Tera2 PCoIP® Zero Client Firmware 4.x and Remote Workstation Card Firmware 4.9

Administrators' Guide

teradici®

Teradici Corporation

#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada

phone +1.604.451.5800 fax +1.604.451.5818

www.teradici.com

Contents

About This Guide

This section describes this document's intended readers and establishes conventions.

Who Should Read This Guide?

This guide is intended for systems administrators who wish to install, configure, deploy, and manage the PCoIP Remote Workstation Card in conjunction with the Tera2 PCoIP Zero Client. Note that all instances of *PCoIP Zero Client* or *zero client* in this document pertain to the Tera2 PCoIP Zero Client firmware 4.x and lower.

For Tera2 PCoIP Zero Client version 5.0.0 and higher, consult the *Tera2 PCoIP Zero Client Administrators' Guide*.

The Teradici Glossary

While working with Teradici technology and reading our documentation, you may encounter terms or abbreviations you're unfamiliar with. Some of these terms, particularly acronyms, are similar and can be confusing.

To help alleviate this confusion, Teradici maintains an online glossary covering both general IT terminology and Teradici-specific phrases and acronyms. The glossary is available at the following URL: https://www.teradici.com/web-help/Glossary/default.htm.

Notes Used in This Guide

Note
Notes include useful information and general advice pertaining to a topic. They may also include important, but not critical, configuration notes.

Caution
Cautions indicate information with a higher level of importance than a regular note. These typically call out configuration conditions that could cause a system to fail.

Warning
Warnings are critically important notes. Warnings can include critical configuration settings, or observations that have security or system health implications.

Tip
Tips are shortcuts or convenience methods that will help you work faster. They may also point out ways to increase efficiency or make use of additional functionality.

Internet
Internet notes generally refer to Internet connectivity requirements or cloud opportunities.

Info
These notes include useful information related to a topic, and may include links to other items.

Related Information
External Resource notes contain links to information on non-Teradici components, including websites of third-party integrations.

Text Conventions

This guide uses several common text conventions to help you easily understand the content, as follows:

Bold text	Used to indicate system objects that you will interact with, such as a menu item or a submit button.
Italic text	Used to indicate the following conventions: • A system object that is present in an interface, but that you do not directly interact with. • A document cross-reference or hyperlink
`Plain Monospace Text`	Indicates file paths or file names. • `\Program Files (x86)\Teradici\PCoIP Agent` • `/etc/pcoipagent/pcoip-agent.conf`
`Red Monospace Text`	Indicates code fragments, keys, variables, and parameters. Examples: • This is the HTML5 `<code>` element. • Set the `pcoip.event_filter_mode` variable.
`Inverse Monospace text`	Used to indicate keyboard buttons, like `Ctrl` or `Shift`.
`Formatted text`	Used to indicate code blocks, including command line interactions.

System Architecture Symbols

In system architecture diagrams, PCoIP components are placed on tiles indicating whether they are deployed in a data center, in the cloud, or can be in either environment:
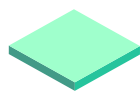
	Data Center component Located in an on-premesis data center		**Cloud component** Located in the cloud		**Hybrid component** Can be located in an on-premesis data center, the cloud, or both
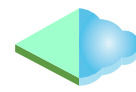
Communications between components are shown using these symbols:
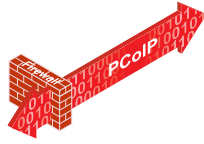
An active PCoIP connection through a firewall.

PCoIP connections become active after a session is negotiated between a host and client and a license is validated.

This symbol shows a PCoIP session traversing a firewall, with no VPN.
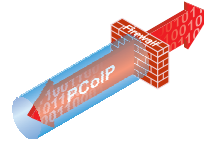
An active PCoIP connection on a VPN and through a firewall.

PCoIP connections become active after a session is negotiated between a host and client and a license is validated.

This symbol shows a PCoIP session traversing a firewall and using a VPN to secure the WAN side of the session.

Introduction

Welcome to Teradici's Tera2 PCoIP® Zero Client and Remote Workstation Card Administrators' Guide. This guide explains how to configure PCoIP device firmware so you can access and manage the hosts and zero clients in your PCoIP deployment. It comprises the following main sections:

- **What's New**: This section explains the new features for each firmware release, and contains links to topics that provide more information about these features.

- **Zero Clients**: This section contains quick start instructions for first time users on how to connect your zero client.

- **Remote Workstation Cards**: This section contains quick start instructions for first time users on how to connect your PCoIP Remote Workstation Card.

- **PCoIP Management Tools**: This section describes how to access and use the following PCoIP management tools:

  - Management Console (MC): The MC lets you centrally control and manage the devices in your PCoIP deployment. This help system explains how to configure a profile (a collection of device configuration settings), which you can then assign to a specific PCoIP group (a set of one or more hosts or clients). The MC is the best tool for medium to large deployments, and is often used in conjunction with a connection broker. For further details, see About the MC.

  - Administrative Web Interface (AWI): The AWI lets you use an Internet browser to remotely access and configure a specific client or host. For further details, see About the AWI.

  - On Screen Display (OSD): The OSD is the graphical user interface (GUI) embedded within a client. It is used to connect the client to a virtual desktop or to a remote workstation card. It is also used to configure the client, and has a subset of the configuration parameters available in the MC and AWI. For further details, see About the OSD.

- **PCoIP Deployment Scenarios**: This section lists the types of connections you can make and the prerequisites for each session connection type. It also describes the most common ways to deploy the hosts and clients in your PCoIP network. Configuration steps are included for each scenario, with links to topics in the GUI Reference where you can find detailed information. The scenarios are the best place to start when configuring a new deployment.

- **GUI Reference**: This section is a detailed reference that describes each configuration parameter that appears in the MC, AWI, and OSD pages. You can use this reference when configuring a device profile using the MC, or when configuring a single device using the AWI or OSD. The GUI Reference is

organized by the categories listed in the MC's **Manage Profiles** page, but also has special sections for AWI and OSD menus that do not corresponding pages in the MC.

- **'How To' Topics**: This section contains procedures for common configuration tasks.
- **Technology Reference**: This section contains definitions for some of the terminology used in the help system.

What's New in Tera2 PCoIP Zero Client Firmware 4.8.x

PCoIP firmware 4.8 is a release for Tera2 Zero Clients only. This firmware version and its subsequent releases contains the following Tera2 Zero Client features. For the latest features and updates, consult the particular version's release notes.

Firmware 4.8 and Subsequent Release Features

Key Release Details	Supported Products	Platforms	Interfaces
CounterPath Bria softphone This release adds Amazon WorkSpaces support to the CounterPath Bria softphone solution. You can enable Bria softphone support via the zero client's Unified Communications (UC) setting. For more information, see Zero Client–to–Bria Softphone Caller Endpoint Prerequisites, MC: Unified Communications, and AWI Tera2 Client: Unified Communications.	Tera2 zero clients	AWS, Horizon VDI	AWI, MC
VMware Horizon 6 RDS-hosted application delivery Zero clients now support VMware Horizon 6 application remoting based on Microsoft Remote Desktop Services (RDS). To configure zero clients to access VMware Horizon streamed applications, select the new **Enable RDS Application Access** option on the **View Connection Server > Session** pages. Note: Applications open in full-screen mode, but can be re-sized once users are in session. For an example, see AWI Client: View Connection Server Session Settings > Advanced Options > Enable RDS Application Access.	Tera2 zero clients	Horizon RDSH	AWI, OSD, MC

Key Release Details	Supported Products	Platforms	Interfaces
Improved CounterPath Bria softphone call handling You can now enable the inbound ringer audio for the CounterPath Bria softphone to play on an external speaker as well as your headset. When this feature is enabled, all VM audio output is sent to both the speaker and the headset. For details, see the **Dual Audio Output Mode** parameter in MC: Audio Permissions and the **Enable Dual Audio Output** parameter in AWI Tera2 Client: Audio Settings and OSD Tera2: Audio Settings.	Tera2 zero clients	AWS, Horizon VDI	AWI, OSD, MC
New Configuration > USB menu A new **Configuration > USB** menu in the AWI allows you to configure settings for USB devices that are attached to zero client ports. The **Enable EHCI** setting is moved to this location (from the **Permissions > USB** menu), and a new **Force Local Cursor Visible** setting has been added. When this feature is enabled, the 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. You can configure these options in the MC from the MC: Peripheral Settings page. In the AWI you can configure them from the new AWI Tera2 Client: USB Settings page.	Tera2 zero clients	all	AWI, MC
Parameter name change The **Desktop Name to Select** parameter on the **Session > View Connection Server** pages has been changed to **Pool Name To Select**. For an example, see AWI Client: View Connection Server Session Settings > Advanced Options > Pool Name to Select.	Tera2 zero clients	Horizon VDI, Horizon DaaS, Horizon RDSH	AWI, MC, OSD
Smart card insertion auto-connect When not in session, inserting a smart card automatically initiates communication with the connection broker. This is equivalent to pressing the **Connect** button on the OSD.	Tera2 zero clients	Horizon VDI, Horizon RDSH	

Key Release Details	Supported Products	Platforms	Interfaces
OneSign domain name selection The last used OneSign domain name will remain at the top of the drop-down list on the Session > View Connection Server + Imprivata OneSign page. For deployments with multiple OneSign domain names, users will be able to quickly select a frequently used logon domain.	Tera2 zero clients	Horizon VDI	AWI, OSD
Failover VCS address for Imprivata OneSign environments This feature allows administrators to configure a **Direct to View** link on zero clients configured for **View Connection Server + Imprivata OneSign** mode. When users click the link, the current OneSign connection or authentication flow is cancelled and a Horizon View authentication flow starts instead. This feature lets OneSign zero client users access their View desktops when the OneSign infrastructure is unavailable. For details, see AWI Client: View Connection Server + Imprivata OneSign Session Settings > Direct To View Address and MC: View Connection Server + Imprivata OneSign Session Settings > OneSign Direct To View Address.	Tera2 zero clients	Horizon VDI	AWI, MC
Buypass Smartcard support The zero client now supports Buypass Smartcards.	Tera2 zero clients	Horizon VDI, Horizon RDSH	
Gemalto IDCore 3020 Smartcard support The zero client now supports the Gemalto IDCore 3020 Smartcard.	Tera2 zero clients	Horizon VDI, Horizon RDSH	

Key Release Details	Supported Products	Platforms	Interfaces
Updated security ciphers for session negotiation SCEP certificate requests now ask for SHA-256 certificates instead of SHA-1 certificates. The list of ciphers used for PCoIP session negotiation is expanded to include several ciphers that use SHA-256 and SHA-384. In addition, the PCoIP firmware now has a new session negotiation security level called **Disable SHA-1**. When this mode is selected, all TLS ciphers that use SHA-1 are disabled. Note: In release 4.8.0, the updated security cipher features are supported on Tera2 zero clients only. Both the client and host endpoints must support the expanded cipher list in order to use a non-SHA-1 cipher. The Session Negotiation Cipher parameter is located on all AWI *Configuration > Session* pages. For an example, see AWI Client: View Connection Server Session Settings > Advanced Options > Session Negotiation Cipher.	Tera2 zero clients	Horizon VDI, Horizon RDSH	AWI
SSLv3 no longer supported To increase security, SSLv3 is no longer supported. The minimum TLS version used for brokering, session negotiation, management, and the AWI is TLS 1.0.	Tera2 zero clients	all	

What's New in Remote Workstation Card Firmware 4.9

PCoIP Remote Workstation Card firmware 4.9 is a firmware release for Tera2 Remote Workstation Cards only. This release includes the following security improvements.

AWI Update to SHA-256 Certificate

The certificate for the administrative web interface (AWI) has been updated to SHA-256.

No support for TLS 1.0 web browser

TLS 1.0 web browser connections are no longer permitted.

Session security mode improvements

Session security mode has been improved as follows:

- **TLS Security Mode:** This setting has two options available.

    - **Suite B**: This setting has not changed in this release.
    - **Maximum Compatibility**: This setting allows use of cipher suites used by older PCoIP Remote Workstation Cards and clients. Supported ciphers for maximum compatibility are listed next, by their protocol and names: 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

- **Blacklisted Cipher Suites:** Enables an administrator to select cipher suites (by protocol name) that should not be used. This setting should be used when security advisories are issued against specific suites.

Upgrade Instructions

The upgrade instructions depend on your Tera2 Remote Workstation platform, as shown below.

> **ℹ Info: Where to find the latest PCoIP software and firmware**
> You can download the latest PCoIP software and firmware from the
> Teradici Support Site.

Windows Platforms

Upgrade your Remote Workstation Card to firmware version **4.9**.

Linux Platforms

1. Upgrade your Remote Workstation Card to firmware version **4.9**. This provides security and stability fixes for remote workstations connected to a Tera2 Zero Client.

2. If you are running Red Hat Enterprise Linux (RHEL) 7.1 or CentOS 7.1 install version **4.9** of the PCoIP Host Software for Linux on your workstation.

3. If you are connecting your workstation to Tera2 PCoIP Zero Clients with an attached Wacom tablet, upgrade your Tera2 PCoIP Zero Client firmware to version **4.8.2-p90**. This is required to maintain local cursor support on the zero client side in conjunction with firmware 4.9 for the Remote Workstation Card.

> **ℹ Info: About patch release 4.8.2-p90**
> Tera2 PCoIP Zero Client firmware 4.8.2-p90 is a patch update to Tera2 PCoIP Zero Client firmware 4.8.2 that adds support for Wacom tablets.
> Get release 4.8.2-p90 by submitting a ticket through the Teradici Support Center.

Tera2 Zero Clients

Configuring a Tera2 Zero Client

Tera2 PCoIP Zero Clients are secure client devices that allow users to connect to a variety of endpoints over a local or wide area IP network. For example, you can use zero clients to connect to the following endpoints:

- PCoIP Remote Workstation Cards
- PCoIP Workstation Access Software
- Amazon WorkSpaces desktops
- VMware Horizon View or VMware Horizon DaaS desktops
- Bria softphone caller endpoints via CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on a VMware Horizon View virtual desktop

Setting up the Zero Client

For detailed instructions on how to physically set up a zero client and connect it to USB devices, monitors, and the network, please see "Tera2 PCoIP® Zero Client Quick Start Guide" (TER1207007) in the Teradici Support Center. This guide has detailed instructions for each step of the installation process.

Static Fallback IP Address

If your network does not support DHCP, the card will use its static fallback IP address. This address is set by the card's manufacturer and can be located in the "**IN OFD:**" (optional factory defaults) section of the zero client's event log, as shown in the example below:

```
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 MC's **Network Settings** page (see Static Fallback IP Address). When set from the MC, the event log will display this address as "**IN FLASH:**" rather than "**IN OFD:**", as shown in the example below:

```
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
```

Note: If you reset the zero client, the static fallback IP address will revert to the factory default, even when this address has been set by the MC.

Establishing a PCoIP Session

Note: Zero clients are pre-configured to connect directly to a PCoIP Remote Workstation Card, but you can easily configure them for any session connection type.

After successfully completing the installation steps outlined in "Tera2 PCoIP® Zero Client Quick Start Guide" (TER1207007), the zero client will be powered on and ready to use. The next step is to initiate a PCoIP session. The easiest way to get started is to connect to a remote workstation card using SLP host discovery.

Note: SLP host discovery requires the 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 remote workstation card so you can select it from the list of available hosts. In addition, the remote workstation card must be configured to accept any peer or to accept the specific MAC address of the zero client. You can configure this from the host AWI Configuration > Session > Direct from Client page.

To connect to a remote workstation card using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the zero client's OSD, select the Direct to Host + SLP Host Discovery connection type, and then click **OK**.

2. Click the **Connect** button.

3. When the **Discovered Hosts** screen appears with a list of available hosts, select the desired one by its IP/MAC address pair, and then click **OK**.

4. If prompted, enter your user name and password, and then click **OK**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

To establish a session using another session connection type:

1. From the zero client's OSD, select the **Options > Configuration > Session** menu.

2. From the **Connection Type** drop-down list, select the desired connection type:

   - Direct to Host
   - PCoIP Connection Manager (Tera2 only)
   - PCoIP Connection Manager + Auto-Logon (Tera2 only)
   - View Connection Server
   - View Connection Server + Auto-Logon

- View Connection Server + Kiosk
- View Connection Server + Imprivata OneSign
- Connection Management Interface

3. After entering the required information, click **OK** on the **Session** page.

4. Click the **Connect** button.

5. If prompted, enter your user name and password.

6. If you are using a brokered connection and have more than one entitlement, select the desired one, and then click **Connect**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

Other Useful Links

The following topics provide more information about connecting zero clients and remote workstation cards.

- PCoIP Endpoints: Gives an overview of the PCoIP clients and hosts you can deploy in your network.
- Connection Prerequisites: Explains the conditions that must be in place before connecting PCoIP clients and hosts.
- **Common LAN Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts from within a LAN.

  - Zero Client to Remote Workstation Card (LAN)
  - Zero Client to Remote Workstation Card via View Connection Server (LAN)
  - Zero Client to Virtual Desktop via View Connection Server (LAN)
- **Common Remote Access Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts remotely.

  - Zero Client to Remote Workstation Card (WAN)
  - Zero Client to Remote Workstation Card via Hardware VPN (WAN)
  - Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)
  - Zero Client to Remote Workstation Card via View Security Server (WAN)
  - Zero Client to Virtual Desktop via View Security Server (WAN)

Remote Workstation Cards

Configuring a Remote Workstation Card

Teradici's PCoIP Remote Workstation Card is a small add-in card that can be integrated into tower workstations, rack mount workstations, computer blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full workstation environment. This information is then communicated in real time over an IP network to the user's PCoIP client.

Installing a Remote Workstation Card

Important! The remote workstation's card's MAC address is located on a sticker on the card. It is important to write down this address before installing the card in the workstation. see KB 15134-1348 in the Teradici Support Site for additional information.

For detailed instructions on how to physically install the card, please see *PCoIP® Remote Workstation Card Quick Start Guide* in the Teradici Support Center. This guide has detailed instructions for each step of the installation process.

Important: When connecting the graphics card to the remote workstation card with the provided cables, always connect the lowest numbered connector on the graphics card to the lowest numbered connector on the remote workstation card, and continue upward.

Some graphics cards have both DVI and DisplayPort connectors. To support 2560x1600 resolution when connecting these graphics cards, connect the lowest numbered *DisplayPort* connector on the graphics card to the lowest number connector on the remote workstation card. Connecting the DVI connector on the graphics card to the remote workstation card will limit you to 1920x1200.

For complete details about the resolutions supported by different connectors and cables, see KB 15134-1607 in the Teradici Support Site.

Establishing a PCoIP Session to a Remote Workstation Card from a Zero Client

Note: For information on how to connect using a Teradici PCoIP® Software Client, see *Teradici PCoIP® Software Clients 1.9 Administrators' Guide*.

After successfully completing the installation steps outlined in PCoIP® Remote Workstation Card Quick Start Guide, the card will be connected to the network and the workstation powered on. The next step is to initiate a PCoIP session from a zero client using SLP host discovery.

Note: SLP host discovery requires the 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 remote workstation card so you can select it from the list of available hosts. In addition, the remote workstation card must be configured to accept any peer or to accept the specific MAC address of the zero client. You can configure this from the host AWI Configuration > Session > Direct from Client page.

By default, DHCP is enabled on the remote workstation card to allow your DHCP server to assign an IP address. If your network does not support DHCP, the card's default IP address will be 192.168.1.100.

To connect to a remote workstation card using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the zero client's OSD, select the Direct to Host + SLP Host Discovery connection type, and then click **OK**.
2. Click the **Connect** button.
3. When the **Discovered Hosts** screen appears with a list of available hosts, select the desired one by its IP/MAC address pair, and then click **OK**.
4. If prompted, enter your user name and password, and then click **OK**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

Installing the PCoIP Host Software

Optionally, you can also install the PCoIP host software package on the workstation to allow you to manage the card directly from the PCoIP host software UI on the workstation.

Note: Before installing this package on the workstation, you must first log in to the remote workstation card from the AWI, and enable the host driver function in the firmware from the **Configuration > Host Driver Function** menu.

For detailed instructions on how to install the PCoIP host software, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) or "PCoIP® Host Software for Linux User Guide" (TER1104006) in the Teradici Support Center.

Other Useful Links

The following topics provide more information about connecting zero clients and remote workstation cards.

- PCoIP Endpoints: Gives an overview of the PCoIP clients and hosts you can deploy in your network.

- [Connection Prerequisites](#): Explains the conditions that must be in place before connecting PCoIP clients and hosts.
- **Common LAN Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts from within a LAN.

  - [Zero Client to Remote Workstation Card (LAN)](#)
  - [Zero Client to Remote Workstation Card via View Connection Server (LAN)](#)
  - [Zero Client to Virtual Desktop via View Connection Server (LAN)](#)

- **Common Remote Access Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts remotely.

  - [Zero Client to Remote Workstation Card (WAN)](#)
  - [Zero Client to Remote Workstation Card via Hardware VPN (WAN)](#)
  - [Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)](#)
  - [Zero Client to Remote Workstation Card via View Security Server (WAN)](#)
  - [Zero Client to Virtual Desktop via View Security Server (WAN)](#)

PCoIP Management Tools

PCoIP Management Console

About the MC

The PCoIP Management Console (MC) lets you centrally manage the devices in your PCoIP deployment. It is packaged as a VMware® virtual machine (VM), running on VMware Player. You can use the MC to view status information for devices, create groups and profiles, configure a profile (a collection of configuration settings) that you can apply to a group (one or more devices that require the same configuration), upload certificates and firmware to devices, control the power settings for devices, manage the monitoring of device event logs, and much more.

The MC topics in this help system describe how to use the MC to configure a device profile. For complete information about how to install, set up, and use the MC, please refer to "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Center.

After you type the IP address of the MC web interface into an Internet Explorer or Mozilla Firefox browser, the browser will use HTTPS (HTTP over an SSL socket) to connect to the MC web interface. The IP address for the MC web interface is configured (either statically or via DHCP) from the MC virtual machine console after installation. Access to the MC is controlled using an administrative password, which is also set from the MC virtual machine console after installation. Full details about these setup procedures are included in the "Teradici PCoIP® Management Console User Manual" (TER0812002).

The MC's HTTPS connection is secured using a PCoIP MC root Certificate Authority (CA) certificate. For information on how to install this certificate, see "Teradici PCoIP® Management Console User Manual" (TER0812002).

The MC is compatible with the following browsers:

- Firefox version 23 or newer
- Internet Explorer 8 and 9
- Internet Explorer 11 in compatibility view

Logging into the MC

To log into the Management Console web interface:

1. From an Internet browser, enter the IP address of the MC web page. The IP address may be a static or dynamic address, depending on how it is determined when the MC is configured:

- **Static IP Address:** The IP address is hard-coded and must be known.
- **Dynamic IP Address:** The IP address is dynamically assigned by the Dynamic Host Configuration Protocol (DHCP) server. You can get it from the DHCP server.

2. From the login page, enter the administrative password. The default value is blank (i.e., "").
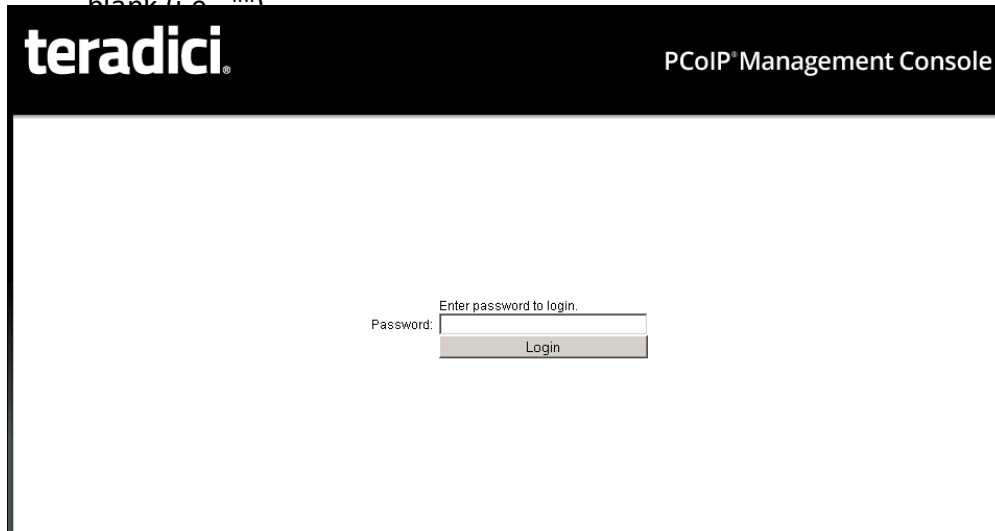
MC Login Page

3. When you first log into the MC, a prompt appears asking you to accept the license agreement. After reading it, click **Agree** at this page. For subsequent logins, this prompt does not appear.

After logging into the MC, the **Home** page appears.

MC Home Page

The MC **Home** page contains links to all the MC functions, and also contains a **Site Status** section that displays summary information about the PCoIP devices discovered by the MC.
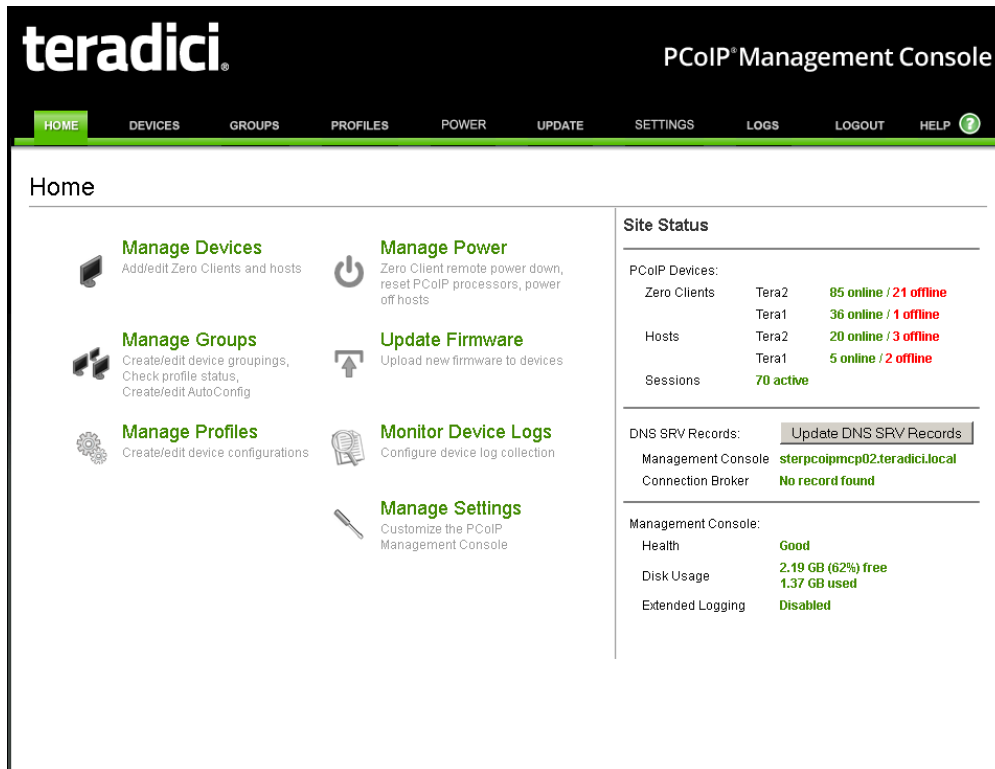
MC Home Page

Device firmware is configured on the MC by defining profiles and then applying them to groups of devices. Clicking the **Profiles** tab displays the **Profile Management** page, which lists allows you to manage the profiles in your system.

MC Profile Management Page

From the **Profile Management** page, you can view, add, duplicate, configure (i.e., set properties for), edit, delete, and export profiles.
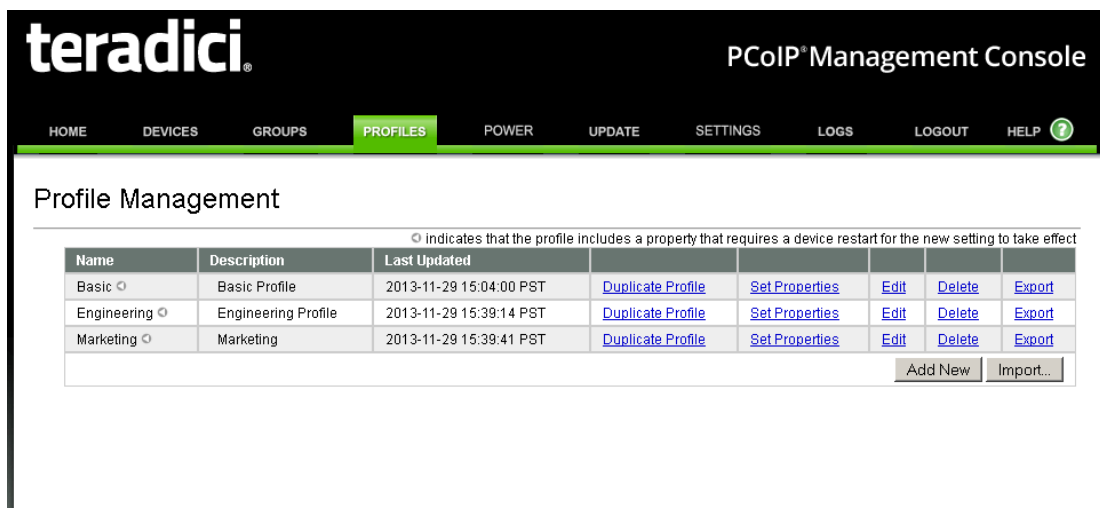
MC Profile Management Page

Once a profile has been created, you can click its **Set Properties** link to display the **Manage Profiles** page and begin defining a device configuration for the profile.

MC Manage Profiles Page

The figure below shows the **Manage Profiles** page for a profile. It contains a list of all the categories used to configure the device firmware.

MC Manage Profiles Page

To configure a category, expand it and click the **Edit Properties** link, shown in the example below.

Edit Properties Link

This displays the **Set Properties** page for that category, from which you can configure the category's individual parameters. The following example shows the parameters for the **Network Configuration** category.
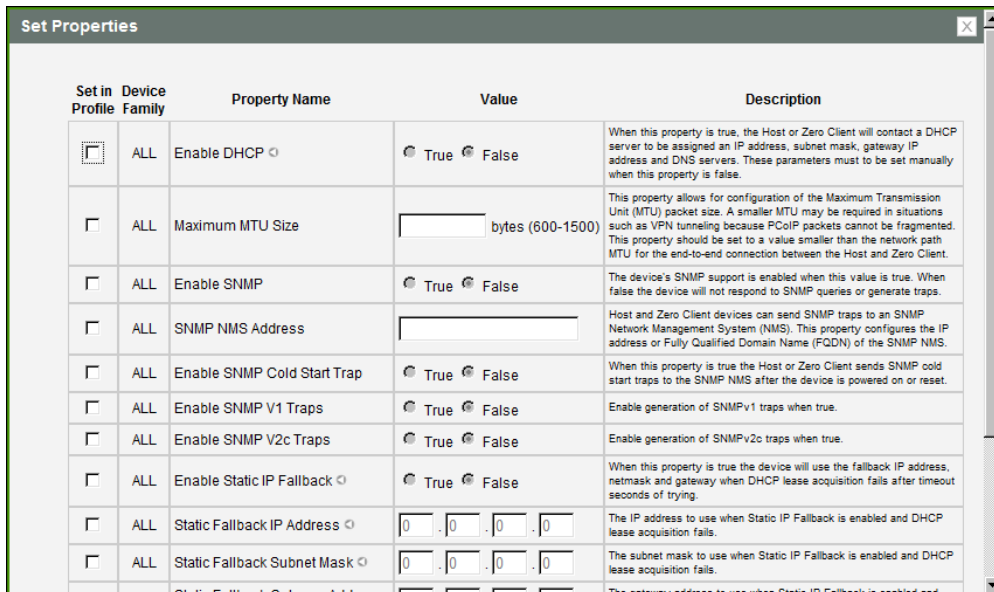
Set Properties Page for Network Configuration

Note: The parameter table for each category has a **Description** column to explain each parameter. These parameters are also explained in the MC sections of the GUI Reference.

After setting the desired properties, the **Manage Profiles** page expands the categories to show their configuration. You can use the expand/collapse links to control the display of this information.

An example of a profile with some of its categories configured is shown below.

Manage Profiles

Back to Profile List

Set Properties - Engineering

Return to Previous Page
Description
Last Updated   2014-10-17 15:16:16 PDT

Expand Categories With Set Values   Collapse All   ○ indicates that the property requires a device restart after being changed

− Network Configuration

Family	Property Name	Value	Description
ALL	Enable DHCP ○	True	When this property is true, the Host or Zero Client will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address and DNS servers. These parameters must to be set manually when this property is false.

Edit Properties

+ Discovery Configuration

− Session Configuration

Family	Property Name	Value	Description
ALL	Session Connection Type ○	Direct to Host	This setting controls how the PCoIP device initiates and receives PCoIP sessions.

Edit Properties

+ Encryption Configuration

+ Bandwidth Configuration

+ Language Configuration

+ OSD Configuration

+ Image Configuration

+ Display Configuration

+ Time Configuration

+ Security Configuration

+ Audio Permissions

− Unified Communications Configuration

Family	Property Name	Value	Description
Tera2	Unified Communications Mode ○	Disabled	This property configures Unified Communications support on Zero Clients.

Edit Properties

+ Power Permissions

− Host Driver Configuration

Family	Property Name	Value	Description
ALL	Enable Host Driver ○	False	On host cards only, this property controls the host driver function. When enabled, the Teradici PCoIP agent running on the host OS can interact with the host card. The MC supports this feature on devices running firmware 3.1.0 or higher.

Edit Properties

+ Event Log Control

MC Manage Profiles Page – Configured

The GUI Reference in this help system contains full details about each category. For information about how to configure or manage a device using these MC pages, please see the appropriate section in the GUI Reference.

For details on how to apply a profile, please refer to "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Documentation Center.

PCoIP Administrative Web Interface

About the AWI

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

After you type the device's IP address into an Internet Explorer or Mozilla Firefox browser, the browser will use HTTPS (HTTP over an SSL socket) 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 KB 15134-529 in the Teradici Support Site. Detailed instructions on how to install the certificate are also included in this KB.

The following browsers are supported in this release:

- Firefox versions 26 (or newer)
- Internet Explorer 7 and 8
- Internet Explorer 11 in compatibility view

Logging into the AWI

To log into the Administrator Web Interface web page for a host or client:

1. From an Internet browser, enter the IP address of the host or client. The IP address may be a static or dynamic address, depending on how the IP addresses are determined within your IP network:

   - **Static IP Address:** The IP address is hard-coded and must be known.
   - **Dynamic IP Address:** The IP address is dynamically assigned by the Dynamic Host Configuration Protocol (DHCP) server. You can get it from the DHCP server.

2. From the **Log In** page, enter the administrative password. The default value is blank (i.e., "").

Log In

Please enter the administrative password to access this device.

Password: [   ]

Idle Timeout: [Never ▼]   [Log In]

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**.

Note: Some networks using DHCP may be able to access the AWI using the PCoIP device name.

Note: Some PCoIP devices have password protection disabled and do not require a password to log in. You can enable or disable password protection through the security settings on the MC's **Manage Profiles** page.

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 PCoIP zero client and PCoIP Remote Workstation Card.

The AWI client **Initial Setup** and host **Initial Setup** pages are not identical. Each one provides parameters that apply to the client and host, respectively.

If configured in the firmware defaults, the **Initial Setup** page appears the first time you log in. After you click **Apply**, the **Home** page appears for subsequent sessions unless the firmware parameters are reset.

Note: 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 host or client. You can display the **Home** page at any time by clicking the **Home** link at the top left section of the menu bar.

AWI Host: Home Page

AWI Client: Home Page

Note: The above figures show 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.

Statistics	Description
PCoIP Device Name	The logical name for the device.
	This field is the name the host or 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. Values include the following:
	• **Asleep**
	• **Canceling**
	• **Connected**
	• **Connection Pending**
	• **Disconnected**
	• **Waking**
802.1X Authentication Status	Indicates whether 802.1x authentication is enabled or disabled on the device.
Session Encryption Type	The type of encryption in use when a session is active:
	• AES-128-GCM
	• SALSA20-256-Round 12
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).

Statistics	Description
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	How much image data is currently 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.
Image Quality	The minimum and maximum quality setting is taken from the **Image** page for the device. The active setting is what's currently being used in the session and only appears on the host.
Image Quality Preference	This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include the following: **Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked. **Disabled:** The **Disable Build to Lossless** field is checked.
Display	The port number for the display.
Maximum Rate	This column shows the refresh rate of the attached display. If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate. If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined."
Input Change Rate	The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video). Note: This option is only available on the host. It does not appear on the client.

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

Note: When you click the **Reset Statistics** button on a host Session Statistics or client Session Statistics page, the statistics reported in the **Home** page are also reset.

Failed Login Attempt Message

As of firmware release 4.1.0, a warning message alerts you if any failed access attempts to the AWI, OSD, or MC were detected since the last successful login. The message provides the date and time of the failed attempt, as shown below in the example warning message on the AWI.

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 Warning

AWI Menus

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

- **Configuration:** The pages under this menu let you configure the various aspects for the device, such as network settings, language, session parameters, etc.
- **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.

Note: The pages only available from the client are marked with a (*C) and the pages only available from the host are marked with an (*H).
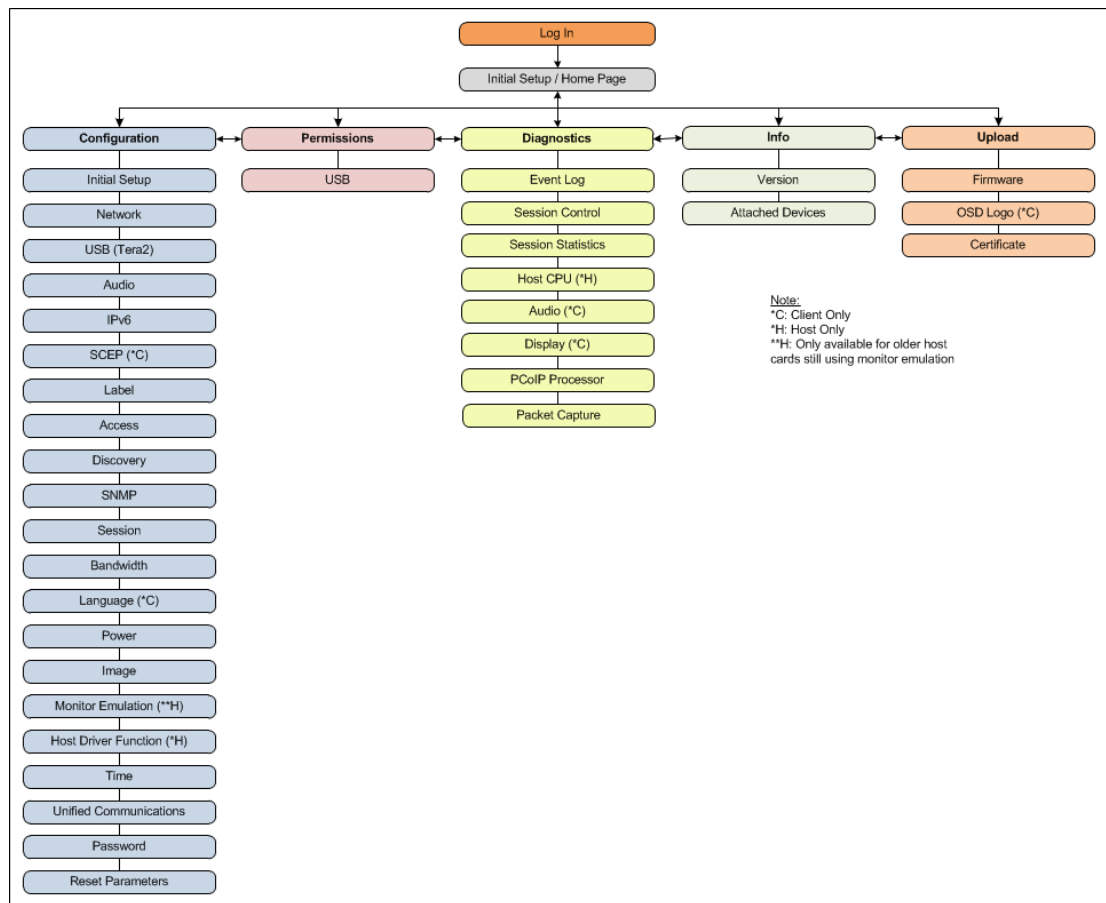
AWI Menu Overview

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

PCoIP On Screen Display

About the OSD

The PCoIP On Screen Display (OSD), shown in the figure below, 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.
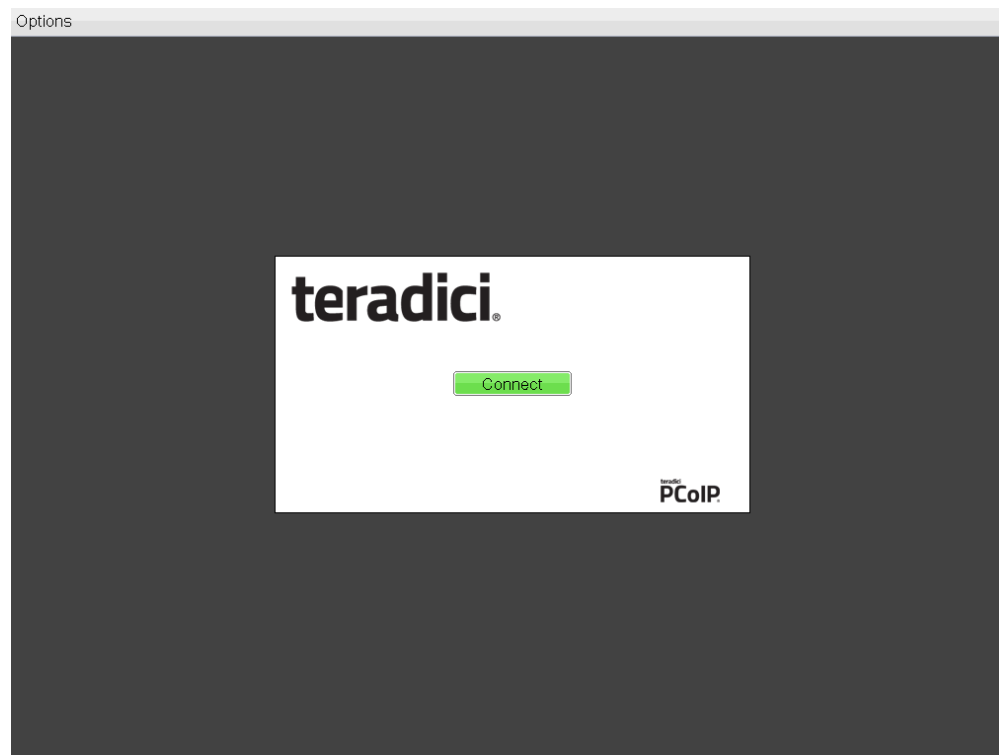
OSD Main Window

An **Options** menu in the upper left-hand corner lets users access various sub-menus for configuring the client and viewing information about it. A **Connect** button in the center of the window lets users connect the client to a virtual desktop or to a remote workstation card.

Connecting to a Session

The OSD allows 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 page.

To connect to a session from the Connect page:

- Enter the requested information (e.g., server name or IP address for Auto Detect, PCoIP Connection Manager, View Connection Server, and Connection Management Interface connection types), and then click **Connect**. If your 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.

- If you have already connected to a server, it will appear in the **Server** drop-down list if your zero client is configured to connect to this server or if it is configured to cache servers in **Last servers used** mode. Simply select the server from the drop-down list and then click **Connect**.

- If your zero client is configured to connect directly to a remote workstation card, you only need to click **Connect**.

Note: For details about how to enable server caching and configure server cache entries, see MC: Auto Detect Session Settings, MC: View Connection Server Session Settings, and MC: PCoIP Connection Manager Session Settings.

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

OSD "Auto Connect" Connect Page

OSD "Direct to Host" Connect Page

While the network connection is initializing, various status messages are displayed above the button to indicate the progress. If problems are experienced during startup—e.g., 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 OSD local GUI disappears, and the session image appears.

Making a Trusted HTTPS Connection

After connecting to the connection server, a user authentication page displays to allow 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 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 examples below show the user authentication screens that display for View Horizon and Amazon WorkSpaces connections when the server's certificate is trusted by the zero client.
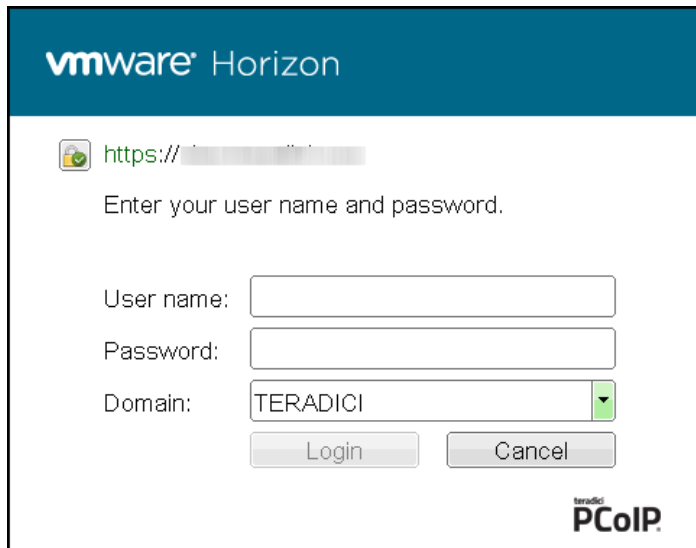
VMware Horizon Trusted HTTPS Connection

Amazon WorkSpaces 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 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 zero client is configured to warn before connecting to untrusted servers.
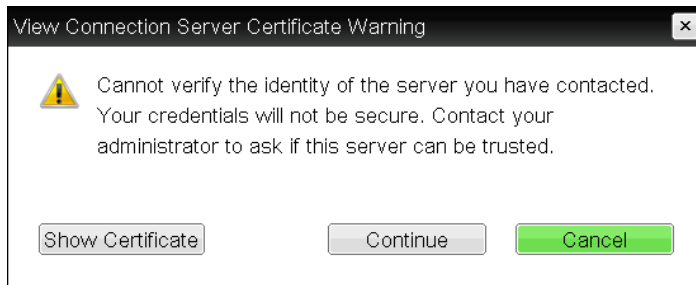
View Connection Server Certificate Warning
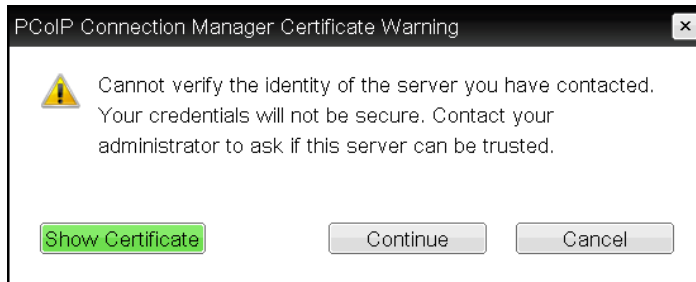
PCoIP Connection Manager Certificate Warning

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 shown in the examples below.
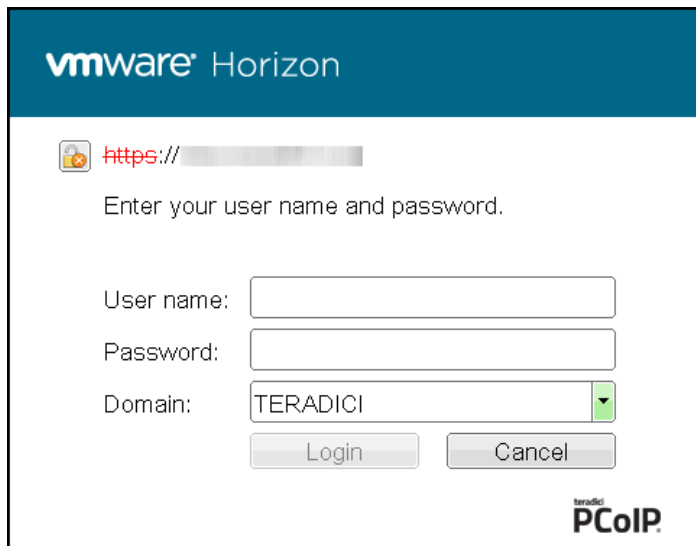
VMware Horizon Untrusted HTTPS Connection

Amazon WorkSpaces Untrusted HTTPS Connection

As an administrator, you can use the **Options > User Settings > Certificate** page, shown below, to prevent users from initiating untrusted server sessions by configuring the 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, as shown below.
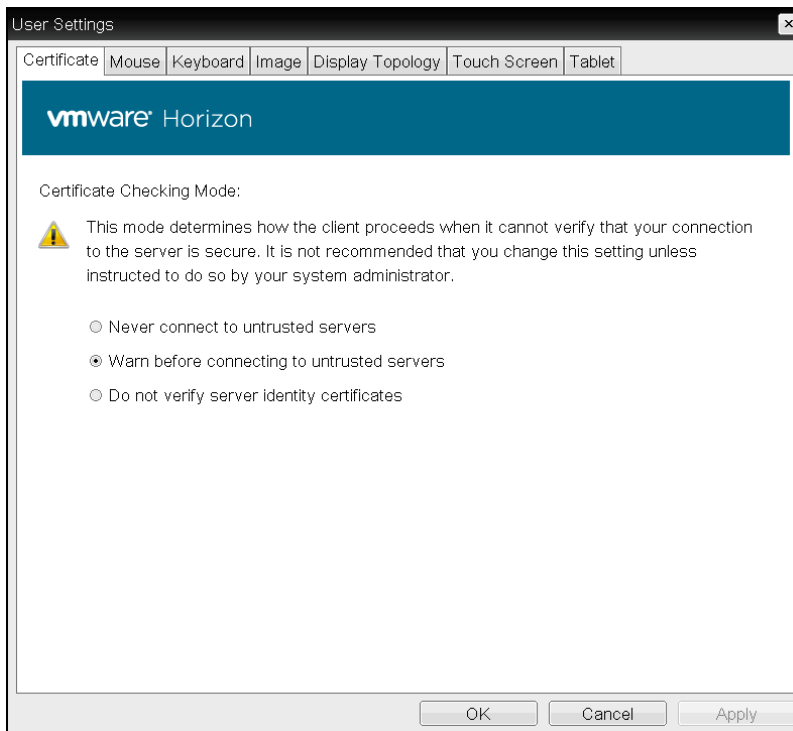
VMware Horizon Certificate Checking Mode Page
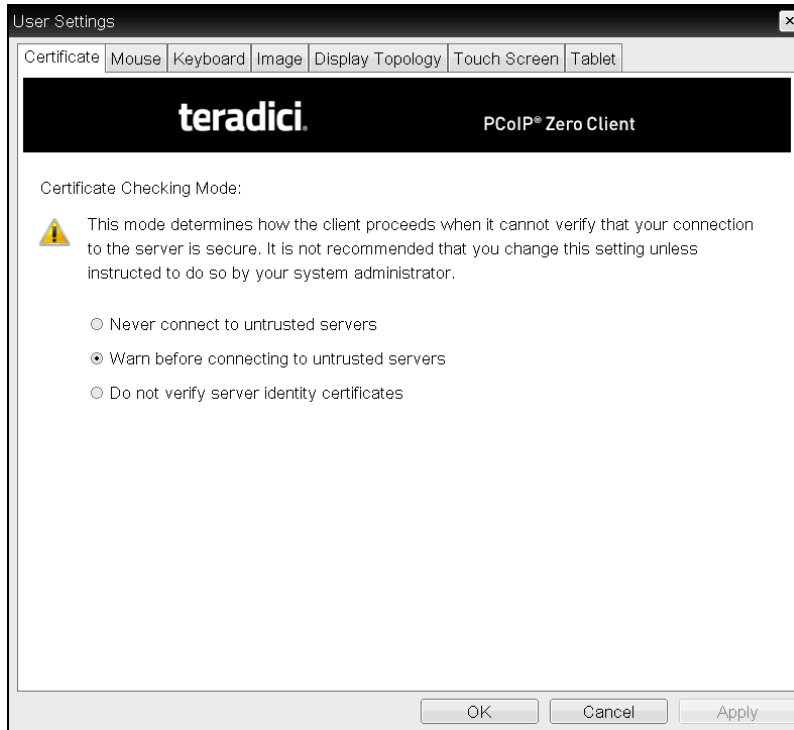
Teradici Certificate Checking Mode

Using the AWI, you can then 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, as shown in the example below.
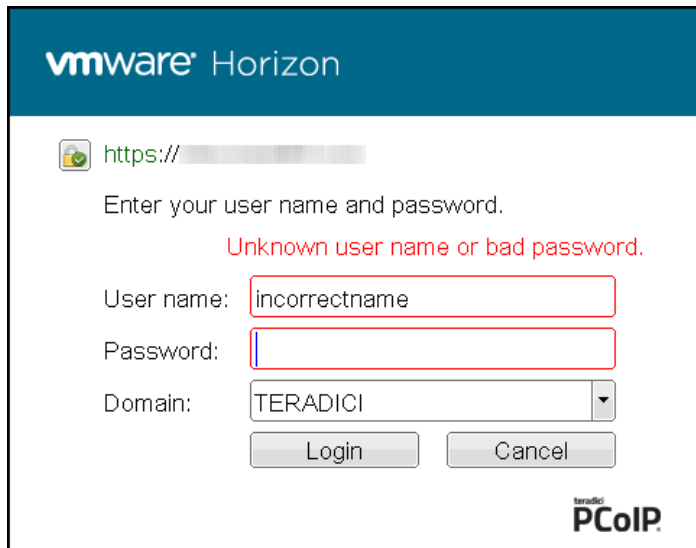
Unknown User Name or Password

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 then select the desired one and click **Connect**.
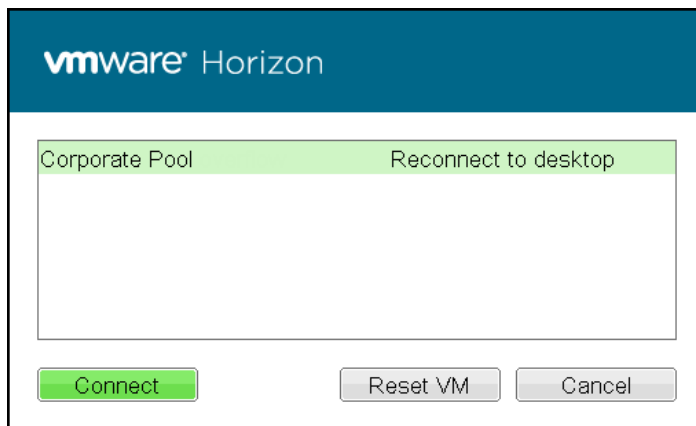
Selecting an Entitlement

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

If the desktop is not available (e.g., 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.

Related Topics

See also:

- For information on how to upload certificates to a profile using the MC, see MC: Certificate Store Management.
- For information on how to upload certificates to a single device using the AWI, see AWI: Certificate Upload Settings.
- 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 Overlay Windows.

Disconnecting from a Session

For Tera1 clients, users can disconnect from a session and return to the OSD by pressing the connect/disconnect button on the device.

For Tera2 clients, users can also disconnect from a virtual desktop session and return to the OSD by pressing the device's connect/disconnect button. However, if a user is in a session with a remote workstation card, pressing this button will pop up the Zero Client Control Panel overlay, shown in the figure below, which provides options to disconnect from the session, to power off the remote workstation, or to cancel the operation.
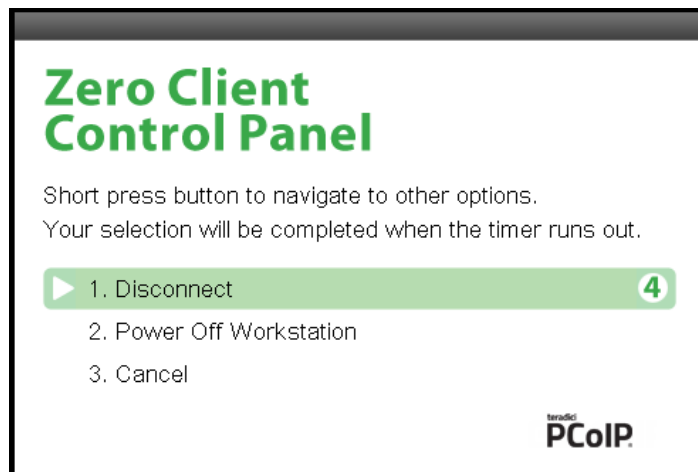
Zero Client Control Panel

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

- Continue to tap the connect/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, then press the Enter key.
- Type the number of the desired option to select it immediately.

During a session, users 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.
- 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 (i.e., not bridged).

Note: the latter two options must also be in place in order for users to use the up/down arrow keys or to type in a number to select a disconnect option on this overlay.

In order to allow users to use the second overlay option (i.e., to power off the workstation), the power permissions on the client must be configured to allow a "hard" power off. You can set this parameter from the MC **Power Permissions** page or from the AWI **Power Permissions** page.

Overlay Windows

Overlay windows occasionally appear on top of the user's PCoIP session to display pertinent information when the status changes—e.g., 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, as shown in the examples below.

Display Link Training Failed

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, the following overlay appears with the message "Display link training failed."
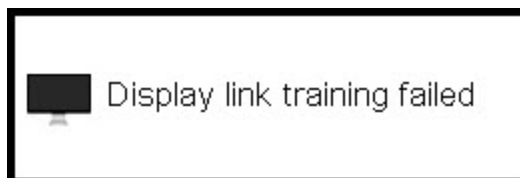
Display Link Training Failed Overlay

Half Duplex Overlay

PCoIP technology is not compatible with half-duplex network connections. When a half-duplex connection is detected, the following overlay appears with the message "Half-duplex network connection."
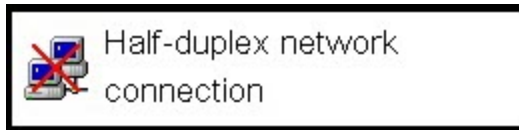
Half Duplex Overlay

Network Connection Lost Overlay

Loss of network connectivity is indicated using an overlay with the message "Network connection lost" over the most recent screen data. This overlay appears when the client network cable is disconnected or when no PCoIP protocol traffic is received by the client for more than two seconds.

Network Connection Lost Overlay

The lost network connection message appears until the network is restored or the timeout expires (and the PCoIP session ends).

Note: 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

This overlay displays on Tera2 clients only. Display resolution may have limitations due to resource constraints when all four ports have large displays connected. If the resolution limit is exceeded, the following overlay appears with the message "No support resolutions found. Please try unplugging other displays."
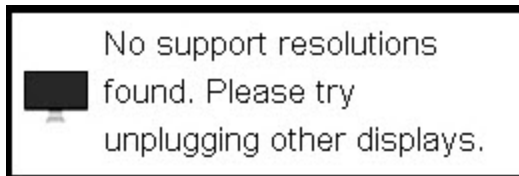
No Support Resolutions Found Overlay

Preparing Desktop Overlay

When a user first logs into a PCoIP session, the following overlay appears with the message "Preparing desktop."
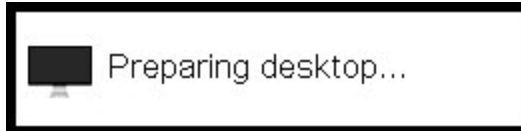
Preparing Desktop Overlay

USB Device Not Authorized Overlay

If an unauthorized USB device is connected, the following overlay appears with the message "USB device not authorized." This overlay lasts for approximately five seconds.

USB Device Not Authorized Overlay

USB Over Current Notice Overlay

If the USB devices connected to the client cannot be handled by the USB ports, the following overlay appears with the message "USB over current notice." This overlay remains until USB devices are removed to meet the current handling of the USB ports.
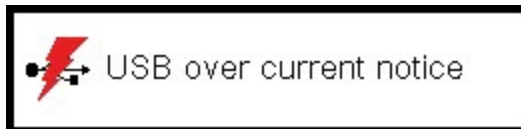
USB Over Current Notice Overlay

USB Device Not Supported Behind a High-speed Hub Overlay

Some USB devices cannot be connected through a high speed (USB 2.0) hub, and should instead be connected directly to the zero client or through a full speed (USB 1.1) hub. If such a device is connected to the zero client through a high speed hub, the following overlay appears with the message "USB device not supported behind high speed hub." This overlay lasts for approximately five seconds.

USB Device Not Supported Behind a High-speed Hub Overlay

Resolution Not Supported Overlay

If the resolution of a monitor connected to the client cannot be supported by the host, the monitor is set to its default resolution and the following overlay appears with the message "Resolution not supported."
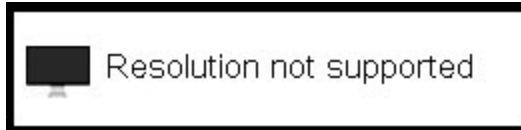
Resolution Not Supported Overlay

Video Source Overlays

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

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

No Source Signal Overlay

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

Source Signal on Other Port Overlay

OSD Menus

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

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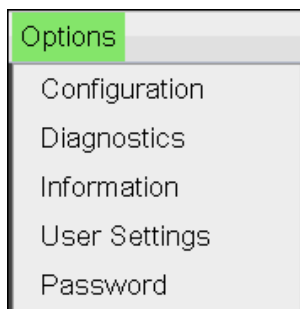
OSD Options Menu

Note: You can hide a single menu item, the entire **Options** menu, or all menus from users. For details, see **MC: OSD Settings**.

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

Deployment Scenarios

PCoIP Endpoints

PCoIP is a flexible technology that lets you deploy both PCoIP hardware endpoints and PCoIP software endpoints in your end-to-end network.

PCoIP Hardware Endpoints

PCoIP hardware endpoints include PCoIP Remote Workstation Cards and zero clients. These devices contain embedded PCoIP processors for image compression/decompression and coding/decoding, respectively. The table below lists the processor name and family for zero clients and remote workstation cards, along with the set of display resolutions the device supports.

Note: The processor name refers to the chipset used in the PCoIP device. For example, TERA2140 is the processor used in the second-generation TERA2140 zero client, and TERA2240 is the processor used in the second-generation TERA2240 PCIe remote workstation card (for tower PC or rack mount workstations) and TERA2240 PCI Mezzanine remote workstation card (for blade workstations). For details on how to display the processor name for your device, see Displaying Processor Information.

Supported Resolutions for PCoIP Remote Workstation Cards and Zero Clients

Processor Name	Maximum No. of Supported Displays and Resolutions	Device Type	Processor Family
TERA1100	2 x 1920x1200	zero client	Tera1
TERA2321	2 x 1920x1200 1 x 2560x1600*	zero client	Tera2
TERA2140	4 x 1920x1200 2 x 2560x1600*	zero client	Tera2
TERA1202	2 x 1920x1200	remote workstation card	Tera1
TERA2220	2 x 1920x1200 1 x 2560x1600	remote workstation card	Tera2
TERA2240	4 x 1920x1200 2 x 2560x1600	remote workstation card	Tera2

Processor Name	Maximum No. of Supported Displays and Resolutions	Device Type	Processor Family
*Tera2 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 zero clients with DVI and/or DisplayPort ports to support this resolution, see DVI and DisplayPort Interfaces.			

You can mix and match any remote workstation card with any zero client. However, when you connect a zero client to a remote workstation card, the maximum supported resolutions for any displays attached to the client will equal the most common denominator between the two devices. For example, if you connect a TERA2140 zero client to a TERA2240 remote workstation card, you can attach up to four 1920x1200 displays or two 2560x1600 displays. However, if you connect a TERA2321 zero client to the same remote workstation card, the options become up to two 1920x1200 displays or one 2560x1600 display.

PCoIP Software Endpoints

A number of software endpoints also support PCoIP, such as the following:

- **Teradici PCoIP® Software Clients**: PCoIP software clients for Windows and Mac OS X that are developed by Teradici.

- **Teradici PCoIP® Mobile Clients**: PCoIP mobile clients for for Android and iOS tablets that are developed by Teradici.

- **Teradici PCoIP® Workstation Access Software**: A PCoIP software application developed by Teradici that allows users to remotely access their workstations using the PCoIP protocol without having to install a PCoIP Remote Workstation Card. You can connect to the PCoIP Access Software using either a Tera2 zero client or a PCoIP software client.

- **VMware Horizon software clients and VDI desktops**: Desktop virtualization products developed by VMware that uses the PCoIP protocol. You can connect to your VMware Horizon VDI desktop using a zero client.

- **VMware Horizon RDS-hosted published desktops and applications**. App-remoting desktops and applications developed by VMware that uses the PCoIP protocol. You can configure a Tera2 zero client to access VMware Horizon RDS-hosted streamed applications and desktops.

- **Amazon WorkSpaces desktops**: Desktop virtualization products developed by Amazon that uses the PCoIP protocol. You can connect to your Amazon WorkSpaces desktop using a Tera2 zero client.

- **PCoIP optimized clients**: Software PCoIP clients that have been optimized to take advantage of thin client platforms, including system on chip (SoC) processors. These clients are developed individually for specific client

platforms in order to deliver the best possible combination of features and performance.

Connection Types

Most connection types are configured from the **Configuration > Session** menu in the AWI or OSD and the **Profiles > Session Configuration** menu in the MC. One exception is the Zero Client-to-Bria Softphone Caller Endpoint connection type, which is configured from the **Configuration > Unified Communications** menu in the AWI and the **Profiles > Unified Communications Configuration** menu in the MC.

The zero client supports the following session connection types:

- Zero Client–to–Remote Workstation Card Connections
- Zero Client–to–PCoIP Connection Manager Connections

    - Teradici PCoIP® Workstation Access Software Connections
    - Amazon WorkSpaces Connections
- Zero Client–to–VMware Horizon VDI, DaaS, and RDS-hosted App-remoting Connections
- Zero Client–to–Bria Softphone Caller Endpoint Connections

Zero Client–to–Remote Workstation Card Connections

You can move high-performance Windows or Linux workstations with PCoIP Remote Workstation Cards into your data center, and then configure sessions between 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.

Depending on the size of your PCoIP deployment, you may wish to use the MC or a connection broker to manage connections between remote workstation cards and zero clients, or you may use the AWI to configure individual hosts and clients remotely. You can even use the OSD to configure settings for a specific zero client.

The following session connection types are available for zero client-to-remote workstation card connections:

- Connecting statically
- Connecting using SLP host discovery
- Connecting using a 3rd party connection broker
- Connecting using the View Connection Server broker

For information on the prerequisites for these connection types, see Zero Client–to–Remote Workstation Card Prequisites.

Connecting Statically

To statically configure a zero client to connect directly to a specific remote workstation card, use the **Direct to Host** session connection type. You will need to provide the DNS name or IP address of the remote workstation card for this option.

You also need to configure a **Direct from Client** session connection type on the remote workstation card. You have the option of allowing 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 on how to configure this option, see the following topics in the GUI Reference:

- MC: Direct to Host: Explains how to use the MC to configure a profile that sets the **Direct to Host** session connection type for zero clients. For information on how to statically link specific hosts and clients using the MC, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Documentation Center.
- AWI Client: Direct to Host: Explains how to use the AWI to statically configure a zero client to connect to a specific remote workstation card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a remote workstation card to accept a connection request from any zero client or from a specific zero client only.
- OSD: Direct to Host: Explains how to use the OSD to statically configure a zero client to connect to a specific remote workstation card.

Connecting Using SLP Host Discovery

If remote workstation cards reside on the same subnet as 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 remote workstation cards on the subnet. With this configuration, the client OSD will list the first 10 cards discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for deployments with more than 10 hosts if a zero client needs to connect to a specific host all the time. In this situation, a 3rd party connection broker is required.

You also need to configure a **Direct from Client** session connection type on the remote workstation card. You have the option of allowing the host to accept a connection request from any zero client or from a specific one only. If the latter, you need to provide the client's MAC address.

For details on how to configure this option, see the following topics in the GUI Reference:

- [MC: Direct to Host + SLP](#): Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for zero clients.

- [AWI Client: Direct to Host + SLP](#): Explains how to use the AWI to configure a zero client to use SLP discovery to connect to a remote workstation card.

- [AWI Host: Direct from Client](#): Explains how to use the AWI to configure a remote workstation card to accept a connection request from any zero client or from a specific client only.

- [OSD: Direct to Host + SLP](#): Explains how to use the OSD to configure a zero client to use SLP discovery to connect to a remote workstation card.

Connecting Using a 3rd Party Connection Broker

A 3rd party connection broker is a resource manager that dynamically assigns host PCs containing remote workstation cards to zero clients based on the identity of the user establishing a connection from the zero client. Connection brokers are also used to allocate a pool of hosts to a group of zero clients. They are typically used in large PCoIP deployments, or when hosts and clients do not reside on the same subnet.

Use the **Connection Management Interface** session connection type on both the host and client for this option. You need to provide the DNS name or IP address for the 3rd party connection broker.

Note: For information about 3rd party connection brokers, see [KB 15134-24](#) in the Teradici Support Site.

For details on how to configure this option, see the following topics in the GUI Reference:

- [MC: Connection Management Interface](#): Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for zero clients and remote workstation cards.

- [AWI Client: Connection Management Interface](#): Explains how to use the AWI to configure a zero client to use a 3rd party connection broker to broker the connection between zero clients and remote workstation cards.

- [AWI Host: Connection Management Interface](#): Explains how to use the AWI to configure a remote workstation card to use a 3rd party connection broker for accepting a connection request from a zero client.

- [OSD: Connection Management Interface](#): Explains how to use the OSD to configure a zero client to use a 3rd party connection broker to broker the connection between a zero client and remote workstation card.

Connecting Using the View Connection Server Broker

You can also use a View Connection Server to broker a connection between zero clients and remote workstation cards.

Note: This is not the same thing as configuring a zero client to connect to a VMware Horizon virtual desktop using a View Connection Server.

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, please refer to "Using PCoIP® Host Cards with VMware View" (TER0911004) in the Teradici Support Documentation Center.

Zero Client–to–PCoIP Connection Manager Connections

The PCoIP Connection Manager implements the PCoIP Broker Protocol for authentication and session initiation. The **PCoIP Connection Manager** session connection type can be used to connect Tera2 zero clients to the following types of remote PCoIP endpoints:

- **Teradici PCoIP® Workstation Access Software**: The PCoIP Access Software is a Teradici application installed on a remote workstation that allows you to remotely access your workstation using the PCoIP protocol without having to install a remote workstation card. Using a Tera2 zero client, you can connect to your PCoIP Access Software using the **PCoIP Connection Manager** or **Auto Detect** session connection type. For details on how to install the PCoIP Access Software in a workstation and use a Tera2 zero client to establish a session, please see "Teradici PCoIP® Workstation Access Software User Guide" (TER1405004) in the Teradici Support Documentation Center. For information on the prerequisites for this connection type, see Zero Client–to–PCoIP Workstation Access Software Prerequisites.

- **Amazon WorkSpaces**: Amazon WorkSpaces is Amazon's desktop computing service in the cloud where cloud-based desktops are provisioned for end users. Using a Tera2 zero client, you can use the **PCoIP Connection Manager** or **Auto Detect** session connection type to connect to your WorkSpaces desktop. For details on how to install and configure the necessary components, and how to use a Tera2 zero client to establish a session, please see "Connecting PCoIP® Zero Clients to Amazon WorkSpaces" (TER1408002) in the Teradici Support Documentation Center. For information on the prerequisites for this connection type, see Zero Client–to–Amazon WorkSpaces Prerequisites.

The following session connection types are available for zero client-to-PCoIP Connection Manager connections:

- Auto Detect
- PCoIP Connection Manager
- PCoIP Connection Manager + Auto-Logon

Auto Detect

To configure a Tera2 zero client to automatically detect the right broker to use on the OSD **Connect** screen, use the **Auto Detect** session connection type and configure the URI for your broker (e.g., a PCoIP Connection Manager or View Connection Server). After making a successful connection, you can select this URI from the **Server** drop-down list on the OSD **Connect** screen.

For details on how to configure this option, see the following topics in the GUI Reference:

- MC: Auto Detect: Explains how to use the MC to configure a profile that sets the **Auto Detect** session connection type for zero clients.
- AWI Tera2 Client: Auto Detect: Explains how to use the AWI to configure a zero client to automatically detect the broker to use on the OSD **Connect** screen.
- OSD Tera2: Auto Detect: Explains how to use the OSD to configure a zero client to automatically detect the broker to use on the OSD **Connect** screen.

PCoIP Connection Manager

To configure a zero client to connect to a PCoIP Access Software instance that is installed in a remote workstation or to an Amazon WorkSpaces desktop, use the **PCoIP Connection Manager** session connection type. You will need to provide the appropriate server URI for the connection type. For instructions, please see "Teradici PCoIP® Workstation Access Software User Guide" (TER1405004) and "Connecting PCoIP® Zero Clients to Amazon WorkSpaces" (TER1408002), respectively.

For details on how to configure this option, see the following topics in the GUI Reference:

- MC: PCoIP Connection Manager: Explains how to use the MC to configure a profile that sets the **PCoIP Connection Manager** session connection type for zero clients.
- AWI Client: PCoIP Connection Manager: Explains how to use the AWI to configure a client to use the **PCoIP Connection Manager** session connection type.
- OSD: PCoIP Connection Manager: Explains how to use the AWI to configure a client to use the **PCoIP Connection Manager** session connection type.

PCoIP Connection Manager + Auto-Logon

You can also use the **PCoIP Connection Manager + Auto-Logon** session connection type to automatically enter user login details when connecting in PCoIP Connection Manager mode. Besides the appropriate server URI, you will need to provide a user name, user password, and domain name.

For details on how to configure this option, see the following topics in the GUI Reference:

- **MC: PCoIP Connection Manager + Auto-Logon**: Explains how to use the MC to configure a profile that sets the **PCoIP Connection Manager + Auto-Logon** session connection type for zero clients. This session connection type is useful when you want to set a default user name and password in a profile.
- **AWI Client: PCoIP Connection Manager + Auto-Logon**: Explains how to use the AWI to configure a client to automatically send user login details when connecting in PCoIP Connection Manager mode.
- **OSD: PCoIP Connection Manager + Auto-Logon**: Explains how to use the OSD to configure a client to automatically send user login details when connecting in PCoIP Connection Manager mode.

Zero Client–to–VMware Horizon Connections

You can configure zero clients to use the PCoIP protocol when connecting 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.

Note: 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 zero clients. After configuring your View Connection Server, select the Enable RDS Application Access check box in **Advanced Options** on the **Session** page.

Depending on the size of your PCoIP deployment, you may wish to use the MC to configure a profile with a **View Connection Server** session connection type, or you may use the AWI or the OSD to configure an individual zero client to use a **View Connection Server** session connection type.

The following session connection types are available for zero client-to-VMware Horizon VDI connections:

- View Connection Server
- View Connection Server + Auto-Logon
- View Connection Server + Kiosk
- View Connection Server + Imprivata OneSign

For information on the prerequisites for these connection types, see Zero Client–to–VMware Horizon Prerequisites.

Auto Detect

To configure a Tera2 zero client to automatically detect the right broker to use on the OSD **Connect** screen, use the **Auto Detect** session connection type and configure the URI for your broker (e.g., a PCoIP Connection Manager or View Connection Server). After making a successful connection, you can select this URI from the **Server** drop-down list on the OSD **Connect** screen.

For details on how to configure this option, see the following topics in the GUI Reference:

- MC: Auto Detect: Explains how to use the MC to configure a profile that sets the **Auto Detect** session connection type for zero clients.
- AWI Tera2 Client: Auto Detect: Explains how to use the AWI to configure a zero client to automatically detect the broker to use on the OSD **Connect** screen.
- OSD Tera2: Auto Detect: Explains how to use the OSD to configure a zero client to automatically detect the broker to use on the OSD **Connect** screen.

View Connection Server

To configure a zero client to connect to a VMware virtual desktop with a manual logon, use the **View Connection Server** session connection type. You will need to provide the DNS name or IP address of the View Connection Server.

For details on how to configure this option, see the following topics in the GUI Reference:

- MC: View Connection Server: Explains how to use the MC to configure a profile that sets the **View Connection Server** session connection type for zero clients.
- AWI Client: View Connection Server: Explains how to use the AWI to configure a zero client to use the **View Connection Server** session connection type.
- OSD: View Connection Server: Explains how to use the OSD to configure a zero client to use the **View Connection Server** session connection type.

View Connection Server + Auto-Logon

To configure zero clients to automatically enter user login details when zero clients connect to a virtual desktop, use the **View Connection Server + Auto-Logon** session connection type. You will need to provide the DNS name or IP address of the View Connection Server, and also the user name, user password, and the domain name to send to the server.

For details on how to configure this option, see the following topics in the GUI Reference:

- **MC: View Connection Server + Auto-Logon**: Explains how to use the MC to configure a profile that sets the **View Connection Server + Auto-Logon** session connection type for zero clllients. This session connection type is useful when you want to set a default user name and password in a profile.

- **AWI Client: View Connection Server + Auto-Logon**: Explains how to use the AWI to configure a zero client to automatically send user login details when connecting to a Horizon desktop.

- **OSD: View Connection Server + Auto-Logon**: Explains how to use the OSD to configure a zero client to automatically send user login details when connecting to a Horizon desktop.

View Connection Server + Kiosk

View Connection Server + Kiosk mode allows you to configure 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.

For details on how to configure this option, see the following topics in the GUI Reference:

- **MC: View Connection Server + Kiosk**: Explains how to use the MC to configure a profile that sets the **View Connection Server + Kiosk** session connection type for zero clients.

- **AWI Client: View Connection Server + Kiosk**: Explains how to use the AWI to configure a zero client to use Kiosk mode when connecting to a Horizon desktop.

- **OSD: View Connection Server + Kiosk**: Explains how to use the OSD to configure a zero client to use Kiosk mode when connecting to a Horizon desktop.

View Connection Server + Imprivata OneSign

View Connection Server + Imprivata OneSign mode allows you to configure zero clients to use Imprivata OneSign proximity card support when connecting to a virtual desktop via a View Connection Server. You will need to provide the DNS name or IP address of the View Connection Server and the bootstrap URL for the OneSign server.

For details on how to configure this option, see the following topics in the GUI Reference:

- **MC: View Connection Server + Imprivata OneSign**: Explains how to use the MC to configure a profile that sets the **View Connection Server + Imprivata**

OneSign session connection type for zero clients.

- AWI Client: View Connection Server + Imprivata OneSign: Explains how to use the AWI to configure a zero client to use Imprivata OneSign mode when connecting to a Horizon desktop.
- OSD: View Connection Server + Imprivata OneSign: Explains how to use the OSD to configure a zero client to use Imprivata OneSign mode when connecting to a Horizon desktop.

Zero Client–to–Bria Softphone Caller Endpoint Connections

The zero client supports interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on a VMware Horizon View or Horizon DaaS desktop.

After using a zero client to connect to a Horizon desktop or an Amazon WorkSpaces desktop, users can initiate Unified Communications (UC) services (e.g., voice, messaging, presence information, and contacts) to caller endpoints using a Bria Virtualized Edition softphone client that is installed on their desktop. Once the Bria client establishes the connection, call traffic is routed directly between the zero client and the caller endpoint, thus offloading this traffic from the data center.

This feature is configured from the **Configuration > Unified Communications** menu in the AWI and the **Profiles > Unified Communications Configuration** menu in the MC. See AWI Tera2 Client: Unified Communications and MC: Unified Communications for details.

For information on the prerequisites for this connection type, see Zero Client–to–Bria Softphone Client Caller Endpoint Prerequisites.

For information on how to troubleshoot softphone calls, see AWI Tera2 Client: Packet Capture.

Connection Prerequisites

This section lists basic requirements for the following connection types you can make using zero clients and remote workstation cards:

- Zero Client–to–Remote Workstation Card Prerequisites
- PCoIP Software Client–to–Remote Workstation Card Prerequisites
- Zero Client–to–PCoIP Workstation Access Software Prerequisites
- Zero Client–to–Amazon WorkSpaces Prerequisites

- [Zero Client–to–VMware Horizon Prerequisites](#)
- [Zero Client–to–Bria Softphone Caller Endpoint Prerequisites](#)

Downloading Firmware Note: To download a specific firmware version for a zero client or remote workstation card, log in to the Teradici [Support Site](#), and then type the desired firmware version into the search box (e.g., "firmware *x.x.x*").

Zero Client–to–Remote Workstation Card Prerequisites

Before [connecting a zero client to a remote workstation card](#), please ensure that the following prerequisites are in place:

- The remote workstation card and zero client have the same firmware versions. For information on how to assign a firmware file to a profile using the MC, see [MC: Firmware Management](#). For information on how to upload firmware to a single host or client using the AWI, see [Uploading Firmware](#).
- You are running a supported OS on the workstation and the Teradici PCoIP host software is installed. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) or "PCoIP® Host Software for Linux User Guide" (TER1104006) in the Teradici Support [Documentation Center](#). If you are using a VMware Connection Server as a broker, View Agent must also be installed on the host PC or workstation.
- The [Host Driver Function](#) is enabled on the 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® Protocol Virtual Desktop Network Design Checklist" (TER1105004) in the Teradici Support [Documentation Center](#).

PCoIP Software Client–to–Remote Workstation Card Prerequisites

Before connecting a a PCoIP software client to a remote workstation card, please ensure that the following prerequisites are in place on the remote workstation card:

- The remote workstation card has firmware 4.2.0 or newer installed (see [Downloading Firmware Note](#)).
- You are running a supported OS on the workstation and the Teradici PCoIP Host Software must be installed in the workstation.

For details about PCoIP software client requirements, more information about remote workstation requirements, and instructions on how to configure the client to connect to a remote workstation card, please see "Teradici PCoIP® Software Clients

User Guide" (TER1307002) in the Teradici Support [Documentation Center](). PCoIP Access SoftwarePCoIP Access Software

Zero Client–to–PCoIP Workstation Access Software Prerequisites

Before [connecting a zero client to a workstation running the Teradici PCoIP® Workstation Access Software](), please ensure that the following prerequisites are in place:

- You are using a Tera2 zero client (TERA2321 or TERA2140 processor) to connect.
- Your zero client has firmware version 4.7.0 or newer installed (see [Downloading Firmware Note]()). For information on how to assign a firmware file to a profile using the MC, see [MC: Firmware Management](). For information on how to upload firmware to a single host or client using the AWI, see [Uploading Firmware]().

- The remote workstation has the PCoIP Access Software installed.

For details about PCoIP Access Software requirements, along with instructions on how to connect to a PCoIP Access Software instance running on a workstation, please see "Teradici PCoIP® Workstation Access Software User Guide" (TER1405004) in the Teradici Support [Documentation Center]().

Zero Client–to–Amazon WorkSpaces Prerequisites

Before [connecting a zero client to an Amazon WorkSpaces desktop](), please ensure that the following prerequisites are in place:

- You are using a Tera2 zero client (TERA2321 or TERA2140 processor) to connect.
- Your zero client has firmware version 4.6.0 or newer installed (see [Downloading Firmware Note]()). For information on how to assign a firmware file to a profile using the MC, see [MC: Firmware Management](). For information on how to upload firmware to a single host or client using the AWI, see [Uploading Firmware]().
- You have an AWS account with Amazon WorkSpaces up and running. For information, please see AWS documentation.
- Your network has full connectivity to your Amazon WorkSpaces. For information, please see AWS documentation.
- You have a PCoIP® Connection Manager for Amazon WorkSpaces appliance installed and configured. For more information, see "Connecting PCoIP® Zero

Clients to Amazon WorkSpaces" (TER1408002) in the Teradici Support [Documentation Center](#).

Zero Client–to–VMware Horizon Prerequisites

Before [connecting a zero client to a VMware Horizon desktop](#), please 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 information about VMware Horizon DaaS and VMware Horizon 6 prerequisites, please refer to VMware documentation. For information on how to assign a firmware file to a profile using the MC, see [MC: Firmware Management](#). For information on how to upload firmware to a single host or client using the AWI, see [Uploading Firmware](#).
- The zero client has firmware version 3.1.0 or newer installed. For connections to VMware Horizon 6 RDS-hosted desktops, the zero client has firmware version 4.6.0 or newer installed. For connections to VMware Horizon 6 RDS-hosted applications, the zero client has firmware version 4.8.0 or newer installed.
- For VMware Horizon connections to RDS-hosted published desktops and applications, you are using a Tera2 zero client (TERA2321 or TERA2140 processor).
- Your network resources meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see "PCoIP® Protocol Virtual Desktop Network Design Checklist" (TER1105004) in the Teradici Support [Documentation Center](#).

Zero Client–to–Bria Softphone Caller Endpoint Prerequisites

Before [using a Bria Virtualized Edition softphone client to connect a zero client to a caller endpoint](#), please ensure that the following prerequisites are in place:

CounterPath Bria Virtualized Edition for PCoIP Zero Clients Softphone Client requirements:

- The CounterPath Bria Virtualized Edition softphone client is installed on a VMware Horizon View desktop, a VMware Horizon DaaS desktop, or an Amazon WorkSpaces desktop.
- Your system contains a SIP-compliant call server.
- If instant messaging and presence information are desired, your system contains an XMPP instant messaging and presence server.

- You are using an analog headset (any type) or one of the following tested USB headsets:

    - Plantronics Blackwire C310 and C320 USB

    - Plantronics Blackwire C435

    - Plantronics Blackwire C510 and C520

    - Plantronics Blackwire C710 and C720
      Note: Other USB headsets may also work with this application, but have not been tested at this time.

Zero client requirements:

- You are using a Tera2 zero client (TERA2321 or TERA2140 processor) to connect.

- Your zero client has firmware version 4.7.0 or newer installed (4.8.0 or newer for Bria softphone support on Amazon WorkSpaces desktops). If your firmware version is prior to 4.5.0, you must install a version 4.5.x or 4.6.0 firmware release before upgrading to version 4.7.0. For more information about the firmware upgrade process, please see "TERA Firmware Release Notes Version 4.x" (TER1204003). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see Uploading Firmware.

- You have enabled Unified Communications (UC) for the zero client. For details, see MC: Unified Communications or AWI Tera2 Client: Unified Communications.

- You have purchased the required licenses for the Bria Virtualized Edition for PCoIP Zero Clients softphone. For more information, please visit the CounterPath store.

- If desired, you have configured VLAN tagging for QoS management of VoIP call data.

Common LAN Scenarios

Connecting over a LAN

LAN connections between PCoIP endpoints can either be direct or brokered by a connection server. The scenarios listed below describe some of the most common ways you can connect PCoIP endpoints over a LAN.

- Scenario 1: Connecting a zero client to a remote workstation card.
- Scenario 2: Using a View Connection Server to broker a connection between a zero client and a remote workstation card.

- **Scenario 3**: Using a View Connection Server to broker a connection between a zero client and a virtual desktop.
- **Scenario 4**: Using the PCoIP Connection Manager broker to establish a connection between a Tera2 zero client and the Teradici PCoIP® Workstation Access Software installed in a workstation.

Zero Client to Remote Workstation Card (LAN)

The figure below shows a PCoIP session between a zero client and remote workstation card from within a LAN.

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center. Please refer to Connection Prerequisites for other conditions that may apply.
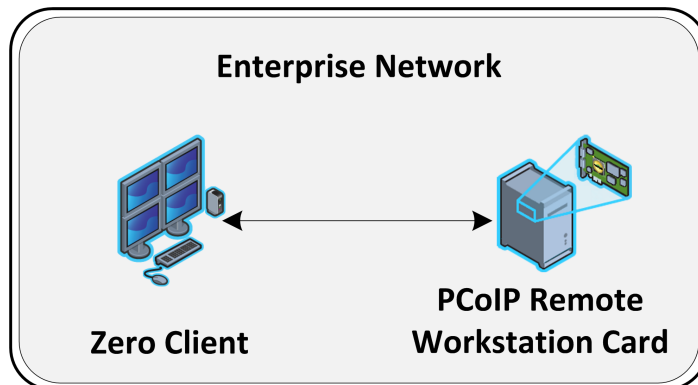
Zero Client to Remote Workstation Card (LAN)

To establish the connection:

1. From the zero client's AWI:

    - Configure the Direct to Host session connection type, and enter the DNS name or IP address of the remote workstation card.

2. From the remote workstation card's AWI:

    - Configure the Direct from Client session connection type, and whether to accept any peer (i.e., zero client) or a specific one.

3. Start a PCoIP session.

4. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

Zero Client to Remote Workstation Card via View Connection Server (LAN)

The figure below shows a zero client establishing a PCoIP session with a remote workstation card from within a LAN using a View Connection Server to connect the endpoints.

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center. This scenario also assumes you have the VMware View Agent software installed on the host PC or workstation. For more information, see "Using PCoIP® Host Cards with VMware View" (TER0911004) in the Teradici Support Documentation Center. Please refer to Connection Prerequisites for other conditions that may apply.

Zero Client to Remote Workstation Card via View Connection Server (LAN)

To establish the connection:

Note: For more information about configuring View Connection Servers, please refer to VMware documentation.

1. From the View Connection Server:

   - Install View Agent on the host workstation.
   - Create a manual pool that is configured to support PCoIP hardware, and then add the workstation to the pool.
   - Ensure that the **Use Secure Tunnel connection to desktop** check box is enabled. (This check box is enabled by default.)
   - Enter the View Connection Server's IP address or domain name for the **External URL** (e.g. **192.168.1.140:443** or **https://myserver.com:443**).

2. From the zero client's AWI:

   - Configure the View Connection Server session connection type, and enter the DNS name or IP address of the View Connection Server.

3. Start a PCoIP session.

Zero Client to Virtual Desktop via View Connection Server (LAN)

The figure below shows a zero client establishing a session with a virtual desktop from within a LAN using a View Connection Server to connect the endpoints.
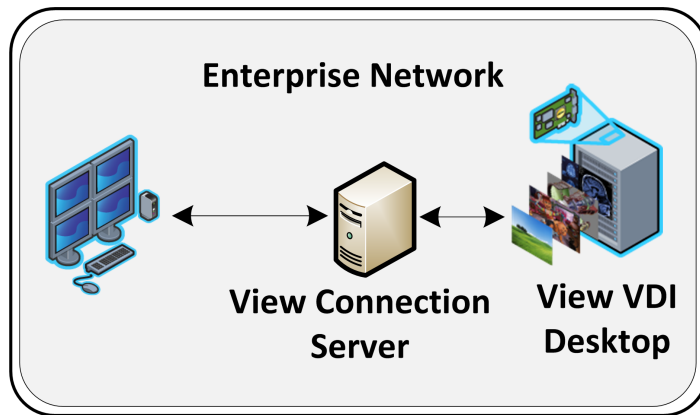
Enterprise Network

View Connection Server

View VDI Desktop

Zero Client to Virtual Desktop via View Connection Server (LAN)

To establish the connection:

Note: For more information about configuring View Connection Servers, please refer to VMware documentation.

1. On the ESXi server:

   - Create a virtual machine (VM).
   - Install Windows and View Agent on the VM.

2. On the View Connection Server:

   - Create a pool, and add the VM to the pool.
   - Ensure that the **Use Secure Tunnel connection to desktop** check box is enabled. (This check box is enabled by default.)
   - Enter the View Connection Server's IP address or domain name for the **External URL** (e.g. **192.168.1.140:443** or **https://myserver.com:443**).

3. From the zero client's AWI:

   - Configure the View Connection Server session connection type, and enter the DNS name or IP address of the View Connection Server.

4. Start a PCoIP session.

5. If necessary, adjust bandwidth and image settings in the PCoIP session variables to optimize performance.

Note: By default, the image settings in the Configure PCoIP image quality levels PCoIP session variable are used to adjust the image quality. However, if you enable the Use image settings from zero client if available parameter in this variable, the image settings you have configured in the zero client's AWI Image page are used instead.

In View 5.2 onwards, image settings are immediately applied when you configure them and then click Apply. This is true whether you are using the image settings from the zero client (i.e., Use image settings from zero client if available is enabled) or from the Configure PCoIP image quality levels PCoIP session variable (i.e., Use image settings from zero client if available is not enabled).

For information on optimizing networks for VMware Horizon connections, please log in to the Teradici Support Site see the following Knowledge Base topics:

- PCoIP session variable settings: KB 15134-276
- Windows desktop experience optimization: KB 15134-242, KB 15134-880

Tera2 Zero Client to PCoIP Workstation Access Software (LAN)

The figure below shows a PCoIP session between a Tera2 zero client and the Teradici PCoIP® Workstation Access Software installed on a workstation. This scenario uses the PCoIP Broker Protocol to connect the endpoints.

See Zero Client–to–PCoIP Workstation Access Software Prerequisites for a list of requirements for this scenario.
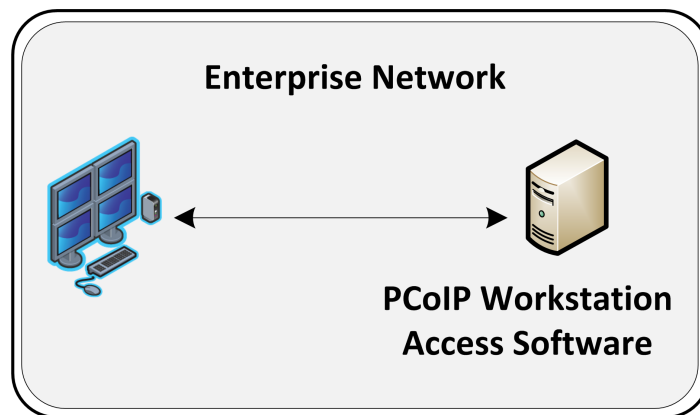
Tera2 Zero Client to PCoIP Workstation Access Software (LAN)

To establish the connection:

1. If you have not installed your own certificates, ensure that your zero client's security mode is *not* set to **Never connect to untrusted servers** on the OSD: Certificate Checking Settings page.

2. Select the Auto Detect or PCoIP Connection Manager session connection type.

3. Enter the fully-qualified computer name or IP address of the host workstation, and then click **OK**.

4. Start a PCoIP session.

For more information about the Teradici PCoIP® Workstation Access Software, please log in to the Teradici Support Site and see the following documentation:

- "Teradici PCoIP® Workstation Access Software User Guide" (TER1405004) in the Teradici Support Documentation Center. Instructions for creating and installing your own certificates for the Teradici PCoIP® Workstation Access Software are also included in this document.

- KB 15134-2055: Describes the firewall rules that are automatically created when the Teradici PCoIP® Workstation Access Software is installed.

Common Remote Access Scenarios

Connecting Remotely

PCoIP sessions between clients and hosts can operate in a wide area network (WAN) that traverses the Internet. You can connect clients and hosts remotely using the following main methods:

- Configuring network address translation (NAT) devices at both ends to implement the necessary IP address and port translation. This method applies only to Tera2 devices that employ UDP-encapsulated IPsec ESP encryption (firmware 4.1.0 or newer).

- Setting up a VPN to connect two trusted networks over an intermediate untrusted network.

- Using a security server/connection server pair to secure and broker the outside client to the trusted inside network.

The scenarios listed below describe some common ways you can connect PCoIP endpoints remotely.

- Scenario 1: Connecting a zero client to a remote workstation card.

- Scenario 2: Connecting a zero client to a remote workstation card over a hardware VPN.

- [Scenario 3](#): Using a third-party broker to connect a zero client to a remote workstation card.

- [Scenario 4](#): Connecting a Tera2 Zero Client to the Teradici PCoIP® Workstation Access Software.

- [Scenario 5](#): Connecting a Tera2 Zero Client to Amazon WorkSpaces.

- [Scenario 6](#): Using a View Security Server/View Connection Server pair to broker a connection between a zero client and a remote workstation card.

- [Scenario 7](#): Using a View Security Server/View Connection Server pair to broker a connection between a zero client and a VMware Horizon virtual desktop.

- [Scenario 8](#): Using a View Security Server/View Connection Server pair to broker a connection between a VMware Horizon software client and a remote workstation card.

- [Scenario 9](#): Using View Connection Servers for remote and internal connections.

Zero Client to Remote Workstation Card (WAN)

As of firmware 4.1.0, Tera2 zero clients and remote workstation cards use [UDP-encapsulated IPsec format](#). Because this encapsulation type supports IP address and port number translation, it is not necessary to set up a VPN when these devices connect remotely. To connect devices with earlier firmware versions, see [Zero Client to Remote Workstation Card Using a Hardware VPN](#).

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support [Documentation Center](#). Please refer to [Connection Prerequisites](#) for other conditions that may apply.

Note: The IP addresses in the following figures are intended as example addresses only.

The figure below shows a Tera2 zero client establishing a PCoIP session with a remote workstation card over a WAN.
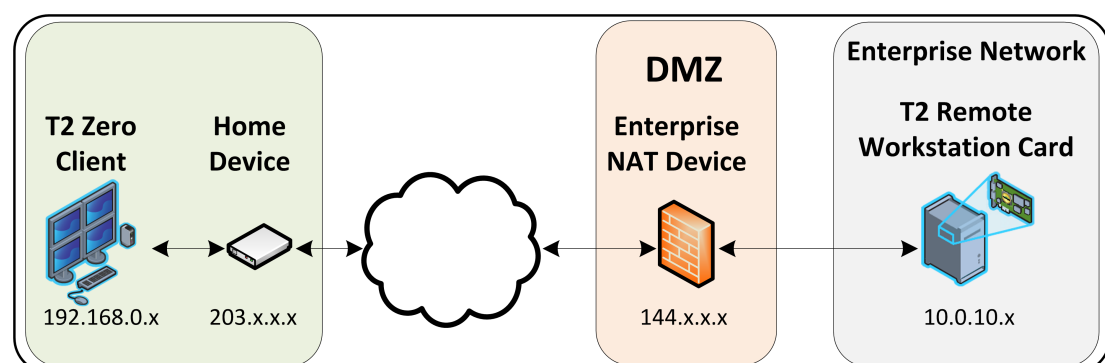
Tera2 Zero Client to Remote Workstation Card (WAN)

You can also have multiple zero clients and remote workstation cards connected behind NAT devices, as shown in the next figure.

Note: In this scenario, an enterprise-level NAT device is required in both the source and destination networks.
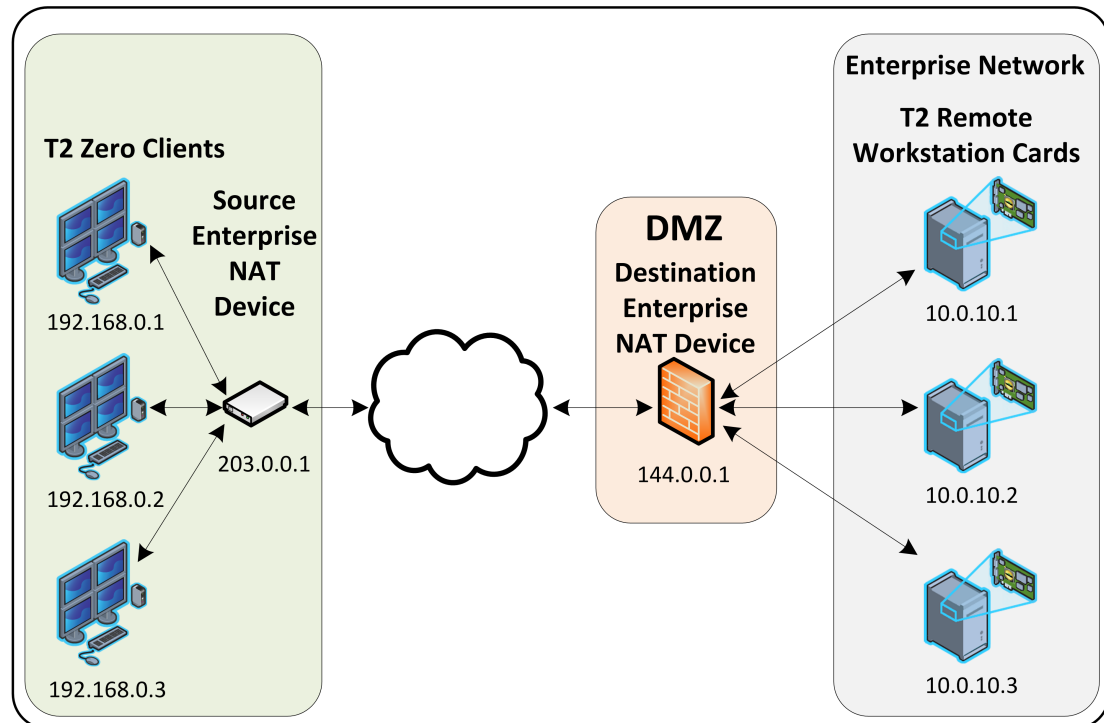
Remote PCoIP Sessions with Multiple Tera2 Devices

To establish the connection:

1. For the first scenario: Configure the enterprise NAT device to redirect TCP/UDP port 4172 to the remote workstation card.
    For the second scenario:

    - Configure the source enterprise NAT device (203.0.0.1) to translate IP address and ports as follows:
      192.168.0.1:4172 to 203.0.0.1:4172
      192.168.0.2:4172 to 203.0.0.1:4173
      192.168.0.3:4172 to 203.0.0.1:4174

    - Configure the destination enterprise NAT device (144.0.0.1) to translate IP addresses and ports as follows:
      144.0.0.1:4172 to 10.0.10.1:4172
      144.0.0.1:4173 to 10.0.10.2:4172
      144.0.0.1:4174 to 10.0.10.3:4172

2. From the zero client's AWI:

   - Configure the Direct to Host session connection type, and enter the IP address of the destination enterprise NAT device.

3. From the remote workstation card's AWI:

   - Configure the Direct from Client session connection type.

4. On your firewall or router, allow both TCP and UDP traffic on the ports you have configured in your NAT devices (4172+).

5. Start a PCoIP session.

6. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For more information on how NAT applications work with PCoIP, please log in to the Teradici Support Site and see KB 15134-18 and KB 15134-1508.

For information on optimizing networks for WAN connections, please log in to the Teradici Support Site and see the following Knowledge Base topics:

- Packet size (MTU) settings: KB 15134-40
- Bandwidth settings: KB 15134-242, KB 15134-88
- Image settings: KB 15134-28, KB 15134-51
- Windows desktop experience optimization: KB 15134-242, KB 15134-880

Zero Client to Remote Workstation Card via Hardware VPN (WAN)

The figure below shows a PCoIP session between a zero client and remote workstation card over a hardware VPN.
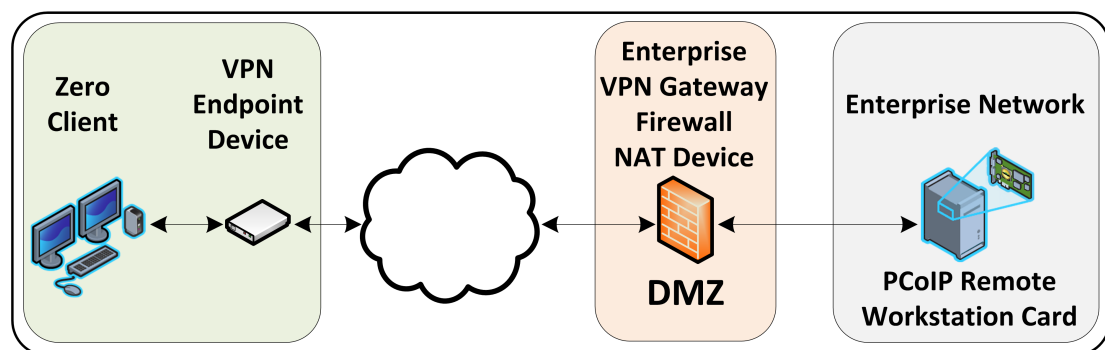
Hardware VPN – Zero Client to Remote Workstation Card (WAN)

A VPN is necessary when connecting the following PCoIP endpoints over the Internet:

- Tera1 zero client to a Tera1 remote workstation card
- Tera2 zero client to a Tera2 remote workstation card when the installed firmware in these devices is prior to release 4.1.0
- Tera2 zero client to a Tera2 remote workstation card when the enterprise NAT device/gateway cannot implement the required IP address and port translation

To establish the connection:

1. At the home network, install a VPN endpoint device (e.g., a router) and establish a VPN session between the endpoint device and the enterprise VPN gateway. For information on how to set up the VPN, please see the documentation for your device.
2. Configure the enterprise VPN gateway/firewall/NAT device to allow IPsec ESP traffic, and also traffic on UDP port 4172 for the PCoIP data stream and on TCP port 4172 for the TCP handshake.
3. From the zero client's AWI:

   - Configure the Direct to Host session connection type, and enter the IP address of the remote workstation card.
   - Configure the address of the home VPN endpoint device as the default gateway.
   - Set the packet MTU to be less than or equal to the largest size supported by the VPN tunnel.

4. From the remote workstation card's AWI:

   - Configure the Direct from Client session connection type.
   - Set the packet MTU to be less than or equal to the largest size supported by the VPN tunnel.

5. Start a PCoIP session.
6. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For information on optimizing networks for WAN connections, please log in to the Teradici Support Site and see the following Knowledge Base topics:

- Packet size (MTU) settings: KB 15134-40
- Bandwidth settings: KB 15134-242, KB 15134-88
- Image settings: KB 15134-28, KB 15134-51
- Windows desktop experience optimization: KB 15134-242, KB 15134-880

Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)

The figure below shows a zero client establishing a PCoIP session with a remote workstation card over a WAN with a 3rd party broker in the enterprise network acting as a connection server.

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center. Please refer to Connection Prerequisites for other conditions that may apply.
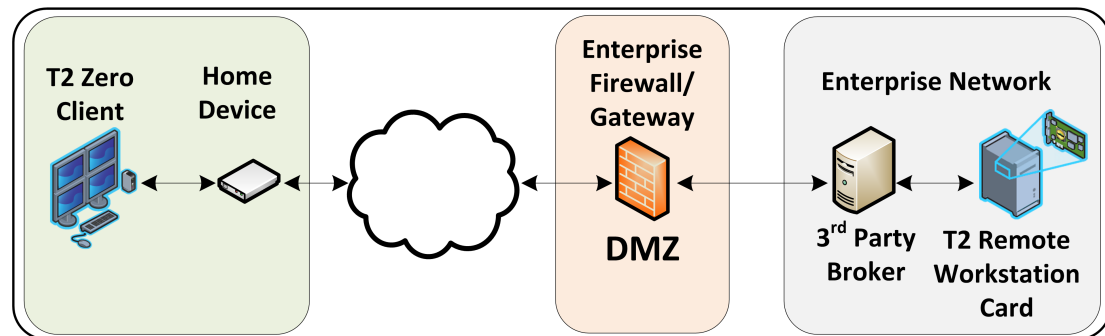
Tera2 Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)

Note: If you are using Tera1 devices, you must first set up a hardware VPN to tunnel from the home device to the enterprise gateway in order for this scenario to work. See Zero Client to Remote Workstation Card Using a Hardware VPN for details.

To establish the connection:

1. Configure the 3rd party broker to redirect traffic from the zero client to the remote workstation card. See documentation for the broker for details.

2. From the zero client's AWI:

   - Configure the Connection Management Interface session connection type, and enter the DNS name or IP address of the connection manager (i.e., the 3rd party broker).

3. From the remote workstation card's AWI:

   - Configure the Connection Management Interface session connection type, and enter the DNS name or IP address of the connection manager.

4. On your firewall or router, allow both TCP and UDP traffic on port 4172.

5. Start a PCoIP session.

6. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For information on optimizing networks for WAN connections, please log in to the Teradici Support Site and see the following Knowledge Base topics:

- Packet size (MTU) settings: KB 15134-40

- Bandwidth settings: KB 15134-242, KB 15134-88

- Image settings: KB 15134-28, KB 15134-51

- Windows desktop experience optimization: KB 15134-242, KB 15134-880

Tera2 Zero Client to PCoIP Workstation Access Software (WAN)

You can connect a Tera2 zero client to the Teradici PCoIP® Workstation Access Software over a WAN by configuring a NAT device to perform the necessary IP address and port translation. This scenario, shown below, uses the PCoIP Broker Protocol to connect the endpoints.
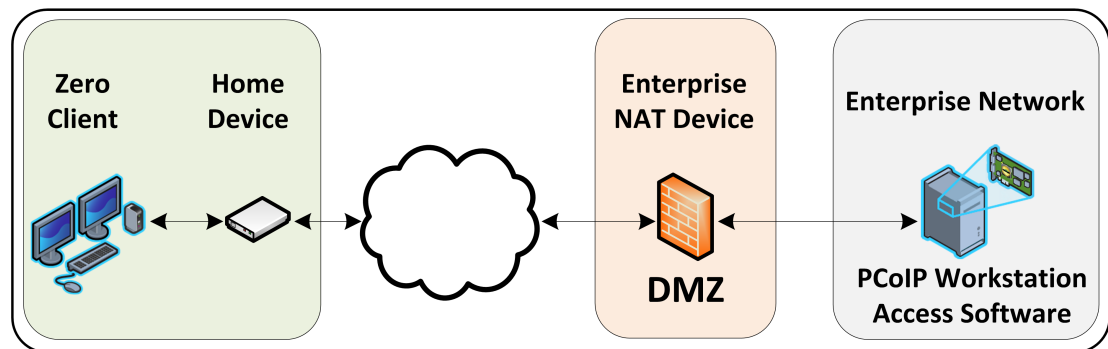
Tera2 Zero Client to PCoIP Workstation Access Software (WAN)

See Zero Client–to–PCoIP Workstation Access Software Prerequisites for a list of requirements for this scenario. In addition, in this release you must also configure the remote workstation with a special registry value. For details, please log in to the Teradici Support Site and see KB 15134-2361.

To establish the connection:

1. Follow KB 15134-2361 to configure a **PCoIPClientConnectionAddress** registry value on the remote workstation with the public IP address of your enterprise NAT router.

2. Before initiating the session, ensure that all prerequisites are in place.

3. If you have not installed your own certificates, ensure that your zero client's security mode is *not* set to **Never connect to untrusted servers** on the OSD: Certificate Checking Settings page.

4. Select the Auto Detect or PCoIP Connection Manager session connection type.

5. Enter the public IP address of your enterprise NAT router, and then click **OK**.

6. Start a PCoIP session.

For more information about the Teradici PCoIP® Workstation Access Software, please log in to the Teradici Support Site and see the following documentation:

- "Teradici PCoIP® Workstation Access Software User Guide" (TER1405004) in the Teradici Support Documentation Center. Instructions for creating and installing your own certificates for the Teradici PCoIP® Workstation Access Software are also included in this document.

- KB 15134-2055: Describes the firewall rules that are automatically created when the Teradici PCoIP® Workstation Access Software is installed.

Tera2 Zero Client to Amazon WorkSpaces (WAN)

The figure below shows a zero client establishing a connection with an Amazon WorkSpaces desktop using a PCoIP® Connection Manager for Amazon WorkSpaces appliance installed in a Virtual Private Cloud (VPC) to authenticate the user and provision the WorkSpace.

Note: Locating the PCoIP® Connection Manager for Amazon WorkSpaces in a VPC is just one way to deploy the appliance. Your company may use a different deployment. For details on how to install and configure the appliance, please see "Connecting PCoIP® Zero Clients to Amazon WorkSpaces" (TER1408002) in the Teradici Support Documentation Center. Providing instructions on how to connect your local network to Amazon WorkSpaces is beyond the scope of this document. Please refer to AWS documentation for information.
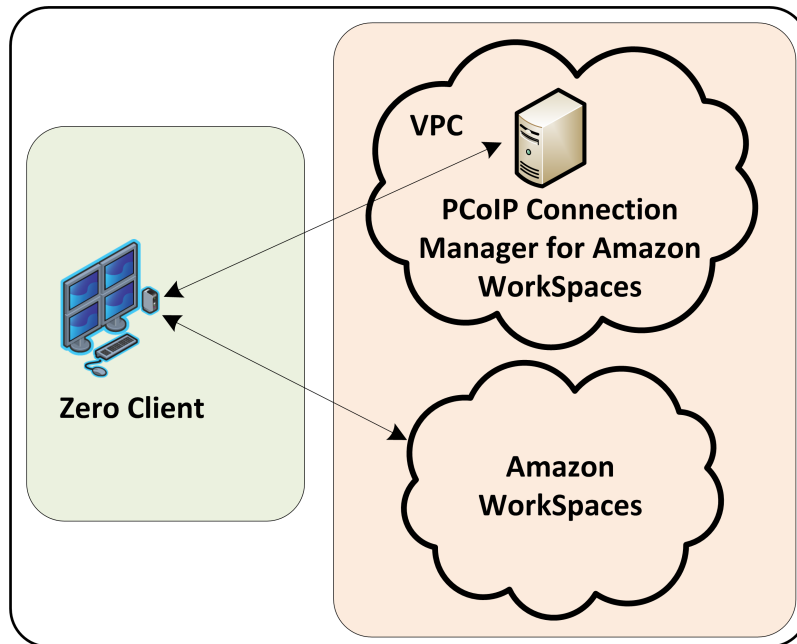
Tera2 Zero Client to Amazon WorkSpaces

See Zero Client–to–Amazon WorkSpaces Prerequisites for a list of requirements for this scenario.

To establish the connection:

1. Before initiating a session, ensure that all prerequisites are in place.
2. If you have not installed your own certificates, ensure that your zero client's security mode is *not* set to **Never connect to untrusted servers** on the OSD: Certificate Checking Settings page.
3. Select the Auto Detect or PCoIP Connection Manager session connection type.
4. Enter the URI (https://*<IP address>*) of your PCoIP® Connection Manager for Amazon WorkSpaces, and then click **OK**.
5. Start a PCoIP session.

For detailed instructions on how to connect a Tera2 zero clients to Amazon WorkSpaces, please refer to "Connecting PCoIP® Zero Clients to Amazon WorkSpaces" (TER1408002) in the Teradici Support Documentation Center.

Zero Client to Remote Workstation Card via View Security Server (WAN)

The figure below shows a zero client establishing a PCoIP session with a remote workstation card over a WAN using a View Security Server and View Connection Server pair to authenticate and connect the endpoints.

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center. This scenario also assumes you have the VMware View Agent software installed on the host PC or workstation. For more information, see "Using PCoIP® Host Cards with VMware View" (TER0911004) in the Teradici Support Documentation Center. Please refer to Connection Prerequisites for other conditions that may apply.

Zero Client to Remote Workstation Card via View Security/Connection Server

To establish the connection:

Note: For more information about configuring View Connection Servers, please refer to VMware documentation.

1. On the View Connection Server:

   - Install View Agent on the host workstation.
   - Create a manual pool that is configured to support PCoIP hardware, and then add the workstation to the pool.
   - Define the pairing password (and pairing timeout) that will be used to pair the View Connection Server and View Security Server.

2. On the View Security Server:

   - Pair the View Security Server with the View Connection Server.
   - Enable the **Use Secure Tunnel connection to desktop** and **Use PCoIP Secure Gateway for PCoIP connections to desktop** check boxes.
   - Enter the View Security Server's IP address for the **External URL** (e.g., **https://12.50.16.151:443**) and for the **PCoIP External URL** (e.g.,**12.50.16.151:4172**). This is the WAN-facing address that remote clients can resolve. Only the port number is different for the two addresses.

3. On your firewall or router:

- Allow both TCP and UDP traffic on port 4172 and TCP traffic on port 443.

4. From the zero client's AWI:

- Configure the View Connection Server session connection type, and enter the DNS name or external IP address of the View Security Server.

5. Start a PCoIP session.

6. If necessary, adjust bandwidth and image parameters on both the host and client to optimize performance.

For information on optimizing networks for VMware Horizon connections, please log in to the Teradici Support Site and see the following Knowledge Base topics:

- PCoIP session variable settings: KB 15134-276
- Windows desktop experience optimization: KB 15134-880

Zero Client to Virtual Desktop via View Security Server (WAN)

The figure below shows a zero client establishing a PCoIP session with a virtual desktop over a WAN using a View Security Server and View Connection Server pair to authenticate and connect the endpoints.
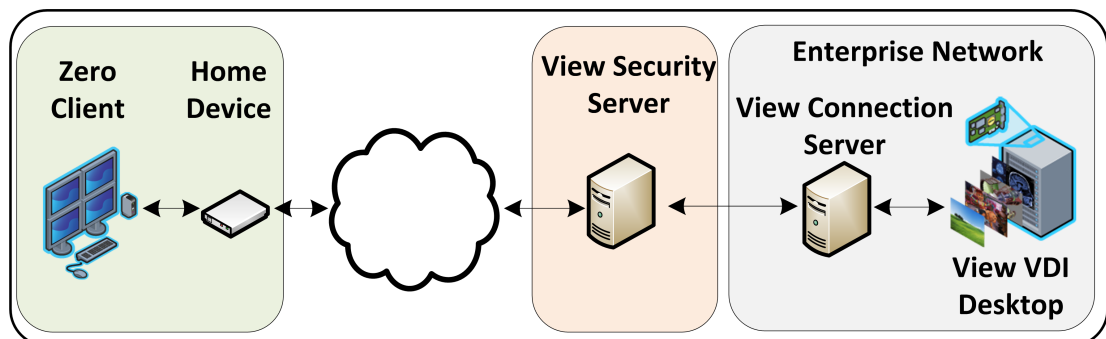
Zero Client to VDI Desktop via View Security/Connection Server

To establish the connection:

Note: For more information about configuring View Connection Servers, please refer to VMware documentation.

1. On the ESXi server:

- Create a virtual machine (VM).
- Install Windows and View Agent on the VM.

2. On the View Connection Server:

   - Create a pool, and add the VM to the pool.
   - Define the pairing password (and pairing timeout) that will be used to pair the View Connection Server and View Security Server.

3. On the View Security Server:

   - Pair the View Security Server with the View Connection Server.
   - Enable the **Use Secure Tunnel connection to desktop** and **Use PCoIP Secure Gateway for PCoIP connections to desktop** check boxes.
   - Enter the View Security Server's IP address for the **External URL** (e.g., **https://12.50.16.151:443**) and for the **PCoIP External URL** (e.g.,**12.50.16.151:4172**). This is the WAN-facing address that remote clients can resolve. Only the port number is different for the two addresses.

4. On your firewall or router:

   - Allow both TCP and UDP traffic on port 4172, and TCP traffic on port 443.

5. From the zero client's AWI:

   - Configure the View Connection Server session connection type, and enter the DNS name or external WAN IP address of the View Security Server.

6. Start a PCoIP session.

7. If necessary, adjust bandwidth and image settings in the PCoIP session variables to optimize performance.

Note: By default, the image settings in the Configure PCoIP image quality levels PCoIP session variable are used to adjust the image quality. However, if you enable the Use image settings from zero client if available parameter in this variable, the image settings you have configured in the zero client's AWI Image page are used instead.

In View 5.2 onwards, image settings are immediately applied when you configure them and then click Apply. This is true whether you are using the image settings from the zero client (i.e., Use image settings from zero client if available is enabled) or from the Configure PCoIP image quality levels PCoIP session variable (i.e., Use image settings from zero client if available is not enabled).

For information on optimizing networks for VMware Horizon connections, please log in to the Teradici Support Site see the following Knowledge Base topics:

- PCoIP session variable settings: KB 15134-276
- Windows desktop experience optimization: KB 15134-242, KB 15134-880

VMware Horizon Software Client to Remote Workstation Card via View Security Server (WAN)

The figure below shows a a VMware Horizon software client establishing a PCoIP session with a remote workstation card over a WAN using a View Security Server and View Connection Server pair to authenticate and connect the endpoints.

Note: All remote workstation card scenarios assume you have the PCoIP host software installed on the host PC or workstation. For details, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center. This scenario also assumes you have the VMware View Agent software installed on the host PC or workstation (see "Using PCoIP® Host Cards with VMware View" (TER0911004) in the Teradici Support Documentation Center) and a View software client installed on your client device (see VMware documentation). Please refer to Connection Prerequisites for other conditions that must be met.
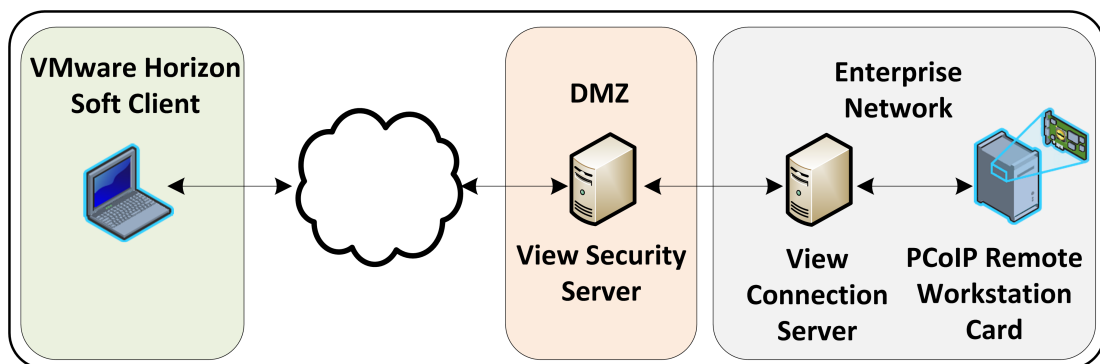
VMware Horizon Soft Client to Remote Workstation Card via View Security Server

To establish the connection:

Note: For more information about configuring View Connection Servers, please refer to VMware documentation.

1. On the View Connection Server:

   - Install View Agent on the host workstation.
   - Create a manual pool that is configured to support PCoIP hardware, and then add the workstation to the pool.
   - Define the pairing password (and pairing timeout) that will be used to pair the View Connection Server and View Security Server.

2. On the View Security Server:

   - Pair the View Security Server with the View Connection Server.

   - Enable the **Use Secure Tunnel connection to desktop** and **Use PCoIP Secure Gateway for PCoIP connections to desktop** check boxes.

   - Enter the View Security Server's IP address for the **External URL** (e.g., **https://12.50.16.151:443**) and for the **PCoIP External URL** (e.g.,**12.50.16.151:4172**). This is the WAN-facing address that remote clients can resolve. Only the port number is different for the two addresses.

3. On your firewall or router:

   - Allow both TCP and UDP traffic on port 4172 and TCP traffic on port 443.

4. From the VMware Horizon soft client:

   - Configure the DNS name or external IP address of the View Security Server.

   - Set the desired certificate checking mode.

5. [Start a PCoIP session](#).

6. If necessary, adjust [bandwidth](#) and [image](#) parameters on both the host and client to optimize performance.

For information on optimizing networks for VMware Horizon connections, please log in to the Teradici [Support Site](#) and see the following Knowledge Base topics:

- PCoIP session variable settings: [KB 15134-276](#)
- Windows desktop experience optimization: [KB 15134-880](#)

Internal vs. External Zero Client to Remote Workstation Card Connections Using View Connection Servers

To avoid limiting session bandwidth for LAN connections, it is recommended to use different View Connection Servers for internal and external connections. The scenario below shows a PCoIP session between a remote workstation card and remote zero client over a WAN (#1) and an alternative configuration for a PCoIP session between the remote workstation card and an internal zero client that is situated within the LAN (#2).
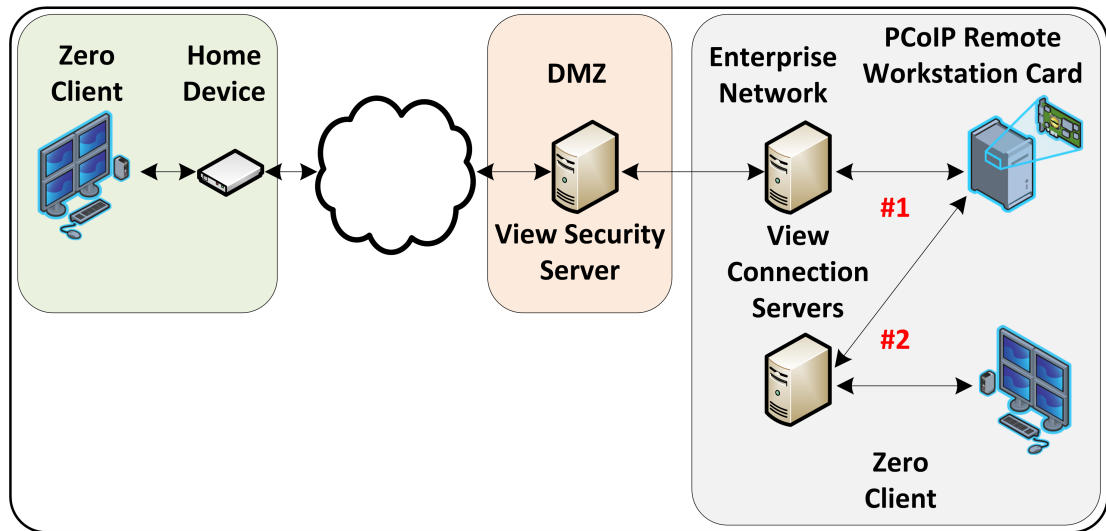
For internal and external scenarios:

- To configure the remote connection, see Zero Client to Remote Workstation Card via View Security Server (WAN).
- To configure the LAN connection, see Zero Client to Remote Workstation Card via View Connection Server (LAN).

Note: For details about encryption and bandwidth metrics for different types of PCoIP sessions, please log in to the Teradici Support Site and see KB 15134-1389.

Security Considerations

PCoIP Zero Client Security Overview

PCoIP zero clients are ultra-secure, easy to manage devices that offer a rich user experience. Based on the TERA chipset by Teradici, they are available in a variety of form factors from a number of trusted OEMs. For example, PCoIP zero clients can be standalone desktop devices, integrated monitors, touch screen displays, and IP phones. With embedded hardware support for PCoIP and no local storage, they are the most trusted client wherever security and performance are critical.

Data Control

When control and lockdown of sensitive data are a primary objective, PCoIP zero clients enable an environment where no application data ever leaves the data center. The virtual machine sends only encrypted PCoIP data to the client. PCoIP zero clients have no local storage, and no sensitive application data is ever processed or stored on the client.

Zero clients also have many security-related settings that are frequently used in high security deployments.

User Authentication

PCoIP zero clients support a number of third-party, hardware-based, user authentication methods including the following:

- SIPR hardware tokens
- Common Access Card (CAC) and Personal Identity Verfication (PIV) smart cards
- SafeNet eToken
- RSA SecurID
- Proximity cards (Imprivata)

For a complete list of supported authentication methods, see KB 15134-299 in the Teradici Support Site.

Encryption

PCoIP zero clients support the following encryption types.

Session negotiation security:

- TLS 1.0 with AES-128-CBC-SHA
- TLS 1.0 with AES-256-CBC-SHA
- Suite B (in hardware host environments only)

Session security:

- AES-128-GCM
- AES-256-GCM
- Salsa20-256-Round12

Zero clients themselves also employ encryption to ensure that information is protected. In the media stream, all media data is encrypted as it moves from the server to the client. This includes display data, USB data, and audio network traffic. In the management channel, all management data is encrypted.

802.1x Network Authentication

PCoIP zero clients support 802.1x network device authentication using EAP-TLS certificates. With 802.1x network authentication, all network end devices must be authenticated before they are granted access to the network. This is a typical method of device authentication for high security environments, providing an additional layer of security beyond username and password credentials.

See Configuring 802.1x Network Device Authentication in the "How To" section for instructions on how to configure zero clients for this type of authentication.

Security Settings Checklist

The table below provides a list of zero client security settings that are frequently used in high security deployments. Your network administrator or your security advisor must determine whether these settings are appropriate for your own network environment.

The links in the **Configuration Category** column below take you to the Management Console page where you can configure the setting for a zero client profile. For instructions on how to enable and configure a setting, see MC Manage Profiles Page.

Note: Many of these settings can also be configured through the AWI or OSD.

Zero Client MC Security Settings

PCoIP Zero Client Security Settings Checklist

Configuration Category	Setting Name	Setting
Network Configuration	Enable SNMP	False
Discovery Configuration	Enable SLP Discovery	False
Session Configuration	Session Connection Type	PCoIP Connection Manager or View Connection Server
	Enable View Connection Server SSL	True Note: This setting only applies to devices with firmware versions prior to 4.0.0. From 4.0.0 on, SSL communication is always used.
	Certificate Check Mode	Reject the unverifiable connection (Secure)
	Certificate Check Lockout Mode	Locked
	Clear Trusted Connection Server Cache	Clear Cache
	Connection Server Cache Mode	Last servers used

⠀

Configuration Category	Setting Name	Setting
	Connection Server Cache Entry (1-25)	Enter the allowed PCoIP Connection Manager or View Connection Server address(es)
	Enable Login Username Caching	False
Encryption Configuration	Session Negotiation Security Level	Maximum Compatibility - in software or mixed host environments Suite B - in hardware-only remote workstation card environments
	T2 Enable AES-128-GCM	True
	T2 Enable AES-256-GCM	True
	T1 Enable AES-128-GCM	True
	T1 Enable Salsa20-256-Round12	True - in software or mixed host environments False - in hardware-only remote workstation card environments
OSD Configuration	Hidden Menu Entries	Hide menus (as desired)
Time Configuration	NTP Server Hostname	<NTP server address>
Security Configuration	Password	Create a password in accordance with the local security policy
	Enable Password Protection	True. This enables password protection for the AWI and the OSD.
	Enable Web Interface	False (disable the web UI if desired)
	Enable Hotkey Parameter Reset	False
	Enable 802.1x Security	True
	Enable 802.1x Authentication Identity	Enter the username configured for the 802.1x authentication.

Configuration Category	Setting Name	Setting
Profile Zero Client USB Authorization /Unauthorization	Example: To allow USB access to HID devices only, click **Add New** and configure these settings:	**Authorized**: Rule Type: **Class** Device Class: **Human Interface Device** Sub Class: **Any** Protocol: **Any** **Unauthorized**: No unauthorization rules. Delete any existing rules. When there are no rules, the MC displays two radio buttons on the **Manage Profiles** page. Select **Erase the device's existing USB unauthorizations and replace them with an empty set**.
	Example: To allow USB access to all devices except mass storage, click **Add New** and configure these settings.	**Authorized**: Rule Type: **Class** Device Class: **Any** Sub Class: **Any** Protocol: **Any** **Unauthorized**: Rule Type: **Class** Device Class: **Mass Storage** Sub Class: **Any** Protocol: **Any**
Certificate Store		VCS certificate issuer (root or intermediate) or VCS certificate. Note that SSL certificates are required in VMware View 5.1 and newer versions. If SSL is turned off in firmware version FW4.0 and older, passwords are sent unencrypted over the network.

Zero Client Smart Card/Hardware Token Configuration

Typically, no configuration is required on the zero client side for the following:

- CAC and PIV smart card user authentication
- SIPR hardware token user authentication

However, for CAC cards that support both the modern PIV and the old-style CAC (GSC-IS) command sets, administrators may want to enable the **Prefer GSC-IS over PIV Endpoint** check box in the MC, AWI, and OSD **View Connection Server** and **View Connection Server + Imprivata Onesign** windows.

GUI Reference

Initial Setup

AWI Host: Initial Setup Page

You can access this page from the **Configuration > Initial Setup** menu.

AWI Host Initial Setup Page

Audio Parameters

Parameter	Description
Enable HD Audio	Enables audio support on the host or client.
Enable Audio Line In	**Enable:** Use the line-in connector found on the client. **Disable:** Use the line-in connector as a microphone input. Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device.

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

Session Parameters

Parameter	Description
Accept Any Client	Lets the host accept any client for a PCoIP session.
Client MAC Address	Lets you specify the client MAC address for a PCoIP session. Note: You cannot set the client MAC address to 00-00-00-00-00-00.

AWI Client: Initial Setup Page

You can access this page from the **Configuration > Initial Setup** menu.

AWI Client Initial Setup Page

Audio Parameters

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

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

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.

Note: When host discovery or connection management is configured on the client, you cannot modify the client session parameters. A message appears on the **Initial Setup Client** page instead of the session parameters.

Configuring the Network

MC: Network Settings

The settings on this page let you configure a profile with the Dynamic Host Configuration Protocol (DHCP), Maximum Transmission Unit (MTU), and Simple Network Managment Protocol parameters.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
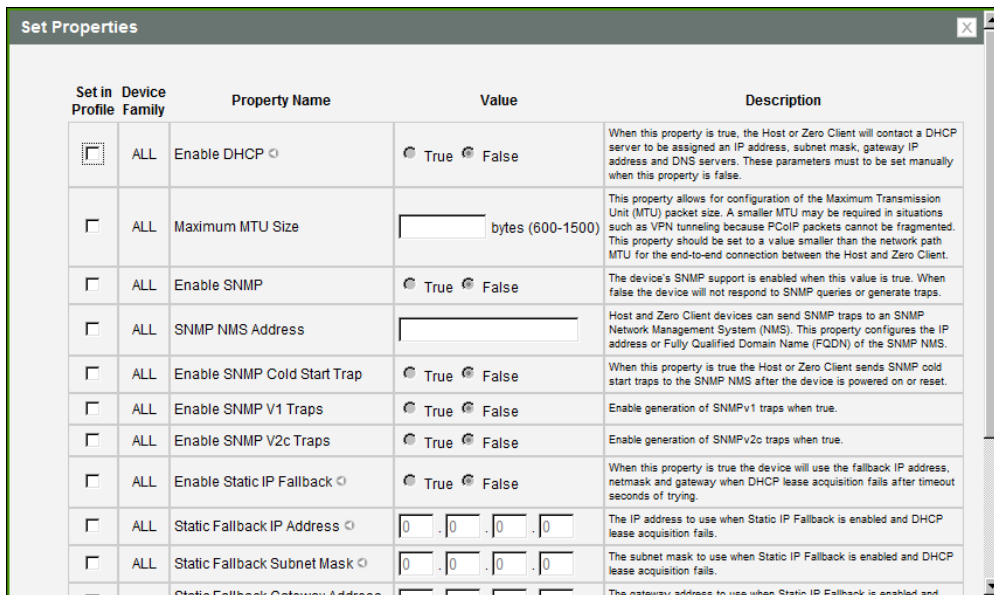
MC Network Configuration

MC Network Configuration Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN).
	When disabled, you must set these parameters manually.
	Note: For MC discovery, the device also requests vendor class options 60/43.
	Note: This property requires a device restart after being changed.
Maximum MTU Size	Lets you configure the **Maximum Transfer Unit** packet size.
	A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client.
	The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.
Enable SNMP	When enabled, the device enables the PCoIP SNMP agent to respond to SNMP requests. Disabling the SNMP agent prevents it from responding to SNMP requests and from generating traps. It also ensures that the PCoIP SNMP MIB cannot be accessed.
SNMP NMS Address	If you want the device to send SNMP traps to an SNMP Network Management System (NMS), enter the IP address or fully qualified domain name (FQDN) of the SNMP NMS.
Enable SNMP Cold Start Trap	When enabled, the device sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset.
Enable SNMP V1 Traps	When enabled, allows generation of SNMPv1 traps.
Enable SNMP V2c Traps	When enabled, allows generation of SNMPv2c traps.
Enable Static IP Fallback	When enabled, the device will use the fallback IP address, netmask and gateway when DHCP lease acquisition fails after timeout seconds of trying.
	Note: This property requires a device restart after being changed.
Static Fallback IP Address	Configures the IP address to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails.
	Note: This property requires a device restart after being changed.

Parameter	Description
Static Fallback Subnet Mask	Configures the subnet mask to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails. Note: This property requires a device restart after being changed.
Static Fallback Gateway Address	Configures the gateway address to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails. Note: This property requires a device restart after being changed.
Static Fallback Timeout	Configures the amount of time in seconds the device will attempt to acquire a DHCP lease before using the fallback address configuration. You must enter a value greater than or equal to 60. Note: It may take up to 30 seconds longer than this value for the fallback configuration to become active. Note: This property requires a device restart after being changed.
SNMP Community Name	Configures the SNMP community name used by the device.

AWI: Client Network Settings

This page lets you configure network settings for the client. You can access this page from the **Configuration > Network** menu. After you update the parameters on this page, click **Apply** to save your changes.

Note: You can also configure network information from the client's **Initial Setup** page.

AWI Network Page

AWI Network Page Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN). When disabled, you must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field. Warning: It is possible to configure an illegal IP address/subnet mask combination (e.g., invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.

Parameter	Description
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 named of the device (e.g., "domain.local"). This field is optional.
FQDN	The fully qualified domain name for the device. The default is pcoip-host-<*MAC*> or pcoip-portal-<*MAC*> where <*MAC*> is the device's MAC address. If used, the domain name is appended (for example, pcoip-host-<*MAC*>.domain.local). This field is read-only on this page. Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.
Ethernet Mode	Lets you configure the Ethernet mode of the device as follows: • **Auto** • **100 Mbps Full-Duplex** • **10 Mbps Full-Duplex** When you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and then click **Apply**, the following warning message appears: "Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?" Click **OK** to change the parameter. Note: You should always set the Ethernet mode to **Auto** and only use **10 Mbps Full-Duplex** or **100 Mbps Full-Duplex** when the other network equipment (e.g., a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.

Parameter	Description
Maximum MTU Size	Lets you configure the **Maximum Transfer Unit** packet size. A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client. The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.
Enable 802.1X Security	Enable this field for each of your devices if your network uses 802.1x security to ensure that only authorized devices access the network. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields.
Authentication	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.
Identity	Enter the identity string used to identify your device to the network.
Client Certificate	Click **Choose** to select the client certificate you want to use for your 802.1x devices. The list of certificates that appears includes the certificates uploaded from the **Certificate Upload** page that contain a private key. The certificate you choose from the **Network** page is linked to the read-only **Client Certificate** field on the **Certificate Upload** page. Note: PCoIP only supports one 802.1x client certificate. Ensure your security details are all contained within the one file. The 802.1x certificate must contain a private key.
Enable 802.1X Support for Legacy Switches	When enabled, allows greater 802.1x compatability for older switches on the network.

AWI: Host Network Settings

This page lets you configure network settings for the host. You can access this page from the **Configuration > Network** menu. After you update the parameters on this page, click **Apply** to save your changes.

Note: You can also configure network information from the host's **Initial Setup** page.

Network

Change the network settings for the device

Enable DHCP:	☑
IP Address:	10 . 0 . 8 . 28
Subnet Mask:	255 . 255 . 255 . 0
Gateway:	10 . 0 . 8 . 1
Primary DNS Server:	192 . 168 . 1 . 50
Secondary DNS Server:	192 . 168 . 1 . 52
Domain Name:	teradici.local
FQDN:	pcoip-host-0030040e638c.teradici.local
Ethernet Mode:	Auto
Enable Gigabit Auto-Negotiation:	☑
Prefer Master for Auto-Negotiation:	☐
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

AWI Network Page Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN). When disabled, you must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field. Warning: It is possible to configure an illegal IP address/subnet mask combination (e.g., invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.

Parameter	Description
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 named of the device (e.g., "domain.local"). This field is optional.
FQDN	The fully qualified domain name for the device. The default is pcoip-host-<*MAC*> or pcoip-portal-<*MAC*> where <*MAC*> is the device's MAC address. If used, the domain name is appended (for example, pcoip-host-<*MAC*>.domain.local). This field is read-only on this page. Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.
Ethernet Mode	Lets you configure the Ethernet mode of the device as follows: ● **Auto** ● **100 Mbps Full-Duplex** ● **10 Mbps Full-Duplex** When you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and then click **Apply**, the following warning message appears: "Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?" Click **OK** to change the parameter. Note: You should always set the Ethernet mode to **Auto** and only use **10 Mbps Full-Duplex** or **100 Mbps Full-Duplex** when the other network equipment (e.g., a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.

Parameter	Description
Enable Gigabit Auto-Negotiation (Tera2 only)	Lets you select the maximum negotiated speed of the network interface. When enabled (the default), the maximum possible speed is 1 Gbps. When disabled, it is 100 Mbps. Note: You may want to disable this feature on the host card if you are experiencing Ethernet packet loss (which can result in loss of network connectivity and PCoIP session loss). This scenario can be caused by Ethernet cabling that is not up to Gigabit Ethernet specification (e.g., old building wiring composed of Cat5 cable). Out-of-specification cable will often still successfully auto-negotiate to 1 Gbps speed, but may subsequently have CRC errors during normal operation. Disabling Gigabit Auto-Negotiation prevents the network interface from advertising to its peer on the network that it supports Gigabit Ethernet operation, and so the maximum possible negotiated speed drops to the next level (100 Mbps).
Prefer Master for Auto-Negotiation (Tera2 only)	When enabled, this setting makes the remote workstation card the master for auto-negotiation. It can be used when a client is connected directly to a remote workstation card without an intervening switch.
Maximum MTU Size	Lets you configure the **Maximum Transfer Unit** packet size. A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client. The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.
Enable 802.1X Security	Enable this field for each of your devices if your network uses 802.1x security to ensure that only authorized devices access the network. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields.
Authentication	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.
Identity	Enter the identity string used to identify your device to the network.

Parameter	Description
Client Certificate	Click **Choose** to select the client certificate you want to use for your 802.1x devices. The list of certificates that appears includes the certificates uploaded from the **Certificate Upload** page that contain a private key. The certificate you choose from the **Network** page is linked to the read-only **Client Certificate** field on the **Certificate Upload** page. Note: PCoIP only supports one 802.1x client certificate. Ensure your security details are all contained within the one file. The 802.1x certificate must contain a private key.
Enable 802.1X Support for Legacy Switches	When enabled, allows greater 802.1x compatability for older switches on the network.

OSD: Network Settings

This page lets you configure network settings for the client. You can access this page from the **Options > Configuration > Network** menu. After you update the parameters on this page, click **Apply** to save your changes.

OSD Network Page

OSD Network Page Parameters

Parameter	Description
Enable DHCP	When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN). When disabled, you must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field. Warning: It is possible to configure an illegal IP address/subnet mask combination (e.g., invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain named of the device (e.g., "domain.local"). This field is optional.
FQDN	The fully qualified domain name for the device. The default is pcoip-host-<*MAC*> or pcoip-portal-<*MAC*> where <*MAC*> is the device's MAC address. If used, the domain name is appended (for example, pcoip-host-<*MAC*>.domain.local). This field is read-only on this page. Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.

Parameter	Description
Ethernet Mode	Lets you configure the Ethernet mode of the device as follows: • **Auto** • **100 Mbps Full-Duplex** • **10 Mbps Full-Duplex** When you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and then click **Apply**, the following warning message appears: "Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?" Click **OK** to change the parameter. Note: You should always set the Ethernet mode to **Auto** and only use **10 Mbps Full-Duplex** or **100 Mbps Full-Duplex** when the other network equipment (e.g., a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.
Enable 802.1X Security	Enable this field for each of your devices if your network uses 802.1x security to ensure that only authorized devices access the network. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields.
Authentication	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.
Identity	Enter the identity string used to identify your device to the network.
Client Certificate	Click **Choose** to select the client certificate you want to use for your 802.1x devices. The list of certificates that appears includes the certificates uploaded from the **Certificate Upload** page that contain a private key. The certificate you choose from the **Network** page is linked to the read-only **Client Certificate** field on the **Certificate Upload** page. Note: PCoIP only supports one 802.1x client certificate. Ensure your security details are all contained within the one file. The 802.1x certificate must contain a private key.

Configuring USB

MC: Help for USB Settings

USB configuration settings for the MC (**Force Local Cursor Visible** and **Enable USB EHCI**) are located on the MC: Peripheral Settings page.

AWI Tera2 Client: USB Settings

The **USB** page lets you configure settings for devices plugged into zero client USB ports. You can access this page for the host or client from the **Configuration > USB** menu.

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.*

[Apply] [Cancel]
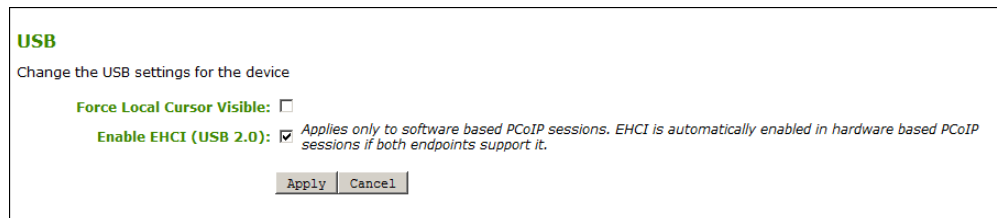
AWI USB Page

AWI USB Page Parameters

Parameter	Description
Force Local Cursor Visible (Tera2 only)	When enabled, the 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.
Enable EHCI (USB 2.0)	Enable this field to configure EHCI (USB 2.0) for devices connected directly to zero client USB ports for sessions with a host running VMware View 4.6 or newer.

Note: This setting applies only to software-based PCoIP sessions. EHCI is automatically enabled in hardware-based PCoIP sessions if both endpoints support it.

Note: 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. |

Label Settings

AWI: Label Settings

The **Label** page lets you assign a device name to the device. You can access this page for the host or client from the **Configuration > Label** menu.

Label

Change the PCoIP device labels

PCoIP Device Name: `pcoip-portal-0030040ddbbc`

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

PCoIP Device Description:

Generic Tag:

Apply Cancel

AWI Label Page

AWI Label Page Parameters

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

OSD: Label Settings

The **Label** page lets you assign a device name to the device. You can access this page from the **Options > Configuration > Label** menu.

OSD Label Page

OSD Label Page Parameters

Parameter	Description
PCoIP Device Name	Lets you give the host or client a logical name. The default is pcoip-host-<*MAC*> or pcoip-portal-<*MAC*>, where <*MAC*> is the device's MAC address.
	This field is the name the host or client registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server.
	It's important to ensure that the **PCoIP Device Name** is unique for each endpoint in the network and follows these naming conventions:
	• The first and last character must be a letter (A-Z or a-z) or a digit (0-9).
	• The remaining characters must be letters, digits, hyphens, or underscores.
	• The length must be 63 characters or fewer.

Parameter	Description
PCoIP Device Description	A description of the device or other information, such as the location of the device's endpoint. Note: The firmware does not use this field. It is provided for administrator use only.
Generic Tag	Generic tag information about the device. Note: The firmware does not use this field. It is provided for administrator use only.

Access Settings

MC: Help for Access Settings

Administrative access settings for the Management Console are located on the following pages:

- Hiding the OSD **Configuration** menu: see **Hide Options -> Configuration** on the OSD Settings page
- Disabling the AWI: see **Enable Web Interface** on the Security Settings page.
- Disabling the management console interface: see **Disable Management Console Interface** on the Security Settings page.

Note: At least one of the device's three management configuration interfaces (OSD, AWI, or MC) must remain enabled at all times.

AWI: Access Settings

The **Access** page lets you prevent the device from being managed by the MC (or any other PCoIP device management tool), and lets you disable administrative access to the device's AWI. It also provides an option to force an administrative password change the next time the AWI or OSD is accessed.

You can access this page from the **Configuration > Access** menu.

Note: At least one of the device's three management configuration interfaces (OSD, AWI, or MC) must remain enabled at all times. If the device has its OSD **Configuration** menu hidden (see MC OSD Settings), you will receive an error message if you try to disable both the MC interface and the AWI from this page. In this situation, only one of these interfaces can be disabled.
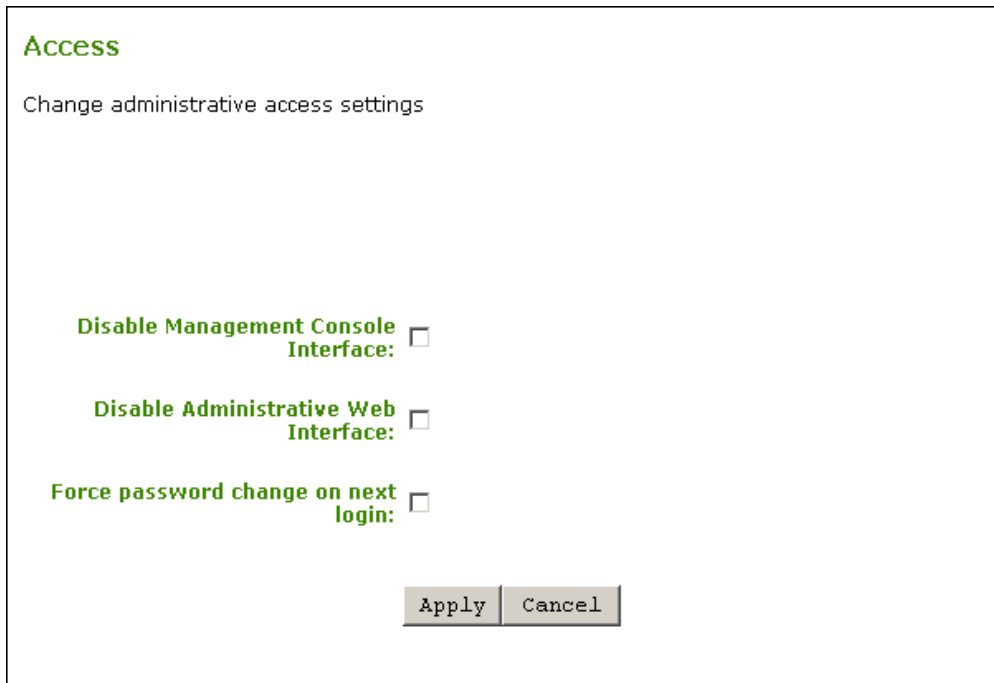
AWI Access Page

AWI Access Page Parameters

Parameter	Description
Disable Management Console Interface	When enabled, the management console interface is disabled, and the device cannot be accessed or managed by the MC (or any other PCoIP device management tool).
Disable Administrative Web Interface	When enabled, the device cannot be accessed or managed 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.

OSD: Access Settings

The **Access** page lets you prevent the device from being managed by the MC (or any other PCoIP device management tool), and lets you disable administrative access to the device's AWI. It also provides an option to force an administrative password change the next time the AWI or OSD is accessed.

You can access this page from the **Options > Configuration > Access** menu.
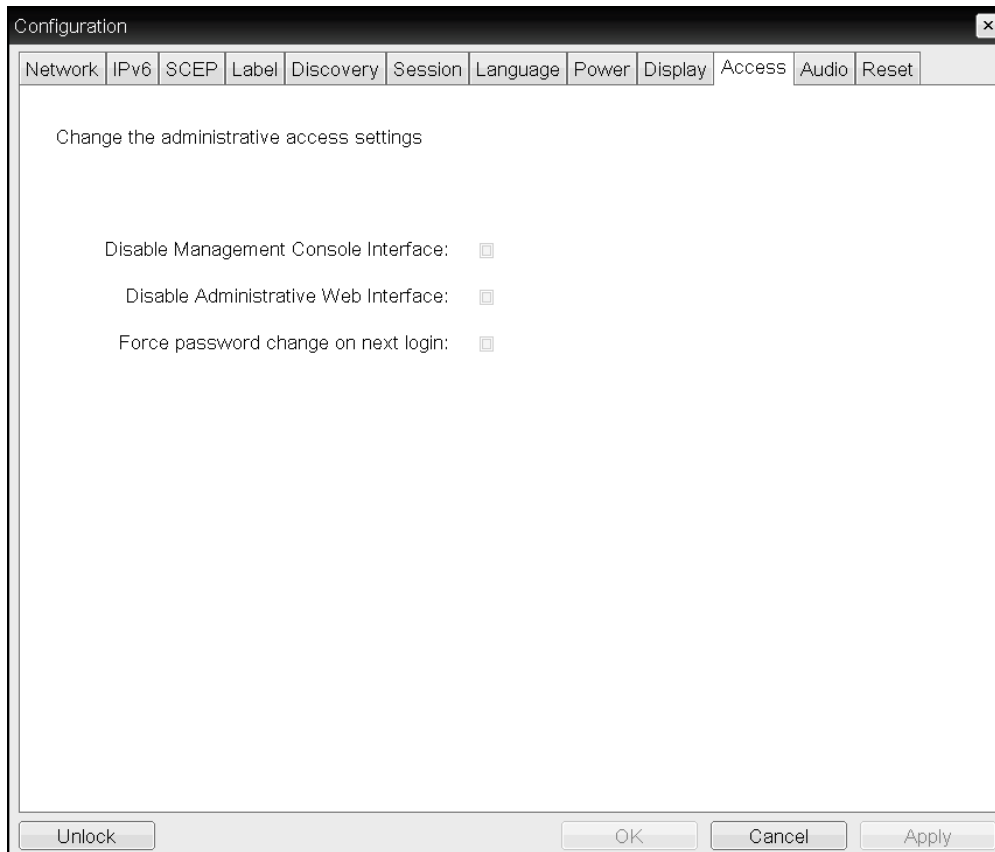
OSD Access Page

OSD Access Page Parameters

Parameter	Description
Disable Management Console Interface	When enabled, the management console interface is disabled, and the device cannot be accessed or managed by the MC (or any other PCoIP device management tool).
Disable Administrative Web Interface	When enabled, the device cannot be accessed or managed 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.

Configuring Device Discovery

MC: Discovery Settings

The settings on this page let you configure a profile to use SLP discovery, a PCoIP MC DNS-based discovery prefix, and/or DNS-SRV discovery to discover hosts and clients dynamically in a PCoIP system without requiring prior knowledge of their locations in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems.

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, the recommended discovery mechanism in this case is to configure DHCP Vendor Class Options directly in the DHCP server. For more information about DHCP Options discovery, see the "Configuring Device Discovery" section of "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](#).

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Discovery Configuration

MC Discovery Configuration Parameters

Parameter	Description
Enable SLP Discovery	When enabled, hosts and clients can be dynamically discovered by SLP management entities. Note: This property requires a device restart after being changed.
PCoIP MC DNS-Based Discovery Prefix	Use this property to direct the device to contact a particular PCoIP MC in environments where there is more than one Management Console in use. There are several restrictions on its operation. Please refer to "Teradici PCoIP® Management Console User Manual" (TER0812002) before using this property. Note: This property requires a device restart after being changed.
Enable DNS-SRV Discovery	When enabled: • Hosts and clients automatically advertise themselves to a connection broker without requiring prior knowledge of its location in the network. • The host or client tries to download and use the DNS SRV record from the DNS server. For more information about this discovery mechanism, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Documentation Center. Note: This property requires a device restart after being changed.
DNS-SRV Discovery Delay	Configures the amount of delay time in seconds between the DNS SRV discovery attempts for connection brokers and the Management Console. DNS SRV discovery continues periodically until the device successfully contacts a connection management server.

AWI: Discovery Settings

The settings on this page let you enable management entities to discover hosts and clients dynamically in the PCoIP system without requiring prior knowledge of their locations in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems.

You can access this from the **Configuration > Discovery** menu.

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, the recommended discovery mechanism in this case is to configure DHCP Vendor Class Options directly in the DHCP server. For more information about DHCP Options discovery, see the "Configuring Device Discovery" section of "Teradici

PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](#).

AWI Discovery Page

AWI Discovery Page Parameters

Parameter	Description
Enable SLP Discovery	When enabled, hosts and clients can be dynamically discovered by SLP management entities.
Enable DNS-SRV Discovery	When enabled: • Hosts and clients automatically advertise themselves to a connection broker without requiring prior knowledge of its location in the network. • The host or client tries to download and use the DNS SRV record from the DNS server. For more information about this discovery mechanism, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](#). Note: The **Enable DNS SRV Discovery** option configures the discovery for connection brokers but does not affect the DNS SRV functionality for the PCoIP Management Console.

Parameter	Description
DNS-SRV Discovery Delay	Configures the amount of delay time in seconds between the DNS SRV discovery attempts for connection brokers and the Management Console. DNS SRV discovery continues periodically until the device successfully contacts a connection management server. Note: Although the **Enable DNS SRV** option does not affect the DNS SRV functionality for the PCoIP Management Console, the DNS SRV Discovery Delay is used for the PCoIP Management Console. When DNS SRV records are not installed, we recommend you set the delay to the maximum value of "9999". This minimizes attempts by the host or client to contact the PCoIP Management Console.

OSD: Discovery Settings

The settings on this page let you enable Service Location Protocol (SLP) management entities to discover hosts and clients dynamically in the PCoIP system without requiring prior knowledge of their locations in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems.

You can access this page from the **Options > Configuration > Discovery** menu.

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, the recommended discovery mechanism in this case is to configure DHCP Vendor Class Options directly in the DHCP server. For more information about DHCP Options discovery, see the "Configuring Device Discovery" section of "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](#).

OSD Discovery Page

OSD Discovery Page Parameter

Parameter	Description
Enable Discovery	When enabled, hosts can be dynamically discovered by SLP management entities.

Configuring SNMP

MC: Help for SNMP Settings

SNMP settings for the Management Console are located on the MC's Network Configuration page.

Note: For more information on using the PCoIP SNMP Agent, see "Using SNMP with a PCoIP® Device User Guide" (TER0805002).

AWI: SNMP Settings

The **SNMP** page lets you enable or disable the host or client SNMP agent. You can access this page from the **Configuration > SNMP** menu.

Note: For more information on using the PCoIP SNMP Agent, see "Using SNMP with a PCoIP® Device User Guide" (TER0805002).

SNMP

Change the SNMP configuration

                Enable SNMP: ☑
Community Name: public

[Apply] [Cancel]

AWI SNMP Page

AWI SNMP Page Parameter

Parameter	Description
Enable SNMP	When enabled, the device enables the PCoIP SNMP agent to respond to SNMP requests. Disabling the SNMP agent prevents it from responding to SNMP requests and from generating traps. It also ensures that the PCoIP SNMP MIB cannot be accessed.
Community Name	Configures the SNMP community name used by the device.

Configuring a Session

Configuring a Session Connection Type

The **Session** pages on the MC, AWI, and OSD let you configure how the host or client device connects to or accepts connections from peer devices. The available configuration options depend on the session connection type you select.

Session Connection Types

The following are the main session connection types:

- 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)
- [Connection Management Interface](#)

Auto Detect

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (e.g., one that uses View Connection Servers and PCoIP 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	Device(s)	Session Connection Options
MC	Client	[Auto Detect](#)
AWI	Client	[Auto Detect](#)
OSD	Client	[Auto Detect](#)

Direct to Host Sessions

A Direct to Host session is a direct connection between a zero client and a remote workstation containing a PCoIP Remote Workstation Card. You can specify a host'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	Device(s)	Session Connection Options
MC	All	[Direct to Host](#) [Direct to Host + SLP Host Discovery](#)
AWI	Host	[Direct from Client](#)
	Client	[Direct to Host](#) [Direct to Host + SLP Host Discovery](#)
OSD	Client	[Direct to Host](#) [Direct to Host + SLP Host Discovery](#)

PCoIP Connection Manager (Tera2 Clients Only)

A PCoIP Connection Manager session is a connection between a Tera2 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	Device(s)	Session Connection Options
MC	All	PCoIP Connection Manager PCoIP Connection Manager + Auto-Logon
AWI	Client	PCoIP Connection Manager PCoIP Connection Manager + Auto-Logon
OSD	Client	PCoIP Connection Manager PCoIP Connection Manager + Auto-Logon

VMware Horizon VDI, DaaS, and RDS-hosted App-remoting Connections

A VMware Horizon session is a connection between a 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.

Note: 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 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

Management Tool	Device(s)	Session Connection Options
MC	All	View Connection Server View Connection Server + Auto-Logon View Connection Server + Kiosk View Connection Server + Imprivata OneSign

Management Tool	Device(s)	Session Connection Options
AWI	Client	View Connection Server View Connection Server + Auto-Logon View Connection Server + Kiosk View Connection Server + Imprivata OneSign
OSD	Client	View Connection Server View Connection Server + Auto-Logon View Connection Server + Kiosk View Connection Server + Imprivata OneSign

Connection Management Interface Sessions

The Connection Management Interface is used to configure an external connection manager as the connection broker.

Connection Management Interface Connections

Management Tool	Device(s)	Session Connection Options
MC	All	Connection Management Interface
AWI	Host	Connection Management Interface
	Client	Connection Management Interface
OSD	Client	Connection Management Interface

MC: Auto Detect Session Settings

Select the **Auto Detect** session connection type from the MC to configure a profile for Tera2 zero clients that lets the device automatically detect which broker protocol a connection server is using so users in a mixed environment (e.g., 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.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Session Connection Type – Auto Detect

MC Session Configuration Parameters

Parameter	Description
Auto Detect Server URI	Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this server, the server name will appear in the **Server** drop-down list on the user's OSD Connect page if the **Auto Detect Server Cache Entry** is enabled and configured (see below).
	Note: The URI must be in the form "https://<*hostname|IP address*>".
Auto Detect Server Cache Entry (1 to 25)	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a connection server URI to which a user is allowed to connect.
	• If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server URI.
	• If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.

MC: Direct to Host Session Settings

Select the **Direct to Host** session connection type from the MC to configure a profile to connect clients directly to hosts.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

Note: For information on how to link specific hosts and clients, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Documentation Center. To configure a specific host with peering properties (e.g., to accept any peer rather than a specific MAC address), use the AWI's Direct from Client session settings.
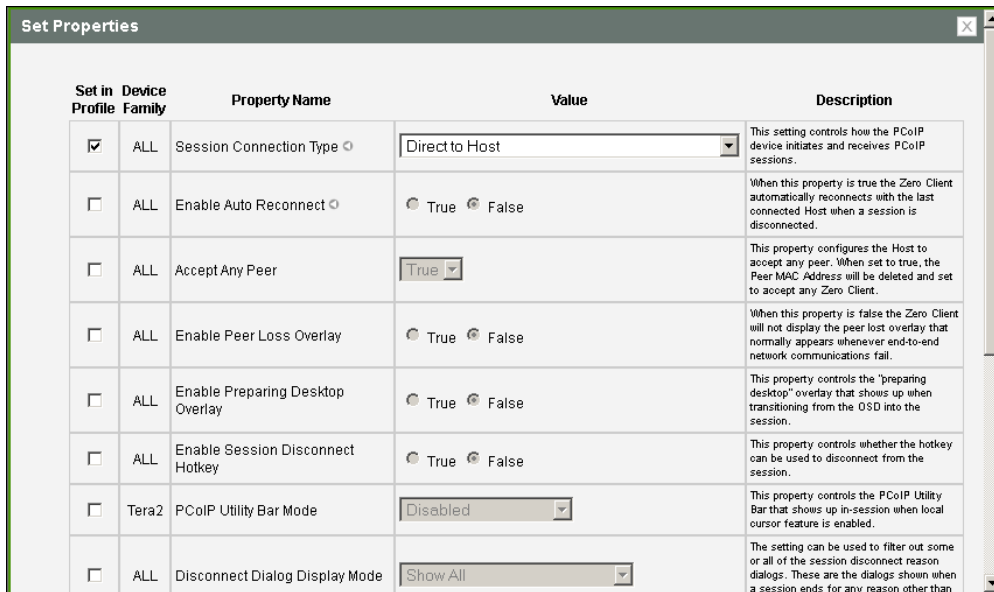
MC Session Connection Type – Direct to Host

MC Session Configuration Parameters

Parameters	Description
Enable Auto Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost. Note: This property requires a device restart after being changed.
Accept Any Peer	When enabled and set to **True**, the host is configured to accept any zero client.

Parameters	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameters	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: Direct to Host Session + SLP Host Discovery Settings

Select the **Direct to Host + SLP Host Discovery** session connection type from the MC to configure a profile to connect clients directly to hosts and to configure clients to use Service Location Protocol (SLP) to discover hosts dynamically.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

Note: For information on how to link specific hosts and clients, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](). To configure a specific host with peering properties (e.g., to accept any peer rather than a specific MAC address), use the AWI's [Direct from Client]() session settings.
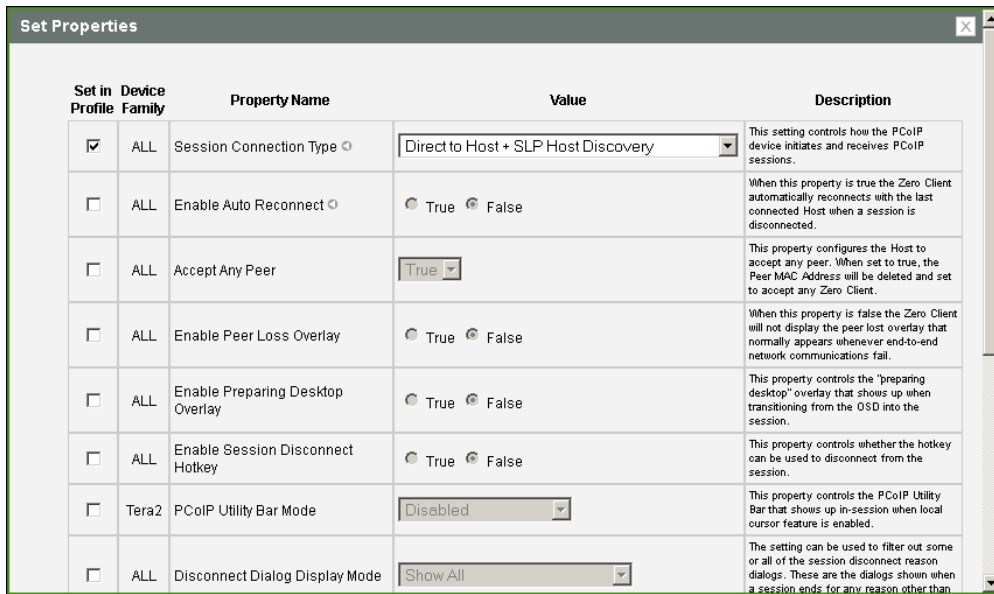
MC Session Connection Type – Direct to Host + SLP Host Discovery

MC Session Configuration Parameters

Parameters	Description
Enable Auto Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost. Note: This property requires a device restart after being changed.
Accept Any Peer	When enabled and set to **True**, the host is configured to accept any zero client.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.

Parameters	Description
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameters	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: View Connection Server Session Settings

Select the **View Connection Server** session connection type from the MC to configure a profile to use a View Connection Server to connect clients to a VMware desktop.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Session Connection Type – View Connection Server

MC Session Configuration Parameters

Parameter	Description
View Connection Server 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. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
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.
Enable View Connection Server SSL	When enabled, enables SSL communication with the connection server. Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the connection server is always enabled.

Parameter	Description
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Clear Trusted Connection Server Cache	When enabled, clears the trusted connection server cache.
Auto Connect Mode	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. Note: 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.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD **Connect** page when a user types in a valid server address, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the **Server** drop-down menu on the OSD **Connect** page. • **Read-only**: Select this option if you want users to select a connection server from a read-only list.
Connection Server Cache Entry (1 to 25)	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a connection server IP address or FQDN to which a user is allowed to connect. • If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server IP address or FQDN. • If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.
Self Help Link Mode	When enabled, enables the Self Help Link on user authentication screens. For a description of this feature, see [Enabling the Self Help Link](#).
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**.
Enable Login Username Caching	When enabled, the username 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. You can upload an OSD logo from the [OSD Logo Upload](#) page.
Prefer GSC-IS Over PIV Endpoint	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.

Parameter	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

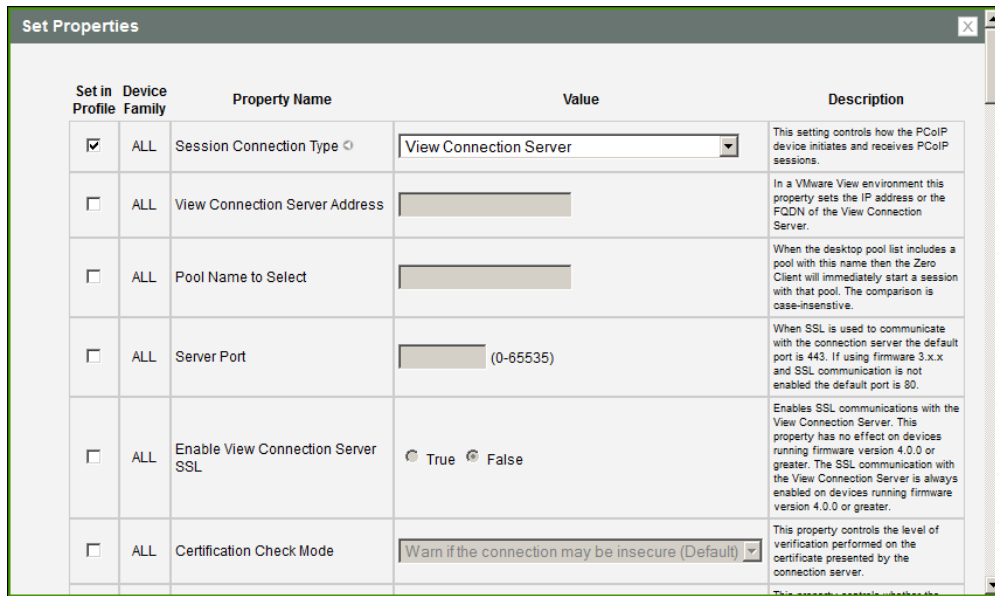| Parameter	Description
Disconnect Dialog Display Mode	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged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

Parameter	Description
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
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. Note: Applications open in full-screen mode, but can be re-sized once users are in session.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: View Connection Server + Auto-Logon Session Settings

Select the **View Connection Server + Auto-Logon** session connection type from the MC to configure a profile to automatically enter users' login details when a View Connection Server is used to connect clients to a VMware desktop.

Important! 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.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Session Connection Type – View Connection Server + Auto-Logon

MC Session Configuration Parameters

Parameter	Description
View Connection Server 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.
Auto-Logon Username	Enter the username for the client (maximum number of characters is 128). This username will be sent to the specified connection server.

Parameter	Description
Auto-Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Auto-Logon 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	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
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.
Enable View Connection Server SSL	When enabled, enables SSL communication with the connection server. Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the connection server is always enabled.
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Clear Trusted Connection Server Cache	When enabled, clears the trusted connection server cache.

Parameter	Description
Auto Connect Mode	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. Note: 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.
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. • **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-only list.
Connection Server Cache Entry (1 to 25)	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a connection server IP address or FQDN to which a user is allowed to connect. • If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server IP address or FQDN. • If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**.

Parameter	Description
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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
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.
	Note: Applications open in full-screen mode, but can be re-sized once users are in session.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header.
	Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: View Connection Server + Kiosk Session Settings

Select the **View Connection Server + Kiosk** session connection type from the MC to configure a profile to use Kiosk mode when when a View Connection Server is used to connect clients to a VMware desktop.

Important! 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.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Session Connection Type – View Connection Server + Kiosk

MC Session Configuration Parameters

Parameter	Description
View Connection Server Address	Enter the View Connection Server's DNS name or IP address.
Use Kiosk Custom Username	When enabled, the login name is presented as "Custom-<*XXX*>", where "*XXX*" is the value of the **Kiosk Mode Custom Username**. When disabled, clients use the MAC-based username of the form "CM-AA:BB:CC:DD:EE:FF."

Parameter	Description
Kiosk Mode Custom Username	When **Use Kiosk Custom Username** is configured to use a custom username of the form "Custom-<*XXX*>", enter the value for the "*XXX*" component. This field is limited to 13 characters.
Kiosk Mode Password	Enter the password to use to access a virtual desktop in Kiosk mode. Note: This setting is optional.
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.
Enable View Connection Server SSL	When enabled, enables SSL communication with the connection server. Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the connection server is always enabled.
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Clear Trusted Connection Server Cache	When enabled, clears the trusted connection server cache.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.

Parameter	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Disconnect Dialog Display Mode	This field lets you control what type of messages appear when a session is disconnected. There are three categories:

Information: User- or administrator-initiated actions affecting the session:

- You have been disconnected because you logged in from another location or your host was shut down or restarted.
- You have been disconnected because an administrator disconnected you.
- You have been disconnected because you logged in from another location.
- You have been disconnected because you disconnected from your workstation.

Warning: System-initiated, but expected actions affecting the session:

- You have been disconnected because your session timed out.

Error: Unexpected system-initiated actions causing session to fail:

- You have been disconnected.
- Unable to connect (0x1001). Please contact your IT administrator.
- Unable to connect (0x1002). Please contact your IT administrator.
- Session closed remotely.
- Session closed remotely (unknown cause).
- You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error

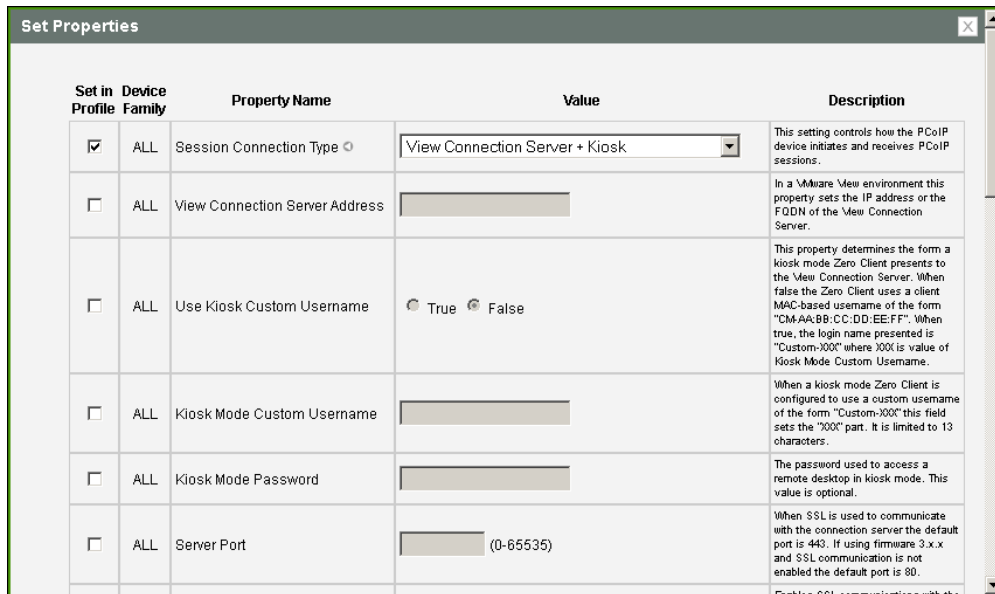| Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
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. Note: Applications open in full-screen mode, but can be re-sized once users are in session.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: View Connection Server + Imprivata OneSign Session Settings

Select the **View Connection Server + Imprivata OneSign** session connection type from the MC to configure a profile to authenticate through the Imprivata OneSign system in addition to a View Connection Server when clients connect to a VMware desktop.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
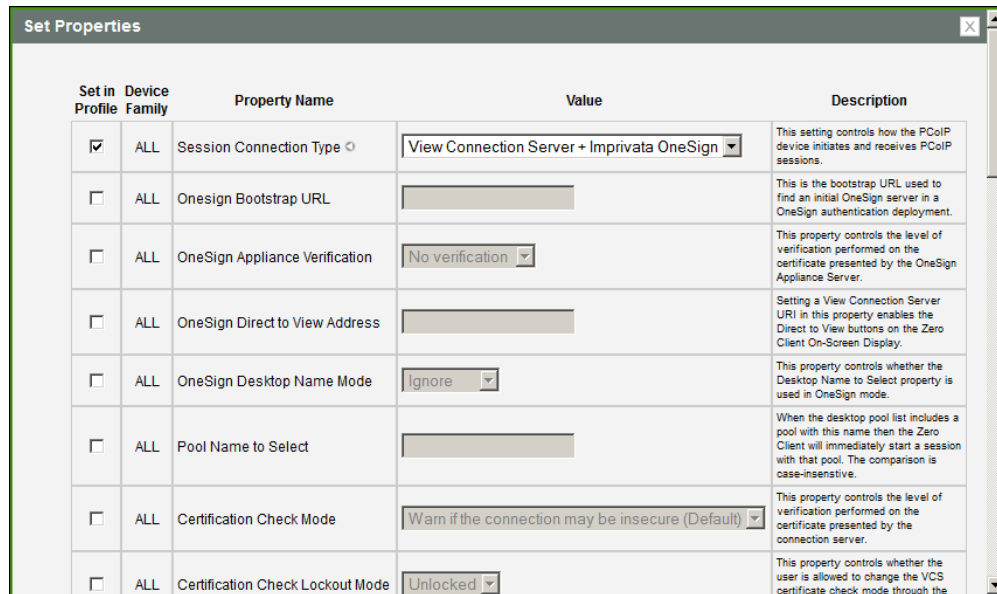
MC Session Connection Type – View Connection Server + Imprivata OneSign

MC Session Configuration Parameters

Parameter	Description
Onesign Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
Onesign Appliance Verification	Select the level of verification performed on the certificate presented by the OneSign appliance server: • **No verification: Connect to any appliance** • **Full verification: Only connect to appliances with verified certificates**

Parameter	Description
OneSign Direct To View Address (Tera2 only)	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 zero client users to access their View desktops when the OneSign infrastructure is unavailable.
Onesign Desktop Name Mode	Select whether the **Desktop Name to Select** property is used in OneSign mode. • **Ignore** • **Use If Set**
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. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Clear Trusted Connection Server Cache	When enabled, clears the trusted connection server cache.
Enable Login Username Caching	When enabled, the username text box automatically populates with the last username entered.

Parameter	Description
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. You can upload an OSD logo from the OSD Logo Upload page.
Prefer GSC-IS Over PIV Endpoint	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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.
Proximity Reader Beep Mode	Configure whether the proximity card reader beeps when a valid card is tapped on the reader in OneSign mode: • **Disabled**: Disables the feature. • **Enabled**: Enables the feature. • **Use Existing Setting**: Uses the existing setting (affects only devices running firmware 4.1.0 or greater)
Invert Wiegand Data	Configure whether or not the RF IDeas proximity reader will invert the Wiegand bits that are read from a user's ID token. This feature is useful when some of the RF IDeas readers in your system are programmed to invert the Wiegand data and others are not. It lets you configure all readers to read the bits in a consistent manner (whether inverted or not inverted), so that all the readers behave the same way from a user's point of view. • **Disabled**: Disables the feature. Wiegand data are not inverted. • **Enabled**: Enables the feature. Wiegand data are inverted. • **Use Existing Setting**: Uses the existing setting (affects only devices running firmware 4.2.0 or greater). Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Restrict Proximity Cards	Configure whether or not proximity cards are restricted to tap-in/tap-out only. When this feature is enabled, the proximity card reader is locally terminated (i.e., it uses drivers in the client's firmware), and proximity cards can only be used for tap-in/tap-out. When this feature is disabled, the proximity card reader is bridged by default (i.e., it uses drivers in the host OS), and proximity cards are not restricted. They can be used for tap-in/tap-out and also during a session—for example, when an application requires in-session authentication. • **True**: Enables the feature. • **False**: Disables the feature. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
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. Note: Applications open in full-screen mode, but can be re-sized once users are in session.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: Connection Management Interface Settings

Select the **Connection Management Interface** session connection type from the MC to configure a profile to use an external connection manager as the connection broker.

This selection requires a device restart after being changed.

Note: External connection managers can simplify the administration effort for large, complex systems. In a managed connection, an external connection manager server communicates with a device, and can remotely control and configure it. The connection manager can also locate an appropriate peer for the device to connect to, and then initiate the connection.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Session Connection Type – Connection Management Interface

MC Session Configuration Parameters

Parameter	Description
CMS Address	Enter the IP address or fully qualified domain name (FQDN) of the connection manager. Note: Many connection managers will automatically set this value in each device they discover.

Parameter	Description
Accept Any Peer	When enabled and set to **True**, the host is configured to accept any zero client.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Event Log Notification	When enabled, the client sends the contents of its event log to the connection management server.
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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). ● **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

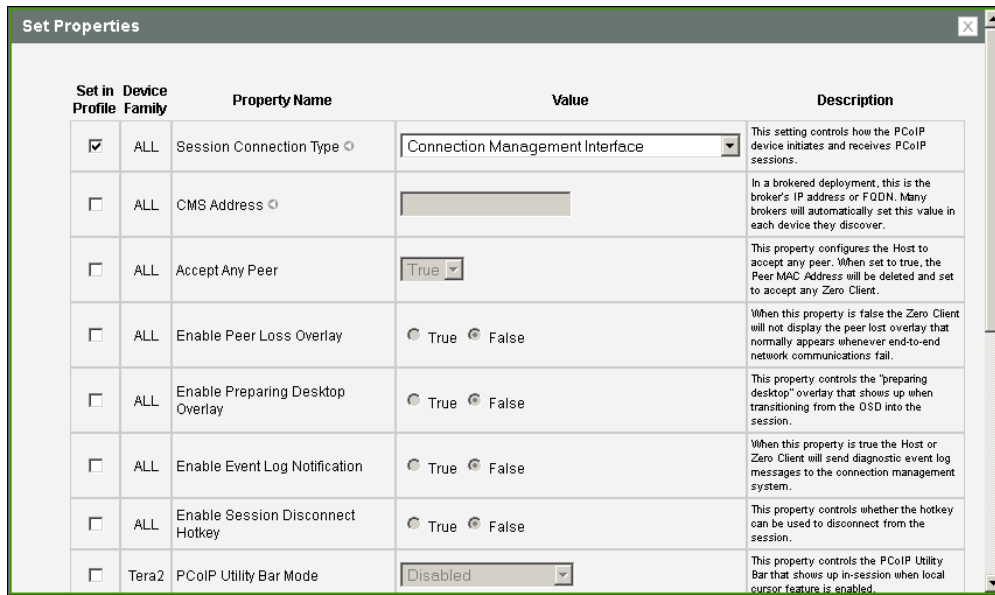| Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

MC: PCoIP Connection Manager Session Settings

Select the **PCoIP Connection Manager** session connection type from the MC to configure a profile to use a PCoIP Connection Manager as the PCoIP session broker.

This selection requires a device restart after being changed.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
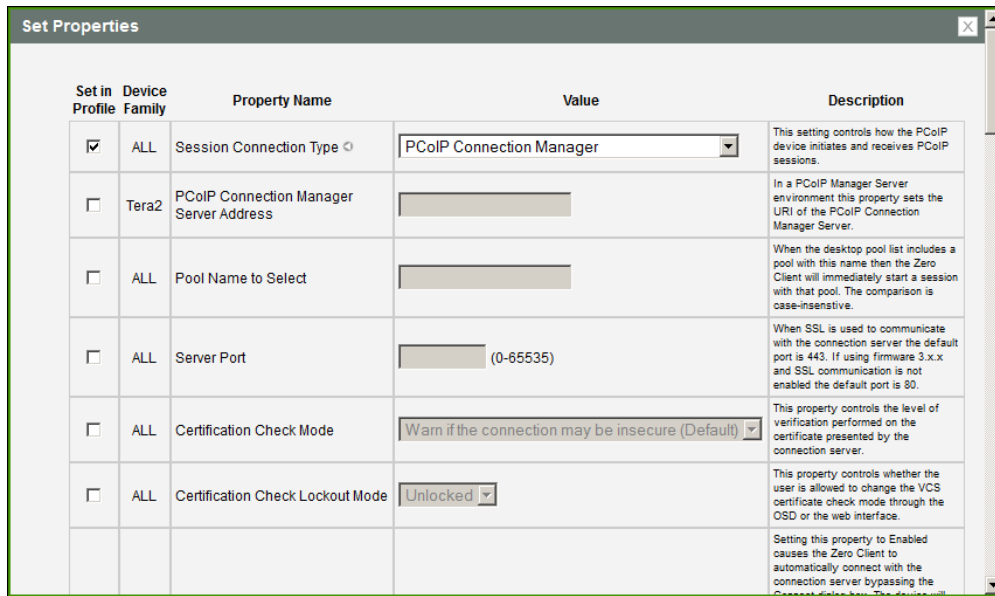
MC Session Connection Type – PCoIP Connection Manager

MC Session Configuration Parameters

Parameter	Description
PCoIP Connection Manager Server Address	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://<*hostname|IP address*>".
Pool Name to Select	Enter the desktop name used by the client when starting a session. Note: This field is case-insensitive.
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.

Parameter	Description
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Auto Connect Mode	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. Note: 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.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD **Connect** page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. ● **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the **Server** drop-down menu on the OSD **Connect** page. ● **Read-only**: Select this option if you want users to select a connection server from a read-only list.
PCM Server Cache Entry (1 to 25)	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a PCoIP Connection Server URI to which a user is allowed to connect. ● If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server URI. ● If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.
Self Help Link Mode	When enabled, enables the Self Help Link on user authentication screens. For a description of this feature, see Enabling the Self Help Link.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.
Enable Login Username Caching	When enabled, the username 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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Parameter	Description
Enable Session Disconnect Hotkey	When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameter	Description
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.
Organization ID	Enter an organization ID for the company (e.g., "mycompany.com"). This field accepts any UTF-8 character. Note: You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

MC: PCoIP Connection Manager + Auto-Logon Session Settings

Select the **PCoIP Connection Manager + Auto-Logon** session connection type from the MC to configure a profile to automatically enter users' login details when a PCoIP Connection Manager is used as the PCoIP session broker.

This selection requires a device restart after being changed.

Important! 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.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

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

MC Session Configuration Parameters

Parameter	Description
PCoIP Connection Manager Server Address	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://<*hostname*|*IP address*>".
Auto-Logon Username	Enter the username for the client (maximum number of characters is 128). This username will be sent to the specified connection server.
Auto-Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Auto-Logon Domain	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.

Parameter	Description
Pool Name to Select	Enter the desktop name used by the client when starting a session. Note: This field is case-insensitive.
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.
Certification Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Warn if the connection may be insecure (Default)**: 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 zero client trust store is empty. • **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed. • **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections.
Certification Check Lockout Mode	Select whether to lock or unlock Certification Check Mode: • **Unlocked**: Select this option to allow users to change the Certification Check Mode setting using the OSD or AWI. • **Locked**: Select this option to prevent users from changing the Certification Check Mode setting.
Auto Connect Mode	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. Note: 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.

Parameter	Description
Connection Server Cache Mode	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a PCoIP Connection Server URI to which a user is allowed to connect. • If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server URI. • If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.
PCM Server Cache Entry (1 to 25)	Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a PCoIP Connection Server URI to which a user is allowed to connect. • If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new connection server is added to the **Server** drop-down menu whenever the user types in a valid server URI. • If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are 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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Session Lost Timeout	Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Tera2 Client: Auto Detect Session Settings

Select the **Auto Detect** session connection type from the **Configuration > Session** page to let the zero client automatically detect which broker protocol a connection server is using so users in a mixed environment (e.g., 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.

AWI Session Connection Type – Auto Detect

AWI Session Page 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 zero client is configured to cache servers. Note: The URI must be in the form "https://<*hostname|IP address*>".

AWI Host: Direct from Client Session Settings

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

AWI Session Connection Type – Direct from Client

AWI Session Page Parameters

Parameters	Description
Accept Any Peer	When enabled, the host accepts connections from any client. When disabled, you must specify the MAC address of the peer you want the host to accept.
Peer MAC Address	Enter the MAC address of the client that is allowed to connect to the host. If the **Accept Any Peer** option is enabled, this field is not required and not editable.
Session Negotiation Cipher	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. *Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option.

Parameters	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center. Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Client: 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 host.

AWI Session Connection Type – Direct to Host

AWI Session Page Parameters

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

Parameters	Description
Wake Host from Low Power State	Select whether to use the 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 host PC button or clicks the **Connect** button on the **Connect** window. • **Wake-On-LAN Enabled + Peer Address**: After you have successfully connected to the 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, allows you to manually enter the MAC address and IP address of the device you want to wake up. Note: 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. Note: • The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet. • For Tera2 clients, you can disable the Wake-On-LAN feature from the AWI Power page or the MC Power Permissions. page.
Host Wake MAC Address	Enter the host's MAC address to complete the host wake up configuration when **Wake-On-LAN Enabled + Peer Address** or **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this MAC address to wake the host computer from a low power state.
Host Wake IP Address	Enter the host's IP address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this IP address to wake the host computer from a low power state.
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.

Parameters	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameters	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameters	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support [Documentation Center](#). Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

Parameters	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories:

Information: User- or administrator-initiated actions affecting the session:

- You have been disconnected because you logged in from another location or your host was shut down or restarted.
- You have been disconnected because an administrator disconnected you.
- You have been disconnected because you logged in from another location.
- You have been disconnected because you disconnected from your workstation.

Warning: System-initiated, but expected actions affecting the session:

- You have been disconnected because your session timed out.

Error: Unexpected system-initiated actions causing session to fail:

- You have been disconnected.
- Unable to connect (0x1001). Please contact your IT administrator.
- Unable to connect (0x1002). Please contact your IT administrator.
- Session closed remotely.
- Session closed remotely (unknown cause).
- You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error

Parameters	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Client: 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 ▾]

Note: this session connection type will enable SLP discovery on this Zero Client.

[Hide Advanced Options]

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: [Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1 ▾]
Enabled Session Ciphers:

AES-256-GCM: ☑
AES-128-GCM: ☑

Disconnect Message Filter: [Show All ▾]
Enable DSCP: ☐
Enable Congestion Notification: ☑

[Apply] [Cancel]

AWI Session Connection Type – Direct to Host + SLP Host Discovery

AWI Session Page Parameters

Parameters	Description
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.

Parameters	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameters	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameters	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support [Documentation Center](#). Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameters	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Tera2 Client: 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.

AWI Session Connection Type – PCoIP Connection Manager

AWI Session Page Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://*<hostname|IP address>*".
Desktop Name to Select	Enter the desktop name used by the client when starting a session. Note: This field is case-insensitive.

Parameter	Description
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 zero client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to allow 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	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. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD **Connect** page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the **Server** drop-down menu on the OSD **Connect** page. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers.
Enable Self Help Link	See Enabling the Self Help Link for details.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Remember Username	When enabled, the username 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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Parameter	Description
Enable Session Disconnect Hotkey	When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center. Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.
Organization ID	Enter an organization ID for the company (e.g., "mycompany.com"). This field accepts any UTF-8 character. Note: You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

Enabling the Self Help Link

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

Parameter	Description
Connection Server	Enter the fully-qualified domain name of the connection server brokering the desktop (e.g., 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 (e.g., *mycompany.com*).
Pool Name to Select	Enter the pool or desktop name for the self-help desktop. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Link Text	Enter the text that you want to appear as hyperlinked text on the **Connect** window.

AWI Tera2 Client: 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.

Important! 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.

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

AWI Session Page Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://<*hostname*|*IP address*>".
Logon Username	Enter the username for the client (maximum number of characters is 128). This username will be sent to the specified connection server.

Parameter	Description
Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Logon Domain Name	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Desktop Name to Select	Enter the desktop name used by the client when starting a session. Note: This field is case-insensitive.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers**: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to allow 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	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. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD **Connect** page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select. ● **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the **Server** drop-down menu on the OSD **Connect** page. ● **Read-only**: Select this option if you want users to select a connection server from a read-only list. Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center. Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Client: 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.

AWI Session Connection Type – View Connection Server

AWI Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.

Parameter	Description
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 zero client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
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. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Connection Server Cache Mode	This field determines whether a connection server is dynamically added to the **Server** drop-down menu on the OSD **Connect** page when a user types in a valid server address, or whether it appears in a read-only list for the user to select. • **Last servers used**: Select this option if you want a list of cached servers that a user has typed in to appear in the **Server** drop-down menu on the OSD **Connect** page. • **Read-only**: Select this option if you want users to select a connection server from a read-only list. Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers.
Enable Self Help Link	See Enabling the Self Help Link for details.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Remember Username	When enabled, the username 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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Note: Applications open in full-screen mode, but can be re-sized once users are in session.
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support [Documentation Center](#). Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

Parameter	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories:

Information: User- or administrator-initiated actions affecting the session:

- You have been disconnected because you logged in from another location or your host was shut down or restarted.
- You have been disconnected because an administrator disconnected you.
- You have been disconnected because you logged in from another location.
- You have been disconnected because you disconnected from your workstation.

Warning: System-initiated, but expected actions affecting the session:

- You have been disconnected because your session timed out.

Error: Unexpected system-initiated actions causing session to fail:

- You have been disconnected.
- Unable to connect (0x1001). Please contact your IT administrator.
- Unable to connect (0x1002). Please contact your IT administrator.
- Session closed remotely.
- Session closed remotely (unknown cause).
- You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

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 then 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:

Parameter	Description
Connection Server	Enter the fully-qualified domain name of the connection server brokering the desktop (e.g., 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 (e.g., *mycompany.com*).
Pool Name to Select	Enter the pool or desktop name for the self-help desktop. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Link Text	Enter the text that you want to appear as hyperlinked text on the **Connect** window.

AWI Client: 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.

Important! 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.

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

AWI Session Page Parameters

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

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

Parameter	Description
Auto Connect	This field determines the client's auto connect behavior after startup: • **Enabled**: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD **Connect** page. • **Disabled**: The client does not automatically connect with the connection server. • **Enabled With Retry On Error**: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Note: 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. Note: 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. • **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-only list. Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers.
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.

Parameter	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Note: Applications open in full-screen mode, but can be re-sized once users are in session.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. • **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center. Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Client: 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.

Important! 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.

AWI Session Connection Type – View Connection Server + Kiosk

AWI Session Page Parameters

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

Parameter	Description
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
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 zero client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Parameter	Description
Enable Session Disconnect Hotkey	When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Note: Applications open in full-screen mode, but can be re-sized once users are in session.
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it.

Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option.

For Tera2 zero clients:

Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.

- **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility.
- **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.
- **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected.
Note: Currently this option can only be used with Amazon WorkSpaces hosts.

For Tera1 zero clients:

Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.

- **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.
- **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center. Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Client: View Connection Server + Imprivata OneSign Session Settings

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

AWI Session Connection Type – View Connection Server + Imprivata OneSign

AWI Session Page Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	Select whether the **Pool Name to Select** property is used in OneSign mode. ● **Ignore the Pool Name to Select field** ● **Use the Pool Name to Select field if set** Note: For Tera1 zero clients, this parameter is called **OneSign Desktop Name Mode**.

Parameter	Description
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Onesign Appliance Verification	Select the level of verification performed on the certificate presented by the OneSign appliance server: • **No verification: Connect to any appliance** • **Full verification: Only connect to appliances with verified certificates**
Direct To View Address (Tera2 only)	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 zero client users to access their View desktops when the OneSign infrastructure is unavailable.
Certificate Check Mode	Select the level of verification performed on the certificate presented by the connection server: • **Never connect to untrusted servers**: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.) • **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the **Certificate Check Mode** settings from the OSD or AWI.
Trusted View Connection Servers	Click the **Show** button to display View Connection Servers for which the client has received a valid certificate. Click the **Clear** button to clear this cache.
Remember Username	When enabled, the username text box automatically populates with the last username entered.

Parameter	Description
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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details.
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Note: Applications open in full-screen mode, but can be re-sized once users are in session.

Parameter	Description
PCoIP Utility Bar Mode (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). • **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.
Pre-session Reader Beep	Configure whether the proximity card reader beeps when a valid card is tapped on the reader in OneSign mode: • **Disabled**: Disables the feature. • **Enabled**: Enables the feature. • **Use Existing Setting**: Uses the existing setting (affects only devices running firmware 4.1.0 or greater)
Invert Wiegand Data	Configure whether or not the RF IDeas proximity reader will invert the Wiegand bits that are read from a user's ID token. This feature is useful when some of the RF IDeas readers in your system are programmed to invert the Wiegand data and others are not. It lets you configure all readers to read the bits in a consistent manner (whether inverted or not inverted), so that all the readers behave the same way from a user's point of view. • **Disabled**: Disables the feature. Wiegand data are not inverted. • **Enabled**: Enables the feature. Wiegand data are inverted. • **Use Existing Setting**: Uses the existing setting (affects only devices running firmware 4.2.0 or greater). Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Restrict Proximity Cards	Configure whether or not proximity cards are restricted to tap-in/tap-out only. When this feature is enabled, the proximity card reader is locally terminated (i.e., it uses drivers in the client's firmware), and proximity cards can only be used for tap-in/tap-out. When this feature is disabled, the proximity card reader is bridged by default (i.e., it uses drivers in the host OS), and proximity cards are not restricted. They can be used for tap-in/tap-out and also during a session—for example, when an application requires in-session authentication. • **Only use proximity cards for tap-in/tap-out**: Enables/disables the feature. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.

Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it.
	Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option.
	For Tera2 zero clients:
	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.
	• **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility.
	• **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.
	• **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts.
	For Tera1 zero clients:
	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.
	• **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.
	• **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support [Documentation Center](#). Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Custom Session SNI	When enabled, sets a customized Server Name Indication (SNI) string on authorized man-in-the-middle-enabled clients. The SNI string is appended to the SSL/TLS HELLO when the client initates an SSL connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

AWI Host: Connection Management Interface Session Settings

Select the **Connection Management Interface** session connection type from the **Configuration > Session** page to configure an external connection manager as the connection broker for the host to use.

Note: External connection managers can simplify the administration effort for large, complex systems. In a managed connection, an external connection manager server

communicates with a device, and can remotely control and configure it. The connection manager can also locate an appropriate peer for the device to connect to, and then initiate the connection.

AWI Session Connection Type – Connection Management Interface (Host)

AWI Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the DNS name or IP address of the connection manager.
Accept Any Peer	When enabled, the host accepts connections from any client. When disabled, you must specify the MAC address of the peer you want the host to accept.
Peer MAC Address	Enter the MAC address of the client that is allowed to connect to the host. If the **Accept Any Peer** option is enabled, this field is not required and not editable.
Session Negotiation Cipher	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. • **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. • **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network. • **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended. • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network. Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support [Documentation Center](#). Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following: • Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session. • VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session. • VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see [PCoIP Packet Format](#).

AWI Client: Connection Management Interface Session Settings

Select the **Connection Management Interface** session connection type from the **Configuration > Session** page to configure an external connection manager other than View Connection Server as the connection broker for the client to use.

Note: External connection managers can simplify the administration effort for large, complex systems. In a managed connection, an external connection manager server communicates with a device, and can remotely control and configure it. The connection manager can also locate an appropriate peer for the device to connect to, and then initiate the connection.

AWI Session Connection Type – Connection Management Interface (Client)

AWI Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the DNS name or IP address of the connection manager.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.

Parameter	Description
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: 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 (Tera2 zero clients only)	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 zero client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (i.e., not bridged). ● **Disabled**: Disables the PCoIP Utility Bar. Note: (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. Note: This feature is configurable from the MC and AWI only. It requires firmware version 4.2.0 or newer.
Enable Event Log Notification	When enabled, the client sends the contents of its event log to the connection management server.

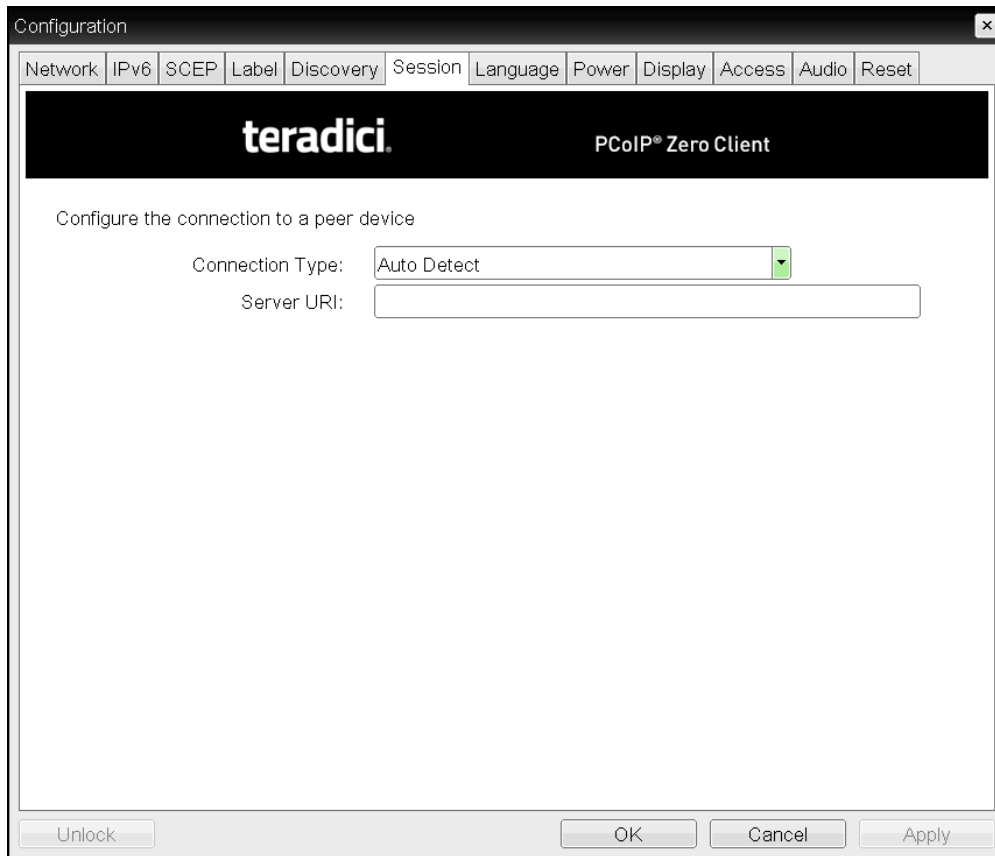| Parameter	Description
Session Negotiation Cipher	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it. Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option. For Tera2 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility. **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected. Note: Currently this option can only be used with Amazon WorkSpaces hosts. For Tera1 zero clients: Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. **Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility. **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.

Parameter	Description
Enabled Session Ciphers	Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.
	• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network.
	• **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or newer, AES-128-GCM is recommended.
	• **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or newer if there is more than about 7 Mbps available on the network.
	Note: For more information about connecting to VMware Horizon virtual desktops, see "Using PCoIP® Zero Clients with VMware View User Guide" (TER0904005) in the Teradici Support Documentation Center.
	Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:
	• Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.
	• VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.
	• VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, allowing intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Transport Congestion Notification	When enabled, transport congestion notification is enabled to allow PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. Note: For more information about the PCoIP transport header, see PCoIP Packet Format.

OSD Tera2: Auto Detect Session Settings

This connection type automatically detects which broker protocol a connection server is using so users in a mixed environment (e.g., 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.
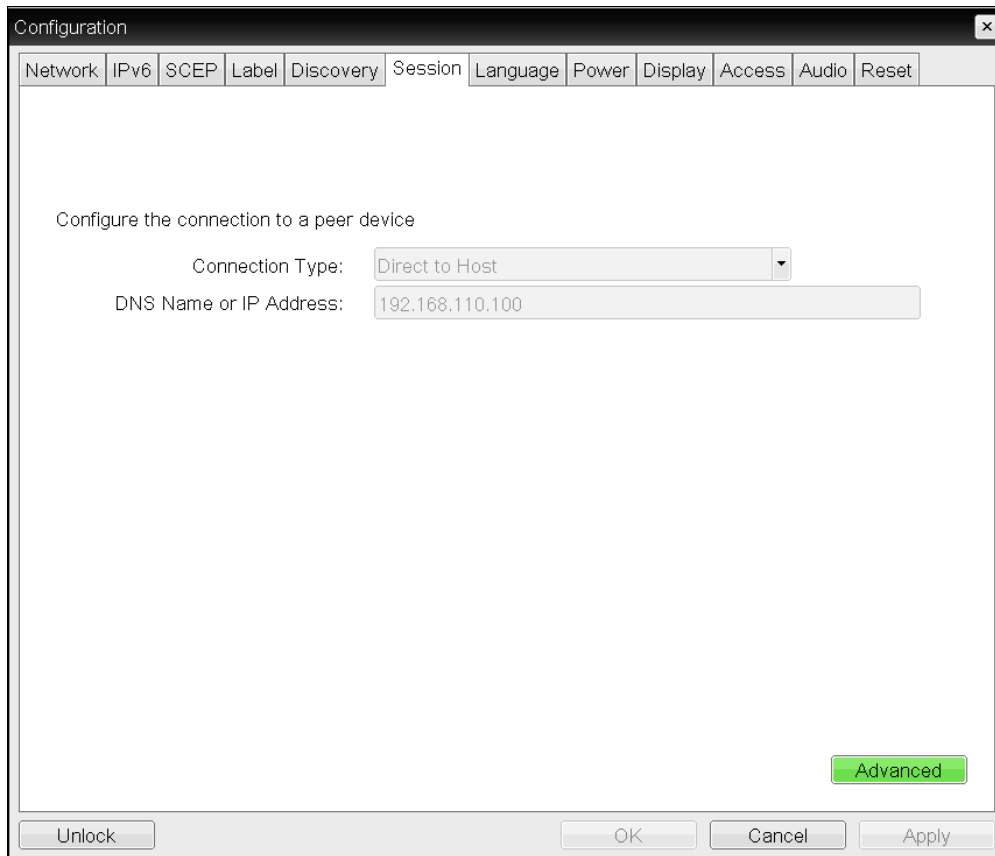
OSD Session Connection Type – Auto Detect

OSD Session Page Parameters

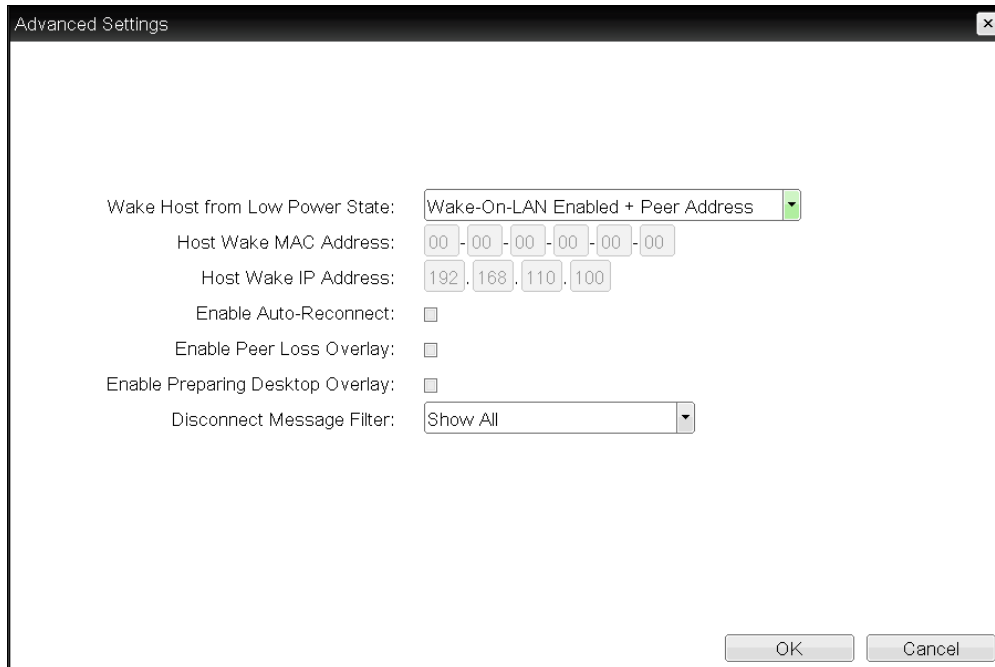| Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this server, it will appear in the **Server** drop-down list on the OSD Connect page if the zero client is configured to cache servers. Note: The URI must be in the form "https://<*hostname|IP address*>".

OSD: Direct to Host Session Settings

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

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

OSD Session Connection Type – Direct to Host

Advanced Settings

OSD Session Page Parameters

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the host.
Wake Host from Low Power State	Select whether to use the 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 host PC button or clicks the **Connect** button on the **Connect** window. • **Wake-On-LAN Enabled + Peer Address**: After you have successfully connected to the 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, allows you to manually enter the MAC address and IP address of the device you want to wake up. Note: 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. Note: • The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet. • For Tera2 clients, you can disable the Wake-On-LAN feature from the AWI Power page or the MC Power Permissions. page.
Host Wake MAC Address	Enter the host's MAC address to complete the host wake up configuration when **Wake-On-LAN Enabled + Peer Address** or **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this MAC address to wake the host computer from a low power state.
Host Wake IP Address	Enter the host's IP address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this IP address to wake the host computer from a low power state
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.

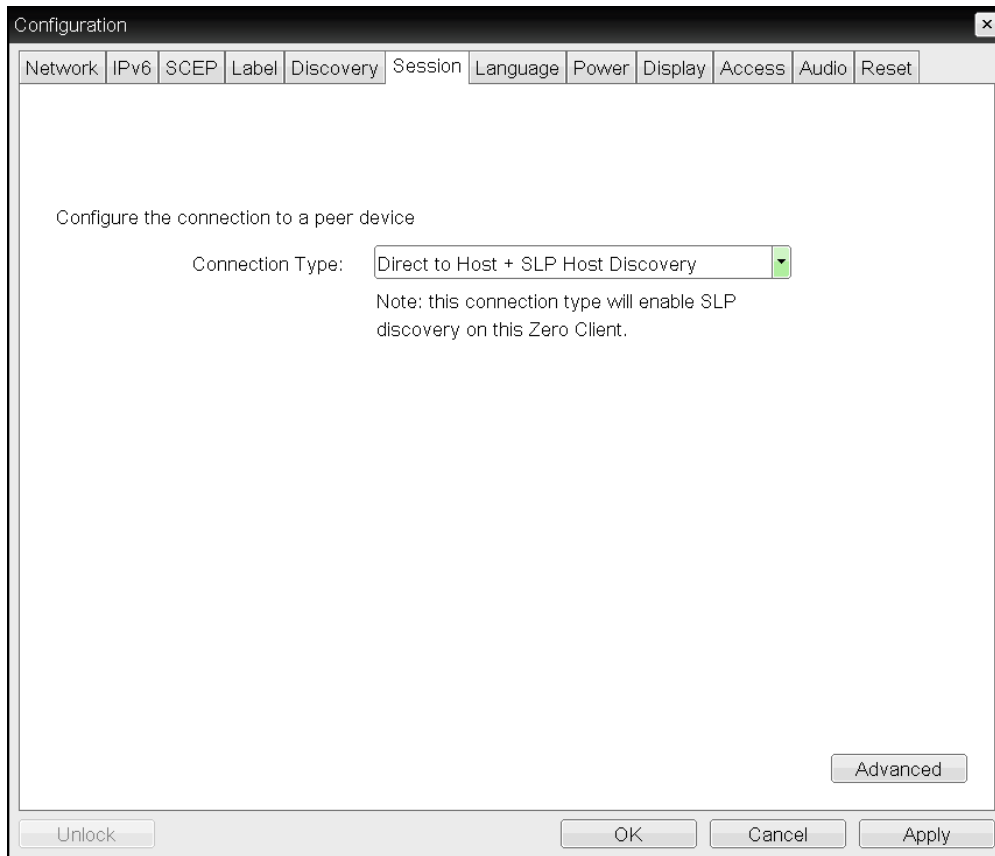| Parameters	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

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

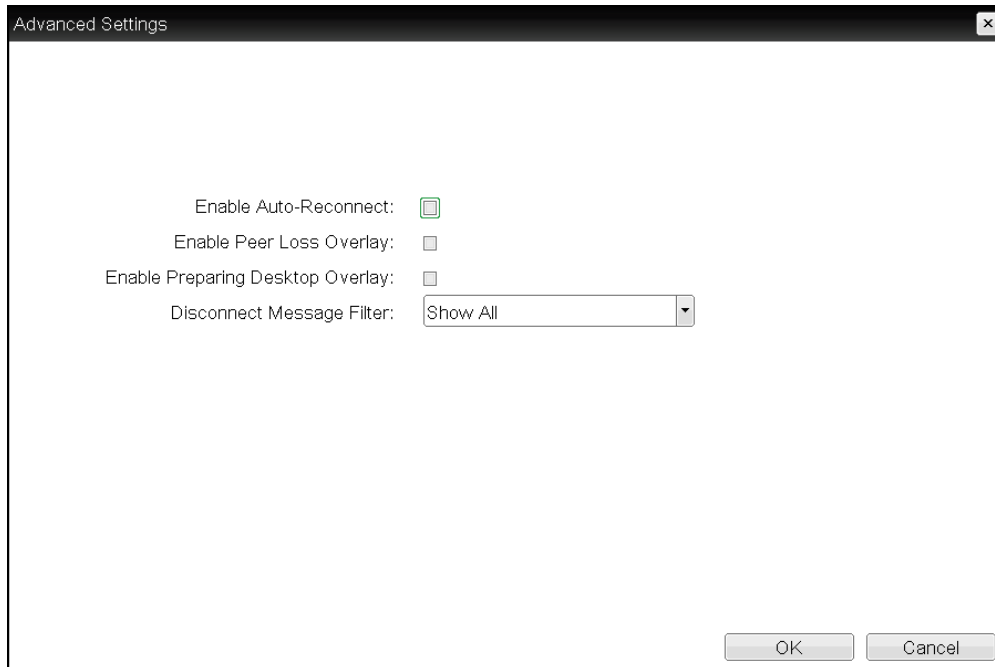| Parameters	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

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

OSD Session Page Parameters

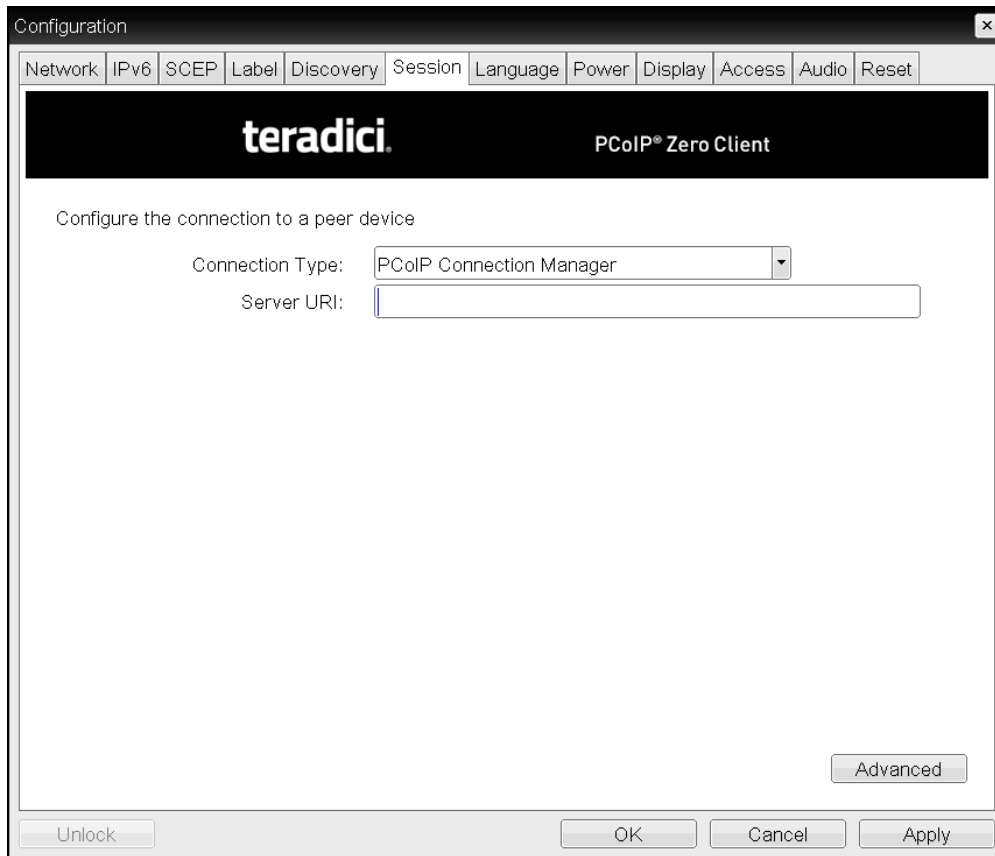| Parameters	Description
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

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

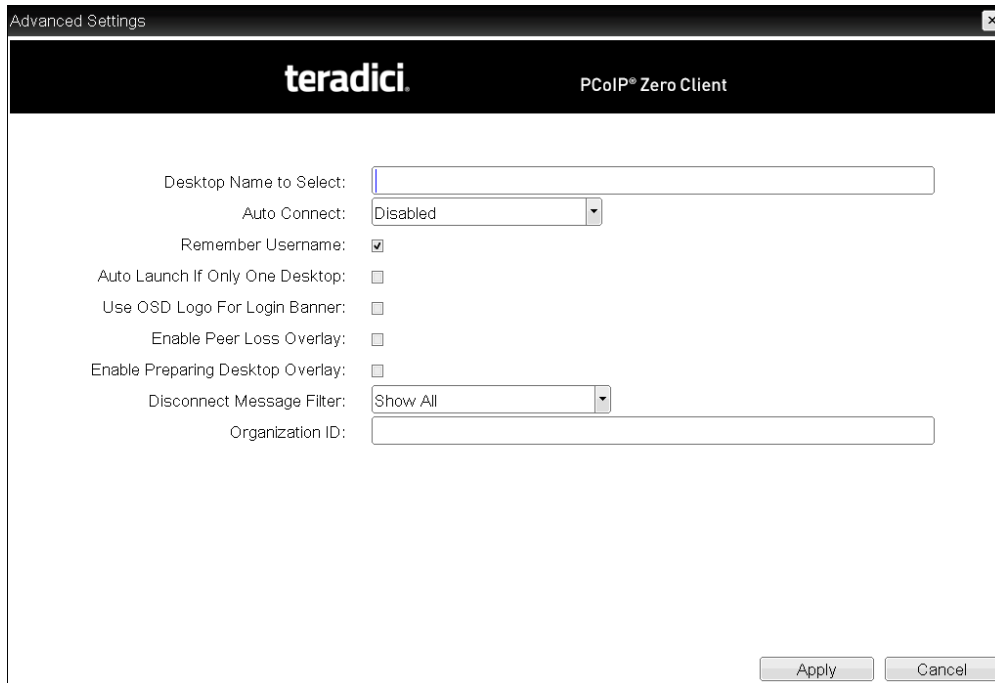| Parameters	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

OSD Tera2: 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.

OSD Session Connection Type – PCoIP Connection Manager

Advanced Settings

OSD Session Page Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://*<hostname|IP address>*".
Desktop Name to Select	Enter the desktop name used by the client when starting a session. Note: This field is case-insensitive.
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. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.
Remember Username	When enabled, the username text box automatically populates with the last username entered.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.

Parameter	Description
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

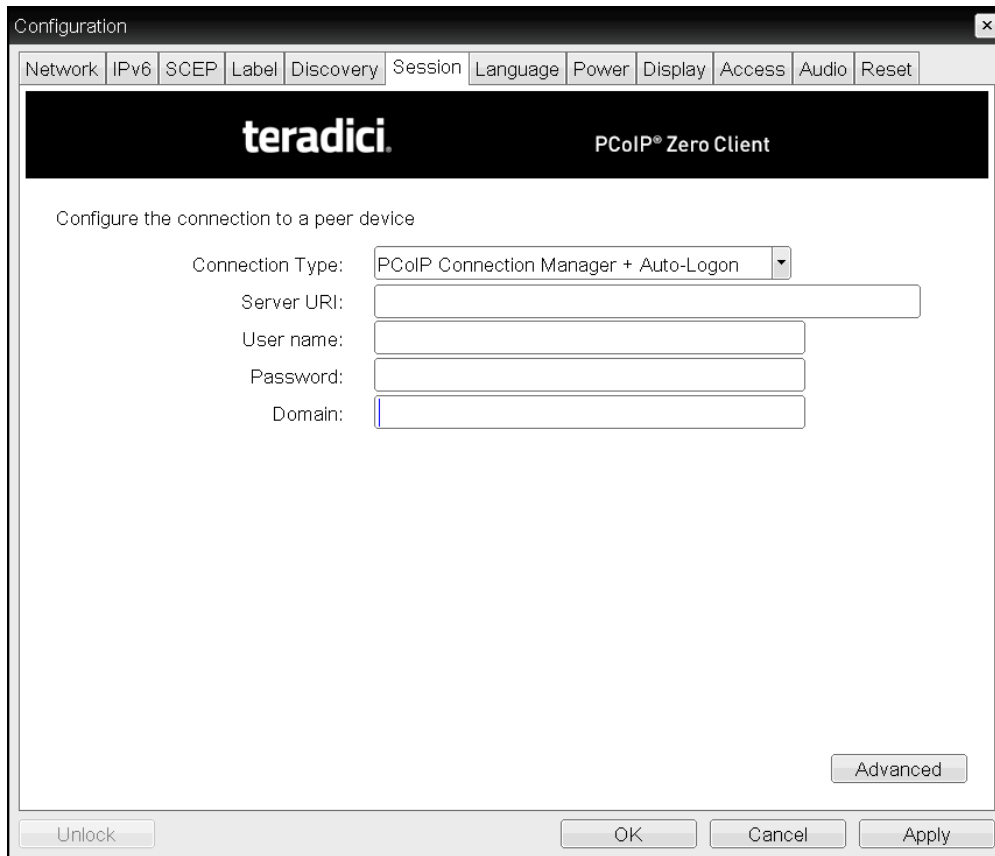| Parameter	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories:
	Information: User- or administrator-initiated actions affecting the session:
	• You have been disconnected because you logged in from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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.
Organization ID	Enter an organization ID for the company (e.g., "mycompany.com"). This field accepts any UTF-8 character. Note: You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

OSD Tera2: PCoIP Connection Manager + Auto-Logon Session Settings
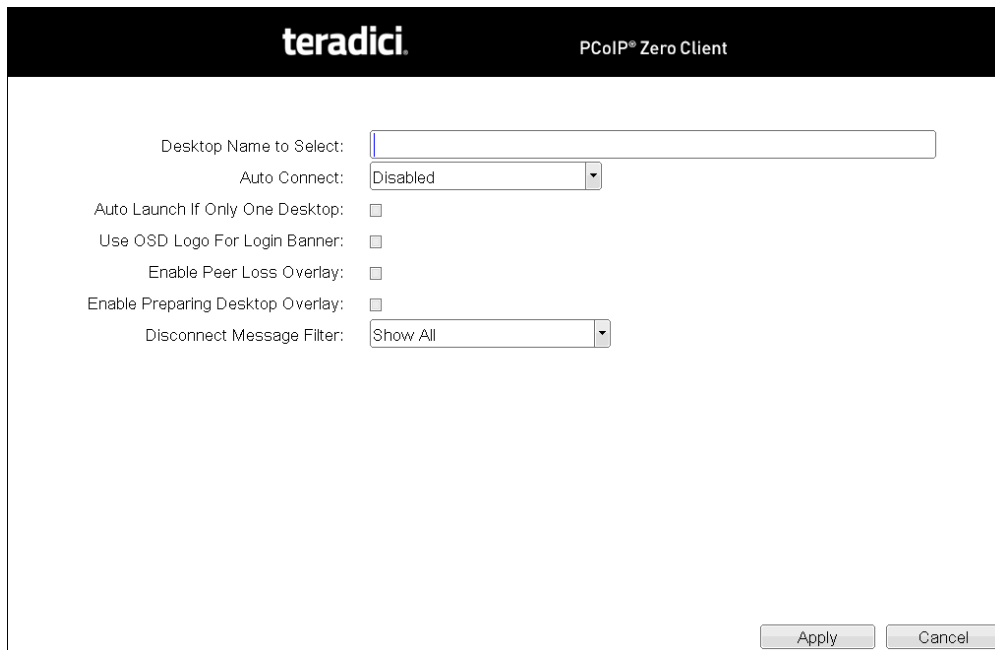
Select the **PCoIP Connection Manager + Auto-Logon** session connection type from the **Options > Configuration > Session** page to configure a client to automatically enter a user's login details when a PCoIP Connection Manager is used as the PCoIP session broker.

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

Important! 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.

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

Advanced Settings

OSD Session Page Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager. Note: The URI must be in the form "https://<*hostname|IP address*>".
User name	Enter the username for the client (maximum number of characters is 128). This username 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. Note: This field is case-insensitive.
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. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.
Auto Launch If Only One Desktop	When enabled, users are automatically connected to a provisioned desktop after user credentials are entered. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.

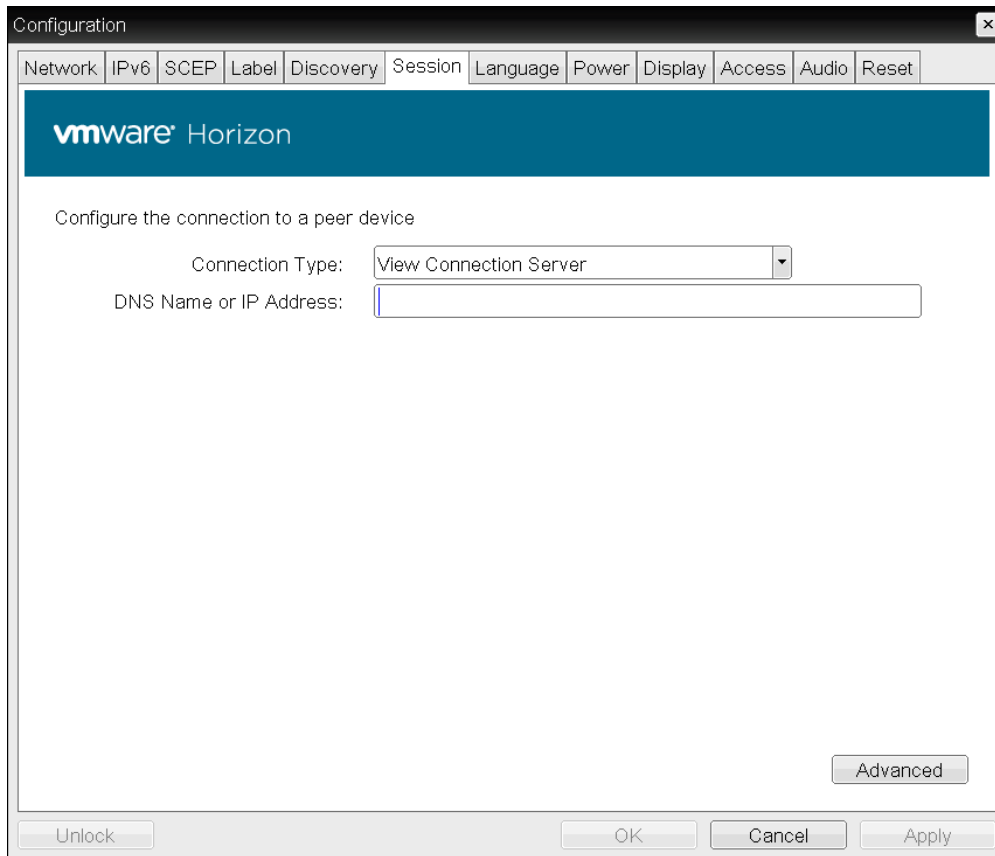| Parameter	Description
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

Parameter	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories:

Information: User- or administrator-initiated actions affecting the session:

- You have been disconnected because you logged in from another location or your host was shut down or restarted.
- You have been disconnected because an administrator disconnected you.
- You have been disconnected because you logged in from another location.
- You have been disconnected because you disconnected from your workstation.

Warning: System-initiated, but expected actions affecting the session:

- You have been disconnected because your session timed out.

Error: Unexpected system-initiated actions causing session to fail:

- You have been disconnected.
- Unable to connect (0x1001). Please contact your IT administrator.
- Unable to connect (0x1002). Please contact your IT administrator.
- Session closed remotely.
- Session closed remotely (unknown cause).
- You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.
- You have been disconnected due to a configuration error

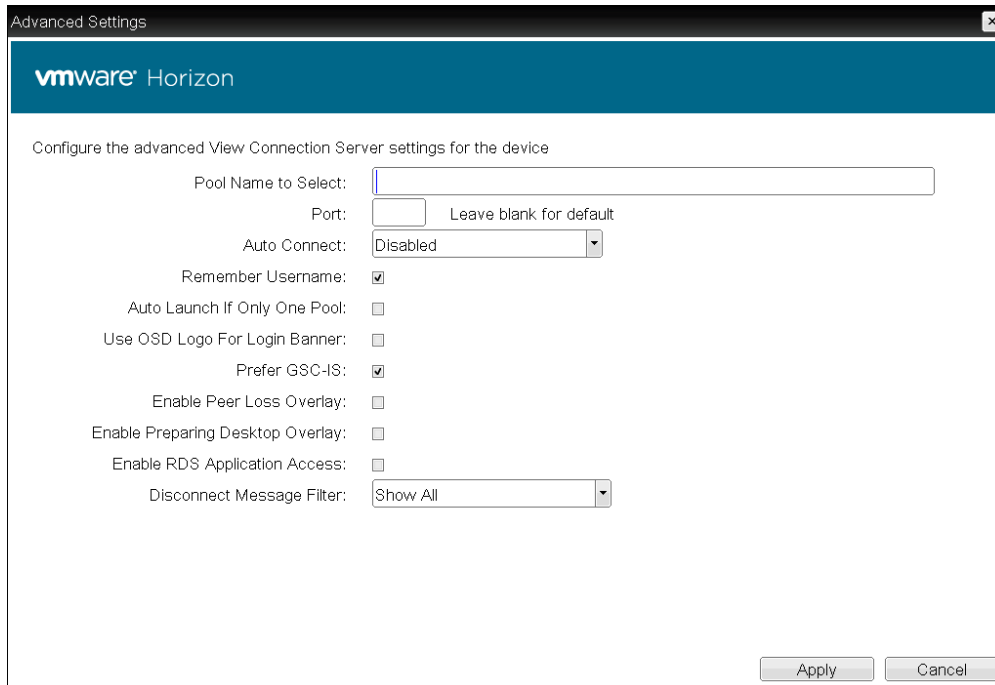| Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

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.

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

OSD Session Connection Type – View Connection Server

Advanced Settings

OSD Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Auto Connect	This field determines the client's auto connect behavior after startup: • **Enabled**: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD **Connect** page. • **Disabled**: The client does not automatically connect with the connection server. • **Enabled With Retry On Error**: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.
Remember Username	When enabled, the username text box automatically populates with the last username entered.

Parameter	Description
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.
	Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**.
	Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.
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.
	Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.
	Note: 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.
	Note: Applications open in full-screen mode, but can be re-sized once users are in session.

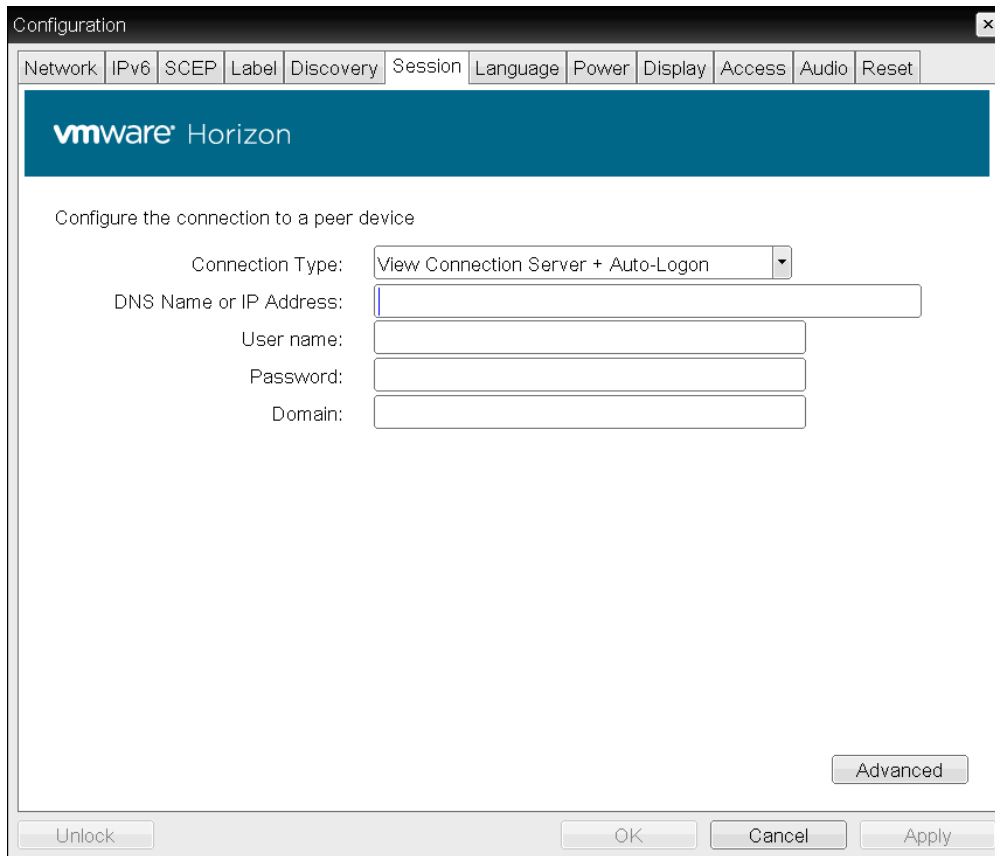| Parameter	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance. Note: For detailed information about the above session disconnect codes, please see <u>KB 15134-872</u> in the Teradici Support Site. You can choose to display: 1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages. 3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages. 4. **Show None** – Don't show any disconnect messages.

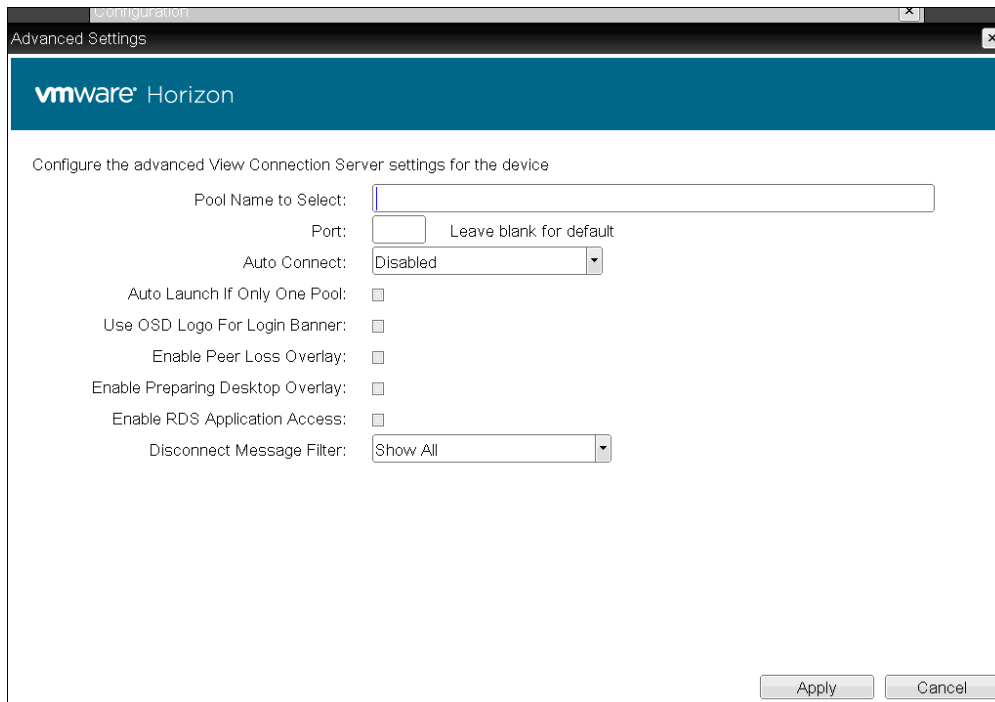# OSD: View Connection Server + Auto-Logon Session Settings

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.

Important! 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.

OSD Session Connection Type – View Connection Server + Auto-Logon

Advanced Settings

OSD Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
User name	Enter the username for the client (maximum number of characters is 128). This username 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	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Auto Connect	This field determines the client's auto connect behavior after startup: • **Enabled**: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD **Connect** page. • **Disabled**: The client does not automatically connect with the connection server. • **Enabled With Retry On Error**: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. Note: 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. Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect.

Parameter	Description
Auto Launch If Only One Pool	When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered. Note: For Tera1 zero clients, this parameter is called **Auto Launch If Only One Desktop**. Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: 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. Note: Applications open in full-screen mode, but can be re-sized once users are in session.

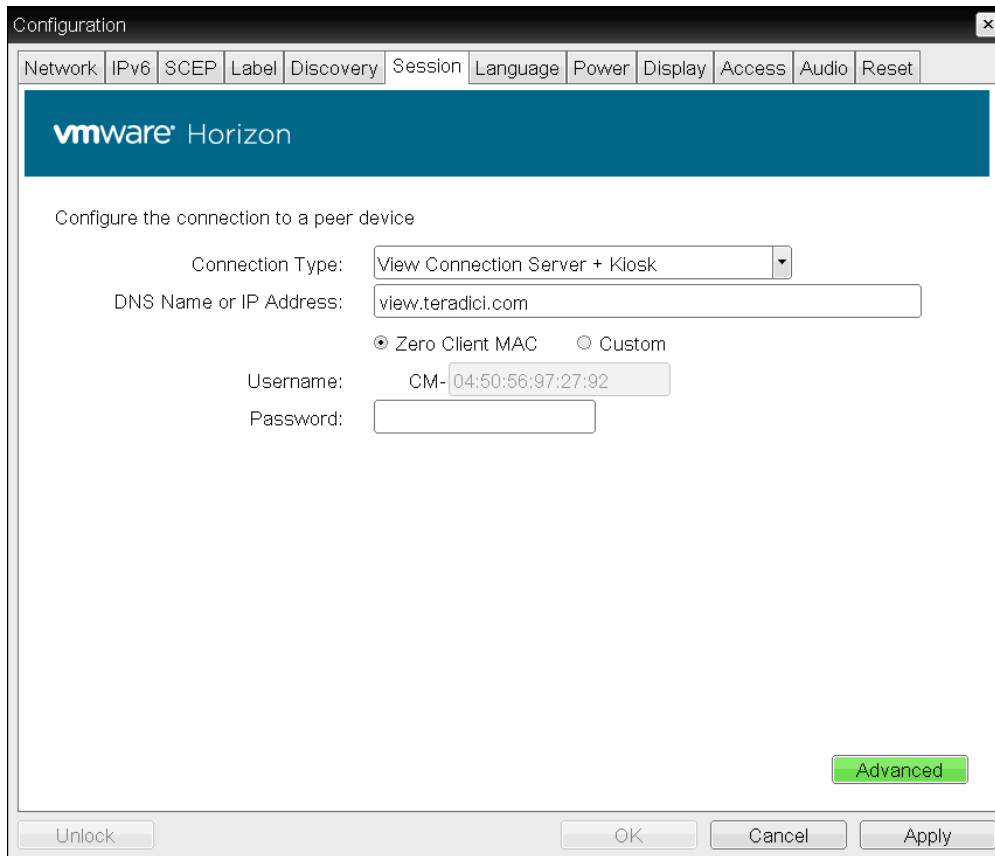| Parameter	Description
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: **Information:** User- or administrator-initiated actions affecting the session: • You have been disconnected because you logged in from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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

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.

Important! 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.

OSD Session Connection Type – View Connection Server + Kiosk

Advanced Settings

OSD Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username	Select the type of username that matches the naming you use for the devices on the View Connection Server. • **Zero Client MAC**: Select this option to automatically populate the **Username** field with the MAC address of the zero client. • **Custom**: Enter the username for the zero client. This username has the prefix "Custom." When **Custom** is selected as the username type, enter the value for this component of the custom username. 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.
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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

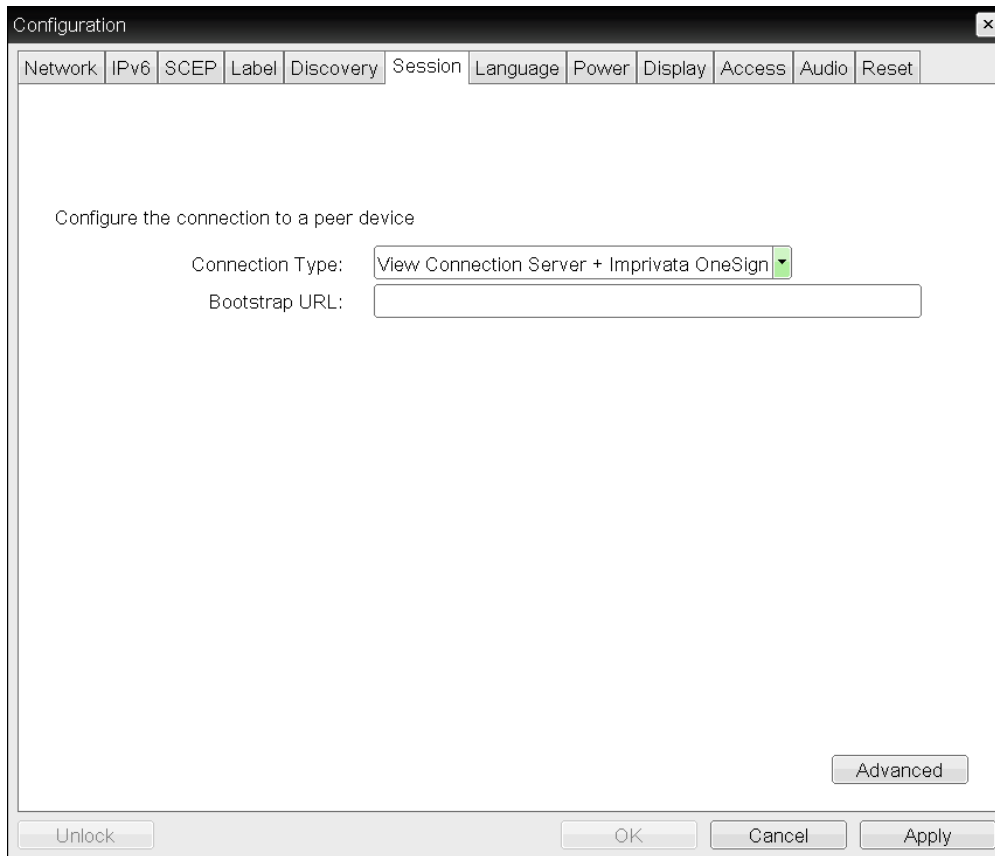| Parameter	Description
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented. Note: Applications open in full-screen mode, but can be re-sized once users are in session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

OSD: View Connection Server + Imprivata OneSign Session Settings

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

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

OSD Session Connection Type – View Connection Server + Imprivata OneSign

Advanced Settings

OSD Session Page Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	Select whether the **Pool Name to Select** property is used in OneSign mode. • **Ignore the Pool Name to Select field** • **Use the Pool Name to Select field if set** Note: For Tera1 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. Note: This field is case-insensitive. For Tera1 zero clients, this parameter is called **Desktop Name to Select**.
Remember Username	When enabled, the username 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. You can upload an OSD logo from the OSD Logo Upload page.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.

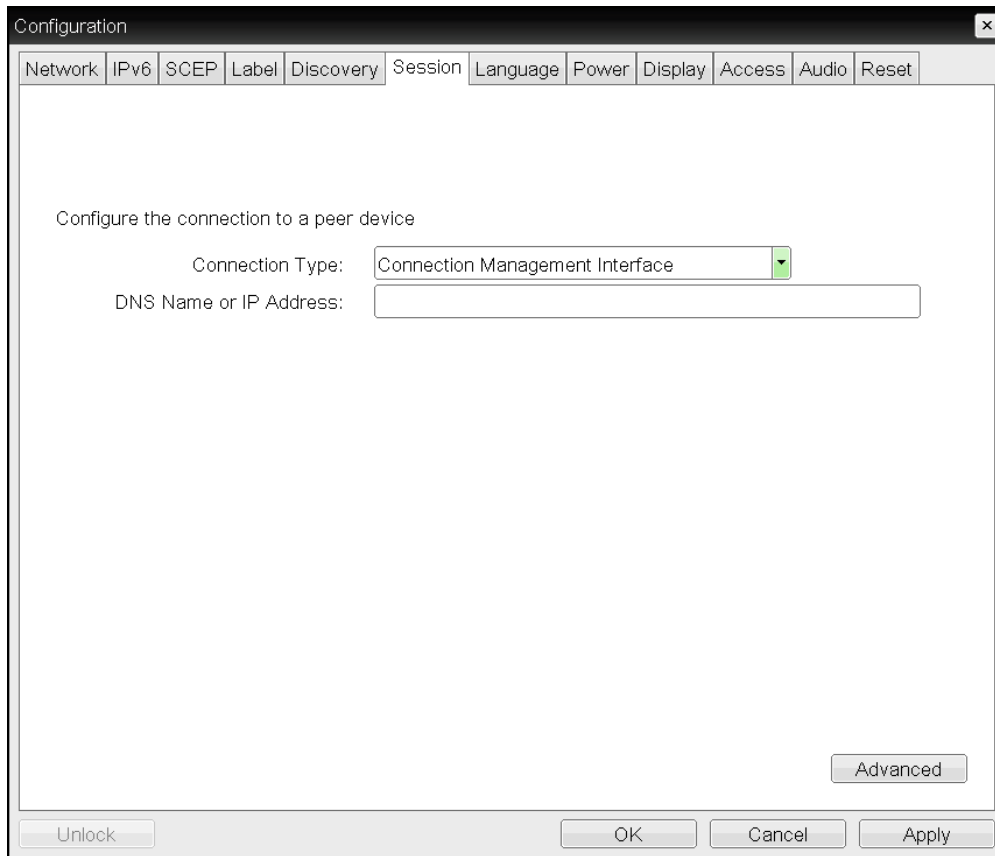| Parameter	Description
Enable RDS Application Access	When enabled *and* users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.
	Note: Applications open in full-screen mode, but can be re-sized once users are in session.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

OSD: Connection Management Interface Session Settings

Select the **Connection Management Interface** session connection type from the **Options > Configuration > Session** page to configure an external connection manager as the connection broker for the client to use.

Note: External connection managers can simplify the administration effort for large, complex systems. In a managed connection, an external connection manager server communicates with a device, and can remotely control and configure it. The connection manager can also locate an appropriate peer for the device to connect to, and then initiate the connection.

OSD Session Connection Type – Connection Management Interface
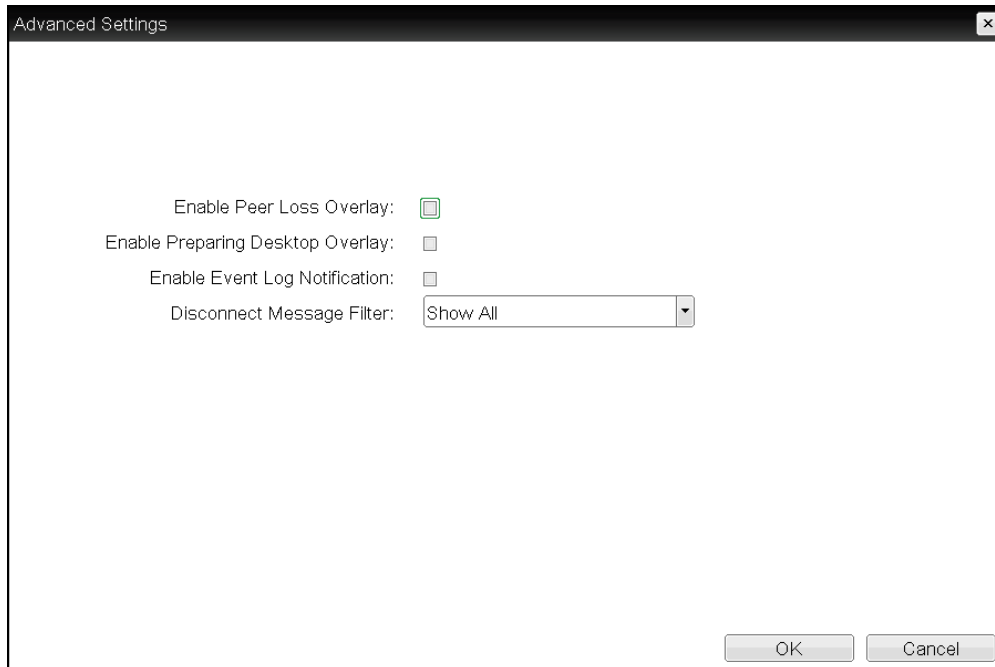
Advanced Settings

AWI Session Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the DNS name or IP address of the connection manager.
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. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC.
Enable Preparing Desktop Overlay	When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in. Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.
Enable Event Log Notification	When enabled, the client sends the contents of its event log to the connection management server.

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

Parameter	Description
	(0x401). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.
	• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.
	Note: For detailed information about the above session disconnect codes, please see KB 15134-872 in the Teradici Support Site.
	You can choose to display:
	1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.
	2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.
	3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.
	4. **Show None** – Don't show any disconnect messages.

Configuring Session Encryption

MC: Encryption Settings

The settings on this page let you configure a profile with the Transport Layer Security (TLS) level to use for negotiating PCoIP sessions between clients and hosts, and also with the encryption scheme that devices will use. At least one encryption scheme must be enabled.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Encryption Configuration

MC Encryption Configuration Parameters

Parameter	Description
Enable AES-128-GCM Encryption (Tera1)	When enabled, uses the AES-128-GCM encryption scheme to secure a PCoIP session. Note: This method offers the best performance between hardware endpoints for Tera1 devices.
Enable Salsa20-256-Round12 Encryption (Tera1)	When enabled, uses the Salsa20-256-Round12 encryption scheme to secure a PCoIP session. Note: This method may offer improved performance for Tera1 clients when connecting to VMware 4 or newer if there is more than about 7 Mbps available on the network

Parameter	Description
Session Negotiation Security Level	*Important*: In release 4.8.0, the security cipher features listed below are supported on Tera2 zero clients only. In order to use a non-SHA-1 cipher, both the client and host endpoints must support it.

Note: For sessions with software hosts, the zero client should be configured to use the **Maximum Compatibility** option.

Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.

- **Maximum Compatibility: TLS 1.0 or higher with RSA keys including ciphers that use SHA-1**: This option provides maximum compatibility.
- **Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security.
- **Disable SHA-1: TLS 1.2 with RSA keys and strong ciphers using only SHA-256 or SHA-384**: When selected, only devices running firmware 4.8.0 or greater are affected.
Note: Currently this option can only be used with Amazon WorkSpaces hosts. |
| Enable AES-128-GCM Encryption (Tera2) | When enabled, uses the AES-128-GCM encryption scheme to secure a PCoIP session. |
| Enable AES-256-GCM Encryption (Tera2) | When enabled, uses the AES-256-GCM encryption scheme to secure a PCoIP session.

Note: This method offers the best performance between hardware endpoints for Tera2 devices. |

AWI: Help for Encryption Settings

Encryption settings for the host and client AWI are located on the **Configuration > Session** page for each session connection type. For details, please refer to the field descriptions in the following topics:

- [AWI Host: Direct from Client Session Settings](#)
- [AWI Client: Direct to Host Session Settings](#)
- [AWI Client: Direct to Host + SLP Host Discovery Session Settings](#)
- [AWI Tera2 Client: PCoIP Connection Manager Settings](#)
- [AWI Tera2 Client: PCoIP Connection Manager + Auto-Logon Settings](#)
- [AWI Client: View Connection Server Session Settings](#)
- [AWI Client: View Connection Server + Auto-Logon Session Settings](#)

- [AWI Client: View Connection Server + Kiosk Session Settings](#)
- [AWI Client: View Connection Server + Imprivata OneSign Session Settings](#)

Configuring Session Bandwidth

MC: Bandwidth Settings

The settings on this page let you configure a profile with the bandwidth parameters for hosts and clients to use during a PCoIP session.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Bandwidth Configuration

MC Bandwidth Configuration Parameters

Parameter	Description
Device Bandwidth Limit	Enter the maximum bandwidth peak for hosts or clients. When configuring hosts, this setting defines the bandwidth from the host to the client (e.g., graphics data). When configuring clients, it defines the bandwidth from the client to the host (e.g., USB data).
	The usable range of the device bandwidth is 1000 to 220000 Kbps for Tera1 devices and 1000 to 600000 Kbps for Tera2 devices.
	The PCoIP processor only uses the required bandwidth up to the **Device Bandwidth Limit** maximum, and dynamically adjusts the bandwidth in response to network congestion. Setting this field to 0 configures the PCoIP processor to use the maximum rate available in the network at any time.
	We recommend setting this field to the limit of the network connected to the client and host.
	Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.
Device Bandwidth Target	Enter the temporary limit on the network bandwidth during periods of congestion. When the host or client detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it.This allows for a more even distribution of bandwidth between users sharing a congested network link.
	Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.

Parameter	Description
Device Bandwidth Floor	Enter the minimum bandwidth when congestion is present and bandwidth is required. This allows 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.
	When configuring hosts, this setting defines the minimum bandwidth from the host to the client (e.g., graphics data).When configuring clients, it defines the minimum bandwidth from the client to the host (e.g., USB data).
	A setting of 0 configures the PCoIP processor to reduce bandwidth to 1000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value.
	Note: 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 8000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm allows a graceful session startup for low bandwidth scenarios (e.g., WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.
	Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.

AWI: Bandwidth Settings

The settings on this page let you control the bandwidth used by a host or client during a PCoIP session. You can access this page from the **Configuration > Bandwidth** menu. The parameters on this page are applied immediately after you click **Apply**.

Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: 90000 kbps (0 = no limit)

Device Bandwidth Target: 0 kbps (0 = disabled)

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

Apply   Cancel

AWI Bandwidth Page

AWI Bandwidth Parameters

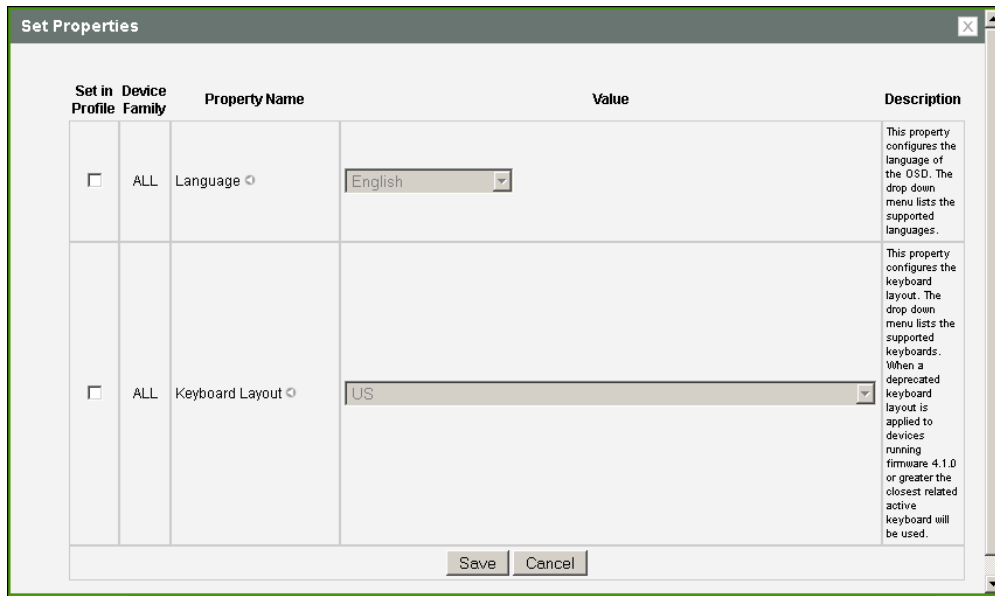| Parameter	Description
Device Bandwidth Limit	Enter the maximum bandwidth peak for hosts or clients. When configuring hosts, this setting defines the bandwidth from the host to the client (e.g., graphics data). When configuring clients, it defines the bandwidth from the client to the host (e.g., USB data).
	The usable range of the device bandwidth is 1000 to 220000 Kbps for Tera1 devices and 1000 to 600000 Kbps for Tera2 devices.
	The PCoIP processor only uses the required bandwidth up to the **Device Bandwidth Limit** maximum, and dynamically adjusts the bandwidth in response to network congestion. Setting this field to 0 configures the PCoIP processor to use the maximum rate available in the network at any time.
	We recommend setting this field to the limit of the network connected to the client and host.
	Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.

Parameter	Description
Device Bandwidth Target	Enter the temporary limit on the network bandwidth during periods of congestion. When the host or client detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it.This allows for a more even distribution of bandwidth between users sharing a congested network link. Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.
Device Bandwidth Floor	Enter the minimum bandwidth when congestion is present and bandwidth is required. This allows 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. When configuring hosts, this setting defines the minimum bandwidth from the host to the client (e.g., graphics data).When configuring clients, it defines the minimum bandwidth from the client to the host (e.g., USB data). A setting of 0 configures the PCoIP processor to reduce bandwidth to 1000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value. Note: 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 8000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm allows a graceful session startup for low bandwidth scenarios (e.g., WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use. Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps.

Configuring the Language

MC: Language Settings

The settings on this page let you configure a profile with the language to use in the OSD user interface.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Language Configuration

MC Language Configuration Parameters

Parameter	Description
Language	Configure the language to use for the OSD user interface. Note: This does not affect the language setting for the actual user session. Note: This property requires a device restart after being changed.
Keyboard Layout	Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped. Note: This property requires a device restart after being changed.

AWI Client: Language Settings

The settings on this page let you configure the language used in the OSD user interface. You can access this page from the **Configuration > Language** menu.

Language

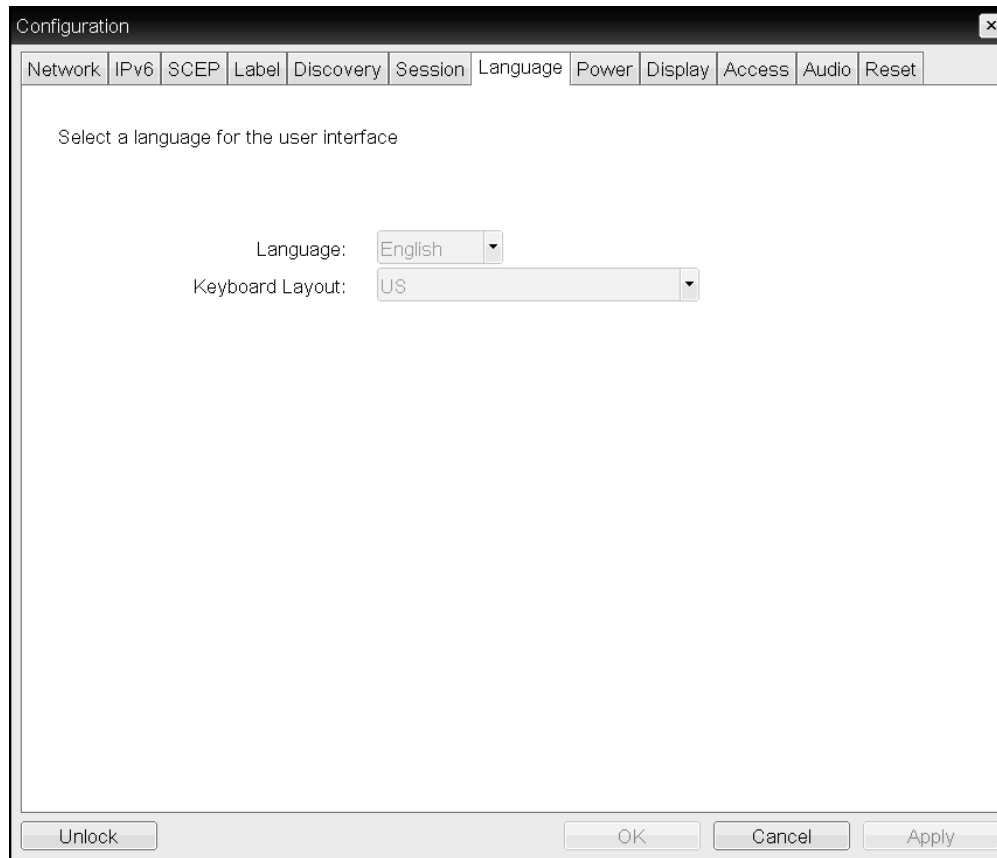Select a language for the local GUI (client only)

Language: English

Keyboard Layout: United States of America ISO-8859-1

Apply   Cancel

AWI Client Language Page

AWI Client Language Parameters

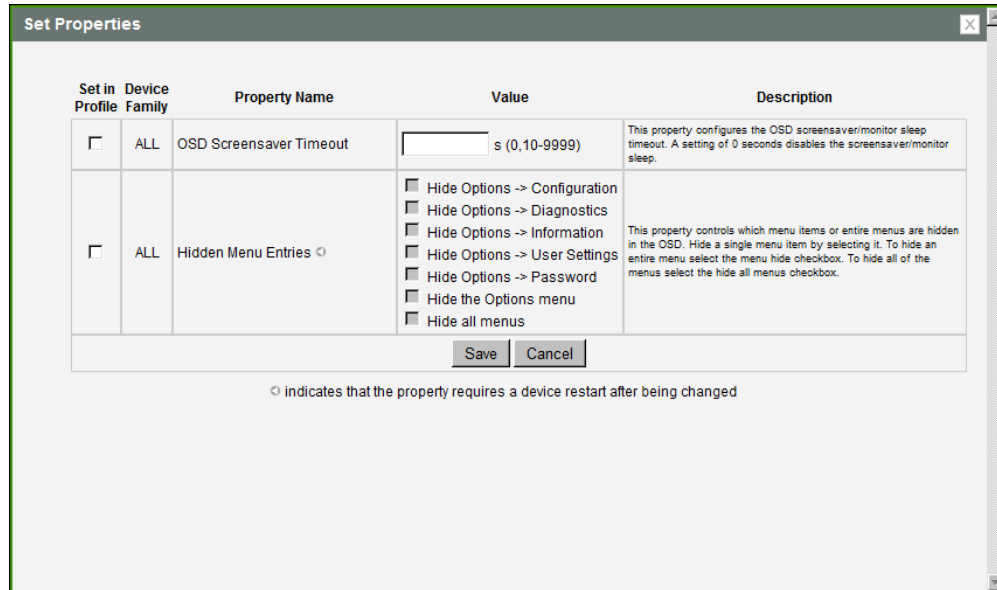| Parameter	Description
Language	Configure the language to use for the OSD user interface. Note: This does not affect the language setting for the actual user session.
Keyboard Layout	Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped.

OSD: Language Settings

The settings on this page let you configure the language used in the OSD user interface. You can access this page from the **Options > Configuration > Language** menu.

OSD Language Page

OSD Language Parameters

Parameter	Description
Language	Configure the language to use for the OSD user interface. Note: This does not affect the language setting for the actual user session.
Keyboard Layout	Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped.

Configuring OSD Parameters

MC: OSD Settings

The settings on this page let you configure a profile with the screen-saver timeout value to use on a device's OSD, and also to control which menus and menu items are

hidden in the OSD.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC OSD Configuration

MC Language Configuration Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is *not* in session.
Hidden Menu Entries	Select the items that you do not want to appear on the OSD local GUI. You can hide a single menu item, the entire **Options** menu, or all menus. Note: This property requires a device restart after being changed.

AWI Client: Help for OSD Screen-saver Settings

The OSD screen-saver timeout setting is located on the AWI **Configuration > Power** page for the following clients:

- Tera2 zero client Power page
- Tera1 zero client Power page

OSD: Help for OSD Screen-saver Settings

The OSD screen-saver timeout setting is located on the OSD **Configuration > Power** page for the following clients:

- Tera2 zero client Power page
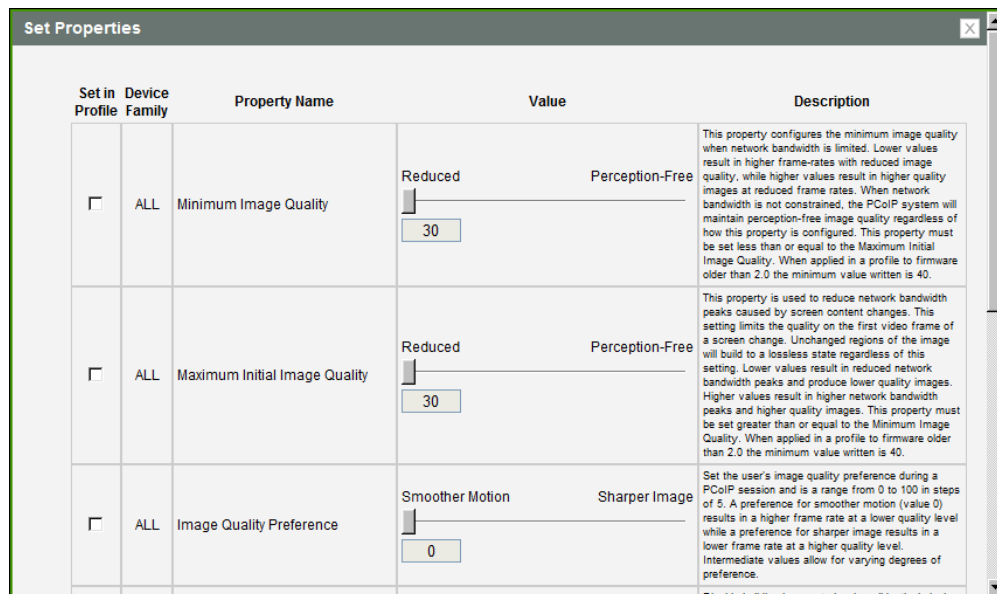- Tera1 zero client Power page

Configuring Image Quality

MC: Image Settings

The **Image** page lets you configure a profile to make changes to the image quality of the PCoIP session.

Note: This setting applies only to sessions between zero clients and hosts.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Image Configuration
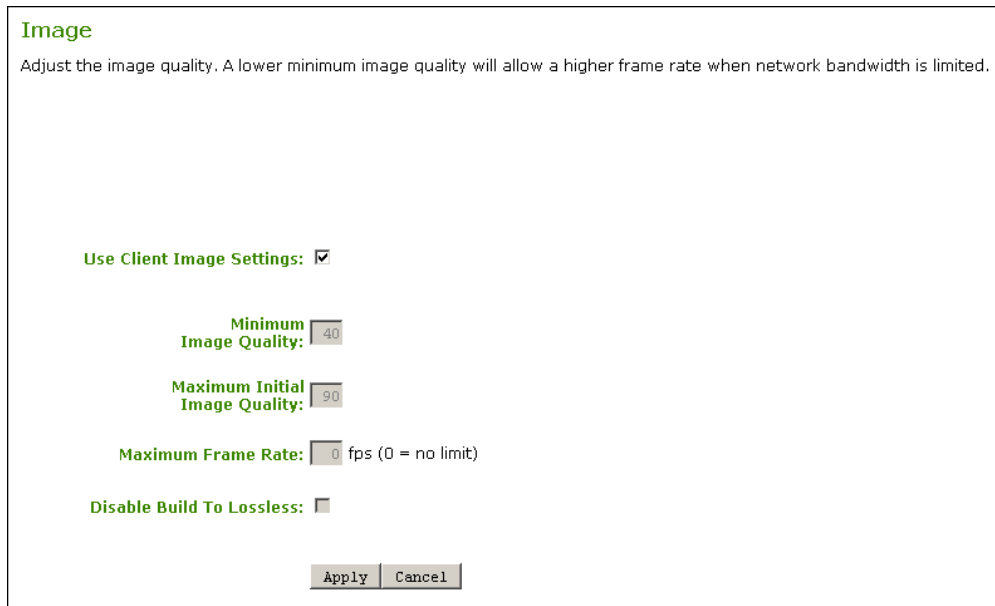
MC Image Configuration Parameters

Parameter	Description
Minimum Image Quality	Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Maximum Initial Image Quality	Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

Parameter	Description
Disable Build to Lossless	Leave this field unchecked 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 (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting. **Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination. If you do choose to turn on this field, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Enable Client Image Settings	When enabled, allows the host the option of using the client's image settings for the session. When disabled, the host's image settings take effect. Note: The Image Quality Preference setting is exempt from this rule.
Maximum Frame Rate	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. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Low Bandwidth Text Codec Mode (TERA2321 zero clients only)	The Low Bandwidth Text Codec is a new compression method that provides improved bandwidth usage when encoding lossless data, such as text and background. It does not apply to lossy data, such as video. Enable this parameter and select **Enabled** to configure a profile for TERA2321 zero clients with this feature.

AWI Host: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can access this page from the **Configuration > Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.

AWI Host Image Page
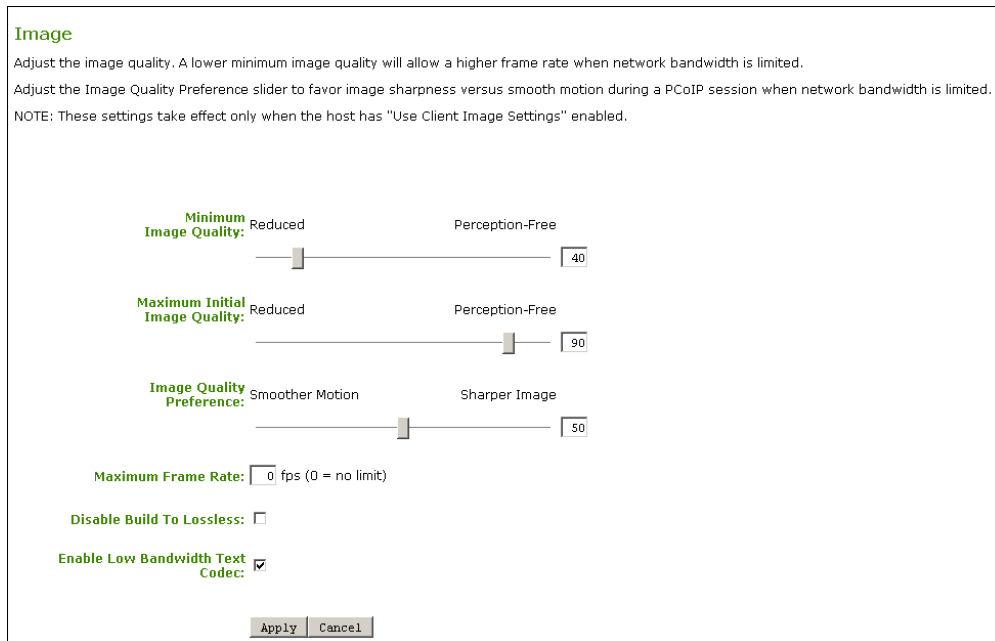
AWI Host Image Page Parameters

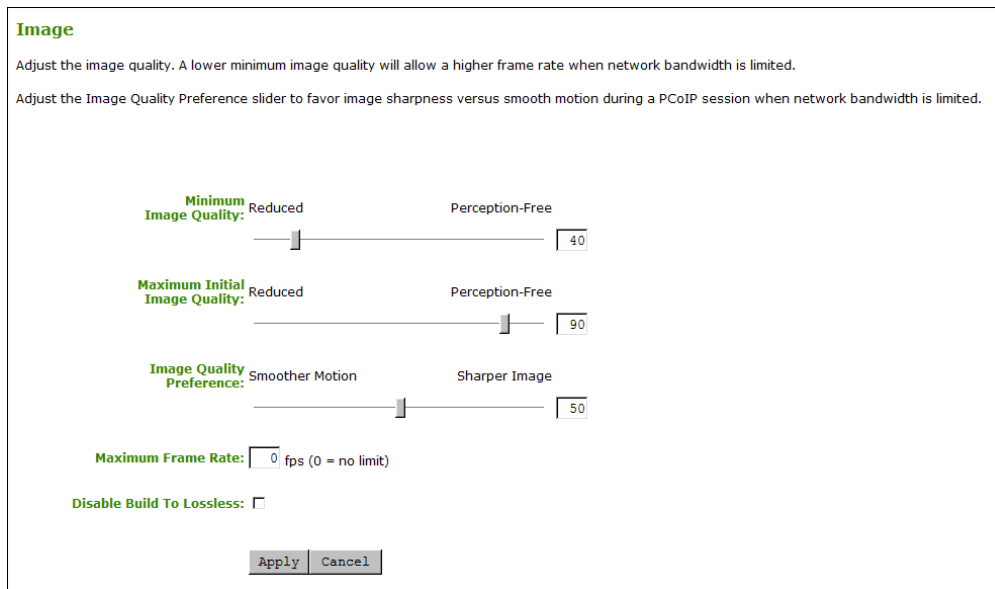| Parameter	Description
Use Client Image Settings	When enabled, the image settings on this page are not editable. The settings that appear (grayed out) are those stored for the host in flash. When disabled, the image settings are editable and are applied to any current sessions.
Minimum Image Quality	Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.

Parameter	Description
Maximum Initial Image Quality	Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Maximum Frame Rate	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. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Disable Build to Lossless	Leave this field unchecked 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 (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting. **Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination. If you do choose to turn on this field, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

AWI Tera2 Client: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can access this page from the **Configuration > Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.

AWI Client Image Page

AWI Client Image Page Parameters

Parameter	Description
Minimum Image Quality	Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate.
	In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter.
	Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.

Parameter	Description
Maximum Initial Image Quality	Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Maximum Frame Rate	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. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Disable Build to Lossless	Leave this field unchecked 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 (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting. **Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination. If you do choose to turn on this field, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

Parameter	Description
Enable Low Bandwidth Text Codec (TERA2321 zero clients only)	When enabled, Low Bandwidth Text Codec Mode will be used for TERA2321 zero clients. The Low Bandwidth Text Codec is a new compression method that provides improved bandwidth usage when encoding lossless data, such as text and background. It does not apply to lossy data, such as video. This option is disabled by default.

AWI Tera1 Client: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can access this page from the **Configuration > Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.

AWI Client Image Page

AWI Client Image Page Parameters

Parameter	Description
Minimum Image Quality	Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Maximum Initial Image Quality	Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**.
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.
Maximum Frame Rate	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. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

Parameter	Description
Disable Build to Lossless	Leave this field unchecked 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 (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.
	Warning: Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination.
	If you do choose to turn on this field, the PCoIP protocol rapidly builds the client image to a high quality image that may be perceptually lossless, but is not a fully lossless state. This may provide some bandwidth savings, but is not recommended for use cases that require images and desktop content to be truly lossless.
	Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

OSD: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can access this page from the **Options > User Settings > Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.
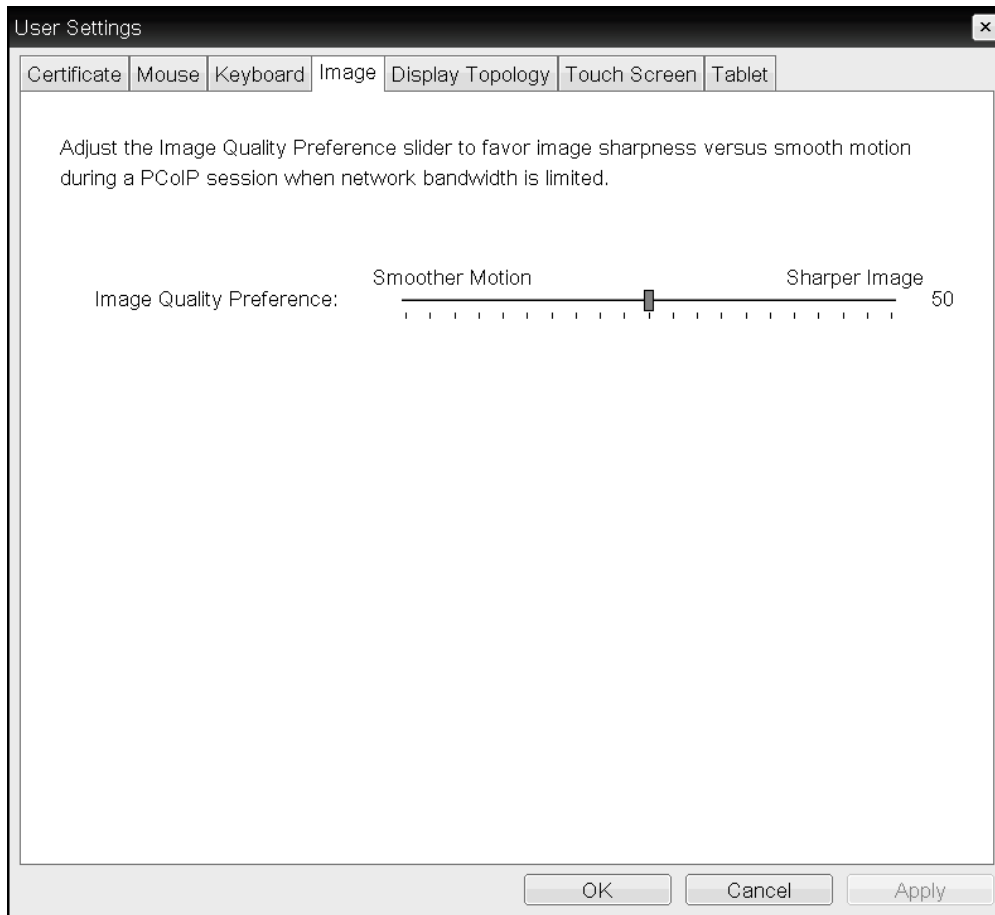
OSD Image Page

Note: In the OSD, this page is available from the **Options->User Settings** menu.

OSD Image Page Parameters

Parameter	Description
Image Quality Preference	Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. Note: This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

Configuring Monitor Emulation and Display Settings

MC: Display Settings

The **Display** page lets you configure a profile to enable or disable the monitor emulation feature. It also allows you to enable display cloning for TERA2321 zero client profiles.

Some PCs and workstations do not boot if a display is not attached. The monitor emulation feature presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host. For further details about Teradici's monitor emulation feature, see Monitor Emulation.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Monitor Emulation Page

MC Monitor Parameters

Parameter	Description
Enable Monitor Emulation on Video Port 1	When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector. The ports are mapped one-to-one and in sequential order (e.g., client port 1 to emulated port 1, and so on).
	When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active and a client display is attached.
	Note: Enabling this field can help resolve problems where video is not present at the client.
	Note: This property requires a device restart after being changed.
Enable Monitor Emulation on Video Port 2	This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector.
	Note: This property requires a device restart after being changed.
Enable Monitor Emulation on Video Port 3	This field affects DDC queries for the port 3 connector, and provides functionality similar to that for the port 1 connector.
	Note: This property requires a device restart after being changed.
Enable Monitor Emulation on Video Port 4	This field affects DDC queries for the port 4 connector, and provides functionality similar to that for the port 1 connector.
	Note: This property requires a device restart after being changed.
Enable Host Hot-Plug Delay	When enabled, allows lengthier hot plug de-assert/assert profiles on the host. Enabling this feature allows the host to resolve black screen issues with certain Linux GPU driver timing expectations.
Enable Display Cloning (TERA2321 zero clients only)	When enabled, display output on Port 1 is cloned on Port 2 so that both displays show the same content.
	Note: If you are connecting a TERA2321 zero client to a remote workstation that does not have the PCoIP host software installed and the host driver function enabled, *and* you are using monitor emulation on the remote workstation, you may experience black screens on the cloned displays. To remedy the problem, you can either install and enable the host software, or you can disable monitor emulation on the video port for the secondary display only.
Enable Preferred Resolution Override	When enabled, devices can be configured to override the preferred (native) resolution of a display on a given port.
	Note: If you enable this property, the preferred override resolution settings on all ports must be set.

Parameter	Description
Preferred Override Resolution on Port 1	When enabled, this property allows you to select a preferred override resolution for the display attached to the specified port. If the display does not support the resolution you select from the drop-down list, the display's native resolution will be used. Note: The **Enable Preferred Resolution Override** property must be enabled and set to **True** when this feature is configured. Note: Setting a dual-link only resolution on a device with a single-link display attached to this port will cause the profile application to fail.
Preferred Override Resolution on Port 2	When enabled, this property allows you to select a preferred override resolution for the display attached to the specified port. If the display does not support the resolution you select from the drop-down list, the display's native resolution will be used. Note: The **Enable Preferred Resolution Override** property must be enabled and set to **True** when this feature is configured. Note: Setting a dual-link only resolution on a device with a single-link display attached to this port will cause the profile application to fail.
Preferred Override Resolution on Port 3	When enabled, this property allows you to select a preferred override resolution for the display attached to the specified port. If the display does not support the resolution you select from the drop-down list, the display's native resolution will be used. Note: The **Enable Preferred Resolution Override** property must be enabled and set to **True** when this feature is configured. Note: Setting a dual-link only resolution on a device with a single-link display attached to this port will cause the profile application to fail.
Preferred Override Resolution on Port 4	When enabled, this property allows you to select a preferred override resolution for the display attached to the specified port. If the display does not support the resolution you select from the drop-down list, the display's native resolution will be used. Note: The **Enable Preferred Resolution Override** property must be enabled and set to **True** when this feature is configured. Note: Setting a dual-link only resolution on a device with a single-link display attached to this port will cause the profile application to fail.
Enable Accelerated Monitor Emulation	When enabled, this property accelerates the delivery of EDID information to host systems that boot up very quickly (e.g., faster than five seconds), causing blank screens on the remote end. Typically, these are systems with solid-state drives (SSDs).

AWI Tera2 Host: Monitor Emulation

The **Monitor Emulation** page lets you enable or disable monitor emulation for the video ports on your remote workstation. You can access this page from the **Configuration > Monitor Emulation** menu.

Some PCs and workstations do not boot if a display is not attached. The monitor emulation feature presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host. For further details about Teradici's monitor emulation feature, see Monitor Emulation.

Note: If monitor emulation is performed in hardware for a device, the the AWI **Configuration** menu will not have a **Monitor Emulation** option. This is the case for most Tera1 remote workstation cards.

AWI Tera2 Host Monitor Emulation Page
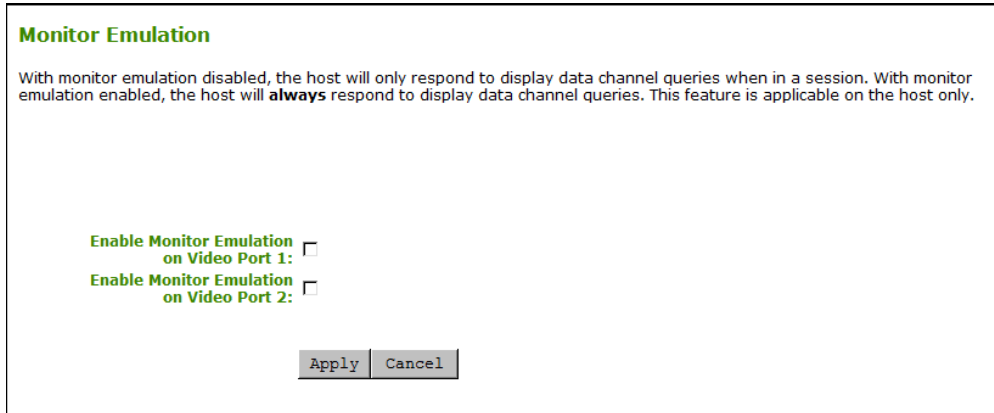
AWI Tera2 Host Monitor Parameters

Parameter	Description
Enable Monitor Emulation on Video Port 1	When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector. The ports are mapped one-to-one and in sequential order (e.g., client port 1 to emulated port 1, and so on). When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active and a client display is attached. Note: Enabling this field can help resolve problems where video is not present at the client.
Enable Monitor Emulation on Video Port 2	This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector.
Enable Monitor Emulation on Video Port 3	This field affects DDC queries for the port 3 connector, and provides functionality similar to that for the port 1 connector.
Enable Monitor Emulation on Video Port 4	This field affects DDC queries for the port 4 connector, and provides functionality similar to that for the port 1 connector.
Enable Host Hot-Plug Delay	When enabled, allows lengthier hot plug de-assert/assert profiles on the host. Enabling this feature allows the host to resolve black screen issues with certain Linux GPU driver timing expectations.
Enable Accelerated Monitor Emulation	When enabled, this property accelerates the delivery of EDID information to host systems that boot up very quickly (e.g., faster than five seconds), causing blank screens on the remote end. Typically, these are systems with solid-state drives (SSDs).

AWI Tera1 Host: Monitor Emulation

The **Monitor Emulation** page lets you enable or disable monitor emulation for the video ports on your remote workstation. You can access this page from the **Configuration > Monitor Emulation** menu.

Some PCs and workstations do not boot if a display is not attached. The monitor emulation feature presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host. For further details about Teradici's monitor emulation feature, see [Monitor Emulation](#).

Note: If monitor emulation is performed in hardware for a device, the the AWI **Configuration** menu will not have a **Monitor Emulation** option. This is the case for most Tera1 remote workstation cards.

Monitor Emulation

With monitor emulation disabled, the host will only respond to display data channel queries when in a session. With monitor emulation enabled, the host will **always** respond to display data channel queries. This feature is applicable on the host only.

Enable Monitor Emulation on Video Port 1: ☐
Enable Monitor Emulation on Video Port 2: ☐

Apply   Cancel

AWI Tera1 Host Monitor Emulation Page

AWI Tera1 Host Monitor Parameters

Parameter	Description
Enable Monitor Emulation on Video Port 1	When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector. The ports are mapped one-to-one and in sequential order (e.g., client port 1 to emulated port 1, and so on). When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active and a client display is attached. Note: Enabling this field can help resolve problems where video is not present at the client.
Enable Monitor Emulation on Video Port 2	This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector.

Configuring Time

MC: Time Settings

The **Time** page lets you configure a profile with the Network Time Protocol (NTP) parameters to use to allow the host and client event logs to be time-stamped based on NTP time.

Note: If the client 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 disabled.

Note: The client does not get time zone or Daylight Saving Time (DST) information from the NTP server.

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

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Time Configuration

MC Time Configuration Parameters

Parameter	Description
NTP Server Hostname	Configure the IP address or fully qualified domain name (FQDN) of the NTP server that the host or client will contact to determine the current time.
NTP Server Port	Configure the port number of the NTP server. The default NTP server port value is 123.
NTP Query Interval	Configure how often (in seconds) the host or client will contact the NTP server to update the current time. The default query interval is 86400 seconds, which is equivalent to 24 hours.

Parameter	Description
Enable DST	Enable or disable the automatic adjustment for Daylight Saving Time (DST).
Time Zone Offset	Select the desired time zone.

AWI: Time Settings

The **Time** page lets you configure Network Time Protocol (NTP) parameters to allow the host and client event logs to be time-stamped based on NTP time.

Note: If the client 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 disabled.

Note: The client does not get time zone or Daylight Saving Time (DST) information from the NTP server.

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

You can access this page from the **Configuration > Time** menu.

AWI Time Page

AWI Time Page Parameters

Parameter	Description
Current Time	Displays the time based on the NTP.
Enable NTP	Enable or disable the NTP feature.
Identify NTP Host by	Select if the NTP host is identified by IP address or by fully qualified domain name (FQDN). If NTP is disabled, this field is not required and is not editable. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose. • **IP Address**: Shows the NTP Host IP address • **FQDN**: Shows the NTP Host DNS name
NTP Host Port	Configure the port number of the NTP server. The default NTP server port value is 123.
NTP Query Interval	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 Savings Time	Enable or disable the automatic adjustment for Daylight Saving Time (DST).

Configuring Security

MC: Security Settings

The settings on this page let you configure a profile with the security parameters to use for hosts and clients.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
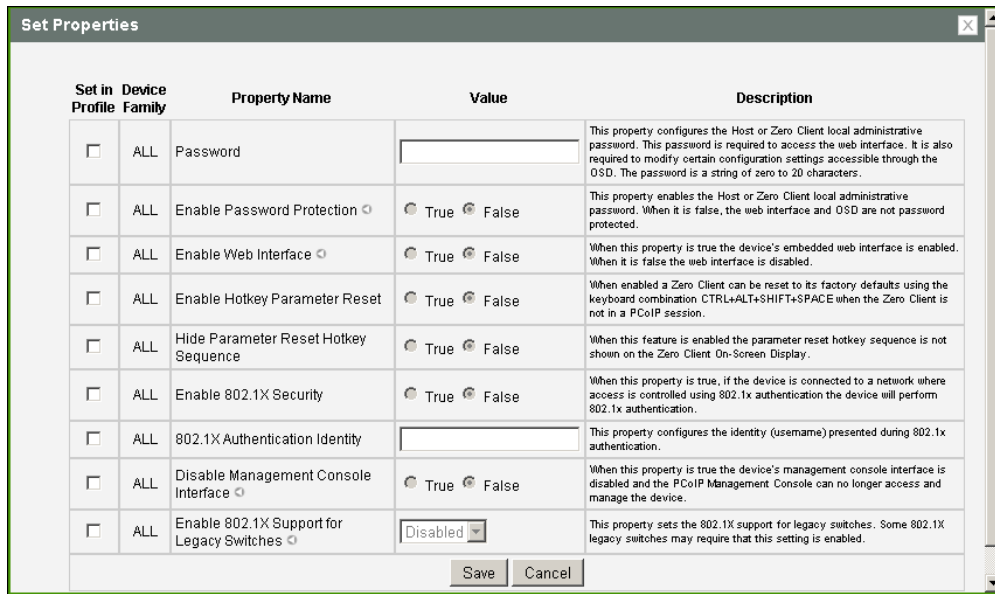
MC Security Configuration

MC Security Configuration Parameters

Parameter	Description
Password	Enter the password for the host or client Administrative Web Interface (AWI). This password is also required to modify certain configuration settings accessible through the client On Screen Display (OSD). This field accepts a string of zero to 20 characters.
Enable Password Protection	When enabled, the host or client AWI password is required. When disabled, the AWI and OSD are not password protected. Note: This property requires a device restart after being changed.
Enable Web Interface	When enabled, the host or client can be accessed and managed using the AWI is enabled. When disabled, the device cannot be accessed or managed using the AWI. Note: This property requires a device restart after being changed.
Enable Hotkey Parameter Reset	When enabled, the client can be reset to its factory defaults using the keyboard combination Ctrl+Alt+Shift+Space when the client is not in a PCoIP session.
Hide Parameter Reset Hotkey Sequence	When enabled, the reset hotkey sequence is not shown on the client OSD.

Parameter	Description
Enable 802.1X Security	When enabled, the device will perform 802.1x authentication if it is connected to a network where access is controlled using 802.1x authentication.
802.1X Authentication Identity	Configure the username to present for 802.1x authentication.
Disable Management Console Interface	When enabled, the management console interface is disabled, and the device cannot be accessed or managed by the MC (or any other PCoIP device management tool). Note: This property requires a device restart after being changed.
Enable 802.1X Support for Legacy Switches	When enabled, allows greater 802.1x compatability for older switches on the network. Note: This property requires a device restart after being changed.

AWI: Help for Security Settings

The following 802.1x security settings for the AWI are located on the Network page (accessed from the **Configuration > Network** menu):

- Enable 802.1x Security
- Authentication
- Identity
- Client Certificate
- Enable 802.1x Legacy Support

The following administrative access security settings for the AWI are located on the Access page (accessed from the **Configuration > Access** menu):

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

OSD: Help for Security Settings

The following administrative access security settings for the OSD are located on the Access page (accessed from the **Options > Configuration > Access** menu):

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

Configuring Audio

MC: Audio Permissions

The settings on this page let you configure a profile with the audio parameters to use for hosts and clients.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Audio Permissions

MC Audio Permissions Parameters

Parameter	Description
Enable Audio	When enabled, configures audio support on the device. Note: This property must be enabled on both the host and the client. When disabled, the audio hardware is not available for the host operating system to enumerate. Note: This property requires a device restart after being changed.

Parameter	Description
Enable Microsoft Windows Vista 64-bit Mode	Enable this option for Windows Vista 64-bit and Windows 7 64-bit version operation systems.
	Warning: Do NOT use this mode with Windows XP 64- or 32-bit operating systems.
	You do not have to enable the 64-bit mode for Linux 64-bit operating systems. Linux kernels should be compiled with the latest PCoIP audio CODEC support.
	Note: This property requires a device restart after being changed.
Enable Audio Line In	Determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input.
Enable Local USB Audio Driver (Tera2 only)	This option locally terminates any USB audio devices that are attached to the zero client.
	When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience.
	When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions.
Audio In Device Type (Tera2 only)	This field applies when the **Enable Local USB Audio Driver** option is enabled and both an analog input device and a USB input device are connected to the zero client. Because only one audio device can be used at a time when devices are locally terminated, select the type of device you wish to use for audio recording:
	• **Analog**: The analog input device plugged into the analog input jack on the zero client will be used for audio recording.
	• **USB**: The USB input device attached to the zero client will be used for audio recording. If more than one is attached, the **Audio Input** options below let you specify the preferred one to use.
Audio In Preferred USB Device Vendor ID (Tera2 only)	Enter the Vendor ID (VID) for the preferred USB audio input device. If a user connects more than one USB audio input device to the zero client, the device specified here will be used for audio input.
	Note: When both the VID and PID are set to 0000, any connected USB audio device will be used for audio input.

Parameter	Description
Audio In Preferred USB Device Product ID (Tera2 only)	Enter the Product ID (PID) for the preferred USB audio input device. If a user connects more than one USB audio input device to the zero client, the device specified here will be used for audio input. Note: When both the VID and PID are set to 0000, any connected USB audio device will be used for audio input.
Audio Out Device Type (Tera2 only)	This field applies when the **Enable Local USB Audio Driver** option is enabled and both an analog output device and a USB output device are connected to the zero client. Because only one audio device can be used at a time when devices are locally terminated, select the type of device you wish to use for audio playback: ● **Analog**: The analog output device plugged into the analog input jack on the zero client will be used for audio playback. ● **USB**: The USB output device attached to the zero client will be used for audio playback. If more than one is attached, the **Audio Output** options below let you specify the preferred one to use.
Audio Out Preferred USB Device Vendor ID (Tera2 only)	Enter the Vendor ID (VID) for the preferred USB audio output device. If a user connects more than one USB audio output device to the zero client, the device specified here will be used for audio output. Note: When both the VID and PID are set to 0000, any connected USB audio device will be used for audio output.
Audio Out Preferred USB Device Product ID (Tera2 only)	Enter the Product ID (PID) for the preferred USB audio output device. If a user connects more than one USB audio output device, the device specified here will be used for audio output. Note: When both the VID and PID are set to 0000, any connected USB audio device will be used for audio output.
Dual Audio Output Mode (Tera2 only)	When enabled, all VM audio is sent to both an external speaker and a USB headset (e.g., the inbound ringer audio for CounterPath Bria softphones).

AWI Tera2 Host: Audio Settings

The **Audio** page lets you configure audio options for the device. You can access this page from the **Configuration > Audio** menu.

Note: After configuring the desired options, click **Apply** and then **Continue** to have your changes take effect.

AWI Tera2 Host Audio Page

AWI Tera2 Host Audio Page Parameters

Parameter	Description
Enable Audio	When enabled, configures audio support on the device. Note: This property must be enabled on both the host and the client. When disabled, the audio hardware is not available for the host operating system to enumerate.
Enable Audio Line In	Determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input. Note: Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device.

AWI Tera2 Client: Audio Settings

The **Audio** page lets you configure audio options for the device. You can access this page from the **Configuration > Audio** menu.

Note: After configuring the desired options, click **Apply** and then **Continue** to have your changes take effect.

AWI Client Audio Page

AWI Client Audio Page Parameters

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

Parameter	Description
Enable Local USB Audio Driver	This option locally terminates any USB audio devices that are attached to the zero client.
	When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience.
	When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions.
	Note: For bi-directional audio support (e.g., microphone as well as playback), the Teradici Audio Driver must be installed on your VM and selected as the default playback device.
	Important! If you are using a USB composite device that contains audio functionality but also has one or more functions that must be bridged (i.e., terminated remotely so the host OS can install the driver), the local USB audio driver cannot be used for the device.
Enable Dual Audio Output (Tera2 only)	When enabled, all VM audio is sent to both an external speaker and a USB headset (e.g., the inbound ringer audio for CounterPath Bria softphones).
Audio Input	The options in this section let you specify the preferred device to use for audio input (recording). They are available when **Enable Local USB Audio Driver** is selected.
Audio Device Type	This field applies when the **Enable Local USB Audio Driver** option is enabled and both an analog input device and a USB input device are connected to the zero client. Because only one audio device can be used at a time when devices are locally terminated, select the type of device you wish to use for audio recording:
	• **Analog**: The analog input device plugged into the analog input jack on the zero client will be used for audio recording.
	• **USB**: The USB input device attached to the zero client will be used for audio recording. If more than one is attached, the **Audio Input** options below let you specify the preferred one to use.
Preferred USB Device Vendor ID	This field is automatically populated with the USB device's vendor ID (VID) after you select the preferred audio input device in the **Attached USB devices** drop-down list and apply your changes. You can also manually enter the VID of the preferred attached USB device.
	Note: This option does not apply to analog audio devices.

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

AWI Tera1 Host: Audio Settings

The **Audio** page lets you configure audio options for the device. You can access this page from the **Configuration > Audio** menu.

Note: After configuring the desired options, click **Apply** and then **Continue** to have your changes take effect.

AWI Tera1 Host Audio Page

AWI Tera1 Host Audio Page Parameters

Parameter	Description
Enable Audio	When enabled, configures audio support on the device.
	Note: This property must be enabled on both the host and the client.
	When disabled, the audio hardware is not available for the host operating system to enumerate.
Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode	Enable this option for Windows Vista 64-bit and Windows 7 64-bit version operation systems.
	Warning: Do NOT use this mode with Windows XP 64- or 32-bit operating systems.
	You do not have to enable the 64-bit mode for Linux 64-bit operating systems. Linux kernels should be compiled with the latest PCoIP audio CODEC support.
Enable Audio Line In	Determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input.
	Note: Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device.

AWI Tera1 Client: Audio Settings

The **Audio** page lets you configure audio options for the device. You can access this page from the **Configuration > Audio** menu.

Note: After configuring the desired options, click **Apply** and then **Continue** to have your changes take effect.

AWI Client Audio Page

AWI Client Audio Page Parameters

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

OSD Tera2: Audio Settings

The **Audio** page lets you configure audio options for the device.

You can access this page from the **Options > Configuration > Audio** menu.
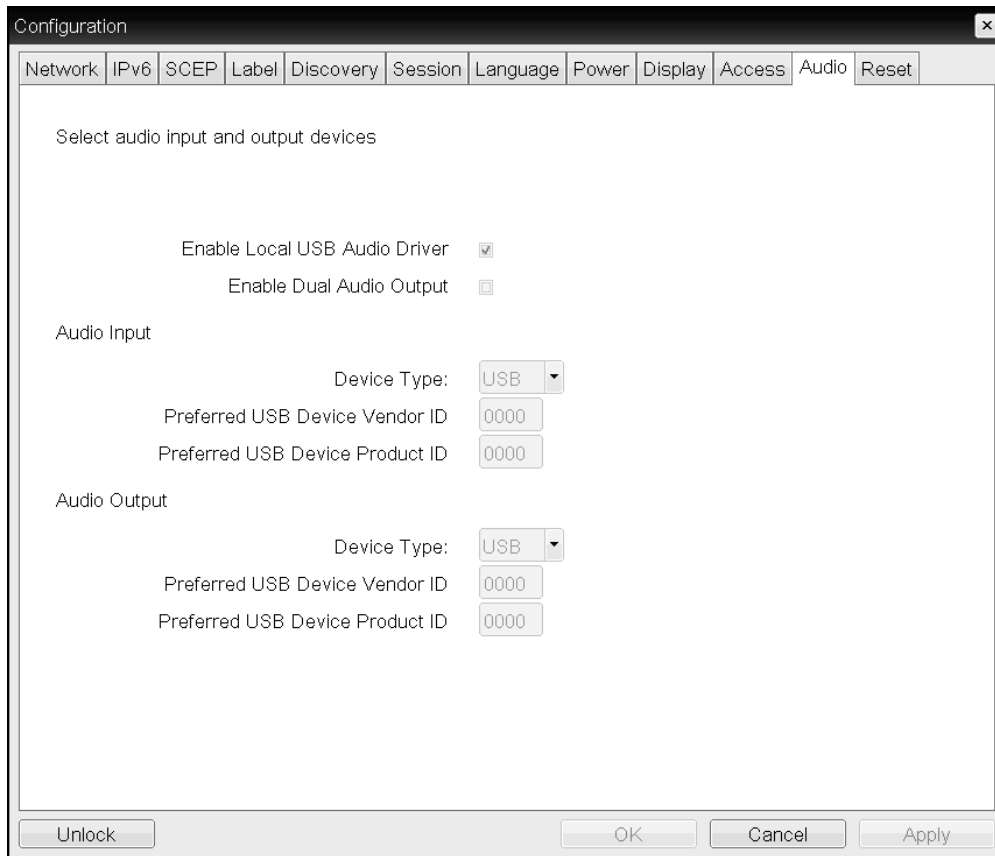
OSD Audio Page

OSD Audio Page Parameters

Parameter	Description
Enable Local USB Audio Driver	This option locally terminates any USB audio devices that are attached to the zero client. When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience. When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions. Note: For bi-directional audio support (e.g., microphone as well as playback), the Teradici Audio Driver must be installed on your VM and selected as the default playback device. **Important**! If you are using a USB composite device that contains audio functionality but also has one or more functions that must be bridged (i.e., terminated remotely so the host OS can install the driver), the local USB audio driver cannot be used for the device.
Enable Dual Audio Output (Tera2 only)	When enabled, all VM audio is sent to both an external speaker and a USB headset (e.g., the inbound ringer audio for CounterPath Bria softphones).
Audio Input	The options in this section let you specify the preferred device to use for audio input (recording). They are available when **Enable Local USB Audio Driver** is selected.
Device Type	This field applies when the **Enable Local USB Audio Driver** option is enabled and both an analog input device and a USB input device are connected to the zero client. Because only one audio device can be used at a time when devices are locally terminated, select the type of device you wish to use for audio recording: • **Analog**: The analog input device plugged into the analog input jack on the zero client will be used for audio recording. • **USB**: The USB input device attached to the zero client will be used for audio recording. If more than one is attached, the **Audio Input** options below let you specify the preferred one to use.
Preferred USB Device Vendor ID	This field is automatically populated with the USB device's vendor ID (VID) after you select the preferred audio input device in the **Attached USB devices** drop-down list and apply your changes. You can also manually enter the VID of the preferred attached USB device. Note: This option does not apply to analog audio devices.

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

Configuring Unified Communications

MC: Unified Communications

The settings on this page let you configure a profile for Tera2 zero clients with Unified Communications (UC) support for interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client.

Note: For details on how to capture network packets to help troubleshoot a Bria Virtualized Edition softphone call, see the AWI Tera2 Client: Packet Capture page.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

Set Properties ☒

Set in Profile	Device Family	Property Name	Value	Description
☐	Tera2	Unified Communications Mode ⟲	Disabled ▾	This property configures Unified Communications support on Zero Clients.

Save   Cancel

⟲ indicates that the property requires a device restart after being changed
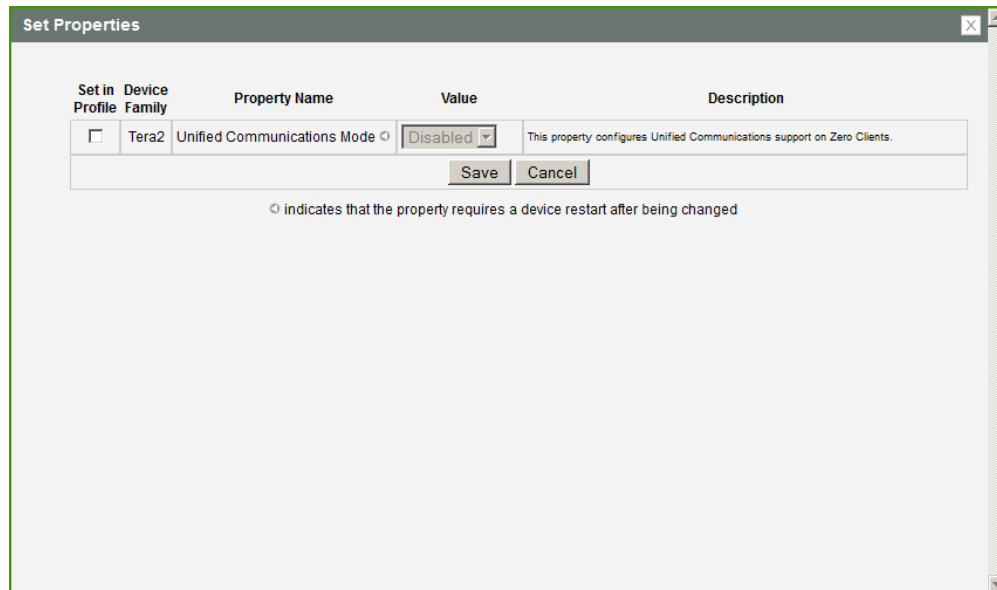
MC Unified Communications

MC Unified Communications Parameters

Parameter	Description
Unified Communications Mode	When enabled, zero clients support interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on a VMware Horizon View or Horizon DaaS desktop.

AWI Tera2 Client: Unified Communications

The **Unified Communications** page lets you configure a Tera2 zero client with Unified Communications (UC) support for interoperability with CounterPath's Bria

Virtualized Edition for PCoIP Zero Clients softphone client. You can access this page from the **Configuration > Unified Communications** menu.

Note: For details on how to capture network packets to help troubleshoot a Bria Virtualized Edition softphone call, see the AWI Tera2 Client: Packet Capture page.

Unified Communications

Change Unified Communications (UC) settings

Enable Unified Communications: ☐

Apply   Cancel
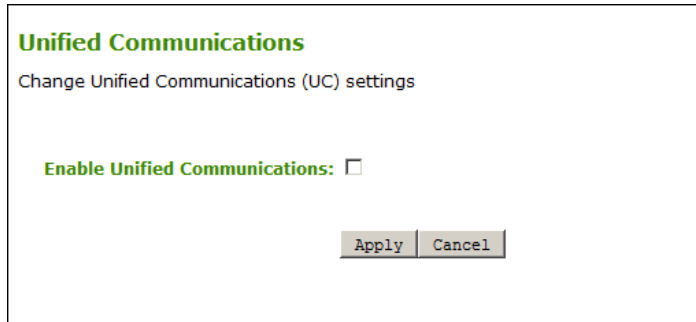
 AWI Tera2 Client Unified Communications Page

AWI Tera2 Client Unified Communications Page Parameters

Parameter	Description
Enable Unified Communications	When enabled, zero clients support interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on a VMware Horizon View or Horizon DaaS desktop.

Configuring Power Settings

MC: Power Permissions

The settings on this page let you configure a profile with power permissions for hosts and clients.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
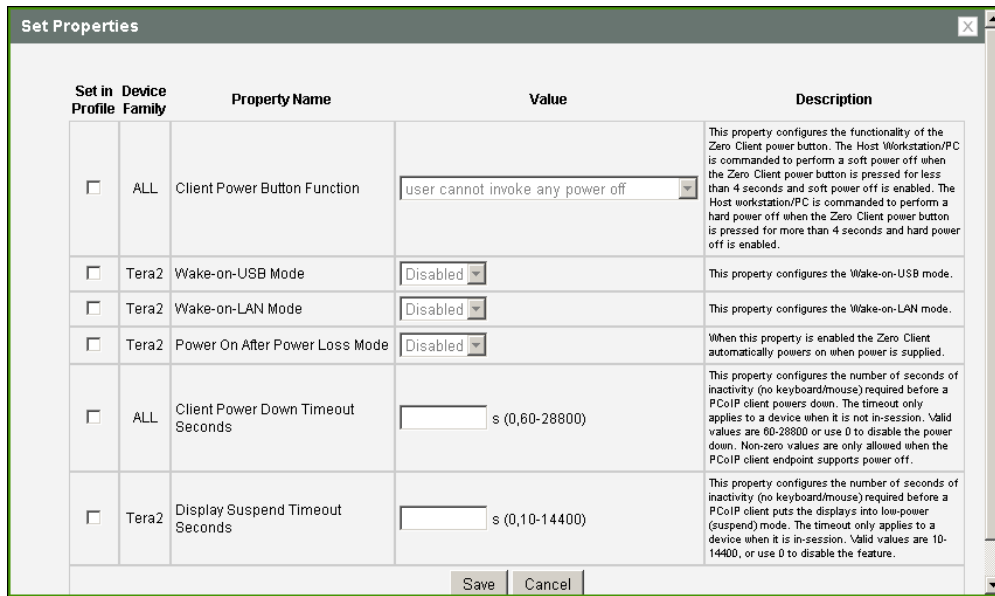
MC Power Permissions

MC Power Permissions Parameters

Parameter	Description
Client Power Button Function	Configure the functionality of the client's remote PC button.
	The host is commanded to perform a soft power off (i.e., to go into sleep mode) when the client's remote PC button is pressed for less than four seconds and soft power off is enabled.
	The host is commanded to perform a hard power off (i.e., to shut down) when the client's remote PC button is pressed for more than four seconds and hard power off is enabled.
	Select from the following options:
	• **user cannot invoke any power off**: Users cannot shut down the host or put it in sleep mode.
	• **user can only invoke a hard power off**: Users can shut down the host but not put it in sleep mode.
	• **user can only invoke a soft power off**: Users can put the host in sleep mode but not shut it down.
	• **user can invoke soft and hard power offs**: Users can put the host in sleep mode and shut it down.

Parameter	Description
Wake-on-USB Mode	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. Note: Clicking or moving the mouse will not power up the client when this feature is enabled.
Wake-on-LAN Mode	When enabled, configures Wake-on-LAN mode in hosts and clients that support this feature. Wake-on-LAN mode allows a device to wake up from sleep mode or a low power state when it receives Wake-on-LAN magic packets.
Power On After Power Loss Mode	When enabled, the client automatically powers back on when power is supplied.
Client Power Down Timeout Seconds	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: Non-zero values are only allowed when the PCoIP client supports powering off. Note: This timeout only applies when the device is *not* in session.
Display Suspend Timeout Seconds	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is in session. Note: When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.

AWI Tera2 Host: Power Settings

The **Power** page lets you configure power settings for the host. You can access this page from the **Configuration > Power** menu.
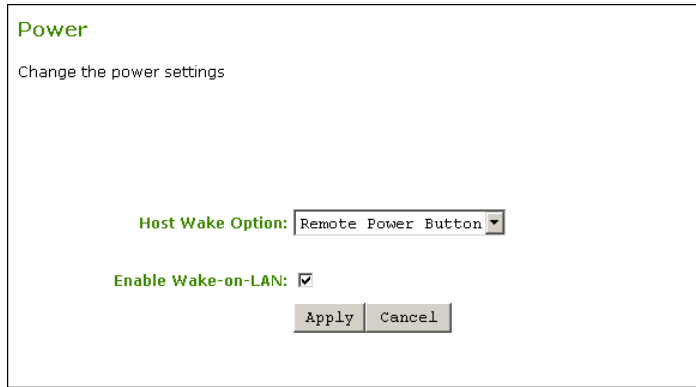
AWI Tera2 Host Power Page

AWI Tera2 Host Power Page Parameters

Parameter	Description
Host Wake Options	Note: The host PC requires sufficient standby power for these options. Configure the wake method used on the host when it is in a low power state and a Wake-on-LAN magic packet is detected on the remote workstation card's network interface card (NIC): • **Remote Power Button**: If the host PC has the remote workstation card power button cable installed, this option may be used. • **PCIe Wake Input**: If the host PC supports "wake on PCIe," this option may be used. Note: For more information, see KB 15134-201 in the Teradici Support Site.
Enable Wake-on-LAN	When enabled, configures the host to wake up from sleep mode when the user sends Wake-on-LAN magic packets to the host by pressing the client's connect/disconnect button or clicking the OSD **Connect** button on the OSD **Connect** window.

AWI Tera1 Host: Power Settings

Wake-on-LAN is the only power setting that is available for Tera1 remote workstation cards. It is always enabled and cannot be disabled through the GUI. For this reason, a Power Settings page does not appear in the AWI for Tera1 remote workstation cards.

Wake-on-LAN configures the host to wake up from sleep mode when the user sends Wake-on-LAN magic packets to the host by pressing the client's remote PC button or clicking the OSD **Connect** button on the OSD **Connect** window.

Note: For more information, see KB 15134-201 in the Teradici Support Site.

AWI Tera2 Client: Power Permissions

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

AWI Tera2 Client Power Page

AWI Tera2 Client Power Page Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is *not* in session.
Display Suspend Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is in session. Note: When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.

Parameter	Description
Auto Power-Off Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: Non-zero values are only allowed when the PCoIP client supports powering off. Note: This timeout only applies when the device is *not* in session.
Remote Host Power Control	Configure the client's remote power setting. Select from the following options: **Power-off not permitted**: Users cannot remotely shut down the host PC from the zero client. When this option is selected, the Zero Client Control Panel on the OSD does not appear when the zero client's connect/disconnect button is pressed. **Hard Power-off only**: Users are able to remotely shut down the host from the zero client. When this option is selected, the Zero Client Control Panel on the OSD appears when the zero client's connect/disconnect button is pressed.
Power On After Power Loss	When enabled, the client automatically powers back on when power is supplied.
Enable Wake-on-USB	When enabled, configures the client to power up when the user presses a key on the keyboard. Wake-on-USB applies when the client is either powered off automatically or as a result of the user holding down the power button. Note: Clicking or moving the mouse will not power up the client when this feature is enabled.
Enable Wake-on-LAN	When enabled, configures the client to wake up from a low power state when it receives Wake-on-LAN magic packets.

AWI Tera1 Client: Power Settings

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

Power
Change the power settings

OSD Screen-Saver Timeout: `300` Seconds (0 = disabled)

Remote Host Power Control: `Soft and Hard Power-off`

Apply | Cancel

AWI Tera1 Client Power Page

AWI Tera1 Client Power Page Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is *not* in session.
Remote Host Power Control	Configure the functionality of the client's remote PC button. The host is commanded to perform a soft power off (i.e., to go into sleep mode) when the client's remote PC button is pressed for less than four seconds and soft power off is enabled. The host is commanded to perform a hard power off (i.e., to shut down) when the client's remote PC button is pressed for more than four seconds and hard power off is enabled. Select from the following options: • **Power-off not permitted**: Users cannot shut down the host or put it in sleep mode. • **Soft Power-off only**: Users can put the host in sleep mode but not shut it down. • **Hard Power-off only**: Users can shut down the host but not put it in sleep mode. • **Soft and Hard Power-off**: Users can put the host in sleep mode and shut it down.

OSD Tera2: Power Settings

The settings on this page let you configure timeout and power settings for the client. You can access this page from the **Options > Configuration > Power** menu.
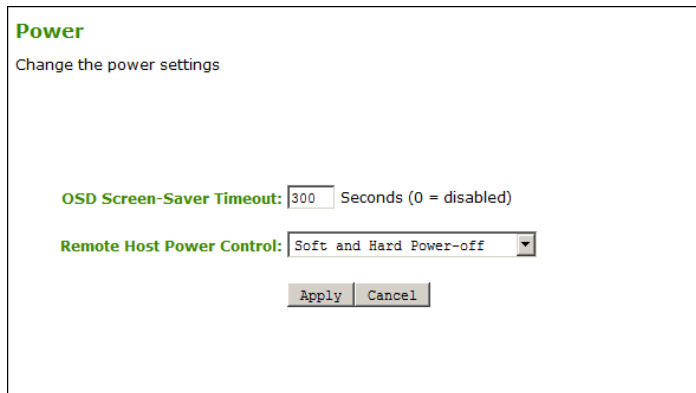
OSD Power Page

OSD Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is *not* in session.
Display Suspend Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is in session. Note: When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.

OSD Tera1: Power Settings

The setting on this page lets you configure the monitor screen-saver timeout for the client. You can access this page from the **Options > Configuration > Power** menu.

OSD Power Page

OSD Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (i.e., 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. Note: This timeout only applies when the device is *not* in session.

Configuring the Host Driver Function

MC: Host Driver Function

The setting on this page lets you configure a profile to enable or disable the PCoIP host software UI on the host computer.

Note: For information about how to install and use the PCoIP host software, see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Host Driver Configuration

MC Host Driver Configuration Parameters

Parameter	Description
Enable Host Driver	When enabled, lets you access the PCoIP host software UI on the host computer. This software lets users enable features such as the following: • Using the local cursor and keyboard feature • Locking the host PC when a session is terminated • Using the Wake-on-LAN function • Viewing host and client network parameters • Disconnecting a session • Viewing host statistics and connection information • Using the client display topology settings on the host When disabled, you do not have access to the PCoIP host software UI on the host computer. Note: This property requires a device restart after being changed.

AWI Host: Host Driver Function

The setting on this page lets you enable or disable the PCoIP host software UI on the host computer. You can access this page from the **Configuration > Host Driver Function** menu.

Note: For information about how to install and use the PCoIP host software, see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center.
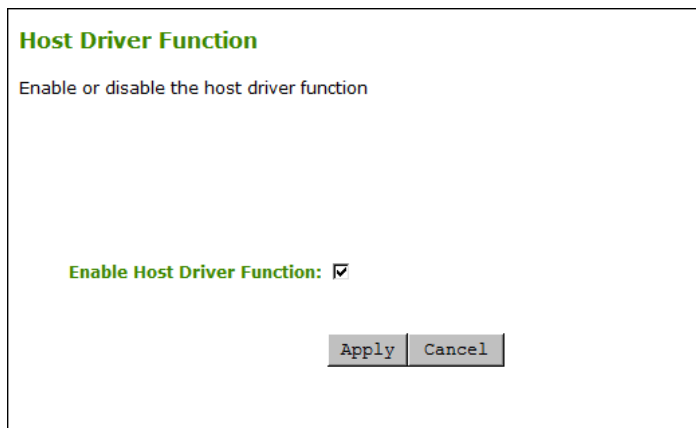
AWI Host Driver Function Page

AWI Host Driver Function Parameters

Parameter	Description
Enable Host Driver Function	When enabled, lets you access the PCoIP host software UI on the host computer. This software lets users enable features such as the following: • Using the local cursor and keyboard feature • Locking the host PC when a session is terminated • Using the Wake-on-LAN function • Viewing host and client network parameters • Disconnecting a session • Viewing host statistics and connection information • Using the client display topology settings on the host When disabled, you do not have access to the PCoIP host software UI on the host computer.

Configuring the Event Log

MC: Event Log Control Settings

The settings on this page let you configure a profile with event log messaging to use for a host or client, and to set the log filtering mode on a device.

You can also enable and configure syslog as the logging protocol to use for collecting and reporting events.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC Event Log Control

MC Event Log Control Parameters

Parameter	Description
Enable Diagnostic Log	When enabled, the device will include connection management-specific messages in the device's event log.
Event Log Filter Mode	Configure the event log filtering mode: • **Terse (deprecated)**: If this option is applied to devices running firmware 4.2.0 or greater, **Verbose** filter mode will be used. • **Verbose**: All event log messages are displayed. • **Disabled**: Disables event logging on the device. This option is not supported for devices running firmware 4.1.2 or lower.
Syslog Server Hostname	Enter the IP address or fully qualified domain name of the syslog server to which the host or client will send event log messages.
Syslog Server Port	Enter port number of the syslog server. Note: The default port number value is 514.
Syslog Facility Number	Enter the facility number for all syslog messages generated by the device.

Parameter	Description
Enhanced Logging Mode Mask	To configure a profile with enhanced logging mode for a specific category, enable this feature and then select the desired category from the drop-down list. Event logs for devices with this feature enabled will have enhanced logging details for the selected category. Note: Enhanced logging may be enabled for only one category at a time. Enhanced logging mode messages can be located in the event log by their Level 3 (**LVL:3**) designation, which indicates a debug-level message. **Enhanced logging mode categories**: • **Audio**: Provides enhanced audio-related details, such as audio compression levels and audio bandwidth. Enable this mode if you are experiencing any problems with audio quality. • **Management Console**: Provides debug-level details for the connection state between the device and the MC. Enable this mode if you are having trouble connecting to or managing the device using the MC. • **Networking**: Provides socket-level details for a device's network connections. Enable this mode for network-related issues—e.g., if the device cannot connect to a peer or broker, or if it cannot get an IP address from a DHCP server. • **OneSign**: Provides enhanced logging for connections using Imprivata's OneSign Single Sign-On proximity cards. Enable this mode to see debug-level messages between a device and a OneSign authentication server. • **Session Negotiation**: Provides pre-session messaging details, such as the full feature set advertised by each device. Enable this mode for low-level session negotiation details. • **SmartCard**: Provides debug-level messages for smart cards. Enable this mode if you experience trouble tapping or logging in using a smart card. • **System**: Provides heartbeat details about the device, such as ambient temperature. Enable this mode for system-level problems. • **USB**: Provides details of the traffic between the device and any connected USB devices. Enable this mode if you are experiencing problems with a connected USB device. • **Video**: Displays enhanced image-related logging information. Enable this mode for image problems, monitor problems, or display topology issues.

AWI: Event Log Settings

The **Event Log** page lets you view and clear event log messages from the host or client, and set the log filtering mode on the device. You can also enable and configure syslog as the logging protocol to use for collecting and reporting events.

You can access this page from the **Diagnostics > Event Log** menu.

Event Log
Configure diagnostic logging options

Enable Event Log: ☑

Event Log Messages: [View] [Clear]

Enable Syslog: ☑
Identify Syslog Host By: ⦿ IP address ○ FQDN
Syslog Host IP Address: [ ] . [ ] . [ ] . [ ]
Syslog Host Port: [514]
Syslog Facility: [19 - local use 3 ▾]

Enhanced logging mode: [Disable]

Category	Enable enhanced logging
AUDIO	○
MANAGEMENT CONSOLE	○
NETWORKING	○
ONESIGN	○
SESSION NEGOTIATION	○
SMARTCARD	○
SYSTEM	○
USB	○
VIDEO	○

[Apply] [Cancel]

AWI Event Log Page – Event Log Selected

AWI Event Log Page Parameters

Parameter	Description
Enable Event Log	When this feature is enabled, logging occurs in verbose mode, and all event log and syslog options are displayed. When this feature is disabled, the logging options are hidden. Disabling the event log disables logging and causes existing persistent event logs to be deleted. If syslog settings are configured, logs will not be sent to a syslog server.
Event log Messages	• **View:** Click to open a browser page that displays the event log messages (with timestamp information) stored on the device. Press **F5** to refresh the browser page log information. • **Clear:** Click to delete all event log messages stored on the device.

Parameter	Description
Enable Syslog	Enable or disable the syslog standard as the logging mechanism for the device. Note: If syslog is enabled, you must configure the remaining fields. If syslog is disabled, these fields are non-editable.
Identify Syslog Host By	Choose if the syslog server host is identified by IP address or by fully qualified domain name (FQDN).
Syslog Host IP Address / Syslog Host DNS name	The parameter that displays depends on which option you choose to identify the syslog server host: • **IP Address**: Enter the IP address for the syslog server host. • **FQDN:** Enter the DNS name for the syslog server host. Note: If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it.
Syslog Host Port	Enter port number of the syslog server. Note: The default port number value is 514.
Syslog Facility	The facility is a number attached to every syslog message used to categorize the source of the syslog messages. The facility is part of the standard syslog header and can be interpreted by all syslog servers. Enter a facility to suit your logging needs. For example, you could configure devices as follows: • Zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 Note: The default facility is set to "19 – local use 3". Cisco routers default to "23 – local use 7".

Parameter	Description
Enhanced logging mode	If you require enhanced logging details in the event log to help troubleshoot a problem with a zero client or remote workstation card, select an enhanced logging category, and then click **Apply** > **Continue**. (To return to normal logging mode, click **Disable**, and then **Apply** > **Continue**.) Note: Enhanced logging may be enabled for only one category at a time. Enhanced logging mode messages can be located in the event log by their Level 3 (**LVL:3**) designation, which indicates a debug-level message. **Enhanced logging mode categories**: ● **Audio**: Provides enhanced audio-related details, such as audio compression levels and audio bandwidth. Enable this mode if you are experiencing any problems with audio quality. ● **Management Console**: Provides debug-level details for the connection state between the device and the MC. Enable this mode if you are having trouble connecting to or managing the device using the MC. ● **Networking**: Provides socket-level details for a device's network connections. Enable this mode for network-related issues—e.g., if the device cannot connect to a peer or broker, or if it cannot get an IP address from a DHCP server. ● **OneSign**: Provides enhanced logging for connections using Imprivata's OneSign Single Sign-On proximity cards. Enable this mode to see debug-level messages between a device and a OneSign authentication server. ● **Session Negotiation**: Provides pre-session messaging details, such as the full feature set advertised by each device. Enable this mode for low-level session negotiation details. ● **SmartCard**: Provides debug-level messages for smart cards. Enable this mode if you experience trouble tapping or logging in using a smart card. ● **System**: Provides heartbeat details about the device, such as ambient temperature. Enable this mode for system-level problems. ● **USB**: Provides details of the traffic between the device and any connected USB devices. Enable this mode if you are experiencing problems with a connected USB device. ● **Video**: Displays enhanced image-related logging information. Enable this mode for image problems, monitor problems, or display topology issues.

OSD: Event Log Settings

The **Event Log** page lets you view, refresh, and clear event log messages from the client. You can access this page from the **Options > Diagnostics > Event Log** menu.
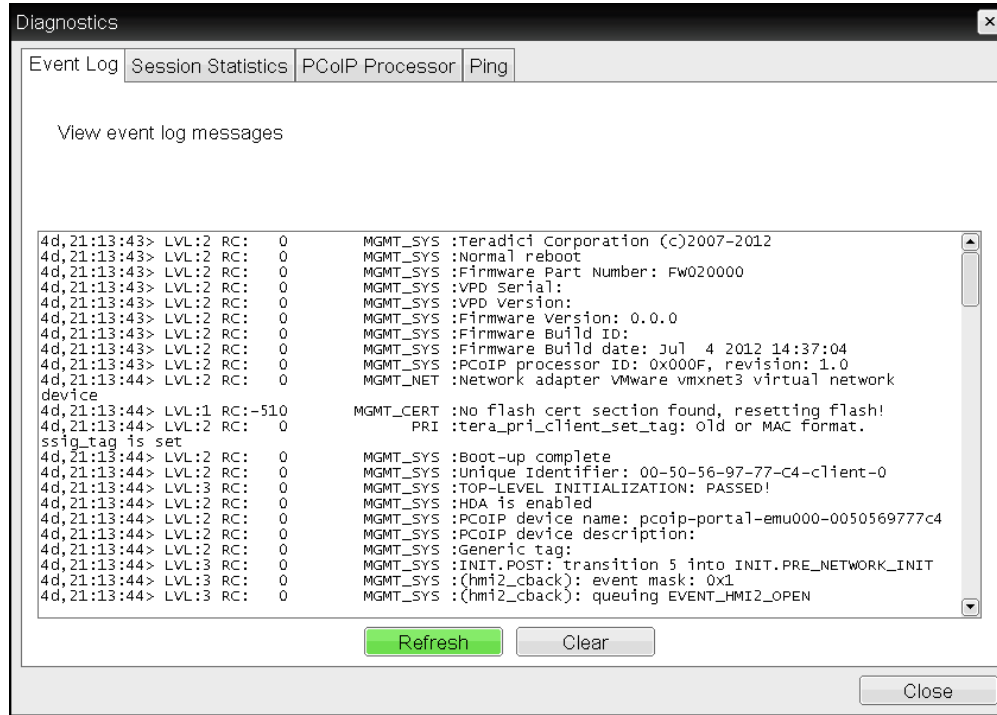
OSD Event Log Page

OSD Event Log Page Parameters

Parameter	Description
Refresh	Click to refresh the log information displayed on this page.
Clear	Click to delete all event log messages stored on the device.

Configuring Peripherals

MC: Peripheral Settings

The setting on this page lets you configure a profile to enable or disable USB Enhanced Host Controller Interface (EHCI) mode on selected devices.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
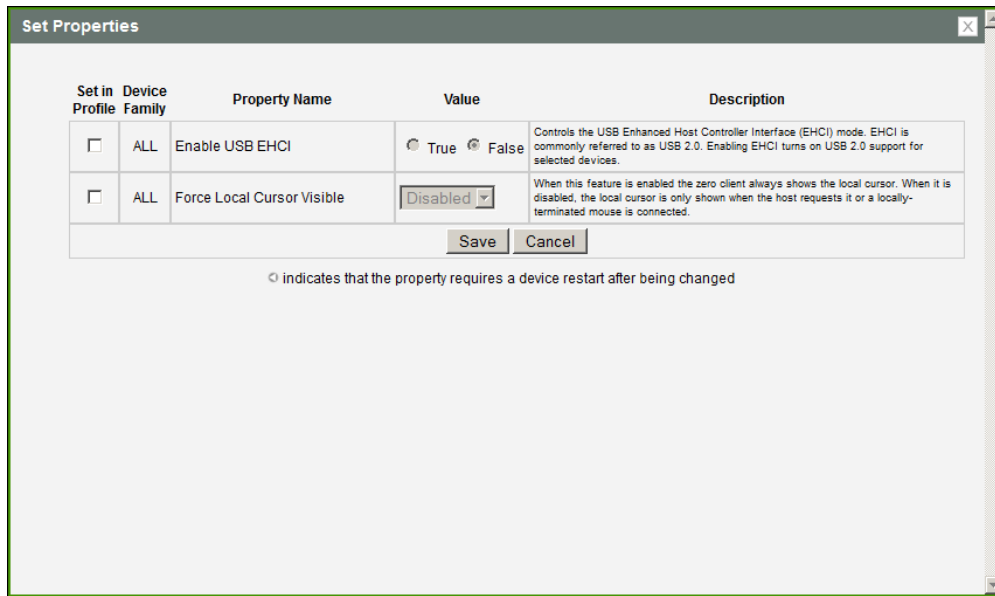
MC Peripheral Configuration

MC Peripheral Configuration Parameters

Parameter	Description
Enable USB EHCI	When enabled, configures EHCI (USB 2.0) for devices connected directly to zero client USB ports for sessions with a host running VMware View 4.6 or newer. Note: 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.
Force Local Cursor Visible (Tera2 only)	When enabled, the 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.

AWI Client: Help for Peripheral Settings

The Enable EHCI setting for the AWI is located as follows:

- Tera2 zero clients: AWI Tera2 Client: USB Settings page (accessed from the **Configuration > USB menu**)
- Tera1 zero clients: AWI Client: USB Permissions page (accessed from the **Permissions > USB** menu)

Configuring IPv6

MC: IPv6 Settings

The settings on this page let you configure a profile to enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware Horizon.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
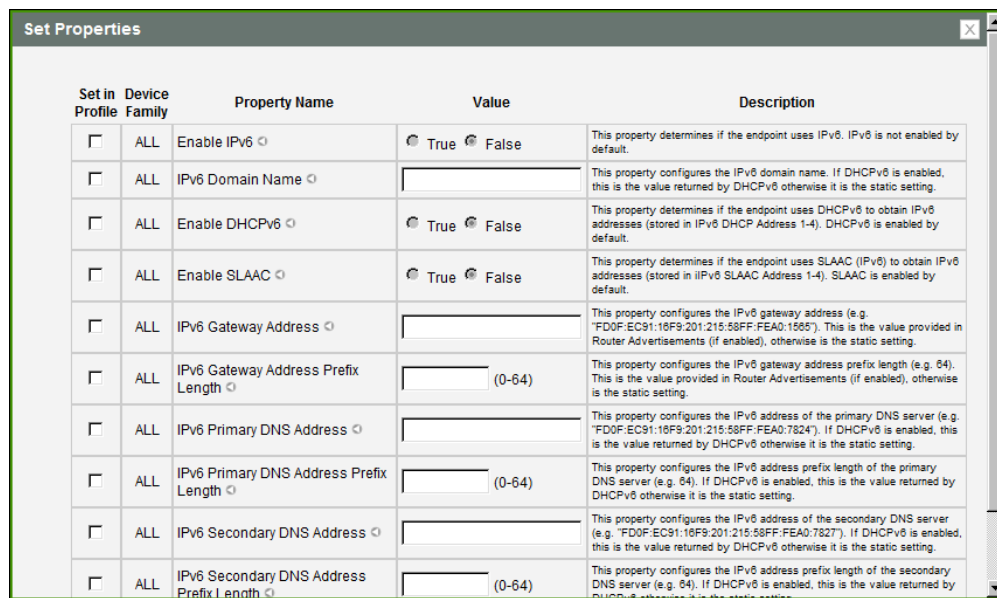
MC IPv6 Configuration

MC IPv6 Configuration Parameters

Parameter	Description
Enable IPv6	This property determines if the device uses IPv6. IPv6 is not enabled by default. Note: This property requires a device restart after being changed.
IPv6 Domain Name	If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting. Note: This property requires a device restart after being changed.

Parameter	Description
Enable DHCPv6	Determines if the device uses DHCPv6 to obtain IPv6 addresses (stored in IPv6 DHCP Address 1-4). DHCPv6 is enabled by default. Note: This property requires a device restart after being changed.
Enable SLAAC	Determines if the endpoint uses Stateless Address Auto-configuration (SLAAC IPv6) to obtain IPv6 addresses (stored in IPv6 SLAAC Address 1-4). SLAAC is enabled by default. Note: This property requires a device restart after being changed.
IPv6 Gateway Address	Configures the IPv6 gateway address (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:1565"). This is the value provided in Router Advertisements (if enabled); otherwise, it is the static setting. Note: This property requires a device restart after being changed.
IPv6 Gateway Address Prefix Length	Configures the IPv6 gateway address prefix length (e.g., 64). This is the value provided in Router Advertisements (if enabled); otherwise, it is the static setting. Note: This property requires a device restart after being changed.
IPv6 Primary DNS Address	Configures the IPv6 address of the primary DNS server (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:7824"). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting. Note: This property requires a device restart after being changed.
IPv6 Primary DNS Address Prefix Length	Configures the IPv6 address prefix length of the primary DNS server (e.g., 64). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting. Note: This property requires a device restart after being changed.
IPv6 Secondary DNS Address	Configures the IPv6 address of the secondary DNS server (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:7827"). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting. Note: This property requires a device restart after being changed.
IPv6 Secondary DNS Address Prefix Length	Configures the IPv6 address prefix length of the secondary DNS server (e.g., 64). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting. Note: This property requires a device restart after being changed.

AWI: IPv6 Settings

The settings on this page let you enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware View.

You can access this page from the **Configuration > IPv6** menu.

IPv6

Change the IPv6 network settings for the device

Enable IPv6:	☐
Link Local Address:	
Gateway:	
Enable DHCPv6:	☐
Primary DNS:	
Secondary DNS:	
Domain Name:	
FQDN:	
Enable SLAAC:	☐
Enable Manual Address:	☐

Apply   Cancel

AWI IPv6 Page

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

AWI IPv6 Page Parameters

Parameter	Description
Enable IPv6	Enable this field to enable IPv6 for your PCoIP devices.
Link Local Address	This field is automatically populated.
Gateway	Enter the IPv6 gateway address.

Parameter	Description
Enable DHCPv6	Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device.
DHCPv6 Addresses	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 (e.g., "domain.local") for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	Enable this field to set up Stateless Address Auto-configuration (SLAAC) for your devices.
SLAAC Addresses	When SLAAC is enabled and the device is rebooted, these fields are automatically populated.
Enable Manual Address	Enable this field to set up a manual (static) address for the device.
Manual Address	Enter the IP address for the device.

OSD: IPv6 Settings

The settings on this page let you enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware View.

You can access this page from the **Options > Configuration > IPv6** menu.

OSD IPv6 Page

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

OSD IPv6 Page Parameters

Parameter	Description
Enable IPv6	Enable this field to enable IPv6 for your PCoIP devices.
Link Local Address	This field is automatically populated.
Gateway	Enter the IPv6 gateway address.
Enable DHCPv6	Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device.
DHCPv6 Addresses	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.

Parameter	Description
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 (e.g., "domain.local") for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	Enable this field to set up Stateless Address Auto-configuration (SLAAC) for your devices.
SLAAC Addresses	When SLAAC is enabled and the device is rebooted, these fields are automatically populated.
Enable Manual Address	Enable this field to set up a manual (static) address for the device.
Manual Address	Enter the IP address for the device.

Configuring SCEP

MC: SCEP Settings

Simple Certificate Enrollment Protocol (SCEP) lets you simplify the retrieval and installation of digital certificates by allowing devices to obtain certificates automatically from a SCEP server. This feature is available for Tera2 zero clients only.

The settings on this page let you configure a profile with SCEP settings. When the profile is applied, the zero clients will submit a request for certificates to the specified SCEP server.

Notes:

- When a 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 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.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.

MC SCEPConfiguration

MC SCEP Configuration Parameters

Parameter	Description
SCEP Server URI	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. Note: This password will be used for all the zero clients associated with this profile.
Use Certificate for 802.1X	Specify whether or not the obtained client certificate will be used for 802.1x authentication.

AWI Tera2 Client: SCEP Settings

Simple Certificate Enrollment Protocol (SCEP) lets you simplify the retrieval and installation of digital certificates by allowing devices to obtain certificates automatically from a SCEP server. This feature is available for Tera2 zero clients only.

You can access this page from the **Configuration > SCEP** menu.

Notes:

- When a 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 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.

To retrieve certificates for a device, enter the URL and password for the SCEP server, and then click **Request Certificates**. Root CA and 802.1x certificates display after these certificates are installed.

AWI SCEP Page

AWI 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 (e.g., in progress, successful, failed).

OSD Tera2: SCEP Settings

Simple Certificate Enrollment Protocol (SCEP) lets you simplify the retrieval and installation of digital certificates by allowing devices to obtain certificates automatically from a SCEP server. This feature is available for Tera2 zero clients only.

You can access this page from the **Options > Configuration > SCEP** menu.

Notes:

- When a 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 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.

To retrieve certificates for a device, enter the URL and password for the SCEP server, and then click **Request Certificates**. Root CA and 802.1x certificates display after these certificates are installed.

OSD Tera2 SCEP Page

OSD Tera2 SCEP Page 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 (e.g., in progress, successful, failed).

Configuring the Display Topology

MC: Display Topology Settings

The settings on this page let you configure a profile with the display topology to use for Tera1 and Tera2 clients.

Note: Use the Dual-Display Zero Client layout for TERA2321 zero client devices.

Note: To enable a property in the MC, click the **Set in Profile** check box and configure the fields as indicated. After you update the properties on this page, click **Save** to save your changes.
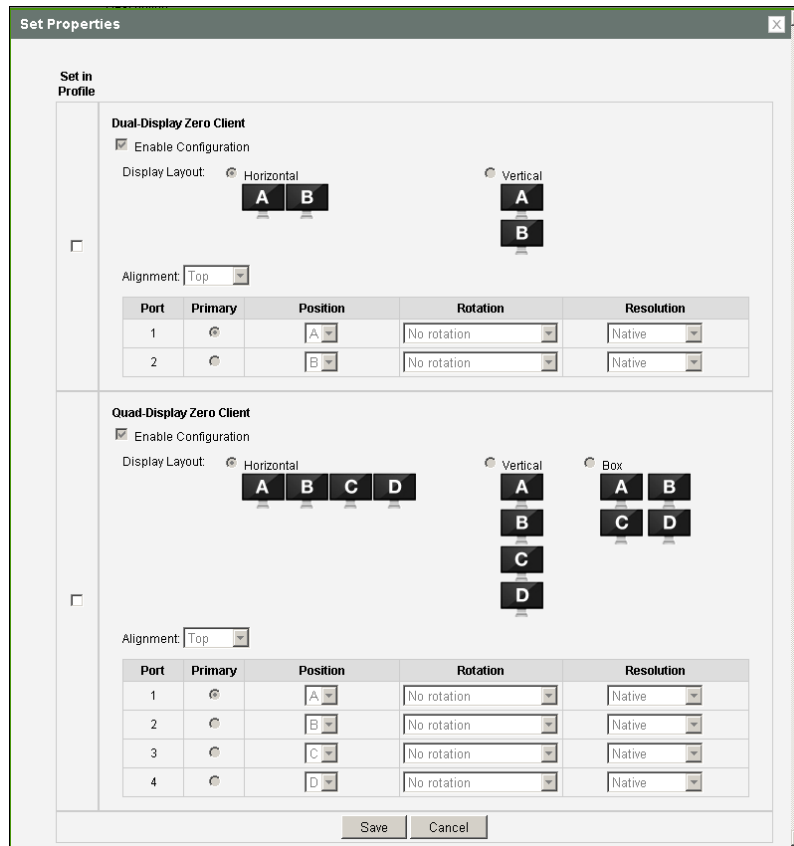
MC Display Topology Configuration

MC Display Topology Configuration Parameters

Parameter	Description
Dual-Display Zero Client	
Enable Configuration	Enable to configure a device that supports two displays per PCoIP chipset.
Display Layout	Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk. • **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram. • **Vertical**: Select to arrange displays vertically, as indicated in the diagram.

Parameter	Description
Alignment	Select how you want displays aligned when they are different sizes. Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout**: • **Top**: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom**: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout**: • **Left**: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.
Primary	Configure which video port on the zero client you want as the primary port. Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1**: Select to configure port 1 on the zero client as the primary port. • **Port 2**: Select to configure port 2 on the zero client as the primary port.
Position	Specify which display is physically connected to each port.

Parameter	Description
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.
Quad-Display Zero Client	
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.
Display Layout	Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk. • **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram. • **Vertical**: Select to arrange displays vertically, as indicated in the diagram. • **Box**: Select to arrange displays in a box formation, as indicated in the diagram.

Parameter	Description
Alignment	Select how you want displays aligned when they are different sizes. Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout**: • **Top**: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom**: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout**: • **Left**: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.
Primary	Configure which video port on the zero client that you want as the primary port. Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1**: Select to configure port 1 on the zero client as the primary port. • **Port 2**: Select to configure port 2 on the zero client as the primary port. • **Port 3**: Select to configure port 3 on the zero client as the primary port. • **Port 4**: Select to configure port 4 on the zero client as the primary port.
Position	Specify which display is physically connected to each port.

Parameter	Description
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

OSD Dual-display: Display Topology Settings

The **Display Topology** page lets users change the display topology for a PCoIP session. You can access this page from the **Options > User Settings > Display Topology** menu on your client OSD.

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 newer. To apply the display topology feature to a PCoIP session between a client and a PCoIP host, you must have the PCoIP host software installed on the host.

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

OSD Dual-display Topology Page

OSD Dual-display Topology Page Parameters

Parameter	Description
Enable Configuration	Enable to configure a device that supports two displays per PCoIP chipset.
Display Layout	Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk. • **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram. • **Vertical**: Select to arrange displays vertically, as indicated in the diagram.

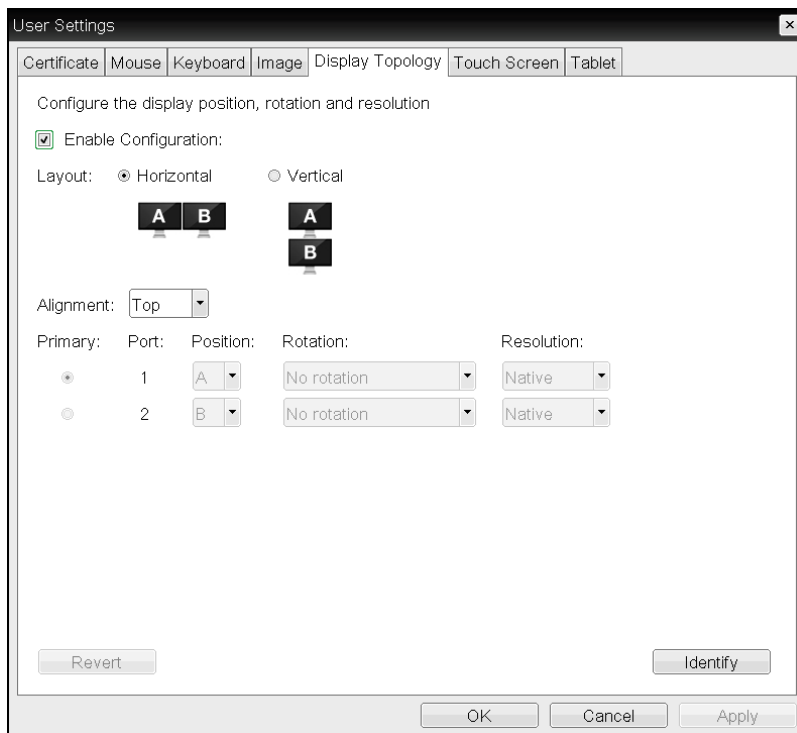| Parameter	Description
Alignment	Select how you want displays aligned when they are different sizes. Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout**: • **Top**: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom**: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout**: • **Left**: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.
Primary	Configure which video port on the zero client you want as the primary port. Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1**: Select to configure port 1 on the zero client as the primary port. • **Port 2**: Select to configure port 2 on the zero client as the primary port.
Position	Specify which display is physically connected to each port.

Parameter	Description
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

OSD Quad-display: Display Topology Settings

The **Display Topology** page lets users change the display topology for a PCoIP session. You can access this page from the **Options > User Settings > Display Topology** menu on your client OSD.

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 newer. To apply the display topology feature to a PCoIP session between a client and a PCoIP host, you must have the PCoIP host software installed on the host.

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

OSD Quad-display Topology Page

OSD Quad-display Topology Page Parameters

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.
Display Layout	Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk. • **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram. • **Vertical**: Select to arrange displays vertically, as indicated in the diagram. • **Box**: Select to arrange displays in a box formation, as indicated in the diagram.

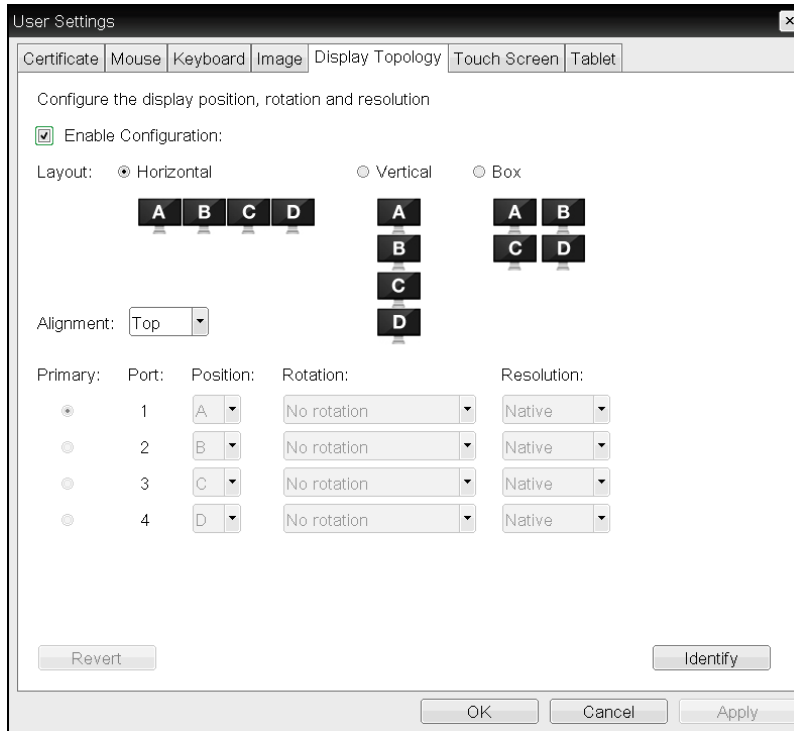| Parameter	Description
Alignment	Select how you want displays aligned when they are different sizes. Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout. **Horizontal layout**: • **Top**: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Bottom**: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. **Vertical layout**: • **Left**: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.
Primary	Configure which video port on the zero client that you want as the primary port. Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session). • **Port 1**: Select to configure port 1 on the zero client as the primary port. • **Port 2**: Select to configure port 2 on the zero client as the primary port. • **Port 3**: Select to configure port 3 on the zero client as the primary port. • **Port 4**: Select to configure port 4 on the zero client as the primary port.
Position	Specify which display is physically connected to each port.

Parameter	Description
Rotation	Configure the rotation of the display in each port: • **No rotation** • **90° clockwise** • **180° rotation** • **90° counter-clockwise**
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

Uploading an OSD Logo

MC: OSD Logo Settings

The **Profile OSD Logo** section is located towards the bottom of the **Manage Profiles** page on the Management Console. It lets you upload an image to a profile that will display on the **Connect** page of a user's local On Screen Display (OSD) GUI.

Note: From the AWI, you can configure the login screen on the OSD to display this logo instead of the default banner by enabling **Use OSD Logo for Login Banner** in the **Session > PCoIP Connection Manager** and **Session > View Connection Server** advanced options.
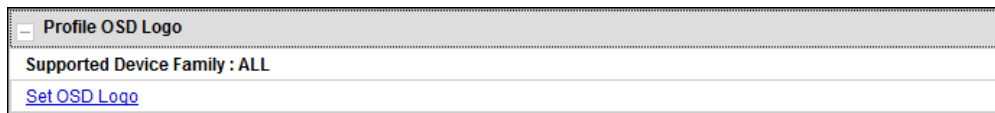
MC Profile OSD Logo Configuration

When you click **Set OSD Logo**, the following screen displays from which you can upload an image file.

MC Add OSD Logo Configuration

MC Add OSD Logo Configuration Parameters

Parameter	Description
Filename	Specify the filename of the logo image you want to upload. You can browse to the target file using the **Browse** button. The file must be accessible to the web browser (i.e., it 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 appears.
Upload	Click **Upload** to transfer the specified image file to the client. A message to confirm the upload appears.

AWI Client: OSD Logo Settings

The **OSD Logo** page lets you upload an image to display on the **Connect** page of the local On Screen Display (OSD) GUI. You can access this page from the **Upload > OSD Logo** menu.

Note: From the AWI, you can configure the login screen on the OSD to display this logo instead of the default banner by enabling **Use OSD Logo for Login Banner** in the **Session > PCoIP Connection Manager** and **Session > View Connection Server** advanced options.
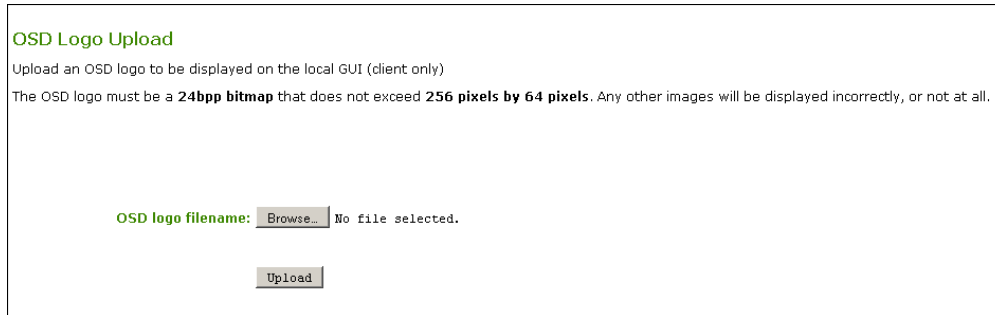
AWI Client OSD Logo Upload Page

AWI Client OSD Logo Upload Page Parameters

Parameter	Description
OSD logo filename	Specify the filename of the logo image you want to upload. You can browse to the target file using the **Browse** button. The file must be accessible to the web browser (i.e., it 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 appears.

Parameter	Description
Upload	Click **Upload** to transfer the specified image file to the client. A message to confirm the upload appears.

Uploading Firmware

MC: Firmware Management

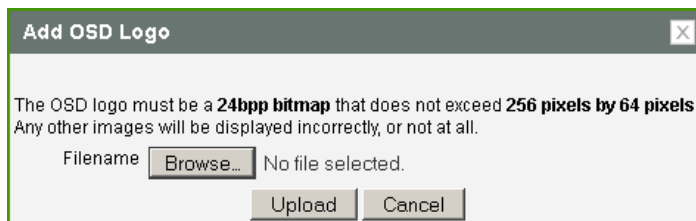The **Profile Firmware** section is located towards the bottom of the **Manage Profiles** page on the Management Console. It lets you assign a firmware file to a profile and configure the upgrade criteria that must be met before the firmware is pushed to each device.

Note: Before you can assign a firmware file to a profile, you must first ensure that the file has been imported into the MC from the **Update > Import Firmware** menu. For more information, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support [Documentation Center](#).
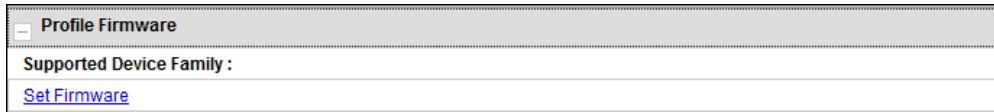
MC Profile Firmware Configuration

When you click **Set Firmware**, the following screen displays.
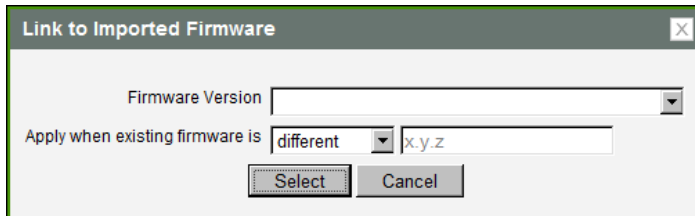
MC Link to Imported Firmware

Select the firmware version from the drop-down menu, and then choose whether the firmware will be overwritten on the device if its version is different from this firmware version or if it is less than the firmware version you enter in the text entry field. Click **Select** when you are finished.
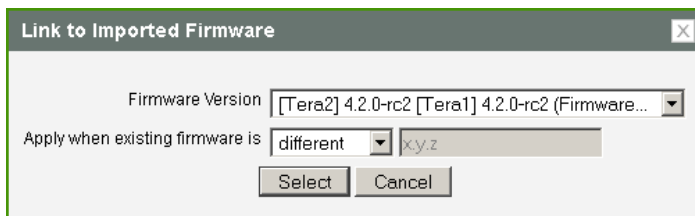
MC Link to Imported Firmware – Configured

MC Link to Imported Firmware Parameters

Parameter	Description
Firmware Version	Select the firmware file that you want to assign to the profile. Note: The firmware file must first be imported into the MC from the **Update > Import Firmware** menu. For more information, see "Teradici PCoIP® Management Console User Manual" (TER0812002) in the Teradici Support Documentation Center.
Apply when existing firmware is	Configure one of the following options from the drop-down menu: • **different**: Select this option if you want to overwrite the firmware on the device only if its version is different from the firmware version you selected. • **less than**: Select this option if you want to overwrite the firmware on the device only if its version is less than the firmware version in the *x.y.z* field, and then enter the version in this field (e.g., 4.1.0).

AWI: Firmware Upload Settings

The **Firmware** page lets you upload a new firmware build to the host or client. You can access this page from the **Upload > Firmware** menu.

Note: The host and client must have the same firmware release version installed.

Firmware Upload

Upload a new firmware build

Firmware build filename: [   ] [Browse...]

[Upload]

AWI Firmware Upload Page

AWI Firmware Upload Page 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 accessible to the web browser (i.e., it must be on a local or accessible network drive). The firmware image must be an ".all" file.

Parameter	Description
Upload	Click the **Upload** button to transfer the specified file to the device. The AWI prompts you to confirm this action to avoid accidental uploads. Note: It's important to ensure that both the host and client have the same firmware release.

See Uploading Firmware in the "How To" section for information on how to use the AWI to upload a firmware release to a zero client or host.

Configuring USB Permissions

MC: USB Permissions

The **Profile Zero Client USB** sections are located towards the bottom of the **Manage Profiles** page on the Management Console. These sections let you configure a profile to retain the USB settings that are configured on clients, to disable the settings, or to add to them.

Note: USB Enhanced Host Controller Interface (EHCI) mode is configured in the Management Console on the MC Peripheral Configuration page.

MC Profile Zero Client USB Configuration

MC Profile Zero Client USB Configuration Parameters

Parameter	Description
Profile Zero Client USB Authorization	Choose one of the following: • **Do not erase the device's existing USB authorizations**: Select this option if you want to use the existing USB authorization settings that are configured on the client. • **Erase the device's existing USB authorizations and replace them with an empty set**: Select this option if you want to remove all USB authorization settings that are configured on the client. • **Add New**: Click this link if you want to add a new USB authorization entry to the existing settings that are configured on the client.
Profile Zero Client USB Unauthorization	Choose one of the following: • **Do not erase the device's existing USB unauthorizations**: Select this option if you want to use the existing USB unauthorization settings that are configured on the client. • **Erase the device's existing USB unauthorizations and replace them with an empty set**: Select this option if you want to disable all USB devices that are configured on the client. • **Add New**: Click this link if you want to add a new USB unauthorization entry to the existing unauthorization settings that are configured on the client.
Profile Zero Client USB Bridged	Choose one of the following: • **Do not erase the device's existing USB bridged settings**: Select this option if you want to use the existing USB bridged settings that are configured on the client. • **Erase the device's existing USB bridged settings and replace them with an empty set**: Select this option if you want to disable all USB bridged settings that are configured on the client. • **Add New**: Click this link if you want to add a new USB bridged entry to the existing settings that are configured on the client.

When you click **Add New** for a USB authorization, unauthorization, or bridged entry, the following screens display, respectively.

USB Authorization – Add New

USB Unauthorization – Add New

USB Bridged – Add New

Add Profile USB – Add New Parameters

Parameter	Description
Rule Type	When adding a new USB authorization or unauthorization entry, select one of the following: • **Class**: The USB device is authorized by its device class, sub-class, and protocol information. • **ID**:The USB device is authorized by its vendor ID and product ID information.
Device Class	This field is enabled when **Class** is selected. Select a supported device class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any device class.
Sub Class	This field is enabled when **Class** is selected. Select a supported device sub class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any sub-class. Note: If **Any** is selected as the device class, this will be the only selection available.
Protocol	This field is enabled when **Class** is selected. Select a supported protocol from the drop-down menu, or select **Any**. Note: If **Any** is selected as the device class or sub-class, this will be the only selection available.
VID	This field is enabled when **ID** is selected, or when you are adding a new USB bridged entry. Enter the vendor ID of the authorized, unauthorized, or bridged device. The valid range is hexadecimal 0-FFFF.
PID	This field is enabled when **ID** is selected, or when you are adding a new USB bridged entry. Enter the product ID of the authorized, unauthorized, or bridged device. The valid range is hexadecimal 0-FFFF.

AWI Host: USB Permissions

The **USB** page is accessed from the **Permissions > USB** menu. It allows you to authorize a "white list" of USB devices and to unauthorize a "black 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.

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

The **USB** 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 unauthorized devices and the consolidated list is used.
- If the host does not have permissions programmed, the client's permissions are used.

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

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

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

USB

Configure the USB permissions table

Authorized Devices: *Table is empty*

Add new

Unauthorized Devices: *Table is empty*

Add new

Apply   Cancel

AWI Host USB Page

AWI Host USB Page Parameters

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

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

When you add a new USB authorized or unauthorized entry, the following parameters display depending on whether you describe the device by **Class** or **ID**.

Device Class Parameters

Device ID Parameters

USB Authorized/Unauthorized Devices Parameters

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

AWI Client: USB Permissions

The **USB** page is accessed from the **Permissions > USB** menu. It allows you to authorize a "white list" of USB devices and to unauthorize a "black 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.

You can also 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.

USB plug events are blocked in the PCoIP zero client hardware for unauthorized USB devices. The host (PCoIP Remote Workstation Card or the host virtual desktop) cannot see or access the device for an additional layer of security.
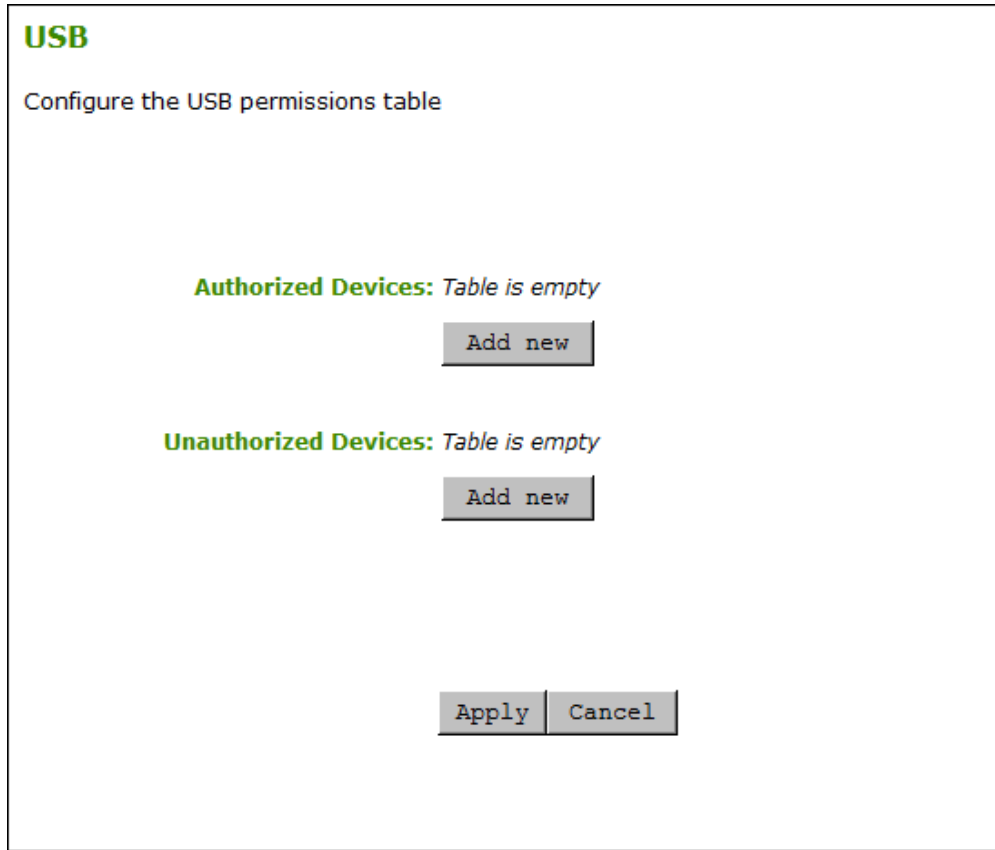
The **USB** page is available on the host and client but the host USB permissions have a higher priority and update the client USB permissions. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP Remote Workstation Card. The following rules apply:

- 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 unauthorized devices and the consolidated list is used.
- If the host does not have permissions programmed, the client's permissions are used.

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

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

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

AWI Client (Tera2) USB Page

AWI Client (Tera1) USB Page

AWI Client USB Page Parameters

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

Parameter	Description
Bridged Devices	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 zero client to bridge specific USB devices so that they use the drivers on the virtual desktop. **Add New:** Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID. **Remove:** Delete a rule for a device or device group from the list. Note: Bridging is a feature supported in firmware 3.3.0 or higher. This rule only affects sessions between a zero client and a soft host running VMware View 4.6 or higher.
Enable EHCI (Tera1 only)	Note: For Tera2 zero clients, this setting is found on the Configuration > USB page. Enable this field to configure EHCI (USB 2.0) for devices connected directly to zero client USB ports for sessions with a host running VMware View 4.6 or newer. Note: This setting applies only to software-based PCoIP sessions. EHCI is automatically enabled in hardware-based PCoIP sessions if both endpoints support it. Note: 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.

When you add a new USB authorized or unauthorized entry, the following parameters display depending on whether you describe the device by **Class** or **ID**.

Device Class Parameters

Device ID Parameters

USB Authorized/Unauthorized Devices Parameters

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

When you add a new USB bridged entry, the following parameters display.

USB Bridged Parameters

USB Bridged Devices Parameters

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

Configuring the Certificate Store

MC: Certificate Store Management

The **Certificate Store** section is located at the bottom of the **Manage Profiles** page on the Management Console. This section lets you configure a profile to retain the certificate settings that are configured on a device, to disable the settings, or to upload a new certificate file to the profile.

The maximum size for a certificate that you can upload to a profile from the MC is 8,176 bytes. You can upload up to 16 certificates to a profile providing you do not exceed the maximum storage size of 98,112 bytes. The available storage field indicates the remaining number of certificates and how much space is left in the certificate store.

Note: If you have authentication problems after uploading a View Connection Server client certificate, please see KB 15134-1084 in the Teradici Support Site for troubleshooting information.

Note: If SCEP is enabled, you can only upload a maximum of 14 additional certificates since two slots are reserved for SCEP server certificates.
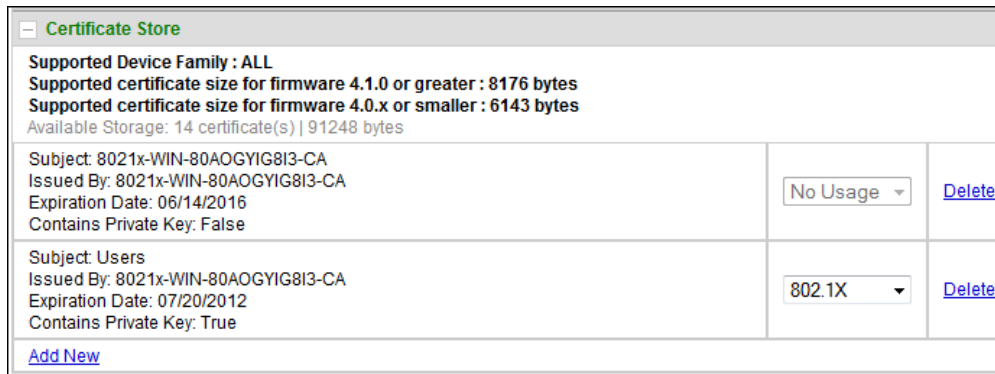
MC Certificate Store Configuration

When you click **Add New**, the following screen displays.
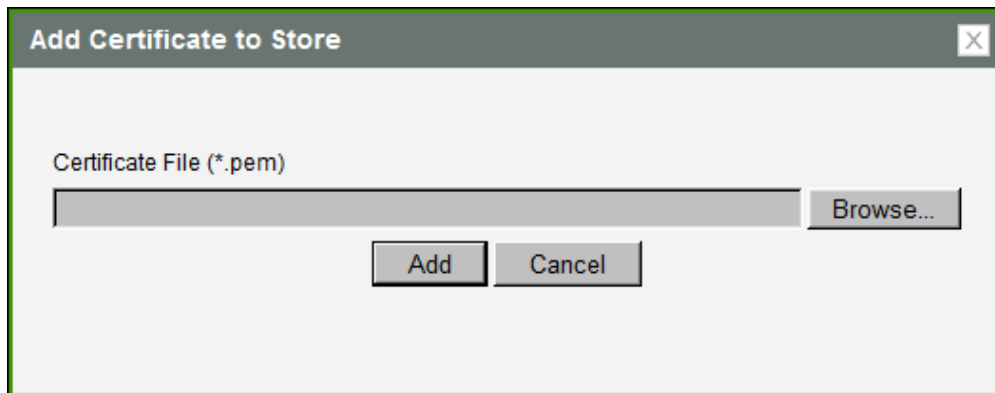
MC Add Certificate to Store

MC Add Certificate to Store Parameters

Parameter	Description
Certificate File (*.pem)	Use the **Browse** button to locate the certificate file, and then click **Add**.

After adding a certificate to the certificate store, you can then select a usage from the drop-down menu in the **Certificate Store** section. This field indicates how the device will use the certificate.

MC Certificate Store

Parameter	Description
No Usage	Select this option when you are adding a certificate that does not contain a private key (e.g., a certificate used to verify a View Connection Server or a PCoIP Connection Manager).
802.1X	Select this option when you are adding a certificate that contains a private key.

Note: This option only appears in the drop-down list if the certificate contains a private key. |

AWI: Certificate Upload Settings

The **Certificate Upload** page lets you upload and manage your CA root and client certificates for remote workstation cards and zero clients. You can access this page from the **Upload > Certificate** menu.

The maximum size for a certificate that you can upload from the AWI is 10,239 bytes. You can upload up to 16 certificates providing you do not 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.

Note: If you have authentication problems after uploading a View Connection Server client certificate, please see KB 15134-1084 in the Teradici Support Site for troubleshooting information.

Note: If SCEP is enabled, you can only upload a maximum of 14 additional certificates since two slots are reserved for SCEP server certificates.

Note: 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 KB 15134-1063 in the Teradici Support Site. For information on 802.1x certificate authentication, see Configuring 802.1x Network Device Authentication.

The following are some general guidelines when using 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 then 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 10,240 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, then copy and save each certificate to its own file.

AWI Certificate Upload Page

AWI Certificate Upload Page Parameters

Parameter	Description
Certificate filename	Upload up to a maximum of 16 root and client certificates.

Parameter	Description
Uploaded Certificates	This displays any uploaded certificates. To delete an uploaded certificate, click the **Remove** button. The deletion process occurs after the device is rebooted. To view the details of a certificate, click the **Detail** button. These certificates appear as options in the **Client Certificate** drop-down menu on the **Network** page.
802.1X Client Certificate	This is a read-only field. It is linked to the **Client Certificate** field on the **Network** page.

Configuring OSD Display Settings

OSD Dual-display: Display Settings

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.

Note: This function is only available through the OSD.

Under normal operation, the GPU in the host computer queries a monitor attached to the 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 KVM devices. The **Enable Attached Display Override** feature in this page allows you to configure the client to advertise default EDID information to the GPU.

Warning: You should 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 drop-down 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 (i.e., perform a hot plug reset).

Important: 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, etc.), ensure that both these fields are enabled.

OSD Tera1 Display Page

OSD Tera1 Display Page Parameters

Parameter	Description
Enable Attached Display Override	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. The following default resolutions are advertised when this option is enabled: • 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 Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.

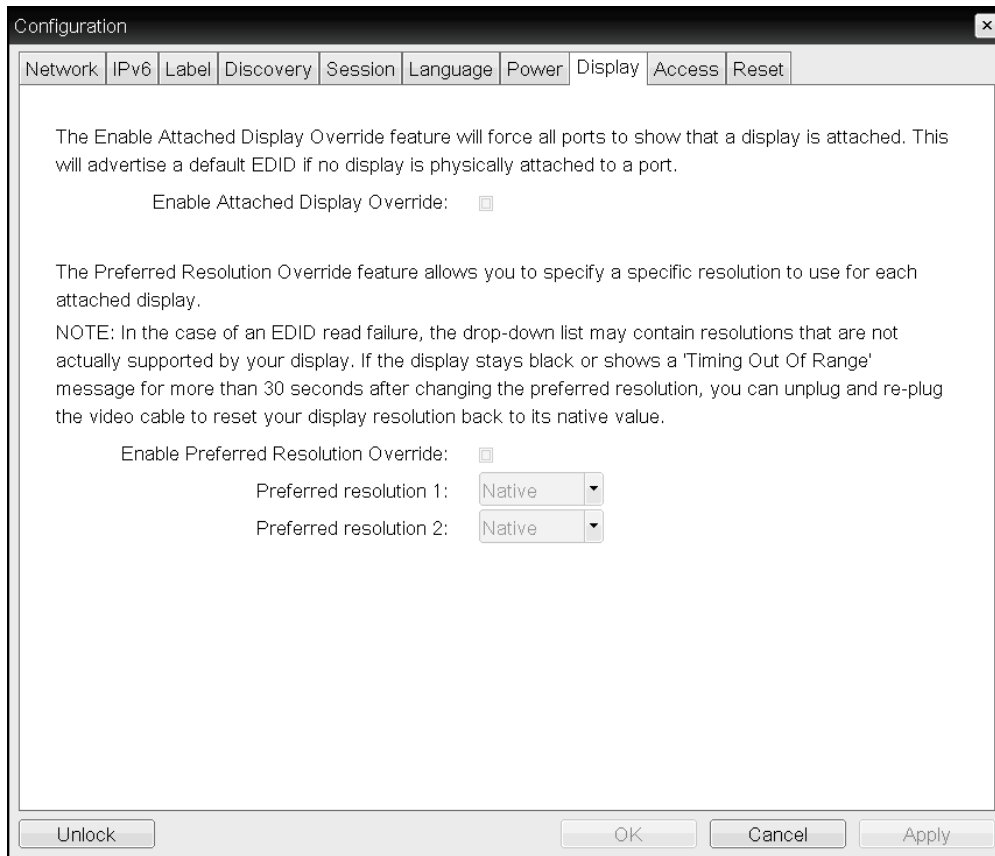| Parameter	Description
Enable Preferred Resolution Override	Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions as above will be advertised, except the preferred resolution you configure here for a display will be sent as the native resolution instead of the default native resolution of 1024x768. • **Preferred resolution 0**: Select the preferred resolution of the display connected to port 1 on the zero client. • **Preferred resolution 1**: Select the preferred resolution of the display connected to port 2 on the zero client. Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled. See "Important" note, above, for information on how to retain a custom resolution in the event of a hot plug, power outage, etc.

OSD Quad-display: Display Settings

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.

Note: This function is only available through the OSD.

Under normal operation, the GPU in the host computer queries a monitor attached to the 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 KVM devices. The **Enable Attached Display Override** feature in this page allows you to configure the client to advertise default EDID information to the GPU.

Warning: You should 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 drop-down 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 (i.e., perform a hot plug reset).

Important: 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, etc.), ensure that both these fields are enabled.

OSD Tera2 Display Page

OSD Tera2 Display Page Parameters

Parameter	Description
Enable Attached Display Override	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. The following default resolutions are advertised when this option is enabled: 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 Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.

Parameter	Description
Enable Preferred Resolution Override	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 as above will be advertised, except the preferred resolution you configure here for a display will be sent as the native resolution instead of the default native resolution of 1024x768. • **Preferred resolution 0**: Select the preferred resolution of the display connected to port 1 on the zero client. • **Preferred resolution 1**: Select the preferred resolution of the display connected to port 2 on the zero client. • **Preferred resolution 2**: Select the preferred resolution of the display connected to port 3 on the zero client. • **Preferred resolution 3**: Select the preferred resolution of the display connected to port 4 on the zero client. Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled. See "Important" note, above, for information on how to retain a custom resolution in the event of a hot plug, power outage, etc.

OSD TERA2321: Display Settings

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.
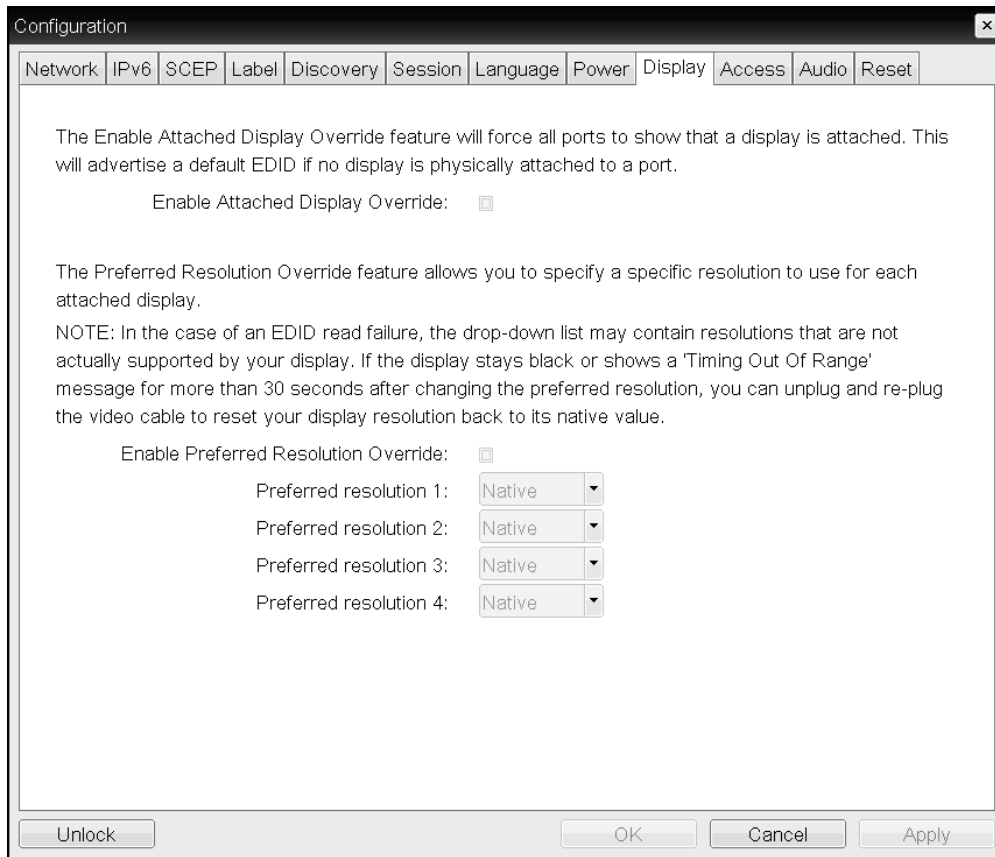
Note: This function is only available through the OSD.

Under normal operation, the GPU in the host computer queries a monitor attached to the 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 KVM devices. The **Enable Attached Display Override** feature in this page allows you to configure the client to advertise default EDID information to the GPU.

Warning: You should 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 drop-down 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 (i.e., perform a hot plug reset).

Important: 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, etc.), ensure that both these fields are enabled.

OSD TERA2321 Display Page

OSD TERA2321 Display Page Parameters

Parameter	Description
Enable Attached Display Override	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. The following default resolutions are advertised when this option is enabled: • 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 Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.

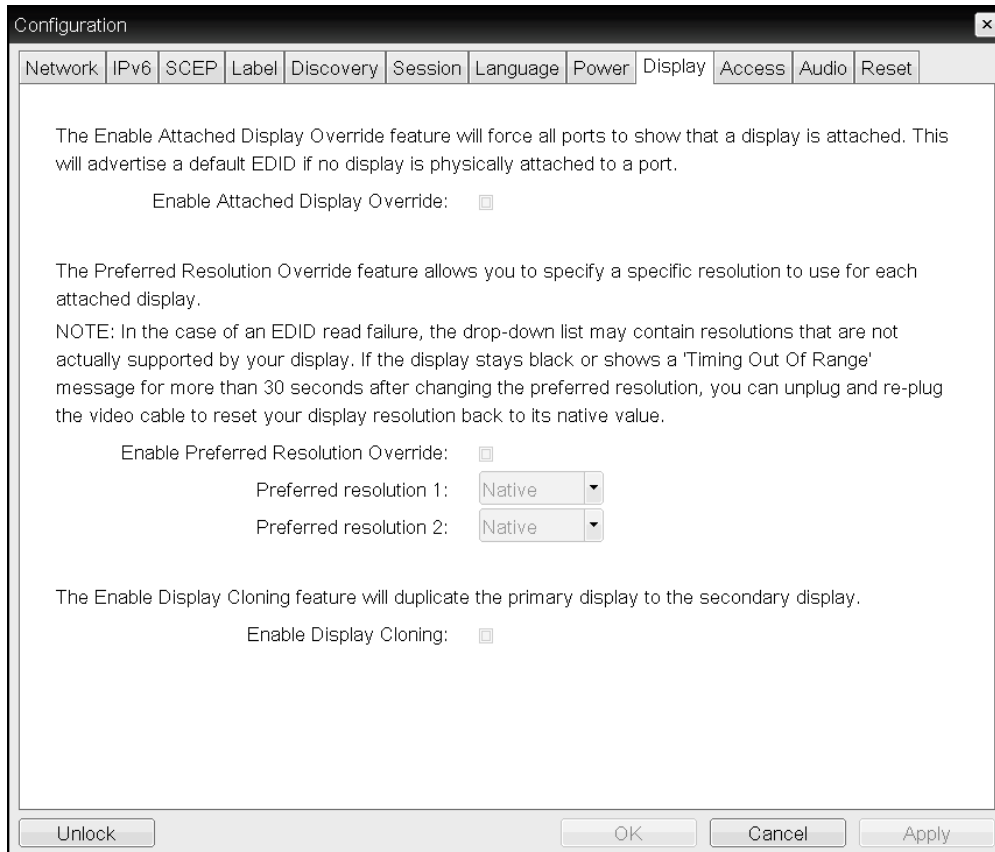| Parameter	Description
Enable Preferred Resolution Override	Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions as above will be advertised, except the preferred resolution you configure here for a display will be sent as the native resolution instead of the default native resolution of 1024x768. • **Preferred resolution 0**: Select the preferred resolution of the display connected to port 1 on the zero client. • **Preferred resolution 1**: Select the preferred resolution of the display connected to port 2 on the zero client. Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled. See "Important" note, above, for information on how to retain a custom resolution in the event of a hot plug, power outage, etc.
Enable Display Cloning	This option is only available for the TERA2321 zero client. Enable the display cloning option if you want the secondary display to mirror the primary display—e.g., for digital signage, trainings, etc. Note: If you are connecting a TERA2321 zero client to a remote workstation that does not have the PCoIP host software installed and the host driver function enabled, *and* you are using monitor emulation on the remote workstation, you may experience black screens on the cloned displays. To remedy the problem, you can either install and enable the host software, or you can disable monitor emulation on the video port for the secondary display only.

Configuring Password Parameters (AWI/OSD)

OSD: Password Settings

The **Password** page lets you update the local administrative password for the device. You can access this page from the **Options > Password** menu.

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 on the MC's Security Configuration page.

Note: 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.
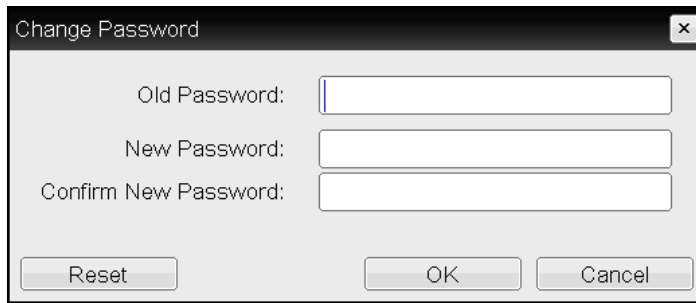
OSD Change Password Page

OSD Change Password Page Parameters

Parameter	Description
Old Password	This field must match the current administrative password before you can update the password.
New Password	The new administrative password for both the AWI and the local OSD GUI.
Confirm New Password	This field must match the **New Password** field for the change to take place.
Reset	If the client password becomes lost, you can click the **Reset** button to request a response code from the 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. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password. Note: 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.

Configuring Reset Parameters (AWI/OSD)

AWI Client: Parameter Reset Settings

The **Reset Parameters** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Configuration > Reset Parameters** menu.

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

Reset

Reset all configuration and permission settings stored on the device

Reset Parameters: [Reset]

Enable keyboard shortcut: ☐ CTRL + ALT + SHIFT + SPACE

Hide keyboard shortcut sequence in OSD: ☐

[Apply] [Cancel]
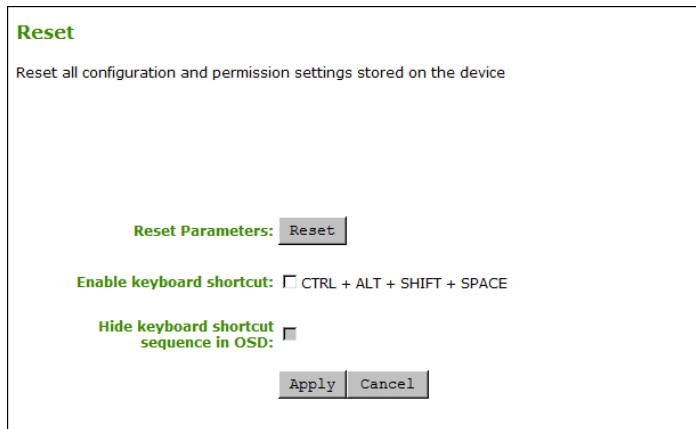
AWI Client Reset Page

AWI Client Reset Parameters

Parameter	Description
Reset Parameters	When you click this button, a prompt appears for confirmation. This is to prevent accidental resets.
Enable Keyboard Shortcut	When enabled, the user can press **CTRL+ALT+SHIFT+SPACE** to automatically reset the parameters and permissions for the device.
Hide keyboard shortcut sequence in OSD	When **Enable Keyboard Shortcut** is enabled and this field is disabled, the keyboard sequence appears on the **Reset Parameters** page for the client. When both **Enable Keyboard Shortcut** and this field are enabled, the keyboard sequence does not appear on the **Reset Parameters** page for the client; however, the user can still use the keyboard sequence to reset the parameter.

AWI Host: Parameter Reset Settings

The **Reset Parameters** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Configuration > Reset Parameters** menu.

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

Reset

Reset all configuration and permission settings stored on the device

Reset Parameters: Reset

Apply Cancel
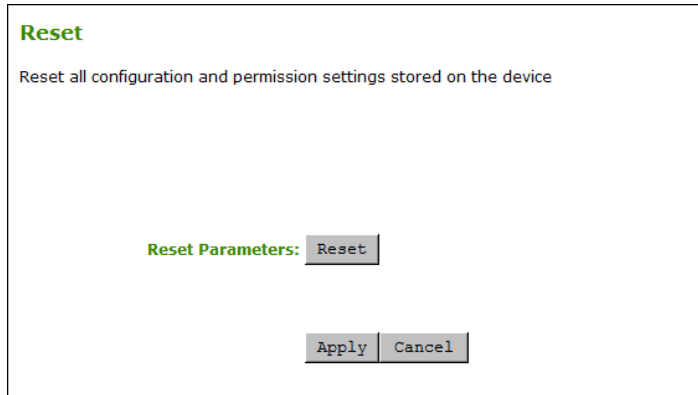
AWI Host Reset Page

AWI Host Reset Parameters

Parameter	Description
Reset Parameters	When you click this button, a prompt appears for confirmation. This is to prevent accidental resets.

OSD: Parameter Reset Settings

The **Reset** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Options > Configuration > Reset** menu.

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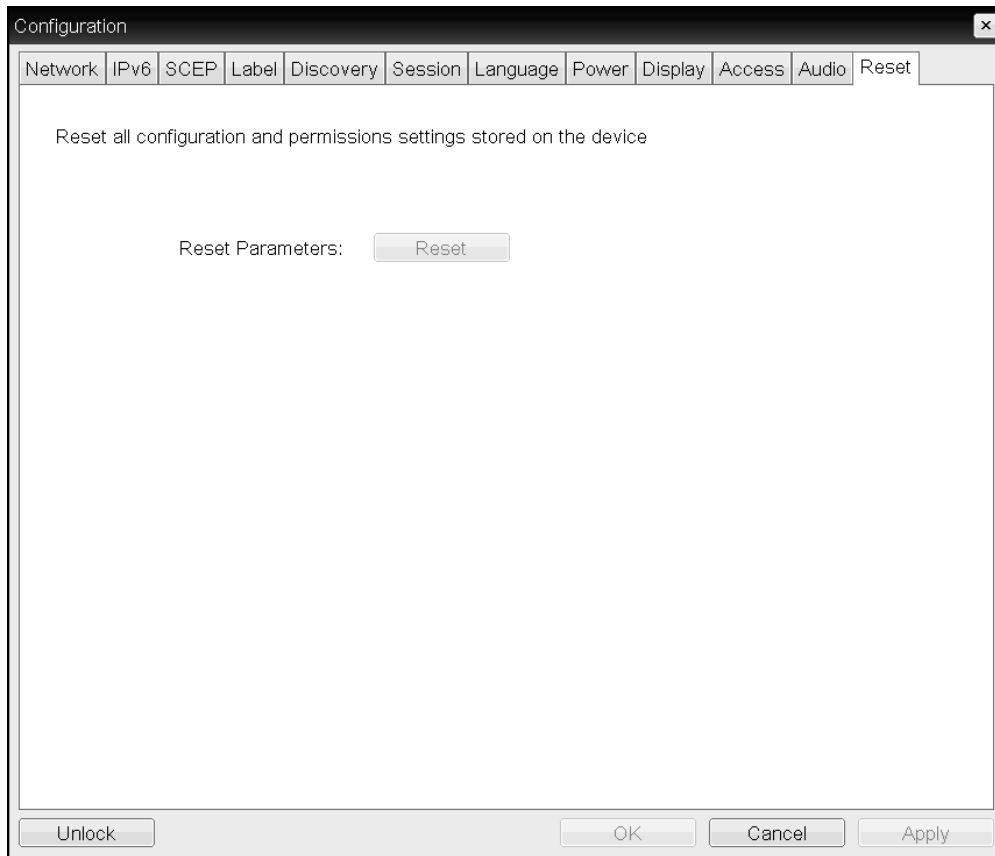
OSD Reset Page

OSD Reset Parameters

Parameter	Description
Reset Parameters	When you click this button, a prompt appears for confirmation. This is to prevent accidental resets.

Viewing Diagnostics (AWI/OSD)

AWI: Help for Event Log Settings

For information about the AWI's **Event Log** page, see AWI: Event Log Settings.

OSD: Help for Event Log Settings

For information about the OSD's **Event Log** page, see OSD: Event Log Settings.

AWI Host: Session Control Settings

The **Session Control** page lets you view information about a device and also allows you to manually disconnect or connect a session. You can access this page from the

Diagnostics > Session Control menu.

```
Session Control
Control the device




            Connection State: Connected to TERA2140 client 192.168.54.133
                         Connect    Disconnect


            Peer IP Address: 192.168.54.133

            Peer MAC Address: 00-30-04-0D-DB-BC
```

AWI Host Session Control Page

AWI Host Session Control Page Parameters

Parameter	Description
Connection State	This field displays the current state for the session. Options include the following: • **Disconnected** • **Connection Pending** • **Connected** Two buttons appear below the **Connection State** field: • **Connect:**This button is disabled for the host. • **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.

AWI Client: Session Control Settings

The **Session Control** page lets you view information about a device and also allows you to manually disconnect or connect a session. You can access this page from the **Diagnostics > Session Control** menu.

AWI Client Session Control Page

AWI Client Session Control Page Parameters

Parameter	Description
Connection State	This field displays the current state for the session. Options include the following: • **Disconnected** • **Connection Pending** • **Connected** Two buttons appear below the **Connection State** field: • **Connect:** If the connection state is **Disconnected**, click this button to initiate a PCoIP session between the client and its peer device. If the connection state is **Connection Pending** or **Connected**, this button is disabled. • **Disconnect:** If the connection state is **Connected** or **Connection Pending**, click this button to end the PCoIP session for the device. If the connection state is **Disconnected**, this button is disabled.
Peer IP	**Peer IP Address:** Displays the IP address for the peer device. When not in session, this field is blank.
Peer MAC Address	**Peer MAC Address:** Displays the MAC address of the peer device. When not in session, this field is blank.

AWI Host: Session Statistics Settings

The **Session Statistics** page lets you view current statistics when a session is active. If a session is not active, the statistics from the last session will display. You can access this page from the **Diagnostics > Session Statistics** menu.

Session Statistics

View statistics for the current session

Connection State: Connected to TERA2140 client 192.168.54.133
802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 42885 / 28458 / 0
Bytes (Sent/Received): 19081850 / 3629012
Round Trip Latency (Min/Avg/Max): 2 / 2 / 5 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 1240 / 5784 / 11568 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 232 / 392 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 39 / 297 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Active/Max): 40 / 90 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

Reset Statistics

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	23 fps	21 fps	Perceptually Lossless
2	N/A	N/A	N/A	N/A
3	60 fps	0 fps	0 fps	Lossless
4	N/A	N/A	N/A	N/A

AWI Host Session Statistics Page

Note: The above figure shows session statistics for a remote workstation card connected to a client with four connected displays. If your deployment uses two displays, information for only two displays will appear in this section.

AWI Host Session Statistics Page Parameters

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Values include the following: • **Asleep** • **Canceling** • **Connected** • **Connection Pending** • **Disconnected** • **Waking**

Parameters	Description
802.1X Authentication Status	Indicates whether 802.1x authentication is enabled or disabled on the device.
PCoIP Packets Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.
Bytes	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms).
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	How much image data is currently being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the **Use Client Image Settings** field is configured on the **Image** page for the host device.
Initial Image Quality	The minimum and maximum quality setting is taken from the **Image** page for the device. The active setting is what's currently being used in the session and only appears on the host.
Image Quality Preference	This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image.

Parameters	Description
Build to Lossless	Options that may appear in this field include the following: **Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked. **Disabled:** The **Disable Build to Lossless** field is checked.
Reset Statistics	Click this button to reset the statistic information on this page. Note: The **Reset Statistics** button also resets the statistics reported in the **Home** page.
Display	The port number for the display.
Maximum Rate	This column shows the refresh rate of the attached display. If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate. If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined."
Input Change Rate	The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video).
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Image Quality	Shows the current lossless state of the attached display: • **Lossy** • **Perceptually lossless** • **Lossless**

AWI Client: Session Statistics Settings

The **Session Statistics** page lets you view current statistics when a session is active. If a session is not active, the statistics from the last session will display. You can access this page from the **Diagnostics > Session Statistics** menu.

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

Reset Statistics

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 Client Session Statistics Page

Note: The above figure shows session statistics for a client with two connected displays. If your deployment uses four displays, information for all four displays will appear in this section.

AWI Client Session Statistics Page Parameters

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Values include the following: • **Asleep** • **Canceling** • **Connected** • **Connection Pending** • **Disconnected** • **Waking**
802.1X Authentication Status	Indicates whether 802.1x authentication is enabled or disabled on the device.
PCoIP Packets Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.
Bytes	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms).
Bandwidth Statistics	**Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor.
Pipeline Processing Rate	How much image data is currently 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.

Parameters	Description
Initial Image Quality	The minimum and maximum quality setting is taken from the **Image** page for the device.
Image Quality Preference	This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include the following: **Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked. **Disabled:** The **Disable Build to Lossless** field is checked.
Reset Statistics	Click this button to reset the statistic information on this page. Note: The **Reset Statistics** button also resets the statistics reported in the **Home** page.
Display	The port number for the display.
Maximum Rate	This column shows the refresh rate of the attached display. If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate. If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined."
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Image Quality	Shows the current lossless state of the attached display: • **Lossy** • **Perceptually lossless** • **Lossless**

OSD: Session Statistics Settings

The **Session Statistics** page lets you view from the last session. You can access this page from the **Options > Diagnostics > Session Statistics** menu.
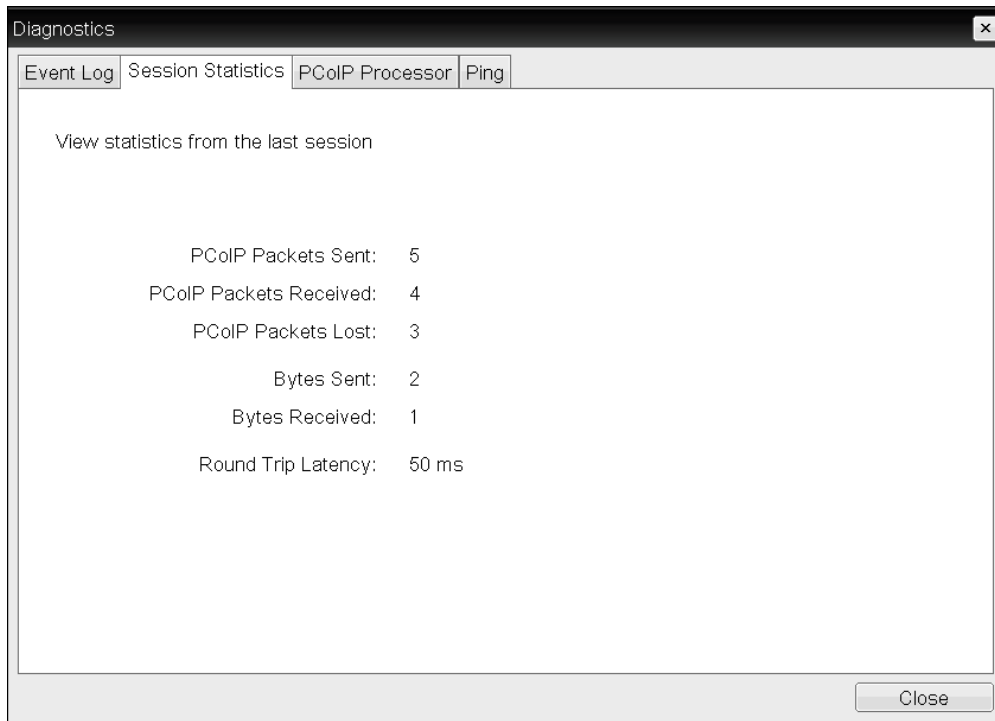
OSD Session Statistics Page

OSD Session Statistics Page Parameters

Parameters	Description
PCoIP Packets Statistics	**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	**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).

AWI Host: Host CPU Settings

The **Host CPU** page lets you view the identity string of the host computer, view the current power state, and change the host's power state. You can access this page from the **Diagnostics > Host CPU** menu.

Host CPU

View identity, view and change power state (host only)

Host Identity:

Current Power State: S0 (On)

Change Power State: [S5 (Soft Off) ▼] [Apply]
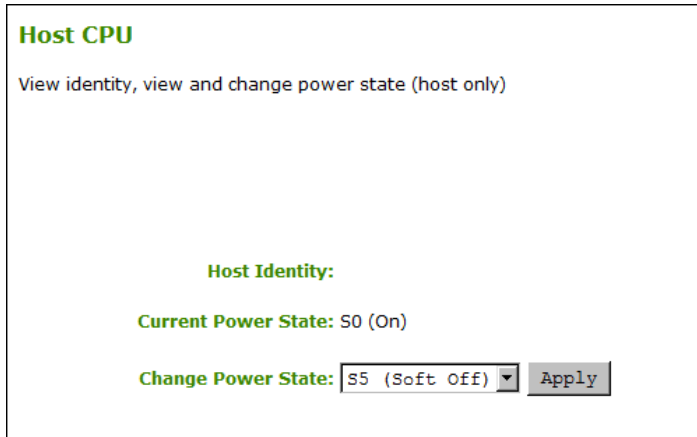
AWI Host CPU Page

AWI Host CPU Page Parameters

Parameters	Description
Host Identity	The identity string of the host computer (if data is available).
Current Power State	The current power state that is configured for the host.
Change Power State	Select one of the following options: • **S5 (Soft Off)**: *Tera1 zero clients*: With this power state setting, users can perform a soft power off of the host PC by pressing the zero client's remote PC button for less than four seconds. *This option is not available for Tera2 zero clients.* • **S5 (Hard Off**): *Tera1 zero clients*: With this power state setting, users can perform a hard power off of the host PC by pressing the zero client's remote PC button for more than four seconds. *Tera2 zero clients*: Users can perform a hard power off of the host PC from the Zero Client Control Panel when the zero client's connect/disconnect button is pressed. Note: To use this feature, the host must have compatible hardware architecture.

AWI Client: Audio Settings

The **Audio** page lets you generate an audio test tone from the client. You can access this page from the **Diagnostics > Audio** menu.

To generate an audio test tone, click **Start** to start the test tone. Click **Stop** to stop the test.

Note: The **Audio** page functionality is only available on a client when the client is not in a PCoIP session.
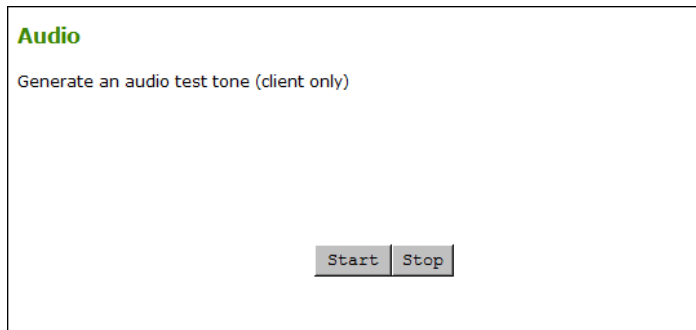
AWI Client Audio Page

AWI Client: Display Settings

The **Display** page lets you initiate and view a test pattern on the client's display. You can access the page from the **Diagnostics > Display** menu.

Note: The test pattern only appears on the **Display** page when the client is not in a PCoIP session. If you click **Start** when the client is in session, an error message appears.
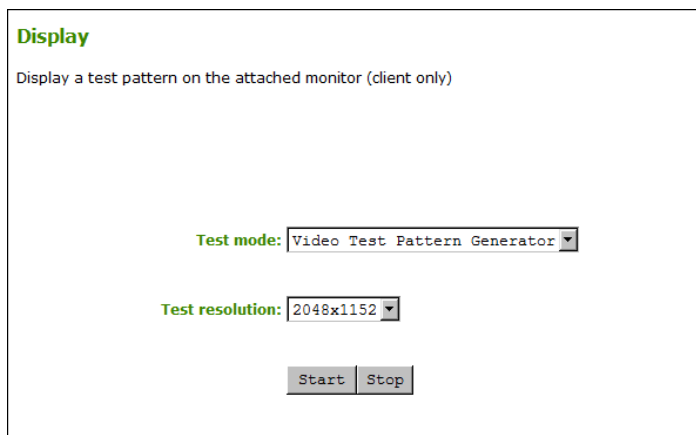
AWI Client Display Page

AWI Client Display Page Parameters

Parameters	Description
Test mode	Set the type of test pattern for the attached monitor(s) as follows: • **Video Test Pattern Generator** • **Pseudo Random Bitstream**
Test resolution	Select the test resolution to use from the drop-down menu.
Start/Stop	Click **Start** to begin the test pattern. Click **Stop** to stop the test.

AWI: PCoIP Processor Settings

The **PCoIP Processor** page lets you reset the host or client and view the uptime of the device's PCoIP processor since the last boot. You can access this page from the **Diagnostics > PCoIP Processor** menu.

PCoIP Processor

Reset the PCoIP device, view the time elapsed since boot

Current Time: 04/15/2013 15:06:12

Time Since Boot: 4 Days 3 Hours 34 Minutes 28 Seconds

Reset PCoIP Processor: Reset
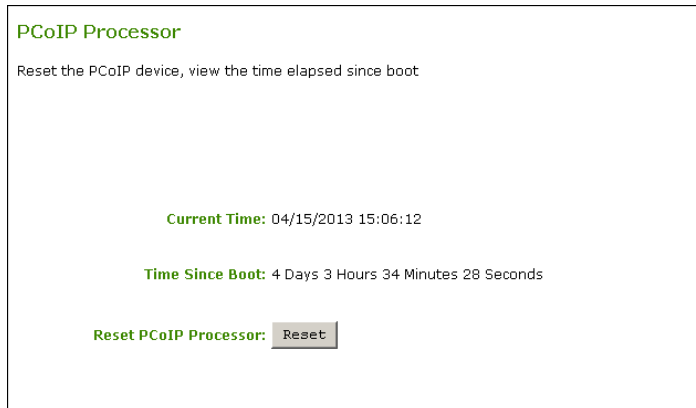
AWI PCoIP Processor Page

AWI PCoIP Processor Page Parameters

Statistics	Description
Current Time	The current time. This feature requires that NTP be enabled and configured.
Time Since Boot (Uptime)	View the uptime of the device's PCoIP processor since the last boot.
Reset PCoIP Processor	Click this button to reset the device.

OSD: PCoIP Processor Settings

The **PCoIP Processor** page lets you view the uptime of the device's PCoIP processor since the last boot. You can access this page from the **Options > Diagnostics > PCoIP Processor** menu.
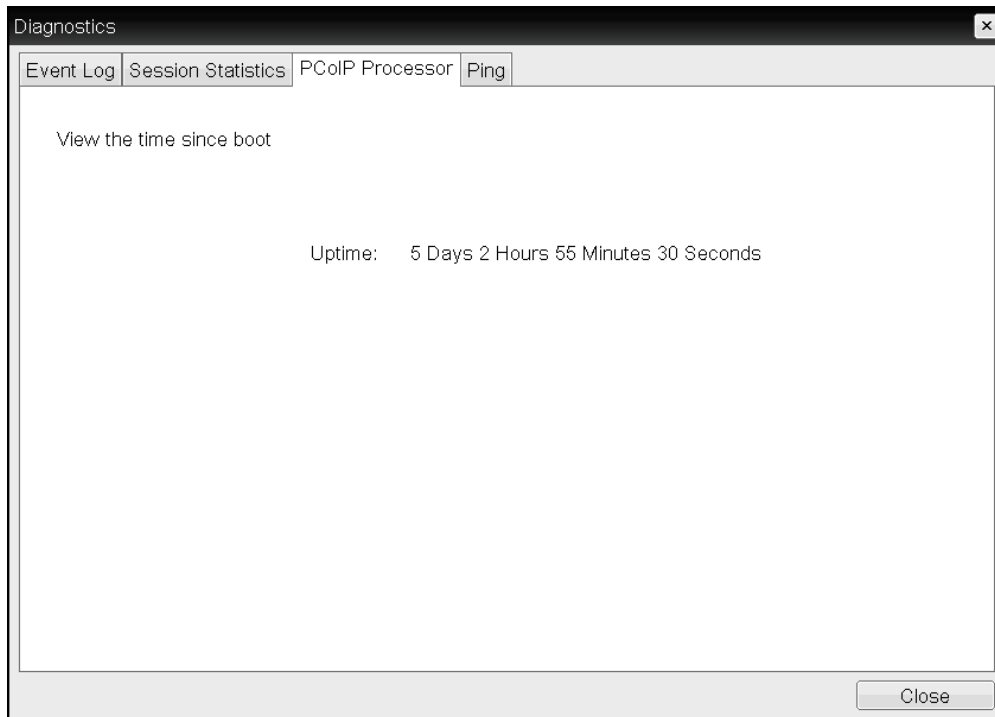
OSD PCoIP Processor Page

AWI Tera2 Client: Packet Capture

The **Packet Capture** page provides a diagnostic tool for capturing packets on the zero client—for example, when troubleshooting calls made with Counterpath's Bria Virtualized Edition for PCoIP Zero Clients softphone client. You can access this page from the **Diagnostics > Packet Capture** menu.

Note: PCoIP traffic is not included in the packet capture. All other network traffic, including Unified Communications media traffic, is captured.

To capture network packets for troubleshooting an issue:

1. Click the **Start** button to initiate packet capture.

2. Repeat the steps required to reproduce the issue (e.g., if you are troubleshooting a call, make the call using the softphone client).

3. Click the **Stop** button to stop packet capture.
   Note: 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.

4. Click the **Download** link, and then save the file to the desired location on your computer.

5. If you have purchased support and maintenance, enter a trouble ticket at Teradici Support with this diagnostic file attached. For complimentary support, please go to the Teradici PCoIP Community Forum.

Packet Capture

Capture network packets for diagnostics

Packet Capture Status: Idle
Bytes (Captured/Max): 0 / 20971520 (0.0 %) in 0 packets
Diagnostic Packet Capture: [Start]
Download Packet Capture: Download
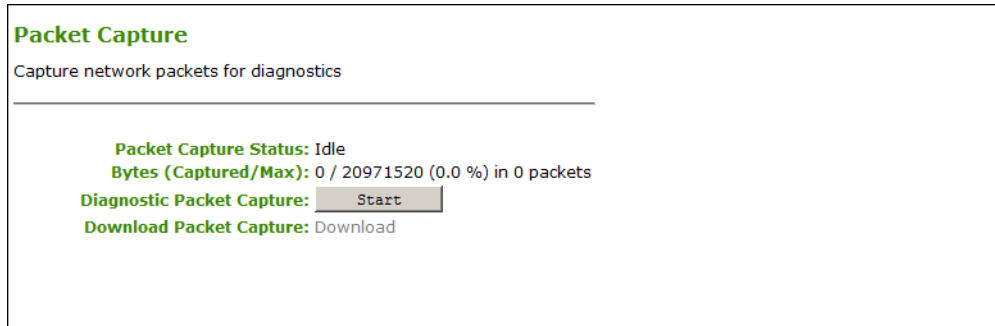
AWI Tera2 Client Packet Capture Page

AWI Tera2 Client Packet Capture Page Parameters

Parameters	Description
Packet Capture Status	Displays the status of the packet capture tool. Values include the following: • **Idle**: Packet capture has not been initiated. Note: After performing a packet capture, the status displays as **Idle** again if you reboot the zero client. • **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 capture and **Stop** to stop capture. Note: 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.
Diagnostic Packet Capture	Click **Download** to save the **packet_capture.bin** file to the desired location on your computer.

OSD: Ping Settings

The **Ping** page lets you ping a device to see if it is reachable across the IP network. This may help you determine if a host is reachable. Because firmware releases 3.2.0 and later force the "do not fragment flag" in the ping command, you can also use this feature to determine the maximum MTU size.

You can access this page from the **Options > Diagnostics > Ping** menu.
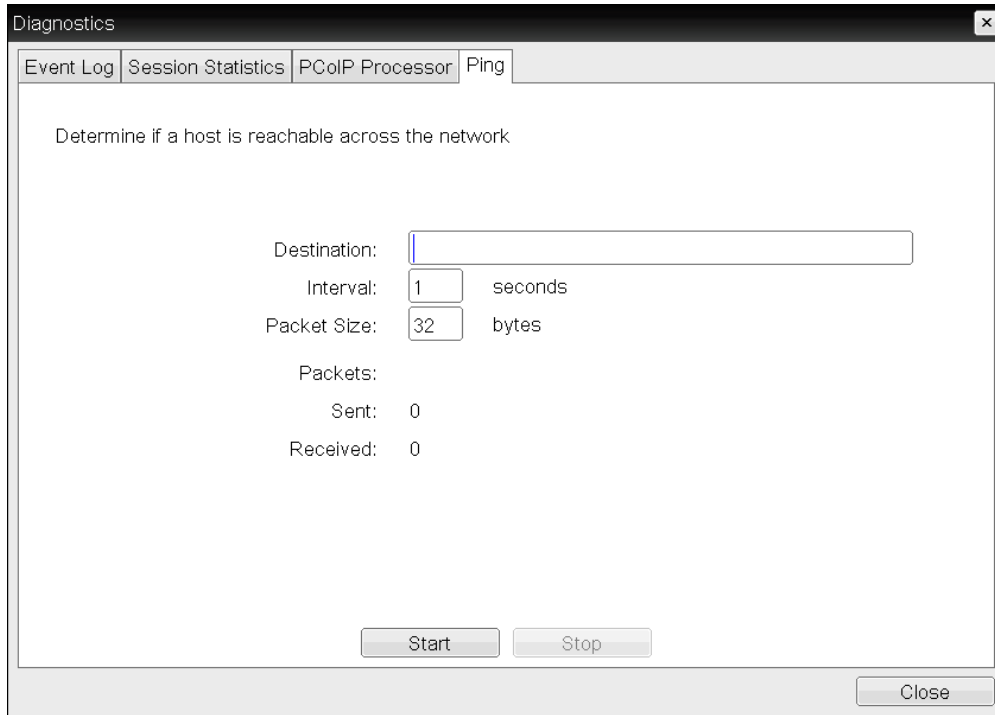
OSD Ping Page

Ping Page Parameters

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.

Viewing Information (AWI/OSD)

AWI: Version Information

The **Version** page lets you view the hardware and firmware version details for a device. You can access this page from the **Info > Version** menu.

Note: The information shown below is for example purposes only. Your version information and build numbers may differ.

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:	4.8.0
Firmware Build ID:	r4_8@17399
Firmware Build Date:	Mar 25 2015 16:53:39
PCoIP Processor Family:	Tera2
PCoIP Processor Revision:	0.0
Bootloader Version:	1.9.0
Bootloader Build ID:	r4_7@16301
Bootloader Build Date:	Jul 2 2014 14:40:47

AWI Version Page

AWI Version Page Parameters

Parameters	Description
VPD Information	**(Vital Product Data)**: Information provisioned by the factory to uniquely identify each host or client: • **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	This information reflects the current firmware details: • **Firmware Version:** Version of the current firmware. • **Firmware Build ID:** Revision code of the current firmware. • **Firmware Build Date:** Build date for the current firmware.
PCoIP Processor Information	This information provides details about the PCoIP processor. • **PCoIP Processor Family**: The processor family—Tera1 or Tera2. • **PCoIP Processor Revision**: The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0.
Bootloader Information	This information reflects the current firmware bootloader details: • **Boatloader Version:** Version of the current bootloader. • **Bootloader Build ID:** Revision code of the current bootloader. • **Bootloader Build Date:** Build date of the current bootloader.

Viewing the Version Information

The **Version** page lets you view the hardware and firmware version details for a device. You can access this page from the **Options > Information > Version** menu.

Note: The information shown below is for example purposes only. Your version information and build numbers may differ.
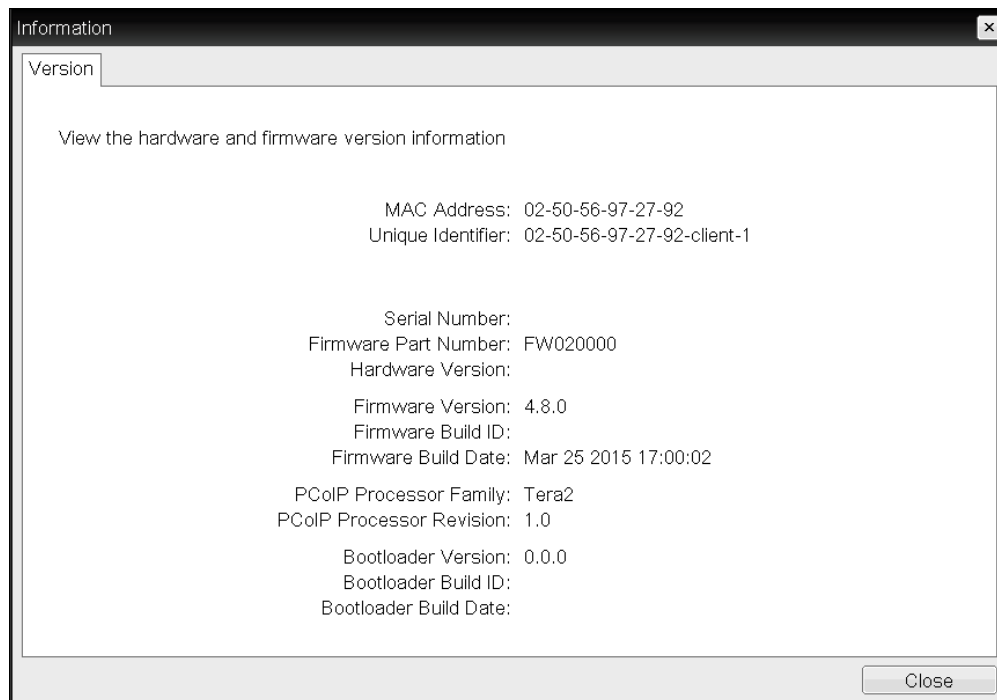
OSD Version Page

OSD Version Page Parameters

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

Parameters	Description
Firmware Information	This information reflects the current firmware details: • **Firmware Version:** Version of the current firmware. • **Firmware Build ID:** Revision code of the current firmware. • **Firmware Build Date:** Build date for the current firmware.
PCoIP Processor Information	This information provides details about the PCoIP processor. • **PCoIP Processor Family**: The processor family—Tera1 or Tera2. • **PCoIP Processor Revision**: The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0.
Bootloader Information	This information reflects the current firmware bootloader details: • **Boatloader Version:** Version of the current bootloader. • **Bootloader Build ID:** Revision code of the current bootloader. • **Bootloader Build Date:** Build date of the current bootloader.

AWI Host: Attached Devices Information

The **Attached Devices** page lets you see information for the displays that are currently attached to the client. You can access this page from the **Info > Attached Devices** page.

Attached Devices

View presently connected monitors

Displays:

Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date
1	BenQ EW2420	Not in Session	DP	1920x1080 @ 60 Hz	V7B00284067	BNQ	7923	30-2011
2	SME2320	Not in Session	DP	No source signal	HVRZA00951	SAM	6B2	42-2010
3	BenQ EW2420	Not in Session	DP	1920x1080 @ 60 Hz	93B02607026	BNQ	7923	10-2011
4	BenQ BL2400	Not in Session	DP	No source signal	92C00369SL0	BNQ	8002	7-2012

    Hide Legend

Legend (Displays):

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

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

AWI Host Attached Devices Page

Note: The above figure shows information for a client with four connected displays. If your deployment uses two displays, information for only two displays will appear on this page.

AWI Host: Attached Devices Page Information

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

AWI Client: Attached Devices Information

The **Attached Devices** page lets you see information for the displays that are currently attached to the client. You can access this page from the **Info > Attached Devices** page.

Attached Devices

View presently connected monitors and USB devices

Displays:

Port	Model	Status	Mode	Resolution	VID	PID	Date	Serial
1	BenQ EW2420	Not in Session	DVI	1920x1080 @ 60 Hz	BNQ	7923	30-2011	V7B00284067
2	BenQ EW2420	Not in Session	DVI	1920x1080 @ 60 Hz	BNQ	7923	10-2011	93B02607026

USB Devices:

Device	Parent	Model	Status	Controller	Internal/External	VID	PID	CSP	Local Driver	Serial
0100	Root 1	USB Optical Mouse	Not in Session	OHCI	External	046D	C05A	00/00/00	Mouse	-
0201	Root 3	USB Keyboard	Not in Session	OHCI	External	046D	C31C	00/00/00	Keyboard, Remote Control	-
0302	Root 0	Plantronics C510-M	Not in Session	OHCI	External	047F	C01A	00/00/00	Multiple Drivers	6393016AB12D4D469347CB646863BC07

Hide Legend

Legend (Displays):

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

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

AWI Client Attached Devices Page

Note: 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 of these functions.) In the USB specification, USB class/subclass/protocol class code information is used to identify a device's functionality so that the right device driver

can be loaded for the device. Depending on the device, this information can be contained in the device descriptor, the interface descriptors, or in both places.

When a device is authorized, the **Device Class**, **Sub Class**, and **Protocol** class code fields displayed in the **Attached Devices** page equal the values read from the device descriptor. For many devices, this is all zeros, indicating that the class code information is contained in the interface descriptors, not the device descriptor—i.e., each interface has its own class/subclass/protocol definitions. However, when a device is *not* authorized, the **Device Class**, **Sub Class**, and **Protocol** fields displayed on this page equal the values read from the interface that caused the device to fail authorization.

AWI Client: Attached Devices Page Information

Statistic	Description
Displays	This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the display attached to each port. Note: 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. See note above for an explanation of the information displayed in the **Device Class**, **Sub Class**, and **Protocol** class code fields.
USB Device Status	Status options include: • **Not Connected**: No device is connected. • **Not in Session**: The device is detected outside of a PCoIP session. • **Not Initialized**: The device is detected in a PCoIP session but the host controller has not initialized the device. • **Failed Authorization**: The device is detected in a PCoIP session but is not authorized. (For more information about USB , see AWI Client: USB 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.

Configuring User Settings (OSD)

OSD: Certificate Checking Settings

The **Certificate** page lets users select how the client behaves if it cannot verify a secure connection to the server. You can access this page from the **Options > User Settings > Certificate** menu.

Note: If **Certificate Check Mode Lockout** is enabled from the AWI, users will not be able to modify the settings on this page.
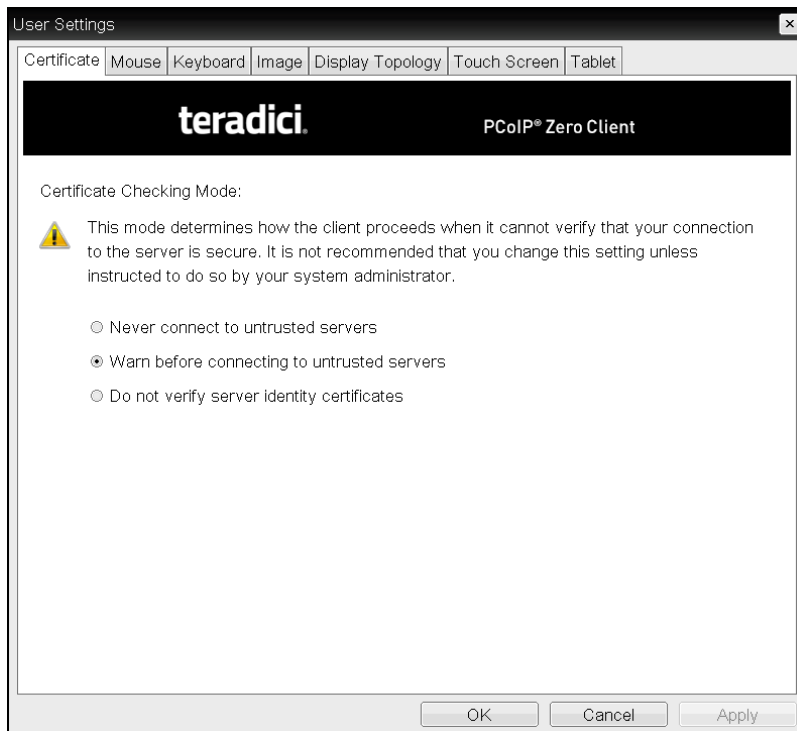
OSD Certificate Page

OSD Certificate Page Parameters

Parameter	Description
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 allow all connections.

MC: Help for Certificate Checking Settings

Certificate checking settings for the Management Console are described in the following topics:

- PCoIP Connection Manager pages
- View Connection Server pages

AWI Client: Help for Certificate Checking Settings

Certificate checking settings for the AWI are described in the following topics:

- PCoIP Connection Manager pages
- View Connection Server pages

OSD: Mouse Settings

The **Mouse** page lets you change the mouse cursor speed settings for the OSD sessions. You can access this page from the **Options > User Settings > Mouse** menu.

You can also configure the mouse cursor speed through the PCoIP host software. For more information, see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center.

Note: The OSD mouse cursor speed setting does not affect the mouse cursor settings when a PCoIP session is active unless the **Local Keyboard Host Driver** function is being used (see "PCoIP® Host Software for Windows User Guide" (TER1008001) for more details). This function is only available through the OSD. It is not available in the AWI.
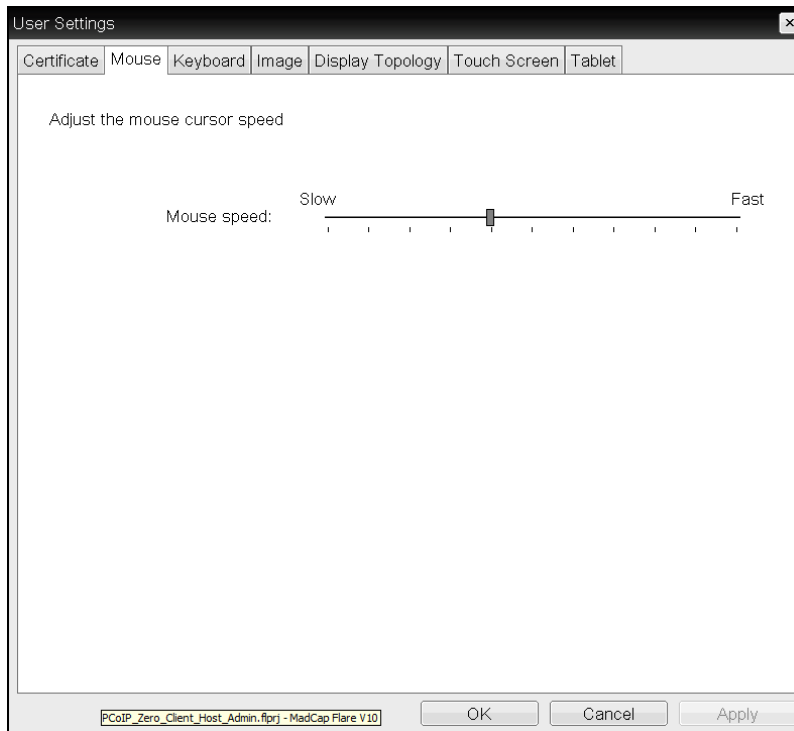
OSD Mouse Page

OSD Mouse Page Parameters

Parameter	Description
Mouse Speed	Move the slider to configure the speed of the mouse cursor.

OSD: Keyboard Settings

The **Keyboard** page lets you change the keyboard character delay and character repeat settings for the OSD session. You can access this page from the **Options > User Settings > Keyboard** menu.

You can also configure the keyboard repeat settings through the PCoIP host software. For more information, see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center.

Note: The keyboard settings do not affect the keyboard settings when a PCoIP session is active unless the **Local Keyboard Host Driver** function is used (see "PCoIP® Host Software for Windows User Guide" (TER1008001) for more details). This function is only available through the OSD. It is not available in the AWI.
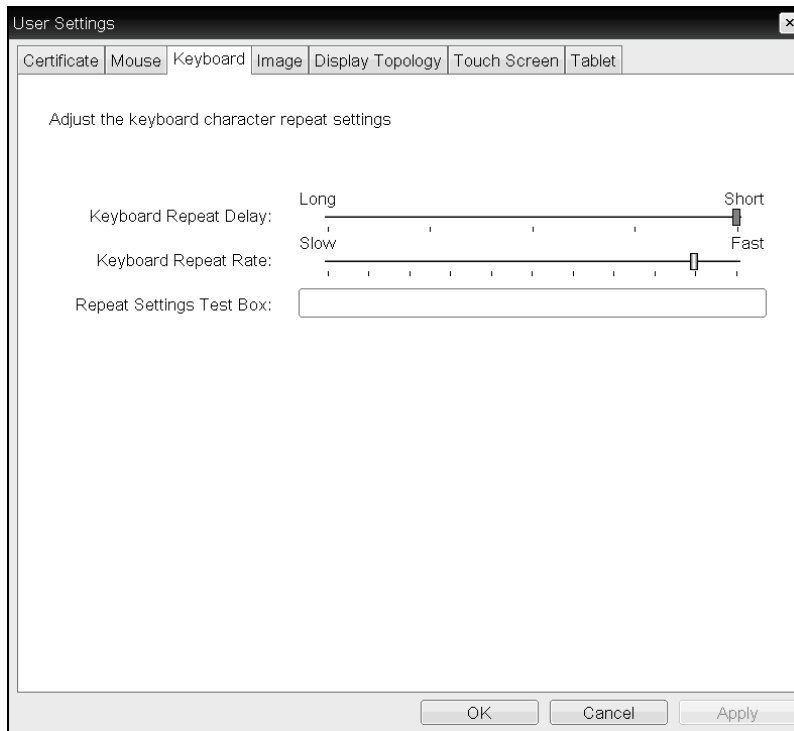
OSD Keyboard Page

OSD Keyboard Page Parameters

Parameter	Description
Keyboard Repeat Delay	Move the slider to configure the time that elapses before a character begins to repeat when it is held down.
Keyboard Repeat Rate	Move the slider to configure the speed at which a character repeats when it is held down.
Repeat Settings Test Box	Type in this box to test the chosen keyboard settings.

OSD: Help for Image Settings

For information about the OSD's **Image** page, see OSD: Image Settings.

OSD: Help for Display Topology Settings

For information about the OSD's **Topology** page, see OSD: Dual-display Topology Settings or OSD: Quad-display Topology Settings.

OSD: Touch Screen Settings

The **Touch Screen** page lets you configure and calibrate settings for an attached Elo TouchSystems touch screen display. See Setting up a Touch Screen Display for more

information about installing and configuring this device.

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

You can access this page from the **Options > User Settings > Touch Screen** menu.

Note: The **Touch Screen** page is only available through the OSD. It is not available from the AWI.
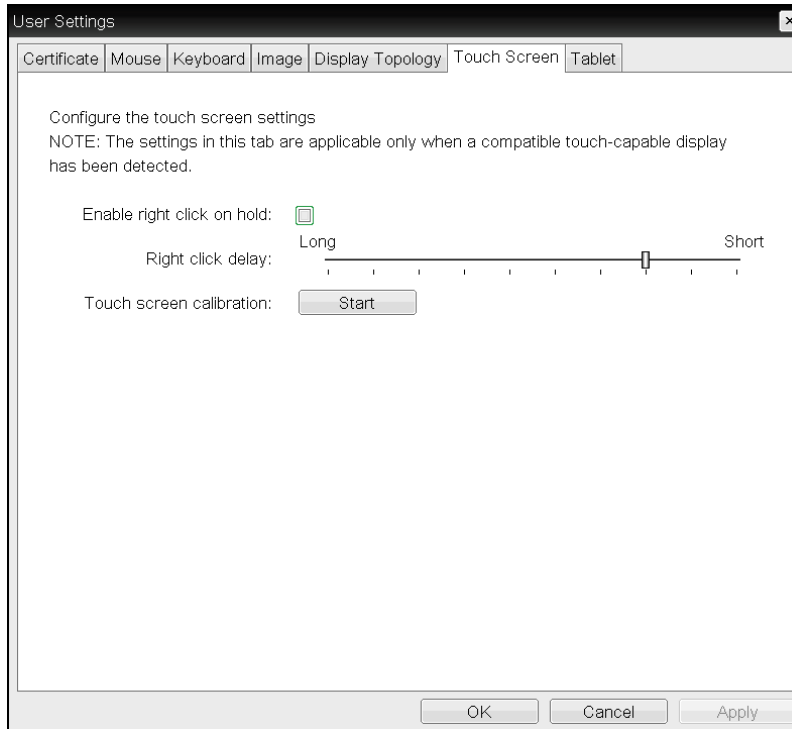
OSD Touch Screen Page

OSD Touch Screen Page Parameters

Parameter	Description
Enable right click on hold	Select this check box to let users generate a right-click when they touch the screen and hold it for a few seconds. If disabled, right-clicking is not supported.
Right click delay	Slide the pointer to the position (between Long and Short) to determine how long the users must touch and hold the screen to generate a right-click.

| Parameter	Description
Touch screen calibration	When you first connect the touch screen to the zero client, the calibration program starts. At the touch screen, touch each of the three targets as they appear.
	To test the calibration, run your finger along the monitor and ensure that the cursor follows it. If it is not successful, the calibration program automatically restarts. Once calibrated, the coordinates are stored in flash.
	To manually start the calibration program, from the OSD **Touch Screen** page, click **Start**. Follow the onscreen prompts.

OSD Tera2: Tablet Settings

The **Tablet** page lets you select whether an attached Wacom tablet is mapped to the entire desktop or to a specific attached monitor. It also lets you specify whether the tablet operates in a left-handed or right-handed orientation. You can access this page from the **Options > User Settings > Tablet** menu.

Note: These options only apply when a Wacom tablet is attached to a Tera2 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 newer). 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 "PCoIP® Host Software for Linux User Guide" (TER1104006) in the Teradici Support [Documentation Center](#).

The **Tablet** page updates automatically to show the number of monitors and tablets that are connected to the zero client. Up to four monitors can be connected, but only two locally connected tablets are supported. When just one monitor is attached, only the **Desktop** icon displays in the screen, and any attached tablets are mapped to the entire desktop.
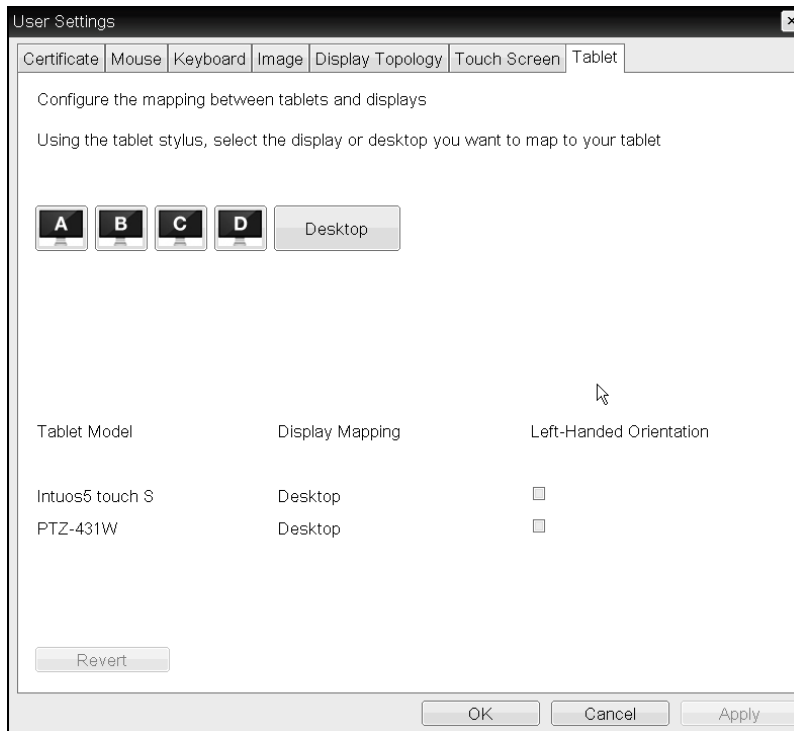
OSD Tablet Page

By default, tablets are mapped to the entire desktop (shown in the **Display Mapping** column in the above figure). 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. 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.

The **Revert** button reverts table mappings to the last applied configuration. To return to default table mappings (**Desktop**), simply unplug a monitor and then reconnect it to the zero client.

Note: Changing the topology settings in the Display Topology page (e.g., after rearranging your physical setup) will also automatically clear the tablet mappings. You will need to reconfigure your tablet setup whenever you apply topology changes.

OSD Tablet Page Parameters

| Parameter	Description
Display and Desktop icons	This section shows the number of displays that are currently attached to the 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**).
Left-Handed Orientation	To configure the tablet for a left-handed orientation: 1. Using either a mouse or the tablet's stylus, select the tablet's **Left-Handed Orientation** check box. 2. Click **Apply**. 3. Rotate the tablet 180° before using it.
Revert	Reverts the tablet settings to the last applied configuration. To revert table mappings to their default setting (**Desktop**), unplug a monitor and then reconnect it to the zero client. Applying topology changes will also clear the tablet configuration and set it to default.

'How To' Topics

Displaying Processor Information

The **Processor** field on the AWI **Home** page for a host or client displays the name of the device's processor, or chipset.

PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

Processor: TERA2140 revision 1.0 (512 MB)
Time Since Boot: 6 Days 16 Hours 37 Minutes 53 Seconds
PCoIP Device Name: pcoip-portal-0030040ddbbc

Connection State: Connected to host 192.168.65.103
802.1X Authentication Status: Disabled
Session Encryption Type: AES-256-GCM

PCoIP Packets (Sent/Received/Lost): 34716 / 52805 / 0
Bytes (Sent/Received): 4401736 / 24021386
Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 120 / 392 / 8000 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 256 / 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	11 fps	Lossy
2	60 fps	0 fps	Lossless
3	N/A	N/A	N/A
4	N/A	N/A	N/A

Processor Information on AWI Home Page

The processor family name displays on the AWI Version page for a host or client.
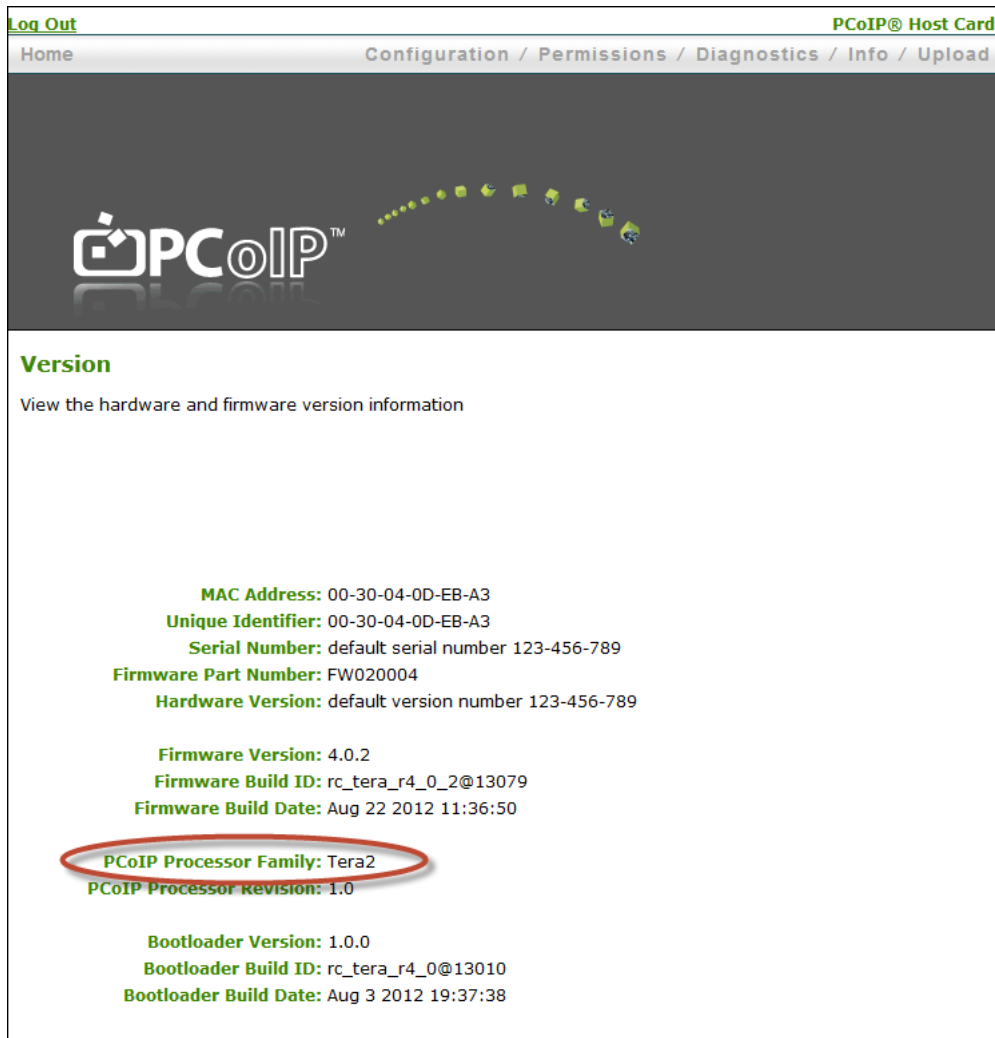
Processor Family Information on AWI Version Page

You can also display the processor family name for a zero client on the OSD Version page for the device.
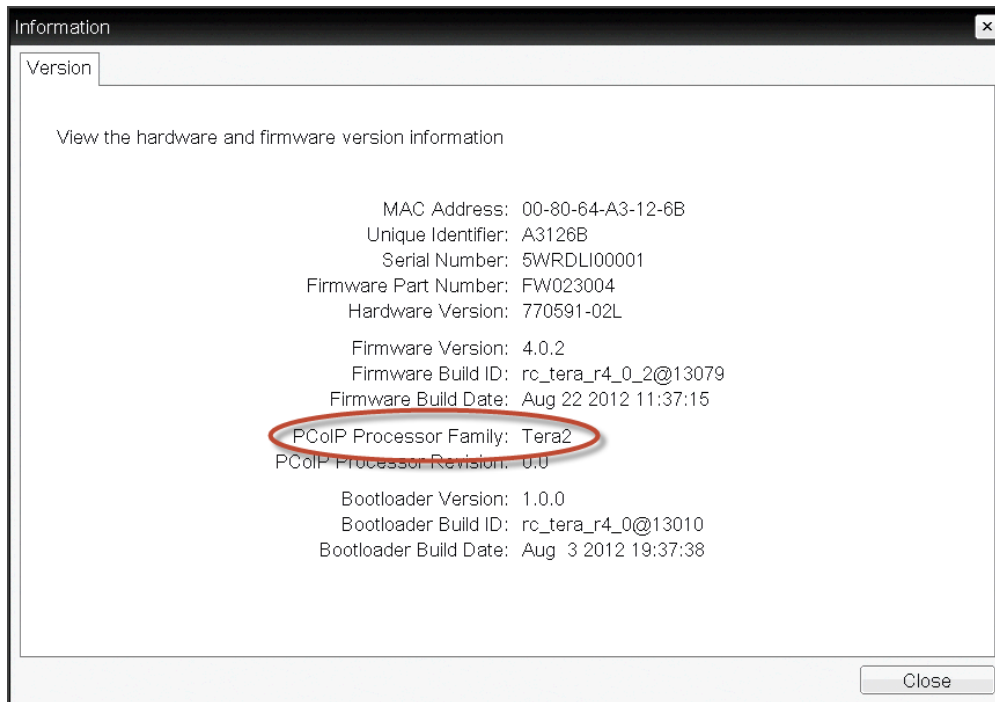
Processor Family Information on OSD Version Page

Configuring a Remote Workstation Card

Teradici's PCoIP Remote Workstation Card is a small add-in card that can be integrated into tower workstations, rack mount workstations, computer blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full workstation environment. This information is then communicated in real time over an IP network to the user's PCoIP client.

Installing a Remote Workstation Card

Important! The remote workstation's card's MAC address is located on a sticker on the card. It is important to write down this address before installing the card in the workstation. see KB 15134-1348 in the Teradici Support Site for additional information.

For detailed instructions on how to physically install the card, please see *PCoIP® Remote Workstation Card Quick Start Guide* in the Teradici Support Center. This guide has detailed instructions for each step of the installation process.

Important: When connecting the graphics card to the remote workstation card with the provided cables, always connect the lowest numbered connector on the graphics card to the lowest numbered connector on the remote workstation card, and continue upward.

Some graphics cards have both DVI and DisplayPort connectors. To support 2560x1600 resolution when connecting these graphics cards, connect the lowest numbered *DisplayPort* connector on the graphics card to the lowest number connector on the remote workstation card. Connecting the DVI connector on the graphics card to the remote workstation card will limit you to 1920x1200.

For complete details about the resolutions supported by different connectors and cables, see KB 15134-1607 in the Teradici Support Site.

Establishing a PCoIP Session to a Remote Workstation Card from a Zero Client

Note: For information on how to connect using a Teradici PCoIP® Software Client, see *Teradici PCoIP® Software Clients 1.9 Administrators' Guide*.

After successfully completing the installation steps outlined in PCoIP® Remote Workstation Card Quick Start Guide, the card will be connected to the network and the workstation powered on. The next step is to initiate a PCoIP session from a zero client using SLP host discovery.

Note: SLP host discovery requires the 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 remote workstation card so you can select it from the list of available hosts. In addition, the remote workstation card must be configured to accept any peer or to accept the specific MAC address of the zero client. You can configure this from the host AWI Configuration > Session > Direct from Client page.

By default, DHCP is enabled on the remote workstation card to allow your DHCP server to assign an IP address. If your network does not support DHCP, the card's default IP address will be 192.168.1.100.

To connect to a remote workstation card using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the zero client's OSD, select the Direct to Host + SLP Host Discovery connection type, and then click **OK**.

2. Click the **Connect** button.

3. When the **Discovered Hosts** screen appears with a list of available hosts, select the desired one by its IP/MAC address pair, and then click **OK**.

4. If prompted, enter your user name and password, and then click **OK**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

Installing the PCoIP Host Software

Optionally, you can also install the PCoIP host software package on the workstation to allow you to manage the card directly from the PCoIP host software UI on the workstation.

Note: Before installing this package on the workstation, you must first log in to the remote workstation card from the AWI, and enable the host driver function in the firmware from the **Configuration > Host Driver Function** menu.

For detailed instructions on how to install the PCoIP host software, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) or "PCoIP® Host Software for Linux User Guide" (TER1104006) in the Teradici Support Center.

Other Useful Links

The following topics provide more information about connecting zero clients and remote workstation cards.

- PCoIP Endpoints: Gives an overview of the PCoIP clients and hosts you can deploy in your network.
- Connection Prerequisites: Explains the conditions that must be in place before connecting PCoIP clients and hosts.
- **Common LAN Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts from within a LAN.
    - Zero Client to Remote Workstation Card (LAN)
    - Zero Client to Remote Workstation Card via View Connection Server (LAN)
    - Zero Client to Virtual Desktop via View Connection Server (LAN)
- **Common Remote Access Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts remotely.
    - Zero Client to Remote Workstation Card (WAN)
    - Zero Client to Remote Workstation Card via Hardware VPN (WAN)
    - Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)
    - Zero Client to Remote Workstation Card via View Security Server (WAN)
    - Zero Client to Virtual Desktop via View Security Server (WAN)

Configuring a Tera2 Zero Client

Tera2 PCoIP Zero Clients are secure client devices that allow users to connect to a variety of endpoints over a local or wide area IP network. For example, you can use zero clients to connect to the following endpoints:

- PCoIP Remote Workstation Cards
- PCoIP Workstation Access Software
- Amazon WorkSpaces desktops
- VMware Horizon View or VMware Horizon DaaS desktops
- Bria softphone caller endpoints via CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on a VMware Horizon View virtual desktop

Setting up the Zero Client

For detailed instructions on how to physically set up a zero client and connect it to USB devices, monitors, and the network, please see "Tera2 PCoIP® Zero Client Quick Start Guide" (TER1207007) in the Teradici Support Center. This guide has detailed instructions for each step of the installation process.

Static Fallback IP Address

If your network does not support DHCP, the card will use its static fallback IP address. This address is set by the card's manufacturer and can be located in the "**IN OFD:**" (optional factory defaults) section of the zero client's event log, as shown in the example below:

```
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 MC's **Network Settings** page (see Static Fallback IP Address). When set from the MC, the event log will display this address as "**IN FLASH:**" rather than "**IN OFD:**", as shown in the example below:

```
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
```

Note: If you reset the zero client, the static fallback IP address will revert to the factory default, even when this address has been set by the MC.

Establishing a PCoIP Session

Note: Zero clients are pre-configured to connect directly to a PCoIP Remote Workstation Card, but you can easily configure them for any session connection type.

After successfully completing the installation steps outlined in "Tera2 PCoIP® Zero Client Quick Start Guide" (TER1207007), the zero client will be powered on and ready to use. The next step is to initiate a PCoIP session. The easiest way to get started is to connect to a remote workstation card using SLP host discovery.

Note: SLP host discovery requires the 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 remote workstation card so you can select it from the list of available hosts. In addition, the remote workstation card must be configured to accept any peer or to accept the specific MAC address of the zero client. You can configure this from the host AWI Configuration > Session > Direct from Client page.

To connect to a remote workstation card using SLP host discovery:

1. From the **Options > Configuration > Session** menu on the zero client's OSD, select the Direct to Host + SLP Host Discovery connection type, and then click **OK**.

2. Click the **Connect** button.

3. When the **Discovered Hosts** screen appears with a list of available hosts, select the desired one by its IP/MAC address pair, and then click **OK**.

4. If prompted, enter your user name and password, and then click **OK**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

To establish a session using another session connection type:

1. From the zero client's OSD, select the **Options > Configuration > Session** menu.

2. From the **Connection Type** drop-down list, select the desired connection type:

   - Direct to Host
   - PCoIP Connection Manager (Tera2 only)
   - PCoIP Connection Manager + Auto-Logon (Tera2 only)
   - View Connection Server
   - View Connection Server + Auto-Logon
   - View Connection Server + Kiosk
   - View Connection Server + Imprivata OneSign
   - Connection Management Interface

3. After entering the required information, click **OK** on the **Session** page.

4. Click the **Connect** button.

5. If prompted, enter your user name and password.

6. If you are using a brokered connection and have more than one entitlement, select the desired one, and then click **Connect**.

When connected successfully, your display shows your desktop on the remote workstation, and the zero client's session LED on the front panel turns green.

Other Useful Links

The following topics provide more information about connecting zero clients and remote workstation cards.

- PCoIP Endpoints: Gives an overview of the PCoIP clients and hosts you can deploy in your network.
- Connection Prerequisites: Explains the conditions that must be in place before connecting PCoIP clients and hosts.
- **Common LAN Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts from within a LAN.
  - Zero Client to Remote Workstation Card (LAN)
  - Zero Client to Remote Workstation Card via View Connection Server (LAN)
  - Zero Client to Virtual Desktop via View Connection Server (LAN)
- **Common Remote Access Scenarios**: Provides a quick overview of how to connect PCoIP clients and hosts remotely.
  - Zero Client to Remote Workstation Card (WAN)
  - Zero Client to Remote Workstation Card via Hardware VPN (WAN)
  - Zero Client to Remote Workstation Card via 3rd Party Broker (WAN)
  - Zero Client to Remote Workstation Card via View Security Server (WAN)
  - Zero Client to Virtual Desktop via View Security Server (WAN)

Uploading Firmware

Uploading a Firmware Release to a Zero Client

To upload a firmware release to a zero client:

1. Log in to the client's AWI.
2. From the **Firmware Upload** page, browse to the folder containing the firmware file. This 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**.

Upload a Firmware Release to a Remote Workstation Card

To upload a firmware release to a PCoIP Remote Workstation Card:

1. Ensure the host PC or workstation is in an idle state (i.e., that all applications are closed).

2. Log into the host's AWI.

3. From the **Firmware Upload** page, browse to the folder containing the firmware file. This file will have an ".all" extension.

4. Double-click the correct "*.all" firmware file.

5. Click **Upload**.

6. 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**.

7. Click **Reset**.

8. Click **OK**.

9. Power off and then power on the host PC or workstation. It is necessary to power off (not just restart) the PC or workstation in order for the changes to take effect on the remote workstation card.

For information on using the MC to assign a firmware release to a profile, see MC: Firmware Management.

Configuring Syslog Settings

You can configure syslog settings for a host or zero client from the device's AWI, or you can use the MC to configure settings for a device profile. Both methods are shown below. Configuration involves entering the IP address or fully qualified domain name (FQDN) for the syslog server, and then specifying the port number and facility to use when sending messages to the syslog server.

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) as the syslog port to use. However, you can use a different port as long as the syslog server is set to receive syslog messages on the same port as the device is set to send them.

Teradici also uses "19 – local use 3" as the default facility under the assumption that this facility is not commonly used. If it is being used, you can select a different facility.

Note: 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.

Note: Ensure that your syslog server can handle the volume of messages sent by a zero client. With some free syslog servers, messages can become lost if the volume is too great.

Setting up Syslog from the AWI

Syslog settings in the AWI are located in the **Event Log** page. To configure syslog settings from the AWI for a single device:

1. From an Internet browser, enter the IP address of the PCoIP zero client or host.
2. Select the **Diagnostics > Event Log** menu to display the **Event Log** page.
3. Check **Enable Syslog**, and then select whether you want to identify the syslog server by its IP address or fully qualified domain name (FQDN).
4. Enter the IP address or FQDN of the syslog server.
5. If the syslog server is configured to receive data on a port other than 514, enter this port number.
6. If you wish the device to use a facility other than the default, select it from the **Syslog Facility** drop-down list.
7. Click **Apply**.
8. At the **Success** page, click **Continue**.

Setting up Syslog from the MC

Syslog settings in the MC are located in the MC's **Event Log** page. To configure syslog settings from the MC for a device profile:

1. From an Internet browser, enter the IP address of the MC.
2. Select the **Profiles** tab.
3. From the **Profile Management** page, click the **Set Properties** link for the desired profile.
4. Expand the **Event Log Control** category, and then click the **Edit Properties** link.
5. Enable **Syslog Server Hostname**, and then enter the IP address or FQDN of the syslog server.

6. Enable **Syslog Server Port**, and then enter the port number used by the syslog server for incoming messages. The device will use this port to send messages.

7. Enable **Syslog Facility Number**, and then enter the facility level number that the device will use when sending messages.

8. Click **Save**.

Note: You must enter a value in both the **Syslog Server Port** and **Syslog Facility Number** fields.

Configuring 802.1x Network Device Authentication

Prerequisites

An 802.1x authentication system requires the following components:

- PCoIP zero client with firmware 4.0.3 or newer
- PCoIP Management Console 1.8.1 or newer
- 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)
- View Connection Server
- A switch with 802.1x support configured

Procedure

Overview

Configuring 802.1x device authentication entails the following steps:

1. In the Windows 2008 server, create a client user.
2. In the Certificate Authority (CA) server, export the root CA certificate.
3. In the CA server, create a certificate template for client authentication.
4. From the CA Web Enrollment interface interface for the certificate server, issue the client certificate.
5. From the machine on which you issued the certificate, export the client certificate.
6. Using OpenSSL, convert the certificate format from .pfx to .pem.
7. In the Windows 2008 server, import the client certificate into the client user account.
8. From the MC or device's AWI, import the certificates.

Note: 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

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 > *<domain.local>* > Users**.

4. Right-click **Users**, select **New > User**, and then follow the wizard.

Export the Root CA Certificate

1. Log in to the Certificate Authority (CA) server.

2. Open a Microsoft Management Console window (e.g.,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 then **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 then 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 **OK.**

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 (e.g., "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**.

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 then 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 (i.e., "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

Note: 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://<*server*>/certsrv/** (e.g., "https://ca.domain.local/certsrv/").

2. Click **Request a certificate** and then **advanced certificate request**.

3. Click **Create and submit a request to this CA**.

4. At 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 (e.g., "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. *Important! 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*](#) *(e.g., "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 **Yes** at the pop-up window.

f. At the **Certificate Issued** window, click **Install this certificate**.

Export the Client Certificate

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (e.g., 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 **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 then 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 **OK**.

8. Repeat steps 5 to 7 again to export the 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.

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

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 then 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 *<client_cert>* 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 *<client_cert>* 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 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.

        In other words, make sure that all the text from **-----BEGIN PRIVATE KEY-----** to **-----END PRIVATE KEY** (including the dashes) in the original .pem file is replaced with the contents of -----**BEGIN RSA PRIVATE KEY** ----- to -----**END RSA PRIVATE KEY-----** (including the dashes) from the RSA .pem file

    c. Save the original .pem file and close it. The certificate is now ready to be uploaded to the zero client.

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 zero client.
5. Right-click the user, and then select **Name Mappings**.
6. In the **X.509 Certificates** section, click **Add**.
7. Locate and select the 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. Leave both identity boxes checked, click **OK**, and then click **OK** again.

Import the Certificates to Client Device

To import the certificates into a profile using the Management Console (MC):

1. From a browser, enter the IP address of the MC web page, and then log in to the MC.
2. From the **Profiles** tab, click **Add New**, and then enter a name for the new profile.

3. Click **Save** to save the profile.

4. Click **Set Properties** to edit the new profile's configuration.

5. In the **Certificate Store** category, click + to expand it, and then click **Add New**.

6. In the **Add Certificate to Store** dialog, click **Browse**, and then upload both the root CA certificate and the certificate with the private key.

7. For the zero client certificate, select **802.1X** from the drop-down list.

8. Expand the **Security Configuration** category, and then click **Edit Properties**.

9. Select **Enable 802.1x Security**, and then set the value to **True**.

10. Select **802.1x Authentication Identity**, enter the user name you have defined for the zero client, and then click **Save**.

11. Apply this profile to the desired group.

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the zero client or remote workstation card.

2. From the AWI menu, select **Upload > Certificate**.

3. Upload both the Root CA certificate and the certificate with the private key, using the **Browse** button to locate each certificate and the **Upload** button to upload them.

4. From the AWI menu, select **Configuration > Network**.

5. Select **Enable 802.1x Security**.

6. Click the **Choose** button 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:** (e.g., "zeroclient@mydomain.local").

Note: For the identity, your Windows server may be configured to use the certificate's **Subject**, the **Subject Alternative Name**, or another field. Please check with your administrator.

9. Click **Apply**, and then **Reset**.

For more information about 802.1x, please see the following Knowledge Base topics in the Teradici Support Site:

- Support for 802.1x on zero clients: KB 15134-590

- Setting up Windows Server 2008 R2 as an 802.1x authentication server: KB 15134-1245

- General 802.1x troubleshooting steps: KB 15134-928

Setting up a Touch Screen Display

These instructions explain how to install an Elo TouchSystems touch screen display, how to configure the firmware if you want the touch screen to be controlled by a driver running on the host, and how to set up auto-logon to bypass authentication when users are connecting to a host with a broker.

Installing the Touch Screen to the Zero Client

1. Plug in the touch screen's USB cable to the zero client's USB port.

2. Attach the monitor cable from the touch screen to any port on the zero client.

Note: You cannot attach multiple touch screens to the zero client, but you can attach a non-touch screen monitor to the zero client in addition to the touch screen as long as the touch screen is attached to the port on the zero client that is configured as the [primary port](#).

3. Plug in the power.

4. Disconnect the zero client session. This initiates the calibration on the touch screen.

Note: 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.

Setting up the Touch Screen as a Bridged Device

Note: 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.

1. Follow the steps in the previous procedure to install the touch screen to your zero client.

2. Log into the zero client AWI.

3. From the **Info** menu, click **Attached Devices**.

4. The touch screen details should appear in this page. Write down the **PID** and the **VID** information.

5. From the **Permissions** menu, click **USB** to display the **USB** page.

6. In the **Bridged Devices** area, click **Add New**.

7. Enter the Vendor ID and Product ID for the touch screen, and then click **Apply**.

8. Restart the zero client session.

9. Install the touch screen driver from Elo TouchSystems. See the Elo TouchSystems documentation for installation and calibration instructions.

Configuring the 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.

1. Log into the AWI for the 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 are using.

4. Enter the connection server's DNS name or IP address.

5. Fill out the user credentials, and then click **Apply**.

Configuring VLAN Tagging for Voice Traffic

VLAN tagging is a method for identifying Ethernet frames so they can be transmitted on a specific virtual LAN. Network administrators often use VLAN tagging to separate out Voice over IP (VoIP) traffic so it can be prioritized ahead of other traffic. This helps to keep latency and jitter to a minimum so call quality can be maintained even when the network is busy.

The zero client supports VLAN tagging for voice traffic when the device is used as a PCoIP caller endpoint for CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client. (For more information about this softphone client, see Zero Client–to–Bria Softphone Caller Endpoint.)

System Requirements for VLAN Tagging

A zero client will automatically tag voice traffic during a Bria Virtualized Edition softphone VoIP call if your system meets the following requirements:

- The zero client is enabled for DHCP (see Network Settings) so it can send requests to the DHCP server and receive responses from the server.
- The zero client is enabled for Unified Communications (UC) support.
- Your DHCP server supports option 60 (vendor class identifier) and option 43 (vendor-specific information).
- Your DHCP server is configured to provide a Voice VLAN ID value in option 43. The configuration for this vendor-specific option is shown in the figure below:

Option sub-code	Type	Name	Description	Example
4	UINT16 (Linux) / Word (Windows)	Voice VLAN ID	16-bit identifier for the Voice VLAN	1016

DHCP Option 43 – Voice VLAN ID Option

When the zero client receives a DHCP offer that contains a Voice VLAN ID value in option 43, it will tag VoIP data with this value and send the traffic out on a secondary interface using the same MAC address that it uses for traffic on its primary interface.

The zero client's secondary interface supports IPv4 only and cannot be accessed via the AWI. However, when this interface is used for voice traffic, the zero client's

event log will display the interface configuration, including its IP address, subnet mask, and default gateway. To see this information, search the event log for "**sec_if_**" entries, as shown in the sample search results below.

```
NOT FOUND:              sec_if_ip_address = 10.0.157.122
NOT FOUND:              sec_if_subnet_mask = 255.255.255.0
NOT FOUND:              sec_if_gateway = 10.0.157.1
NOT FOUND:              sec_if_ip_address = 10.0.157.122
NOT FOUND:              sec_if_primary_dns = 192.168.65.2
NOT FOUND:              sec_if_seconary_dns = 0.0.0.0
```

When Unified Communications support is enabled on the zero client, the event log will show "**UC Provider: 1**" for the **uc_options** entry, as shown below. When it is not enabled, it will show "**UC Provider: 0**".

```
IN FLASH:                          uc_options = UC Provider: 1
```

To see the VLAN tag, search for "**dhcp_get_pcoip_option43_vlan_id**". The following example shows a VLAN tag of **1157**.

```
MGMT_NET:        dhcp_get_pcoip_option43_vlan_id Voice VLAN is present ID =1157 (0x485)
```

Configuring DHCP Option 43

To configure a Windows 2008 DHCP server to send a Voice VLAN tag in option 43:

1. Open the DHCP Server console (**Administrative Tools > DHCP**).
2. Expand the tree for the server.
3. Right-click on **IPv4** and select **Define Vendor Classes**.
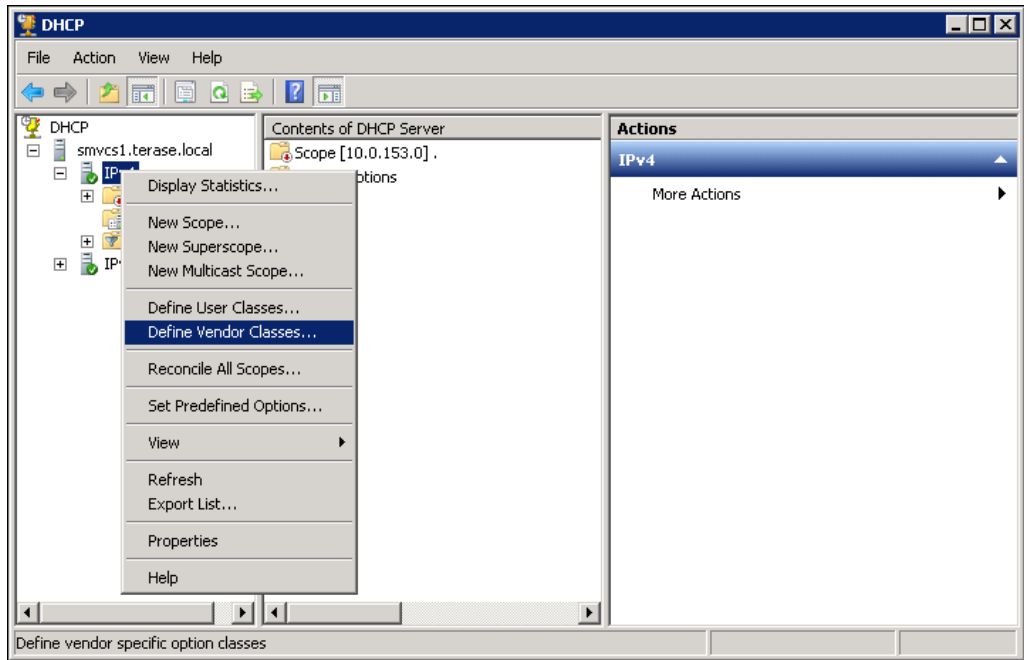
4. Check your DHCP vendor classes and choose one of the following:

- Your DHCP server may already have a **PCoIP Endpoint** vendor class— for example, if you have previously set up DHCP options to configure PCoIP devices with the address of the Management Console for device discovery. If the **PCoIP Endpoint** vendor class displays in the **Available classes** list, as shown below, close the **DHCP Vendor Classes** dialog and go to step 7.
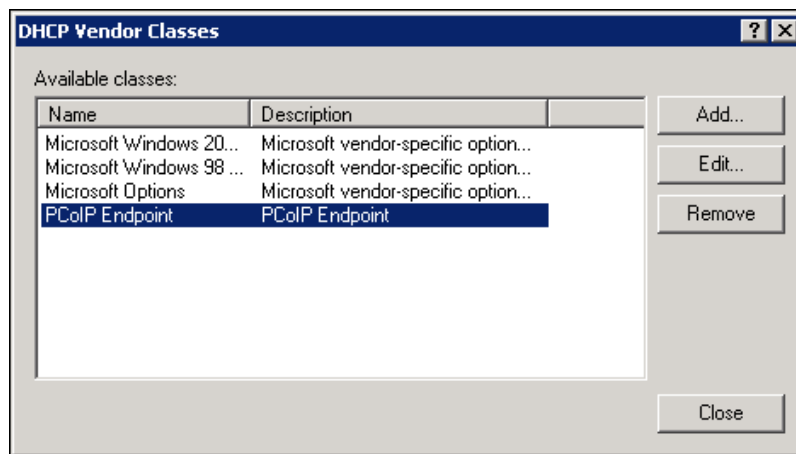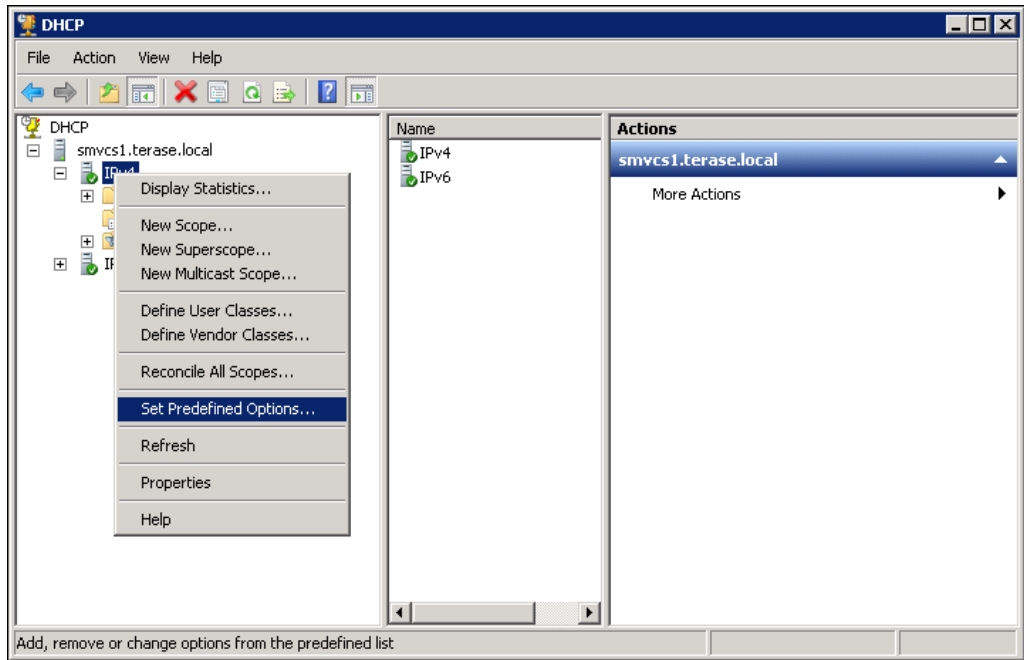
- If **PCoIP Endpoint** has not been added, click **Add** to add a new vendor class, and continue to the next step.
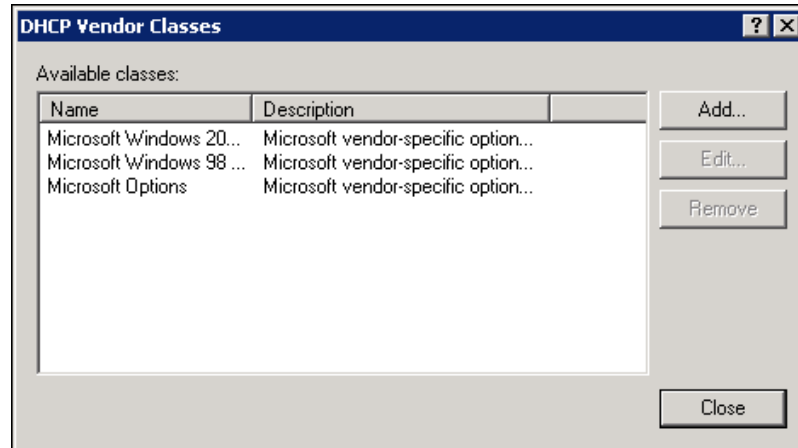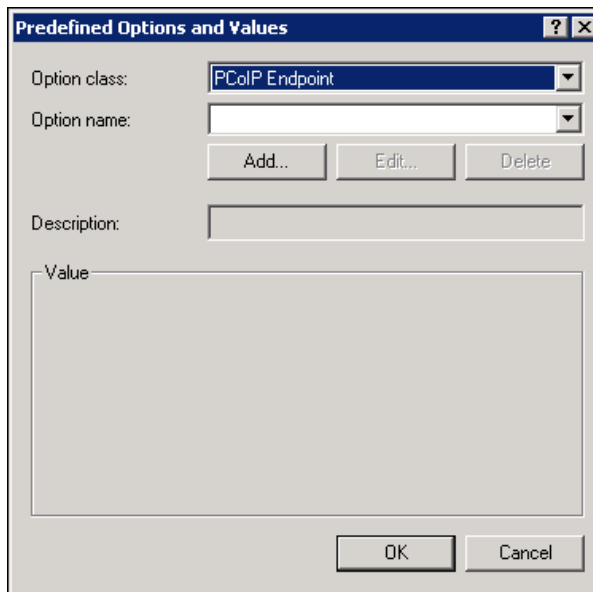

5. In the **Display name** field, enter **PCoIP Endpoint**, and add a description. Also add **PCoIP Endpoint** in the vendor ID **ASCII** column.
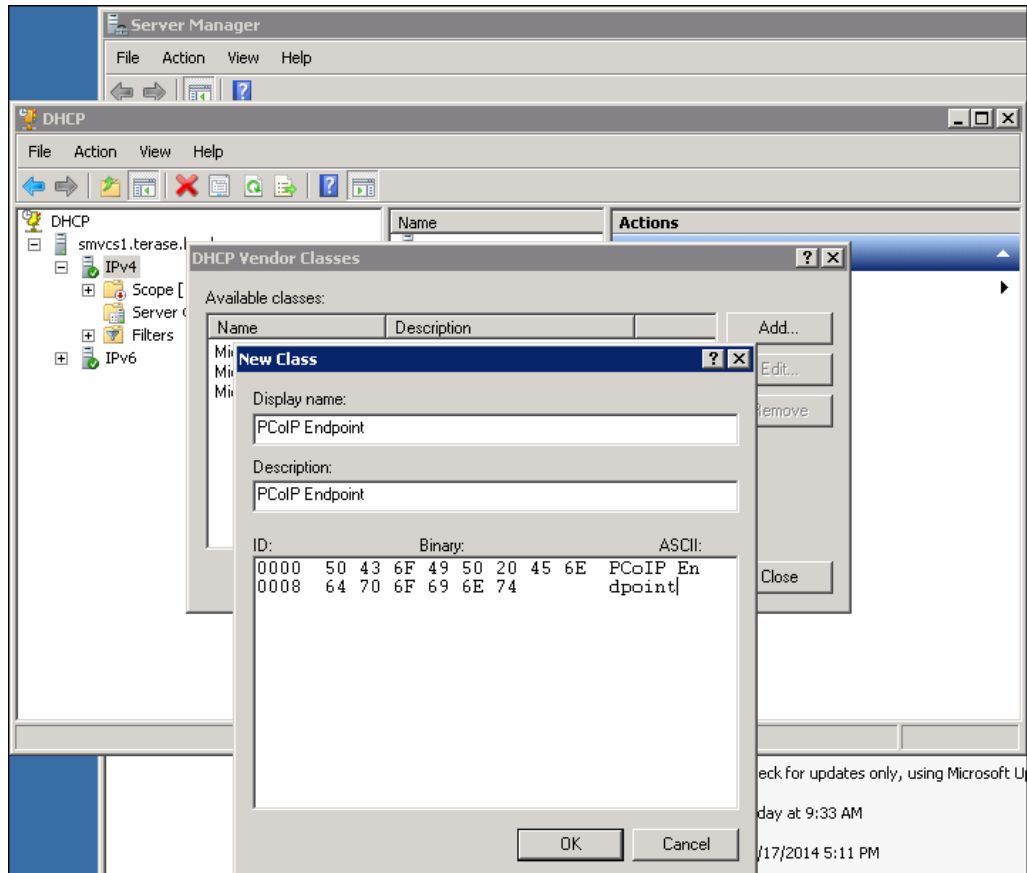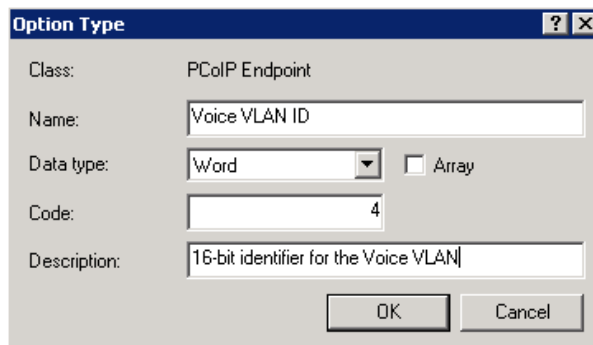
6. Click **OK** and then **Close**.

7. Right-click on **IPv4** in the tree and select **Set Predefined Options**.

8. In the **Option class** field, select **PCoIP Endpoint**, and then click **Add**.

9. In the **Option Type** dialog, enter the following information:

    a. Name: **Voice VLAN ID**

    b. Data type: **Word**

    c. Code: **4**

    d. Description: **16-bit identifier for the Voice VLAN**
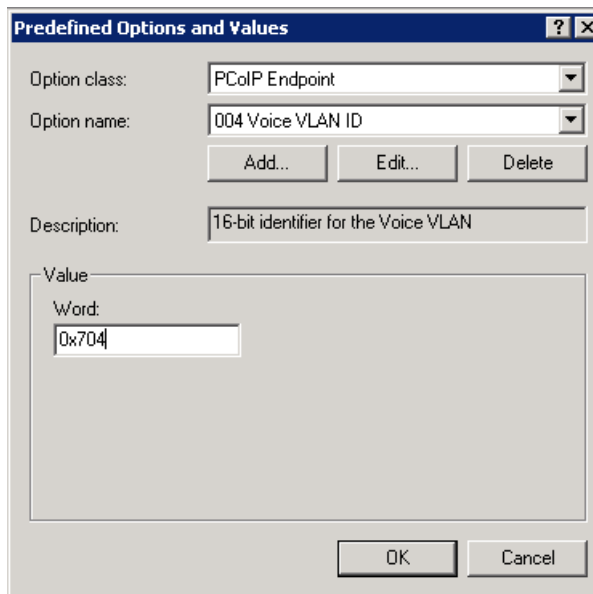
10. When you are finished, click **OK**.

11. In the **Value** field, enter a default value (in hexadecimal) for the Voice VLAN ID option.

12. If you want to set a different Voice VLAN ID value for a specific scope, expand the desired scope tree within your IPv4 tree.

13. Right-click on **Scope Options** and select **Configure Options**.
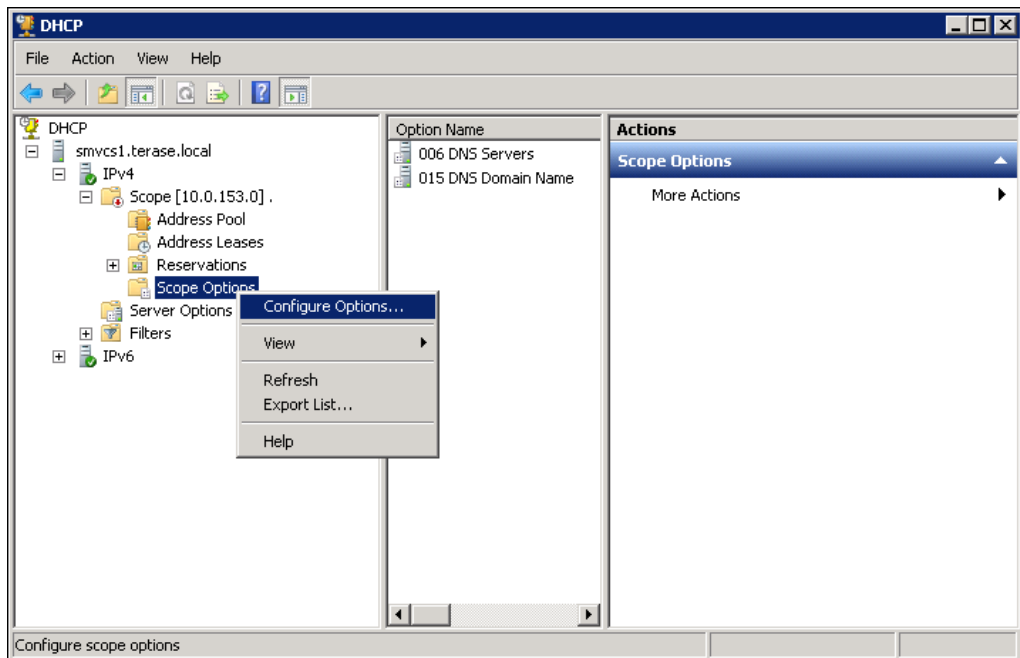
14. Click on the **Advanced** tab and select the **PCoIP Endpoint** vendor class.

15. Enable the check box for the **004 Voice VLAN ID** option, and then enter a value in the **Data entry** field. This value will apply only to your selected scope.
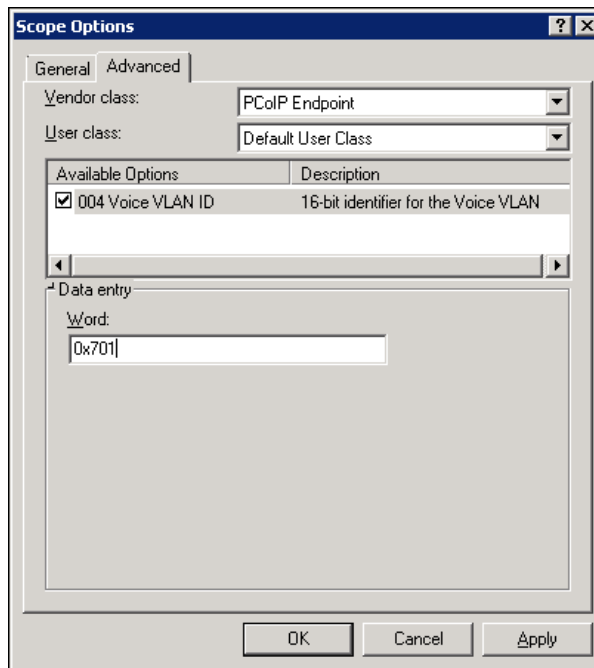
16. Click **OK**.

Technology Reference

PCoIP Connection Brokers

PCoIP connection brokers are resource managers that dynamically assign host PCs to zero clients based on the identity of the user establishing a connection from the zero client. Connection brokers are also used to allocate a pool of hosts to a group of zero clients. If the zero clients in a PCoIP deployment are configured to always connect to the same host (i.e., a static one-to-one pairing), then a connection broker is not required.

For connecting clients and hosts, a number of 3rd party connection brokers support the PCoIP technology. For more information, see KB 15134-24 in the Teradici Support Site.

For VDI implementations, the View Connection Server broker is used to connect zero clients to VMware Horizon virtual desktops. You can also use the View Connection Server broker to connect PCoIP clients and host PCs. For more information, see "Using PCoIP® Host Cards with VMware View" (TER0911004) in the Teradici Support Documentation Center.

DVI and DisplayPort Interfaces

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

- TERA2321 DVI-I dual-display PCoIP zero client: contains two DVI ports.
- TERA2321 DP+DVI-I dual-display PCoIP zero client: contains one DVI port and one DisplayPort port.
- TERA2140 DVI-D quad-display PCoIP zero client: contains four DVI ports.
- TERA2140 DP quad-display PCoIP zero client: contains four DisplayPort ports.

Support for 2560x1600 Display Resolution

All of the above 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 zero client to achieve 2560x1600 resolution on a connected display.
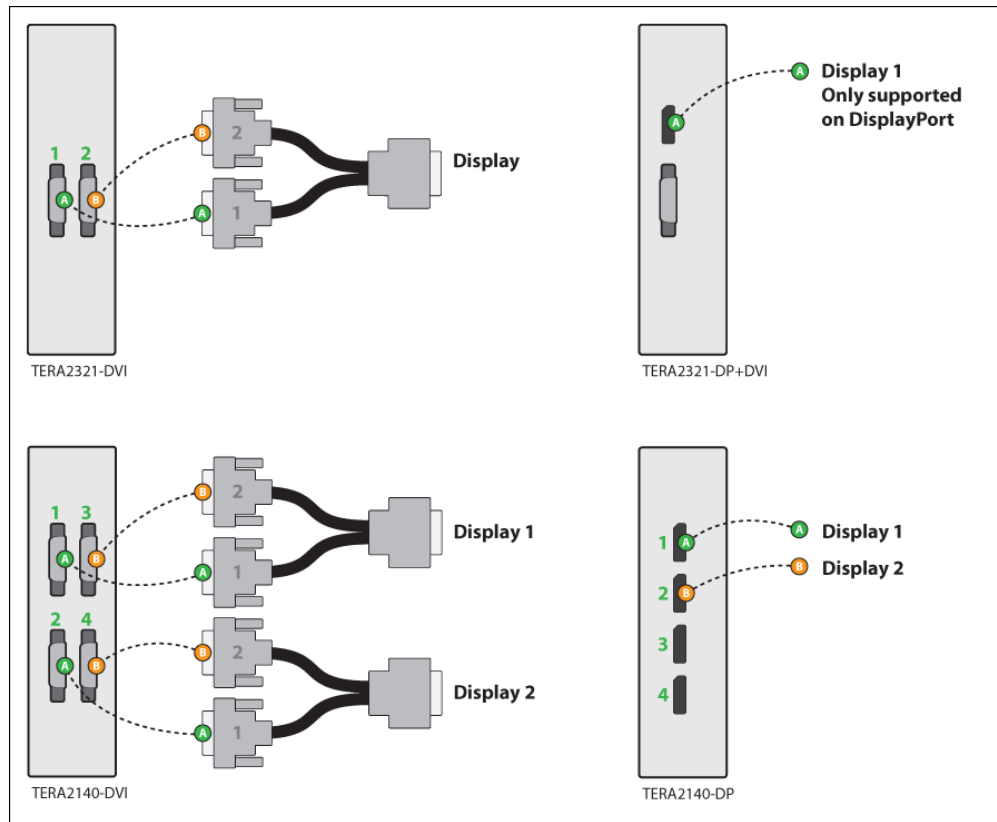
DVI and DisplayPort Connectors for 2560x1600 Resolution

- TERA2321 DVI-I dual-display PCoIP zero client: This 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 zero client, as shown in the above illustration (upper left).

- TERA2321 DP+DVI-I dual-display PCoIP zero client: This zero client supports one 2560x1600 monitor on the DisplayPort interface only. Connect the connector on a DisplayPort cable to the DisplayPort port on the zero client, as shown in the above illustration (upper right).

- TERA2140 DVI-D quad-display 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 above illustration (lower left). These connectors must be connected to ports on the client exactly as shown.

- TERA2140 DP quad-display PCoIP zero client: This zero client supports up to two 2560x1600 monitors. For each one, connect the connector on a DisplayPort cable to a DisplayPort port on the zero client, as shown in the above illustration (lower right).

Note: For details about other resolution options, see PCoIP Endpoints.

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, it allows the zero client to terminate input from the mouse and keyboard, and to draw the cursor on the attached display(s).

For more information about this feature and instructions on how to enable it, please see "PCoIP® Host Software for Windows User Guide" (TER1008001) in the Teradici Support Documentation Center.

Monitor Emulation

Teradici's monitor emulation feature for Tera1 and Tera2 remote workstation cards presents a generic display to ensure the boot process completes. It is intended to alleviate issues related to graphics cards that do not enable Display Port or DVI ports when no monitor is detected and/or do not honor hot plug events. These issues can occur during initial BIOS/OS boot or at some time after a full OS boot.

Enabling monitor emulation will provide the motherboard/GPU BIOS, OS, and GPU software driver a valid EDID. In general, the firmware will respond with the last connected monitor EDID when monitor emulation is enabled. If no display has been connected to a port since the device was factory programmed, a default EDID is used. The default monitor definitions shown below.

Monitor Name	TERA DEFAULT
Manufacturer ID	XXX
Monitor Serial Number	000000000000
Established Timing Supported	640x480 @ 60Hz (IBM,VGA) 800x600 @ 60Hz (VESA) 1024x768 @ 60Hz (VESA)
Standard Timing Supported	1280x1024 @60Hz
Native Resolution	1024x768 @60Hz
Monitor Range Limits Description	Min Vertical Freq – 50 Hz Max Vertical Freq – 75 Hz Min Horiz. Freq – 30 KHz Max Horiz. Freq – 82 KHz Pixel Clock – 140 MHz

EDID Revision	1.4

Note: This feature can be disabled to prevent GPUs from driving unwanted display outputs. When in session, the true hotplug/display state is only bridged from the client if the Teradici host agent is installed. This implies that a GPU may drive emulated ports with a video signal, even if the port on the client does not have an attached display.

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 then communicated in real time over an IP network to the user's PCoIP zero client.

For complete details about PCoIP Remote Workstation Cards, see the Teradici website at http://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 allow users to override settings or the **PCoIP Session Variables > Overridable Administrator Defaults** list to prevent users from overriding settings.

Note: 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, please see KB 15134-349 in the Teradici Support Site. For detailed information on each PCoIP session variable, see KB 15134-348.

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
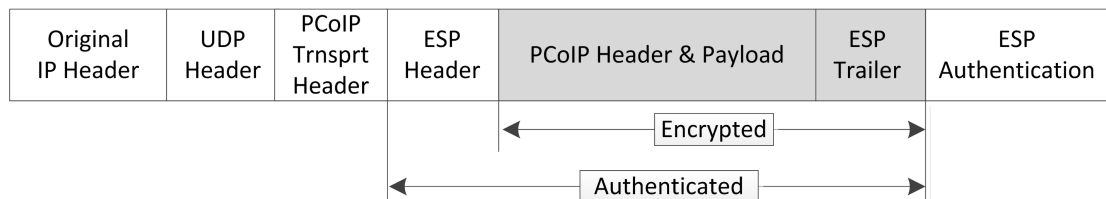
unencrypted PCoIP transport header field is also present for devices with firmware 4.1.0+ installed and/or for scenarios using View 5.1+. The PCoIP transport header allows network devices to make better QoS decisions for PCoIP traffic.

Note: 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 KB 15134-114 in the Teradici Support Site.

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 figure below. This figure also shows the location of the PCoIP transport header in a UDP-encapsulated ESP packet.

Original IP Header	UDP Header	PCoIP Trnsprt Header	ESP Header	PCoIP Header & Payload	ESP Trailer	ESP Authentication

UDP-encapsulated ESP Packet Format

IPsec ESP Packet Format

IPsec ESP encapsulation is the default packet format for direct connections that involve a Tera1 zero client and/or Tera1 remote workstation card.

The IPsec ESP packet format is illustrated in the figure below. This figure also shows the location of the PCoIP transport header in an IPsec ESP packet.

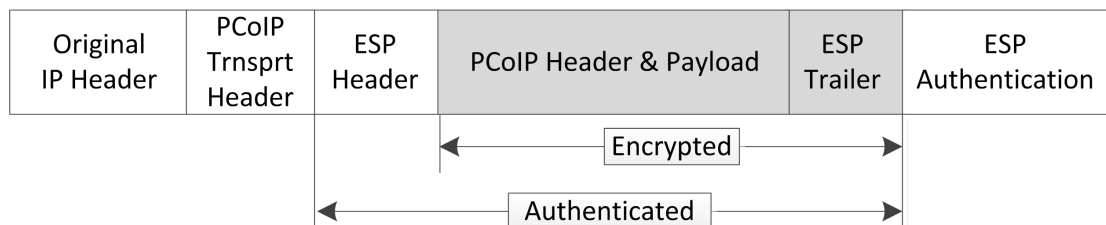| Original IP Header	PCoIP Trnsprt Header	ESP Header	PCoIP Header & Payload	ESP Trailer	ESP Authentication

IPsec ESP Packet Format

PCoIP Zero Clients

PCoIP zero clients are secure client endpoints that allow 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, zero clients provide a rich multi-media experience for users, who can interact with their desktops from any type of zero client, and even continue the same session as they move between zero client devices.

For complete details about PCoIP zero clients, see the Teradici website at http://www.teradici.com.

Requirements for Trusted Server Connections

When connecting a 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 Making a Trusted HTTPS Connection and Making an Untrusted HTTPS Connection for examples).

- **Closed padlock with green "https" text**: The connection is secured with HTTPS and the server's certificate is trusted by the 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 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 tables below show which requirements are necessary for each zero client certificate checking mode.

Note: If you use **Auto Detect** mode to connect, either the View Connection Server or PCoIP Connection Manager criteria are applied, depending on the server type.

View Connection Server Requirements

When connecting to a View Connection Server, the certificate requirements are as follows:

View Connection Server Certificate Requirements

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Valid according to computer clock (not expired and not valid only in the future).	Required	The certificate is accepted if the time is not valid but all other requirements are met. Warn the user before proceeding.	Not checked
Certificate subject or a subject alternative name must match the VCS address.	Required	Not required if the server certificate is self-signed. Warn the user before proceeding. Required for all CA-signed certificates.	Not checked
Certificate must have the serverAuth enhanced key usage.	Required	Required	Not checked
Certificate chain of trust must be rooted in device's local certificate store.	Required	Not required if the server certificate is self-signed. Warn the user before proceeding. Required for all CA-signed certificates.	Not checked
Certificate must not be revoked (checked using OCSP (Offensive Security Certified Professional) only if there is a OCSP responder address in the certificate).	Required	Required	Not checked

PCoIP Connection Manager Requirements

When connecting to a PCoIP Connection Manager, the certificate requirements are as follows:

PCoIP Connection Manager Certificate Requirements

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Valid according to computer clock (not expired and not valid only in the future).	Required	Required	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 Offensive Security Certified Professional (OSCP) only if there is a OCSP responder address in the certificate).	Required	Required	Not checked
RSA Key Length must be at least 1024 bits.	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, [zero clients](), and PCoIP Remote Workstation Cards. Using syslog for logging allows 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 allow 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 MC.

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.