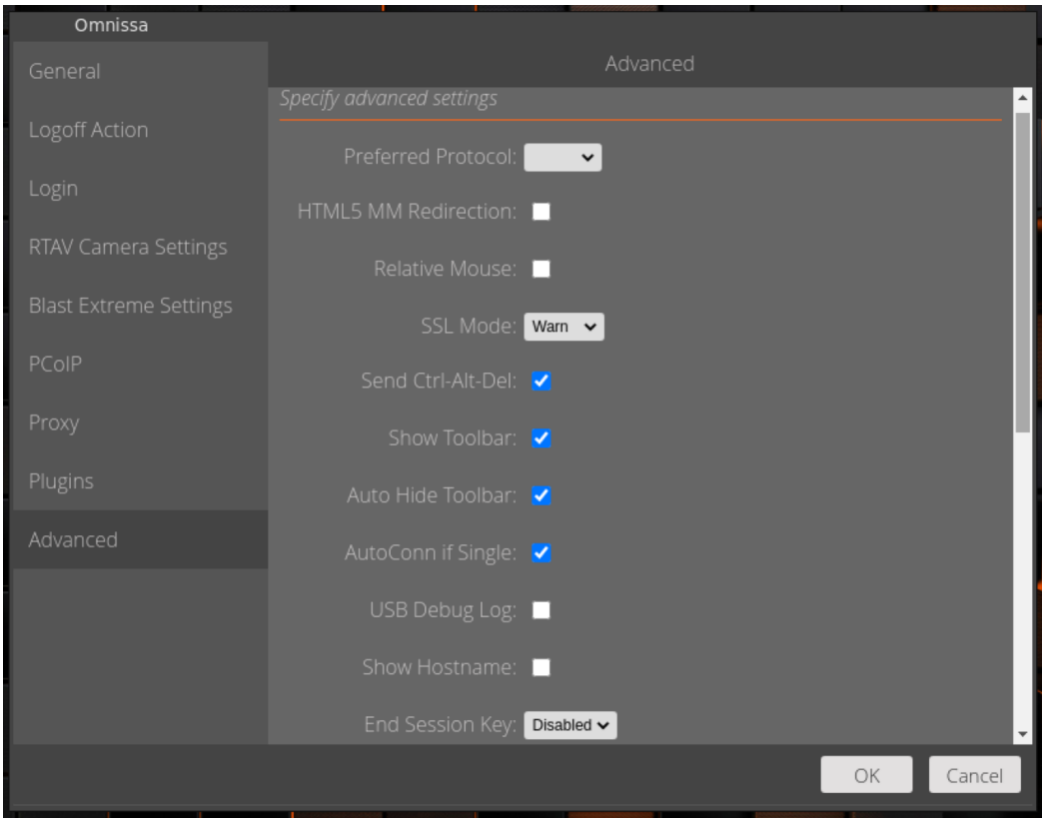


- Plugins (various): This tab gives administrators the ability to enable (default) or disable the various plugins or virtual channels the Omnissa horizon client can utilize.

  Although, many of these can be enabled/disabled on the agent side, it can be useful to disable it on the client side, if users are connecting to multiple environments that don't have the same policies applied or weren't configured the same.

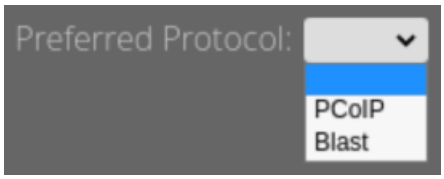
Advanced

The Advanced section of the “Omnissa Horizon Settings” allows additional customization to be carried out.



- **Preferred Protocol**: You can specify the communication protocol you use to connect to your VDI. Setting the protocol on the client should take precedence over the default protocol set for the desktop pool because the pool setting in horizon administrator console must allow the user to select which protocol they wish to use.

  Easily confirm the protocol selected, by launching Omnissa Horizon Performance Tracker on the desktop you connected to, and the protocol should show either PCoIP or Blast.



- **HTML5 MM Redirection**: With HTML5 Multimedia Redirection, if an end user uses the Google Chrome or Microsoft Edge browser in a remote desktop, HTML5 multimedia content is sent to the client system, which reduces the load on the ESXi host. The client plays the multimedia content, and the user has a better audio and video experience.

  Consult Omnissa Horizon documentation for further guidance on enabling this functionality Agent side.

- **Relative Mouse**: If you use the Blast display protocol or the PCoIP display protocol when using 3D applications in a remote desktop, mouse performance improves when you enable the relative mouse feature.

  In most circumstances, if you are using applications that do not require 3D rendering, the Horizon Client transmits information about mouse pointer movements by using absolute coordinates. Using absolute coordinates, the client renders the mouse movements locally, which improves performance, especially if you are outside the corporate network.

  For work that requires using graphics-intensive applications, such as AutoCAD, or for playing 3D video games, you can improve mouse performance by enabling the relative mouse feature, which uses relative, rather than absolute, coordinates.

- **SSL Mode**: Used for verifying/bypassing the connection server certificate.
  Accept – This will ignore server certificate validation (This is least secure and not recommended)

  Warn – When connecting to a server with a self-signed certificate will prompt to connect, view certificate, or cancel.

  If connecting to a server with a certificate signed by a CA, it will proceed if the signing CA certificates are installed on the client system, or it will present an SSL error stating the connection is untrusted and the user will be unable to connect. (default)

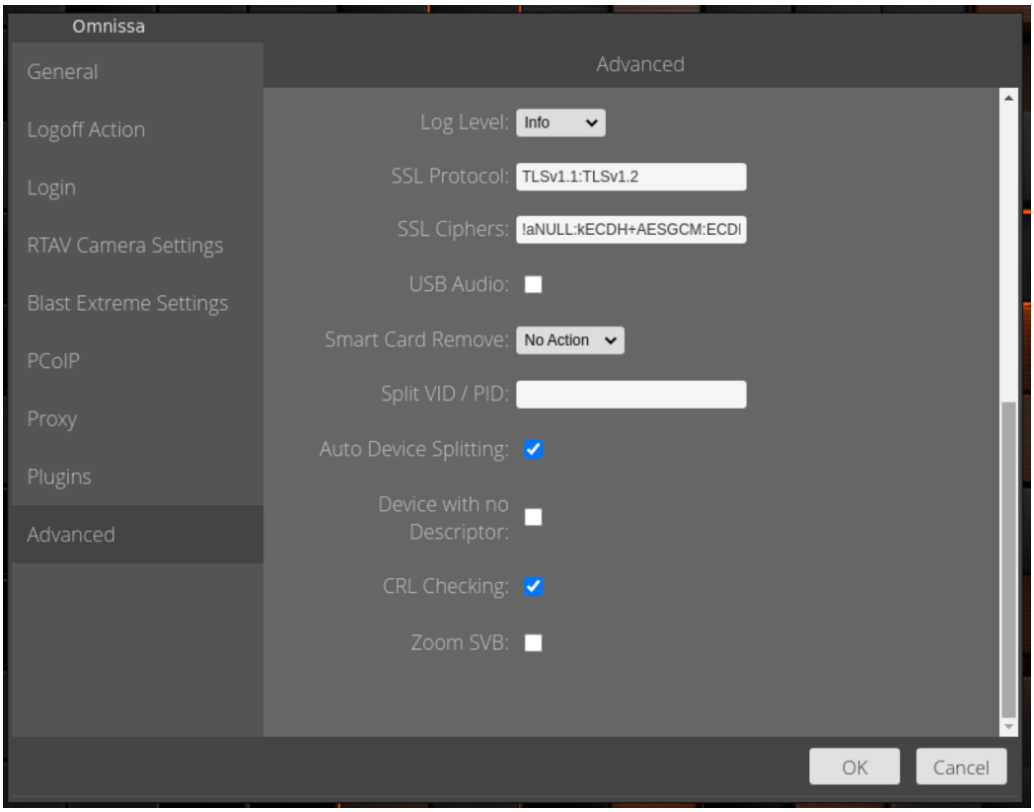
  Reject – signing CA certificates must be installed on the endpoint device or an SSL error will be present, and the user will be unable to connect. (This is the most secure option)

- **Send Ctrl-Alt-Del**: If enabled, when the user presses CTRL ALT DEL on the Thin Client, it will send the key combination to the Windows virtual desktop and present the windows security screen. When disabled, it will present the user with the options to: Send CTRL ALT DEL, Disconnect, or Cancel. This option is enabled by default.

- **Show Toolbar**: This allows you to show the Omnissa menu bar dropdown when in the session. The Omnissa tool bar will be accessible in session, pinned at the top of the screen.

- **Auto Hide Toolbar**: Auto Hide the toolbar when enabled. The Omnissa toolbar will automatically be unpinned (hidden) while in session.

- **AutoConn if single**: Switching this option, will enable automatic connection if just one desktop is assigned to the logging in user.
- **USB Debug Log**: Enable USB Tracing
- **Show Hostname**: Enabling this option will display the host name of the client inside the Horizon Authentication login screen. It is useful for end users who can provide 10ZiG Manager administrators with the hostname required for shadowing their session.
- **End Session Key**: Allows you to configure a hotkey to disconnect the session. Set this option to CTRL-F12 to give users the ability to quickly disconnect their VDI session. This will also close the Omnissa broker, regardless of whether the "Connect Once" option is enabled or not.



- **Log level**: Configure the logging level for the Omnissa Horizon Client. Options are All, Trace, Debug, Info, Warning, Error and Fatal.
- **SSL Protocol**: Supported versions of SSL protocol that are used.
- **SSL Ciphers**: Supported Cyphers used by the Horizon Client connection

- **USB Audio**: Enabling this option disables RTAV and allows the redirection of USB audio devices via USB Redirection. This option should only be enabled by system administrators and is generally advised by 10ZiG not to enable it.

- **Smart Card remove**: Can be configured to “No Action” or “Disconnect” depending on the desired behaviour. Used with smart card login (see Smart Card Service applet > Advanced > Enable Smart Card Login). However, the setting on the Horizon Connection Server takes precedence.

- **Split VID / PID**: Allows for the splitting of USB Composite devices which have multiple interfaces on the same VID/PID. In general, USB redirection is not needed for standard functionality such as audio, video, HID input, etc. However, in some special circumstances, a device may need to be redirected into a VDI session for full functionality, or if it requires a specific driver to function. Further information can be found under Omnissa Horizon documentation under the section ‘Configuring Device Splitting Policy Settings for Composite USB Devices’ https://docs.omnissa.com/bundle/Horizon-Remote-Desktop-FeaturesV2406/page/ConfiguringDeviceSplittingPolicySettingsforCompositeUSBDevices.html

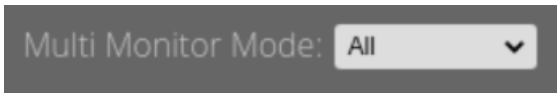
- **Auto Device Splitting**: If enabled, this attempts to perform as above in “Split VID/PID”, automatically without user input.

- **Device with no Descriptor**: This allows the device to be redirected even if the Horizon Client fails to get the device descriptors.

- **CRL checking**: This allows the device to check for a CRL or Certificate Revocation List from a Certificate Authority(CA), to prove that any existing certificates are still valid or have been revoked before they are due to expire. It’s a recommendation to disable this option where CRL checking is not possible. For example, behind a private or air gapped network without access to public CRL’s.

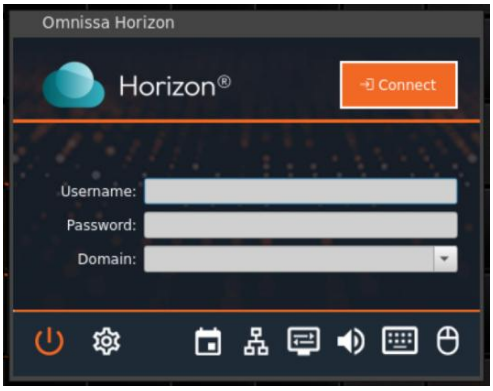
- **Zoom SVB**: Enable the override to allow for the use of Smart Virtual Backgrounds with Zoom Optimization inside the virtual desktop. Only recommended for performance devices due to the resources this requires.

  Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional field “Multi Monitor Mode”, allowing you to specify additional monitor setups for additional monitors.



Saving your settings

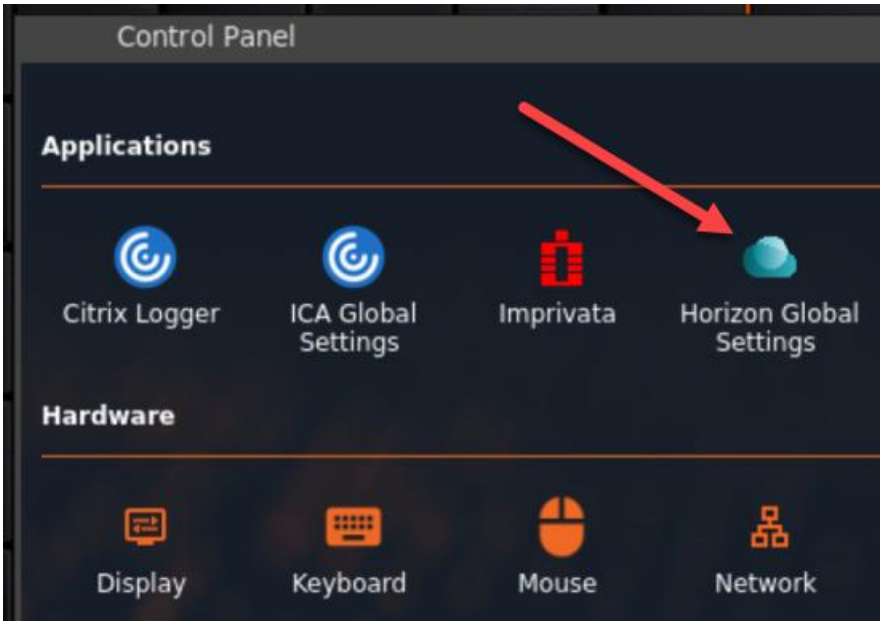
Once you're comfortable with all the settings for your 10ZiG NOS-O client, just click the "OK" button and you'll be taken back to the Horizon login screen.



Editing your connection settings

If you need to go back into your settings for your client connection at any time, then just click the "Gear" icon in the bottom left of the login screen, indicated here with the "red arrow" below.

Once inside the "Control Panel", just click the "Horizon Global Settings" icon and you'll be taken back into the "Settings" console again.

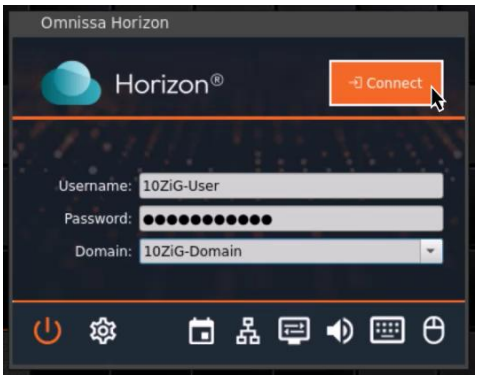


Omnissa Horizon Connection Examples

Here are a few examples of what your connection box might look like, along with the settings required to enable them.

Keyed-in credentials

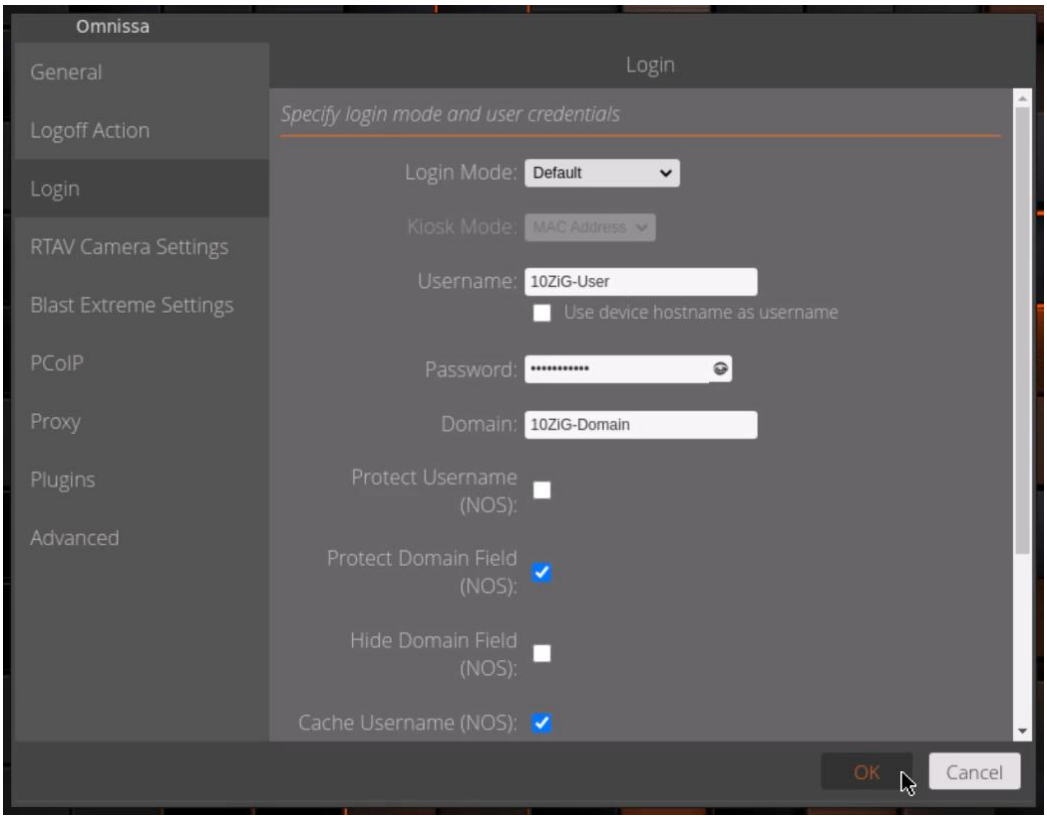
Here, we just key in the credentials and click “Connect”.



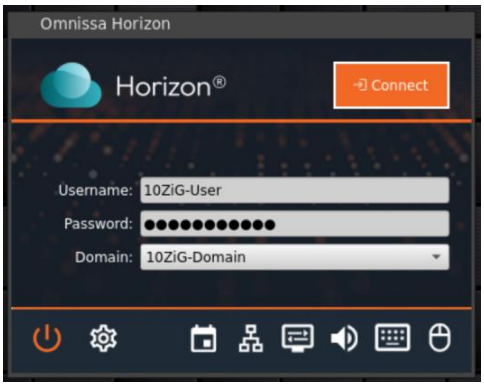
Caching credentials and protecting the domain

Go into the “Horizon Global Settings” inside the “Control Panel”, select login on the left menu and then key in the Username, Password and Domain.

Once you’ve done that, tick “Protect Domain Field”, “Cache Username”, click “OK” and then close the “Control Panel”.



The login box should look something like below :-



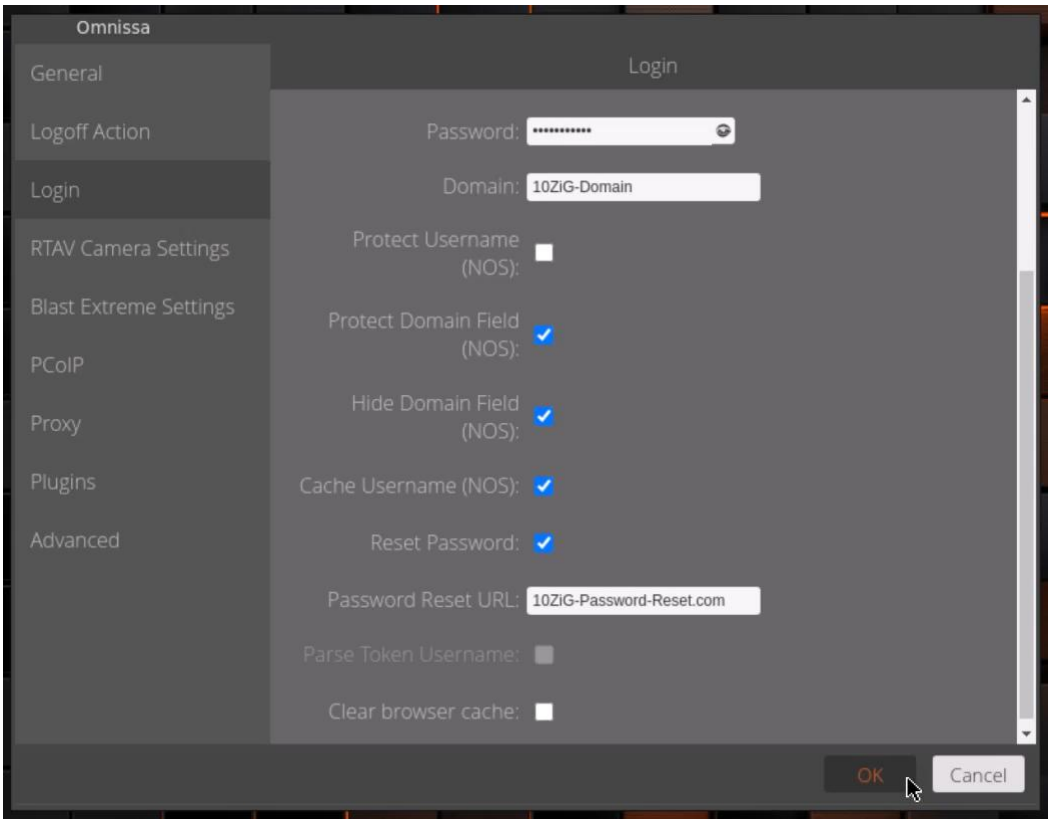
Notice that the Domain field is now presented as a drop down selection and cannot be typed into.

Enabling Password reset link and hiding the domain

Go into the “Horizon Global Settings” inside the “Control Panel”, select login on the left menu and then click “Hide Domain Field”.

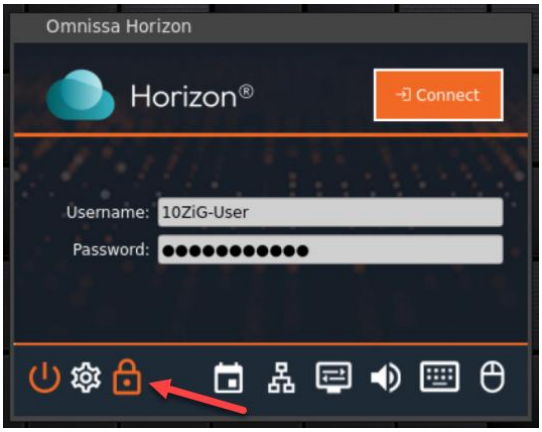
Once you’ve done that, tick the box named “Reset Password” and then type in the URL of your company’s reset password page as shown.

Click “OK” to save then changes and exit the control panel.



Notice that the login box now has a new keylock icon on there. Pointed to by the “Red Arrow” below.

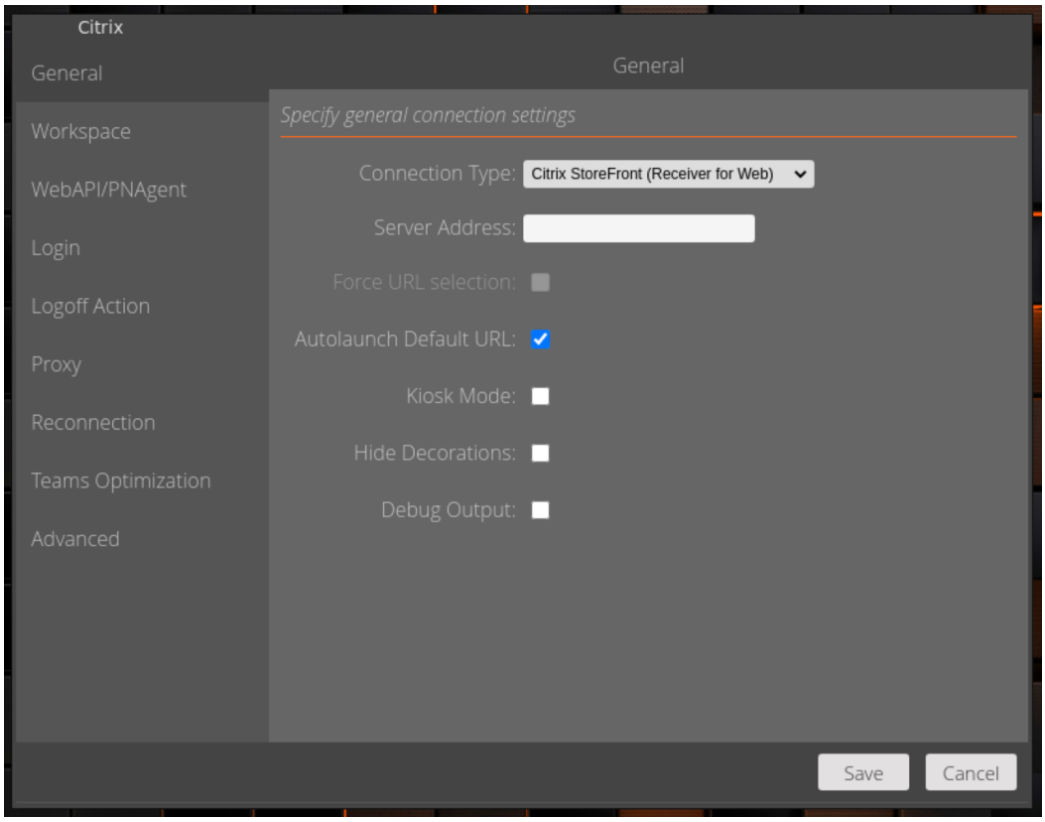
Clicking this will open the site that you completed above in the “Password Reset URL”.



NOS for Citrix NOS-C

General

After the initial setup you will be taken to the “Citrix Settings” screen, where you can begin to configure your Citrix connections.



- **Connection type:** You have several ways in which to connect to your Citrix environment, these are listed in the dropdown. Options available are :-

  Citrix Workspace(Self-Service), Citrix Storefront(Receiver for web) and WebAPI(Formerly PNAgent/Services).

  Contact your system administrators for information on which is applicable to you.

- **Server Address:** Type in the IP or FQDN(Full Qualified Domain Name) server address of the Citrix server.

- **Force URL Selection**: When multiple server addresses are defined in the Server URL field (comma separated), the default behavior is to use the first URL listed. To force users to select which server to connect to, enable this option.

- **Autolaunch Default URL**: Default URL can be specified in the Server Address Box. Disabling this will present the user with the choice of URL to select. You can have multiple URL's for different Citrix environments separated by a comma in the server address field.

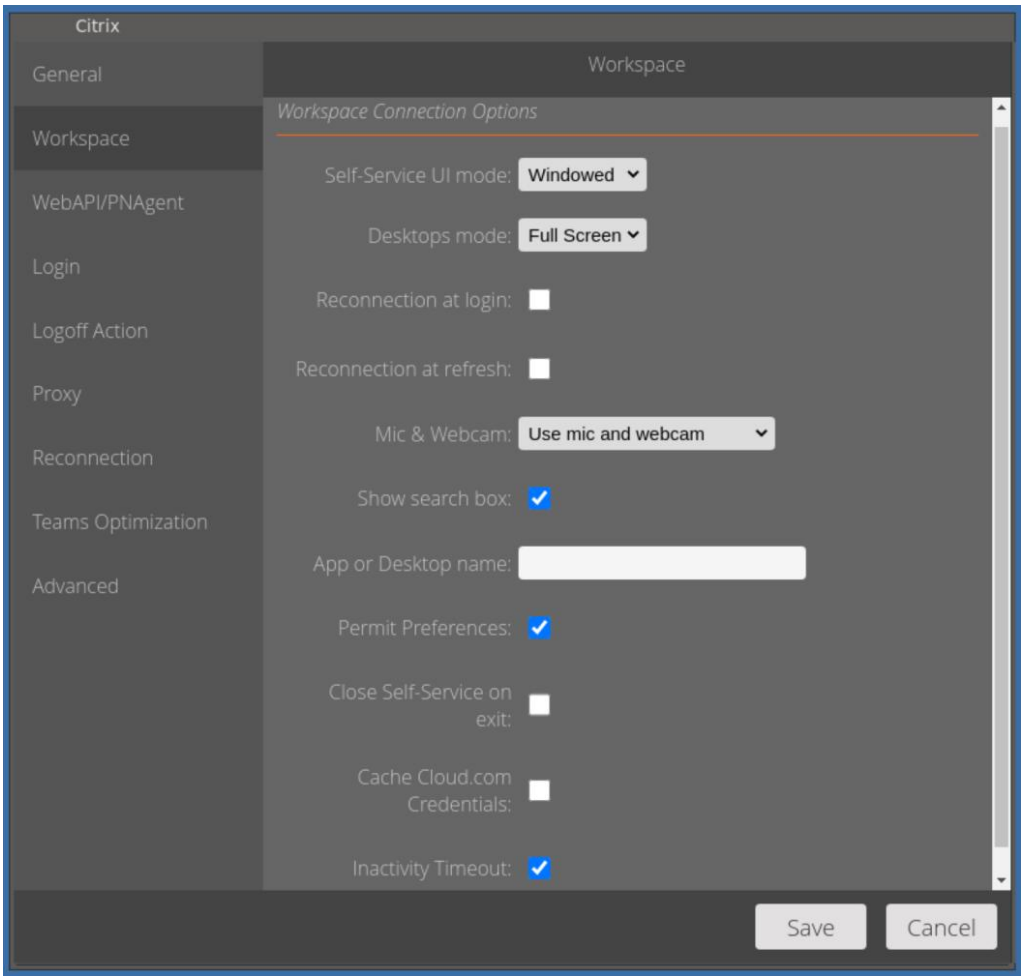
- **Kiosk Mode**: Enabling this option hides the local Thin Client desktop launchpad. This option should only be used with "Receiver for Web". Verify the launchpad is hidden when enabled. Note: Administrators can bring the launchpad back by pressing CTRL+ALT+M

- **Hide Decorations**: Enabling this feature hides the quit option from the Web Browser, when using "Receiver for Web" connection type. Verify the top bar and quit button are not shown when using the "Receiver for Web" connection.

- **Debug Output**: Enabling this option displays a live debug Window in the Citrix session top right hand corner and provides live metrics from the session. Not available with "Citrix Workspace(Self-Service)" connection type.

Workspace

This section enables you to customize the session setup for your Citrix Workspace connections and are only applicable when using the “Self-Service” connection type defined under “General”.



- **Self-Service UI mode**: The two options when connecting in “Self-Service” mode are Windowed(default) or Full screen.
- **Desktops mode**: This option lets you determine if the Citrix desktops will be opened in a window or full screen.
- **Reconnection at login**: This will reconnect to your previous existing session when logging back in to Citrix.
- **Reconnection at refresh**: When refreshing the desktops, re-launch the disconnected Citrix session.

- **Mic and Webcam**: This option allows you to pass through the Mic and Webcam to the Citrix desktops once connected.

- **Show search box**: Enabling this feature will display a search box when logged in to Citrix to search for desktops/applications available to the user.

- **App or Desktop name**: This is the name of the default app or desktop that you wish to launch when the Citrix session starts.

- **Permit Preferences**: Permit Citrix Workspace App preferences. When enabled and logged into the Citrix Workspace App go to cog icon (workspace app settings) and select Preferences - the preferences window should open.

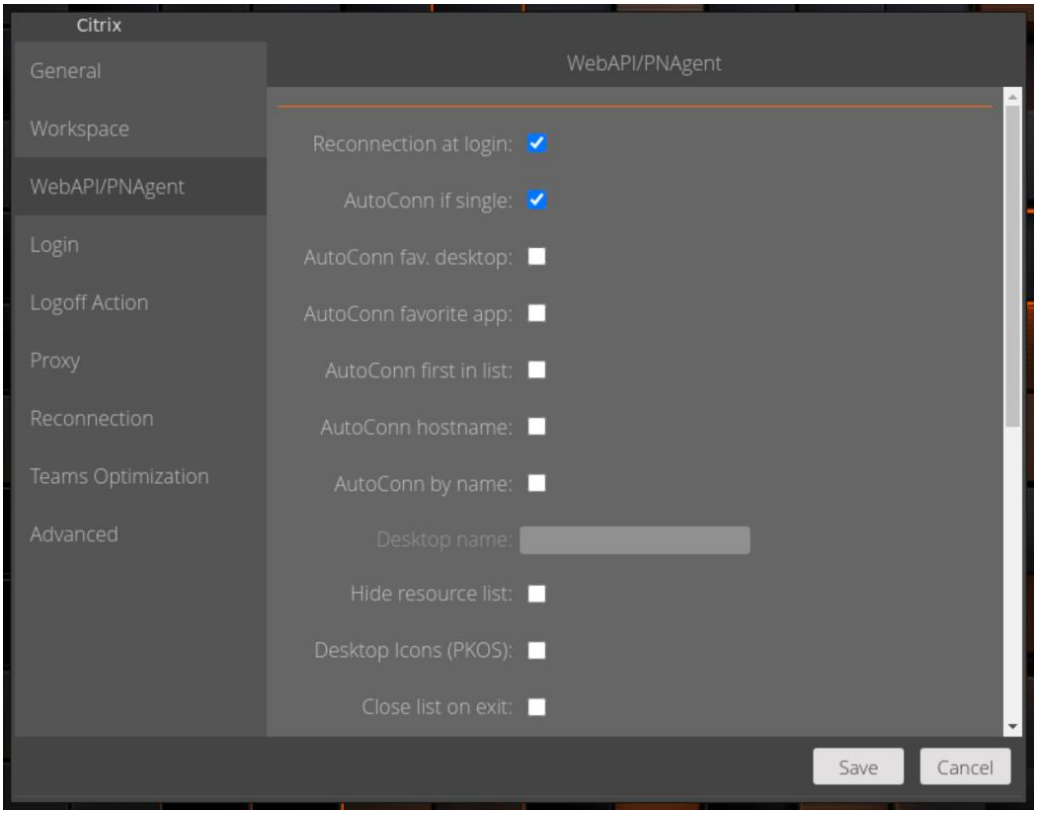
- **Close Self-Service on exit**: This will close the list of available Desktops/Applications when the user disconnects/logs off the session.

- **Cache Cloud.com Credentials**: Enable this option to cache the last logged on user's credentials when connecting to a Citrix cloud environment. Cached credentials will persist following a reboot and won't require the user to reauthenticate, based on the timeout policy set in the Citrix cloud admin console. This option is disabled by default, credentials are not cached, and users need to authenticate each time they launch the Citrix Workspace App (Self Service Connection).

- **Inactivity Timeout:** Enabling this feature here will switch on the "Inactivity Timeout" option for the Workspace App. Once inside the Workspace App, you can set the time before the Citrix session signs your users out.

WebAPI/PNAgent

This section enables you to customize the session setup for your Citrix Storefront(WebAPI/PNAgent) connections and is only applicable to this particular Citrix Storefront connection type as defined in “General”.



- **Reconnect at login**: Switching this option, will enable automatic session reconnection after StoreFront/PNAgent authentication.
- **AutoConn if single**: Switching this option, will enable automatic connection if just one desktop is assigned to the logging in user.
- **AutoConn fav. desktop**: Switching this option on will enable automatic connection to the first favorite desktop assigned to the logging in user. (StoreFront WebAPI only)
- **AutoConn favorite. app**: Switching this option on will enable automatic connection to the first favorite application assigned to the logging in user. (StoreFront WebAPI only)
- **AutoConn first in list**: Switching this option on, will enable automatic connection to the first desktop in the list of assigned desktops to the logging in user.
- **AutoConn hostname**: This will enable automatic connection to the desktop with a description that matches the Thin Client hostname.

- **AutoConn by name**: This will enable automatic connection to the first desktop with a description that matches the specific string in the “Desktop name” field below it.

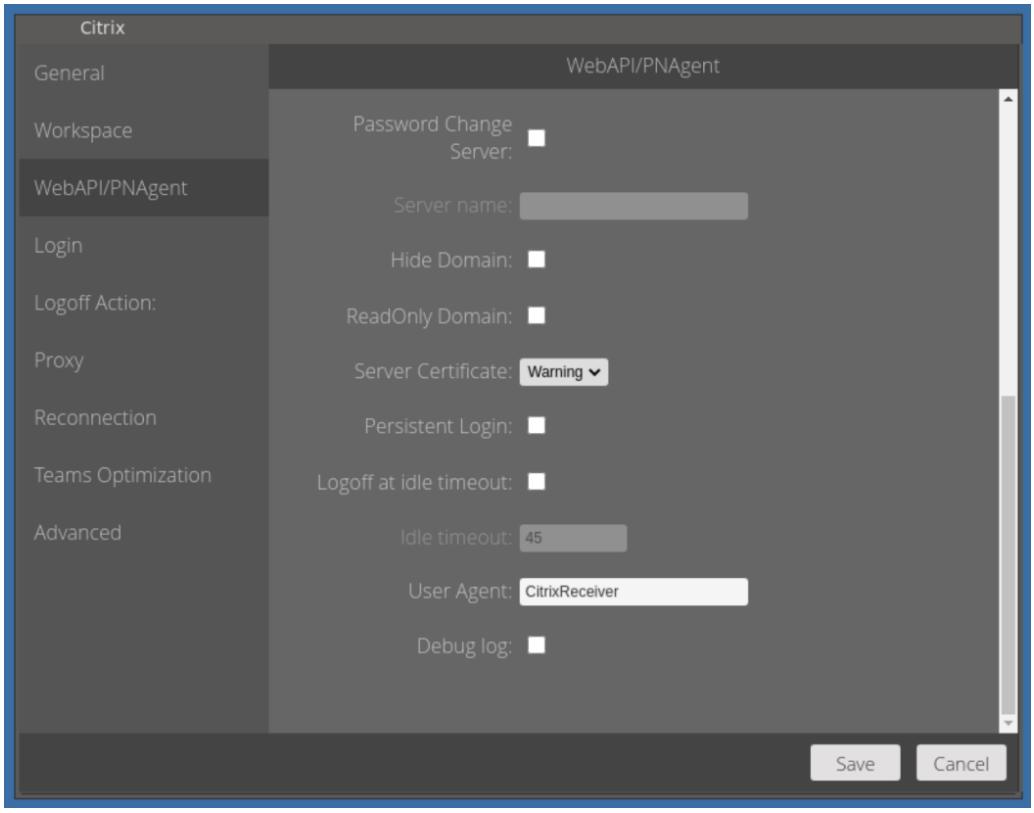
- **Desktop name**: This is the name of the desktop that will be matched against when ticking the “AutoConn by name” field above it. Wildcards allowed in this field are * and ?.

- **Hide resource list**: This will hide the desktop and app resource icon container after authentication has taken place. To be used with one of the AutoConn options above (otherwise you log in and nothing happens)

- **Desktop icons(PKOS)**: If you’re using a PKOS operating system, once authenticated to your Citrix Session, the available resources will be added as shortcuts to the PKOS desktop.

- **Hide Taskbar list menu**: To be used with SideBar/TaskBar. After logging in through WebAPI/PNAgent, Citrix has an extra icon in SB/TB which can be clicked to access a menu. Verify with this enabled that the menu icon in the SB/TB is hidden after logging in.

- **Close list on exit**: This will close the desktop and app resource icon container after disconnect/logoff.

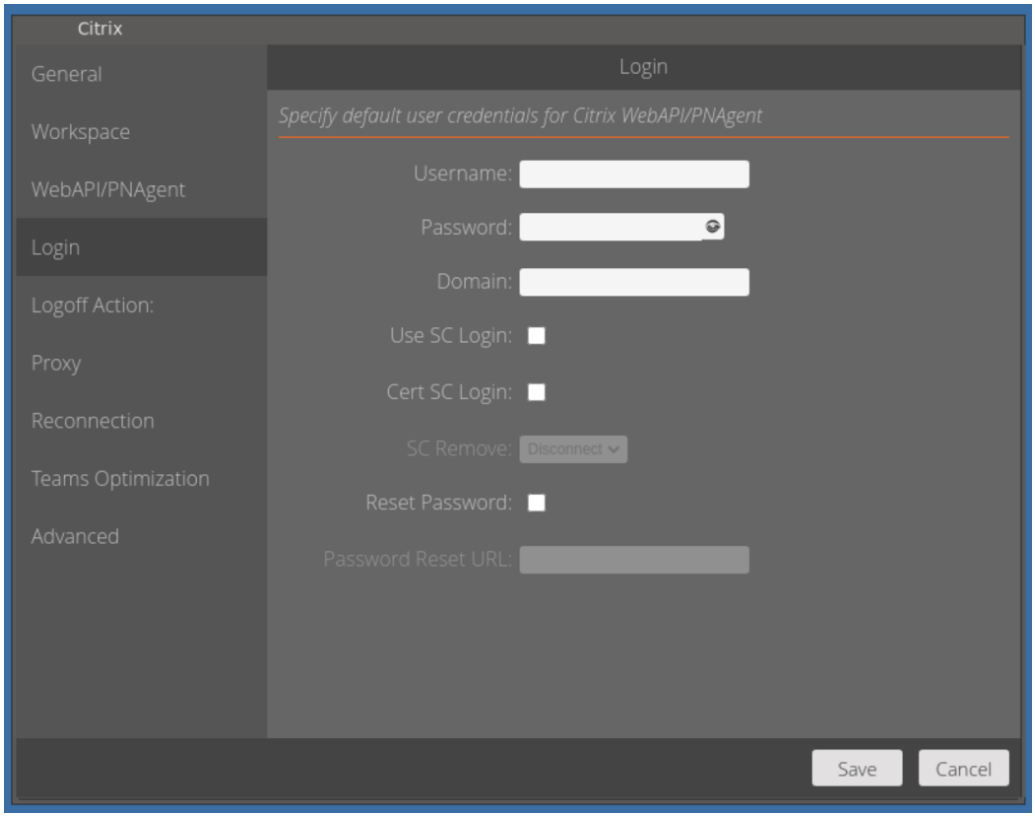


- **Password Change Server**: Enabling this will enable use of a direct ICA connection to change the user password.

- **Server name**: This is the password change server name that was enabled to point to in the “Password Change Server” field above.
- **Hide Domain**: Enabling this will hide the domain field from the authentication window.
- **ReadOnly Domain**: Enabling this will show the domain name but won’t allow for its modification in the authentication window.
- **Server Certificate**: This dropdown list determines the behavior of the connection if a Certificate Authentication error occurs. Options are “Accept”, “Warning” or “Reject”.
- **Persistent Login**: This leaves the list of available Apps/Desktops open when exiting a Citrix Session.
- **Logoff at idle timeout**: Enabling this will logoff the user from the connected Citrix desktop following the period of inactivity that is set in the “Idle timeout” field below it.
- **Idle timeout**: This is the amount of idle time before desktop logoff in minutes. The “Logoff at idle timeout” field above needs to be enabled for this to be available.
- **User Agent**: Used to rewrite the User Agent of the Client browser. This field is used to route the client to the appropriate Storefront stores/sites by means of a profile (setup on the server side). The default User Agent field value is ‘CitrixReceiver’ but can be changed to another value such as ‘iPad’ (or some other User Agent value defined on the NetScaler) to route those users/devices to the proper store/site.
- **Debug log:** Enabling this will write log information to /tmp/tzstorefront.log

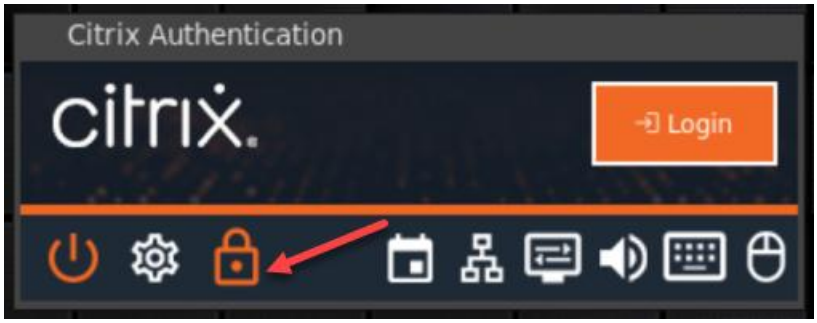
Login

In this section you can customize the way that you want your users to login to their Citrix Storefront(WebAPI/PNAgent) connection.



- **Username, Password and Domain**: These are the credentials that match your specific environment.
- **Use SC Login**: Enable this setting to allow use of Smart Card login. This option will not work when using an actual smart card with user certificates installed (if your smartcard requires a PIN to access the user certs then this option is not correct - use the Cert SC login option instead).
- **Cert SC login**: Enable this setting to allow use of Certificate based Smart Card login. A PIN is required to access the user certs.
- **SC remove**: If you intend to use Cert-based SC login, then you have the option to choose what happens when the smart card is removed from the reader. The choices available are to take “No Action” or “Disconnect” the session.
- **Reset Password and Password Reset URL**: Ticking this box, will enable you to then specify a password reset URL in the box below.

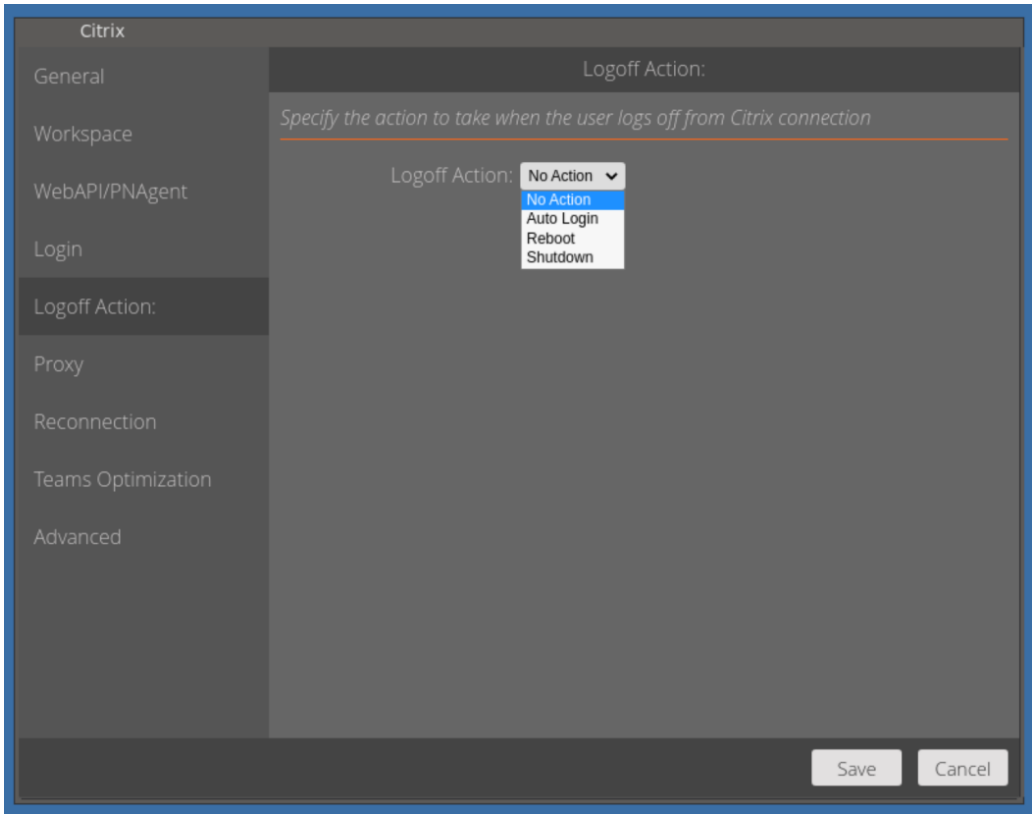
If you do specify a “Password Reset URL”, this will then be made available as a keylock clickable link on the login box, as pointed to by the red arrow in the image below.



Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional field called “Use LDAP Credentials”. This will allow you to use your network domain credentials to log in.

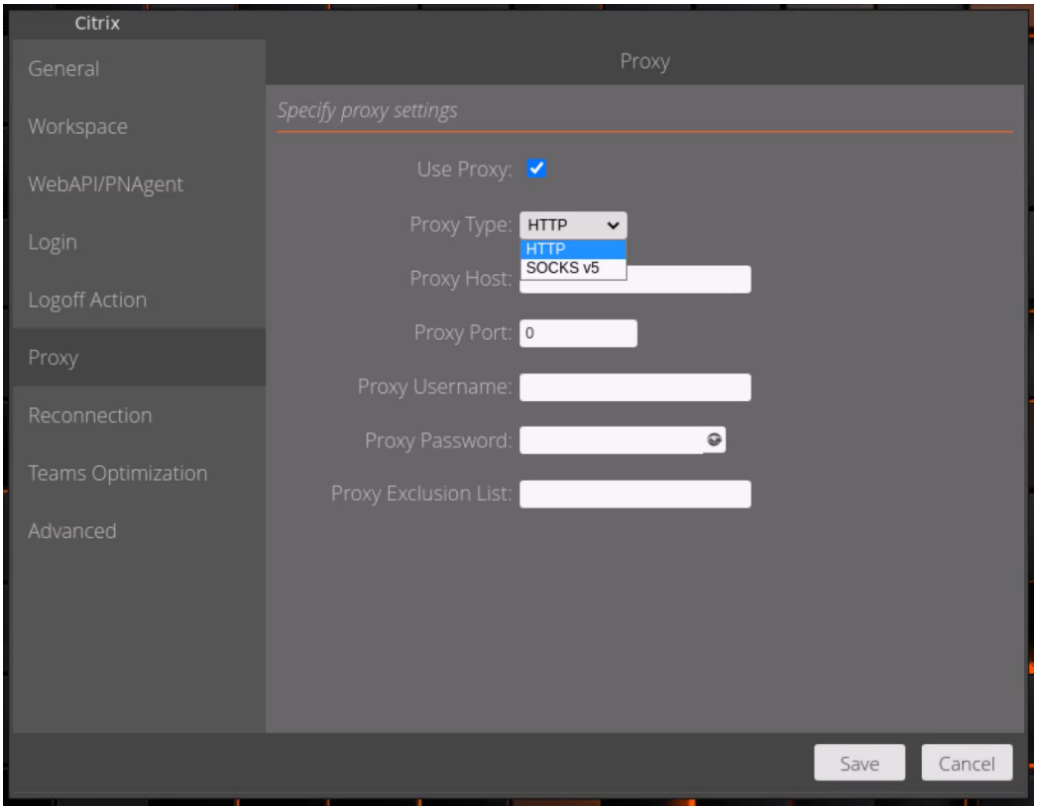
Logoff Action

There are 4 options available when logging off from the active Citrix session, “Auto Login” again, Reboot” the Thin Client or “Shutdown” and power off the device or “No Action”.



Proxy

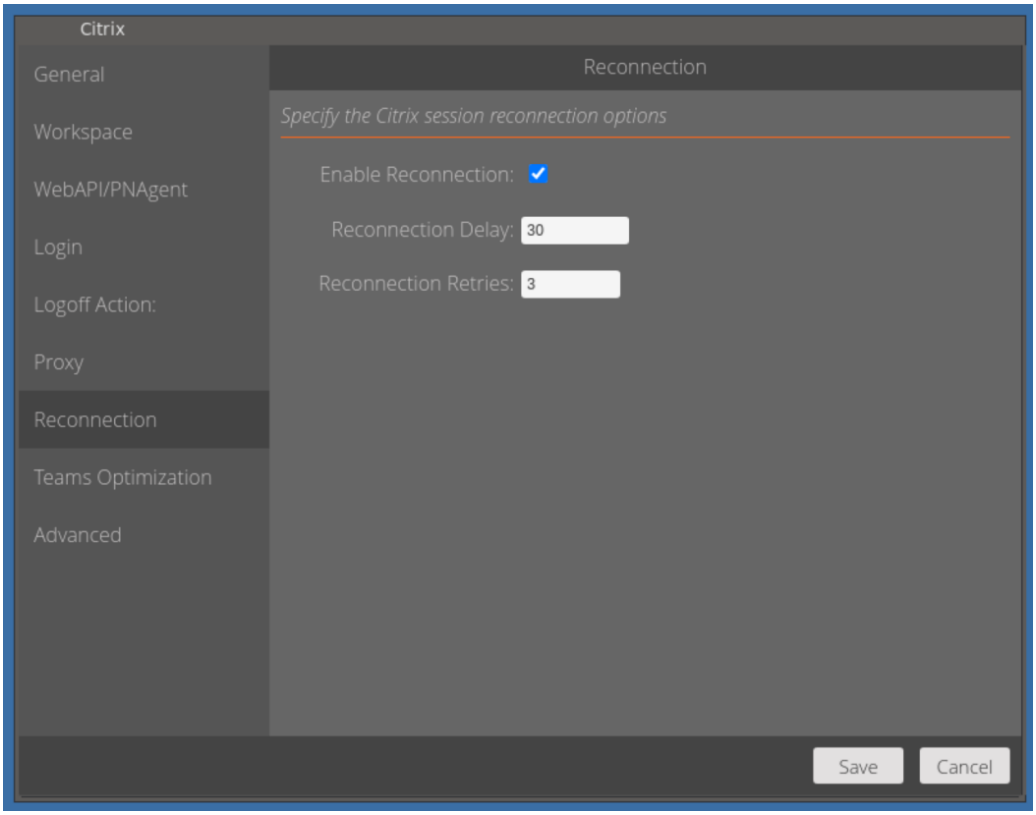
If your network is set to use a Proxy, here is where you will type in the connection information.



- **Use Proxy:** Enables Proxy connection.
- **Type:** Options are HTTP and SOCKS v5.
- **Proxy Host:** Type in the proxy host IP or FQDN hostname.
- **Proxy Port:** Assign port number.
- **Proxy Exclusion List:** If you have multiple sites or addresses that you wish to bypass the proxy, then type them in here and use a comma to separate the list of exclusions.

Reconnection

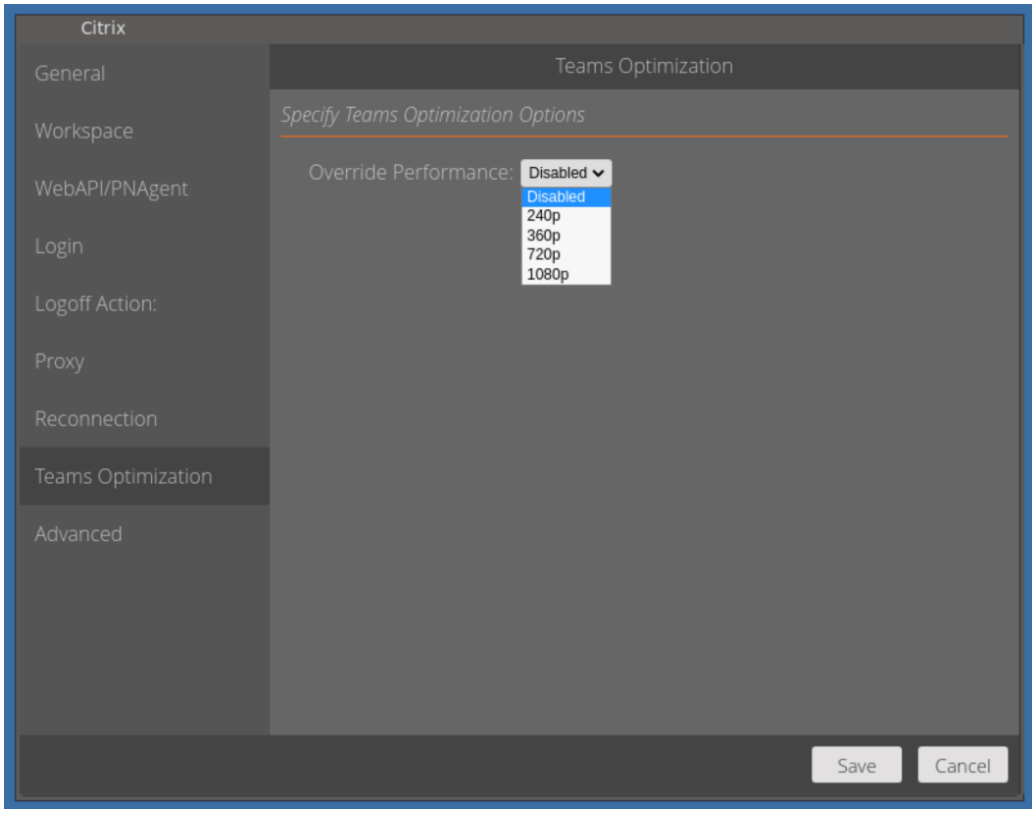
This section allows you to set reconnections if your session disconnects for whatever reason.



- **Enable Reconnection**: This switches automatic reconnection on.
- **Reconnection Delay**: The amount of time taken following disconnection, that a reconnect will be attempted. In this example above, after 30 seconds of being disconnected, the reconnect will be attempted.
- **Reconnection Retries**: This is the maximum number of retry attempts. This example will try 3 times to reconnect before it stops trying.

Teams Optimization

This section allows you to optimize Microsoft Teams sessions inside the VDI.

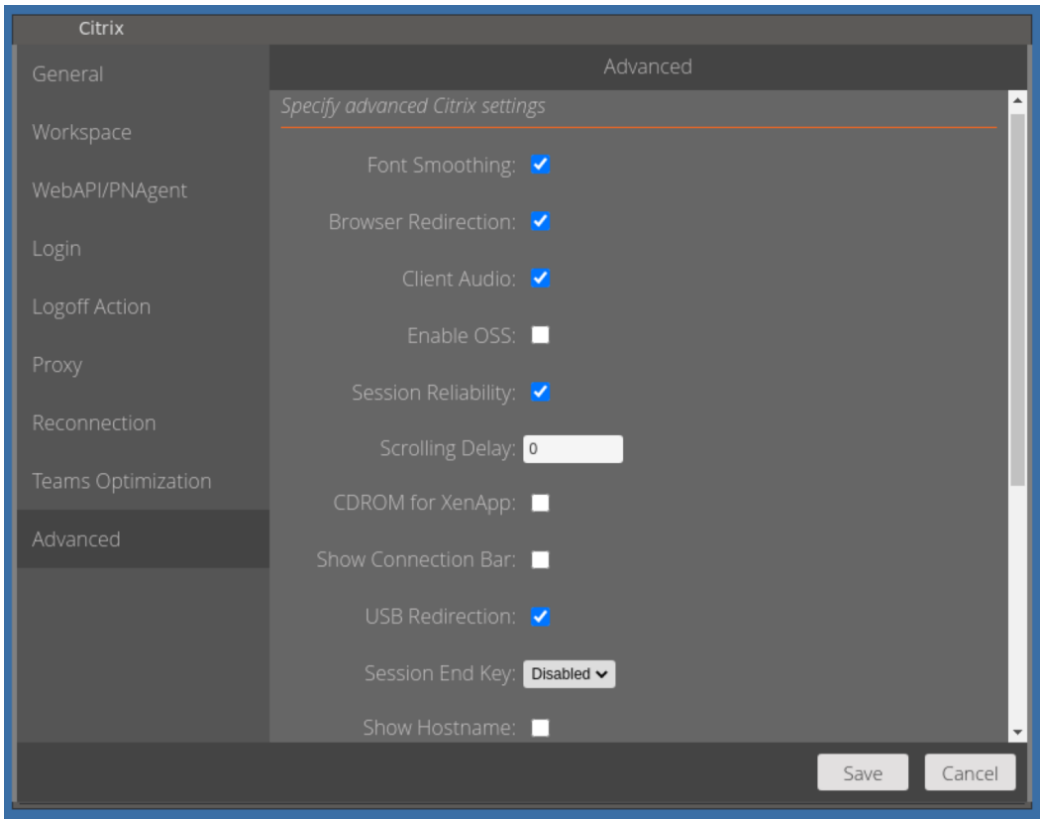


- **Override Performance**: This allows you to select the webcam encoding size on the Thin Client, ready for the VDI. The maximum resolution currently supported is 720p. However, this is dependent on the hardware being used and must be adjusted with caution, accordingly.

  If this is disabled, Citrix Workspaces App(CWA) will use the platform estimator to determine the “Teams” webcam encoding rate and size.

Advanced

The Advanced section of “Citrix Settings” allows additional customization to be carried out.



- **Font Smoothing:** Enables the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.

- **Browser Redirection:** Allows for the redirection of client browser viewport content directly to the Thin Client and thus reducing overhead inside. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL. Note: This is available on “Citrix Receiver for Linux” minimum version 13.9

- **Client Audio:** Allows for the configuration of client audio within an ICA session. In the desktop session, when this setting is disabled, the speaker-icon on the taskbar will have a red-X and show "No Audio Output device is installed". When enabled, the speaker will not have a red-X and the Citrix HDX Audio volume slider will be adjustable.

- **Enable OSS:** Allows off-screen drawing surfaces to be used when constructing the image to be displayed. This reduces flicker.

- **Session Reliability:** Establishes an ICA session on TCP port 2598 (instead of port 1494) when connecting to Presentation Server. When connected to the VDI, open a cmd prompt and run: "ctxsession /v". If you have session reliability turned on you should see port 2598 used rather than 1494.

- **Scrolling Delay:** Set scrolling delay in msec. Set to a larger value to prevent over scrolling.

- **Disable XRender:** Disables XRender.

- **CDROM for XenAPP:** Allow automatic connection of CD-ROM drives.

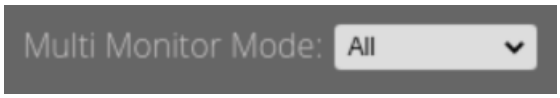
- **Show Connection Bar**: Enable to show connection bar at the top of the VDI session.

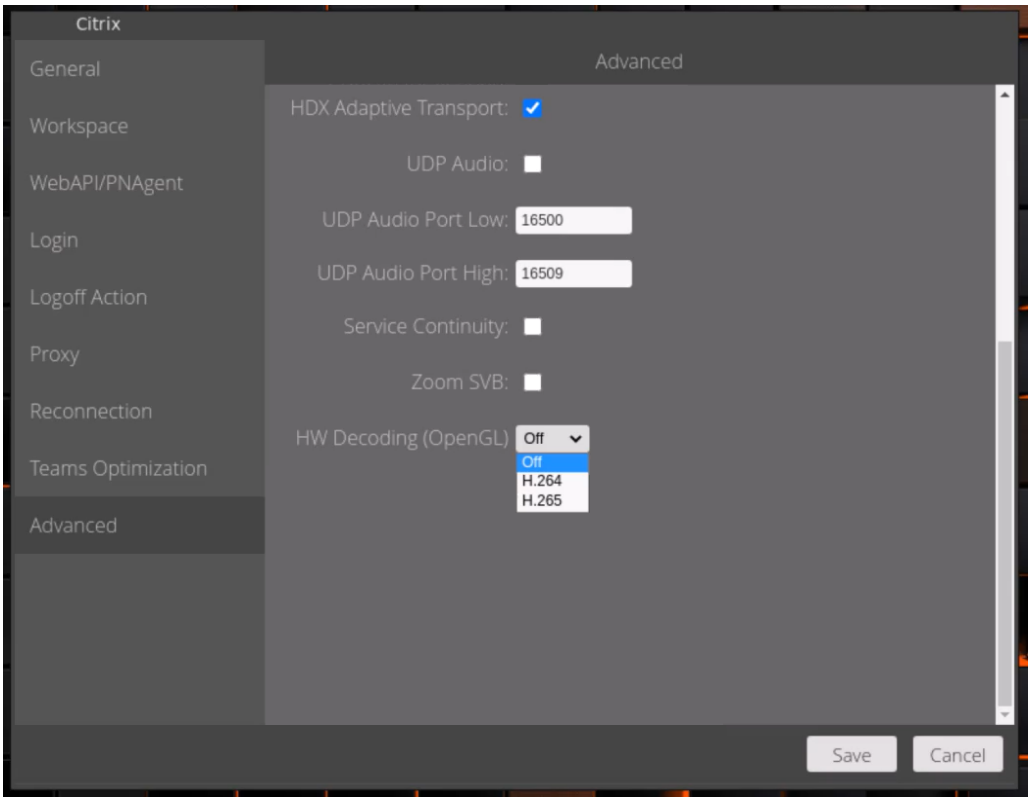
- **USB Redirection**: This makes locally attached USB devices appear as generic USB devices inside the virtual desktop on the VDI's OS. With this enabled, plug in a USB device and find the device name in USB Devices applet and set it to Include. Verify it shows as a USB device in the VDI session. For example, verify USB webcam can be used in session by setting its device class to Include.

- **Session End Key**: This is a hot key that can be used to end a current running session. Keys available are F9, F10, F11, F12 or disabled.

- **Show Hostname**: If you wish for the Thin Client hostname to appear on the "Launchpad", then enable this option. This is useful for end users who can provide 10ZiG Manager administrators with the hostname required for shadowing their session.

  Note: If you're running your connection in "Full Desktop" mode, then you will see an additional field "Multi Monitor Mode" at the top of the page, allowing you to specify additional monitor setups for additional monitors.





- **HDX Adaptive Transport**: Set this to enabled, to take advantage of EDT, Enlightened Data Transport. EDT improves data throughput for all ICA virtual channels on potentially unreliable networks, providing a better and more consistent user experience.

- **UDP Audio:** Enable this option to allow audio transport over UDP for a better audio experience in low-bandwidth situations.

- **UDP Audio Ports Low and High range:** The Audio UDP port range specifies the range of port numbers that the Windows VDA uses to exchange audio packet data with the user device. By default, the range is 16500 through 16509.

- **Service Continuity**: Service continuity removes or minimizes dependence on the availability of components involved in the connection process. Users can launch their Citrix DaaS apps and desktops regardless of the cloud services health status.

- **Zoom SVB(Smart Virtual Background):** Enable the override to allow for the use of Smart Virtual Backgrounds with Zoom Optimization inside the virtual desktop. Only recommended performance devices due to the resources this requires.

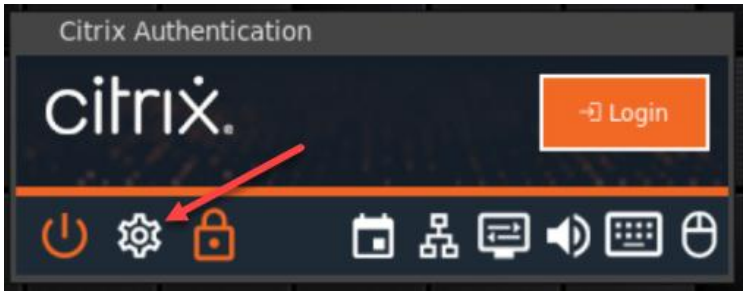
- **HW Decoding)OpenGL):** CWA2408, in the context of Citrix Workspace app for Linux, indicates support for hardware decoding of H.264 and H.265 video codecs, particularly leveraging the GPU for H.265 decoding when available. This means that the client device's graphics card can be used to decode video streams, improving performance and reducing CPU load.

Saving your settings

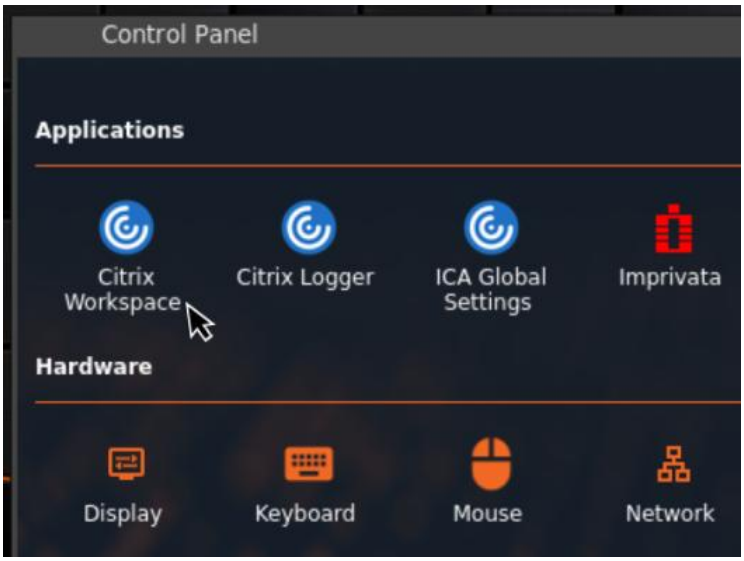
Once you're comfortable with all the settings for your 10ZiG NOS-C client, just click the "OK" button and you'll be taken back to the Citrix login screen.

Editing your connection settings

If you need to edit your connection settings again, then click the "Gear" icon in the bottom left of the "Login" screen as shown by the red arrow below.



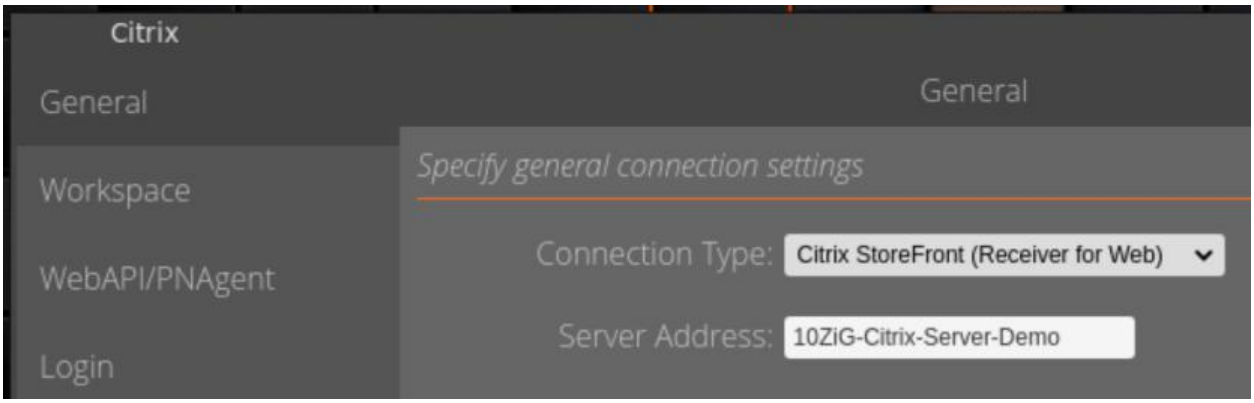
You'll be taken back into the "Control Panel", where you can click the "Citrix Workspace" icon in the top left and then make changes as outlined in the previous sections of this guide.



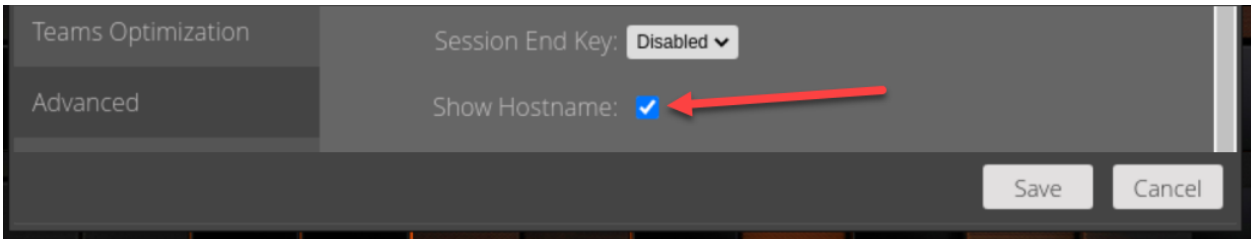
Citrix Connection Examples

Here are a few of the switches enabled in various settings sections and what your connection box might look like.

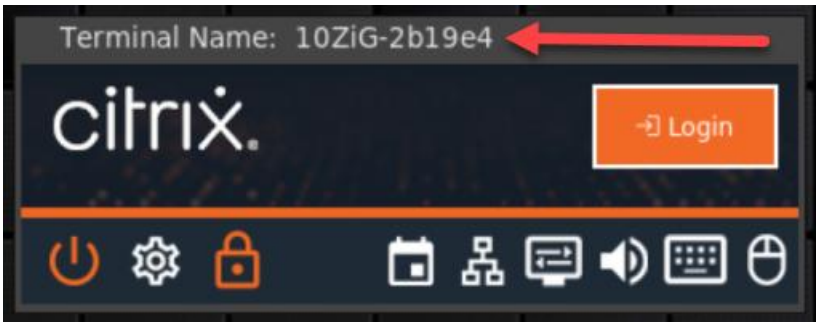
Inside the settings menu, select “General” menu option, select the “Connection type” to be Citrix StoreFront(Receiver for Web) and key in the Server Address.



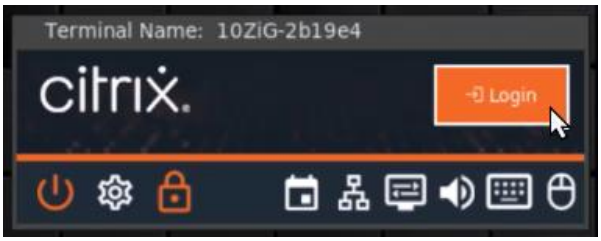
Next, we’re going to enable the client hostname to be displayed on the “Launchpad”.
Click on the “Advanced” menu option and then scroll down to “Show Hostname” setting, as shown by the red arrow below.

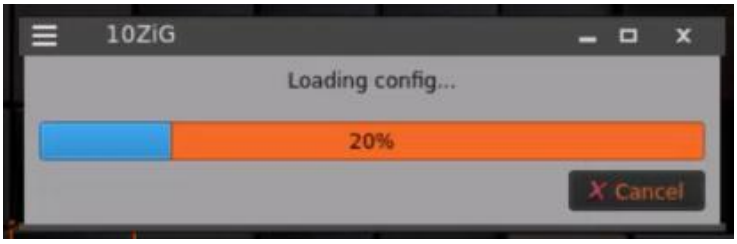


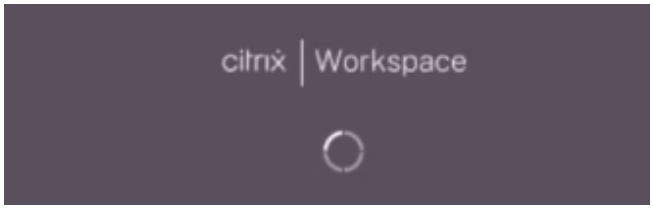
Tick this box, click “SAVE” in the bottom right and then close the “Control Panel”.
Your login box should now display the hostname of your Thin Client as below.

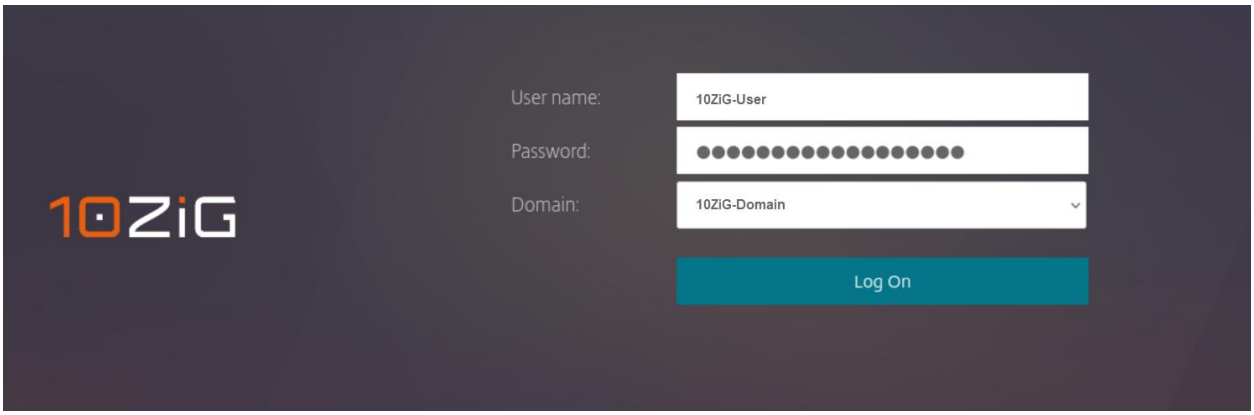


If you click the login button in the top right corner of the “Launchpad” then you’ll see a typical “StoreFront” login process as follows :-





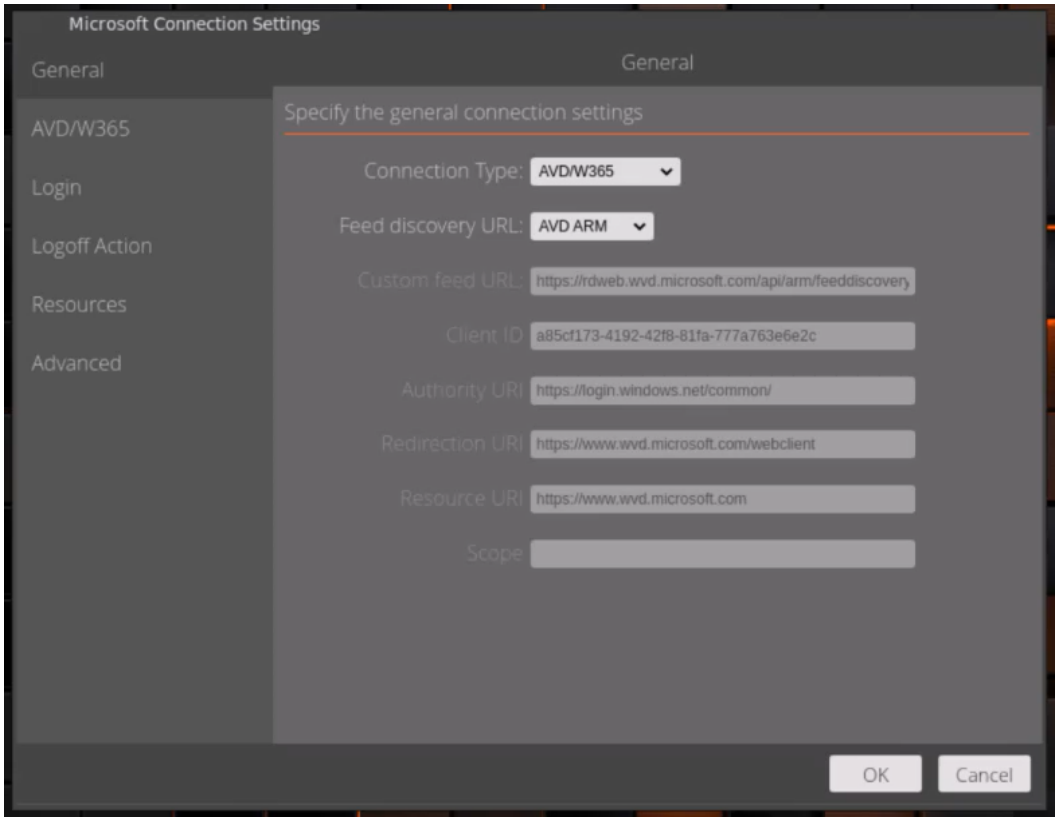




NOS for Microsoft NOS-M

Azure Virtual Desktop and Windows 365 Cloud PC(AVD/W365)

General

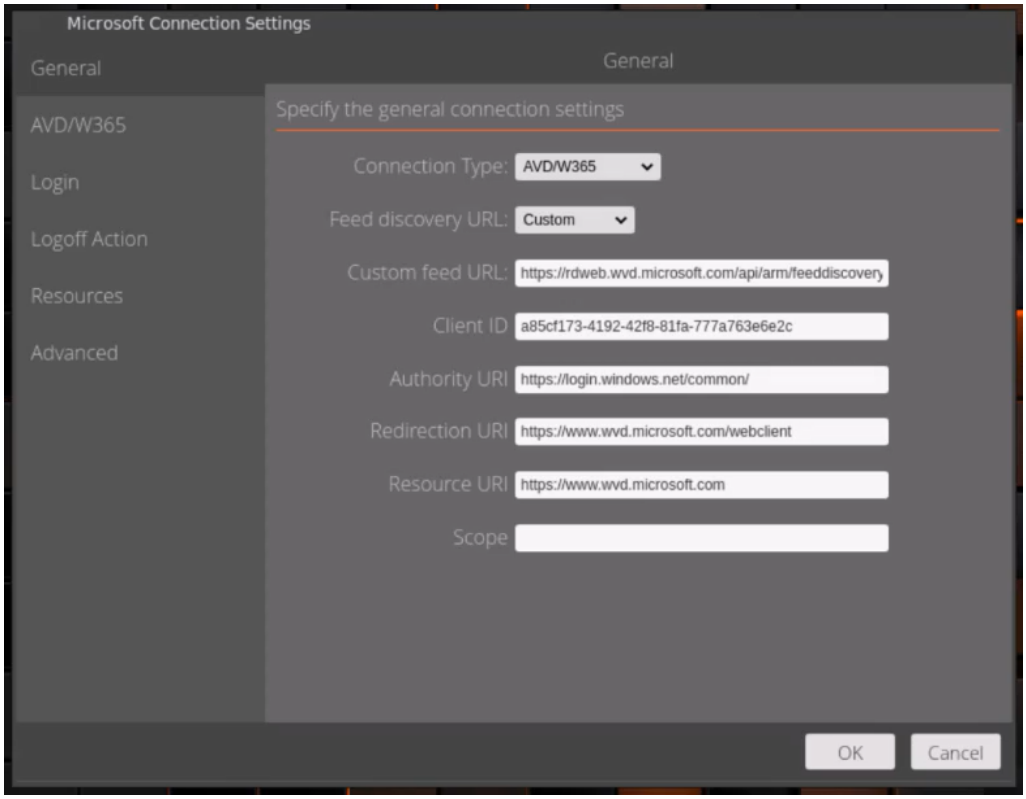


- **Connection Type:** There are 3 available that include AVD/W365 (Azure Virtual Desktop and Windows 365) , RDWeb webfeed and Direct RDP and all the configuration features inside the different types will be referenced in the following screens.

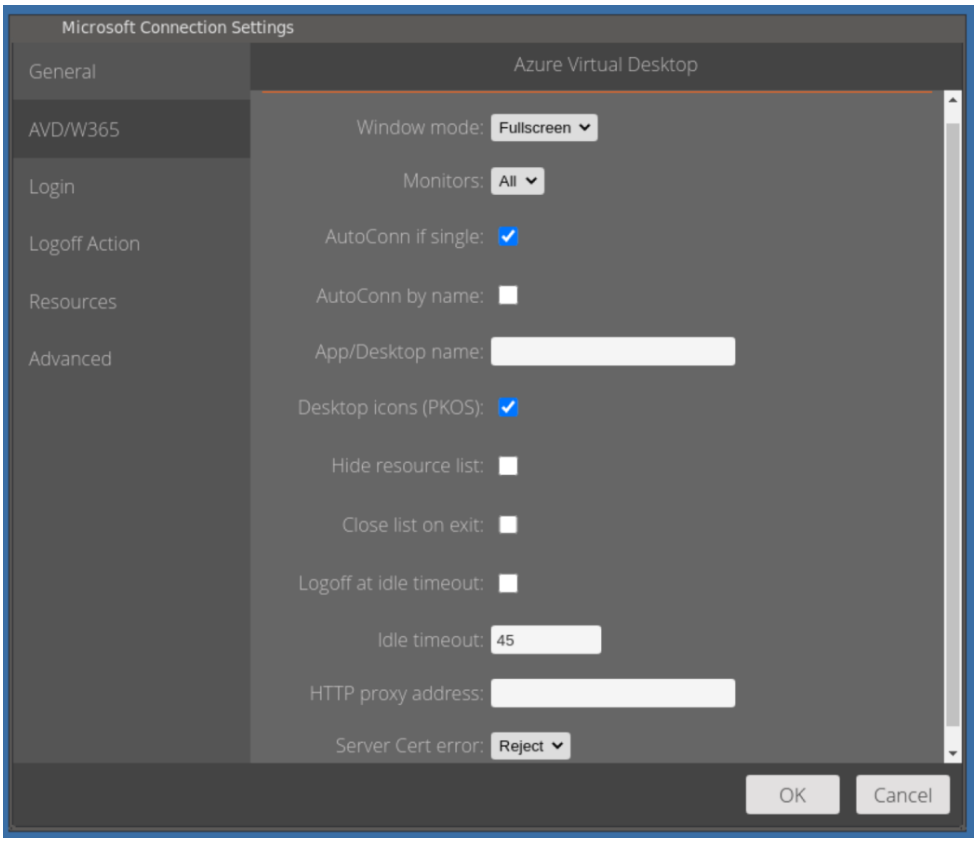
- **Feed discovery URL:** There are 4 URLs that can be supplied, “AVD ARM” (Default) – Spring 2020 Update, supporting Azure Resource Manager, “AVD Classic” – Fall 2019 Update, “AVD US Gov” and “Custom”.

  If you click on each of the feed discovery URL options in the drop down list, then you’ll see the default settings for all the different Feed discovery URLs.

  If you select the “Custom” option, then you will have to opportunity to supply your own custom settings, as shown below.



AVD/W365



- **Window mode:** Set to Fullscreen (Default), Windowed or Maximized as required.
- **Monitors:** Set the monitor topology as required. By default, desktops and applications display to "All" monitors.
- **Autoconn if single:** Following user authentication to Azure Virtual Desktop or Windows 365 Cloud PC, if the user has access to just a single desktop or application, then this automatic connection will be performed where this option is enabled.
- **Autoconn by name**: As an alternative option, it is possible to auto connect to desktops or applications by name and define that application or desktop name in the field below it.
- **Desktop icons(PKOS)**: If you're using a PKOS operating system, once authenticated to AVD, the available resources will be added as shortcuts to the PKOS desktop.
- **Hide resource list**: Following user authentication, the resource list containing desktops and applications can be hidden to the user by enabling this option.

- **Close list on exit**: Where the user connects to a desktop or application, the resource list can be automatically closed when logging out of them. This is useful in hotdesking scenarios.

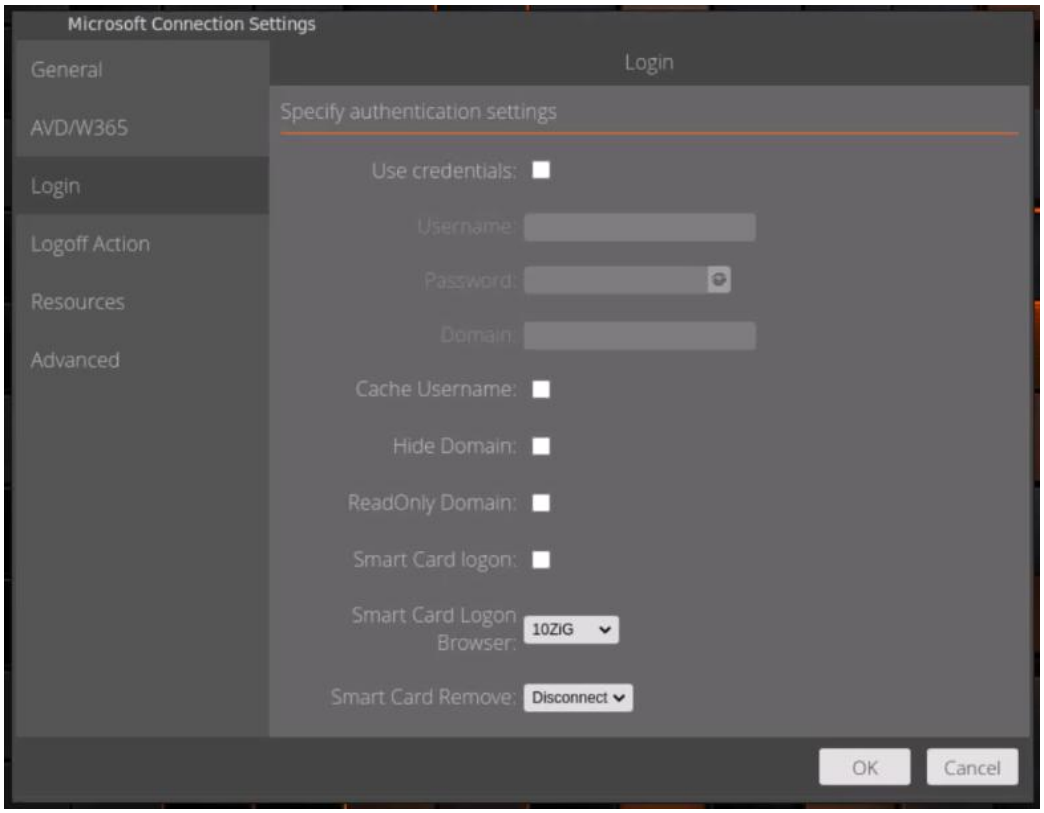
- **Logoff at idle timeout**: Enable this option to log users off from their Azure Virtual Desktop session automatically where idle timeout occurs.

- **Idle timeout**: Specify the idle timeout in minutes.

- **HTTP proxy address**: The address of your proxy server in the format of “host:port”, for example 192.165.177.211:443

- **Server Cert error:** Sets the level of cert validation to “Accept” or “Reject”.

Login



- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **Cache Username**: Enabling this, will ensure that the last logged on user is remembered for next login.

- **Hide Domain**: When this is enabled, the domain field is hidden to the user during login. This is useful in scenarios where you do not want to expose the Domain name / Tenant name to the users during authentication. When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

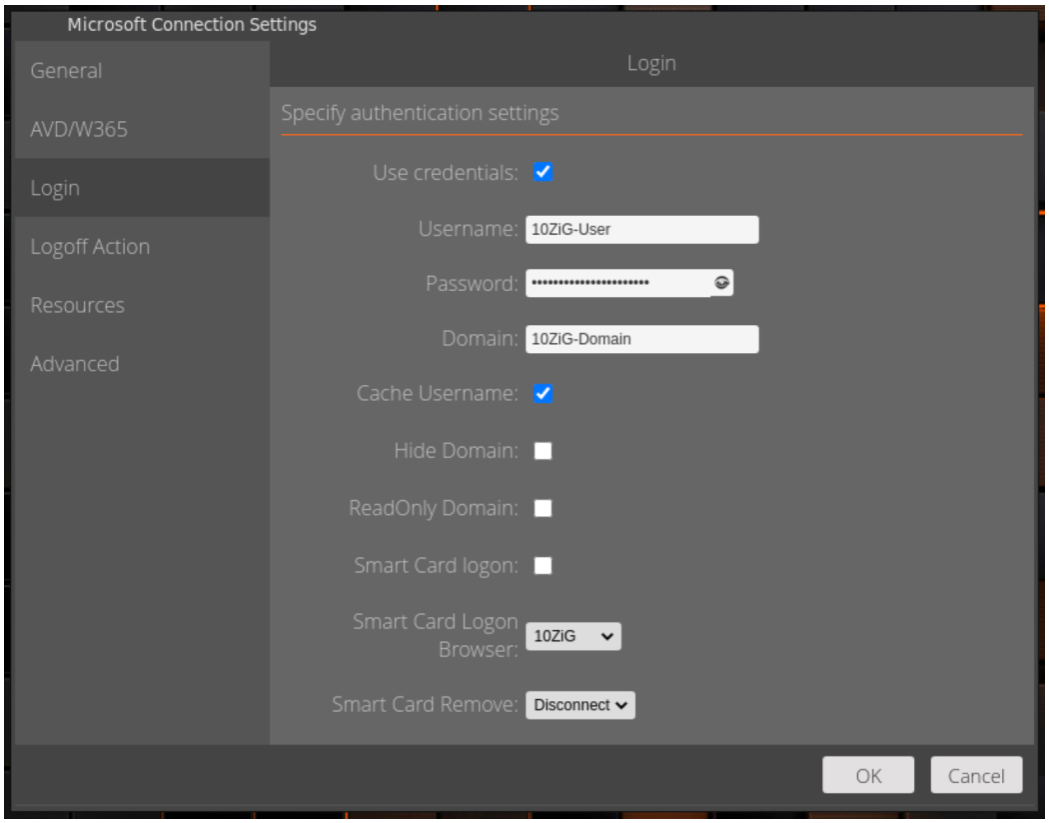
- **ReadOnly Domain**: When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

- **Smart Card logon**: Tick this box to enable smart card logons and then select the type of card to use, “Microsoft” or “10ZiG cards. The default card type is set to “10ZiG Browser” and we recommend using this one only, unless you’re advised by 10ZiG Tech Support Teams to use the Microsoft one.

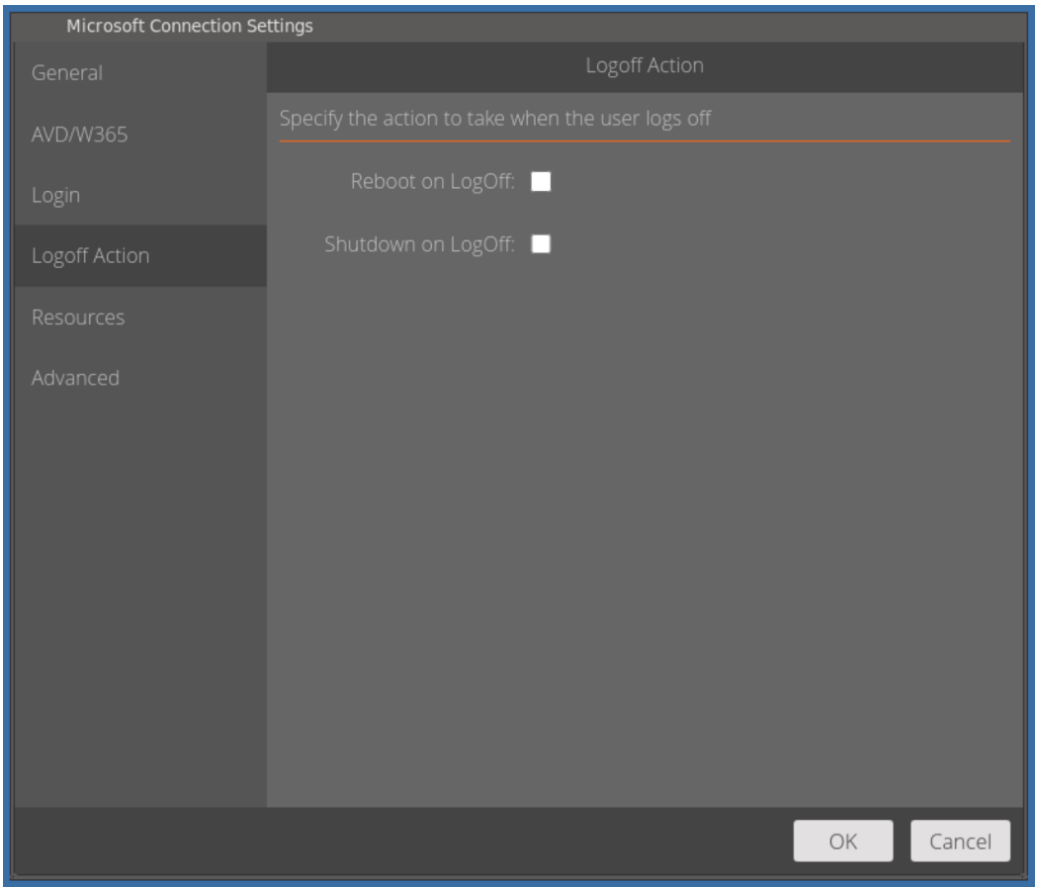
- **Smart Card Remove**: This can be set to either “Disconnect” (from the AVD session), or “No Action”.

  Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional field called “Use LDAP Credentials”. This will allow you to use your network domain credentials to log in.

Example of Cached login details



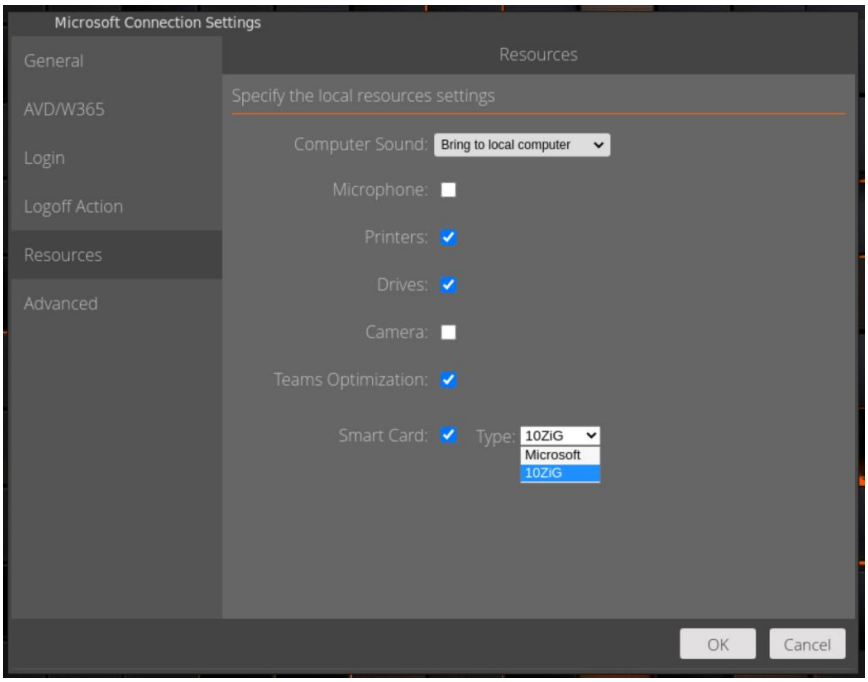
Logoff Action



- **Reboot on LogOff**: Enabling this option will reboot the Thin Client once your user has logged off their current AVD session.

- **Shutdown on LogOff**: Enabling this will shut down and power off the Thin Client.

Resources



- **Computer Sound**: You have 3 options regarding sound settings and redirection. You can choose to “Bring to local computer”, “Do not play” or “Leave at remote computer”.

- **Microphone**: Enable this option for bidirectional audio. The audio device can be configured under the Control Pane, in the Audio section.

- **Printers**: Enable this option to bring printers from this device to the virtual desktop.

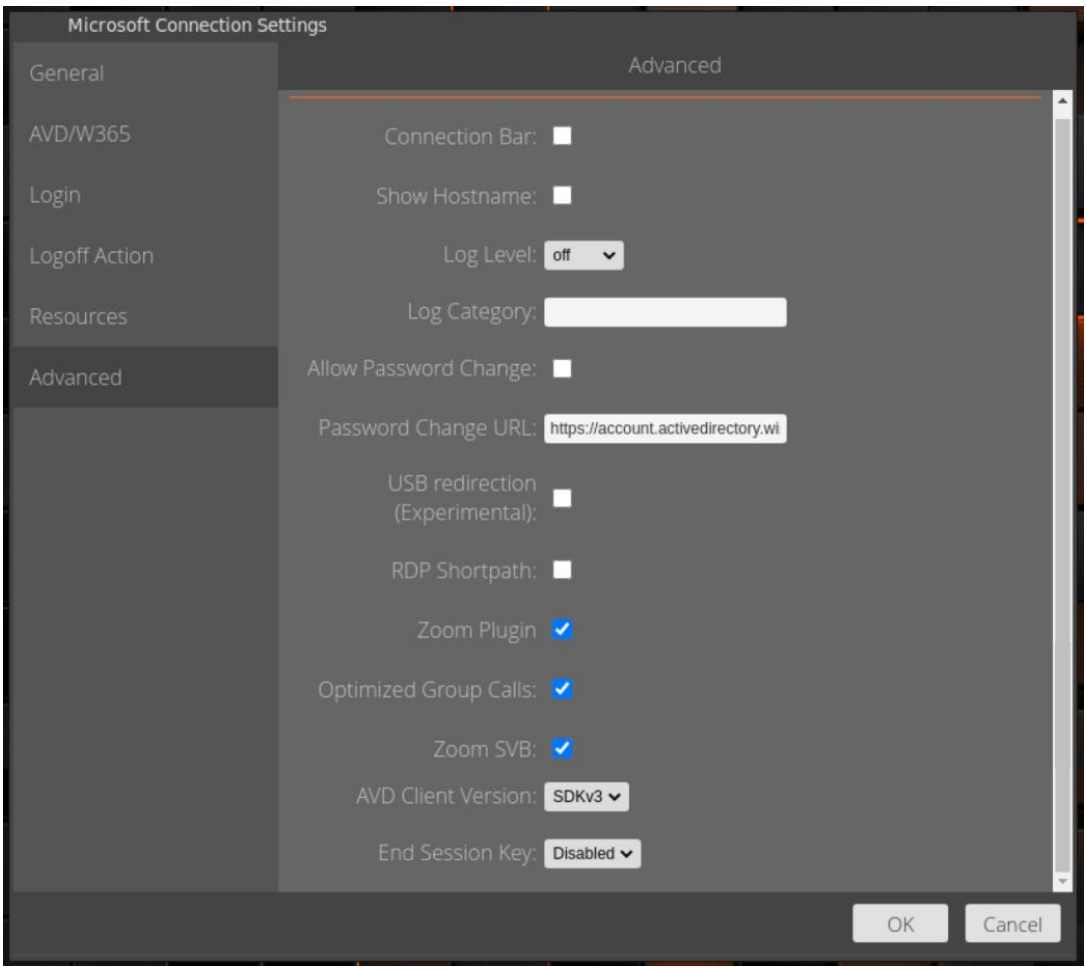
- **Drives**: Enabling this option will enable Client Drive Redirection (Mass Storage Only).

- **Camera**: Enable this to redirect webcams to your virtual desktop. Use the frame rate option to specify the fps when delivering camera content to the VM.

- **Teams Optimization**: Enable this option to optimize Microsoft Teams inside the VDI and redirect audio and video to the Thin Client. You can check if this is active inside the “Teams” app in the VDI by going into the profile menu, selecting “About” and “Version”. You will see the “AVD Media Optimized” in the version banner text.

- **Smart Card**: Enable this option for Smart Card Authentication, to login to your Azure Virtual Desktops. The default card type is set to “10ZiG Browser” and we recommend using this one only, unless you’re advised by 10ZiG Tech Support Teams to use the Microsoft one.

Advanced



- **Connection Bar**: Enable this option to display a connection bar which is displayed whilst connecting to desktops and applications. This is a useful feature in combination with the Sidebar / Taskbar. See Sidebar / Taskbar for further details.

- **Show Hostname**: Enable this option to display the endpoint hostname at the Microsoft Remote Desktop Authentication login screen. This is useful for end users who can provide 10ZiG Manager administrators with the hostname required for shadowing their session.

- **Log Level**: Enable debug logging here, see Troubleshooting & Debug for further information.

- **Allow Password Change**: Enable this option to allow users to change their password when required and also on demand.

- **Password Change URL**:The Password Change URL is contacted using a kiosk based secure browser but can be changed here. The default address it connects to is **'https://account.activedirectory.windowsazure.com/changepassword.aspx'**.

- **USB redirection (Experimental)**: Enable this option, at user discretion to redirect your USB devices through to the VDI. Note: This is an experimental feature and as such may produce differing results.

- **RDP Shortpath**: RDP Shortpath is a feature of Azure Virtual Desktop that establishes a direct UDP-based transport between a supported Windows Remote Desktop client and session host. This article shows you how to configure RDP Shortpath for managed networks and public networks. For more information, see this article below : Configure RDP Shortpath - Azure Virtual Desktop | Microsoft Learn

- **Zoom Plugin**: Enable this is option for Zoom VDI Optimization. This can be used if the matching plugin is installed to the Windows desktop.

- **Optimized Group Calls**: This option can negotiate "optimized" bandwidth that helps to fix black video stream during group calls.

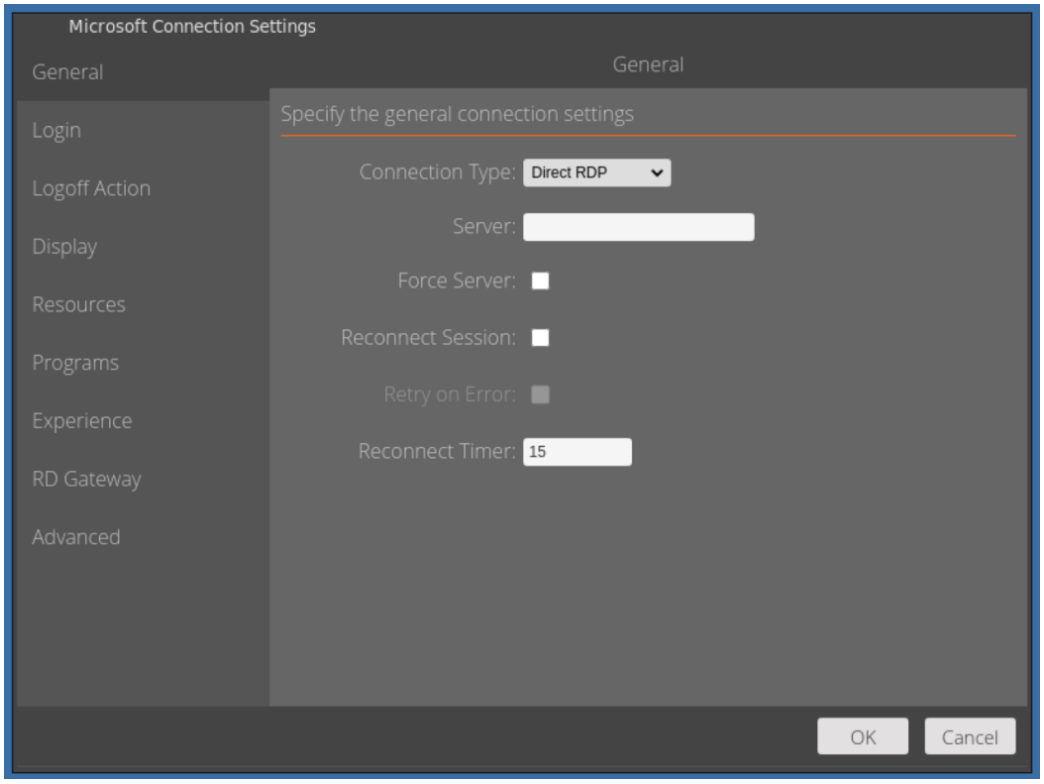
- **Zoom SVB**: Enable the override to allow for the use of Smart Virtual Backgrounds with Zoom Optimization inside the virtual desktop.

- **AVD Client Version**: This drop down box allows you to choose from several different AVD clients.

- **End Session Key**: This is a hot key that can be used to end a current running session. It can be disabled or set to be "CTRL_F12".

Direct RDP

General



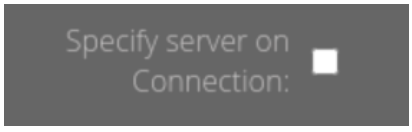
- **Server**: This is where you can enter a single server or multiple URL addresses of the remote desktop connection broker. If multiples are used, then they should be comma separated.

- **Force Server**: If you enter multiple server URLs in the “Server URL” field, comma separated, a drop-down menu is added to launchpad and forces the user to select the server before connecting.

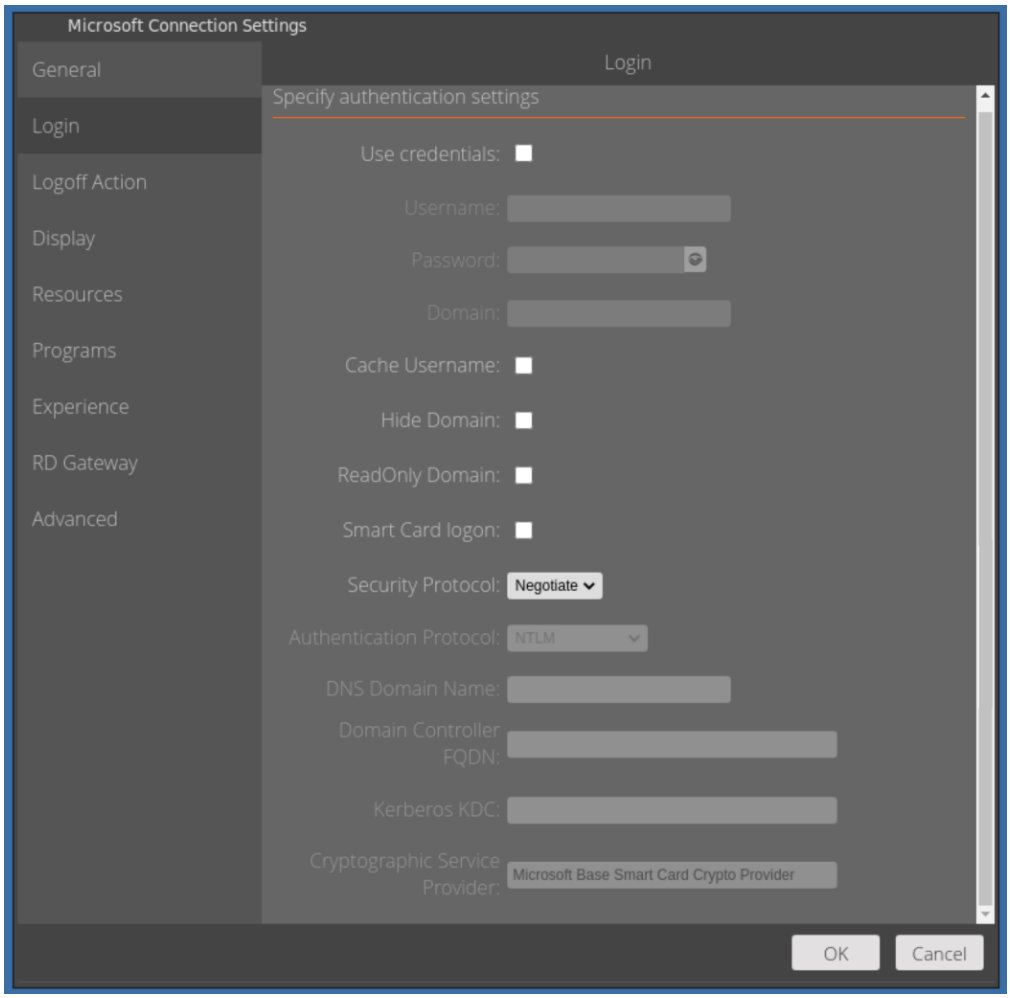
- **Reconnect Session**: When set, this should automatically attempt to reconnect after logging off or disconnecting from a session.

- **Reconnect Timer**: Set the timeout for the reconnect prompt, following disconnection.

Note: If you’re running in “Full Desktop” mode, then you will see an additional field called “Specify server on connection”. This allows you to specify the server details at auth process.



Login



- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **Cache Username**: Enabling this, will ensure that the last logged on user is remembered for the next login.

- **Hide Domain**: When this is enabled, the domain field is hidden to the user during login. This is useful in scenarios where you do not want to expose the Domain name / Tenant name to the users during authentication. When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

- **ReadOnly Domain**: When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

- **Smart Card logon:** If you enable this, then you can attach a smart card device to your client and use this as the logon option. The remote desktop authentication screen will look like this below. If you do enable this, then the credentials options will be greyed out.

The values below are to be used when implementing Smart Card Logons.

- **Security Protocol**: This is where you can specify a level of Network Authentication for the protocol type. Options are “Negotiate”, “RDP”, “NLA”, or “TLS”.

- **Authentication Protocol:** Options are “NTLM”, “Kerberos” and “NTLM+Kerberos”

- **DNS Domain Name:** This is the domain name that your domain controller resides in.

- **Security Protocol**: This is where you can specify a level of Network Authentication for the protocol type. Options are “Negotiate”, “RDP”, “NLA”, or “TLS”.

- **Domain Controller FQDN:** This is the fully qualified domain name of the domain controller on your network. You can supply multiple domain controllers by separating them with commas.

- **Kerberos KDC:** If you’re using a Kerberos Key Distribution Center, then this is where you can supply the proxy server details. You need to enable “NLA” above, to modify these settings.

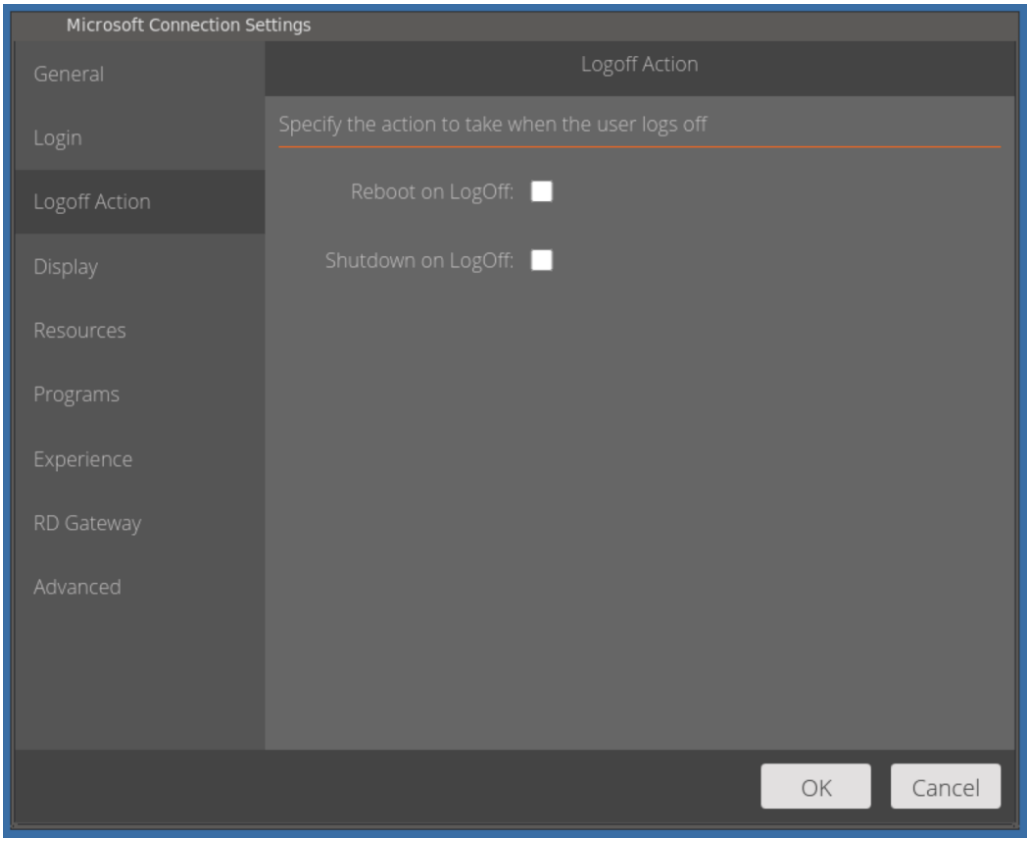
- **Cryptographic Service Provider:** This information is required for the NLA smart card logon and is the name of the Cryptographic Service Provider that Windows logon uses to handle the user certificate. This information can be capture using on Windows the command line certutil -scinfo | findstr Provider .

  For most cards is “Microsoft Base Smart Card Crypto Provider” but it can vary based on the installed Windows middleware and how it is configured.

For example, for IDPrime 930 cards and SafeNet Windows middleware, this value is “eToken Base Cryptographic Provider” or “Microsoft Base Smart Card Crypto Provider”.

Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional field called “Use LDAP Credentials”. This will allow you to use your network domain credentials to log in.

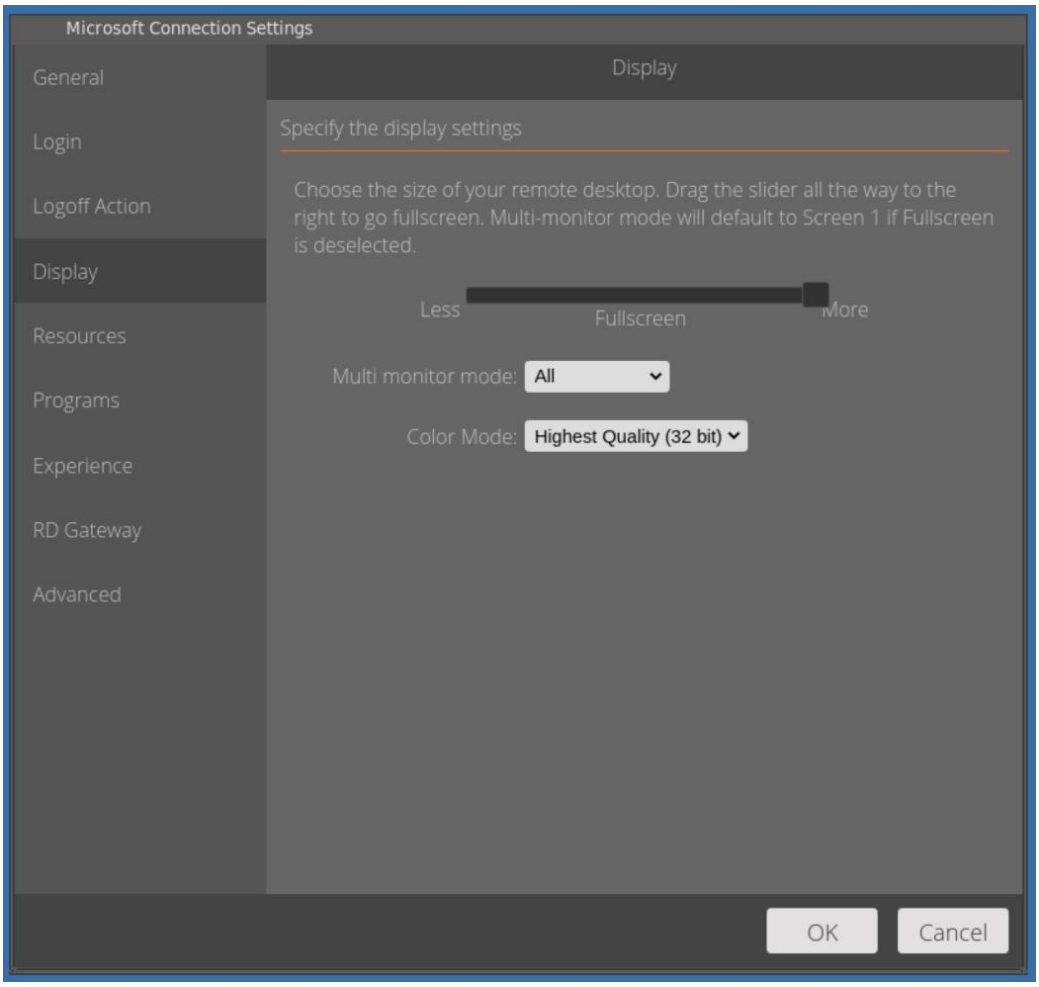
Logoff Action



- **Reboot on LogOff**: Enabling this option will reboot the Thin Client once your user has logged off their current AVD session.

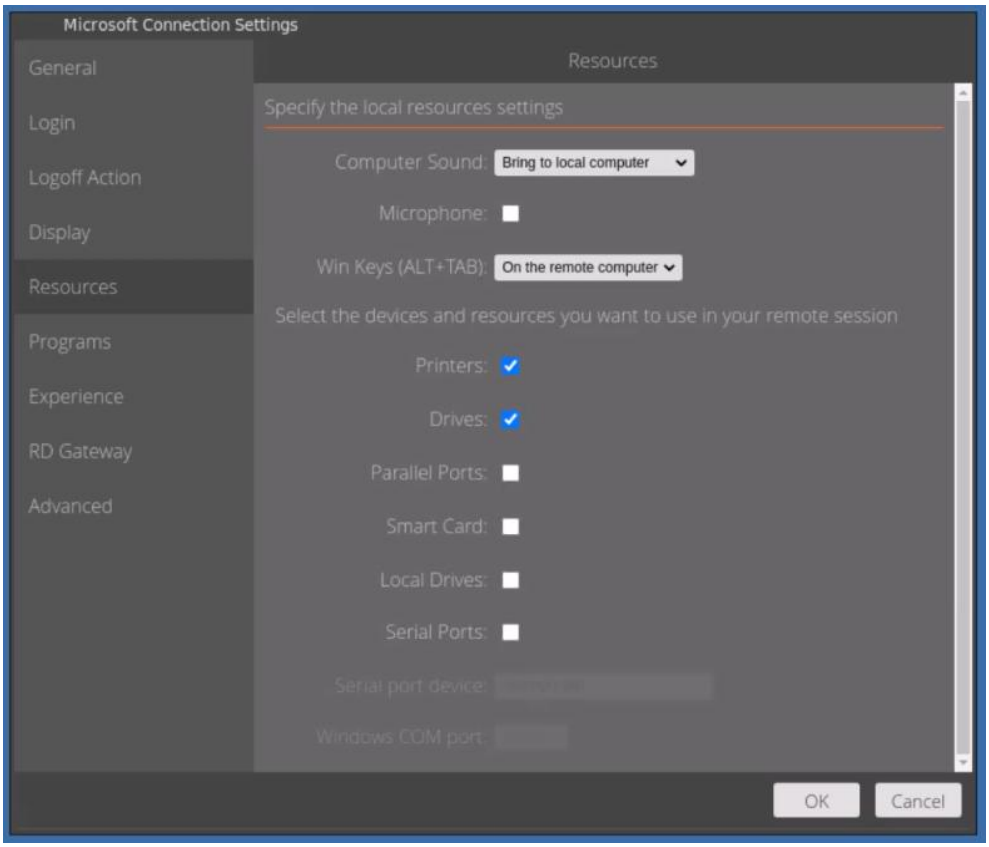
- **Shutdown on LogOff**: Enabling this will shut down and power off the Thin Client.

Display



- **Multi Monitor Mode:** Options are for display on monitor 1, 2, 3 or all together.
- **Color Mode:** Changes the color options to suit the particular connection performance. This ranges from 256 colors to “Highest Quality(32 bit)”.

Resources



- **Computer sound:** You have 3 options regarding sound settings and redirection. You can choose to “Bring to local computer”, “Do not play” or “Leave at remote computer”.

- **Microphone:** Verify the VDI session receives audio input from the Thin Client’s local mic.

- **Win Keys(ALT+TAB):** With these options enabled, verify ALT+TAB operates in the VDI session or on the Thin Client.

- **Printers:** Enabling this option will enable you to attach a local printer to the Thin Client and then print to it from within the VDI desktop.

- **Drives:** This passes USB mass storage devices to the VDI session.

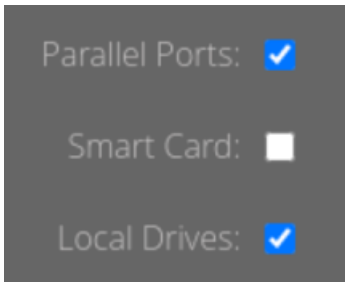
- **Smart Card:** This option, when enabled will pass the smart card through to the VDI desktop.

- **Serial Ports:** Tick this option to gain access to serial port configurations below.

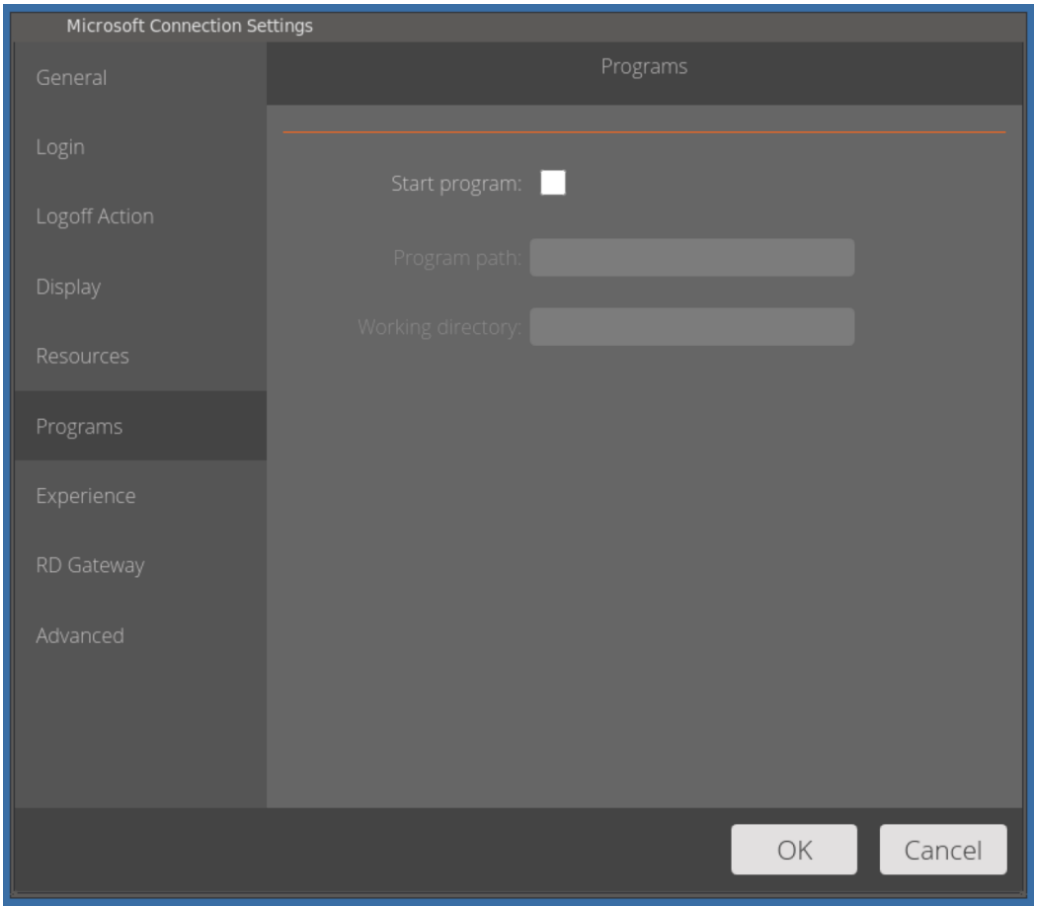
- **Serial Port:** If you connect a USB foot to the 10ZiG 6000q, then serial port device “/dev/ttyUSB0" is made available to the VDI.

- **Windows COM port:** With the USB foot attached, you can specify what COM port number will be passed to the VDI.

  Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional 2 fields available called “Parallel Ports” and “Local Drives”, so these can also be made available to your remote sessions if required.



Programs

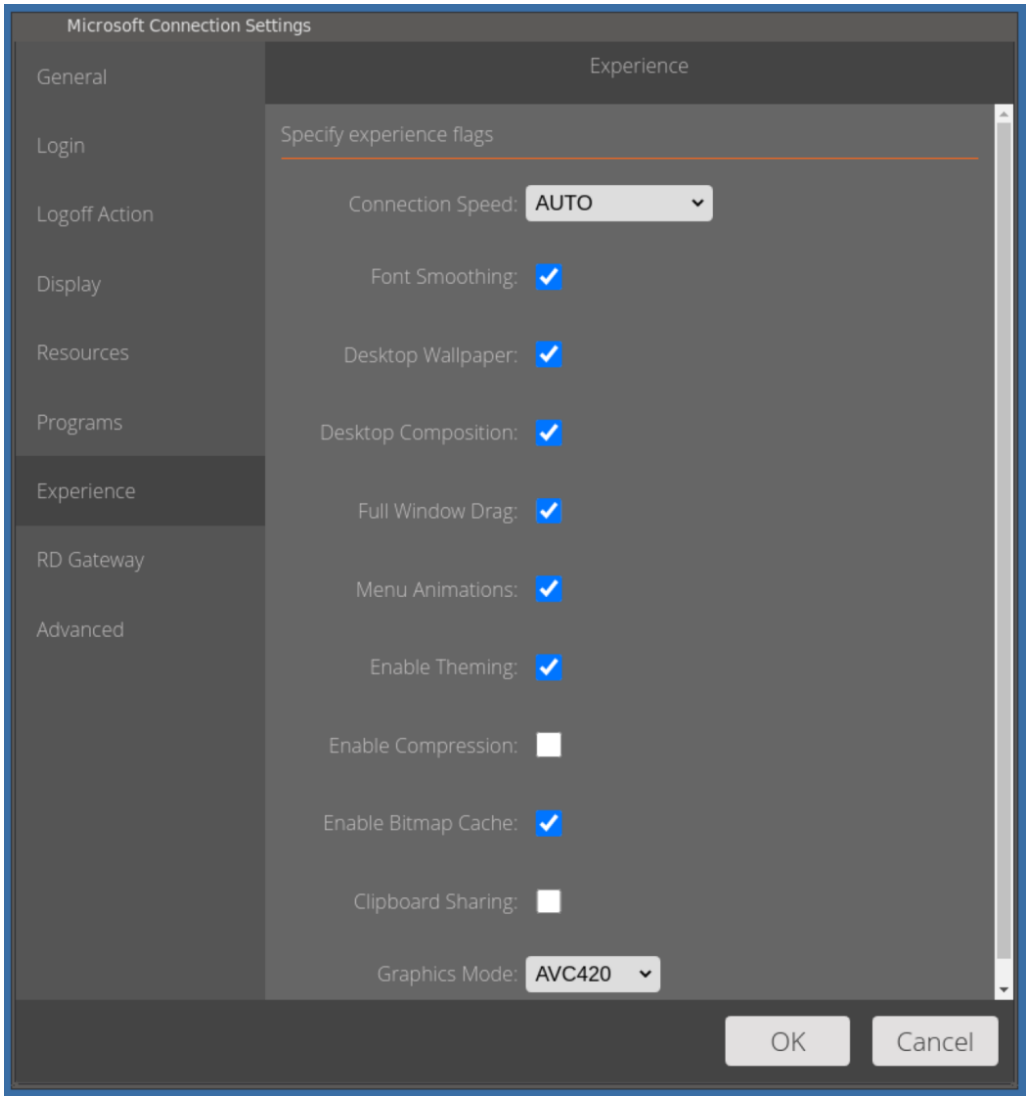


- **Start program:** When enabled, the Program path, and Working directory fields are available to be set below this field.

- **Program path:** Add a program path, such as C:\Windows\System32\notepad.exe. After you establish an RDP connection to a Remote Desktop you will see the “Notepad” program launches.

- **Working directory:** This is the working directory in which the program name above will be launched from.

Experience



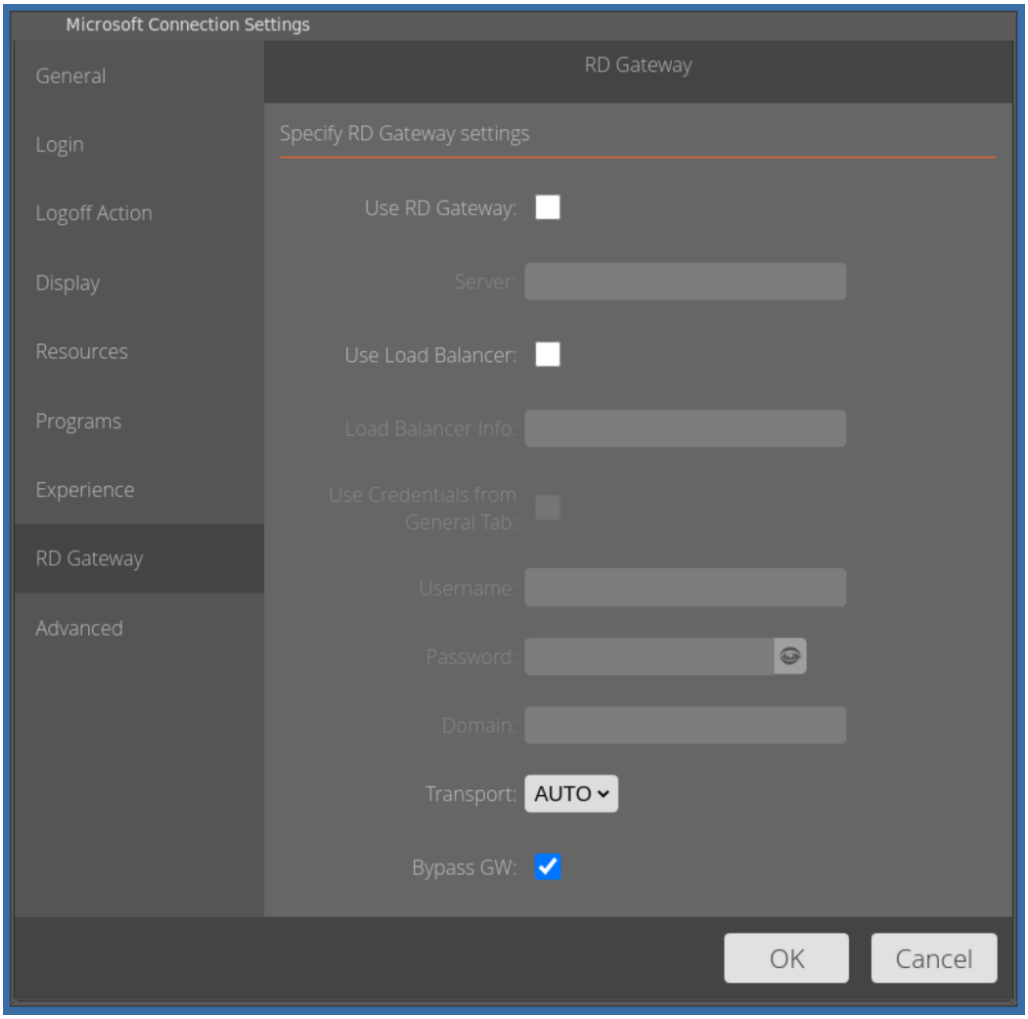
- **Connection speed:** You can adjust this value to suit your individual performance needs, or just leave it as “Auto” to negotiate the best speed available.

- **Font Smoothing:** Enables the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.

- **Desktop Wallpaper:** Verify when enabled, the remote desktop shows the wallpaper and when disabled the remote desktop's wallpaper should not be shown.

- **Desktop Composition:** This option either enables or disables the “Aero” effects content of the remote Windows desktop.
- **Full window drag :** When the option is enabled, dragging the remote desktop window should show its content, when disabled, the content will be blank.
- **Menu Animations:** When enabled, the right-click context menus show their animations when opening and closing. Disabled, the right-click context menus show no animation.
- **Enable Theming:** Determines whether themes are permitted when you log on to the remote computer.
- **Enable Compression:** Determines whether bulk compression is enabled when it's transmitted by RDP to the local computer.
- **Enable Bitmap Cache:** Determines whether bitmaps are cached on the local Thin Client (disk-based cache). Bitmap caching can improve the performance of your remote session.
- **Clipboard Sharing:** When enabled, you can copy and paste text from the local client to the remote Windows desktop session and from the remote session to the local client.
- **Graphics Mode:** This feature lets you specify which codec to use during the RDP session. Available options are RDP, RemoteFX, AVC420(Default) and AVC444.

RD Gateway



- **Use RD Gateway:** A RD Gateway allows you to establish a RDP connection to a Windows system but tunneled through a HTTPS connection.

- **Server:** The address of your RD Gateway Server.

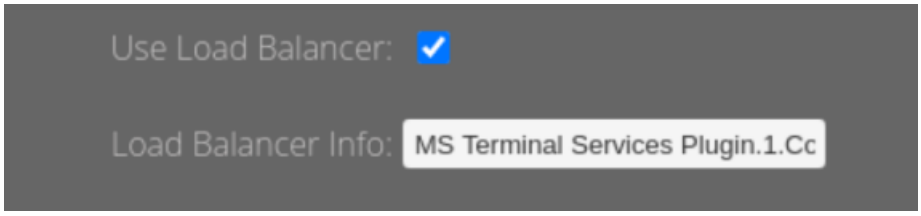
- **Load Balancer Info:** This is the address of your load balancer server within your corporation.

  To obtain the address of your load balancer server, follow the steps below :-

  1. On Windows 10 or later PC, open up a web browser and type the address below. https://YourRDWebBrokerHostName/rdweb (Where YourRDWebBrokerHostName is

the server name hosting the RD Web Broker role) which should take you to the RD web access page.

2. When prompted, log in using valid credentials, and you'll be taken to a page which lists all of your available apps and desktops.
3. Single click on one of the apps/desktops that is a part of your broker collection, this should then download a ".rdp" file (if clicking it tries to launch the session instead, try using a different browser).
4. To get the relevant information needed, right click the ".rdp" file and select "Open with…" and select an editor such as "Notepad".
5. Once opened, look towards the bottom of the file and you should see a line that starts "loadbalanceinfo:s:tsv://". The rest of the string after this point will be unique to each environment, copy or make note of everything that appears after "tsv://" and head back to the thin client. For this example, let's assume the load balancer info we copied following the "tsv://" is MS Terminal Services Plugin.1.CollectionName
6. Inside the RD Gateway configuration screen again on your 10ZiG NOS-M client, tick the box named "Use Load Balancer" and just type or paste the copied value into the "Load Balance Info:" field. See below, using our assumed example.



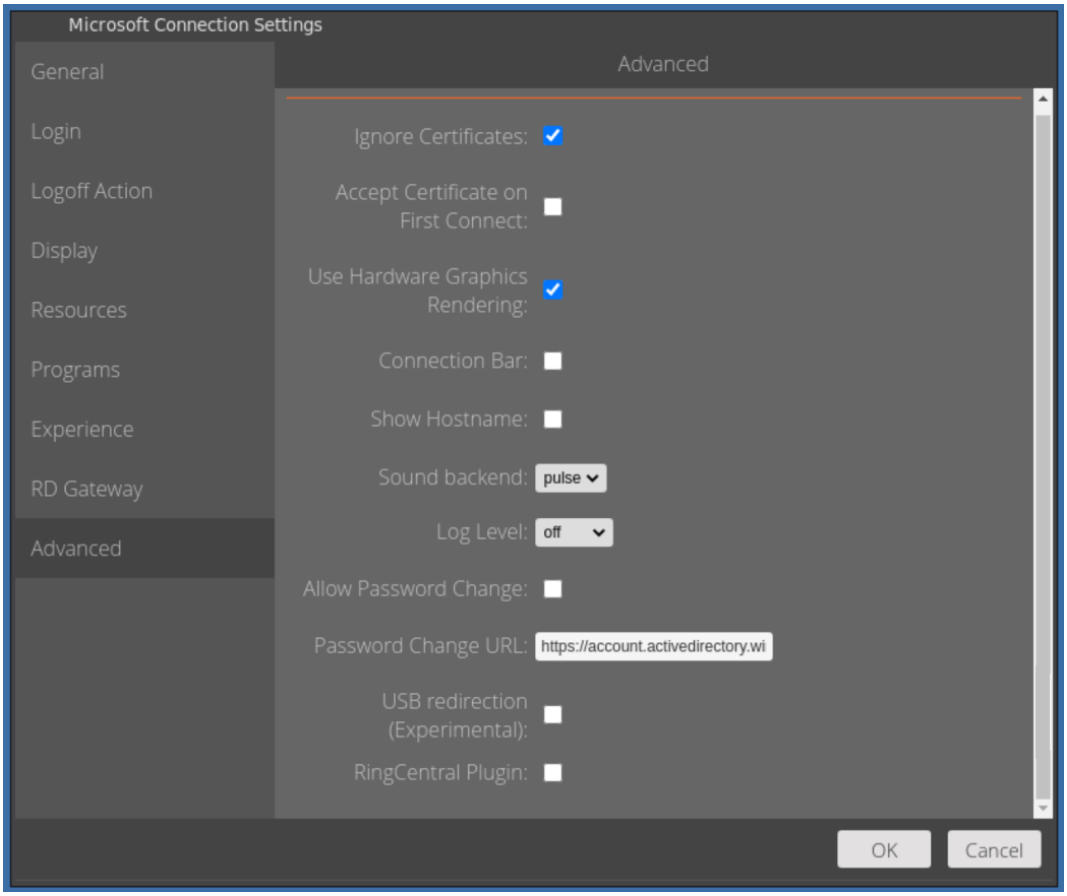
- **Use Credentials from General Tab:** Tick this box to use the credentials supplied at the time of connection or the credentials stored in the "General" tab which will be used both to authenticate to the gateway server and to the remote desktop .

- **Username, Password, Domain:** Enter the username, password, and domain to use for authentication to the remote desktop gateway server. These parameters should be used when Use GW Credentials is enabled.

- **Transport:** This sets the transport protocol to be used by the connection to the RD Gateway. Possible values are "AUTO"(Default), "PC" and "HTTP".

- **Bypass GW:** This option is enabled by default, verify when checked that the gateway settings set are bypassed.

Advanced



- **Ignore Certificates:**
  This option will allow you to ignore server certificates checking when connecting to your RDP server. If you tick this option, then the field “Accept Certificate on First Connect” is not available.

- **Use Hardware Graphics Rendering:**
  Leave this box ticked to take advantage of hardware graphics rendering on your Thin Client where available. This option will offload the video decoding process to the graphical processing unit, rather than in software. In some instances, it can increase performance.

- **Connection Bar:** Determines whether the connection bar appears at the top of the VDI screen in the session.

- **Show Hostname:** Enabling this will display the hostname of the Thin Client in the “Launchpad”.

- **Sound backend:** Possible values are to use pulse or alsa sound configurations. Select the sound system that is used on the client when redirecting audio from the host machine to the client machine. The recommended and default option is pulse, where certain audio devices are having issues, alsa can be tried to determine if it offers a better user experience.

- **Log Level:** Sets the level of log information to be captured during the RDP sessions and is set to “off” by default.

- **Allow Password Change:** When enabled, a padlock icon is added to the launchpad to allow users to click on it to open ZeroWeb to access a self-service password reset web portal.

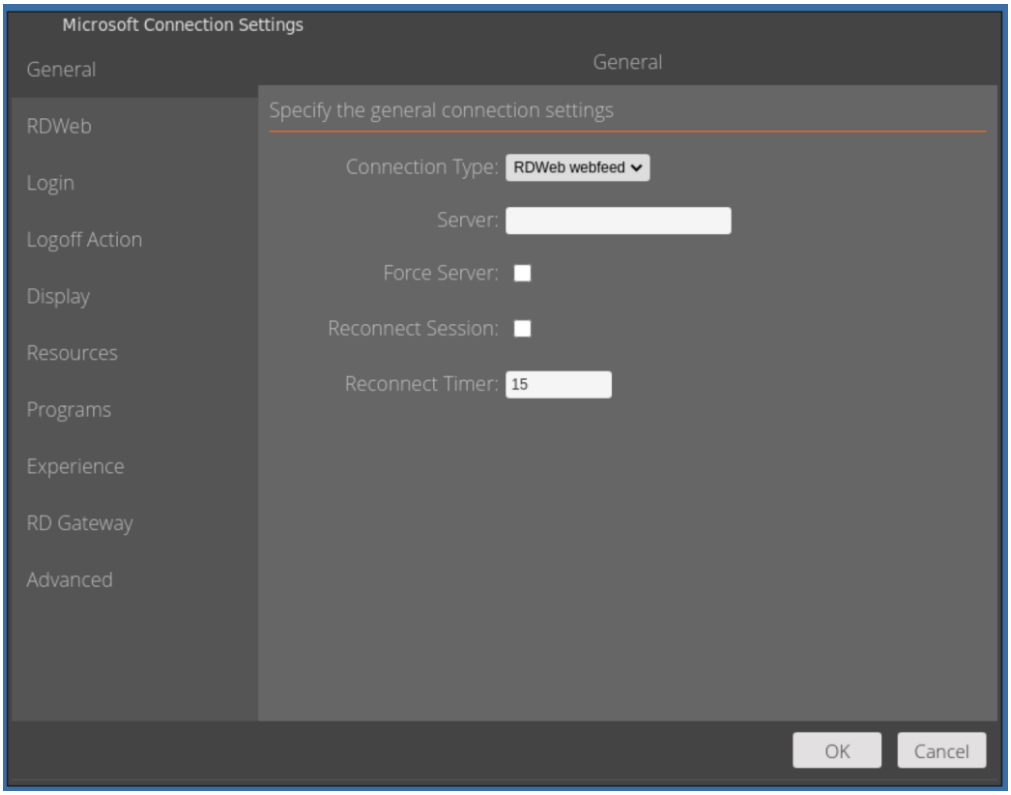
- **Password Change URL:** Define the self-service password reset URL that is to be used when the password reset icon is clicked on the launchpad.

- **USB redirection(Experimental):** Enable this option, at user discretion to redirect your USB devices through to the VDI. Note: This is an experimental feature and as such may produce differing results.

- **RingCentral Plugin:** Enable this option to integrate with the RingCentral app to improve the audio quality of your phone calls.

RDWeb webfeed

General



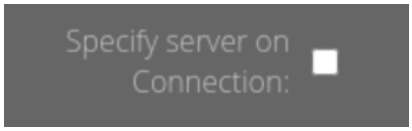
- **Server:** This is where you can enter a single server or multiple URL addresses of the remote desktop connection broker. If multiples are used, then they should be comma separated.

- **Force Server:** If you enter multiple server URLs in the “Server URL” field, comma separated, a drop-down menu is added to launchpad and forces user to select the server before connecting.

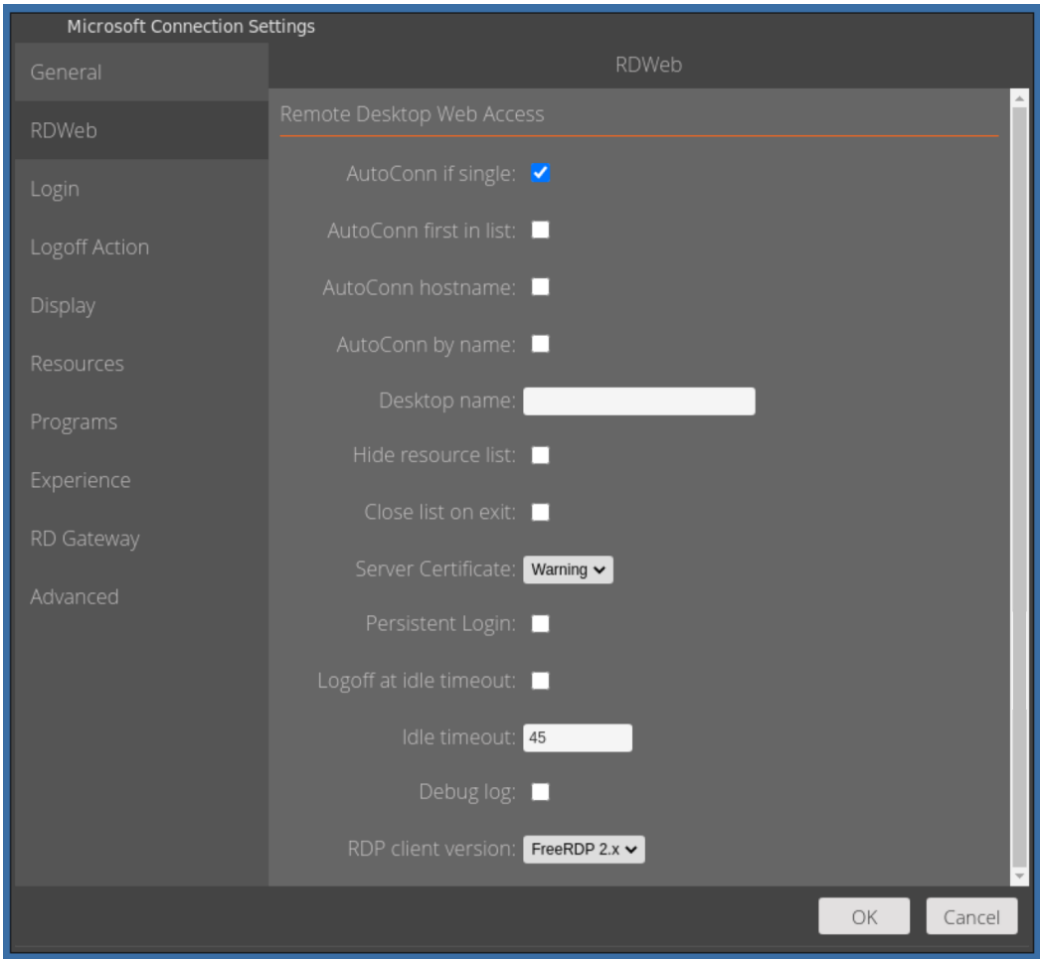
- **Reconnect Session:** When set, this should automatically attempt to reconnect after logging off or disconnecting from a session.

- **Reconnect Timer:** Set the timeout for the reconnect prompt, following disconnect.

- **Note**: If you’re running in “Full Desktop” mode, then you will see an additional field called “Specify server on connection”. This allows you to specify the server details at auth process.



RDWeb



- **AutoConn if single**: Switching this option, will enable automatic connection if just one desktop is assigned to the logging in user.
- **AutoConn first in list**: Switching this option on, will enable automatic connection to the first desktop in the list of assigned desktops to the logging in user.
- **AutoConn hostname**: When enabled, this option will auto connect to a desktop with the same name as the unit hostname.
- **AutoConn by name**: Enabling this option will allow you to specify a desktop name in the following field to auto connect to.
- **Hide resource list**: This will hide the connection broker.

- **Close list on exit:** This auto closes the connection broker after disconnecting from a session.

- **Server Certificate**: This dropdown list determines the behavior of the connection if a Certificate Authentication error occurs. Options are “Accept”, “Warning” or “Reject”.

- **Persistent Login**: To be used with auto login. When you save the credentials in the configuration, the connection goes straight to showing the user entitled app list (Resource List, icon container). When you click "Logoff", the icon container is closed, and you return to the login dialog box. When the Persistent Login is unchecked, the password is removed from the GUI (security). If you want to keep the password there after disconnecting, ready to be used for login, you must check the Persistent Login check box.

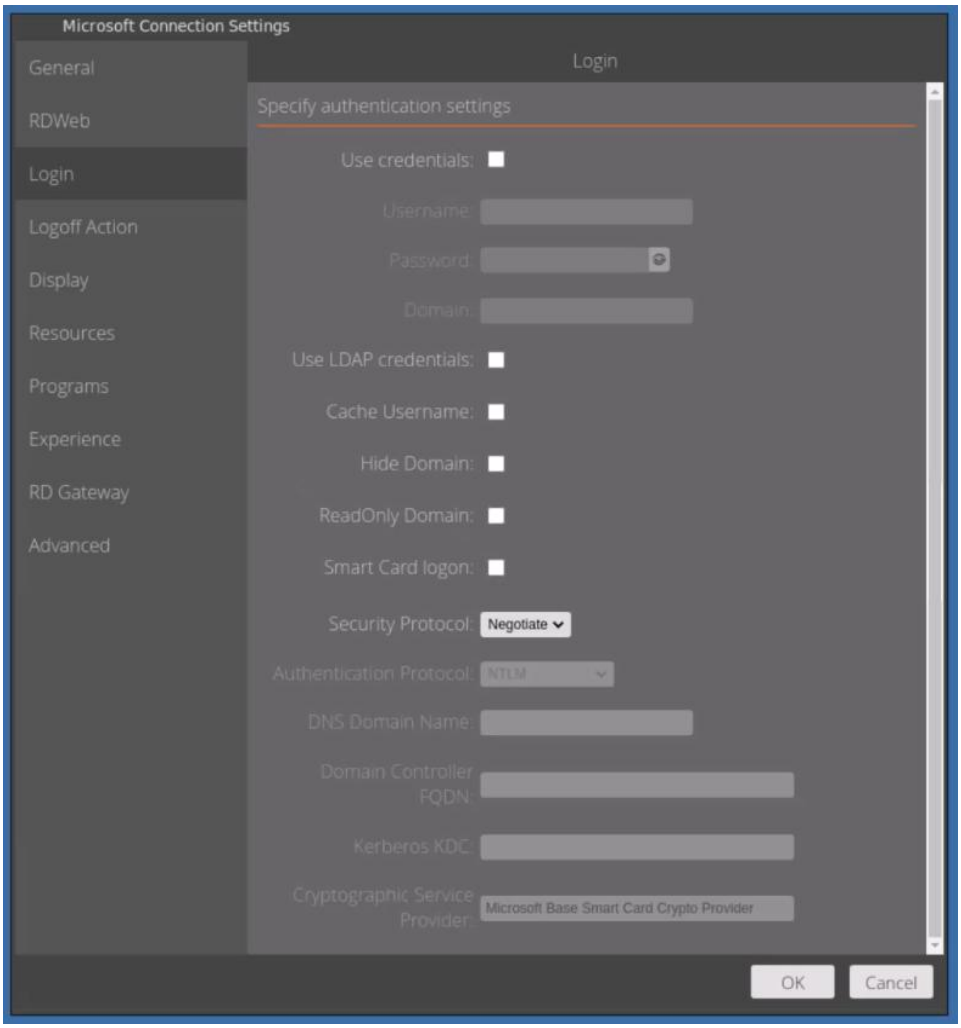
- **Logoff at idle timeout**: After enabling this option, verify the timeout can be edited. After testing idle timeout, disable this option and verify the session does not disconnect after the specified time of inactivity.

- **Idle timeout**: Sets the number to disconnect after inactivity.

- **Debug log**: Enabling this option creates the log files /tmp/tzrdweb.log and /tmp/tzrdweb.xml

- **RDP client version**: This drop down gives you the option to use one of 2 RDP versions, “FreeRDP 2.x” or “10ZiG AVD”. The default is “FreeRDP 2.x”.

Login



- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **Cache Username**: Enabling this, will ensure that the last logged on user is remembered for the next login.

- **Hide Domain**: When this is enabled, the domain field is hidden to the user during login. This is useful in scenarios where you do not want to expose the Domain name / Tenant name to the users during authentication. When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

- **ReadOnly Domain**: When “ReadOnly Domain” is enabled, this prevents the user from editing the Domain name / Tenant name during login.

- **Smart Card logon:** If you enable this, then you can attach a smart card device to your client and use this as the logon option. The remote desktop authentication screen will look like this below. If you do enable this, then the credentials options will be greyed out.

The values below are to be used when implementing Smart Card Logons.

- **Security Protocol**: This is where you can specify a level of Network Authentication for the protocol type. Options are “Negotiate”, “RDP”, “NLA”, or “TLS”.

- **Authentication Protocol:** Options are “NTLM”, “Kerberos” and “NTLM+Kerberos”

- **DNS Domain Name:** This is the domain name that your domain controller resides in.

- **Security Protocol**: This is where you can specify a level of Network Authentication for the protocol type. Options are “Negotiate”, “RDP”, “NLA”, or “TLS”.

- **Domain Controller FQDN:** This is the fully qualified domain name of the domain controller on your network. You can supply multiple domain controllers by separating them with commas.

- **Kerberos KDC:** If you’re using a Kerberos Key Distribution Center, then this is where you can supply the proxy server details. You need to enable “NLA” above, to modify these settings.

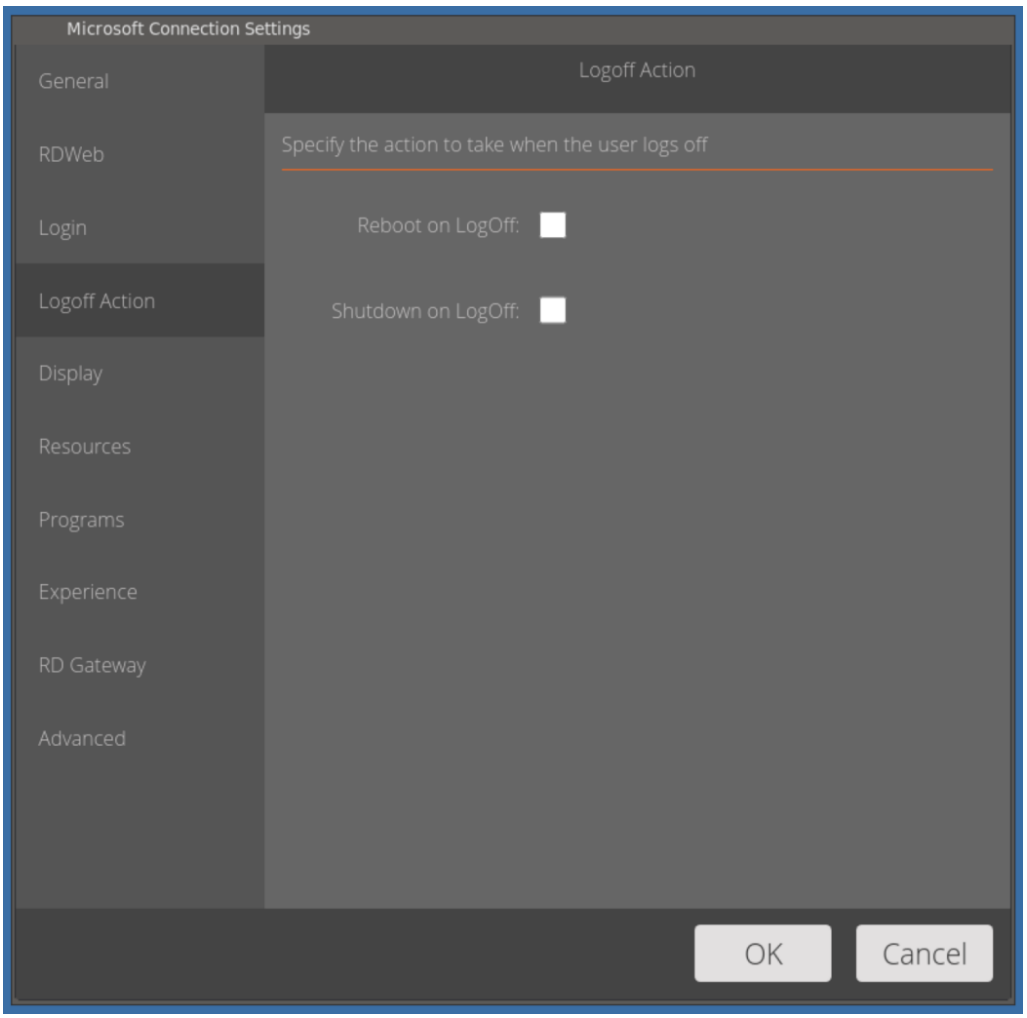
- **Cryptographic Service Provider:** This information is required for the NLA smart card logon and is the name of the Cryptographic Service Provider that Windows logon uses to handle the user certificate. This information can be capture using on Windows the command line certutil -scinfo | findstr Provider .

  For most cards is “Microsoft Base Smart Card Crypto Provider” but it can vary based on the installed Windows middleware and how it is configured.

  For example, for IDPrime 930 cards and SafeNet Windows middleware, this value is “eToken Base Cryptographic Provider” or “Microsoft Base Smart Card Crypto Provider”.

  Note: If you’re running your connection in “Full Desktop” mode, then you will see an additional field called “Use LDAP Credentials”. This will allow you to use your network domain credentials to log in.

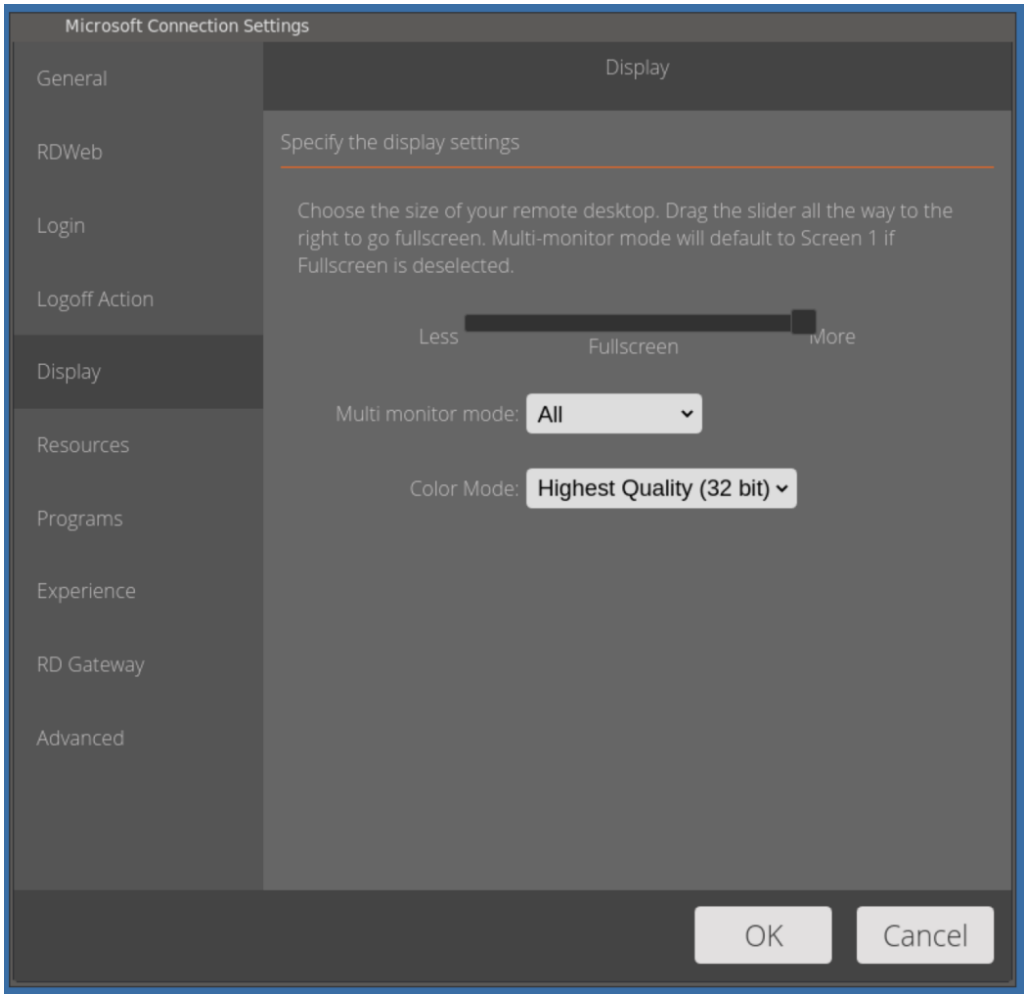
Logoff Action



- **Reboot on LogOff**: Enabling this option will reboot the Thin Client once your user has logged off their current AVD session.

- **Shutdown on LogOff**: Enabling this will shut down and power off the client.

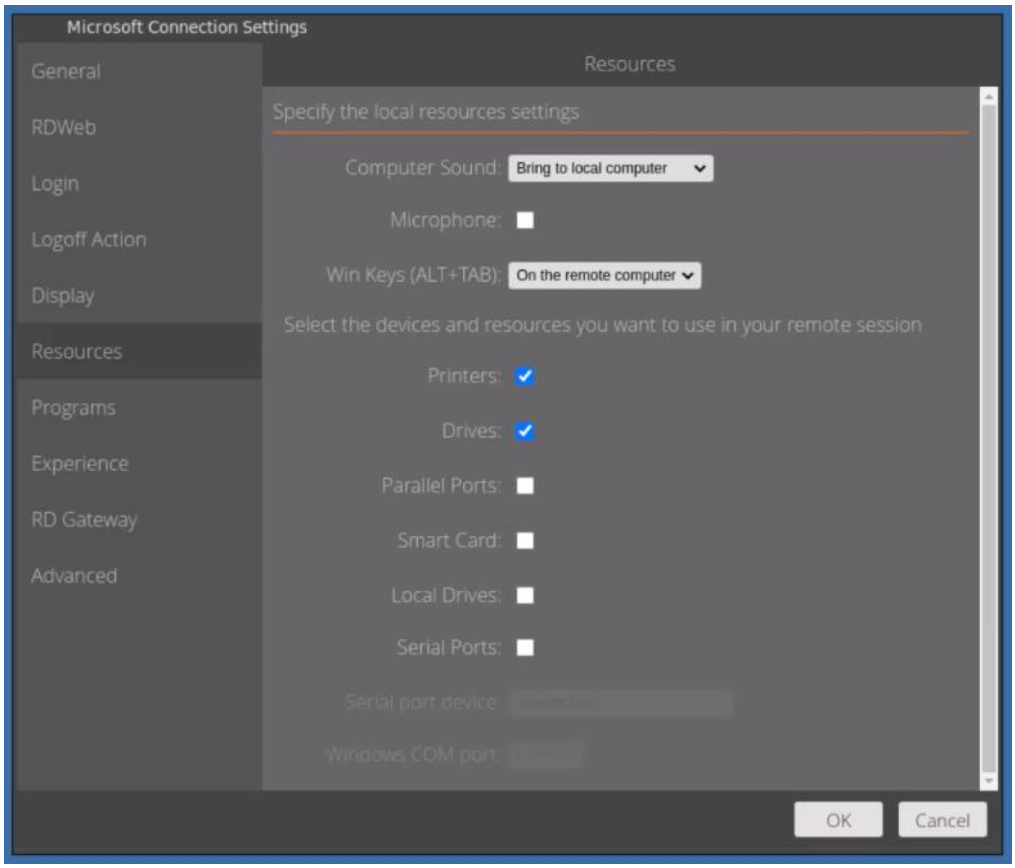
Display



- **Multi Monitor Mode:** Options are for display on monitor 1, 2 or both together.

- **Color Mode:** Changes the color options to suit the particular connection performance. This ranges from 256 colors to “Highest Quality(32 bit)”.

Resources



- **Computer sound:** With "Bring to local computer" enabled, verify the audio from the VDI session can be heard from the Thin Client. Other options include "Do no play" and "Leave at remote computer"

- **Microphone:** Verify the VDI session receives audio input from the Thin Client's local mic.

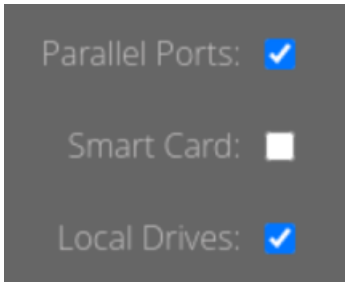
- **Win Keys(ALT+TAB):** With these options enabled verify ALT+TAB operates in the VDI session or on the Thin Client.

- **Drives:** This passes USB mass storage devices to the VDI session.

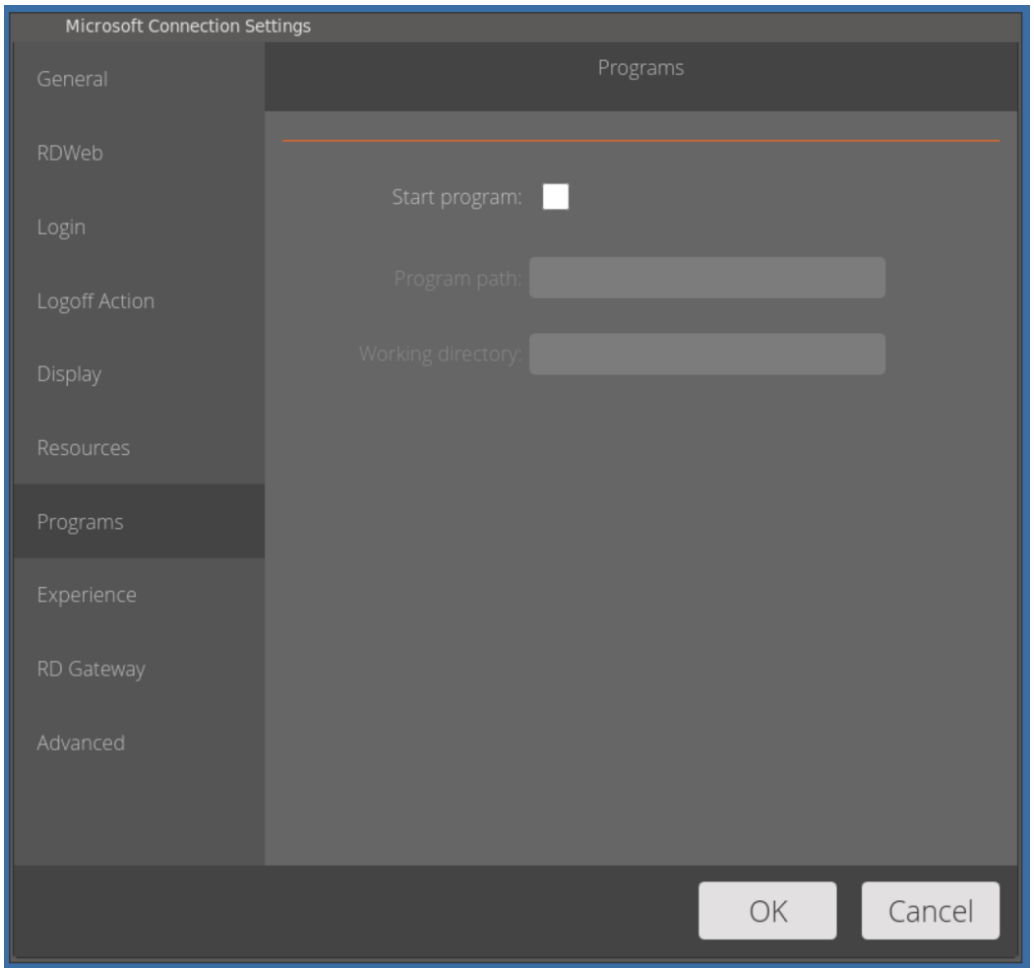
- **Printers:** Enabling this option will enable you to attach a local printer to the Thin Client and then print to it from within the VDI desktop.

- **Smart Card:** This option, when enabled will pass the smart card through to the VDI desktop.

- **Serial Ports:** Tick this option to gain access to serial port configurations below.
- **Serial Port:** If you connect a USB foot to the 10ZiG 6000q, then serial port device “/dev/ttyUSB0" is made available to the VDI.
- **Windows COM port:** With the USB foot attached, you can specify what COM port number will be passed to the VDI.
- **Note:** If you’re running your connection in “Full Desktop” mode, then you will see an additional 2 fields available called “Parallel Ports” and “Local Drives”, so these can also be made available to your remote sessions if required.

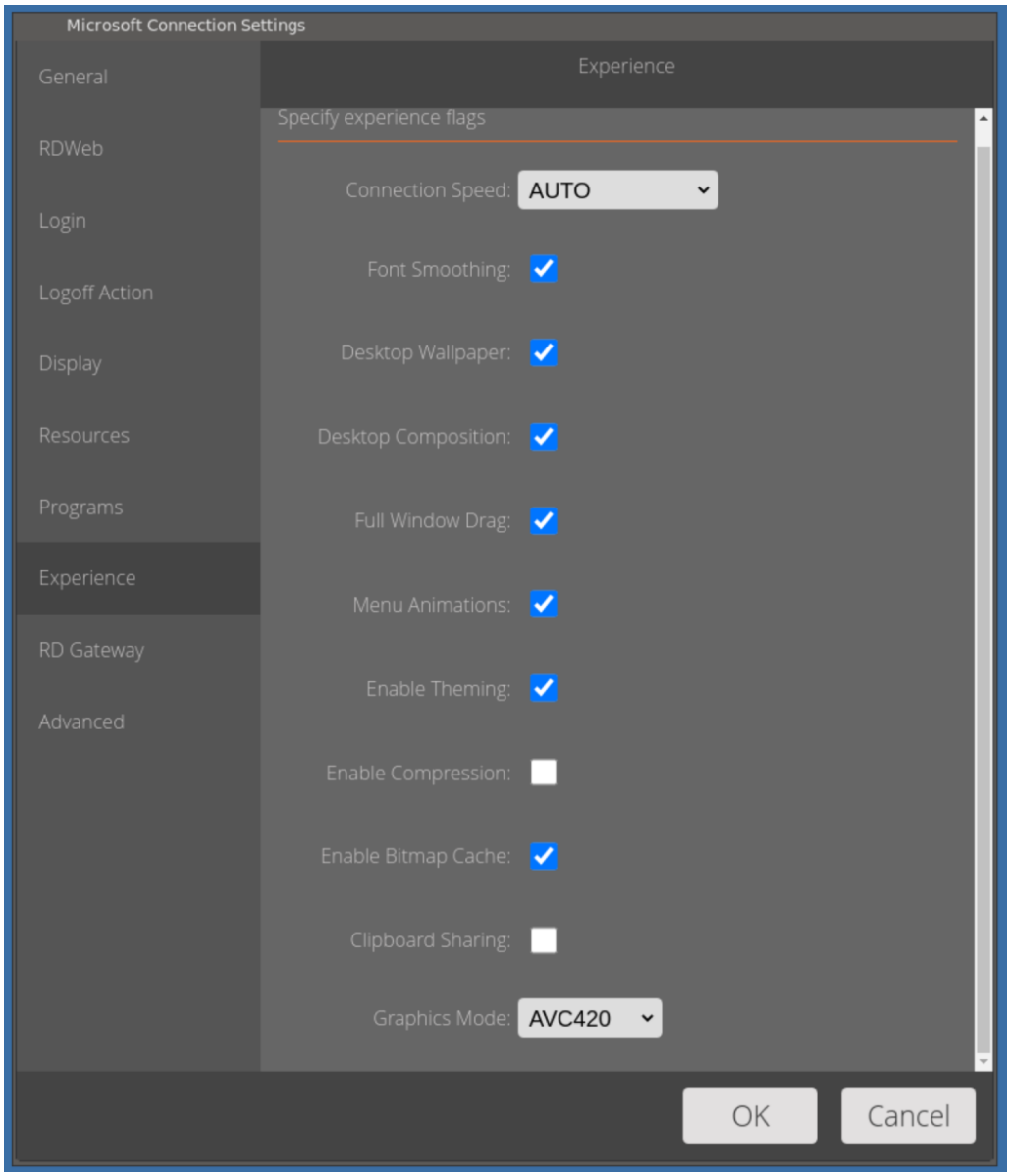


Programs



- **Start program:** When enabled, the Program path, and Working directory fields are available to be set below this field.
- **Program path:** Add a program path, such as C:\windows\system32\notepad.exe. After you establish an RDP connection to a Remote Desktop you will see the “Notepad” program launches.
- **Working directory:** This is the working directory in which the program name above will be launched from.

Experience



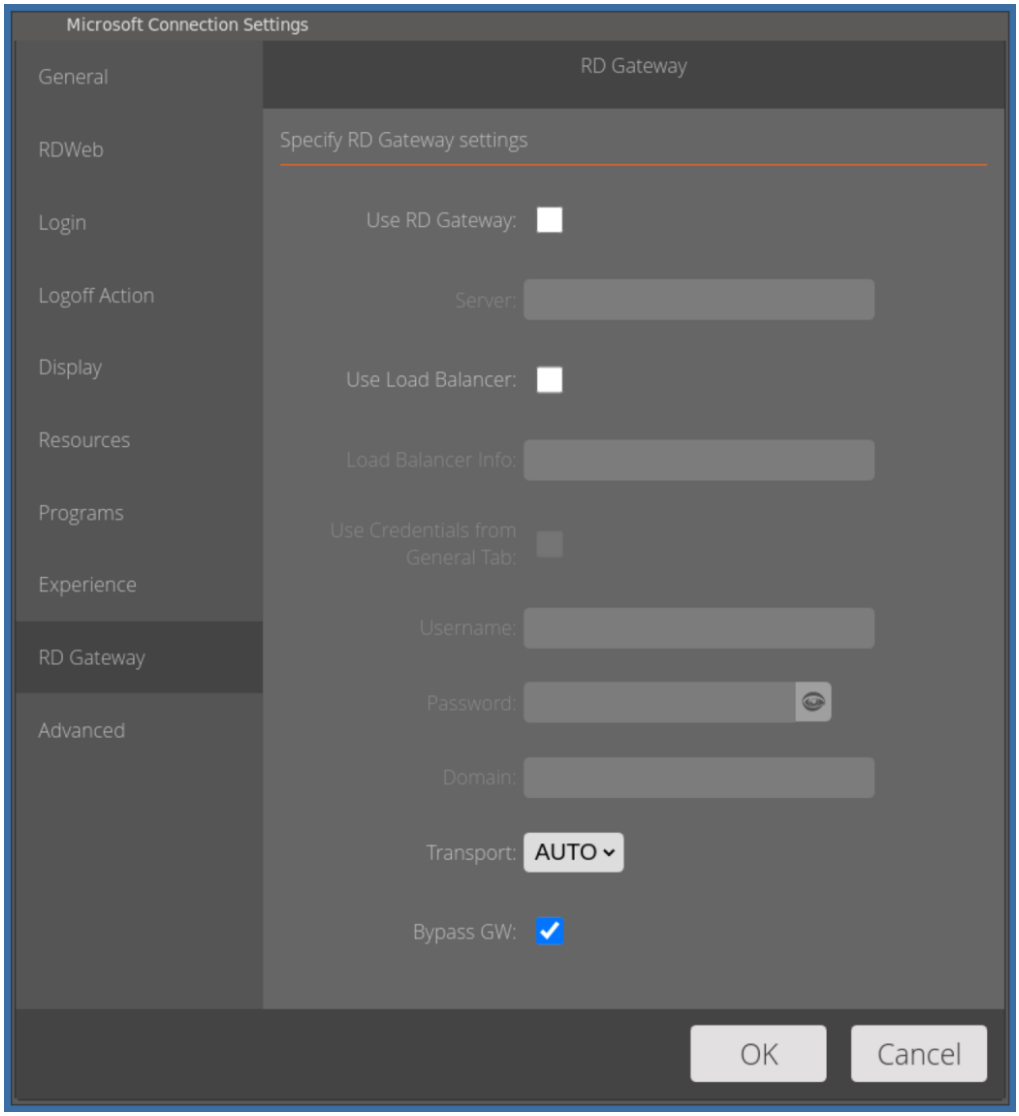
- **Connection speed:** You can adjust this value to suit your individual performance needs, or just leave it as “Auto” for it to negotiate the best speed available.

- **Font Smoothing:** Enables the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.

- **Desktop Wallpaper:** Verify when enabled, the remote desktop shows the wallpaper and when disabled the remote desktop's wallpaper should not be shown.

- **Desktop Composition:** This option either enables or disables the “Aero” effects content of the remote Windows desktop.
- **Full window drag :** When the option is enabled, dragging the remote desktop window should show its content, when disabled, the content will be blank.
- **Menu Animations:** When enabled, the right-click context menus show their animations when opening and closing. Disabled, the right-click context menus show no animation.
- **Enable Theming:** Determines whether themes are permitted when you log on to the remote computer.
- **Enable Compression:** Determines whether bulk compression is enabled when it's transmitted by RDP to the local computer.
- **Enable Bitmap Cache:** Determines whether bitmaps are cached on the local Thin Client (disk-based cache). Bitmap caching can improve the performance of your remote session.
- **Clipboard Sharing:** When enabled, you can copy and paste text from the local client to the remote Windows desktop session and from the remote session to the local client.
- **Graphics Mode:** This feature lets you specify which CODECS to use during the RDP session. Available options are RDP, RemoteFX, AVC420(Default) and AVC444.

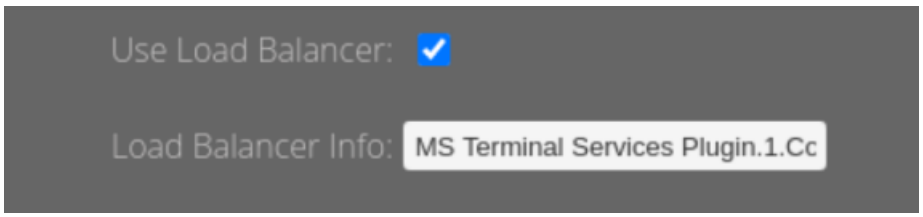
RD Gateway



- **Use RD Gateway:** A RD Gateway allows you to establish a RDP connection to a Windows system but tunneled through a HTTPS connection.
- **Server:** The address of your RD Gateway Server.
- **Load Balancer Info:** This is the address of your load balancer server within your corporation.

  To obtain the address of your load balancer server, follow the steps below :-

1. On Windows 10 or later PC, open up a web browser and type the address below. https://YourRDWebBrokerHostName/rdweb (Where YourRDWebBrokerHostName is the server name hosting the RD Web Broker role) which should take you to the RD web access page.
2. When prompted, log in using valid credentials, and you'll be taken to a page which lists all of your available apps and desktops.
3. Single click on one of the apps/desktops that is a part of your broker collection, this should then download a ".rdp" file (if clicking it tries to launch the session instead, try using a different browser).
4. To get the relevant information needed, right click the ".rdp" file and select "Open with…" and select an editor such as "Notepad".
5. Once opened, look towards the bottom of the file and you should see a line that starts "loadbalanceinfo:s:tsv://". The rest of the string after this point will be unique to each environment, copy or make note of everything that appears after "tsv://" and head back to the thin client. For this example, let's assume the load balancer info we copied following the "tsv://" is MS Terminal Services Plugin.1.CollectionName
6. Inside the RD Gateway configuration screen again on your 10ZiG NOS-M client, tick the box named "Use Load Balancer" and just type or paste the copied value into the "Load Balance Info:" field. See below, using our assumed example.



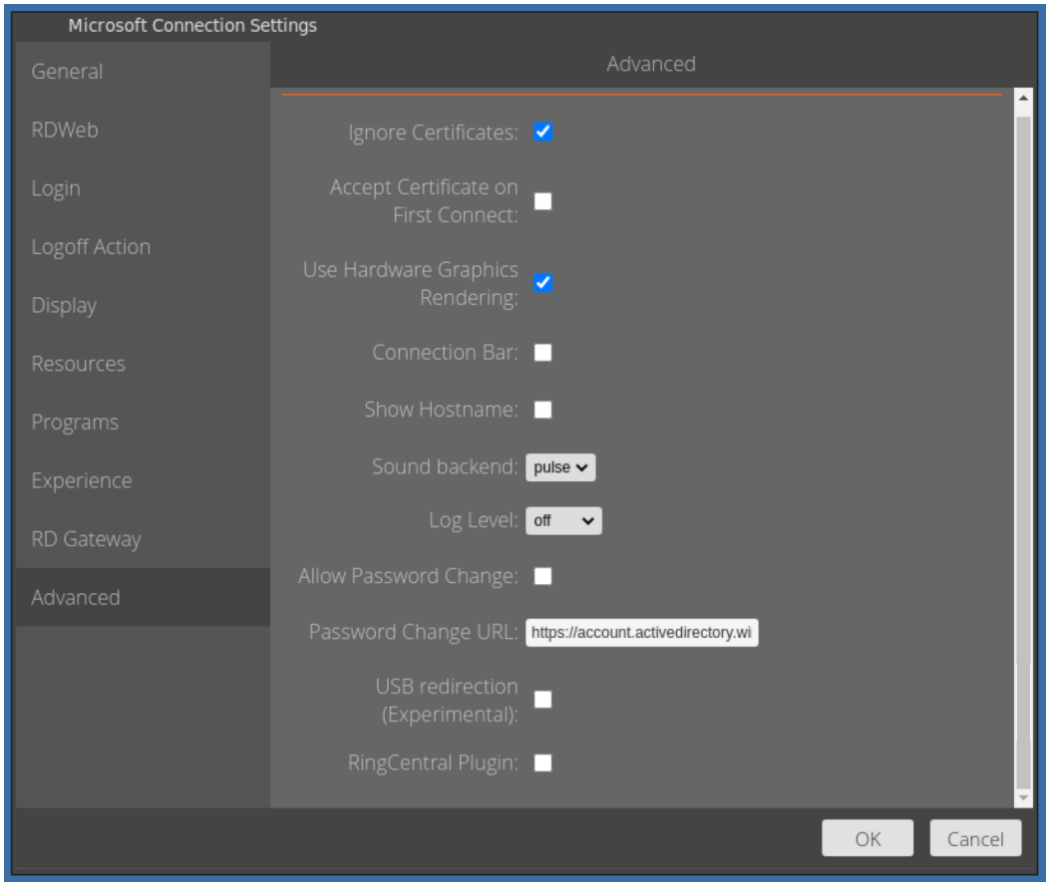
- **Use Credentials from General Tab:** Tick this box to use the credentials supplied at the time of connection or the credentials stored in the "General" tab which will be used both to authenticate to the gateway server and to the remote desktop .

- **Username, Password, Domain:** Enter the username, password, and domain to use for authentication to the remote desktop gateway server. These parameters should be used when Use GW Credentials is enabled.

- **Transport:** This sets the transport protocol to be used by the connection to the RD Gateway. Possible values are "AUTO"(Default), "PC" and "HTTP".

- **Bypass GW:** This option is enabled by default, verify when checked that the gateway settings set are bypassed.

Advanced



- **Ignore Certificates:**
  This option will allow you to ignore server certificates checking when connecting to your RDP server. If you tick this option, then the field “Accept Certificate on First Connect” is not available.

- **Accept Certificate on First Connect:** Accept certificate unconditionally on first connect and deny on subsequent connections if the certificate does not match.

- **Use Hardware Graphics Rendering:**
  Leave this box ticked to take advantage of hardware graphics rendering on your Thin Client where available. This option will offload the video decoding process to the graphical processing unit, rather than in software. In some instances, it can increase performance.

- **Connection Bar:** Determines whether the connection bar appears at the top of the VDI screen in the session.

- **Show Hostname:** Enabling this will display the hostname of the Thin Client in the “Launchpad”.

- **Sound backend:** Possible values are to use pulse or alsa sound configurations. Select the sound system that is used on the client when redirecting audio from the host machine to the client machine. The recommended and default option is pulse, where certain audio devices are having issues, alsa can be tried to determine if it offers a better user experience.

- **Log Level:** Sets the level of log information to be captured during the RDP sessions and is set to “off” by default.

- **Allow Password Change:** When enabled, a padlock icon is added to the launchpad to allow users to click on it to open ZeroWeb to access a self-service password reset web portal.

- **Password Change URL:** Define the self-service password reset URL that is to be used when the password reset icon is clicked on the launchpad.

- **USB redirection(Experimental):** Enable this option, at user discretion to redirect your USB devices through to the VDI. Note: This is an experimental feature and as such may produce differing results.

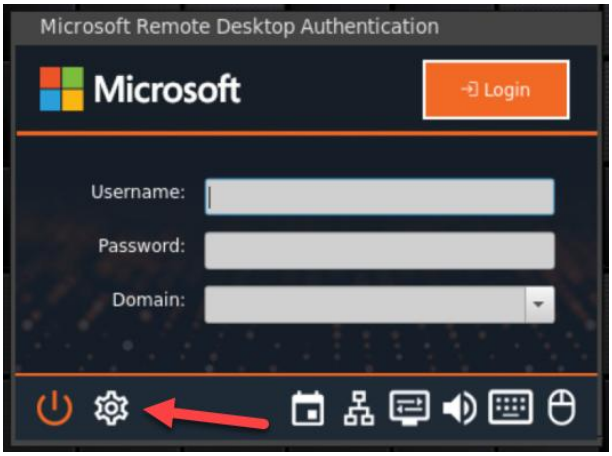
- **RingCentral Plugin:** Enable this option to integrate with the RingCentral app to improve the audio quality of your phone calls.

Saving your settings

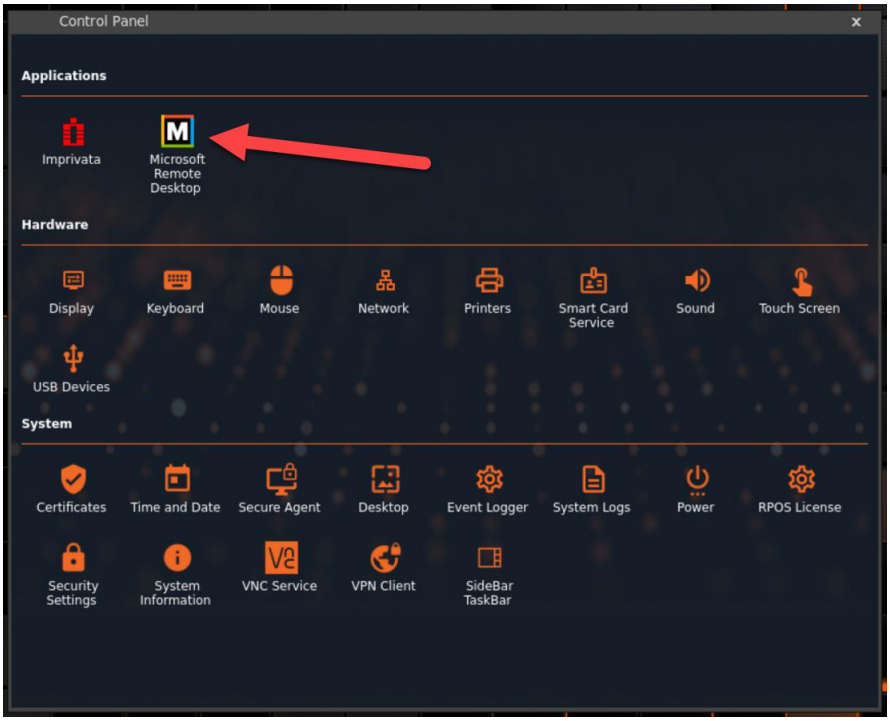
Once you're comfortable with all the settings for your 10ZiG NOS-M client, just click the "OK" button and you'll be taken back to the Microsoft Remote Desktop Authentication screen.

Editing your connection settings

If you need to edit your connection settings again, then click the "Gear" icon in the bottom left of the "Login" screen as shown by the "red arrow" below.



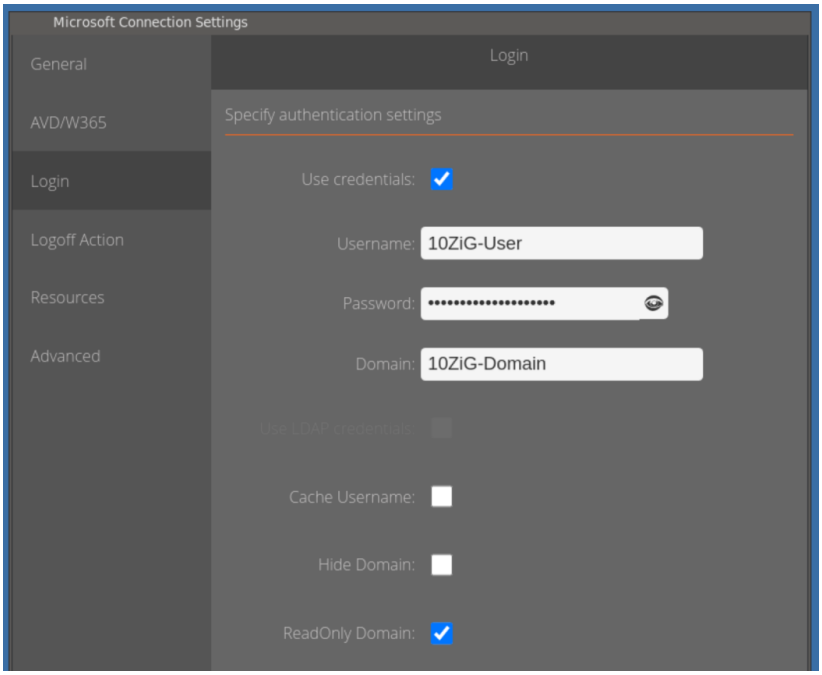
You'll be taken back into the "Control Panel", where you can click the "Microsoft Remote Desktop" icon in the top left and then make changes as outlined in the previous sections of this guide.



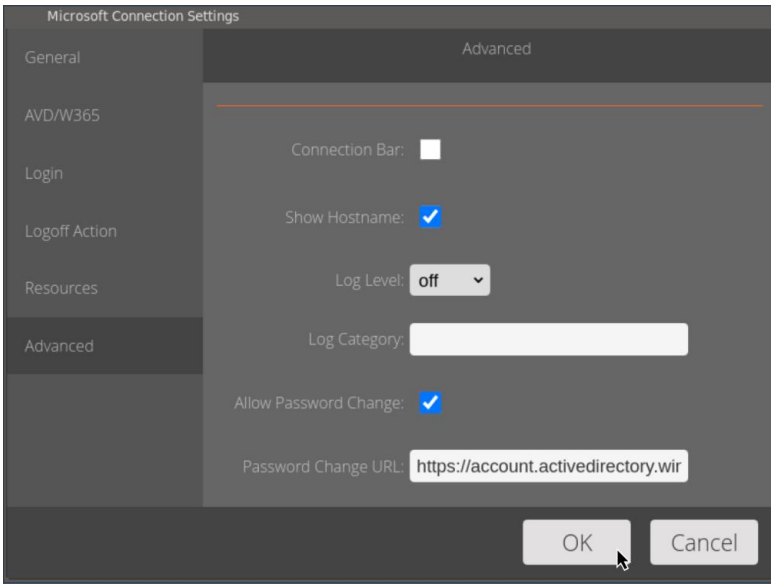
Azure Virtual Desktop – Connection setting examples

Here are some examples of how to setup your “Microsoft Remote Desktop Authentication” login screen.

Inside the “Control Panel”, click on “Microsoft Remote Desktop” icon, and then select the “Login” tab in the left menu. Tick the “Use credentials” box, key in the “Username”, “Password” and “Domain” fields and then tick the “ReadOnly Domain” box.

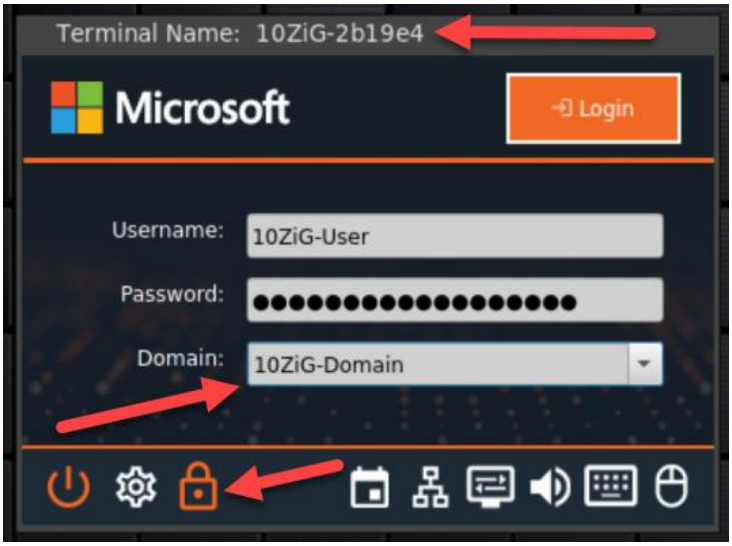


Finally, click on the “Advanced” menu option, tick “Show Hostname” and then “Allow Password Change” boxes. Click “OK” to save the changes.



Close the “Control Panel” as below.

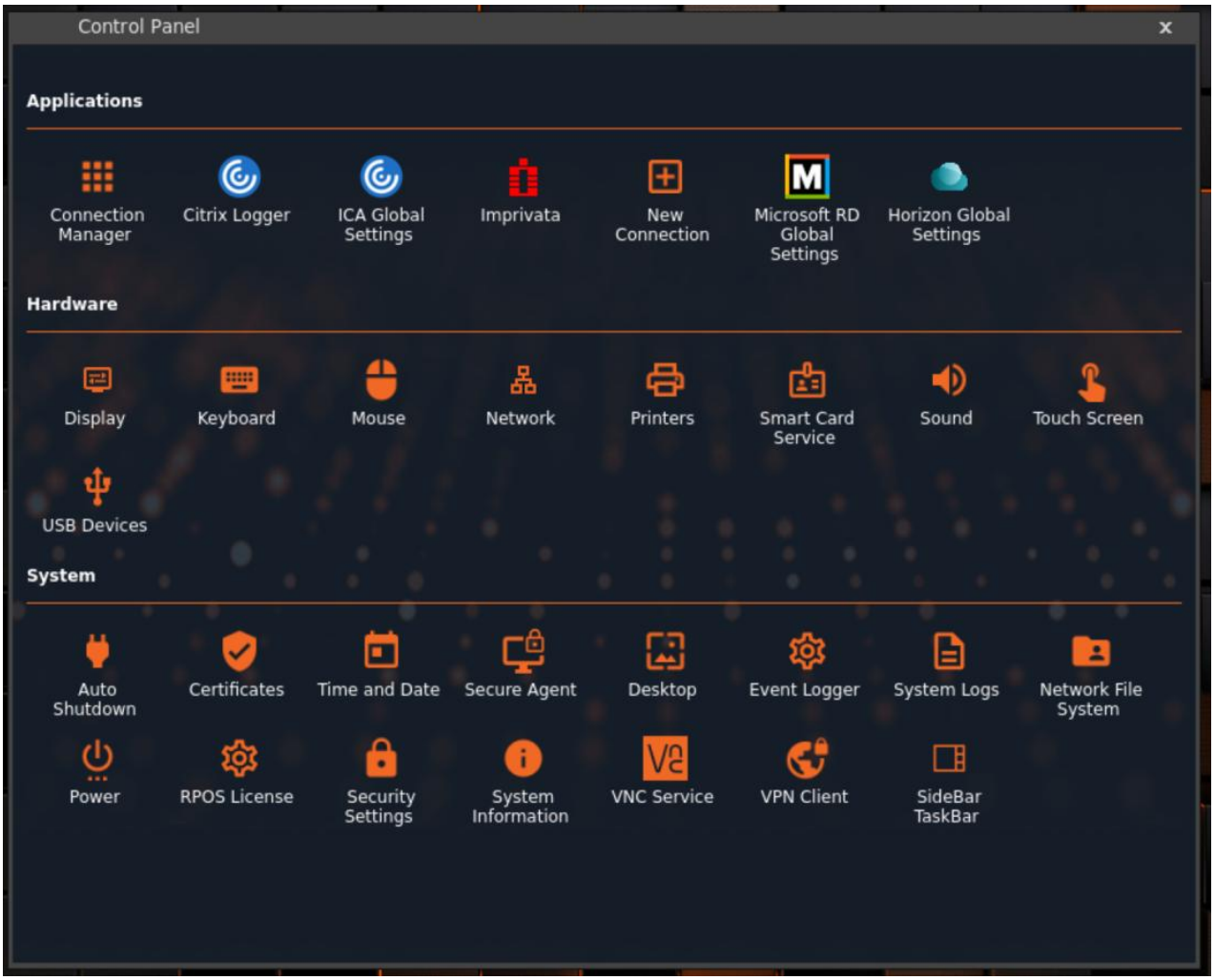
Your login screen should now look like the one below. Notice that the “Password Change” icon is present, the terminal hostname is displayed on the top bar and the domain field is “Read Only”, indicated by the red arrows.



Control Panel Settings

We mentioned how to access the Control Panel earlier on in this guide in the section named "Access to the Control Panel", click the link to the left to jump back to that section.

As a reminder, just look out for and click the "Gear" icon and you'll be taken into "Control Panel", where you have the ability to further customize your 10ZiG Thin Client's "Application", "Hardware and "System" settings.

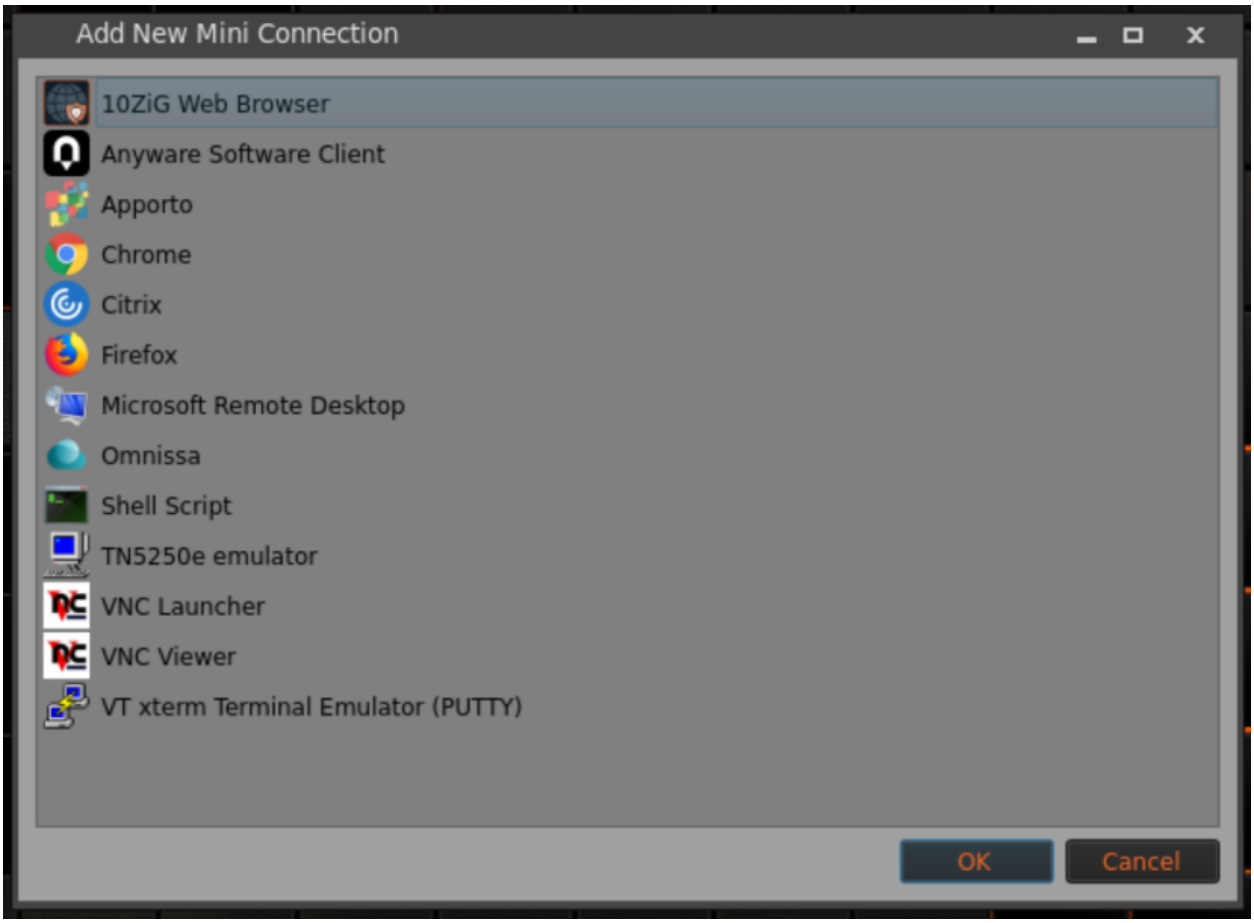


Applications

Connection Manager

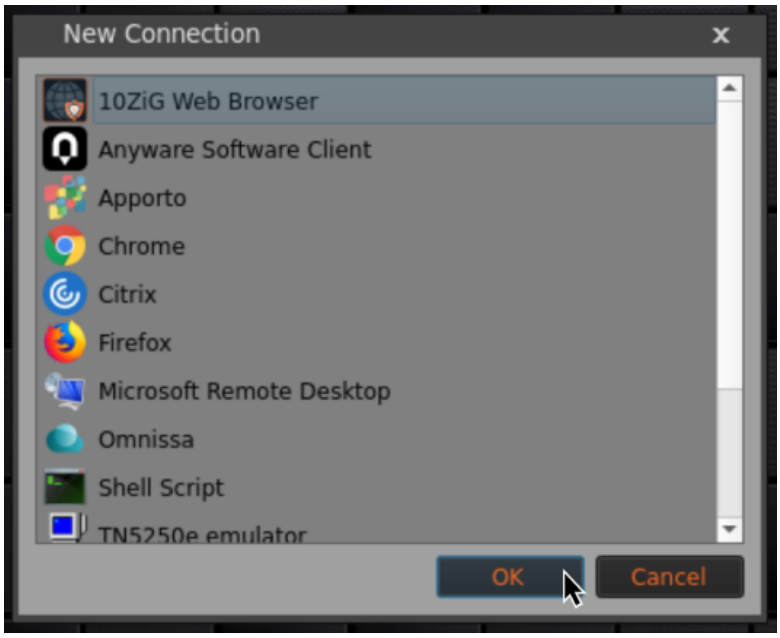
The Connection Manager allows you to create and customize your own connection types. The Connection Manager can also be launched from the right-click context menu and taskbar in “Full Desktop” mode and runs by default as the controlling window in Portal Mode.

Currently supported connection types are listed below and include the “10ZiG Web Browser”, “Anyware Software Client”, “Apporto”, “Chrome”, “Citrix”, “Firefox”, “Microsoft Remote Desktop”, “Omnissa”, “Shell Script”, “TN5250e Emulator”, “VNC Launcher”, “VNC Viewer” and “VT xterm Terminal Emulator(PUTTY)”



Creating a New Connection using the Connection Manager

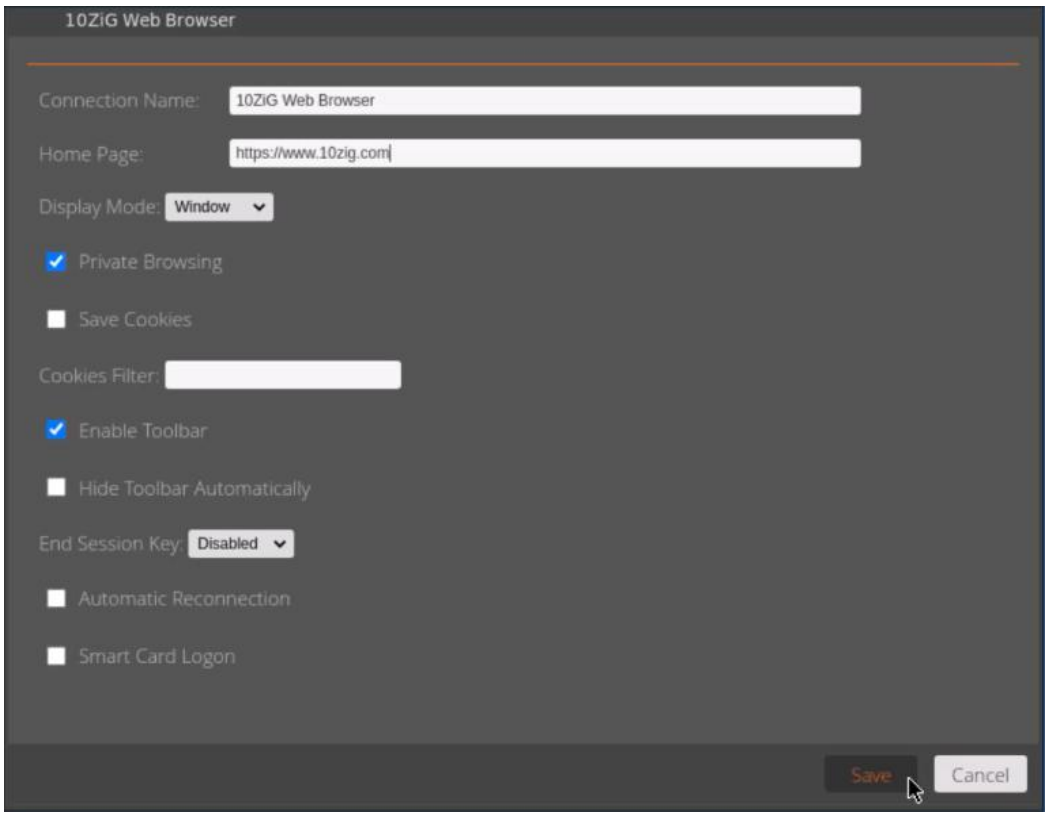
Click on the “Connection Manager” inside the Control Panel in in “Full Desktop” mode or from inside the “Connection Manager” in “WBT” mode. Click “New" and then on the “New Connection” screen, highlight your desired connection type and click “OK” or just double-click it.



The example above shows selecting a “10ZiG Web Browser” connection type to start the setup process for.

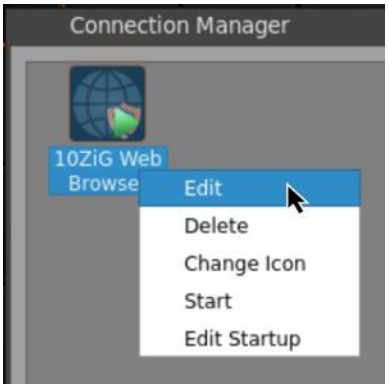
Saving your settings

Once you have completed your connection setup and you're happy with the contents, then simply click "Save" in the bottom right of the dialog box or click "Cancel" to exit the dialog without saving.



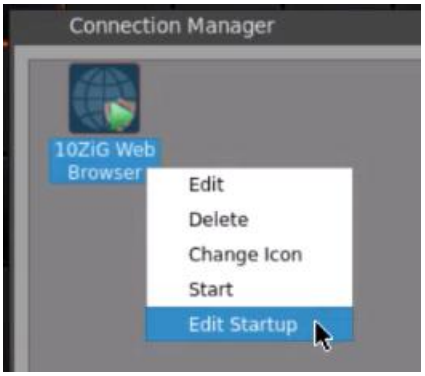
Editing your Connection settings

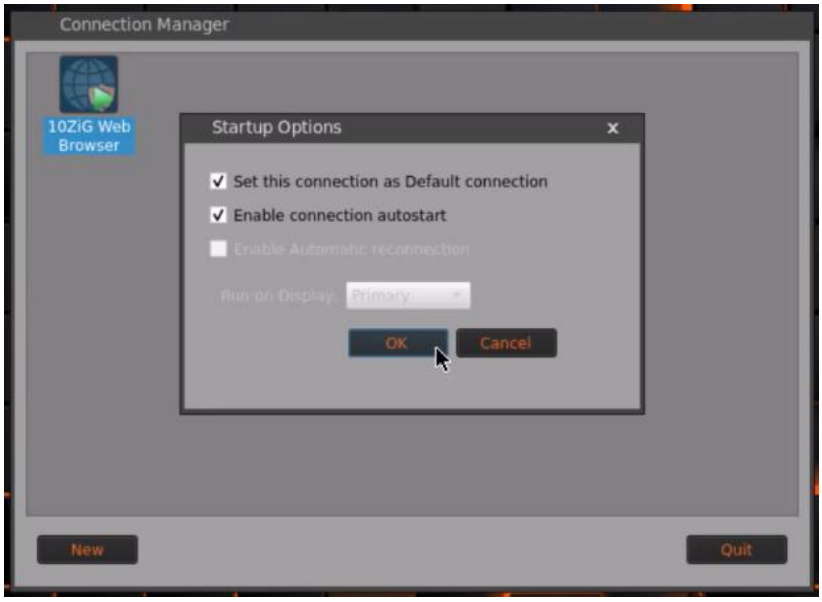
If you're operating in "Full Desktop" or "Portal Mode", editing your settings is the same. You just need to right click on the icon, whether it's on the desktop or inside the "Connection Manager" and then select "Edit" from the drop-down menu. Once you have finished editing the settings, just click "Save".



Startup options for your Connections in Kiosk Mode

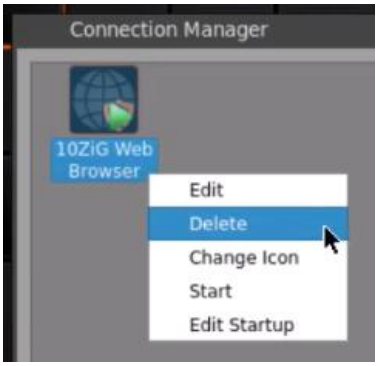
If you run your Thin Client desktop in “Kiosk” mode, you have to set one of your connections to be the default connection that starts up at boot and also set “Enable connection autostart” so that the connection restarts each time you close it.





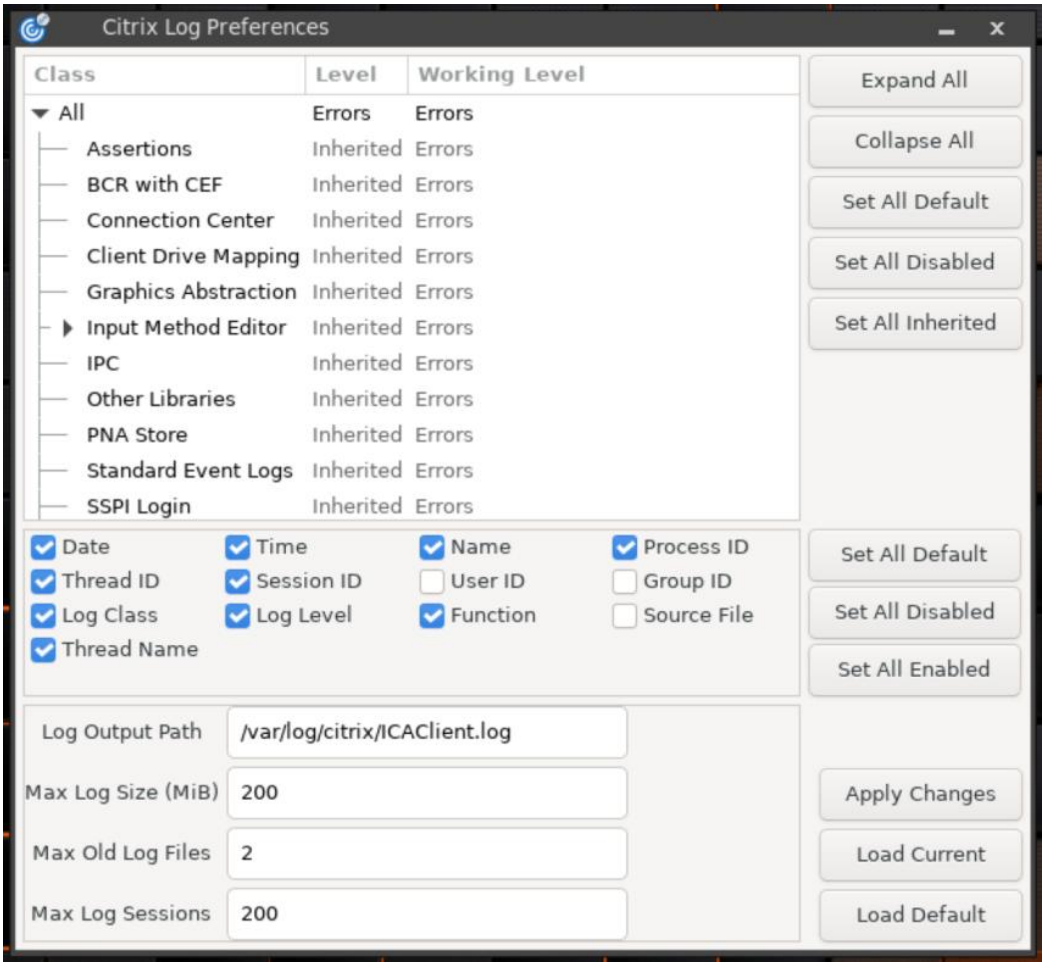
Deleting your Connection settings

If you want to delete the connection altogether, you just need to right click on the icon, whether it’s on the desktop or inside the “Connection Manager” and then select “Delete” from the drop-down menu.



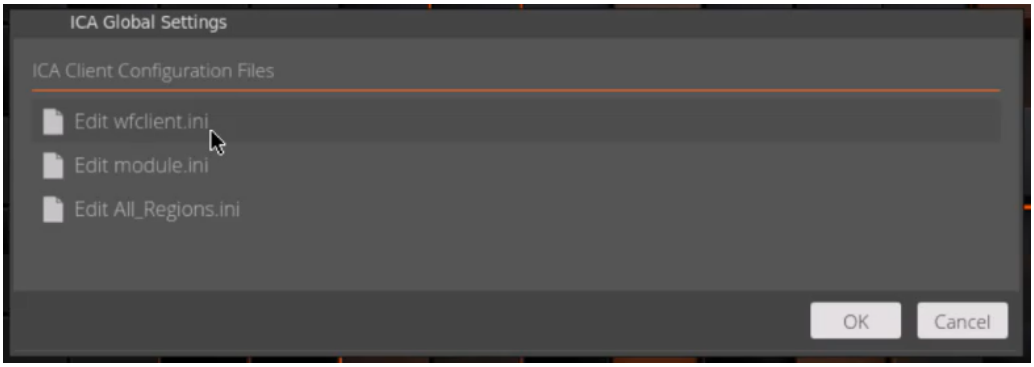
Citrix Logger

Citrix Logger allows you to fully customize the amount of log information stored when launching and running your Citrix connection sessions. The log output path is set to /var/log/citrix/ICAClient.log by default and can be changed to suit your particular requirements.

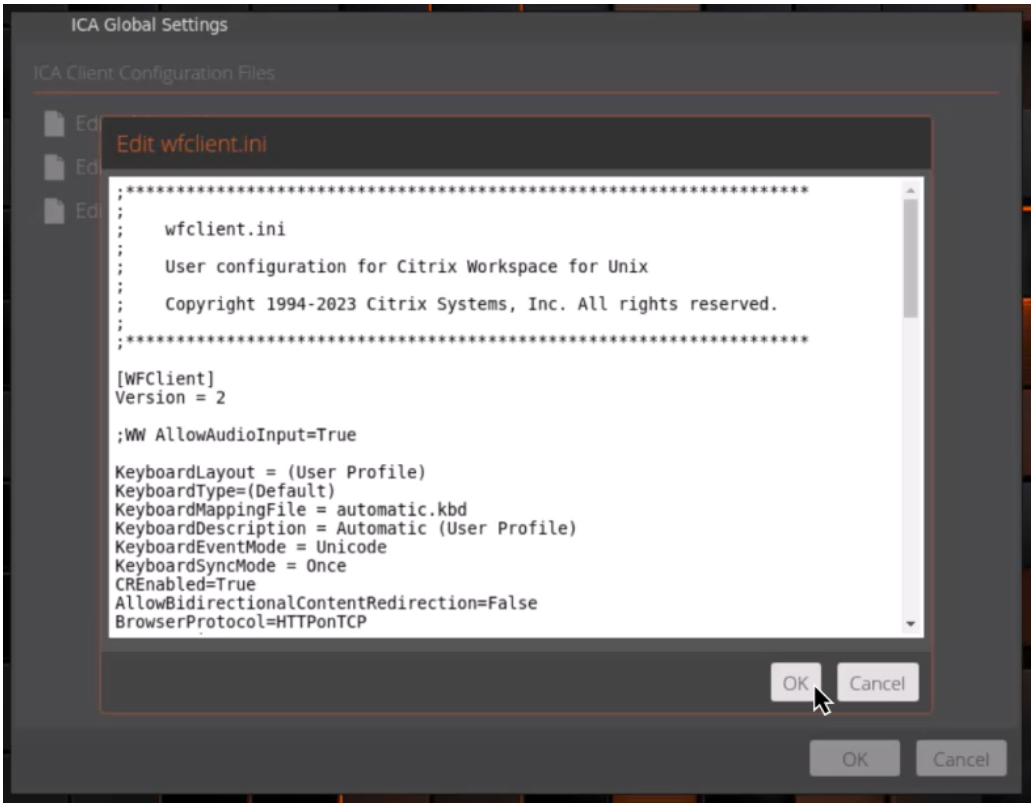


ICA Global Settings

This area controls global settings for ICA sessions. This assists in setting some of the standard settings for ICA clients to enable the same display settings, devices, hot-keys, servers and firewall and proxy settings. Inside the ICA Global Settings dialog box, click on any of the edit “wfclient.ini”, “modeule.ini” or “All_Regions.ini” to change the settings specific to those files and click “OK” inside the ini file editor to save your changes.

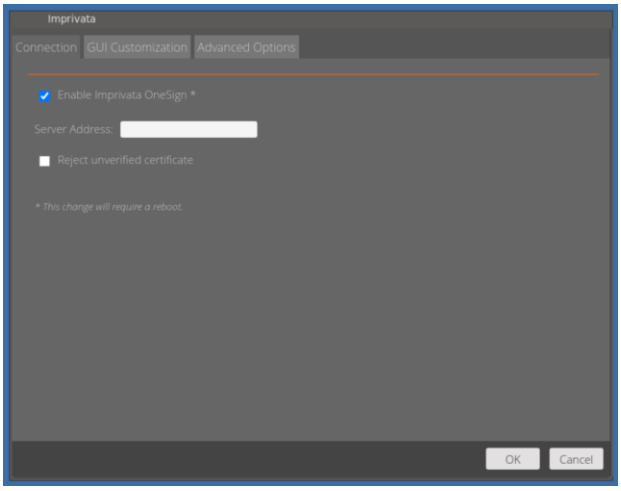


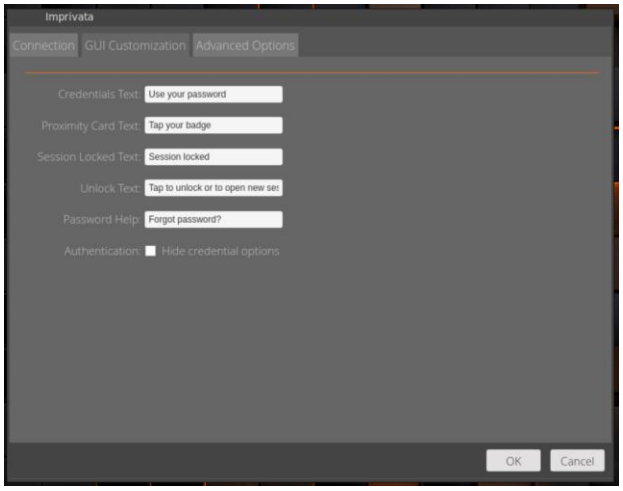
The example below shows editing of the “wfclient.ini”.

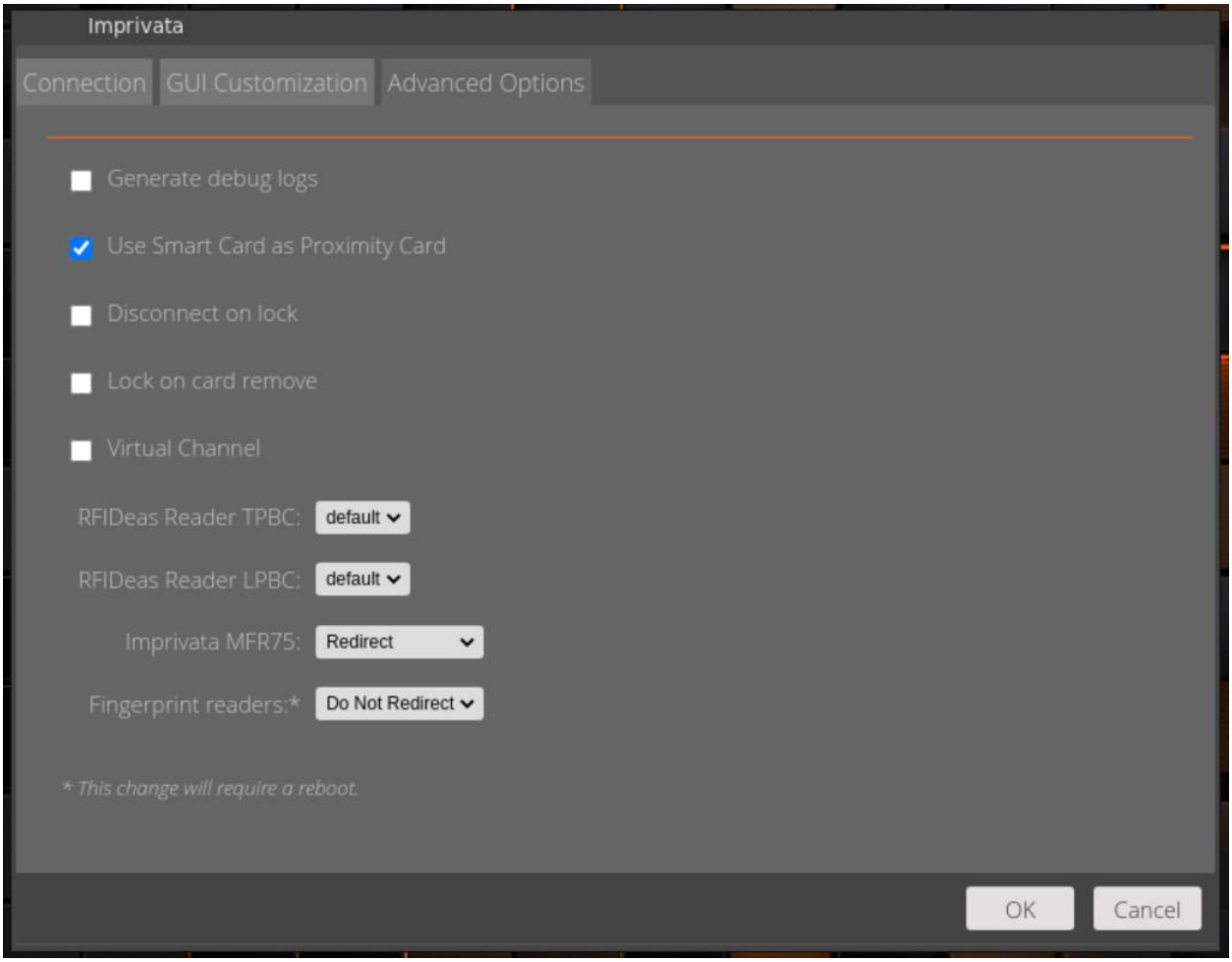


Imprivata

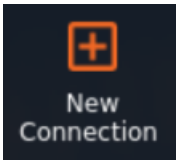
If you intend to use your Thin Client with Imprivata OneSign, then this is where you'll find the configuration screens needed to setup and fine tune it.



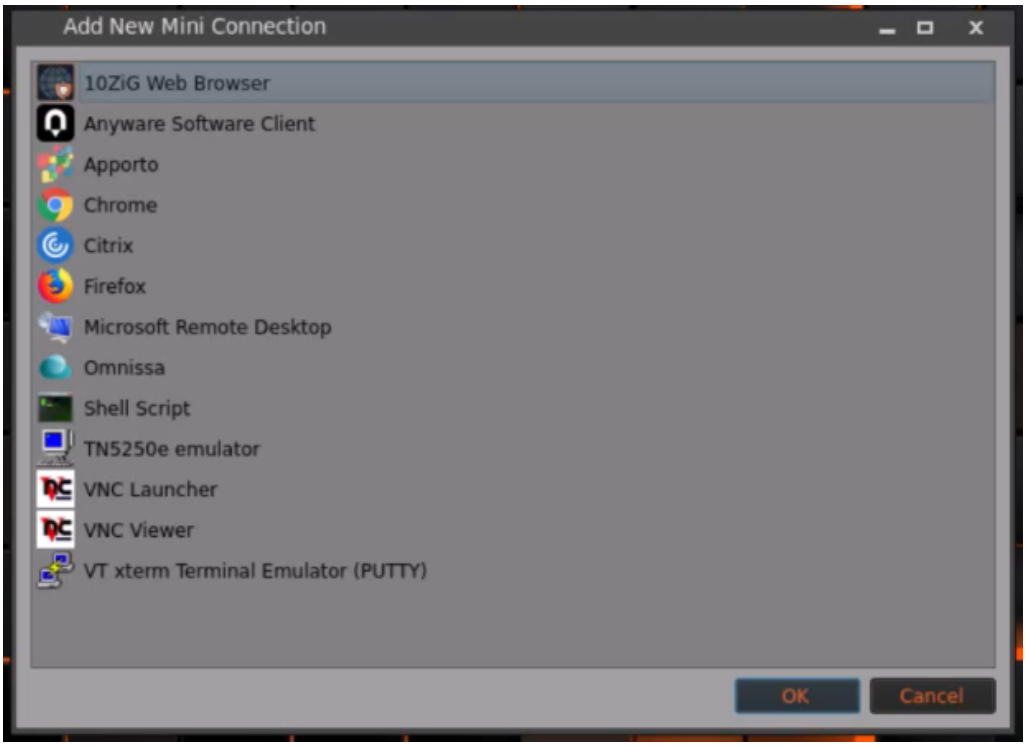




New Connection



The “New Connection” option can be found inside the Control Panel in both “Portal” and “Full Desktop” modes and on the taskbar in “Full Desktop” mode. It also appears as “Add Connection” in the right click context menu in “Full Desktop” mode as shown below.

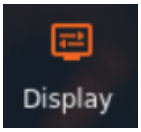


“Add Connection” from Right click context menu in “Full Desktop” mode.

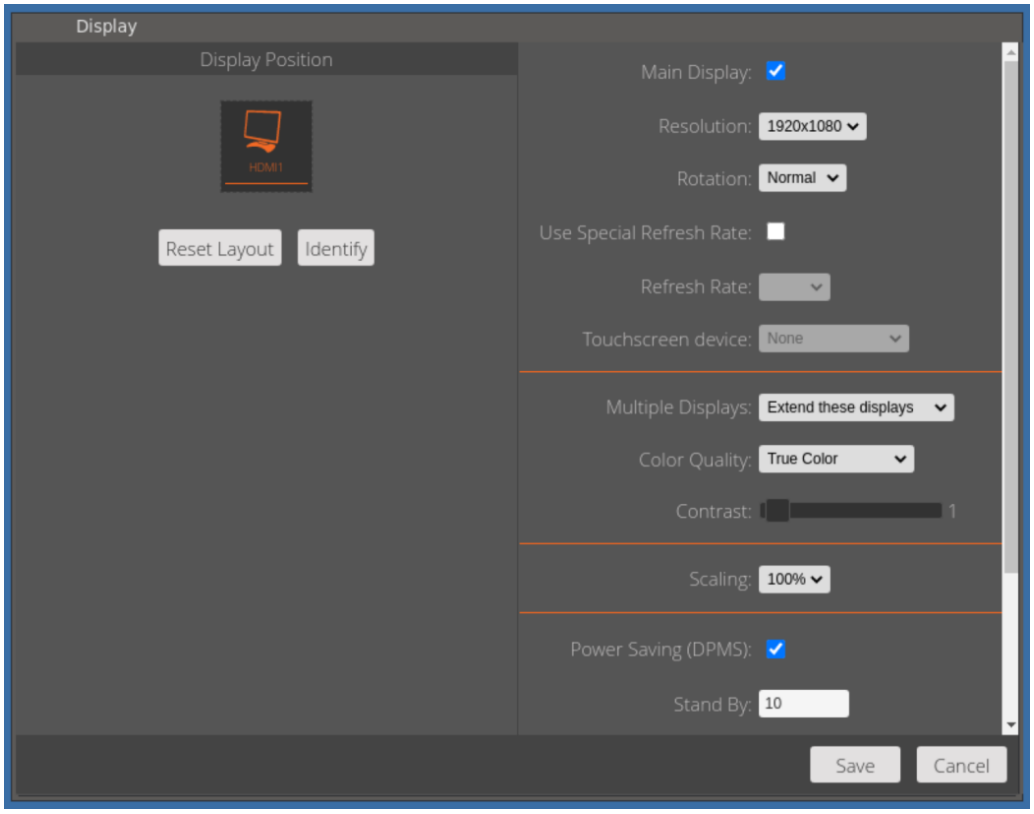
“New Connection” from taskbar.

Hardware

Display

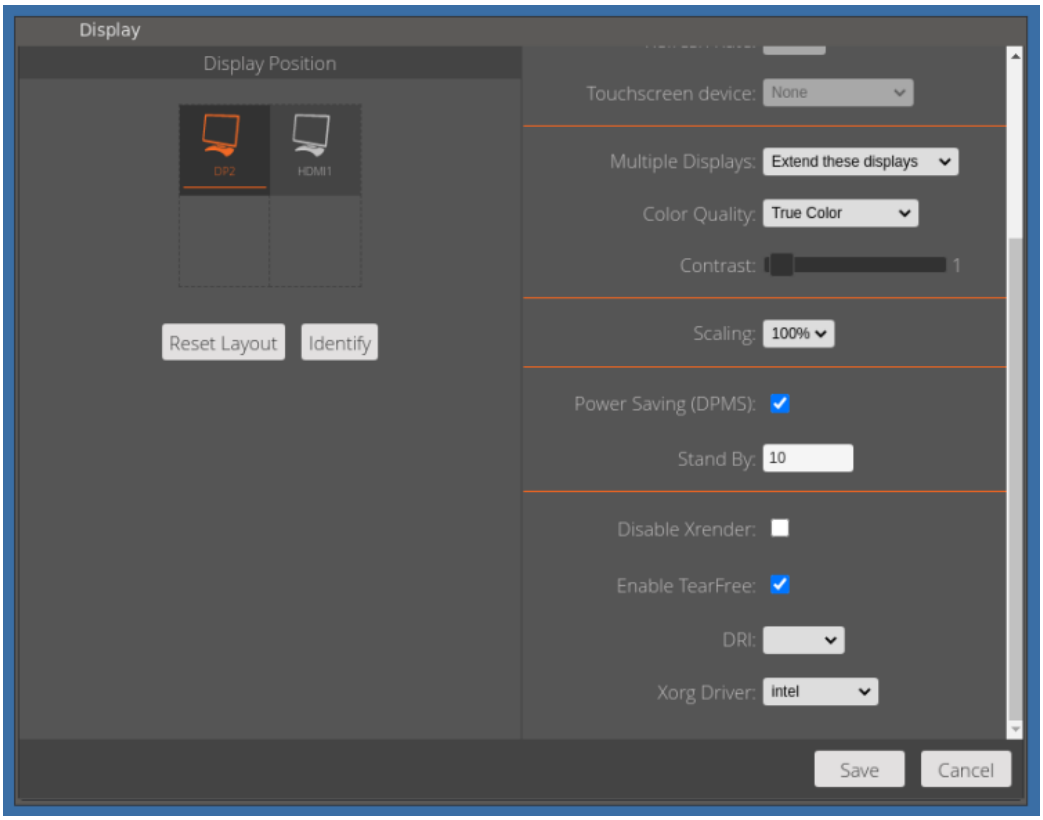


The Display Settings window allows you to configure your screen resolution along with the refresh rate and the color quality. Other options here include rotation and support for multiple displays, if detected.



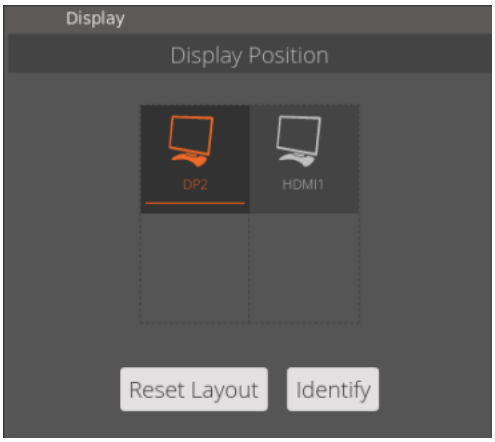
Dual Monitors

When multiple displays are detected, you will be given the option to select “Main Display” for either HDMI1 or DP2(shown here), and either to duplicate or extend these displays.



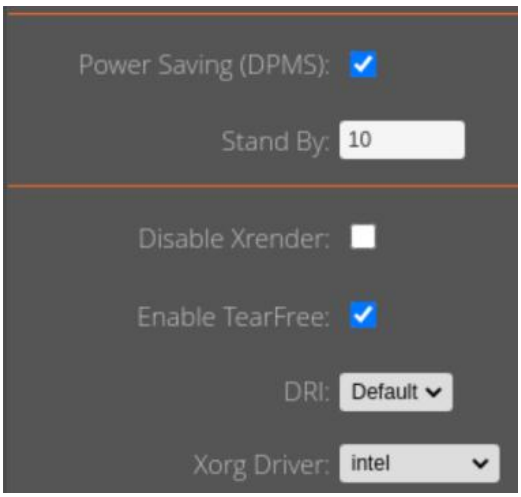
You can change the resolution of each monitor by selecting the resolution you want for HDMI1 and DP2.

If you choose to extend these displays you can choose the position of the 2nd monitor to Right, Left, or Inverted depending on how you wish your display topology to be.



Power Saving (DPMS)

You can also enable Power Saving(DPMS) settings and also specify how long, in minutes, to wait before going to standby mode.



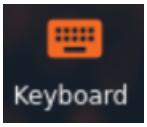
Xrender is on by default, clicking “Disable Xrender”, will disable it, but may affect webcam handling as a result. TearFree is also enabled to improve display performance.

DRI Direct Rendering Infrastructure version. Further information can be found here regarding DRI https://en.wikipedia.org/wiki/Direct_Rendering_Infrastructure

Enabling “Restart Xorg on hotplug event” will force a refresh of the displays, to make sure any hotplugs are detected correctly.

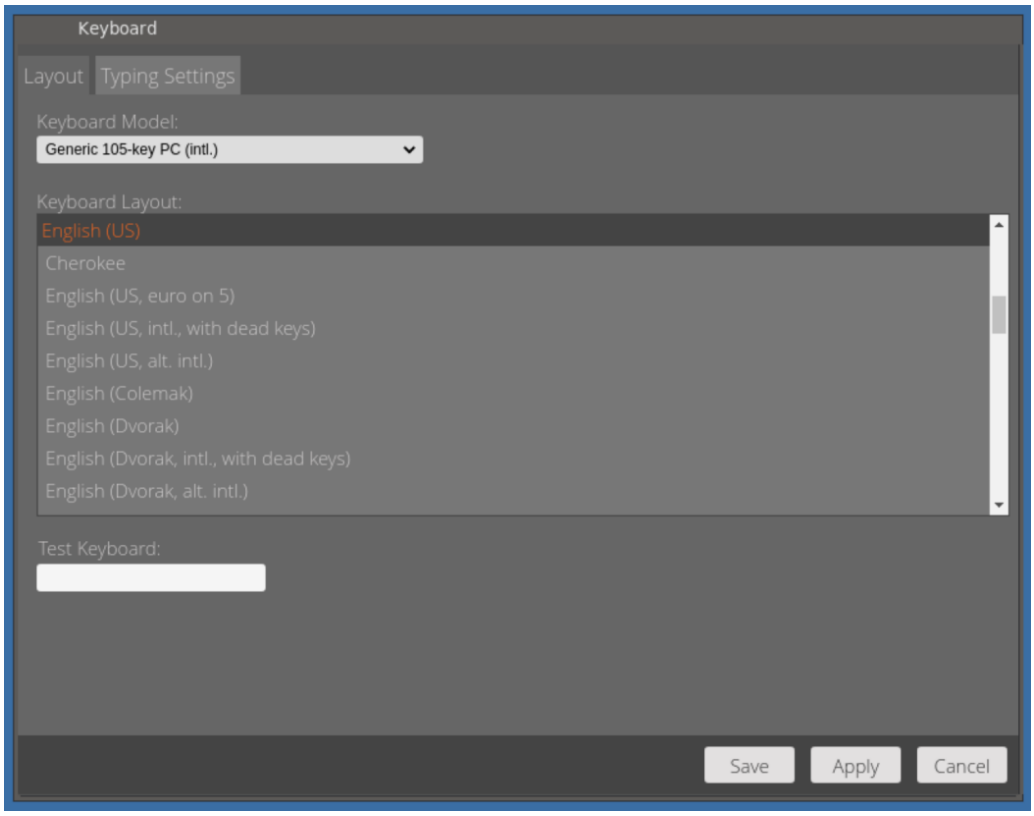
Please note: This should only be changed under advice from 10ZiG Support.

Keyboard



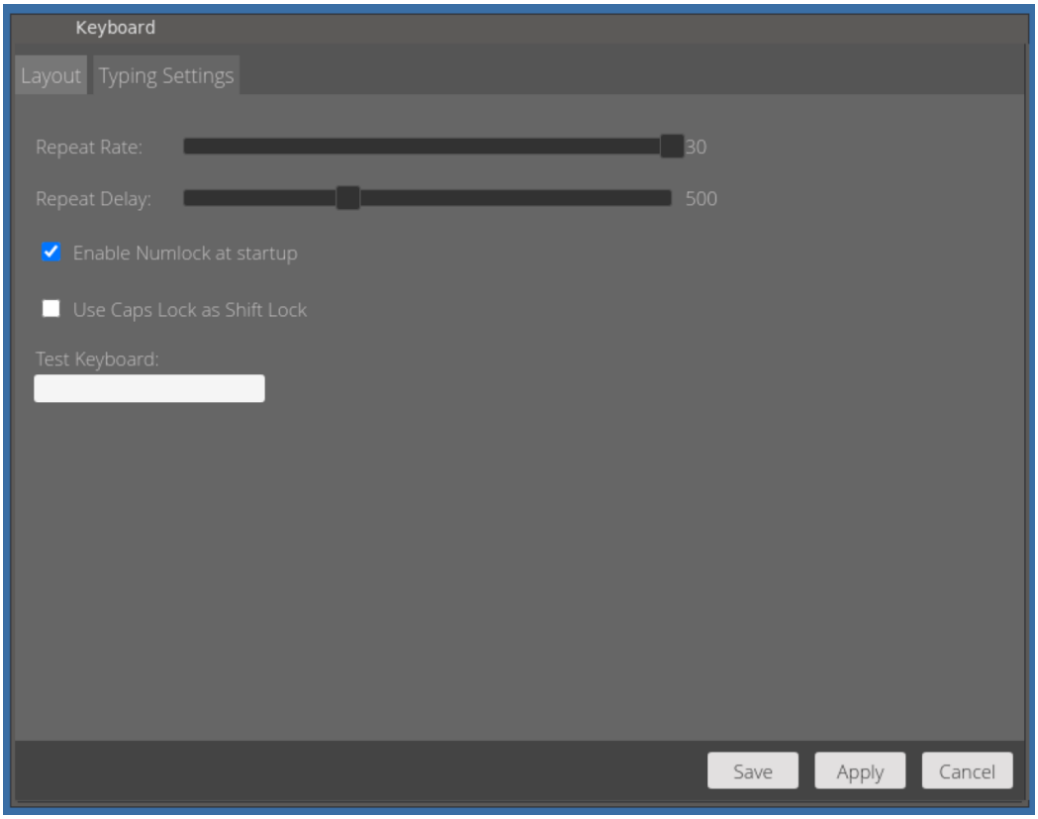
Opening the **Keyboard** window displays the **Layout Tab** which allows you to select the keyboard model and country layout, as well as test keystroke output in the **Test Keyboard:** dialog box.

Layout

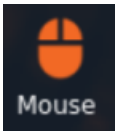


Keyboard – Typing Settings

You can also set the keyboard character “Repeat Rate” and “Repeat delay”, by moving the slider bars left and right. You also have the ability to “Enable Numlock at startup” and use the “Caps Lock as Shift Lock” by using the checkboxes, as shown below.

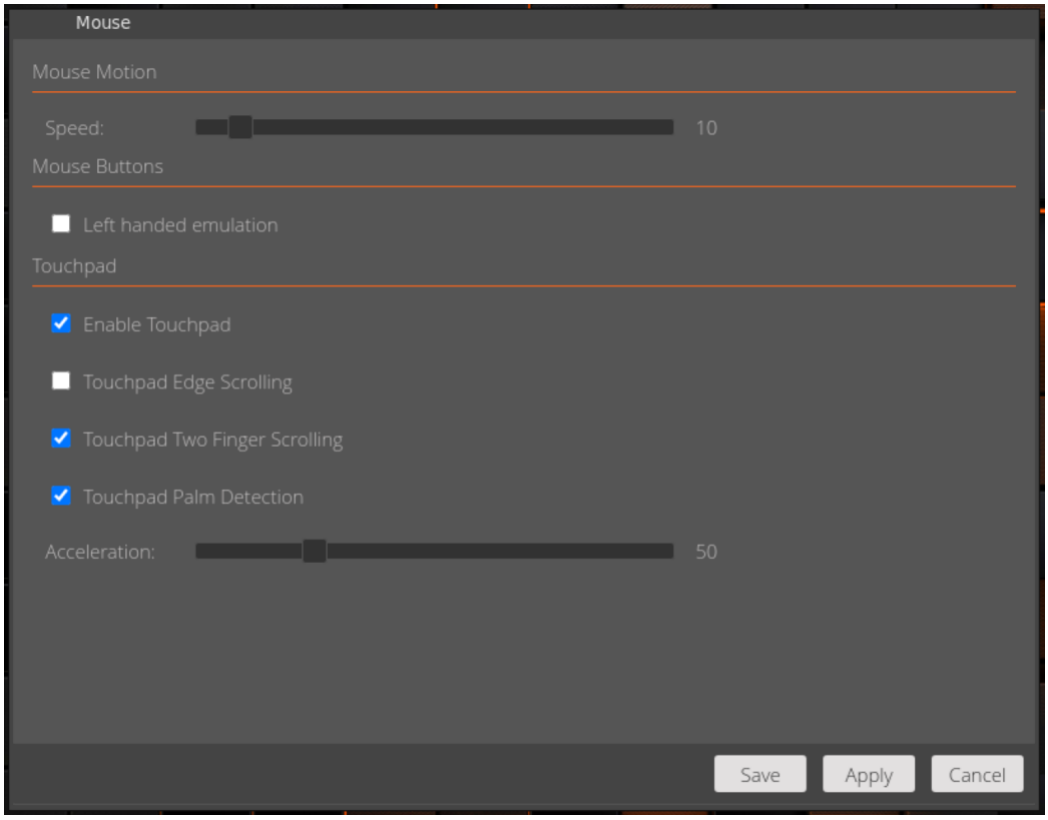


Mouse



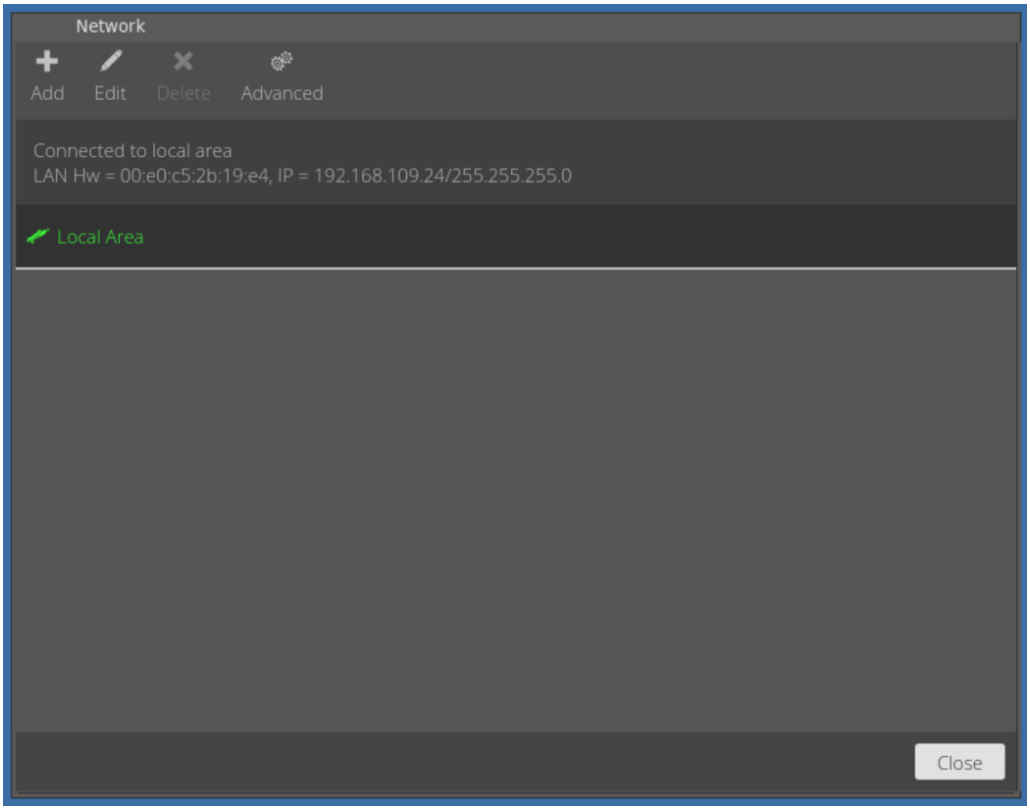
The Mouse window allows you to set the mouse speed, and acceleration settings. You may also configure the mouse buttons for 3 button emulation or for left-handed users.

If you have a touchpad connected to your Thin Client, then enabling this option will allow you to access its scrolling and detection options also.



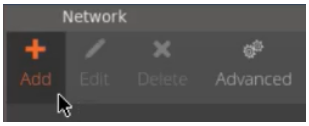
Network

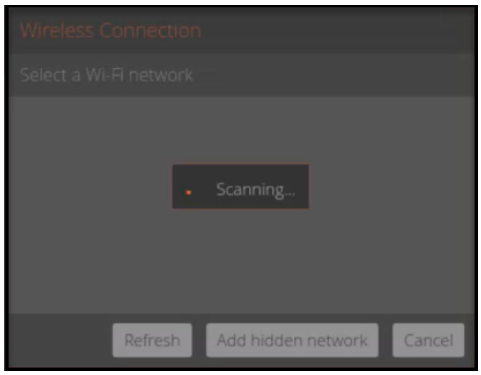
Here you will find options to configure your network settings. If only one type of connection is available, it will be automatically set to **Default**. Highlighted in green below.

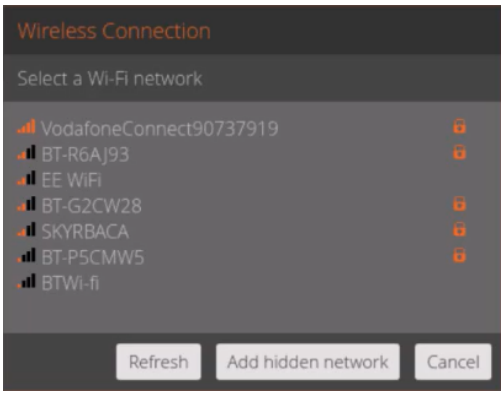


Wireless Network Connection (Additional Hardware Opt.)

Open the Network Configuration applet by clicking on the Network Icon, now click the “Add” button and the Wireless Connection properties will open, and you’ll see the “Scanning Wireless” message appear and then see a list of Broadcasted SSIDs in your environment, choose the wireless access point you would like to connect to and then click the “OK” button.

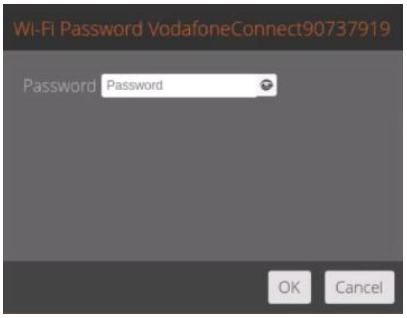




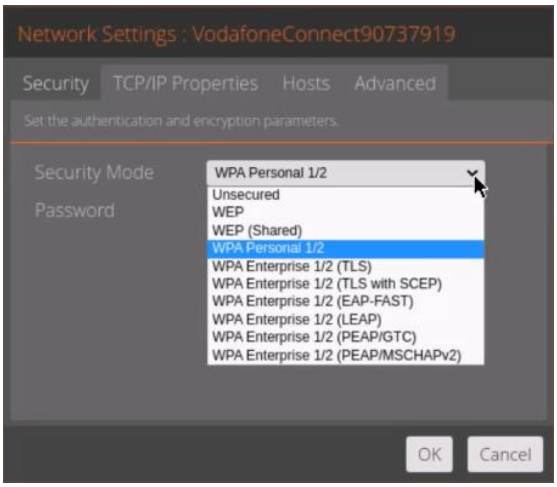


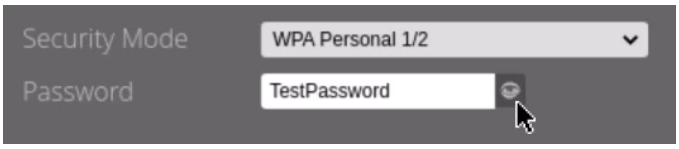
If you don’t see the SSID that matches your Wi-Fi network, just click the “Refresh” button and it should appear in the list. Check with you network administrator to make sure that it’s not hidden. If it is hidden, then just click the “Add hidden network” button and you’ll be able to add it in there. See below.

Once you’ve selected your network, then you’ll be prompted to type in your wireless network password as below.

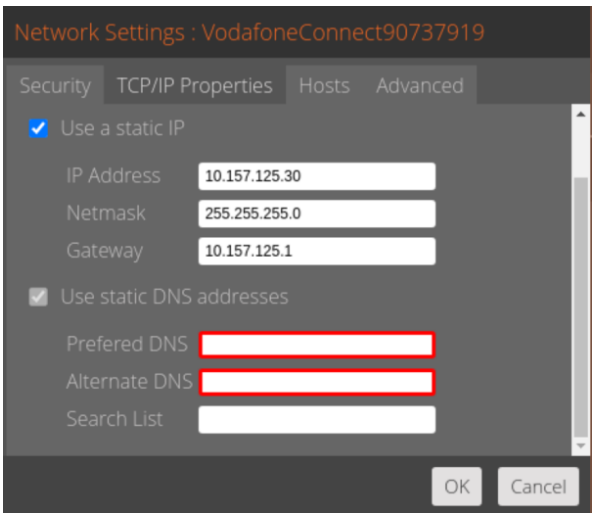


If you highlight your network adapter in the list and then click “Edit”, you’ll now see the network settings for your wireless device, and additional configuration tabs for it. Inside the security tab choose your “Security Mode” from the dropdown list and type in your passphrase (if applicable to your security mode choice). If you uncheck the box next to passphrase your passphrase will be shown in plain text.

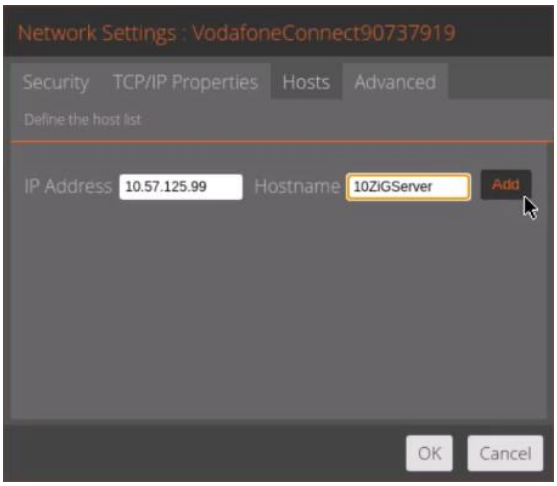


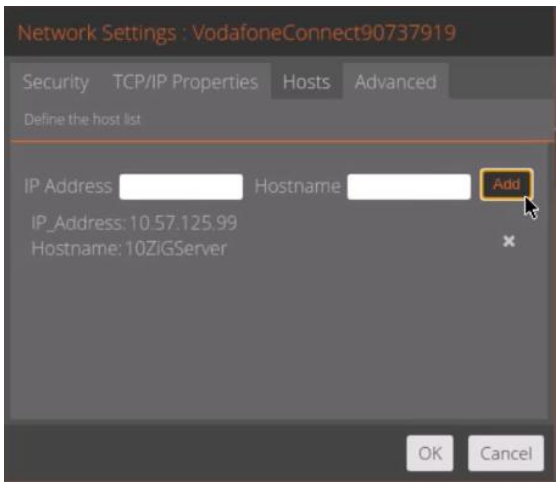


From the “TCP/IP Properties” tab, you can set a **static IP address** if used in your environment and also use specific **DNS server** addresses.



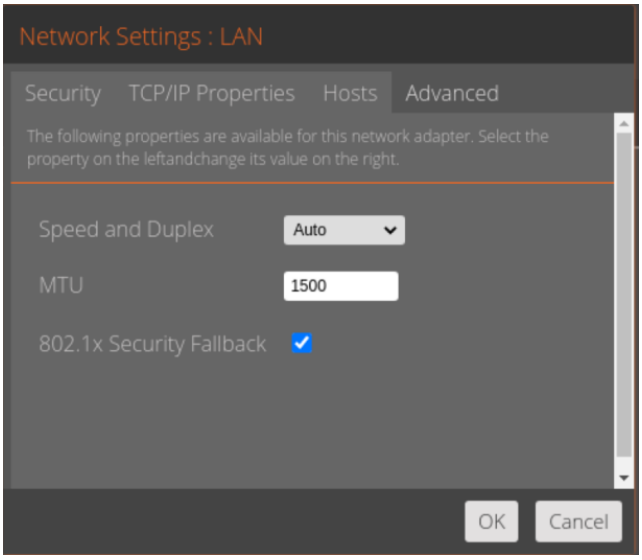
Using the “Hosts” tab you can define the host list for the wireless connection. Just click in the box below “Define the host list. Format : Ip_Address hostname” and start typing the IP address, followed by its hostname.





If you click on the “Advanced” tab, you’ll be able to set the “Speed and Duplex”, “MTU” and “802.1x Security Fallback” options for the adapter.

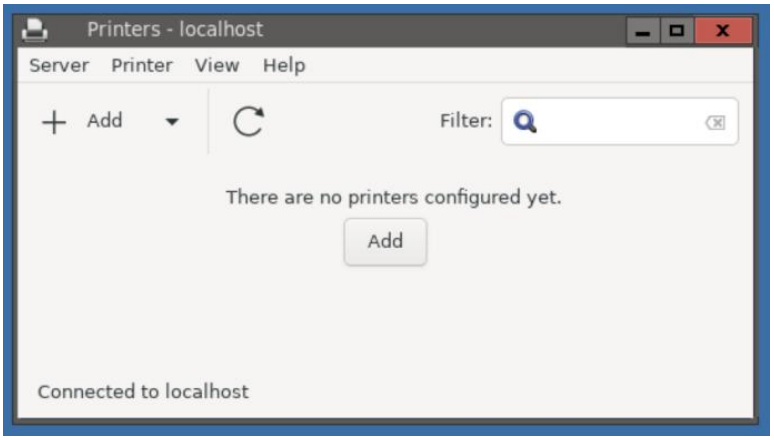
If you need any further information regarding setup of 802.1x and SCEP, 10ZiG have a document titled “SCEP setup v2”. Please contact your Technical Support team and they’ll be happy to provide you with a copy of the guide.



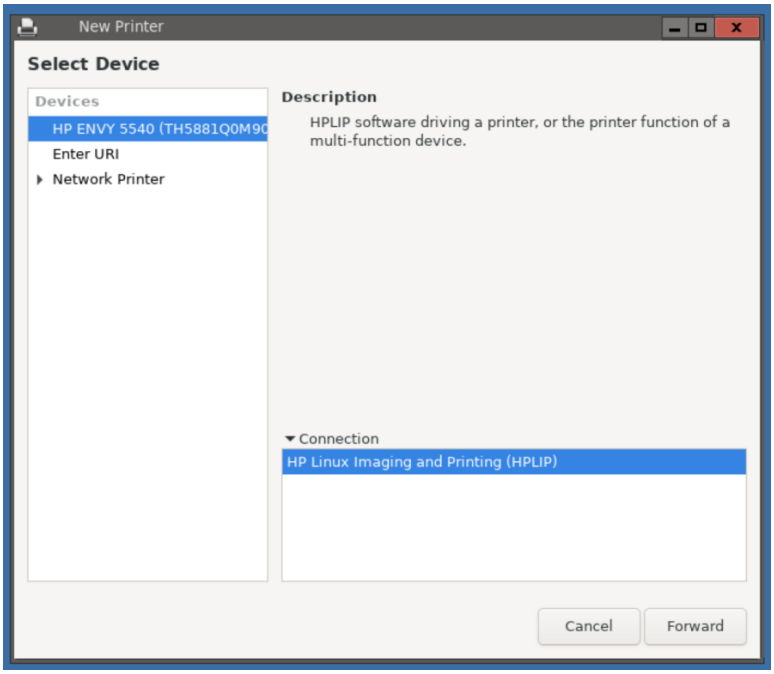
Printers

The Printers applet allows you to add a local or network printer and gives you the ability to fully configure it on your client endpoint.

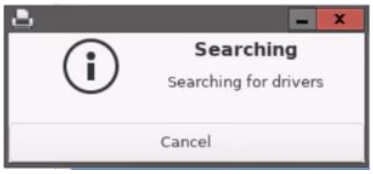
Configuring Local USB Printer



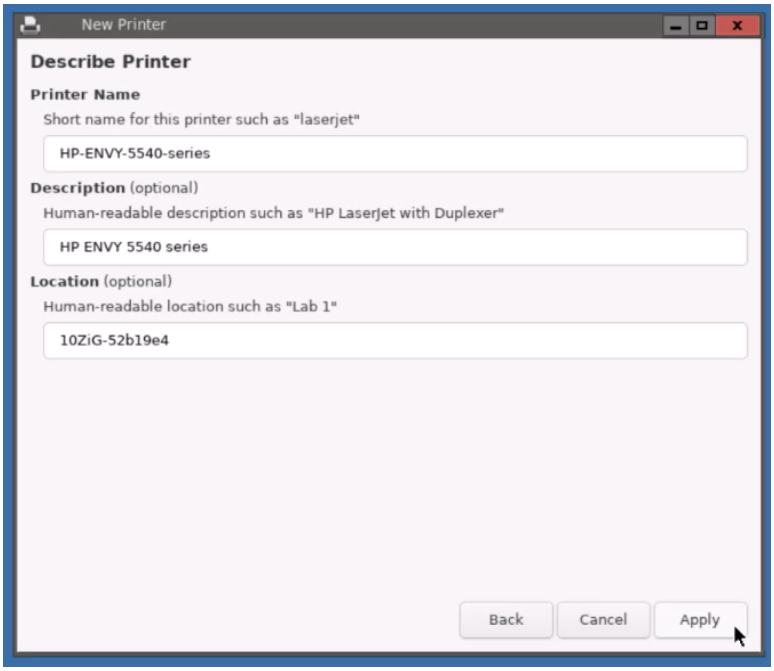
Clicking “Add” inside the applet, will allow you to discover any printers, locally or on your network.



Once you've found your printer, click "Forward" and its drivers will be searched for and then installed locally on your endpoint.



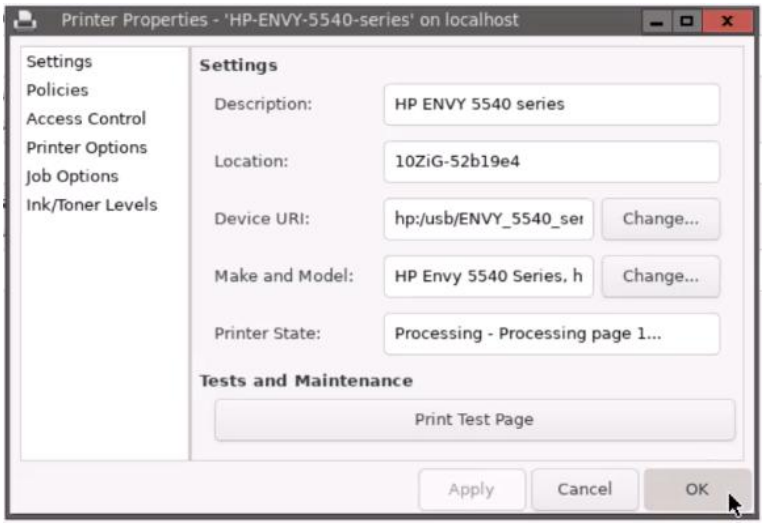
You then have options to describe the device in more detail to suit your requirements as below.



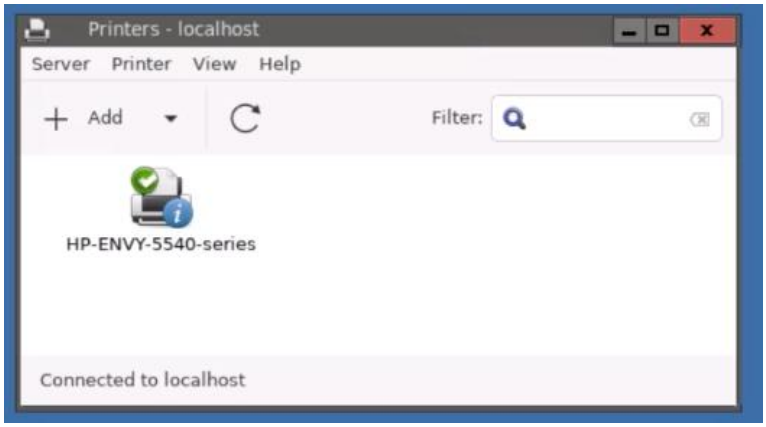
During the setup process, you have the option to "Print Test Page".

Once the printer is added, further options will become available for configuration such as :-

Settings
Policies
Access Control
Printer Options
Job Options
Ink/Toner Level information

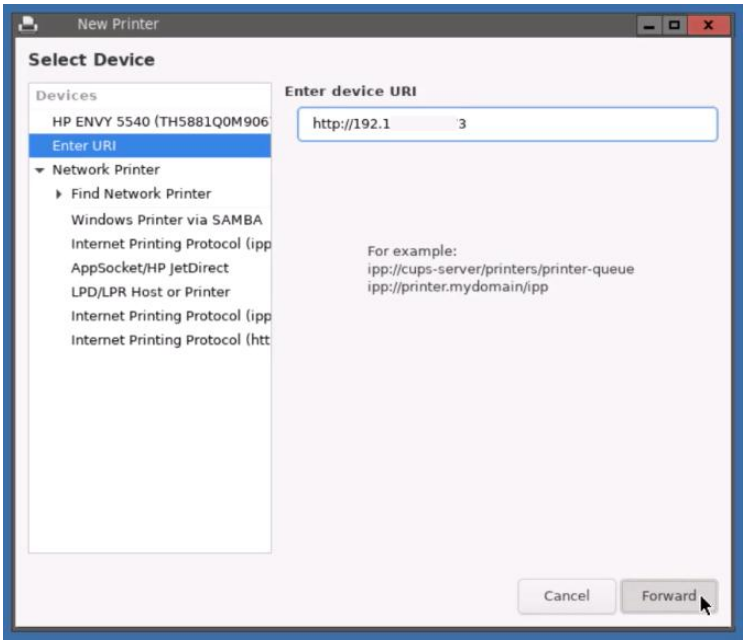


Once complete, your printer will show up in the list of configured devices on your physical client endpoint.

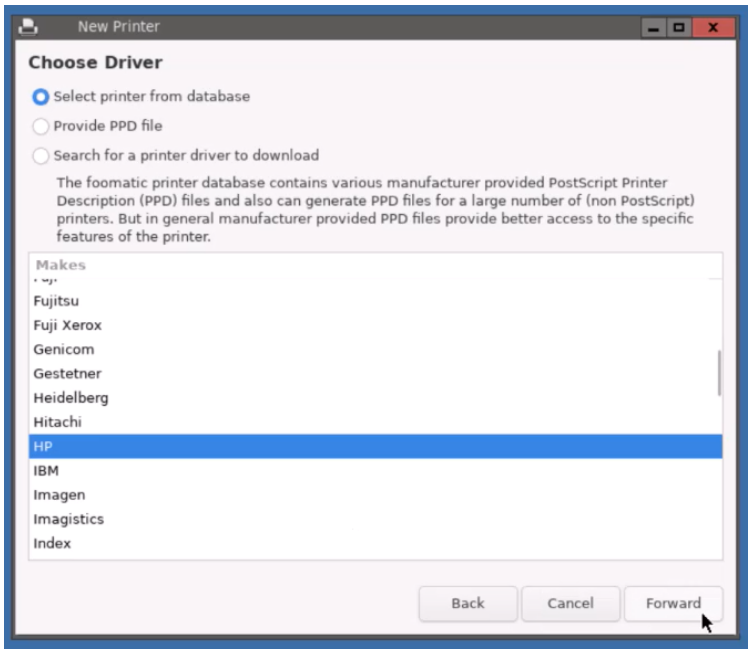


Configuring a Network Printer

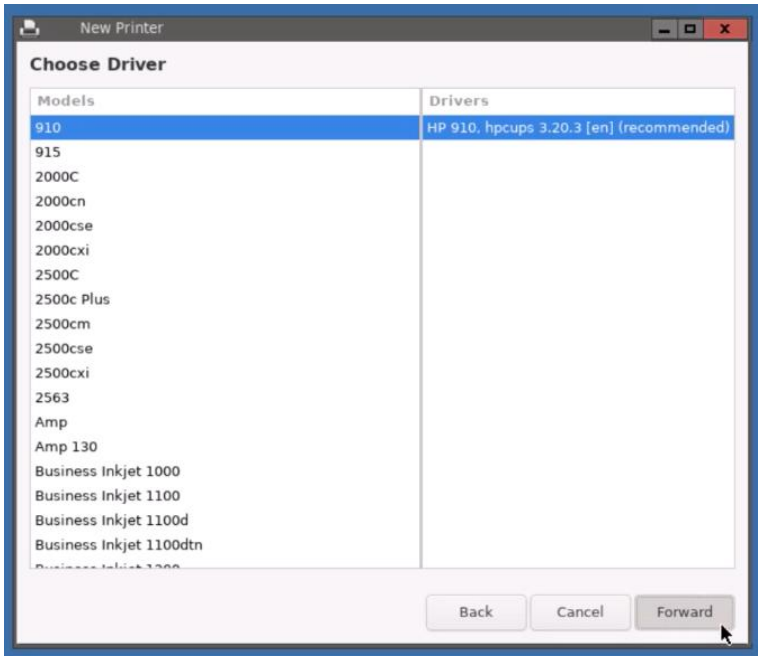
If adding a network printer, you can either select the connection type from the “Network” Printer dropdown list or just type in the device URI.



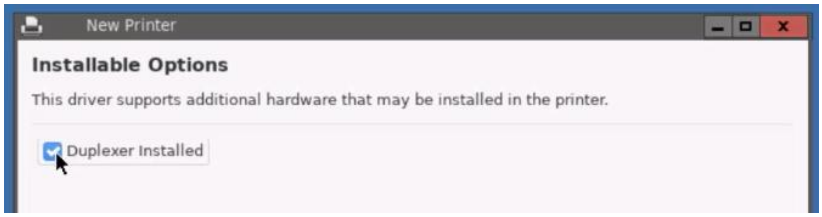
Choose the printer vendor from the list provided.



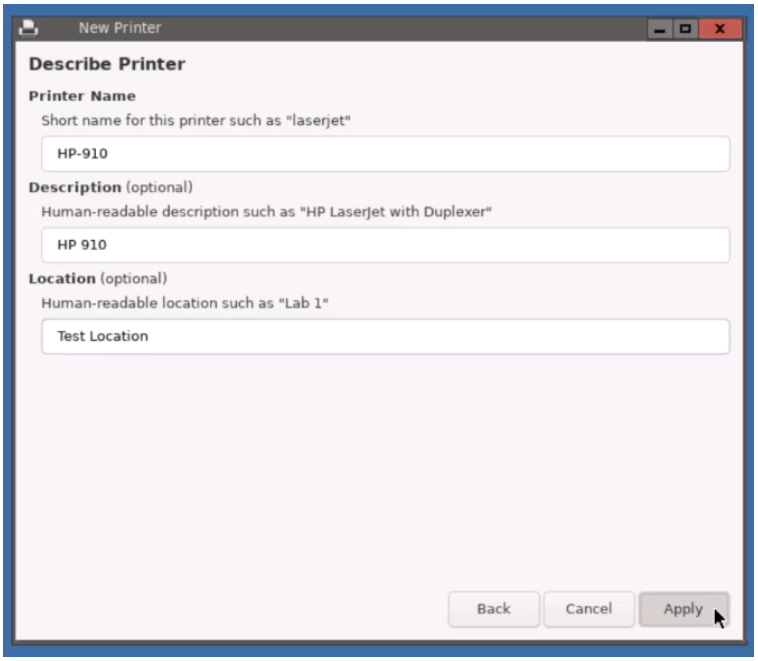
Choose the appropriate drivers.



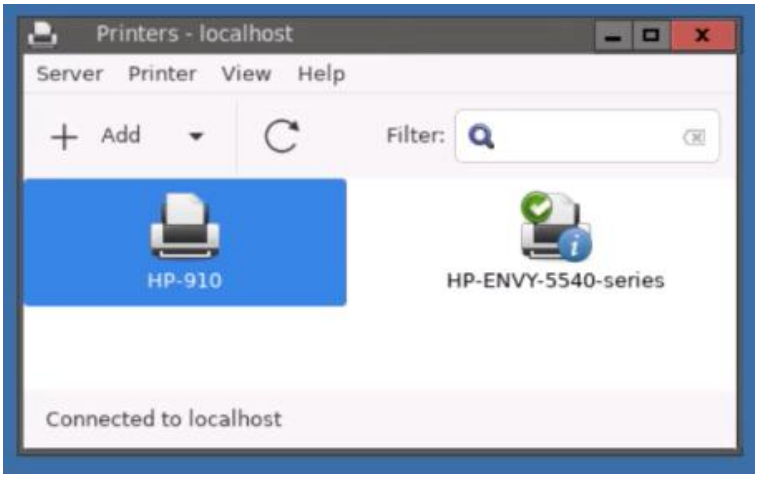
Select Installable Options.



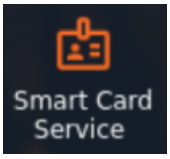
Describe the printer.



The network printer was added successfully.

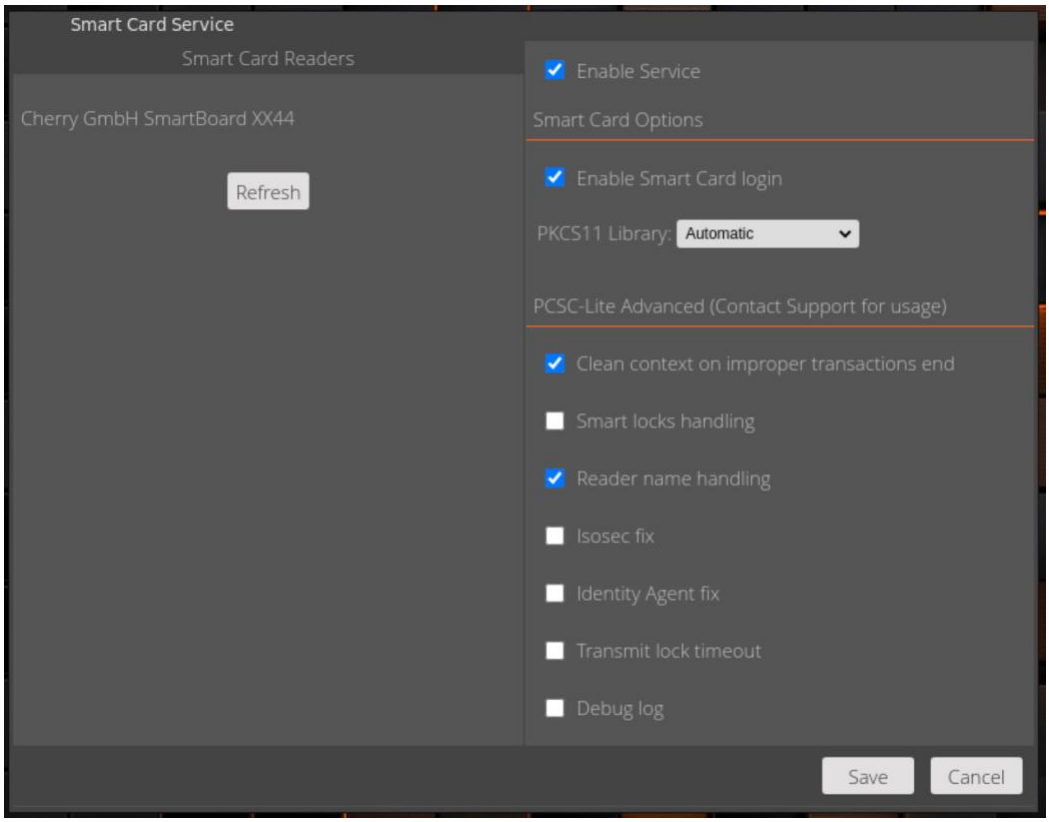


Smart Card Service



This service allows you to Enable or Disable your Smart Card Service and Reader Device.

Unless you require specific settings for your readers, these settings can be left as default. Contact 10ZiG Support for information on advanced setup of your reader.

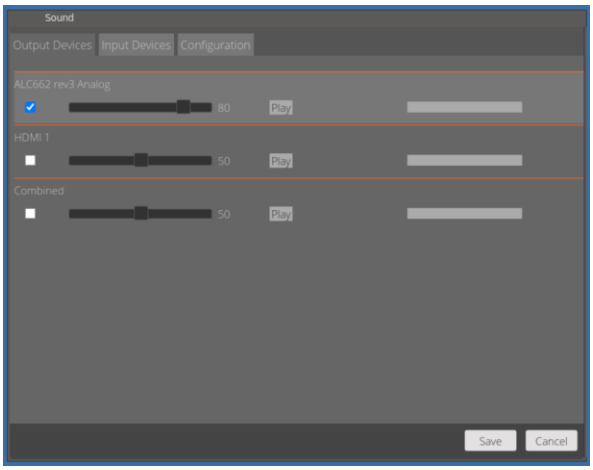


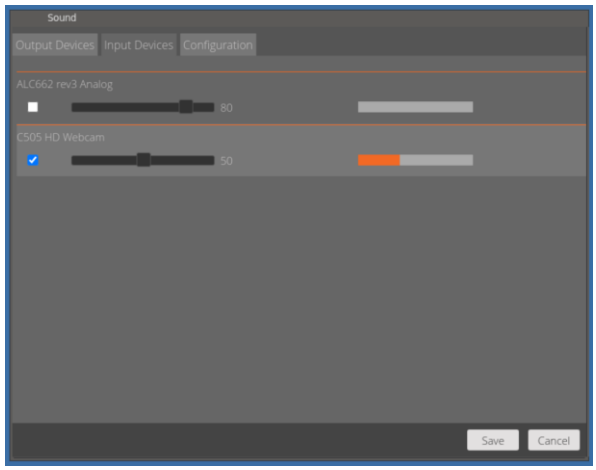
Sound

The Sound window allows you to control the speaker (Output:) and microphone (Input:) volumes and also lists the audio devices being used.

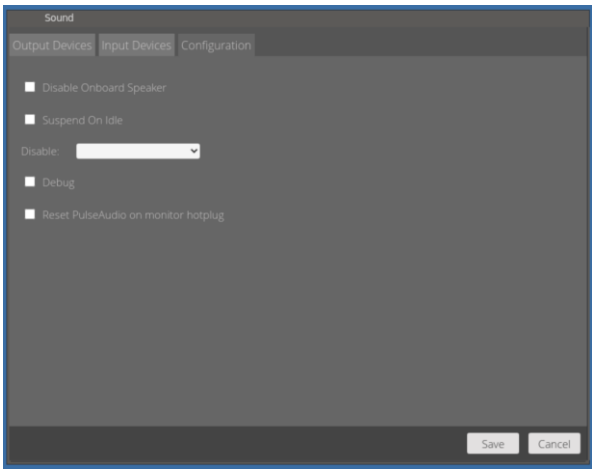
The output devices tab lists all connected output devices and gives you the ability to select your preferred device, set the volume and test its output by clicking the “Play” button.

The input devices tab lists all available input devices and lets you select your preferred device for input. This example below displays the integrated microphone of the C505 HD Webcam.

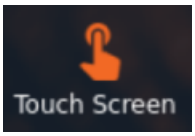




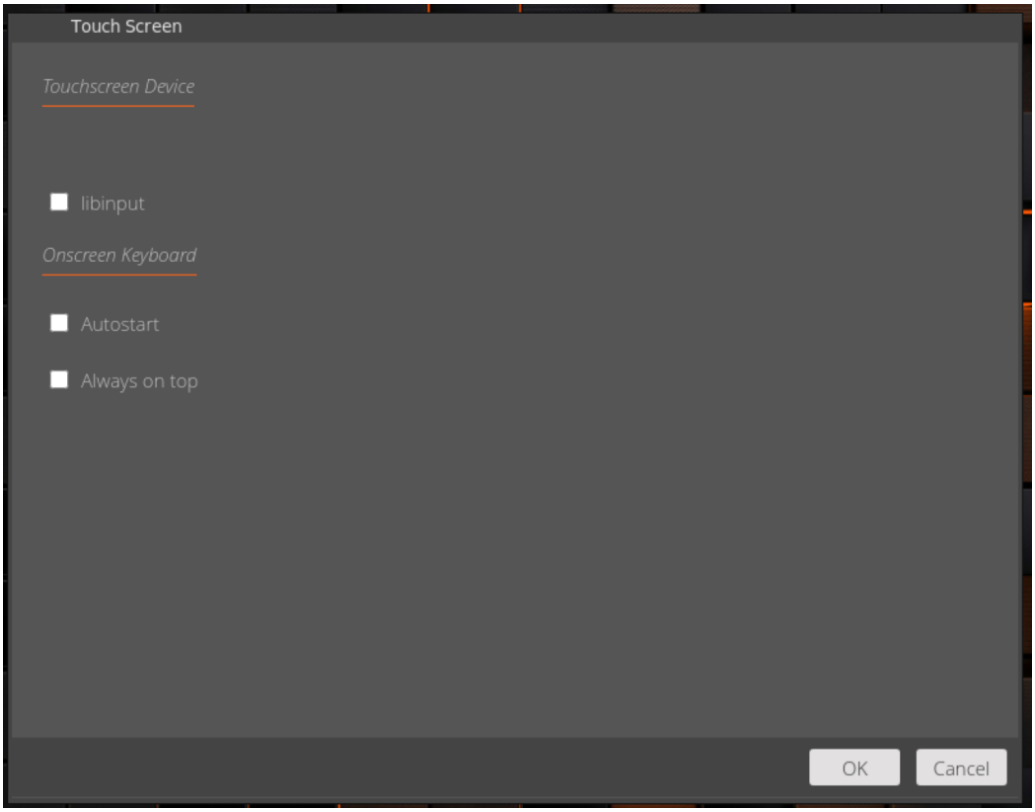
You also have the ability to configure options such as disabling the onboard speaker if you’re using external speakers and also suspend these devices to save power if the client device is idle.



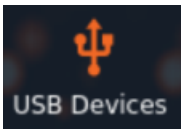
Touch Screen



If you have a touch screen attached to your Thin Client, then it will appear inside this dialog under the “Touchscreen Device” heading. You also have the option to autostart the onscreen keyboard and also set it to remain on top of other desktop items.



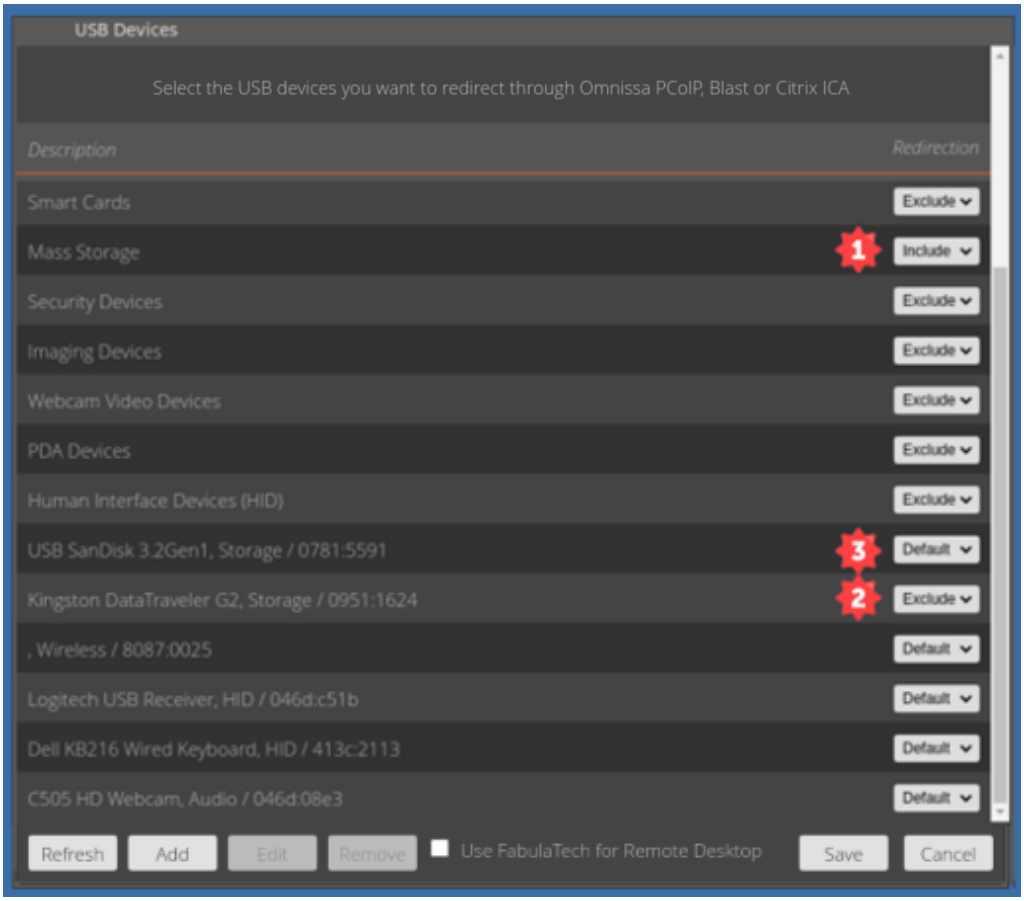
USB Devices



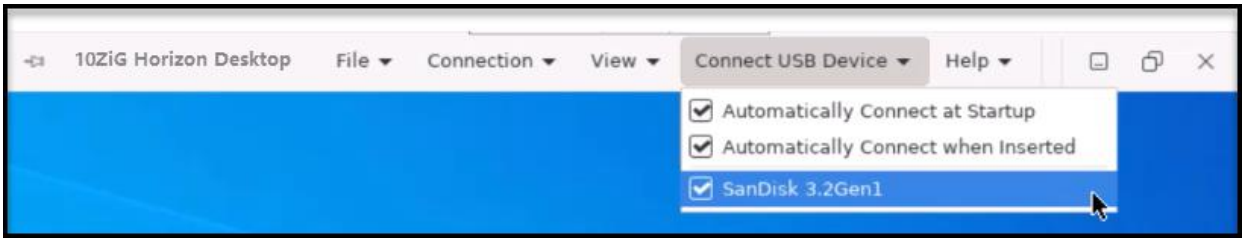
USB Devices for Omnissa and Citrix can be controlled here. Looking at the screenshot below, you can see a list of categorized device classes listed at the top of the grid and individually attached devices can be seen towards the bottom.

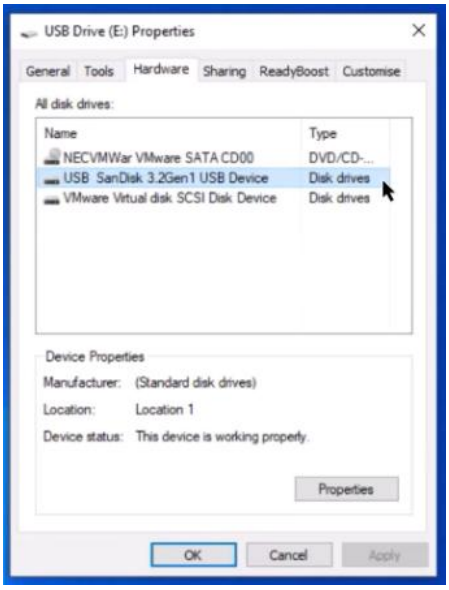
You can include or exclude whole groups of classed devices from being passed to the VDI and also include, exclude, or set individual devices to default. If you set the individual device to default, then it will inherit the state of its parent class above.

Using the example below, with 2 “Mass Storage” devices attached, we might want to include the whole of the “Mass Storage” device class to be passed to the VDI 1 but then set the “Kingston Technology DataTraveler” to be excluded 2 and leave the “SanDisk” device as default. 3

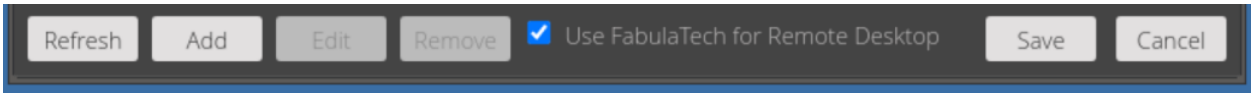


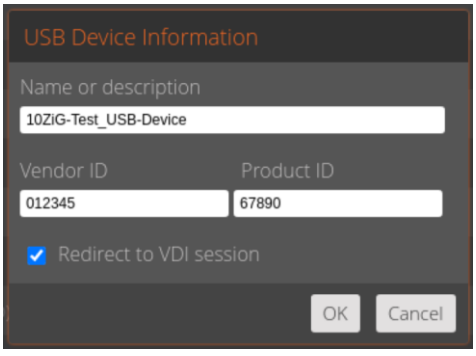
If we then launch an Omnissa Horizon session, we should see only the “SanDisk” inside the Horizon “toolbar” and inside Windows “File Explorer”, as it would have inherited the “include” status of its parent class “Mass Storage”. The “Kingston” device however is not available, as expected.





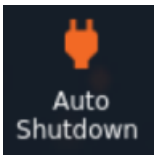
You also have the ability to manually add in any of your USB devices or take advantage of FabulaTech USB device redirection if you have the server component installed on your Remote Desktops.



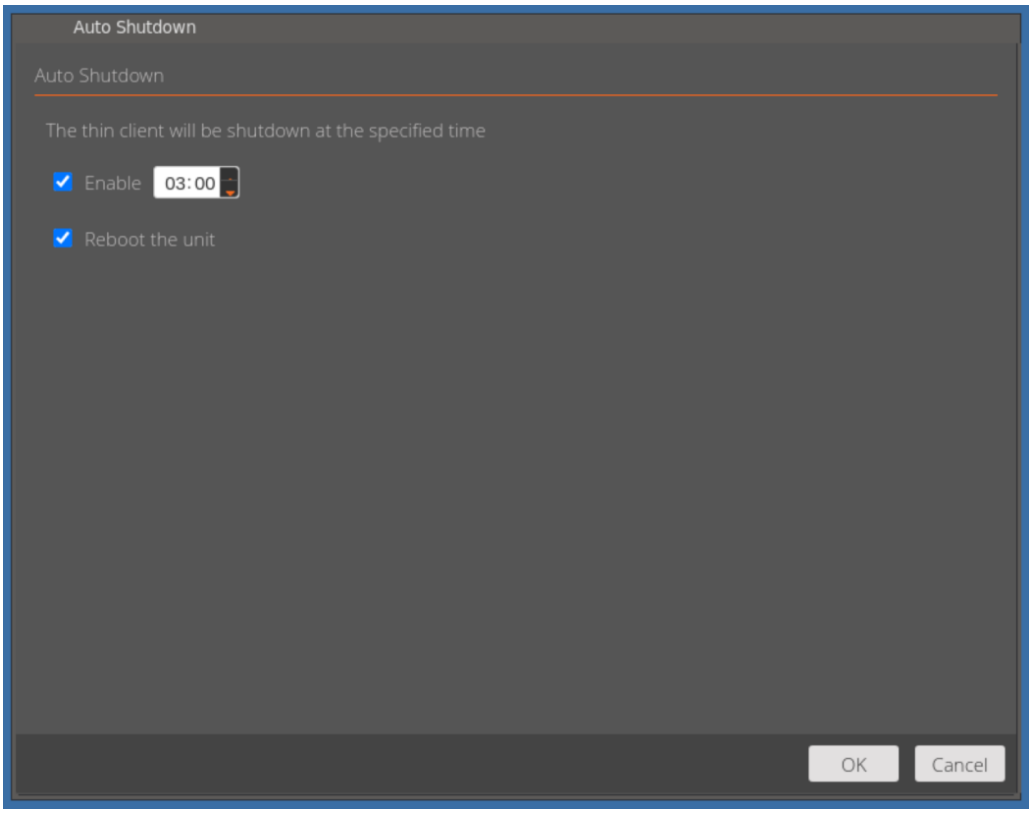


System

Auto Shutdown



Auto Shutdown allows you to set a local time to automatically shut down the client. Tick the “Enable” box and then select a time to shut down with the scroll arrows. To reboot instead of shutting down and powering off, just tick “Reboot the unit”. The example below, reboots the device each day at 03:00 hours(3am).



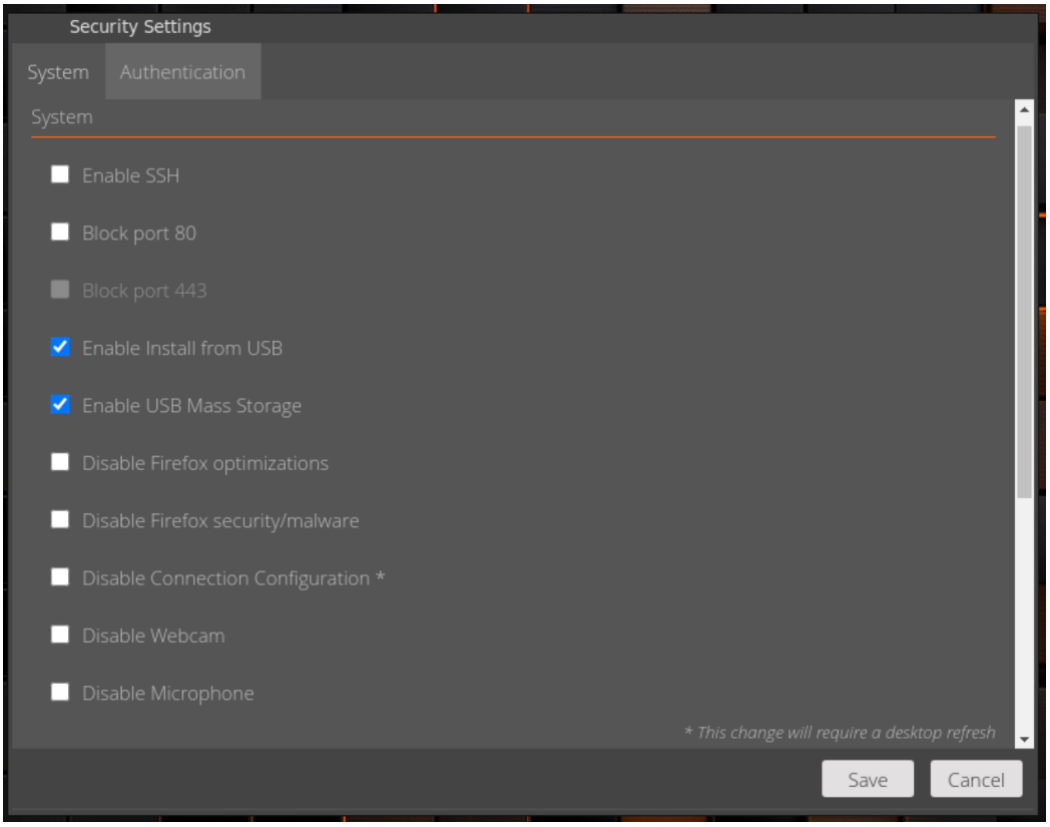
Certificates

The Certificates applet opens the Certificate Manager and allows administrators to delete or show the certificates that are currently installed on your NOS Unit.

Importing Certificates

You can import Certificates to your units two ways, via USB or the 10ZiG Manager.

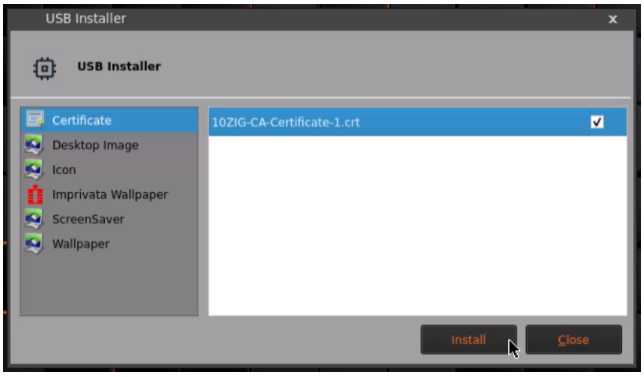
In Security Settings click “Enable Install from USB” and click “SAVE” if you intend to import certificates locally from USB storage.



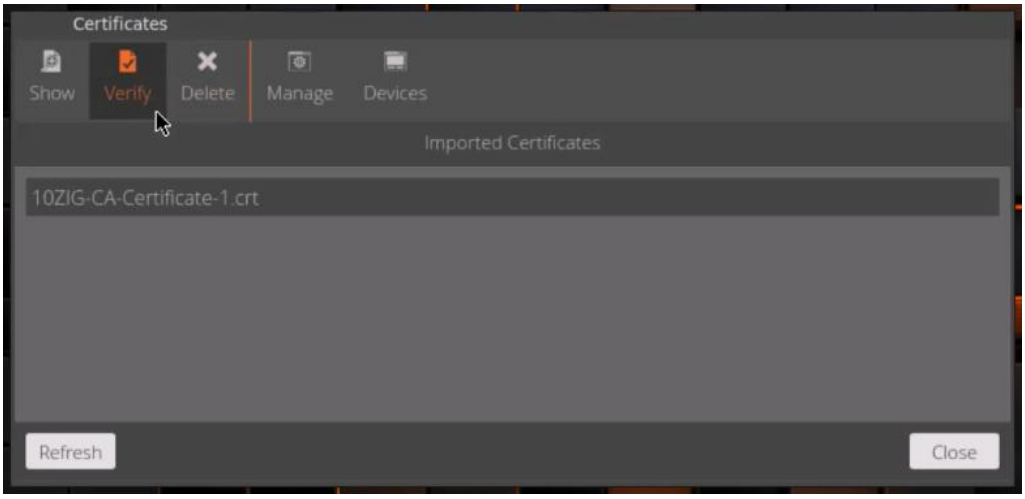
Importing a Certificate from a USB storage device

To import a certificate, insert a USB drive (Formatted to FAT32) into the unit that contains the certificate file.

You will see the list of certificates displayed on screen, simply click any that you wish to import and then click “Install”, as below. You should see the “Installing certificates” dialog box and then you’ll be returned to the “USB Installer” dialog box.



Once the certificates have been installed successfully, close the “USB Installer” dialog box, go into the “Control Panel” and click on the “Certificates” icon under the “System” heading and you’ll see the newly imported certificate inside there.

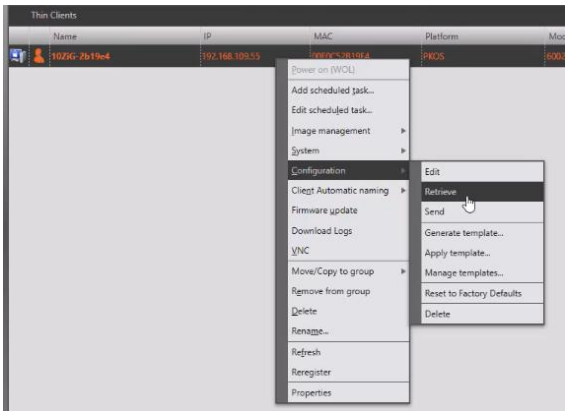


If you highlight the certificate and then click “Verify”, the certificate will be checked for its validity and a dialog box will be displayed to indicate this.

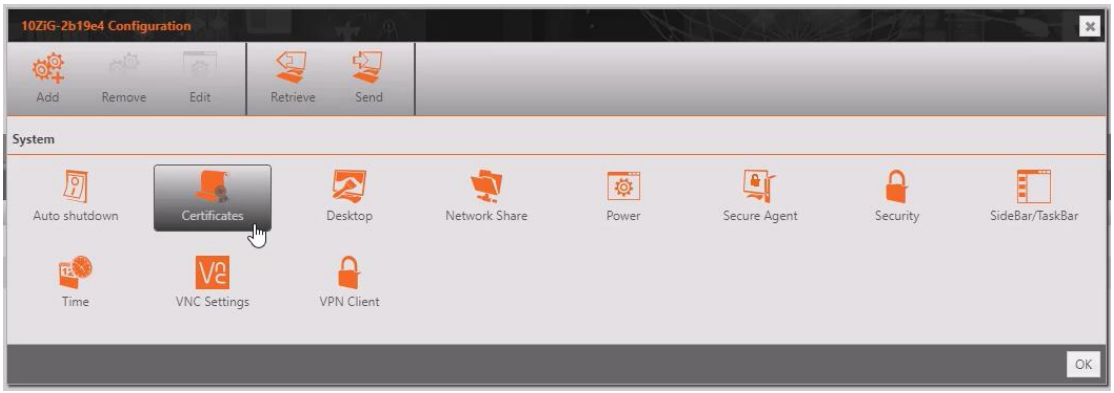
Importing a Certificate from the 10ZiG Manager Web Console

Just as you can import certificates locally on the 10ZiG NOS Thin Client, you can also import them remotely, by using the “10ZiG Manager Web Console”.

Open the “10ZiG Manager Web Console”, highlight the Thin client that you wish to update certificates for, right click and select “Configuration” and “Retrieve”.

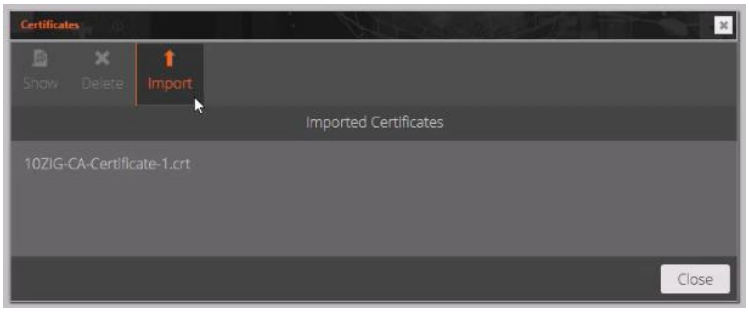


Once retrieved, go in the “Configuration” menu again and select “Edit” this time. Once displayed, double-click the “Certificates” icon under the “System” heading as shown below.

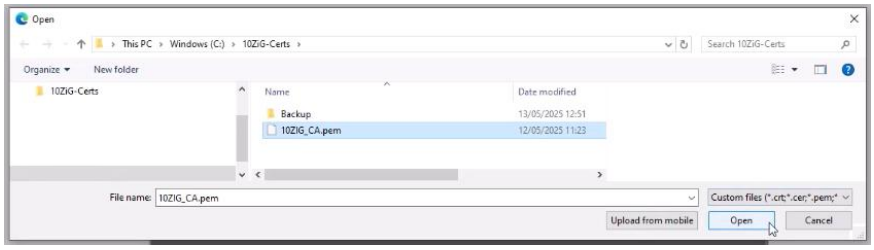


Once the “Certificates” dialog box opens, notice the already installed certificate that we imported locally on the 10ZiG Thin Client earlier.

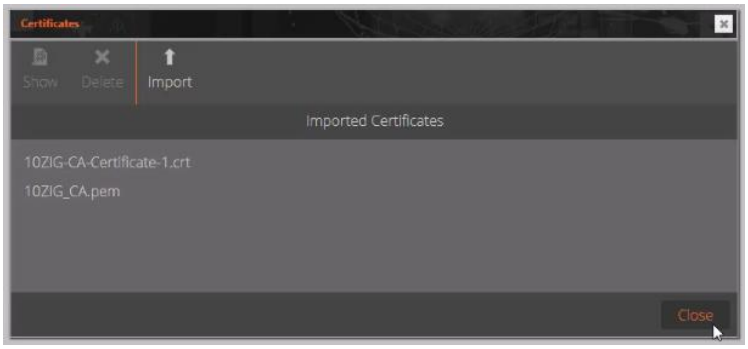
Click “Import” to locate a new certificate that will be saved on the “10ZiG Manager Server” and sent with the next configuration download to the client.



When the “Import Certificate” dialog box appears, just click the “Select Certificate File” button, navigate to the certificate file you wish to import and then click “Open”.

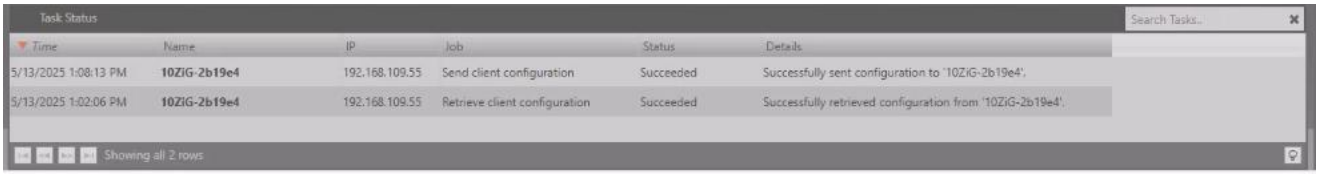


Once the “Import Certificate” dialog show the correct certificate name, just click “Import” and you’ll see the newly imported certificate displayed alongside the original one added locally via USB earlier.

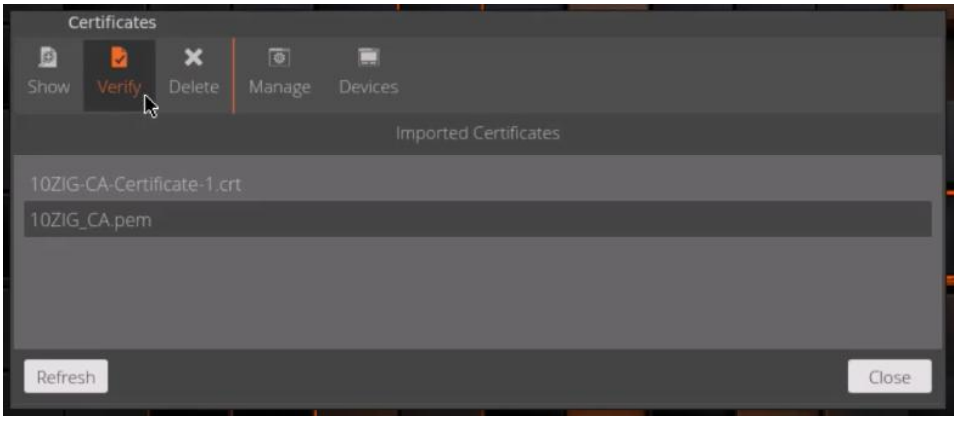


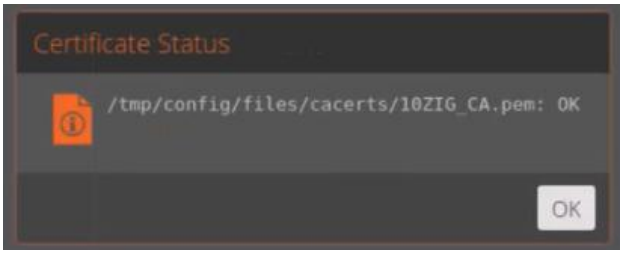
Now that we’ve added a new certificate to the configuration, we need to send it back down to the 10ZiG Thin Client and then check that it got there successfully.

Whilst still inside the configuration screen for this client, click the “Send” button in the top right of the dialog box and wait for the successful “Send client configuration” message to appear in the “Task Status” window of the Web Console.

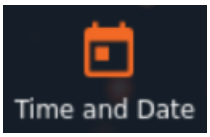


On the 10ZiG Thin Client again, if we open “Certificates” inside the “Control Panel”, we can see that our recently transmitted configuration successfully imported the certificate named “10ZiG_CA.pem” and if we highlight it and click “Verify”, it checks out successfully as expected.

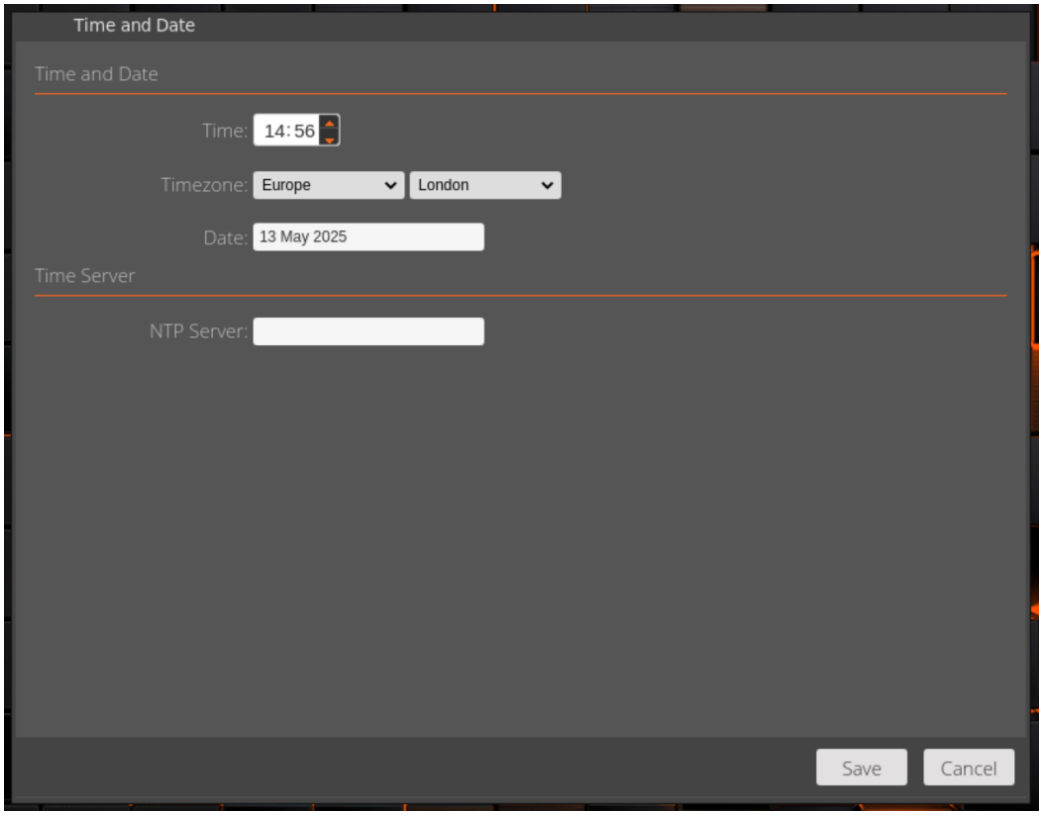




Time & Date



The Time and Date applet allows administrators to set the current time and date, time zone and if an NTP time server will be used.



The time server field allows you to sync your unit with an NTP server either internal or external. (Note: you must have internet access to use an external time server).

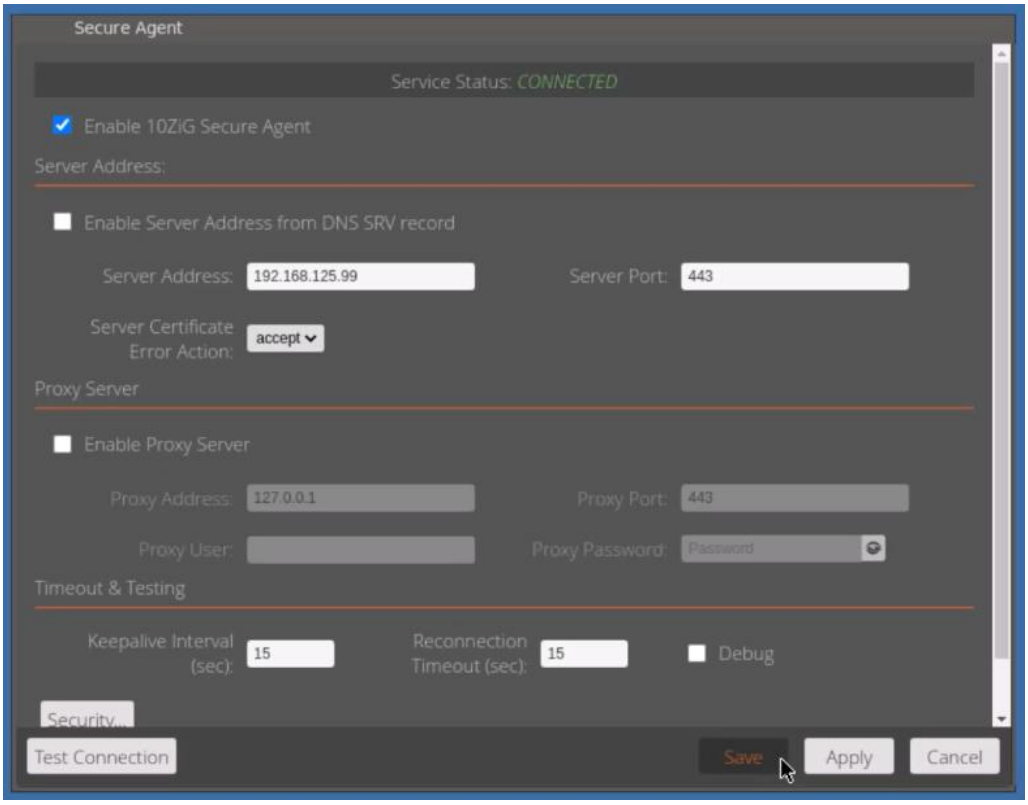
You can also get access to the “Time and Date” settings via the NOS-O, NOS-C and NOS-M “Authentication” login boxes, by clicking the white “Calendar” icon as shown below indicated by the “red arrow”.

Secure Agent

10ZiG Secure Agent allows you to use our Secure Connector technology to manage your devices. By default, the 10ZiG Secure Agent is enabled, but does not contain any address or port information.

If you have a DNS SRV record configured to point to your 10ZiG Manager Server, then this will connect automatically to it.

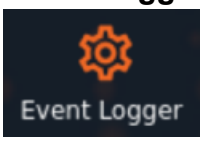
Alternatively, simply fill in the server and port information and click the “SAVE” button, and the Secure Agent will check in with the 10ZiG Manager.



Desktop

The Desktop applet was mentioned at the beginning of this guide in the section called “The Flexible PeakOS Desktop“, as it is fundamental to the initial setup of your Thin Client. Click this link to jump back to that section.

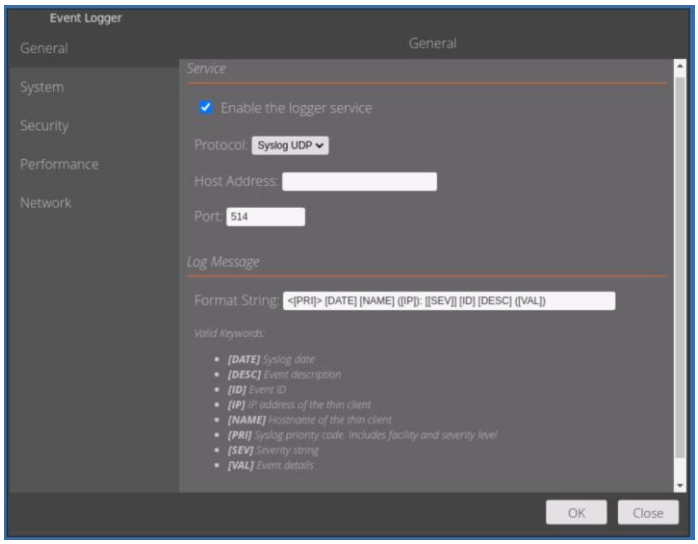
Event Logger



The event logger allows an administrator to track security and device management related events happening on a 10ZiG client. These events are sent to a remote log server. Syslog over UDP/TCP is the only protocol currently supported.

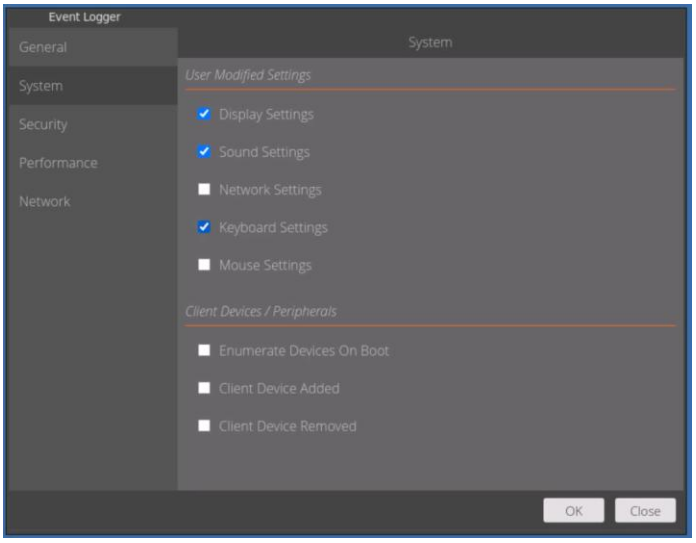
You can create your own syslog strings to pass back to your Syslog server, as shown in the "Format String" under the "Log Message" heading below.

General

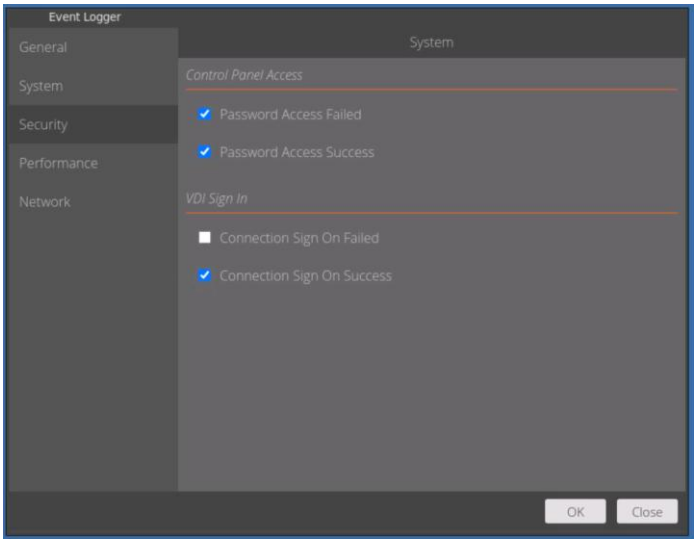


To select the types of event data that get written to the logs, simply click on any of the 4 Event Category tabs ("System", "Security", "Performance" and "Network"), and then select any or all of those types of Event name/ID record to be included in your syslog transfers. See below.

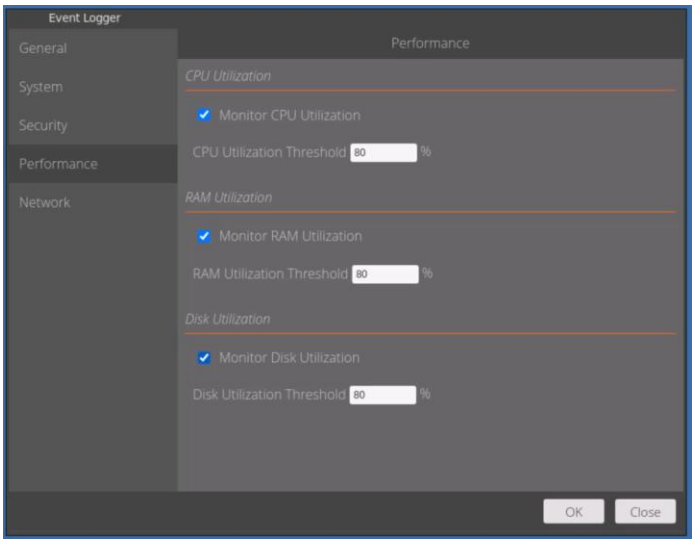
System Events



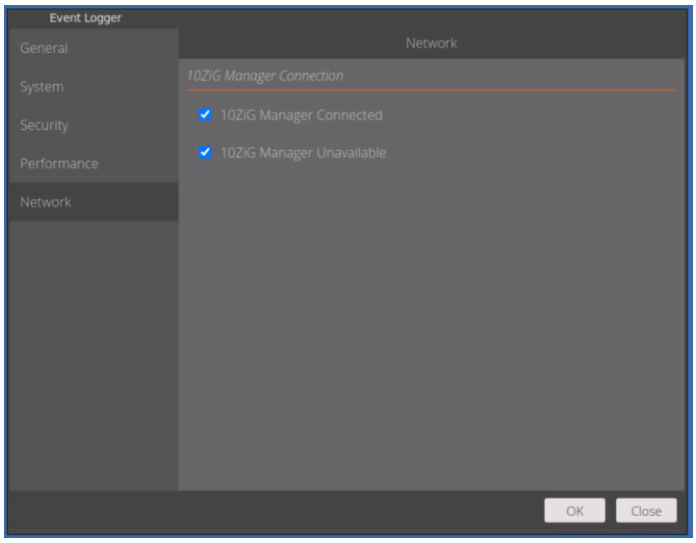
Security Events



Performance Events



Network Events



Valid Keywords for the Format String.

Below, are the possible keyword values for the “Format String”

- **[PRI]** - Syslog priority code. Includes facility and severity level
- **[DATE]** - Syslog date
- **[NAME]** - Hostname of the thin client
- **[IP]** - IP address of the thin client
- **[ID]** - Event ID
- **[DESC]** - Event description
- **[VAL]** - Event details
- **[SEV]** - Severity string

Examples of Security Events being triggered

This example below shows the events that are triggered if a password is enabled on the “Control Panel” and a user login to the “Control Panel” either succeeds or fails.

Succeeded Login Results

May 16 12:15:03 10ZiG01 (172.16.8.90): [info] sec02 Control Panel Password Access: Success (localuser)

Failed Login Results

May 16 12:14:52 10ZiG01 (172.16.8.90): [err] sec01 Control Panel Password Access: Failed (localuser)

On the following page, there is a complete list of all possible triggered events, along with their respective IDs, Categories, Descriptions and Severity indicators.

Complete list of Event IDs

ID	Category	Description	Severity
sys01	system	Client Powered On	info
sys02	system	Client Rebooted	info
sys03	system	Client Shutdown	info
sys04	system	Client Powered Off	info
sys05	system	Client Connected Devices	info
sys06	system	Client Device Added	notice
sys07	system	Client Device Removed	notice
sys08	system	User Modified Setting: Display	notice
sys09	system	User Modified Setting: Sound	notice
sys10	system	User Modified Setting: Network	notice
sys11	system	User Modified Setting: Keyboard	notice
sys12	system	User Modified Setting: Mouse	notice
sec01	security	Control Panel Password Access: Failed	err
sec02	security	Control Panel Password Access: Success	info
sec03	security	Connection Sign On: Success	info
sec04	security	Connection Sign On: Failed	err
perf01	performance	CPU Utilization	warn
perf02	performance	RAM Utilization	warn
perf03	performance	DISK Utilization	warn
net01	network	N/A	
net02	network	10ZiG Manager Connected	info
net03	network	10ZiG Manager Unavailable	err
net04	network	Network Connected	info

System Logs

Selecting a log file from the left hand menu will enable you to view it in the right window.

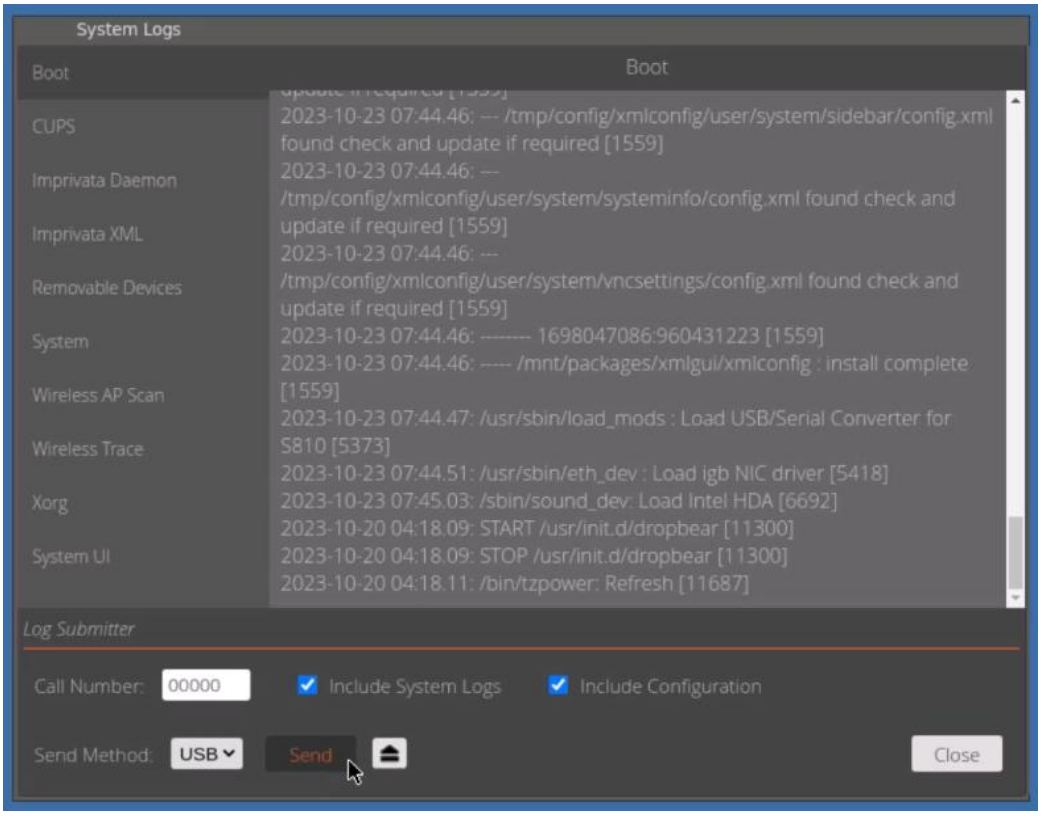
If you wish to send your collated logs to a 10ZiG support technician, you have two ways of doing this, you can either write them to an attached USB device for use later or retrieve them using the “10ZiG Manager Web Console”.

If you have already logged a call with technical support and have a call reference, then you can enter that in the “Call Number” field in the bottom left of the screen.

Collecting Logs via a USB storage device

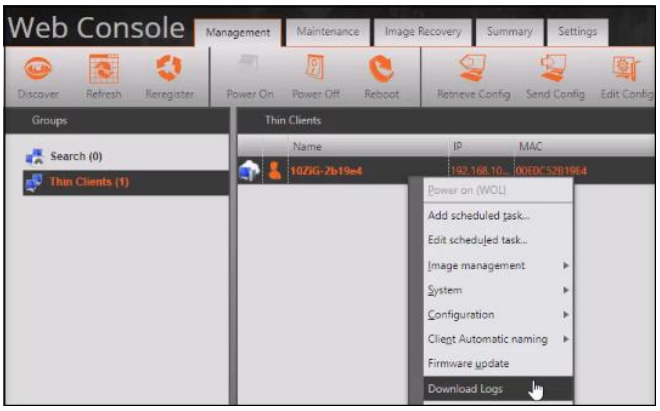
Once you are viewing the log you would like to send, select, tick either of the “System” or “Configuration” log options and click the “Send” button and it will be saved to your USB storage.

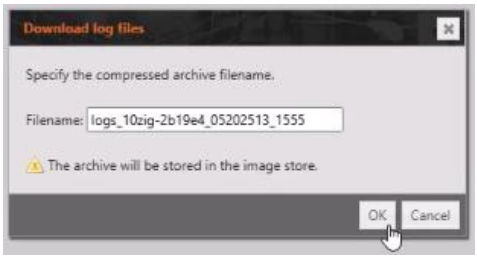
Remember, if you “Send” to USB, always click the “Eject USB” button, to make sure your logs are saved securely.

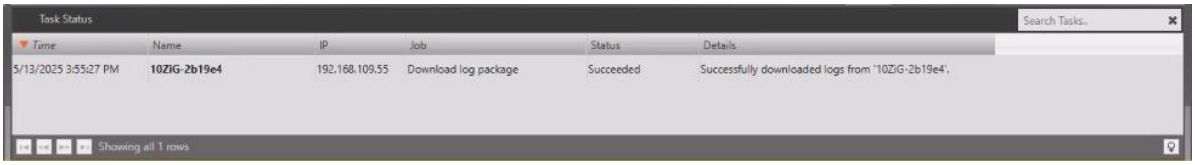


Collecting Logs via the 10ZiG Manager Web Console

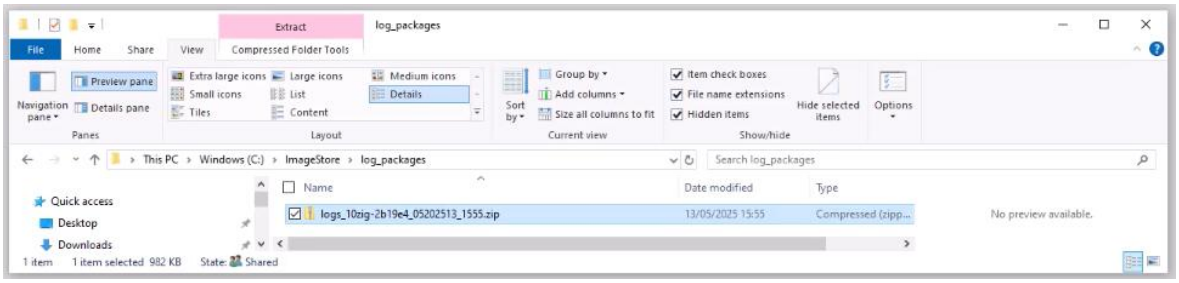
Inside the Web Console, right click on your Thin Client and click “Download Logs” from the drop-down menu. When the dialog box appears, a default log filename is already completed on the form, but if you prefer, just type in your own filename, and click “OK”. Notice that the dialog states that the archive will be stored in the “Image Store” on your 10ZiG Manager Server.



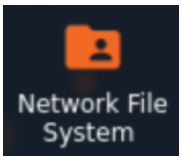




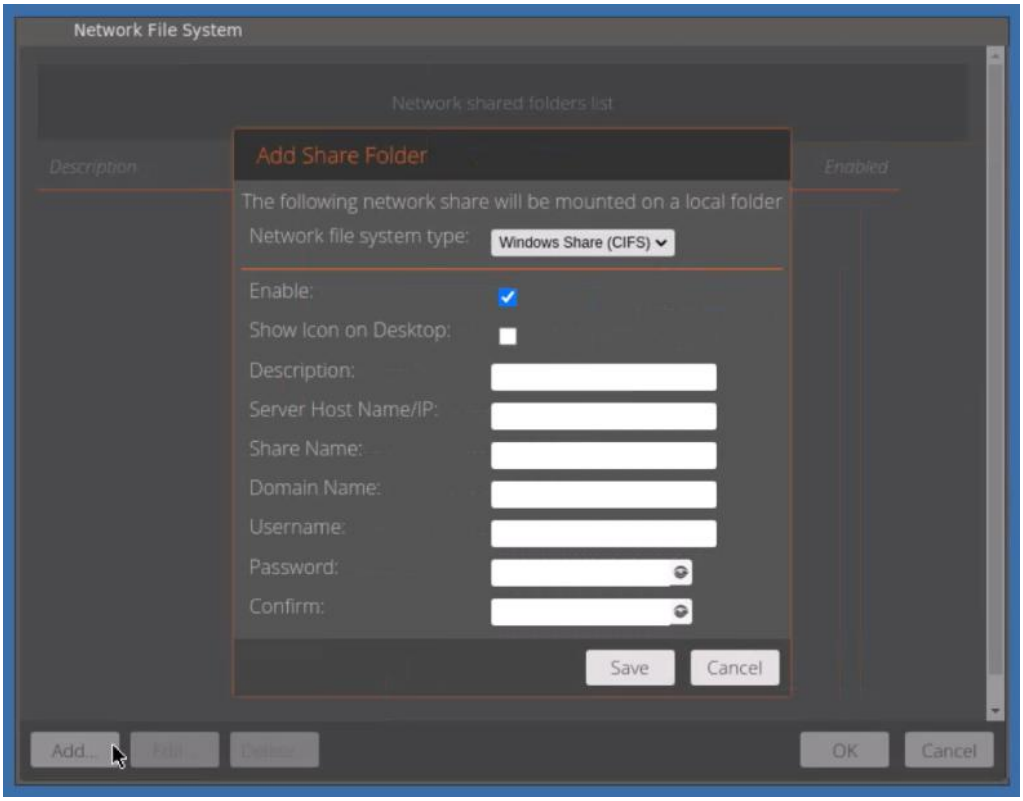
Once the logs have been uploaded, if you navigate to the “Image Store”, you’ll see the recently created log file inside a sub-folder called “log_packages”, matching the filename above.



Network File System



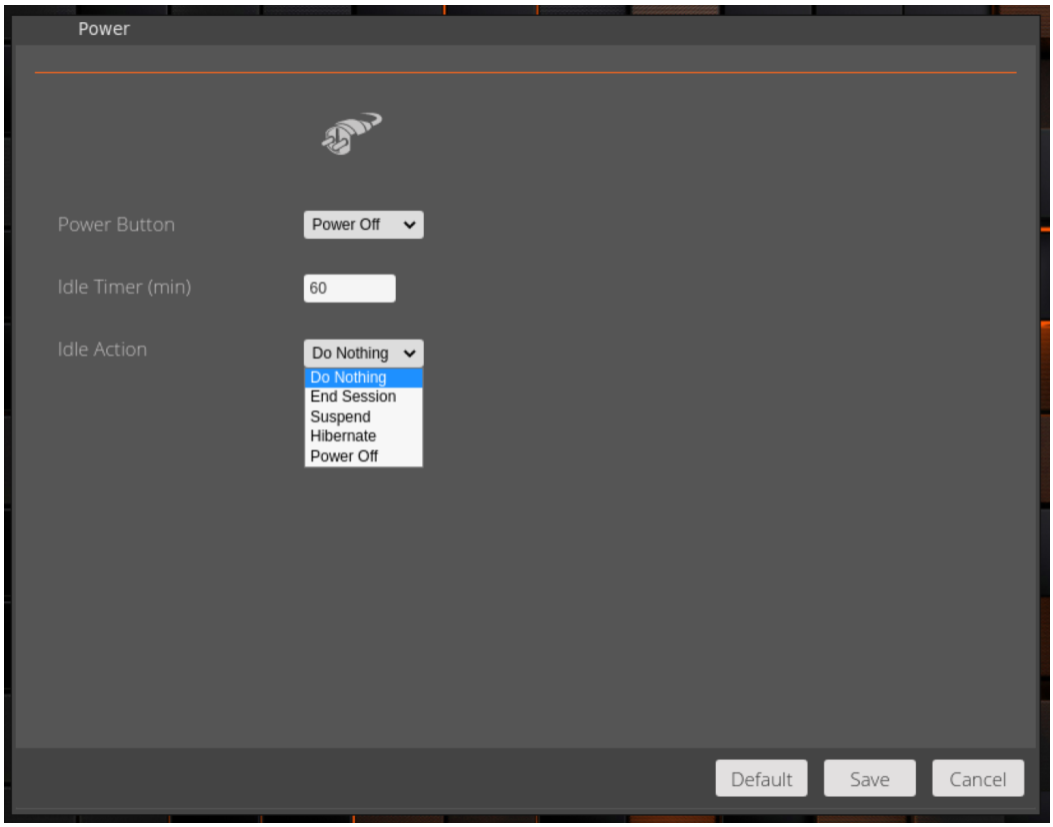
The Network File System applet will allow you to create remote network file share connections to your Thin Client. You have the option to mount a Windows “CIFS” or Linux “NFS” type connection.



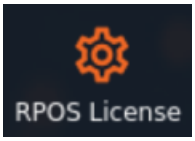
Power

Inside the “Power Management” screen, you have the ability to decide what the power button does when you depress it on your 10ZiG client. The options available are, “Hibernate”, “Power Off”, “End Session”, “Suspend”, or “Do nothing”.

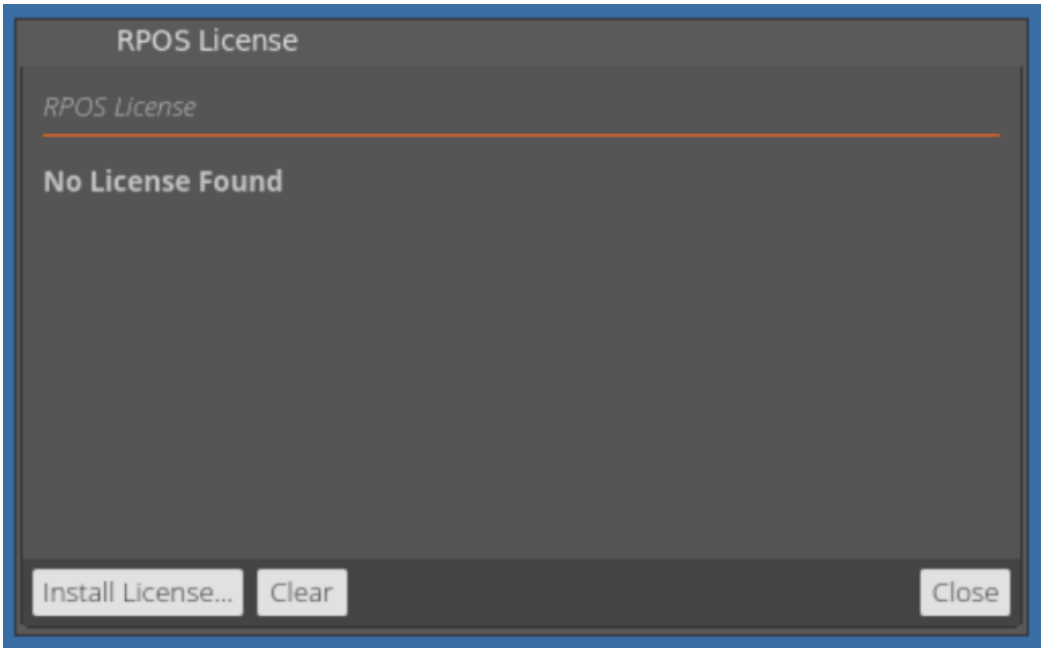
You also have the option to choose what to do if the device is idle for a specific period of time. Setting the idle timer will then allow you to select the “Idle Action”. These actions are the same as the “Power Button” actions above.



RPOS License



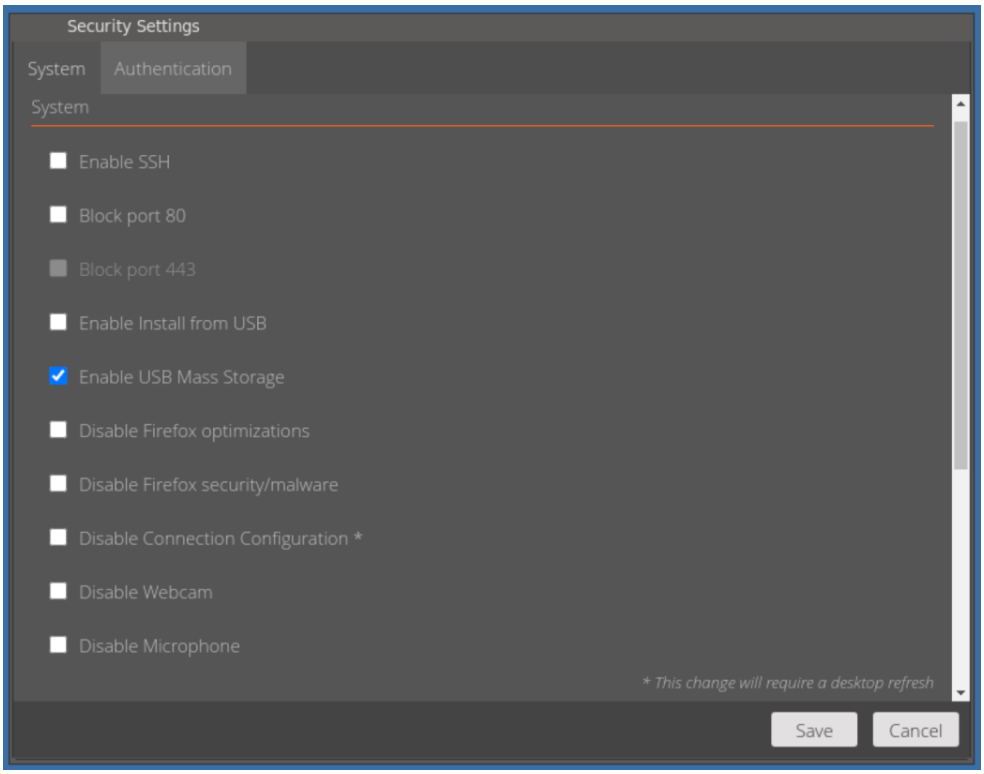
If you are running RepurpOS on a third party device, then you can use this screen to import your 10ZiG RepurpOS licenses.



Security settings

System

Security Settings allows administrators to set a password to be able to modify certain hardware settings. You can also enable installation from USB Mass Storage for thumb drives or external USB drives. This is also where you can enable the SSH Client option or disable webcam and microphone use.



There are two additional options related to behavioral configuration of the Mozilla “Firefox” browser.

The first one is “Disable Firefox optimizations” and ticking this option will disable some of the background network chatter that Firefox creates when launched. It is recommended to enable this option if you experience network issues due to “boot storms” / “login storms” when all units are opening Firefox at the same time. Otherwise, it is recommended to leave it unchecked by default.

The other “Firefox” configuration option is “Disable Firefox security/malware”. Enable this to disable remaining background chatter options which are generally used for security purposes. This disables important security features from Firefox such as: Malware protection, tracking protection, and TLS/SSL certification revocation check. This option should only be enabled on the advisory of a network administrator that has deemed it necessarily safe and secure to disable this background chatter from Firefox.

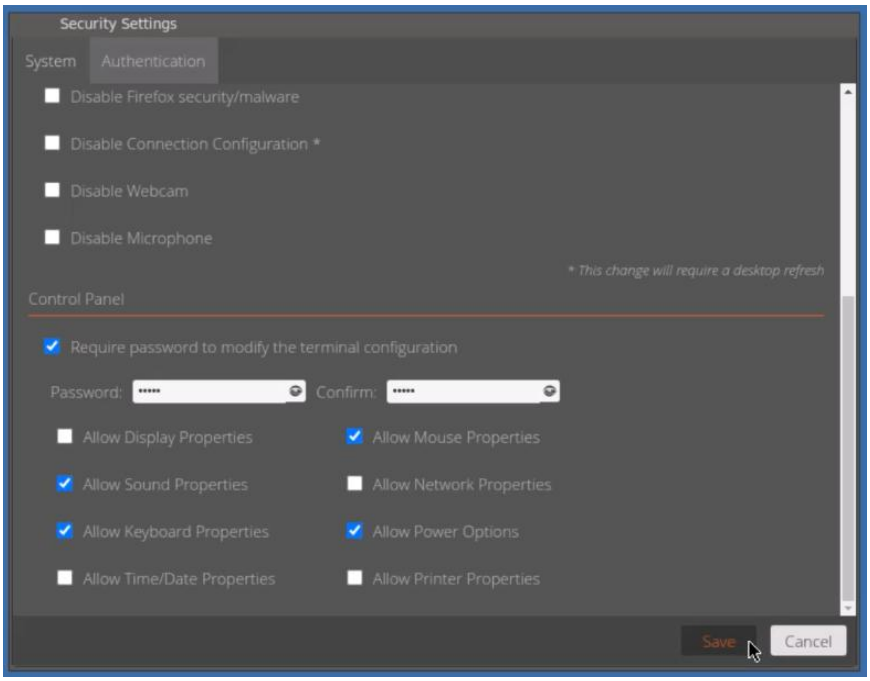
Enable Default Browser

There is an option further down this page called “Enable Default Browser”. If you disable this option, then any hyperlinks that are clicked inside the OS, will not open a web browser as an additional security feature.

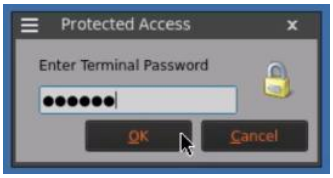
Control Panel Options inside Security Settings

If you scroll down whilst still inside the “System” tab, then you can specify the password that is required if you wish to access and then modify any Control Panel settings. You can also specify which Control Panel applets to allow on the Start Menu.

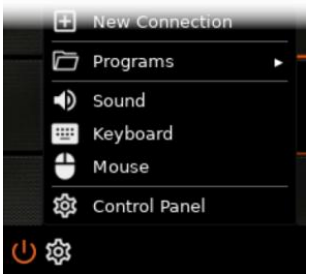
The screen below shows how to set the Control Panel password, and also which items are ticked that will be allowed in the Start Menu as default accessible items.



If you “Save” those options and then close and re-open the Control Panel, you will see the login box below, that will need to be authenticated in order to gain access to the Control Panel applets.



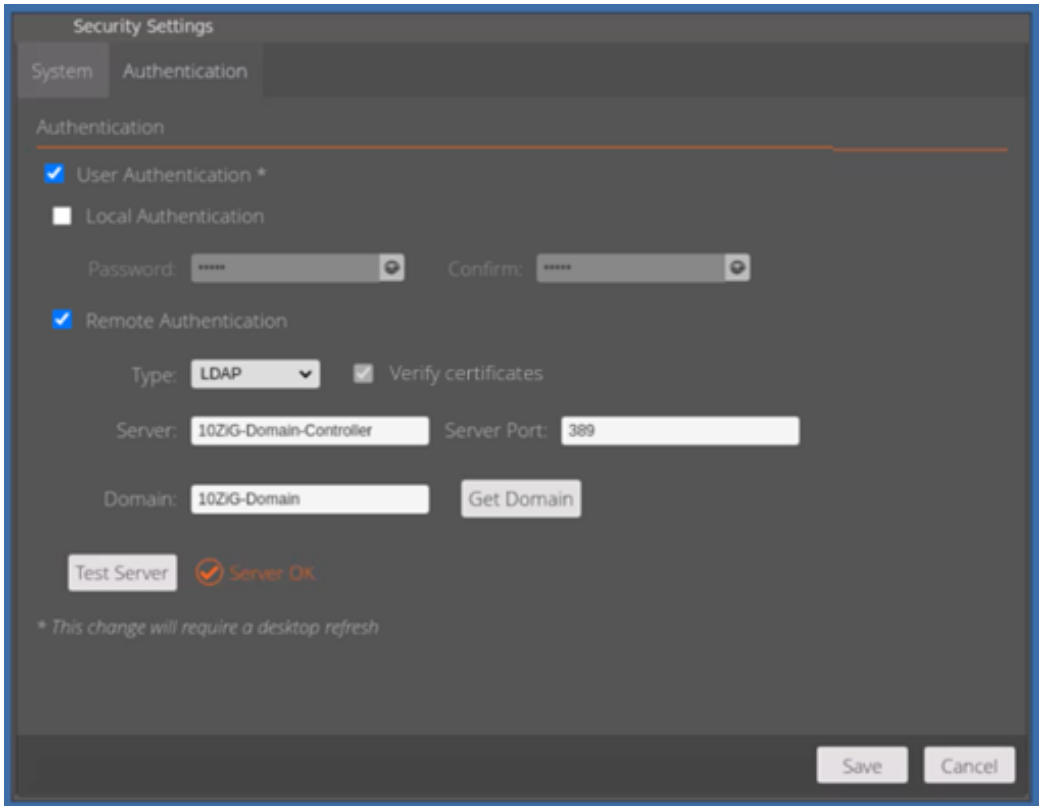
If you click the gears icon in the “Start Menu”, you’ll only see those Control Panel applets listed above, namely Sound, Keyboard, Mouse and Power Options.



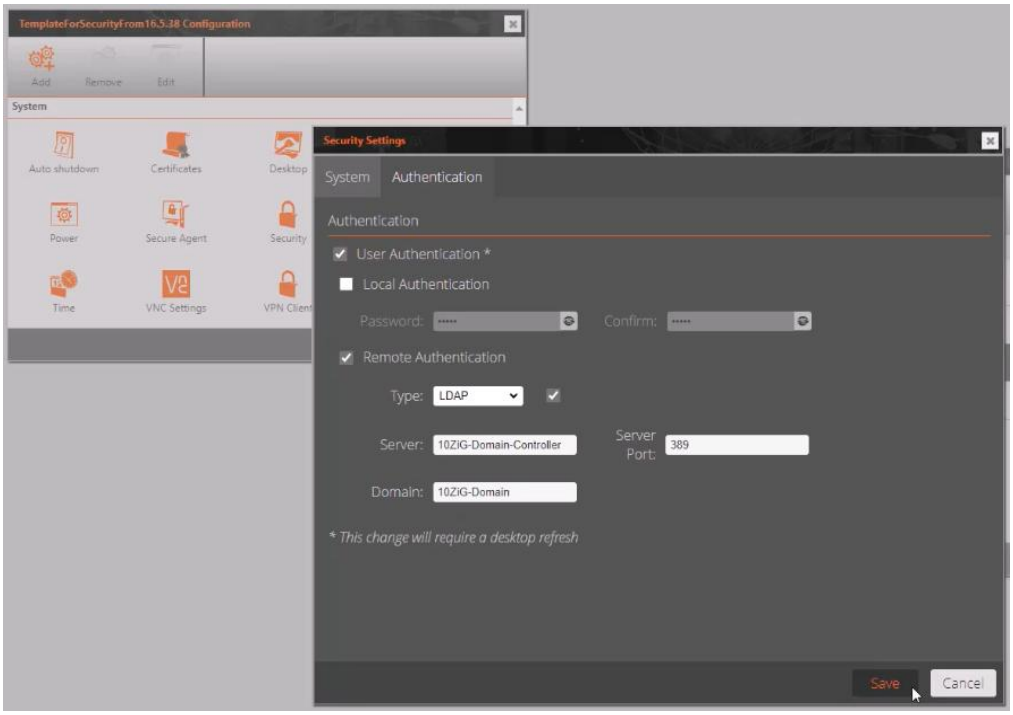
Authentication

Inside the authentication tab, you can specify the local user authentication or even specify LDAP domain network authentication. After you tick the “User Authentication” box, then you have a choice to either allow “Local Authentication” or have the device authenticate with your network domain controller.

The example below shows how to set up the LDAP connection for your thin client locally.

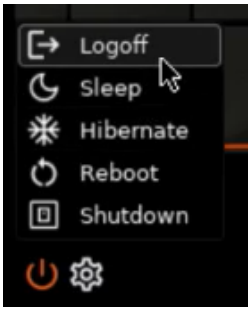


However, you can also do this by editing your configs or templates for your devices or device groups via the 10ZiG Manager Web Console. See below.

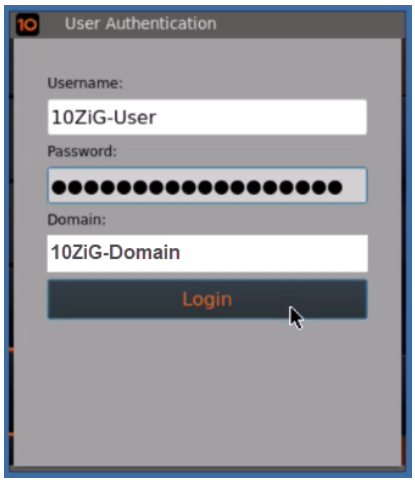


You can also tick the “Local Authentication” box and specify a password here or again via the 10ZiG Manager Web Console. After applying the changes, if you log off or restart the thin client, then you’ll be presented with the appropriate login box for your current authentication type. See below for examples of login types.

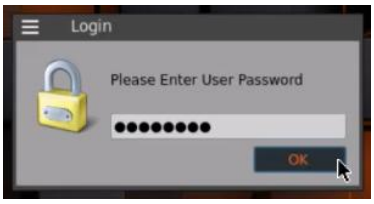
Logging off the client



Logging on via LDAP



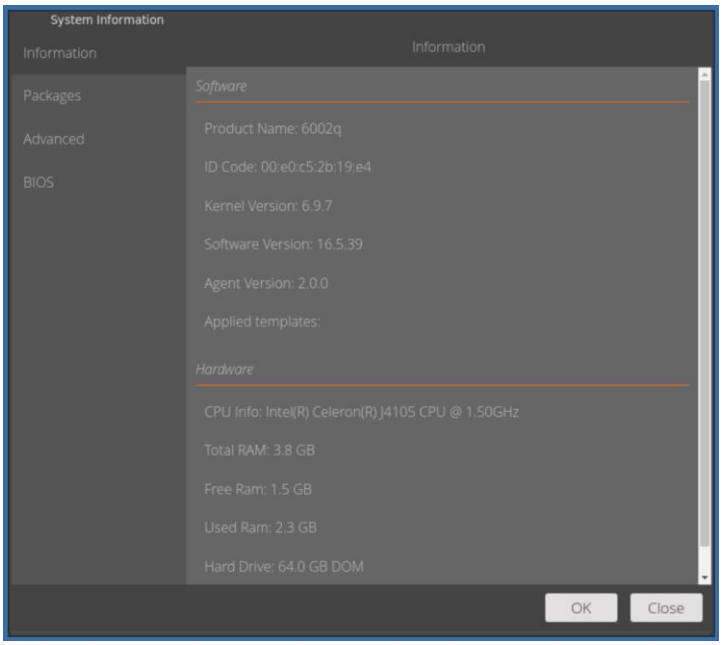
Logging on as a local user



System Information

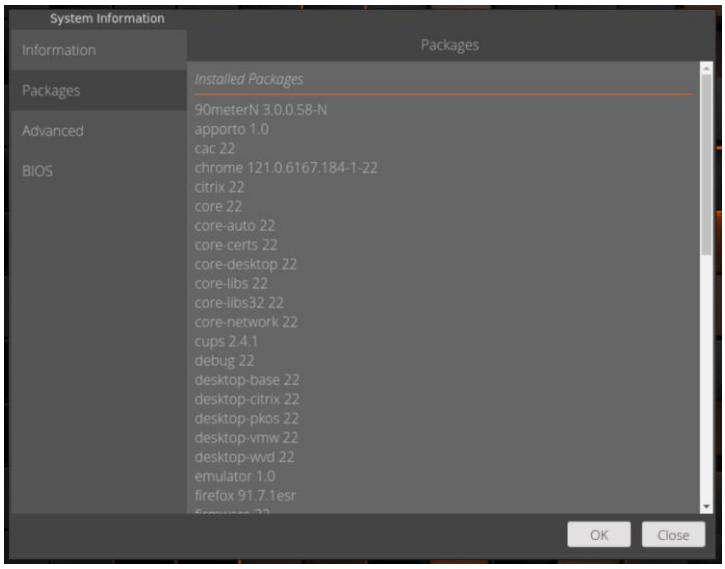
Information

The General option will allow administrators to identify the product name, the firmware version, the applied template (if any), and the name of the unit. The name can be easily changed by using the Change Name button.



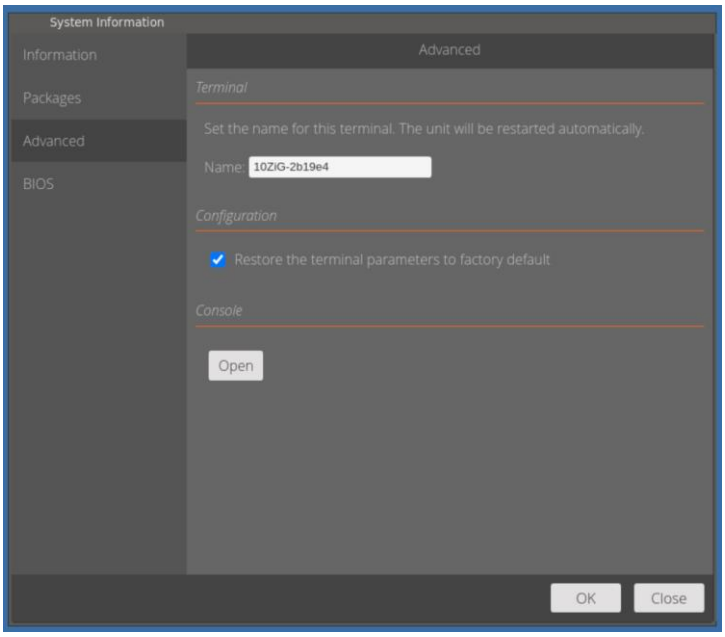
Packages

Selecting Packages will show the currently installed Linux packages on the Thin Client.

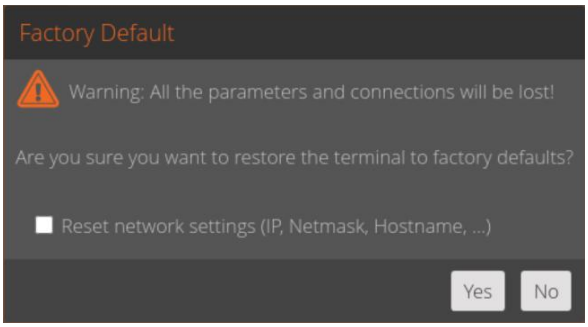


Advanced

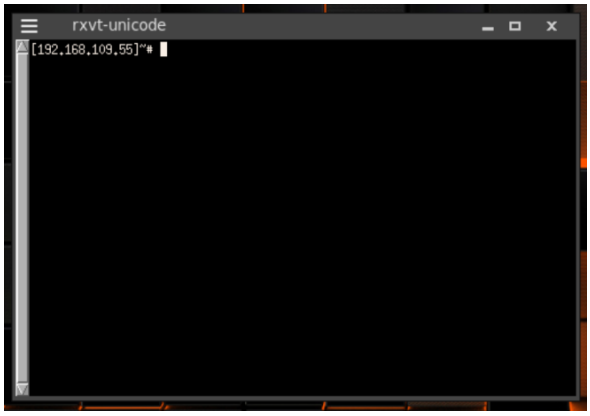
The Advanced options allow you to view more detailed info about the unit. Including CPU, HD size, RAM, Firmware and Kernel. You can also set the unit back to factory defaults, as well as launch a Linux console screen, by clicking the “Open” button.



Factory Default message

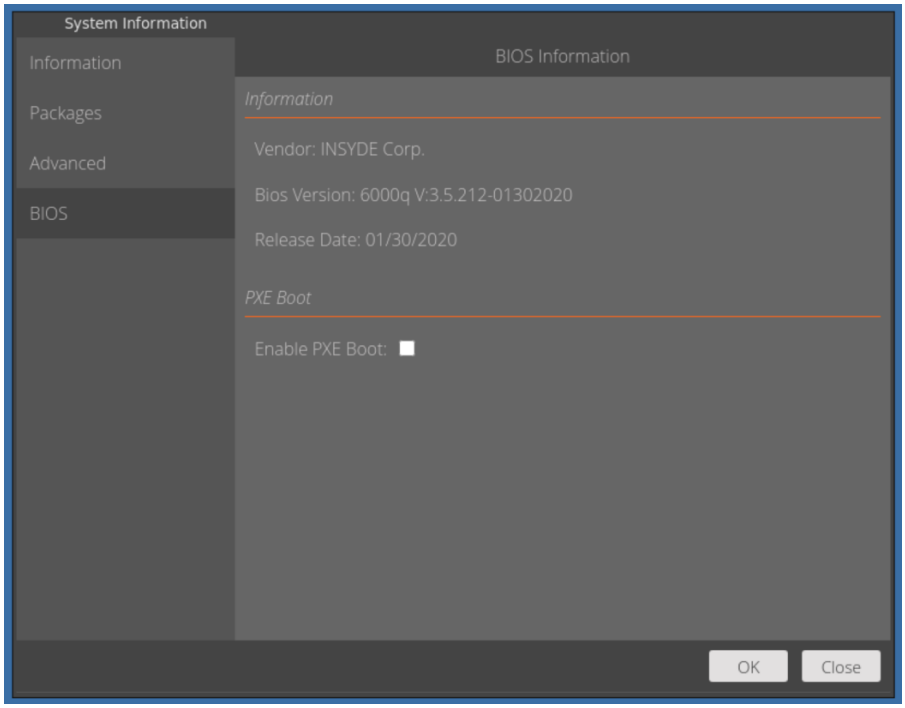


Console Screen



BIOS

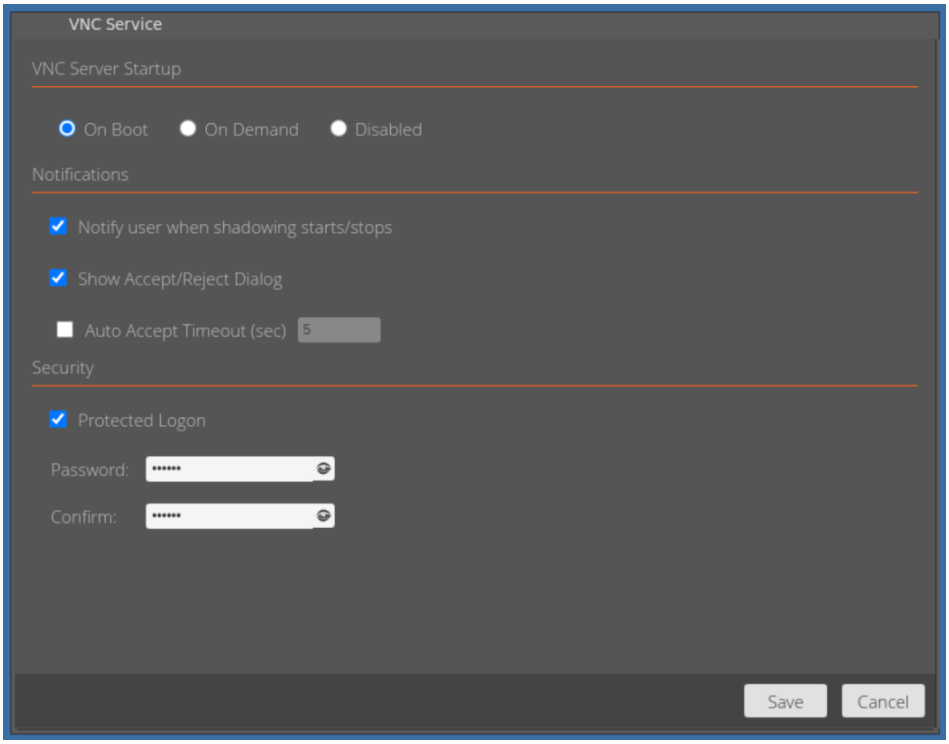
This screen gives you information relating to the BIOS and also allows you to set the boot mode to be PXE boot. Just tick the box, reboot the device and it will PXE boot on the next boot up.



VNC Service

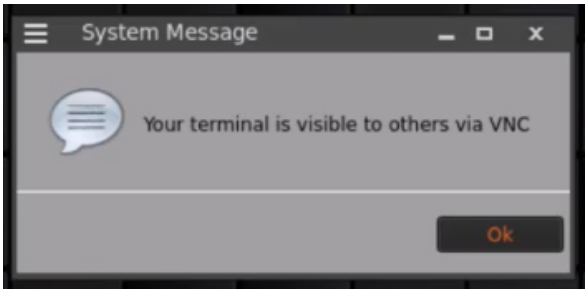
Here, you can edit the settings used to remotely connect to the unit using VNC (Virtual Network Computing). “Start VNC Server” options include “On Boot”, so that any VNC client can connect, “On Demand”, so only “Cloud Manager” connections are allowed or “Disable”, so that no connections are allowed. For added security, the “Show Accept/Reject Dialog” is on by default and gives the user of the remote device the option to accept or reject the incoming connection.

You also have the ability to set a password locally, that the client needs in order to gain access to the 10ZiG Thin Client.

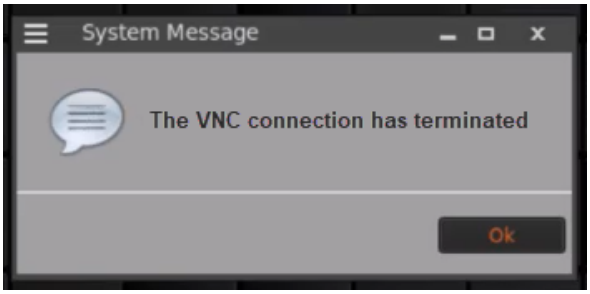


If you switch on the “Notify user when shadowing starts/stops” option, then your user will see the following notification messages when a shadow session starts and end respectively.

Start Shadowing



End Shadowing



VPN Client

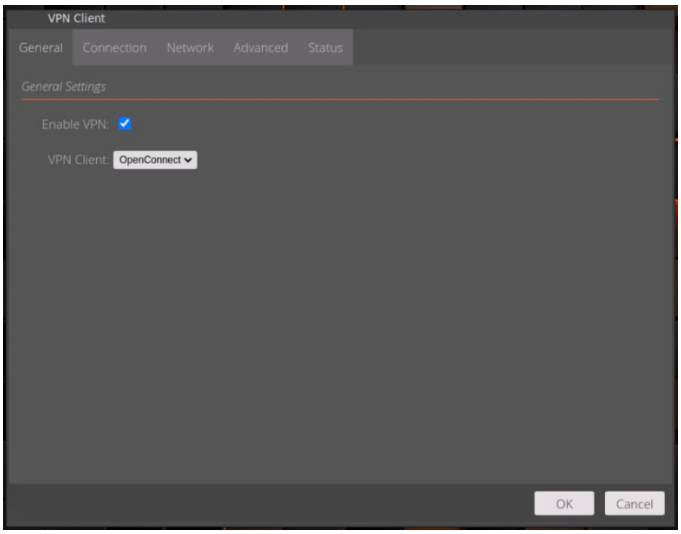
The VPN Client GUI runs on top of “OpenConnect”. OpenConnect is a cross-platform multi-protocol SSL VPN client which supports a number of VPN protocols as listed below.

- Cisco AnyConnect
- Array Networks SSL VPN
- Juniper SSL VPN
- Pulse Connect Secure
- Palo Alto Networks GlobalProtect SSL VPN
- F5 Big-IP SSL VPN
- Fortinet Fortigate SSL VPN

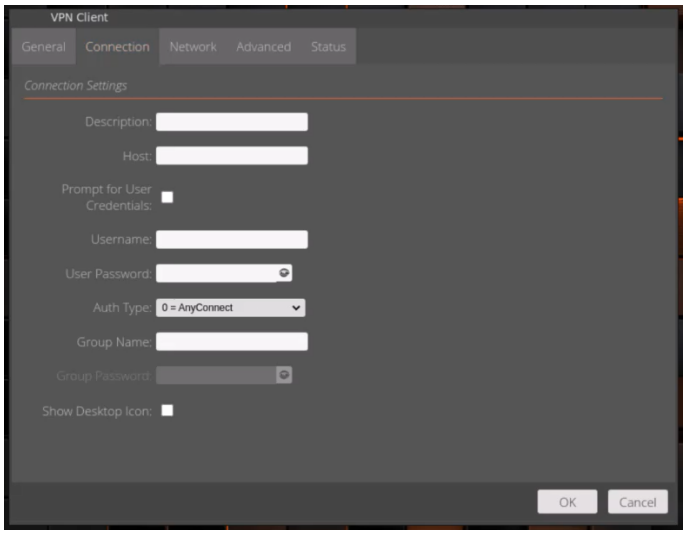
Contact your network or systems administrator if you need to set up this VPN client.

VPN Client GUI Screens

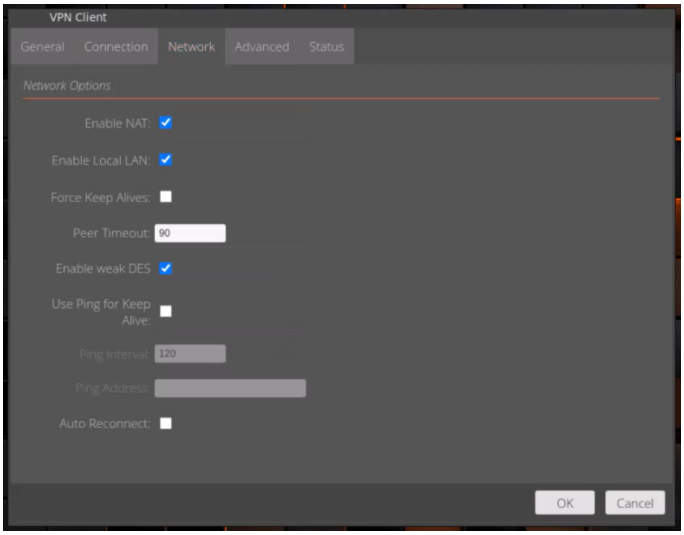
General



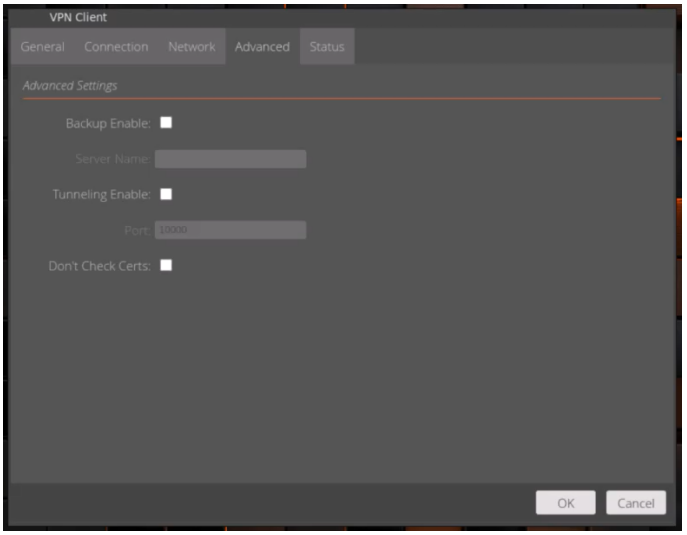
Connection



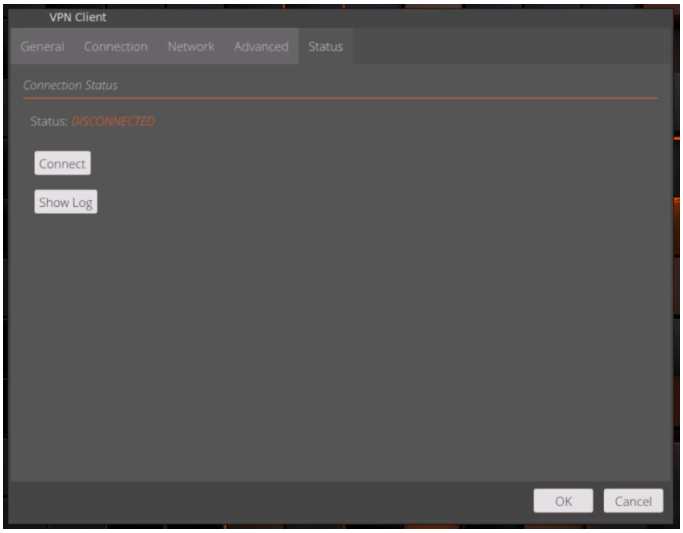
Network



Advanced



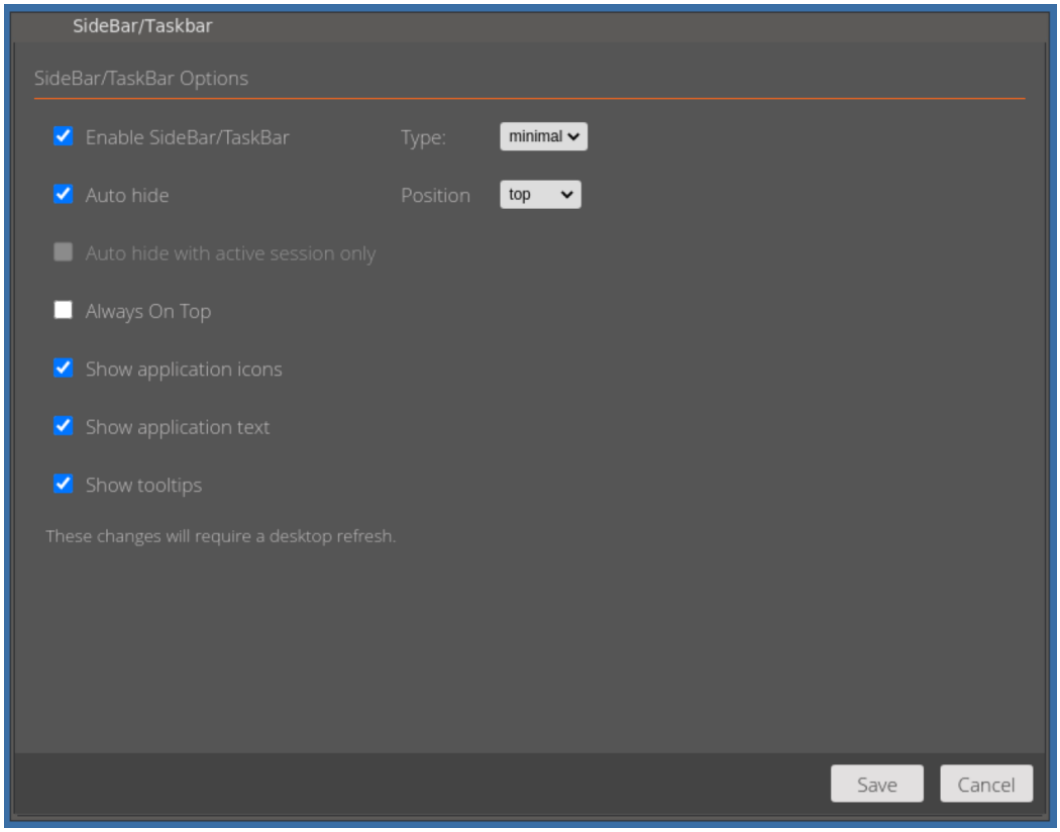
Status



SideBar/TaskBar

Enabling the SideBar/Taskbar gives you the ability see the current windowed tasks running on your 10ZiG Thin Client. You have multiple options available, including the type of bar, such as “full” length or “minimal” sized bar. You can also choose where to position it on screen and if you want it to display as icons, text, or both.

If you don’t always want visibility of it, then you have the option to “Auto hide” when not required.



Using the settings in the example above, here is the “SideBar/TaskBar” being displayed at the top of the screen, with the “Control Panel” task running.

For more information, FAQs, and helpful hints, please browse to
https://www.10zig.com/resources/support_faq

END OF DOCUMENT