# PCoIP Zero Client and Host Administrator Guide

TER1206003

Issue 1

Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada
p +1 604 451 5800 f +1 604 451 5818
www.teradici.com

The information contained in this document 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.

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/teradici/pat.php for more information.

# Contents

# Table of Figures

# Table of Tables

# 1 Welcome

## 1.1 Introduction

Welcome to Teradici's PCoIP Zero Client and Host Administrator WebHelp. This help system explains how to configure PCoIP device firmware so you can access and manage the hosts and zero clients in your PCoIP deployment. It comprises the following main sections:

- **What's New**: This section explains the new features for each firmware release, and contains links to topics that provide more information about these features.
- **PCoIP Management Tools**: This section describes how to access and use the following PCoIP management tools:
  - Management Console (MC): The MC lets you centrally control and manage the devices in your PCoIP deployment. This help system explains how to configure a profile (a collection of device configuration settings), which you can then assign to a specific PCoIP group (a set of one or more hosts or clients). The MC is the best tool for medium to large deployments, and is often used in conjunction with a connection broker. For further details, see About the MC.
  - Administrative Web Interface (AWI): The AWI lets you use an Internet browser to remotely access and configure a specific client or host. For further details, see About the AWI.
  - On Screen Display (OSD): The OSD is the graphical user interface (GUI) embedded within a client. It is used to connect the client to a virtual desktop or to a host in a remote workstation. It is also used to configure the client, and has a subset of the configuration parameters available in the MC and AWI. For further details, see About the OSD.
- **PCoIP Deployment Scenarios**: This section illustrates and describes the most common ways to deploy the hosts and clients in your PCoIP network. Configuration steps are included for each scenario, with links to topics in the PCoIP GUI Reference where you can find detailed information. The scenarios are the best place to start when configuring a new deployment.
- **PCoIP GUI Reference**: This section is a detailed reference that describes each configuration parameter that appears in the MC, AWI, and OSD pages. You can use this reference when configuring a device profile using the MC, or when configuring a single device using the AWI or OSD. The PCoIP GUI Reference is organized by the categories listed in the MC's **Manage Profiles** page, but also has special sections for AWI and OSD menus that do not corresponding pages in the MC.
- **PCoIP Technology Reference**: This section contains definitions for some of the terminology used in the help system.

# 2 What's New

## 2.1 What's New in Firmware 4.0.2

The Teradici firmware 4.0.2 release provides the following features and enhancements:

- **Tera2 processor family support**: Firmware 4.0.2 supports the new Tera2 processor family to deliver enhanced display capabilities, imaging performance, memory, power management, and other important functions. For example, the TERA2140 zero client can support up to four displays (DVI-D or DisplayPort) and can perform image encoding at speeds of up to 300 million pixels per second (Mpps) for remote workstations and 50 Mpps for virtual desktops. For complete product details on second-generation PCoIP zero clients and host cards containing these new Tera2 processors, see the Teradici website at http://www.teradici.com. For a list of all the host cards and zero clients supported in this firmware release, see PCoIP Host Cards and Zero Clients.

- **Processor family information**: You can now display information about the processor family and chipset in your device a number of ways. For details, see Displaying Processor Information.

- **Display topology configuration enhancements**: To support the new Tera2 display capabilities, the Display Topology Configuration page on the Management Console (MC) and the Display Topology settings on the On Screen Display (OSD) now let you configure layout, alignment, and resolution properties for dual-display and quad-display topologies.

- **Preferred resolution override enhancements**: In this release, an expanded list of default resolutions is included when you configure a zero client to advertise default Extended Display Identification Data (EDID) information to the graphics processing unit (GPU) in a host workstation. For Tera2 clients, you can now configure preferred (default) resolutions for up to four displays. For details, see OSD Tera2: Display Settings.

- **Expanded list of test display resolutions**: The **Display** page on the Administrator Web Interface (AWI) now contains an expanded list of display resolutions for viewing a test pattern on a zero client. For details about how to configure a test pattern, see AWI Client: Display Settings.

- **New Tera2 disconnect options**: When a user is in a session with a remote workstation, pressing the connect/disconnect button on a Tera2 zero client pops up a new dialog that lets the user select whether to disconnect from the session or to power off the remote workstation. Users can also use a Ctrl+Alt+F12 hotkey sequence to display this pop-up dialog. For details about this new feature, see Disconnecting from a Session.

- **Enhanced OSD messaging**: Messaging on the OSD has been enhanced with new overlay windows and also new in-line messages that appear on the OSD's **Connect** page. For example, if a user does not enter the correct user name or password, or if the Caps Lock key is on, a message displays above the **Connect** button on this page to alert the user. Network connection lost/down/up messages also display in this location, replacing the network icons that used to appear in the lower right-hand corner. For details, see Connecting to a Session and Overlay Windows.

- **Management Console cached VCS address enhancement**: You can now configure up to 25 cached View Connection Server addresses from the Management Console's **Session Configuration – View Connection Server** page. These servers are displayed in a drop-down list on the OSD **Connect** page when users use a VMware View Connection Server to connect to a virtual desktop. For details, see MC: View Connection Server Session Settings.

- **Imprivata OneSign configuration enhancements**: New parameters on the **View Connection Server – Imprivata OneSign** page allow you to configure a OneSign server desktop name. When the desktop pool list includes a pool with this name, the zero client will start a session with this desktop. You can configure a profile with this option from the MC: View Connection Server + Imprivata OneSign page, or you can configure a specific zero client from the AWI Client: view Connection Server + Imprivata Onesign page or OSD: View Connection Server + Imprivata Onesign page.

- **Online help for administrators**: PCoIP zero client and host card administrator documentation is now delivered as online help in this release, with a full GUI Reference that includes how to configure device firmware using three PCoIP administrator tools—the MC, the AWI, and the OSD. It also contains topics for common PCoIP device deployment scenarios, providing illustrations, descriptions, and links to configuration details for each one.

# 3 PCoIP Management Tools

## 3.1 About the MC

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

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

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

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

The following browsers have been tested with this release:

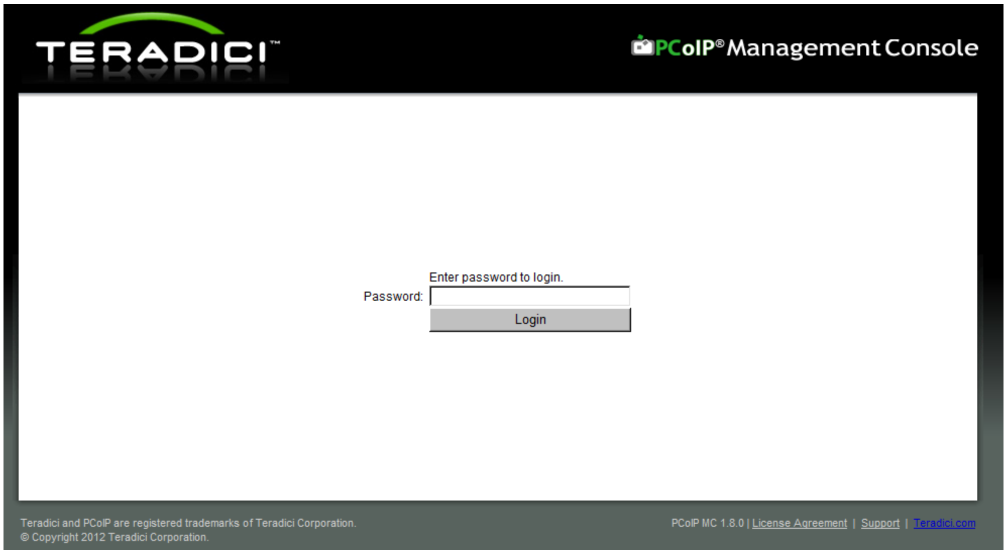
- Firefox version 3 or later
- Internet Explorer 7.0 and 8.0

If you try to log into the MC web interface using a different browser, an error message appears that lists the supported browsers.

## 3.2 Logging into the MC

To log into the Management Console web interface:

1. From an Internet browser, enter the IP address of the MC web page. The IP address may be a static or dynamic address, depending on how it is determined when the MC is configured:
   - **Static IP Address:** The IP address is hard-coded and must be known.
   - **Dynamic IP Address:** The IP address is dynamically assigned by the Dynamic Host Configuration Protocol (DHCP) server. You can get it from the DHCP server.
2. From the login page, enter the administrative password. The default value is blank (i.e., "").



TERADICI™
PCoIP® Management Console
Password:
Login
PCoIP MC 1.8.0 | License Agreement | Support | Teradici.com

Enter password to login.

Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2012 Teradici Corporation.

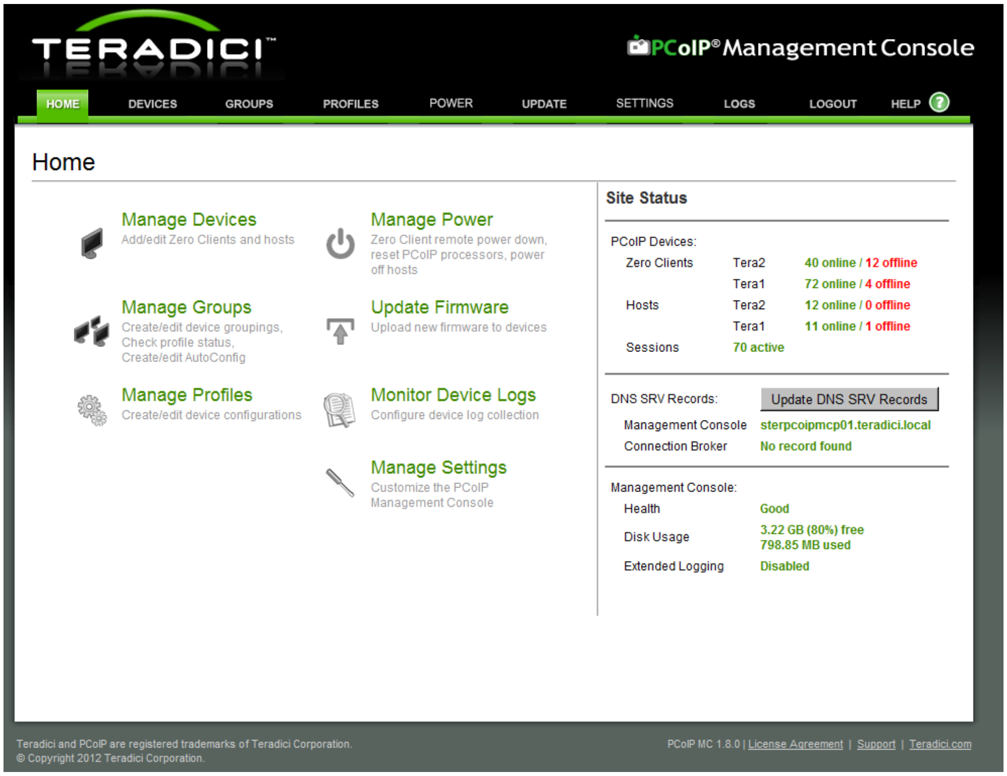
**Figure 3-1: MC Login Page**

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

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

## 3.3 MC Home Page

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


TERADICI
PCoIP® Management Console
HOME
DEVICES
GROUPS
PROFILES
POWER
UPDATE
SETTINGS
LOGS
LOGOUT
HELP
Home
Manage Devices
Add/edit Zero Clients and hosts
Manage Power
Zero Client remote power down, reset PCoIP processors, power off hosts
Manage Groups
Create/edit device groupings, Check profile status, Create/edit AutoConfig
Update Firmware
Upload new firmware to devices
Manage Profiles
Create/edit device configurations
Monitor Device Logs
Configure device log collection
Manage Settings
Customize the PCoIP Management Console
Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2012 Teradici Corporation.
PCoIP MC 1.8.0 | License Agreement | Support | Teradici.com

Site Status

| | | |
|---|---|---|
| PCoIP Devices: | | |
| Zero Clients | Tera2 | 40 online / 12 offline |
| | Tera1 | 72 online / 4 offline |
| Hosts | Tera2 | 12 online / 0 offline |
| | Tera1 | 11 online / 1 offline |
| Sessions | 70 active | |

DNS SRV Records: Update DNS SRV Records

| | |
|---|---|
| Management Console | sterpcoipmcp01.teradici.local |
| Connection Broker | No record found |

Management Console:

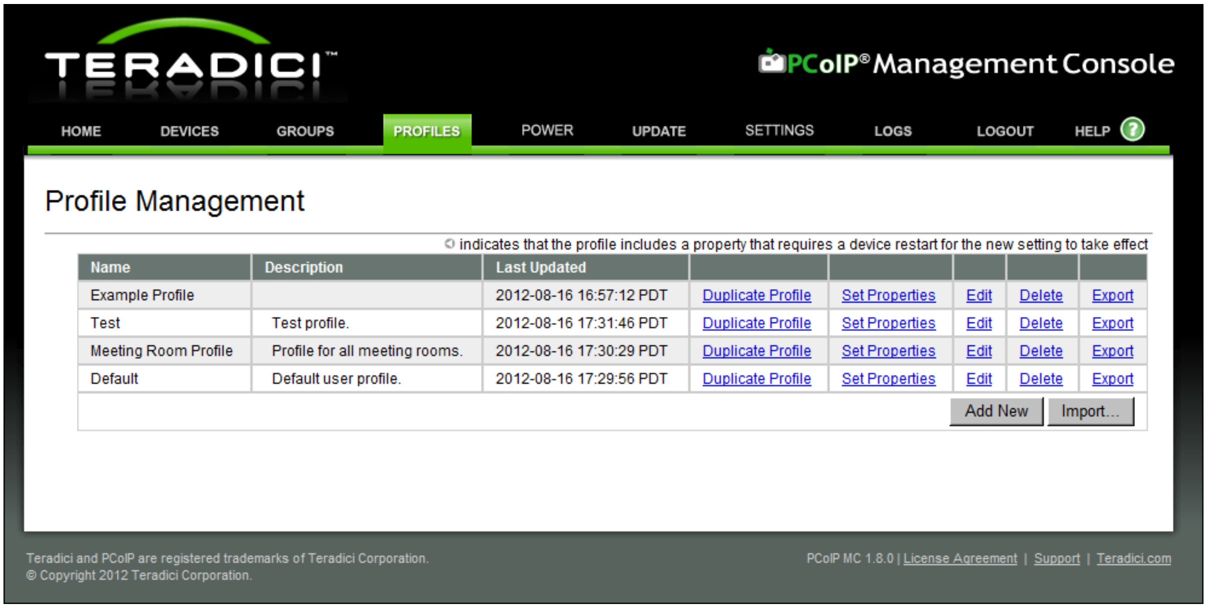
| | |
|---|---|
| Health | Good |
| Disk Usage | 3.22 GB (80%) free<br>798.85 MB used |
| Extended Logging | Disabled |

**Figure 3-2: MC Home Page**

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

## 3.4 MC Profile Management Page

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



Profile Management

indicates that the profile includes a property that requires a device restart for the new setting to take effect

| Name | Description | Last Updated | | | | | |
|---|---|---|---|---|---|---|---|
| Example Profile | | 2012-08-16 16:57:12 PDT | Duplicate Profile | Set Properties | Edit | Delete | Export |
| Test | Test profile. | 2012-08-16 17:31:46 PDT | Duplicate Profile | Set Properties | Edit | Delete | Export |
| Meeting Room Profile | Profile for all meeting rooms. | 2012-08-16 17:30:29 PDT | Duplicate Profile | Set Properties | Edit | Delete | Export |
| Default | Default user profile. | 2012-08-16 17:29:56 PDT | Duplicate Profile | Set Properties | Edit | Delete | Export |

Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2012 Teradici Corporation.

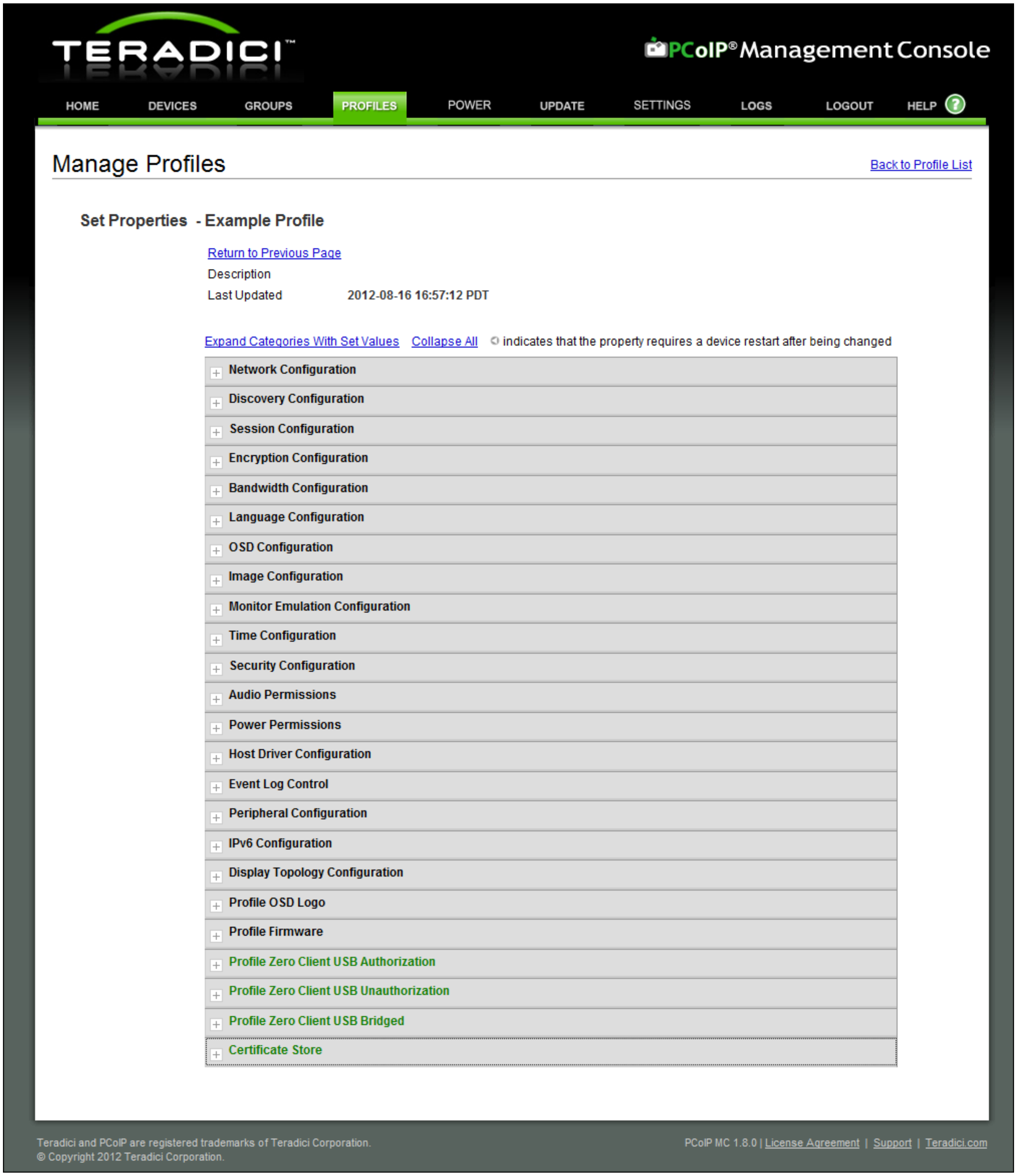
PCoIP MC 1.8.0 | License Agreement | Support | Teradici.com

**Figure 3-3: MC Profile Management Page**

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

## 3.5 MC Manage Profiles Page

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



Manage Profiles

Back to Profile List

Set Properties - Example Profile

Return to Previous Page

Description

Last Updated 2012-08-16 16:57:12 PDT

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

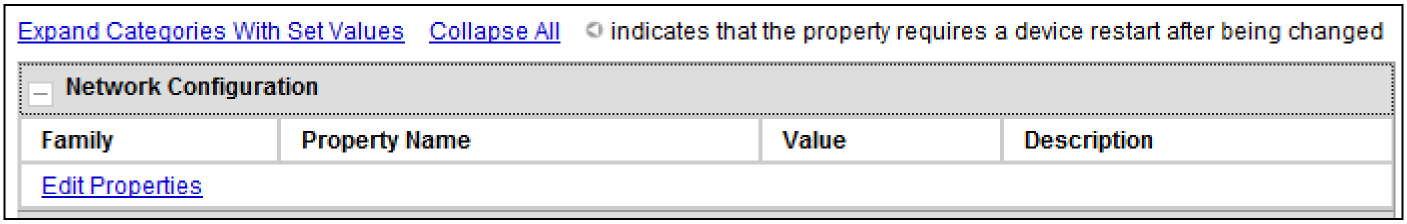
- Network Configuration
- Discovery Configuration
- Session Configuration
- Encryption Configuration
- Bandwidth Configuration
- Language Configuration
- OSD Configuration
- Image Configuration
- Monitor Emulation Configuration
- Time Configuration
- Security Configuration
- Audio Permissions
- Power Permissions
- Host Driver Configuration
- Event Log Control
- Peripheral Configuration
- IPv6 Configuration
- Display Topology Configuration
- Profile OSD Logo
- Profile Firmware
- Profile Zero Client USB Authorization
- Profile Zero Client USB Unauthorization
- Profile Zero Client USB Bridged
- Certificate Store

Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2012 Teradici Corporation.

PCoIP MC 1.8.0 | License Agreement | Support | Teradici.com

**Figure 3-4: MC Manage Profiles Page**

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



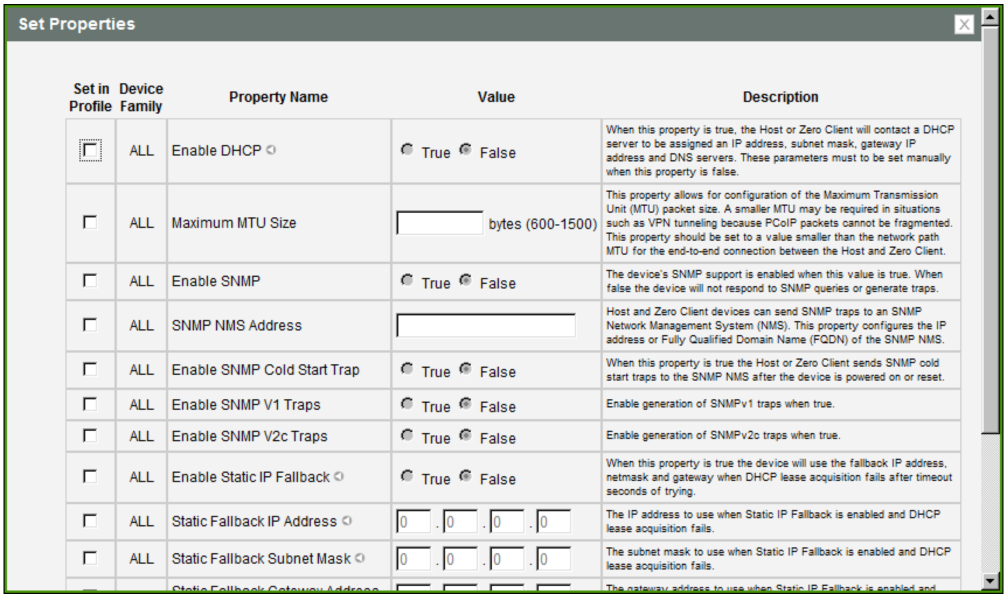
Expand Categories With Set Values   Collapse All   ↺ indicates that the property requires a device restart after being changed

**Network Configuration**

| Family | Property Name | Value | Description |
|---|---|---|---|
| Edit Properties | | | |

Figure 3-5: Edit Properties Link

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



Set Properties

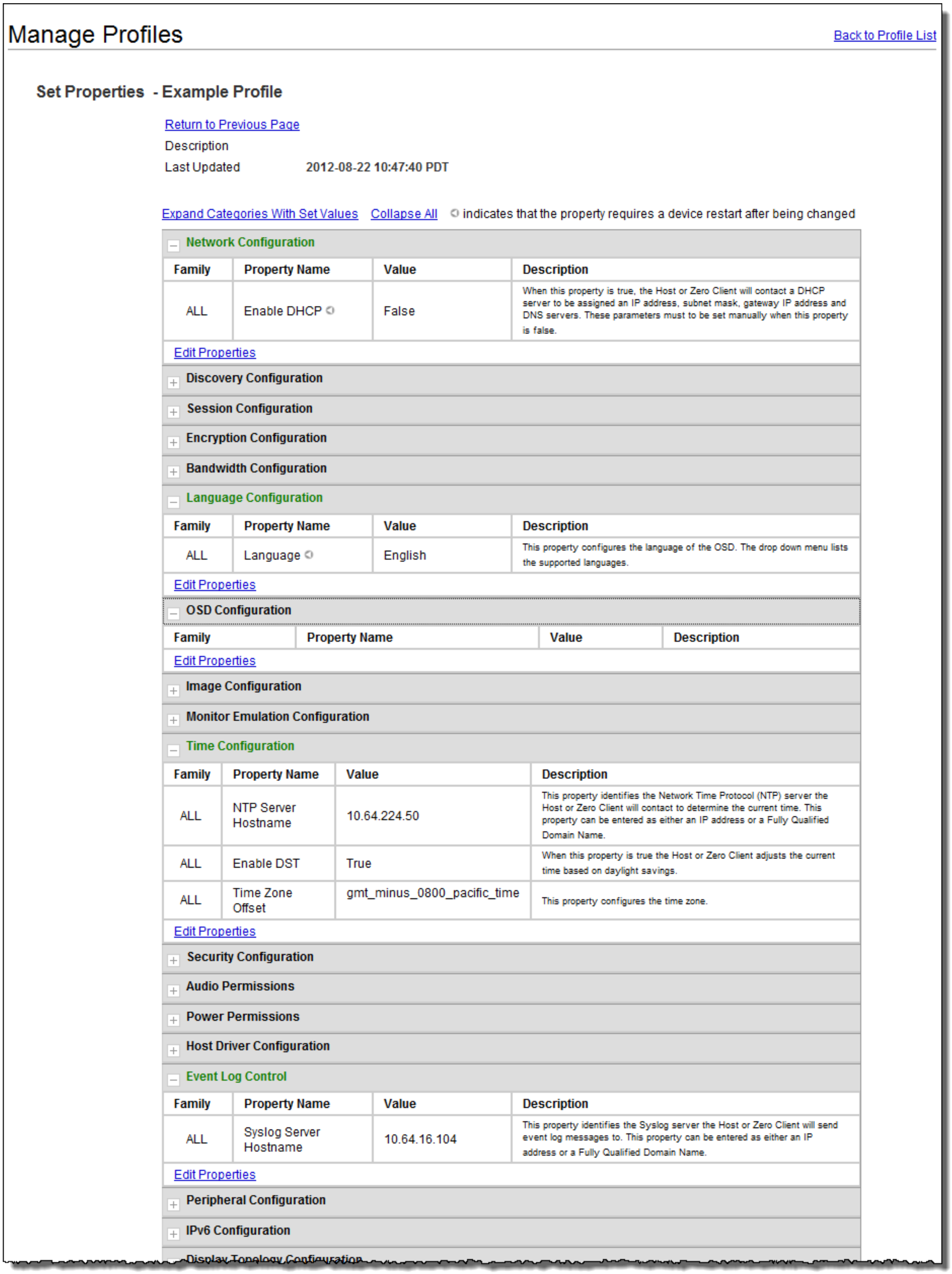
| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable DHCP ↺ | ○ True ● False | When this property is true, the Host or Zero Client will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address and DNS servers. These parameters must to be set manually when this property is false. |
| □ | ALL | Maximum MTU Size | bytes (600-1500) | This property allows for configuration of the Maximum Transmission Unit (MTU) packet size. A smaller MTU may be required in situations such as VPN tunneling because PCoIP packets cannot be fragmented. This property should be set to a value smaller than the network path MTU for the end-to-end connection between the Host and Zero Client. |
| □ | ALL | Enable SNMP | ○ True ● False | The device's SNMP support is enabled when this value is true. When false the device will not respond to SNMP queries or generate traps. |
| □ | ALL | SNMP NMS Address | | Host and Zero Client devices can send SNMP traps to an SNMP Network Management System (NMS). This property configures the IP address or Fully Qualified Domain Name (FQDN) of the SNMP NMS. |
| □ | ALL | Enable SNMP Cold Start Trap | ○ True ● False | When this property is true the Host or Zero Client sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset. |
| □ | ALL | Enable SNMP V1 Traps | ○ True ● False | Enable generation of SNMPv1 traps when true. |
| □ | ALL | Enable SNMP V2c Traps | ○ True ● False | Enable generation of SNMPv2c traps when true. |
| □ | ALL | Enable Static IP Fallback ↺ | ○ True ● False | When this property is true the device will use the fallback IP address, netmask and gateway when DHCP lease acquisition fails after timeout seconds of trying. |
| □ | ALL | Static Fallback IP Address ↺ | 0 . 0 . 0 . 0 | The IP address to use when Static IP Fallback is enabled and DHCP lease acquisition fails. |
| □ | ALL | Static Fallback Subnet Mask ↺ | 0 . 0 . 0 . 0 | The subnet mask to use when Static IP Fallback is enabled and DHCP lease acquisition fails. |
| | | Static Fallback Gateway Address | | The gateway address to use when Static IP Fallback is enabled and |

Figure 3-6: Set Properties Page for Network Configuration

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

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

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



Manage Profiles

Back to Profile List

Set Properties - Example Profile

Return to Previous Page

| | |
|---|---|
| Description | |
| Last Updated | 2012-08-22 10:47:40 PDT |

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

⊟ Network Configuration

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

Edit Properties

⊞ Discovery Configuration

⊞ Session Configuration

⊞ Encryption Configuration

⊞ Bandwidth Configuration

⊟ Language Configuration

| Family | Property Name | Value | Description |
|---|---|---|---|
| ALL | Language ↻ | English | This property configures the language of the OSD. The drop down menu lists the supported languages. |

Edit Properties

⊟ OSD Configuration

| Family | Property Name | Value | Description |
|---|---|---|---|

Edit Properties

⊞ Image Configuration

⊞ Monitor Emulation Configuration

⊟ Time Configuration

| Family | Property Name | Value | Description |
|---|---|---|---|
| ALL | NTP Server Hostname | 10.64.224.50 | This property identifies the Network Time Protocol (NTP) server the Host or Zero Client will contact to determine the current time. This property can be entered as either an IP address or a Fully Qualified Domain Name. |
| ALL | Enable DST | True | When this property is true the Host or Zero Client adjusts the current time based on daylight savings. |
| ALL | Time Zone Offset | gmt_minus_0800_pacific_time | This property configures the time zone. |

Edit Properties

⊞ Security Configuration

⊞ Audio Permissions

⊞ Power Permissions

⊞ Host Driver Configuration

⊟ Event Log Control

| Family | Property Name | Value | Description |
|---|---|---|---|
| ALL | Syslog Server Hostname | 10.64.16.104 | This property identifies the Syslog server the Host or Zero Client will send event log messages to. This property can be entered as either an IP address or a Fully Qualified Domain Name. |

Edit Properties

⊞ Peripheral Configuration

⊞ IPv6 Configuration

⊞ Display Topology Configuration

**Figure 3-7: MC Manage Profiles Page – Configured**

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

For details on how to apply a profile, please refer to the "PCoIP Management Console User Manual" (TER0812002).

## 3.6 About the AWI

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

After you type the device's IP address into an Internet Explorer or Mozilla Firefox browser, the browser will use HTTPS (HTTP over an SSL socket) to connect to the device's AWI web page. Access to the AWI is controlled using an administrative password, which can be optionally disabled.

The AWI's HTTPS connection is secured using a PCoIP root Certificate Authority (CA) certificate. To avoid warning messages when you log into the AWI, it is recommended that you install this certificate in your browser. The certificate file ("cacert.pem") is always included in a firmware release, but you can also download it directly from the Teradici support site. For detailed instructions on how to install the certificate, see Knowledge Base support topic 15134-529 on the Teradici support site.

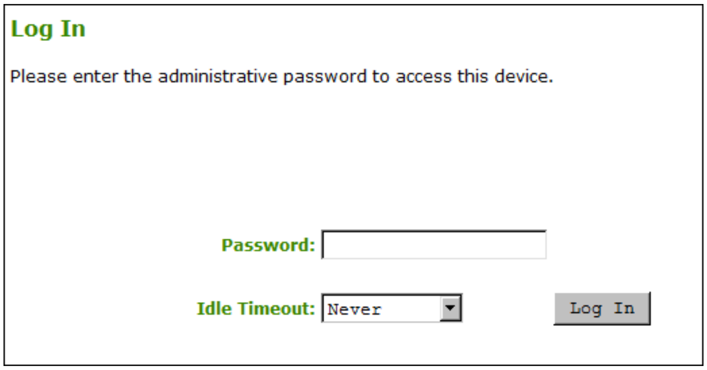
The following browsers have been tested with this release:

- Firefox version 3 or later
- Internet Explorer 7.0 and 8.0

## 3.7 Logging into the AWI

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

1. From an Internet browser, enter the IP address of the host or client. The IP address may be a static or dynamic address, depending on how the IP addresses are determined within your IP network:
   - **Static IP Address:** The IP address is hard-coded and must be known.
   - **Dynamic IP Address:** The IP address is dynamically assigned by the Dynamic Host Configuration Protocol (DHCP) server. You can get it from the DHCP server.
2. From the **Log In** page, enter the administrative password. The default value is blank (i.e., "").



Log In

Please enter the administrative password to access this device.

Password:

Idle Timeout: Never

**Figure 3-8: AWI Log In Page**

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

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

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

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

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

## 3.8 AWI Initial Setup Page

The AWI's **Initial Setup** page contains the audio, network, and session configuration parameters that you must set before a client or host device can be used. This page helps to simplify initial setup and reduce the time for new users to establish a session between a PCoIP zero client and PCoIP host card in a remote workstation.

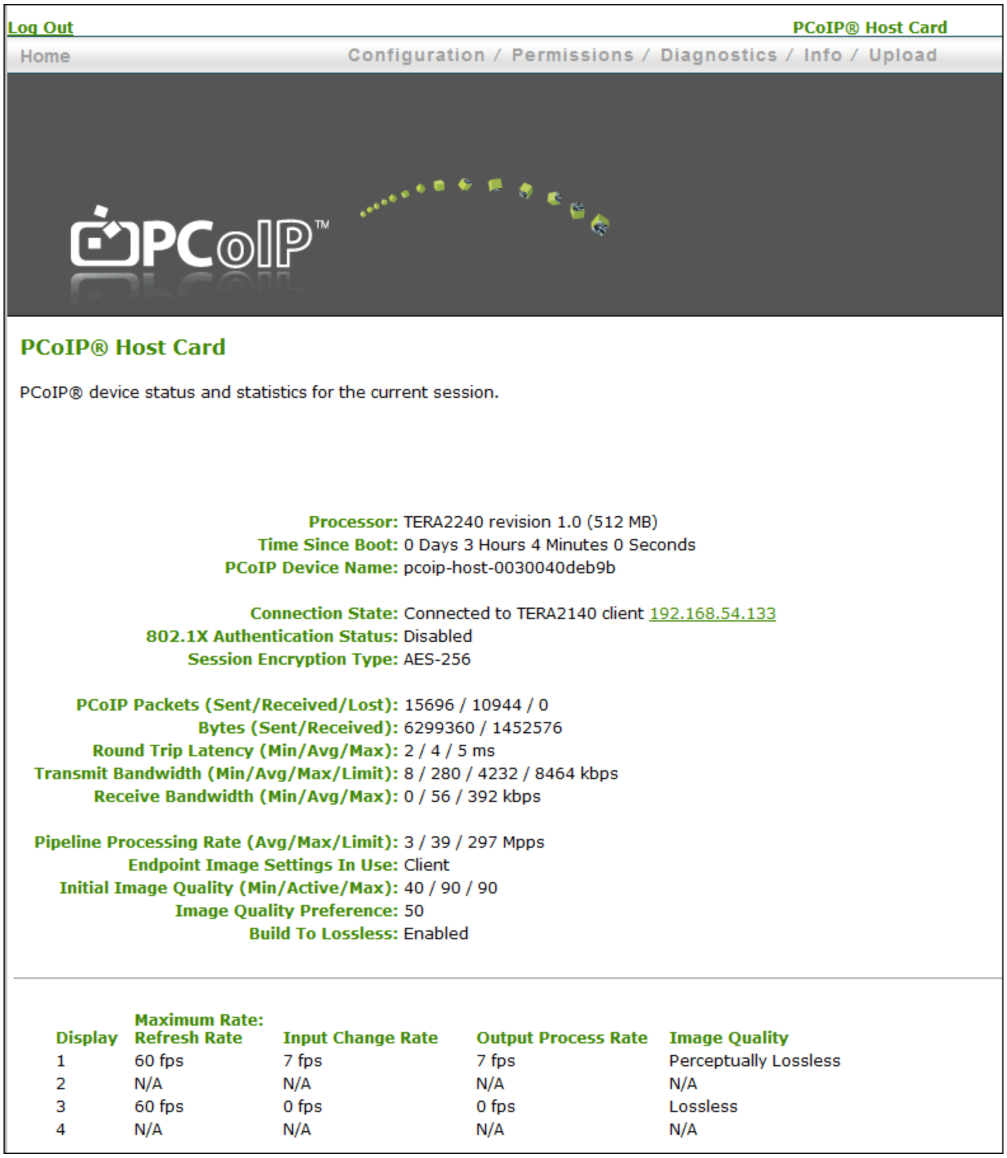
The AWI client **Initial Setup** and host **Initial Setup** pages are not identical. Each one provides parameters that apply to the client and host, respectively.

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

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

## 3.9 AWI Home Page

The AWI **Home** page displays a statistics summary for the host or client. You can display the **Home** page at any time by clicking the **Home** link at the top left section of the menu bar.



PCoIP® Host Card

PCoIP® device status and statistics for the current session.

**Processor:** TERA2240 revision 1.0 (512 MB)
**Time Since Boot:** 0 Days 3 Hours 4 Minutes 0 Seconds
**PCoIP Device Name:** pcoip-host-0030040deb9b

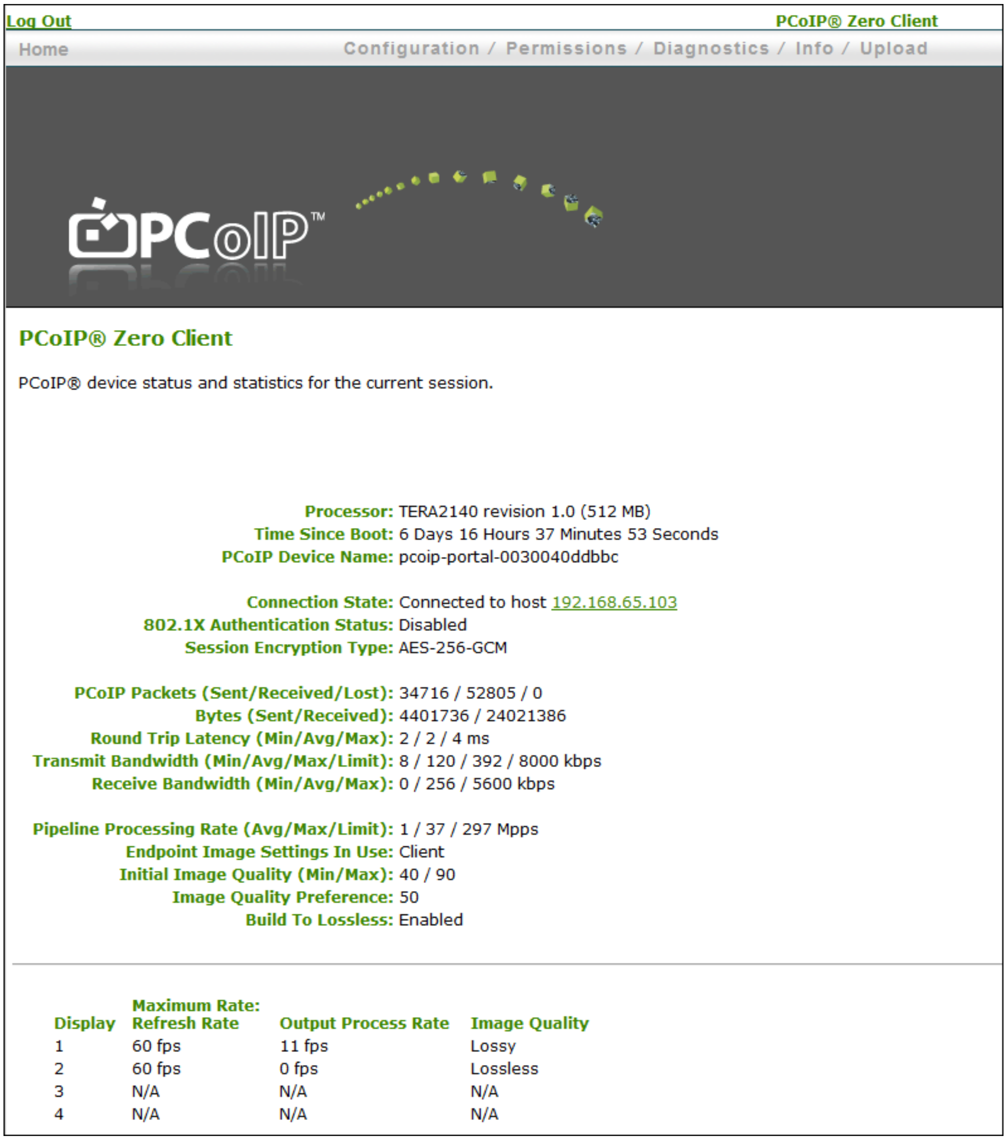
**Connection State:** Connected to TERA2140 client 192.168.54.133
**802.1X Authentication Status:** Disabled
**Session Encryption Type:** AES-256

**PCoIP Packets (Sent/Received/Lost):** 15696 / 10944 / 0
**Bytes (Sent/Received):** 6299360 / 1452576
**Round Trip Latency (Min/Avg/Max):** 2 / 4 / 5 ms
**Transmit Bandwidth (Min/Avg/Max/Limit):** 8 / 280 / 4232 / 8464 kbps
**Receive Bandwidth (Min/Avg/Max):** 0 / 56 / 392 kbps

**Pipeline Processing Rate (Avg/Max/Limit):** 3 / 39 / 297 Mpps
**Endpoint Image Settings In Use:** Client
**Initial Image Quality (Min/Active/Max):** 40 / 90 / 90
**Image Quality Preference:** 50
**Build To Lossless:** Enabled

| Display | Maximum Rate:<br>Refresh Rate | Input Change Rate | Output Process Rate | Image Quality |
|---|---|---|---|---|
| 1 | 60 fps | 7 fps | 7 fps | Perceptually Lossless |
| 2 | N/A | N/A | N/A | N/A |
| 3 | 60 fps | 0 fps | 0 fps | Lossless |
| 4 | N/A | N/A | N/A | N/A |

**Figure 3-9: AWI Host: Home Page**



PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

```
                        Processor: TERA2140 revision 1.0 (512 MB)
                  Time Since Boot: 6 Days 16 Hours 37 Minutes 53 Seconds
                PCoIP Device Name: pcoip-portal-0030040ddbbc

                 Connection State: Connected to host 192.168.65.103
      802.1X Authentication Status: Disabled
          Session Encryption Type: AES-256-GCM

  PCoIP Packets (Sent/Received/Lost): 34716 / 52805 / 0
             Bytes (Sent/Received): 4401736 / 24021386
       Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 120 / 392 / 8000 kbps
       Receive Bandwidth (Min/Avg/Max): 0 / 256 / 5600 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 37 / 297 Mpps
       Endpoint Image Settings In Use: Client
       Initial Image Quality (Min/Max): 40 / 90
            Image Quality Preference: 50
                   Build To Lossless: Enabled
```

| Display | Maximum Rate: Refresh Rate | Output Process Rate | Image Quality |
|---|---|---|---|
| 1 | 60 fps | 11 fps | Lossy |
| 2 | 60 fps | 0 fps | Lossless |
| 3 | N/A | N/A | N/A |
| 4 | N/A | N/A | N/A |

Figure 3-10: AWI Client: Home Page

Note: The above figures show session statistics for devices that can support four connected displays. If your deployment only supports two displays, information for these two displays will appear in the bottom area of the page.

Table 3-1: AWI Home Page Statistics

| Statistics | Description |
|---|---|
| Processor | PCoIP processor type, version, and RAM size |
| Time Since Boot | Length of time that the PCoIP processor has been running. |
| PCoIP Device Name | The logical name for the device. |

| Statistics | Description |
|---|---|
| | This field is the name the host or client registers with the DNS server if DHCP is enabled or the system is configured to support registering the hostname with the DNS server. (See the PCoIP Device Name parameter on the **Label** page.) |
| Connection State | The current (or last) state of the PCoIP session. Values include the following:<br>• **Asleep**<br>• **Canceling**<br>• **Connected**<br>• **Connection Pending**<br>• **Disconnected**<br>• **Waking** |
| 802.1X Authentication Status | Indicates whether 802.1X authentication is enabled or disabled on the device. |
| Session Encryption Type | The type of encryption in use when a session is active:<br>• AES-128-GCM<br>• SALSA20-256-Round 12 |
| PCoIP Packets Statistics | **PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session.<br>**PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session.<br>**PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session. |
| Bytes | **Bytes Sent:** The total number of bytes sent in the current/last session.<br>**Bytes Received:** The total number of bytes received in the current/last session. |
| Round Trip Latency | The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms). |
| Bandwidth Statistics | **Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels.<br>**Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor. |
| Pipeline Processing Rate | How much image data is currently being processed by the image engine (in megapixels per second). |
| Endpoint Image Settings In Use | Displays if the image settings being used are configured within the client or within the host. This is based on how the **Use Client Image Settings** field is configured on the **Image** page for the host device. |

| Statistics | Description |
|---|---|
| Image Quality | The minimum and maximum quality setting is taken from the **Image** page for the device.<br>The active setting is what’s currently being used in the session and only appears on the host. |
| Image Quality Preference | This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image. |
| Build to Lossless | Options that may appear in this field include the following:<br>**Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked.<br>**Disabled:** The **Disable Build to Lossless** field is checked. |
| Display | The port number for the display. |
| Maximum Rate | This column shows the refresh rate of the attached display.<br>If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate.<br>If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined." |
| Input Change Rate | The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video).<br>Note: This option is only available on the host. It does not appear on the client. |
| Output Process Rate | The frame rate currently being sent from the image engine on the host to the client. |
| Image Quality | Shows the current lossless state of the attached display:<br>• **Lossy**<br>• **Perceptually lossless**<br>• **Lossless** |

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

## 3.10 AWI Menus

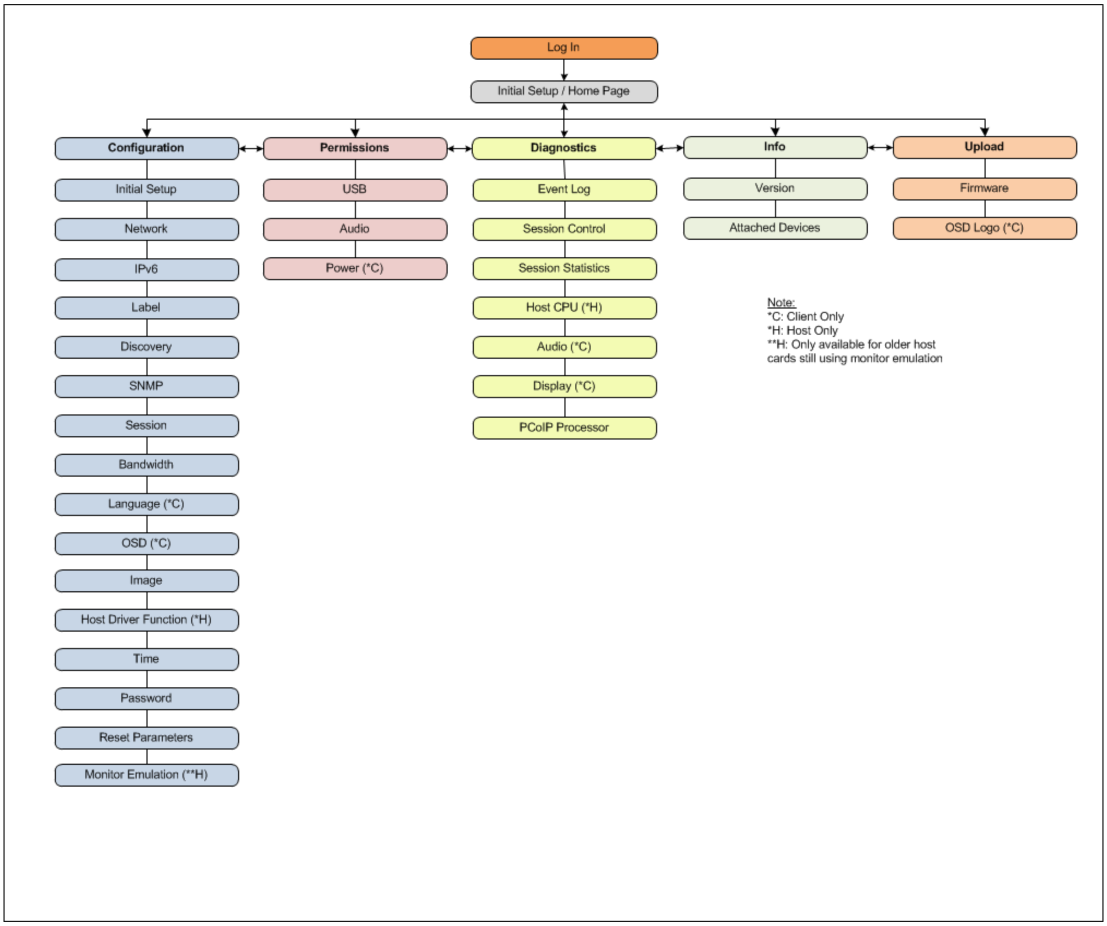
The AWI has five main menus that link to the various configuration and status pages.

- **Configuration:** The pages under this menu let you configure the various aspects for the device, such as network settings, language, session parameters, etc.
- **Permissions:** The pages under this menu let you set up the permissions for the USB, audio, and power on the client, and for the USB and audio on the host.
- **Diagnostics:** The pages under this menu help you troubleshoot the device.

- **Info:** The pages listed this menu let you view firmware information and the devices currently attached to the device.
- **Upload:** The pages under this menu let you upload a new firmware version, an OSD logo, and your certificates to the device.

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

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



Note:
*C: Client Only
*H: Host Only
**H: Only available for older host cards still using monitor emulation

**Figure 3-11: AWI Menu Overview**

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

## 3.11 About the OSD

The PCoIP On Screen Display (OSD), shown in the figure below, is a graphical user interface (GUI) embedded within the client. It displays when the client is powered on and a

PCoIP session is not in progress. The only exception to this is when the client is configured for a managed startup or auto-reconnect.

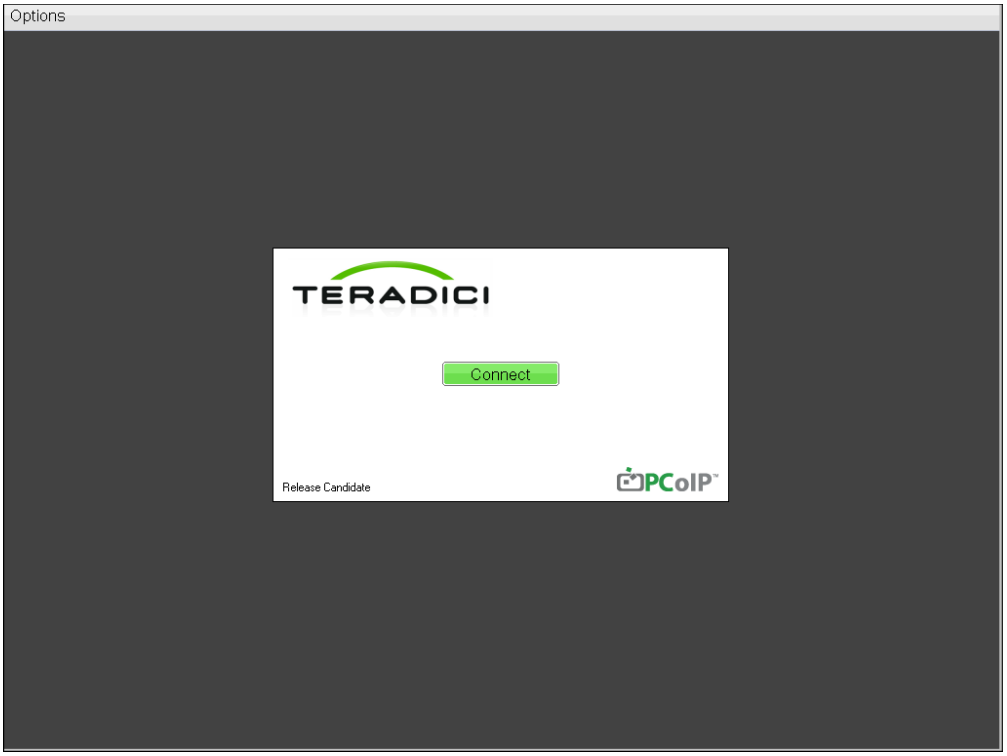


**Figure 3-12: OSD Main Window**

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 host card in a remote workstation.

## 3.12 Connecting to a Session

The OSD allows users to create a session between the client and a host card on a remote workstation (or between the client and a virtual desktop) by clicking the green **Connect** button in the center of the **Connect** window. Once the connection is established, the OSD local GUI disappears, and the session image appears.

The following figure shows the **Connect** window for a Direct to Host session type—i.e., when the client is connecting to a host card in a remote workstation.

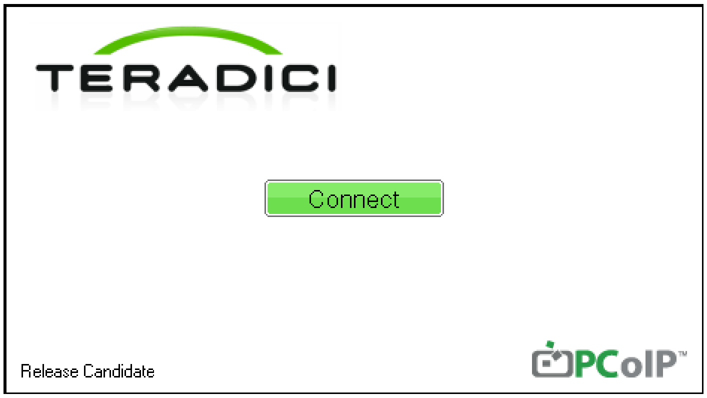


Figure 3-13: OSD Direct to Host Connect Window

While the network connection is initializing, various status messages are displayed above the button to indicate the progress, such as the message shown below.

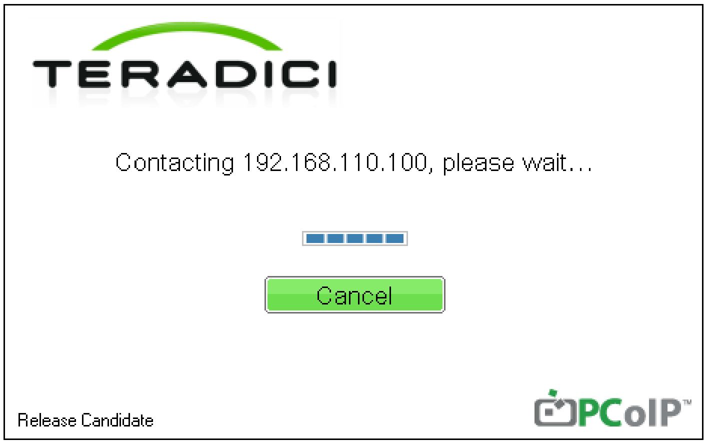
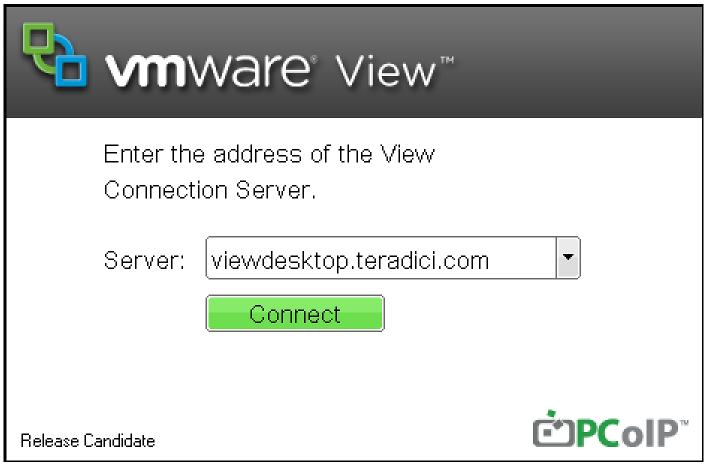

Contacting 192.168.110.100, please wait…

Figure 3-14: OSD Connection Status

If problems are experienced during startup—e.g., if the connection cannot be made or a DHCP lease fails—other messages display in this area to indicate the nature of the problem.

The following figure shows the **Connect** window for a View Connection Server connection—i.e., when the client is using a VMware View Connection Server to connect to a virtual desktop.



Enter the address of the View Connection Server.

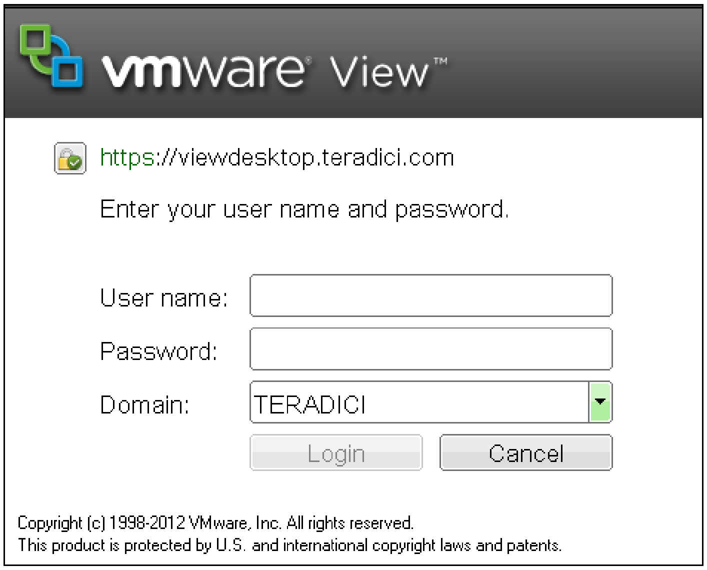
Server: viewdesktop.teradici.com

**Figure 3-15: OSD View Connection Server Connect Window**

Note: you can change the logo that appears above the **Connect** button by uploading a replacement image using the **Upload > OSD Logo** menu from a client's AWI.

While the connection is initializing, status messages may also display above the **Connect** button to inform users of the connection progress or to alert them to a problem.

After connecting to the View Connection Server, the virtual desktop login page appears to



https://viewdesktop.teradici.com

Enter your user name and password.

User name:

Password:

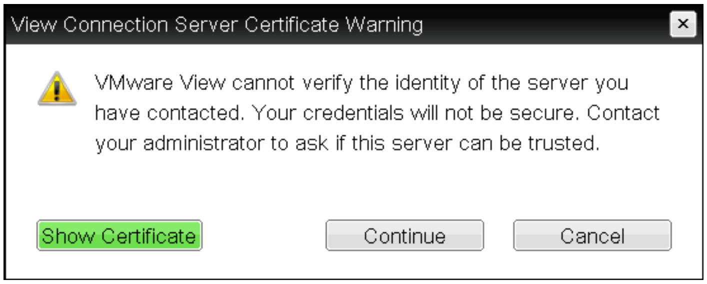
Domain: TERADICI

Copyright (c) 1998-2012 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright laws and patents.

**Figure 3-16: Virtual Desktop Login Page**

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.

If the correct trusted SSL root certificate for the VMware View Connection Server has not been installed in the client, the following warning appears.

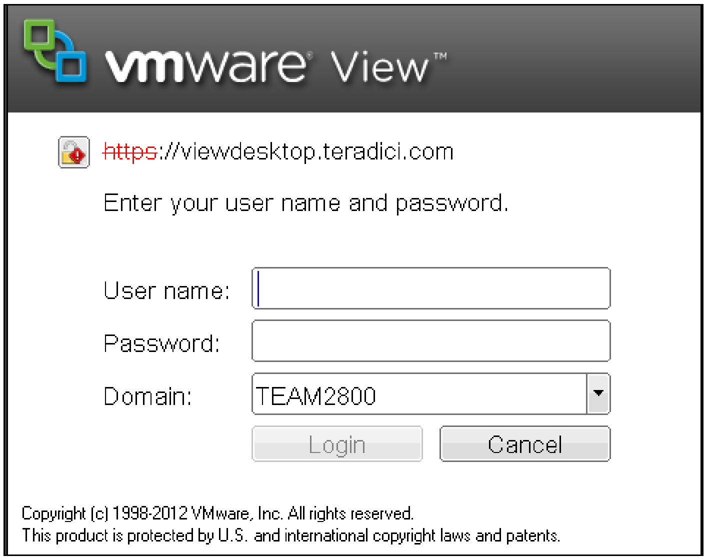


View Connection Server Certificate Warning

VMware View cannot verify the identity of the server you have contacted. Your credentials will not be secure. Contact your administrator to ask if this server can be trusted.

**Figure 3-17: OSD View Connection Server Certificate Warning**

If the user clicks **Continue** at this warning, the session will not be secure. This is indicated by the warning icon on the lock in the upper left of the window and also by the red "https" with strikethrough formatting, which tells users that the secure HTTPS protocol will not be used for the connection.



~~https~~://viewdesktop.teradici.com

Enter your user name and password.

User name:

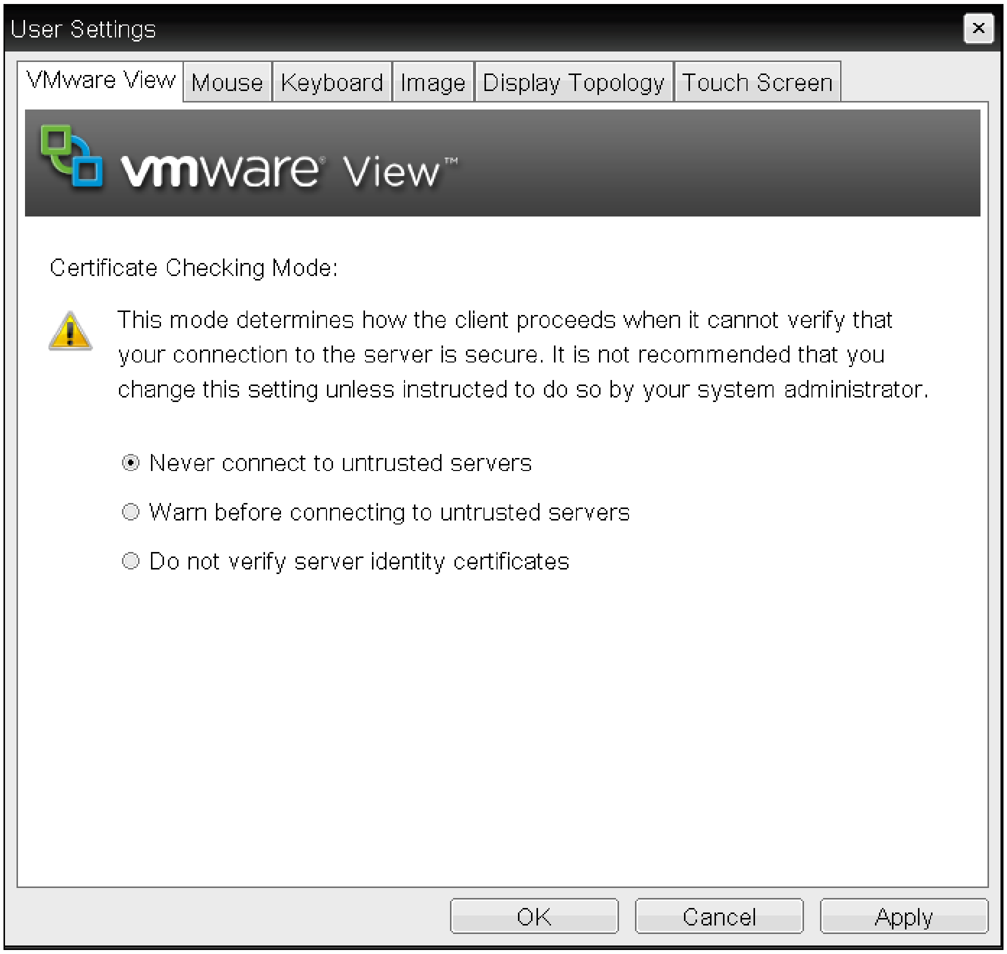
Password:

Domain: TEAM2800

Copyright (c) 1998-2012 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright laws and patents.

**Figure 3-18: OSD Login Screen with Insecure Warning**

As an administrator, you can use the Options > User Settings > VMware View page, shown below, to prevent users from initiating insecure sessions by configuring the zero client to refuse a connection to a server that cannot be verified.



Certificate Checking Mode:

This mode determines how the client proceeds when it cannot verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

● Never connect to untrusted servers

○ Warn before connecting to untrusted servers

○ Do not verify server identity certificates

**Figure 3-19: OSD VMware View Page**

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

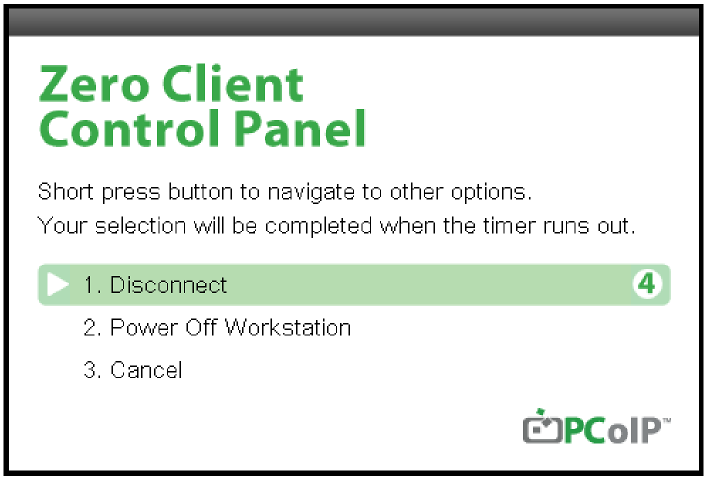
**See also**:

- For information about how to upload certificates to a profile using the MC, see MC: Certificate Store Management.
- For information on how to upload certificates to a single device using the AWI, see AWI: Certificate Upload Settings.
- For information on other OSD messages that may appear on top of a user's session during startup or after a session has been established, see Overlay Windows.

## 3.13 Disconnecting from a Session

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

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



Zero Client Control Panel

Short press button to navigate to other options.
Your selection will be completed when the timer runs out.

1. Disconnect 4
2. Power Off Workstation
3. Cancel

**Figure 3-20: Zero Client Control Panel**

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

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

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

- Enable Session Disconnect Hotkey must be enabled in the advanced options on the **Session – View Connection Server** page.
- The **Enable Local Cursor and Keyboard** feature must be enabled on the PCoIP host software on the host computer. For details, see "PCoIP Host Software User Guide (TER0810001)".
- On the client, the keyboard must be recognized as locally connected (i.e., not bridged).

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

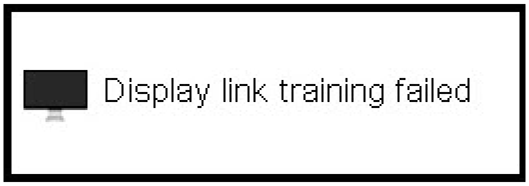
In order to allow users to use the second overlay option (i.e., to power off the workstation), the power permissions on the client must be configured to allow a "hard" power off. You can set this parameter from the MC **Power Permissions** page or from the AWI **Power Permissions** page.

## 3.14 Overlay Windows

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

### 3.14.1 Display Link Training Failed

This overlay only displays on Tera2 clients that contain DisplayPort display interfaces (as opposed to DVI interfaces). The DisplayPort protocol requires a link training sequence for adapting to differing cable lengths and signal qualities. If this training does not succeed, the following overlay appears with the message "Display link training failed."

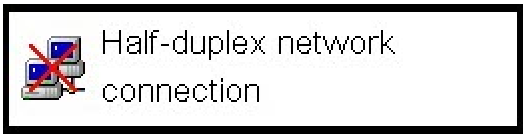


Display link training failed

**Figure 3-21: Display Link Training Failed Overlay**

### 3.14.2 Half Duplex Overlay

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

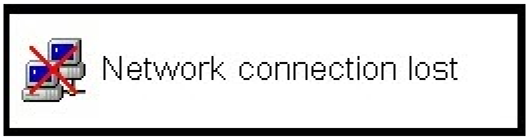


Half-duplex network
connection

**Figure 3-22: Half Duplex Overlay**

### 3.14.3 Network Connection Lost Overlay

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



Network connection lost

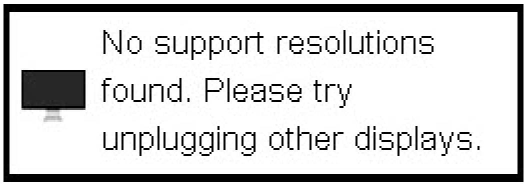
**Figure 3-23: Network Connection Lost Overlay**

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

Note: It is not recommended to use this notification message when using PCoIP devices with virtual desktops. Normal scheduling within the virtual desktop hypervisor can falsely trigger this message. To prevent this problem, you can disable the **Enable Peer Loss Overlay** setting.

### 3.14.4 No Support Resolutions Found

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

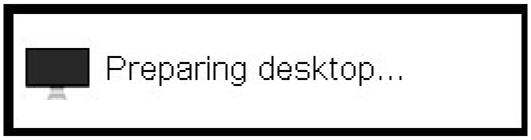


No support resolutions found. Please try unplugging other displays.

**Figure 3-24: No Support Resolutions Found Overlay**

### 3.14.5 Preparing Desktop Overlay

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

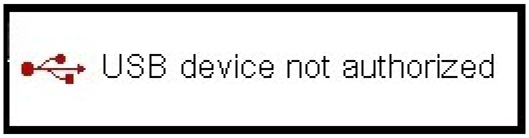


Preparing desktop...

**Figure 3-25: Preparing Desktop Overlay**

### 3.14.6 USB Device Not Authorized Overlay

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



USB device not authorized

**Figure 3-26: USB Device Not Authorized Overlay**

### 3.14.7 USB Over Current Notice Overlay

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

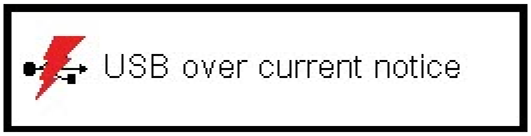

USB over current notice

Figure 3-27: USB Over Current Notice Overlay

### 3.14.8 USB Device Not Supported Behind a High-speed Hub Overlay

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

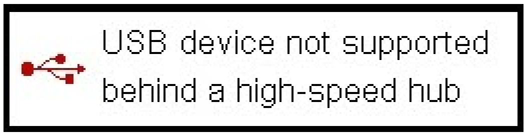

USB device not supported behind a high-speed hub

Figure 3-28: USB Device Not Supported Behind a High-speed Hub Overlay

### 3.14.9 Resolution Not Supported Overlay

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

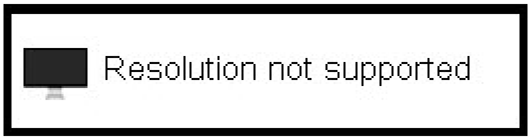

Resolution not supported

Figure 3-29: Resolution Not Supported Overlay

### 3.14.10Video Source Overlays

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

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

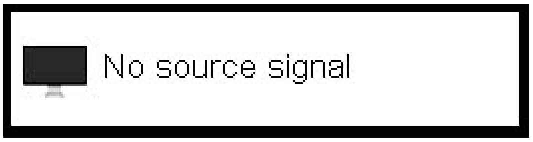

No source signal

Figure 3-30: No Source Signal Overlay

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

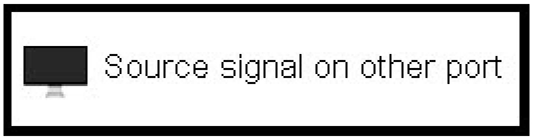

Source signal on other port

**Figure 3-31: Source Signal on Other Port Overlay**

## 3.15 OSD Menus

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

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

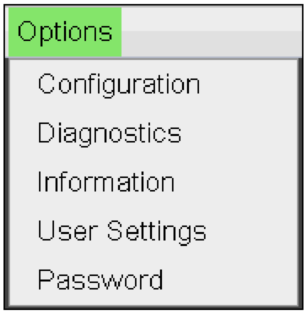


**Figure 3-32: OSD Options Menu**

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

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

# 4 PCoIP Deployment Scenarios

## 4.1 PCoIP Host Cards and Zero Clients

The following table lists the PCoIP host cards and zero clients you can deploy in your PCoIP network. It also lists the set of display resolutions each device supports.

Note: The processor name refers to the chipset used in the PCoIP device. For example, TERA2140 is the processor used in the second-generation TERA2140 zero client, and TERA2240 is the processor used in the second-generation TERA2240 PCIe host card (for tower PC or rack mount workstations) and TERA2240 PCI Mezzanine host card (for blade workstations). For full details about Teradici PCoIP processors, see the Teradici website at http://www.teradici.com.

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

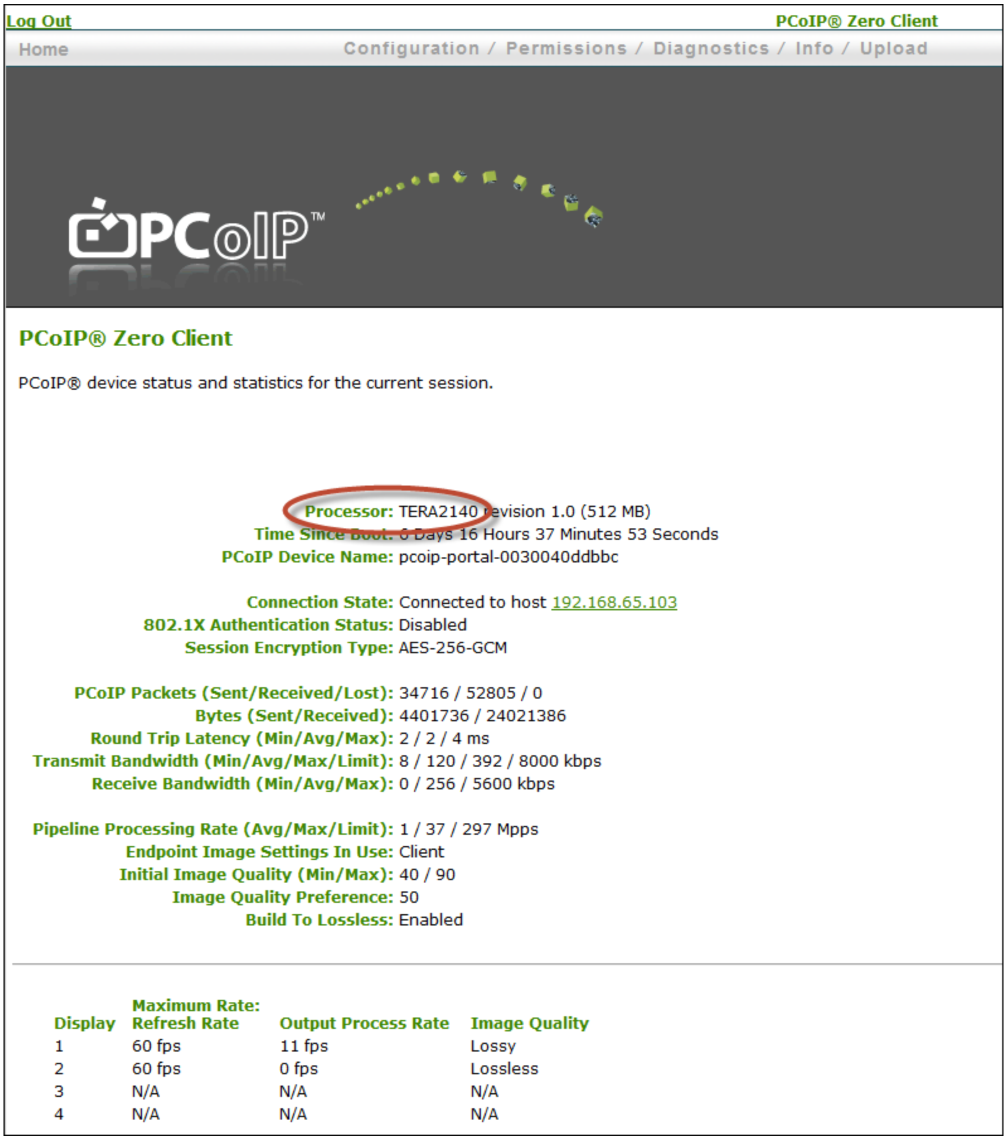
**Table 4-1: Supported Resolutions for PCoIP Host Cards and Zero Clients**

| Processor Name | Maximum No. of Supported Resolutions | Device Type | Processor Family |
|---|---|---|---|
| TERA1100 | 2 x 1920x1200 | zero client | Tera1 |
| TERA2321 | 2 x 1920x1200<br>1 x 2560x1600* | zero client | Tera2 |
| TERA2140 | 4 x 1920x1200<br>2 x 2560x1600* | zero client | Tera2 |
| TERA1202 | 2 x 1920x1200 | host card | Tera1 |
| TERA2220 | 2 x 1920x1200<br>1 x 2560x1600 | host card | Tera2 |
| TERA2240 | 4 x 1920x1200<br>2 x 2560x1600 | host card | Tera2 |

*Tera2 zero clients support 2560x1600 resolution on attached displays using either DVI or DisplayPort interfaces. For instructions on how to connect cables to Tera2 zero clients with DVI and/or DisplayPort ports to support this resolution, see DVI and DisplayPort Interfaces.

### 4.1.1 Displaying Processor Information

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



**PCoIP® Zero Client**

PCoIP® device status and statistics for the current session.

Processor: TERA2140 revision 1.0 (512 MB)
Time Since Boot: 0 Days 16 Hours 37 Minutes 53 Seconds
PCoIP Device Name: pcoip-portal-0030040ddbbc

Connection State: Connected to host 192.168.65.103
802.1X Authentication Status: Disabled
Session Encryption Type: AES-256-GCM

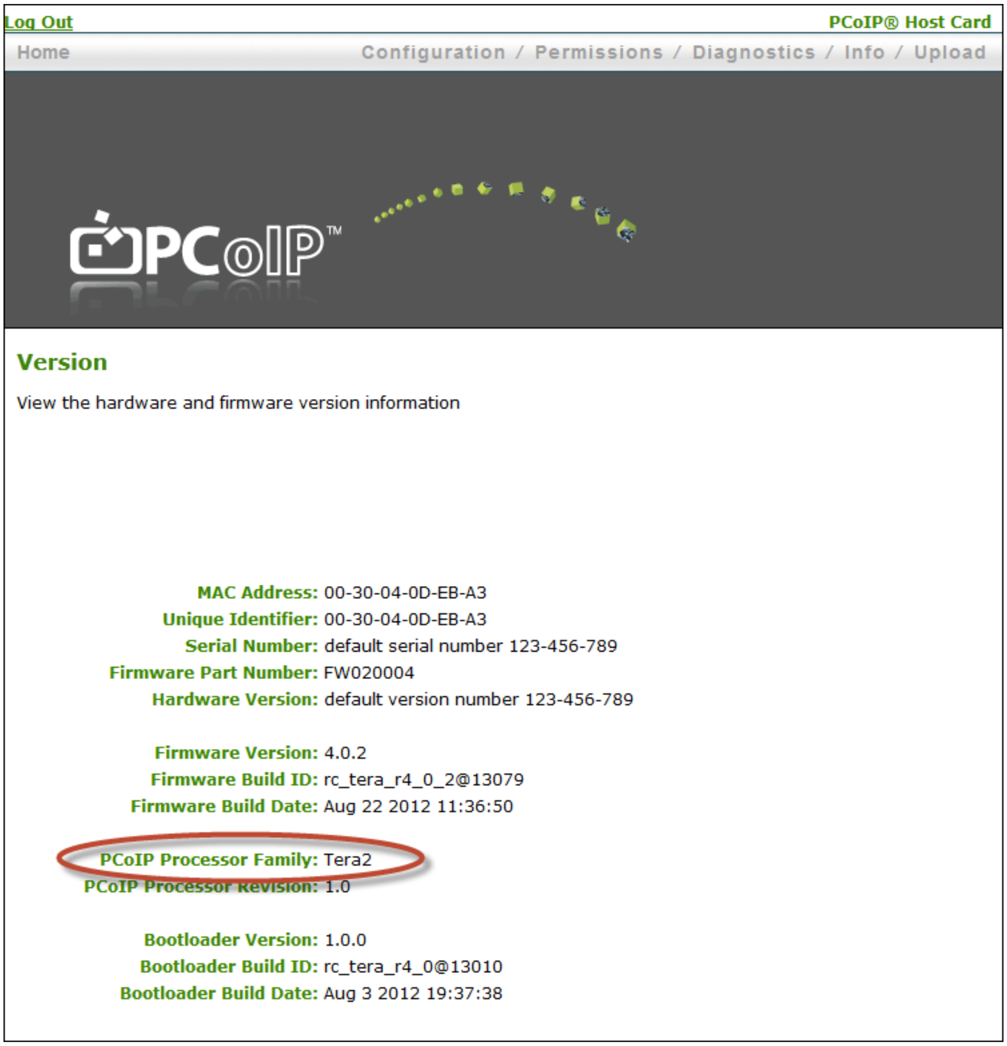
PCoIP Packets (Sent/Received/Lost): 34716 / 52805 / 0
Bytes (Sent/Received): 4401736 / 24021386
Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 120 / 392 / 8000 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 256 / 5600 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 37 / 297 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Max): 40 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

| Display | Maximum Rate:<br>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 |

**Figure 4-1: Processor Information on AWI Home Page**

The processor family name displays on the AWI Version page for a host or client.



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

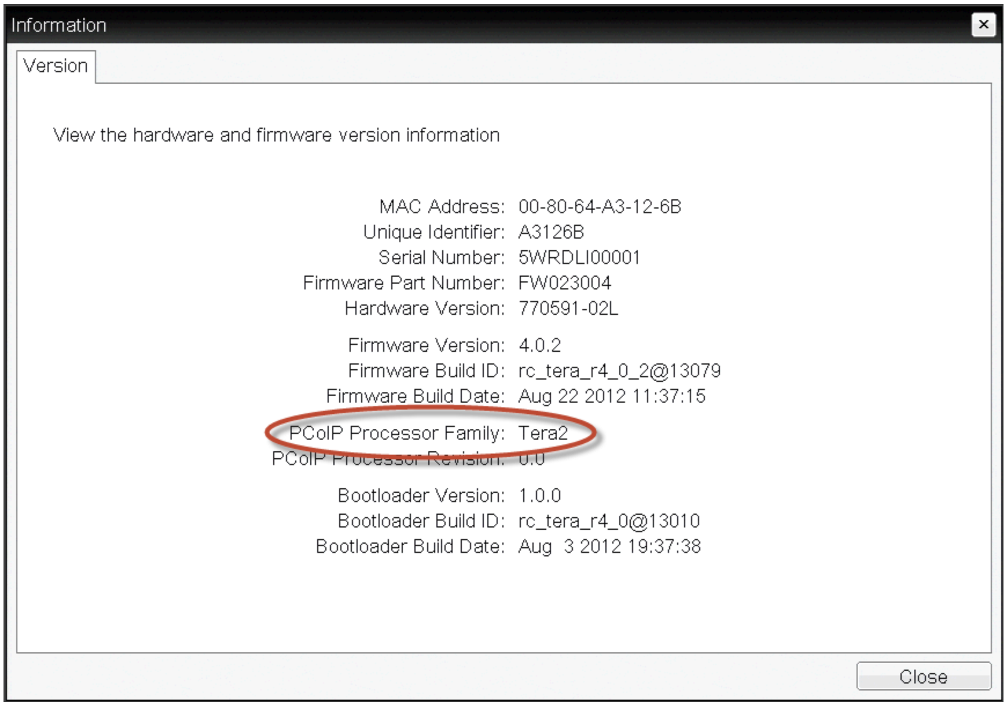
Firmware Version: 4.0.2
Firmware Build ID: rc_tera_r4_0_2@13079
Firmware Build Date: Aug 22 2012 11:36:50

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

**Figure 4-2: Processor Family Information on AWI Version Page**

You can also display the processor family name for a zero client on the OSD Version page for the device.



View the hardware and firmware version information

MAC Address: 00-80-64-A3-12-6B
Unique Identifier: A3126B
Serial Number: 5WRDLI00001
Firmware Part Number: FW023004
Hardware Version: 770591-02L

Firmware Version: 4.0.2
Firmware Build ID: rc_tera_r4_0_2@13079
Firmware Build Date: Aug 22 2012 11:37:15

PCoIP Processor Family: Tera2
PCoIP Processor Revision: 0.0

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

**Figure 4-3: Processor Family Information on OSD Version Page**

## 4.2 Connecting a TERA1100 Zero Client to a TERA1202 Host Card

This topic explains how to configure a connection between a first-generation TERA1100 zero client and a first-generation TERA1202 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

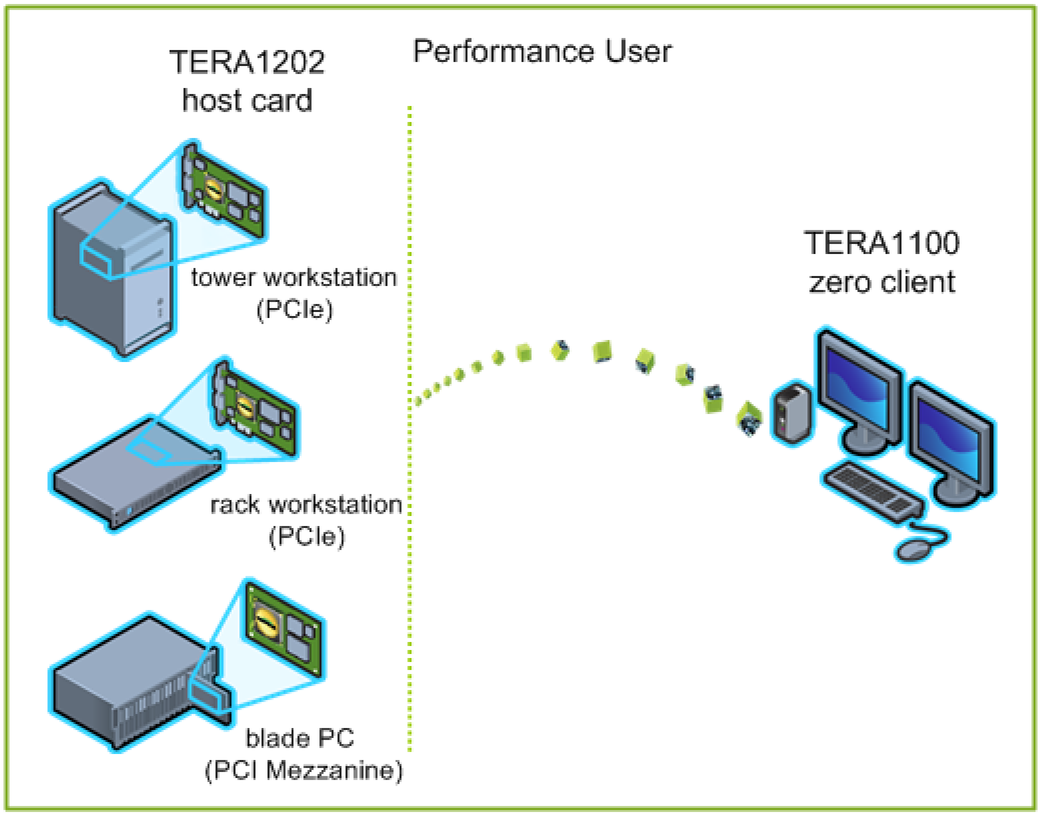


**Figure 4-4: Connecting a TERA1100 Zero Client to a TERA1202 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.3 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture,

see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.3.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.3.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.3.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.3.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.3.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.3.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language | OSD: Language Settings |

| | | |
|---|---|---|
| | Settings | |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera1 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.4 Connecting a TERA2321 Zero Client to a TERA1202 Host Card

This topic explains how to configure a connection between a second-generation TERA2321 zero client and a first-generation TERA1202 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

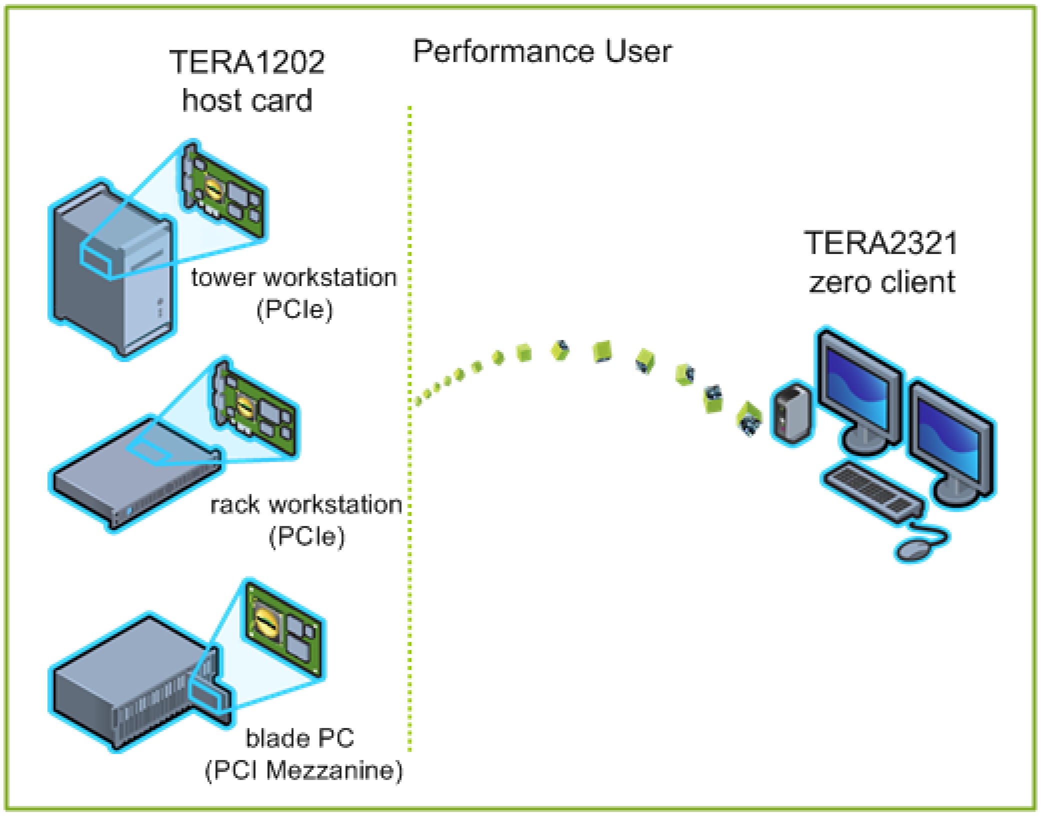


**Figure 4-5: Connecting a TERA2321 Zero Client to a TERA1202 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.5 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.5.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.5.2 Connecting Hosts and Clients Statically

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

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

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

- MC: Direct to Host: Explains how to use the MC to configure a profile that sets the **Direct to Host** session connection type for client devices. For information on how to statically link specific hosts and clients using the MC, see the "PCoIP Management Console User Manual" (TER0812002).
- AWI Client: Direct to Host: Explains how to use the AWI to statically configure a client to connect to a specific host card.

- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.

### 4.5.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.5.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.

- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.5.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.5.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

Note: The TERA2321 zero client has the same display topology options as first-generation TERA1100 clients. This is reflected in links to display topology pages in this section.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host | AWI Host: Direct from Client | OSD: Direct to Host |

| | | |
|---|---|---|
| MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera1 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |

| | | |
|---|---|---|
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.6 Connecting a TERA2140 Zero Client to a TERA1202 Host Card

This topic explains how to configure a connection between a second-generation TERA2140 zero client and a first-generation TERA1202 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

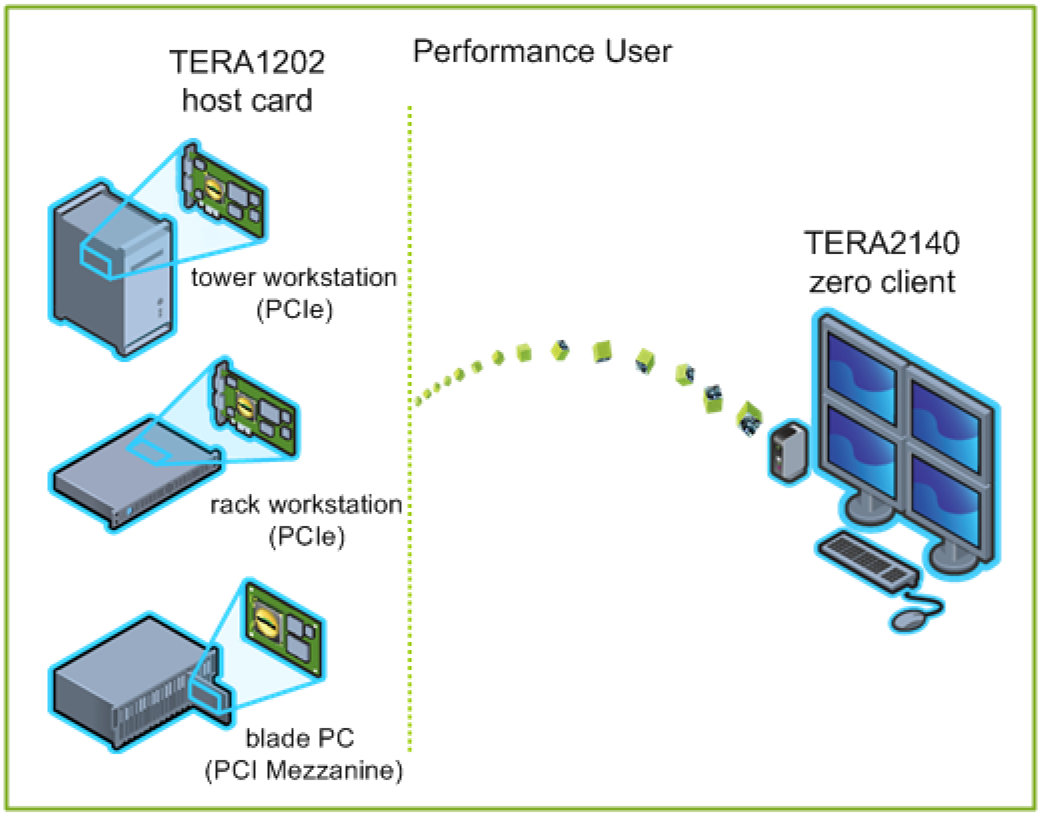


**Figure 4-6: Connecting a TERA2140 Zero Client to a TERA1202 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation

through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.7 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.7.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.7.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.7.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.7.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.7.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.7.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |

| | | |
|---|---|---|
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera1 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera2: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |

| | | |
|---|---|---|
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.8 Connecting a TERA1100 Zero Client to a TERA2220 Host Card

This topic explains how to configure a connection between a first-generation TERA1100 zero client and a second-generation TERA2220 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

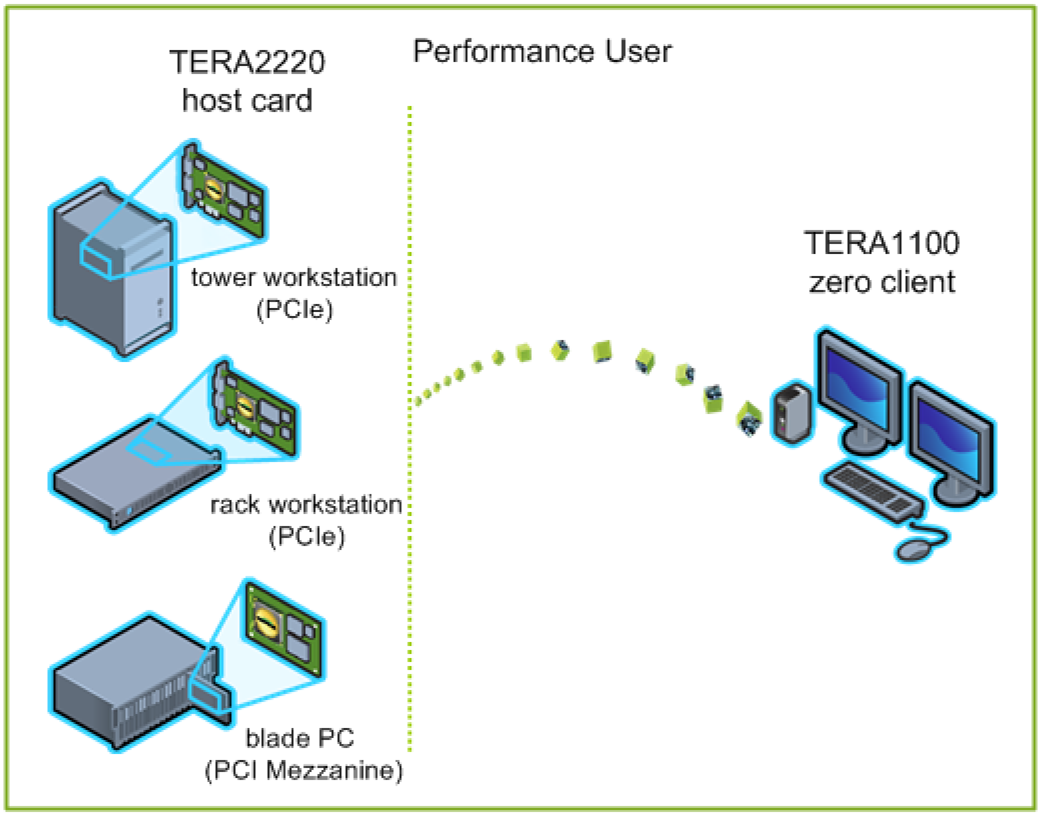


**Figure 4-7: Connecting a TERA1100 Zero Client to a TERA2220 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation

through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.9 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.9.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.9.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.9.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.9.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.9.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.9.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |

| | | |
|---|---|---|
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |

| | | |
|---|---|---|
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.10 Connecting a TERA2321 Zero Client to a TERA2220 Host Card

This topic explains how to configure a connection between a second-generation TERA2321 zero client and a second-generation TERA2220 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

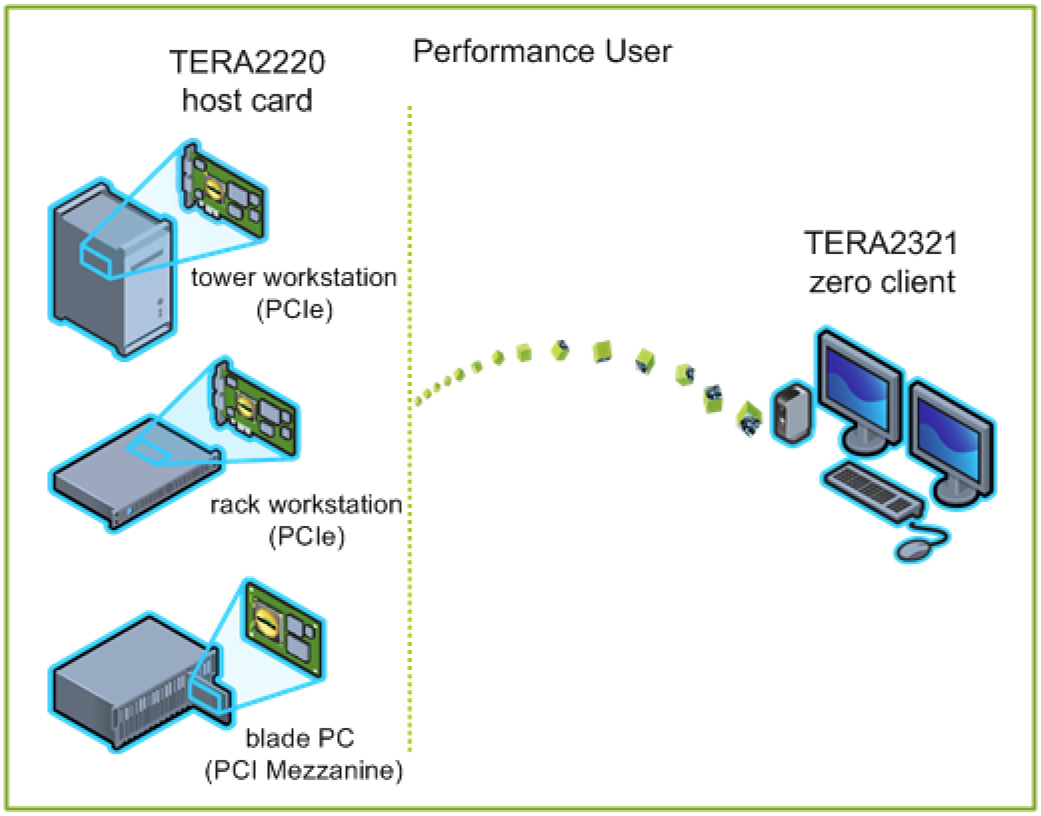


Figure 4-8: Connecting a TERA2321 Zero Client to a TERA2220 Host Card

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation

through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.11 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.11.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.11.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.11.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.11.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.11.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.11.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

Note: The TERA2321 zero client has the same display topology options as first-generation TERA1100 clients. This is reflected in links to display topology pages in this section.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |

| | | |
|---|---|---|
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo | |

| | | |
|---|---|---|
| | Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.12 Connecting a TERA2140 Zero Client to a TERA2220 Host Card

This topic explains how to configure a connection between a a second-generation TERA2140 zero client and a second-generation TERA2220 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

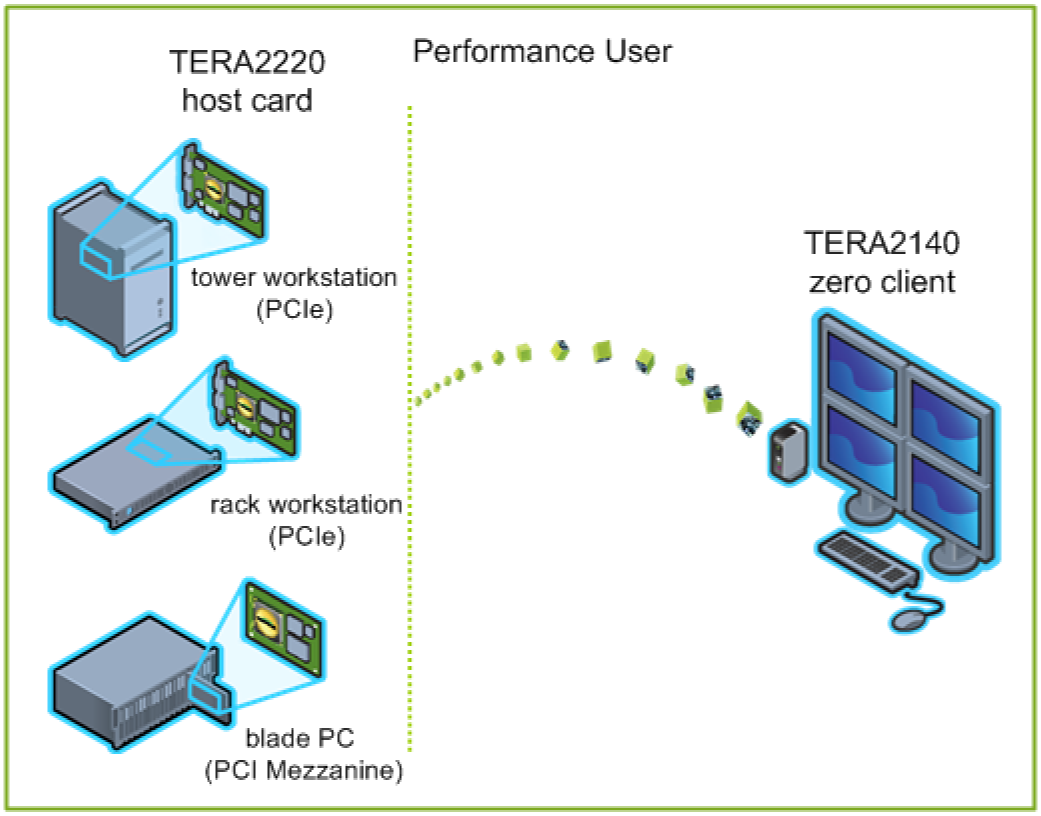


Figure 4-9: Connecting a TERA2140 Zero Client to a TERA2220 Host Card

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.13 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.13.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.13.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.13.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.13.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.13.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.13.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |

| | | |
|---|---|---|
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera2: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo | |

| | | |
|---|---|---|
| | Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.14 Connecting a TERA1100 Zero Client to a TERA2240 Host Card

This topic explains how to configure a connection between a first-generation TERA1100 zero client and a second-generation TERA2240 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

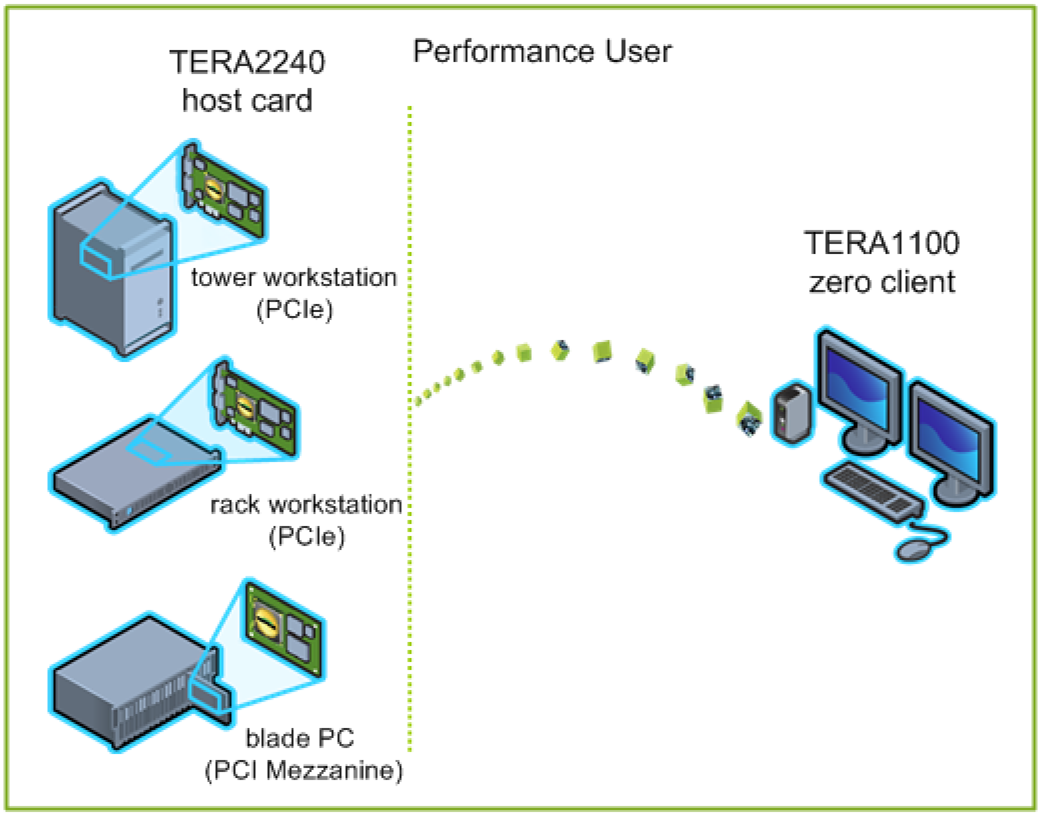


**Figure 4-10: Connecting a TERA1100 Zero Client to a TERA2240 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.15 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.15.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.15.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.15.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.15.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

## 4.15.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

## 4.15.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |

| | | |
|---|---|---|
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo | |

| | | |
|---|---|---|
| | Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.16 Connecting a TERA2321 Zero Client to a TERA2240 Host Card

This topic explains how to configure a connection between a second-generation TERA2321 zero client and a second-generation TERA2240 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

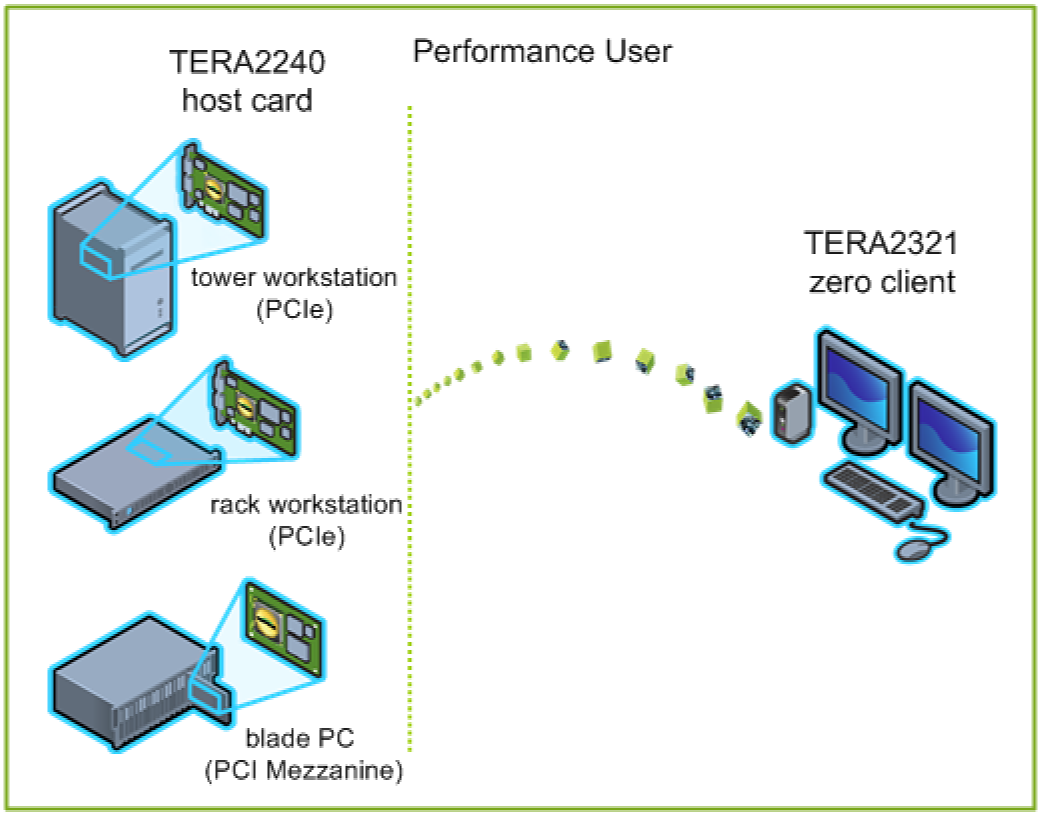


**Figure 4-11: Connecting a TERA2321 Zero Client to a TERA2240 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.17 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.17.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.17.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.17.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.17.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.17.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.17.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

Note: The TERA2321 zero client has the same display topology options as first-generation TERA1100 clients. This is reflected in links to display topology pages in this section.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using | AWI: Label Settings | OSD: Label Settings |

| | | |
|---|---|---|
| the MC, see the "PCoIP Management Console User Manual" (TER0812002). | | |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |

| | | |
|---|---|---|
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.18 Connecting a TERA2140 Zero Client to a TERA2240 Host Card

This topic explains how to configure a connection between a second-generation TERA2140 zero client and a second-generation TERA2240 host card.

Note: To determine what host card and zero client you have, see Displaying Processor Information. To see the display options for your client and host, see PCoIP Host Cards and Zero Clients.

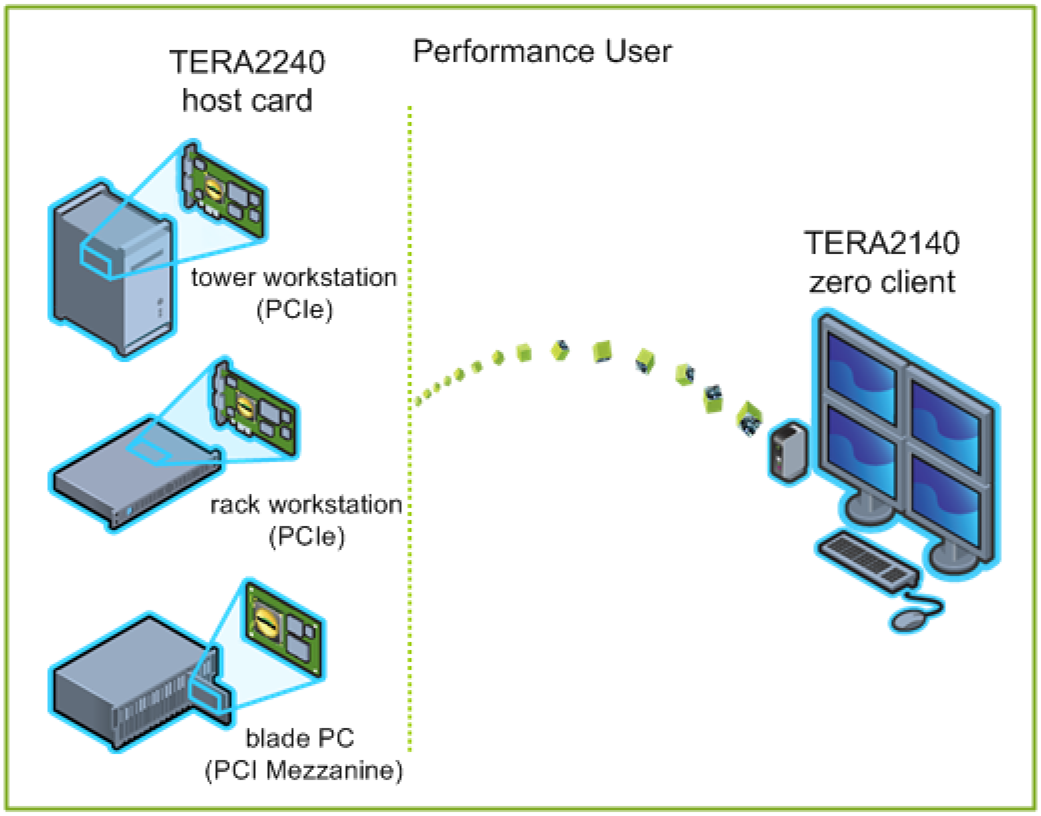


**Figure 4-12: Connecting a TERA2140 Zero Client to a TERA2240 Host Card**

The left side of the diagram shows some of the form factors for a remote workstation in which a host card can be installed, such as a tower workstation, a rack workstation, or a blade workstation. The zero client on the right can connect to the remote workstation through a direct host-client assignment, through SLP discovery, through a VMware View Connection Server broker, or through another 3rd party connection broker. These connection options are explained below.

Note: Other client options include PCoIP-enabled displays, phones, laptops, iPads, and other PCoIP-enabled mobile platforms.

## 4.19 Prerequisites

The following conditions must be met before connecting a host card and zero client:

- The host card and zero client must have the same firmware versions. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture,

see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

### 4.19.1 Session Connection Type

Depending on the size of your PCoIP deployment, you may wish to use the Management Console or a connection broker to manage connections between host cards and zero clients, or you may use the AWI to configure individual hosts and clients to use a direct session connection type.

Note: You can also use the OSD to set the client side of the session connection type configuration.

Four connection options are available:

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

### 4.19.2 Connecting Hosts and Clients Statically

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

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

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

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

### 4.19.3 Connecting Hosts and Clients Using SLP Host Discovery

If hosts reside on the same network subnet as clients, you can use the **Direct to Host + SLP** session connection type to configure clients to use Service Location Protocol (SLP) to discover the hosts on the subnet. With this configuration, the client OSD will list the first 10 hosts discovered. The user can then select the desired one and connect to it.

Note: SLP host discovery is not suitable for larger deployments with more than 10 hosts if a client might need to connect to any one of them. In this situation, a 3rd party connection broker is required.

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

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

- MC: Direct to Host + SLP: Explains how to use the MC to configure a profile that sets the **Direct to Host + SLP** session connection type for client devices.
- AWI Client: Direct to Host + SLP: Explains how to use the AWI to configure a client to use SLP discovery to connect to a host card.
- AWI Host: Direct from Client: Explains how to use the AWI to configure a host card to accept a connection request from any client or from a specific client only.
- OSD: Direct to Host + SLP: Explains how to use the OSD to configure a client to use SLP discovery to connect to a host card.

### 4.19.4 Connecting Hosts and Clients Using a 3rd Party Connection Broker

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

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

Note: For information about 3rd party connection brokers, see Knowledge Base support topic 15134-24 on the Teradici support site.

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

- MC: Connection Management Interface: Explains how to use the MC to configure a profile that sets the **Connection Management Interface** session connection type for client and host devices.
- AWI Client: Connection Management Interface: Explains how to use the AWI to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.
- AWI Host: Connection Management Interface: Explains how to use the AWI to configure a host to use a 3rd party connection broker for accepting a connection request from a client.
- OSD: Connection Management Interface: Explains how to use the OSD to configure a client to use a 3rd party connection broker to broker the connection between the client and a host card.

### 4.19.5 Connecting Hosts and Clients Using the VMware View Connection Server Broker

You can also use the VMware View Connection Server broker to broker a connection between clients and host cards.

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

For this option, VMware View Agent must be installed on the host workstation, and a number of other configuration requirements for both the client and host must be in place. For complete details, please refer to "Using PCoIP Host Cards with VMware View" (TER0911004).

### 4.19.6 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Host: Initial Setup<br>AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: Discovery Settings | AWI: Discovery Settings | OSD: Discovery Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: Direct to Host<br>MC: Direct to Host + SLP Host Discovery<br>MC: Connection Management Interface | AWI Host: Direct from Client<br>AWI Client: Direct to Host<br>AWI Client: Direct to Host + SLP Host Discovery<br>AWI Host: Connection Management Interface<br>AWI Client: Connection Management Interface | OSD: Direct to Host<br>OSD: Direct to Host + SLP Host Discovery<br>OSD: Connection Management Interface |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language | OSD: Language Settings |

| | | |
|---|---|---|
| | Settings | |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Host: Image Settings<br>AWI Client: Image Settings | OSD: Image Settings |
| MC: Monitor Emulation | AWI Tera2 Host: Monitor Emulation | |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Host: Audio Permissions<br>AWI Client: Audio Permissions | |
| MC: Power Permissions | AWI Client: Power Permissions | |
| MC: Host Driver Function | AWI Host: Host Driver Function | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera2: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Host: USB Permissions<br>AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.20 Connecting a TERA1100 Zero Client to a VMware View Virtual Desktop

This topic explains how to configure a connection between a first-generation TERA1100 zero client and a VMware View virtual desktop.

Note: To determine what zero client you have, see Displaying Processor Information. To see the display options for this client, see PCoIP Host Cards and Zero Clients.

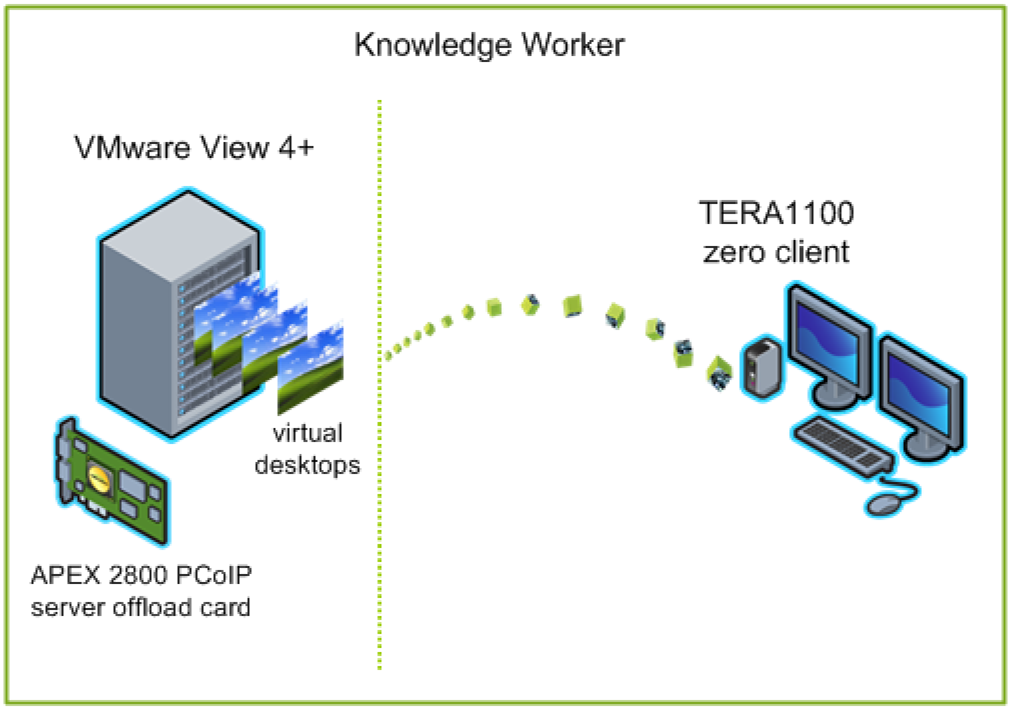


**Figure 4-13: Connecting a TERA1100 Zero Client to a VMware View Virtual Desktop**

The left side of the diagram shows a typical server-hosted VMware View implementation—a set of virtual desktops (often referred to as virtual desktop infrastructure, or VDI) and an APEX 2800 server offload card, which provides hardware-accelerated PCoIP image encoding. The zero client on the right connects to a VMware View virtual desktop using a VMware View Connection Server broker. You can configure users to connect to a VMware View virtual desktop using manual or automatic logon, using VMware View Kiosk mode (to provide multiple users access to information on a desktop), or using Imprivata OneSign technology (to provide proximity card support for VDI roaming implementations). These VMware View configuration options are described below.

Note: For information about the APEX 2800, see the "Teradici APEX 2800 Server Offload Card Administrator's Guide" (TER1109003). For information on how to configure VMware View for use with a PCoIP zero client, see the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).

## 4.21 Prerequisites

The following conditions must be met before connecting a zero client to a VMware View virtual desktop:

- The VMware View installation, which includes the VMware View Manager and VMware View Agent, must be version 4.0.1 or newer. For more information, refer to VMware documentation and also the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).
- The zero client firmware version must be 3.1.0 or newer. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

## 4.22 Session Connection Type

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

Four connection options are available:

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

### 4.22.1 View Connection Server

To configure a client to connect to a VMware virtual desktop, use the **View Connection Server** session connection type. You need to provide the IP address (or DNS name) of the VMware View Connection Server for this option.

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

- MC: View Connection Server: Explains how to use the MC to configure a profile that sets the **View Connection Server** session connection type for client devices.
- AWI Client: View Connection Server: Explains how to use the AWI to configure a client to connect to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server: Explains how to use the OSD to configure a client to connect to a virtual desktop via a VMware View Connection Server.

### 4.22.2 View Connection Server + Auto-Logon

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

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

- MC: View Connection Server + Auto-Logon: Explains how to use the MC to configure a profile that sets the **View Connection Server + Auto-Logon** session connection type for client devices.
- AWI Client: View Connection Server + Auto-Logon: Explains how to use the AWI to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Auto-Logon: Explains how to use the OSD to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.

### 4.22.3 View Connection Server + Kiosk

VMware View Kiosk mode allows you to configure 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 need to provide the IP address (or DNS name) of the VMware View Connection Server and the kiosk user name—either a custom user name for the kiosk or its MAC address.

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

- MC: View Connection Server + Kiosk: Explains how to use the MC to configure a profile that sets the **View Connection Server + Kiosk** session connection type for client devices.
- AWI Client: View Connection Server + Kiosk: Explains how to use the AWI to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Kiosk: Explains how to use the OSD to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.

### 4.22.4 View Connection Server + Imprivata OneSign

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

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

- MC: View Connection Server + Imprivata OneSign: Explains how to use the MC to configure a profile that sets the **View Connection Server + Imprivata OneSign** session connection type for client devices.
- AWI Client: View Connection Server + Imprivata OneSign: Explains how to use the AWI to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Imprivata OneSign: Explains how to use the OSD to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.

## 4.22.5 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: View Connection Server<br>MC: View Connection Server + Auto-Logon<br>MC: View Connection Server + Kiosk<br>MC: View Connection Server + Imprivata OneSign | AWI Client: View Connection Server<br>AWI Client: View Connection Server + Auto-Logon<br>AWI Client: View Connection Server + Kiosk<br>AWI Client: View Connection Server + Imprivata OneSign | OSD: View Connection Server<br>OSD: View Connection Server + Auto-Logon<br>OSD: View Connection Server + Kiosk<br>OSD: View Connection Server + Imprivata OneSign |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Client: Image Settings | OSD: Image Settings |

| | | |
|---|---|---|
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Client: Audio Permissions | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.23 Connecting a TERA2321 Zero Client to a VMware View Virtual Desktop

This topic explains how to configure a connection between a second-generation TERA2321 zero client and a VMware View virtual desktop.

Note: To determine what zero client you have, see Displaying Processor Information. To see the display options for this client, see PCoIP Host Cards and Zero Clients.

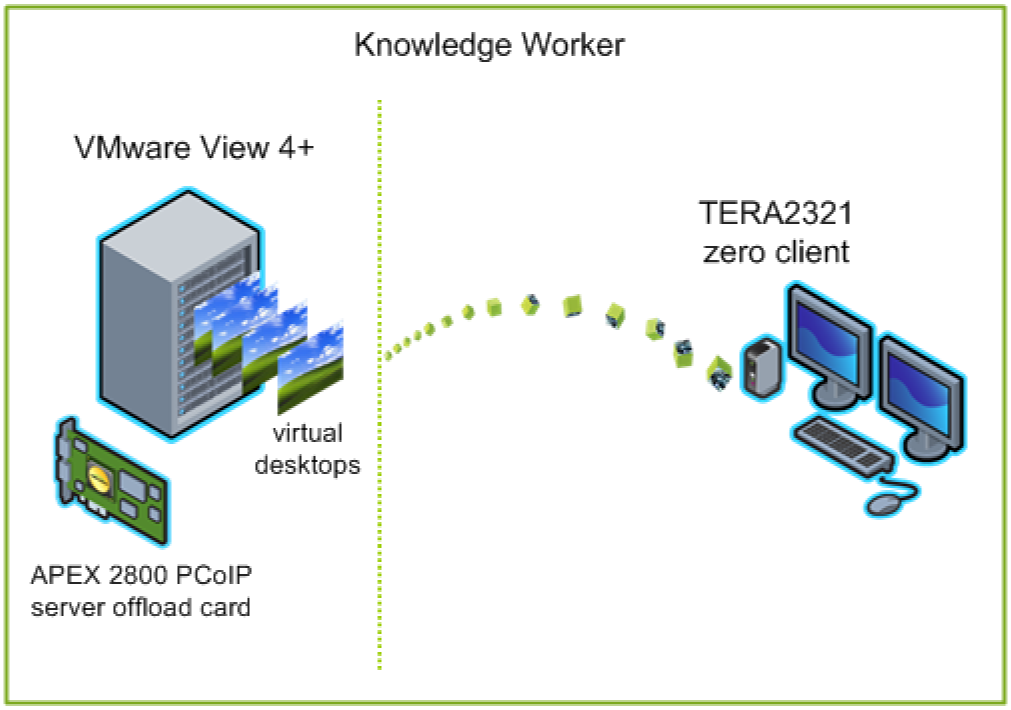


**Figure 4-14: Connecting a TERA2321 Zero Client to a VMware View Virtual Desktop**

The left side of the diagram shows a typical server-hosted VMware View implementation—a set of virtual desktops (often referred to as virtual desktop infrastructure, or VDI) and an APEX 2800 server offload card, which provides hardware-accelerated PCoIP image encoding. The zero client on the right connects to a VMware View virtual desktop using a VMware View Connection Server broker. You can configure users to connect to a VMware View virtual desktop using manual or automatic logon, using VMware View Kiosk mode (to provide multiple users access to information on a desktop), or using Imprivata OneSign technology (to provide proximity card support for VDI roaming implementations). These VMware View configuration options are described below.

Note: For information about the APEX 2800, see the "Teradici APEX 2800 Server Offload Card Administrator's Guide" (TER1109003). For information on how to configure VMware View for use with a PCoIP zero client, see the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).

## 4.24 Prerequisites

The following conditions must be met before connecting a zero client to a VMware View virtual desktop:

- The VMware View installation, which includes the VMware View Manager and VMware View Agent, must be version 4.0.1 or newer. For more information, refer to VMware documentation and also the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).

- The zero client firmware version must be 3.1.0 or newer. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

## 4.25 Session Connection Type

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

Four connection options are available:

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

### 4.25.1 View Connection Server

To configure a client to connect to a VMware virtual desktop, use the **View Connection Server** session connection type. You need to provide the IP address (or DNS name) of the VMware View Connection Server for this option.

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

- MC: View Connection Server: Explains how to use the MC to configure a profile that sets the **View Connection Server** session connection type for client devices.
- AWI Client: View Connection Server: Explains how to use the AWI to configure a client to connect to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server: Explains how to use the OSD to configure a client to connect to a virtual desktop via a VMware View Connection Server.

### 4.25.2 View Connection Server + Auto-Logon

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

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

- MC: View Connection Server + Auto-Logon: Explains how to use the MC to configure a profile that sets the **View Connection Server + Auto-Logon** session connection type for client devices.
- AWI Client: View Connection Server + Auto-Logon: Explains how to use the AWI to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Auto-Logon: Explains how to use the OSD to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.

### 4.25.3 View Connection Server + Kiosk

VMware View Kiosk mode allows you to configure 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 need to provide the IP address (or DNS name) of the VMware View Connection Server and the kiosk user name—either a custom user name for the kiosk or its MAC address.

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

- MC: View Connection Server + Kiosk: Explains how to use the MC to configure a profile that sets the **View Connection Server + Kiosk** session connection type for client devices.
- AWI Client: View Connection Server + Kiosk: Explains how to use the AWI to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Kiosk: Explains how to use the OSD to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.

### 4.25.4 View Connection Server + Imprivata OneSign

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

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

- MC: View Connection Server + Imprivata OneSign: Explains how to use the MC to configure a profile that sets the **View Connection Server + Imprivata OneSign** session connection type for client devices.
- AWI Client: View Connection Server + Imprivata OneSign: Explains how to use the AWI to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Imprivata OneSign: Explains how to use the OSD to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.

### 4.25.5 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

Note: The TERA2321 zero client has the same display topology options as first-generation TERA1100 clients. This is reflected in links to display topology pages in this section.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: View Connection Server<br>MC: View Connection Server + Auto-Logon<br>MC: View Connection Server + Kiosk<br>MC: View Connection Server + Imprivata OneSign | AWI Client: View Connection Server<br>AWI Client: View Connection Server + Auto-Logon<br>AWI Client: View Connection Server + Kiosk<br>AWI Client: View Connection Server + Imprivata OneSign | OSD: View Connection Server<br>OSD: View Connection Server + Auto-Logon<br>OSD: View Connection Server + Kiosk<br>OSD: View Connection Server + Imprivata OneSign |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Client: Image Settings | OSD: Image Settings |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Client: Audio Permissions | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral | |

| | | |
|---|---|---|
| | Settings | |
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera1: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.26 Connecting a TERA2140 Zero Client to a VMware View Virtual Desktop

This topic explains how to configure a connection between a second-generation TERA2140 zero client and a VMware View virtual desktop.

Note: To determine what zero client you have, see Displaying Processor Information. To see the display options for this client, see PCoIP Host Cards and Zero Clients.

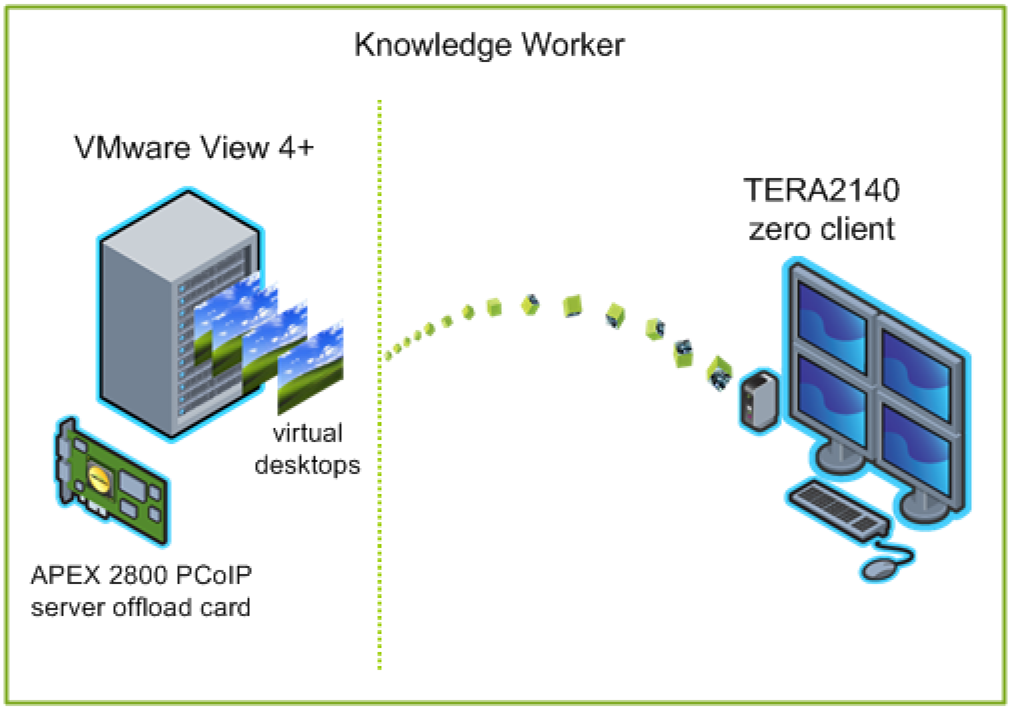


**Figure 4-15: Connecting a TERA2140 Zero Client to a VMware View Virtual Desktop**

The left side of the diagram shows a typical server-hosted VMware View implementation—a set of virtual desktops (often referred to as virtual desktop infrastructure, or VDI) and an APEX 2800 server offload card, which provides hardware-accelerated PCoIP image encoding. The zero client on the right connects to a VMware View virtual desktop using a VMware View Connection Server broker. You can configure users to connect to a VMware View virtual desktop using manual or automatic logon, using VMware View Kiosk mode (to provide multiple users access to information on a desktop), or using Imprivata OneSign technology (to provide proximity card support for VDI roaming implementations). These VMware View configuration options are described below.

Note: For information about the APEX 2800, see the "Teradici APEX 2800 Server Offload Card Administrator's Guide" (TER1109003). For information on how to configure VMware View for use with a PCoIP zero client, see the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).

## 4.27 Prerequisites

The following conditions must be met before connecting a zero client to a VMware View virtual desktop:

- The VMware View installation, which includes the VMware View Manager and VMware View Agent, must be version 4.0.1 or newer. For more information, refer to VMware documentation and also the "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).

- The zero client firmware version must be 3.1.0 or newer. For information how to upload firmware using the MC, see the "PCoIP Management Console User Manual" (TER0812002). For information on how to assign a firmware file to a profile using the MC, see MC: Firmware Management. For information on how to upload firmware to a single host or client using the AWI, see AWI: Firmware Upload Settings.
- Your network resources must be able to meet bandwidth, QoS, latency, jitter, and packet loss requirements. For more information about designing PCoIP network architecture, see the "PC-over-IP Protocol Virtual Desktop Network Design Checklist" (TER1105004).

## 4.28 Session Connection Type

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

Four connection options are available:

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

### 4.28.1 View Connection Server

To configure a client to connect to a VMware virtual desktop, use the **View Connection Server** session connection type. You need to provide the IP address (or DNS name) of the VMware View Connection Server for this option.

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

- MC: View Connection Server: Explains how to use the MC to configure a profile that sets the **View Connection Server** session connection type for client devices.
- AWI Client: View Connection Server: Explains how to use the AWI to configure a client to connect to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server: Explains how to use the OSD to configure a client to connect to a virtual desktop via a VMware View Connection Server.

### 4.28.2 View Connection Server + Auto-Logon

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

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

- MC: View Connection Server + Auto-Logon: Explains how to use the MC to configure a profile that sets the **View Connection Server + Auto-Logon** session connection type for client devices.
- AWI Client: View Connection Server + Auto-Logon: Explains how to use the AWI to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Auto-Logon: Explains how to use the OSD to configure a client to automatically enter the user's login details when connecting to a virtual desktop via a VMware View Connection Server.

### 4.28.3 View Connection Server + Kiosk

VMware View Kiosk mode allows you to configure 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 need to provide the IP address (or DNS name) of the VMware View Connection Server and the kiosk user name—either a custom user name for the kiosk or its MAC address.

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

- MC: View Connection Server + Kiosk: Explains how to use the MC to configure a profile that sets the **View Connection Server + Kiosk** session connection type for client devices.
- AWI Client: View Connection Server + Kiosk: Explains how to use the AWI to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Kiosk: Explains how to use the OSD to configure a client to use Kiosk mode when connecting to a virtual desktop via a VMware View Connection Server.

### 4.28.4 View Connection Server + Imprivata OneSign

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

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

- MC: View Connection Server + Imprivata OneSign: Explains how to use the MC to configure a profile that sets the **View Connection Server + Imprivata OneSign** session connection type for client devices.
- AWI Client: View Connection Server + Imprivata OneSign: Explains how to use the AWI to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.
- OSD: View Connection Server + Imprivata OneSign: Explains how to use the OSD to configure a client to use Imprivata OneSign mode when connecting to a virtual desktop via a VMware View Connection Server.

### 4.28.5 Other Configuration Links

To configure the full range of firmware parameters for this session type, see the following topics.

Note: Some configuration functions are not available in the OSD.

| Using the MC | Using the AWI | Using the OSD |
|---|---|---|
| | AWI Client: Initial Setup | |
| MC: Network Settings | AWI: Network Settings | OSD: Network Settings |
| For information on how to manage device naming using the MC, see the "PCoIP Management Console User Manual" (TER0812002). | AWI: Label Settings | OSD: Label Settings |
| MC: SNMP Settings | AWI: SNMP Settings | |
| MC: View Connection Server<br>MC: View Connection Server + Auto-Logon<br>MC: View Connection Server + Kiosk<br>MC: View Connection Server + Imprivata OneSign | AWI Client: View Connection Server<br>AWI Client: View Connection Server + Auto-Logon<br>AWI Client: View Connection Server + Kiosk<br>AWI Client: View Connection Server + Imprivata OneSign | OSD: View Connection Server<br>OSD: View Connection Server + Auto-Logon<br>OSD: View Connection Server + Kiosk<br>OSD: View Connection Server + Imprivata OneSign |
| MC: Encryption Settings | AWI: Encryption Settings | |
| MC: Bandwidth Settings | AWI: Bandwidth Settings | |
| MC: Language Settings | AWI Client: Language Settings | OSD: Language Settings |
| MC: OSD Settings | AWI: OSD Settings | OSD: OSD Settings |
| MC: Image Settings | AWI Client: Image Settings | OSD: Image Settings |
| MC: Time Settings | AWI: Time Settings | |
| MC: Security Settings | AWI: Security Settings | |
| MC: Audio Permissions | AWI Client: Audio Permissions | |
| MC: Event Log Settings | AWI: Event Log Settings | OSD: Event Log Settings |
| MC: Peripheral Settings | AWI Client: Peripheral Settings | |

| | | |
|---|---|---|
| MC: IPv6 Settings | AWI: IPv6 Settings | OSD: IPv6 Settings |
| MC: Display Topology Settings | | OSD Tera2: Display Topology Settings |
| MC: OSD Logo Settings | AWI Client: OSD Logo Settings | |
| MC: Firmware Management | AWI: Firmware Upload Settings | |
| MC: USB Permissions | AWI Client: USB Permissions | |
| MC: Certificate Store Management | AWI: Certificate Upload Settings | |
| MC: VMware View Certificate Checking Settings | AWI Client: VMware View Certificate Checking Settings | OSD: VMware View Certificate Checking Settings |

## 4.29 Connecting a VMware View Client to a VMware View Virtual Desktop

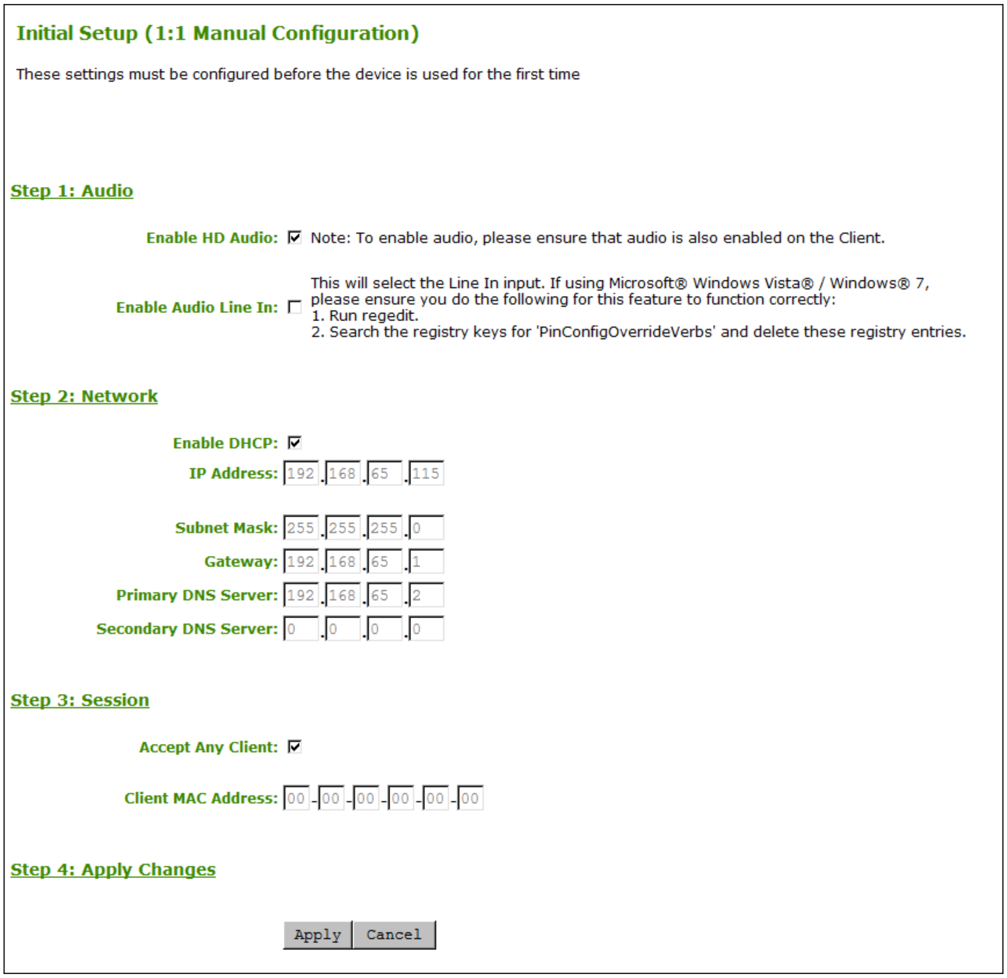
You can also take advantage of PCoIP protocol technology by connecting to a VMware View virtual desktop through a VMware View 4 (or newer) software client that is installed on your PC, laptop, phone, or mobile platform. Please refer to the VMware View documentation for details on how to install and manage this VMware View VDI solution.

# 5 PCoIP GUI Reference

## 5.1 Initial Setup

### 5.1.1 AWI Host: Initial Setup Page

You can display 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 Client.

Enable Audio Line In: □ This will select the Line In input. If using Microsoft® Windows Vista® / Windows® 7, please ensure you do the following for this feature to function correctly:
1. Run regedit.
2. Search the registry keys for 'PinConfigOverrideVerbs' and delete these registry entries.

Step 2: Network

Enable DHCP: ☑

IP Address: 192 . 168 . 65 . 115

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 65 . 1

Primary DNS Server: 192 . 168 . 65 . 2

Secondary DNS Server: 0 . 0 . 0 . 0

Step 3: Session

Accept Any Client: ☑

Client MAC Address: 00 - 00 - 00 - 00 - 00 - 00

Step 4: Apply Changes

**Figure 5-1: AWI Host Initial Setup Page**

**Table 5-1: Audio Parameters**

| Parameter | Description |
|---|---|
| Enable HD Audio | Enables audio support on the host or client. |
| Enable Microsoft® Windows Vista® 64-bit Mode | Enables 64-bit mode on the host. This mode should only be used for Windows Vista 64-bit and Windows 7® 64-bit versions to ensure audio works correctly. |

| Parameter | Description |
|---|---|
| | Note: Enabling 64-bit mode is not required for Linux, Windows 7® 32-bit, Windows Vista 32-bit, or Windows XP (32-bit or 64-bit). |
| Enable Audio Line In | **Enable:** Use the line-in connector found on the client.<br>**Disable:** Use the line-in connector as a microphone input.<br>Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device. |

**Table 5-2: Network Parameters**

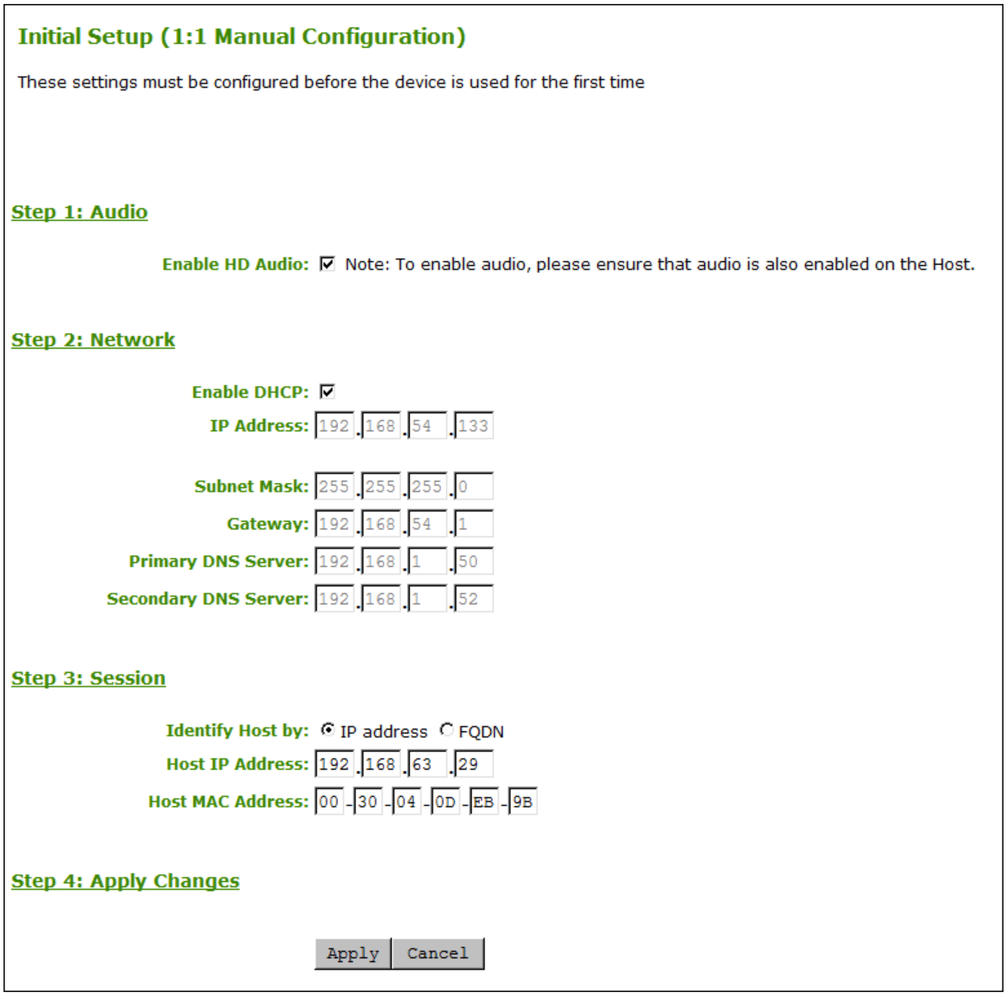
| Parameter | Description |
|---|---|
| Enable DHCP | Enables DHCP (as opposed to using manual IP address configuration) |
| IP Address | Device's IP address |
| Subnet Mask | Device's subnet mask |
| Gateway | Device's gateway IP address |
| Primary DNS Server | Device's primary DNS IP address |
| Secondary DNS Server | Device's secondary DNS IP address |

**Table 5-3: Session Parameters**

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

### 5.1.2 AWI Client: Initial Setup Page

You can display 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: 192 . 168 . 54 . 133

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 54 . 1

Primary DNS Server: 192 . 168 . 1 . 50

Secondary DNS Server: 192 . 168 . 1 . 52

**Step 3: Session**

Identify Host by: ● IP address ○ FQDN

Host IP Address: 192 . 168 . 63 . 29

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

**Step 4: Apply Changes**

**Figure 5-2: AWI Client Initial Setup Page**

**Table 5-4: Audio Parameters**

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

**Table 5-5: Network Parameters**

| Parameter | Description |
|---|---|
| Enable DHCP | Enables DHCP (as opposed to using manual IP address configuration) |
| IP Address | Device’s IP address |
| Subnet Mask | Device’s subnet mask |

| Parameter | Description |
|---|---|
| Gateway | Device's gateway IP address |
| Primary DNS Server | Device's primary DNS IP address |
| Secondary DNS Server | Device's secondary DNS IP address |

**Table 5-6: Session Parameters**

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

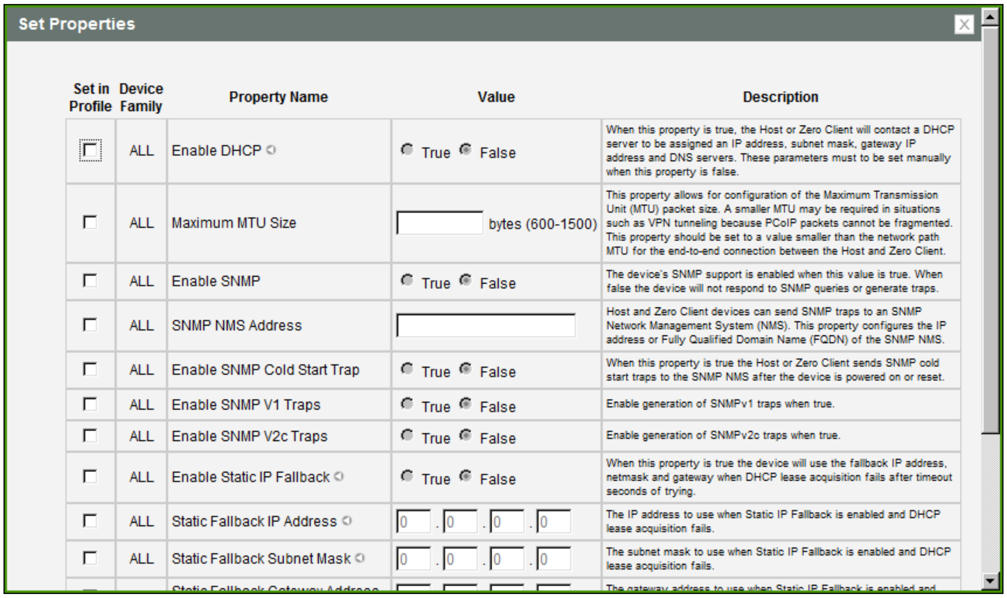
Note: When host discovery or connection management is configured on the client, you cannot modify the client session parameters. A message appears on the **Initial Setup Client** page instead of the session parameters.

# 5.2 Configuring the Network

## 5.2.1 MC: Network Settings

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

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable DHCP | ○ True ● False | When this property is true, the Host or Zero Client will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address and DNS servers. These parameters must to be set manually when this property is false. |
| □ | ALL | Maximum MTU Size | bytes (600-1500) | This property allows for configuration of the Maximum Transmission Unit (MTU) packet size. A smaller MTU may be required in situations such as VPN tunneling because PCoIP packets cannot be fragmented. This property should be set to a value smaller than the network path MTU for the end-to-end connection between the Host and Zero Client. |
| □ | ALL | Enable SNMP | ○ True ● False | The device's SNMP support is enabled when this value is true. When false the device will not respond to SNMP queries or generate traps. |
| □ | ALL | SNMP NMS Address | | Host and Zero Client devices can send SNMP traps to an SNMP Network Management System (NMS). This property configures the IP address or Fully Qualified Domain Name (FQDN) of the SNMP NMS. |
| □ | ALL | Enable SNMP Cold Start Trap | ○ True ● False | When this property is true the Host or Zero Client sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset. |
| □ | ALL | Enable SNMP V1 Traps | ○ True ● False | Enable generation of SNMPv1 traps when true. |
| □ | ALL | Enable SNMP V2c Traps | ○ True ● False | Enable generation of SNMPv2c traps when true. |
| □ | ALL | Enable Static IP Fallback | ○ True ● False | When this property is true the device will use the fallback IP address, netmask and gateway when DHCP lease acquisition fails after timeout seconds of trying. |
| □ | ALL | Static Fallback IP Address | 0 . 0 . 0 . 0 | The IP address to use when Static IP Fallback is enabled and DHCP lease acquisition fails. |
| □ | ALL | Static Fallback Subnet Mask | 0 . 0 . 0 . 0 | The subnet mask to use when Static IP Fallback is enabled and DHCP lease acquisition fails. |
| | | Static Fallback Gateway Address | | The gateway address to use when Static IP Fallback is enabled and |

Figure 5-3: MC Network Configuration

Table 5-7: MC Network Configuration Parameters

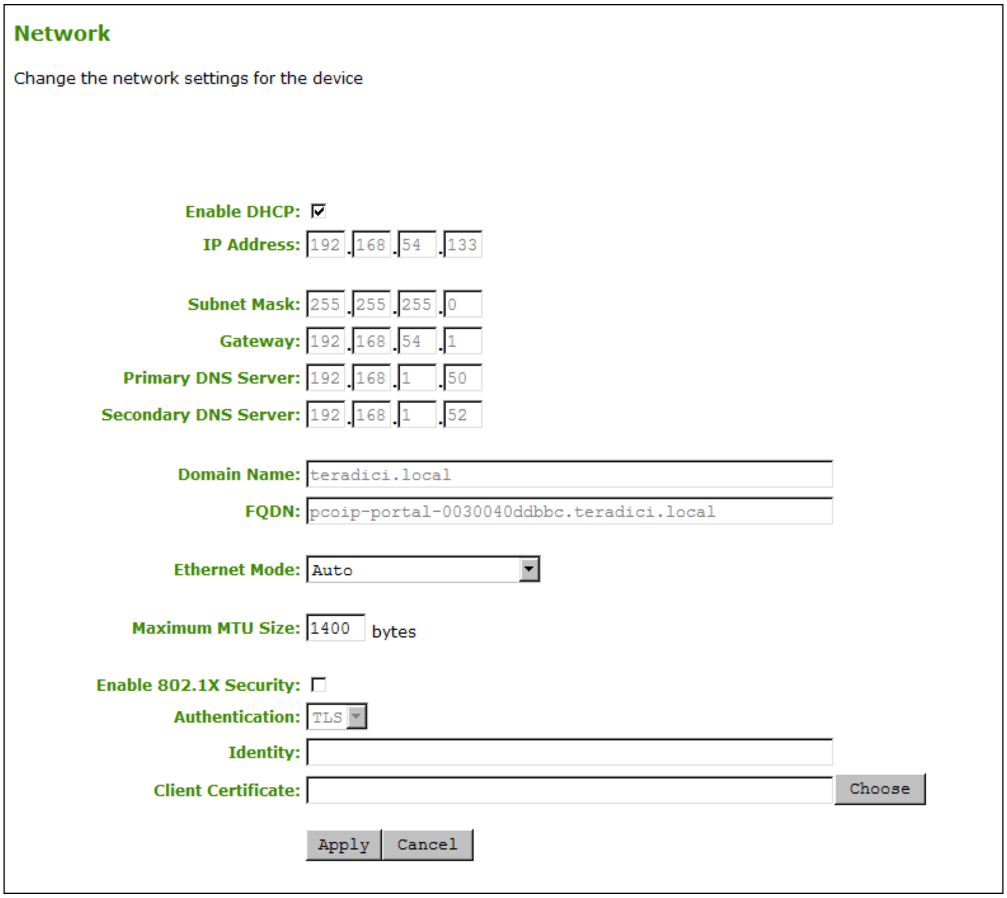
| Parameter | Description |
|---|---|
| Enable DHCP | When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN).<br>When disabled, you must set these parameters manually.<br>Note: For MC discovery, the device also requests vendor class options 60/43.<br>Note: This property requires a device restart after being changed. |
| Maximum MTU Size | Lets you configure the **Maximum Transfer Unit** packet size.<br>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.<br>The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions.<br>Note: The default MTU is 1400 for sessions between PCoIP zero clients and PCoIP host cards.<br>The default MTU is 1300 for sessions with PCoIP software (in the host or client) such as VMware View. |
| 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. |

| Parameter | Description |
|---|---|
| SNMP NMS Address | If you want the device to send SNMP traps to an SNMP Network Management System (NMS), enter the IP address or fully qualified domain name (FQDN) of the SNMP NMS. |
| Enable SNMP Cold Start Trap | When enabled, the device sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset. |
| Enable SNMP V1 Traps | When enabled, allows generation of SNMPv1 traps. |
| Enable SNMP V2c Traps | When enabled, allows generation of SNMPv2c traps. |
| Enable Static IP Fallback | When enabled, the device will use the fallback IP address, netmask and gateway when DHCP lease acquisition fails after timeout seconds of trying.<br>Note: This property requires a device restart after being changed. |
| Static Fallback IP Address | Configures the IP address to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails.<br>Note: This property requires a device restart after being changed. |
| Static Fallback Subnet Mask | Configures the subnet mask to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails.<br>Note: This property requires a device restart after being changed. |
| Static Fallback Gateway Address | Configures the gateway address to use when **Static IP Fallback** is enabled and DHCP lease acquisition fails.<br>Note: This property requires a device restart after being changed. |
| Static Fallback Timeout | Configures the amount of time in seconds the device will attempt to acquire a DHCP lease before using the fallback address configuration. You must enter a value greater than or equal to 60.<br>Note: It may take up to 30 seconds longer than this value for the fallback configuration to become active.<br>Note: This property requires a device restart after being changed. |
| SNMP Community Name | Configures the SNMP community name used by the device. |

### 5.2.2 AWI: Network Settings

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

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



Network

Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 54 . 133

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 54 . 1

Primary DNS Server: 192 . 168 . 1 . 50

Secondary DNS Server: 192 . 168 . 1 . 52

Domain Name: teradici.local

FQDN: pcoip-portal-0030040ddbbc.teradici.local

Ethernet Mode: Auto

Maximum MTU Size: 1400 bytes

Enable 802.1X Security: □

Authentication: TLS

Identity:

Client Certificate:

Figure 5-4: AWI Network Page

Table 5-8: AWI Network Page Parameters

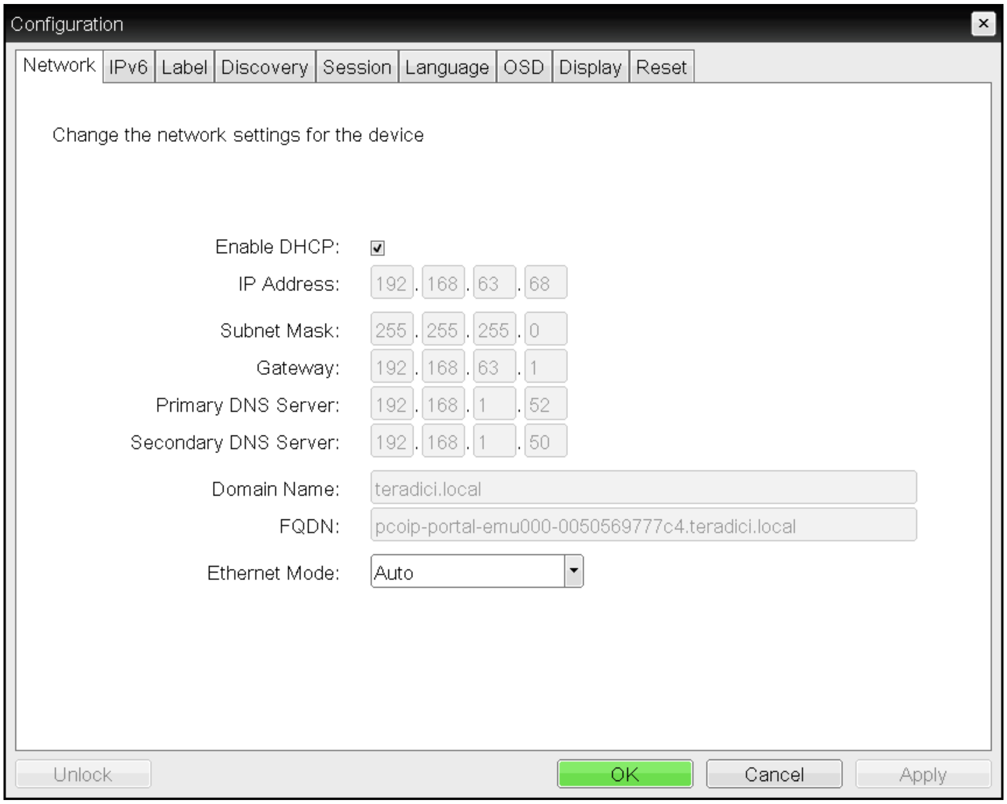
| Parameter | Description |
|---|---|
| Enable DHCP | When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN).<br>When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

| Parameter | Description |
|---|---|
| Primary DNS Server | The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address. |
| Secondary DNS Server | The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address. |
| Domain Name | The domain named of the host or client (e.g., "domain.local"). This field is optional. |
| FQDN | The fully qualified domain name for the host or client. The default is pcoip-host-<MAC> or pcoip-portal-<MAC> where <MAC> is the host or client's MAC address. If used, the domain name is appended (for example, pcoip-host-<MAC>.domain.local). This field is read-only on this page.<br>Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured. |
| Ethernet Mode | Lets you configure the Ethernet mode of the host or client as follows:<br>● **Auto**<br>● **100 Mbps Full-Duplex**<br>● **10 Mbps Full-Duplex**<br>When you choose **10 Mbps Full Duplex** or **100 Mbps Full-Duplex** and then click **Apply**, the following warning message appears:<br>"Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?"<br>Click **OK** to change the parameter.<br>Note: You should always set the Ethernet mode to **Auto** and only use **10 Mbps Full-Duplex** or **100 Mbps Full-Duplex** when the other network equipment (e.g., a switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet mode may result in the network operating at half-duplex, which is not supported by the PCoIP protocol. The session will be severely degraded and eventually dropped. |
| Maximum MTU Size | Lets you configure the **Maximum Transfer Unit** packet size.<br>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.<br>The **Maximum MTU Size** range is 600 to 1500 bytes for all firmware versions.<br>Note: The default MTU is 1400 for sessions between PCoIP zero clients and PCoIP host cards. |

| Parameter | Description |
|---|---|
| | The default MTU is 1300 for sessions with PCoIP software (in the host or client) such as VMware View. |
| Enable 802.1X Security | Enable this field for each of your hosts and zero clients if your network uses 802.1X security. If enabled, configure the **Authentication**, **Identity**, and **Client Certificate** fields. |
| Authentication | This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported. |
| Identity | Enter the identity string used to identify your device to the network. |
| Client Certificate | Click **Choose** to select the client certificate you want to use for your 802.1X devices. The list of certificates that appears includes the certificates uploaded from the **Certificate Upload** page that contain a private key. The certificate you choose from the **Network** page is linked to the read-only **Client Certificate** field on the **Certificate Upload** page.<br>Note: PCoIP only supports one 802.1X client certificate. Ensure your security details are all contained within the one file. The 802.1X certificate must contain a private key. |

### 5.2.3 OSD: Network Settings

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



Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 63 . 68

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 63 . 1

Primary DNS Server: 192 . 168 . 1 . 52

Secondary DNS Server: 192 . 168 . 1 . 50

Domain Name: teradici.local

FQDN: pcoip-portal-emu000-0050569777c4.teradici.local

Ethernet Mode: Auto

**Figure 5-5: OSD Network Page**

**Table 5-9: OSD Network Page Parameters**

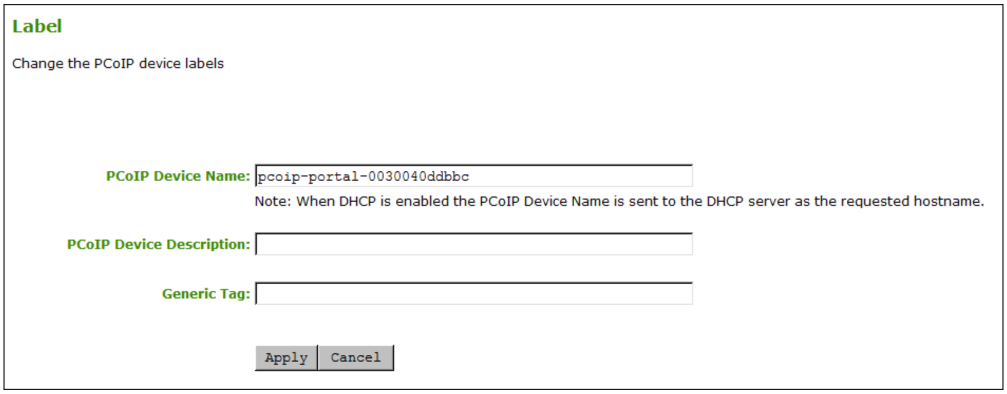
| Parameter | Description |
|---|---|
| Enable DHCP | When enabled, the device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers, and also requests a domain name (option 15), host name (option 12), and client fully qualified domain name (FQDN).<br>When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

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

## 5.3 Label Settings

### 5.3.1 AWI: Label Settings

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



Label

Change the PCoIP device labels

PCoIP Device Name: pcoip-portal-0030040ddbbc

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

PCoIP Device Description:

Generic Tag:

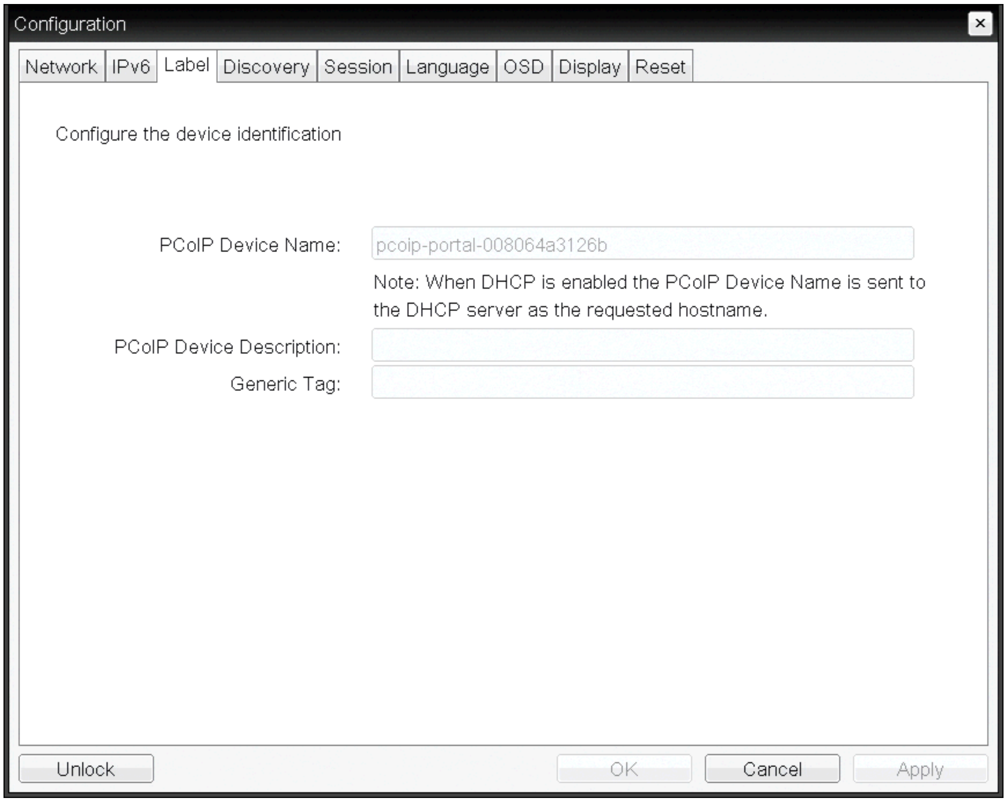
**Figure 5-6: AWI Label Page**

**Table 5-10: AWI Label Page Parameters**

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

## 5.3.2 OSD: Label Settings

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



Configure the device identification

PCoIP Device Name: pcoip-portal-008064a3126b

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

PCoIP Device Description:

Generic Tag:

**Figure 5-7: OSD Label Page**

**Table 5-11: OSD Label Page Parameters**

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

| Parameter | Description |
|---|---|
| | administrator use only. |

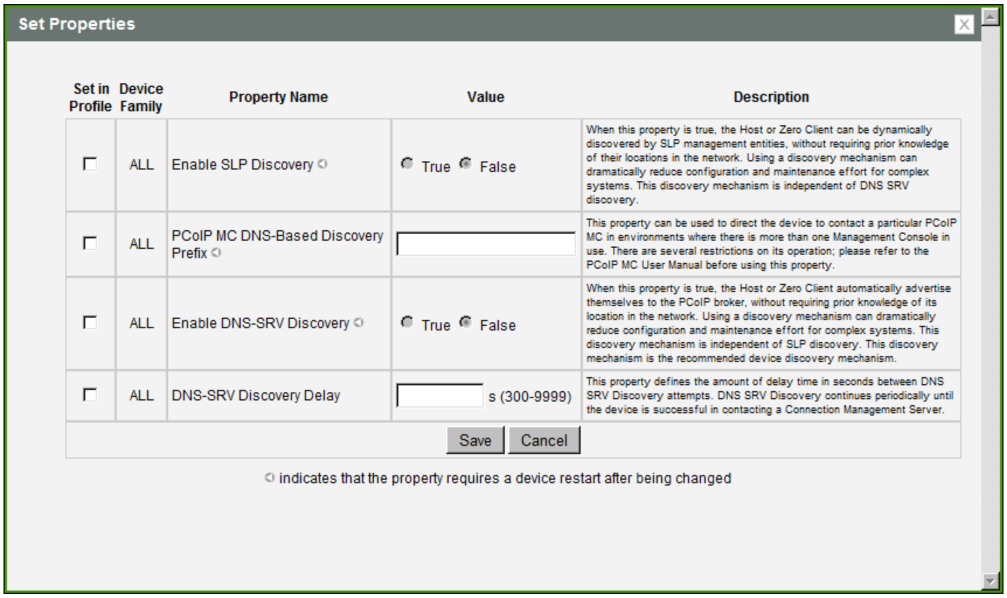
# 5.4 Configuring Device Discovery

## 5.4.1 MC: Discovery Settings

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

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, DNS-SRV discovery is recommended.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable SLP Discovery ◌ | ○ True ● False | When this property is true, the Host or Zero Client can be dynamically discovered by SLP management entities, without requiring prior knowledge of their locations in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems. This discovery mechanism is independent of DNS SRV discovery. |
| □ | ALL | PCoIP MC DNS-Based Discovery Prefix ◌ | | This property can be used to direct the device to contact a particular PCoIP MC in environments where there is more than one Management Console in use. There are several restrictions on its operation; please refer to the PCoIP MC User Manual before using this property. |
| □ | ALL | Enable DNS-SRV Discovery ◌ | ○ True ● False | When this property is true, the Host or Zero Client automatically advertise themselves to the PCoIP broker, without requiring prior knowledge of its location in the network. Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems. This discovery mechanism is independent of SLP discovery. This discovery mechanism is the recommended device discovery mechanism. |
| □ | ALL | DNS-SRV Discovery Delay | s (300-9999) | This property defines the amount of delay time in seconds between DNS SRV Discovery attempts. DNS SRV Discovery continues periodically until the device is successful in contacting a Connection Management Server. |

◌ indicates that the property requires a device restart after being changed

Figure 5-8: MC Discovery Configuration

Table 5-12: MC Discovery Configuration Parameters

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

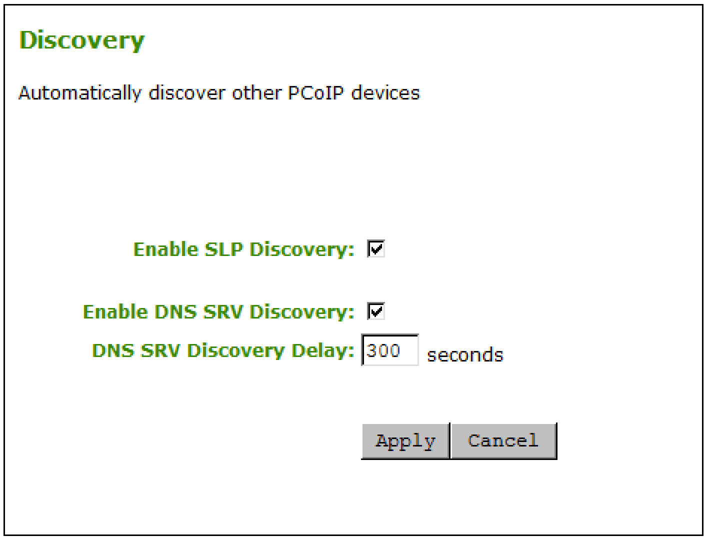
| Parameter | Description |
|---|---|
| | Note: This property requires a device restart after being changed. |
| PCoIP MC DNS-Based Discovery Prefix | Use this property to direct the device to contact a particular PCoIP MC in environments where there is more than one Management Console in use. There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

### 5.4.2 AWI: Discovery Settings

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

You can display this page for the host or client from the **Configuration** > **Discovery** menu.

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, DNS-SRV discovery is recommended.



Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery: ☑

Enable DNS SRV Discovery: ☑

DNS SRV Discovery Delay: 300 seconds

**Figure 5-9: AWI Discovery Page**

**Table 5-13: AWI Discovery Page Parameters**

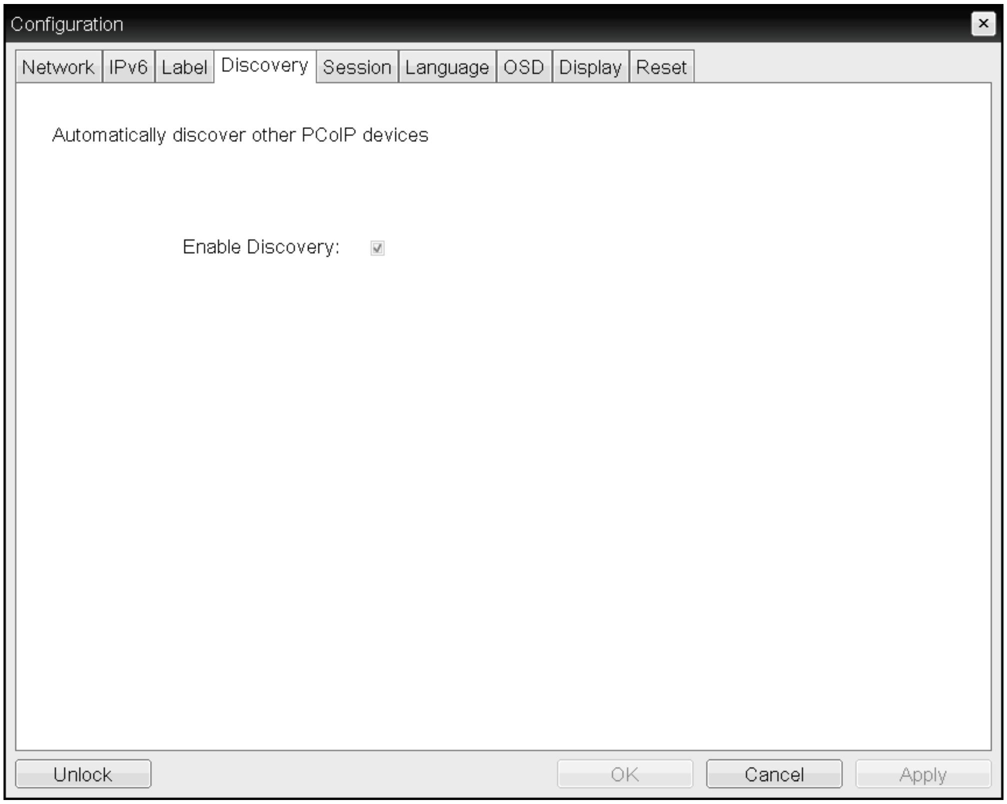
| Parameter | Description |
|---|---|
| Enable SLP Discovery | When enabled, hosts and clients can be dynamically discovered by SLP management entities. |
| Enable DNS-SRV Discovery | When enabled:<br>• Hosts and clients automatically advertise themselves to a connection broker without requiring prior knowledge of its location in the network.<br>• The host or client tries to download and use the DNS SRV record from the DNS server.<br>For more information about this discovery mechanism, see the "PCoIP Management Console User Manual" (TER0812002).<br>Note: The **Enable DNS SRV Discovery** option configures the discovery for connection brokers but does not affect the DNS SRV functionality for the PCoIP Management Console. |
| DNS-SRV Discovery Delay | Configures the amount of delay time in seconds between the DNS SRV discovery attempts for connection brokers and the Management Console. DNS SRV discovery continues periodically until the device successfully contacts a connection management server.<br>Note: Although the **Enable DNS SRV** option does not affect the DNS SRV functionality for the PCoIP Management Console, the DNS SRV Discovery Delay is used for the PCoIP Management Console. When DNS SRV records are not installed, we recommend you set the delay to the maximum value of “9999”. This minimizes attempts by the host or client to contact the PCoIP Management Console. |

### 5.4.3 OSD: Discovery Settings

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

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

Note: SLP discovery mechanism requires all PCoIP devices and the MC to reside on the same network subnet. For SLP discovery to work across subnets, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, DNS-SRV discovery is recommended. You can configure this from the AWI **Discovery** page or the MC **Discovery Configuration** page.



Automatically discover other PCoIP devices

Enable Discovery: ☑

**Figure 5-10: OSD Discovery Page**

**Table 5-14: OSD Discovery Page Parameter**

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

# 5.5 Configuring SNMP

## 5.5.1 MC: Help for SNMP Settings

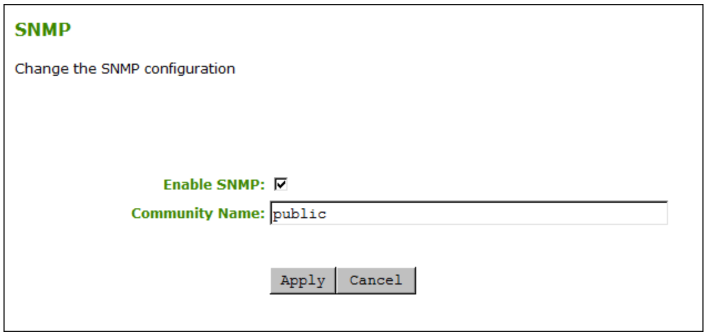
SNMP settings for the Management Console are located on the MC's Network Configuration page.

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

## 5.5.2 AWI: SNMP Settings

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

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



SNMP

Change the SNMP configuration

Enable SNMP: ☑

Community Name: public

**Figure 5-11: AWI SNMP Page**

**Table 5-15: AWI SNMP Page Parameter**

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

# 5.6 Configuring a Session

## 5.6.1 Configuring a Session

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

### Session Connection Types

There are three main session connection types:

- Direct to Host (with option to use SLP host discovery)
- View Connection Server (with various options)
- Connection Management Interface

## Direct to Host Sessions

A Direct to Host session is a direct connection between a zero client and a remote workstation containing a PCoIP host 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 cllients to automatically reconnect to a host when a session is lost.

**Table 5-16: Direct Session Connections**

| Management Tool | Device(s) | Session Connection Options |
|---|---|---|
| MC | All device families | Direct to Host<br>Direct to Host + SLP Host Discovery |
| AWI | Host | Direct from Client |
| | Client | Direct to Host<br>Direct to Host + SLP Host Discovery |
| OSD | Client | Direct to Host<br>Direct to Host + SLP Host Discovery |

## VMware View Virtual Desktop Connections

A VMware View session is a connection between a zero client and a VMware View virtual desktop using VMware View Connection Server as the connection manager (also known as the connection broker). You can configure VMware View sessions in basic mode, Auto-Logon mode, VMware View Kiosk mode, and Imprivata OneSign mode.

**Table 5-17: Direct Session Connections**

| Management Tool | Device(s) | Session Connection Options |
|---|---|---|
| MC | All device families | View Connection Server<br>View Connection Server + Auto-Logon<br>View Connection Server + Kiosk<br>View Connection Server + Imprivata OneSign |

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

### Connection Management Interface Sessions

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

**Table 5-18: Direct Session Connections**

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

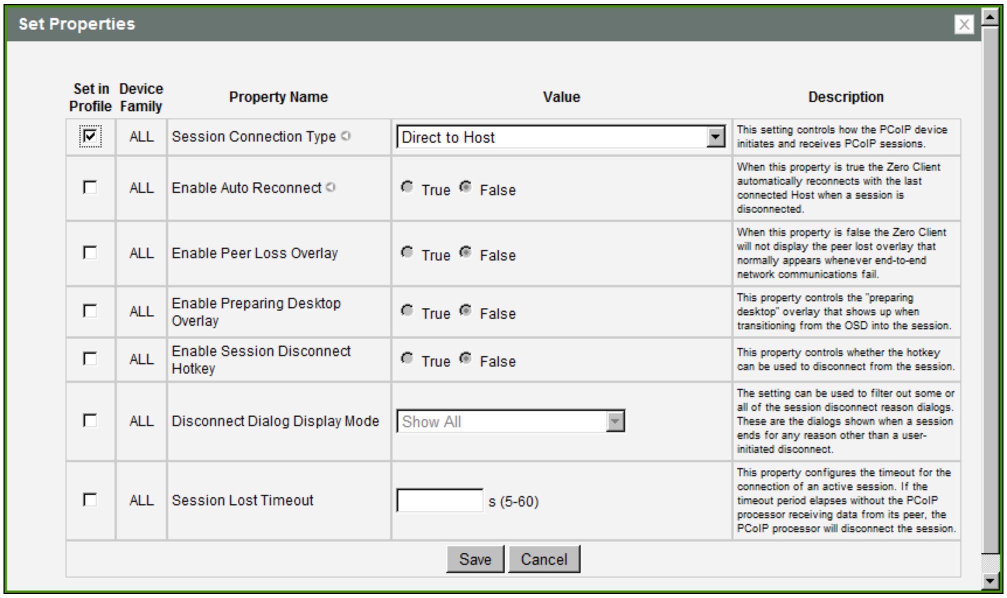
## 5.6.2 MC: Direct to Host Session Settings

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

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

This selection requires a device restart after being changed.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | Direct to Host | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| □ | ALL | Enable Auto Reconnect | ○ True ● False | When this property is true the Zero Client automatically reconnects with the last connected Host when a session is disconnected. |
| □ | ALL | Enable Peer Loss Overlay | ○ True ● False | When this property is false the Zero Client will not display the peer lost overlay that normally appears whenever end-to-end network communications fail. |
| □ | ALL | Enable Preparing Desktop Overlay | ○ True ● False | This property controls the "preparing desktop" overlay that shows up when transitioning from the OSD into the session. |
| □ | ALL | Enable Session Disconnect Hotkey | ○ True ● False | This property controls whether the hotkey can be used to disconnect from the session. |
| □ | ALL | Disconnect Dialog Display Mode | Show All | The setting can be used to filter out some or all of the session disconnect reason dialogs. These are the dialogs shown when a session ends for any reason other than a user-initiated disconnect. |
| □ | ALL | Session Lost Timeout | s (5-60) | This property configures the timeout for the connection of an active session. If the timeout period elapses without the PCoIP processor receiving data from its peer, the PCoIP processor will disconnect the session. |

**Figure 5-12: MC Session Connection Type – Direct to Host**

**Table 5-19: MC Session Configuration Parameters**

| Parameters | Description |
|---|---|
| Enable Auto Reconnect | When enabled, lets the client automatically reconnect with the last connected host when a session is lost.<br>Note: This property requires a device restart after being changed. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you. |

| Parameters | Description |
|---|---|
| | • You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active |

| Parameters | Description |
|---|---|
| | session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

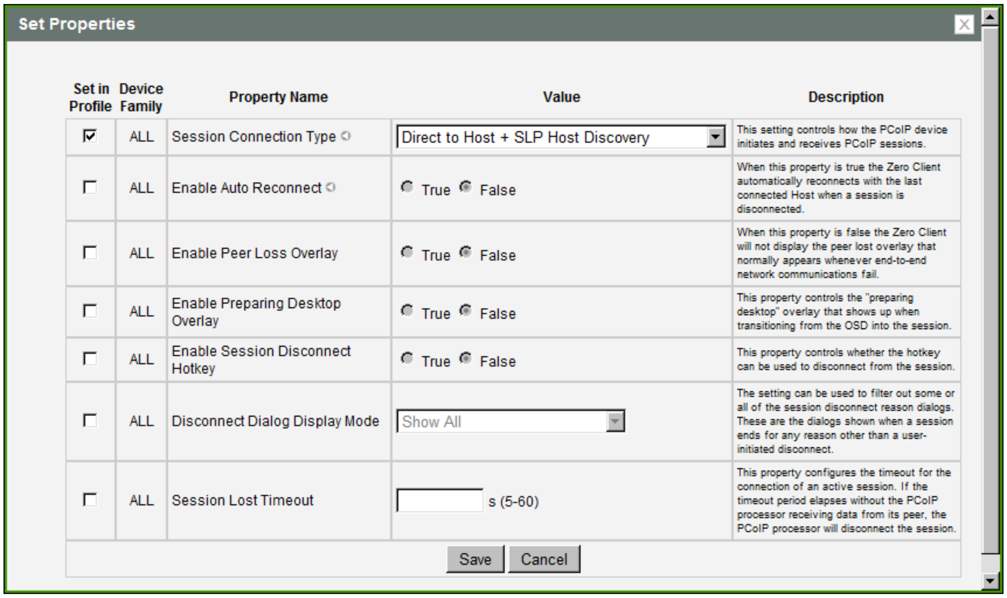
## 5.6.3 MC: Direct to Host Session + SLP Host Discovery Settings

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

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

This selection requires a device restart after being changed.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | Direct to Host + SLP Host Discovery | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| ☐ | ALL | Enable Auto Reconnect | ○ True ● False | When this property is true the Zero Client automatically reconnects with the last connected Host when a session is disconnected. |
| ☐ | ALL | Enable Peer Loss Overlay | ○ True ● False | When this property is false the Zero Client will not display the peer lost overlay that normally appears whenever end-to-end network communications fail. |
| ☐ | ALL | Enable Preparing Desktop Overlay | ○ True ● False | This property controls the "preparing desktop" overlay that shows up when transitioning from the OSD into the session. |
| ☐ | ALL | Enable Session Disconnect Hotkey | ○ True ● False | This property controls whether the hotkey can be used to disconnect from the session. |
| ☐ | ALL | Disconnect Dialog Display Mode | Show All | The setting can be used to filter out some or all of the session disconnect reason dialogs. These are the dialogs shown when a session ends for any reason other than a user-initiated disconnect. |
| ☐ | ALL | Session Lost Timeout | s (5-60) | This property configures the timeout for the connection of an active session. If the timeout period elapses without the PCoIP processor receiving data from its peer, the PCoIP processor will disconnect the session. |

**Figure 5-13: MC Session Connection Type – Direct to Host + SLP Host Discovery**

**Table 5-20: MC Session Configuration Parameters**

| Parameters | Description |
|---|---|
| Enable Auto Reconnect | When enabled, lets the client automatically reconnect with the last connected host when a session is lost.<br>Note: This property requires a device restart after being changed. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also |

| Parameters | Description |
|---|---|
| | appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error |

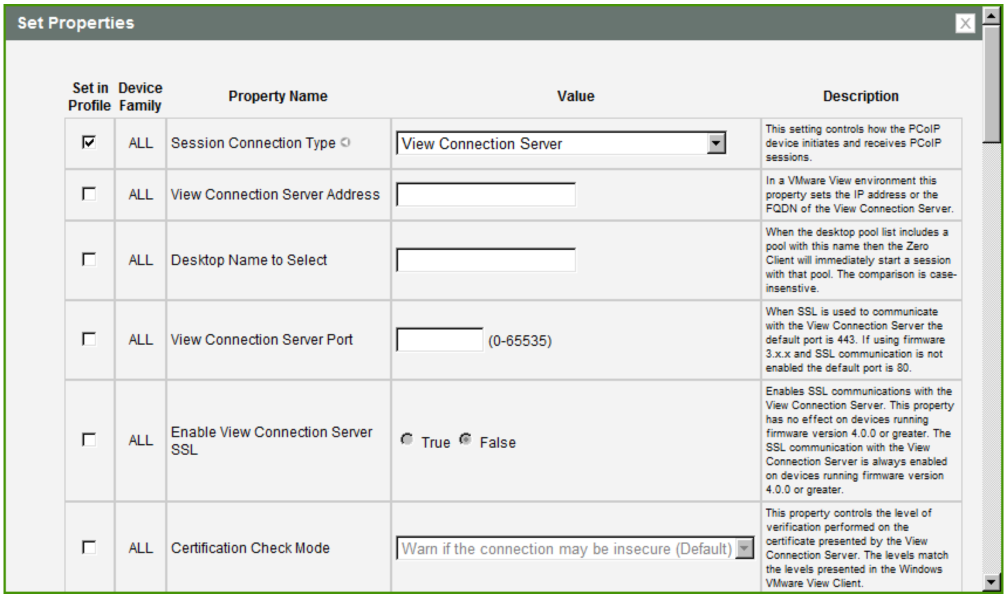
| Parameters | Description |
|---|---|
| | (0x400). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

### 5.6.4 MC: View Connection Server Session Settings

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

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

This selection requires a device restart after being changed.



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | View Connection Server | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| □ | ALL | View Connection Server Address | | In a VMware View environment this property sets the IP address or the FQDN of the View Connection Server. |
| □ | ALL | Desktop Name to Select | | When the desktop pool list includes a pool with this name then the Zero Client will immediately start a session with that pool. The comparison is case-insenstive. |
| □ | ALL | View Connection Server Port | (0-65535) | When SSL is used to communicate with the View Connection Server the default port is 443. If using firmware 3.x.x and SSL communication is not enabled the default port is 80. |
| □ | ALL | Enable View Connection Server SSL | ○ True ● False | Enables SSL communications with the View Connection Server. This property has no effect on devices running firmware version 4.0.0 or greater. The SSL communication with the View Connection Server is always enabled on devices running firmware version 4.0.0 or greater. |
| □ | ALL | Certification Check Mode | Warn if the connection may be insecure (Default) | This property controls the level of verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client. |

**Figure 5-14: MC Session Connection Type – View Connection Server**

**Table 5-21: MC Session Configuration Parameters**

| **Parameter** | **Description** |
|---|---|
| View Connection Server Address | Enter the IP address or the fully qualified domain name (FQDN) of the View Connection Server. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |
| View Connection Server Port | When SSL is used to communicate with the View Connection Server, the default port is 443. If SSL communication is not enabled, the default port is 80.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Enable View Connection Server SSL | When enabled, enables SSL communication with the View Connection Server.<br>Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the View Connection Server is always enabled. |
| Certification Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>• **Warn if the connection may be insecure (Default)**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>• **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not |

| Parameter | Description |
|---|---|
| | installed.<br>- **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections. |
| Certification Check Lockout Mode | Set this property to **Locked** to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Clear Trusted Connection Server Cache | When enabled, clears the trusted View Connection Server cache. |
| Enable View Connection Server Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated. |
| Connection Server Cache Mode | This field determines whether a View 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.<br>- **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.<br>- **Read-only**: Select this option if you want users to select a View Connection Server from a read-only list. |
| Connection Server Cache Entry (1 to 25) | Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a View Connection Server IP address or FQDN to which a user is allowed to connect.<br>- If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new View Connection Server is added to the **Server** drop-down menu whenever the user types in a valid server IP address or FQDN.<br>- If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu. |
| Self Help Link Mode | When enabled, enables the Self Help Link on VMware View user authentication screens. |
| Auto Launch If Only One Desktop | When enabled, users are automatically connected to their virtual desktop after user credentials are entered. |
| Enable Login Username Caching | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Prefer GSC-IS Over PIV Endpoint | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a |

| Parameter | Description |
|---|---|
| | 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. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance. |

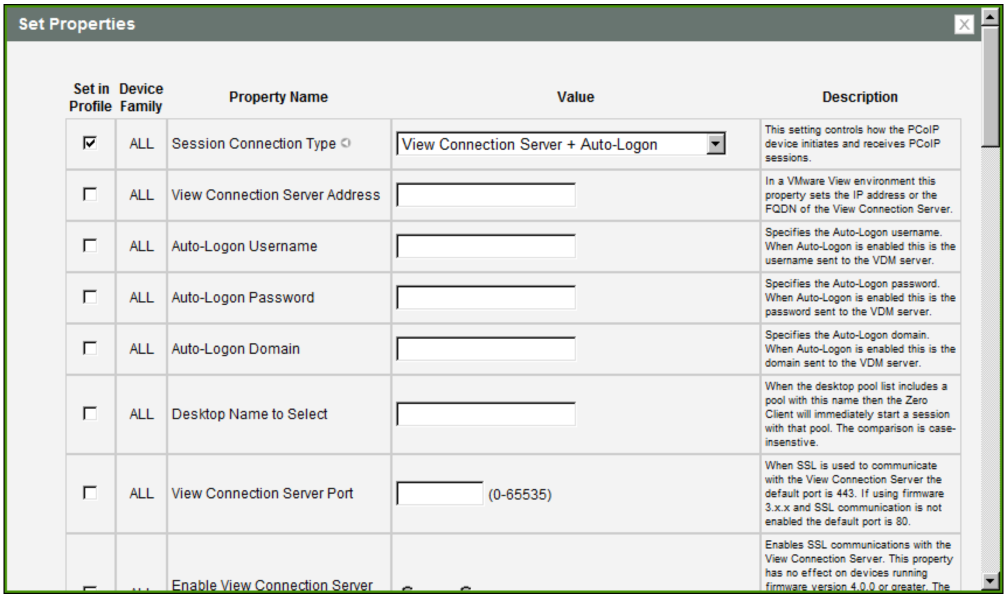
| Parameter | Description |
|---|---|
|  | - You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

### 5.6.5 MC: View Connection Server + Auto-Logon Session Settings

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

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

This selection requires a device restart after being changed.



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | View Connection Server + Auto-Logon | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| ☐ | ALL | View Connection Server Address | | In a VMware View environment this property sets the IP address or the FQDN of the View Connection Server. |
| ☐ | ALL | Auto-Logon Username | | Specifies the Auto-Logon username. When Auto-Logon is enabled this is the username sent to the VDM server. |
| ☐ | ALL | Auto-Logon Password | | Specifies the Auto-Logon password. When Auto-Logon is enabled this is the password sent to the VDM server. |
| ☐ | ALL | Auto-Logon Domain | | Specifies the Auto-Logon domain. When Auto-Logon is enabled this is the domain sent to the VDM server. |
| ☐ | ALL | Desktop Name to Select | | When the desktop pool list includes a pool with this name then the Zero Client will immediately start a session with that pool. The comparison is case-insenstive. |
| ☐ | ALL | View Connection Server Port | (0-65535) | When SSL is used to communicate with the View Connection Server the default port is 443. If using firmware 3.x.x and SSL communication is not enabled the default port is 80. |
| | | Enable View Connection Server | | Enables SSL communications with the View Connection Server. This property has no effect on devices running firmware version 4.0.0 or greater. The |

**Figure 5-15: MC Session Connection Type – View Connection Server + Auto-Logon**

**Table 5-22: MC Session Configuration Parameters**

| Parameter | Description |
|---|---|
| View Connection Server Address | Enter the IP address or the fully qualified domain name (FQDN) of the View Connection Server. |
| Auto-Logon Username | Enter the username to send to the specified View Connection Server. |
| Auto-Logon Password | Enter the password to send to the specified View Connection Server. |
| Auto-Logon Domain | Enter the domain to send to the specified View Connection Server. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |
| View Connection Server Port | When SSL is used to communicate with the View Connection Server, the default port is 443. If SSL communication is not enabled, the default port is 80.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Enable View Connection Server SSL | When enabled, enables SSL communication with the View Connection Server.<br>Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the View Connection Server is always enabled. |
| Certification Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server: |

| Parameter | Description |
|---|---|
| | • **Warn if the connection may be insecure (Default)**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>• **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed.<br>• **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections. |
| Certification Check Lockout Mode | Set this property to **Locked** to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Clear Trusted Connection Server Cache | When enabled, clears the trusted View Connection Server cache. |
| Enable View Connection Server Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated. |
| Connection Server Cache Mode | This field determines whether a View 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.<br>• **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.<br>• **Read-only**: Select this option if you want users to select a View Connection Server from a read-only list. |
| Connection Server Cache Entry (1 to 25) | Enable the desired number of fields (up to 25) that may appear in the cache on a user's OSD **Connect** page, and for each one, enter a View Connection Server IP address or FQDN to which a user is allowed to connect.<br>• If **Last servers used** is selected in the **Connection Server Cache Mode** field, a new View Connection Server is added to the **Server** drop-down menu whenever the user types in a valid server IP address or FQDN.<br>• If **Read-only** is selected, a user can only select a server from a read-only list in the **Server** drop-down menu. |
| Auto Launch If Only One Desktop | When enabled, users are automatically connected to their virtual desktop after user credentials are entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also |

| Parameter | Description |
|---|---|
| | appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error |

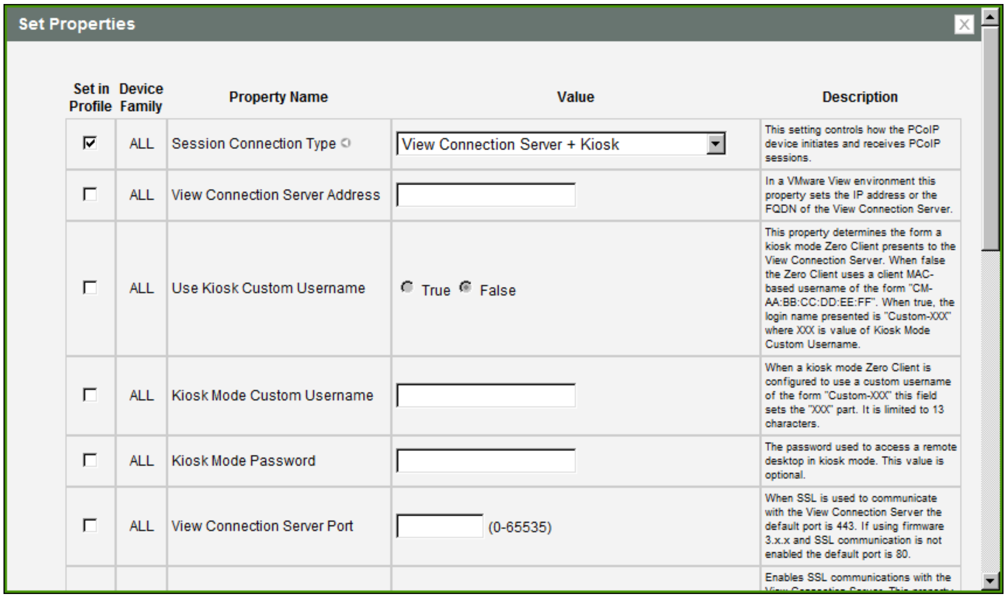
| Parameter | Description |
|---|---|
| | (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

## 5.6.6 MC: View Connection Server + Kiosk Session Settings

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

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

This selection requires a device restart after being changed.



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | View Connection Server + Kiosk | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| □ | ALL | View Connection Server Address | | In a VMware View environment this property sets the IP address or the FQDN of the View Connection Server. |
| □ | ALL | Use Kiosk Custom Username | ○ True ● False | This property determines the form a kiosk mode Zero Client presents to the View Connection Server. When false the Zero Client uses a client MAC-based username of the form "CM-AA:BB:CC:DD:EE:FF". When true, the login name presented is "Custom-XXX" where XXX is value of Kiosk Mode Custom Username. |
| □ | ALL | Kiosk Mode Custom Username | | When a kiosk mode Zero Client is configured to use a custom username of the form "Custom-XXX" this field sets the "XXX" part. It is limited to 13 characters. |
| □ | ALL | Kiosk Mode Password | | The password used to access a remote desktop in kiosk mode. This value is optional. |
| □ | ALL | View Connection Server Port | (0-65535) | When SSL is used to communicate with the View Connection Server the default port is 443. If using firmware 3.x.x and SSL communication is not enabled the default port is 80. |
| | | | | Enables SSL communications with the |

**Figure 5-16: MC Session Connection Type – View Connection Server + Kiosk**

**Table 5-23: MC Session Configuration Parameters**

| Parameter | Description |
|---|---|
| View Connection Server Address | Enter the IP address or the fully qualified domain name (FQDN) of the View Connection Server. |
| Use Kiosk Custom Username | When enabled, the login name is presented as "Custom-<*XXX*>", where "*XXX*" is the value of the **Kiosk Mode Custom Username**. When disabled, clients use the MAC-based username of the form "CM-AA:BB:CC:DD:EE:FF." |
| Kiosk Mode Custom Username | When **Use Kiosk Custom Username** is configured to use a custom username of the form "Custom-<*XXX*>", enter the value for the "*XXX*" component. This field is limited to 13 characters. |
| Kiosk Mode Password | Enter the password to use to access a virtual desktop in Kiosk mode.<br>Note: This setting is optional. |
| View Connection Server Port | When SSL is used to communicate with the View Connection Server, the default port is 443. If SSL communication is not enabled, the default port is 80.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Enable View Connection Server SSL | When enabled, enables SSL communication with the View Connection Server.<br>Note: This property has no effect on devices running firmware version 4.0.0 or greater because SSL communication with the View Connection Server is always enabled. |

| Parameter | Description |
|---|---|
| Certification Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>- **Warn if the connection may be insecure (Default)**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>- **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed.<br>- **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections. |
| Certification Check Lockout Mode | Set this property to **Locked** to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Clear Trusted Connection Server Cache | When enabled, clears the trusted View Connection Server cache. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Enable Peer Loss Overlay | When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>- You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>- You have been disconnected because an administrator disconnected you.<br>- You have been disconnected because you logged in from another location.<br>- You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the |

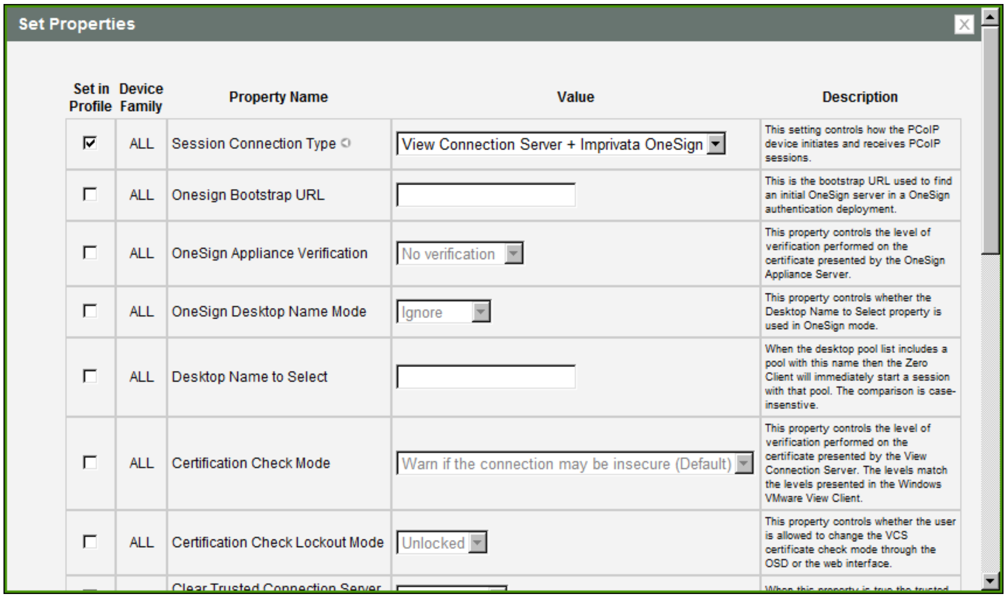
| Parameter | Description |
|---|---|
| | session:<br>● You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>● You have been disconnected.<br>● Unable to connect (0x1001). Please contact your IT administrator.<br>● Unable to connect (0x1002). Please contact your IT administrator.<br>● Session closed remotely.<br>● Session closed remotely (unknown cause).<br>● You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

### 5.6.7 MC: View Connection Server + Imprivata OneSign Session Settings

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

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

This selection requires a device restart after being changed.



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | View Connection Server + Imprivata OneSign | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| □ | ALL | Onesign Bootstrap URL | | This is the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment. |
| □ | ALL | OneSign Appliance Verification | No verification | This property controls the level of verification performed on the certificate presented by the OneSign Appliance Server. |
| □ | ALL | OneSign Desktop Name Mode | Ignore | This property controls whether the Desktop Name to Select property is used in OneSign mode. |
| □ | ALL | Desktop Name to Select | | When the desktop pool list includes a pool with this name then the Zero Client will immediately start a session with that pool. The comparison is case-insenstive. |
| □ | ALL | Certification Check Mode | Warn if the connection may be insecure (Default) | This property controls the level of verification performed on the certificate presented by the View Connection Server. The levels match the levels presented in the Windows VMware View Client. |
| □ | ALL | Certification Check Lockout Mode | Unlocked | This property controls whether the user is allowed to change the VCS certificate check mode through the OSD or the web interface. |
| | | Clear Trusted Connection Server | | When this property is true the trusted |

**Figure 5-17: MC Session Connection Type – View Connection Server + Imprivata OneSign**

**Table 5-24: MC Session Configuration Parameters**

| Parameter | Description |
|---|---|
| View Connection Server Address | Enter the IP address or the fully qualified domain name (FQDN) of the View Connection Server. |
| Onesign Bootstrap URL | Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment. |
| Onesign Appliance Verification | Select the level of verification performed on the certificate presented by the OneSign appliance server:<br>• **No verification: Connect to any appliance**<br>• **Full verification: Only connect to appliances with verified certificates** |
| Onesign Desktop Name Mode | Select whether the **Desktop Name to Select** property is used in OneSign Mode: |

| Parameter | Description |
|---|---|
| | - **Ignore**<br>- **Use If Set** |
| Desktop Name to Select | Enter the desktop name. When the desktop pool list includes a pool with this name, the client will immediately start a session with that pool.<br>Note: This field is case-insensitive. |
| Certification Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>- **Warn if the connection may be insecure (Default)**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>- **Reject the unverifiable connection (Secure)**: Configure the client to reject the connection if a trusted, valid certificate is not installed.<br>- **Allow the unverifiable connection (Not Secure)**: Configure the client to allow all connections. |
| Certification Check Lockout Mode | Set this property to **Locked** to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Clear Trusted Connection Server Cache | When enabled, clears the trusted View Connection Server cache. |
| Enable Login Username Caching | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Prefer GSC-IS Over PIV Endpoint | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing | When enabled, the "Preparing Desktop" overlay appears on the |

| Parameter | Description |
|---|---|
| Desktop Overlay | display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance. |

| Parameter | Description |
|---|---|
| | • You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

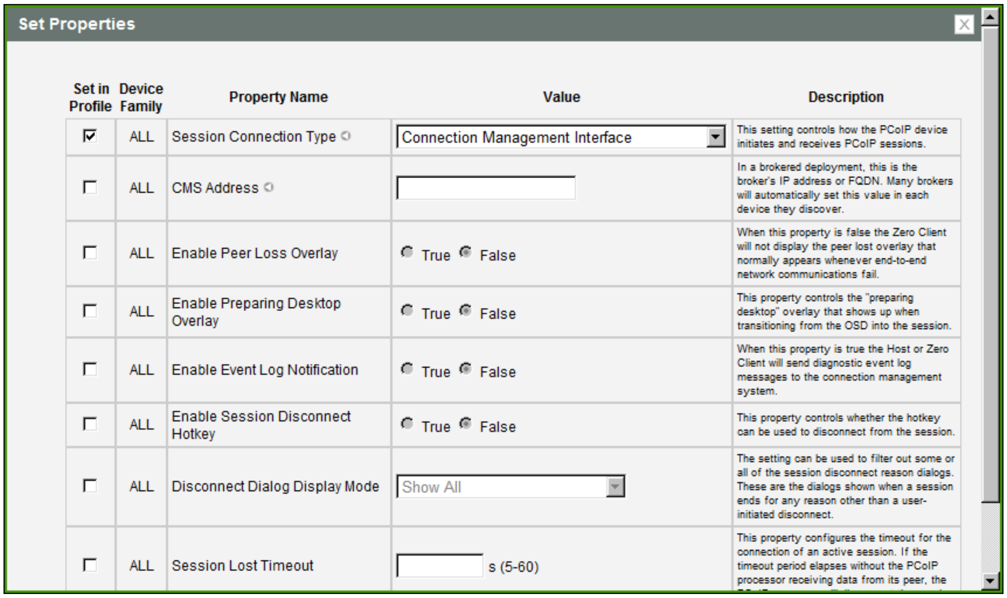
### 5.6.8 MC: Connection Management Interface Settings

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

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

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

This selection requires a device restart after being changed.



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☑ | ALL | Session Connection Type | Connection Management Interface | This setting controls how the PCoIP device initiates and receives PCoIP sessions. |
| □ | ALL | CMS Address | | In a brokered deployment, this is the broker's IP address or FQDN. Many brokers will automatically set this value in each device they discover. |
| □ | ALL | Enable Peer Loss Overlay | ○ True ● False | When this property is false the Zero Client will not display the peer lost overlay that normally appears whenever end-to-end network communications fail. |
| □ | ALL | Enable Preparing Desktop Overlay | ○ True ● False | This property controls the "preparing desktop" overlay that shows up when transitioning from the OSD into the session. |
| □ | ALL | Enable Event Log Notification | ○ True ● False | When this property is true the Host or Zero Client will send diagnostic event log messages to the connection management system. |
| □ | ALL | Enable Session Disconnect Hotkey | ○ True ● False | This property controls whether the hotkey can be used to disconnect from the session. |
| □ | ALL | Disconnect Dialog Display Mode | Show All | The setting can be used to filter out some or all of the session disconnect reason dialogs. These are the dialogs shown when a session ends for any reason other than a user-initiated disconnect. |
| □ | ALL | Session Lost Timeout | s (5-60) | This property configures the timeout for the connection of an active session. If the timeout period elapses without the PCoIP processor receiving data from its peer, the |

**Figure 5-18: MC Session Connection Type – Connection Management Interface**

**Table 5-25: MC Session Configuration Parameters**

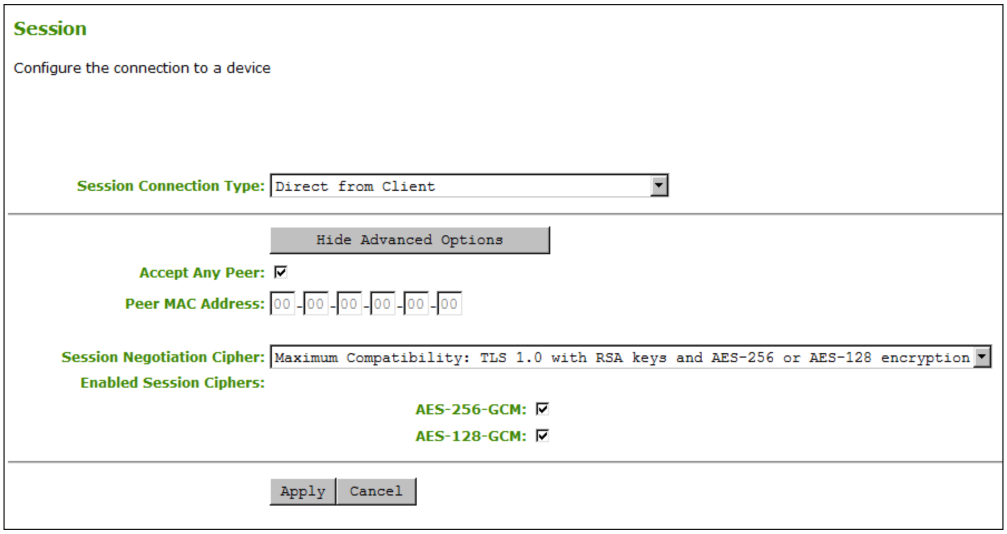
| **Parameter** | **Description** |
|---|---|
| CMS Address | Enter the IP address or fully qualified domain name (FQDN) of the connection manager.<br>Note: Many connection managers will automatically set this value in each device they discover. |
| Enable Peer Loss Overlay | When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Dialog Display Mode | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you. |

| Parameter | Description |
|---|---|
| | • You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |
| Session Lost Timeout | Enter the timeout (in seconds) for the connection of the active |

| Parameter | Description |
|---|---|
| | session. The valid timeout range for this field is 5 to 60 seconds. The session will be disconnected when this timeout period expires. |

## 5.6.9 AWI Host: Direct from Client Session Settings

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



Session

Configure the connection to a device

Session Connection Type: Direct from Client

Accept Any Peer: ☑

Peer MAC Address: 00-00-00-00-00-00

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

**Figure 5-19: AWI Session Connection Type – Direct from Client**

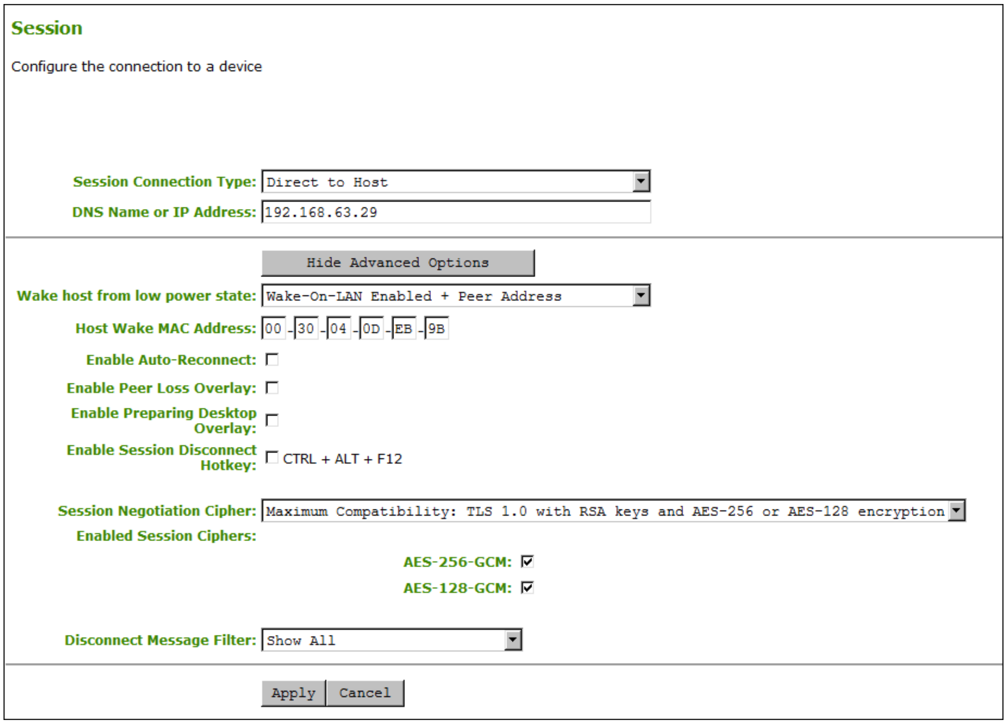
**Table 5-26: AWI Session Page Parameters**

| Parameters | Description |
|---|---|
| Accept Any Peer | When enabled, the host accepts connections from any client. When disabled, you must specify the MAC address of the peer you want the host to accept. |
| Peer MAC Address | Enter the MAC address of the client that is allowed to connect to the host. If the **Accept Any Peer** option is enabled, this field is not required and not editable. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled. |

| Parameters | Description |
|---|---|
| | ● **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>● **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>● **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>● Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>● VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>● VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |

## 5.6.10 AWI Client: Direct to Host Session Settings

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



**Session**

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 192.168.63.29

Wake host from low power state: Wake-On-LAN Enabled + Peer Address

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

Enable Auto-Reconnect: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

Figure 5-20: AWI Session Connection Type – Direct to Host

### Table 5-27: AWI Session Page Parameters

| Parameters | Description |
|---|---|
| DNS Name or IP Address | Enter the IP address or DNS name for the host. |
| Wake host from low power state | Enable or disable the client to automatically wake up the host when the user presses the client's remote PC button or clicks the **Connect** button on the **Connect** window.<br>• **Wake-On-LAN Disabled**: When selected, disables the wake up feature. This option is selected by default.<br>• **Wake-On-LAN Enabled + Peer Address**: When selected, enables the wake-up feature and displays the **Host Wake MAC Address** field so you can enter the host's MAC address. Use this option when the client and host are connected to the same network.<br>• **Wake-On-LAN Enabled + Custom Address**: When selected, enables the wake-up feature and displays the **Host Wake MAC Address** and **Host Wake IP Address** fields so you can enter both addresses for the host. Use this option when the host is connected to a different network from the client.<br>Note:<br>• The feature only works with hardware hosts. It does not work with software hosts as they cannot be put into a low power state.<br>• The hardware host must be able to support waking from low |

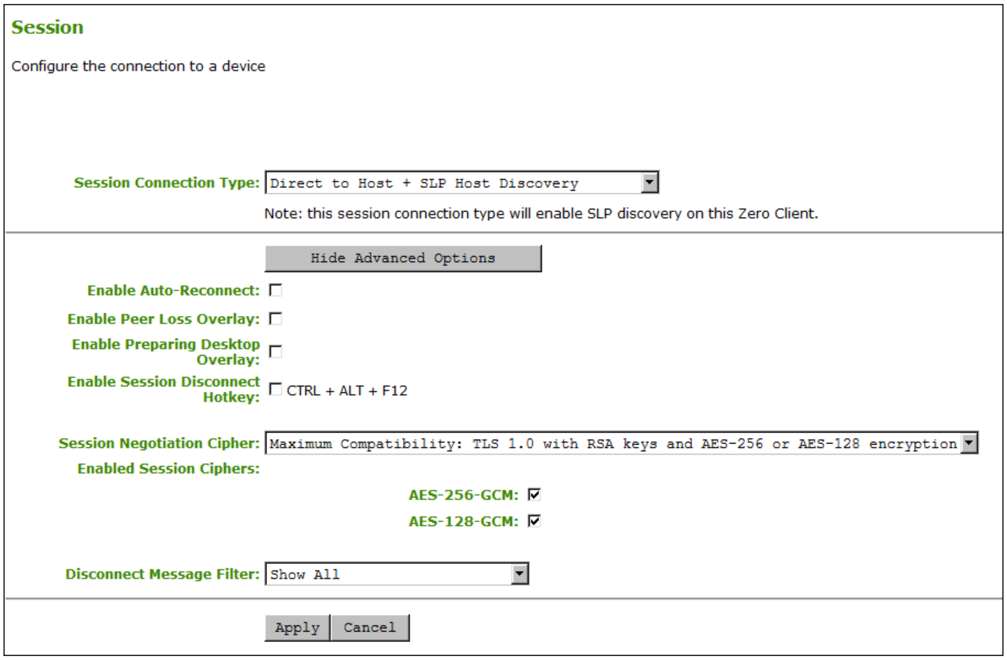
| Parameters | Description |
|---|---|
| | power state (off/hibernate/sleep) when it receives a wake-on-LAN packet. |
| Host Wake MAC Address | Enter the host's MAC address to complete the host wake up configuration when **Wake-On-LAN Enabled + Peer Address** or **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this MAC address to wake the host computer from a low power state. |
| Host Wake IP Address | Enter the host's IP address to complete the host wake up configuration when **Wake-On-LAN Enabled + Custom Address** is selected. The client will send a "magic packet" to this IP address to wake the host computer from a low power state. |
| Enable Auto-Reconnect | When enabled, lets the client automatically reconnect with the last connected host when a session is lost. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation |

| Parameters | Description |
|---|---|
| | Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>- **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>- **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>- Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>- VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>- VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>- You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>- You have been disconnected because an administrator disconnected you.<br>- You have been disconnected because you logged in from another location.<br>- You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>- You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>- You have been disconnected.<br>- Unable to connect (0x1001). Please contact your IT administrator.<br>- Unable to connect (0x1002). Please contact your IT administrator.<br>- Session closed remotely.<br>- Session closed remotely (unknown cause). |

| Parameters | Description |
|---|---|
| | • You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

## 5.6.11 AWI Client: Direct to Host + SLP Host Discovery Session Settings

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



Session

Configure the connection to a device

Session Connection Type: Direct to Host + SLP Host Discovery

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

Enable Auto-Reconnect: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

Figure 5-21: AWI Session Connection Type – Direct to Host + SLP Host Discovery

### Table 5-28: AWI Session Page Parameters

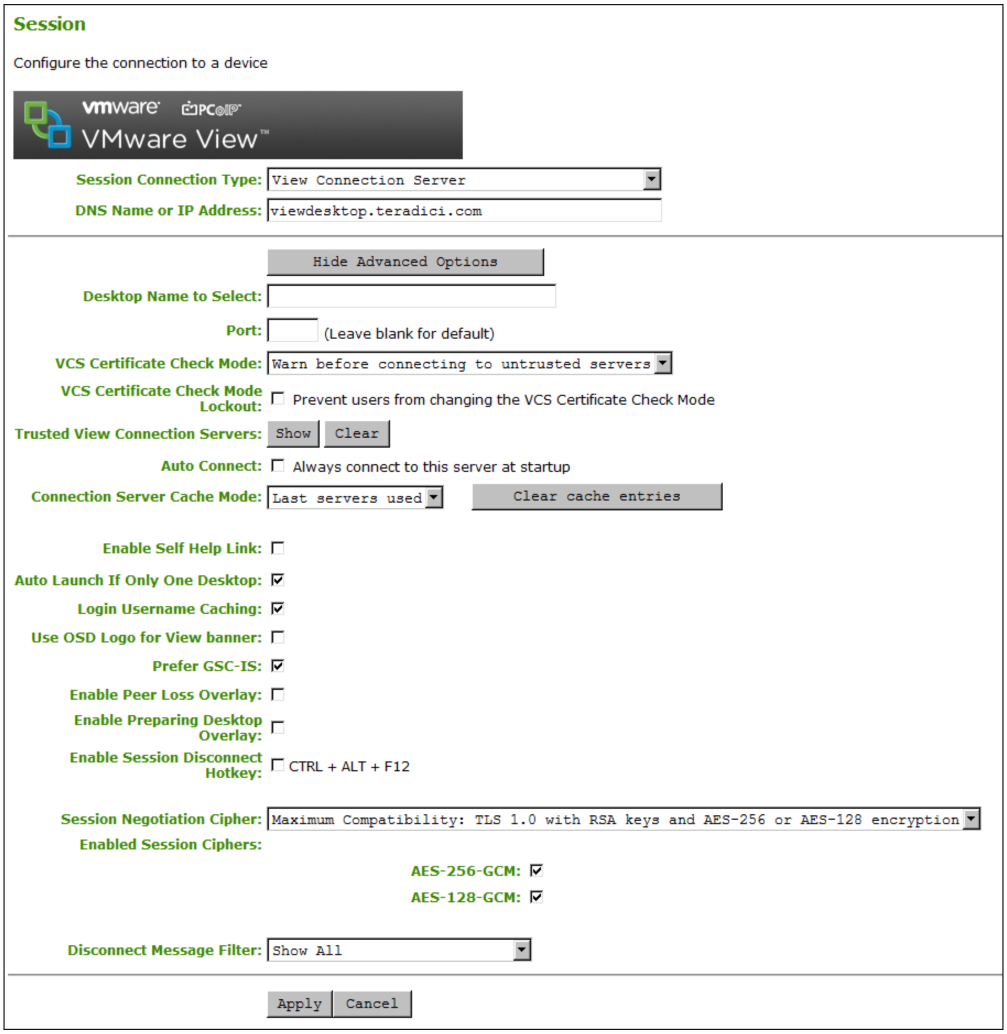
| Parameters | Description |
|---|---|
| Enable Auto-Reconnect | When enabled, lets the client automatically reconnect with the last connected host when a session is lost. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |

| Parameters | Description |
|---|---|
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>- **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>- **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>- **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>- **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>- **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>- Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>- VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>- VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>- You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>- You have been disconnected because an administrator disconnected you.<br>- You have been disconnected because you logged in from another location. |

| Parameters | Description |
|---|---|
|  | • You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

## 5.6.12 AWI Client: View Connection Server Session Settings

Select the **View Connection Server** session connection type from the **Configuration > Session** page to configure the client to use a VMware View Connection Server to connect to a virtual desktop.


Session

Configure the connection to a device

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

Desktop Name to Select:
Port: (Leave blank for default)
VCS Certificate Check Mode: Warn before connecting to untrusted servers
VCS Certificate Check Mode Lockout: □ Prevent users from changing the VCS Certificate Check Mode
Trusted View Connection Servers: Show Clear
Auto Connect: □ Always connect to this server at startup
Connection Server Cache Mode: Last servers used Clear cache entries

Enable Self Help Link: □
Auto Launch If Only One Desktop: ☑
Login Username Caching: ☑
Use OSD Logo for View banner: □
Prefer GSC-IS: ☑
Enable Peer Loss Overlay: □
Enable Preparing Desktop Overlay: □
Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption
Enabled Session Ciphers:
AES-256-GCM: ☑
AES-128-GCM: ☑

Disconnect Message Filter: Show All

**Figure 5-22: AWI Session Connection Type – View Connection Server**

**Table 5-29: AWI Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |

| Parameter | Description |
|---|---|
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| VCS Certificate Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>• **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.)<br>• **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>• **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.) |
| VCS Certificate Check Mode Lockout | Enable to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Trusted View Connection Servers | Click the **Show** button to display VMware View Connection Servers for which the client has received a valid certificate.<br>Click the **Clear** button to clear this cache. |
| Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated.<br>Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect. |
| Connection Server Cache Mode | This field determines whether a View 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.<br>• **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.<br>• **Read-only**: Select this option if you want users to select a View Connection Server from a read-only list.<br>Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers. |
| Enable Self Help Link | See Enabling the Self Help Link for details. |
| Auto Launch If Only One Desktop | When enabled, users are automatically connected to their virtual desktop after user credentials are entered.<br>Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops. |

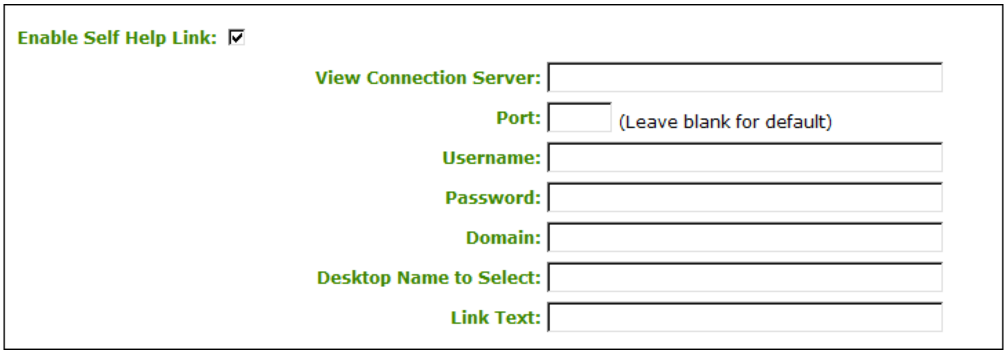
| Parameter | Description |
|---|---|
| Login Username Caching | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Prefer GSC-IS | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when |

| Parameter | Description |
|---|---|
| | connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>• **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>• **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>• Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>• VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>• VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error |

| Parameter | Description |
|---|---|
| | (0x201). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>- You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

## Enabling the Self Help Link

The **Self Help Link** option lets you configure a self-help link for users that will appear on the **Connect** window. Configuring the logon details ensures that a user is automatically logged into the virtual machine when the user clicks the self-help link.



Enable Self Help Link: ☑

View Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Desktop Name to Select:

Link Text:

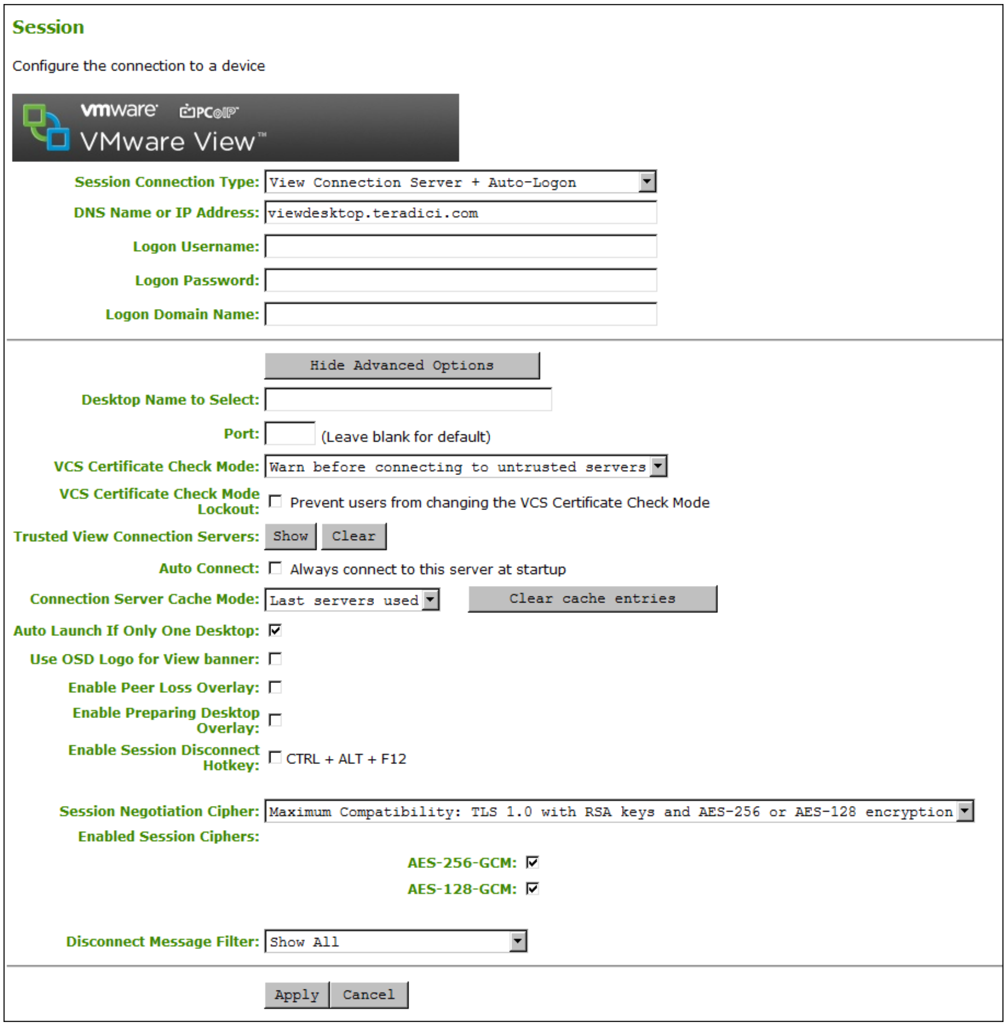
**Figure 5-23: Enable Self Help Link Options**

When you enable this field, the following options appear:

| Parameter | Description |
|---|---|
| View Connection Server | Enter the name of the View Connection Server hosting the self-help virtual machine. |
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Username | To password protect the virtual machine for the self-help link, enter a username in this field. |
| Password | To password protect the virtual machine for the self-help link, enter a password in this field. |
| Domain | Enter the domain name used by the virtual machine for the self-help link. |
| Desktop Name to Select | Enter the pool/desktop name used by the virtual machine for the self-help link. |
| Link Text | Enter the text that you want to appear as hyperlinked text on the **Connect** window |

### 5.6.13 AWI Client: View Connection Server + Auto-Logon Session Settings

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



**Session**

Configure the connection to a device

Session Connection Type: View Connection Server + Auto-Logon

DNS Name or IP Address: viewdesktop.teradici.com

Logon Username:

Logon Password:

Logon Domain Name:

Desktop Name to Select:

Port: (Leave blank for default)

VCS Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers: Show Clear

Auto Connect: □ Always connect to this server at startup

Connection Server Cache Mode: Last servers used Clear cache entries

Auto Launch If Only One Desktop: ☑

Use OSD Logo for View banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

**Figure 5-24: AWI Session Connection Type – View Connection Server + Auto-Logon**

**Table 5-30: AWI Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Logon Username | Enter the username for the client. |
| Logon Password | Enter the password for the client. |
| Logon Domain Name | Enter the domain name for the client. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |

| Parameter | Description |
|---|---|
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| VCS Certificate Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>• **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.)<br>• **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>• **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.) |
| VCS Certificate Check Mode Lockout | Enable to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Trusted View Connection Servers | Click the **Show** button to display VMware View Connection Servers for which the client has received a valid certificate.<br>Click the **Clear** button to clear this cache. |
| Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated.<br>Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect. |
| Connection Server Cache Mode | This field determines whether a View 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.<br>• **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.<br>• **Read-only**: Select this option if you want users to select a View Connection Server from a read-only list.<br>Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers. |
| Enable Self Help Link | See Enabling the Self Help Link for details. |
| Auto Launch If Only One Desktop | When enabled, users are automatically connected to their virtual desktop after user credentials are entered.<br>Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops. |

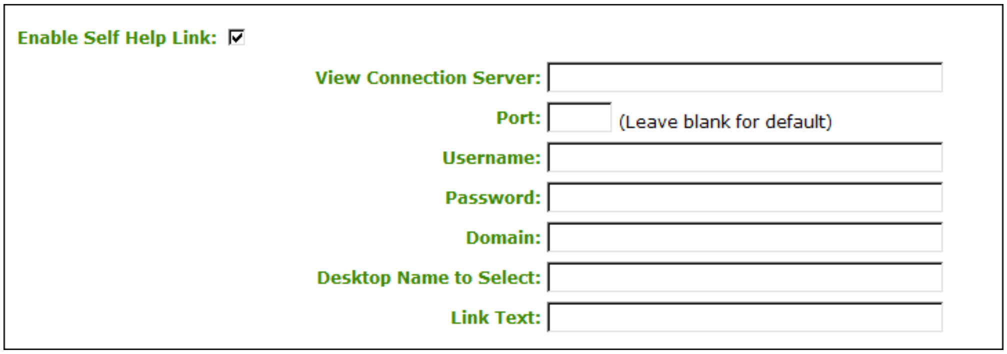
| Parameter | Description |
|---|---|
| Login Username Caching | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Prefer GSC-IS | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when |

| Parameter | Description |
|---|---|
| | connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>• **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>• **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>• Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>• VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>• VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error |

| Parameter | Description |
|---|---|
| | (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

## Enabling the Self Help Link

The **Self Help Link** option lets you configure a self-help link for users that will appear on the **Connect** window. Configuring the logon details ensures that a user is automatically logged into the virtual machine when the user clicks the self-help link.



Enable Self Help Link: ☑

View Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Desktop Name to Select:

Link Text:

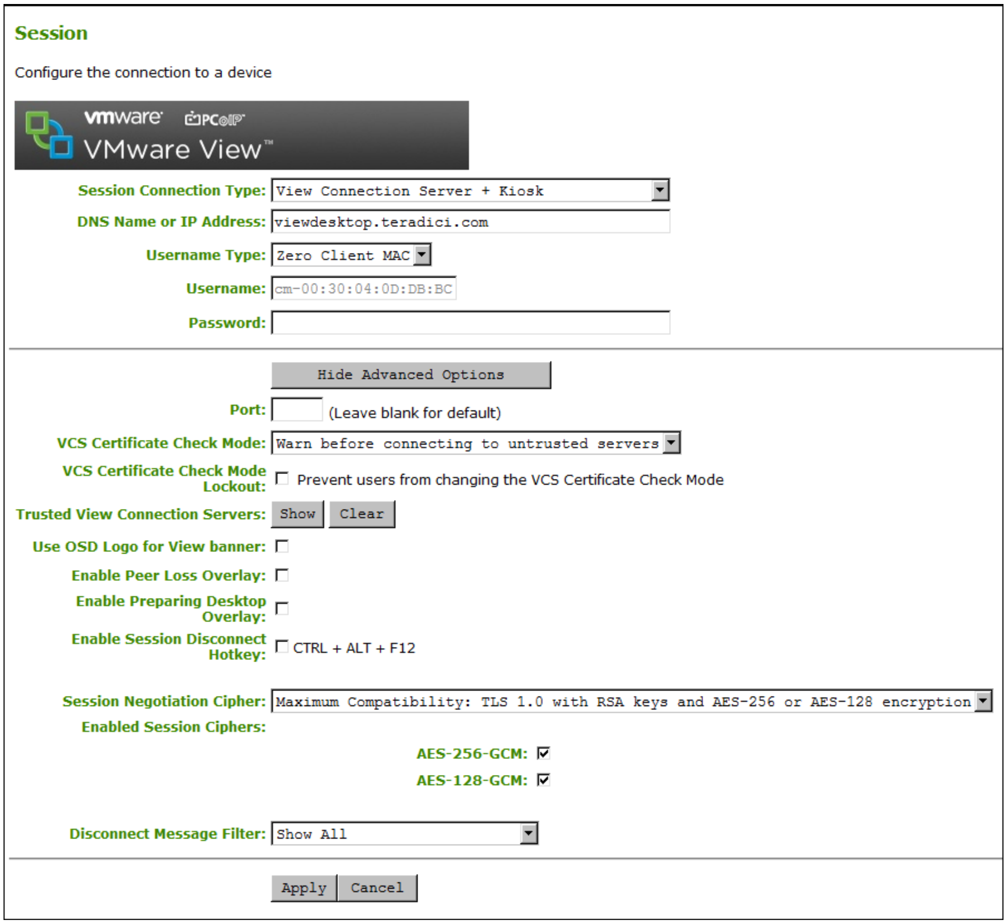
**Figure 5-25: Enable Self Help Link Options**

When you enable this field, the following options appear:

| Parameter | Description |
|---|---|
| View Connection Server | Enter the name of the View Connection Server hosting the self-help virtual machine. |
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Username | To password protect the virtual machine for the self-help link, enter a username in this field. |
| Password | To password protect the virtual machine for the self-help link, enter a password in this field. |
| Domain | Enter the domain name used by the virtual machine for the self-help link. |
| Desktop Name to Select | Enter the pool/desktop name used by the virtual machine for the self-help link. |
| Link Text | Enter the text that you want to appear as hyperlinked text on the **Connect** window |

### 5.6.14 AWI Client: View Connection Server + Kiosk Session Settings

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



**Session**

Configure the connection to a device

Session Connection Type: View Connection Server + Kiosk

DNS Name or IP Address: viewdesktop.teradici.com

Username Type: Zero Client MAC

Username: cm-00:30:04:0D:DB:BC

Password:

Port: (Leave blank for default)

VCS Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers: Show Clear

Use OSD Logo for View banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

**Figure 5-26: AWI Session Connection Type – View Connection Server + Kiosk**

**Table 5-31: AWI Session Page Parameters**

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

| Parameter | Description |
|---|---|
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| VCS Certificate Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>● **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.)<br>● **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>● **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.) |
| VCS Certificate Check Mode Lockout | Enable to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Trusted View Connection Servers | Click the **Show** button to display VMware View Connection Servers for which the client has received a valid certificate.<br>Click the **Clear** button to clear this cache. |
| Connection Server Cache Mode | This field determines whether a View 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.<br>● **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.<br>● **Read-only**: Select this option if you want users to select a View Connection Server from a read-only list.<br>Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing | When enabled, the "Preparing Desktop" overlay appears on the |

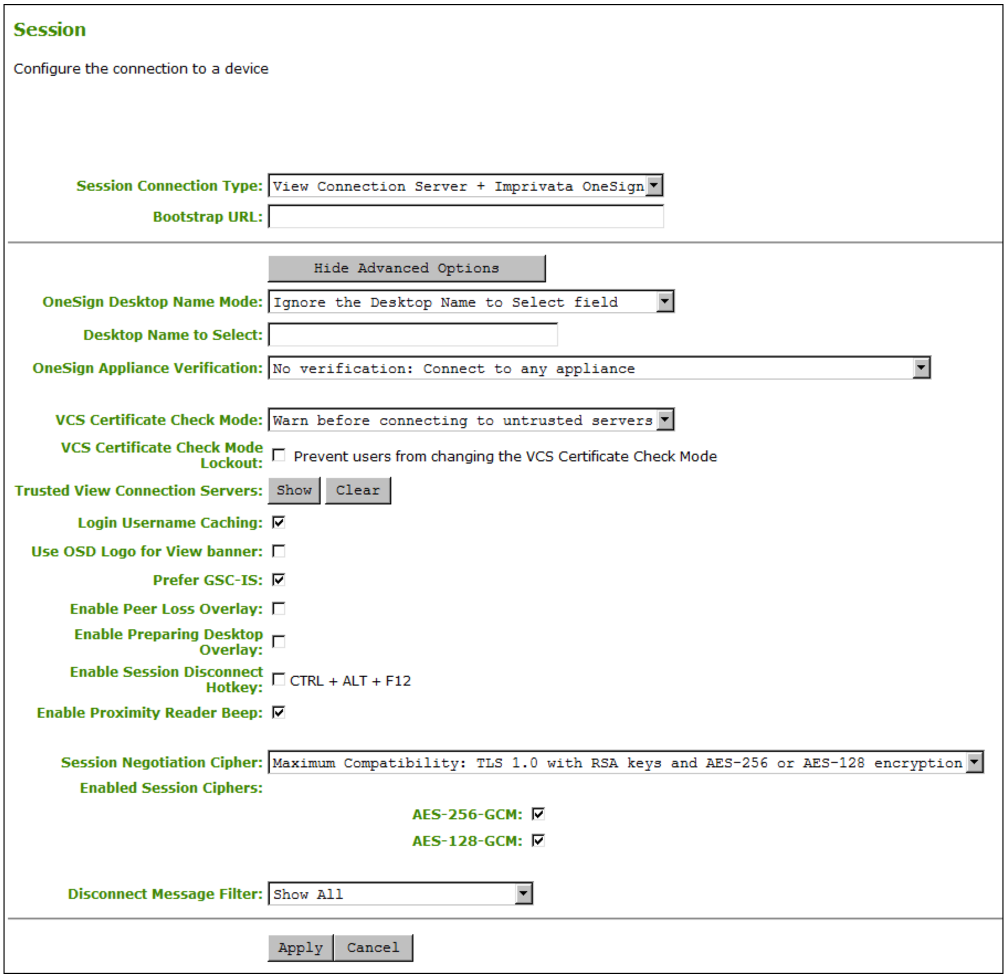
| Parameter | Description |
|---|---|
| Desktop Overlay | display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>● **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>● **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>● **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>● **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>● **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>● Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>● VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>● VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |

| Parameter | Description |
|---|---|
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect |

| Parameter | Description |
|---|---|
| | messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

## 5.6.15 AWI Client: View Connection Server + Imprivata OneSign Session Settings

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



Session

Configure the connection to a device

Session Connection Type: View Connection Server + Imprivata OneSign

Bootstrap URL:

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

Desktop Name to Select:

OneSign Appliance Verification: No verification: Connect to any appliance

VCS Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers:

Login Username Caching: ☑

Use OSD Logo for View banner: ☐

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Enable Session Disconnect Hotkey: ☐ CTRL + ALT + F12

Enable Proximity Reader Beep: ☑

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

**Figure 5-27: AWI Session Connection Type – View Connection Server + Imprivata OneSign**

**Table 5-32: AWI Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Bootstrap URL | Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment. |
| Onesign Desktop Name Mode | Select whether the **Desktop Name to Select** property is used in OneSign Mode:<br>• **Ignore**<br>• **Use If Set** |
| Desktop Name to Select | Enter the desktop name. When the desktop pool list includes a pool with this name, the client will immediately start a session with that pool.<br>Note: This field is case-insensitive. |
| Onesign Appliance Verification | Select the level of verification performed on the certificate presented by the OneSign appliance server:<br>• **No verification: Connect to any appliance**<br>• **Full verification: Only connect to appliances with verified certificates** |
| VCS Certificate Check Mode | Select how the client behaves if it cannot verify a secure connection to the View Connection Server:<br>• **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.)<br>• **Warn before connecting to untrusted servers**: Configure the client to display a warning if an unsigned or expired certificate is encountered, or if the certificate is not self-signed and the zero client trust store is empty. (This option is selected by default.)<br>• **Do not verify server identity certificates**: Configure the client to allow all connections. (This option is not secure.) |
| VCS Certificate Check Mode Lockout | Enable to prevent users from changing the **VCS Certificate Check Mode** settings from the OSD. |
| Trusted View Connection Servers | Click the **Show** button to display VMware View Connection Servers for which the client has received a valid certificate.<br>Click the **Clear** button to clear this cache. |
| Login Username Caching | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |

| Parameter | Description |
|---|---|
| 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. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>• **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended. |

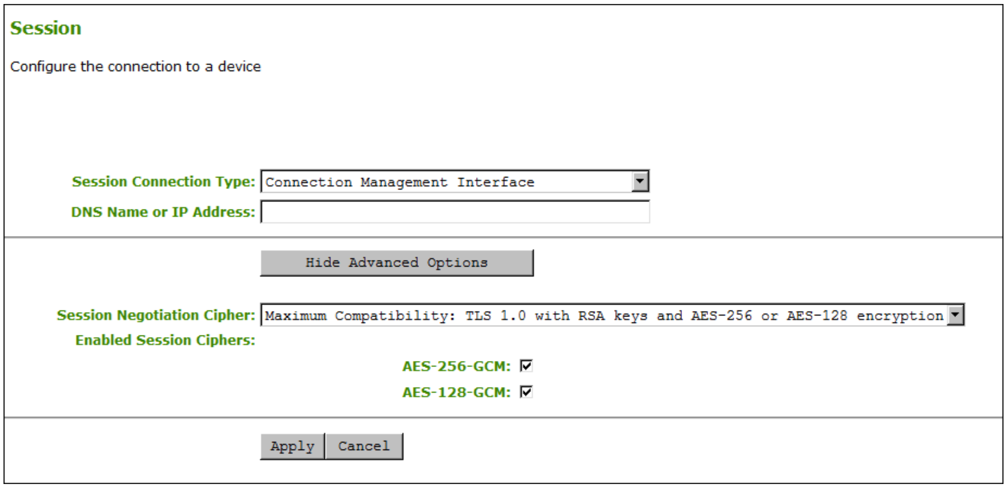
| Parameter | Description |
|---|---|
| | • **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>• Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>• VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>• VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance. |

| Parameter | Description |
|---|---|
| | • You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

## 5.6.16 AWI Host: Connection Management Interface Session Settings

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

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



Session

Configure the connection to a device

Session Connection Type: Connection Management Interface

DNS Name or IP Address:

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

**Figure 5-28: AWI Session Connection Type – Connection Management Interface (Host)**

**Table 5-33: AWI Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the DNS name or IP address of the connection manager. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>• **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>• **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>• **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>• **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>• **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual |

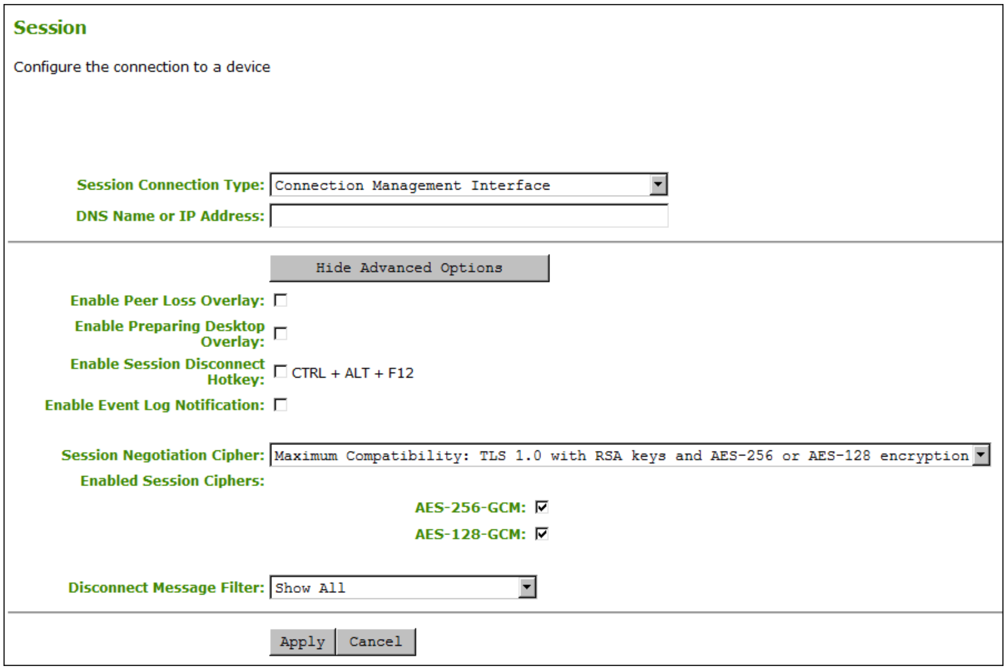
| Parameter | Description |
|---|---|
| | desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>• Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>• VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>• VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance. |

| Parameter | Description |
|---|---|
| | • You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

### 5.6.17 AWI Client: Connection Management Interface Session Settings

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

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



Session

Configure the connection to a device

Session Connection Type: Connection Management Interface

DNS Name or IP Address:

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: □ CTRL + ALT + F12

Enable Event Log Notification: □

Session Negotiation Cipher: Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

Disconnect Message Filter: Show All

**Figure 5-29: AWI Session Connection Type – Connection Management Interface (Client)**

**Table 5-34: AWI Session Page Parameters**

| **Parameter** | **Description** |
|---|---|
| DNS Name or IP Address | Enter the DNS name or IP address of the connection manager. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Session Disconnect Hotkey | When enabled, users can press the Ctrl+Alt+F12 hotkey sequence to pop up the "Zero Client Control Panel" overlay, which lets them disconnect the current session on the workstation or power off the workstation.<br>Note: Before users can use this disconnect hotkey sequence, certain other configuration options must be in place. See Disconnecting from a Session for details. |

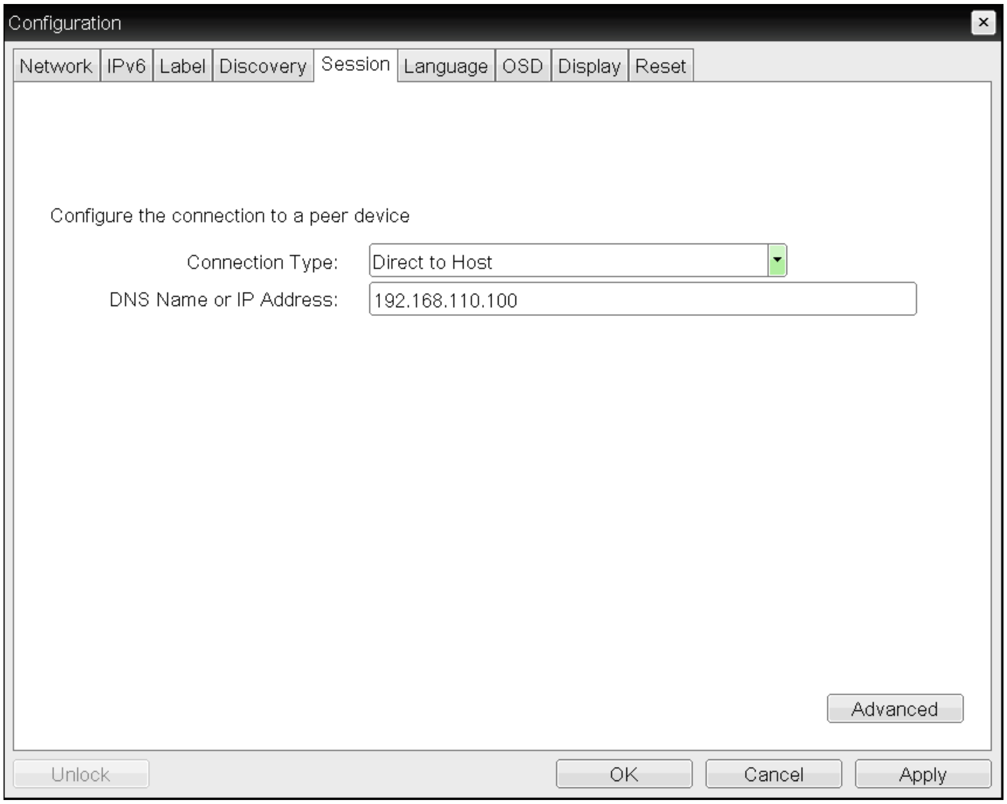
| Parameter | Description |
|---|---|
| Enable Event Log Notification | When enabled, the client sends the contents of its event log to the connection management server. |
| Session Negotiation Cipher | Configure the Transport Layer Security (TLS) cipher the client will use to negotiate the TLS session between the PCoIP client and the PCoIP host:<br>● **TLS 1.0 with RSA keys and AES-256 or AES-128 encryption**: This option provides maximum compatibility.<br>● **TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption**. This option provides a higher level of security. |
| Enabled Session Ciphers | Enable or disable an encryption mode for the device. By default, all encryption modes that pertain to a device are enabled.<br>● **AES-128-GCM** (Tera1 and Tera2): An encryption method implemented in first-generation Tera1 and second-generation Tera2 processors. This method offers the best performance between hardware endpoints for Tera1 devices. AES-128-GCM also may offer improved performance for Tera2 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network.<br>● **AES-256-GCM** (Tera2 only): A more secure encryption method implemented in second-generation Tera2 processors that offers the best performance between hardware endpoints. When connecting to VMware 4 or later, AES-128-GCM is recommended.<br>● **Salsa20-256-Round12** (Tera1 only): A lighter encryption method implemented in firmware that may offer improved performance for Tera1 clients when connecting to VMware View 4 or later if there is more than about 7 Mbps available on the network.<br>Note: For more information about connecting to VMware View virtual desktops, see "Using PCoIP Zero Clients with VMware View User Guide" (TER0904005).<br>Note: The enabled encryption mode must match between the host and client for a session to be established. If more than one mode is enabled, the firmware selects the following:<br>● Host to Tera1 or Tera2 clients: AES-128-GCM or AES-256-GCM for the PCoIP session.<br>● VMware View 4.5 and later to Tera1 client: SALSA20-256-Round12 for the PCoIP session.<br>● VMware View 4.5 and later to Tera2 client: AES-128-GCM for the PCoIP session. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>● You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>● You have been disconnected because an administrator |

| Parameter | Description |
|---|---|
| | disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

## 5.6.18 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.

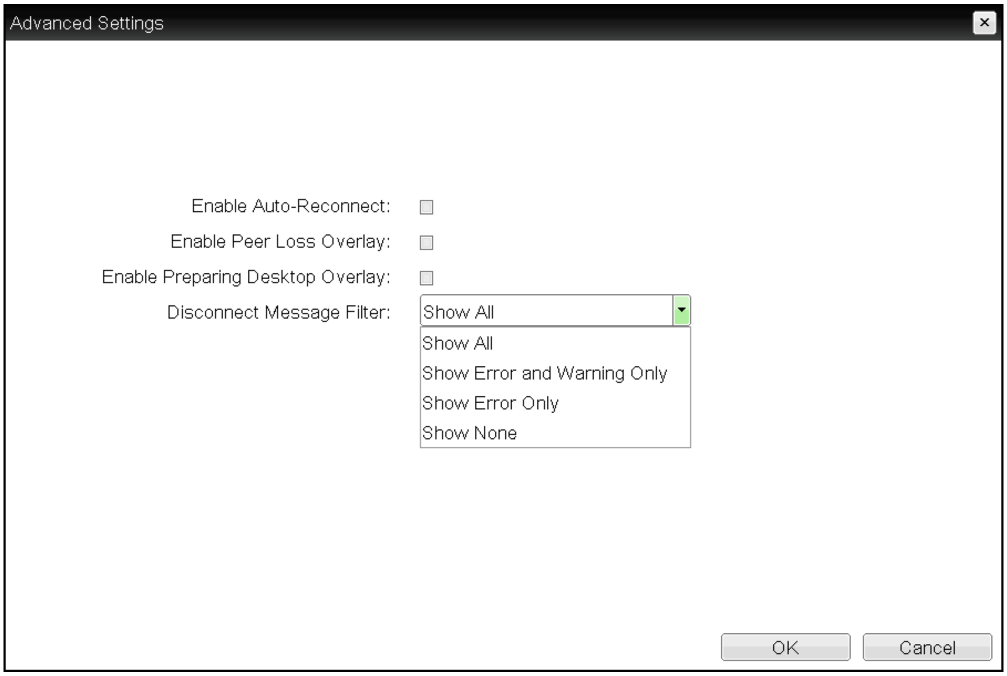


Configure the connection to a peer device

Connection Type: Direct to Host

DNS Name or IP Address: 192.168.110.100

Figure 5-30: OSD Session Connection Type – Direct to Host



Enable Auto-Reconnect: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-31: Advanced Settings**

**Table 5-35: OSD Session Page Parameters**

| **Parameters** | **Description** |
|---|---|
| DNS Name or IP Address | Enter the IP address or DNS name for the host. |
| 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. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session: |

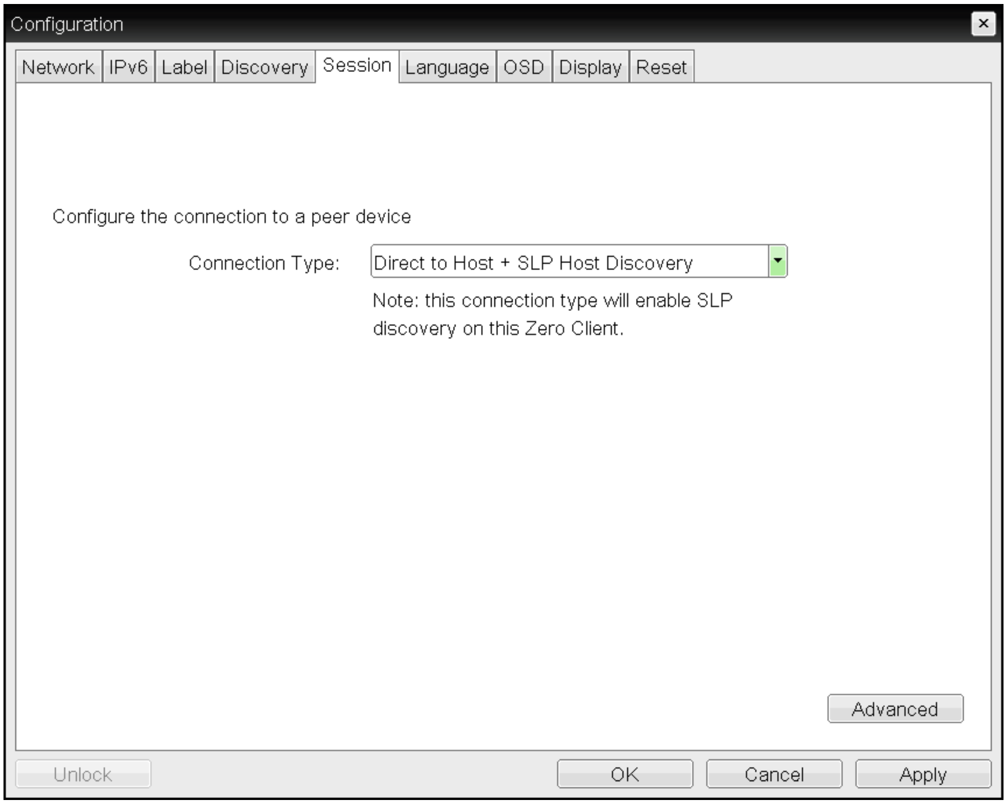
| Parameters | Description |
|---|---|
| | • You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages |

| Parameters | Description |
|---|---|
| | and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

### 5.6.19 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.

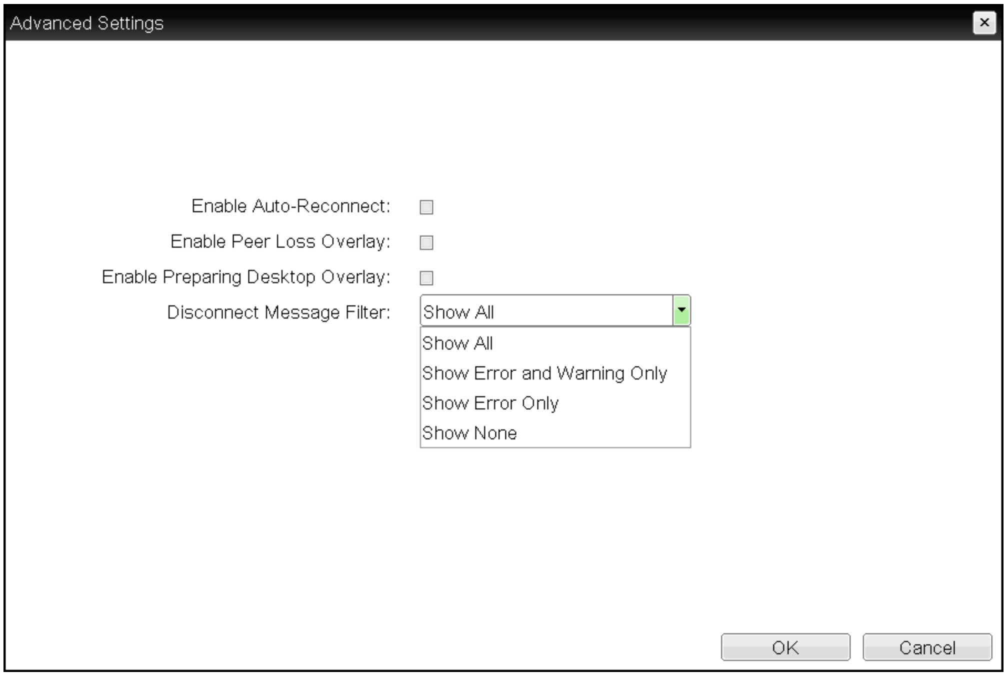


Configure the connection to a peer device

Connection Type: Direct to Host + SLP Host Discovery

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

**Figure 5-32: OSD Session Connection Type – Direct to Host + SLP Host Discovery**



Advanced Settings

Enable Auto-Reconnect: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-33: Advanced Settings**

**Table 5-36: OSD Session Page Parameters**

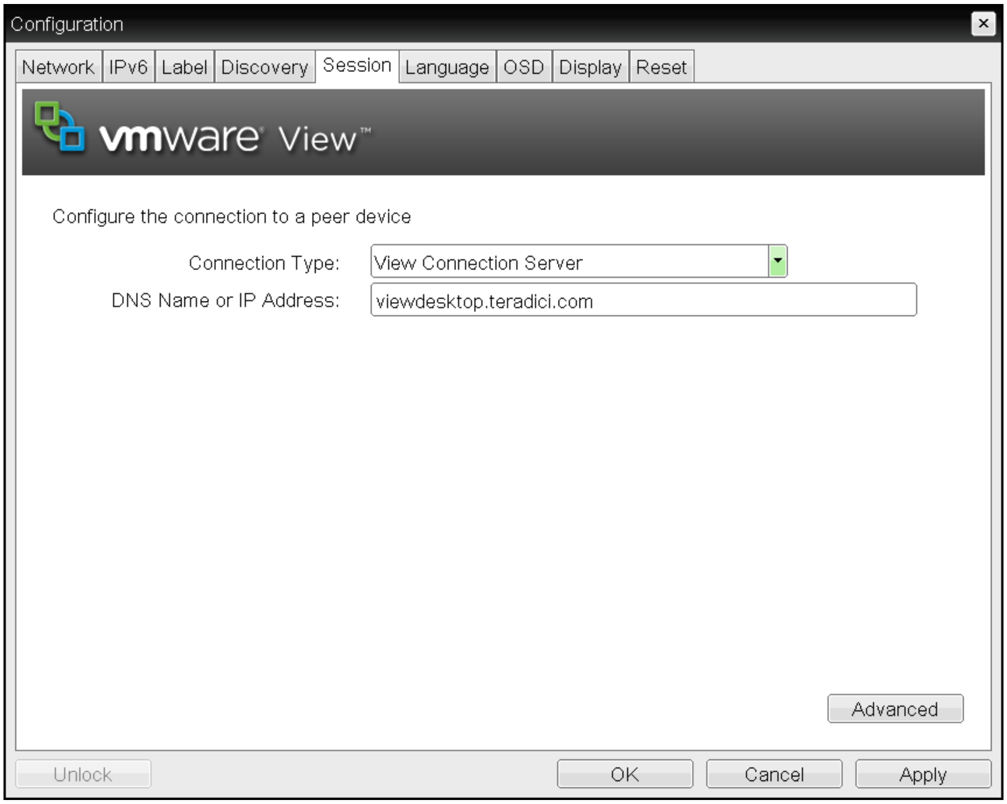
| Parameters | Description |
|---|---|
| Enable Auto-Reconnect | When enabled, lets the client automatically reconnect with the last connected host when a session is lost. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>● You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>● You have been disconnected because an administrator |

| Parameters | Description |
|---|---|
| | disconnected you.<br>● You have been disconnected because you logged in from another location.<br>● You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>● You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>● You have been disconnected.<br>● Unable to connect (0x1001). Please contact your IT administrator.<br>● Unable to connect (0x1002). Please contact your IT administrator.<br>● Session closed remotely.<br>● Session closed remotely (unknown cause).<br>● You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>● You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

## 5.6.20 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 VMware View Connection Server to connect to a virtual desktop.

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

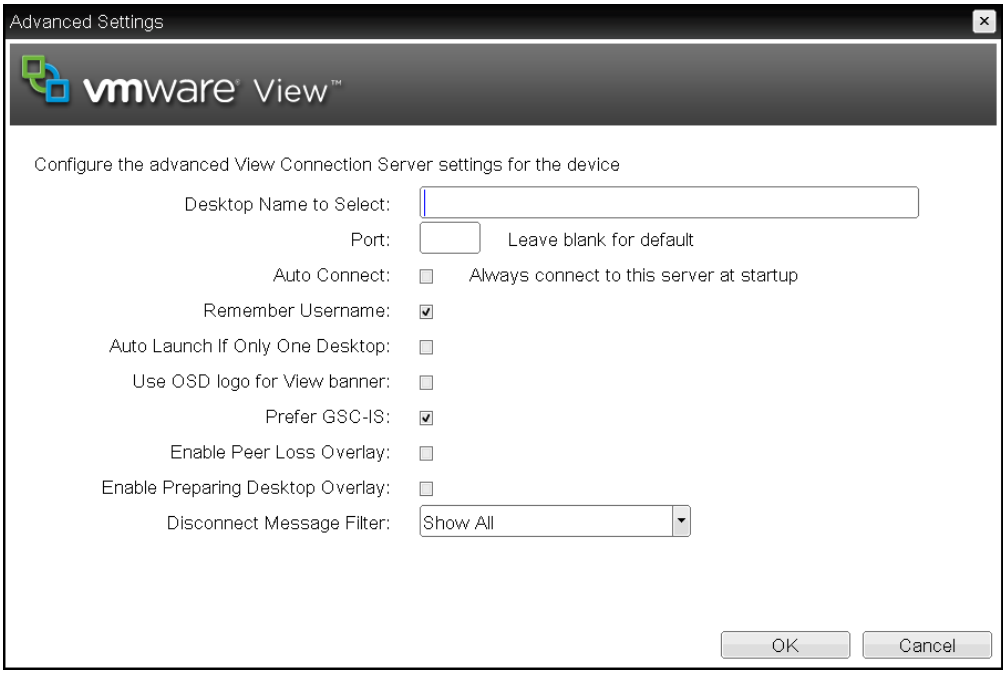


Configure the connection to a peer device

Connection Type: View Connection Server

DNS Name or IP Address: viewdesktop.teradici.com

**Figure 5-34: OSD Session Connection Type – View Connection Server**



Advanced Settings

Configure the advanced View Connection Server settings for the device

Desktop Name to Select:

Port: Leave blank for default

Auto Connect: □ Always connect to this server at startup

Remember Username: ☑

Auto Launch If Only One Desktop: □

Use OSD logo for View banner: □

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-35: Advanced Settings**

**Table 5-37: OSD Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated.<br>Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect. |
| Remember Username | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |

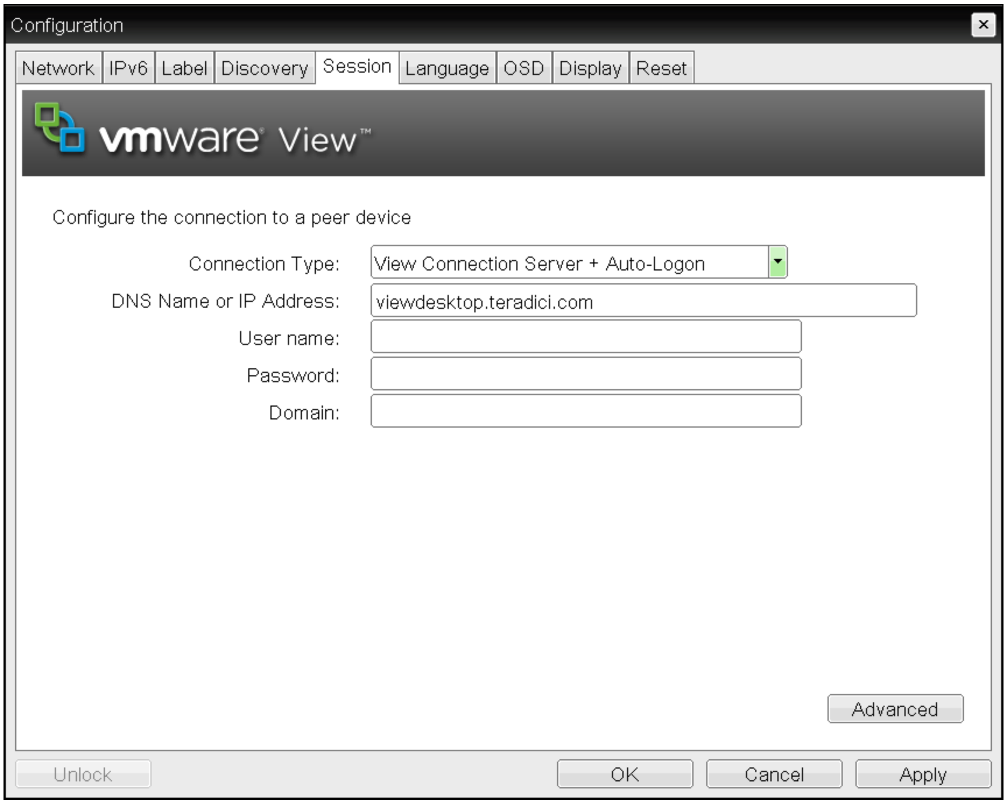
| Parameter | Description |
|---|---|
| Prefer GSC-IS | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint 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. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error |

| Parameter | Description |
|---|---|
| | (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

## 5.6.21 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 the user connects to a virtual desktop via a VMware View Connection Server.

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



Configuration

Configure the connection to a peer device

Connection Type: View Connection Server + Auto-Logon

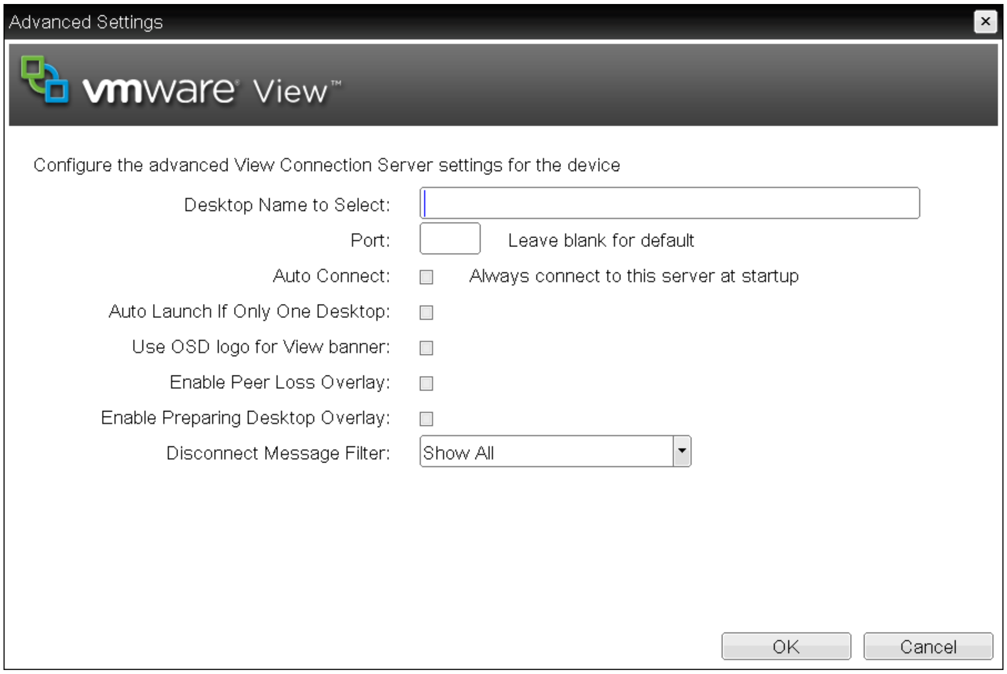
DNS Name or IP Address: viewdesktop.teradici.com

User name:

Password:

Domain:

**Figure 5-36: OSD Session Connection Type – View Connection Server + Auto-Logon**



Advanced Settings

Configure the advanced View Connection Server settings for the device

Desktop Name to Select:

Port: Leave blank for default

Auto Connect: □ Always connect to this server at startup

Auto Launch If Only One Desktop: □

Use OSD logo for View banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-37: Advanced Settings**

**Table 5-38: OSD Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| User name | Enter the username for the client. |
| Password | Enter the password for the client. |
| Domain | Enter the domain name for the client. |
| Desktop Name to Select | Enter the pool/desktop name used by the client when starting a session.<br>Note: This setting is optional. |
| Port | By default this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Auto Connect | When enabled, the client automatically connects to the selected View Connection Server whenever the client powers up or when a session with the virtual desktop is terminated.<br>Note: After enabling **Auto Connect**, the client must be power-cycled for the change to take effect. |
| Auto Launch If Only One Desktop | When enabled, users are automatically connected to their virtual desktop after user credentials are entered.<br>Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |

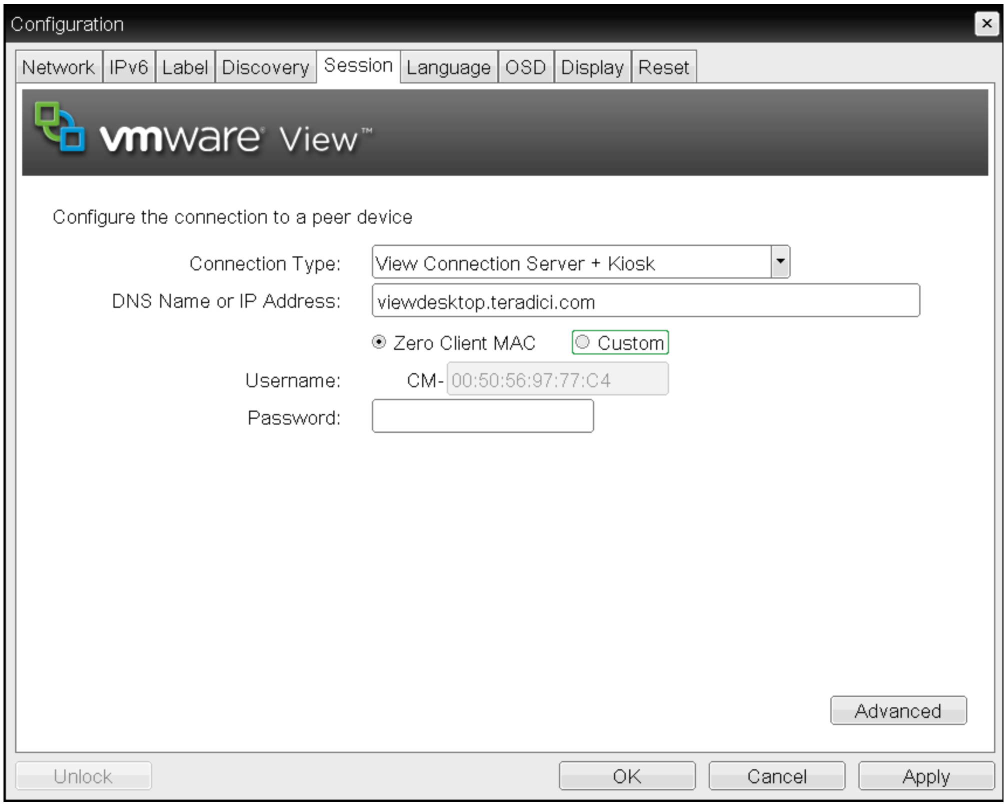
| Parameter | Description |
|---|---|
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect |

| Parameter | Description |
|---|---|
| | messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

## 5.6.22 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 virtual desktop via a VMware View Connection Server.

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



Configure the connection to a peer device

Connection Type: View Connection Server + Kiosk

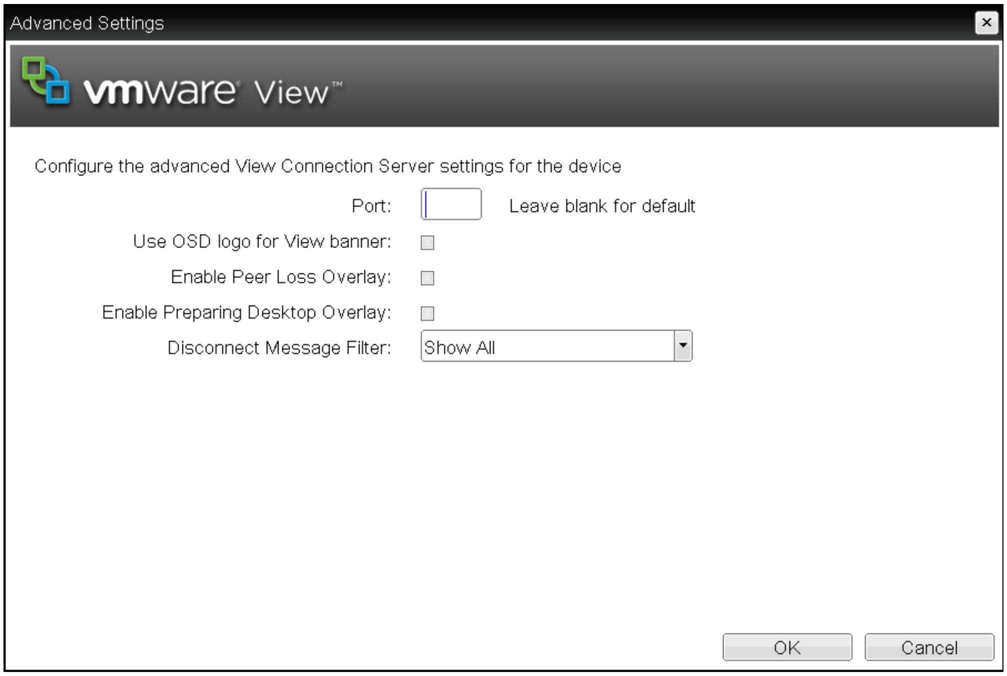
DNS Name or IP Address: viewdesktop.teradici.com

● Zero Client MAC ○ Custom

Username: CM- 00:50:56:97:77:C4

Password:

**Figure 5-38: OSD Session Connection Type – View Connection Server + Kiosk**



Configure the advanced View Connection Server settings for the device

Port: Leave blank for default

Use OSD logo for View banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-39: Advanced Settings**

**Table 5-39: OSD Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Username Type | Select the type of username that matches the naming you use for the devices on the View Connection Server.<br>• **Zero Client MAC**: Select this option to automatically populate the **Username** field with the MAC address of the zero client.<br>• **Custom**: Enter the username for the zero client. This username has the prefix "Custom." |
| Username | When **Custom** is selected as the username type, enter the value for this component of the custom username. This field is limited to 13 characters. |
| 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 this field is blank, and port 443 is used to communicate with the View Connection Server.<br>If your network is set up to use a non-standard port for secure connections, enter the port number. |
| Use OSD Logo for View | When enabled, the PCoIP zero client OSD logo appears during login |

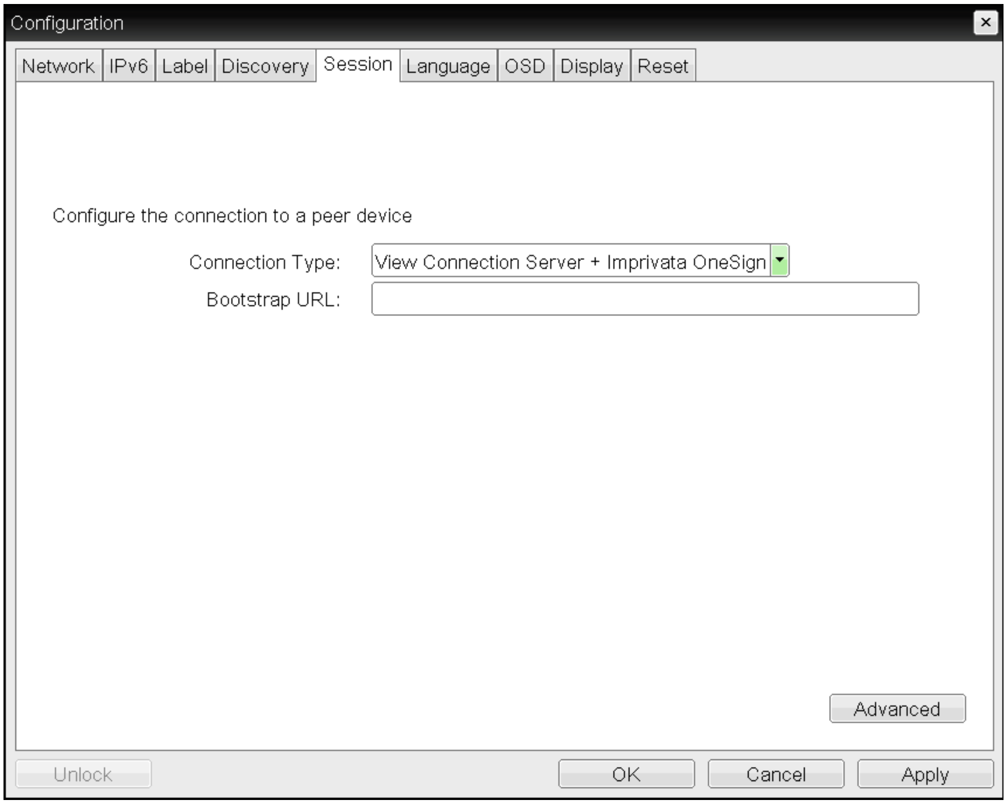
| Parameter | Description |
|---|---|
| Banner | in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session:<br>• You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance. |

| Parameter | Description |
|---|---|
| | • You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages and displays only Error messages.<br>4. **Show None** – Don’t show any disconnect messages. |

### 5.6.23 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 virtual desktop.

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



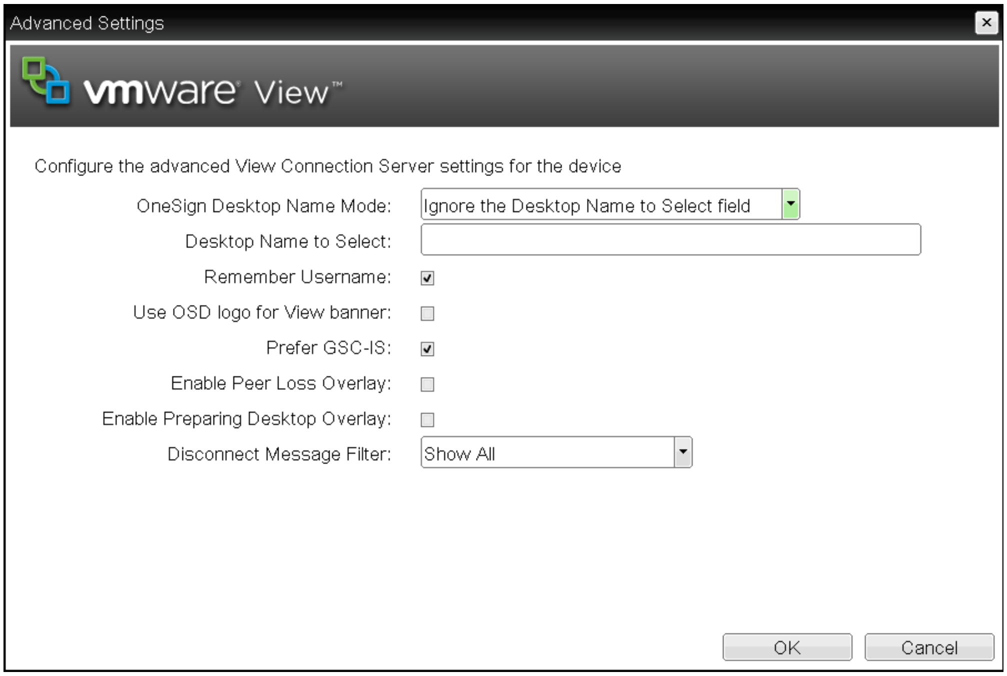
Configuration

Configure the connection to a peer device

Connection Type: View Connection Server + Imprivata OneSign

Bootstrap URL:

**Figure 5-40: OSD Session Connection Type – View Connection Server + Imprivata OneSign**



Advanced Settings

Configure the advanced View Connection Server settings for the device

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

Desktop Name to Select:

Remember Username: ☑

Use OSD logo for View banner: □

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

**Figure 5-41: Advanced Settings**

**Table 5-40: OSD Session Page Parameters**

| Parameter | Description |
|---|---|
| DNS Name or IP Address | Enter the VMware View Connection Server's DNS name or IP address. |
| Bootstrap URL | Enter the bootstrap URL used to find an initial OneSign server in a OneSign authentication deployment. |
| Onesign Desktop Name Mode | Select whether the **Desktop Name to Select** property is used in OneSign Mode:<br>- **Ignore the Desktop Name to Select field**<br>- **Use the Desktop Name to Select field if set** |
| Desktop Name to Select | Enter the desktop name. When the desktop pool list includes a pool with this name, the client will immediately start a session with that pool.<br>Note: This field is case-insensitive. |
| Remember Username | When enabled, the username text box automatically populates with the last username entered. |
| Use OSD Logo for View Banner | When enabled, the PCoIP zero client OSD logo appears during login in place of the VMware View banner. You can upload an OSD logo from the OSD Logo Upload page. |
| Prefer GSC-IS | When selected, the GSC-IS interface is used if a smart card supports more than one interface such as CAC (GSC-IS) and PIV endpoint. If a smart card supports only one interface, such as either CAC or PIV endpoint, then only the CAC or PIV endpoint interface is used regardless of this setting. This only affects smart card access performed outside of PCoIP sessions. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session: |

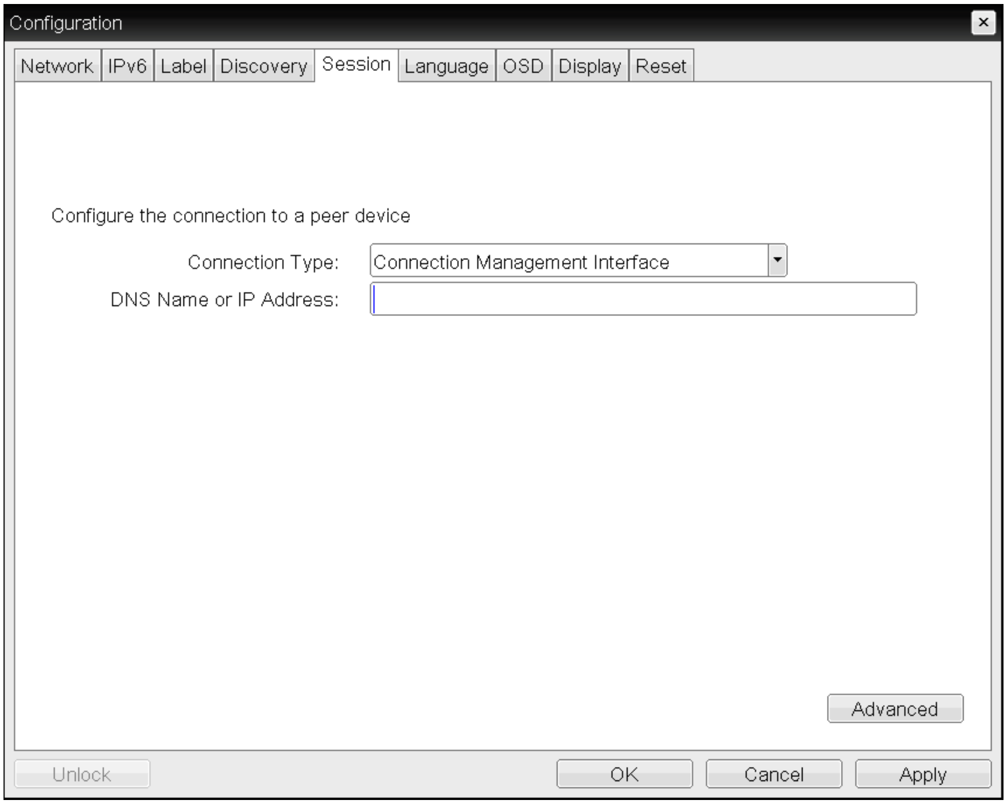
| Parameter | Description |
|---|---|
| | • You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages |

| Parameter | Description |
|---|---|
| | and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

### 5.6.24 OSD: Connection Management Interface Session Settings

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

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

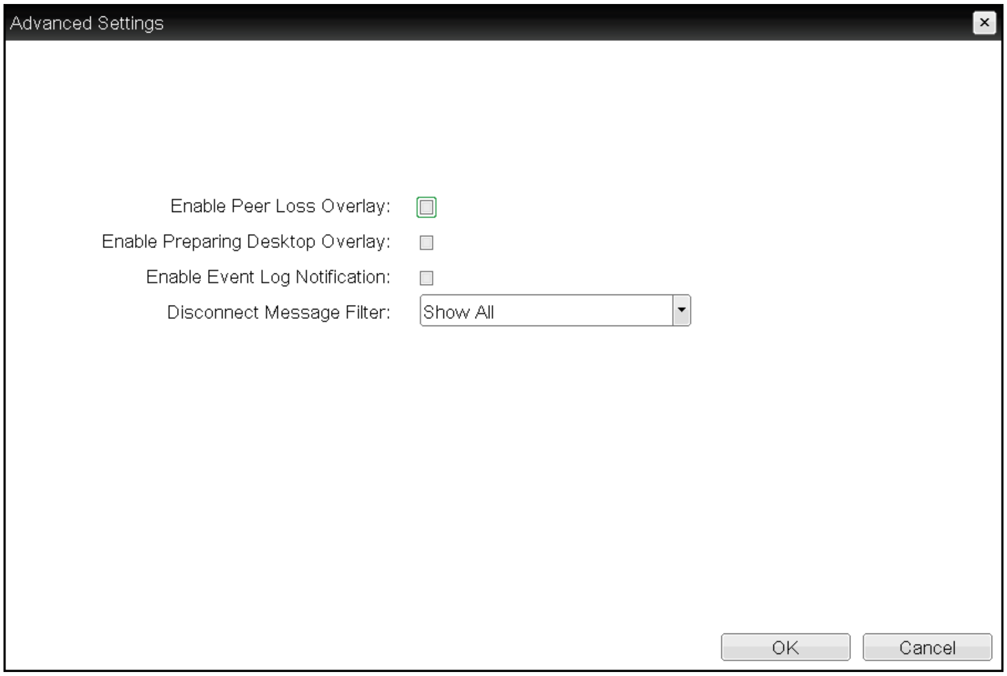


Configure the connection to a peer device

Connection Type: Connection Management Interface

DNS Name or IP Address:

Figure 5-42: OSD Session Connection Type – Connection Management Interface


Advanced Settings

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Event Log Notification: □

Disconnect Message Filter: Show All

**Figure 5-43: Advanced Settings**

**Table 5-41: AWI Session Page Parameters**

| **Parameter** | **Description** |
|---|---|
| DNS Name or IP Address | Enter the DNS name or IP address of the connection manager. |
| Enable Peer Loss Overlay | When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message.<br>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, AWI, or MC. |
| Enable Preparing Desktop Overlay | When enabled, the "Preparing Desktop" overlay appears on the display(s) when users log in.<br>Note: This overlay provides assurance that login is proceeding if the desktop takes more than a few seconds to appear. |
| Enable Event Log Notification | When enabled, the client sends the contents of its event log to the connection management server. |
| Disconnect Message Filter | This field lets you control what type of messages appear when a session is disconnected. There are three categories:<br>**Information:** User- or administrator-initiated actions affecting the session: |

| Parameter | Description |
|---|---|
| | • You have been disconnected because you logged in from another location or your host was shut down or restarted.<br>• You have been disconnected because an administrator disconnected you.<br>• You have been disconnected because you logged in from another location.<br>• You have been disconnected because you disconnected from your workstation.<br>**Warning:** System-initiated, but expected actions affecting the session:<br>• You have been disconnected because your session timed out.<br>**Error:** Unexpected system-initiated actions causing session to fail:<br>• You have been disconnected.<br>• Unable to connect (0x1001). Please contact your IT administrator.<br>• Unable to connect (0x1002). Please contact your IT administrator.<br>• Session closed remotely.<br>• Session closed remotely (unknown cause).<br>• You have been disconnected due to a configuration error (0x100). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x201). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x300). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x301). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x302). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x303). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x305). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x400). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x401). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x402). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x403). Please contact your IT administrator for assistance.<br>• You have been disconnected due to a configuration error (0x404). Please contact your IT administrator for assistance.<br>You can choose to display:<br>1. **Show All** messages – This option shows all disconnect messages including Info, Warning, and Error messages.<br>2. **Show Error and Warnings Only** – This option hides info messages and displays only error and warning messages.<br>3. **Show Error Only** – This option hides Info and Warning messages |

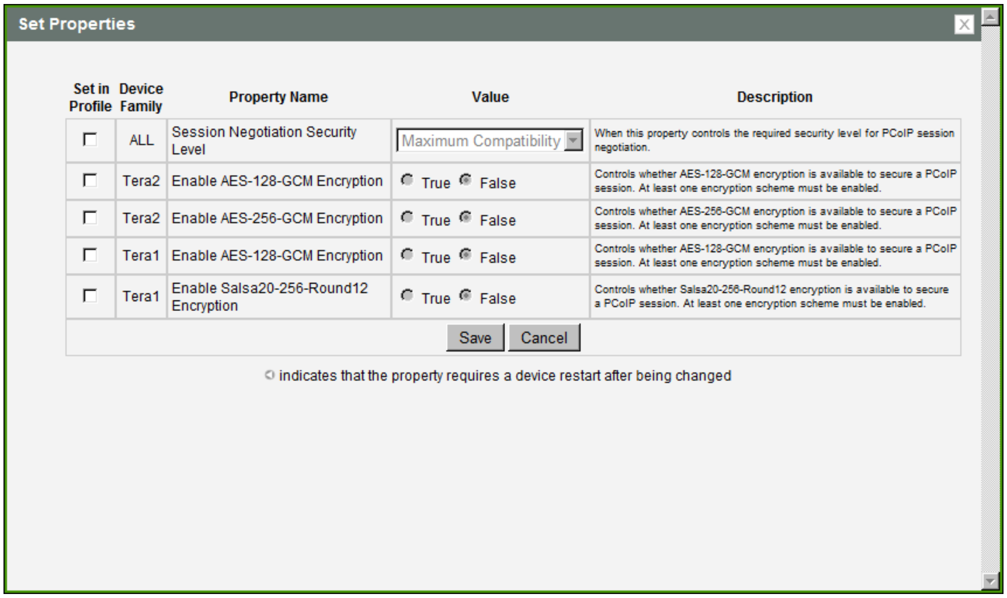
| Parameter | Description |
|---|---|
| | and displays only Error messages.<br>4. **Show None** – Don't show any disconnect messages. |

# 5.7 Configuring Session Encryption

## 5.7.1 MC: Encryption Settings

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

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Session Negotiation Security Level | Maximum Compatibility | When this property controls the required security level for PCoIP session negotiation. |
| □ | Tera2 | Enable AES-128-GCM Encryption | ○ True ● False | Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled. |
| □ | Tera2 | Enable AES-256-GCM Encryption | ○ True ● False | Controls whether AES-256-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled. |
| □ | Tera1 | Enable AES-128-GCM Encryption | ○ True ● False | Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled. |
| □ | Tera1 | Enable Salsa20-256-Round12 Encryption | ○ True ● False | Controls whether Salsa20-256-Round12 encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled. |

indicates that the property requires a device restart after being changed

**Figure 5-44: MC Encryption Configuration**

**Table 5-42: MC Encryption Configuration Parameters**

| Parameter | Description |
|---|---|
| Session Negotiation Security Level | Configure the required security level for PCoIP session negotiation:<br>• **Maximum Compatibility**<br>• **Suite B**: This option provides a higher level of security. |
| Enable AES-128-GCM Encryption (Tera2) | When enabled, uses the AES-128-GCM encryption scheme to secure a PCoIP session. |
| Enable AES-256-GCM Encryption (Tera2) | When enabled, uses the AES-256-GCM encryption scheme to secure a PCoIP session. |

| Parameter | Description |
|---|---|
| | Note: This method offers the best performance between hardware endpoints for Tera2 devices. |
| Enable AES-128-GCM Encryption (Tera1) | When enabled, uses the AES-128-GCM encryption scheme to secure a PCoIP session.<br>Note: This method offers the best performance between hardware endpoints for Tera1 devices. |
| Enable Salsa20-256-Round12 Encryption (Tera1) | When enabled, uses the Salsa20-256-Round12 encryption scheme to secure a PCoIP session.<br>Note: This method may offer improved performance for Tera1 clients when connecting to VMware 4 or later if there is more than about 7 Mbps available on the network |

### 5.7.2 AWI: Help for Encryption Settings

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

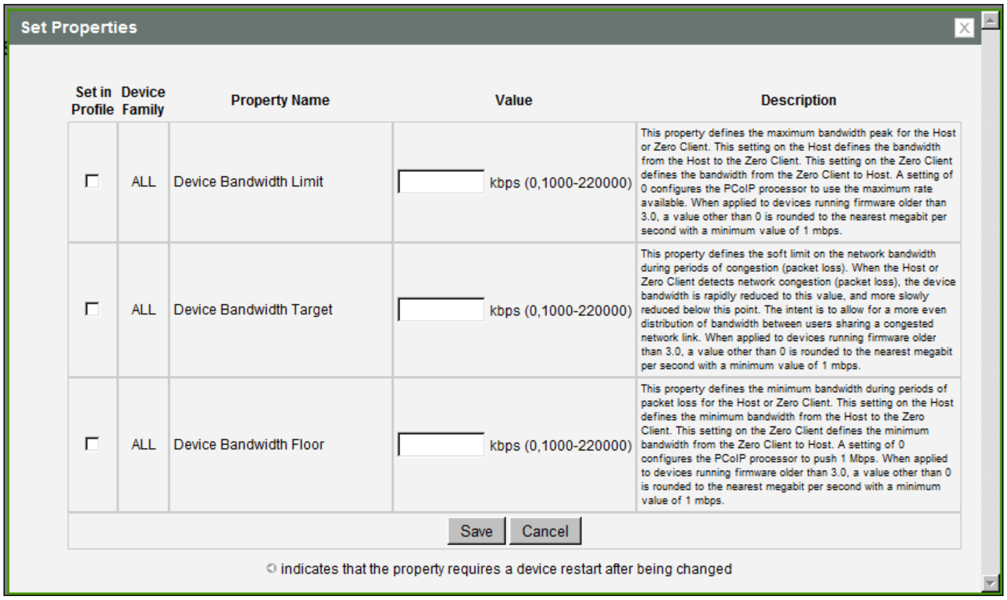
- AWI Host: Direct from Client Session Settings
- AWI Client: Direct to Host Session Settings
- AWI Client: Direct to Host + SLP Host Discovery Session Settings
- AWI Client: View Connection Server Session Settings
- AWI Client: View Connection Server + Auto-Logon Session Settings
- AWI Client: View Connection Server + Kiosk Session Settings
- AWI Client: View Connection Server + Imprivata OneSign Session Settings

## 5.8 Configuring Session Bandwidth

### 5.8.1 MC: Bandwidth Settings

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

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☐ | ALL | Device Bandwidth Limit | kbps (0,1000-220000) | This property defines the maximum bandwidth peak for the Host or Zero Client. This setting on the Host defines the bandwidth from the Host to the Zero Client. This setting on the Zero Client defines the bandwidth from the Zero Client to Host. A setting of 0 configures the PCoIP processor to use the maximum rate available. When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest megabit per second with a minimum value of 1 mbps. |
| ☐ | ALL | Device Bandwidth Target | kbps (0,1000-220000) | This property defines the soft limit on the network bandwidth during periods of congestion (packet loss). When the Host or Zero Client detects network congestion (packet loss), the device bandwidth is rapidly reduced to this value, and more slowly reduced below this point. The intent is to allow for a more even distribution of bandwidth between users sharing a congested network link. When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest megabit per second with a minimum value of 1 mbps. |
| ☐ | ALL | Device Bandwidth Floor | kbps (0,1000-220000) | This property defines the minimum bandwidth during periods of packet loss for the Host or Zero Client. This setting on the Host defines the minimum bandwidth from the Host to the Zero Client. This setting on the Zero Client defines the minimum bandwidth from the Zero Client to Host. A setting of 0 configures the PCoIP processor to push 1 Mbps. When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest megabit per second with a minimum value of 1 mbps. |

indicates that the property requires a device restart after being changed

Figure 5-45: MC Bandwidth Configuration

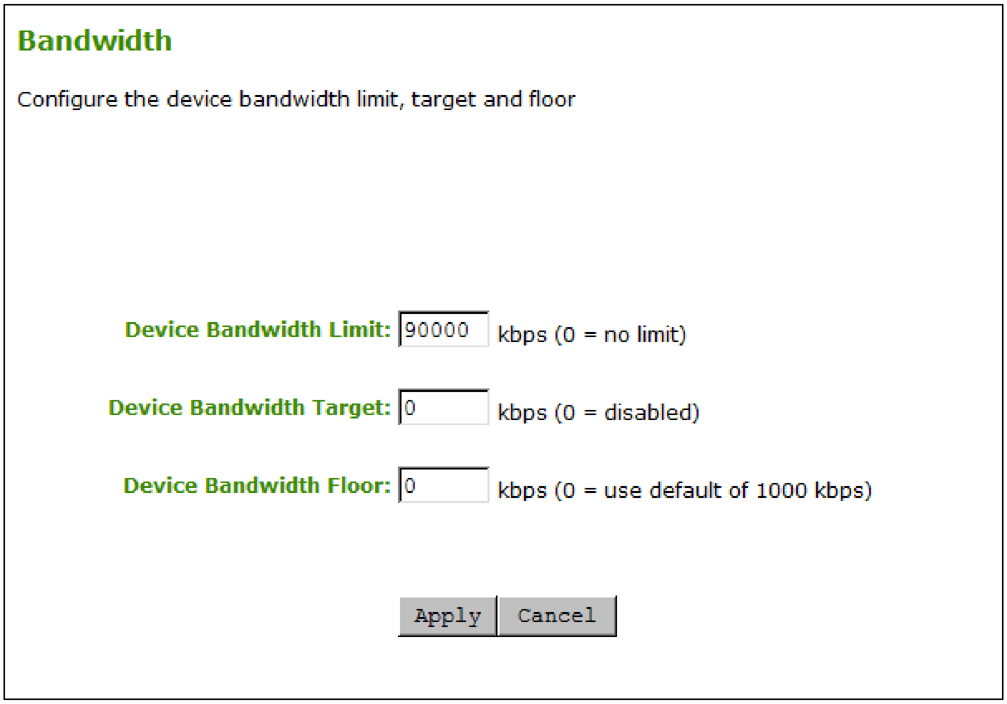
Table 5-43: MC Bandwidth Configuration Parameters

| Parameter | Description |
|---|---|
| Device Bandwidth Limit | Enter the maximum bandwidth peak for hosts or clients. When configuring hosts, this setting defines the bandwidth from the host to the client (e.g., graphics data). When configuring clients, it defines the bandwidth from the client to the host (e.g., USB data).<br>The usable range of the device bandwidth is 1000 to 220000 Kbps.<br>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.<br>We recommend setting this field to the limit of the network connected to the client and host.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps. |
| Device Bandwidth Target | Enter the temporary limit on the network bandwidth during periods of congestion. When the host or client detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it.This allows for a more even distribution of bandwidth between users sharing a congested network link.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps. |
| Device Bandwidth Floor | Enter the minimum bandwidth when congestion is present and bandwidth is required. This allows you to optimize performance for a |

| Parameter | Description |
|---|---|
| | network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor.<br>When configuring hosts, this setting defines the minimum bandwidth from the host to the client (e.g., graphics data).When configuring clients, it defines the minimum bandwidth from the client to the host (e.g., USB data).<br>A setting of 0 configures the PCoIP processor to reduce bandwidth to 1000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value.<br>Note: The firmware implements a slow-start algorithm that increases the bandwidth used until the required bandwidth is reached, network congestion is detected, or the **Device Bandwidth Limit** is met. It begins at the lesser of the **Device Bandwidth Limit** and 8000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm allows a graceful session startup for low bandwidth scenarios (e.g., WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps. |

### 5.8.2 AWI: Bandwidth Settings

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



Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: 90000 kbps (0 = no limit)

Device Bandwidth Target: 0 kbps (0 = disabled)

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

**Figure 5-46: AWI Bandwidth Page**

**Table 5-44: AWI Bandwidth Parameters**

| Parameter | Description |
|---|---|
| Device Bandwidth Limit | Enter the maximum bandwidth peak for hosts or clients. When configuring hosts, this setting defines the bandwidth from the host to the client (e.g., graphics data). When configuring clients, it defines the bandwidth from the client to the host (e.g., USB data).<br>The usable range of the device bandwidth is 1000 to 220000 Kbps.<br>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.<br>We recommend setting this field to the limit of the network connected to the client and host.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps. |
| Device Bandwidth Target | Enter the temporary limit on the network bandwidth during periods of congestion. When the host or client detects packet loss, the device bandwidth is rapidly reduced to this value, and then more slowly reduced below it.This allows for a more even distribution of bandwidth between users sharing a congested network link.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, |

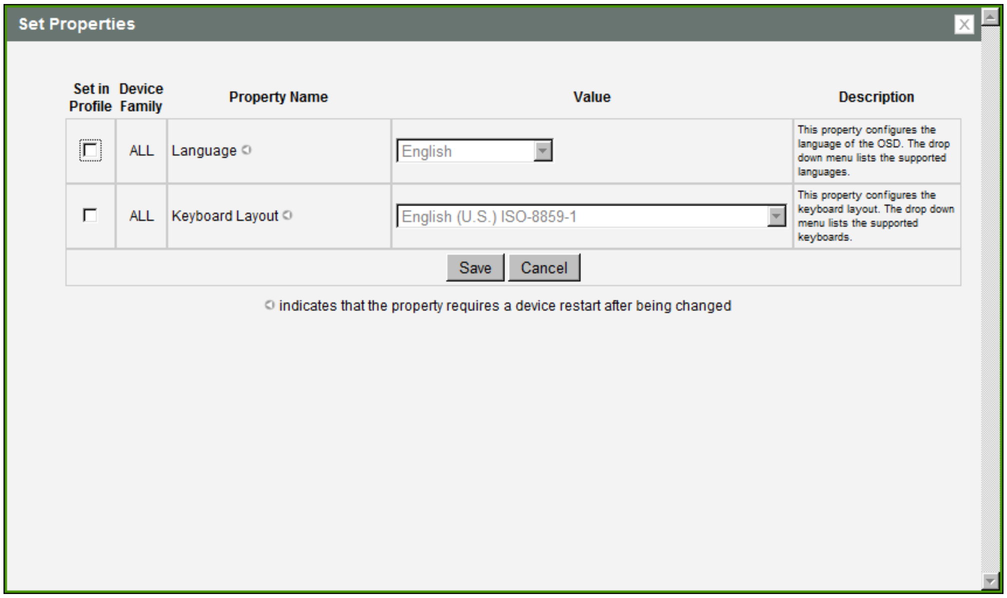
| Parameter | Description |
|---|---|
| | with a minimum value of 1 Mbps. |
| Device Bandwidth Floor | Enter the minimum bandwidth when congestion is present and bandwidth is required. This allows you to optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor.<br>When configuring hosts, this setting defines the minimum bandwidth from the host to the client (e.g., graphics data).When configuring clients, it defines the minimum bandwidth from the client to the host (e.g., USB data).<br>A setting of 0 configures the PCoIP processor to reduce bandwidth to 1000 Kbps during these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value.<br>Note: The firmware implements a slow-start algorithm that increases the bandwidth used until the required bandwidth is reached, network congestion is detected, or the **Device Bandwidth Limit** is met. It begins at the lesser of the **Device Bandwidth Limit** and 8000 Kbps, and increases the bandwidth used within seconds. The slow-start algorithm allows a graceful session startup for low bandwidth scenarios (e.g., WAN scenarios). After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.<br>Note: When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest Megabit per second, with a minimum value of 1 Mbps. |

# 5.9 Configuring the Language

## 5.9.1 MC: Language Settings

The settings on this page let you configure a profile with the language to use in the OSD user interface.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Language ◌ | English | This property configures the language of the OSD. The drop down menu lists the supported languages. |
| □ | ALL | Keyboard Layout ◌ | English (U.S.) ISO-8859-1 | This property configures the keyboard layout. The drop down menu lists the supported keyboards. |

◌ indicates that the property requires a device restart after being changed

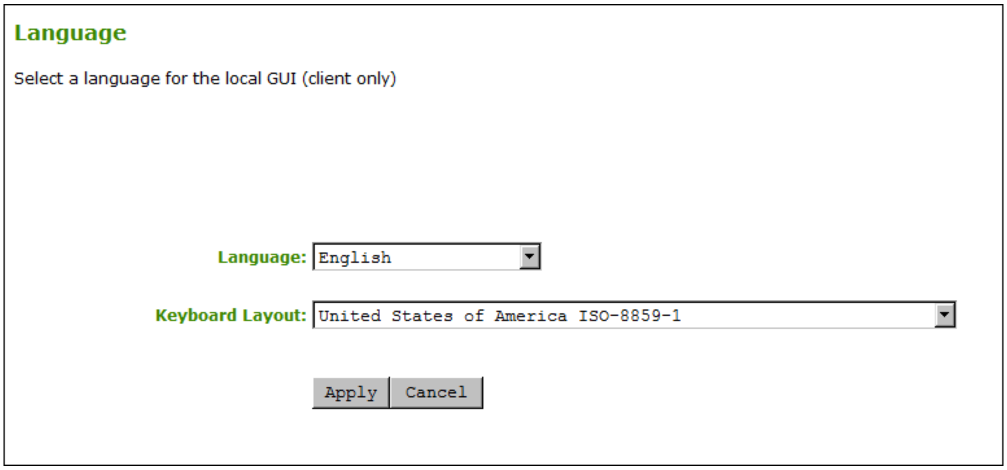
**Figure 5-47: MC Language Configuration**

**Table 5-45: MC Language Configuration Parameters**

| Parameter | Description |
|---|---|
| Language | Configure for the OSD user interface.<br>Note: This does not affect the language setting for the actual user session.<br>Note: This property requires a device restart after being changed. |
| Keyboard Layout | Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped.<br>Note: This property requires a device restart after being changed. |

## 5.9.2 AWI Client: Language Settings

The settings on this page let you configure the language used in the OSD user interface. You can display this page from the **Configuration** > **Language** menu.



Language

Select a language for the local GUI (client only)

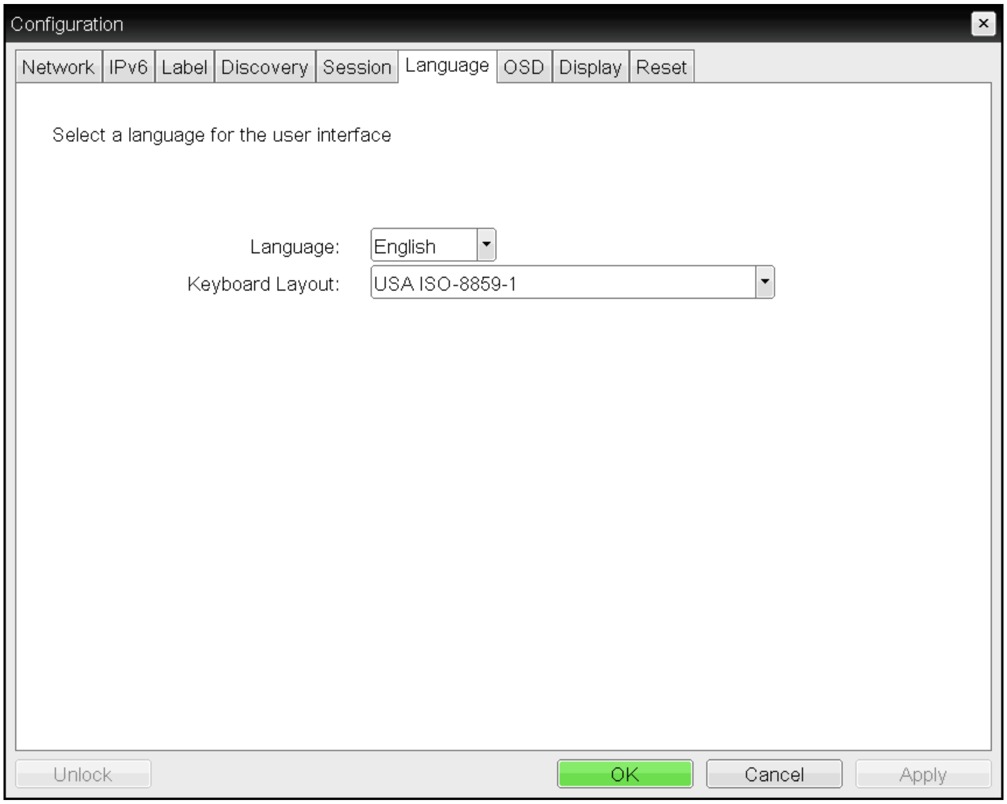
**Figure 5-48: AWI Client Language Page**

**Table 5-46: AWI Client Language Parameters**

| Parameter | Description |
|---|---|
| Language | Configure for the OSD user interface.<br>Note: This does not affect the language setting for the actual user session. |
| Keyboard Layout | Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped. |

## 5.9.3 OSD: Language Settings

The settings on this page let you configure the language used in the OSD user interface. You can display this page from the **Options** > **Configuration** > **Language** menu.



Select a language for the user interface

Language: English

Keyboard Layout: USA ISO-8859-1

**Figure 5-49: OSD Language Page**

**Table 5-47: OSD Language Parameters**

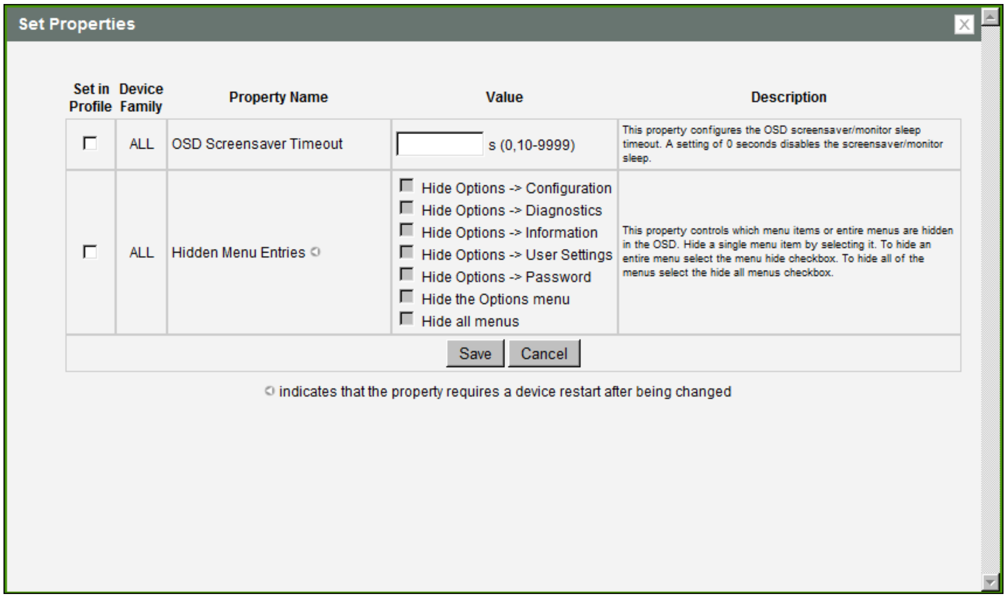
| Parameter | Description |
|---|---|
| Language | Configure for the OSD user interface.<br>Note: This does not affect the language setting for the actual user session. |
| Keyboard Layout | Change the layout of the keyboard. When the user starts a session, this setting is pushed to the virtual machine. If the PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO is set to allow the keyboard layout setting, it is used during the user's session. If this GPO is not set to allow the setting, it is dropped. |

# 5.10 Configuring OSD Parameters

## 5.10.1 MC: OSD Settings

The settings on this page let you configure a profile with the screen-saver timeout value to use on a device's OSD, and also to control which menus and menu items are hidden in the OSD.

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | OSD Screensaver Timeout | s (0,10-9999) | This property configures the OSD screensaver/monitor sleep timeout. A setting of 0 seconds disables the screensaver/monitor sleep. |
| □ | ALL | Hidden Menu Entries ○ | □ Hide Options -> Configuration<br>□ Hide Options -> Diagnostics<br>□ Hide Options -> Information<br>□ Hide Options -> User Settings<br>□ Hide Options -> Password<br>□ Hide the Options menu<br>□ Hide all menus | This property controls which menu items or entire menus are hidden in the OSD. Hide a single menu item by selecting it. To hide an entire menu select the menu hide checkbox. To hide all of the menus select the hide all menus checkbox. |

○ indicates that the property requires a device restart after being changed

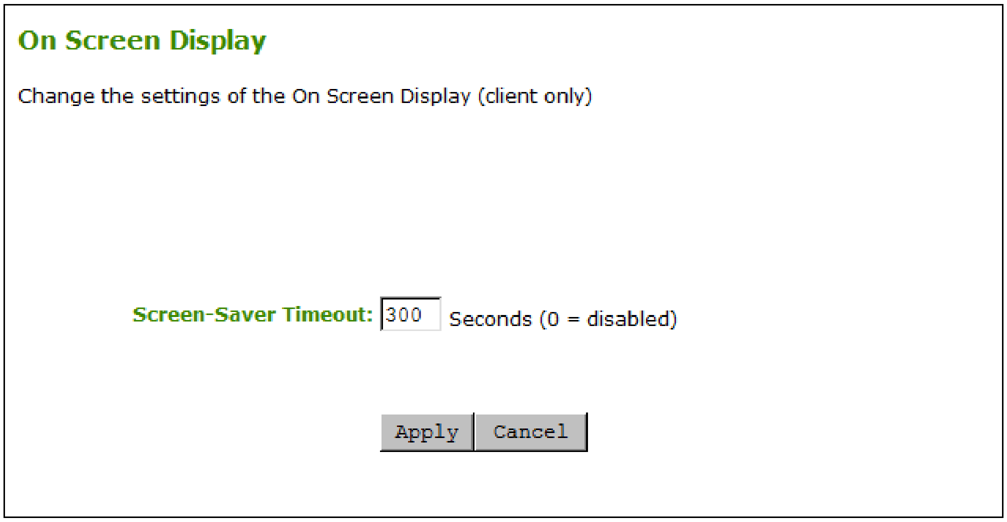
**Figure 5-50: MC OSD Configuration**

**Table 5-48: MC Language Configuration Parameters**

| Parameter | Description |
|---|---|
| OSD Screensaver Timeout | Configure the OSD screen-saver timeout with the number of seconds to wait (10 to 9999) before the attached displays are put into low-power mode. A setting of 0 seconds disables the screen-saver. |
| Hidden Menu Entries | Select the items that you do not want to appear on the OSD local GUI. You can hide a single menu item, the entire **Options** menu, or all menus.<br>Note: This property requires a device restart after being changed. |

## 5.10.2 AWI Client: OSD Settings

The settings on this page let you set the monitor screen-saver timeout for the local OSD. You can display this page from the **Configuration** > **OSD** menu.



On Screen Display

Change the settings of the On Screen Display (client only)

Screen-Saver Timeout: 300 Seconds (0 = disabled)

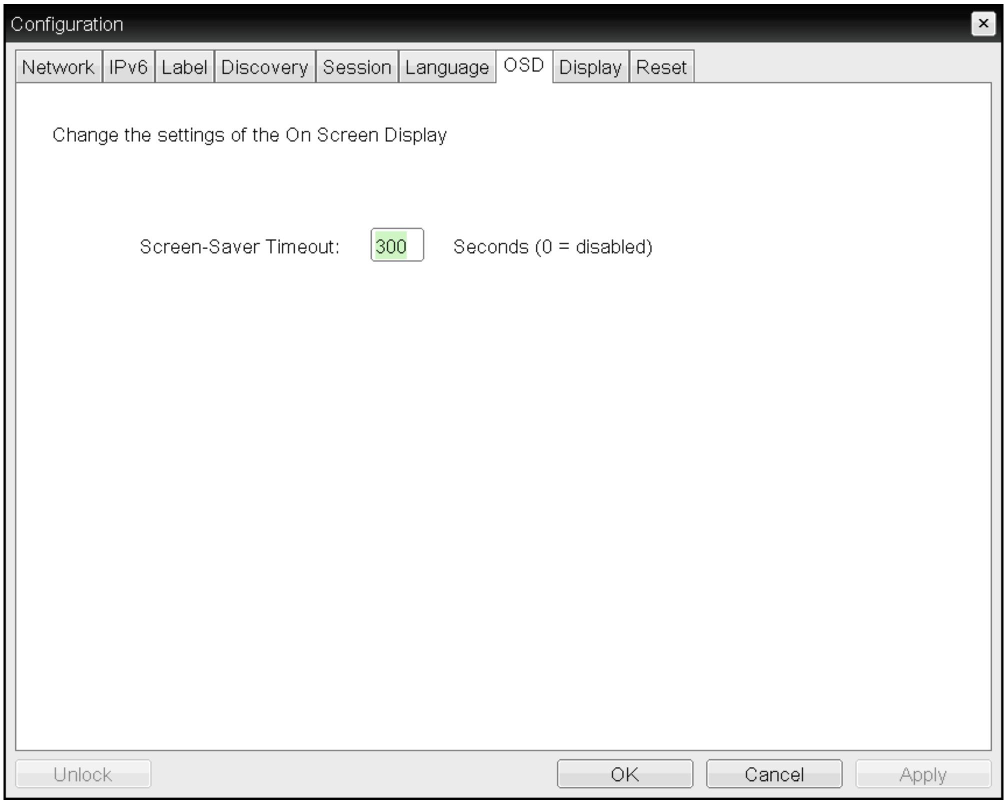
Figure 5-51: AWI On Screen Display Page

Table 5-49: AWI OSD Parameters

| Parameter | Description |
|---|---|
| Screen-Saver Timeout | Configure the OSD screen-saver timeout with the number of seconds to wait (10 to 9999) before the attached displays are put into low-power mode. A setting of 0 seconds disables the screen-saver. |

## 5.10.3 OSD: OSD Settings

The settings on this page let you set the monitor screen-saver timeout for the local OSD. You can display this page from the **Options** > **Configuration** > **OSD** menu.



Change the settings of the On Screen Display

Screen-Saver Timeout: 300 Seconds (0 = disabled)

**Figure 5-52: OSD OSD Page**

**Table 5-50: OSD OSD Parameters**

| Parameter | Description |
|---|---|
| Screen-Saver Timeout | Configure the OSD screen-saver timeout with the number of seconds to wait (10 to 9999) before the attached displays are put into low-power mode. A setting of 0 seconds disables the screen-saver. |

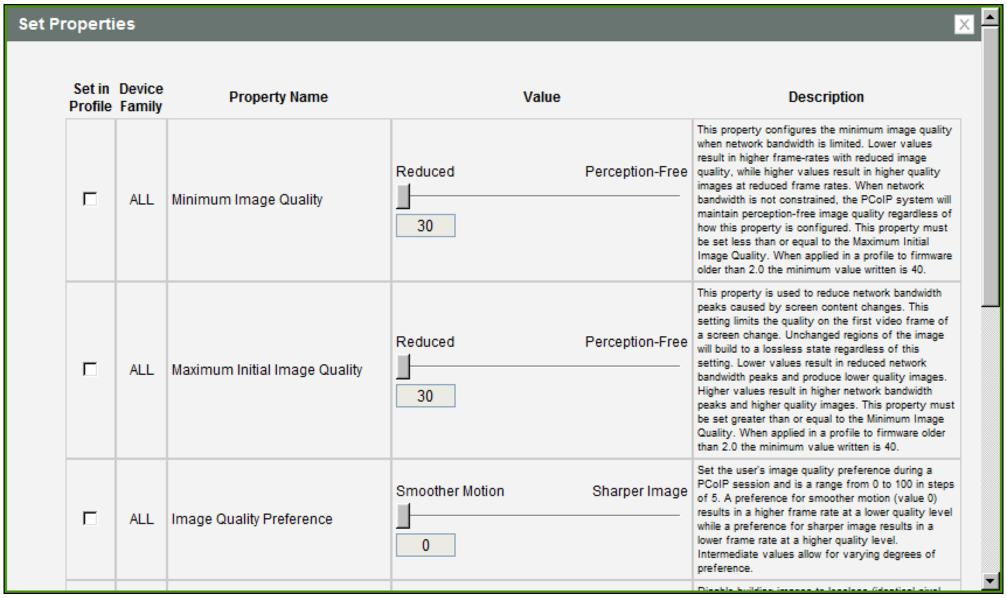
# 5.11 Configuring Image Quality

## 5.11.1 MC: Image Settings

The **Image** page lets you configure a profile to make changes to the image quality of the PCoIP session.

Note: This setting applies only to sessions between zero clients and hosts.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| ☐ | ALL | Minimum Image Quality | Reduced — Perception-Free<br>30 | This property configures the minimum image quality when network bandwidth is limited. Lower values result in higher frame-rates with reduced image quality, while higher values result in higher quality images at reduced frame rates. When network bandwidth is not constrained, the PCoIP system will maintain perception-free image quality regardless of how this property is configured. This property must be set less than or equal to the Maximum Initial Image Quality. When applied in a profile to firmware older than 2.0 the minimum value written is 40. |
| ☐ | ALL | Maximum Initial Image Quality | Reduced — Perception-Free<br>30 | This property is used to reduce network bandwidth peaks caused by screen content changes. This setting limits the quality on the first video frame of a screen change. Unchanged regions of the image will build to a lossless state regardless of this setting. Lower values result in reduced network bandwidth peaks and produce lower quality images. Higher values result in higher network bandwidth peaks and higher quality images. This property must be set greater than or equal to the Minimum Image Quality. When applied in a profile to firmware older than 2.0 the minimum value written is 40. |
| ☐ | ALL | Image Quality Preference | Smoother Motion — Sharper Image<br>0 | Set the user's image quality preference during a PCoIP session and is a range from 0 to 100 in steps of 5. A preference for smoother motion (value 0) results in a higher frame rate at a lower quality level while a preference for sharper image results in a lower frame rate at a higher quality level. Intermediate values allow for varying degrees of preference. |

**Figure 5-53: MC Image Configuration**

**Table 5-51: MC Image Configuration Parameters**

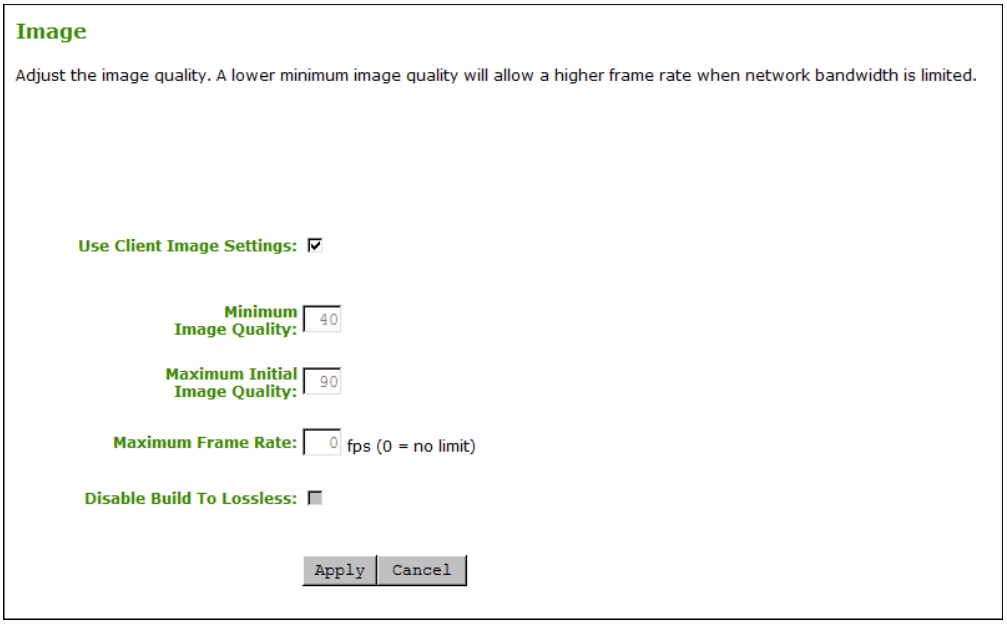
| Parameter | Description |
|---|---|
| Minimum Image Quality | Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate.<br>In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter.<br>Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Maximum Initial Image Quality | Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks.<br>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.<br>Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Image Quality Preference | Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5. |

| Parameter | Description |
|---|---|
| | Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Disable Build to Lossless | Leave this field unchecked to retain the PCoIP protocol's build-to-lossless feature, where images continue to be refined in the background until they reach a fully lossless state (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.<br>**Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination.<br>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.<br>If you have any questions about this field setting, contact Teradici support.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Enable Client Image Settings | When enabled, allows the host the option of using the client's image settings for the session. When disabled, the host's image settings take effect.<br>Note: The Image Quality Preference setting is exempt from this rule. |
| Maximum Frame Rate | The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |

### 5.11.2 AWI Host: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can display this page from the **Configuration** > **Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.



Image

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

Use Client Image Settings: ☑

Minimum Image Quality: 40

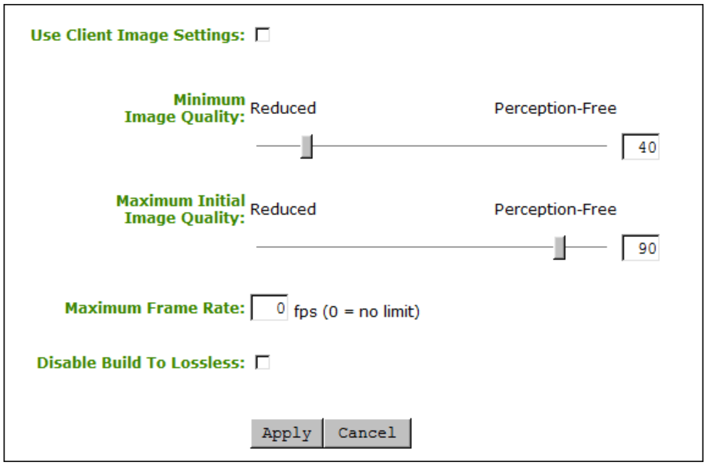
Maximum Initial Image Quality: 90

Maximum Frame Rate: 0 fps (0 = no limit)

Disable Build To Lossless: □

**Figure 5-54: AWI Host Image Page**

Note: When the **Use Client Image Settings** field is not selected, the text boxes on this page are replaced with sliders, as shown below.



Use Client Image Settings: □

Minimum Image Quality: Reduced — Perception-Free 40

Maximum Initial Image Quality: Reduced — Perception-Free 90

Maximum Frame Rate: 0 fps (0 = no limit)

Disable Build To Lossless: □

**Figure 5-55: AWI Host Image Page – Use Client Image Settings Disabled**

**Table 5-52: AWI Host Image Page Parameters**

| Parameter | Description |
|---|---|
| Use Client Image Settings | When enabled, the image settings on this page are not editable. The settings that appear (grayed out) are those stored for the host in flash.<br>When disabled, the image settings are editable and are applied to any current sessions. |

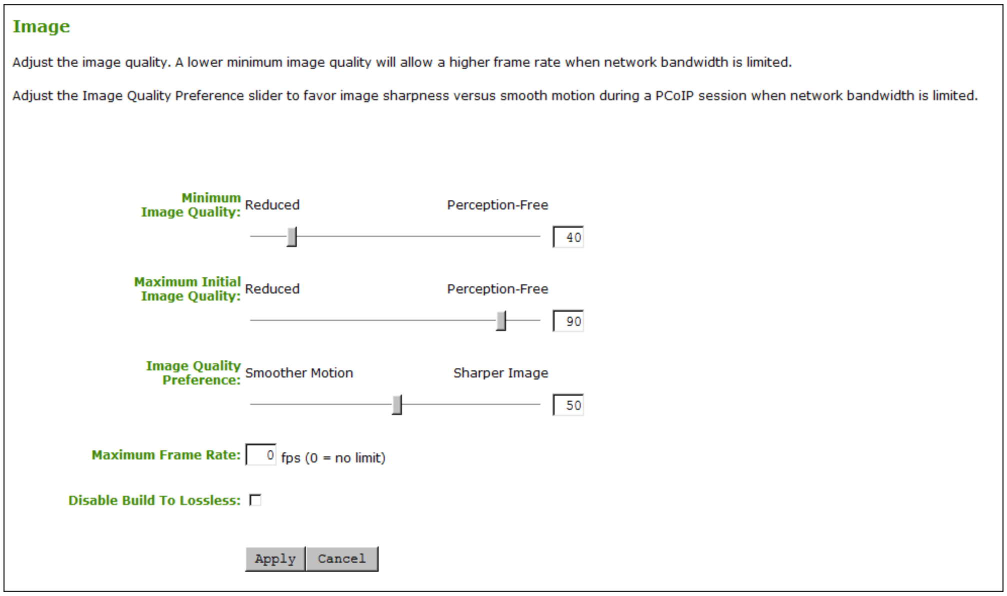
| Parameter | Description |
|---|---|
| Minimum Image Quality | Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate.<br>In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter.<br>Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Maximum Initial Image Quality | Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks.<br>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.<br>Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Image Quality Preference | Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Maximum Frame Rate | The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Disable Build to Lossless | Leave this field unchecked to retain the PCoIP protocol's build-to-lossless feature, where images continue to be refined in the background until they reach a fully lossless state (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.<br>**Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination.<br>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 |

| Parameter | Description |
|---|---|
| | 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.<br>If you have any questions about this field setting, contact Teradici support.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |

## 5.11.3 AWI Client: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can display this page from the **Configuration** > **Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.



Image

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

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

Minimum Image Quality: Reduced — Perception-Free 40

Maximum Initial Image Quality: Reduced — Perception-Free 90

Image Quality Preference: Smoother Motion — Sharper Image 50

Maximum Frame Rate: 0 fps (0 = no limit)

Disable Build To Lossless: □

Figure 5-56: AWI Client Image Page

Table 5-53: AWI Client Image Page Parameters

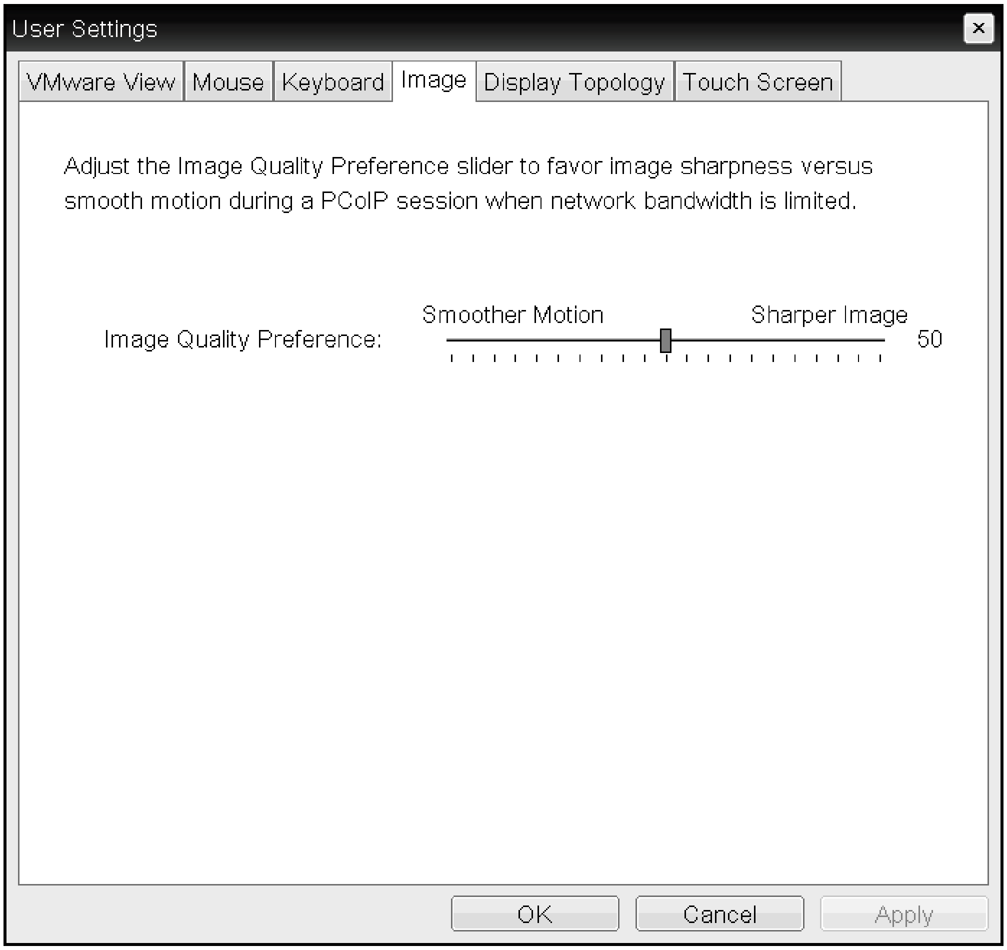
| Parameter | Description |
|---|---|
| Minimum Image Quality | Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate.<br>In environments where the network bandwidth is constrained, move the slider towards **Reduced** to allow higher frame rates. Move the slider towards **Perception-Free** to allow for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. |

| Parameter | Description |
|---|---|
| | Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Maximum Initial Image Quality | Move the slider towards **Reduced** to reduce the network bandwidth peaks caused by screen content changes, but produce lower quality images. Move the slider towards **Perception-Free** to produce higher quality images but also higher bandwidth peaks.<br>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.<br>Note: The **Maximum Initial Image Quality** must be greater than or equal to the **Minimum Image Quality**. |
| Image Quality Preference | Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Maximum Frame Rate | The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |
| Disable Build to Lossless | Leave this field unchecked to retain the PCoIP protocol's build-to-lossless feature, where images continue to be refined in the background until they reach a fully lossless state (i.e., identical pixel-for-pixel rendering when compared to the host image source). This is the default (recommended) setting.<br>**Warning:** Turning on the **Disable Build to Lossless** field will degrade the image presented to the user by the zero client. Do not turn on this field unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination.<br>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.<br>If you have any questions about this field setting, contact Teradici support.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |

### 5.11.4 OSD: Image Settings

The **Image** page lets you make changes to the image quality of the PCoIP session. You can display this page from the **Options** > **User Settings** > **Image** menu.

Note: This setting applies only to sessions between zero clients and hosts.



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

Image Quality Preference: Smoother Motion — Sharper Image 50

Figure 5-57: OSD Image Page

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

Table 5-54: OSD Image Page Parameters

| Parameter | Description |
|---|---|
| Image Quality Preference | Move the slider towards **Smoother Motion** to result in a higher frame rate at a lower quality level. Move the slider towards **Sharper Image** to result in a lower frame rate at a higher quality level. The range is from 0 to 100 in steps of 5.<br>Note: This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier. |

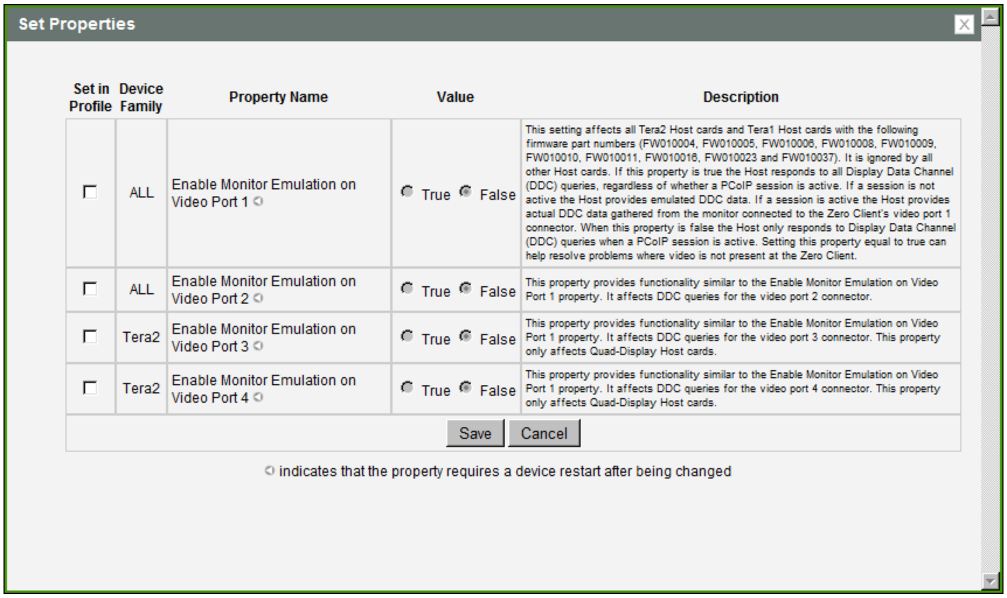
# 5.12 Configuring Monitor Emulation

## 5.12.1 MC: Monitor Emulation

The **Monitor Emulation** page lets you configure a profile to enable or disable the monitor emulation feature. This page is only available on host cards still using monitor emulation. It is disabled and non-editable on the client.

Some PCs and workstations do not boot if a display is not attached. Monitor emulation presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host.

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable Monitor Emulation on Video Port 1 ◁ | ○ True ● False | This setting affects all Tera2 Host cards and Tera1 Host cards with the following firmware part numbers (FW010004, FW010005, FW010006, FW010008, FW010009, FW010010, FW010011, FW010016, FW010023 and FW010037). It is ignored by all other Host cards. If this property is true the Host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active the Host provides emulated DDC data. If a session is active the Host provides actual DDC data gathered from the monitor connected to the Zero Client's video port 1 connector. When this property is false the Host only responds to Display Data Channel (DDC) queries when a PCoIP session is active. Setting this property equal to true can help resolve problems where video is not present at the Zero Client. |
| □ | ALL | Enable Monitor Emulation on Video Port 2 ◁ | ○ True ● False | This property provides functionality similar to the Enable Monitor Emulation on Video Port 1 property. It affects DDC queries for the video port 2 connector. |
| □ | Tera2 | Enable Monitor Emulation on Video Port 3 ◁ | ○ True ● False | This property provides functionality similar to the Enable Monitor Emulation on Video Port 1 property. It affects DDC queries for the video port 3 connector. This property only affects Quad-Display Host cards. |
| □ | Tera2 | Enable Monitor Emulation on Video Port 4 ◁ | ○ True ● False | This property provides functionality similar to the Enable Monitor Emulation on Video Port 1 property. It affects DDC queries for the video port 4 connector. This property only affects Quad-Display Host cards. |

◁ indicates that the property requires a device restart after being changed

**Figure 5-58: MC Monitor Emulation Page**

**Table 5-55: MC Monitor Parameters**

| Parameter | Description |
|---|---|
| Enable Monitor Emulation on Video Port 1 | When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector.<br>When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active.<br>Note: Enabling this field can help resolve problems where video is not present at the client.<br>Note: This property requires a device restart after being changed. |

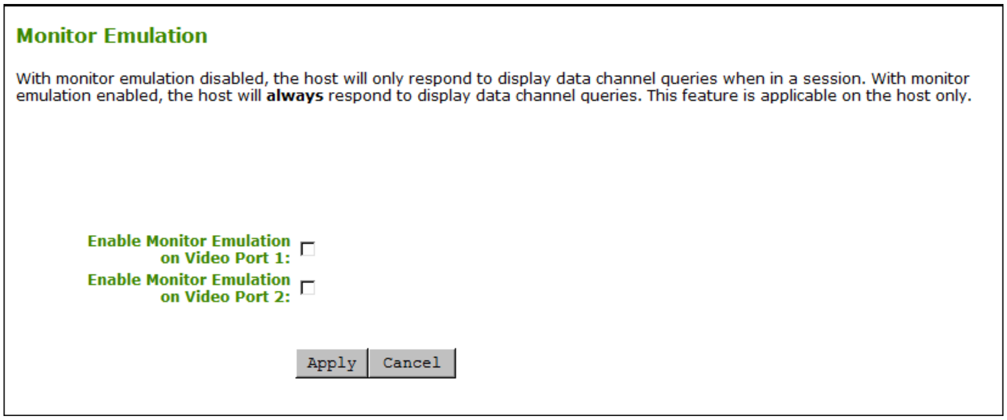
| Parameter | Description |
|---|---|
| Enable Monitor Emulation on Video Port 2 | This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector.<br>Note: This property requires a device restart after being changed. |
| Enable Monitor Emulation on Video Port 3 | This field affects DDC queries for the port 3 connector, and provides functionality similar to that for the port 1 connector.<br>Note: This property requires a device restart after being changed. |
| Enable Monitor Emulation on Video Port 4 | This field affects DDC queries for the port 4 connector, and provides functionality similar to that for the port 1 connector.<br>Note: This property requires a device restart after being changed. |

## 5.12.2 AWI Tera1 Host: Monitor Emulation

The **Monitor Emulation** page lets you enable or disable the monitor emulation feature. This page is only available on host cards still using monitor emulation. It is disabled and non-editable on the client.

Some PCs and workstations do not boot if a display is not attached. Monitor emulation presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host.

You can display this page from the **Configuration > Monitor Emulation** menu.



Monitor Emulation

With monitor emulation disabled, the host will only respond to display data channel queries when in a session. With monitor emulation enabled, the host will **always** respond to display data channel queries. This feature is applicable on the host only.

Enable Monitor Emulation on Video Port 1: □

Enable Monitor Emulation on Video Port 2: □

**Figure 5-59: AWI Tera1 Host Monitor Emulation Page**

**Table 5-56: AWI Tera1 Host Monitor Parameters**

| Parameter | Description |
|---|---|
| Enable Monitor Emulation on DVI-1 | When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector.<br>When disabled, the host only responds to Display Data Channel |

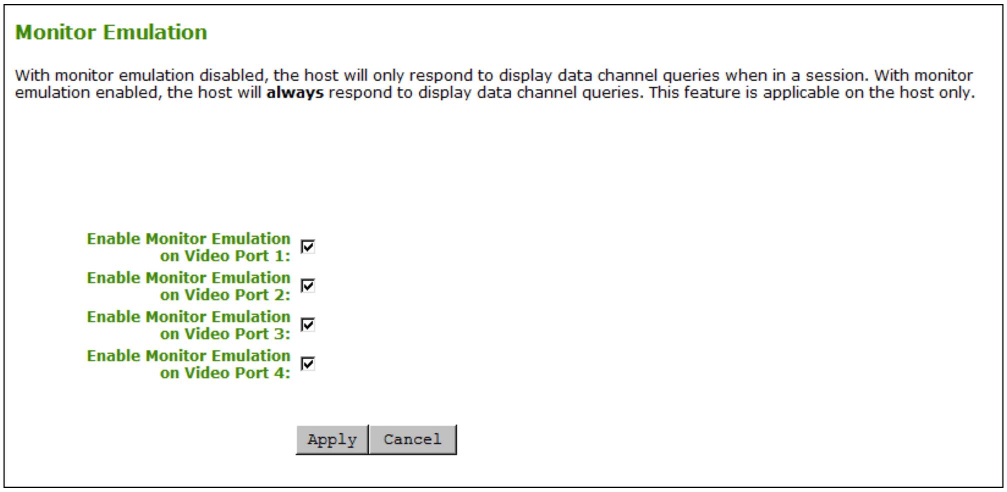
| Parameter | Description |
|---|---|
| | (DDC) queries when a PCoIP session is active.<br>Note: Enabling this field can help resolve problems where video is not present at the client. |
| Enable Monitor Emulation on DVI-2 | This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector. |

## 5.12.3 AWI Tera2 Host: Monitor Emulation

The **Monitor Emulation** page lets you enable or disable the monitor emulation feature. This page is only available on host cards still using monitor emulation. It is disabled and non-editable on the client.

Some PCs and workstations do not boot if a display is not attached. Monitor emulation presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host.

You can display this page from the **Configuration** > **Monitor Emulation** menu.



Monitor Emulation

With monitor emulation disabled, the host will only respond to display data channel queries when in a session. With monitor emulation enabled, the host will **always** respond to display data channel queries. This feature is applicable on the host only.

Enable Monitor Emulation on Video Port 1: ☑

Enable Monitor Emulation on Video Port 2: ☑

Enable Monitor Emulation on Video Port 3: ☑

Enable Monitor Emulation on Video Port 4: ☑

**Figure 5-60: AWI Tera2 Host Monitor Emulation Page**

**Table 5-57: AWI Tera2 Host Monitor Parameters**

| Parameter | Description |
|---|---|
| Enable Monitor Emulation on Video Port 1 | When enabled, the host responds to all Display Data Channel (DDC) queries, regardless of whether a PCoIP session is active. If a session is not active, the host provides emulated DDC data. If a session is active, the host provides actual DDC data gathered from the monitor connected to the client's port 1 connector.<br>When disabled, the host only responds to Display Data Channel (DDC) queries when a PCoIP session is active.<br>Note: Enabling this field can help resolve problems where video is not present at the client. |

| Parameter | Description |
|---|---|
| Enable Monitor Emulation on Video Port 2 | This field affects DDC queries for the port 2 connector, and provides functionality similar to that for the port 1 connector. |
| Enable Monitor Emulation on Video Port 3 | This field affects DDC queries for the port 3 connector, and provides functionality similar to that for the port 1 connector. |
| Enable Monitor Emulation on Video Port 4 | This field affects DDC queries for the port 4 connector, and provides functionality similar to that for the port 1 connector. |

## 5.13 Configuring Time

### 5.13.1 MC: Time Settings

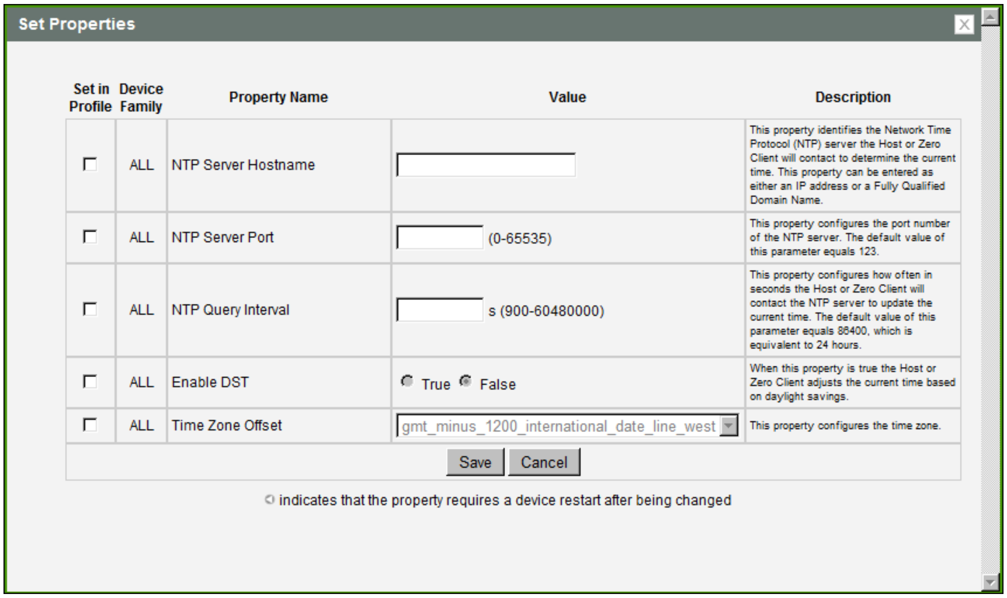
The **Time** page lets you configure a profile with the Network Time Protocol (NTP) parameters to use to allow the host and client event logs to be time-stamped based on NTP time.

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

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

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

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | NTP Server Hostname | | This property identifies the Network Time Protocol (NTP) server the Host or Zero Client will contact to determine the current time. This property can be entered as either an IP address or a Fully Qualified Domain Name. |
| □ | ALL | NTP Server Port | (0-65535) | This property configures the port number of the NTP server. The default value of this parameter equals 123. |
| □ | ALL | NTP Query Interval | s (900-60480000) | This property configures how often in seconds the Host or Zero Client will contact the NTP server to update the current time. The default value of this parameter equals 86400, which is equivalent to 24 hours. |
| □ | ALL | Enable DST | ○ True ● False | When this property is true the Host or Zero Client adjusts the current time based on daylight savings. |
| □ | ALL | Time Zone Offset | gmt_minus_1200_international_date_line_west | This property configures the time zone. |

○ indicates that the property requires a device restart after being changed

**Figure 5-61: MC Time Configuration**

**Table 5-58: MC Time Configuration Parameters**

| Parameter | Description |
|---|---|
| NTP Server Hostname | Configure the IP address or fully qualified domain name (FQDN) of the NTP server that the host or client will contact to determine the current time. |
| NTP Server Port | Configure the port number of the NTP server. The default NTP server port value is 123. |
| NTP Query Interval | Configure how often (in seconds) the host or client will contact the NTP server to update the current time. The default query interval is 86400 seconds, which is equivalent to 24 hours. |
| Enable DST | Enable or disable the automatic adjustment for Daylight Saving Time (DST). |
| Time Zone Offset | Select the desired time zone. |

## 5.13.2 AWI: Time Settings

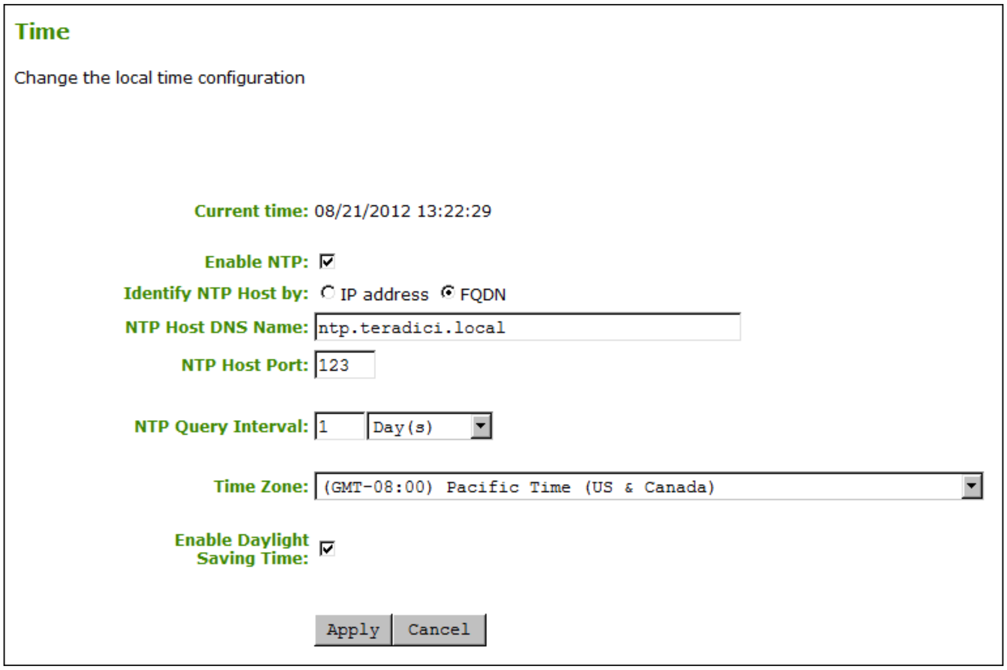
The **Time** page lets you configure Network Time Protocol (NTP) parameters to allow the host and client event logs to be time-stamped based on NTP time.

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

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

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

You can display this page for the host or client from the **Configuration** > **Time** menu.



Time

Change the local time configuration

Current time: 08/21/2012 13:22:29

Enable NTP: ☑

Identify NTP Host by: ○ IP address ● FQDN

NTP Host DNS Name: ntp.teradici.local

NTP Host Port: 123

NTP Query Interval: 1 Day(s)

Time Zone: (GMT-08:00) Pacific Time (US & Canada)

Enable Daylight Saving Time: ☑

**Figure 5-62: AWI Time Page**

**Table 5-59: AWI Time Page Parameters**

| Parameter | Description |
|---|---|
| Current Time | Displays the time based on the NTP. |
| Enable NTP | Enable or disable the NTP feature. |
| Identify NTP Host by | Select if the NTP host is identified by IP address or by fully qualified domain name (FQDN). If NTP is disabled, this field is not required and is not editable. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose.<br>• **IP Address**: Shows the NTP Host IP address<br>• **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. |

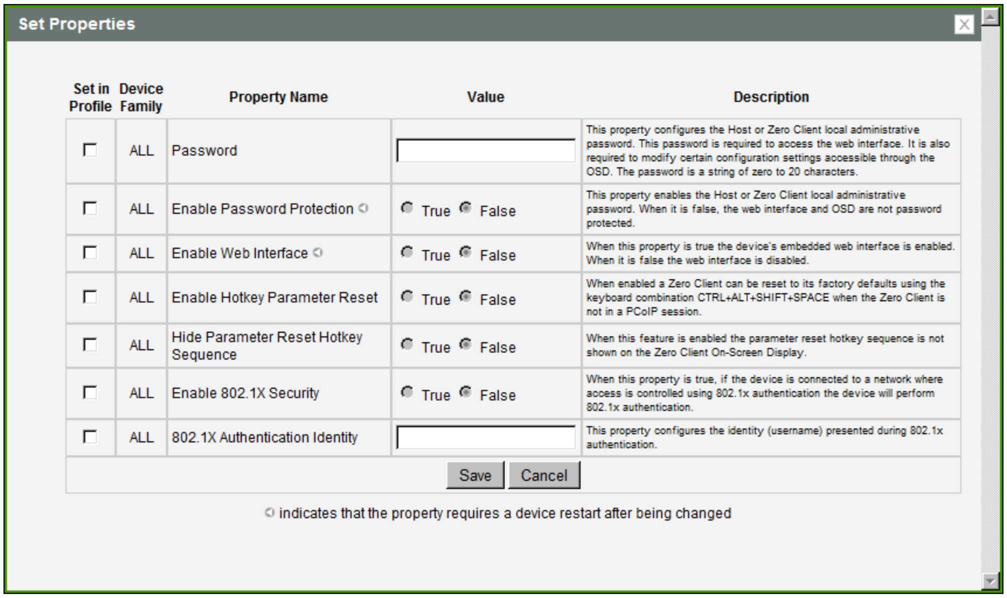
| Parameter | Description |
|---|---|
| Enable Daylight Savings Time | Enable or disable the automatic adjustment for Daylight Saving Time (DST). |

# 5.14 Configuring Security

## 5.14.1 MC: Security Settings

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

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Password | | This property configures the Host or Zero Client local administrative password. This password is required to access the web interface. It is also required to modify certain configuration settings accessible through the OSD. The password is a string of zero to 20 characters. |
| □ | ALL | Enable Password Protection ◁ | ○ True ● False | This property enables the Host or Zero Client local administrative password. When it is false, the web interface and OSD are not password protected. |
| □ | ALL | Enable Web Interface ◁ | ○ True ● False | When this property is true the device's embedded web interface is enabled. When it is false the web interface is disabled. |
| □ | ALL | Enable Hotkey Parameter Reset | ○ True ● False | When enabled a Zero Client can be reset to its factory defaults using the keyboard combination CTRL+ALT+SHIFT+SPACE when the Zero Client is not in a PCoIP session. |
| □ | ALL | Hide Parameter Reset Hotkey Sequence | ○ True ● False | When this feature is enabled the parameter reset hotkey sequence is not shown on the Zero Client On-Screen Display. |
| □ | ALL | Enable 802.1X Security | ○ True ● False | When this property is true, if the device is connected to a network where access is controlled using 802.1x authentication the device will perform 802.1x authentication. |
| □ | ALL | 802.1X Authentication Identity | | This property configures the identity (username) presented during 802.1x authentication. |

◁ indicates that the property requires a device restart after being changed

**Figure 5-63: MC Security Configuration**

**Table 5-60: MC Security Configuration Parameters**

| Parameter | Description |
|---|---|
| Password | Enter the password for the host or client Administrative Web Interface (AWI). This password is also required to modify certain configuration settings accessible through the client On Screen Display (OSD).<br>This field accepts a string of zero to 20 characters. |
| Enable Password Protection | When enabled, the host or client AWI password is required. When disabled, the AWI and OSD are not password protected. |
| Enable Web Interface | When enabled, the host or client's AWI is enabled. When disabled, the AWI is disabled. |

| Parameter | Description |
|---|---|
| Enable Hotkey Parameter Reset | When enabled, the client can be reset to its factory defaults using the keyboard combination Ctrl+Alt+Shift+Space when the client is not in a PCoIP session. |
| Hide Parameter Reset Hotkey Sequence | When enabled, the reset hotkey sequence is not shown on the client OSD. |
| Enable 802.1X Security | When enabled, the device will perform 802.1X authentication if it is connected to a network where access is controlled using 802.1X authentication. |
| 802.1X Authentication Identity | Configure the username to present for 802.1X authentication. |

### 5.14.2 AWI: Help for Security Settings

Security settings for the AWI are located on the AWI's Network Settings page (accessed from the **Configuration > Network** menu). See the descriptions for the following fields on this page:

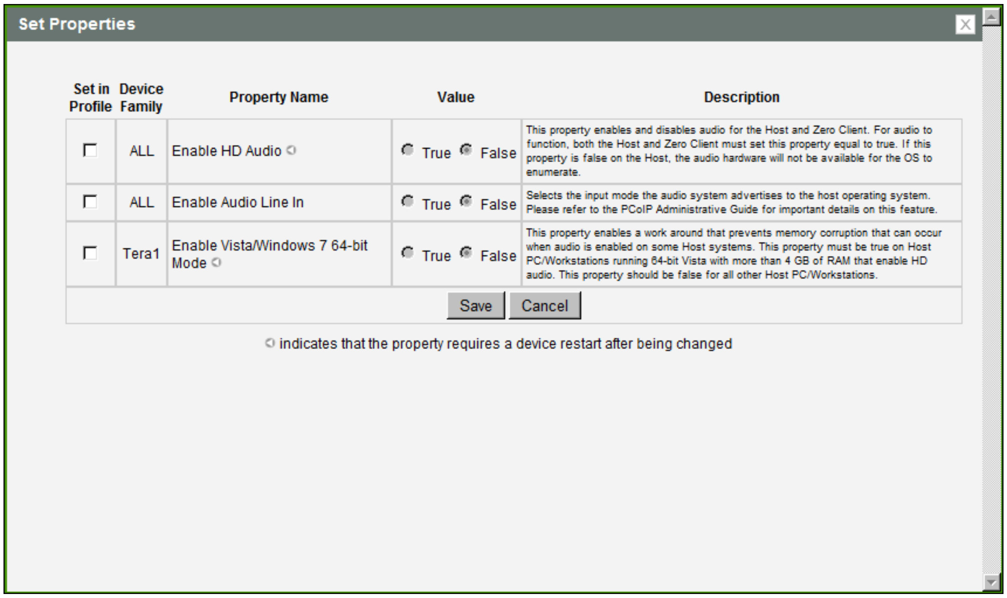
- Enable 802.1X Security
- Authentication
- Identity
- Client Certificate

## 5.15 Configuring Audio Permissions

### 5.15.1 MC: Audio Permissions

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

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable HD Audio ◁ | ○ True ● False | This property enables and disables audio for the Host and Zero Client. For audio to function, both the Host and Zero Client must set this property equal to true. If this property is false on the Host, the audio hardware will not be available for the OS to enumerate. |
| □ | ALL | Enable Audio Line In | ○ True ● False | Selects the input mode the audio system advertises to the host operating system. Please refer to the PCoIP Administrative Guide for important details on this feature. |
| □ | Tera1 | Enable Vista/Windows 7 64-bit Mode ◁ | ○ True ● False | This property enables a work around that prevents memory corruption that can occur when audio is enabled on some Host systems. This property must be true on Host PC/Workstations running 64-bit Vista with more than 4 GB of RAM that enable HD audio. This property should be false for all other Host PC/Workstations. |

◁ indicates that the property requires a device restart after being changed

**Figure 5-64: MC Audio Permissions**

**Table 5-61: MC Audio Permissions Parameters**

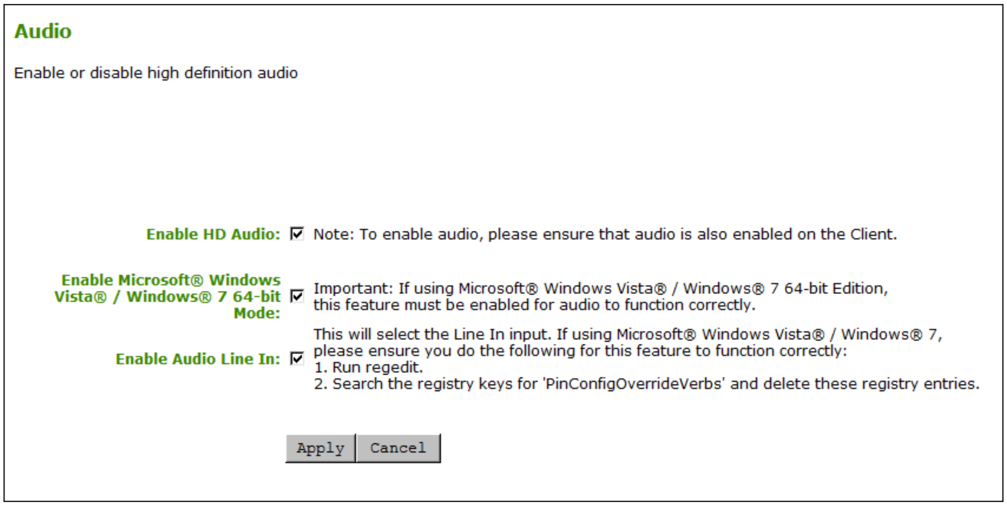
| Parameter | Description |
|---|---|
| Enable HD Audio | Enable to configure audio support on the device.<br>Note: This property must be enabled on both the host and the client.<br>When disabled, the audio hardware is not available for the host operating system to enumerate.<br>Note: This property requires a device restart after being changed. |
| Enable Audio Line In | This property determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input. |
| Enable Microsoft Windows Vista 64-bit Mode | Enable this option for Windows Vista 64-bit and Windows 7 64-bit version operation systems.<br>Warning: Do NOT use this mode with Windows XP 64 or 32-bit operating systems.<br>You do not have to enable the 64-bit mode for Linux 64-bit operating systems. Linux kernels should be compiled with the latest PCoIP audio CODEC support.<br>Note: This property requires a device restart after being changed. |

## 5.15.2 AWI Tera1 Host: Audio Permissions

You can configure the audio permissions from the **Initial Setup** page when you start your first session.

For subsequent sessions, use the **Audio** page (accessed from the **Permissions** > **Audio** menu) to configure the audio permissions for the device. After you update the options on this page, click **Apply** to save your changes.

To display the **Audio** page from the Administrative Web Interface, select the **Permissions** menu, and then click **Audio**.



Audio

Enable or disable high definition audio

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

Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode: ☑ Important: If using Microsoft® Windows Vista® / Windows® 7 64-bit Edition, this feature must be enabled for audio to function correctly.

Enable Audio Line In: ☑ This will select the Line In input. If using Microsoft® Windows Vista® / Windows® 7, please ensure you do the following for this feature to function correctly:
1. Run regedit.
2. Search the registry keys for 'PinConfigOverrideVerbs' and delete these registry entries.

**Figure 5-65: AWI Tera1 Host Audio Page**

**Table 5-62: AWI Tera1 Host Audio Page Parameters**

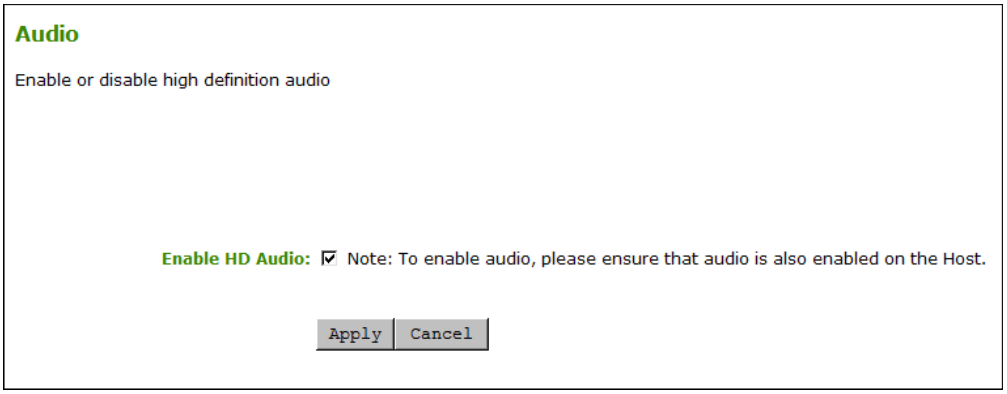
| Parameter | Description |
|---|---|
| Enable HD Audio | Enable to configure audio support on the device.<br>Note: This property must be enabled on both the host and the client.<br>When disabled, the audio hardware is not available for the host operating system to enumerate. |
| Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode | Enable this option for Windows Vista 64-bit and Windows 7 64-bit version operation systems.<br>Warning: Do NOT use this mode with Windows XP 64 or 32-bit operating systems.<br>You do not have to enable the 64-bit mode for Linux 64-bit operating systems. Linux kernels should be compiled with the latest PCoIP audio CODEC support. |
| Enable Audio Line In | This property determines the input mode the audio system advertises to the host operating system. When enabled, the line-in connector found on the client is used as a standard line-in input. When disabled, the line-in connector found on the client is used as a microphone input.<br>Note: Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device. |

### 5.15.3 AWI Client: Audio Permissions

You can configure the audio permissions from the Initial Setup page when you start your first session.

For subsequent sessions, use the **Audio** page (accessed from the **Permissions** > **Audio** menu) to configure the audio permissions for the device. After you update the options on this page, click **Apply** to save your changes.

To display the **Audio** page from the Administrative Web Interface, select the **Permissions** menu, and then click **Audio**.


Audio

Enable or disable high definition audio

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

**Figure 5-66: AWI Client Audio Page**

**Table 5-63: AWI Client Audio Page Parameters**

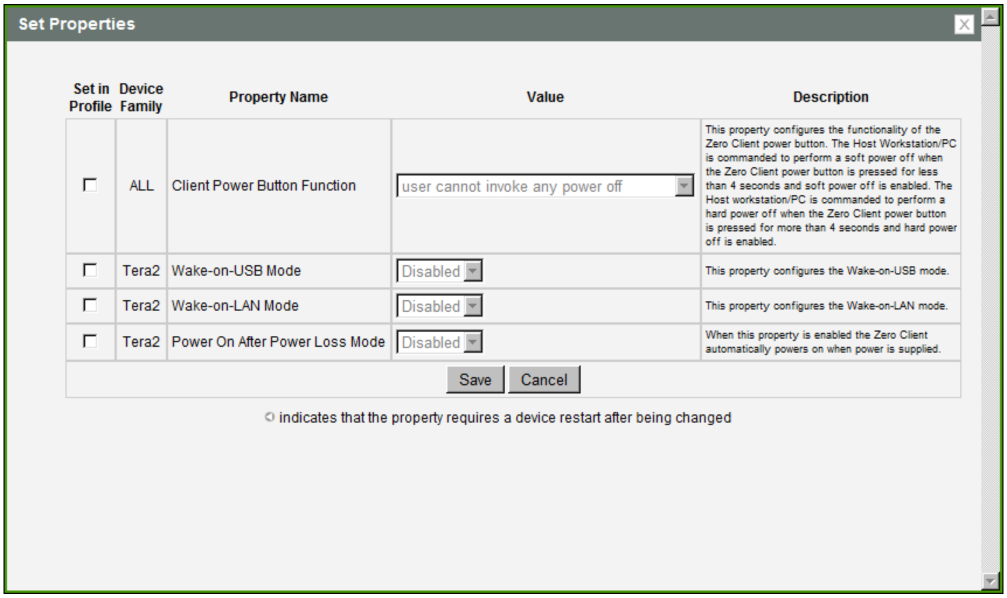
| Parameter | Description |
|---|---|
| Enable HD Audio | Enable to configure audio support on the device.<br>Note: This property must be enabled on both the host and the client.<br>When disabled, the audio hardware is not available for the host operating system to enumerate. |

## 5.16 Configuring Power Permissions

### 5.16.1 MC: Power Permissions

The settings on this page let you configure a profile with power permissions for hosts and clients.

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Client Power Button Function | user cannot invoke any power off | This property configures the functionality of the Zero Client power button. The Host Workstation/PC is commanded to perform a soft power off when the Zero Client power button is pressed for less than 4 seconds and soft power off is enabled. The Host workstation/PC is commanded to perform a hard power off when the Zero Client power button is pressed for more than 4 seconds and hard power off is enabled. |
| □ | Tera2 | Wake-on-USB Mode | Disabled | This property configures the Wake-on-USB mode. |
| □ | Tera2 | Wake-on-LAN Mode | Disabled | This property configures the Wake-on-LAN mode. |
| □ | Tera2 | Power On After Power Loss Mode | Disabled | When this property is enabled the Zero Client automatically powers on when power is supplied. |

○ indicates that the property requires a device restart after being changed

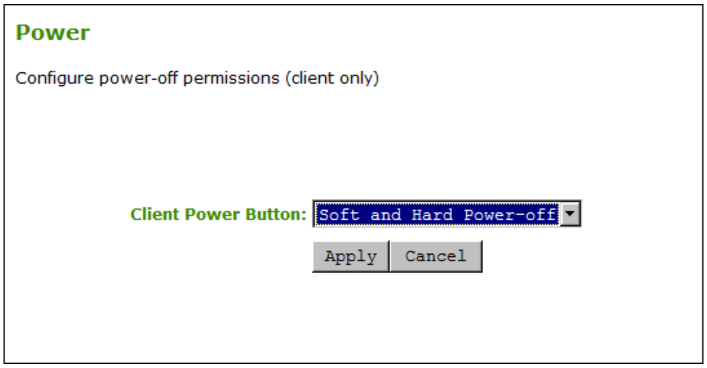
**Figure 5-67: MC Power Permissions**

**Table 5-64: MC Power Permissions Parameters**

| Parameter | Description |
|---|---|
| Client Power Button Function | This property configures the functionality of the client's remote PC button.<br>The host is commanded to perform a soft power off (i.e., to go into sleep mode) when the client's remote PC button is pressed for less than four seconds and soft power off is enabled.<br>The host is commanded to perform a hard power off (i.e., to shut down) when the client's remote PC button is pressed for more than four seconds and hard power off is enabled.<br>Select from the following options:<br>• **user cannot invoke any power off**: Users cannot shut down the host or put it in sleep mode.<br>• **user can only invoke a hard power off**: Users can shut down the host but not put it in sleep mode.<br>• **user can only invoke a soft power off**: Users can put the host in sleep mode but not shut it down.<br>• **user can invoke soft and hard power offs**: Users can put the host in sleep mode and shut it down. |
| Wake-on-USB Mode | When enabled, configures the host to wake up from sleep mode when the user moves the mouse or presses a key on the keyboard. |
| Wake-on-LAN Mode | When enabled, configures the host to wake up from sleep mode when the user presses the client's **Remote PC** button or clicks the **Connect** button on the **Connect** window. |
| Power On After Power Loss Mode | When enabled, the client automatically powers back on when power is supplied. |

## 5.16.2 AWI Tera1 Client: Power Permissions

The **Power** page lets you configure host power-off permissions for the client. You can access this page from the **Permissions** > **Power** menu.



Power

Configure power-off permissions (client only)

Client Power Button: Soft and Hard Power-off

**Figure 5-68: AWI Tera1 Client Power Page**

**Table 5-65: AWI Tera1 Client Power Page Parameters**

| Parameter | Description |
|---|---|
| Client Power Button | This property configures the functionality of the client's remote PC button.<br>The host is commanded to perform a soft power off (i.e., to go into sleep mode) when the client's remote PC button is pressed for less than four seconds and soft power off is enabled.<br>The host is commanded to perform a hard power off (i.e., to shut down) when the client's remote PC button is pressed for more than four seconds and hard power off is enabled.<br>Select from the following options:<br>• **Power-off not permitted**: Users cannot shut down the host or put it in sleep mode.<br>• **Soft Power-off only**: Users can put the host in sleep mode but not shut it down.<br>• **Hard Power-off only**: Users can shut down the host but not put it in sleep mode.<br>• **Soft and Hard Power-off**: Users can put the host in sleep mode and shut it down. |

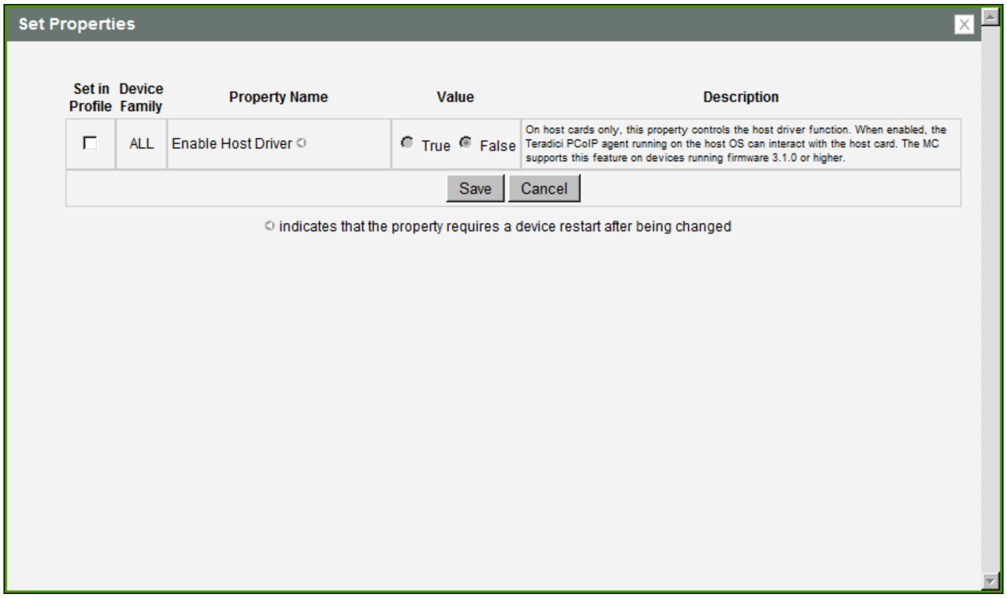
# 5.17 Configuring the Host Driver Function

## 5.17.1 MC: Host Driver Function

The setting on this page lets you configure a profile to enable or disable the PCoIP host software UI on the host computer.

Note: For information about how to install and use the PCoIP host software, see the "PCoIP Host Software User Guide (TER0810001)".

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



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

◌ indicates that the property requires a device restart after being changed

**Figure 5-69: MC Host Driver Configuration**

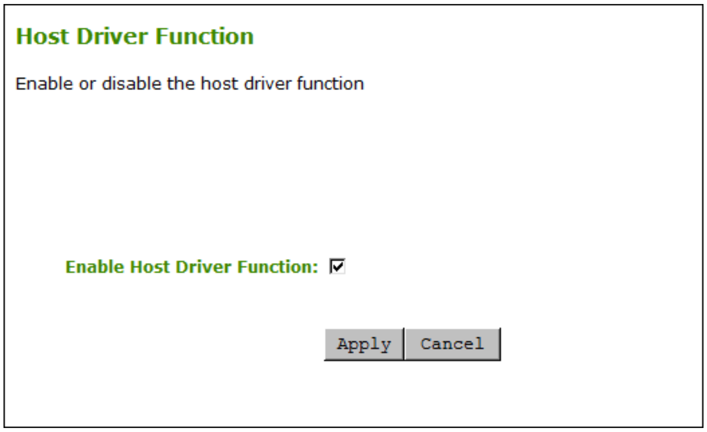
**Table 5-66: MC Host Driver Configuration Parameters**

| Parameter | Description |
|---|---|
| Enable Host Driver | When enabled, lets you access the PCoIP host software UI on the host computer. This software lets users enable features such as the following:<br>• Using the local cursor and keyboard feature<br>• Locking the host PC when a session is terminated<br>• Using the Wake-on-LAN function<br>• Viewing host and client network parameters<br>• Disconnecting a session<br>• Viewing host statistics and connection information<br>• Using the client display topology settings on the host<br>When disabled, you do not have access to the PCoIP host software UI on the host computer.<br>Note: This property requires a device restart after being changed. |

## 5.17.2 AWI Host: Host Driver Function

The setting on this page lets you enable or disable the PCoIP host software UI on the host computer. You can access this page from the **Configuration > Host Driver Function** menu.

Note: For information about how to install and use the PCoIP host software, see the "PCoIP Host Software User Guide (TER0810001)".



Host Driver Function

Enable or disable the host driver function

Enable Host Driver Function: ☑

Figure 5-70: AWI Host Driver Function Page

Table 5-67: AWI Host Driver Function Parameters

| Parameter | Description |
|---|---|
| Enable Host Driver Function | When enabled, lets you access the PCoIP host software UI on the host computer. This software lets users enable features such as the following:<br>• Using the local cursor and keyboard feature<br>• Locking the host PC when a session is terminated<br>• Using the Wake-on-LAN function<br>• Viewing host and client network parameters<br>• Disconnecting a session<br>• Viewing host statistics and connection information<br>• Using the client display topology settings on the host<br>When disabled, you do not have access to the PCoIP host software UI on the host computer. |

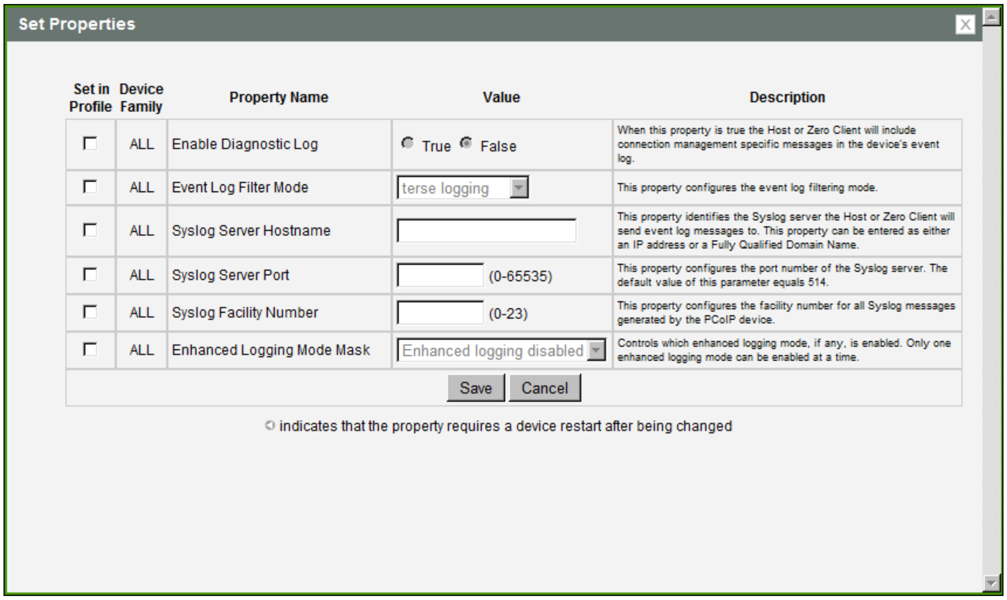
# 5.18 Configuring the Event Log

## 5.18.1 MC: Event Log Settings

The settings on this page let you configure a profile with event log messaging to use for a host or client, and to set the log filtering mode on a device.

You can also enable and configure syslog as the logging protocol to use for collecting and reporting events.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable Diagnostic Log | ○ True ● False | When this property is true the Host or Zero Client will include connection management specific messages in the device's event log. |
| □ | ALL | Event Log Filter Mode | terse logging | This property configures the event log filtering mode. |
| □ | ALL | Syslog Server Hostname | | This property identifies the Syslog server the Host or Zero Client will send event log messages to. This property can be entered as either an IP address or a Fully Qualified Domain Name. |
| □ | ALL | Syslog Server Port | (0-65535) | This property configures the port number of the Syslog server. The default value of this parameter equals 514. |
| □ | ALL | Syslog Facility Number | (0-23) | This property configures the facility number for all Syslog messages generated by the PCoIP device. |
| □ | ALL | Enhanced Logging Mode Mask | Enhanced logging disabled | Controls which enhanced logging mode, if any, is enabled. Only one enhanced logging mode can be enabled at a time. |

indicates that the property requires a device restart after being changed

**Figure 5-71: MC Event Log Control**

**Table 5-68: MC Event Log Control Parameters**

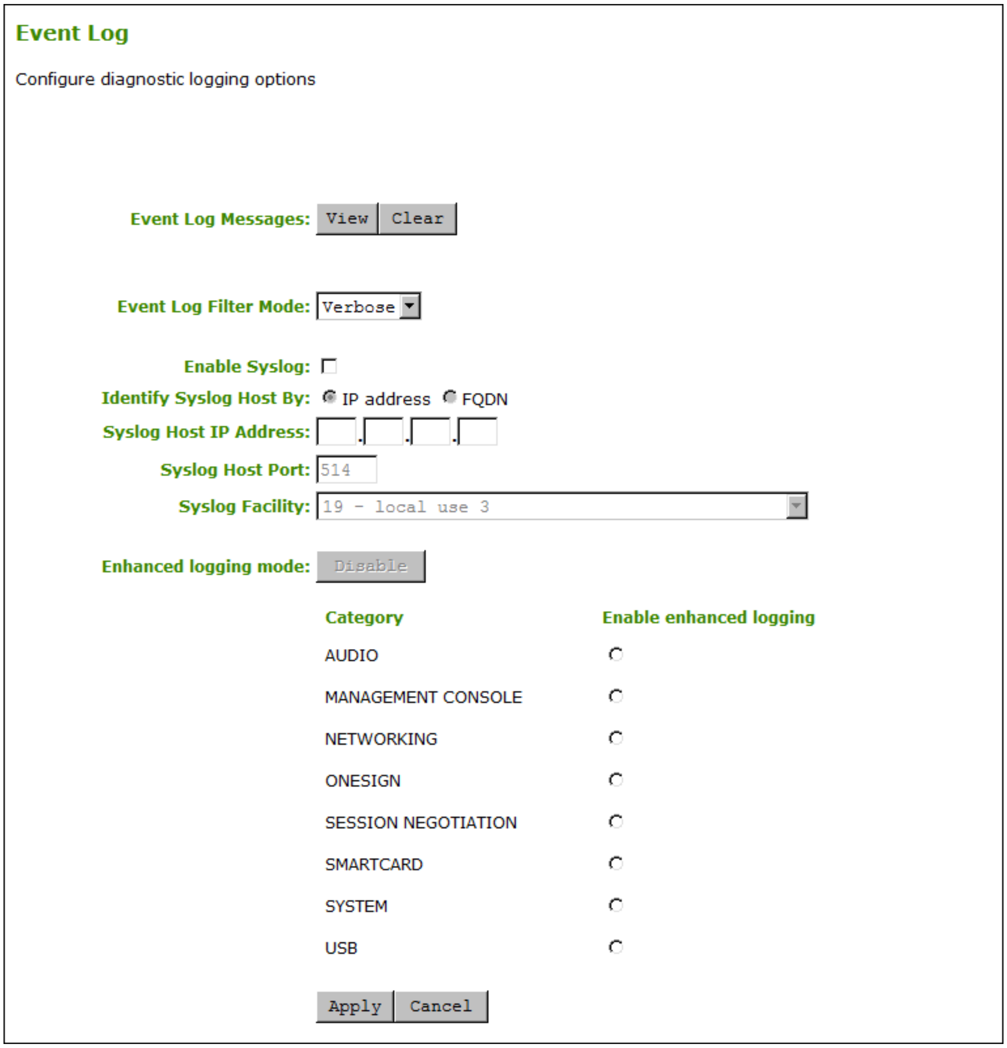
| Parameter | Description |
|---|---|
| Enable Diagnostic Log | When enabled, the device will include connection management-specific messages in the device's event log. |
| Event Log Filter Mode | Configure the event log filtering mode as terse or verbose. |
| Syslog Server Hostname | Enter the IP address or fully qualified domain name of the syslog server to which the host or client will send event log messages. |
| Syslog Server Port | Enter port number of the syslog server.<br>Note: The default port number value is 514. |
| Syslog Facility Number | Enter the facility number for all syslog messages generated by the device. |
| Enhanced Logging Mode Mask | To enable enhanced logging mode, select one of the following categories:<br>• Audio<br>• Management Console<br>• Video<br>• Networking<br>• Session Negotiation<br>• Smart Card<br>• System<br>• USB<br>• OneSign |

| Parameter | Description |
|---|---|
| | Note: You can only enable enhanced logging for one of the above categories at any one time. |

## 5.18.2 AWI: Event Log Settings

The **Event Log** page lets you view and clear event log messages from the host or client, and set the log filtering mode on the device. You can access this page for the host or client from the **Diagnostics > Event Log** menu.

You can also enable and configure syslog as the logging protocol to use for collecting and reporting events.



Event Log

Configure diagnostic logging options

Event Log Filter Mode: Verbose

Enable Syslog: □

Identify Syslog Host By: ● IP address ○ FQDN

Syslog Host IP Address: . . .

Syslog Host Port: 514

Syslog Facility: 19 - local use 3

| Category | Enable enhanced logging |
|---|---|
| AUDIO | ○ |
| MANAGEMENT CONSOLE | ○ |
| NETWORKING | ○ |
| ONESIGN | ○ |
| SESSION NEGOTIATION | ○ |
| SMARTCARD | ○ |
| SYSTEM | ○ |
| USB | ○ |

**Figure 5-72: AWI Event Log Page**

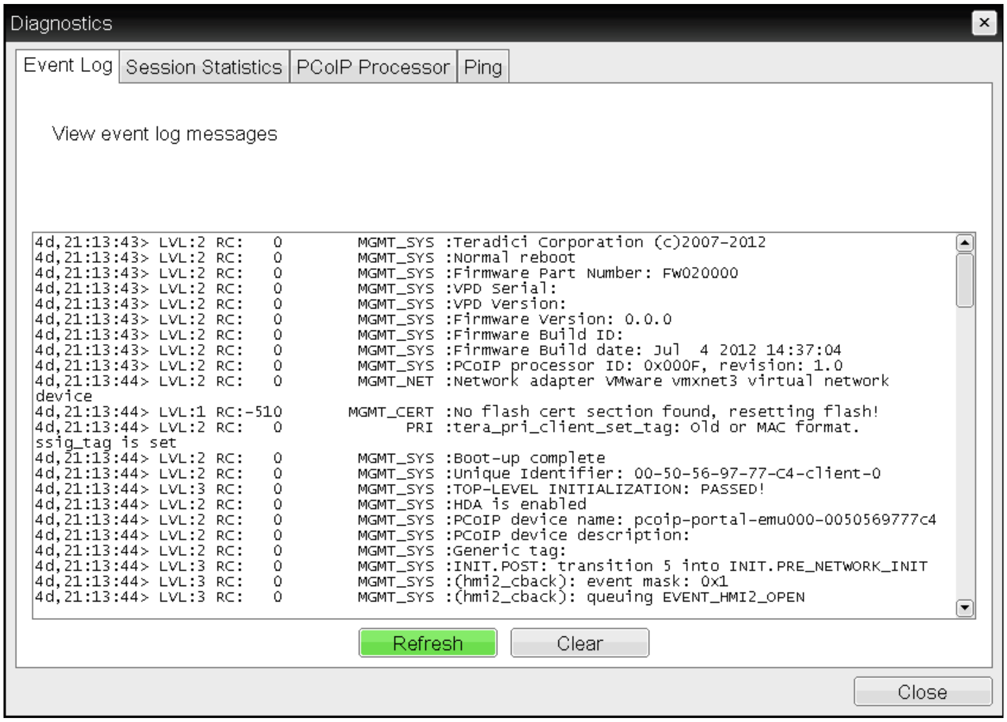
**Table 5-69: AWI Event Log Page Parameters**

| **Parameter** | **Description** |
|---|---|
| Event log Messages | **View:** Click to open a browser page that displays the event log messages (with timestamp information) stored on the device. Press **F5** to refresh the browser page log information.<br>**Clear:** Click to delete all event log messages stored on the device. |
| Event Log Filter Mode | Click the pull-down menu to select an event log filtering mode:<br>• **Verbose** (default setting)<br>• **Terse** |
| Enable Syslog | Enable or disable the syslog standard as the logging mechanism for the device.<br>Note: If syslog is enabled, you must configure the remaining fields. If syslog is disabled, these fields are non-editable. |
| Identify Syslog Host By | Choose if the syslog server host is identified by IP address or by fully qualified domain name (FQDN). |
| Syslog Host IP Address / Syslog Host DNS name | The parameter that displays depends on which option you choose to identify the syslog server host:<br>• **IP Address**: Enter the IP address for the syslog server host.<br>• **FQDN:** Enter the DNS name for the syslog server host.<br>Note: If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. |
| Syslog Host Port | Enter port number of the syslog server.<br>Note: The default port number value is 514. |
| Syslog Facility | The facility is a number attached to every syslog message used to categorize the source of the syslog messages. The facility is part of the standard syslog header and can be interpreted by all syslog servers.<br>Enter a facility to suit your logging needs. For example, you could configure devices as follows:<br>• Zero clients to use facility 19<br>• Cisco routers to use facility 20<br>• VMware ESX hosts to use facility 21<br>Note: The default facility is set to “19 – local use 3”. Cisco routers default to “23 – local use 7”. |
| Enhanced logging mode | To enable enhanced logging mode, select one of the following categories:<br>• Audio<br>• Management Console<br>• Video<br>• Networking<br>• Session Negotiation |

| Parameter | Description |
|---|---|
| | • Smart Card<br>• System<br>• USB<br>• OneSign<br>Note: You can only enable enhanced logging for one of the above categories at any one time. |

### 5.18.3 OSD: Event Log Settings

The **Event Log** page lets you view, refresh, and clear event log messages from the client. You can access this page from the **Options** > **Diagnostics** > **Event Log** menu.



```
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Teradici Corporation (c)2007-2012
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Normal reboot
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Firmware Part Number: FW020000
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :VPD Serial:
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :VPD Version:
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Firmware Version: 0.0.0
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Firmware Build ID:
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :Firmware Build date: Jul  4 2012 14:37:04
4d,21:13:43> LVL:2 RC:   0        MGMT_SYS :PCoIP processor ID: 0x000F, revision: 1.0
4d,21:13:44> LVL:2 RC:   0        MGMT_NET :Network adapter VMware vmxnet3 virtual network
device
4d,21:13:44> LVL:1 RC:-510       MGMT_CERT :No flash cert section found, resetting flash!
4d,21:13:44> LVL:2 RC:   0             PRI :tera_pri_client_set_tag: Old or MAC format.
ssig_tag is set
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :Boot-up complete
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :Unique Identifier: 00-50-56-97-77-C4-client-0
4d,21:13:44> LVL:3 RC:   0        MGMT_SYS :TOP-LEVEL INITIALIZATION: PASSED!
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :HDA is enabled
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :PCoIP device name: pcoip-portal-emu000-0050569777c4
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :PCoIP device description:
4d,21:13:44> LVL:2 RC:   0        MGMT_SYS :Generic tag:
4d,21:13:44> LVL:3 RC:   0        MGMT_SYS :INIT.POST: transition 5 into INIT.PRE_NETWORK_INIT
4d,21:13:44> LVL:3 RC:   0        MGMT_SYS :(hmi2_cback): event mask: 0x1
4d,21:13:44> LVL:3 RC:   0        MGMT_SYS :(hmi2_cback): queuing EVENT_HMI2_OPEN
```

**Figure 5-73: OSD Event Log Page**

**Table 5-70: OSD Event Log Page Parameters**

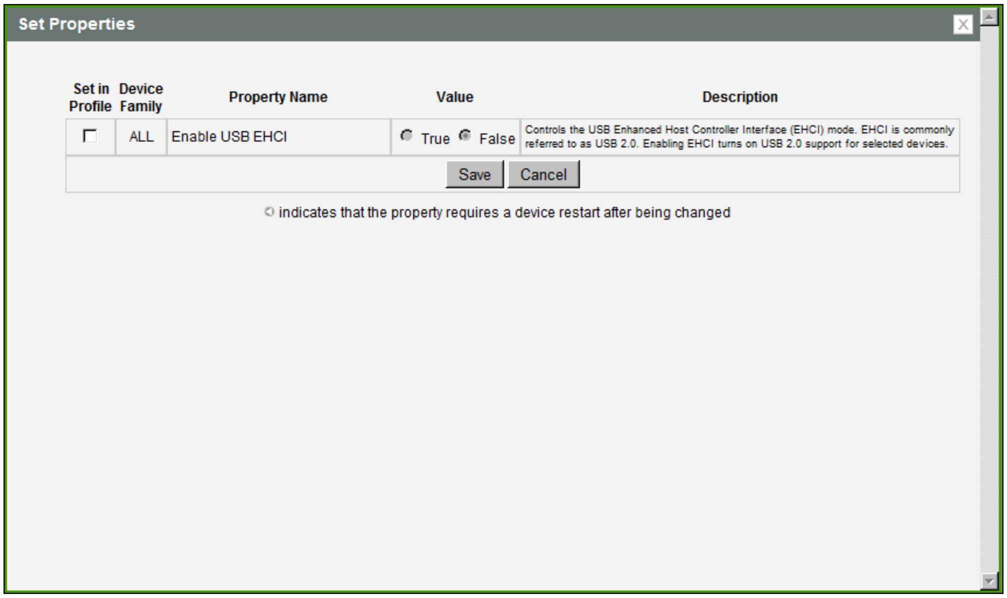
| Parameter | Description |
|---|---|
| Refresh | Click to refresh the log information displayed on this page. |
| Clear | Click to delete all event log messages stored on the device. |

# 5.19 Configuring Peripherals

## 5.19.1 MC: Peripheral Settings

The setting on this page lets you configure a profile to enable or disable USB Enhanced Host Controller Interface (EHCI) mode on selected devices.

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



Set Properties

| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable USB EHCI | ○ True ● False | Controls the USB Enhanced Host Controller Interface (EHCI) mode. EHCI is commonly referred to as USB 2.0. Enabling EHCI turns on USB 2.0 support for selected devices. |

○ indicates that the property requires a device restart after being changed

**Figure 5-74: MC Peripheral Configuration**

**Table 5-71: MC Peripheral Configuration Parameters**

| Parameter | Description |
|---|---|
| Enable USB EHCI | When enabled, configures EHCI (USB 2.0) for devices connected directly to zero client USB ports for sessions with a host running VMware View 4.6 or later.<br>Note: This feature cannot be enabled on clients with less than 128 MB of RAM. Devices with isochronous endpoints will not operate at USB 2.0 speeds. |

## 5.19.2 AWI Client: Help for Peripheral Settings

Peripheral USB EHCI settings for the AWI are located on the AWI Client: USB Permissions page (accessed from the **Permissions** > **USB** menu).

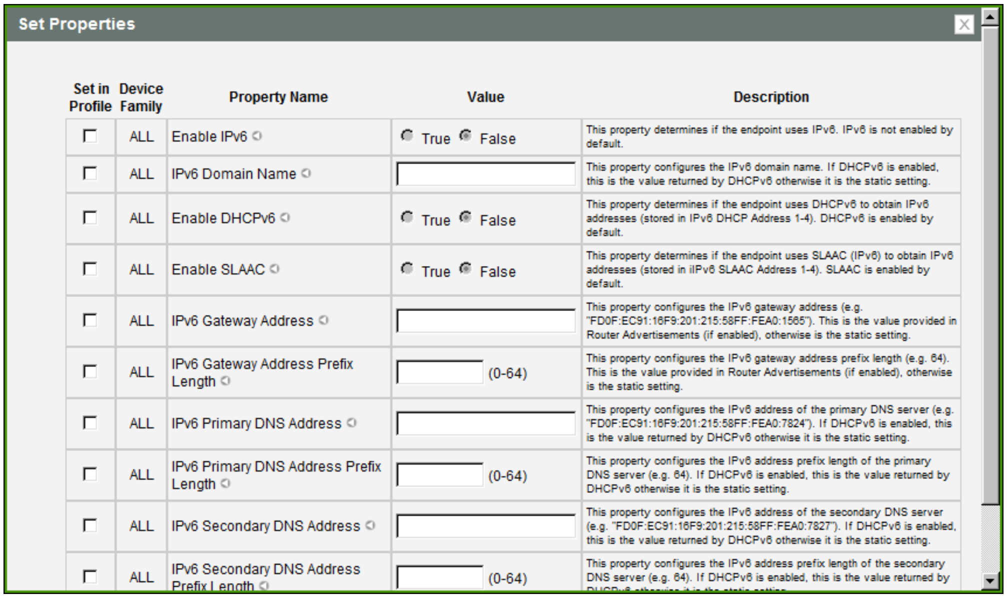
# 5.20 Configuring IPv6

## 5.20.1 MC: IPv6 Settings

The settings on this page let you configure a profile to enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware View.

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



| Set in Profile | Device Family | Property Name | Value | Description |
|---|---|---|---|---|
| □ | ALL | Enable IPv6 | ○ True ● False | This property determines if the endpoint uses IPv6. IPv6 is not enabled by default. |
| □ | ALL | IPv6 Domain Name | | This property configures the IPv6 domain name. If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting. |
| □ | ALL | Enable DHCPv6 | ○ True ● False | This property determines if the endpoint uses DHCPv6 to obtain IPv6 addresses (stored in IPv6 DHCP Address 1-4). DHCPv6 is enabled by default. |
| □ | ALL | Enable SLAAC | ○ True ● False | This property determines if the endpoint uses SLAAC (IPv6) to obtain IPv6 addresses (stored in iIPv6 SLAAC Address 1-4). SLAAC is enabled by default. |
| □ | ALL | IPv6 Gateway Address | | This property configures the IPv6 gateway address (e.g. "FD0F:EC91:16F9:201:215:58FF:FEA0:1565"). This is the value provided in Router Advertisements (if enabled), otherwise is the static setting. |
| □ | ALL | IPv6 Gateway Address Prefix Length | (0-64) | This property configures the IPv6 gateway address prefix length (e.g. 64). This is the value provided in Router Advertisements (if enabled), otherwise is the static setting. |
| □ | ALL | IPv6 Primary DNS Address | | This property configures the IPv6 address of the primary DNS server (e.g. "FD0F:EC91:16F9:201:215:58FF:FEA0:7824"). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting. |
| □ | ALL | IPv6 Primary DNS Address Prefix Length | (0-64) | This property configures the IPv6 address prefix length of the primary DNS server (e.g. 64). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting. |
| □ | ALL | IPv6 Secondary DNS Address | | This property configures the IPv6 address of the secondary DNS server (e.g. "FD0F:EC91:16F9:201:215:58FF:FEA0:7827"). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting. |
| □ | ALL | IPv6 Secondary DNS Address Prefix Length | (0-64) | This property configures the IPv6 address prefix length of the secondary DNS server (e.g. 64). If DHCPv6 is enabled, this is the value returned by |

**Figure 5-75: MC IPv6 Configuration**

**Table 5-72: MC IPv6 Configuration Parameters**

| Parameter | Description |
|---|---|
| Enable IPv6 | This property determines if the device uses IPv6. IPv6 is not enabled by default.<br>Note: This property requires a device restart after being changed. |
| IPv6 Domain Name | If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| Enable DHCPv6 | Determines if the device uses DHCPv6 to obtain IPv6 addresses (stored in IPv6 DHCP Address 1-4). DHCPv6 is enabled by default.<br>Note: This property requires a device restart after being changed. |
| Enable SLAAC | Determines if the endpoint uses Stateless Address Auto-configuration (SLAAC IPv6) to obtain IPv6 addresses (stored in IPv6 |

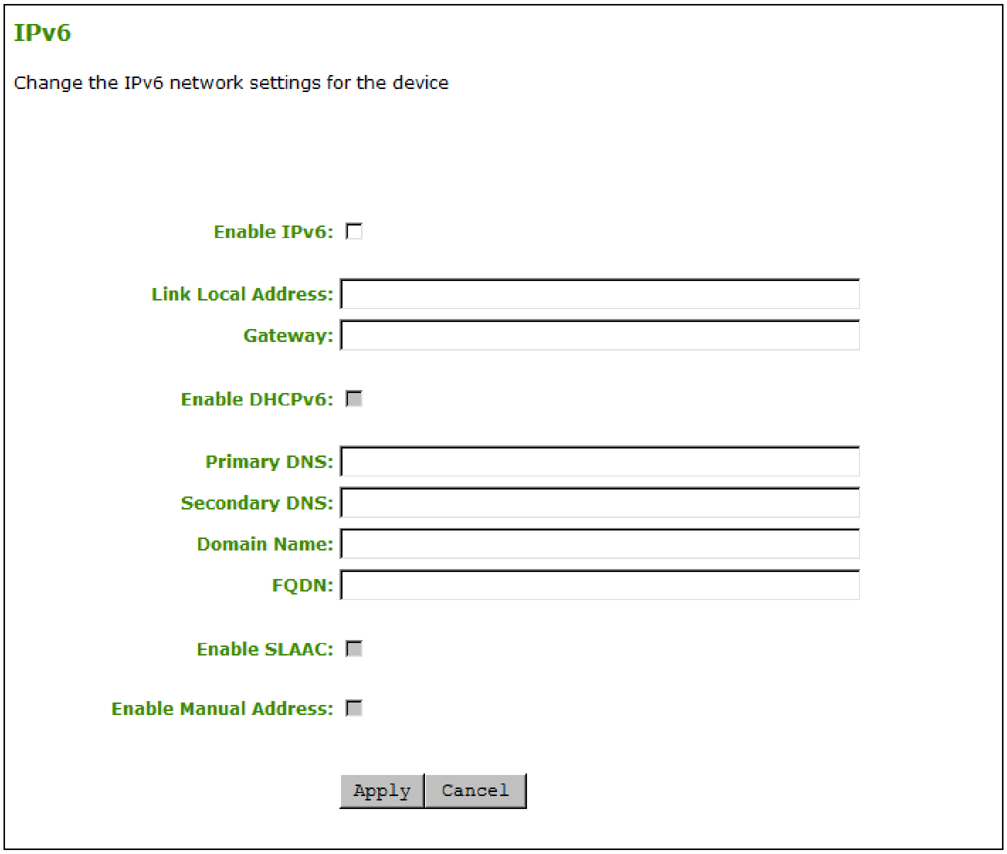
| Parameter | Description |
|---|---|
| | SLAAC Address 1-4). SLAAC is enabled by default.<br>Note: This property requires a device restart after being changed. |
| IPv6 Gateway Address | Configures the IPv6 gateway address (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:1565"). This is the value provided in Router Advertisements (if enabled); otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| IPv6 Gateway Address Prefix Length | Configures the IPv6 gateway address prefix length (e.g., 64). This is the value provided in Router Advertisements (if enabled); otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| IPv6 Primary DNS Address | Configures the IPv6 address of the primary DNS server (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:7824"). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| IPv6 Primary DNS Address Prefix Length | Configures the IPv6 address prefix length of the primary DNS server (e.g., 64). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| IPv6 Secondary DNS Address | Configures the IPv6 address of the secondary DNS server (e.g., "FD0F:EC91:16F9:201:215:58FF:FEA0:7827"). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |
| IPv6 Secondary DNS Address Prefix Length | Configures the IPv6 address prefix length of the secondary DNS server (e.g., 64). If DHCPv6 is enabled, this is the value returned by DHCPv6; otherwise, it is the static setting.<br>Note: This property requires a device restart after being changed. |

### 5.20.2 AWI: IPv6 Settings

The settings on this page let you enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware View.

You can access this page for the host or client from the **Configuration** > **IPv6** menu.



IPv6

Change the IPv6 network settings for the device

Enable IPv6: □

Link Local Address:

Gateway:

Enable DHCPv6: □

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC: □

Enable Manual Address: □

**Figure 5-76: AWI IPv6 Page**

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

**Table 5-73: AWI IPv6 Page Parameters**

| Parameter | Description |
|---|---|
| Enable IPv6 | Enable this field to enable IPv6 for your PCoIP devices. |
| Link Local Address | This field is automatically populated. |
| Gateway | Enter the IPv6 gateway address. |
| Enable DHCPv6 | Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device. |
| DHCPv6 Addresses | When DHCPv6 is enabled and the device is rebooted, the server automatically populates these fields with addresses for the device. |
| Primary DNS | The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| Secondary DNS | The device's secondary DNS IP address. If DHCPv6 is enabled, this |

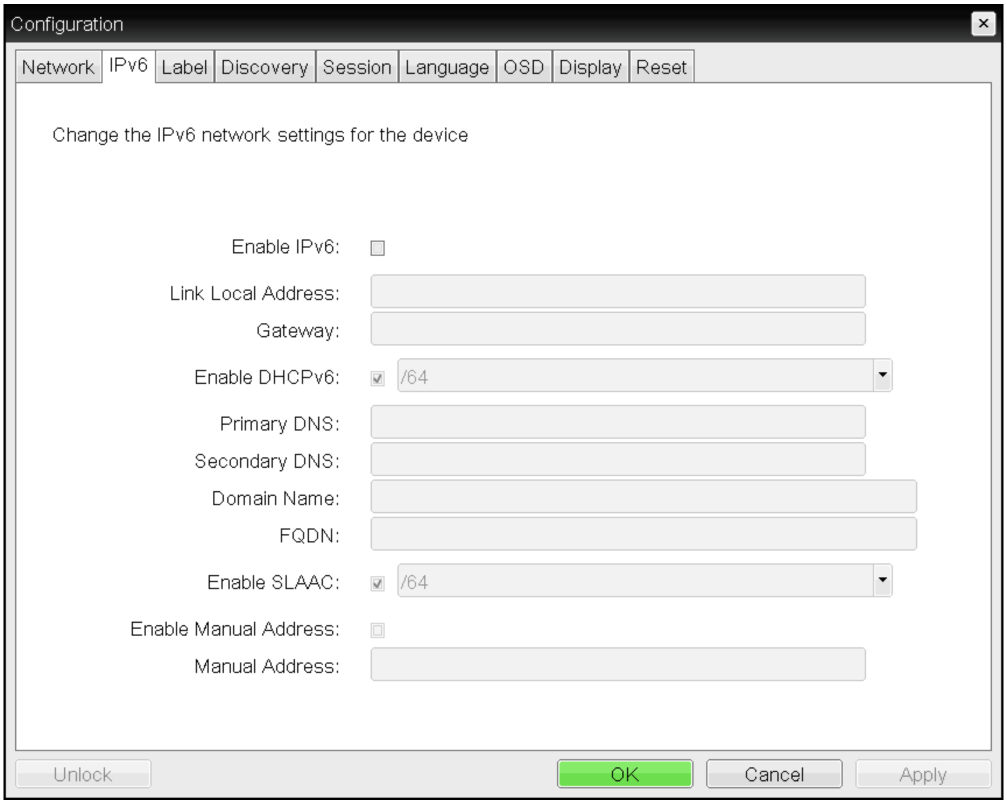
| Parameter | Description |
|---|---|
| | field is automatically populated by the DHCPv6 server. |
| Domain Name | The domain name used (e.g., "domain.local") for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| FQDN | The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| Enable SLAAC | Enable this field to set up Stateless Address Auto-configuration (SLAAC) for your devices. |
| SLAAC Addresses | When SLAAC is enabled and the device is rebooted, these fields are automatically populated. |
| Enable Manual Address | Enable this field to set up a manual (static) address for the device. |
| Manual Address | Enter the IP address for the device. |

### 5.20.3 OSD: IPv6 Settings

The settings on this page let you enable IPv6 for PCoIP devices connected to an IPv6 network.

Note: IPv6 is not currently supported by VMware View.

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



Change the IPv6 network settings for the device

Enable IPv6: □

Link Local Address:

Gateway:

Enable DHCPv6: ☑ /64

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC: ☑ /64

Enable Manual Address: □

Manual Address:

**Figure 5-77: OSD IPv6 Page**

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

**Table 5-74: OSD IPv6 Page Parameters**

| Parameter | Description |
|---|---|
| Enable IPv6 | Enable this field to enable IPv6 for your PCoIP devices. |
| Link Local Address | This field is automatically populated. |
| Gateway | Enter the IPv6 gateway address. |
| Enable DHCPv6 | Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device. |
| DHCPv6 Addresses | When DHCPv6 is enabled and the device is rebooted, the server automatically populates these fields with addresses for the device. |
| Primary DNS | The device's primary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| Secondary DNS | The device's secondary DNS IP address. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |

| Parameter | Description |
|---|---|
| Domain Name | The domain name used (e.g., "domain.local") for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| FQDN | The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is automatically populated by the DHCPv6 server. |
| Enable SLAAC | Enable this field to set up Stateless Address Auto-configuration (SLAAC) for your devices. |
| SLAAC Addresses | When SLAAC is enabled and the device is rebooted, these fields are automatically populated. |
| Enable Manual Address | Enable this field to set up a manual (static) address for the device. |
| Manual Address | Enter the IP address for the device. |

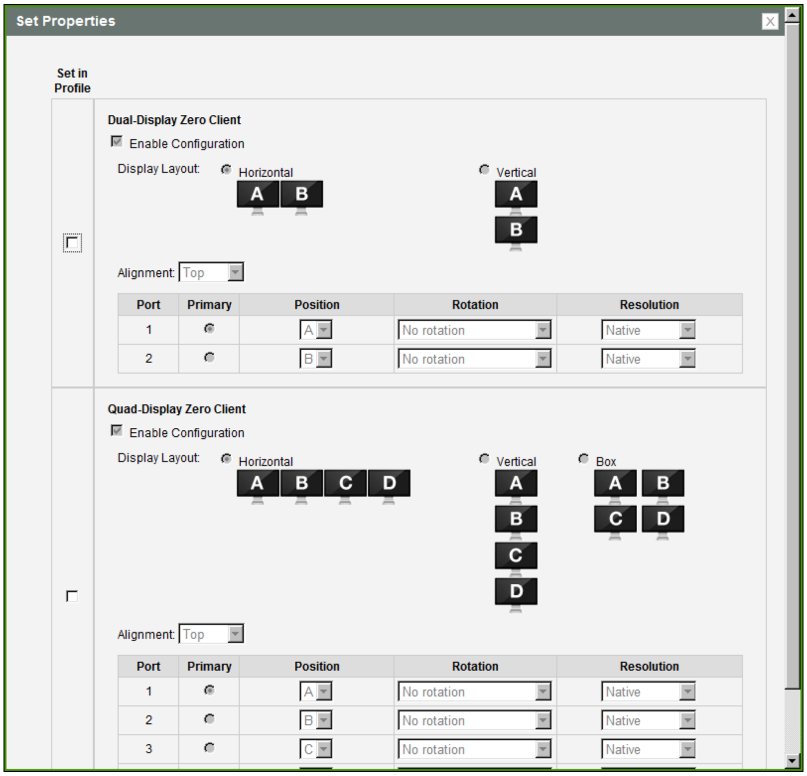
## 5.21 Configuring the Display Topology

### 5.21.1 MC: Display Topology Settings

The settings on this page let you configure a profile with the display topology to use for Tera1 and Tera2 clients.

Note: Use the Dual-Display Zero Client layout for TERA2321 zero client devices.

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



Set Properties

Set in Profile

☐

Dual-Display Zero Client

☑ Enable Configuration

Display Layout: ● Horizontal ○ Vertical

Alignment: Top

| Port | Primary | Position | Rotation | Resolution |
|---|---|---|---|---|
| 1 | ● | A | No rotation | Native |
| 2 | ○ | B | No rotation | Native |

☐

Quad-Display Zero Client

☑ Enable Configuration

Display Layout: ● Horizontal ○ Vertical ○ Box

Alignment: Top

| Port | Primary | Position | Rotation | Resolution |
|---|---|---|---|---|
| 1 | ● | A | No rotation | Native |
| 2 | ○ | B | No rotation | Native |
| 3 | ○ | C | No rotation | Native |

**Figure 5-78: MC Display Topology Configuration**

**Table 5-75: MC Display Topology Configuration Parameters**

| Parameter | Description |
|---|---|
| **Dual-Display Zero Client** | |
| Enable Configuration | Enable to configure a device that supports two displays per PCoIP chipset. |
| Display Layout | Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk.<br>• **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram.<br>• **Vertical**: Select to arrange displays vertically, as indicated in the diagram. |
| Alignment | Select how you want displays aligned when they are different sizes.<br>Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.<br>**Horizontal layout**:<br>• **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. |

| Parameter | Description |
|---|---|
| | • **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **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.<br>**Vertical layout**:<br>• **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.<br>• **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes. |
| Primary | Configure which video port on the zero client you want as the primary port.<br>Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).<br>• **Port 1**: Select to configure port 1 on the zero client as the primary port.<br>• **Port 2**: Select to configure port 2 on the zero client as the primary port. |
| Position | Specify which display is physically connected to each port. |
| Rotation | Configure the rotation of the display in each port:<br>• **No rotation**<br>• **90° clockwise**<br>• **180° rotation**<br>• **90° counter-clockwise** |
| Resolution | The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used. |
| **Quad-Display Zero Client** | |
| Enable Configuration | Enable to configure a device that supports four displays per PCoIP chipset. |
| Display Layout | Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk. |

| Parameter | Description |
|---|---|
| | • **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram.<br>• **Vertical**: Select to arrange displays vertically, as indicated in the diagram.<br>• **Box**: Select to arrange displays in a box formation, as indicated in the diagram. |
| Alignment | Select how you want displays aligned when they are different sizes.<br>Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.<br>**Horizontal layout**:<br>• **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.<br>• **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **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.<br>**Vertical layout**:<br>• **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.<br>• **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes. |
| Primary | Configure which video port on the zero client that you want as the primary port.<br>Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).<br>• **Port 1**: Select to configure port 1 on the zero client as the primary port.<br>• **Port 2**: Select to configure port 2 on the zero client as the primary port.<br>• **Port 3**: Select to configure port 3 on the zero client as the primary port.<br>• **Port 4**: Select to configure port 4 on the zero client as the primary port. |

| Parameter | Description |
|---|---|
| Position | Specify which display is physically connected to each port. |
| Rotation | Configure the rotation of the display in each port:<br>• **No rotation**<br>• **90° clockwise**<br>• **180° rotation**<br>• **90° counter-clockwise** |
| Resolution | The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used. |

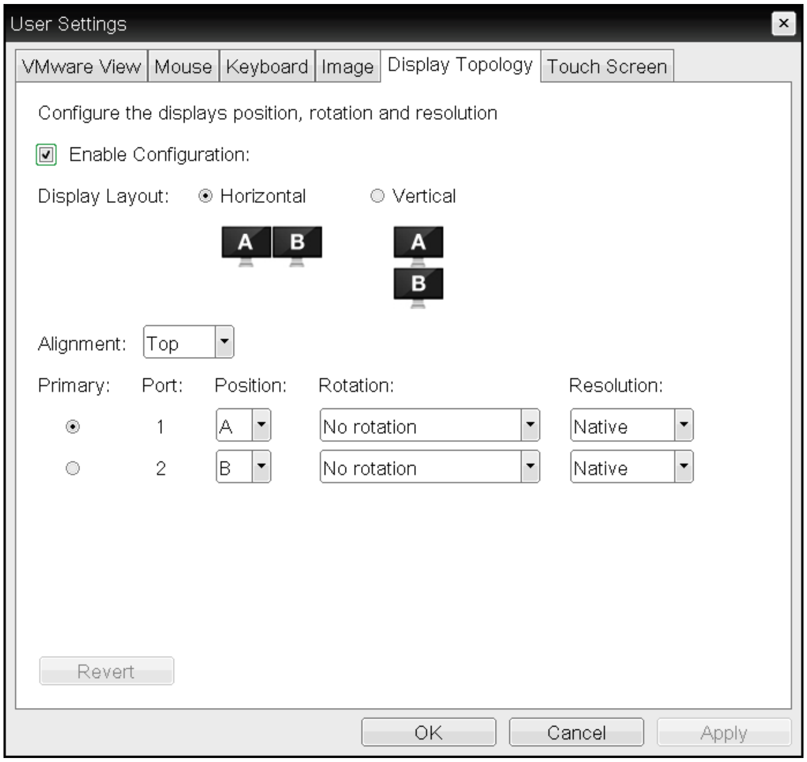
### 5.21.2 OSD Dual-display: Display Topology Settings

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

To apply the display topology feature to a PCoIP session between a client and a VMware View virtual desktop, you must have VMware View 4.5 or later. To apply the display topology feature to a PCoIP session between a client and a PCoIP host, you must have the PCoIP host software installed on the host.

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

Note: This page with the dual monitor layout also displays if you are using the TERA2321 zero client device as your client.



Configure the displays position, rotation and resolution

☑ Enable Configuration:

Display Layout: ● Horizontal ○ Vertical

Alignment: Top

| Primary: | Port: | Position: | Rotation: | Resolution: |
|---|---|---|---|---|
| ● | 1 | A | No rotation | Native |
| ○ | 2 | B | No rotation | Native |

Figure 5-79: OSD Tera1 Display Topology Page

Table 5-76: OSD Tera1 Display Topology Page Parameters

| Parameter | Description |
|---|---|
| Enable Configuration | Enable to configure a device that supports two displays per PCoIP chipset. |
| Display Layout | Select the layout for the displays (A and B). This setting should reflect the physical layout of the displays on the desk.<br>• **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram.<br>• **Vertical**: Select to arrange displays vertically, as indicated in the diagram. |
| Alignment | Select how you want displays aligned when they are different sizes.<br>Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.<br>**Horizontal layout**:<br>• **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.<br>• **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between |

| Parameter | Description |
|---|---|
| | displays of different sizes.<br>• **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.<br>**Vertical layout**:<br>• **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.<br>• **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes. |
| Primary | Configure which video port on the zero client you want as the primary port.<br>Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).<br>• **Port 1**: Select to configure port 1 on the zero client as the primary port.<br>• **Port 2**: Select to configure port 2 on the zero client as the primary port. |
| Position | Specify which display is physically connected to each port. |
| Rotation | Configure the rotation of the display in each port:<br>• **No rotation**<br>• **90° clockwise**<br>• **180° rotation**<br>• **90° counter-clockwise** |
| Resolution | The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used. |

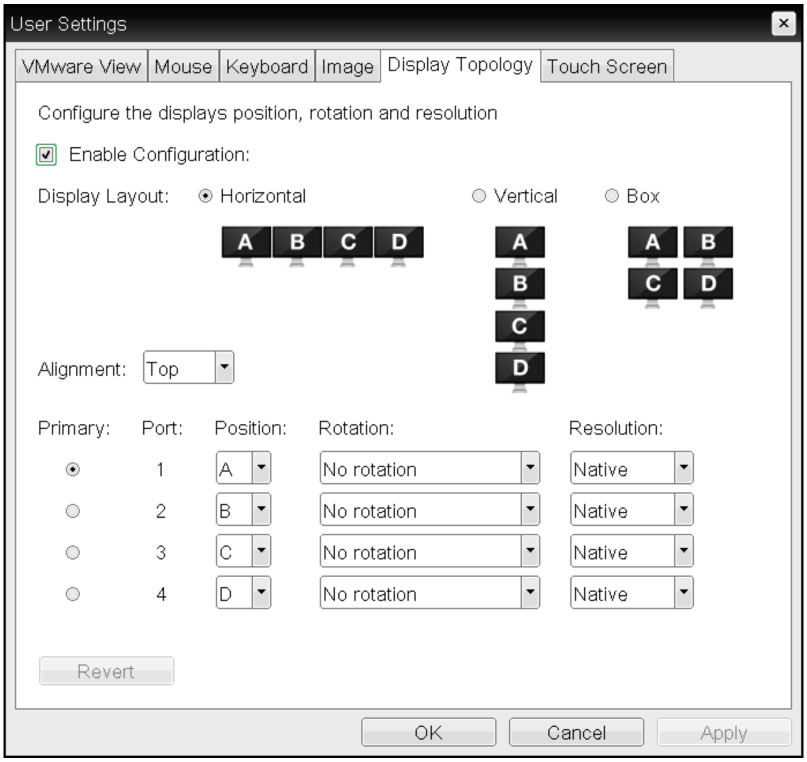
### 5.21.3 OSD Quad-display: Display Topology Settings

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

To apply the display topology feature to a PCoIP session between a client and a VMware View virtual desktop, you must have VMware View 4.5 or later. To apply the display topology feature to a PCoIP session between a client and a PCoIP host, you must have the PCoIP host software installed on the host.

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

Note: If you are using the TERA2321 zero client device as your client, a dual monitor layout displays on this page instead of the quad monitor layout.



Configure the displays position, rotation and resolution

☑ Enable Configuration:

Display Layout: ● Horizontal ○ Vertical ○ Box

Alignment: Top

| Primary: | Port: | Position: | Rotation: | Resolution: |
|---|---|---|---|---|
| ● | 1 | A | No rotation | Native |
| ○ | 2 | B | No rotation | Native |
| ○ | 3 | C | No rotation | Native |
| ○ | 4 | D | No rotation | Native |

**Figure 5-80: OSD Tera2 Display Topology Page**

**Table 5-77: OSD Tera2 Display Topology Page Parameters**

| **Parameter** | **Description** |
|---|---|
| Enable Configuration | Enable to configure a device that supports four displays per PCoIP chipset. |
| Display Layout | Select the layout for the displays (A, B, C, and D). This setting should reflect the physical layout of the displays on the desk.<br>• **Horizontal**: Select to arrange displays horizontally, as indicated in the diagram.<br>• **Vertical**: Select to arrange displays vertically, as indicated in the diagram.<br>• **Box**: Select to arrange displays in a box formation, as indicated in the diagram. |

| Parameter | Description |
|---|---|
| Alignment | Select how you want displays aligned when they are different sizes.<br>Note: This setting affects which area of the screen to use when users move the cursor from one display to the other. The alignment options that appear in the drop-down list depend on the selected display layout.<br>**Horizontal layout**:<br>• **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.<br>• **Center**: Select to horizontally center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **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.<br>**Vertical layout**:<br>• **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.<br>• **Center**: Select to vertically center displays. With this setting, use the center area of the screen when navigating between displays of different sizes.<br>• **Right**: Select to align displays on the right. With this setting, use the right area of the screen when navigating between displays of different sizes. |
| Primary | Configure which video port on the zero client that you want as the primary port.<br>Note: The display that is connected to the primary port becomes the primary display (i.e., the display that contains the OSD menus before you initiate a PCoIP session and the display that is requested for the Windows taskbar after you initiate the session).<br>• **Port 1**: Select to configure port 1 on the zero client as the primary port.<br>• **Port 2**: Select to configure port 2 on the zero client as the primary port.<br>• **Port 3**: Select to configure port 3 on the zero client as the primary port.<br>• **Port 4**: Select to configure port 4 on the zero client as the primary port. |
| Position | Specify which display is physically connected to each port. |
| Rotation | Configure the rotation of the display in each port:<br>• **No rotation**<br>• **90° clockwise**<br>• **180° rotation**<br>• **90° counter-clockwise** |

| Parameter | Description |
|---|---|
| Resolution | The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used. |

# 5.22 Uploading an OSD Logo

## 5.22.1 MC: OSD Logo Settings

The **Profile OSD Logo** section is located towards the bottom of the **Manage Profiles** page on the Management Console. It lets you upload an image to a profile that will display on the **Connect** page of a user's local On Screen Display (OSD) GUI.

Note: You can configure the **VMware View** login screen on the OSD to display this logo instead of the VMware View banner by enabling **Use OSD Logo for View Banner** in the advanced options on the AWI **Session – View Connection Server** page.

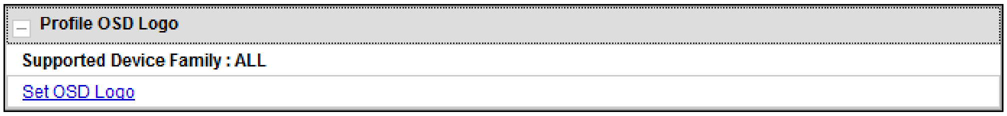
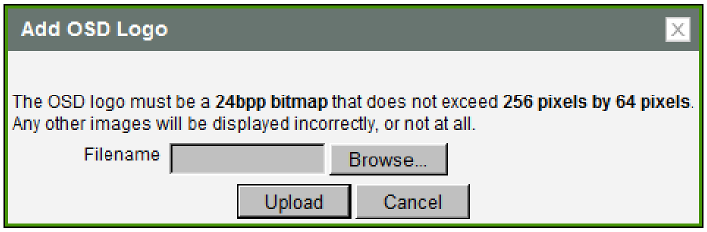


Figure 5-81: MC Profile OSD Logo Configuration

When you click **Set OSD Logo**, the following screen displays from which you can upload an image file.



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

Figure 5-82: MC Add OSD Logo Configuration

Table 5-78: MC Add OSD Logo Configuration Parameters

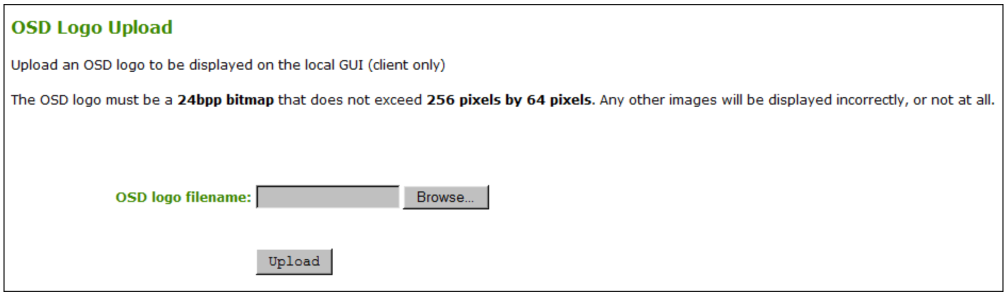
| Parameter | Description |
|---|---|
| Filename | Specify the filename of the logo image you want to upload. You can browse to the target file using the **Browse** button.<br>The file must be accessible to the web browser (i.e., it must be on a local or accessible network drive). The 24 bpp (bits per pixel) image must be in BMP format, and its dimensions cannot exceed 256 pixels in width and 64 pixels in height. If the file extension is incorrect, an error message appears. |

| Parameter | Description |
|---|---|
| Upload | Click **Upload** to transfer the specified image file to the client. A message to confirm the upload appears. |

### 5.22.2 AWI Client: OSD Logo Settings

The **OSD Logo** page lets you upload an image to display on the **Connect** page of the local On Screen Display (OSD) GUI. You can access the **OSD Logo** page from the **Upload** > **OSD Logo** menu.

Note: You can configure the **VMware View** login screen on the OSD to display this logo instead of the VMware View banner by enabling **Use OSD Logo for View Banner** in the advanced options on the AWI **Session – View Connection Server** page.



OSD Logo Upload

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

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

OSD logo filename: [ ] Browse...

Upload

Figure 5-83: AWI Client OSD Logo Upload Page

Table 5-79: AWI Client OSD Logo Upload Page Parameters

| Parameter | Description |
|---|---|
| OSD logo filename | Specify the filename of the logo image you want to upload. You can browse to the target file using the **Browse** button.<br>The file must be accessible to the web browser (i.e., it must be on a local or accessible network drive). The 24 bpp (bits per pixel) image must be in BMP format, and its dimensions cannot exceed 256 pixels in width and 64 pixels in height. If the file extension is incorrect, an error message appears. |
| Upload | Click **Upload** to transfer the specified image file to the client. A message to confirm the upload appears. |

## 5.23 Uploading Firmware

### 5.23.1 MC: Firmware Management

The **Profile Firmware** section is located towards the bottom of the **Manage Profiles** page on the Management Console. It lets you assign a firmware file to a profile and configure the upgrade criteria that must be met before the firmware is pushed to each device.

Note: Before you can assign a firmware file to a profile, you must first ensure that the file has been imported into the MC from the **Update > Import Firmware** menu. For more information, see the "PCoIP Management Console User Manual" (TER0812002).

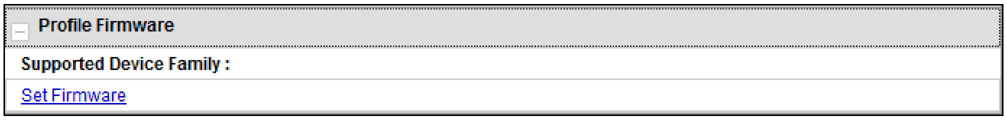
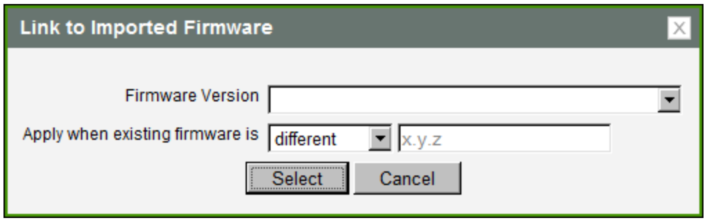


Figure 5-84: MC Profile Firmware Configuration

When you click **Set Firmware**, the following screen displays.

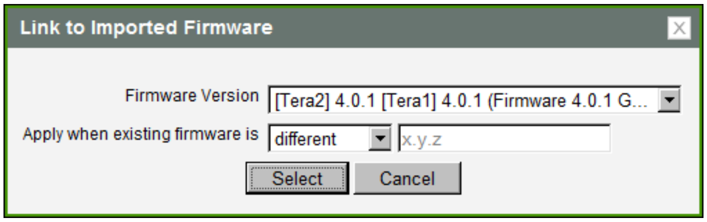


Firmware Version:

Apply when existing firmware is: different x.y.z

Figure 5-85: MC Link to Imported Firmware

Select the firmware version from the drop-down menu, and then choose whether the firmware will be overwritten on the device if its version is different from this firmware version or if it is less than the firmware version you enter in the text entry field. Click **Select** when you are finished.



Firmware Version: [Tera2] 4.0.1 [Tera1] 4.0.1 (Firmware 4.0.1 G...

Apply when existing firmware is: different x.y.z

Figure 5-86: MC Link to Imported Firmware – Configured

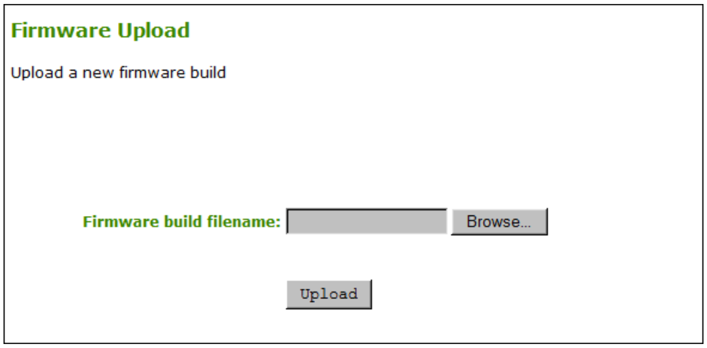
Table 5-80: MC Link to Imported Firmware Parameters

| Parameter | Description |
|---|---|
| Firmware Version | Select the firmware file that you want to assign to the profile.<br>Note: The firmware file must first be imported into the MC from the **Update > Import Firmware** menu. For more information, see the "PCoIP Management Console User Manual" (TER0812002). |
| Apply when existing firmware is | Configure one of the following options from the drop-down menu:<br>• **different**: Select this option if you want to overwrite the firmware on the device only if its version is different from the firmware version you selected.<br>• **less than**: Select this option if you want to overwrite the firmware on the device only if its version is less than the firmware version in the *x.y.z* field, and then enter the version in this field (e.g., 4.0.2). |

## 5.23.2 AWI: Firmware Upload Settings

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

Note: The host and client must have the same firmware release version installed.



Firmware Upload

Upload a new firmware build

Firmware build filename: [ ] Browse...

Figure 5-87: AWI Firmware Upload Page

Table 5-81: AWI Firmware Upload Page Parameters

| Parameter | Description |
|---|---|
| Firmware build filename | The filename of the firmware image to be uploaded. You can browse to the file using the **Browse** button. The file must be accessible to the web browser (i.e., it must be on a local or accessible network drive). The firmware image must be an ".all" file. |
| 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.<br>Note: It's important to ensure that both the host and client have the same firmware release. |

**To upload a firmware release to a client**:

1. Log in to the client's AWI.
2. From the **Firmware Upload** page, browse to the folder containing the firmware file. This file will have an ".all" extension.
3. Double-click the correct "*.all" firmware file.
4. Click **Upload**.
5. Click **OK** to confirm that you want to proceed with the upload. The operation may take a few minutes. When completed, the AWI page displays two buttons—**Reset** and **Continue**.
6. Click **Reset**.
7. Click **OK**.

**To upload a firmware release to a host**:

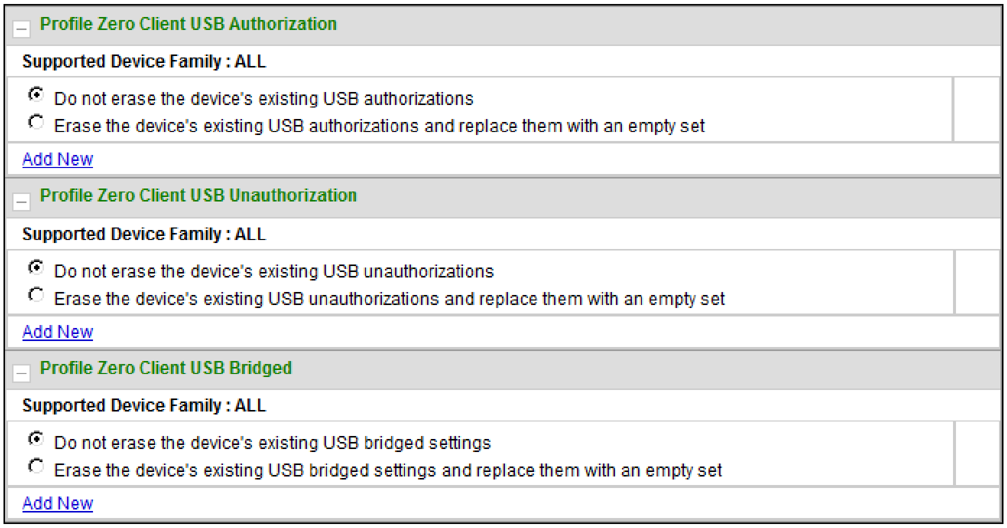
1. Ensure the host PC or workstation is in an idle state (i.e., that all applications are closed).
2. Log into the host's AWI.
3. From the **Firmware Upload** page, browse to the folder containing the firmware file. This file will have an ".all" extension.
4. Double-click the correct "*.all" firmware file.
5. Click **Upload**.
6. Click **OK** to confirm that you want to proceed with the upload. The operation may take a few minutes. When completed, the AWI page displays two buttons—**Reset** and **Continue**.
7. Click **Reset**.
8. Click **OK**.
9. Power off and then power on the host PC or workstation. It is necessary to power off (not just restart) the PC or workstation in order for the changes to take effect on the host card.

# 5.24 Configuring USB Permissions

## 5.24.1 MC: USB Permissions

The **Profile Zero Client USB**sections are located towards the bottom of the **Manage Profiles** page on the Management Console. These sections let you configure a profile to retain the USB settings that are configured on clients, to disable the settings, or to add to them.

Note: USB Enhanced Host Controller Interface (EHCI) mode is configured in the Management Console on the MC Peripheral Configuration page.



Profile Zero Client USB Authorization

Supported Device Family : ALL

● Do not erase the device's existing USB authorizations
○ Erase the device's existing USB authorizations and replace them with an empty set

Add New

Profile Zero Client USB Unauthorization

Supported Device Family : ALL

● Do not erase the device's existing USB unauthorizations
○ Erase the device's existing USB unauthorizations and replace them with an empty set

Add New

Profile Zero Client USB Bridged

Supported Device Family : ALL

● Do not erase the device's existing USB bridged settings
○ Erase the device's existing USB bridged settings and replace them with an empty set

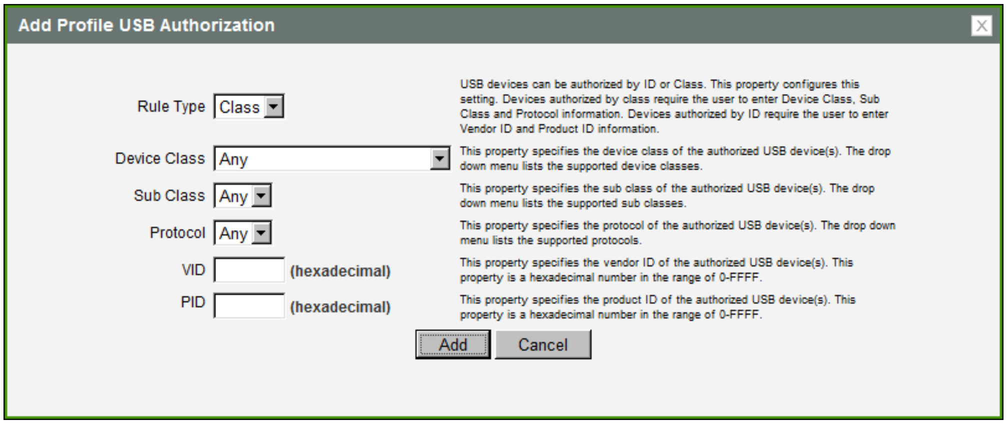
Add New

**Figure 5-88: MC Profile Zero Client USB Configuration**

**Table 5-82: MC Profile Zero Client USB Configuration Parameters**

| Parameter | Description |
|---|---|
| Profile Zero Client USB Authorization | Choose one of the following:<br>• **Do not erase the device's existing USB authorizations**: Select this option if you want to use the existing USB authorization settings that are configured on the client.<br>• **Erase the device's existing USB authorizations and replace them with an empty set**: Select this option if you want to remove all USB authorization settings that are configured on the client.<br>• **Add New**: Click this link if you want to add a new USB authorization entry to the existing settings that are configured on the client. |
| Profile Zero Client USB Unauthorization | Choose one of the following:<br>• **Do not erase the device's existing USB unauthorizations**: Select this option if you want to use the existing USB unauthorization settings that are configured on the client.<br>• **Erase the device's existing USB unauthorizations and replace them with an empty set**: Select this option if you want to disable all USB devices that are configured on the client.<br>• **Add New**: Click this link if you want to add a new USB unauthorization entry to the existing unauthorization settings that are configured on the client. |
| Profile Zero Client USB Bridged | Choose one of the following:<br>• **Do not erase the device's existing USB bridged settings**: Select this option if you want to use the existing USB bridged settings that are configured on the client.<br>• **Erase the device's existing USB bridged settings and replace them with an empty set**: Select this option if you want to disable all USB bridged settings that are configured on the client.<br>• **Add New**: Click this link if you want to add a new USB bridged entry to the existing settings that are configured on the client. |

When you click **Add New** for a USB authorization, unauthorization, or bridged entry, the following screens display, respectively.



Add Profile USB Authorization

Rule Type: Class — USB devices can be authorized by ID or Class. This property configures this setting. Devices authorized by class require the user to enter Device Class, Sub Class and Protocol information. Devices authorized by ID require the user to enter Vendor ID and Product ID information.

Device Class: Any — This property specifies the device class of the authorized USB device(s). The drop down menu lists the supported device classes.

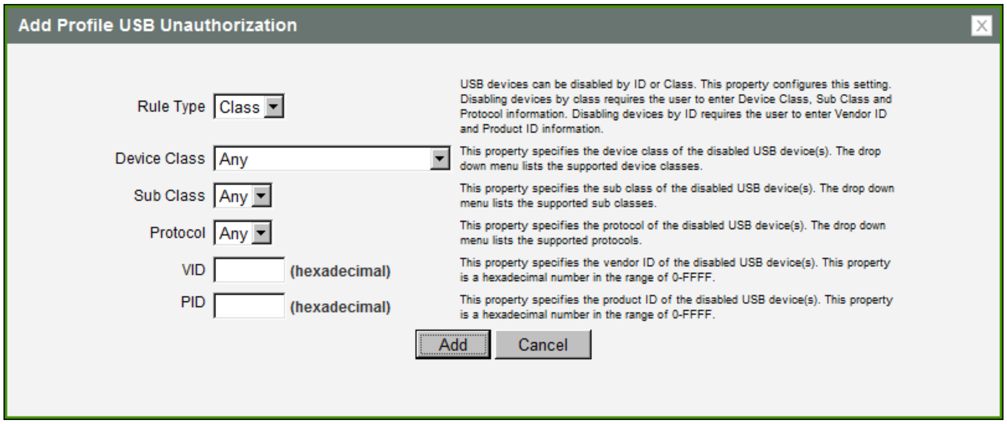
Sub Class: Any — This property specifies the sub class of the authorized USB device(s). The drop down menu lists the supported sub classes.

Protocol: Any — This property specifies the protocol of the authorized USB device(s). The drop down menu lists the supported protocols.

VID (hexadecimal) — This property specifies the vendor ID of the authorized USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

PID (hexadecimal) — This property specifies the product ID of the authorized USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

Figure 5-89: USB Authorization – Add New



Add Profile USB Unauthorization

Rule Type: Class — USB devices can be disabled by ID or Class. This property configures this setting. Disabling devices by class requires the user to enter Device Class, Sub Class and Protocol information. Disabling devices by ID requires the user to enter Vendor ID and Product ID information.

Device Class: Any — This property specifies the device class of the disabled USB device(s). The drop down menu lists the supported device classes.

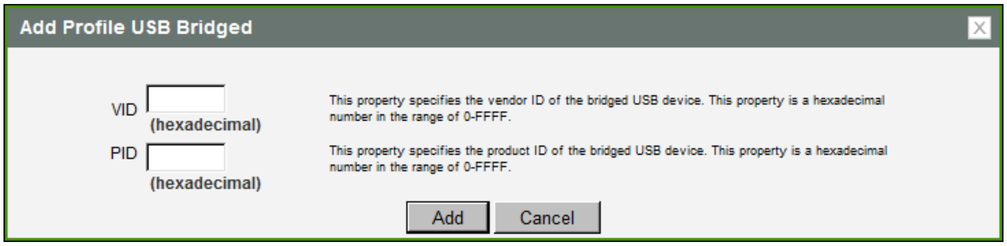
Sub Class: Any — This property specifies the sub class of the disabled USB device(s). The drop down menu lists the supported sub classes.

Protocol: Any — This property specifies the protocol of the disabled USB device(s). The drop down menu lists the supported protocols.

VID (hexadecimal) — This property specifies the vendor ID of the disabled USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

PID (hexadecimal) — This property specifies the product ID of the disabled USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

Figure 5-90: USB Unauthorization – Add New



Add Profile USB Bridged

VID (hexadecimal) — This property specifies the vendor ID of the bridged USB device. This property is a hexadecimal number in the range of 0-FFFF.

PID (hexadecimal) — This property specifies the product ID of the bridged USB device. This property is a hexadecimal number in the range of 0-FFFF.

Figure 5-91: USB Bridged – Add New

**Table 5-83: Add Profile USB – Add New Parameters**

| Parameter | Description |
|---|---|
| Rule Type | When adding a new USB authorization or unauthorization entry, select one of the following:<br>• **Class**: The USB device is authorized by its device class, sub-class, and protocol information.<br>• **ID**:The USB device is authorized by its vendor ID and product ID information. |

| Parameter | Description |
|---|---|
| Device Class | This field is enabled when **Class** is selected.<br>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.<br>Select a supported device sub class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any sub-class.<br>Note: If **Any** is selected as the device class, this will be the only selection available. |
| Protocol | This field is enabled when **Class** is selected.<br>Select a supported protocol from the drop-down menu, or select **Any**.<br>Note: If **Any** is selected as the device class or sub-class, this will be the only selection available. |
| VID | This field is enabled when **ID** is selected, or when you are adding a new USB bridged entry.<br>Enter the vendor ID of the authorized, unauthorized, or bridged device. The valid range is hexadecimal 0-FFFF. |
| PID | This field is enabled when **ID** is selected, or when you are adding a new USB bridged entry.<br>Enter the product ID of the authorized, unauthorized, or bridged device. The valid range is hexadecimal 0-FFFF. |

### 5.24.2 AWI Client: USB Permissions

The **USB** page is accessed from the **Permissions** > **USB** menu. It allows you to authorize a "white list" of USB devices and to unauthorize a "black list" of USB devices based on ID or Class. You can use wildcards (or specify "any") to reduce the number of entries needed to define all devices.

You can also configure devices that need to be bridged to the host, and enable USB 2.0 Enhanced Host Controller Interface (EHCI) mode for certain USB devices.

USB plug events are blocked in the PCoIP zero client hardware for unauthorized USB devices. The host (PCoIP host card or the host virtual desktop) cannot see or access the device for an additional layer of security.

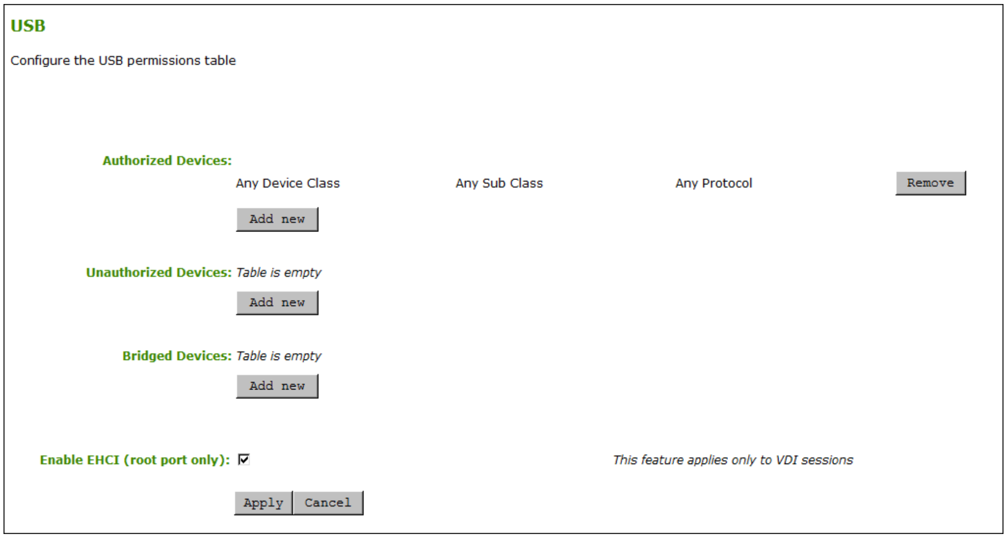
The **USB** page is available on the host and client but the host USB permissions have a higher priority and update the client USB permissions. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP host card. The following rules apply:

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

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

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

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



USB

Configure the USB permissions table

Authorized Devices: Any Device Class | Any Sub Class | Any Protocol

Unauthorized Devices: *Table is empty*

Bridged Devices: *Table is empty*

Enable EHCI (root port only): ☑ *This feature applies only to VDI sessions*

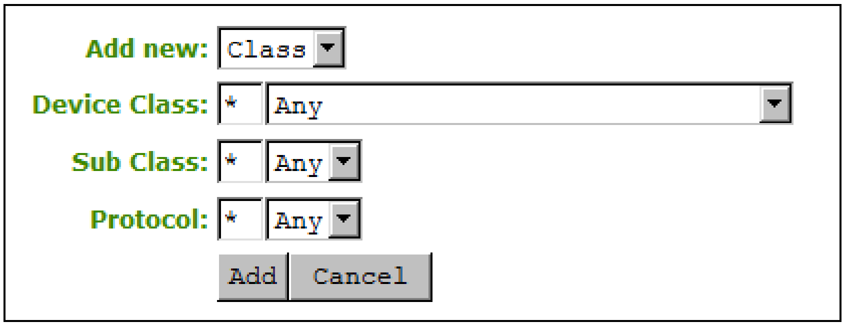
**Figure 5-92: AWI Client USB Page**

**Table 5-84: AWI Client USB Page Parameters**

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

| Parameter | Description |
|---|---|
| | **Remove:** Delete a rule for a device or device group from the list. |
| Bridged Devices | PCoIP zero clients locally terminate HID devices when connecting to VMware View virtual desktops. However, some devices advertise as HID but use different drivers. These devices may need to be bridged to the host rather than locally terminated. This setting lets you force the zero client to bridge specific USB devices so that they use the drivers on the virtual desktop.<br>**Add New:** Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.<br>**Remove:** Delete a rule for a device or device group from the list.<br>Note: Bridging is a feature supported in firmware 3.3.0 or higher. This rule only affects sessions between a zero client and a soft host running VMware View 4.6 or higher. |
| Enable EHCI (root port only) | Enable this field to configure EHCI (USB 2.0) for devices connected directly to zero client USB ports for sessions with a host running VMware View 4.6 or later.<br>Note: This feature cannot be enabled on clients with less than 128 MB of RAM. Devices with isochronous endpoints will not operate at USB 2.0 speeds. |

When you add a new USB authorized or unauthorized entry, the following parameters display depending on whether you describe the device by **Class** or **ID**.



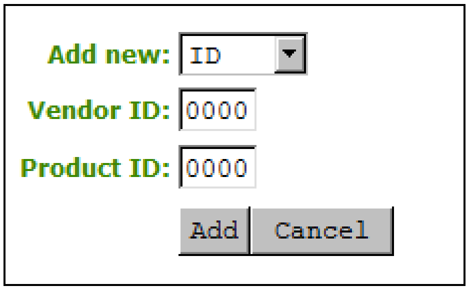
Add new: Class

Device Class: * Any

Sub Class: * Any

Protocol: * Any

**Figure 5-93: Device Class Parameters**



Add new: ID

Vendor ID: 0000

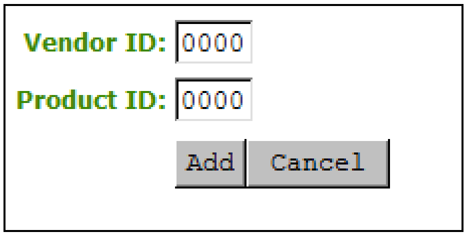
Product ID: 0000

**Figure 5-94: Device ID Parameters**

**Table 5-85: USB Authorized/Unauthorized Devices Parameters**

| Parameter | Description |
|---|---|
| Add new | When adding a new USB authorization or unauthorization entry, select one of the following:<br>• **Class**: The USB device is authorized by its device class, sub-class, and protocol information.<br>• **ID**:The USB device is authorized by its vendor ID and product ID information. |
| Device Class | This field is enabled when **Class** is selected.<br>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.<br>Select a supported device sub class from the drop-down menu, or select **Any** to authorize or unauthorize (disable) any sub-class.<br>Note: If **Any** is selected as the device class, this will be the only selection available. |
| Protocol | This field is enabled when **Class** is selected.<br>Select a supported protocol from the drop-down menu, or select **Any**.<br>Note: If **Any** is selected as the device class or sub-class, this will be the only selection available. |
| Vendor ID | This field is enabled when **ID** is selected.<br>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.<br>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.



Vendor ID: 0000

Product ID: 0000

**Figure 5-95: USB Bridged Parameters**

**Table 5-86: USB Bridged Devices Parameters**

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

### 5.24.3 AWI Host: USB Permissions

The **USB** page is accessed from the **Permissions** > **USB** menu. It allows you to authorize a "white list" of USB devices and to unauthorize a "black list" of USB devices based on ID or Class. You can use wildcards (or specify "any") to reduce the number of entries needed to define all devices.

USB plug events are blocked in the PCoIP zero client hardware for unauthorized USB devices. The host (PCoIP host card or the host virtual desktop) cannot see or access the device for an additional layer of security.

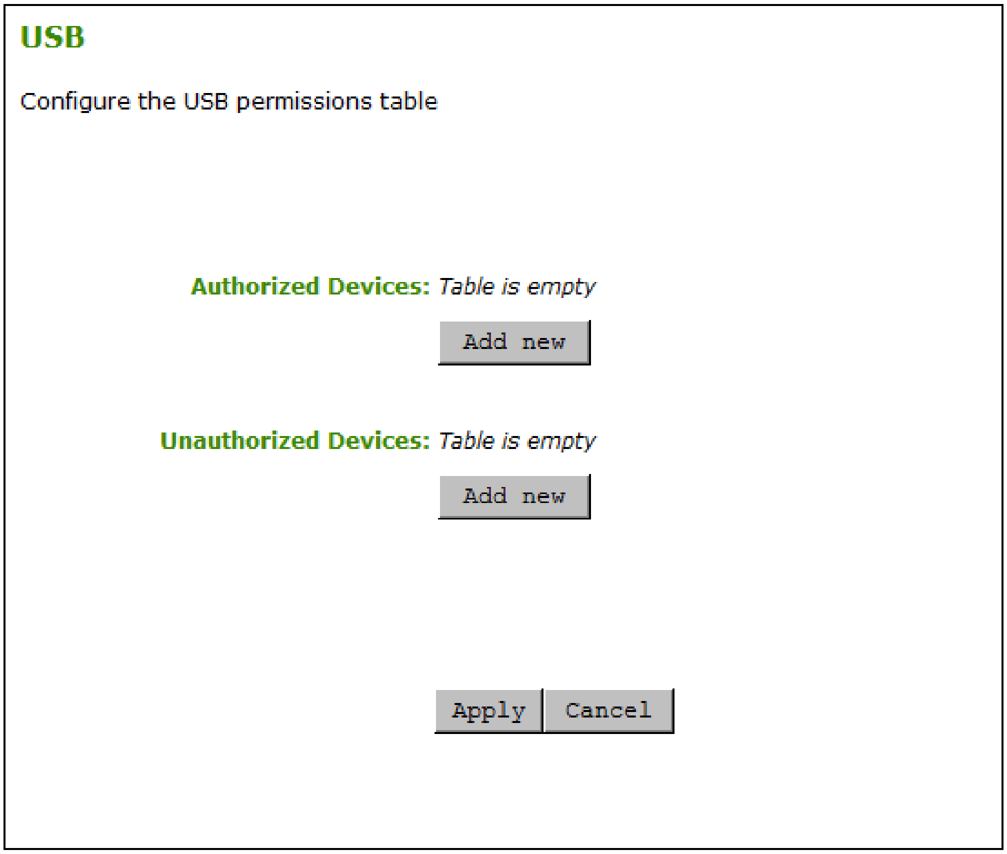
The **USB** page is available on the host and client but the host USB permissions have a higher priority and update the client USB permissions. It is strongly recommended you only set the USB permissions on the host when connecting to a PCoIP host card. The following rules apply:

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

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

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

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



USB

Configure the USB permissions table

Authorized Devices: *Table is empty*

Unauthorized Devices: *Table is empty*

**Figure 5-96: AWI Host USB Page**

**Table 5-87: AWI Host USB Page Parameters**

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

When you add a new USB authorized or unauthorized entry, the following parameters display depending on whether you describe the device by **Class** or **ID**.

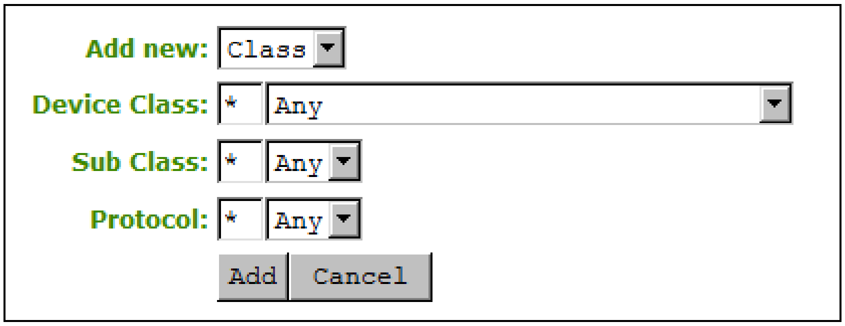


**Figure 5-97: Device Class Parameters**

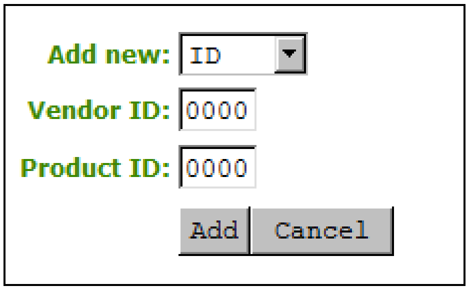


**Figure 5-98: Device ID Parameters**

**Table 5-88: USB Authorized/Unauthorized Devices Parameters**

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

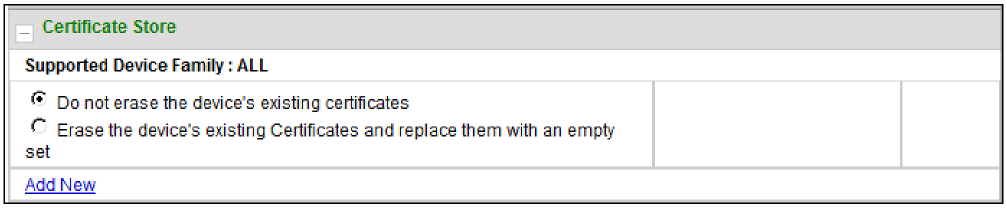
| Parameter | Description |
|---|---|
| | selection available. |
| Vendor ID | This field is enabled when **ID** is selected.<br>Enter the vendor ID of the authorized (or unauthorized) device. The valid range is hexadecimal 0-FFFF. |
| Protocol ID | This field is enabled when **ID** is selected.<br>Enter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

## 5.25 Configuring the Certificate Store

### 5.25.1 MC: Certificate Store Management

The **Certificate Store** section is located at the bottom of the **Manage Profiles** page on the Management Console. This section lets you configure a profile to retain the certificate settings that are configured on a device, to disable the settings, or to upload a new certificate file to the profile.

Note: You can upload up to 16 certificate files into a profile and set their usages.



Certificate Store

Supported Device Family : ALL

● Do not erase the device's existing certificates

○ Erase the device's existing Certificates and replace them with an empty set

Add New

**Figure 5-99: MC Certificate Store Configuration**

**Table 5-89: MC Certificate Store Configuration Parameters**

| Parameter | Description |
|---|---|
| Do not erase the device's existing certificates | Select this option if you want the profile to use the existing certificate settings that are configured on the device. |
| Erase the device's existing Certificates and replace them with an empty set | Select this option if you want the profile to disable all certificates that are configured on the device. |
| Add New | Lets you upload a new certificate file to the profile. |

When you click **Add New**, the following screen displays.

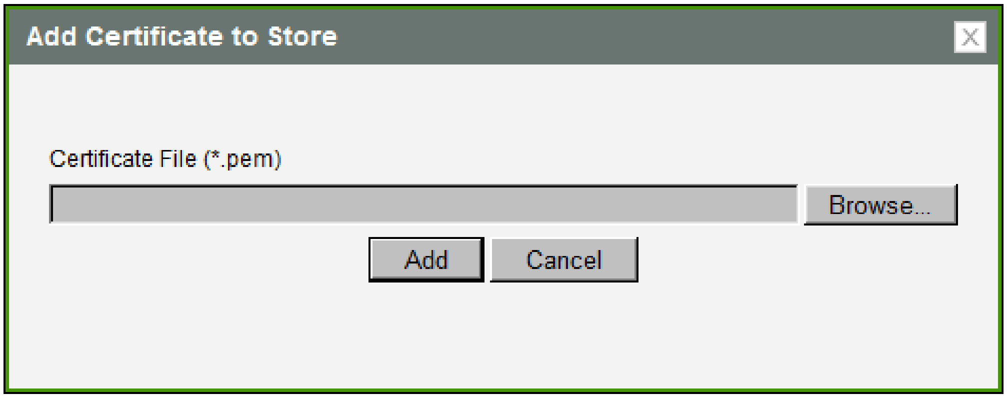
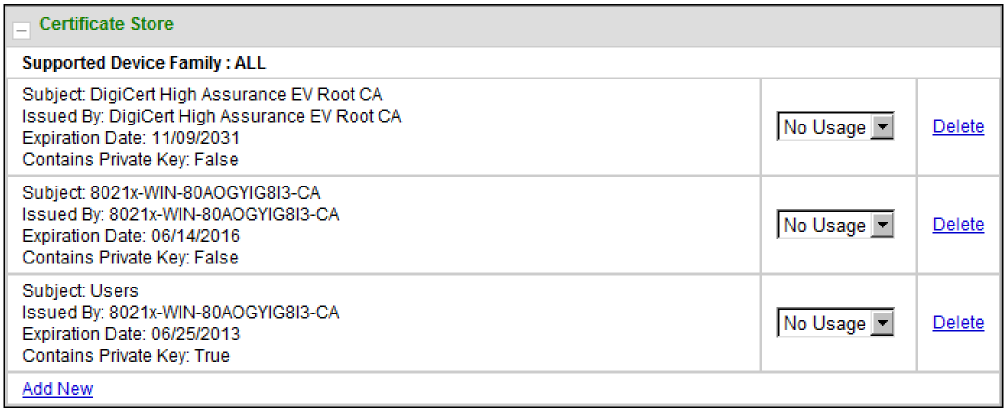


**Figure 5-100: MC Add Certificate to Store**

**Table 5-90: MC Add Certificate to Store Parameters**

| Parameter | Description |
|---|---|
| Certificate File (*.pem) | Use the **Browse** button to locate the certificate file, and then click **Add**.<br>Note: You can add up to a maximum of 16 certificate files to a profile. |

After adding a certificate, you can then select a usage from the drop-down menu in the **Certificate Store** section.



Supported Device Family : ALL

Subject: DigiCert High Assurance EV Root CA
Issued By: DigiCert High Assurance EV Root CA
Expiration Date: 11/09/2031
Contains Private Key: False

Subject: 8021x-WIN-80AOGYIG8I3-CA
Issued By: 8021x-WIN-80AOGYIG8I3-CA
Expiration Date: 06/14/2016
Contains Private Key: False

Subject: Users
Issued By: 8021x-WIN-80AOGYIG8I3-CA
Expiration Date: 06/25/2013
Contains Private Key: True

**Figure 5-101: MC Certificate Store**

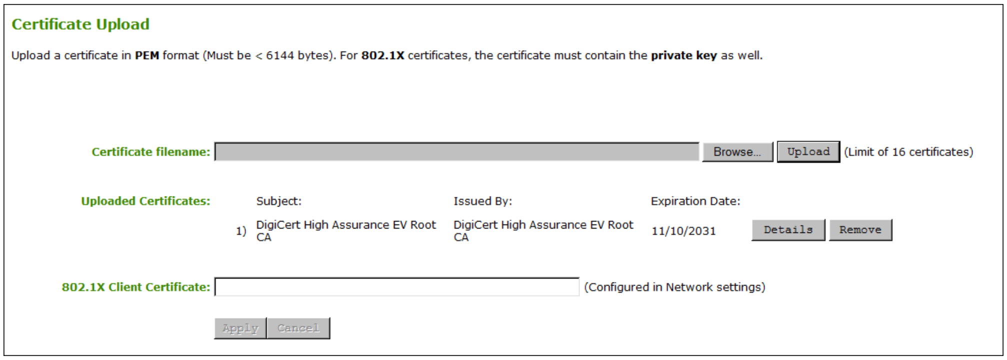
## 5.25.2 AWI: Certificate Upload Settings

The **Certificate Upload** page lets you upload and manage your CA root and client certificates. You can access this page from the **Upload** > **Certificate** menu.

Note: You can upload up to 16 certificates. As of Firmware Release 3.5, 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.

The following are some general guidelines when using 802.1X authentication. For detailed information, see Knowledge Base support topic 15134-1063 on the Teradici support site.

- 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 zero device, selecting the correct 802.1X client certificate from the drop-down list, and then applying your settings.
- The 802.1X server CA root certificate must be in .pem format, but should not need to contain a private key. If the certificate is in a different format, you must convert it to .pem format before uploading it. This certificate does not require configuration from the **Network** page.
- Both the 802.1X client certificate and the 802.1X server CA root certificate must be less than 6 KB; otherwise, you will not be able to upload them. Some certificate files may contain multiple certificates. If your certificate file is too large and it has multiple certificates within, you can open the file in a text editor, then copy and save each certificate to its own file.



Certificate Upload

Upload a certificate in **PEM** format (Must be < 6144 bytes). For **802.1X** certificates, the certificate must contain the **private key** as well.

Certificate filename: (Limit of 16 certificates)

Uploaded Certificates:

| | Subject: | Issued By: | Expiration Date: |
|---|---|---|---|
| 1) | DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA | 11/10/2031 |

802.1X Client Certificate: (Configured in Network settings)

Figure 5-102: AWI Certificate Upload Page

Table 5-91: AWI Certificate Upload Page 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** |

| Parameter | Description |
|---|---|
| | **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. |

# 5.26 Configuring an OSD Display Override

## 5.26.1 OSD Dual-display: Display Settings

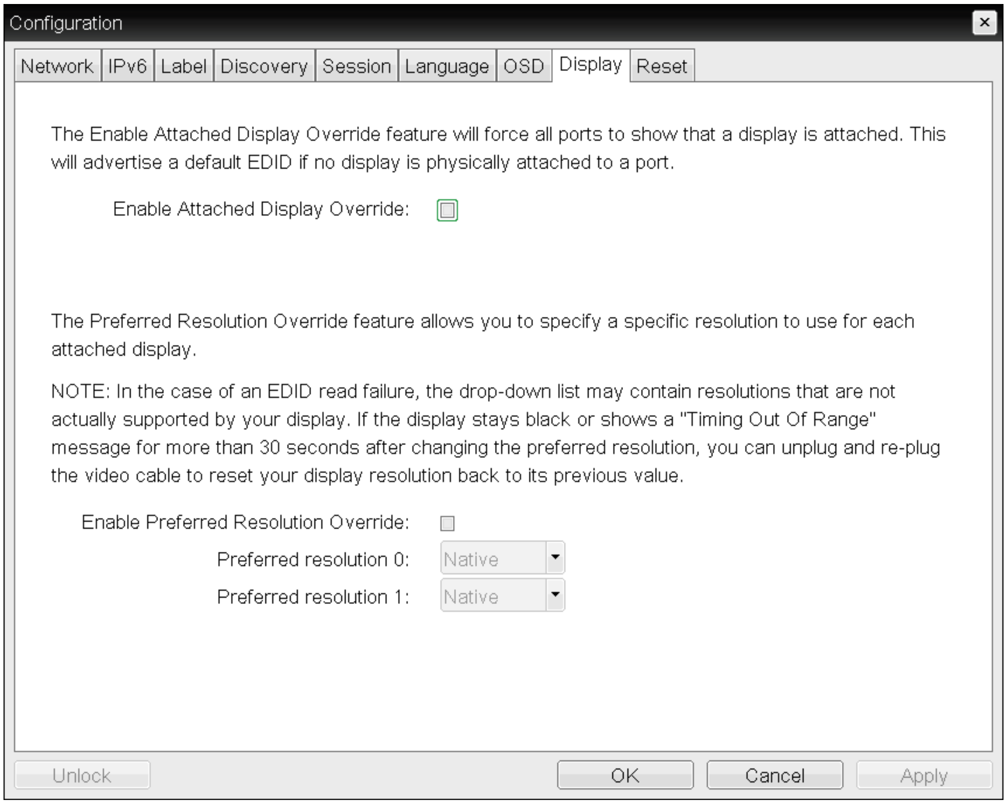
The **Display** page lets you enable the Extended Display Identification Data (EDID) override mode.

Note: This function is only available through the OSD.

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

Warning: You should only enable the Preferred Resolution 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 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.

Note: Preferred resolution settings for only two monitors will display on this page if you are using the TERA2321 zero client device as your client.



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

Enable Attached Display Override: □

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

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

Enable Preferred Resolution Override: □

Preferred resolution 0: Native

Preferred resolution 1: Native

Figure 5-103: OSD Tera1Display Page

**Table 5-92: OSD Tera1 Display Page Parameters**

| Parameter | Description |
|---|---|
| Enable Attached Display Override | This option is intended for legacy systems. It configures the client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. In versions of Windows prior to Windows 7, once the host had no EDID information, it would assume no monitors were attached and would never recheck. This option ensures that the host always has EDID information when the client is in session.<br>The following default resolutions are advertised when this option is enabled:<br>• 2560x1600 @60 Hz<br>• 2048x1152 @60 Hz<br>• 1920x1440 @60 Hz<br>• 1920x1200 @60 Hz<br>• 1920x1080 @60 Hz<br>• 1856x1392 @60 Hz<br>• 1792x1344 @60 Hz<br>• 1680x1050 @60 Hz<br>• 1600x1200 @60 Hz<br>• 1600x900 @60 Hz |

| Parameter | Description |
|---|---|
| | - 1440x900 @60 Hz<br>- 1400x1050 @60 Hz<br>- 1366x768 @60 Hz<br>- 1360x768 @60 Hz<br>- 1280x1024 @60 Hz<br>- 1280x960 @60 Hz<br>- 1280x800 @60 Hz<br>- 1280x768 @60 Hz<br>- 1280x720 @60 Hz<br>- 1024x768 @60 Hz<br>- 848x480 @60 Hz<br>- 800x600 @60 Hz<br>- 640x480 @60 Hz<br>Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled. |
| Enable Preferred Resolution Override | Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions as above will be advertised, except the preferred resolution you configure here for a display will be sent as the native resolution instead of the default native resolution of 1024x768.<br>- **Preferred resolution 0**: Select the preferred resolution of the display connected to port 1 on the zero client.<br>- **Preferred resolution 1**: Select the preferred resolution of the display connected to port 2 on the zero client.<br>Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled. |

## 5.26.2 OSD Quad-display: Display Settings

The **Display** page lets you enable the Extended Display Identification Data (EDID) override mode.

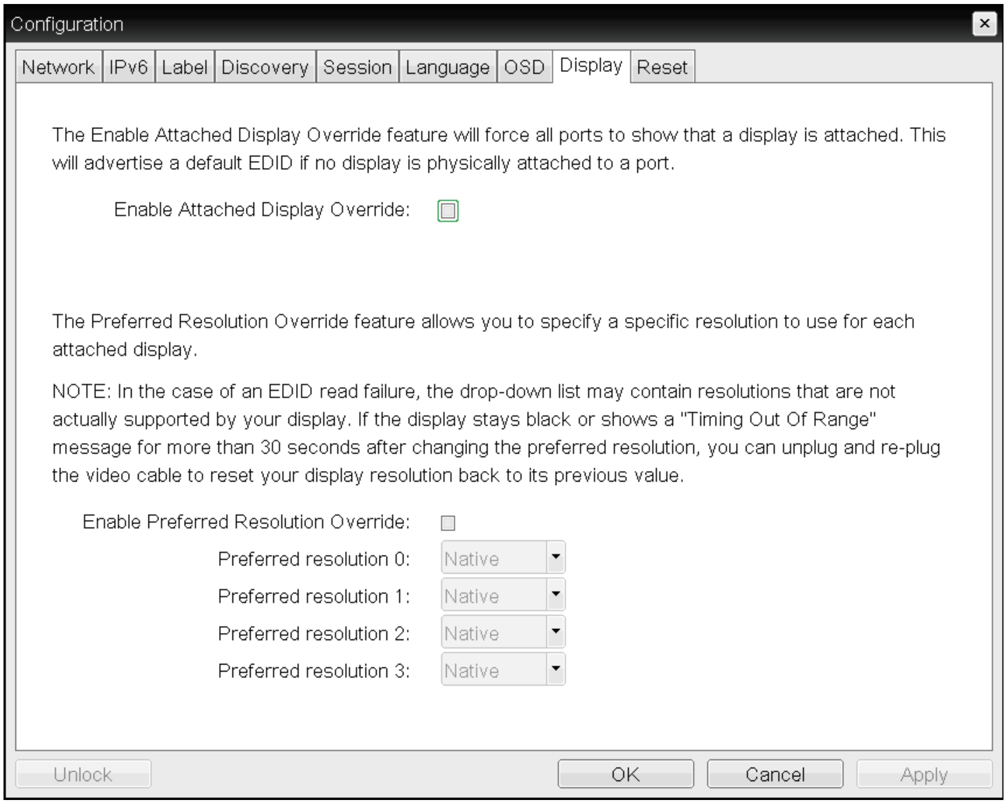
Note: This function is only available through the OSD.

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

Warning: You should only enable the Preferred Resolution 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 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.

Note: If you are using the TERA2321 zero client device as your client, preferred resolution settings for only two monitors will display on this page, as shown here.



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

Enable Attached Display Override: □

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

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

Enable Preferred Resolution Override: □

Preferred resolution 0: Native

Preferred resolution 1: Native

Preferred resolution 2: Native

Preferred resolution 3: Native

**Figure 5-104: OSD Tera2 Display Page**

**Table 5-93: OSD Tera2 Display Page Parameters**

| **Parameter** | **Description** |
|---|---|
| Enable Attached Display Override | This option is intended for legacy systems. It configures the client to send default EDID information to the host when a monitor cannot be detected or is not attached to the client. In versions of Windows prior to Windows 7, once the host had no EDID information, it would assume no monitors were attached and would never recheck. This option ensures that the host always has EDID information when the client is in session.<br>The following default resolutions are advertised when this option is enabled:<br>• 2560x1600 @60 Hz<br>• 2048x1152 @60 Hz<br>• 1920x1440 @60 Hz<br>• 1920x1200 @60 Hz<br>• 1920x1080 @60 Hz |

| Parameter | Description |
|---|---|
| | • 1856x1392 @60 Hz<br>• 1792x1344 @60 Hz<br>• 1680x1050 @60 Hz<br>• 1600x1200 @60 Hz<br>• 1600x900 @60 Hz<br>• 1440x900 @60 Hz<br>• 1400x1050 @60 Hz<br>• 1366x768 @60 Hz<br>• 1360x768 @60 Hz<br>• 1280x1024 @60 Hz<br>• 1280x960 @60 Hz<br>• 1280x800 @60 Hz<br>• 1280x768 @60 Hz<br>• 1280x720 @60 Hz<br>• 1024x768 @60 Hz<br>• 848x480 @60 Hz<br>• 800x600 @60 Hz<br>• 640x480 @60 Hz<br>Any displays attached to the client will be set to the native resolution of 1024x768 when this option is enabled. |
| Enable Preferred Resolution Override | Enable this option when a display is attached but cannot be detected by the system, and you want to specify a preferred resolution for the display. The same default list of resolutions as above will be advertised, except the preferred resolution you configure here for a display will be sent as the native resolution instead of the default native resolution of 1024x768.<br>• **Preferred resolution 0**: Select the preferred resolution of the display connected to port 1 on the zero client.<br>• **Preferred resolution 1**: Select the preferred resolution of the display connected to port 2 on the zero client.<br>• **Preferred resolution 2**: Select the preferred resolution of the display connected to port 3 on the zero client.<br>• **Preferred resolution 3**: Select the preferred resolution of the display connected to port 4 on the zero client.<br>Any displays attached to the client will be set to their specified preferred resolutions when this option is enabled. |

## 5.27 Configuring Password and Reset Parameters (AWI/OSD)

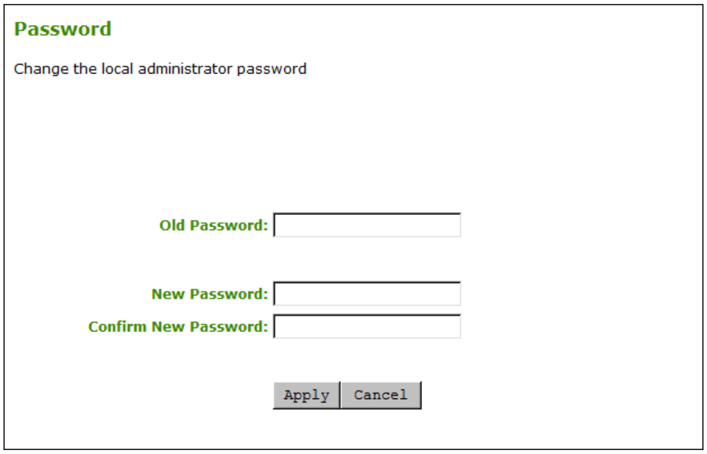
### 5.27.1 AWI: Password Settings

The **Password** page lets you update the local administrative password for the device. You can access this page for the host or client 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 on the MC's Security Configuration page.

Note: This parameter affects the AWI and the local OSD GUI. Take care when updating the client password as the client may become unusable if the password is lost.



Password

Change the local administrator password

Old Password:

New Password:

Confirm New Password:

Figure 5-105: AWI Password Page

Table 5-94: AWI Password Page Parameters

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

### 5.27.2 OSD: Password Settings

The **Password** page lets you update the local administrative password for the device. You can access this page from the **Options** > **Password** menu.

The password can be a maximum of 20 characters. Some PCoIP devices have password protection disabled by default, and the **Password** page is not available on these devices. You can enable password protection for these devices on the MC's Security Configuration page.

Note: This parameter affects the AWI and the local OSD GUI. Take care when updating the client password as the client may become unusable if the password is lost.

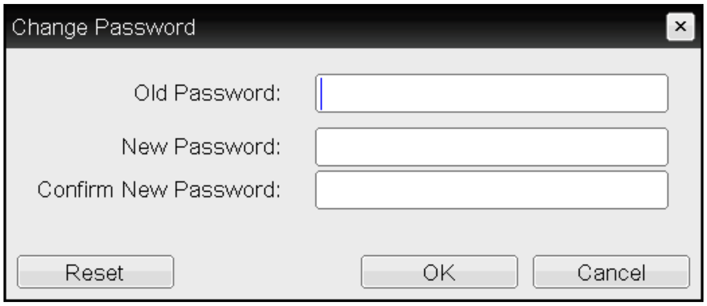


**Figure 5-106: OSD Change Password Page**

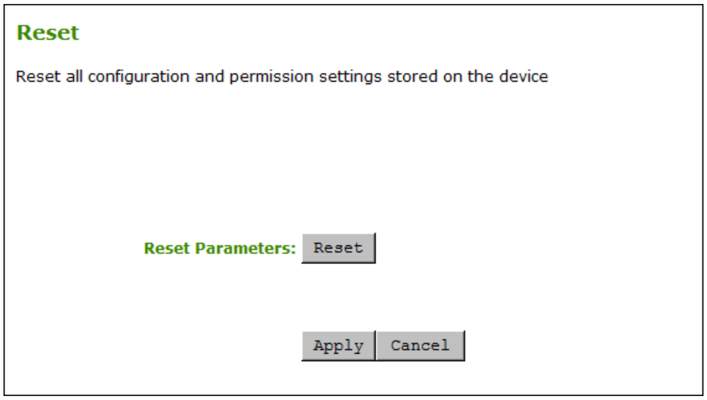
**Table 5-95: OSD Change Password Page Parameters**

| Parameter | Description |
|---|---|
| Old Password | This field must match the current administrative password before you can update the password. |
| New Password | The new administrative password for both the AWI and the local OSD GUI. |
| Confirm New Password | This field must match the **New Password** field for the change to take place. |
| Reset | If the client password becomes lost, you can click the **Reset** button to request a response code from the zero client vendor. The challenge code is sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password.<br>Note: Contact the client vendor for more information when an authorized password reset is required. This option is not available through the AWI. It is only available through the OSD. |

## 5.27.3 AWI Host: Parameter Reset Settings

The **Reset Parameters** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Configuration** > **Reset Parameters** menu.

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



Reset

Reset all configuration and permission settings stored on the device

Reset Parameters: Reset

Figure 5-107: AWI Host Reset Page

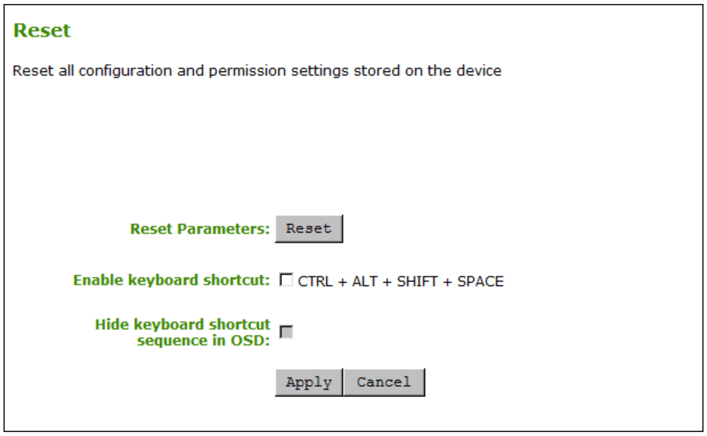
Table 5-96: AWI Host Reset Parameters

| Parameter | Description |
|---|---|
| Reset Parameters | When you click this button, a prompt appears for confirmation. This is to prevent accidental resets. |

## 5.27.4 AWI Client: Parameter Reset Settings

The **Reset Parameters** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Configuration** > **Reset Parameters** menu.

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



Reset

Reset all configuration and permission settings stored on the device

Reset Parameters: Reset

Enable keyboard shortcut: ☐ CTRL + ALT + SHIFT + SPACE

Hide keyboard shortcut sequence in OSD: ☐

Figure 5-108: AWI Client Reset Page

Table 5-97: AWI Client Reset Parameters

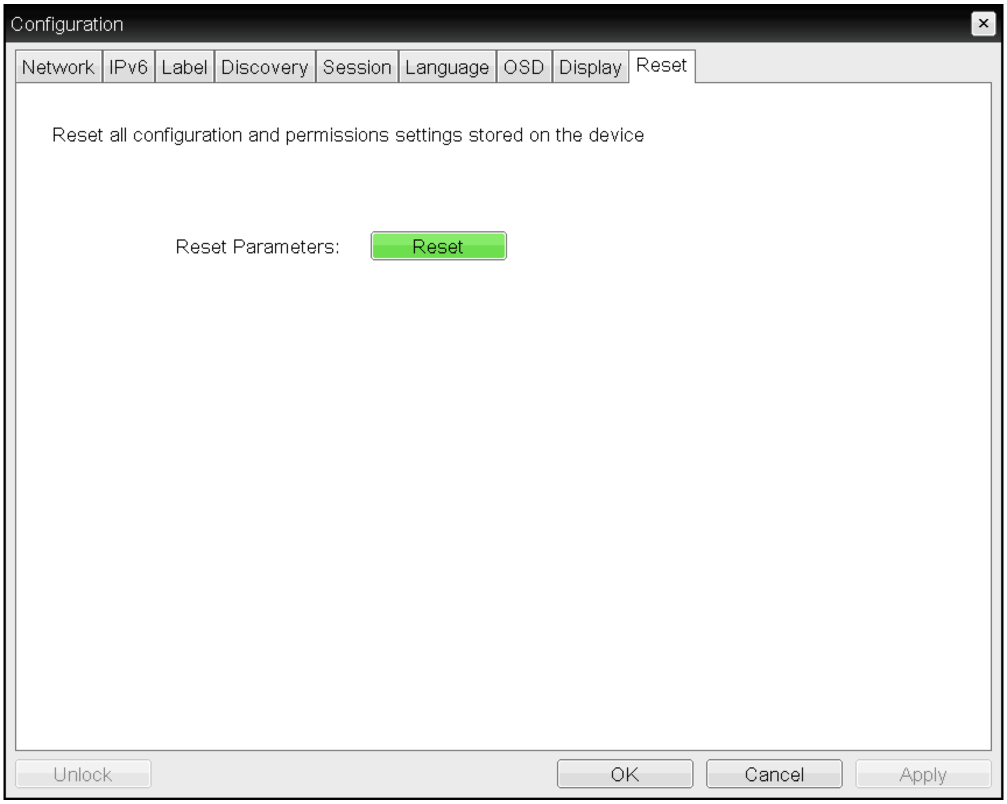
| Parameter | Description |
|---|---|
| Reset Parameters | When you click this button, a prompt appears for confirmation. This is |

| Parameter | Description |
|---|---|
| | 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.<br>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. |

## 5.27.5 OSD: Parameter Reset Settings

The **Reset** page lets you reset configuration and permissions to factory default values stored in flash memory. You can access this page from the **Options** > **Configuration** > **Reset** menu.

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



Reset all configuration and permissions settings stored on the device

Reset Parameters: Reset

Figure 5-109: OSD Reset Page

**Table 5-98: OSD Reset Parameters**

| Parameter | Description |
|---|---|
| Reset Parameters | When you click this button, a prompt appears for confirmation. This is to prevent accidental resets. |

# 5.28 Viewing Diagnostics (AWI/OSD)

## 5.28.1 AWI: Help for Event Log Settings

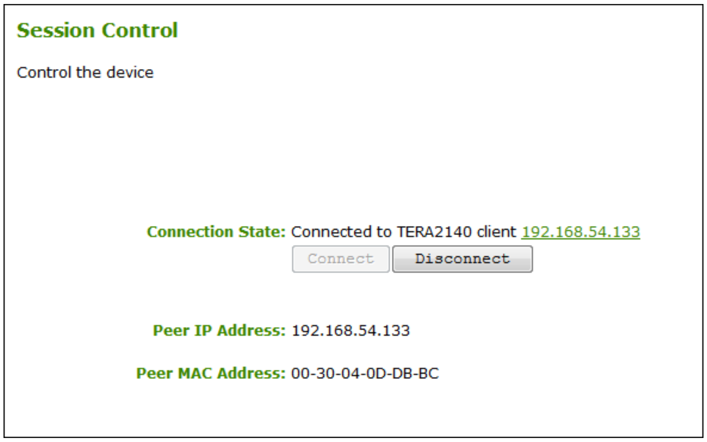
For information about the AWI's **Event Log** page, see AWI: Event Log Settings.

## 5.28.2 OSD: Help for Event Log Settings

For information about the OSD's **Event Log** page, see OSD: Event Log Settings.

## 5.28.3 AWI Host: Session Control Settings

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



Session Control

Control the device

Connection State: Connected to TERA2140 client 192.168.54.133

Peer IP Address: 192.168.54.133

Peer MAC Address: 00-30-04-0D-DB-BC

**Figure 5-110: AWI Host Session Control Page**

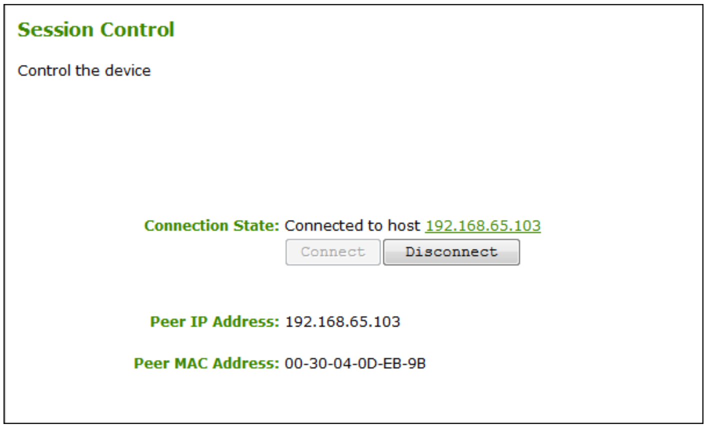
**Table 5-99: AWI Host Session Control Page Parameters**

| Parameter | Description |
|---|---|
| Connection State | This field displays the current state for the session. Options include the following:<br>• **Disconnected**<br>• **Connection Pending**<br>• **Connected**<br>Two buttons appear below the **Connection State** field:<br>• **Connect:**This button is disabled for the host. |

| Parameter | Description |
|---|---|
|  | • **Disconnect:** If the connection state is **Connected** or **Connection Pending**, click this button to end the PCoIP session for the device. If the connection state is **Disconnected**, this button is disabled. |
| Peer IP | **Peer IP Address:** Displays the IP address for the peer device. When not in session, this field is blank. |
| Peer MAC Address | **Peer MAC Address:** Displays the MAC address of the peer device. When not in session, this field is blank. |

## 5.28.4 AWI Client: Session Control Settings

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



Session Control

Control the device

Connection State: Connected to host 192.168.65.103

Peer IP Address: 192.168.65.103

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

**Figure 5-111: AWI Client Session Control Page**

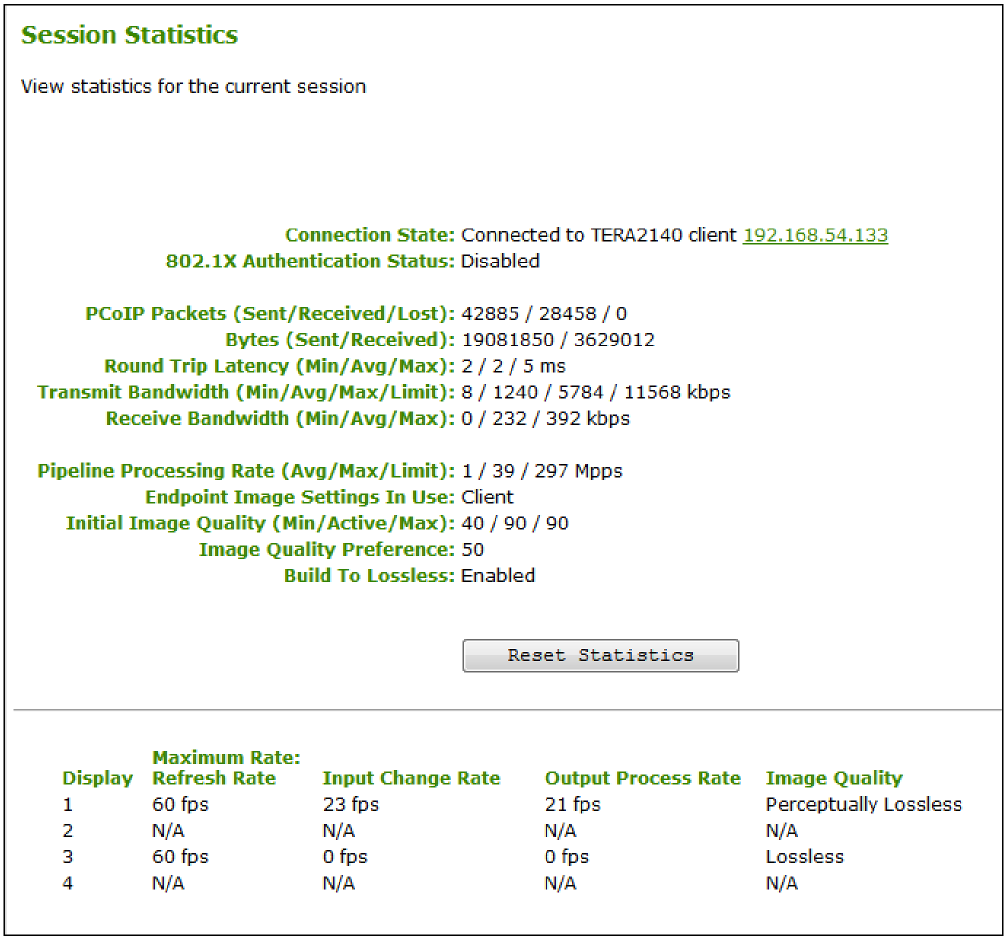
**Table 5-100: AWI Client Session Control Page Parameters**

| Parameter | Description |
|---|---|
| Connection State | This field displays the current state for the session. Options include the following:<br>• **Disconnected**<br>• **Connection Pending**<br>• **Connected**<br>Two buttons appear below the **Connection State** field:<br>• **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.<br>• **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. |

| Parameter | Description |
|---|---|
| Peer IP | **Peer IP Address:** Displays the IP address for the peer device. When not in session, this field is blank. |
| Peer MAC Address | **Peer MAC Address:** Displays the MAC address of the peer device. When not in session, this field is blank. |

## 5.28.5 AWI Host: Session Statistics Settings

The **Session Statistics** page lets you view current statistics when a session is active. If a session is not active, the statistics from the last session will display. You can view this page from the **Diagnostics > Session Statistics** menu.



Session Statistics

View statistics for the current session

Connection State: Connected to TERA2140 client 192.168.54.133
802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 42885 / 28458 / 0
Bytes (Sent/Received): 19081850 / 3629012
Round Trip Latency (Min/Avg/Max): 2 / 2 / 5 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 1240 / 5784 / 11568 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 232 / 392 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 39 / 297 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Active/Max): 40 / 90 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

| Display | Maximum Rate:<br>Refresh Rate | Input Change Rate | Output Process Rate | Image Quality |
|---|---|---|---|---|
| 1 | 60 fps | 23 fps | 21 fps | Perceptually Lossless |
| 2 | N/A | N/A | N/A | N/A |
| 3 | 60 fps | 0 fps | 0 fps | Lossless |
| 4 | N/A | N/A | N/A | N/A |

**Figure 5-112: AWI Host Session Statistics Page**

Note: The above figure shows session statistics for a host card connected to a client with four connected displays. If your deployment uses two displays, information for only two displays will appear in this section.

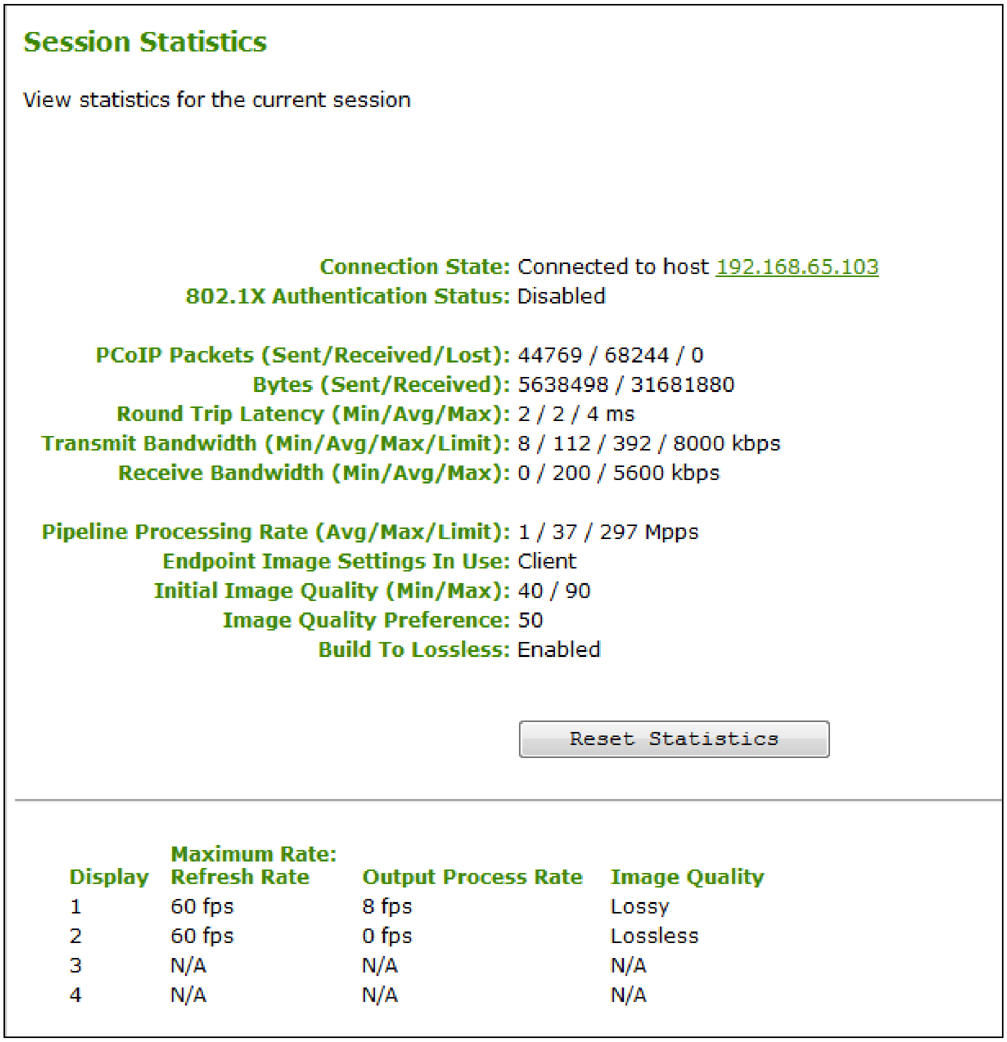
**Table 5-101: AWI Host Session Statistics Page Parameters**

| Parameters | Description |
|---|---|
| Connection State | The current (or last) state of the PCoIP session. Values include the following:<br>● **Asleep**<br>● **Canceling**<br>● **Connected**<br>● **Connection Pending**<br>● **Disconnected**<br>● **Waking** |
| 802.1X Authentication Status | Indicates whether 802.1X authentication is enabled or disabled on the device. |
| PCoIP Packets Statistics | **PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session.<br>**PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session.<br>**PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session. |
| Bytes | **Bytes Sent:** The total number of bytes sent in the current/last session.<br>**Bytes Received:** The total number of bytes received in the current/last session. |
| Round Trip Latency | The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms). |
| Bandwidth Statistics | **Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels.<br>**Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor. |
| Pipeline Processing Rate | How much image data is currently being processed by the image engine (in megapixels per second). |
| Endpoint Image Settings In Use | Displays if the image settings being used are configured within the client or within the host. This is based on how the **Use Client Image Settings** field is configured on the **Image** page for the host device. |
| Initial Image Quality | The minimum and maximum quality setting is taken from the **Image** page for the device.<br>The active setting is what's currently being used in the session and only appears on the host. |

| Parameters | Description |
|---|---|
| Image Quality Preference | This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image. |
| Build to Lossless | Options that may appear in this field include the following:<br>**Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked.<br>**Disabled:** The **Disable Build to Lossless** field is checked. |
| Reset Statistics | Click this button to reset the statistic information on this page.<br>Note: The **Reset Statistics** button also resets the statistics reported in the **Home** page. |
| Display | The port number for the display. |
| Maximum Rate | This column shows the refresh rate of the attached display.<br>If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate.<br>If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined." |
| Input Change Rate | The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video). |
| Output Process Rate | The frame rate currently being sent from the image engine on the host to the client. |
| Image Quality | Shows the current lossless state of the attached display:<br>● **Lossy**<br>● **Perceptually lossless**<br>● **Lossless** |

## 5.28.6 AWI Client: Session Statistics Settings

The **Session Statistics** page lets you view current statistics when a session is active. If a session is not active, the statistics from the last session will display. You can view 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 |

**Figure 5-113: AWI Client Session Statistics Page**

Note: The above figure shows session statistics for a client with two connected displays. If your deployment uses four displays, information for all four displays will appear in this section.

**Table 5-102: AWI Client Session Statistics Page Parameters**

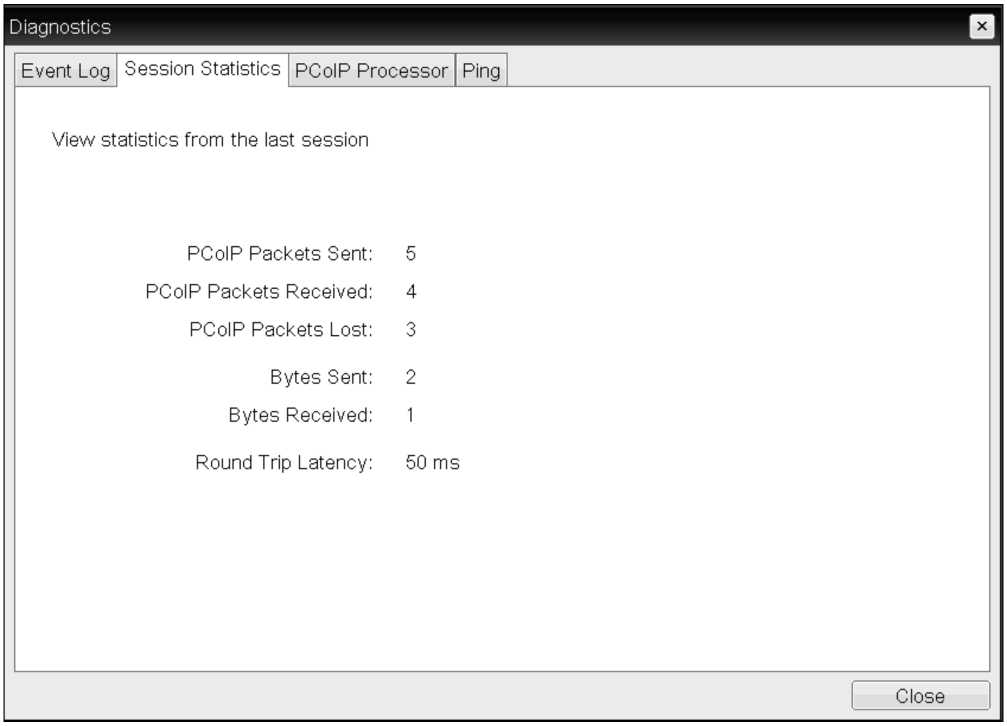
| Parameters | Description |
|---|---|
| Connection State | The current (or last) state of the PCoIP session. Values include the following:<br>• **Asleep**<br>• **Canceling**<br>• **Connected**<br>• **Connection Pending**<br>• **Disconnected** |

| Parameters | Description |
|---|---|
| | - **Waking** |
| 802.1X Authentication Status | Indicates whether 802.1X authentication is enabled or disabled on the device. |
| PCoIP Packets Statistics | **PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session.<br>**PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session.<br>**PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session. |
| Bytes | **Bytes Sent:** The total number of bytes sent in the current/last session.<br>**Bytes Received:** The total number of bytes received in the current/last session. |
| Round Trip Latency | The minimum, average, and maximum round-trip PCoIP system and network latency in milliseconds (+/- 1 ms). |
| Bandwidth Statistics | **Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera processor. The active bandwidth limit is the maximum amount of network traffic the Tera processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels.<br>**Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera processor. |
| Pipeline Processing Rate | How much image data is currently being processed by the image engine (in megapixels per second). |
| Endpoint Image Settings In Use | Displays if the image settings being used are configured within the client or within the host. This is based on how the **Use Client Image Settings** field is configured on the **Image** page for the host device. |
| Initial Image Quality | The minimum and maximum quality setting is taken from the **Image** page for the device. |
| Image Quality Preference | This setting is taken from the **Image Quality Preference** field on the **Image** page. The value determines if the image is set to a smoother versus a sharper image. |
| Build to Lossless | Options that may appear in this field include the following:<br>**Enabled:** The **Disable Build to Lossless** field on the **Image** page is unchecked.<br>**Disabled:** The **Disable Build to Lossless** field is checked. |
| Reset Statistics | Click this button to reset the statistic information on this page.<br>Note: The **Reset Statistics** button also resets the statistics reported in the **Home** page. |

| Parameters | Description |
|---|---|
| Display | The port number for the display. |
| Maximum Rate | This column shows the refresh rate of the attached display.<br>If the **Maximum Rate** field on the **Image** page is set to 0 (i.e., there is no limit), the maximum rate is taken from the monitor's refresh rate.<br>If the **Maximum Rate** field on the **Image** page is set to a value greater than 0, the refresh rate shows as "User Defined." |
| Output Process Rate | The frame rate currently being sent from the image engine on the host to the client. |
| Image Quality | Shows the current lossless state of the attached display:<br>• **Lossy**<br>• **Perceptually lossless**<br>• **Lossless** |

## 5.28.7 OSD:Session Statistics Settings

The **Session Statistics** page lets you view from the last session. You can view this page from the **Options** > **Diagnostics** > **Session Statistics** menu.



View statistics from the last session

PCoIP Packets Sent: 5
PCoIP Packets Received: 4
PCoIP Packets Lost: 3
Bytes Sent: 2
Bytes Received: 1
Round Trip Latency: 50 ms

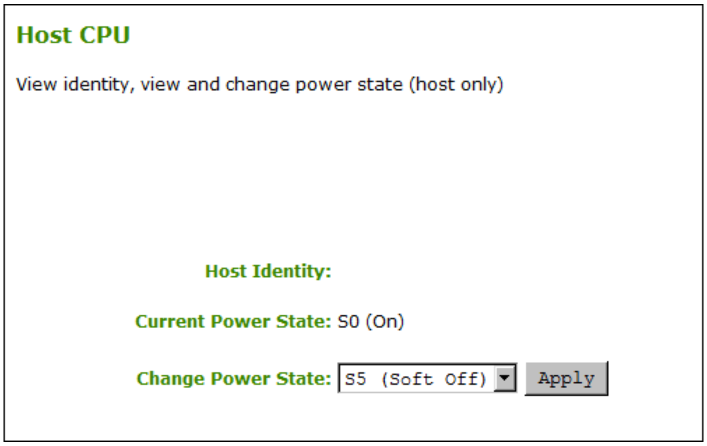
**Figure 5-114: OSD Session Statistics Page**

**Table 5-103: OSD Session Statistics Page Parameters**

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

## 5.28.8 AWI Host: Host CPU Settings

The **Host CPU** page lets you view the identity string of the host computer, view the current power state, and change the host's power state. You can access this page from the **Diagnostics** > **Host CPU** menu.



Host CPU

View identity, view and change power state (host only)

Host Identity:

Current Power State: S0 (On)

Change Power State: S5 (Soft Off)

**Figure 5-115: AWI Host CPU Page**

**Table 5-104: AWI Host CPU Page Parameters**

| Parameters | Description |
|---|---|
| Host Identity | The identity string of the host computer (if data is available). |
| Current Power State | The current power state that is configured for the host. |
| Change Power State | Select one of the following options:<br>• **S5 (Soft Off)**: Configures the client's remote PC button to perform a soft power off of the host (i.e., to put the host in sleep mode) |

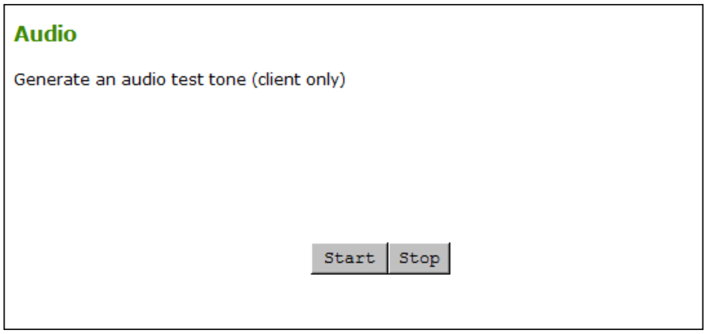
| Parameters | Description |
|---|---|
| | when the button is pressed for less than four seconds.<br>• **S5 (Hard Off)**: Configures the client' remote PC button to perform a hard power off of the host (i.e., a device shutdown) when the button is pressed for more than four seconds.<br>Note: To use this feature, the host must have compatible hardware architecture. |

## 5.28.9 AWI Client: Audio Settings

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

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

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


Audio

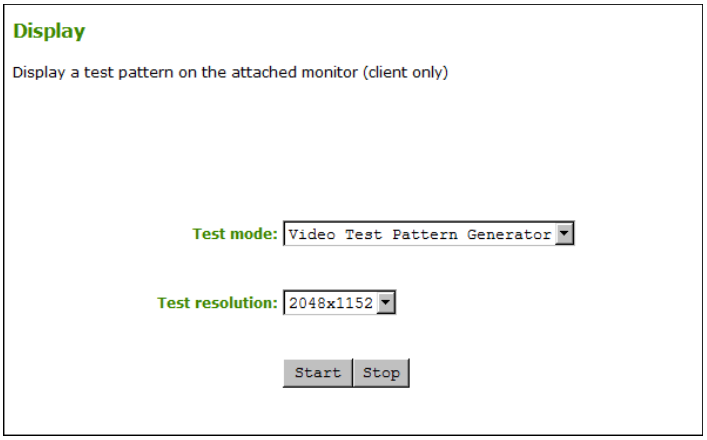
Generate an audio test tone (client only)

**Figure 5-116: AWI Client Audio Page**

## 5.28.10AWI Client: Display Settings

The **Display** page lets you initiate and view a test pattern on the client's display. You can access the page from the **Diagnostics** > **Display** menu.

Note: The test pattern only appears on the **Display** page when the client is not in a PCoIP session. If you click **Start** when the client is in session, an error message appears.



Display

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

Test mode: Video Test Pattern Generator

Test resolution: 2048x1152

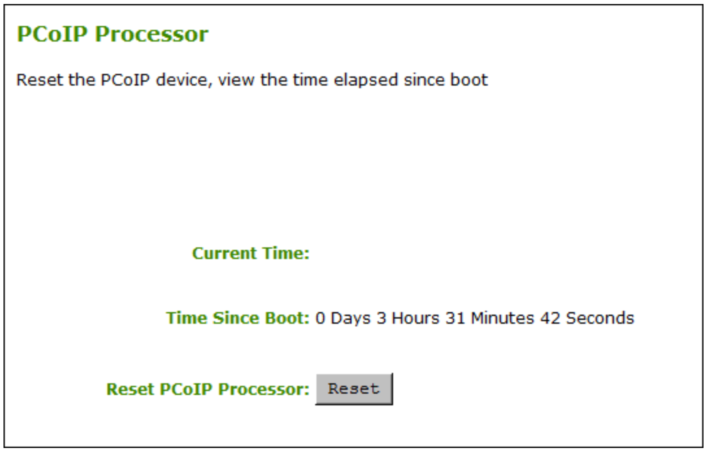
Figure 5-117: AWI Client Display Page

Table 5-105: AWI Client Display Page Parameters

| Parameters | Description |
|---|---|
| Test mode | Set the type of test pattern for the attached monitor(s) as follows:<br>• **Video Test Pattern Generator**<br>• **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. |

## 5.28.11AWI: PCoIP Processor Settings

The **PCoIP Processor** page lets you reset the host or client and view the uptime of the device's PCoIP processor since the last boot. You can access this page from the **Diagnostics** > **PCoIP Processor** menu.



PCoIP Processor

Reset the PCoIP device, view the time elapsed since boot

Current Time:

Time Since Boot: 0 Days 3 Hours 31 Minutes 42 Seconds

Reset PCoIP Processor:

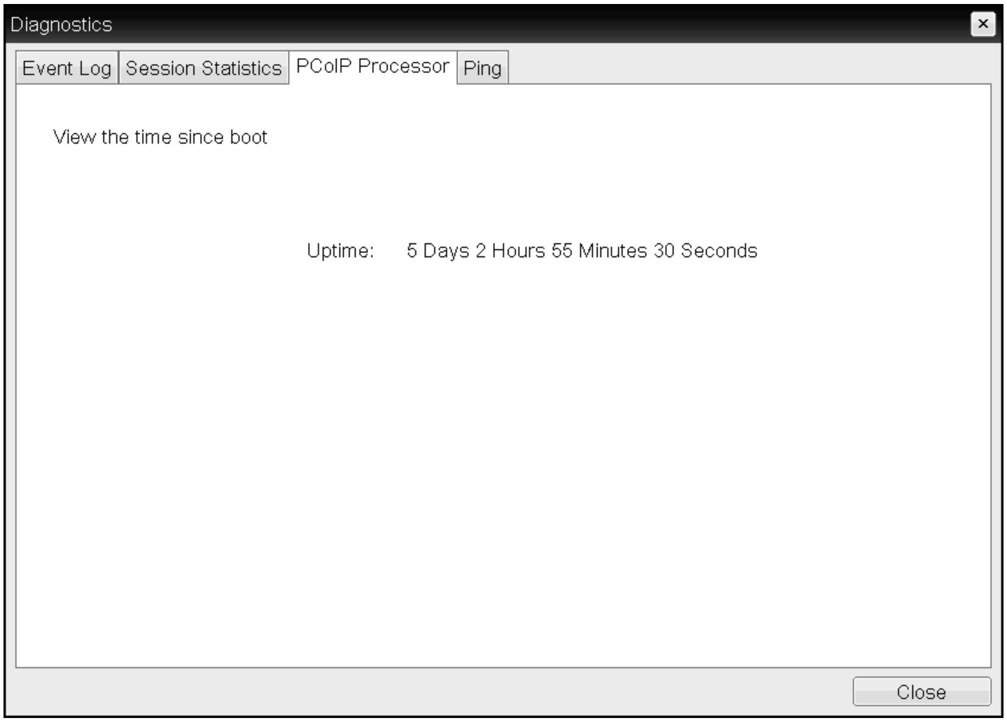
Figure 5-118: AWI PCoIP Processor Page

**Table 5-106: AWI PCoIP Processor Page Parameters**

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

## 5.28.12OSD: PCoIP Processor Settings

The **PCoIP Processor** page lets you view the uptime of the device's PCoIP processor since the last boot. You can access this page from the **Options** > **Diagnostics** > **PCoIP Processor** menu.



View the time since boot

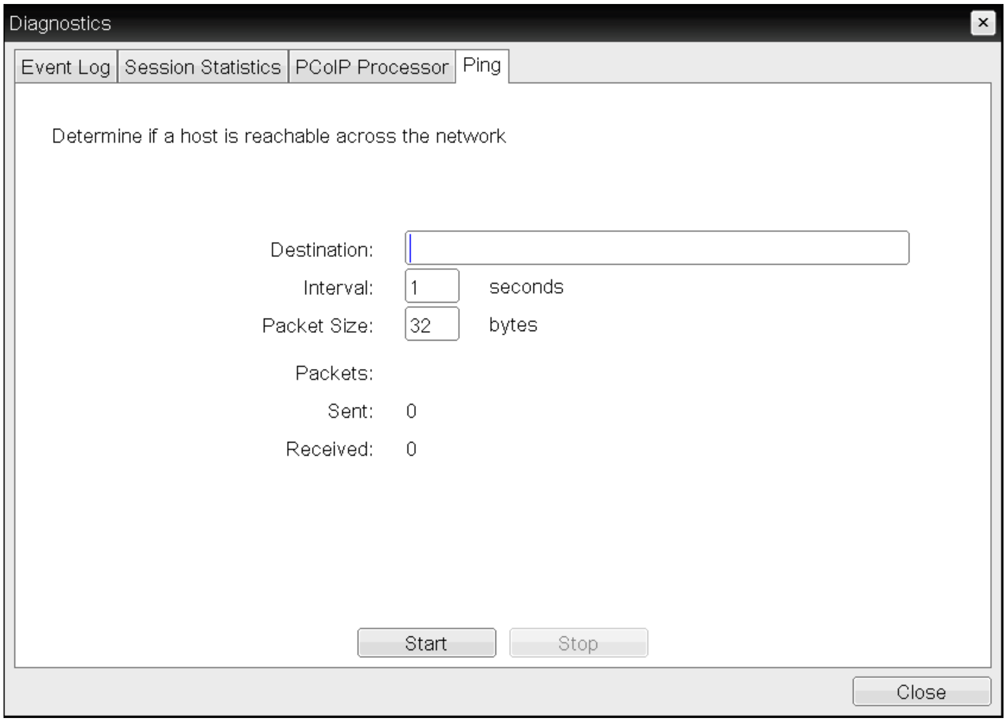
Uptime: 5 Days 2 Hours 55 Minutes 30 Seconds

**Figure 5-119: OSD PCoIP Processor Page**

## 5.28.13OSD: Ping Settings

The **Ping** page lets you ping a device to see if it is reachable across the IP network. This may help you determine if a host is reachable. Because firmware releases 3.2.0 and later force the “do not fragment flag” in the ping command, you can also use this feature to determine the maximum MTU size.

You can access this page from the **Options** > **Diagnostics** > **Ping** menu.



Determine if a host is reachable across the network

Destination:

Interval: 1 seconds

Packet Size: 32 bytes

Packets:

Sent: 0

Received: 0

**Figure 5-120: OSD Ping Page**

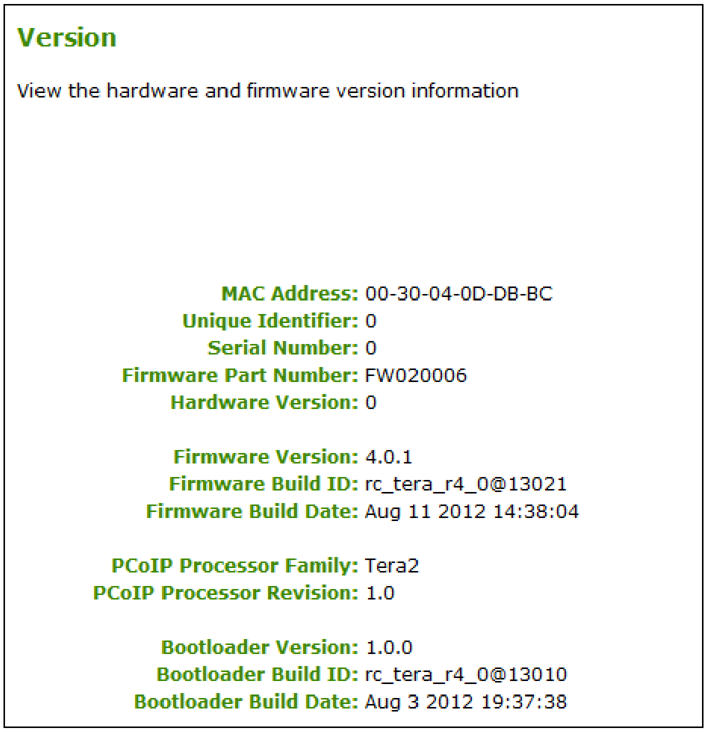
**Table 5-107: Ping Page Parameters**

| Parameter | Description |
|---|---|
| Destination | IP address or fully qualified domain name (FQDN) to ping. |
| Interval | Interval between ping packets. |
| Packet Size | Size of the ping packet. |
| Packets Sent | Number of ping packets transmitted. |
| Packets Received | Number of ping packets received. |

# 5.29 Viewing Information (AWI/OSD)

## 5.29.1 AWI: Version Information

The **Version** page lets you view the hardware and firmware version details for a device. You can access this page from the **Info** > **Version** menu.



Version

View the hardware and firmware version information

| | |
|---|---|
| MAC Address: | 00-30-04-0D-DB-BC |
| Unique Identifier: | 0 |
| Serial Number: | 0 |
| Firmware Part Number: | FW020006 |
| Hardware Version: | 0 |
| Firmware Version: | 4.0.1 |
| Firmware Build ID: | rc_tera_r4_0@13021 |
| Firmware Build Date: | Aug 11 2012 14:38:04 |
| 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 |

**Figure 5-121: AWI Version Page**

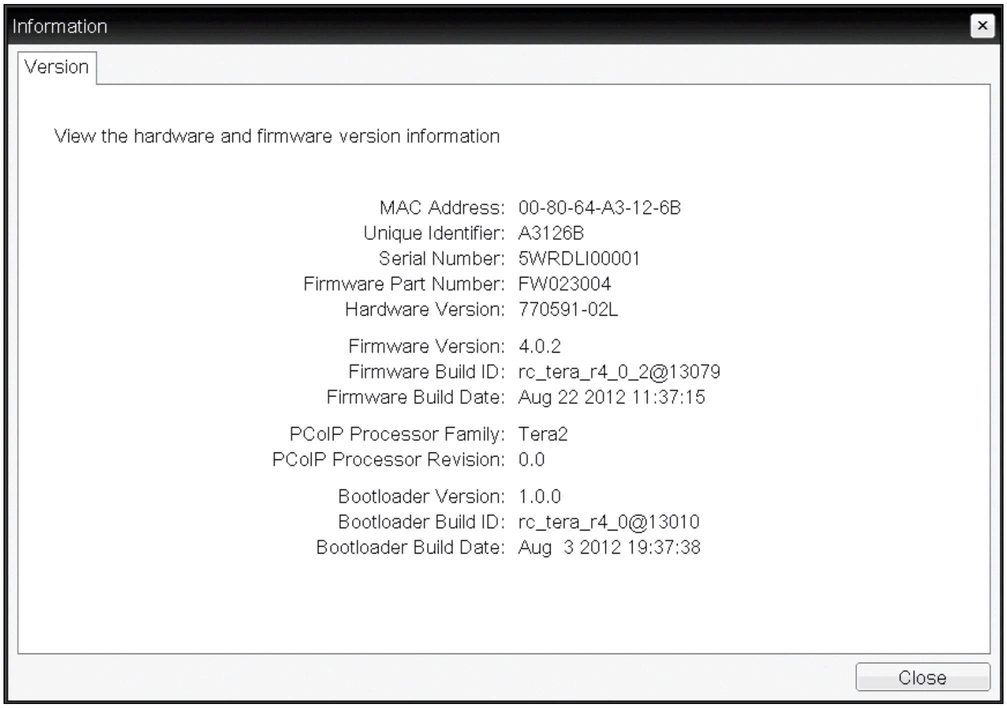
**Table 5-108: AWI Version Page Parameters**

| Parameters | Description |
|---|---|
| VPD Information | **(Vital Product Data)**: Information provisioned by the factory to uniquely identify each host or client:<br>• **MAC Address:** Host/client unique MAC address.<br>• **Unique Identifier:** Host/client unique identifier.<br>• **Serial Number:** Host/client unique serial number.<br>• **Firmware Part Number:** Part number of the current firmware.<br>• **Hardware Version:** Host/client hardware version number. |
| Firmware Information | This information reflects the current firmware details:<br>• **Firmware Version:** Version of the current firmware.<br>• **Firmware Build ID:** Revision code of the current firmware.<br>• **Firmware Build Date:** Build date for the current firmware. |
| PCoIP Processor Information | This information provides details about the PCoIP processor.<br>• **PCoIP Processor Family**: The processor family—Tera1 or Tera2.<br>• **PCoIP Processor Revision**: The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0. |
| Bootloader Information | This information reflects the current firmware bootloader details:<br>• **Boatloader Version:** Version of the current bootloader.<br>• **Bootloader Build ID:** Revision code of the current bootloader. |

| Parameters | Description |
|---|---|
| | • **Bootloader Build Date:** Build date of the current bootloader. |

## 5.29.2 Viewing the Version Information

The **Version** page lets you view the hardware and firmware version details for a device. You can access this page from the **Options > Information > Version** menu.



View the hardware and firmware version information

```
          MAC Address:  00-80-64-A3-12-6B
    Unique Identifier:  A3126B
        Serial Number:  5WRDLI00001
 Firmware Part Number:  FW023004
     Hardware Version:  770591-02L

     Firmware Version:  4.0.2
    Firmware Build ID:  rc_tera_r4_0_2@13079
  Firmware Build Date:  Aug 22 2012 11:37:15

PCoIP Processor Family:  Tera2
PCoIP Processor Revision:  0.0

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

**Figure 5-122: OSD Version Page**

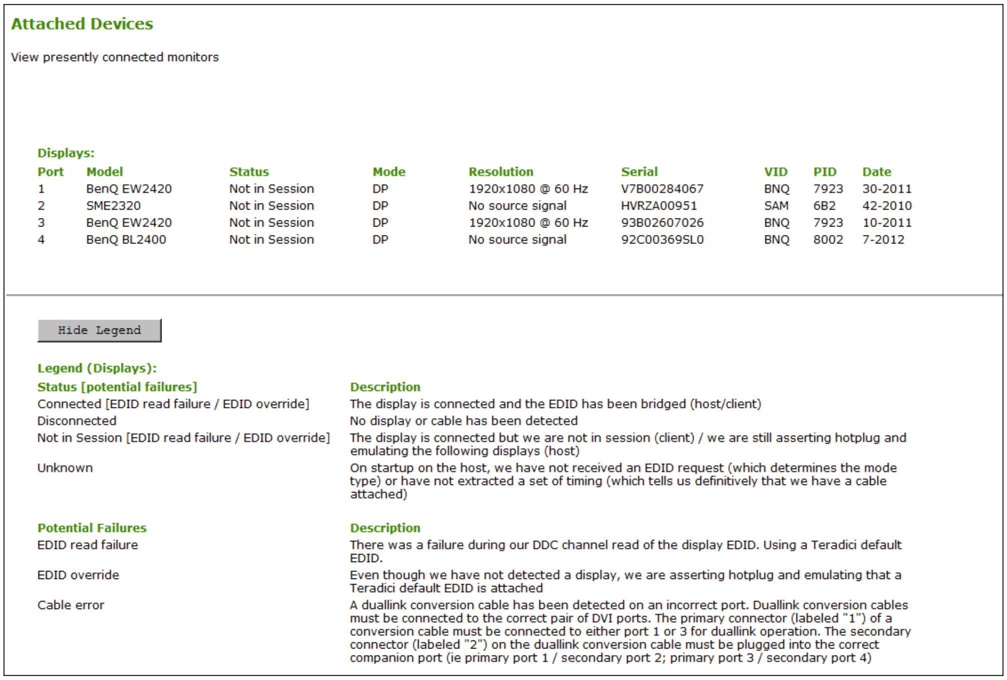
**Table 5-109: OSD Version Page Parameters**

| Parameters | Description |
|---|---|
| VPD Information | **(Vital Product Data)**: Information provisioned by the factory to uniquely identify each host or client:<br>• **MAC Address:** Host/client unique MAC address.<br>• **Unique Identifier:** Host/client unique identifier.<br>• **Serial Number:** Host/client unique serial number.<br>• **Firmware Part Number:** Part number of the current firmware.<br>• **Hardware Version:** Host/client hardware version number. |
| Firmware Information | This information reflects the current firmware details:<br>• **Firmware Version:** Version of the current firmware.<br>• **Firmware Build ID:** Revision code of the current firmware.<br>• **Firmware Build Date:** Build date for the current firmware. |

| Parameters | Description |
|---|---|
| PCoIP Processor Information | This information provides details about the PCoIP processor.<br>• **PCoIP Processor Family**: The processor family—Tera1 or Tera2.<br>• **PCoIP Processor Revision**: The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0. |
| Bootloader Information | This information reflects the current firmware bootloader details:<br>• **Boatloader Version:** Version of the current bootloader.<br>• **Bootloader Build ID:** Revision code of the current bootloader.<br>• **Bootloader Build Date:** Build date of the current bootloader. |

## 5.29.3 AWI Host: Attached Devices Information

The **Attached Devices** page lets you see information for the displays that are currently attached to the client.



Attached Devices

View presently connected monitors

Displays:

| Port | Model | Status | Mode | Resolution | Serial | VID | PID | Date |
|---|---|---|---|---|---|---|---|---|
| 1 | BenQ EW2420 | Not in Session | DP | 1920x1080 @ 60 Hz | V7B00284067 | BNQ | 7923 | 30-2011 |
| 2 | SME2320 | Not in Session | DP | No source signal | HVRZA00951 | SAM | 6B2 | 42-2010 |
| 3 | BenQ EW2420 | Not in Session | DP | 1920x1080 @ 60 Hz | 93B02607026 | BNQ | 7923 | 10-2011 |
| 4 | BenQ BL2400 | Not in Session | DP | No source signal | 92C00369SL0 | BNQ | 8002 | 7-2012 |

Legend (Displays):

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

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

**Figure 5-123: AWI Host Attached Devices Page**

Note: The above figure shows information for a client with four connected displays. If your deployment uses two displays, information for only two displays will appear on this page.

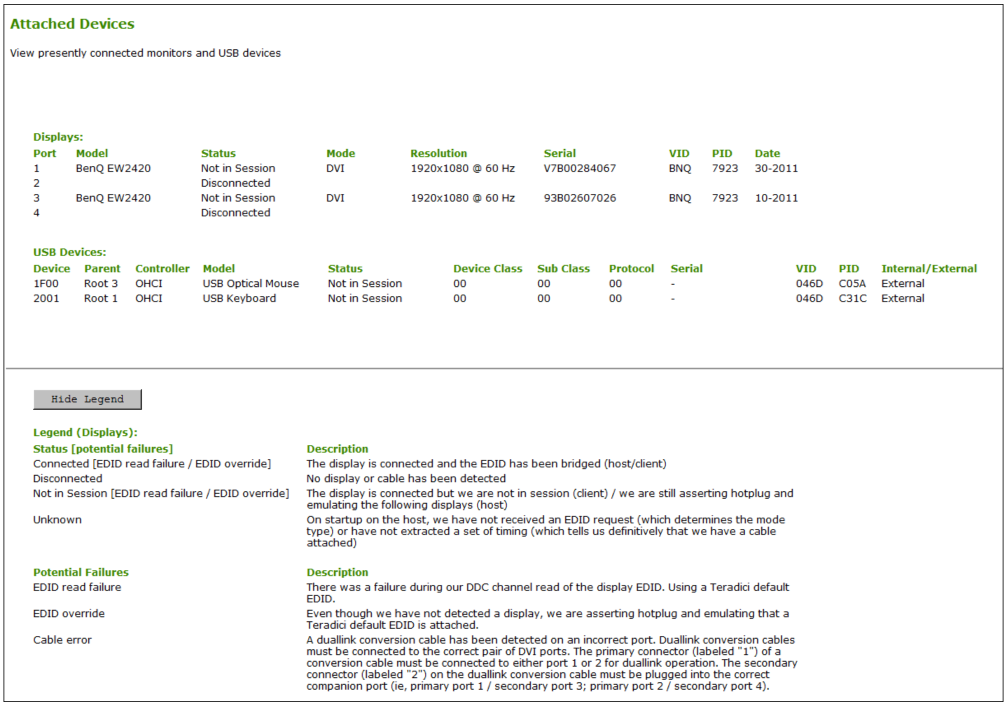
**Table 5-110: AWI Host: Attached Devices Page Information**

| Statistic | Description |
|---|---|
| Displays | This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the display attached to each port. |

| Statistic | Description |
|---|---|
|  | Note: This option is only available when the host is in a PCoIP session. |

## 5.29.4 AWI Client: Attached Devices Information

The **Attached Devices** page lets you see information for the displays that are currently attached to the client.



Attached Devices

View presently connected monitors and USB devices

Displays:

| Port | Model | Status | Mode | Resolution | Serial | VID | PID | Date |
|---|---|---|---|---|---|---|---|---|
| 1 | BenQ EW2420 | Not in Session | DVI | 1920x1080 @ 60 Hz | V7B00284067 | BNQ | 7923 | 30-2011 |
| 2 |  | Disconnected |  |  |  |  |  |  |
| 3 | BenQ EW2420 | Not in Session | DVI | 1920x1080 @ 60 Hz | 93B02607026 | 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 | Not in Session | 00 | 00 | 00 | - | 046D | C05A | External |
| 2001 | Root 1 | OHCI | USB Keyboard | Not in Session | 00 | 00 | 00 | - | 046D | C31C | External |

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). |

**Figure 5-124: AWI Client Attached Devices Page**

**Table 5-111: AWI Client: Attached Devices Page Information**

| Statistic | Description |
|---|---|
| Displays | This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the display attached to each port.<br>Note: This option is only available when the host is in a PCoIP session. |
| USB Devices | This section displays the port mode, model, status, device class, sub-class, protocol, vendor identification (VID), and product identification (PID) of the USB device attached to the client. |
| USB Device Status | Status options include:<br>● **Not Connected**: No device is connected.<br>● **Not in Session**: The device is detected outside of a PCoIP |

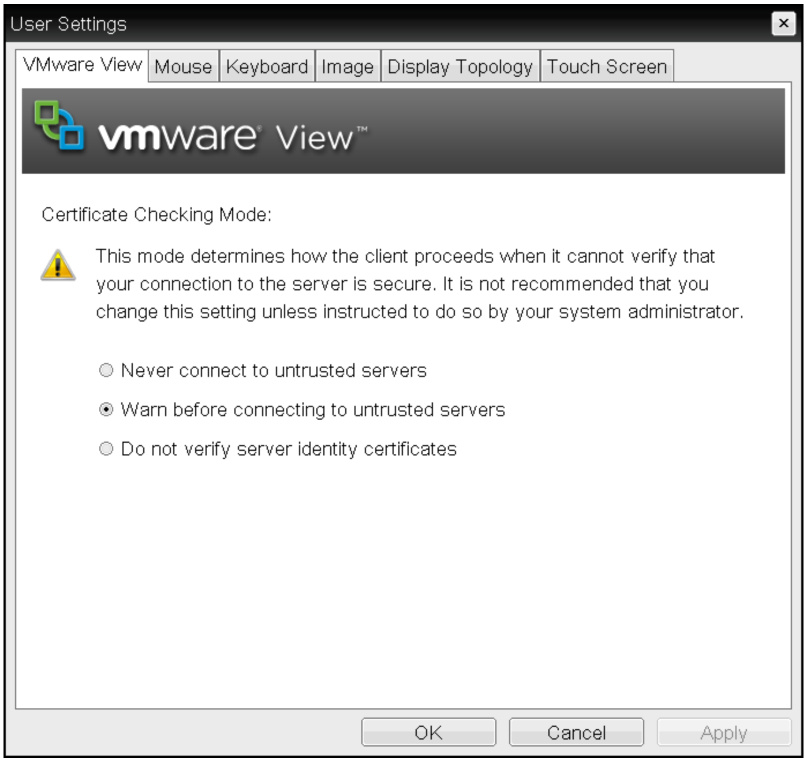
| Statistic | Description |
|---|---|
| | session.<br>- **Not Initialized**: The device is detected in a PCoIP session but the host controller has not initialized the device.<br>- **Failed Authorization**: The device is detected in a PCoIP session but is not authorized. (For more information about USB , see AWI Clientt: USB Permissions).<br>- **Locally Connected**: The device is detected and authorized but locally terminated in a PCoIP session (for example, a local cursor).<br>- **Connected**: The device is detected and authorized in a PCoIP session. |

# 5.30 Configuring User Settings (OSD)

## 5.30.1 OSD: VMware View Certificate Checking Settings

The **VMware View** 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 > VMware View** menu.

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



Certificate Checking Mode:

This mode determines how the client proceeds when it cannot verify that your connection to the server is secure. It is not recommended that you change this setting unless instructed to do so by your system administrator.

○ Never connect to untrusted servers

● Warn before connecting to untrusted servers

○ Do not verify server identity certificates

**Figure 5-125: OSD VMware View Page**

**Table 5-112: OSD VMware View Page Parameters**

| Parameter | Description |
|---|---|
| Never connect to untrusted servers | Configures the client to reject the connection if a trusted, valid certificate is not installed. |
| Warn before connecting to untrusted servers | Configures the client to display a warning if an unsigned or expired certificate is encountered, or when the certificate is not self-signed and the client trust store is empty. |
| Do not verify server identity certificates | Configures the client to allow all connections. |

## 5.30.2 MC: Help for VMware View Certificate Checking Settings

Certificate checking settings for the Management Console are located on the MC's View Connection Server pages.

## 5.30.3 AWI Client: Help for VMware View Certificate Checking Settings

Certificate checking settings for the AWI are located on the AWI client  View Connection Server pages.

## 5.30.4 OSD: Mouse Settings

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

You can also configure the mouse cursor speed through the PCoIP host software. For more information, see the "PCoIP Host Software User Guide (TER0810001)".

Note: The OSD mouse cursor speed setting does not affect the mouse cursor settings when a PCoIP session is active unless the **Local Keyboard Host Driver** function is being used (see the "PCoIP Host Software User Guide (TER0810001)" for more details). This function is only available through the OSD. It is not available in the AWI.

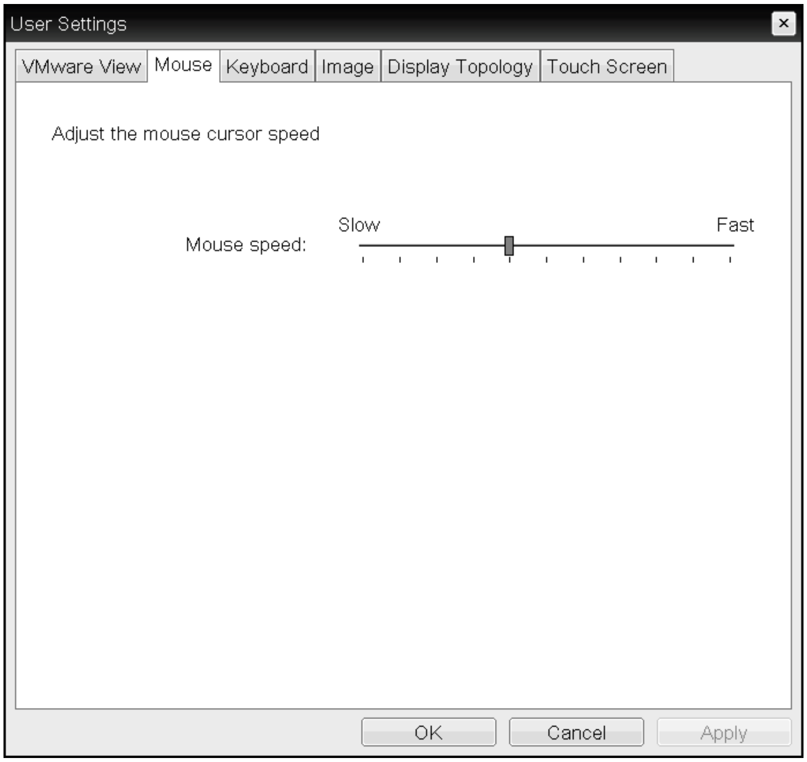


Figure 5-126: OSD Mouse Page

Table 5-113: OSD Mouse Page Parameters

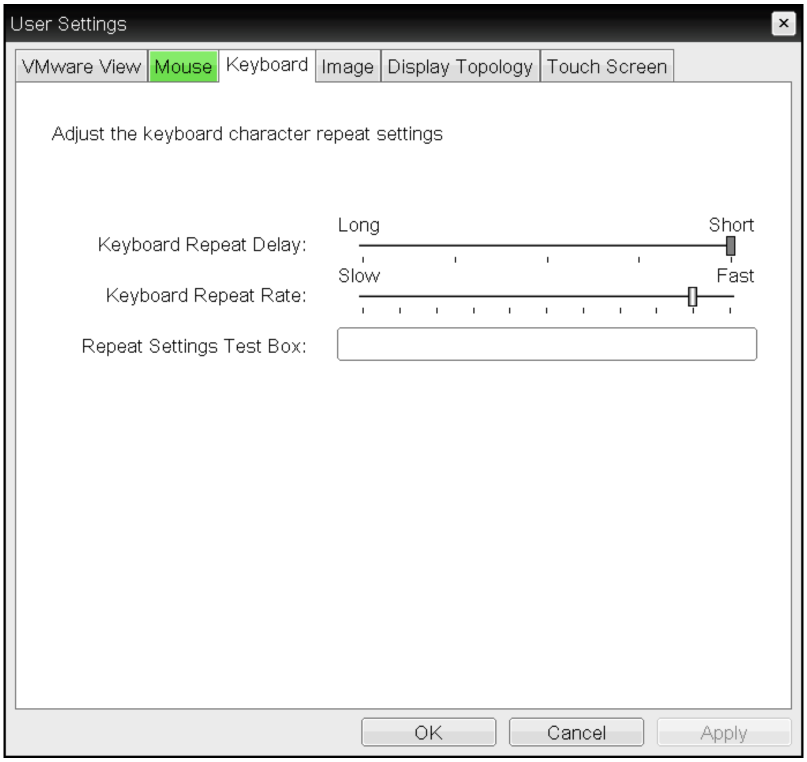
| Parameter | Description |
|---|---|
| Mouse Speed | Move the slider to configure the speed of the mouse cursor. |

## 5.30.5 OSD: Keyboard Settings

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

You can also configure the keyboard repeat settings through the PCoIP host software. For more information, see the "PCoIP Host Software User Guide (TER0810001)".

Note: The keyboard settings do not affect the keyboard settings when a PCoIP session is active unless the **Local Keyboard Host Driver** function is used (see the "PCoIP Host Software User Guide (TER0810001)" for more details). This function is only available through the OSD. It is not available in the AWI.



User Settings

Adjust the keyboard character repeat settings

Keyboard Repeat Delay:

Keyboard Repeat Rate:

Repeat Settings Test Box:

**Figure 5-127: OSD Keyboard Page**

**Table 5-114: OSD Keyboard Page Parameters**

| Parameter | Description |
|---|---|
| Keyboard Repeat Delay | Move the slider to configure the time that elapses before a character begins to repeat when it is held down. |
| Keyboard Repeat Rate | Move the slider to configure the speed at which a character repeats when it is held down. |
| Repeat Settings Test Box | Type in this box to test the chosen keyboard settings. |

### 5.30.6 OSD: Help for Image Settings

For information about the OSD's **Image** page, see OSD: Image Settings.

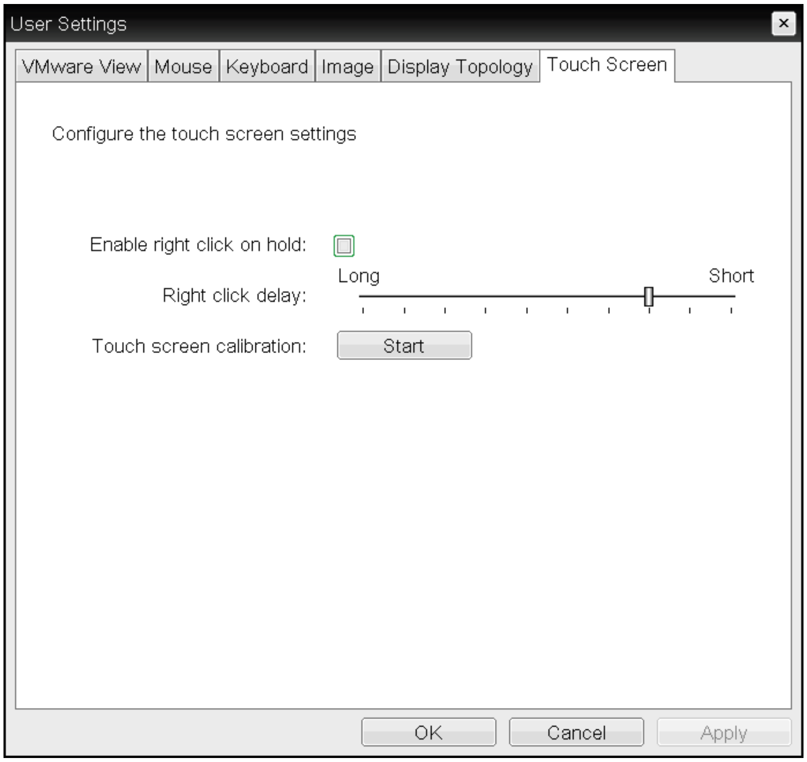
### 5.30.7 OSD: Help for Display Topology Settings

For information about the OSD's **Topology** page, see OSD: Tera1 Display Topology Settings or OSD: Tera2 Display Topology Settings.

## 5.30.8 OSD: Touch Screen Settings

The **Touch Screen** page lets you configure and calibrate settings for an attached Elo TouchSystems touch screen display. You can access this page from the **Options** > **User Settings** > **Touch Screen** menu.

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



Configure the touch screen settings

Enable right click on hold: □

Right click delay: Long — Short

Touch screen calibration: Start

**Figure 5-128: OSD Touch Screen Page**

**Table 5-115: OSD Touch Screen Page Parameters**

| Parameter | Description |
|---|---|
| Enable right click on hold | Select this checkbox to let users generate a right-click when they touch the screen and hold it for a few seconds. If disabled, right-clicking is not supported. |
| Right click delay | Slide the pointer to the position (between Long and Short) to determine how long the users must touch and hold the screen to generate a right-click. |
| Touch screen calibration | When you first connect the touch screen to the zero client, the calibration program starts. At the touch screen, touch each of the three targets as they appear.<br>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 |

| Parameter | Description |
|---|---|
| | automatically restarts. Once calibrated, the coordinates are stored in flash.<br>To manually start the calibration program, from the OSD **Touch Screen** page, click **Start**. Follow the onscreen prompts. |

### Installing the Touch Screen to the Zero Client

1. Plug in the touch screen's USB cable to the zero client's USB port.
2. Attach the monitor cable from the touch screen to the DVI 1 port on the zero client.

   Note: You can attach a non-touch screen monitor to the zero client in addition to the touch screen. (You cannot attach multiple touch screens to the zero client.) Because the touch screen must be attached to DVI1, the second non-touch screen monitor must be attached to DVI 2. If you only have the touch screen attached to the zero client, it can be attached to either DVI 1 or DVI 2.

3. Plug in the power.
4. Disconnect the zero client session. This initiates the calibration on the touch screen.

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

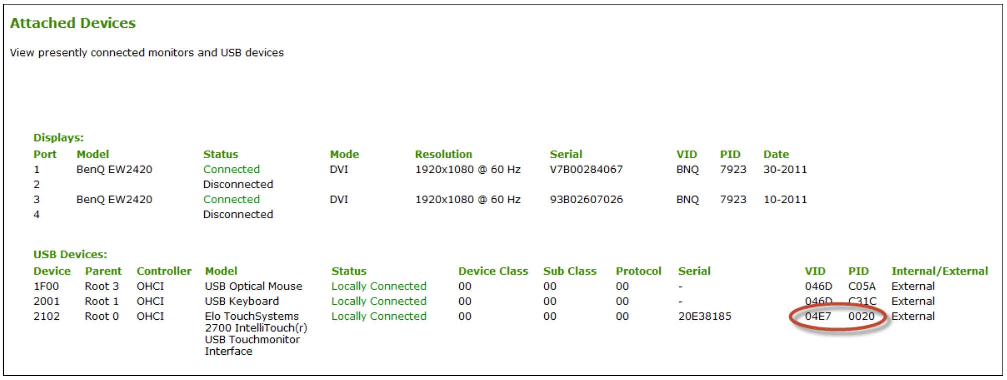
5. Follow the touch screen prompts. You can test the calibration with your finger (the cursor should move with your finger). If the screen is not properly calibrated, the system automatically restarts the calibration program.

### Setting up the Touch Screen as a Bridged Device

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

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

1. Follow the steps in the previous procedure to install the touch screen to your zero client.
2. Log into the Administrative Web Interface for the zero client.
3. From the **Info** menu, click **Attached Devices**.
4. The touch screen details should appear in this page. Write down the **PID** and the **VID** information.



**Attached Devices**

View presently connected monitors and USB devices

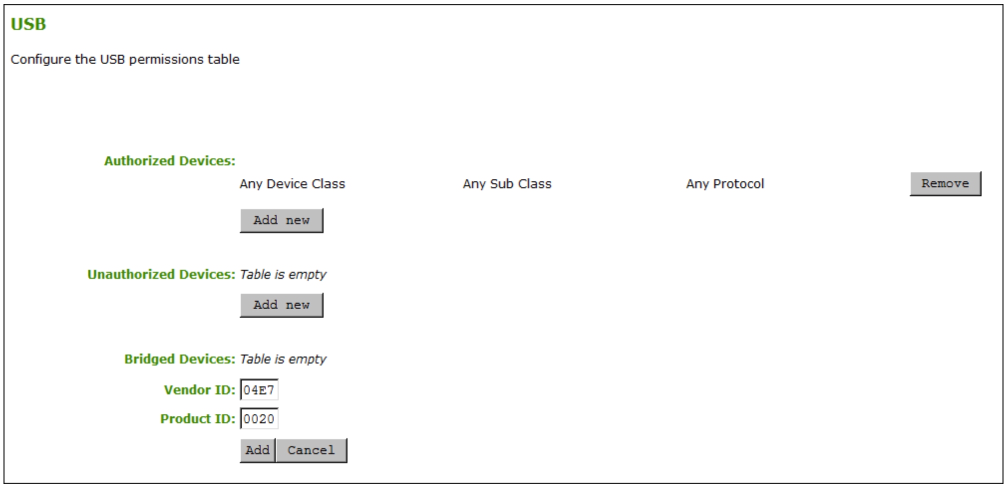
**Displays:**

| Port | Model | Status | Mode | Resolution | Serial | VID | PID | Date |
|---|---|---|---|---|---|---|---|---|
| 1 | BenQ EW2420 | Connected | DVI | 1920x1080 @ 60 Hz | V7B00284067 | BNQ | 7923 | 30-2011 |
| 2 | | Disconnected | | | | | | |
| 3 | BenQ EW2420 | Connected | DVI | 1920x1080 @ 60 Hz | 93B02607026 | 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 |

5. From the **Permissions** menu, click **USB** to display the **USB** page.
6. In the **Bridged Devices** area, click **Add New**.



**USB**

Configure the USB permissions table

**Authorized Devices:** Any Device Class Any Sub Class Any Protocol

**Unauthorized Devices:** *Table is empty*

**Bridged Devices:** *Table is empty*

**Vendor ID:** 04E7

**Product ID:** 0020

7. Enter the Vendor ID and Product ID for the touch screen, and then click **Apply**.
8. Restart the zero client session.
9. Install the touch screen driver from Elo TouchSystems. See the Elo TouchSystems documentation for installation and calibration instructions.

### Configuring the Zero Client to Automatically Log into a VMware View Host

To make logging into the touch screen device easier, you can choose to bypass the keyboard from the **VMware View Login** window. If you choose to set this up, the user needs to touch **Connect** at the **VMware View Login** window (otherwise, the user must enter the username and password, and then touch **Connect**).

1. Log into the Administrative Web Interface.
2. From the **Configuration** menu, select **Session**.
3. In the **Session Connection Type** drop-down menu, select **View Connection Server + Auto-Logon**.
4. Enter the VMware View Connection server's DNS name or IP address.
5. Fill out the user credentials, and then click **Apply**.

# 6 PCoIP Technology Reference

## 6.1 PCoIP Host Cards

PCoIP host cards are small add-in cards that can be integrated into tower PCs, rack mount PCs, PC blades, and server blades. The card's TERA-series processor performs advanced display compression algorithms to encode a user's full desktop environment. This information is then communicated in real time over an IP network to the user's PCoIP zero client.

For complete details about PCoIP host cards, see the Teradici website at http://www.teradici.com.

## 6.2 PCoIP Zero Clients

PCoIP zero clients are secure client endpoints that allow users to connect to a virtual desktop or remote host workstation over a local or wide area IP network. They can take many form factors, such as small stand-alone devices, PCoIP integrated displays, VoIP phones, and touch-screen monitors. Zero clients support multiple wide-screen formats, HD audio, and local USB peripherals. They also have extensive USB security and authentication features, including multiple-factor authentication for use with proximity cards and smart cards.

Powered by a single TERA-series processor, zero clients provide a rich multi-media experience for users, who can interact with their desktops from any type of zero client, and even continue the same session as they move between zero client devices.

For complete details about PCoIP zero clients, see the Teradici website at http://www.teradici.com.

## 6.3 DVI and DisplayPort Interfaces

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

- TERA2321 DVI-I dual-display PCoIP zero client: contains two DVI ports.
- TERA2321 DP+DVI-I dual-display PCoIP zero client: contains one DVI port and one DisplayPort port.
- TERA2140 DVI-D quad-display PCoIP zero client: contains four DVI ports.
- TERA2140 DP quad-display PCoIP zero client: contains four DisplayPort ports.

### 6.3.1 Support for 2560x1600 Display Resolution

All of the above zero clients also support 2560x1600 resolution for attached monitors with either DVI or DisplayPort interfaces. However, a custom dual-link DVI cable adapter is required to support this resolution for DVI interfaces.

The following figure illustrates how to connect video cables to each type of zero client to achieve 2560x1600 resolution on a connected display.

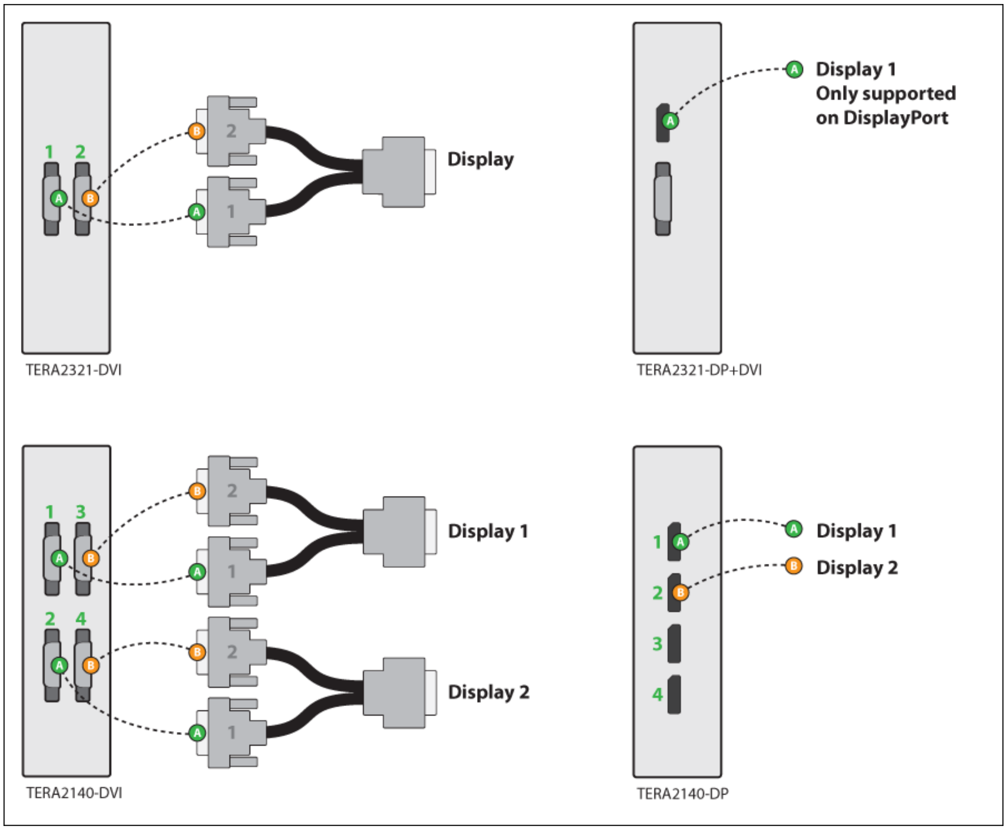


**Figure 6-1: DVI and DisplayPort Connectors for 2560x1600 Resolution**

- TERA2321 DVI-I dual-display PCoIP zero client: This zero client supports one 2560x1600 monitor. Connect the two DVI-I cable connectors on a custom dual-link DVI-I cable adapter to the two DVI-I ports on the zero client, as shown in the above illustration (upper left).
- TERA2321 DP+DVI-I dual-display PCoIP zero client: This zero client supports one 2560x1600 monitor on the DisplayPort interface only. Connect the connector on a DisplayPort cable to the DisplayPort port on the zero client, as shown in the above illustration (upper right).
- TERA2140 DVI-D quad-display PCoIP zero client: This client supports up to two 2560x1600 resolution monitors. For each monitor, connect the two DVI-D cable connectors on a custom dual-link DVI-D cable adapter to the two DVI-D ports that are shown in the above illustration (lower left). These connectors must be connected to ports on the client exactly as shown.
- TERA2140 DP quad-display PCoIP zero client: This zero client supports up to two 2560x1600 monitors. For each one, connect the connector on a DisplayPort cable to a DisplayPort port on the zero client, as shown in the above illustration (lower right).

Note: For details about other resolution options, see PCoIP Host Cards and Zero Clients.

## 6.4 PCoIP Connection Brokers

PCoIP connection brokers are resource managers that dynamically assign host PCs to zero clients based on the identity of the user establishing a connection from the zero client. Connection brokers are also used to allocate a pool of hosts to a group of zero clients. If the zero clients in a PCoIP deployment are configured to always connect to the same host (i.e., a static one-to-one pairing), then a connection broker is not required.

For connecting zero clients and host PCs, a number of 3rd party connection brokers support the PCoIP technology. For more information, see Knowledge Base support topic 15134-24 on the Teradici support site.

For VDI implementations, the VMware View connection broker is used to connect zero clients to VMware View virtual desktops. You can also use the VMware View connection broker to connect PCoIP clients and host PCs. For more information, see "Using PCoIP Host Cards with VMware View" (TER0911004).

## 6.5 APEX 2800 PCoIP Server Offload Card

The APEX 2800 PCoIP server offload 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 the APEX 2800 PCoIP server offload card, see the Teradici website at http://www.teradici.com.

# 7 Glossary of Acronyms

**256-bit Salsa20**
Salsa20 is a 256-bit stream cypher encryption algorithm.

**AC**
Alternating Current

**AES**
Advanced Encryption Standard

**AWI**
Administrator Web Interface. A PCoIP device used for monitoring and configuring PCoIP zero clients and host cards. To connect to the AWI, simply enter the PCoIP device IP address into a supported browser.

**BIOS**
Basic Input/Output System

**CA**
Certificate Authorities

**CAC**
Common Access Card. A smart card variant.

**CAD**
Computer Aided Design

**CMI**
Connection Management Interface. An interface provided by the host or client that is used to communicate with an external connection management server.

**CMS**
Connection Management Server. An external third-party management entity capable of managing hosts and clients. Also known as a connection broker.

**DA**
Directory Agent

**DDC**
Display Data Channel

**DDC/CI**
Display Data Channel/Command Interface

**DHCP**
Dynamic Host Configuration Protocol

**DMS-59**
A 59-pin connector used on computer video cards that is capable of combining two DVI streams into one connector.

**DNS**
Domain Name System

**DNS-SRV**
Domain Name System Service Record

**DVI**
Digital Visual Interface

**EDID**
Extended Display Identification Data

**EEPROM**

Electrically Erasable Programmable Read-Only Memory

**ESP**

Encapsulating Security Payload

**Fps**

Frames per second. The display data frame update rate.

**FQDN**

Fully Qualified Domain Name

**GPIO**

General Purpose Input/Output

**GPO**

Group Policy Object

**GPU**

Graphics Processing Unit

**GUI**

Graphical User Interface

**HD**

High Definition

**HDCP**

High-bandwidth Digital Content Protection

**HID**

Human Interface Device

**HomePlug**

A networking technology through power lines.

**HPDET**

Hot Plug Detect

**HTML**

Hyper Text Markup Language

**ID**

Identification

**IP**

Internet Protocol

**IPsec**

Internet Protocol Security

**IPsec-ESP**

Internet Protocol Security-Encapsulated Security Payload

**IPv4**

Internet Protocol Version 4. The dominant network-layer protocol on the Internet.

**IPv6**

Internet Protocol Version 6. The successor to IPv4.

**LAN**

Local Area Network

**LED**

Light-Emitting Diode

**MAC**

Media Access Control. A unique hardware identifier.

**Mbps**

Megabits per second

**MC**

Management Console

### MIB

Management Information Base. Used by SNMP.

### MTU

Maximum Transmission Unit

### NAT

Network Address Translation

### NTP

Network Time Protocol

### OHCI

Open Host Controller Interface

### OS

Operating System

### OSD

On Screen Display. The interface presented by a zero client. The OSD displays connection dialogs as well as local configuration options that are accessible to both users and administrators. If desired, administrators can lock down or hide the configuration options from users.

### PC

Personal Computer

### PCI

Peripheral Component Interconnect

### PCLe

Peripheral Component Interconnect Express

### PCoIP

Personal Computer over Internet Protocol

### PCoIP Host

The host side of a PCoIP system.

### PCoIP Zero Client

The client (portal) side of a PCoIP system. Also known as a PCoIP portal.

### PC-over-IP

Personal Computer over Internet Protocol

### POST

Power On Self Test

### RDP

Remote Desktop Protocol

### RFC

Request for Comments. Internet standards documents.

### SA

Service Agent

### SLAAC

Stateless Address Auto-Configuration

### SLP

Service Location Protocol

### SNMP

Simple Network Management Protocol

### SSL

Secure Socket Layer. A security protocol.

**TERA1100**

A first-generation Teradici processor supporting PCoIP zero client functionality.

**TERA1200**

A first-generation Teradici processor supporting PCoIP host functionality.

**TERA2140**

A second-generation Teradici processor supporting PCoIP zero client functionality.

**TERA2220**

A second-generation Teradici processor supporting PCoIP host functionality.

**TERA2240**

A second-generation Teradici processor supporting PCoIP host functionality.

**TERA2321**

A second-generation Teradici processor supporting PCoIP zero client functionality.

**UA**

User Agent

**UDP**

User Datagram Protocol

**UI**

User Interface

**USB**

Universal Serial Bus

**VDI**

Virtual Desktop Infrastructure

**VGA**

Video Graphics Array

**VM**

Virtual Machine

**VPD**

Vital Product Data. Factory provisioned information to uniquely identify a host or client.

**VPD (alternate)**

Virtual Desktop Platform

**VPN**

Virtual Private Network

**WAN**

Wide Area Network. An extended corporate continental network.

**WI-FI**

A trade name for IEEE 802.11 wireless technologies.

**WOL**

Wake-on-LAN

**WOU**

Wake-on-USB

# 8 Index