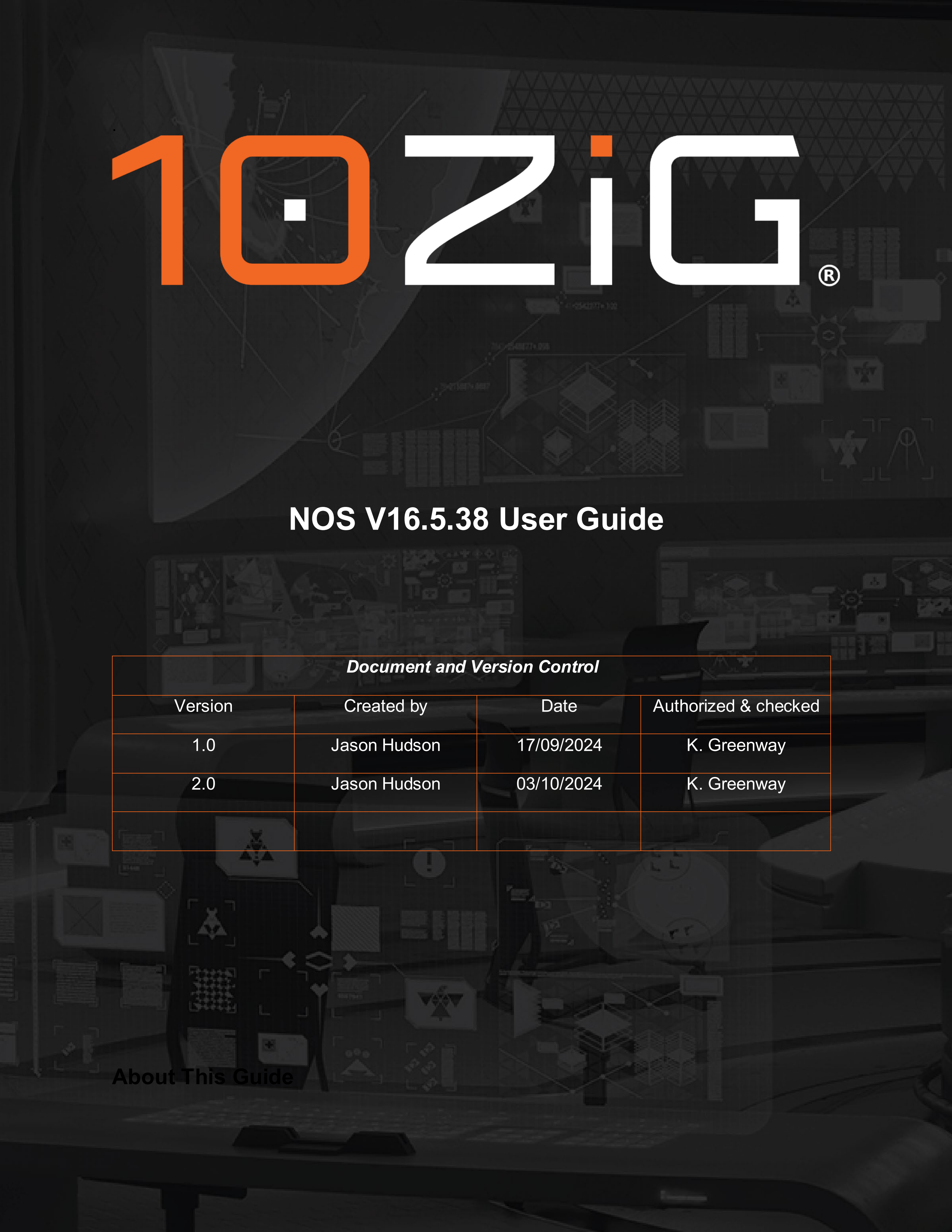


NOS V16.5.38 User Guide

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

About This Guide

Thank you for choosing from the 10ZiG Technology series of zero clients which are specifically designed for power users in an office environment. 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.

Getting Started

Packing List

The following components are included in the package:

- Zero 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 zero client, please contact your region's nearest Technical Support Center. While 10ZiG Technology does provide technical support for its Linux-based zero 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

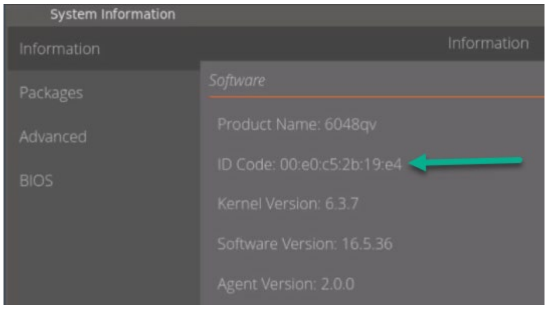
sales@10zig.eu

www.10zig.eu

ID Code

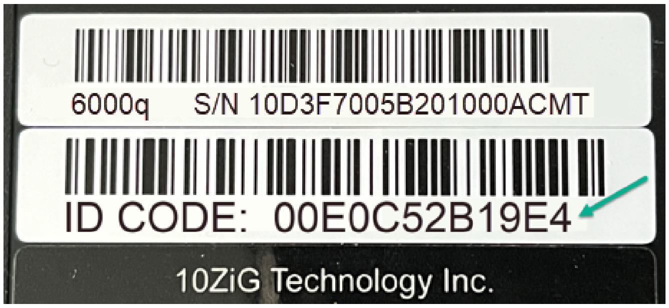
Each Thin client has a unique **ID CODE:** which is the **MAC address** of the unit. The sticker with this information may be found either on the side, bottom, near the video output port or on a slide out tab on the back of the unit, depending on which model you have. Please have this number available 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



Product Name: 6048qv
ID Code: 00:e0:c5:2b:19:e4
Kernel Version: 6.3.7
Software Version: 16.5.36
Agent Version: 2.0.0

The Device's Information Sticker



Introduction

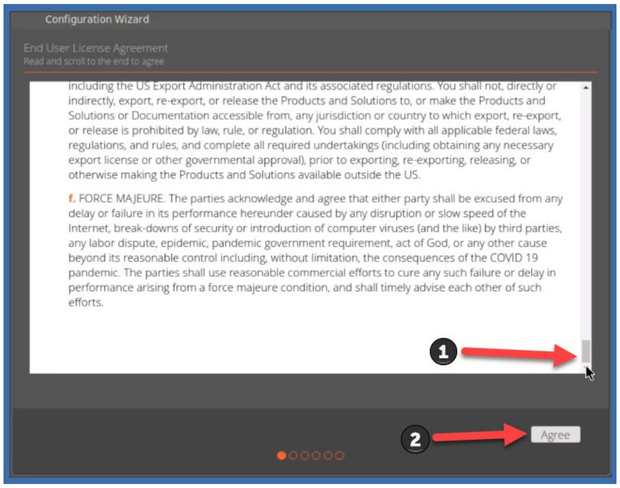
This guide provides the user with instructions for the hardware configuration of the Linux-based Zero Client and explains the various utilities used to accomplish these tasks. Typically, a Zero Client is configured locally and then used as a template to configure other units. These saved configuration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

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 ❶ and click “Agree” ❷

EULA



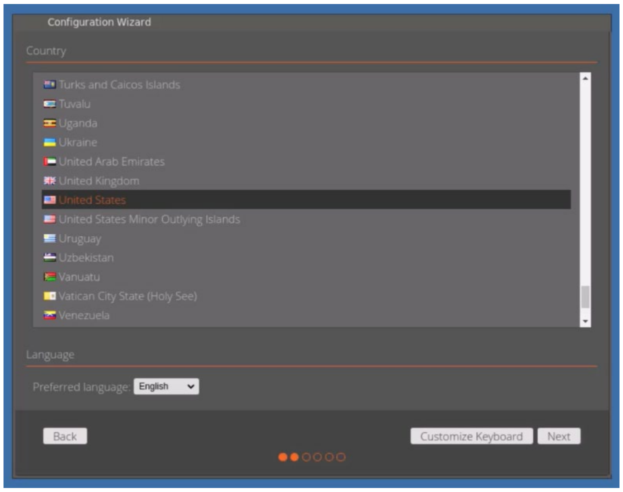
Configuration Wizard

End User License Agreement
Read and scroll to the end to agree

including the US Export Administration Act and its associated regulations. You shall not, directly or indirectly, export, re-export, or release the Products and Solutions to, or make the Products and Solutions or Documentation accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the Products and Solutions available outside the US.

f. FORCE MAJEURE. The parties acknowledge and agree that either party shall be excused from any delay or failure in its performance hereunder caused by any disruption or slow speed of the Internet, break-downs of security or introduction of computer viruses (and the like) by third parties, any labor dispute, epidemic, pandemic government requirement, act of God, or any other cause beyond its reasonable control including, without limitation, the consequences of the COVID 19 pandemic. The parties shall use reasonable commercial efforts to cure any such failure or delay in performance arising from a force majeure condition, and shall timely advise each other of such efforts.

Country and Language settings



Configuration Wizard

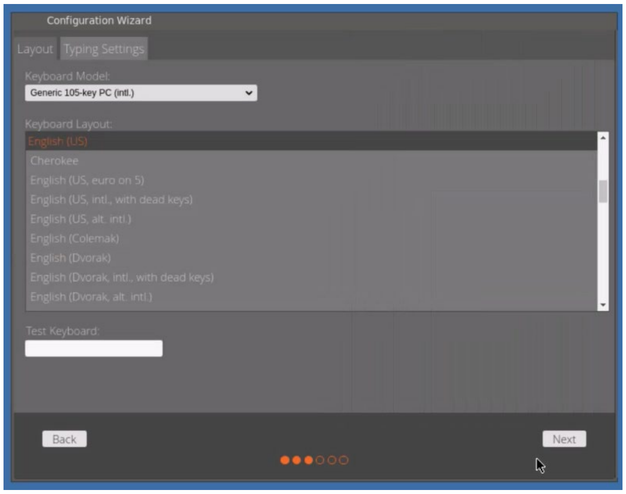
Country

- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- Uzbekistan
- Vanuatu
- Vatican City State (Holy See)
- Venezuela

Language

Preferred language: English

Keyboard settings



Configuration Wizard

Layout | Typing Settings

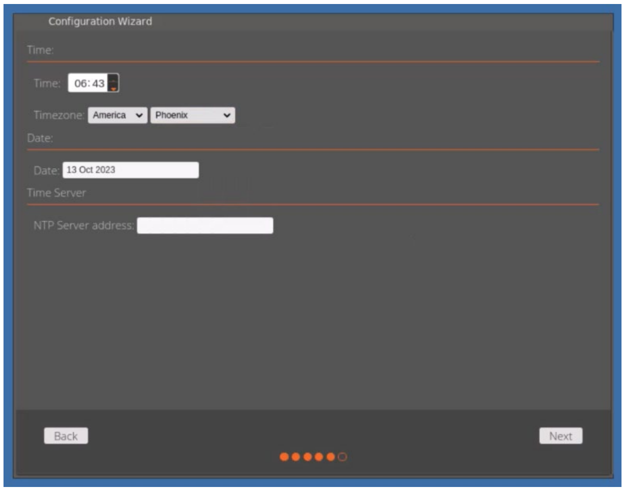
Keyboard Model: Generic 105-key PC (intl.)

Keyboard Layout:

- English (US)
- Cherokee
- English (US, euro on 5)
- English (US, intl., with dead keys)
- English (US, alt. intl.)
- English (Colemak)
- English (Dvorak)
- English (Dvorak, intl., with dead keys)
- English (Dvorak, alt. intl.)

Test Keyboard:

Time and Date settings



Configuration Wizard

Time:

Time: 06:43

Timezone: America Phoenix

Date:

Date: 13 Oct 2023

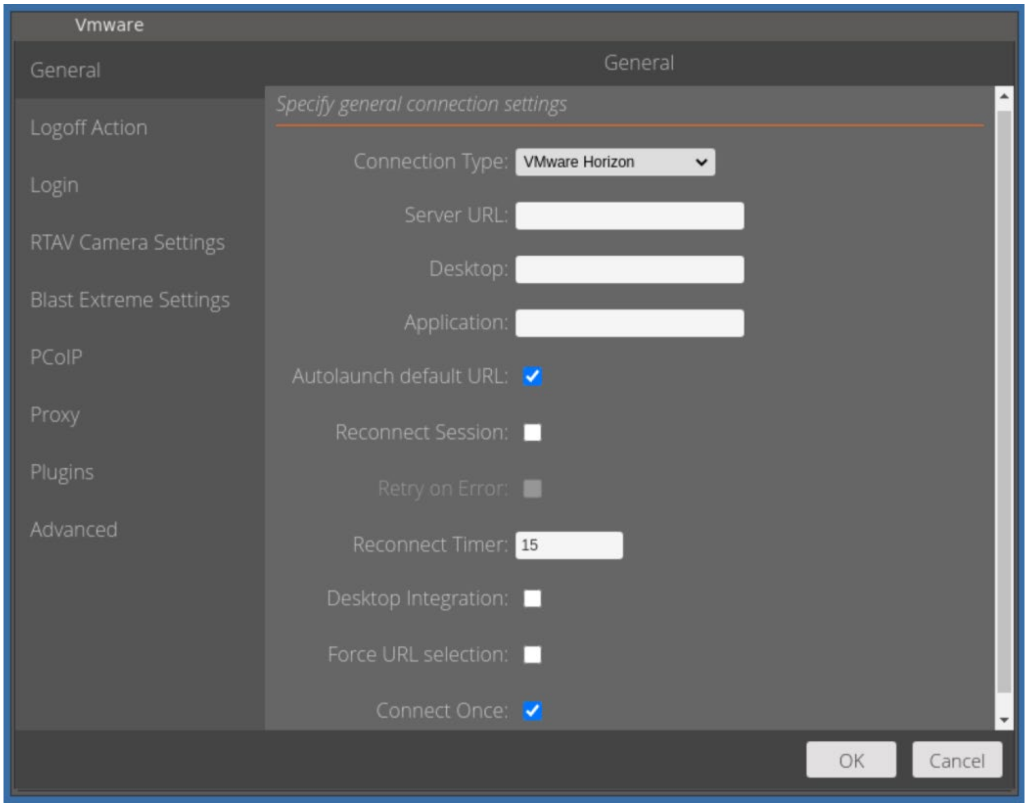
Time Server

NTP Server address:

NOS for VMware NOS-V

General

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



General

Specify general connection settings

Connection Type: VMware Horizon

Server URL:

Desktop:

Application:

Autolaunch default URL: ☑

Reconnect Session: □

Retry on Error: □

Reconnect Timer: 15

Desktop Integration: □

Force URL selection: □

Connect Once: ☑

- **Connection type**: The type of connection you wish to set up, either a “VMware Horizon” or “VMware 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 VMware server environment.

- **Desktop**: The name of the published VMware desktop you would like to connect to by default.

- **Application**: The name of the published VMware 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 VMware 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).

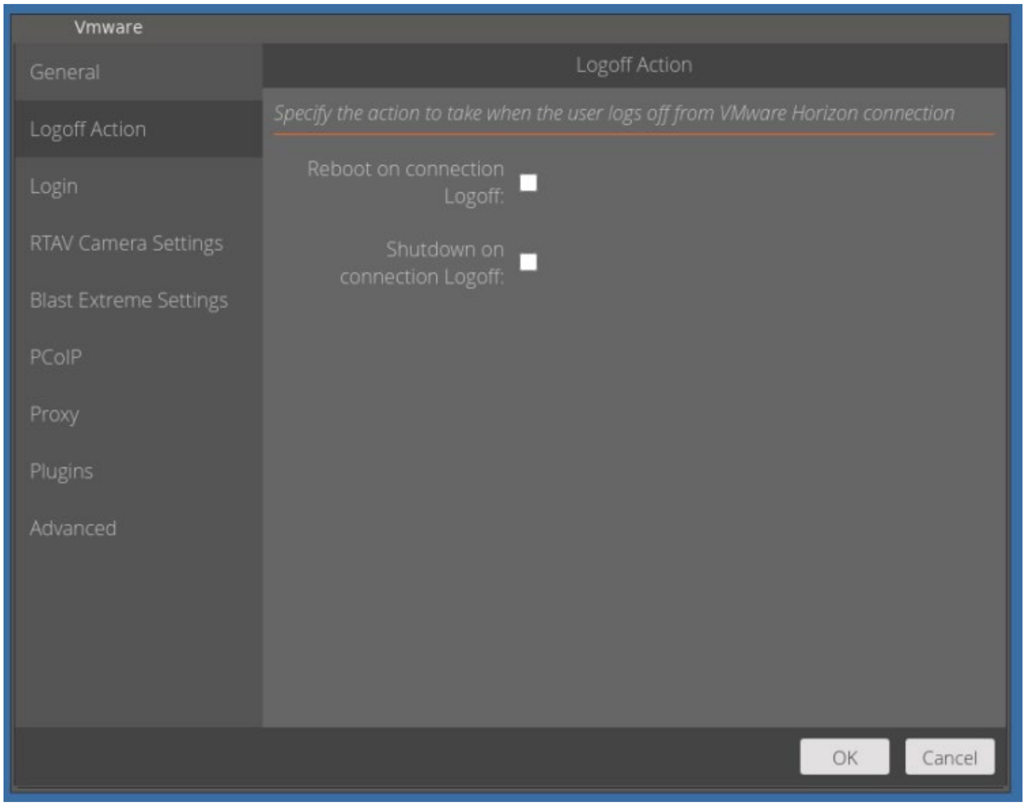
- **Desktop Integration**: Enabling this, separates VMware’s message prompts that usually display as a banner within the Horizon client, to a local dialog box instead. This can useful when users are prone to entering wrong credentials – the horizon client will re-prompt for an incorrect password, but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

- **Connect Once**: On session logoff or password error/expiry, the VMware Client is closed automatically where this option is enabled.

Logoff Action

Allows you to control the behavior of the NOS-V client, following disconnect and logoff from VMware remote session.



Specify the action to take when the user logs off from VMware Horizon connection

Reboot on connection Logoff: □

Shutdown on connection Logoff: □

- **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.

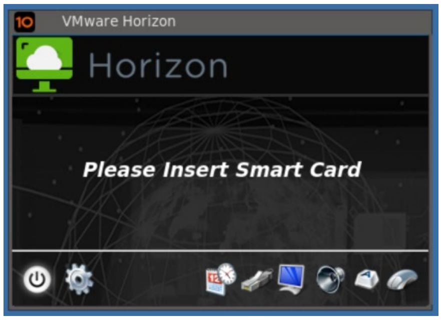
Login

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

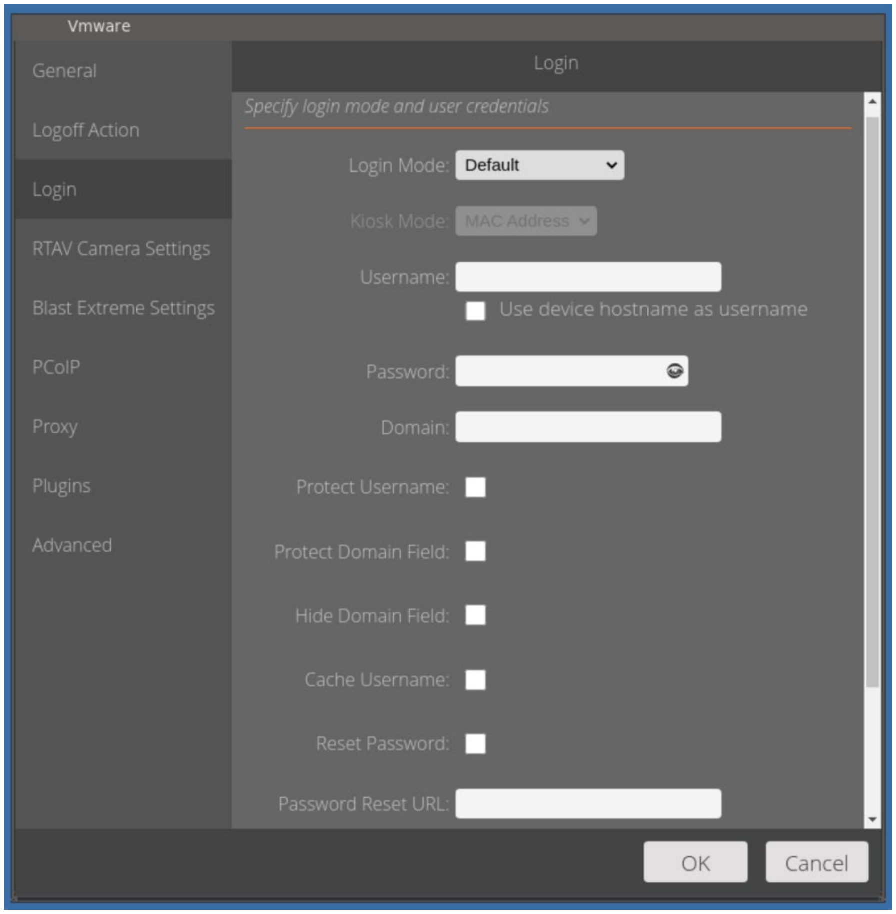
- **Login Mode**: There are several ways that you can configure the NOS-V client when it comes to logging in to your VMware sessions. These are :-

  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.



Please Insert Smart Card



Specify login mode and user credentials

Login Mode: Default

Kiosk Mode: MAC Address

Username:

□ Use device hostname as username

Password:

Domain:

Protect Username: □

Protect Domain Field: □

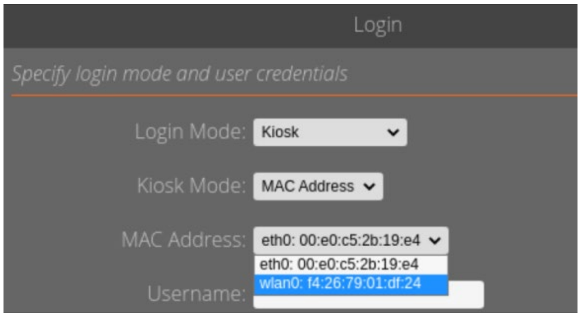
Hide Domain Field: □

Cache Username: □

Reset Password: □

Password Reset URL:

- **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.



Login

Specify login mode and user credentials

Login Mode: Kiosk

Kiosk Mode: MAC Address

MAC Address: eth0: 00:e0:c5:2b:19:e4

eth0: 00:e0:c5:2b:19:e4
wlan0: f4:26:79:01:df:24

Username:

- **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.

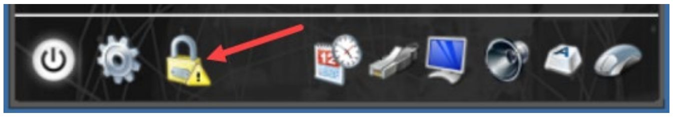
- **Protect Username**: If you have selected “Login Mode” to be “SCLogin” for smart card use, the username will be greyed out at the connect screen.

- **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 VMware settings and ‘Parse Token Username’ option is enabled, the following should be transmitted at point of login.

  ```
  Vmware-view --serverURL=’horizonservername’ -q --userName=’username’ --passcode=’password’
  ```

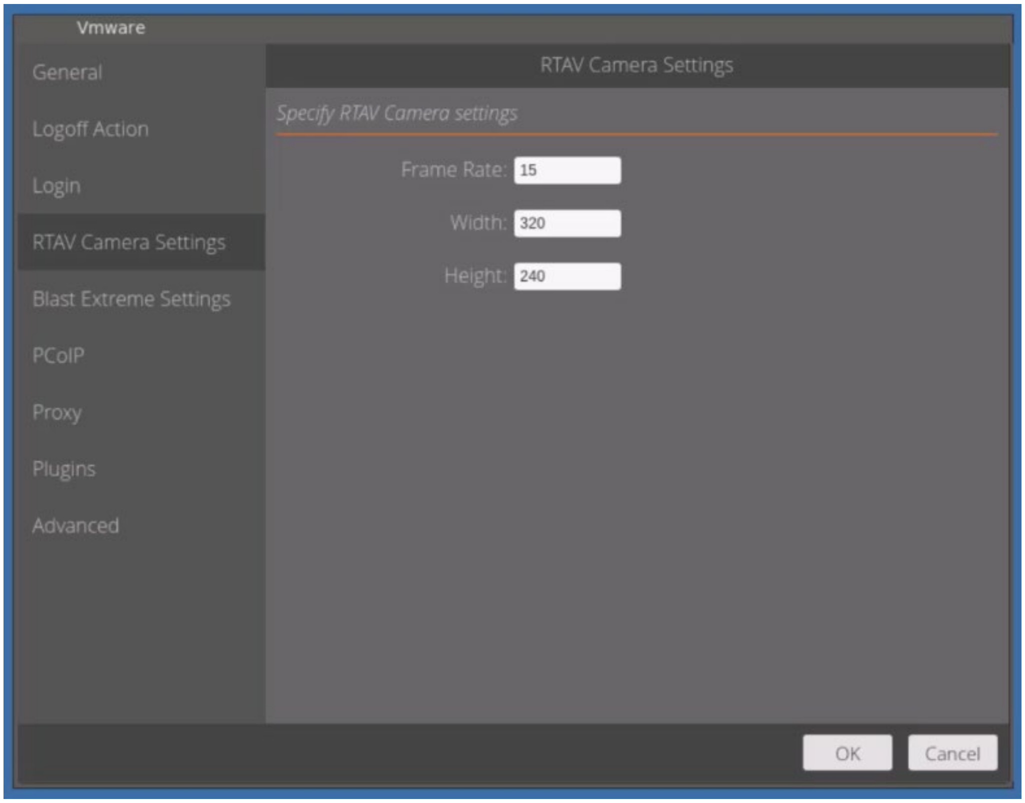
  Note: The following commands are used in place of a ‘Default’ login. The usage in this scenario of --userName vs --tokenUserName causes the VMware client to cache the username field, so that the user is only required to enter their username once during login. Where as in scenario #1, the user is required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

RTAV(Real Time Audio and Video) Camera Settings

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



Specify RTAV Camera settings

Frame Rate: 15

Width: 320

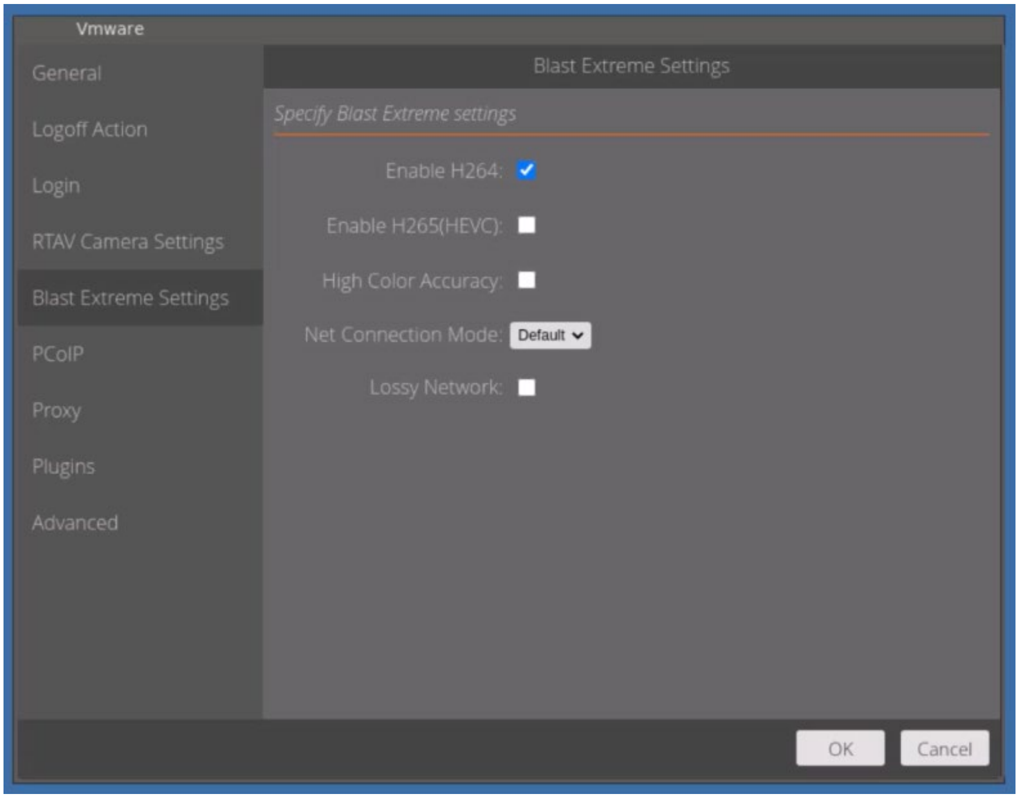
Height: 240

- **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 a VMware virtual channel for transmitting Audio/Video. This allows you to control the Frame rate for the video feed. VMware 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 VMware 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.



Blast Extreme Settings

Specify Blast Extreme settings

Enable H264: ☑

Enable H265(HEVC): □

High Color Accuracy: □

Net Connection Mode: Default

Lossy Network: □

- **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.

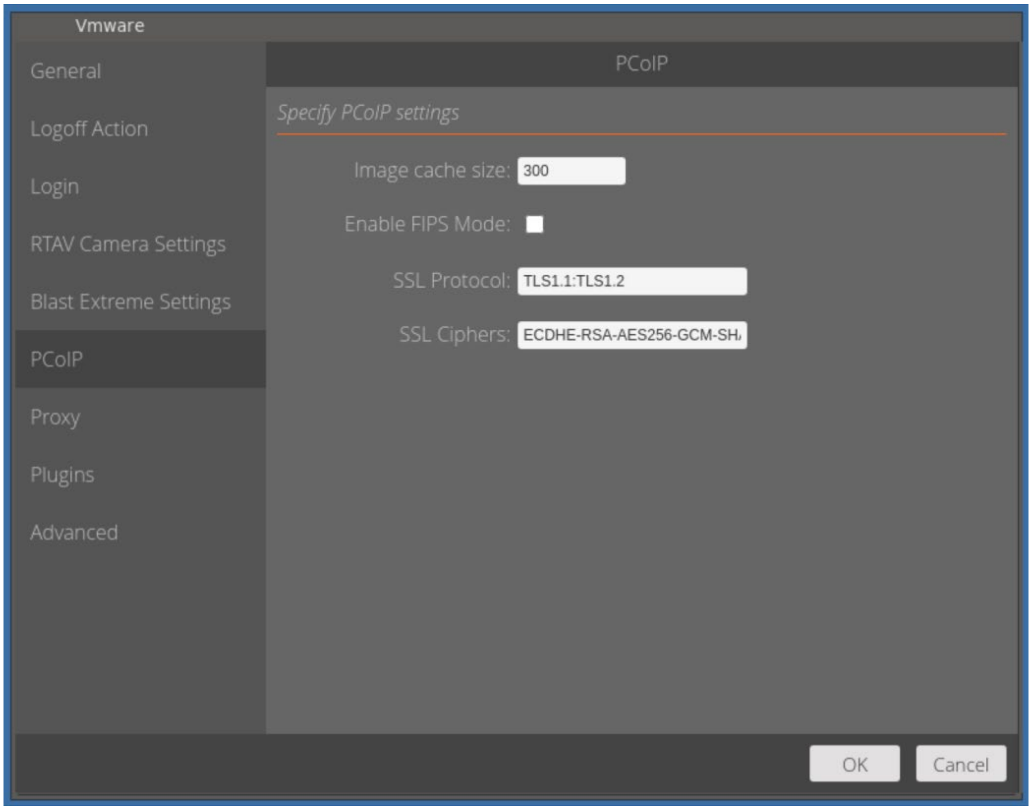


Image cache size: 300

Enable FIPS Mode: □

SSL Protocol: TLS1.1:TLS1.2

SSL Ciphers: ECDHE-RSA-AES256-GCM-SH/

- **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.

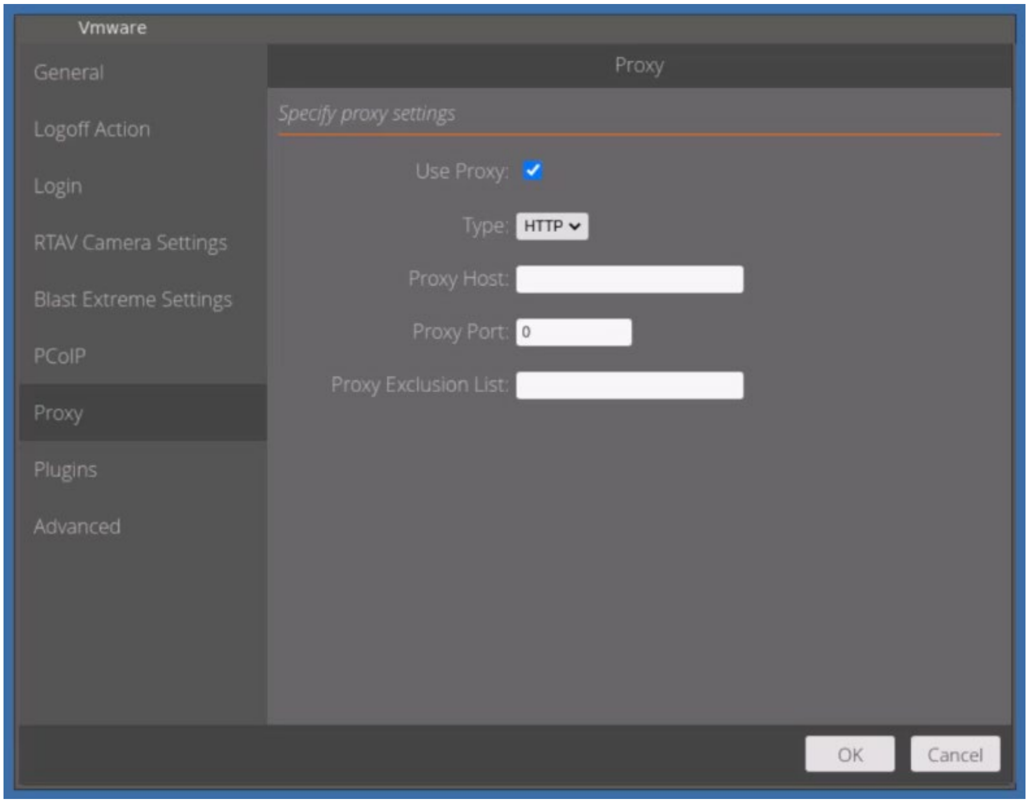
- **Enable FIPS Mode**: You can enable FIPS (Federal Information Processing Standard) Compatible mode so that the client uses FIPS-compliant cryptographic algorithms when communicating with remote desktops.

- **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.



Proxy

Specify proxy settings

Use Proxy: ☑

Type: HTTP

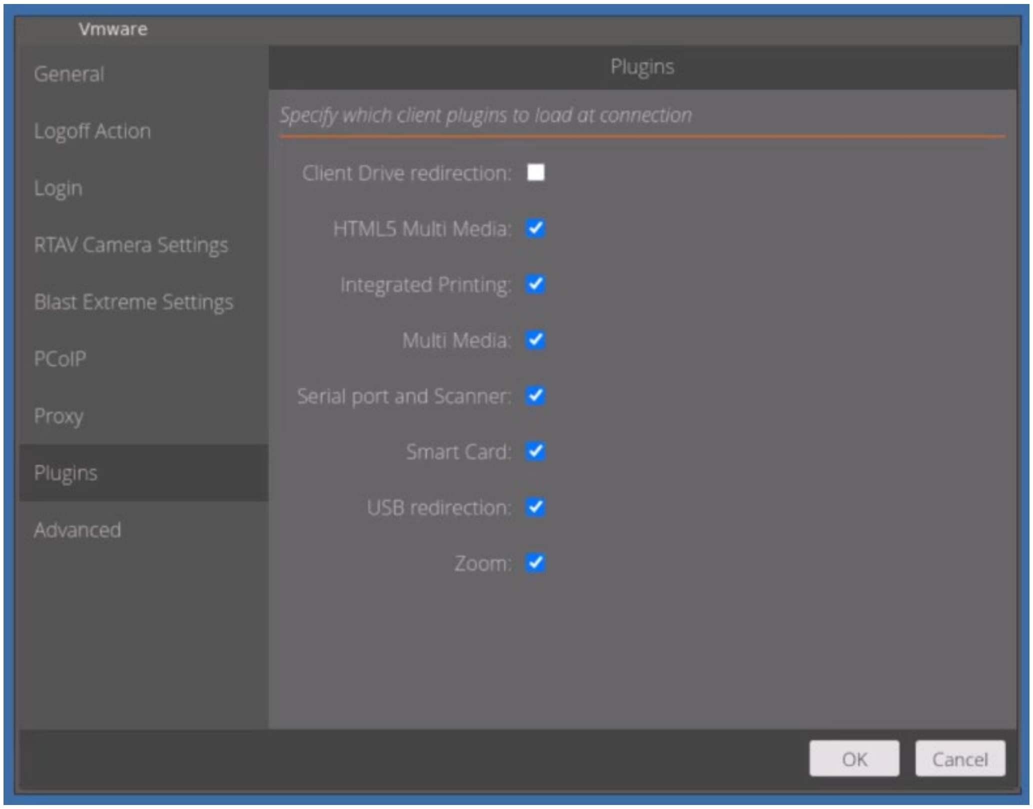
Proxy Host:

Proxy Port: 0

Proxy Exclusion List:

- **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



Specify which client plugins to load at connection

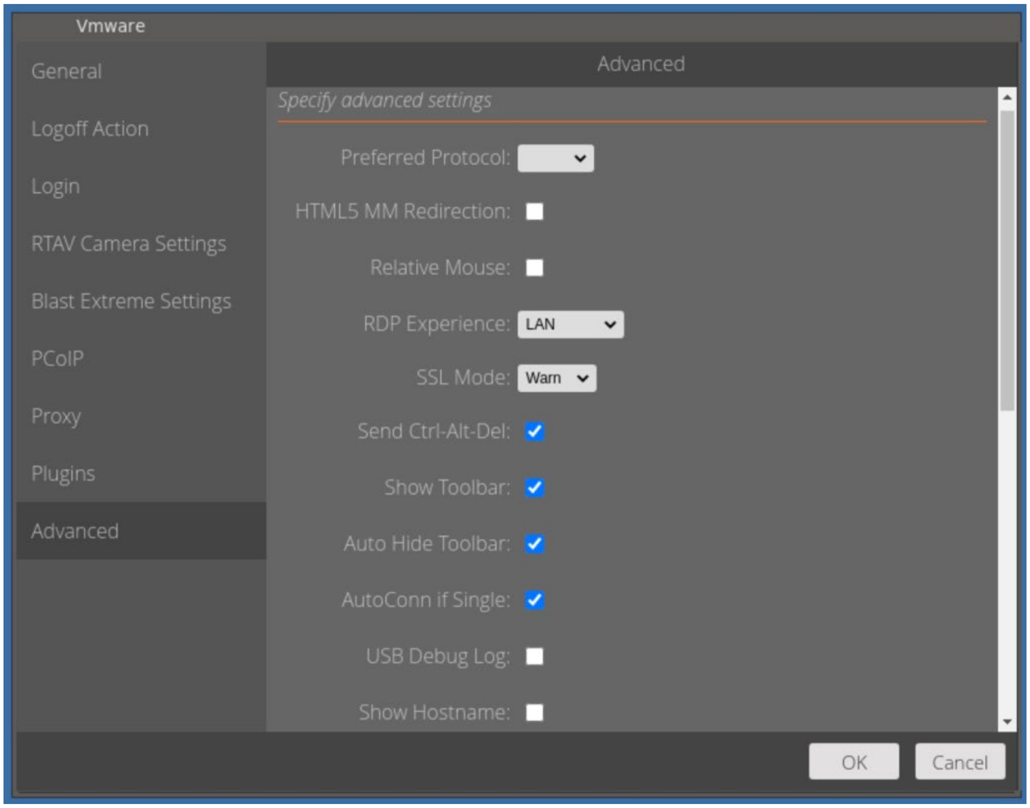
Client Drive redirection: □
HTML5 Multi Media: ☑
Integrated Printing: ☑
Multi Media: ☑
Serial port and Scanner: ☑
Smart Card: ☑
USB redirection: ☑
Zoom: ☑

- Plugins (various): This tab gives administrators the ability to enable (default) or disable the various plugins or virtual channels the VMware 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 “VMware Horizon Settings” allows additional customization to be carried out.



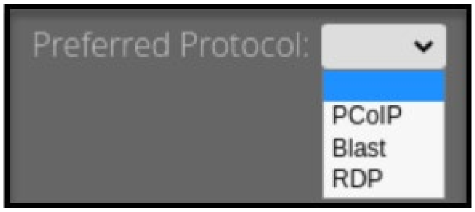
Advanced

Specify advanced settings

Preferred Protocol:
HTML5 MM Redirection: □
Relative Mouse: □
RDP Experience: LAN
SSL Mode: Warn
Send Ctrl-Alt-Del: ☑
Show Toolbar: ☑
Auto Hide Toolbar: ☑
AutoConn if Single: ☑
USB Debug Log: □
Show Hostname: □

- **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 VMware Horizon Performance Tracker on the desktop you connected to, and the protocol should show either PCoIP, Blast or RDP.



- **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 VMware 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.

- **RDP experience**: This sets the session quality relative to the network performance when using RDP as the protocol.

- **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.

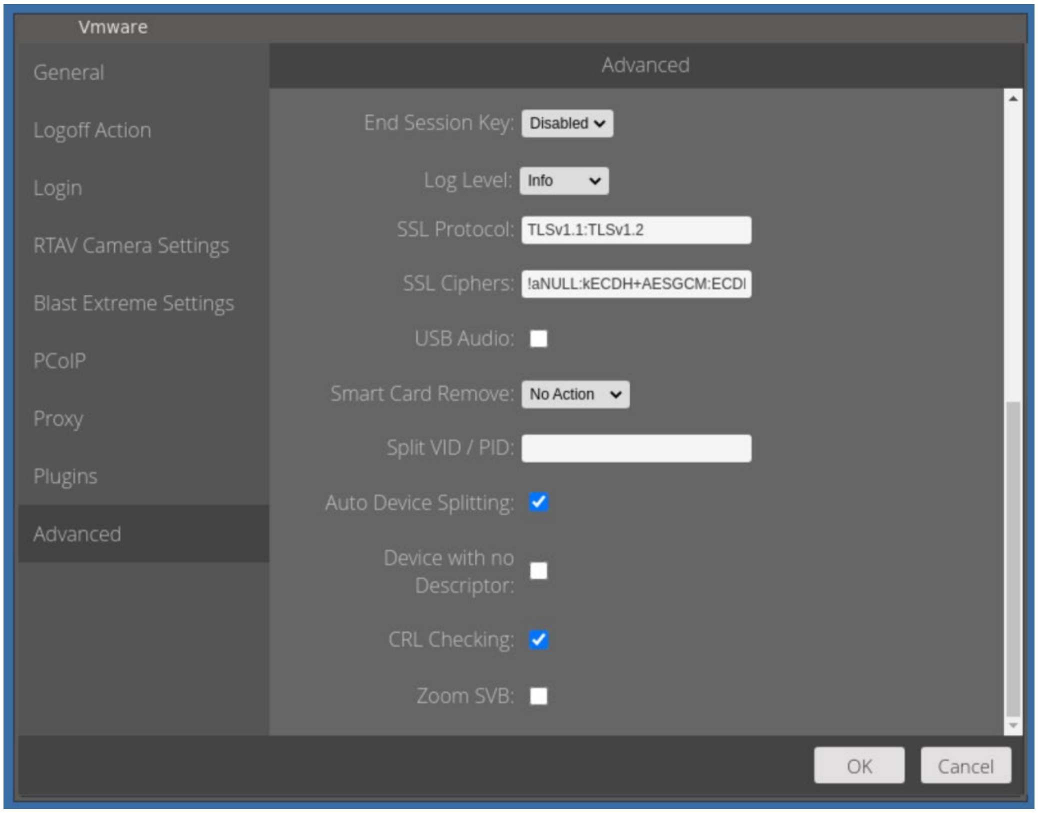
- **Show Toolbar**: This allows you to show the VMware menu bar dropdown when in the session. The VMware tool bar will be accessible in session, pinned at the top of the screen.

- **Auto Hide Toolbar**: Auto Hide the toolbar when enabled. The VMware 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 VMware Authentication login screen. It is useful for end users who can provide 10ZiG Manager administrators with the hostname required for shadowing their session.



Advanced

End Session Key: Disabled

Log Level: Info

SSL Protocol: TLSv1.1:TLSv1.2

SSL Ciphers: !aNULL:kECDH+AESGCM:ECDI

USB Audio: □

Smart Card Remove: No Action

Split VID / PID:

Auto Device Splitting: ☑

Device with no Descriptor: □

CRL Checking: ☑

Zoom SVB: □

- **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 VMware broker, regardless of whether the “Connect Once” option is enabled or not.

- **Log level**: Configure the logging level for the VMware 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 VMware Horizon documentation under the section 'Configuring Device Splitting Policy Settings for Composite USB Devices' https://docs.vmware.com/en/VMware-Horizon/2212/horizon-remote-desktop-features/GUID-16FA160C-475A-42A8-A4A1-33096BC41FC9.html

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

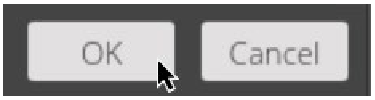
- **Device with no Descriptor**: This allows the device to be redirected even if the Horizon Client fails to get the device descriptors.

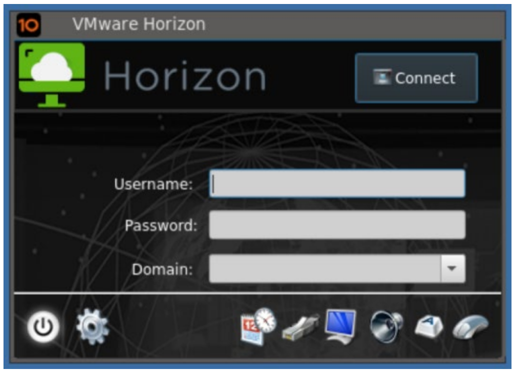
- **CRL checking**: This allows the device to check for a CRL or Certificate Revocation List from a Certificate Authority(CA), to prove that any existing certificates are still valid or have been revoked before they are due to expire. It's a recommendation to disable this option where CRL checking is 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.

Saving your settings

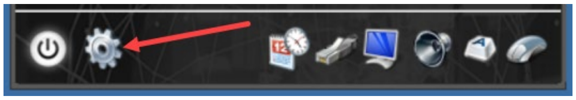
Once you're comfortable with all the settings for your 10ZiG NOS-V client, just click the "OK" button and you'll be taken back to the Horizon login screen.



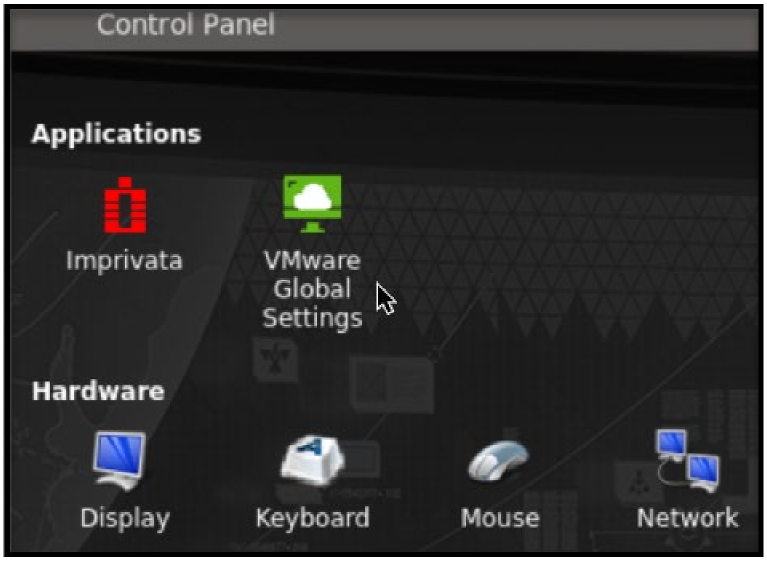


Editing your connection settings

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 "VMware Global Settings" icon and you'll be taken back into the "Settings" console again.

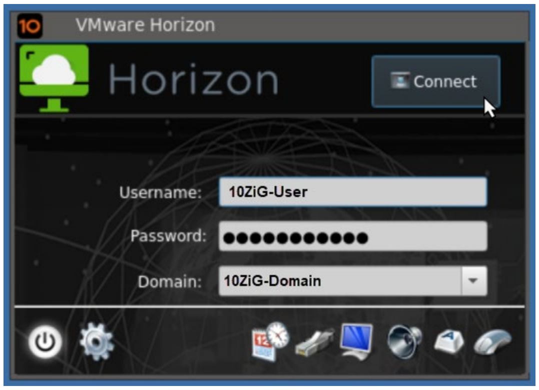


VMware Horizon Connection Examples

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”.



Username: 10ZiG-User

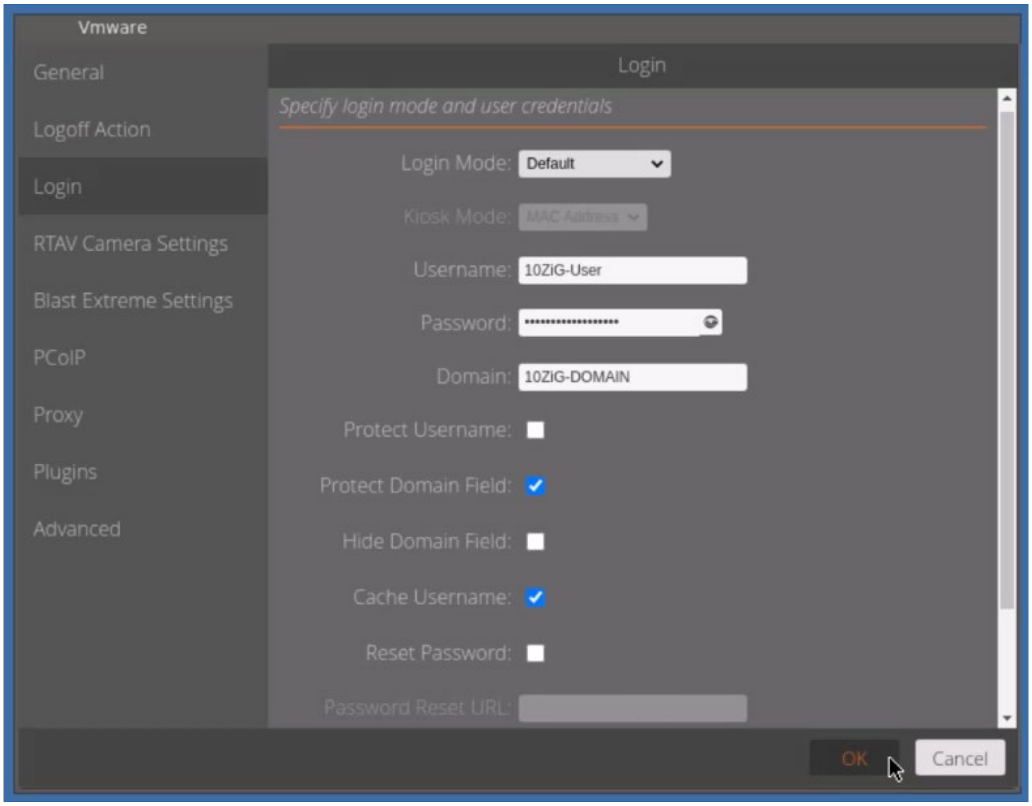
Password: ●●●●●●●●●●●

Domain: 10ZiG-Domain

Caching credentials and protecting the domain

Go into the “VMware 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”.



Login

Specify login mode and user credentials

Login Mode: Default

Kiosk Mode: MAC Address

Username: 10ZiG-User

Password: ••••••••••••••••••

Domain: 10ZIG-DOMAIN

Protect Username: □

Protect Domain Field: ☑

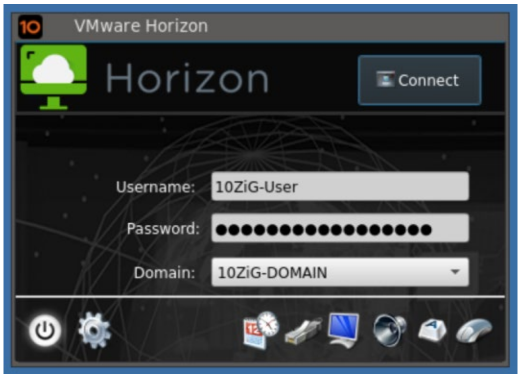
Hide Domain Field: □

Cache Username: ☑

Reset Password: □

Password Reset URL:

The login box should look something like below :-



Username: 10ZiG-User

Password: ●●●●●●●●●●●●●●●●●●

Domain: 10ZiG-DOMAIN

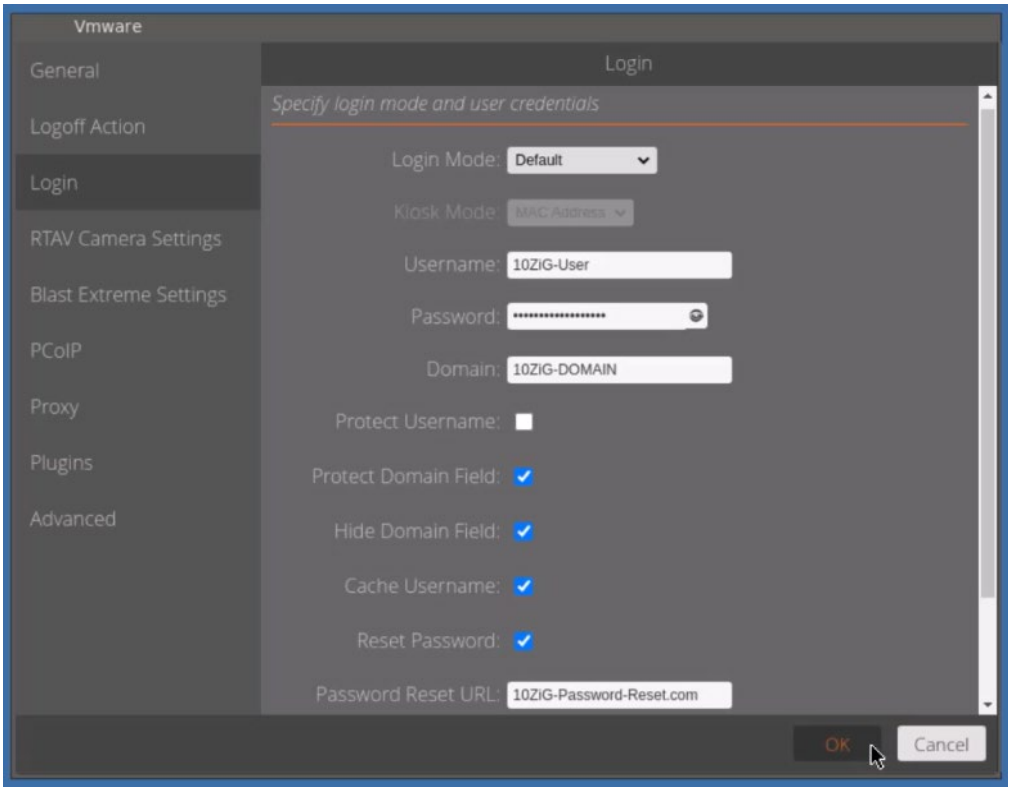
Notice that the Domain field is now presented as a drop down selection and cannot be typed into.

Enabling Password reset link and hiding the domain

Go into the “VMware 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.



Specify login mode and user credentials

Login Mode: Default

Kiosk Mode: MAC Address

Username: 10ZiG-User

Password: ••••••••••••••••••

Domain: 10ZiG-DOMAIN

Protect Username: ☐

Protect Domain Field: ☑

Hide Domain Field: ☑

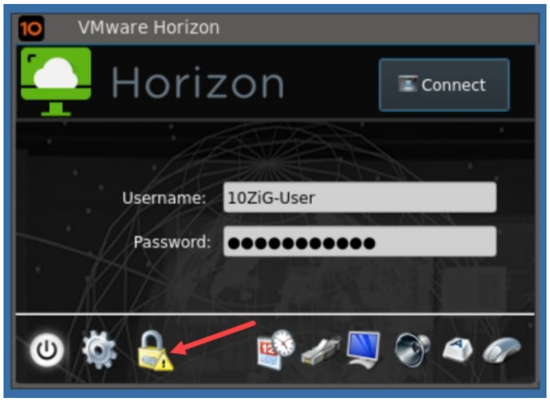
Cache Username: ☑

Reset Password: ☑

Password Reset URL: 10ZiG-Password-Reset.com

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”.



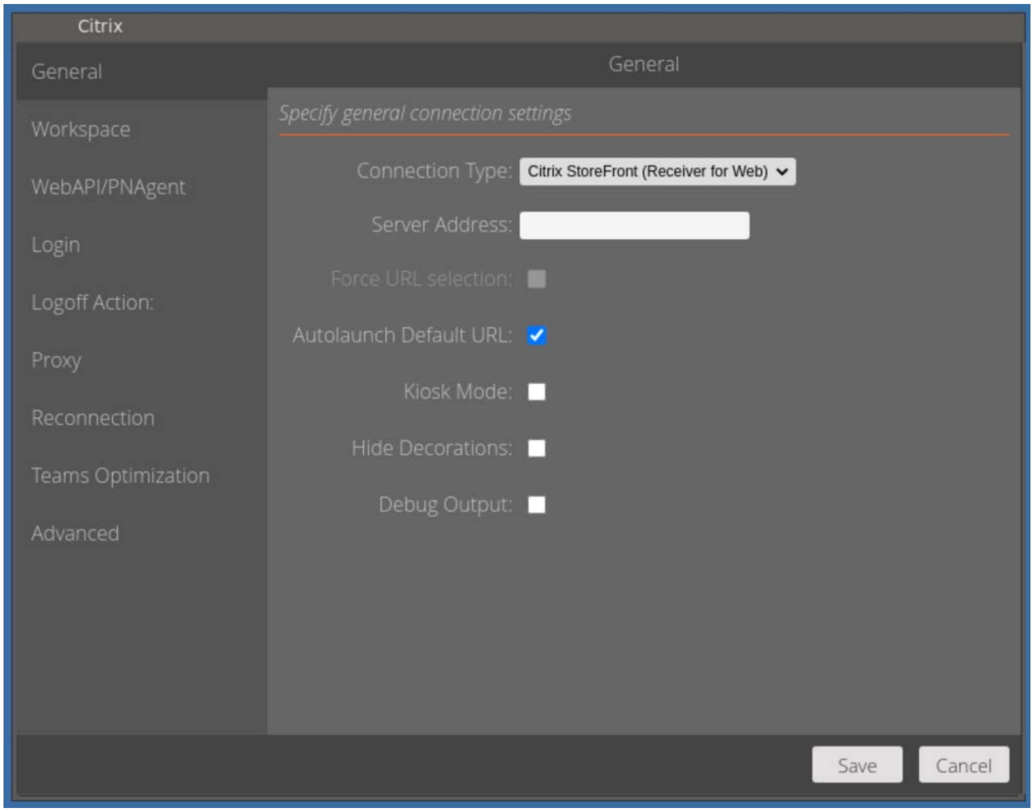
Username: 10ZiG-User

Password: ●●●●●●●●●●●●

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.



Specify general connection settings

Connection Type: Citrix StoreFront (Receiver for Web)

Server Address:

Force URL selection: ☐

Autolaunch Default URL: ☑

Kiosk Mode: ☐

Hide Decorations: ☐

Debug Output: ☐

- **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, Citrix Storefront Receiver for web(default) and Citrix Storefront WebAPI/PNAgent.

  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.

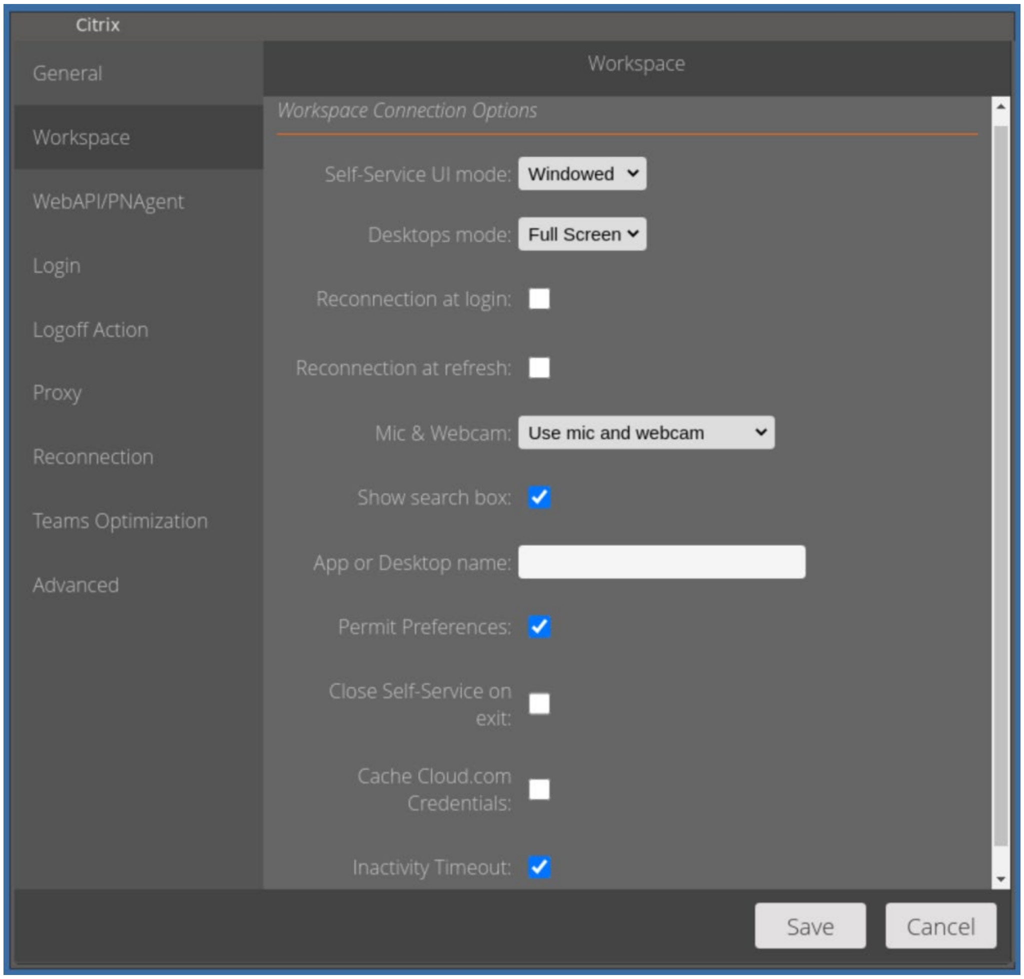
- **Kiosk Mode**: Enabling this option hides the local Thin Client desktop launchpad. This option should only be used with "Receiver for Web". Verify the launchpad is hidden when enabled. Note: Administrators can bring the launchpad back by pressing CTRL+ALT+M

- **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”.



Workspace Connection Options

Self-Service UI mode: Windowed

Desktops mode: Full Screen

Reconnection at login: □

Reconnection at refresh: □

Mic & Webcam: Use mic and webcam

Show search box: ☑

App or Desktop name:

Permit Preferences: ☑

Close Self-Service on exit: □

Cache Cloud.com Credentials: □

Inactivity Timeout: ☑

- **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.

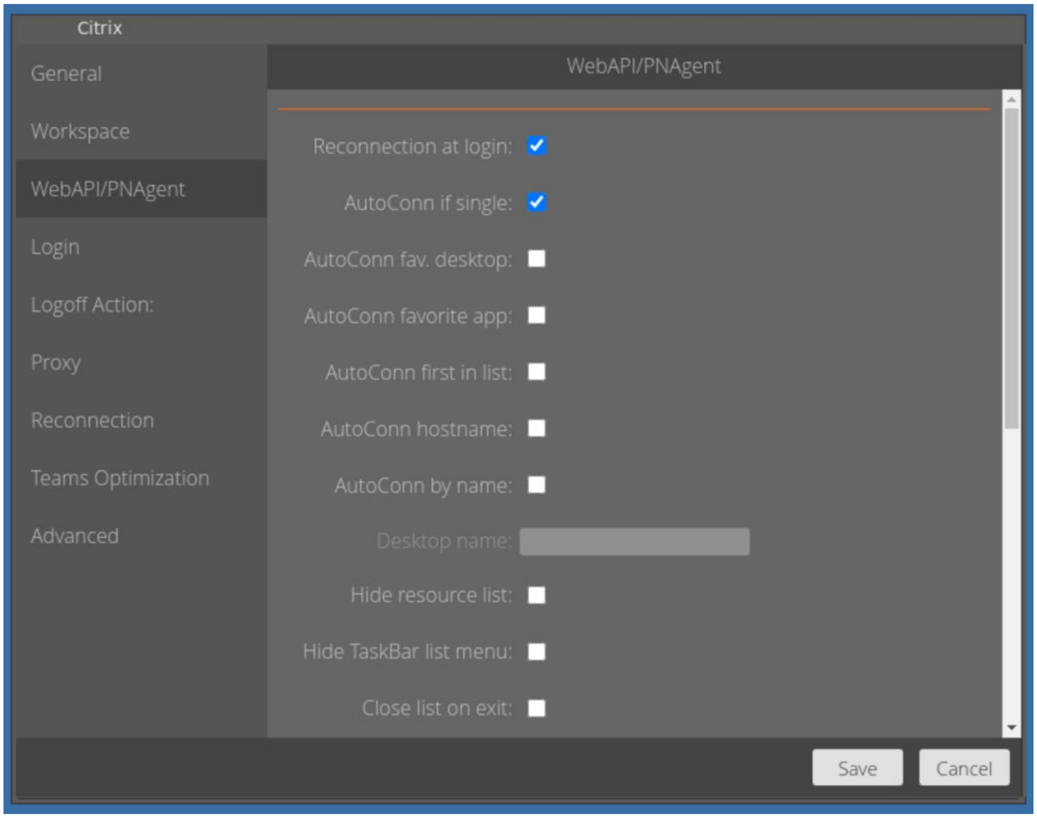
- **Close Self-Service on exit**: This will close the list of available Desktops/Applications when the user disconnects/logs off the session.

- **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”.



Reconnection at login: ☑
AutoConn if single: ☑
AutoConn fav. desktop: □
AutoConn favorite app: □
AutoConn first in list: □
AutoConn hostname: □
AutoConn by name: □
Desktop name:
Hide resource list: □
Hide TaskBar list menu: □
Close list on exit: □

- **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.

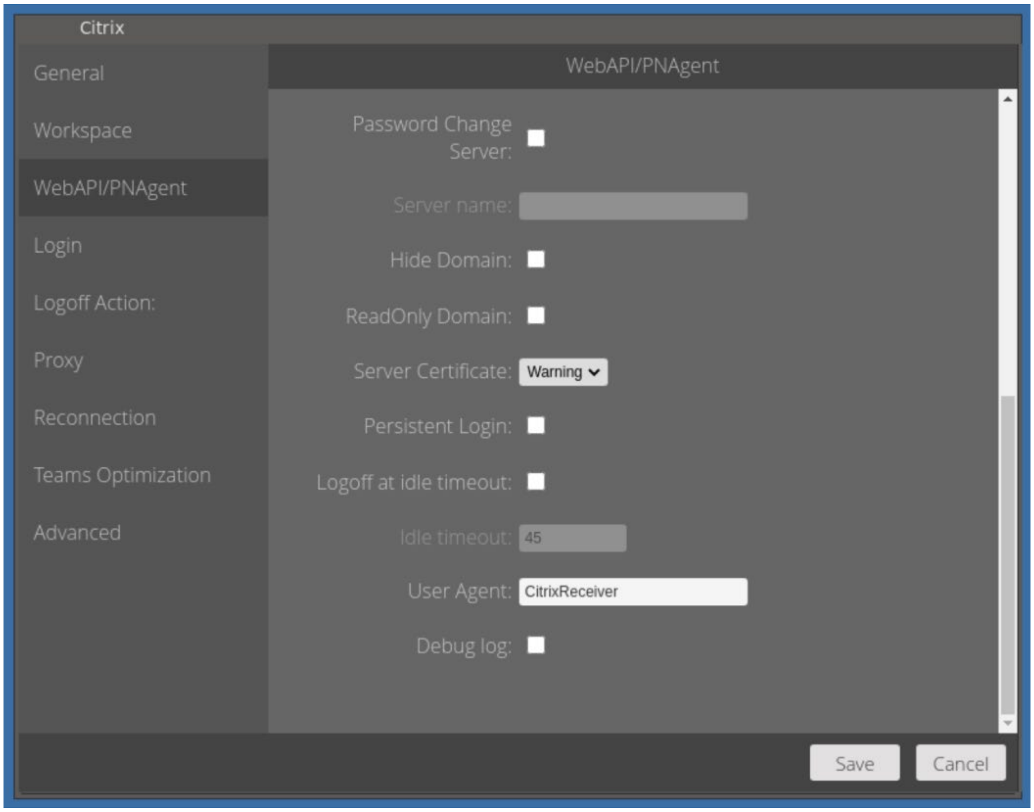
- **AutoConn by name**: This will enable automatic connection to the first desktop with a description that matches the specific string in the “Desktop name” field below it.

- **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)

- **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: □

Server name:

Hide Domain: □

ReadOnly Domain: □

Server Certificate: Warning

Persistent Login: □

Logoff at idle timeout: □

Idle timeout: 45

User Agent: CitrixReceiver

Debug log: □

- **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.

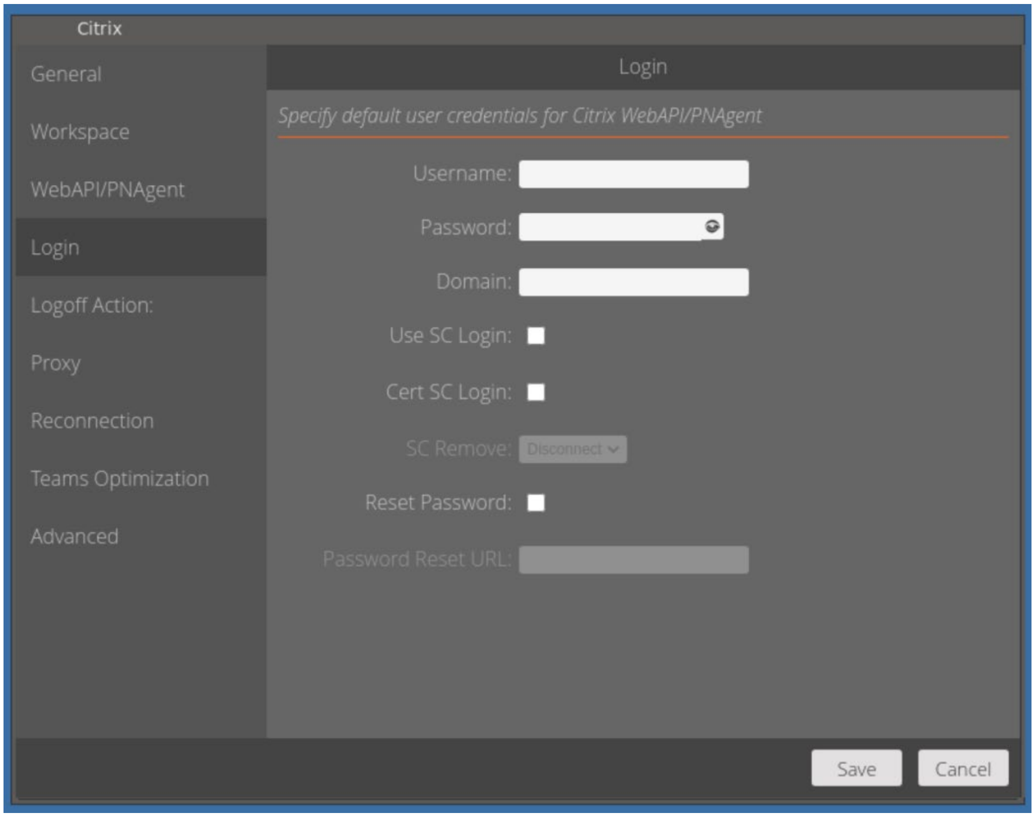
- **Idle timeout**: This is the amount of idle time before desktop logoff in minutes. The "Logoff at idle timeout" field above needs to be enabled for this to be available.

- **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.



Login

Specify default user credentials for Citrix WebAPI/PNAgent

Username:

Password:

Domain:

Use SC Login: □

Cert SC Login: □

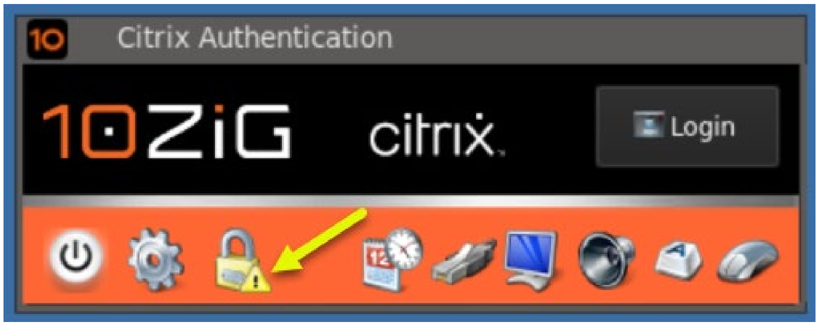
SC Remove: Disconnect

Reset Password: □

Password Reset URL:

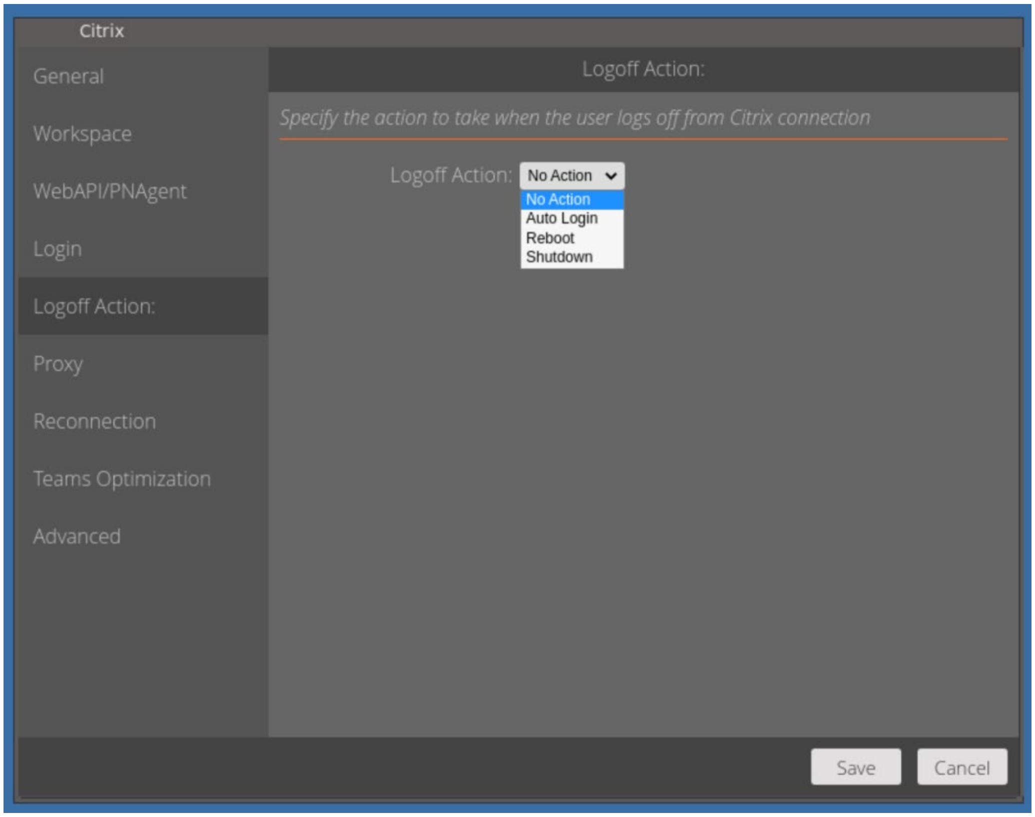
- **Username, Password and Domain**: These are the credentials that match your specific environment.
- **Use SC Login**: Enable this setting to allow use of Smart Card login. This option will not work when using an actual smart card with user certificates installed (if your smartcard requires a PIN to 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 yellow arrow in the image below.



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”.

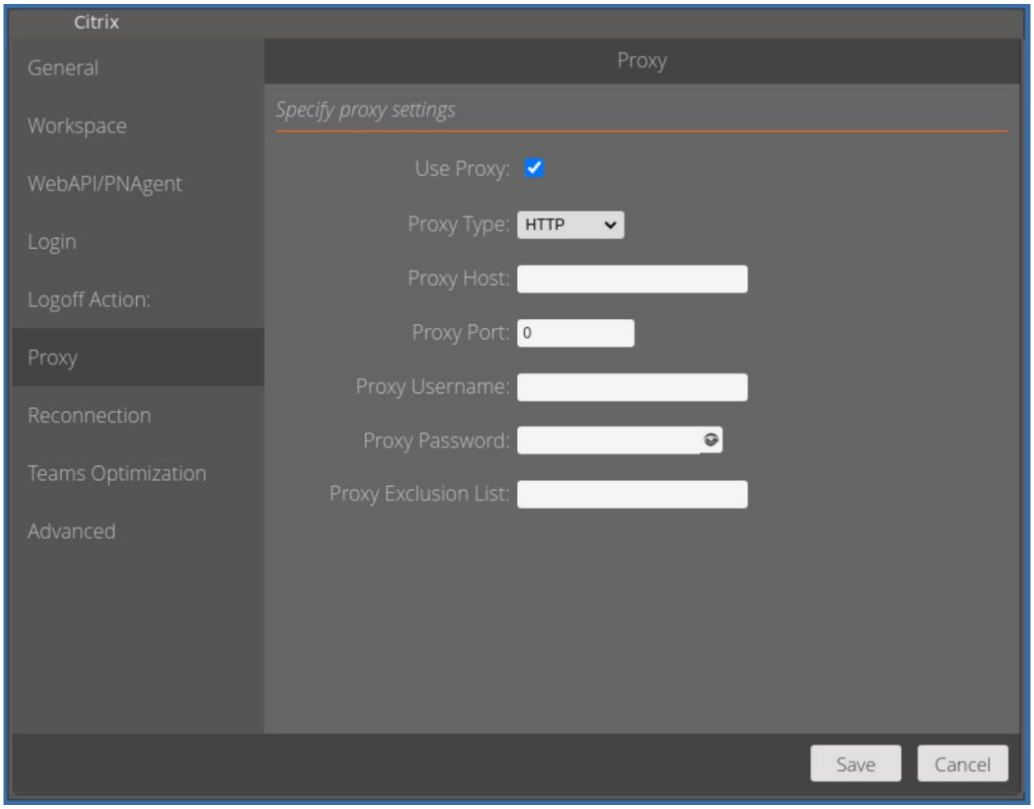


Specify the action to take when the user logs off from Citrix connection

Logoff Action: No Action

Proxy

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



Specify proxy settings

Use Proxy: ☑

Proxy Type: HTTP

Proxy Host:

Proxy Port: 0

Proxy Username:

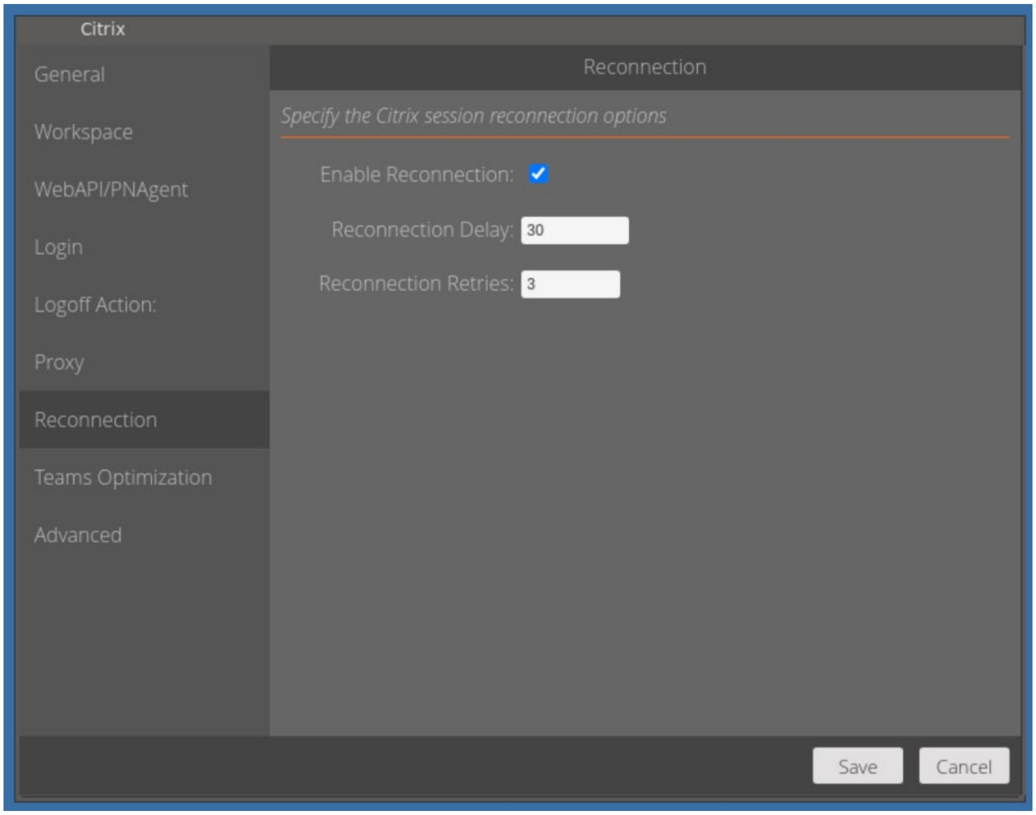
Proxy Password:

Proxy Exclusion List:

- **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.



Specify the Citrix session reconnection options

Enable Reconnection: ☑

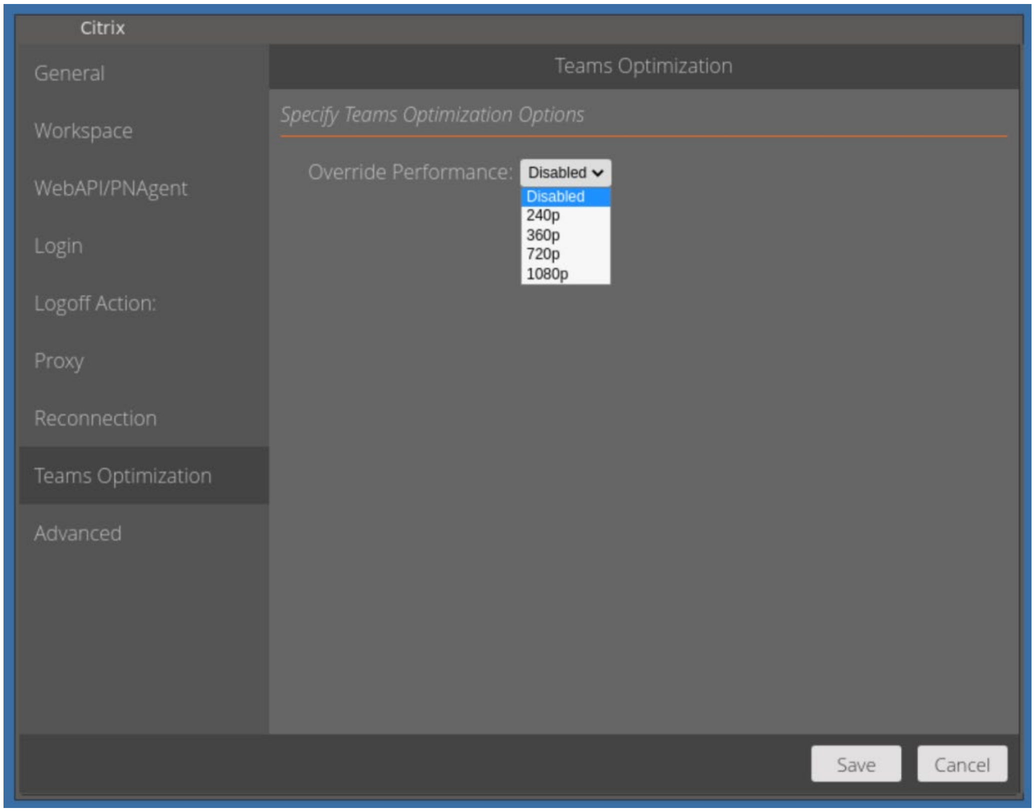
Reconnection Delay: 30

Reconnection Retries: 3

- **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.



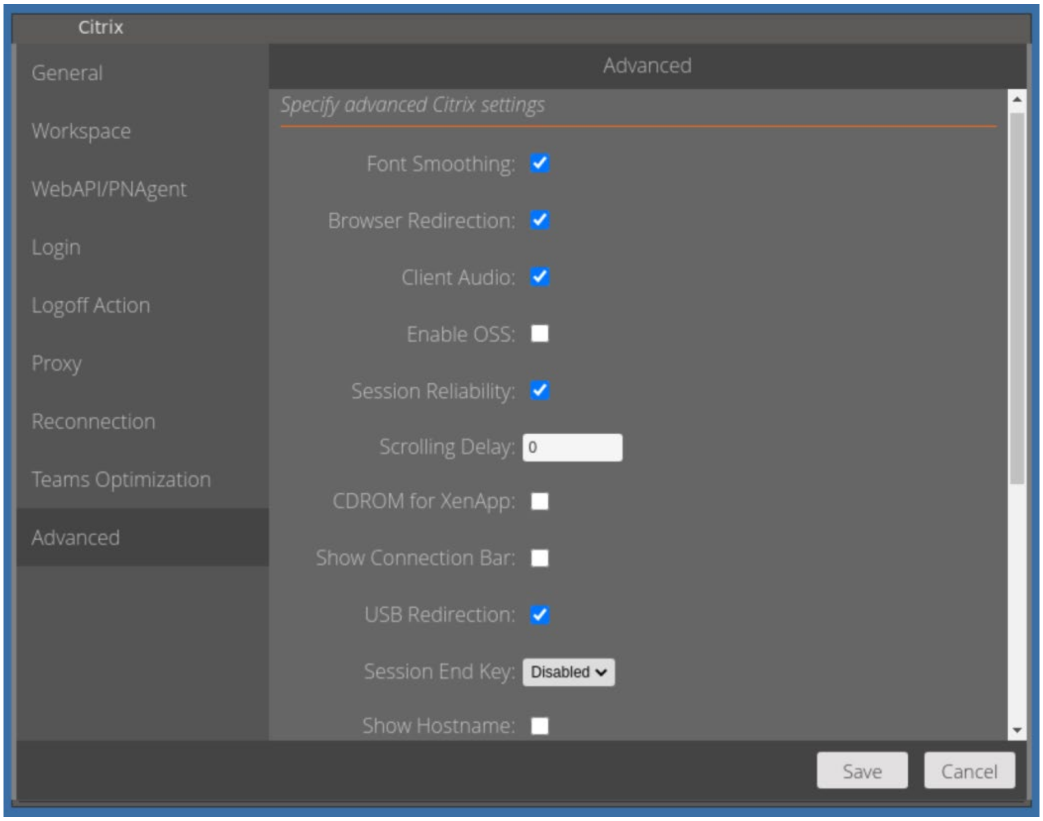
Override Performance: Disabled

- **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.



Advanced

Specify advanced Citrix settings

Font Smoothing: ☑

Browser Redirection: ☑

Client Audio: ☑

Enable OSS: □

Session Reliability: ☑

Scrolling Delay: 0

CDROM for XenApp: □

Show Connection Bar: □

USB Redirection: ☑

Session End Key: Disabled

Show Hostname: □

- **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.

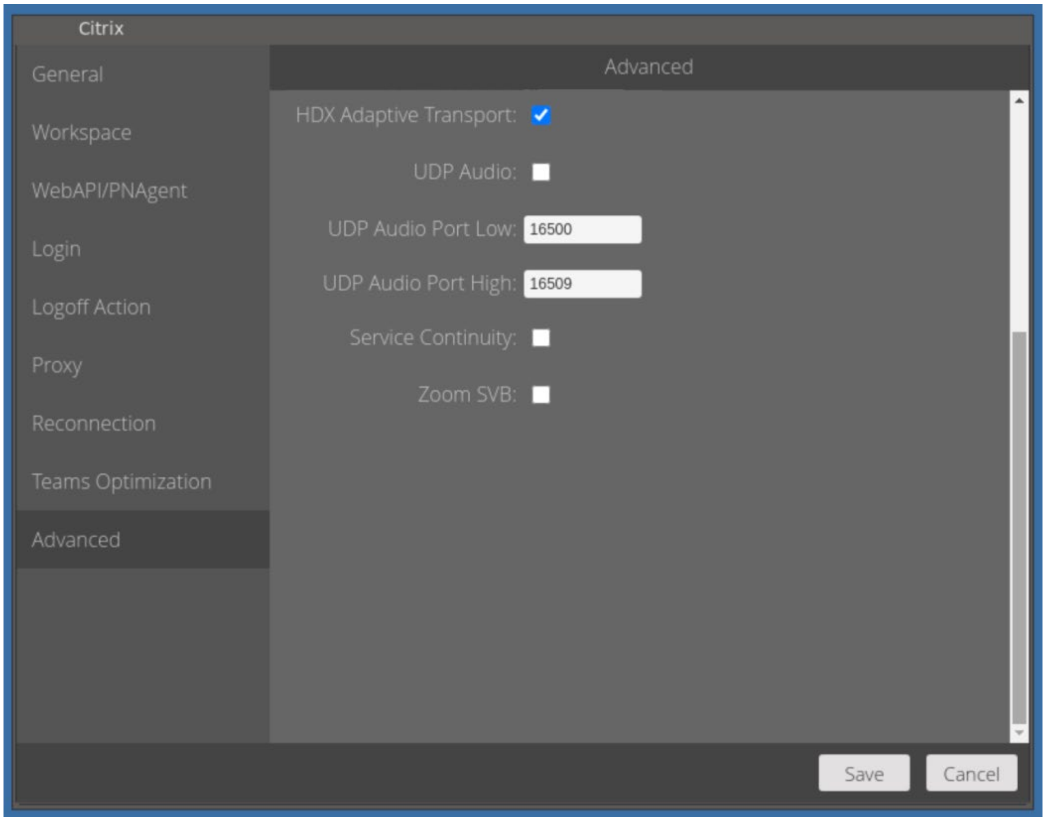
- **CDROM for XenAPP:** Allow automatic connection of CD-ROM drives.

- **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.



HDX Adaptive Transport: ☑

UDP Audio: □

UDP Audio Port Low: 16500

UDP Audio Port High: 16509

Service Continuity: □

Zoom SVB: □

- **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.

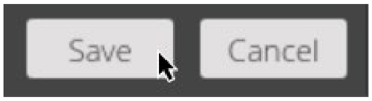
- **UDP Audio Ports Low and High range:** The Audio UDP port range specifies the range of port numbers that the Windows VDA uses to exchange audio packet data with the user device. By default, the range is 16500 through 16509.

- **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 for performance devices due to the resources this requires.

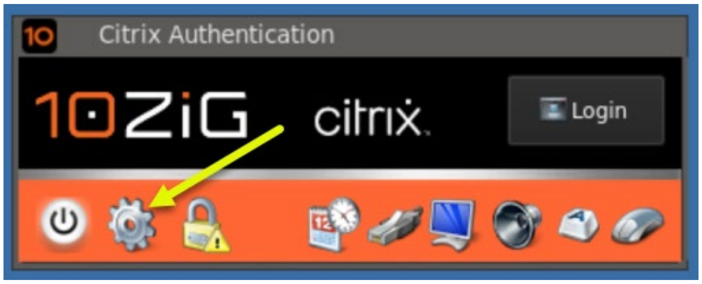
Saving your settings

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.

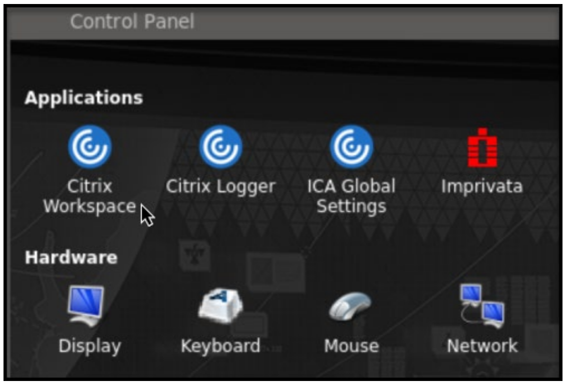


Editing your connection settings

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 "yellow arrow" below.



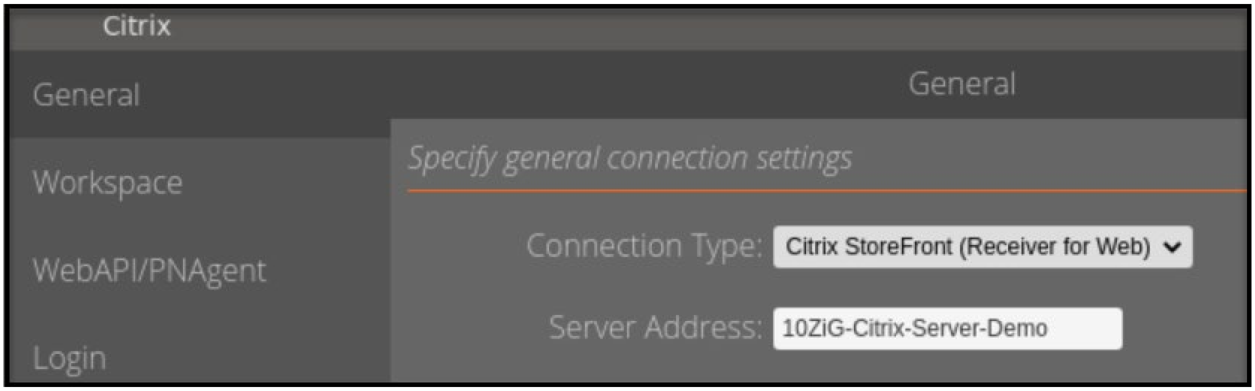
You'll be taken back into the "Control Panel", where you can click the "Citrix Workspace" icon in the top left and then make changes as outlined in the previous sections of this guide.



Citrix Connection Examples

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

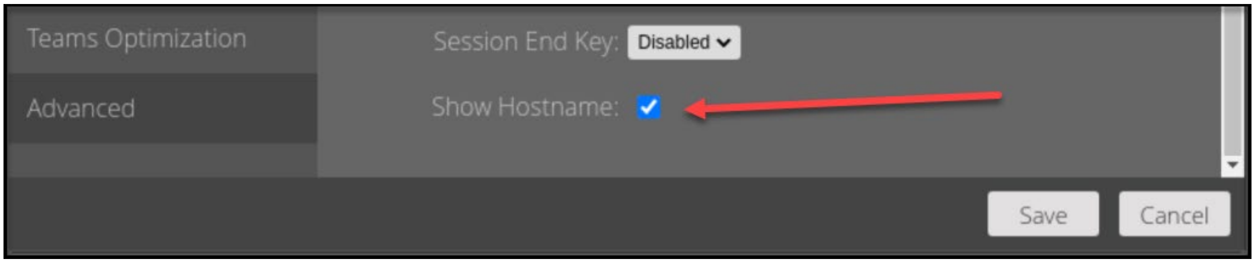
Inside the settings menu, select "General" menu option, select the "Connection type" to be Citrix StoreFront(Receiver for Web) and key in the Server Address.



Connection Type: Citrix StoreFront (Receiver for Web)

Server Address: 10ZiG-Citrix-Server-Demo

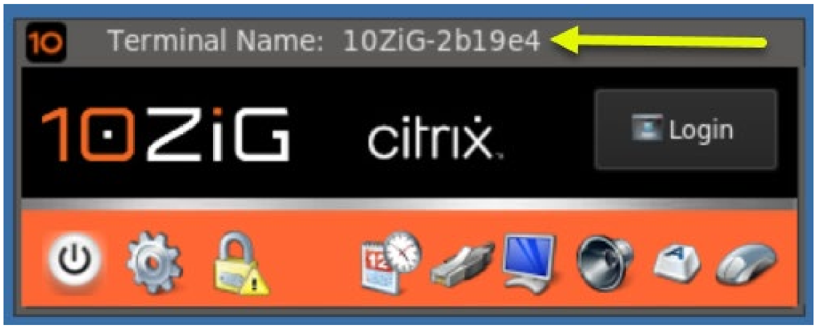
Next, we're going to enable the client hostname to be displayed on the "Launchpad". Click on the "Advanced" menu option and then scroll down to "Show Hostname" setting, as shown by the red arrow below.



Session End Key: Disabled

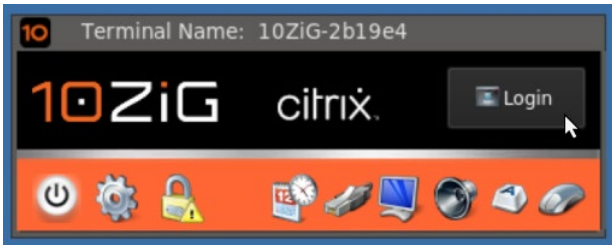
Show Hostname: ☑

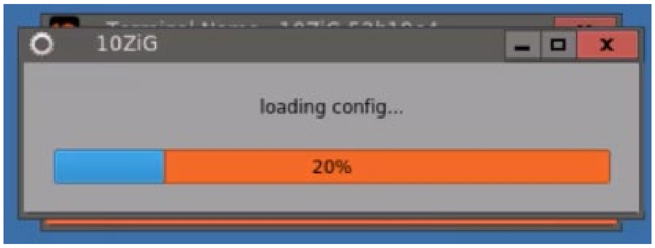
Tick this box, click "SAVE" in the bottom right and then close the "Control Panel". Your login box should now display the hostname of your Thin Client as below.

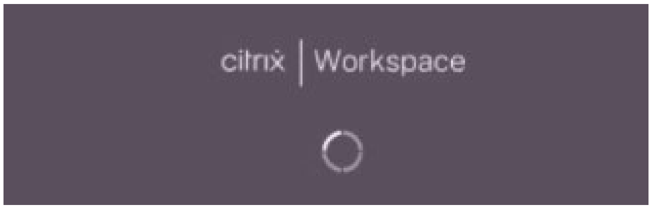


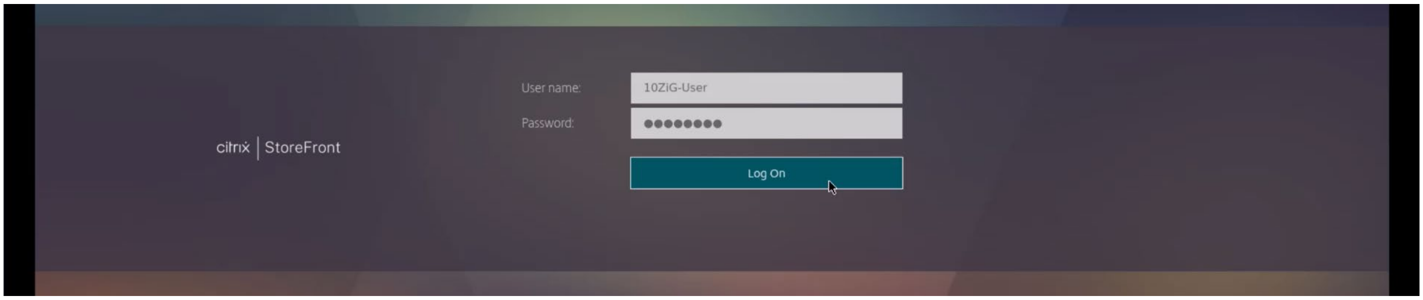
Terminal Name: 10ZiG-2b19e4

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 :-









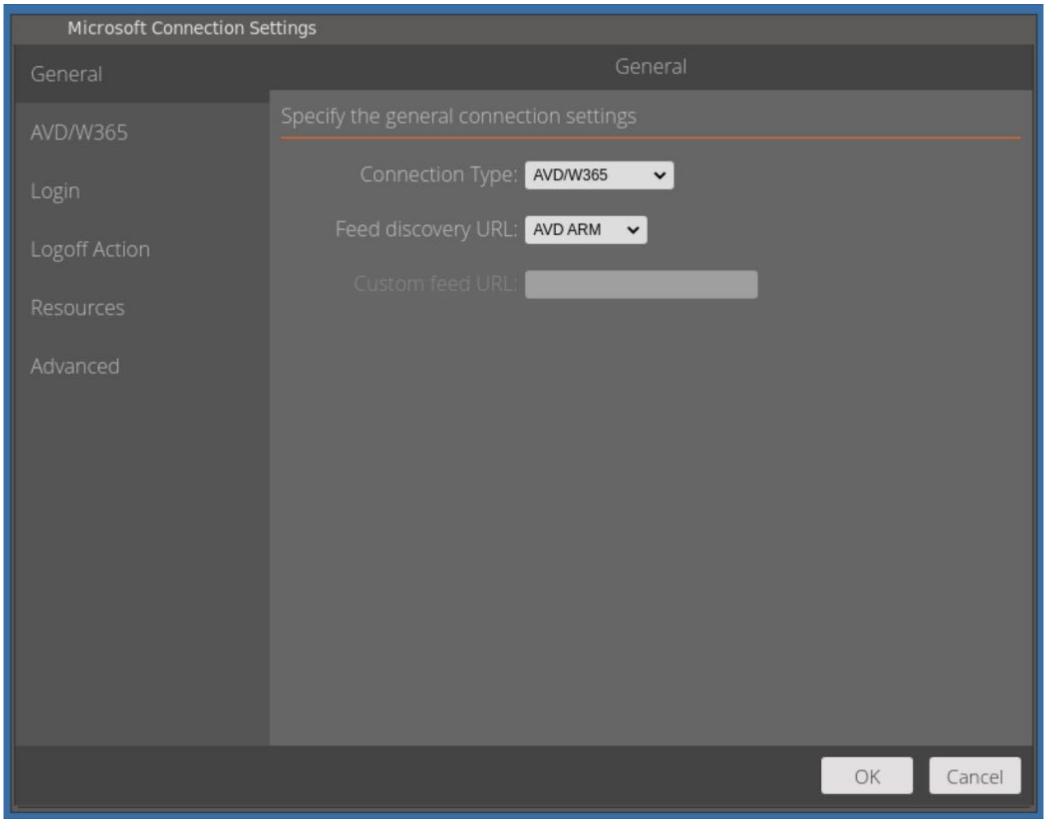
User name: 10ZiG-User

Password: ●●●●●●●●

NOS for Microsoft NOS-M

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

General



Specify the general connection settings

Connection Type: AVD/W365

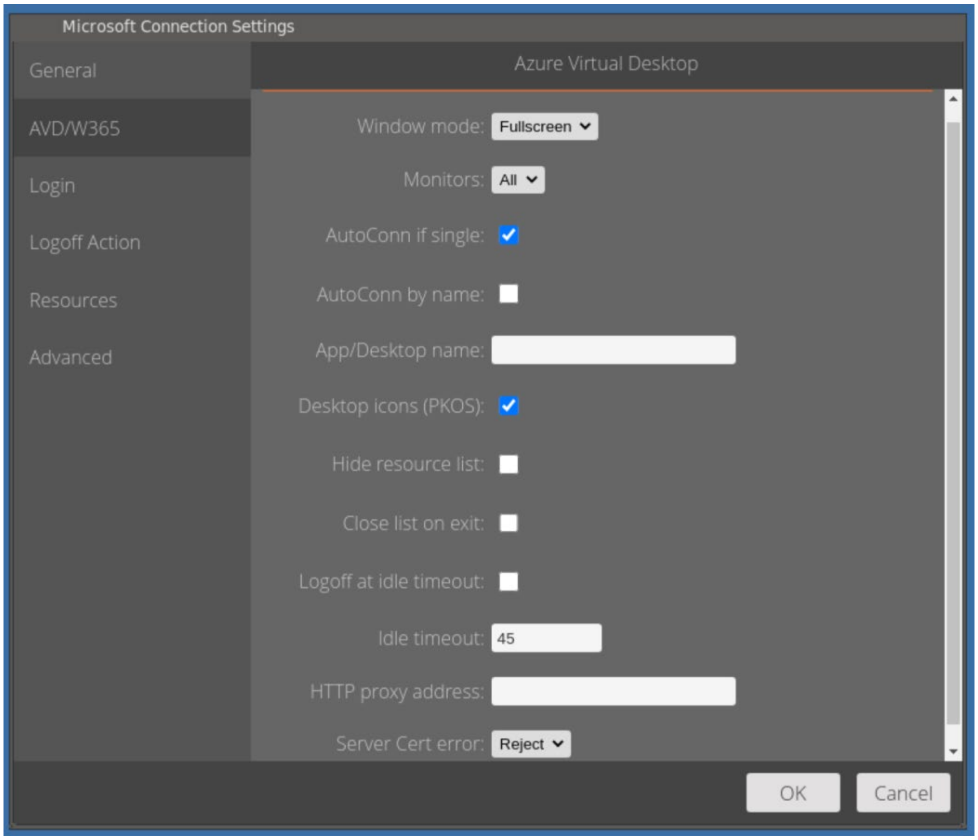
Feed discovery URL: AVD ARM

Custom feed URL:

- **Connection Type:** There are 3 available that include Azure Virtual Desktop(AVD) that also includes connections to Windows 365 Cloud PC, 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”.

AVD/W365



Azure Virtual Desktop

Window mode: Fullscreen

Monitors: All

AutoConn if single: ☑

AutoConn by name: □

App/Desktop name:

Desktop icons (PKOS): ☑

Hide resource list: □

Close list on exit: □

Logoff at idle timeout: □

Idle timeout: 45

HTTP proxy address:

Server Cert error: Reject

- **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.

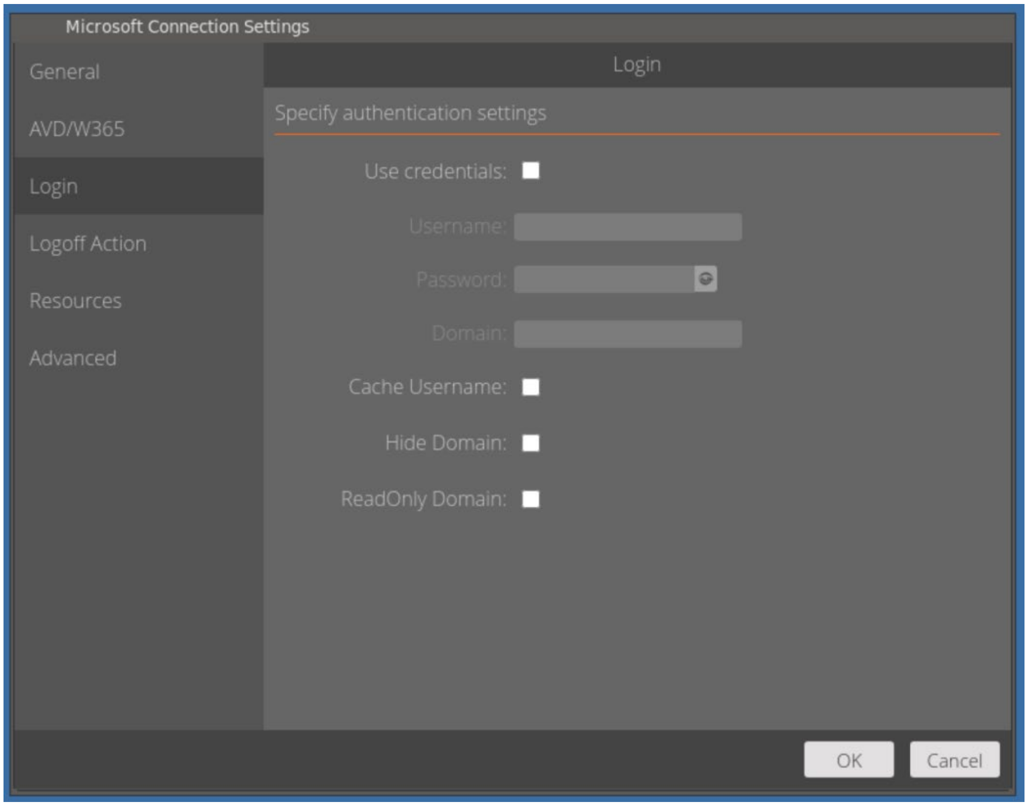
- **Logoff at idle timeout**: Enable this option to log users off from their Azure Virtual Desktop session automatically where idle timeout occurs.

- **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



Microsoft Connection Settings

Login

Specify authentication settings

Use credentials: □

Username:

Password:

Domain:

Cache Username: □

Hide Domain: □

ReadOnly Domain: □

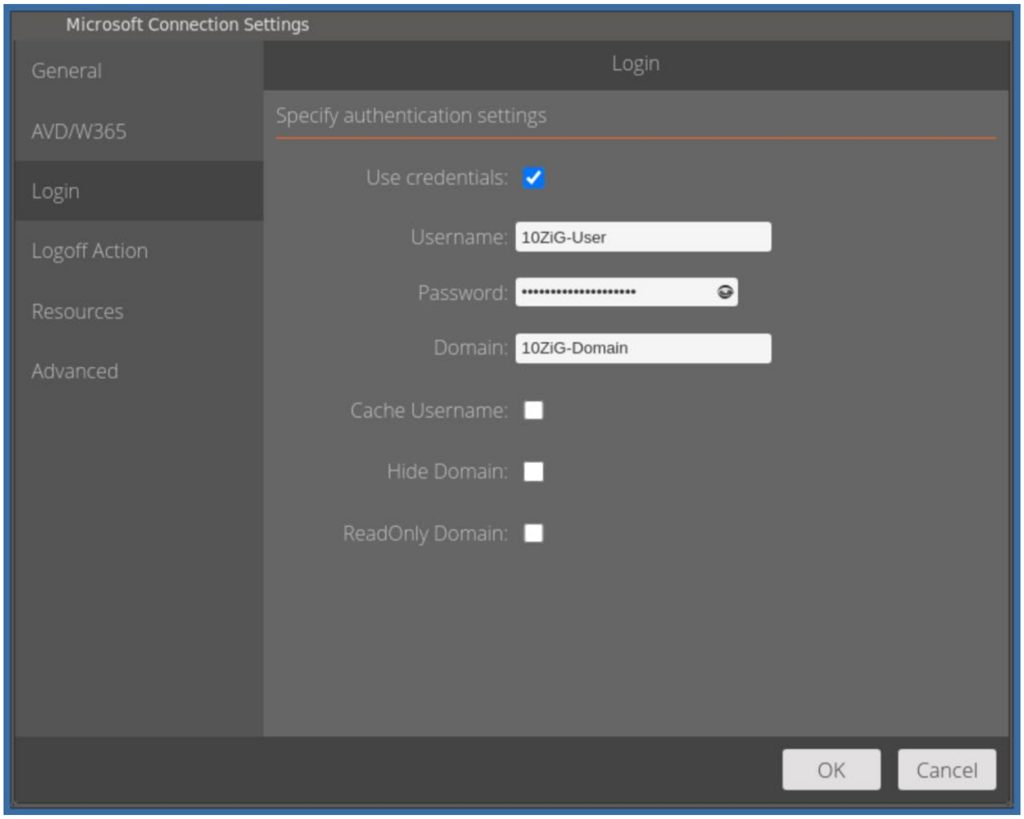
- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **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.

Example of Cached login details



Microsoft Connection Settings

Login

Specify authentication settings

Use credentials: ☑

Username: 10ZiG-User

Password: ••••••••••••••••••••

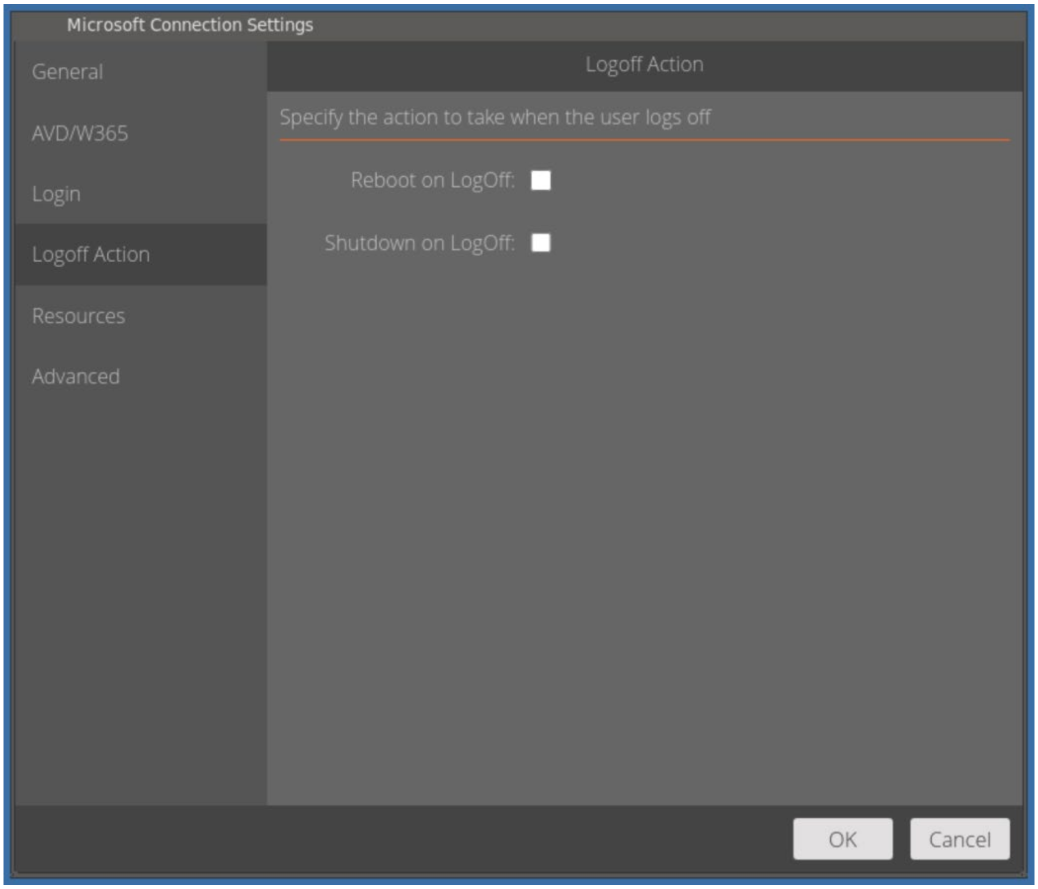
Domain: 10ZiG-Domain

Cache Username: □

Hide Domain: □

ReadOnly Domain: □

Logoff Action



Logoff Action

Specify the action to take when the user logs off

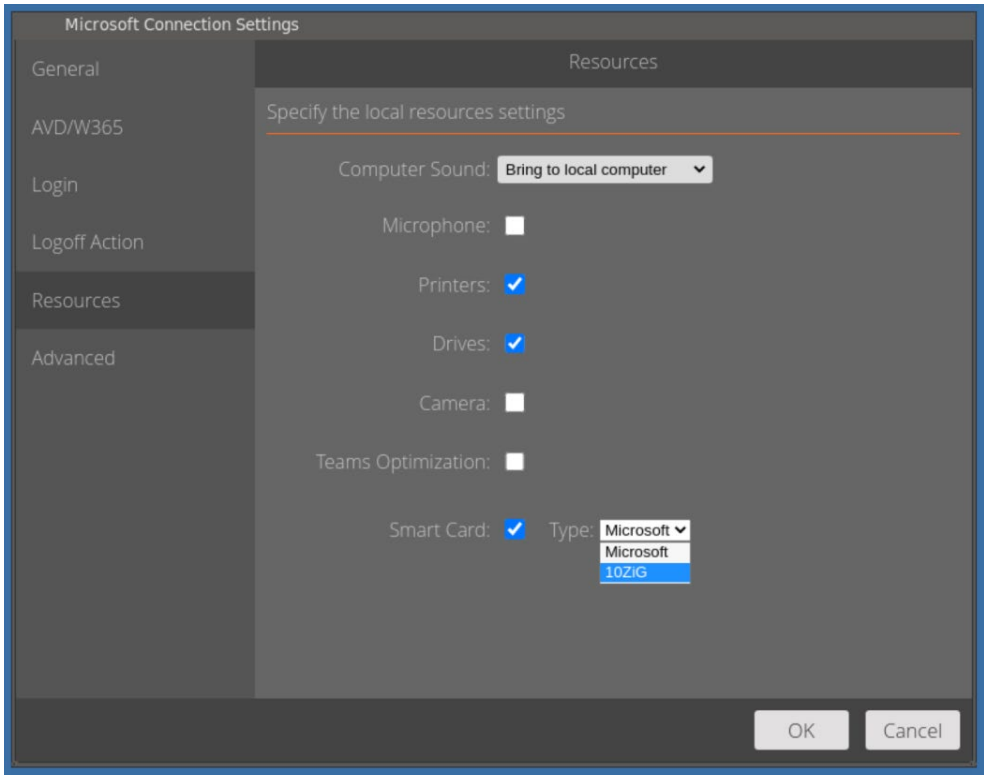
Reboot on LogOff: □

Shutdown on LogOff: □

- **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



Microsoft Connection Settings

Resources

Specify the local resources settings

Computer Sound: Bring to local computer

Microphone: □

Printers: ☑

Drives: ☑

Camera: □

Teams Optimization: □

Smart Card: ☑ Type: Microsoft

- **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.

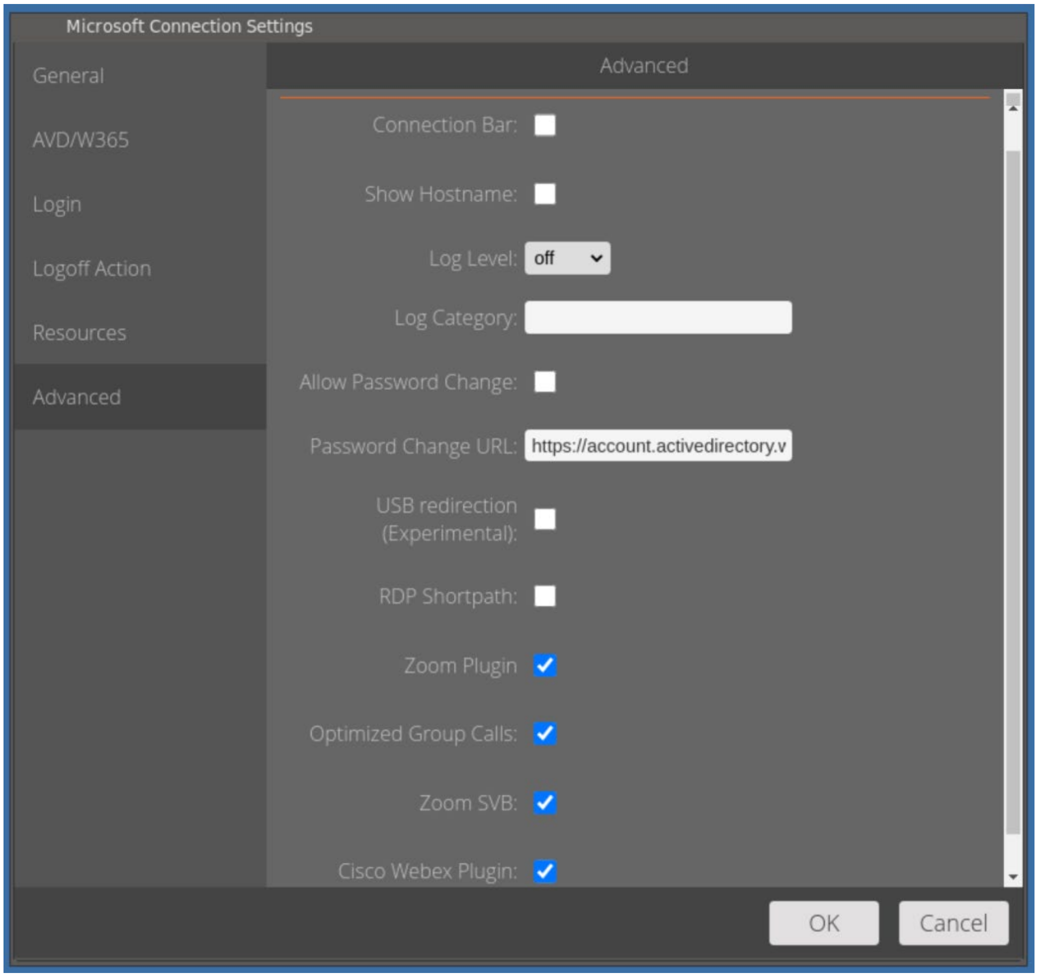
- **Drives**: Enabling this option will enable Client Drive Redirection (Mass Storage Only).

- **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 redirection of Smart Cards into your Azure Virtual Desktops. Select your card “Type” from the drop down menu on the right.

Advanced



Connection Bar: □

Show Hostname: □

Log Level: off

Log Category:

Allow Password Change: □

Password Change URL: https://account.activedirectory.v

USB redirection (Experimental): □

RDP Shortpath: □

Zoom Plugin ☑

Optimized Group Calls: ☑

Zoom SVB: ☑

Cisco Webex Plugin: ☑

- **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.

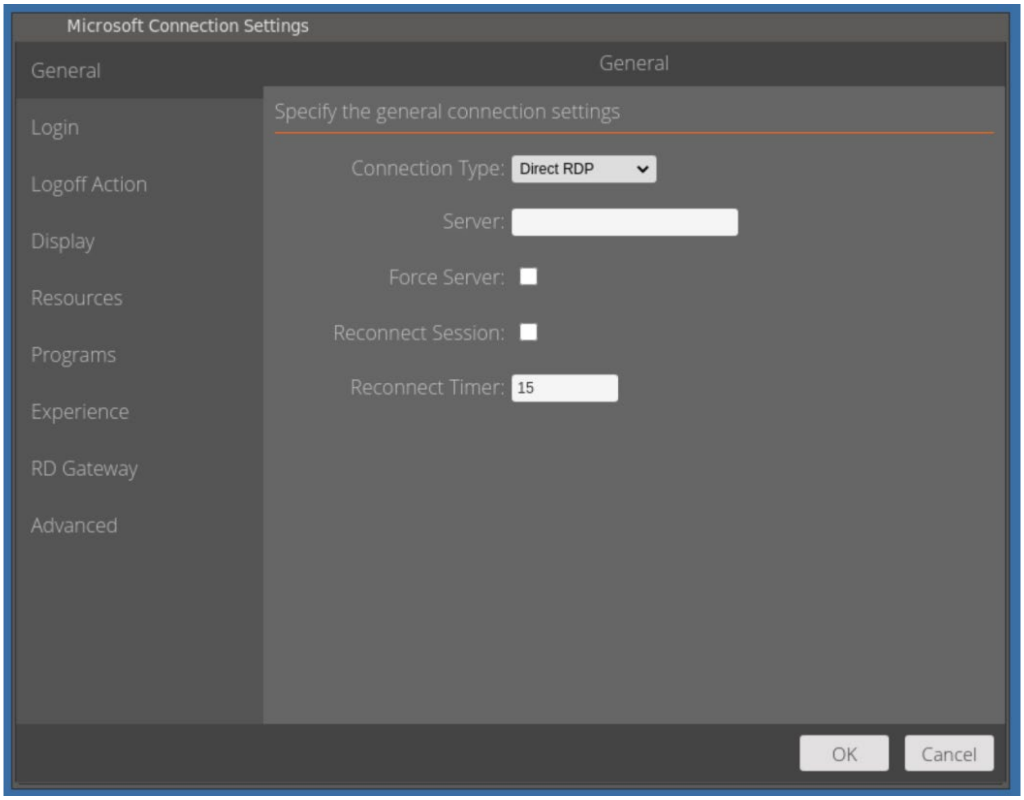
- **Optimized Group Calls**: This option can negotiate “optimized” bandwidth that helps to fix black video stream during group calls.

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

- **Cisco Webex Plugin**: Enable this option to allow user to access the Webex app functionality inside the virtual desktop.

Direct RDP

General



General

Specify the general connection settings

Connection Type: Direct RDP

Server:

Force Server: □

Reconnect Session: □

Reconnect Timer: 15

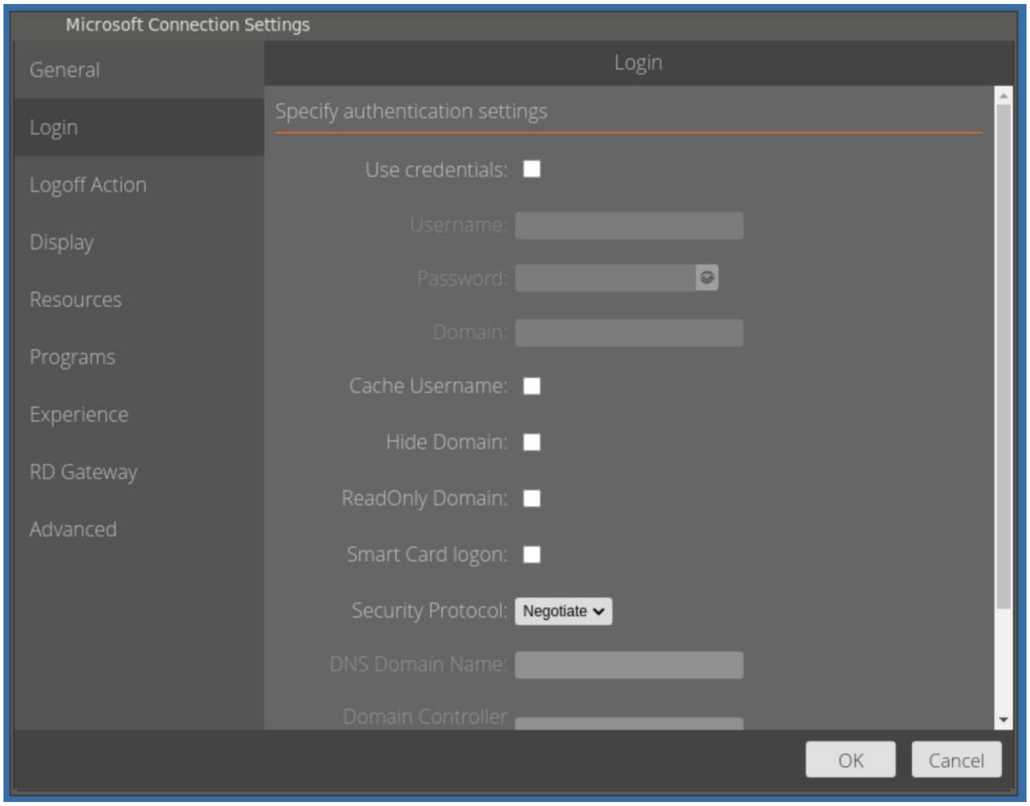
- **Server**: This is where you can enter a single server or multiple URL addresses of the remote desktop connection broker. If multiples are used, then they should be comma separated.

- **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.

Login



Specify authentication settings

Use credentials: □

Username:

Password:

Domain:

Cache Username: □

Hide Domain: □

ReadOnly Domain: □

Smart Card logon: □

Security Protocol: Negotiate

DNS Domain Name:

Domain Controller

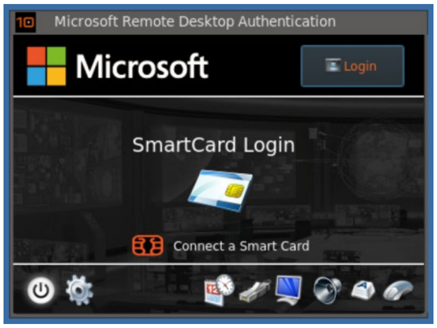
- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **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:** 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.



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

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

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

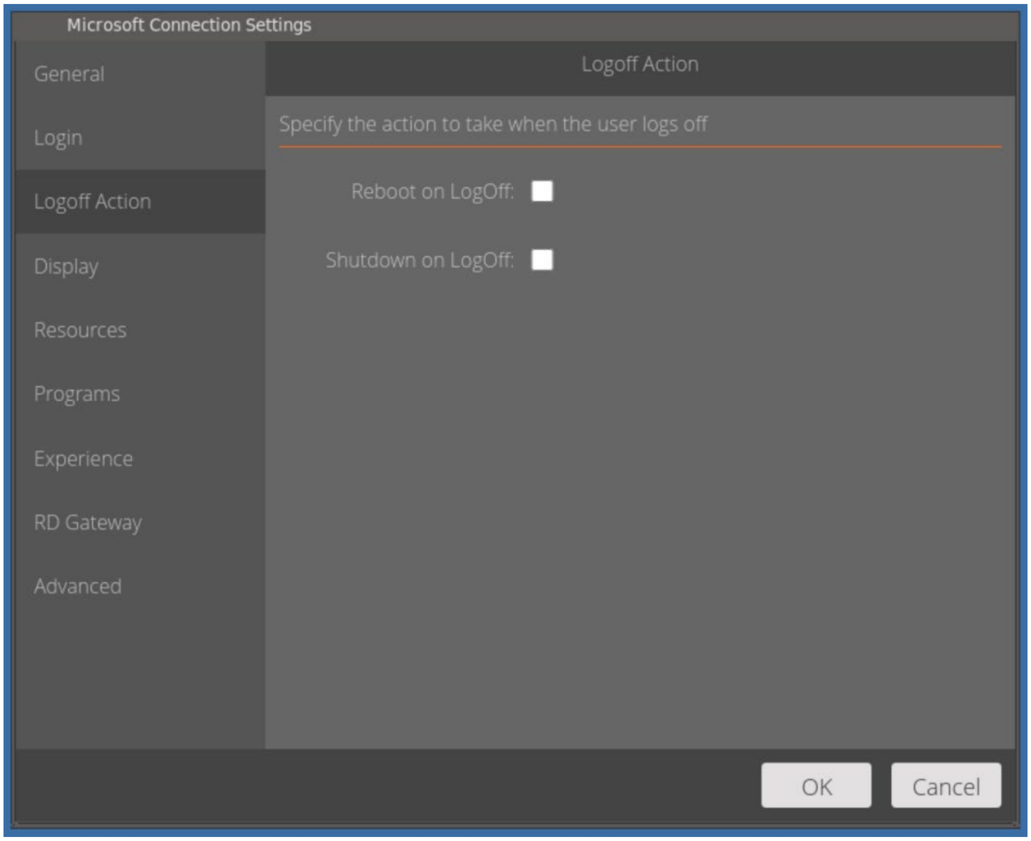
- **Domain Controller FQDN:** This is the fully qualified domain name of the domain controller on your network. You can supply multiple domain controllers by separating them with commas.

- **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”.

Logoff Action



Logoff Action

Specify the action to take when the user logs off

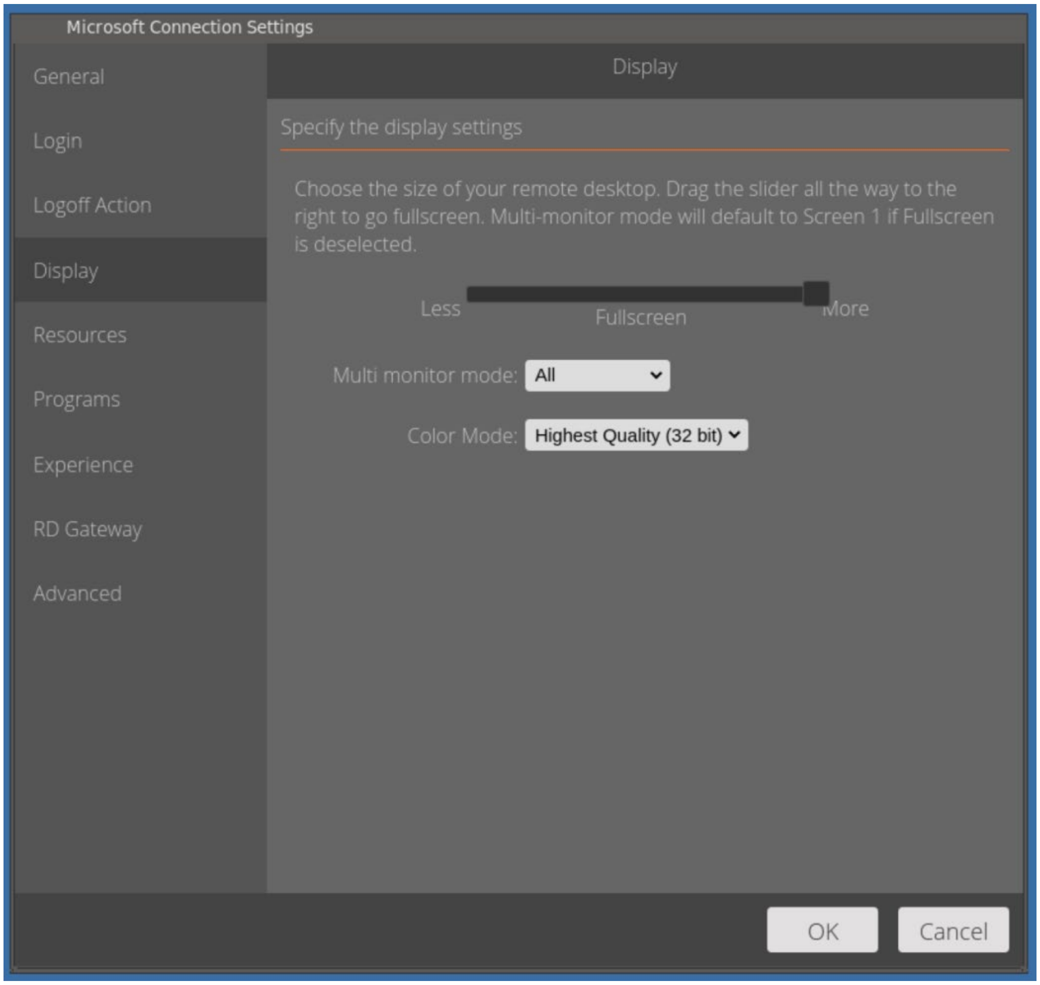
Reboot on LogOff: □

Shutdown on LogOff: □

- **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



Specify the display settings

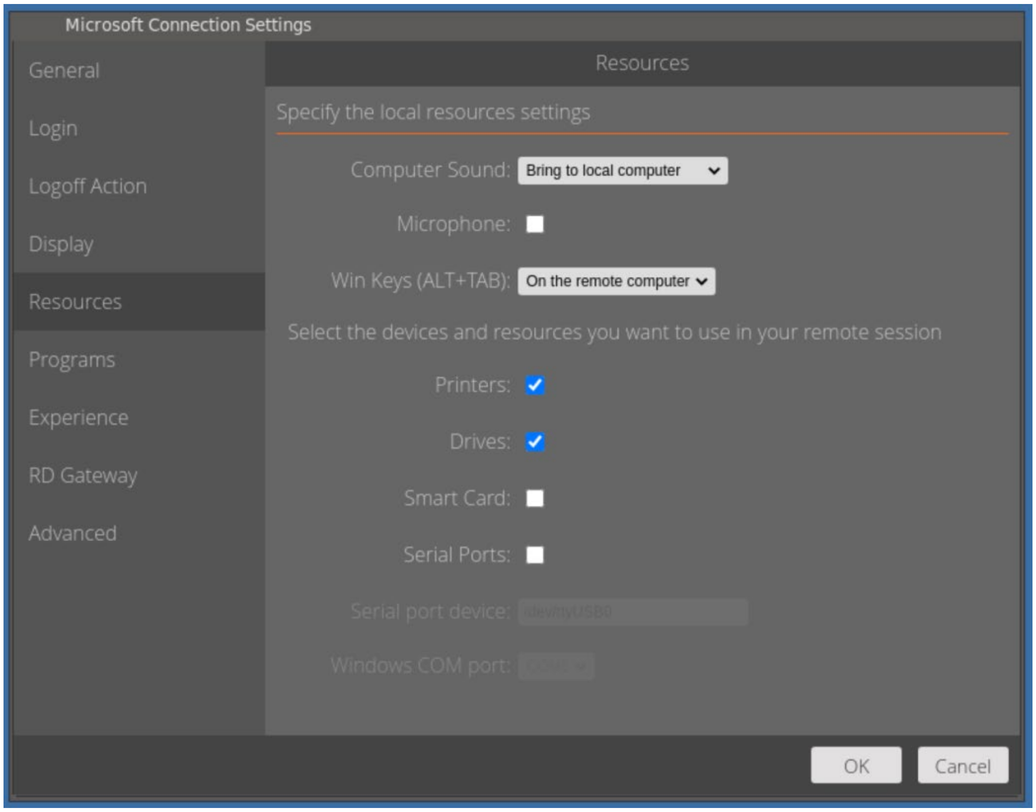
Choose the size of your remote desktop. Drag the slider all the way to the right to go fullscreen. Multi-monitor mode will default to Screen 1 if Fullscreen is deselected.

Multi monitor mode: All

Color Mode: Highest Quality (32 bit)

- **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



Resources

Specify the local resources settings

Computer Sound: Bring to local computer

Microphone: □

Win Keys (ALT+TAB): On the remote computer

Select the devices and resources you want to use in your remote session

Printers: ☑

Drives: ☑

Smart Card: □

Serial Ports: □

Serial port device: /dev/ttyUSB0

Windows COM port: COM1

- **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.

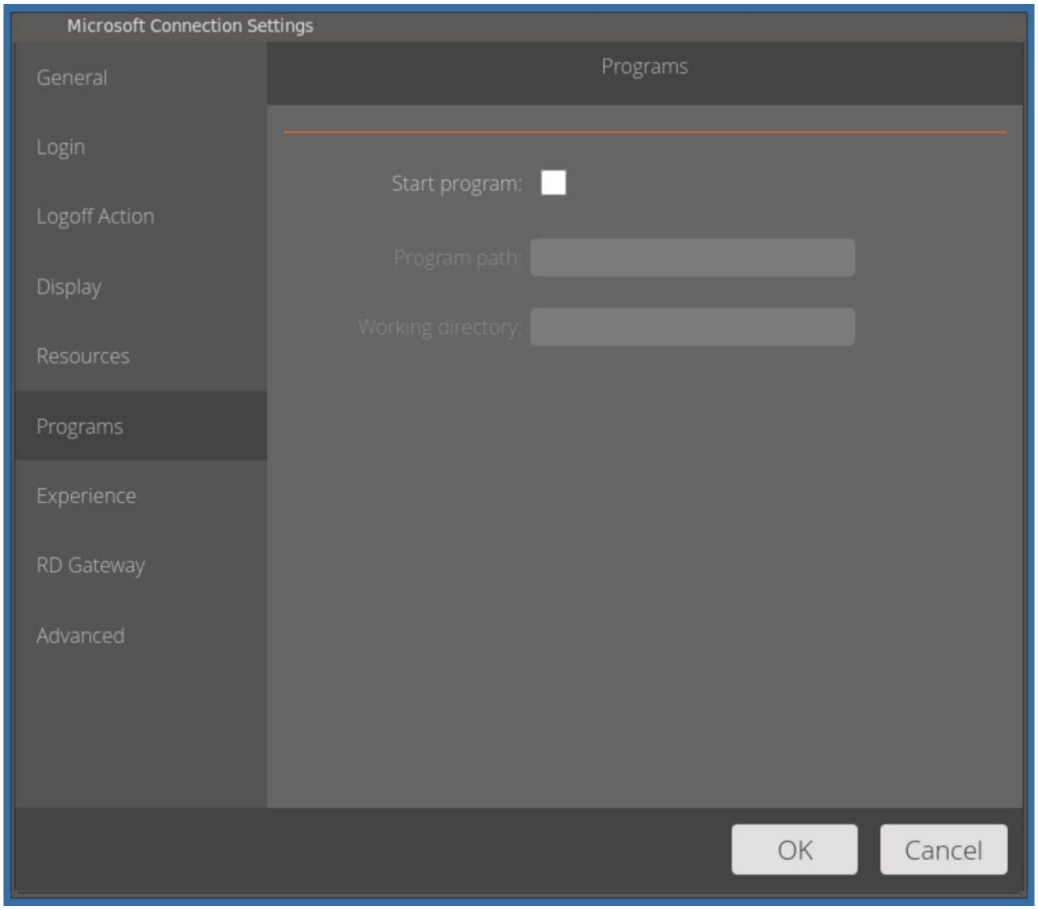
- **Printers:** Enabling this option will enable you to attach a local printer to the Thin Client and then print to it from within the VDI desktop.

- **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.

Programs

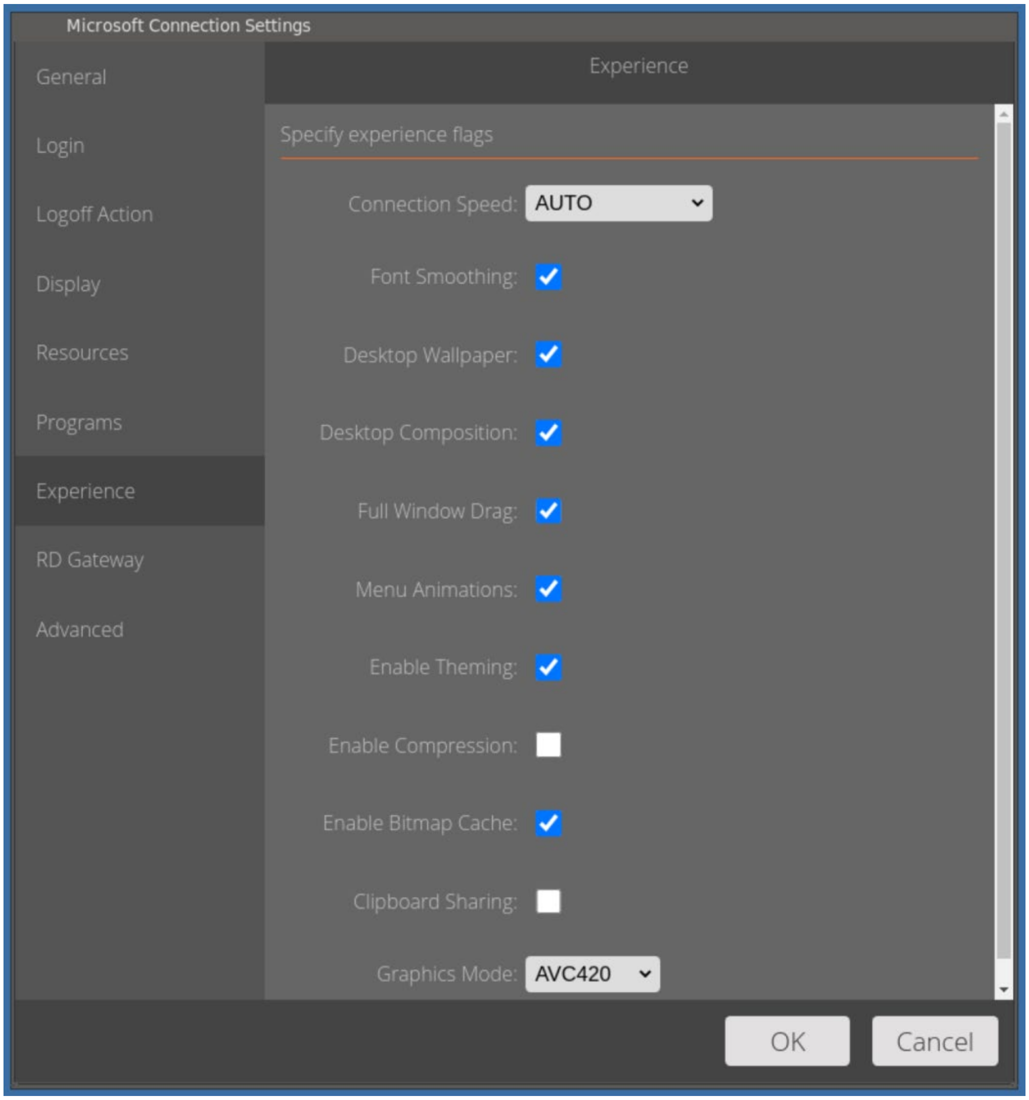


- **Start program:** When enabled, the Program path, and Working directory fields are available to be set below this field.

- **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



Experience

Specify experience flags

Connection Speed: AUTO

Font Smoothing: ☑

Desktop Wallpaper: ☑

Desktop Composition: ☑

Full Window Drag: ☑

Menu Animations: ☑

Enable Theming: ☑

Enable Compression: □

Enable Bitmap Cache: ☑

Clipboard Sharing: □

Graphics Mode: AVC420

- **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.

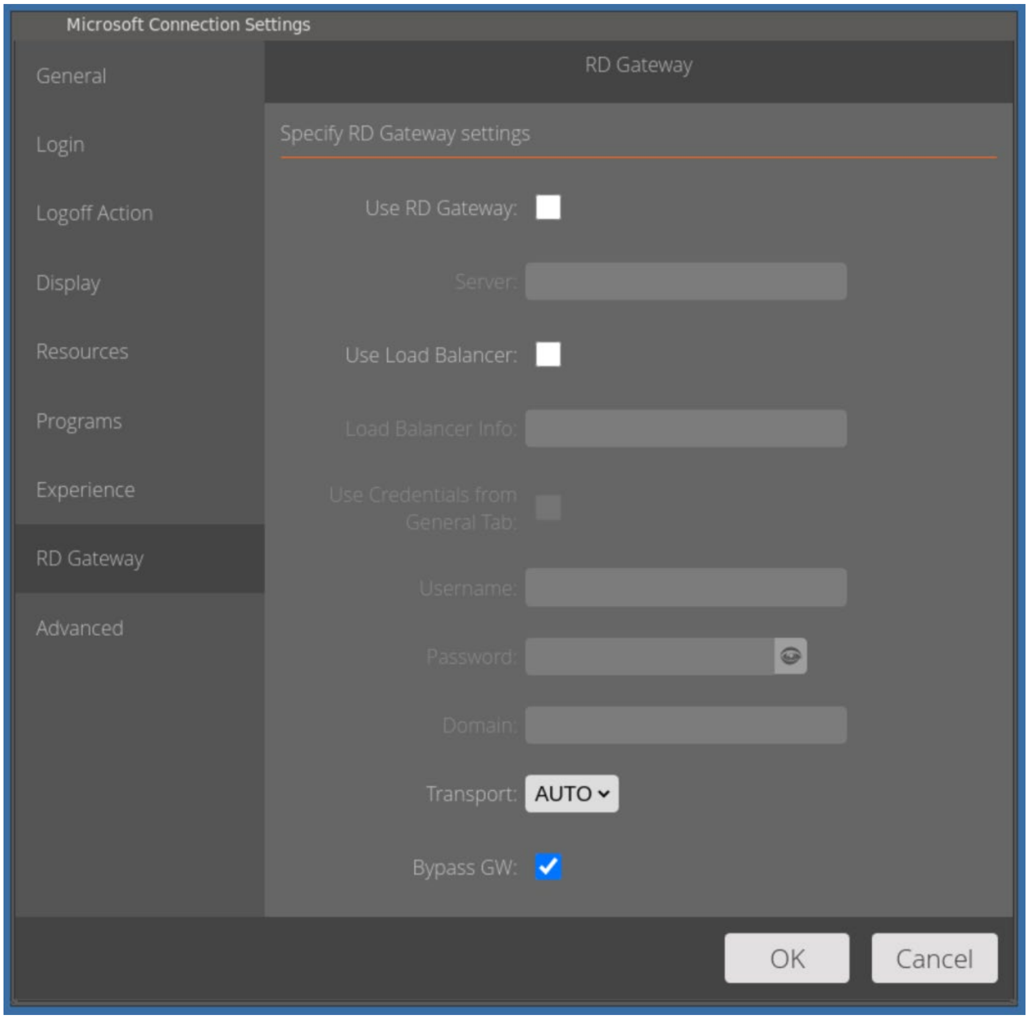
- **Enable Compression:** Determines whether bulk compression is enabled when it's transmitted by RDP to the local computer.

- **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: □
Server:
Use Load Balancer: □
Load Balancer Info:
Use Credentials from General Tab: □
Username:
Password:
Domain:
Transport: AUTO
Bypass GW: ☑

- **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.

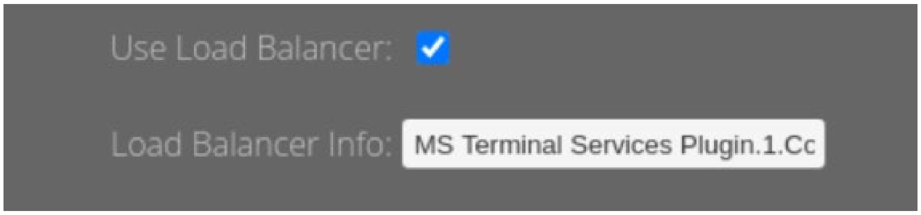
- **Load Balancer Info:** This is the address of your load balancer server within your corporation.

  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 Load Balancer: ☑

Load Balancer Info: MS Terminal Services Plugin.1.Cc

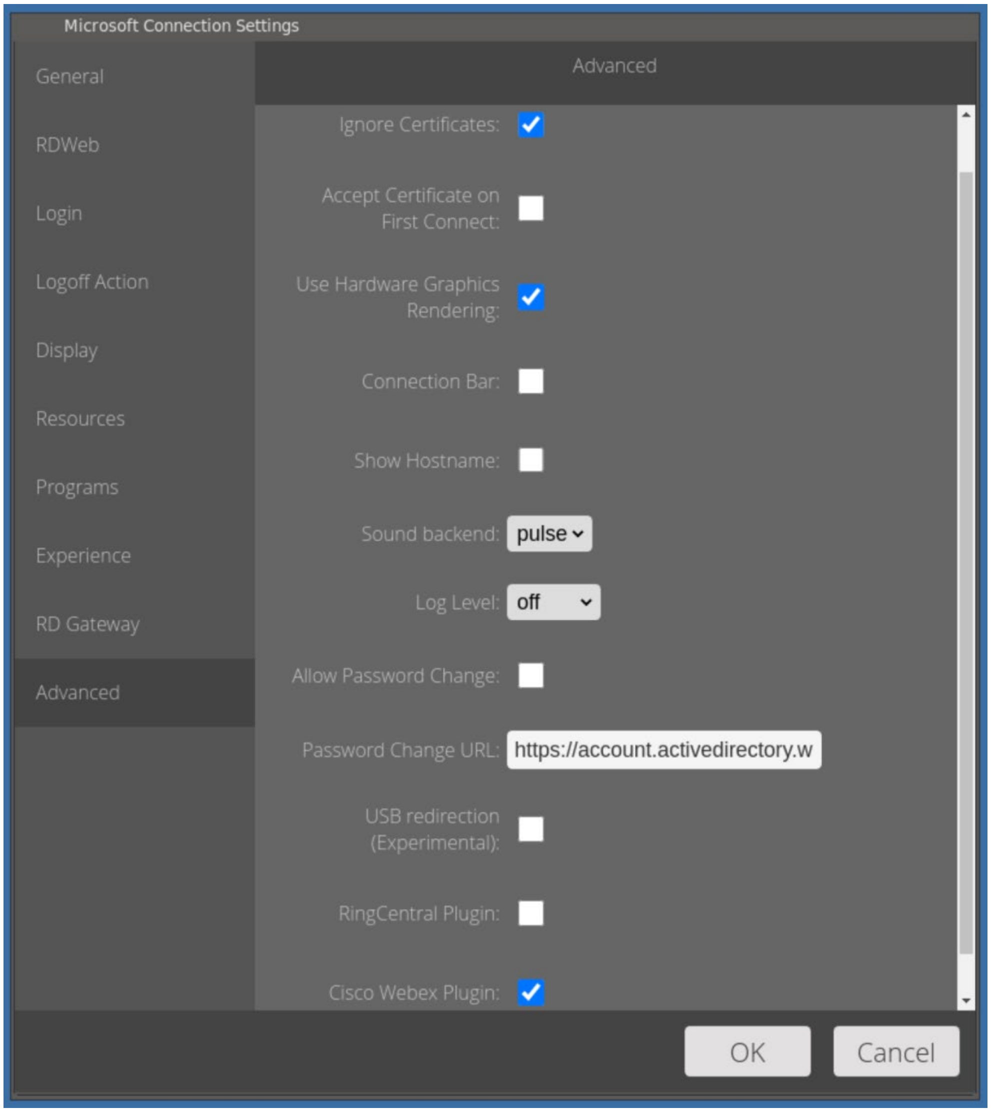
- **Use Credentials from General Tab:** Tick this box to use the credentials supplied at the time of connection or the credentials stored in the "General" tab which will be used both to authenticate to the gateway server and to the remote desktop .

- **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



Microsoft Connection Settings

Advanced

Ignore Certificates: ☑

Accept Certificate on First Connect: □

Use Hardware Graphics Rendering: ☑

Connection Bar: □

Show Hostname: □

Sound backend: pulse

Log Level: off

Allow Password Change: □

Password Change URL: https://account.activedirectory.w

USB redirection (Experimental): □

RingCentral Plugin: □

Cisco Webex Plugin: ☑

- **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.

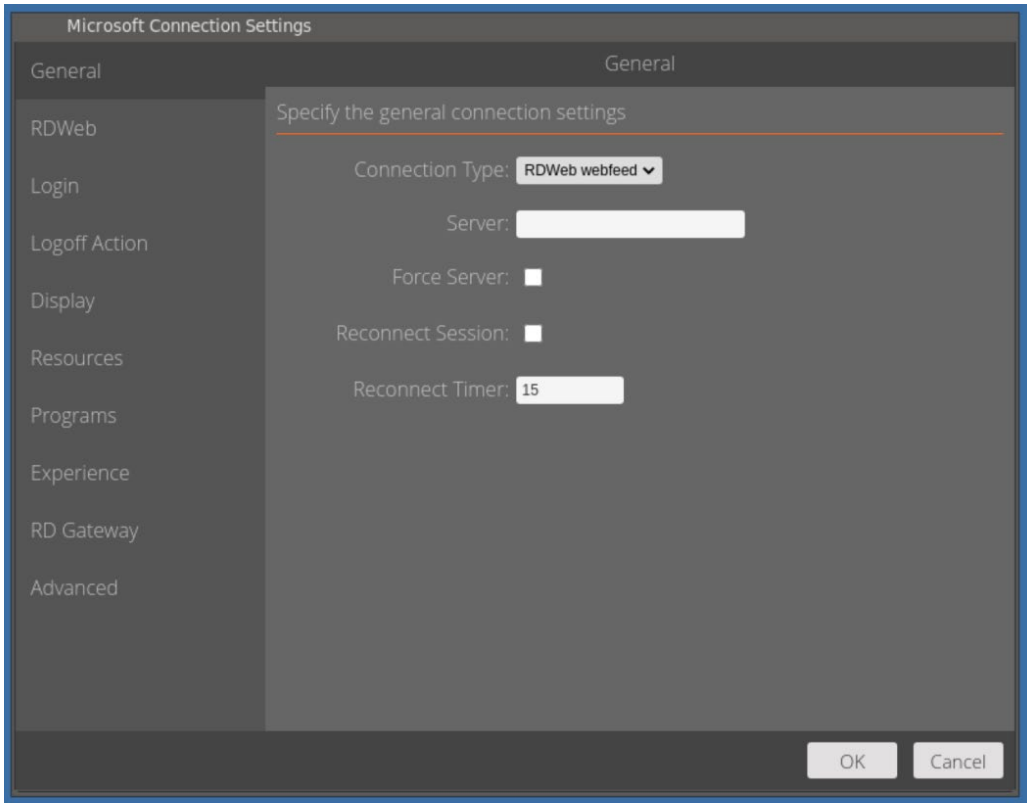
- **USB redirection(Experimental):** Enable this option, at user discretion to redirect your USB devices through to the VDI. Note: This is an experimental feature and as such may produce differing results.

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

- **Cisco Webex Plugin**: Enable this option to allow user to access the Webex app functionality inside the virtual desktop.

RDWeb webfeed

General



General

Specify the general connection settings

Connection Type: RDWeb webfeed

Server:

Force Server: □

Reconnect Session: □

Reconnect Timer: 15

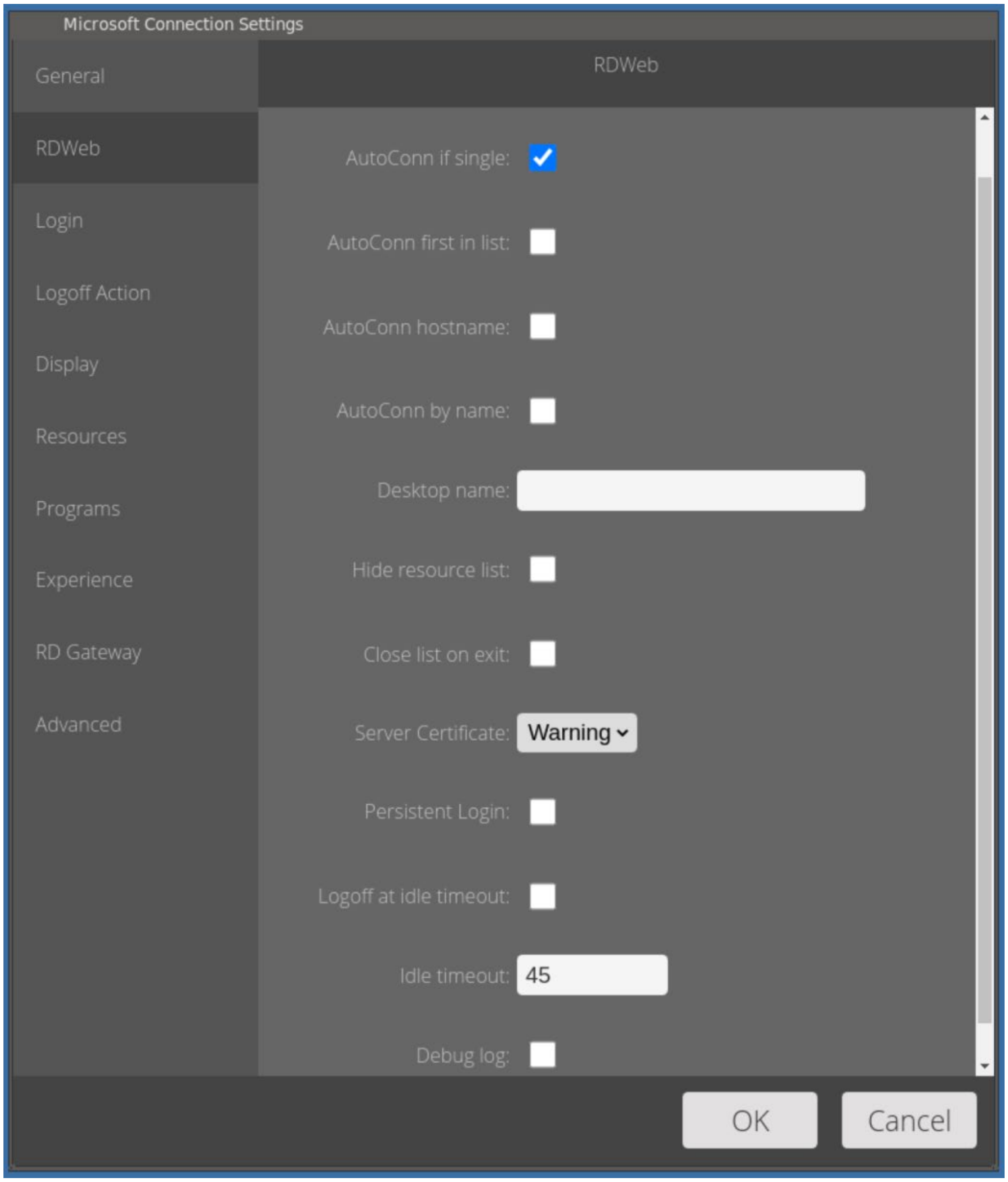
- **Server:** This is where you can enter a single server or multiple URL addresses of the remote desktop connection broker. If multiples are used, then they should be comma separated.

- **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 disconnection.

RDWeb



Microsoft Connection Settings

RDWeb

AutoConn if single: ☑

AutoConn first in list: □

AutoConn hostname: □

AutoConn by name: □

Desktop name:

Hide resource list: □

Close list on exit: □

Server Certificate: Warning

Persistent Login: □

Logoff at idle timeout: □

Idle timeout: 45

Debug log: □

- **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”.

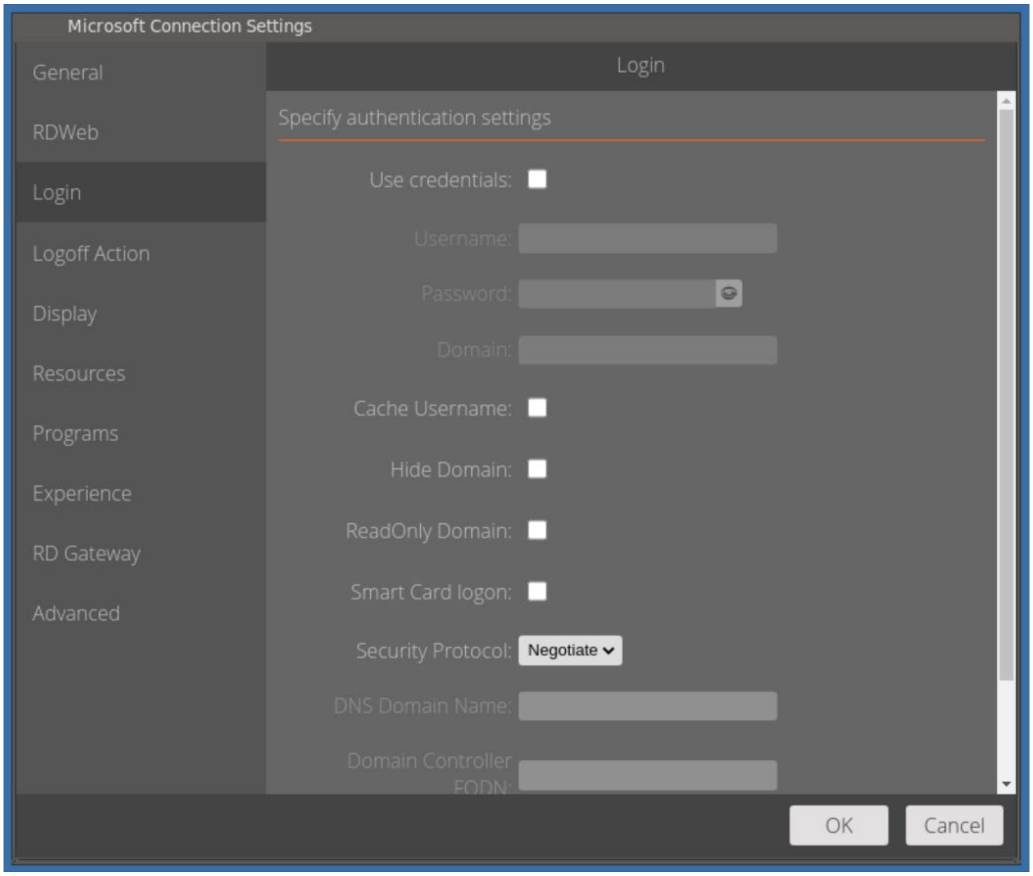
- **Persistent Login**: To be used with auto login. When you save the credentials in the configuration, the connection goes straight to showing the user entitled app list (Resource List, icon container). When you click "Logoff", the icon container is closed, and you return to the login dialog box. When 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

Login



Specify authentication settings

Use credentials: □

Username:

Password:

Domain:

Cache Username: □

Hide Domain: □

ReadOnly Domain: □

Smart Card logon: □

Security Protocol: Negotiate

DNS Domain Name:

Domain Controller FQDN:

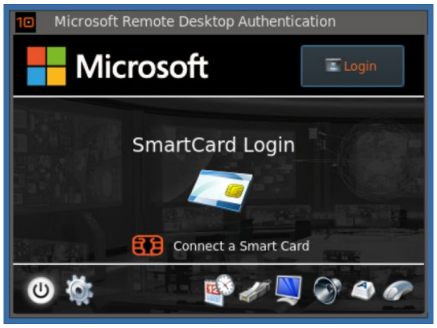
- **Use Credentials:** If you enable this, then the credentials fields below it will be used at login until changed or disabled. See the example above.

- **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:** 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.



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

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

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

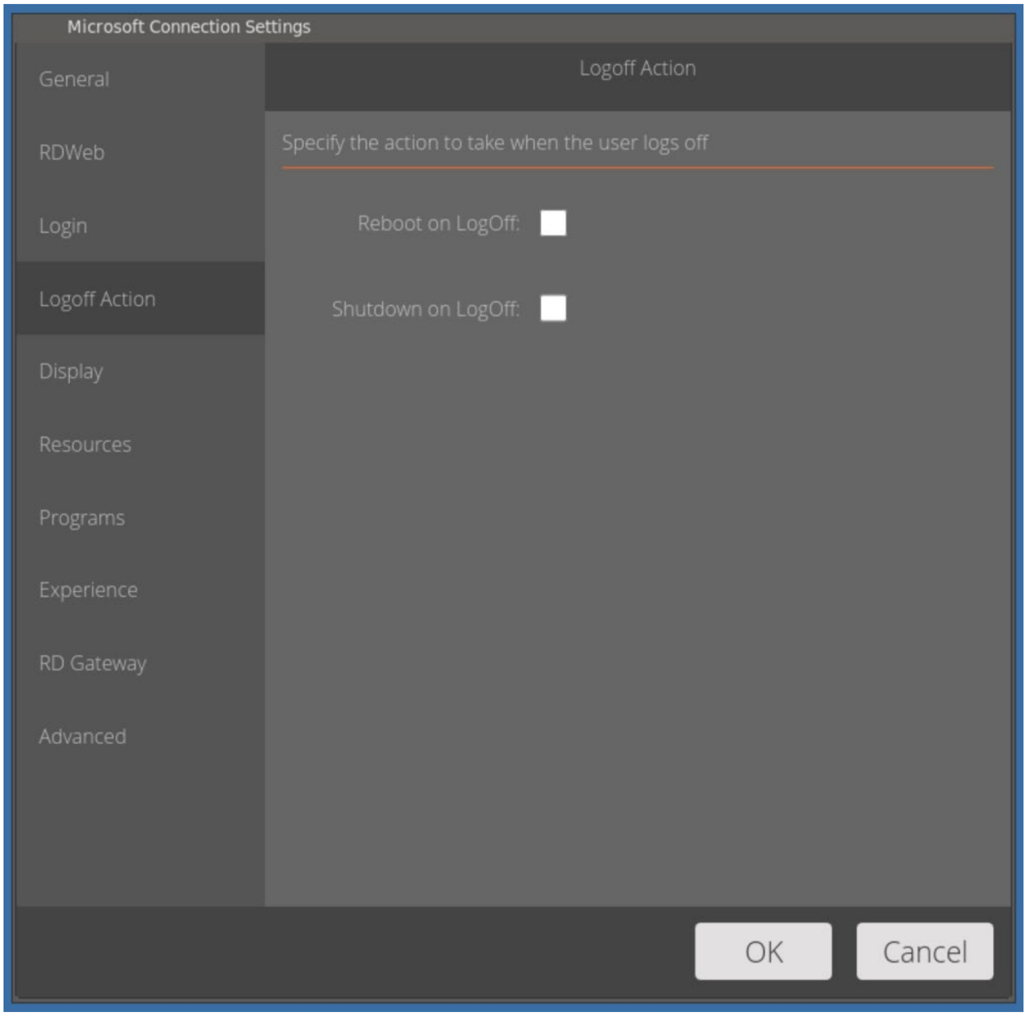
- **Domain Controller FQDN:** This is the fully qualified domain name of the domain controller on your network. You can supply multiple domain controllers by separating them with commas.

- **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”.

Logoff Action



Specify the action to take when the user logs off

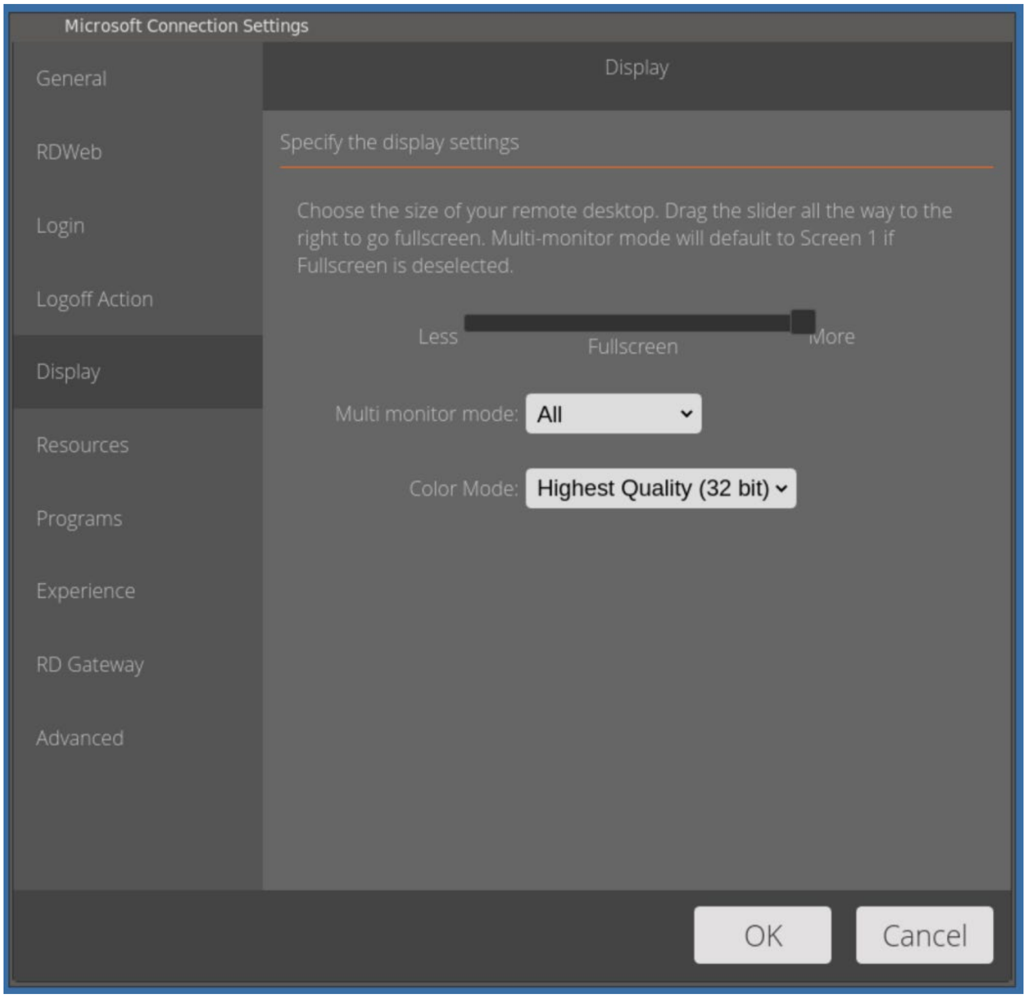
Reboot on LogOff: □

Shutdown on LogOff: □

- **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



Microsoft Connection Settings

Display

Specify the display settings

Choose the size of your remote desktop. Drag the slider all the way to the right to go fullscreen. Multi-monitor mode will default to Screen 1 if Fullscreen is deselected.

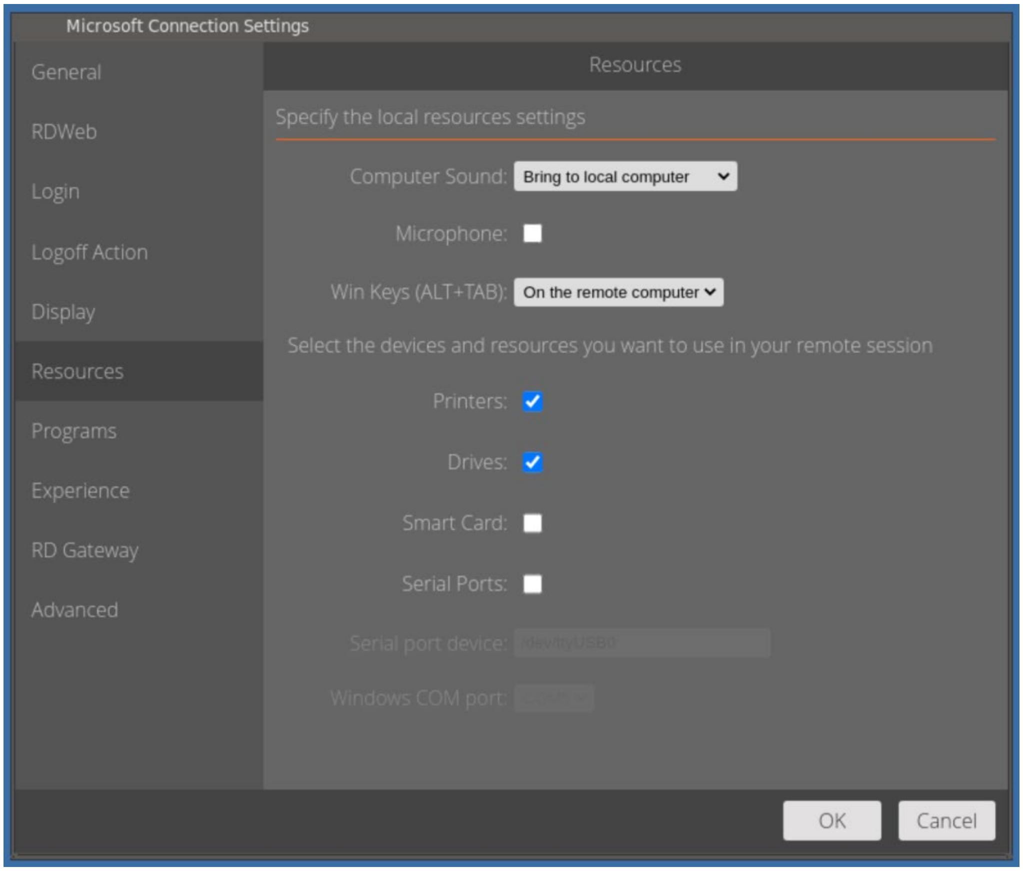
Fullscreen

Multi monitor mode: All

Color Mode: Highest Quality (32 bit)

- **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



Resources

Specify the local resources settings

Computer Sound: Bring to local computer

Microphone: □

Win Keys (ALT+TAB): On the remote computer

Select the devices and resources you want to use in your remote session

Printers: ☑

Drives: ☑

Smart Card: □

Serial Ports: □

Serial port device: /dev/ttyUSB0

Windows COM port:

- **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.

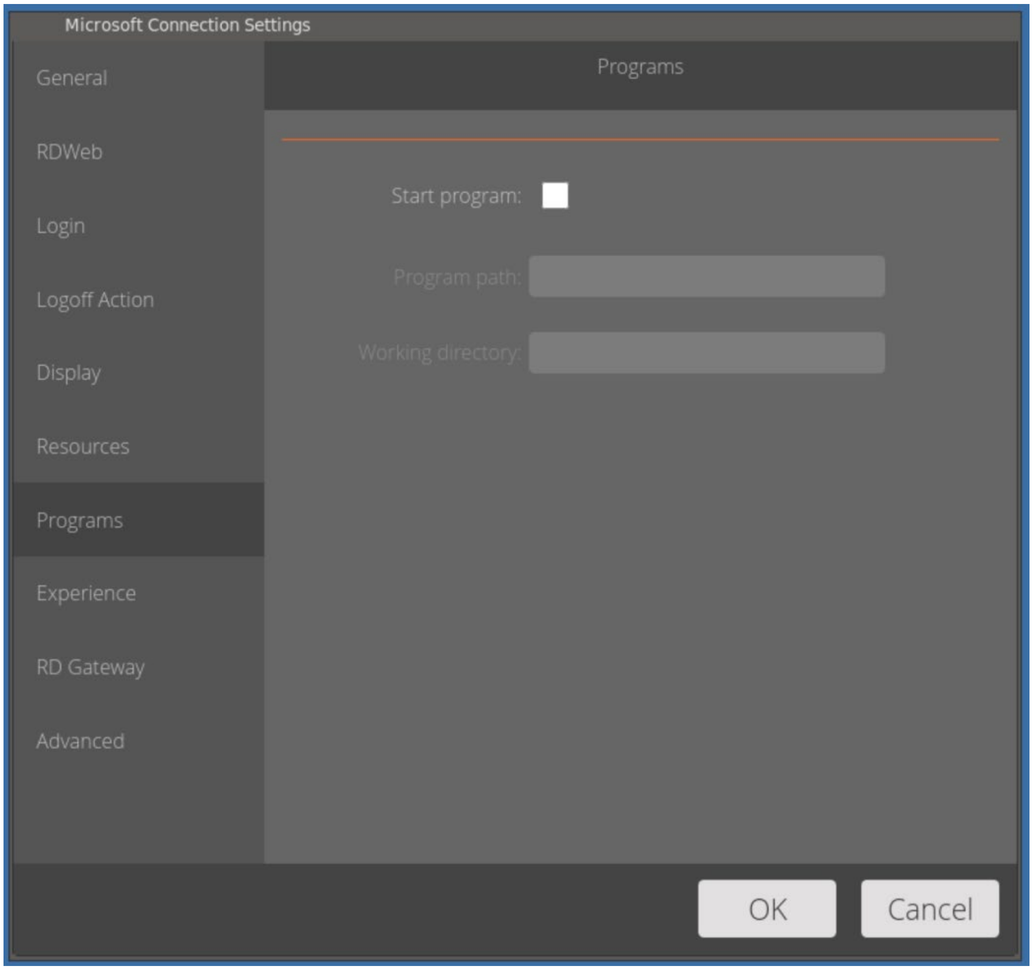
- **Smart Card:** This option, when enabled will pass the smart card through to the VDI desktop.

- **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.

Programs



Start program: □

Program path:

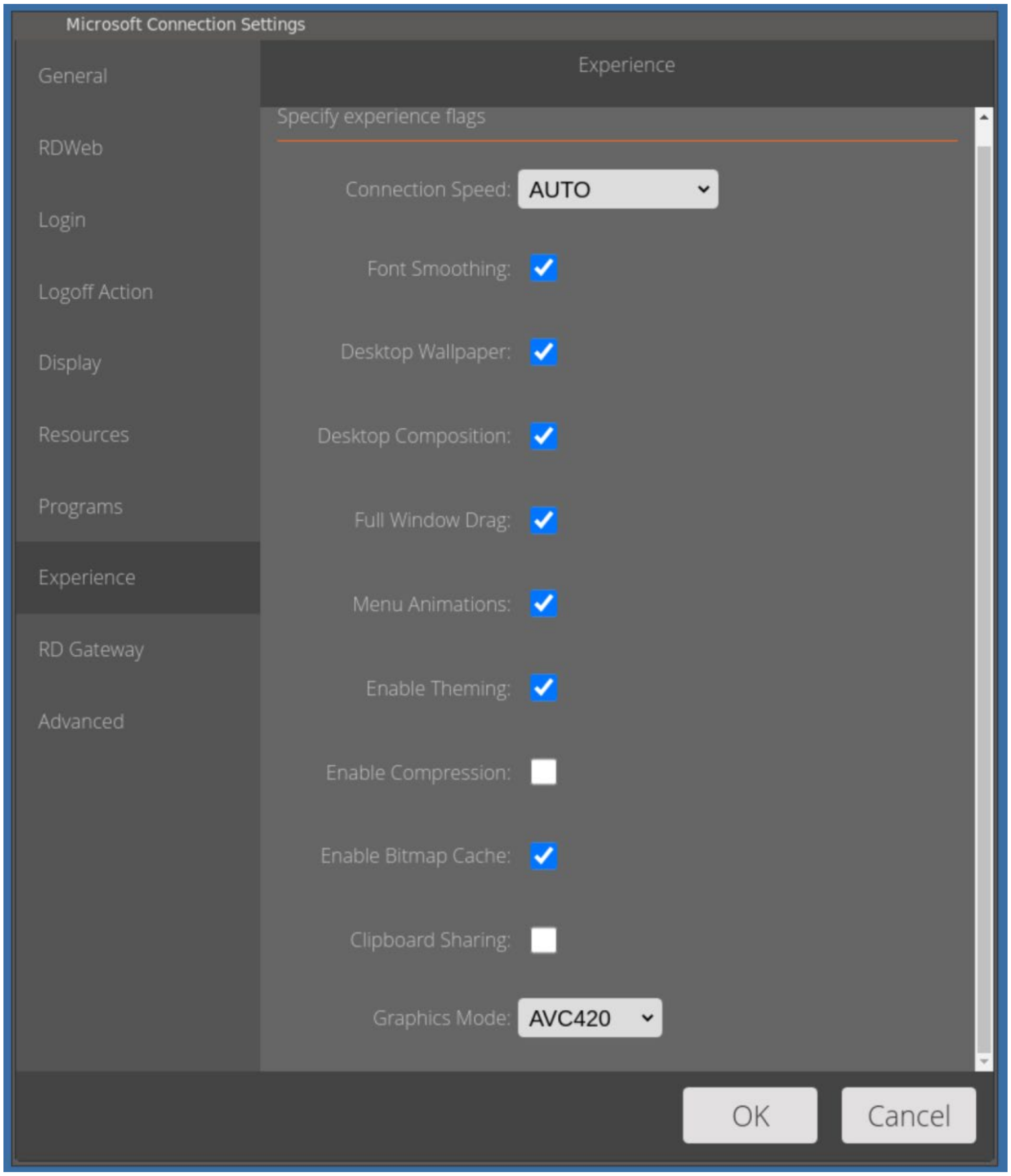
Working directory:

- **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



Microsoft Connection Settings

Experience

Specify experience flags

Connection Speed: AUTO

Font Smoothing: ☑

Desktop Wallpaper: ☑

Desktop Composition: ☑

Full Window Drag: ☑

Menu Animations: ☑

Enable Theming: ☑

Enable Compression: □

Enable Bitmap Cache: ☑

Clipboard Sharing: □

Graphics Mode: AVC420

- **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.

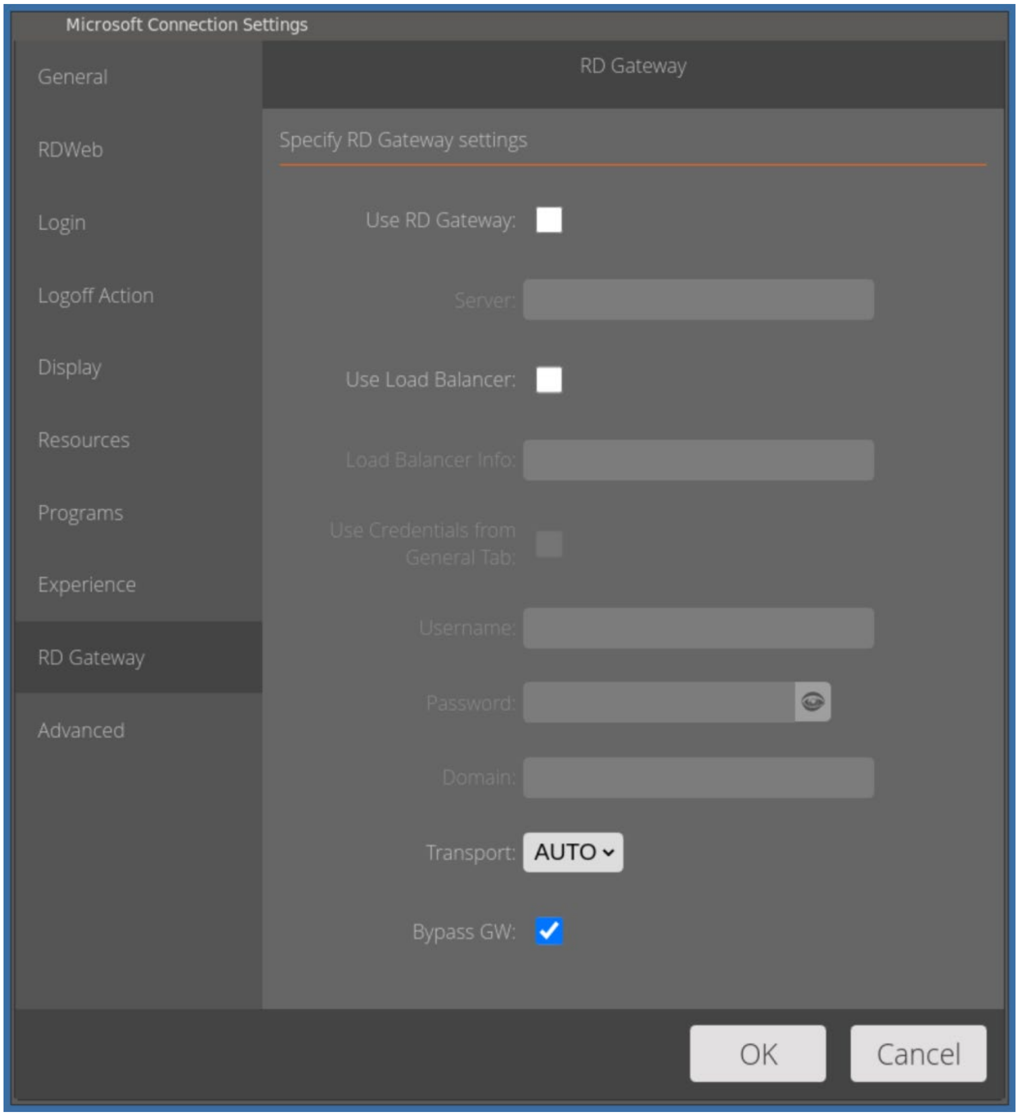
- **Enable Compression:** Determines whether bulk compression is enabled when it's transmitted by RDP to the local computer.

- **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



Specify RD Gateway settings

Use RD Gateway: ☐

Server:

Use Load Balancer: ☐

Load Balancer Info:

Use Credentials from General Tab: ☐

Username:

Password:

Domain:

Transport: AUTO

Bypass GW: ☑

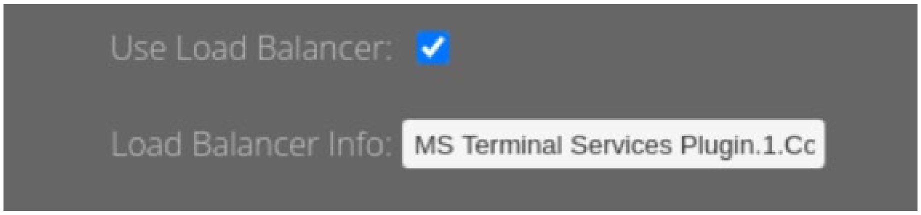
- **Use RD Gateway:** A RD Gateway allows you to establish a RDP connection to a Windows system but tunneled through a HTTPS connection.

- **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 Load Balancer: ☑

Load Balancer Info: MS Terminal Services Plugin.1.Cc

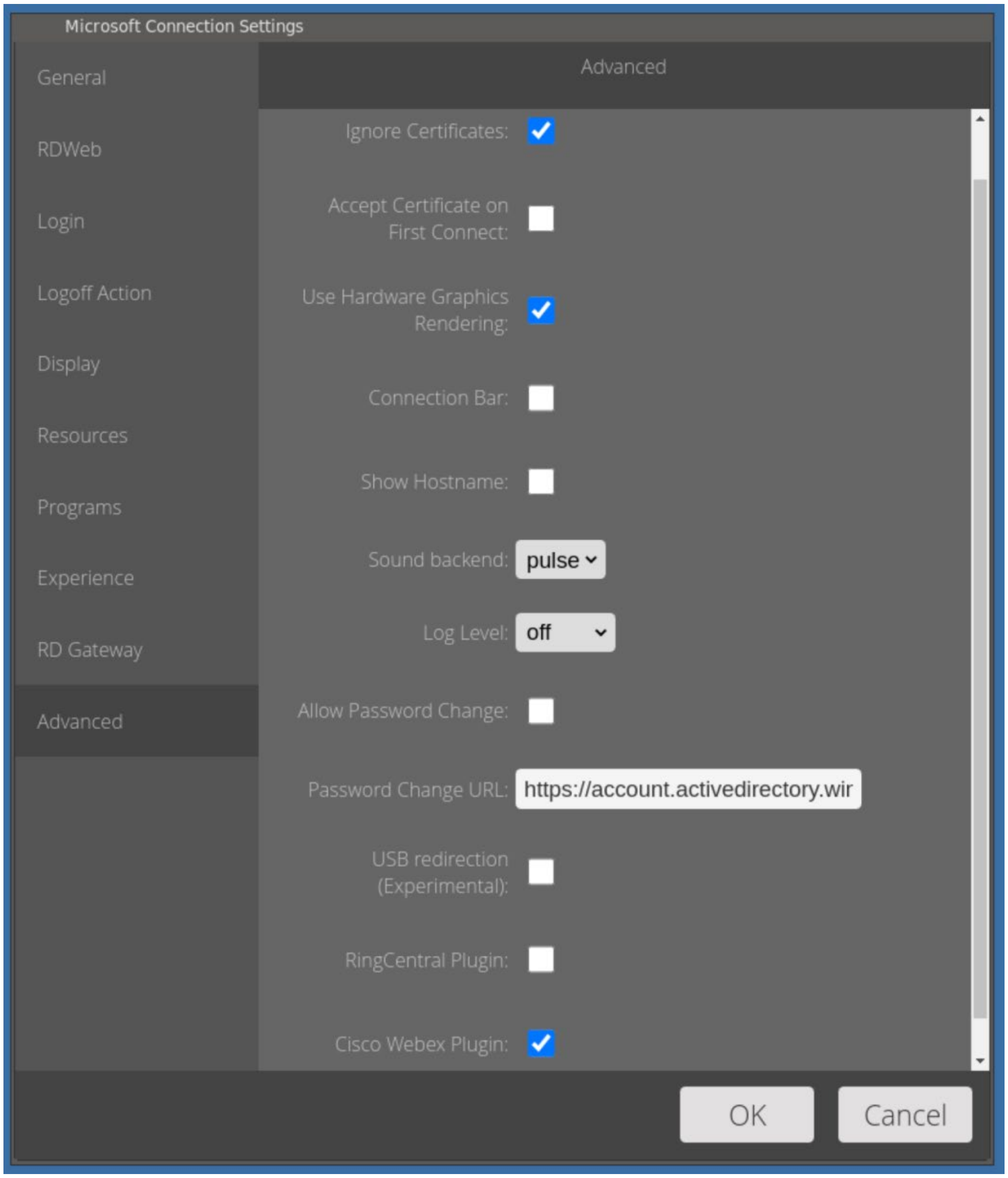
- **Use Credentials from General Tab:** Tick this box to use the credentials supplied at the time of connection or the credentials stored in the "General" tab which will be used both to authenticate to the gateway server and to the remote desktop .

- **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



Microsoft Connection Settings

Advanced

Ignore Certificates: ☑

Accept Certificate on First Connect: □

Use Hardware Graphics Rendering: ☑

Connection Bar: □

Show Hostname: □

Sound backend: pulse

Log Level: off

Allow Password Change: □

Password Change URL: https://account.activedirectory.wir

USB redirection (Experimental): □

RingCentral Plugin: □

Cisco Webex Plugin: ☑

- **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.

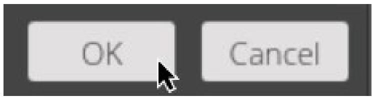
- **USB redirection(Experimental):** Enable this option, at user discretion to redirect your USB devices through to the VDI. Note: This is an experimental feature and as such may produce differing results.

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

- **Cisco Webex Plugin**: Enable this option to allow user to access the Webex app functionality inside the virtual desktop.

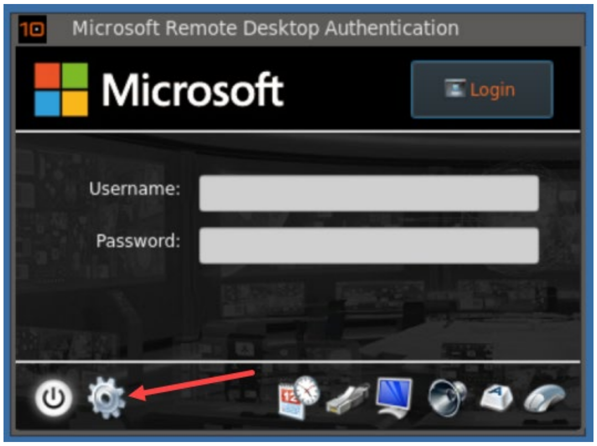
Saving your settings

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.

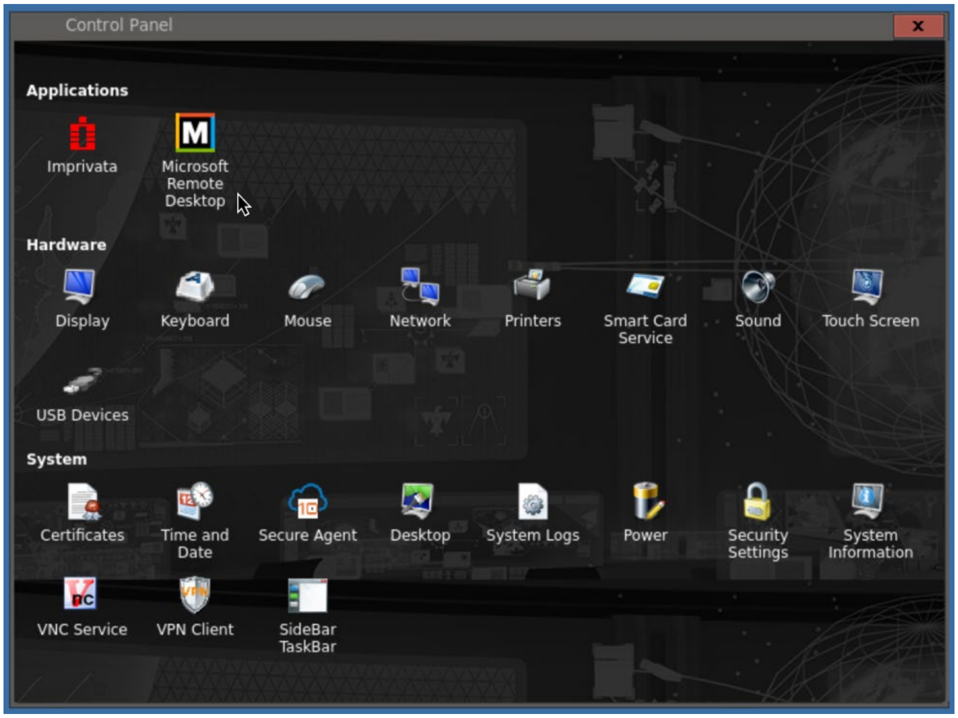


Editing your connection settings

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.



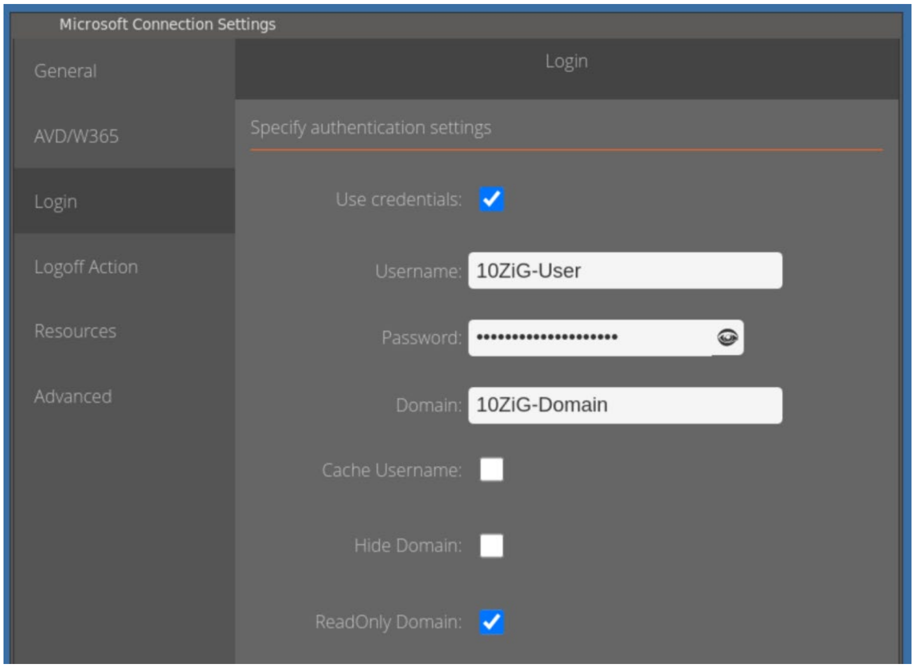
You'll be taken back into the "Control Panel", where you can click the "Microsoft Remote Desktop" icon in the top left and then make changes as outlined in the previous sections of this guide.



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.



Specify authentication settings

Use credentials: ☑

Username: 10ZiG-User

Password: ••••••••••••••••••••

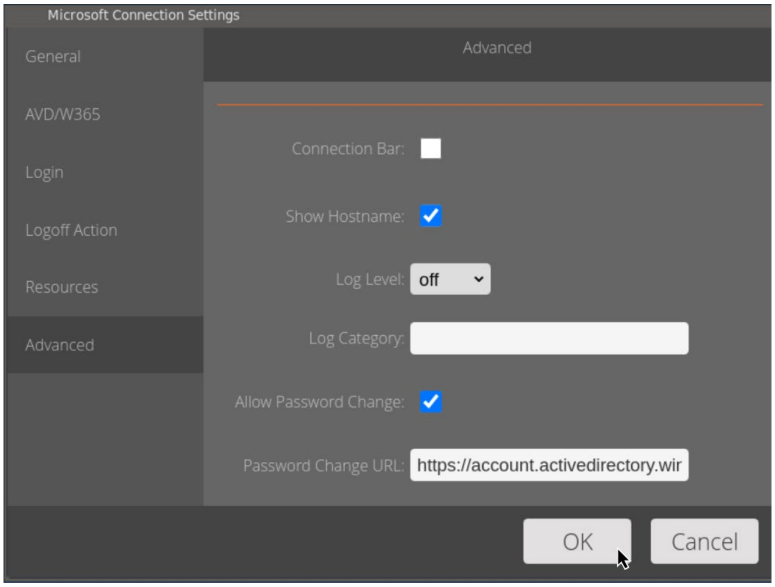
Domain: 10ZiG-Domain

Cache Username: □

Hide Domain: □

ReadOnly Domain: ☑

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



Connection Bar: □

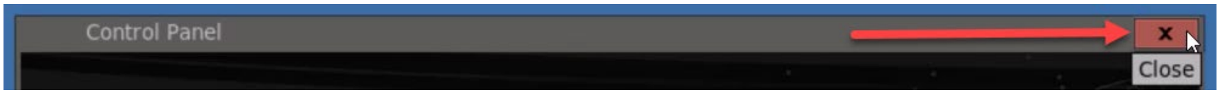
Show Hostname: ☑

Log Level: off

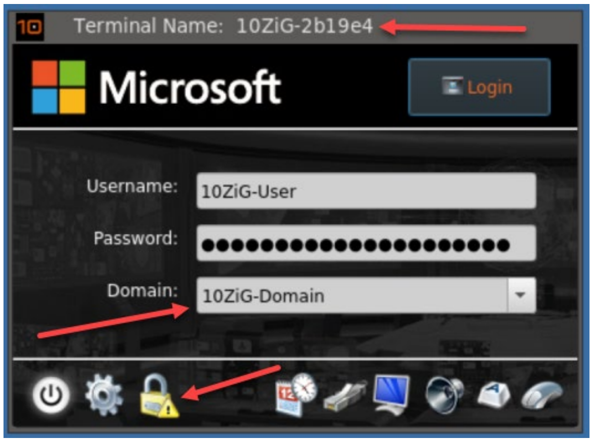
Log Category:

Allow Password Change: ☑

Password Change URL: https://account.activedirectory.wir



Your login screen should now look something like 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.


Terminal Name: 10ZiG-2b19e4

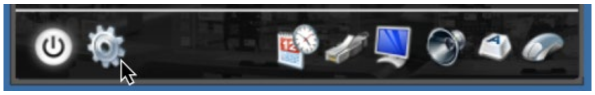
Username: 10ZiG-User

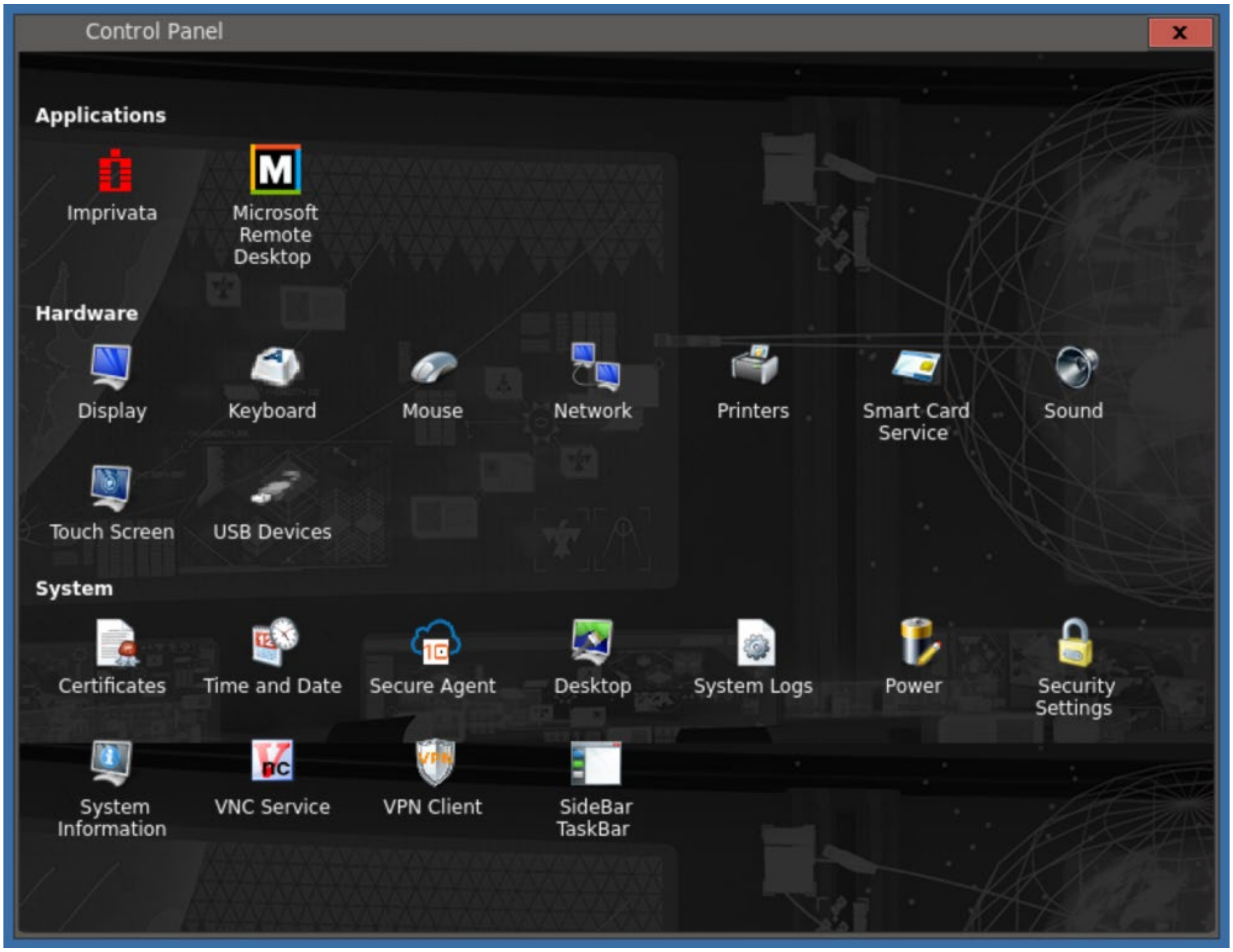
Password: ●●●●●●●●●●●●●●●●●●●●●

Domain: 10ZiG-Domain

Control Panel Settings

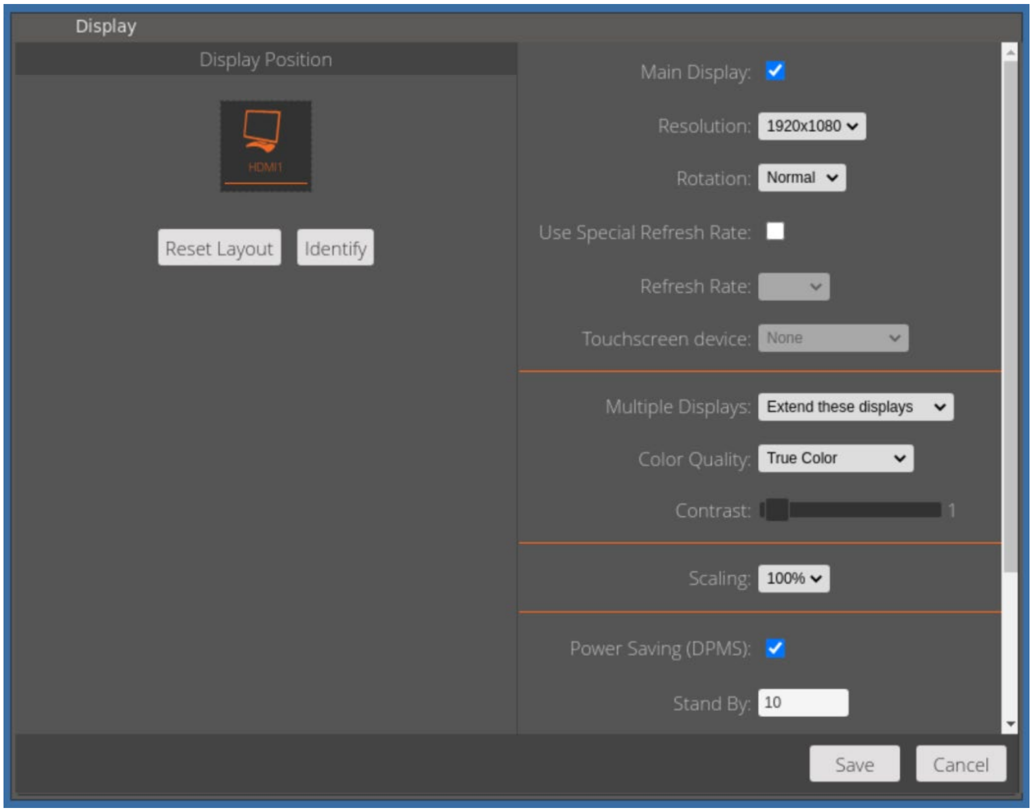
From any of the NOS platforms, on the login screen, if you click on “Gear” icon, then you’ll be taken into “Control Panel “, where you have the ability to further customize your 10ZiG zero client’s “Application”, “Hardware and “System” settings.





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.



Main Display: ☑

Resolution: 1920x1080

Rotation: Normal

Use Special Refresh Rate: □

Refresh Rate:

Touchscreen device: None

Multiple Displays: Extend these displays

Color Quality: True Color

Contrast: 1

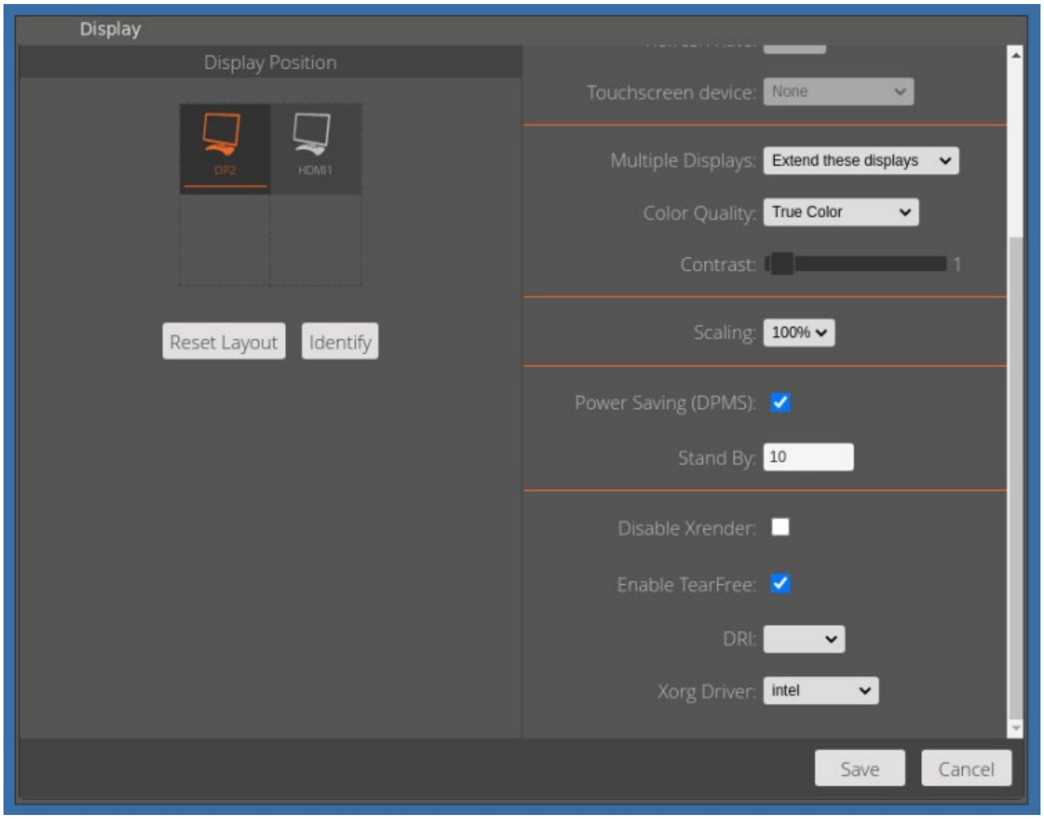
Scaling: 100%

Power Saving (DPMS): ☑

Stand By: 10

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.



Touchscreen device: None

Multiple Displays: Extend these displays

Color Quality: True Color

Contrast: 1

Scaling: 100%

Power Saving (DPMS): ☑

Stand By: 10

Disable Xrender: □

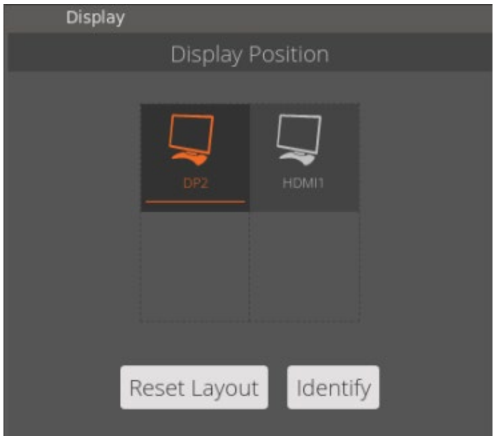
Enable TearFree: ☑

DRI:

Xorg Driver: intel

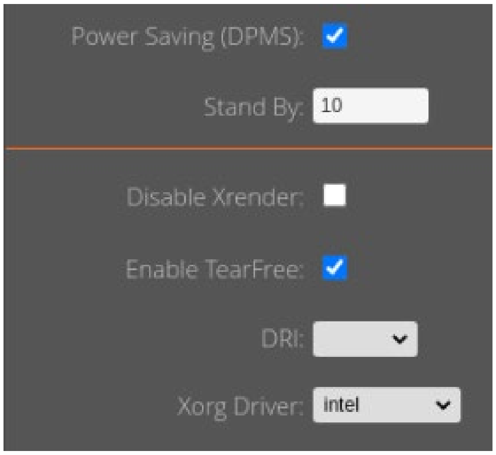
You can change the resolution of each monitor by selecting the resolution you want for HDMI1 and DP2.

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.



Power Saving (DPMS): ☑

Stand By: 10

Disable Xrender: □

Enable TearFree: ☑

DRI:

Xorg Driver: intel

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

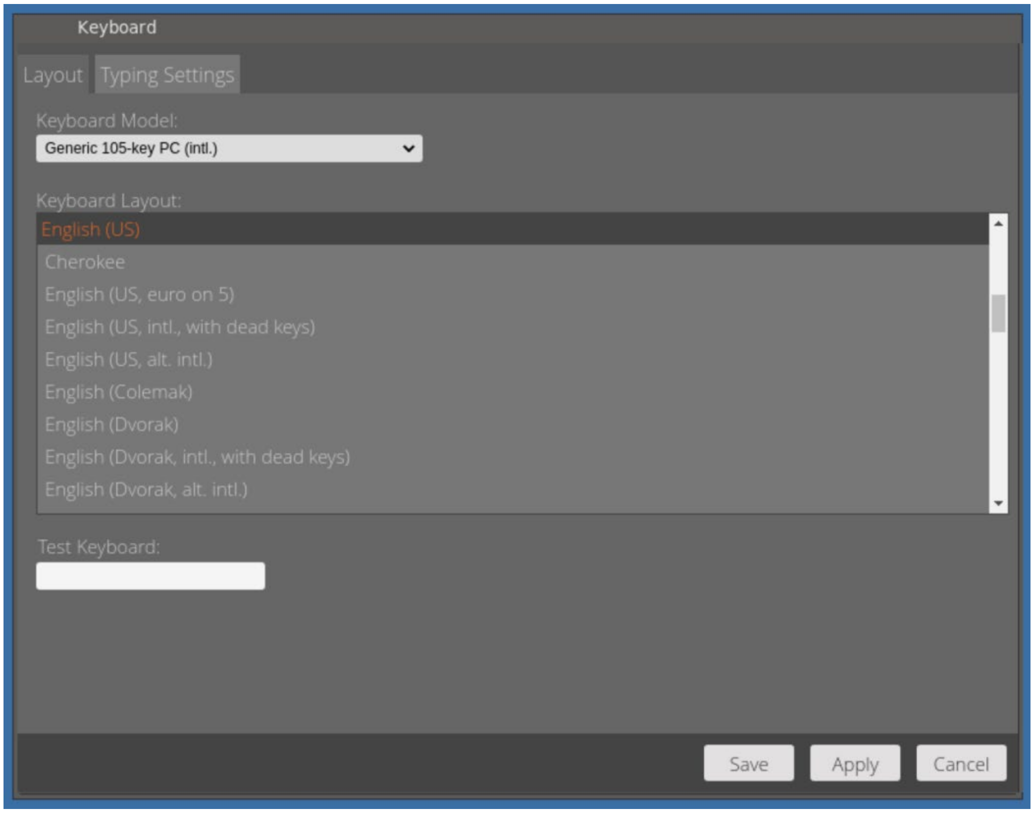
Enabling “Restart Xorg on hotplug event” will force a refresh of the displays, to make sure any hotplugs are detected correctly.

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 Model:

Generic 105-key PC (intl.)

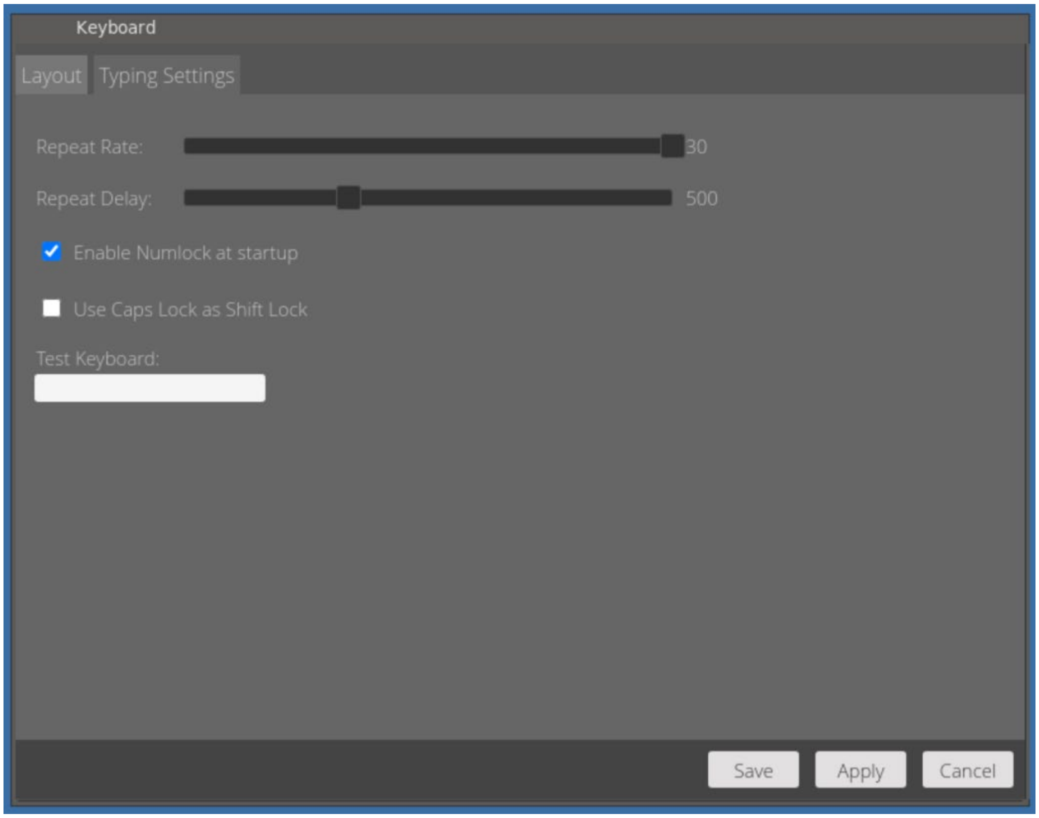
Keyboard Layout:

- English (US)
- Cherokee
- English (US, euro on 5)
- English (US, intl., with dead keys)
- English (US, alt. intl.)
- English (Colemak)
- English (Dvorak)
- English (Dvorak, intl., with dead keys)
- English (Dvorak, alt. intl.)

Test Keyboard:

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.



Repeat Rate: 30

Repeat Delay: 500

☑ Enable Numlock at startup

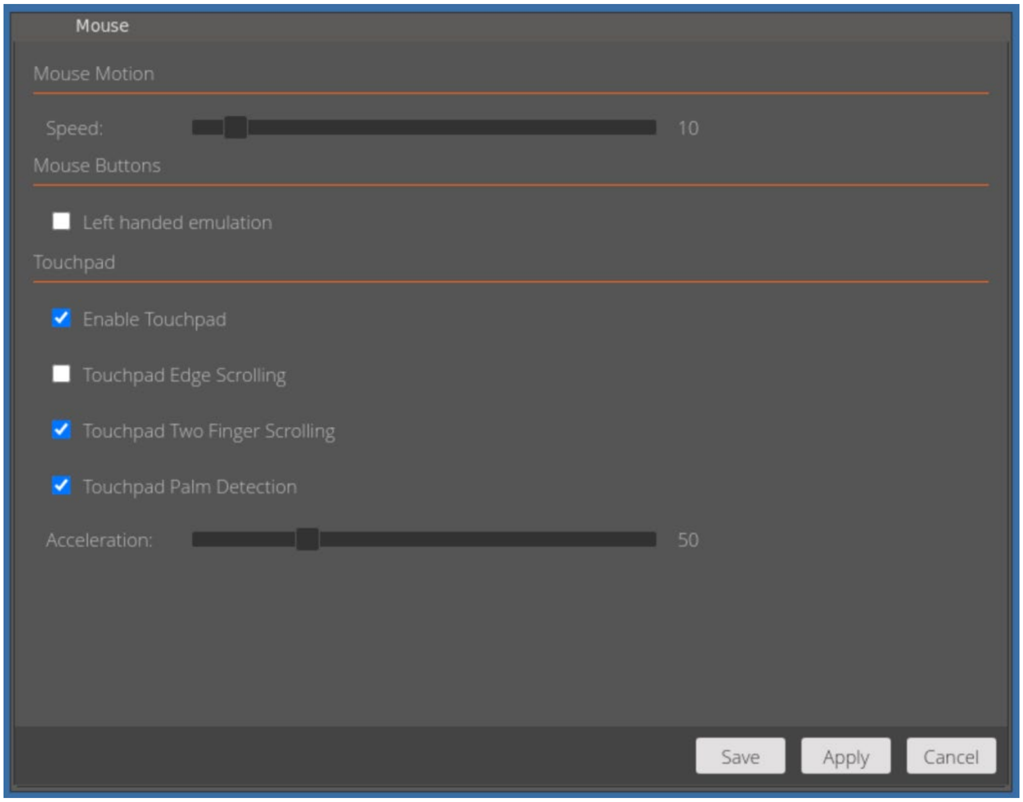
☐ Use Caps Lock as Shift Lock

Test Keyboard:

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 zero client, then enabling this option will allow you access its scrolling and detection options also.



Mouse

Mouse Motion

Speed: 10

Mouse Buttons

□ Left handed emulation

Touchpad

☑ Enable Touchpad

□ Touchpad Edge Scrolling

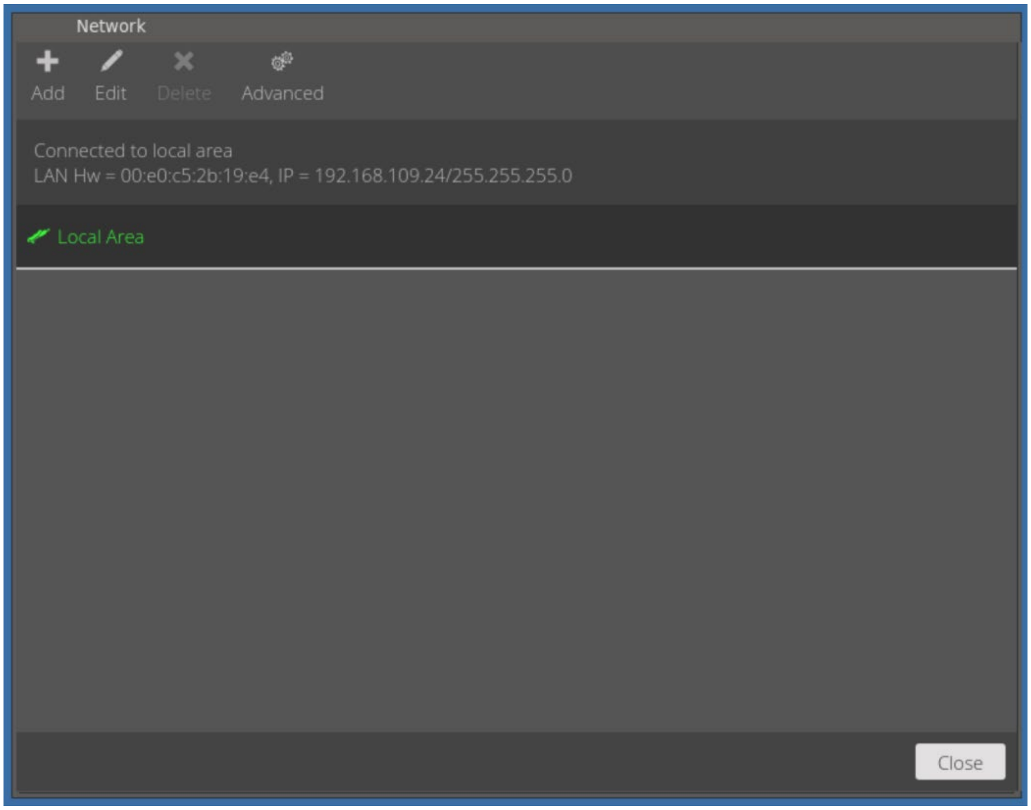
☑ Touchpad Two Finger Scrolling

☑ Touchpad Palm Detection

Acceleration: 50

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.

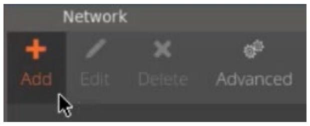


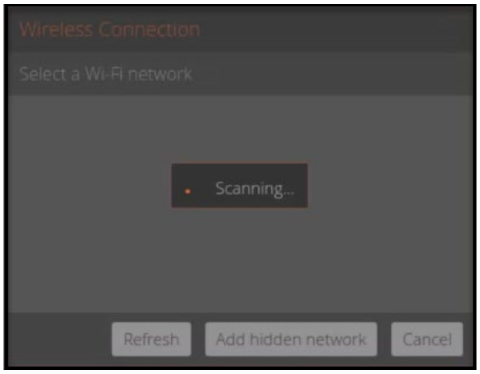
Connected to local area
LAN Hw = 00:e0:c5:2b:19:e4, IP = 192.168.109.24/255.255.255.0

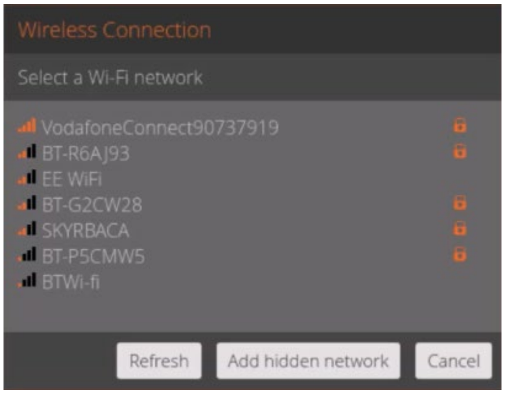
✓ Local Area

Wireless Network Connection (**Additional Hardware Opt.**)

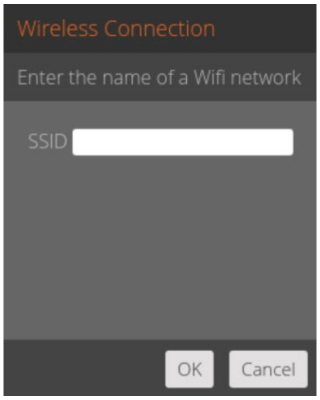
Open the Network Configuration applet by double clicking on the Network Icon, now click the “Add” button and the Wireless Connection properties will open, and you’ll see the “Scanning Wireless” message appear and then see a list of Broadcasted SSIDs in your environment, choose the wireless access point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



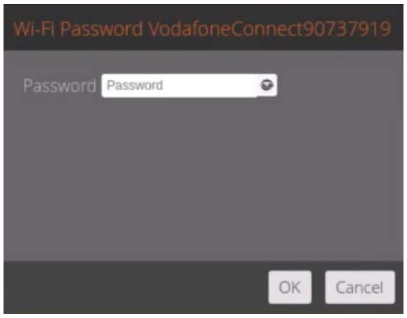




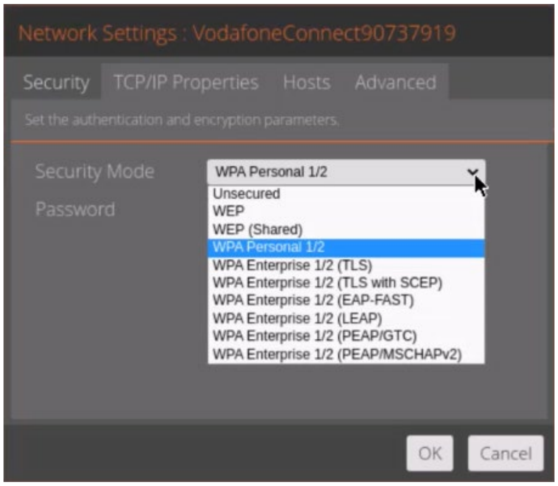
If you don’t see the SSID that matches your Wi-Fi network, just click the “Refresh” button and it should appear in the list. Check with you network administrator to make sure that it’s not hidden. If it is hidden, then just click the “Add hidden network” button and you’ll be able to add it in there.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



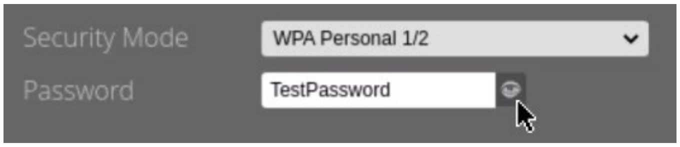
Network Settings : VodafoneConnect90737919

Set the authentication and encryption parameters.

Security Mode: WPA Personal 1/2

Password

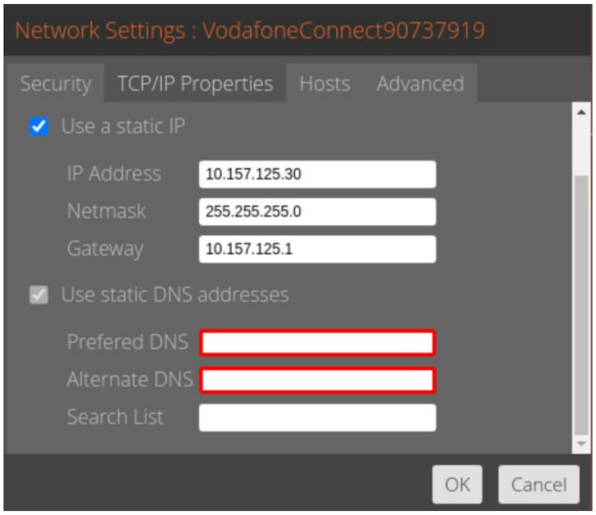
Security
TCP/IP Properties
Hosts
Advanced
Unsecured
WEP
WEP (Shared)
WPA Personal 1/2
WPA Enterprise 1/2 (TLS)
WPA Enterprise 1/2 (TLS with SCEP)
WPA Enterprise 1/2 (EAP-FAST)
WPA Enterprise 1/2 (LEAP)
WPA Enterprise 1/2 (PEAP/GTC)
WPA Enterprise 1/2 (PEAP/MSCHAPv2)
OK
Cancel



Security Mode: WPA Personal 1/2

Password: TestPassword

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.



Network Settings : VodafoneConnect90737919

☑ Use a static IP

IP Address: 10.157.125.30

Netmask: 255.255.255.0

Gateway: 10.157.125.1

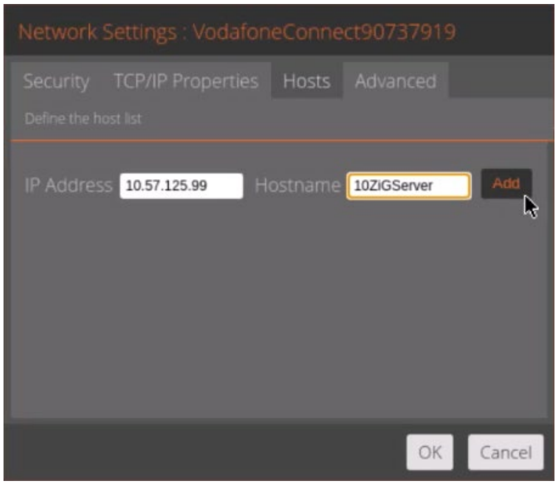
☑ Use static DNS addresses

Prefered DNS:

Alternate DNS:

Search List:

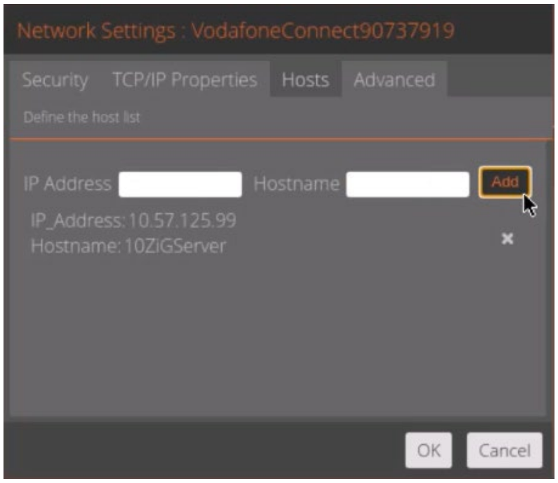
Using the “Hosts” tab you can define the host list for the wireless connection. Just click in the box below “Define the host list. Format : Ip_Address hostname” and start typing the IP address, followed by its hostname.



Network Settings : VodafoneConnect90737919

Define the host list

IP Address: 10.57.125.99
Hostname: 10ZiGServer



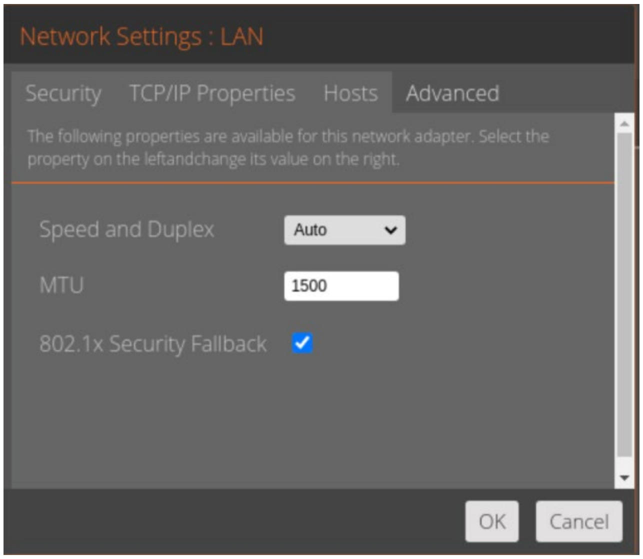
Network Settings : VodafoneConnect90737919

Define the host list

IP_Address: 10.57.125.99
Hostname: 10ZiGServer

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.



Network Settings : LAN

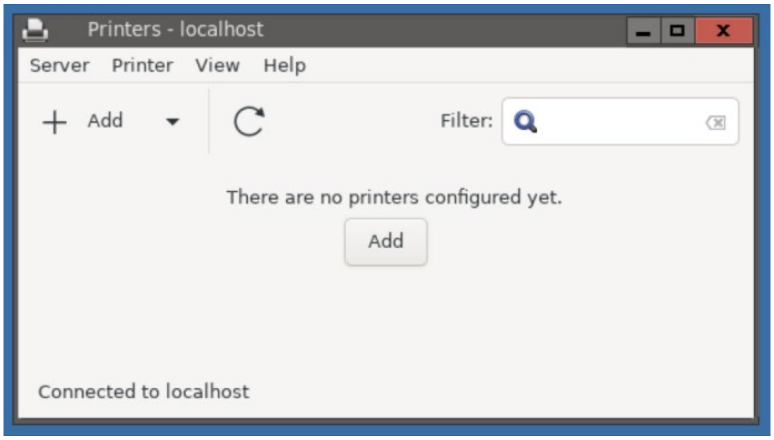
The following properties are available for this network adapter. Select the property on the leftandchange its value on the right.

Speed and Duplex: Auto
MTU: 1500
802.1x Security Fallback ☑

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.

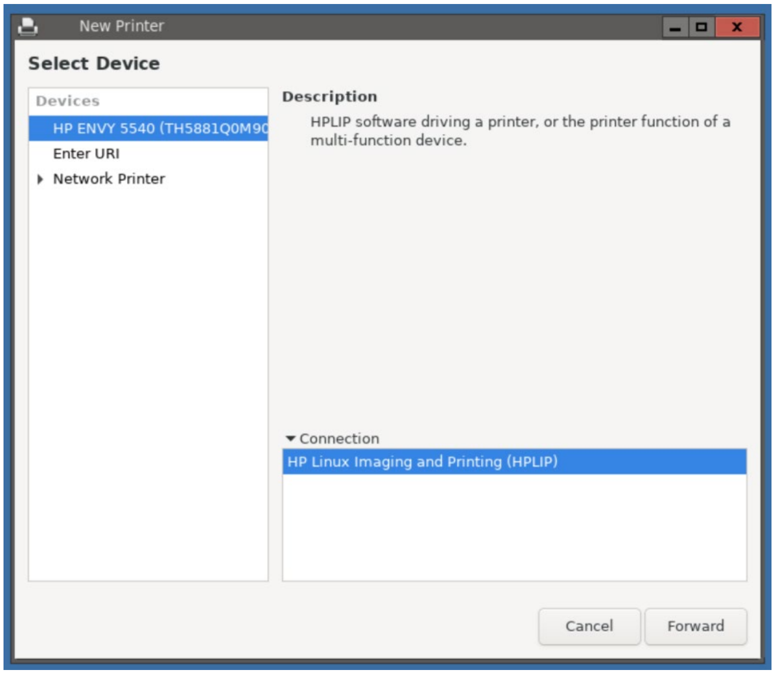
Configuring Local USB Printer



There are no printers configured yet.

Connected to localhost

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



Select Device

HP ENVY 5540 (TH5881Q0M9C

Enter URI

Network Printer

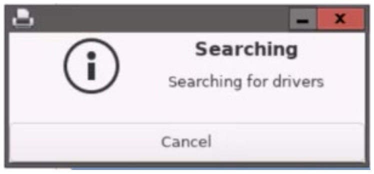
Description

HPLIP software driving a printer, or the printer function of a multi-function device.

Connection

HP Linux Imaging and Printing (HPLIP)

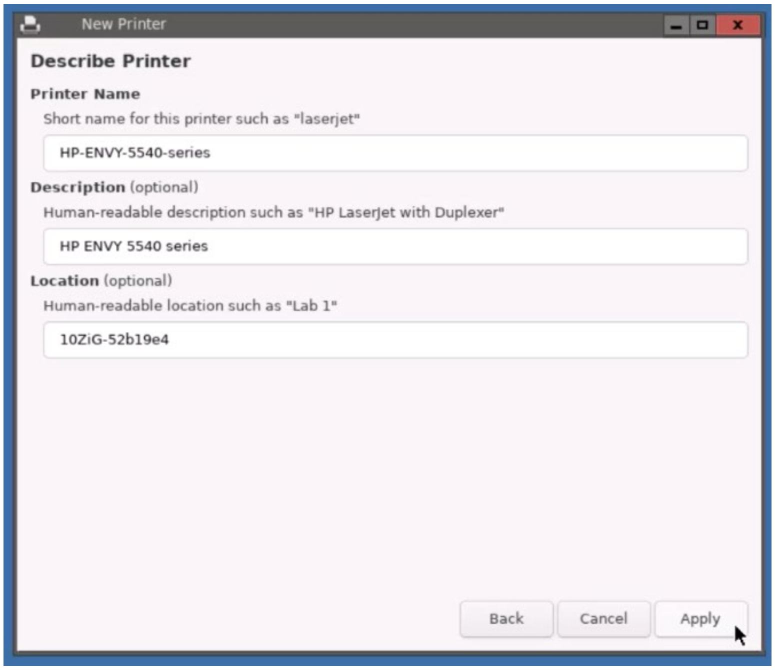
Once you've found your printer, click "Forward" and its drivers will be searched for and then installed locally on your endpoint.



Searching

Searching for drivers

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



Describe Printer

Printer Name

Short name for this printer such as "laserjet"

HP-ENVY-5540-series

Description (optional)

Human-readable description such as "HP LaserJet with Duplexer"

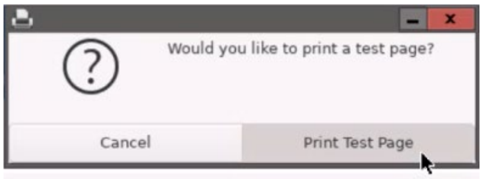
HP ENVY 5540 series

Location (optional)

Human-readable location such as "Lab 1"

10ZiG-52b19e4

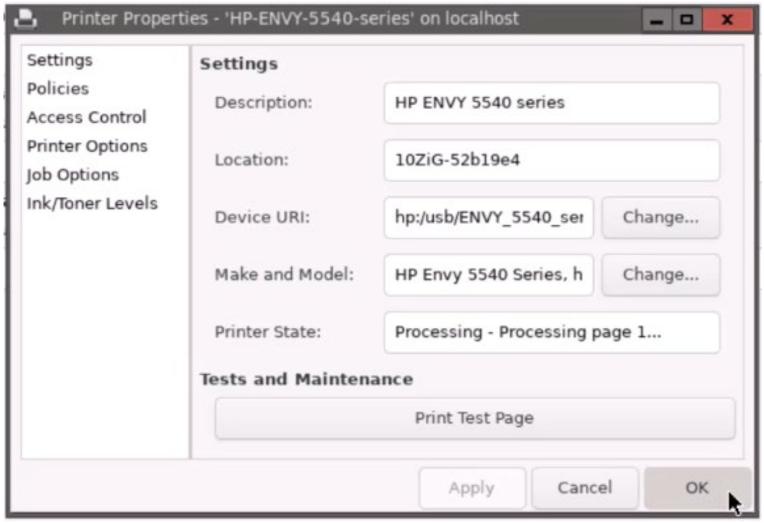
During the setup process, you have the option to "Print Test Page".



Would you like to print a 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



Printer Properties - 'HP-ENVY-5540-series' on localhost

Settings

Description: HP ENVY 5540 series

Location: 10ZiG-52b19e4

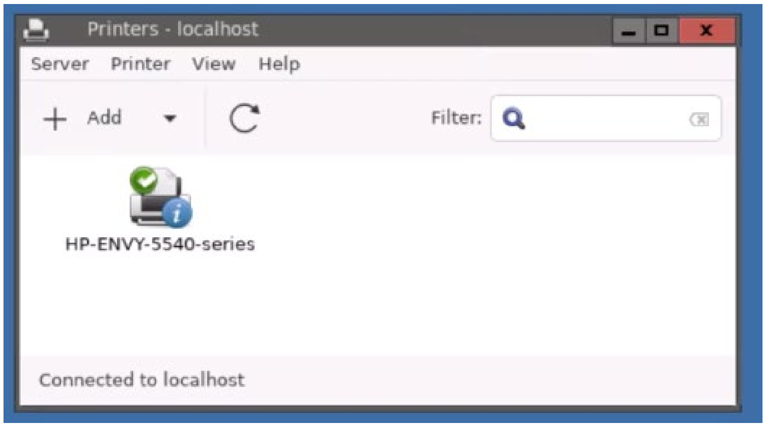
Device URI: hp:/usb/ENVY_5540_ser

Make and Model: HP Envy 5540 Series, h

Printer State: Processing - Processing page 1...

Tests and Maintenance

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

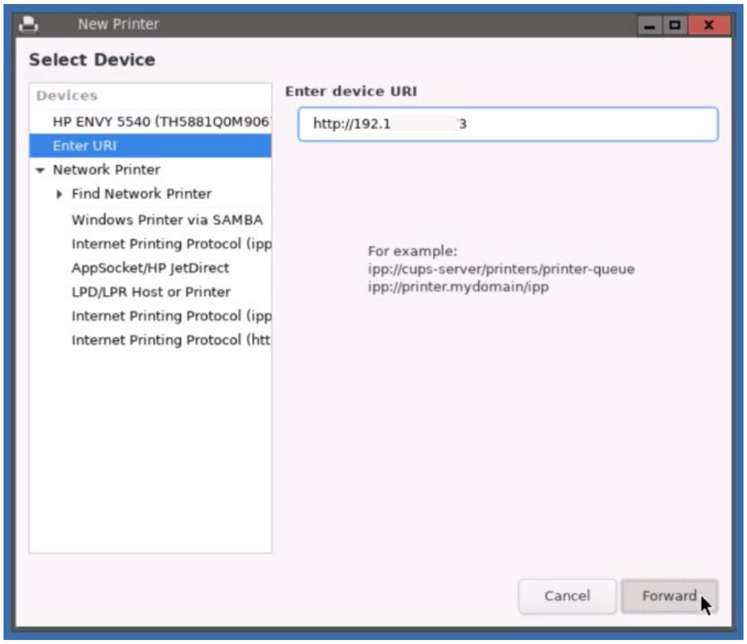


Printers - localhost

Connected to localhost

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.



New Printer

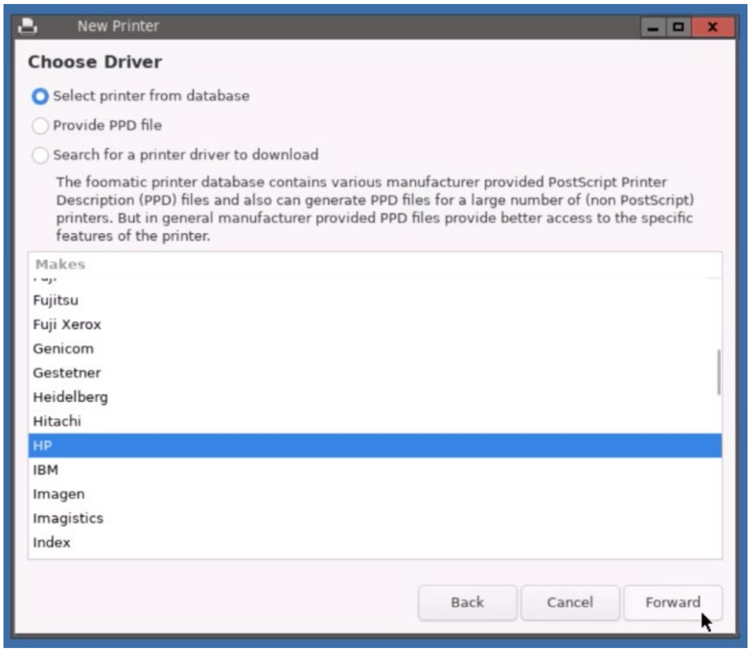
Select Device

Devices
- HP ENVY 5540 (TH5881Q0M906
- Enter URI
- Network Printer
  - Find Network Printer
  - Windows Printer via SAMBA
  - Internet Printing Protocol (ipp
  - AppSocket/HP JetDirect
  - LPD/LPR Host or Printer
  - Internet Printing Protocol (ipp
  - Internet Printing Protocol (htt

Enter device URI: http://192.1 3

For example:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp

Choose the printer vendor from the list provided.



New Printer

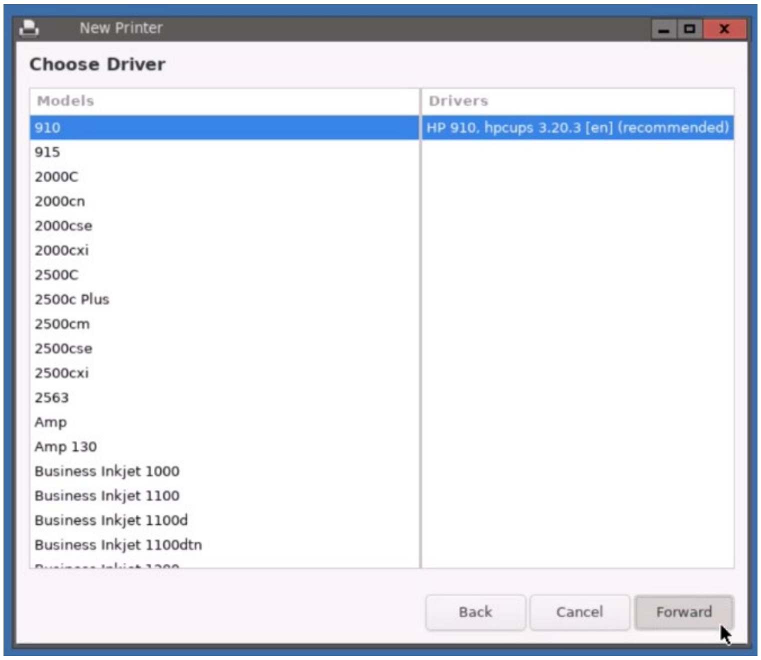
Choose Driver

- ● Select printer from database
- ○ Provide PPD file
- ○ Search for a printer driver to download

The foomatic printer database contains various manufacturer provided PostScript Printer Description (PPD) files and also can generate PPD files for a large number of (non PostScript) printers. But in general manufacturer provided PPD files provide better access to the specific features of the printer.

Makes
- Fujitsu
- Fuji Xerox
- Genicom
- Gestetner
- Heidelberg
- Hitachi
- HP
- IBM
- Imagen
- Imagistics
- Index

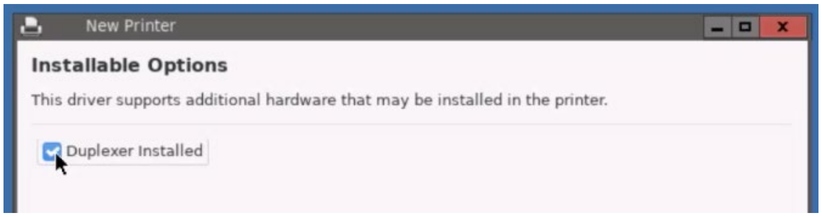
Choose the appropriate drivers.



Choose Driver

Models	Drivers
910	HP 910, hpcups 3.20.3 [en] (recommended)
915	
2000C	
2000cn	
2000cse	
2000cxi	
2500C	
2500c Plus	
2500cm	
2500cse	
2500cxi	
2563	
Amp	
Amp 130	
Business Inkjet 1000	
Business Inkjet 1100	
Business Inkjet 1100d	
Business Inkjet 1100dtn	

Select Installable Options.

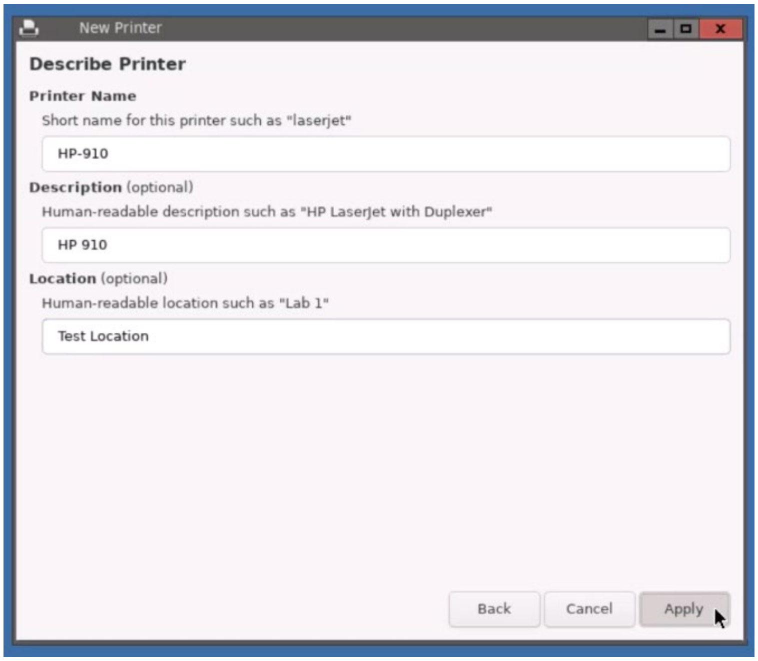


Installable Options

This driver supports additional hardware that may be installed in the printer.

☑ Duplexer Installed

Describe the printer.



Describe Printer

Printer Name

Short name for this printer such as "laserjet"

HP-910

Description (optional)

Human-readable description such as "HP LaserJet with Duplexer"

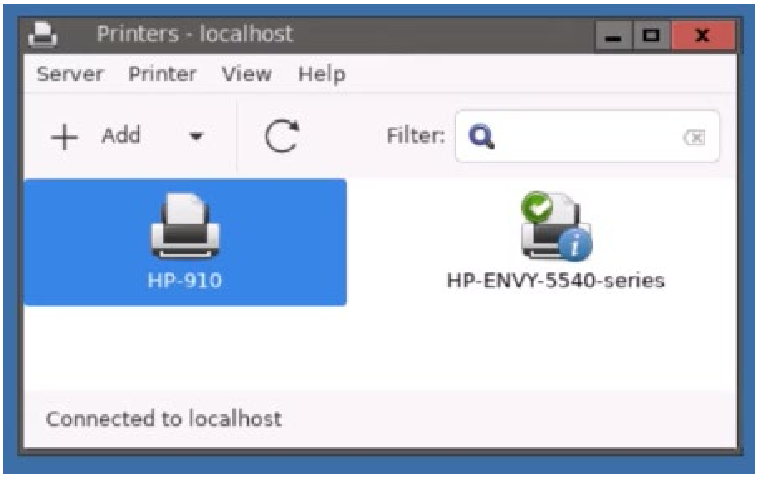
HP 910

Location (optional)

Human-readable location such as "Lab 1"

Test Location

The network printer added successfully.

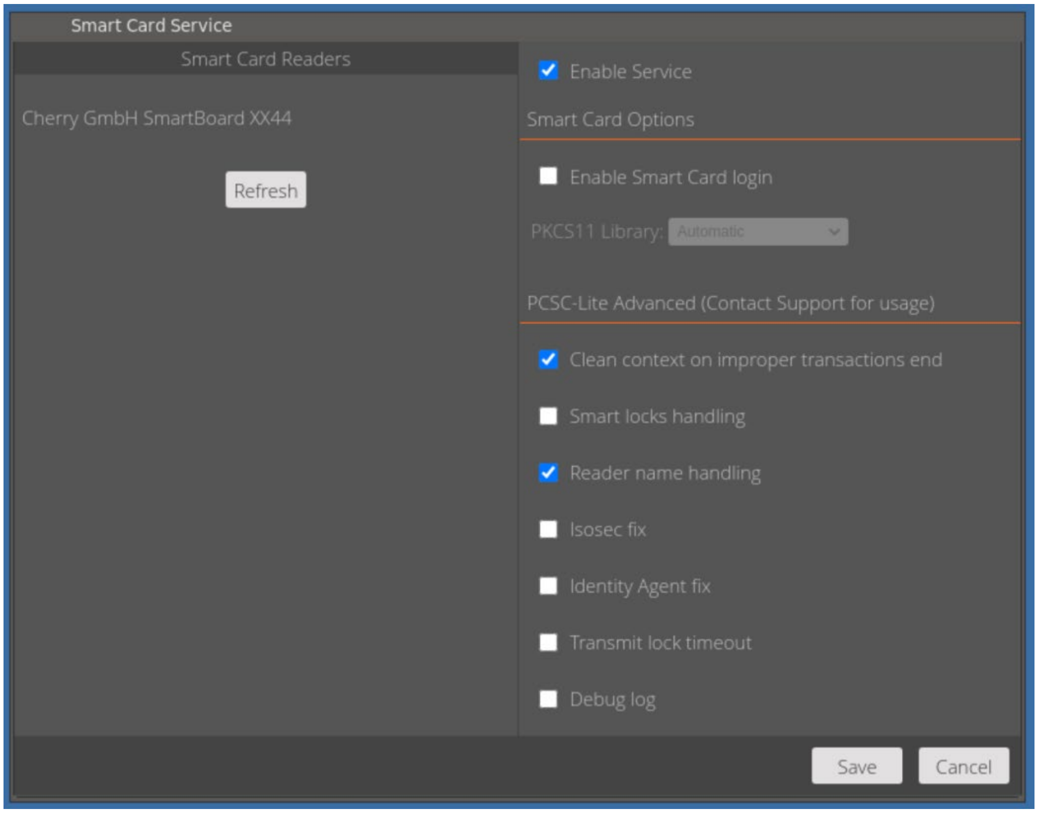


Connected to localhost

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.



Smart Card Service

Smart Card Readers

Cherry GmbH SmartBoard XX44

☑ Enable Service

Smart Card Options

☐ Enable Smart Card login

PKCS11 Library: Automatic

PCSC-Lite Advanced (Contact Support for usage)

☑ Clean context on improper transactions end

☐ Smart locks handling

☑ Reader name handling

☐ Isosec fix

☐ Identity Agent fix

☐ Transmit lock timeout

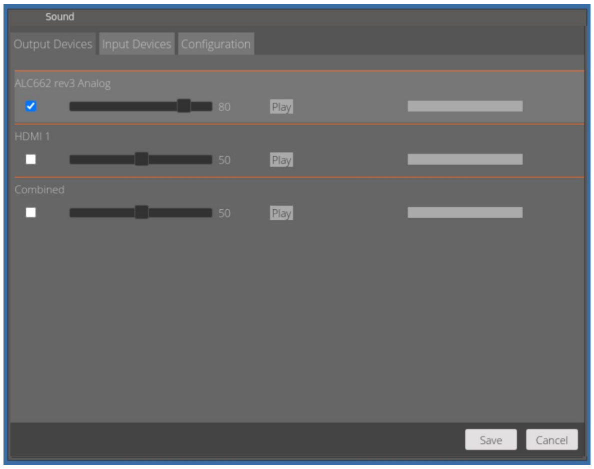
☐ Debug log

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.

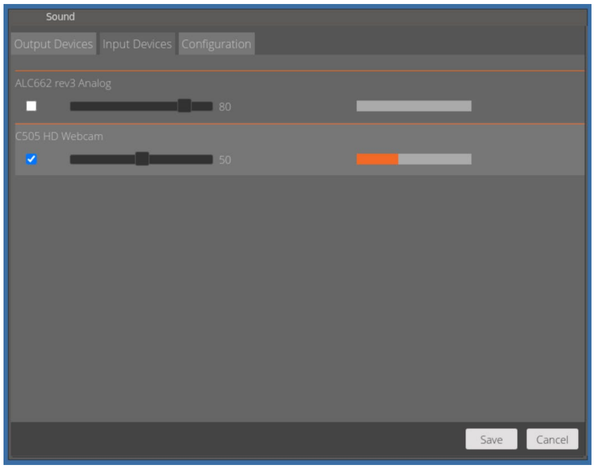
The input devices tab lists all available input devices and lets you select your preferred device for input. This example below displays the integrated microphone of the C505 HD Webcam.



ALC662 rev3 Analog
☑ 80

HDMI 1
☐ 50

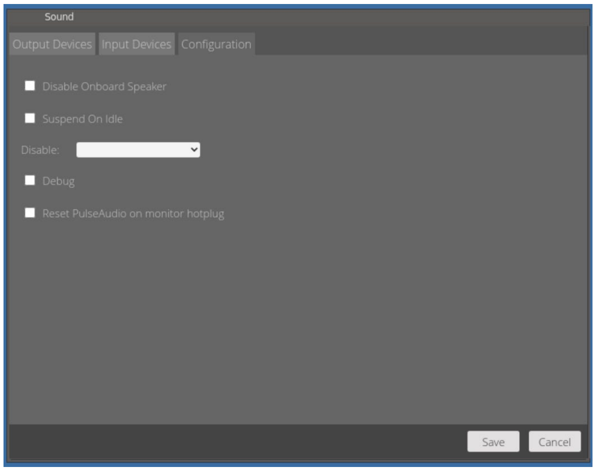
Combined
☐ 50



ALC662 rev3 Analog
☐ 80

C505 HD Webcam
☑ 50

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.



☐ Disable Onboard Speaker

☐ Suspend On Idle

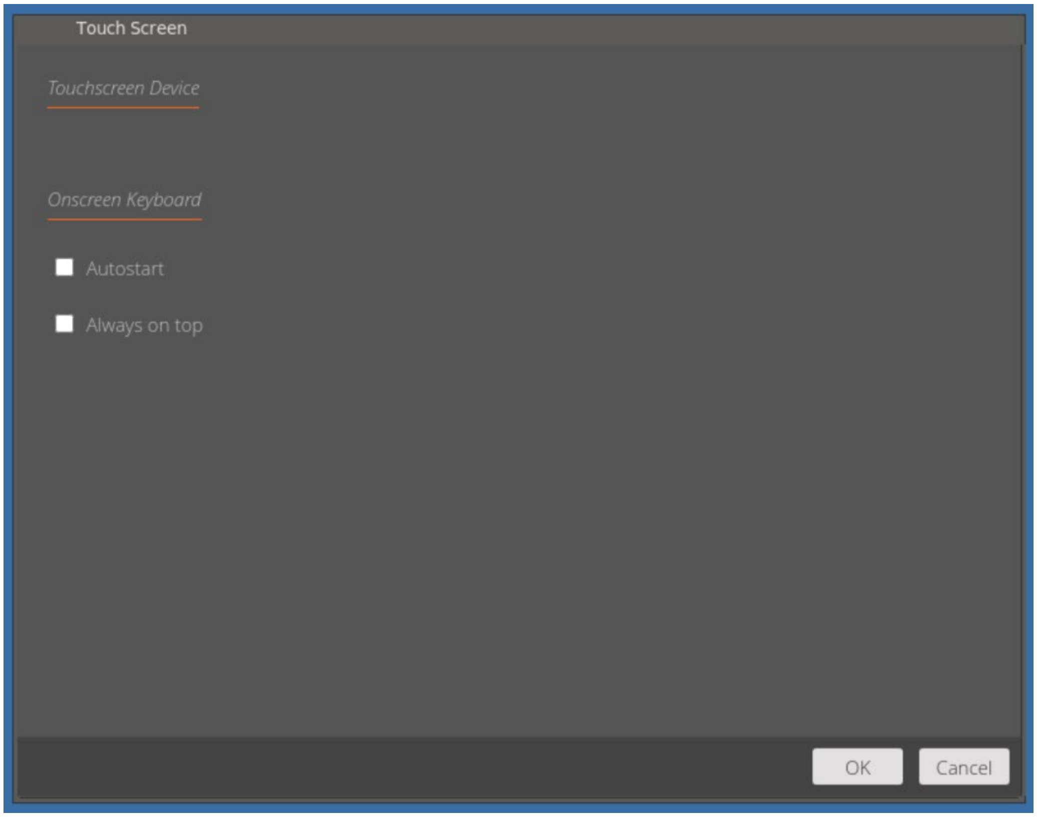
Disable:

☐ Debug

☐ Reset PulseAudio on monitor hotplug

Touch Screen

This is where you can find any touch screen devices that are attached to your Zero Client. You can also set options for the Onscreen keyboard, so that when the screen is plugged in, the onscreen keyboard appears and also that it is "Always on top".



Touch Screen

Touchscreen Device

Onscreen Keyboard

☐ Autostart

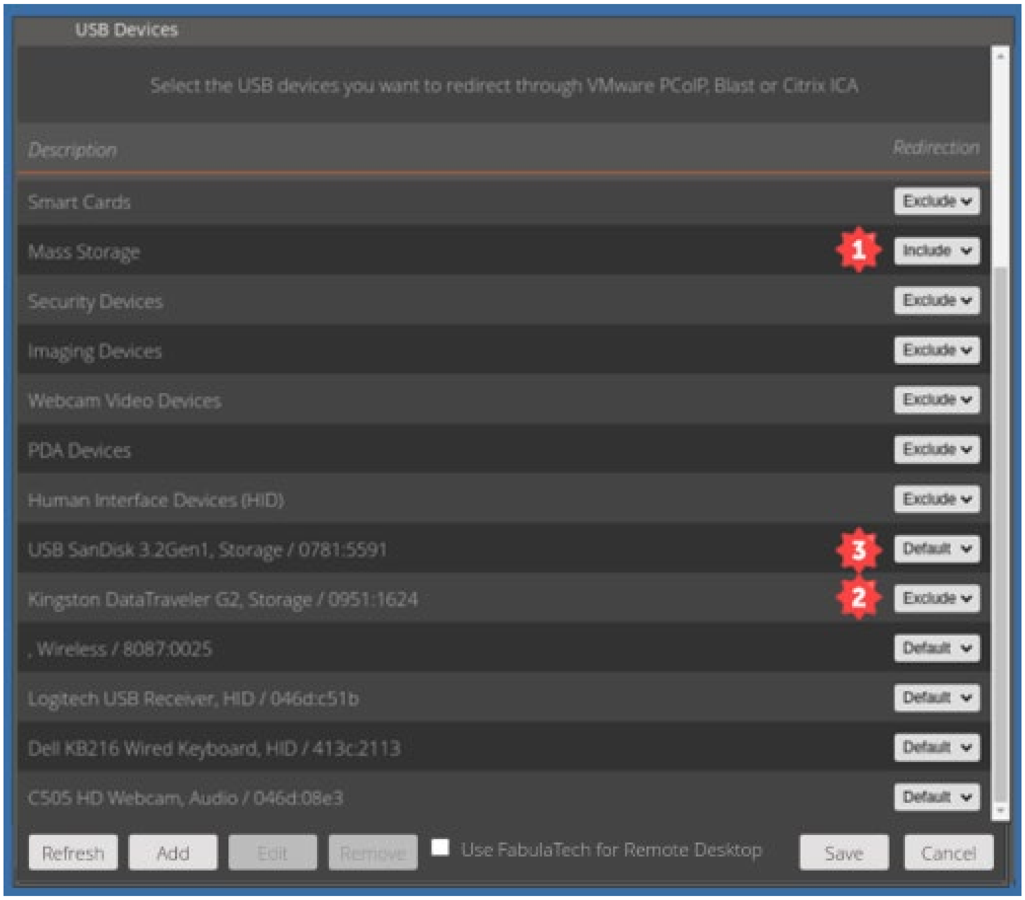
☐ Always on top

USB Devices

USB Devices for VMware 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

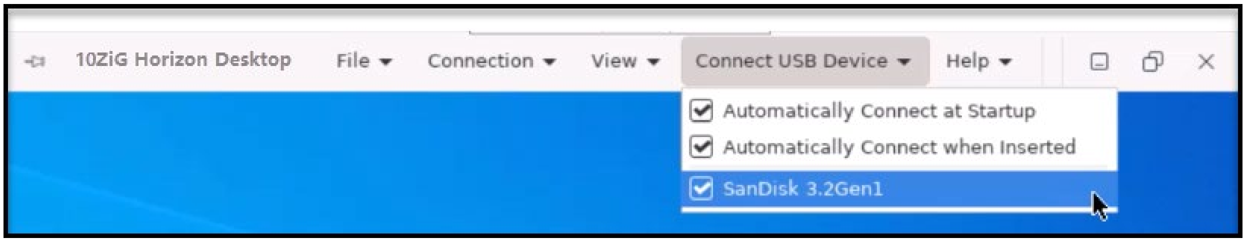


USB Devices

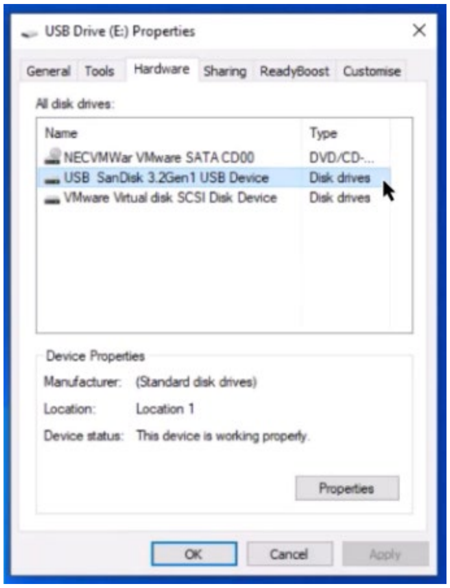
Select the USB devices you want to redirect through VMware PCoIP, Blast or Citrix ICA

Description		Redirection
Smart Cards		Exclude
Mass Storage	1	Include
Security Devices		Exclude
Imaging Devices		Exclude
Webcam Video Devices		Exclude
PDA Devices		Exclude
Human Interface Devices (HID)		Exclude
USB SanDisk 3.2Gen1, Storage / 0781:5591	3	Default
Kingston DataTraveler G2, Storage / 0951:1624	2	Exclude
, Wireless / 8087:0025		Default
Logitech USB Receiver, HID / 046d:c51b		Default
Dell KB216 Wired Keyboard, HID / 413c:2113		Default
C505 HD Webcam, Audio / 046d:08e3		Default

If we then launch a VMware 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.



☑ Automatically Connect at Startup
☑ Automatically Connect when Inserted
☑ SanDisk 3.2Gen1



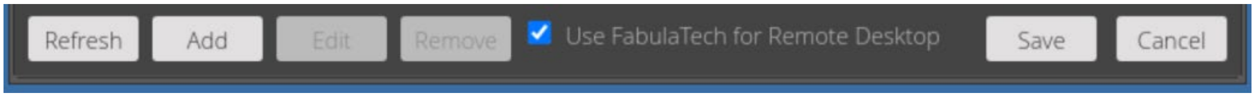
All disk drives:

Name	Type
NECVMWar VMware SATA CD00	DVD/CD-...
USB SanDisk 3.2Gen1 USB Device	Disk drives
VMware Virtual disk SCSI Disk Device	Disk drives

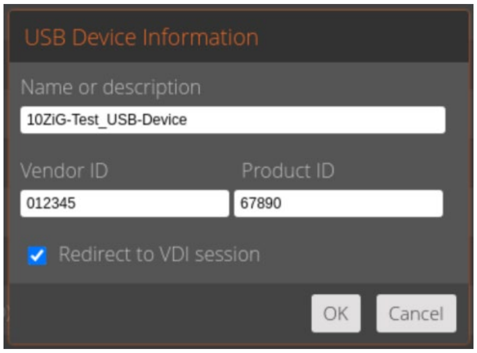
Device Properties

Manufacturer: (Standard disk drives)
Location: Location 1
Device status: This device is working properly.

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.



☑ Use FabulaTech for Remote Desktop



Name or description: 10ZiG-Test_USB-Device

Vendor ID: 012345
Product ID: 67890

☑ Redirect to VDI session

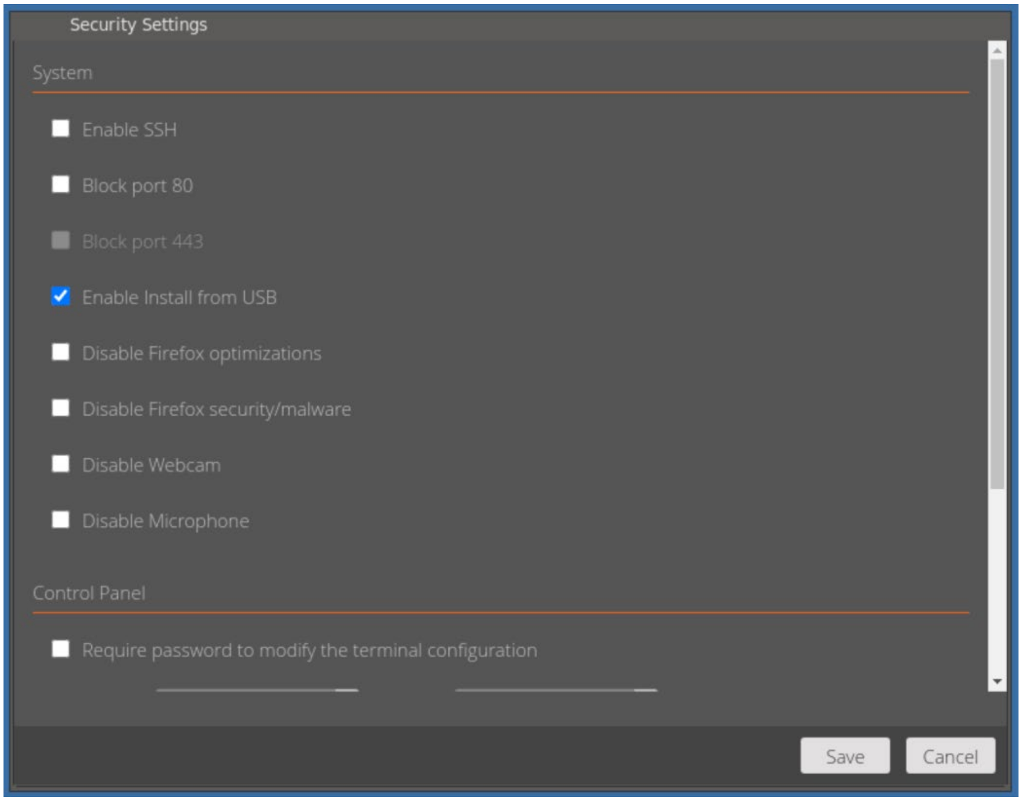
Certificates

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.



Security Settings

System

□ Enable SSH

□ Block port 80

□ Block port 443

☑ Enable Install from USB

□ Disable Firefox optimizations

□ Disable Firefox security/malware

□ Disable Webcam

□ Disable Microphone

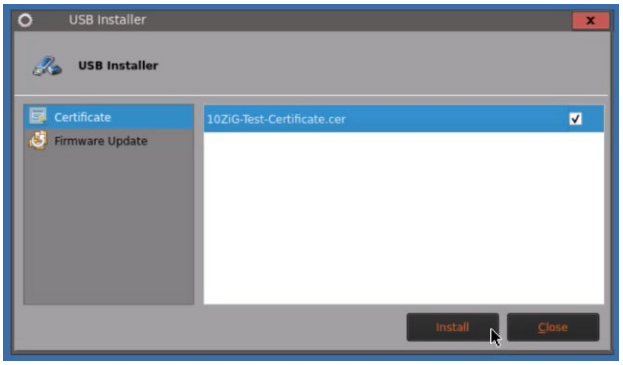
Control Panel

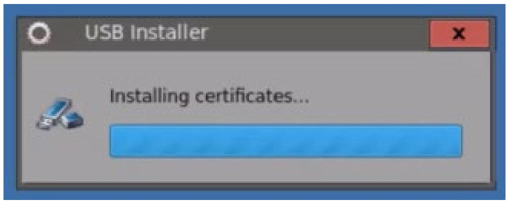
□ Require password to modify the terminal configuration

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.

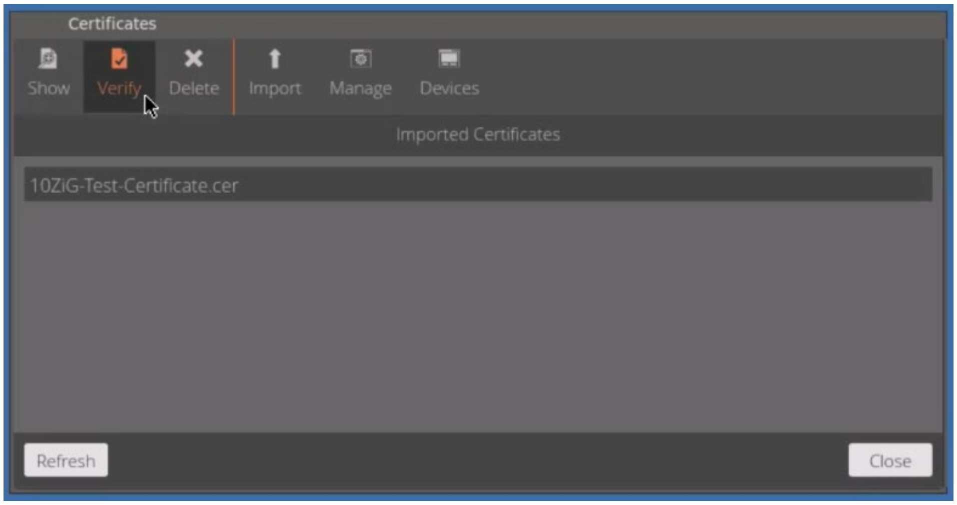
You will see the list of certificates displayed on screen, simply click any that you wish to import and then click “Install”, as below. You should see the “Installing certificates” dialog box and then you’ll be returned to the “USB Installer” dialog box.



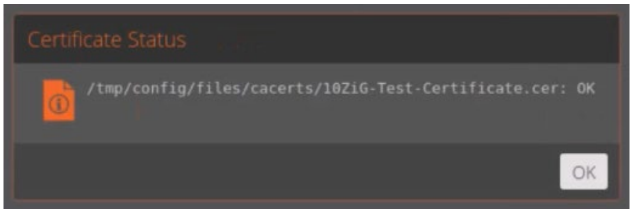


Installing certificates...

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.

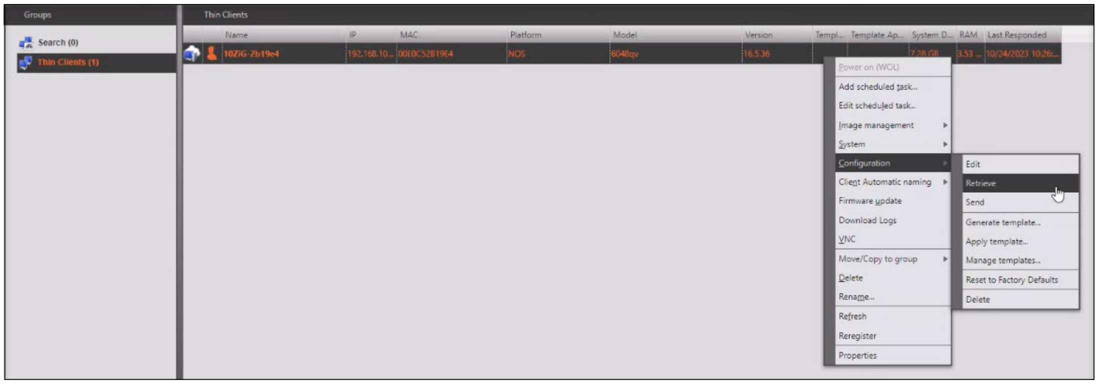


```
/tmp/config/files/cacerts/10ZiG-Test-Certificate.cer: OK
```

Importing a Certificate from the 10ZiG Manager Web Console

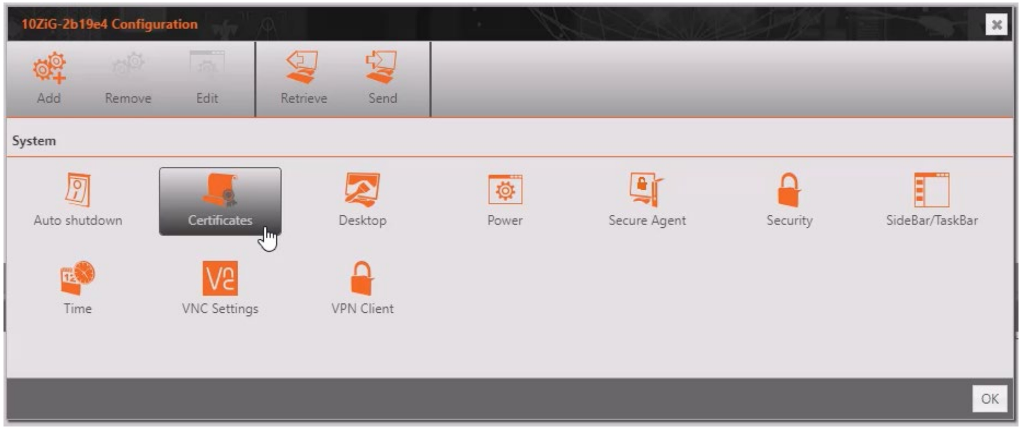
Just as you can import certificates locally on the 10ZiG NOS zero client, you can also import them remotely, by using the “10ZiG Manager Web Console”.

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



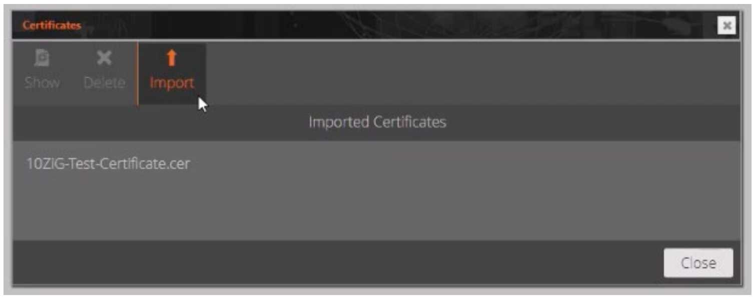
Name	IP	MAC	Platform	Model	Version	Templ...	Template Ap...	System D...	RAM	Last Responded
10ZiG-2b19e4	192.168.10...	00E0C52B19E4	NOS	6048qv	16.5.36			7.28 GB	3.53 ...	10/24/2023 10:26:...

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.



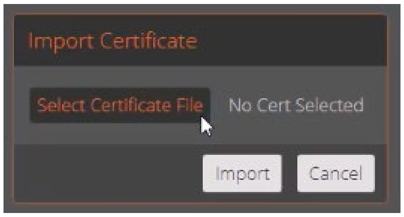
Once the “Certificates” dialog box opens, notice the already installed certificate that we imported locally on the 10ZiG zero client earlier.

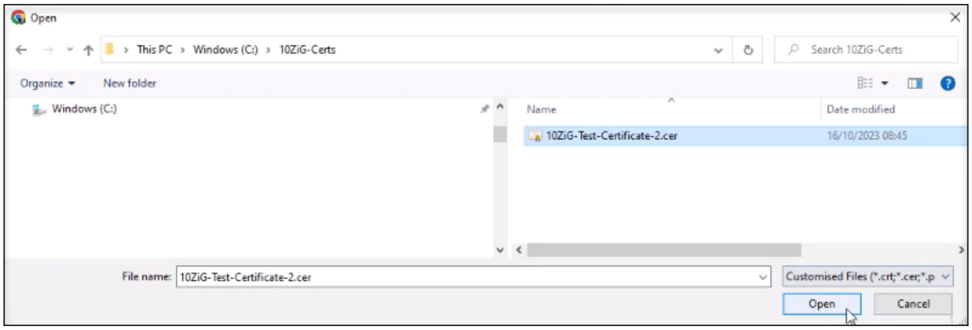
Click “Import” to locate a new certificate that will be saved on the “10ZiG Manager Server” and sent with the next configuration download to the client.



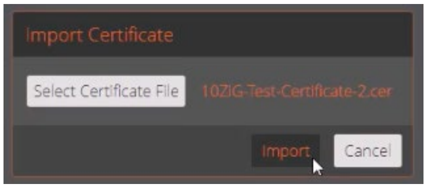
10ZiG-Test-Certificate.cer

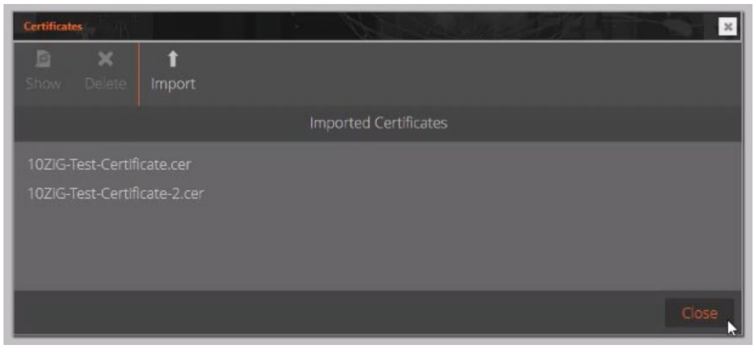
When the “Import Certificate” dialog box appears, just click the “Select Certificate File” button, navigate to the certificate file you wish to import and then click “Open”.




Open
This PC › Windows (C:) › 10ZiG-Certs
Search 10ZiG-Certs
Organize
New folder
Windows (C:)
Name
Date modified
10ZiG-Test-Certificate-2.cer
16/10/2023 08:45
File name:
10ZiG-Test-Certificate-2.cer
Customised Files (*.crt;*.cer;*.p
Open
Cancel

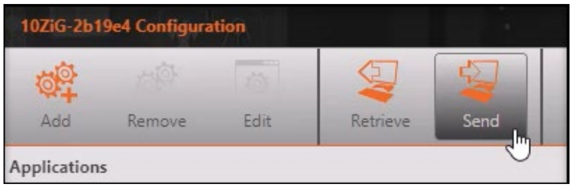
Once the “Import Certificate” dialog show the correct certificate name, just click “Import” and you’ll see the newly imported certificate displayed alongside the original one added locally via USB earlier.

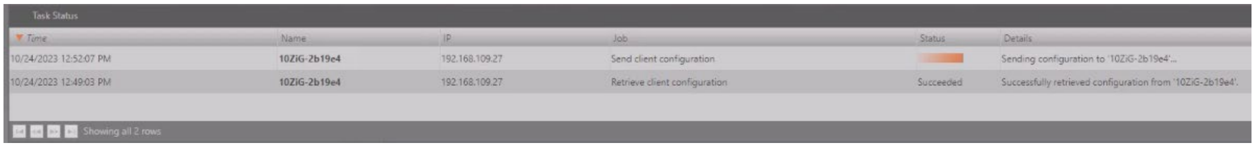




Now that we’ve added a new certificate to the configuration, we need to send it back down to the 10ZiG zero client and then check that it got there successfully.

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.

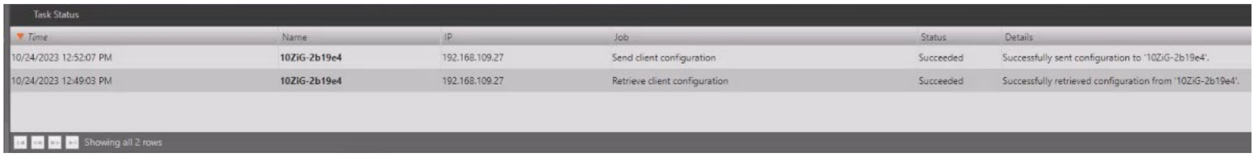




Task Status

Time	Name	IP	Job	Status	Details
10/24/2023 12:52:07 PM	10ZiG-2b19e4	192.168.109.27	Send client configuration		Sending configuration to '10ZiG-2b19e4'...
10/24/2023 12:49:03 PM	10ZiG-2b19e4	192.168.109.27	Retrieve client configuration	Succeeded	Successfully retrieved configuration from '10ZiG-2b19e4'.

Showing all 2 rows

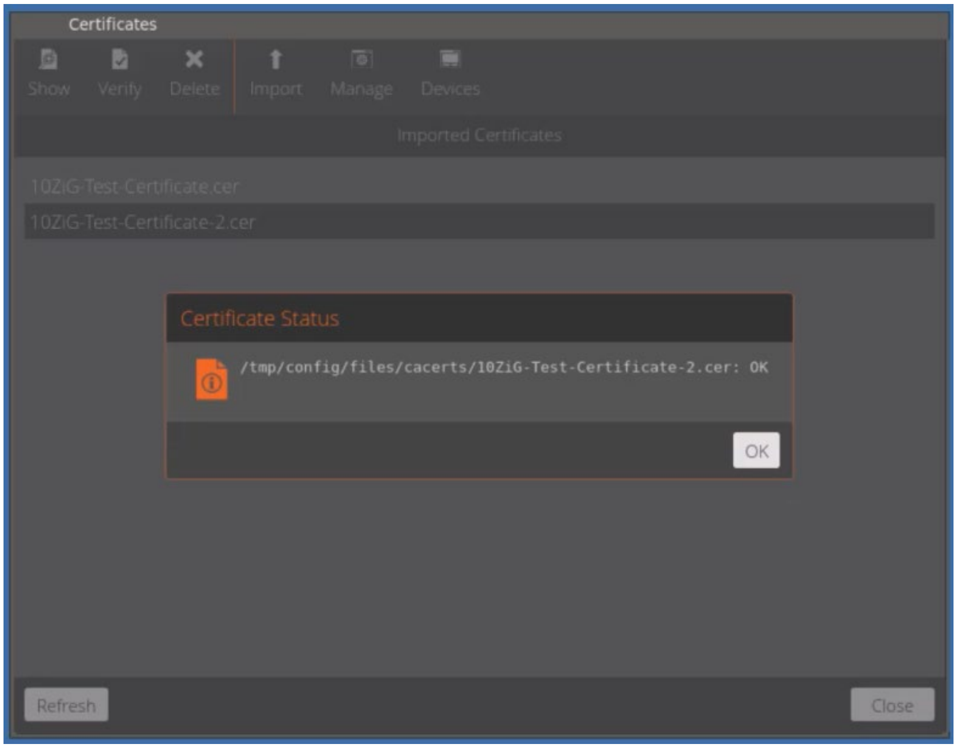


Task Status

Time	Name	IP	Job	Status	Details
10/24/2023 12:52:07 PM	10ZiG-2b19e4	192.168.109.27	Send client configuration	Succeeded	Successfully sent configuration to '10ZiG-2b19e4'.
10/24/2023 12:49:03 PM	10ZiG-2b19e4	192.168.109.27	Retrieve client configuration	Succeeded	Successfully retrieved configuration from '10ZiG-2b19e4'.

Showing all 2 rows

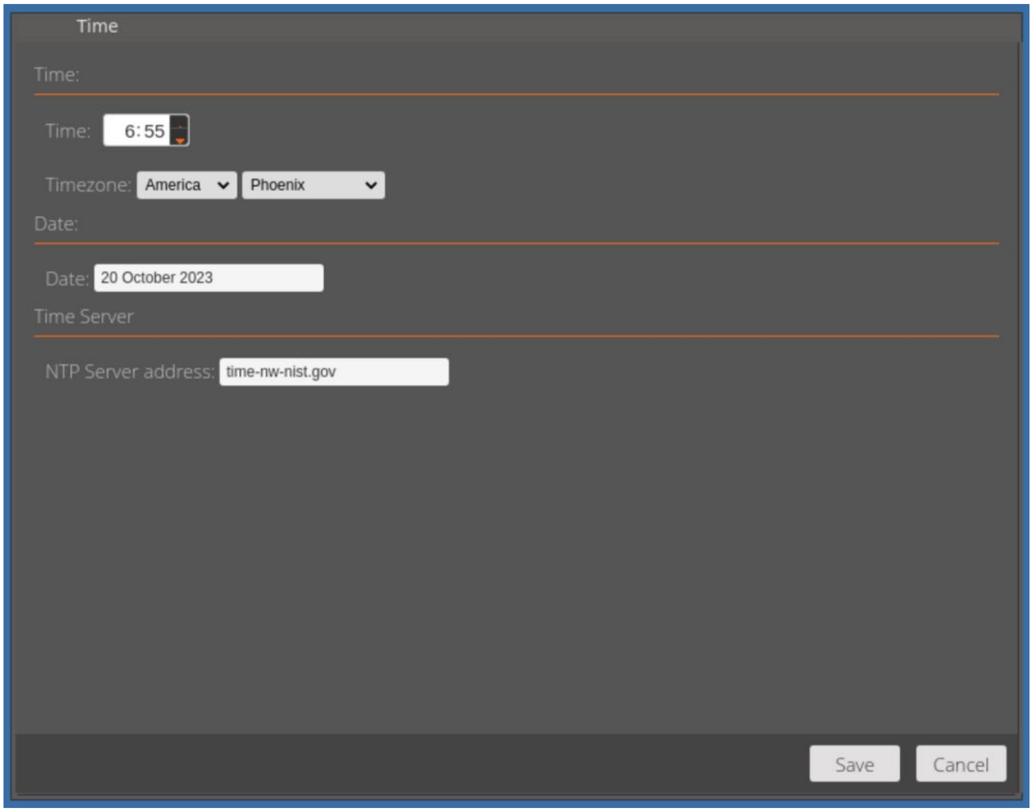
On the 10ZiG zero client again, if we open "Certificates" inside the "Control Panel", we can see that our recently transmitted configuration successfully imported the certificate named "10ZiG-Test-Certifictae-2" and if we highlight it and click "Verify", it checks out successfully as expected.



```
/tmp/config/files/cacerts/10ZiG-Test-Certificate-2.cer: OK
```

Time & Date

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



Time

Time:

Time: 6:55

Timezone: America Phoenix

Date:

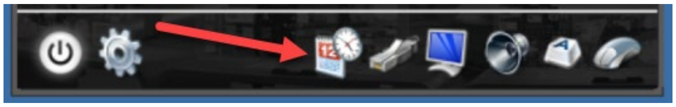
Date: 20 October 2023

Time Server

NTP Server address: time-nw-nist.gov

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-V, NOS-C and NOS-M “Authentication” login boxes, by clicking the “Clock” icon as shown below indicated by the “red arrow”.

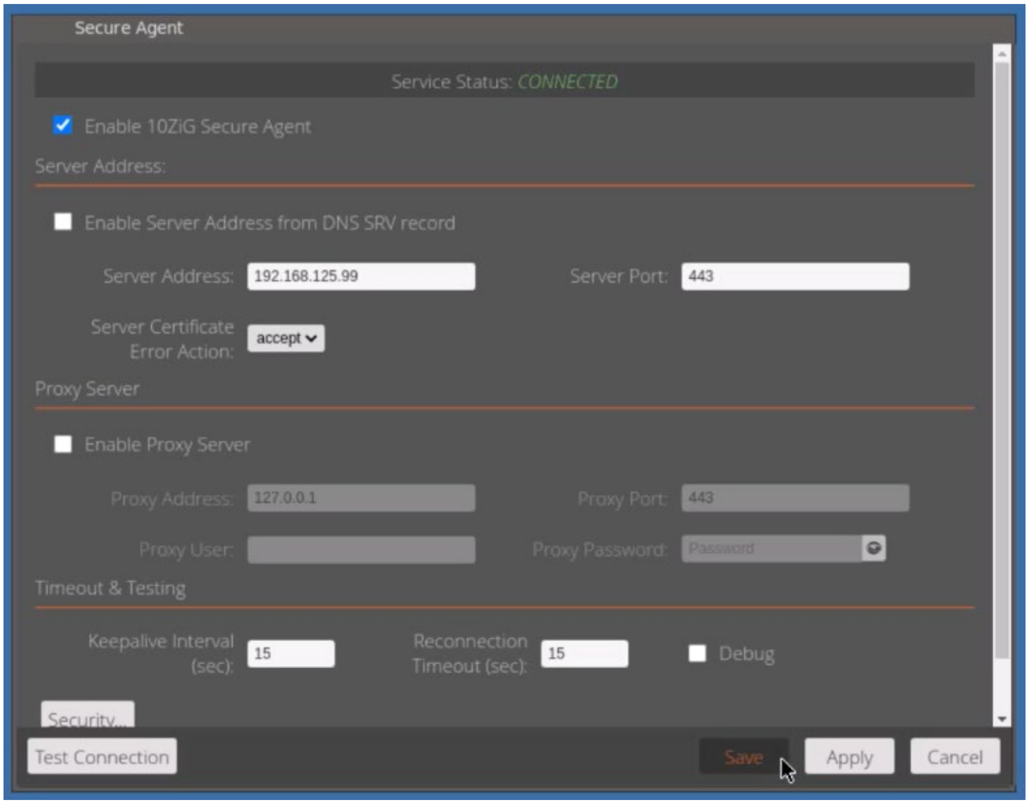


Secure Agent

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.



Secure Agent

Service Status: CONNECTED

☑ Enable 10ZiG Secure Agent

Server Address:

□ Enable Server Address from DNS SRV record

Server Address: 192.168.125.99 Server Port: 443

Server Certificate Error Action: accept

Proxy Server

□ Enable Proxy Server

Proxy Address: 127.0.0.1 Proxy Port: 443

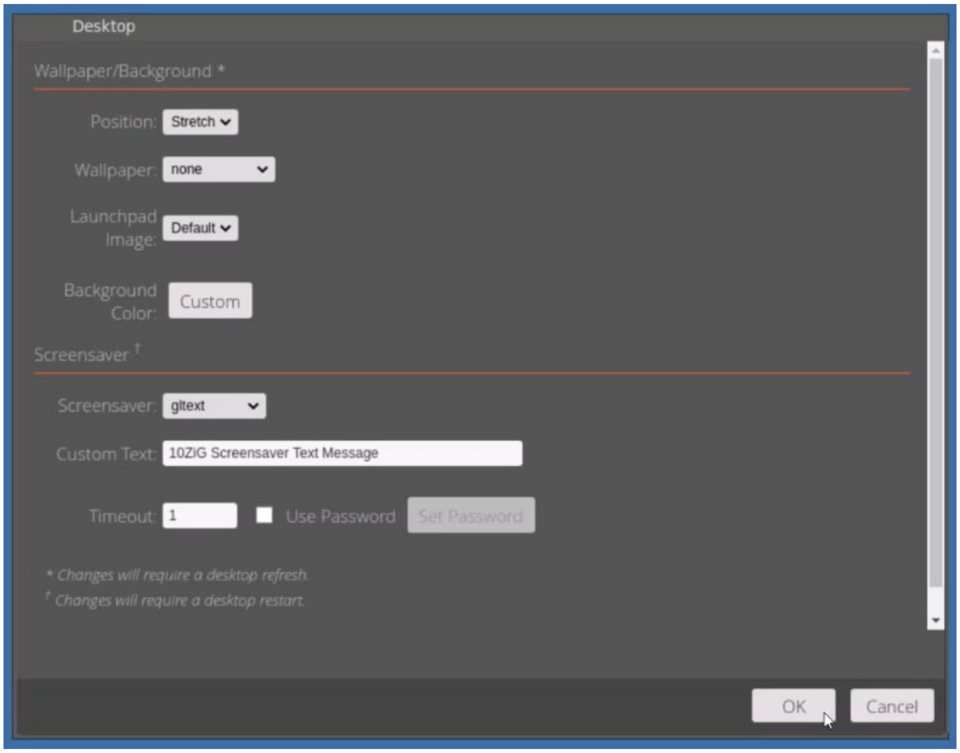
Proxy User: Proxy Password: Password

Timeout & Testing

Keepalive Interval (sec): 15 Reconnection Timeout (sec): 15 □ Debug

Desktop

The desktop functionality allows you to manage the look and feel of your zero client desktops, from the ability to set the wallpaper/background and also a screensaver of your choice. If you want to display some custom text for your screensaver, then you can do this by selecting the screensaver type to be "gltext" and then typing in your own screensaver message to be displayed, in the "Custom Text" box beneath. The "Timeout" value in minutes specifies the inactivity time of mouse and keyboard before the screensaver launches. See the screensaver example below and what the screensaver looks like when it launches.



Desktop

Wallpaper/Background *

Position: Stretch

Wallpaper: none

Launchpad Image: Default

Background Color: Custom

Screensaver †

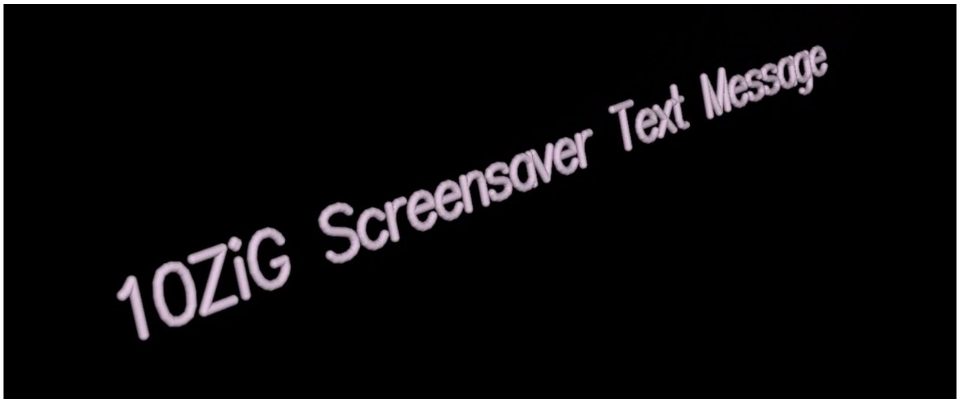
Screensaver: gltext

Custom Text: 10ZiG Screensaver Text Message

Timeout: 1 □ Use Password

* Changes will require a desktop refresh.

† Changes will require a desktop restart.



System Logs

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

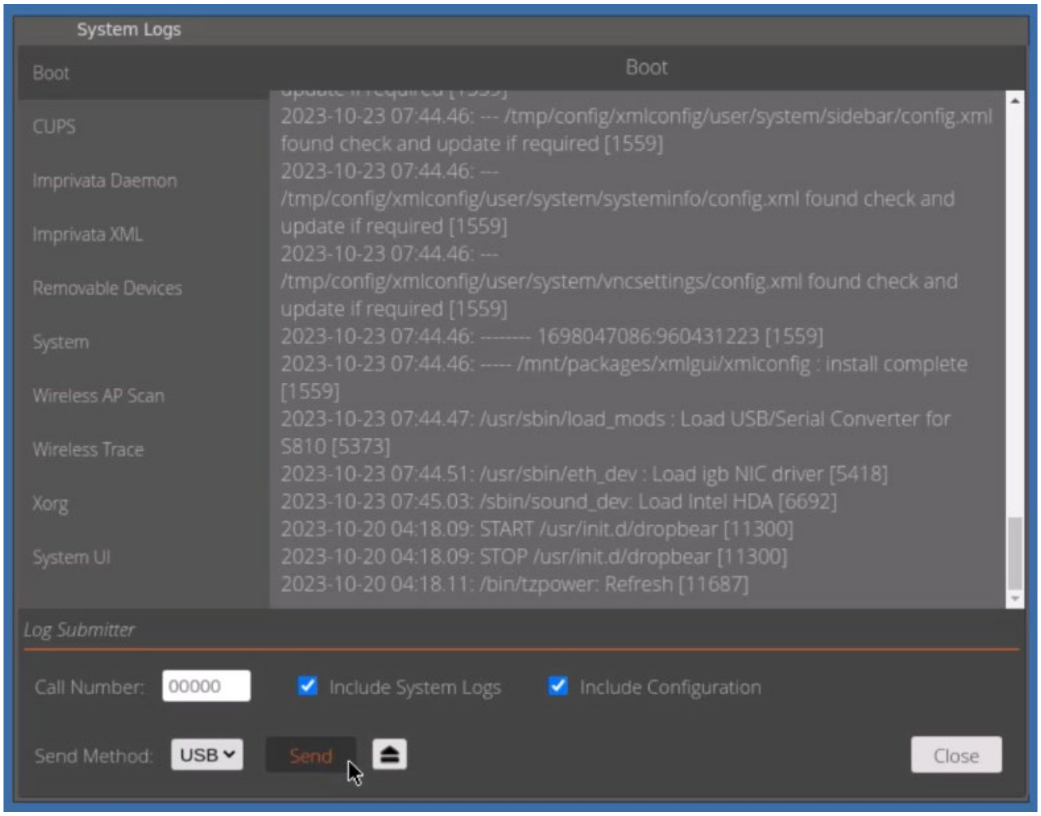
If you wish to send your collated logs to a 10ZiG support technician, you have two ways of doing this, you can either write them to an attached USB device for use later or retrieve them using the “10ZiG Manager Web Console”.

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.



```
2023-10-23 07:44.46: --- /tmp/config/xmlconfig/user/system/sidebar/config.xml
found check and update if required [1559]
2023-10-23 07:44.46: ---
/tmp/config/xmlconfig/user/system/systeminfo/config.xml found check and
update if required [1559]
2023-10-23 07:44.46: ---
/tmp/config/xmlconfig/user/system/vncsettings/config.xml found check and
update if required [1559]
2023-10-23 07:44.46: -------- 1698047086:960431223 [1559]
2023-10-23 07:44.46: ----- /mnt/packages/xmlgui/xmlconfig : install complete
[1559]
2023-10-23 07:44.47: /usr/sbin/load_mods : Load USB/Serial Converter for
S810 [5373]
2023-10-23 07:44.51: /usr/sbin/eth_dev : Load igb NIC driver [5418]
2023-10-23 07:45.03: /sbin/sound_dev: Load Intel HDA [6692]
2023-10-20 04:18.09: START /usr/init.d/dropbear [11300]
2023-10-20 04:18.09: STOP /usr/init.d/dropbear [11300]
2023-10-20 04:18.11: /bin/tzpower: Refresh [11687]
```

Call Number: 00000

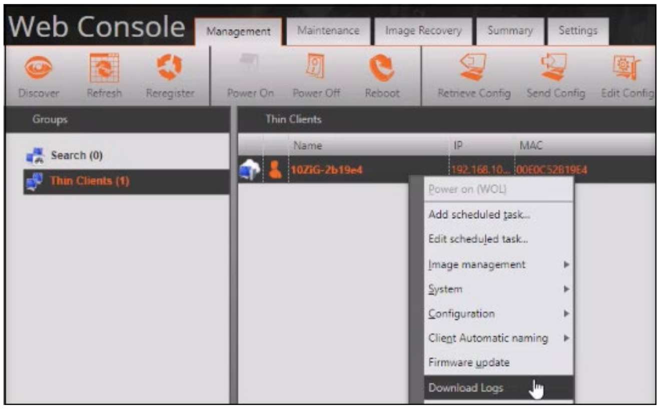
☑ Include System Logs

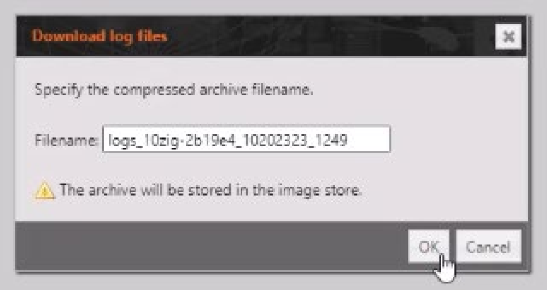
☑ Include Configuration

Send Method: USB

Collecting Logs via the 10ZiG Manager Web Console

Inside the Web Console, right click on your zero 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.



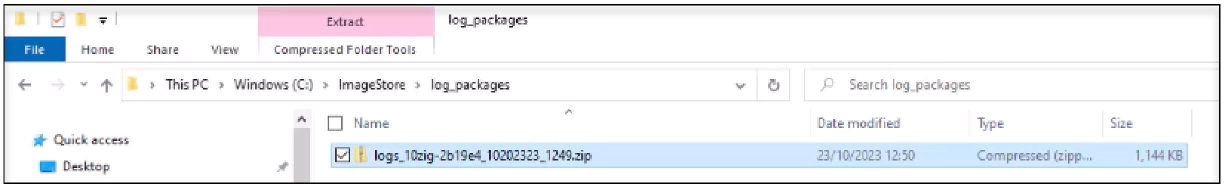


Specify the compressed archive filename.

Filename: logs_10zig-2b19e4_10202323_1249

The archive will be stored in the image store.

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.

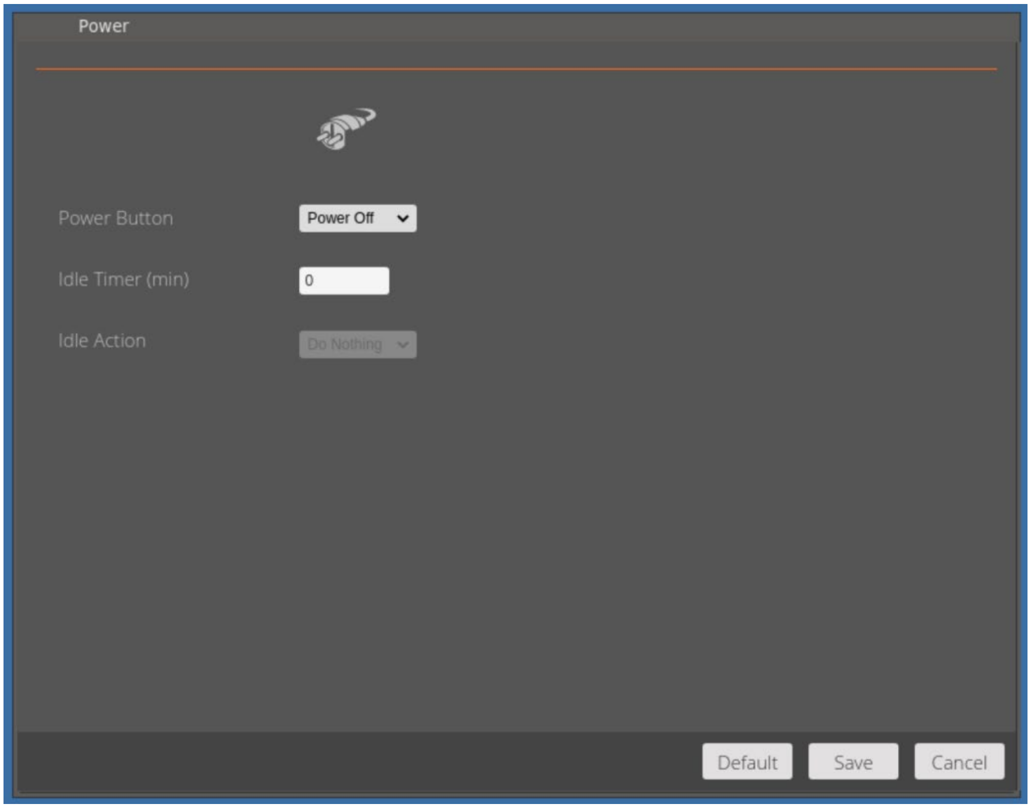


Name	Date modified	Type	Size
☑ logs_10zig-2b19e4_10202323_1249.zip	23/10/2023 12:50	Compressed (zipp...	1,144 KB

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, “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.



Power

Power Button: Power Off

Idle Timer (min): 0

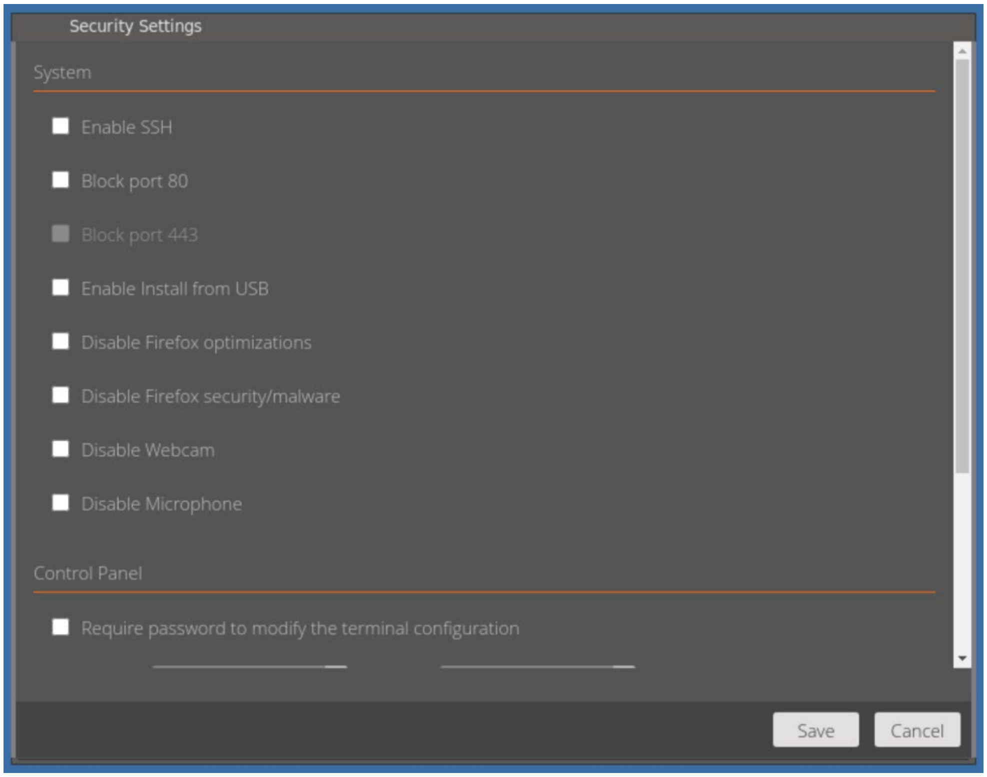
Idle Action: Do Nothing

Security settings

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.



Security Settings

System

□ Enable SSH

□ Block port 80

□ Block port 443

□ Enable Install from USB

□ Disable Firefox optimizations

□ Disable Firefox security/malware

□ Disable Webcam

□ Disable Microphone

Control Panel

□ Require password to modify the terminal configuration

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

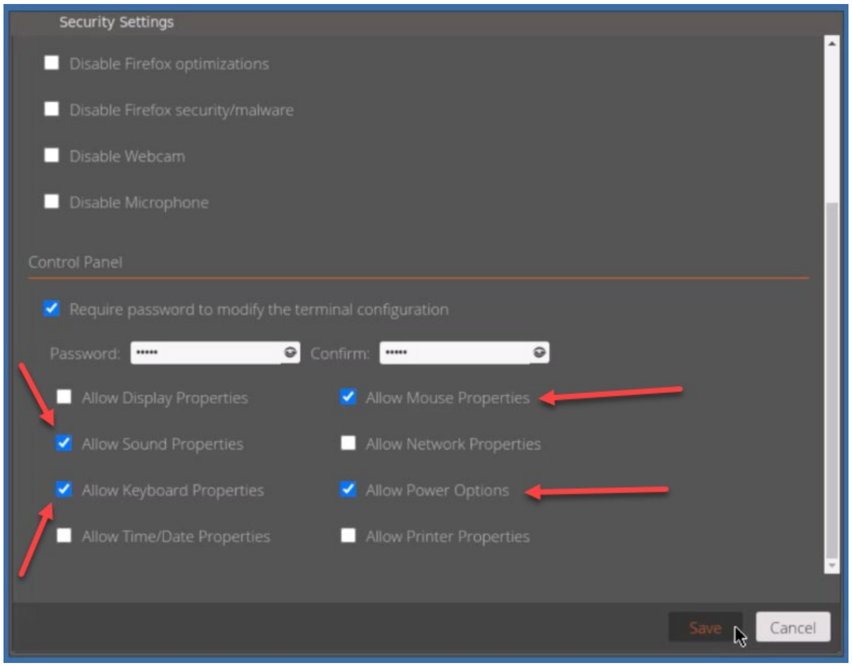
The first one is “Disable Firefox optimizations” and ticking this option will disable some of the background network chatter that Firefox creates when launched. It is recommended to enable this option if you experience network issues due to “boot storms” / “login storms” when all units are opening Firefox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

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.



Security Settings

□ Disable Firefox optimizations

□ Disable Firefox security/malware

□ Disable Webcam

□ Disable Microphone

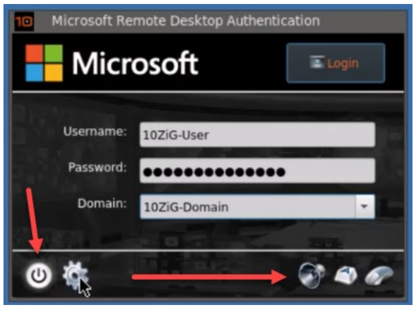
Control Panel

☑ Require password to modify the terminal configuration

Password: ••••• Confirm: •••••

□ Allow Display Properties	☑ Allow Mouse Properties
☑ Allow Sound Properties	□ Allow Network Properties
☑ Allow Keyboard Properties	☑ Allow Power Options
□ Allow Time/Date Properties	□ Allow Printer Properties

If you “Save” those options and then close and re-open the Control Panel using the “Gears” icon in the login Launchpad(below), then you’ll have to enter the previously set password(above) to gain access to the Control Panel window.

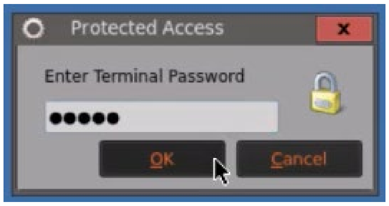


Microsoft Remote Desktop Authentication

Username: 10ZiG-User

Password: ••••••••••••••

Domain: 10ZiG-Domain



Protected Access

Enter Terminal Password

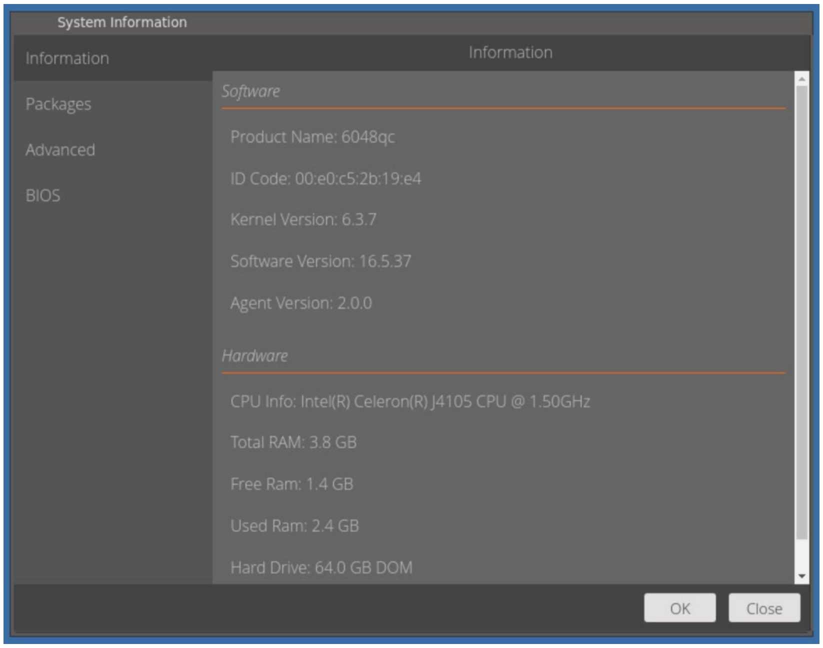
●●●●●

Also notice that you only have access to “Sound”, “Keyboard”, “Mouse” and “Power” options from the launchpad, that were ticked in the Control Panel options in the “Security Settings” previously. See the red arrows above.

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.



Software

Product Name: 6048qc

ID Code: 00:e0:c5:2b:19:e4

Kernel Version: 6.3.7

Software Version: 16.5.37

Agent Version: 2.0.0

Hardware

CPU Info: Intel(R) Celeron(R) J4105 CPU @ 1.50GHz

Total RAM: 3.8 GB

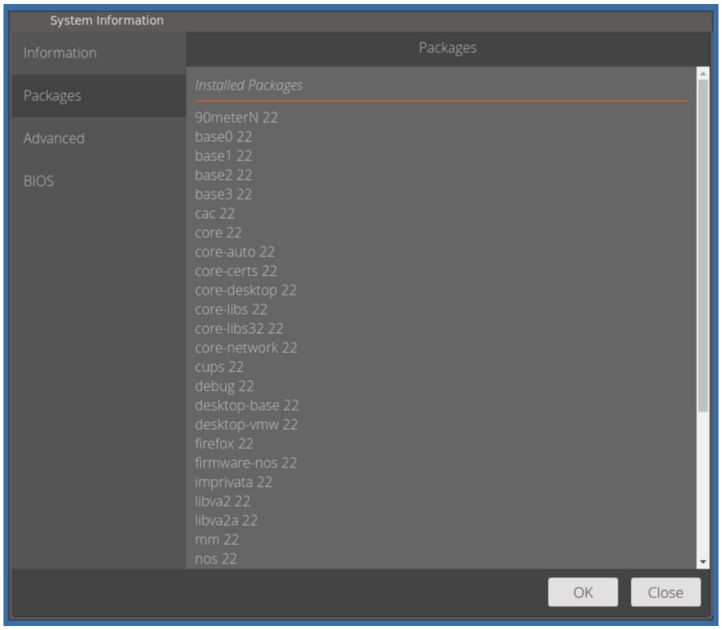
Free Ram: 1.4 GB

Used Ram: 2.4 GB

Hard Drive: 64.0 GB DOM

Packages

Selecting Packages will show the currently installed Linux packages on the zero client.

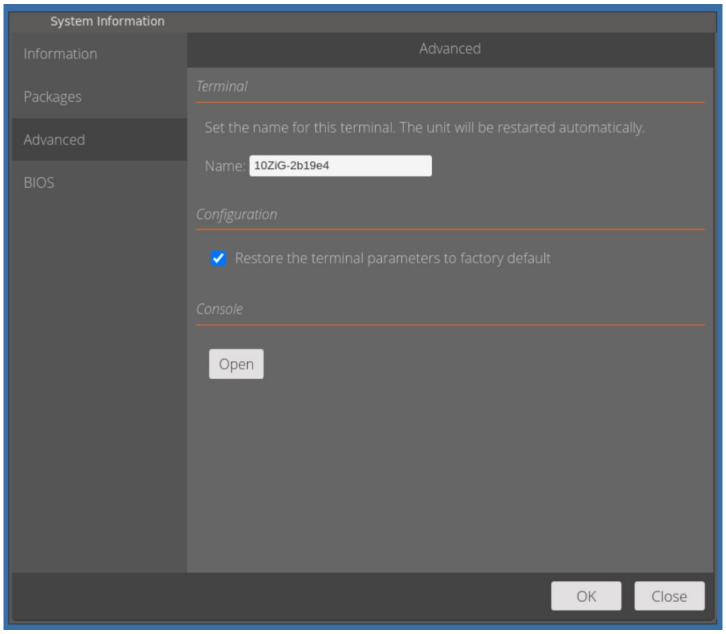


Installed Packages

```
90meterN 22
base0 22
base1 22
base2 22
base3 22
cac 22
core 22
core-auto 22
core-certs 22
core-desktop 22
core-libs 22
core-libs32 22
core-network 22
cups 22
debug 22
desktop-base 22
desktop-vmw 22
firefox 22
firmware-nos 22
imprivata 22
libva2 22
libva2a 22
mm 22
nos 22
```

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.



System Information

Advanced

Terminal

Set the name for this terminal. The unit will be restarted automatically.

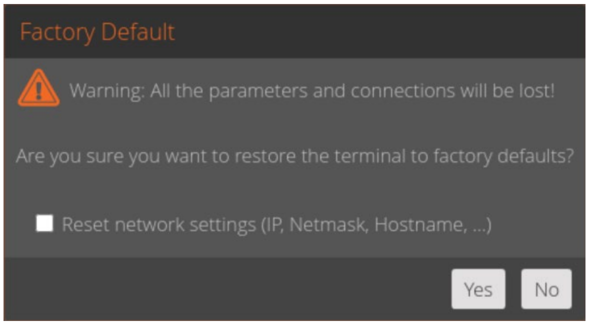
Name: 10ZiG-2b19e4

Configuration

☑ Restore the terminal parameters to factory default

Console

Factory Default message



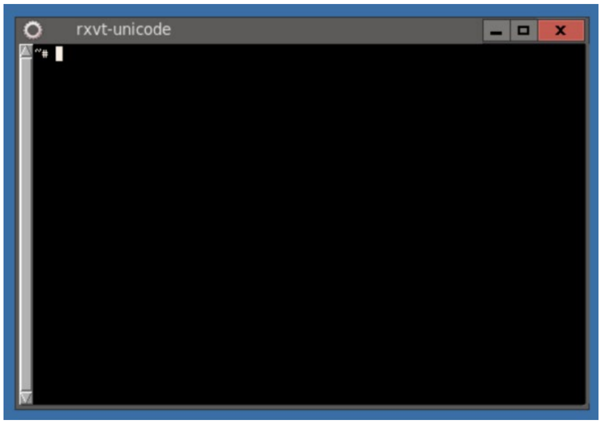
Factory Default

Warning: All the parameters and connections will be lost!

Are you sure you want to restore the terminal to factory defaults?

☐ Reset network settings (IP, Netmask, Hostname, ...)

Console Screen



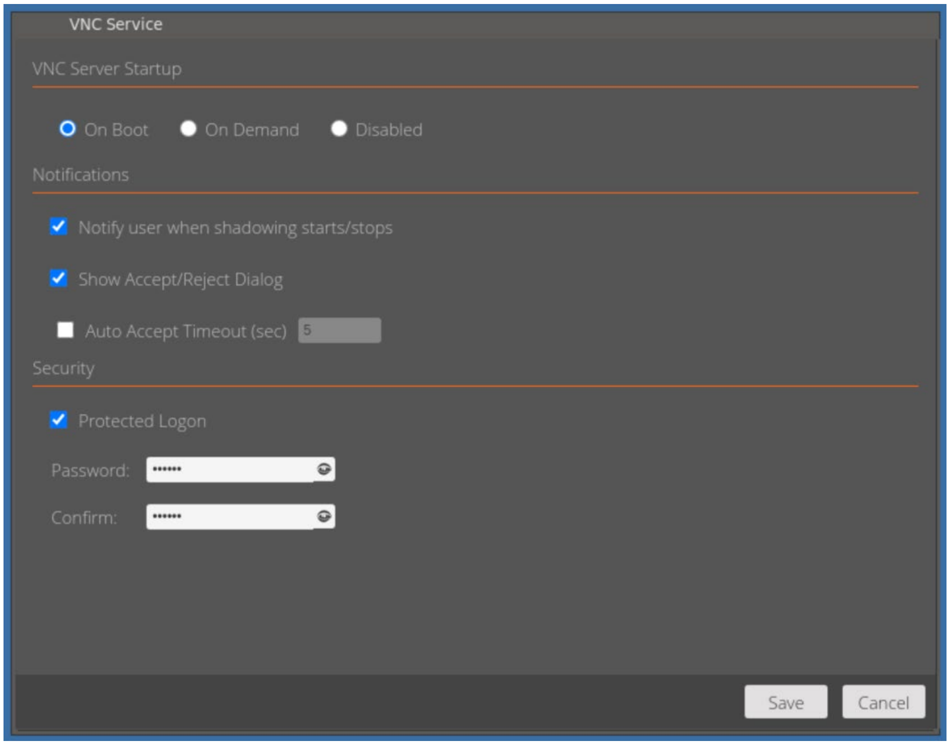
rxvt-unicode

```
~# 
```

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. You can choose to show and accept or reject dialog to the user from the client connection and auto-accept after a timeout period.

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



VNC Service

VNC Server Startup

● On Boot ○ On Demand ○ Disabled

Notifications

☑ Notify user when shadowing starts/stops

☑ Show Accept/Reject Dialog

□ Auto Accept Timeout (sec) 5

Security

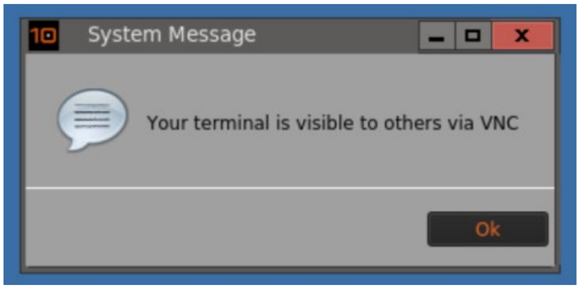
☑ Protected Logon

Password: ••••••

Confirm: ••••••

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.

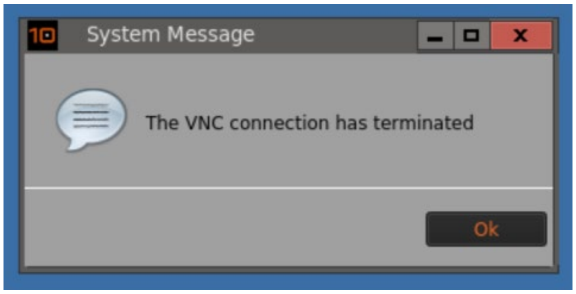
Start Shadowing



System Message

Your terminal is visible to others via VNC

End Shadowing



System Message

The VNC connection has terminated

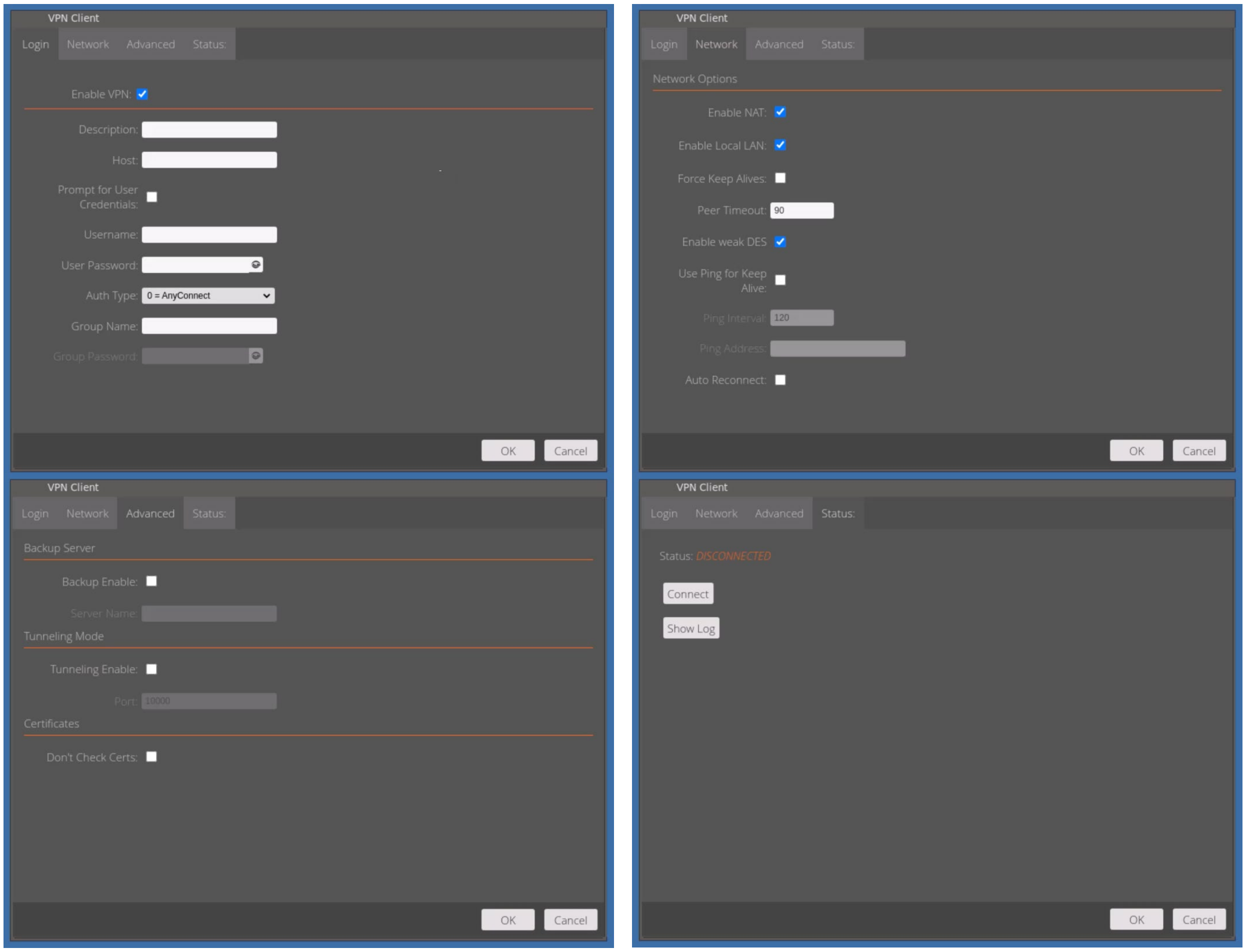
VPN Client

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



Enable VPN: ☑
Description:
Host:
Prompt for User Credentials: □
Username:
User Password:
Auth Type: 0 = AnyConnect
Group Name:
Group Password:

Network Options
Enable NAT: ☑
Enable Local LAN: ☑
Force Keep Alives: □
Peer Timeout: 90
Enable weak DES ☑
Use Ping for Keep Alive: □
Ping Interval: 120
Ping Address:
Auto Reconnect: □

Backup Server
Backup Enable: □
Server Name:
Tunneling Mode
Tunneling Enable: □
Port: 10000
Certificates
Don't Check Certs: □

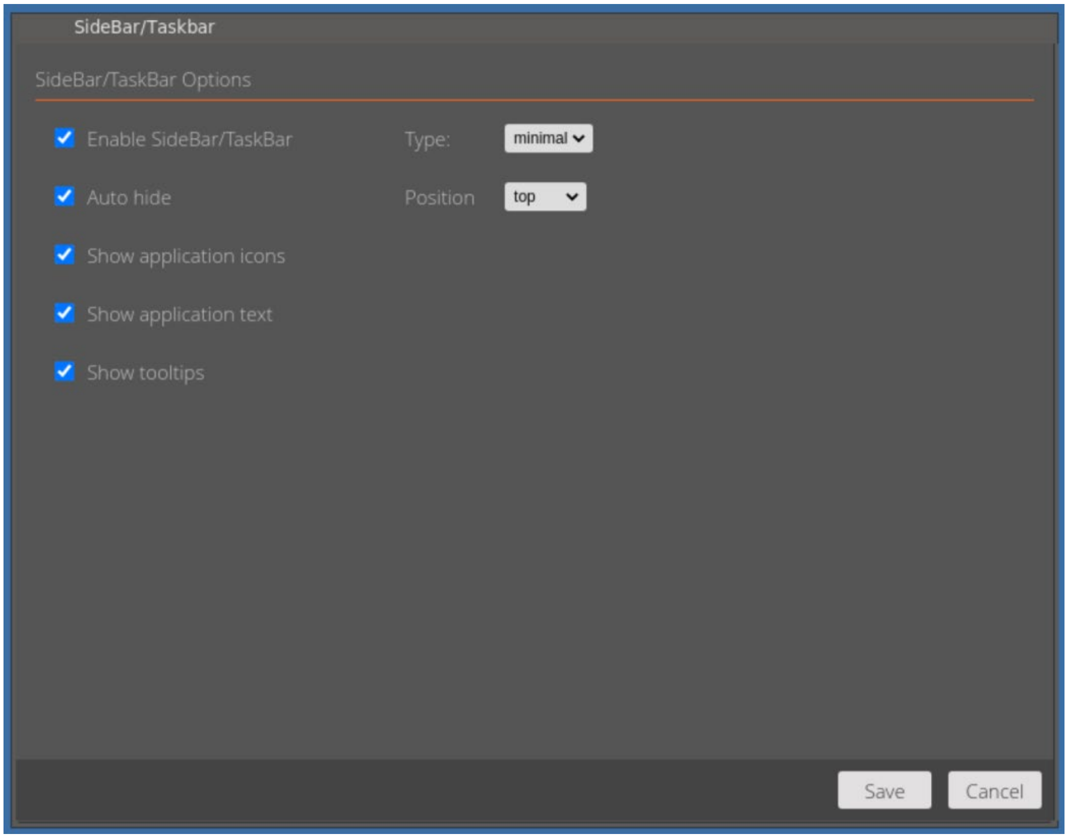
Status: DISCONNECTED

SideBar/TaskBar

SideBar TaskBar

Enabling the SideBar/Taskbar gives you the ability see the current windowed tasks running on your 10ZiG zero 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.



SideBar/Taskbar

SideBar/TaskBar Options

☑ Enable SideBar/TaskBar

Type: minimal

☑ Auto hide

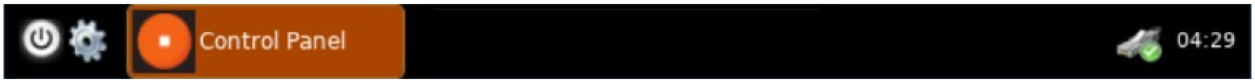
Position top

☑ Show application icons

☑ Show application text

☑ Show tooltips

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 http://faq.10zigsupport.com.