

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 PColP® Zero Clients in a PColP 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 release 6.2. 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 zero clients and remote workstation cards, see the [PCoIP® Management Console Administrators' Guide](#).

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

- [Teradici PCoIP® Standard Agent for Windows Administrators' Guide](#)
- [Teradici PCoIP® Standard Agent for Linux Administrators' Guide](#)
- [Teradici PCoIP® Graphics Agent for Windows Administrators' Guide](#)
- [Teradici PCoIP® Graphics Agent for Linux Administrators' Guide](#)
- [Remote Workstation Card Firmware 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](#).

What's New in Release 6.3

This documents Tera2 PCoIP Zero Client firmware only. This release contains the following Tera2 PCoIP Zero Client new features:

New Smart Cards for Horizon View

- SafeNet AT SC650 v3.2
- Entrust PIV 2.4.2R0
- Oberthur/IDEMIA Cosmo V8 ID-ONE PIV 2.4.0/2.4.1

Removed AES-128 in PCoIP session

PCoIP session can only be encrypted with AES-256

Low light interface

[User Interface](#) can be made less bright, to accommodate low light environments.

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 PCoIP Remote Workstations. These workstations use PCoIP Remote Workstation Cards or run Teradici Cloud Access Software, Amazon WorkSpaces desktops, and VMware Horizon desktops. Since they do not have general purpose CPUs, local data storage, or application operating systems, Tera2 PCoIP Zero Clients are very 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.

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 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. For more information, see [About the PCoIP On-Screen Display](#).
- **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. For more information, see [About the PCoIP Administrative Web Interface](#).
- **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 further information see [PCoIP Management Console](#), or see [PCoIP Management Console or PCoIP® Management Console Administrators' Guide](#) for configuration and technical procedures.

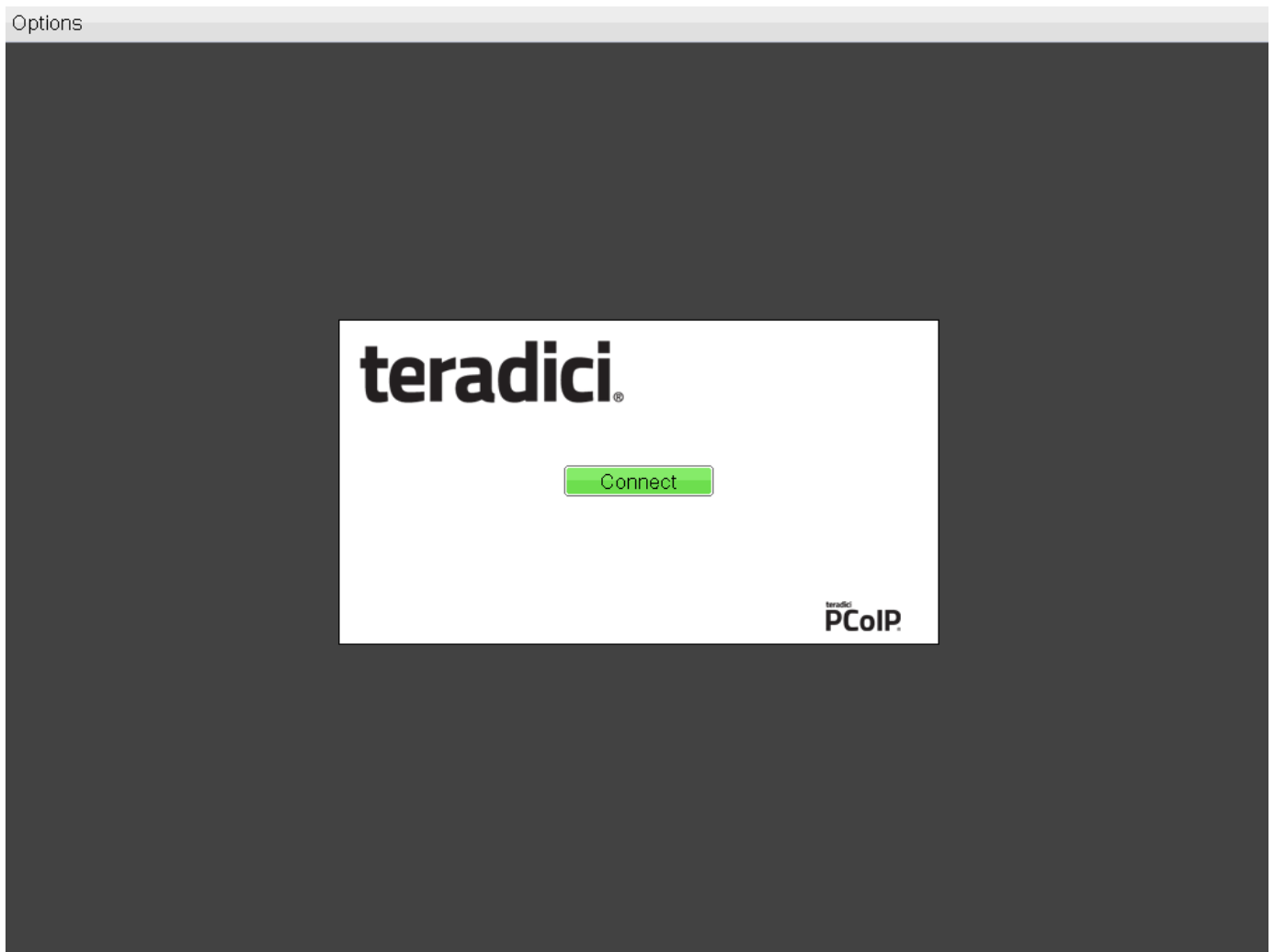


Secure Environments

Use the PCoIP Management Console in secure environments to configure and manage your Zero Clients after disabling the Zero Client AWI.

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.

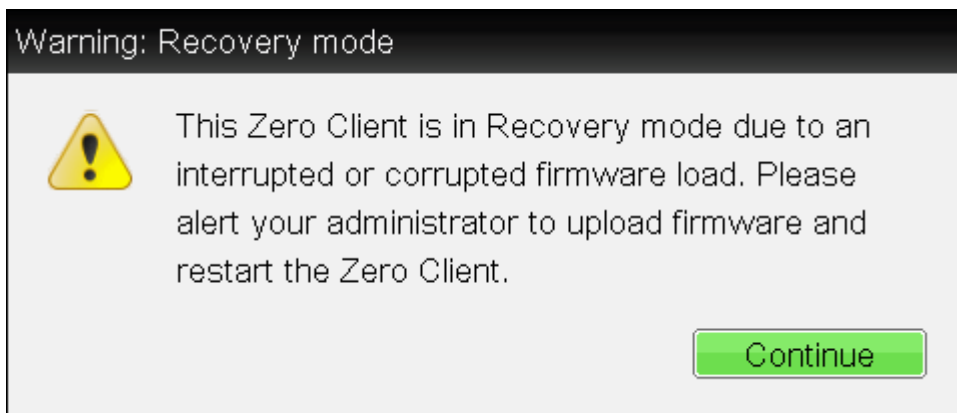
OSD Recovery Mode

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.

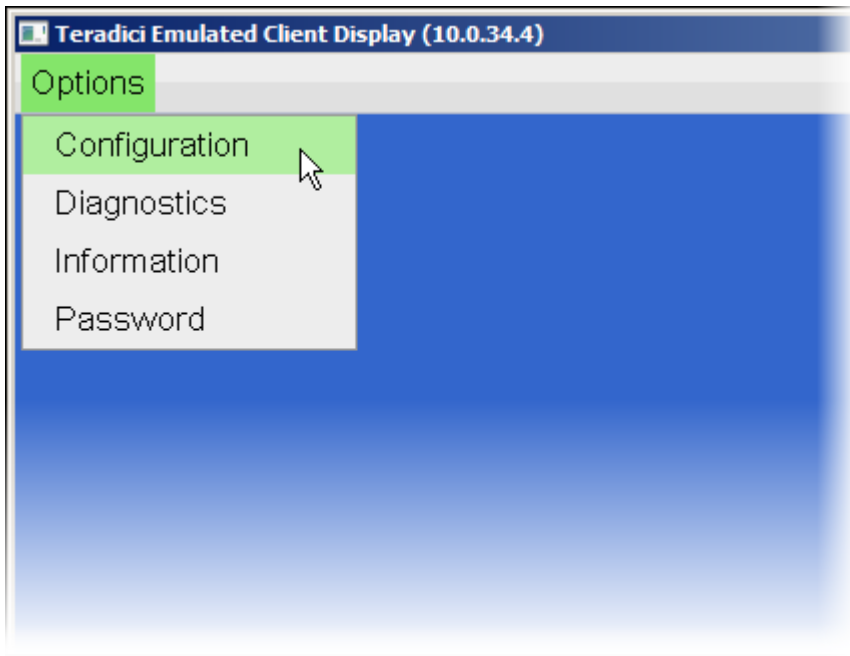
When the client is in recovery mode, the OSD screen displays the following initial screen:



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

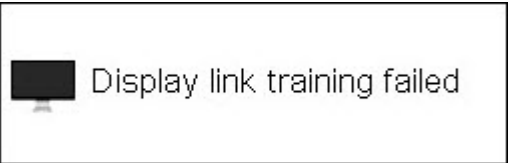
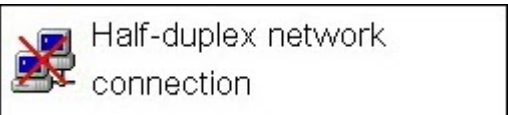

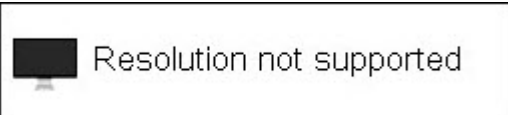

- **Configuration:** Lets you correct the problem by changing the [network configuration](#) (including [IPv6 settings](#)), [clearing the management state](#), and resetting the configuration and permissions settings stored on the device.
- **Diagnostics:** Displays the client's [event log](#) messages.
- **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.

About Overlay Windows

Overlay Window	Description
 <p>Display link training failed overlay</p>	<p>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: <i>Display link training failed</i>.</p>
 <p>Half duplex overlay</p>	<p>PCoIP technology is not compatible with half-duplex network connections. When a half-duplex connection is detected, this overlay appears with the message: <i>Half-duplex network connection</i>.</p>
 <p>Network connection lost overlay</p>	<p>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.</p> <p>The lost network connection message appears until the network is restored or the timeout expires (and the PCoIP session ends).</p> <p>Consider disabling this notification message in sessions to virtual desktops.</p> <p>Tip: Consider disabling this notification message in sessions to virtual desktops</p> <p>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.</p>
 <p>No support resolutions found overlay</p>	<p>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: <i>No support resolutions found. Please Try unplugging other displays</i>.</p>
 <p>Preparing desktop...</p>	<p>When a user first logs into a PCoIP session, this overlay appears with the message: <i>Preparing desktop...</i></p>

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
 <p data-bbox="145 768 391 797">No source signal overlay</p>	<p data-bbox="722 640 1452 913">When no video source is connected to the host, this overlay appears with the message: <i>No source signal</i>. 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.)</p>
 <p data-bbox="145 1104 496 1133">Source signal on other port overlay</p>	<p data-bbox="722 976 1445 1167">When a video source to the host does not correspond to the video port used on the client, this overlay appears with the message: <i>Source signal on other port</i>. 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.</p>

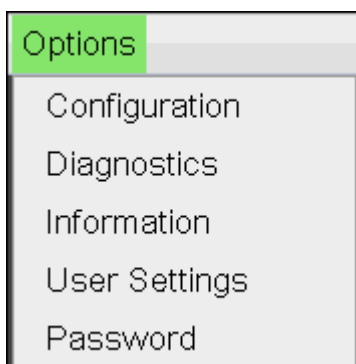
OSD Menu

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

OSD Menus

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.

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 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.

Log In

Please enter the administrative password to access this device.

Password:

Idle Timeout:

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**.

Logging into the Administrative Web Interface

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, network, and session 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.



PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

Processor: TERA2321 revision 0.0 (512 MB)
Time Since Boot: 7 Days 7 Hours 1 Minutes 12 Seconds
PCoIP Device Name: pcoip-portal-0030040f8ba3

Connection State: Connected to VDI host 192.168.63.216
Connection Duration: 0 Days 8 Hours 24 Minutes 35 Seconds
802.1X Authentication Status: Disabled
Session Encryption Type: AES-128-GCM

PCoIP Packets (Sent/Received/Lost): 1108849 / 983422 / 547 (0.0 %)

Bytes (Sent/Received): 155727102 / 434504596

Round Trip Latency (Min/Avg/Max): 1 / 1 / 11 ms

Transmit Bandwidth (Min/Avg/Max/Limit): 0 / 8 / 264 / 8000 kbps

Receive Bandwidth (Min/Avg/Max): 0 / 0 / 9056 kbps

Pipeline Processing Rate (Avg/Max): 0 / 40 Mpps

Endpoint Image Settings In Use: Host
Initial Image Quality (Min/Max): 50 / 80
Image Quality Preference: 45
Build To Lossless: Disabled

Display	Maximum Rate: User Defined	Output Process Rate	Image Quality
1	24 fps	0 fps	Lossy
2	24 fps	0 fps	Lossy

AWI: Home page

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.
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



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:

teradici
PCoIP

Log In

Please enter the administrative password to access this device.

This Zero Client is in Recovery mode due to an interrupted or corrupted firmware load. Please alert your administrator to upload firmware and restart the Zero Client.

Password:

Idle Timeout:

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.

Log Out PCoIP® Zero Client

Home Configuration / Diagnostics / Info / Upload

teradici[®] PCoIP

PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

This Zero Client is in Recovery mode due to an interrupted or corrupted firmware load. Please alert your administrator to upload firmware and restart the Zero Client.

Processor: TERA2140 revision 1.0 (128 MB)
Time Since Boot: 19 Days 6 Hours 12 Minutes 7 Seconds
PCoIP Device Name: pcoip-portal-emu001-025056972792

Connection State: Disconnected
Connection Duration:
802.1X Authentication Status: N/A
Session Encryption Type: Not in Session

PCoIP Packets (Sent/Received/Lost): 5 / 4 / 3 (37.5 %)
Bytes (Sent/Received): 2 / 1
Round Trip Latency (Min/Avg/Max): 10 / 50 / 100 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 10000 / 50000 / 110000 / 100000 kbps
Receive Bandwidth (Min/Avg/Max): 1000 / 2000 / 5000 kbps

Pipeline Processing Rate (Avg/Max): 0 / 0 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Max): 10 / 20
Image Quality Preference: 30
Build To Lossless: Enabled

Display	Maximum Rate: User Defined	Output Process Rate	Image Quality
1	N/A	N/A	N/A
2	N/A	N/A	N/A
3	N/A	N/A	N/A
4	N/A	N/A	N/A

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.

AWI Recovery Mode Options

- **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](#).

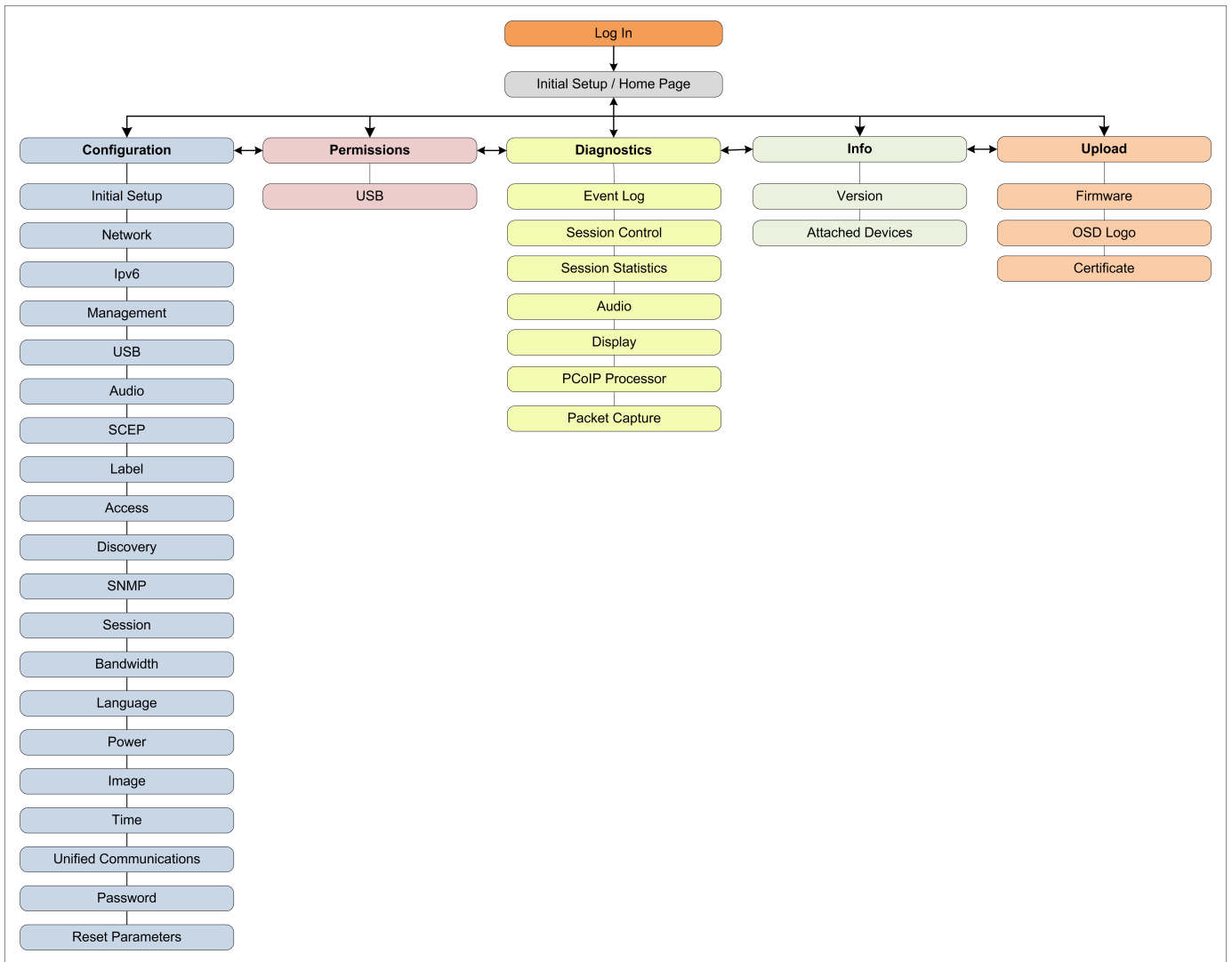
AWI Menu

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



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.

Supported Displays and Resolutions

- **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:

Tera2 PCoIP Zero Client Processor	Maximum No. of Supported Displays and Resolutions
TERA2321	2 x 1920x1200 1 x 2560x1600*
TERA2140	4 x 1920x1200 2 x 2560x1600*

*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](#).

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:

- [Connecting the Tera2 PCoIP Zero Client to the Network](#)
- [Configuring Initial Setup Parameters](#)
- [Securing Your Tera2 PCoIP Zero Client](#)

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 host 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.

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 host 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.

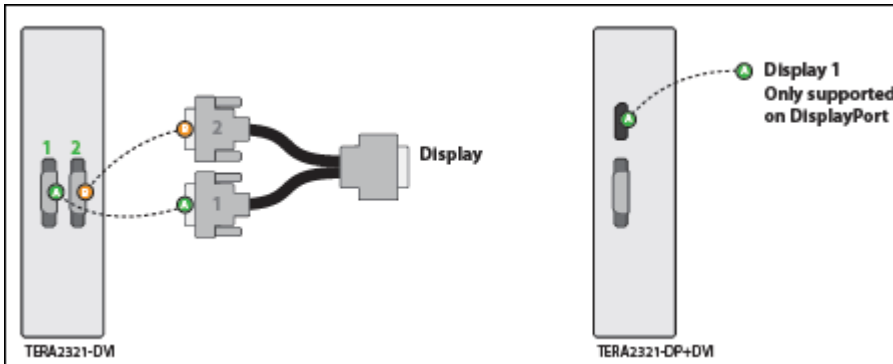
Connect monitors using correct ports

To ensure the best experience, connect monitors to the zero client ports in sequential order

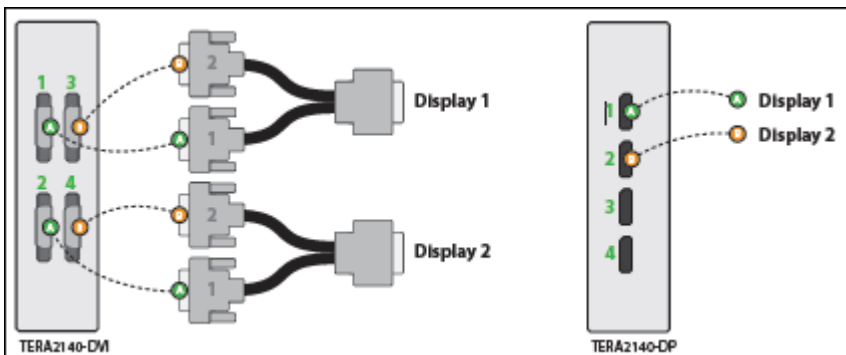
Connecting the Tera2 PCoIP Zero Client to the Network

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.

Initial Setup (1:1 Manual Configuration)

These settings must be configured before the device is used for the first time

Step 1: Audio

Enable HD Audio: Note: To enable audio, please ensure that audio is also enabled on the Host.

Step 2: Network

Enable DHCP:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:

Step 3: Session

Identify Host by: IP address FQDN

Host IP Address:

Host MAC Address:

Step 4: Apply Changes

AWI Initial Setup page

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

Audio Parameters

Parameter	Description
Enable HD Audio	Enables audio support on the client.

Configuring Initial Setup Parameters

Configuring other audio parameters

You can configure other audio parameters from the OSD and AWI Audio pages. To configure audio parameters from these pages, see [Configuring Audio](#).

Network Parameters

Parameter	Description
Enable DHCP	Enables DHCP (as opposed to using manual IP address configuration)
IP Address	Device's IP address
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 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 Network Settings](#).

Session Parameters

Parameter	Description
Identify Host By	Specifies the host identify method
Host IP Address	Specifies the host IP address
Host MAC Address	Specifies the host MAC address. You can set the host MAC address to 00-00-00-00-00-00 to ignore this field when a session starts.

Configuring Initial Setup Parameters

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, network, and session parameters.
3. 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 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

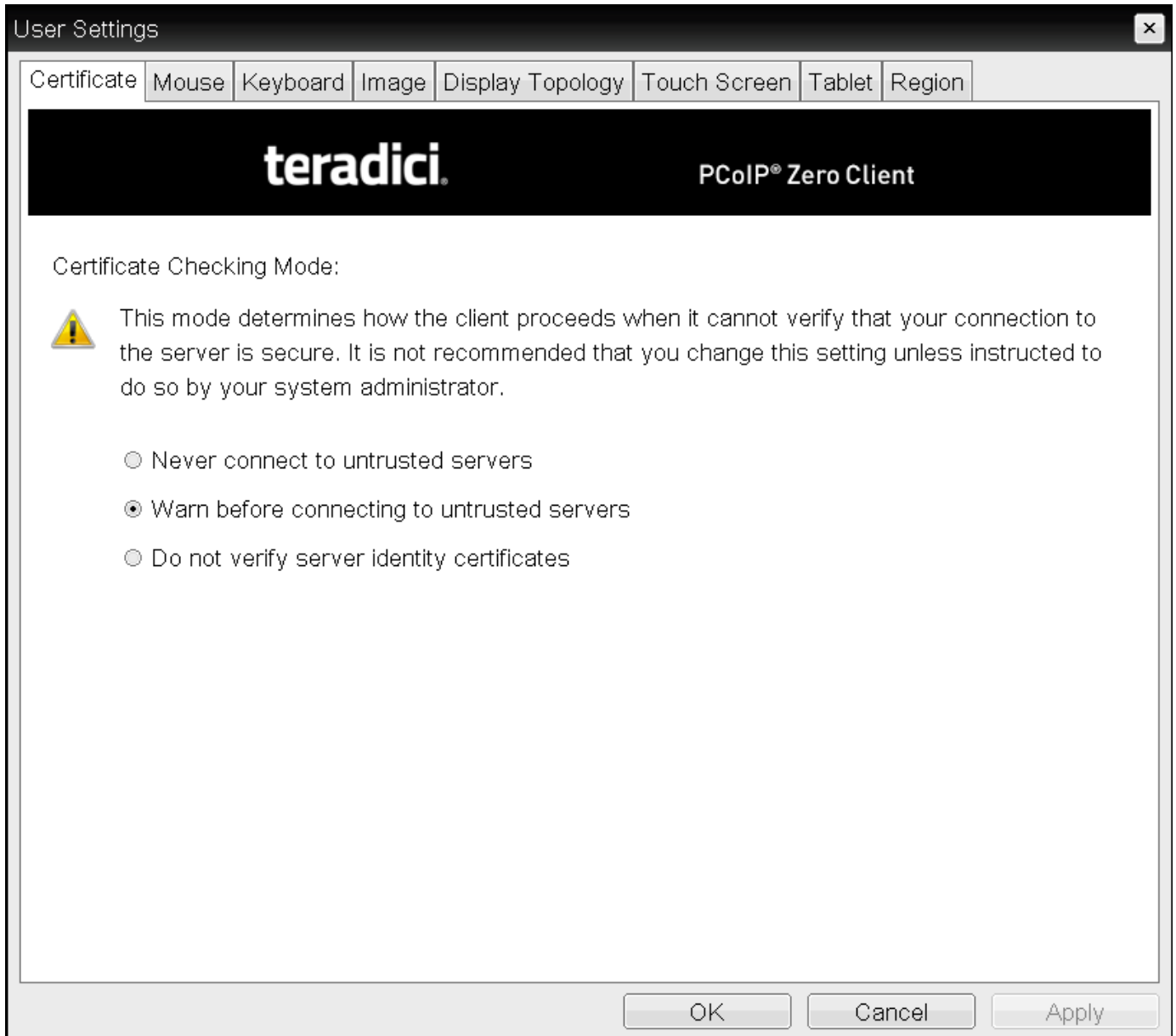
Out of the box, the Tera2 PCoIP Zero Client is configured with the following security settings:

- 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

Setting Certificate Checking Mode

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 than 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 1.1 or higher with RSA keys**

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**.

[Log Out](#)
PCoIP® Zero Client

Home Configuration / Permissions / Diagnostics / Info / Upload



Session

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 10.0.155.213

Hide Advanced Options

Wake Host from Low Power State: Wake-On-LAN Enabled + Peer Address:▼

Host Wake MAC Address: 00 - 30 - 04 - 13 - B2 - 8B

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

TLS Security Mode: Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption

Peer-to-Peer Certificate: 2.) endpoint

Disconnect Message Filter: Show All

Enable DSCP:

Enable Congestion Notification:

Apply
Cancel

Establishing a PCoIP Connection

Tera2 PCoIP Zero Clients can connect to the following hardware and software host endpoints:

- PCoIP Remote Workstation cards see [Connecting to PCoIP Remote Workstation Cards](#).
- Teradici Cloud Access Software see [Connecting to Teradici Cloud Access Software](#).
- Amazon WorkSpaces desktops see [Connecting to Amazon WorkSpaces Desktops](#).
- VMware Horizon desktops and applications see [Connecting to VMware Horizon Desktops and Applications](#).

Configuring a Session Connection Type

The Session pages on the AWI and OSD let you configure how the device connects to PCoIP endpoints. The available configuration options depend on the session connection type you select.

Session Connection Types

The following are the main session connection types:

- [Amazon Workspaces](#)
- [Auto Detect](#)
- [Direct to Host](#) (with option for SLP host discovery)
- [PCoIP Connection Manager](#) (with option for Auto-Logon)
- [View Connection Server](#) (with various options)

Amazon Workspaces

The **Amazon WorkSpaces** session connection type allows the client to connect directly to your Amazon WorkSpaces desktop through multi-factor authentication. Amazon WorkSpaces session type uses an Amazon connection manager which requires multi-factor authentication when connecting to Amazon WorkSpaces.

Management Tool	Session Connection Options
AWI	Amazon WorkSpaces
OSD	Amazon WorkSpaces

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

Direct to Host

Connection Managers) do not have to manually reconfigure the session type each time they switch brokers.

Auto Detect is the default session connection type.

Auto Detect Connections

Management Tool	Session Connection Options
AWI	Auto Detect
OSD	Auto Detect

Direct to Host

A Direct to Host session is a direct connection between a Tera2 PCoIP Zero Client and a remote workstation containing a PCoIP Remote Workstation Card. You can specify a Remote Workstation Card's DNS name or IP address, or you can configure clients to use Service Location Protocol (SLP) to discover a host. You can also configure clients to automatically reconnect to a host when a session is lost.

Direct Session Connections

Management Tool	Session Connection Options
AWI	Direct to Host Direct to Host + SLP Host Discovery
OSD	Direct to Host Direct to Host + SLP Host Discovery

PCoIP Connection Manager

A PCoIP Connection Manager session is a connection between a Tera2 PCoIP Zero Client and a PCoIP endpoint using the PCoIP Connection Manager as a broker. You can configure this session type in basic mode or Auto-Logon mode.

PCoIP Connection Manager Connections

Management Tool	Session Connection Options
AWI	PCoIP Connection Manager PCoIP Connection Manager + Auto-Logon
OSD	PCoIP Connection Manager PCoIP Connection Manager + Auto-Logon

View Connection Server

A VMware Horizon session is a connection between a Tera2 PCoIP Zero Client and a VMware Horizon VDI desktop, DaaS desktop, or RDS-hosted desktop using View Connection Server as the connection manager (also known as the connection broker). You can configure this session type in basic mode, Auto-Logon mode, View Connection Server + Kiosk mode, and View Connection Server + Imprivata OneSign mode.

VMWare RDS-hosted application connections support different session types

VMWare Horizon RDS-hosted application connections are supported on the **View Connection Server**, **View Connection Server + Auto-Logon**, **View Connection Server + Kiosk**, and **View Connection Server + Imprivata OneSign** session types for Tera2 PCoIP Zero Clients. After configuring your View Connection Server, select the [Enable RDS Application Access](#) check box in **Advanced Options** on the Session page.

VMware Horizon Connections

View Connection Server

Management Tool	Session Connection Options
AWI	View Connection Server View Connection Server + Auto-Logon View Connection Server + Kiosk View Connection Server + Imprivata OneSign
OSD	View Connection Server View Connection Server + Auto-Logon View Connection Server + Kiosk View Connection Server + Imprivata OneSign

OSD: Amazon WorkSpaces Session Settings

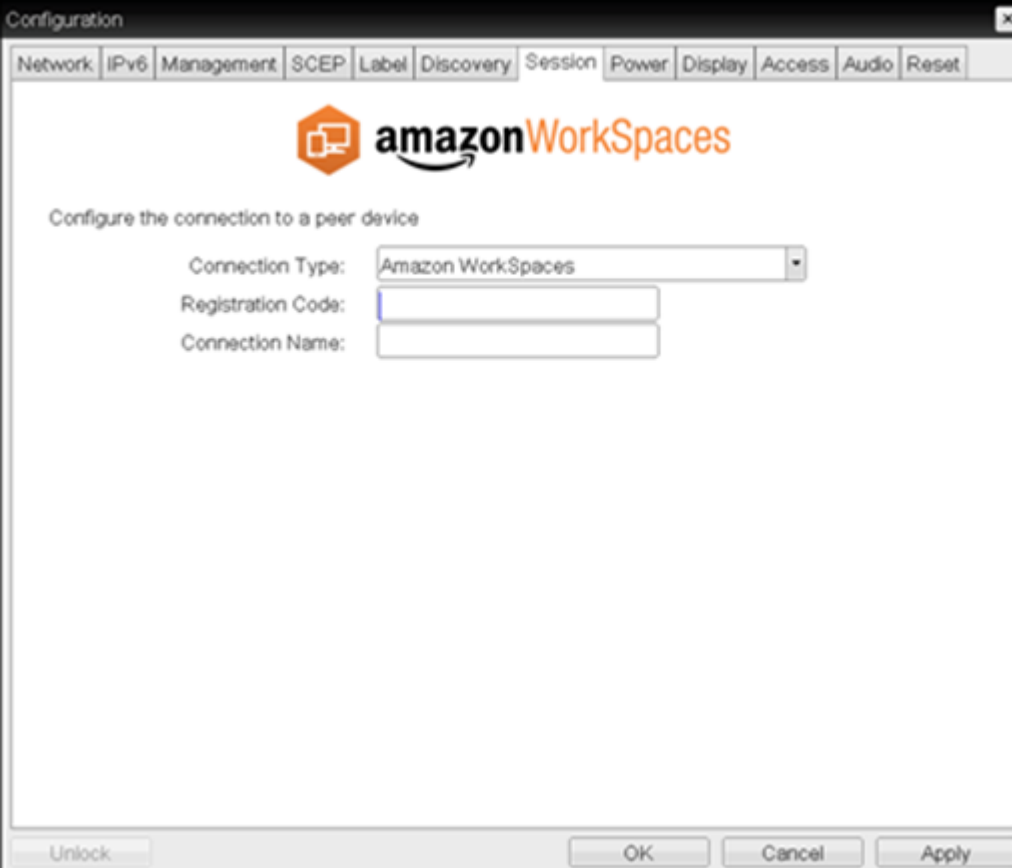
Use the Amazon WorkSpaces session Connection Type to connect directly to your Amazon WorkSpaces desktop through multi-factor authentication. This connection type removes the need to deploy and manage the PCoIP Connection Manager for Amazon WorkSpaces in order to connect zero clients to Amazon WorkSpaces.

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.



Configuration

Network IPv6 Management SCEP Label Discovery Session Power Display Access Audio Reset



Configure the connection to a peer device

Connection Type: Amazon WorkSpaces

Registration Code:

Connection Name:

Unlock OK Cancel Apply

OSD: Amazon WorkSpaces Session Settings

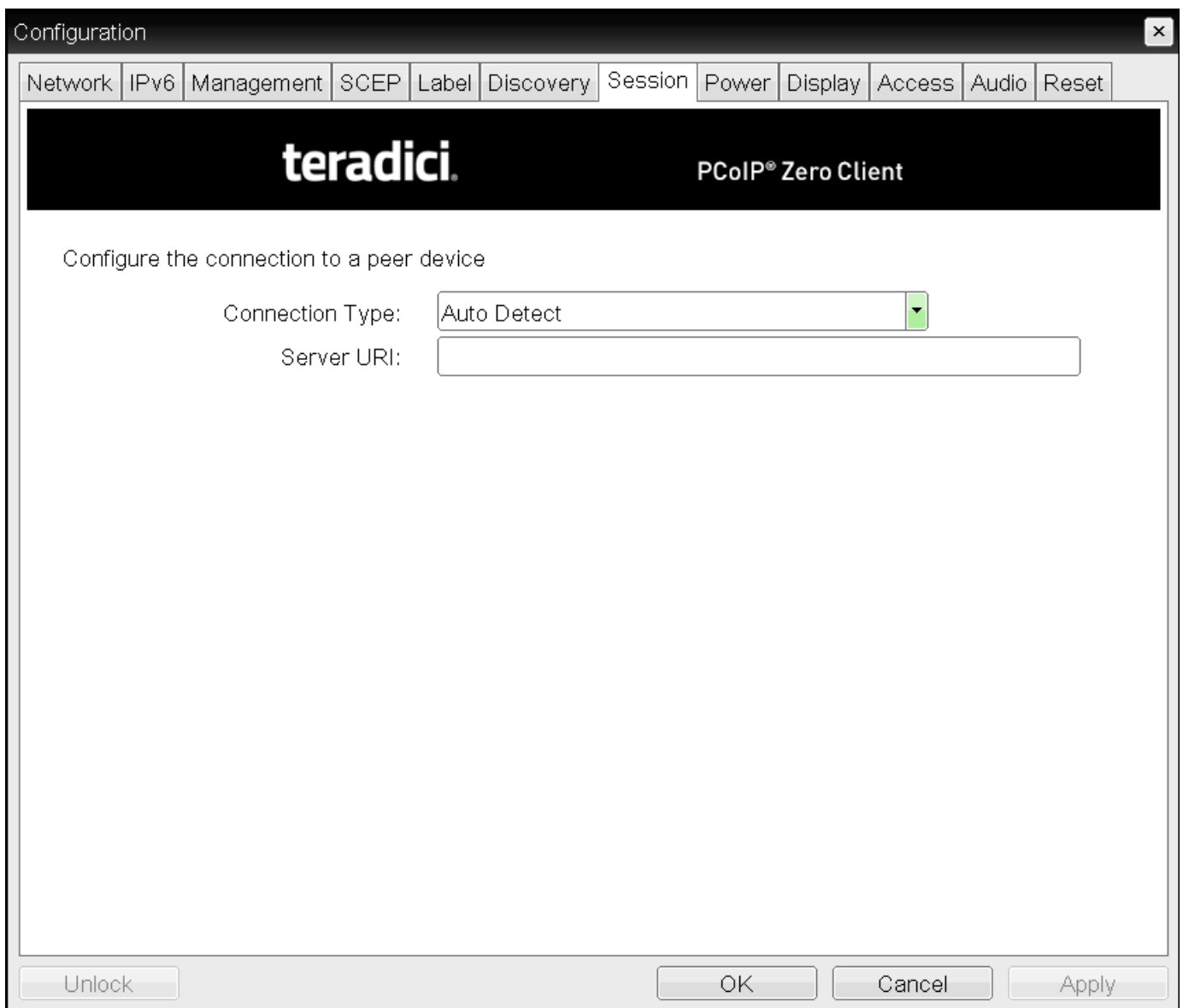
The following parameters can be found on the OSD Session tab for the Amazon WorkSpaces selection.

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.



OSD session connection type – Auto Detect

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

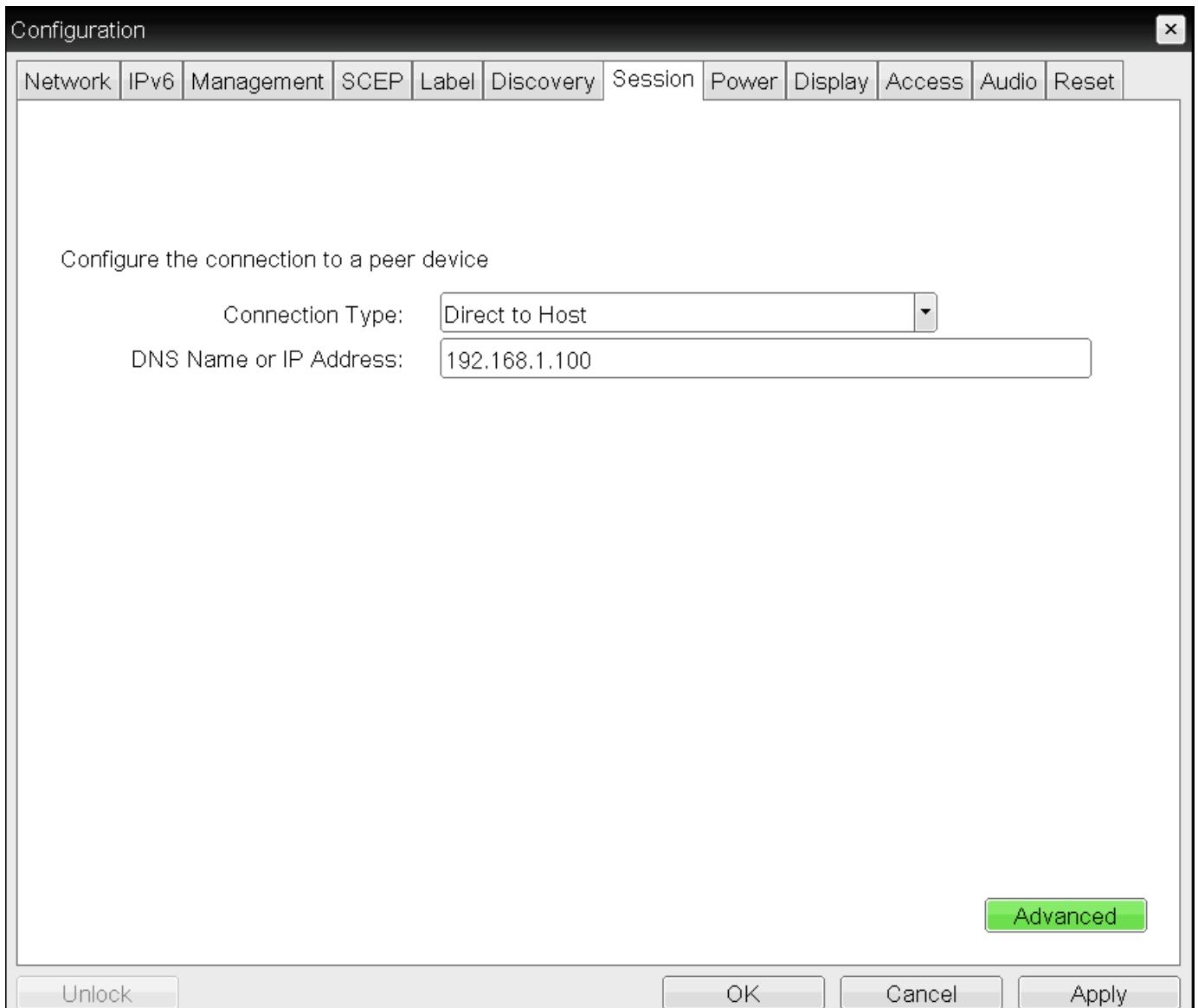
OSD Auto Detect Parameters

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this 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.</p> <p>Type the URL in the form <code>https://<hostname IP address></code> .</p> <p>The URL must be in the form <code>https://<hostname IP address></code></p>

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.



The screenshot shows a window titled "Configuration" with a close button (X) in the top right corner. The window has a tabbed interface with the following tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session (selected), Power, Display, Access, Audio, and Reset. The main content area contains the text "Configure the connection to a peer device". Below this text, there are two fields: "Connection Type:" with a dropdown menu showing "Direct to Host", and "DNS Name or IP Address:" with a text input field containing "192.168.1.100". At the bottom right of the main content area, there is a green button labeled "Advanced". At the bottom of the window, there are four buttons: "Unlock", "OK", "Cancel", and "Apply".

OSD Session Connection Type – Direct to Host

OSD: Direct to Host Session Settings

The screenshot shows a dialog box titled "Advanced Settings" with a close button (X) in the top right corner. The dialog contains the following settings:

- Wake Host from Low Power State: Wake-On-LAN Enabled + Peer Address (dropdown menu)
- Host Wake MAC Address: 00 - 00 - 00 - 00 - 00 - 00 (text input)
- Host Wake IP Address: 192 . 168 . 110 . 100 (text input)
- Enable Auto-Reconnect:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Disconnect Message Filter: Show All (dropdown menu)

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Advanced Settings

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

OSD Direct to Host Parameters

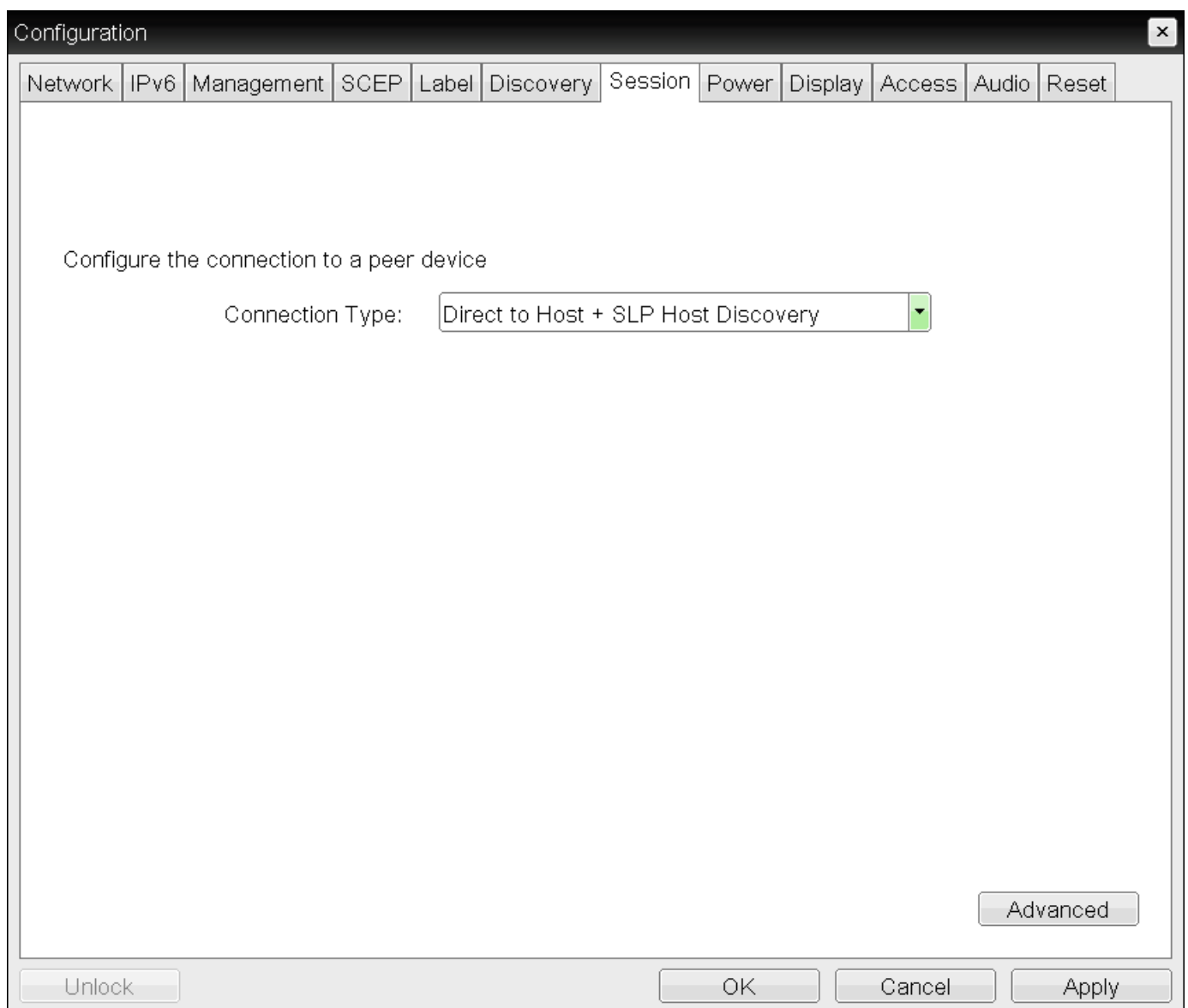
OSD: Direct to Host Session Settings

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the host.
Wake Host from Low Power State	<p>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 .</p> <ul style="list-style-type: none"> • 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 host 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 host 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. <p>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 <i>Power page</i>.</p>
Host Wake MAC Address	<p>Enter the host's MAC address to complete the host wake up configuration when Wake-On-LAN Enabled + Custom Address is selected.</p> <p>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.</p>
Host Wake IP Address	<p>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.</p>
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	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.

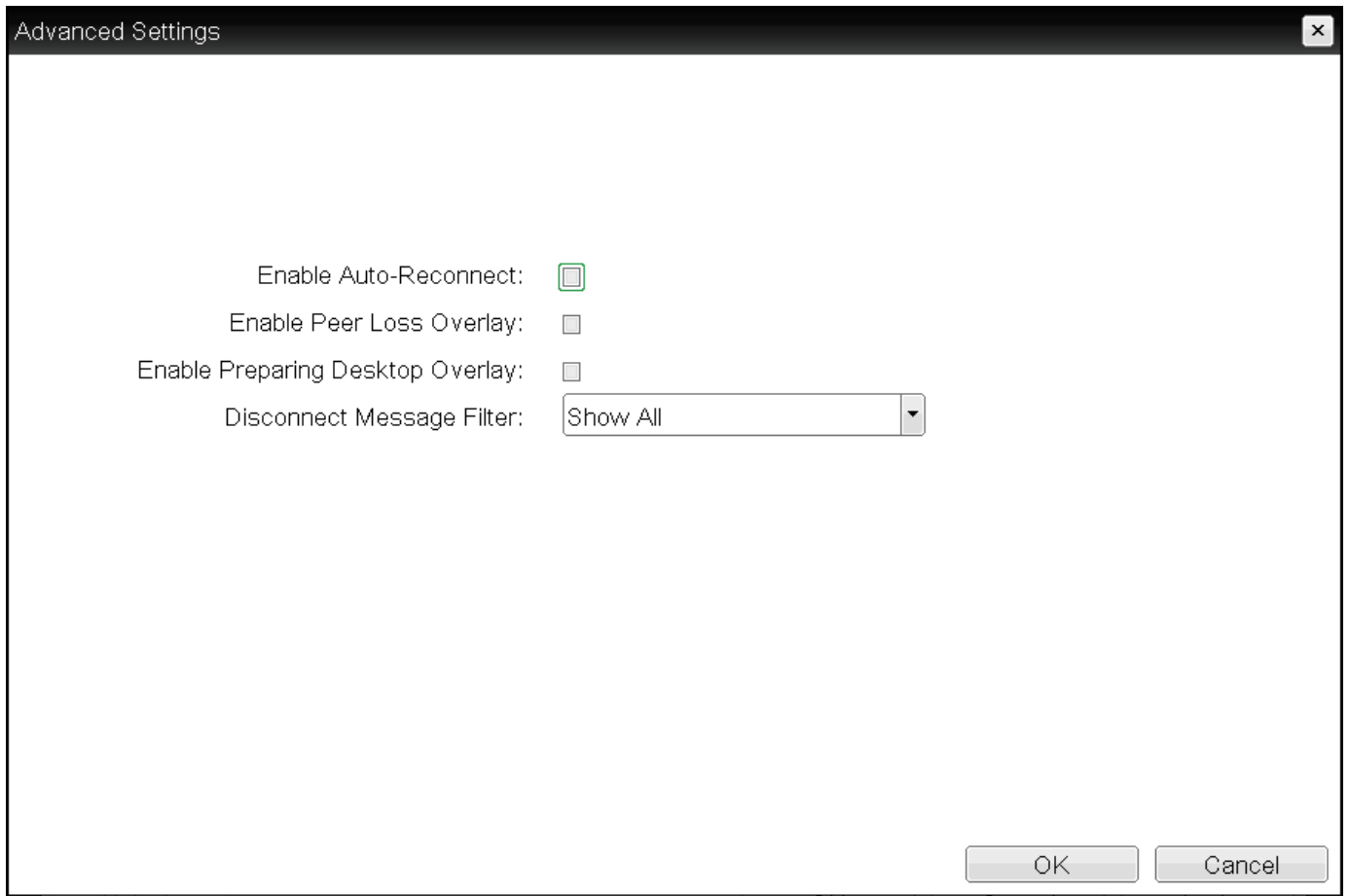
OSD: Direct to Host + SLP Host Discovery Session Settings

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.

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

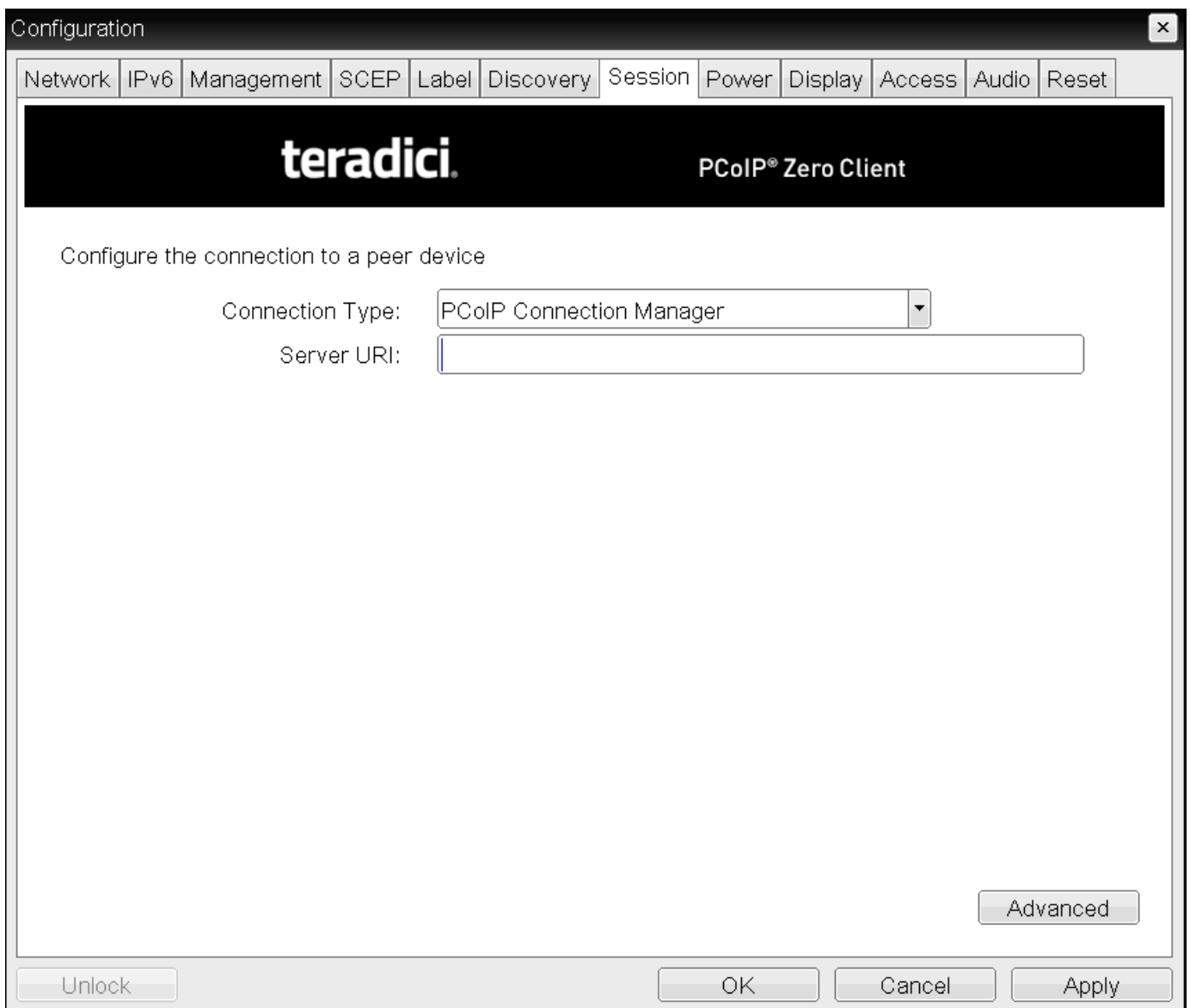
OSD: Direct to Host + SLP Host Discovery Session Settings

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	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p>This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • 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. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • 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 (0x201). Contact your IT

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.

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



The screenshot shows the 'Configuration' window for a Teradici PCoIP Zero Client. The 'Session' tab is selected in the top navigation bar. The window title is 'Configuration' and it includes a close button (X) in the top right corner. The main content area features the Teradici logo and the text 'PCoIP® Zero Client'. Below this, the instruction 'Configure the connection to a peer device' is displayed. The 'Connection Type' is set to 'PCoIP Connection Manager' in a dropdown menu, and the 'Server URI' field is empty. At the bottom right of the main area is an 'Advanced' button. The bottom of the window contains an 'Unlock' button on the left and 'OK', 'Cancel', and 'Apply' buttons on the right.

OSD Session connection type – PCoIP Connection Manager

OSD: PCoIP Connection Manager Session Settings

The screenshot shows a window titled "Advanced Settings" with a close button (X) in the top right corner. The window has a black header bar with the "teradici." logo on the left and "PCoIP® Zero Client" on the right. The main content area is white and contains the following settings:

- Desktop Name to Select: [Empty text input field]
- Auto Connect: [Dropdown menu with "Disabled" selected]
- Remember Username:
- Auto Launch If Only One Desktop:
- Use OSD Logo For Login Banner:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Disconnect Message Filter: [Dropdown menu with "Show All" selected]
- Organization ID: [Empty text input field]

At the bottom right of the dialog, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD PCoIP Connection Manager Parameters

OSD: PCoIP Connection Manager Session Settings

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.</p> <p>The URL must be in the form https://<hostname> or https://<ip address>.</p>
Desktop Name to Select	Enter the desktop name used by the client when starting a session.
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p> <p>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.</p> <p>After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p>This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
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	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p>This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

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.

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

Take precautions to secure zero clients

Passwords are stored locally in retrievable form when 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.

The image shows a configuration window titled "Configuration" with a close button (X) in the top right corner. Below the title bar is a navigation menu with tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The "Session" tab is currently selected. The main content area has a black header with the "teradici" logo on the left and "PCoIP® Zero Client" on the right. Below the header, the text "Configure the connection to a peer device" is displayed. The configuration fields are as follows:

- Connection Type: A dropdown menu with "PCoIP Connection Manager + Auto-Logon" selected.
- Server URI: An empty text input field.
- User name: An empty text input field.
- Password: An empty text input field.
- Domain: An empty text input field.

At the bottom right of the configuration area is an "Advanced" button. At the bottom of the window are four buttons: "Unlock", "OK", "Cancel", and "Apply".

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

The screenshot shows a window titled "Advanced Settings" with a close button in the top right corner. The window has a black header bar with the "teradici." logo on the left and "PCoIP® Zero Client" on the right. Below the header, the settings are as follows:

- Desktop Name to Select: [Empty text input field]
- Auto Connect: [Dropdown menu with "Disabled" selected]
- Auto Launch If Only One Desktop: [Unchecked checkbox]
- Use OSD Logo For Login Banner: [Unchecked checkbox]
- Enable Peer Loss Overlay: [Unchecked checkbox]
- Enable Preparing Desktop Overlay: [Unchecked checkbox]
- Disconnect Message Filter: [Dropdown menu with "Show All" selected]

At the bottom right of the dialog, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD PCoIP Connection Manager + Auto-Logon Parameters

OSD: PCoIP Connection Manager + Auto-Logon Session Settings

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.</p> <p>The URL must be in the form https://<hostname> or https://<ip address>.</p>
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.
Desktop Name to Select	Enter the desktop name used by the client when starting a session.
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p> <p>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.</p> <p>After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p>This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
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	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss

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: View Connection Server Session Settings

The image shows a VMware Horizon Configuration window titled "Configuration" with a close button (X) in the top right corner. The window has a tabbed interface with the following tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The "Session" tab is currently selected. Below the tabs is a blue header bar with the VMware Horizon logo. The main content area is titled "Configure the connection to a peer device" and contains two fields: "Connection Type:" with a dropdown menu set to "View Connection Server", and "DNS Name or IP Address:" with an empty text input field. At the bottom right of the main area is an "Advanced" button. The bottom of the window features a row of four buttons: "Unlock", "OK", "Cancel", and "Apply".

OSD Session connection type – View Connection Server

OSD: View Connection Server Session Settings

The screenshot shows a window titled "Advanced Settings" with the VMware Horizon logo at the top. Below the logo, the text reads "Configure the advanced View Connection Server settings for the device". The settings are as follows:

- Pool Name to Select: [Empty text box]
- Port: [Empty text box] Leave blank for default
- Auto Connect: [Disabled] (dropdown menu)
- Remember Username:
- Auto Launch If Only One Pool:
- Use OSD Logo For Login Banner:
- Prefer GSC-IS:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Enable RDS Application Access:
- Enable IPv6 Address Resolution:
- Prefer IPv6 for FQDN Resolution:
- Disconnect Message Filter: [Show All] (dropdown menu)

At the bottom right, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD View Connection Server Parameters

OSD: View Connection Server Session Settings

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	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <p>This field is case-insensitive.</p>
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	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p> <p>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.</p> <p>After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
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 selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of

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 zero clients

Passwords are stored locally in retrievable form when 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.

The image shows a VMware Horizon Configuration window titled "Configuration" with a close button (X) in the top right corner. The window has a tabbed interface with the following tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The "Session" tab is currently selected. Below the tabs is a blue header bar with the VMware Horizon logo. The main content area is titled "Configure the connection to a peer device" and contains the following fields:

- Connection Type: A dropdown menu with "View Connection Server + Auto-Logon" selected.
- DNS Name or IP Address: A text input field.
- User name: A text input field.
- Password: A text input field.
- Domain: A text input field.

At the bottom right of the main content area is an "Advanced" button. At the bottom of the window are four buttons: "Unlock", "OK", "Cancel", and "Apply".

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

OSD: View Connection Server + Auto-Logon Session Settings

The screenshot shows a dialog box titled "Advanced Settings" with the VMware Horizon logo at the top. Below the logo, the text reads "Configure the advanced View Connection Server settings for the device". The settings are as follows:

- Pool Name to Select: [Empty text box]
- Port: [Empty text box] Leave blank for default
- Auto Connect: [Disabled] (dropdown menu)
- Auto Launch If Only One Pool:
- Use OSD Logo For Login Banner:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Enable RDS Application Access:
- Enable IPv6 Address Resolution:
- Prefer IPv6 for FQDN Resolution:
- Disconnect Message Filter: [Show All] (dropdown menu)

At the bottom right, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD View Connection Server + Auto-Logon Parameters


OSD: View Connection Server + Auto-Logon Session Settings

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.
Pool Name to Select	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <p>This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p>
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	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p> <p>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.</p> <p>After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>For Tera1 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop.</p> <p>This feature only applies to users who are entitled to a single desktop. It does not apply to</p>

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 zero clients**

Passwords are stored locally in retrievable form when 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.

The image shows a VMware Horizon Configuration window titled "Configuration" with a close button (X) in the top right corner. The window has a tabbed interface with the following tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The "Session" tab is currently selected. Below the tabs is a blue header with the VMware Horizon logo. The main content area is titled "Configure the connection to a peer device" and contains the following fields and options:

- Connection Type:** A dropdown menu set to "View Connection Server + Kiosk".
- DNS Name or IP Address:** An empty text input field.
- Radio Buttons:** Two options are present: "Zero Client MAC" (selected with a radio button) and "Custom" (unselected).
- Username:** A text input field containing "CM-02:50:56:97:27:92".
- Password:** An empty password input field.
- Advanced:** A button located at the bottom right of the configuration area.

At the bottom of the window, there are four buttons: "Unlock", "OK", "Cancel", and "Apply".

OSD Session connection type – View Connection Server + Kiosk

OSD: View Connection Server + Kiosk Session Settings

The screenshot shows a dialog box titled "Advanced Settings" with the VMware Horizon logo at the top. Below the logo, the text reads "Configure the advanced View Connection Server settings for the device". The settings are as follows:

- Port: Leave blank for default
- Use OSD Logo For Login Banner:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Enable RDS Application Access:
- Enable IPv6 Address Resolution:
- Prefer IPv6 for FQDN Resolution:
- Disconnect Message Filter:

At the bottom right, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD View Connection Server + Kiosk Parameters

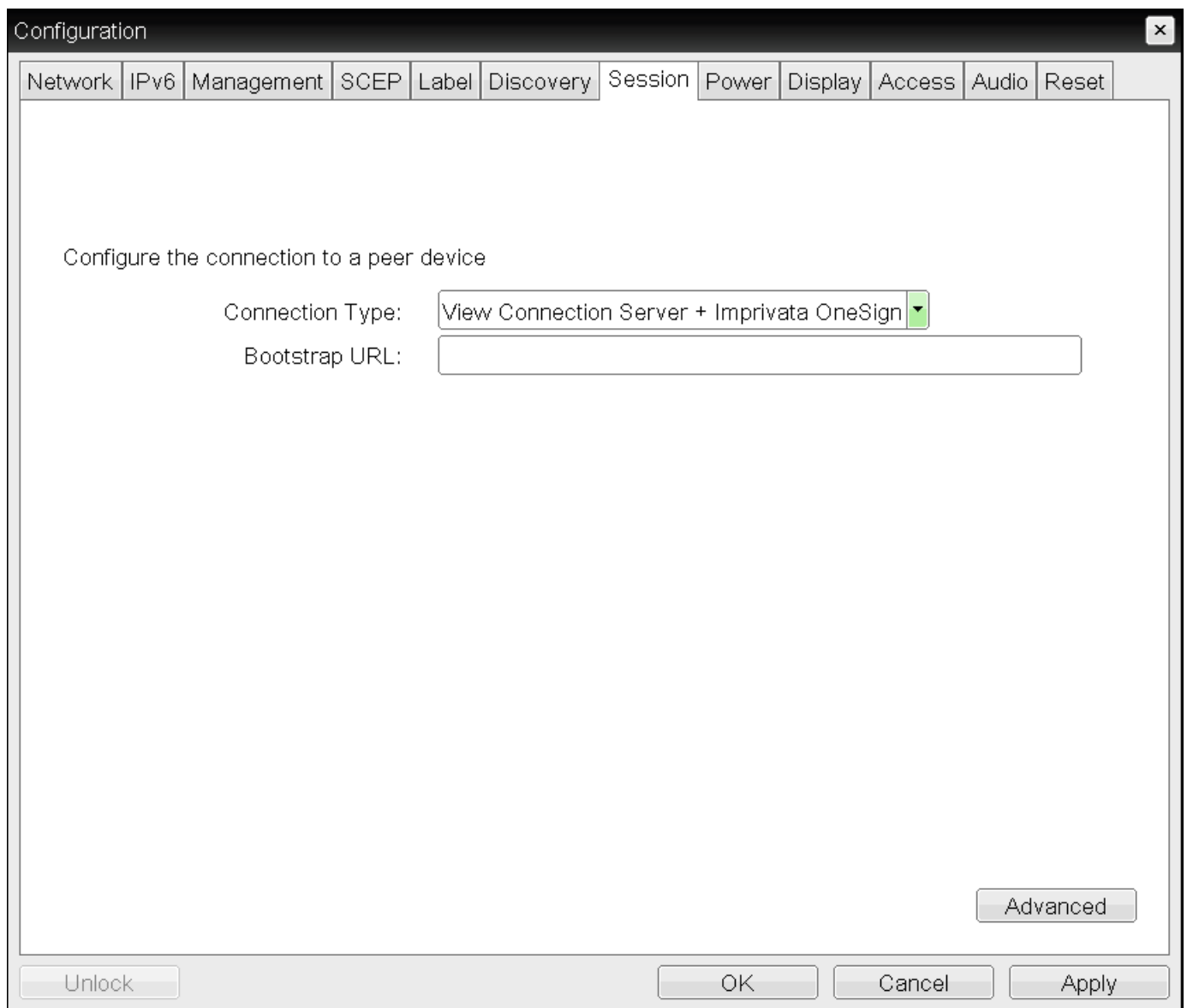
OSD: View Connection Server + Kiosk Session Settings

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username	<p>Select the type of user name that matches the naming you use for the devices on the View Connection Server.</p> <ul style="list-style-type: none"> • 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'. <p>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.</p>
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	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p>This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable RDS Application Access	<p>When enabled and users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p>Applications open in full-screen mode, but can be re-sized once users are in session.</p>
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.

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.



The screenshot shows a 'Configuration' dialog box with a tabbed interface. The 'Session' tab is selected. The dialog contains the following elements:

- Tabbed interface: Network, IPv6, Management, SCEP, Label, Discovery, **Session**, Power, Display, Access, Audio, Reset.
- Text: 'Configure the connection to a peer device'
- Form fields:
 - Connection Type: A dropdown menu with 'View Connection Server + Imprivata OneSign' selected.
 - Bootstrap URL: An empty text input field.
- Buttons: 'Advanced' (bottom right), 'Unlock' (bottom left), 'OK', 'Cancel', and 'Apply' (bottom center).

OSD Session Connection Type - View Connection Server + Imprivata OneSign

The screenshot shows a dialog box titled "Advanced Settings" with the VMware Horizon logo at the top. Below the logo, the text reads "Configure the advanced View Connection Server settings for the device". The settings are as follows:

- OneSign Pool Name Mode: (dropdown menu)
- Pool Name to Select:
- Remember Username:
- Use OSD Logo For Login Banner:
- Prefer GSC-IS:
- Enable Peer Loss Overlay:
- Enable Preparing Desktop Overlay:
- Enable RDS Application Access:
- Enable IPv6 Address Resolution:
- Prefer IPv6 for FQDN Resolution:
- Disconnect Message Filter: (dropdown menu)

At the bottom right, there are two buttons: "Apply" and "Cancel".

Advanced Settings

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

OSD View Connection Server + Imprivata OneSign Parameters

OSD: View Connection Server + Imprivata OneSign Session Settings

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	<p>Select whether the Pool Name to Select property is used in OneSign mode.</p> <ul style="list-style-type: none"> 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
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 selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC 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.

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. This connection type removes the need to deploy and manage the PCoIP Connection Manager for Amazon WorkSpaces in order to connect 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.

Session

Configure the connection to a device

Session Connection Type: Amazon WorkSpaces ▼

AWS Registration Code:

AWS Connection Name:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers ▼

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Auto Connect: Disabled ▼

Connection Server Cache Mode: Last servers used ▼

Auto Launch If Only One Desktop:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled ▼

TLS Security Mode: Maximum Compatibility: TLS 1.1 or higher with RSA keys ▼

Disconnect Message Filter: Show All ▼

Enable DSCP:

Enable Congestion Notification:

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.
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <p>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.</p> <p>After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Connection Server Cache	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

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.

Session
Configure the connection to a device

Session Connection Type:

Server URI:

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) of the current connection broker. Once a successful connection has been made to this 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. The URL must be in the form https://<hostname> or https://<ip address> .

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.

Session

Configure the connection to a device

Session Connection Type:

DNS Name or IP Address:

Wake Host from Low Power State:

Host Wake MAC Address:

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode:

Session Negotiation Cipher Suites:

Disconnect Message Filter:

Enable DSCP:

Enable Congestion Notification:

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

AWI: Direct to Host Session Settings

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the Remote Workstation Card.
Wake Host from Low Power State	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>If the host 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 host 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.</p> <p>The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet.</p> <p>You can disable the Wake-On-LAN feature from the AWI Power page.</p>
Host Wake MAC Address	<p>Enter the host's MAC address to complete the host wake up configuration when Wake-On-LAN Enabled + Custom Address is selected.</p> <p>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.</p>
Host Wake IP Address	<p>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.</p>
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	When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the 'Zero

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.

Session

Configure the connection to a device

Session Connection Type: Direct to Host + SLP Host Discovery ▼

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled ▼

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys ▼

Disconnect Message Filter: Show All ▼

Enable DSCP:

Enable Congestion Notification:

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

AWI: Direct to Host + SLP Host Discovery Session Settings

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.
Enable Session Disconnect Hotkey	When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the 'Zero Client Control Panel' overlay, which lets them disconnect the current session on the workstation or power off the workstation. <ul style="list-style-type: none"> • Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. 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). <ul style="list-style-type: none"> • 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. <p>This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
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. <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.1 or higher with RSA keys: This option provides maximum compatibility. • Suite B: TLS 1.2 with Suite B-compliant 102-bit elliptic curve encryption: This option provides a

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.

Session

Configure the connection to a device

Session Connection Type: PCoIP Connection Manager ▼

Server URI:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers ▼

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Auto Connect: Disabled ▼

Connection Server Cache Mode: Last servers used ▼

Enable Self Help Link:

Auto Launch If Only One Desktop:

Remember Username:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled ▼

TLS Security Mode: Maximum Compatibility: TLS 1.1 or higher with RSA keys ▼

Disconnect Message Filter: Show All ▼

Enable DSCP:

Enable Congestion Notification:

Organization ID:

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

AWI: PCoIP Connection Manager Session Settings

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.</p> <p>The URL must be in the form https://<hostname> or https://<ip address>.</p>
Desktop Name to Select	<p>Enter the desktop name used by the client when starting a session.</p> <p>This field is case-insensitive.</p>
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • 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	<p>When enabled, prevents users from changing the Certificate Check Mode settings from the OSD.</p>
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p> <p>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.</p>
Connection Server Cache Mode	<p>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.</p> <ul style="list-style-type: none"> • 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. • Read-only: Select this option if you want users to select a connection server from a read-

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:

Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Pool Name to Select:

Link Text:

Enable Self Help Link options


When you enable this field, the following options appear:

Enabling the Self Help Link

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.

 **Take precautions to secure zero clients**

Passwords are stored locally in retrievable form when 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.

Session

Configure the connection to a device

Session Connection Type: PCoIP Connection Manager + Auto-Logon

Server URI: https://lterwkstn90.teradici.local

Logon Username:

Logon Password:

Logon Domain Name:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used

Auto Launch If Only One Desktop:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter: Show All

Enable DSCP:

Enable Congestion Notification:

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

AWI: PCoIP Connection Manager + Auto-Logon Session Settings

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.</p> <p>The URL must be in the form 'https://<hostname</p>
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	<p>Enter the desktop name used by the client when starting a session.</p> <p>This field is case sensitive.</p>
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • 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.
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <p>Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page.</p> <p>Disabled: The client does not automatically connect with the connection server.</p> <p>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.</p>

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: View Connection Server Session Settings

Session

Configure the connection to a device

Session Connection Type: View Connection Server
DNS Name or IP Address: view.teradici.com

Hide Advanced Options

Pool Name to Select:

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Trusted View Connection Servers: Show Clear

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used Clear cache entries

Enable Self Help Link:

Auto Launch If Only One Pool:

Remember Username:

Use OSD Logo For Login Banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:

Prefer IPv6 for FQDN Resolution:

Apply Cancel

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

AWI: View Connection Server Session Settings

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.
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 address, or whether it appears in a read-only list for the user to select.

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:

Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Pool Name to Select:

Link Text:

Enable Self Help Link options


When you enable this field, the following options appear:

Enabling the Self Help Link

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 zero clients**

Passwords are stored locally in retrievable form when 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.

Session

Configure the connection to a device

Session Connection Type: View Connection Server + Auto-Logon

DNS Name or IP Address: view.teradici.com

Logon Username:

Logon Password:

Logon Domain Name:

Hide Advanced Options

Pool Name to Select:

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Trusted View Connection Servers: Show Clear

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used Clear cache entries

Auto Launch If Only One Pool:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:

Prefer IPv6 for FQDN Resolution:

Apply Cancel

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

AWI: View Connection Server + Auto-Logon Session Settings

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	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <p>This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p>
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	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • 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	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>
Auto Connect	This field determines the client's auto connect behavior after startup:

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 zero clients

Passwords are stored locally in retrievable form when 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.

Session

Configure the connection to a device

Session Connection Type: View Connection Server + Kiosk

DNS Name or IP Address: view.teradici.com

Username Type: Zero Client MAC

Username: cm-00:30:04:0E:47:B9

Password:

Hide Advanced Options

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Trusted View Connection Servers: Show Clear

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:

Prefer IPv6 for FQDN Resolution:

Apply Cancel

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

AWI: View Connection Server + Kiosk Session Settings

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username Type	<p>Select the type of user name that matches the naming you use for the devices on the View Connection Server.</p> <ul style="list-style-type: none"> • 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	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • 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	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>
Use OSD Logo for Login	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.

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.

Session

Configure the connection to a device

Session Connection Type: View Connection Server + Imprivata OneSign

Bootstrap URL: https://steronesign01.teradici.local

Hide Advanced Options

OneSign Pool Name Mode: Ignore the Pool Name to Select field

Pool Name to Select:

OneSign Appliance Verification: No verification: Connect to any appliance

Direct To View Address:

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: Prevent users from changing the Certificate Check Mode

Trusted View Connection Servers:

Remember Username:

Use OSD Logo For Login Banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

Pre-session Reader Beep: Use Existing Setting

Invert Wiegand Data: Use Existing Setting

Restrict Proximity Cards: Only use proximity cards for tap-in/tap-out

Session Negotiation Cipher Suites: Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:

Prefer IPv6 for FQDN Resolution:

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

AWI: View Connection Server + Imprivata OneSign Session Settings

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	<p>Select whether the Pool Name to Select property is used in OneSign mode.</p> <ul style="list-style-type: none"> • Ignore the Pool Name to Select field • Use the Pool Name to Select field if set <p>For Tera1 PCoIP Zero Clients, this parameter is called OneSign Desktop Name Mode.</p>
Pool Name to Select	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <p>This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p>
Onesign Appliance Verification	<p>Select the level of verification performed on the certificate presented by the OneSign appliance server:</p> <ul style="list-style-type: none"> • 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	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • 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	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.

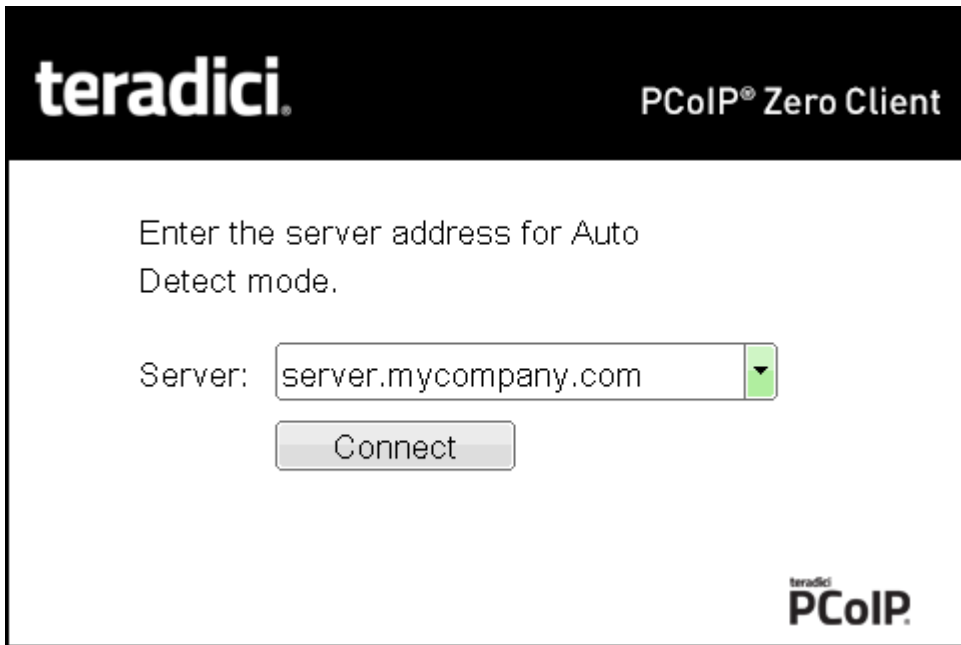
Connecting to a Session

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.

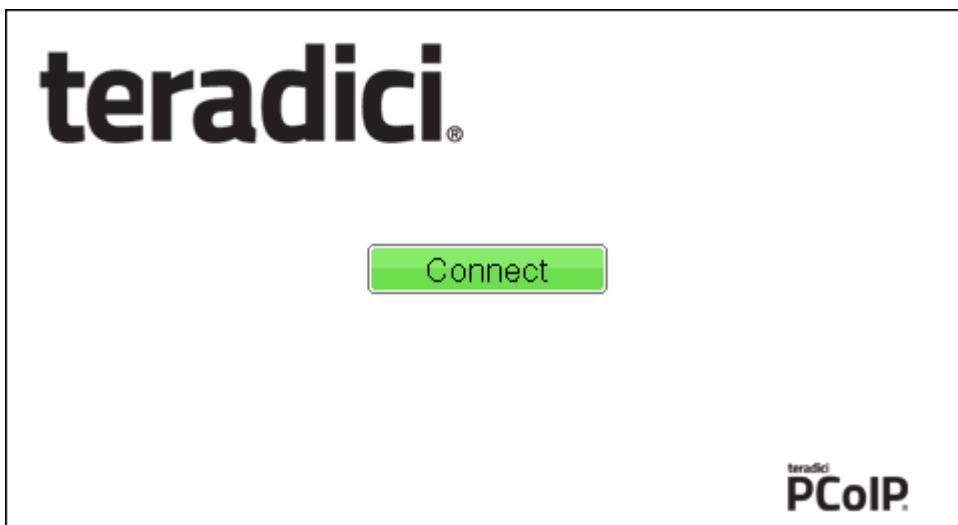
Connecting to a Session from the Connect Window

1. Enter the requested information (for example, server name or IP address for Auto Detect, PCoIP Connection Manager, View Connection Server, and Connection Management Interface connection types), 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.

Appendix A

More information about the supported smart cards and USB smart card readers see [Appendix A: Smart Cards](#).

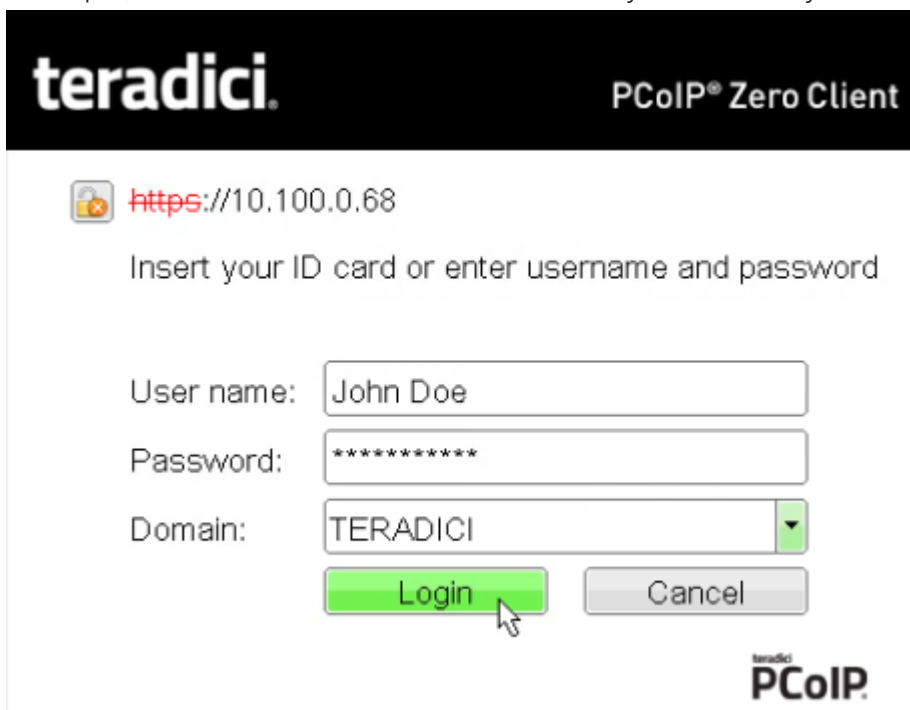
Before connecting to a session using a smart card, connect the USB smart card reader into the Tera2 PCoIP Zero Client.

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.



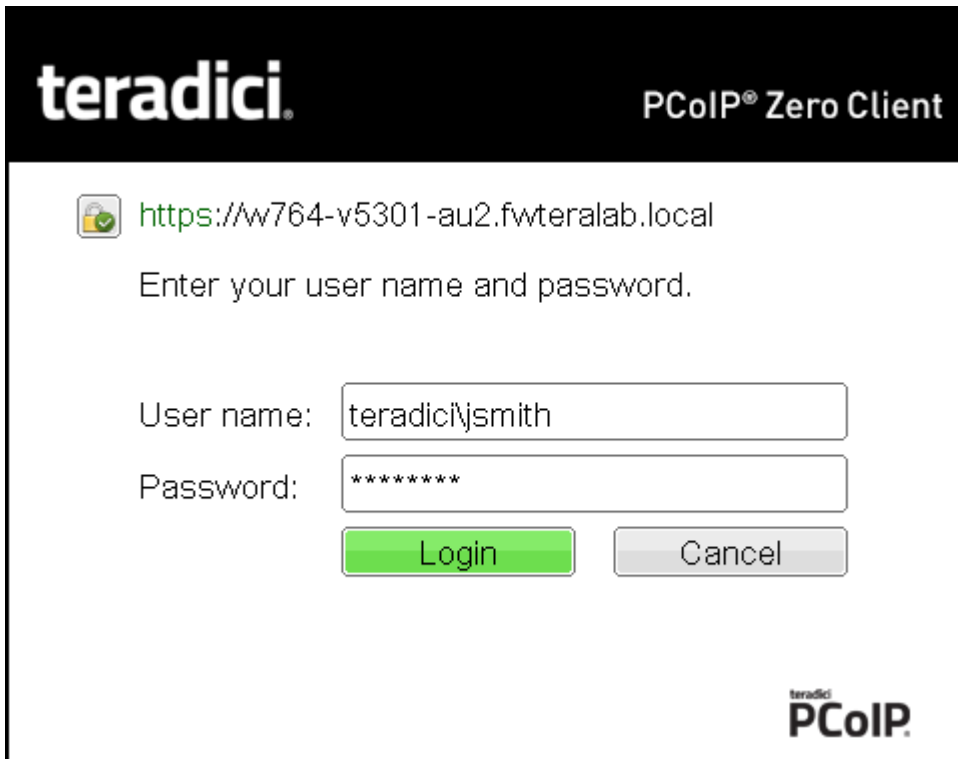
2. If required, type your credentials.

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.

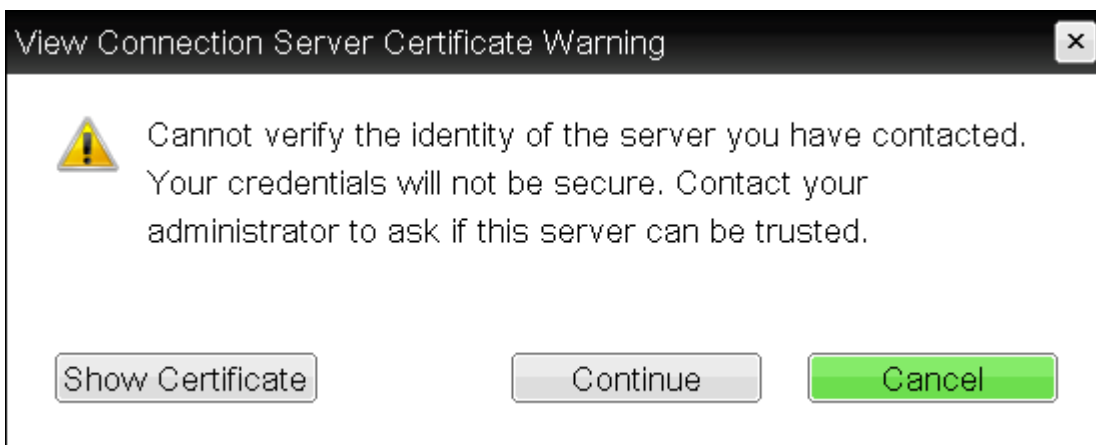
The following image shows the user authentication screen when the Tera2 PCoIP Zero Client trusts the server's certificate. When connecting to other host types, such as VMware Horizon and Amazon WorkSpaces, you will see a similar authentication screen.



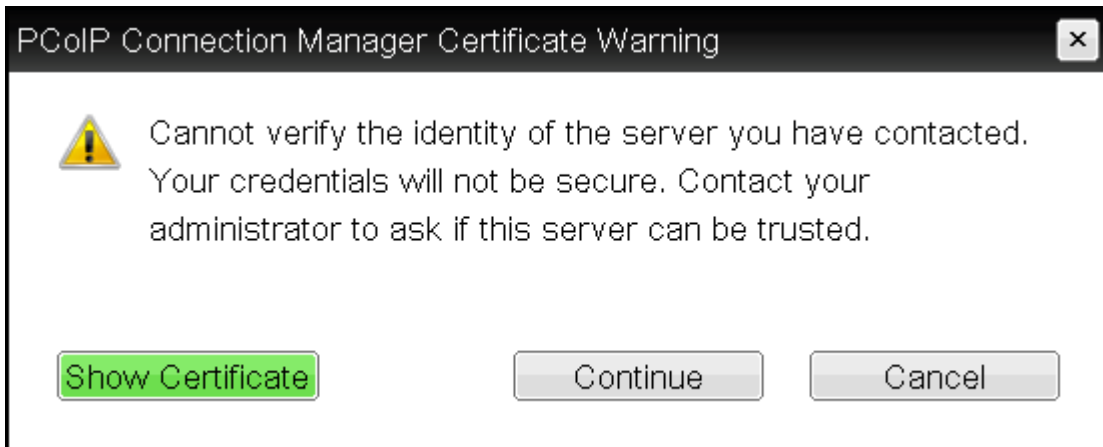
Tera2 PCoIP Zero Client trusted HTTPS connection

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.

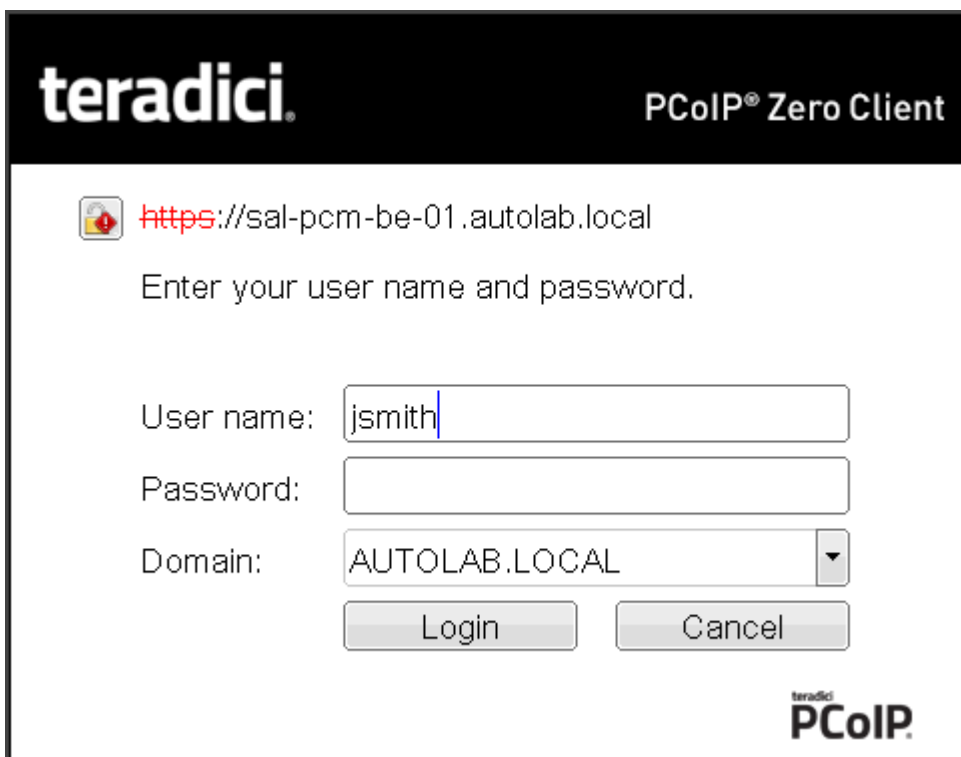


View Connection Server Certificate Warning



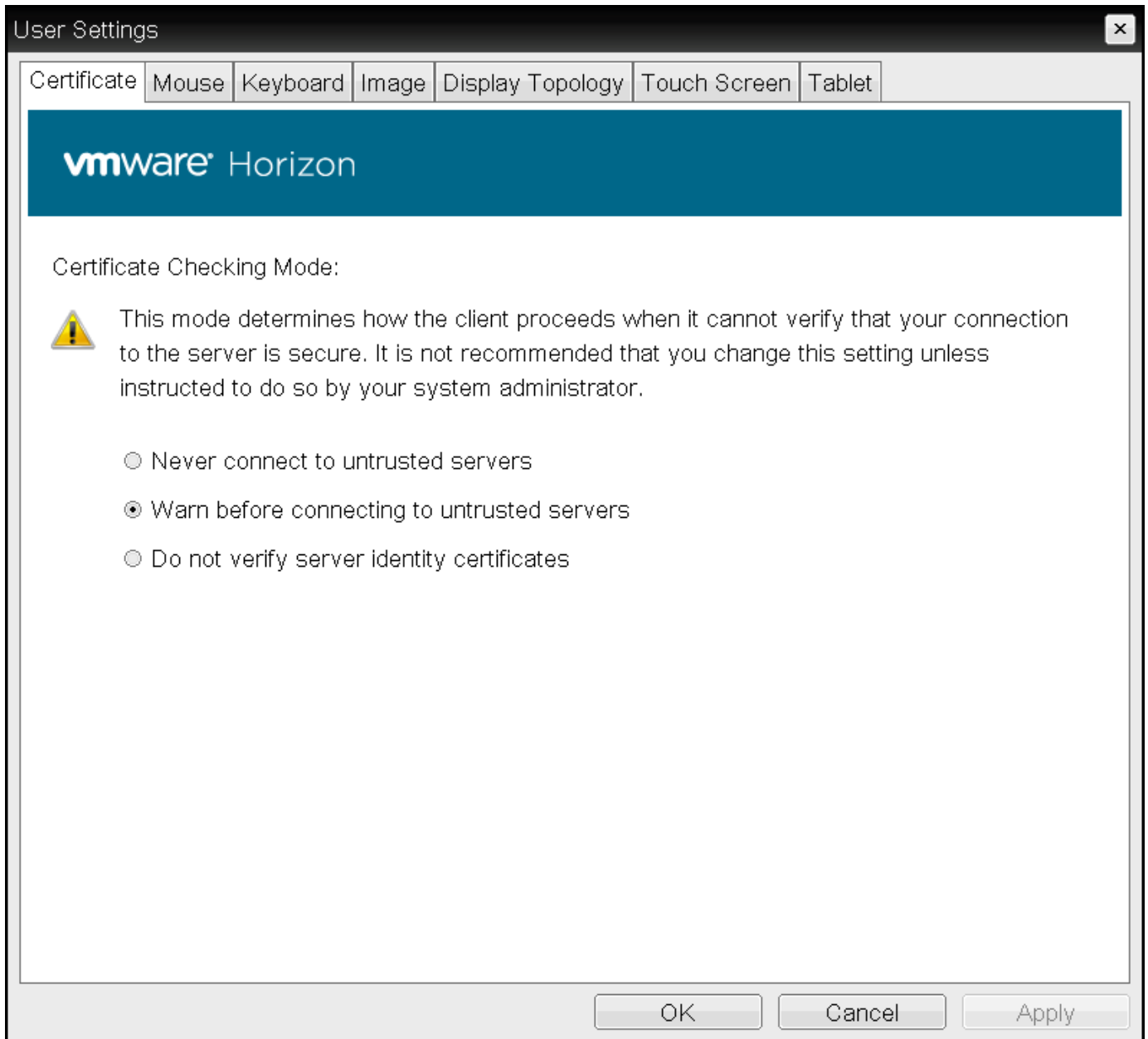
PCoIP Connection Manager Certificate Warning

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.

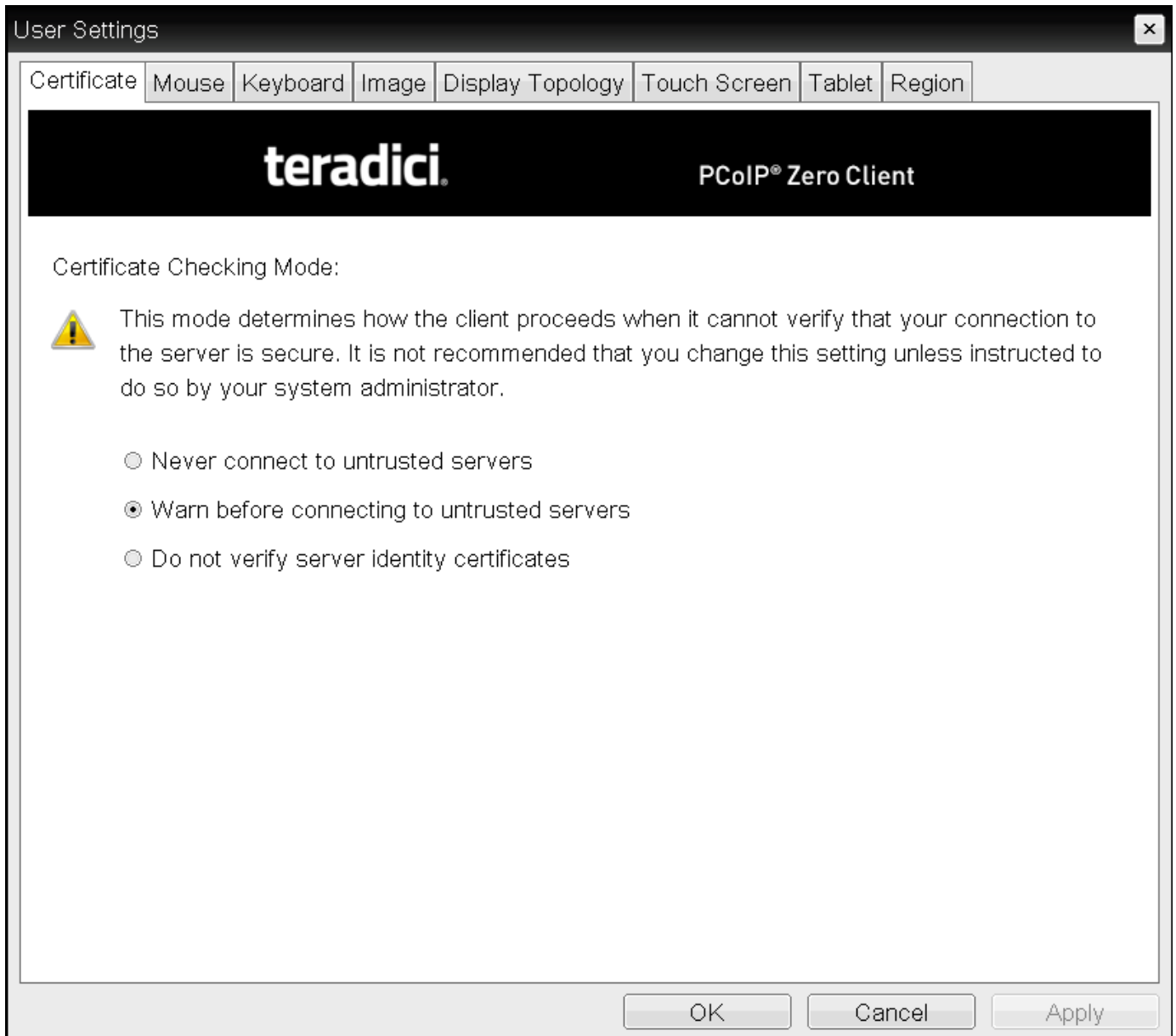


Tera2 PCoIP Zero Client untrusted HTTPS connection

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

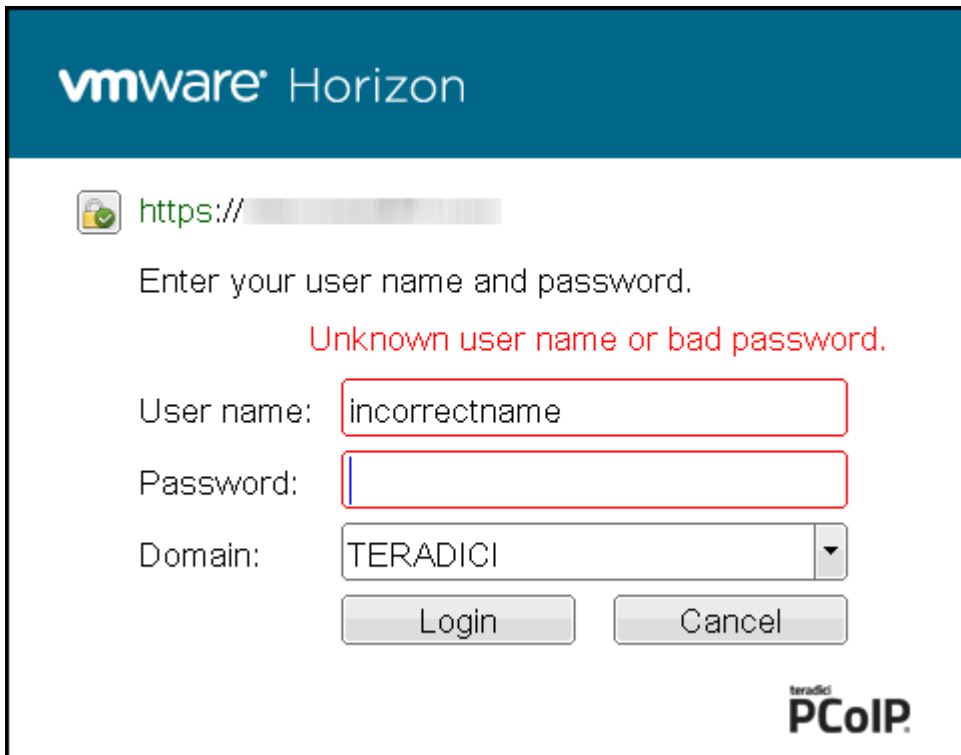


Teradici Certificate Checking Mode

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.

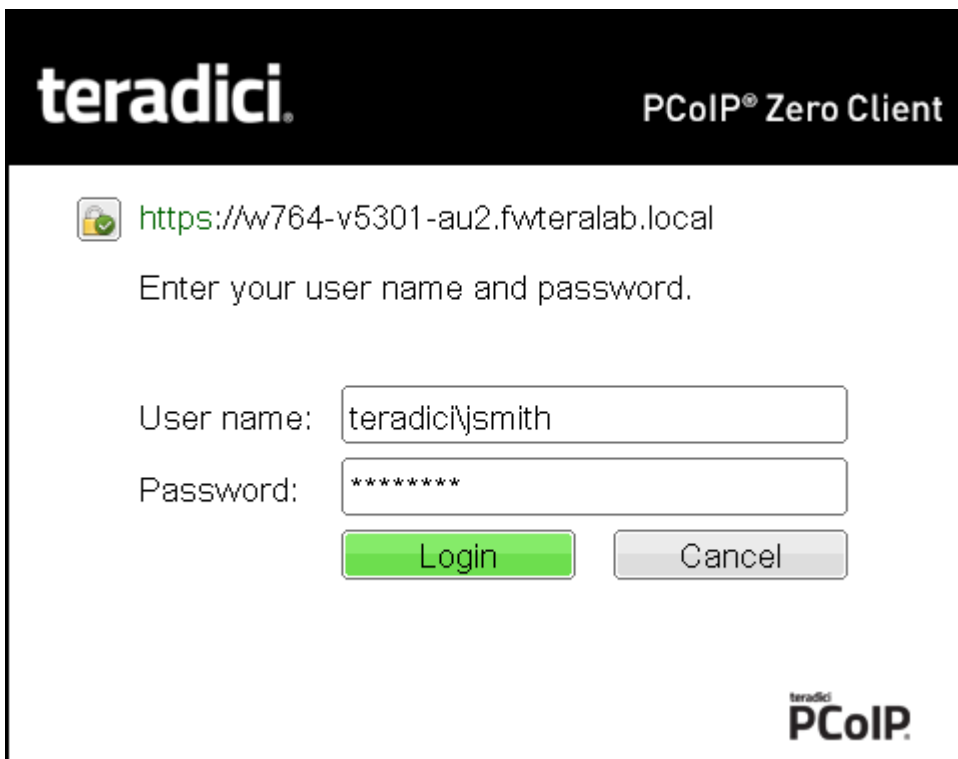
Authenticating the User

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

Connecting to a Desktop



teradici PCoIP® Zero Client

 <https://w764-v5301-au2.fwteralab.local>

Enter your user name and password.

User name:

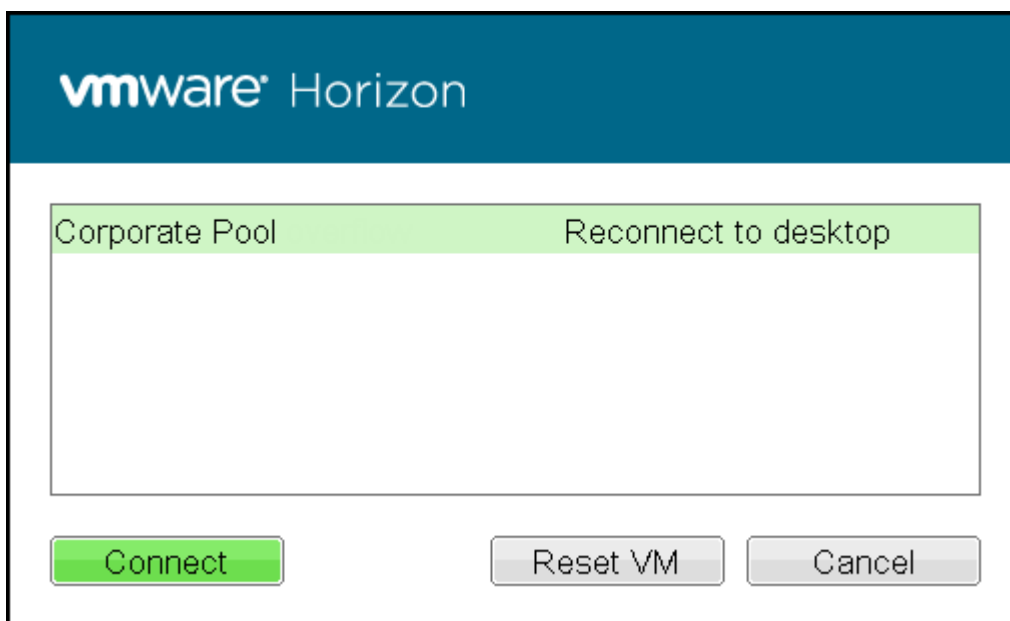
Password:

teradici
PCoIP

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**.



vmware Horizon

Corporate Pool	Reconnect to desktop
----------------	----------------------

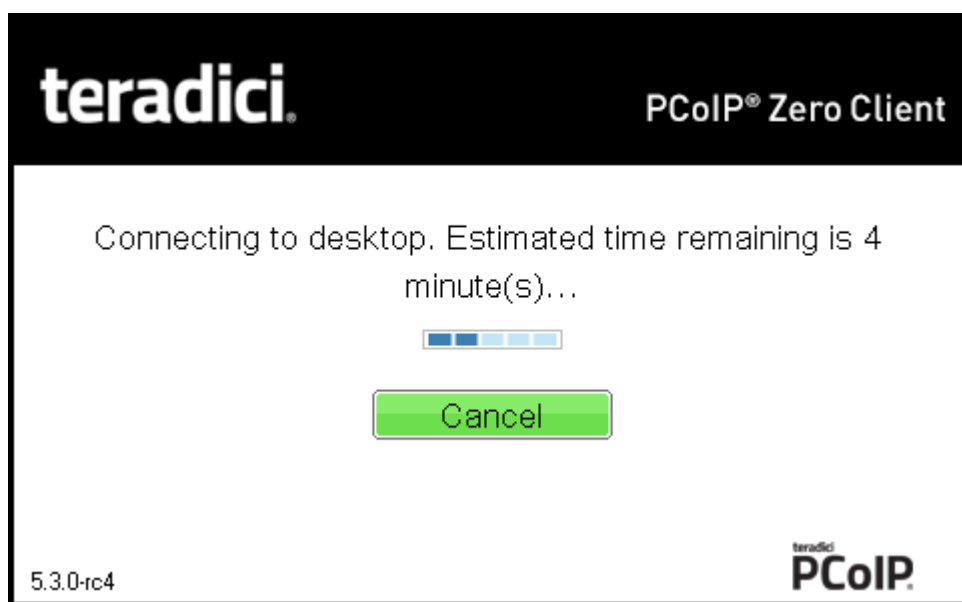
Selecting an entitlement

Connecting to a Desktop

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 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.

Configuration Options

- 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](#)
- [Connecting using a third-party connection broker](#)
- [Connecting using the View Connection Server](#)

Connecting Statically

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 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.

Connecting Using the View Connection Server

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](#).

Connection Instructions

These instructions explain how to configure a Tera2 PCoIP Zero Client to connect to a PCoIP Remote Workstation Card. If you are using a broker to connect, see the documentation from your equipment supplier for instructions on how to configure the broker.

Before connecting, you will need to know the IP address or Fully Qualified Domain Name (FQDN) of your PCoIP Remote Workstation Card.

Connecting Directly Using SLP Host Discovery

After successfully completing the installation steps outlined in [PCoIP® Tera2 Zero Client Quick Start Guide](#), the client will be powered on and ready to use. The next step is to initiate a PCoIP

Connecting Directly Without Using SLP Host Discovery

session with a PCoIP Remote Workstation Card. The easiest way to get started is to use SLP host discovery.

Tera2 PCoIP Zero Client and the host PC must reside on the same subnet

SLP host discovery requires the Tera2 PCoIP Zero Client and host PC to reside on the same subnet. You also need to know the IP address and/or MAC address of the PCoIP Remote Workstation Card so you can select it from the list of available hosts. In addition, the PCoIP Remote Workstation Card must be configured to accept any peer or to accept the specific MAC address of the Tera2 PCoIP Zero Client. You can configure this from the host AWI **Configuration > Session > Direct from Client** page.

To connect directly using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the [Direct to Host + SLP Host Discovery](#) connection type, and click **OK**.
2. Click the **Connect** button.
3. When the **Discovered Hosts** screen appears with a list of available hosts, select your PCoIP Remote Workstation Card by its IP/MAC address pair, and click **OK**.
4. When prompted, enter your remote workstation's login credentials.

Advanced settings

For details about advanced settings, see [Direct to Host + SLP Host Discovery](#).

Connecting Directly Without Using SLP Host Discovery

To connect directly without using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the Direct to Host connection type.
2. Enter the DNS name or IP address of the PCoIP Remote Workstation Card, and click **OK**.
3. Click the **Connect** button.
4. When prompted, enter your remote workstation's login credentials.

Advanced settings

For details about advanced settings, see [Direct to Host](#).

Connecting Using a Broker

To connect using a broker:

1. 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 a third-party broker.
2. Enter the DNS name or IP address of the broker, and click **OK**.
3. Click the **Connect** button.
4. 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.

The Cloud Access Software supports two deployment scenarios:

- Deskside deployment: Connecting directly to a physical workstation.
- Data center deployment: Connecting to a physical or virtualized workstation either directly or via a compatible third-party broker.

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 the Cloud Access Software installed.

For details on available Cloud Access hosts, see the [All Access Architecture Guide](#)

For workstation requirements and Cloud Access agent installation details, see the respective agent Administrators' Guide found at the [Teradici support site](#)

Configuration Options

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

- [AWI: Auto Connect](#)
- [OSD: Auto Connect](#)
- [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 (desktide 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.
 - The 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.
- 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](#).
- You have a PCoIP® Connection Manager for Amazon WorkSpaces appliance installed and configured. See [PCoIP Connection Manager for Amazon WorkSpaces Administrators' Guide](#).

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.

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

You will need to know the IP address of your PCoIP Connection Manager for Amazon WorkSpaces appliance when using this connection type.

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](#)
- [Configuration Options](#)
- [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](#)

Connection Instructions

- [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**.

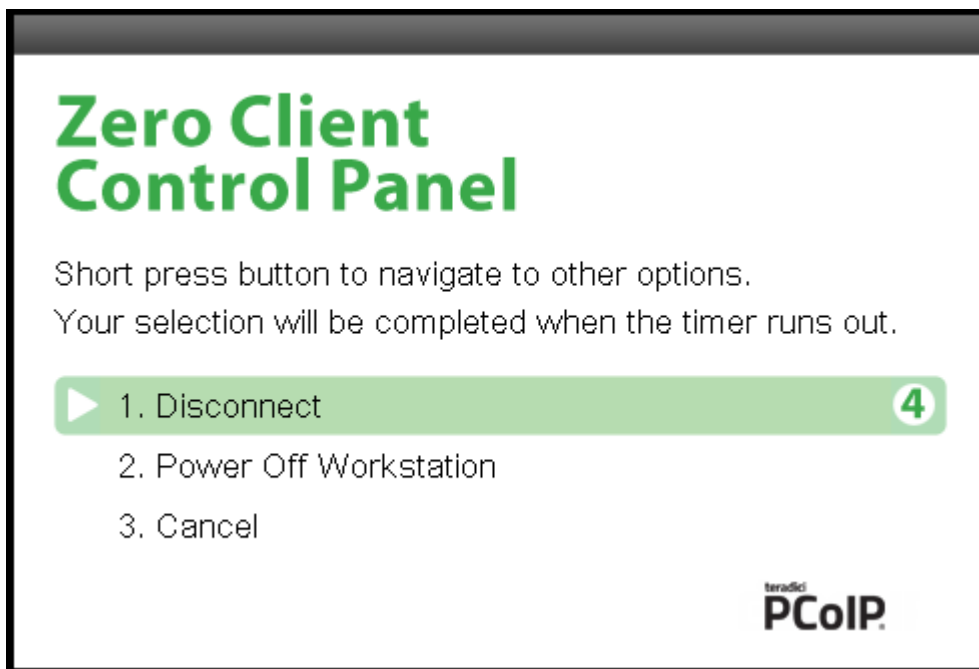
To connect using the View Connection Server and Imprivata OneSign connection type:

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.

!!! Note "Advanced settings For details about advanced settings, see [OSD: View Connection Server + Imprivata OneSign](#).

Disconnecting from a Session

You can disconnect from a virtual desktop session and return to the OSD by pressing the device's **Connect** or **Disconnect** button. However, if a user is in a session with a PCoIP Remote Workstation Card, pressing this button will display the Zero Client Control Panel overlay, which provides options to disconnect from the session, to power off the remote workstation, or to cancel the operation.



Zero Client Control Panel

You can select an option from this overlay in a number of ways:

- Continue to tap the **Connect** or **Disconnect** button to toggle between options until the desired one is highlighted, then wait for the four-second countdown to complete.
- Use the up/down arrow keys on the keyboard to highlight the desired option, and press the Enter key.
- Type the number of the desired option to select it immediately.

During a session, you can also use a **Ctrl**+**Alt**+**F12** hotkey sequence to display this overlay, providing the following options are configured in advance:

- [Enable Session Disconnect Hotkey](#) must be enabled in the advanced options on the **Session – View Connection Server** page.

Disconnecting from a Session

- The **Enable Local Cursor and Keyboard** feature must be enabled on the PCoIP host software on the host computer.
- On the client, the keyboard must be recognized as locally connected (that is, not bridged).

Selecting the disconnect option

To use the up/down arrow keys, or to type in a number to select a disconnect option on this overlay, ensure that **Enable Local Cursor and Keyboard** feature is enabled and the keyboard is locally connected.

For users to use the second overlay option (that is, to power off the workstation), the power permissions on the client must be configured to enable a 'hard' power off. You can set this parameter from the [AWI Power Permissions](#) page.

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](#)

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 the Tera2 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 Mode

	Low		Medium		High
	Automatic	Manual	Automatic	Manual	Manual
Can be discovered by endpoint managers	✓	x	x	x	x
Can automatically discover endpoint managers using DNS	✓	x	✓	x	x
Can trust endpoint managers using DNS	✓	x	x	x	x
Can manually connect to endpoint managers	x	✓	x	✓	✓
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](#).

Medium Security Mode

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 [Staging Clients Using an Endpoint Manager](#).

Additional Security Tip

You can compliment security configurations by disabling the AWI interface and use the PCoIP Management Console to configure your PCoIP Endpoints.

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 3.1 Administrators' Guide](#).

Custom peer-to-peer certificates can also be used to secure 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. 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 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

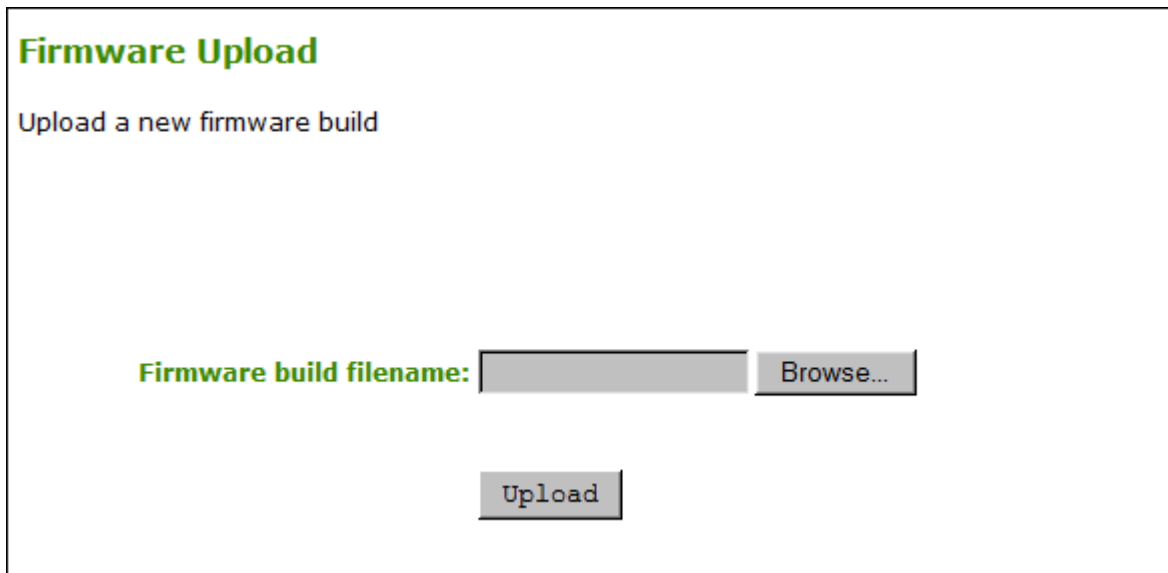
An installed certificate is required to connect to an endpoint manager in *medium* or *high* security levels; however, out of the box, the Tera2 PCoIP Zero Client's local certificate store is empty and it can only connect using the *low* security level.

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**.

Uploading 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.

teradici
PCoIP

Certificate Upload

Upload a certificate in **PEM** format (Must be < 10238 bytes). For **802.1X** and **Peer-to-Peer** certificates, the certificate must contain the **private key** as well.

Certificate filename: No file selected. (Limit of 16 certificates)

Available Storage: 161840 bytes

Uploaded Certificates:

Subject:	Issued By:	Expiration Date:	
1) Philip Suite B Root CA	Philip Suite B Root CA	06/23/2024	<input type="button" value="Details"/> <input type="button" value="Remove"/>
2) endpoint	Philip Suite B Root CA	01/01/2020	<input type="button" value="Details"/> <input type="button" value="Remove"/>

Selected Peer-to-Peer Certificate: (Configured in Session settings)

Selected 802.1X Client Certificate: (Configured in Network settings)

AWI Certificate Upload Page

The maximum certificate size that you can upload from the AWI is 10,237 bytes. You can upload up to 16 certificates providing you don't exceed the maximum storage size of 98,112 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 <i>Client Certificate</i> 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	–	✓	✓	✓
Challenge Password	–	✓	✓	✓
CA Issuer Identifier	–	✓	✓	✓
Root CA	–	✓	✓	✓
Client Certificate	–	✓	✓	✓
Request Certificates (a 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.

The Tera2 PCoIP Zero Client generates its own 2048-bit SCEP RSA private key

When a Tera2 PCoIP Zero Client boots up, the device generates its own 2048-bit SCEP RSA private key. This key is used to construct a PKCS#10-formatted certificate request, which is then delivered to the SCEP server.

SCEP certificate naming conventions

SCEP certificates are configured with the requested certificate Subject as the PCoIP Device Name and the Subject Alternative as the device MAC address (all in lower case and with no dashes). This naming convention is not configurable.

SCEP scenarios and tested SCEP server setups

For information on the best SCEP scenarios and tested SCEP server setups, see [What are the best scenarios and setups Teradici uses to test its implementation of SCEP? \(KB 1366\)](#).

Obtaining Certificates Automatically Using SCEP

The screenshot shows a 'Configuration' window with a tabbed interface. The 'SCEP' tab is selected. The window title is 'Configuration' with a close button (X) in the top right corner. The tabs are: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The main content area is titled 'Configure SCEP (Simple Certificate Enrollment Protocol) settings and request certificates'. It contains the following fields and controls:

- SCEP Server URL:
- Challenge Password:
- Root CA Certificate:
- Client Certificate:
-
- Status:

At the bottom of the window, there are four buttons: 'Unlock', 'OK', 'Cancel', and 'Apply'.

SD SCEP page

The screenshot shows the 'SD SCEP' page. The title is 'SCEP' in green. Below the title is the instruction 'Configure SCEP settings and retrieve certificates'. The page contains the following fields and controls:

- SCEP Server URL:
- Challenge Password:
- Root CA:
- Client Certificate:
-
- Status:

AWI SCEP page

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

Obtaining Certificates Automatically Using SCEP

SCEP Parameters

Parameter	Description
SCEP Server URL	Enter the URL for the SCEP server that is configured to issue certificates for the device.
Challenge Password	Enter the password to present to the SCEP server.
Root CA	Displays the name of the root CA certificate that has been installed in the device.
Client Certificate	Displays the name of the client certificate that has been installed in the device.
Request Certificates	After entering the SCEP server address and password, click this button to retrieve certificates.
Status	Displays the status of the request (for example, in progress, successful, failed).

To obtain certificates automatically from a SCEP server:

1. Open the SCEP page:
 - From the OSD, select **Options > Configuration > SCEP**.
 - From the AWI, select **Configuration > SCEP**.
2. Enter the URL and password for the SCEP server.
3. To retrieve the certificate, click **Request Certificates**. The Root CA and 802.1x certificates display after these certificates are installed.
4. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI. The **Status** section displays the status of the request (for example, in progress, successful, or failed).

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.

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.

Assigning the IP Address 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
```

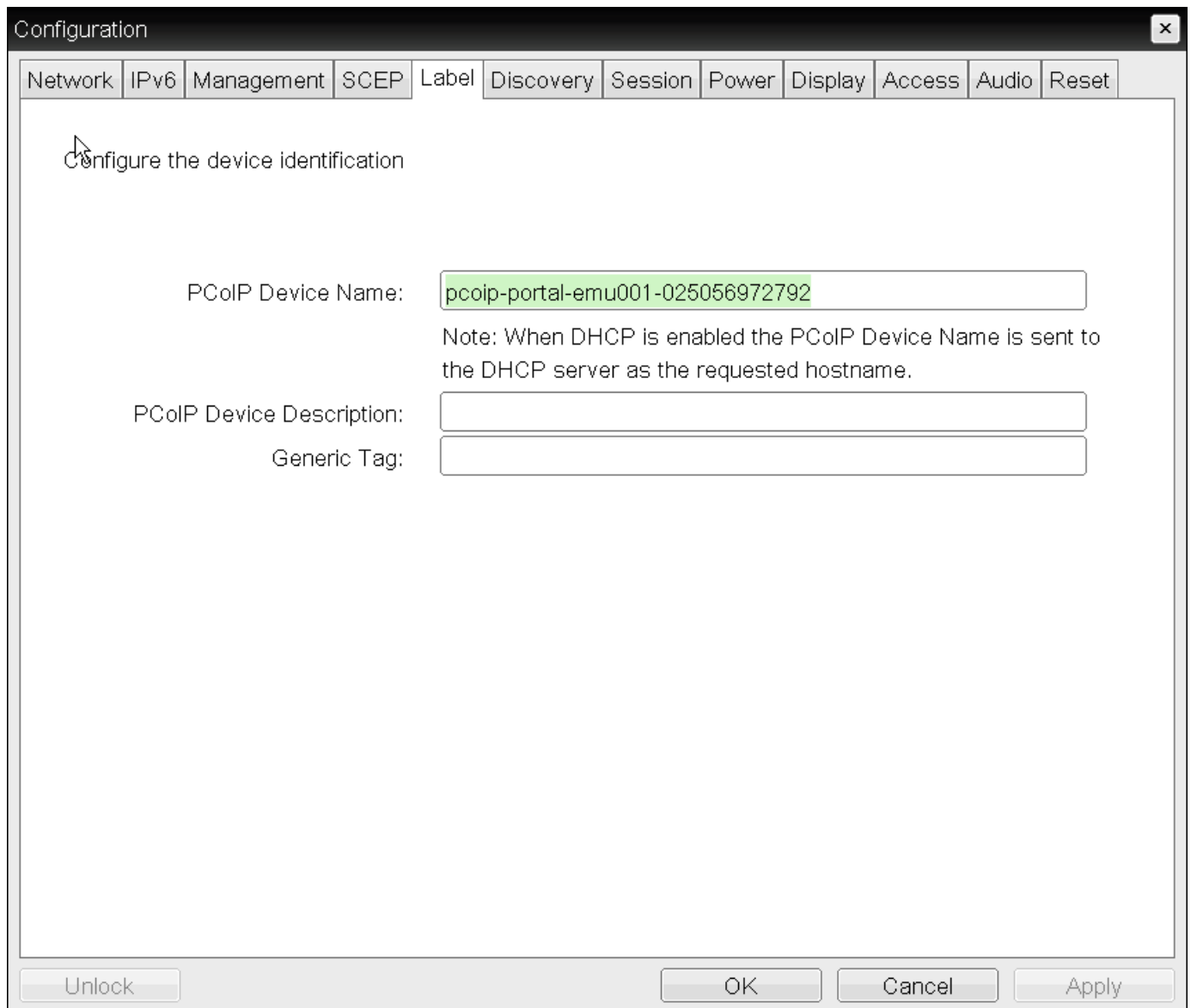
If you reset the client (see [Resetting Your Tera2 PCoIP Zero Client](#)), the static fallback IP address will revert to the factory default, even when it has been set by the PCoIP Management Console.

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

Assigning a Device Name from the AWI

The following parameters display on the OSD Label page:

OSD Label Parameters

Parameter	Description
PCoIP Device Name	<p>Lets you give the device a logical name. The default is pcoip-portal-, where is the device's MAC address.</p> <p>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.</p> <p>It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions:</p> <ul style="list-style-type: none">• 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	<p>A description of the device or other information, such as the location of the device's endpoint.</p> <p>The firmware does not use this field. It is provided for administrator use only.</p>
Generic Tag	<p>Generic tag information about the device.</p> <p>The firmware does not use this field. It is provided for administrator use only.</p>

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.

Assigning a Device Name from the AWI

Label

Change the PCoIP device labels

PCoIP Device Name:

Note: When DHCP is enabled the PCoIP Device Name is sent to the DHCP server as the requested hostname.

PCoIP Device Description:

Generic Tag:

AWI Label page

The following parameters display on the AWI Label page:

AWI Label Parameters

Assigning a Device Name from the AWI

Parameter	Description
PCoIP Device Name	<p>Lets you give the device a logical name. The default is pcoip-portal-, where is the device's MAC address.</p> <p>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.</p> <p>It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions:</p> <ul style="list-style-type: none">• 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	<p>A description of the device or other information, such as the location of the device's endpoint.</p> <p>The firmware does not use this field. It is provided for administrator use only.</p>
Generic Tag	<p>Generic tag information about the device.</p> <p>The firmware does not use this field. It is provided for administrator use only.</p>

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**.

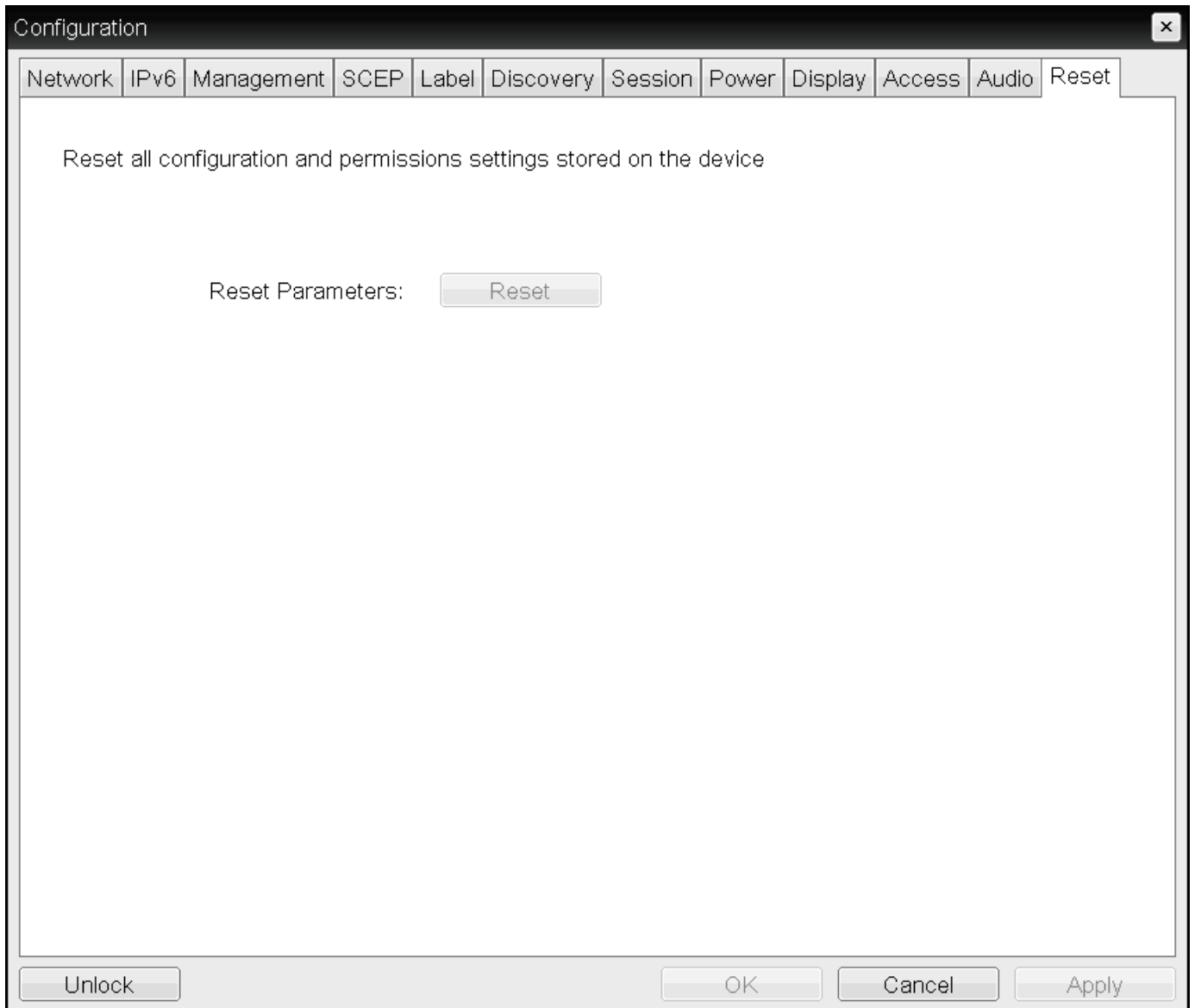
Resetting Your Tera2 PCoIP Zero Client

Setting	Default	AWI	OSD	Management Console
Reset Parameters (a button)	—	✓	✓	✓
Enable keyboard shortcut	Disabled	✓	✓	✓
Hide keyboard shortcut sequence in OSD	Disabled	✓	✓	✓

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.

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.

Resetting Your Tera2 PCoIP Zero Client



OSD Reset page

Reset


Reset all configuration and permission settings stored on the device

Reset Parameters:

Enable keyboard shortcut: CTRL + ALT + SHIFT + SPACE

Hide keyboard shortcut sequence in OSD:

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**+

Configuring a Reset Shortcut

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.

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.

OSD Logo Upload

Upload an OSD logo to be displayed on the local GUI (client only)

The OSD logo must be a **24bpp bitmap** that does not exceed **256 pixels by 64 pixels**. Any other images will be displayed incorrectly, or not at all.

OSD logo filename: No file selected.

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-logout 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.

Configuring the Touch Screen from the OSD

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.

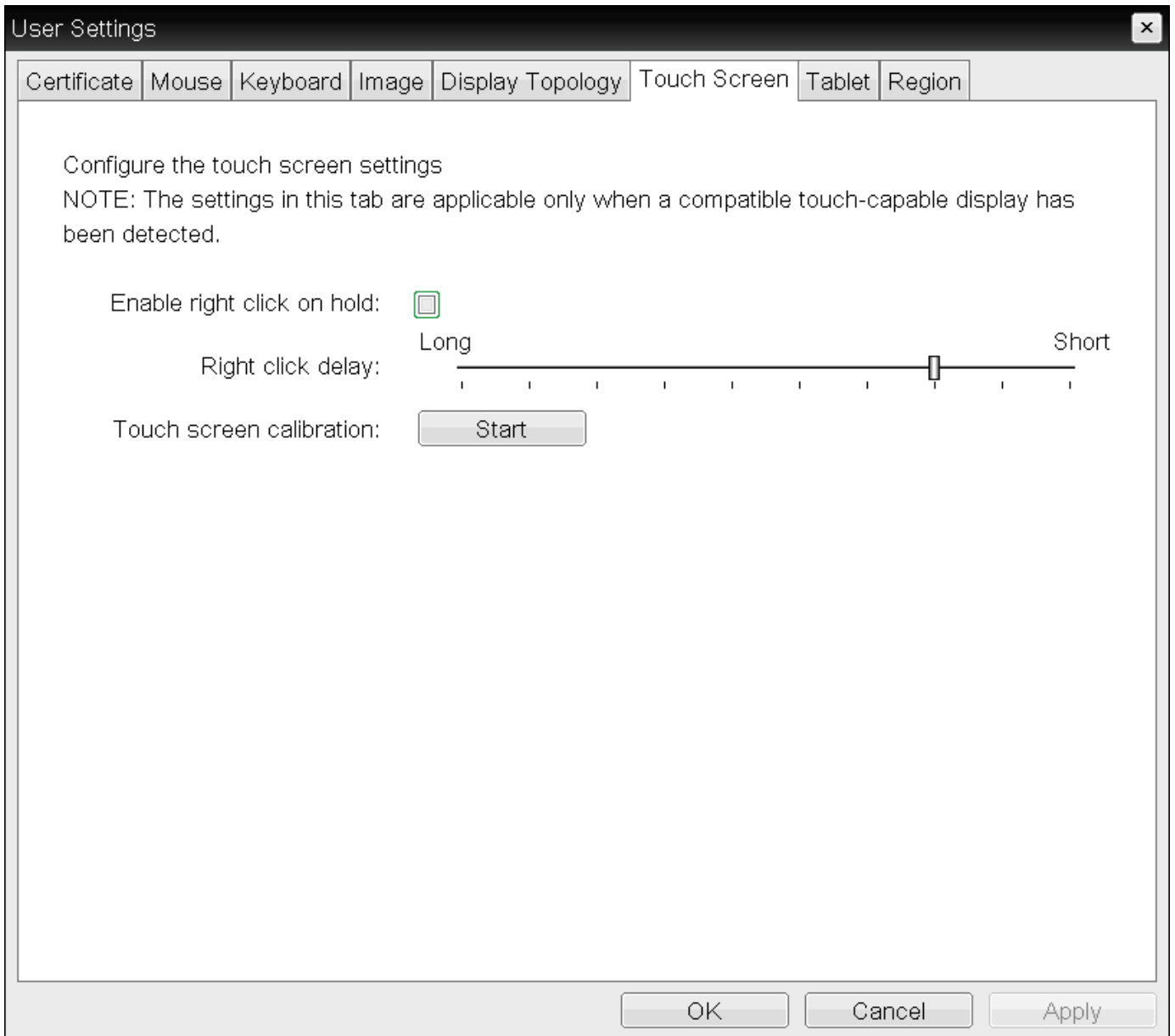
5. Follow the touch screen prompts. You can test the calibration with your finger (the cursor should move with your finger). If the screen is not properly calibrated, the system automatically restarts the calibration program.

Configuring the Touch Screen from the OSD

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

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

Configuring the Touch Screen from the OSD



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

Setting up the Touch Screen as a Bridged Device

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	<p>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.</p> <p>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.</p> <p>To manually start the calibration program, from the OSD Touch Screen page, click Start. Follow the onscreen prompts.</p>

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

<p>Legend (Displays):</p> <p>Status [potential failures]</p> <p>Connected [EDID read failure / EDID override]</p> <p>Disconnected</p> <p>Not in Session [EDID read failure / EDID override]</p> <p>Unknown</p> <p>Potential Failures</p> <p>EDID read failure</p> <p>EDID override</p> <p>Cable error</p>	<p>Description</p> <p>The display is connected and the EDID has been bridged (host/client)</p> <p>No display or cable has been detected</p> <p>The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)</p> <p>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)</p> <p>Description</p> <p>There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.</p> <p>Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached.</p> <p>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).</p>
--	---

The following information displays on the AWI Attached Devices page:

Attached Devices Information

Viewing Information About Attached Devices

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.
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: <ul style="list-style-type: none">• 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.


Viewing Information About Attached Devices

To view device information:

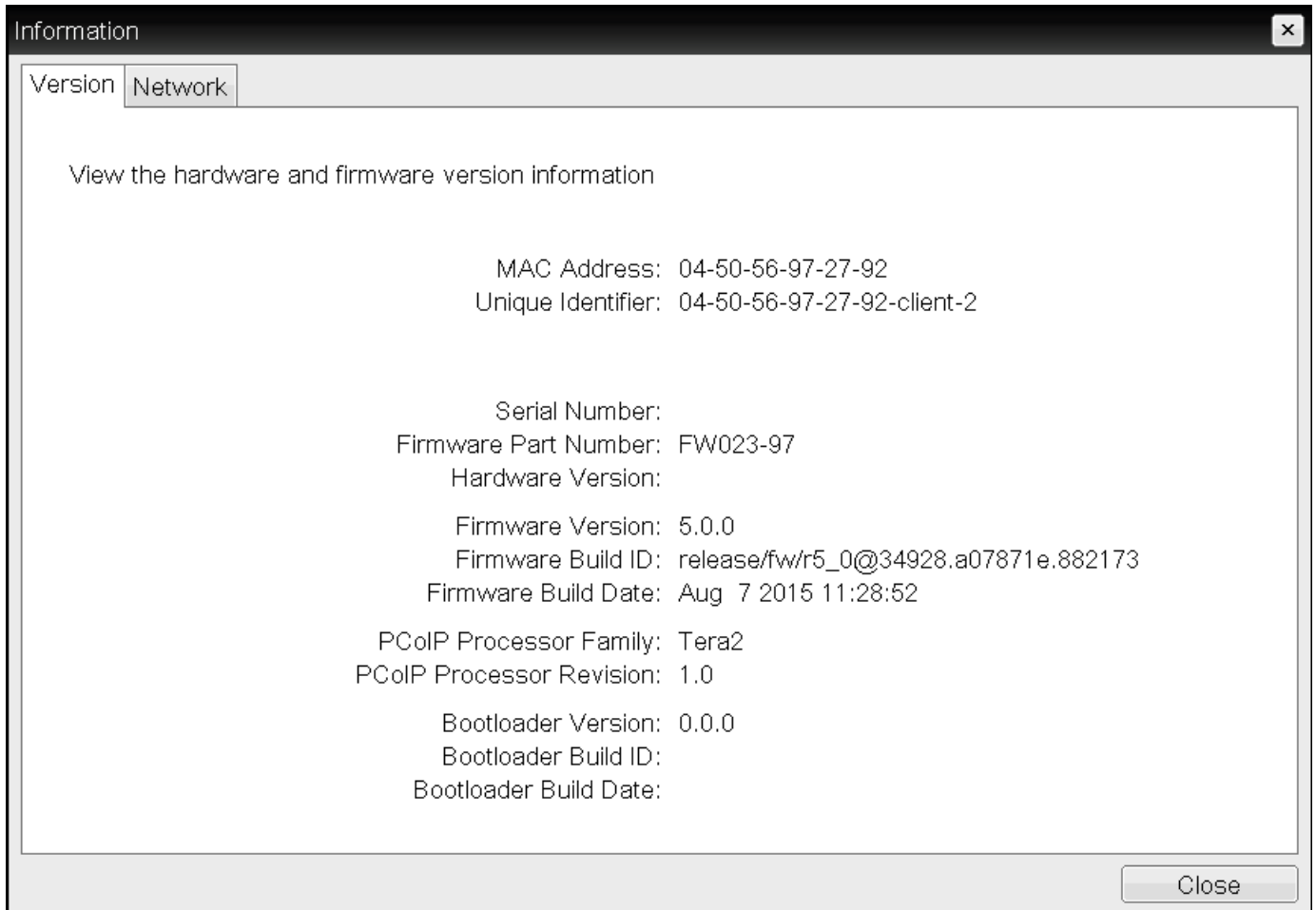
1. From the AWI, select **Info > Attached Devices**.
2. From the AWI **Attached Devices** page, view information for the devices attached to your Tera2 PCoIP Zero Client.

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](#).



The screenshot shows a window titled "Information" with a close button in the top right corner. Inside the window, there are two tabs: "Version" (selected) and "Network". Below the tabs, the text reads "View the hardware and firmware version information". The information is displayed in a list format:

- MAC Address: 04-50-56-97-27-92
- Unique Identifier: 04-50-56-97-27-92-client-2
- Serial Number:
- Firmware Part Number: FW023-97
- Hardware Version:
- Firmware Version: 5.0.0
- Firmware Build ID: release/fw/r5_0@34928.a07871e.882173
- Firmware Build Date: Aug 7 2015 11:28:52
- PCoIP Processor Family: Tera2
- PCoIP Processor Revision: 1.0
- Bootloader Version: 0.0.0
- Bootloader Build ID:
- Bootloader Build Date:

A "Close" button is located in the bottom right corner of the window.

OSD Version page (sample data only)

Version

View the hardware and firmware version information

MAC Address: 00-30-04-0E-47-B9

Unique Identifier: 00-30-04-0E-47-B9

Serial Number: L12110001326

Firmware Part Number: FW023020

Hardware Version: 6293D008120-A

Firmware Version: 5.0.0-rc3

Firmware Build ID: release/fw/r5_0@34928.a07871e.882045

Firmware Build Date: Aug 7 2015 11:12:57

PCoIP Processor Family: Tera2

PCoIP Processor Revision: 0.0

Bootloader Version: 2.0.0

Bootloader Build ID: r4_8@17300

Bootloader Build Date: Feb 17 2015 12:19:58

AWI Version page (sample data only)

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

Version Parameters

Viewing Hardware and Firmware Information

Parameters	Description
VPD Information	<p>(Vital Product Data): Information provisioned by the factory to uniquely identify each device:</p> <ul style="list-style-type: none">• 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.
Firmware Information	<p>This information reflects the current firmware details:</p> <ul style="list-style-type: none">• 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	<p>This information provides details about the PCoIP processor.</p> <ul style="list-style-type: none">• 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	<p>This information reflects the current firmware bootloader details:</p> <ul style="list-style-type: none">• 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**.

Viewing Hardware and Firmware Information

2. From the AWI Home page, or the OSD or AWI *Version* pages, view the hardware and firmware information.

Configuring Your Tera2 PCoIP Zero Client

You can configure your Tera2 PCoIP Zero Client in many ways, so that it will operate in your specific setup and environment.

Configuring Access to Management Tools

Secure Environments

Disable the AWI and use the PCoIP Management Console to configure endpoints in environments that have high security requirements.

Setting	Default	AWI	OSD	Management Console
Disable Management Console Interface	Disabled	✓	✓	✓
Disable Administrative Web Interface	Disabled	✓	✓	✓
Force password change on next login	Disabled	✓	✓	✓


From the OSD and AWI, you can:

- Prevent a PCoIP management tool from managing the Tera2 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.

At least one of the Tera2 PCoIP Zero Client's three management configuration interfaces (OSD, AWI, or PCoIP Management Console) must remain enabled at all times. If you hide the OSD Configuration menu, you will receive an error message if you try to disable both the PCoIP Management Console interface and the AWI.

 **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.



PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

There have been 1 failed attempts to log in to the Administrative Web Interface since the last successful login. The last failed attempt was at 03/20/2014 19:39:06 UTC.

Processor: TERA2321 revision 0.0 (512 MB)
Time Since Boot: 0 Days 1 Hours 22 Minutes 40 Seconds
PCoIP Device Name: pcoip-portal-0030040e47b9

Connection State: Connected to VDI host 192.168.63.29
Connection Duration: 0 Days 1 Hours 18 Minutes 11 Seconds
802.1X Authentication Status: Disabled
Session Encryption Type: AES-128-GCM

PCoIP Packets (Sent/Received/Lost): 256743 / 533958 / 1 (0.0 %)
Bytes (Sent/Received): 34451890 / 298575332
Round Trip Latency (Min/Avg/Max): 1 / 1 / 2 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 0 / 144 / 296 / 8000 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 904 / 10400 kbps

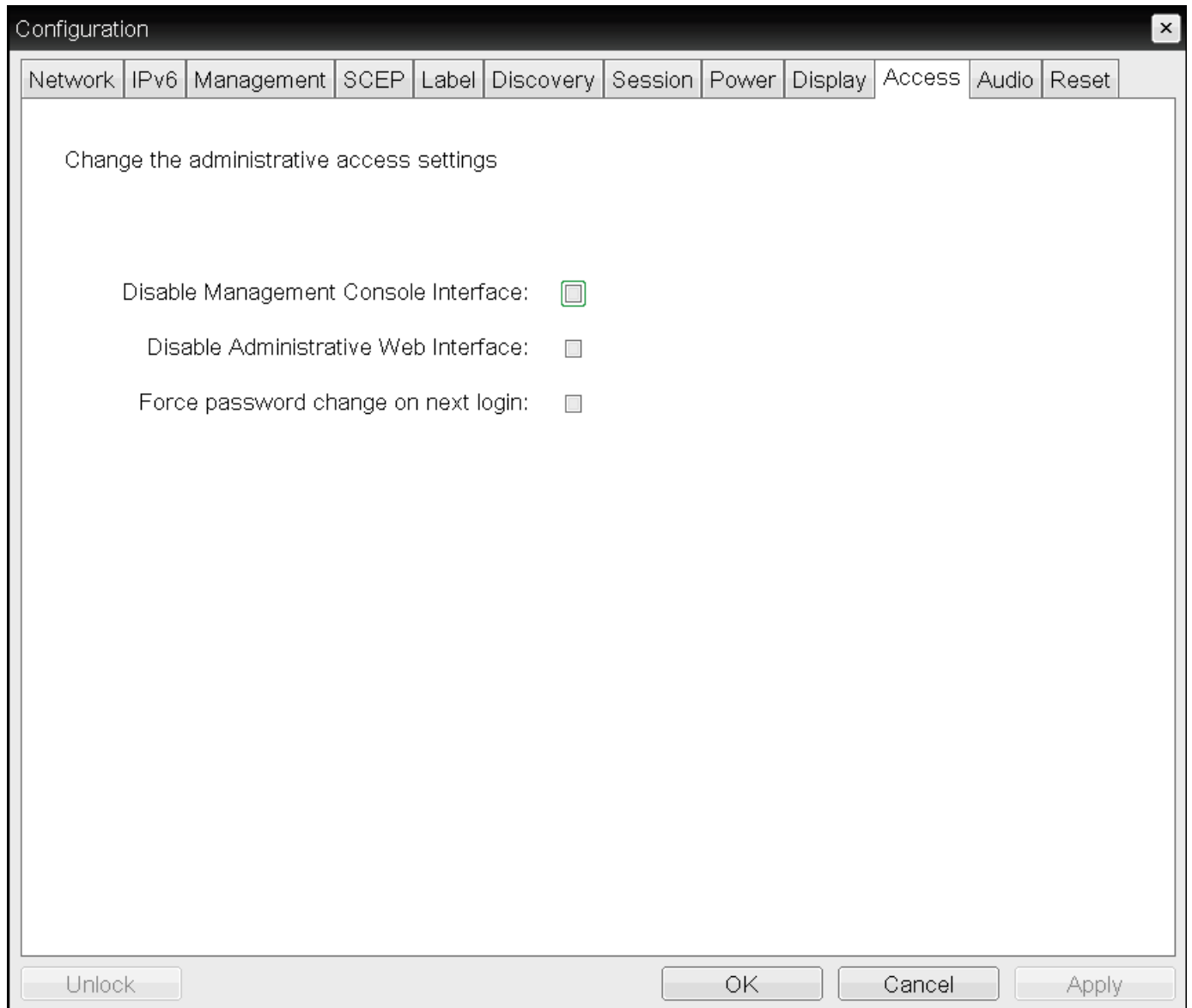
Pipeline Processing Rate (Avg/Max/Limit): 0 / 20 / 148 Mpps
Endpoint Image Settings In Use: Host
Initial Image Quality (Min/Max): 50 / 90
Image Quality Preference: 50
Build To Lossless: Disabled

Display	Maximum Rate: User Defined	Output Process Rate	Image Quality
1	24 fps	9 fps	Lossy
2	24 fps	1 fps	Lossy

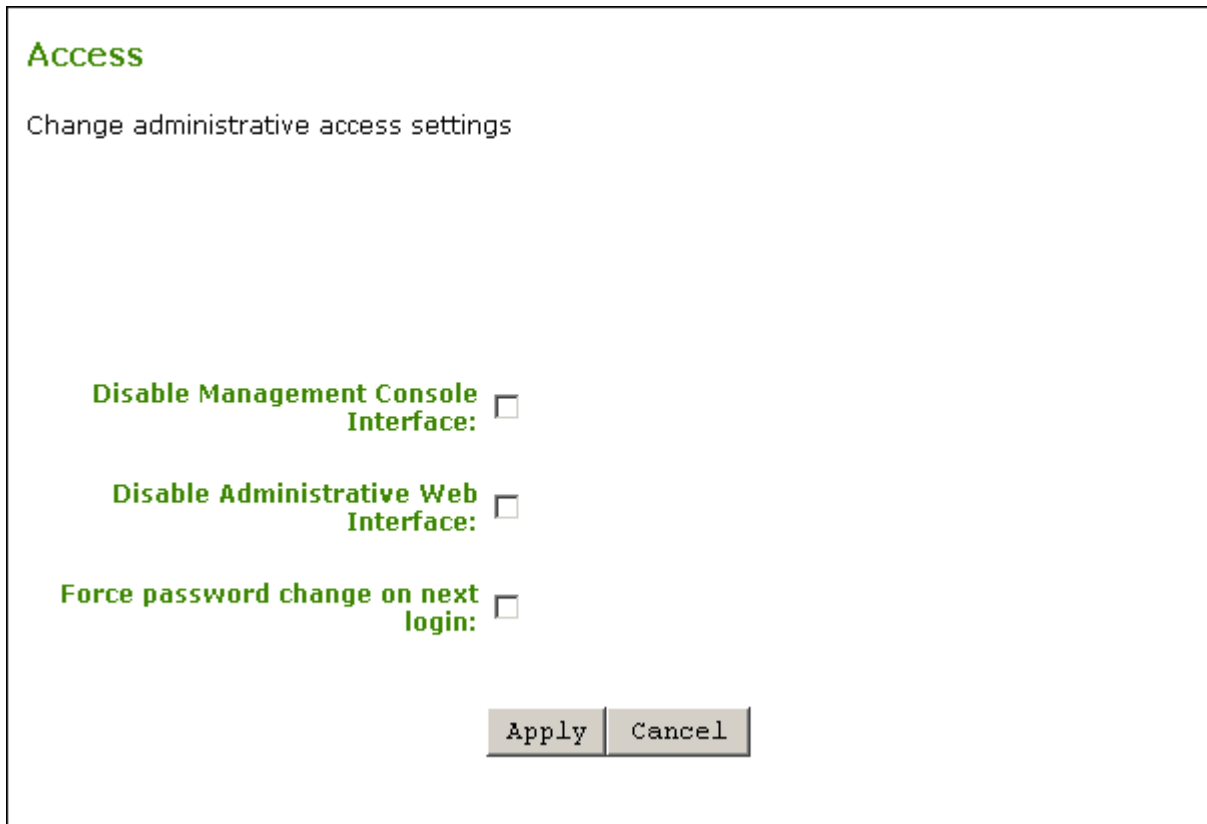
Failed login attempt message (from AWI)

Configuring Access to Management Tools

You can configure access settings from the OSD and AWI Access pages (shown next).



OSD Access page



The screenshot shows a configuration window titled "Access" with the subtitle "Change administrative access settings". It contains three settings, each with a checkbox:

- Disable Management Console Interface:**
- Disable Administrative Web Interface:**
- Force password change on next login:**

At the bottom of the window are two buttons: "Apply" and "Cancel".

AWI Access page

To configure access settings:

1. Open the Access page:
 - From the OSD, select Options > Configuration > Access.
 - From the AWI, select Configuration > Access.
2. From the OSD or AWI Access page, select one of the access settings:
 - **Disable Management Console Interface:** When enabled, the management console interface is disabled, and the PCoIP Management Console (or any other PCoIP device management tool) can't access or manage the Tera2 PCoIP Zero Client.
 - **Disable Administrative Web Interface:** When enabled, you can't access or manage the Tera2 PCoIP Zero Client using the AWI.
 - **Force password change on next login:** When enabled, the administrative password must be changed the next time either the AWI or OSD is accessed. The new password may be blank.
3. To save your updates, click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Audio

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

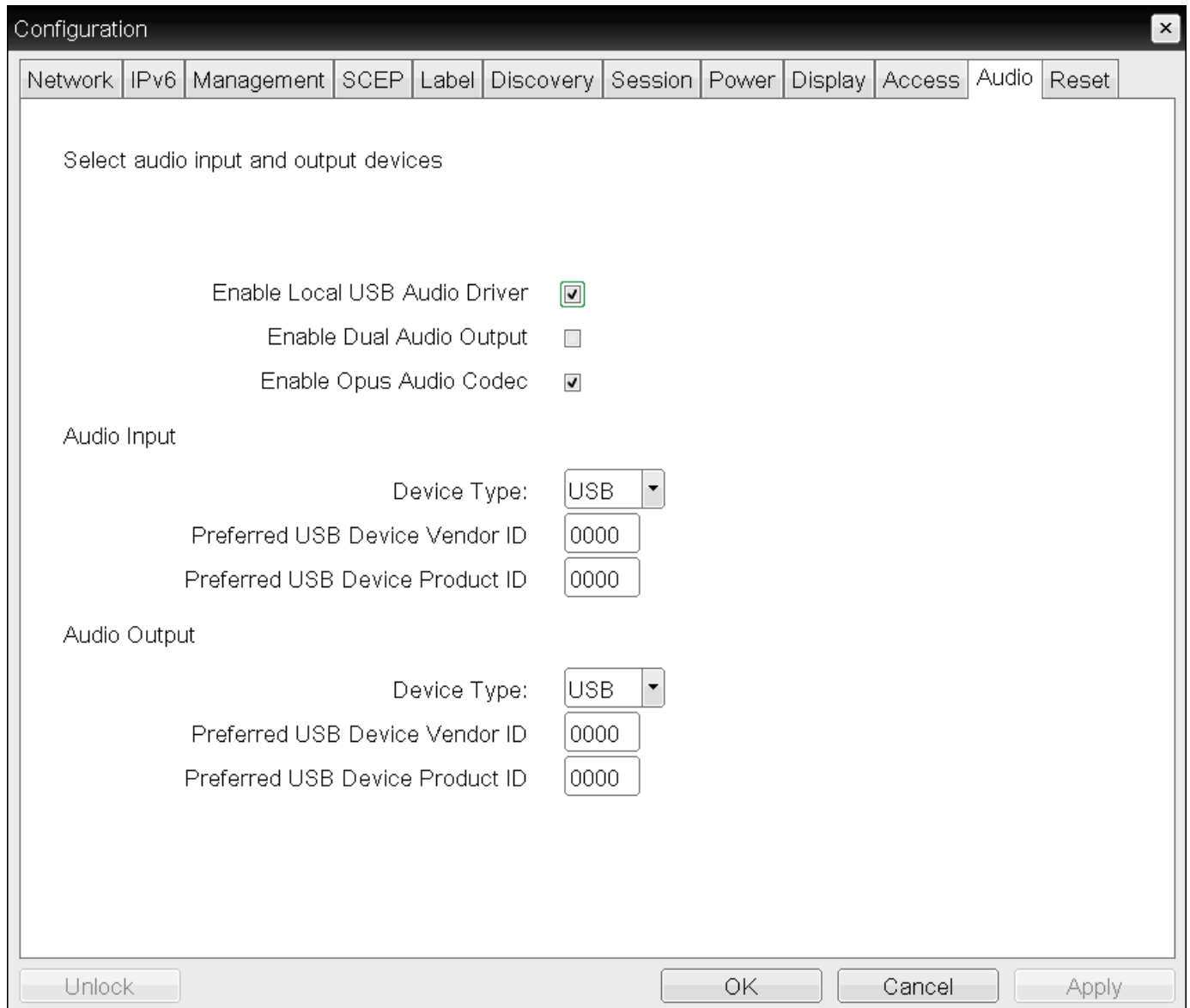
You can configure audio settings for the Tera2 PCoIP Zero Client from both the OSD and AWI.

Configuring Audio

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).



The screenshot shows a configuration window titled "Configuration" with a close button in the top right corner. The window has a tabbed interface with the following tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The "Audio" tab is selected. The main content area is titled "Select audio input and output devices" and contains the following settings:

- Enable Local USB Audio Driver:
- Enable Dual Audio Output:
- Enable Opus Audio Codec:
- Audio Input:
 - Device Type: USB (dropdown menu)
 - Preferred USB Device Vendor ID: 0000 (text input)
 - Preferred USB Device Product ID: 0000 (text input)
- Audio Output:
 - Device Type: USB (dropdown menu)
 - Preferred USB Device Vendor ID: 0000 (text input)
 - Preferred USB Device Product ID: 0000 (text input)

At the bottom of the window, there are four buttons: "Unlock", "OK", "Cancel", and "Apply".

OSD Audio page

Configuring Audio

Audio

Change audio settings

Enable Audio: Note: To enable audio, please ensure that audio is also enabled on the Host.

Enable Local USB Audio Driver: For optimal performance, install the Teradici Audio Driver on your VM and select it as the default playback device. Note: This feature is not supported when connected to PCoIP Host Cards.

Enable Dual Audio Output: Play VM audio to USB and analog devices.

Enable Opus Audio Codec: Use Opus audio codec for VM audio.

Audio Input

Audio Device Type: USB

Preferred USB Device Vendor ID: 047F

Preferred USB Device Product ID: C01A

Attached USB devices:

Audio Output

Audio Device Type: USB

Preferred USB Device Vendor ID: 047F

Preferred USB Device Product ID: C01A

Attached USB devices:

Apply Cancel

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

Configuring Audio

Category	Parameter	Description
Audio		
	Enable Audio (AWI only)	<p>When enabled, configures audio support on the device.</p> <p>This property must be enabled on both the host and the client.</p> <p>When disabled, the audio hardware is not available for the host operating system to enumerate.</p>
	Enable Local USB Audio Driver	<p>This option locally terminates any USB audio devices that are attached to the Tera2 PCoIP Zero Client.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
	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 .
	Audio Device Type	This field applies when you enable the Enable Local USB Audio Driver option and

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	x	✓	✓
Certificate Check Mode Lockout	Disabled	✓	x	✓

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 Workspace](#)
- [PCoIP Connection Manager](#)
- [View Connection Server](#)

Configuring Discovery

Setting	Default	AWI	OSD	Management Console
Internal Endpoint Manager URI	—	✓	x	✓
External Endpoint Manager URI	—	✓	x	✓
Manager Discovery Mode	Automatic	✓	x	✓
Endpoint Bootstrap Manager URI	—	✓	x	x
Enable Discovery	Enabled	x	✓	✓
Enable SLP Discovery	Enabled	✓	x	✓
Enable DNS-SRV Discovery	Enabled	✓	x	✓
DNS-SRV Discovery Delay	300	✓	x	✓

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

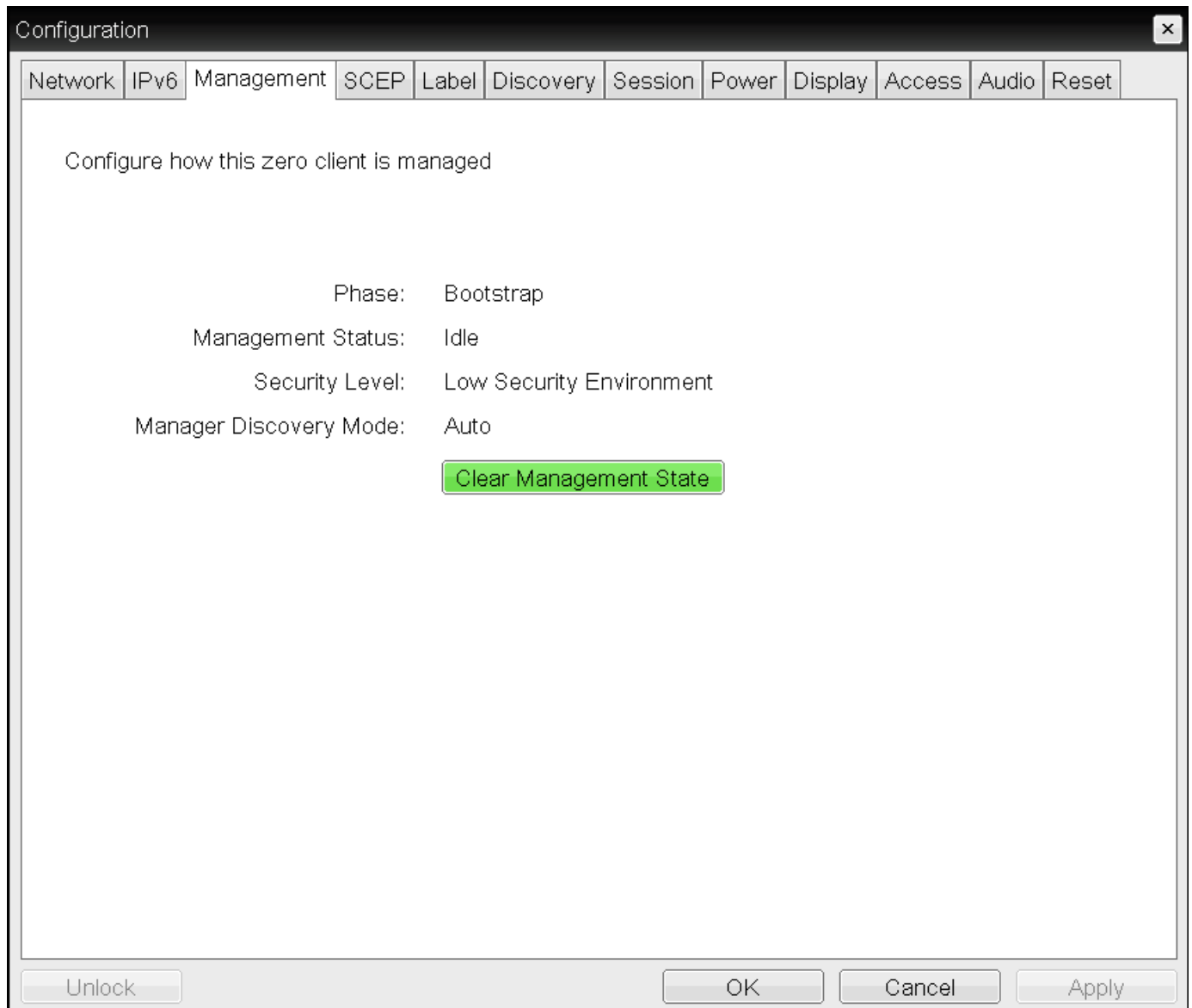
For detailed information about discovery methods, see [Connecting to an Endpoint Manager](#).

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

Configuring the Discovery Method

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.

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.153.242:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Automatic

Discovery Method	Discovery Outcome	Endpoint Bootstrap Manager Address	Certificate Fingerprint
DHCP Options	Successfully found an Endpoint manager address	10.0.153.242	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
DNS SRV Records	Not used		

EM Topology:

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.153.242:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

Clear Management State

Apply Cancel

AWI Management page – automatic discovery mode

Configuring the Discovery Method

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.157.21:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Manual

Endpoint Bootstrap Manager URI: Clear Management State First

EM Topology:	URI Type	EM URI	Certificate Fingerprint
Internal EM URI:		wss://10.0.157.21:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:			

Clear Management State

Apply Cancel

AWI Management page – manual discovery mode

The following discovery parameters display on the AWI Management page:

Discovery Parameters

Configuring the Discovery Method

Parameter	Description
Internal Endpoint Manager URI	<p>This field displays when the security level is set to High Security Environment - Bootstrap phase disabled.</p> <p>Enter the URI for the internal Endpoint Manager using the following format, and click Apply:</p> <pre>wss://<internal EM IP address/FQDN>:[port number]</pre> <p>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.</p>
External Endpoint Manager URI (optional)	<p>This optional field displays the security level is set to High Security Environment - Bootstrap phase disabled.</p> <p>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.</p> <p>If desired, enter the URI for the external Endpoint Manager using the following format, and click Apply:</p> <pre>wss://<external EM IP address/FQDN>:[port number]</pre> <p>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.</p>
Manager Discovery Mode	<p>Select the correct discovery mode:</p> <ul style="list-style-type: none">• 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	<p>When Manager Discover Mode is set to Automatic, this section displays the device discovery method your system is using.</p> <ul style="list-style-type: none">• 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

Configuring SLP Discovery

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

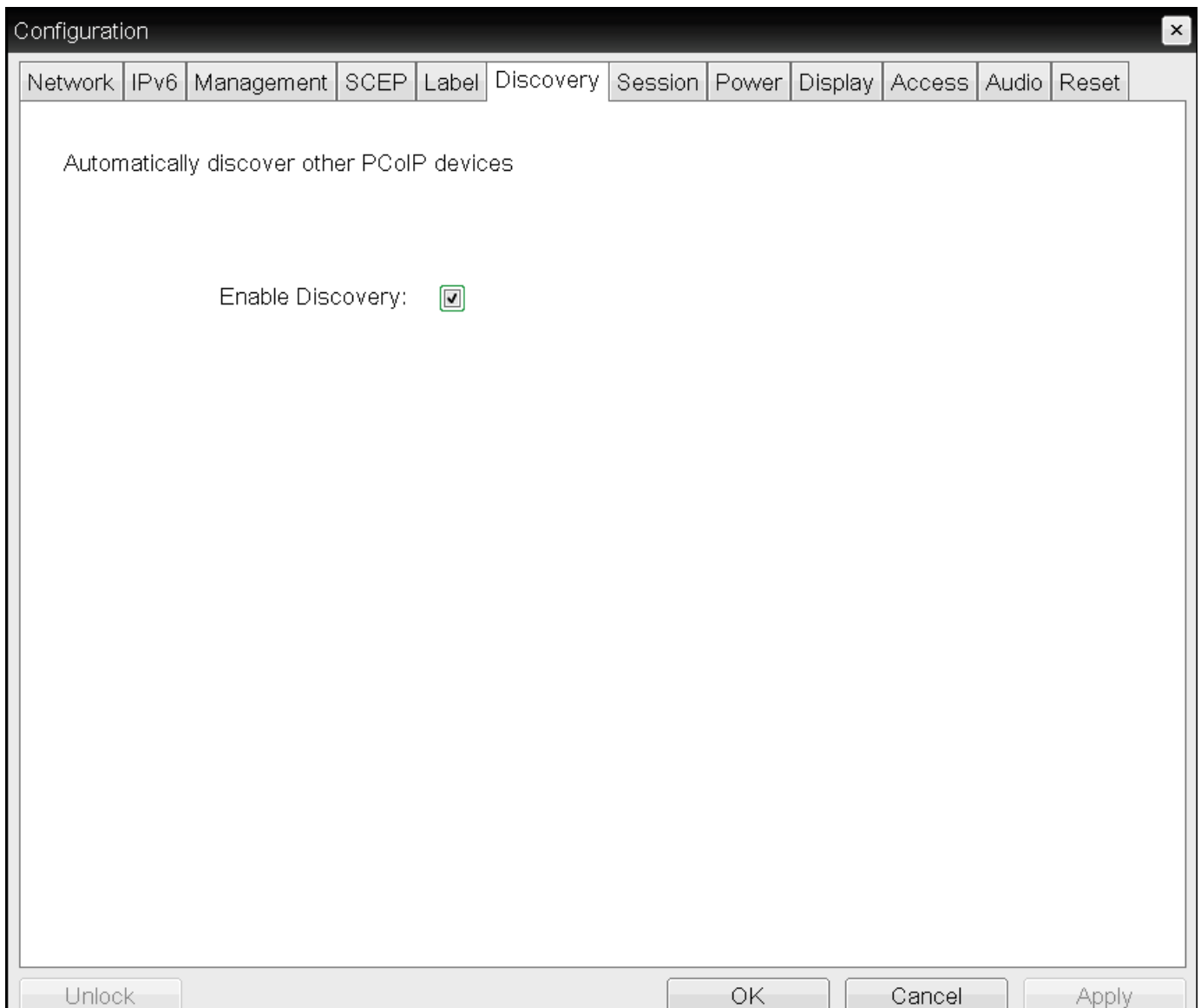


Devices and PCoIP Management Console must reside on the same subnet

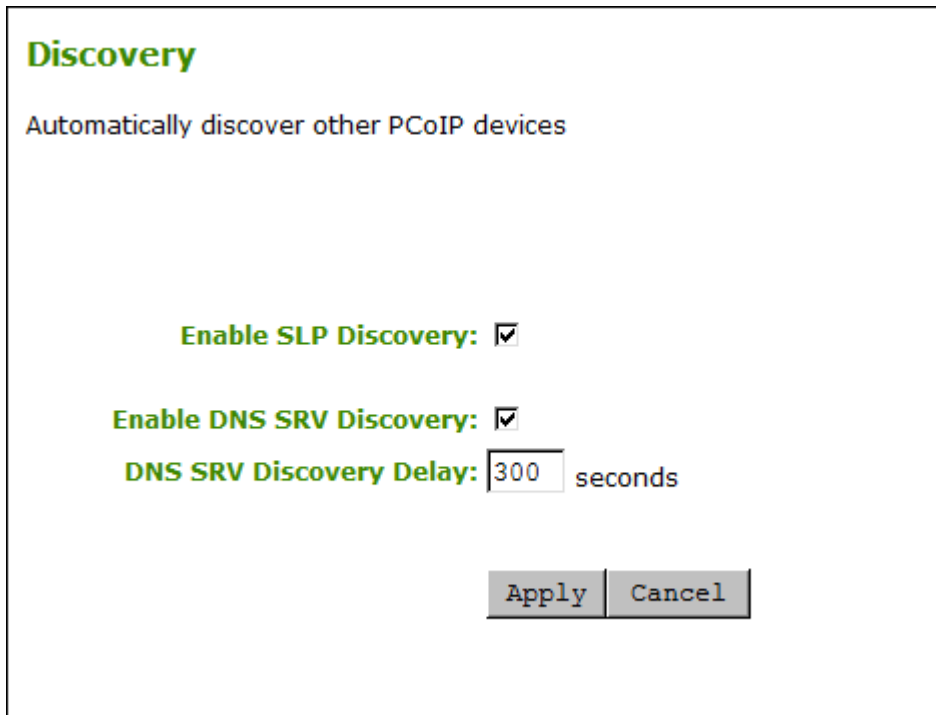
SLP discovery requires all PCoIP devices and the PCoIP Management Console to reside on the same network subnet. For SLP discovery to work across subnets, you must configure routers to forward multicast traffic between subnets. Because most deployments do not enable this, the recommended discovery mechanism for this case is to configure DHCP Vendor Class Options directly in the DHCP server.

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

Configuring SLP Discovery



OSD Discovery page



Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

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.



The screenshot shows the 'Discovery' configuration page. At the top, it says 'Automatically discover other PCoIP devices'. Below this, there are three settings: 'Enable SLP Discovery' with a checked checkbox, 'Enable DNS SRV Discovery' with a checked checkbox, and 'DNS SRV Discovery Delay' with a text input field containing '300' and the unit 'seconds'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

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.

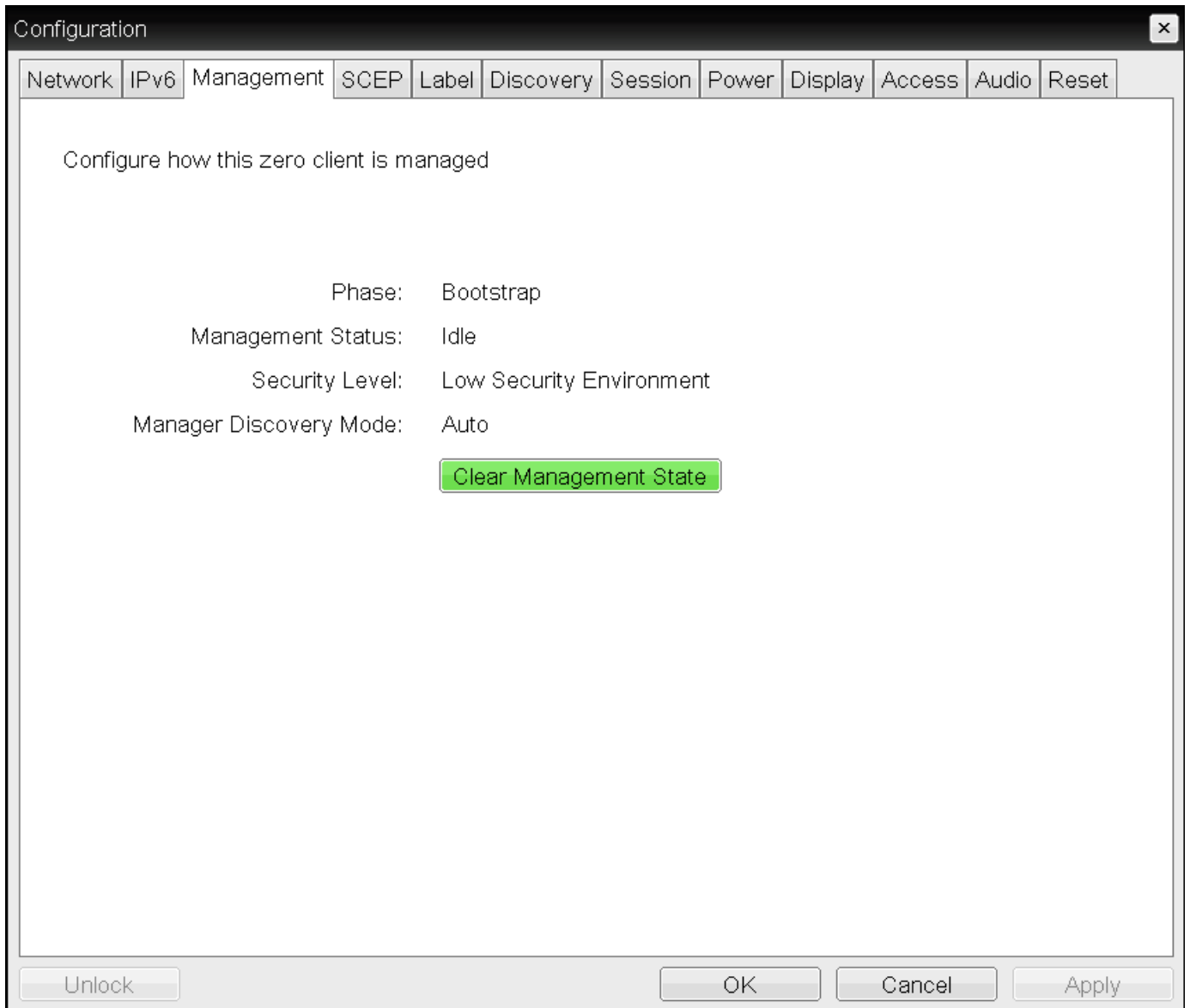
Clearing the management state removes the current endpoint manager information for the client. Once the client is managed by an endpoint manager, you must clear its management state before the client can accept a new endpoint manager.

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

i **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.

Clearing the Management State



OSD Management page

Clearing the Management State

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.153.242:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Automatic

Discovery Method	Discovery Outcome	Endpoint Bootstrap Manager Address	Certificate Fingerprint
DHCP Options	Successfully found an Endpoint manager address	10.0.153.242	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
DNS SRV Records	Not used		

EM Topology:

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.153.242:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

AWI Management page – automatic discovery mode

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.157.21:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Manual

Endpoint Bootstrap Manager URI:

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.157.21:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

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	—	x	✓	✓
Layout	—	x	✓	✓
Alignment	—	x	✓	✓
Primary/Position/Rotation/Resolution	—	x	✓	✓

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

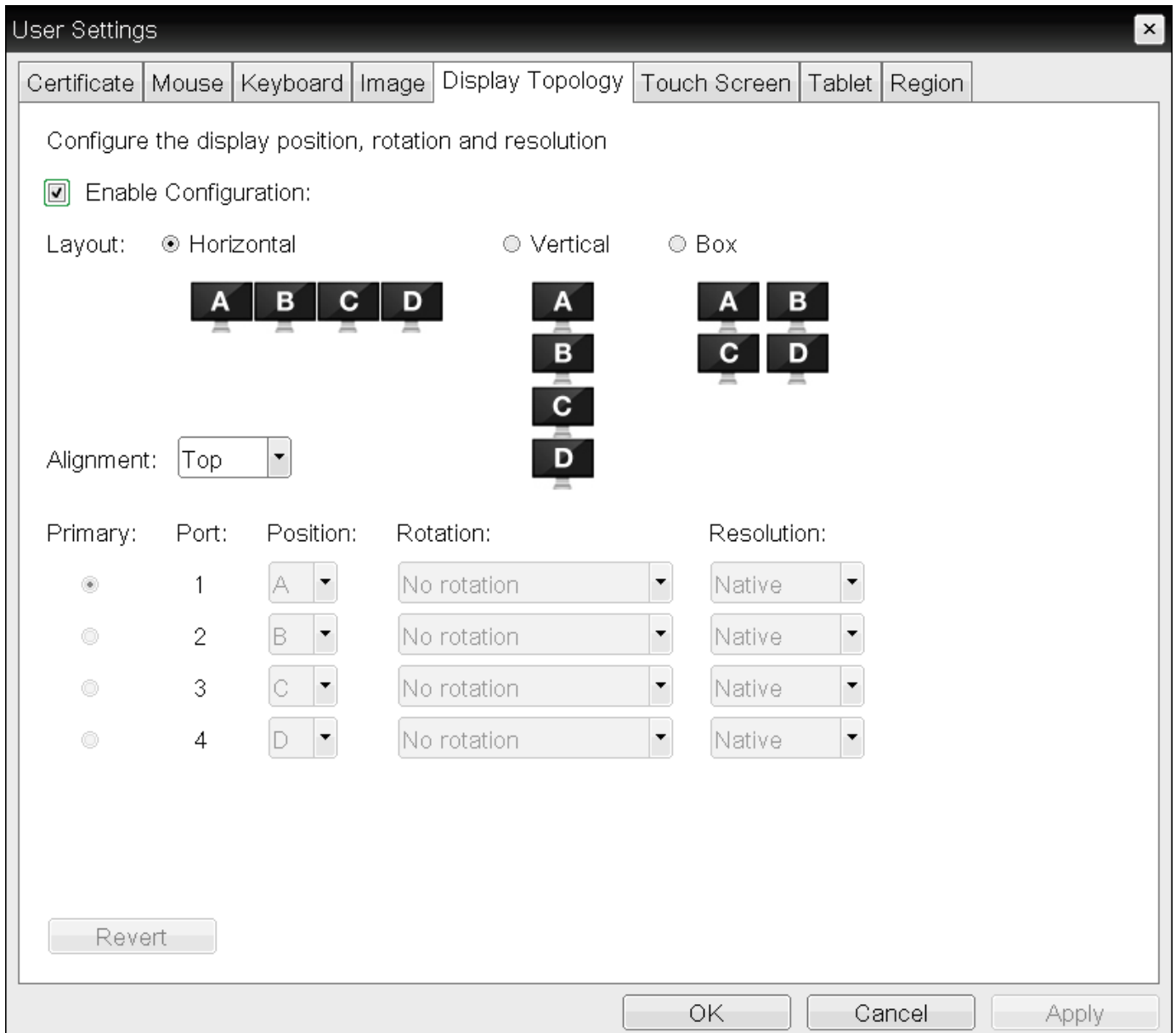
Before applying the display topology feature to a PCoIP session

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 PCoIP host 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.

Configuring a Quad Display Topology



OSD Quad-display Topology page

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

OSD Quad-display Topology Parameters

Configuring a Quad Display Topology

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.
Display Layout	<p>Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk.</p> <ul style="list-style-type: none"> • 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	<p>Select how you want displays aligned when they are different sizes.</p> <p>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.</p> <p>Horizontal layout:</p> <ul style="list-style-type: none"> • 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. <p>Vertical layout:</p> <ul style="list-style-type: none"> • 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.
Primary	<p>Configure which video port on the Tera2 PCoIP Zero Client that you want as the primary port.</p> <p>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).</p> <ul style="list-style-type: none"> • 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.

Configuring a Quad Display Topology

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	—	✓	✓	x
Subnet Mask	—	✓	✓	x
Gateway	—	✓	✓	x
Primary DNS Server	—	✓	✓	x
Secondary DNS Server	—	✓	✓	x
Domain Name	—	✓	✓	x
FQDN	—	✓	✓	x
Ethernet Mode	Auto	✓	✓	x
Maximum MTU Size	1200 bytes	✓	x	✓
Enable 802.1X security	—	✓	✓	✓
Identity	—	✓	✓	✓
Authentication	TLS	✓	x	x
Client Certificate	—	✓	✓	✓
Enable 802.1X Support for Legacy Switches	—	✓	x	✓

Configuring IPv4 Network Settings

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 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).

Configuring IPv4 Network Settings

Configuration ✕

Network | IPv6 | Management | SCEP | Label | Discovery | Session | Power | Display | Access | Audio | Reset

Change the network settings for the device

Enable DHCP:

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

Primary DNS Server: . . .

Secondary DNS Server: . . .

Domain Name:

FQDN:

Ethernet Mode: ▾

Enable 802.1X Security:

Identity:

Client Certificate: ▾

OSD Network page

Configuring IPv4 Network Settings

Network

Change the network settings for the device

Enable DHCP:

IP Address: 10 . 0 . 157 . 39

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 10 . 0 . 157 . 1

Primary DNS Server: 192 . 168 . 65 . 2

Secondary DNS Server: 0 . 0 . 0 . 0

Domain Name: terase.local

FQDN: pcoip-portal-0030040e47c0.terase.local

Ethernet Mode: Auto

Maximum MTU Size: 1200 bytes

Enable 802.1X Security:

Authentication: TLS

Identity:

Client Certificate: Choose

Enable 802.1X Support for Legacy Switches:

Apply Cancel

AWI Network page

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

Network Parameters

Configuring IPv4 Network Settings

Parameter	Description
Enable DHCP	<p>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).</p> <p>When disabled, you must set these parameters manually.</p>
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.
Subnet Mask	<p>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.</p> <p>Warning: Take care when setting the subnet mask</p> <p>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.</p>
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	<p>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.</p> <p>To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.</p>
Ethernet Mode	<p>Lets you configure the Ethernet mode of the client as follows:</p> <ul style="list-style-type: none">• Auto• 100 Mbps Full-Duplex

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	—	✓	✓	x
IPv6 Gateway	—	✓	✓	✓
Enable DHCPv6	—	✓	✓	✓
Enable DHCPv6 Addresses	—	✓	x	x
Primary IPv6 DNS	—	✓	✓	✓
Secondary IPv6 DNS	—	✓	✓	✓
Domain Name	—	✓	✓	✓
FQDN	—	✓	✓	x
Enable SLAC	—	✓	✓	✓
SLAAC Addresses	—	✓	x	x
Enable Manual Address	—	✓	✓	x
Manual Address	—	x	✓	x

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

Configuring IPv6 Network Settings

Configuration ✕

Network IPv6 Management SCEP Label Discovery Session Power Display Access Audio Reset

Change the IPv6 network settings for the device

Enable IPv6:

Link Local Address:

Gateway:

Enable DHCPv6: /64 ▼

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC: /64 ▼

Enable Manual Address:

Manual Address:

OSD IPv6 page

IPv6

Change the IPv6 network settings for the device

Enable IPv6:

Link Local Address:

Gateway:

Enable DHCPv6:

DHCPv6 Addresses: / 64
 / 64
 / 64
 / 64

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC:

SLAAC Addresses: / 64
 / 64
 / 64
 / 64

Enable Manual Address:

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

Configuring IPv6 Network Settings

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

Setting	Default	AWI	OSD	Management Console
Old Password	—	✓	✓	x
New Password	—	✓	✓	x
Confirm New Password	—	✓	✓	x
Reset (a button)	—	x	✓	x

From the OSD and AWI Password page, as shown next, you can update the local administrative password for the device. This parameter affects the AWI and the local OSD GUI. Take care when updating the client password as the client may become unusable if the password is lost. From the OSD, you can also reset the password if you forget it.

The screenshot shows a 'Change Password' dialog box with the following elements:

- Title bar: Change Password (with a close button 'X')
- Old Password: [Input field]
- New Password: [Input field]
- Confirm New Password: [Input field]
- Buttons: Reset, OK, Cancel

OSD Change Password page

teradici
PCoIP

Password

Change the local administrator password

Old Password:

New Password:

Confirm New Password:

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

Configuring OSD and AWI Password

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 only)	<p>If you forget the password, you can click Reset to request a response code from the Tera2 PCoIP Zero Client vendor. The challenge code is sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. If you enter the response code correctly, the Tera2 PCoIP Zero Client's password is reset to an empty string. You must enter a new password.</p> <p>Contact the client vendor for more information when an authorized password reset is required. This option is not available through the AWI. It is only available through the OSD.</p>

To update or reset the password:

1. Open the Password page: From the OSD, select **Options > Password**. From the AWI, select **Configuration > Password**.
2. From the Password page, update the password settings, or click **Reset** to request a response code from the Tera2 PCoIP Zero Client vendor.
3. Click **OK** from the OSD, or click **Apply** from the AWI.

Configuring Power Settings

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

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

Configuring Power Settings

The image shows a 'Configuration' window with a tabbed interface. The 'Power' tab is selected. The window title is 'Configuration' and it has a close button (X) in the top right corner. The tabs are: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The main content area is titled 'Change the power settings' and contains two settings:

- OSD Screen-Saver Timeout: Seconds (0 = disabled)
- Display Suspend Timeout: Seconds (0 = disabled)

At the bottom of the window, there are four buttons: 'Unlock', 'OK', 'Cancel', and 'Apply'.

OSD Power page

Configuring Power Settings

Power

Change the power settings

OSD Screen-Saver Timeout: Seconds (0 = disabled)

Display Suspend Timeout: Seconds (0 = disabled)

Auto Power-Off Timeout: Seconds (0 = disabled)

Remote Host Power Control: ▼

Power On After Power Loss:

Enable Wake-on-USB:

Enable Wake-on-LAN:

AWI Power page

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

Power Parameters

Configuring Power Settings

Parameter	Description
OSD Screen-Saver Timeout	<p>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.</p> <p>This timeout only applies when the device is not in session.</p>
Display Suspend Timeout	<p>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.</p> <p>This timeout only applies when the device is in session.</p> <p>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.</p>
Auto Power-Off Timeout	<p>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.</p> <p>Non-zero values are only enabled when the Tera2 PCoIP Zero Client supports powering off.</p> <p>This timeout only applies when the device is not in session.</p>
Remote Host Power Control	<p>Configure the client's remote power setting.</p> <p>Select from the following options:</p> <ul style="list-style-type: none"> • 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. <p>For more information about the Zero Client Control Panel overlay window, see Disconnecting from a Session.</p>
Power On After Power Loss	<p>When enabled, the client automatically powers back on when power is supplied.</p>

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	✓	x	✓
Medium Security Environment	—	✓	x	✓
High Security Environment	—	✓	x	✓
Peer-to-Peer Certificate	—	✓	x	x

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 endpoint 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](#)

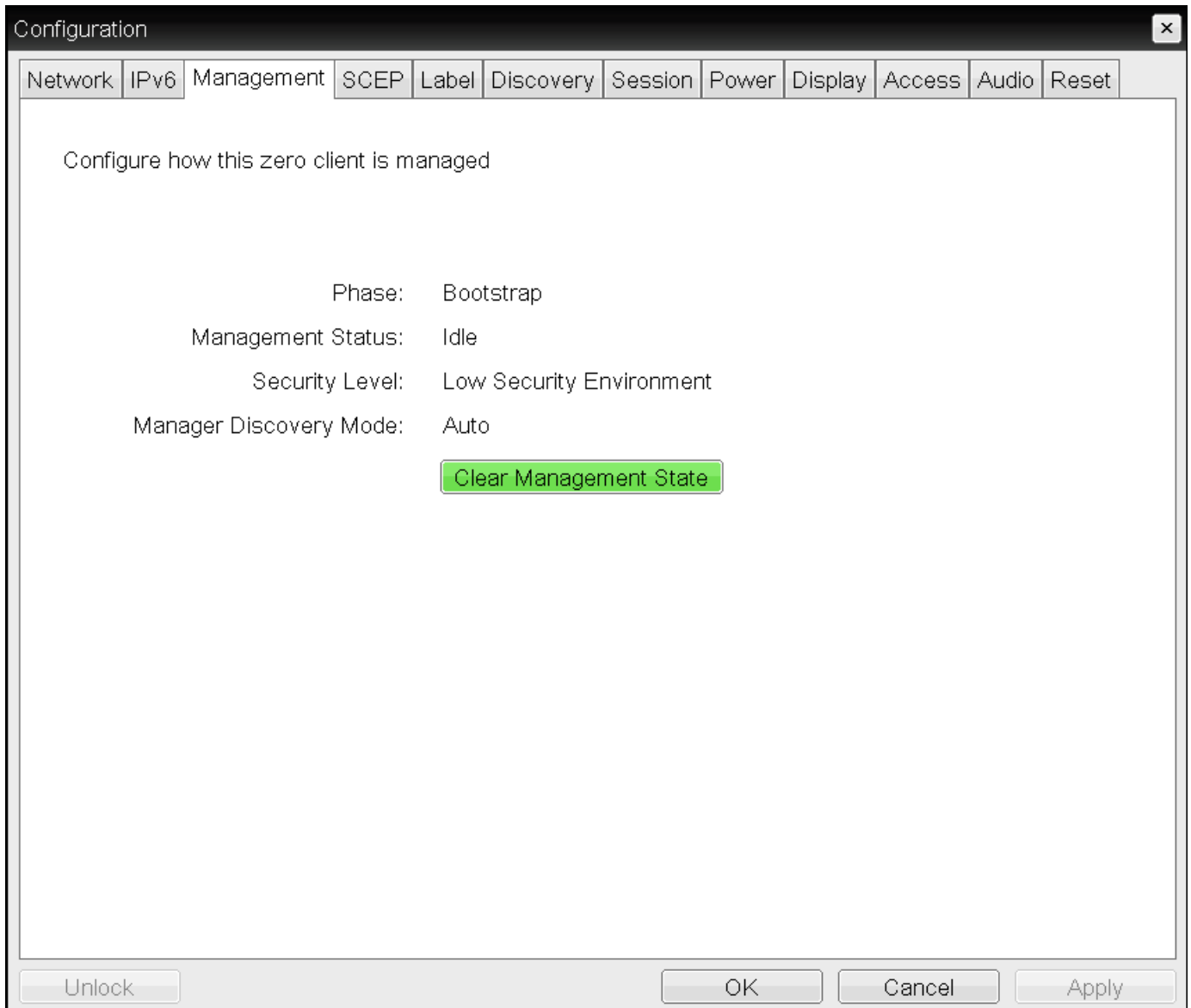
Security level implications

The security level setting has major implications for device discovery and connectivity with endpoint managers like the PCoIP Management 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.

Viewing the 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.

Configuring the Security Level

- **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.

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.153.242:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Automatic

Discovery Method	Discovery Outcome	Endpoint Bootstrap Manager Address	Certificate Fingerprint
DHCP Options	Successfully found an Endpoint manager address	10.0.153.242	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
DNS SRV Records	Not used		

EM Topology:

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.153.242:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

Clear Management State

Apply Cancel

AWI Management page – automatic discovery mode

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.157.21:5172

Security Level: Low Security Environment - Zero Client is discoverable by Endpoint Managers

Manager Discovery Mode: Manual

Endpoint Bootstrap Manager URI: Clear Management State First

URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://10.0.157.21:5172	B7:62:71:01:85:27:46:BB:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:		

Clear Management State

Apply Cancel

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	✓	x	✓
Device Bandwidth Targett	0	✓	x	✓
Device Bandwidth Floort	0	✓	x	✓

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

Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: kbps (0 = no limit)

Device Bandwidth Target: kbps (0 = disabled)

Device Bandwidth Floor: kbps (0 = use default of 1000 kbps)

AWI Bandwidth page

The following parameters display on the AWI Bandwidth page:

Bandwidth Parameters

Configuring Session Bandwidth

Parameter	Description
Device Bandwidth Limit	<p>Enter the maximum bandwidth peak from the client to the host (for example, USB data).</p> <p>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.</p> <p>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.</p> <p>We recommend setting this field to the limit of the network connected to the client and host.</p> <p>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.</p>
Device Bandwidth Target	<p>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.</p>
Device Bandwidth Floor	<p>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.</p> <p>This setting defines the minimum bandwidth from the client to the host (for example, USB data).</p> <p>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.</p> <p>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.</p> <p>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.</p>

Configuring Session Bandwidth

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.

Configuring SNMP Settings

Setting	Default	AWI	OSD	Management Console
Enable SNMP	Enabled	✓	x	✓
Community Name	public	✓	x	✓

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

SNMP

Change the SNMP configuration

Enable SNMP:

Community Name:

AWI SNMP page

 **Information: PCoIP SNMP Agent**

For more information on using the PCoIP SNMP Agent, see Using [SNMP with a PCoIP® Device User Guide](#).

To configure SNMP settings:

1. From the AWI, select **Configuration > SNMP**.
2. From the AWI SNMP page, do the following:
 - Select or clear the **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

Configuring SNMP Settings

responding to SNMP requests and from generating traps. It also ensures that the PCoIP SNMP MIB cannot be accessed.

- For **Community Name**, enter the SNMP community name used by the device.

3. Click **Apply**.

Configuring USB Settings and Permissions

| Setting | Default | AWI | OSD | Management Console | | :-: | :-: | :-: | :-: | :-: | | ✓ | Force Local Cursor Visible | Disabled | ✓ | x | x | | Enable EHCI (USB 2.0) | Enabled | ✓ | x | ✓ | | Authorized Devices (Add new) | - | ✓ | x | ✓ | | Unauthorized Devices (Add new) | - | ✓ | x | ✓ | | Bridged Devices (Add new) | - | ✓ | x | ✓ | | Devices Forced to USB 1.1 (Add new) | - | ✓ | x | x |

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.

i **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.

USB

Change the USB settings for the device

Force Local Cursor Visible:

Enable EHCI (USB 2.0): Applies only to software based PCoIP sessions. EHCI is automatically enabled in hardware based PCoIP sessions if both endpoints support it.

The following parameters display on the AWI USB parameters page:

USB Parameters

Configuring USB Permissions from the AWI

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)	<p>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.</p> <p>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).</p> <p>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.</p>

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

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

Configuring USB Permissions from the AWI

USB
Configure USB device management

Authorized Devices:
Any Device Class Any Sub Class Any Protocol

Unauthorized Devices: *Table is empty*

Bridged Devices: *Table is empty*

Devices Forced to USB 1.1: *Table is empty*

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 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.

Configuring USB Permissions from the AWI

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:

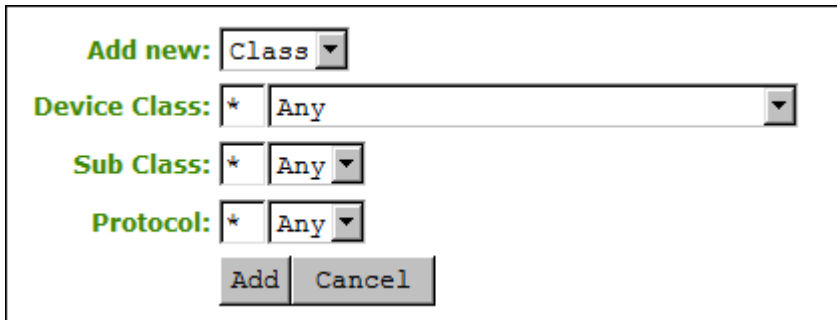
AWI USB Permissions Parameters

Configuring USB Permissions from the AWI

Parameter	Description
Authorized Devices	<p>Specify the authorized USB devices for the device:</p> <p>Add New: add a new device or device group to the list. This enables USB authorization by ID or Class:</p> <ul style="list-style-type: none"> • 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. <p>Remove: Delete a rule for a device or device group from the list.</p>
Unauthorized Devices	<p>Specify the unauthorized USB devices for the device.</p> <p>Add New: add a new device or device group to the list. This enables USB unauthorization by ID or Class:</p> <ul style="list-style-type: none"> • 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. <p>Remove: Delete a rule for a device or device group from the list.</p>
Bridged Devices	<p>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.</p> <p>Add New: Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.</p> <p>Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information.</p> <p>Remove: Delete a rule for a device or device group from the list.</p>
Devices Forced to USB 1.1	<p>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.</p> <p>Add New: Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.</p> <p>Remove: Delete a rule for a device or device group from the list.</p> <p>Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information.</p>

Configuring USB Permissions from the AWI

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**.

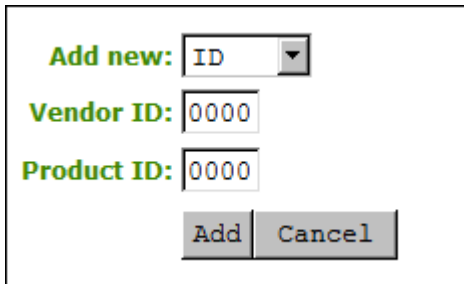


The screenshot shows a dialog box titled "Add new:" with a dropdown menu set to "Class". Below this, there are three rows of configuration options, each with a green asterisk icon and a dropdown menu:

- Device Class:** * Any
- Sub Class:** * Any
- Protocol:** * Any

At the bottom of the dialog are two buttons: "Add" and "Cancel".

Device class parameters



The screenshot shows a dialog box titled "Add new:" with a dropdown menu set to "ID". Below this, there are two rows of configuration options, each with a green asterisk icon and a text input field:

- Vendor ID:** * 0000
- Product ID:** * 0000

At the bottom of the dialog are two buttons: "Add" and "Cancel".

Device ID parameters

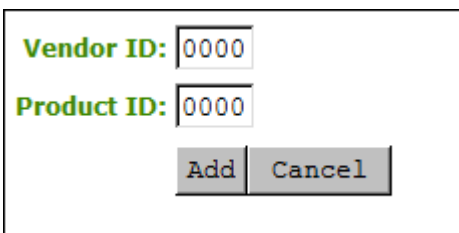
The following parameters display when you authorize or unauthorize USB device parameters:

USB Authorized/Unauthorized Devices Parameters

Configuring USB Permissions from the AWI

Parameter	Description
Add new	When adding a new USB authorization or unauthorization entry, select one of the following: <ul style="list-style-type: none">• 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 .
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.



Vendor ID: 0000
Product ID: 0000
Add Cancel

USB Bridged Parameters

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

USB Bridged Devices Parameters

Configuring USB Permissions from the AWI

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**.

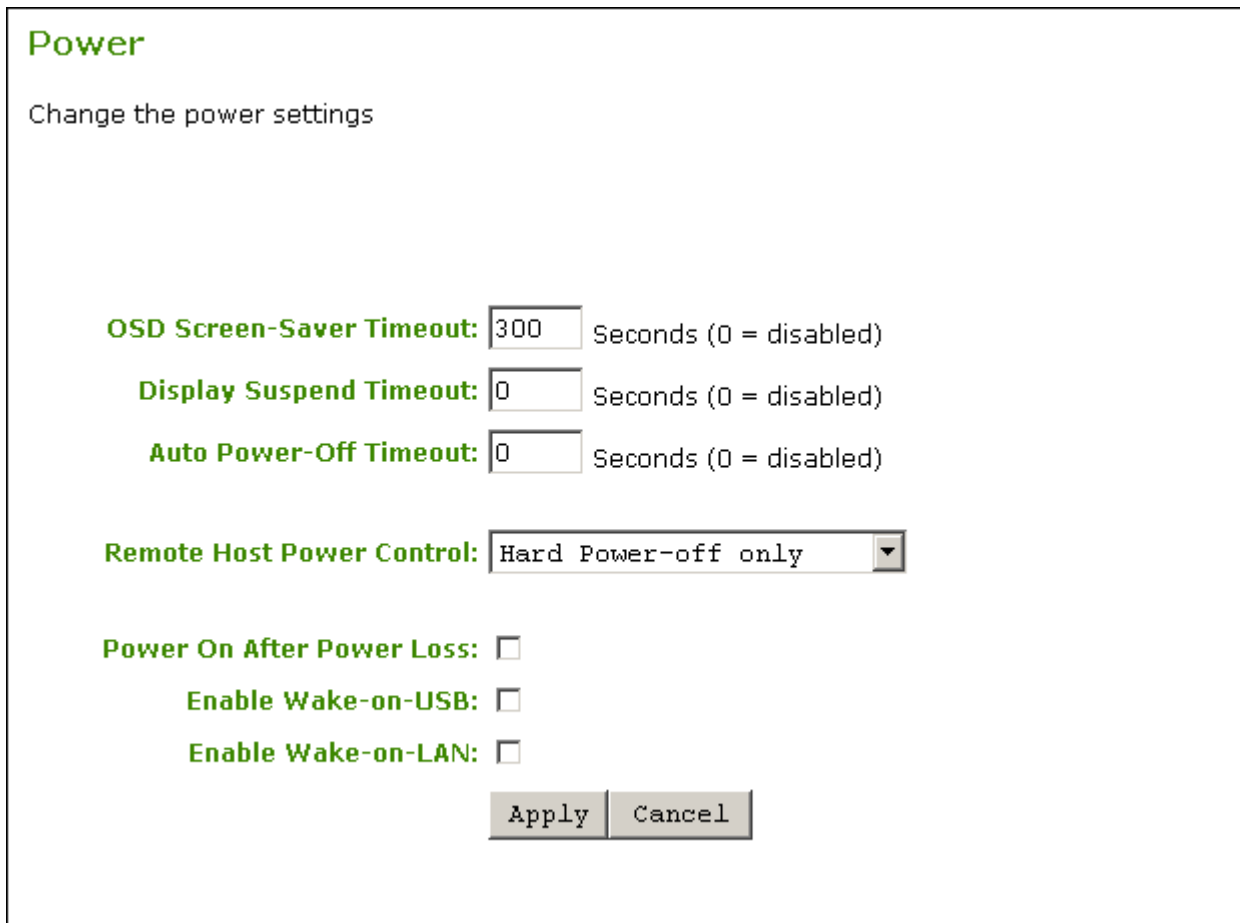
Configuring User Settings

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. If you are unable to view or see a particular user settings tab, please consult your administrator.

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.



Power

Change the power settings

OSD Screen-Saver Timeout: Seconds (0 = disabled)

Display Suspend Timeout: Seconds (0 = disabled)

Auto Power-Off Timeout: Seconds (0 = disabled)

Remote Host Power Control: ▼

Power On After Power Loss:

Enable Wake-on-USB:

Enable Wake-on-LAN:

AWI Power page

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

AWI Power Parameters

AWI: Power Permissions

Parameter	Description
OSD Screen-Saver Timeout	<p>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.</p> <p>This timeout only applies when the device is not in session.</p>
Display Suspend Timeout	<p>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.</p> <p>This timeout only applies when the device is in session.</p> <p>When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.</p>
Auto Power-Off Timeout	<p>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.</p> <p>Non-zero values are only enabled when the PCoIP client supports powering off.</p> <p>This timeout only applies when the device is not in session.</p>
Remote Host Power Control	<p>Configure the client's remote power setting. Select from the following options:</p> <ul style="list-style-type: none"> • .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	<p>When enabled, the client automatically powers back on when power is supplied.</p>
Enable Wake-on-USB	<p>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.</p> <p>Clicking or moving the mouse will not power up the client when this feature is enabled.</p>

Configuring OSD Language

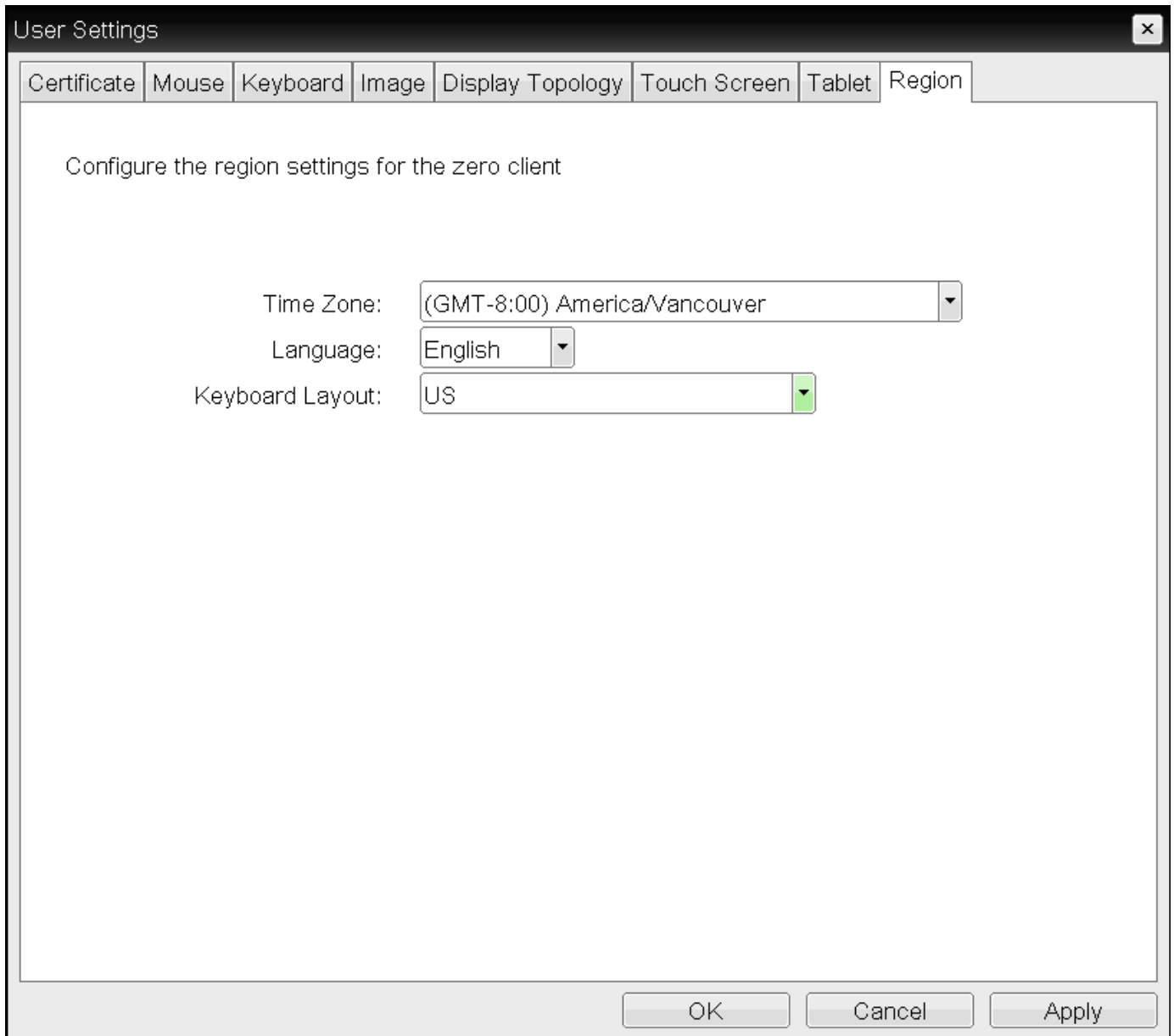
Setting	Default	AWI	OSD	Management Console
Language	English	✓	✓	✓
Keyboard Layout	US	✓	✓	✓
OSD Region Tab Lockout	Disabled	✓	x	✓

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.

Configuring OSD Language



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.

Configuring OSD Language

Language
Select a language for the local GUI (client only)

Language: English

Keyboard Layout: US

OSD Region Tab Lockout Prevent users from changing the controls in the OSD Region tab

Apply Cancel

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 PColP 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	✓	x
Identify NTP Host by	—	✓	x	✓
NTP Host DNS Name	—	✓	x	✓
NTP Host Pory	—	✓	x	✓
NTP Query Interval	—	✓	x	✓
Time Zone	Europe/London (UTC+0:00)	✓	✓	✓
Enable Daylight Saving Time	Disabled	✓	x	✓

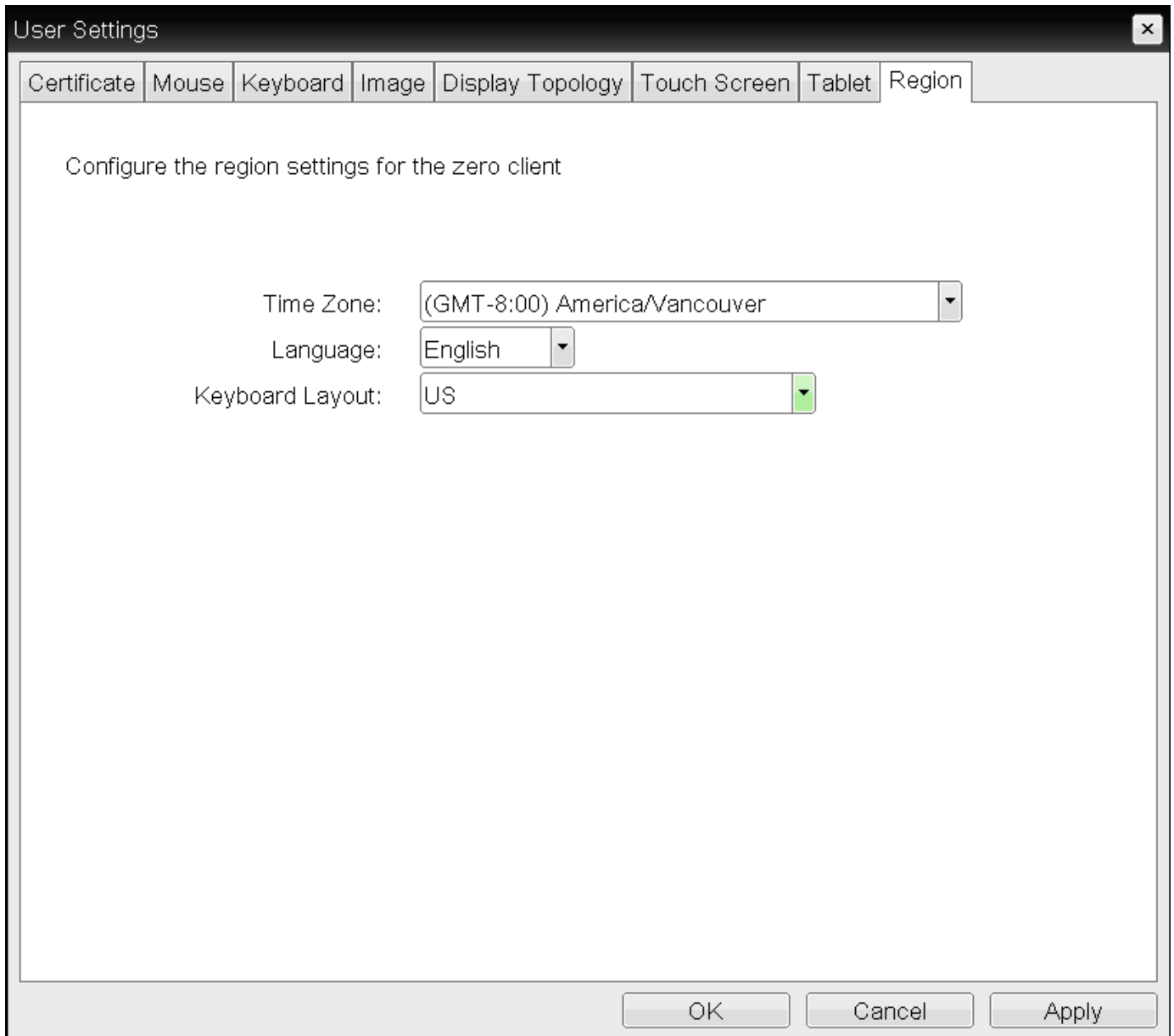
You can set the time zone for the Tera2 PCoIP Zero Client from both the OSD and AWI.

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.

Configuring Time Settings



OSD Region page

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

Configuring Time Settings

Time

Change the local time configuration

Current time: 10/20/2015 10:32:33

Enable NTP:

Identify NTP Host by: IP address FQDN

NTP Host DNS Name:

NTP Host Port:

NTP Query Interval:

Time Zone:

Enable Daylight Saving Time:

AWI Time page

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

Time Parameters

Configuring Time Settings

Parameter	Description
Current Time (AWI only)	Displays the time based on the NTP.
Enable NTP (AWI only)	Enable or disable the NTP feature.
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. <ul style="list-style-type: none">• 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.

Configuring Time Settings

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	✓	x	✓
Maximum Initial Image Quality	90	✓	x	✓
Image Quality Preference	50	✓	x	✓
Maximum Frame Rate	0 fps	✓	x	✓
Disable Build to Lossless	Disabled	✓	x	✓
Enable Low Bandwidth Text Codec	Disabled	✓	x	✓

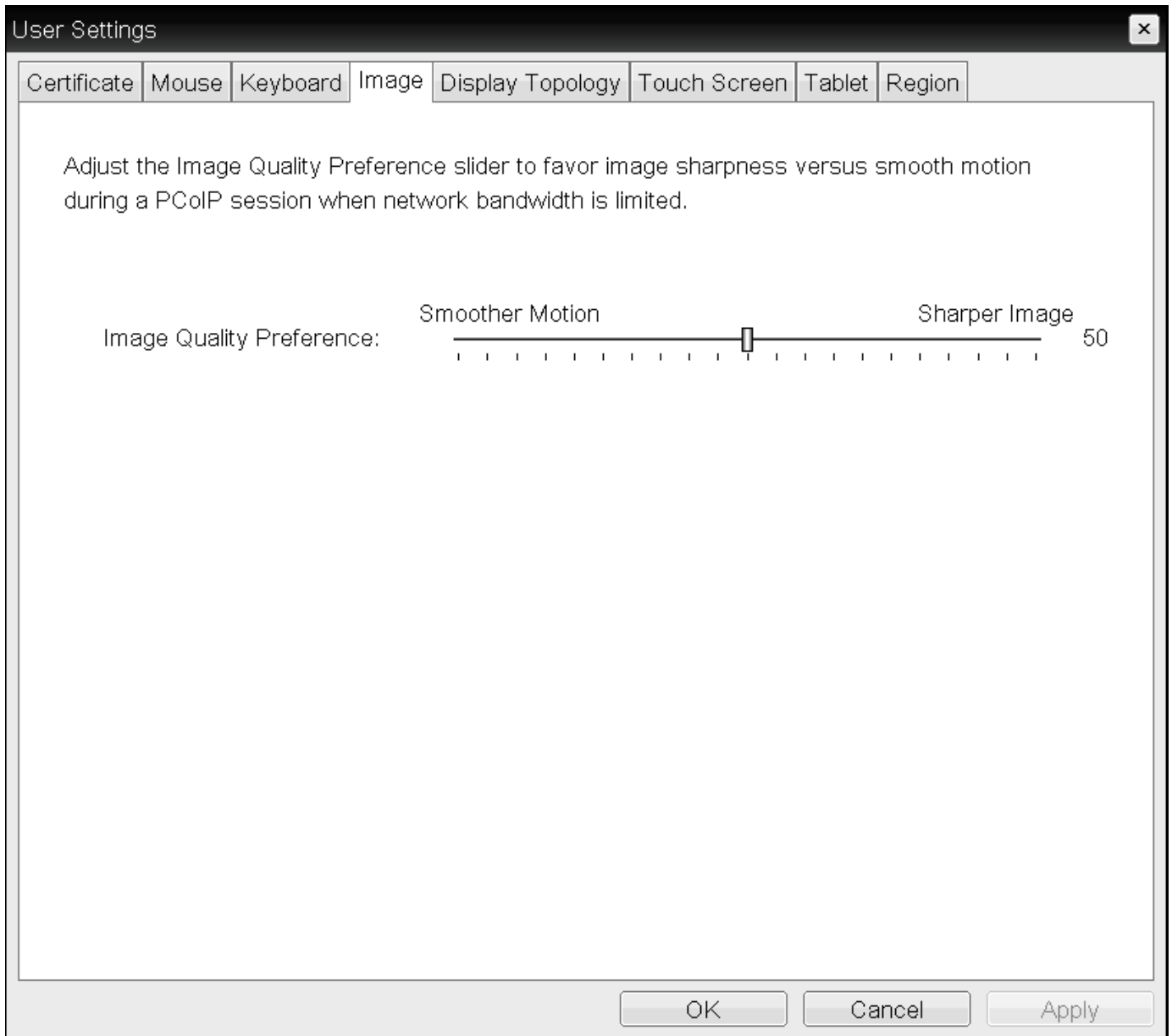
If desired, you can adjust the quality of the images you see during PCoIP sessions. You can set image quality preferences from both the OSD and AWI; however, you can configure many more settings from the AWI, including minimum image quality, maximum frame rate, and maximum initial image quality.

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.

Configuring Image Quality



OSD Image page

You adjust the image quality setting, as well as other advanced settings, from the AWI Image page, as shown next.

Configuring Image Quality

Image

Adjust the image quality. A lower minimum image quality will allow a higher frame rate when network bandwidth is limited.

Adjust the Image Quality Preference slider to favor image sharpness versus smooth motion during a PCoIP session when network bandwidth is limited.

NOTE: These settings take effect only when the host has "Use Client Image Settings" enabled.

The screenshot shows the AWI Image configuration page with the following settings:

- Minimum Image Quality:** Slider set to 40, ranging from Reduced to Perception-Free.
- Maximum Initial Image Quality:** Slider set to 90, ranging from Reduced to Perception-Free.
- Image Quality Preference:** Slider set to 50, ranging from Smoother Motion to Sharper Image.
- Maximum Frame Rate:** Input field set to 0 fps (0 = no limit).
- Disable Build To Lossless:**
- Enable Low Bandwidth Text Codec:**

Buttons for **Apply** and **Cancel** are located at the bottom.

AWI Image page

The following image parameters display on the OSD and AWI *Image* pages:

Image Parameters

Configuring Image Quality

Parameter	Description
Minimum Image Quality (AWI only)	<p>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.</p> <p>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.</p> <p>The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.</p>
Maximum Initial Image Quality (AWI only)	<p>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.</p> <p>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.</p> <p>The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.</p>
Image Quality Preference	<p>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.</p> <p>This setting doesn't work in PCoIP sessions with VMware Horizon virtual desktops that run release 5.0 or earlier.</p>
Maximum Frame Rate (AWI only)	<p>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.</p>
Disable Build to Lossless (AWI only)	<p>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.</p> <p>Warning: Selecting the <i>Disable Build to Lossless</i> check box degrades images.</p>

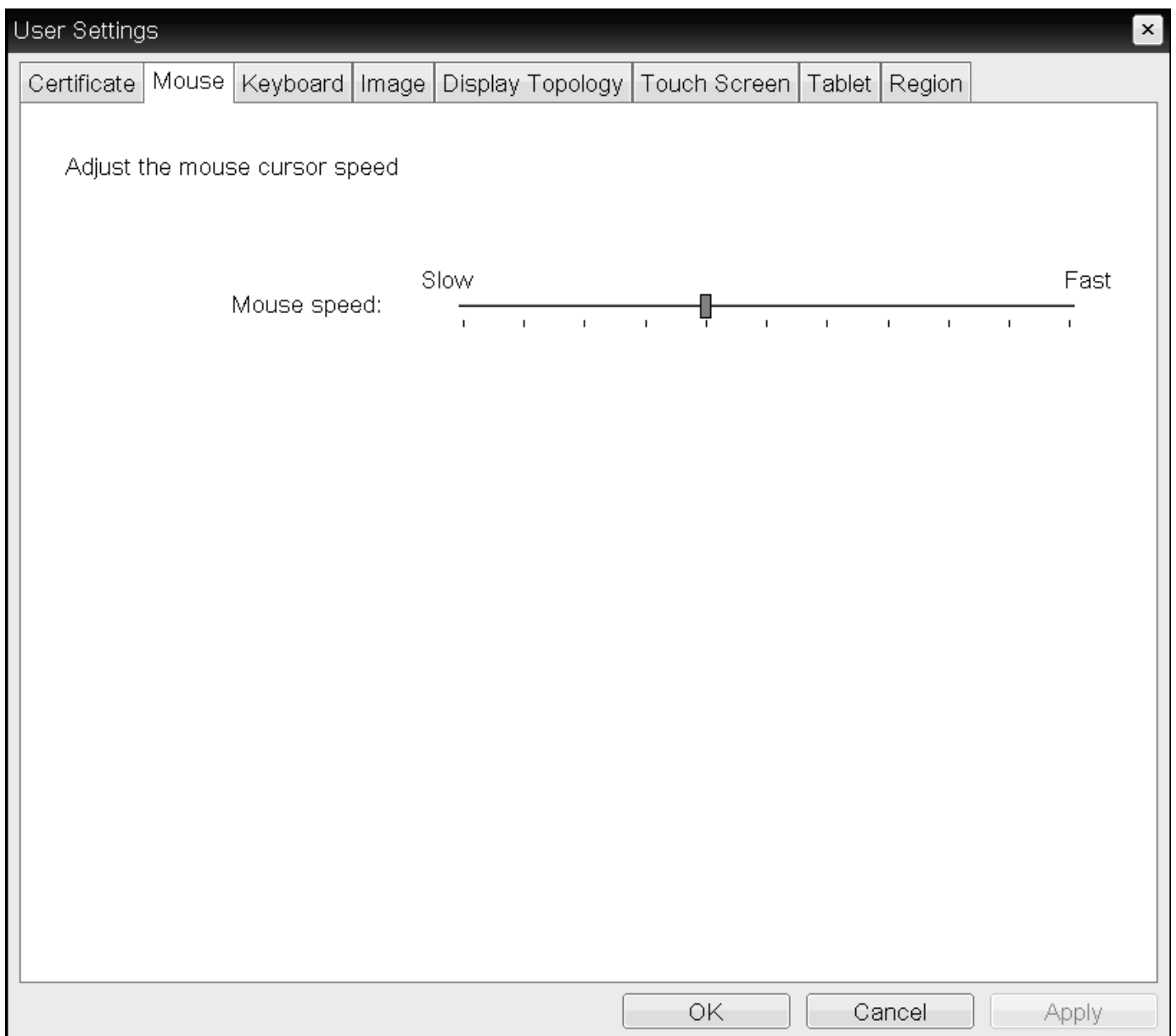
To configure image quality:

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 Speed

Setting	Default	AWI	OSD	Management Console
Mouse speed	40	x	✓	x

From the OSD Mouse page, as shown next, you can change the mouse cursor speed.



OSD Mouse page

Configuring Mouse Speed

Mouse settings 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](#).

To change the mouse cursor speed:

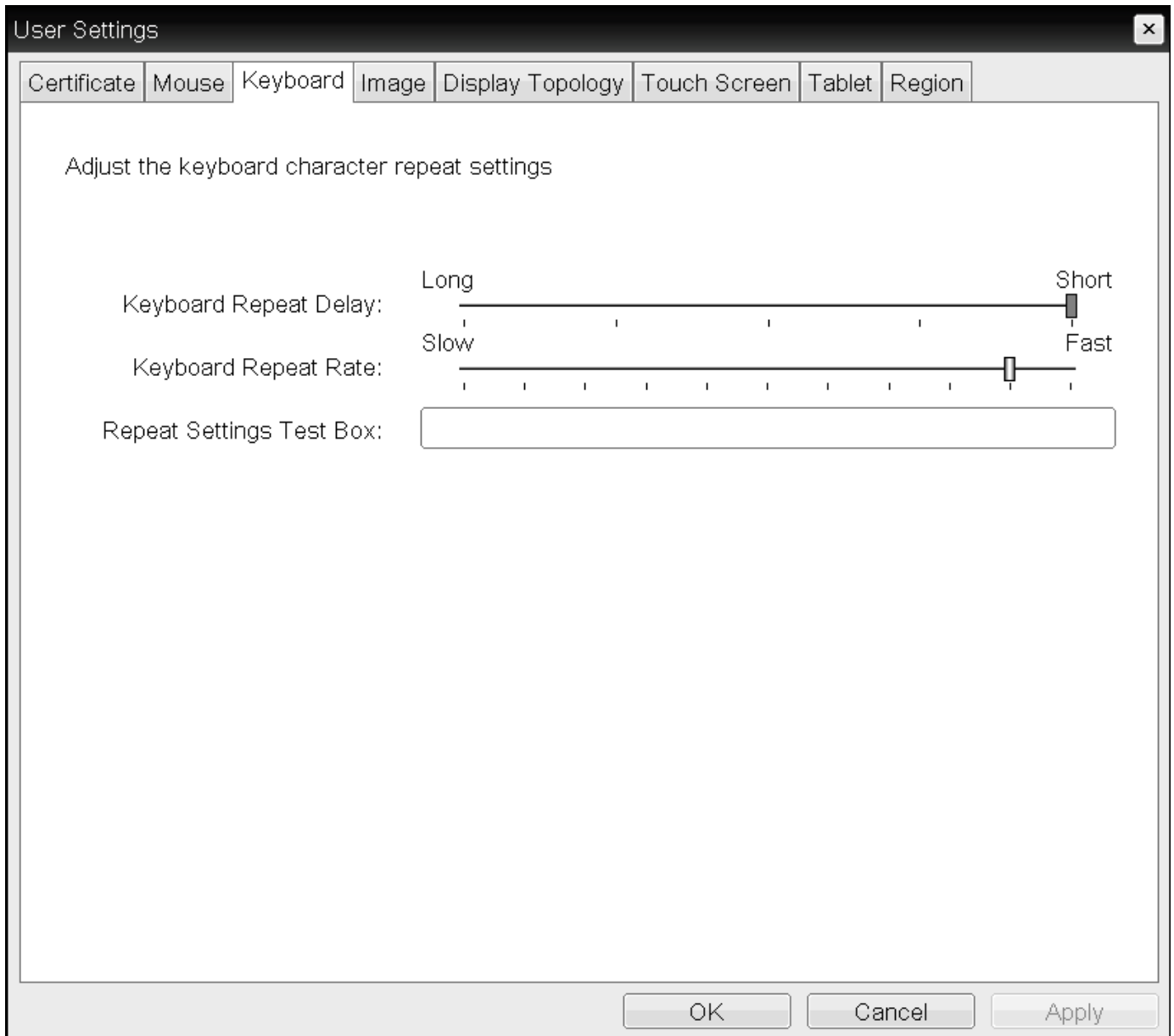
1. From the OSD, select **Options > User Settings > Mouse**.
2. From the OSD Mouse page, move the slider to adjust the mouse cursor speed.
3. Click **OK**.

Configuring Keyboard Settings

Setting	Default	AWI	OSD	Management Console
Keyboard Repeat Delay	100	x	✓	✓
Keyboard Repeat Rate	90	x	✓	✓
Repeat Settings Test Box	N/A	x	✓	✓

From the OSD **Keyboard** page, as shown next, you can change the keyboard character delay and character repeat settings.

Configuring Keyboard 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**.

Configuring Multiple Displays

Setting	Default	AWI	OSD	Management Console
Enable Configuration	Disabled	x	✓	✓
Layout	—	x	✓	✓
Alignment	—	x	✓	✓
Primary	—	x	✓	✓
Position	—	x	✓	✓
Rotation	—	x	✓	✓
Resolution	—	x	✓	✓

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

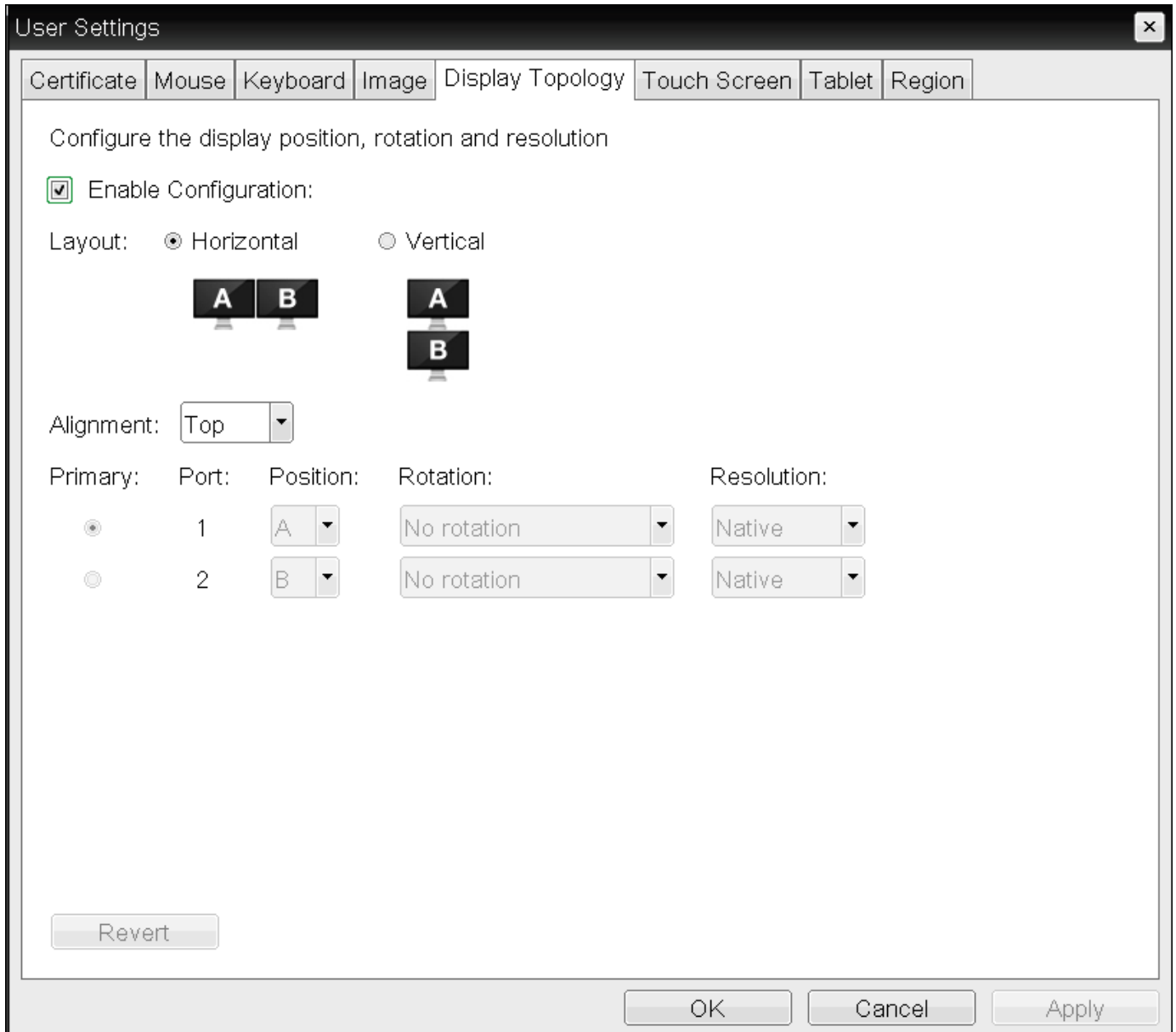
- To apply the display topology feature to a PCoIP session between a client and a VMware Horizon virtual desktop, you must have VMware View 4.5 or higher.
- To apply the display topology feature to a PCoIP session between a client and a PCoIP Remote Workstation Card, you must have the PCoIP host software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

Configuring Two Displays

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. <ul style="list-style-type: none">• 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. <p>Note: This setting affects which area of the screen to use when users move the cursor from one display to the other.</p> The alignment options that appear in the drop-down list depend on the selected display layout. <p>Horizontal layout:</p> <ul style="list-style-type: none">• 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. <p>Vertical layout:</p> <ul style="list-style-type: none">• 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.
Primary	Configure which video port on the Tera2 PCoIP Zero Client you want as the primary port. <p>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).</p> <ul style="list-style-type: none">• 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.

Configuring Four Displays

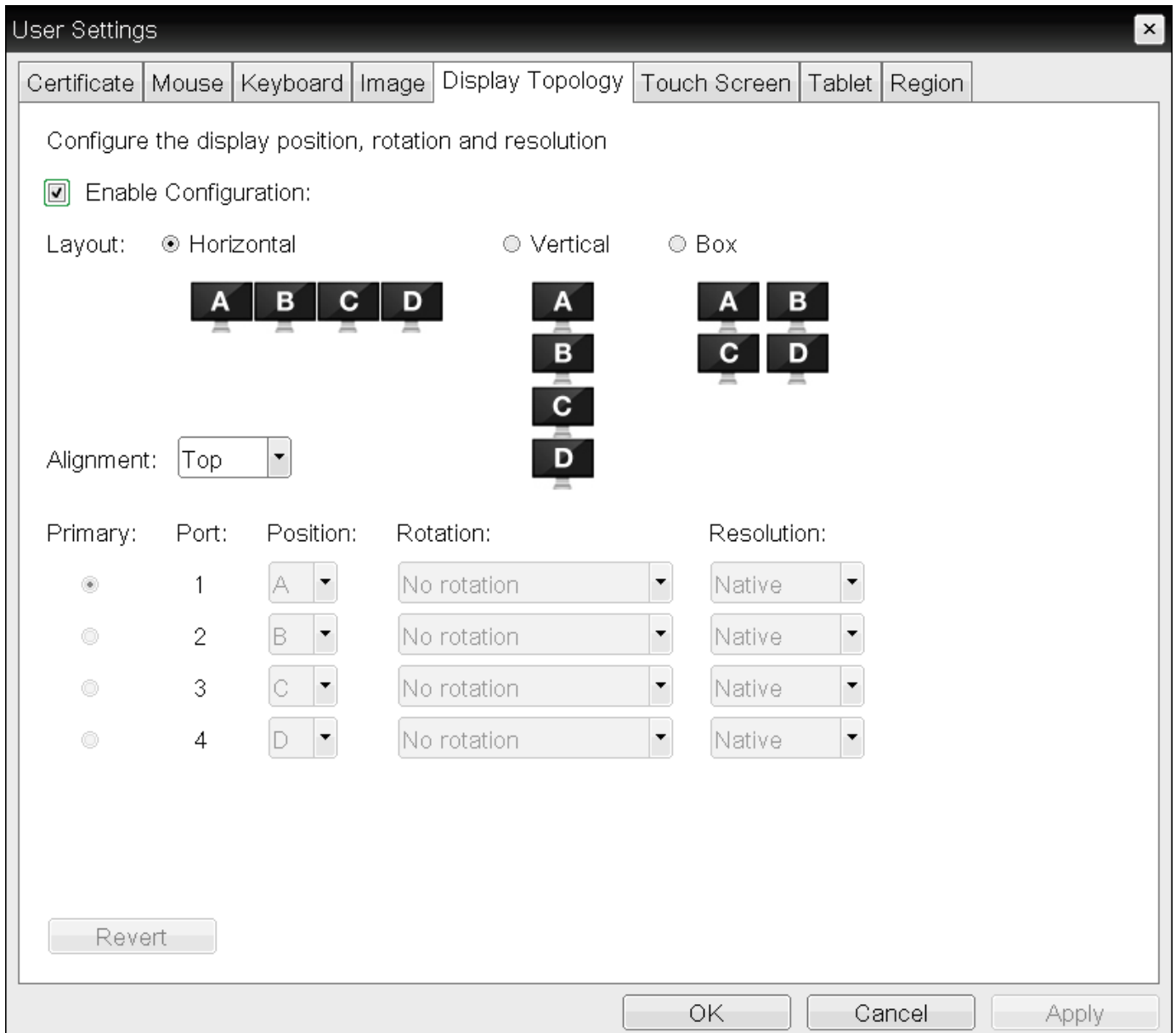
To configure display settings:

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.

Configuring Four Displays



OSD Display Topology page (for four displays)

The following parameters display on the OSD *Display Topology* page:

Display Topology Parameters (Four-Display Configuration)

Configuring Four Displays

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.
Display Layout	<p>Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk.</p> <ul style="list-style-type: none"> • 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	<p>Select how you want displays aligned when they are different sizes.</p> <p>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.</p> <p>Horizontal layout:</p> <ul style="list-style-type: none"> • 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. <p>Vertical layout:</p> <ul style="list-style-type: none"> • 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.
Primary	<p>Configure which video port on the Tera2 PCoIP Zero Client that you want as the primary port.</p> <p>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).</p> <ul style="list-style-type: none"> • 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.

Configuring Four Displays

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**.

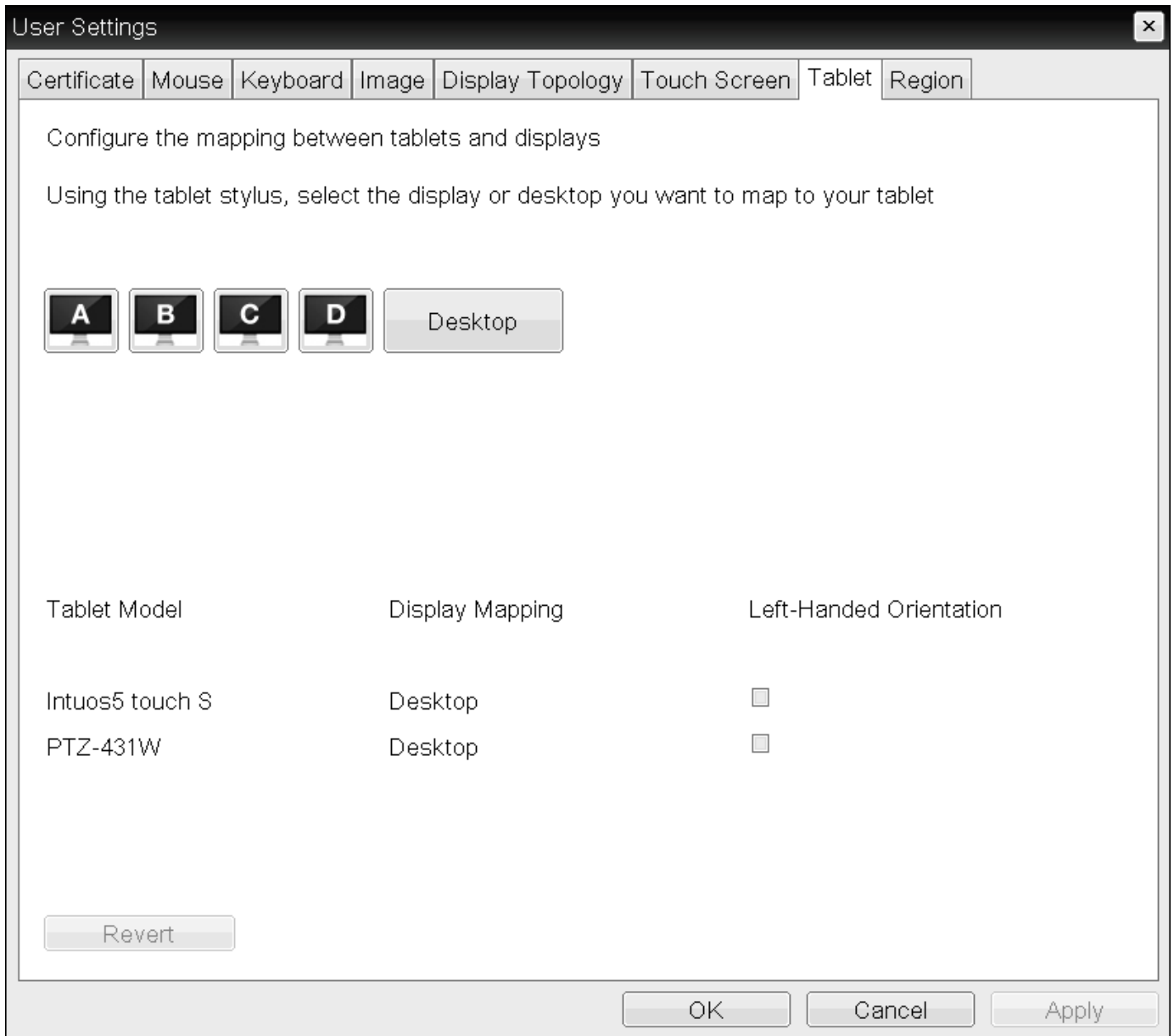
Configuring Tablet Settings

Setting	Default	AWI	OSD	Management Console
Select display or desktop to map to tablet	—	x	✓	x
Left-handed orientation	Disabled	x	✓	x
Revert (a button)	—	x	✓	x

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.

Configuring Tablet Settings



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 host 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.

Configuring Tablet Settings

- 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**.

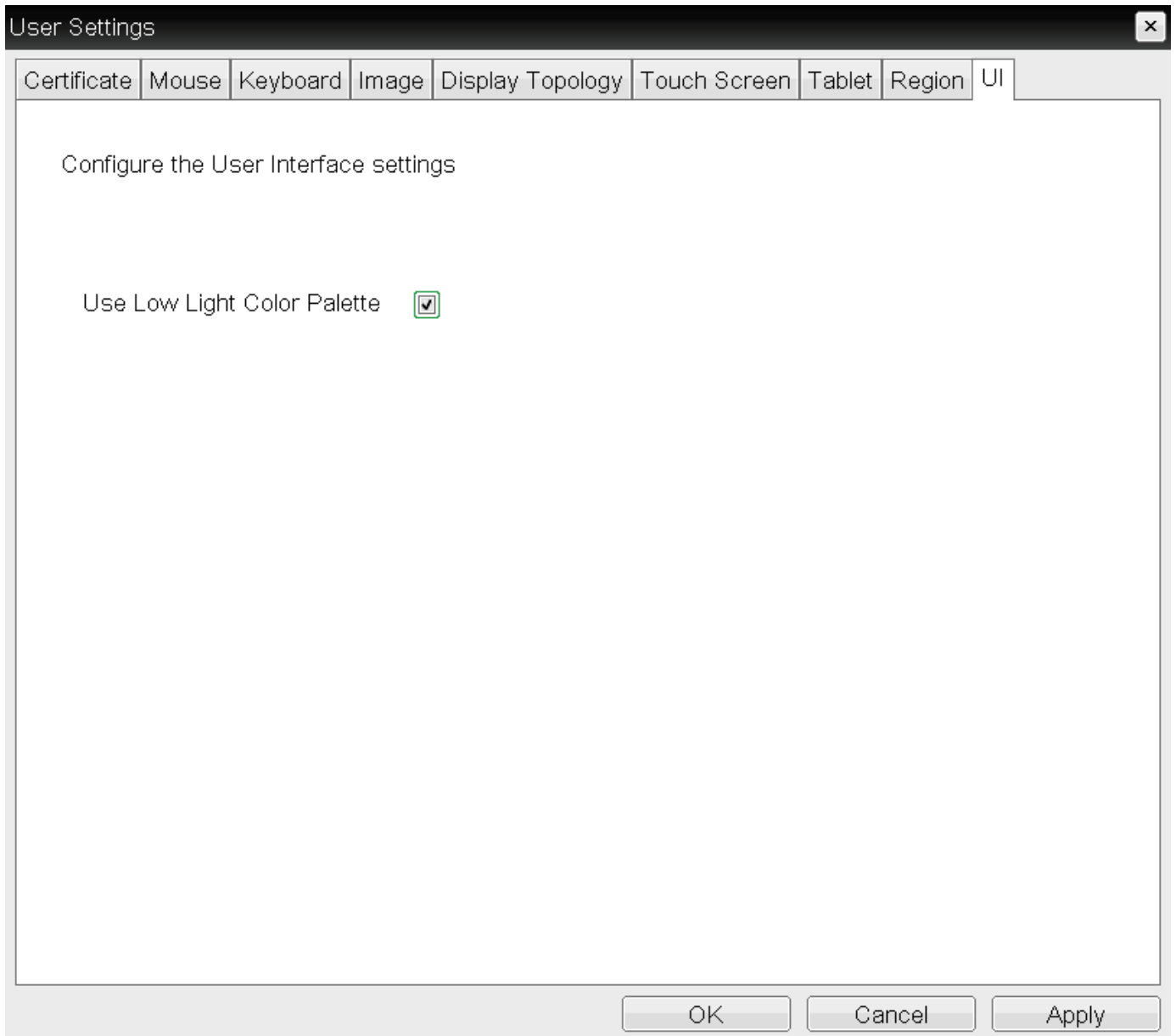
Configuring User Interface

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.

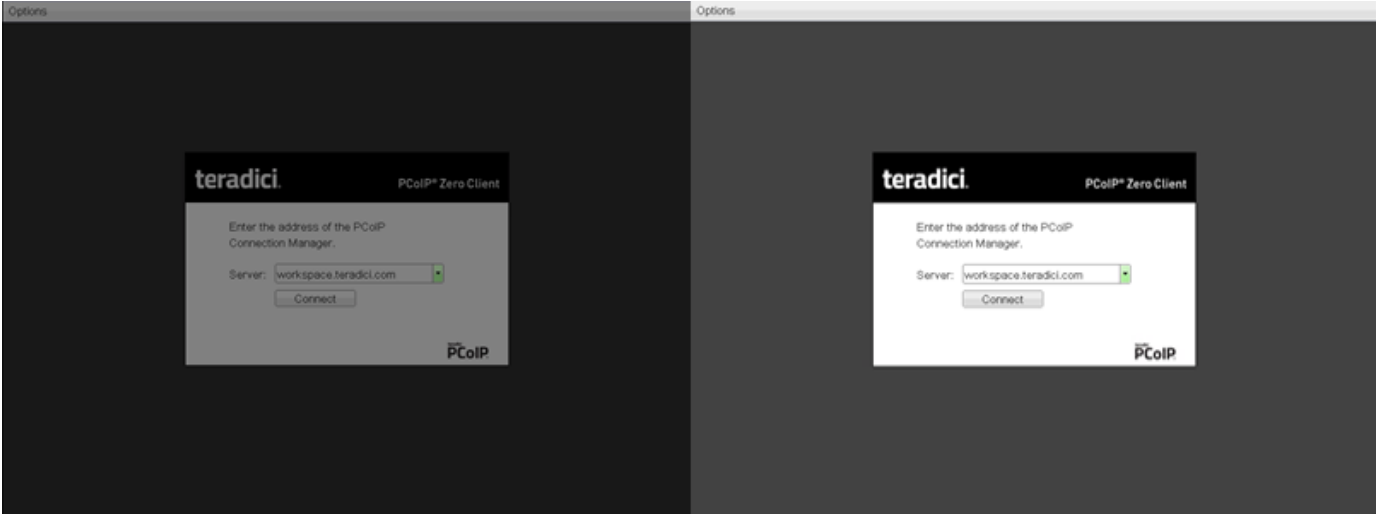
Configuring User Interface



Low Light Setting

The image below shows the difference in brightness when using the low light setting.

Configuring User Interface



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)	✓	x	x
Client Certificate	–	✓	✓	✓
Enable 802.1X Support for Legacy Switches	–	✓	x	✓

This section describes the components you need to configure 802.1x authentication, and the detailed steps you need to follow to configure the authentication.

Preparing for 802.1x Configuration

Before you begin the configuration process, make sure you have these components:

- Tera2 PCoIP Zero Client with firmware 4.0.3 or later
- PCoIP Management Console 1.8.1 or later
- Windows Server 2008 R2 with AD DS (Active Directory Domain Services)
- Windows Server 2008 R2 with AD CS (Active Directory Certificate Services)
- Windows Server 2008 R2 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 Client User.](#)
2. [Export the Root CA Certificate.](#)
3. [Create a Certificate Template for Client Authentication.](#)
4. [Issue the Client Certificate.](#)
5. [Export the Client Certificate.](#)
6. [Convert the Certificate Format from .pfx to .pem.](#)
7. [Import the Client Certificate into the Client User Account.](#)
8. [Import the Certificates to the Client Device.](#)

The following sections assume you are using Windows Server 2008 R2

The instructions in the following sections are based on Windows Server 2008 R2. If you are using a newer version of Windows Server, the steps may vary slightly.

Create a Client User

In the Windows 2008 server, create a client user.

To create a client user:

1. Log in to the Windows 2008 server.
2. Click **Start > Administrative Tools > Server Manager**.
3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > ## > Users**.
4. Right-click Users, select **New > User**, and follow the wizard.

Export the Root CA Certificate

In the Certificate Authority (CA) server, export the root CA certificate.

Create a Certificate Template for Client Authentication

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 **Finish**, and **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)**.
 - 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 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 **General** tab, enter a name for the template (for example, **PCoIP Zero Client 802.1x**) and change the validity period to match the organization's security policy.
 - c. From the **Request Handling** tab, select **Allow private key to be exported**.

Issue the Client Certificate

- d. From the *Subject Name* tab, select **Supply in the request**.
 - e. From the Security tab, select the user who will be requesting the certificate, and give Enroll permission to this user.
 - f. 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 Zero Client 802.1x**), and then click **OK**. The template will now appear in the *Certificate Templates* list.
 8. Close the window.

Issue the Client Certificate

From the CA Web Enrollment interface for the certificate server, issue the client certificate.

To issue the 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.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format **https:///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, **Zero Client 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.

Export the Client Certificate

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 Client User](#) (for example, `ZeroClient@mydomain.local`)

- c. In the Additional Options section, set the Request Format to PKCS10.
- d. If desired, enter a name in the Friendly Name field.
- e. Click Submit, and then click Yes at the pop-up window.
- f. From the Certificate Issued window, click Install this certificate.

Export the 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 wizard to export the certificate:
 - 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 **Finish**, and then click **OK**.
8. Repeat Steps 5 to 7 again to export the Tera2 PCoIP Zero Client 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.

Convert the Certificate Format from .pfx to .pem

9. Save this `.cer` file to a location where it can be accessed by the Windows 2008 server 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 <http://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, and enter the following command to convert the certificate format from `.pfx` to `.pem`: `C:\OpenSSL-Win32\bin\openssl.exe pkcs12 -in <client_cert>.pfx -out <client_cert>.pem -nodes` where is the name of the `.pfx` certificate file you saved to your local machine.
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: `C:\OpenSSL-Win32\bin\openssl.exe rsa -in <client_cert>.pem -out <client_cert>_rsa.pem` where is the name of the `.pem` certificate file you created in the previous step.
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 Tera2 PCoIP Zero Client 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.

Import the Client Certificate into the Client User Account

- c. Save the original **.pem** file and close it. The certificate is now ready to be uploaded to the Tera2 PCoIP Zero Client.

Import the Client Certificate into the Client User Account

In the Windows 2008 server, import the client certificate into the client user account.

To import the client certificate into the client user account:

1. Log in to the Windows 2008 server.
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 Tera2 PCoIP Zero Client.
5. Right-click the user, and select **Name Mappings**.
6. In the **X.509 Certificates** section, click **Add**.
7. Locate and select the Tera2 PCoIP Zero Client certificate you exported that does not contain the private key (This file was saved to a network location in step 9 of [Export the Client Certificate](#).)
8. Make sure both identity boxes are selected. Click **OK**, and then click **OK** again.

Import the Certificates to the Client Device

From the device's AWI, import the certificates.


To import the certificates into a profile using the PCoIP Management Console, see the PCoIP® Management Console 3.1 Administrators' Guide.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the Tera2 PCoIP Zero Client or PCoIP Remote Workstation Card.
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.

Import the Certificates to the Client Device

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, `zeroclient@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 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 \(KB 1088\)](#)

Display Override Overview

Under normal operation, the GPU in the host computer queries a monitor attached to the Tera2 PCoIP Zero Client to determine the monitor's capabilities. These are reported in the 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 two-monitor setup, or a four-monitor setup.

Configuring Display Override Settings (Dual)

Setting	Default	AWI	OSD	Management Console
Enable Attached Display Override	—	x	✓	✓
Enable Preferred Resolution Override	—	x	✓	✓
Enable Display Cloning	—	x	✓	✓

From the OSD *Display* page, shown next, you can enable the Extended Display Identification Data (EDID) override mode for a setup with two or four attached displays.

Configuring Display Override Settings (Dual)

Configuration ✕

Network | IPv6 | Management | SCEP | Label | Discovery | Session | Power | **Display** | Access | Audio | Reset

The Enable Attached Display Override feature will force all ports to show that a display is attached. This will advertise a default EDID if no display is physically attached to a port.

Enable Attached Display Override:

The Preferred Resolution Override feature allows you to specify a specific resolution to use for each attached display.

NOTE: In the case of an EDID read failure, the drop-down list may contain resolutions that are not actually supported by your display. If the display stays black or shows a 'Timing Out Of Range' message for more than 30 seconds after changing the preferred resolution, you can unplug and re-plug the video cable to reset your display resolution back to its native value.

Enable Preferred Resolution Override:

Preferred resolution 1:

Preferred resolution 2:

The Enable Display Cloning feature will duplicate the primary display to the secondary display.

Enable Display Cloning:

OSD Display page (two-display setup)

Configuring Display Override Settings (Dual)

Configuration ✕

Network IPv6 Management SCEP Label Discovery Session Power Display Access Audio Reset

The Enable Attached Display Override feature will force all ports to show that a display is attached. This will advertise a default EDID if no display is physically attached to a port.

Enable Attached Display Override:

The Preferred Resolution Override feature allows you to specify a specific resolution to use for each attached display.

NOTE: In the case of an EDID read failure, the drop-down list may contain resolutions that are not actually supported by your display. If the display stays black or shows a 'Timing Out Of Range' message for more than 30 seconds after changing the preferred resolution, you can unplug and re-plug the video cable to reset your display resolution back to its native value.

Enable Preferred Resolution Override:

Preferred resolution 1:

Preferred resolution 2:

Preferred resolution 3:

Preferred resolution 4:

Unlock OK Cancel Apply

OSD Display page (four-display setup)

Enable the Enable Attached Display Override feature when there is no valid EDID information

Only enable 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 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).

Configuring Display Override Settings (Dual)

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 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.

The following parameters display on the OSD Display page:

Display Parameters

Configuring Display Override Settings (Dual)

Parameter	Description
Enable Attached Display Override	<p>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.</p> <p>The following default resolutions are advertised when this option is enabled:</p> <ul style="list-style-type: none">• 2560x1600 @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 <p>When this option is enabled, all displays attached to the Tera2 PCoIP Zero Client will be set to the native resolution of 1024x768.</p>
Enable Preferred Resolution	<p>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 will</p>

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**.

Configuring Display Override Settings (Quad)

Setting	Default	AWI	OSD	Management Console
Enable Attached Display Override	—	x	✓	✓
Enable Preferred Resolution Override	—	x	✓	✓
Enable Display Cloning	—	x	✓	✓

From the OSD *Display* page, as shown next, you can enable the Extended Display Identification Data (EDID) override mode for a setup with two or four attached displays.

The Display page lets you enable the Extended Display Identification Data (EDID) override mode. You can access this page from the **Options > Configuration > Display** menu.

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 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.

Configuring Display Override Settings (Quad)

Configuration

Network IPv6 Management SCEP Label Discovery Session Power Display Access Audio Reset

The Enable Attached Display Override feature will force all ports to show that a display is attached. This will advertise a default EDID if no display is physically attached to a port.

Enable Attached Display Override:

The Preferred Resolution Override feature allows you to specify a specific resolution to use for each attached display.

NOTE: In the case of an EDID read failure, the drop-down list may contain resolutions that are not actually supported by your display. If the display stays black or shows a 'Timing Out Of Range' message for more than 30 seconds after changing the preferred resolution, you can unplug and re-plug the video cable to reset your display resolution back to its native value.

Enable Preferred Resolution Override:

Preferred resolution 1: Native

Preferred resolution 2: Native

Preferred resolution 3: Native

Preferred resolution 4: Native

Unlock OK Cancel Apply

OSD TERA2140 Display page

The following parameters display on the TERA2140 OSD *Display* page:

OSD TERA2140 Display Parameters

Configuring Display Override Settings (Quad)

Parameter	Description
Enable Attached Display Override	<p>This option is intended for legacy systems. It configures the client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. In versions of Windows prior to Windows 7, once the host had no EDID information, it would assume no monitors were attached and would never recheck. This option ensures that the host always has EDID information when the client is in session.</p> <p>The following default resolutions are advertised when this option is enabled:</p> <ul style="list-style-type: none"> • 2560x1600 @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 <p>Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.</p>
Enable Default	<p>Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions is advertised</p>

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	✓	x	✓
Enable Syslog	Enabled	✓	x	✓
Identify Syslog Host By	IP Address	✓	x	✓
Syslog Host IP Address / Syslog Host DNS Name		✓	x	✓
Syslog Host Port	514	✓	x	✓
Syslog Facility	19 – local use	✓	x	✓

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.

Enabling Event Log

You enable the event log, as well as syslog settings, from the AWI *Event Log* page, as shown next.

Event Log

Configure diagnostic logging options

Enable Event Log:

Event Log Messages:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: . . .

Syslog Host Port:

Syslog Facility:

Enhanced logging mode:

Category	Enable enhanced logging
AUDIO	<input type="radio"/>
MANAGEMENT CONSOLE	<input type="radio"/>
NETWORKING	<input type="radio"/>
ONESIGN	<input type="radio"/>
SESSION NEGOTIATION	<input type="radio"/>
SMARTCARD	<input type="radio"/>
SYSTEM	<input type="radio"/>
USB	<input type="radio"/>
VIDEO	<input type="radio"/>

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.

Enabling Syslog

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.

Enabling Syslog



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

Enabling Syslog

Parameter	Description
Enable Syslog	<p>Enable or disable the syslog standard as the logging mechanism for the device.</p> <p>You must configure all fields when syslog is enabled.</p> <p>If you enable syslog, you must configure the remaining fields. If you disable syslog, you can't edit the fields.</p>
Identify Syslog Host By	<p>Choose if the syslog server host is identified by its IP address or by its Fully Qualified Domain Name (FQDN).</p>
Syslog Host IP Address / Syslog Host DNS name	<p>The parameter that displays depends on which option you choose to identify the syslog server host:</p> <ul style="list-style-type: none">• IP Address: Enter the IP address for the syslog server host.• FQDN: Enter the DNS name for the syslog server host. <p>If you enter an invalid IP address or DNS name, a message displays to prompt you to correct it.</p>
Syslog Host Port	<p>Enter the port number of the syslog server. The default port number is 514.</p>
Syslog Facility	<p>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.</p> <p>Enter a facility to suit your logging needs. For example, you could configure devices as follows:</p> <ul style="list-style-type: none">• Zero clients to use facility 19• Cisco routers to use facility 20• VMware ESX hosts to use facility 21 <p>The default facility is set to 19 – local use 3. Cisco routers default to 23 – local use 7.</p>

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)	—	x	✓	x
Refresh (F5)	—	✓	✓	x
Clear (a button)	—	✓	✓	x
Enable Event Log	Enabled	✓	✓	✓
Enable Syslog	Enabled	✓	x	✓
Enable Syslog Host By IP Address	—	x	✓	x
Syslog Host IP Address	—	x	✓	x
Syslog Host Port	514	x	✓	x
Syslog Facility	19 – local use 3	✓	x	x
Enhanced logging mode	Disabled	x	✓	x

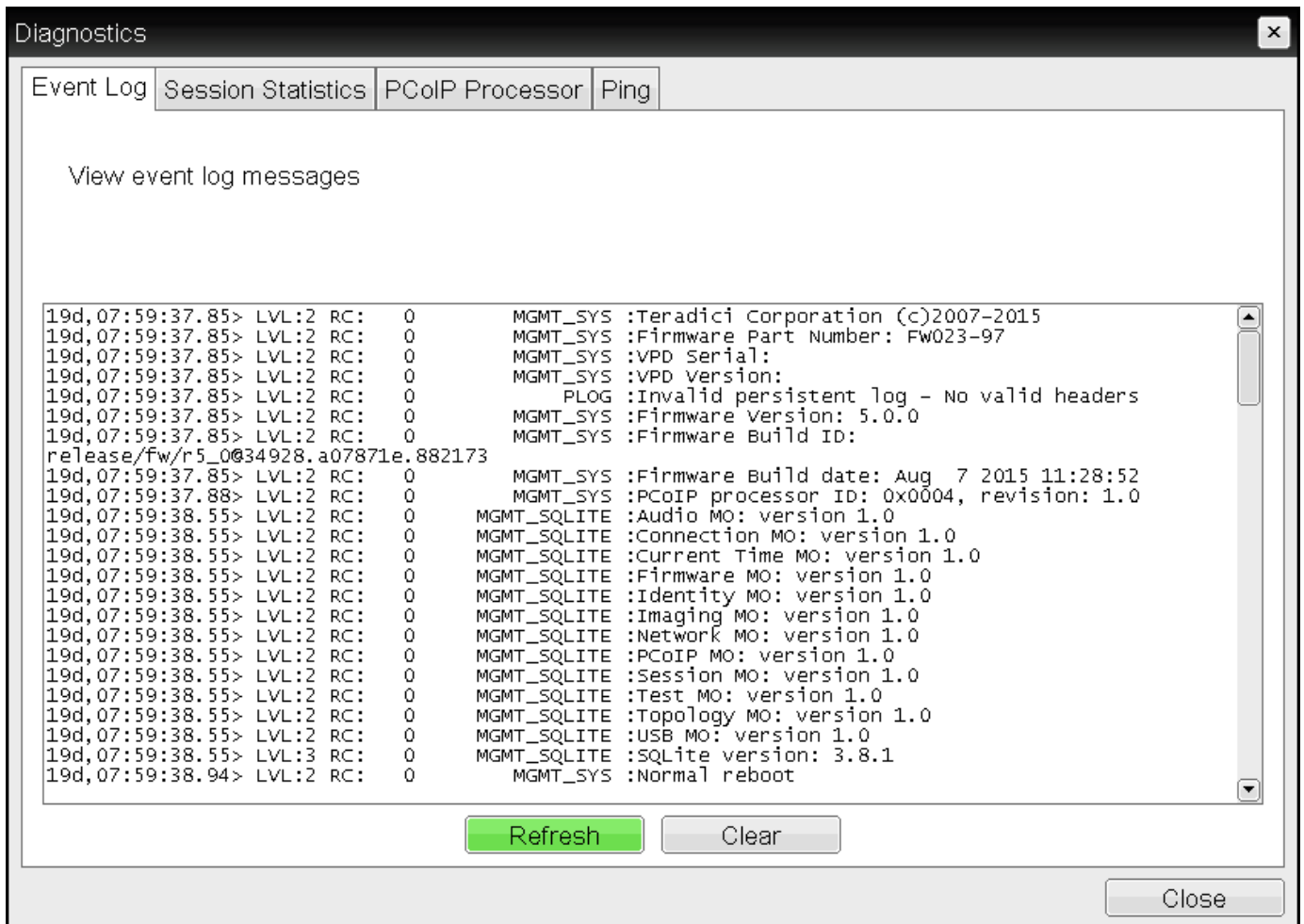
From the OSD and AWI, you can view and clear all the event log messages stored on your Tera2 PCoIP Zero Client.

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.

Event Log
Configure diagnostic logging options

Enable Event Log:

Event Log Messages:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: . . .

Syslog Host Port:

Syslog Facility: ▼

Enhanced logging mode:

Category	Enable enhanced logging
AUDIO	<input type="radio"/>
MANAGEMENT CONSOLE	<input type="radio"/>
NETWORKING	<input type="radio"/>
ONESIGN	<input type="radio"/>
SESSION NEGOTIATION	<input type="radio"/>
SMARTCARD	<input type="radio"/>
SYSTEM	<input type="radio"/>
USB	<input type="radio"/>
VIDEO	<input type="radio"/>

AWI Event Log page

The following parameters display on the AWI Event Log page.

AWI Event Log Parameters

Performing Logging Tasks from the AWI

Parameter	Description
Enable Event Log	<p>When this feature is enabled, logging occurs in verbose mode, and all event log and syslog options display.</p> <p>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.</p>
Event log Messages	<ul style="list-style-type: none"> • 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	<p>Enable or disable the syslog standard as the logging mechanism for the device.</p> <p>Note: If you enable syslog, you must configure the remaining fields. If you disable syslog, you can't edit the fields.</p>
Identify Syslog Host By	<p>Choose if the syslog server host is identified by its IP address or by its Fully Qualified Domain Name (FQDN).</p>
Syslog Host IP Address / Syslog Host DNS name	<p>The parameter that displays depends on which option you choose to identify the syslog server host:</p> <ul style="list-style-type: none"> • IP Address: Enter the IP address for the syslog server host. • FQDN: Enter the DNS name for the syslog server host. <p>If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it.</p>
Syslog Host Port	<p>Enter the port number of the syslog server. The default port number value is 514.</p>
Syslog Facility	<p>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.</p> <p>Enter a facility to suit your logging needs. For example, you could configure devices as follows:</p> <ul style="list-style-type: none"> • Zero clients to use facility 19 • Cisco routers to use facility 20 • VMware FSX hosts to use facility 21

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.

i 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	✓	x	✓

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](#)).

Configuring Enhanced Logging Mode

Event Log

Configure diagnostic logging options

Enable Event Log:

Event Log Messages:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: . . .

Syslog Host Port:

Syslog Facility:

Enhanced logging mode:

Category	Enable enhanced logging
AUDIO	<input type="radio"/>
MANAGEMENT CONSOLE	<input type="radio"/>
NETWORKING	<input type="radio"/>
ONESIGN	<input type="radio"/>
SESSION NEGOTIATION	<input type="radio"/>
SMARTCARD	<input type="radio"/>
SYSTEM	<input type="radio"/>
USB	<input type="radio"/>
VIDEO	<input type="radio"/>

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.

Configuring Enhanced Logging Mode

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)	—	✓	✓	x
Refresh (a button on the OSD, F5 from the AWI)	—	✓	✓	x
Clear (a button)	—	✓	✓	x

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).

Viewing Event Logs

The screenshot shows a window titled "Diagnostics" with a close button in the top right corner. Below the title bar are four tabs: "Event Log" (selected), "Session Statistics", "PCoIP Processor", and "Ping". The main area contains the text "View event log messages" and a scrollable list of log entries. At the bottom of the window are three buttons: "Refresh" (green), "Clear" (grey), and "Close" (grey).

```
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :Teradici Corporation (c)2007-2015
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :Firmware Part Number: Fw023-97
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :VPD Serial:
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :VPD Version:
19d,07:59:37.85> LVL:2 RC: 0 PLOG :Invalid persistent log - No valid headers
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :Firmware Version: 5.0.0
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :Firmware Build ID:
release/fw/r5_0@34928.a07871e.882173
19d,07:59:37.85> LVL:2 RC: 0 MGMT_SYS :Firmware Build date: Aug 7 2015 11:28:52
19d,07:59:37.88> LVL:2 RC: 0 MGMT_SYS :PCoIP processor ID: 0x0004, revision: 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Audio MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Connection MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Current Time MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Firmware MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Identity MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Imaging MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Network MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :PCoIP MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Session MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Test MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :Topology MO: version 1.0
19d,07:59:38.55> LVL:2 RC: 0 MGMT_SQLITE :USB MO: version 1.0
19d,07:59:38.55> LVL:3 RC: 0 MGMT_SQLITE :SQLite version: 3.8.1
19d,07:59:38.94> LVL:2 RC: 0 MGMT_SYS :Normal reboot
```

OSD Event Log page

Viewing Event Logs

Event Log

Configure diagnostic logging options

Enable Event Log:

Event Log Messages:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: . . .

Syslog Host Port:

Syslog Facility:

Enhanced logging mode:

Category	Enable enhanced logging
AUDIO	<input type="radio"/>
MANAGEMENT CONSOLE	<input type="radio"/>
NETWORKING	<input type="radio"/>
ONESIGN	<input type="radio"/>
SESSION NEGOTIATION	<input type="radio"/>
SMARTCARD	<input type="radio"/>
SYSTEM	<input type="radio"/>
USB	<input type="radio"/>
VIDEO	<input type="radio"/>

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.

Viewing Event Logs

- 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)	N/A	✓	✓	x

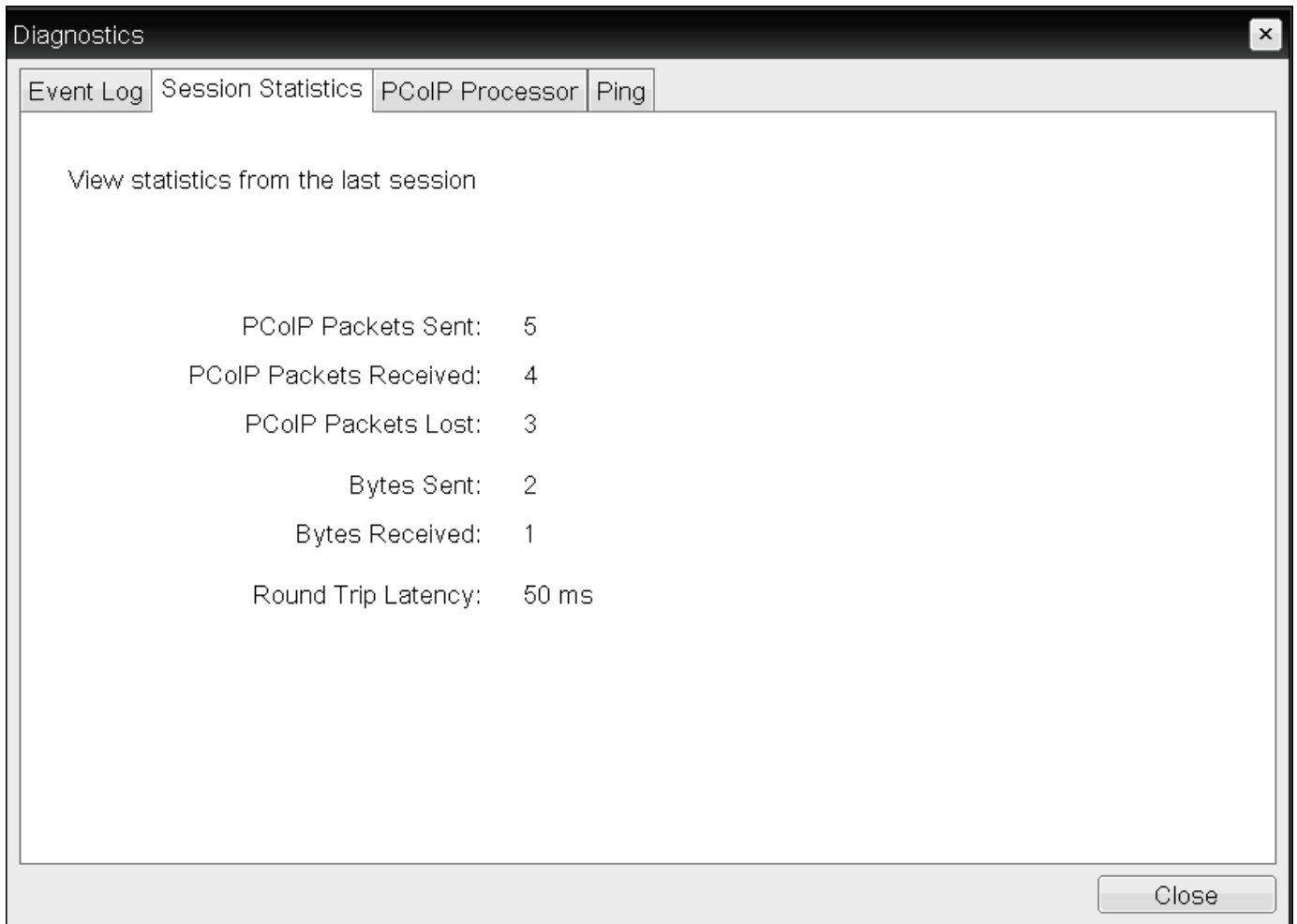
The OSD displays session statistics from the last PCoIP session.

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](#)).

Session Statistics

View statistics for the current session

Connection State: Connected to host [192.168.65.103](#)

802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 44769 / 68244 / 0

Bytes (Sent/Received): 5638498 / 31681880

Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms

Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 112 / 392 / 8000 kbps

Receive Bandwidth (Min/Avg/Max): 0 / 200 / 5600 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 37 / 297 Mpps

Endpoint Image Settings In Use: Client

Initial Image Quality (Min/Max): 40 / 90

Image Quality Preference: 50

Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Output Process Rate	Image Quality
1	60 fps	8 fps	Lossy
2	60 fps	0 fps	Lossless
3	N/A	N/A	N/A
4	N/A	N/A	N/A

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

Viewing and Resetting Session Statistics from the AWI

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Possible connection states are: <ul style="list-style-type: none"> • 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	<p>PCoIP Packets Sent: The total number of PCoIP packets sent in the current/last session.</p> <p>PCoIP Packets Received: The total number of PCoIP packets received in the current/last session.</p> <p>PCoIP Packets Lost: The total number of PCoIP packets lost in the current/last session.</p>
Bytes	<p>Bytes Sent: The total number of bytes sent in the current/last session.</p> <p>Bytes Received: The total number of bytes received in the current/last session.</p>
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (± 1 ms).
Bandwidth Statistics	<p>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.</p> <p>**Receive Bandwidth: The minimum, average, and maximum traffic received by the Tera processor.</p>
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	The minimum and maximum quality setting is taken from the Image page for the device.

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.

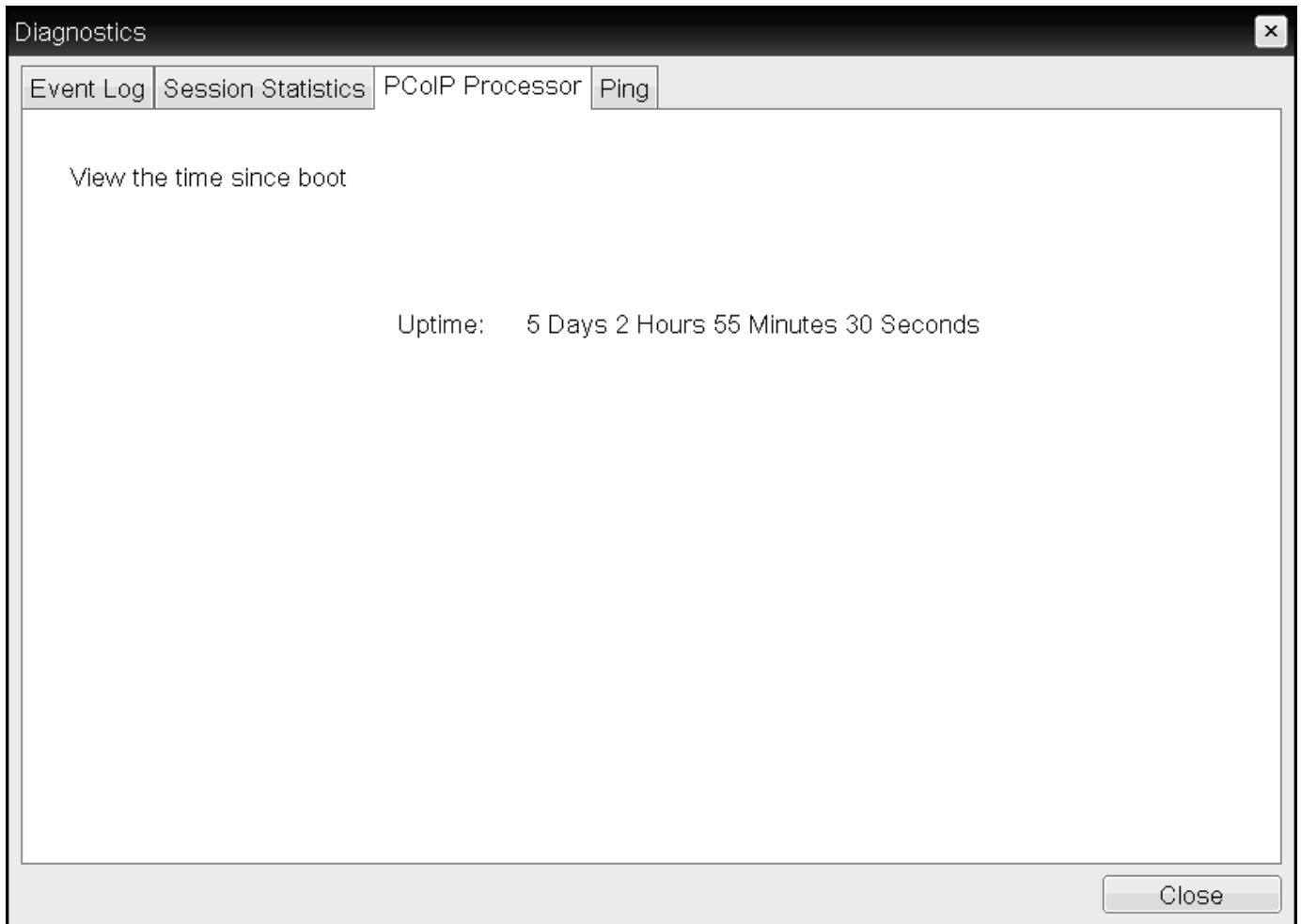
Viewing PCoIP Processor Statistics

Setting	Default	AWI	OSD	Management Console
Reset PCoIP Processor (a button)	N/A	✓	✓	x

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.

PCoIP Processor

Reset the PCoIP device, view the time elapsed since boot

Current Time: 08/10/2015 17:20:58

Time Since Boot: 0 Days 5 Hours 49 Minutes 49 Seconds

Reset 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	—	x	✓	x
Interval	1	x	✓	x
Packet Size	32	x	✓	x
Sent	—	x	✓	x
Received	—	x	✓	x
Start (a button)	—	x	✓	x
Stop (a button)	—	x	✓	x

From the OSD Ping page, as shown next, you can ping a host to see if it's reachable across the IP network.

Pinging the Host

Diagnostics

Event Log | Session Statistics | PCoIP Processor | Ping

Determine if a host is reachable across the network

Destination:

Interval: seconds

Packet Size: bytes

Packets:

Sent: 0

Received: 0

Start Stop Close

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

Pinging the Host

Parameter	Description
Destination	IP address or Fully Qualified Domain Name (FQDN) to ping.
Interval	Interval between ping packets.
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	✓	x	x
Disconnect (a button)	Enabled if a session is connected / Disabled if a session is disconnected	✓	x	x

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.

Session Control

Control the device

Connection State: Connected to host [192.168.65.103](#)

Peer IP Address: 192.168.65.103

Peer MAC Address: 00-30-04-0D-EB-9B

AWI Session Control page

The following parameters display on the AWI Session Control page:

Session Control Parameters

Controlling Sessions

Parameter	Description
Connection State	<p>This field displays the current state of the session. Options include the following:</p> <ul style="list-style-type: none">• Disconnected• Connection Pending• Connected <p>Two buttons appear below the Connection State field:</p> <ul style="list-style-type: none">• 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.

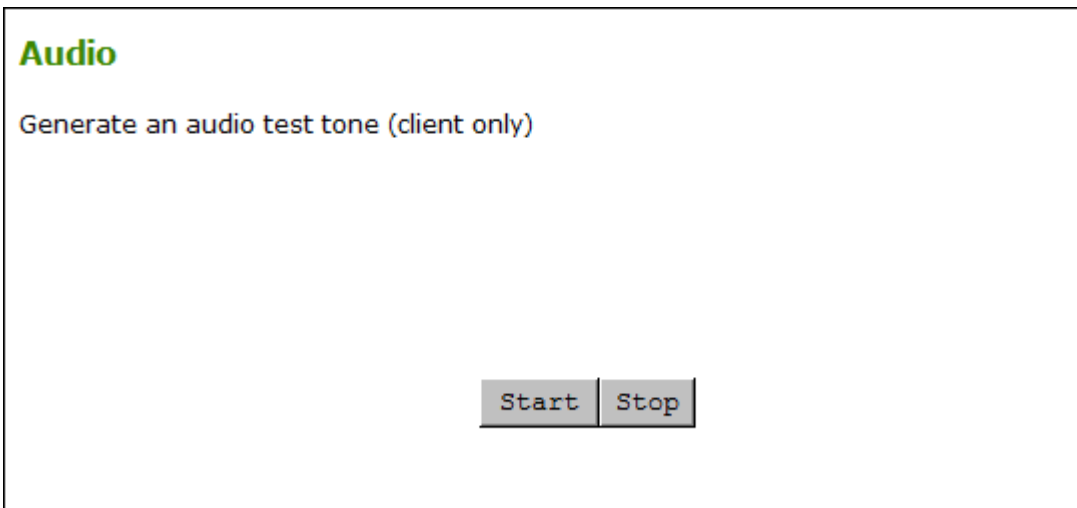
To manually disconnect from or connect to a session:

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)	-	✓	x	x
Stop (a button)	-	✓	x	x

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	✓	x	x
Test resolution	2048x1152	✓	x	x
Start (a button)	-	✓	x	x
Stop (a button)	-	✓	x	x

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.

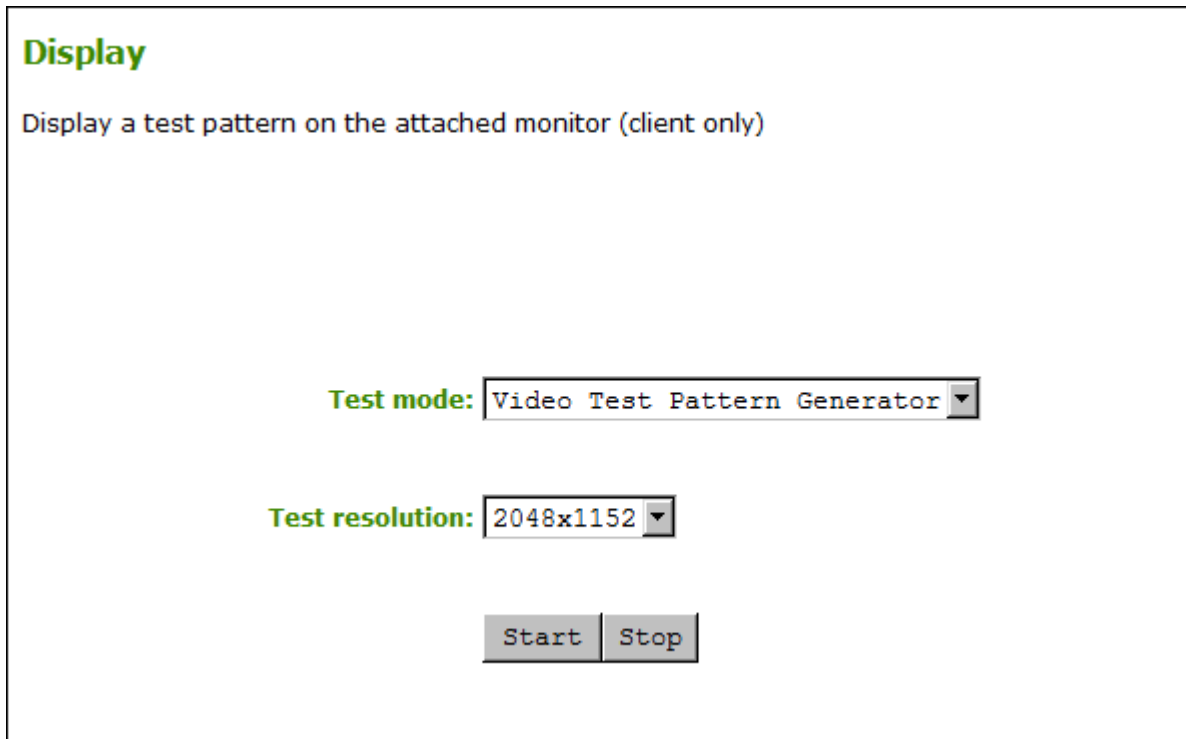
Display

Display a test pattern on the attached monitor (client only)

Test mode: Video Test Pattern Generator ▼

Test resolution: 2048x1152 ▼

Start Stop

The image shows a screenshot of a web interface titled "Display". Below the title is the instruction "Display a test pattern on the attached monitor (client only)". There are two dropdown menus: "Test mode" set to "Video Test Pattern Generator" and "Test resolution" set to "2048x1152". At the bottom are two buttons labeled "Start" and "Stop".

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)	-	✓	x	x
Download (a link)	-	✓	x	x

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.

Packet Capture

Capture network packets for diagnostics


Packet Capture Status: Idle

Bytes (Captured/Max): 0 / 20971520 (0.0 %) in 0 packets

Diagnostic Packet Capture:

Download Packet Capture: Download

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:

Using the Packet Capture Tool

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.
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 <code>packet_capture.bin</code> 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 Tera2 PCoIP Zero Client exchanges information with several services while connecting to endpoint managers, connection managers, and PCoIP hosts. The various communication phases are described here, together with the set of cipher algorithms available to each phase. The topics include:

- [Encrypting Browser Connections](#)
- [Encrypting Endpoint Discovery](#)
- [Encrypting Endpoint Manager Administration](#)
- [Encrypting Pre-Session Communications with VMware Horizon Environments](#)
- [Encrypting Pre-Session Communications with PCoIP Connection Managers](#)
- [Encrypting PCoIP Session Negotiation with PCoIP Hosts](#)
- [In-Session Encryption](#)

Encrypting Browser Connections

You can manage Tera2 PCoIP Zero Clients using a browser connection to the AWI. These secure connections require Transport Layer Session (TLS) 1.1 or TLS 1.2 compliant browsers. Browsers configured to use SSLv3 and TLS 1.0 are not supported.

The following cipher suites are used to secure a browser connection to the AWI:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA



Recommended Web Browsers

Recommended web browsers are Firefox, Chrome, Internet Explorer 11, and Edge.

Encrypting Endpoint Discovery

Tera2 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 Tera2 PCoIP Zero Client, communications between the endpoint manager and the Tera2 PCoIP Zero Client are established securely using one of the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA



Minimum SSL Version

There is a minimum required SSL version of TLS 1.1

Encrypting Endpoint Manager Administration

Once an endpoint manager discovers a Tera2 PCoIP Zero Client, it uses the PCoIP Management Protocol to administer the endpoint. Communications between endpoint managers and Tera2 PCoIP Zero Clients are secured using one of the following cipher suites:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Minimum SSL Version

There is a minimum required SSL version of TLS 1.1.

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 Tera2 PCoIP Zero Client communicates with a Horizon Connection Server over port 443 using one of the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

System Configuration Requirements

These cipher suites can only be configured at the host, and have a minimum required SSL version of TLS 1.1.

Encrypting Pre-Session Communications with PCoIP Connection Managers

Before a PCoIP session is negotiated with a PCoIP host using a PCoIP Connection Manager, each user is authenticated and then selects a desktop from a list of authorized resources. To complete this authentication process, the Tera2 PCoIP Zero Client communicates with a PCoIP Connection Manager over port 443 using one of the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

System Configuration Requirements

These cipher suites can only be configured at the host, and have a minimum required SSL version of TLS 1.1.

Encrypting PCoIP Session Negotiation with PCoIP Hosts

After user authentication and resource selection, PCoIP sessions are negotiated between the Tera2 PCoIP Zero Client and the PCoIP host. These negotiations take place before the PCoIP session is established, and are secured using these Max Compatibility and Suite B cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

In-Session Encryption

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Minimum SSL Version

These Max Compatibility security level cipher suites have a minimum required SSL version of TLS 1.1.

The following Suite B security level cipher suite has a minimum required SSL version of TLS 1.2, and applies only to Remote Workstation Card connections:

- TLS_ECDHE_ECDSA_RSA_WITH_AES_256_GCM_SHA384

In-Session Encryption

Once a PCoIP session has been negotiated and the connection established, Tera2 PCoIP Zero Clients encrypt the session data using AES-256-GCM encryption algorithm. This algorithm secures all PCoIP communications during an active PCoIP session.

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 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 3.1.2 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 Client](#) [How 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

Frequently Asked Questions

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.

For connecting clients and hosts, a number of third-party connection brokers support the PCoIP technology. For VDI implementations, the View Connection Server broker is used to connect Tera2 PCoIP Zero Clients to VMware Horizon virtual desktops. You can also use the View Connection Server broker to connect PCoIP clients and host PCs.

DVI and DisplayPort Interfaces

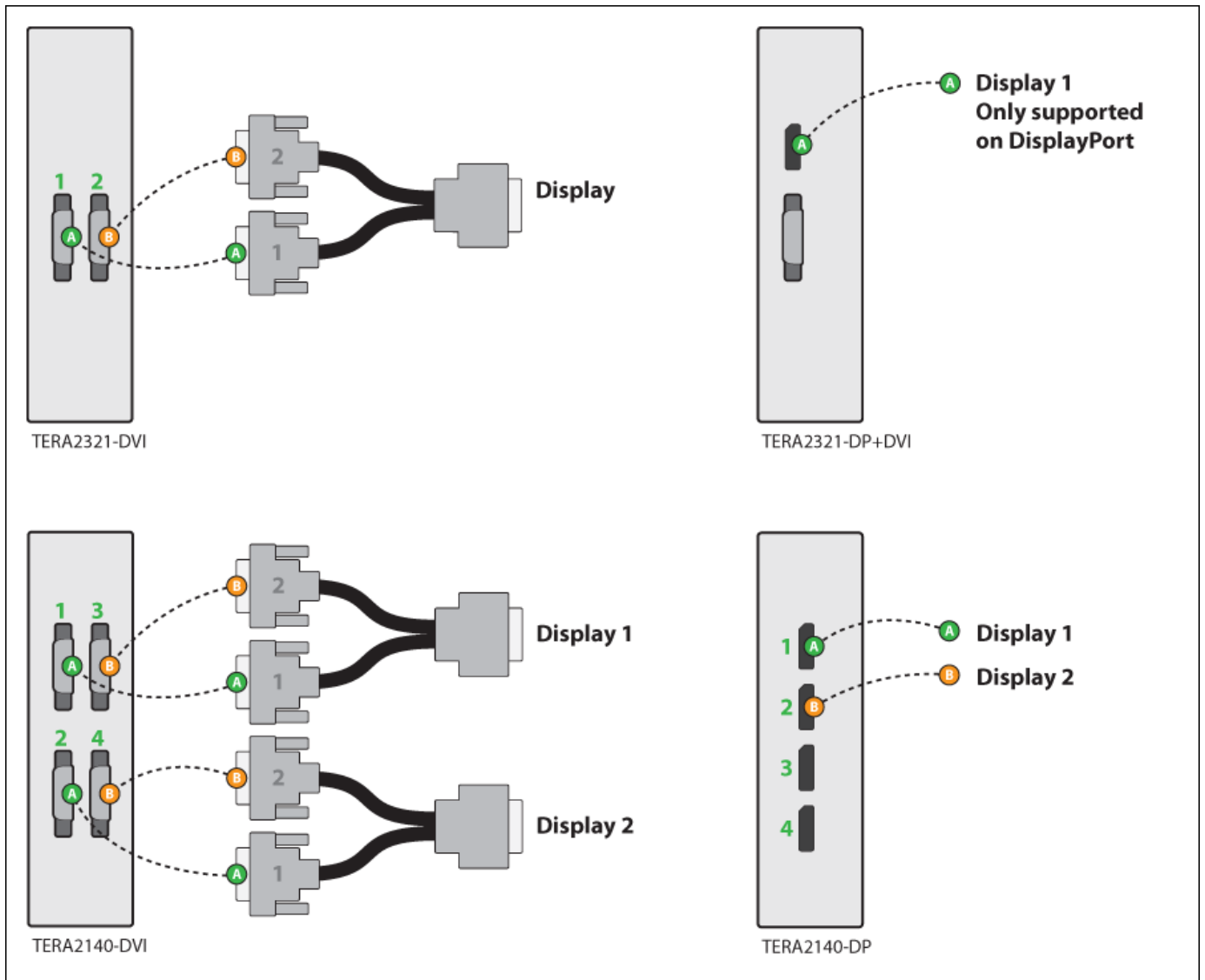
Tera2 PCoIP Zero Clients support both DVI and DisplayPort digital display interfaces. The following port options are available for these clients:

- 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 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 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).

DVI and DisplayPort Connectors for 2560x1600 Resolution

- 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 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 at www.teradici.com.

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.

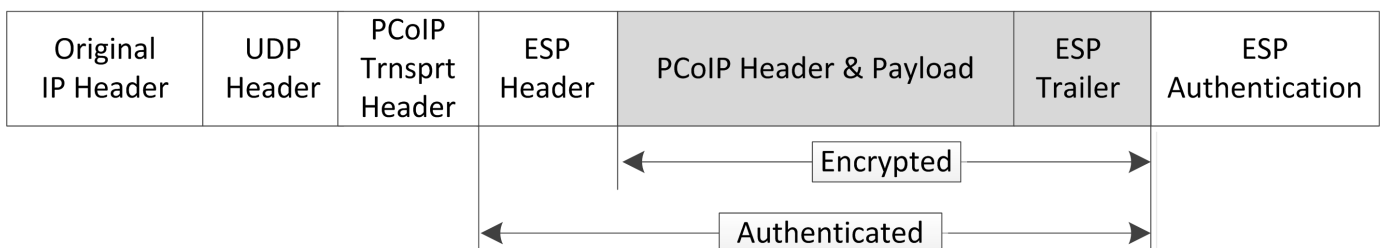
TCP/UDP port 4172 assigned to the PCoIP protocol

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.

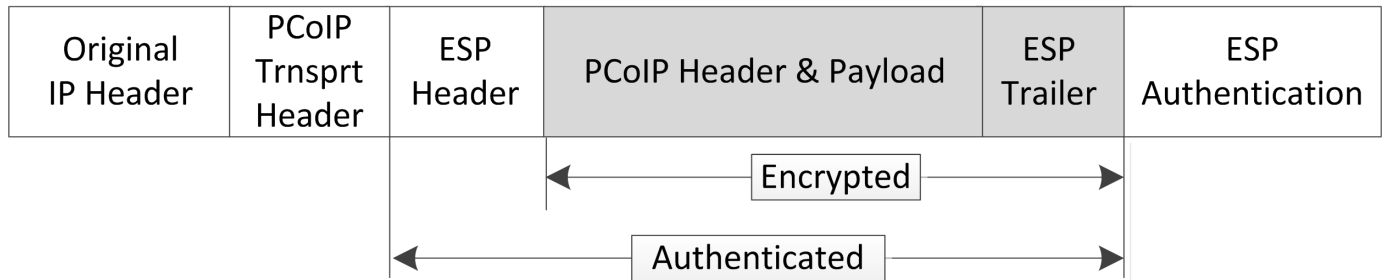
The UDP-encapsulated ESP packet format is illustrated in the following figure. This figure also shows the location of the PCoIP transport header in a UDP-encapsulated ESP packet.



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 at www.teradici.com.

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

PCoIP Connection Manager 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 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

PCoIP Connection Manager 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 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.

For complete details about PCoIP Hardware Accelerator, see the Teradici website at www.teradici.com.

Appendix A: Smart Cards

This appendix provides the requirements to support pre-session smart card authentication when connecting to VMware Horizon (View) now 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.

PCoIP zero clients support pre-session smart card authentication when connected to VMware View virtual desktops that meet the system configuration requirements listed below.

Remote Workstation Cards

Pre-session smart card authentication to remote workstations using PCoIP host cards is not supported at this time.

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.

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

Virtual Desktop Requirements

- 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 zero clients)
- Castles Technology EZM110CU (built into selected ClearCube zero clients)
- Castles Technology EZM110PU (built into selected ClearCube zero clients)
- Cherry SmartBoard keyboard
- Dell Smart Card USB keyboard SK3205
- Gemalto PC Twin HWP108765C
- Gemalto PC Twin HWP108760D
- Gemalto PC USB-SW
- HP KUS0133 Smart Card Keyboard
- Leadtek Alcor Reader
- OmniKey 3021
- OmniKey 3121

Known Smart Card Readers compatible with SC650/SIPR

- 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

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:

Tested Smartcard Models

Model	Specification and/or Applet	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
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

Notes:

1. Your card may be on the supported card list however the applet of the card may not be supported.
2. Windows 8 virtual machines require ActiveClient 7.0 or newer. The old version (e.g. 6.x) will install but will not work as expected.
3. 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 host 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

Appendix B: Tablets

PCoIP Zero Clients support locally terminating Wacom tablets when the PCoIP Zero Client is connecting to a PCoIP Remote Workstation Card installed in a Linux workstation that has PCoIP Host Software for Linux installed. Supported Wacom tablets require the correct firmware uploaded to the Zero Client as newer tablet models can be added to newer firmware releases. To ensure you have the most complete set of supported Wacom tablets, use the latest release of PCoIP Firmware.

In some networks users may notice a visible lag between the movement of the tablet stylus and the movement of the cursor. Using the the local tablet driver feature in the host software 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 [Features tab](#) .

Wacom tablets connected to PCoIP Zero Clients connecting to a PCoIP Remote Workstation Card installed in a Windows workstation, and tablets not listed in either of the supported tablets tables in this appendix will be bridged to the host PC.

Supported tablets

Each new firmware release may include support for newer tablets. Be sure to read the *release notes* of the zero client firmware being used to make sure your tablet is supported.

Supported tablets that use absolute co-ordinates while in-session and in the OSD

Description	Model	Product ID
Intuos Pro Medium	PTH-660	0x0357
Intuos Pro Large	PTH-860	0x0358

Supported tablets that use absolute co-ordinates while in-session and relative co-ordinates while in the OSD

Supported tablets that use absolute co-ordinates while in-session and relative co-ordinates while in the OSD

Supported tablets that use absolute co-ordinates while in-session and relative co-ordinates while in the OSD

Description	Model	Product ID
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		0x00C5
Cintiq 21UX	DTZ-2100	0x003F
Cintiq 21UX2	DTK-2100	0x00CC
Cintiq 22HD	DTK-2200	0x00FA
Cintiq 22HDT	DTH-2200 (pen)	0x005B
Cintiq 24HD	DTK-2400	0x00F4
Cintiq 24HD touch	DTH-2400	0x00F8
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

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.

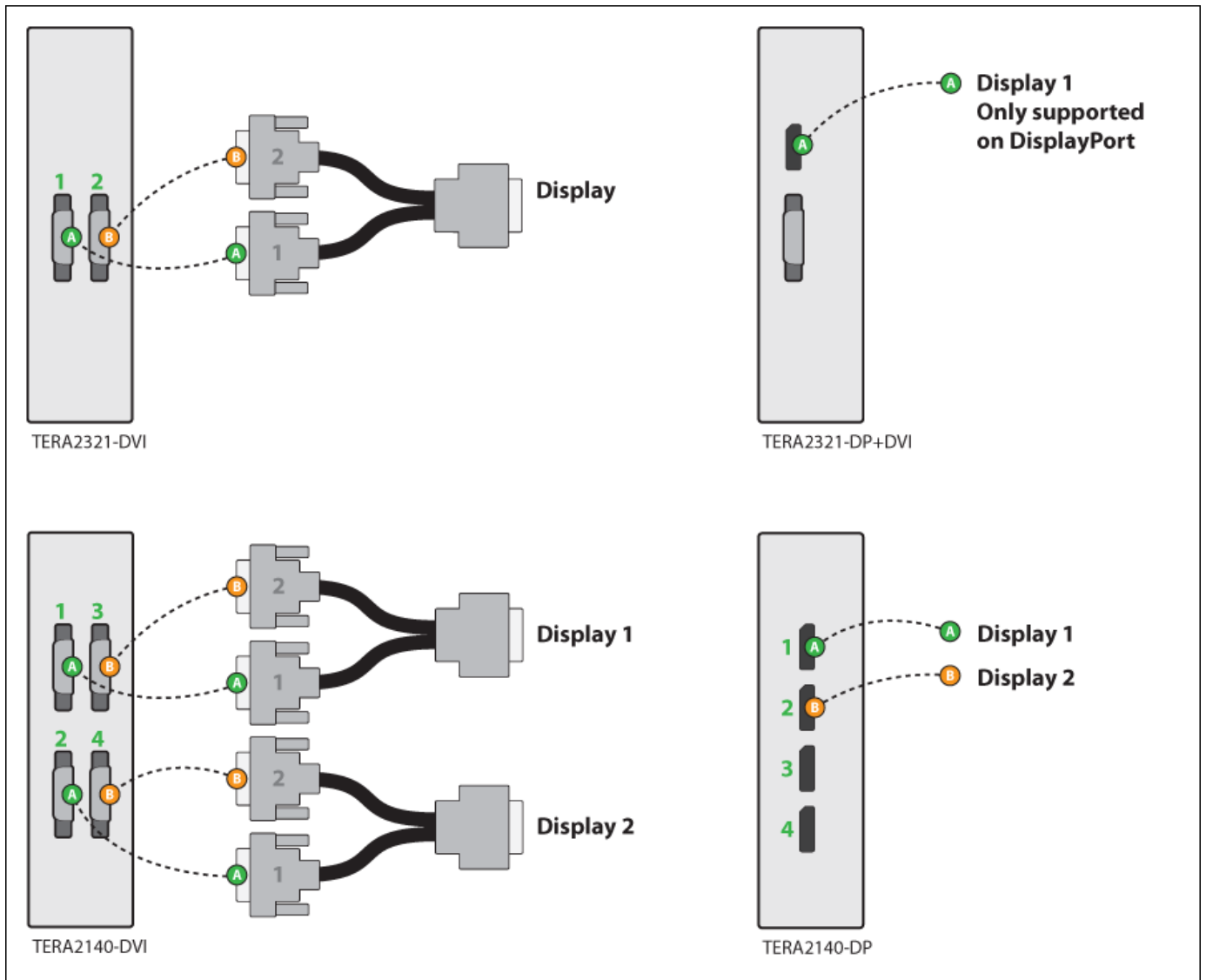
DIRECT CONNECT TO THE REMOTE WORKSTATION CARD

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 host 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 RESOLUTION MONITORS

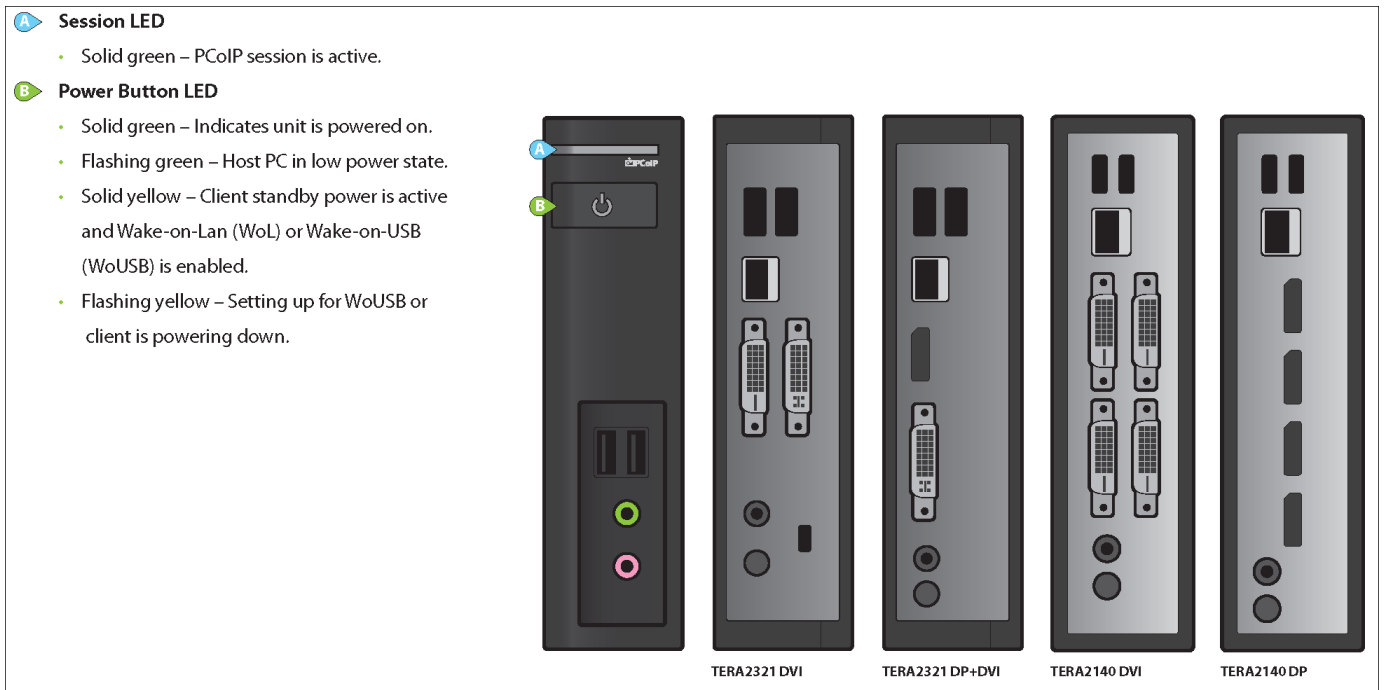


LED STATUS INDICATORS

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.



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 host 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 2560x1600

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 2560x1600
- 1-2 DisplayPort monitors up to 1920x1200 + 1 DisplayPort monitor up to 2560x1600

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

PCoIP Zero Client Firmware 6.3 Release Notes

Release Overview

PCoIP Zero Client Firmware 6.3.0 is a firmware release for PCoIP Zero Clients (not PCoIP Remote Workstation Cards).

This release is a feature release with functional changes and bug fixes over [release 6.2](#). These release notes provide a summary of key feature additions, compatibility notes, resolved issues, and known issues for this release.

Note: only All Access subscribers are eligible to receive this release.

What's New in Release 6.3

New Smart Cards for Horizon View

- SafeNet AT SC650 v3.2
- Entrust PIV 2.4.2R0
- Oberthur/IDEMIA Cosmo V8 ID-ONE PIV 2.4.0/2.4.1

Removed AES-128 in PCoIP session

PCoIP session can only be encrypted with AES-256

Low light interface

User interface can be made less bright, to accommodate low light environments.

Important Notes and Requirements

- Zero clients with firmware 5.x or 6.x can only be managed by PCoIP Management Console 2.0 or higher.

Release Downloads

- If you are upgrading your Tera2 firmware from a 4.x release:
 - Use PCoIP Management Console 1.10.3 through 1.10.8 **or** the the zero client's AWI to upgrade the zero client to firmware 5.0 or higher.
 - If you are upgrading directly to a 6.x release, you must upgrade from firmware version 4.7 or 4.8.
- This download includes an **.all** file for use by the Administrative Web Interface (AWI) and a **.pcoip** file for use by PCoIP Management Console 2.0 and higher.
- The **.pcoip** file contains zero client firmware 6.2.0 for PCoIP Zero Clients only.

Release Downloads

- [Zero Client Firmware 6.3.0](#)

Related Documents and Software

- [PCoIP® Zero Client Firmware 6.3 Administrators' Guide](#)
- [Remote Workstation Card Firmware 5.1 Administrators' Guide](#)
- [Remote Workstation Card Firmware 5.1 Release Notes](#)
- [PCoIP® Management Console 19.05.0 Administrators' Guide](#)
- [Open-source and third-party components](#)

Release History

Version	Date	Description
6.3.0 GA	May, 2019	General Availability
6.2.0 GA	February, 2019	General Availability
6.1.1 GA	November 22, 2018	General Availability bug fix and security update
6.1 GA	July 4, 2018	General Availability

Compatibility

Compatibility

Compatibility Notes	Workstation	VMware Horizon	Amazon WorkSpaces	Teradici Cloud Access Platform
Release 6.3.0 is verified with VMware Horizon 7.8 and 7.7. It is also compatible with one major release of Horizon prior to this. Other versions of Horizon may also be compatible, but will need to be verified in your specific deployment environment. VMware Horizon 6.2.1 is now the minimum release required to connect with zero clients on this firmware release.		X		
PCoIP Connection Manager for Amazon WorkSpaces 1.0.7 or higher is required in order to connect to Amazon WorkSpaces using the PCoIP Connection Manager session type.			X	
Management requires a compatible endpoint manager such as PCoIP Management Console release 2.0 or higher. However, PCoIP Management Console 3.2 or higher is recommended.				
While mixed firmware release operation is not generally supported, this firmware release has been tested to work with Remote Workstation Cards on Remote Workstation Card firmware 5.1.0.	X	X		
Release 6.3 is compatible with the Leostream Connection Broker version 8. It is not compatible with earlier versions of the Leostream Connection Broker. Note: After upgrading from PCoIP Zero Client Firmware 4.x to 5.0 or higher, the session connection type for the Zero Client must be changed to PCoIP Connection Manager, with the address of the Leostream Connection Broker. Also ensure the Leostream Connection Broker has had 'Enable TLSv1.1 protocol' enabled in the Connection Broker Security Options section of the Connection Broker > System > Settings page.	X	X		X
Supported browsers are Firefox, Chrome, and Microsoft Edge. Versions of the browsers tested are those that were available prior to release Web				

Resolved Issues

VMWare UAG with MFA connection issue has been resolved | 80406

Users can successfully connect when all of the following are enabled: * Unified Access Gateway (UAG) * View Disclaimer * Multi-Factor Authentication (MFA)

Known Issues

VMware pool names are blank if they are too long | 76282

The VMware pool names will be populated as blank if they exceed 65 characters.

Certificates with unreadable DNs are not logged | 75044

Certificates with unreadable Domain Names (DN) will not be logged if the firmware is unable to match any certificates against known CAs.

Stylus cannot wake up display. | 74801

If the display goes to sleep, the stylus on a Wacom tablet cannot be used to wake it up.

WORKAROUND

Use mouse or keyboard to wake up display.

VCS Communication error with SC650 BLADE and Horizon 7.5 | 72839

VCS Communication Error is encountered when an SC650 blade smartcard is used to authenticate with a VCS Horizon 7.5.0. This is not an issue with Horizon 7.4 or earlier.

WORKAROUND

Recommendation is to not upgrade to Horizon 7.5 at this time.

Zero client in Auto Detect crashes upon receipt of invalid certificate chain | 71136

The zero client may crash with the error: {quote}0d,00:00:00.00> LVL:1 RC: 0 MGMT_SYS :***
CRITICAL ERROR CONTEXT DUMP ***

0d,00:00:00.00> LVL:1 RC: 0 MGMT_SYS :Reset cause: SOFTWARE {quote} when it is is configured for either one of the VMware Horizon connection types, or Auto Detect, and is presented with an invalid certificate chain (such as one containing duplicate entries).

WORKAROUND

Verify and correct the certificate chain.

Mouse and keyboard briefly unresponsive after session launch with Wacom tablet connected | 71111

Mouse and keyboard devices may be unresponsive when launching a session from the Zero Client if a PTH-660 or PTH-860 Wacom tablet is connected. The mouse and keyboard will become responsive after a few seconds.

Internet Explorer 11 does not trust the Administrative Web Interface certificate | 71084

Internet Explorer 11 does not trust the Administrative Web Interface certificate if the AWI is accessed via IP address (it will trust the certificate when using the FQDN).

802.1x not disabled after all certificates removed | 70037

Removing the certificates set to be used for 802.1x will not disable 802.1x.

WORKAROUND

After removing the 802.1x certificates, manually disable 802.1x.

Certificates with long subject names populated using the Cyrillic alphabet cannot be parsed by the zero client. | 68434

Certificates with long subject names populated using the Cyrillic alphabet cannot be parsed by the zero client.

WORKAROUND

Use a shorter subject name in the certificate.

USB Isochronous devices need to be on a root port in order to work. | 68340

USB Isochronous devices (such as audio or video devices) need to be on a root port in order to work.

WORKAROUND

Availability of the root port varies from manufacturer to manufacturer, and they should be engaged to determine if they have a root port available on their zero client model. If available, use the root port for Isochronous device types.

Zero Client cannot establish a PCoIP session after Qualys scan | 65940

Zero Client is unable to establish a PCoIP session after some Qualys scans.

WORKAROUND

Disable the Administrative Web Interface will solve this issue.

For all security conscious customers, we recommend disabling the Administrative Web Interface.

Zero client attempts to resume session when Amazon WorkSpaces host initiates disconnect | 65214

Amazon WorkSpaces can support Ctrl+Alt+F12 as a means to cause the connection to disconnect. If the zero client is configured to have Enable Session Disconnect HotKey turned off, then when the user enters Ctrl+Alt+F12, the Amazon WorkSpace will catch the command and

initiate a disconnect. When this disconnect occurs the zero client will attempt to resume the session.

WORKAROUND

Ensure Enable Session Disconnect Hotkey is set to on for the zero client so that the zero client manages the disconnect.

Incorrect error presented when certificate uploaded via AWI | 65165

When uploading a certificate via AWI, even though the certificate is uploaded into the certificate store the following error may be displayed: Error. The upload did not complete. Please try again.

WORKAROUND

Verify the certificate is in the certificate store. If it is, ignore the error.

Zero clients may reboot if a Nessus scan is performed while SNMP is enabled. | 62970

Zero clients may reboot if a Nessus scan is performed while SNMP is enabled.

WORKAROUND

Disable SNMP on the zero client.

Setting timezone to UTC in Management Console results in UTC+0 Europe/Dublin | 62959

If the Management Console is configured to push the timezone setting of (UTC+0:00) UTC to the zero client, the zero client will set itself to (UTC+0:00) Europe/Dublin or (UTC+0:00) Europe/London. This timezone makes use of daylight savings time. There is no option in the zero client for (UTC+0:00) UTC.

WORKAROUND

There is no option in the zero client for (UTC+0:00) UTC. However, if UTC+0:00 without daylight savings is required, then (UTC+0:00) Atlantic/Reykjavik can be used instead.

Press power button once to turn on the client

SIPR token authentication may fail with multiple certificates on card | 62201

The zero client will fail to complete SIPR token smart card authentication against VMware Horizon View when the smart card contains more than two certificates.

WORKAROUND

Ensure that the card has no more than two certificates.

Change in button timing for entering manual recovery | 61350

Beginning with firmware 5.2.1, the power button sequence to boot a zero client from powered down into the recovery image is:

Press power button once to turn on the client

Wait for one second

Triple tap power button

Zero client boots into the recovery image

From firmware 5.0.0 to 5.2.0, it was possible to triple tap the power button immediately after turning on the zero client. This is no longer supported.

Mouse cursor briefly unresponsive after zero client reboot | 60568

The On-Screen Display's mouse cursor may be unresponsive for a few seconds after a zero client reboot when a web browser is connected to the zero client's Administrative Web Interface.

Zero Client is unable to use IPv6 VMware Horizon View when DHCPv6 is not available | 47650

If the zero client is configured for IPv6, and it cannot connect a DHCPv6 server, it will be unable to connect to a desktop when brokered by an IPv6 VMware Horizon View Connection Server. The zero client displays the message 'CONFIGURATION_ERROR - IPv6 capability required: Your VMware Horizon View Client addressing configuration is not compatible with this View Server..'

Security scanners may report zero client to be susceptible to CVE-2004-0230 | 45883

Security scanners may report that the zero client is susceptible to CVE-2004-0230. This CVE exists in TCP stacks in devices that implement the Border Gateway Protocol. While this is a significant issue for routers that implement the Border Gateway Protocol, it is not a significant issue for zero clients.

Mouse wheel problem occurs with Belkin Advanced Secure Keyboard/Mouse Switch | 42387

Mouse wheel scroll-down does not work while in a PCoIP session. This occurs when the mouse is connected to a zero client through a Belkin Advanced Secure Keyboard/Mouse (KM) Switch. This problem has been observed while using KM models F1DN102K, F1DN104K, and F1DN108K.

WORKAROUND

On Tera2 Zero Clients, bridge the KM and enable the *Force Local Cursor Visible* on the zero client *Configuration > USB Administrative Web Interface*.

Zero client fails to resolve FQDN with a label that starts or ends with an underscore | 40824

A zero client will not resolve an FQDN that begins or ends with the underscore character (for example, `_myhost.teradici.local`).

Restrict Proximity Card setting does not work with VMware Horizon RDSH | 40754

The Restrict Proximity Card setting does not work with VMware Horizon RDSH sessions when set to disabled.

Enumeration failures with Western Digital portable hard drives | 39419

Western Digital Passport external portable hard drives connected to a zero client internal hub may fail to enumerate.

WORKAROUND

Connect the drive to a zero client root hub port, or connect the drive to an external hub that is connected to the zero client, then restart the PCoIP session and disconnect/reconnect the drive.

Manual IPv6 gateway address is overwritten on reset | 34901

Although the IPv6 Gateway address is displayed as an editable field on the zero client Administrative Web Interface (AWI), changes to this field are not respected by the zero client firmware. Instead, the IPv6 gateway is determined using IPv6 Router Advertisement.

Zero client AWI cannot be accessed when IPv6 Link Local Address is entered in the IPv6 Manual address field | 33783

Configuring a zero client in IPv6 mode to manual addresses and setting the IPv6 Manual Address to the same value as the Link Local Address will make the zero client Administrative Web Interface (AWI) unreachable.

WORKAROUND

Use the On-Screen Display (OSD) to reconfigure the IPv6 address settings.

Evoluent VerticalMouse 4 does not work when connected behind a hub during active session | 33706

The Evoluent VerticalMouse 4 device does not work if the device is bridged and the user connects the device to a zero client behind a hub (external or built-in hub port) while a session is active.

WORKAROUND

Avoid plugging the device into a hub port while a session is active or connect the device to a zero client root port. Alternatively, disconnect and reconnect the session after plugging the mouse into a zero client behind a hub.

Elo Touch monitor may lose calibration in OSD after used in bridged mode with certain Elo Multi-Touch drivers | 30150

An Elo Touch monitor connected to a zero client may lose its calibration settings and be unstable in the On-Screen Display (OSD) when the zero client connects to a PCoIP host running certain versions of the Elo Multi-Touch driver, and when the monitor is calibrated using Elo Multi-Touch driver on the host.

WORKAROUND

Use version 5.5.3 of the Elo Multi-Touch driver. This issue has not been observed with this driver version.

RDR-7L82AKU smart card reader does not work with OneSign 4.9 SP1 HF11 and newer | 22448

RFIDeas RDR-7L82AKU proximity card readers do not detect cards after logging in to a virtual desktop running Imprivata OneSign 4.9 SP1 HF11 or newer.

WORKAROUND

Revert Imprivata OneSign installation to a version older than 4.9 SP1 HF11.

Gemalto IDCore 3020 smart cards is missing correct driver in Windows 7 | 22315

By default, Gemalto IDCore 3020 smart cards work in pre-session. However, the card does not work while in-session for Windows 7 virtual desktops.

WORKAROUND

Install the correct driver from a default Windows 7 installation: 1. From the zero client administrative web interface, bridge the smart card reader. 2. Without the smart card inserted, log in to the virtual desktop with username/password. 3. Insert the smart card. Windows 7 should

recognize the smart card and reader and automatically install the correct drivers. 4. Log off Windows to disconnect the session. 5. From the zero client administrative web interface, remove the bridge configuration for the smart card reader. 6. Log in with the smart card. The smart card should be fully accessible.

OneSign cannot authenticate after changing Session Connection Type | 21653

After changing a zero client's Session Connection Type from View Connection Server + Kiosk to View Connection Server + OneSign, the Zero Client is unable to negotiate a PCoIP session with VMware View using OneSign authentication.

WORKAROUND

Restart the zero client.

After display is turned off, screen does not wake up by pushing zero client button | 21484

When the On-Screen Display (OSD) Screensaver timeout expires, it will turn off the display after the end of a PCoIP session brokered by a PCoIP Connection Manager. Clicking the zero client's physical button does not wake the display.

OSD cursor briefly stops responding to mouse input | 21382

The On-Screen Display (OSD) cursor stops responding to mouse input for a few seconds after pressing the Apply button on the AWI USB Permissions page, or while loading the AWI Attached Devices page. It will behave as expected shortly after.

Disconnecting a session with auto-reconnect enabled causes an alert dialog | 21082

With the auto-reconnect feature enabled, users may see an alert dialog briefly on screen before the PCoIP session is reconnected. The message shown is "Unable to connect (0x1001). Please contact your IT administrator." This message can be safely ignored.

Switching between DVI and DisplayPort connectors may cause screen to go blank on HP Z27i displays | 19353

HP Z27i displays connected to a zero client's DisplayPort connectors may not show the remote desktop content when the zero client starts a PCoIP session to a workstation access card, and the card's previous session was from a zero client with displays attached to its DVI ports.

Temporary IPv6 addressing causes failure when connecting zero clients to any soft host | 15923

Zero clients cannot establish a connection to any soft host that has temporary IPv6 addressing enabled.