

Tera2 PCoIP[®] Zero Client Firmware

Version 5.4

Administrators' Guide



TER1504003-5.4

Teradici Corporation

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

phone +1.604.451.5800 fax +1.604.451.5818

www.teradici.com



The information contained in this documentation represents the current view of Teradici Corporation as of the date of publication. Because Teradici must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Teradici, and Teradici cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. TERADICI MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Teradici Corporation.

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Visit <http://www.teradici.com/about-teradici/pat.php> for more information.

© 2004-2016 Teradici Corporation. All rights reserved.

Teradici, PC-over-IP, and PCoIP are trademarks of Teradici Corporation and may be registered in the United States and/or other countries. Any other trademarks or registered trademarks mentioned in this release are the intellectual property of their respective owners.

Contents

About This Guide	9
Conventions Used in This Guide	9
Who Should Read This Guide?	9
Understanding Terms Used in This Guide	9
Text Conventions	9
Notes Used in This Guide	11
Welcome	12
What's New	13
What's New in Firmware 5.4.0	13
Tera2 PCoIP Zero Client FAQs	14
What is a Tera2 PCoIP Zero Client?	14
How Do I Configure a Tera2 PCoIP Zero Client?	15
How Do I Find My Tera2 PCoIP Zero Client's IP Address?	15
How Do I Update the Tera2 PCoIP Zero Client Firmware?	15
What Hosts Can a Tera2 PCoIP Zero Client Connect To?	16
Do Tera2 PCoIP Zero Clients Work with the Bria Softphone Client?	16
What Devices Can I Attach to my Tera2 PCoIP Zero Client?	16
Configuration and Management Tools	17
About the PCoIP On-Screen Display	17
Connecting to a Session	18
Disconnecting from a Session	26
OSD Recovery Mode	28
About Overlay Windows	29
OSD Menus	31
About the PCoIP Administrative Web Interface	32
Logging into the Administrative Web Interface	33
AWI Initial Setup Page	34
AWI Home Page	34
AWI Recovery Mode	38
AWI Menus	40
Tera2 PCoIP Zero Client Connection Types	42
Connecting to PCoIP Remote Workstation Cards	42
Prerequisites	42
Configuration Options	43
Connection Instructions	45

Connecting to Teradici Cloud Access Software	46
Prerequisites	47
Configuration Options	47
Connection Instructions	47
Connecting to Amazon WorkSpaces Desktops	49
Prerequisites	49
Configuration Options	50
Connection Instructions	50
Connecting to VMware Horizon Desktops and Applications	52
Prerequisites	52
Supported Connection Types	52
Connection Instructions	53
GUI Reference	56
Initial Setup	56
AWI: Initial Setup	56
Configuring the Network	57
OSD: Network Settings	57
AWI: Network Settings	61
Configuring IPv6	64
OSD: IPv6 Settings	64
AWI: IPv6 Settings	66
Configuring Management Options	68
OSD: Management	68
AWI: Management	70
Configuring USB Settings	76
AWI: USB Settings	76
AWI: USB Permissions	77
Configuring Audio Settings	82
OSD: Audio Settings	82
AWI: Audio Settings	85
Configuring SCEP Settings	89
OSD: SCEP Settings	89
AWI: SCEP Settings	91
Configuring Label Settings	92
OSD: Label Settings	92
AWI: Label Settings	94
Configuring Access Settings	95
OSD: Access Settings	95

AWI: Access Settings	96
Configuring Device Discovery	98
OSD: Discovery Settings	98
AWI: Discovery Settings	99
Configuring SNMP Settings	101
AWI: SNMP Settings	101
Configuring a Session	102
Configuring a Session Connection Type	102
OSD: Auto Detect Session Settings	104
OSD: Direct to Host Session Settings	105
OSD: Direct to Host + SLP Host Discovery Session Settings	110
OSD: PCoIP Connection Manager Session Settings	114
OSD: PCoIP Connection Manager + Auto-Logon Session Settings	119
OSD: View Connection Server Session Settings	125
OSD: View Connection Server + Auto-Logon Session Settings	131
OSD: View Connection Server + Kiosk Session Settings	137
OSD: View Connection Server + Imprivata OneSign Session Settings	142
AWI: Auto Detect Session Settings	147
AWI: Direct to Host Session Settings	148
AWI: Direct to Host + SLP Host Discovery Session Settings	154
AWI: PCoIP Connection Manager Session Settings	158
AWI: PCoIP Connection Manager + Auto-Logon Session Settings	166
AWI: View Connection Server Session Settings	173
AWI: View Connection Server + Auto-Logon Session Settings	183
AWI: View Connection Server + Kiosk Session Settings	190
AWI: View Connection Server + Imprivata OneSign Session Settings	196
Configuring Session Bandwidth	204
AWI: Bandwidth Settings	204
Configuring Language	206
OSD: Help for Language Settings	206
AWI: Language Settings	206
Configuring Power Settings	207
OSD: Power Settings	207
AWI: Power Permissions	209
Configuring Image Quality	211
OSD: Help for Image Settings	211
AWI: Image Settings	211
Configuring Time Settings	214
OSD: Help for Time Settings	214

AWI: Time Settings	214
Configuring Unified Communications	216
AWI: Unified Communications	216
Configuring a Password	217
OSD: Password Settings	217
AWI: Password Settings	218
Configuring Reset Parameters	220
OSD: Reset Settings	220
AWI Client: Reset Settings	221
Performing Diagnostics	222
OSD: Event Log	222
OSD: Session Statistics	223
OSD: PCoIP Processor	224
OSD: Ping	225
AWI: Event Log	226
AWI: Session Control	230
AWI: Session Statistics	231
AWI: Audio Test	233
AWI: Display Test	234
AWI: PCoIP Processor	235
AWI: Packet Capture	235
Viewing Information	237
OSD: Version	237
OSD: Network	239
AWI: Version	239
AWI: Attached Devices	241
Uploading Files	242
AWI: Firmware Upload	242
AWI: OSD Logo	243
AWI: Certificate Upload	244
Configuring a Display Override	246
OSD: EDID Override Settings (Dual)	246
OSD: EDID Override Settings (Quad)	249
Configuring OSD User Settings	253
OSD: Certificate Checking Mode Settings	253
OSD: Mouse Settings	254
OSD: Keyboard Settings	255
OSD: Image Settings	257
OSD: Display Topology Settings (Dual)	258

OSD: Display Topology Settings (Quad)	261
OSD: Touch Screen Settings	264
OSD: Tablet Settings	266
OSD: Region Settings	269
How To Topics	271
How to Assign an IP Address to a Tera2 PCoIP Zero Client	271
Dynamic Assignment	271
Static Assignment	272
How to Display Processor Information	273
How to Upload Firmware to a Tera2 PCoIP Zero Client	275
How to Upload a Certificate to a Tera2 PCoIP Zero Client	276
How to Troubleshoot a Tera2 PCoIP Zero Client in Recovery Mode	276
How to Configure an Endpoint Manager	277
Automatic Discovery via DHCP or DNS Server Provisioning	277
Manual Discovery Initiated by an Endpoint Manager	278
Configuring a Tera2 PCoIP Zero Client with an Endpoint Manager	279
How to Configure VLAN Tagging for Voice Traffic	280
System Requirements for VLAN Tagging	280
Configuring DHCP Option 43	281
How to Set up a Touch Screen Display	288
Installing the Touch Screen to the Zero Client	288
Setting up the Touch Screen as a Bridged Device	289
Configuring the Zero Client to Automatically Log into a Host Brokered by a Connection Manager	290
How to Configure a PCoIP Zero Client as a Bria Softphone Endpoint	291
How to Configure 802.1x Network Device Authentication	292
Prerequisites	292
Procedure	292
How to Configure Syslog Settings	297
Setting up Syslog from the AWI	298
Security	299
Configuring Security Settings	299
AWI 802.1x Settings	299
AWI Management Settings	299
Encryption Settings	300
When a Zero Client is Used as a Server	300
When a Zero Client is Used as a Client	301

Failed Login Attempt Message	304
Technology Reference	305
DVI and DisplayPort Interfaces	305
Support for 2560x1600 Display Resolution	305
Local Cursor and Keyboard	307
Remote Workstation Cards	307
Teradici Cloud Access Platform	307
PCoIP Software Session Variables	307
PCoIP Packet Format	308
UDP-encapsulated ESP Packet Format	308
IPsec ESP Packet Format	309
Tera2 PCoIP Zero Clients	309
Requirements for Trusted Server Connections	309
View Connection Server Requirements	310
PCoIP Connection Manager Requirements	311
Syslog	312
Teradici PCoIP Hardware Accelerator (APEX 2800)	312

About This Guide

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

Conventions Used in This Guide

This section describes the visual conventions used in this guide.

Who Should Read This Guide?

This guide is for administrators who are configuring Tera2 PCoIP® Zero Client firmware for release 5.0 and later.

Understanding Terms Used in This Guide

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 clarify many of the terms you'll encounter, 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>.

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.
<i>Italic text</i>	Used to indicate the following conventions: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • \Program Files (x86)\Teradici\PCoIP Agent • /etc/pcoipagent/pcoip-agent.conf
Red Monospace Text	Indicates code fragments, keys, variables, and parameters. Examples: <ul style="list-style-type: none"> • This is the HTML5 <code><code></code> element. • Set the <code>pcoip.event_filter_mode</code> variable.
Inverse Monospace text	Used to indicate keyboard buttons, like <code>Ctrl</code> or <code>Shift</code> .

Formatted text

Used to indicate code blocks, including command line interactions.

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.



Info

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



Related

These notes contain links to resources found outside this guide. Examples include links to other documents, third-party websites, and software downloads.

Welcome

Welcome to Teradici's Tera2 PCoIP® Zero Client Administrators' Guide. This documentation explains how to configure Tera2 PCoIP Zero Client firmware for release 5.0 and later.

To get started, see the following topics:

- For information about Tera2 PCoIP Zero Clients, see [PCoIP Zero Client FAQs](#).
- For details about configuration tools, see [About the OSD](#) and [About the AWI](#).
- For information about how to connect Tera2 PCoIP Zero Clients to host endpoints, see [Connecting PCoIP Zero Clients](#).
- For details about each Tera2 PCoIP Zero Client configuration page, see [Using the GUI Reference](#).
- For some specific 'how to' topics, see [Common Tasks](#).

What's New

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

This guide documents Tera2 PCoIP Zero Client firmware only.

For help configuring firmware 4.x for Tera1 and Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards, or for help configuring 1.10.x Management Console firmware profiles for clients and hosts, see [Tera2 PCoIP Zero Client Firmware 4.x and Remote Workstation Card Firmware 4.9 Administrators' Guide](#).

What's New in Firmware 5.4.0

This release contains the following Tera2 PCoIP Zero Client features:

Firmware 5.4.0 Release Features

Key Release Details	Platform
Added support for the OMNIKEY 5127-mini when used in Imprivata OneSign environments.	VDI
<p>The Enhanced BasicCard, Payflex, and Open Platform smart cards can be used for single sign-on authentication. The smart cards can be used with the Gemalto IDBridge CT30 and Rocketek RT-SCR1 card readers when the connection is brokered by a PCoIP Broker Protocol-compliant broker with Teradici Cloud Access Software or Teradici Cloud Access Platform hosts.</p>	

Tera2 PCoIP Zero Client FAQs

This section addresses the following:

- What is a Tera2 PCoIP Zero Client?
- How do I physically set up a Tera2 PCoIP Zero Client?
- How do I configure a Tera2 PCoIP Zero Client?
- How do I find my Tera2 PCoIP Zero Client’s IP address?
- How do I update Tera2 PCoIP Zero Client firmware?
- What hosts can a Tera2 PCoIP Zero Client connect to?
- Do Tera2 PCoIP Zero Clients work with the Bria softphone client?
- What devices can I attach to a Tera2 PCoIP Zero Client?

What is a Tera2 PCoIP Zero Client?

Tera2 PCoIP Zero Clients are hardware- and firmware-based endpoints that enable users to connect remotely to PCoIP Remote Workstations, workstations running Teradici Cloud Access Software, Teradici Cloud Access Platform desktops and workstations, Amazon WorkSpaces desktops, and VMware Horizon and VMware Horizon DaaS virtual desktops. Because they do not have general purpose CPUs, local data storage, or application operating systems, Tera2 PCoIP Zero Clients are ultra secure and easy to manage. Tera2 PCoIP Zero Clients contain upgradable firmware that enables you to customize your client with various features.

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

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

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

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

*Tera2 PCoIP Zero Clients support 2560x1600 resolution on attached displays using either DVI (with Y-cable) or DisplayPort interfaces. For instructions on how to connect cables to Tera2 PCoIP Zero Clients with DVI and/or DisplayPort ports to support this resolution, see [DVI and DisplayPort Interfaces](#).

Advanced Encryption Standard (AES) is employed for PCoIP session encryption. Tera2 PCoIP Zero Clients support both AES-128-GCM and AES-256-GCM encryption. For more information, see [Encryption Settings](#).

**Resource: Physically Setting Up a Tera2 PCoIP Zero Client**

For detailed instructions on how to physically set up a Tera2 PCoIP Zero Client and connect it to USB devices, monitors, and a network, see the [PCoIP® Tera2 Zero Client Quick Start Guide](#). This guide has detailed instructions for each step of the installation process.

How Do I Configure a Tera2 PCoIP Zero Client?

The following configuration and management tools are available for Tera2 PCoIP Zero Clients:

- **On-Screen Display (OSD):** The Tera2 PCoIP Zero Client's pre-session built-in interface for configuring the device's firmware.
- **Administrative Web Interface (AWI):** A web-based interface for configuring a specific Tera2 PCoIP Zero Client's firmware remotely after typing the client's IP address into the browser's address bar.
- **Teradici zero client management software:** A management tool for configuring and managing multiple PCoIP Zero Clients remotely. Teradici's management software is the PCoIP Management Console. For information about the PCoIP Management Console, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

How Do I Find My Tera2 PCoIP Zero Client's IP Address?

The Tera2 PCoIP Zero Client's address displays in the **IP Address** field when you select **Options > Information > Network** or **Options > Configuration > Network** from the client's OSD.

For more information, see [How to Assign an IP Address to a PCoIP Zero Client](#).

How Do I Update the Tera2 PCoIP Zero Client Firmware?

The firmware version that is currently installed in your Tera2 PCoIP Zero Client displays in the **Firmware Version** field when you select **Options > Information** from the client's OSD or **Info > Version** from the client's AWI. For instructions on how to upload a different firmware release version, see [How to Upload Firmware to a PCoIP Zero Client](#).

What Hosts Can a Tera2 PCoIP Zero Client Connect To?

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

- [PCoIP Remote Workstation Cards](#)
- [Teradici Cloud Access Software](#)
- [Teradici Cloud Access Platform desktops and workstations](#)
- [Amazon WorkSpaces Desktops](#)
- [VMware Horizon Desktops](#)

Do Tera2 PCoIP Zero Clients Work with the Bria Softphone Client?

The Tera2 PCoIP Zero Client supports interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on [Bria softphone caller endpoints](#), such as [Teradici Cloud Access Platform desktops and workstations](#), [VMware Horizon desktops](#), and [Amazon WorkSpaces desktops](#). See [How to Configure a PCoIP Zero Client as a Bria Softphone Endpoint](#) for details.

What Devices Can I Attach to my Tera2 PCoIP Zero Client?

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

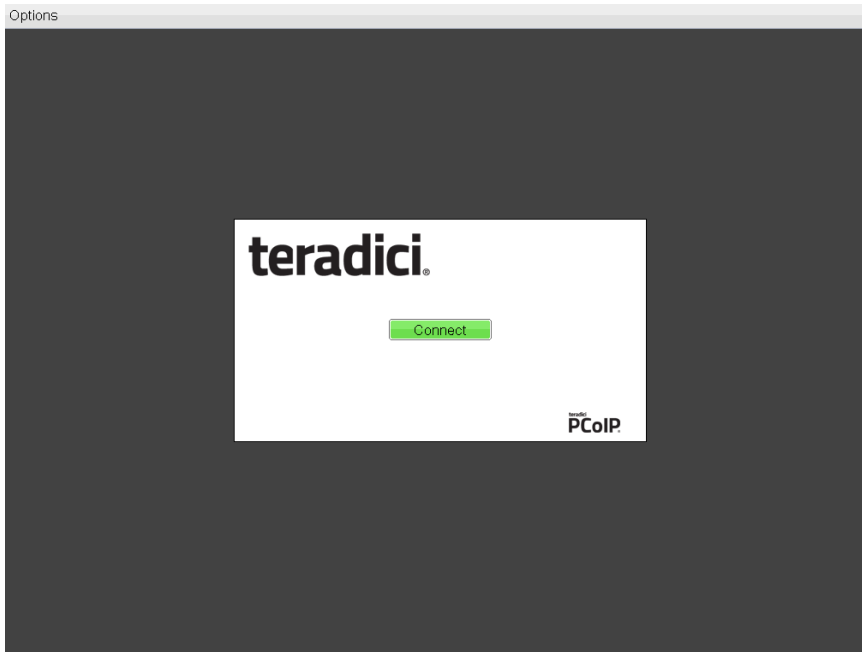
Configuration and Management Tools

This section explains some of the configuration and management tools available. These include the:

- PCoIP On-Screen Display, which enables users to create a PCoIP session between the client and a remote resource.
- On-Screen Display Recovery mode, which is a special version of the Tera2 PCoIP Zero Client firmware that takes effect when the client experiences a problem that renders it unable to operate.
- Overlay windows, which occasionally appear on top of the user's PCoIP session to display pertinent information when the status changes—for example, when the network connection is lost or an unauthorized USB device is plugged in.
- On-Screen Display menus that link to OSD configuration, information, and status pages.
- PCoIP Administrative Web Interface (AWI) that enables you to interact remotely with a PCoIP endpoint.
- AWI Recovery Mode Recovery mode, which is a special version of the Tera2 PCoIP Zero Client firmware that takes effect when the client experiences a problem that renders it unable to operate.
- AWI menus that link to different configuration and status pages.

About the PCoIP On-Screen Display

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



OSD main window

An **Options** menu 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 PCoIP Remote Workstation Card.

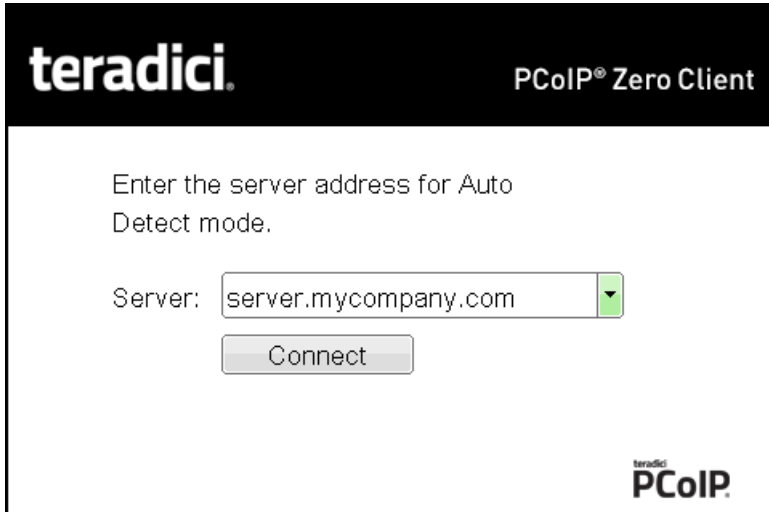
Connecting to a Session

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

Connecting to a Session from the Connect Window

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

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



OSD Auto Detect window



OSD Direct to Host connect window

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

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

Connecting to a Session Using Smart Cards

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

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

For more information about the supported smart cards and USB smart card readers you can use with a PCoIP Connection Manager, see [Supported Smart Cards and USB Smart Card Readers for Tera2 PCoIP Zero Clients \(KB 15134-3060\)](#). For more information about the

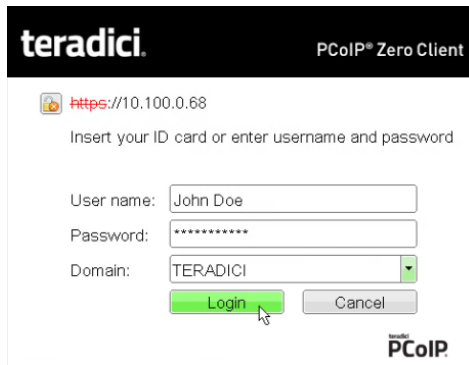
requirements to support pre-session smart card authentication with VMware View virtual desktops, see [What are the requirements to support pre-session smart card authentication? \(KB 15134-299\)](#).

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

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

To connect to a session using a smart card:

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



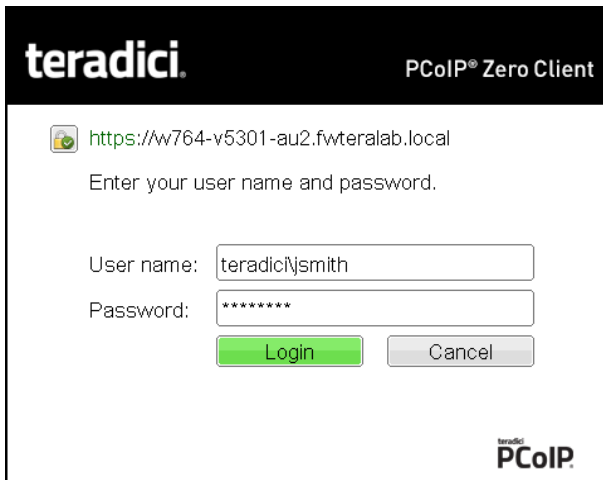
2. If required, type your credentials.

Making a Trusted HTTPS Connection

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

If the correct trusted SSL root certificate for the server has been installed in the Tera2 PCoIP Zero Client and all other certificate requirements are met for the configured certificate checking mode (see [Requirements for Trusted Server Connections on page 309](#)), the icon at the top of this page shows a closed padlock symbol with a green check mark, and the 'https' in the server's URI also displays in green text.

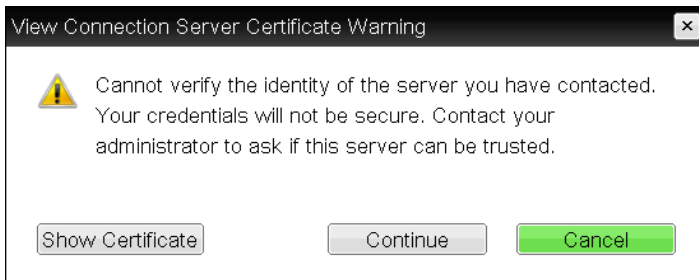
The following image shows the user authentication screen when the Tera2 PCoIP Zero Client trusts the server's certificate. When connecting to other host types, such as VMware Horizon and Amazon WorkSpaces, you will see a similar authentication screen.



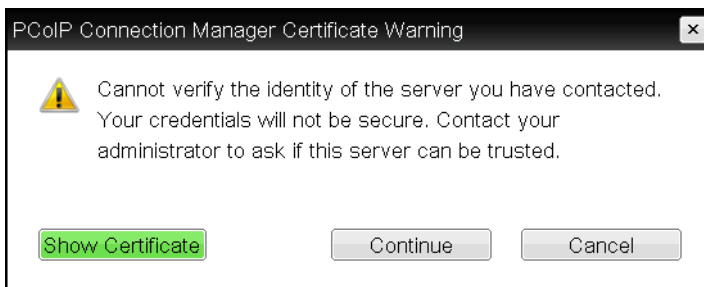
Tera2 PCoIP Zero Client trusted HTTPS connection

Making an Untrusted HTTPS Connection

If the correct trusted SSL root certificate for a connection server has not been installed in the Tera2 PCoIP Zero Client, or if other certificate requirements are not met (see [Requirements for Trusted Server Connections on page 309](#)), a warning such as the following appears if your Tera2 PCoIP Zero Client is configured to warn before connecting to untrusted servers.

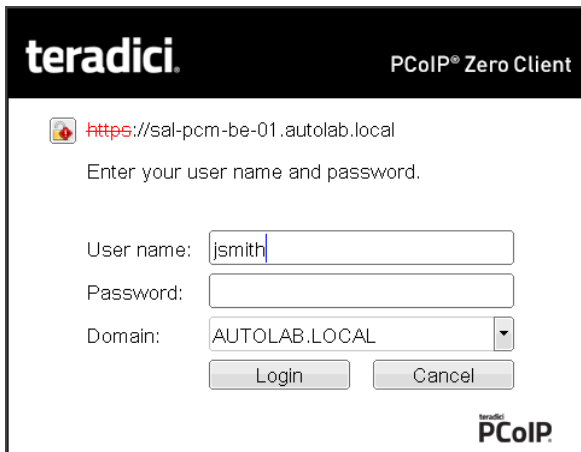


View Connection Server Certificate Warning



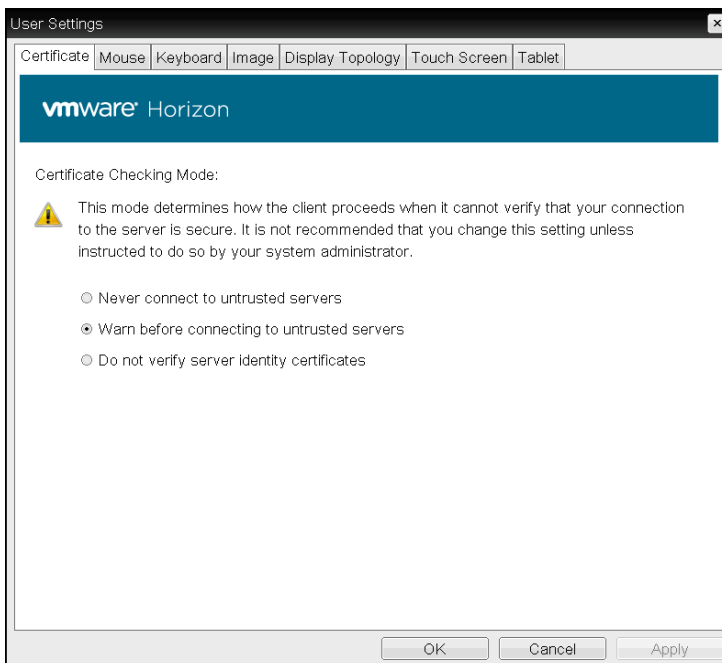
PCoIP Connection Manager Certificate Warning

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

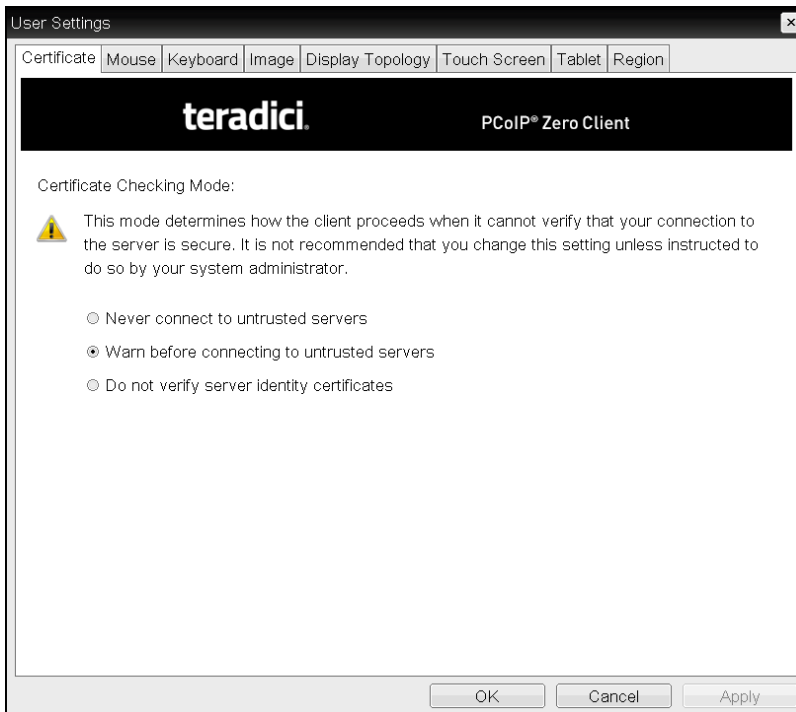


Tera2 PCoIP Zero Client untrusted HTTPS connection

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



VMware Horizon Certificate Checking Mode page

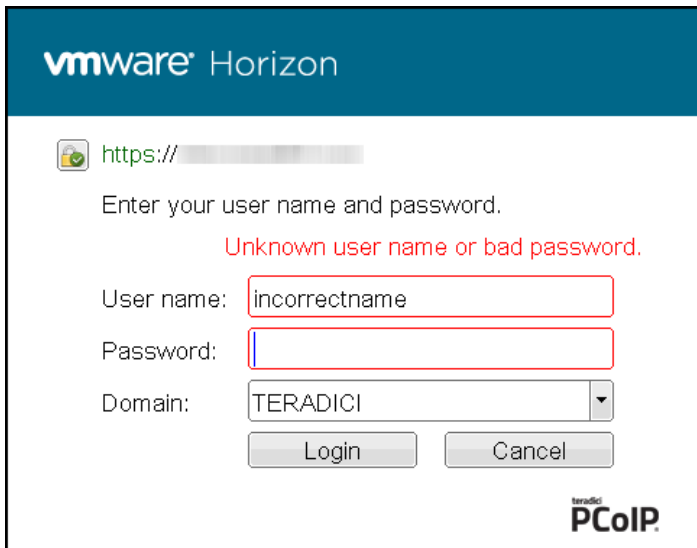


Teradici Certificate Checking Mode

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

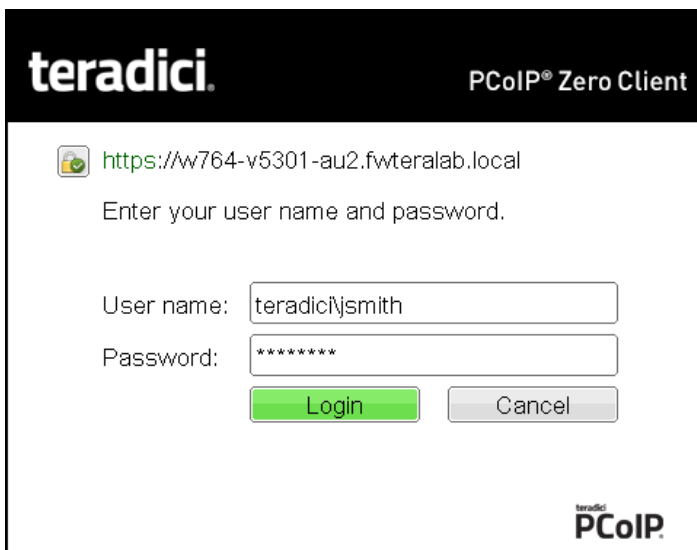
Authenticating the User

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

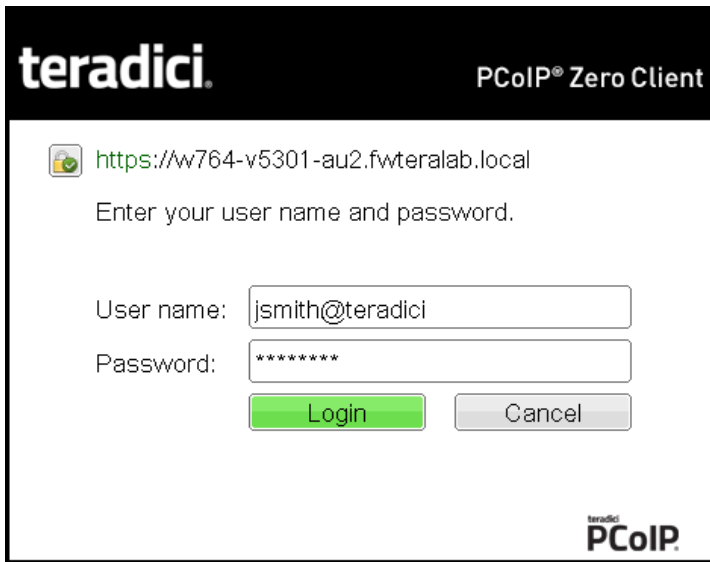


Unknown user name or password

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



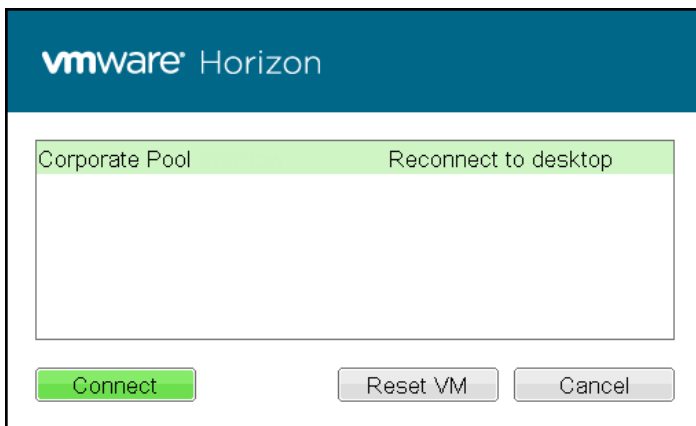
Tera2 PCoIP Zero Client with domain field hidden



Tera2 PCoIP Zero Client with domain field hidden

Connecting to a Desktop

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

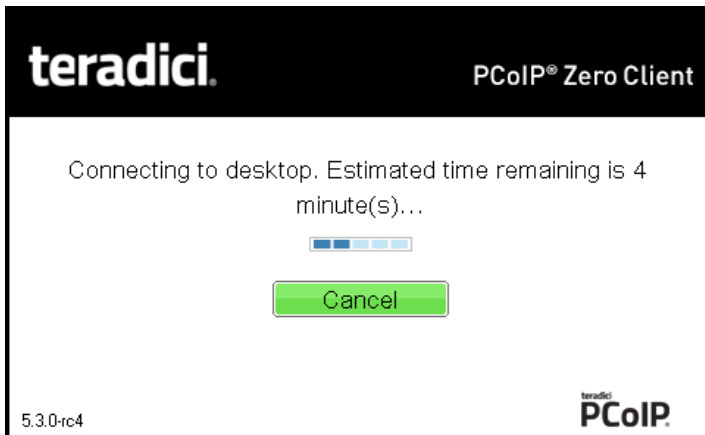


Selecting an entitlement

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

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

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



Notification with estimated length of time before connecting



Related: Uploading certificates to a single device

For information on how to upload certificates to a single device using the AWI, see [AWI: Certificate Upload on page 244](#).

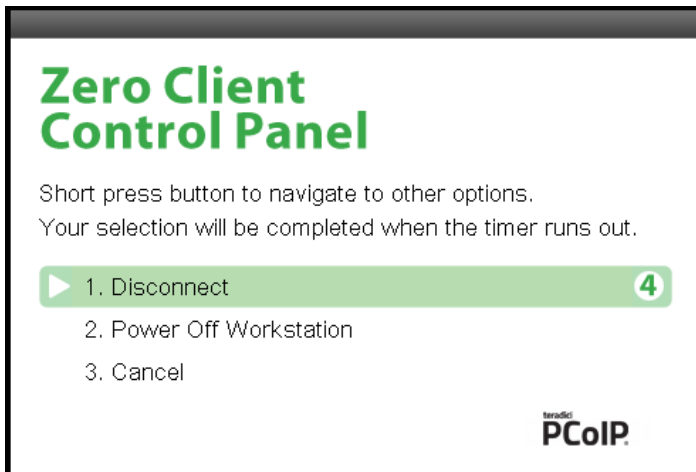


Related: OSD messages on startup or after a session has been established

For information on other OSD messages that may appear on top of a user's session during startup or after a session has been established, see [About Overlay Windows on page 29](#).

Disconnecting from a Session

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



Zero Client Control Panel

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

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

During a session, 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 (that is, not bridged).



Note: Selecting the disconnect option

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

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

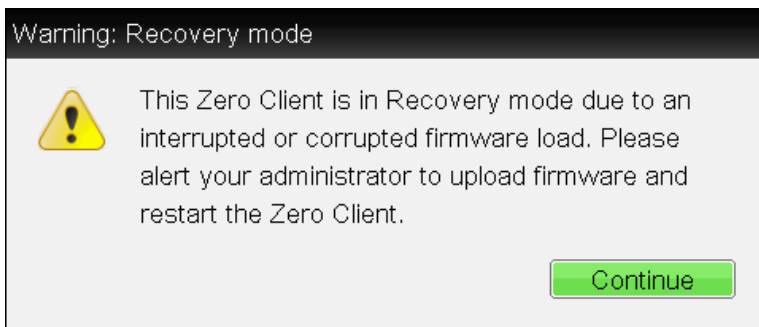
OSD Recovery Mode

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

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

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

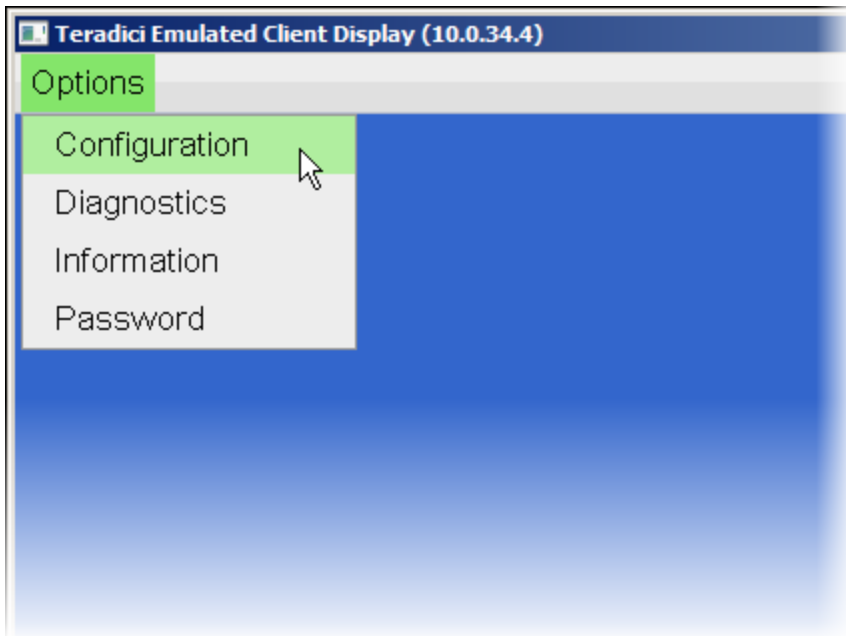
When the client is in recovery mode, the OSD screen displays the following initial screen:



OSD recovery mode

OSD Recovery Mode Options

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



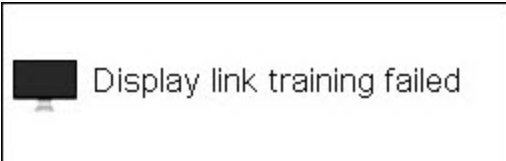
OSD recovery mode available options







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

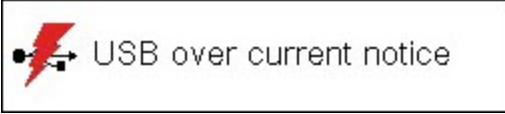
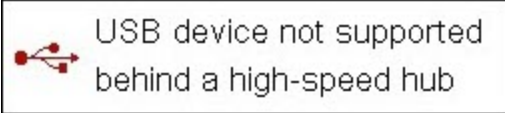
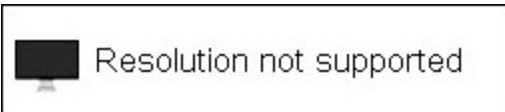


See also: [How to Troubleshoot a Tera2 PCoIP Zero Client in Recovery Mode on page 276](#).

About Overlay Windows

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

Overlay window	Description
 <p data-bbox="240 1766 578 1793">Display link training failed overlay</p>	<p data-bbox="792 1600 1398 1818">This overlay only displays on Tera2 clients that contain DisplayPort display interfaces (as opposed to DVI interfaces). The DisplayPort protocol requires a link training sequence for adapting to differing cable lengths and signal qualities. If this training does not succeed, this overlay appears with the message <i>Display link training failed</i>.</p>

Overlay window	Description
 <p>Half-duplex network connection</p> <p>Half duplex overlay</p>	<p>PCoIP technology is not compatible with half-duplex network connections. When a half-duplex connection is detected, this overlay appears with the message <i>Half-duplex network connection</i>.</p>
 <p>Network connection lost</p> <p>Network connection lost overlay</p>	<p>Loss of network connectivity is indicated using an overlay with the message <i>Network connection lost</i> over the most recent screen data. This overlay appears when the client network cable is disconnected or when no PCoIP protocol traffic is received by the client for more than two seconds.</p> <p>The lost network connection message appears until the network is restored or the timeout expires (and the PCoIP session ends).</p> <div data-bbox="792 821 889 919" style="background-color: #4CAF50; color: white; padding: 5px; display: inline-block; margin-bottom: 5px;">  </div> <p>Tip: Consider disabling this notification message in sessions to virtual desktops</p> <p>It is not recommended to use this notification message when using PCoIP devices with virtual desktops. Normal scheduling within the virtual desktop hypervisor can falsely trigger this message. To prevent this problem, you can disable the Enable Peer Loss Overlay setting.</p>
 <p>No support resolutions found. Please try unplugging other displays.</p> <p>No support resolutions found overlay</p>	<p>Display resolution may have limitations due to resource constraints when all four ports have large displays connected. If the resolution limit is exceeded, this overlay appears with the message <i>No support resolutions found. Please Try unplugging other displays</i>.</p>
 <p>Preparing desktop...</p> <p>Preparing desktop overlay</p>	<p>When a user first logs into a PCoIP session, this overlay appears with the message <i>Preparing desktop...</i></p>
 <p>USB device not authorized</p> <p>USB device not authorized overlay</p>	<p>If an unauthorized USB device is connected, this overlay appears with the message <i>USB device not authorized</i>. This overlay lasts for approximately five seconds.</p>

Overlay window	Description
 <p>USB over current notice overlay</p>	<p>If the USB devices connected to the client cannot be handled by the USB ports, this overlay appears with the message <i>USB over current notice</i>. This overlay remains until USB devices are removed to meet the current handling of the USB ports.</p>
 <p>USB device not supported behind a high-speed hub overlay</p>	<p>Some USB devices cannot be connected through a high speed (USB 2.0) hub, and should instead be connected directly to the Tera2 PCoIP Zero Client or through a full speed (USB 1.1) hub. If such a device is connected to the Tera2 PCoIP Zero Client through a high speed hub, this overlay appears with the message <i>USB device not supported behind high speed hub</i>. This overlay lasts for approximately five seconds.</p>
 <p>Resolution not supported overlay</p>	<p>If the resolution of a monitor connected to the client cannot be supported by the host, the monitor is set to its default resolution and this overlay appears with the message <i>Resolution not supported</i>.</p>
<p>Video Source Overlays Improper connection of the host video source is denoted by two possible overlays, as shown next. These overlays appear for approximately five minutes. The monitor is put into sleep mode approximately 15 seconds after they appear.</p>	
 <p>No source signal overlay</p>	<p>When no video source is connected to the host, this overlay appears with the message <i>No source signal</i>. This helps you debug a situation where the host does not have the video source connected or the host PC has stopped driving a video signal. To correct this, connect the host PC video to the host. (This message can also be triggered by the host going into display power save mode.)</p>
 <p>Source signal on other port overlay</p>	<p>When a video source to the host does not correspond to the video port used on the client, this overlay appears with the message <i>Source signal on other port</i>. This helps you debug a situation where the video source is connected to the wrong port. To correct this, swap the video ports at the host or the client.</p>

OSD Menus

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

- **Configuration:** This menu contains links to pages that let you define how the device operates and interacts with its environment. Each tab has an **OK**, **Cancel**, and **Apply**

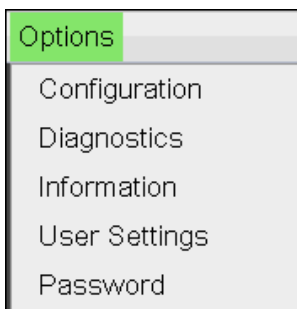
button that lets you accept or cancel the settings changes made.

- **Diagnostics:** This menu contains links to pages that help diagnose issues concerning the client.
- **Information:** The page under this menu displays hardware and firmware version information about the device and the client's IP address.
- **User Settings:** This menu contains links to pages that let users define mouse, keyboard, image, display topology, touch screen, tablet, and region settings, and also the certificate checking mode.
- **Password:** The page under this menu lets you update the administrative password for the device.



Note: Password option appears when password protection is enabled

The **Password** menu option is only present in the OSD for devices that are configured with password protection enabled. If this option is not visible in the **Options** menu, you can make it visible by using a PCoIP Management Console profile to enable password protection for the device. You can also use a PCoIP Management Console profile to hide a single menu item, the entire **Options** menu, or all menus from users. For details, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).



OSD Options menu

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

About the PCoIP Administrative Web Interface

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

After you type the device's IP address into an Internet Explorer, Mozilla Firefox, or Google Chrome browser, the browser will use HTTPS to connect to the device's AWI web page.

Access to the AWI is controlled using an administrative password, which can be optionally disabled.

The AWI's HTTPS connection is secured using a PCoIP root Certificate Authority (CA) certificate. To avoid warning messages when you log into the AWI, it is recommended that you install this certificate in your browser. The certificate file (cacert.pem) is always included in a firmware release, but you can also download it directly from [How do I install the PCoIP Root Certificate in my Browser for secure access the Administrative Web Interface? \(KB 15134-529\)](#). Detailed instructions on how to install the certificate are also included in the KB.

The following browsers are supported in this release:

- Firefox: current version
- Chrome: current version
- Microsoft Edge: current version
- Internet Explorer 11

Logging into the Administrative Web Interface

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

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



Note: Contact your reseller for your device's AWI password

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

Log In

Please enter the administrative password to access this device.

Password:

Idle Timeout: Never ▼

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 PCoIP devices do not require a password to log in**

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

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

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

AWI Initial Setup Page


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

**Note: Complex environments require further configuration**

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

AWI Home Page

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



PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

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

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

PCoIP Packets (Sent/Received/Lost): 1108849 / 983422 / 547 (0.0 %)
Bytes (Sent/Received): 155727102 / 434504596
Round Trip Latency (Min/Avg/Max): 1 / 1 / 11 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 0 / 8 / 264 / 8000 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 0 / 9056 kbps

Pipeline Processing Rate (Avg/Max): 0 / 40 Mpps
Endpoint Image Settings In Use: Host
Initial Image Quality (Min/Max): 50 / 80
Image Quality Preference: 45
Build To Lossless: Disabled

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

AWI: Home page

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

AWI Home Page Statistics

Statistics	Description
Processor	PCoIP processor type, version, and RAM size
Time Since Boot	Length of time that the PCoIP processor has been running.

Statistics	Description
PCoIP Device Name	<p>The logical name for the device.</p> <p>This field is the name the client registers with the DNS server if DHCP is enabled or the system is configured to support registering the hostname with the DNS server. (See the PCoIP Device Name parameter on the <i>Label</i> page.)</p>
Connection State	<p>The current (or last) state of the PCoIP session. Possible connection states are:</p> <ul style="list-style-type: none"> • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
Connection Duration	<p>Displays the length of time the device has been connected to a host endpoint.</p>
802.1X Authentication Status	<p>Indicates whether 802.1x authentication is enabled or disabled on the device.</p>
Session Encryption Type	<p>Displays the encryption algorithm in use when a session is active.</p>
PCoIP Packets Statistics	<p>PCoIP Packets Sent: The total number of PCoIP packets sent in the current/last session.</p> <p>PCoIP Packets Received: The total number of PCoIP packets received in the current/last session.</p> <p>PCoIP Packets Lost: The total number of PCoIP packets lost in the current/last session.</p>
Bytes	<p>Bytes Sent: The total number of bytes sent in the current/last session.</p> <p>Bytes Received: The total number of bytes received in the current/last session.</p>
Round Trip Latency	<p>The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms).</p>

Statistics	Description
Bandwidth Statistics	<p>Transmit Bandwidth: The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels.</p> <p>Receive Bandwidth: The minimum, average, and maximum traffic received by the Tera processor.</p>
Pipeline Processing Rate	Shows the average and maximum amount of image data being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the <i>Use Client Image Settings</i> field is configured on the Image page for the host device.
Initial Image Quality	<p>The minimum and maximum quality setting is taken from the Image page for the device.</p> <p>The active setting is what's currently being used in the session and only appears on the host.</p>
Image Quality Preference	This setting is taken from the <i>Image Quality Preference</i> field on the Image page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	<p>Options that may appear in this field include the following:</p> <p>Enabled: The <i>Disable Build to Lossless</i> field on the Image page is unchecked.</p> <p>Disabled: The <i>Disable Build to Lossless</i> field is checked.</p>
Display	The port number for the display.
Maximum Rate: Refresh Rate	<p>This column shows the refresh rate of the attached display.</p> <p>If the <i>Maximum Rate</i> field on the Image page is set to 0 (that is, there is no limit), the maximum rate is taken from the monitor's refresh rate.</p> <p>If the <i>Maximum Rate</i> field on the Image page is set to a value greater than 0, the refresh rate shows as User Defined.</p>
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Initial Image Quality	<p>Shows the current lossless state of the attached display:</p> <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless



Note: Clicking Reset Statistics also resets statistics on Home page

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

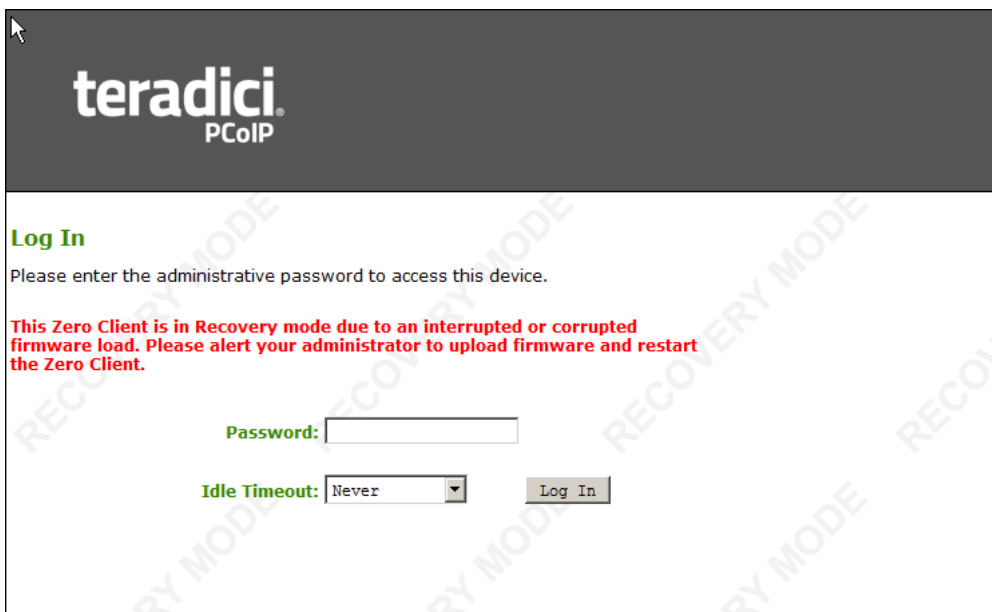
AWI Recovery Mode

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

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

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

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



AWI recovery mode

AWI Recovery Mode Options

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

[Log Out](#) PCoIP® Zero Client

Home Configuration / Diagnostics / Info / Upload

teradici
PCoIP

PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

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

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

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

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

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

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

AWI recovery mode – home page

- **Configuration:** Enables you to correct the problem by changing the [network configuration](#) (including [IPv6 settings](#)), clearing the [management state](#), updating the client’s administrative [password](#), and [resetting](#) the configuration and permissions settings stored on the device.
- **Diagnostics:** Displays the client’s [event log](#) messages and lets you [reset](#) the PCoIP processor.
- **Information:** Displays hardware and firmware [version information](#) about the client.
- **Upload:** Lets you upload [firmware](#) and [certificates](#) for a client.

You can also use the Management Console to upload firmware and certificates to a group of Tera2 PCoIP Zero Clients. For details, see [PCoIP® Management Console 2.4 Administrators' Guide](#).

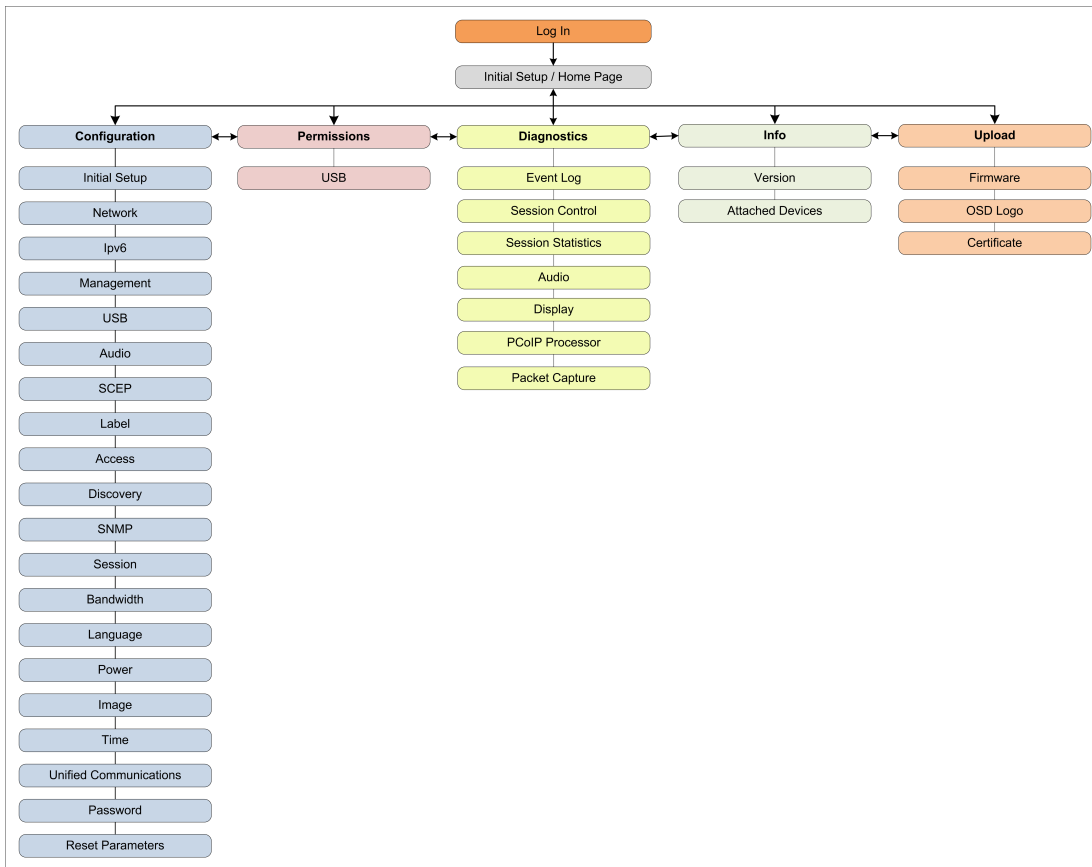
See also: [How to Troubleshoot a Tera2 PCoIP Zero Client in Recovery Mode on page 276](#).

AWI Menus

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

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

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



AWI menu overview



Related: Refer to GUI Reference section

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

Tera2 PCoIP Zero Client Connection Types

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

- PCoIP Remote Workstation cards
- Teradici Cloud Access Software
- Teradici Cloud Access Platform desktops and workstations
- Amazon WorkSpaces desktops
- VMware Horizon View and DaaS desktops

Connecting to PCoIP Remote Workstation Cards

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

This topic includes information on the following sections:

- [Prerequisites](#)
- [Configuration Options](#)
- [Connection Instructions](#)



Note: Remote Workstation Cards use firmware version 4.9

At the time of this documentation release, the current firmware version available for Remote Workstation Cards was version 4.9. Tera2 PCoIP Zero Clients running firmware 5.4 were tested with Remote Workstation Cards running version 4.9. However, Management Console 2.0 is required to manage Tera2 PCoIP Zero Clients running firmware 5.0.0 and later, and Management Console 1.x is required to manage Remote Workstation Cards running firmware version 4.9. You should take this into consideration when making the decision to upgrade Tera2 PCoIP Zero Clients to FW 5.0.0 and later.

Prerequisites

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

- The PCoIP Remote Workstation Card and Tera2 PCoIP Zero Client have compatible firmware versions. For information on how to upload firmware, see [How to Upload Firmware to a Tera2 PCoIP Zero Client on page 275](#).
- You are running a supported OS on the workstation and the Teradici PCoIP host software is installed. For details, see [PCoIP® Host Software for Windows User Guide](#) or

[PCoIP® Host Software for Linux User Guide](#). If you are using a VMware Connection Server as a broker, View Agent must also be installed on the host PC or workstation.

- The Host Driver Function is enabled on the PCoIP Remote Workstation Card.
- Your network resources meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see [PCoIP Protocol Network Design Checklist](#).

Configuration Options

The following session connection types are available for Tera2 PCoIP Zero Client-to-PCoIP Remote Workstation Card connections:

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

Connecting Statically

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

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

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

- [AWI: Direct to Host Session Settings on page 148](#)
- [OSD: Direct to Host Session Settings on page 105](#)

Connecting Using SLP Host Discovery

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

**Note: Do not select SLP host discovery with more than 10 hosts**

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

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

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

- [AWI: Direct to Host + SLP Host Discovery Session Settings on page 154](#)
- [OSD: Direct to Host + SLP Host Discovery Session Settings on page 110](#)

Connecting Using a Third-Party Connection Broker

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

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

For more information, see [Can I use a connection broker with PCoIP technology? \(KB 15134-24\)](#)

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

- [AWI: PCoIP Connection Manager Session Settings on page 158](#)
- [OSD: PCoIP Connection Manager Session Settings on page 114](#)

Connecting Using the View Connection Server

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

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

- [AWI: View Connection Server Session Settings on page 173](#)
- [OSD: View Connection Server Session Settings on page 125](#)

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

Connection Instructions

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

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

Connecting Directly Using SLP Host Discovery

After successfully completing the installation steps outlined in [PCoIP® Tera2 Zero Client Quick Start Guide](#), the client will be powered on and ready to use. The next step is to initiate a PCoIP session with a PCoIP Remote Workstation Card. The easiest way to get started is to use SLP host discovery.



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

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

To connect directly using SLP host discovery:

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



Related Information: Advanced settings

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

Connecting Directly Without Using SLP Host Discovery

To connect directly without using SLP host discovery:

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



Related Information: Advanced settings

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

Connecting Using a Broker:

To connect using a broker:

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select one of the following connection types:
 - [View Connection Server](#) if you are using a VMware broker
 - [PCoIP Connection Manager](#) if you are using a third-party broker.
2. Enter the DNS name or IP address of the broker, and click **OK**.
3. Click the **Connect** button.
4. When prompted, enter your remote workstation's login credentials.



Related Information: Advanced settings

For details about advanced settings, see [View Connection Server](#) or [PCoIP Connection Manager](#).

Connecting to Teradici Cloud Access Software

Teradici Cloud Access Software, also known as Cloud Access Software, is a Teradici application that enables users to remotely access a physical or virtualized remote workstation using the PCoIP protocol without having to install a PCoIP Remote Workstation Card.

The Cloud Access Software supports two deployment scenarios:

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

This topic includes information on the following sections:

- [Prerequisites](#)
- [Configuration Options](#)
- [Connection Instructions](#)

Prerequisites

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

- You are using a Tera2 PCoIP Zero Client (TERA2321 or TERA2140 processor) to connect.
- The remote workstation has the Cloud Access Software installed. For details on how to install the Cloud Access Software in a workstation, see the [Cloud Access Software 2.7, Architecture Guide](#).

For details about workstation requirements, see the [Cloud Access Software 2.7, Architecture Guide](#).

Configuration Options

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

- [AWI: Auto Connect](#)
- [OSD: Auto Connect](#)
- [AWI: PCoIP Connection Manager](#)
- [OSD: PCoIP Connection Manager](#)
- [AWI: PCoIP Connection Manager + Auto-Logon](#)
- [OSD: PCoIP Connection Manager + Auto-Logon](#)

Connection Instructions

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



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

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

Connecting Using Auto Detect

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

To connect using Auto Detect connection type:

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

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

Connecting Using PCoIP Connection Manager

To connect using the PCoIP Connection Manager connection type:

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



Related Information: Advanced settings

For details about advanced settings, see [OSD: PCoIP Connection Manager Session Settings on page 114](#).

Connecting Using PCoIP Connection Manager + Auto-Logon

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

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



Related Information: Advanced settings

For details about advanced settings, see [OSD: PCoIP Connection Manager + Auto-Logon Session Settings on page 119](#).

Connecting to Amazon WorkSpaces Desktops

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

This topic includes information on the following sections:

- [Prerequisites](#)
- [Configuration Options](#)
- [Connection Instructions](#)

Prerequisites

For the best user experience, Teradici recommends using firmware version 5.3 or later with Amazon WorkSpaces (hourly pricing).

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

- You are using a Tera2 PCoIP Zero Client (TERA2321 or TERA2140 processor) to connect.
- You have an AWS account with Amazon WorkSpaces up and running. For information, see AWS documentation.

- Your network has full connectivity to your Amazon WorkSpaces. For information, see AWS documentation.
- You have a PCoIP® Connection Manager for Amazon WorkSpaces appliance installed and configured. See [Connecting PCoIP® Zero Clients to Amazon WorkSpaces](#).

Configuration Options

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

- [AWI: Auto Connect](#)
- [OSD: Auto Connect](#)
- [AWI: PCoIP Connection Manager](#)
- [OSD: PCoIP Connection Manager](#)
- [AWI: PCoIP Connection Manager + Auto-Logon](#)
- [OSD: PCoIP Connection Manager + Auto-Logon](#)

Connection Instructions

Before connecting, you will need to know the IP address of your PCoIP Connection Manager for Amazon WorkSpaces appliance.



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

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

Connecting Using Auto Detect

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

To connect using the Auto Detect connection type:

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



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

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

Connecting Using PCoIP Connection Manager

To connect using the PCoIP Connection Manager connection type:

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



Related Information: Advanced settings

For details about advanced settings, see [OSD: PCoIP Connection Manager Session Settings on page 114](#).

Connecting Using PCoIP Connection Manager + Auto-Logon

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

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



Related Information: Advanced settings

For details about advanced settings, see [OSD: PCoIP Connection Manager + Auto-Logon Session Settings on page 119](#).

Connecting to VMware Horizon Desktops and Applications

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

This topic includes information on the following sections:

- [Prerequisites](#)
- [Configuration Options](#)
- [Connection Instructions](#)

Prerequisites

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

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

Supported Connection Types

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

- [AWI: View Connection Server](#)
- [OSD: View Connection Server](#)
- [AWI: View Connection Server + Auto-Logon](#)
- [OSD: View Connection Server + Auto-Logon](#)
- [AWI: View Connection Server + Kiosk](#)
- [OSD: View Connection Server + Kiosk](#)
- [AWI: View Connection Server + Imprivata OneSign](#)
- [OSD: View Connection Server + Imprivata OneSign](#)

Connection Instructions

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

Connecting with Auto Detect

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

To connect using the Auto Detect connection type:

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



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

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

Connecting with View Connection Server

To connect using the View Connection Server connection type:

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

**Related Information: Advanced settings**

For details about advanced settings, see [OSD: View Connection Server Session Settings on page 125](#).

Connecting with View Connection Server + Auto-Logon

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

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

**Related Information: Advanced settings**

For details about advanced settings, see [OSD: View Connection Server + Auto-Logon Session Settings on page 131](#).

Connecting with View Connection Server + Kiosk

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

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

1. From the **Options > Configuration > Session** menu on the Tera2 PCoIP Zero Client's OSD, select the [View Connection Server + Kiosk](#) connection type.
2. In the **DNS Name or IP Address** field, enter the DNS name or IP address of your View Connection Server (or VMware Horizon DaaS Desktop Portal).
3. Select whether to populate the **Username** field with the MAC address of the Tera2 PCoIP Zero Client (Zero Client MAC option) or use a customer name (Custom option).
4. If you have selected **Custom**, enter the custom name of the client.

5. Enter the password for the kiosk virtual machine.
6. If you are making a VMware Horizon RDS-hosted application connection:
 - a. Click **Advanced**.
 - b. Click to enable the **Enable RDS Application Access** option.
 - c. Click **Apply** and then **OK**.
7. Click the **Connect** button.



Related Information: Advanced settings

For details about advanced settings, see [OSD: View Connection Server + Kiosk Session Settings on page 137](#).

Connecting with View Connection Server + Imprivata OneSign

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



Note: Type 'https://' before the fully qualified computer name

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

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

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



Related Information: Advanced settings

For details about advanced settings, see [OSD: View Connection Server + Imprivata OneSign Session Settings on page 142](#).

GUI Reference

This section provides screen shots and field descriptions for the OSD and AWI pages.

Initial Setup

AWI: Initial Setup

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

Initial Setup (1:1 Manual Configuration)

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

Step 1: Audio

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

Step 2: Network

Enable DHCP:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:

Step 3: Session

Identify Host by: IP address FQDN

Host IP Address:

Host MAC Address:

Step 4: Apply Changes

AWI Initial Setup page

The following parameters can be found on the Initial Setup page.

Audio Parameters

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

Network Parameters

Parameter	Description
Enable DHCP	Enables DHCP (as opposed to using manual IP address configuration)
IP Address	Device's IP address

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

Session Parameters



Note: Message appears for certain session connection types

What appears in this section depends on the session connection type you have configured. When *Direct to Host + SLP Host Discovery* or *Connection Management Interface* is selected, a message appears instead of session parameters. When the client is configured to connect to a specific host, the following session parameters appear:

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

Configuring the Network

OSD: Network Settings

This page lets you configure network settings for the device. 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.

The screenshot shows a 'Configuration' window with a 'Network' tab selected. The window title is 'Configuration' and it has a close button (X) in the top right corner. Below the title bar is a navigation bar with tabs: Network, IPv6, Management, SCEP, Label, Discovery, Session, Power, Display, Access, Audio, and Reset. The main content area is titled 'Change the network settings for the device'. It contains the following settings:

- Enable DHCP:
- IP Address: 10 . 0 . 34 . 4
- Subnet Mask: 255 . 255 . 255 . 0
- Gateway: 10 . 0 . 34 . 1
- Primary DNS Server: 192 . 168 . 1 . 50
- Secondary DNS Server: 192 . 168 . 1 . 52
- Domain Name: teradici.local
- FQDN: pcolp-portal-emu001-025056972792.teradici.local
- Ethernet Mode: Auto (dropdown menu)
- Enable 802.1X Security:
- Identity: (text field)
- Client Certificate: (dropdown menu)



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

OSD Network page

The following are network setting parameters which can be configured from the OSD Network page.


OSD Network Parameters

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

Parameter	Description
Subnet Mask	<p>The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Warning: Take care when setting the subnet mask</p> <p>It is possible to configure an invalid IP address/subnet mask combination (for example, invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.</p> </div> </div>
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain name of the device (for example, domain.local). This field is optional.
FQDN	<p>The fully qualified domain name for the device. The default is pcoip-portal-<MAC> where <MAC> is the device's MAC address. If used, the domain name is appended (for example, pcoip-portal-<MAC>.domain.local). This field is read-only on this page.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note: DHCP option 81 must be available and configured</p> <p>To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.</p> </div> </div>

Parameter	Description
Ethernet Mode	<p>Lets you configure the Ethernet mode of the client as follows:</p> <ul style="list-style-type: none"> • Auto • 100 Mbps Full-Duplex • 10 Mbps Full-Duplex <p>When you choose 10 Mbps Full Duplex or 100 Mbps Full-Duplex and click Apply, the following warning message appears:</p> <div style="border: 1px solid #800000; padding: 5px; margin-bottom: 10px;">  <p>Warning: Different parameters may result in a loss of network connectivity</p> <p>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.</p> </div> <p>Click OK to change the parameter.</p> <div style="border: 1px solid #008080; padding: 5px; margin-bottom: 10px;">  <p>Note: Use 10 Mbps Full-Duplex and 100 Mbps Full-Duplex with caution</p> <p>You should always set the Ethernet mode to Auto and only use 10 Mbps Full-Duplex or 100 Mbps Full-Duplex when the other network equipment (for example, a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.</p> </div>
Enable 802.1X Security	<p>Enable this field for each of your PCoIP Remote Workstation Cards and Tera2 PCoIP Zero Clients if your network uses 802.1x security to ensure that only authorized devices access the network. If enabled, configure the Authentication, Identity, and Client Certificate fields.</p>
Authentication	<p>This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.</p>
Identity	<p>Enter the identity string used to identify your device to the network.</p>

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: 802.1x client certificate must contain all security details**
 PCoIP only supports one 802.1x client certificate. Ensure your security details are all contained within the one file. The 802.1x certificate must contain a private key.

AWI: Network Settings

This page lets you configure network settings for the device. You can access this page from the **Configuration > Network** menu. After you update the parameters on this page, click **Apply** to save your changes. You can also configure network information from the [Initial Setup](#) page.

Network

Change the network settings for the device

Enable DHCP:

IP Address: 10 . 0 . 157 . 39

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 10 . 0 . 157 . 1

Primary DNS Server: 192 . 168 . 65 . 2

Secondary DNS Server: 0 . 0 . 0 . 0

Domain Name: terase.local

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

Ethernet Mode: Auto

Maximum MTU Size: 1200 bytes

Enable 802.1X Security:

Authentication: TLS

Identity: _____

Client Certificate: _____ **Choose**



Enable 802.1X Support for Legacy Switches:



Apply **Cancel**


AWI Network page

The following are network setting parameters which can be configured from the AWI Network page.

AWI Network Parameters

Parameter	Description
Enable DHCP	<p>When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client Fully Qualified Domain Name (FQDN).</p> <p>When disabled, you must set these parameters manually.</p>
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	<p>The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field.</p> <div style="border: 1px solid #c00000; padding: 5px; margin-top: 10px;">  <p>Warning: Take care when setting the subnet mask It is possible to configure an invalid IP address/subnet mask combination (for example, invalid mask) that leaves the device unreachable. Take care when setting the subnet mask.</p> </div>
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain name of the device (for example, domain.local). This field is optional.
FQDN	<p>The fully qualified domain name for the device. The default is pcoip-portal-<MAC> where <MAC> is the device's MAC address. If used, the domain name is appended (for example, pcoip-portal-<MAC>.domain.local). This field is read-only on this page.</p> <div style="border: 1px solid #00a0c0; padding: 5px; margin-top: 10px;">  <p>Note: DHCP option 81 must be available and configured To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.</p> </div>

Parameter	Description
Ethernet Mode	<p>Lets you configure the Ethernet mode of the client as follows:</p> <ul style="list-style-type: none"> • Auto • 100 Mbps Full-Duplex • 10 Mbps Full-Duplex <p>When you choose 10 Mbps Full Duplex or 100 Mbps Full-Duplex and click Apply, the following warning message appears:</p> <div style="border: 1px solid #800000; padding: 5px; margin-bottom: 10px;">  <p>Warning: Different parameters may result in a loss of network connectivity</p> <p>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.</p> </div> <p>Click OK to change the parameter.</p> <div style="border: 1px solid #008080; padding: 5px; margin-bottom: 10px;">  <p>Note: Use 10 Mbps Full-Duplex and 100 Mbps Full-Duplex with caution</p> <p>You should always set the Ethernet mode to Auto and only use 10 Mbps Full-Duplex or 100 Mbps Full-Duplex when the other network equipment (for example, a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped.</p> </div>
Maximum MTU Size	<p>Lets you configure the Maximum Transfer Unit packet size.</p> <p>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.</p> <p>The Maximum MTU Size range is 600 to 1500 bytes for all firmware versions. The default MTU size is 1200.</p>
Enable 802.1X Security	<p>Enable this field for each of your PCoIP Remote Workstation Cards and Tera2 PCoIP Zero Clients if your network uses 802.1x security to ensure that only authorized devices access the network. If enabled, configure the Authentication, Identity, and Client Certificate fields.</p>
Authentication	<p>This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported.</p>

Parameter	Description
Identity	Enter the identity string used to identify your device to the network.
Client Certificate	<p>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.</p> <div style="border: 1px solid #00a651; padding: 5px; margin-top: 10px;">  <p>Note: 802.1x client certificate must contain all security details PCoIP only supports one 802.1x client certificate. Ensure your security details are all contained within the one file. The 802.1x certificate must contain a private key.</p> </div>
Enable 802.1X Support for Legacy Switches	When enabled, enables greater 802.1x compatability for older switches on the network.

Configuring IPv6

OSD: IPv6 Settings

Options on the IPv6 page enable you to change the network settings for the/your device.

You can access this page from the **Options > Configuration > IPv6** menu.

OSD IPv6 page



Note: Restart your device

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

The following are IPv6 setting parameters which can be configured from the OSD IPv6 page.

OSD IPv6 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.

Parameter	Description
Primary DNS	The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Secondary DNS	The device's secondary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Domain Name	The domain name used (for example, 'domain.local') for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	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.

AWI: IPv6 Settings

Options on the IPv6 page enable you to change the network settings for the/your device.

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:

DHCPv6 Addresses: / 64

/ 64

/ 64

/ 64

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC:

SLAAC Addresses: / 64

/ 64

/ 64

/ 64

Enable Manual Address:

AWI IPv6 page



Note: Restart your device

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

The following are IPv6 setting parameters which can be configured from the AWI IPv6 page.

AWI IPv6 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.

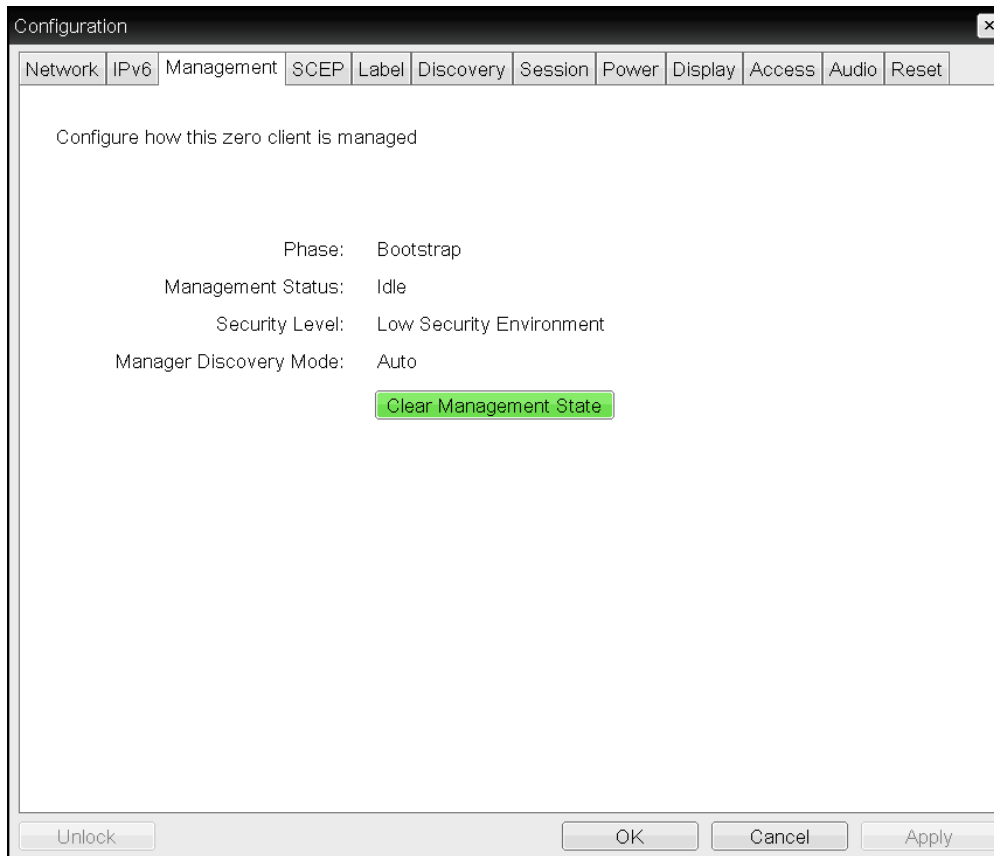
Parameter	Description
DHCPv6 Addresses	When DHCPv6 is enabled and the device is rebooted, the server automatically populates these fields with addresses for the device.
Primary DNS	The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Secondary 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 (for example, 'domain.local') for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
FQDN	The fully qualified domain name for the client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server.
Enable SLAAC	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 Management Options

OSD: Management

The **Management** page contains information about how the Tera2 PCoIP Zero Client is discovered and managed by an Endpoint Manager EM, for example, the PCoIP Management Console. It also enables you to clear the management state for a client. You can access this page from the **Configuration > Management** menu.

To configure management options for the client, see [AWI: Management on page 70](#).



OSD Management page

The following are management parameters which can be configured from the OSD Management page.

OSD Management Parameters

Parameter	Description
Phase	<p>Displays the connection phase for the Tera2 PCoIP Zero Client:</p> <ul style="list-style-type: none"> • Bootstrap: During this phase the client receives the URI for the Endpoint Manager and (optionally) its public certificate fingerprint. • Transition: An interim stage where the client has received Endpoint Manager information and is attempting to connect to the Endpoint Manager. • Managed: The client has successfully connected to the Endpoint Manager and now listens for communications from the PCoIP Management Console Endpoint Manager (for example, applying a new profile, updating firmware).

Parameter	Description
Security Level	<p>Select the desired security level:</p> <ul style="list-style-type: none"> • Low Security Environment - Zero Client is discoverable by Endpoint Managers: This security level is intended for manual discovery initiated by the PCoIP Management Console when the client has an empty certificate store. It enables the client to use trust information retrieved during the bootstrapping and discovery process. Low security can also be used for DHCP or DNS auto discovery when the DHCP or DNS server provisions the endpoint with the Endpoint Bootstrap Manager certificate's fingerprint. Low security enables easy deployment. For information on how to use PCoIP Management Console Enterprise Edition to discover clients manually, see the PCoIP® Management Console 2.4 Administrators' Guide. • Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate: This security level improves security by requiring the client to have a trusted PCoIP Management Console certificate in its certificate store in order for discovery to succeed. The certificate can be provisioned either by the vendor when an endpoint is shipped or by manually uploading the PCoIP Management Console's certificate to the endpoint. Clients configured with medium security can use DHCP or DNS auto discovery, but cannot use manual discovery initiated by the PCoIP Management Console. • High Security Environment - Bootstrap phase disabled: With this security level, an administrator must manually enter an internal (and optionally an external) URI for the PCoIP Management Console. The administrator must also upload a trusted PCoIP Management Console certificate to the endpoint. Clients configured for high security cannot use DHCP or DNS auto discovery or manual discovery initiated by the PCoIP Management Console. See Configuring a PCoIP Zero Client with an Endpoint Manager for details on how to configure clients in a high security environment.
Manager Discovery Mode	<p>Select the desired discovery mode:</p> <ul style="list-style-type: none"> • Automatic: When this option is set, the client attempts to receive the Endpoint Bootstrap Manager connection information from a DHCP server or DNS server. • Manual: When this option is set, the user provisions the Endpoint Bootstrap Manager in the Endpoint Bootstrap Manager URI field.
Clear Management State	<p>Click this button to clear the current Endpoint Manager information for the client. Once an endpoint is managed by a PCoIP Management Console, its management state must be cleared before the endpoint will accept a new PCoIP Management Console.</p>

AWI: Management

The **Management** page is accessed from the **Configuration > Management** menu. From this page you can:

- View information about how a Tera2 PCoIP Zero Client is discovered and managed by an Endpoint Manager, for example, Teradici's PCoIP Management Console Enterprise Edition, version 2.0+.
- Set the device's security level and discovery method.
- (For high security environments only) configure the uniform resource identifier (URI) of the client's Endpoint Manager to enable the device to be discovered directly by the Endpoint Manager.
- Clear the device's management state.



Note: PCoIP Management Console operates as both the Endpoint Bootstrap Manager and Endpoint Manager

In this release, PCoIP Management Console 2.0+ operates as both the Endpoint Bootstrap Manager and the Endpoint Manager.

About Discovery Methods

If your zero client is using [automatic discovery](#), your system must be configured either for DHCP vendor class option discovery or DNS service record discovery, and the client's security level must be set to low or medium. When the client is powered on, it receives the uniform resource identifier (URI) for the Endpoint Bootstrap Manager (that is, the PCoIP Management Console) to which it should connect from its DHCP or DNS server during the bootstrap phase. Optionally, it may also obtain the Endpoint Bootstrap Manager certificate's fingerprint from the DHCP or DNS server. For details about how to configure your DHCP or DNS server for automatic discovery, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

You can also [manually configure an Endpoint Manager](#) (that is, a PCoIP Management Console) from a client's AWI **Management** page. This method can only be used for devices that are configured for a high security environment.

Before discovery can take place, clients also need a PCoIP Management Console certificate [uploaded to their certificate store](#). This can be either an issuer certificate (that is, the root CA certificate or intermediate certificate that was used to issue a PCoIP Management Console server's public key certificate) or the PCoIP Management Console server's public key certificate itself. The only exceptions to this certificate requirement are as follows:

- The client is configured for low security, is using DHCP or DNS discovery, *and* the DHCP or DNS server has provisioned it with the Endpoint Bootstrap Manager certificate's fingerprint (that is, the PCoIP Management Console server certificate's hash, or digital signature).
- The client is configured for low security *and* is using the [PCoIP Management Console's manual discovery method](#).

The following table summarizes the certificate requirements for clients based on their discovery method and security level:

Certificate Requirements for Tera2 PCoIP Zero Clients

Discovery Method	Low Security	Medium Security	High Security
DHCP/DNS discovery <i>without</i> Endpoint Bootstrap Manager fingerprint provisioned	certificate required	certificate required	N/A
DHCP/DNS discovery <i>with</i> Endpoint Bootstrap Manager fingerprint provisioned	certificate <i>not</i> required	certificate required	N/A
Discovery initiated by a device configured for a high security environment	certificate required	certificate required	certificate required
Manual discovery initiated by the PCoIP Management Console	certificate <i>not</i> required	N/A	N/A



Related Information: PCoIP Management Console certificates

For information about PCoIP Management Console certificates, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

Configuring the Management Page

The information that displays on the **Management** page depends on whether the client is using automatic or manual discovery.

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.153.242:5172

Security Level:

Manager Discovery Mode:

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

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

AWI Management page – automatic discovery mode

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.157.21:5172

Security Level:

Manager Discovery Mode:

Endpoint Bootstrap Manager URI:

EM Topology:	URI Type: <input type="text" value="wss://10.0.157.21:5172"/>	EM URI: <input type="text" value=""/>	Certificate Fingerprint: <input type="text" value="87:62:71:01:85:27:46:8B:E3:E9:5C:E2:34:2C:85:76:7D:7A:F1:7F:6A:4D:5C:0B:AA:2B:99:BD:D5:A9:28:91"/>
	External EM URI: <input type="text" value=""/>		

AWI Management page – manual discovery mode

The following are management parameters which can be configured from the AWI Management page.


AWI Management Parameters






Note: Use the PCoIP Management Console's IP address and certificate fingerprint

Use your PCoIP Management Console's IP address and certificate fingerprint when specifying this information for an Endpoint Bootstrap Manager or Endpoint Manager.

Parameter	Description
Phase	<p>Displays the connection phase for the Tera2 PCoIP Zero Client:</p> <ul style="list-style-type: none"> • Bootstrap: During this phase the client receives the URI for the Endpoint Manager and (optionally) its public certificate fingerprint. • Transition: An interim stage where the client has received Endpoint Manager information and is attempting to connect to the Endpoint Manager. • Managed: The client has successfully connected to the Endpoint Manager and now listens for communications from the PCoIP Management Console Endpoint Manager (for example, applying a new profile, updating firmware).
Management Status	<p>Possible connection states:</p> <ul style="list-style-type: none"> • Idle: The client is waiting for connection information. • Connecting: The client has received the Endpoint Manager information and is attempting to connect to the Endpoint Manager. • Retrying: If the client is unable to connect to the Endpoint Manager, it will retry intermittently for five minutes. • Connected: The client has successfully connected to the Endpoint Manager.

Parameter	Description
Security Level	<p>Select the desired security level:</p> <ul style="list-style-type: none"> Low Security Environment - Zero Client is discoverable by Endpoint Managers: This security level is intended for manual discovery initiated by the PCoIP Management Console when the client has an empty certificate store. It enables the client to use trust information retrieved during the bootstrapping and discovery process. Low security can also be used for DHCP or DNS auto discovery when the DHCP or DNS server provisions the endpoint with the Endpoint Bootstrap Manager certificate's fingerprint. Low security enables easy deployment. For information on how to use PCoIP Management Console Enterprise Edition to discover clients manually, see the PCoIP® Management Console 2.4 Administrators' Guide. Medium Security Environment - Endpoint Bootstrap Manager must be trusted by installed certificate: This security level improves security by requiring the client to have a trusted PCoIP Management Console certificate in its certificate store in order for discovery to succeed. The certificate can be provisioned either by the vendor when an endpoint is shipped or by manually uploading the PCoIP Management Console's certificate to the endpoint. Clients configured with medium security can use DHCP or DNS auto discovery, but cannot use manual discovery initiated by the PCoIP Management Console. High Security Environment - Bootstrap phase disabled: With this security level, an administrator must manually enter an internal (and optionally an external) URI for the PCoIP Management Console. The administrator must also upload a trusted PCoIP Management Console certificate to the endpoint. Clients configured for high security cannot use DHCP or DNS auto discovery or manual discovery initiated by the PCoIP Management Console. See Configuring a PCoIP Zero Client with an Endpoint Manager for details on how to configure clients in a high security environment.
Internal Endpoint Manager URI	<p>This field displays when the security level is set to High Security Environment - Bootstrap phase disabled.</p> <p>Enter the URI for the internal Endpoint Manager using the following format, and click Apply:</p> <pre>wss://<internal EM IP address/FQDN>:[port number]</pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: URL requires a secured WebSocket (wss://) prefix</p> <p>This URL requires a secured WebSocket (wss://) prefix. The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.</p> </div>

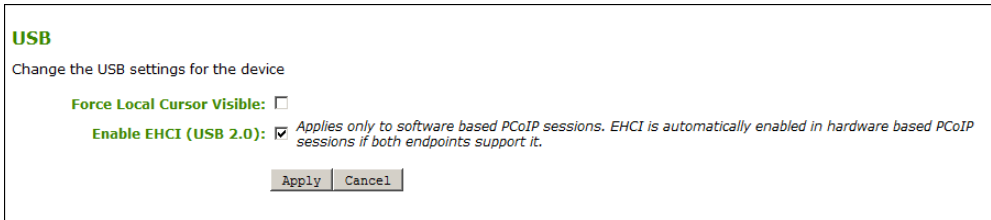
Parameter	Description
External Endpoint Manager URI (optional)	<p>This optional field displays the security level is set to High Security Environment - Bootstrap phase disabled.</p> <p>If the client is unable to connect to the internal Endpoint Manager, it will attempt to connect to the external Endpoint Manager if this field is configured.</p> <p>If desired, enter the URI for the external Endpoint Manager using the following format, and click Apply: <code>wss://<external EM IP address/FQDN>:[port number]</code></p> <div style="border: 1px solid #00a09a; padding: 5px; margin-top: 10px;">  <p>Note: URL requires a secured WebSocket (wss://) prefix This URL requires a secured WebSocket (wss://) prefix. The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.</p> </div>
Manager Discovery Mode	<p>Select the desired discovery mode:</p> <ul style="list-style-type: none"> • Automatic: When this option is set, the client attempts to receive the Endpoint Bootstrap Manager connection information from a DHCP server or DNS server. • Manual: When this option is set, the user provisions the Endpoint Bootstrap Manager in the Endpoint Bootstrap Manager URI field.
Discovery Information	<p>When the Manager Discover Mode is set to Automatic, this section displays the device discovery method your system is using.</p> <ul style="list-style-type: none"> • Discovery Method: Displays the type of automatic discovery mechanism your system is configured to use (for example, PCoIP Management Console DNS SRV record discovery, DHCP vendor-specific options discovery). • Discovery Outcome: Displays the discovery result for the configured discovery methods. • Endpoint Bootstrap Manager Address: If the client has been discovered using one of the discovery methods, displays the IP address for the Endpoint Bootstrap Manager. • Certificate Fingerprint: Displays the certificate fingerprint (that is, the certificate's digital signature) that was used to authenticate the Endpoint Bootstrap Manager.

Parameter	Description
Endpoint Manager Topology	<p>When the client has been automatically discovered by an Endpoint Manager, this section displays information about the connection.</p> <p> Note: If client used manual discovery, information does not display If the client has used manual discovery, this information does not display.</p> <ul style="list-style-type: none"> • URI Type: Displays whether the client is connected to an internal Endpoint Manager or an external one. • Endpoint Manager URI: Displays the URI (uniform resource identifier) for the Endpoint Manager the client is currently using. • Certificate Fingerprint: Displays the certificate fingerprint (digital signature) that was used to authenticate the Endpoint Manager.
Endpoint Bootstrap Manager URI	<p>This field displays when the discovery mode is set to Manual.</p> <p>Enter the URI for the Endpoint Bootstrap Manager the client will connect to for bootstrap information using the following format, and click Apply: <code>wss://<EBM IP address/FQDN>:[port number]</code></p> <p> Note: URL requires a secured WebSocket (wss://) prefix This URL requires a secured WebSocket (wss://) prefix. The PCoIP Management Console's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.</p>
Clear Management State	<p>Click this button to clear the current Endpoint Manager information for the client. Once an endpoint is managed by a PCoIP Management Console, its management state must be cleared before the endpoint will accept a new PCoIP Management Console.</p>

Configuring USB Settings

AWI: USB Settings

The **USB** page lets you configure settings for devices plugged into Tera2 PCoIP Zero Client USB ports. You can access this page from the **Configuration > USB** menu.



AWI USB page

The following are USB parameters which can be configured from the AWI USB parameters page.

AWI USB Parameters

Parameter	Description
Force Local Cursor Visible	When enabled, the Tera2 PCoIP Zero Client always shows the local cursor . When disabled, the local cursor is only shown when the host requests it or a locally-terminated mouse is connected.
Enable EHCI (USB 2.0)	Enable this field to configure EHCI (USB 2.0) for devices connected directly to Tera2 PCoIP Zero Client USB ports for sessions with a host running VMware View 4.6 or newer.



Note: Setting applies only to software-based PCoIP sessions

This setting applies only to software-based PCoIP sessions. EHCI is automatically enabled in hardware-based PCoIP sessions if both endpoints support it. If you want the device to operate in OHCI (USB 1.1) mode, add it to the [Devices Forced to USB 1.1](#) table on the **Permissions > USB** page.



Note: Feature cannot be used on clients with less than 128 MB of RAM

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.

AWI: USB Permissions

The **USB** page is accessed from the **Permissions > USB** menu. It enables 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 from this page, and enable USB 2.0 Enhanced Host Controller Interface (EHCI) mode for certain USB devices. In cases where a bridged USB device that is capable of EHCI (USB 2.0) does not perform normally over

PCoIP, you can use the Devices Forced to USB 1.1 table to override that device to use OHCI (USB 1.1) instead of EHCI (USB 2.0), which may provide a better experience.

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

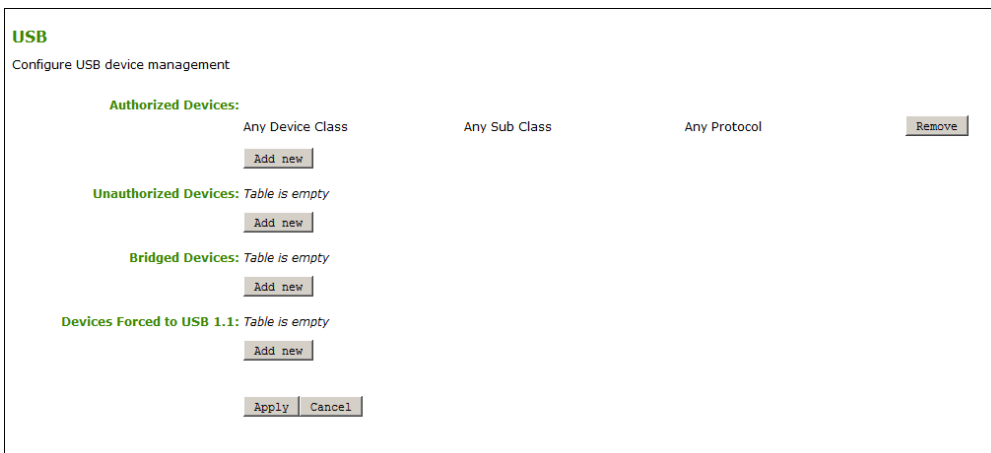
The **USB** page is available on the host and client but the host USB permissions have a higher priority and update the client USB permissions. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP Remote Workstation Card. The following rules apply:

- 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 USB permissions page

The following are permissions parameters which can be configured from the AWI USB permissions page.

AWI USB Permissions Parameters

Parameter	Description
Authorized Devices	<p>Specify the authorized USB devices for the device:</p> <p>Add New: add a new device or device group to the list. This enables USB authorization by ID or Class:</p> <ul style="list-style-type: none"> • ID: The USB device is authorized by its Vendor ID and Product ID. • Class: The USB device is authorized by Device Class, Sub Class, and Protocol. <p>Remove: Delete a rule for a device or device group from the list.</p>
Unauthorized Devices	<p>Specify the unauthorized USB devices for the device.</p> <p>Add New: add a new device or device group to the list. This enables USB devices to be unauthorized by ID or Class:</p> <ul style="list-style-type: none"> • ID: The USB device is unauthorized by its Vendor ID and Product ID • Class: The USB device is unauthorized by Device Class, Sub Class, and Protocol. <p>Remove: Delete a rule for a device or device group from the list.</p>
Bridged Devices	<p>Tera2 PCoIP Zero Clients locally terminate HID devices when connecting to VMware Horizon virtual desktops. However, some devices advertise as HID but use different drivers. These devices may need to be bridged to the host rather than locally terminated. This setting lets you force the Tera2 PCoIP Zero Client to bridge specific USB devices so that they use the drivers on the virtual desktop.</p> <p>Add New: Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.</p> <p> Note: Bridging requires host support Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information.</p> <p>Remove: Delete a rule for a device or device group from the list.</p>

Parameter	Description
Devices Forced to USB 1.1	<p>In cases where a bridged USB device that is capable of EHCI (USB 2.0) does not perform normally over PCoIP, you can use this table to override that device to use OHCI (USB 1.1) instead of EHCI (USB 2.0), which may provide a better experience.</p> <p>Add New: Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.</p> <p>Remove: Delete a rule for a device or device group from the list.</p> <p> Note: Bridging requires host support Bridging requires host support; USB bridging is not supported by all PCoIP hosts. See your host's guide for more information.</p>

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.

Add new:

Device Class: *

Sub Class: *

Protocol: *

Device class parameters

Add new:

Vendor ID:

Product ID:

Device ID parameters

The following are explanations for USB authorized/unauthorized device parameters:

USB Authorized/Unauthorized Devices Parameters

Parameter	Description
Add new	When adding a new USB authorization or unauthorization entry, select one of the following: <ul style="list-style-type: none"> • Class: The USB device is authorized by its device class, sub-class, and protocol information. • ID: The USB device is authorized by its vendor ID and product ID information.
Device Class	This field is enabled when Class is selected. Select a supported device class from the drop-down menu, or select Any to authorize or unauthorize (disable) any device class.
Sub Class	This field is enabled when Class is selected. Select a supported device sub class from the drop-down menu, or select Any to authorize or unauthorize (disable) any sub-class.
Protocol	This field is enabled when Class is selected. Select a supported protocol from the drop-down menu, or select Any .
Vendor ID	This field is enabled when ID is selected. Enter the vendor ID of the authorized (or unauthorized) device. The valid range is hexadecimal 0-FFFF.
Protocol ID	This field is enabled when ID is selected. Enter the product ID of the (authorized or unauthorized) device. The valid range is hexadecimal 0-FFFF.

When you add a new USB bridged entry, the following parameters display.

The screenshot shows a dialog box with the following elements:

- Vendor ID:** A text input field containing the value "0000".
- Product ID:** A text input field containing the value "0000".
- Buttons:** Two buttons labeled "Add" and "Cancel" are positioned below the input fields.

USB Bridged Parameters

The following are explanations for USB bridged device parameters:

USB Bridged Devices Parameters

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

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

Configuring Audio Settings

OSD: 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

The following are audio parameters which can be configured from the OSD Audio page.

OSD Audio Parameters

Parameter	Description
Enable Local USB Audio Driver	<p>This option locally terminates any USB audio devices that are attached to the Tera2 PCoIP Zero Client.</p> <p>When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience.</p> <p>When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions.</p> <div style="margin-top: 10px;">  <p>Note: Install the Teradici Audio Driver for audio support For bi-directional audio support (for example, microphone as well as playback), the Teradici Audio Driver must be installed on your VM and selected as the default playback device.</p> </div> <div style="margin-top: 10px;">  <p>Caution: Local USB audio driver cannot be used for all configurations If you are using a USB composite device that contains audio functionality but also has one or more functions that must be bridged (that is, terminated remotely so the host OS can install the driver), the local USB audio driver cannot be used for the device.</p> </div>
Enable Dual Audio Output	When enabled, all VM audio is sent to both an external speaker and a USB headset (for example, the inbound ringer audio for CounterPath Bria softphones).
Enable Opus Audio Codec	When enabled, the Opus audio codec is used for audio output from software hosts to clients if supported by the host.
Audio Input	The options in this section let you specify the preferred device to use for audio input (recording). They are available when Enable Local USB Audio Driver is selected.

Parameter	Description
Device Type	<p>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 Tera2 PCoIP 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:</p> <ul style="list-style-type: none"> • Analog: The analog input device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio recording. • USB: The USB input device attached to the Tera2 PCoIP Zero Client will be used for audio recording. If more than one is attached, the <i>Audio Input</i> options let you specify the preferred one to use.
Preferred USB Device Vendor ID	<p>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.</p> <div data-bbox="430 840 527 934" style="float: left; margin-right: 10px;">  </div> <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p>
Preferred USB Device Product ID	<p>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.</p> <div data-bbox="430 1134 527 1228" style="float: left; margin-right: 10px;">  </div> <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p>
Attached USB devices	<p>In the drop-down list, select the preferred USB device to use for audio input.</p> <div data-bbox="430 1365 527 1459" style="float: left; margin-right: 10px;">  </div> <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p>
Audio Output	<p>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.</p>

Parameter	Description
Device Type	<p>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 Tera2 PCoIP 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:</p> <ul style="list-style-type: none"> • Analog: The analog output device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio playback. • USB: The USB output device attached to the Tera2 PCoIP Zero Client will be used for audio playback. If more than one is attached, the Audio Output options let you specify the preferred one to use.
Preferred USB Device Vendor ID	<p>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.</p> <p> Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p>
Preferred USB Device Product ID	<p>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.</p> <p> Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p>
Attached USB devices	<p>In the drop-down list, select the preferred USB device to use for audio output.</p>

AWI: Audio Settings

The Audio page lets you configure audio options for the device. You can access this page from the **Configuration > Audio** menu.

Audio
Change audio settings

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

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

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

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

Audio Input

Audio Device Type:

Preferred USB Device Vendor ID:

Preferred USB Device Product ID:

Attached USB devices:

Audio Output

Audio Device Type:

Preferred USB Device Vendor ID:


Preferred USB Device Product ID:



Attached USB devices:




AWI Audio page



The following are audio parameters which can be configured from the AWI Audio page.

AWI Client Audio Parameters

Parameter	Description
Enable Audio	When enabled, configures audio support on the device.
	<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note: Enable the property on both host and client</p> <p>This property must be enabled on both the host and the client.</p> </div> </div>
	When disabled, the audio hardware is not available for the host operating system to enumerate.

Parameter	Description
Enable Local USB Audio Driver	<p>This option locally terminates any USB audio devices that are attached to the Tera2 PCoIP Zero Client.</p> <p>When enabled, the audio stream is moved out of the PCoIP USB data channel and into a PCoIP audio data channel that handles lost and out-of-sequence packets without retransmitting them. The audio data are also compressed, resulting in bandwidth savings and a much improved sound experience.</p> <p>When this option is not enabled, USB audio devices are bridged to the host, and the audio stream is embedded in the PCoIP USB data channel as uncompressed audio data. This data channel retransmits lost and out-of-sequence packets, which can affect audio performance in adverse network conditions.</p> <div style="margin-top: 10px;">  <p>Note: Install the Teradici Audio Driver for audio support For bi-directional audio support (for example, microphone as well as playback), the Teradici Audio Driver must be installed on your VM and selected as the default playback device.</p> </div> <div style="margin-top: 10px;">  <p>Caution: Local USB audio driver cannot be used for all configurations If you are using a USB composite device that contains audio functionality but also has one or more functions that must be bridged (that is, terminated remotely so the host OS can install the driver), the local USB audio driver cannot be used for the device.</p> </div>
Enable Dual Audio Output	<p>When enabled, all VM audio is sent to both an external speaker and a USB headset (for example, the inbound ringer audio for CounterPath Bria softphones).</p>
Enable Opus Audio Codec	<p>When enabled, the Opus audio codec is used for audio output from software hosts to clients if supported by the host.</p>
Audio Input	<p>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.</p>

Parameter	Description
Audio Device Type	<p>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 Tera2 PCoIP 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:</p> <ul style="list-style-type: none"> • Analog: The analog input device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio recording. • USB: The USB input device attached to the Tera2 PCoIP Zero Client will be used for audio recording. If more than one is attached, the <i>Audio Input</i> options let you specify the preferred one to use.
Preferred USB Device Vendor ID	<p>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.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p> </div>
Preferred USB Device Product ID	<p>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.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p> </div>
Attached USB devices	<p>In the drop-down list, select the preferred USB device to use for audio input.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p> </div>
Audio Output	<p>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.</p>

Parameter	Description
Audio Device Type	<p>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 Tera2 PCoIP 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:</p> <ul style="list-style-type: none"> • Analog: The analog output device plugged into the analog input jack on the Tera2 PCoIP Zero Client will be used for audio playback. • USB: The USB output device attached to the Tera2 PCoIP Zero Client will be used for audio playback. If more than one is attached, the Audio Output options let you specify the preferred one to use.
Preferred USB Device Vendor ID	<p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p> </div>
Preferred USB Device Product ID	<p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: Option does not apply for analog audio devices This option does not apply to analog audio devices.</p> </div>
Attached USB devices	<p>In the drop-down list, select the preferred USB device to use for audio output.</p>

Configuring SCEP Settings

OSD: SCEP Settings

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

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



Note: Device generates its own 2048-bit SCEP RSA private key

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



Note: SCEP certificate naming conventions

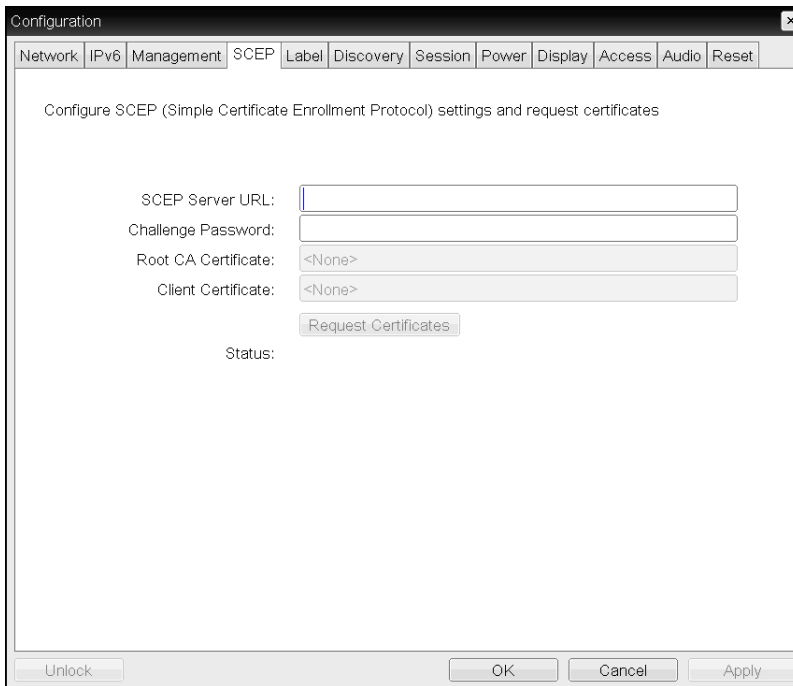
SCEP certificates are configured with the requested certificate 'Subject' as the PCoIP Device Name and the 'Subject Alternative' as the device MAC address (all in lower case and with no dashes). This naming convention is not configurable.



Related Information: SCEP scenarios and tested SCEP server setups

For information on the best SCEP scenarios and tested SCEP server setups, see [What are the best scenarios and setups Teradici uses to test its implementation of SCEP? \(KB 15134-1518\)](#).

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 SCEP page

The following parameters can be found on the OSD SCEP page.

OSD SCEP Parameters

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

AWI: SCEP Settings

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

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



Note: Device generates its own 2048-bit SCEP RSA private key

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



Note: SCEP certificate naming conventions

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



Related Information: SCEP scenarios and tested SCEP server setups

For information on the best SCEP scenarios and tested SCEP server setups, see [What are the best scenarios and setups Teradici uses to test its implementation of SCEP? \(KB 15134-1518\)](#).

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.

SCEP
Configure SCEP settings and retrieve certificates

SCEP Server URL:

Challenge Password:

Root CA:

Client Certificate:

Status:

AWI SCEP page

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

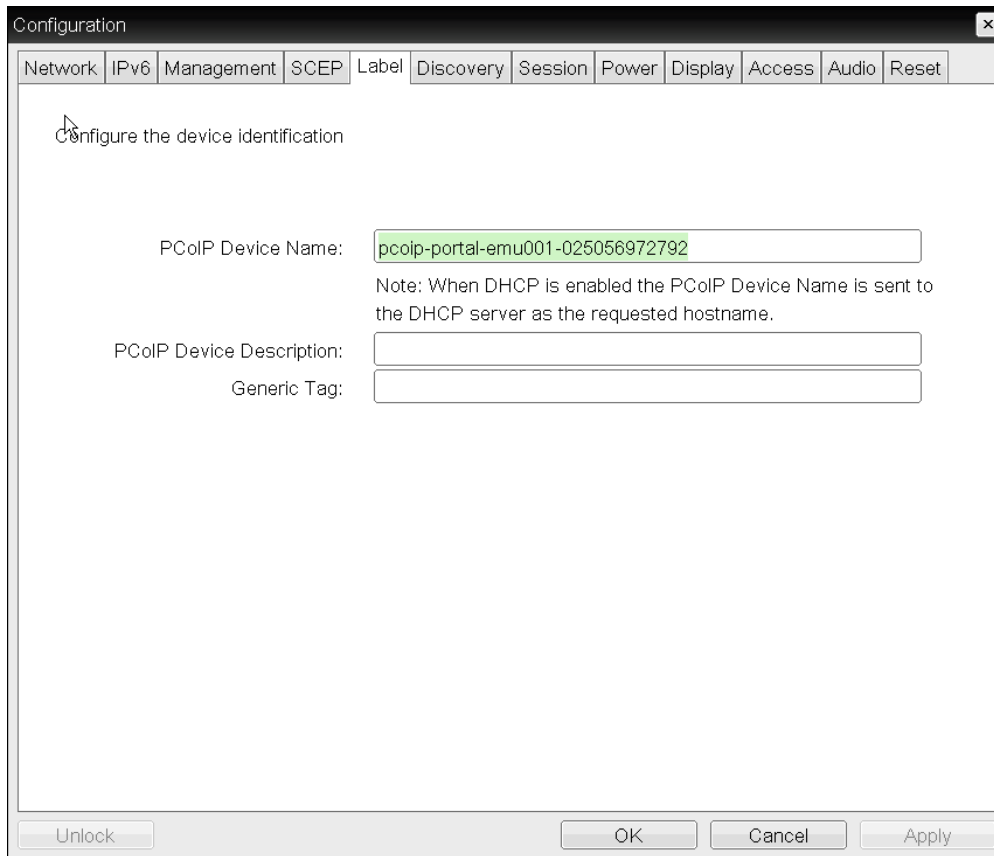
AWI SCEP Parameters

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 (for example, in progress, successful, failed).

Configuring Label Settings

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

The following parameters can be found on the OSD Label page.

OSD Label Parameters

Parameter	Description
PCoIP Device Name	<p>Lets you give the device a logical name. The default is pcoip-portal-<MAC>, where <MAC> is the device's MAC address.</p> <p>This field is the name the device registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server.</p> <p>It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions:</p> <ul style="list-style-type: none"> • The first and last character must be a letter (A-Z or a-z) or a digit (0-9). • The remaining characters must be letters, digits, hyphens, or underscores. • The length must be 63 characters or fewer.

Parameter	Description
PCoIP Device Description	<p>A description of the device or other information, such as the location of the device's endpoint.</p> <div style="display: flex; align-items: center;">  <p>Note: Field not used by firmware The firmware does not use this field. It is provided for administrator use only.</p> </div>
Generic Tag	<p>Generic tag information about the device.</p> <div style="display: flex; align-items: center;">  <p>Note: Field not used by firmware The firmware does not use this field. It is provided for administrator use only.</p> </div>

AWI: Label Settings

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

Label

Change the PCoIP device labels

PCoIP Device Name:

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



PCoIP Device Description:

Generic Tag:

AWI Label page

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

AWI Label Parameters

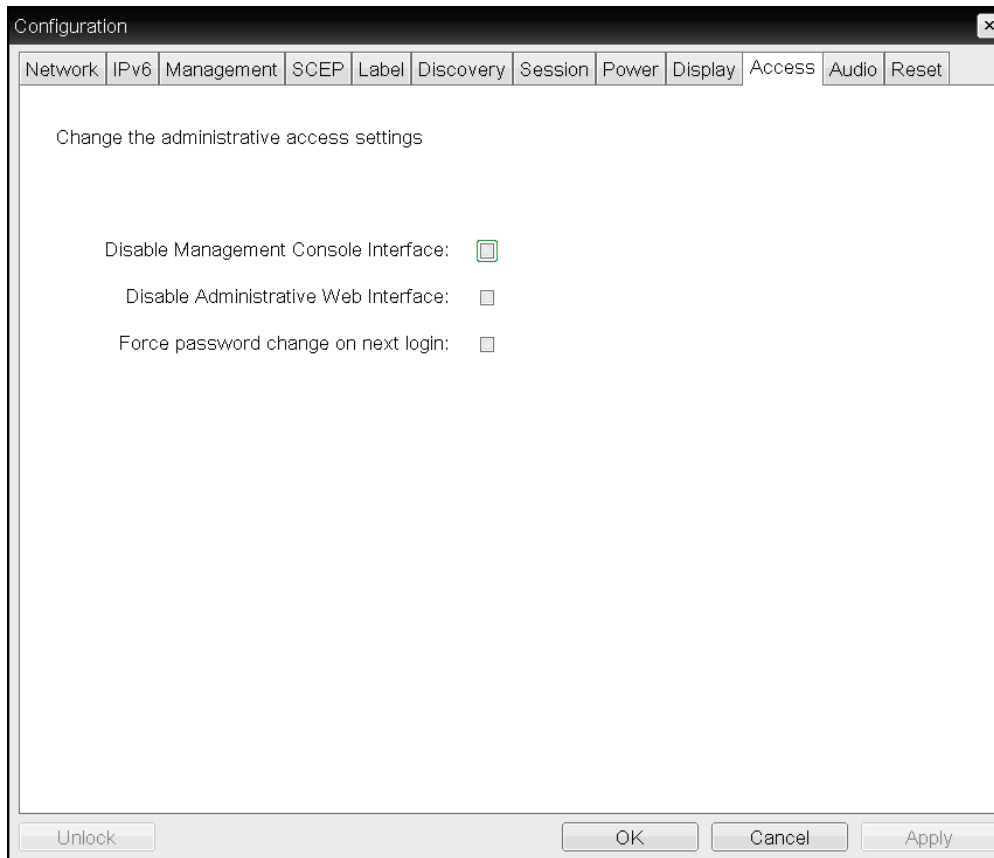
Parameter	Description
PCoIP Device Name	<p>Lets you give the device a logical name. The default is pcoip-portal-<MAC>, where <MAC> is the device's MAC address.</p> <p>This field is the name the device registers with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server.</p> <p>It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions:</p> <ul style="list-style-type: none"> • The first and last character must be a letter (A-Z or a-z) or a digit (0-9). • The remaining characters must be letters, digits, hyphens, or underscores. • The length must be 63 characters or fewer.
PCoIP Device Description	<p>A description of the device or other information, such as the location of the device's endpoint.</p> <div style="display: flex; align-items: center;">  <div> <p>Note: Field not used by firmware</p> <p>The firmware does not use this field. It is provided for administrator use only.</p> </div> </div>
Generic Tag	<p>Generic tag information about the device.</p> <div style="display: flex; align-items: center;">  <div> <p>Note: Field not used by firmware</p> <p>The firmware does not use this field. It is provided for administrator use only.</p> </div> </div>

Configuring Access Settings

OSD: Access Settings

The Access page lets you prevent the device from being managed by the PCoIP Management Console (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

The following parameters can be found on the OSD Access page.

OSD Access 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 PCoIP Management Console (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.

AWI: Access Settings

The Access page lets you prevent the device from being managed by the PCoIP Management Console (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: Enable at least one of the device's configuration interfaces

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

Access

Change administrative access settings

Disable Management Console Interface:

Disable Administrative Web Interface:

Force password change on next login:

AWI Access page

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

AWI Access 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 PCoIP Management Console (or any other PCoIP device management tool).
Disable Administrative Web Interface	When enabled, the device cannot be accessed or managed using the AWI.

Parameter	Description
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

OSD: Discovery Settings

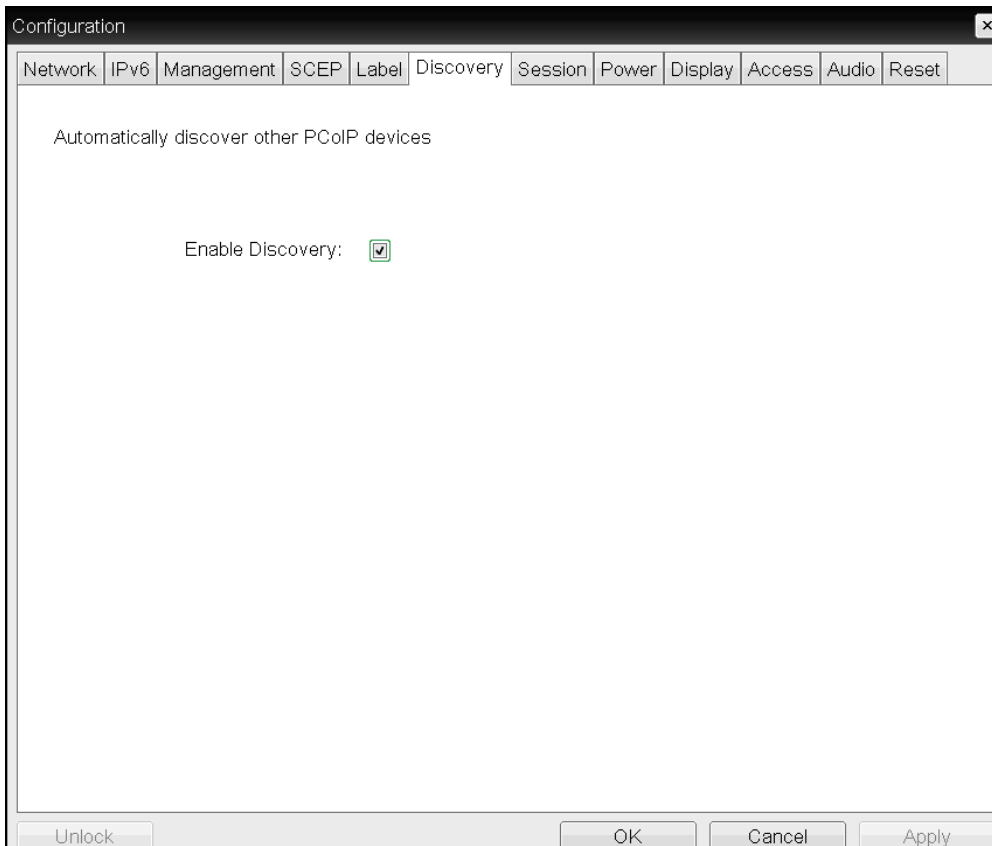
The settings on this page let you enable Service Location Protocol (SLP) management entities to discover devices dynamically in the PCoIP system without requiring prior knowledge of their locations in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort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

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



Note: Devices and PCoIP Management Console should reside on same subnet

SLP discovery mechanism requires all PCoIP devices and the PCoIP Management Console 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 enable this, the recommended discovery mechanism in this case is to configure DHCP Vendor Class Options directly in the DHCP server.



OSD Discovery page

The following parameters can be found on the OSD Discovery page.

OSD Discovery Parameters

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

AWI: Discovery Settings

The settings on this page let you enable management entities to discover devices 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: Devices and PCoIP Management Console should reside on same subnet

SLP discovery mechanism requires all PCoIP devices and the PCoIP Management Console 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 enable this, the recommended discovery mechanism in this case is to configure DHCP Vendor Class Options directly in the DHCP server.

Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable DNS SRV Discovery:


DNS SRV Discovery Delay: seconds

AWI Discovery page

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

AWI Discovery Parameters

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

Parameter	Description
Enable DNS-SRV Discovery	<p>When enabled:</p> <ul style="list-style-type: none"> • Devices automatically advertise themselves to a connection broker without requiring prior knowledge of its location in the network. • The device tries to download and use the DNS SRV record from the DNS server. <div style="border: 1px solid #00a0c0; padding: 5px; margin-top: 10px;">  <p>Note: Enabling DNS SRV Discovery option configures the discovery for connection brokers The <i>Enable DNS SRV Discovery</i> option configures the discovery for connection brokers but does not affect the DNS SRV functionality for the PCoIP Management Console.</p> </div>
DNS-SRV Discovery Delay	<p>Configures the amount of delay time in seconds between the DNS SRV discovery attempts for connection brokers and the PCoIP Management Console. DNS SRV discovery continues periodically until the device successfully contacts a connection management server.</p> <p>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 client to contact the PCoIP Management Console.</p>

Configuring SNMP Settings

AWI: SNMP Settings

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



Related Information: PCoIP SNMP Agent

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

SNMP

Change the SNMP configuration

Enable SNMP:

Community Name:

AWI SNMP page

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

AWI SNMP Parameters

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

Session Connection Types

The following are the main session connection types:

- [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)

Auto Detect

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

Auto Detect is the default session connection type.

Auto Detect Connections

Management Tool	Session Connection Options
AWI	Auto Detect
OSD	Auto Detect

Direct to Host

A Direct to Host session is a direct connection between a Tera2 PCoIP Zero Client and a remote workstation containing a PCoIP Remote Workstation Card. You can specify a 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	Session Connection Options
AWI	Direct to Host
	Direct to Host + SLP Host Discovery
OSD	Direct to Host
	Direct to Host + SLP Host Discovery

PCoIP Connection Manager

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

PCoIP Connection Manager Connections

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

View Connection Server

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



Note: VMWare RDS-hosted application connections support different session types

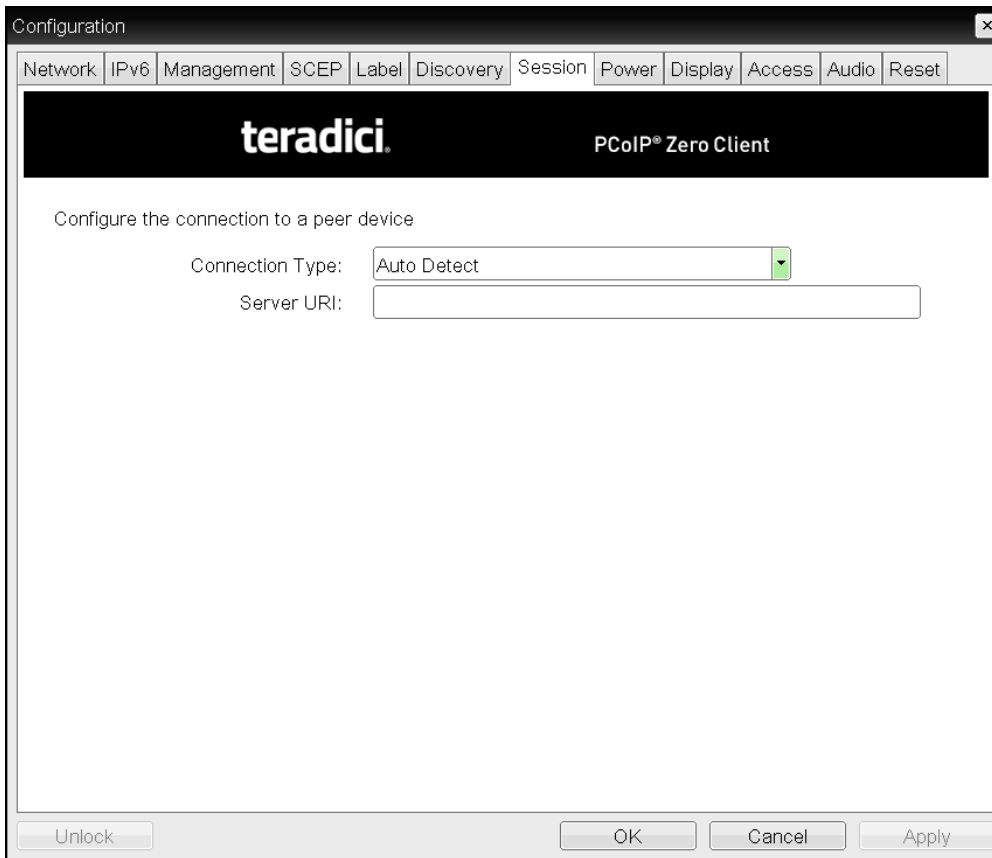
VMWare Horizon RDS-hosted application connections are supported on the **View Connection Server**, **View Connection Server + Auto-Logon**, **View Connection Server + Kiosk**, and **View Connection Server + Imprivata OneSign** session types for Tera2 PCoIP Zero Clients. After configuring your View Connection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

VMware Horizon Connections

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

OSD: Auto Detect Session Settings

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



OSD session connection type – Auto Retect

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

OSD Auto Detect Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this server, it will appear in the Server drop-down list on the OSD Connect page if the Tera2 PCoIP Zero Client is configured to cache servers.



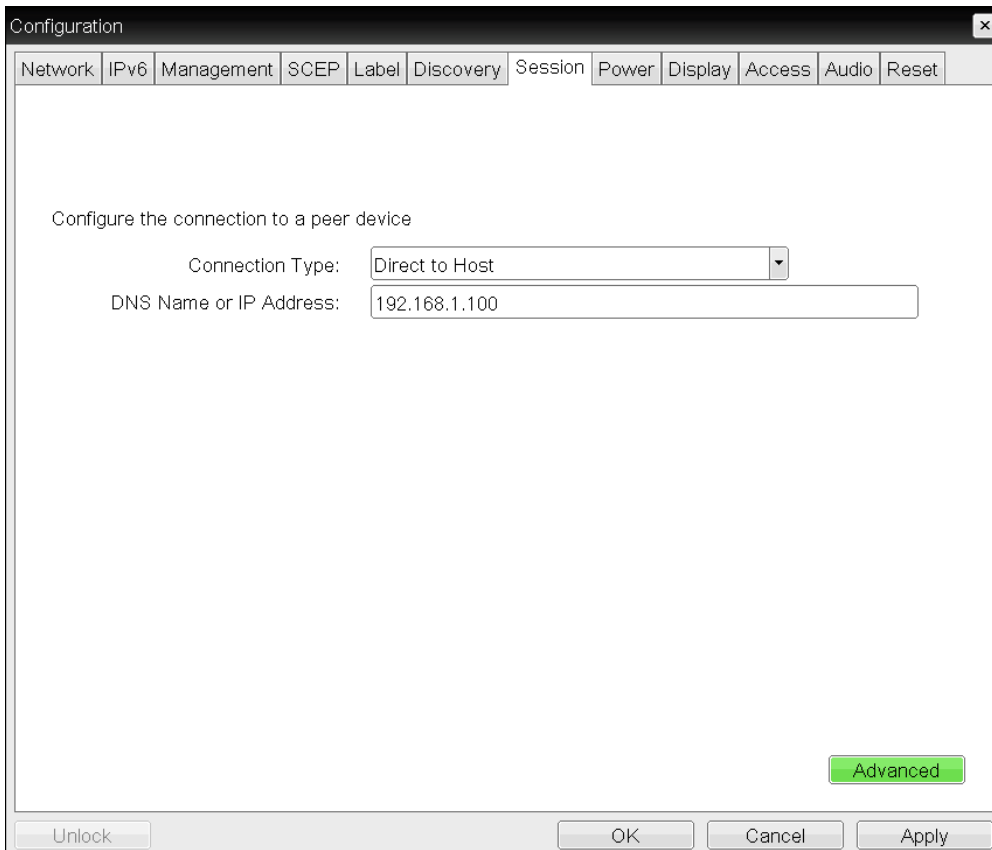
Note: Type the URL in the form 'https://<hostname|IP address>'.

The URL must be in the form 'https://<hostname|IP address>'.

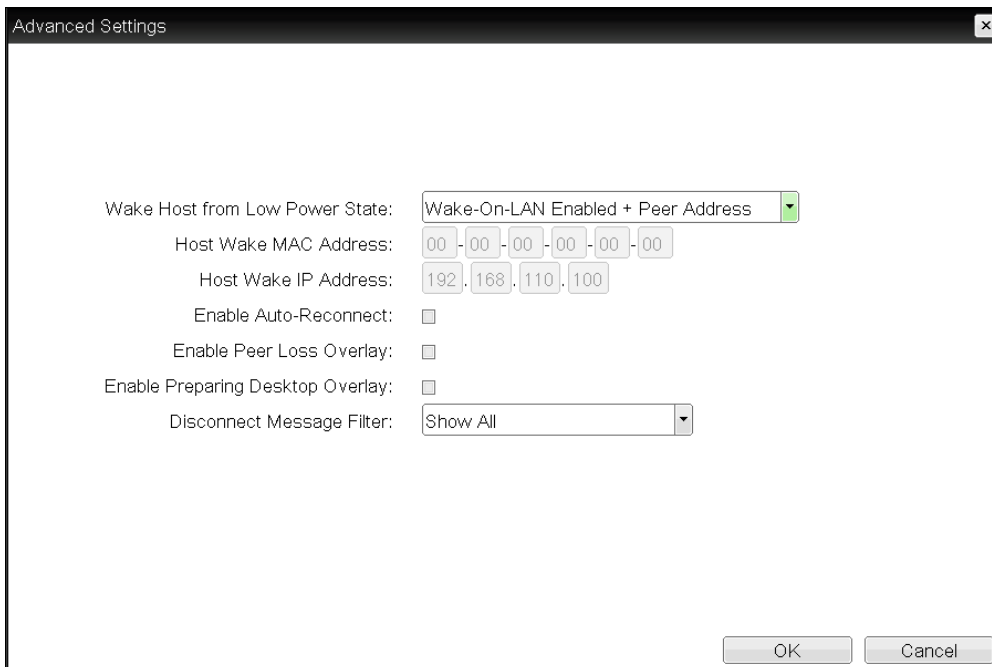
OSD: Direct to Host Session Settings

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


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

OSD Direct to Host Parameters

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the host.
Wake Host from Low Power State	<p>Select whether to use the PCoIP Remote Workstation Card's MAC and IP address or a custom MAC and IP address when configuring the Wake-On-LAN feature on a client. This feature wakes up the host when the user presses the client's host PC button or clicks the Connect button on the Connect window.</p> <ul style="list-style-type: none"> • Wake-On-LAN Enabled + Peer Address: After you have successfully connected to the PCoIP Remote Workstation Card, both the card's MAC address and IP address are automatically populated in the Host Wake MAC Address and Host Wake IP Address fields. • Wake-On-LAN Enabled + Custom Address: When selected, enables you to manually enter the MAC address and IP address of the device you want to wake up. <p> Note: MAC and IP address of the host PC's network interface card (NIC) will automatically be populated in certain situations</p> <p>If the host software is installed in the host PC and the Use host PC NIC for Wake-on-LAN setting is enabled in the Features > Power Management section of the host software GUI, the MAC address and IP address of the host PC's network interface card (NIC) will automatically be populated in the Host Wake MAC Address and Host Wake IP Address fields.</p> <p> Note: Hardware host must support waking from low power state</p> <p>The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet.</p> <p> Note: Disabling the Wake-On-LAN feature</p> <p>You can disable the Wake-On-LAN feature from the AWI Power page.</p>
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.

Parameters	Description
Host Wake IP Address	Enter the host's IP address to complete the host wake up configuration when Wake-On-LAN Enabled + Custom Address is selected. The client will send a 'magic packet' to this IP address to wake the host computer from a low power state.
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	<p>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.</p> <div data-bbox="516 709 613 814" style="float: left; margin-right: 10px;"> </div> <p>Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <div data-bbox="516 1029 613 1134" style="float: left; margin-right: 10px;"> </div> <p>Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

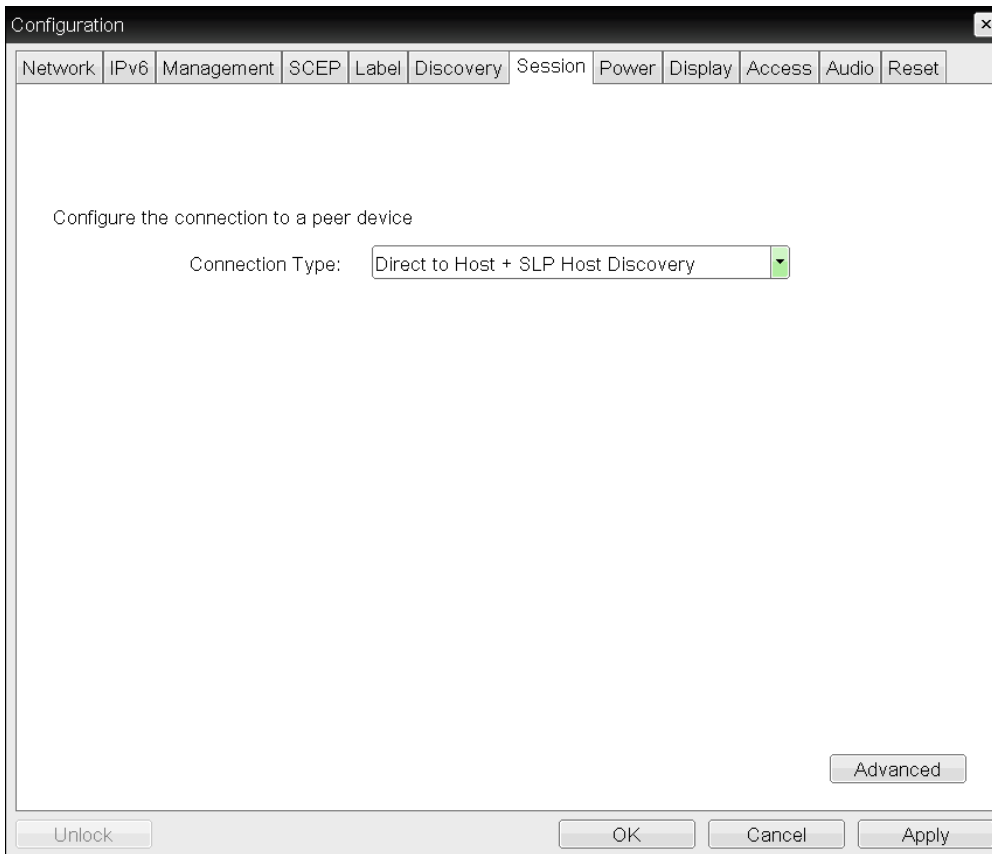
Parameters	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameters	Description
	<ul style="list-style-type: none"> • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div style="margin-top: 10px;">  <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> </div> <p>You can choose to display:</p> <ol style="list-style-type: none"> 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.

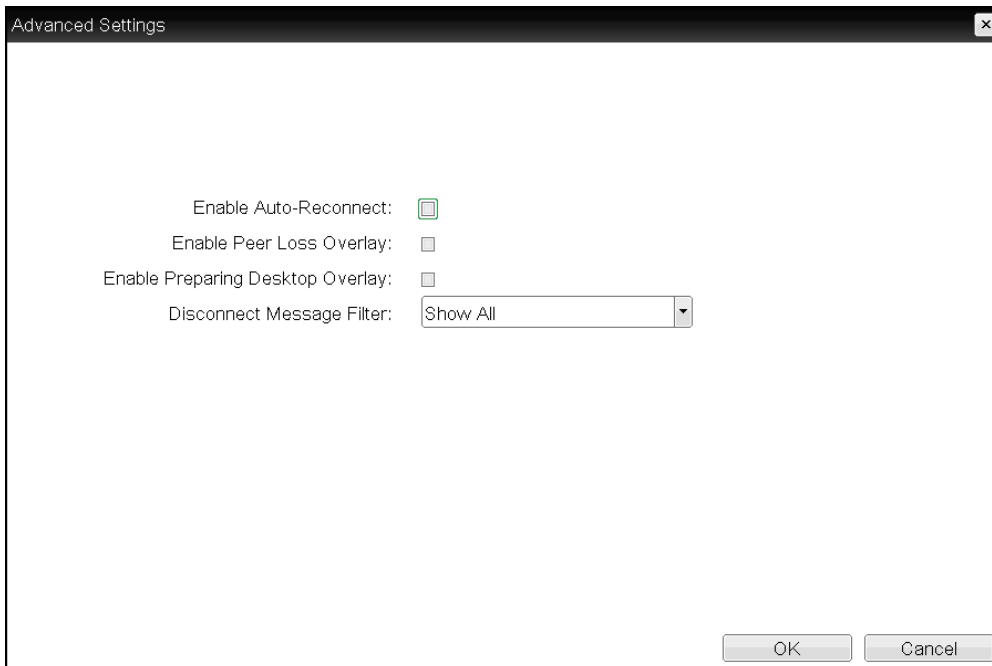
OSD: Direct to Host + SLP Host Discovery Session Settings

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

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

OSD Direct to Host + SLP Host Discovery Parameters

Parameters	Description
Enable Auto-Reconnect	When enabled, lets the client automatically reconnect with the last connected host when a session is lost.
Enable Peer Loss Overlay	<p>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.</p> <div data-bbox="537 604 639 705" style="float: left; margin-right: 10px;">  </div> <p>Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <div data-bbox="537 924 639 1024" style="float: left; margin-right: 10px;">  </div> <p>Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

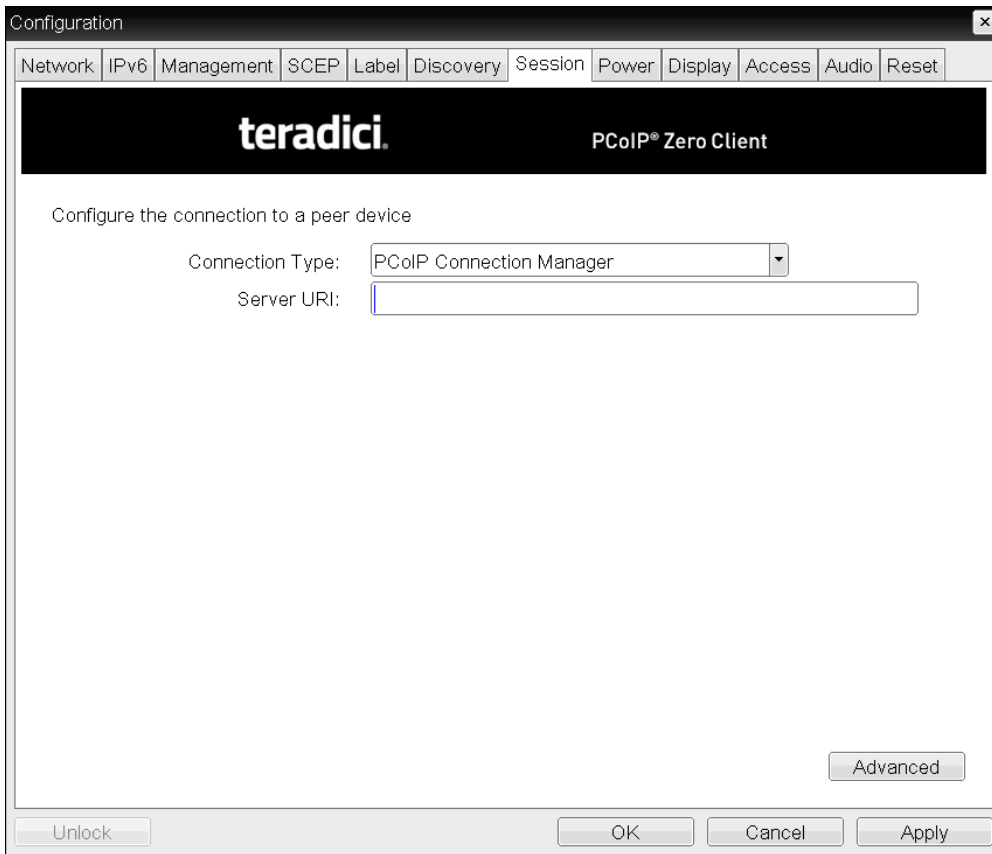
Parameters	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameters	Description
	<ul style="list-style-type: none"> • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div style="margin-top: 10px;">  <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> </div> <p>You can choose to display:</p> <ol style="list-style-type: none"> 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.

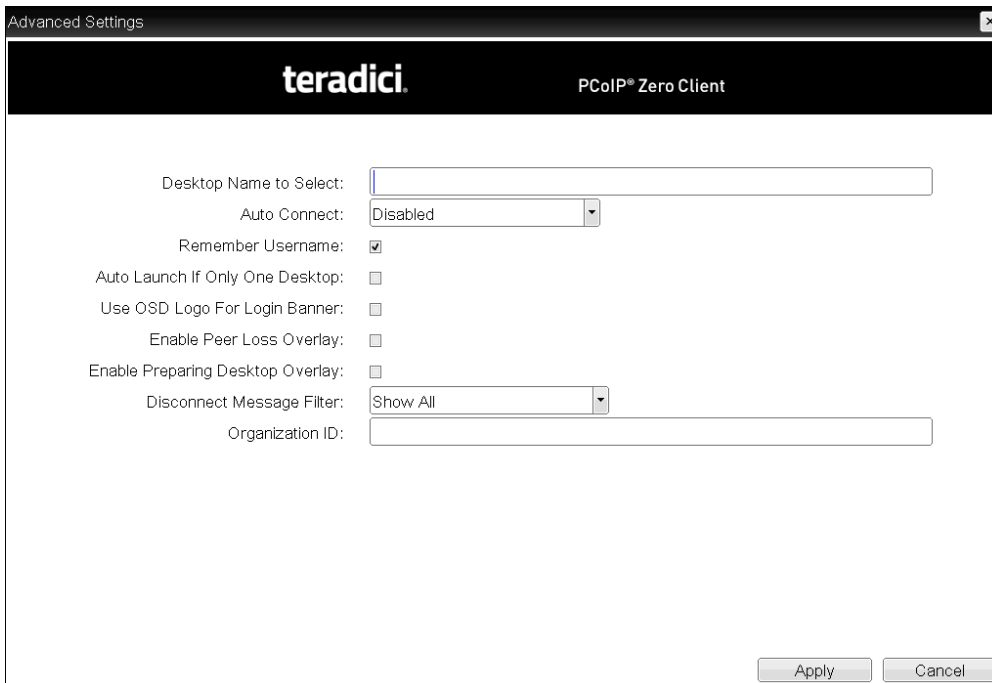
OSD: PCoIP Connection Manager Session Settings

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

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

OSD PCoIP Connection Manager Parameters

Parameter	Description
Server URI	<p>Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.</p> <p> Note: Type the URL in the form 'https://<hostname IP address>'. The URL must be in the form 'https://<hostname IP address>'.</p>
Desktop Name to Select	<p>Enter the desktop name used by the client when starting a session.</p>
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart the client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Remember Username	<p>When enabled, the user name text box automatically populates with the last username entered.</p>

Parameter	Description
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p> Note: Feature applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="532 552 636 653" style="float: left; margin-right: 10px;"> </div> <div data-bbox="643 552 1177 667"> <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> </div> <p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. Show None – Don't show any disconnect messages.

Organization ID

Enter an organization ID for the company (for example, 'mycompany.com'). This field accepts any UTF-8 character.



Note: Specify parameter if the PCoIP Connection Manager requests it

You only need to specify this parameter if the PCoIP Connection Manager requests it. The organization ID is used for certain types of PCoIP Broker Protocol authentication messages.

OSD: PCoIP Connection Manager + Auto-Logon Session Settings

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

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



Caution: Take precautions to secure zero clients

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

Configuration

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

teradici PCoIP® Zero Client

Configure the connection to a peer device

Connection Type: PCoIP Connection Manager + Auto-Logon

Server URI:

User name:

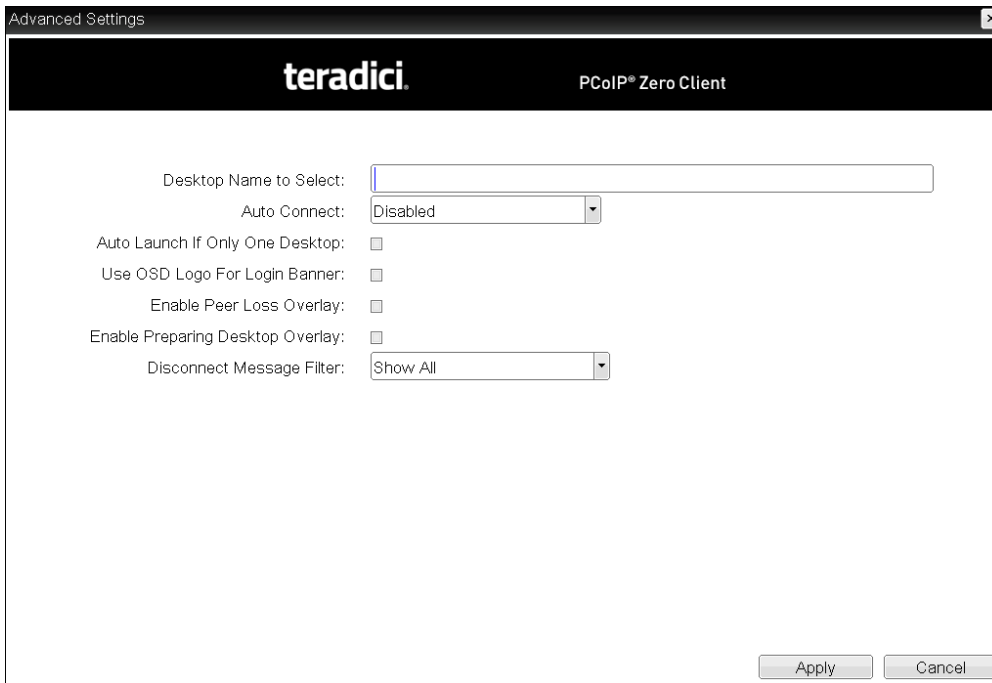
Password:

Domain:

Advanced

Unlock OK Cancel Apply


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






Advanced Settings

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


OSD PCoIP Connection Manager + Auto-Logon Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.
	 <p>Note: Type the URL in the form 'https://<hostname IP address>'. The URL must be in the form 'https://<hostname IP address>'.</p>
User name	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Domain	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.

Parameter	Description
Desktop Name to Select	Enter the desktop name used by the client when starting a session.
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart the client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p> Note: Feature applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.

Parameter	Description
<p>Enable Peer Loss Overlay</p>	<p>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.</p> <div data-bbox="535 472 641 577"> </div> <p>Note: Option only available for a Tera2 PCoIP Zero Client</p> <p>This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
<p>Enable Preparing Desktop Overlay</p>	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <div data-bbox="535 787 641 892"> </div> <p>Note: Preparing Desktop overlay provides notification that login is proceeding</p> <p>This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. Show None – Don't show any disconnect messages.

OSD: View Connection Server Session Settings

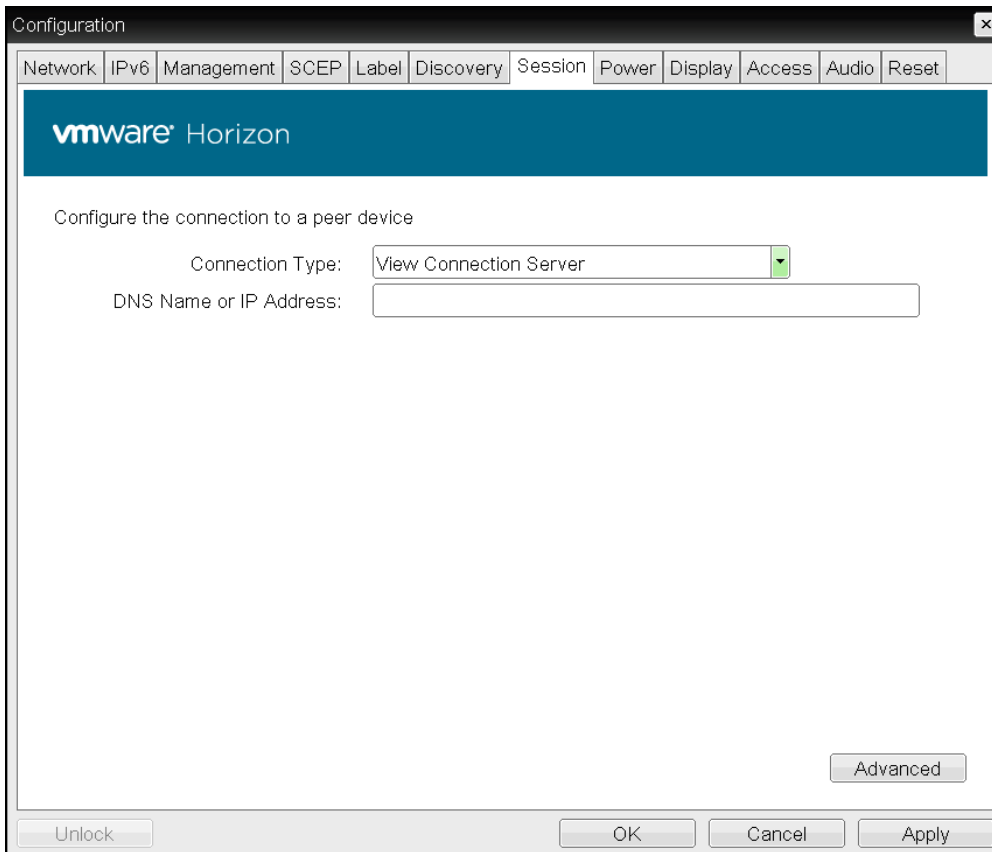
Select the **View Connection Server** session connection type from the **Options > Configuration > Session** page to configure a client to use a View Connection Server as the broker when connecting to a VMware desktop.



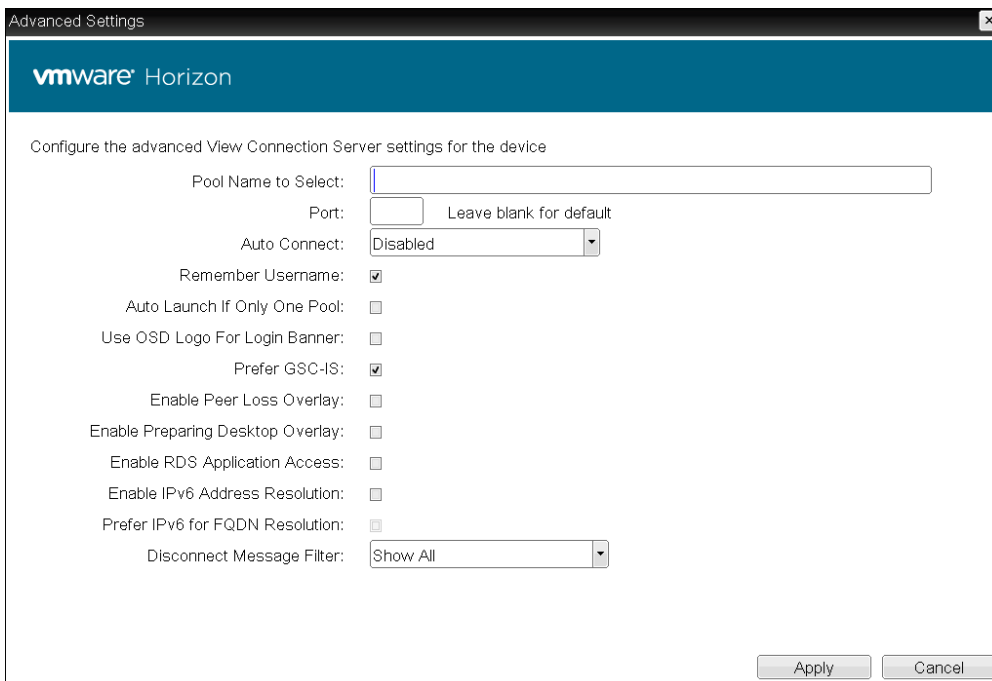
Note: Connecting a View Connection Server to a workstation

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

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






OSD Session connection type – View Connection Server







Advanced Settings

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


OSD View Connection Server Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool. <div style="margin-top: 10px;">  <p>Note: Field is case-insensitive This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p> </div>
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: <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <div style="margin-top: 10px;">  <p>Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> </div> <div style="margin-top: 10px;">  <p>Note: Restart the client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p> </div>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.

Parameter	Description
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>For Tera1 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop.</p> <p> Note: Feature applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>
Prefer GSC-IS	<p>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.</p>
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

Parameter	Description
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p> </div>
Enable IPv6 Address Resolution	<p>This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.</p>
Prefer IPv6 for FQDN Resolution	<p>When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.</p>

Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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.



Caution: Take precautions to secure zero clients

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

The screenshot shows a 'Configuration' window with a tabbed interface. The 'Session' tab is selected. The window title is 'Configuration'. Below the tabs, there is a blue header with the VMware Horizon logo. The main content area is titled 'Configure the connection to a peer device'. It contains the following fields:

- Connection Type: View Connection Server + Auto-Logon (dropdown menu)
- DNS Name or IP Address: (text input field)
- User name: (text input field)
- Password: (text input field)
- Domain: (text input field)

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

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

The screenshot shows an 'Advanced Settings' window with a tabbed interface. The 'Session' tab is selected. The window title is 'Advanced Settings'. Below the tabs, there is a blue header with the VMware Horizon logo. The main content area is titled 'Configure the advanced View Connection Server settings for the device'. It contains the following settings:


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




At the bottom right of the main area are 'Apply' and 'Cancel' buttons.




Advanced Settings

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


OSD View Connection Server + Auto-Logon Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
User name	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Domain	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
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: Field is case-insensitive This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.

Parameter	Description
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart the client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>For Tera1 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop.</p> <p> Note: Feature only applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>

Parameter	Description
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p> Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p>
Enable IPv6 Address Resolution	<p>This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.</p>
Prefer IPv6 for FQDN Resolution	<p>When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.</p>

Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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.



Caution: Take precautions to secure zero clients

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

The screenshot shows the 'Configuration' window for VMware Horizon. The 'Session' tab is selected. The main heading is 'vmware Horizon'. Below it, the instruction reads 'Configure the connection to a peer device'. The 'Connection Type' is set to 'View Connection Server + Kiosk'. The 'DNS Name or IP Address' field is empty. The 'Zero Client MAC' radio button is selected, and the 'Username' field contains 'CM-02:50:56:97:27:92'. The 'Password' field is empty. At the bottom right, there is an 'Advanced' button. At the very bottom of the window are 'Unlock', 'OK', 'Cancel', and 'Apply' buttons.

OSD Session connection type – View Connection Server + Kiosk

The screenshot shows the 'Advanced Settings' window for VMware Horizon. The main heading is 'vmware Horizon'. Below it, the instruction reads 'Configure the advanced View Connection Server settings for the device'. The 'Port' field is empty with the text 'Leave blank for default' next to it. There are several checkboxes: 'Use OSD Logo For Login Banner', 'Enable Peer Loss Overlay', 'Enable Preparing Desktop Overlay', 'Enable RDS Application Access', 'Enable IPv6 Address Resolution', and 'Prefer IPv6 for FQDN Resolution', all of which are currently unchecked. The 'Disconnect Message Filter' dropdown menu is set to 'Show All'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Advanced Settings

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



OSD View Connection Server + Kiosk Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username	<p>Select the type of user name that matches the naming you use for the devices on the View Connection Server.</p> <ul style="list-style-type: none"> • Zero Client MAC: Select this option to automatically populate the Username field with the MAC address of the Tera2 PCoIP Zero Client. • Custom: Enter the user name for the Tera2 PCoIP Zero Client. This user name has the prefix 'Custom'. <p>When Custom is selected as the user name type, enter the value for this component of the custom user name. This field is limited to 13 characters.</p>
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.




Note: Option only available for a Tera2 PCoIP Zero Client

This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.

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

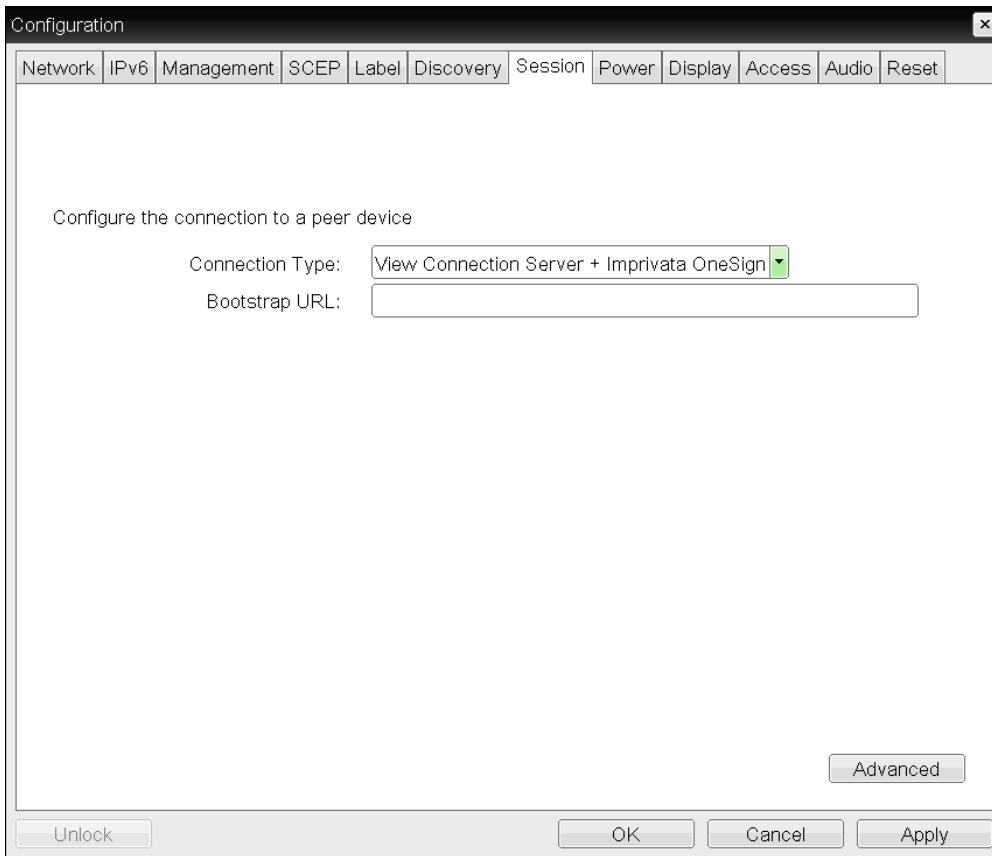
Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. Show None – Don't show any disconnect messages.

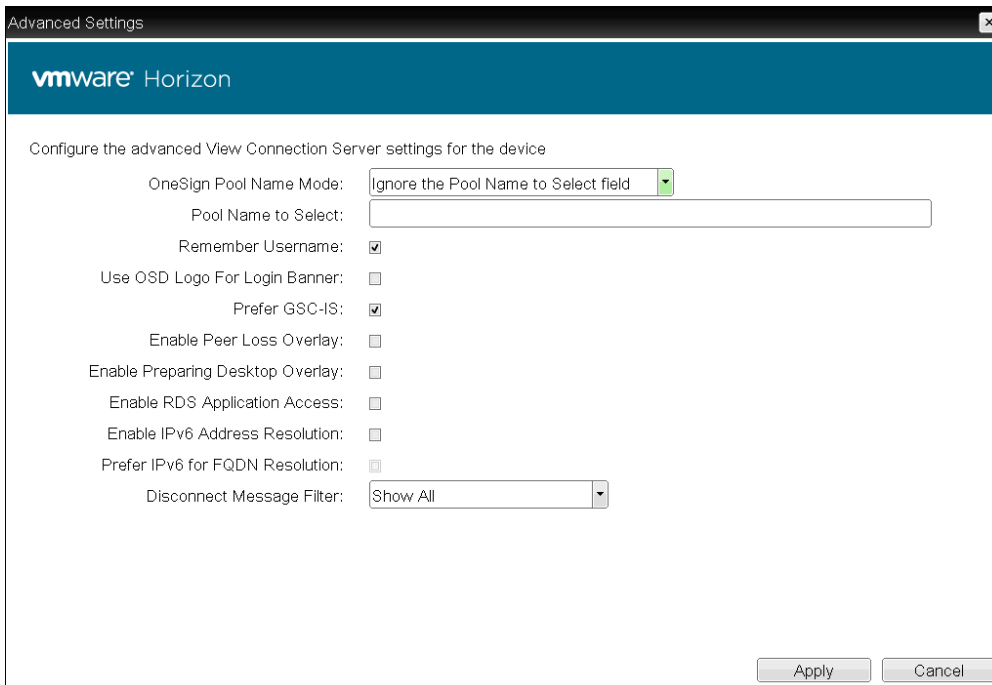
OSD: View Connection Server + Imprivata OneSign Session Settings

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


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

OSD View Connection Server + Imprivata OneSign Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	<p>Select whether the Pool Name to Select property is used in OneSign mode.</p> <ul style="list-style-type: none"> • Ignore the Pool Name to Select field • Use the Pool Name to Select field if set <p>For Tera1 PCoIP Zero Clients, this parameter is called OneSign Desktop Name Mode.</p>
Pool Name to Select	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <p> Note: Field is case-insensitive This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>

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

Parameter	Description
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. Show None – Don't show any disconnect messages.

AWI: Auto Detect Session Settings

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

Session
Configure the connection to a device

Session Connection Type:

Server URI:

AWI Session connection type – Auto Detect

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

AWI Auto Detect Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this server, it will appear in the Server drop-down list on the OSD Connect page if the Tera2 PCoIP Zero Client is configured to cache servers.



**Note: Type the URL in the form 'https://<hostname|IP address>'.
The URL must be in the form 'https://<hostname|IP address>'.**

AWI: Direct to Host Session Settings

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

Session

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 10.0.34.207

Hide Advanced Options

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

Host Wake MAC Address: 00-30-04-0E-8F-A2

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All

Enable DSCP:

Enable Congestion Notification:

Apply Cancel

AWI Session connection type – Direct to Host


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

AWI Direct to Host Parameters


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

Parameters	Description
<p>Wake Host from Low Power State</p>	<p>Select whether to use the PCoIP Remote Workstation Card's MAC and IP address or a custom MAC and IP address when configuring the Wake-On-LAN feature on a client. This feature wakes up the host when the user presses the client's host PC button or clicks the Connect button on the Connect window.</p> <ul style="list-style-type: none"> • Wake-On-LAN Enabled + Peer Address: After you have successfully connected to the PCoIP Remote Workstation Card, both the card's MAC address and IP address are automatically populated in the Host Wake MAC Address and Host Wake IP Address fields. • Wake-On-LAN Enabled + Custom Address: When selected, enables you to manually enter the MAC address and IP address of the device you want to wake up. <div data-bbox="576 787 673 882" style="float: left; margin-right: 10px;"> </div> <p>Note: MAC and IP address of the host PC's network interface card (NIC) will automatically be populated in certain situations</p> <p>If the host software is installed in the host PC and the Use host PC NIC for Wake-on-LAN setting is enabled in the Features > Power Management section of the host software GUI, the MAC address and IP address of the host PC's network interface card (NIC) will automatically be populated in the Host Wake MAC Address and Host Wake IP Address fields.</p> <div data-bbox="535 1186 633 1281" style="float: left; margin-right: 10px;"> </div> <p>Note: Hardware host must support waking from low power state</p> <p>The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet.</p> <div data-bbox="535 1386 633 1480" style="float: left; margin-right: 10px;"> </div> <p>Note: Disabling the Wake-On-LAN feature</p> <p>You can disable the Wake-On-LAN feature from the AWI Power page.</p>
<p>Host Wake MAC Address</p>	<p>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.</p>
<p>Host Wake IP Address</p>	<p>Enter the host's IP address to complete the host wake up configuration when Wake-On-LAN Enabled + Custom Address is selected. The client will send a 'magic packet' to this IP address to wake the host computer from a low power state..</p>

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	<p>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.</p> <div data-bbox="537 562 638 659"> </div> <p>Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <div data-bbox="537 877 638 974"> </div> <p>Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>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.</p> <div data-bbox="537 1234 638 1331"> </div> <p>Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>

Parameters	Description
<p>PCoIP Utility Bar Mode</p>	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <div style="border: 1px solid #00a0c0; padding: 5px; margin-top: 10px;">  <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p> </div>
<p>Session Negotiation Cipher Suites</p>	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameters	Description
	<ul style="list-style-type: none"> • You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div style="margin-top: 10px;">  <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> </div> <p>You can choose to display:</p> <ol style="list-style-type: none"> 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, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .

AWI: Direct to Host + SLP Host Discovery Session Settings

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

Session

Configure the connection to a device

Session Connection Type: Direct to Host + SLP Host Discovery

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All



Enable DSCP:



Enable Congestion Notification:

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

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

AWI Direct to Host + SLP Host Discovery Parameters

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.
	<div style="display: flex; align-items: flex-start;">  <div> <p>Note: Option only available for a Tera2 PCoIP Zero Client</p> <p>This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p> </div> </div>
Enable Preparing Desktop Overlay	When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.
	<div style="display: flex; align-items: flex-start;">  <div> <p>Note: Preparing Desktop overlay provides notification that login is proceeding</p> <p>This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p> </div> </div>

Parameters	Description
Enable Session Disconnect Hotkey	<p>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.</p> <div data-bbox="537 474 639 573" style="float: left; margin-right: 10px;">  </div> <p>Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <div data-bbox="537 1302 639 1400" style="float: left; margin-right: 10px;">  </div> <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
<p>Disconnect Message Filter</p>	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameters	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="537 552 639 653" style="float: left; margin-right: 10px;"> </div> <p data-bbox="646 552 1169 581">Related Information: Session disconnect codes</p> <p data-bbox="646 583 1179 665">For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> <p data-bbox="532 726 821 756">You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .

AWI: PCoIP Connection Manager Session Settings

Select the **PCoIP Connection Manager** session connection type from the **Configuration > Session** page to configure the client to use a PCoIP Connection Manager as the PCoIP session broker.

Session
Configure the connection to a device

Session Connection Type: PCoIP Connection Manager

Server URI: https://1terwkstn90.teradici.local

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers

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

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used

Enable Self Help Link:

Auto Launch If Only One Desktop:

Remember Username:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All

Enable DSCP:


Enable Congestion Notification:



Organization ID:




AWI Session connection type – PCoIP Connection Manager




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

AWI PCoIP Connection Manager Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.
<div style="display: flex; align-items: center;">  <p>Note: Type the URL in the form 'https://<hostname IP address>'. The URL must be in the form 'https://<hostname IP address>'.</p> </div>	
Desktop Name to Select	Enter the desktop name used by the client when starting a session. This field is case-insensitive.



Parameter	Description
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	<p>When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.</p>
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>

Parameter	Description
Connection Server Cache Mode	<p>This field determines whether a connection server is dynamically added to the Server drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select.</p> <ul style="list-style-type: none"> • Last servers used: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. • Read-only: Select this option if you want users to select a connection server from a read-only list. <p> Note: Use PCoIP Management Console to pre-populate available connection servers You can use the PCoIP Management Console to pre-populate the list of available connection servers.</p>
Enable Self Help Link	See Enabling the Self Help Link for details.
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p> Note: Feature only applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>

Parameter	Description
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <p> Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>

Parameter	Description
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
<p>Disconnect Message Filter</p>	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x402).

Parameter	Description
	<p>Contact your IT administrator for assistance.</p> <ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <p> Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> <p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .
Organization ID	Enter an organization ID for the company (for example, 'mycompany.com'). This field accepts any UTF-8 character.
	<p> Note: Specify parameter if the PCoIP Connection Manager requests it 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.</p>

Enabling the Self Help Link

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

automatically log users in to the desktop that you specify. You also configure the link text that you want to appear on the Connect window.

Enable Self Help Link:

Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Pool Name to Select:

Link Text:

Enable Self Help Link options

When you enable this field, the following options appear:

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

AWI: PCoIP Connection Manager + Auto-Logon Session Settings

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



Caution: Take precautions to secure zero clients

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

Session

Configure the connection to a device

Session Connection Type: PCoIP Connection Manager + Auto-Logon ▼

Server URI: https://1terwkstn90.teradici.local

Logon Username:

Logon Password:

Logon Domain Name:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers ▼

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

Auto Connect: Disabled ▼

Connection Server Cache Mode: Last servers used ▼

Auto Launch If Only One Desktop:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled ▼

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

Disconnect Message Filter: Show All ▼


Enable DSCP:




Enable Congestion Notification:





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


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

AWI PCoIP Connection Manager + Auto-Logon Parameters

Parameter	Description
Server URI	Enter the Uniform Resource Identifier (URI) for the PCoIP Connection Manager.
	 <p>Note: Type the URL in the form 'https://<hostname IP address>'. The URL must be in the form 'https://<hostname IP address>'.</p>
Logon Username	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Logon Domain Name	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Desktop Name to Select	Enter the desktop name used by the client when starting a session. This field is case-insensitive.
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.

Parameter	Description
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Connection Server Cache Mode	<p>This field determines whether a connection server is dynamically added to the Server drop-down menu on the OSD Connect page when a user types in a valid server URI, or whether it appears in a read-only list for the user to select.</p> <ul style="list-style-type: none"> • Last servers used: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. • Read-only: Select this option if you want users to select a connection server from a read-only list. <p> Note: Use PCoIP Management Console to pre-populate available connection servers You can use the PCoIP Management Console to pre-populate the list of available connection servers.</p>

Parameter	Description
Auto Launch If Only One Desktop	<p>When enabled, users are automatically connected to a provisioned desktop after user credentials are entered.</p> <p> Note: Feature only applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>

Parameter	Description
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <div data-bbox="532 919 634 1020" style="border: 1px solid black; padding: 5px; width: 60px; height: 48px; margin-bottom: 5px;">  </div> <p>Note: Configure the feature from the PCoIP Management Console and AWI only</p> <p>This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="532 552 634 653" style="float: left; margin-right: 10px;"> </div> <p data-bbox="646 552 1166 579">Related Information: Session disconnect codes</p> <p data-bbox="646 583 1174 667">For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> <p data-bbox="532 728 816 756">You can choose to display:</p> <ol style="list-style-type: none"> <li data-bbox="532 779 1256 840">1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. <li data-bbox="532 850 1187 911">2. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. <li data-bbox="532 921 1261 982">3. Show Error Only – This option hides Info and Warning messages and displays only Error messages. <li data-bbox="532 993 1127 1020">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, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .

AWI: View Connection Server Session Settings

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



Note: Connecting a View Connection Server to a workstation

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

Session

Configure the connection to a device

Session Connection Type: View Connection Server

DNS Name or IP Address: view.teradici.com

Pool Name to Select:

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers:

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used

Enable Self Help Link:

Auto Launch If Only One Pool:

Remember Username:

Use OSD Logo For Login Banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:

Prefer IPv6 for FQDN Resolution:




AWI Session Connection type – View Connection Server




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




AWI View Connection Server Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.
<div style="display: flex; align-items: center;"> <div> <p>Note: Field is case-insensitive</p> <p>This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p> </div> </div>	

Parameter	Description
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.
Trusted View Connection Servers	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>

Parameter	Description
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Connection Server Cache Mode	<p>This field determines whether a connection server is dynamically added to the Server drop-down menu on the OSD Connect page when a user types in a valid server address, or whether it appears in a read-only list for the user to select.</p> <ul style="list-style-type: none"> • Last servers used: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. • Read-only: Select this option if you want users to select a connection server from a read-only list. <p> Note: Use PCoIP Management Console to pre-populate available connection servers You can use the PCoIP Management Console to pre-populate the list of available connection servers.</p>
Enable Self Help Link	See Enabling the Self Help Link for details.

Parameter	Description
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>For Tera2 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop.</p> <p> Note: Feature only applies to single desktop user This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Remember Username	<p>When enabled, the user name text box automatically populates with the last username entered.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>
Prefer GSC-IS	<p>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.</p>
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>

Parameter	Description
Enable Session Disconnect Hotkey	<p>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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p> Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p>
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <p> Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>

Parameter	Description
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="535 546 641 651" style="float: left; margin-right: 10px;"> </div> <p data-bbox="646 546 1169 577">Related Information: Session disconnect codes</p> <p data-bbox="646 577 1169 661">For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> <p data-bbox="535 724 812 756">You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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 TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

Enabling the Self Help Link

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

Enable Self Help Link:

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

AWI: View Connection Server + Auto-Logon Session Settings

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



Caution: Take precautions to secure zero clients

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

Session
Configure the connection to a device

Session Connection Type: View Connection Server + Auto-Logon

DNS Name or IP Address: view.teradici.com

Logon Username:

Logon Password:

Logon Domain Name:

Pool Name to Select:

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers:

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used

Auto Launch If Only One Pool:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:


Enable IPv6 Address Resolution:




Prefer IPv6 for FQDN Resolution:

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



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

AWI View Connection Server + Auto-Logon Parameters


Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address. For VMware Horizon DaaS, this is the DNS name or IP address of the VMware Horizon DaaS Desktop Portal.
Logon Username	Enter the user name for the client (maximum number of characters is 128). This user name will be sent to the specified connection server.
Logon Password	Enter the password for the client (maximum number of characters is 128). This password will be sent to the specified connection server.
Logon Domain Name	Enter the domain for the client (maximum number of characters is 256). This domain will be sent to the specified connection server.
Pool Name to Select	Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.
	 <p>Note: Field is case-insensitive This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p>
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.

Parameter	Description
Trusted View Connection Servers	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>
Auto Connect	<p>This field determines the client's auto connect behavior after startup:</p> <ul style="list-style-type: none"> • Enabled: The client automatically connects with the connection server after startup and a PCoIP session ends, bypassing the OSD Connect page. • Disabled: The client does not automatically connect with the connection server. • Enabled With Retry On Error: The client will continuously attempt to contact the connection server. After a connection failure, the client waits before attempting to connect again. This wait time increases with each successive failure. The wait interval is not configurable. <p> Note: Devices running 4.1.1 or lower do not support Retry On Error Devices running firmware 4.1.1 or lower do not support Retry On Error behavior and will always perform a single attempt to contact the connection server when this option is selected.</p> <p> Note: Restart client after enabling Auto Connect After enabling Auto Connect, the client must be power-cycled for the change to take effect.</p>
Connection Server Cache Mode	<p>This field determines whether a connection server is dynamically added to the Server drop-down menu on the OSD Connect page when a user types in a valid server address, or whether it appears in a read-only list for the user to select.</p> <ul style="list-style-type: none"> • Last servers used: Select this option if you want a list of cached servers that a user has typed in to appear in the Server drop-down menu on the OSD Connect page. • Read-only: Select this option if you want users to select a connection server from a read-only list. <p> Note: Use PCoIP Management Console to pre-populate available connection servers You can use the PCoIP Management Console to pre-populate the list of available connection servers.</p>

Parameter	Description
Auto Launch If Only One Pool	<p>When enabled, users are automatically connected to a provisioned desktop or application after user credentials are entered.</p> <p>For Tera2 PCoIP Zero Clients, this parameter is called Auto Launch If Only One Desktop.</p> <p> Note: Feature only applies to single desktop users This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
Use OSD Logo for Login Banner	<p>When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.</p>
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>

Parameter	Description
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p> Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p>
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <p> Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance.
	 <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p>
	<p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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 TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

AWI: View Connection Server + Kiosk Session Settings

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



Caution: Take precautions to secure zero clients

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

Session
Configure the connection to a device

Session Connection Type: View Connection Server + Kiosk

DNS Name or IP Address: view.teradici.com

Username Type: Zero Client MAC

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

Password:

Port: (Leave blank for default)

Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers:

Use OSD Logo For Login Banner:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

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

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:

Enable IPv6 Address Resolution:





Prefer IPv6 for FQDN Resolution:


AWI Session Connection type – View Connection Server + Kiosk

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

AWI View Connection Server + Kiosk Parameters

Parameter	Description
DNS Name or IP Address	Enter the View Connection Server's DNS name or IP address.
Username Type	<p>Select the type of user name that matches the naming you use for the devices on the View Connection Server.</p> <ul style="list-style-type: none"> • Zero Client MAC: Select this option to automatically populate the Username field with the MAC address of the Tera2 PCoIP Zero Client. • Custom: Enter the user name for the Tera2 PCoIP Zero Client. This user name has the prefix 'Custom'.
Username	When Custom is selected as the user name type, enter the value for this component of the custom user name. This field is limited to 13 characters.
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.
Port	By default, port 443 is used to communicate with the connection server. If your network is set up to use a non-standard port for secure connections, enter the port number.
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.
Trusted View Connection Servers	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>

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.
Enable Peer Loss Overlay	<p>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.</p> <p> Note: Option only available for a Tera2 PCoIP Zero Client This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>When enabled, users can press the <code>Ctrl+Alt+F12</code> 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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p> Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p>

Parameter	Description
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <div style="border: 1px solid #00a09a; padding: 5px; margin-top: 10px;">  <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p> </div>
Session Negotiation Cipher Suites	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="535 546 641 651" style="float: left; margin-right: 10px;"> </div> <p data-bbox="646 546 1169 577">Related Information: Session disconnect codes</p> <p data-bbox="646 577 1169 661">For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> <p data-bbox="535 724 812 756">You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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 TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

AWI: View Connection Server + Imprivata OneSign Session Settings

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

Session
Configure the connection to a device

Session Connection Type: View Connection Server + Imprivata OneSign

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

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

Pool Name to Select:

OneSign Appliance Verification: No verification: Connect to any appliance

Direct To View Address:

Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers:

Remember Username:

Use OSD Logo For Login Banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey: CTRL + ALT + F12

Enable RDS Application Access:

PCoIP Utility Bar Mode: Disabled

Pre-session Reader Beep: Use Existing Setting

Invert Wiegand Data: Use Existing Setting

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

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

Disconnect Message Filter: Show All

Custom Session SNI:

Enable DSCP:

Enable Congestion Notification:


Enable IPv6 Address Resolution:


Prefer IPv6 for FQDN Resolution:




AWI Session Connection type – View Connection Server + Imprivata OneSign


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

AWI View Connection Server + Imprivata OneSign Parameters

Parameter	Description
Bootstrap URL	Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment.
OneSign Pool Name Mode	<p>Select whether the Pool Name to Select property is used in OneSign mode.</p> <ul style="list-style-type: none"> • Ignore the Pool Name to Select field • Use the Pool Name to Select field if set <p>For Tera1 PCoIP Zero Clients, this parameter is called OneSign Desktop Name Mode.</p>
Pool Name to Select	<p>Enter the pool name. When the list includes a pool with this name, the client will immediately start a session with that pool.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Field is case-insensitive This field is case-insensitive. For Tera1 PCoIP Zero Clients, this parameter is called Desktop Name to Select.</p> </div>
Onesign Appliance Verification	<p>Select the level of verification performed on the certificate presented by the OneSign appliance server:</p> <ul style="list-style-type: none"> • No verification: Connect to any appliance • Full verification: Only connect to appliances with verified certificates
Direct To View Address	Enter the address of the View Connection Server to use when OneSign servers cannot be reached. When configured, a Direct to View link occurs on the OSD Connect page and user authentication screens. When users click the link, it cancels the current OneSign connection or authentication flow and starts a Horizon View authentication flow instead. This feature provides a mechanism for OneSign PCoIP Zero Client users to access their View desktops when the OneSign infrastructure is unavailable.

Parameter	Description
Certificate Check Mode	<p>Select the level of verification performed on the certificate presented by the connection server:</p> <ul style="list-style-type: none"> • Never connect to untrusted servers: Configure the client to reject the connection if a trusted, valid certificate is not installed. (This is the most secure option.) • Warn before connecting to untrusted servers: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the Tera2 PCoIP Zero Client trust store is empty. (This option is selected by default.) • Do not verify server identity certificates: Configure the client to enable all connections. (This option is not secure.)
Certificate Check Mode Lockout	When enabled, prevents users from changing the Certificate Check Mode settings from the OSD or AWI.
Trusted View Connection Servers	<p>Click the Show button to display View Connection Servers for which the client has received a valid certificate.</p> <p>Click the Clear button to clear this cache.</p>
Remember Username	When enabled, the user name text box automatically populates with the last username entered.
Use OSD Logo for Login Banner	When enabled, the OSD logo banner appears at the top of login screens in place of the default banner.
Prefer GSC-IS	When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions.
Enable Peer Loss Overlay	When enabled, the 'Network Connection Lost' overlay appears on the display(s) when a loss of network connectivity is detected. Normal hypervisor scheduling delays can falsely trigger this message.
	<p> Note: Option only available for a Tera2 PCoIP Zero Client</p> <p>This option is only available for a Tera2 PCoIP Zero Client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or PCoIP Management Console.</p>

Parameter	Description
Enable Preparing Desktop Overlay	<p>When enabled, the 'Preparing Desktop' overlay appears on the display(s) when users log in.</p> <p> Note: Preparing Desktop overlay provides notification that login is proceeding This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear.</p>
Enable Session Disconnect Hotkey	<p>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.</p> <p> Note: Set up configuration options before using hotkey Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session on page 26 for details.</p>
Enable RDS Application Access	<p>When enabled <i>and</i> users connect to a VMware Horizon View Connection Server that offers applications, a list of available applications will be presented.</p> <p> Note: Applications open in full-screen mode but can be resized Applications open in full-screen mode, but can be resized once users are in session.</p>

Parameter	Description
PCoIP Utility Bar Mode	<p>When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged).</p> <ul style="list-style-type: none"> • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. <div style="border: 1px solid #00a09a; padding: 5px; margin-top: 10px;">  <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p> </div>
Pre-session Reader Beep	<p>Configure whether the proximity card reader beeps when a valid card is tapped on the reader in OneSign mode:</p> <ul style="list-style-type: none"> • 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)

Parameter	Description
<p>Invert Wiegand Data</p>	<p>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.</p> <ul style="list-style-type: none"> • 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). <div data-bbox="537 730 639 827"> </div> <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
<p>Restrict Proximity Cards</p>	<p>Configure whether or not proximity cards are restricted to tap-in/tap-out only.</p> <p>When this feature is enabled, the proximity card reader is locally terminated (that is, it uses drivers in the client's firmware), and proximity cards can only be used for tap-in/tap-out.</p> <p>When this feature is disabled, the proximity card reader is bridged by default (that is, it uses drivers in the host OS), and proximity cards are not restricted. They can be used for tap-in/tap-out and also during a session—for example, when an application requires in-session authentication.</p> <ul style="list-style-type: none"> • Only use proximity cards for tap-in/tap-out: Enables/disables the feature. <div data-bbox="537 1392 639 1488"> </div> <p>Note: Configure the feature from the PCoIP Management Console and AWI only This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.</p>
<p>Session Negotiation Cipher Suites</p>	<p>Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host.</p> <ul style="list-style-type: none"> • Maximum Compatibility: TLS 1.0 or higher with RSA keys: 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
<p>Disconnect Message Filter</p>	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User- or administrator-initiated actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because you logged in from another location or your host was shut down or restarted. • You have been disconnected because an administrator disconnected you. • You have been disconnected because you logged in from another location. • You have been disconnected because you disconnected from your workstation. <p>Warning: System-initiated, but expected actions affecting the session:</p> <ul style="list-style-type: none"> • You have been disconnected because your session timed out. <p>Error: Unexpected system-initiated actions causing session to fail:</p> <ul style="list-style-type: none"> • You have been disconnected. • Unable to connect (0x1001). Contact your IT administrator. • Unable to connect (0x1002). Contact your IT administrator. • Session closed remotely. • Session closed remotely (unknown cause). • You have been disconnected due to a configuration error (0x100). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x201). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x300). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x301). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x302). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x303). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x305). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x400). Contact your IT administrator for assistance. • You have been disconnected due to a configuration error (0x401). Contact your IT administrator for assistance.

Parameter	Description
	<ul style="list-style-type: none"> You have been disconnected due to a configuration error (0x402). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x403). Contact your IT administrator for assistance. You have been disconnected due to a configuration error (0x404). Contact your IT administrator for assistance. <div data-bbox="535 546 641 651" style="float: left; margin-right: 10px;"> </div> <div data-bbox="646 546 1177 661"> <p>Related Information: Session disconnect codes For detailed information about the session disconnect codes, see What do the PCoIP server log disconnect codes mean? (KB 15134-872).</p> </div> <p>You can choose to display:</p> <ol style="list-style-type: none"> Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. Show Error and Warnings Only – This option hides info messages and displays only Error and Warning messages. Show Error Only – This option hides Info and Warning messages and displays only Error messages. 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 TLS HELLO when the client initiates a connection with the host.
Enable DSCP	When enabled, the device populates the Differentiated Services Code Point (DSCP) field in the IP header, enabling intermediate network nodes to prioritize PCoIP traffic accordingly.
Enable Congestion Notification	When enabled, transport congestion notification is enabled to enable PCoIP endpoints to react accordingly if an intermediate network node sets the congestion notification bit in either the IP header or PCoIP transport header. For more information about the PCoIP transport header, see PCoIP Packet Format on page 308 .
Enable IPv6 Address Resolution	This setting supports VMware Horizon View 6.1 implementations, which enable View-brokered IPv6 sessions on IPv6-only networks. When enabled, clients can advertise IPv6 and FQDN capability to the View connection Server and receive IPv6 and FQDN peer addresses back.
Prefer IPv6 for FQDN Resolution	When enabled, the client's IPv6 address is preferred for FQDN resolution when the client requests a session.

Configuring Session Bandwidth

AWI: Bandwidth Settings

The settings on this page let you control the bandwidth used by a device 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: kbps (0 = no limit)

Device Bandwidth Target: kbps (0 = disabled)



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

AWI Bandwidth page

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

AWI Bandwidth Parameters

Parameter	Description
Device Bandwidth Limit	<p>Enter the maximum bandwidth peak from the client to the host (for example, USB data).</p> <p>The usable range of the device bandwidth is 1,000 to 220,000 Kbps for Tera1 devices and 1,000 to 600,000 Kbps for Tera2 devices.</p> <p>The PCoIP processor only uses the required bandwidth up to the Device Bandwidth Limit maximum, and dynamically adjusts the bandwidth in response to network congestion. Setting this field to 0 configures the PCoIP processor to use the maximum rate available in the network at any time.</p> <p>We recommend setting this field to the limit of the network connected to the client and host.</p> <div data-bbox="537 793 638 894"> </div> <p>Note: Values rounded to the nearest megabit per second</p> <p>When applied to devices running firmware lower than 3.0, a value other than 0 is rounded to the nearest megabit per second, with a minimum value of 1 Mbps.</p>
Device Bandwidth Target	<p>Enter the temporary limit on the network bandwidth during periods of congestion. When the device detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it. This enables for a more even distribution of bandwidth between users sharing a congested network link.</p>

Parameter	Description
Device Bandwidth Floor	<p data-bbox="537 308 1240 464">Enter the minimum bandwidth when congestion is present and bandwidth is required. This enables you to optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor.</p> <p data-bbox="537 485 1252 546">This setting defines the minimum bandwidth from the client to the host (for example, USB data).</p> <p data-bbox="537 567 1273 688">A setting of 0 configures the PCoIP processor to reduce bandwidth to 1,000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value.</p> <div data-bbox="537 730 1192 1094">  <p data-bbox="646 730 1131 785">Note: Firmware implements algorithm that increases bandwidth</p> <p data-bbox="646 789 1192 1094">The firmware implements a slow-start algorithm that increases the bandwidth used until the required bandwidth is reached, network congestion is detected, or the Device Bandwidth Limit is met. It begins at the lesser of the Device Bandwidth Limit and 8,000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm enables a graceful session startup for low bandwidth scenarios (for example, WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.</p> </div> <div data-bbox="537 1157 1187 1299">  <p data-bbox="646 1157 1156 1211">Note: Values rounded to the nearest megabit per second</p> <p data-bbox="646 1215 1187 1299">When applied to devices running firmware lower than 3.0, a value other than 0 is rounded to the nearest megabit per second, with a minimum value of 1 Mbps.</p> </div>

Configuring Language

OSD: Help for Language Settings

OSD language settings are located in the OSD's [Region](#) page, which is accessed from the **Options > User Settings** menu.

AWI: 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:

Keyboard Layout:

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

AWI Language page

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

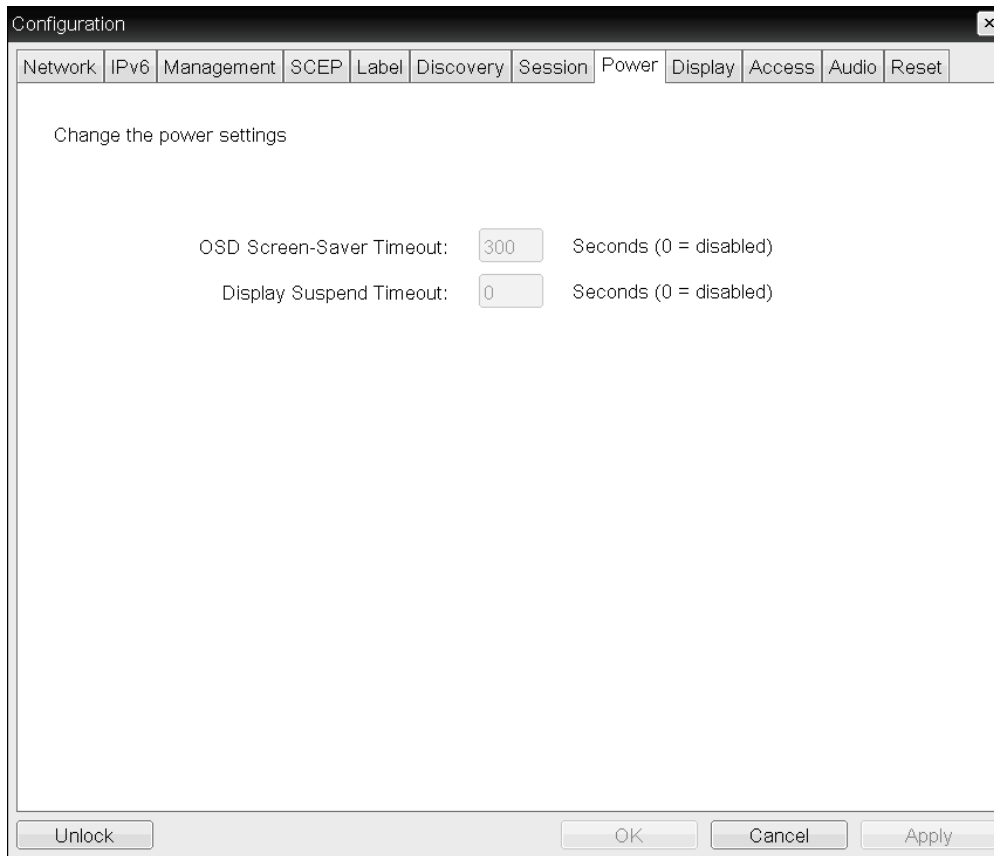
AWI Language Parameters

Parameter	Description
Language	Configure the language to use for the OSD user interface. 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 enable the keyboard layout setting, it is used during the user's session. If this GPO is not set to enable the setting, it is dropped.
OSD Region Tab Lockout	When selected, prevents users from changing the controls in the OSD Region tab.

Configuring Power Settings

OSD: Power Settings

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



OSD Power page

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



OSD Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 9999, or use 0 to disable the feature.



Note: Timeout only applies when the device is not in session

This timeout only applies when the device is *not* in session.

Parameter	Description
Display Suspend Timeout	<p>Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 14400 seconds, or use 0 to disable the feature.</p> <p> Note: Timeout only applies when the device is in session This timeout only applies when the device is in session.</p> <p> Note: Feature requires local mouse and keyboard When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.</p>

AWI: Power Permissions

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

Power

Change the power settings

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

Display Suspend Timeout: Seconds (0 = disabled)

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

Remote Host Power Control:

Power On After Power Loss:






Enable Wake-on-USB:


Enable Wake-on-LAN:

AWI Power page

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

AWI Power Parameters

Parameter	Description
OSD Screen-Saver Timeout	<p>Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 9999, or use 0 to disable the feature.</p> <p> Note: Timeout only applies when the device is not in session This timeout only applies when the device is <i>not</i> in session.</p>
Display Suspend Timeout	<p>Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client puts its attached displays into low power mode. Valid values are 10 to 14400 seconds, or use 0 to disable the feature.</p> <p> Note: Timeout only applies when the device is in session This timeout only applies when the device is in session.</p> <p> Note: Feature requires local mouse and keyboard When connected to a workstation, this feature requires Local Mouse and Keyboard to be enabled.</p>
Auto Power-Off Timeout	<p>Configure the number of seconds to wait after a period of inactivity (that is, no keyboard or mouse action) before the client powers down. Valid values are 60 to 28800 seconds, or use 0 to disable the power down.</p> <p> Note: PCoIP client must support powering off Non-zero values are only enabled when the PCoIP client supports powering off.</p> <p> Note: Timeout only applies when the device is not in session This timeout only applies when the device is <i>not</i> in session.</p>

Parameter	Description
Remote Host Power Control	<p>Configure the client's remote power setting.</p> <p>Select from the following options:</p> <ul style="list-style-type: none"> • Power-off not permitted: Users cannot remotely shut down the host PC from the Tera2 PCoIP Zero Client. When this option is selected, the Zero Client Control Panel on the OSD does not appear when the PCoIP Zero Client's connect/disconnect button is pressed. • Hard Power-off only: Users are able to remotely shut down the host from the Tera2 PCoIP Zero Client. When this option is selected, the Zero Client Control Panel on the OSD appears when the Tera2 PCoIP Zero Client's connect/disconnect button is pressed.
Power On After Power Loss	When enabled, the client automatically powers back on when power is supplied.
Enable Wake-on-USB	When enabled, configures the client to power up when the user presses a key on the keyboard. Wake-on-USB applies when the client is either powered off automatically or as a result of the user holding down the power button.
	 <p>Note: Clicking or moving mouse will not turn on client Clicking or moving the mouse will not power up the client when this feature is enabled.</p>
Enable Wake-on-LAN	When enabled, configures the client to wake up from a low power state when it receives Wake-on-LAN magic packets.

Configuring Image Quality

OSD: Help for Image Settings

OSD image settings are located in the OSD's Image page, which is accessed from the **Options > User Settings** menu.

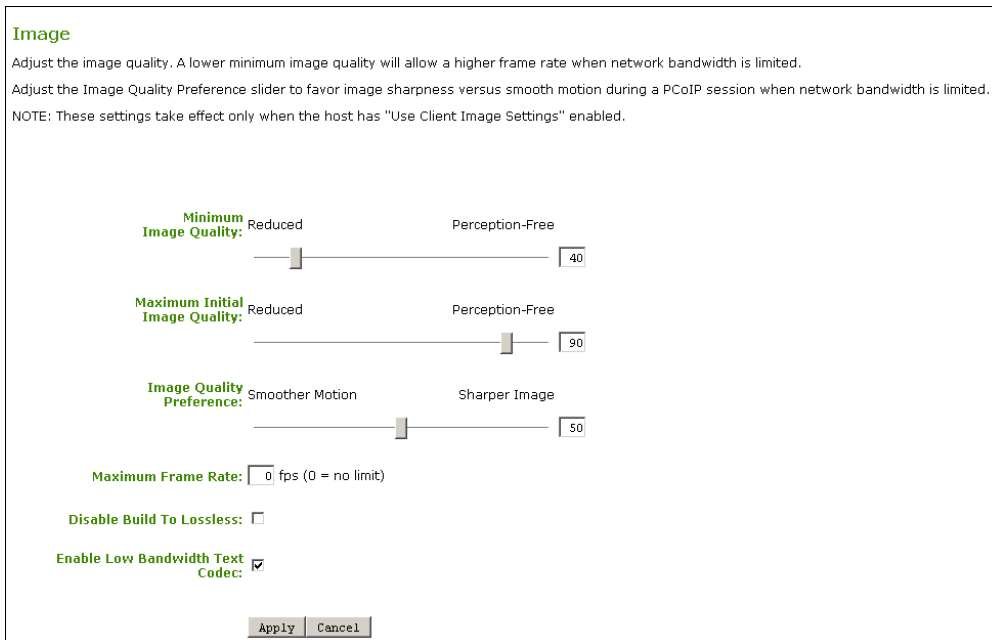
AWI: Image Settings

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: Setting only applies to sessions between zero clients and PCoIP Remote Workstation Cards

This setting applies only to sessions between Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards.




AWI Image page

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

AWI Image Parameters

Parameter	Description
Minimum Image Quality	<p>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.</p> <p>In environments where the network bandwidth is constrained, move the slider towards Reduced to enable higher frame rates. Move the slider towards Perception-Free to enable for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the Minimum Image Quality parameter.</p> <p>The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.</p>

Parameter	Description
<p>Maximum Initial Image Quality</p>	<p>Move the slider towards Reduced to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards Perception-Free to produce higher quality images but also higher bandwidth peaks.</p> <p>This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter.</p> <p>The Maximum Initial Image Quality must be greater than or equal to the Minimum Image Quality.</p>
<p>Image Quality Preference</p>	<p>Move the slider towards Smoother Motion to result in a higher frame rate at a lower quality level. Move the slider towards Sharper Image to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5.</p> <p>This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or lower.</p>
<p>Maximum Frame Rate</p>	<p>The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.</p>

Parameter	Description
Disable Build to Lossless	<p>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 (that is, identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.</p> <div style="border: 1px solid #800000; padding: 5px; margin-top: 10px;">  <p>Warning: Turning on Disable Build to Lossless field degrades images</p> <p>Turning on the Disable Build to Lossless field will degrade the image presented to the user by the Tera2 PCoIP Zero Client. Do not turn on this field unless it has been determined by the administrator of the Tera2 PCoIP Zero Client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the Tera2 PCoIP Zero Client administrator to make this determination.</p> <p>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.</p> </div> <p>This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or lower.</p>
Enable Low Bandwidth Text Codec (TERA2321 PCoIP Zero Clients only)	<p>When enabled, Low Bandwidth Text Codec Mode will be used for TERA2321 PCoIP Zero Clients.</p> <p>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.</p> <p>This option is disabled by default.</p>

Configuring Time Settings

OSD: Help for Time Settings

OSD time settings are located in the OSD's Region page, which is accessed from the **Options > User Settings** menu.

AWI: Time Settings

The Time page lets you configure Network Time Protocol (NTP) parameters to enable the device's event logs to be time-stamped based on NTP time.



Note: Server address overrides manually configured server

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



Note: NTP server does not provide time zone information

The device does not get time zone or Daylight Saving Time (DST) information from the NTP server.



Note: Enabling user events to correlate with log entries

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

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

Time ⏏

Change the local time configuration

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

Enable NTP:

Identify NTP Host by: IP address FQDN

NTP Host DNS Name:

NTP Host Port:

NTP Query Interval: ▾

Time Zone: ▾

Enable Daylight Saving Time:

AWI Time page

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

AWI Time Parameters

Parameter	Description
Current Time	Displays the time based on the NTP.
Enable NTP	Enable or disable the NTP feature.

Parameter	Description
Identify NTP Host by	<p>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.</p> <ul style="list-style-type: none"> • 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 Unified Communications

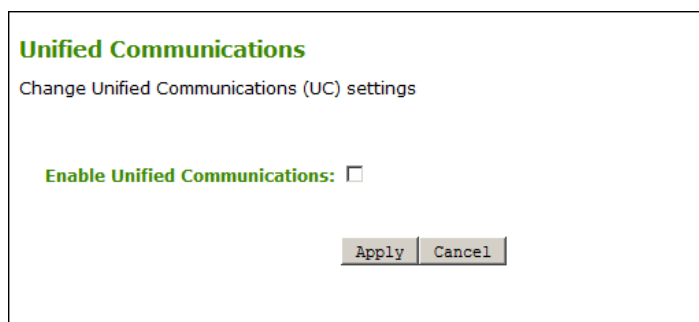
AWI: Unified Communications

The Unified Communications page lets you configure a Tera2 PCoIP 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: Capturing network packets

For details on how to capture network packets to help troubleshoot a Bria Virtualized Edition softphone call, see the [AWI: Packet Capture](#) page.



AWI Unified Communications page

The following parameters can be found on the AWI Unified Communications page.

AWI Unified Communications Parameters

Parameter	Description
Enable Unified Communications	When enabled, Tera2 PCoIP 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 a Password

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 from the MC. For details, see [PCoIP® Management Console 2.4 Administrators’ Guide](#).



Note: Parameter affects AWI and the local OSD GUI

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

The following parameters can be found on the OSD Change Password page.

OSD Change Password Parameters

Parameter	Description
Old Password	This field must match the current administrative password before you can update the password.
New Password	The new administrative password for both the AWI and the local OSD GUI.

Parameter	Description
Confirm New Password	This field must match the New Password field for the change to take place.
Reset	<p>If the client password becomes lost, you can click the Reset button to request a response code from the Tera2 PCoIP Zero Client vendor. The challenge code is sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password.</p> <p> Note: Contact client vendor for more information Contact the client vendor for more information when an authorized password reset is required. This option is not available through the AWI. It is only available through the OSD.</p>

AWI: Password Settings

The **Password** page lets you update the local administrative password for the device. You can access this page from the **Configuration > 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 from the MC. For details, see [PCoIP® Management Console 2.4 Administrators' Guide](#).



Note: Parameter affects AWI and the local OSD GUI

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.

teradici
PCoIP

Password

Change the local administrator password

Old Password:

New Password:


Confirm New Password:

AWI Password page

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

AWI Password Parameters

Parameter	Description
Old Password	This field must match the current administrative password before you can update the password.
New Password	The new administrative password for both the AWI and the local OSD GUI.
Confirm New Password	This field must match the New Password field for the change to take place.

Parameter	Description
Reset	<p>If the client password becomes lost, you can click the Reset button to request a response code from the PCoIP Zero Client vendor. The challenge code is sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password.</p> <div data-bbox="537 537 639 636" style="float: left; margin-right: 10px;">  </div> <p>Note: Contact the client vendor when an authorized password reset is needed Contact the client vendor for more information when an authorized password reset is required. This option is not available through the AWI. It is only available through the OSD.</p>

Configuring Reset Parameters

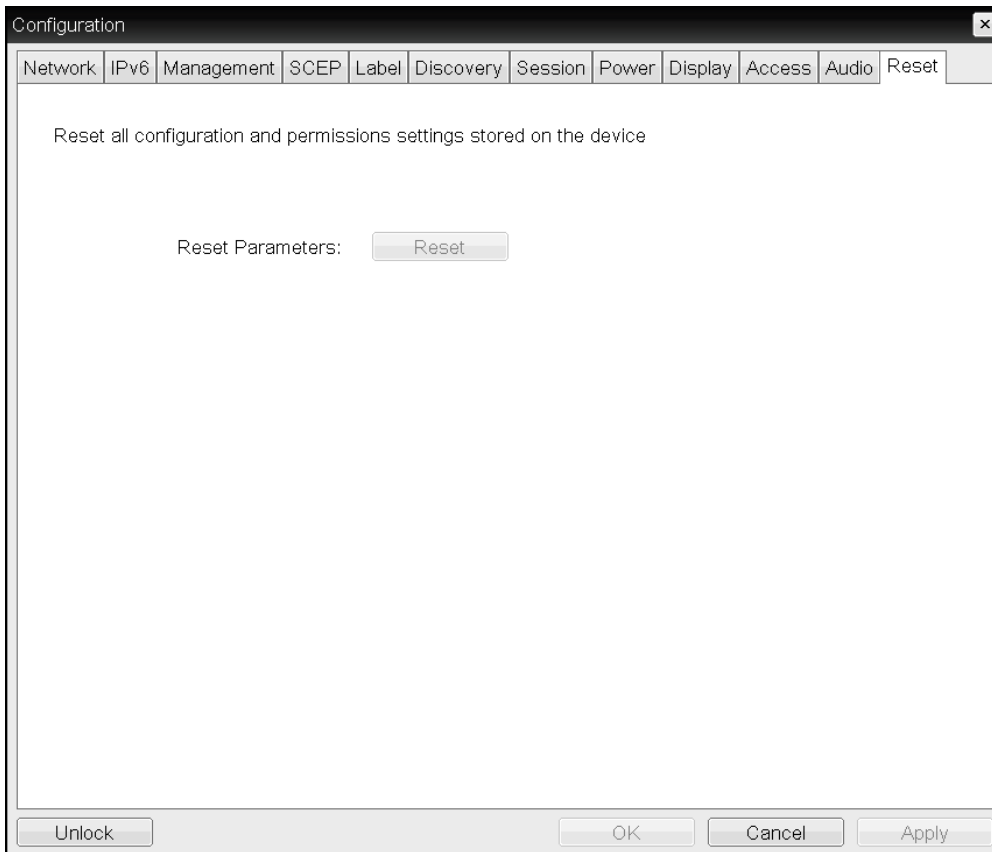
OSD: Reset Settings

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 does not revert the firmware

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



OSD Reset page

The following parameters can be found on the OSD Reset page.

OSD Reset Parameters

Parameter	Description
Reset Parameters	Resets parameters to factory default values stored in flash memory. When you click this button, a prompt appears for confirmation to prevent accidental resets.

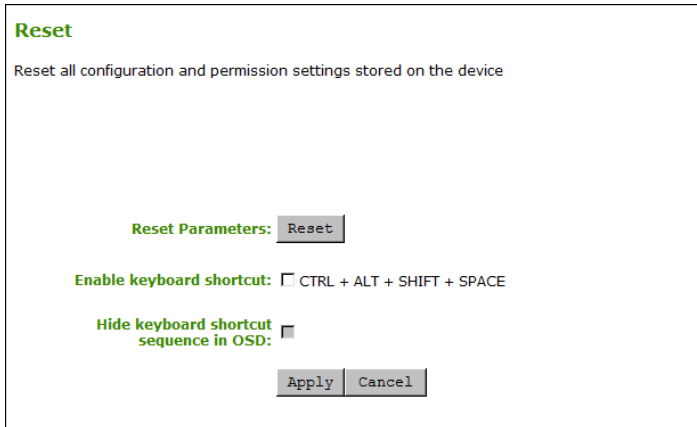
AWI Client: Reset Settings

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 does not revert the firmware

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



AWI Client Reset page

The following parameters can be found on the AWI Client Rest page.

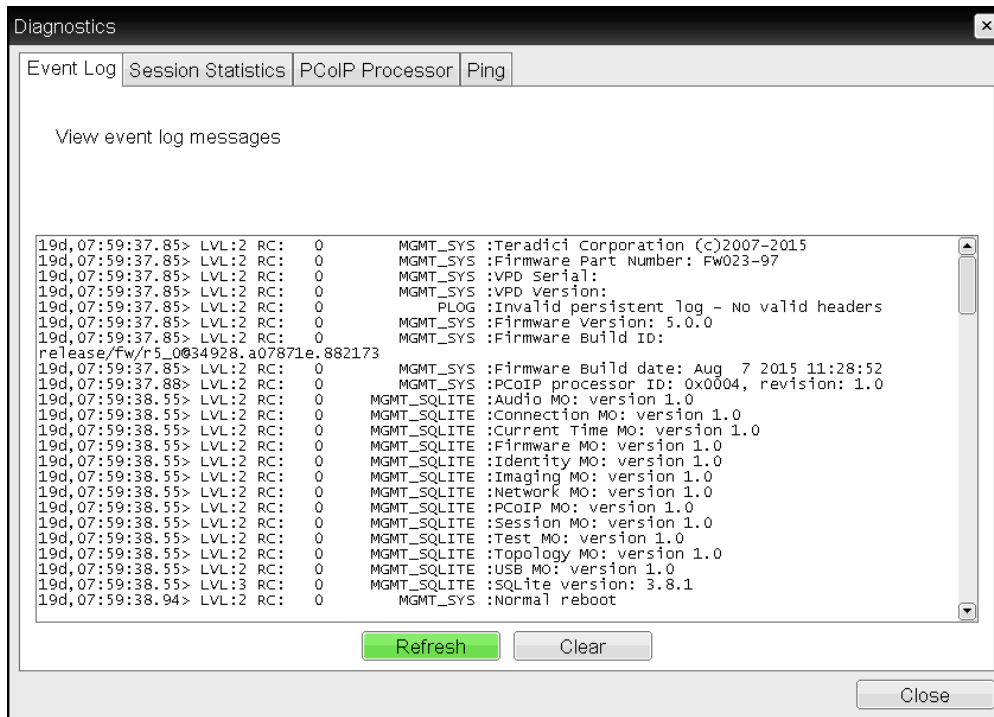
AWI Client Reset Parameters

Parameter	Description
Reset Parameters	Resets parameters to factory default values stored in flash memory. When you click this button, a prompt appears for confirmation to prevent accidental resets.
Enable Keyboard Shortcut	When enabled, the user can press the specified combination of keys 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.

Performing Diagnostics

OSD: Event Log

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

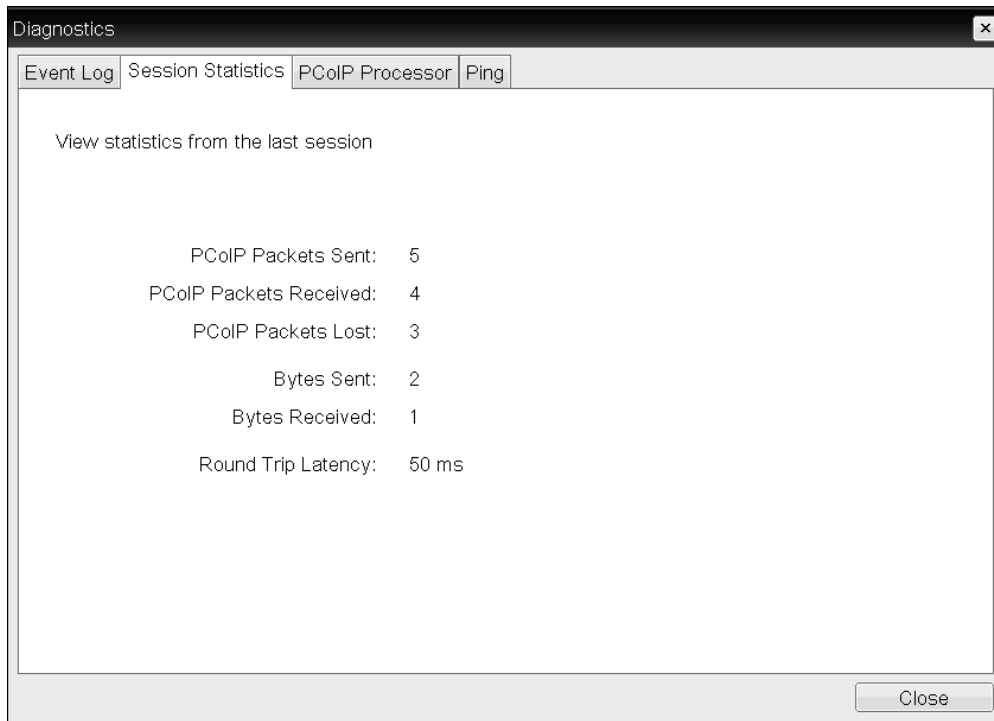
The following parameters can be found on the OSD Event Log page.

OSD Event Log 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.

OSD: Session Statistics

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

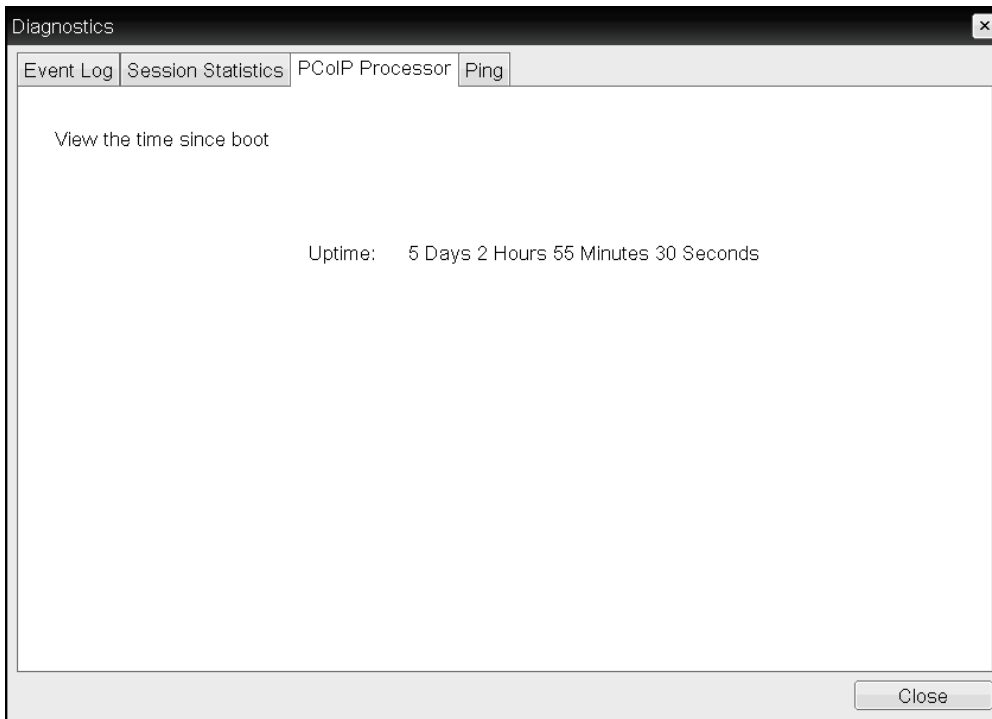
The following parameters can be found on the OSD Session Statistics page.

OSD Session Statistics Parameters

Parameters	Description
PCoIP Packets Statistics	<p>PCoIP Packets Sent: The total number of PCoIP packets sent in the last session.</p> <p>PCoIP Packets Received: The total number of PCoIP packets received in the last session.</p> <p>PCoIP Packets Lost: The total number of PCoIP packets lost in the last session.</p>
Bytes	<p>Bytes Sent: The total number of bytes sent in the last session.</p> <p>Bytes Received: The total number of bytes received in the last session.</p>
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms).

OSD: PCoIP Processor

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.

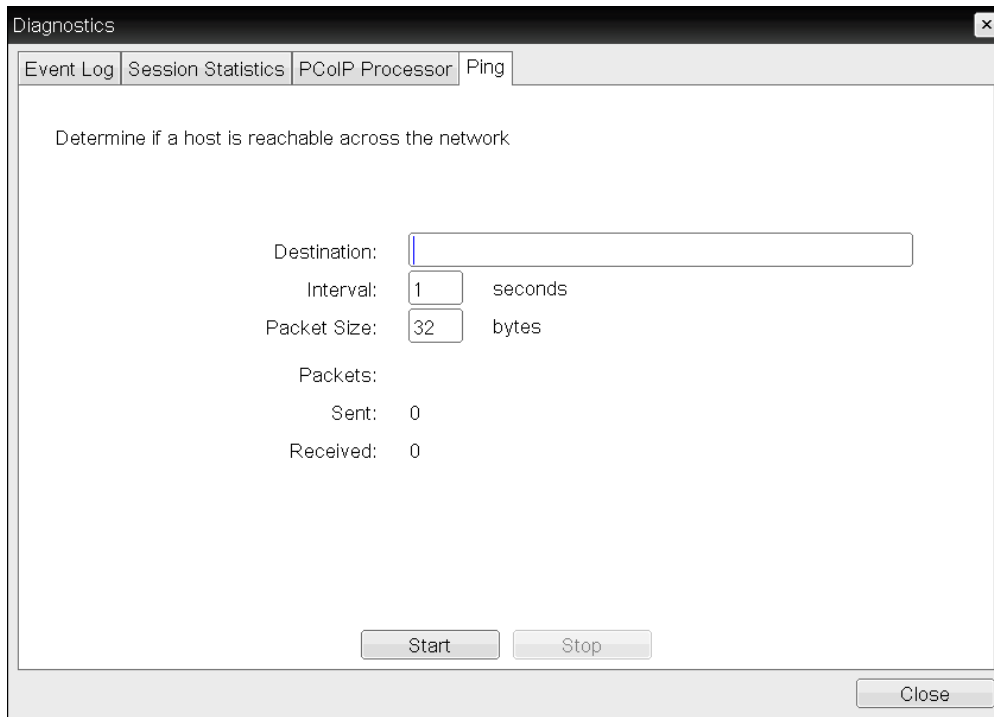


OSD PCoIP Processor page

OSD: Ping

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

The following parameters can be found on the OSD Ping page.

Ping Parameters

Parameter	Description
Destination	IP address or Fully Qualified Domain Name (FQDN) to ping.
Interval	Interval between ping packets.
Packet Size	Size of the ping packet.
Packets Sent	Number of ping packets transmitted.
Packets Received	Number of ping packets received.

AWI: Event Log

The Event Log page lets you view and clear event log messages 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:

Syslog Facility: 19 - local use 3 ▼

Enhanced logging mode: Disable

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


Apply Cancel


AWI Event Log – Event Log selected

The following parameters can be found on the AWI Event Log page.

AWI Event Log Parameters

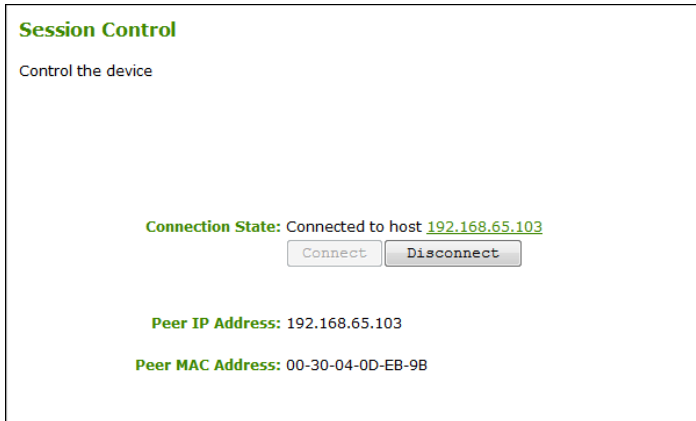
Parameter	Description
Enable Event Log	<p>When this feature is enabled, logging occurs in verbose mode, and all event log and syslog options are displayed.</p> <p>When this feature is disabled, the logging options are hidden. Disabling the event log disables logging and causes existing persistent event logs to be deleted. If syslog settings are configured, logs will not be sent to a syslog server.</p>

Parameter	Description
Event log Messages	<ul style="list-style-type: none"> • View: Click to open a browser page that displays the event log messages (with timestamp information) stored on the device. Press F5 to refresh the browser page log information. • Clear: Click to delete all event log messages stored on the device.
Enable Syslog	<p>Enable or disable the syslog standard as the logging mechanism for the device.</p> <div style="border: 1px solid #00a09a; padding: 5px; margin-top: 10px;">  <p>Note: Configure remaining fields when syslog is enabled If syslog is enabled, you must configure the remaining fields. If syslog is disabled, these fields are non-editable.</p> </div>
Identify Syslog Host By	<p>Choose if the syslog server host is identified by IP address or by Fully Qualified Domain Name (FQDN).</p>
Syslog Host IP Address / Syslog Host DNS name	<p>The parameter that displays depends on which option you choose to identify the syslog server host:</p> <ul style="list-style-type: none"> • IP Address: Enter the IP address for the syslog server host. • FQDN: Enter the DNS name for the syslog server host. <p>If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it.</p>
Syslog Host Port	<p>Enter port number of the syslog server. The default port number value is 514.</p>
Syslog Facility	<p>The facility is a number attached to every syslog message 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.</p> <p>Enter a facility to suit your logging needs. For example, you could configure devices as follows:</p> <ul style="list-style-type: none"> • Zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 <p>The default facility is set to '19 – local use 3'. Cisco routers default to '23 – local use 7'.</p>

Parameter	Description
Enhanced logging mode	<p>If you require enhanced logging details in the event log to help troubleshoot a problem with a Tera2 PCoIP Zero Client or PCoIP Remote Workstation Card, select an enhanced logging category, and click Apply > Continue. (To return to normal logging mode, click Disable, and Apply > Continue.)</p>
	<p> Note: Enhanced logging may be enabled for one category at a time</p> <p>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.</p>
	<p>Enhanced logging mode categories:</p> <ul style="list-style-type: none"> • Audio: Provides enhanced audio-related details, such as audio compression levels and audio bandwidth. Enable this mode if you are experiencing any problems with audio quality. • Management Console: Provides debug-level details for the connection state between the device and the MC. Enable this mode if you are having trouble connecting to or managing the device using the MC. • Networking: Provides socket-level details for a device’s network connections. Enable this mode for network-related issues—for example, if the device cannot connect to a peer or broker, or if it cannot get an IP address from a DHCP server. • OneSign: Provides enhanced logging for connections using Imprivata’s OneSign Single Sign-On proximity cards. Enable this mode to see debug-level messages between a device and a OneSign authentication server. • Session Negotiation: Provides pre-session messaging details, such as the full feature set advertised by each device. Enable this mode for low-level session negotiation details. • SmartCard: Provides debug-level messages for smart cards. Enable this mode if you experience trouble tapping or logging in using a smart card. • System: Provides heartbeat details about the device, such as ambient temperature. Enable this mode for system-level problems. • USB: Provides details of the traffic between the device and any connected USB devices. Enable this mode if you are experiencing problems with a connected USB device. • Video: Displays enhanced image-related logging information. Enable this mode for image problems, monitor problems, or display topology issues.

AWI: Session Control

The Session Control page lets you view information about a device and also enables you to manually disconnect or connect a session. You can access this page from the **Diagnostics > Session Control** menu.



AWI Session Control page

The following parameters can be found on the AWI Session Control page.

AWI Session Control Parameters

Parameter	Description
Connection State	<p>This field displays the current state for the session. Options include the following:</p> <ul style="list-style-type: none"> • Disconnected • Connection Pending • Connected <p>Two buttons appear below the Connection State field:</p> <ul style="list-style-type: none"> • Connect: If the connection state is Disconnected, click this button to initiate a PCoIP session between the client and its peer device. If the connection state is Connection Pending or Connected, this button is disabled. • Disconnect: If the connection state is Connected or Connection Pending, click this button to end the PCoIP session for the device. If the connection state is Disconnected, this button is disabled.
Peer IP	<p>Peer IP Address: Displays the IP address for the peer device. When not in session, this field is blank.</p>
Peer MAC Address	<p>Peer MAC Address: Displays the MAC address of the peer device. When not in session, this field is blank.</p>

AWI: Session Statistics

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

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

AWI Session Statistics page




Note: Figure shows client statistics with two connected displays

The 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.

The following parameters can be found on the AWI Session Statistics page.

AWI Session Statistics Parameters

Parameters	Description
Connection State	<p>The current (or last) state of the PCoIP session. Possible connection states are:</p> <ul style="list-style-type: none"> • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	<p>Indicates whether 802.1x authentication is enabled or disabled on the device.</p>
PCoIP Packets Statistics	<p>PCoIP Packets Sent: The total number of PCoIP packets sent in the current/last session.</p> <p>PCoIP Packets Received: The total number of PCoIP packets received in the current/last session.</p> <p>PCoIP Packets Lost: The total number of PCoIP packets lost in the current/last session.</p>
Bytes	<p>Bytes Sent: The total number of bytes sent in the current/last session.</p> <p>Bytes Received: The total number of bytes received in the current/last session.</p>
Round Trip Latency	<p>The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms).</p>
Bandwidth Statistics	<p>Transmit Bandwidth: The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels.</p> <p>Receive Bandwidth: The minimum, average, and maximum traffic received by the Tera processor.</p>
Pipeline Processing Rate	<p>Shows the average and maximum amount of image data being processed by the image engine (in megapixels per second).</p>
Endpoint Image Settings In Use	<p>Displays if the image settings being used are configured within the client or within the host. This is based on how the <i>Use Client Image Settings</i> field is configured on the Image page for the host device.</p>

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 <i>Image Quality Preference</i> 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 <i>Disable Build to Lossless</i> field on the Image page is unchecked. Disabled: The <i>Disable Build to Lossless</i> field is checked.
Reset Statistics	Click this button to reset the statistic information on this page.  Note: Reset Statistics button resets statistics reported on Home page The Reset Statistics button also resets the statistics reported in the Home page.
Display	The port number for the display.
Maximum Rate: Refresh Rate	This column shows the refresh rate of the attached display. If the <i>Maximum Rate</i> field on the Image page is set to 0 (that is, there is no limit), the maximum rate is taken from the monitor's refresh rate. If the <i>Maximum Rate</i> 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.
Initial Image Quality	Shows the current lossless state of the attached display: <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless

AWI: Audio Test

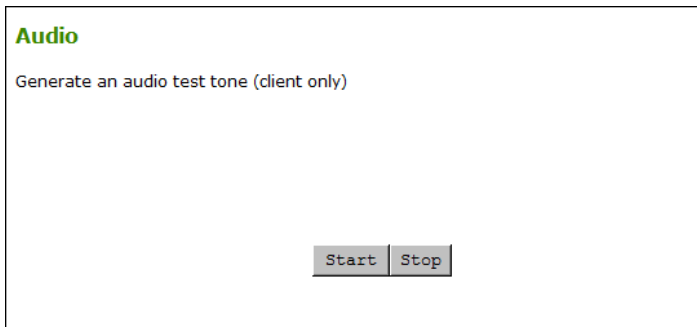
The Audio page lets you generate an audio test tone from the device. You can access this page from the **Diagnostics > Audio** menu.

To generate an audio test tone, click **Start** to start the test tone. Click **Stop** to stop the test.



Note: Audio page is only available for certain PCoIP sessions

The Audio page functionality is only available on a client when the client is not in a PCoIP session.



AWI Client Audio page

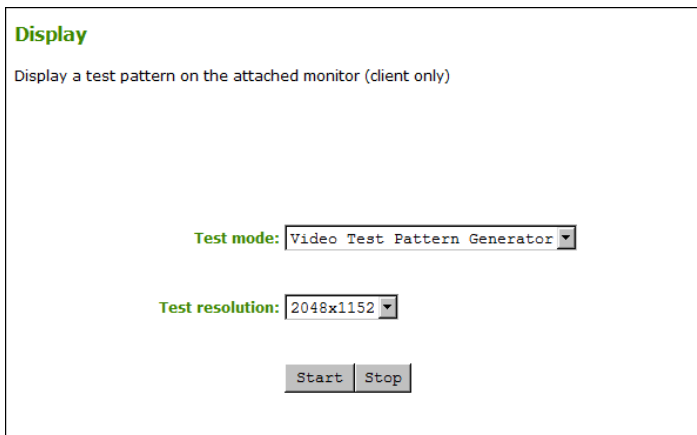
AWI: Display Test

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: Test pattern only appears for certain PCoIP session

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 Display page

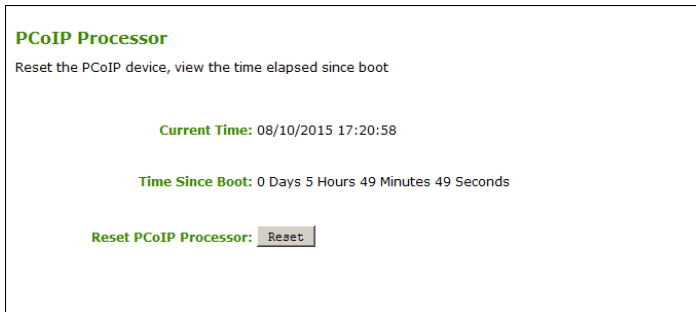
The following parameters can be found on the AWI Display Parameters page.

AWI Display Parameters

Parameters	Description
Test mode	Set the type of test pattern for the attached monitor(s) as follows: <ul style="list-style-type: none"> • 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

The PCoIP Processor page lets you reset the device 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.



AWI PCoIP Processor page

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

AWI PCoIP Processor Parameters

Statistics	Description
Current Time	The current time. This feature requires that NTP be enabled and configured .
Time Since Boot	View the uptime of the device’s PCoIP processor since the last boot.
Reset PCoIP Processor	Click this button to reset the device.

AWI: Packet Capture

The Packet Capture page provides a diagnostic tool for capturing packets on the Tera2 PCoIP 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 not included in the packet capture

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 (for example, if you are troubleshooting a call, make the call using the softphone client).
3. Click the **Stop** button to stop packet capture.



Note: Packet_capture.bin file contains network packets

Packets are captured into a binary file called **packet_capture.bin**. A maximum of 20 MB of data can be captured. If you do not stop the capture, it will automatically stop when it reaches the maximum size.

4. Click the **Download** link.
5. Save the file to the desired location on your computer.



Packet Capture
Capture network packets for diagnostics

Packet Capture Status: Idle
Bytes (Captured/Max): 0 / 20971520 (0.0 %) in 0 packets
Diagnostic Packet Capture:
Download Packet Capture: [Download](#)

AWI Packet Capture page

The following parameters can be found on the AWI Packet Capture page.

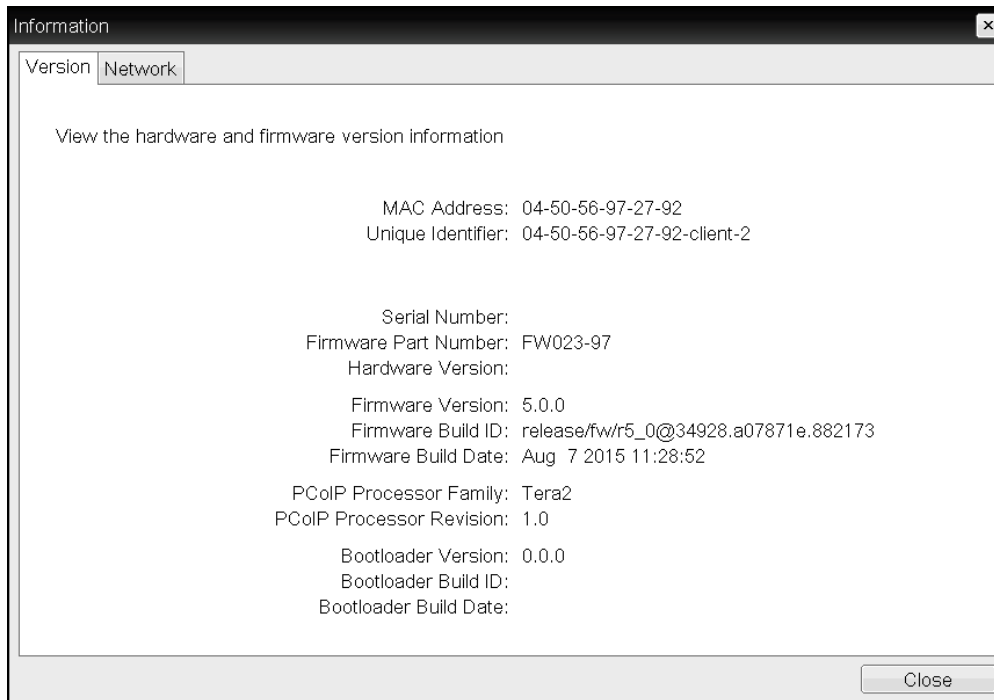
AWI Packet Capture Parameters

Parameters	Description
Packet Capture Status	<p>Displays the status of the packet capture tool. Values include the following:</p> <ul style="list-style-type: none"> • Idle: Packet capture has not been initiated. <div style="display: flex; align-items: flex-start;">  <p>Note: After packet capture, status displays Idle status after restarting zero client After performing a packet capture, the status displays as Idle again if you reboot the Tera2 PColP Zero Client.</p> </div> <ul style="list-style-type: none"> • 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	<p>Click Start to start capture and Stop to stop capture.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Packet_capture.bin file contains network packets Packets are captured into a binary file called packet_capture.bin. A maximum of 20 MB of data can be captured. If you do not stop the capture, it will automatically stop when it reaches the maximum size.</p> </div>
Diagnostic Packet Capture	Click Download to save the packet_capture.bin file to the desired location on your computer.

Viewing Information

OSD: Version

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. The information shown is for example purposes only. Your version information and build numbers may differ.



OSD Version page

The following parameters can be found on the OSD Version page.

OSD Version Parameters

Parameters	Description
VPD Information	<p>(Vital Product Data): Information provisioned by the factory to uniquely identify each device:</p> <ul style="list-style-type: none"> • MAC Address: Host/client unique MAC address. • Unique Identifier: Host/client unique identifier. • Serial Number: Host/client unique serial number. • Firmware Part Number: Part number of the current firmware. • Hardware Version: Host/client hardware version number.
Firmware Information	<p>This information reflects the current firmware details:</p> <ul style="list-style-type: none"> • Firmware Version: Version of the current firmware. • Firmware Build ID: Revision code of the current firmware. • Firmware Build Date: Build date for the current firmware.
PCoIP Processor Information	<p>This information provides details about the PColP processor.</p> <ul style="list-style-type: none"> • PCoIP Processor Family: The processor family (for example, Tera2). • PCoIP Processor Revision: The silicon revision of the PColP processor. Revision B of the silicon is denoted by a 1.0.

Parameters	Description
Bootloader Information	<p>This information reflects the current firmware bootloader details:</p> <ul style="list-style-type: none"> • Bootloader Version: Version of the current bootloader. • Bootloader Build ID: Revision code of the current bootloader. • Bootloader Build Date: Build date of the current bootloader.

OSD: Network

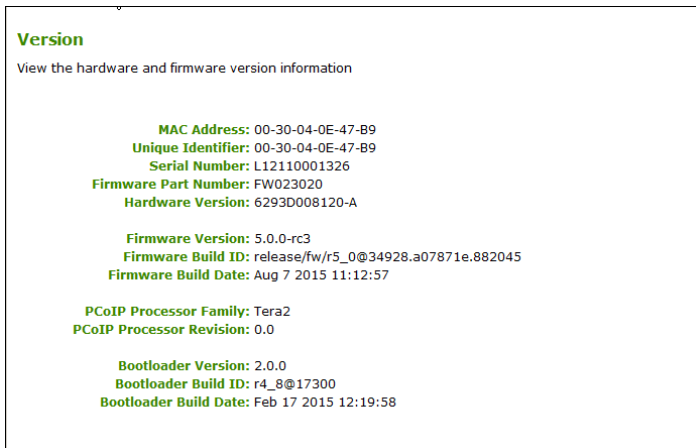
The Network page lets you view the IP address of the device. You can access this page from the **Options > Information > Network** menu.



OSD Network page

AWI: Version

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. The information shown is for example purposes only. Your version information and build numbers may differ.



AWI Version page

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

AWI Version Parameters

Parameters	Description
VPD Information	<p>(Vital Product Data): Information provisioned by the factory to uniquely identify each device:</p> <ul style="list-style-type: none"> • MAC Address: Host/client unique MAC address. • Unique Identifier: Host/client unique identifier. • Serial Number: Host/client unique serial number. • Firmware Part Number: Part number of the current firmware. • Hardware Version: Host/client hardware version number.
Firmware Information	<p>This information reflects the current firmware details:</p> <ul style="list-style-type: none"> • Firmware Version: Version of the current firmware. • Firmware Build ID: Revision code of the current firmware. • Firmware Build Date: Build date for the current firmware.
PCoIP Processor Information	<p>This information provides details about the PCoIP processor.</p> <ul style="list-style-type: none"> • PCoIP Processor Family: The processor family (for example, Tera2). • PCoIP Processor Revision: The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0.
Bootloader Information	<p>This information reflects the current firmware bootloader details:</p> <ul style="list-style-type: none"> • Boatloader Version: Version of the current bootloader. • Bootloader Build ID: Revision code of the current bootloader. • Bootloader Build Date: Build date of the current bootloader.

AWI: Attached Devices

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	Connected	DVI	1920x1080 @ 60 Hz	BNQ	7923	30-2011	V7B00284067
2	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	BNQ	7923	10-2011	93B02607026

USB Devices:

Device	Parent	Model	Status	Controller	Internal/External	VID	PID	CSP	Local Driver	Serial
0400	Root 1	USB Optical Mouse	Locally Connected	OHCI	External	046D	C05A	00/00/00	Mouse	-
0501	Root 3	USB Keyboard	Locally Connected	OHCI	External	046D	C31C	00/00/00	Keyboard, Remote Control	-
0602	Root 0	Plantronics CS20-M	Locally Connected	OHCI	External	047F	C036	00/00/00	Multiple Drivers	45FC57D7A84E204EA43D73B5C8F45591

Legend (Displays):

Status [potential failures]	Description
Connected [EDID read failure / EDID override]	The display is connected and the EDID has been bridged (host/client)
Disconnected	No display or cable has been detected
Not in Session [EDID read failure / EDID override]	The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)
Unknown	On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)
Potential Failures	Description
EDID read failure	There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.
EDID override	Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached.
Cable error	A duallink conversion cable has been detected on an incorrect port. Duallink conversion cables must be connected to the correct pair of DVI ports. The primary connector (labeled "1") of a conversion cable must be connected to either port 1 or 2 for duallink operation. The secondary connector (labeled "2") on the duallink conversion cable must be plugged into the correct companion port (ie, primary port 1 / secondary port 3; primary port 2 / secondary port 4).

AWI Client Attached Devices page




Note: USB device possesses single device and interface descriptor

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—that is, 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 Information

Statistic	Description
Displays	This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the display attached to each port. This option is only available when the host is in a PCoIP session.
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.
	 <p>Note: USB device possesses single device and interface descriptor</p> <p>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.</p>
USB Device Status	<p>Status options include:</p> <ul style="list-style-type: none"> • Not Connected: No device is connected. • Not in Session: The device is detected outside of a PCoIP session. • Not Initialized: The device is detected in a PCoIP session but the host controller has not initialized the device. • Failed Authorization: The device is detected in a PCoIP session but is not authorized. (For more information about USB, see AWI: USB Permissions on page 77.) • 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.

Uploading Files

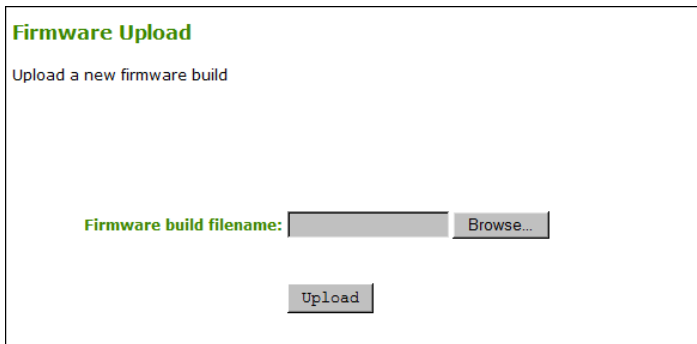
AWI: Firmware Upload

The Firmware page lets you upload a new firmware build to the device. You can access this page from the **Upload > Firmware** menu.



Note: Host and client must use the same firmware version

If you are connecting to a PCoIP Remote Workstation Card, the host and client must have the same firmware release version installed.



AWI Firmware Upload page

The following parameters can be found on the AWI Firmware Upload page.

AWI Firmware Upload Parameters

Parameter	Description
Firmware build filename	The filename of the firmware image to be uploaded. You can browse to the file using the Browse button. The file must be accessible to the web browser (that is, it must be on a local or accessible network drive). The firmware image must be an '.all' file.
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: Host and client must use the same firmware version

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.

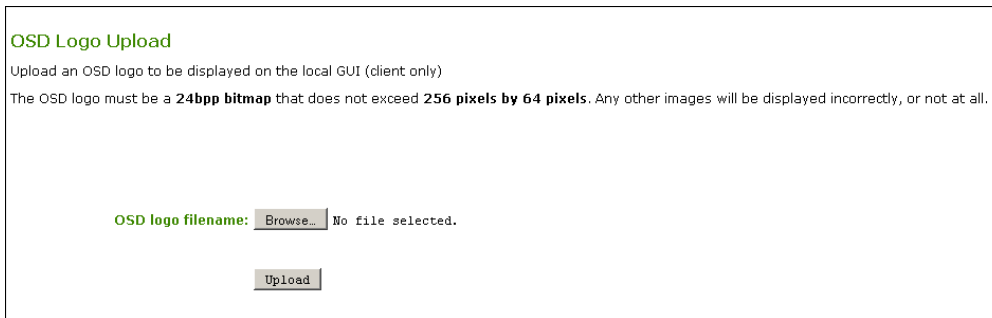
AWI: OSD Logo

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: Configuring the login screen on the OSD

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 OSD Logo Upload page

The following parameters can be found on the AWI OSD Logo Upload page.

AWI OSD Logo Upload 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 (that is, 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: Certificate Upload

The Certificate Upload page lets you upload and manage your CA root and client certificates for Tera2 PCoIP 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 10,237 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.

**Related Information: Authentication problems**

If you have authentication problems after uploading a View Connection Server client certificate, see [View Connection Server Client Certificates \(KB 15134-1084\)](#) for troubleshooting information.

**Note: Upload up to 14 additional certificates with SCEP enabled**

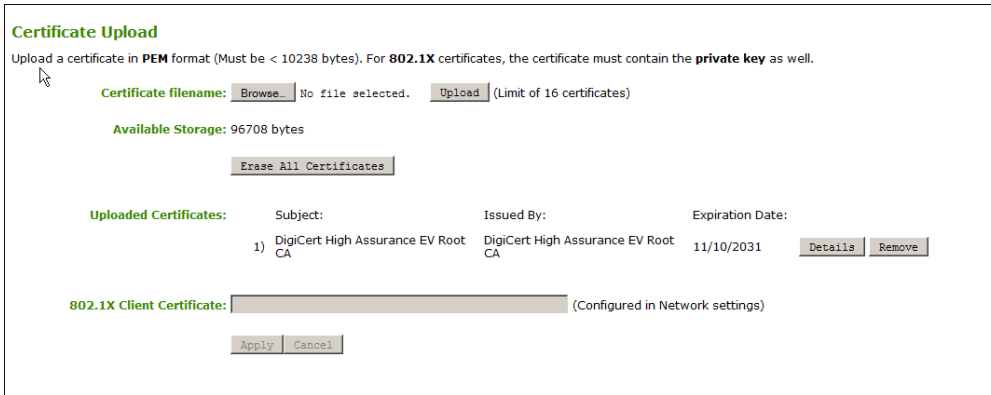
If SCEP is enabled, you can only upload a maximum of 14 additional certificates since two slots are reserved for SCEP server certificates.

**Note: Include all security information in 802.1x client certificate**

The PCoIP protocol reads just one 802.1x client certificate for 802.1x compliant networks. Make sure you include all the security information for your PCoIP devices in that client certificate. For more information about uploading certificates, see [Certificate management for PCoIP Zero Clients and Remote Workstation Cards \(KB 15134-1063\)](#). For information on 802.1x certificate authentication, see [How to Configure 802.1x Network Device Authentication on page 292](#).

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 applying your settings.
- The 802.1x server CA root certificate must be in .pem format, but should not need to contain a private key. If the certificate is in a different format, you must convert it to .pem format before uploading it. This certificate does not require configuration from the **Network** page.
- Both the 802.1x client certificate and the 802.1x server CA root certificate must be less than 10,238 bytes; otherwise, you will not be able to upload them. Some certificate files may contain multiple certificates. If your certificate file is too large and it has multiple certificates within, you can open the file in a text editor, copy and save each certificate to its own file.



AWI Certificate Upload Page

The following parameters can be found on the AWI Certificate Upload page.

AWI Certificate Upload Parameters

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

Configuring a Display Override

OSD: EDID Override Settings (Dual)

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: Function only available through OSD

This function is only available through the OSD.

Under normal operation, the GPU in the host computer queries a monitor attached to the Tera2 PCoIP Zero Client to determine the monitor’s capabilities. These are reported in the EDID information. In some situations, a monitor may be connected to a client in a way that prevents the client from reading the EDID information, such as when connecting through certain KVM devices. The **Enable Attached Display Override** feature in this page enables you to configure the client to advertise default EDID information to the GPU.



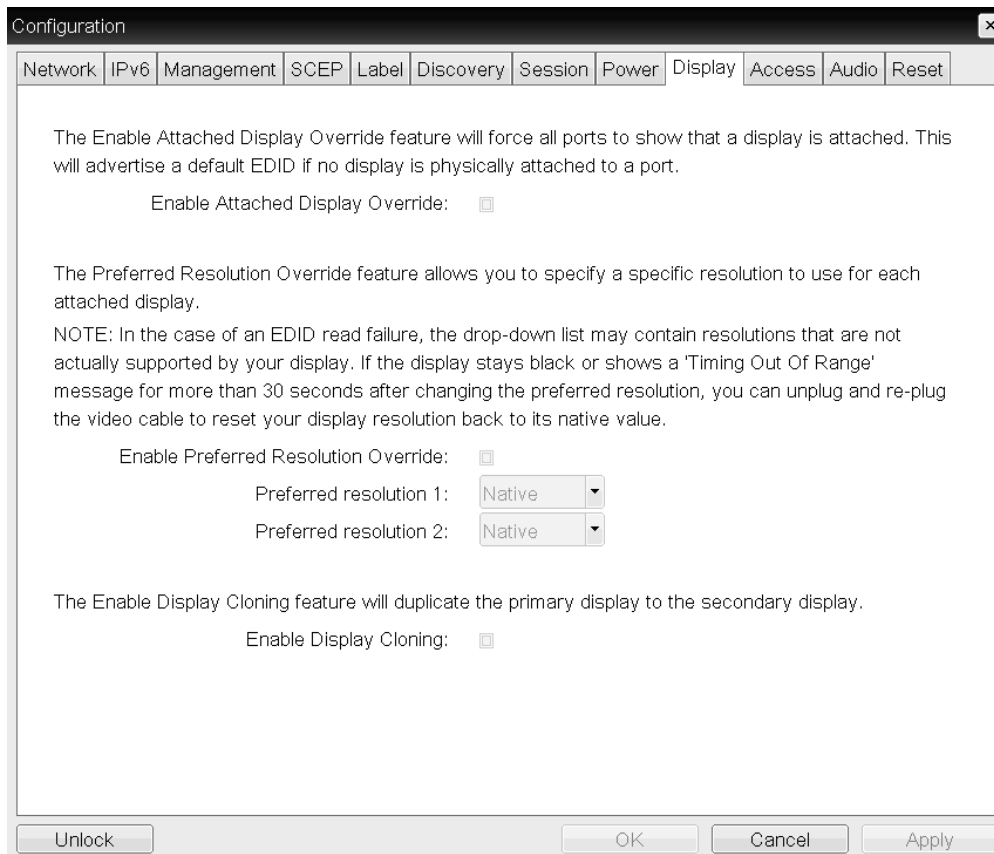
Warning: Enable the Enable Attached Display Override feature when there is no valid EDID information

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 (that is, perform a hot plug reset).



Caution: Performing a hot plug reset won't revert the display for a custom resolution

If you have set a custom resolution, performing a hot plug reset will *not* cause the display to revert to its previous resolution if both **Enable Attached Display Override** and **Enable Preferred Resolution Override** are enabled at the same time. If you want to retain your custom resolution in the event of a hot plug (or power outage, and so on), ensure that both these fields are enabled.





OSD TERA2321 Display page

The following parameters can be found on the OSD TERA2321 Display page.

OSD TERA2321 Display Parameters

Parameter	Description
Enable Attached Display Override	<p>This option is intended for legacy systems. It configures the client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. In versions of Windows prior to Windows 7, once the host had no EDID information, it would assume no monitors were attached and would never recheck. This option ensures that the host always has EDID information when the client is in session.</p> <p>The following default resolutions are advertised when this option is enabled:</p> <ul style="list-style-type: none"> • 2560x1600 @60 Hz • 2048x1152 @60 Hz • 1920x1440 @60 Hz • 1920x1200 @60 Hz • 1920x1080 @60 Hz • 1856x1392 @60 Hz • 1792x1344 @60 Hz • 1680x1050 @60 Hz • 1600x1200 @60 Hz • 1600x900 @60 Hz • 1440x900 @60 Hz • 1400x1050 @60 Hz • 1366x768 @60 Hz • 1360x768 @60 Hz • 1280x1024 @60 Hz • 1280x960 @60 Hz • 1280x800 @60 Hz • 1280x768 @60 Hz • 1280x720 @60 Hz • 1024x768 @60 Hz • 848x480 @60 Hz • 800x600 @60 Hz • 640x480 @60 Hz <p>Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.</p>

Parameter	Description
Enable Preferred Resolution Override	<p>Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of 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.</p> <ul style="list-style-type: none"> • Preferred resolution 0: Select the preferred resolution of the display connected to port 1 on the Tera2 PCoIP Zero Client. • Preferred resolution 1: Select the preferred resolution of the display connected to port 2 on the Tera2 PCoIP Zero Client. <p>Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled.</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;">  <p>Caution: Performing a hot plug reset will <i>not</i> cause the display to revert to previous resolution If you have set a custom resolution, performing a hot plug reset will <i>not</i> cause the display to revert to its previous resolution if both Enable Attached Display Override and Enable Preferred Resolution Override are enabled at the same time. If you want to retain your custom resolution in the event of a hot plug (or power outage, and so on), ensure that both these fields are enabled.</p> </div>
Enable Display Cloning	<p>Enable the display cloning option if you want the secondary display to mirror the primary display—for example, for digital signage, trainings, and so on.</p> <div style="border: 1px solid teal; padding: 5px; margin-top: 10px;">  <p>Note: Connecting a Tera2 PCoIP Zero Client to a remote workstation If you are connecting a TERA2321 PCoIP Zero Client to a remote workstation that does not have the PCoIP host software installed and the host driver function enabled, <i>and</i> 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.</p> </div>

OSD: EDID Override Settings (Quad)

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: Function only available through OSD**

This function is only available through the OSD.

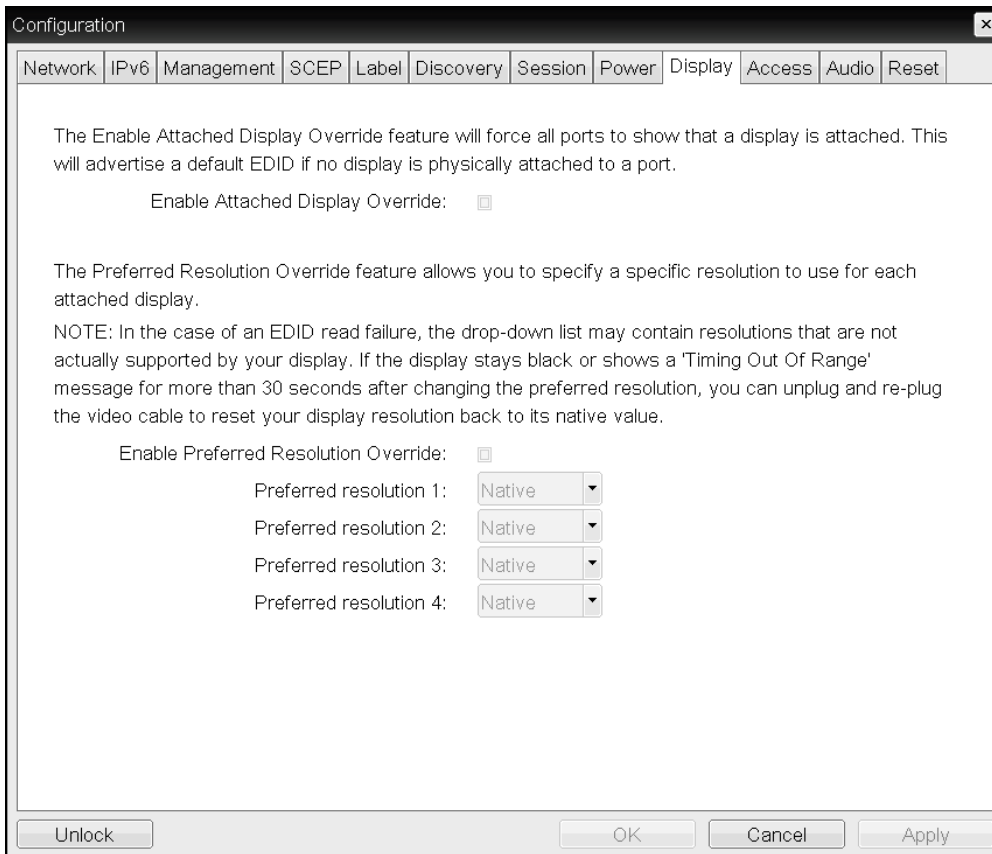
Under normal operation, the GPU in the host computer queries a monitor attached to the Tera2 PCoIP Zero Client to determine the monitor's capabilities. These are reported in the EDID information. In some situations, a monitor may be connected to a client in a way that prevents the client from reading the EDID information, such as when connecting through certain KVM devices. The **Enable Attached Display Override** feature in this page enables you to configure the client to advertise default EDID information to the GPU.

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

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 (that is, perform a hot plug reset).

**Caution: Performing a hot plug reset won't revert the display for a custom resolution**

If you have set a custom resolution, performing a hot plug reset will *not* cause the display to revert to its previous resolution if both **Enable Attached Display Override** and **Enable Preferred Resolution Override** are enabled at the same time. If you want to retain your custom resolution in the event of a hot plug (or power outage, and so on), ensure that both these fields are enabled.



OSD TERA2140 Display page

The following parameters can be found on the OSD TERA2140 Display page.

OSD TERA2140 Display Parameters

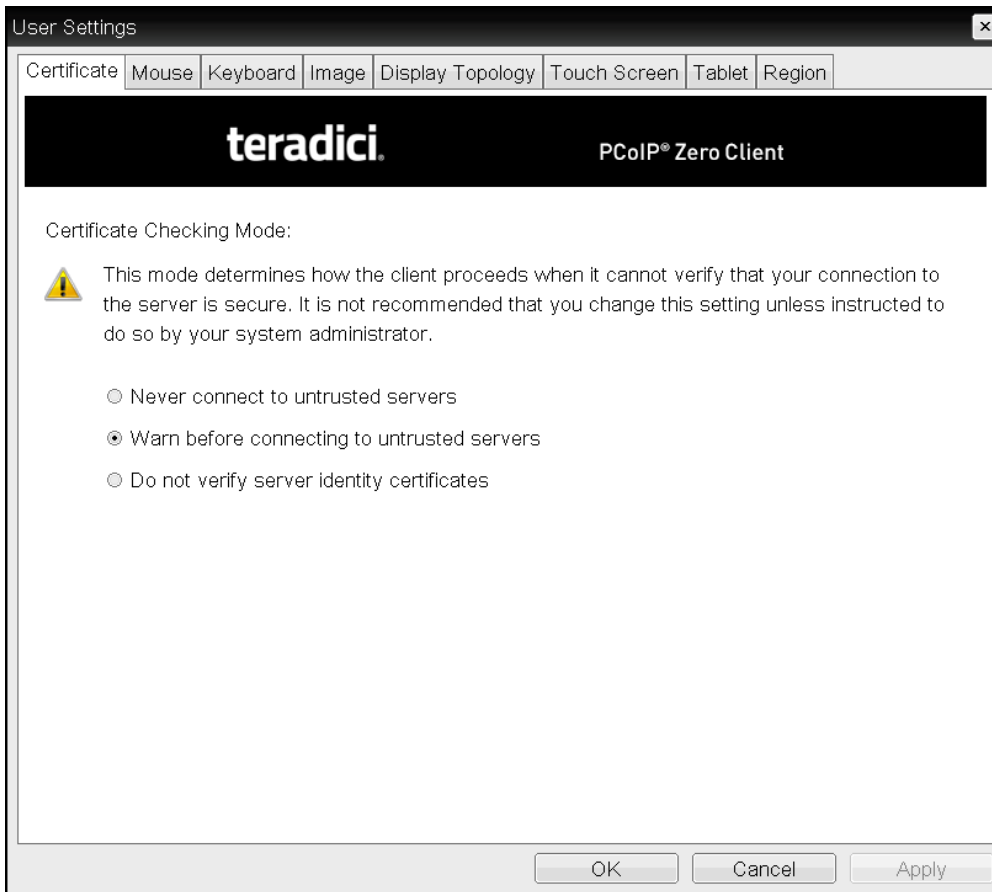
Parameter	Description
Enable Attached Display Override	<p>This option is intended for legacy systems. It configures the client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. In versions of Windows prior to Windows 7, once the host had no EDID information, it would assume no monitors were attached and would never recheck. This option ensures that the host always has EDID information when the client is in session.</p> <p>The following default resolutions are advertised when this option is enabled:</p> <ul style="list-style-type: none"> • 2560x1600 @60 Hz • 2048x1152 @60 Hz • 1920x1440 @60 Hz • 1920x1200 @60 Hz • 1920x1080 @60 Hz • 1856x1392 @60 Hz • 1792x1344 @60 Hz • 1680x1050 @60 Hz • 1600x1200 @60 Hz • 1600x900 @60 Hz • 1440x900 @60 Hz • 1400x1050 @60 Hz • 1366x768 @60 Hz • 1360x768 @60 Hz • 1280x1024 @60 Hz • 1280x960 @60 Hz • 1280x800 @60 Hz • 1280x768 @60 Hz • 1280x720 @60 Hz • 1024x768 @60 Hz • 848x480 @60 Hz • 800x600 @60 Hz • 640x480 @60 Hz <p>Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled.</p>

Parameter	Description
Enable Preferred Resolution Override	<p>Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of 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.</p> <ul style="list-style-type: none"> • Preferred resolution 0: Select the preferred resolution of the display connected to port 1 on the Tera2 PCoIP Zero Client. • Preferred resolution 1: Select the preferred resolution of the display connected to port 2 on the Tera2 PCoIP Zero Client. • Preferred resolution 2: Select the preferred resolution of the display connected to port 3 on the Tera2 PCoIP Zero Client. • Preferred resolution 3: Select the preferred resolution of the display connected to port 4 on the Tera2 PCoIP Zero Client. <p>Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled.</p> <p>See Important note for information on how to retain a custom resolution in the event of a hot plug, power outage, and so on.</p>

Configuring OSD User Settings

OSD: Certificate Checking Mode 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. If **Certificate Check Mode Lockout** is enabled from the AWI, users will not be able to modify the settings on this page.



OSD Certificate Checking Mode page

The following parameters can be found on the OSD Certificate page.

OSD Certificate Checking Mode 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 enable all connections.

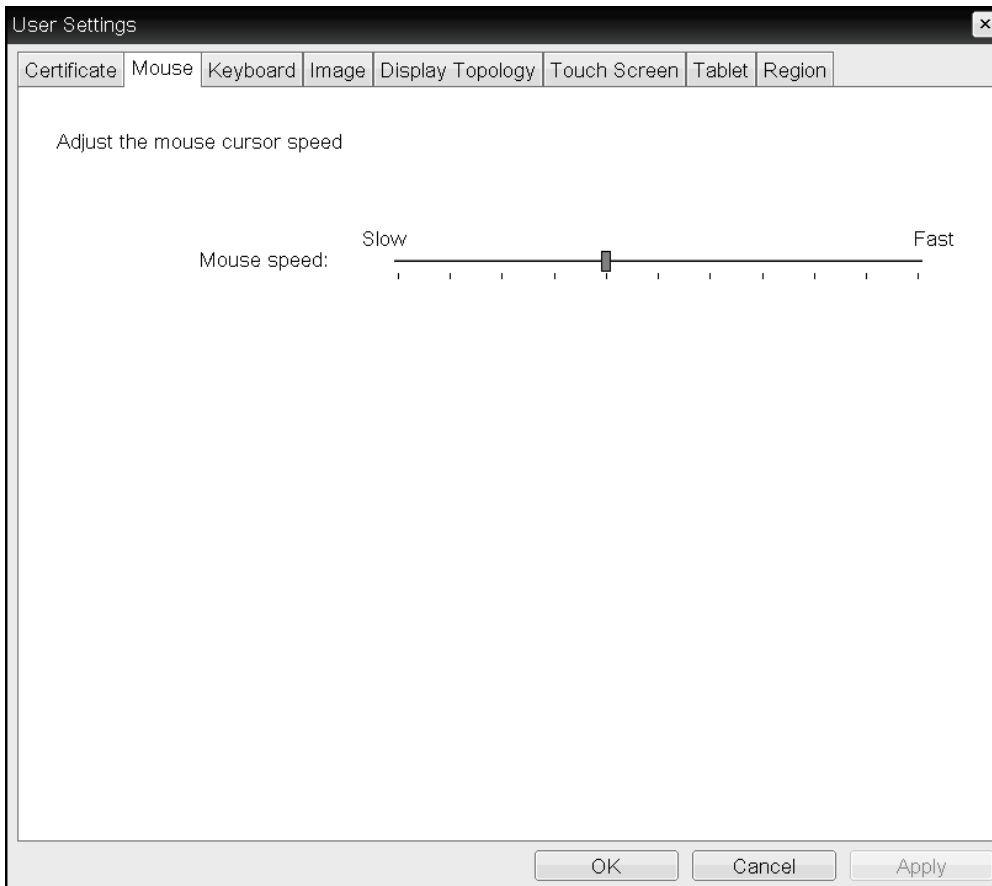
OSD: Mouse Settings

The Mouse page lets you change the mouse cursor speed. You can access this page from the **Options > User Settings > Mouse** menu.



Note: Settings only apply when you are using OSD

These settings only apply while you are using the OSD. They have no effect on keyboard settings during PCoIP sessions.



OSD Mouse page

The following parameters can be found on the OSD Mouse page.

OSD Mouse Parameters

Parameter	Description
Mouse Speed	Move the slider to configure the speed of the mouse cursor.

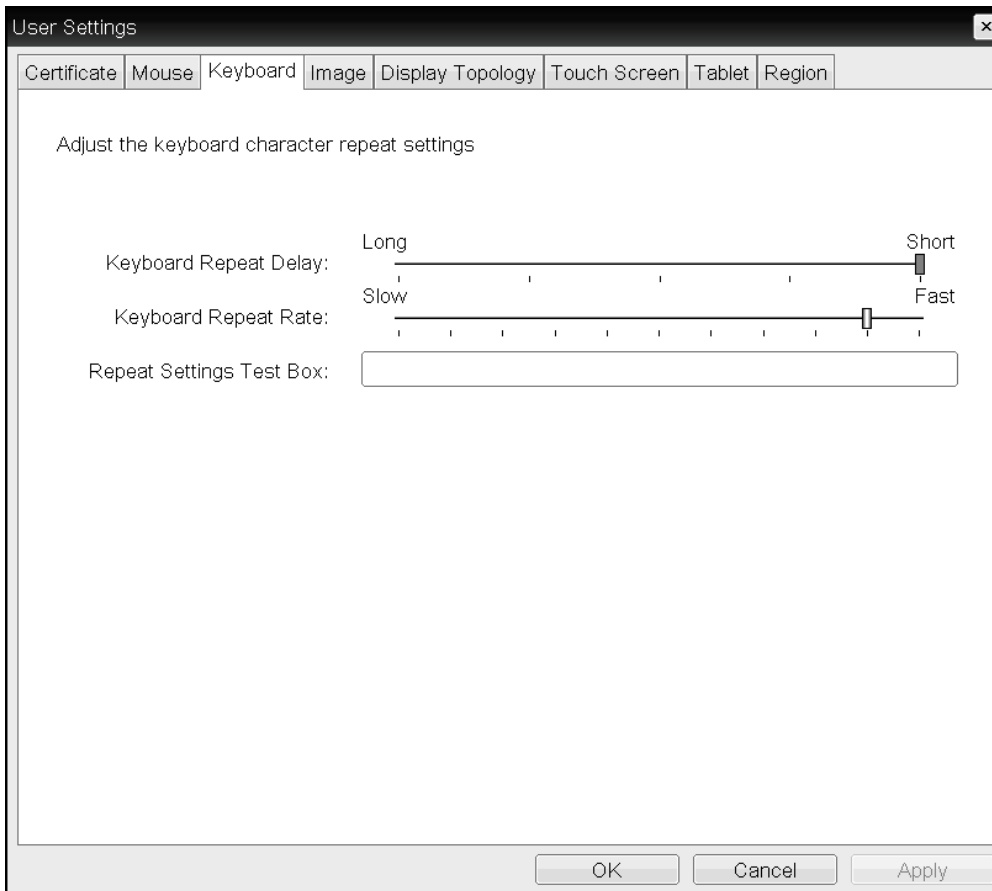
OSD: Keyboard Settings

The Keyboard page lets you change the keyboard character delay and character repeat settings. You can access this page from the **Options > User Settings > Keyboard** menu.



Note: Settings only apply when you are using OSD

These settings only apply while you are using the OSD. They have no effect on keyboard settings during PCoIP sessions.



OSD Keyboard page

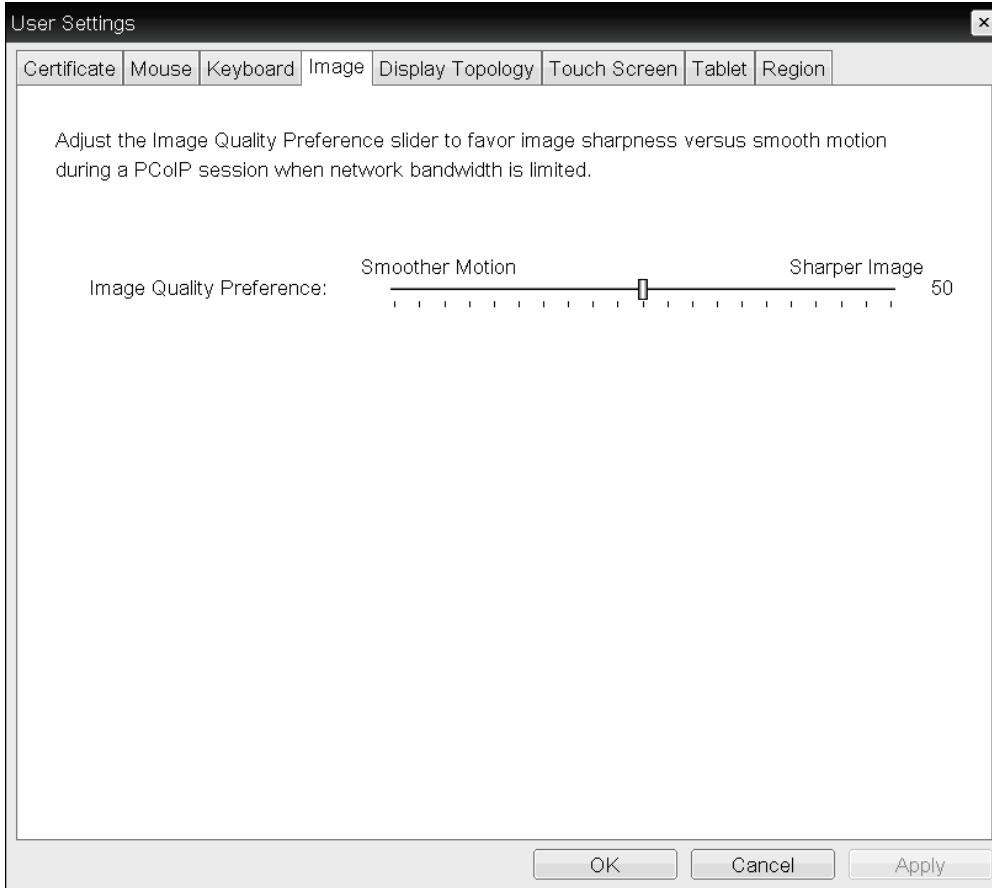
The following parameters can be found on the OSD Keyboard page.

OSD Keyboard 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: 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. This setting applies only to sessions between Tera2 PCoIP Zero Clients and PCoIP Remote Workstation Cards.



OSD Image page

In the OSD, this page is available from the **Options->User Settings** menu.

OSD Image 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: Setting does not work with PCoIP settings with VMware Horizon virtual desktops

This setting does not work in PCoIP sessions with VMware Horizon virtual desktops running release 5.0 or earlier.

OSD: Display Topology Settings (Dual)

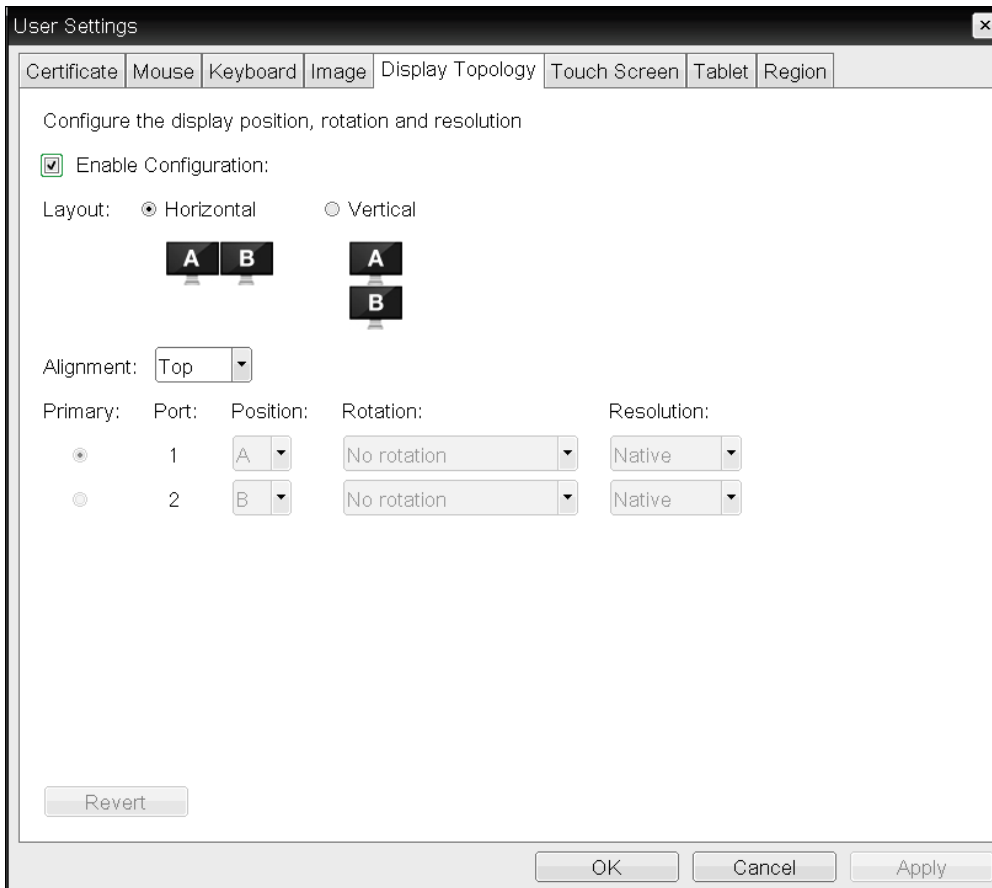
The Display Topology page lets users change the display topology for a PCoIP session. You can access this page from the **Options > User Settings > Display Topology** menu on your client OSD.

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 higher. To apply the display topology feature to a PCoIP session between a client and a PCoIP Remote Workstation Card, you must have the PCoIP host software installed on the host.



Note: Changing display topology settings using page

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

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

OSD Dual-display Topology Parameters

Parameter	Description
Enable Configuration	Enable to configure a device that supports two displays per PCoIP chipset.
Display Layout	<p>Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk.</p> <ul style="list-style-type: none"> Horizontal: Select to arrange displays horizontally, as indicated in the diagram. Vertical: Select to arrange displays vertically, as indicated in the diagram.

Parameter	Description
Alignment	<p>Select how you want displays aligned when they are different sizes.</p> <div data-bbox="516 380 618 478"> </div> <p>Note: Setting affects area of screen to use This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.</p> <p>Horizontal layout:</p> <ul style="list-style-type: none"> • Top: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • Center: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • Bottom: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. <p>Vertical layout:</p> <ul style="list-style-type: none"> • Left: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • Center: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • Right: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.

Parameter	Description
Primary	<p>Configure which video port on the Tera2 PCoIP Zero Client you want as the primary port.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note: Display connected to the primary port becomes the primary display</p> <p>The display that is connected to the primary port becomes the primary display (that is, the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).</p> </div> </div> <ul style="list-style-type: none"> • Port 1: Select to configure port 1 on the Tera2 PCoIP Zero Client as the primary port. • Port 2: Select to configure port 2 on the Tera2 PCoIP Zero Client as the primary port.
Position	Specify which display is physically connected to each port.
Rotation	<p>Configure the rotation of the display in each port:</p> <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	<p>The display resolution can be configured for a PCoIP session between a virtual machine or host and a Tera2 PCoIP Zero Client. The Tera2 PCoIP Zero Client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.</p>

OSD: Display Topology Settings (Quad)

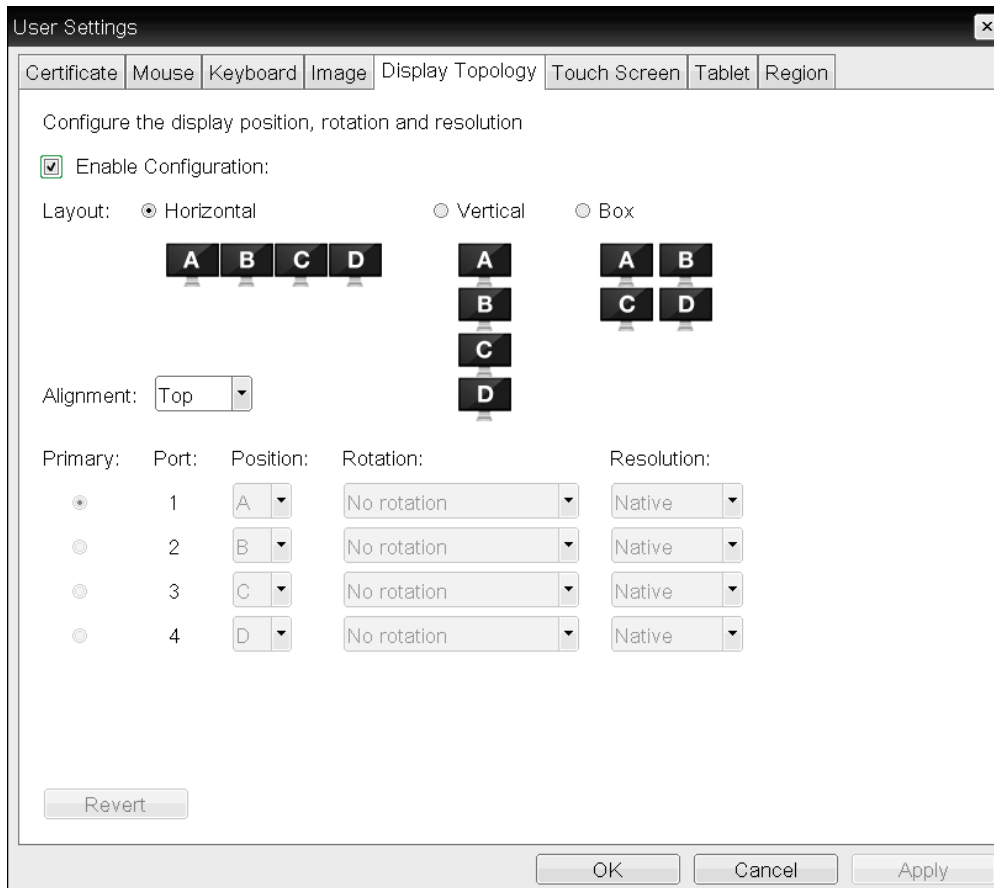
The Display Topology page lets users change the display topology for a PCoIP session. You can access this page from the **Options > User Settings > Display Topology** menu on your client OSD.

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 higher. To apply the display topology feature to a PCoIP session between a client and a PCoIP Remote Workstation Card, you must have the PCoIP host software installed on the host.



Note: Changing display topology settings using page

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





OSD Quad-display Topology page

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

OSD Quad-display Topology Parameters

Parameter	Description
Enable Configuration	Enable to configure a device that supports four displays per PCoIP chipset.
Display Layout	<p>Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk.</p> <ul style="list-style-type: none"> • Horizontal: Select to arrange displays horizontally, as indicated in the diagram. • Vertical: Select to arrange displays vertically, as indicated in the diagram. • Box: Select to arrange displays in a box formation, as indicated in the diagram.

Parameter	Description
Alignment	<p>Select how you want displays aligned when they are different sizes.</p> <div data-bbox="537 380 638 478">  </div> <p>Note: Setting affects area of screen to use This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.</p> <p>Horizontal layout:</p> <ul style="list-style-type: none"> • Top: Select to align displays at the top. With this setting, use the top area of the screen when navigating between displays of different sizes. • Center: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • Bottom: Select to align displays at the bottom. With this setting, use the bottom area of the screen when navigating between displays of different sizes. <p>Vertical layout:</p> <ul style="list-style-type: none"> • Left: Select to align displays on the left. With this setting, use the left area of the screen when navigating between displays of different sizes. • Center: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes. • Right: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes.

Parameter	Description
Primary	<p>Configure which video port on the Tera2 PCoIP Zero Client that you want as the primary port.</p> <div style="border: 1px solid #00a0c0; padding: 5px; margin-top: 10px;">  <p>Note: Display connected to the primary port becomes primary display The display that is connected to the primary port becomes the primary display (that is, the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).</p> </div> <ul style="list-style-type: none"> • Port 1: Select to configure port 1 on the Tera2 PCoIP Zero Client as the primary port. • Port 2: Select to configure port 2 on the Tera2 PCoIP Zero Client as the primary port. • Port 3: Select to configure port 3 on the Tera2 PCoIP Zero Client as the primary port. • Port 4: Select to configure port 4 on the Tera2 PCoIP Zero Client as the primary port.
Position	Specify which display is physically connected to each port.
Rotation	<p>Configure the rotation of the display in each port:</p> <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	<p>The display resolution can be configured for a PCoIP session between a virtual machine or host and a Tera2 PCoIP Zero Client. The Tera2 PCoIP Zero Client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.</p>

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: Supported touch screens

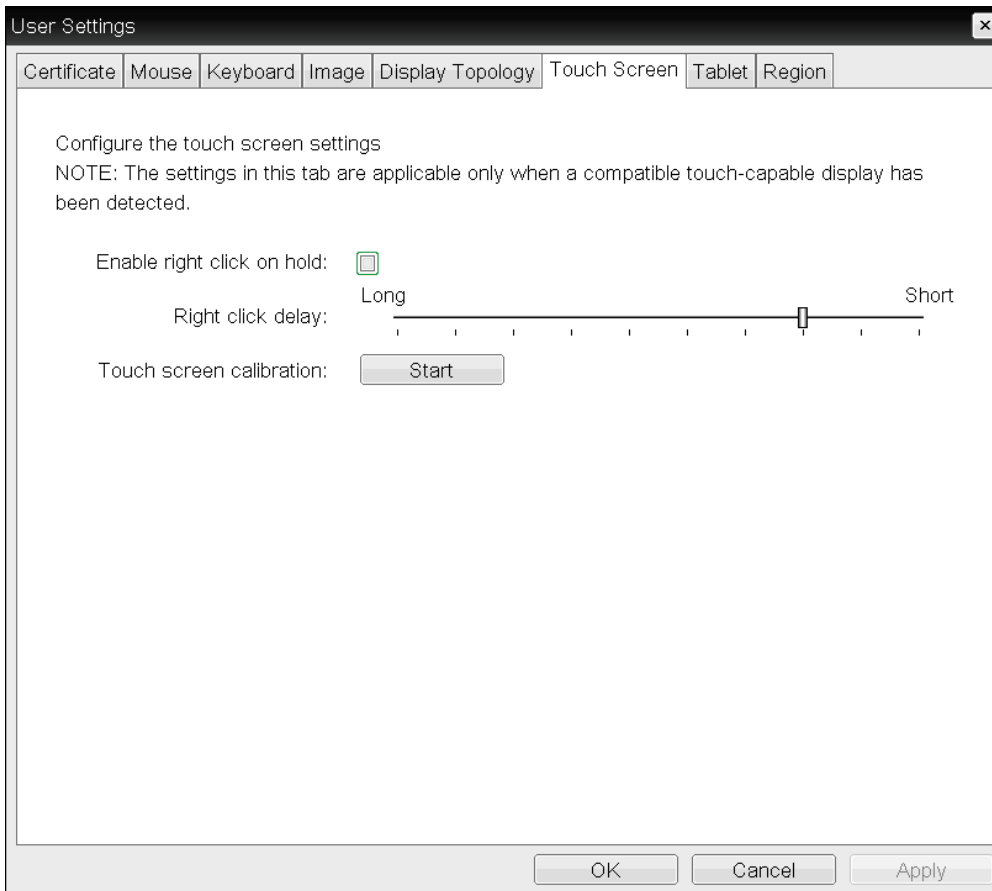
Elo IntelliTouch and Elo AccuTouch are the only Elo TouchSystems touch screens supported.

You can access this page from the **Options > User Settings > Touch Screen** menu.



Note: Touch screen page only available through OSD

The Touch Screen page is only available through the OSD. It is not available from the AWI.



OSD Touch Screen page

The following parameters can be found on the OSD Touch Screen page.

OSD Touch Screen Parameters

Parameter	Description
Enable right click on hold	Select this check box to let users generate a right-click when they touch the screen and hold it for a few seconds. If disabled, right-clicking is not supported.
Right click delay	Slide the pointer to the position (between Long and Short) to determine how long the users must touch and hold the screen to generate a right-click.

Parameter	Description
Touch screen calibration	<p>When you first connect the touch screen to the Tera2 PCoIP Zero Client, the calibration program starts. At the touch screen, touch each of the three targets as they appear.</p> <p>To test the calibration, run your finger along the monitor and ensure that the cursor follows it. If it is not successful, the calibration program automatically restarts. Once calibrated, the coordinates are stored in flash.</p> <p>To manually start the calibration program, from the OSD Touch Screen page, click Start. Follow the onscreen prompts.</p>

OSD: 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: Options apply when you attach to a Wacom tablet

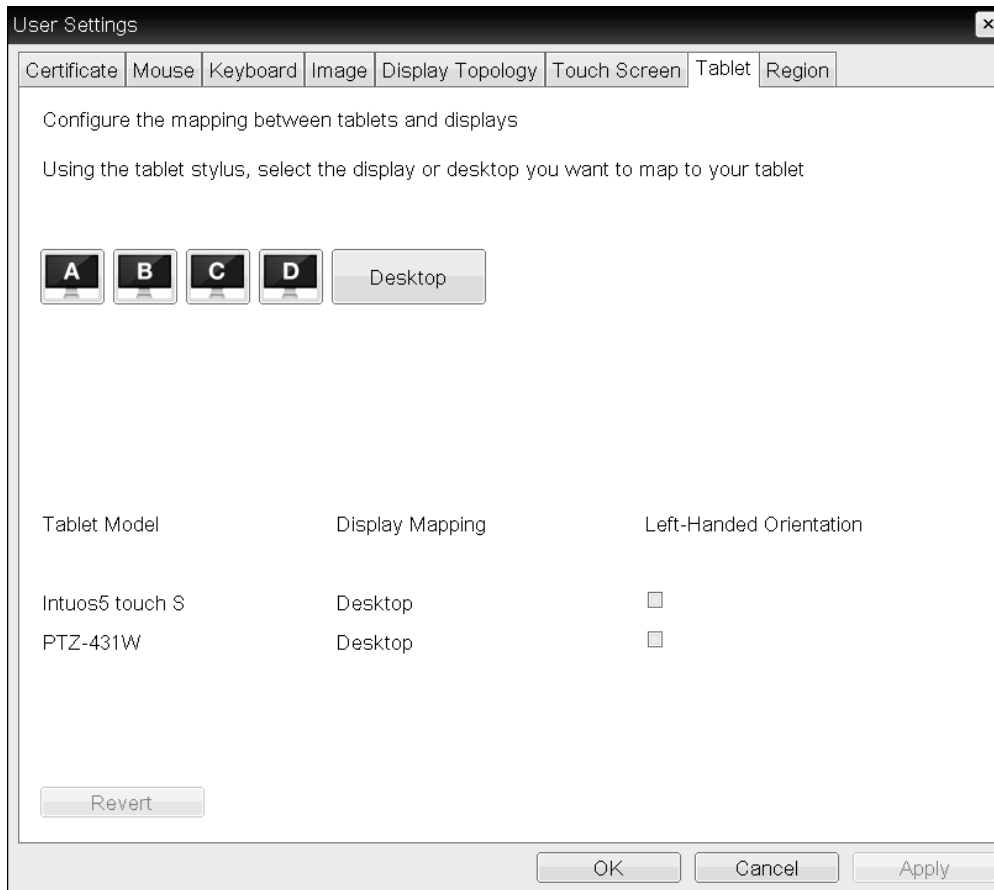
These options only apply when a Wacom tablet is attached to a Tera2 PCoIP Zero Client that is connected to a remote Linux workstation, and the 'local tablet driver' feature is enabled in the remote workstation's host software (PCoIP Host Software for Linux, version 4.5.0 or newer). When enabled, this 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 the [PCoIP® Host Software for Linux User Guide](#).

The following Wacom tablet models are supported:

Product ID	Description
0x00B0	Wacom Intuos3 4x5
0x00B1	Wacom Intuos3 6x8
0x00B2	Wacom Intuos3 9x12
0x00B3	Wacom Intuos3 12x12
0x00B4	Wacom Intuos3 12x19
0x00B5	Wacom Intuos3 6x11
0x00B7	Wacom Intuos3 4x6
0x00B8	Wacom Intuos4 4x6

Product ID	Description
0x00B9	Wacom Intuos4 6x9
0x00BA	Wacom Intuos4 8x13
0x00BB	Wacom Intuos4 12x19
0x00BC	Wacom Intuos4 WL
0x0026	Wacom Intuos5 touch S
0x0027	Wacom Intuos5 touch M
0x0028	Wacom Intuos5 touch L
0x0029	Wacom Intuos5 S
0x002A	Wacom Intuos5 M
0x0314	Wacom Intuos Pro S
0x0315	Wacom Intuos Pro M
0x0317	Wacom Intuos Pro L
0x00F4	Wacom Cintiq 24HD
0x00F8	Wacom Cintiq 24HD touch
0x003F	Wacom Cintiq 21UX
0x00C5	Wacom Cintiq 20WSX
0x00C6	Wacom Cintiq 12WX
0x0304	Wacom Cintiq 13HD
0x0057	Wacom DTK2241
0x0059	Wacom DTK2242
0x00CC	Wacom Cintiq 21UX2
0x00FA	Wacom Cintiq 22HD
0x005B	Wacom Cintiq 22HDT

The Tablet page updates automatically to show the number of monitors and tablets that are connected to the Tera2 PCoIP Zero Client. Up to four monitors can be connected, but only two locally connected tablets are supported at a time. 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. 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 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 reconnect it to the Tera2 PCoIP Zero Client.



Note: Changing the topology settings clears the tablet mappings

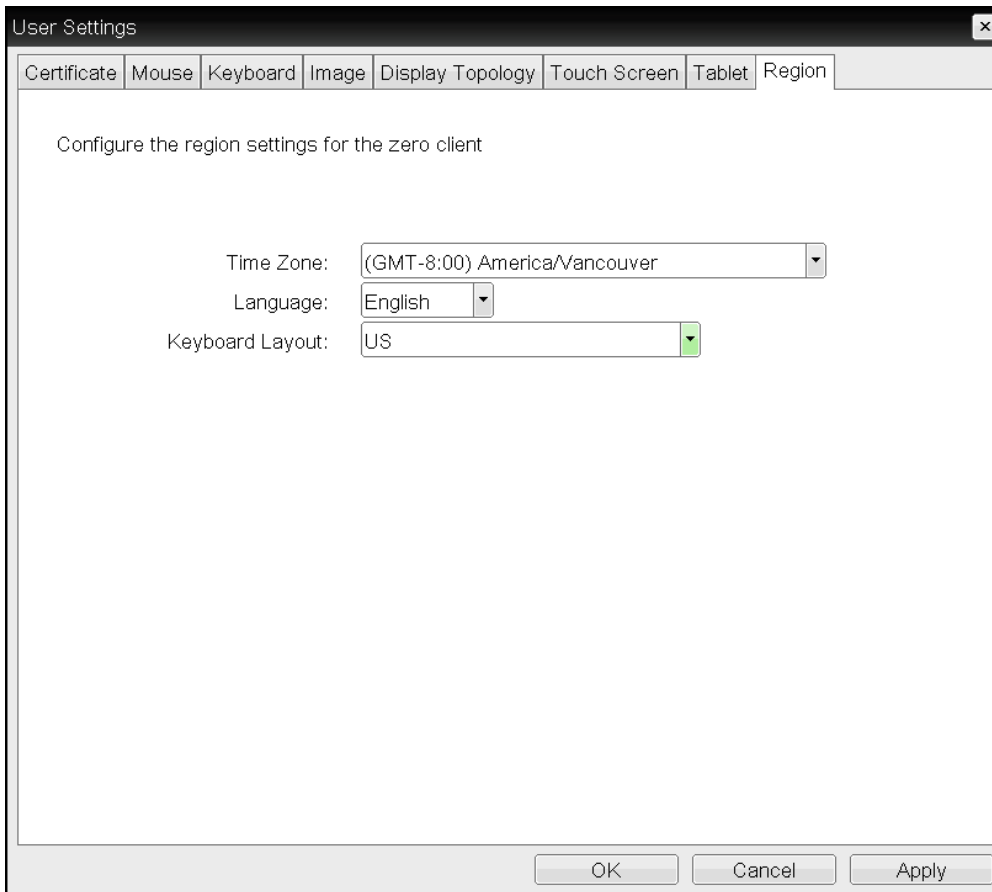
Changing the topology settings in the [Display Topology](#) page (for example, after rearranging your physical setup) will also automatically clear the tablet mappings. You will need to reconfigure your tablet setup whenever you apply topology changes.

OSD Tablet Parameters

Parameter	Description
Display and Desktop icons	This section shows the number of displays that are currently attached to the Tera2 PCoIP Zero Client. When just one monitor is attached, only the Desktop icon appears in this area, and any attached tablets are mapped to the entire desktop.
Tablet Model	Shows the model number of each attached Wacom tablet.
Display Mapping	Shows the current mapping configuration for each attached tablet (A , B , C , or D , or Desktop).
Left-Handed Orientation	To configure the tablet for a left-handed orientation: <ol style="list-style-type: none"> Using either a mouse or the tablet's stylus, select the tablet's Left-Handed Orientation check box. Click Apply. 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 reconnect it to the Tera2 PCoIP Zero Client. Applying topology changes will also clear the tablet configuration and set it to default.

OSD: Region Settings

The settings on this page let you configure the time zone, language, and keyboard layout for the zero client. You can access this page from the **Options > User Settings > Region** menu.



OSD Region page

The following parameters can be found on the OSD Region page.

OSD Region Parameters

Parameter	Description
Time Zone	Configure the time zone for your region.
Language	Configure the language to use for the OSD user interface. 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 enable the keyboard layout setting, it is used during the user's session. If this GPO is not set to enable the setting, it is dropped.

How To Topics

This section contains instructions for some common tasks you may wish to perform.

- How to find and assign a Tera2 PCoIP Zero Client's IP address
- How to display the device's processor information
- How to upload firmware
- How to upload a certificate
- How to troubleshoot a Tera2 PCoIP Zero Client in recovery mode
- How to configure an Endpoint Manager
- How to configure VLAN traffic for voice traffic
- How to set up a touch screen display
- How to configure a Tera2 PCoIP Zero Client as a Bria softphone endpoint
- How to configure 802.1x network device authentication
- How to configure Syslog settings

How to Assign an IP Address to a Tera2 PCoIP Zero Client

When a Tera2 PCoIP Zero Client is powered on for the first time, you can display its IP address by selecting **Options > Configuration > Network** from the client's OSD. If desired, you can manually change this address from the [Network](#) page.

IP addresses can be assigned to clients dynamically or statically.

Dynamic Assignment

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



Note: Client may receive a different IP address when turned off

If the client is subsequently powered off for a period of time that exceeds its DHCP lease time, the client may receive a different IP address when it is powered on again. You can avoid this problem by using a DHCP reservation to permanently associate the IP address received from the DHCP server with the device.

Static Assignment

If your network does not support DHCP, the Tera2 PCoIP Zero Client will use its static fallback IP address the first time it is powered on. This address is set by the device's manufacturer. You can statically assign an IP address from the client's Network page. Because all Tera2 PCoIP Zero Clients from the same manufacturer will have the same default IP address, you can only deploy a single client at a time when you assign IP addresses statically.

To statically assign an IP address:

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



Note: Locating the factory default IP address for a client

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

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

Factory default IP address for a client in the OFD section

The static fallback IP address can also be set from the Management Console (MC), in which case the event log will display the address as being '**IN FLASH:**' rather than '**IN OFD:**'.

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

Setting the static fallback IP address from the Management Console

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

How to Display Processor Information

The **Processor** field on the AWI Home page for a client displays the name of the device's processor, or chipset.

The screenshot shows the PCoIP Zero Client interface. At the top, there are navigation links: 'Log Out' and 'PCoIP® Zero Client'. Below that is a breadcrumb trail: 'Home Configuration / Permissions / Diagnostics / Info / Upload'. The main content area features the PCoIP logo and a title 'PCoIP® Zero Client'. Underneath, it states 'PCoIP® device status and statistics for the current session.' The processor information is listed as 'Processor: TERA2140 Revision 1.0 (512 MB)', with 'Processor: TERA2140' circled in red. Other statistics include 'Time Since Boot: 0 Days 16 Hours 37 Minutes 53 Seconds', 'PCoIP Device Name: pcoip-portal-0030040ddbcb', 'Connection State: Connected to host 192.168.65.103', '802.1X Authentication Status: Disabled', and 'Session Encryption Type: AES-256-GCM'. Network and pipeline statistics are also provided. At the bottom, there is a table with columns for 'Display', 'Maximum Rate: Refresh Rate', 'Output Process Rate', and 'Image Quality'.

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 client.

The screenshot shows the 'Version' page of the PCoIP Host Card. The page has a navigation bar at the top with 'Log Out' on the left and 'PCoIP® Host Card' on the right. Below the navigation bar is a breadcrumb trail: 'Home / Configuration / Permissions / Diagnostics / Info / Upload'. The main content area features the PCoIP logo and a decorative arc of small icons. The 'Version' section is titled 'Version' and contains the text 'View the hardware and firmware version information'. The information is presented in a list of key-value pairs, with the 'PCoIP Processor Family: Tera2' line circled in red. The information includes MAC Address, Unique Identifier, Serial Number, Firmware Part Number, Hardware Version, Firmware Version, Firmware Build ID, Firmware Build Date, PCoIP Processor Family, PCoIP Processor Revision, Bootloader Version, Bootloader Build ID, and Bootloader Build Date.

Log Out **PCoIP® Host Card**

Home Configuration / Permissions / Diagnostics / Info / Upload

Version

View the hardware and firmware version information

MAC Address: 00-30-04-0D-EB-A3
Unique Identifier: 00-30-04-0D-EB-A3
Serial Number: default serial number 123-456-789
Firmware Part Number: FW020004
Hardware Version: default version number 123-456-789

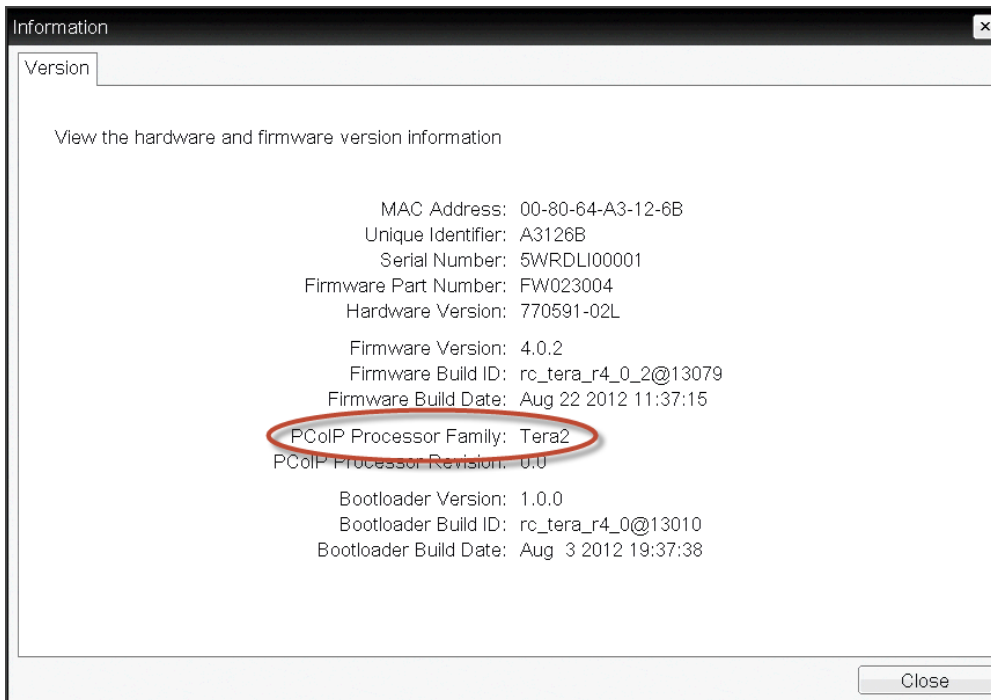
Firmware Version: 4.0.2
Firmware Build ID: rc_tera_r4_0_2@13079
Firmware Build Date: Aug 22 2012 11:36:50

PCoIP Processor Family: Tera2
PCoIP Processor Revision: 1.0

Bootloader Version: 1.0.0
Bootloader Build ID: rc_tera_r4_0@13010
Bootloader Build Date: Aug 3 2012 19:37:38

Processor Family Information on AWI Version Page

You can also display the processor family name for a Tera2 PCoIP Zero Client on the [OSD Version page](#) for the device.



Processor Family Information on OSD Version Page

How to Upload Firmware to a Tera2 PCoIP Zero Client

To upload a firmware release to a client:

1. Log in to the client's AWI.
2. Select the **Upload > Firmware** menu and 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**.



Note: To downgrade the firmware to an earlier version, reset the device to factory defaults

If you want to downgrade the firmware to an earlier version, Teradici recommends that you first [reset the device parameters to factory defaults](#), and upload the earlier version of the firmware and [reconfigure your device settings](#).

How to Upload a Certificate to a Tera2 PCoIP Zero Client

To upload a certificate to a client:

1. Log in to the client's AWI.
2. Select the **Upload > Certificate** menu and browse to the folder containing the certificate file. This file will have a **'.pem'** extension.
3. Double-click the correct **'*.pem'** certificate file.
4. Click **Upload**.
5. Click **OK** to confirm that you want to proceed with the upload.
6. Click **Continue**.

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

How to Troubleshoot a Tera2 PCoIP Zero Client in Recovery Mode

If your Tera2 PCoIP Zero Client firmware goes into recovery mode, here are some steps to troubleshoot the problem:

- It is possible that the client was forced into recovery mode by a user repeatedly tapping the power button when turning on the zero client. If so, rebooting the zero client will return it to the main firmware.
- If the zero client does not load the main firmware but boots into the recovery image immediately when powered up, then it is likely that a firmware upload operation was interrupted and the client does not contain a valid firmware image. [Upload a new firmware image](#) to the zero client and reboot the client to return to working firmware.
- If the zero client attempts to boot to the main firmware images a few times (the splash screen is displayed for a bit) but eventually switches to the recovery image, then it is likely that the firmware configuration is not valid. [Reset the device parameters to factory defaults](#) to clear this problem and re-provision the device.

How to Configure an Endpoint Manager

This topic explains how to configure your Tera2 PCoIP Zero Client for discovery by an Endpoint Manager, for example, Teradici's PCoIP Management Console Enterprise Edition. For more information about endpoint managers, see [AWI: Management on page 70](#) and also the [PCoIP® Management Console 2.4 Administrators' Guide](#).

Tera2 PCoIP Zero Clients support three main discovery methods:

- [Automatic discovery via DHCP or DNS Server Provisioning](#)
- [Manual Discovery Initiated by an Endpoint Manager](#)
- [Configuring a PCoIP Zero Client with an Endpoint Manager](#)

Automatic Discovery via DHCP or DNS Server Provisioning

To configure automatic discovery via DHCP or DNS server provisioning:

1. From the AWI **Configuration** menu, select **Management**.
2. In the **Security Level** drop-down list, select *either* **Medium Security Environment** or **Low Security Environment**:
 - **Medium Security Environment – Endpoint Bootstrap Manager must be trusted by installed certificate:** If you select this security level, your DHCP or DNS server must provision the client with the PCoIP Management Console's uniform resource identifier (URI), *and* the zero client must have a PCoIP Management Console certificate in its trusted certificate store.
 - **Low Security Environment – Zero Client is discoverable by Endpoint Managers:** If you select this security level, your DHCP or DNS server must provision the client with the PCoIP Management Console's URI *and* its certificate fingerprint.
3. In the **Manager Discovery Mode** drop-down list, select **Automatic**.
4. Click **Apply** and then **Continue**.

Once the device is discovered, its discovery information and Endpoint Manager topology are displayed in the **Management** page:

Management
Configure how this zero client is managed

Phase: Managed

Management Status: Connected to Endpoint Manager: 10.0.153.242:5172

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

Manager Discovery Mode: Automatic

Discovery Method	Discovery Outcome	Endpoint Bootstrap Manager Address	Certificate Fingerprint
Discovery Information: DHCP Options	Successfully found an Endpoint manager address 10.0.153.242		B7:62:71:01:85:27:46:8B:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
DNS SRV Records	Not used		

EM Topology:	URI Type	EM URI	Certificate Fingerprint
Internal EM URI:	wss://	10.0.153.242:5172	B7:62:71:01:85:27:46:8B:E3:E9:5C:E2:34:2C:B5:76:7D:7A:F1:7F:6A:4D:5C:DB:AA:2B:99:BD:D5:A9:28:91
External EM URI:			

Clear Management State

Apply Cancel

Successful automatic discovery



Related Information: Configuring your system for automatic discovery

For information about how to configure your system for automatic discovery, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

Manual Discovery Initiated by an Endpoint Manager

Complete these steps in the following sequence.

To configure manual discovery initiated by an Endpoint Manager (PCoIP Management Console 2.0):

1. From the AWI **Configuration** menu, select **Management**.
2. In the **Security Level** drop-down list, select **Low Security Environment**.
3. If the client is not in the **Idle** state, click **Clear Management State** and then **Continue**.
4. Click **Apply** and **Continue** once more.

Once the device is discovered, its discovery information and Endpoint Manager topology are displayed in the **Management** page:

Successful manual discovery initiated by an Endpoint Manager (PCoIP Management Console 2.0)



Related Information: Initiating discovery from a PCoIP Management Console

For information about initiating discovery from a PCoIP Management Console, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

Configuring a Tera2 PCoIP Zero Client with an Endpoint Manager

Complete these steps in the following sequence.

To configure a PCoIP Zero Client with an Endpoint Manager:

1. From AWI **Configuration** menu, select **Management**.
2. Optionally, in the **Security Level** drop-down list, select **High Security Environment**.
3. In the **Manager Discovery Mode** drop-down list, select **Manual**.
4. If the zero client is not in the **Idle** state, click **Clear Management State** and then **Continue**.
5. Enter the URI for your PCoIP Management Console.

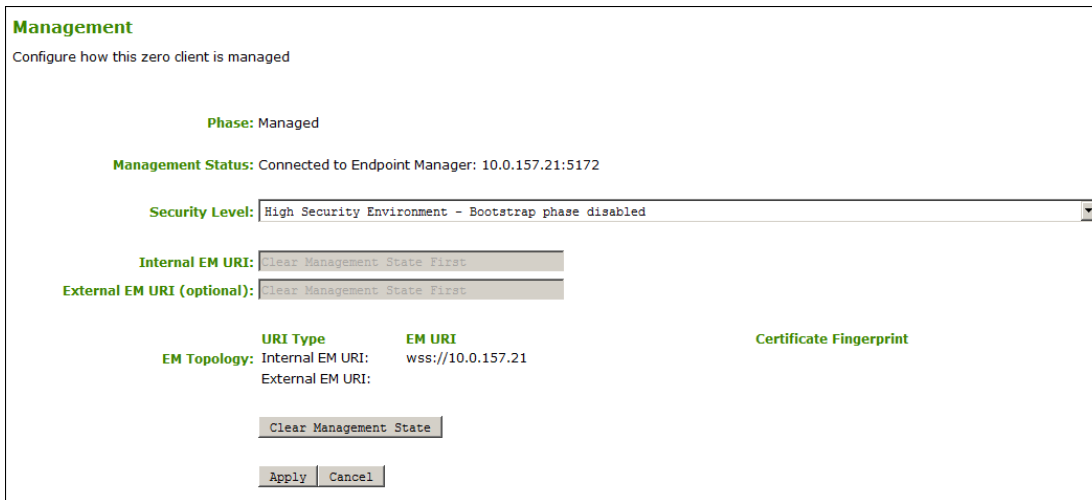


Note: Uniform Resource Identifier requires a secured WebSocket prefix

URIs require a secured WebSocket prefix (for example, `wss://<internal EM IP address/FQDN>:[port number]`). The MC's listening port is 5172. Entering this port number is optional. If you do not include it, port 5172 will be used by default.

6. Click **Apply** and then **Continue** once more.

Once the device is discovered, its Endpoint Manager topology is displayed in the **Management** page:



Successful discovery initiated by a zero client

How to Configure 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 Tera2 PCoIP 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 Tera2 PCoIP Zero Clients softphone client. For more information about this softphone client, see [AWI: Unified Communications on page 216](#).

System Requirements for VLAN Tagging

A Tera2 PCoIP Zero Client will automatically tag voice traffic during a Bria Virtualized Edition softphone VoIP call if your system meets the following requirements:

- The Tera2 PCoIP 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 Tera2 PCoIP 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.

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 Tera2 PCoIP 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 Tera2 PCoIP 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 Tera2 PCoIP 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 following sample search results.

```
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_secondary_dns = 0.0.0.0
```

When [Unified Communications](#) support is enabled on the Tera2 PCoIP Zero Client, the event log will show 'UC Provider: 1' for the **uc_options** entry. When it is not enabled, it will show 'UC Provider: 0'.

```
IN FLASH:          uc_options = UC Provider: 1
```

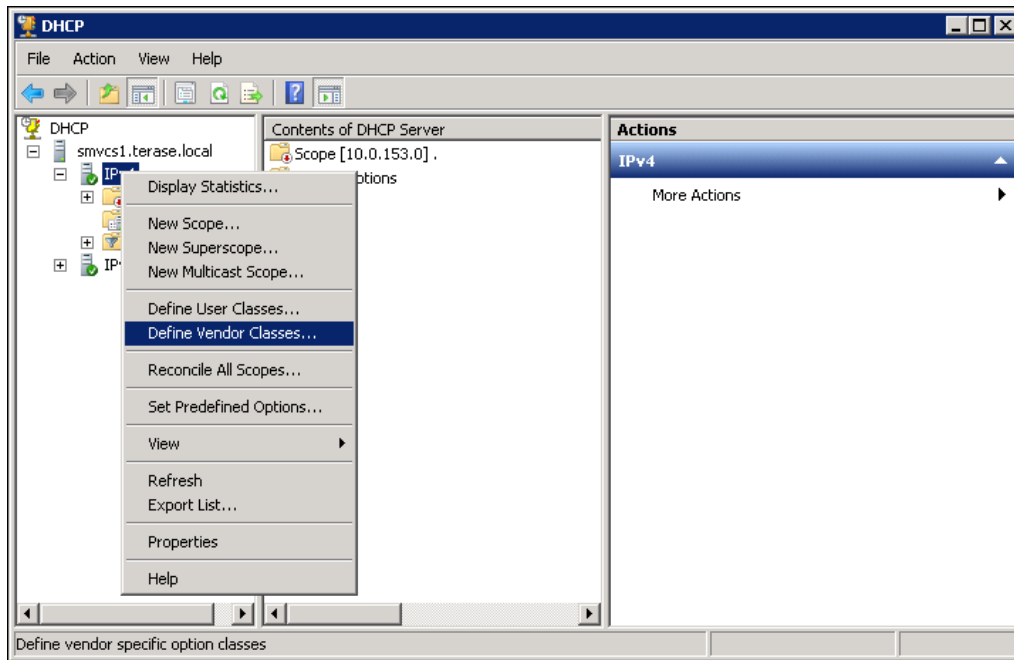
To see the VLAN tag, search for '**dhcp_get_pcoip_option43_vlan_id**'. The following example shows a VLAN tag of **1157**.

```
MGMT_NET:          dhcp_get_pcoip_option43_vlan_id Voice VLAN is present ID =1157 (0x485)
```

Configuring DHCP Option 43

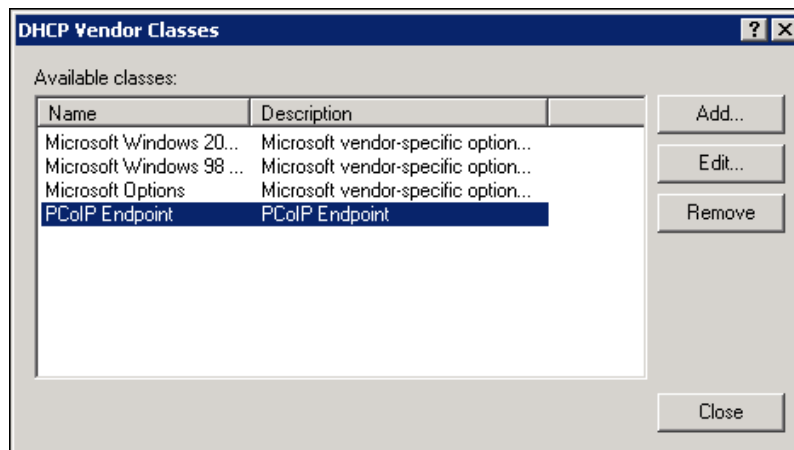
To configure a Windows 2008 DHCP server to send a Voice VLAN tag in option 43:

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**.



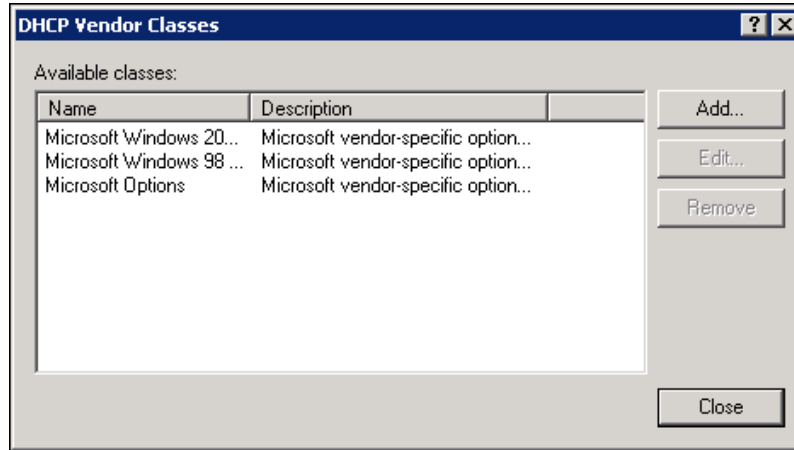
Select Define Vendor Classes

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, close the DHCP Vendor Classes dialog and go to Step 7.



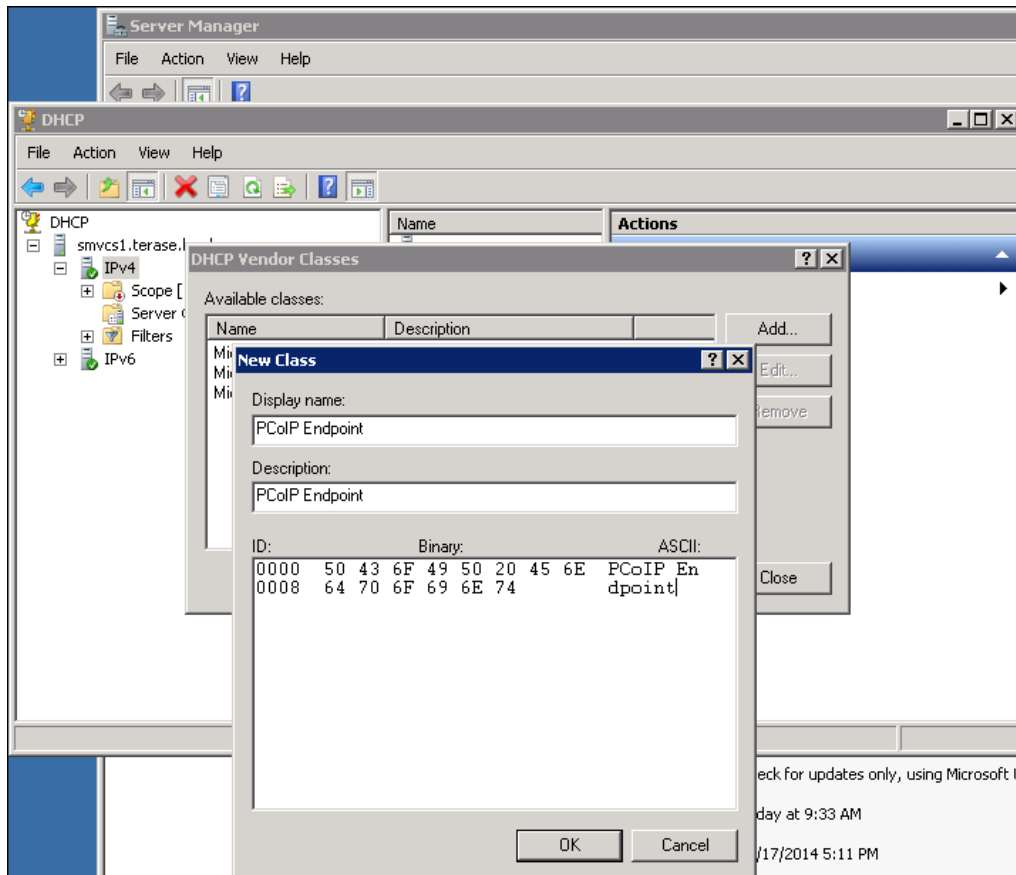
Check the DHCP vendor classes

- If *PCoIP Endpoint* has not been added, click **Add** to add a new vendor class, and continue to the next step.



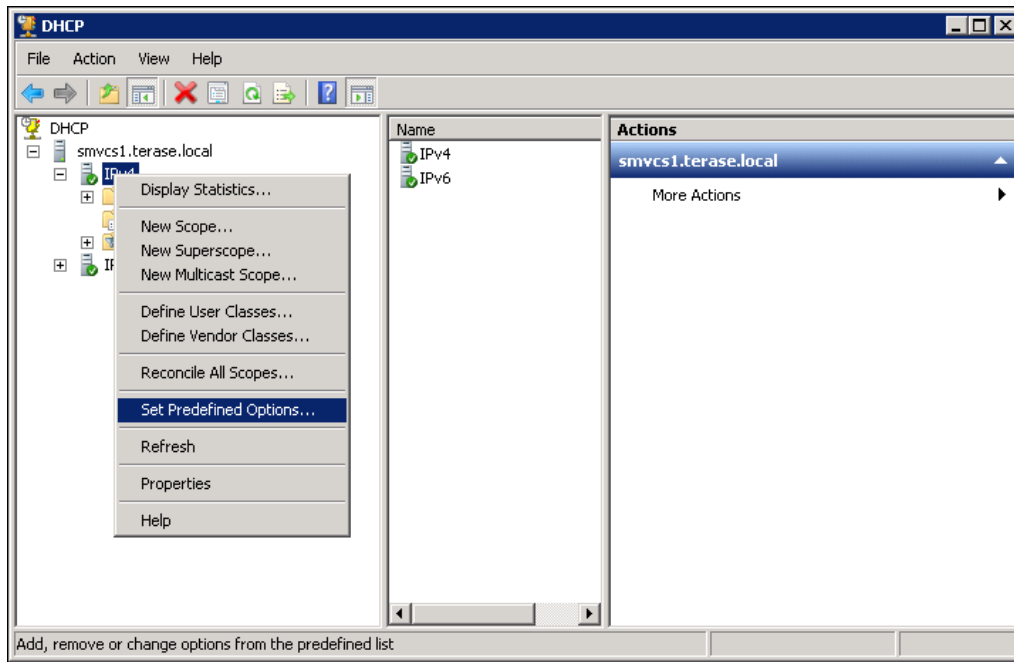
Add a new vendor class

5. In the **Display name** field, enter **PCoIP Endpoint**, and add a description. Also add **PCoIP Endpoint** in the vendor ID **ASCII** column.



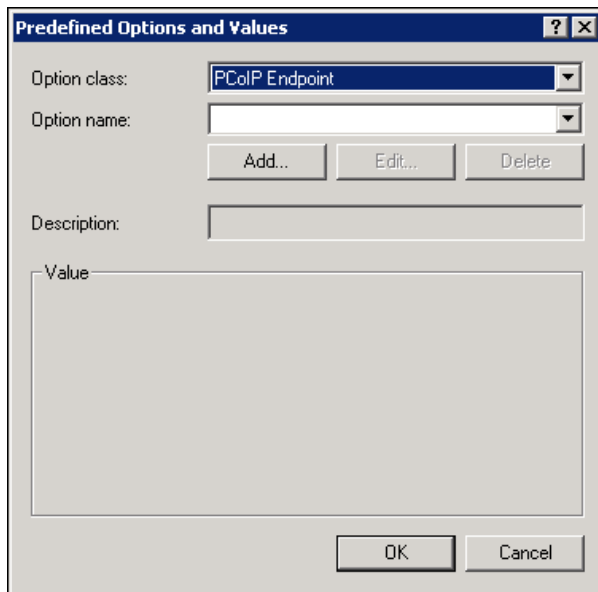
New Class dialog

6. Click **OK** and then **Close**.
7. Right-click on **IPv4** in the tree and select **Set Predefined Options**.



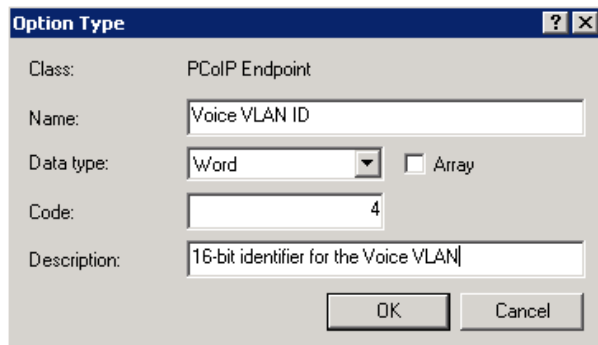
Selecting Set Predefined Options

8. In the **Option class** field, select **PCoIP Endpoint**, and click **Add**.



Configuring the Predefined Options and Values dialog

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**.

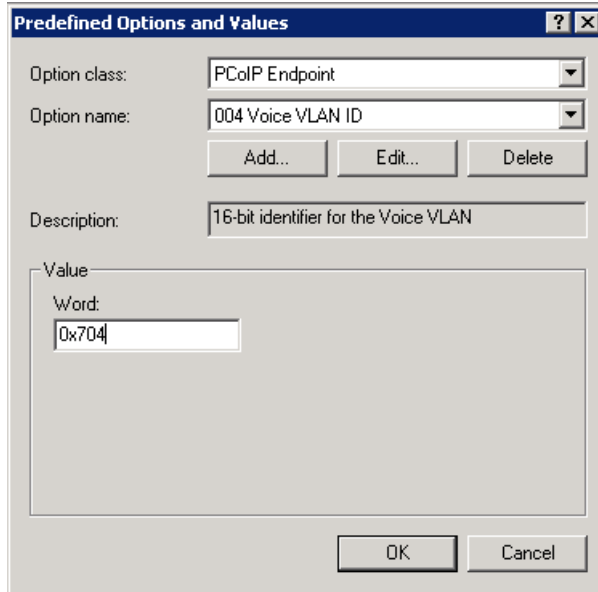


The image shows a dialog box titled "Option Type". It contains the following fields and controls:

- Class: PCoIP Endpoint
- Name: Voice VLAN ID
- Data type: Word (selected in a dropdown menu), with an unchecked checkbox for "Array".
- Code: 4
- Description: 16-bit identifier for the Voice VLAN
- Buttons: OK and Cancel

Configuring the Option Type dialog

11. In the **Value** field, enter a default value (in hexadecimal) for the Voice VLAN ID option.



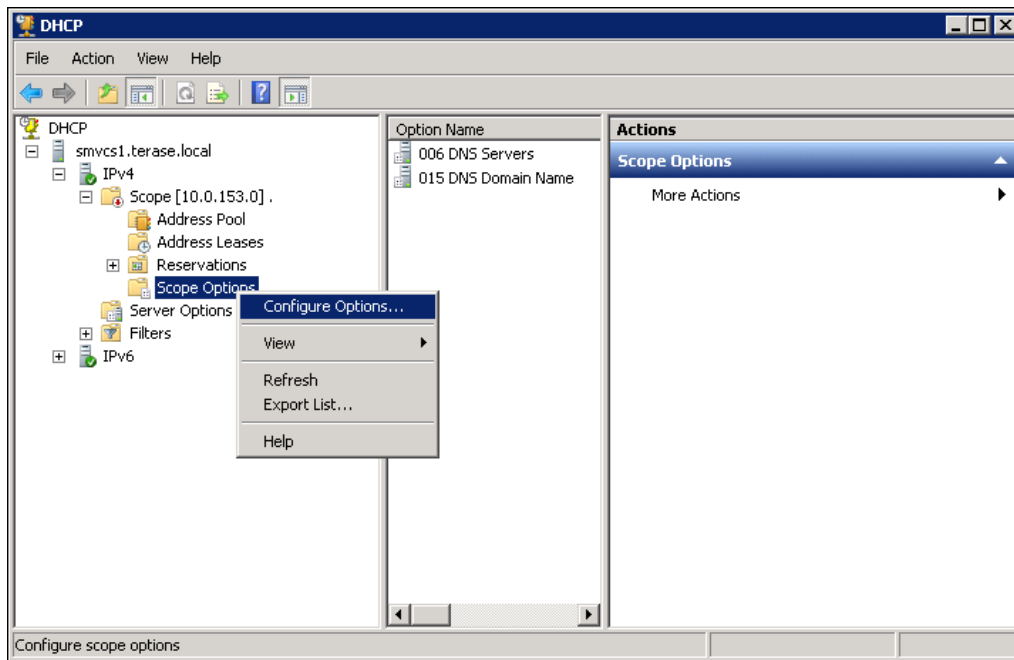
The image shows a dialog box titled "Predefined Options and Values". It contains the following fields and controls:

- Option class: PCoIP Endpoint
- Option name: 004 Voice VLAN ID
- Buttons: Add..., Edit..., Delete
- Description: 16-bit identifier for the Voice VLAN
- Value section:
 - Word: 0x704
- Buttons: OK and Cancel

Entering the default value for the Voice VLAN ID option

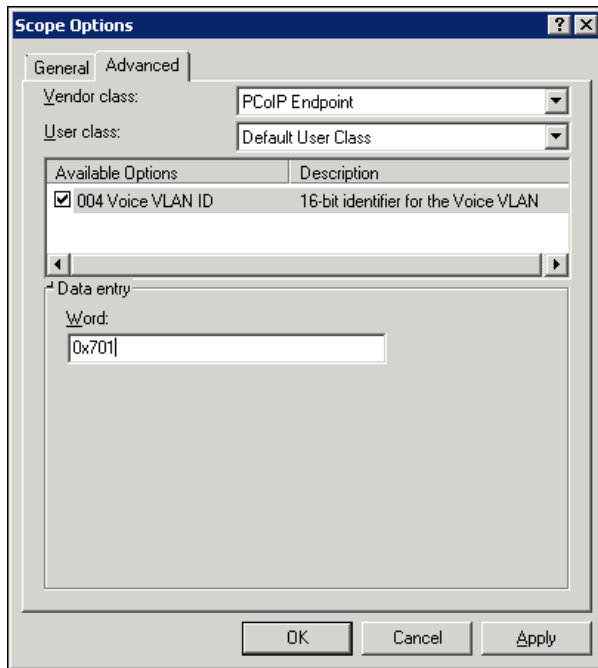
12. If you want to set a different Voice VLAN ID value for a specific scope, expand the desired scope tree within your IPv4 tree.

13. Right-click on **Scope Options** and select **Configure Options**.



Selecting the 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 enter a value in the **Data entry** field. This value will apply only to your selected scope.



Configuring the Scope Options dialog

16. Click **OK**.

How to Set 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

To install the touch screen to the zero client:

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



Note: Do not attach multiple touch screens to the PCoIP Zero Client

You cannot attach multiple touch screens to the Tera2 PCoIP Zero Client, but you can attach additional non-touch screens to the Tera2 PCoIP Zero Client in addition to the touch screen as long as the touch screen is attached to the port on the Tera2 PCoIP Zero Client that is configured as the [primary port](#).

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



Note: Touch screen's co-ordinates are saved in flash memory

Once the touch screen is calibrated, the co-ordinates are saved in flash memory. You can manually recalibrate the screen as required through the OSD [Touch Screen](#) page.

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

Setting up the Touch Screen as a Bridged Device



Note: Setting up a touch screen as a bridged device is optional

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

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

To set up the touch screen as a bridged device:

1. Follow the steps in the previous procedure to install the touch screen to your Tera2 PCoIP Zero Client.
2. Log into the Tera2 PCoIP Zero Client AWI.
3. From the **Info** menu, click **Attached Devices**. The touch screen details appear on this page.
4. Write down the **PID** and the **VID** information.

Attached Devices											
View presently connected monitors and USB devices											
Displays:											
Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date			
1	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	V7800284067	BNQ	7923	30-2011			
2		Disconnected									
3	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	93802607026	BNQ	7923	10-2011			
4		Disconnected									
USB Devices:											
Device	Parent	Controller	Model	Status	Device Class	Sub Class	Protocol	Serial	VID	PID	Internal/External
1F00	Root 3	OHCI	USB Optical Mouse	Locally Connected	00	00	00	-	046D	C05A	External
2001	Root 1	OHCI	USB Keyboard	Locally Connected	00	00	00	-	046D	C31C	External
2102	Root 0	OHCI	Elo TouchSystems 2700 IntelliTouch(r) USB Touchmonitor Interface	Locally Connected	00	00	00	20E38185	04E7	0020	External

VID and PID numbers

5. From the **Permissions** menu, click **USB** to display the **USB** page.
6. In the **Bridged Devices** area, click **Add New**.

USB permissions table

7. Enter the Vendor ID and Product ID for the touch screen, and then click **Apply**.
8. Restart the Tera2 PCoIP 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.

To configure the zero client to automatically log into a host brokered by a connection manager:

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

How to Configure a PCoIP Zero Client as a Bria Softphone Endpoint

The Tera2 PCoIP Zero Client supports interoperability with CounterPath's Bria Virtualized Edition for PCoIP Zero Clients softphone client installed on [Teradici Cloud Access Platform desktops and workstations](#), [VMware Horizon desktops](#), and [Amazon WorkSpaces desktops](#).



Related Information: Bria Virtualized Edition softphone client

For instructions on how to purchase, install, and use the Bria Virtualized Edition softphone client on your desktop or workstation, see Bria Virtualized Edition softphone client documentation.

To configure a Tera2 PCoIP Zero Client as a Bria Softphone Endpoint:

1. Log in to the PCoIP Zero Client's AWI.
2. Select the **Configuration > Unified Communications** menu.
3. Enable the **Enable Unified Communications** check box if it is unchecked.
4. Click **Apply**.
5. Click **Reset**.

When Unified Communications (UC) is enabled, users can use their Tera2 PCoIP Zero Client to connect to a PCoIP desktop or workstation and use the Bria Virtualized Edition softphone client to initiate UC services (for example, voice, messaging, presence information, and contacts) with caller endpoints. Once the Bria softphone client establishes the connection, call traffic is routed directly between the Tera2 PCoIP Zero Client and the caller endpoint, thus offloading this traffic from the data center. If desired, you can set up [VLAN tagging](#) for QoS management of users' VoIP call data.

Tera2 PCoIP Zero Clients support any type of analog headset. In addition, the following USB headsets have been tested with this application:

- Plantronics Blackwire C310 and C320 USB
- Plantronics Blackwire C435
- Plantronics Blackwire C510 and C520
- Plantronics Blackwire C710 and C720



Note: Tera2 PCoIP Zero Clients may support other USB headsets

Other USB headsets may also work with this application, but have not been tested at this time.

How to Configure 802.1x Network Device Authentication

Prerequisites

An 802.1x authentication system requires the following components:

- Tera2 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)
- A switch with 802.1x support configured

Procedure

Overview

To configure 802.1x device authentication, perform 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: Following sections assume you are using Windows Server 2008 R2

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

Create a Client User

To create a client user:

1. Log in to the Windows 2008 server.
2. Click **Start > Administrative Tools > Server Manager**.

3. Navigate to **Roles > Active Directory Domain Services > Active Directory Users and Computers > <domain.local> > Users**.
4. Right-click **Users**, select **New > User**, and follow the wizard.

Export the Root CA Certificate

To export the root CA certificate:

1. Log in to the Certificate Authority (CA) server.
2. Open a Microsoft Management Console window (for example, enter **mmc.exe** in the **Start** menu search field).
3. From the console window, select **File > Add/Remove Snap-in**.
4. Add the **Certificates** snap-in, selecting **Computer account** and then **Local computer**.
5. Click **Finish**, and **OK** to close the Add or Remove Snap-ins dialog.
6. From the console, select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
7. In the right panel, right-click the certificate, and select **All Tasks > Export**.
8. Follow the wizard to export the certificate:
 - a. Select **Base-64 encoded X.509 (.CER)**.
 - b. Click **Browse**, specify a name and location for the certificate, and click **Save**.
 - c. Click **Finish**, and then **OK**.

Create a Certificate Template for Client Authentication

To create a certificate template for client authentication:

1. From the CA server, click **Start > Administrative Tools > Certification Authority**.
2. Expand the tree for your CA.
3. Right-click **Certificate Templates**, and click **Manage**.
4. Right-click the **Computer** template, and click **Duplicate Template**.
5. Configure the template as follows:
 - a. From the **Compatibility** tab, select **Windows Server 2003**.
 - b. From the **General** tab, enter a name for the template (for example, 'PCoIP Zero Client 802.1x') and change the validity period to match the organization's security policy.
 - c. From the **Request Handling** tab, select **Allow private key to be exported**.
 - d. From the **Subject Name** tab, select **Supply in the request**.
 - e. From the **Security** tab, select the user who will be requesting the certificate, and give **Enroll** permission to this user.
 - f. Click **OK** and close the **Certificate Templates Console** window.

6. From the Certification Authority window, right-click **Certificate Templates**, select **New**, and click **Certificate Template to Issue**.
7. Select the certificate you just created (that is, 'PCoIP Zero Client 802.1x'), and click **OK**. The template will now appear in the **Certificate Templates** list.
8. Close the window.

Issue the Client Certificate

To issue the client certificate:



Note: Use Internet Explorer to log in to certificate server

Do not use any other browser except Internet Explorer to log into the certificate server.

1. Using Internet Explorer on your local machine, go to your Certificate Authority URL using the format **https://<server>/certsrv/** (for example, '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 (for example, 'Zero Client 802.1x').
 - b. In the **Identifying Information for Offline Template** section, enter the account name in the **Name** field. The other fields are not required.



Caution: Enter the same name as the universal principal name of the client user

The name you enter in the Name field must be the universal principal name (UPN) of the client user you created in [Create a Client User](#) (for example, 'ZeroClient@mydomain.local').

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

Export the Client Certificate

To export the client certificate:

1. From the machine on which you issued the certificate, open a Microsoft Management Console window (for example, enter **mmc.exe** in the **Start** menu search field).
2. From the console window, select **File > Add/Remove Snap-in**.
3. Add the **Certificates** snap-in, selecting **My user account**.
4. Click **Finish**, and then **OK** to close the Add or Remove Snap-ins dialog.
5. Select **Certificates - Current User > Personal > Certificates**.
6. In the right panel, right-click the certificate, and select **All Tasks > Export**.
7. Follow the wizard to export the certificate:
 - a. Click **Yes, export the private key**.
 - b. Select **Personal Information Exchange - PKCS #12 (.PFX)**.
 - c. Enter a password for the certificate.
 - d. Click **Browse**, specify a name and location for the certificate, and click **Save**.
 - e. Click **Finish**, and then **OK**.
8. Repeat Steps 5 to 7 again to export the Tera2 PCoIP Zero Client certificate, but this time *without* the private key (**No, do not export the private key**), selecting the **DER encoded binary X.509 (.CER)** format instead of the PKCS format.
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

To convert the certificate format from .pfx to .pem:

1. Download and install Windows OpenSSL from <http://www.slproweb.com/products/Win32OpenSSL.html>. (The light version is sufficient.)
2. Copy the .pfx client certificate file you saved above to the `C:\OpenSSL-Win32\bin` directory.
3. Open a command prompt window, and enter the following command to convert the certificate format from .pfx to .pem:


```
C:\OpenSSL-Win32\bin\openssl.exe pkcs12 -in <client_cert>.pfx
-out <client_cert>.pem -nodes
```

 where `<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 Tera2 PCoIP Zero Client certificate requires its private key in RSA format, you need to replace its private key with this RSA private key.
 - b. Copy the entire contents of the RSA .pem file (everything from -----BEGIN RSA PRIVATE KEY ----- to -----END RSA PRIVATE KEY-----), and paste it into the original .pem file, replacing its private key with this RSA private key.

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 Tera2 PCoIP Zero Client.

Import the Client Certificate into the Client User Account

To import the client certificate into the client user account:

1. Log in to the Windows 2008 server.
2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. From the **View** menu, select **Advanced Features**.
4. Navigate to the user you created for the Tera2 PCoIP Zero Client.
5. Right-click the user, and select **Name Mappings**.
6. In the **X.509 Certificates** section, click **Add**.
7. Locate and select the Tera2 PCoIP Zero Client certificate you exported that does not contain the private key (This file was saved to a network location in Step 9 of [Export the Client Certificate](#).)
8. Leave both identity boxes checked, click **OK**, and click **OK** again.

Import the Certificates to Client Device

To import the certificates into a profile using the PCoIP Management Console, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

To import the certificates to a device using the AWI:

1. From a browser, log into the AWI for the Tera2 PCoIP Zero Client or PCoIP Remote Workstation Card.
2. From the AWI 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 click **Select**.
8. Enter the identity name of the certificate. Typically, this is the universal principal name (UPN) that appears after **Subject:** (for example, 'zeroclient@mydomain.local').

**Note: Windows server may be configured to use the certificate's Subject, the Subject Alternative Name, or another field**

For the identity, your Windows server may be configured to use the certificate's **Subject**, the **Subject Alternative Name**, or another field. Check with your administrator.

9. Click **Apply**, and then **Reset**.

For more information about 802.1x, see the following Knowledge Base topics:

- Support for 802.1x on Tera2 PCoIP Zero Clients: [Do PCoIP Zero Clients support network authentication or 802.1x? \(KB 15134-590\)](#)
- Setting up Windows Server 2008 R2 as an 802.1x authentication server: [How to setup Windows Server 2008 R2 as an 802.1X Authentication Server \(KB 15134-1245\)](#)
- General 802.1x troubleshooting steps: [PCoIP TROUBLESHOOTING STEPS: IEEE 802.1x Network Authentication \(KB 15134-928\)](#)

How to Configure Syslog Settings

You can configure syslog settings for a Tera2 PCoIP Zero Client from the device's AWI, or you can use PCoIP Management Console to configure settings for a device profile. Configuration involves entering the IP address or Fully Qualified Domain Name (FQDN) for the syslog server, and 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: Facility values used by Cisco equipment

Cisco IOS devices, CatOS switches, and VPN 3000 concentrators use the '23 – local use 7' facility. Cisco PIX firewalls use the '20 – local use 4' facility.



Note: Ensure the syslog server can manage volume of messages

Ensure that your syslog server can handle the volume of messages sent by a Tera2 PCoIP 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 Tera2 PCoIP Zero Client or host.
2. Select the **Diagnostics > Event Log** menu to display the Event Log page.
3. Check **Enable Syslog**, and 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**.

Security

Tera2 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, Tera2 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, zero clients are the most trusted client wherever security and performance are critical.

Configuring Security Settings

You can configure security settings for individual Tera2 PCoIP Zero Client devices from the AWI. Administrative access security settings can be configured from both the AWI and OSD. For information on how to configure security for multiple devices from the PCoIP Management Console, see the [PCoIP® Management Console 2.4 Administrators' Guide](#).

AWI 802.1x Settings

The following settings are located on the AWI [Network](#) page (accessed from the **Configuration > Network** menu):

- Enable 802.1x Security
- Authentication
- Identity
- Client Certificate
- Enable 802.1x Legacy Support

See [Configuring 802.1x Network Device Authentication](#) in the 'How To' Topics section for instructions on how to configure Tera2 PCoIP Zero Clients for 802.1x authentication.

AWI Management Settings

You can configure how a Tera2 PCoIP Zero Client will be managed from the AWI through the Administrative Access Settings.

Additional AWI and OSD security settings are available through PCoIP Management Console profile properties, including password settings and the option to hide some OSD menus. For more information, see the Managing Profiles section of the [PCoIP® Management Console 2.4 Administrators' Guide](#) and the tooltip in the profile's Security section.

Administrative Access Settings

The following administrative access settings are located on the [Access](#) page (accessed from the AWI **Configuration > Access** menu and the OSD **Options > Configuration > Access** menu):

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

Encryption Settings

This section lists the cipher suites and encryption algorithms available when using a Zero Client in a PCoIP session to a PCoIP host. A PCoIP Host defined in this document is a hardware or software end point that communicates with the PCoIP protocol.

There are a variety of secure connections made to establish a PCoIP session depending on your deployment. Each set of encryptions are listed from the ways in which the Zero Client is being used, either as a server or a client.

When a Zero Client is Used as a Server

Connecting to the AWI Using a Browser

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



Note: Use Firefox, Chrome, Internet Explorer 11, and Edge

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

The following list identifies the cipher suites used to secure a browser to AWI session in order of preference:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_TLS_RSA_WITH_AES_128_CBC_SHA_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA

Endpoint Management Tools Endpoint Discovery

Zero Clients not yet managed by PCoIP endpoint management tools such as PCoIP Management Console 2 listen for management tools to manage it. When a request for

management of a zero client occurs, the process that establishes communications between the management tool and the zero client (endpoint discovery) is done securely using one of the following list of supported cipher algorithms. There is a minimum required SSL version of TLS 1.1:

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

When a Zero Client is Used as a Client

PCoIP Management Protocol (Manual or Automatic Provisioning with Desired Endpoint Manager)

Once a management tool discovers a zero client to manage, the PCoIP Management Protocol securely administers the zero client using one of the following listed cipher suites. There is a minimum required SSL version of TLS 1.1:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

User Authentication and Resource Selection in a VMware Horizon (View) Environment

Zero clients connecting to a PCoIP host in a VMware Horizon environment must first be authenticated before being offered a permitted PCoIP host. Authentication is securely performed by a Horizon (View) Connection Server over port 443 using one of the supported cipher suites. As of firmware 5.1, configurations of the cypher suites can only be configured at the host, and have a minimum required SSL version of TLS 1.0:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

User Authentication and Resource Selection in a PCoIP Connection Manager Environment

Zero clients connecting to a PCoIP host in an environment that uses a PCoIP Connection Manager must first be authenticated before being offered a permitted PCoIP host. Authentication is securely performed by a PCoIP Connection Manager over port 443 using one of the supported cipher suites.

The complete list of supported cipher suites can only be configured at the host, and have a minimum required SSL version of TLS 1.0:

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

PCoIP Session Negotiation to a PCoIP Host

Prior to data being transferred between a Tera2 PCoIP Zero Client and a PCoIP host, the session must be negotiated. Negotiation communications are securely completed using one of the following Max Compatibility and Suite B cipher suites:

Max Compatibility security level cipher suites have a minimum required SSL version of TLS 1.0

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

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

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


- TLS_ECDHE_ECDSA_RSA_WITH_AES_256_GCM_SHA384

PCoIP Session Cipher Algorithms

Tera2 PCoIP Zero Clients enable the AES-128-GCM and AES-256-GCM session encryption algorithms for all PCoIP data sessions. As of firmware release 5.0, these algorithms are now host-only settings and can no longer be configured from the client's AWI.

Failed Login Attempt Message

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

Technology Reference

PCoIP connection brokers are resource managers that dynamically assign host PCs to Tera2 PCoIP Zero Clients based on the identity of the user establishing a connection from the Tera2 PCoIP Zero Client. Connection brokers are also used to allocate a pool of hosts to a group of Tera2 PCoIP Zero Clients. If the Tera2 PCoIP Zero Clients in a PCoIP deployment are configured to always connect to the same host (that is, a static one-to-one pairing), then a connection broker is not required.

For connecting clients and hosts, a number of third-party connection brokers support the PCoIP technology. For more information, see [Can I use a connection broker with PCoIP technology? \(KB 15134-24\)](#).

For VDI implementations, the View Connection Server broker is used to connect Tera2 PCoIP Zero Clients to VMware Horizon virtual desktops. You can also use the View Connection Server broker to connect PCoIP clients and host PCs. For more information, see [Using PCoIP® Host Cards with VMware View](#).

DVI and DisplayPort Interfaces

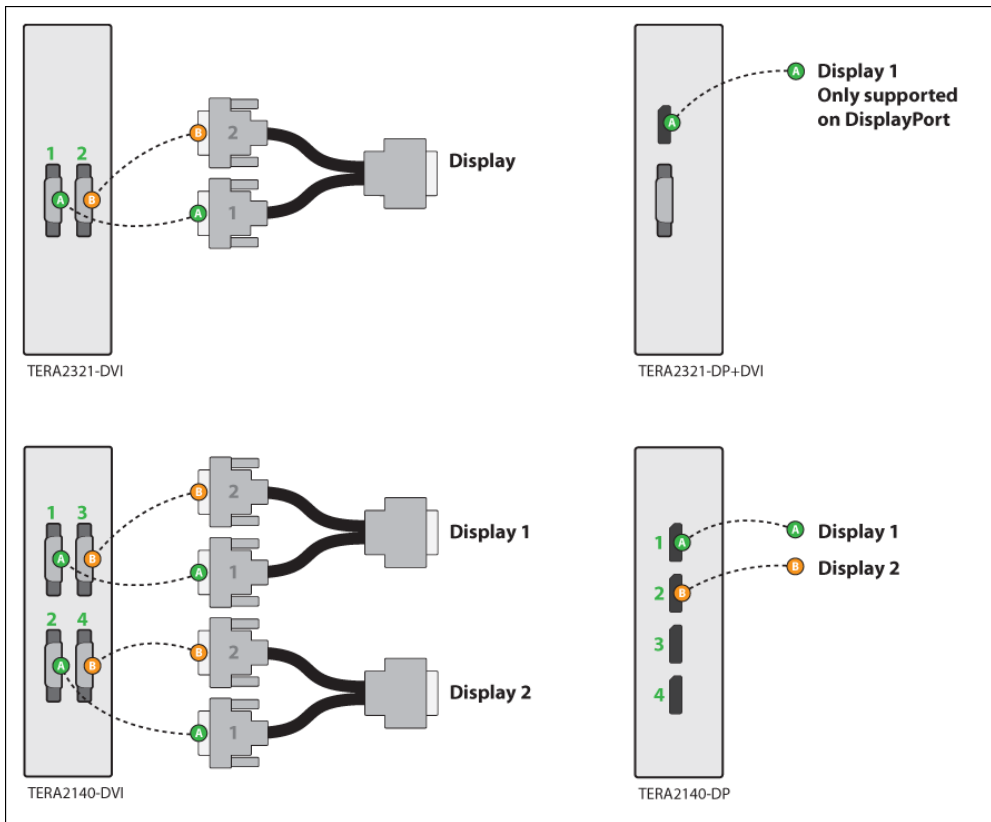
Tera2 PCoIP Zero Clients support both DVI and DisplayPort digital display interfaces. The following port options are available for these clients:

- TERA2321 DVI-I dual-display Tera2 PCoIP Zero Client: contains two DVI ports.
- TERA2321 DP+DVI-I dual-display Tera2 PCoIP Zero Client: contains one DVI port and one DisplayPort port.
- TERA2140 DVI-D quad-display Tera2 PCoIP Zero Client: contains four DVI ports.
- TERA2140 DP quad-display Tera2 PCoIP Zero Client: contains four DisplayPort ports.

Support for 2560x1600 Display Resolution

All of the previous Tera2 PCoIP Zero Clients also support 2560x1600 resolution for attached monitors with either DVI or DisplayPort interfaces. However, a custom dual-link DVI cable adapter is required to support this resolution for DVI interfaces.

The following figure illustrates how to connect video cables to each type of Tera2 PCoIP Zero Client to achieve 2560x1600 resolution on a connected display.



Connecting video cables to each type of Tera2 PCoIP Zero Client

DVI and DisplayPort Connectors for 2560x1600 Resolution

- TERA2321 DVI-I dual-display Tera2 PCoIP Zero Client: This PCoIP Zero Client supports one 2560x1600 monitor. Connect the two DVI-I cable connectors on a custom dual-link DVI-I cable adapter to the two DVI-I ports on the Tera2 PCoIP Zero Client, as shown in the previous illustration (upper left).
- TERA2321 DP+DVI-I dual-display Tera2 PCoIP Zero Client: This Tera2 PCoIP Zero Client supports one 2560x1600 monitor on the DisplayPort interface only. Connect the connector on a DisplayPort cable to the DisplayPort port on the Tera2 PCoIP Zero Client, as shown in the previous illustration (upper right).
- TERA2140 DVI-D quad-display Tera2 PCoIP Zero Client: This client supports up to two 2560x1600 resolution monitors. For each monitor, connect the two DVI-D cable connectors on a custom dual-link DVI-D cable adapter to the two DVI-D ports that are shown in the previous illustration (lower left). These connectors must be connected to ports on the client exactly as shown.
- TERA2140 DP quad-display Tera2 PCoIP Zero Client: This Tera2 PCoIP Zero Client supports up to two 2560x1600 monitors. For each one, connect the connector on a DisplayPort cable to a DisplayPort port on the Tera2 PCoIP Zero Client, as shown in the previous illustration (lower right).

Local Cursor and Keyboard

Local cursor and keyboard is a feature of the PCoIP Host Software that improves usability for PCoIP sessions operating over WAN connections (latency > 40 ms). When enabled, it enables the Tera2 PCoIP 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, see the [PCoIP® Host Software for Windows User Guide](#).

Remote Workstation Cards

PCoIP Remote Workstation Cards are small add-in cards that can be integrated into tower PCs, rack mount PCs, PC blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full desktop environment. This information is communicated in real time over an IP network to the user's Tera2 PCoIP Zero Client.

For complete details about PCoIP Remote Workstation Cards, see the Teradici website at www.teradici.com.

Teradici Cloud Access Platform

The Teradici Cloud Access Platform is an extensible platform developed by Teradici that solution providers can integrate into their offerings to deliver secure virtual desktops and workstations using PCoIP technology.

For information about the Cloud Access Platform, you can find the set of Teradici Cloud Access Platform documents in the [Teradici Support Center](#).

PCoIP Software Session Variables

The PCoIP software session variables in Microsoft's Group Policy Object (GPO) editor let you configure users' desktops with a collection of parameters that affect PCoIP sessions with soft hosts. These variables are defined in a GPO administrative template file called `pcoip.adm`, which is located on the View Connection Server installation directory

```
(\\'servername'\c$\Program Files\VMware\VMware  
View\Server\extras\GroupPolicyFiles\pcoip.adm).
```

You can enable and configure PCoIP software session variables in either the Group Policy Object editor's **PCoIP Session Variables > Overridable Administrator Defaults** list to enable users to override settings or the **PCoIP Session Variables > Overridable Administrator Defaults** list to prevent users from overriding settings.



Note: Applying Group Policy Object administrative template file for large workplace environments

For large environments, you can apply `pcoip.adm` to a Windows Active Directory organizational unit (OU) or to a machine that you are configuring as a template for a desktop pool. For further details, see *VMware View 5 with PCoIP Network Optimization Guide* from the [VMware Documentation](#) website.

For instructions on how to load the PCoIP session variables template to a virtual machine’s GPO editor, see [How do I set up or override PCoIP software session variables on a virtual machine? \(KB 15134-349\)](#). For detailed information on each PCoIP session variable, see [What are PCoIP session variable GPOs? \(KB 15134-348\)](#).

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 or later installed and/or for scenarios using View 5.1 or later. The PCoIP transport header enables network devices to make better QoS decisions for PCoIP traffic.



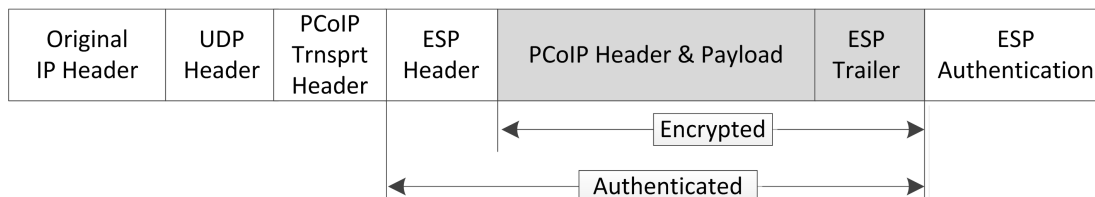
Note: TCP/UDP port 4172 assigned to the PCoIP protocol

TCP/UDP port 4172 is the Internet Assigned Numbers Authority (IANA) port assigned to the PCoIP protocol. UDP port 4172 is used for the session data, and TCP port 4172 is used for the session handshake. For more information about TCP/UDP ports that are used for PCoIP technology, see [What are the required TCP/UDP ports for PCoIP technology? \(KB 15134-114\)](#)

UDP-encapsulated ESP Packet Format

UDP-encapsulated ESP is the default packet format for Tera2 devices with firmware 4.1.0 installed. It is also used for Tera1 devices with firmware 3.x+ installed that connect remotely via a View Security Gateway.

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

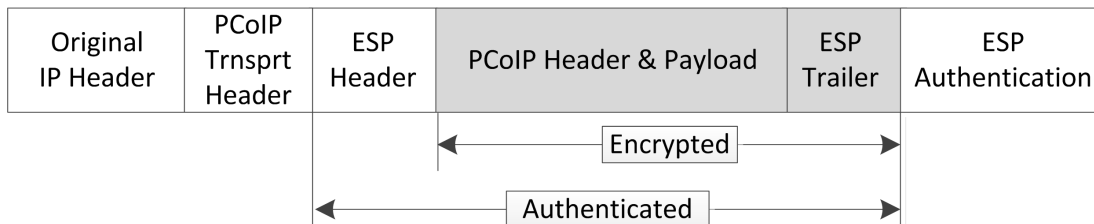


UDP-encapsulated ESP Packet Format

IPsec ESP Packet Format

IPsec ESP encapsulation is the default packet format for direct connections that involve a Tera1 PCoIP Zero Client and/or Tera1 PCoIP Remote Workstation Card.

The IPsec ESP packet format is illustrated in the following figure. This figure also shows the location of the PCoIP transport header in an IPsec ESP packet.



IPsec ESP Packet Format

Tera2 PCoIP Zero Clients

Tera2 PCoIP Zero Clients are secure client endpoints that enable users to connect to a virtual desktop or remote host workstation over a local or wide area IP network. They can take many form factors, such as small stand-alone devices, PCoIP integrated displays, VoIP phones, and touch-screen monitors. Zero clients support multiple wide-screen formats, HD audio and local USB peripherals, and are IPv6-ready. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards and smart cards.

Powered by a single TERA-series processor, Tera2 PCoIP Zero Clients provide a rich multi-media experience for users, who can interact with their desktops from any type of Tera2 PCoIP Zero Client, and even continue the same session as they move between Tera2 PCoIP Zero Client devices.

For complete details about Tera2 PCoIP Zero Clients, see the Teradici website at www.teradici.com.

Requirements for Trusted Server Connections

When connecting a Tera2 PCoIP Zero Client to a PCoIP endpoint using a **View Connection Server** or **PCoIP Connection Manager** session connection type, the padlock icon and 'https' text on the user login screen indicates whether the HTTPS connection is trusted or untrusted (see [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 Tera2 PCoIP Zero Client.

- **Open padlock with red strikethrough 'https:' text:** The connection is secured with HTTPS, but the server's certificate is not trusted by the Tera2 PCoIP Zero Client.

This section explains the certificate requirements that must be in place for each server type in order to have a [trusted HTTPS connection](#). The following tables show which requirements are necessary for each Tera2 PCoIP Zero Client [certificate checking mode](#).



Note: Criteria applied for Auto Detect mode

If you use Auto Detect mode to connect, either the View Connection Server or PCoIP Connection Manager criteria are applied, depending on the server type.

View Connection Server Requirements

When connecting to a View Connection Server, the certificate requirements are as follows:

View Connection Server Certificate Requirements

Certificate Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Valid according to computer clock (not expired and not valid only in the future).	Required	The certificate is accepted if the time is not valid but all other requirements are met. Warn the user before proceeding.	Not checked
Certificate 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 Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Certificate must not be revoked (checked using OSCP (Offensive Security Certified Professional) only if there is a OSCP 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 Requirement	Never connect to untrusted servers	Warn before connecting to untrusted servers	Do not verify server certificates
Certificate must not be revoked (checked using Offensive Security Certified Professional (OSCP) only if there is a OSCP 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, [PCoIP Zero Clients](#), and [PCoIP Remote Workstation Cards](#). Using syslog for logging enables you to centralize the storage of log messages and to capture and maintain a longer history of log data. It also provides a set of tools to filter and report on syslog data.

Syslog messages include a facility level (from decimal 0 to 23) that indicates the application or operating system component that is generating the log message. For example, a facility level of '0' indicates a kernel message, a facility level of '1' indicates a user-level message, and a facility level of '2' indicates a message from a mail system. Processes and daemons that have not been explicitly assigned a facility may use any of the eight 'local use' facilities ('16 – local use 0' to '23 – local use 7') or they may use the '1 – user-level' facility. Facilities enable for easy filtering of messages generated by a device.

Syslog messages are also assigned a severity level from 0 to 7, where a severity level of '0' indicates an emergency panic condition and a severity level of '7' indicates a debug-level message useful to developers but not for operations.

See [Configuring Syslog Settings](#) in the 'How To' section for information on how to configure syslog from the AWI and PCoIP Management Console.

Teradici PCoIP Hardware Accelerator (APEX 2800)

The Teradici PCoIP Hardware Accelerator card provides hardware-accelerated PCoIP image encoding for virtual desktop infrastructure (VDI) implementations. The card constantly

monitors the graphic encoding demands of each virtual machine, dynamically switching the image compression tasks from software image encoding in the CPU to hardware image encoding, and back again. This offloading is performed instantly and seamlessly, as needed, without the user noticing the switch.

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