What's New in 21.10

This release contains new features, bug fixes and security updates.

Added Smart Card Support

Added support for the following Thales smart cards:

- IDPrime 930 FIPS 140 L2
- IDPrime 930 FIPS 140 L3
- IDPrime 3930 FIPS 140 L2
- IDPrime 940
- IDPrime 3940
- eToken 5110

Increased Number of AWS Registration Codes Cached Entries from 10 to 50

Overview

The PCoIP® Zero Client Firmware Administrators' Guide provides administrators the necessary information to configure and deploy PCoIP Zero Clients. It provides configuration steps for connecting to a variety of hosts, and contains links to related documentation that may be required to successfully complete a PCoIP solution. It assumes thorough knowledge of conventions and networking concepts, including firewall configuration and the PCoIP protocol.

Who Should Read This Guide?

This guide is written for IT administrators who are managing and configuring Tera2 PCoIP® Zero Clients in a PCoIP environment.

Understanding Terms and Conventions in Teradici guides

For information on the industry specific terms, abbreviations, text conventions, and graphic symbols used in this guide, see Using Teradici Product and Component Guides and the Teradici Glossary.

Using This Guide

This guide explains how to configure Tera2 PCoIP Zero Client firmware for this release. This guide describes your Tera2 PCoIP Zero Client's capabilities, and explains how to set up, configure, and manage your Tera2 PCoIP Zero Client. It also answers frequently asked questions.

Use the following list for quick access to the topics covered in this guide:

- Who Should Read This Guide?: Outlines the document's intended readers and provides industry specific terms, abbreviations, text conventions, and graphic symbols used in this guide that you may find useful.
- Introducing Your Tera2 PCoIP Zero Client: Describes the main features of the Tera2 PCoIP Zero Client, outlines the peripherals you can attach to it, and lists the hosts the Tera2 PCoIP Zero Client can connect to. You'll also learn about the configuration tools—the pre-session display, and the Teradici PCoIP Management Console—and learn about support for common features under typical deployment scenarios.
- Setting Up Your Tera2 PCoIP Zero Client: Describes how to set up your Tera2 PCoIP Zero Client, and outlines what you need to do to secure the Tera2 PCoIP Zero Client.
- Establishing a PCoIP Connection: Shows you how to connect to a PCoIP agent, PCoIP Remote Workstation Card, Amazon Spokesperson, or Horizon Desktops, and how to disconnect from a PCoIP session.
- Managing Your Tera2 PCoIP Zero Client Describes all the settings you can configure using your Tera2 PCoIP Zero Client's pre-session display, Administrative Web Interface (AWI), and the Teradici PCoIP Management Console. This section also describes how to connect to an endpoint manager, view information about your Tera2 PCoIP Zero Client, reset the device, and upload certificates and firmware.

Getting More Information

In addition to this guide, the Tera2 PCoIP Zero Client documentation includes Release Notes

For detailed information on using the PCoIP Management Console to manage deployments with large numbers of PCoIP Zero Clients and Remote Workstation Cards, see the PCoIP® Management Console Administrators' Guide.

For information on installing and configuring additional Tera2 Remote Workstation Cards and Tera2 PCoIP Zero Clients so that you can use additional monitors on your desk, see Tera2 PCoIP® Multi-Monitor Deployment Guide.

For information about administering PCoIP hosts, see one of the following Administrators' Guides:

Windows Hosts

- Teradici PCoIP® Standard Agent for Windows Administrators' Guide
- Teradici PCoIP® Graphics Agent for Windows Administrators' Guide

Linux Hosts

- Teradici PCoIP® Standard Agent for Linux Administrators' Guide
- Teradici PCoIP® Graphics Agent for Linux Administrators' Guide

Remote Workstation Card Hosts

- Remote Workstation Card Firmware Administrators' Guide

Release Notes

Release Notes for PCoIP Zero Client firmware releases can be found at the Teradici support site on the release notes page.

About the Tera2 PCoIP Zero Client

This section provides an overview of your Tera2 PCoIP Zero Client. It also describes the devices and PCoIP hosts that can connect to it, introduces the tools you use to manage your Tera2 PCoIP Zero Client, and summarizes support for common features under typical deployment scenarios.

Introducing Your Tera2 PCoIP Zero Client

Tera2 PCoIP Zero Clients are hardware and firmware-based endpoints that enable users to connect remotely to Workstations using the PCoIP protocol. Workstations use PCoIP Remote Workstation Cards or run Teradici Cloud Access Software while Amazon WorkSpaces desktops, and VMware Horizon desktops use an agent that supports the PCoIP protocol. Since Zero Clients do not have general purpose CPUs, local data storage, or application operating systems, they are very secure and easy to manage. Tera2 PCoIP Zero Clients contain upgradable firmware that enables you to customize your client with new features.

Tera2 PCoIP Zero Clients come in many forms, such as small stand-alone devices, PCoIP integrated displays, and touch-screen monitors. They support multiple wide-screen formats, HD audio and local USB peripherals, and are IPv6-ready. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards, smart cards, and One-Time-Passwords (OTP).

Tera2 PCoIP Zero Clients are powered by a single TERA2321 or TERA2140 processor.

Advanced Encryption Standard (AES) is employed for PCoIP session encryption. Tera2 PCoIP Zero Clients support AES-256-GCM encryption. For more information, see Encryption Settings.

About the Management Tools

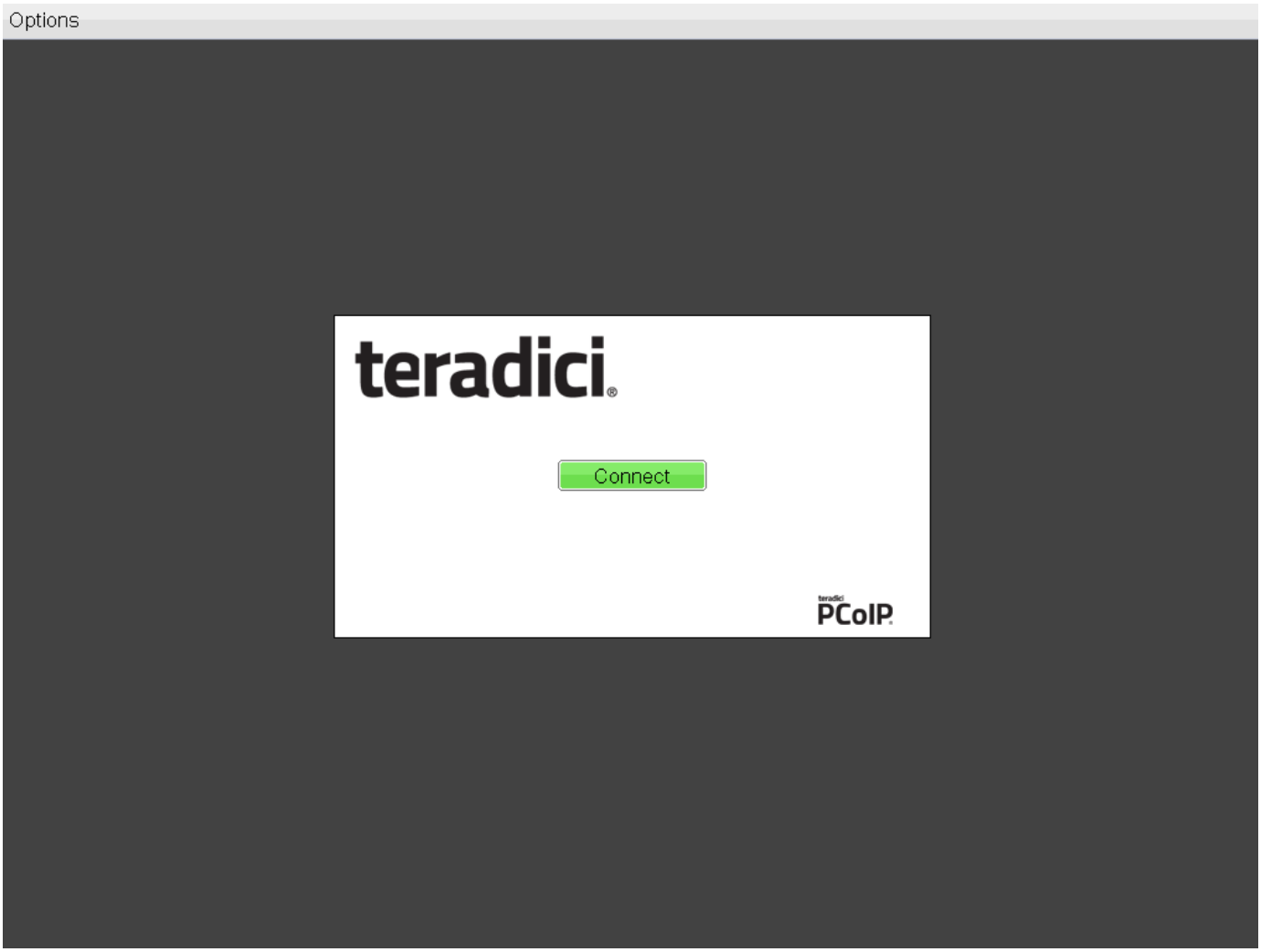
The following configuration and administrative management tools are available for PCoIP Zero Clients:

- **PCoIP On-Screen Display (OSD):** The PCoIP Zero Client's pre-session built-in interface for configuring the device's firmware. For more information, see About the PCoIP On-Screen Display.
- **PCoIP Administrative Web Interface (AWI):** A web-based interface for configuring a specific PCoIP Zero Client's firmware remotely after typing the client's IP address into the browser's address bar. For more information, see About the PCoIP Administrative Web Interface.
- **PCoIP Zero Client Administrative Management Software:** A management tool for configuring and managing multiple PCoIP Zero Clients remotely. Teradici's management software is the PCoIP Management Console. For further information see PCoIP Management Console, or see PCoIP® Management Console Administrators' Guide for configuration and technical procedures.

> **Secure Environments**
>
> Use the PCoIP Management Console in secure environments to configure and manage your Zero Clients after disabling the Zero Client AWI and OSD Configuration selections.

About the PCoIP On-Screen Display

The PCoIP On-Screen Display (OSD) is a graphical user interface (GUI) embedded within the client. It displays when the client is powered on and a PCoIP session is not in progress. The only exception to this is when the client is configured for a managed startup or auto-reconnect.



OSD main window

An **Options** menu at the top-left enables users to access various sub-menus to configure the client and view information about it. A **Connect** button in the center of the window enables users to connect the client to a virtual desktop or to a PCoIP Remote Workstation Card.

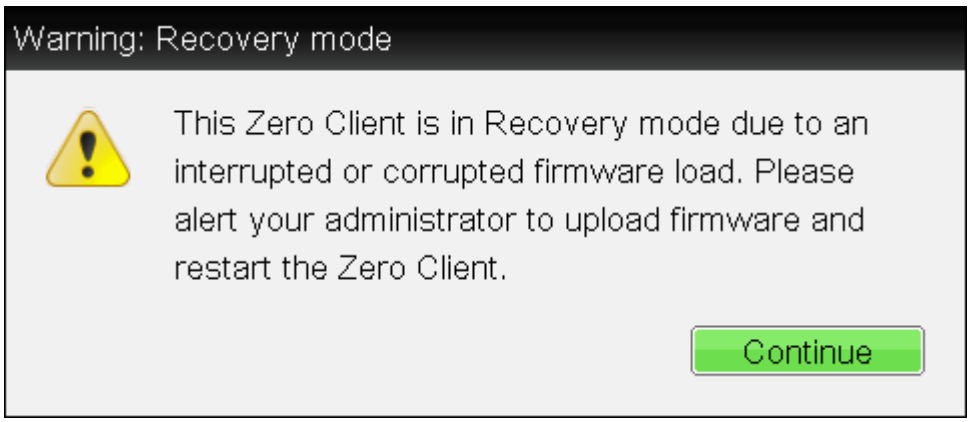
OSD Recovery Mode

Recovery mode is a special mode of the Tera2 PCoIP Zero Client firmware that takes effect when the client experiences a problem that renders it unable to operate. Recovery mode automatically becomes active under the following conditions:

- A firmware update fails.
- The client has an invalid configuration.
- The client has been unable to complete its boot sequence after a number of attempts.

This mode lets you correct the configuration, or upload a replacement firmware or certificate file.

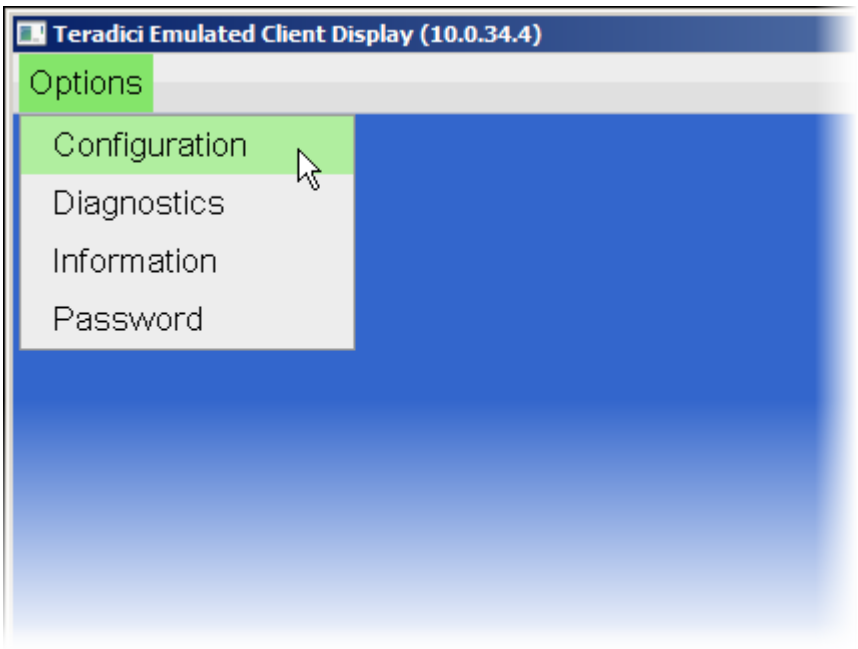
When the client is in recovery mode, the OSD screen displays the following initial screen:



OSD recovery mode

OSD Recovery Mode Options

Select the **Options** menu to see the available options for configuring and displaying information when the client is in recovery mode.



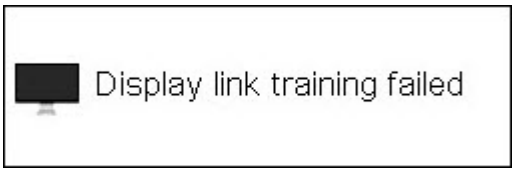
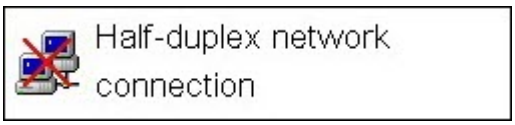
OSD recovery mode available options

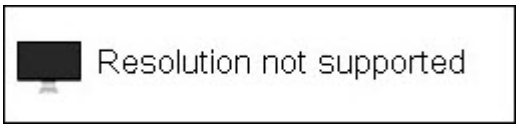
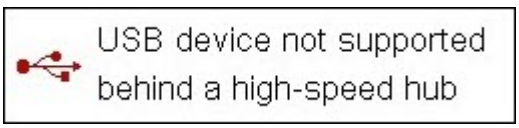
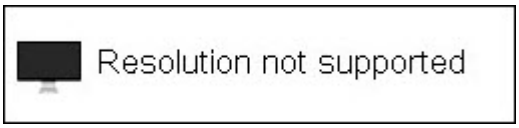
- **Configuration:** Lets you correct the problem by changing the network configuration (including IPv6 settings), clearing the management state, and resetting the configuration and permissions settings stored on the device.
- **Diagnostics:** Displays the client's event log messages.
- **Information:** Displays hardware and firmware version information about the client.
- **Password:** Enables you to update the client's administrative password.

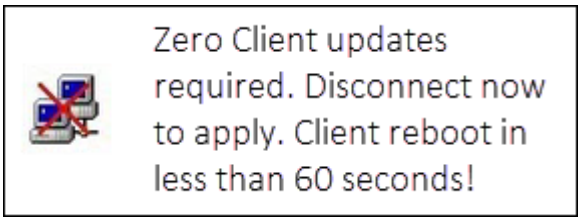
See also: Troubleshooting a Tera2 PCoIP Zero Client in Recovery Mode.

About Overlay Windows

Overlay windows occasionally appear on top of the user's PCoIP session to display pertinent information when the status changes, for example, when the network connection is lost or an unauthorized USB device is plugged in. These overlays show network, USB device, and monitor statuses as icons and text.

Overlay Window	Description
 Display link training failed overlay	This overlay only displays on Tera2 clients that contain DisplayPort display interfaces (as opposed to DVI interfaces). The DisplayPort protocol requires a link training sequence for adapting to differing cable lengths and signal qualities. If this training does not succeed, this overlay appears with the message: ***Display link training failed***.
 Half duplex overlay	PCoIP technology is not compatible with half-duplex network connections. When a half-duplex connection is detected, this overlay appears with the message: ***Half-duplex network connection***.
 Network connection lost overlay	Loss of network connectivity is indicated using an overlay with the message Network connection lost over the most recent screen data. This overlay appears when the client network cable is disconnected or when no PCoIP protocol traffic is received by the client for more than two seconds. The lost network connection message appears until the network is restored or the timeout expires (and the PCoIP session ends). **Consider disabling this notification message in sessions to virtual desktops.** **Tip: Consider disabling this notification message in sessions to virtual desktops** It is not recommended to use this notification message when using PCoIP devices with virtual desktops. Normal scheduling within the virtual desktop hypervisor can falsely trigger this message. To prevent this problem, you can disable the Enable Peer Loss Overlay setting. No support resolutions found overlay setting.

Overlay Window	Description
 No support resolutions found overlay	Display resolution may have limitations due to resource constraints when all four ports have large displays connected. If the resolution limit is exceeded, this overlay appears with the message: *No support resolutions found. Please Try unplugging other displays.*
 Preparing desktop overlay	When a user first logs into a PCoIP session, this overlay appears with the message: *Preparing desktop...*
 USB device not authorized overlay	If an unauthorized USB device is connected, this overlay appears with the message USB device not authorized. This overlay lasts for approximately five seconds.
 USB over current notice overlay	If the USB devices connected to the client cannot be handled by the USB ports, this overlay appears with the message USB over current notice. This overlay remains until USB devices are removed to meet the current handling of the USB ports.
 USB device not supported behind a high-speed hub overlay	Some USB devices cannot be connected through a high speed (USB 2.0) hub, and should instead be connected directly to the Tera2 PCoIP Zero Client or through a full speed (USB 1.1) hub. If such a device is connected to the Tera2 PCoIP Zero Client through a high speed hub, this overlay appears with the message: *USB device not supported behind high speed hub. This overlay lasts for approximately five seconds.*
 Resolution not supported overlay	If the resolution of a monitor connected to the client cannot be supported by the host, the monitor is set to its default resolution and this overlay appears with the message: *Resolution not supported.*

Overlay Window	Description
 Reboot overlay	If a configuration change via AWI or Management Console profile application requires a PCoIP Zero Client reboot, the user will be provided with a warning of the pending reboot. This will allow the user to save any work they may have open. This setting is disabled by default. This setting can be enabled and configured with any of 4 timing options. See PCoIP Management Console profile documentation for profile management information. This setting can be found in the Management Console profile under the POWER section or on the AWI Configuration > Reset page. Available options: • 0 seconds (disabled) • 30 seconds • 60 seconds (1 minute) • 300 seconds(5 minutes)

Video Source Overlays

Improper connection of the host video source is denoted by two possible overlays, as shown next. These overlays appear for approximately five minutes. The monitor is put into sleep mode approximately 15 seconds after they appear.

Overlay Window	Description
 No source signal overlay	When no video source is connected to the host, this overlay appears with the message: ***No source signal.*** This helps you debug a situation where the host does not have the video source connected or the host PC has stopped driving a video signal. To correct this, connect the host PC video to the host. (This message can also be triggered by the host going into display power save mode.)

Overlay Window	Description
 Source signal on other port overlay	When a video source to the host does not correspond to the video port used on the client, this overlay appears with the message: *Source signal on other port*. This helps you debug a situation where the video source is connected to the wrong port. To correct this, swap the video ports at the host or the client.

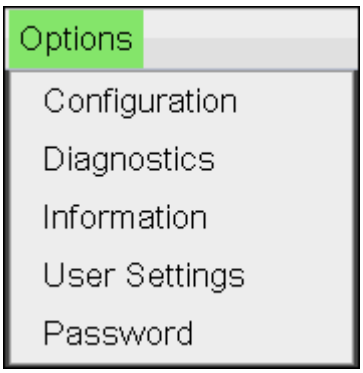
OSD Menus

The **Options** menu in the upper left corner has five sub-menus that link to OSD configuration, information, and status pages:

- **Configuration:** This menu contains links to pages that let you define how the device operates and interacts with its environment. Each tab has an **OK**, **Cancel**, and **Apply** button that lets you accept or cancel the settings changes made.
- **Diagnostics:** This menu contains links to pages that help diagnose issues concerning the client.
- **Information:** The page under this menu displays hardware and firmware version information about the device and the client's IP address.
- **User Settings:** This menu contains links to pages that let users define mouse, keyboard, image, display topology, touch screen, tablet, and region settings, and also the certificate checking mode.
- **Password:** The page under this menu lets you update the administrative password for the device.

Password option appears when password protection is enabled.

The **Password** menu option is only present in the OSD for devices that are configured with password protection enabled. If this option is not visible in the **Options** menu, you can make it visible by using a PCoIP Management Console profile to enable password protection for the device. You can also use a PCoIP Management Console profile to hide a single menu item, the entire **Options** menu, or all menus from users. For details, see the PCoIP® Management Console Administrators' Guide.



OSD Options menu

The GUI Reference in this documentation contains full details about each page. For information about how to configure or manage a device using these OSD pages, see the appropriate section in the GUI Reference.

About the PCoIP Administrative Web Interface

The PCoIP Administrative Web Interface (AWI) enables you to interact remotely with a PCoIP endpoint. From the AWI, you can manage and configure a client, view important information about it, and upload firmware and certificates to it.

> **Disabled by default**
>
> As of firmware 6.4, the AWI is disabled by default. See Configuring Access to Management Tools for instructions on how to enable the AWI.

After you type the device's IP address into an Microsoft Edge, Mozilla Firefox, or Google Chrome browser, the browser will use HTTPS to connect to the device's AWI web page. Access to the AWI is controlled using an administrative password, which can be optionally disabled. The Zero Client supports one AWI login at a time. If a user attempts to login to the AWI while another user is logged in, the AWI provides a warning that a user is currently logged in. Should a user continue to login the existing user is disconnected.

The AWI's HTTPS connection is secured using a PCoIP root Certificate Authority (CA) certificate. To avoid warning messages when you log into the AWI, it is recommended that you install this certificate in your browser. The certificate file (cacert.pem) is always included in a firmware release, but you can also download it directly from How do I get the fix the unsecure browser warning when accessing the Management Console 2.x and 3.x web interface? (1406). Detailed instructions on how to install the certificate are also included in the knowledgebase article.

The following browsers are supported in this release:

- Firefox: current version
- Chrome: current version
- Microsoft Edge: current version

Logging into the Administrative Web Interface

To log into the Administrative Web Interface (AWI) web page:

1. Using a web browser, enter the client's IP address in the address bar. According to network requirements, this address may be either a static or dynamic address as follows:
   - **Static IP Address:** The IP address is hard-coded and must be known.
   - **Dynamic IP Address:** The Dynamic Host Configuration Protocol (DHCP) server dynamically assigns the IP address. You can get it from the DHCP server.
2. From the *Log In* page, enter the administrative password.

> **Contact your reseller for your device's AWI password**
>
> Contact your reseller to obtain the default password for your device's AWI.

AWI Log In page

3. To change idle timeout (the time after which the device is automatically logged off), select an option from the **Idle Timeout** drop-down menu.
4. Click **Log In**.

> **Some PCoIP devices do not require a password to log in**
>
> Some PCoIP devices have password protection disabled and do not require a password to log in.

If configured in the firmware defaults, the Initial Setup page appears the first time you log in. You can configure audio, network, and session parameters on this page. After you click **Apply**, the *Home* page appears for each subsequent session. This page provides an overview of the device status.

If a warning message appears when you try to log in, then a session is already in progress on that device. Only one user can log into a device at one time. When a new session logs in, the current session is ended and the previous user is returned to the *Log In* page.

AWI Initial Setup Page

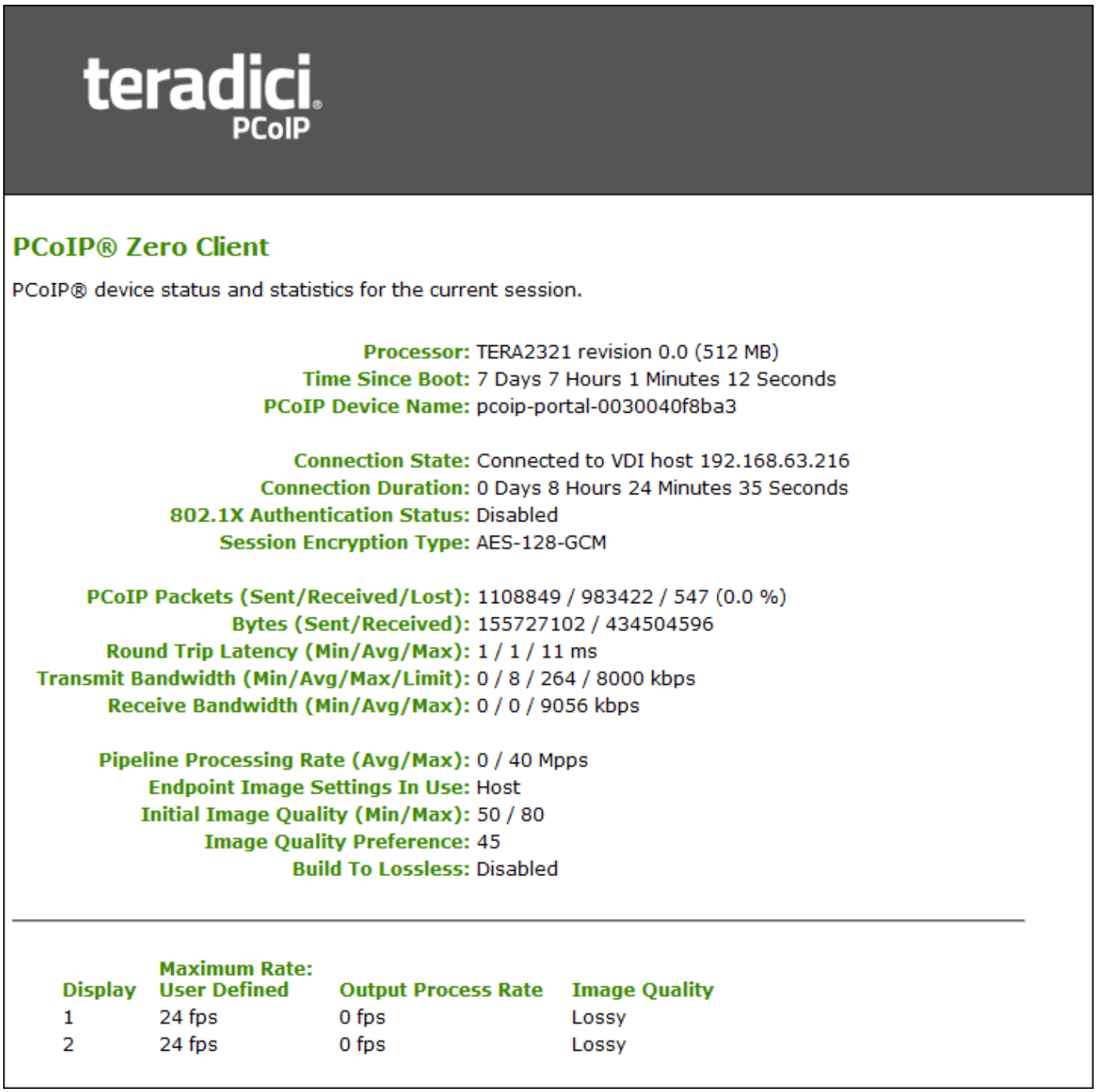
The AWI's Initial Setup page contains the audio, and network configuration parameters that you must set before a client or host device can be used. This page helps to simplify initial setup and reduce the time for new users to establish a session between a Tera2 PCoIP Zero Client and PCoIP Remote Workstation Card.

Complex environments require further configuration

More complex environments that use host discovery or connection management systems require further configuration than is available on the Initial Setup page.

AWI Home Page

The AWI Home page displays a statistics summary for the Tera2 PCoIP Zero Client. You can display the Home page at any time by clicking the **Home** link at the top left section of the menu bar.



AWI: Home page

The previous figure shows session statistics for devices that can support four connected displays. If your deployment only supports two displays, information for these two displays will appear in the bottom area of the page.

AWI Home Page Statistics

Statistics	Description
Processor	PCoIP processor type, version, and RAM size
Time Since Boot	Length of time that the PCoIP processor has been running.
PCoIP Device Name	The logical name for the device. This field is the name the client registers with the DNS server if DHCP is enabled or the system is configured to support registering the hostname with the DNS server. (See the PCoIP Device Name parameter on the Label page.)
Connection State	The current (or last) state of the PCoIP session. Possible connection states are: • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
Connection Duration	Displays the length of time the device has been connected to a host endpoint.
802.1X Authentication Status	Indicates whether 802.1X authentication is enabled or disabled on the device.
Session Encryption Type	Displays the encryption algorithm in use when a session is active.
PCoIP Packets Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.

Statistics	Description
Bytes	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (± 1 ms).
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	Shows the average and maximum amount of image data being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the Use Client Image Settings field is configured on the Image page for the host device.
Initial Image Quality	The minimum and maximum quality setting is taken from the Image page for the device. The active setting is what's currently being used in the session and only appears on the host.
Image Quality Preference	This setting is taken from the Image Quality Preference field on the Image page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include the following: **Enabled:** The Disable Build to Lossless field on the Image page is unchecked. **Disabled:** The Disable Build to Lossless field is checked.
Display	The port number for the display.
Maximum Rate: Refresh Rate	This column shows the refresh rate of the attached display. If the *Maximum Rate* field on the Image page is set to 0 (that is, there is no limit), the maximum rate is taken from the monitor's refresh rate. If the *Maximum Rate* field on the Image page is set to a value greater than 0, the refresh rate shows as User Defined.

Statistics	Description
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Image Quality	Shows the current lossless state of the attached display: • Lossy • Perceptually lossless • Lossless

Clicking Reset Statistics also resets statistics on Home page

When you click the **Reset Statistics** button on the Session Statistics page, the statistics reported in the Home page are also reset.

AWI Recovery Mode

Recovery mode is a special mode of the Tera2 PCoIP Zero Client firmware that takes effect when the client experiences a problem that renders it unable to operate. Recovery mode automatically becomes active under the following conditions:

- A firmware update fails.
- The client has an invalid configuration.
- The client has been unable to complete its boot sequence after a number of attempts.

This mode lets you correct the configuration, or upload a replacement firmware or certificate file.

When the client is in recovery mode, the following AWI login screen displays when you enter the client's IP address in your browser's address bar:

AWI recovery mode

AWI Recovery Mode Options

After logging in, the AWI displays the recovery mode Home page. The menus at the top show the available options for configuring and displaying information.

AWI recovery mode – home page

- **Configuration:** Enables you to correct the problem by changing the network configuration (including IPv6 settings), clearing the management state, updating the client's administrative password, and resetting the configuration and permissions settings stored on the device.

- **Diagnostics:** Displays the client's event log messages and lets you reset the PCoIP processor.
- **Information:** Displays hardware and firmware version information about the client.
- **Upload:** Lets you upload firmware and certificates for a client.
  You can also use the Management Console to upload firmware and certificates to a group of Tera2 PCoIP Zero Clients. For details, see PCoIP® Management Console Administrators' Guide.

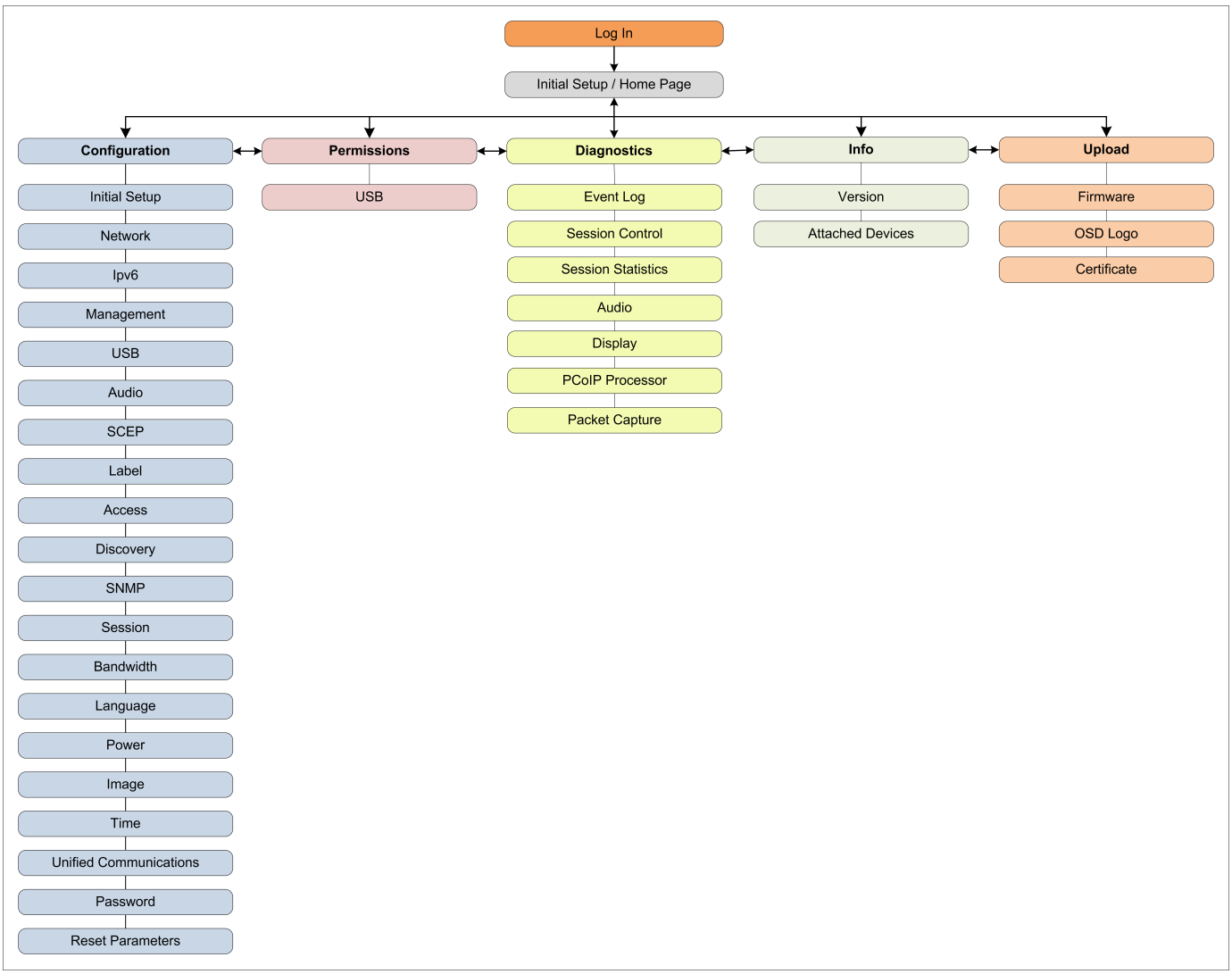
See also: Troubleshooting a Tera2 PCoIP Zero Client in Recovery Mode.

AWI Menus

The AWI has five main menus that link to the various configuration and status pages:

- **Configuration:** The pages under this menu let you configure the various aspects for the device, such as network settings, language, session parameters, and so on.
- **Permissions:** The pages under this menu let you set up the permissions for the USB on the client and host.
- **Diagnostics:** The pages under this menu help you troubleshoot the device.
- **Info:** The pages listed this menu let you view firmware information and the devices currently attached to the device.
- **Upload:** The pages under this menu let you upload a new firmware version, an OSD logo, and your certificates to the device.

The following figure shows the menus and pages available in the AWI.



AWI menu overview

Refer to GUI Reference section

The GUI Reference in this documentation contains full details about each page. For information about how to configure or manage a device using these AWI pages, see the appropriate section in the GUI Reference.

What Can You Connect To Using Your Tera2 PCoIP Zero Client?

Your Tera2 PCoIP Zero Client can connect to wide variety of host desktops and peripherals. This section provides an overview of your connection options. It describes:

- PCoIP Host Support
- Device Support
- Supported Displays and Resolutions

Physically Setting Up a Tera2 PCoIP Zero Client

For instructions on how to physically set up a Tera2 PCoIP Zero Client and connect it to USB devices, monitors, and a network, see the Connecting the Tera2 PCoIP Zero Client to the Network and knowledge base article 1025. This guide has detailed instructions for each step of the installation process.

PCoIP Host Support

Tera2 PCoIP Zero Clients are pre-configured to connect directly to PCoIP Connection Manager or VMware Horizon brokers, but you can easily configure them for any session connection type. Tera2 PCoIP Zero Clients can connect to the following PCoIP host endpoints:

- PCoIP Remote Workstation Cards
- Teradici Cloud Access Software
- Amazon WorkSpaces Desktops
- VMware Horizon Desktops

Device Support

The Tera2 PCoIP Zero Client supports the following devices:

- **Monitors:** Depending on the Tera2 PCoIP Zero Client model, you can attach up to four monitors.

- **Analog devices:** You can attach analog output devices such as headphones and speakers to the Tera2 PCoIP Zero Client's analog output (line out) jack and analog input devices such as microphones and recording devices to the client's analog input (line in) jack.
- **USB devices:** You can attach a variety of USB devices to your Tera2 PCoIP Zero Client. USB human interface device (HID) devices (for example, keyboards, mice, Wacom tablets) are locally terminated by the client. Non-HID devices (for example, mass storage devices, some printers, non-isochronous scanners) are automatically bridged when the USB permissions are set to allow the device. The drivers for many of these devices need to be installed in the host operating system (OS).

Supported Displays and Resolutions

Tera2 PCoIP Zero Clients support from one to four displays at the following resolutions:

PCoIP Zero Client Processor Name	Maximum No. of Supported Displays and Resolutions
TERA2321	1 x 3840x2160 [2] See 4K Capabilities 1 x 2560x1600 [1] 2 x 1920x1200
TERA2140	2 x 3840x2160 [2] See 4K Capabilities 2 x 2560x1600 [1] 4 x 1920x1200

4K Capabilities

4k resolutions are supported on 4K UHD monitors connected to PCoIP Zero Client DisplayPort models using firmware 20.01 or newer, while connected to:

- Remote Workstation Cards running firmware 20.01 or newer
- Cloud Access Software host agents with supported configurations
- Horizon View agents with supported configurations

EDID and timing behavior

The PCoIP Zero Client will attempt to use the native timing of the monitor's EDID. 4K 60 Hz timings are not supported and the Zero Client will search for a 4K @ 30 Hz timing instead.

EDID does not have 4K @ 30 Hz Timing

If your monitor supports 4K but does not have an EDID that contains a 4k resolution of 3840x2160 @ 30 Hz, you can use the OSD's Enable Preferred Resolution Override

Review each configuration and understand its use case before determining which 4K configuration to use. Frame rates will adapt automatically based on the content being displayed. Along with having a 4K UHD monitor, it is recommended that the network connection between the Remote Workstation Card and Zero Client is 1Gb or higher.

Possible 4K Zero Client Configurations

- Dual DisplayPort (TERA2321) PCoIP Zero Clients can support 1 4K UHD @ 30 Hz display at 15 frames per second (FPS) for full screen. A video that takes up half of the screen can run at 30 FPS
- Quad DisplayPort (TERA2140) can support up to 2 4K UHD @ 30 Hz displays, both running 15 FPS simultaneously, or 1 running 15 FPS for a full screen and the other static. A video that takes up half of the screen can run at 30 FPS

4K Requirements

- 4K firmware 20.01 or newer
- DisplayPort model of a quad (TERA2140) or dual (TERA2321) zero client
- 1 Gb connection between the client and host (for a better experience)

4K Host Requirements

4K host requirements are found in their respective Administrators' Guides

- PCoIP Remote Workstation Card Administrative Guide
- Cloud Access Software Host Agent Administrative Guides
- VMware Documentation

1. Tera2 PCoIP Zero Clients support 2560x1600 resolution on attached displays using either DVI (with Y-cable) or DisplayPort interfaces. For instructions on how to connect cables to Tera2 PCoIP Zero Clients with DVI and/or DisplayPort ports to support this resolution, see knowledge base article 1025.
2. Tera2 PCoIP Zero Clients support 3840x2160 (4K UHD) resolution at 15 FPS on attached displays using Display Port interfaces when the changing content is full screen. A video that takes up half of the screen can run at 30 FPS.

Setting Up Your Tera2 PCoIP Zero Client

This section describes how to connect your Tera2 PCoIP Zero Client to the network. You'll also learn how to configure initial setup parameters, as well as secure your Tera2 PCoIP Zero Client so that you can establish a successful PCoIP session.

The topics include:

- Enabling the AWI
- Connecting the Tera2 PCoIP Zero Client to the Network
- Configuring Initial Setup Parameters
- Securing Your Tera2 PCoIP Zero Client
- Reset Notification

Connecting Peripherals

1. Connect USB keyboard and mouse.
2. Connect one end of the Ethernet cable to the zero client and the other end to a switch/router. The switch or router should be on the same network as the Remote Workstation Card or virtual desktop server. For more advanced network environments, visit the Teradici technical support site.
3. Connect monitor cables to the zero client.
4. Connect speakers and/or headphones (optional). Connect power supply to the zero client and a power source.

Press the front panel PCoIP button to power on the zero client after your peripherals are connected to the zero client.

Reset Notification

You can have your PCoIP Zero Client display a pop up message that notifies you that your PCoIP Zero Client is about to restart. This feature is beneficial when performing a remote configuration

change via the AWI or a PCoIP Management Console profile update that requires the PCoIP Zero Client to reboot. Enabling this feature can provide you the time to save important work before the reboot happens. This setting can be found in the AWI *Reset Parameters* page and in the Management Console profile *Power* section.

This feature has 4 configurable options.

- 0 seconds (disabled)
- 30 seconds
- 60 seconds (1 minute)
- 300 seconds(5 minutes)

Connecting the Tera2 PCoIP Zero Client to the Network

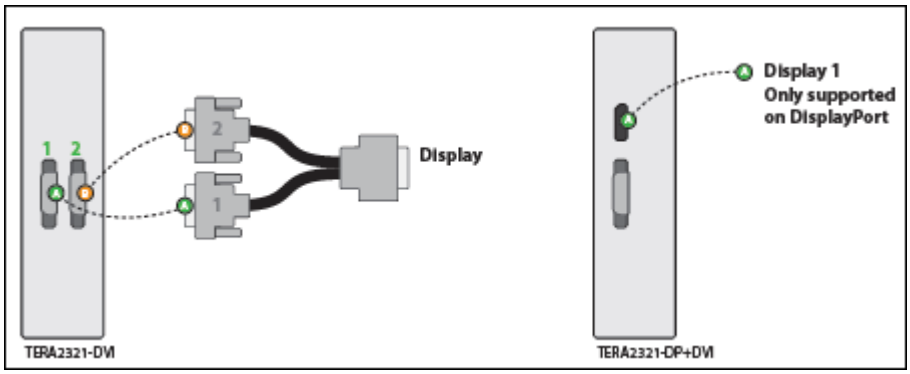
To connect the Tera2 PCoIP Zero Client:

1. Connect a USB keyboard and mouse to any of the Tera2 PCoIP Zero Client USB ports.
2. Connect one end of the Ethernet cable to the Tera2 PCoIP Zero Client and the other end to a switch/router. The switch or router should be on the same network as the Remote Workstation Card or virtual desktop server if there is not a PCoIP Management Console that is managing the PCoIP endpoints.
3. Connect monitor cables to the Tera2 PCoIP Zero Client.

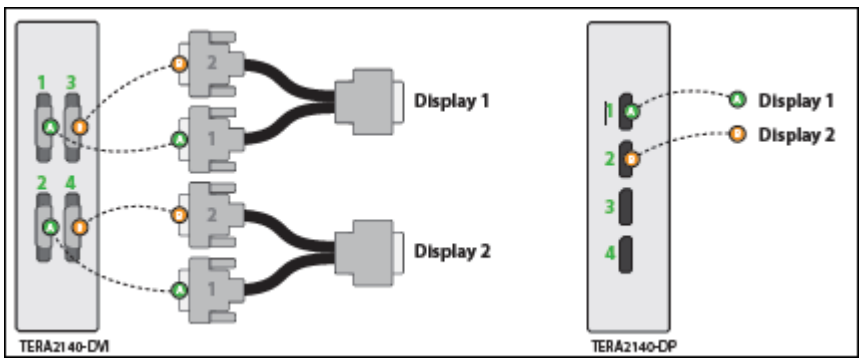
> **Connect monitors using correct ports**
>
> To ensure the best experience, connect monitors to the zero client ports in sequential order

Supporting 2560 x 1600 resolutions

Ensure your cables are connected as shown when configuring monitors for 2560 x 1600 resolutions. For more information see knowledge base article 1025



Single Display at 2560 x 1600 Resolution



Dual Displays at 2560 x 1600 Resolutions

Connecting to Remote Workstation Cards

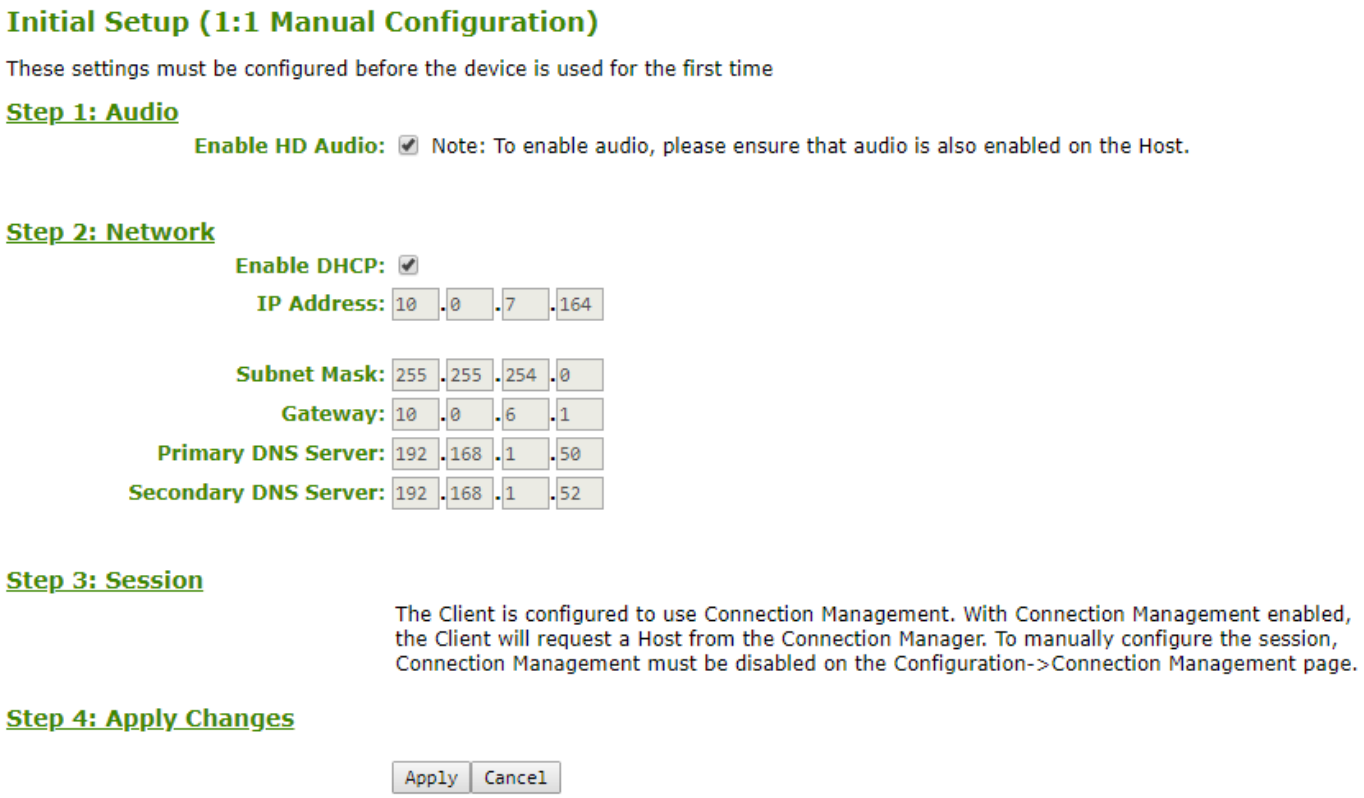
For additional information when connecting monitor cables using PCoIP Remote Workstation Cards, refer to the Remote Workstation Card Administrators' Guide - Installation section

4. (Optional) Connect speakers and/or headphones to the Tera2 PCoIP Zero Client.
5. Connect the power supply to the Tera2 PCoIP Zero Client and a power source.
6. Press the front panel button to power on the Tera2 PCoIP Zero Client.

Configuring Initial Setup Parameters

Before you use your Tera2 PCoIP Zero Client for the first time, you need to configure initial setup parameters, including setting basic audio, network, and session information.

You can perform this initial setup from the AWI *Initial Setup* page, shown next.



AWI Initial Setup page

The following parameters display on the AWI *Initial Setup* page:

Audio Parameters

Category	Parameter	Description
Audio	Enable HD Audio	Enables audio support on the client
Network	Enable DHCP	Enables DHCP (as opposed to using manual IP address configuration)
	IP Address	Device's IP address

Category	Parameter	Description
	Subnet Mask	Device's subnet mask
	Gateway	Device's gateway IP address
	Primary DNS Server	Device's primary DNS IP address
	Secondary DNS Server	Device's secondary DNS IP address

You can also configure network settings from the OSD and AWI Network and Audio pages

You can configure the initial setup settings, as well as other network settings, from the OSD and AWI Network pages. To configure network settings from these pages, see Configuring Audio and Configuring Network Settings.

Session Parameters

Session parameters are configured from the AWI **Configuration -> Session** page.

To configure initial setup parameters from the AWI:

1. From the AWI, select **Configuration > Initial Setup**.
2. From the AWI *Initial Setup* page, configure audio, and network parameters.
3. Browse to **Configuration > Session** and select your preferred session type.
4. Click **Apply** to save your configuration.

Securing Your Tera2 PCoIP Zero Client

The security needs of your deployment are driven by your specific environment. You can configure Tera2 PCoIP Zero Clients to meet security requirements for a range of scenarios, from high-security environments to trusted environments.

Securing your Tera2 PCoIP Zero Client involves some or all of these tasks, depending on your deployment needs:

- **Disable the AWI:** For high security environments, the Administrative Web Interface should be disabled and the PCoIP Management Console used as the tool for configuring PCoIP endpoints. See Configuring Access to Management Tools
- **Disable SLP Discovery:** Ensure SLP Discovery is disabled and configure your PCoIP Zero Client to connect to a specific PCoIP host.
- **Peering to Your Remote Workstation Card:** Zero Clients can be peered to a unique Remote Workstation Card allowing for a secure connection between dedicated PCoIP Zero Clients and Remote Workstation Cards using custom peer-to-peer certificates. See Peering Remote Workstation Cards
- **Setting the Certificate Checking Mode:** Configure how the Tera2 PCoIP Zero Client behaves if it can't verify a secure connection to the server. See Setting Certificate Checking Mode.
- **Uploading certificates to the Tera2 PCoIP Zero Client:** Depending on the certificate checking mode you choose, you may have to upload server certificates to the Tera2 PCoIP Zero Client's certificate store. See Uploading Certificates.
- **Configuring the Tera2 PCoIP Zero Client with an Endpoint Manager:** Configure your Tera2 PCoIP Zero Client for either automatic or manual discovery by an endpoint manager. See Connecting to an Endpoint Manager.
- **Configuring 802.1X Network Device Authentication:** Configure 802.1X network device authentication for enhanced security. See Configuring 802.1X Network Device Authentication.
- **Configuring Access to Management Tools:** Configure a PCoIP device management tool for managing the Tera2 PCoIP Zero Client, disable administrative access to the Tera2 PCoIP Zero Client's AWI, or force an administrative password change the next time someone accesses the AWI or OSD. See Configuring Access to Management Tools.

You can access additional security functionality from the PCoIP Management Console

You can configure security settings for multiple devices from the PCoIP Management Console, as well as access additional AWI and OSD security settings (including password settings and the option to hide OSD menus). For more information, see the PCoIP® Management Console Administrators' Guide.

Default Security Mode

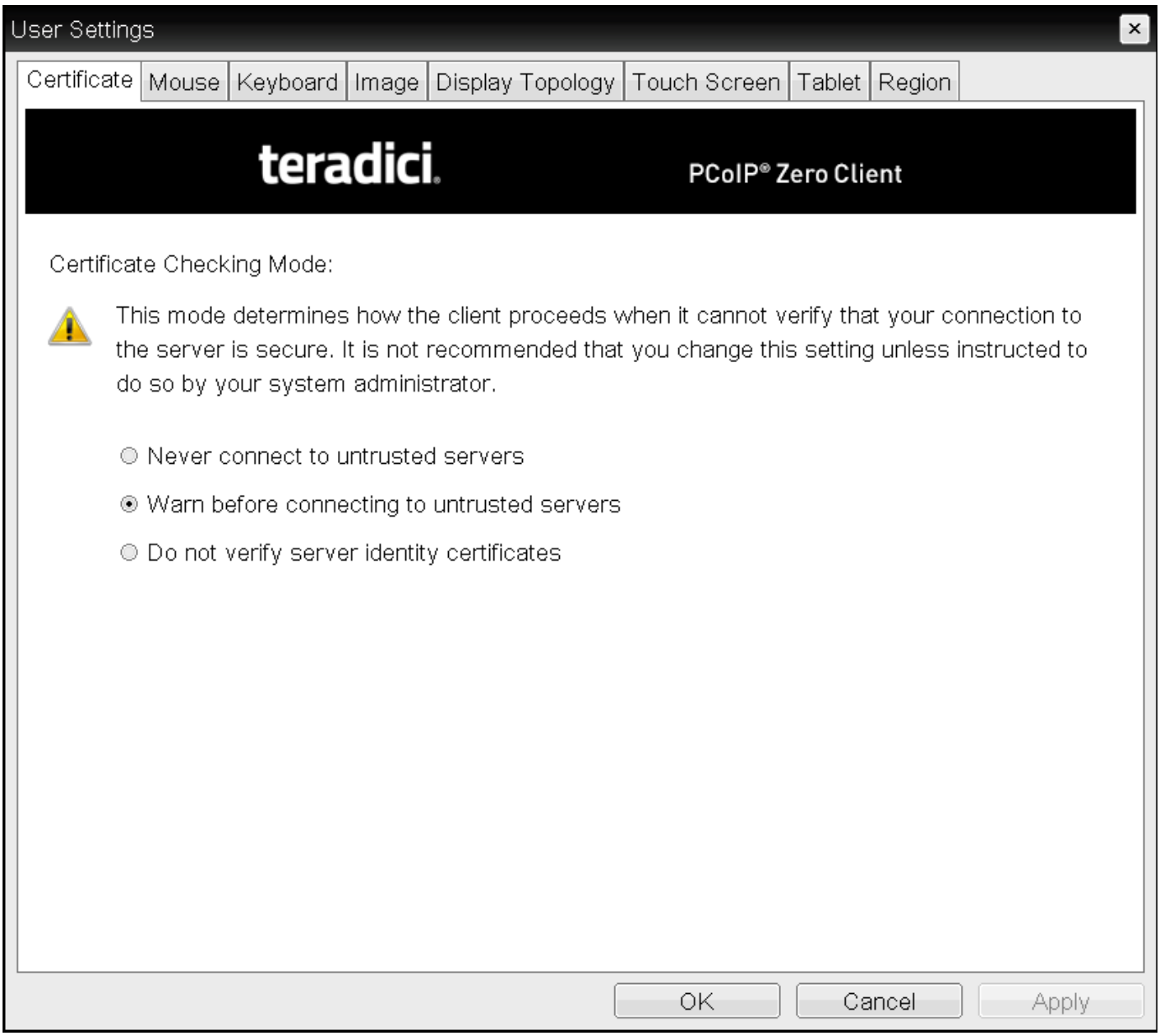
Out of the box, the Tera2 PCoIP Zero Client is configured with the following security settings:

- The **Certificate Checking Mode** is set to Warn before connecting to untrusted servers. See Setting Certificate Checking Mode.
- The **Security Level** is set to Low. See About Tera2 PCoIP Zero Client Security Levels.
- The **security certificate store** is empty. See About Certificates and Uploading Certificates.

Setting Certificate Checking Mode

When the Tera2 PCoIP Zero Client can't verify a secure connection to the host or connection broker, its behavior is determined by the ***Certificate Checking Mode*** option.

You configure this option from the OSD ***Certificate*** page (shown next).



OSD Certificate page

Trusting Servers

Server trust is established by certificates. Certificates are uploaded to the Tera2 PCoIP Zero Client through endpoint managers such as the PCoIP Management Console. For more information, see Performing Common Tasks.

Preventing users from changing the Certificate Checking Mode option

You can prevent users from changing the *Certificate Checking Mode* option on the OSD *Certificate* page. To do this, access the *Certificate Check Mode Lockout* option found in the advanced options for any of the *PCoIP® Connection Manager* or *View Connection Server* session connection types.

To set the Certificate Checking Mode:

1. From the OSD, select **Options > User Settings > Certificate**.
2. From the OSD *Certificate* page, choose one of the *Certificate Checking Mode* options:
   - **Never connect to untrusted servers**: Configures the client to reject the connection if a trusted, valid certificate is not installed.
   - **Warn before connecting to untrusted servers**: Configures the client to display a warning if an unsigned or expired certificate is encountered, or when the certificate is not self-signed and the client trust store is empty.
   - **Do not verify server identity certificates**: Configures the client to enable all connections.
3. Click **OK**.

Peering Zero Clients to Remote Workstation Cards

PCoIP Zero Clients can be peered (paired) to Remote Workstation Cards using custom certificates to establish a secure PCoIP peer-to-peer connection. This optional but recommended configuration allows for a more secure connection then the default connection. The custom peer-to-peer certificate and the root certificate must be present in both the Zero Client and Remote Workstation card certificate store. The custom certificate must then be applied to the Peer-to-Peer Certificate field, which is displayed when the **Direct to Host** *Session Connection Type* and **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption** *TLS Security Mode* options are selected.

Changing Session Connection Type

If you need to change your Session Connection Type from connecting to Remote Workstation Cards, be sure to change the TLS Security Mode to **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**

Remote Workstation Card Configuration

Ensure you follow the same procedure on your peered (paired) Remote Workstation Card before attempting to connect to it. See the PCoIP Remote Workstation Card Administrators' Guide for details.

Peer-to-Peer connections

The peer-to-peer connection using certificates supports connections between PCoIP Zero Clients and Remote Workstation Cards only. This configuration is done via the AWI.

Important: OCSP (Online Certificate Status Protocol)

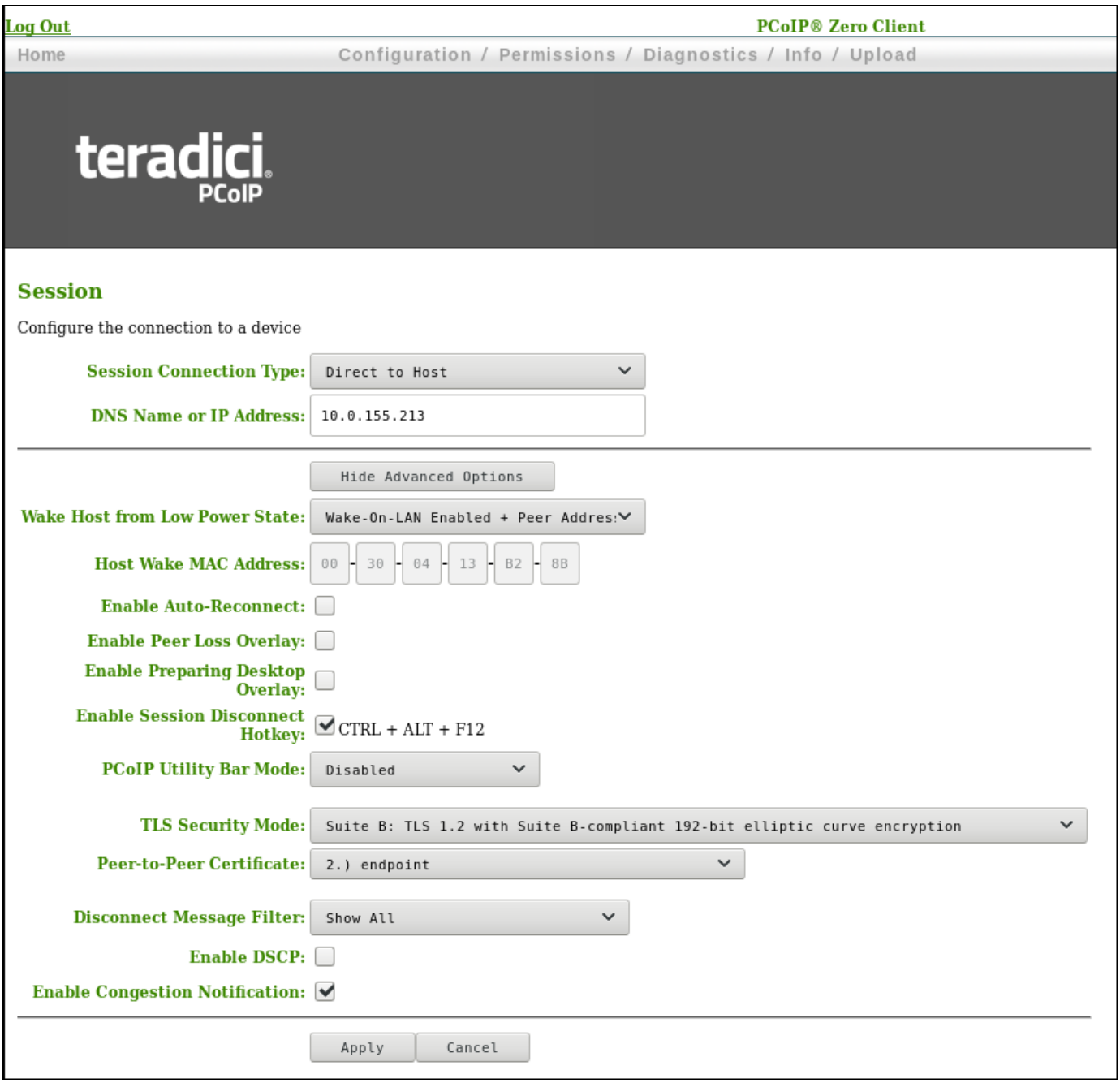
OCSP (Online Certificate Status Protocol) is currently not supported for custom peer-to-peer certificates

To configuring a secure peer-to-peer connection for a PCoIP Remote Workstation Card:

1. Upload both your custom peer-to-peer certificate and your root certificate to your PCoIP Zero Client certificate store. See Uploading Certificates.

> **Remote Workstation Certificate**
>
> Ensure the desired trusted certificate is uploaded to the Remote Workstation Card certificate store.

2. Select **Direct to Host** for the Session Connection Type on the *Session* page.
3. Enter the DNS Name or IP Address of the Remote Workstation Card that you are going to have a peer-to-peer connection with.
4. Select **Show Advanced Options**.
5. Select the TLS Security Mode option **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**.
6. Select the correct **Peer-to-Peer Certificate**. (If it is not displayed, you have not yet uploaded it to the certificate store)
7. Select **Apply**.



Establishing a PCoIP Connection

Tera2 PCoIP Zero Clients can establish a PCoIP session with a variety of hardware and software PCoIP hosts. Zero Clients establish a session by setting its session connection type via the OSD or AWI to connect to a supported host.

You can find Zero Client configuration information for supported hosts in the following topics:

- Connecting to PCoIP Remote Workstation Cards.
- Connecting to Teradici Cloud Access Software.
- Connecting to Amazon WorkSpaces Desktops.
- Connecting to VMware Horizon Desktops and Applications.

OSD: Amazon WorkSpaces Session Settings

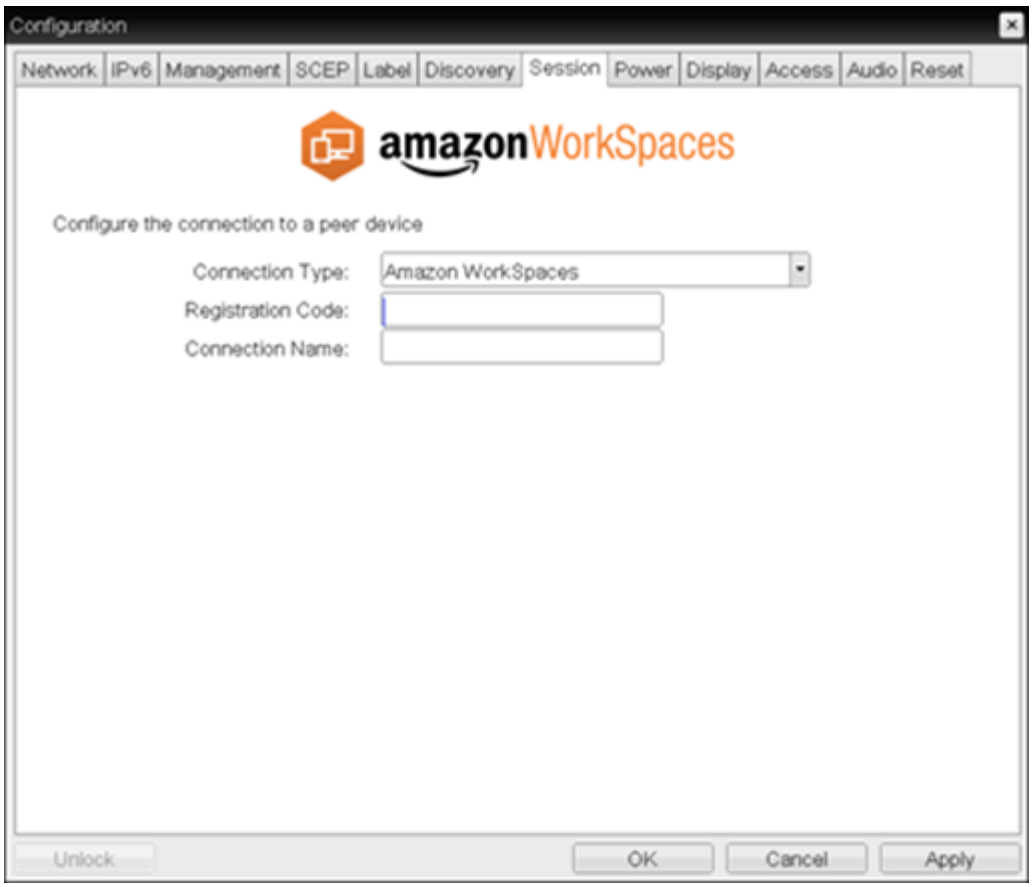
Use the Amazon WorkSpaces session Connection Type to connect directly to your Amazon WorkSpaces desktop through multi-factor authentication when connecting with PCoIP Zero Clients on firmware 6.0 or later. This connection type removes the need to deploy and manage the PCoIP Connection Manager for Amazon WorkSpaces in order to connect PCoIP Zero Clients to Amazon WorkSpaces.

Security Consideration

The connection manager determines the security requirements. Amazon connection manager requires multi-factor authentication when connecting to Amazon WorkSpaces.

Advanced Options

Advanced parameters for this session type are accessible from the AWI.



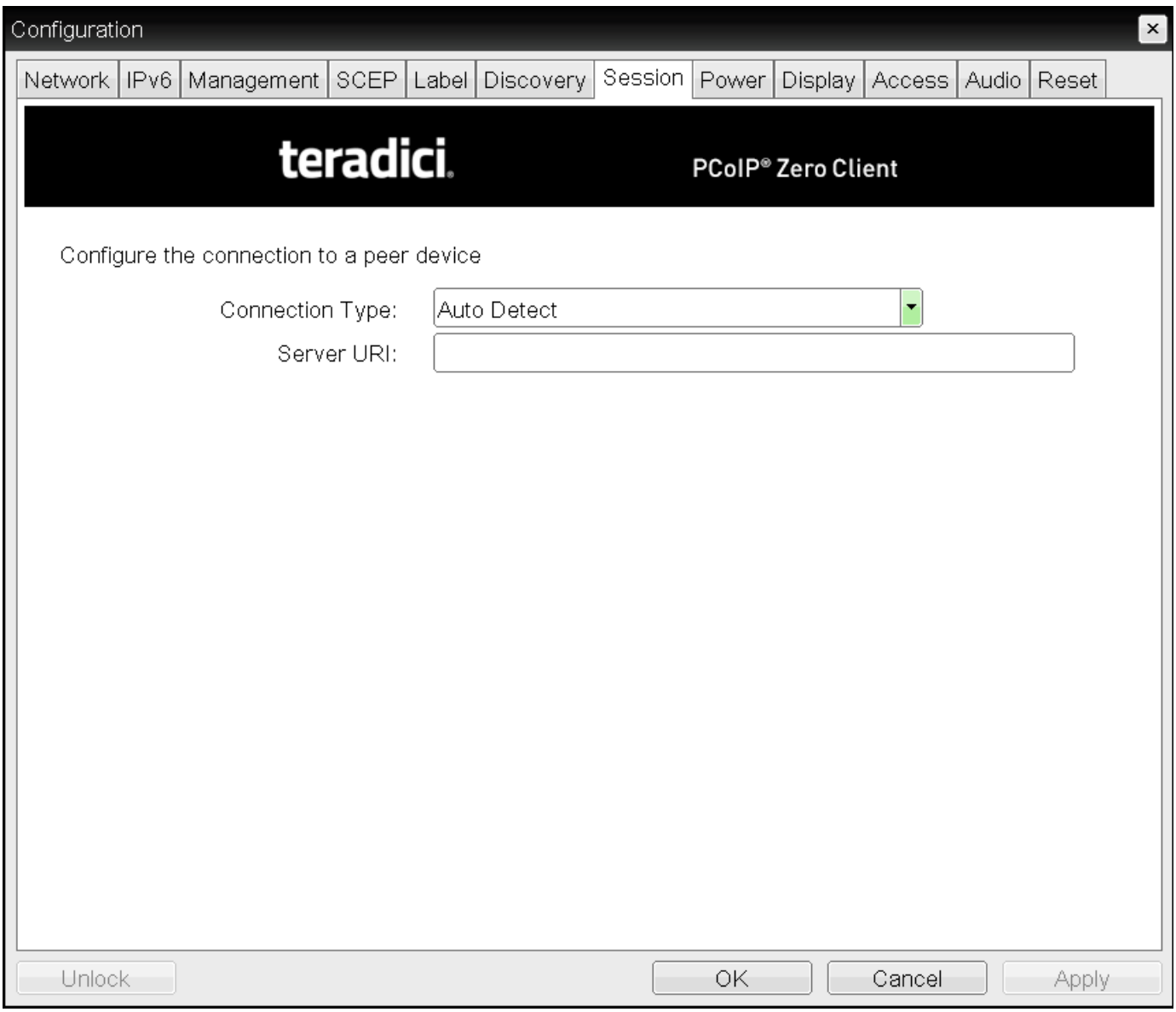
The following parameters can be found on the OSD Session tab for the Amazon WorkSpaces selection.

OSD Amazon WorkSpaces Parameters

Parameter	Description
Registration Code	Enter the code provided by Amazon when your Workspace was created.
Connection Name	The name you gave your connection displayed in the OSD when you turn your zero client on.

OSD: Auto Detect Session Settings

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers. Once a successful connection has been made, the server URI will automatically appear in the **Server** drop-down list on the user's OSD **Connect** screen, along with any other desktops the user has successfully connected to. Additionally, you can use **Auto Detect** when connecting directly to Cloud Access Software.



OSD session connection type – Auto Detect

The following parameters can be found on the OSD Auto Detect page.

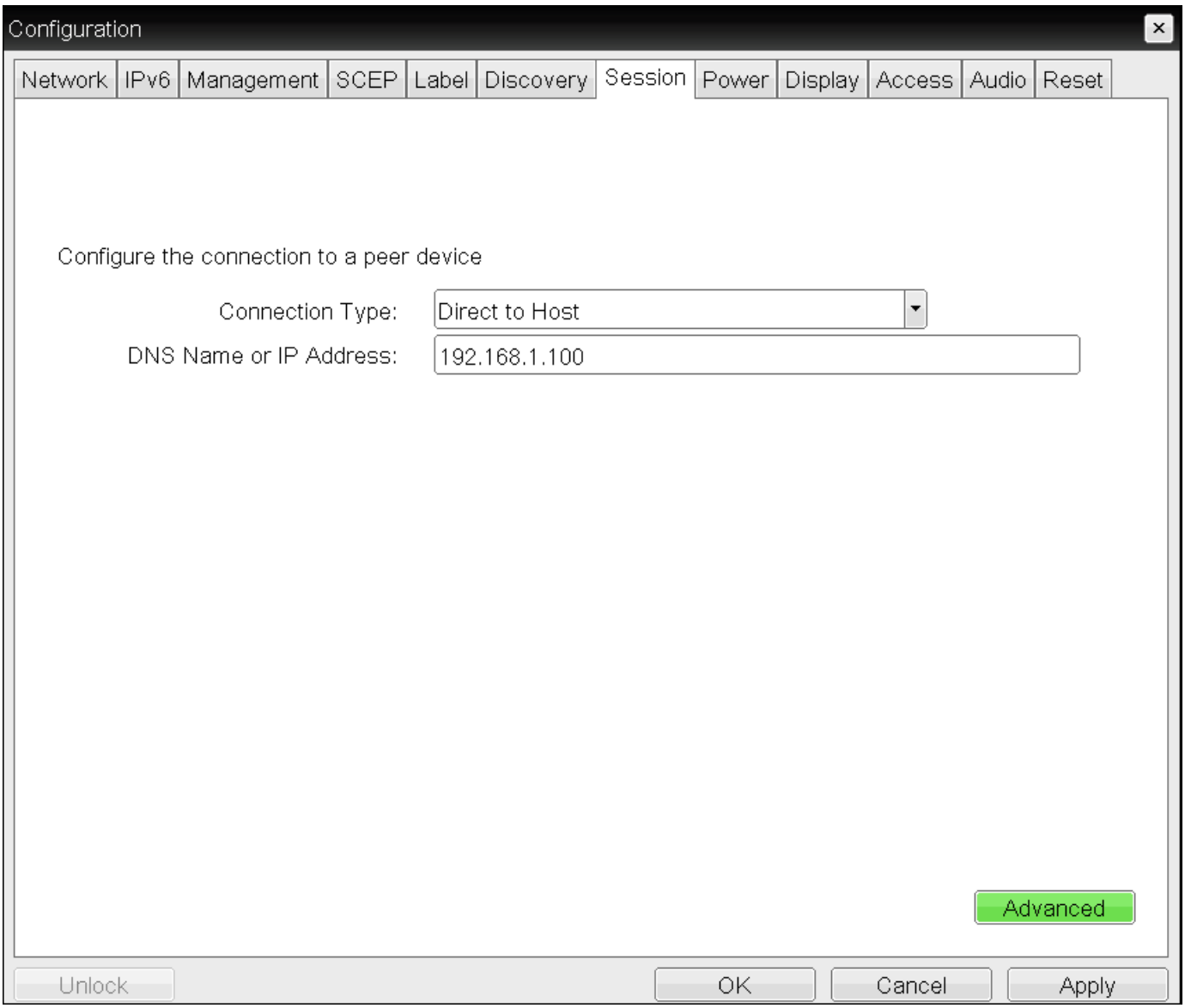
OSD Auto Detect Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**. Once a successful connection has been made to a connection server, it will appear in the Server drop-down list on the OSD Connect page if the Tera2 PCoIP Zero Client is configured to cache servers.

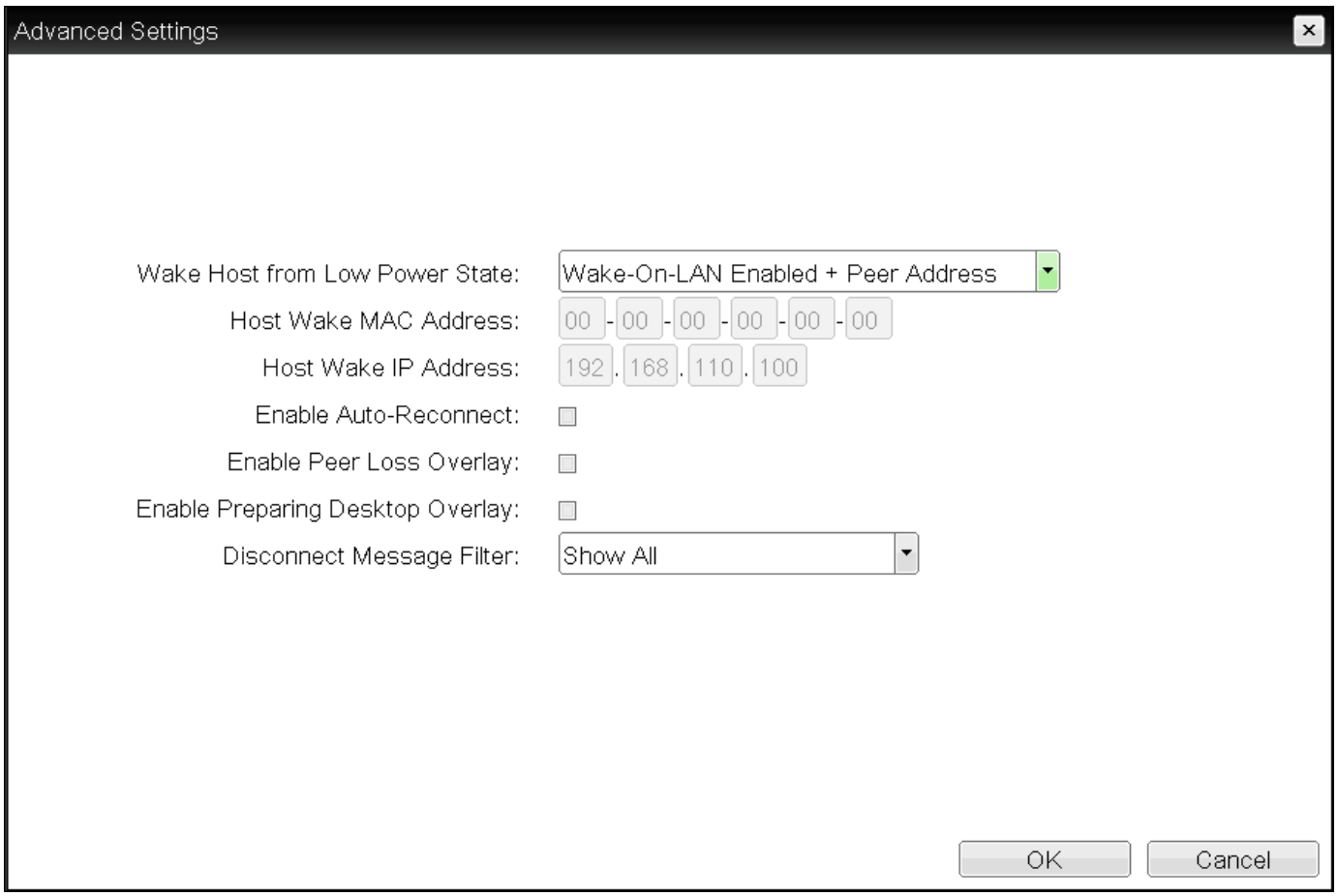
OSD: Direct to Host Session Settings

Select the **Direct to Host** session connection type from the **Options > Configuration > Session** page to configure a client to connect directly to a host.

Click the **Advanced** button to configure advanced settings for this option.



OSD Session Connection Type – Direct to Host



Advanced Settings

The following parameters can be found on the OSD Direct to Host page.

OSD Direct to Host Parameters

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the host.

Parameters	Description
Wake Host from Low Power State	Select whether to use the PCoIP Remote Workstation Card's MAC and IP address or a custom MAC and IP address when configuring the Wake-On-LAN feature on a client. This feature wakes up the host when the user presses the client's power button, a key on the keyboard, or clicks the **Connect** button on the Connect window . • **Wake-On-LAN Enabled + Peer Address:** After you have successfully connected to the PCoIP Remote Workstation Card, both the card's MAC address and IP address are automatically populated in the **Host Wake MAC Address** and **Host Wake IP Address**. • **Wake-On-LAN Enabled + Custom Address:** When selected, enables you to manually enter the MAC address and IP address of the device you want to wake up. If the Remote Workstation Card Software is installed in the host PC and the **Use host PC NIC for Wake-on-LAN** setting is enabled in the **Features > Power Management** section of the Remote Workstation Card Software GUI, the MAC address and IP address of the host PC's network interface card (NIC) will automatically be populated in the **Host Wake MAC Address** and **Host Wake IP Address** read-only fields. The hardware on the host PC must be able to support waking from low power state (off/ hibernate/sleep) when it receives a wake-on-LAN packet. You can disable the Wake-On-LAN feature from the AWI *Power page*.
Host Wake MAC Address	Enter the host's MAC address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. When **Wake-On-LAN Enabled + Peer Address** is selected, the host's MAC address is populated after a successful connection. The client will send a 'magic packet' to the MAC address to wake the host computer from a low power state. The client will send a 'magic packet' to this MAC address to wake the host computer from a low power state.
Host Wake IP Address	Enter the host's IP address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a 'magic packet' to this IP address to wake the host computer from a low power state.
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

Parameters	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

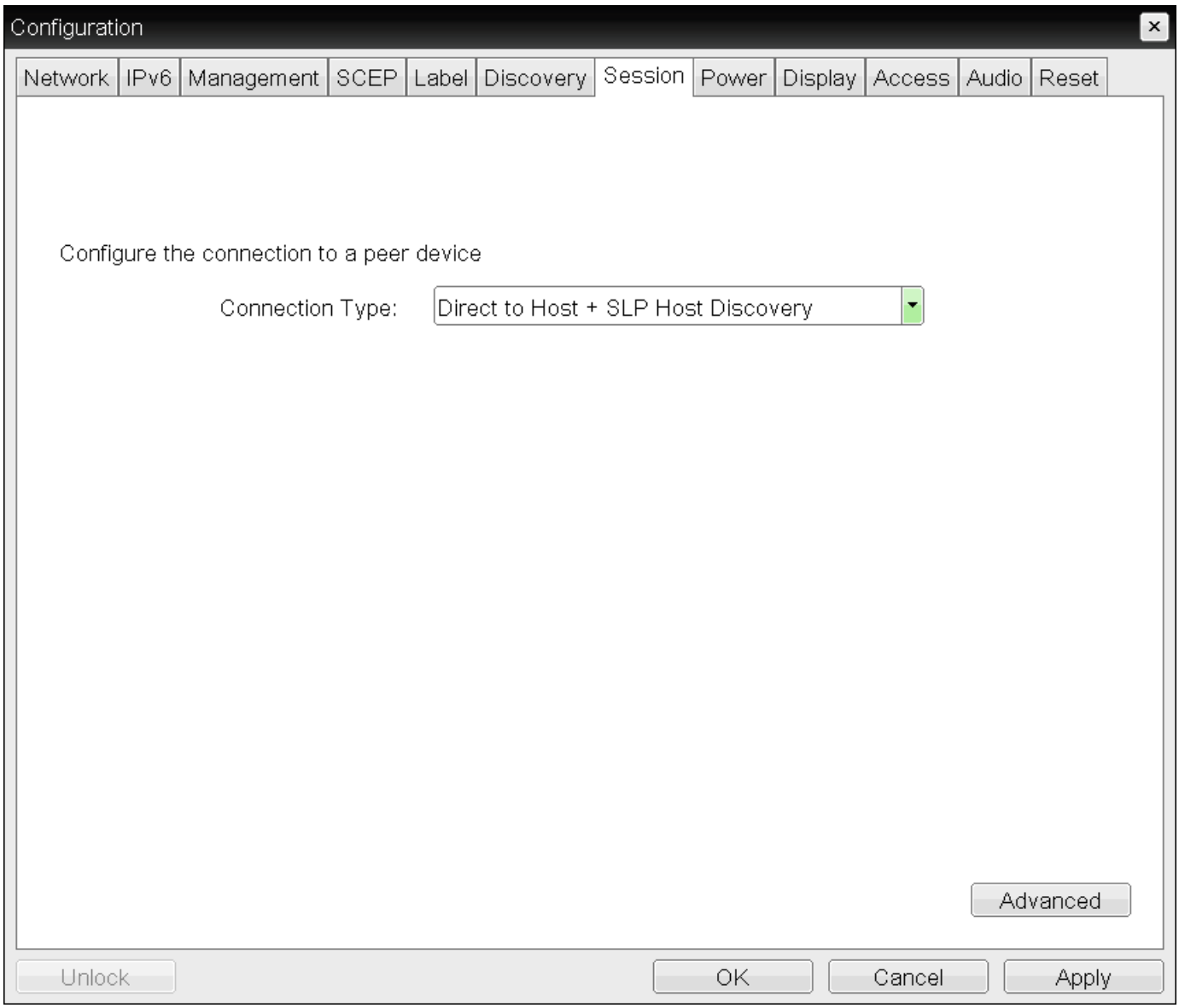
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

OSD: Direct to Host + SLP Host Discovery Session Settings

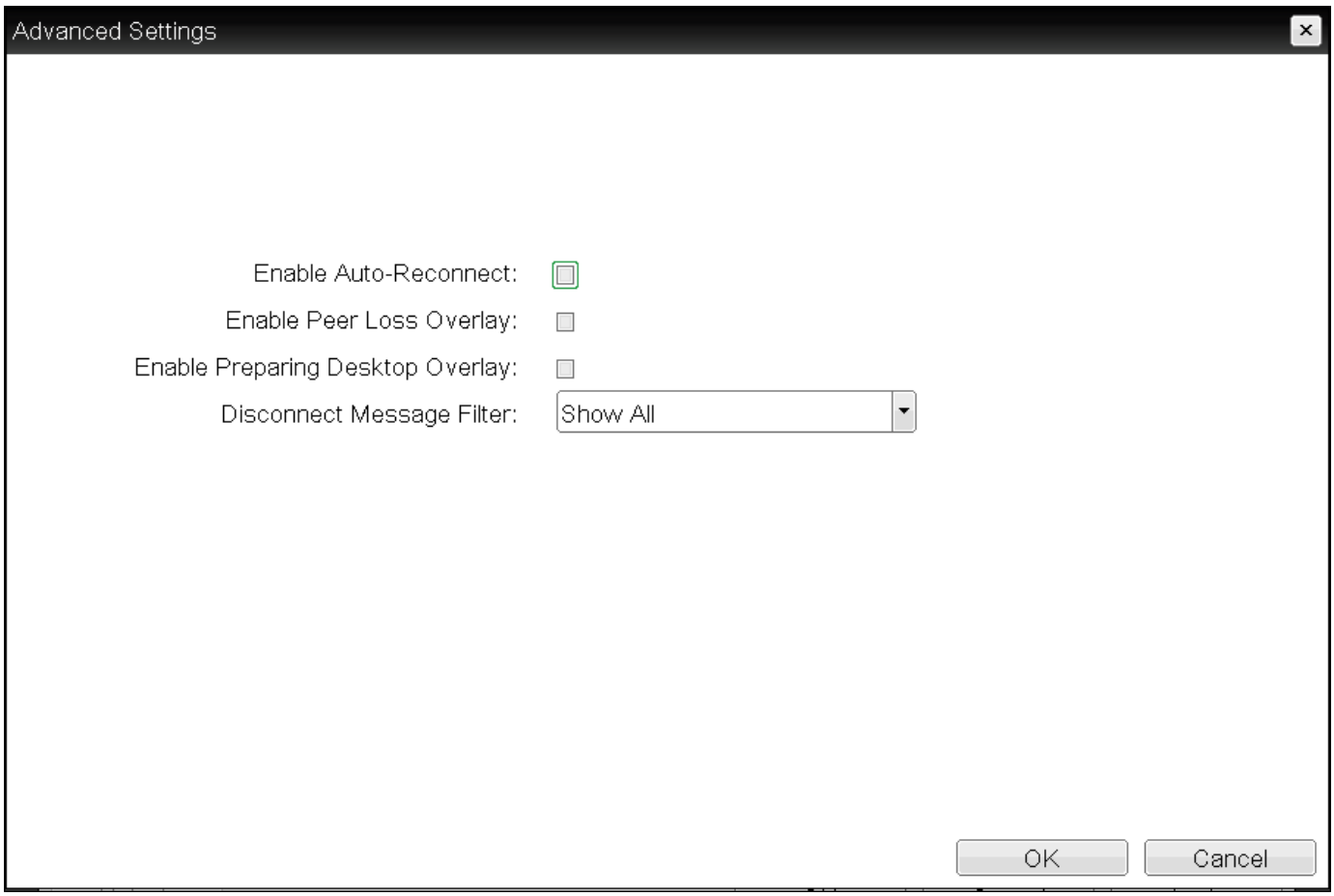
Select the **Direct to Host + SLP Host Discovery** session connection type from the **Options > Configuration > Session** page to configure a client to connect directly to a host and to use Service Location Protocol (SLP) to discover the host automatically.

> **Disabling SLP Host Discovery**
>
> Teradici recommends disabling SLP discovery to create a secure environment.

Click the **Advanced** button to configure advanced settings for this option.



OSD session connection type – Direct to Host + SLP Host Discovery



Advanced Settings

The following parameters can be found on the OSD Direct to Host + SLP Host Discovery page.

OSD Direct to Host + SLP Host Discovery Parameters

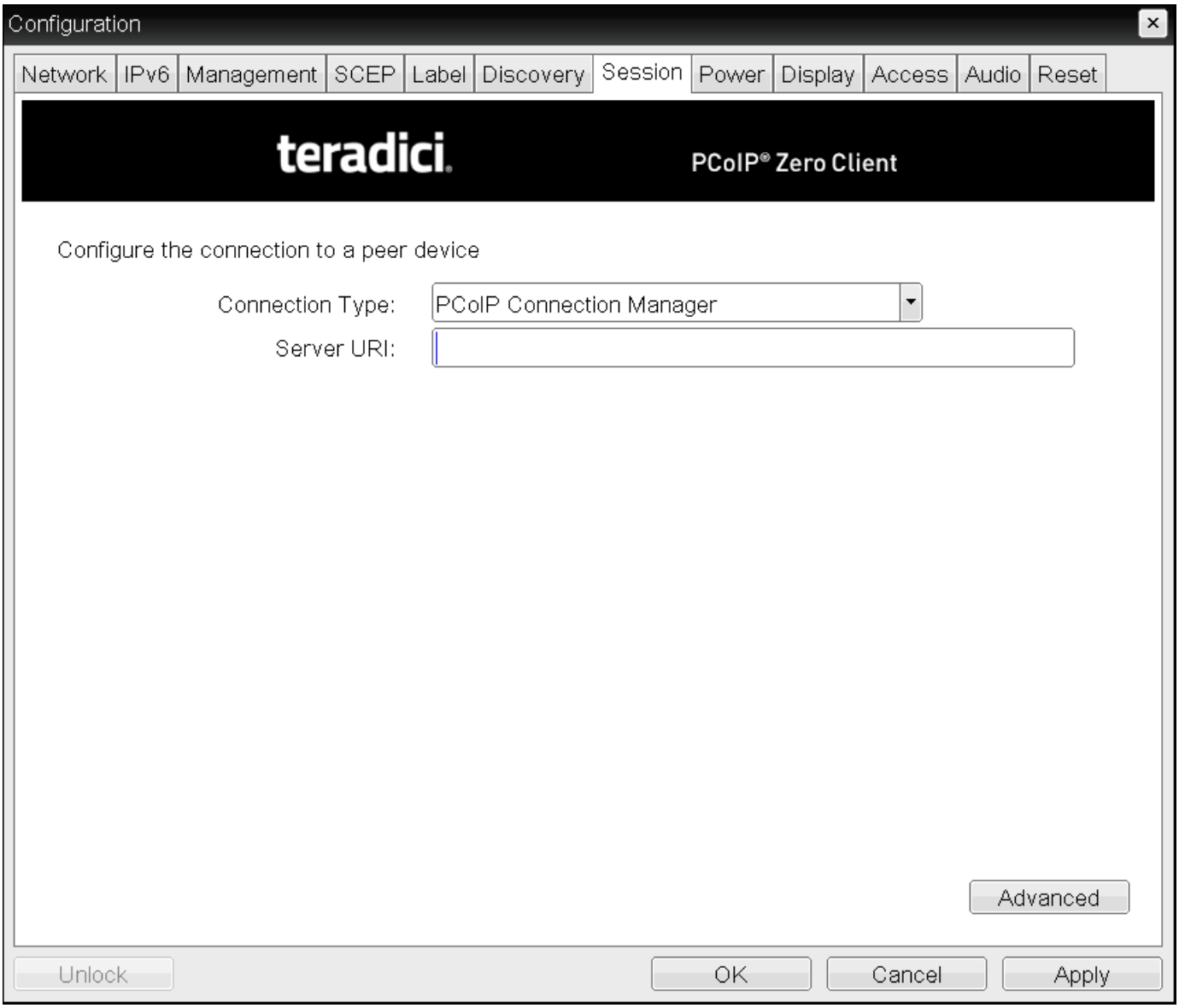
Parameters	Description
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

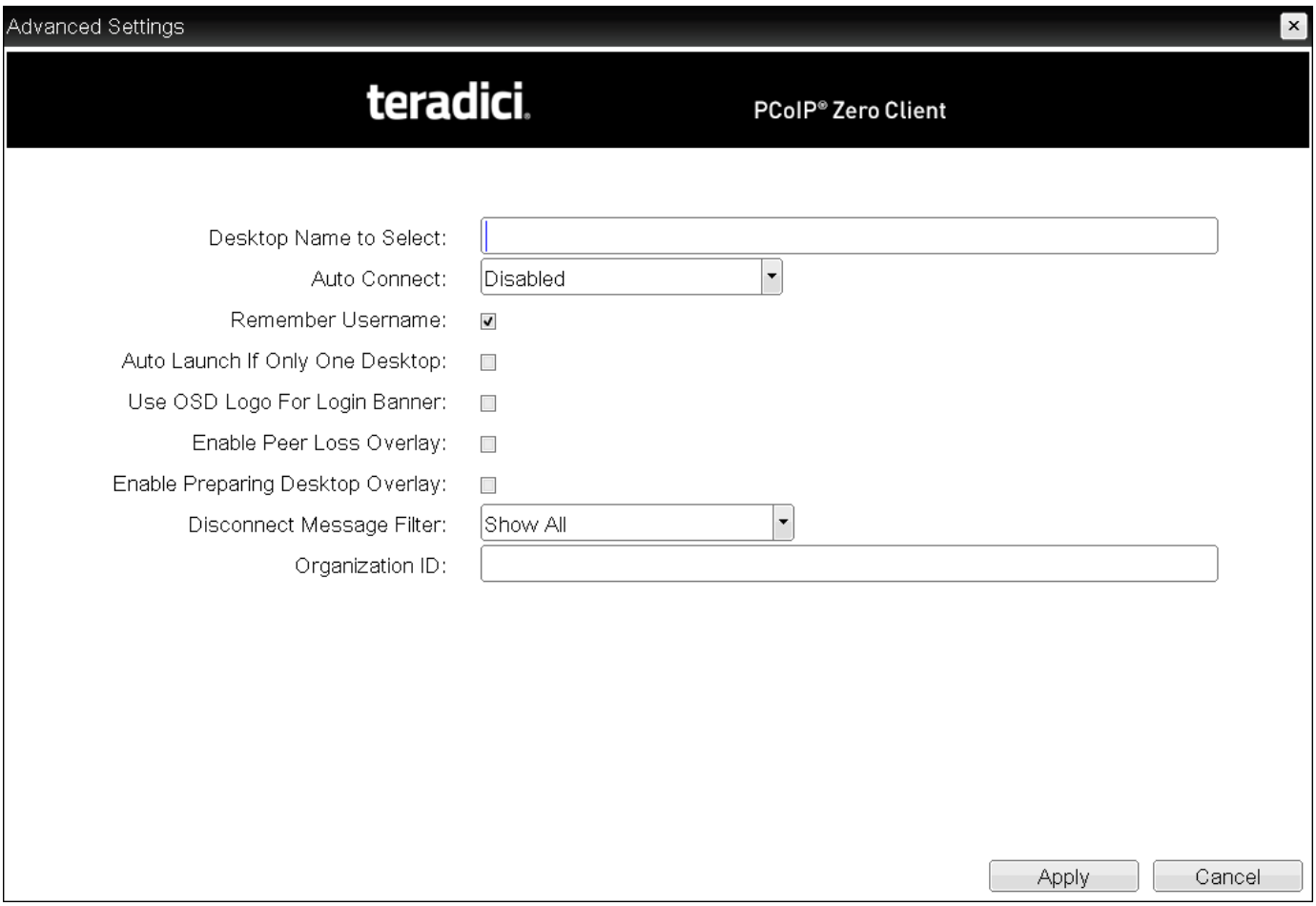
OSD: PCoIP Connection Manager Session Settings

Select the **PCoIP Connection Manager** session connection type from the **Options > Configuration > Session** page to configure the client to use a PCoIP Connection Manager as the PCoIP session broker or when connecting to a Cloud Access Software host.

Click the **Advanced** button to configure advanced settings for this option.



OSD Session connection type – PCoIP Connection Manager



Advanced Settings

The following parameters can be found on the OSD PCoIP Connection Manager page.

OSD PCoIP Connection Manager Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**.
Desktop Name to Select	Enter the desktop name used by the client when starting a session.

Parameter	Description
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

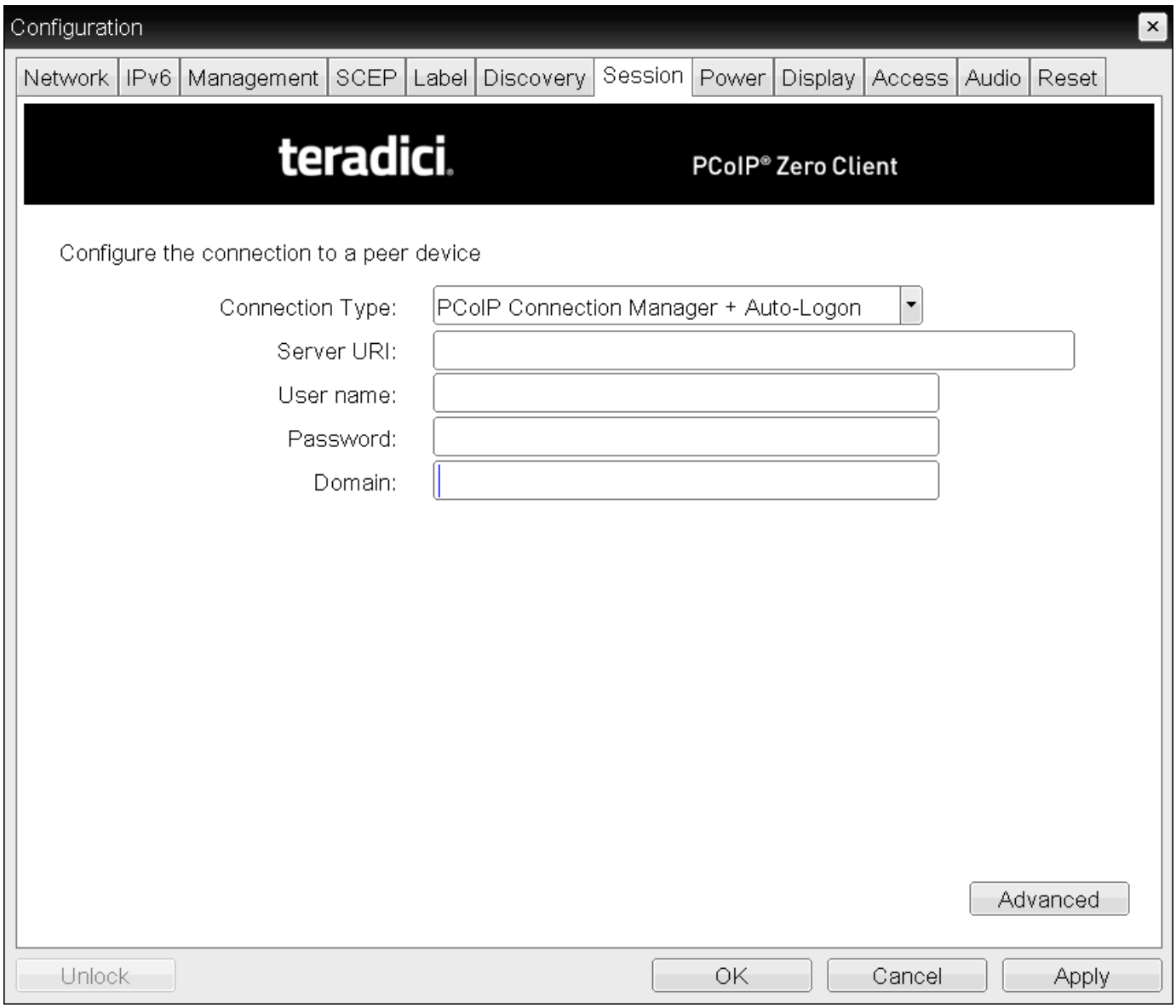
Parameter	Description
Organization ID	Enter an organization ID for the company (for example, 'mycompany.com'). This field accepts any UTF-8 character. You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

OSD: PCoIP Connection Manager + Auto-Logon Session Settings

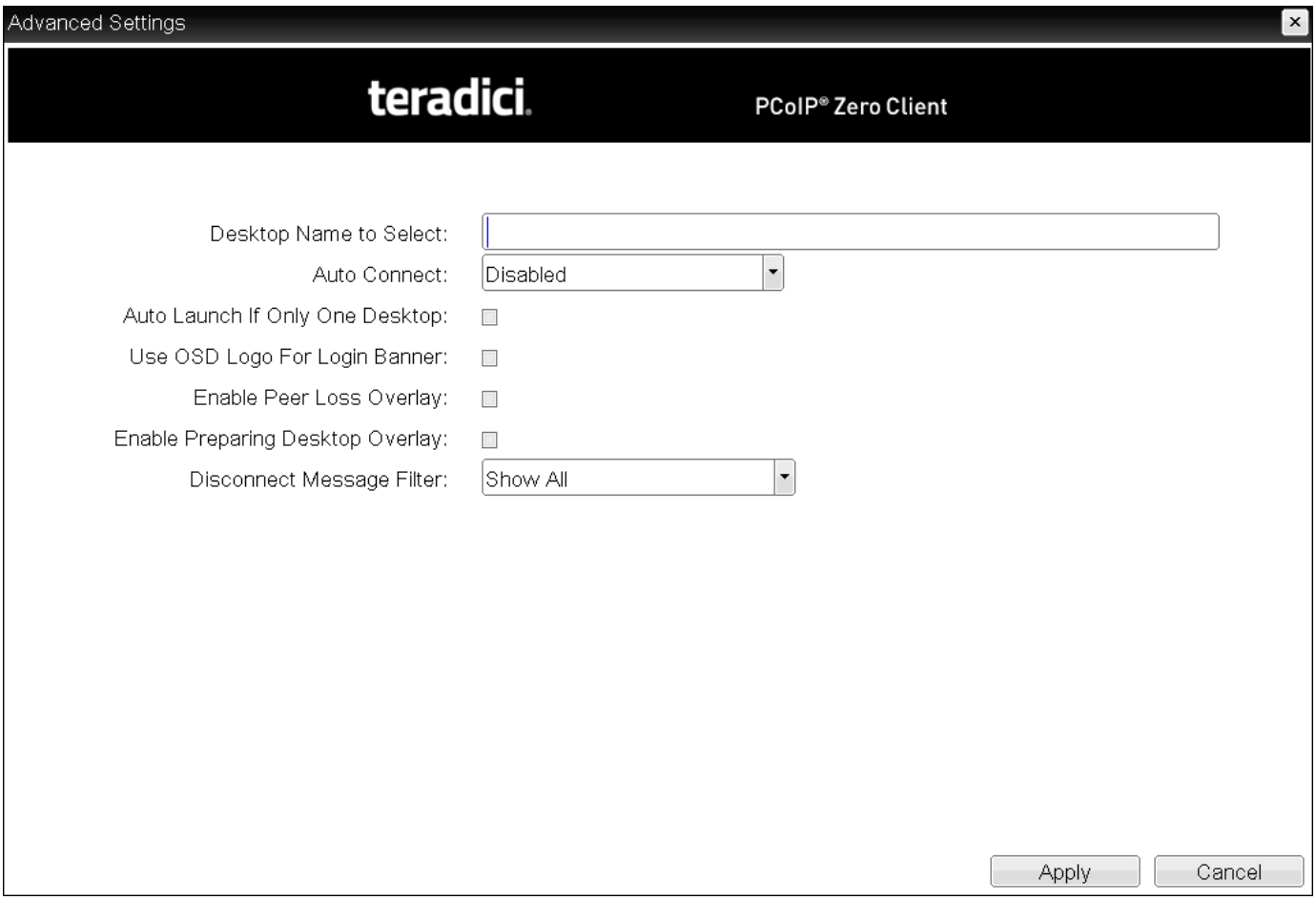
Select the **PCoIP Connection Manager + Auto-Logon** session connection type from the **Options > Configuration > Session** page to configure a client to automatically enter a user's login details when a PCoIP Connection Manager is used as the PCoIP session broker, or when connecting directly to a Cloud Access Software host.

Click the **Advanced** button to configure advanced settings for this option.

> **Take precautions to secure PCoIP Zero Clients**
>
> Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



OSD Session Connection Type – PCoIP Connection Manager + Auto-Logon



Advanced Settings

The following parameters can be found on the OSD PCoIP Connection Manager + Auto-Logon page.

OSD PCoIP Connection Manager + Auto-Logon Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**.
User name	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.

Parameter	Description
Domain	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Desktop Name to Select	Enter the desktop name used by the client when starting a session.
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

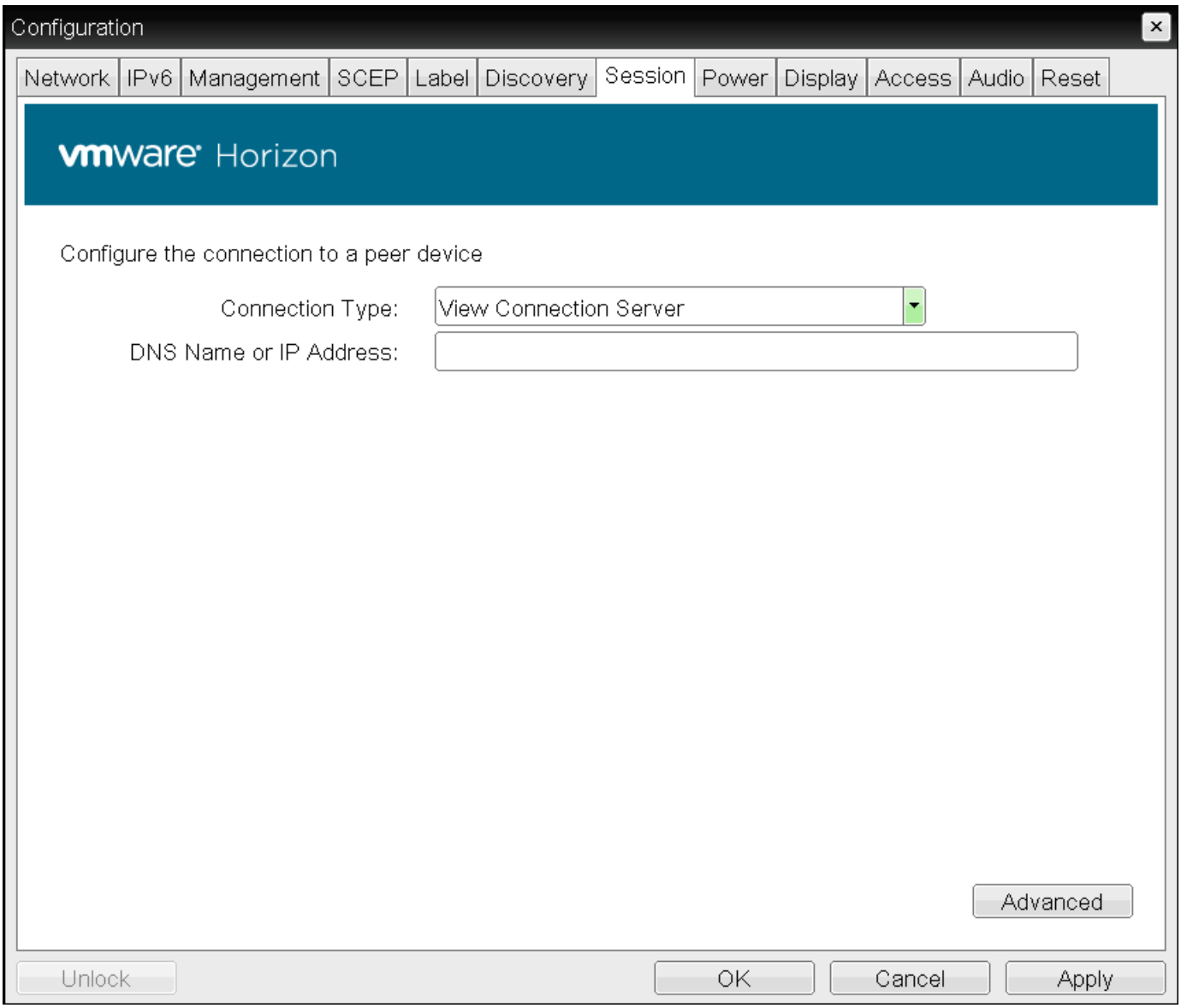
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

OSD: View Connection Server Session Settings

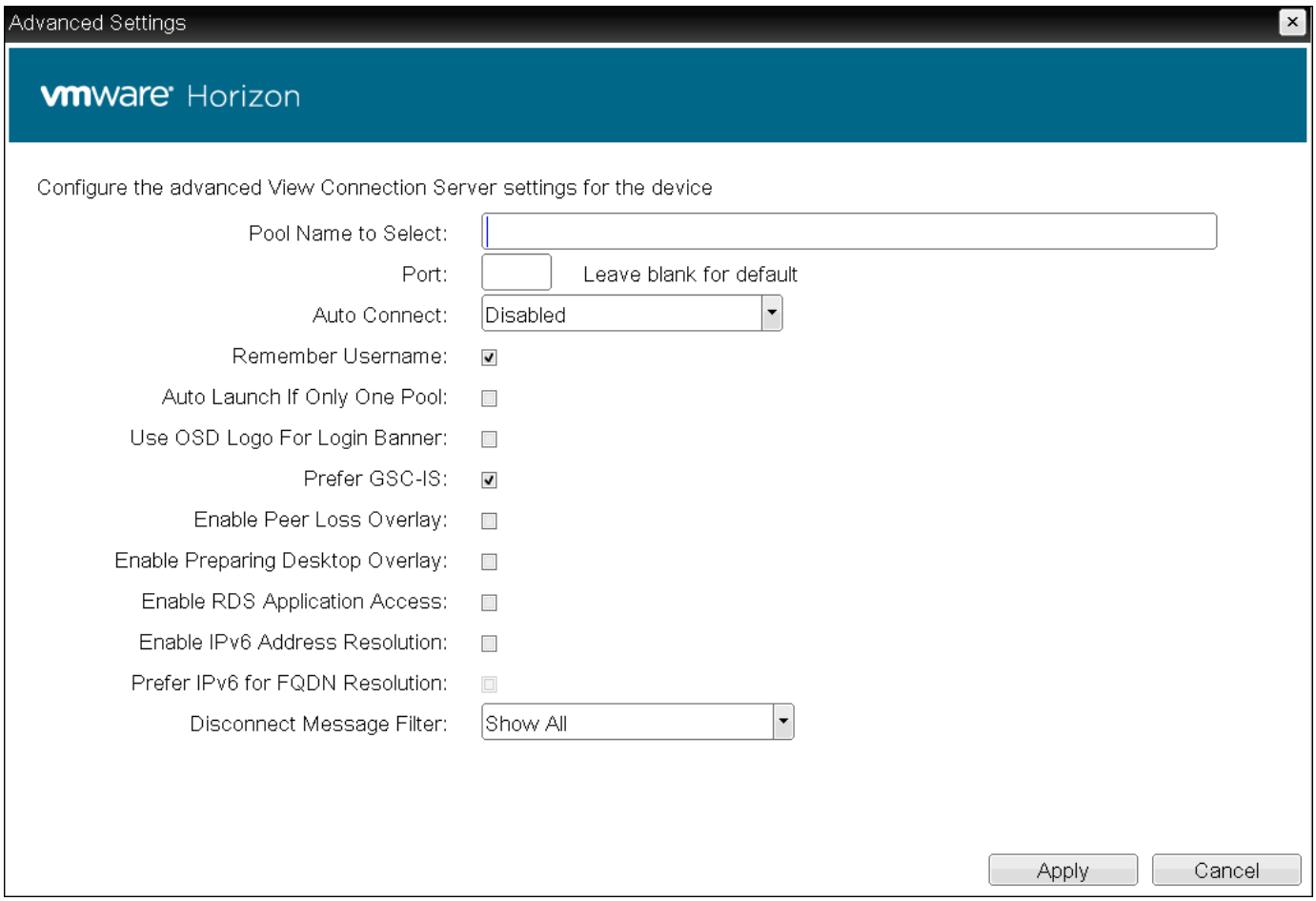
Select the **View Connection Server** session connection type from the **Options > Configuration > Session** page to configure a client to use a View Connection Server as the broker when connecting to a VMware desktop.

> **Connecting a View Connection Server to a workstation**
>
> You can also use a View Connection Server to connect to a workstation with a PCoIP Remote Workstation Card installed. For this option, VMware View Agent must be installed on the remote workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, refer to *Using PCoIP® Host Cards with VMware View*.

Click the **Advanced** button to configure advanced settings for this option.



OSD Session connection type – View Connection Server



Advanced Settings

The following parameters can be found on the OSD View Connection Server page.

OSD View Connection Server Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.

Parameter	Description
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When enabled, if a smart card (CAC) supports more than one interface such as GSC-IS and PIV then GSC-IS is used. However in the case where the card supports both GSC-IS and PIV, and only PIV objects are configured on the card then the connection may fail. If this is the case uncheck the box and retest. If a smart card supports only one interface, such as either GSC-IS or PIV endpoint, then only the GSC-IS or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

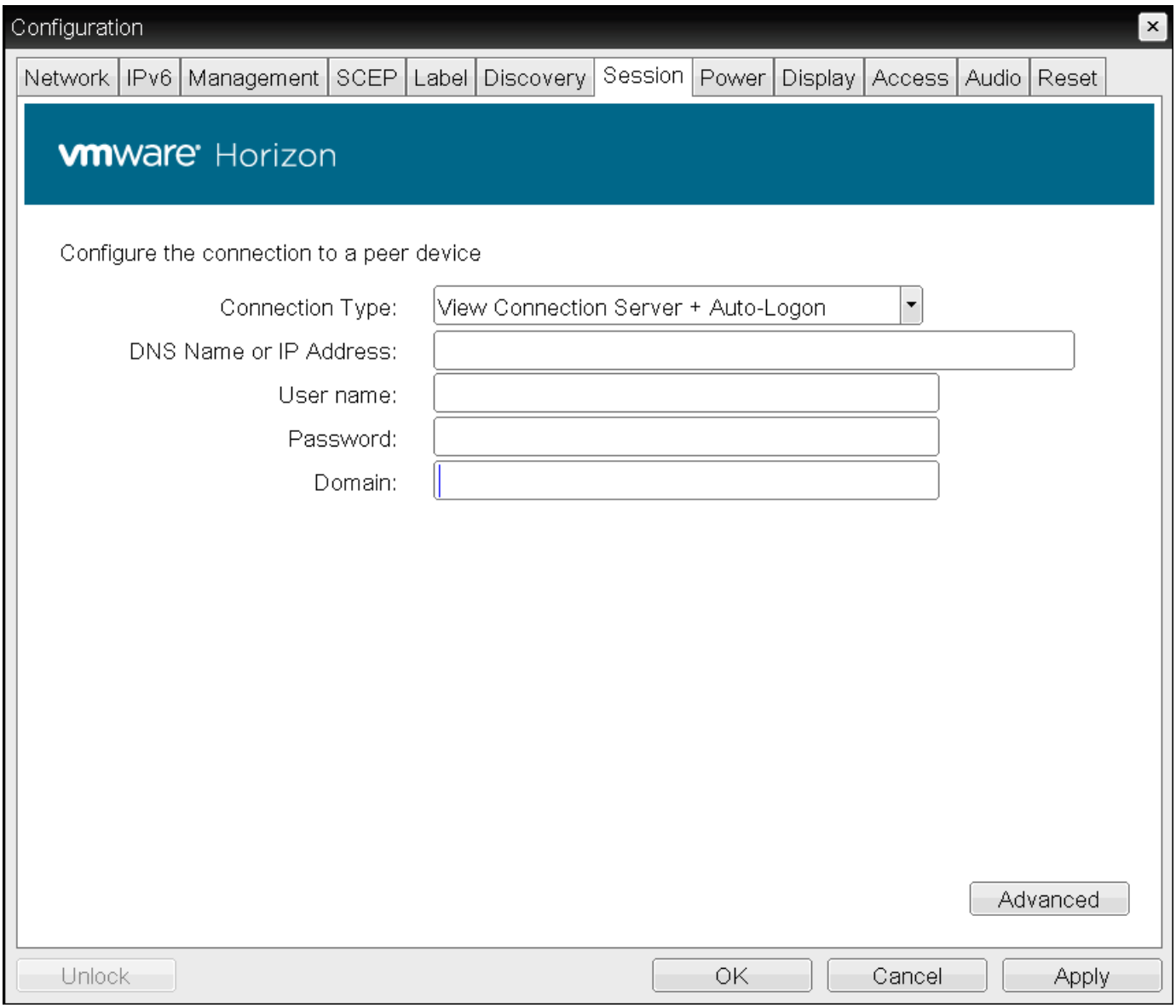
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

OSD: View Connection Server + Auto-Logon Session Settings

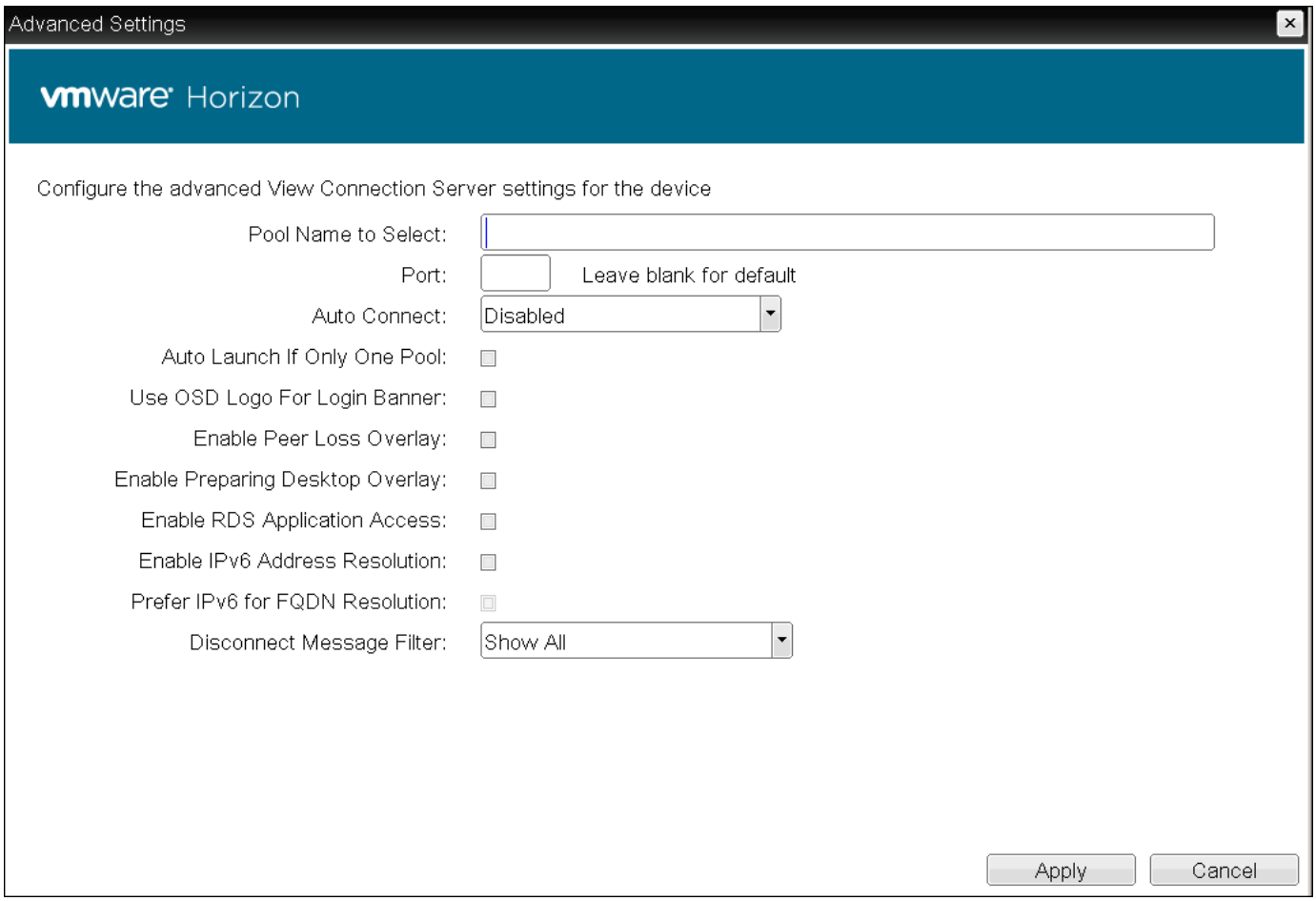
Select the **View Connection Server + Auto-Logon** session connection type from the **Options > Configuration > Session** page to configure a client to automatically enter a user's login details when a View Connection Server is used to connect to a VMware desktop.

Click the **Advanced** button to configure advanced settings for this option.

> **Take precautions to secure PCoIP Zero Clients**
>
> Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



OSD Session connection type – View Connection Server + Auto-Logon



Advanced Settings

The following parameters can be found on the OSD View Connection Server + Auto-Logon page.

OSD View Connection Server + Auto-Logon Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
User name	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Domain	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.

Parameter	Description
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. For Tera1 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

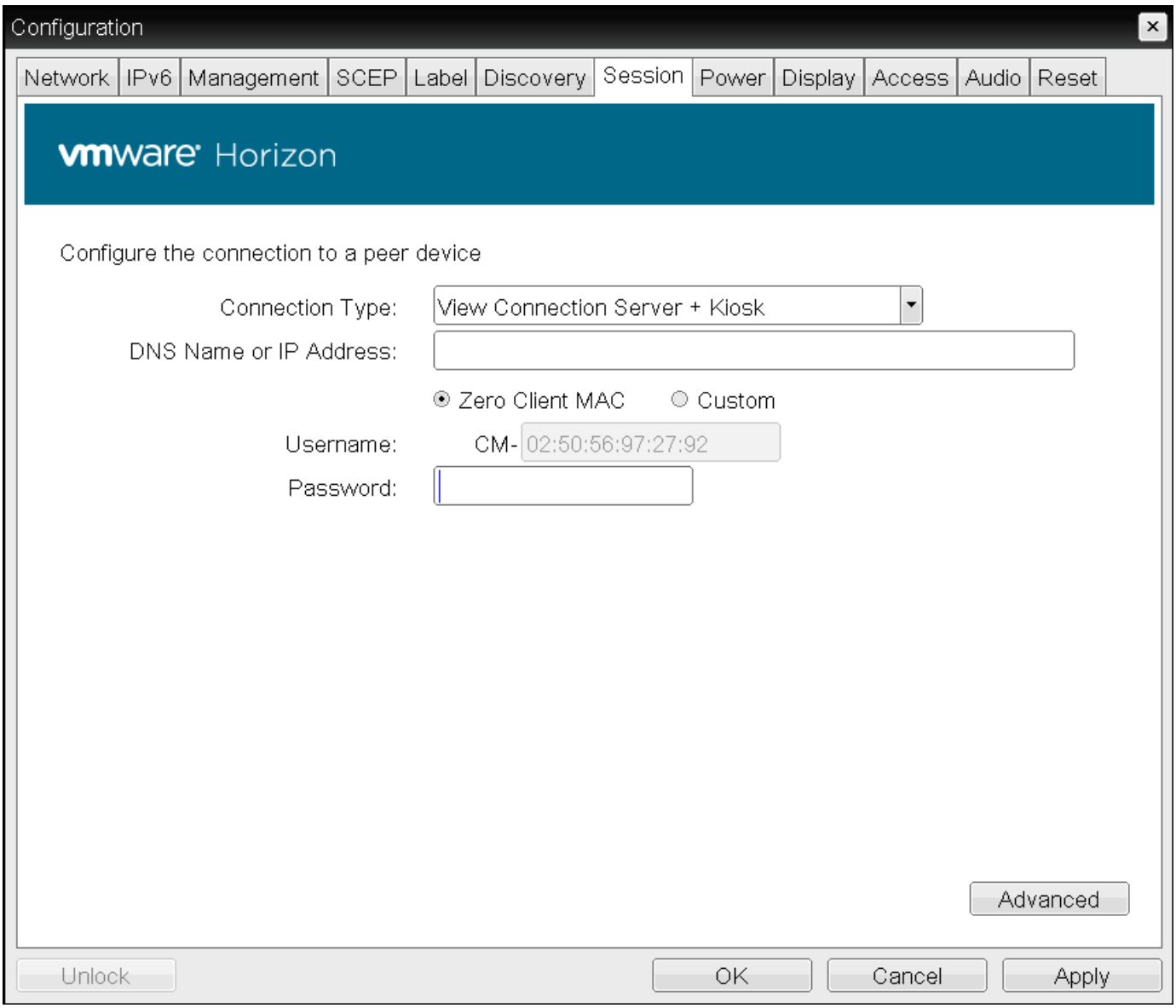
OSD: View Connection Server + Kiosk Session Settings

Select the **View Connection Server + Kiosk** session connection type from the **Options > Configuration > Session** page to configure a client to use Kiosk mode when connecting to a VMware desktop via a View Connection Server.

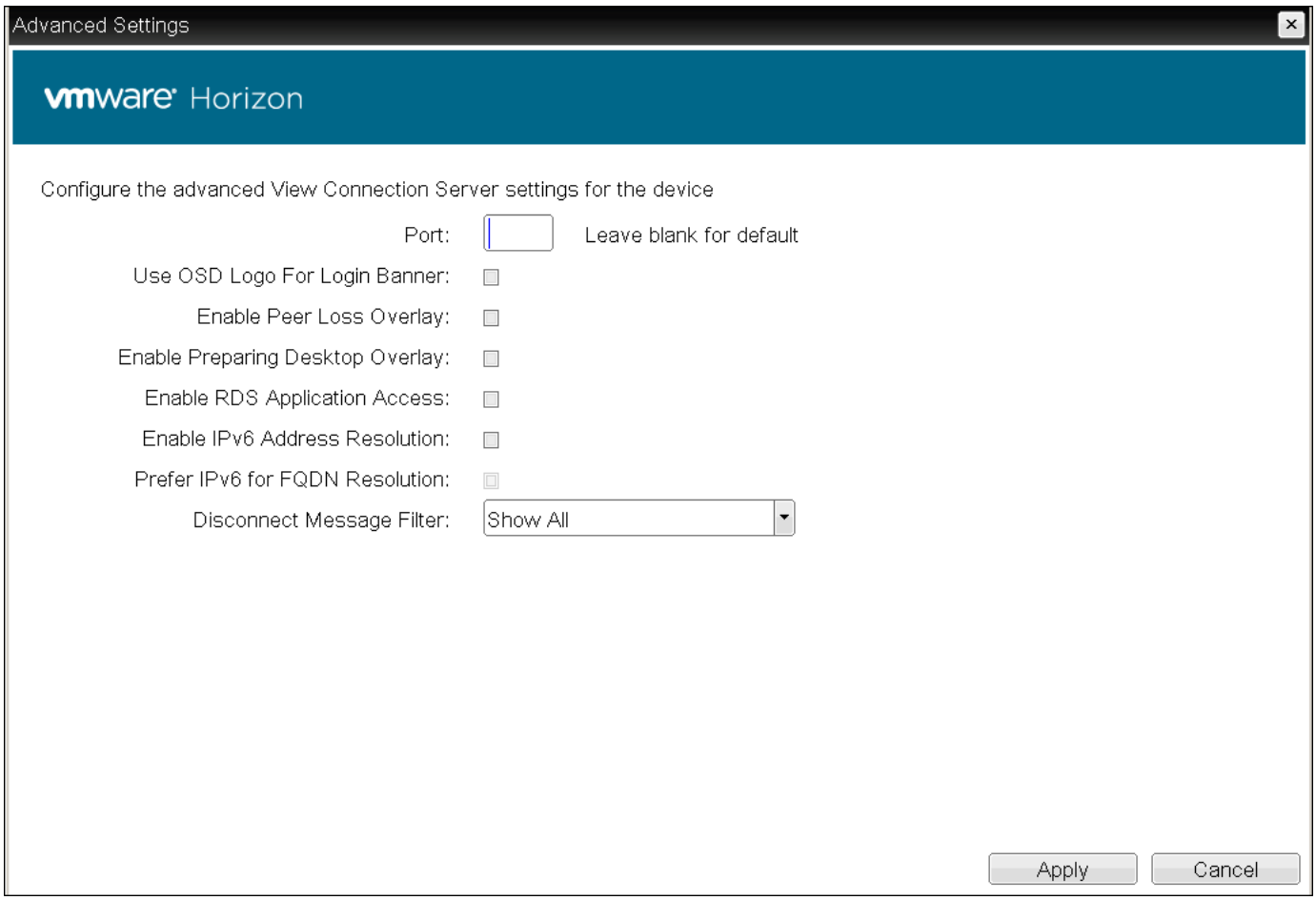
Click the **Advanced** button to configure advanced settings for this option.

Take precautions to secure PCoIP Zero Clients

Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



OSD Session connection type – View Connection Server + Kiosk



Advanced Settings

The following parameters can be found on the OSD View Connection Server + Kiosk page.

OSD View Connection Server + Kiosk Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username	Select the type of user name that matches the naming you use for the devices on the View Connection Server. • **Zero Client MAC**: Select this option to automatically populate the Username field with the MAC address of the Tera2 PCoIP Zero Client. • **Custom**: Enter the user name for the Tera2 PCoIP Zero Client. This user name has the prefix 'Custom'. When **Custom** is selected as the user name type, enter the value for this component of the custom user name. This field is limited to 13 characters.

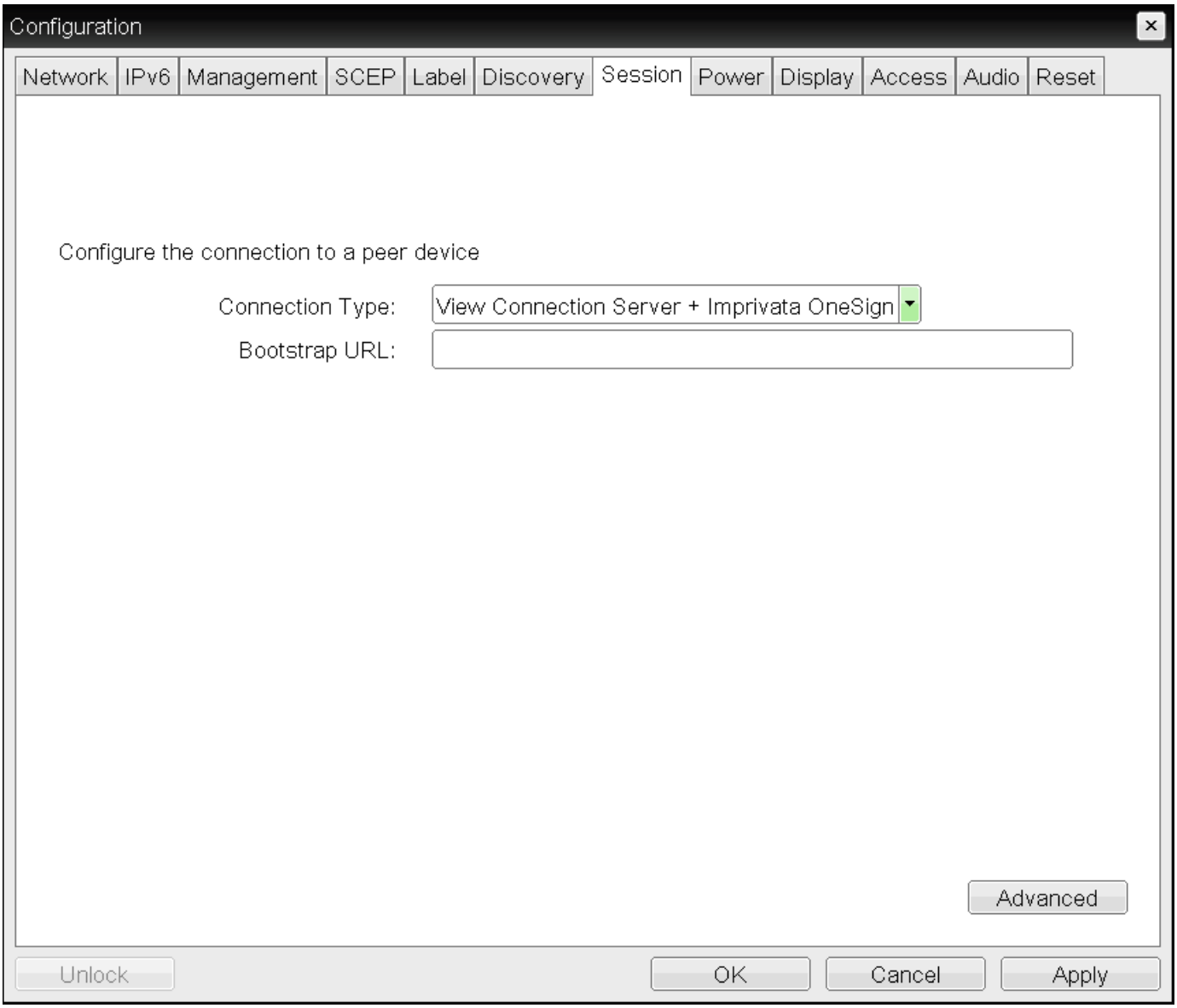
Parameter	Description
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client’s IPv6 address is preferred for FQDN resolution when the client requests a session.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

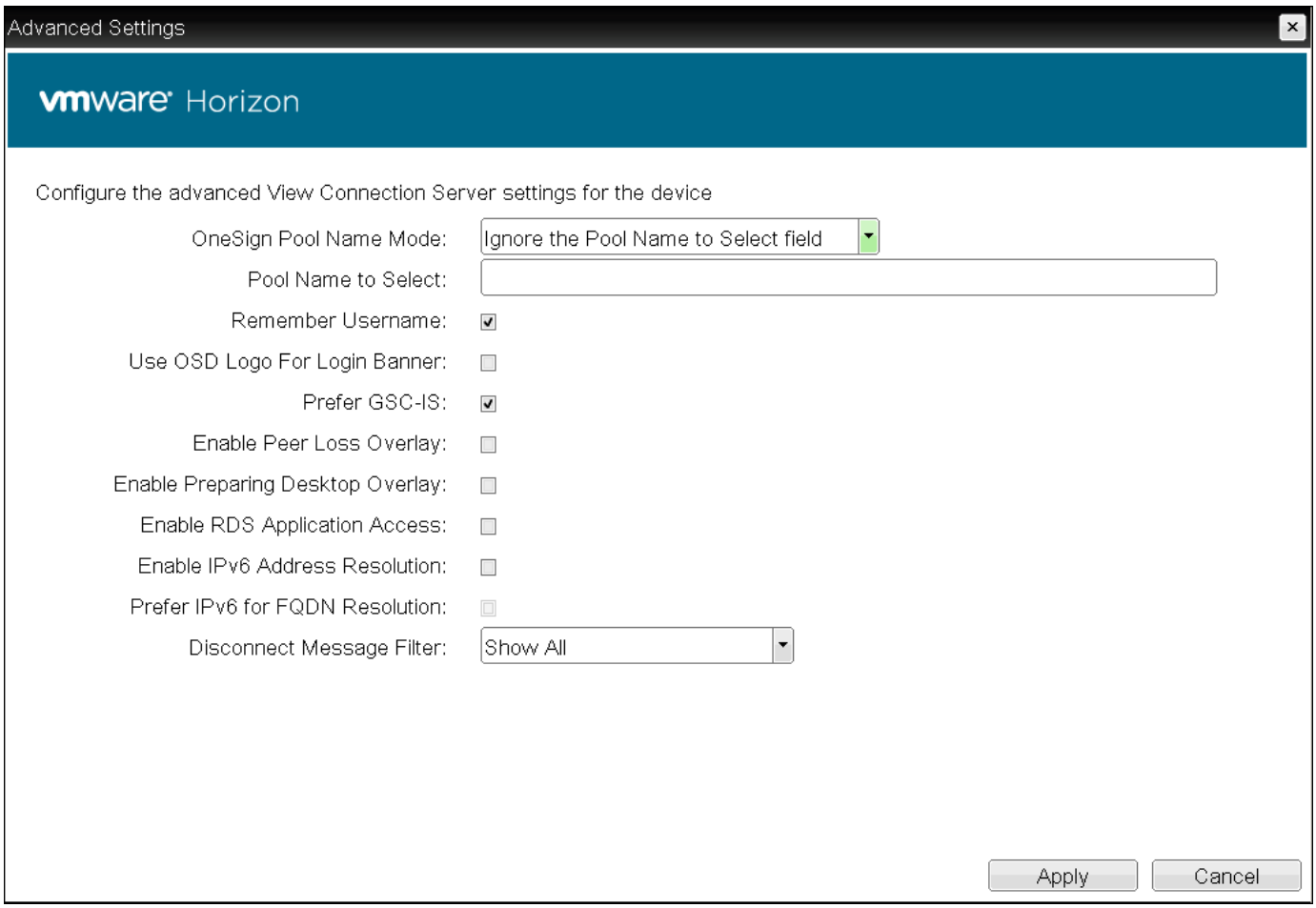
OSD: View Connection Server + Imprivata OneSign Session Settings

Select the **View Connection Server + Imprivata OneSign** session connection type from the **Options > Configuration > Session** page to configure a client to authenticate through the Imprivata OneSign system in addition to a View Connection Server when connecting to a VMware desktop.

Click the **Advanced** button to configure advanced settings for this option.



OSD Session Connection Type - View Connection Server + Imprivata OneSign



Advanced Settings

The following parameters can be found on the OSD View Connection Server + Imprivata OneSign page.

OSD View Connection Server + Imprivata OneSign Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	Select whether the Pool Name to Select property is used in OneSign mode. • Ignore the Pool Name to Select field • Use the Pool Name to Select field if set For Tera1 PCoIP Zero Clients, this parameter is called OneSign Desktop Name Mode.

Parameter	Description
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When enabled, if a smart card (CAC) supports more than one interface such as GSC-IS and PIV then GSC-IS is used. However in the case where the card supports both GSC-IS and PIV, and only PIV objects are configured on the card then the connection may fail. If this is the case uncheck the box and retest. If a smart card supports only one interface, such as either GSC-IS or PIV endpoint, then only the GSC-IS or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client’s IPv6 address is preferred for FQDN resolution when the client requests a session.

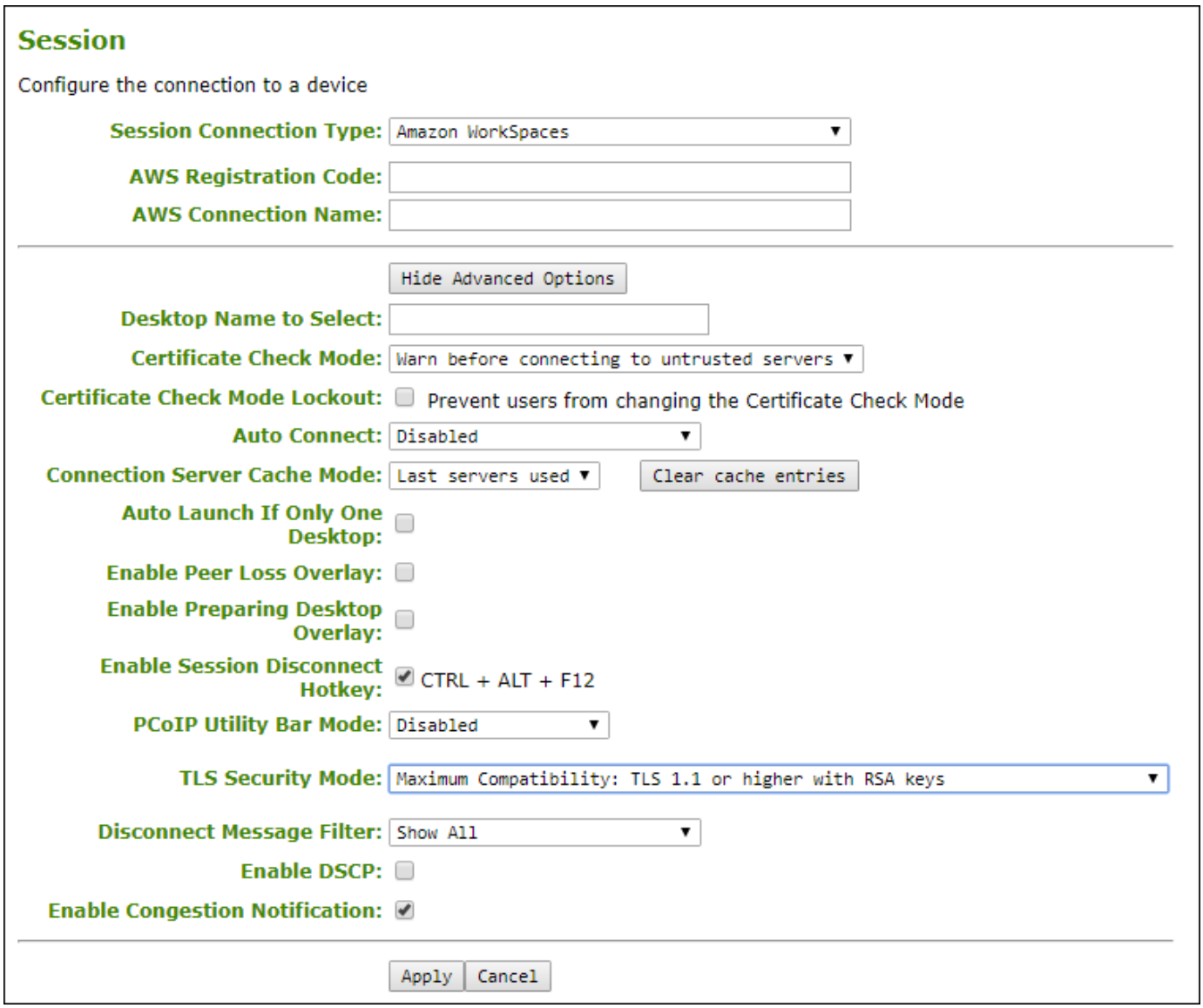
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

AWI: Amazon WorkSpaces

Select the **Amazon WorkSpaces** session connection type from the **Configuration > Session** page to configure the client to connect directly to your Amazon WorkSpaces desktop through multi-factor authentication when connecting with PCoIP Zero Clients on firmware 6.0 or newer. This connection type removes the need to deploy and manage the PCoIP Connection Manager for Amazon WorkSpaces in order to connect PCoIP Zero Clients to Amazon WorkSpaces.

Security

The connection manager determines the security requirements. Amazon WorkSpaces session type uses an Amazon connection manager which requires multi-factor authentication when connecting to Amazon WorkSpaces.



AWI Session Connection type – Amazon WorkSpaces

The following parameters can be found in the AWI Session tab when the Amazon WorkSpaces connection type is selected with the advanced tab showing.

AWI Amazon WorkSpaces

Parameter	Description
AWS Registration Code	Enter the registration code from the invitation email sent after creating your Amazon WorkSpace.

Parameter	Description
AWS Connection Name	Enter a name for this registered Amazon WorkSpace instance.
Desktop Name to Select	Enter the desktop name used by the client when starting a session. This field is case-insensitive.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD.
Auto Connect	This field determines the client's auto connect behavior after startup: • **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • **Disabled:** The client does not automatically connect with the connection server. • **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines which Amazon Workspaces a user can select from the connection drop-down menu on the OSD Connect page. • **Last servers used**: Select this option if you want users to select the cached list of Amazon WorkSpaces. The drop-down lists the previous 50 WorkSpaces that the Zero Client established a successful connection to. If the cache is not cleared, new connections will begin to replace WorkSpaces that were previously cached starting at the oldest saved connection first. • **Read-only**: Select this option if you want users to select an Amazon WorkSpace from a read-only list. This list is created from a PCoIP Management Console profile that has Broker Address Cache List entries. and it will replace the Amazon WorkSpaces cached entries when applied to the Zero Client.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.

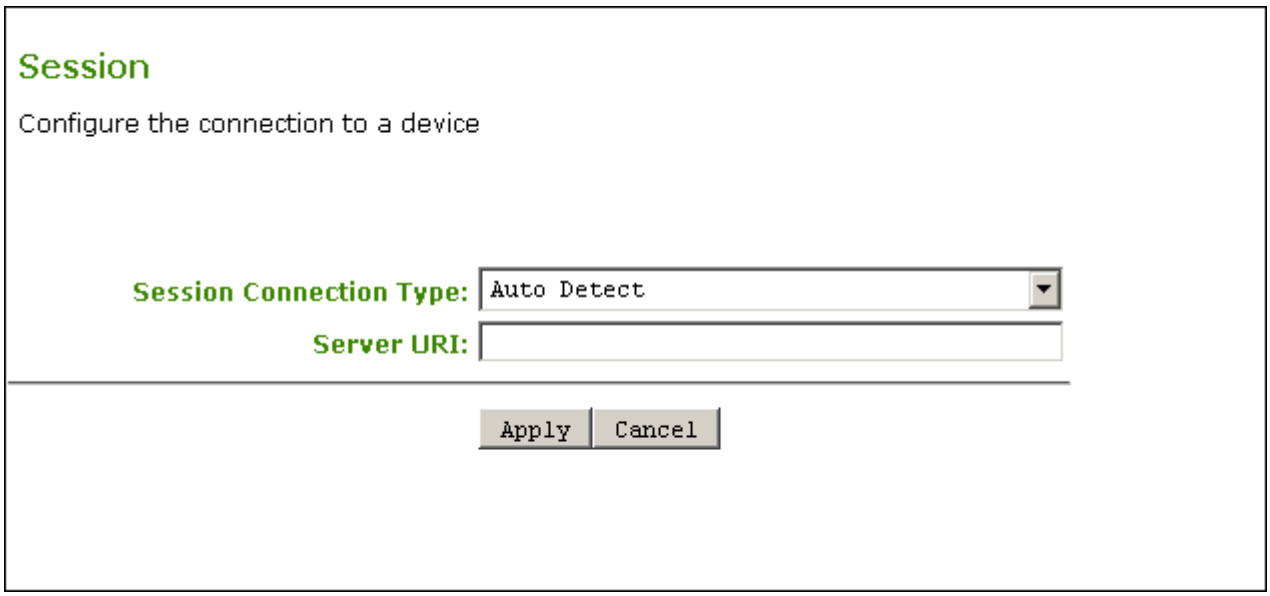
Parameter	Description
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI: Auto Detect Session Settings

Select the **Auto Detect** session connection type from the **Configuration > Session** page to let the Tera2 PCoIP Zero Client automatically detect which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers. Once a successful connection has been made, the server URI will automatically appear in the **Server** drop-down list on the user's OSD **Connect** screen, along with any other desktops the user has successfully connected to. Additionally, you can use **Auto Detect** when connecting directly to Cloud Access Software.



AWI Session connection type – Auto Detect

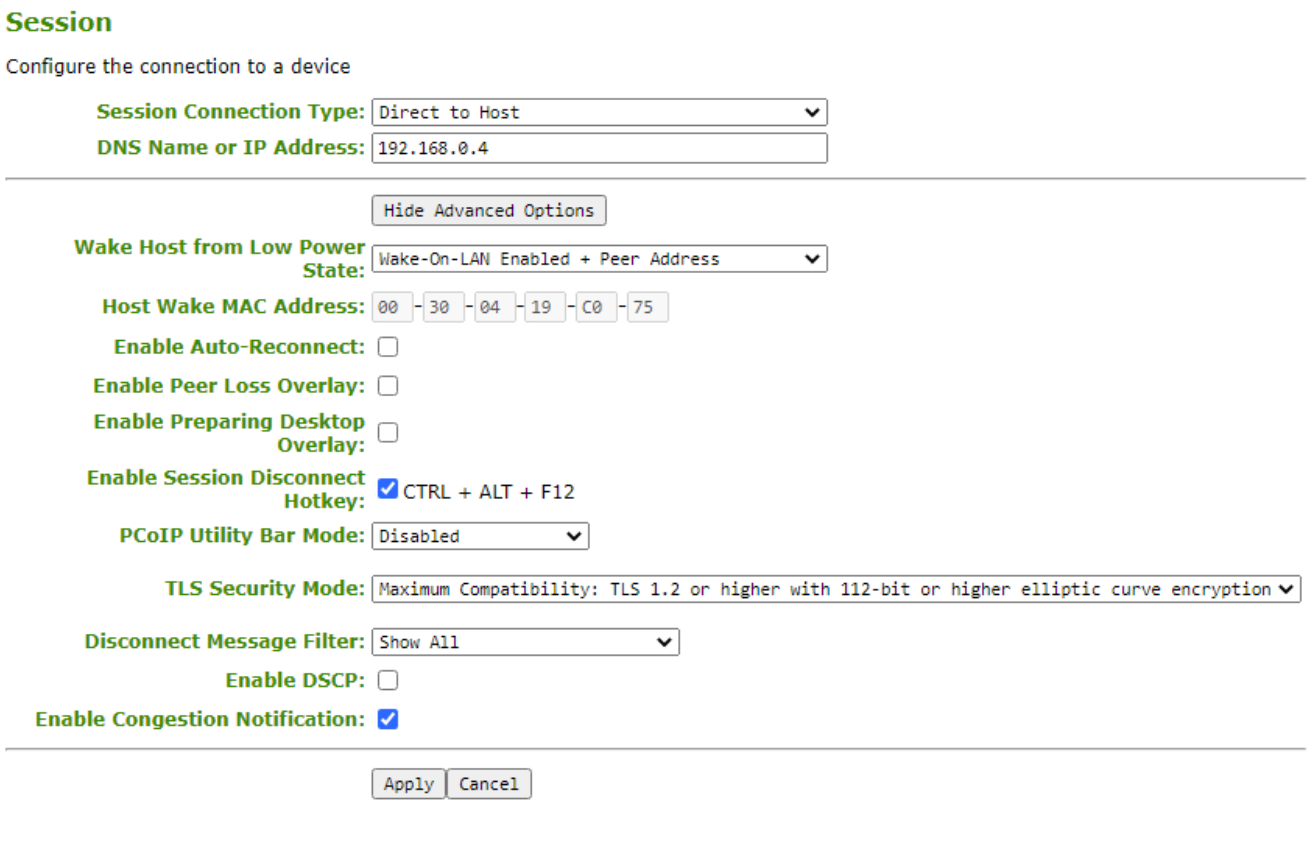
The following parameters can be found on the AWI Auto Detect page.

AWI Auto Detect Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**. Once a successful connection has been made to a connection server, it will appear in the Server drop-down list on the OSD Connect page if the Tera2 PCoIP Zero Client is configured to cache servers.

AWI: Direct to Host Session Settings

Select the **Direct to Host** session connection type from the **Configuration > Session** page to configure the client to connect directly to a Remote Workstation Card.



AWI Session connection type – Direct to Host

The following parameters can be found on the AWI Direct to Host page.

AWI Direct to Host Parameters

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the Remote Workstation Card.

Parameters	Description
Wake Host from Low Power State	Select whether to use the PCoIP Remote Workstation Card's MAC and IP address or a custom MAC and IP address when configuring the Wake-On-LAN feature on a client. This feature wakes up the host when the user presses the client's power button, a key on the keyboard, or clicks the **Connect** button on the Connect window. • **Wake-On-LAN Enabled + Peer Address:** After you have successfully connected to the PCoIP Remote Workstation Card, both the card's MAC address and IP address are automatically populated in the **Host Wake MAC Address** and **Host Wake IP Address** fields. • **Wake-On-LAN Enabled + Custom Address:** When selected, enables you to manually enter the MAC address and IP address of the device you want to wake up. If the Remote Workstation Card Software is installed in the host PC and the **Use host PC NIC for Wake-on-LAN** setting is enabled in the **Features > Power Management** section of the Remote Workstation Card Software GUI, the MAC address and IP address of the host PC's network interface card (NIC) will automatically be populated in the **Host Wake MAC Address** and **Host Wake IP Address** fields. The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet. You can disable the Wake-On-LAN feature from the AWI Power page.
Host Wake MAC Address	Enter the host's MAC address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. When **Wake-On-LAN Enabled + Peer Address** is selected, the host's MAC address is populated after a successful connection. The client will send a 'magic packet' to the MAC address to wake the host computer from a low power state.
Host Wake IP Address	Enter the host's IP address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a 'magic packet' to this IP address to wake the host computer from a low power state.
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

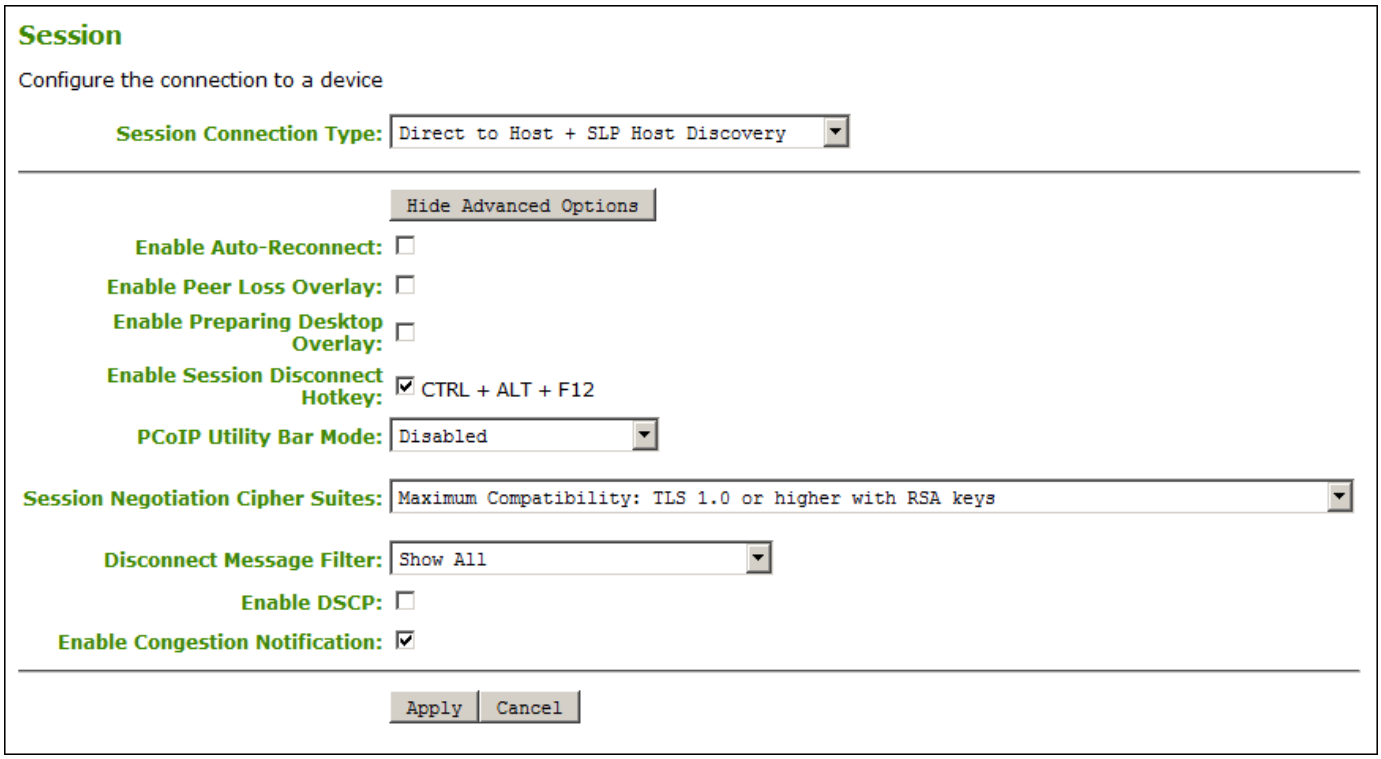
Parameters	Description
Enable Preparing Desktop Overlay	When a user first logs into a PCoIP session, this overlay appears with the message: **Preparing desktop...**
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameters	Description
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI: Direct to Host + SLP Host Discovery Session Settings

Select the **Direct to Host + SLP Host Discovery** session connection type from the **Configuration > Session** page to configure the client to connect directly to a host and to use Service Location Protocol (SLP) to discover the host automatically.



AWI Session connection type – Direct to Host + SLP Host Discovery

The following parameters can be found on the AWI Direct to Host + SLP Host Discovery page.

AWI Direct to Host + SLP Host Discovery Parameters

Parameters	Description
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.

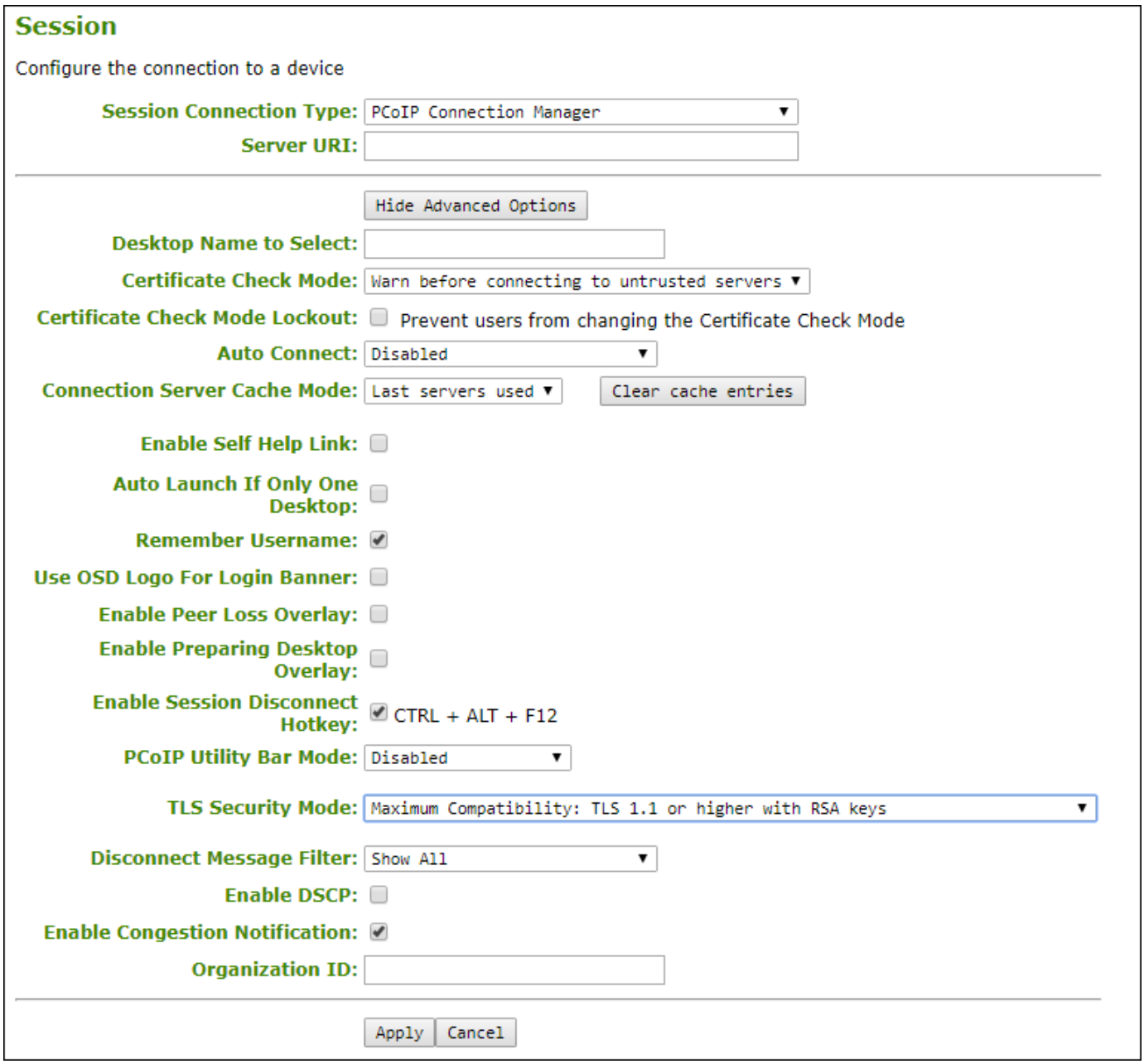
Parameters	Description
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameters	Description
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI: PCoIP Connection Manager Session Settings

Select the PCoIP Connection Manager session connection type from the Configuration > Session page to configure the client to use a PCoIP Connection Manager as the PCoIP session broker or when connecting to a Cloud Access Software host.



AWI Session connection type – PCoIP Connection Manager

The following parameters can be found on the AWI PCoIP Connection Manager page.

AWI PCoIP Connection Manager Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**.
Desktop Name to Select	Enter the desktop name used by the client when starting a session. This field is case-insensitive.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD.
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. The cache lists the previous 25 servers that established a successful connection. If the cache is not cleared, new connections will begin to replace servers that were previously cached starting at the oldest saved connection first. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. This list is created using the PCoIP Management Console. This list will replace the cached listed servers when it is selected for use.
Enable Self Help Link	See Enabling the Self Help Link for details.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

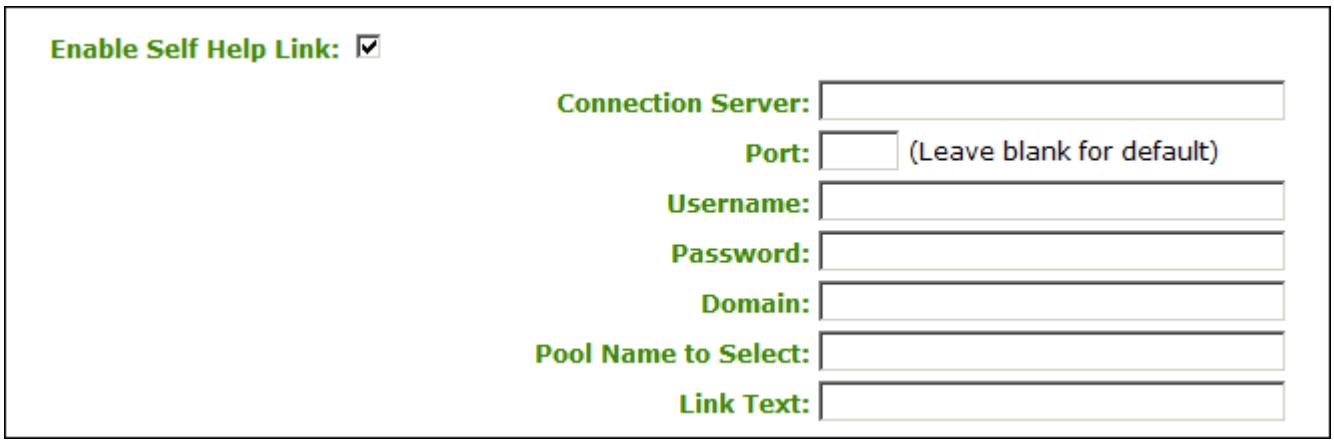
Parameter	Description
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.
Organization ID	Enter an organization ID for the company (for example, 'mycompany.com'). This field accepts any UTF-8 character. You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

Enabling the Self Help Link

The **Self Help Link** option lets you configure a self-help link that will appear on the OSD Connect window. When users click this link, they are automatically connected to a specific desktop that can be used as a corporate resource—for example, a desktop containing IT help information. After enabling this option, you configure all the necessary details to automatically log users in to the desktop that you specify. You also configure the link text that you want to appear on the Connect window.



Enable Self Help Link options

When you enable this field, the following options appear:

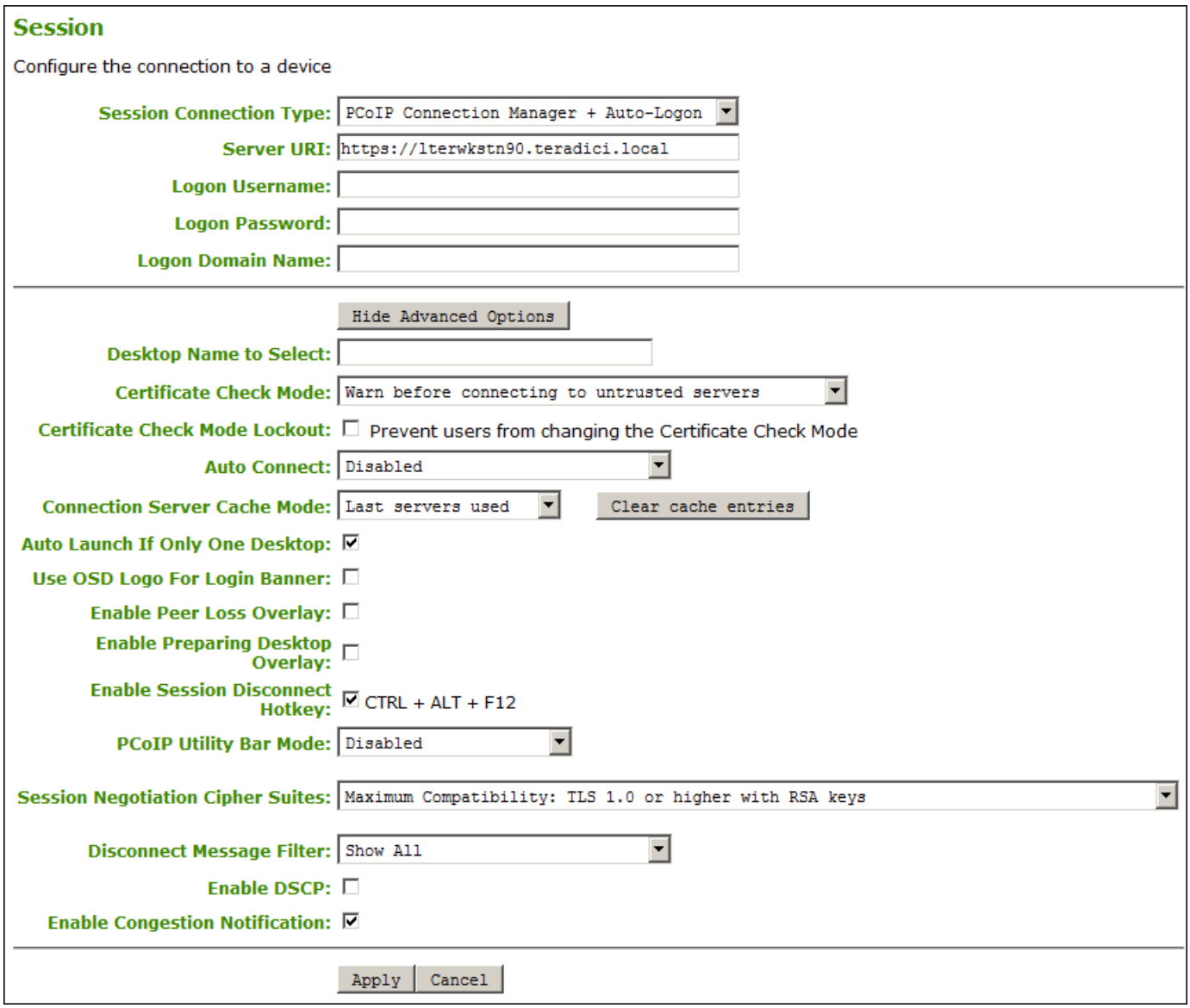
Parameter	Description
Connection Server	Enter the fully-qualified domain name of the connection server brokering the desktop (for example, a PCoIP Connection Manager for a PCoIP Connection Manager session connection type, or a View Connection Server for a View Connection Server session connection type).
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Username	To password protect the self-help desktop, enter a username in this field.
Password	To password protect the self-help desktop, enter a password in this field.
Domain	Enter the domain name for the self-help desktop (for example, mycompany.com).
Pool Name to Select	Enter the pool or desktop name for the self-help desktop.
Link Text	Enter the text that you want to appear as hyperlinked text on the Connect window.

AWI: PCoIP Connection Manager + Auto-Logon Session Settings

Select the **PCoIP Connection Manager + Auto-Logon** session connection type from the **Configuration > Session** page to configure the client to automatically enter a user's login details when a PCoIP Connection Manager is used as the PCoIP session broker, or when connecting directly to a Cloud Access Software host.

Take precautions to secure PCoIP Zero Clients

Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



AWI Session Connection type – PCoIP Connection Manager + Auto-Logon

The following parameters can be found on the AWI PCoIP Connection Manager + Auto-Logon page.

AWI PCoIP Connection Manager + Auto-Logon Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager or the Cloud Access Software host when connecting directly to Cloud Access Software. The URI must be in the form **https://<host FQDN>** or **https://<ip address>**.

Parameter	Description
Logon Username	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Logon Domain Name	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Desktop Name to Select	Enter the desktop name used by the client when starting a session. This field is case sensitive.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.

Parameter	Description
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. The cache lists the previous 25 servers that established a successful connection. If the cache is not cleared, new connections will begin to replace servers that were previously cached starting at the oldest saved connection first. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. This list is created using the PCoIP Management Console. This list will replace the cached listed servers when it is selected for use.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

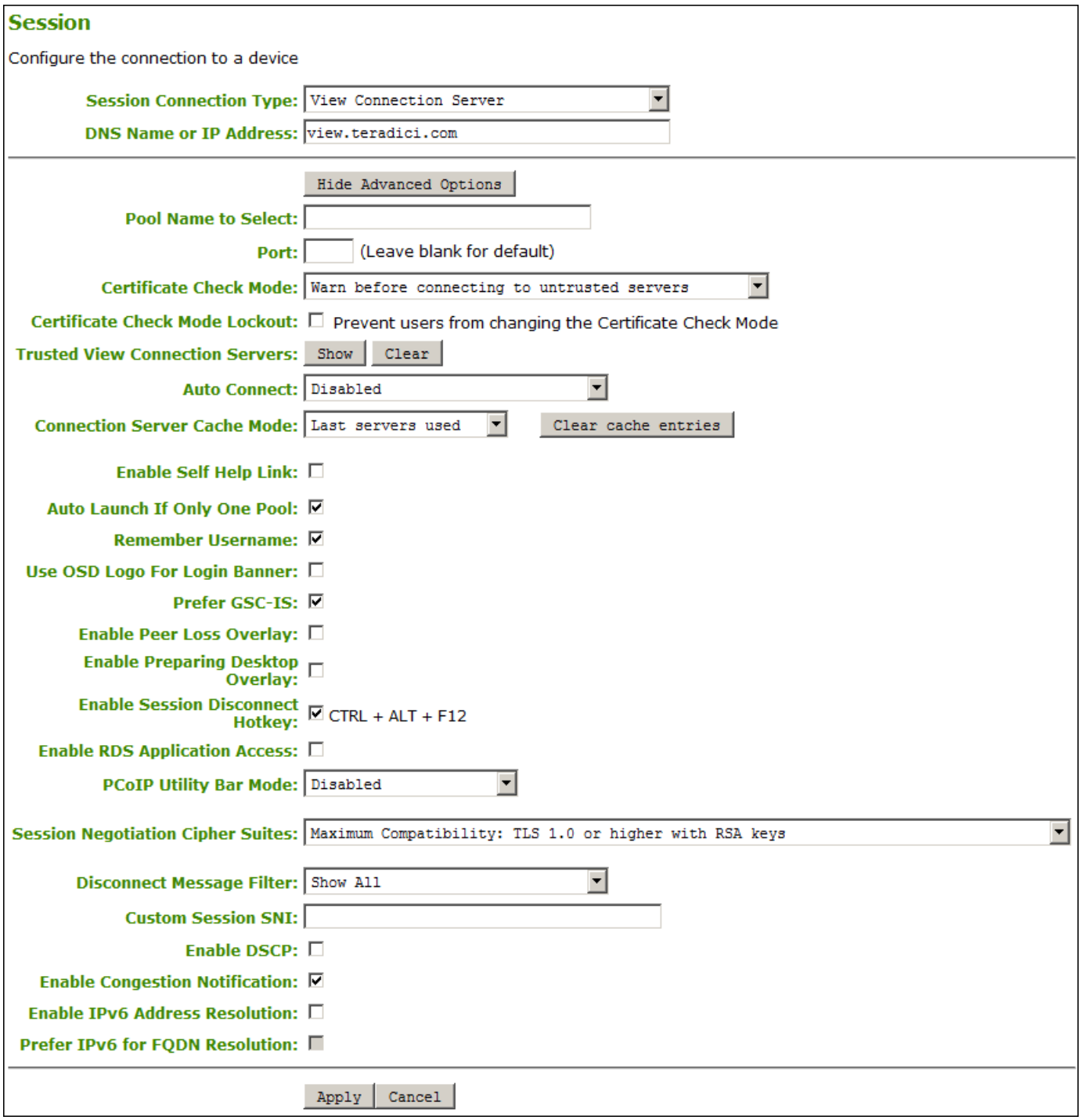
Parameter	Description
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI: View Connection Server Session Settings

Select the View Connection Server session connection type from the ***Configuration > Session*** page to configure the client to use a View Connection Server as the broker when connecting to a VMware desktop.

Connecting a View Connection Server to a workstation

You can also use a View Connection Server to connect to a workstation with a PCoIP Remote Workstation Card installed. For this option, VMware View Agent must be installed on the remote workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, refer to Using PCoIP® Host Cards with VMware View or reference KB 1044.



AWI Session Connection type – View Connection Server

The following parameters can be found on the AWI View Connection Server page.

AWI View Connection Server Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling Auto Connect, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. The cache lists the previous 25 servers that established a successful connection. If the cache is not cleared, new connections will begin to replace servers that were previously cached starting at the oldest saved connection first. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. This list is created using the PCoIP Management Console. This list will replace the cached listed servers when it is selected for use.
Enable Self Help Link	See Enabling the Self Help Link for details.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. For Tera2 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop. • This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When enabled, if a smart card (CAC) supports more than one interface such as GSC-IS and PIV then GSC-IS is used. However in the case where the card supports both GSC-IS and PIV, and only PIV objects are configured on the card then the connection may fail. If this is the case uncheck the box and retest. If a smart card supports only one interface, such as either GSC-IS or PIV endpoint, then only the GSC-IS or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

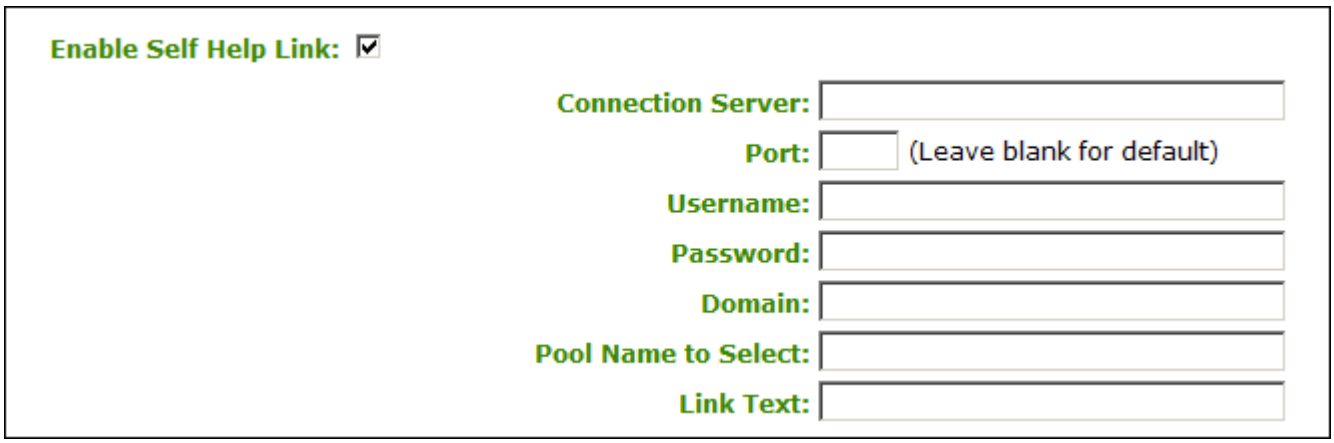
Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. • This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. • Applications open in full-screen mode, but can be re-sized once users are in session.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). **Disabled:** Disables the PCoIP Utility Bar. By default, the utility bar is disabled. **Enabled:** Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. **Enabled and Pinned:** Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. **Maximum Compatibility:** TLS 1.2 or higher with 112-bit or higher elliptic curve encryption: This option provides maximum compatibility. **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

Enabling the Self Help Link

The **Self Help Link** option lets you configure a self-help link that will appear on the OSD Connect window. When users click this link, they are automatically connected to a specific desktop that can be used as a corporate resource—for example, a desktop containing IT help information. After enabling this option, you configure all the necessary details to automatically log users in to the desktop that you specify. You also configure the link text that you want to appear on the Connect window.



Enable Self Help Link options

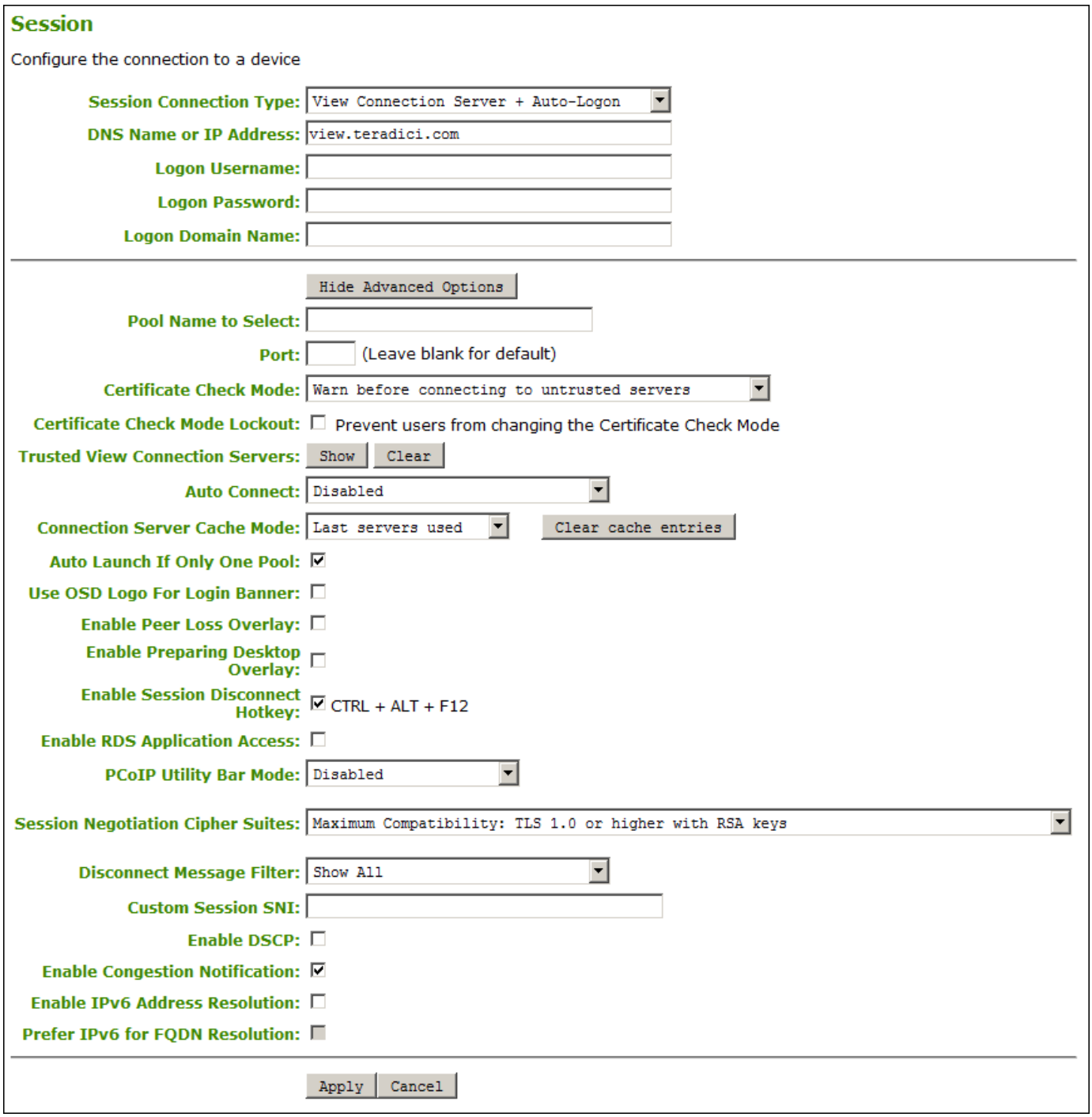
When you enable this field, the following options appear:

Parameter	Description
Connection Server	Enter the fully-qualified domain name of the connection server brokering the desktop (for example, a PCoIP Connection Manager for a PCoIP Connection Manager session connection type, or a View Connection Server for a View Connection Server session connection type).
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Username	To password protect the self-help desktop, enter a username in this field.
Password	To password protect the self-help desktop, enter a password in this field.
Domain	Enter the domain name for the self-help desktop (for example, mycompany.com).
Pool Name to Select	Enter the pool or desktop name for the self-help desktop.
Link Text	Enter the text that you want to appear as hyperlinked text on the Connect window.

AWI: View Connection Server + Auto-Logon Session Settings

Select the **View Connection Server + Auto-Logon** session connection type from the **Configuration > Session** page to configure the client to automatically enter a user's login details when a View Connection Server is used to connect to a VMware desktop.

> **Take precautions to secure PCoIP Zero Clients**
>
> Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



AWI Session Connection type – View Connection Server + Auto-Logon

The following parameters can be found on the AWI View Connection Server + Auto-Logon page.

AWI View Connection Server + Auto-Logon Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Logon Username	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Logon Domain Name	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.

Parameter	Description
Auto Connect	This field determines the client's auto connect behavior after startup: **Enabled:** The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. **Disabled:** The client does not automatically connect with the connection server. **Enabled With Retry On Error:** The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected. After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. The cache lists the previous 25 servers that established a successful connection. If the cache is not cleared, new connections will begin to replace servers that were previously cached starting at the oldest saved connection first. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. This list is created using the PCoIP Management Console. This list will replace the cached listed servers when it is selected for use.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. For Tera2 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop. This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

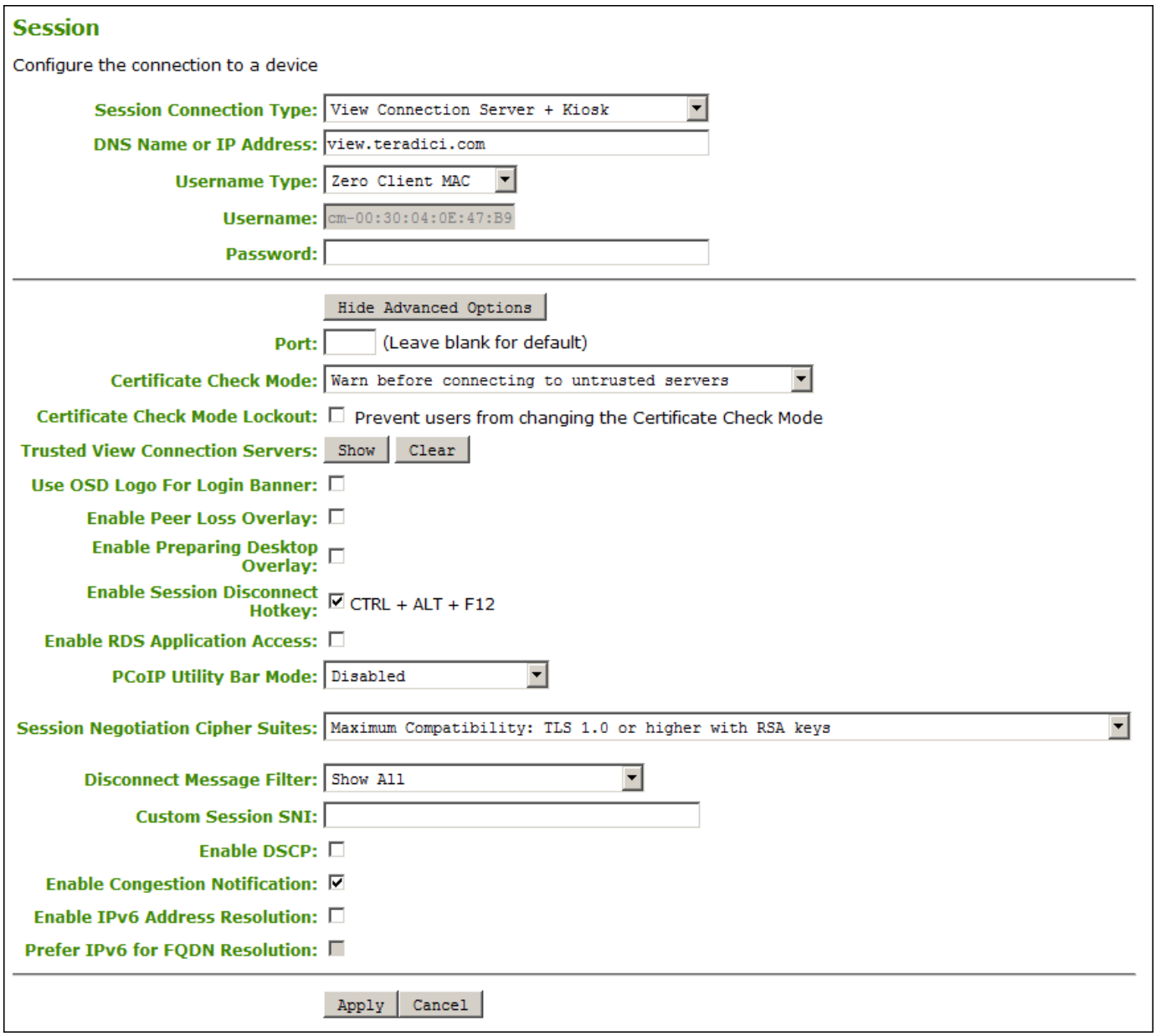
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

AWI: View Connection Server + Kiosk Session Settings

Select the **View Connection Server + Kiosk session** connection type from the **Configuration > Session page** to configure the client to use Kiosk mode when a View Connection Server is used to connect to a VMware desktop.

> **Take precautions to secure PCoIP Zero Clients**
>
> Passwords are stored locally in retrievable form when PCoIP Zero Clients are configured with this session connection type. For this reason, it should not be used in high security environments. Ensure that you take precautions to prevent theft of the zero client if you do use this session connection type.



AWI Session Connection type – View Connection Server + Kiosk

The following parameters can be found on the AWI Session Connection Server + Kiosk page.

AWI View Connection Server + Kiosk Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.

Parameter	Description
Username Type	Select the type of user name that matches the naming you use for the devices on the View Connection Server. • **Zero Client MAC:** Select this option to automatically populate the Username field with the MAC address of the Tera2 PCoIP Zero Client. • **Custom:** Enter the user name for the Tera2 PCoIP Zero Client. This user name has the prefix 'Custom'.
Username	When Custom is selected as the user name type, enter the value for this component of the custom user name. This field is limited to 13 characters.
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.

Parameter	Description
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.

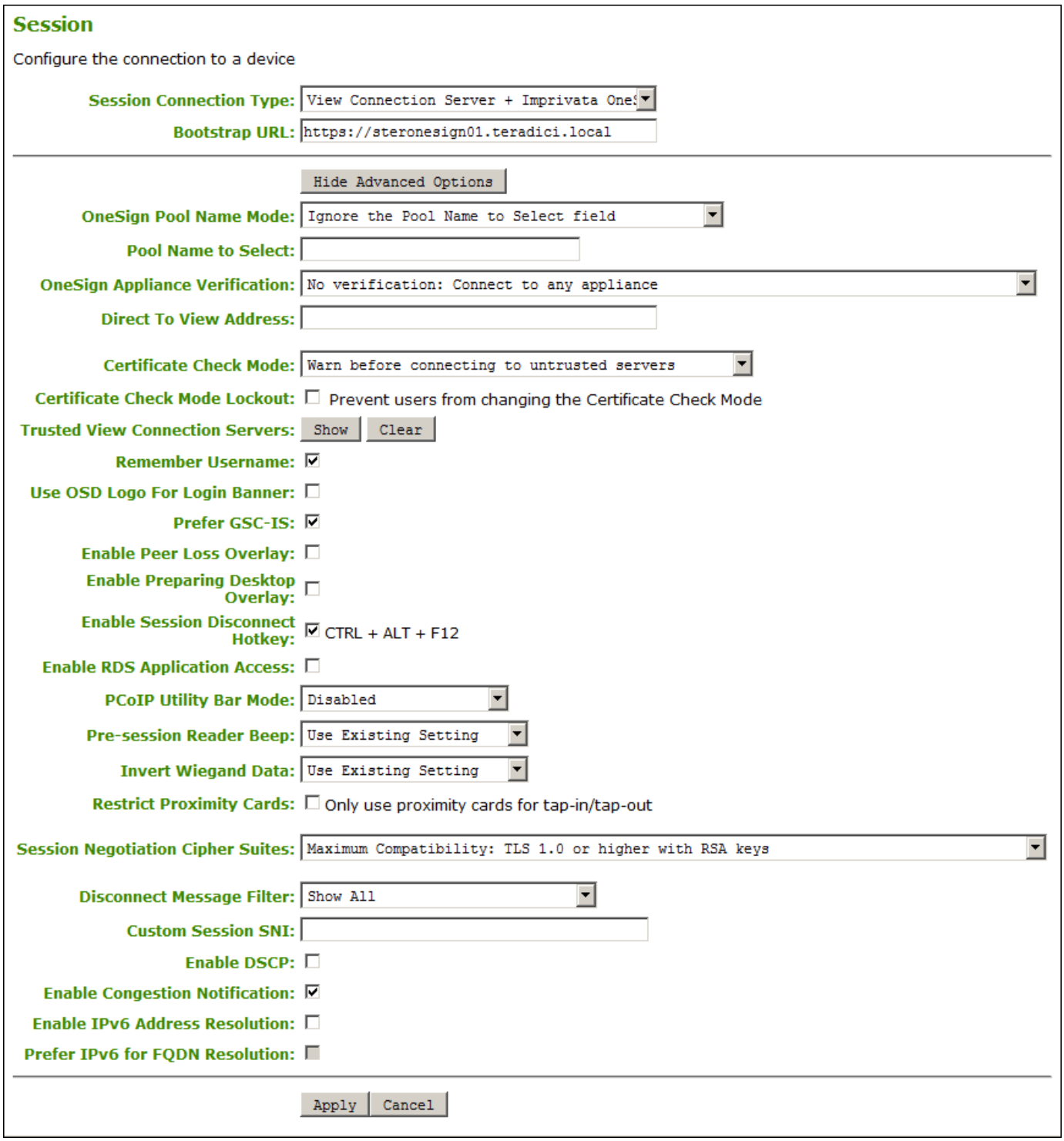
Parameter	Description
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

AWI: View Connection Server + Imprivata OneSign Session Settings

Select the View Connection Server + Imprivata OneSign session connection type from the Configuration > Session page to configure the client to authenticate through the Imprivata OneSign system in addition to a View Connection Server when connecting to a VMware desktop.



AWI Session Connection type – View Connection Server + Imprivata OneSign

The following parameters can be found on the AWI View Connection Server + Imprivata OneSign page.

AWI View Connection Server + Imprivata OneSign Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	Select whether the Pool Name to Select property is used in OneSign mode. • **Ignore the Pool Name to Select field** • **Use the Pool Name to Select field if set** For Tera1 PCoIP Zero Clients, this parameter is called OneSign Desktop Name Mode.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.
Onesign Appliance Verification	Select the level of verification performed on the certificate presented by the OneSign appliance server: • **No verification:** Connect to any appliance • **Full verification:** Only connect to appliances with verified certificates
Direct To View Address	Enter the address of the View Connection Server to use when OneSign servers cannot be reached. When configured, a Direct to View link occurs on the OSD Connect page and user authentication screens. When users click the link, it cancels the current OneSign connection or authentication flow and starts a Horizon View authentication flow instead. This feature provides a mechanism for OneSign PCoIP Zero Client users to access their View desktops when the OneSign infrastructure is unavailable.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers:** Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers:** Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates:** Configure the client to enable all connections. (This option is not secure.)

Parameter	Description
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When enabled, if a smart card (CAC) supports more than one interface such as GSC-IS and PIV then GSC-IS is used. However in the case where the card supports both GSC-IS and PIV, and only PIV objects are configured on the card then the connection may fail. If this is the case uncheck the box and retest. If a smart card supports only one interface, such as either GSC-IS or PIV endpoint, then only the GSC-IS or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in. This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Session Disconnect Hotkey	When enabled, users can press the `Ctrl`+`Alt`+`F12` hotkey sequence to quickly disconnect a PCoIP session. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Applications open in full-screen mode, but can be re-sized once users are in session.

Parameter	Description
PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For **Direct to Host** session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • **Disabled**: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • **Enabled**: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • **Enabled and Pinned**: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Pre-session Reader Beep	Configure whether the proximity card reader beeps when a valid card is tapped on the reader in OneSign mode: • **Disabled:** Disables the feature. • **Enabled:** Enables the feature. • **Use Existing Setting:** Uses the existing setting (affects only devices running firmware 4.1.0 or greater)
Invert Wiegand Data	Configure whether or not the rf IDEAS proximity reader will invert the Wiegand bits that are read from a user's ID token. This feature is useful when some of the rf IDEAS readers in your system are programmed to invert the Wiegand data and others are not. It lets you configure all readers to read the bits in a consistent manner (whether inverted or not inverted), so that all the readers behave the same way from a user's point of view. • **Disabled:** Disables the feature. Wiegand data are not inverted. • **Enabled:** Enables the feature. Wiegand data are inverted. • **Use Existing Setting:** Uses the existing setting (affects only devices running firmware 4.2.0 or greater). This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.

Parameter	Description
Restrict Proximity Cards	Configure whether or not proximity cards are restricted to tap-in/tap-out only. When this feature is enabled, the proximity card reader is locally terminated (that is, it uses drivers in the client's firmware), and proximity cards can only be used for tap-in/tap-out. When this feature is disabled, the proximity card reader is bridged by default (that is, it uses drivers in the host OS), and proximity cards are not restricted. They can be used for tap-in/tap-out and also during a session—for example, when an application requires in-session authentication. • **Only use proximity cards for tap-in/tap-out:** Enables/disables the feature. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption.** This option provides a higher level of security.

Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. **Warning:** System-initiated, but expected actions affecting the session: • You have been disconnected because your session timed out. **Error:** Unexpected system-initiated actions causing session to fail: • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance.

Parameter	Description
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format.
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

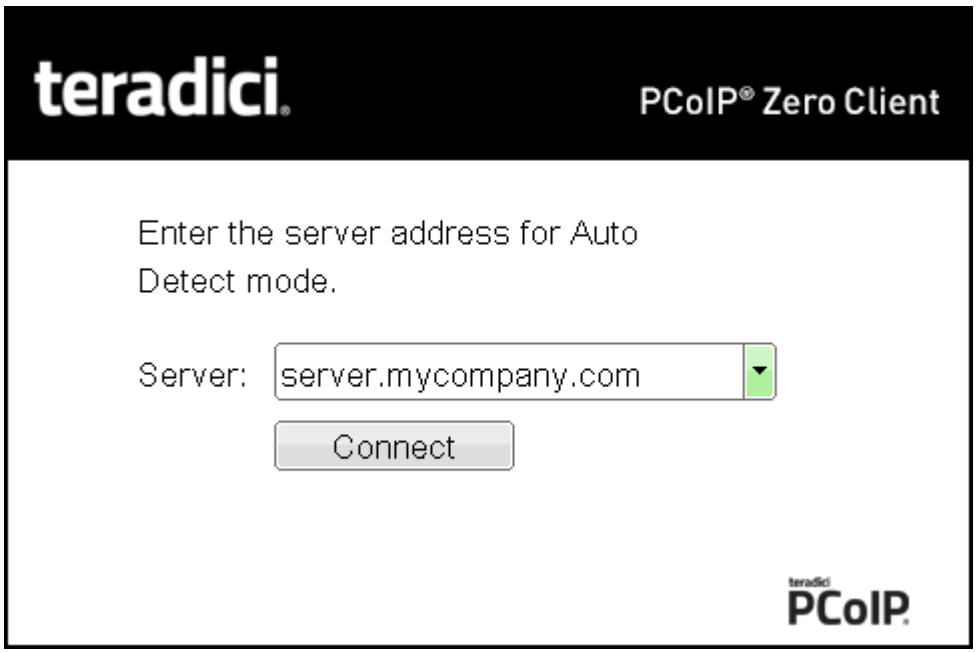
Connecting to a Session

The OSD enables users to create a PCoIP session between the client and a remote resource by clicking the green **Connect** button in the center of the Connect window.

Connecting to a Session from the Connect Window

1. Enter the requested information (for example, server name or IP address for Auto Detect, PCoIP Connection Manager, View Connection Server) and click **Connect**. If your Tera2 PCoIP Zero Client is configured to cache servers in **Last servers used** mode, this server name will subsequently appear in the Server drop-down list after a successful connection is made.
2. If you have already connected to a server, it will appear in the Server drop-down list if your Tera2 PCoIP Zero Client is configured to connect to this server or if it is configured to cache servers in **Last servers used** mode. Select the server from the drop-down list and click **Connect**.
3. If your Tera2 PCoIP Zero Client is configured to connect directly to a PCoIP Remote Workstation Card, you only need to click **Connect**.

The Connect window differs slightly depending on the session connection type you configure. The following examples show the Connect window for the Auto Detect and Direct to Host session connection type.



OSD Auto Detect window

OSD Direct to Host connect window

While the network connection is initializing, various status messages are displayed above the button to indicate the progress. If problems are experienced during startup—for example, if the connection cannot be made or a DHCP lease fails—other messages display in this area to indicate the nature of the problem.

Once the connection is established, the local GUI disappears, and the session image appears.

Connecting to a Session Using Smart Cards

Users can connect to a session using smart cards when connected to VMware View virtual desktops or a PCoIP Connection Manager that supports this feature.

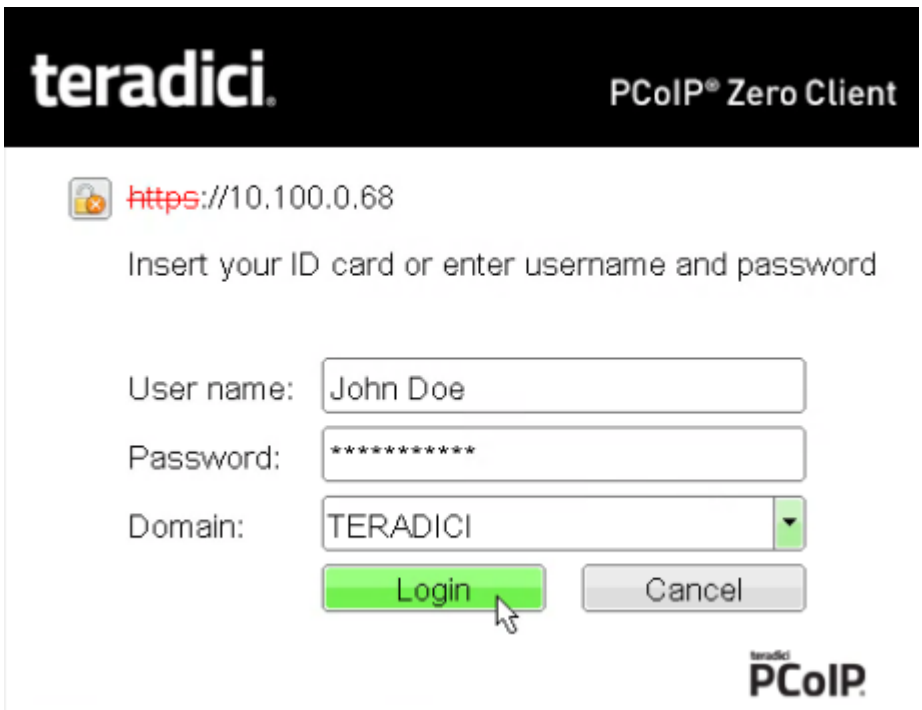
This section addresses using smart cards when connected to a PCoIP Connection Manager.

Before connecting to a session using a smart card, connect the USB smart card reader into the Tera2 PCoIP Zero Client.

While the network connection is initializing, various status messages are displayed to indicate the progress. If problems are experienced during startup—for example, if the connection cannot be made—other messages display in this area to indicate the nature of the problem. Once the connection is established, the local GUI disappears, and the session image appears.

To connect to a session using a smart card:

1. Insert a supported smart card into a supported USB smart card reader. The Connect window appears. The Connect window may differ slightly depending on your configuration: for example, the **User name** and **Domain** fields may be read-only.



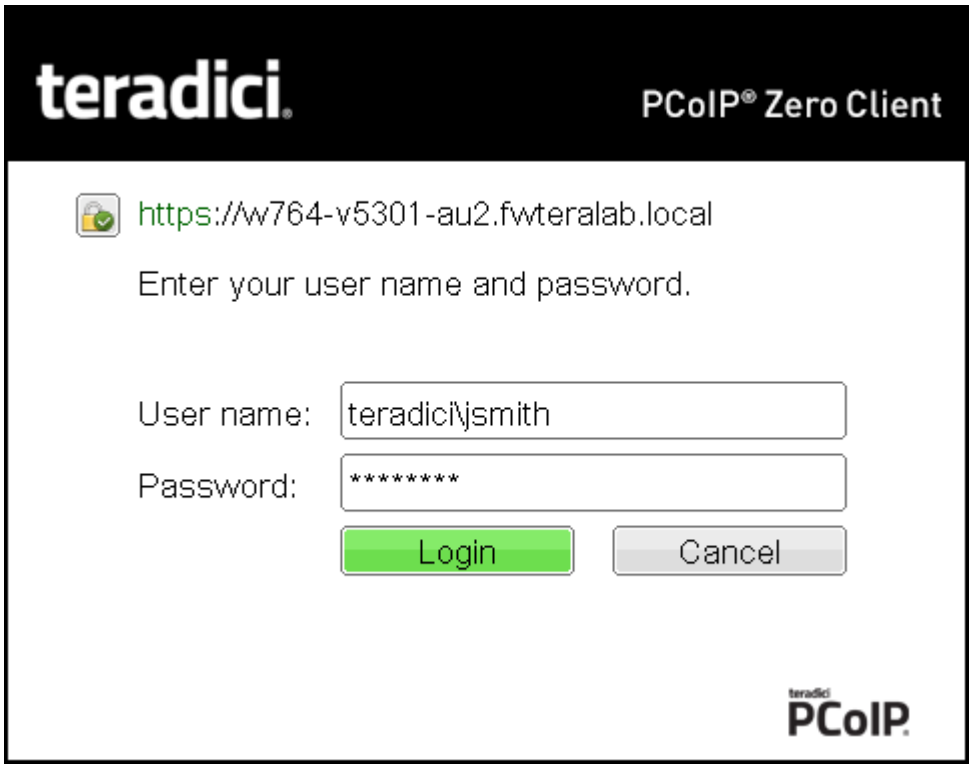
2. If required, type your credentials.

Making a Trusted HTTPS Connection

After connecting to the connection server, a user authentication page displays to enable the user to enter login credentials. The banner on this page indicates the type of connection.

If the correct trusted SSL root certificate for the server has been installed in the Tera2 PCoIP Zero Client and all other certificate requirements are met for the configured certificate checking mode (see Requirements for Trusted Server Connections), the icon at the top of this page shows a closed padlock symbol with a green check mark, and the 'https' in the server's URI also displays in green text.

The following image shows the user authentication screen when the Tera2 PCoIP Zero Client trusts the server's certificate. When connecting to other host types, such as VMware Horizon and Amazon WorkSpaces, you will see a similar authentication screen.

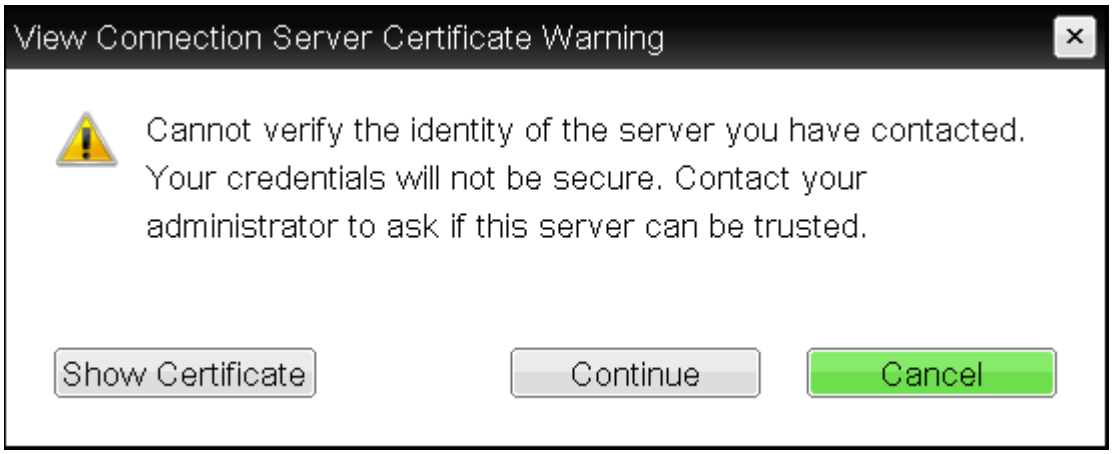


Tera2 PCoIP Zero Client trusted HTTPS connection

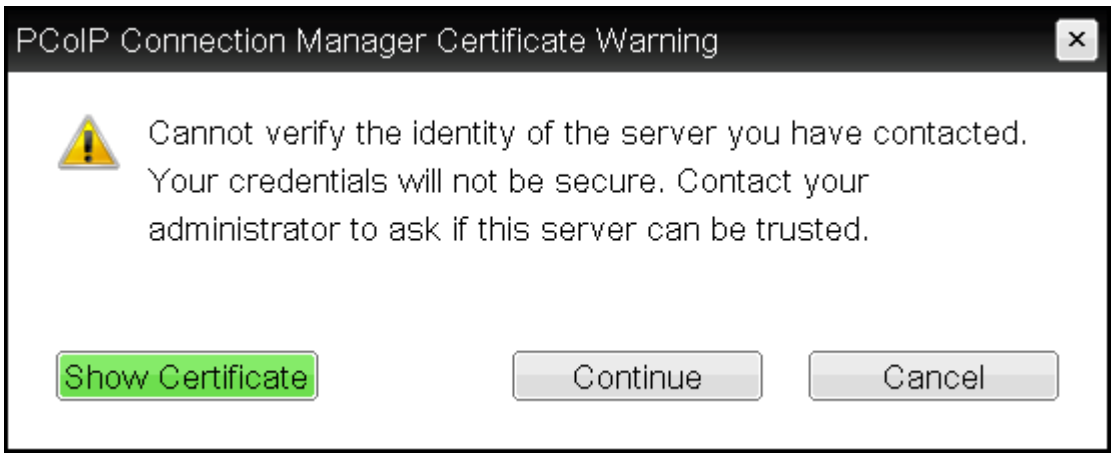
Making an Untrusted HTTPS Connection

If the correct trusted SSL root certificate for a connection server has not been installed in the Tera2 PCoIP Zero Client, or if other certificate requirements are not met (see Requirements for

Trusted Server Connections), a warning such as the following appears if your Tera2 PCoIP Zero Client is configured to warn before connecting to untrusted servers.

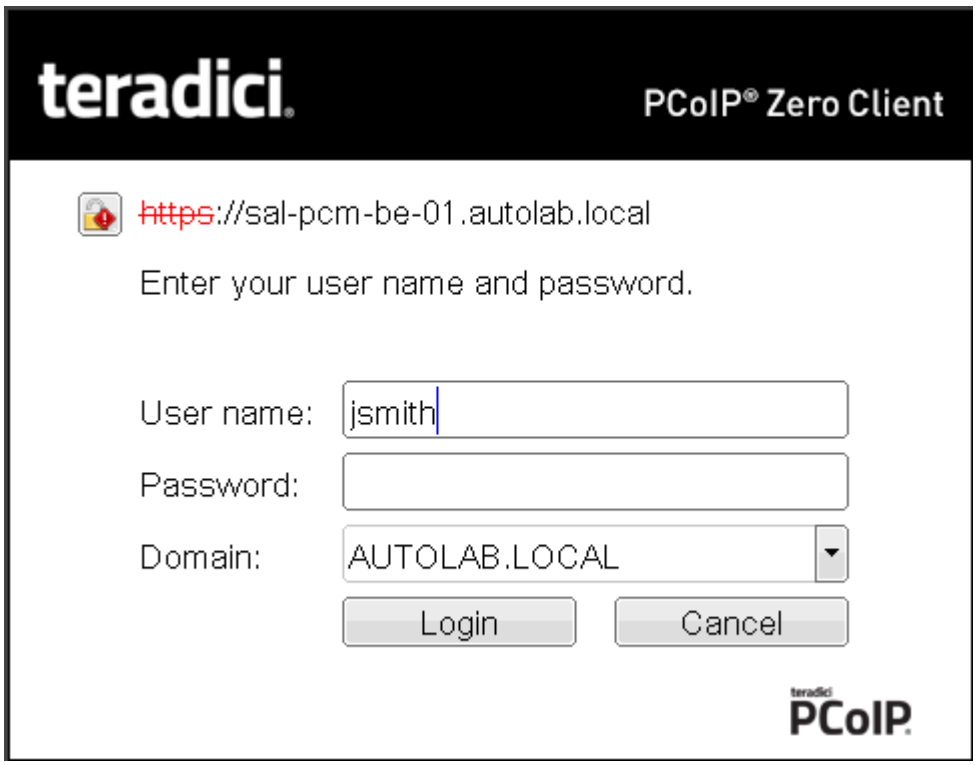


View Connection Server Certificate Warning



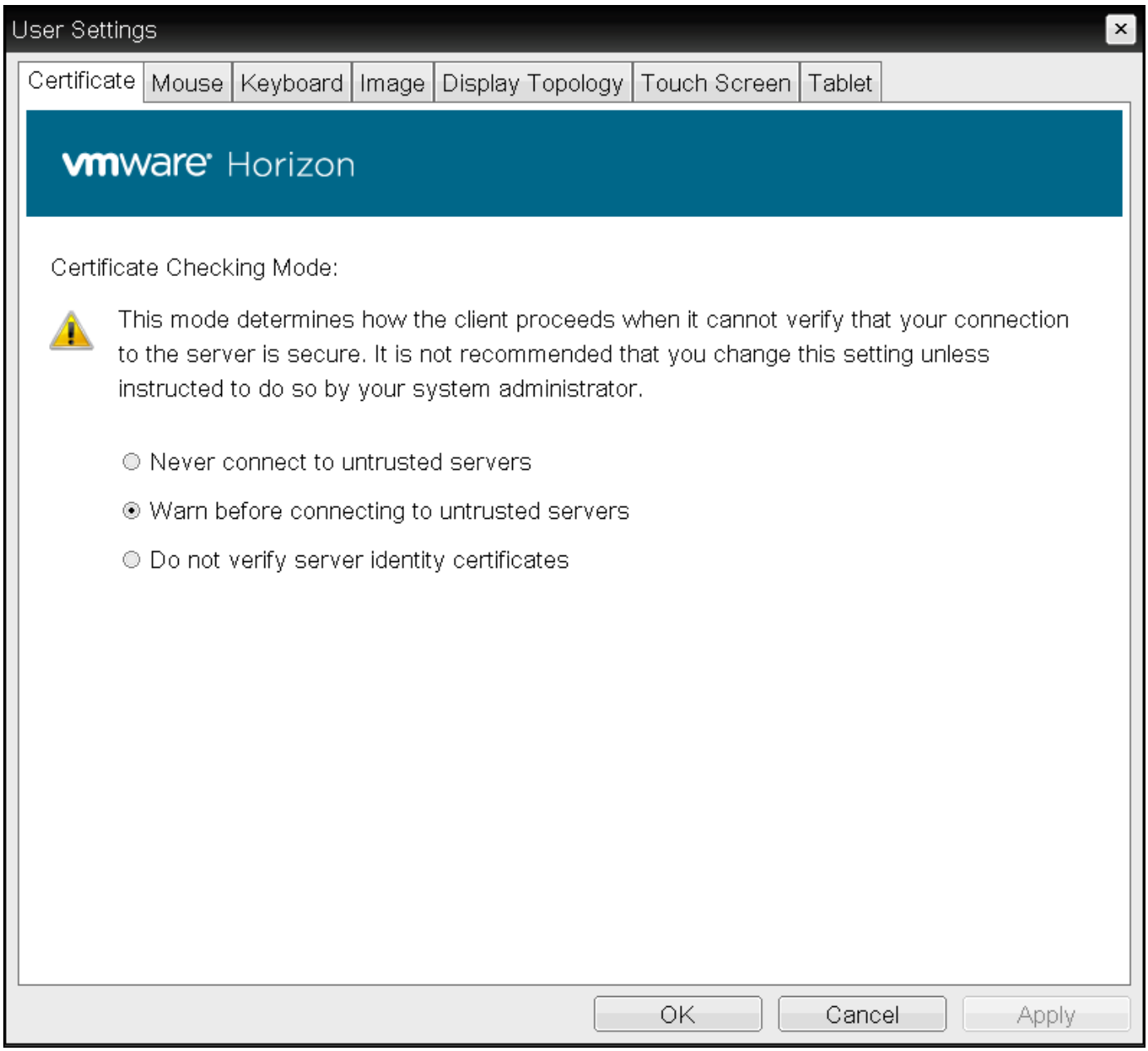
PCoIP Connection Manager Certificate Warning

If the user clicks **Continue** at this warning, the connection will still be secured with HTTPS, but an open padlock icon with a red 'x' will display on the login screen, along with red 'https' text with strikethrough formatting, as seen in the top row of the following image. When connecting to other host types, such as VMware Horizon and Amazon WorkSpaces, you will see a similar screen.

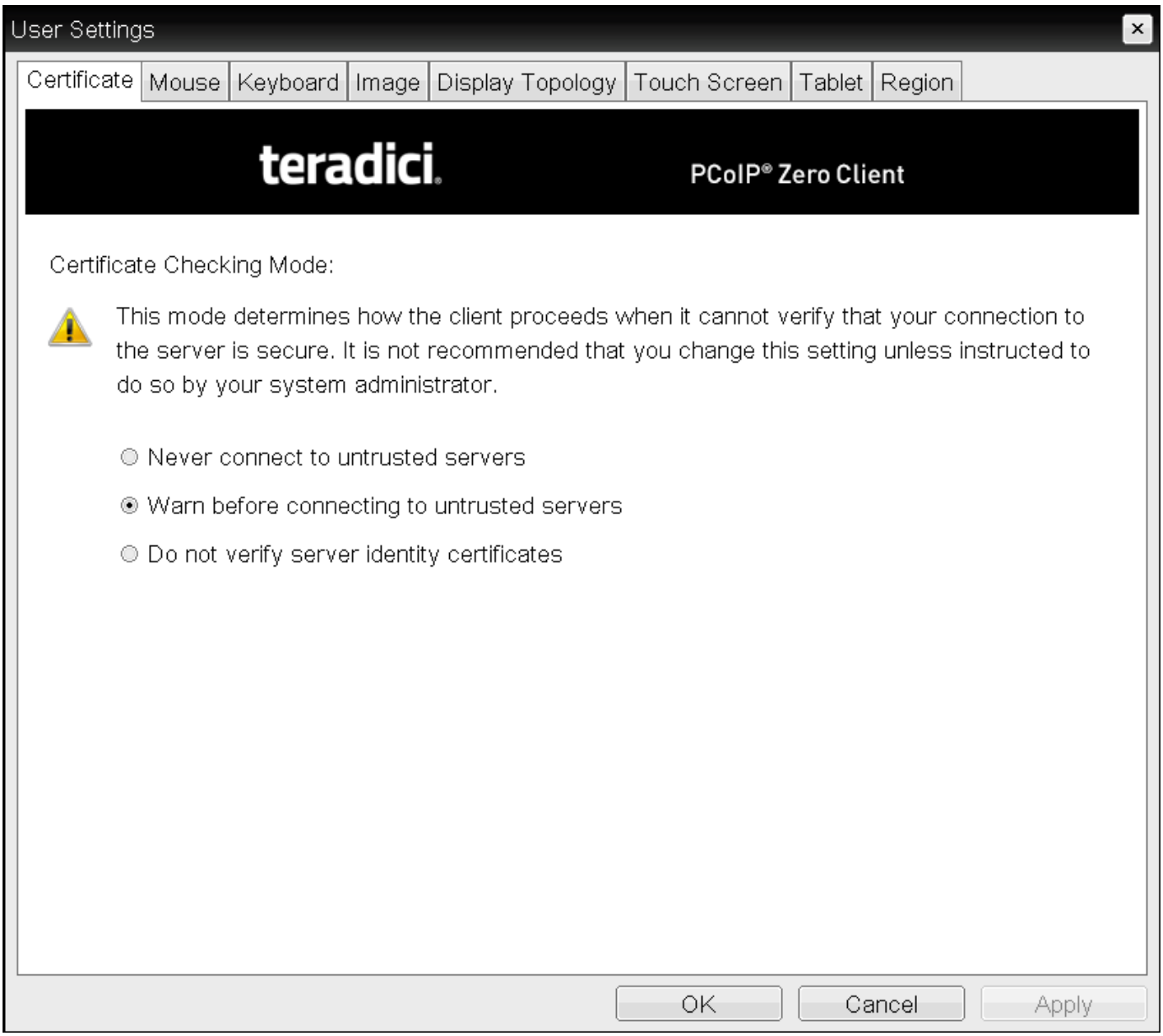


Tera2 PCoIP Zero Client untrusted HTTPS connection

As an administrator, you can use the Options > User Settings > Certificate page to prevent users from initiating untrusted server sessions by configuring the Tera2 PCoIP Zero Client to refuse a connection to a server that cannot be verified. Depending on the configured server type, this page has a different banner.



VMware Horizon Certificate Checking Mode page

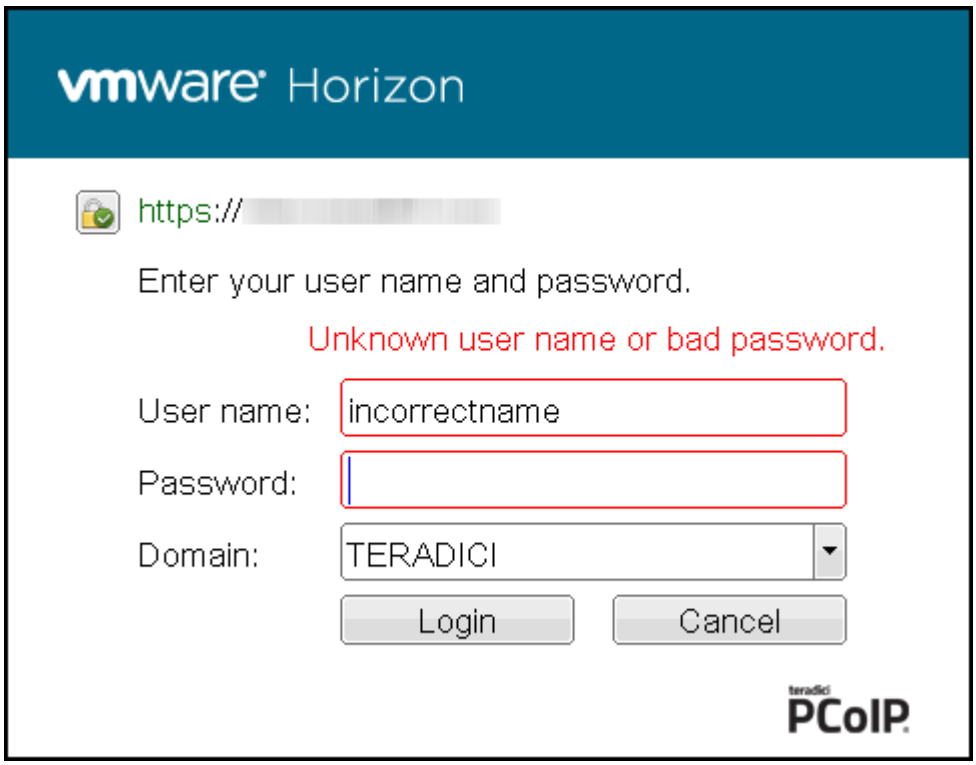


Teradici Certificate Checking Mode

Using the AWI, you can enable Certificate Check Mode Lockout from the **Session – View Connection Server** or **Session – PCoIP Connection Manager** page to prevent users from changing this setting.

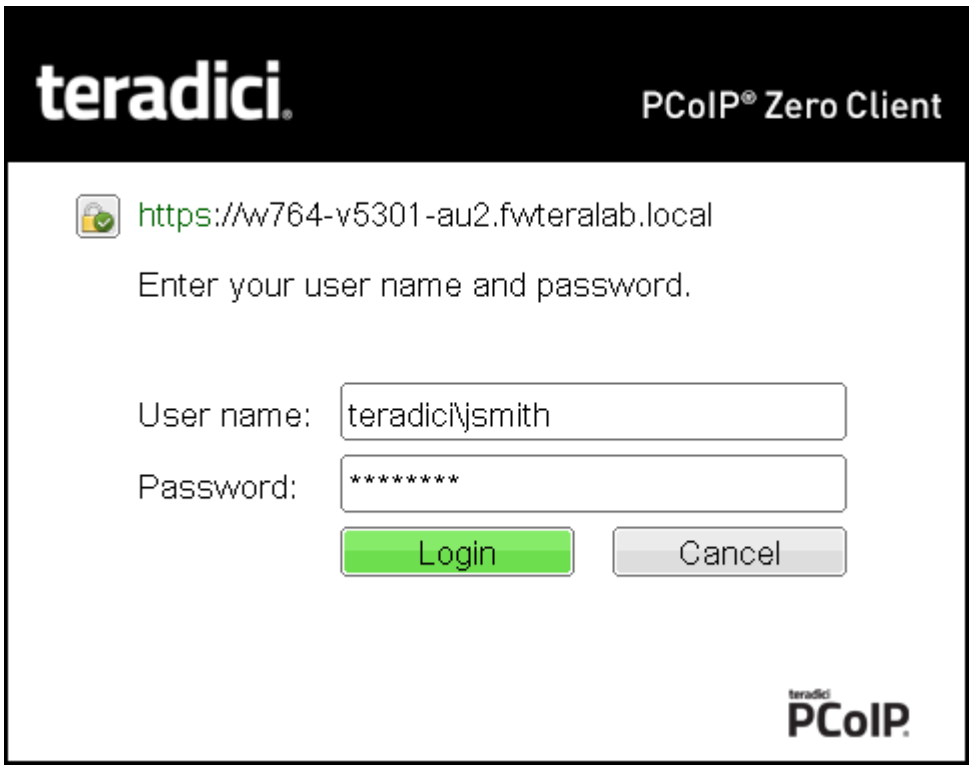
Authenticating the User

After the user sends the login credentials, the server performs authentication. If the user name and password are not entered correctly, or if the Caps Lock key is on, a message displays on this page to indicate these problems.

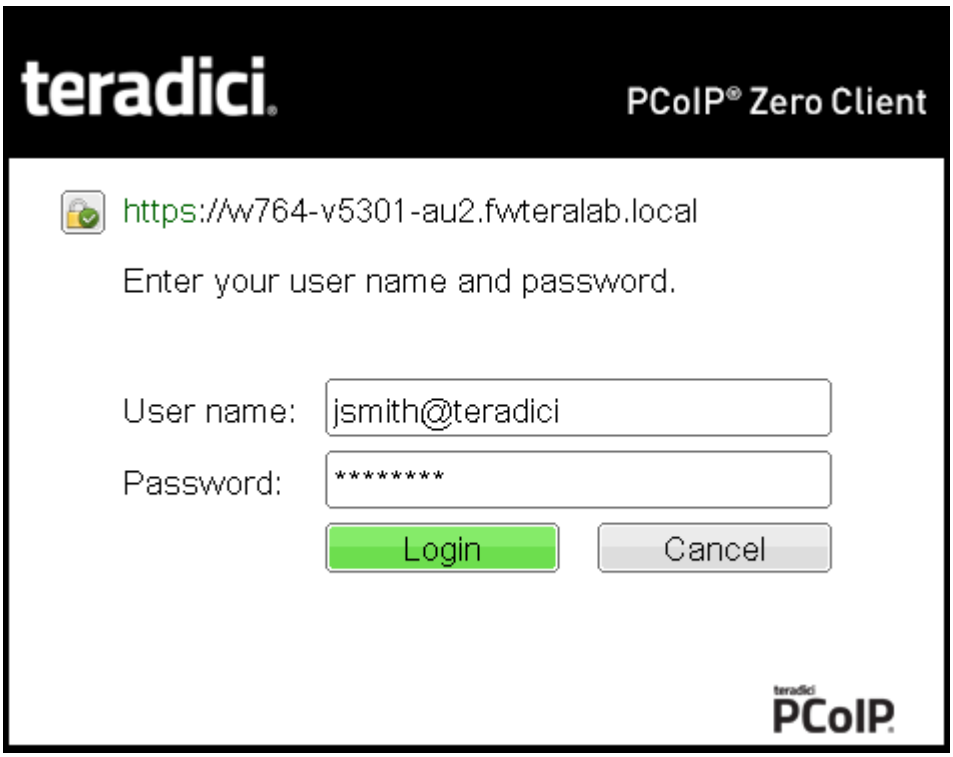


Unknown user name or password

All connections support the down-level logon user name format (DOMAIN\user) in the **User name** field. If using a compatible PCoIP Connection Manager (see its release details for more information), UPN (user@domain) is also supported in the **User name** field.



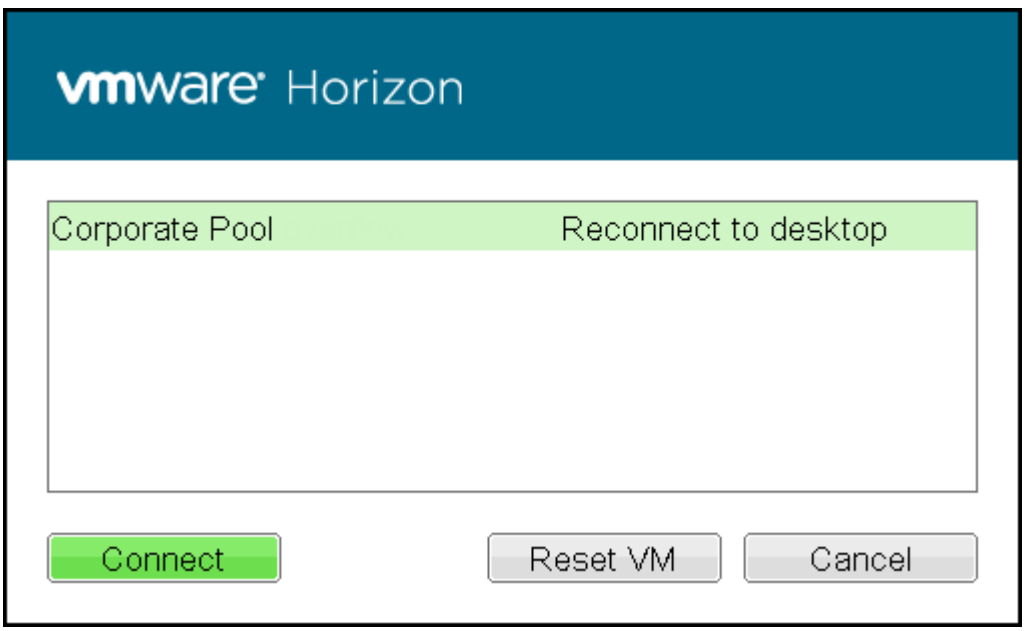
Tera2 PCoIP Zero Client with domain field hidden



Tera2 PCoIP Zero Client with domain field hidden

Connecting to a Desktop

If the user is not configured to connect automatically to a desktop, a list of one or more desktops to which the user is entitled displays. The user may select the desired one and click **Connect**.

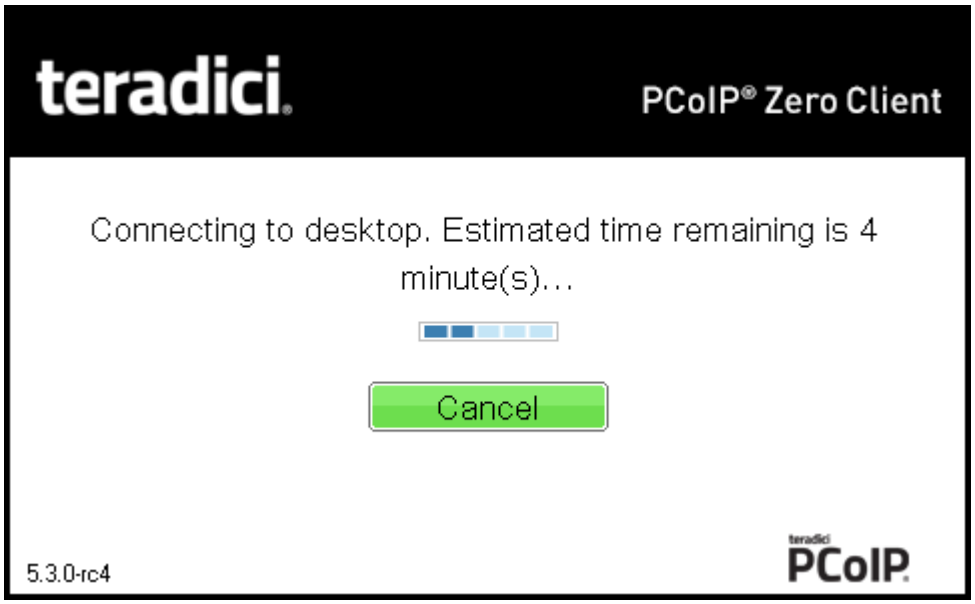


Selecting an entitlement

If the desktop is available, a message displays on the Connect screen to inform the user that the server is preparing the desktop. After a few seconds, the PCoIP session is established and the user connected.

If the desktop is not available (for example, if the desktop is in the process of rebooting), a second message also flashes on the Connect screen to inform the user that the assigned desktop source for this desktop is not currently available. The firmware continuously attempts to connect until the desktop is ready or the user clicks Cancel to cancel the operation.

If a PCoIP Connection Manager provides the estimated remaining time to connect to a user's desktop, the zero client will display the remaining time to the user.



Notification with estimated length of time before connecting

Uploading certificates to a single device

For information on how to upload certificates to a single device using the AWI, see Uploading Firmware.

OSD messages on startup or after a session has been established

For information on other OSD messages that may appear on top of a user's session during startup or after a session has been established, see About Overlay Windows.

Connecting to PCoIP Remote Workstation Cards

You can move high-performance Windows or Linux workstations with PCoIP Remote Workstation Cards into your data center, and configure sessions between Tera2 PCoIP Zero Clients and these workstation hosts over a LAN or WAN. This type of configuration provides a secure, reliable, and easy-to-manage solution that meets the needs of users who have dedicated computers with graphically demanding applications.

Direct connections with no-IP networks

While PCoIP Zero Clients and Remote Workstation Cards can be configured to be directly connected via a no-IP network (a cable connecting both units together with no network devices in between), it is not a configuration that is supported by Teradici. For more information see KB 1297.

This topic includes information on the following sections:

- Prerequisites
- Configuration Options
- Connection Instructions

Prerequisites

Before connecting a Tera2 PCoIP Zero Client to a PCoIP Remote Workstation Card, ensure that the following conditions are met:

- The PCoIP Remote Workstation Card and Tera2 PCoIP Zero Client have compatible firmware versions. For information on how to upload firmware, see Uploading Firmware.
- You have the correct certificates installed and configured on both devices. See About Certificates
- You are running a supported OS on the workstation and the Teradici PCoIP Host Software is installed. For details, see PCoIP® Host Software for Windows User Guide or PCoIP® Host Software for Linux User Guide. If you are using a VMware Connection Server as a broker, View Agent must also be installed on the host PC or workstation.

- The Host Driver Function is enabled on the PCoIP Remote Workstation Card.
- Your network resources meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see PCoIP Session Planning Administrators' Guide.

Configuration Options

The following session connection types are available for PCoIP Zero Client-to-PCoIP Remote Workstation Card connections:

> **Best Security Practices**
>
> Teradici highly recommends using custom peer-to-peer certificates to create a more secure environment when connecting to your Remote Workstation Card. Contact your IT department to ensure your deployment is in accordance with your Company's security policy. See Peering Zero Clients to Remote Workstation Cards for details.

- Connecting direct to host
- Connecting using SLP host discovery
- Connect using Cloud Access Manager
- Connecting using a third-party connection broker
- Connecting using the View Connection Server

Connecting Statically Direct to Host

To statically configure a Tera2 PCoIP Zero Client to connect directly to a specific PCoIP Remote Workstation Card, use the Direct to Host session connection type. You will need to provide the DNS name or IP address of the PCoIP Remote Workstation Card for this option.

You also need to configure a Direct from Client session connection type on the PCoIP Remote Workstation Card. You have the option of enabling the host to accept a connection request from any client or from a specific client only. If the latter, you need to provide the client's MAC address.

For details about how to configure the session connection type, see the following topics in the GUI Reference:

- AWI: Direct to Host Session Settings
- OSD: Direct to Host Session Settings

Connecting Using SLP Host Discovery

If PCoIP Remote Workstation Cards reside on the same subnet as Tera2 PCoIP Zero Clients, you can use the Direct to Host + SLP session connection type to configure clients to use Service Location Protocol (SLP) to discover the PCoIP Remote Workstation Cards on the subnet. With this configuration, the client OSD will list the first 10 cards discovered. The end user can select the desired one and connect to it.

> **Do not select SLP host discovery with more than 10 hosts**
>
> SLP host discovery is not suitable for deployments with more than 10 hosts if a Tera2 PCoIP Zero Client requires an ongoing connection. In this situation, a connection broker is required.

You also need to configure a **Direct from Client** session connection type on the PCoIP Remote Workstation Card. You have the option of enabling the host to accept a connection request from any Tera2 PCoIP Zero Client or from a specific one only. If the latter, you need to provide the client's MAC address.

For details about how to configure the session connection type, see the following topics in the GUI Reference:

- AWI: Direct to Host + SLP Host Discovery Session Settings
- OSD: Direct to Host + SLP Host Discovery Session Settings

Connecting using Cloud Access Manager

Cloud Access Manager enables brokering host PCs containing PCoIP Remote Workstation Cards with a Remote Workstation Card Agent installed to Tera2 PCoIP Zero Clients based on the identity of the user establishing a connection from the Tera2 PCoIP Zero Client. The PCoIP Remote Workstation Card Agent for Windows introduces Teradici brokering to a Teradici Remote

Workstation Card deployment, allowing the desktop to be managed by Teradici Cloud Access Manager or by third-party brokers like Leostream. Cloud Access Manager is best suited smaller Remote Desktop Card deployments.

Cloud Access Manager requires the **PCoIP Connection Manager** session connection type.

For more information, see Connection broker support with PCoIP technology (1044

For details about how to configure the session connection type, see the following topics in the GUI Reference:

- AWI: PCoIP Connection Manager Session Settings
- OSD: PCoIP Connection Manager Session Settings

Connecting Using a Third-Party Connection Broker

A third-party connection broker is a resource manager that dynamically assigns host PCs containing PCoIP Remote Workstation Cards to Tera2 PCoIP Zero Clients based on the identity of the user establishing a connection from the Tera2 PCoIP Zero Client. Connection brokers are also used to allocate a pool of hosts to a group of Tera2 PCoIP Zero Clients. They are typically used in large PCoIP deployments, or when hosts and clients do not reside on the same subnet.

Third-party brokers use the **PCoIP Connection Manager** session connection type.

For more information, see Connection broker support with PCoIP technology (1044

For details about how to configure the session connection type, see the following topics in the GUI Reference:

- AWI: PCoIP Connection Manager Session Settings
- OSD: PCoIP Connection Manager Session Settings

Connecting Using the View Connection Server

You can also use a View Connection Server to broker a connection between Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards.

For details about how to configure the session connection type, see the following topics in the GUI Reference:

- AWI: View Connection Server Session Settings
- OSD: View Connection Server Session Settings

For this option, VMware View Agent must be installed on the remote workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, refer to Using PCoIP® Host Cards with VMware View.

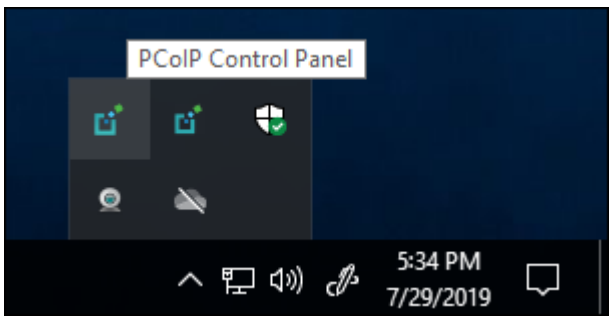
Connecting Using Cloud Access Manager or a Third Party Broker

To connect using a broker:

1. If using Using Cloud Access Manager or a Third Party Broker, ensure the Remote Workstation Card Agent is installed on the remote workstation.

   Identifying the Remote Workstation Card Agent is Installed

   Once the Remote Workstation Card Agent is installed on the host PC, the **PCoIP Control Panel** icon will be displayed in the list of active programs running on your taskbar. Hover your mouse over the PCoIP icon to confirm the **PCoIP Control Panel** is installed. In most cases you will also have the PCoIP Host Software installed.

2. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select one of the following connection types:
   - View Connection Server if you are using a VMware broker
   - PCoIP Connection Manager if you are using Cloud Access Manager or a third-party broker.

3. Enter the DNS name or IP address of the broker, and click **OK**.
4. Click the **Connect** button.
5. When prompted, enter your remote workstation's login credentials.

Advanced settings

For details about advanced settings, see View Connection Server or PCoIP Connection Manager.

Connecting to Teradici Cloud Access Software

Teradici Cloud Access Software, also known as Cloud Access Software, is a Teradici application that enables users to remotely access a physical or virtualized remote workstation using the PCoIP protocol without having to install a PCoIP Remote Workstation Card. To ease administration burdens, consider brokering with Teradici's Cloud Access Manager or a third party broker compatible with the PCoIP broker protocol. Teradici technology partners with compatible connection brokers can be found here. See the appropriate broker documentation for brokering requirements and configuration steps.

The Cloud Access Software supports two deployment scenarios using Auto Detect and PCoIP Connection Manager Zero Client session connection types:

- Deskside deployment: Connecting directly to a physical workstation.
- Data center deployment: Connecting to a physical or virtualized workstation either directly, brokering with Teradici's Cloud Access Manager, or via a compatible third-party broker from one of our technology partners such as Leostream.

This topic includes information on the following sections:

- Prerequisites
- Configuration Options
- Connection Instructions

Prerequisites

Before connecting a Tera2 PCoIP Zero Client to a workstation running the Teradici Cloud Access Software, ensure that the following prerequisites are in place:

- You are using a Tera2 PCoIP Zero Client (TERA2321 or TERA2140 processor) to connect.
- The remote workstation has Cloud Access Software installed.
  For details on available Cloud Access hosts, see the Teradici Cloud Access Architecture Guide
  For workstation requirements and Cloud Access Agent installation details, see the respective agent Administrators' Guide found at the Teradici support site.

- If using a broker, see the appropriate broker documentation.
  - Cloud Access Manager
  - See your third party broker documentation. For a list of compatible third party brokers see our list of Connection Brokering Technology Partners.

Configuration Options

For both deskside and data center deployments, the following session connection types are available for PCoIP Zero Client-to-Cloud Access Software connections:

- AWI: Auto Detect
- OSD: Auto Detect
- AWI: PCoIP Connection Manager
- OSD: PCoIP Connection Manager
- AWI: PCoIP Connection Manager + Auto-Logon
- OSD: PCoIP Connection Manager + Auto-Logon

Connection Instructions

Before connecting, you will need to know the IP address or Fully Qualified Domain Name (FQDN) of your physical or virtualized workstation if you are connecting directly (deskside deployment). If you are connecting using a third-party broker (data center deployment), you will need to know the IP address or FQDN of the PCoIP Connection Manager. See the documentation from your equipment supplier for instructions on how to configure your broker.

Type 'https://' before the IP address or fully qualified computer name

The syntax of the ***Server URI*** (uniform resource identifier) field on the Session page requires **https://** before the IP address or FQDN. If you do not enter it, https:// will automatically be inserted when you click **OK**.

Connecting Using Auto Detect

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers.

To connect using Auto Detect connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the Auto Detect connection type.
2. In the **Server URI** field, enter the FQDN or IP address of one of the following and click **OK**:
   - Your workstation, if you are connecting directly.
   - PCoIP Connection Manager, if you are connecting through a third-party broker.
3. Click the **Connect** button.
4. When prompted, enter your login credentials.

After you make a successful connection using Auto Detect, the IP address or FQDN of your host is automatically saved in the **Server** drop-down list on the OSD Connect dialog, along with the IP address or FQDN of any other hosts to which you have connected.

Connecting Using PCoIP Connection Manager

To connect using the PCoIP Connection Manager connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the PCoIP Connection Manager connection type.
2. In the **Server URI** field, enter the FQDN or IP address of one of the following and click **OK**:
   - Your workstation, if you are connecting directly.
   - PCoIP Connection Manager, if you are connecting through a third-party broker.
3. Click the **Connect** button.
4. When prompted, enter your login credentials.

Advanced settings

For details about advanced settings, see OSD: PCoIP Connection Manager Session Settings.

Connecting Using PCoIP Connection Manager + Auto-Logon

To connect using the PCoIP Connection Manager and Auto-Logon connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the PCoIP Connection Manager + Auto-Logon connection type.
2. In the Server URI field, enter the FQDN or IP address of one of the following, and click **OK**:
   - Your workstation, if you are connecting directly.
   - The PCoIP Connection Manager, if you are connecting through a third-party broker.
3. Enter the user name, password, and domain name for the user to be automatically logged in.
4. Click the **Connect** button.

Advanced settings

For details about advanced settings, see OSD: PCoIP Connection Manager + Auto-Logon Session Settings.

Connecting to Amazon WorkSpaces Desktops

Amazon WorkSpaces is a fully managed cloud-based desktop service that enables end users to access their documents, applications, and resources. Tera2 PCoIP Zero Clients together with Amazon WorkSpaces provide a secure, easy to manage solution for delivering users with a rich desktop experience.

This topic includes information on the following sections:

- Prerequisites
- Configuration Options
- Connection Instructions

Prerequisites

For the best user experience, Teradici recommends using firmware version 6.0 or later with Amazon WorkSpaces (hourly pricing).

Before connecting a Tera2 PCoIP Zero Client to an Amazon WorkSpaces desktop, ensure that the following prerequisites are in place:

- You are using a Tera2 PCoIP Zero Client (TERA2321 or TERA2140 processor) to connect.

  Firmware Versions

  - PCoIP Zero Clients on firmware 6.0+ can connect directly to Amazon WorkSpaces using Multifactor Authentication.
  - Firmware 21.10+ can cache up to 50 registration codes
  - Firmware up to 20.07 can cache up to 10 registration codes

- You have an AWS account with Amazon WorkSpaces up and running. For information, see AWS documentation.
- Your network has full connectivity to your Amazon WorkSpaces. For information, see AWS documentation.

Configuration Options

The following session connection types are available for Tera2 PCoIP Zero Client-to-Amazon WorkSpaces connections:

- AWI: Amazon WorkSpaces
- OSD: Amazon WorkSpaces Session Settings
- AWI: Auto Detect Session Settings
- OSD: Auto Detect Session Settings
- AWI: PCoIP Connection Manager Session Settings
- OSD: PCoIP Connection Manager Session Settings
- AWI: PCoIP Connection Manager + Auto-Logon Session Settings
- OSD: PCoIP Connection Manager + Auto-Logon Session Settings

Connection Instructions

Connecting to Amazon WorkSpaces Directly

> **Multi-factor Authentication (MFA)**
>
> When connecting directly, Amazon WorkSpaces may require multi-factor authentication in order to connect. This may be regardless of how you have set up your Amazon WorkSpaces. You are also required to use firmware 6.0 or newer on your PCoIP Zero Client when connecting directly.

To connect using Amazon WorkSpaces session connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the OSD: Amazon WorkSpaces Session Settings connection type.
2. Enter the registration code from the invitation email sent after creating your Amazon WorkSpace.
3. Enter a name for this registered Amazon WorkSpace instance.
4. Click the **Connect** button.

Connecting to Amazon WorkSpaces using the PCoIP Connection Manager for Amazon WorkSpaces

PCoIP Connection Manager for Amazon WorkSpaces is required to connect to Amazon WorkSpaces when using PCoIP Zero Clients with firmware releases older than 6.0. You will need to know the IP address of your PCoIP Connection Manager for Amazon WorkSpaces appliance when using this connection type.

Using the correct firmware

Teradici recommends directly connecting to Amazon WorkSpaces when using PCoIP Zero Clients with firmware 6.0 or newer.

Type 'https://' before the IP address or fully qualified computer name

The syntax of the Server URI (uniform resource identifier) field on the Session page requires **https://** before the IP address or FQDN. If you do not enter it, **https://** will automatically be inserted when you click **OK**.

Connecting Using Auto Detect

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers.

To connect using the Auto Detect connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the Auto Detect connection type.
2. In the **Server URI** field, enter the IP address of your PCoIP Connection Manager for Amazon WorkSpaces, and click **OK**.
3. Click the **Connect** button.
4. When prompted, enter your login credentials.

After connecting using Auto Detect, the system saves your host's IP address or fully qualified computer name

After you make a successful connection using Auto Detect, the IP address or FQDN of your host is automatically saved in the **Server** drop-down list on the OSD Connect dialog, along with the IP address or FQDN of any other hosts to which you have connected.

Connecting Using PCoIP Connection Manager

To connect using the PCoIP Connection Manager connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the PCoIP Connection Manager connection type.
2. In the **Server URI** field, enter the IP address of your PCoIP Connection Manager for Amazon WorkSpaces, and click **OK**.
3. Click the **Connect** button.
4. When prompted, enter your login credentials.

Advanced settings

For details about advanced settings, see OSD: PCoIP Connection Manager Session Settings.

Connecting Using PCoIP Connection Manager + Auto-Logon

To connect using the PCoIP Connection Manager and Auto-Logon connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the PCoIP Connection Manager + Auto-Logon connection type.
2. In the **Server URI** field, enter the IP address of your PCoIP Connection Manager for Amazon WorkSpaces, and click **OK**.
3. Enter the user name, password, and domain name for the user to be automatically logged in.
4. Click the **Connect** button.

Advanced settings

For details about advanced settings, see OSD: PCoIP Connection Manager + Auto-Logon Session Settings.

Connecting to VMware Horizon Desktops and Applications

VMware Horizon View provides remote desktop capabilities to users using the PCoIP protocol and VMware's virtualization technology. You can configure Tera2 PCoIP Zero Clients to connect to desktops in a VMware Horizon VDI or DaaS environment, or when connecting to VMware Horizon app-remoting desktops and applications published on an RDS server.

This topic includes information on the following sections:

- Prerequisites
- Connection Types
- Connection Instructions

Prerequisites

Before connecting a Tera2 PCoIP Zero Client to a VMware Horizon desktop, ensure that the following prerequisites are in place:

- The VMware Horizon View installation, which includes the VMware View Manager and VMware View Agent, are version 4.0.1 or newer.
- For VMware Horizon connections to RDS-hosted published desktops and applications, you are using a Tera2 PCoIP Zero Client (TERA2321 or TERA2140 processor).
- our network resources meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the PCoIP Session Planning Guide.

Supported Connection Types

The following session connection types are available for Tera2 PCoIP Zero Client-to-VMware Horizon connections:

- AWI: View Connection Server

- OSD: View Connection Server
- AWI: View Connection Server + Auto-Logon
- OSD: View Connection Server + Auto-Logon
- AWI: View Connection Server + Kiosk
- OSD: View Connection Server + Kiosk
- AWI: View Connection Server + Imprivata OneSign
- OSD: View Connection Server + Imprivata OneSign

Connection Instructions

Before connecting, you will need to know the DNS name or IP address of your View Connection Server. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.

Connecting with Auto Detect

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers.

To connect using the Auto Detect connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the Auto Detect connection type.
2. In the **Server URI** field, enter the DNS name or IP address of your View Connection Server (or VMware Horizon DaaS Desktop Portal), and click **OK**.
3. Click the **Connect** button.
4. When prompted, enter your login credentials.

After connecting using Auto Detect, the system saves your host's IP address or fully qualified computer name

After you make a successful connection using Auto Detect, the IP address or FQDN of your host is automatically saved in the Server drop-down list on the OSD Connect dialog, along with the IP address or FQDN of any other hosts to which you have connected.

Connecting with View Connection Server

To connect using the View Connection Server connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the View Connection Server] connection type.
2. In the **DNS Name** or **IP Address** field, enter the DNS name or IP address of your View Connection Server (or VMware Horizon DaaS Desktop Portal).
3. If you are making a VMware Horizon RDS-hosted application connection:
   a. Click **Advanced**.
   b. Click to enable the **Enable RDS Application Access** option.
   c. Click **Apply** and then **OK**.
4. Click the **Connect** button.
5. When prompted, enter your login credentials.

Advanced settings

For details about advanced settings, see OSD: View Connection Server Session Settings.

Connecting with View Connection Server + Auto-Logon

To connect using the View Connection Server and Auto-Logon connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the View Connection Server + Auto-Logon connection type.
2. In the **DNS Name** or **IP Address** field, enter the DNS name or IP address of your View Connection Server (or VMware Horizon DaaS Desktop Portal).
3. Enter the user name, password, and domain name for the user to be automatically logged in.

4. If you are making a VMware Horizon RDS-hosted application connection:
    a. Click **Advanced**.
    b. Click to enable the **Enable RDS Application Access** option.
    c. Click **Apply** and then **OK**.
5. Click the **Connect** button.

> **Advanced settings**
>
> For details about advanced settings, see OSD: View Connection Server + Auto-Logon.

Connecting with View Connection Server + Kiosk

View Connection Server + Kiosk mode enables you to configure Tera2 PCoIP Zero Clients to connect to a desktop that will be used for a kiosk implementation, such as when multiple users connect to a desktop to obtain information that is not specific to any one individual. At minimum, you will need to provide the DNS name or IP address of the View Connection Server and the kiosk user name—either a custom user name for the kiosk or its MAC address.

To connect using the View Connection Server and Kiosk connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the View Connection Server + Kiosk connection type.
2. In the **DNS Name** or **IP Address** field, enter the DNS name or IP address of your View Connection Server (or VMware Horizon DaaS Desktop Portal).
3. Select whether to populate the **Username** field with the MAC address of the Tera2 PCoIP Zero Client (Zero Client MAC option) or use a customer name (Custom option).
4. If you have selected **Custom**, enter the custom name of the client.
5. Enter the password for the kiosk virtual machine.
6. If you are making a VMware Horizon RDS-hosted application connection:
    a. Click **Advanced**.
    b. Click to enable the **Enable RDS Application Access** option.
    c. Click **Apply** and then **OK**.

d. Click the **Connect** button.

> **Advanced settings**
>
> For details about advanced settings, see OSD: View Connection Server + Kiosk.

Connecting with View Connection Server + Imprivata OneSign

Imprivata OneSign enables users to access corporate networks, desktops, and applications with a single sign on. It also provides a range of authentication options that include proximity cards, smart cards, tokens, and other methods.

> **Type 'https://' before the fully qualified computer name**
>
> The syntax of the **Bootstrap URL** (uniform resource locator) field on the Session page requires **https://** before the FQDN. If you do not enter it, **https://** will automatically be inserted when you click **OK**.

To connect using the View Connection Server and Imprivata OneSign connection type:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the View Connection Server + Imprivata OneSign connection type.
2. In the **Bootstrap URL** field, enter the DNS of your OneSign authentication server.
3. If you are making a VMware Horizon RDS-hosted application connection:
   a. Click **Advanced**.
   b. Click to enable the **Enable RDS Application Access** option.
   c. Click **Apply** and then **OK**.
4. Click the **Connect** button.

> **Advanced settings**
>
> For details about advanced settings, see OSD: View Connection Server + Imprivata OneSign.

Disconnecting from a Session

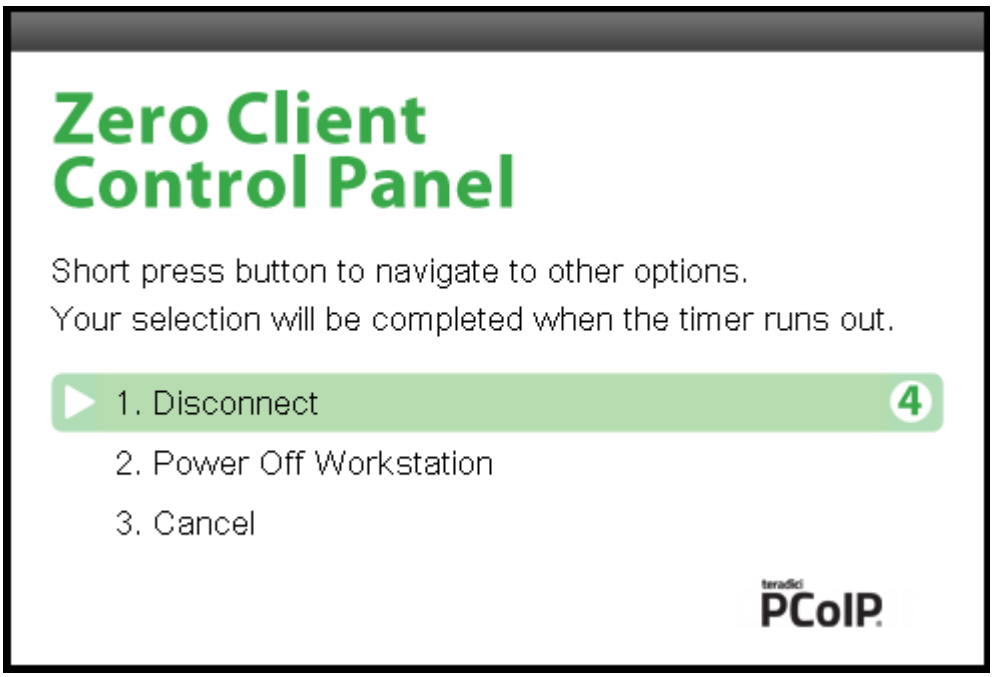
Disconnecting from a Virtual Desktop

You can disconnect from a virtual desktop session and return to the OSD by either of the following options.

- Pressing `Ctrl`+`Alt`+`F12` which requires the Enable Session Disconnect Hotkey enabled in the advanced options on the AWI Session page.
- Pressing the device's **Connect/Disconnect** button.

Disconnecting from a Remote Workstation Card

If you are in a session with a PCoIP Remote Workstation Card and if the Zero Client AWI Power Parameter ***Remote Host Power Control*** is set to **Hard Power-off only**, the zero client connect/disconnect button will display the Zero Client Control Panel to control session disconnects. If the ***Remote Host Power Control*** is set to **Power-off not permitted**, the zero client connect/disconnect button will initiate a connect or disconnect of a PCoIP session.



Zero Client Control Panel

To make a selection, tap the **Connect/Disconnect** button to toggle between options until the desired one is highlighted, then wait for the four-second countdown to complete.

If you have installed and configured the Remote Workstation Card Software on the host computer, additional keyboard functionality is provided, allowing you to:

- use the up/down arrow keys on the keyboard to highlight the zero client control panel desired option, and press `Enter` to make the selection.
- use the keyboard number keys (1, 2, 3) that matches the control panel option to select it immediately.
- use the `Ctrl`+`Alt`+`F12` shortcut sequence to display the zero client control panel.

To ensure full functionality of the keyboard when in a session with the Remote Workstation Card ensure all the following settings are made.

- On the zero client, the keyboard must be recognized as locally connected (not bridged).
- The Host Driver Function is enabled on the Remote Workstation Card firmware.
- The **Enable Local Cursor and Keyboard** feature is enabled on the installed Remote Workstation Card Software for Linux or Windows on the host computer.
- The Remote Workstation Card Software for Linux or Windows is installed on the host computer and the **Enable Local Cursor and Keyboard** feature is enabled.
- (Optional) Enable Session Disconnect Hotkey must be enabled in the advanced options on the Session page to enable the `Ctrl`+`Alt`+`F12` shortcut sequence.

Managing Your Tera2 PCoIP Zero Client

This section shows you how to manage your Tera2 PCoIP Zero Client. You'll learn how to perform common tasks, view information about your Tera2 PCoIP Zero Client, configure your Tera2 PCoIP Zero Client, and perform diagnostics, such as viewing and configuring logging information, testing audio, and viewing session statistics. The topics include:

- Performing Common Tasks
- Viewing Information About your Tera2 PCoIP Zero Client
- Configuring Your Tera2 PCoIP Zero Client
- Performing Diagnostics

Performing Common Tasks

This section describes common tasks you may perform on a regular basis, such as connecting to an endpoint manager, and uploading firmware and certificates. Other tasks you may perform on a less regular basis include setting up touch screen displays, configuring the OSD to display a custom logo, and resetting the Tera2 PCoIP Zero Client to its factory default values.

Additional tasks you need to perform

For tasks you need to perform to set up your Tera2 PCoIP Zero Client, see Setting Up Your Tera2 PCoIP Zero Client.

Connecting to an Endpoint Manager

Tera2 PCoIP Zero Clients are managed in groups by an endpoint manager, such as the PCoIP Management Console. Endpoint managers are also the recommended method to configure your zero client to maintain a high security environment.

Before the endpoint manager can administer a client, the client must see the endpoint manager and establish a connection to it. This connection process is called discovery. Discovery can be automatic or manual, and can be initiated from either side; endpoint managers can discover clients, and clients can discover endpoint managers.

Available discovery methods are determined by your chosen security settings, discovery modes, and installed certificates, as described in the following sections:

- About Tera2 PCoIP Zero Client Security Levels
- About Certificates
- Endpoint Manager Discovery Methods
- Staging Clients Using an Endpoint Manager

About Tera2 PCoIP Zero Client Security Level Settings

The Discovery Mode setting described in this article is found on the ***Management*** page and configures how endpoint managers are discovered by the Tera2 PCoIP Zero Client.

Discovery in this context does not refer to discovery of the Tera2 PCoIP Zero Client by endpoint managers. For instructions on having an endpoint manager discover your Tera2 PCoIP Zero Client, see Endpoint Manager Discovery Methods.

There are three available security level settings in the Tera2 PCoIP Zero Client: low, medium, and high. These settings determine whether theTera2 PCoIP Zero Client can be discovered by an endpoint manager, how an endpoint manager can be discovered by the Tera2 PCoIP Zero Client, and also dictate whether a certificate must be installed in the Tera2 PCoIP Zero Client for discovery to succeed.

The security level is configured on the Management page of the OSD or AWI (see Configuring Security Level). Detailed instructions for allowing discovery under most scenarios, including security level settings, are described in Endpoint Manager Discovery Methods.

The general implications of each security mode are summarized in the following table and described in detail next.

Tera2 PCoIP Zero Client behavior in low, medium, or high security modes and using automatic or manual discovery modes

	Low Security	Low Security	Medium Security	Medium Security	High Security
	Automatic	Manual	Automatic	Manual	Manual
Can be discovered by endpoint managers	✔	✘	✘	✘	✘
Can automatically discover endpoint managers using DNS	✔	✘	✔	✘	✘

	Low Security	Low Security	Medium Security	Medium Security	High Security
Can trust endpoint managers using DNS	✔	✖	✖	✖	✖
Can manually connect to endpoint managers	✖	✔	✖	✔	✔
Can trust endpoint managers using an installed certificate	✔	✔	✔	✔	✔

Low Security Mode

In low security mode, both automatic and manual discovery methods are available. Certificates are not required in automatic manager discovery mode if the DNS server is configured to provision the Tera2 PCoIP Zero Client with the URI of the endpoint manager's bootstrap server and its certificate fingerprint.

In automatic discovery mode:

- The client can use DNS to automatically discover endpoint managers.
- The client is discoverable by endpoint managers.
- The client can use DNS to trust the endpoint manager. DNS must be configured to provision your client with the URI and certificate fingerprint of the endpoint manager's bootstrap server.

> **DNS server configuration information**
>
> For details about how to configure your DNS server for automatic discovery, see the PCoIP® Management Console 3.1 Administrators' Guide.

In *manual* discovery mode:

- The client must be manually configured with the endpoint manager's bootstrap server URI.
- The client is not discoverable by endpoint managers.
- The client must have an installed certificate to trust the endpoint manager.

Certificates are installed by an endpoint manager

If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the client's certificate store, one must be installed by the endpoint manager. See Staging Clients Using an Endpoint Manager.

Medium Security Mode

In medium security mode, the Tera2 PCoIP Zero Client cannot be discovered by endpoint managers. The Tera2 PCoIP Zero Client can discover endpoint managers automatically or manually. Certificates are required in medium security mode.

In automatic discovery mode:

- The client can use DNS to automatically discover endpoint managers.
- The client is not discoverable by endpoint managers.
- The client must have an installed certificate to trust the endpoint manager.

Certificates are installed by an endpoint manager

If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the client's certificate store, one must be installed. See Staging Clients Using an Endpoint Manager.

In manual discovery mode:

- The client is not discoverable by endpoint managers.
- The client must be manually configured with the endpoint manager's bootstrap server URI.
- The client must have an installed certificate to trust the endpoint manager.

Certificates are installed by an endpoint manager

If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the client's certificate store, one must be installed. See Staging Clients Using an Endpoint Manager.

High Security Mode

In high security mode, the discovery bootstrap phase is disabled. All settings must be manually configured, and certificates are required:

- The client is not discoverable by endpoint managers.
- The client must be manually configured with the endpoint managers' internal (and, optionally, external) URI.
- The client must have an installed certificate to trust the endpoint manager.

> **Certificates are installed by an endpoint manager**
>
> If a certificate for the endpoint manager has not previously been installed by an endpoint manager in the client's certificate store, one must be installed. See See Staging Clients Using an Endpoint Manager.

> **Additional Security Tip**
>
> Teradici recommends disabling the AWI interface to reduce the attack surface on the Zero Client. Teradici recommends exclusively using the PCoIP Management Console to configure the Zero Client.

About Certificates

Certificates can be used to trust endpoint managers at all security levels, but are required when using ***medium*** or ***high*** security.

If a PCoIP Management Console certificate is required, you can use an ***issuer certificate***—either the root CA certificate, or the intermediate certificate used to issue the PCoIP Management Console's public key certificate, or the PCoIP Management Console's ***public key certificate***.

PCoIP Management Console certificates

For complete information about PCoIP Management Console components, including the Endpoint Bootstrap Manager and PCoIP Management Console certificates, see the PCoIP® Management Console Administrators' Guide.

Custom peer-to-peer certificates can also be used to secure PCoIP Zero Clients connecting to Remote Workstation Cards in your deployment. See Peering Remote Workstation Cards for further details on how to upload and apply custom peer-to-peer certificates.

Endpoint Manager Discovery Methods

From the AWI Management page, you can set the Tera2 PCoIP Zero Client's Security Level setting and discovery method. From the OSD Management page, you can view these settings. To view and set these settings, see Configuring Security Level and Configuring Discovery.

Zero Client Security Level settings

The AWI Management page has specific Security Level settings that are configured for management discovery. For Zero Client security recommendations see Securing Your Tera2 PCoIP Zero Client

There are several ways to register your Tera2 PCoIP Zero Client with an endpoint manager. These methods are outlined next.

The methods include:

- Automatic Endpoint Manager Discovery Using DNS
- Discovering the Client Manually from the Endpoint Manager
- Discovering the Endpoint Manager Manually from the Client Using Low or Medium Security Mode
- Discovering the Endpoint Manager Manually from the Client Using High Security Mode

The availability of these methods is determined by the Tera2 PCoIP Zero Client's security settings, and whether or not it has a certificate installed to trust the endpoint manager.

Information about security levels

For complete information about the various security levels and discovery settings, see About Tera2 PCoIP Zero Client Security Levels.

Automatic Endpoint Manager Discovery Using DNS

Tera2 PCoIP Zero Clients can use DNS to automatically find an endpoint manager. To use automatic endpoint manager discovery, you must configure the environment for DNS service record discovery, and the Tera2 PCoIP Zero Client's security level must be set to low or medium.

Medium or high security requires an installed certificate

In order to use medium or high security, the Tera2 PCoIP Zero Client must have been provisioned with a certificate using an endpoint manager.
For more information, see Staging Clients Using an Endpoint Manager.

DNS server Configuration Information

For details about how to configure your DNS server for automatic discovery, see the PCoIP® Management Console Administrators' Guide.

To configure the Tera2 PCoIP Zero Client for automatic endpoint discovery:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.
2. Set the *Security Level* option to **Low** or **Medium**.
3. Set the Manager Discovery Mode option to Automatic.
4. Click **Apply**.

After the Tera2 PCoIP Zero Client discovers the endpoint manager, the automatic discovery results appear on the Management page.

Configuring your system for automatic discovery

For information about how to configure your system for automatic discovery from the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

Discovering the Client Manually from the Endpoint Manager

Endpoint managers can be configured to discover endpoints like the Tera2 PCoIP Zero Client. This discovery method requires configuration on both the Tera2 PCoIP Zero Client and the endpoint manager.

To configure the Tera2 PCoIP Zero Client to be discoverable by an endpoint manager:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.
2. Set the *Security Level* option to **Low**.
3. Set the Manager Discovery Mode to **Automatic**.
4. Click **Apply**.

After the Tera2 PCoIP Zero Client is discovered, the endpoint manager topology appears on the Management page.

Initiating discovery from the PCoIP Management Console

For more information about initiating discovery from the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

Discovering the Endpoint Manager Manually from the Client Using Low or Medium Security Mode

In low or medium security modes, you can manually discover the endpoint manager by manually providing the URI for its bootstrap server.

Manual discovery requires a certificate

When manual discovery mode is used, DNS cannot be used to trust the endpoint manager. The Tera2 PCoIP Zero Client must have been previously provisioned with a certificate using an endpoint manager.

For more information, see Staging Clients Using an Endpoint Manager.

To configure a PCoIP Zero Client with an endpoint manager in low or medium security mode:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.
2. Set the *Security Level* option to **Low** or **Medium**.
3. Set the *Manager Discovery Mode* to **Manual**.
4. In the Manual Discovery section, type the bootstrap server's URI.

> **Bootstrap server URI must use a secured WebSocket prefix**
>
> URIs are in this format and require a secured WebSocket prefix: `wss://<internal EM IP address/FQDN>[:port number]` The PCoIP Management Console's listening port is 5172. If you omit the port number, port 5172 will be used by default.

5. Click Apply.

After the Tera2 PCoIP Zero Client discovers the endpoint manager, the endpoint manager topology appears on the Management page.

Discovering the Endpoint Manager Manually from the Client Using High Security Mode

In high security mode, automatic discovery is disabled entirely; you must register the Tera2 PCoIP Zero Client manually with the endpoint manager from the client.

> **Manual discovery requires a certificate**
>
> When manual discovery mode is used, DNS cannot be used to trust the endpoint manager. TheTera2 PCoIP Zero Client must have been previously provisioned with a certificate using an endpoint manager.
>
> For more information, see Staging Clients Using an Endpoint Manager.

To configure a PCoIP Zero Client with an endpoint manager using high security mode:

1. From the AWI, select **Configuration > Management**. The AWI Management page displays.
2. Set the *Security Level* option to **High**.

3. In the Endpoint Manager URI for Direct Connect section, find the Internal URI field and type the endpoint manager's URI. You can also provide an external URI, if needed.

> **Endpoint manager URI must use a secured WebSocket prefix**
>
> URIs are in this format and require a secured WebSocket prefix:
> `wss://<internal EM IP address/FQDN>[:port number]`
> The PCoIP Management Console's listening port is 5172. If you omit the port number, port 5172 will be used by default.

4. Click **Apply**.

After the Tera2 PCoIP Zero Client discovers the endpoint manager, the endpoint manager topology appears on the Management page.

Staging Clients Using an Endpoint Manager

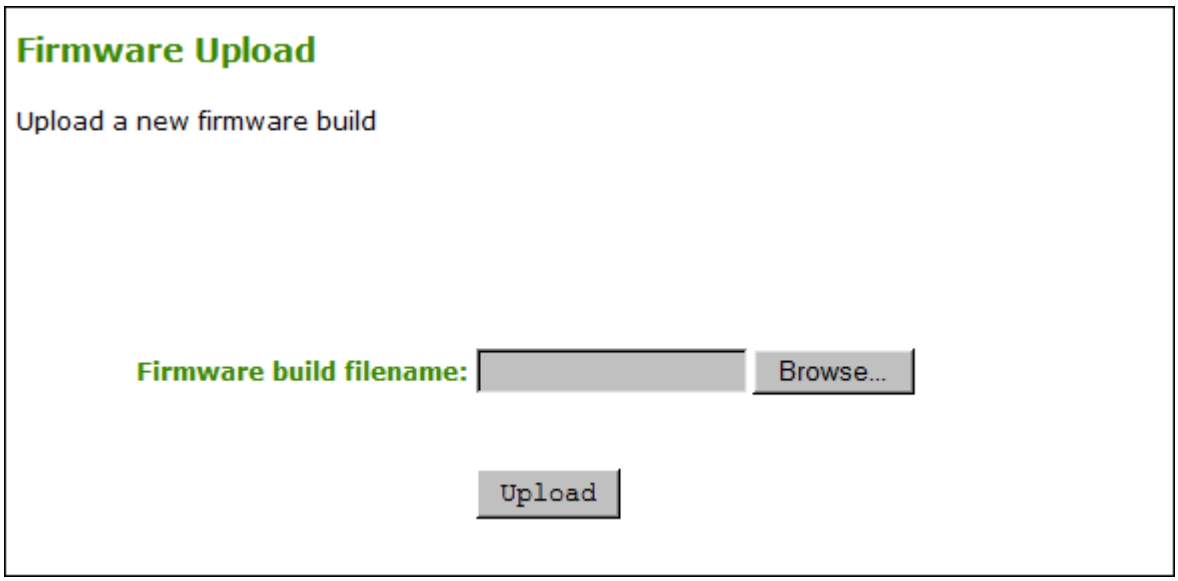
An installed certificate is required to connect to an endpoint manager in ***medium*** or ***high*** security levels; however, out of the box, the Tera2 PCoIP Zero Client's local certificate store is empty and it can only connect using the ***low*** security level.

To deploy a system using ***medium*** or ***high*** security settings, you must stage the device by connecting to an endpoint manager in ***low*** security mode and installing any required certificates.

Once the certificate has been installed, you can connect using any security level.

Uploading Firmware

You can upload new firmware to your Tera2 PCoIP Zero Client from the AWI Firmware *Upload* page as shown next.



AWI Firmware Upload page

The following parameters display on the AWI Firmware Upload page:

Firmware Upload Parameters

Parameter	Description
Firmware build filename	The filename of the firmware image to be uploaded. You can browse to the file using the **Browse** button. The file must be on a local or accessible network drive. The firmware image must be an `.all` file.
Upload	Click **Upload** to transfer the specified file to the device. The AWI prompts you to confirm this action to avoid accidental uploads.

To upload a firmware release to a client:

1. From the AWI, select **Upload > Firmware**.
2. Click **Browse** to browse to the folder containing the firmware file. The file will have an `.all` extension.

3. Double-click the correct `*.all` firmware file.
4. Click **Upload**.
5. Click **OK** to confirm that you want to proceed with the upload. The operation may take a few minutes. When completed, the AWI page displays two buttons: **Reset** and **Continue**.
6. Click **Reset**.
7. Click **OK**.

Important Information

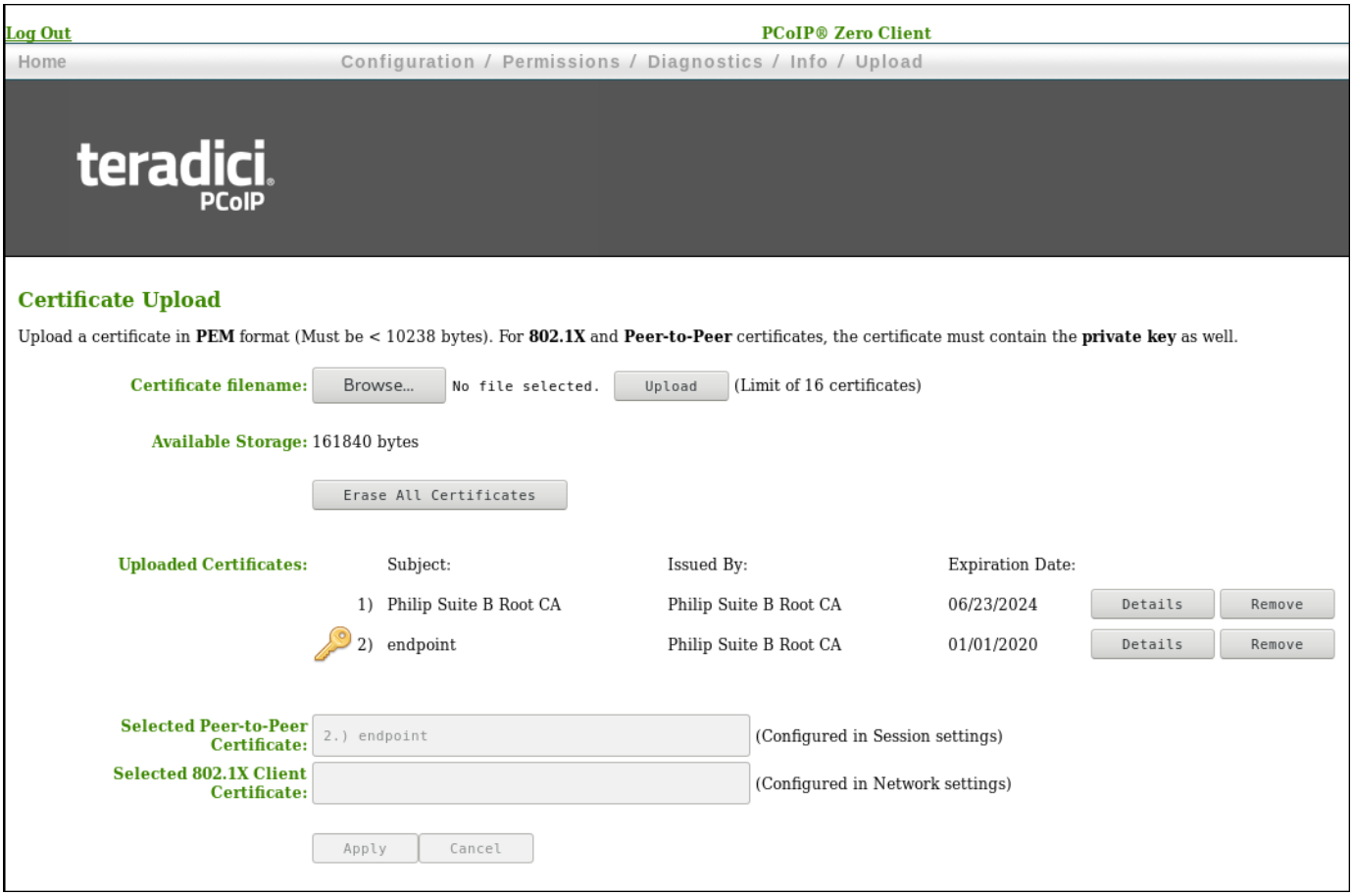
If you're connecting to a PCoIP Remote Workstation Card, it is recommended that the host and client use compatible firmware releases. Refer to your Zero Client and Remote Workstation Card firmware release notes for compatibility details.

As of firmware 5.0.0, Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards have separate ***.all*** files for uploading firmware to the device.

If you want to downgrade the firmware to an earlier version, Teradici recommends that you first reset the device parameters to the factory defaults, upload an earlier version of the firmware, and reconfigure your device settings. To reset the device, see Resetting Your Tera2 PCoIP Zero Client.

Uploading Certificates

You can upload and manage your CA root and client certificates for Tera2 PCoIP Zero Clients from the AWI's *Certificate Upload* page, shown below.



AWI Certificate Upload Page

Certificates used in PCoIP firmware must be in PEM format with a maximum file size of 10,237 bytes, and maximum RSA key size of 4096 bits. You can upload up to 16 certificates providing you don't exceed the maximum storage size of 163,648 bytes. The available storage field lets you know how much space is left in the certificate store.

You can simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a Simple Certificate Enrollment Protocol (SCEP) server. With SCEP enabled, you can only upload a maximum of 14 additional certificates, since two slots are reserved for SCEP server certificates. To upload certificates automatically using SCEP, see Obtaining Certificates Automatically Using SCEP.

Authentication issues

If you have authentication issues after uploading a Connection Server client certificate, see PCoIP TROUBLESHOOTING STEPS: View Connection Server Client Certificates (KB 1363) for further information.

Include all security information in 802.1X client certificate

The PCoIP protocol reads just one 802.1X client certificate for 802.1X compliant networks. Make sure you include all the security information for your PCoIP devices in that client certificate. For more information about uploading certificates, see Certificate management for PCoIP Zero Clients and Remote Workstation Cards (KB 1561). For information on 802.1X certificate authentication, see Configuring 802.1X Network Device Authentication.

802.1X Authentication

Use the following when you use 802.1X authentication:

- 802.1X authentication requires two certificates—an 802.1X client certificate and an 802.1X server CA root certificate.
- The 802.1X client certificate must be in .pem format and contain a private key that uses RSA encryption. If the certificate is in a different format, you must first convert the certificate, including the private key, to .pem format before uploading it.
- After uploading the 802.1X client certificate from the Certificate Upload page, you must configure 802.1X authentication from the Network page. This entails enabling 802.1X authentication, entering an identity string for the device, selecting the correct 802.1X client certificate from the drop-down list, and applying your settings.
- The 802.1X server CA root certificate must be in .pem format, but should not need to contain a private key. If the certificate is in a different format, you must convert it to .pem format before uploading it. This certificate does not require configuration from the **Network** page.
- Both the 802.1X client certificate and the 802.1X server CA root certificate must be less than 10,238 bytes; otherwise, you will not be able to upload them. Some certificate files may contain multiple certificates. If your certificate file is too large and it has multiple certificates within, you can open the file in a text editor, copy and save each certificate to its own file.

The following settings display on the AWI Certificate Upload page.

Certificate Upload Parameters

Parameter	Description
Certificate filename	Used to select a certificate to upload. You can upload up to a maximum of 16 root and client certificates.
Uploaded Certificates	This displays any uploaded certificates. To delete an uploaded certificate, click the **Remove** button. The deletion process occurs after the device is rebooted. To view the details of a certificate, click the **Detail** button. These certificates appear as options in the *Client Certificate* drop-down menu on the **Network** page.
Selected Peer-to-Peer Certificate	This is a read-only field. It is linked to the **Peer-to-Peer Certificate** field on the *Session* page.
802.1X Client Certificate	This is a read-only field. It is linked to the **Client Certificate** field on the *Network* page.

To upload a certificate to a client:

1. From the AWI, select the **Upload > Certificate**.
2. Browse to the folder containing the certificate file. This file will have a `.pem` extension.
3. Double-click the correct `.pem` certificate file.
4. Click **Upload**.
5. Click **OK** to confirm that you want to proceed with the upload.
6. Click **Continue**.

If the certificate uploads successfully, it will appear in the *Uploaded Certificates* list on this page.

Obtaining Certificates Automatically Using SCEP

Setting	Default	AWI	OSD	Management Console
SCEP Server URL	–	✔	✔	✔
Certificate usage	–	✔	✔	✔
Challenge Password	–	✔	✔	✔
Issuing CA Certificate	–	✔	✔	✔
Client Certificate	–	✔	✔	✔
CA Identifier	–	✔	✔	✔
Request Certificates (button)	–	✔	✔	✔
Status	–	✔	✔	✔

You can simplify the retrieval and installation of digital certificates by enabling devices to obtain certificates automatically from a Simple Certificate Enrollment Protocol (SCEP) server. You can obtain certificates for:

- **Administrative Web Interface**: Allows you to use SCEP to request a custom certificate for the Administrative Web Interface (AWI).
- **802.1X**: Allows you to use SCEP to request a custom certificate to use in your 802.1X configuration.

> **Enabling 802.1X**
>
> Enabling 802.1X also requires enabling 802.1X in the **Configuration > Networking** page of the OSD or AWI.

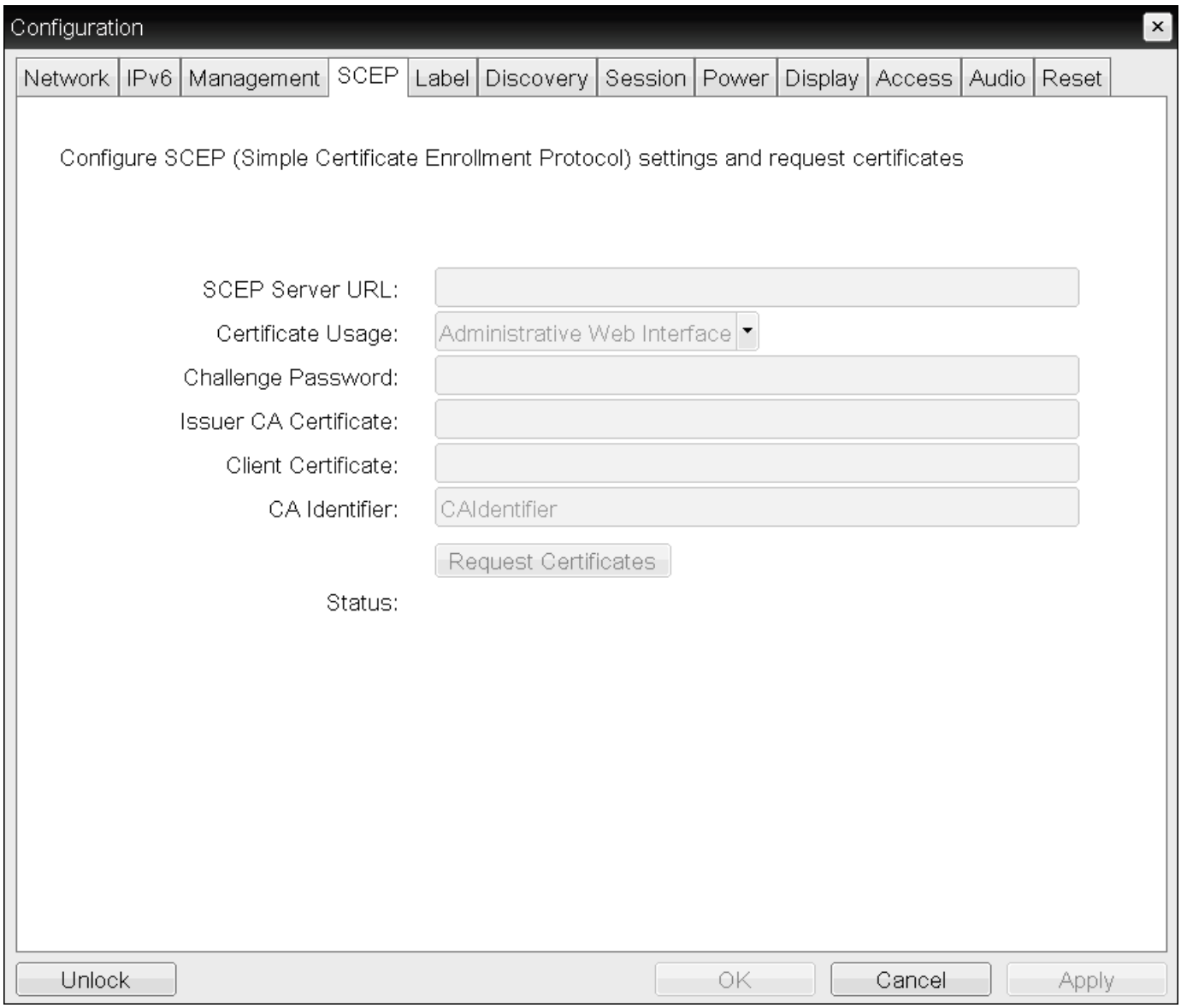
SCEP Behaviors

The following behaviors are observed when using SCEP to obtain your 802.1X or AWI certificates.

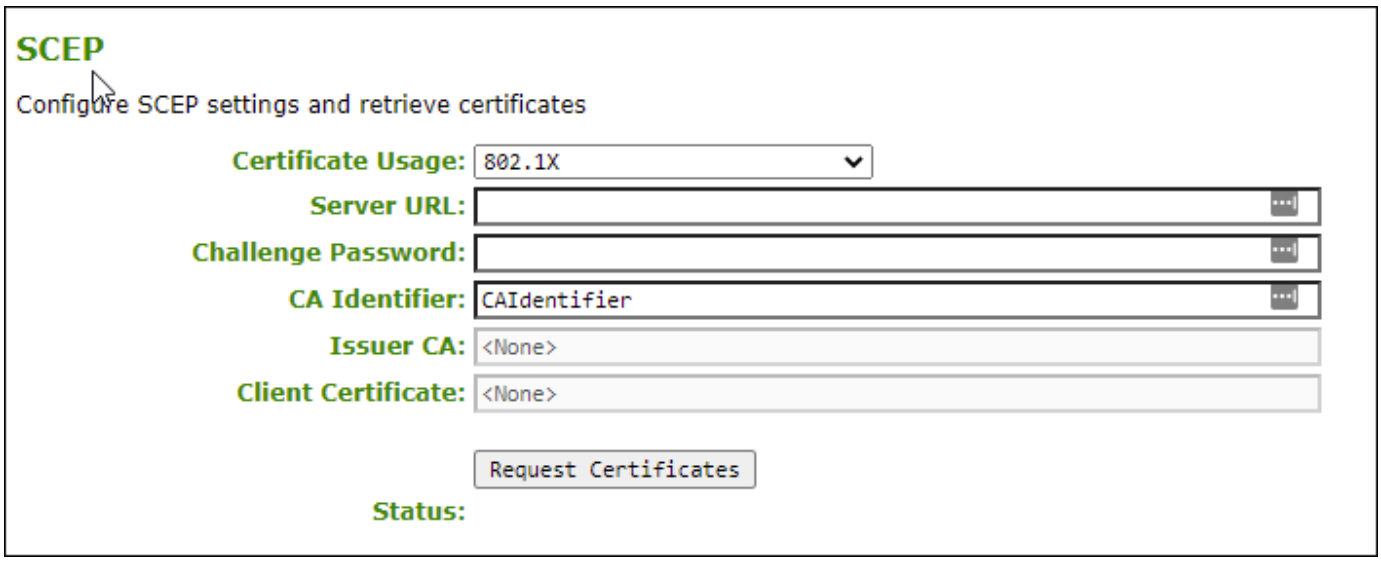
- A successful SCEP request for a certificate will install the SCEP certificate in the endpoints certificate store.
- A successful SCEP request for a certificate will no longer store the Root CA certificate in the endpoints certificate store.
- The OSD and AWI SCEP tab will display the Subject and Issuer names of the SCEP client certificate.
- Deleting an AWI SCEP certificate will cause it to revert to using the default AWI certificate. A reboot is required.
- Removing a 802.1X SCEP certificate happens immediately. The endpoint will fail 802.1X authentication on the next connection attempt or on the next automatic polling with the 802.1X switch.
- Additional successful SCEP requests will overwrite any previously installed SCEP certificates for the same usage.
- The Tera2 endpoint generates its own 3072-bit SCEP RSA private key when a certificate is requested. This key is used to construct a PKCS#10-formatted certificate request, which is then delivered to the SCEP server.
- Endpoint SCEP certificate requests include the following parameters:
  - **Subject Name**: PCoIP Device Name
  - **Subject Alt Name**: MAC Address, User Principal Name (UPN), and the Fully Qualified Domain Name (FQDN)

The following cryptography algorithms are used to generate a Zero Client SCEP request:

- Content Key Encryption Algorithm: RSAES-OAEP
- Hash Algorithm: SHA384
- Content Encryption Algorithm: AES-256-CBC



OSD SCEP page



AWI SCEP page

The following settings display on the OSD and AWI **SCEP** pages:

SCEP Parameters

Parameter	Description
SCEP Server URL	Enter the URL for the SCEP server that is configured to issue certificates for the device.
Certificate Usage	There are two options: • **Administrative Web Interface**: Automatically request a custom certificate for connections to the AWI. • **802.1X**: Automatically request a custom certificate for use in your 802.1X configuration.
Challenge Password	Enter the password required by the SCEP server
Issuer CA Certificate	Displays the Issuer CA certificate that signed the client certificate. (The endpoint no longer stores the Root CA certificate)
Client Certificate	Displays the name of the client certificate that has been installed in the device.
CA Identifier	A string provided by your CA issuer that uniquely identifies the Certificate Authority when providing certificates for SCEP requests.
Request Certificates (button)	After entering the SCEP server address, password, certificate usage, and CA Identifier, click this button to retrieve certificates.

Parameter	Description
Status	Displays the status of the request (for example, requesting, successful, failed).

To obtain certificates using SCEP:

1. Open the SCEP page:
   - From the OSD, select **Options > Configuration > SCEP**.
   - From the AWI, select **Configuration > SCEP**.
2. Select the **Certificate Usage** type.
3. Enter the URL and challenge password for the SCEP server.
4. Enter the **CA Identifier** if required. Provide a valid CA Identifier or use "CAIdentifier" (default).
5. Click **Request Certificates** to retrieve the certificate. The issuing CA and client certificates display after a successful SCEP request.

The **Status** section displays the status of the request such as Requesting, Request completed, or Request failed.

To delete your SCEP certificate:

1. Browse to the AWI **Upload > Certificates** page.
2. Click the **Remove** button beside the certificate you wish to remove.
3. Click **Apply** and then **Continue**.

Assigning an IP Address to a Tera2 PCoIP Zero Client

When a Tera2 PCoIP Zero Client is powered on for the first time, you can display its IP address by logging into the OSD and selecting **Options > Configuration > Network**.

If you want, you can manually change the IP address either dynamically or statically.

Assigning the IP Address Dynamically

If your network supports DHCP and your Tera2 PCoIP Zero Client is enabled for DHCP, the Tera2 PCoIP Zero Client will automatically receive an IP address from your DHCP server when it's first powered on. One advantage to dynamic IP address assignment is that you can deploy multiple Tera2 PCoIP Zero Clients simultaneously in your network.

The Tera2 PCoIP Zero Client may receive a different IP address when it's powered off

- If the client is subsequently powered off for a period of time that exceeds its DHCP lease time, the client may receive a different IP address when it's powered on again. You can avoid this issue by using a DHCP reservation to permanently associate the IP address received from the DHCP server with the device.
- As well, if there is no available DHCP server when the zero client powers on, after 4 attempts the zero client will use it's fall back IP address. Only a power reset will initiate a DHCP request at this point.

Assigning the IP Address Statically

If your network doesn't support DHCP, the Tera2 PCoIP Zero Client will use its static fallback IP address the first time it's powered on. This address is set by the device's manufacturer.

You can statically assign an IP address from the Tera2 PCoIP Zero Client's OSD Network page. Because all Tera2 PCoIP Zero Clients from the same manufacturer will have the same default IP address, you can only deploy a single client at a time when you assign IP addresses statically.

You can also configure an IP address from the AWI Initial Setup page

You can also assign an IP address (and other network settings) from the AWI Initial Setup page. To configure the IP address from this page, see Configuring Initial Setup Parameters.

To statically assign an IP address from the OSD:

1. From the OSD, select **Options > Configuration > Network**.
2. From the OSD *Network* page, select **Unlock**. If required, enter a password to make changes.
3. Ensure that *Enable DHCP* is not selected, and then enter the client's IP address and other network addresses.
4. Click **Apply, and then click Reset to reset the device so the changes can take effect.

Locating the factory default IP address

You can locate the factory default IP address for a client in the IN OFD: (optional factory defaults) section of the the device's event log:

```
IN OFD:          enable_static_ip_fallback = enabled
IN OFD:         static_ip_fallback_timeout = 120
IN OFD:      static_ip_fallback_ip_address = 192.168.1.50
IN OFD:         static_ip_fallback_gateway = 192.168.1.1
IN OFD:     static_ip_fallback_subnet_mask = 255.255.255.0
```

The static fallback IP address can also be set from the PCoIP Management Console. In this case, the event log will display the address as being *IN FLASH:* rather than *IN OFD:*

```
IN OFD:          enable_static_ip_fallback = enabled
IN OFD:         static_ip_fallback_timeout = 120
IN FLASH:    static_ip_fallback_ip_address = 192.168.1.101
IN OFD:         static_ip_fallback_gateway = 192.168.1.1
IN OFD:     static_ip_fallback_subnet_mask = 255.255.255.0
```

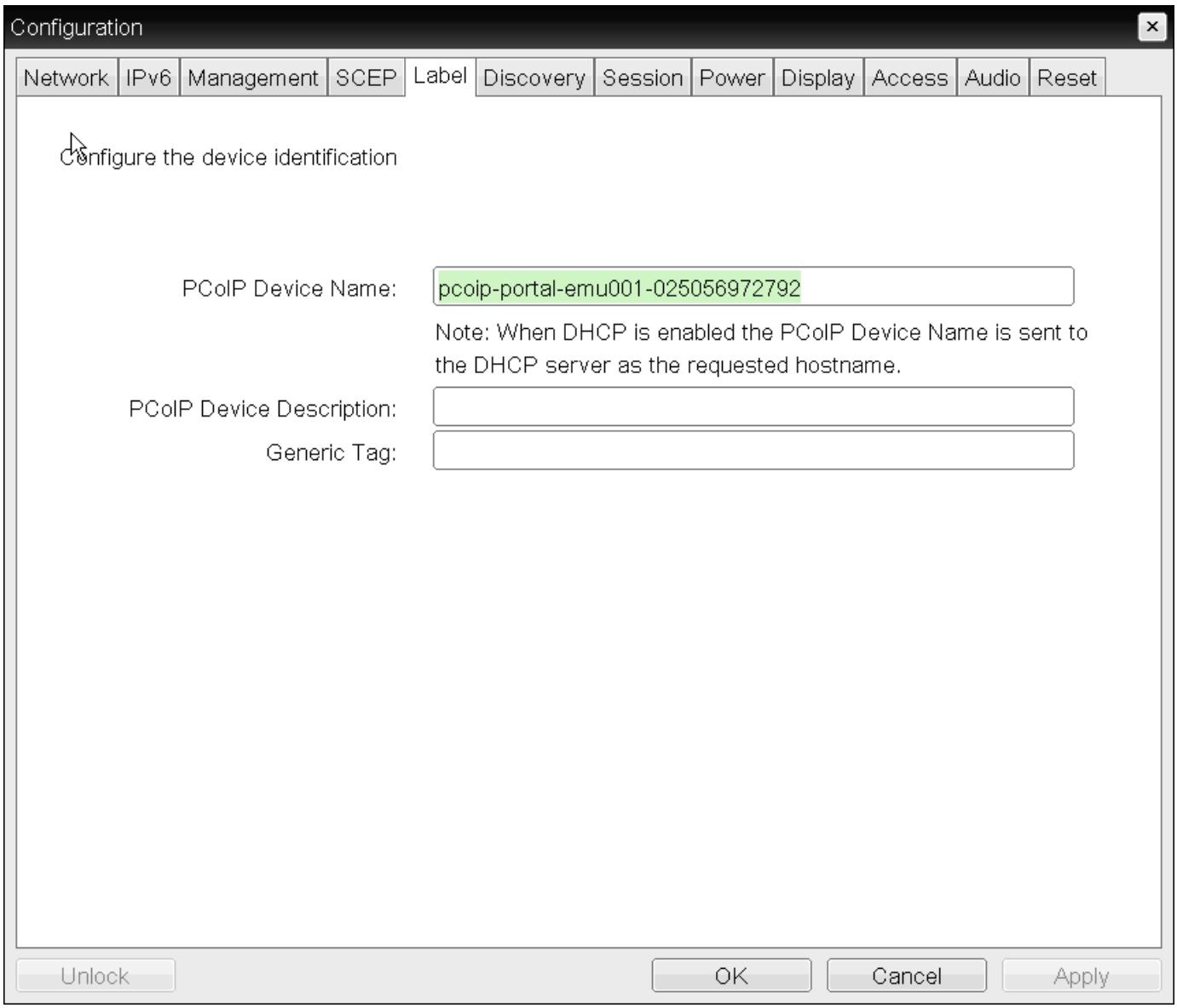
If you reset the client (see Resetting Your Tera2 PCoIP Zero Client), the static fallback IP address will revert to the factory default, even when it has been set by the PCoIP Management Console.

Assigning a Name to Your Tera2 PCoIP Zero Client

You can assign a name to your Tera2 PCoIP Zero Client, as well as add a description and additional information about the device. You can use the OSD or AWI to assign the information.

Assigning a Device Name from the OSD

You can configure a device name from the OSD Label page, as shown next.



OSD Label page

The following parameters display on the OSD Label page:

OSD Label Parameters

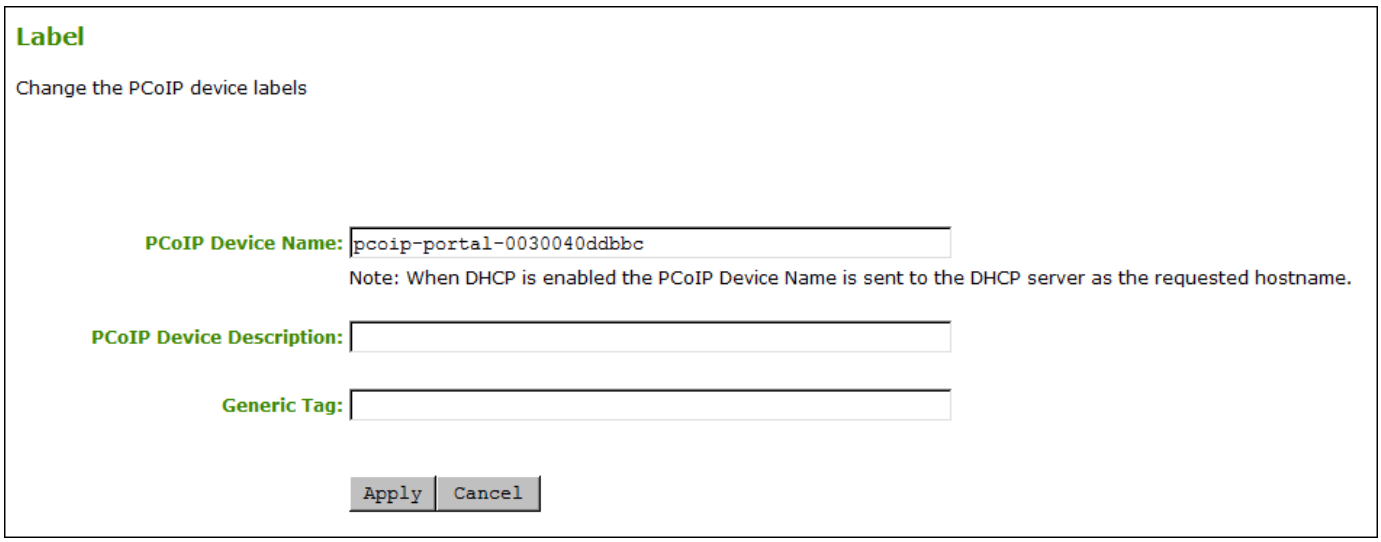
Parameter	Description
PCoIP Device Name	Lets you give the device a logical name. The default is pcoip-portal-*<MAC>*, where *<MAC>* is the device's MAC address. This field is the name the device registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server. It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions: • The first and last character must be a letter (A-Z or a-z) or a digit (0-9). • The remaining characters must be letters, digits, hyphens, or underscores. • The length must be 63 characters or fewer.
PCoIP Device Description	A description of the device or other information, such as the location of the device's endpoint. The firmware does not use this field. It is provided for administrator use only.
Generic Tag	Generic tag information about the device. The firmware does not use this field. It is provided for administrator use only.

To assign a device name from the OSD:

1. From the OSD, select **Options > Configuration > Label**.
2. From the OSD ***Label*** page, enter a device name, a description, and additional information (if necessary).
3. Click **OK**.

Assigning a Device Name from the AWI

You can assign a device name from the AWI Label page, shown next.



AWI Label page

The following parameters display on the AWI Label page:

AWI Label Parameters

Parameter	Description
PCoIP Device Name	Lets you give the device a logical name. The default is pcoip-portal-, where is the device's MAC address. This field is the name the device registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server. It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions: • The first and last character must be a letter (A-Z or a-z) or a digit (0-9). • The remaining characters must be letters, digits, hyphens, or underscores. • The length must be 63 characters or fewer.
PCoIP Device Description	A description of the device or other information, such as the location of the device's endpoint. The firmware does not use this field. It is provided for administrator use only.
Generic Tag	Generic tag information about the device. The firmware does not use this field. It is provided for administrator use only.

To assign a device name from the AWI:

1. From the AWI, select Configuration > Label.
2. From the AWI Label page, enter a device name, a description, and additional information (if necessary).
3. Click **Apply**.

Resetting Your Tera2 PCoIP Zero Client

Setting	Default	AWI	OSD	Management Console
Reset Parameters (a button)	–	✔	✔	✔
Enable keyboard shortcut	Disabled	✔	✘	✔
Hide keyboard shortcut sequence in OSD	Disabled	✔	✘	✔
Remote Reset Notification timeout (seconds)	None	✔	✘	✔

You can reset the Tera2 PCoIP Zero Client's parameters to the factory default values stored in flash memory. You can also enable a keyboard shortcut to reset device parameters.

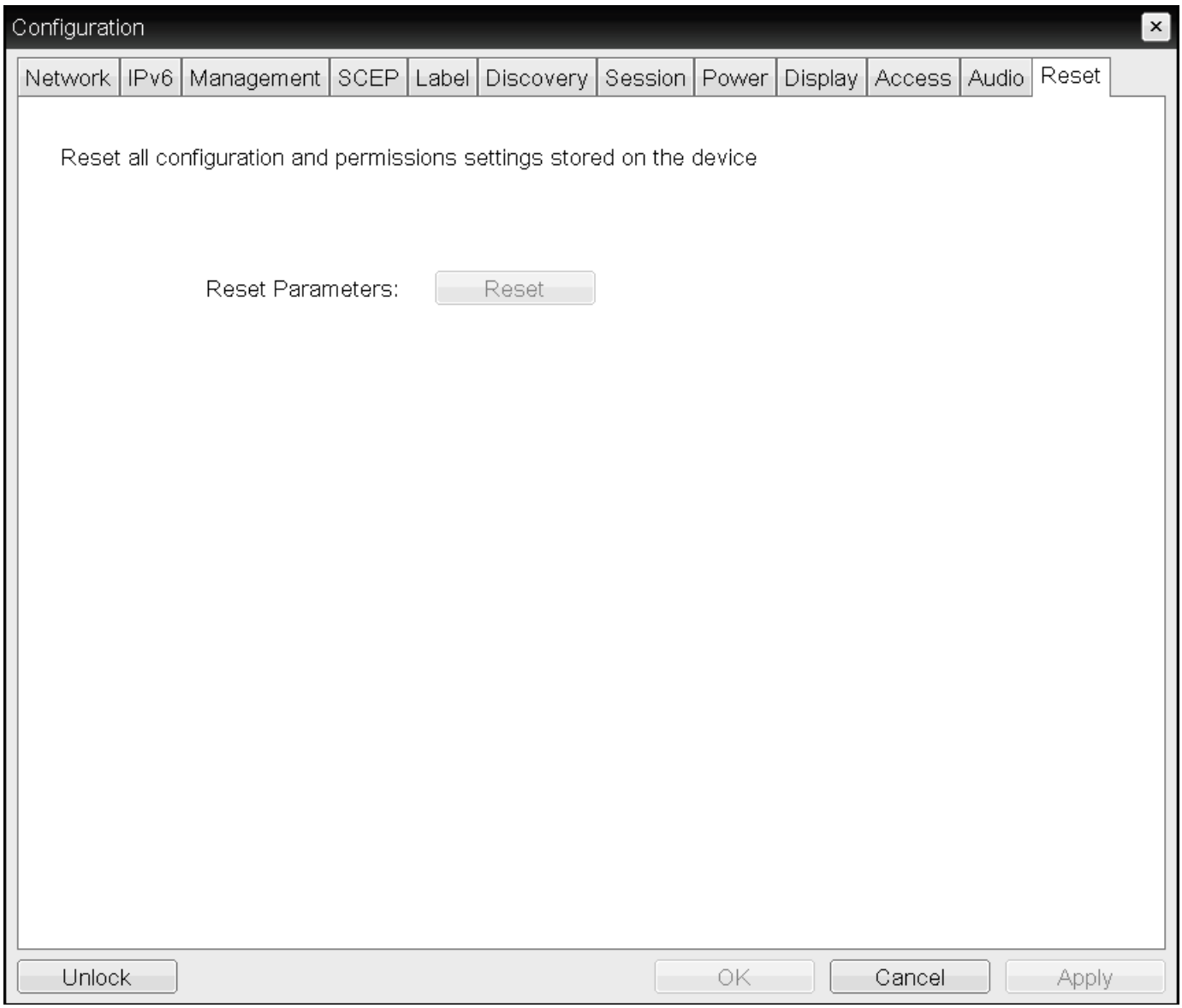
Before resetting your endpoint, you should have a thorough understanding of your current Zero Client configuration. If you do a factory reset then all configurations are removed including access to the AWI. The one exception is any custom OSD logo you may have uploaded will remain unchanged.

Access after a factory reset

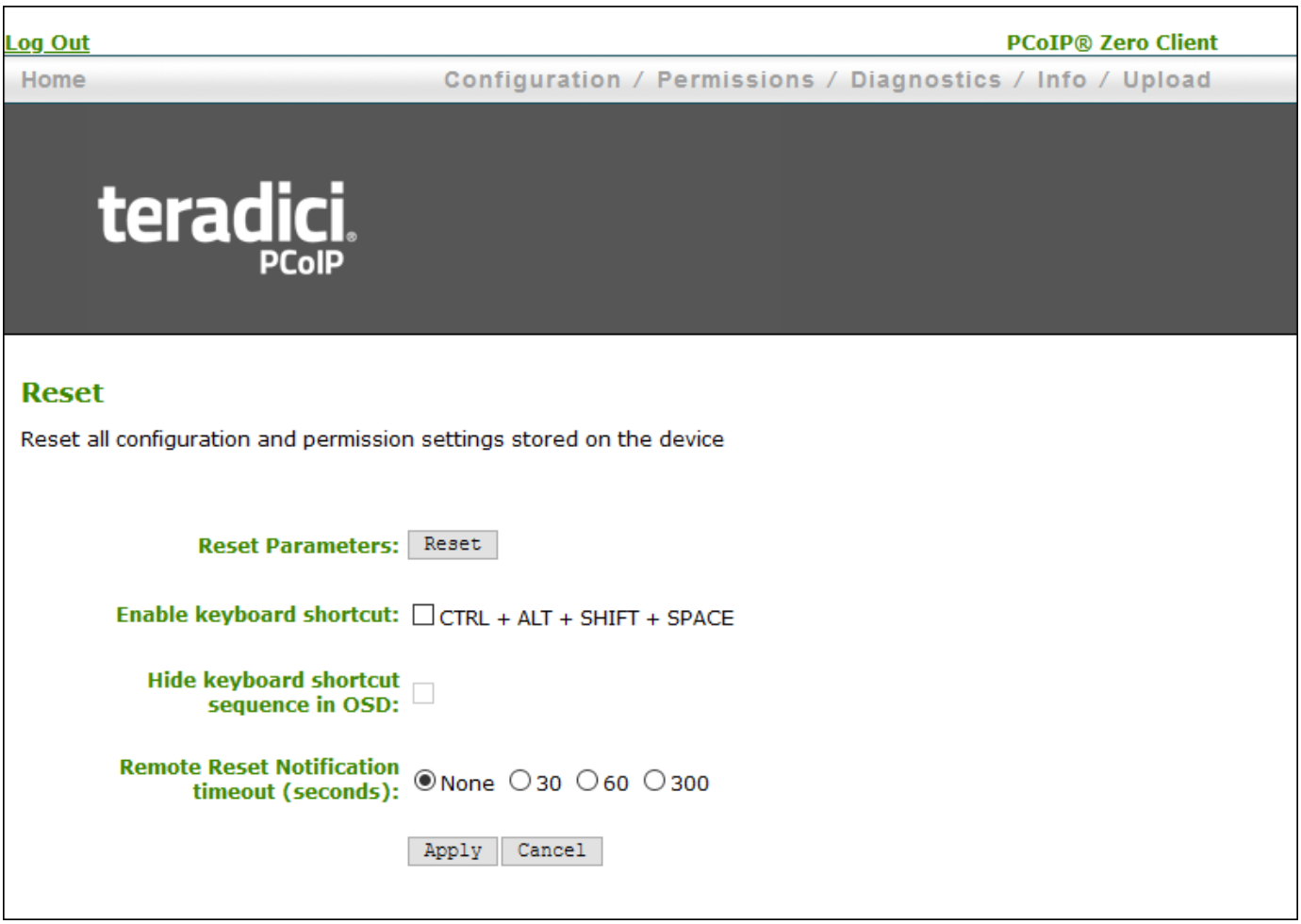
A factory reset may require you to access the OSD to perform additional configurations or it may require your endpoint to be able to connect to a Management Console so the AWI can be enabled if disabled should you not be at the location of your endpoint.

- Off premises Zero Clients remotely managed by Management Console
  If your Zero Client is located at your home and is being remotely managed by Management Console and you perform a factory reset, you must follow the guide for remote management (Connecting to a Remote Endpoint from OSD) and ensure you modify the Zero Client network settings from the OSD screen to add the custom domain name to the network settings and reboot then Zero Client.
- Zero Clients configured for autodiscovery
  If your endpoint was managed by a Management Console prior to performing a factory reset, the settings to connect to your Management Console will be lost. To get your endpoint back into the Management Console when on premises, you should have your endpoint configured for auto discovery. For further DHCP and DNS autoconfiguration directions, see Configuring Endpoints for autodiscovery using DNS or Configuring Endpoints for Auto Discovery Using DHCP. When configured for autodiscovery, your endpoint will automatically check back into the management console when connected to the network. After it establishes communication with the Management Console, ensure it is in the correct Management Console Group and apply any profiles that are required for that endpoint. See Configuring Discovery for information on where to configure your Zero Client discovery settings.
- Manual Discovery
  If your endpoint was configured for manual discovery prior to performing a factory reset, you might have additional configurations to perform. For instance, when using self-signed certificates you might have to upload this certificate to the Zero Client certificate store and then enter the public URL for the Management Console. After this, the Management Console administrator would have to manually rediscover the endpoint. To do this you will need access to the Zero Client OSD or AWI. See Configuring Access to Management Tools

You can reset parameters from both the OSD or AWI Reset pages, as shown next. From the AWI Reset page, you can configure the reset shortcut.



OSD Reset page



AWI Reset page

Factory Default Values

Resetting parameters to factory default values does not revert the firmware or clear the custom OSD logo.

Resetting Parameters

From the OSD and AWI Reset pages, you can reset parameters to the factory default values stored in flash memory.

To reset parameters:

1. Open the Reset page:
   - From the OSD, select **Options > Configuration > Reset**.
   - From the AWI, select **Configuration > Reset**.

2. From the OSD or AWI *Reset* page, click **Reset**. When you click **Reset**, a prompt appears to confirm you want to reset the parameters.

Configuring a Reset Shortcut

From the AWI, you can enable a keyboard shortcut (`Ctrl`+`Alt`+`Shift`+`Space`) to reset your Tera2 PCoIP Zero Client's parameters to its factory default values. When enabled, you can use the shortcut to automatically reset device parameters.

You enable the shortcut on the AWI *Reset* page. After you enable the shortcut, you can choose to display or hide the shortcut on the OSD *Reset* page. If you choose to hide the shortcut on the OSD page, you can still use the shortcut to reset parameters.

To enable the reset keyboard shortcut:

1. From the AWI, select **Configuration > Reset Parameters**.
2. From the AWI *Reset* page, do the following:
    - To enable the shortcut, select the **Enable keyboard shortcut** check box. When enabled, you can use the shortcut to automatically reset device parameters.
    - To display the shortcut on the OSD *Reset* page, clear the **Hide keyboard shortcut sequence in OSD** check box.
    - To prevent the shortcut from displaying on the OSD *Reset* page, select the **Hide keyboard shortcut sequence in OSD** check box. Even though the shortcut doesn't display, you can still use the shortcut to reset device parameters.

Configuring Remote Reset Notification timeout (seconds)

If a configuration change (AWI or Management Console profile application) requires a PCoIP Zero Client reboot, the administrator can configure a notification warning of the pending reboot that will be seen on the monitor. This will allow the user to save any work they may have open.

1. Select either the 30, 60, or 300 second option and apply the setting.

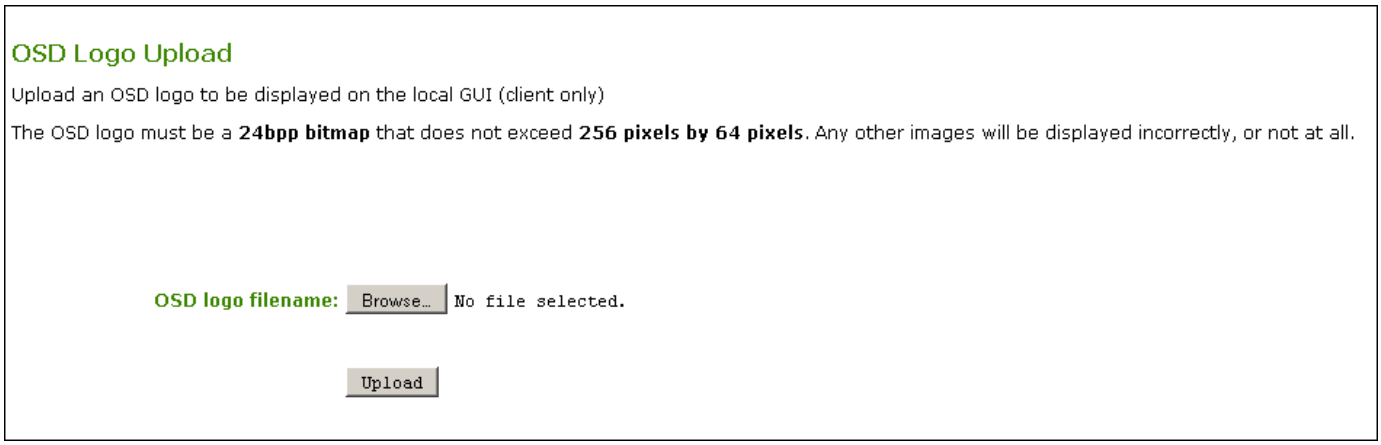
Displaying an OSD Logo

From the AWI, you can upload an image to display on the OSD Connect page.

After you've uploaded an image, you can configure the image to display on OSD login screens (instead of the default banner). You can do this if you've configured your Tera2 PCoIP Zero Client to use a PCoIP Connection Manager as the PCoIP session broker, or a View Connection Server as the broker when connecting to a VMware desktop.

Displaying a Logo on the OSD Connect Page

From the *OSD Logo Upload* page, as shown next, you can upload an image to display on the OSD Connect page.



To display a logo on the OSD Connect page:

1. From the AWI, select **Upload > OSD Logo**.
2. From the *OSD Logo Upload* page, click **Browse** to search for a logo file. The file must be on a local or accessible network drive.
   The 24 bpp (bits per pixel) image must be in BMP format, and its dimensions cannot exceed 256 pixels in width and 64 pixels in height. If the file extension is incorrect, an error message displays.
3. Click **Upload** to transfer the specified image file to the client. A message confirming the upload displays.

Displaying a Logo on OSD Login Screens

You can configure the image you uploaded to display on the OSD Connect page to display at the top of OSD login screens. You can do this if you've configured your Tera2 PCoIP Zero Client to use a PCoIP Connection Manager as the PCoIP session broker, or a View Connection Server as the broker when connecting to a VMware desktop.

To enable a logo to display on OSD login screens:

1. If you haven't already done so, upload an image to display on the OSD ***Connect*** page.
2. From the AWI, select **Configuration > Session**.
3. Select the **Use OSD Logo for Login Banner** check box to enable the OSD logo banner to display at the top of login screens (instead of the default banner).
4. Click **Apply**.

Setting Up a Touch Screen Display

This topic explains how to install and configure an Elo TouchSystems touch screen display for your Tera2 PCoIP Zero Client. You'll learn how to:

- Install an Elo TouchSystems touch screen display (see Installing the Touch Screen Display).
- Configure and calibrate settings for an attached Elo TouchSystems touch screen display (see Configuring the Touch Screen from the OSD).
- Configure the firmware if you want the touch screen to be controlled by a driver running on the host (see Setting up the Touch Screen as a Bridged Device)
- Set up auto-logon to bypass authentication when users are connecting to a host with a broker (see Configuring the Tera2 PCoIP Zero Client to Automatically Log into a Host Brokered by a Connection Manager).

Installing the Touch Screen Display

The following procedure shows you how to Install an Elo TouchSystems touch screen display.

To install an Elo TouchSystems touch screen display:

1. Plug in the touch screen's USB cable to the Tera2 PCoIP Zero Client's USB port.
2. Attach the monitor cable from the touch screen to any port on the Tera2 PCoIP Zero Client.

> **Don't attach multiple touch screens to the PCoIP Zero Client**
>
> You can't attach multiple touch screens to the Tera2 PCoIP Zero Client, but you can attach additional non-touch screens to the Tera2 PCoIP Zero Client in addition to the touch screen as long as the touch screen is attached to the port on the Tera2 PCoIP Zero Client that is configured as the primary port.

3. Plug in the power.
4. Disconnect the Tera2 PCoIP Zero Client session. This initiates the calibration on the touch screen.

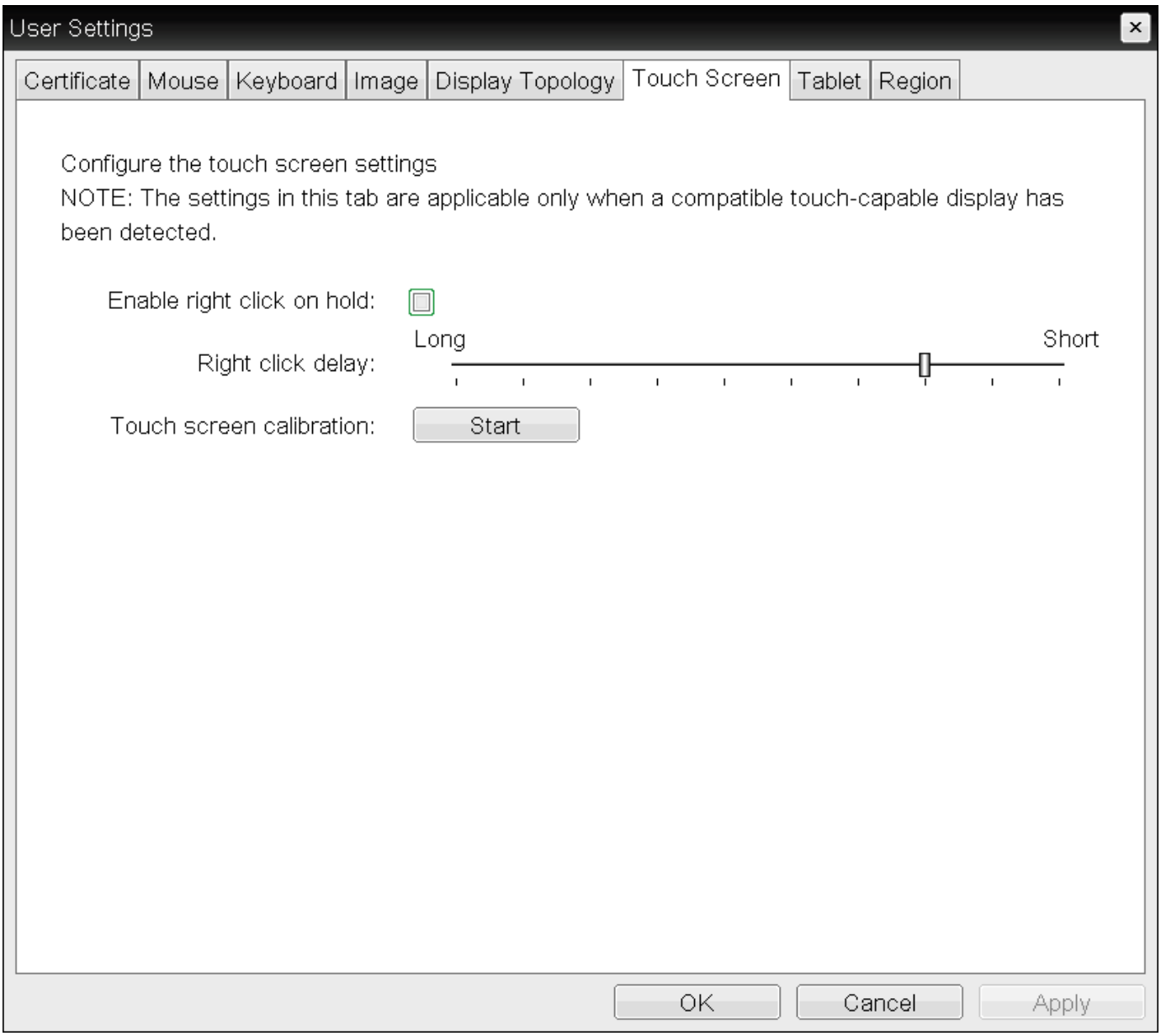
> **Touch screen's co-ordinates are saved in flash memory**
>
> Once the touch screen is calibrated, the co-ordinates are saved in flash memory. You can manually recalibrate the screen as required through the OSD Touch Screen page.

5. Follow the touch screen prompts. You can test the calibration with your finger (the cursor should move with your finger). If the screen is not properly calibrated, the system automatically restarts the calibration program.

Configuring the Touch Screen from the OSD

Setting	Default	AWI	OSD	Management Console
Enable right click on hold	Disabled	✖	✔	✖
Right click delay	Set for a shorter delay	✖	✔	✖
Touch screen calibration (N/A; You must press **Start** to begin calibration) ✖	✔	✖		

The OSD Touch Screen page, as shown next, enables you configure and calibrate settings for an attached Elo TouchSystems touch screen display.



OSD Touch Screen page

Supported touch screens

Elo IntelliTouch and Elo AccuTouch are the only Elo TouchSystems touch screens supported.

The following parameters display on the OSD Touch Screen page.

OSD Touch Screen Parameters

Parameter	Description
Enable right click on hold	Select this check box to let users generate a right-click when they touch the screen and hold it for a few seconds. If disabled, right-clicking is not supported.
Right click delay	Slide the pointer to the position (between Long and Short) to determine how long the users must touch and hold the screen to generate a right-click.
Touch screen calibration	When you first connect the touch screen to the Tera2 PCoIP Zero Client, the calibration program starts. At the touch screen, touch each of the three targets as they appear. To test the calibration, run your finger along the monitor and ensure that the cursor follows it. If it is not successful, the calibration program automatically restarts. Once calibrated, the coordinates are stored in flash. To manually start the calibration program, from the OSD Touch Screen page, click **Start**. Follow the onscreen prompts.

To configure a touch screen from the OSD:

1. From the OSD, select **Options > User Settings > Touch Screen.**
2. From the OSD *Touch Screen* page, update the touch screen settings.
3. Click **OK**.

Setting up the Touch Screen as a Bridged Device

> **Setting up a touch screen as a bridged device is optional**
>
> This procedure is optional and only necessary if you want the touch screen to be set up as a bridged device.

While a session is active a user may want the touch screen to be controlled by a driver running on the host. To set this up the touch screen must be added to the list of bridge devices.

To set up the touch screen as a bridged device:

1. Install the touch screen to your Tera2 PCoIP Zero Client (see Installing the Touch Screen Display).

2. Log into the Tera2 PCoIP Zero Client AWI.
3. From the AWI Info menu, click **Attached Devices**. The Attached Devices page displays (as shown next), showing the PID and VID information.

   VID and PID numbers

   Write down the PID and the VID information. From the Permissions menu, click USB to display the USB permissions page. In the Bridged Devices section, click **Add New**. Enter the Vendor ID and Product ID for the touch screen (as shown next), and then click Add.

   USB permissions page

   Restart the Tera2 PCoIP Zero Client session. Install the touch screen driver from Elo TouchSystems. See the Elo TouchSystems documentation for installation and calibration instructions.

Configuring the Tera2 PCoIP Zero Client to Automatically Log into a Host Brokered by a Connection Manager

To make logging into the touch screen device easier, you can configure auto-logon to bypass the keyboard when using a broker as a connection manager.

If you choose to set this up, users simply need to touch Connect at the Login window instead of also having to enter their login credentials.

To configure the Tera2 PCoIP Zero Client to automatically log into a host brokered by a connection manager:

1. Log into the AWI for the Tera2 PCoIP Zero Client.
2. From the Configuration menu, select Session.
3. In the Session Connection Type drop-down menu, select **PCoIP Connection Manager + Auto-Logon** or **View Connection Server + Auto-Logon**, depending on the connection server you're using.
4. Enter the connection server's DNS name or IP address.
5. Complete the user credentials, and then click **Apply**.

Viewing Information About your Tera2 PCoIP Zero Client

From time to time, you'll want to view information about your Tera2 PCoIP Zero Client so you can complete certain tasks or troubleshoot issues. Information you can view includes your Tera2 PCoIP Zero Client's IP address, hardware, firmware, and processor information, and information about attached devices, such as monitors and USB devices.

Obtaining More Information About Your Tera2 PCoIP Zero Client

To view additional information about your Tera2 PCoIP Zero Client, such as statistical and logging information, see Performing Diagnostics. You can also view processor and statistical information from the AWI Home page.

Viewing the IP Address

You can view your Tera2 PCoIP Zero Client's IP address from the OSD ***Network*** page.

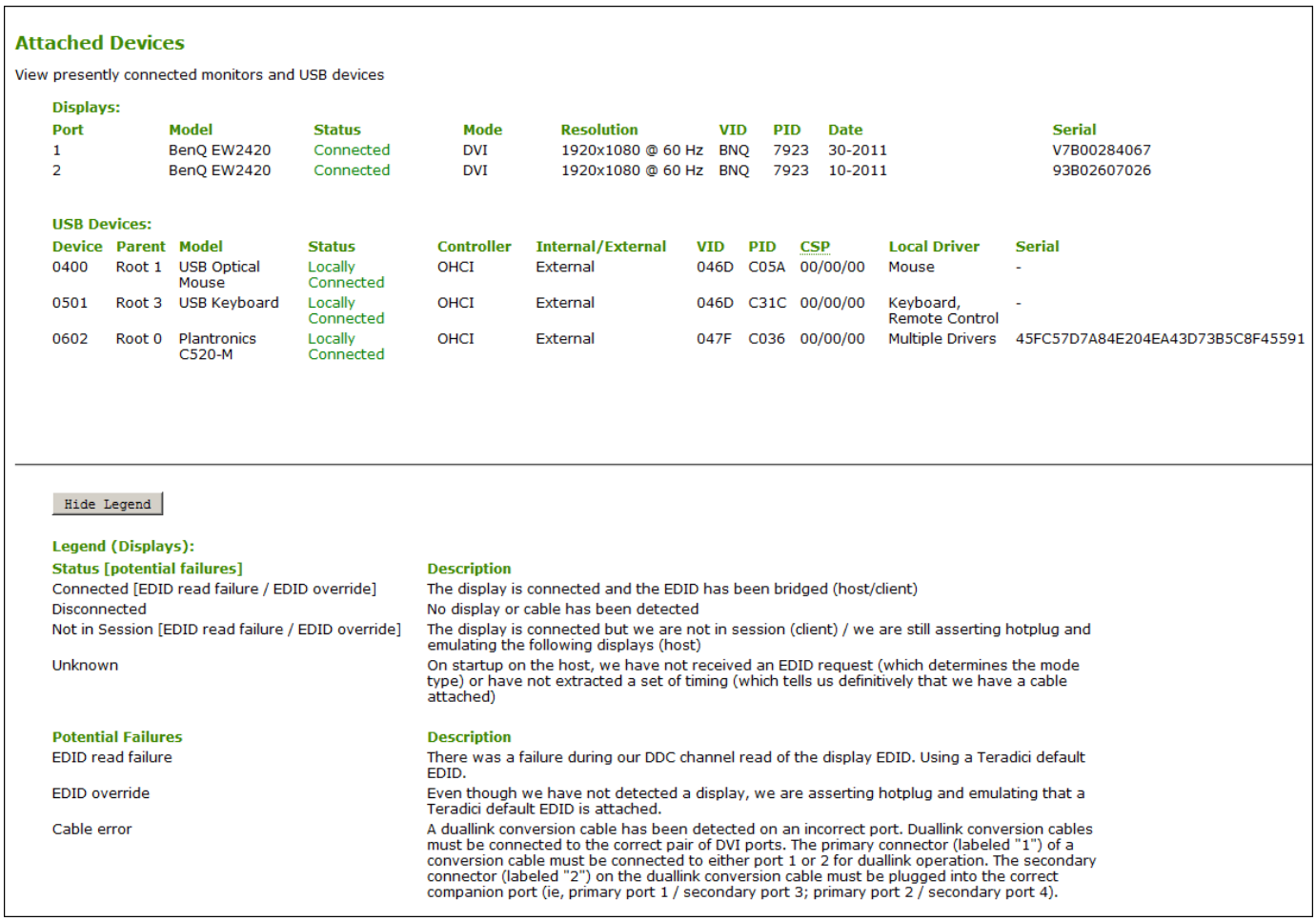
To view the Tera2 PCoIP Zero Client IP address:

- From the OSD, choose **Options > Information > Network.**

The OSD ***Network*** page displays, as shown next, showing the device's IP address.

Viewing Information About Attached Devices

You can view information about the devices (such as keyboards, mice, monitors, and tablets) attached to your Tera2 PCoIP Zero Client. The information displays on the AWI *Attached Devices* page, as shown next.



Attached Devices

View presently connected monitors and USB devices

Displays:

Port	Model	Status	Mode	Resolution	VID	PID	Date	Serial
1	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	BNQ	7923	30-2011	V7B00284067
2	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	BNQ	7923	10-2011	93B02607026

USB Devices:

Device	Parent	Model	Status	Controller	Internal/External	VID	PID	CSP	Local Driver	Serial
0400	Root 1	USB Optical Mouse	Locally Connected	OHCI	External	046D	C05A	00/00/00	Mouse	-
0501	Root 3	USB Keyboard	Locally Connected	OHCI	External	046D	C31C	00/00/00	Keyboard, Remote Control	-
0602	Root 0	Plantronics C520-M	Locally Connected	OHCI	External	047F	C036	00/00/00	Multiple Drivers	45FC57D7A84E204EA43D73B5C8F45591

Hide Legend

Legend (Displays):

Status [potential failures]	Description
Connected [EDID read failure / EDID override]	The display is connected and the EDID has been bridged (host/client)
Disconnected	No display or cable has been detected
Not in Session [EDID read failure / EDID override]	The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)
Unknown	On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)

Potential Failures	Description
EDID read failure	There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.
EDID override	Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached.
Cable error	A duallink conversion cable has been detected on an incorrect port. Duallink conversion cables must be connected to the correct pair of DVI ports. The primary connector (labeled "1") of a conversion cable must be connected to either port 1 or 2 for duallink operation. The secondary connector (labeled "2") on the duallink conversion cable must be plugged into the correct companion port (ie, primary port 1 / secondary port 3; primary port 2 / secondary port 4).

The following information displays on the AWI Attached Devices page:

Attached Devices Information

Statistic	Description
Displays	This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the display attached to each port. This option is only available when the host is in a PCoIP session.

Statistic	Description
USB Devices	This section displays the port mode, model, status, device class, subclass, protocol, vendor identification (VID), and product identification (PID) of the USB device attached to the client.
USB Device Status	Status options include: • **Not Connected:** No device is connected. • **Not in Session:** The device is detected outside of a PCoIP session. • **Not Initialized:** The device is detected in a PCoIP session but the host controller has not initialized the device. • **Failed Authorization:** The device is detected in a PCoIP session but is not authorized. (For more information about USB, see Configuring USB Settings and Permissions. • **Locally Connected:** The device is detected and authorized but locally terminated in a PCoIP session (for example, a local cursor). • **Connected:** The device is detected and authorized in a PCoIP session.

Each USB device possesses one device descriptor and an interface descriptor for each device function

Every USB device has a single device descriptor as well as an interface descriptor for each of the device's functions. (For example, a USB device with a camera, microphone, and button would have an interface descriptor for each function.)
In the USB specification, the USB Device Class, Sub Class, and Protocol class code fields identify a device's functionality so that the correct device driver will load for the device. Depending on the device, this information can display in either the device descriptor or the interface descriptors, or in both.

If a device is authorized, the Device Class, Sub Class, and Protocol class code fields that display on the *Attached Devices* page are the same values obtained from the device descriptor.

If a device is ***not*** authorized, the Device Class, Sub Class, and Protocol class code fields that display on the ***Attached Devices*** page are the same values obtained from the interface that caused the device to fail authorization.

To view device information:

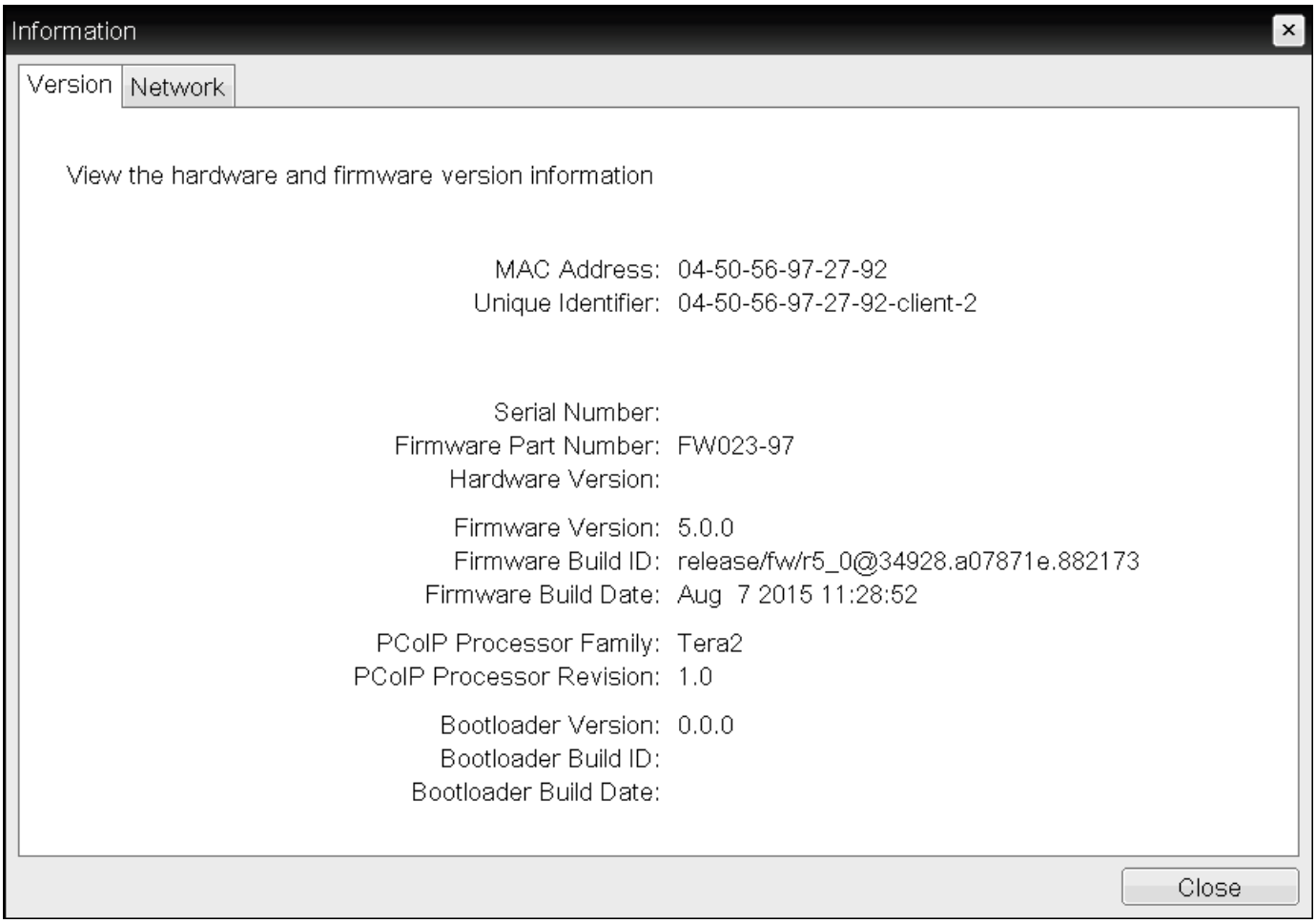
1. From the AWI, select **Info > Attached Devices**.
2. From the AWI ***Attached Devices*** page, view information for the devices attached to your Tera2 PCoIP Zero Client.

Viewing Hardware and Firmware Information

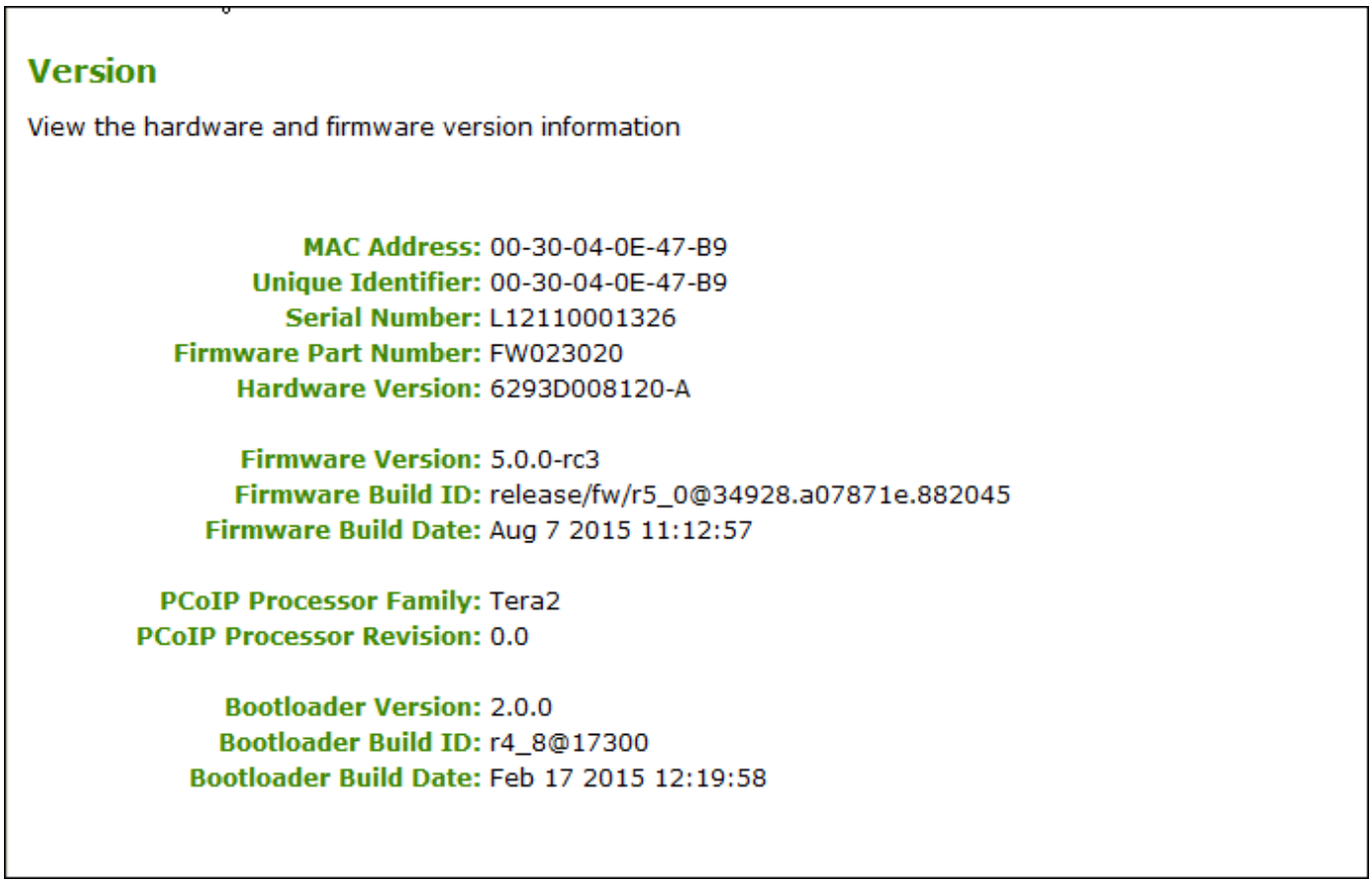
You can view the device's hardware and firmware details from both the OSD and AWI. The information displays on the OSD and AWI Version pages.

Processor information is also available on the AWI Home page

You can view processor and statistical information about your setup from the AWI Home page. For more information about the AWI Home page, see AWI Home Page.



OSD Version page (sample data only)



AWI Version page (sample data only)

The following parameters display on the OSD and AWI Version pages:

Version Parameters

Parameters	Description
VPD Information	(**Vital Product Data**): Information provisioned by the factory to uniquely identify each device: • **MAC Address:** Host/client unique MAC address. • **Unique Identifier:** Host/client unique identifier. • **Serial Number:** Host/client unique serial number. • **Firmware Part Number:** Part number of the current firmware. • **Hardware Version:** Host/client hardware version number.

Parameters	Description
Firmware Information	This information reflects the current firmware details: • **Firmware Version:** Version of the current firmware. • **Firmware Build ID:** Revision code of the current firmware. • **Firmware Build Date:** Build date for the current firmware.
PCoIP Processor Information	This information provides details about the PCoIP processor. • **PCoIP Processor Family:** The processor family (for example, Tera2). • **PCoIP Processor Revision:** The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0.
Bootloader Information	This information reflects the current firmware bootloader details: • **Boatloader Version:** Version of the current bootloader. • **Bootloader Build ID:** Revision code of the current bootloader. • **Bootloader Build Date:** Build date of the current bootloader.

To view hardware and firmware information:

1. Do one of the following:
   - Open the AWI *Home* page.
   - Open the OSD __ page: From the OSD, select **Options > Information > Version**.
   - Open the AWI *Version* page: From the AWI, select **Info > Version**.
2. From the AWI Home page, or the OSD or AWI *Version* pages, view the hardware and firmware information.

Configuring Your PCoIP Zero Client

Using either the OSD or AWI PCoIP Zero Client administrative interfaces, you can configure the PCoIP Zero Client to connect to a variety of hosts under different security requirements. These configurable parameters allow your Zero Client to comply with your company's security policies.

In large secure environments, a management tool such as the PCoIP Management Console is recommended to manage multiple PCoIP endpoints remotely, with the OSD configuration options restricted and the AWI administrative interface disabled. Descriptions of configurable parameters are found in this section of the the PCoIP Zero Client Administrators' Guide while information on how to apply configurations via the PCoIP Management Console are found in the PCoIP Management Console Administrators' Guide.

Configuring Access to Management Tools

Secure Environments

Disable the AWI and use the PCoIP Manamgement Console to configure endpoints in environments that have high security requirements. Consider hiding the OSD for extra security.

Setting	Default	AWI	OSD	Management Console
Disable Management Console Interface	Disabled	✔	✔	✔
Disable Administrative Web Interface	Enabled (FW 6.4+)	✔	✔	✔
Force password change on next login	Disabled	✔	✔	✔
Require password protection for User Settings	Disabled	✔	✖	✔

From the OSD and AWI, you can:

- Prevent a PCoIP administrative tool from managing the PCoIP Zero Client.
- Disable administrative access to the Tera2 PCoIP Zero Client's AWI.
- Force an administrative password change the next time someone accesses the AWI or OSD.

From the AWI only, you can:

- Apply the zero client administrative password to the OSD User Settings.

Do Not Disable all 3 Administrative Interfaces

At least one of the PCoIP Zero Client's three administrative configuration interfaces (OSD, AWI, or PCoIP Management Console) must remain enabled at all times. If you have hidden the OSD Configuration menu using the PCoIP Management Console, and you try to disable both the PCoIP Management Console interface and the AWI, you will receive an error message.

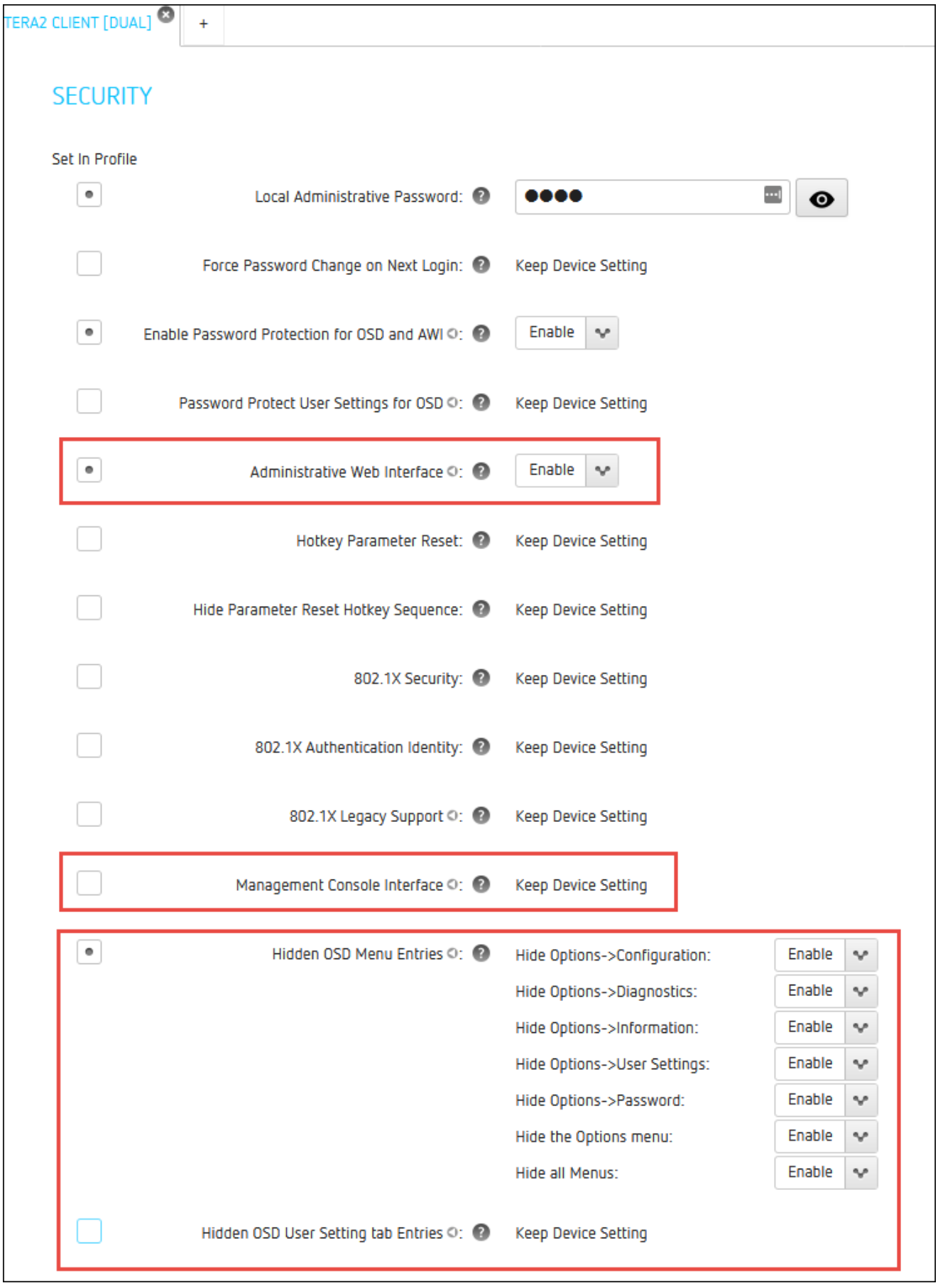
As of firmware 6.4, the Administrative Web Interface is disabled by default. You can enable the AWI by using the OSD or by the PCoIP Management Console.

You can configure administrative access settings from the OSD, AWI Access pages, as well as the PCoIP Management Console. In secure environments, the AWI, OSD, or sections of the OSD may not be available. In these cases, settings must be managed by the PCoIP Management Console if deployed.

For more information on using PCoIP Management Console profiles, see the PCoIP Management Console Adminsitrators' Guide

Configure Administrative Access Settings via the PCoIP Management Console

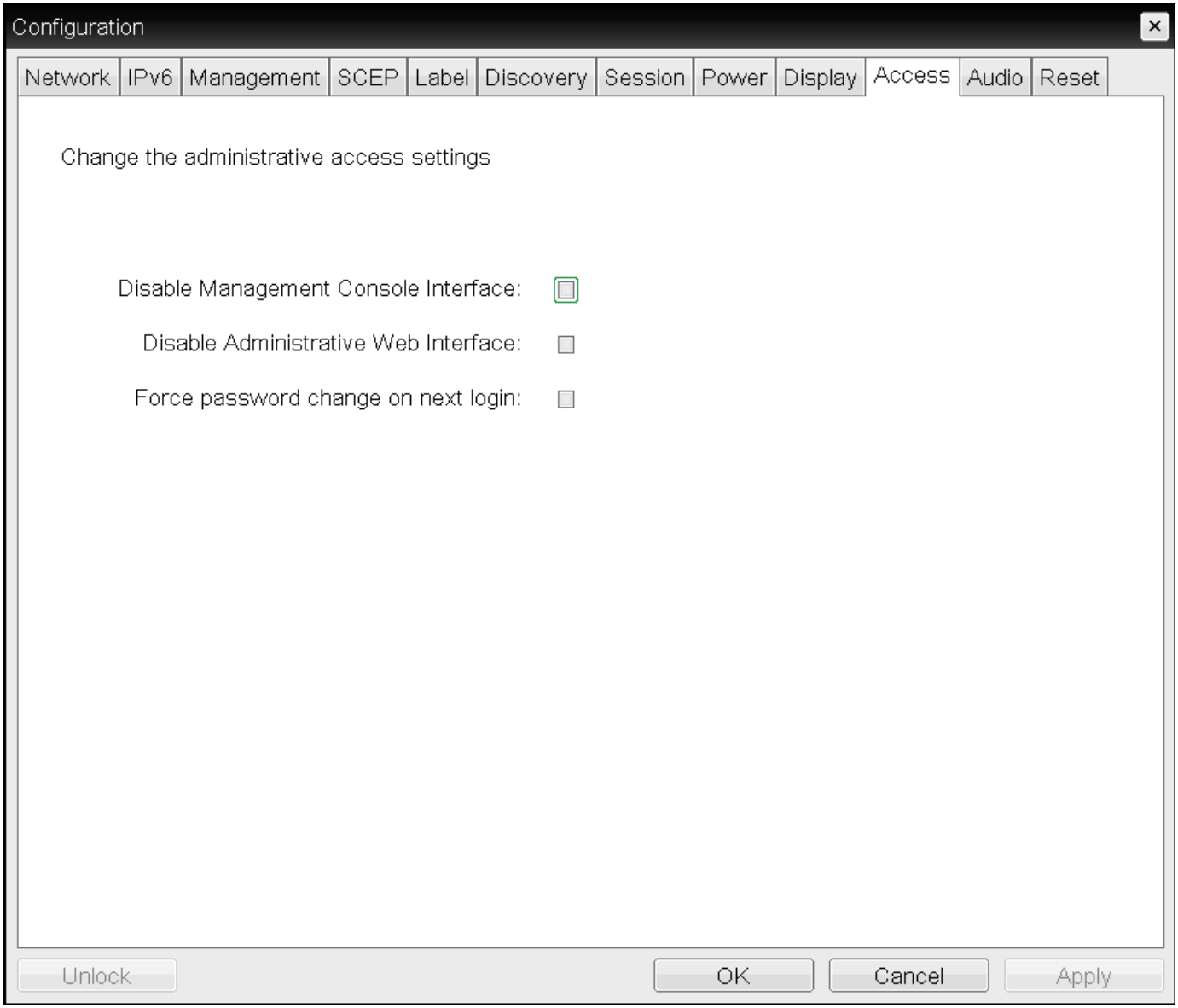
1. Follow your IT security policy and if applicable, configure a new or existing profile to enable the **Administrative Web Interface** or the appropriate parameters of the OSD Menu found in SECURITY section of the PCoIP Management Console profile.



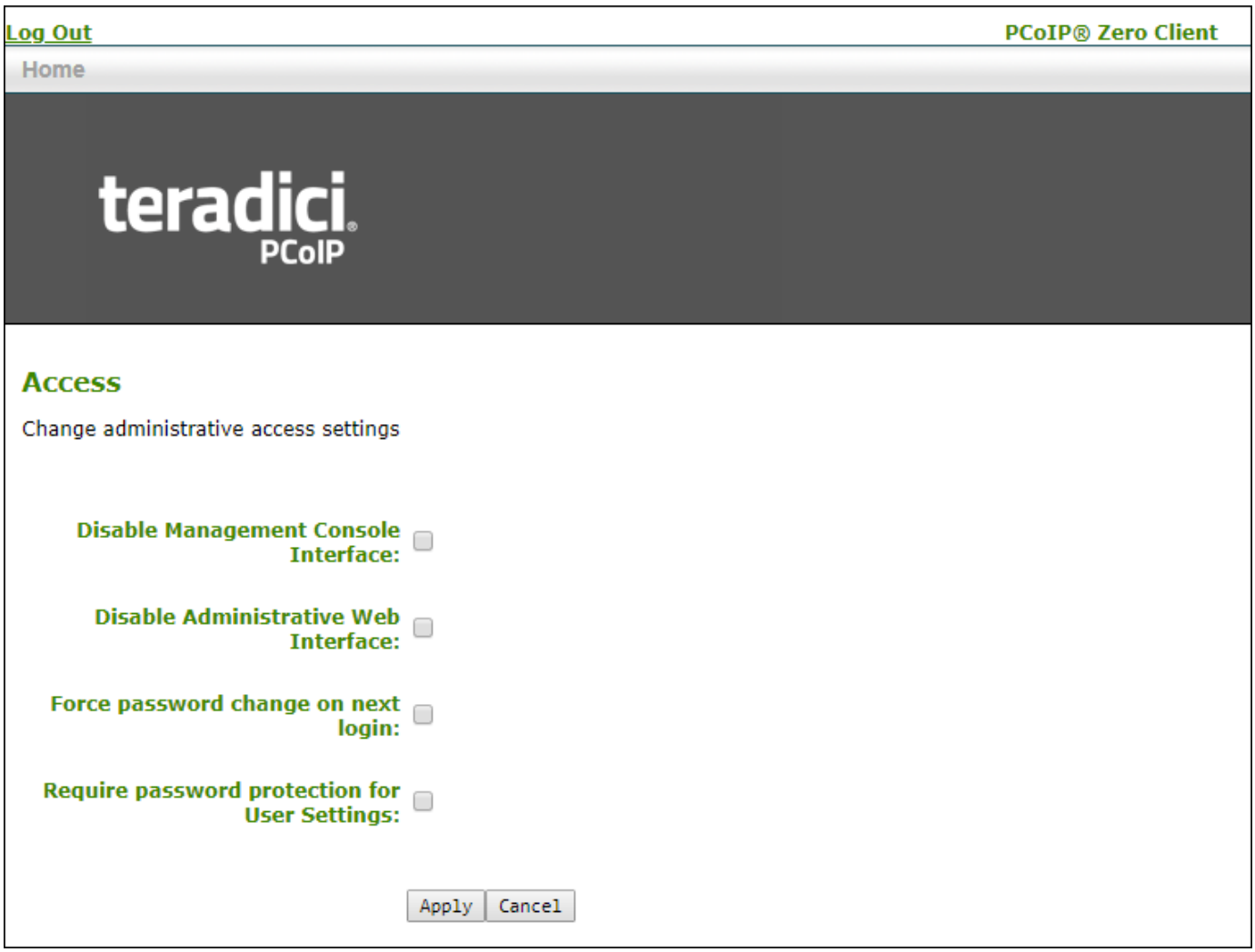
Profile Management Access Settings

2. Apply the profile to your Zero Client.

The following instructions provided consider the case when the AWI is disabled and the OSD is available. The images show that the settings in the OSD and AWI are the same, thus the same instructions apply to changes done via the AWI when it is available. The exception being the OSD does not have **Require password protection for User Settings** and either the AWI or PCoIP Management Console must be used to configure this setting.



OSD Access page



AWI Access page

To Disable or Enable the Administrative Web or PCoIP Management Console Interface

1. From the OSD, select **Options > Configuration > Access**.
2. Uncheck the **Disable Administrative Web Interface:** or **Disable Management Console Interface:** option to enable either interface. When either option is selected, you can't access or manage the Tera2 PCoIP Zero Client using the selected interface.
3. Click **Apply** and then **OK** to save your changes in the OSD.

To Force an AWI Password Change

When this option is selected, a new password is required when you next access your zero client AWI.

1. From the OSD, select **Options > Configuration > Access**.
2. Select the **Force password change on next login:** option.
3. Click **Apply** and then **OK** to save your changes in the OSD.

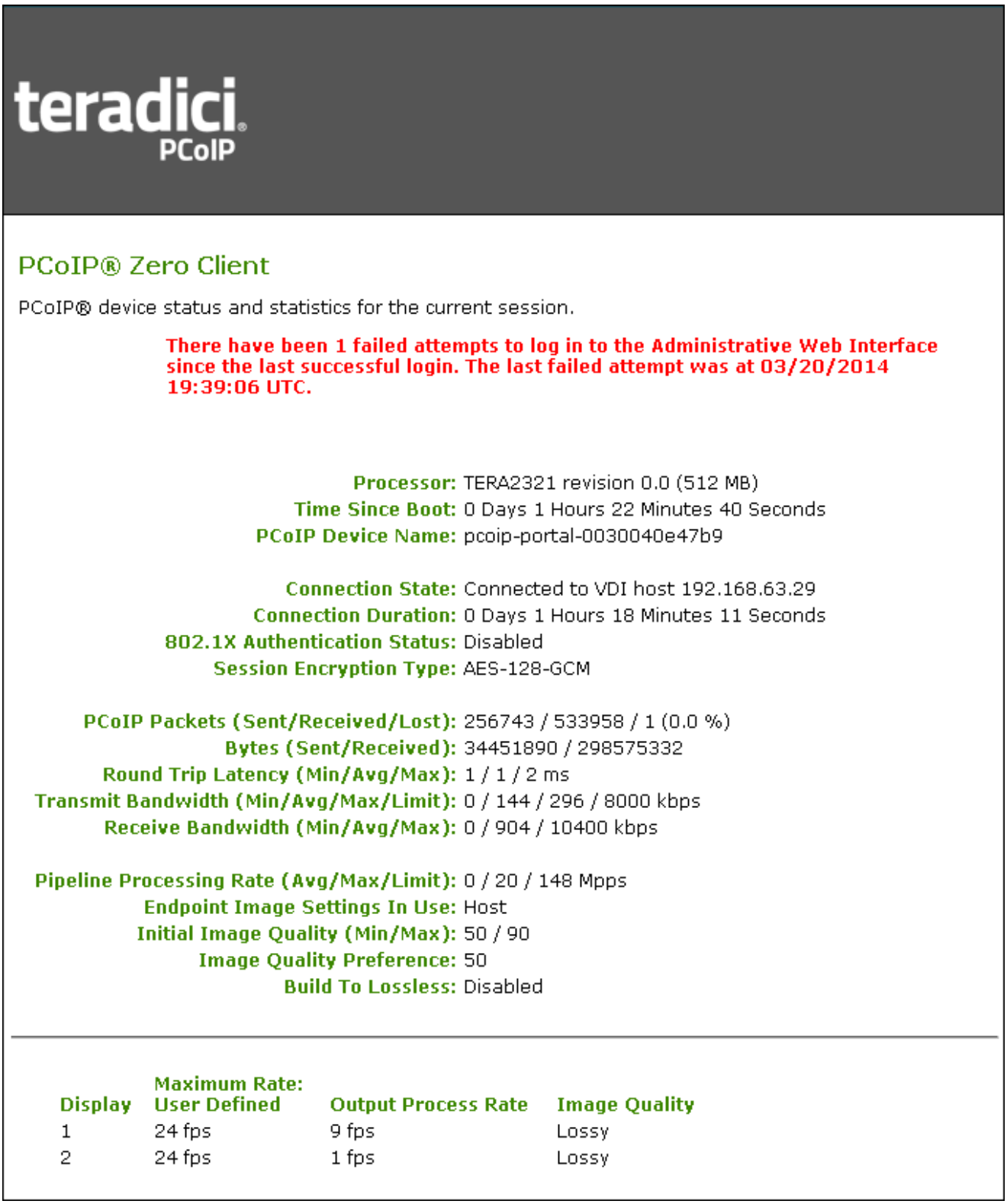
The **Require password protection for User Settings** setting cannot be configured from the OSD therefore the following steps are from the AWI. When **Require password protection for User Settings** is selected, the Zero Client AWI password is required to change any settings located in **OSD > User Settings**.

To Require a Password for OSD User Settings

1. Ensure there is a password applied to the zero client. See Configuring OSD and AWI Password
2. From an enabled AWI, select **Options > Configuration > Access**.
3. Enable the **Require password protection for User Settings** option.
4. Click **Apply** and then **OK** to save your changes in the OSD.

Failed Login Attempt Warning

A warning message displays if any failed access attempts to the AWI or OSD were detected since the last successful login. The message provides the date and time of the failed attempt, as shown next.



Failed login attempt message (from AWI)

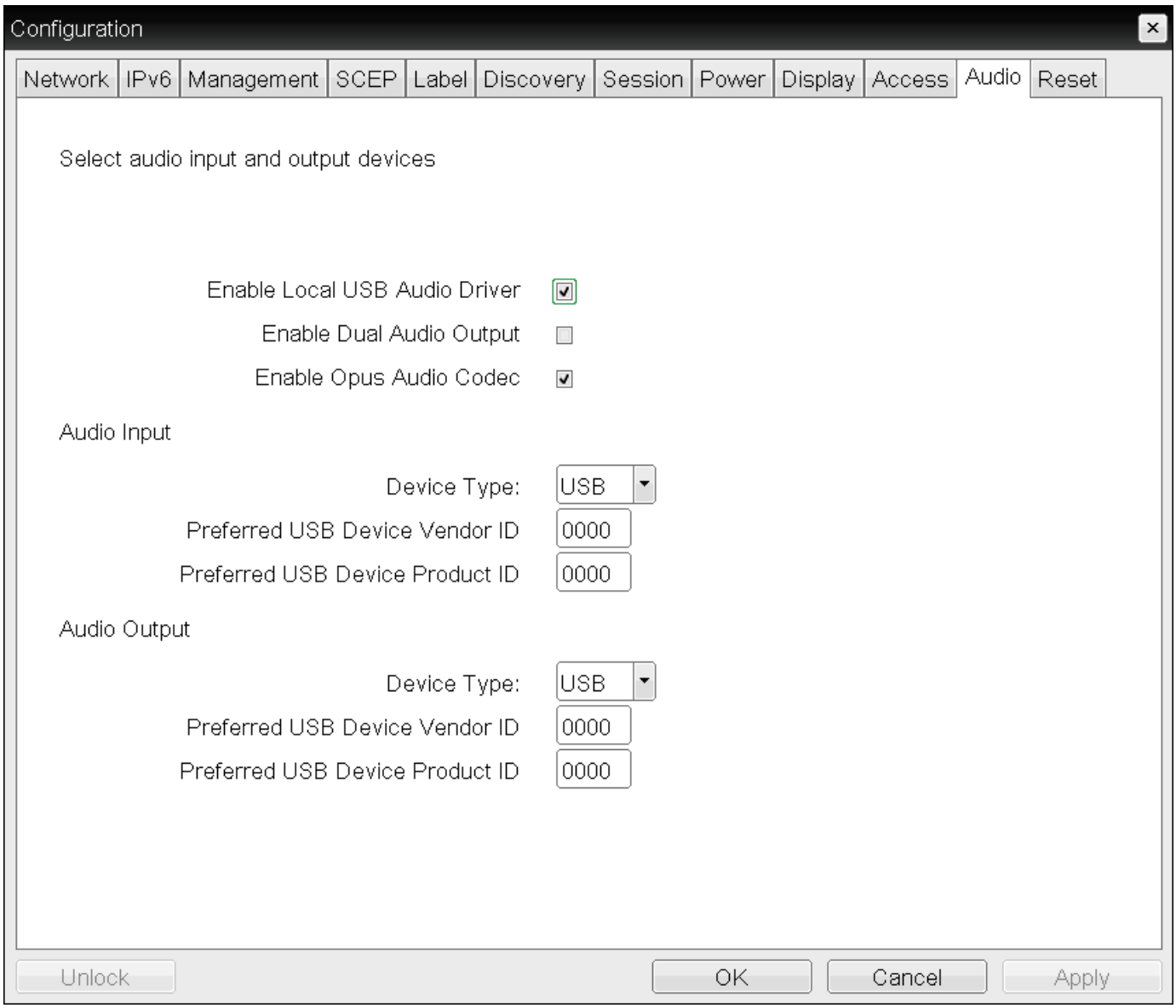
Configuring Audio

Setting	Default	AWI	OSD	Management Console
Enable HD Audio	Disabled	✔	✘	✔
Enable Audio	Enabled	✔	✘	✔
Enable Local USB Audio Driver	Enabled	✔	✔	✔
Enable Dual Audio Output	–	✔	✔	✘
Enable Opus Audio Codec	Enabled	✔	✔	✘
Audio Input				
Device Type	USB	✔	✔	✔
Preferred USB Device Vendor ID	0000	✔	✔	✔
Preferred USB Device Product ID	0000	✔	✔	✔
Attached USB devices	–	✔	✘	✘
Audio Output				
Device Type	USB	✔	✔	✔
Preferred USB Device Vendor ID	0000	✔	✔	✔
Preferred USB Device Product ID	0000	✔	✔	✔
Attached USB devices	–	✔	✘	✘

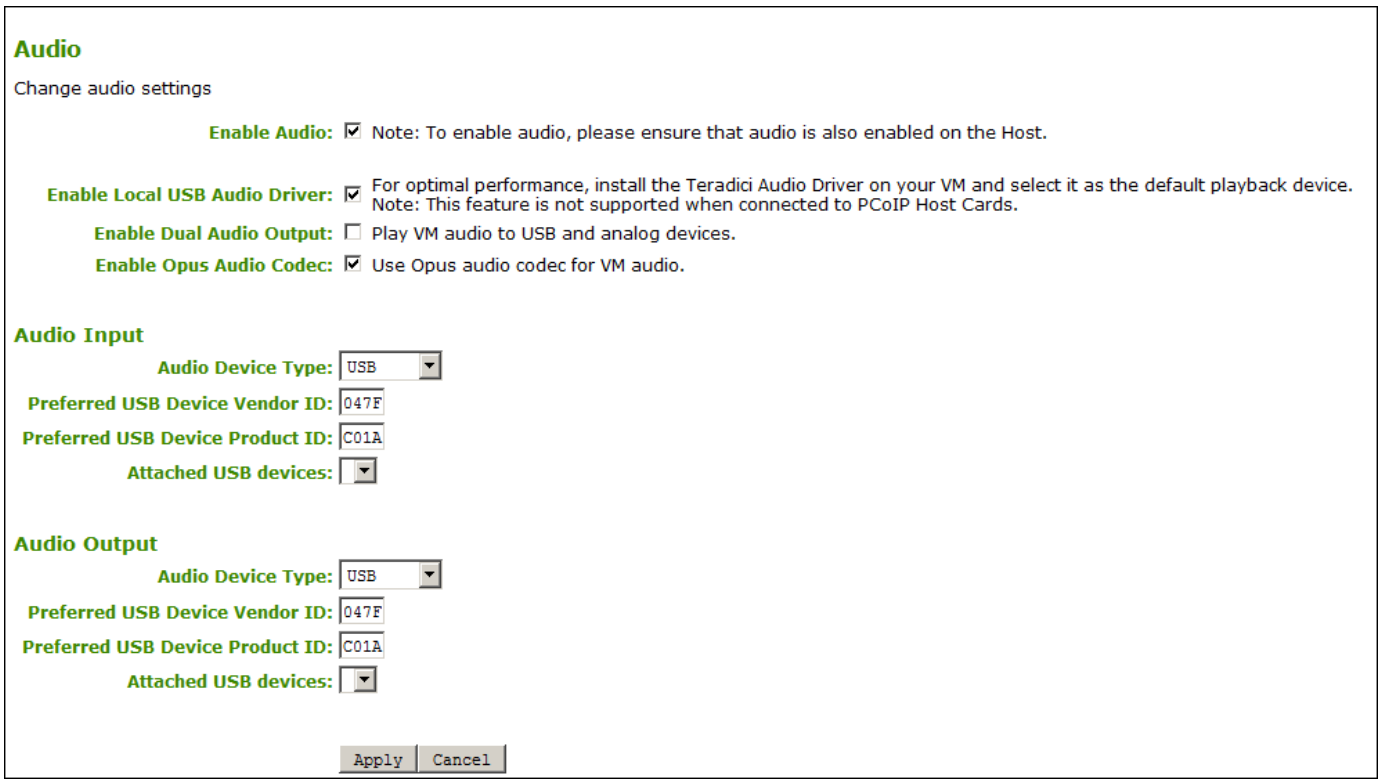
Enabling HD audio

You enable HD audio from the AWI Initial Setup page. To enable HD audio, see Configuring Initial Setup Parameters.

You configure audio parameters from the OSD and AWI ***Audio*** pages (shown next).



OSD Audio page



AWI Audio page

When connected USB audio devices are not available

USB devices can be restricted using the USB permissions tables. If your USB device does not appear as a selectable device check your USB permissions configurations.

The following parameters display on the OSD and AWI Audio pages:

Audio Parameters

Category	Parameter	Description
Audio		
	Enable Audio (AWI only)	When enabled, configures audio support on the device. This property must be enabled on both the host and the client. When disabled, the audio hardware is not available for the host operating system to enumerate.

Category	Parameter	Description
	Enable Local USB Audio Driver	This option locally terminates any USB audio devices that are attached to the Tera2 PCoIP Zero Client. When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience. When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions. For bi-directional audio support (for example, microphone as well as playback), the Teradici Audio Driver must be installed on your VM and selected as the default playback device. **Caution:** If you use a USB composite device that contains audio functionality but also has one or more functions that must be bridged (that is, terminated remotely so the host OS can install the driver), you can't use the local USB audio driver for the device.
	Enable Dual Audio Output	When enabled, all VM audio is sent to both an external speaker and a USB headset.
	Enable Opus Audio Codec	When enabled, the Opus audio codec is used for audio output from software hosts to clients if supported by the host.
Audio Input		The options in this section enable you specify the preferred device to use for audio input (recording). The options are available when you select **Enable Local USB Audio Driver**.

Category	Parameter	Description
	Audio Device Type	This field applies when you enable the **Enable Local USB Audio Driver** option and both an analog input device and a USB input device are connected to the Tera2 PCoIP Zero Client. Since you can only use one audio device at a time when devices are locally terminated, select the type of device you want to use: • **Analog:** The analog input device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio recording. • **USB:** The USB input device attached to the Tera2 PCoIP Zero Client will be used for audio recording. If more than one is attached, the Audio Input options let you specify the preferred one to use.
	Preferred USB Device Vendor ID	This field is automatically populated with the USB device's vendor ID (VID) after you select the preferred audio input device in the **Attached USB devices** list and apply your changes. You can also manually enter the VID of the preferred attached USB device. This option doesn't apply to analog audio devices.
	Preferred USB Device Product ID	This field is automatically populated with the USB device's product ID (PID) after you select the preferred audio input device in the **Attached USB devices** drop-down list and apply your changes. You can also manually enter the PID of the preferred attached USB device. This option does not apply to analog audio devices.
	Attached USB devices (AWI only)	In the list, select the preferred USB device to use for audio input. This option doesn't apply to analog audio devices.
Audio Output		The options in this section enable you to specify the preferred device to use for audio output (playback). The options are available when you select **Enable Local USB Audio Driver**.

Category	Parameter	Description
	Audio Device Type	This field applies when you enable the **Enable Local USB Audio Driver** option and both an analog output device and a USB output device are connected to the Tera2 PCoIP Zero Client. Since you can use only one audio device at a time when devices are locally terminated, select the type of device you want to use: • **Analog:** The analog output device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio playback. • **USB:** The USB output device attached to the Tera2 PCoIP Zero Client will be used for audio playback. If more than one is attached, the Audio Output options enable you specify the preferred one to use.
	Preferred USB Device Vendor ID	This field is automatically populated with the USB device's vendor ID (VID) after you select the preferred audio output device in the **Attached USB devices** list and apply your changes. You can also manually enter the VID of the preferred attached USB device. This option doesn't apply to analog audio devices.
	Preferred USB Device Product ID	This field is automatically populated with the USB device's product ID (PID) after you select the preferred audio output device in the Attached USB devices drop-down list and apply your changes. You can also manually enter the PID of the preferred attached USB device. This option doesn't apply to analog audio devices.
	Attached USB devices (AWI only)	In the list, select the preferred USB device to use for audio output.

To configure audio settings:

1. Open the Audio page:
   - From the OSD, select **Options > Configuration > Audio**.
   - From the AWI, select **Configuration > Audio**.
2. From the OSD or AWI Audio page, update the audio settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Certificate Checking Mode

Setting	Default	AWI	OSD	Management Console
Certificate Checking Mode	Warn before connecting to untrusted servers	✗	✓	✓
Certificate Check Mode Lockout	Disabled	✓	✗	✓

The ***Certificate Checking Mode*** option configures how the Tera2 PCoIP Zero Client behaves if it can't verify a secure connection to the server. You configure this setting from the OSD. To configure this setting, see Setting Certificate Checking Mode.

Enabling the ***Certificate Check Mode Lockout*** option prevents users from changing the Certificate Checking Mode option on the OSD. You enable this option from the advanced settings for any of the following session types:

- Amazon WorkSpaces
- PCoIP Connection Manager
- View Connection Server

Configuring Discovery

Setting	Default	AWI	OSD	Management Console
Internal Endpoint Manager URI	–	✔	✘	✔
External Endpoint Manager URI	–	✔	✘	✔
Manager Discovery Mode	Automatic	✔	✘	✔
Endpoint Bootstrap Manager URI	–	✔	✘	✘
Enable Discovery	Enabled	✘	✔	✔
Enable SLP Discovery	Disabled	✔	✘	✔
Enable DNS-SRV Discovery	Enabled	✔	✘	✔
DNS-SRV Discovery Delay	300	✔	✘	✔

You can configure discovery settings from the AWI and OSD ***Management*** and ***Discovery*** pages.

The AWI and OSD ***Management*** pages contain information about how the Tera2 PCoIP Zero Client is discovered by an endpoint manager. The discovery can be automatic or manual, and initiated either by the endpoint manager or the Tera2 PCoIP Zero Client.

From the AWI and OSD Discovery pages, you can enable Service Location Protocol (SLP) management entities to discover devices dynamically without requiring prior knowledge of their locations in the network. You can also enable DNS SRV discovery to enable and configure discovery settings for connection brokers.

Detailed information about discovery methods

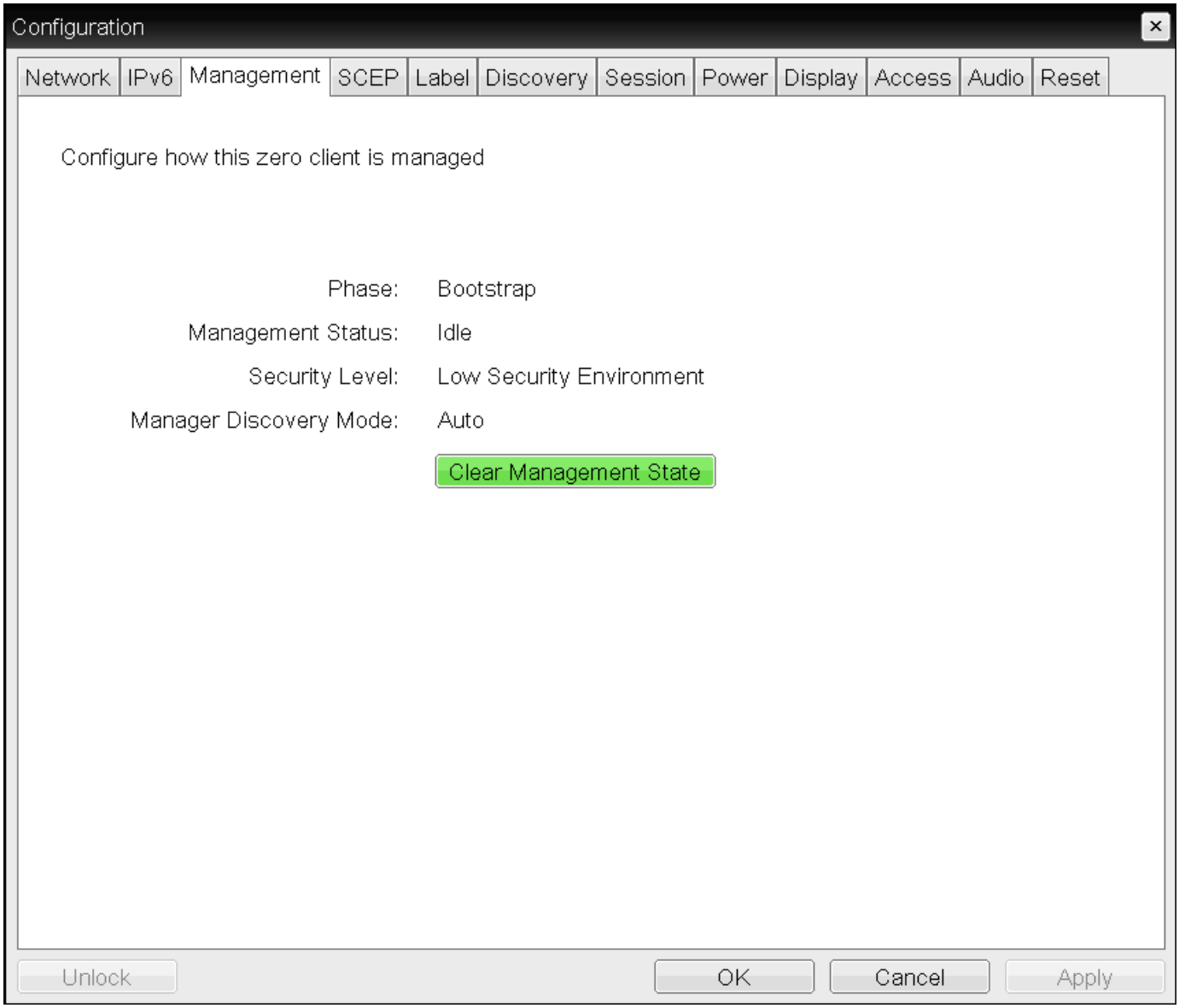
For detailed information about discovery methods, see Connecting to an Endpoint Manager.

Viewing Discovery Information

From the OSD *MANAGEMENT* page (shown next), you can view the discovery mode.

Clearing the Tera2 PCoIP Zero Client's management state

From the Management page, you also have the option to remove the current endpoint manager information for the client. To clear the management information, see Clearing the Management State.



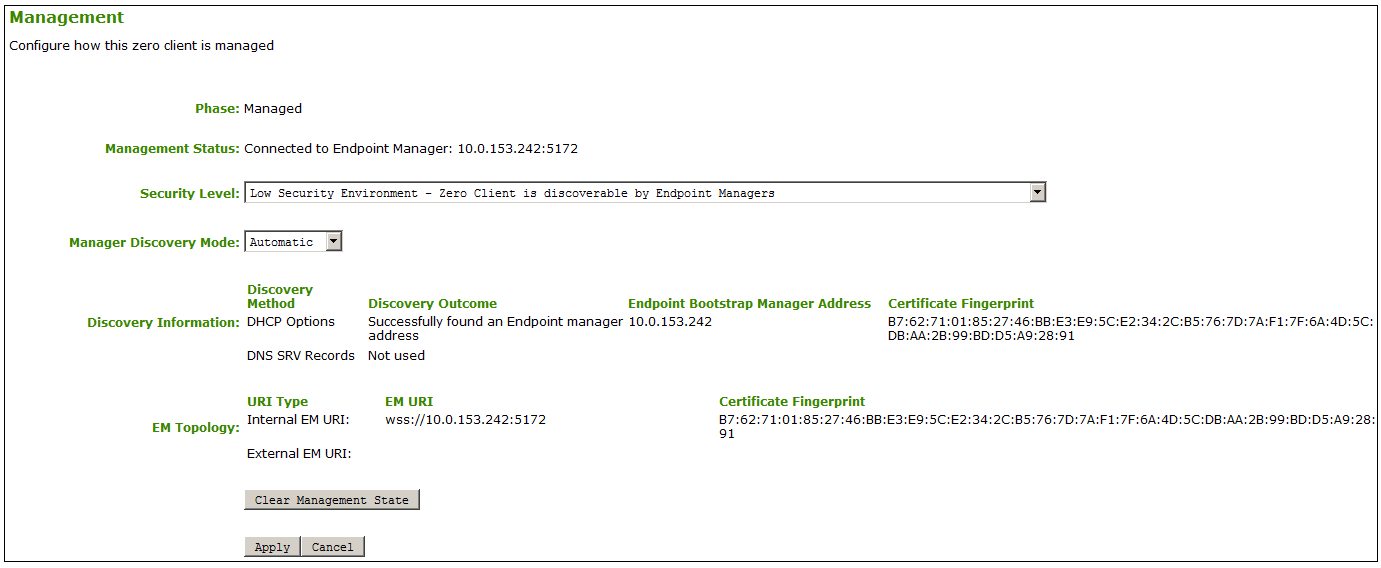
OSD Management page

To view discovery information:

1. From the OSD, select **Configuration > Management**.
2. From the OSD *Management* page, view the *Manager Discovery Mode* setting. The setting will be one of the following:
   - **Automatic:** When this option is set, the client attempts to receive the Endpoint Bootstrap Manager connection information from a DHCP server or DNS server.
   - **Manual:** When this option is set, the user provisions the Endpoint Bootstrap Manager in the **Endpoint Bootstrap Manager URI** field.
3. Click **OK**.

Configuring the Discovery Method

Using the AWI *Management* page (shown next), you can configure the discovery method to use. The information that displays on the page depends on whether the client uses automatic or manual discovery.



AWI Management page – automatic discovery mode

AWI Management page – manual discovery mode

The following discovery parameters display on the AWI Management page:

Discovery Parameters

Parameter	Description
Internal Endpoint Manager URI	This field displays when the security level is set to **High Security Environment - Bootstrap phase disabled**. Enter the URI for the internal Endpoint Manager using the following format, and click **Apply**: `wss://<internal EM IP address/FQDN>:[port number]` This URL requires a secured WebSocket (wss://) prefix. The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.

Parameter	Description
External Endpoint Manager URI (optional)	This optional field displays the security level is set to **High Security Environment - Bootstrap phase disabled**. If the client is unable to connect to the internal Endpoint Manager, it will attempt to connect to the external Endpoint Manager if this field is configured. If desired, enter the URI for the external Endpoint Manager using the following format, and click **Apply**: `wss://<external EM IP address/FQDN>:[port number]` **This URL requires a secured WebSocket (wss://) prefix**. The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.
Manager Discovery Mode	Select the correct discovery mode: • **Automatic:** When this option is set, the client attempts to receive the Endpoint Bootstrap Manager connection information from a DHCP server or DNS server. • **Manual:** When this option is set, the user provisions the Endpoint Bootstrap Manager in the **Endpoint Bootstrap Manager URI** field.
Discovery Information	When ***Manager Discover Mode*** is set to Automatic, this section displays the device discovery method your system is using. • **Discovery Method:** Displays the type of automatic discovery mechanism your system is configured to use (for example, PCoIP Management Console DNS SRV record discovery, DHCP vendor-specific options discovery). • **Discovery Outcome:** Displays the discovery result for the configured discovery methods. • **Endpoint Bootstrap Manager Address:** If the client has been discovered using one of the discovery methods, displays the IP address for the Endpoint Bootstrap Manager. • **Certificate Fingerprint:** Displays the certificate fingerprint (that is, the certificate's digital signature) that was used to authenticate the Endpoint Bootstrap Manager.

Parameter	Description
Endpoint Manager Topology	When the client has been automatically discovered by an Endpoint Manager, this section displays information about the connection. If the client used manual discovery, this information does not display. • **URI Type:** Displays whether the client is connected to an internal Endpoint Manager or an external one. • **Endpoint Manager URI:** Displays the URI (uniform resource identifier) for the Endpoint Manager the client is currently using. • **Certificate Fingerprint:** Displays the certificate fingerprint (digital signature) that was used to authenticate the Endpoint Manager.
Endpoint Bootstrap Manager URI	This field displays when the discovery mode is set to **Manual**. Enter the URI for the Endpoint Bootstrap Manager the client will connect to for bootstrap information using the following format, and click **Apply**: `wss://<EBM IP address/FQDN>:[port number]` **This URL requires a secured WebSocket (wss://) prefix.** The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.

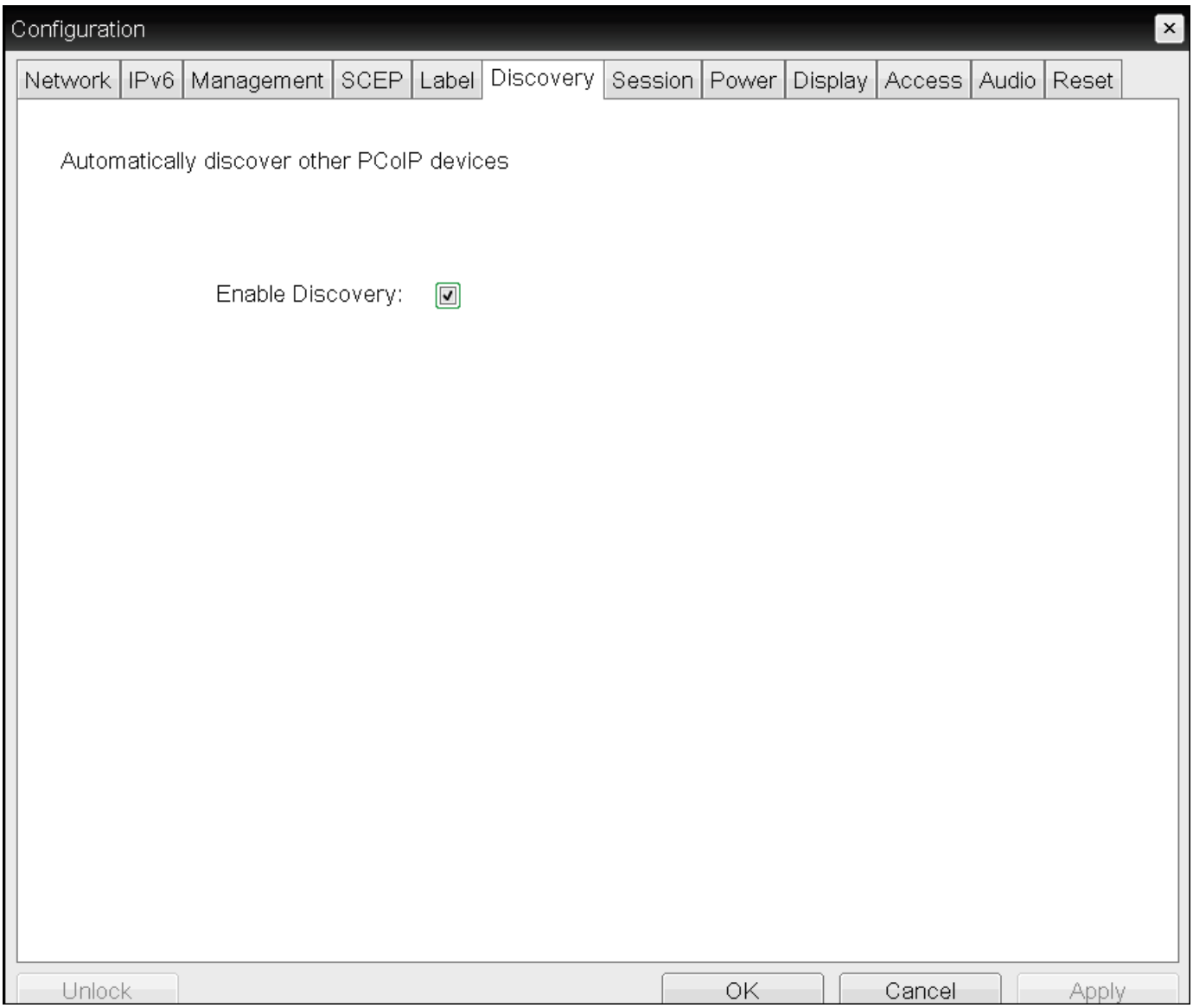
Configuring SLP Discovery

Enable Service Location Protocol (SLP) discovery so that SLP management entities can dynamically discover devices without requiring prior knowledge of their network configuration.

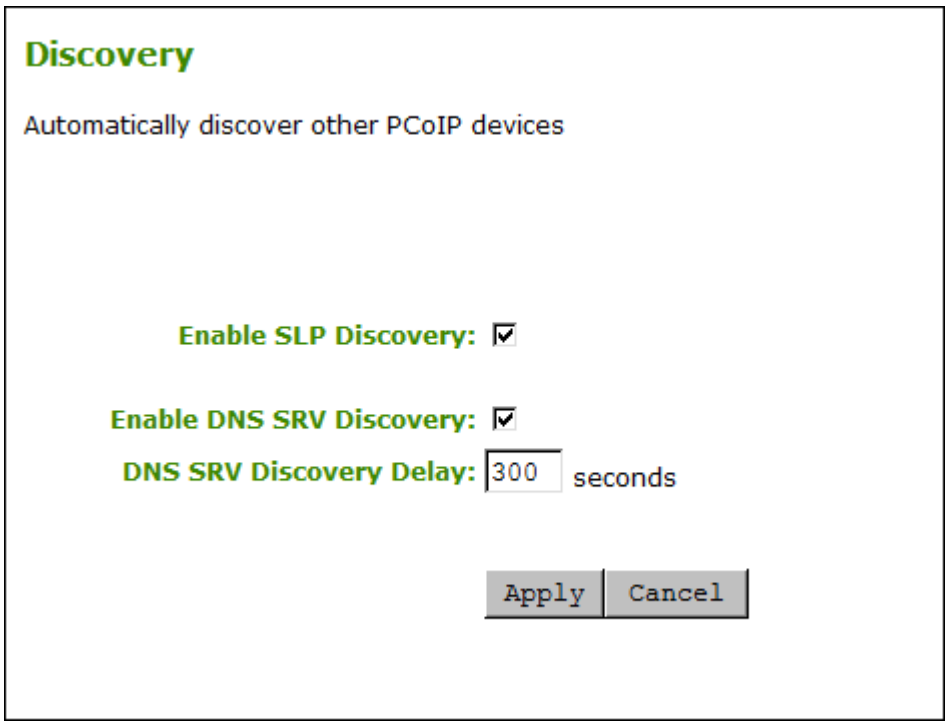
Devices must reside on the same subnet

- Teradici recommends configuring DHCP Vendor Class Options directly in the DHCP server to discover PCoIP endpoints
- SLP discovery requires all PCoIP devices to reside on the same network subnet. For SLP discovery to work across subnets, you must configure routers to forward multicast traffic between subnets.

You enable SLP discovery from the OSD and AWI Discovery pages, shown next:



OSD Discovery page



AWI Discovery page

To enable SLP discovery:

1. Open the *Discovery* page:
   - From the OSD, select **Options > Configuration > Discovery**.
   - From the AWI, select **Configuration > Discovery**.
2. From the *Discovery* page, enable SLP discovery so that SLP management entities can dynamically discover devices. Do one of the following:
   - From the OSD, select **Enable Discovery**.
   - From the AWI, select **Enable SLP Discovery**.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring DNS-SRV Discovery for Connection Brokers

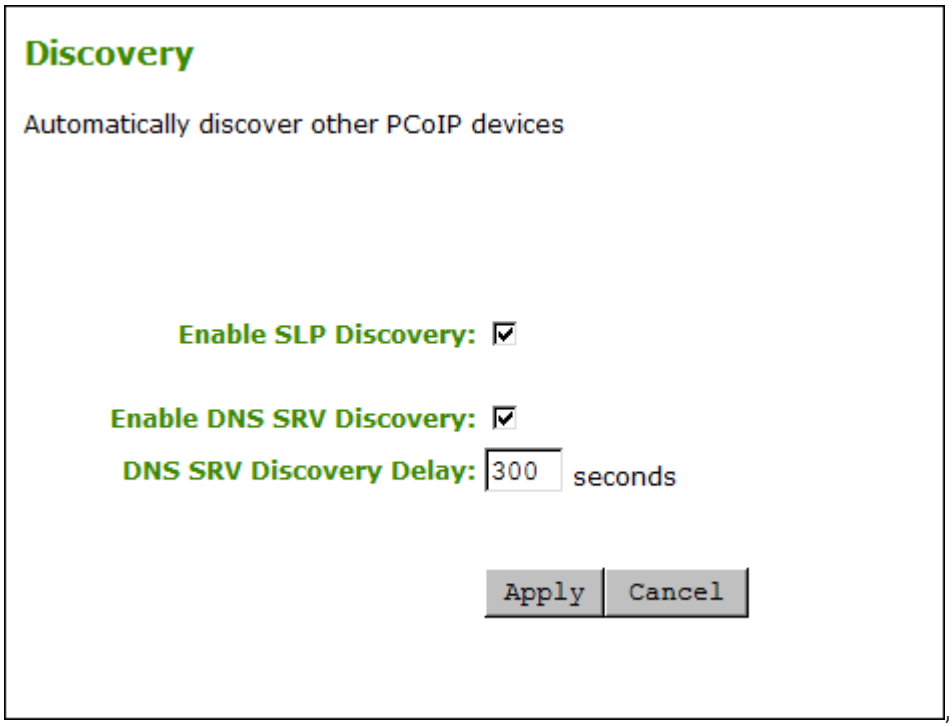
Enable DNS-SRV discovery for connection brokers so that:

- A device can automatically advertise itself to a connection broker without the broker having prior knowledge of the device's whereabouts on the network.
- The device can download and use the DNS SRV record from the DNS server.

Enabling DNS SRV Discovery option configures the discovery for connection brokers

The *Enable DNS SRV Discovery* option configures discovery for connection brokers, but doesn't affect DNS SRV functionality for the PCoIP Management Console.

You enable DNS-SRV discovery for connection brokers from the AWI Discovery page, shown next. From this page, you can also configure the delay between the DNS SRV discovery attempts for connection brokers and the PCoIP Management Console. DNS SRV discovery continues periodically until the device successfully contacts a connection management server.



AWI Discovery page

To configure DNS-SRV discovery for connection brokers:

1. From the AWI, select **Configuration > Discovery**. The *Discovery* page displays.
2. Select or clear **Enable DNS SRV Discovery.** When enabled, devices automatically advertise themselves to a connection broker, and download and use the DNS SRV record from the DNS server.
3. For *DNS SRV Discovery Delay*, enter the amount of time (in seconds) between DNS SRV discovery attempts between connection brokers and the PCoIP Management Console.

> **DNS SRV Discovery Delay and the PCoIP Management Console**
>
> The Enable DNS SRV option doesn't affect the DNS SRV functionality for the PCoIP Management Console; however, the DNS SRV Discovery Delay option does. When DNS SRV records are not installed, it is recommended that you set the delay to the maximum value of **9999**. This minimizes attempts by the client to contact the PCoIP Management Console.

4. To save your updates, click **Apply**.

Clearing the Management State

Setting	Default	AWI	OSD	Management Console
Clear Management State (a button)	–	✔	✔	✔

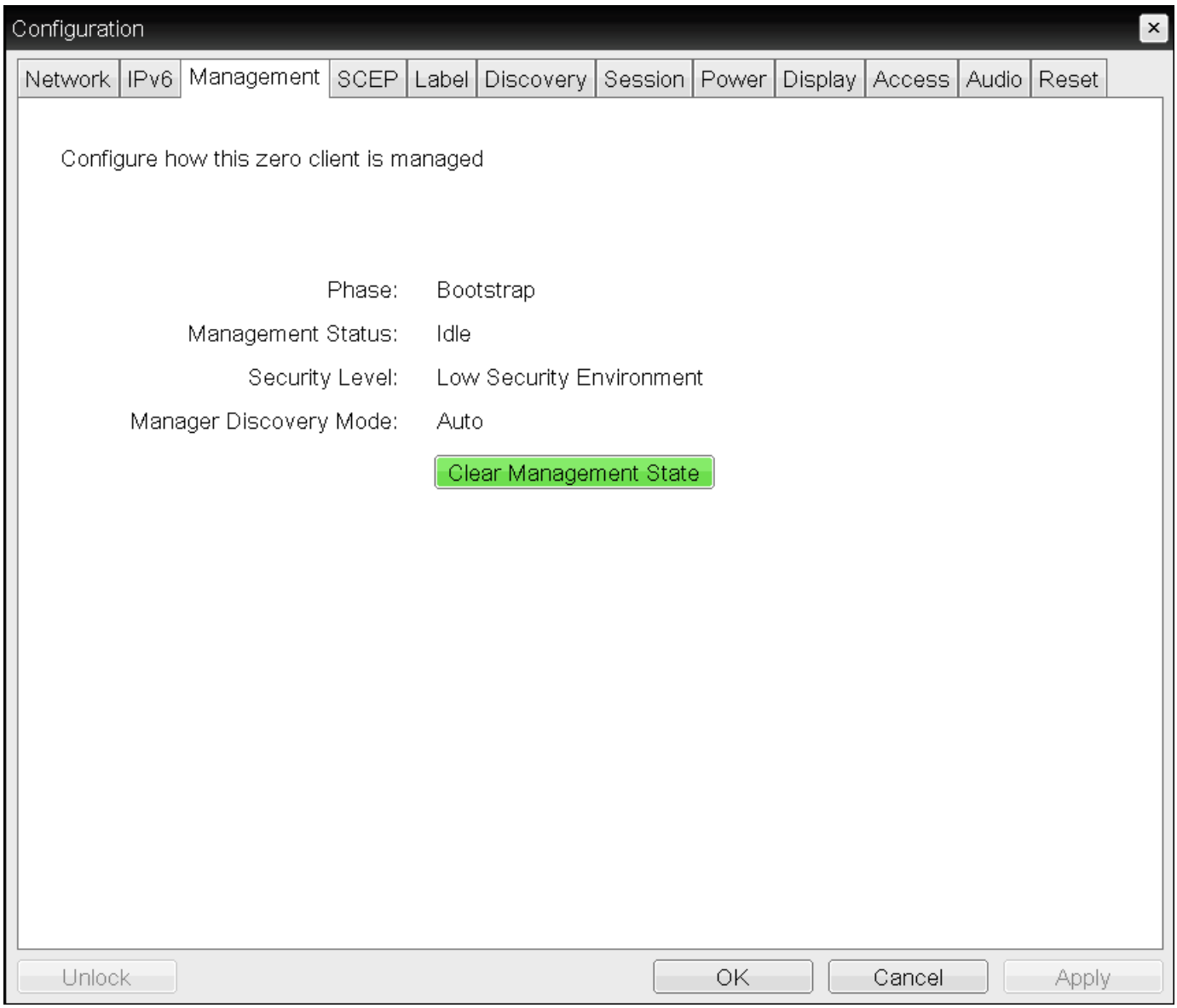
From the AWI and OSD, you can clear the Tera2 PCoIP Zero Client's management state.

Clearing the management state removes the current endpoint manager information for the client. Once the client is managed by an endpoint manager, you must clear its management state before the client can accept a new endpoint manager.

You clear the management state from the AWI and OSD ***Management*** pages, shown next.

Discovery settings determine what displays on the AWI Management page

The information that displays on the AWI Management page depends on whether the client uses automatic or manual discovery.



OSD Management page

AWI Management page – automatic discovery mode

AWI Management page – manual discovery mode

To clear the management state:

1. From the OSD or AWI, select **Configuration > Management**.
2. From the OSD or AWI Management page, click **Clear Management State** so that the endpoint will accept a new endpoint manager.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring a Quad Display Topology

Setting	Default	AWI	OSD	Management Console
Enable Configuration	–	✗	✓	✓
Layout	–	✗	✓	✓
Alignment	–	✗	✓	✓
Primary/Position/Rotation/Resolution	–	✗	✓	✓

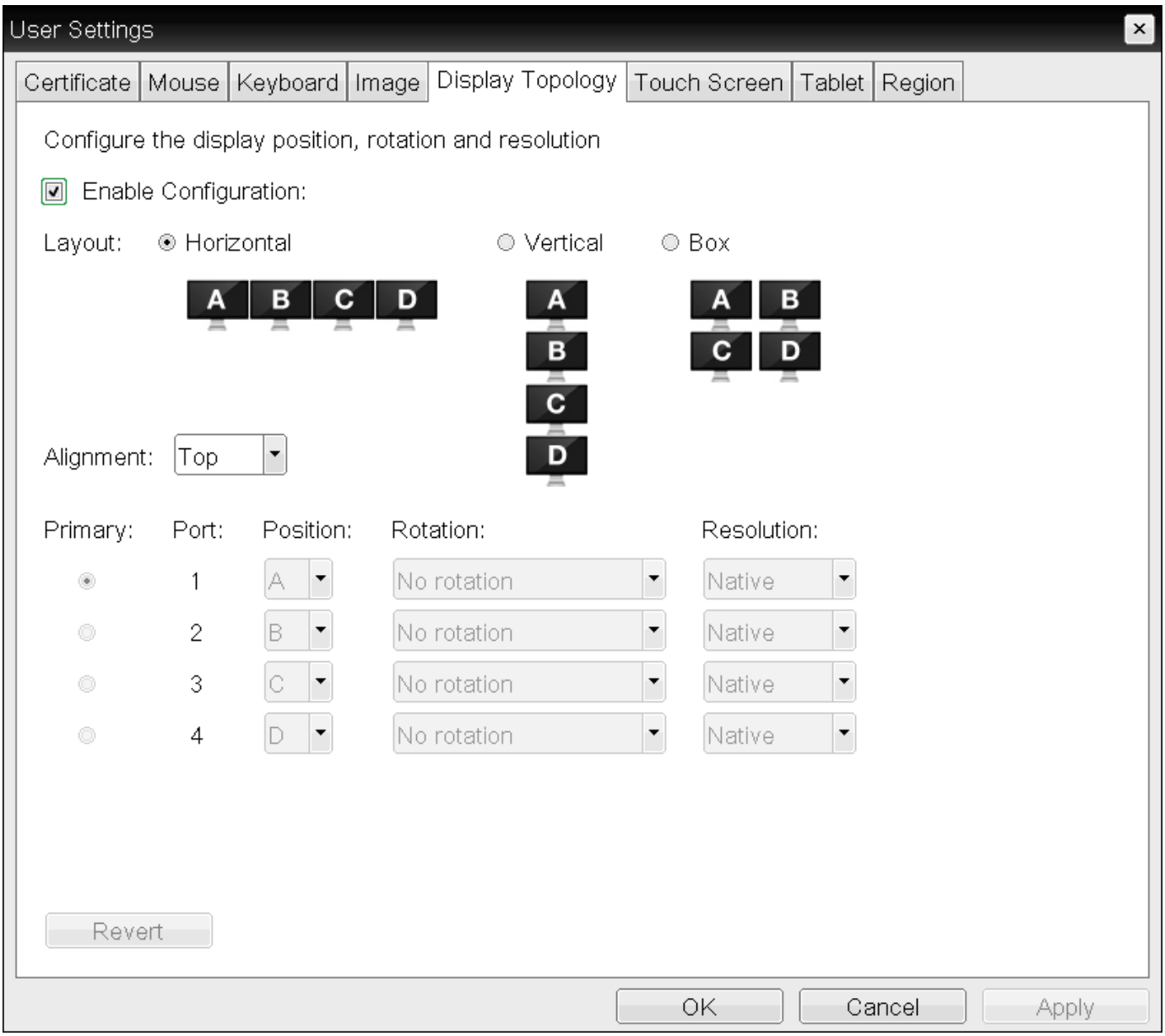
The Display Topology page lets users change the display topology for a PCoIP session.

Before applying the display topology feature to a PCoIP session

To apply the display topology feature to a PCoIP session between a client and a VMware Horizon virtual desktop, you must have VMware View 4.5 or higher. To apply the display topology feature to a PCoIP session between a client and a PCoIP Remote Workstation Card, you must have the Remote Workstation Card Software installed on the host.

Use the OSD, rather than Windows Display Settings, to change display topology settings

Always change the display topology settings using this OSD Display Topology page. Do not try to change these settings using the Windows Display Settings in a virtual machine when using VMware View.



OSD Quad-display Topology page

The following parameters can be found on the OSD Quad-display Topology page.

OSD Quad-display Topology Parameters

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.

Parameter	Description
Display Layout	Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk. • **Horizontal:** Select to arrange displays horizontally, as indicated in the diagram. • **Vertical:** Select to arrange displays vertically, as indicated in the diagram. • **Box:** Select to arrange displays in a box formation, as indicated in the diagram.
Alignment	Select how you want displays aligned when they are different sizes. This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout:** • **Top:** Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center:** Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom:** Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout:** • **Left:** Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center:** Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right:** Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.

Parameter	Description
Primary	Configure which video port on the Tera2 PCoIP Zero Client that you want as the primary port. The display that is connected to the primary port becomes the primary display (that is, the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1:** Select to configure port 1 on the Tera2 PCoIP Zero Client as the primary port. • **Port 2:** Select to configure port 2 on the Tera2 PCoIP Zero Client as the primary port. • **Port 3:** Select to configure port 3 on the Tera2 PCoIP Zero Client as the primary port. • **Port 4:** Select to configure port 4 on the Tera2 PCoIP Zero Client as the primary port.
Position	Specify which display is physically connected to each port.
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a Tera2 PCoIP Zero Client. The Tera2 PCoIP Zero Client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

To configure display settings:

1. From the OSD, select **Options > User Settings > Display Topology**.
2. From the OSD *Display Topology* page, update the settings for the attached displays.
3. Click **OK**.

Configuring IPv4 Network Settings

Setting	Default	AWI	OSD	Management Console
Enable DHCPv4	Enabled	✔	✔	✔
IP Address	–	✔	✔	✖
Subnet Mask	–	✔	✔	✖
Gateway	–	✔	✔	✖
Primary DNS Server	–	✔	✔	✖
Secondary DNS Server	–	✔	✔	✖
Domain Name	–	✔	✔	✖
FQDN	–	✔	✔	✖
Ethernet Mode	Auto	✔	✔	✖
Maximum MTU Size	1200 bytes	✔	✖	✔
Enable 802.1X security	–	✔	✔	✔
Identity	–	✔	✔	✔
Authentication	TLS	✔	✖	✖
Client Certificate	–	✔	✔	✔
Enable 802.1X Support for Legacy Switches	–	✔	✖	✔

From the OSD and ***AWI Network*** pages, you can manually configure network settings if DHCP is disabled, as well as configure 802.1X security to ensure that only authorized devices access the network.

The Static Fallback Network Configuration

The PCoIP Zero Client has a default static fallback configuration that is applied if enabled and a DHCP server is not found on the network. The specific configuration can be different for different brand names of PCoIP Zero Clients. This configuration can be disabled or enabled, and configured through the Management Console. The configurable settings are found in the NETWORK category of a profile when IPv4 is enabled and DHCPv4 is disabled. The configurable settings are:

- Static Fallback IPv4 Address: The IPv4 address applied to the zero client when a DHCPv4 server is not reached.
- Static Fallback IPv4 Subnet Mask: The IPv4 subnet mask applied to the zero client when a DHCPv4 server is not reached.
- Static Fallback IPv4 Gateway: The IPv4 gateway address applied to the zero client when a DHCPv4 server is not reached.
- Static Fallback IPv4 Timeout: The time it takes before the static fallback configuration is applied.

From the OSD and AWI, you can also configure IPv6 network settings. To configure IPv6 settings, see Configuring IPv6 Network Settings.

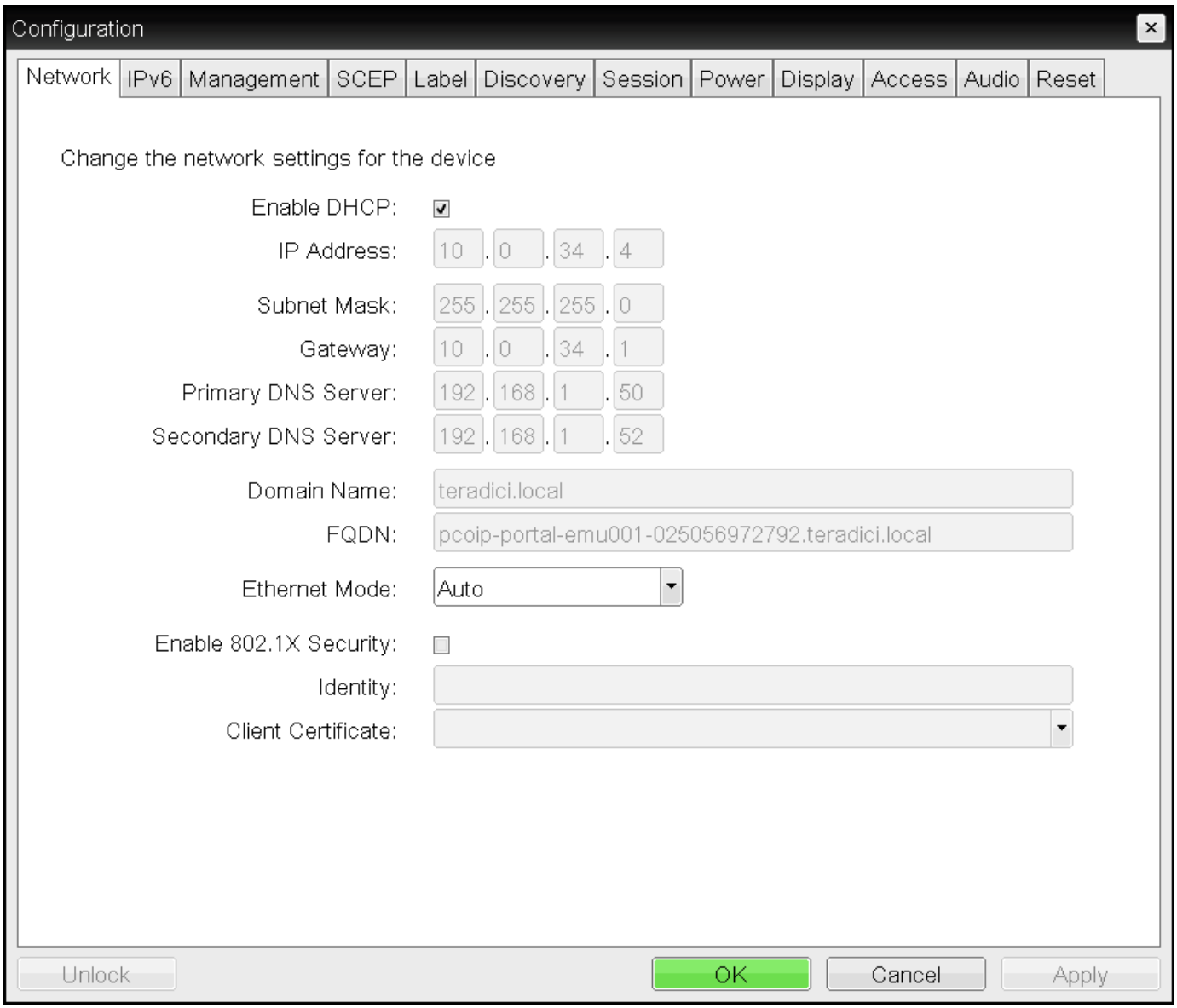
You can also configure a subset of network settings from the AWI Initial Setup page.

You can also configure network settings (DHCP, IP address, subnet mask, gateway, and primary and secondary DNS servers) from the AWI Initial Setup page. To configure network settings from this page, see Configuring Initial Setup Parameters.

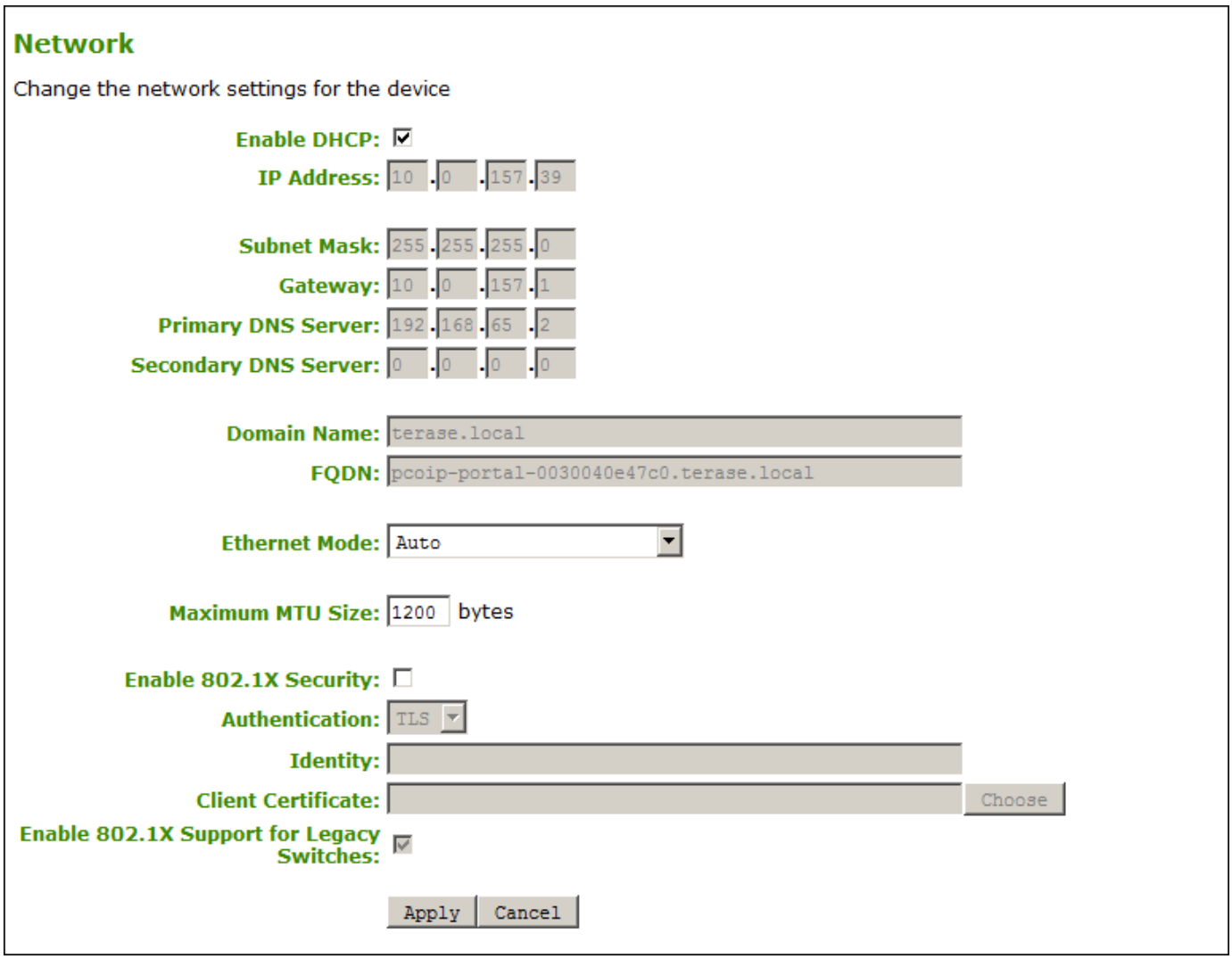
Setting up 802.1X authentication

For a description of all the components you need to configure 802.1X authentication, as well as the detailed steps you need to follow to configure the authentication, see Configuring 802.1X Network Device Authentication.

You configure network settings from the OSD and AWI Network pages (shown next).



OSD Network page



AWI Network page

The following parameters display on the OSD and AWI Network pages:

Network Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client Fully Qualified Domain Name (FQDN). When disabled, you must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.

Parameter	Description
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field. **Warning: Take care when setting the subnet mask** It is possible to configure an invalid IP address/subnet mask combination (for example, invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain name of the device (for example, domain.local). This field is optional.
FQDN	The fully qualified domain name for the device. The default is pcoip-portal- where is the device's MAC address. If used, the domain name is appended (for example, pcoip-portal-.domain.local). This field is read-only on this page. To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.

Parameter	Description
Ethernet Mode	Lets you configure the Ethernet mode of the client as follows: • **Auto** • **100 Mbps Full-Duplex** • **10 Mbps Full-Duplex** When you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and click**Apply**, the following warning message appears: **Warning: Different parameters may result in a loss of network connectivity** When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Click **OK** to change the parameter. **Note: Use 10 Mbps Full-Duplex and 100 Mbps Full-Duplex with caution** You should always set the Ethernet mode to **Auto** and only use **10 Mbps Full-Duplex** or **100 Mbps Full-Duplex** when the other network equipment (for example, a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.
Maximum MTU Size (AWI only)	Lets you configure the Maximum Transfer Unit packet size. A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client. The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.
Enable 802.1X Security	Enable this field for each of your PCoIP Remote Workstation Cards and Tera2 PCoIP Zero Clients if your network uses 802.1X security to ensure that only authorized devices access the network. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields.
Authentication (AWI only)	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.

Parameter	Description
Identity	Enter the identity string used to identify your device to the network. Should be the Common Name (CN) or subject name (SN) of the 802.1X certificate entered in the Client Certificate field.
Client Certificate	Click **Choose** to select the client certificate you want to use for your 802.1X devices. The list of certificates that appears includes the certificates uploaded from the Certificate Upload page that contain a private key. The certificate you choose from the Network page is linked to the read-only **Client Certificate** field on the Certificate Upload page. **Note: 802.1X client certificate must contain all security details** PCoIP only supports one 802.1X client certificate. Ensure your security details are all contained within the one file. The 802.1X certificate must contain a private key.
Enable 802.1X Support for Legacy Switches (AWI only)	When enabled, enables greater 802.1X compatibility for older switches on the network.

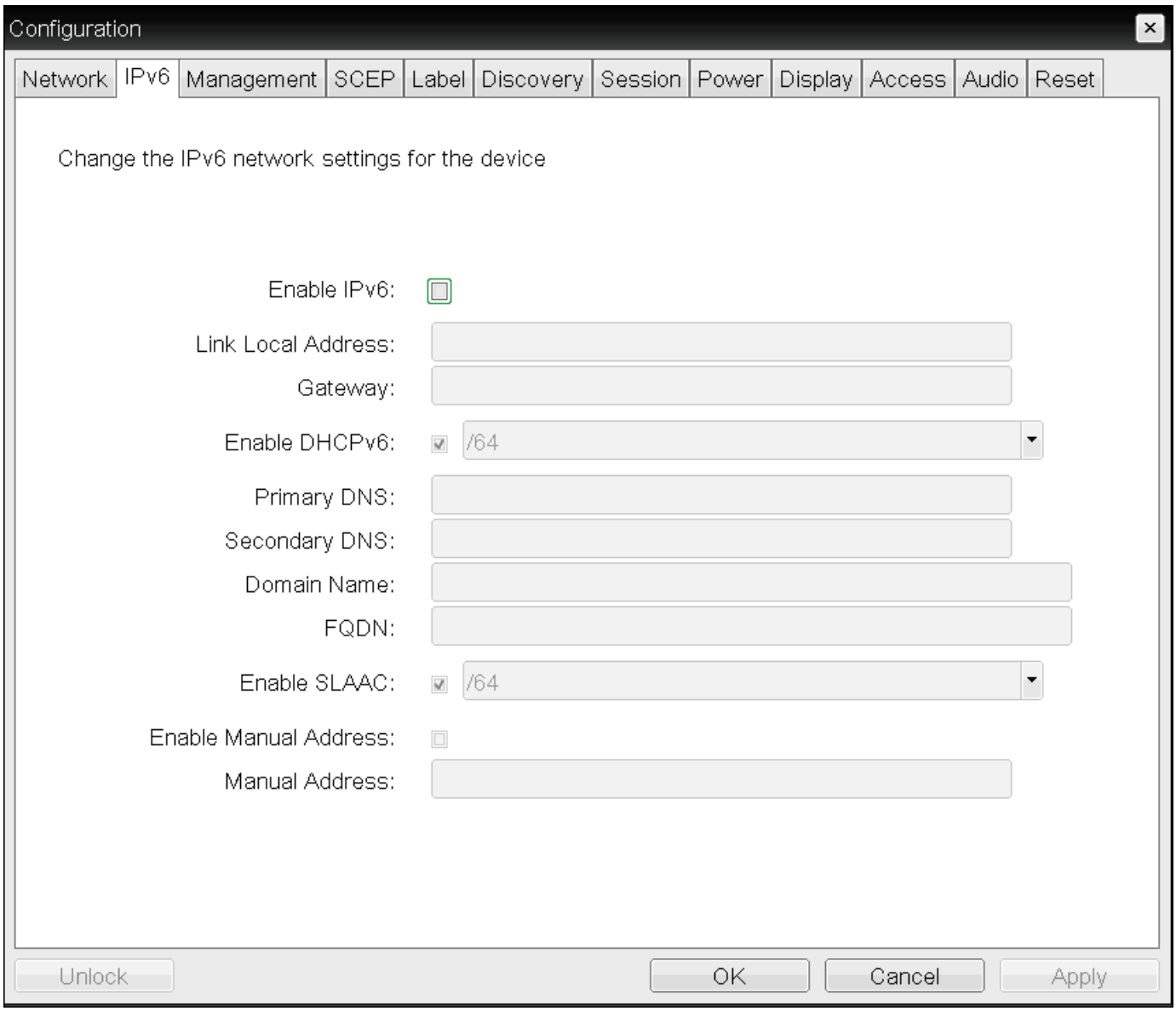
To configure network settings:

1. Open the Network page:
    - From the OSD, select **Options > Configuration > Network**.
    - From the AWI, select **Configuration > Network**.
2. From the OSD or AWI ***Network*** page, configure the network settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

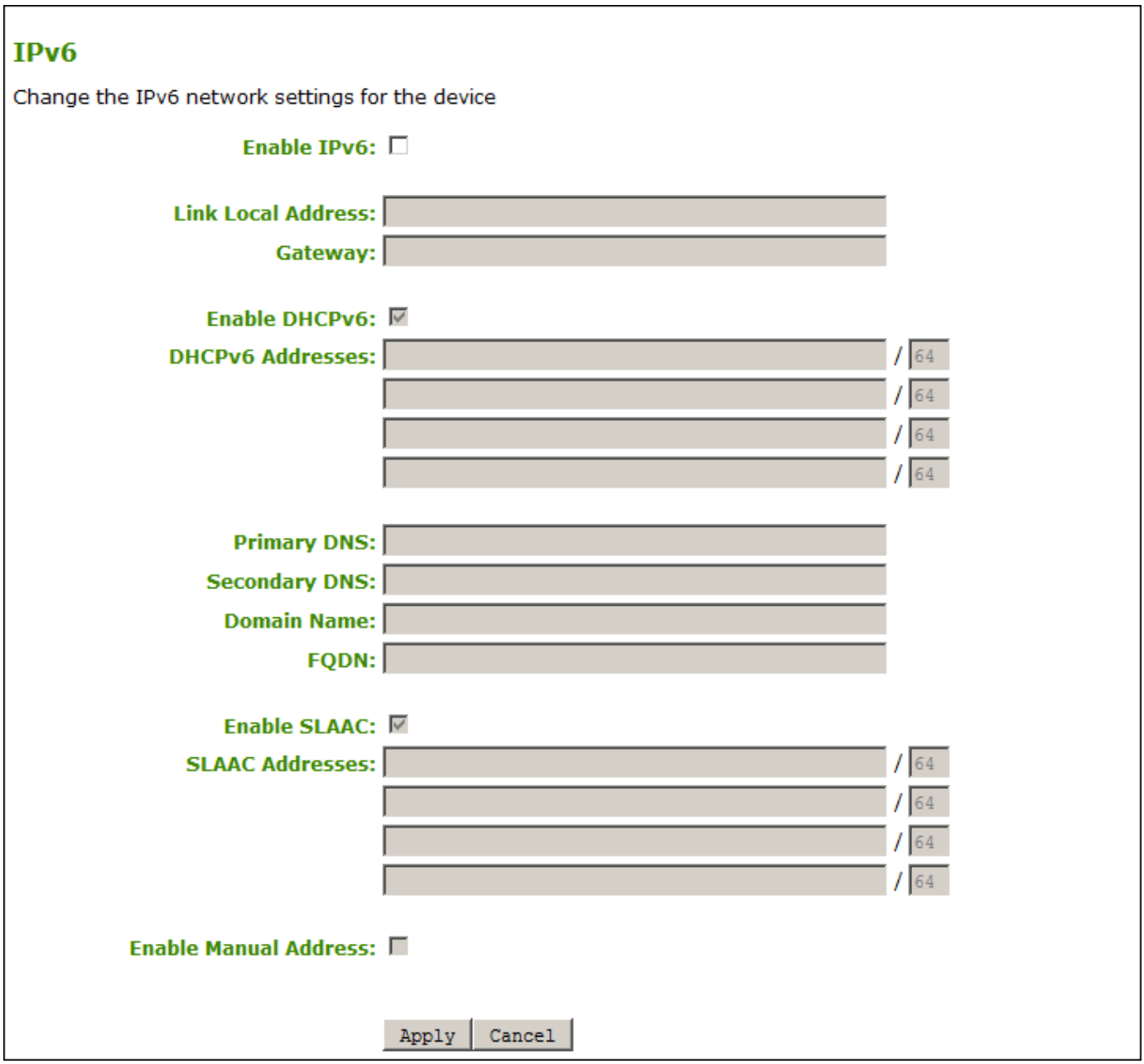
Configuring IPv6 Network Settings

Setting	Default	AWI	OSD	Management Console
Enable IPv6	Disabled	✔	✔	✔
Link Local Address	–	✔	✔	✖
IPv6 Gateway	–	✔	✔	✔
Enable DHCPv6	–	✔	✔	✔
Enable DHCPv6 Addresses	–	✔	✖	✖
Primary IPv6 DNS	–	✔	✔	✔
Secondary IPv6 DNS	–	✔	✔	✔
Domain Name	–	✔	✔	✔
FQDN	–	✔	✔	✖
Enable SLAC	–	✔	✔	✔
SLAAC Addresses	–	✔	✖	✖
Enable Manual Address	–	✔	✔	✖
Manual Address	–	✖	✔	✖

Options on the OSD and AWI IPv6 pages (shown next), enable you to change the network settings for your device.



OSD IPv6 page



AWI IPv6 page

Restart your device

When you make a change to one of the settings on this page, you must reboot your device for the change to take effect.

The following parameters display on the OSD and AWI IPv6 pages:

IPv6 Parameters

Parameter	Description
Enable IPv6	Select the check box to enable IPv6 for your PCoIP devices.
Link Local Address	This field is automatically populated.
Gateway	Enter the IPv6 gateway address.
Enable DHCPv6	Select the check box to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device.
DHCPv6 Addresses (AWI only)	When DHCPv6 is enabled and the device is rebooted, the server automatically populates these fields with addresses for the device.
Primary DNS	The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Secondary DNS	The device's secondary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Domain Name	The domain name used (for example, domain.local) for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	Select the check box to set up Stateless Address Auto-configuration (SLAAC) for your devices.
SLAAC Addresses (AWI only)	When SLAAC is enabled and the device is rebooted, these fields are automatically populated.
Enable Manual Address	Select this check box to set up a manual (static) address for the device.
Manual Address (OSD only)	Enter the IP address for the device.

To configure IPv6 settings:

1. Open the IPv6 page:
   - From the OSD, select **Options > Configuration > IPv6**.
   - From the AWI, select **Configuration > IPv6**.
2. From the IPv6 page, update the IPv6 network settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.
4. Reboot your device for the updates to take place.

Configuring OSD and AWI Password

The OSD Password page is only visible when there is a password applied to your zero client. OEMs have the option of applying a password in a new product. Consult your IT department or PCoIP Zero Client OEM documentation for OEM default password information. Steps to alter password configurations are included in this topic.

Setting	Default	AWI	OSD	Management Console
Old Password	–	✔	✔	✖ (See note)
New Password	–	✔	✔	✖ (See note)
Confirm New Password	–	✔	✔	✖ (See note)
Reset (Challenge/Response)	–	✖	✔	✖

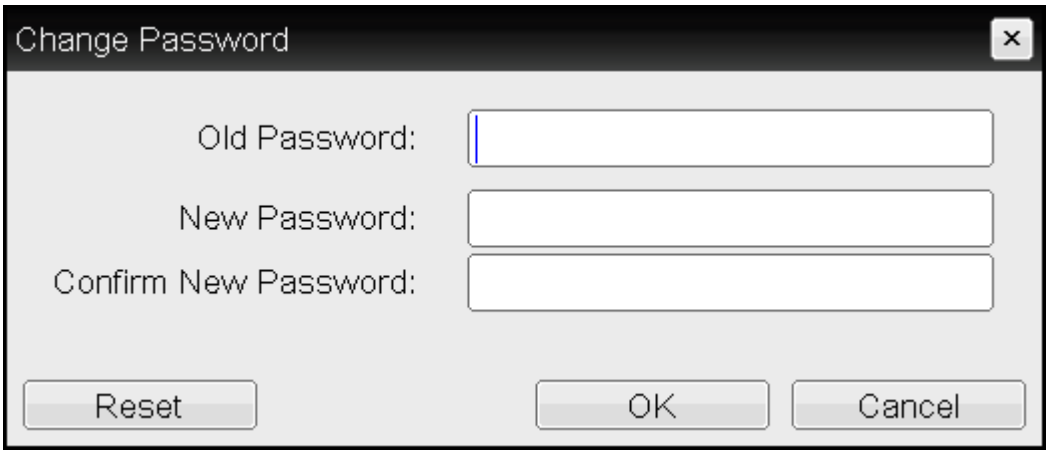
Note: Changing the Password with PCoIP Management Console

The OSD and AWI password can be managed by the PCoIP Management Console but not via the same parameters as seen in a password change dialog. If the zero client already has established communication with a PCoIP Management Console, then any password entered in the profile will be applied to the zero client. The parameters in the PCoIP Management Console profile that must be configured to apply or change a PCoIP Zero Client password are:

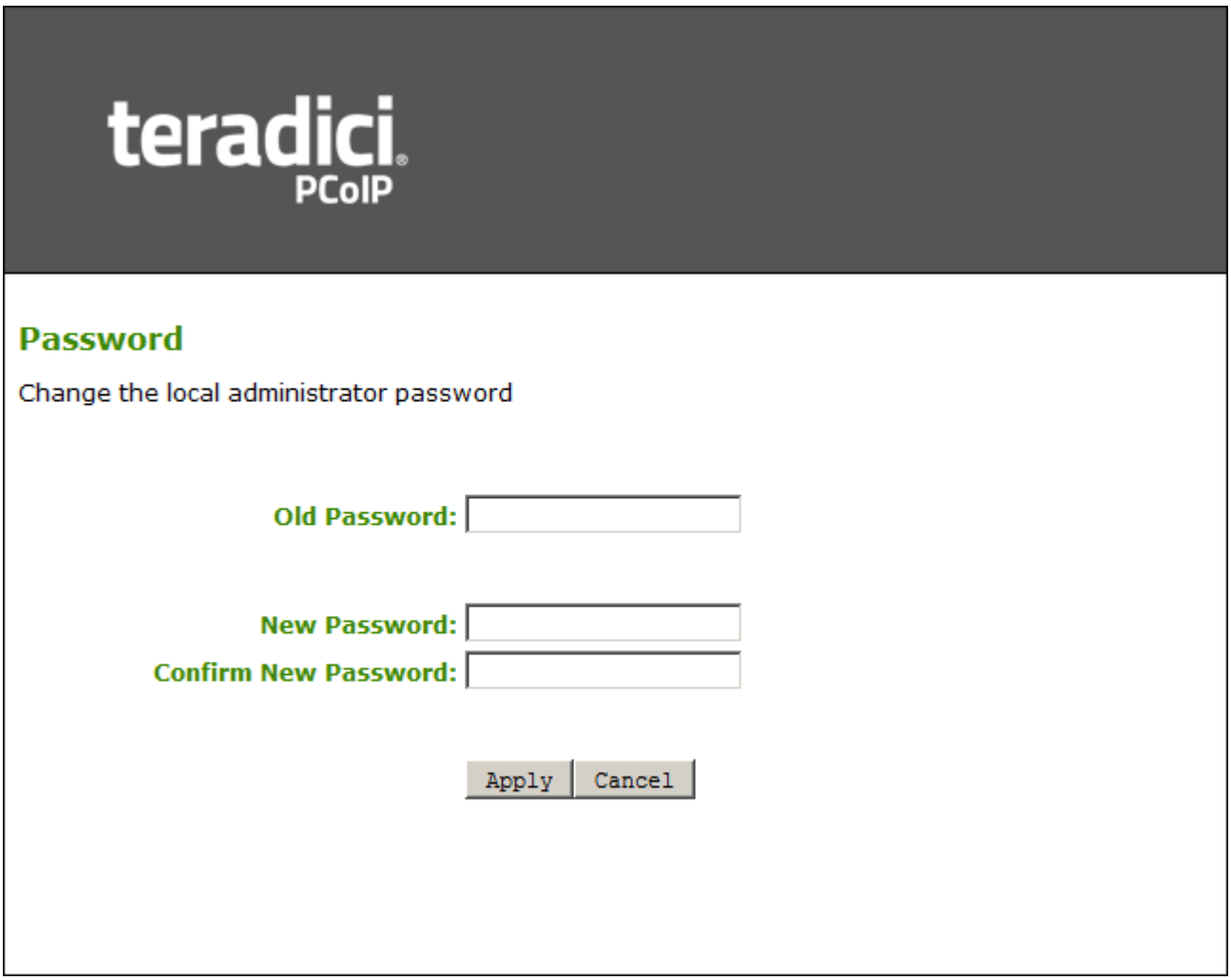
- **Local Administrative Password**: The password entered in this parameter becomes the active password on any zero client that has this profile applied to it successfully.
- **Enable Password Protection for AWI and OSD Configuration**: This enables and disables password protection on the zero client. If enabled, the value in the Local Administrative Password parameter is used. If no value is entered then an empty password will be required before changes to the OSD or AWI can be made. For more information on applying profiles see PCoIP Management Console Administrators' Guide.

From the OSD and AWI Password page, as shown next, you can update the local administrative password for the zero client. Applying a password affects access to the AWI and the ability to make changes in the **OSD > Options > Configuration** section. Take care when updating the zero client password as the zero client may become unusable if the password is lost. From the OSD, you can

also reset the password if you forget it. This process requires external communication with Teradici or the Zero Client vendor.



OSD Change Password page



AWI Password page

The password can be a maximum of 20 characters. Some PCoIP devices have password protection disabled by default, and the Password page is not available on these devices. You can enable password protection for these devices from the PCoIP Management Console. For details, see PCoIP® Management Console Administrators' Guide.

The following settings display on the Password page:

Password Parameters

Parameter	Description
Old Password	This field must match the current administrative password before you can update the password.
New Password	The new administrative password for both the AWI and the local OSD interface.
Confirm New Password	This field must match the New Password field for the change to take place.
Reset (OSD - Challenge/ Response)	This option is not available through the AWI. If you forget the password, you can click **Reset** to generate a challenge code. You must then provide that challenge code to a Zero Client vendor or to Teradici in order to obtain a response code. Once the response code is entered in the PCoIP Zero Client correctly, the password is reset to an empty string where you may enter a new password. In order to obtain the response code, you must meet certain criteria. • **PCoIP Zero Client Vendors:** The vendor qualifies the request before returning a response code. Contact the client vendor for more information when an authorized password reset is required. • **Teradici:** You must be a valid Teradici Subscription holder. Generate your response code by browsing to the password technical resource and selecting the **Password Reset > I am OEM partner, or I have challenge code to reset zero client password** option.

To update or change the password:

1. Open the Password page:
   - From the OSD, select **Options > Password**.
   - From the AWI, select **Configuration > Password**.

2. Update the password and select:
    - From the OSD select **OK**
    - From the AWI select **Apply**

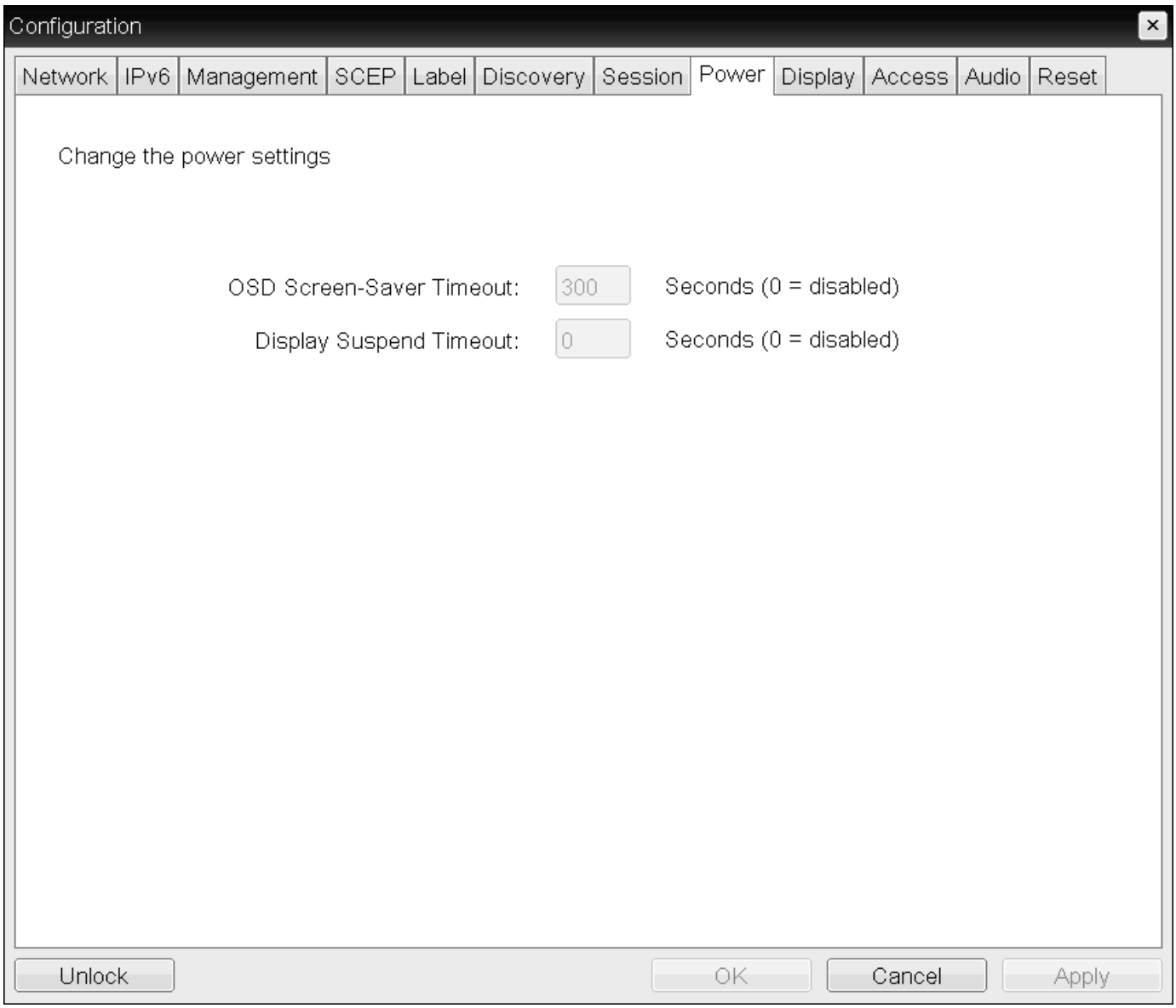
To Reset the password using the challenge code

1. From the OSD, open the Password page by browsing to **Options > Password**.
2. Select **Reset**.
3. Copy the Challenge code down to submit it to Teradici or your Zero Client OEM.
    - If you do not have a valid Teradici subscription, contact your Zero Client OEM and ask for the response code. You will have to provide the challenge code to obtain it.
        - From the challenge code window seen in step 2, enter the response code and select **OK** twice.
        - Enter your desired password and select **OK**.
    - If you have a valid Teradici subscription or are an OEM:
        - Login to the Teradici Support Site (requires subscription)
        - Browse to the password technical support resource area to obtain your response code.
        - Enter the response code in the reset window seen in step 2 and select **OK** twice.
        - Enter your desired password and select **OK**.

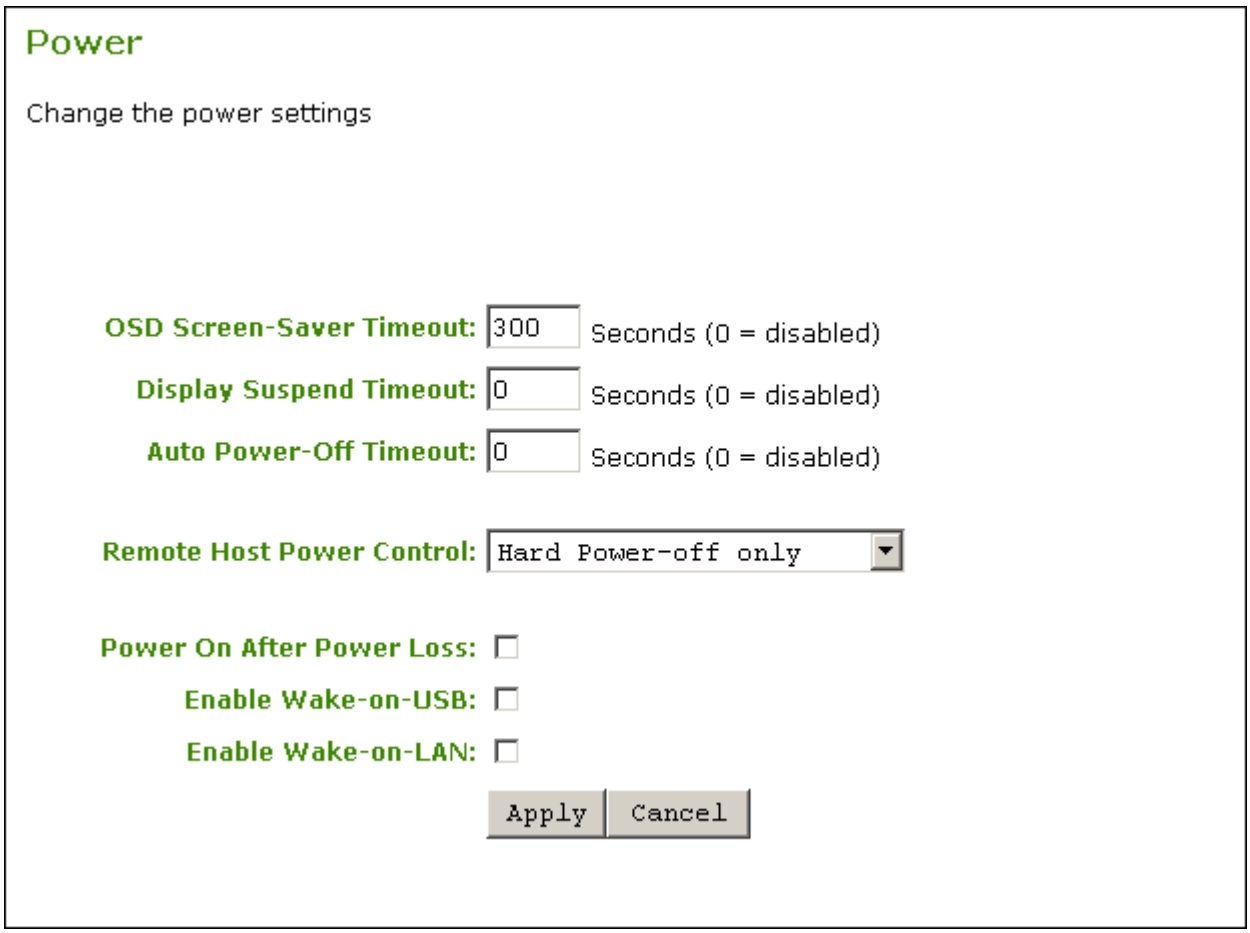
Configuring Power Settings

Setting	Default	AWI	OSD	Management Console
OSD Screen Saver Timeout	–	✓	✓	✓
Display Suspend Timeout	–	✓	✓	✓
Auto Power-Off Timeout	–	✓	✗	✓
Remote Host Power Control	–	✓	✗	✓
Power On After Power Loss	–	✓	✗	✓
Enable Wake-on-USB	–	✓	✗	✓
Enable Wake-on-LAN	–	✓	✗	✓

From the OSD and AWI Power pages as shown next, you can configure timeout and power settings for the device.



OSD Power page



AWI Power page

The following settings display on the OSD and AWI Power pages:

Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are **10** to **9999**, or use **0** to disable the feature. This timeout only applies when the device is not in session.

Parameter	Description
Display Suspend Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are **10** to **14400** seconds, or use **0** to disable the feature. This timeout only applies when the device is in session. When connected to a workstation, this feature requires you to enable the local mouse and keyboard feature. For more information about this feature and instructions on how to enable it, see the PCoIP® Host Software for Windows User Guide.
Auto Power-Off Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client powers down. Valid values are **60** to **28800** seconds, or use **0** to disable the power down. Non-zero values are only enabled when the Tera2 PCoIP Zero Client supports powering off. This timeout only applies when the device is not in session.
Remote Host Power Control	Configure the client's remote power setting. Select from the following options: • **Power-off not permitted:** Users can't remotely shut down the host PC from the Tera2 PCoIP Zero Client. When you select this option, the Zero Client Control Panel overlay window doesn't appear when you press the Tera2 PCoIP Zero Client's Connect/Disconnect button. • **Hard Power-off only:** Users are able to remotely shut down the host from the Tera2 PCoIP Zero Client. When this option is selected, the Zero Client Control Panel overlay window appears when you press the Tera2 PCoIP Zero Client's Connect/Disconnect button. For more information about the Zero Client Control Panel overlay window, see Disconnecting from a Session.
Power On After Power Loss	When enabled, the client automatically powers back on when power is supplied.
Enable Wake-on-USB	When enabled, configures the client to power up when the user presses a key on the keyboard. Wake-on-USB applies when the client is either powered off automatically or as a result of the user holding down the power button. Clicking or moving the mouse won't power up the client when this feature is enabled.

Parameter	Description
Enable Wake-on-LAN	When enabled, configures the client to wake up from a low power state when it receives Wake-on-LAN magic packets.

To configure power settings and permissions:

1. Open the Power page:
    - From the OSD, select **Options > Configuration > Power**.
    - From the AWI, select **Configuration > Power**.
2. Update the power settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Security Level

Setting	Default	AWI	OSD	Management Console
Low Security Environment	Enabled	✔	✘	✔
Medium Security Environment	–	✔	✘	✔
High Security Environment	–	✔	✘	✔
Peer-to-Peer Certificate	–	✔	✘	✘

You can view your Tera2 PCoIP Zero Client's security level from the OSD Management page and configure the security level from the AWI Management page. In high security environments, the OSD and AWI may be disabled and managed by a PCoIP enpoint manager. See Connecting to an Endpoint Manager.

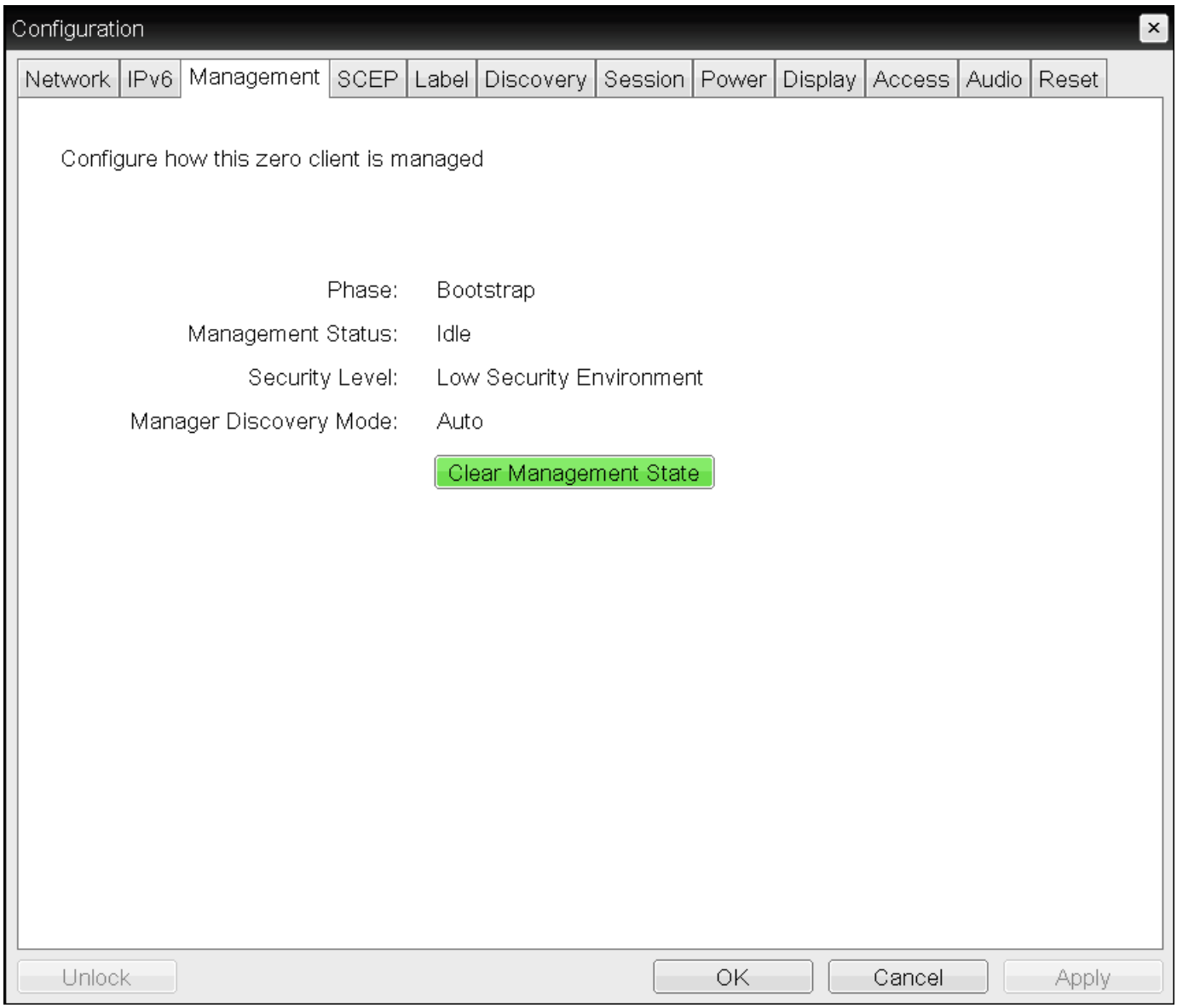
The AWI Management page has specific ***Security Level*** settings that allow for different methods of discovery by PCoIP endpoint managers. Setting the Security Level determines if your Tera2 PCoIP Zero Client will be discoverable by endpoint managers. For Zero Client security recommendations see Securing Your Tera2 PCoIP Zero Client

Security level implications

The security level setting has major implications for device discovery and connectivity with endpoint managers like the PCoIP Managment Console. For detailed information, see About Tera2 PCoIP Zero Client Security Levels.

Viewing the Security Level

From the OSD Management page (shown next), you can view the Tera2 PCoIP Zero Client's security level.



OSD Management page

To view the security level using the OSD:

1. From the OSD, select **Configuration > Management**.
2. From the OSD Management page, view the ***Security Level*** setting. The setting will be either:
    - **Low:** Discoverable by endpoint managers. This is the only security mode where certificates are optional.
    - **Medium:** Not discoverable by endpoint manager, and the installed certificate must trust the endpoint bootstrap manager.

- **High:** Not discoverable by endpoint managers, and the bootstrap phase is disabled. All endpoint manager connection configuration is manual. The installed certificate must trust the endpoint manager.

3. Click **Ok**.

Configuring the Security Level

From the AWI ***Management*** page, you can configure the Tera2 PCoIP Zero Client's security level.

The information that displays on the AWI Management page (shown next) depends on whether the client uses automatic or manual discovery.

AWI Management page – automatic discovery mode

AWI Management page – manual discovery mode

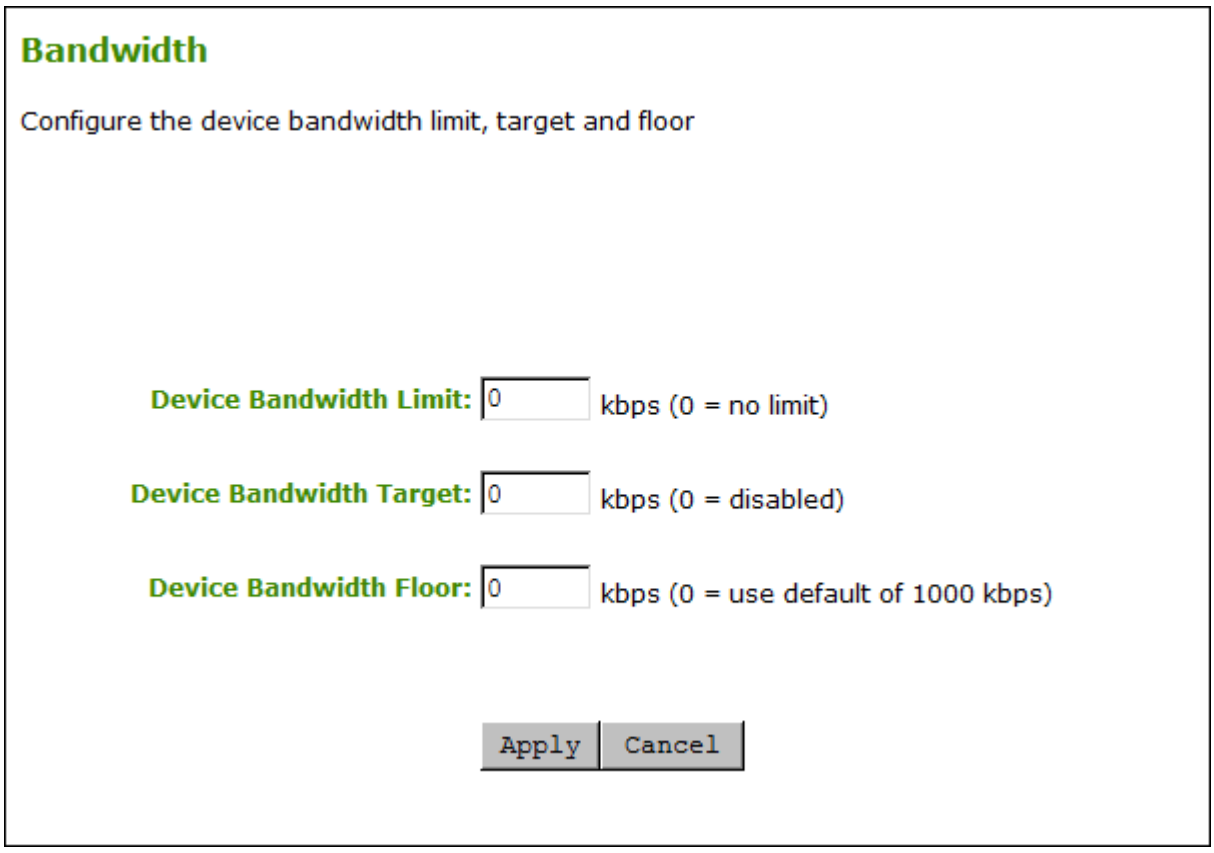
To configure the security level:

1. From the AWI, select **Configuration > Management**.
2. From the AWI Management page, set the ***Security Level*** setting to one of the following:
   - **Low:** Discoverable by endpoint managers. This is the only security mode where certificates are optional.
   - **Medium:** Not discoverable by endpoint manager, and the installed certificate must trust the endpoint bootstrap manager.
   - **High:** Not discoverable by endpoint managers, and the bootstrap phase is disabled. All endpoint manager connection configuration is manual. The installed certificate must trust the endpoint manager.
3. Click **Ok**.

Configuring Session Bandwidth

Setting	Default	AWI	OSD	Management Console
Device Bandwidth Limit	0	✔	✖	✔
Device Bandwidth Target	0	✔	✖	✔
Device Bandwidth Floor	0	✔	✖	✔

From the AWI ***Bandwidth*** page as shown next, you can control the bandwidth that your Tera2 PCoIP Zero Client uses during a PCoIP session.



AWI Bandwidth page

The following parameters display on the AWI Bandwidth page:

Bandwidth Parameters

Parameter	Description
Device Bandwidth Limit	Enter the maximum bandwidth peak from the client to the host (for example, USB data). The usable range of the device bandwidth is 1,000 to 220,000 Kbps for Tera1 devices and 1,000 to 600,000 Kbps for Tera2 devices. The PCoIP processor only uses the required bandwidth up to the **Device Bandwidth Limit** maximum, and dynamically adjusts the bandwidth in response to network congestion. Setting this field to 0 configures the PCoIP processor to use the maximum rate available in the network at any time. We recommend setting this field to the limit of the network connected to the client and host. When applied to devices running firmware lower than 3.0, a value other than 0 is rounded to the nearest megabit per second, with a minimum value of 1 Mbps.
Device Bandwidth Target	Enter the temporary limit on the network bandwidth during periods of congestion. When the device detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it. This enables for a more even distribution of bandwidth between users sharing a congested network link.
Device Bandwidth Floor	Enter the minimum bandwidth when congestion is present and bandwidth is required. This enables you to optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor. This setting defines the minimum bandwidth from the client to the host (for example, USB data). A setting of 0 configures the PCoIP processor to reduce bandwidth to 1,000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value. The firmware implements a slow-start algorithm that increases the bandwidth used until the required bandwidth is reached, network congestion is detected, or the **Device Bandwidth** Limit is met. It begins at the lesser of the **Device Bandwidth Limit** and 8,000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm enables a graceful session startup for low bandwidth scenarios (for example, WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use. When applied to devices running firmware lower than 3.0, a value other than 0 is rounded to the nearest megabit per second, with a minimum value of 1 Mbps.

To configure session bandwidth:

1. From the AWI, select **Configuration > Bandwidth**.
2. From the AWI *Bandwidth* page, update the bandwidth settings.
3. Click **Apply** to apply your updates immediately.

SNMP Overview

Knowledge of using and configuring Simple Network Management Protocol (SNMP) and an SNMP manager is required before enabling SNMP. See your SNMP manager documentation.

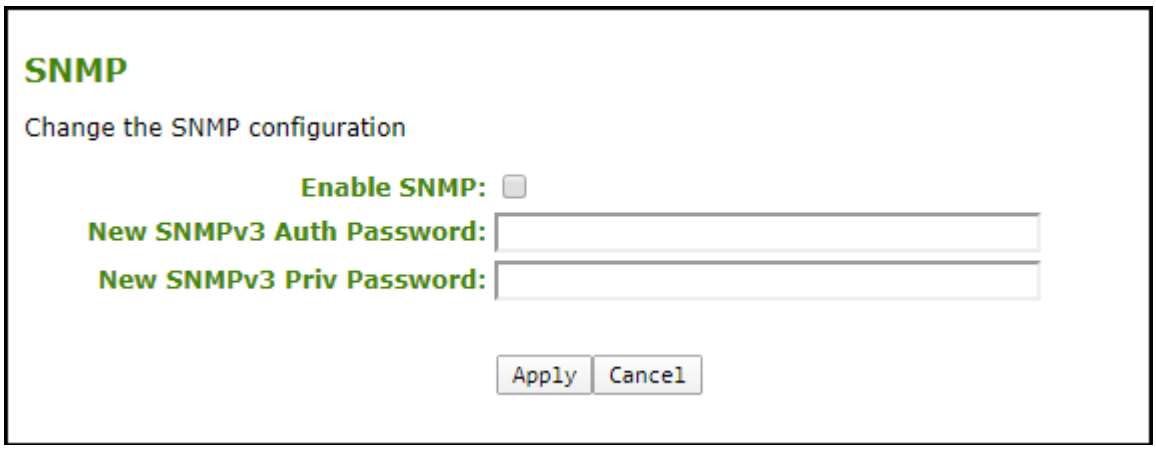
Simple Network Management Protocol (SNMP) allows an administrator to monitor hardware and software endpoints through an SNMP agent. The agent can be enabled on the device you are monitoring, and a SNMP manager can then view the data. From the AWI SNMP page you can enable or disable the SNMP agent. Once enabled, enter the auth and priv password values. The SNMP manager also requires configuration with the correct user name and protocols for SNMPv3 authentication. The SNMPv3 manager must use a username of **pcoip_authpriv**, using another value will cause the connection to fail. The **authentication password** provides user authentication using the SHA protocol while the **private password** provides the encryption key using the AES protocol.

Teradici has provided a MIBv2 and User Guide for download to help collect PCoIP related data on the PCoIP endpoint.

SNMP Configuration

Setting	Default	AWI	OSD	Management Console
Enable SNMP	Disabled	✔	✘	✔
SNMPv3 Auth Password	–	✔	✘	✔
SNMPv3 Priv Password	–	✔	✘	✔

From the AWI SNMP page, you can enable or disable the device's SNMP agent.



AWI SNMP page

To configure SNMPv3 perform the following steps:

1. From the AWI, select **Configuration > SNMP**.
2. Select **Enable SNMP** check box.

   When enabled, the device enables the PCoIP SNMP agent to respond to SNMP requests. Disabling the SNMP agent prevents it from responding to SNMP requests and from generating traps. It also ensures that the PCoIP SNMP MIB cannot be accessed.
3. For **SNMPv3 Auth Password**, enter an 8 - 16 character password to identify the agent with the manager.
4. For **SNMPv3 Priv Password**, enter an 8 - 16 character password to activate encryption of the data stream with the manager.
5. Click **Apply**.

SNMPv3 Manager Tool

For connectivity from the SNMPv3 manager, configure the manager with the username of **pcoip_authpriv**. Using another value will cause the connection to fail.

Configuring USB Settings and Permissions

Setting	Default	AWI	OSD	Management Console
Force Local Cursor Visible	Disabled	✔	✘	✘
Enable EHCI (USB 2.0)	Enabled	✔	✘	✔
Authorized Devices (Add new)	Any, Any, Any	✔	✘	✔
Unauthorized Devices (Add new)	empty	✔	✘	✔
Bridged Devices (Add new)	empty	✔	✘	✔
Devices Forced to USB 1.1 (Add new)	empty	✔	✘	✘

From the AWI, you can configure USB settings and permissions.

Configure USB settings to enable the Tera2 PCoIP Zero Client to always show the local cursor, and to configure EHCI (USB 2.0).

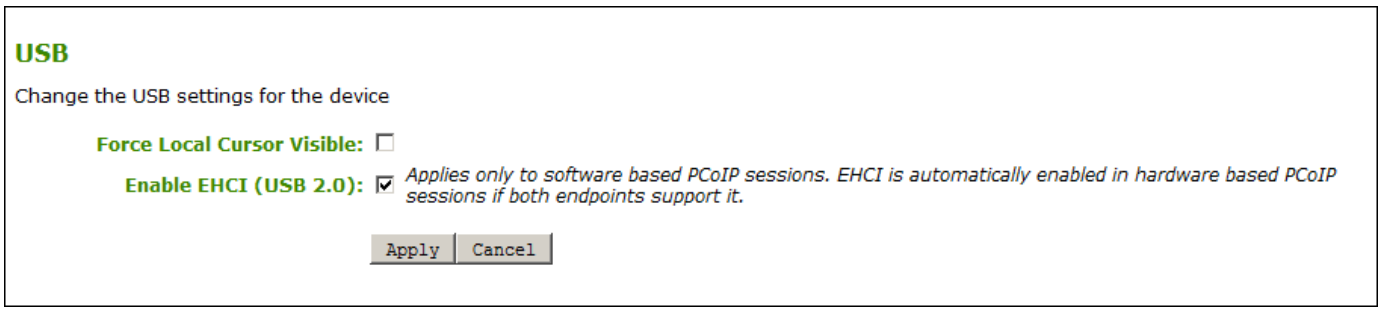
Configure USB permissions to authorize and unauthorize certain USB devices, configure devices that need to be bridged to the host, and enable USB 2.0 Enhanced Host Controller Interface (EHCI) mode.

Configuring USB audio devices

For information about configuring USB audio devices, see Configuring Audio.

Configuring USB Settings

From the AWI ***USB*** settings page, as shown next, you can configure parameters for devices plugged into Tera2 PCoIP Zero Client USB ports.



The following parameters display on the AWI USB parameters page:

USB Parameters

Parameter	Description
Force Local Cursor Visible	When enabled, the Tera2 PCoIP Zero Client always shows the local cursor. When disabled, the local cursor is only shown when the host requests it or a locally-terminated mouse is connected. For information about the local cursor feature, see Local Cursor and Keyboard.
Enable EHCI (USB 2.0)	Enable this field to configure EHCI (USB 2.0) for devices connected directly to Tera2 PCoIP Zero Client USB ports for sessions with a host running VMware View 4.6 or newer. This setting applies only to software-based PCoIP sessions. EHCI is automatically enabled in hardware-based PCoIP sessions if both endpoints support it. If you want the device to operate in OHCI (USB 1.1) mode, add it to the Devices Forced to USB 1.1 table on the AWI USB permissions page (see Configuring USB Permissions from the AWI). This feature cannot be enabled on clients with less than 128 MB of RAM. Devices with isochronous endpoints will not operate at USB 2.0 speeds.

To configure USB settings:

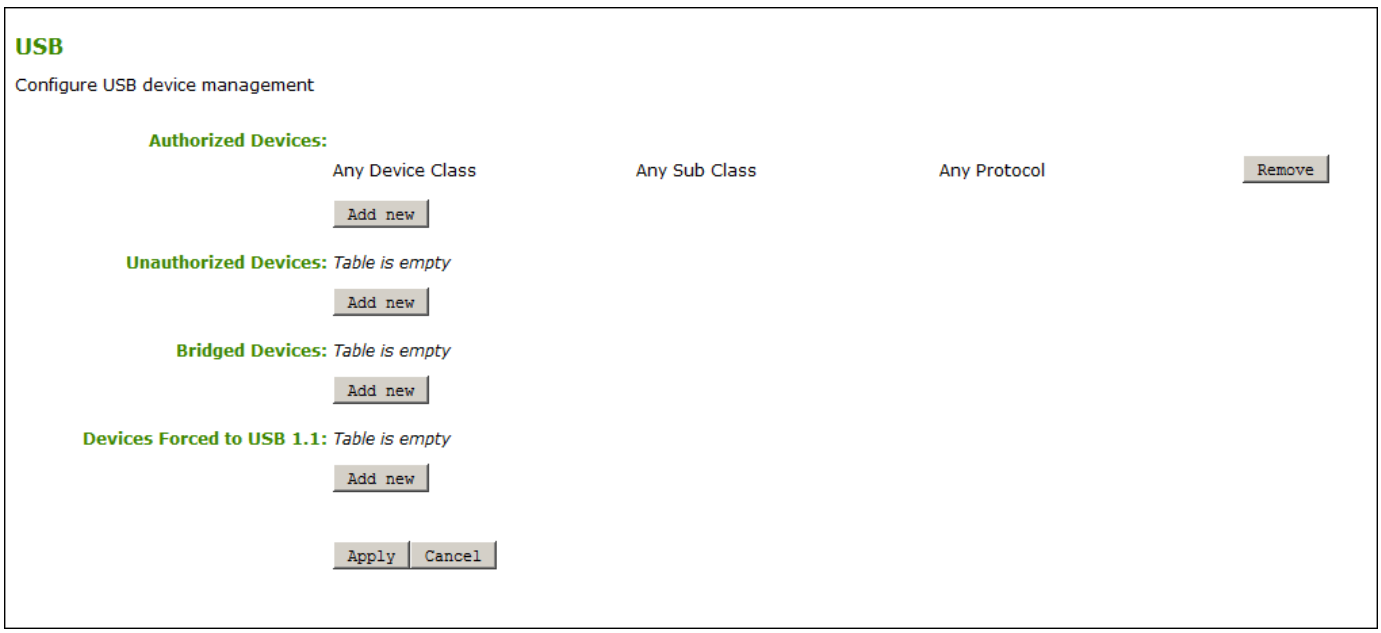
1. From the AWI, select **configuration > USB**.
2. From the AWI *USB* page, update the USB settings.
3. Click **Apply**.

Configuring USB Permissions from the AWI

Note: USB rules best practice for Tera2 Zero Clients

To avoid unexpected behavior, Teradici strongly advises users of Tera2 Zero Clients to configure these device rules in *both* the PCoIP agent and the Tera2 Zero Client.

From the AWI USB permissions page as shown next, you can configure USB permissions.



AWI USB permissions page

From this page, you can:

- Authorize and unauthorize a list of USB devices based on ID or Class. You can use wildcards (or specify any) to reduce the number of entries needed to define all devices.
- Configure devices that need to be bridged to the host, and enable USB 2.0 Enhanced Host Controller Interface (EHCI) mode for certain USB devices.
  If a bridged USB device that is capable of EHCI (USB 2.0) does not perform normally over PCoIP, you can use the **Devices Forced to USB 1.1** table to force the device to use OHCI (USB 1.1) instead of EHCI (USB 2.0), which may provide a better experience.

USB plug events are blocked in the Tera2 PCoIP Zero Client hardware for unauthorized USB devices. The host (PCoIP Remote Workstation Card or the host desktop) cannot see or access the device for an additional layer of security.

The USB permissions page (**AWI > Permissions > USB**) is available on the host and client but the host USB permissions have a higher priority and update the client USB permissions. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP Remote Workstation Card. The following rules apply:

- If the host has permissions programmed (authorized and/or unauthorized), the permissions are sent to the client. If the client has any unauthorized devices, they are added to the host's
- If the host does not have permissions programmed, the client's permissions are used.

The factory defaults have no USB permissions configured on the host. The factory defaults for the client USB permissions are 'any, any, any' (that is, authorized USB devices). Depending on the host implementation (for example, hardware PCoIP host or software PCoIP host), you can configure the USB permissions as required on the client and/or host.

The host USB permissions are only updated at the start of a PCoIP session. They are authorized in the following order of priority (from highest to lowest):

- Unauthorized Vendor ID/Product ID
- Authorized Vendor ID/Product ID
- Unauthorized Device Class/Sub Class/Protocol
- Authorized Device Class/Sub Class/Protocol

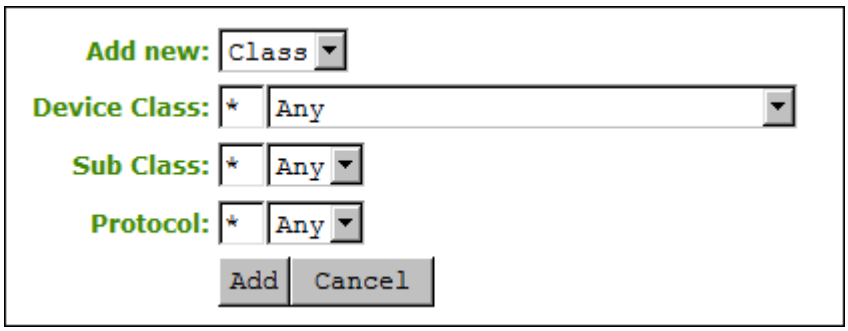
The following parameters display on the AWI USB permissions page:

AWI USB Permissions Parameters

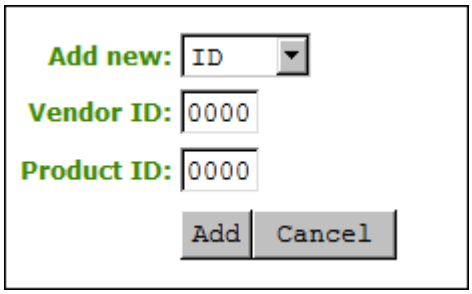
Parameter	Description
Authorized Devices	Specify the authorized USB devices for the device: **Add New:** add a new device or device group to the list. This enables USB authorization by ID or Class: • **ID:** The USB device is authorized by its Vendor ID and Product ID. • **Class:** The USB device is authorized by Device Class, Sub Class, and Protocol. **Remove:** Delete a rule for a device or device group from the list.

Parameter	Description
Unauthorized Devices	Specify the unauthorized USB devices for the device. **Add New:** add a new device or device group to the list. This enables USB unauthorization by ID or Class: • **ID:** The USB device is unauthorized by its Vendor ID and Product ID. • **Class:** The USB device is unauthorized by Device Class, Sub Class, and Protocol. **Remove:** Delete a rule for a device or device group from the list.
Bridged Devices	Tera2 PCoIP Zero Clients locally terminate HID devices when connecting to VMware Horizon virtual desktops. However, some devices advertise as HID but use different drivers. These devices may need to be bridged to the host rather than locally terminated. This setting lets you force the Tera2 PCoIP Zero Client to bridge specific USB devices so that they use the drivers on the virtual desktop. **Add New:** Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID. Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information. **Remove:** Delete a rule for a device or device group from the list.
Devices Forced to USB 1.1	If a bridged USB device that is capable of EHCI (USB 2.0) does not perform normally over PCoIP, you can use this table to force the device to use OHCI (USB 1.1) instead of EHCI (USB 2.0), which may provide a better experience. **Add New:** Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID. **Remove:** Delete a rule for a device or device group from the list. Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information.

The following figures show the parameters that display when you add a new USB authorized or unauthorized entry. The parameters that display depend on whether you describe the device by **Class** or **ID**.



Device class parameters



Device ID parameters

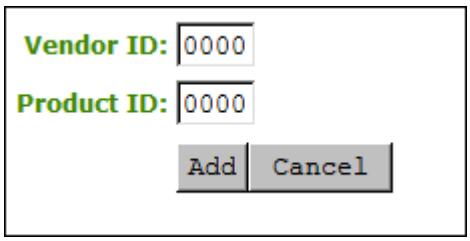
The following parameters display when you authorize or unauthorize USB device parameters:

USB Authorized/Unauthorized Devices Parameters

Parameter	Description
Add new	When adding a new USB authorization or unauthorization entry, select one of the following: • **Class:** The USB device is authorized by its device class, sub-class, and protocol information. • **ID**:The USB device is authorized by its vendor ID and product ID information.
Device Class	This field is enabled when **Class** is selected. Select a supported device class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any device class.
Sub Class	This field is enabled when **Class** is selected. Select a supported device sub class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any sub-class.
Protocol	This field is enabled when **Class** is selected. Select a supported protocol from the drop-down menu, or select **Any**.

Parameter	Description
Vendor ID	This field is enabled when **ID** is selected. Enter the vendor ID of the authorized (or unauthorized) device. The valid range is hexadecimal 0-FFFF.
Protocol ID	This field is enabled when **ID** is selected. Enter the product ID of the (authorized or unauthorized) device. The valid range is hexadecimal 0-FFFF.

The following figure shows the parameters that display when you add a new USB bridged entry.



USB Bridged Parameters

The following parameters display when you add a new USB bridged entry:

USB Bridged Devices Parameters

Parameter	Description
Vendor ID	Enter the vendor ID of the bridged device. The valid range is hexadecimal 0-FFFF.
Protocol ID	Enter the product ID of the bridged device. The valid range is hexadecimal 0-FFFF.

To configure USB permissions from the AWI:

1. From the AWI, select **Configuration > USB**.
2. From the AWI *USB* page, update the USB permissions.
3. Click **Apply**.

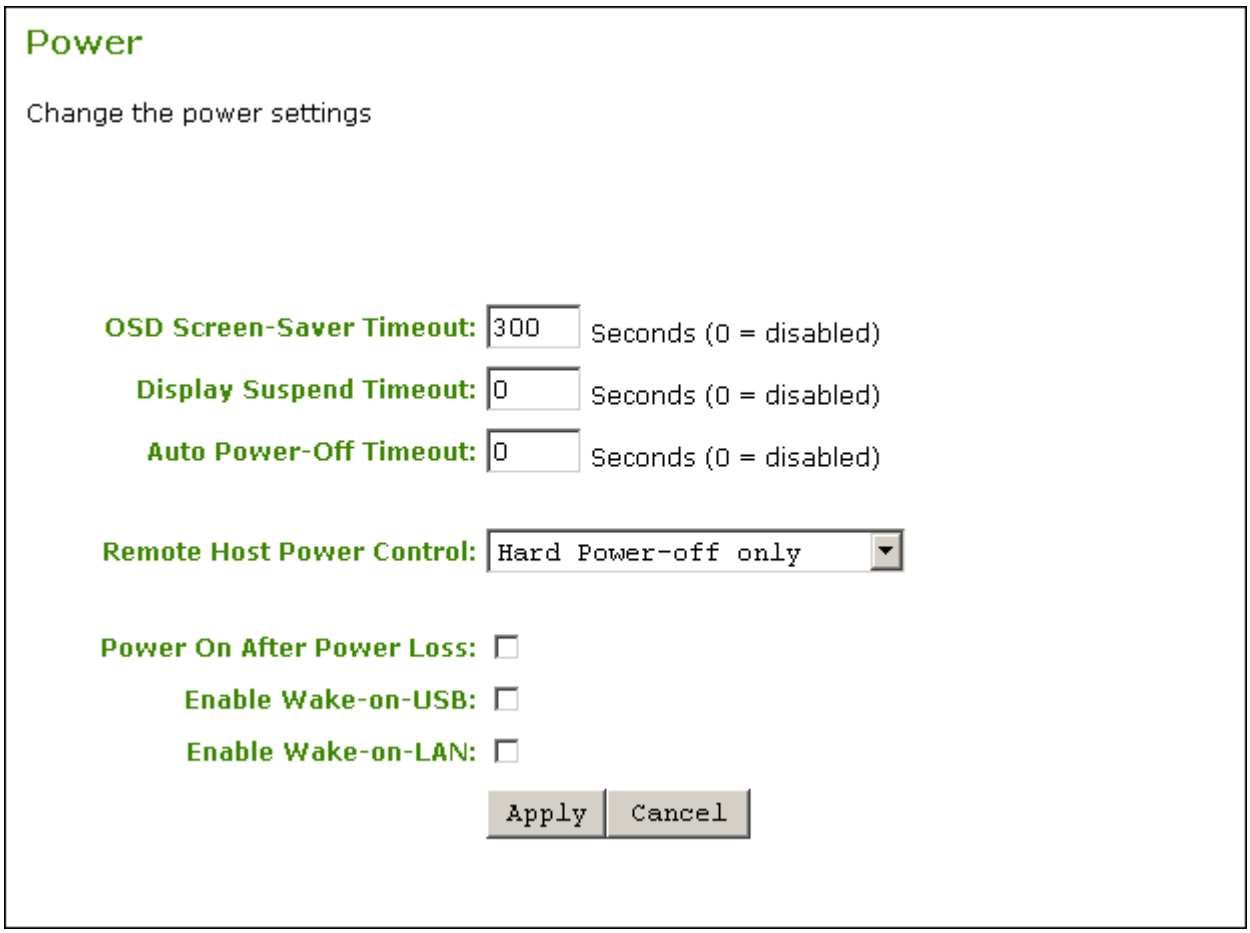
Configuring User Settings

This section describes how you can customize your environment to suit your personal preferences. For example, you can configure regional settings (such as the timezone and daylight saving time), configure multiple monitors to accommodate your physical desktop, and configure the language and keyboard layout to use for the OSD user interface. You can also adjust the image quality during PCoIP sessions.

If your Zero Client is managed by an administrator via the management console, the administrator may have hidden some or all of the ***User Settings*** configuration tabs and the features found on those tabs. If you are unable to view or see a particular user settings tab or a feature for your PCoIP Zero Client, please consult your administrator or visit the Management Console Administrators' Guide section on Hidden OSD Menus and Settings.

AWI: Power Permissions

The Power page lets you configure timeout and power settings for the device. You can access this page from the **Configuration > Power** menu.



AWI Power page

The following parameters can be found on the AWI Power page.

AWI Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 9999, or use 0 to disable the feature. This timeout only applies when the device is not in session.

Parameter	Description
Display Suspend Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 14400 seconds, or use 0 to disable the feature. This timeout only applies when the device is in session. When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.
Auto Power-Off Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client powers down. Valid values are 60 to 28800 seconds, or use 0 to disable the power down. Non-zero values are only enabled when the PCoIP client supports powering off. This timeout only applies when the device is not in session.
Remote Host Power Control	Configure the client's remote power setting. Select from the following options: • .**Power-off not permitted:** Users cannot remotely shut down the host PC from the Tera2 PCoIP Zero Client. When this option is selected, the Zero Client Control Panel on the OSD does not appear when the PCoIP Zero Client's connect/disconnect button is pressed. • **Hard Power-off only:** Users are able to remotely shut down the host from the Tera2 PCoIP Zero Client. When this option is selected, the Zero Client Control Panel on the OSD appears when the Tera2 PCoIP Zero Client's connect/disconnect button is pressed.
Power On After Power Loss	When enabled, the client automatically powers back on when power is supplied.
Enable Wake-on-USB	When enabled, configures the client to power up when the user presses a key on the keyboard. Wake-on-USB applies when the client is either powered off automatically or as a result of the user holding down the power button. Clicking or moving the mouse will not power up the client when this feature is enabled.
Enable Wake-on-LAN	When enabled, configures the client to wake up from a low power state when it receives Wake-on-LAN magic packets.

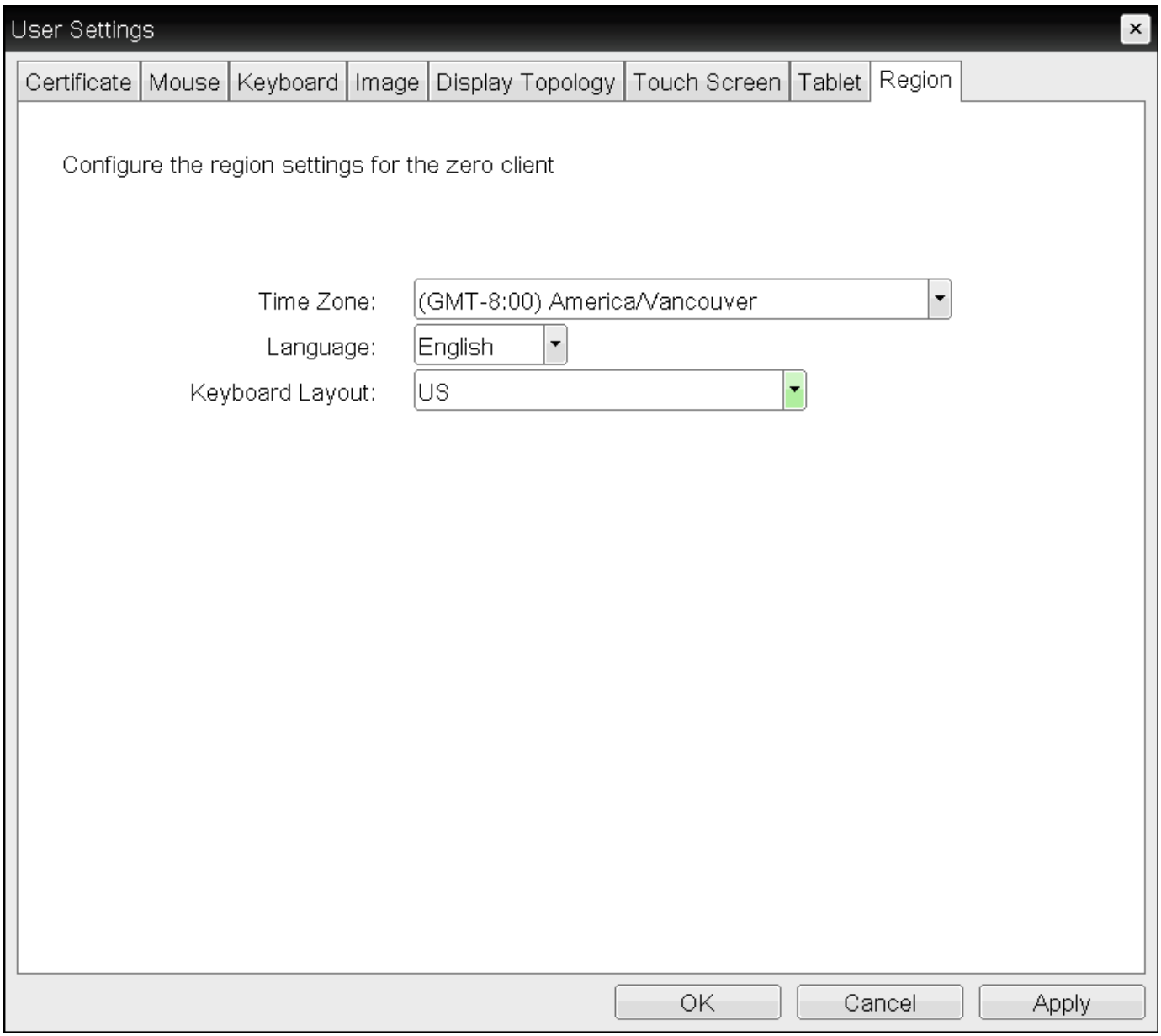
Configuring OSD Language

Setting	Default	AWI	OSD	Management Console
Language	English	✔	✔	✔
Keyboard Layout	US	✔	✔	✔
OSD Region Tab Lockout	Disabled	✔	✖	✔

When you configure OSD language settings, you configure the language to use for the OSD user interface, as well as the keyboard layout to use when you type information within the OSD. Note that updating the OSD language doesn't affect the language setting for the actual PCoIP session.

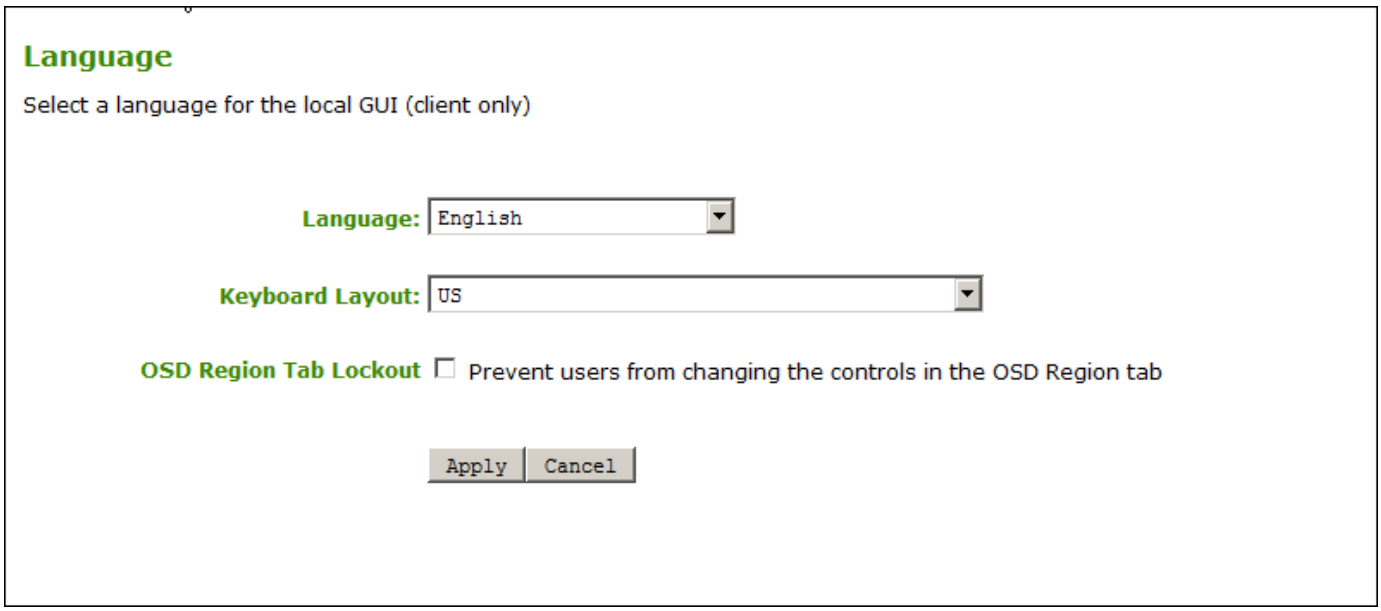
You can update language settings from both the OSD and AWI. From the AWI, you can also enable a setting to prevent users from changing the language settings (as well as the time zone) from the OSD.

From the OSD ***Region*** page, as shown next, you can update language and keyboard settings.



OSD Region page

From the AWI ***Language*** page, as shown next, you can update language and keyboard settings. In addition, you can enable a setting to prevent users from changing the configuration on the OSD ***Region*** page.



AWI Language page

To update language settings:

1. Do one of the following:
   - From the OSD, select **Options > User Settings > Region**
   - From the AWI, select **Configuration > Language**.
2. From the OSD Region page or the AWI Language page, do the following:
   - From the Language list, select the language to use for the OSD user interface.
   - From the Keyboard Layout list, select the keyboard layout to use when you type information within the OSD. When a session starts, this setting is pushed to the virtual machine. If the PCoIP Use Enhanced Keyboard on Windows Client if available GPO setting is configured to enable the keyboard layout setting, the layout is used during the user's session.
   - (AWI only) Select or clear the **OSD Region Tab Lockout** check box. When selected, users can't change the settings on the OSD Region page.
3. To save your updates, click OK from the OSD, or click **Apply** from the AWI.

Configuring Time Settings

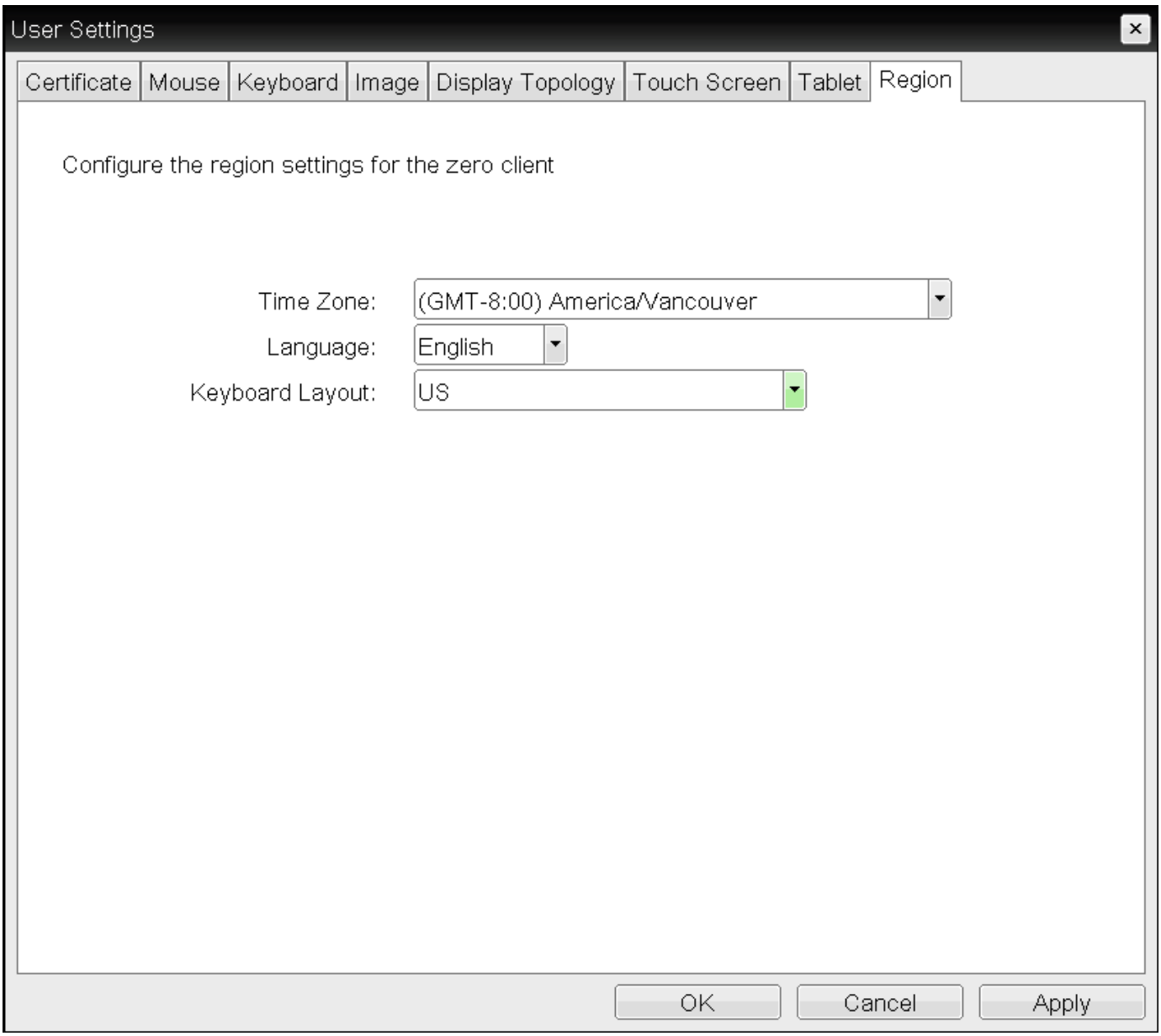
Setting	Default	AWI	OSD	Management Console
	Enable NTP	Disabled	✔	✖
Identify NTP Host by	—	✔	✖	✔
NTP Host DNS Name	—	✔	✖	✔
NTP Host Port	—	✔	✖	✔
NTP Query Interval	—	✔	✖	✔
Time Zone	Europe/London (UTC+0:00)	✔	✔	✔
Enable Daylight Saving Time	Disabled	✔	✖	✔

You can set the time zone for the Tera2 PCoIP Zero Client from both the OSD and AWI.

Additionally, from the AWI, you can:

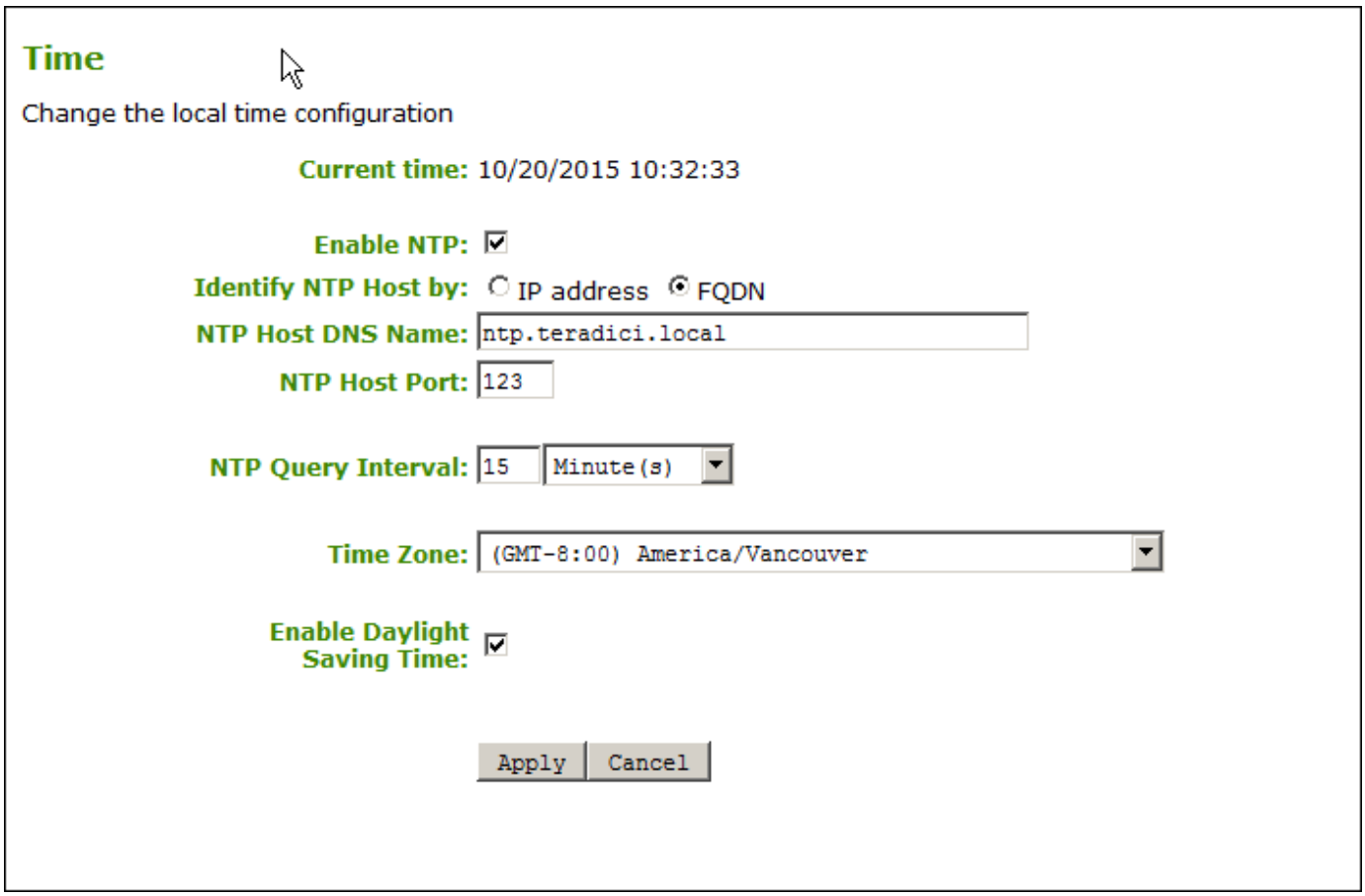
- Enable Daylight Saving Time
- Configure Network Time Protocol (NTP) parameters to time-stamp Tera2 PCoIP Zero Client event logs to use NTP time.

You set the time zone for the Tera2 PCoIP Zero Client from the OSD ***Region*** page, as shown next.



OSD Region page

From the AWI ***Time*** page, as shown next, you can set the time zone, enable Daylight Saving Time, and configure NTP.



AWI Time page

The following time parameters display on the OSD ***Region*** and AWI ***Time*** pages:

Time Parameters

Parameter	Description
Current Time (AWI only)	Displays the time based on the NTP.
Enable NTP (AWI only)	Enable or disable the NTP feature.

Parameter	Description
Identify NTP Host by (AWI only)	Select if the NTP host is identified by IP address or by Fully Qualified Domain Name (FQDN). If NTP is disabled, this field is not required and is not editable. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose. • **IP Address:** Shows the NTP Host IP address • **FQDN:** Shows the NTP Host DNS name.
NTP Host Port (AWI only)	Configure the port number of the NTP server. The default NTP server port value is 123.
NTP Query Interval (AWI only)	Configure the query interval. The first field is for the interval period and the second field is for the time unit in minutes, hours, days, or weeks.
Time Zone	Select the local time zone.
Enable Daylight Saving Time (AWI only)	Enable or disable the automatic adjustment for Daylight Saving Time (DST).

To configure time settings:

1. Do one of the following:
   - From the OSD, select **Options > User Settings > Region**.
   - From the AWI, **Configuration > Time**.
2. From the OSD Region page or the AWI *Time* page, update the time settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Server address overrides manually configured server

If the device is configured for DHCP and the DHCP server provides an NTP server address, this address will override any manually configured NTP server. It will also enable NTP if it is.

NTP server does not provide time zone information

The device does not obtain time zone or Daylight Saving Time information from the NTP server.

Enabling user events to correlate with log entries

To simplify system troubleshooting, set the NTP parameters to enable user events to correlate with the relevant diagnostic event log entries.

Configuring Image Quality

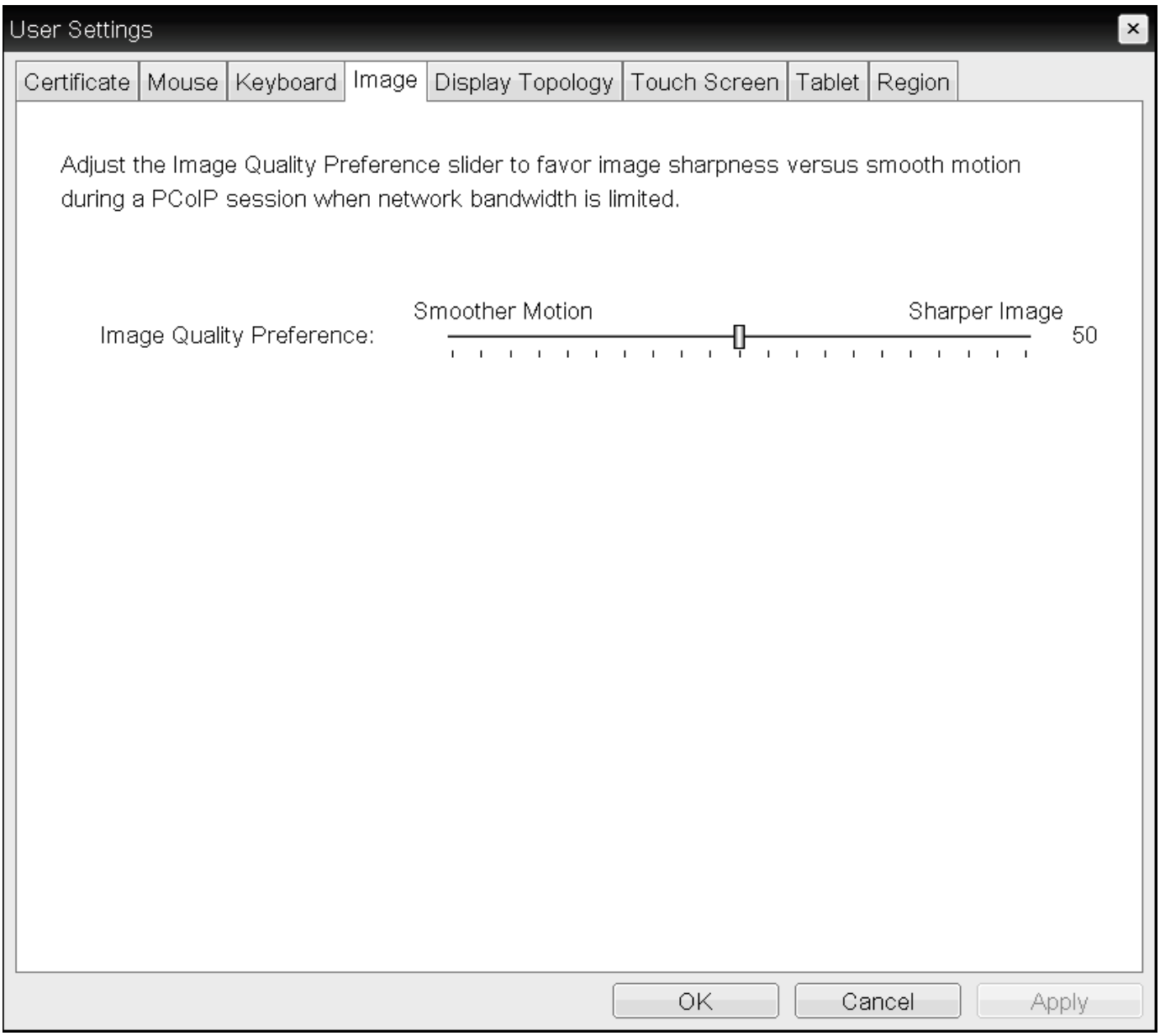
Setting	Default	AWI	OSD	Management Console
Minimum Image Quality	40	✔	✖	✔
Maximum Initial Image Quality	90	✔	✖	✔
Image Quality Preference	50	✔	✖	✔
Maximum Frame Rate	0 fps	✔	✖	✔
Disable Build to Lossless	Disabled	✔	✖	✔
Enable Low Bandwidth Text Codec	Disabled	✔	✖	✔

If desired, you can adjust the quality of the images you see during PCoIP sessions. You can set image quality preferences from both the OSD and AWI; however, you can configure many more settings from the AWI, including minimum image quality, maximum frame rate, and maximum initial image quality.

Image quality settings only apply to sessions with PCoIP Remote Workstation Cards

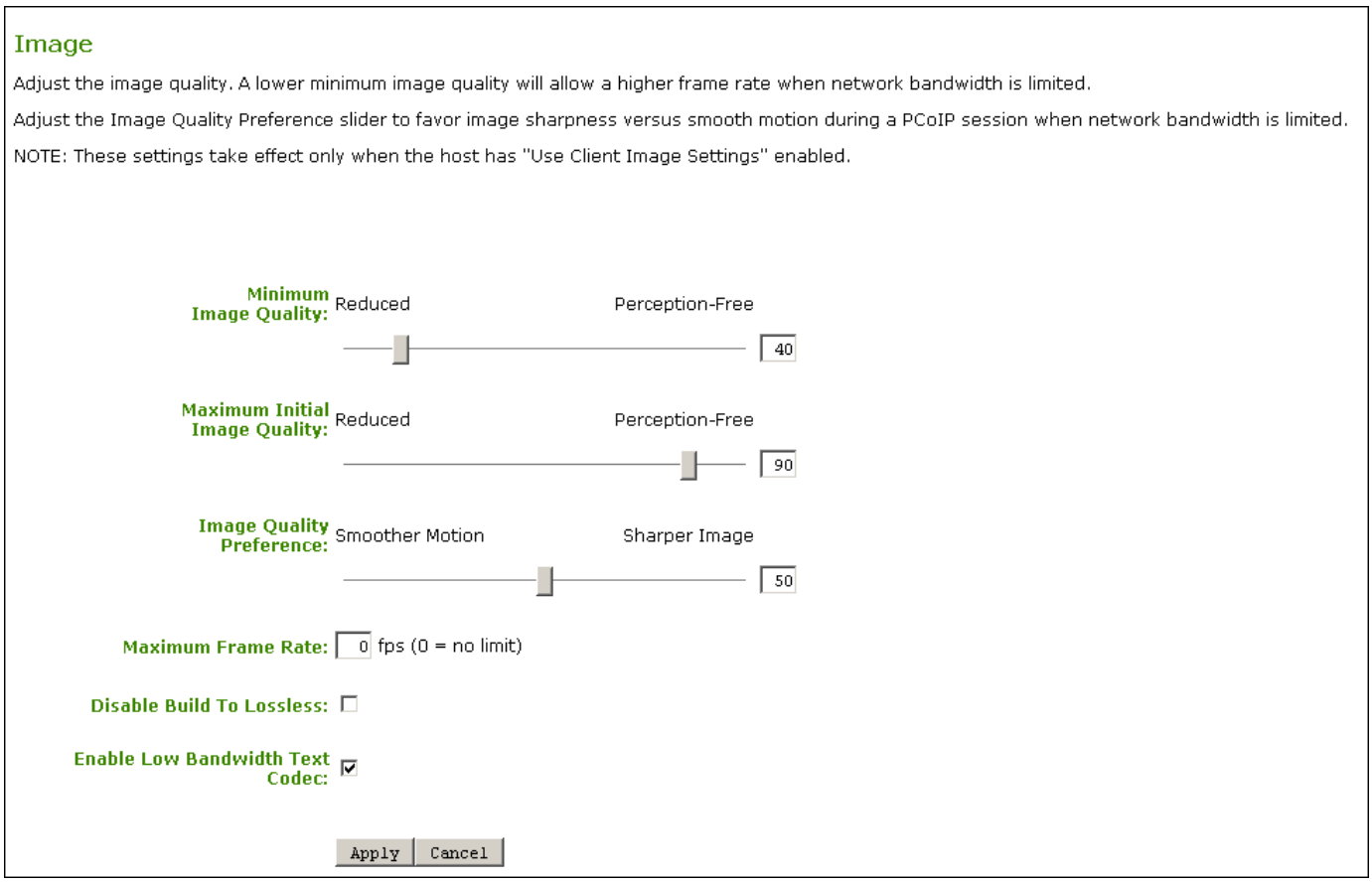
Image quality settings apply only to sessions between Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards.

You adjust the image quality setting from the OSD ***Image*** page, as shown next.



OSD Image page

You adjust the image quality setting, as well as other advanced settings, from the AWI Image page, as shown next.



AWI Image page

The following image parameters display on the OSD and AWI *Image* pages:

Image Parameters

Parameter	Description
Minimum Image Quality (AWI only)	Enables you to compromise image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, move the slider towards **Reduced** to enable higher frame rates. Move the slider towards **Perception-Free** to enable for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.

Parameter	Description
Maximum Initial Image Quality (AWI only)	Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. **This setting doesn't work in PCoIP sessions with VMware Horizon virtual desktops that run release 5.0 or earlier.**
Maximum Frame Rate (AWI only)	The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.
Disable Build to Lossless (AWI only)	Clear this check box to retain the PCoIP protocol's build-to-lossless feature, where images continue to be refined in the background until they reach a fully lossless state (that is, identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting. **Warning: Selecting the *Disable Build to Lossless* check box degrades images.** Selecting the Disable Build to Lossless check box degrades the images presented to the user. Don't select this check box unless your administrator decides that users don't require optimal image quality to perform critical functions. If you select this check box, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless. **This setting does not work in PCoIP sessions with VMware Horizon virtual desktops that run release 5.0 or earlier.**

Parameter	Description
Enable Low Bandwidth Text Codec (TERA2321 PCoIP Zero Clients only) (AWI only)	When enabled, Low Bandwidth Text Codec Mode will be used for TERA2321 PCoIP Zero Clients. The Low Bandwidth Text Codec is a new compression method that provides improved bandwidth usage when encoding lossless data, such as text and background. It does not apply to lossy data, such as video.

To configure image quality:

1. Open the *Image* page:
   - From the OSD, select **Options > User Settings > Image**.
   - From the AWI, select **Configuration > Image**.
2. From the OSD or AWI Image page, update the image settings.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Mouse

Setting	Default	AWI	OSD	Management Console
Mouse speed	40	✖	✔	✖
Relative Mouse	disabled	✔(hidden)	✖	✖

Mouse Speed

Mouse speed only apply when you use the OSD

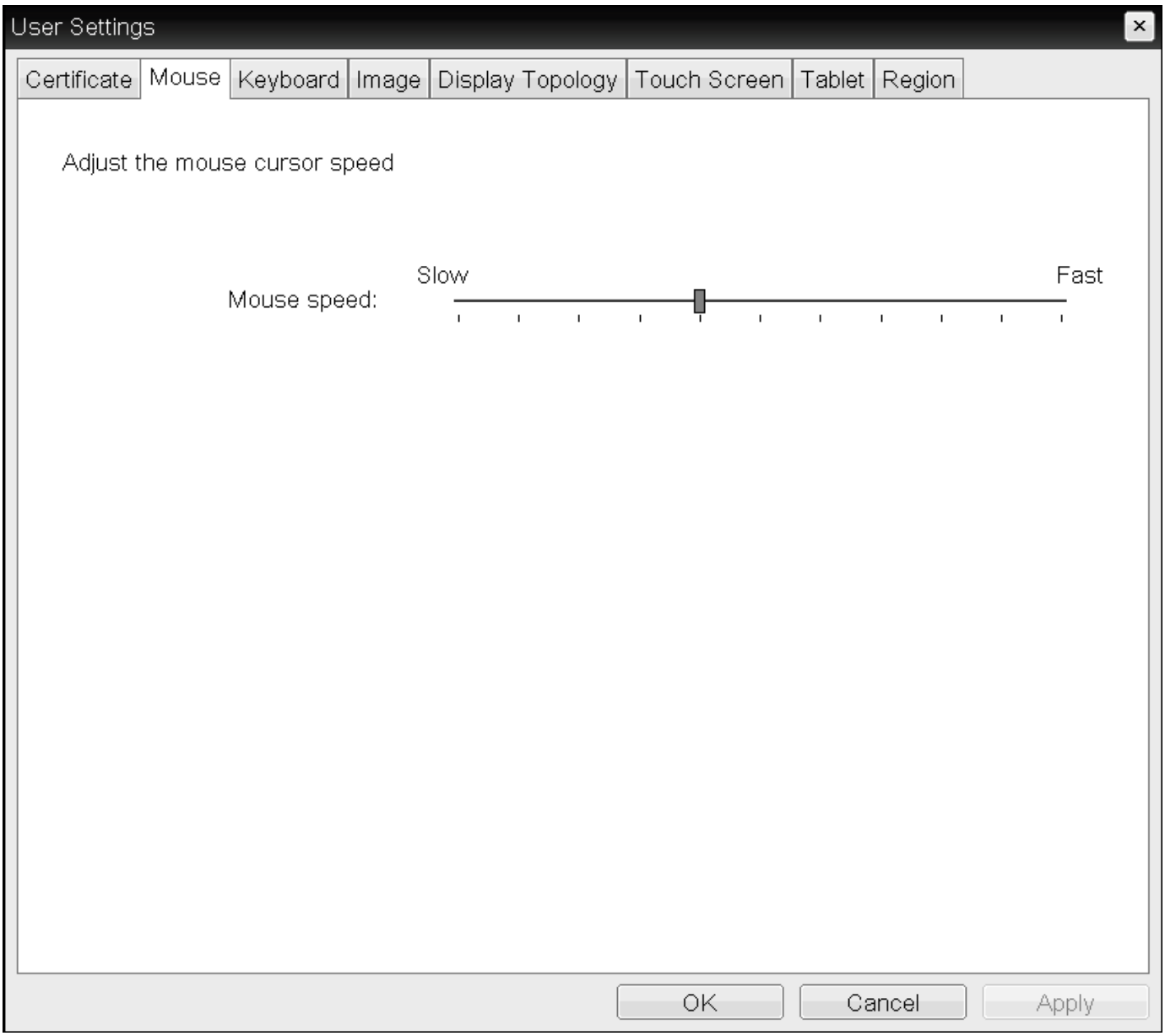
Mouse cursor speed only applies when you use the OSD. They have no effect on keyboard settings during PCoIP sessions.

Local cursor and keyboard feature

Local cursor and keyboard is a feature of the PCoIP Host Software that improves usability for PCoIP sessions operating over WAN connections (latency > 40 ms). When enabled, the Tera2 PCoIP Zero Client can terminate input from the mouse and keyboard, and draw the cursor on the attached display(s).

For more information about this feature and instructions on how to enable it, see the PCoIP® Host Software for Windows User Guide.

From the OSD Mouse page, as shown next, you can change the mouse cursor speed.



OSD Mouse page

To change the mouse cursor speed:

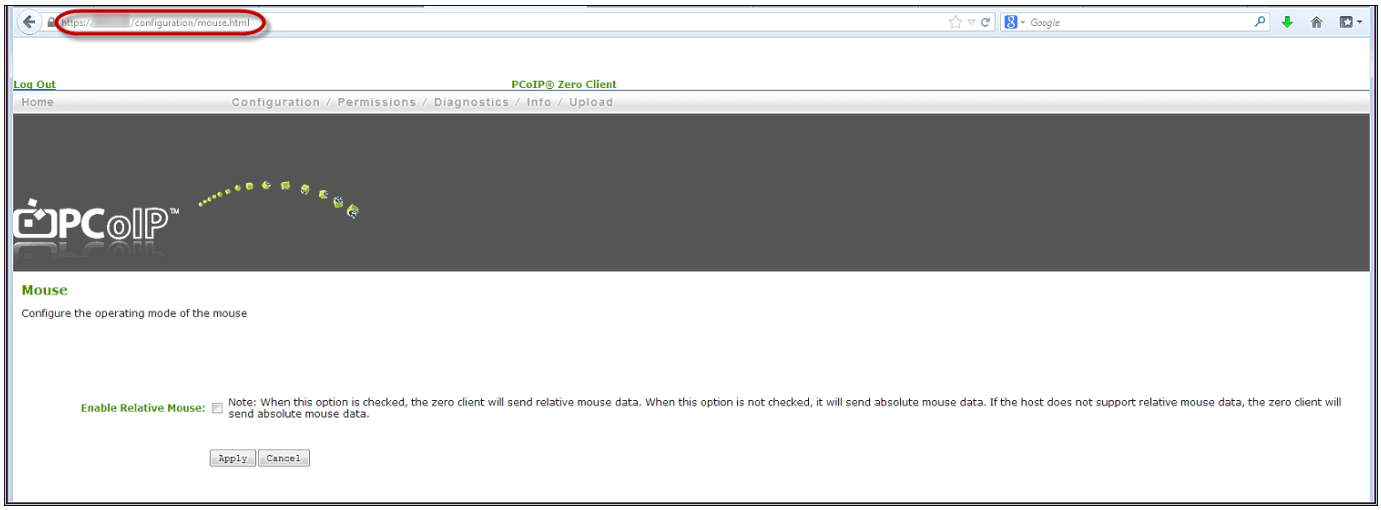
1. From the OSD, select **Options > User Settings > Mouse**.
2. From the OSD Mouse page, move the slider to adjust the mouse cursor speed.
3. Click **OK**.

Mouse (Relative Mouse)

PCoIP Zero Clients support the Relative Mouse option when connecting to supported Windows software hosts. It is a method of translating mouse movements as a delta from the last mouse position rather than a move to an absolute position on the screen. This type of mouse control is used in many CAD/CAM, Visual Effects and First-Person Gaming software. In a CAD program you may want to control an objects orientation in 3-D with mouse movements. Moving the mouse to the left or right rotates the object around the Z-axis, and moving the mouse up or down rotates the object around the X-axis. As you continue to move the mouse left the object continues to rotate about the axis, and the rotation is not bounded by the mouse stopping at the boarders of the screen.

In fact while in relative mouse mode, the mouse cursor is not visible as the position of the mouse is not important, the mouse is only being used to control movements - up/down or left/right.

Applications that use relative mouse movements generally provide methods for entering or exiting relative mouse mode, for instance clicking on an object with the middle button. While the middle button is held down the object may be controlled using relative mouse movements.



AWI Mouse page

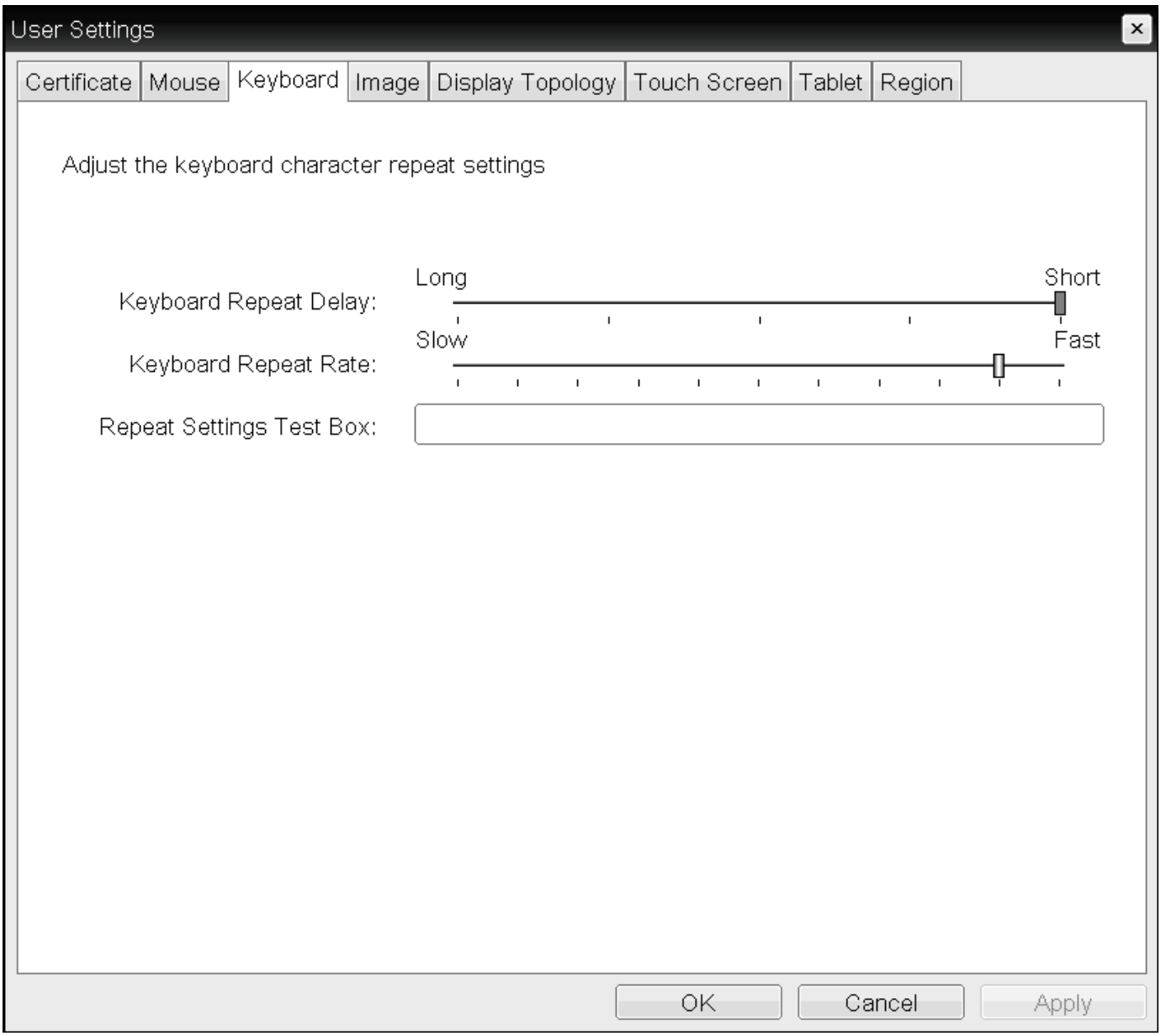
To enable relative mouse:

1. Log into your Zero Client AWI.
2. Enter **https://<zero_client_ip_address>/configuration/mouse.html** in the URL field.
3. Select the **Enable Relative Mouse** check box.
4. Click **Apply**.

Configuring Keyboard Settings

Setting	Default	AWI	OSD	Management Console
Keyboard Repeat Delay	100	✗	✓	✓
Keyboard Repeat Rate	90	✗	✓	✓
Repeat Settings Test Box	–	✗	✓	✓
Keyboard Scan Code Filters	–	✗	✗	✓

From the OSD ***Keyboard*** page, as shown next, you can change the keyboard character delay and character repeat settings.



OSD Keyboard page

Keyboard settings only apply when you use the OSD

Keyboard settings only apply when you use the OSD. They have no effect on keyboard settings during PCoIP sessions.

Local cursor and keyboard feature

Local cursor and keyboard is a feature of the PCoIP Host Software that improves usability for PCoIP sessions operating over WAN connections (latency > 40 ms). When enabled, the Tera2 PCoIP Zero Client can terminate input from the mouse and keyboard, and draw the cursor on the attached display(s).

For more information about this feature and instructions on how to enable it, see the PCoIP® Host Software for Windows User Guide.

To change keyboard parameters:

1. From the OSD, select **Options > User Settings > Keyboard**.
2. From the OSD *Keyboard* page, do the following:
   - For *Keyboard Repeat Delay*, move the slider to configure the time that elapses before a character begins to repeat when pressed down.
   - For *Keyboard Repeat Rate*, move the slider to configure the speed at which a character repeats when pressed down.
   - In the *Repeat Settings Test Box* box, type a character to test the delay and repeat settings.
3. Click **OK**.

Keyboard Scan Code Filters

Keyboard Scan Code Filters allow you to create rules that prevent the operation of certain keys or key combinations on the attached keyboard. Each filter consists of a Scan Code, Lock State and Modifier State. An example of a Keyboard Scan Code Filter rule would be when an administrator would want to block a screenshot of the whole screen using `PrtScr` while allowing a screenshot of only the Active Window using `Alt`+`PrtScr`. These settings can only be set by applying a properly configured Management Console profile to the Zero Client.

To create and apply a Keyboard Scan Code Filter, see the PCoIP Management Console Administrators' Guide Keyboard Scan Code Filters topic.

Configuring Multiple Displays

Setting	Default	AWI	OSD	Management Console
Enable Configuration	Disabled	✗	✓	✓
Layout	–	✗	✓	✓
Alignment	–	✗	✓	✓
Primary	–	✗	✓	✓
Position	–	✗	✓	✓
Rotation	–	✗	✓	✓
Resolution	–	✗	✓	✓

Depending on the Tera2 PCoIP Zero Client you have, you can attach up to two or four displays to your device. Using the OSD ***Display Topology*** page, you can configure the position, rotation, and resolution of the attached displays.

Before you configure multiple displays, make sure your setup has these components

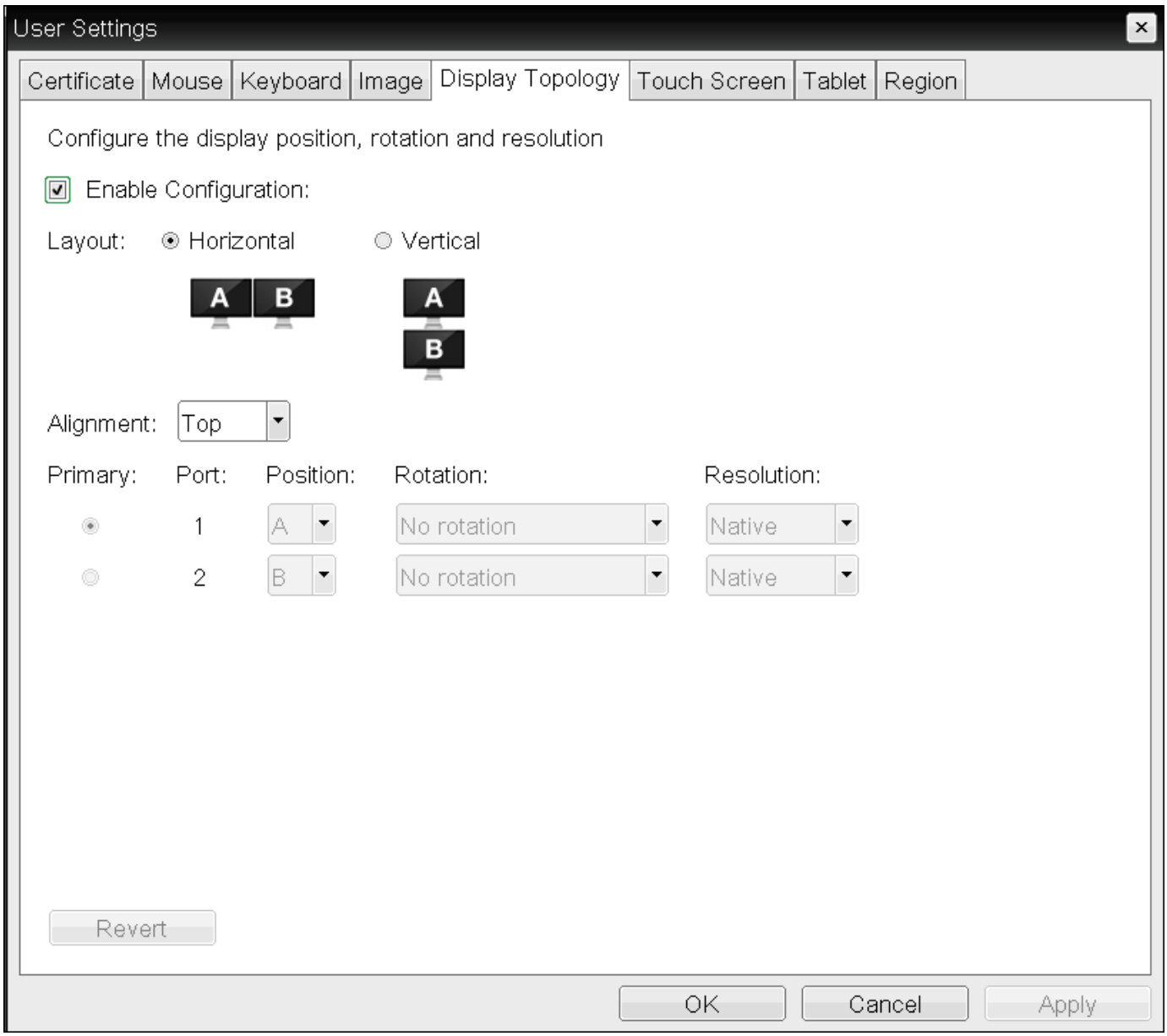
- To apply the display topology feature to a PCoIP session between a client and a VMware Horizon virtual desktop, you must have VMware View 4.5 or higher.
- To apply the display topology feature to a PCoIP session between a client and a PCoIP Remote Workstation Card, you must have the Remote Workstation Card Software installed on the host.

Use the OSD, not the Windows Display Settings, to configure display settings

Always change the display topology settings using the OSD Display Topology page. Don't change these settings from the Windows Display configuration page in a virtual machine when using VMware View.

Configuring Two Displays

If your Tera2 PCoIP Zero Client supports two attached displays, The OSD Display Topology page, as shown next, enables you to configure the display topology for the attached displays.



OSD Display Topology page (for two displays)

The following parameters display on the OSD *Display Topology* page:

Display Topology Parameters (Two-Display Configuration)

Parameter	Description
Enable Configuration	Enable to configure a device that supports two displays per PCoIP chipset.
Display Layout	Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk. • **Horizontal:** Select to arrange displays horizontally, as indicated in the diagram. • **Vertical:** Select to arrange displays vertically, as indicated in the diagram.
Alignment	Select how you want displays aligned when they are different sizes. **Note: This setting affects which area of the screen to use when users move the cursor from one display to the other.** The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout:** • **Top:** Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center:** Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom:** Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout:** • **Left:** Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center:** Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right:** Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.

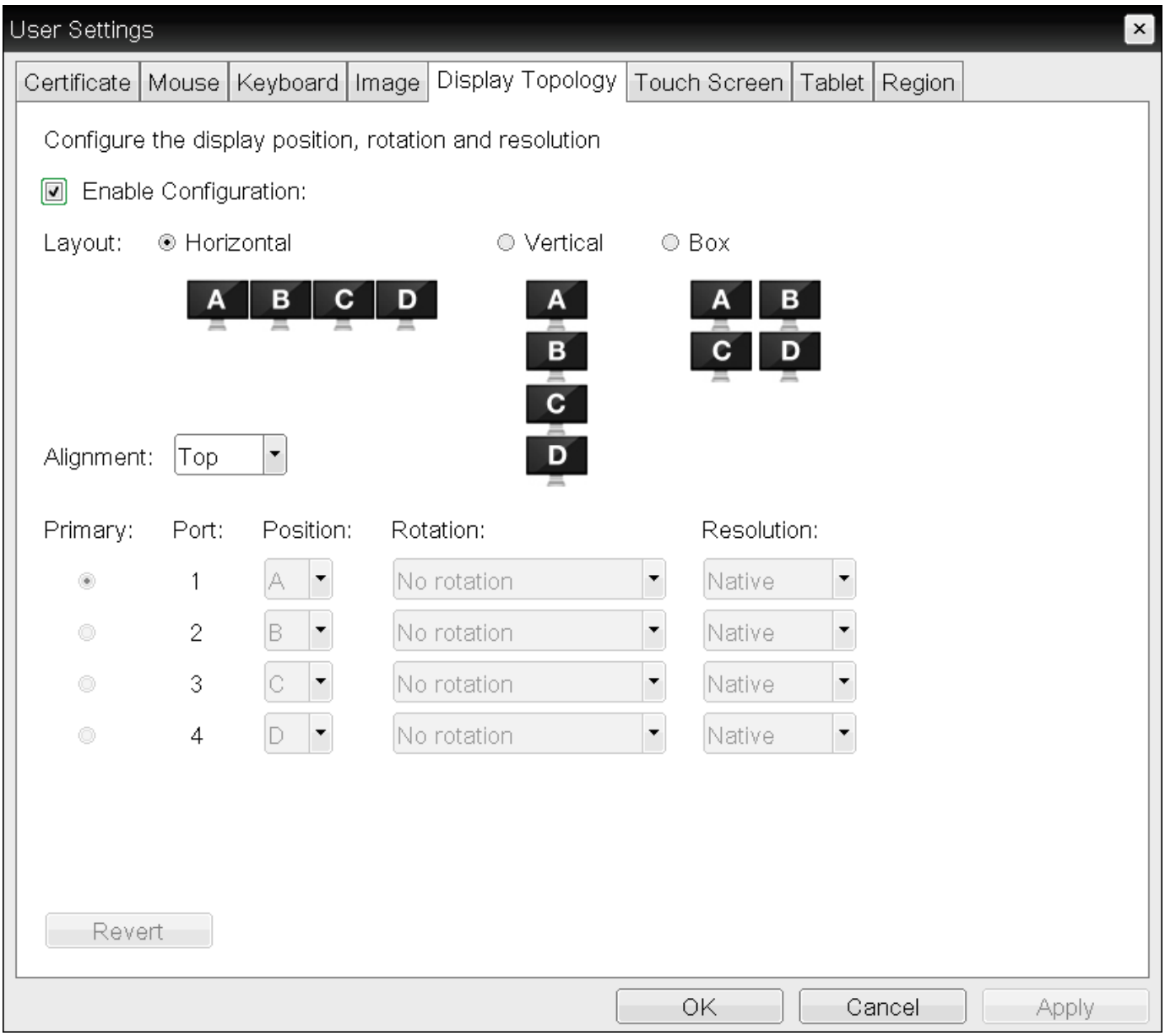
Parameter	Description
Primary	Configure which video port on the Tera2 PCoIP Zero Client you want as the primary port. **The display that is connected to the primary port becomes the primary display** (that is, the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1:** Select to configure port 1 on the Tera2 PCoIP Zero Client as the primary port. • **Port 2:** Select to configure port 2 on the Tera2 PCoIP Zero Client as the primary port.
Position	Specify which display is physically connected to each port.
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a Tera2 PCoIP Zero Client. The Tera2 PCoIP Zero Client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

To configure display settings:

1. From the OSD, select **Options > User Settings > Display Topology**.
2. From the OSD ***Display Topology*** page, configure the settings for the attached displays.
3. Click **OK**.

Configuring Four Displays

If your Tera2 PCoIP Zero Client supports four attached displays, The OSD ***Display Topology*** page, as shown next, enables you to configure the display topology for the attached displays.



OSD Display Topology page (for four displays)

The following parameters display on the OSD *Display Topology* page:

Display Topology Parameters (Four-Display Configuration)

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.

Parameter	Description
Display Layout	Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk. • **Horizontal:** Select to arrange displays horizontally, as indicated in the diagram. • **Vertical:** Select to arrange displays vertically, as indicated in the diagram. • **Box:** Select to arrange displays in a box formation, as indicated in the diagram.
Alignment	Select how you want displays aligned when they are different sizes. This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout:** • **Top:** Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center:** Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom:** Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout:** • **Left:** Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center:** Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right:** Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.

Parameter	Description
Primary	Configure which video port on the Tera2 PCoIP Zero Client that you want as the primary port. The display that is connected to the primary port becomes the primary display (that is, the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1:** Select to configure port 1 on the Tera2 PCoIP Zero Client as the primary port. • **Port 2:** Select to configure port 2 on the Tera2 PCoIP Zero Client as the primary port. • **Port 3:** Select to configure port 3 on the Tera2 PCoIP Zero Client as the primary port. • **Port 4:** Select to configure port 4 on the Tera2 PCoIP Zero Client as the primary port.
Position	Specify which display is physically connected to each port.
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a Tera2 PCoIP Zero Client. The Tera2 PCoIP Zero Client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

To configure display settings:

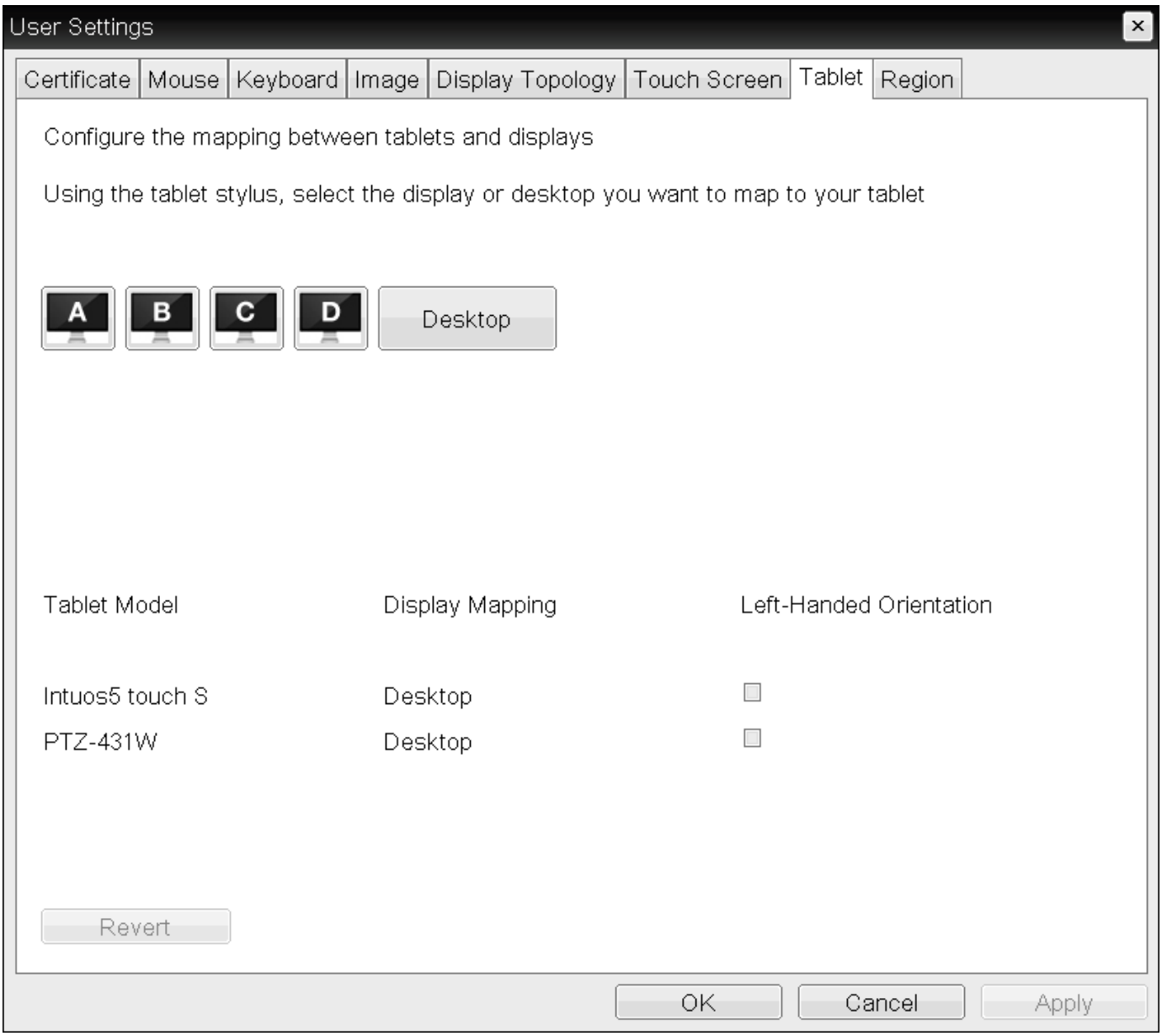
1. From the OSD, select **Options > User Settings > Display Topology**.
2. From the OSD *Display Topology* page, configure the settings for the attached displays.
3. Click **OK**.

Configuring Tablet Settings

Setting	Default	AWI	OSD	Management Console
Select display or desktop to map to tablet	–	✗	✓	✗
Left-handed orientation	Disabled	✗	✓	✗
Revert (a button)	–	✗	✓	✗

From the OSD ***Tablet*** page, you can select whether to map an attached Wacom tablet to the entire desktop or to a specific attached monitor. You can also specify whether the tablet operates in a left-handed or right-handed orientation.

The OSD ***Tablet*** page, as shown next, updates automatically to show the number of monitors and tablets that are connected to the Tera2 PCoIP Zero Client. You can connect up to four monitors, but your Tera2 PCoIP Zero Client only supports two locally connected tablets at a time. When just one monitor is attached, only the Desktop icon displays on the screen, and any attached tablets are mapped to the entire desktop. By default, tablets are mapped to the entire desktop.



OSD Tablet page

Changing display topology settings clears the tablet mappings

Changing topology settings on the Display Topology page (for example, after you rearrange your display setup) automatically clears the tablet mappings. You need to reconfigure your tablet setup whenever you apply topology changes. For information about configuring display topology, see Configuring Multiple Displays.

Tablet settings only apply in certain environments and setups

Tablet settings only apply when a Wacom tablet is attached to a Tera2 PCoIP Zero Client that is connected to a remote Linux workstation, and the local tablet driver feature is enabled in the remote workstation's Remote Workstation Card Software (PCoIP Host Software for Linux, version 4.5.0 or later). When enabled, this driver locally renders the cursor when its movement is initiated by the tablet. This feature is useful in WAN environments to help lessen the effects of high network latency. For more information, see the PCoIP® Host Software for Linux User Guide

The following parameters display on the OSD Tablet page:

OSD Tablet Parameters

Parameter	Description
Display and Desktop icons	This section shows the number of displays that are currently attached to the Tera2 PCoIP Zero Client. When just one monitor is attached, only the **Desktop** icon appears in this area, and any attached tablets are mapped to the entire desktop.
Tablet Model	Shows the model number of each attached Wacom tablet.
Display Mapping	Shows the current mapping configuration for each attached tablet (**A, B, C,** or **D,** or **Desktop**). You can map more than one attached tablet to the desktop or to the same display, or you can map each attached tablet to a different display.
Left-Handed Orientation	Configures the tablet for a left-handed orientation. Select the check box for a left-handed orientation. Clear the check box for a right-handed orientation.
Revert	Reverts the tablet settings to the last applied configuration.

To configure tablet settings:

1. From the OSD, select **Options > User Settings > Tablet**.
2. From the OSD *Tablet* page, configure the tablet settings:
    - To map a tablet to a display, use the tablet's stylus to tap the desired display icon (**A, B, C,** or **D**) on the screen, and then click **Apply**. The **Display Mapping** column will update with your selection.

- To configure the tablet for a left-handed orientation, use either a mouse or the tablet's stylus to select the tablet's **Left-Handed Orientation** check box, and then click **Apply**. Rotate the tablet 180° before using it. Clear the check box for a right-handed orientation.
- To revert mappings to the last applied configuration, click **Revert**.
- To return to the default tablet mappings (**Desktop**), unplug a monitor and reconnect it to the Tera2 PCoIP Zero Client. Applying topology settings (see Configuring Multiple Displays) will also clear the tablet configuration and reset it to the default configuration. You need to reconfigure your tablet setup whenever you apply topology changes.

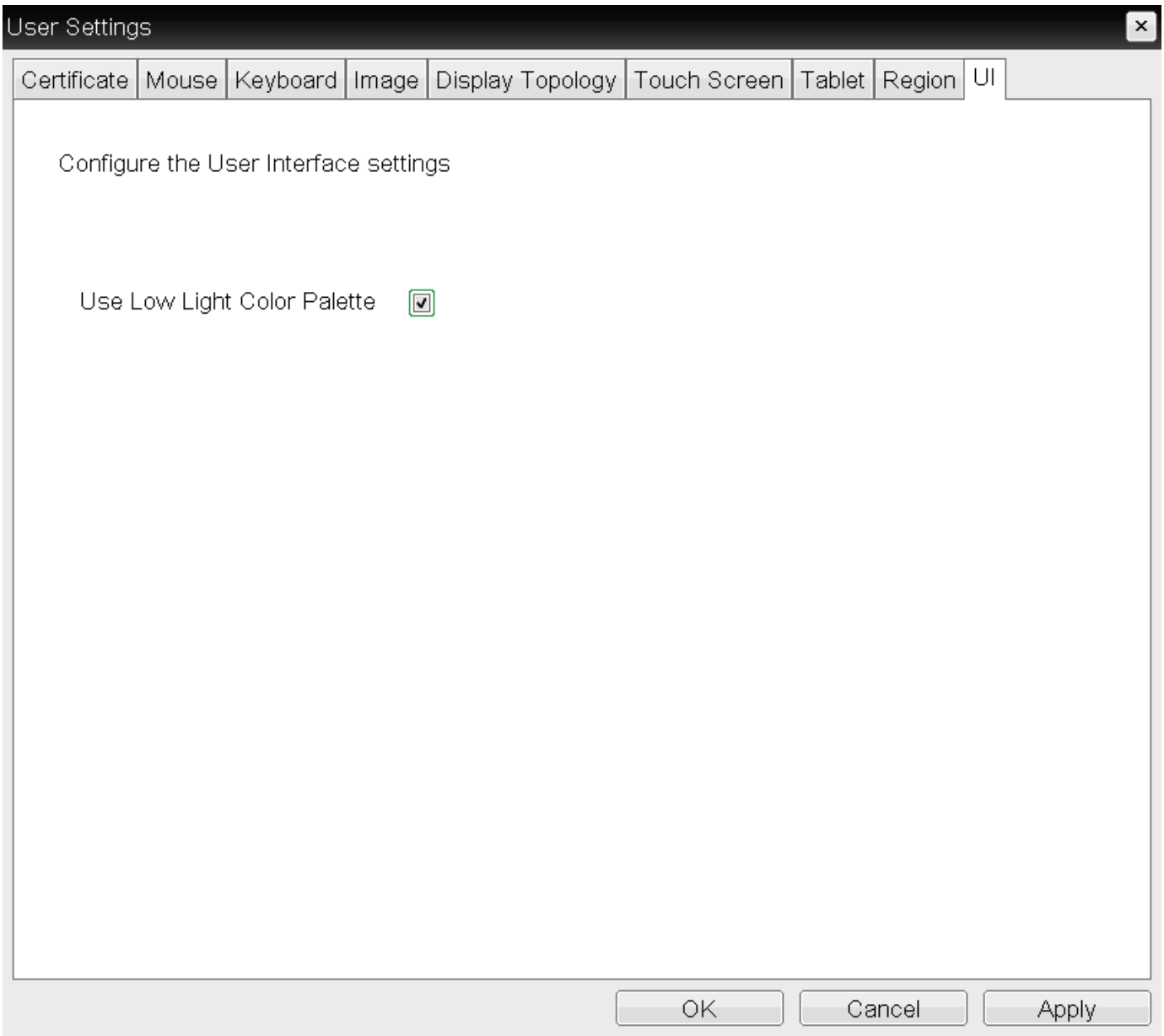
3. Click **OK**.

Configuring User Interface

The User Interface tab of the On Screen Display (OSD) allows you to change the color palette of the OSD making the OSD appear less bright to accommodate low light environments. This setting can be locked or removed by the PCoIP Management Console.

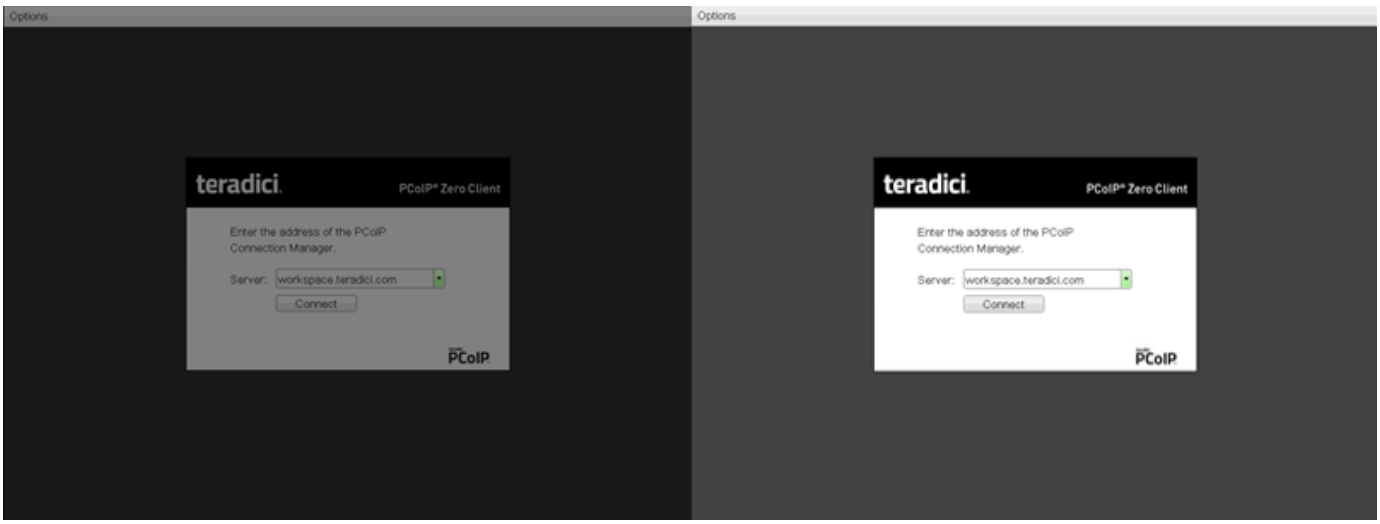
Processor Reset

Changes to this setting requires a PCoIP Processor reset before the change takes effect.



Low Light Setting

The image below shows the difference in brightness when using the low light setting.


Options
teradici
PCoIP® Zero Client
Enter the address of the PCoIP Connection Manager.
Server:
workspace.teradici.com
Connect
PCoIP
Options
teradici
PCoIP® Zero Client
Enter the address of the PCoIP Connection Manager.
Server:
workspace.teradici.com
Connect
PCoIP

Configuring 802.1X Network Device Authentication

Setting	Default	AWI	OSD	Management Console
Enable 802.1X security	–	✔	✔	✔
Identity	–	✔	✔	✔
Authentication	TLS (this is the only available setting)	✔	✖	✖
Client Certificate	–	✔	✔	✔
Enable 802.1X Support for Legacy Switches	–	✔	✖	✔

This section describes the components you need to configure 802.1X authentication, and the detailed steps you need to follow to configure the authentication. The instructions provided in this topic were done on a Microsoft Windows Server 2019 Datacenter. If you are performing these instructions from a different version of Microsoft Server, or another OS, you will have to consult your server documentation for any changes in procedures.

Preparing for 802.1X Configuration

The supported 802.1X configuration has the PCoIP Zero Client pre-populated with a proper certificate. It then connects and presents the certificate to the 802.1X switch and is authenticated. PCoIP Zero Clients will also connect under a different configuration of the switch which has the MAC address of authorized endpoints stored in it's configuration.

Using certificates to sign other certificates

If a certificate is used to sign another certificate, it must have the digitalSignature key usage field enabled.

Before you begin the configuration process, make sure you have these components:

- Tera2 PCoIP Zero Client with firmware 5.x or newer
- PCoIP Management Console 2 or newer
- Windows Server 2019 with AD DS (Active Directory Domain Services)
- Windows Server 2019 with AD CS (Active Directory Certificate Services)
- Windows Server 2019 with NPS (Network Policy and Access Services)
- A switch with 802.1X support configured

Configuring Devices for 802.1X Authentication

To configure 802.1X device authentication, complete the following steps:

1. Create a 802.1X Client User.
2. Export the Root CA Certificate.
3. Create a Certificate Template for 802.1X Client Authentication.
4. Issue the 802.1X Client Certificate.
5. Export the 802.1X Client Certificate.
6. Convert the Certificate Format from .pfx to .pem.
7. Import the 802.1X Client Certificate into the Client User Account.
8. Import the Certificates to the 802.1X Client Device.

The following sections assume you are using Windows Server 2019 Datacenter

The instructions in the following sections are based on Windows Server 2019 Datacenter. If you are using a newer version of Windows Server, the steps may vary slightly.

Create a 802.1X Client User

In the Windows server, create a 802.1X client user.

Create a 802.1X Client User

1. Log in to the Windows server.
2. Click **Start > Windows Administrative Tools > Active Directory Users and Computers**.
3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > <your_domain.local> > Users**.
4. Right-click Users, select **New > User**, and follow the wizard.
   (Example: Create a user called pcoip_endpoint which would have a UPN name of pcoip_endpoint@<mydomain.local>)

Export the Root CA Certificate

In the Certificate Authority (CA) server, export the root CA certificate.

To export the root CA certificate:

1. Log in to the Certificate Authority (CA) server.
2. Open a Microsoft Management Console window (for example,enter **mmc.exe** in the **Start** menu search field).
3. From the console window, select **File > Add/Remove Snap-in**.
4. Add the **Certificates** snap-in, selecting **Computer account** and then **Local computer**.
5. Click **OK** to close the *Add or Remove Snap-ins* dialog.
6. From the console, select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
7. In the right panel, right-click the certificate, and select **All Tasks > Export**.
8. Follow the wizard to export the certificate:
   a. Select **Base-64 encoded X.509 (.CER)** and click **Next**.
   b. Click **Browse**, specify a name and location for the certificate, and then click **Save**.
   c. Click **Finish**, and then click **OK**.

Create a Certificate Template for 802.1X Client Authentication

In the CA Server, create a certificate template for client authentication.

To create a certificate template for client authentication:

1. From the CA Server, click **Start > Administrative Tools > Certification Authority**.
2. Expand the tree for your CA.
3. Right-click **Certificate Templates**, and then click **Manage**.
4. Right-click the *Computer* template, and then click **Duplicate Template**.
5. Configure the template as follows:
    a. From the *Compatibility* tab, select **Windows Server 2003**.
    b. From the *Extensions* tab, ensure the **Digital signature** is included in the certificate **Key Usage**
    c. From the *General* tab, enter a name for the template (for example, **PCoIP Endpoint 802.1X**) and change the validity period to match the organization's security policy.
    d. From the *Request Handling* tab, select **Allow private key to be exported**.
    e. From the *Subject Name* tab, select **Supply in the request** and then click **OK**.
    f. From the *Security* tab, select the user who will be requesting the certificate, and give **Enroll** permission to this user.
    g. Click **OK** and close the *Certificate Templates Console* window.
6. From the *Certification Authority* window, right-click **Certificate Templates**, select **New**, and then click **Certificate Template to Issue**.
7. Select the certificate you just created (that is, **PCoIP Endpoint 802.1X**), and then click **OK**. The template will now appear in the *Certificate Templates* list.
8. Close the window.

Issue the 802.1X Client Certificate

From the CA Web Enrollment interface for the certificate server, issue the client certificate.

To issue the 802.1X client certificate:

Use Internet Explorer to log in to certificate server

Do not use any other browser except Internet Explorer to log into the certificate server or some options may not appear.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format **https://<server&tgt/certsrv/** (for example, https://ca.domain.local/certsrv/).
2. Click **Request a certificate** and then click **advanced certificate request**.
3. Click **Create and submit a request to this CA**.
4. From the pop-up window, click **Yes**.
5. Fill out the *Advanced Certificate Request* form as follows:
   a. In the *Certificate Template* section, select the certificate for clients (for example, **PCoIP Endpoint 802.1X**).
   b. In the *Identifying Information for Offline Template* section, enter the account name in the *Name* field. The other fields are not required.
   The other fields are not required.

      Enter the same name as the universal principal name of the client user

      The name you enter in the *Name* field must be the universal principal name (UPN) of the client user you created in Create a 802.1X Client User(for example, **pcoip_endpoint@mydomainlocal**)

   c. In the *Key Options* section, check **Mark keys as exportable**.
   d. In the *Additional Options* section, set the Request Format to **PKCS10**.
   e. If desired, enter a name in the *Friendly Name* field.
   f. Click **Submit**.
   g. From the *Certificate Issued* window, click the **Install this certificate** link.
   (This will save the certificate in the **Current User > Personal** store.)

Export the 802.1X Client Certificate

From the machine on which you issued the certificate, export the client certificate.

To export the client certificate:

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (for example, enter `mmc.exe` in the **Start** menu search field).
2. From the console window, select **File > Add/Remove Snap-in**.
3. Add the **Certificates** snap-in, selecting **My user account**.
4. Click **Finish**, and then click **OK** to close the *Add or Remove Snap-ins* dialog.
5. Select **Certificates - Current User > Personal > Certificates**.
6. In the right panel, right-click the certificate, and select **All Tasks > Export**.
7. Follow the Certificate Export wizard to export the certificate by clicking **Next**:
    a. Click **Yes, export the private key**.
    b. Select **Personal Information Exchange - PKCS #12 (.PFX)**.
    c. Enter a password for the certificate.
    d. Click **Browse**, specify a name and location for the certificate, and then click **Save**.
    e. Click **Next**, **Finish**, and then click **OK**.
8. Repeat Steps 5 to 7 again to export the PCoIP endpoint certificate, but this time without the private key (**No, do not export the private key**), selecting the **DER encoded binary X.509 (.CER)** format instead of the PKCS format.
9. Save this `.cer` file to a location where it can be accessed by the Domain Controller and imported into Active Directory.

Convert the Certificate Format from .pfx to .pem

Using OpenSSL, convert the certificate format from .pfx to .pem.

To convert the certificate format from .pfx to .pem:

1. Download and install Windows OpenSSL from https://www.slproweb.com/products/Win32OpenSSL.html. (The light version is sufficient.)
2. Copy the **.pfx** client certificate file you saved above to the **C:\OpenSSL-Win32\bin** directory.

3. Open a command prompt window (C:\OpenSSL-Win32\bin), and enter the following command to convert the certificate format from **.pfx** to **.pem** where ***<client_cert>*** is the name of the **.pfx** certificate file you saved to your local machine.

   ```
   openssl.exe pkcs12 -in <client_cert>.pfx -out <client_cert>.pem -nodes
   ```

4. When prompted, enter the password for the certificate file.
5. At the command prompt, enter the following command to create an RSA private key file where is the name of the .pem certificate file you created in the previous step.

   ```
   openssl.exe rsa –in <client_cert>.pem –out < client_cert>_rsa.pem
   ```

6. In Notepad:
   a. Open both the original .pem file and the RSA .pem file you just created. The RSA **.pem** file contains only an RSA private key. Because the PCoIP Endpoint certificate requires its private key in RSA format, you need to replace its private key with this RSA private key.
   b. Copy the entire contents of the RSA .pem file (everything from `-----BEGIN RSA PRIVATE KEY -----` to `-----END RSA PRIVATE KEY-----`), and paste it into the original .pem file, replacing its private key with this RSA private key.

      RSA .pem file

      In other words, make sure that all the text from `-----BEGIN PRIVATE KEY-----` to `-----END PRIVATE KEY` (including the dashes) in the *original .pem* file is replaced with the contents of `-----BEGIN RSA PRIVATE KEY -----` to `-----END RSA PRIVATE KEY-----` (including the dashes) from the RSA .pem file.

   c. Save the original **.pem** file and close it. The certificate is now ready to be uploaded to the PCoIP Endpoint.

Import the 802.1X Client Certificate into the Client User Account

In the Windows Domain Controller, import the client certificate into the client user account.

To import the 802.1X client certificate into the client user account:

1. Log in to the Windows Domain Controller.
2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. From the **View** menu, select **Advanced Features**.

4. Navigate to the user you created for the PCoIP Endpoint.
5. Right-click the user, and select **Name Mappings**.
6. In the ***X.509 Certificates*** section, click **Add**.
7. Locate and select the PCoIP Endpoint certificate you exported that does not contain the private key (This file was saved to a network location in step 9 of Export the 802.1X Client Certificate.)
8. Make sure both identity boxes are selected and click **OK**, and then click **OK** again.

Import the Certificates to the 802.1X Client Device

From the PCoIP endpoint's AWI, import the certificates.

To import the certificates into a profile using the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the PCoIP Endpoint.
2. From the AWI, select **Upload > Certificate**.
3. Upload both the Root CA certificate and the certificate with the private key, using the Browse button to locate each certificate and the Upload button to upload them.
4. From the OSD or AWI, select **Configuration > Network**.
5. Select **Enable 802.1X Security**.
6. Click **Choose** beside the ***Client Certificate*** field.
7. Select the certificate with the private key, and then click **Select**.
8. Enter the identity name of the certificate. Typically, this is the universal principal name (UPN) that appears after Subject: (for example, **pcoip_endpoint@mydomain.local**).

> **Windows server may be configured to use the certificate's Subject, the Subject Alternative Name, or another field**
>
> For the identity name, your Windows server may be configured to use the certificate's ***Subject***, the ***Subject Alternative Name***, or another field. Check with your administrator.

9. To enable greater 802.1X compatibility for older switches on the network, select **Enable 802.1X Support for Legacy Switches**. This setting is only available from the PCoIP endpoints AWI *Network* page.
10. Click **Apply**, and then click **Reset**.

> **Getting more information about 802.1X**
>
> For more information about 802.1X, see the following Knowledge Base articles, available from the Teradici Support Center:
>
> - Do PCoIP Zero Clients and PCoIP Remote Workstation Cards support network authentication or 802.1X? (KB 1357)
> - How to set up Windows Server 2008 R2 as an 802.1X Authentication Server (KB 1336)
> - PCoIP Troubleshooting Steps: IEEE 802.1X Network Authentication (KB 1088)

To disable 802.1X authentication on your endpoint:

Disabling 802.1X requires the deselection of the **Enable 802.1X Security** option in the AWI **Configuration > Network** page. It is also recommended that you remove all 802.1X certificates from the endpoint certificate store.

1. Using the AWI browse to **Configuration > Network**.
2. De-select **Enable 802.1X Security**.
3. Browse to **Upload > Certificate**.
4. Select the **Remove** button beside all 802.1X certificates.
5. Click on the **Apply** button.

Configuring Display Override Settings

Under normal operation, the GPU in the host computer queries a monitor attached to the PCoIP Zero Client to determine the monitor's capabilities. These are reported in the Extended Display Identification Data (EDID) information. In some situations, a monitor may be connected to a client in a way that prevents the client from reading the EDID information, such as when connecting through certain devices, such as keyboards and mice. You can configure the **Enable Attached Display Override** feature to enable the client to advertise default EDID information to the host's processor.

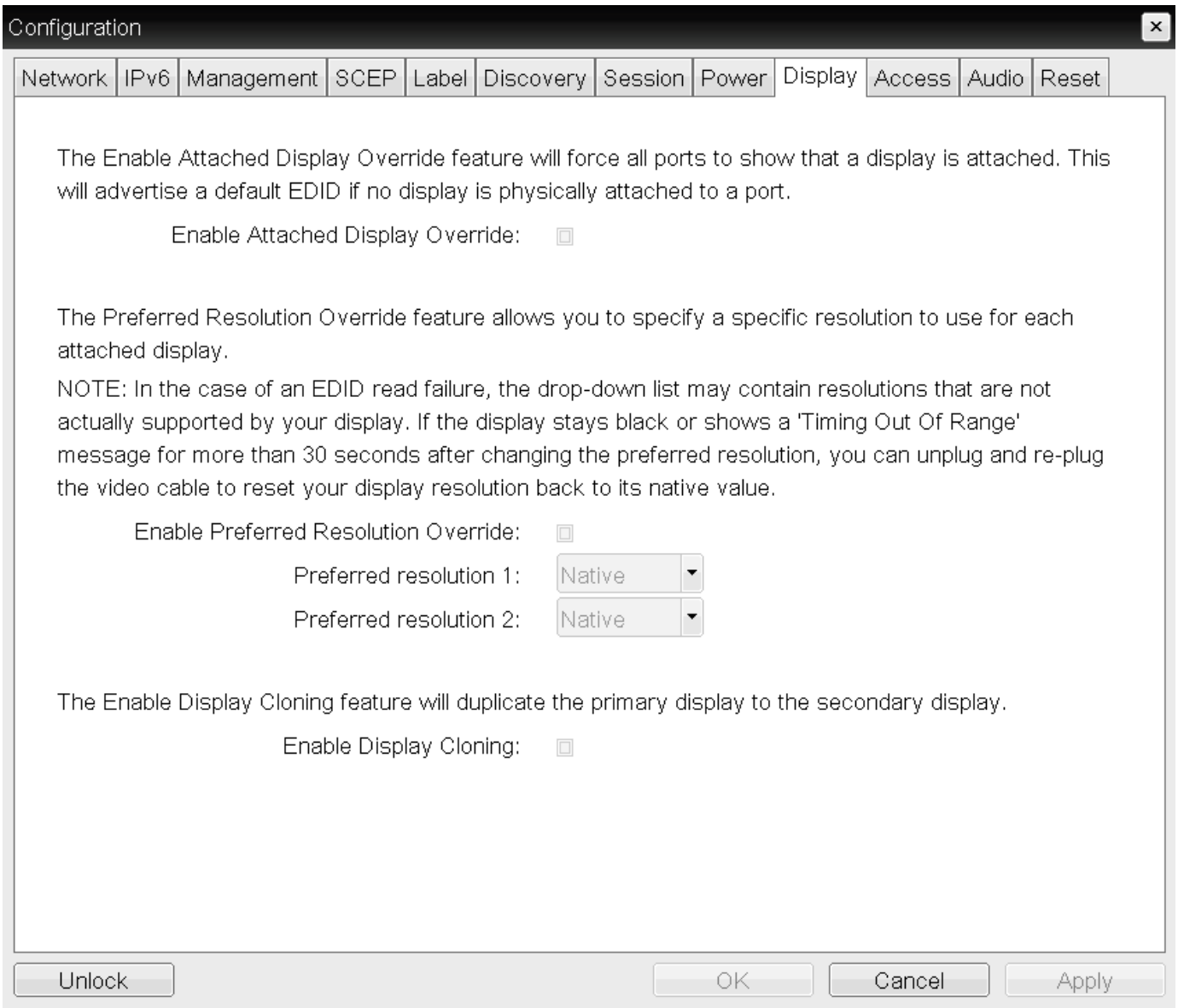
You can configure display override settings for a dual monitor or quad monitor setup.

Setting	Default	AWI	OSD	Management Console
Enable Attached Display Override	–	✗	✓	✓
Enable Preferred Resolution Override	–	✗	✓	✓
Enable Display Cloning [1]	–	✗	✓ (TERA2321)	✓ (TERA2321)

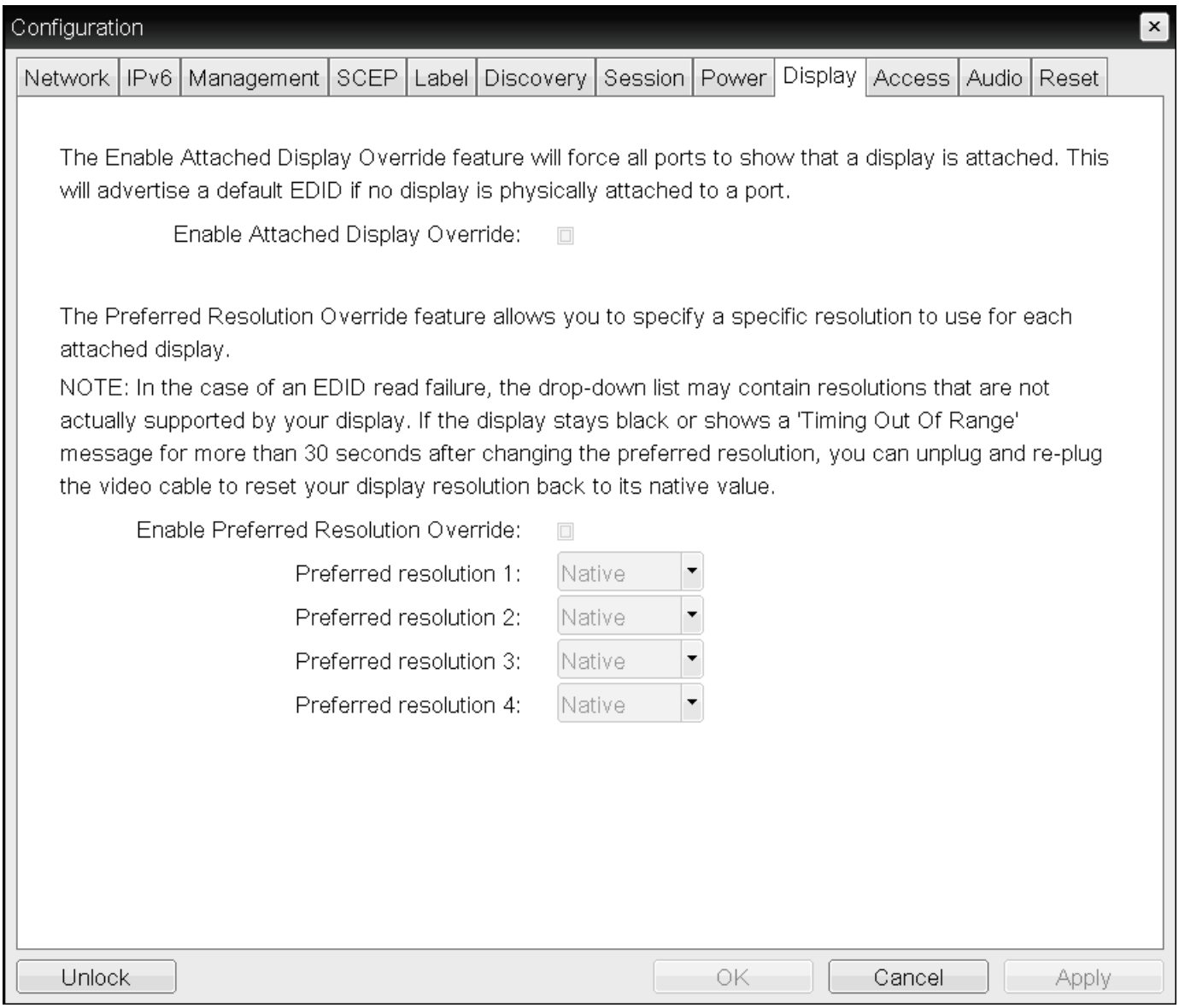
Setting not available

Display Cloning is ***not*** a supported feature on PCoIP Zero Client quad models (TERA2140).

From the OSD ***Display*** page, you can enable the Extended Display Identification Data (EDID) override mode for a setup with two or four attached displays.



TERA232 OSD Display page (dual display models)



TERA2140 OSD Display page (quad display models)

Activate the Enable Attached Display Override feature when there is no valid EDID information

Only activate the **Enable Attached Display Override** feature when there is no valid EDID information and your monitor display characteristics are understood. In the case of an EDID read failure, the list may contain resolutions that are not actually supported by your display. If the Enable Attached Display Override feature is not enabled, and the display stays black or shows a **Timing Out of Range** message for more than 30 seconds after you activate **Enable Preferred Resolution Override:** and set a **Preferred resolution**, you can unplug and re-plug the video cable to reset your display resolution back to its previous value (that is, perform a hot plug reset).

Performing a hot plug reset won't revert the display for a custom resolution

If you have set a custom resolution, performing a hot plug reset will not cause the display to revert to its previous resolution if both **Enable Attached Display Override** and **Enable Preferred Resolution Override** are activated at the same time. If you want to retain your custom resolution in the event of a hot plug (or power outage, and so on), ensure that both these fields are activated.

The following parameters display on the OSD Display page:

Display Parameters

Enable Attached Display Override

This option is intended for legacy systems. It configures the Tera2 PCoIP Zero Client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. For Windows versions earlier than Windows 7, if the host didn't have EDID information, it would assume no monitors were attached. This option ensures that the host always has EDID information when the client is in a session.

The following default resolutions are advertised when this option is enabled:

- 3840x1440 @60 Hz
- 3840x2160 @30 Hz
- 3840x2160 @25 Hz
- 3840x2160 @24 Hz
- 2560x1600 @60 Hz
- 2560x1440 @60 Hz
- 2560x1080 @60 Hz
- 2048x1152 @60 Hz
- 1920x1440 @60 Hz
- 1920x1200 @60 Hz
- 1920x1080 @60 Hz
- 1856x1392 @60 Hz
- 1792x1344 @60 Hz
- 1680x1050 @60 Hz
- 1600x1200 @60 Hz
- 1600x900 @60 Hz
- 1440x900 @60 Hz
- 1400x1050 @60 Hz
- 1366x768 @60 Hz
- 1360x768 @60 Hz
- 1280x1024 @60 Hz
- 1280x960 @60 Hz
- 1280x800 @60 Hz
- 1280x768 @60 Hz
- 1280x720 @60 Hz
- 1024x768 @60 Hz
- 848x480 @60 Hz
- 800x600 @60 Hz
- 640x480 @60 Hz

Parameter	Description
Enable Preferred Resolution Override	Enable this option when a display is attached but can't be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions listed for the **Enable Attached Display Override** will be advertised, except that the display resolution you configure here will be sent as the native resolution, instead of the default native resolution of 1024x768. • **Preferred resolution 1:** Select the preferred resolution of the display connected to the Tera2 PCoIP Zero Client's port 1. • **Preferred resolution 2:** Select the preferred resolution of the display connected to the Tera2 PCoIP Zero Client's port 2. • **Preferred resolution 3:** Select the preferred resolution of the display connected to the Tera2 PCoIP Zero Client's port 3. • **Preferred resolution 4:** Select the preferred resolution of the display connected to the Tera2 PCoIP Zero Client's port 4. When you enable this option, all displays attached to the client will be set to their specified preferred resolution. **Caution: Performing a hot plug reset will not cause the display to revert to previous resolution.** If you have set a custom resolution, performing a hot plug reset will not cause the display to revert to its previous resolution if both **Enable Attached Display Override** and **Enable Preferred Resolution Override** are enabled at the same time. If you want to retain your custom resolution in the event of a hot plug (or power outage, and so on), ensure that both these fields are enabled.
Enable Display Cloning [1] (TERA2321 only)	Enable the display cloning option if you want the secondary display to mirror the primary display—for example, for digital signage or trainings.

Black screens when connecting a PCoIP Zero Client to a Remote Workstation Card

If you are connecting a TERA2321 PCoIP Zero Client to a remote workstation that does not have the Remote Workstation Card Software installed and the host driver function enabled, and you are using monitor emulation on the remote workstation, you may experience black screens on the cloned displays. To remedy the problem, you can either install and enable the Remote Workstation Card Software, or you can disable monitor emulation on the video port for the secondary display only.

To configure display override settings:

1. From the OSD, select **Options > Configuration > Display**.

2. From the *Display* page, update the display settings.
3. To save your updates click **OK**.

---

1. The **Enable Display Cloning** setting is only found on dual display PCoIP Zero Client models (TERA2321)

Performing Diagnostics

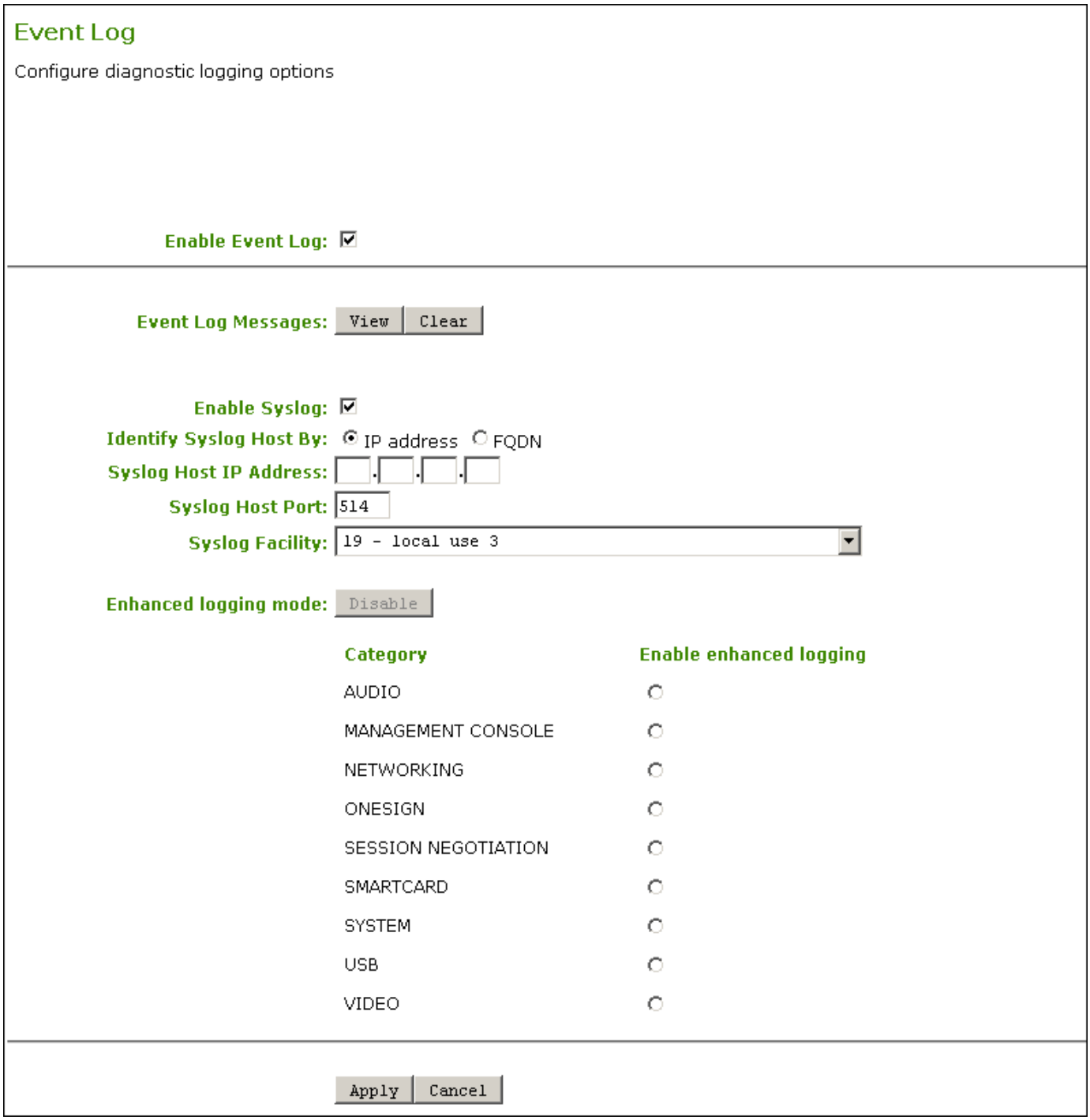
This section describes the tools you can use and the tasks you can perform to help you diagnose and troubleshoot issues with your Tera2 PCoIP Zero Client. Using diagnostic tools, you can also gather important information and statistics to help you optimize your environment and test your Tera2 PCoIP Zero Client's performance.

Configuring the Event Log and Syslog

Setting	Default	AWI	OSD	Management Console
Enable Event Log	Enabled	✔	✖	✔
Enable Syslog	Enabled	✔	✖	✔
Identify Syslog Host By	IP Address	✔	✖	✔
Syslog Host IP Address / Syslog Host DNS Name		✔	✖	✔
Syslog Host Port	514	✔	✖	✔
Syslog Facility	19 – local use	✔	✖	✔

To view and manage logs, as well as set up other logging options such as syslog and enhanced logging mode, you need to enable the event log.

You enable the event log, as well as syslog settings, from the AWI *Event Log* page, as shown next.



AWI Event Log page

Enabling Event Log

Enable the event log so that logging occurs in verbose mode. When you enable the event log, you can view event logs from the OSD and AWI, as well as access and configure other logging options, such as syslog and enhanced logging mode.

When you disable the event log, you won't be able to access logging options, all existing event logs will be deleted, and logging will be disabled. If you've configured syslog settings, logs won't be sent to the syslog server.

To enable the event log:

1. From the AWI, select **Diagnostics > Event Log**.
2. From the AWI *Event Log* page, select the *Enable Event Log* check box.
3. Click **Apply**.

Enabling Syslog

To configure syslog, you'll need to enable syslog, enter the IP address or Fully Qualified Domain Name (FQDN) for the syslog server, and specify the port number and facility to use to send messages to the syslog server.

Before you can enable syslog, you must enable the event log

Before you can access and configure syslog settings, you need to select the **Enable Event Log** check box (see Enabling Event Log).

Syslog default values

Teradici uses UDP to send syslog messages to a centralized syslog server. Because most servers use port 514 for incoming messages, Teradici recommends you configure port **514** (the default port number) as the syslog port. However, you can use a different port as long as the syslog server receives the syslog messages on the same port that the device sends the messages.

Teradici also uses **19 – local use 3** as the default facility because this facility isn't commonly used. If you use it, select a different facility.

Facility values used by Cisco equipment

Cisco IOS devices, CatOS switches, and VPN 3000 concentrators use the **23 – local use 7** facility.
Cisco PIX firewalls use the **20 – local use 4** facility.

Ensure that the syslog server can manage the volume of messages

Ensure that your syslog server can handle the volume of messages that the Tera2 PCoIP Zero Client sends. With certain free syslog servers, messages are lost if the volume is too great.

The following syslog settings display on the AWI Event Log page:

Syslog Parameters

Parameter	Description
Enable Syslog	Enable or disable the syslog standard as the logging mechanism for the device. **You must configure all fields when syslog is enabled.** If you enable syslog, you must configure the remaining fields. If you disable syslog, you can't edit the fields.
Identify Syslog Host By	Choose if the syslog server host is identified by its IP address or by its Fully Qualified Domain Name (FQDN).
Syslog Host IP Address / Syslog Host DNS name	The parameter that displays depends on which option you choose to identify the syslog server host: • **IP Address:** Enter the IP address for the syslog server host. • **FQDN:** Enter the DNS name for the syslog server host. If you enter an invalid IP address or DNS name, a message displays to prompt you to correct it.
Syslog Host Port	Enter the port number of the syslog server. The default port number is **514**.

Parameter	Description
Syslog Facility	The facility is a number attached to every syslog message. The number categorizes the source of the syslog messages. The facility is part of the standard syslog header and all syslog servers can interpret it. Enter a facility to suit your logging needs. For example, you could configure devices as follows: • Zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 The default facility is set to **19 – local use 3**. Cisco routers default to **23 – local use 7**.

Detailed information about the AWI Event Log page

For more information about the settings on the AWI Event Log page, including information about syslog settings, see Performing Logging Tasks.

To configure syslog settings:

1. From the AWI, select **Diagnostics > Event Log**.
2. From the AWI *Event Log* page, do the following:
   - Select the **Enable Syslog** check box.
   - For **Identify Syslog Host By**, select whether you want to identify the syslog server by its IP address or FQDN.
   - In the **Syslog Host IP Address / Syslog Host DNS Name** box(es), enter the IP address or FQDN of the syslog server.
   - If the syslog server is configured to receive data on a port other than 514, enter another port number in the **Syslog Host Port** box.
   - If you want the device to use a facility other than the default facility, select it from the Syslog Facility list.
   - Click **Apply**.
3. From the *Success* page, click **Continue**.

Performing Logging Tasks

Setting	Default	AWI	OSD	Management Console
Refresh (a button)	–	✗	✓	✗
Refresh (F5)	–	✓	✓	✗
Clear (a button)	–	✓	✓	✗
Enable Event Log	Enabled	✓	✓	✓
Enable Syslog	Enabled	✓	✗	✓
Enable Syslog Host By IP Address	–	✗	✓	✗
Syslog Host IP Address	–	✗	✓	✗
Syslog Host Port	514	✗	✓	✗
Syslog Facility	19 – local use 3	✓	✗	✗
Enhanced logging mode	Disabled	✗	✓	✗

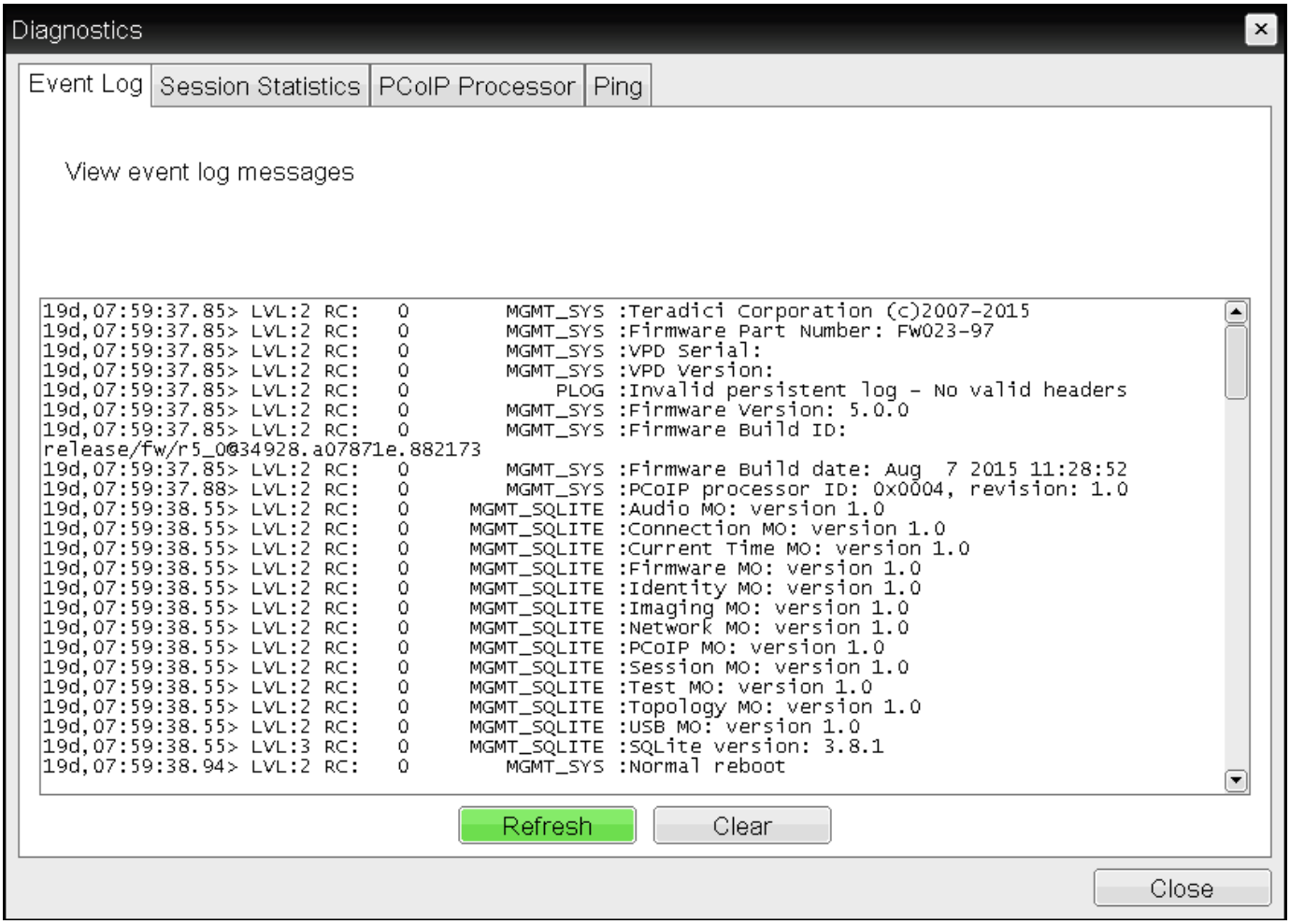
From the OSD and AWI, you can view and clear all the event log messages stored on your Tera2 PCoIP Zero Client.

From the AWI, you can perform additional logging tasks, including:

- Enabling or disabling logging.
- Enabling and configuring syslog as the logging protocol to use to collect and report events. (For more information about configuring syslog, see Configuring the Event Log and Syslog.)
- Enabling enhanced logging mode for specific components, such as USB or video components.

Performing Logging Tasks from the OSD

The OSD ***Event Log*** page, as shown next, enables you to view, refresh, and clear event log messages.



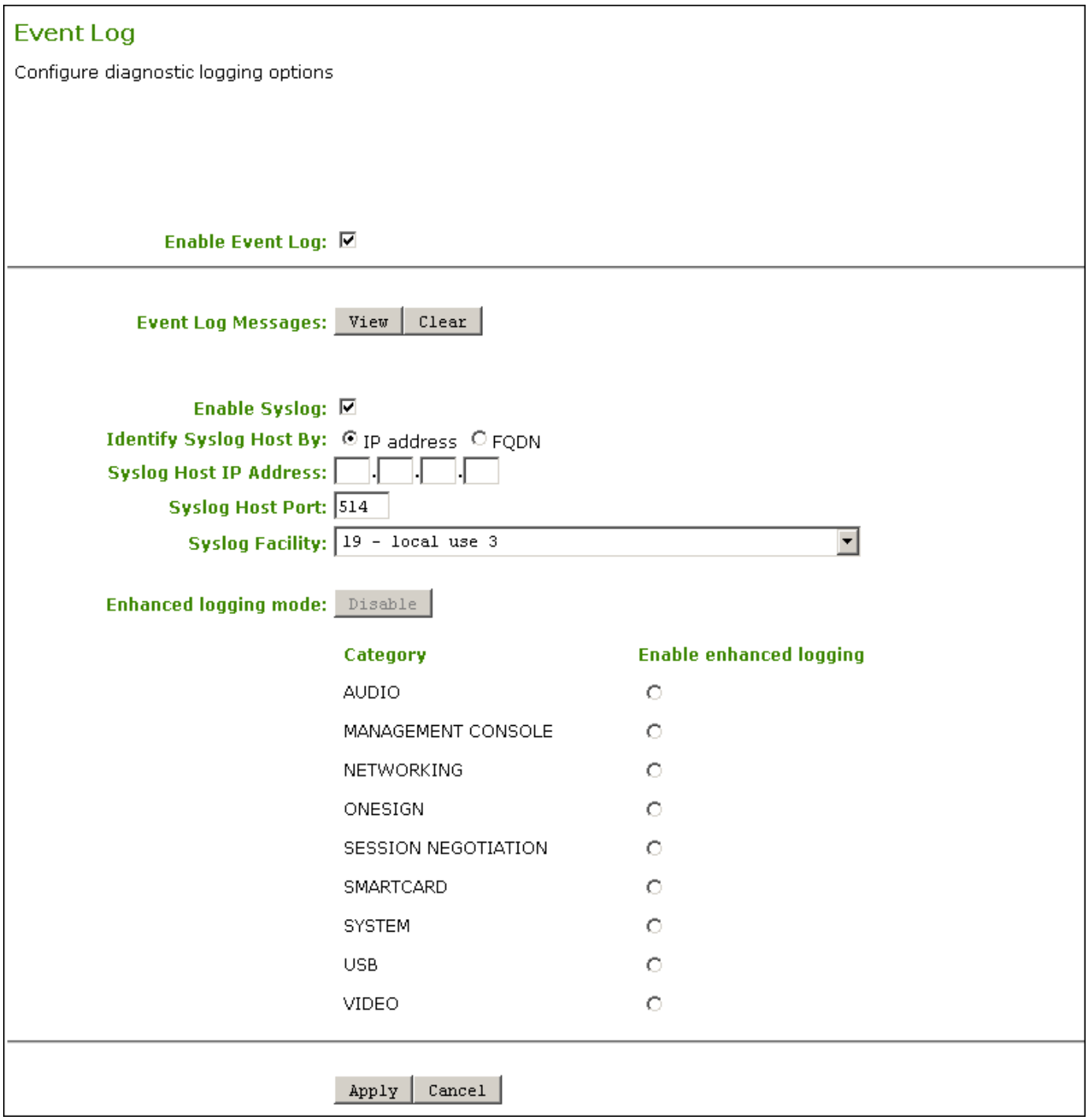
OSD Event Log page

To view or clear event log messages:

1. From the OSD, select **Options > Diagnostics > Event Log**.
2. From the OSD ***Event Log*** page, you can:
    a. View all the event log messages stored on the Tera2 PCoIP Zero Client.
    b. Click **Refresh** to refresh the log information displayed on the page.
    c. Click **Clear** to delete all the event log messages stored on the Tera2 PCoIP Zero Client.
    d. Click **Close**.

Performing Logging Tasks from the AWI

The AWI ***Event Log*** page, as shown next, enables you to enable or disable logging, view and clear event log messages, and set the log filtering mode. You can also enable and configure syslog as the logging protocol to use to collect and report events.



AWI Event Log page

The following parameters display on the AWI Event Log page.

AWI Event Log Parameters

Parameter	Description
Enable Event Log	When this feature is enabled, logging occurs in verbose mode, and all event log and syslog options display. When this feature is disabled, the logging options are hidden. Disabling the event log disables logging and deletes existing persistent event logs. If you configure syslog settings, logs won't be sent to a syslog server.
Event log Messages	• **View:** Click to open a browser page that displays the event log messages (with timestamp information) stored on the device. Press F5 to refresh the browser page log information. • **Clear:** Click to delete all event log messages stored on the device.
Enable Syslog	Enable or disable the syslog standard as the logging mechanism for the device. **Note: If you enable syslog, you must configure the remaining fields.** If you disable syslog, you can't edit the fields.
Identify Syslog Host By	Choose if the syslog server host is identified by its IP address or by its Fully Qualified Domain Name (FQDN).
Syslog Host IP Address / Syslog Host DNS name	The parameter that displays depends on which option you choose to identify the syslog server host: • **IP Address:** Enter the IP address for the syslog server host. • **FQDN:** Enter the DNS name for the syslog server host. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it.
Syslog Host Port	Enter the port number of the syslog server. The default port number value is 514.

Parameter	Description
Syslog Facility	The facility is a number attached to every syslog message. The number categorizes the source of the syslog messages. The facility is part of the standard syslog header and all syslog servers can interpret it. Enter a facility to suit your logging needs. For example, you could configure devices as follows: • Zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 The default facility is set to '19 – local use 3'. Cisco routers default to '23 – local use 7'.

Parameter	Description
Enhanced logging mode	If you require enhanced logging details in the event log to help troubleshoot a problem with a Tera2 PCoIP Zero Client or PCoIP Remote Workstation Card, select an enhanced logging category, and click **Apply > Continue**. (To return to normal logging mode, click **Disable**, and then **Apply > Continue**.) **Enhanced logging may be enabled for only one category at a time.** Enhanced logging mode messages can be located in the event log by their Level 3 (LVL:3) designation, which indicates a debug-level message. **Enhanced logging mode categories:** • **Audio:** Provides enhanced audio-related details, such as audio compression levels and audio bandwidth. Enable this mode if you are experiencing any problems with audio quality. • **Management Console:** Provides debug-level details for the connection state between the device and the MC. Enable this mode if you are having trouble connecting to or managing the device using the MC. • **Networking:** Provides socket-level details for a device's network connections. Enable this mode for network-related issues—for example, if the device cannot connect to a peer or broker, or if it cannot get an IP address from a DHCP server. • **OneSign:** Provides enhanced logging for connections using Imprivata's OneSign Single Sign-On proximity cards. Enable this mode to see debug-level messages between a device and a OneSign authentication server. • **Session Negotiation:** Provides pre-session messaging details, such as the full feature set advertised by each device. Enable this mode for low-level session negotiation details. • **SmartCard:** Provides debug-level messages for smart cards. Enable this mode if you experience trouble tapping or logging in using a smart card. • **System:** Provides heartbeat details about the device, such as ambient temperature. Enable this mode for system-level problems. • **USB:** Provides details of the traffic between the device and any connected USB devices. Enable this mode if you are experiencing problems with a connected USB device. • **Video:** Displays enhanced image-related logging information. Enable this mode for image problems, monitor problems, or display topology issues.

To perform Event Log tasks from the AWI:

1. From the AWI, select **Diagnostics > Event Log**.

2. From the AWI *Event Log* page, you can:
   - Select or clear the **Enable Event Log** check box.
   - View all the event log messages stored on the Tera2 PCoIP Zero Client.
   - Press F5 to refresh the browser page displaying the log information.
   - Click **Clear** to delete all the event log messages stored on the Tera2 PCoIP Zero Client.
   - In the *Syslog* section, enable and configure syslog settings.

     More information on configuring syslog

     For detailed instructions on configuring syslog settings, see Configuring the Event Log and Syslog.

   - In the *Enhanced Logging Mode* section, enable specific enhanced logging mode categories.
3. Click **Apply**.

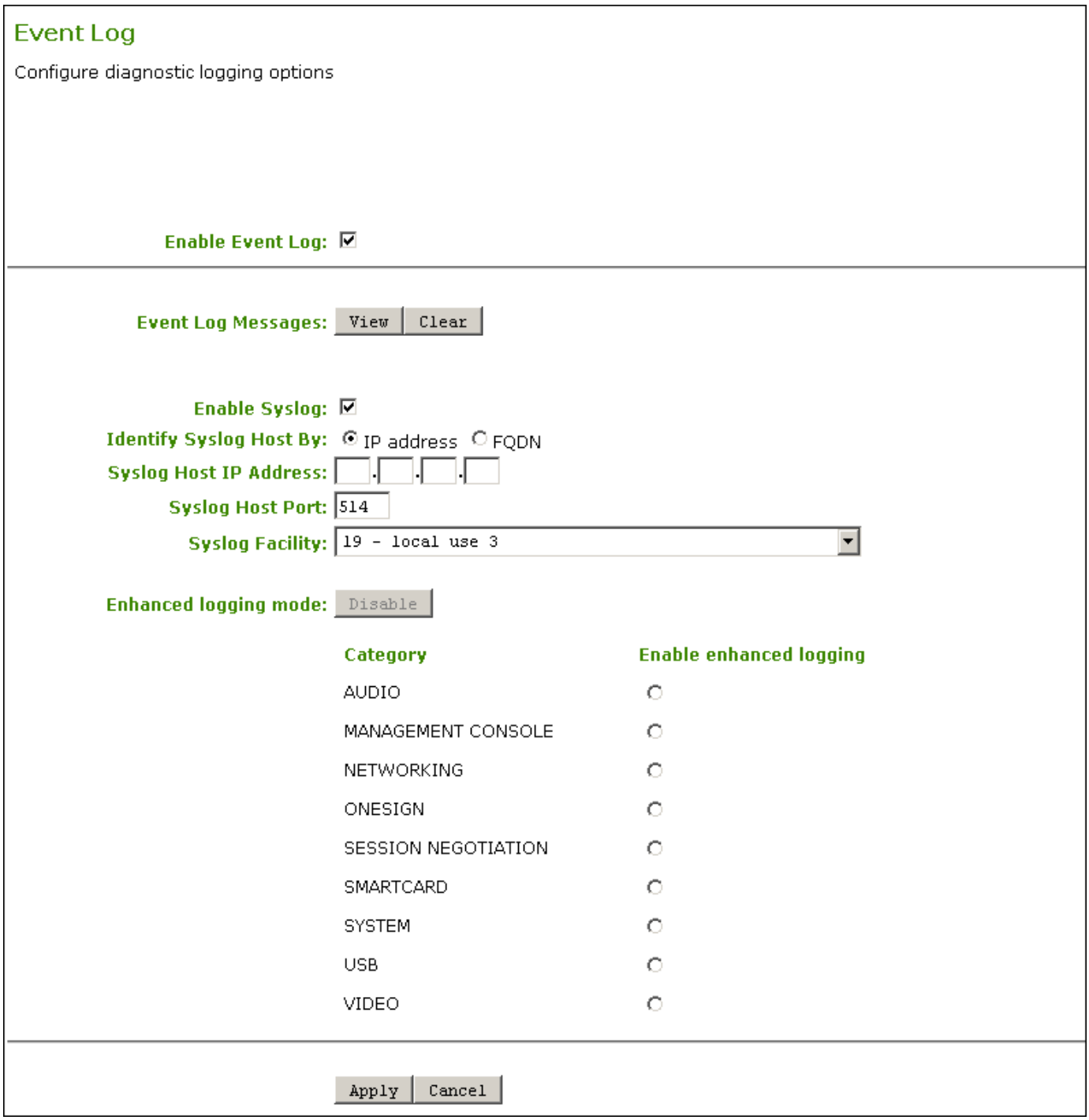
Configuring Enhanced Logging Mode

Setting	Default	AWI	OSD	Management Console
Enhanced logging mode	Disabled	✔	✖	✔

From the AWI ***Event Log*** page, as shown next, you can perform additional logging tasks, including enabling enhanced logging mode for specific components. Enabling this mode provides advanced information in the event log to help you troubleshoot issues you may encounter with specific devices (such as USB or video components).

Before you can enable enhanced logging mode, you must enable the event log

Before you can access and configure syslog settings, you need to select the Enable Event Log check box (see Configuring Enhanced Logging Mode).



AWI Event Log page

You can only enable enhanced logging for one category at a time

You can only apply enhanced logging mode to one category at a time. Enhanced logging mode messages display in the event log by their Level 3 (**LVL:3**) designation, which indicates a debug-level message.

At any given time, you can enable enhanced logging mode for any one of the following categories:

- **Audio:** Provides enhanced audio-related details, such as audio compression levels and audio bandwidth. Enable this mode if you experience issues with audio quality.
- **Management Console:** Provides debug-level details for the connection state between the device and the PCoIP Management Console. Enable this mode if have issues connecting to or managing the device using the PCoIP Management Console.
- **Networking:** Provides socket-level details for a device's network connections. Enable this mode for network-related issues—for example, if the device can't connect to a peer or broker, or if it can't obtain an IP address from a DHCP server.
- **OneSign:** Provides enhanced logging for connections using Imprivata's OneSign Single Sign-On proximity cards. Enable this mode to see debug-level messages between a device and a OneSign authentication server.
- **Session Negotiation:** Provides pre-session messaging details, such as the full feature set advertised by each device. Enable this mode for low-level session negotiation details.
- **SmartCard:** Provides debug-level messages for smart cards. Enable this mode if you experience issues tapping or logging in using a smart card.
- **System:** Provides heartbeat details about the device, such as ambient temperature. Enable this mode for system-level issues.
- **USB:** Provides details of the traffic between the device and any connected USB devices. Enable this mode if you are experiencing issues with a connected USB device.
- **Video:** Displays enhanced image-related logging information. Enable this mode for image, monitor, or display topology issues.

To enable enhanced logging mode:

1. From the AWI, select **Diagnostics > Event Log**.
2. From the AWI *Event Log* page, select an enhanced logging mode category.
   (To return to normal logging mode, click **Disable**.)
3. Click **Apply**.

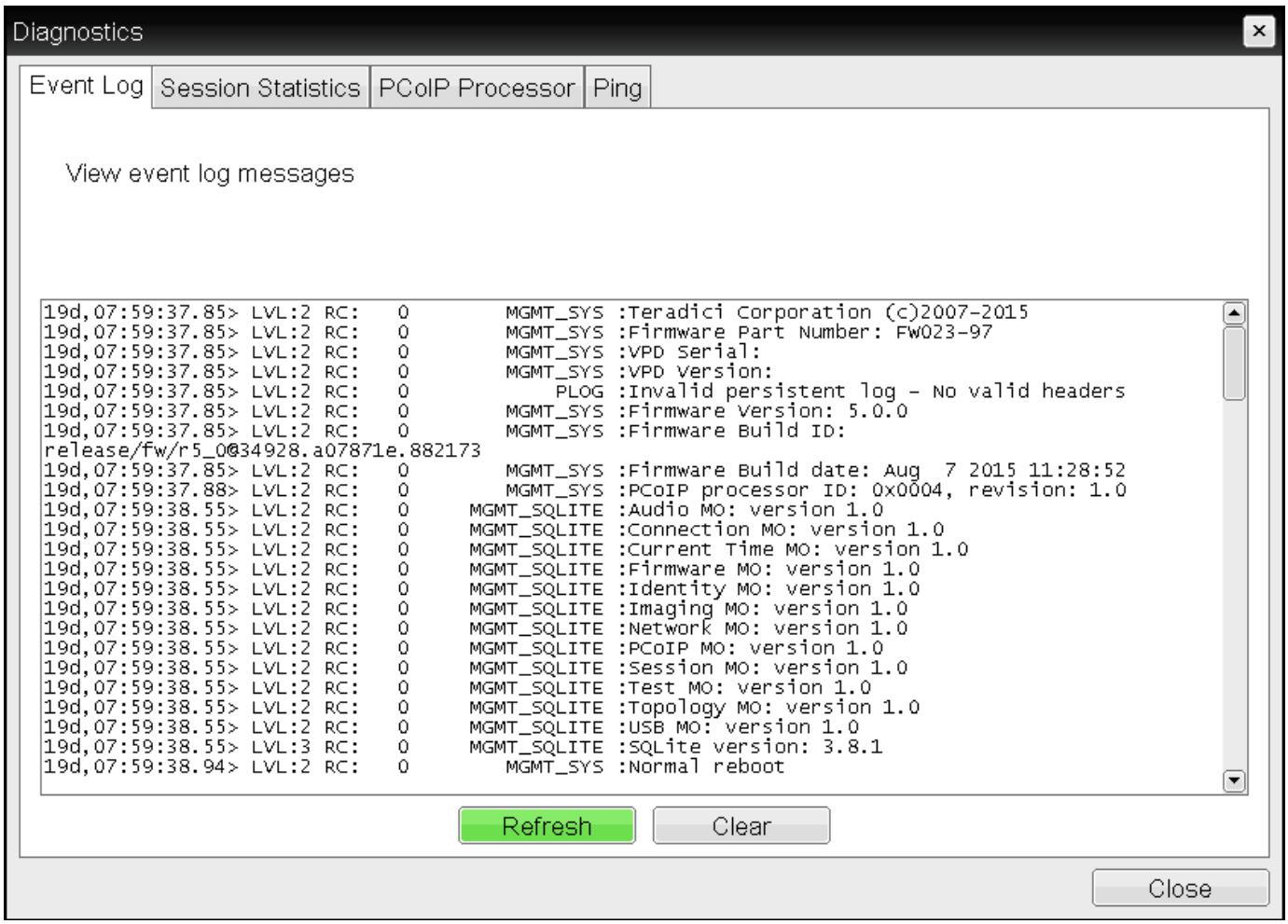
Viewing Event Logs

Setting	Default	AWI	OSD	Management Console
View (a button on the AWI, a list of messages on the OSD)	–	✔	✔	✘
Refresh (a button on the OSD, F5 from the AWI)	–	✔	✔	✘
Clear (a button)	–	✔	✔	✘

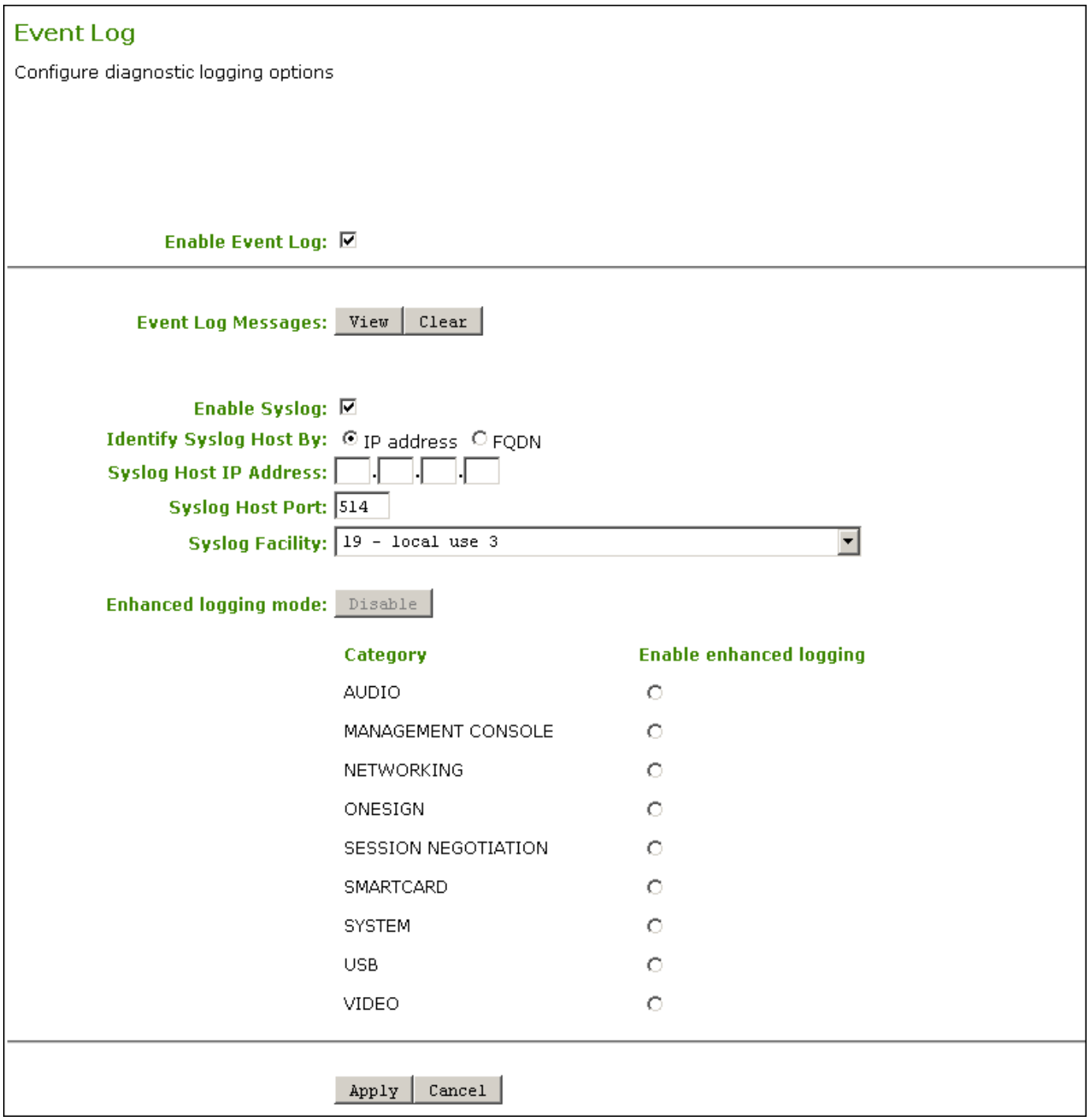
From the OSD and AWI Event Log pages, as shown next, you can view, refresh, and clear the event log messages stored on your Tera2 PCoIP Zero Client.

The event log must be enabled if you want to view event log messages

To view event log messages, make sure the event log is enabled. To enable the event log, see Viewing Event Logs).



OSD Event Log page



AWI Event Log page

To view, refresh, and clear event log messages from the OSD:

1. From the OSD, select **Options > Diagnostics > Event Log**.
2. From the OSD *Event Log* page, you can:
   - Scroll to view all the event log messages stored on the Tera2 PCoIP Zero Client.

- Click **Refresh** to refresh the information that displays on the page and view the most updated event log information.
- Click **Clear** to delete all the event log messages stored on the Tera2 PCoIP Zero Client.

3. Click Close.

To view, refresh, and clear event log messages from the AWI:

1. From the AWI, select **Diagnostics > Event Log**.
2. From the AWI *Event Log* page, you can:
   - Click **View** to open a browser page to display the event log messages (with time stamp information) stored on the Tera2 PCoIP Zero Client.
   - Press F5 to refresh the browser page displaying the log information.
   - Click **Clear** to delete all the event log messages stored on the Tera2 PCoIP Zero Client.
3. Click **Apply**.

Viewing and Resetting Session Statistics

Setting	Default	AWI	OSD	Management Console
Reset Statistics (button)	–	✔	✔	✖

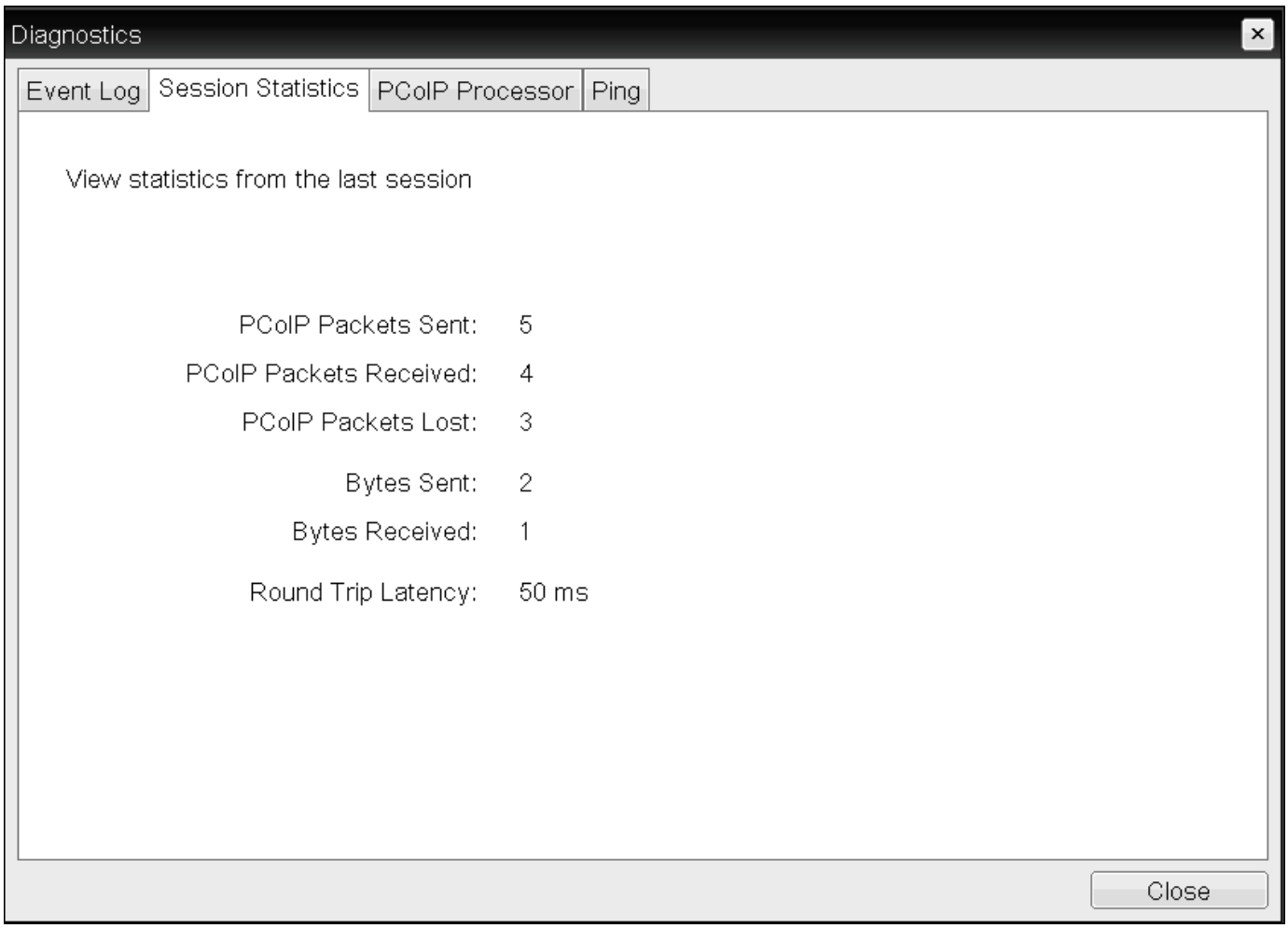
The OSD displays session statistics from the last PCoIP session.

The AWI displays session statistics for the current session. If a session isn't active, the AWI displays statistics for the previous PCoIP session.

You can view much more detailed statistical information from the AWI. In addition, you can reset the statistics for the current session from the AWI.

Viewing Session Statistics from the OSD

From the OSD ***Session Statistics*** page, as shown next, you can view statistics from the last session.



OSD Session Statistics page

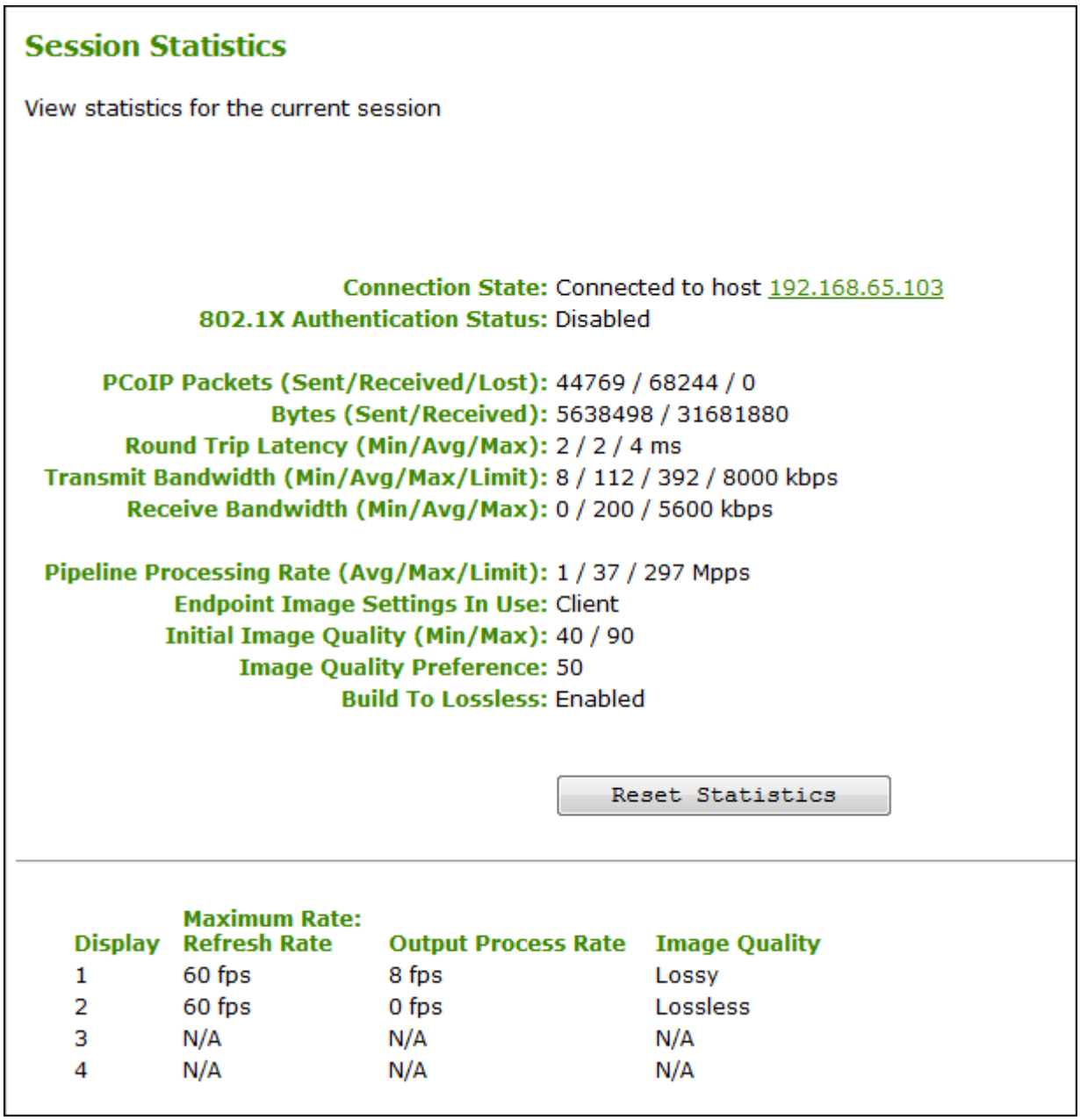
To view session statistics from the OSD:

1. From the OSD, select **Options > Diagnostics > Session Statistics**.
2. From the OSD *Session Statistics* page, you can view the following information:
   - **PCoIP Packets Sent:** The total number of PCoIP packets sent in the last session.
   - **PCoIP Packets Received:** The total number of PCoIP packets received in the last session.
   - **PCoIP Packets Lost:** The total number of PCoIP packets lost in the last session.
   - **Bytes Sent:** The total number of bytes sent in the last session.
   - **Bytes Received:** The total number of bytes received in the last session.
   - **Round Trip Latency:** The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (± 1 ms).
3. Click **Close**.

Viewing and Resetting Session Statistics from the AWI

The AWI Session Statistics page (shown next) displays statistics for the current session. If a session isn't active, the statistics from the last session display.

You can also reset session statistics from the AWI. When you reset statistics, you also reset the statistics that display on the AWI Home page (see AWI Home Page).



AWI Session Statistics page

The sample AWI Session Statistics page shows client statistics for a two-display setup

The sample page shows session statistics for a client with two connected displays. If your deployment uses four displays, information about all four displays will display on the page.

The following information displays on the AWI Session Statistics page:

WI Session Statistics Information

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Possible connection states are: • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	Indicates whether 802.1X authentication is enabled or disabled on the device.
PCoIP Packets Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.
Bytes	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (± 1 ms).

Parameters	Description
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth: The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	Shows the average and maximum amount of image data being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the Use Client Image Settings field is configured on the Image page for the host device.
Initial Image Quality	The minimum and maximum quality setting is taken from the **Image** page for the device.
Image Quality Preference	This setting is taken from the *Image Quality Preference* field on the Image page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include the following: • **Enabled:** The Disable Build to Lossless field on the Image page is unchecked. • **Disabled:** The Disable Build to Lossless field is checked.
Reset Statistics	Click this button to reset the statistic information on this page. **The Reset Statistics button also resets the statistics that display on the AWI Home page.**
Display	The port number for the display.
Maximum Rate: Refresh Rate	This column shows the refresh rate of the attached display. If the *Maximum Rate* field on the Image page is set to 0 (that is, there is no limit), the maximum rate is taken from the monitor's refresh rate. If the *Maximum Rate* field on the Image page is set to a value greater than 0, the refresh rate shows as User Defined.
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.

Parameters	Description
Initial Image Quality	Shows the current lossless state of the attached display: • .Lossy • Perceptually lossless • Lossless

To display session statistics:

1. From the AWI, select **Diagnostics > Session Statistics**.
2. From the AWI *Session Statistics* page, you can:
    - View the statistics for the current or previous PCoIP session.
    - Click **Reset Statistics** to reset the statistics for the current session.

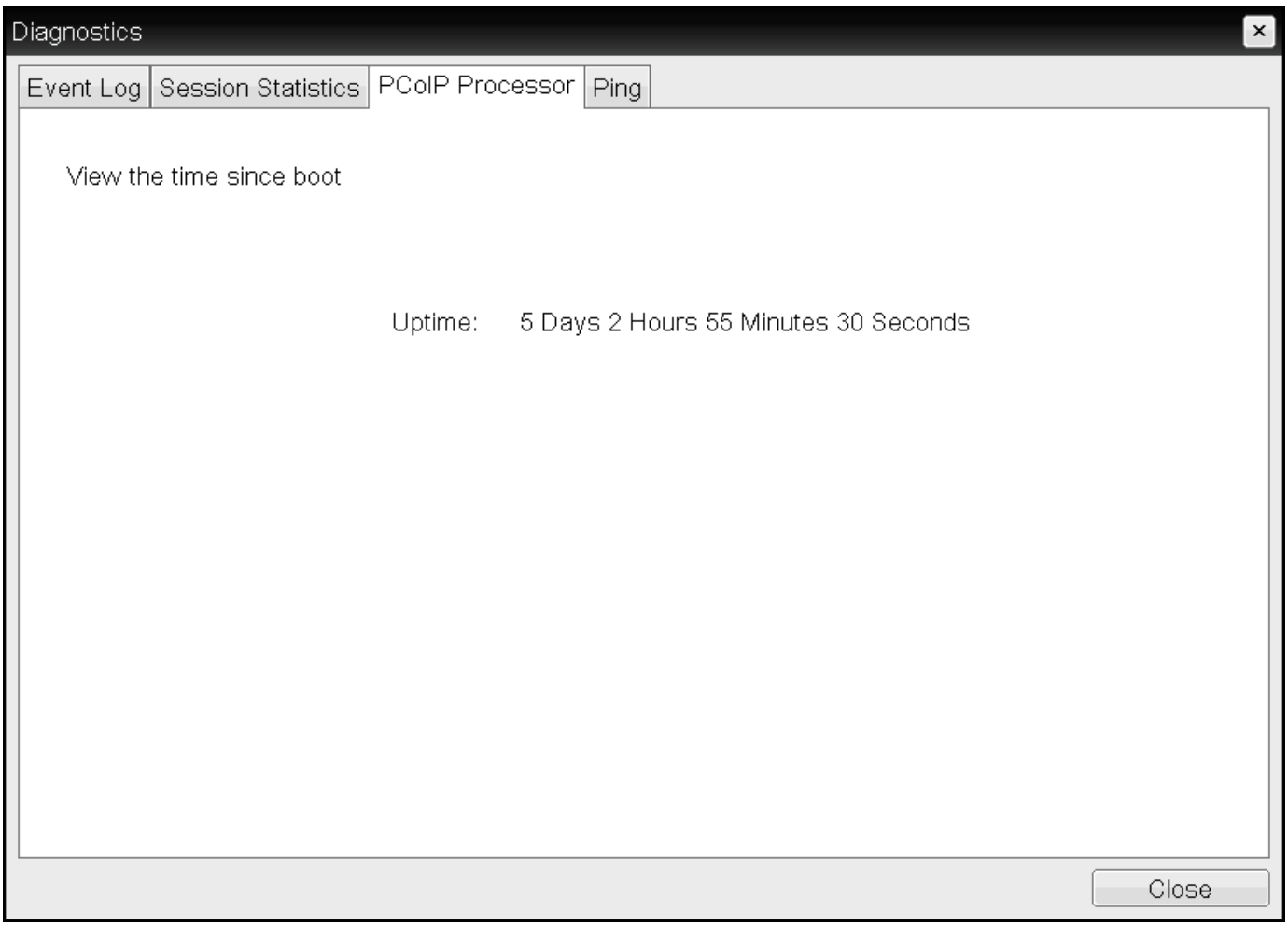
Viewing PCoIP Processor Statistics

Setting	Default	AWI	OSD	Management Console
Reset PCoIP Processor (a button)	–	✔	✔	✖

From the OSD and AWI, you can view the time elapsed since the Tera2 PCoIP Zero Client's PCoIP processor last re-booted. The AWI also enables you to view the current time and reset the Tera2 PCoIP Zero Client's PCoIP processor.

Viewing PCoIP Processor Statistics from the OSD

The OSD ***PCoIP Processor*** page, as shown next, enables you to view the time elapsed since the Tera2 PCoIP Zero Client's PCoIP processor last re-booted.



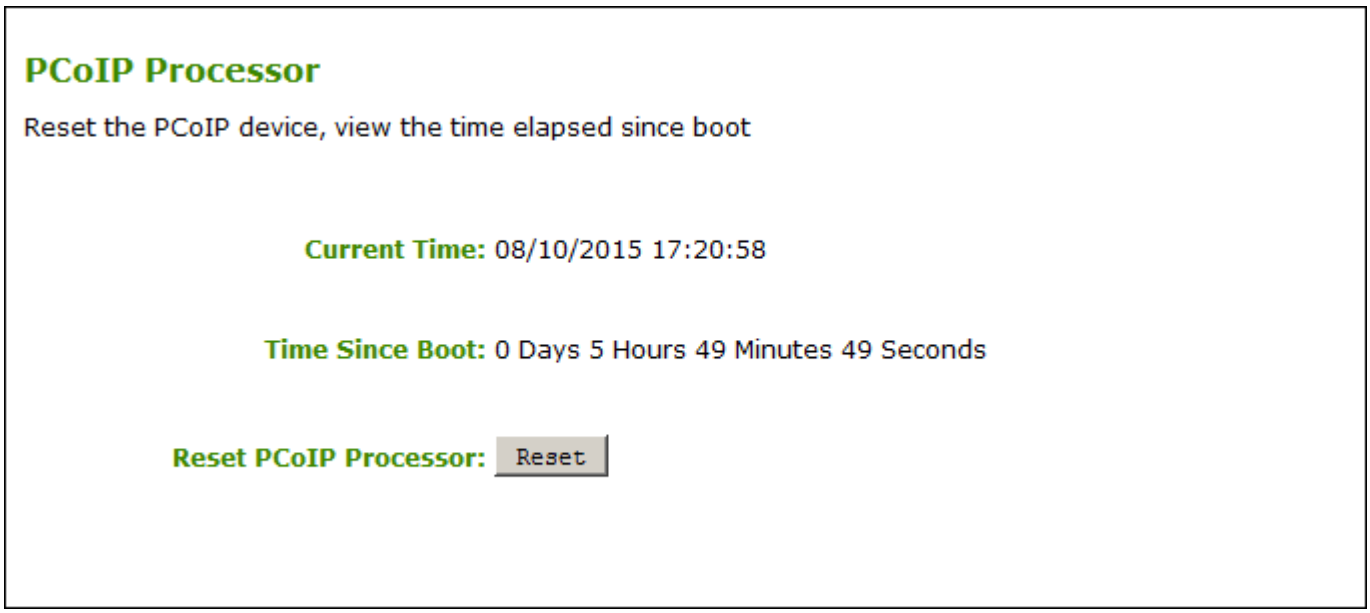
OSD PCoIP Processor page

To view PCoIP processor information:

1. From the OSD, select **Options > Diagnostics > PCoIP Processor**.
2. From the OSD ***PCoIP Processor*** page, view the time elapsed since the Tera2 PCoIP Zero Client's PCoIP processor last re-booted.
3. Click **Close**.

Viewing and Resetting PCoIP Processor Statistics from the AWI

From the AWI ***PCoIP Processor*** page, as shown next, you can view the current time, as well as view the time elapsed since the Tera2 PCoIP Zero Client's PCoIP processor last re-booted. You can also reset the Tera2 PCoIP Zero Client's PCoIP processor.



AWI PCoIP Processor page

To view and reset PCoIP processor information from the AWI:

1. From the AWI, select **Diagnostics > PCoIP Processor**.
2. From the AWI *PCoIP Processor* page, you can:
3. View the current time, as well as the time elapsed since the Tera2 PCoIP Zero Client's PCoIP processor last re-booted.

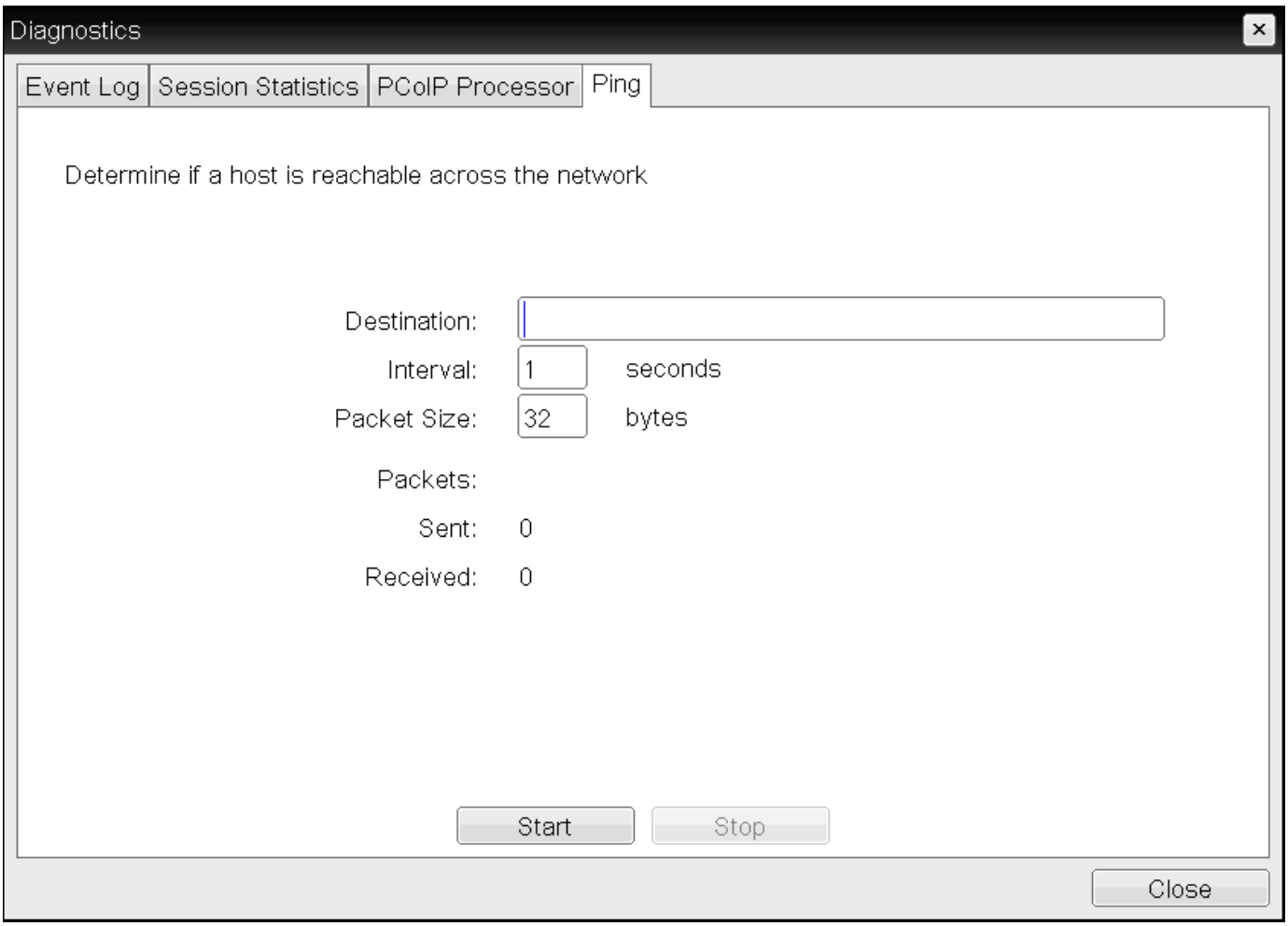
> **You must enable Network Time Protocol for the current time to display**
>
> For the current time to display, you must enable Network Time Protocol (NTP) and configure NTP parameters. To enable and configure NTP, see Configuring Time Settings.

4. Click **Reset** to start collecting fresh statistics.

Pinging the Host

Setting	Default	AWI	OSD	Management Console
Destination	–	✗	✓	✗
Interval	1	✗	✓	✗
Packet Size	32	✗	✓	✗
Sent	–	✗	✓	✗
Received	–	✗	✓	✗
Start (a button)	–	✗	✓	✗
Stop (a button)	–	✗	✓	✗

From the OSD Ping page, as shown next, you can ping a host to see if it's reachable across the IP network.



OSD Ping page

You can use the ping feature to determine the maximum MTU size

Because firmware releases 3.2.0 and later force the do not fragment flag in the ping command, you can ping a host to determine the maximum MTU size.

The following parameters display on the OSD Ping page:

Ping Parameters

Parameter	Description
Destination	IP address or Fully Qualified Domain Name (FQDN) to ping.
Interval	Interval between ping packets.

Parameter	Description
Packet Size	Size of the ping packet.
Packets Sent	Number of ping packets transmitted.
Packets Received	Number of ping packets received.
Start/Stop	Press **Start** or **Stop** to start or stop the ping.

To ping a host:

1. From the OSD, select **Options > Diagnostics > Ping**.
2. Click **Start** to start the ping. To stop the ping, click **Stop**.
3. Click **Close**.

Controlling Sessions

Setting	Default	AWI	OSD	Management Console
Connect (a button)	Enabled if a session is disconnected / Disabled if a session is connected	✔	✖	✖
Disconnect (a button)	Enabled if a session is connected / Disabled if a session is disconnected	✔	✖	✖

The AWI *Session Control* page, as shown next, displays current status of the session (for example, connected, connection pending, or disconnected), and enables you to manually disconnect from or connect to a session.

AWI Session Control page

The following parameters display on the AWI Session Control page:

Session Control Parameters

Parameter	Description
Connection State	This field displays the current state of the session. Options include the following: • **Disconnected** • **Connection Pending** • **Connected** Two buttons appear below the Connection State field: • **Connect:** If the connection state is **Disconnected**, click this button to initiate a PCoIP session between the client and its peer device. If the connection state is **Connection Pending** or **Connected**, this button is disabled. • **Disconnect:** If the connection state is **Connected** or **Connection Pending**, click this button to end the PCoIP session for the device. If the connection state is **Disconnected**, this button is disabled.
Peer IP	**Peer IP Address:** Displays the IP address for the peer device. When not in session, this field is blank.
Peer MAC Address	**Peer MAC Address:** Displays the MAC address of the peer device. When not in session, this field is blank.

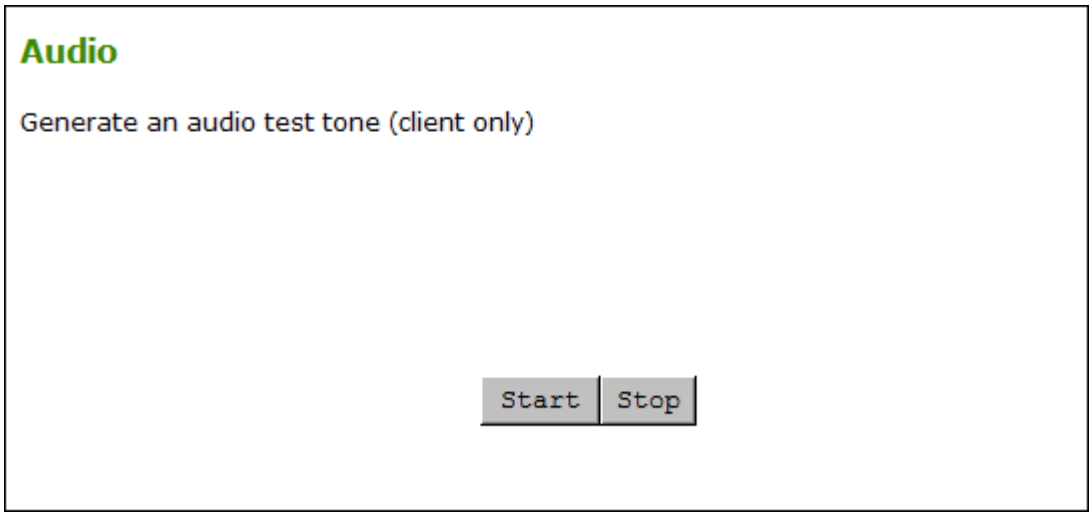
To manually disconnect from or connect to a session:

1. From the AWI, select **Diagnostics > Session Control**.
2. From the AWI *Session Control* page, you can:
    - View the connection status.
    - Click **Connect** to initiate a PCoIP session.
    - Click **Disconnect** to end the PCoIP session.

Testing Audio

Setting	Default	AWI	OSD	Management Console
Start (a button)	–	✔	✘	✘
Stop (a button)	–	✔	✘	✘

From the AWI *Audio* page, as shown next, you can generate an audio test tone from the Tera2 PCoIP Zero Client.



AWI Audio Page

You can't perform audio tests during a PCoIP session

You can only start and stop an audio test from the Tera2 PCoIP Zero Client if the client isn't in a PCoIP session.

To generate an audio test tone:

1. From the AWI, select **Diagnostics>Audio**.
2. From the AWI *Audio* page, click **Start** to start the test tone, or click **Stop** to stop the test.

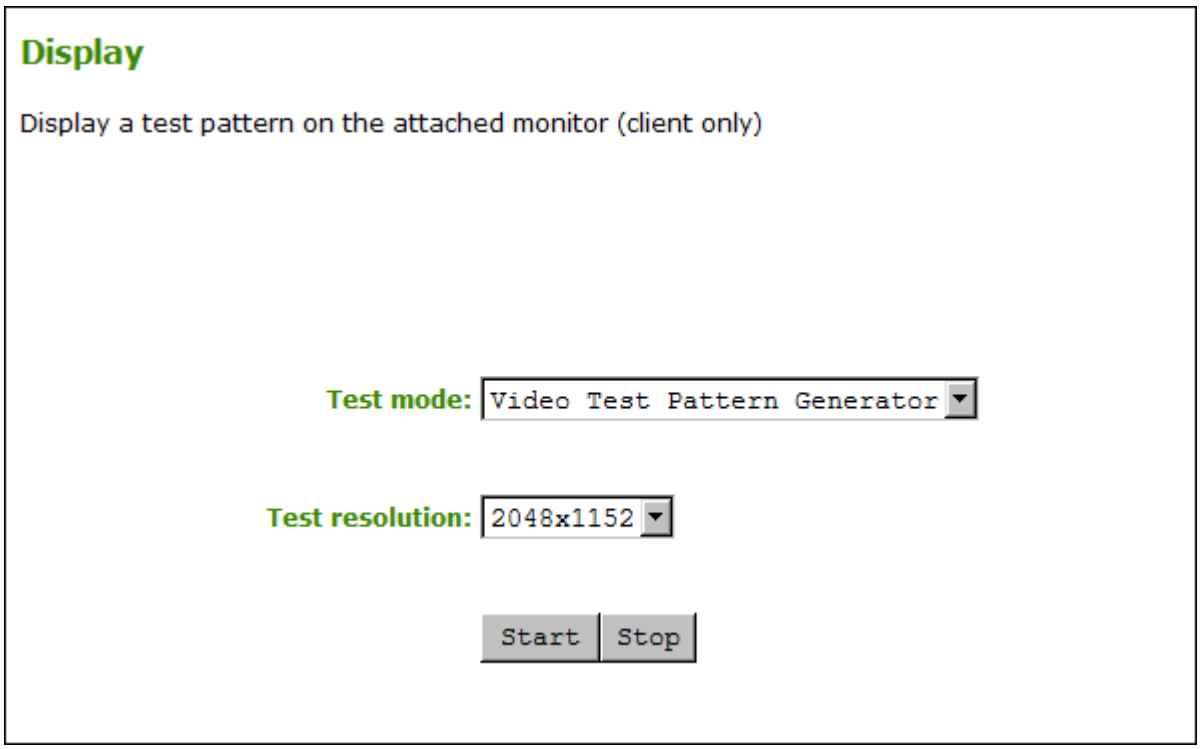
Testing Attached Displays

Setting	Default	AWI	OSD	Management Console
Test mode	Video Test Pattern Generator	✔	✘	✘
Test resolution	2048x1152	✔	✘	✘
Start (a button)	–	✔	✘	✘
Stop (a button)	–	✔	✘	✘

From the AWI ***Display*** page, as shown next, you can initiate and view a visual test pattern on the Tera2 PCoIP Zero Client's attached display(s).

You can't display test patterns during PCoIP sessions

The test pattern only displays when the Tera2 PCoIP Zero Client isn't in a PCoIP session. If you click **Start** when the Tera2 PCoIP Zero Client is in a session, an error message displays.



AWI Display page

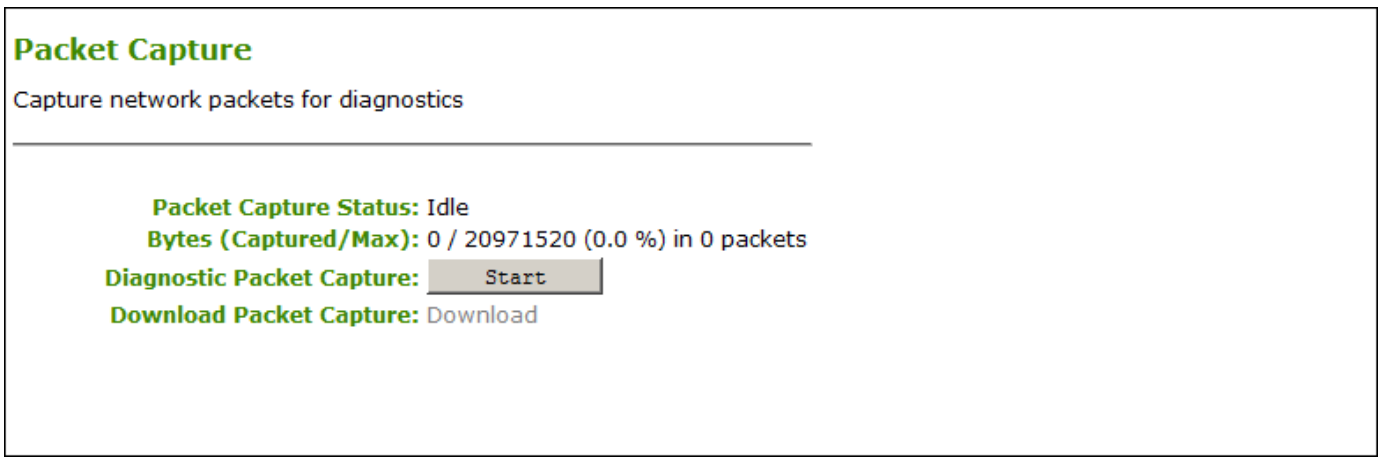
To initiate a test pattern:

1. From the AWI, select **Diagnostics > Display**.
2. From the AWI *Display* page, do the following:
   - From the **Test mode** list, select the type of test pattern to display on the Tera2 PCoIP Zero Client's attached display(s).
   - From the **Test resolution** list, select the test resolution to use.
   - Click **Start** to display a test pattern on the Tera2 PCoIP Zero Client's attached display(s). Click **Stop** to stop the test.

Using the Packet Capture Tool

Setting	Default	AWI	OSD	Management Console
Start (a button)	–	✔	✘	✘
Download (a link)	–	✔	✘	✘

The AWI Packet Capture page, as shown next, provides a diagnostic tool to capture network packets on the Tera2 PCoIP Zero Client. Using the packet capture tool may be requested by Teradici support.



AWI Packet Capture page

PCoIP traffic isn't included in the Packet Capture

PCoIP traffic is not included in the packet capture. All other network traffic, is captured.

The following parameters display on the AWI *Packet Capture* page:

Parameters	Description
Packet Capture Status	Displays the status of the packet capture tool. Values include: - **Idle**: Packet capture has not been initiated. - **Running**: Packet capture is in progress. - **Stopped**: Packet capture has been stopped.

Parameters	Description
Bytes (Captured/ Max)	Shows the number of captured bytes over the maximum number you can capture (in numeric and percentage format) along with the number of packets captured.
Diagnostic Packet Capture	Click **Start** to start the capture and click **Stop** to stop the capture.
Diagnostic Packet Capture	Click **Download** to save `packet_capture.bin` to the desired location on your computer.

Idle Status

After performing a packet capture, the status displays as **Idle** if you reboot the Tera2 PCoIP Zero Client.

`packet_capture.bin` contains network packets

Packets are captured into a binary file called `packet_capture.bin`. A maximum of 20 MB of data can be captured. If you don't stop the capture, it will automatically stop when it reaches the maximum.

To capture network packets to troubleshoot an issue:

1. from the AWI, select **Diagnostics > Packet Capture**.
2. From the AWI *Packet Capture* page, click **Start** to initiate the packet capture.
3. Repeat the steps required to reproduce the issue.
4. Click **Stop** to stop the packet capture.

   The `packet_capture.bin` file contains network packets

   Packets are captured into a binary file called `packet_capture.bin`. A maximum of 20 MB of data can be captured. If you do not stop the capture, it will automatically stop when it reaches the maximum size.

5. Click the **Download** link.
6. Save `packet_capture.bin` to a location on your computer.

Troubleshooting a Tera2 PCoIP Zero Client in Recovery Mode

If your Tera2 PCoIP Zero Client firmware goes into recovery mode, here are some ideas to troubleshoot the problem:

- It is possible that the Tera2 PCoIP Zero Client was forced into recovery mode by a user repeatedly tapping the power button when turning it on. If so, reboot the Tera2 PCoIP Zero Client to return it to the main firmware.
- If the Tera2 PCoIP Zero Client doesn't load the main firmware but boots into the recovery image immediately after powering up, then it's likely that a firmware upload operation was interrupted and the Tera2 PCoIP Zero Client doesn't contain a valid firmware image. Upload a new firmware image to the Tera2 PCoIP Zero Client and reboot the client to return to working firmware. To upload new firmware, see Uploading Firmware.
- If the Tera2 PCoIP Zero Client attempts to boot to the main firmware a few times (the splash screen will display for a short period of time) but eventually switches to the recovery image, then it's possible that the firmware configuration isn't valid. Reset the zero client parameters to factory defaults to clear the issue and re-provision the device. To reset the zero client parameters, see Resetting Your Tera2 PCoIP Zero Client.

Security Cipher Suites

The PCoIP Zero Client exchanges information with several services while connecting to endpoint managers, connection managers, and PCoIP hosts. The various communication phases are described followed by the set of supported cipher algorithms available to each phase.

The minimum *TLS Security Mode* for Maximum Compatibility and Suite B across all Zero Client session types have been updated to:

- **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**
- **Suite B: TLS 1.2 or higher with Suite B-compliant 192-bit elliptic curve encryption**

> **Tip regarding elliptic curve encryption**
>
> Security strength in bits of elliptic curve encryption is ½ of the key size.
>
> Examples:
>
> - If elliptic curve encryption uses the P-384 curve (which needs a 384-bit key), then the security strength is 384/2 = 192 bits.
> - If elliptic curve encryption uses the P-224 curve (which needs a 224-bit key), then the security strength is 224/2 = 112 bits.

TLS connections have a preferred order of Cipher suite/Elliptic Curve Cryptography (ECC) that is determined by the TLS server when the connection is TLS Server based. Client based connections have no order of preference. The two TLS server based communication phases described below—**Encrypting Browser Connections** and **Encrypting Endpoint Discovery**.

The following links describes the communication phases used when establishing a PCoIP session, and lists it's supported cipher suite and supported ECC curve.

- Encrypting Browser Connections
- Encrypting Endpoint Discovery
- Encrypting Pre-Session Amazon WorkSpaces Regional Code Lookup
- Encrypting Connections to Environments Using Smart Cards with OneSign Server

- Encrypting Pre-Session Communications with PCoIP Connection Managers or Brokering Agents
- Encrypting PCoIP Session Negotiation with PCoIP Hosts
- Encrypting Endpoint Manager Administration
- Encrypting RADIUS Server Using EAP-TLS During 802.1X Authentication
- Encrypting Pre-Session Communications with VMware Horizon Environments
- In-Session Encryption

Encrypting Browser Connections

PCoIP Zero Clients allow a browser to connect to the Administrative Web Interface (AWI) over a secure connection. This connection is a TLS server controlled connection and thus the order of the listed Cipher Suites and ECC Curves are important, with cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and elliptic curve NIST P-256 as being most preferred.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Minimum TLS version

This TLS server based connection requires TLS 1.2 or higher with 112-bit or higher elliptic curve encryption. The Elliptic Curve Cryptography (ECC) cipher suite curve preference is determined by the TLS server.

Recommended web browsers

Recommended web browsers are Firefox, Chrome, and Edge.

Encrypting Endpoint Discovery

PCoIP Zero Clients that are not managed by an endpoint manager, such as the PCoIP Management Console, listen for incoming discovery requests.

When an endpoint discovery request from an endpoint manager is received by the PCoIP Zero Client, communications between the endpoint manager and the PCoIP Zero Client are established securely using one of the supported cipher suites and ECC curves.

This connection is a TLS server controlled connection and thus the order of the listed Cipher Suites and ECC Curves are important, with cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and elliptic curve NIST P-256 as being most preferred.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Minimum TLS version

This TLS server based connection requires TLS 1.2 or higher with 112-bit or higher elliptic curve encryption. The Elliptic Curve Cryptography (ECC) cipher suite curve preference is determined by the TLS server.

Encrypting Pre-Session Amazon WorkSpaces Regional Code Lookup

Direct connections from a Zero Client to an Amazon WorkSpace requires a secure regional code lookup. The common cipher suites are used to perform the regional code lookup prior to the connection to Amazon WorkSpaces is established.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Encrypting Connections to Environments Using Smart Cards with OneSign Server

Environments that have implemented OneSign servers to use smart card security solutions are required to have a secure connection connection to the smart card server.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Encrypting Pre-Session Communications with PCoIP Connection Managers or Brokering Agents

Before a PCoIP session is negotiated with a PCoIP host using a PCoIP Connection Manager or brokering agent, each user is authenticated and then selects a desktop from a list of authorized resources. To complete this authentication process, the PCoIP Zero Client uses a cipher suite to securely communicate with a PCoIP Connection Manager, Remote Workstation Card Broker Agent or Cloud Access Manager broker agent over port 443.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384

- NIST P-521
- NIST P-224

Connections to Remote Workstation Card

Connections to Remote Workstation Card use a subset of the common cipher suites.

Encrypting PCoIP Session Negotiation with PCoIP Hosts

After user authentication and resource selection, PCoIP sessions are negotiated between the PCoIP Zero Client and the PCoIP host. A host can be a PCoIP Remote Workstation Card, Cloud Access Software Agent, or Amazon WorkSpace instance. Secure negotiations take place before the PCoIP session is established, and are secured using either **Maximum Compatibility** or **Suite B** (Remote Workstation Card only) cipher suites.

Secure Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Connections to Remote Workstation Card

Connections to Remote Workstation Card use a subset of the common cipher suites.

- **Maximum Compatibility: TLS 1.2 or higher with 112-bit or higher elliptic curve encryption**: Maximum Compatibility cipher suites allow secure negotiation using any of the common cipher suites to offer flexibility for your network security requirements.

  Connections to Remote Workstation Cards are limited to two of the common cipher suites and any compatible ECC.

  Supported cipher suites:

  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

  Supported Elliptic Curves (no order of preference):

  - NIST P-256
  - NIST P-384
  - NIST P-521
  - NIST P-224
- **Suite B**: Suite B applies only to Remote Workstation Card connections. It offers the greatest security for negotiating session connections with a PCoIP client and uses one of the common cipher security suites.

  Supported cipher suite:

  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

  Supported elliptic curve:

  - NIST P-384

Encrypting Endpoint Manager Administration

Once an endpoint manager discovers a PCoIP Zero Client, it uses the PCoIP Management Protocol to administer the endpoint. Communications between endpoint managers and PCoIP Zero Clients are secured using one of the supported cipher suites.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Encrypting RADIUS server using EAP-TLS during 802.1X authentication

In environments that have implemented an 802.1X radius server, the radius server uses the following secure communications to authenticate the endpoint.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

Encrypting Pre-Session Communications with VMware Horizon Environments

Before a PCoIP session is negotiated with a PCoIP host in a VMware Horizon environment, each user is authenticated and then selects a desktop from a list of authorized resources. To complete this authentication process, the PCoIP Zero Client communicates with a Horizon Connection Server over port 443 using one of the supported cipher suites.

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Supported Elliptic Curve:

- NIST P-256
- NIST P-384
- NIST P-521
- NIST P-224

System Configuration

These cipher suites can only be configured at the host.

In-Session Encryption

Once a PCoIP session has been negotiated and the connection established, PCoIP Zero Clients encrypt the session data using AES-256-GCM encryption algorithm. This algorithm secures all PCoIP communications during an active PCoIP session.

Supported Session Algorithm:

- AES-256-GCM

Frequently Asked Questions

This section provides answers to some commonly-asked questions about the Tera2 PCoIP Zero Client. For additional information, see Getting More Information, or the Teradici Support Center.

Q: What is a Tera2 PCoIP Zero Client?

A: Tera2 PCoIP Zero Clients are hardware- and firmware-based endpoints that enable users to connect remotely to PCoIP Remote Workstations, workstations running Teradici Cloud Access Software, Teradici Cloud Access Platform desktops and workstations, Amazon WorkSpaces desktops, and VMware Horizon and VMware Horizon DaaS virtual desktops. Because they do not have general purpose CPUs, local data storage, or application operating systems, Tera2 PCoIP Zero Clients are ultra secure and easy to manage. Tera2 PCoIP Zero Clients contain upgradable firmware that enables you to customize your client with various features. Tera2 PCoIP Zero Clients come in many forms, such as small stand-alone devices, PCoIP integrated displays, and touch-screen monitors. They support multiple wide-screen formats, HD audio and local USB peripherals, and are IPv6-ready. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards, smart cards, and One-Time-Passwords (OTP). Tera2 PCoIP Zero Clients are powered by a single TERA2321 or TERA2140 processor. For more information about your Tera2 PCoIP Zero Client, see About the Tera2 PCoIP Zero Client.

Q: How do I set up my Tera2 PCoIP Zero Client?

A: For instructions on how to set up a Tera2 PCoIP Zero Client and connect it to USB devices, monitors, and a network, see the Connecting the Tera2 PCoIP Zero Client to the Network. This guide has detailed instructions for each step of the installation process.

Q: How do I configure a Tera2 PCoIP Zero Client?

A: The following configuration and administrative management tools are available for Tera2 PCoIP Zero Clients: - **PCoIP On-Screen Display (OSD):** The Tera2 PCoIP Zero Client's pre-session built-in interface for configuring the device's firmware. - **PCoIP Administrative Web Interface (AWI):** A web-based interface for configuring a specific Tera2 PCoIP Zero Client's firmware remotely after typing the client's IP address into the browser's address bar. - **Teradici zero client management software:** A management tool for configuring and managing multiple PCoIP Zero Clients remotely. Teradici's

management software is the PCoIP Management Console. For information about the PCoIP Management Console, see the PCoIP® Management Console Administrators' Guide.

Q: How do I find my Tera2 PCoIP Zero Client's IP Address?

A: The Tera2 PCoIP Zero Client's address displays in the **IP Address** field when you select **Options > Information > Network** or **Options > Configuration > Network** from the client's OSD.

For more information, see How to Assign an IP Address to a PCoIP Zero ClientHow do I find the IP address of my newly installed PCoIP Zero Client or PCoIP Remote Workstation card? (1360).

Q: How do I update the Tera2 PCoIP Zero Client firmware?

A: The firmware version that is currently installed in your Tera2 PCoIP Zero Client displays in the **Firmware Version** field when you select **Options > Information** from the client's OSD or **Info > Version** from the client's AWI. For instructions on how to upload a different firmware release version, see How to Upload Firmware to a PCoIP Zero Client.

Q:What hosts can a Tera2 PCoIP Zero Client connect to?

A: Tera2 PCoIP Zero Clients are pre-configured to connect directly to PCoIP Connection Manager or VMware Horizon brokers, but you can easily configure them for any session connection type. Tera2 PCoIP Zero Clients can connect to PCoIP Remote Workstation Cards, Teradici Cloud Access Software, Teradici Cloud Access Platform desktops and workstations, Amazon WorkSpaces Desktops, and VMware Horizon Desktops. For more information, see What Can You Connect To Using Your Tera2 PCoIP Zero Client?.

Q: What devices can I attach to my Tera2 PCoIP Zero Client?

A: You can attach the following devices:

- **Monitors**: Depending on the Tera2 PCoIP Zero Client model, you can attach up to four monitors.
- **Analog devices**: You can attach analog output devices such as headphones and speakers to the Tera2 PCoIP Zero Client's analog output (line out) jack, and analog input devices such as microphones and recording devices to the client's analog input (line in) jack.
- **USB devices:** You can attach a variety of USB devices to your Tera2 PCoIP Zero Client. USB human interface device (HID) devices (for example, keyboards, mice, Wacom tablets) are locally terminated by the client. Non-HID devices (for example, mass storage devices, some printers, non-isochronous scanners) are automatically bridged when the USB permissions are

set to allow the device. The drivers for many of these devices need to be installed in the host operating system.

PCoIP Connection Brokers

PCoIP connection brokers are resource managers that dynamically assign host PCs to Tera2 PCoIP Zero Clients based on the identity of the user establishing a connection from the Tera2 PCoIP Zero Client. Connection brokers are also used to allocate a pool of hosts to a group of Tera2 PCoIP Zero Clients. If the Tera2 PCoIP Zero Clients in a PCoIP deployment are configured to always connect to the same host (that is, a static one-to-one pairing), then a connection broker is not required. Hosts consist of virtual machines or workstations with the appropriate PCoIP Agents installed and can include workstations with the Remote Workstation Card installed. The hosts can exist on premises or in the cloud.

For connecting clients and hosts, a number of PCoIP compatible connection brokers are available.

- Cloud Access Manager offers brokering for PCoIP Zero Clients and PCoIP Software Clients connecting to Cloud Access Software (CAS) and workstation hosts that have any of the PCoIP Agents installed.
- The Horizon/View Connection Server broker is used to connect Tera2 PCoIP Zero Clients to VMware Horizon virtual desktops and workstations with the Remote Workstation Card installed.
- Third party brokers are provided by Teradici Connection Brokering Technology Partners such as Leostream. Technology Partners can be found here.

DVI and DisplayPort Interfaces

Tera2 PCoIP Zero Clients support both DVI and DisplayPort digital display interfaces. The following port options are available for these clients:

- TERA2321 DVI-I dual-display Tera2 PCoIP Zero Client: contains two DVI ports.
- TERA2321 DP+DVI-I dual-display Tera2 PCoIP Zero Client: contains one DVI port and one DisplayPort port.
- TERA2140 DVI-D quad-display Tera2 PCoIP Zero Client: contains four DVI ports.
- TERA2140 DP quad-display Tera2 PCoIP Zero Client: contains four DisplayPort ports.

Support for 3840x2160 (4K UHD) Display Resolution

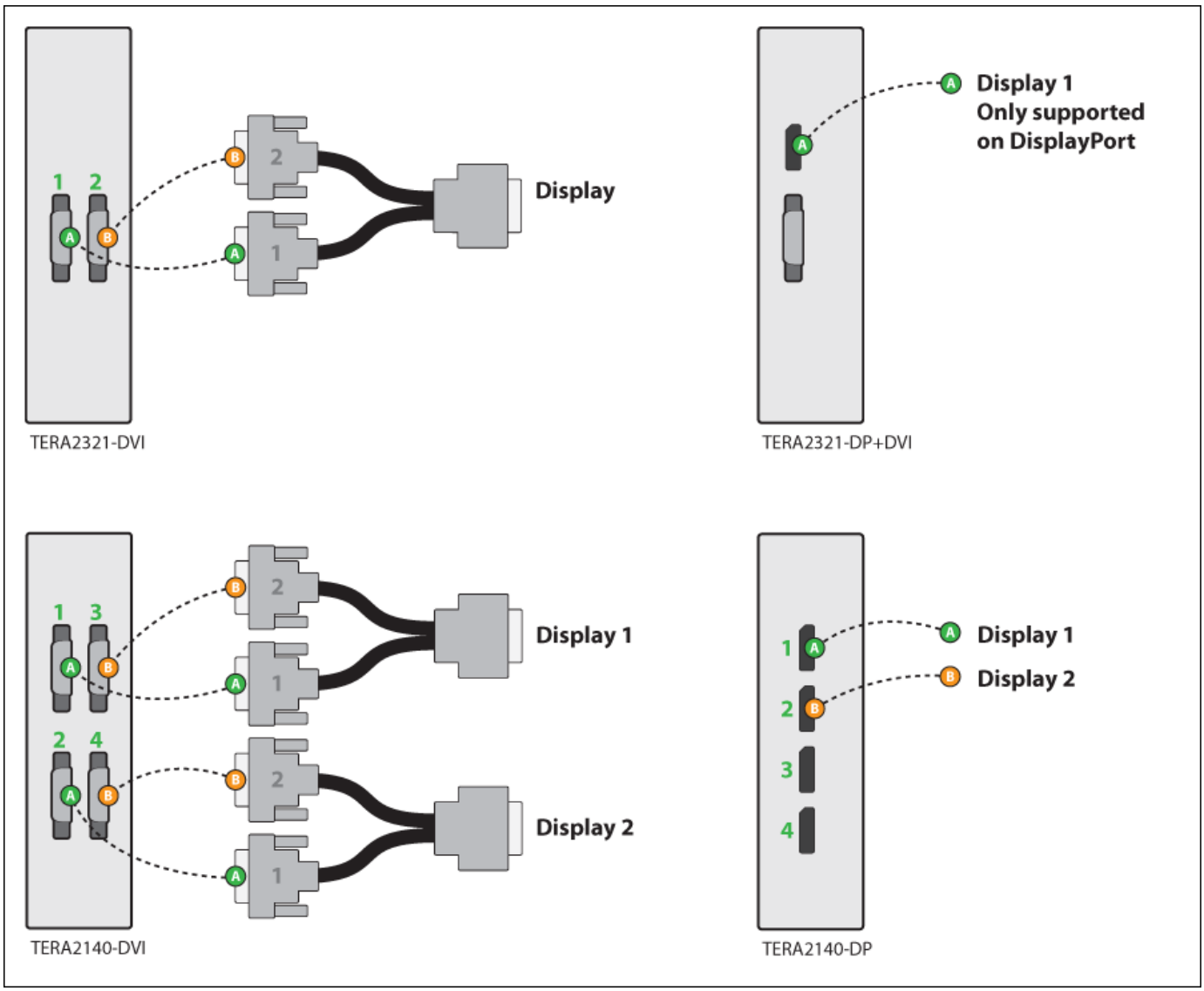
3840x2160 resolution is supported on DisplayPort interfaces only. The Zero Client will drive the monitor at 30 Hz.

> **Framerates**
>
> When playing full screen video, the framerate will be below 15 FPS.

Support for 2560x1600 Display Resolution

All of the previous Tera2 PCoIP Zero Clients also support 2560x1600 resolution for attached monitors with either DVI or DisplayPort interfaces. However, a custom dual-link DVI cable adapter is required to support this resolution for DVI interfaces.

The following figure illustrates how to connect video cables to each type of Tera2 PCoIP Zero Client to achieve 2560x1600 resolution on a connected display.



Connecting video cables to each type of Tera2 PCoIP Zero Client

DVI and DisplayPort Connectors for 2560x1600 Resolution

- TERA2321 DVI-I dual-display Tera2 PCoIP Zero Client: This PCoIP Zero Client supports one 2560x1600 monitor. Connect the two DVI-I cable connectors on a custom dual-link DVI-I cable adapter to the two DVI-I ports on the Tera2 PCoIP Zero Client, as shown in the previous illustration (upper left).
- TERA2321 DP+DVI-I dual-display Tera2 PCoIP Zero Client: This Tera2 PCoIP Zero Client supports one 2560x1600 or 3840x2160 monitor on the DisplayPort interface only. Connect the connector on a DisplayPort cable to the DisplayPort port on the Tera2 PCoIP Zero Client, as shown in the previous illustration (upper right).

- TERA2140 DVI-D quad-display Tera2 PCoIP Zero Client: This client supports up to two 2560x1600 resolution monitors. For each monitor, connect the two DVI-D cable connectors on a custom dual-link DVI-D cable adapter to the two DVI-D ports that are shown in the previous illustration (lower left). These connectors must be connected to ports on the client exactly as shown.
- TERA2140 DP quad-display Tera2 PCoIP Zero Client: This Tera2 PCoIP Zero Client supports up to two 2560x1600 or 3840x2160 monitors. For each one, connect the connector on a DisplayPort cable to a DisplayPort port on the Tera2 PCoIP Zero Client, as shown in the previous illustration (lower right).

Local Cursor and Keyboard

Local cursor and keyboard is a feature of the PCoIP Host Software that improves usability for PCoIP sessions operating over WAN connections (latency > 40 ms). When enabled, the Tera2 PCoIP Zero Client can terminate input from the mouse and keyboard, and draw the cursor on the attached display(s).

For more information about this feature and instructions on how to enable it, see the PCoIP® Host Software for Windows User Guide.

Remote Workstation Cards

PCoIP Remote Workstation Cards are small add-in cards that can be integrated into tower PCs, rack mount PCs, PC blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full desktop environment. This information is communicated in real time over an IP network to the user's Tera2 PCoIP Zero Client.

For complete details about PCoIP Remote Workstation Cards, see the Teradici website.

PCoIP Software Session Variables

The PCoIP software session variables in Microsoft's Group Policy Object (GPO) editor let you configure users' desktops with a collection of parameters that affect PCoIP sessions with soft hosts. These variables are defined in a GPO administrative template file called `pcoip.adm`, which is located on the View Connection Server installation directory (\'servername'\c$\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles\pcoip.adm).

You can enable and configure PCoIP software session variables in either the Group Policy Object editor's **PCoIP Session Variables > Overridable Administrator Defaults** list to enable users to override settings or the **PCoIP Session Variables > Overridable Administrator Defaults** list to prevent users from overriding settings.

> **Applying Group Policy Object administrative template file for large workplace environments**
>
> For large environments, you can apply `pcoip.adm` to a Windows Active Directory organizational unit (OU) or to a machine that you are configuring as a template for a desktop pool. For further details, see ***VMware View 5 with PCoIP Network Optimization Guide*** from the VMware Documentation website.

For instructions on how to load the PCoIP session variables template to a virtual machine's GPO editor, see How do I set up or override PCoIP software session variables on a virtual machine? (KB 1085). For detailed information on each PCoIP session variable, see What are PCoIP session variable GPOs? (KB 1660).

PCoIP Packet Format

PCoIP is a real-time technology that uses UDP as the transport-layer protocol. PCoIP supports two encryption types—UDP-encapsulated ESP and native IPsec ESP. An unencrypted PCoIP transport header field is also present for devices with firmware 4.1.0 or later installed and/or for scenarios using View 5.1 or later. The PCoIP transport header enables network devices to make better QoS decisions for PCoIP traffic.

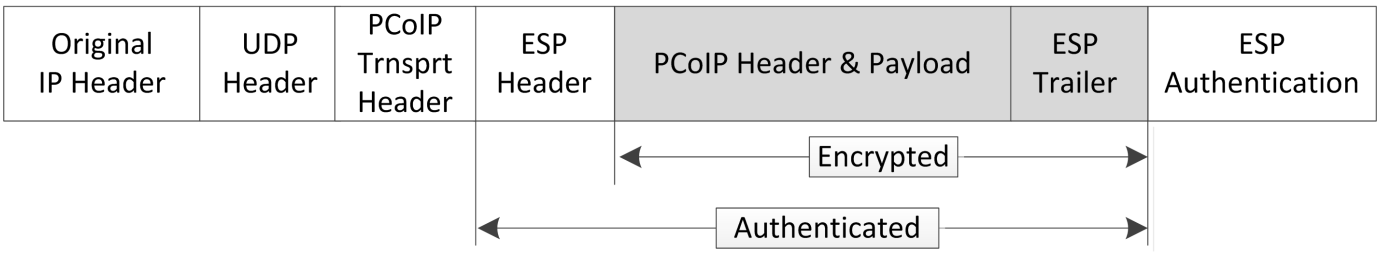
TCP/UDP port 4172 assigned to the PCoIP protocol

TCP/UDP port 4172 is the Internet Assigned Numbers Authority (IANA) port assigned to the PCoIP protocol. UDP port 4172 is used for the session data, and TCP port 4172 is used for the session handshake. For more information about TCP/UDP ports that are used for PCoIP technology, see What are the required TCP/UDP ports for PCoIP technology? (KB 1351).

UDP-encapsulated ESP Packet Format

UDP-encapsulated ESP is the default packet format for Tera2 devices with firmware 4.1.0 installed. It is also used for Tera1 devices with firmware 3.x+ installed that connect remotely via a View Security Gateway.

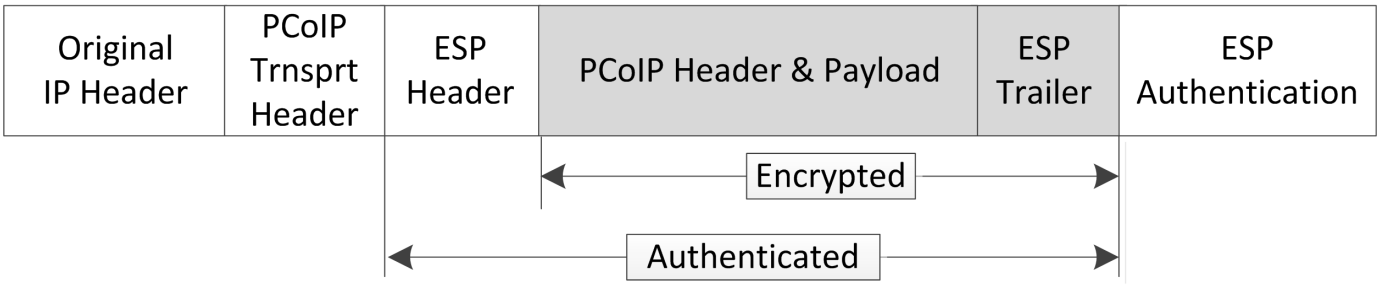
The UDP-encapsulated ESP packet format is illustrated in the following figure. This figure also shows the location of the PCoIP transport header in a UDP-encapsulated ESP packet.



UDP-encapsulated ESP Packet Format

IPsec ESP Packet Format

IPsec ESP encapsulation is the default packet format for direct connections that involve a Tera1 PCoIP Zero Client and/or Tera1 PCoIP Remote Workstation Card. The IPsec ESP packet format is illustrated in the following figure. This figure also shows the location of the PCoIP transport header in an IPsec ESP packet.



IPsec ESP Packet Format

Tera2 PCoIP Zero Clients

Tera2 PCoIP Zero Clients are secure client endpoints that enable users to connect to a virtual desktop or remote host workstation over a local or wide area IP network. They can take many form factors, such as small stand-alone devices, PCoIP integrated displays, VoIP phones, and touch-screen monitors. Zero clients support multiple wide-screen formats, HD audio and local USB peripherals, and are IPv6-ready. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards and smart cards.

Powered by a single TERA-series processor, Tera2 PCoIP Zero Clients provide a rich multi-media experience for users, who can interact with their desktops from any type of Tera2 PCoIP Zero Client, and even continue the same session as they move between Tera2 PCoIP Zero Client devices.

For complete details about Tera2 PCoIP Zero Clients, see the Teradici website.

Requirements for Trusted Server Connections

When connecting a Tera2 PCoIP Zero Client to a PCoIP endpoint using a **View Connection Server** or **PCoIP Connection Manager** session connection type, the padlock icon and 'https' text on the user login screen indicates whether the HTTPS connection is trusted or untrusted, see Connecting a Session for details.

- **Closed padlock with green 'https' text:** The connection is secured with HTTPS and the server's certificate is trusted by the Tera2 PCoIP Zero Client.
- **Open padlock with red strikethrough 'https:' text:** The connection is secured with HTTPS, but the server's certificate is not trusted by the Tera2 PCoIP Zero Client.

This section explains the certificate requirements that must be in place for each server type in order to have a trusted HTTPS connection. The following tables show which requirements are necessary for each Tera2 PCoIP Zero Client certificate checking mode.

> **Criteria Applied for Auto Detect Mode**
>
> If you use Auto Detect mode to connect, either the View Connection Server or PCoIP Connection Manager criteria are applied, depending on the server type.

View Connection Server Requirements

When connecting to a View Connection Server, the certificate requirements are as follows:

View Connection Server Certificate Requirements

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Valid according to computer clock (not expired and not valid only in the future).	Required	The certificate is accepted if the time is not valid but all other requirements are met. Warn the user before proceeding.	Not checked

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Certificate subject or a subject alternative name must match the VCS address.	Required	Not required if the server certificate is self-signed. Warn the user before proceeding. Required for all CA-signed certificates.	Not checked
Certificate must have the serverAuth enhanced key usage.	Required	Required	Not checked
Certificate chain of trust must be rooted in device's local certificate store.	Required	Not required if the server certificate is self-signed. Warn the user before proceeding. Required for all CA-signed certificates.	Not checked
Certificate must not be revoked (checked using OCSP (Offensive Security Certified Professional) only if there is a OCSP responder address in the certificate).	Required	Required	Not checked

PCoIP Connection Manager Requirements

When connecting to a PCoIP Connection Manager, the certificate requirements are as follows:

PCoIP Connection Manager Certificate Requirements

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Valid according to computer clock (not expired and not valid only in the future).	Required	The certificate is accepted if the time is not valid but all other requirements are met. Warn the user before proceeding.	Not checked

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Certificate subject or a subject alternative name must match the VCS address.	Required	Not required if the server certificate is self-signed. Warn the user before proceeding. Required for all CA-signed certificates.	Not checked
Certificate must have the serverAuth enhanced key usage.	Required	Required	Not checked
Certificate chain of trust must be rooted in device's local certificate store.	Required	Warn the user when certificate is not trusted.	Not checked
Certificate must not be revoked (checked using OCSP (Offensive Security Certified Professional) only if there is a OCSP responder address in the certificate).	Required	Required	Not checked

Syslog

The syslog protocol is a standard for logging program messages to a database. It is commonly used to monitor devices that do not have a large amount of storage capacity, such as networking devices, ESX servers, PCoIP Zero Clients, and PCoIP Remote Workstation Cards. Using syslog for logging enables you to centralize the storage of log messages and to capture and maintain a longer history of log data. It also provides a set of tools to filter and report on syslog data.

Syslog messages include a facility level (from decimal 0 to 23) that indicates the application or operating system component that is generating the log message. For example, a facility level of '0' indicates a kernel message, a facility level of '1' indicates a user-level message, and a facility level of '2' indicates a message from a mail system. Processes and daemons that have not been explicitly assigned a facility may use any of the eight 'local use' facilities ('16 – local use 0' to '23 – local use 7') or they may use the '1 – user-level' facility. Facilities enable for easy filtering of messages generated by a device.

Syslog messages are also assigned a severity level from 0 to 7, where a severity level of '0' indicates an emergency panic condition and a severity level of '7' indicates a debug-level message useful to developers but not for operations.

See Configuring Syslog Settings in the 'How To' section for information on how to configure syslog from the AWI and PCoIP Management Console.

Teradici PCoIP Hardware Accelerator (APEX 2800)

The Teradici PCoIP Hardware Accelerator card provides hardware-accelerated PCoIP image encoding for virtual desktop infrastructure (VDI) implementations. The card constantly monitors the graphic encoding demands of each virtual machine, dynamically switching the image compression tasks from software image encoding in the CPU to hardware image encoding, and back again. This offloading is performed instantly and seamlessly, as needed, without the user noticing the switch.

Smart Cards

This reference provides the requirements to support pre-session smart card authentication when connecting to VMware Horizon (View) know to work with the latest firmware. It also lists Supported Smart Cards and USB Smart Card Readers for Tera2 PCoIP Zero Clients Connected to PCoIP Connection Managers

Smart Card Dependencies

It is important to test your smart card in your deployment. Changes to smart card vendor and middleware software may cause smart cards to become ineffective in your deployment.

Smart Card Authentication with Leostream Broker (Beta)

Pre-session smart card support with PCoIP Zero Clients when connecting to Remote Workstation Cards or Cloud Access Software with Leostream broker — supported with PCoIP Zero Client firmware 6.4 and Leostream version 9.0.35 beta (Contact Leostream for details on their generally available release). Smart cards cannot be used for single sign-on to a workstation for this solution.

PCoIP Zero Clients support pre-session smart card authentication when connecting to VMware View virtual desktops that meet the system configuration requirements listed below. For deployments that meet these requirements, PCoIP Zero Clients can also read and process smart card information and allows SSO (single sign-on) authentication of the user prior to session establishment.

System Requirements

When used with VMware View 4.5 or higher with smart card authentication enabled, the firmware securely transfers the attached smart card properties to the View Connection Server for authentication and SSO of a user prior to a session. The Zero Client only supports 75 distinguished names when using Smart Card authentication.

Note on distinguished names

The distinguished names are retrieved from the keystore file that is created on the View Connection Server (VCS). The keystore file contains a list of all customer certificates being used.

Smart Card Certificate Requirements

- Key usage must be set to digital signature
- Subject common name and/or subject alternative name (other name) must be set
- Enhanced key usage must include client authentication and/or smart card logon
- Key length must not be larger than 2048 bit

Virtual Desktop Requirements

- VMware View 4.5 or higher
- VM Guest OS: Windows 10 and Windows 7 with VMware View Agent PCoIP smart card component installed
- PCoIP zero client firmware 3.2.0 or newer (where those smart cards supported in later firmware releases are indicated as such)
- The Agent's PCoIP smart card component must be installed for the guest OS to see the smart card reader (this is not installed by default)

Supported USB Smart Card Readers

Warning

Not all readers will function properly with all smart card solutions.

- Alcor AU9540-GBS (built into selected Samsung PCoIP Zero Clients)
- Castles Technology EZM110CU (built into selected ClearCube PCoIP Zero Clients)
- Castles Technology EZM110PU (built into selected ClearCube PCoIP Zero Clients)
- Cherry SmartBoard keyboard

- Dell Smart Card USB keyboard SK3205
- Gemalto PC Twin HWP108765C
- Gemalto PC Twin HWP108760D
- Gemalto PC USB-SW
- Gemalto IDBridge CR20/CT30/CT31
- HP KUS0133 Smart Card Keyboard
- Leadtek Alcor Reader
- OmniKey 3021
- OmniKey 3121
- OmniKey 5321 (Note: the 5321 CLi variant is currently not supported)
- Omnikey 5421
- Peripheral Dynamics PT-3901
- SCR331
- SCR333
- SCR335
- SCR3310
- SCR3310/v2.0

Known Smart Card Readers compatible with SC650/SIPR

- Omnikey 3021
- Omnikey 3121
- Omnikey 5321
- ClearCube Zero Client with a built-in Omnikey 3021 reader
- Gemalto GemPC Twin
- SCM SCR3310 v2

Tested Smartcard Models

GSC-IS and PIV Authentication Flow

The default authentication flow prior to firmware 6.5 was to use the GSC-IS driver before the PIV driver. Now the PIV driver is used first before the GSC-IS driver. If required, you can change the default authentication flow by enabling the **Prefer GSC-IS** setting. See advanced settings for View Connection Server session type.

When enabled, if a smart card (CAC) supports more than one interface such as GSC-IS and PIV then GSC-IS is used. However in the case where the card supports both GSC-IS and PIV, and only PIV objects are configured on the card then the connection may fail. If this is the case uncheck the box and retest. If a smart card supports only one interface, such as either GSC-IS or PIV endpoint, then only the GSC-IS or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.

Tip: Viewing all columns of a table

Scroll to the bottom of the table and use the horizontal scroll bar to view all columns of large tables

Teradici has tested these specific smart card models:

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
Cyberflex Access 64K V2c	CAC (GSC-IS) ActivClient v2.6.1 applet	ActivIdentity	3.2.0 and higher	3.2.0 and higher	Also referred to as the Gemalto Access 64KV2 Note 2,3
ID-One Cosmo v5.2D 64K	CAC (GSC-IS) ActivClient v2.6.1 applet	ActivIdentity	3.2.0 and higher	3.2.0 and higher	Also referred to as the Oberthur Cosmo64 V5.2D Note 2,3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
ID-One Cosmo v5.2 72K	CAC (GSC-IS) ActivClient v2.6.1 applet	ActivIdentity	3.2.0 and higher	3.2.0 and higher	Also referred to as the Oberthur ID One V5.2 Note 2,3
Cyberflex Access v2c 64K	CAC (GSC-IS) ActivClient v2.6.1 applet	ActivIdentity	3.2.0 and higher	3.2.0 and higher	Also referred to as the Gemalto Access 64KV2. Note 2, 3
ID-One Cosmo v5.2D 72K	CAC(PIV Transitional) ActivClient v2.6.2 applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Oberthur ID One V5.2 Dual This card has both contact and contactless interfaces. Only contact interfaces are supported. Note 2, 3
Gemalto GemCombiXpresso R4 dual interface	CAC(PIV Transitional) ActivClient v2.6.2 applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Gemalto GCX4 72K DI This card has both contact and contactless interfaces. Only contact interfaces are supported. Note 2, 3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
ID-One Cosmo v5.2D 72K	CAC (PIV Endpoint) ActivClient v2.6.2 applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Oberthur ID One V5.2 Dual This card has both contact and contactless interfaces. Only contact interfaces are supported. Note 2, 3
Gemalto GemCombiXpresso R4 dual interface	CAC (PIV Endpoint) ActivClient v2.6.2 applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Gemalto GCX4 72K DI This card has both contact & contactless interfaces. Only contact interfaces are supported. Note 2, 3
Gemalto TOP DL GX4 144K	CAC (PIV Endpoint) ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Gemalto TOP DL GX4 144K. This card has both contact and contactless interfaces. Only contact interfaces are supported. Note 2, 3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
Oberthur ID-One Cosmo 128 v5.5 for DoD CAC	CAC (PIV Endpoint) ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Oberthur ID One 128 v5.5 Dual. This card has both contact & contactless interfaces. Only contact interfaces are supported. Note 2 below
CosmopolIC 64K V5.2	CAC (GSC-IS) ActivClient v2.6.2 applet	ActivIdentity	3.2.0 and higher	3.2.0 and higher	Note 2, 3
ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3.2	CAC (PIV Endpoint) ActivClient v2.3.2 applet	ActivIdentity	3.4.0 and higher	3.4.0 and higher	A PIV Endpoint card uses the T=1 protocol Note 2, 3
GemCombiXpresso	CAC (PIV Endpoint) ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Gemalto TOP DL GX4 72K Note 2, 3
ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK	CAC (PIV Endpoint ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Also referred to as the Oberthur CS PIV End Point v1.08 FIPS 201 Note 2, 3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
ID-One Cosmo v7.0 128K	CAC (PIV Endpoint) ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Note 2, 3
SmartCafe Expert 144K DI v3.2	CAC (PIV Endpoint) ActivClient v2.6.2b applet	ActivIdentity	3.3.0 and higher	3.2.0 and higher	Note 2, 3
Cyberflex Access 64K V2c	ACS PKI 1.12	Gemalto Access Client	4.0.0 and higher	3.2.0 and higher	Note 3
Cyberflex Access 64K V2c	ACS PKI 1.14	Gemalto Access Client	4.0.0 and higher	3.2.0 and higher	Note 3
Axalto Cryptoflex .NET	Gemalto .NET	Gemalto/ Windows	3.4.1 and higher	3.2.0 and higher	Implements the Gemalto .NET standard. The middleware is built into Windows. Note 3
SIPR Token (SafeNet SC650)	Coolkey applet	90meter	3.5.1 and higher	3.2.0 and higher	This card uses 3V power, which many readers do not supply. Please see the reader list for compatible readers. Note 3
SafeNet SC650	SafeNet PKI	SafeNet SHAC	4.1.0 and higher	4.1.0 and higher	Note 3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
SafeNet SC650 Blade	SafeNet PKI	SafeNet SHAC	5.1.0 and higher	5.1.0 and higher	Note 3
Atos CardOS	CardOS	CardOS API	4.1.0 and higher	4.1.0 and higher	Note 3
eToken 4100	eToken Java	SafeNet Authentication Client	5.1.1 and higher	5.1.1 and higher	Note 3
eToken 5100	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3
eToken 5105	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3
eToken 5200	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3
eToken 5205	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3
eToken NG-OTP 72k	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3
eToken 72k Pro (IN FW 4.1.0)	eToken Java	SafeNet Authentication Client	4.1.0 and higher	4.1.0 and higher	Note 3

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
Gemalto IDCore 3020 PIV	PIV	Windows NIST SP 800-73 PIV (can be provisioned with Charismathics Security Token Configurator 5.0.2)	4.8.0 and higher	4.8.0 and higher	Note 3 Install user cert using Charismathics STC Key Pair Import Key Pair from PFX-File
Buypass	Buypass Proprietary	Buypass Proprietary	4.8.0 and higher	4.8.0 and higher	Note 3 Requires Buypass Middleware version 6.3.0.45 or later
SIPR Token (G&D Sm@rtCafé Expert)	Coolkey applet	90meter	5.4.1 and higher	3.2.0 and higher	Note 3 This G&D card works in all known readers
Gemalto IDPrime MD 830 w/o Secure Messaging (enhancements in FW 6.4), IDPrime MD 840, IDPrime MD 3810	Gemalto Proprietary	Gemalto	5.5.0 and higher	5.5.0 and higher	Note 3 Gemalto IDPrime MD 830(Level 2) with firmware 6.1.0 or higher supports smart cards provisioned with SafeNet Authentication Client

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
PIVkey C980	PIV	Taglio PIVKey Installer-User-7.1.0.5 (https://pivkey.com/download/pkuser.zip)	5.5.1 and higher	4.8.0 and higher	Note 3 Install user cert using Versasec vSEC_CMS_K2.0 from certificate PFX-File. vSEC-CMS_K2.0.exe can be downloaded as part of https://pivkey.com/pkadmin.zip Certificate can be mapped to container using pivkeytool.exe, which is also included in the Installer-Admin file in pkadmin.zip. More information from https://pivkey.zendesk.com/hc/en-us
Crescendo 144K FIPS	PIV	Actividentity	5.5.1 and higher	5.5.1 and higher	Note 3 For Pre-session authentication, “Prefer GSC-IS” must be disabled in AWI Advanced Session Connection configuration
HID Crescendo 144K FIPS Stand-Alone card	CAC (GSC-IS 2.1)	Actividentity	6.1.0 and higher	6.1.0 and higher	Note 3 Tested when provisioned onto G&D Sm@rtCafe Expert 144K v7 cards.

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
Thales/Gemalto/ SafeNet eToken 5110	eToken Java	SHAC 2.12.020	6.1.0 and higher	6.1.0 and higher	Note 3
SafeNet AT SC650 v3.2	Entrust PIV 2.4.2R0	Windows NIST SP 800-73 PIV (bridged only) or ActiveIdentity	6.3.0 and higher	6.3.0 and higher	
Entrust	Entrust PIV 2.4.2R0	Windows NIST SP 800-73 PIV (bridged only) or ActiveIdentity	6.3.0 and higher	6.3.0 and higher	
Oberthur/IDEMIA ID-One Cosmo v8.0, v8.1	ID-One PIV 2.4.0 and 2.4.1	ActivIdentity	6.4.0 and higher	6.3.0 and higher	Supported Readers Include IDBridge CT30/ SCR3310/SCR3310 v2.0/Omnikey OK3121/Omnikey 3021
Oberthur/IDEMIA ID-One Cosmo v8.0 Alt Token	CAC V2.7.4 Applets	ActivIdentity	6.4.0 and higher	6.4.0 and higher	
G+D Sm@rtCafe Expert v7.0	CAC V2.7.5 Applets	ActivIdentity	6.4.0 and higher	6.4.0 and higher	

Product Name	Applet Version	Middleware Provider	Pre-Session Authentication	In-Session Use	Comments
Gemalto IDPrime MD 830 Rev B • Level 3 • Level 2 with Secure Messaging Enabled	IDPrime Java Applet 4.3.5.D with Secure Messaging	Safenet Authentication Client 10.7	6.4.0 and higher	6.4.0 and higher	
IDEMIA Cosmo 8.1 r2	IAS-ECC V1.0.1	SecMaker Net iD Enterprise 6.8.0.22	21.03.0 and higher	21.03.0 and higher	
Thales IDPrime 930 FIPS 140 L2	IDPrime Java Applet 4.5.0E	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	
Thales IDPrime 930 FIPS 140 L3	IDPrime Java Applet 4.5.0E	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	
Thales IDPrime 3930 FIPS 140 L2	IDPrime Java Applet 4.5.0E	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	
Thales IDPrime 940	IDPrime Java Applet 4.4.2.A	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	
Thales IDPrime 3940	IDPrime Java Applet 4.5.0E	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	
Thales/Gemalto/ SafeNet eToken 5110	eToken Java Applet 1.7.7	Safenet Authentication Client 10.8 R2	21.10.0 and higher	21.10.0 and higher	Note 3

Notes:

1. Your card may be on the supported card list however the applet of the card may not be supported.
2. Solutions must be validated in user environments before selecting a solution, as environmental differences including network conditions or other components may impact support.

Undocumented Smart Card Support

For smart card authentication and SSO, the smart card must meet one of the following specifications:

- GSC-IS v2.0 and v2.1 cards (firmware 3.2.0 or higher)
- PIV transitional cards (firmware 3.4.0 or higher)
- PIV endpoint cards (firmware 3.4.0 or higher)
- Gemalto .NET
- Gemalto Access Client
- CoolKey
- CardOS 4.3b / 4.4 (excluding eToken. Supported on Tera2 with FW 4.1.0 and higher)

The communication protocol between the smart card and the reader is referred to as T=X, where X is 0 or 1. Firmware 3.2.0 and higher supports T=0. Firmware 3.4.0 and higher supports T=1.

Support for additional smart card variants will be added to future firmware releases.

Pre-session smart card authentication to remote workstations using PCoIP Remote Workstation Cards is not supported at this time.

Supported Smart Cards and USB Smart Card Readers for Tera2 PCoIP Zero Clients Connected to PCoIP Connection Managers

When used with a PCoIP Connection Manager that supports ID card authentication, the firmware securely transfers the attached ID card identifier to the PCoIP Connection Manager before a session is established.

Virtual Desktop Requirements

- Tera2 PCoIP Zero Client firmware 5.4 or later
- Teradici PCoIP Multi-Session Agent running on Windows Server 2016

Supported USB Smart Card Readers

- Gemalto IDBridge CT30 (legacy name: PC USB TR and PC TWIN)
- Rocketek RT-SCR1

Supported Smart Card Models

Teradici has tested these specific smart card models:

- Enhanced BasicCard
- Payflex Smart Card
- Open Platform Smart Card

Proximity cards and readers that are interoperable with PCoIP Zero Clients

This reference article is specific to Tera2 Zero Clients in VMWare Horizon environments using Imprivata OneSign with proximity cards.

The following proximity card peripherals were tested and are currently supported in firmware release 3.5.x and newer.

13.56 MHz proximity card models:

- HID iCLASS DL
- MIFARE
- HID iCLASS
- DESFire

13.56 MHz proximity reader models:

- HID iCLASS AIR ID Enroll RDR-7582AKU
- RF Ideas Air ID 82 Series RDR-7L82AKU (LEGIC-Prime only) (Note: reports of 15 seconds to initialize) **

125 kHz proximity card model:

- HID Prox

125 kHz proximity reader models:

- HID pcProx RDR-6081 AKU
- HID pcProx RDR-6082 AKU
- OMNIKEY 5325 Prox
- OMNIKEY 5325 CL Prox

Simultaneous operating frequency reader models (125kHz AND 13.56MHz):

- WAVEID pcProx Plus RDR-80582AKU (LEGIC-Advant) - (Is a re-branded HDW-IMP-80 which works)
- RF Ideas HID pcProx Plus RDR-80581 AKU
- OMNIKEY 5127 CK
- OMNIKEY 5127-mini (beginning with PCoIP Zero Client firmware version 5.4.0)
- OMNIKEY 5427 CK

Tablet Support

Overview

In some networks, users may notice a visible lag between the movement of the tablet stylus and the movement of the cursor on the display. This lag can be created by conditions such as large distances between client and host where stylus input coordinates must travel back and forth to the host before the cursor moves. This is considered a bridged configuration because the driver for the tablet is ***bridged*** to the host PC. To minimize the affects of the visible lag, Teradici has embedded a tablet driver in PCoIP Zero Client firmware which reduces the distance required for data to travel between the stylus and local cursor. This allows better performance for users such as artists that work in graphic intensive environments. Supported tablets that can take advantage of this driver are described as ***locally terminated*** to the PCoIP Zero Client.

High Latency Networks

Connecting to a Remote Workstation Card on a Linux PC using the Host Software for Linux with the local tablet driver feature enabled, helps improve the user experience by reducing the effects of latency in some networks where network latency exceeds 25 ms. To activate this feature, check the **Enable Local Tablet Driver** located on the PCoIP Host Software for Linux Features tab.

Supported Wacom tablets require the correct firmware uploaded to the PCoIP Zero Client as newer tablet models can be added to newer firmware releases. New supported tablet models can be identified by reviewing firmware release notes. To ensure you have the most complete set of supported Wacom tablets, use the latest release of PCoIP Firmware.

Unsupported tablets attached to clients connecting to Remote Workstation Cards will be bridged to the host PC.

Unsupported Tablets

Other unsupported tablets may work, but have not been tested and should not be used in production environments.

Absolute and Relative Co-ordinates

Supported tablets generally use absolute co-ordinates while in-session and relative co-ordinates while in pre-session such as when using the OSD. When using absolute co-ordinates, the local cursor will appear at the same position on the display as the stylus is on the tablet. As an example, if your stylus is at the center of the tablet, the cursor will appear at the center of your display. If using relative co-ordinates, the cursor will move a given direction and distance based on the motion the stylus moved across the tablet. As an example, if your stylus reaches the edge of the tablet, your cursor remains where it is on your display until you move your stylus from the edge and move it again starting at any point on the working tablet area.

Hosts

PCoIP Zero Clients support locally terminating Wacom tablets when a PCoIP Zero Client connects to any of the following hosts:

- Windows workstations with Cloud Access Software Graphics Agent installed.
  See the appropriate release of the Administrators' Guide and Release Notes for Cloud Access Software Graphics Agent for Windows
- Linux workstations with both a PCoIP Remote Workstation Card inserted and PCoIP Host Software for Linux installed.
  Review the appropriate release of the Host Software for Linux Administrators' Guide
- Windows and Linux Virtual Machines with Cloud Access Software installed.
  Review the appropriate release of the host Administrators' Guide and Release Notes for Cloud Access Software

Linux and Windows Virtual Machines

Virtual Machines with Cloud Access Software host agents installed may have special requirements for bridging of tablets and for local termination. For the latest information on requirements for Cloud Access Software graphics or standard agents, please see the version of the host agent Administrators' Guide used in your deployment.

- Cloud Access Software Graphics Agent for Linux
- Cloud Access Software Standard Agent for Linux
- Cloud Access Software Graphics Agent for Windows
- Cloud Access Software Standard Agent for Windows

The supported tablet tables are separated by Windows and Linux host operating systems

Tablets with PCoIP Zero Client Local Termination Support when Connecting to Linux Based Hosts

Description Model/Product ID	Cloud Access Software for Linux	Remote Workstation Card
Cintiq DTK-2241 / 0x0057	–	✔
Cintiq DTH-2242 / 0x0059	–	✔
Cintiq 12WX DTZ-1201W / 0x00C6	–	✔
Cintiq 13HD DTK-1300 / 0x0304	–	✔
Cintiq 13HD touch DTK-1300 / 0x0333	–	✔
Cintiq 20WSX DTZ-2000W / 0x00C5	–	–
Cintiq 21UX DTZ-2100 / 0x003F	–	–
Cintiq 21UX2 DTK-2100 / 0x00CC	–	–
Cintiq 22HD [4] DTK-2200 / 0x00FA	✔ [2] [3]	✔
Cintiq 22HDT(pen) non-touch DTH-2200 / 0x005B	– [2]	✔

Description Model/Product ID	Cloud Access Software for Linux	Remote Workstation Card
Cintiq 24HD DTK-2400 / 0x00F4	–	✔
Cintiq 24HD touch DTH-2400 / 0x00F8	–	✔
Cintiq 24 Pro DTH-2420 / 0x0351	✔[2] [3]	–
Cintiq 24 Pro non-touch [5] DTK-2420 / 0x037C	✔[2] [3]	–
Cintiq 32 Pro DTH-3220 / 0x0352	✔[2] [3]	–
Cintiq 27QHD DTH-2400 / 0x032A	–	✔
Cintiq 27QHD touch DTH-2400 / 0x032A	–	✔
Intuos3 4x5 PTZ-430 / 0x00B0	–	✔
Intuos3 6x8 PTZ-630 / 0x00B1	–	✔
Intuos3 9x12 PTZ-930 / 0X00B2	–	✔
Intuos3 12x12 PTZ-1230 / 0X00B3	–	✔
Intuos3 12x19 PTZ-1231W / 0X00B4	–	✔
Intuos3 6x11 PTZ-631W / 0X00B5	–	✔

Description Model/Product ID	Cloud Access Software for Linux	Remote Workstation Card
Intuos3 4x6 PTZ-431W / 0X00B7	–	✔
Intuos4 4x6 PTK-440 / 0X00B8	✔[2] [3]	✔
Intuos4 6x9 PTK-640 / 0X00B9	–	✔
Intuos4 8x13 PTK-840 / 0X00BA	–	✔
Intuos4 12x19 PTK-1240 / 0X00BB	–	✔
Intuos4 WL PTK-540-WL / 0X00BC	–	✔
Intuos5 touch Sm PTH-460 / 0X0026	–	✔
Intuos5 touch Med PTH-650 / 0X0027	–	✔
Intuos5 touch Lg PTH-850 / 0X0028	–	✔
Intuos5 S PTK-450 / 0X0029	–	✔
Intuos5 M PTK-650 / 0X002A	–	✔
Intuos Pro Small PTH-451 / 0X0314	✔[2]	✔
Intuos Pro Small (pen) PTH-460 / 0X0392	–	–

Description Model/Product ID	Cloud Access Software for Linux	Remote Workstation Card
Intuos Pro Medium [1] PTH-660 / 0x0357	✔ [2] [3]	✔
Intuos Pro Large [1] PTH-860 / 0x0358	✔ [2] [3]	✔
Intuos PT S CTH-480 / 0x0302	–	✔
Intuos PT M CTR-680 / 0x0303	–	✔
Intuos S CTL-480 / 0x030E	–	✔
Intuos P M CTL-680 / 0x0323	–	✔

Tablets with PCoIP Zero Client Local Termination Support when Connecting to Windows Based Hosts

Description Model/Product ID	Cloud Access Software for Windows	Remote Workstation Card
Cintiq 22HD [4] DTK-2200 / 0x00FA	✔ [2]	–
Cintiq 22HDT(pen)non-touch[^6] DTH-2200 / 0x005B	✔	–
Cintiq 24 Pro DTH-2420 / 0x0351	✔ [2]	–
Cintiq 24 Pro non-touch [5] DTK-2420 / 0x037C	✔ [2]	–

Description Model/Product ID	Cloud Access Software for Windows	Remote Workstation Card
Cintiq 32 Pro DTH-3220 / 0x0352	✔ [2]	–
Intuos Pro S PTH-451 / 0X0314	✔ [2]	–
Intuos Pro Small PTH-460 / 0X0392	–	–
Intuos Pro Medium [1] PTH-660 / 0x0357	✔ [2]	–
Intuos Pro Large [1] PTH-860 / 0x0358	✔ [2]	–
Intuos4 4x6 PTK-440 / 0X00B8	✔ [2]	–

Network Latency when connecting to Windows hosts

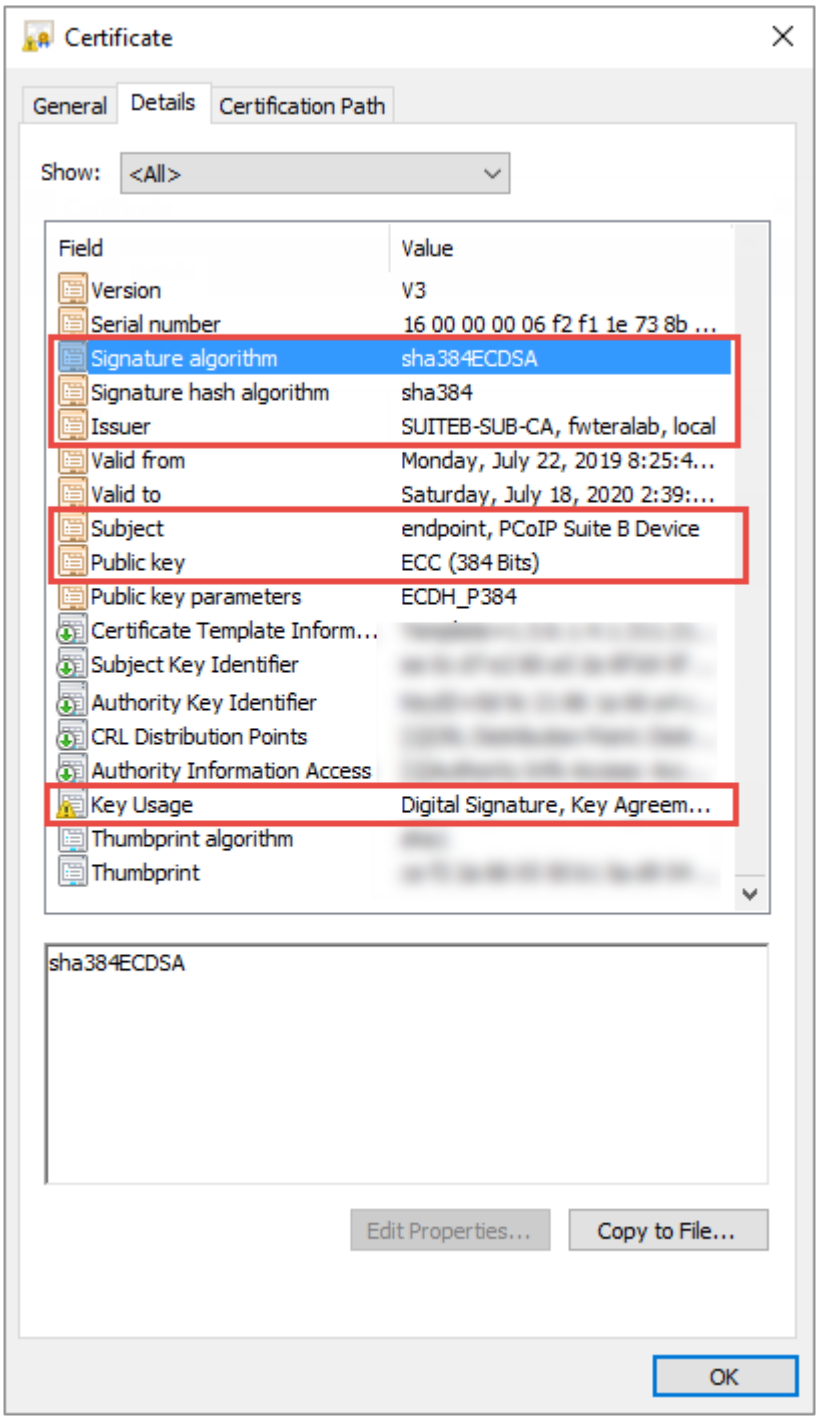
Supported tablets require low-latency environments. Tablets attached to clients connecting to Windows hosts in network environments with greater than 25ms latency will show reduced responsiveness and are not recommended.

1. Uses absolute co-ordinates while in-session and while in pre-session (when using the OSD)
2. Support for bridging to host PC with Cloud Access Software installed
3. Bare metal support for Cloud Access Software. Installation of Graphics Agent requires some additional configuration. See the extra installation instructions for Ubuntu and RHEL/CentOS
4. Requires Wacom Windows driver version 6.3.41-1
5. Cannot be driven at 4K resolutions

Creating and Applying Custom Certificates

In order to securely connect your PCoIP Zero Client to a Remote Workstation Card, the certificates must meet PCoIP Zero Client and PCoIP Remote Workstation Card Suite B requirements and both devices must be configured correctly.

This reference provides the Suite B certificate requirements so that you can create your own custom certificate to securely connect your PCoIP Zero Client to a Remote Workstation Card. It also provides the configuration steps to connect your endpoints using the **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption** TLS Security Mode parameter.



Required Certificate Parameters

All Certificate Requirements (Root/Client/Server)

- **Subject** and **Issuer** name must be valid (both the CN and O and cannot be empty).
- **Signature algorithm** must be SHA-384ECDSA.

- **Signature hash algorithm** must be SHA-384.
- **Public key** needs to be an 384 bit elliptic curve key that was generated from the secp384r1 curve (commonly known as the P-384 curve).
- Must be generated as unencrypted .pem files.

Client Certificate Specific Requirements

- **Key Usage** must be Digital Signature or omitted.
- Self signed certificates are not allowed.

Server Certificate Specific Requirements

- **Key Usage** must be Key Agreement, Key Encipherment or omitted.
- Self signed certificates are not allowed.

> **Notes**
>
> - The validity period is optional.
> - The Certificate Revocation List (CRL) lookup and Online Certificate Status Protocol (OCSP) is not used.
> - If certificate key usage has both Digital Signature and Key Agreement (or if certificate has no Key Usage), then it is possible to use the same certificate on both host and client.
> - See samples for Zero Client (client), Remote Workstation Card (server), and Root CA certificates.
> - The Generate_Certificate_Script package has been provided to demonstrate how to generate custom certificates. Unzip and run the **example_suiteb_all_gen.sh** script (certificates will be created in the **certificates** folder).

Perform the following configuration steps on the Remote Workstation Card and Zero Client to establish a secure connection with your custom certificates.

Remote Workstation Card Configuration

1. Login to the Remote Workstation Card AWI.
2. Browse to **Upload > Certificate** and **Upload** both the issuer (example_suite_b_root_ca_cert.pem) and client (example_suite_b_server.pem) certificates.
3. Browse to **Configuration > Session**.

4. Select **Direct from Client** for session connection type and select **Show Advanced Options**.
5. Select **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption** for TLS Security Mode parameter.
6. Select the correct Server certificate for the **Peer-to-Peer Certificate** parameter.

Zero Client Configuration

1. Login to the Zero Client AWI.
2. Browse to **Upload > Certificate** and **Upload** both the issuer (example_suite_b_root_ca_cert.pem) and client (example_suite_b_client.pem) certificates.
3. Browse to **Configuration > Session**.
4. Select **Direct to Host** for the Session Connection Type and enter the IP address of the Remote Workstation Card that you are connecting to for the **DNS Name** or **IP Address** parameter.
5. Select **Show Advanced Options** and select **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption** for the TLS Security Mode parameter.
6. Select the correct Client certificate for the **Peer-to-Peer Certificate** parameter.
7. From the OSD connect to your Remote Workstation Card.

> **Note**
>
> If a custom peer to peer certificate is applied and a connection is made, and the custom certificates is removed from the certificate store on either device, a subsequent connection will not establish.

PCoIP Zero Client Quick Start Guide

ESTABLISHING A PCoIP CONNECTION

Your PCoIP Zero Client is pre-configured to connect directly to a PCoIP Remote Workstation Card, but can be configured to use a third party connection broker such as VMware Horizon to connect to virtual desktops or PCoIP Remote Workstation Cards. You can also connect to Teradici Cloud Access Agents.

DIRECT CONNECT TO THE REMOTE WORKSTATION CARD

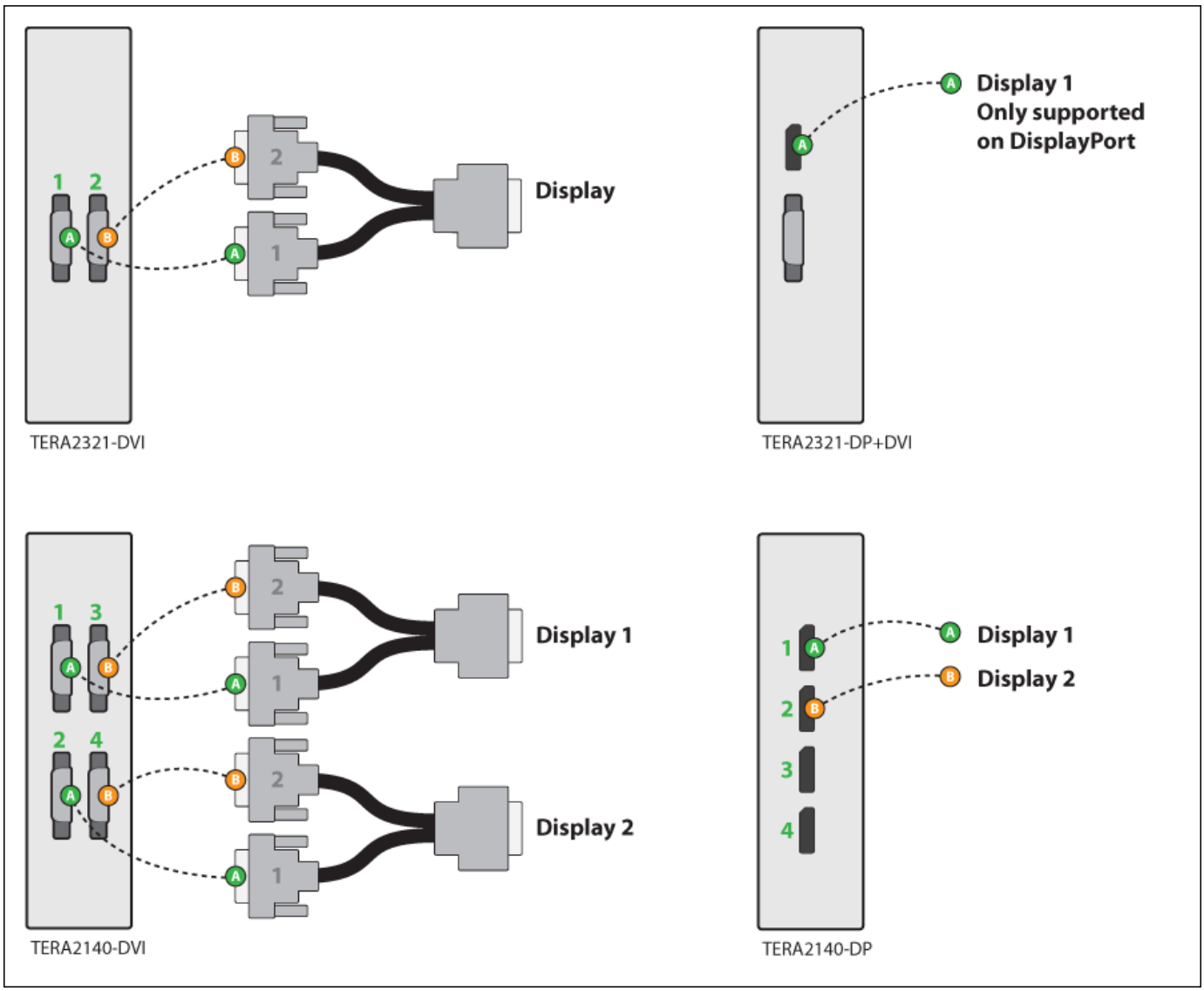
1. Power on host PC with PCoIP Remote Workstation Card.
2. Power on the Zero Client and the connected displays.
3. Ensure the Zero Client is on the same network as the Remote Workstation Card.
4. Wait until the **Connect** dialog appears on screen.
5. Select **Connect** and you will see the message **Discovering hosts, please wait....**
6. A list of available hosts is displayed.
7. Select the Remote Workstation Card you wish to connect to and click **OK**.
8. The display will show the host PC screen and the Zero Client's Session LED on the front panel will turn green indicating a successful PCoIP connection.

DIRECT CONNECT TO A TERADICI CLOUD ACCESS AGENT

1. Power on a host PC with Cloud Access Agent installed. (Standard Agent or Graphics Agent).
2. Power on the Zero Client and the connected displays.
3. Wait until the **Connect** dialog appears on screen.
4. Browse to the OSD Session Page (**Options > Configuration > Session**)
5. Change the Session Connection Type to **Auto Connect** and enter the IP address of the host PC.
6. Select **OK** and then **Connect**.

INSTRUCTIONS FOR 2560X1600 / 3840x2160 RESOLUTION MONITORS

(Only DisplayPort models support 3840x2160 (4K UHD) resolution)



LED STATUS INDICATORS

Session LED

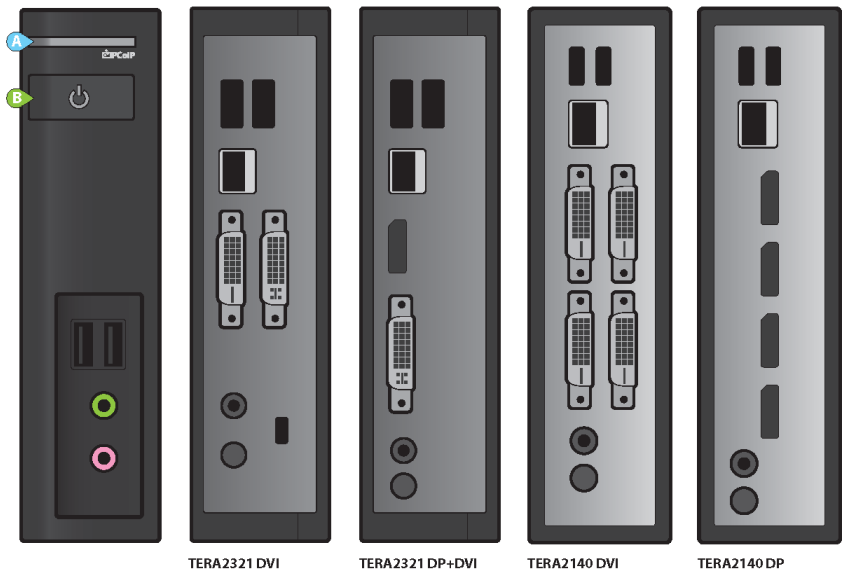
- Solid green – PCoIP session is active.
- Power Button LED**
- Solid green – Indicates unit is powered on.
- Flashing green – Host PC in low power state.
- Solid yellow – Client standby power is active and Wake-on-Lan (WoL) or Wake-on-USB (WoUSB) is enabled.
- Flashing yellow – Setting up for WoUSB or client is powering down.

A Session LED

- Solid green – PCoIP session is active.

B Power Button LED

- Solid green – Indicates unit is powered on.
- Flashing green – Host PC in low power state.
- Solid yellow – Client standby power is active and Wake-on-Lan (WoL) or Wake-on-USB (WoUSB) is enabled.
- Flashing yellow – Setting up for WoUSB or client is powering down.



INSTALLATION STEPS

1. Connect USB keyboard and mouse.
2. Connect one end of the Ethernet cable to the zero client and the other end to a switch/router. The switch or router should be on the same network as the Remote Workstation Card or virtual desktop server.
   For more advanced network environments, visit the Teradici Support Site
3. Connect monitor cables to the zero client.
4. Connect speakers and/or headphones (optional).
5. Connect power supply to the zero client and a power source.
6. Press front panel button to power on the zero client.

BUTTON OPERATION

- Press to turn on (when off or in WoL/WoUSB suspend mode)
- Press and hold to turn off
- When in-session
- When connected to a virtual desktop - Press to disconnect.
- When connected to a PCoIP Remote Workstation Card - Press to show zero client control panel with options to disconnect, or power off the workstation.

RESOLUTION OPTIONS

Model TERA2321 DVI

- 1-2 DVI monitors up to 1920x1200
- 1 DVI + 1 VGA monitor up to 1920x1200
- 1 DVI monitor up to 2560x1600*

Model TERA2321 DP+DVI

- 1 DisplayPort + 1 DVI or VGA monitor up to 1920x1200
- 1 DisplayPort monitor up to 3840x2160

Model TERA2140 DVI

- 1-4 DVI monitors up to 1920x1200
- 1-2 DVI monitors up to 2560x1600
- 1-2 DVI monitors up to 1920x1200 + 1 DVI monitor up to 2560x1600

Model TERA2140 DP

- 1-4 DisplayPort monitors up to 1920x1200
- 1-2 DisplayPort monitors up to 3840x2160
- 1-2 DisplayPort monitors up to 1920x1200 + 1 DisplayPort monitor up to 3840x2160

RESOURCES

Available at the Teradici Support Site:

- Zero Client
- Remote Workstation Card
- Session Planning Guide
- Using PCoIP Host Cards with VMware View Guide

MODELS

- TERA2321 DVI Dual Display PCoIP Zero Client

- TERA2321 DVI+DP Dual Display PCoIP Zero Client
- TERA2140 DVI Quad Display PCoIP Zero Client
- TERA2140 DP Quad Display PCoIP Zero Client