PCoIP Administrator's Guide

TER0606004

Issue 14

PCoIP CONNECTED

TERADICI

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.

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

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Teradici Corporation. All rights reserved.

Teradici, PC-over-IP, and PCoIP are registered trademarks of Teradici Corporation.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision History

Version	Date	Description
14	September 16, 2011	Updated for Firmware Release 3.4.1 • Support for .Net cards

13	June 8, 2011	Updated for Firmware Release 3.4.0
		• New banner at the top of the Administrative Web Interface page
		• RDP is no longer supported
		• Diagnostic enhancements:
		  ○ Syslog support
		  ○ Additional log reporting for specific categories of messages (such as Audio, USB, video)
		• **Reset Host CPU** button from **Host CPU** page removed
		• New OSD page in the **User Settings** window called **Touch Screen**. Lets users configure and calibrate Elo TouchSystems touch screen displays with IntelliTouch surface acoustic wave and AccuTouch five-wire resistive touch screen technologies.

12	April 18, 2011	Updated for Firmware Release 3.3.1.
11	February 2011	• Updated for Firmware Release 3.3. • Incorporated information from Administrative notes (which documented features for Firmware Release 3.2.0).
10	Apr 06, 2010	• Updated for Firmware Release 3.1.0. • Updated On Screen Display (OSD) section with appropriate references to the Administrative Web Interface section. • Updated Appendix B: Client Language and Keyboard Support to include Belgian, Danish, Finnish, Norwegian, Polish, Swedish and Turkish keyboards.
9	Dec 08, 2009	• Updated for Firmware Release 3.0 • Simplified to endpoint terms “client” and “host card” • Updated description for Home webpage • Added description for Enable AES-128-GCM and Enable SALSA20-256-Round12 • Updated description to use kbps for Bandwidth • Updated description for OSD configuration • Updated description for USB permission • Updated description for Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode for Windows 7 64-bit • Updated Session Statistics description for improved session stats • Added USB Over Current Notice Overlay description • Updated Appendix B: Client Language and Keyboard Support to include the Korean dubeolsik keyboard
8	Oct 22, 2009	• Updated for Firmware Release 2.3 • Added notes about Host and Portal webpage banners • Added description for SNMP enable feature
7	Jun 15, 2009	• Updated for Firmware Release 2.2

Version	Date	Description
		• Added description for enable display override • Clarified Network Connection Lost overlay description (2 seconds of network inactivity)
6	May 14, 2009	• Updated for Firmware Release 2.1 • Modified to note some PCoIP devices have password webpage and password protection disabled by default • Updated to note some webpages are only available for Host or Portal • Added Domain Name and FQDN parameter details • Added description for Label webpage • Added description for VMware View webpage • Updated description (Device Bandwidth Floor) for Bandwidth webpage • Updated figure for Image webpage • Added description for Host Driver Function webpage • Updated description (removed Enable Audio Compression) for Audio webpage
5	Nov 25, 2008	• Improved document wording and fixed errors • Updated for Firmware Release 1.8 • Adjusted formatting; replaced bitmap graphics w/ GIFs to reduce file size
4	Sep 12, 2008	• Updated for Firmware Release 1.4 • Added menu navigation overview (Figure 1 2: Administrative Web Interface Overview) • Added Initial Setup/Home webpage information • Added Initial Setup webpage details • Updated Enable Auto-Reconnect detail • Updated Ethernet Mode for Host • Added Enable Vista64 Mode • Added Half-Duplex Overlay • Added Video Source Overlays)
3	May 26, 2008	• Updated for Firmware Release 1.00 • Updated text and figure references to Portal • Added warning to Ethernet Mode section concerning PC-over-IP Half-Duplex in compatibility • Clarified when Device Bandwidth Limit and Device Bandwidth Target are applied • Updated USB Permissions documentation for USB authorization/unauthorization functionality • Added USB devices status descriptions in Table 1 13: VPD Information • Attached Devices - USB Devices
2	April 7, 2008	• Augmented definitions (see Definitions Section) • Updated for Firmware Release 0.19 • Updated PCoIP Processor Information description • Removed VLAN place holder from Network Configuration Webpage • Added Maximum MTU Size in Network web configuration

Version	Date	Description
		• Added DNS SRV in Discovery web configuration • Updated Session web configuration ordering • Added Device Bandwidth Target to Bandwidth web configuration • Updated RDP web configuration • Added Maximum Initial Image Quality to Image web configuration • Added Time web configuration • Added Firmware Part Number in Version web information • Updated Firmware Upload build filename web information • Updated RDP OSD configuration • Added Firmware Part Number in Version OSD information • Clarified Bandwidth and Image Configuration Example • Removed TERA1x00 Firmware Defaults appendix to enhance in separate Application Note • Updated for Firmware Release 0.20 • Added Bandwidth Statistics • Updated RDP compatibility information
1	January 15, 2008	Initial release

Contents

Table of Figures

Table of Tables

.

Definitions

Definition	Description
CA	Certificate Authorities
CMI	Connection Management Interface – interface provided by the host or client, used to communicate with an external connection management server
CMS	Connection Management Server – an external management entity (third party) that manages and controls the host/client through the CMI interface
DDC	Display Data Channel
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS SRV	Domain Name System Service Record
EDID	Extended Display Identification Data
FQDN	Fully Qualified Domain Name
GPU	Graphics Processing Unit
GUI	Graphical User Interface presented by the client On Screen Display when not operating in a PC-over-IP session
HPDET	Hot Plug Detect MC PC-over-IP Management Console (PCoIP MC)
MIB	Management Information Base
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OS	Operating System
OSD	On Screen Display
PC-over-IP®	Personal Computer over Internet Protocol
PCoIP®	Personal Computer over Internet Protocol (PC-over-IP)
PCoIP Zero Client	Desktop side of PC-over-IP system (that is, client). For example, PCoIP Portal or PCoIP Integrated Display)
PCoIP Host	Host side of PC-over-IP system
RDP	Remote Desktop Protocol Note: RDP is not supported in firmware releases after 3.2.2
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer (security protocol)
TERA1100	Teradici device supporting PC-over-IP client functionality
TERA1200	Teradici device supporting PC-over-IP host functionality
VPD	Vital Product Data – Factory provisioned information to uniquely identify a host or client
VPN	Virtual Private Network
zero client	See PCoIP zero client

1 Introduction

As a user or administrator you can interact with your PCoIP® zero clients and host cards (or "clients" and "hosts") through the embedded HTTPS web interface (i.e., Administrative Web Interface) and On Screen Display (OSD). To minimize the total learning curve and maximize the accessibility, the web interface and OSD are organized as similarly as possible and are structured in a task-oriented fashion.

- **Administrative Web Interface**: Lets you configure the hosts and clients through an Internet Web browser.
- **OSD**: Lets you configure the client through the graphical user interface (GUI). Messages appear overlaid on the user display as required. The OSD has a subset of parameters available in the Administrative Web Interface.

Note: This guide describes the interface for PCoIP protocol devices such as PCoIP zero clients and PCoIP host cards. This document does not describe the Administrative Web Interface for PCoIP software integrated into products such as VMware View.

The configuration features are also available through some connection brokers and the PCoIP Management Console (web-based tool used to manage multiple PCoIP endpoints). These features are not described in this guide. For more information on the PCoIP Management Console, see the *PCoIP Management Console User Manual* (TER0812002).

1.1 About this Document

This document is divided into the following sections:

Title	Description	Section
Introduction	This section describes the document structure and introduces you to the Administrative Web Interface and OSD.	1
Administrative Overview	This section describes the Administrative Overview, login details and its onscreen menus.	2
On Screen Display (OSD) Overview	This section describes the OSD, how to log in, and its screen options.	3
Configuring the Device	This section describes the options available from the **Configuration** menu. It covers how to configure the device.	4
Setting up User Permissions	This section describes how to configure the options from the **Permissions** menu (such as configuring the USB devices, audio settings, and power-off permissions).	5
Using the Diagnostic Tools	This section describes how to use the options available from the **Diagnostic** menu. These options help you troubleshoot the device by letting you view device statistics, generate test tones and patterns, reset the device, ping the device, and so on.	6

Title	Description	Section
Viewing Device Information	This section describes the options available in the **Information** menu. These options let you see which firmware version is currently installed on the device and view the attached devices.	7
Uploading to the Device	This section describes the options available in the **Upload** menu. It describes the steps to upload firmware to the device and steps to upload a logo that will appear on the **OSD Connect** page.	8
Configuring the User Settings	This section describes the options available from the **User Settings** menu in the OSD. These options include changing the mouse cursor speed settings, changing the keyboard repeat settings, changing the image settings, and configuring the display topology.	5
About the Overlay Pages	This section describes the overlay messages that can appear during a PCoIP session.	10
Using CAC Smart Cards with PCoIP Zero Clients	This section describes which CAC Smart Cards are supported and the steps you must take to connect the CAC Smart Card to the device.	11
Usage Examples	This section let you see examples of doing things like setting up a peer-to-peer direct connection, configuring the device for DHCP and enabling host discovery. It also has different scenarios for configuring your bandwidth and imaging.	Appendix A
Client Language and Keyboard Support	This section lists the language and keyboards supported by the PCoIP client.	Appendix B

1.2 Menu and Page Overview

The Administrative Web Interface and OSD have various menus and pages. The following table lists the pages according to their menus and if they are available in the Administrative Web Interface, OSD, or both.

Note: Many of the pages available from the OSD include a subset of parameters that are available in the Administrative Web Interface.

Table 1-1: Configuration Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
Initial Setup	AWI	Both	4.1
Network	Both	Both	4.2
Label	Both	Both	4.3
Connection Management	Both	Both	4.10
VMware View	Both	Client	4.5
VMware View Advanced Note: In the OSD, this page is available from the **VMware View** page	Both	Client	4.6
VMware View Kiosk Mode Note: In the OSD, this page is available from the **VMware View** page	Both	Client	4.7
Discovery	Both	Both	4.8
SNMP	AWI	Both	4.9
Session	Both	Both	4.10
Bandwidth	AWI	Both	4.11
Language	Both	Client	4.12
OSD	Both	Client	4.21
Image Note: In the OSD, this page is available from the **User Settings** menu	AWI	Client	4.14
Monitor Emulation	AWI	Host	4.15
Host Driver Function	AWI	Host	4.16
Time	AWI	Both	4.17
Password	AWI	Both	4.18
Reset Parameters	Both	Both	4.19
Display	OSD	Client	4.20

Table 1-2: Permissions Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
USB	AWI	Both	5.1
Audio	AWI	Both	5.2
Power	AWI	Client	5.3

Table 1-3: Diagnostics Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
Event Log	Both	Both	6.1
Session Control	AWI	Both	6.2
Session Statistics	Both	Both	6.3
Host CPU	AWI	Host	6.4
Audio	AWI	Client	6.5
Display	AWI	Client	6.6
PCoIP Processor	Both	Both	6.7
Ping	OSD	Client	6.8

Table 1-4: Info Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
Version	Both	Both	7.1
Attached Devices	AWI	Both	7.2

Table 1-5: Upload Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
Firmware	AWI	Both	8.1
OSD Logo	AWI	Client	8.2

Table 1-6: User Settings Menu

Page Name	Administrative Web Interface (AWI), OSD, or Both	Client, Host, or Both	Section
Mouse	OSD	Client	9.1
Keyboard	OSD	Client	9.2
Image	OSD	Client	4.14
Display Topology	OSD	Client	9.4

2 Administrative Web Interface Overview

The PCoIP Administrative Web Interface lets you interact remotely with the device through an Internet browser. The host and client webpages have unique banners to easily identify each.

2.1 About the Page Layout

The following screenshot shows an example of an Administrative Web Interface page from a host. It has are seven basic regions:

Log Out: Log out of the Administrative Web Interface.

PCoIP endpoint: Displays PCoIP endpoint information.

- PCoIP® host card
- PCoIP® zero client

Home button: Click to navigate to the **Home** page.

Drop-down menus: The toolbar at the top part of the page lets you easily find pages through its menus: Configuration, Permissions, Diagnostics, Info, and Upload.

Webpage information: Displays the title and summary of the current page.

Data field: A configurable or read-only parameter (inline help appears when appropriate).

Apply/Cancel buttons: Each page that includes editable parameters has two buttons:

- **Apply:** Store the edited parameters in flash.
- **Cancel:** Reset the edited parameters to the values currently stored in flash.

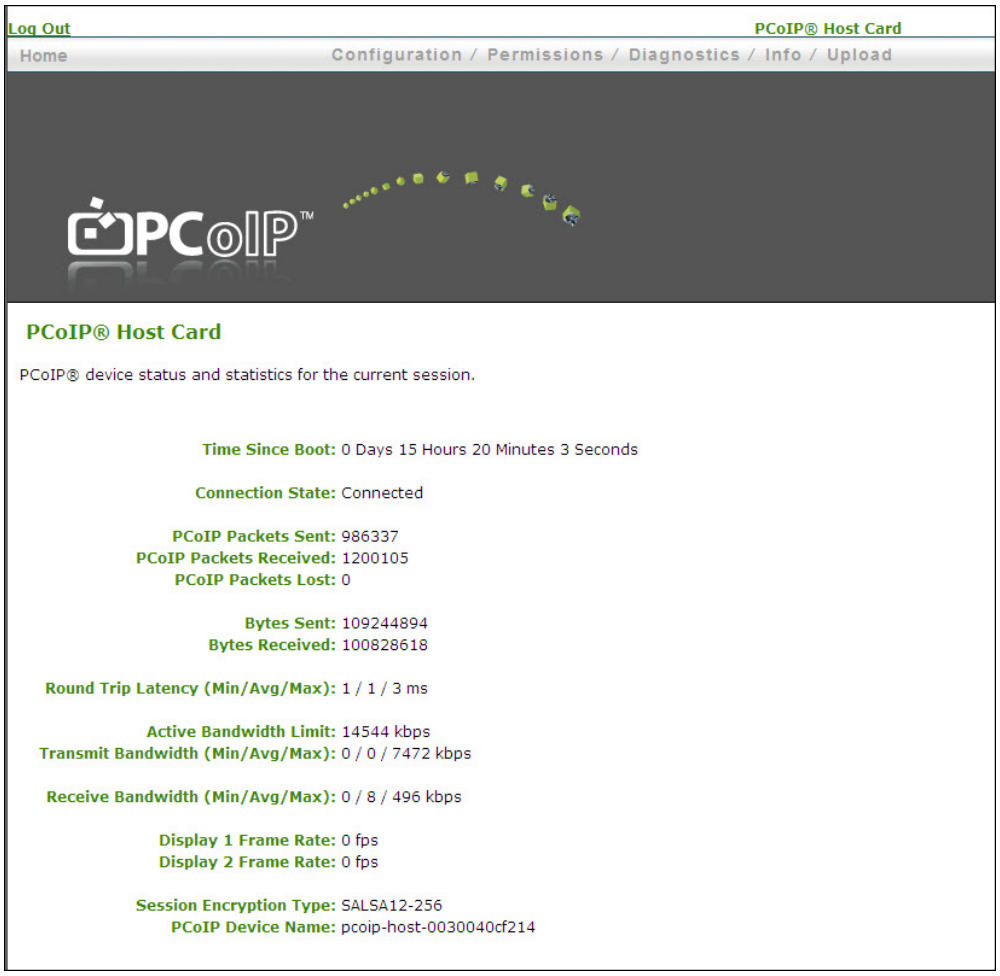


Figure 2-1: Administrative Web Interface Home Page (Host)

2.2 Supported Web Browsers

The webpage servers on the host and client were tested and are compatible with the following web browsers:

- Firefox 1.5, 2.0, 3.0, 3.5, 3.6
- Internet Explorer 6.0, 7.0, 8.0

Note: Other browsers may also be compatible.

We strongly recommend you install the CA root certificate in your browser to avoid warning messages from appearing when you log into the Administrative Web Interface. See sections 2.4.1 and 2.4.2 for details.

2.3 Administrative Web Interface IP Address

To access the Administrative Web Interface:

1. Browse to the IP address of the host or client. The IP address used depends 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. Enter the IP address into the browser. (For example, https://192.168.1.123)

Note: Some networks using DHCP may be able to access the Administrative Web Interface using the PCoIP device name. For more information about configuring the IP address details, see section 4.2.

2.4 Administrative Interface Security

The Administrative Web Interface uses HTTP over an SSL socket (HTTPS). You cannot access it without an administrative password. The HTTPS connection is secured using a Teradici self-signed certificate.

Note: Some PCoIP devices have password protection disabled and do not require a password to login. You can enable or disable the password protection through the PCoIP Management Console.

.

2.4.1 Installing the CA Root Certificate for Firefox

You can install a Certificate Authorities (CA) root certificate in the Internet browser to avoid the browser security warnings.

1. From the **Tools** menu, select **Internet Options**.
2. From the **Content** tab, select **Certificates**.
3. From the **Trusted Root Certification Authorities** tab, select **Import**.
4. Follow the onscreen directions to import the certificate. The certificate file is part of the firmware release. The file is called "cacert.pem". Ensure you use the Trusted Root Certification Authorities certificate store.

Note: You can also download the cacert.pem file directly from the Teradici support site.

2.4.2 Installing the CA Root Certificate for Internet Explorer

You can install a Certificate Authorities (CA) root certificate in the Internet browser to avoid the browser security warnings.

Note: The following steps are specific to Internet Explorer version 7 and might vary slightly for previous or future versions.

1. From the **Tools** menu, select **Options**.
2. Select the **Advanced** icon at the top of the page.
3. From the **Encryption** tab, select **View Certificates**.
4. From the **Authorities** tab, select **Import**.
5. Follow the onscreen directions to import the certificate. The certificate file is part of the firmware release. The file is called "cacert.pem". Check the option labeled **Trust this CA** to identify web sites.

Note: You can also download the cacert.pem file from the Teradici support site.

2.5 Logging In

To log into the Administrative Web Interface:

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

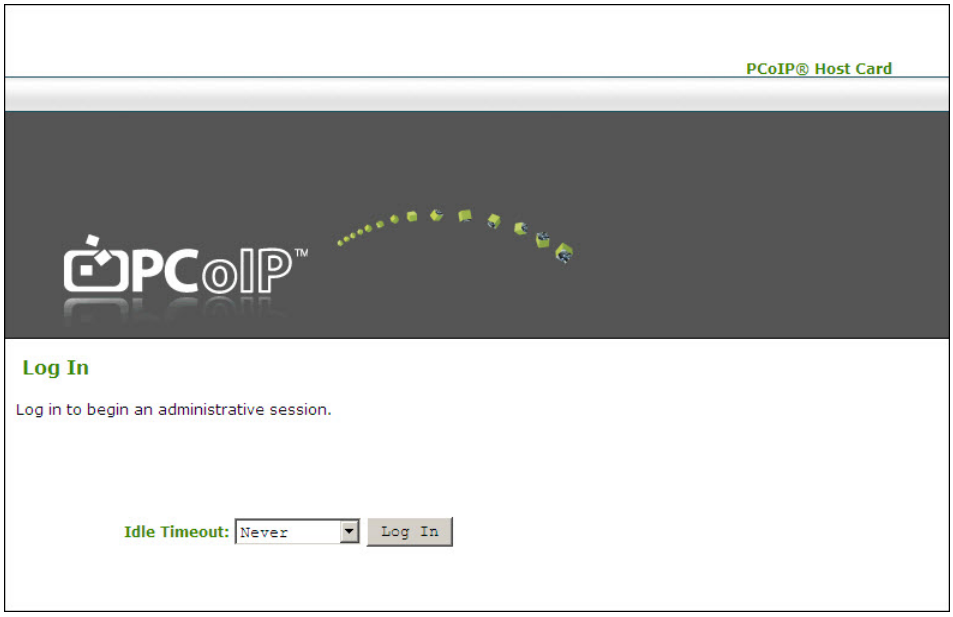


Figure 2-2: Administrative Web Interface Log In Page (Host)

2. To change the time after which the device is automatically logged off, set the **Idle Timeout** field to:
   - 1 minute
   - 5 minutes
   - 15 minutes
   - 30 minutes
   - Never
3. Click **Log In**. When you first login to a device, the **Home Page** appears. It provides an overview of the device status. If configured in the firmware defaults, the **Initial Setup** page optionally appears the first time you log in.

Note: Some PCoIP devices have password protection disabled by default. You do not need a password to login. You can enable or disable password protection for the **Log In** page using the PCoIP Management Console. For details, see the *PCoIP Management Console User Manual* (TER0812002).

If a warning message appears when you try to log in, a session is already in progress on that device. Only one administrator can log into a device at one time. Logging into a session already in progress terminates that session

2.6 Viewing the Home Page

The **Home** page displays a summary of the host or client. The first time you log into the Administrative Web Interface, the **Initial Setup** page appears. The **Home** page appears for each subsequent session. To display the **Home** page, click the **Home** link at the top left section of the menu bar.

Note: When you click the **Reset Statistics** button, the statistics reported in the **Home** page are also reset. For details about resetting the statistics, see section 6.3.

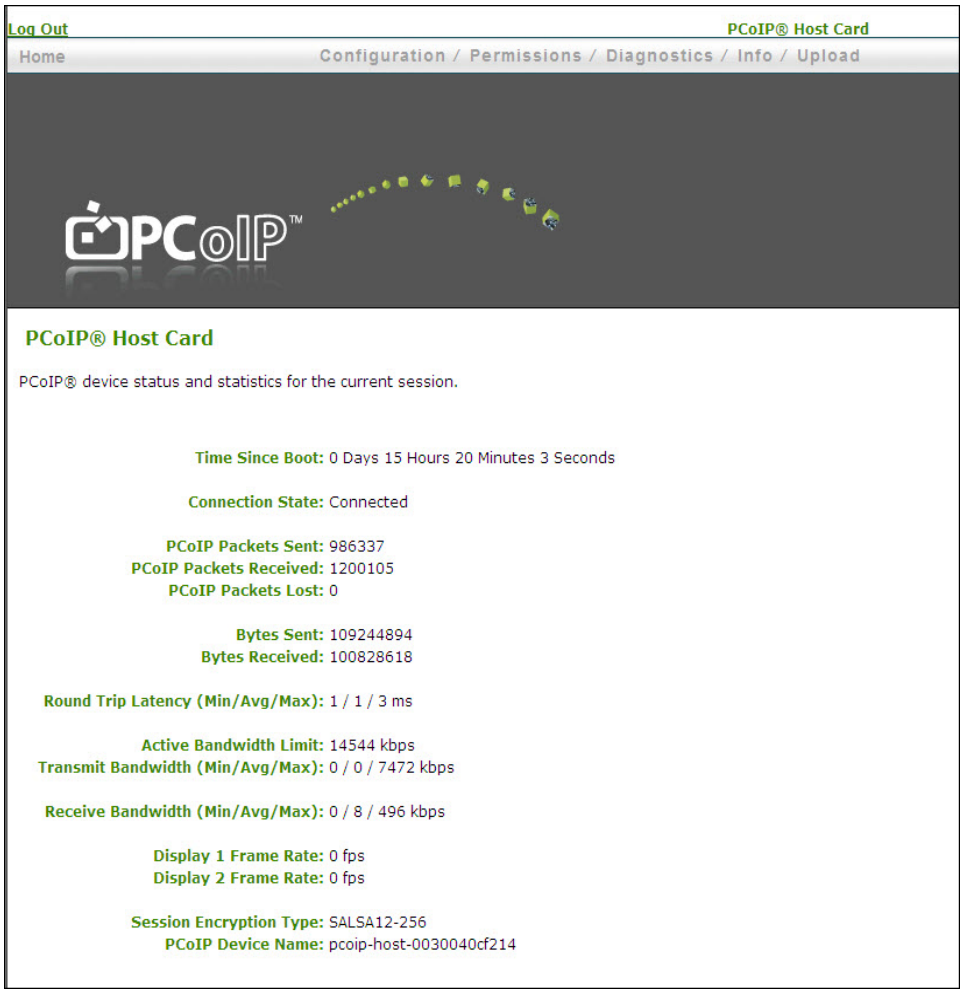


Figure 2-3: Administrative Web Interface Home Page (Host Card)

Table 2-1: Home Page Statistics

Statistics	Description	For Further Details
Time Since Boot	Length of time that the PCoIP processor has been running.	See section 6.3
Connection State	Possible states: Disconnected, Connection Pending, Connected.	See section 6.3
PCoIP Packets	• Packets Sent • Packets Received • Packets Lost	See section 6.3
Byte Statistics	• Bytes Sent • Bytes Received	See section 6.3
Round Trip Latency	Approximate network min, average, and max round trip latency (e.g., client to host and back to client).	See section 6.3
Bandwidth Statistics:	• Active Bandwidth Limit is the transmit bandwidth PCoIP processors may generate. • Transmit Bandwidth is the min, average and max traffic transmitted. • Receive Bandwidth is the min, average, and max traffic received.	See section 6.3
Display Frame Rates	This field is the name the host or client registers with the DNS server if: • DHCP is enabled • the system is configured to support registering the hostname with the DNS server • Display rate for video content through PCoIP protocol. For example, if nothing is currently changing, Frame Rate is 0 fps.	See section 4.3
Session Encryption Type	The type of encryption configured for the device. Options include AES-128-GCM and SALSA20-256-Round 12.	See section 4.10
PCoIP Device Name	The logical name for the device. This field is the name the host or client registers with the DNS server if: • DHCP is enabled • the system is configured to support registering the hostname with the DNS server	See section 4.3

2.7 About the Administrative Interface Menus

The Administrative Web Interface has five menus that link to the various configuration and status pages.

Configuration: The pages off this menu let you configure the various aspects for the device, such as network settings, language, session parameters, and so on. See section 4.

Permissions: The pages off this menu let you set up the client permissions for the USB, audio, and power. See section 5.

Diagnostics: The pages off this menu help you troubleshoot the device. See section 6.

Info: The pages off this menu let you view firmware information and the devices currently attached to the device. See section 7.

Upload: The pages off this menu let you upload a new firmware version as well as an OSD logo to the device. See section 8.

The following figure shows the menus and pages available in the Administrative Web Interface.

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).

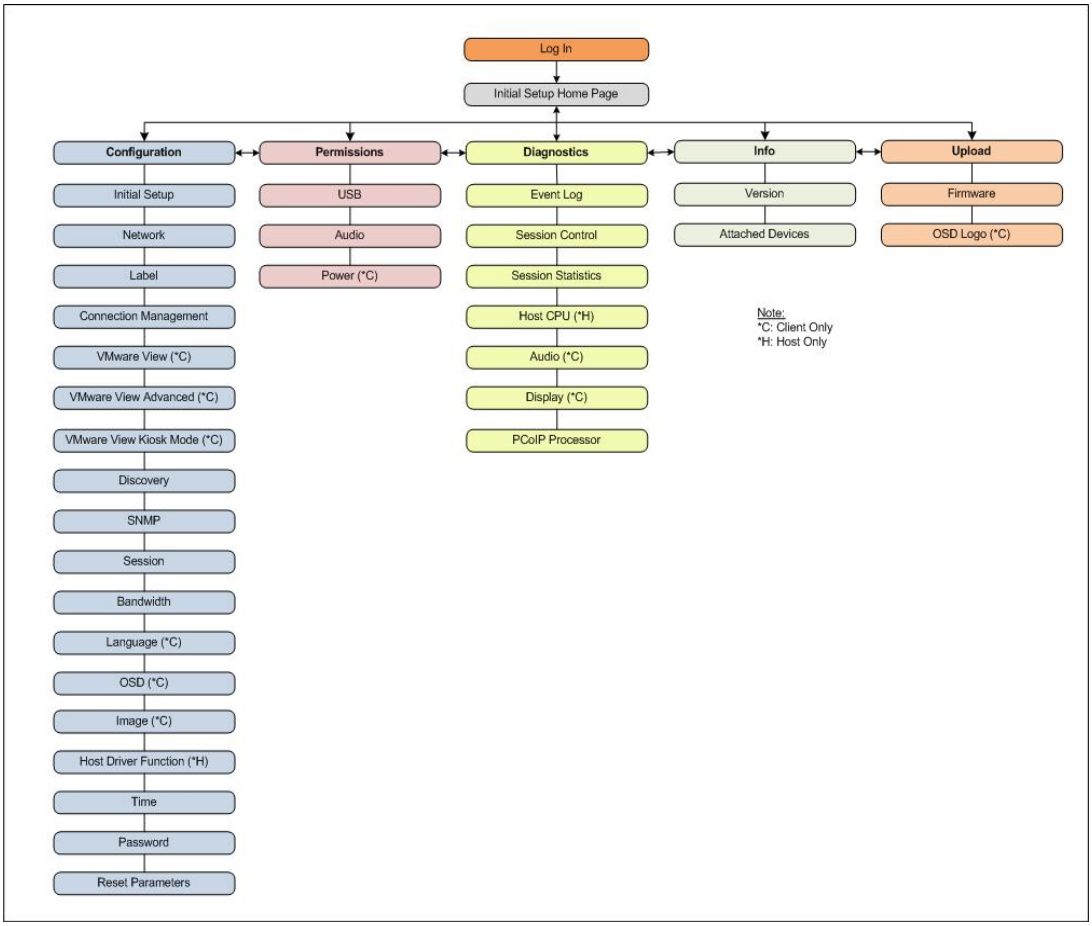


Figure 2-4: Administrative Web Interface Menu Overview

2.7.1 Viewing the Configuration Menu

The **Configuration** menu contains links to pages that define how the device operates and interacts with its environment.

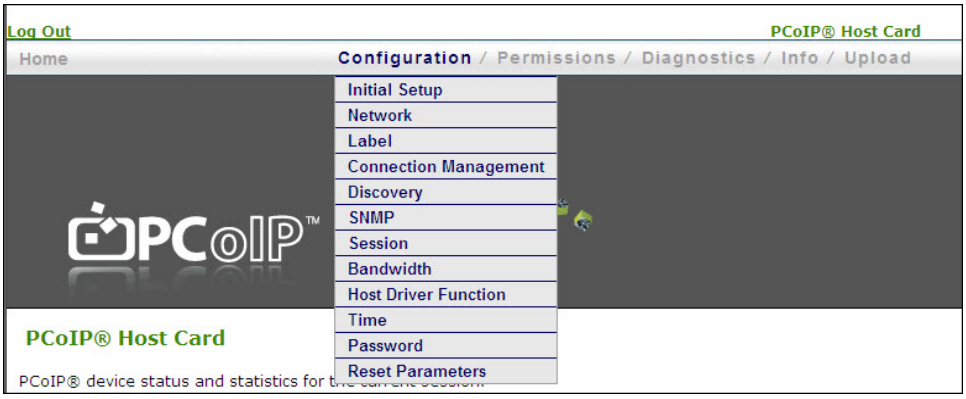


Figure 2-5: Administrative Web Interface Configuration Menu (Host)

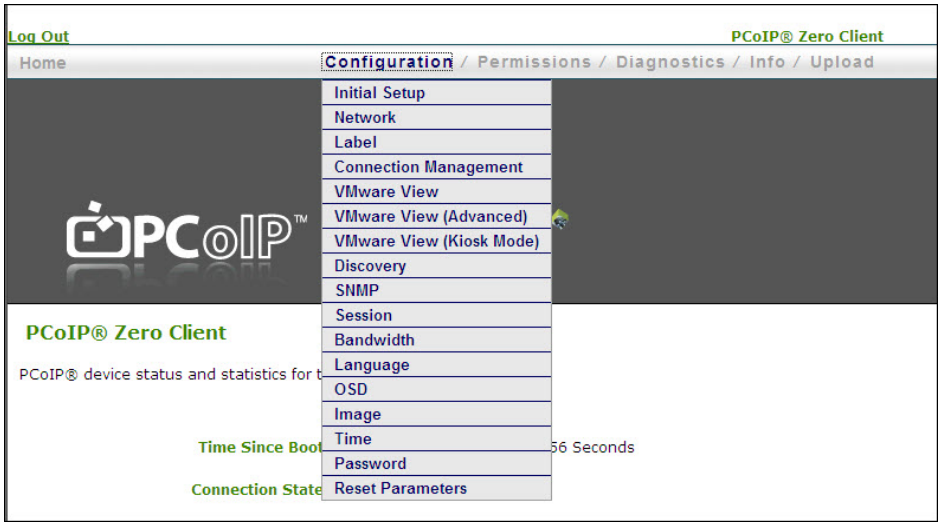


Figure 2-6: Administrative Web Interface Configuration Menu (Client)

For more information about the Configuration options, see section 4.

2.7.2 Viewing the Permissions Menu

The **Permissions** menu contains links to pages that define the range of functionality exposed to the user.

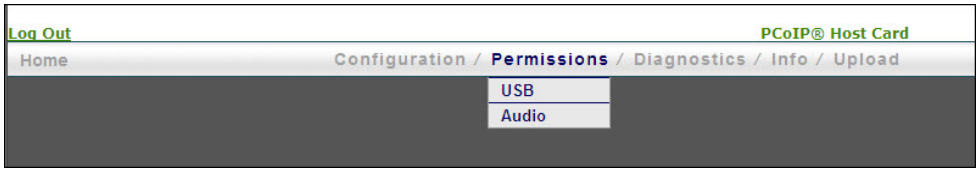


Figure 2-7: Administrative Web Interface Permissions Menu (Host)

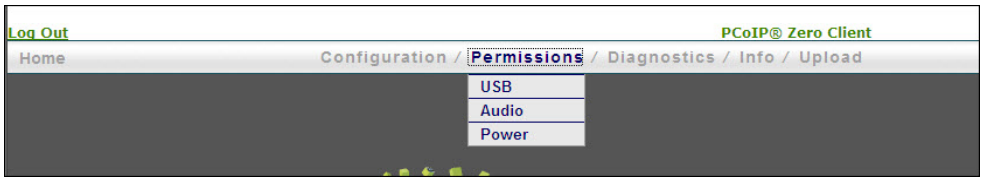


Figure 2-8: Administrative Web Interface Permissions Menu (Client)

For details on each of the Permissions options, see section 6.3.

2.7.3 About the Diagnostics Menu

The **Diagnostics** menu contains links to pages with run-time information and functions that may be useful for troubleshooting.

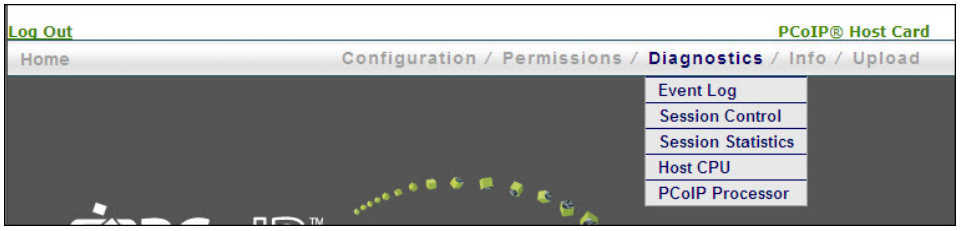


Figure 2-9: Administrative Web Interface Diagnostics Menu (Host)

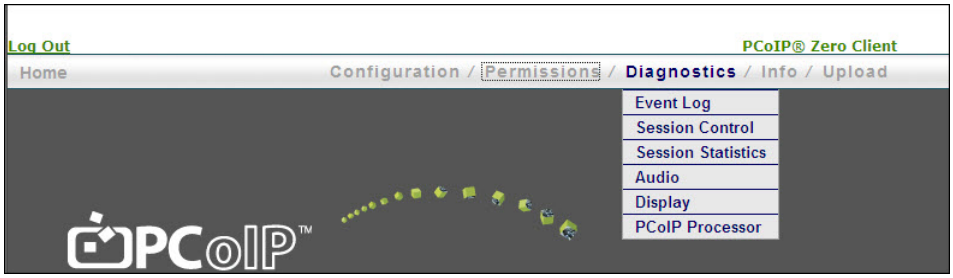


Figure 2-10: Administrative Web Interface Diagnostics Menu (Client)

For details on each of the Diagnostic options, see section 6.

2.7.4 About the Information Menu

The **Info** menu has links to pages that show information about the device.

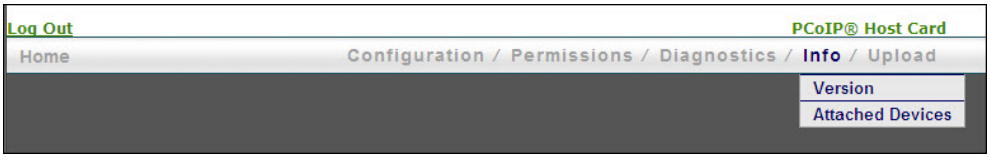


Figure 2-11: Administrative Web Interface Information Menu (Host)

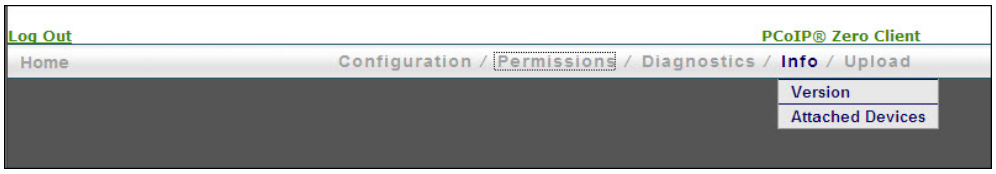


Figure 2-12: Administrative Web Interface Information Menu (Client)

For details on each of the Information options, see section 7.

2.7.5 About the Upload Menu

The **Upload** menu contains links to pages that you can use to upload files to the device.

Figure 2-13: Administrative Web Interface Upload Menu (Host)

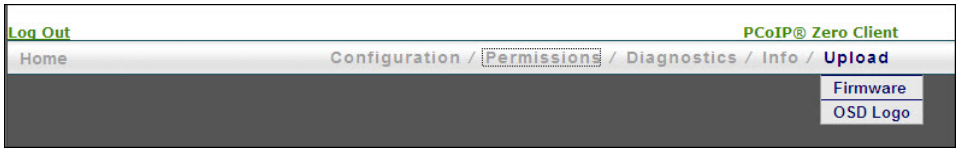


Figure 2-14: Administrative Web Interface Upload Menu (Client)

For information on each of the Upload options, see section 8.

3 Working with the On Screen Display (OSD)

The On Screen Display (OSD) local GUI appears on the client when the device is powered on and a PCoIP session is not in progress. The OSD lets the user connect to a host device through the **Connect** screen.

The **Connect** screen also lets the user access the **Options** page, which provides a subset of the functionality provided by the Administrative Web Interface.

To access the **Options** page, click the **Options** menu on the **Connect** screen.

3.1 About the Connect Screen

The **Connect** screen appears during the startup except when the client is configured for a managed startup or auto-reconnect.

You can change the logo that appears above the **Connect** button by uploading a replacement image through the Administrative Web Interface.

The **Network** icon at the bottom right of the **Connect** screen shows the status of the network connection. Users must wait until the **Network Ready** icon appears as shown in the bottom right corner of the following figure:

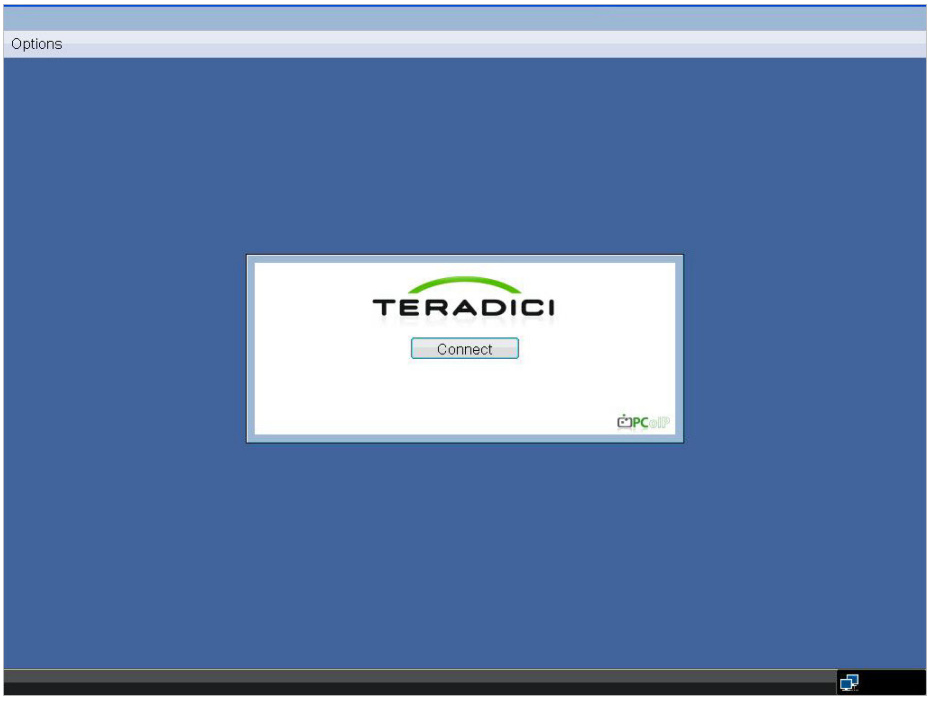


Figure 3-1: OSD Connect Window

A red X over the network icon means that either the network is not properly connected or that the connection is still being initialized (that is, during client bootup).

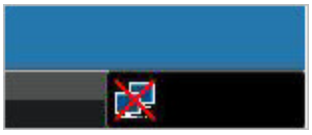


Figure 3-2: Network Not Ready (detail)

Figure 3-3: Network Ready (detail)

3.1.1 Connect Button

Click the **Connect** button to start a PCoIP session. When the PCoIP connection is pending, the OSD local GUI displays a "Connection Pending" message. When the connection is established, the OSD local GUI disappears and is replaced with the session image.

Figure 3-4: OSD Connect Screen (Connecting)

3.2 About the OSD Options Menu

There are five pages available from the **Options** menu:

Configuration: This option lets you configure various aspects for the device such as the network settings, peer connection, session parameters, and so on. For details about the options, see section 4.

Diagnostics: This option helps you troubleshoot the device. For details about the option, see section 6.

Information: This option lets you view certain details about the device. For details about the options, see section 7.

User Settings: This option lets the user define mouse and keyboard settings, as well as the PCoIP protocol image quality. For details about the options, see section 5.

Password: This option lets you update the administrative password for the device. For details about the options, see section 4.18.

4 Configuring the Device

The **Configuration** option on the Administrative Web Interface and OSD lets you configure various aspects for the device. This section walks you through the full set of configuration options.

Note: The **OSD** configuration options are a subset of the options available in the Administrative Web Interface. To make changes to the configuration settings you need an administrative password. You do not need a password to view the **Diagnostic** and **Information** menus.

Firmware 3.3.0 or newer lets you disable the OSD and Administrative Web Interface from the PCoIP Management Console. See sections 4.21 and 4.22 for more details.

4.1 Initial Setup Page

The **Initial Setup** page contains the configuration parameters that the administrator must set when first using the client and host devices. The page simplifies the out-of-box experience and reduces the time for new users to establish a one-to-one PCoIP session, or sessions between a PCoIP zero client and PCoIP host card in a remote workstation. More complex environments that use host discovery or connection management systems require further configuration.

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

The client and host **Initial Setup** pages are not identical and provide parameters that apply to the client and host respectively.

After you update the settings on this page, click **Apply**.

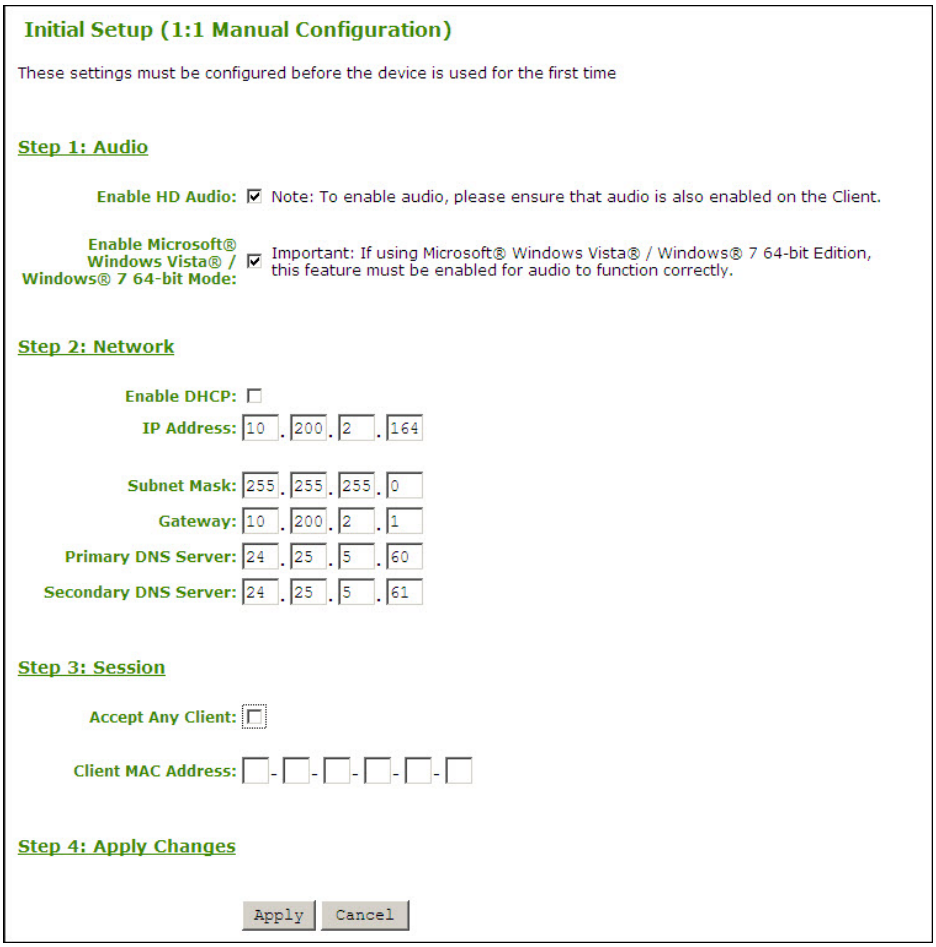


Figure 4-1: Initial Setup Page (Host)

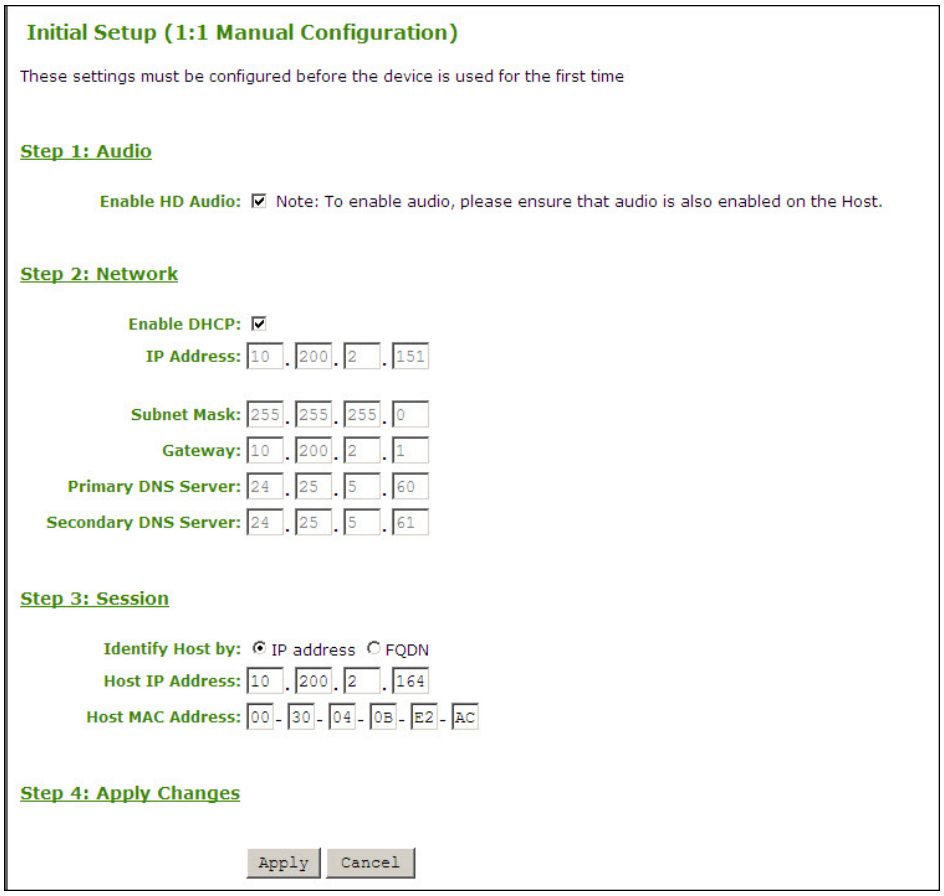


Figure 4-2: Initial Setup Page (Client)

Table 4-1: Audio Parameters

For details on configuring the full set of **Audio** parameters, see section 5.2.

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. This option is only available on the host. It does not appear on the client. Note: Enabling 64-bit mode is not required for Linux or Windows XP (32-bit or 64-bit).

Table 4-2: Network Parameters

For details on configuring the full set of **Network** parameters, see section 4.2.

Parameter	Description
Enable DHCP	Enables DHCP versus manual configuration
IP Address	Device's IP address
Subnet Mask	Device's subnet mask
Gateway	Device's gateway IP address

Parameter	Description
Primary DNS Server	Device's primary DNS IP address
Secondary DNS Server	Device's secondary DNS IP address

Table 4-3: Session Parameters (Host)

For details on configuring the full set of **Session** parameters, see section 4.10.

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.

Parameter	Description
Identify Host by	Specifies the host identify method.
Host IP Address	Specifies the host IP address.
Host MAC Address	Specifies the host MAC address. You can set the host MAC address to 0-0-0-0-0-0 to ignore this field when a session starts. Note: You cannot set the client MAC address to 0-0-0-0-0-0.

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

4.2 Configuring the Network Settings

You can configure the host and client network settings from the **Initial Setup** page or **Network** page. After you update the parameters on this page, click **Apply** to save your changes.

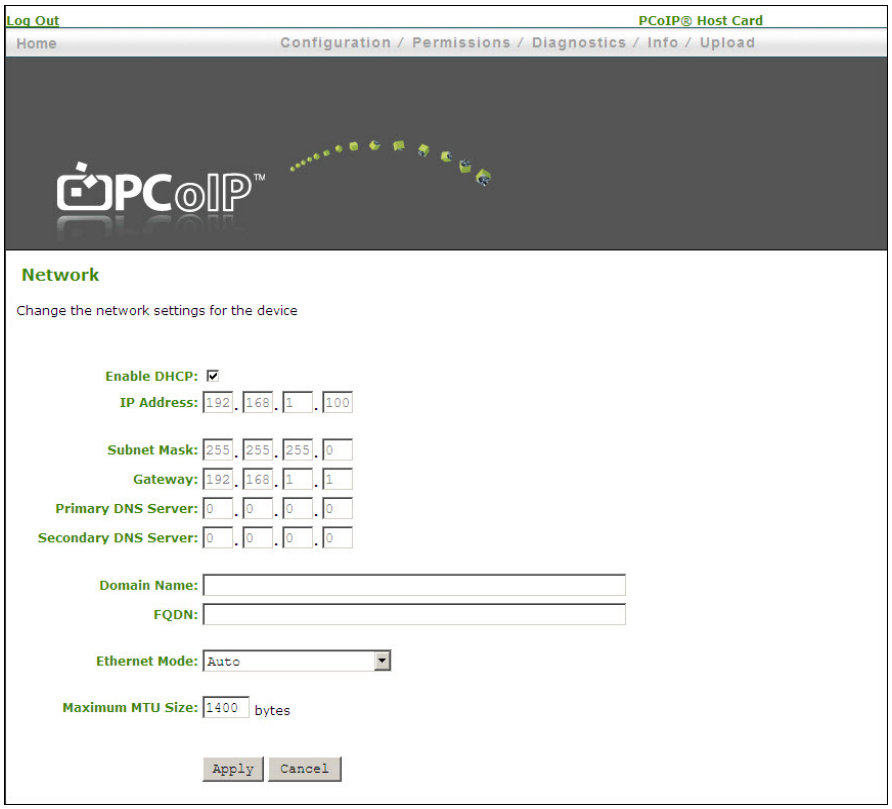


Figure 4-3: Administrator Web Interface Network Page

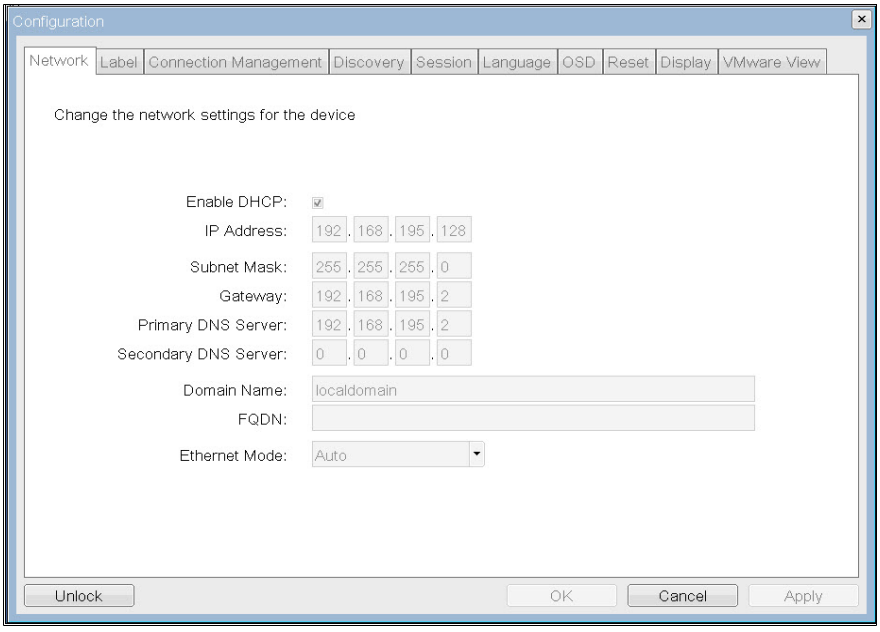


Figure 4-4: OSD Network Page

Table 4-4: 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. The firmware requests a domain name (option 15), host name (option 12), and client FQDN (option 81). When disabled: You must set these parameters manually.
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field. Warning: It is possible to configure an illegal IP Address/Subnet Mask combination (e.g., invalid mask) that leaves the device unreachable. Take care when setting the Subnet Mask.
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a Connection Manager, the Connection Manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a Connection Manager, the Connection Manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain named used (for example, 'domain.local'). This field is optional. This field specifies the host or client's domain.
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. 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: • Auto • 10 Mbps • Full-Duplex • 100 Mbps Full-Duplex When you choose 10 Mbps Full Duplex or 100 Mbps Full-Duplex and then click **Apply**, this warning message appears: "Warning: When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?" Click **OK** to change the parameter. Note: You should always set the Ethernet Mode to Auto and only use 10 Mbps Full-Duplex of 100 Mbps Full-Duplex when the other network equipment (for example, switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet

Parameter	Description
	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. A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the **Maximum MTU Size** to a value smaller than the network path MTU for the end-to-end connection between the host and client. The **Maximum MTU Size** range is 500 to 1500 bytes. Note: the default MTU is 1400 for sessions between PCoIP zero clients and PCoIP host cards. The default MTU is 1300 for sessions with PCoIP software (in the host or client) such as VMware View.

4.3 Adding Custom Information for the Device

The **Label** page is available from the host or client. The **Label** page lets you add information for the device.

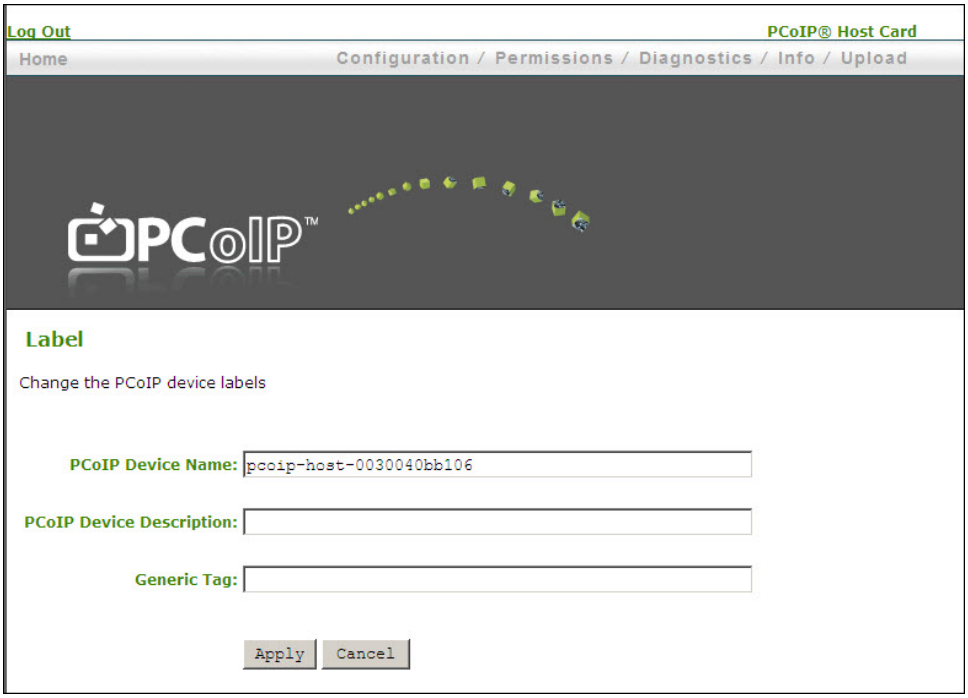


Figure 4-5: Administrative Web Interface Label Page

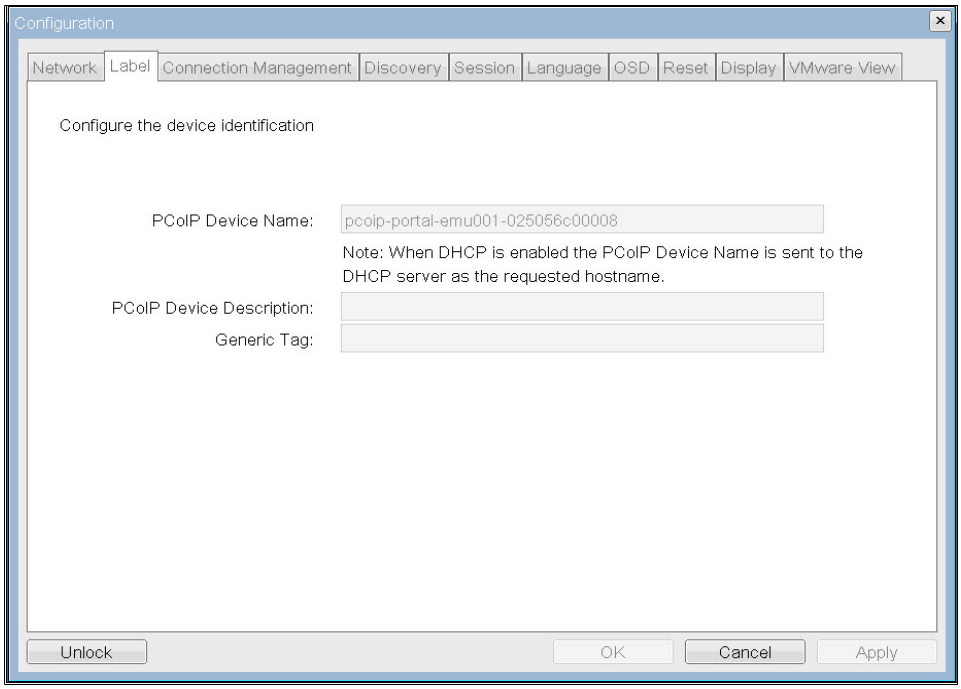


Figure 4-6: OSD Label Page

Table 4-5: Label Page Parameters

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

4.4 Enabling or Disabling Connection Management

The **Connection Management** page lets you enable or disable connection management and specify the IP address of the connection manager that is not VMware View.

VMware View connection management settings are in a dedicated **OSD** tab. See sections 4.5 and 4.6 for details.

In a managed connection, an external connection manager server:

- communicates with and can remotely control and configure the device.
- can locate an appropriate peer for the device to connect to and initiate the connection.
- can simplify the administration effort for large, complex systems.

Figure 4-7: Administrative Web Interface Connection Management Page

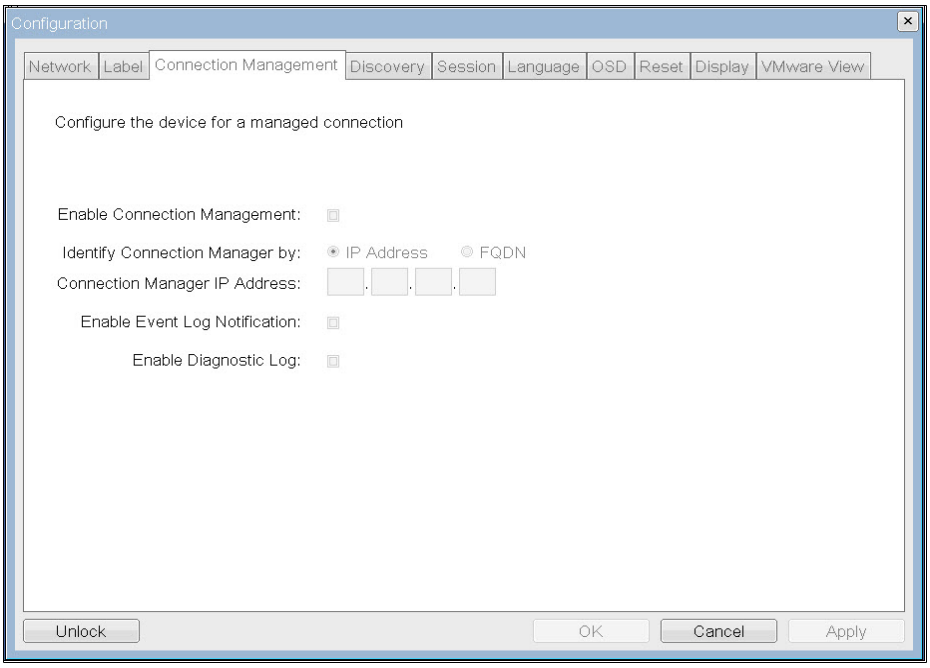


Figure 4-8: OSD Connection Management Page

Table 4-6: Connection Management Page Parameters

Parameter	Description
Enable Connection Management	When enabled, you can configure and control the device by using an external connection manager.
Identify Connection Manager By	Lets you choose if the connection manager is identified by an IP address or by an FQDN. If **Connection Management** is disabled, this field is not required and is not editable.
Enable Event Log Notification	Controls if the host and client devices send the contents of their event logs to the connection management server.
Enable Diagnostic Log	Controls if connection management specific debug messages are written to the event log of the host and client devices.

4.5 Configuring for Use with a VMware View Connection Server

The **VMware View** page lets you configure your client for use with a VMware View Connection server. The **VMware View** page is only available on a client. It is not available on the host.

Figure 4-9: Administrative Web Interface VMware View Page (Client Only)

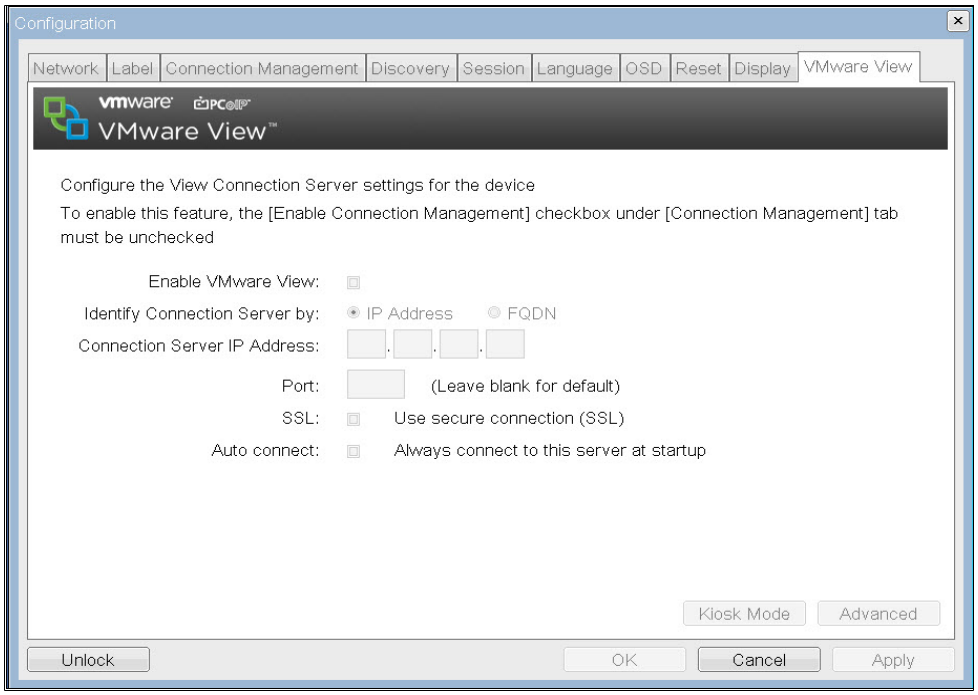


Figure 4-10: OSD VMware View Page

Figure 4-11: OSD VMware View Page Connection Server Options

Table 4-7: VMware View Page Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Enable VMware View</td><td>When enabled, you can configure the client for use with a VMware View Connection Server.
Note: To enable the VMware View feature, the Enable Connection Management checkbox on the Connection Management page must be unchecked.
If VMware View is disabled, the remaining fields are not required and are not editable.</td></tr>
<tr><td>Identify Connection Server by</td><td>Choose how the connection manager is identified:
IP Address
FQDN</td></tr>
<tr><td>Connection Server FQDN</td><td>When FQDN is enabled, you can enter the URL used to specify the VMware View Connection Server. Some examples of valid URL formats include:
myconnectionserver.teradici.com
http://myconnectionserver.teradici.com
https://myconnectionserver.teradici.com/</td></tr>
<tr><td>Port</td><td>Specify the port used to communicate to the VMware View Connection server.
Specify if you want the client to communicate with the VMware View Connection server over a secure connection using SSL.
If SSL is enabled and the port number is blank, port 443 is used. By default, the Port field is blank.
If SSL is disabled and the port number is blank, port 80 is used. By default, the Port field is blank.
If the port number and SSL settings are not entered properly, an error message may pop up and prevent you from connecting to a VMware View Connection server.
Note: If the entered port number matches the default port number, the next time you view the VMware View tab, the Port number field is blank.</td></tr>
<tr><td>SSL</td><td>The SSL setting is configurable in both the VMware View Connection server and from the VMware View page on the client. The SSL setting in the VMware View Connection server is the master setting that overrides the local setting in the client. The results of the SSL setting in the VMware View Connection server and from the VMware View page appears in the following table.
<table>
<tr><th rowspan="2"></th><th rowspan="2"></th><th colspan="2">VMware View Connection Server</th></tr>
<tr><th>SSL disabled</th><th>SSL enabled</th></tr>
<tr><td rowspan="2">VMware View Page</td><td>SSL disabled</td><td>SSL disabled</td><td>SSL enabled</td></tr>
<tr><td>SSL enabled</td><td>View Connection Server communication error</td><td>SSL enabled</td></tr>
</table>
For example, if SSL is enabled in the VMware View Connection server but is disabled from the VMware View page, the resulting SSL mode is enabled.
By default, the SSL field is blank.</td></tr>
</table>

Parameter	Description
	Note: For security, we recommended using Port 443 and enabling SSL from the **VMware View** page and in View Connection server, as the authentication password to the View Connection server is not encrypted when the resulting SSL mode is disabled. With SSL disabled, the user's login password is not encrypted and can be captured using network protocol tools. When using SSL, we suggest that you configure the SSL setting on the View Connection server (master) to ensure the SSL is used regardless of the client's **SSL** field configuration.
Auto connect	Specify if the client should always connect with the VMware View Connection server at startup. When **Auto connect** is enabled, the client automatically connects to the VMware View Connection server whenever the client powers up or when a session with the virtual desktop is terminated. The user sees the user credentials login dialog box on the OSD instead of the **Connect** dialog box After enabling auto connect, the client must be power-cycled for the change to take effect.
Connection Server Cache Mode	Set this field to: • Last five servers used: These appear on the **Connection Server** entry box on the **OSD VMware View Connect** page. • Read-only Note: The PCoIP Management Console can be used to pre-populate the list of available connection servers.

4.6 Configuring the VMware View Advanced Settings

The **Advanced** button from the **VMware View** page lets you set advanced VMware View parameters for the zero client.

To display the **Advanced Settings** page from the Administrative Web Interface:

1. From the **Configuration** menu, click **VMware View (Advanced)**.

The **Advanced Settings** page appears:

Figure 4-12: Administrative Web Interface VMware View Advanced Settings Page

To display the **Advanced Settings** page from the OSD:

1. From the **Configuration** menu, click the **VMware View** tab. The **VMware View** page appears.
2. Click the **Advanced** button.

The **Advanced Settings** page appears.

Figure 4-13: OSD VMware View Advanced Settings Page

Table 4-8: VMware View Advanced Configuration Page Parameters

Parameters	Description
Auto Launch If Only One Desktop	When enabled and the user credentials are entered, users are automatically connected to their virtual desktop. Note: This feature is for users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.
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. You can upload a custom OSD logo via the Administrative Web Interface.
Prefer GSC-IS	When selected, the CAC GSC 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 the **Prefer GSC-IS** setting. This only affects smart card access performed outside of PCoIP sessions. **Prefer GSC-IS** is selected by default.
Enable Auto-Logon	When enabled, the logon information is automatically entered. The user does not need to enter a username or password when connecting to the device.
Logon Username	The name of the user.
Logon Password	The user's password.
Logon Domain Name	The domain name for the client being configured.
Desktop Name to Select	Enter the pool/desktop name used by a zero client when starting a session.

4.7 Configuring Kiosk Mode

You can configure kiosk mode through the OSD or the Administrative Web Interface. Kiosk mode requires a properly configured VMware View environment. See the applicable VMware View documentation for more information.

To configure the kiosk mode settings from the Administrative Web Interface:

1. Log in to the Administrative Web Interface for the client.
2. From the **Configuration** menu, select **VMware View (Kiosk Mode)**.

   The **Kiosk Mode** page appears:

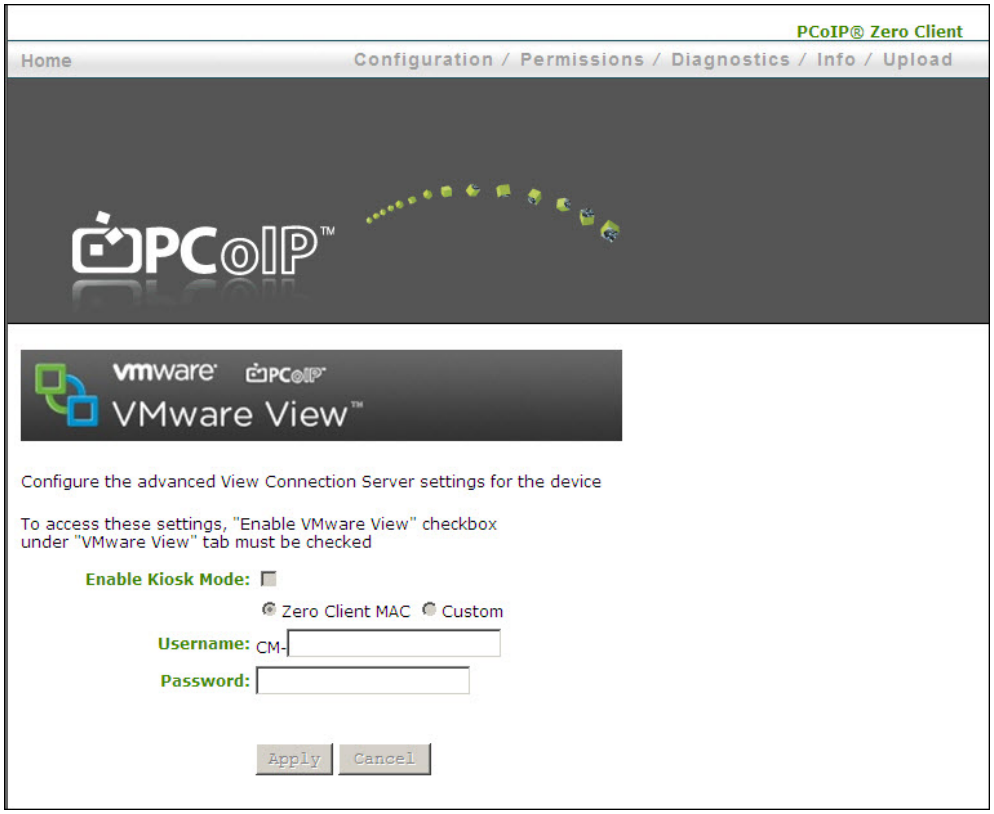


Figure 4-14: Administrative Web Interface Kiosk Mode Page

To configure the kiosk mode settings from the OSD:

1. From the **Configuration** menu, click the **VMware View** tab.
2. Click **Kiosk Mode**.

   The **Kiosk Mode** page appears.

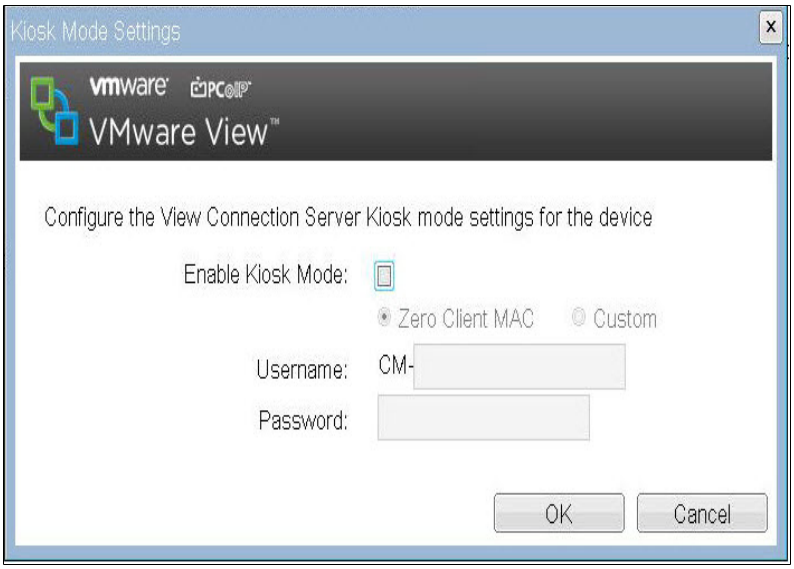


Figure 4-15: OSD Kiosk Mode Page

Table 4-9: Kiosk Mode Page Parameters

Parameters	Description
Enable Kiosk Mode	When enabled, the PCoIP zero client automatically logs in on powerup to a pre-defined virtual desktop. Users do not need to enter their credentials.
Zero Client MAC Option	If the **Zero Client MAC** option is selected, the username is automatically entered based on the unique MAC address of the PCoIP zero client.
Custom Option	If the **Custom** option is selected, the username is set to “CM” and the username is entered.
Password	The **Password** field is used as the session password when kiosk mode automatically logs the PCoIP zero client into the predefined virtual desktop.

4.8 Configuring the Discovery Mechanism

Use the settings on the **Discovery Configuration** page to ease the discovery of hosts and clients in your PCoIP system and dramatically reduce the configuration and maintenance effort for complex systems. This discovery mechanism is independent of DNS SRV discovery.

Note: For SLP discovery to work, routers must be configured to forward multicast traffic between subnets. Because most deployments do not allow this, DNS-SRV Discovery is the recommended discovery mechanism.

Figure 4-16: Administrative Web Interface Discovery Page (Client)

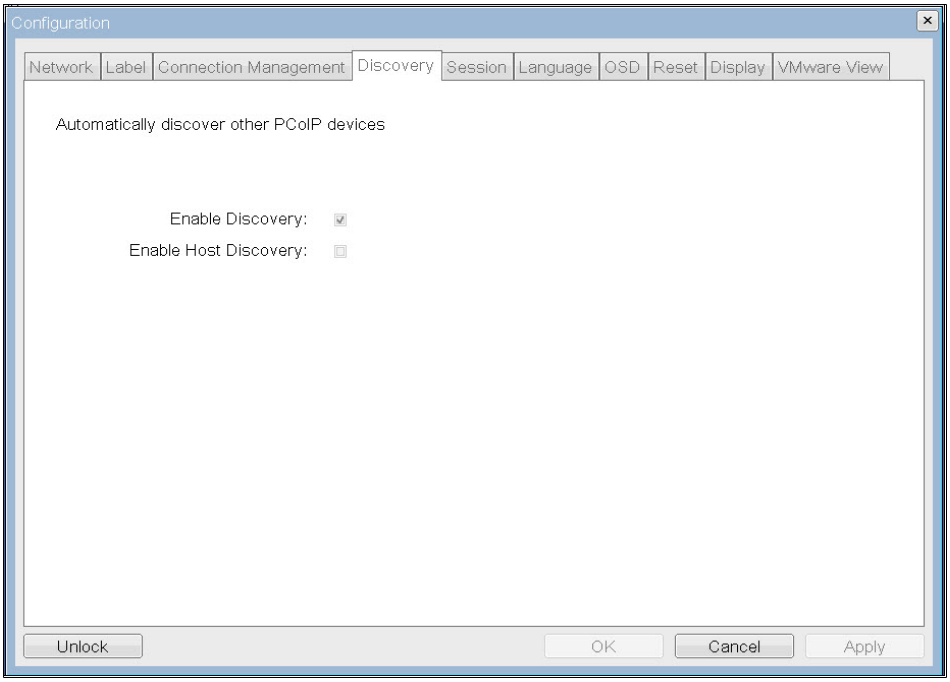


Figure 4-17: OSD Discovery Page

Table 4-10: Discovery Page Parameters

Parameters	Description
Enable SLP Discovery	When enabled, the hosts and clients can be dynamically discovered by SLP management entities without requiring prior knowledge of their locations in the network.
Enable Host Discovery	Lets the client discover hosts that are not in a PCoIP session. When enabled, the client can display up to 10 available hosts in the order that they were discovered. It is expected that the **Enable Host Discovery** feature is used with a small number of hosts. Note: This option is only available on a client. It is not available on the host.
Enable DNS SRV	When enabled: • Hosts and clients can be dynamically discovered by a connection broker discovery method that uses DNS SRV resource records without knowing their locations in the network. • The host or client tries to download and use the DNS SRV record from the DNS server. Note: The **Enable DNS SRV** option configures the discovery for connection brokers but does not affect the DNS SRV functionality for the PCoIP Management Console.
DNS SRV Discovery Delay	Configure the amount of delay time in seconds between the DNS SRV Discovery attempts for connection brokers and the PCoIP Management Console. DNS SRV Discovery continues periodically until the device successfully contacts a Connection Management server. 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.

4.9 Configuring the SNMP Agent

The **SNMP** page lets you enable or disable the host or client SNMP agent.

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

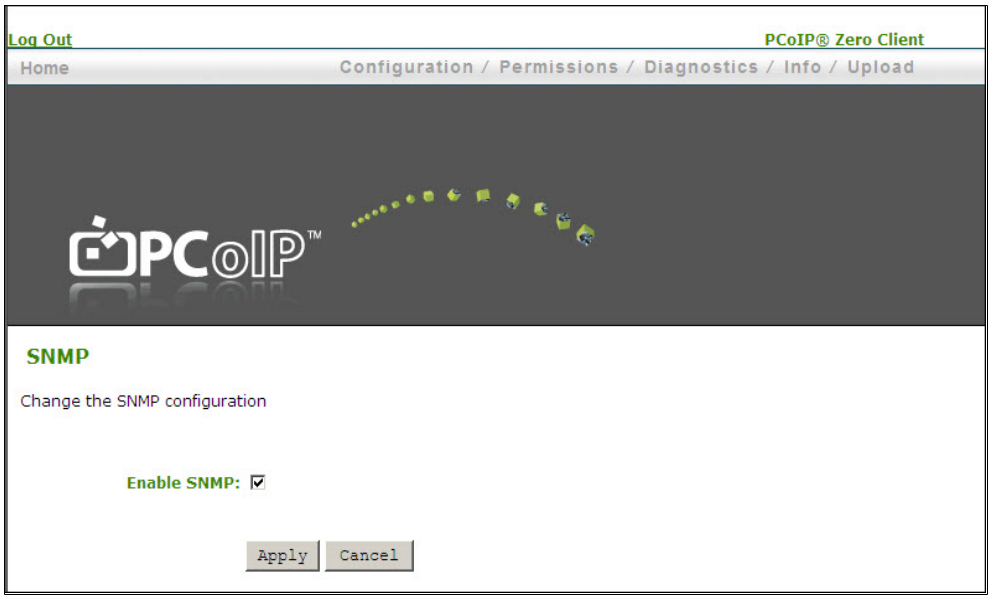


Figure 4-18: Administrative Web Interface SNMP Agent Page

Table 4-11: SNMP Agent Page Parameters

Parameters	Description
Enable SNMP	When enabled, the host or client enables the PCoIP SNMP agent. Disabling the SNMP agent ensures that the PCoIP SNMP MIB cannot be accessed.

4.10 Configuring the Connections between Devices

The **Session** page lets you configure how the host or client device connects to or accepts connections from peer devices.

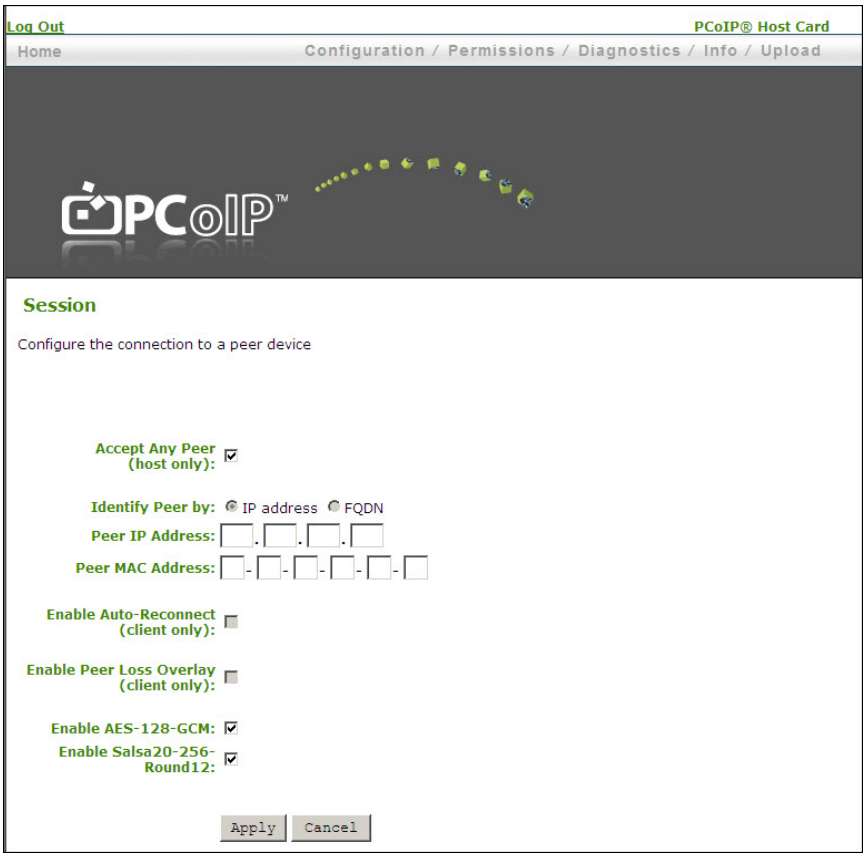


Figure 4-19: Administrative Web Interface Session Page (Host)

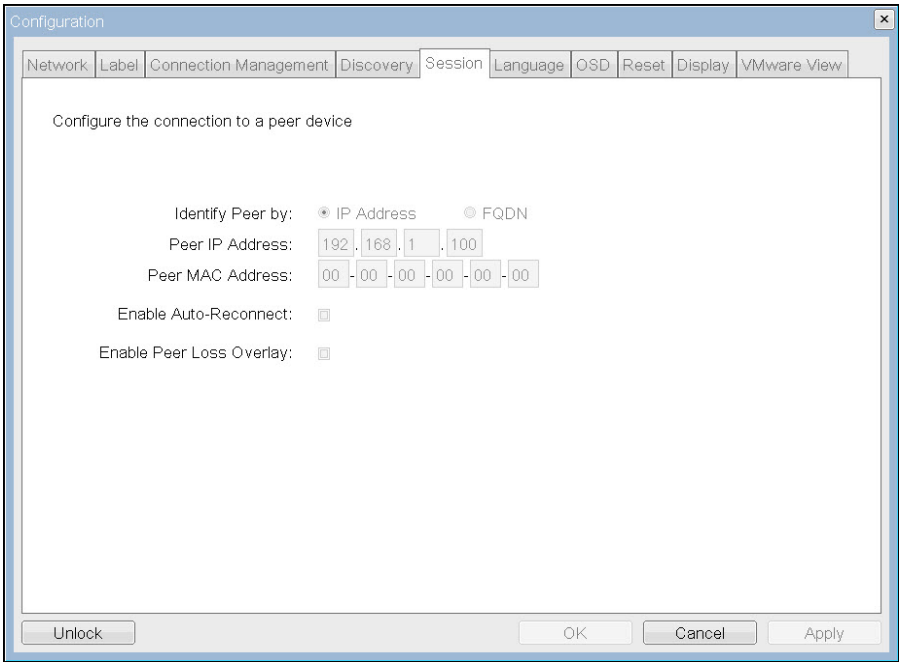


Figure 4-20: OSD Session Page

Note: The parameters on this page are different for the host and client. If a host is configured to accept any peer, some of the fields on this page become non-editable. If **Accept Any Peer** is disabled the user must enter the peer (client) MAC address and the IP address is non-editable.

Table 4-12: Session Page Parameters

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Accept Any Peer</td><td>If enabled, the host accepts connections from any client. If this option is disabled, you must specify the MAC address of the peer you want the host to accept.
Note: This option is only available on a host. It is disabled and non-editable on the client.</td></tr>
<tr><td>Identify Peer By</td><td>Choose if the device is identified by its IP and MAC address or by the FQDN. If the Accept Any Peer option is enabled, these fields are not required and not editable on the host.
The following table shows the peer identify parameters available for either method. If you enter an invalid IP address or DNS name, the web interface prompts you to correct it.
You can set the Peer MAC Address to 00-00 00-00-00-00 on a zero client and the field is ignored.
<table>
<tr><th>Peer Identify Method</th><th>Data Fields</th><th>Comment</th></tr>
<tr><td rowspan="2">Peer IP/MAC</td><td>Peer IP address</td><td>PCoIP client</td></tr>
<tr><td>Peer MAC address</td><td>PCoIP client</td></tr>
<tr><td rowspan="2">Peer FQDN</td><td>Peer DNS Name</td><td>PCoIP client</td></tr>
<tr><td>Peer MAC address</td><td>PCoIP client</td></tr>
</table></td></tr>
<tr><td>Enable Auto-Reconnect</td><td>Lets the client automatically reconnect with the last connected host when a session is lost.
Note: This setting is only available on a zero client.</td></tr>
<tr><td>Enable Peer Loss Overlay</td><td>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. This option is disabled by default.
Note: This option is only available for a zero client. It is disabled and non-editable on the host. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.</td></tr>
<tr><td>Enable AES-128-GCM</td><td>Configure the AES-128-GCM encryption for the host or client. AES-128-GCM is an encryption method implemented in the TERA1x100 processor that allows best performance between hardware endpoints.
Note: The enabled encryption must match between the host and client for a session to be established. If both modes are enabled, the firmware selects:
• Host to client: AES-128-GCM for the PCoIP session
• VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session</td></tr>
<tr><td>Enable SALSA20-256-Round 12</td><td>Configure SALSA20-256-Round 12 encryption for the host or client. SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 or higher when there is more than about 7 Mbps available on the network. (See TER0904005 Using PCoIP Zero Clients with VMware View 4 User Guide for more information.)
Note: The enabled encryption must match between the host and client</td></tr>
</table>

Parameters	Description
	for a session to be established. If both modes are enabled, the firmware selects: • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session

4.11 Controlling the Bandwidth for PCoIP Sessions

The **Bandwidth** page lets you control the bandwidth used by the device during a PCoIP session. This applies to sessions between PCoIP zero clients and PCoIP host cards in a remote workstation.

The parameters in this page are applied after you click **Apply**.

To configure the bandwidth used with a VMware View virtual desktop, adjust the PCoIP GPO session variables. See *VMware View 4 to PCoIP Client WAN Network Guidelines* for more information.

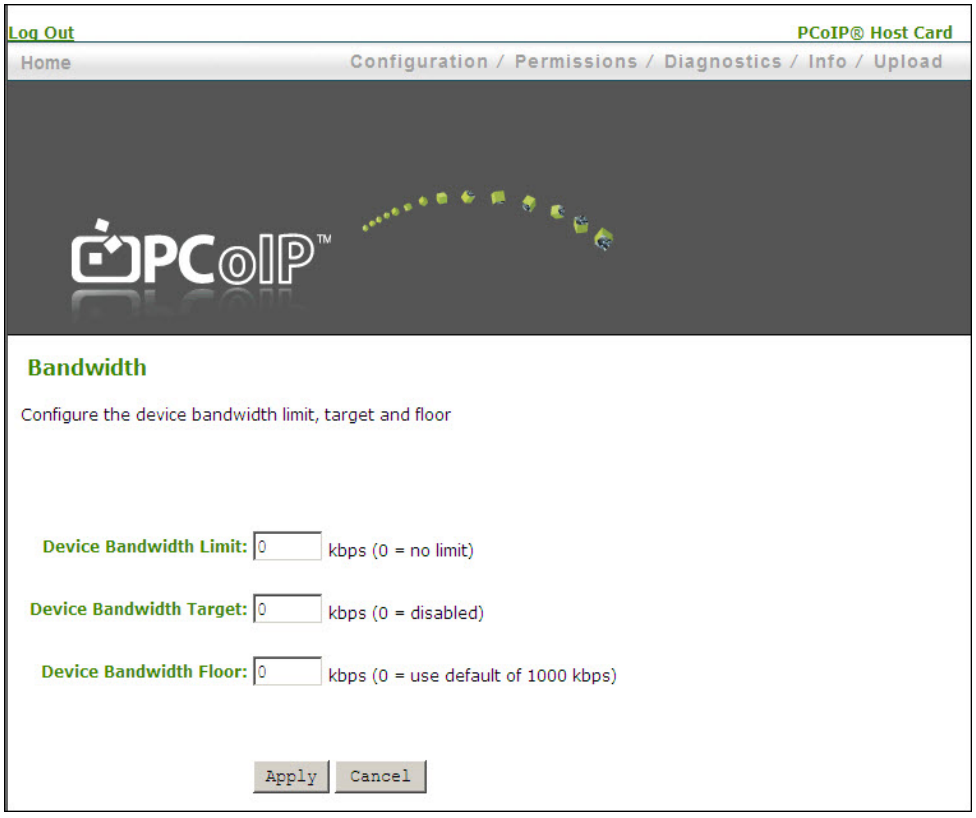


Figure 4-21: Administrative Web Interface Bandwidth Page

Table 4-13: Bandwidth Page Parameters

Parameters	Description
Device Bandwidth Limit	Defines the maximum bandwidth peak for the PCoIP system. The bandwidth setting defines the bandwidth based on which side is sending data: • **On the host side:** from the host to the client (e.g., graphics data) • **On the client side:** from the client to the host (e.g., USB data) The usable range of the device bandwidth is 1000 to 220,000 kbps. The PCoIP processor only uses the required bandwidth up to the **Device Bandwidth Limit** maximum. The PCoIP processor dynamically adjusts the bandwidth in response to network congestion. Setting the **Device Bandwidth Limit** to 0 configures the PCoIP processor to adjust the bandwidth depending on network congestion. If there is no congestion, there is no limit on bandwidth. That is, the processor uses the maximum rate available. We recommend setting this field to the limit of the network connected to the client and host. Note: The setting in this field is applied immediately after you click **Apply**.
Device Bandwidth Target	Defines the temporary limit on the network bandwidth during periods of congestion (packet loss). When the network experiences congestion, the device bandwidth is reduced rapidly to the target value and more slowly below this value. This allows for a more even distribution of bandwidth between users sharing a congested network link. After the congestion is alleviated, the bandwidth used increases depending on the available network resources up to the **Device Bandwidth Limit**. You should have a good understanding of the network topology before setting this to a non-zero value.
Device Bandwidth Floor	Lets you configure the bandwidth floor used by the firmware when congestion is present and when bandwidth is required. This lets you optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used drops below the floor. A setting of 0 lets the firmware reduce bandwidth to 1000 kbps for these network impairments. You should have a good understanding of the network topology before setting this to a non-zero value. Note: The firmware implements a Slow Start Algorithm that: • increases the bandwidth used until the bandwidth required is reached, network congestion is detected, or the **Device Bandwidth Limit** is reached • begins at the lesser of the **Device Bandwidth Limit** and 8000 kbps • increases the bandwidth used within seconds • allows a graceful session startup for low bandwidth scenarios (for example, WAN) After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.

4.12 Setting the User Interface Language

The **Language** page lets you change the user interface language.

Note: This setting affects the local OSD GUI. It is only available on the client.

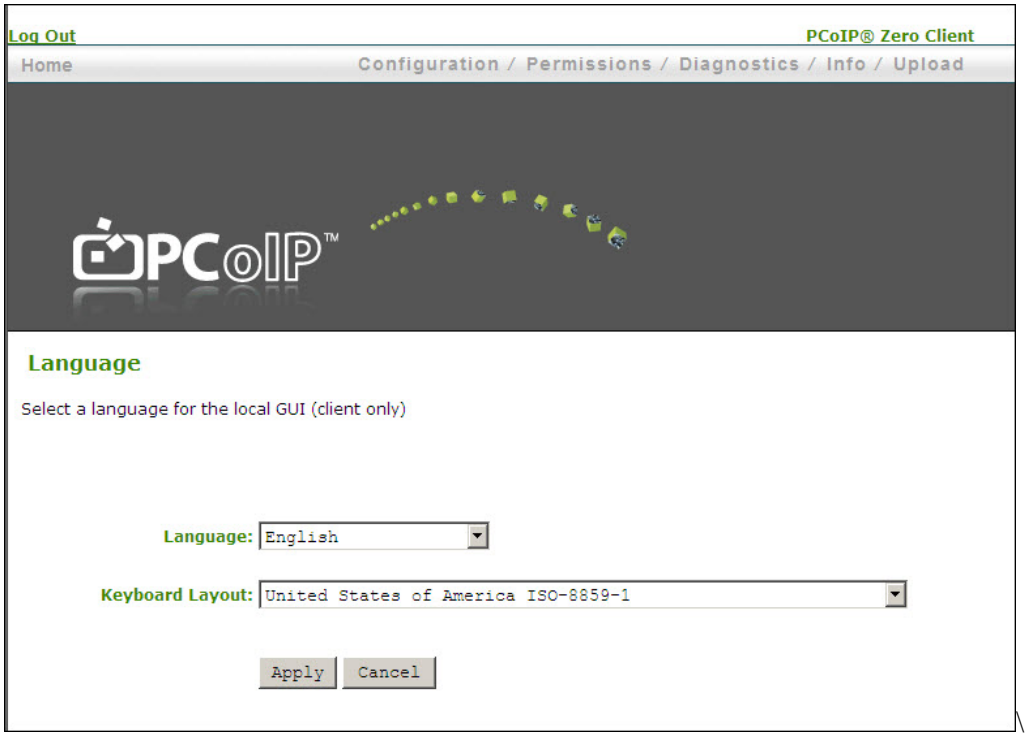


Figure 4-22: Administrative Web Interface Language Page

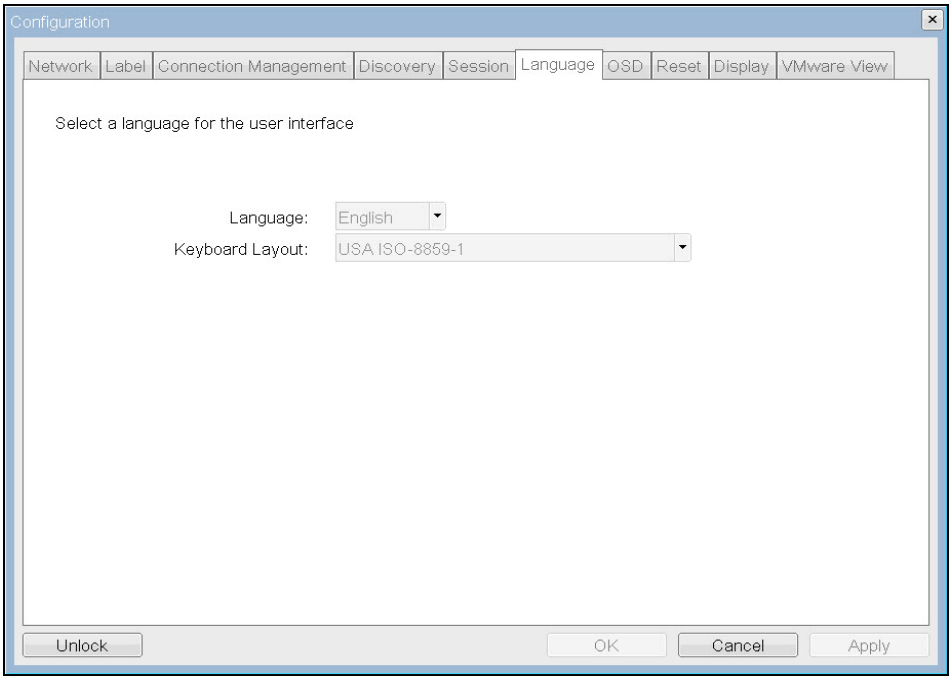


Figure 4-23: OSD Language Page

Table 4-14: Language Page Parameters

For a list of supported languages and keyboard layouts, see section Appendix B.

Parameters	Description
Language	Configure the OSD language. This setting only determines the language for the OSD only. It 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 Windows GPO is set to allow the keyboard layout setting, it is used during the user's session. If the Windows GPO is not set to allow the setting, it is dropped.

4.13 Configuring the OSD Screen-save Timeout

The **OSD** page lets you set the screen-saver timeout on the **On Screen Display** parameter.

Note: The **OSD** page is only available on the client. It is unavailable on the host.

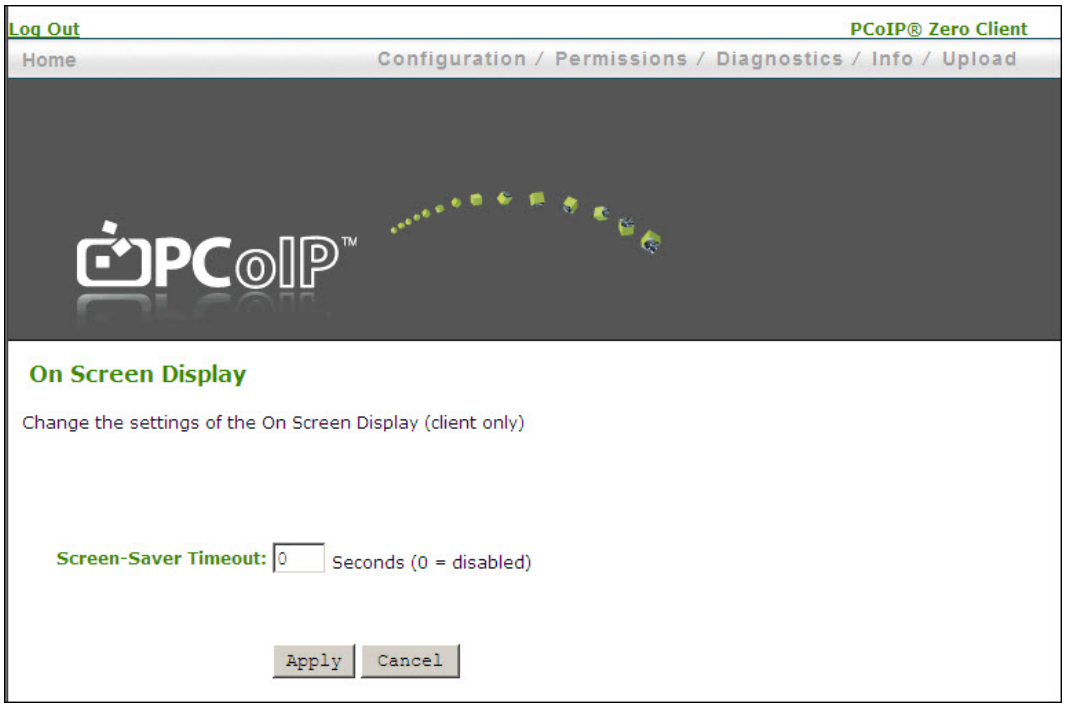


Figure 4-24: Administrative Web Interface OSD Page

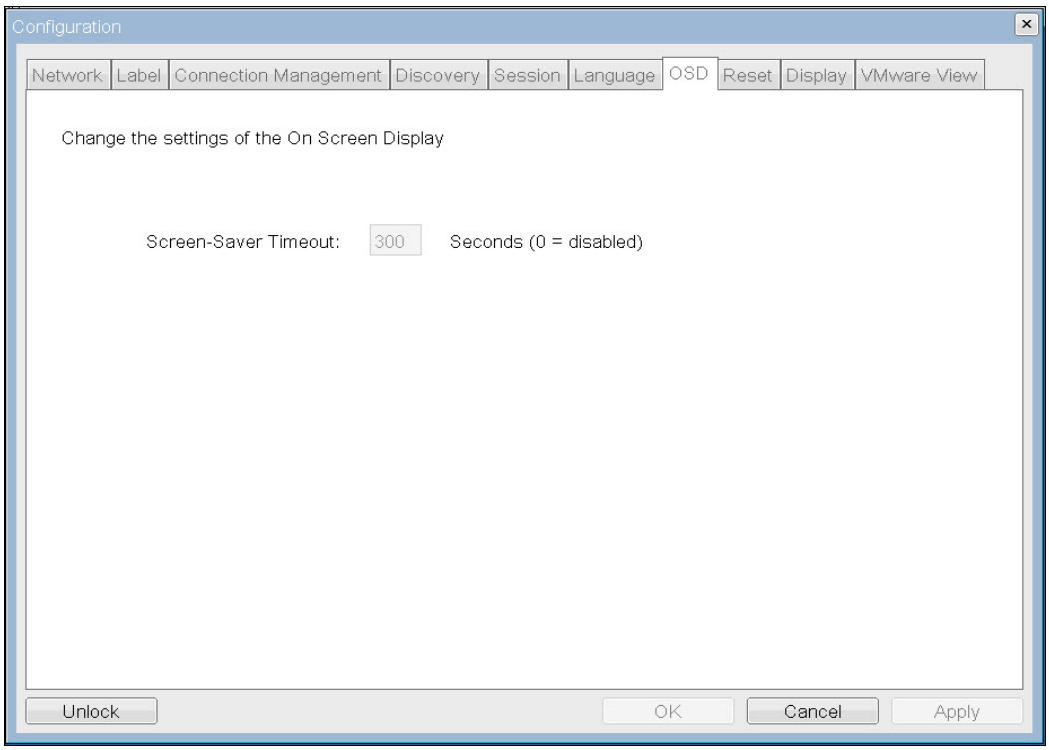


Figure 4-25: OSD-OSD Page

Table 4-15: OSD Page Parameters

Parameters	Description
Screen-saver Timeout	Configure the screen-saver timeout before the client puts the attached displays into low-power mode. You can configure the timeout mode in seconds, up to 9999 seconds. A setting of 0 seconds disables the screen-saver.

4.14 Adjusting the Image Quality

The **Image** page lets you make changes to the image quality of the PCoIP session. This applies to sessions between PCoIP zero clients and PCoIP host cards in a remote workstation.

To configure the image quality settings with a VMware View virtual desktop, adjust the PCoIP session variables. See *VMware View 4 to PCoIP Client WAN Network Guidelines* for more information.

Note: The **Image** page is only available on the client. It is not available on the host.

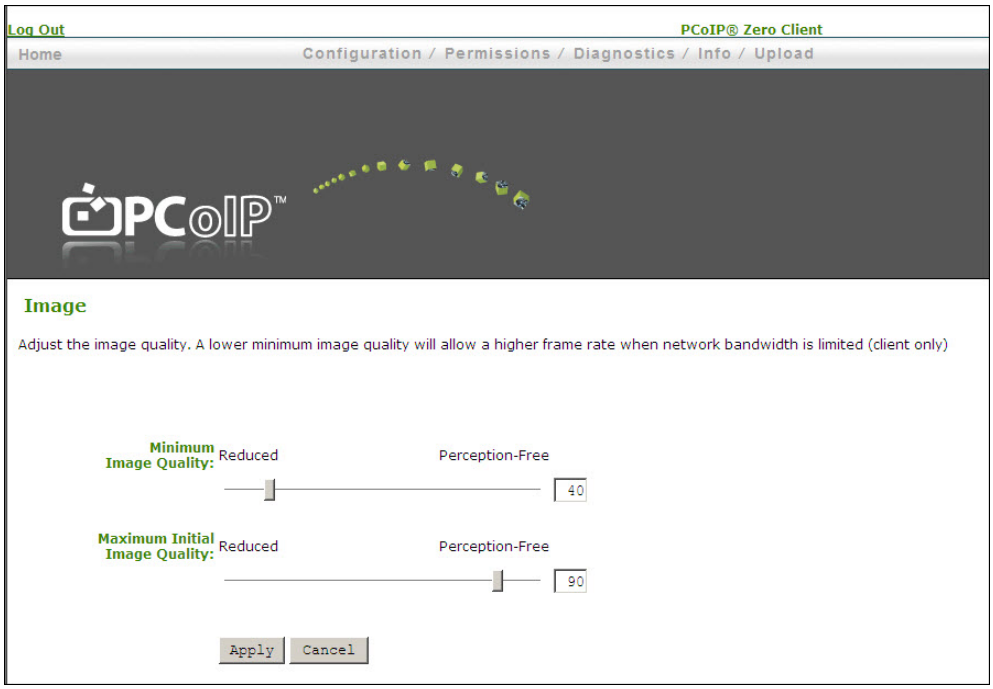


Figure 4-26: Administrative Web Interface Image Page

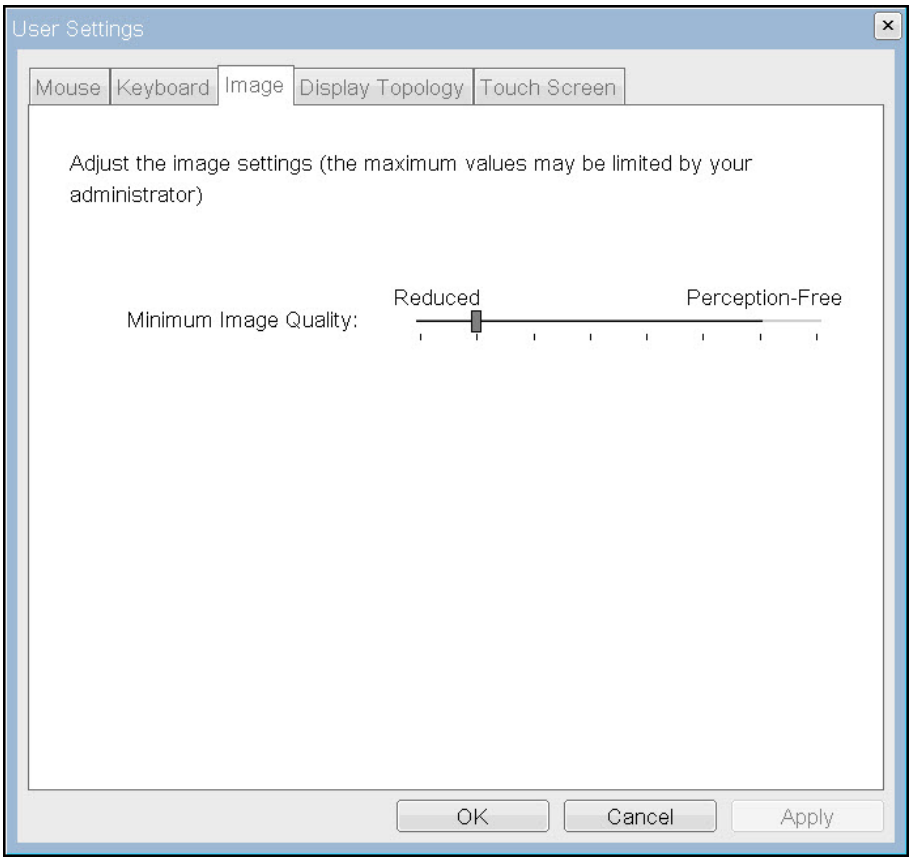


Figure 4-27: OSD Image Page

Table 4-16: Image Page Parameters

For more details about adjusting the image quality, see section 9.4.

Parameter	Description
Minimum Image Quality	Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate. In environments where the network bandwidth is constrained, moving the slider towards **Reduced** allows higher frame rates. Moving the slider towards **Perception-Free** allows for higher image quality. When network bandwidth is not constrained, the PCoIP system maintains perception-free quality regardless of the **Minimum Image Quality** parameter. Note: The **Minimum Image Quality** must be less than or equal to the **Maximum Initial Image Quality**.
Maximum Initial Image Quality	Use the slider to reduce the network bandwidth peaks caused by screen content changes. This parameter limits the initial quality on the first display frame of a screen change. Unchanged regions of the image are built to a lossless state regardless of this parameter. Note: The **Maximum Image Quality**: • must be greater than or equal to the **Minimum Image Quality**

Parameter	Description
	• does not have a corresponding parameter on the OSD as it is an administrator-only parameter

4.15 Enabling Monitor Emulation

The **Monitor Emulation** page lets you enable or disable the monitor emulation feature. This option is only available on a host. 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.

Note: Some PCoIP host devices do not require firmware monitor emulation and the **Monitor Emulation** page is not available.

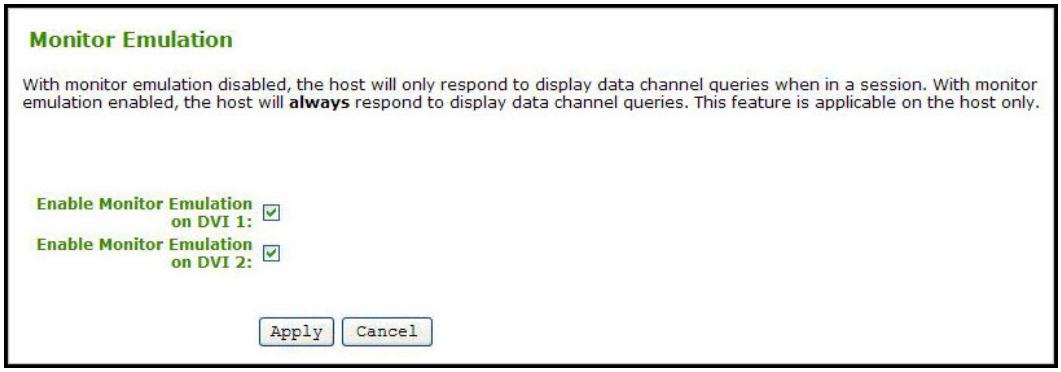


Figure 4-28: Administrative Web Interface Monitor Emulation Page

When **Enable Monitor Emulation** is:

- **Disabled:** Only the host responds to Display Data Channel (DDC) when in a PCoIP session.
- **Enabled:** The host uses emulated data for DDC queries regardless if in a PCoIP session of not.

Independent **Enable Monitor Emulation** fields are available for both monitor ports, DVI1 and DVI2.

4.16 Enabling the Host Driver Function

The **Host Driver Function** page lets you enable or disable the host driver function.

Note: The **Host Driver Function** page is only available on the host. It is not available on the client.

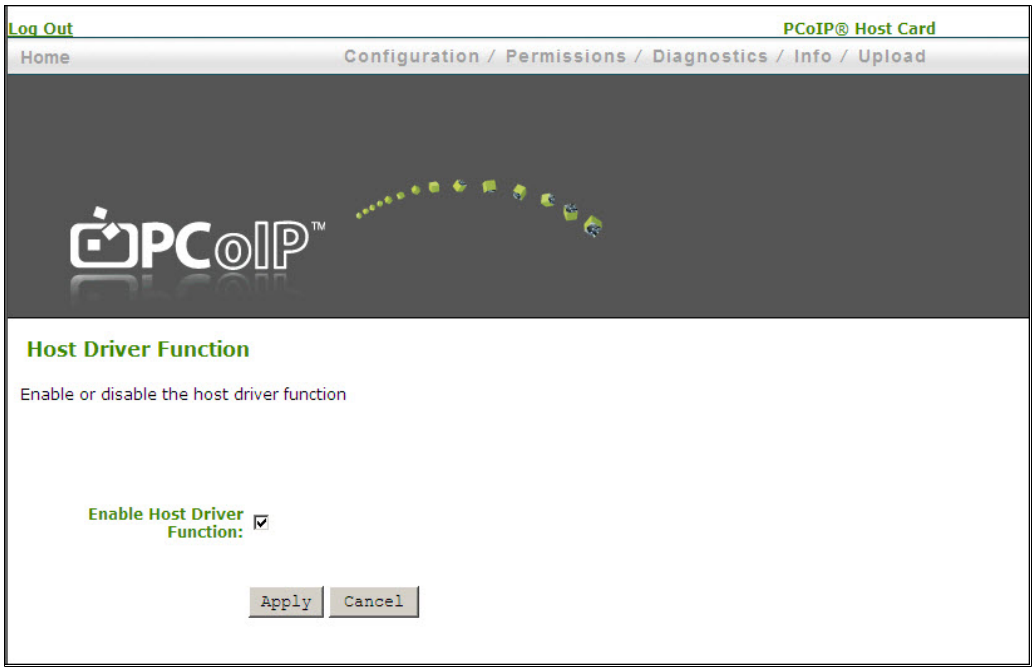


Figure 4-29: Administrative Web Interface Host Driver Function Page

The **Enable Host Driver Function** checkbox enables a PCoIP host driver function to allow the following enhanced features:

- Host PC lock when a session is terminated
- Local cursor and keyboard
- Network interface for Wake on LAN function
- Host and client network parameters view
- Session statistics view
- Update of the host topology settings with the client settings

4.17 Configuring the NTP Parameters

The **Time** page lets you configure the Network Time Protocol (NTP) parameters to allow the event logs of the host and client to be time-stamped based on NTP time.

Note: To simplify system troubleshooting, set the NTP parameters to allow correlation of user events to the relevant diagnostic event log entries.

Figure 4-30: Administrative Web Interface Time Page

Table 4-17: 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	Choose if the NTP host is identified by IP address or by FQDN. If NTP is disabled, this field is not required and is not editable. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose: • **IP Address**: Shows the NTP Host IP address • **FQDN**: Shows the NTP Host DNS name
NTP Host Port	Lets you configure the NTP port number.
NTP Query Interval	Lets you configure the query interval. The first field is for the interval period and the second field is for the time unit in Minute(s), Hour(s), Day(s), and Week(s).
Time Zone	Lets you select the local time zone.
Enable Daylight Savings Time	Enable or disable the automatic adjustment for daylight savings time.

4.18 Updating the Password for a Device

The **Password** page lets you update the local administrative password for the device. The password can be a maximum of 20 characters. Some PCoIP devices have password protection disabled by default. The **Password** page is not available on these devices. Password protection can be enabled through the PCoIP Management Console for these devices.

Note: This parameter affects the web interface and the local OSD GUI. Take care when updating the client password as the client may become unusable if the password is lost.

Figure 4-31: Administrative Web Interface Change Password Page

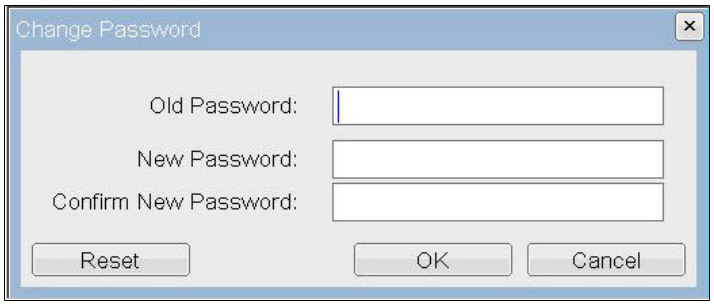


Figure 4-32: OSD Change Password Page

Table 4-18: 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 web interface and the local OSD GUI.
Confirm New Password	This field must match the **New Password** field for the change to take place.
Reset	If, for some reason, the client password is lost, you can click the **Reset** button to request a response code from their client vendor. The challenge code can be sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password. Note: Contact the client vendor for more information when an authorized password reset is required. This option is not available through the Administrative Web Interface. It is only available through the OSD.

4.19 Resetting the Parameters to Factory Default Values

The **Reset Parameters** button lets you reset configuration and permissions to factory default values stored in flash. When you click this button, a prompt appears for confirmation. This is to prevent accidental resets.

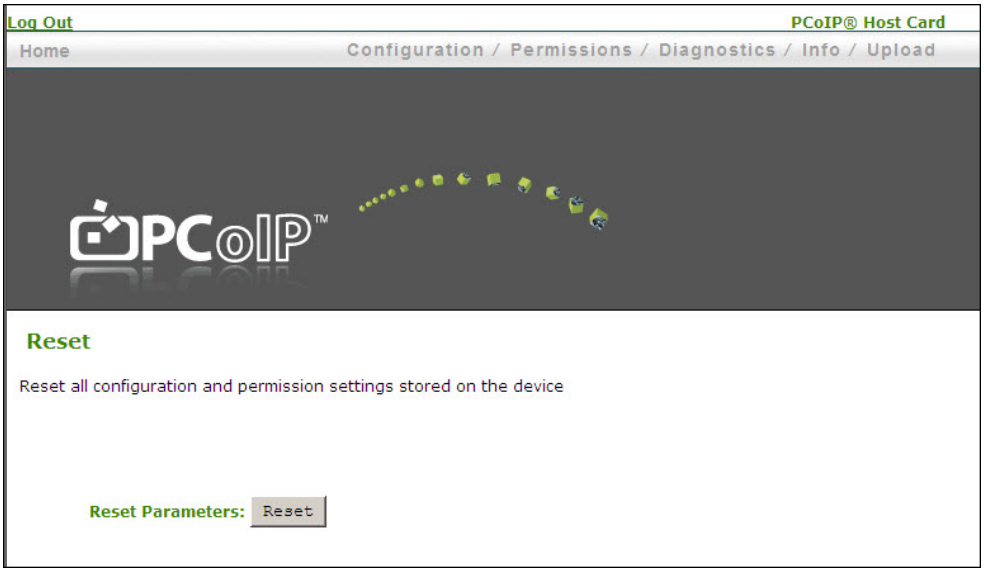


Figure 4-33: Administrative Web Interface Reset Page

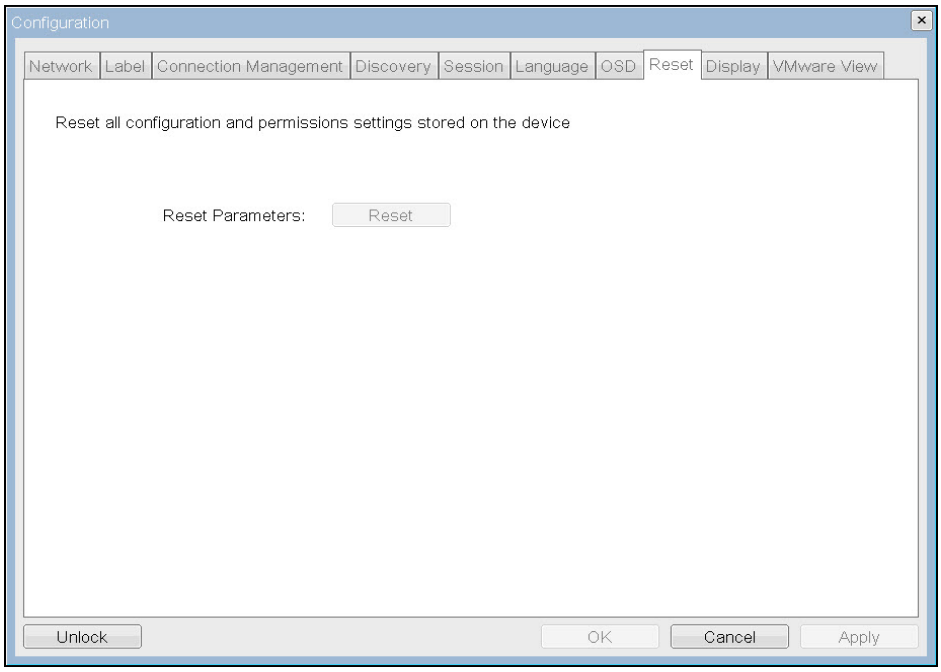


Figure 4-34: OSD Reset Page

4.20 Configuring the EDID Override Mode

The **Display** page lets you enable the EDID override mode.

Note: This function is only available through the OSD.

Under normal operation, the GPU in the host computer queries the monitor 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 connecting through some KVM devices. In this case, configure the client to report default EDID information to the GPU by enabling the display override mode.

The client provides EDID information to the host GPU that indicates the following resolutions are supported:

- 800x600 @60 Hz
- 1280x800 @60 Hz
- 1280x960 @60Hz
- 1280x1024 @60 Hz (native resolution advertised)
- 1600x1200 @60 Hz
- 1680x1050 @60 Hz
- 1920x1080 @60 Hz
- 1920x1200 @60 Hz

WARNING: Enabling display override forces default-monitor display information that may not comply with the connected monitor and results in a blank monitor. Only enable display override when there is no valid EDID information and monitor display characteristics are understood.

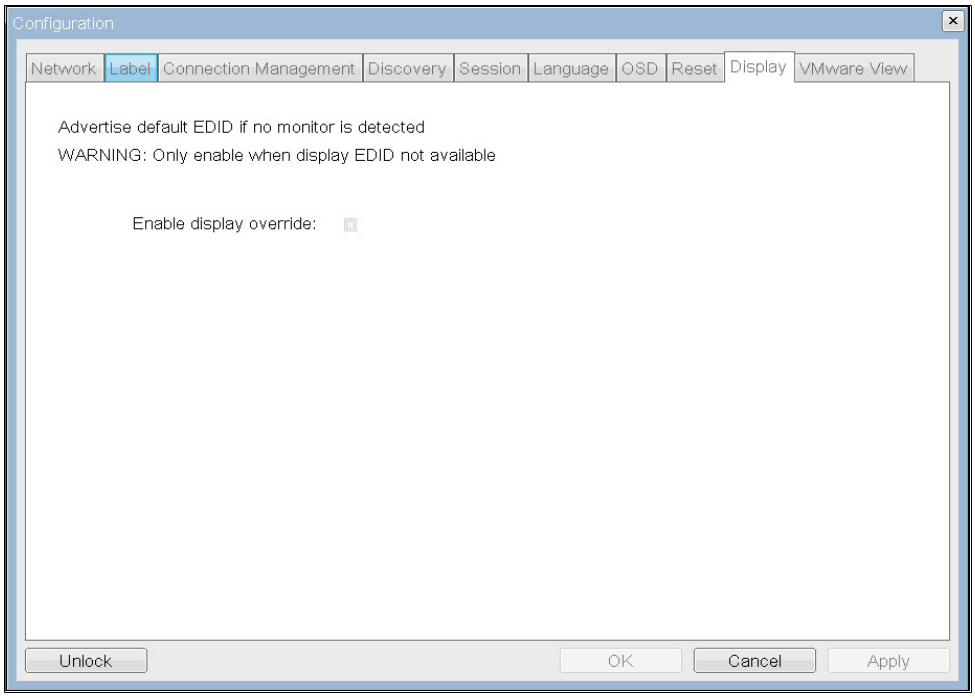


Figure 4-35: OSD Display Page

4.21 Enabling or Disabling the OSD Configuration Menus

You can enable or disable the PCoIP zero client configuration menus through the PCoIP Management Console (you must have release 1.4.x or higher). Disabling the OSD **Configuration** menu means that to configure the device, you must use the Administrative Web Interface (if enabled) or the PCoIP Management Console.

To enable or disable the OSD **Configuration** menu for a client:

1. Log in to the PCoIP Management Console.
2. Edit the profile for the group or device.
3. Select the **OSD Configuration** option.
4. Check the **Set in Profile** option for the **Hidden Menu Entries**.
5. Check any of the available options that you want to hide in the OSD.
6. Click **Save**.
7. Apply the profile to the zero client.
8. Restart the zero client.

Note: For these changes to take effect, you must restart the device.

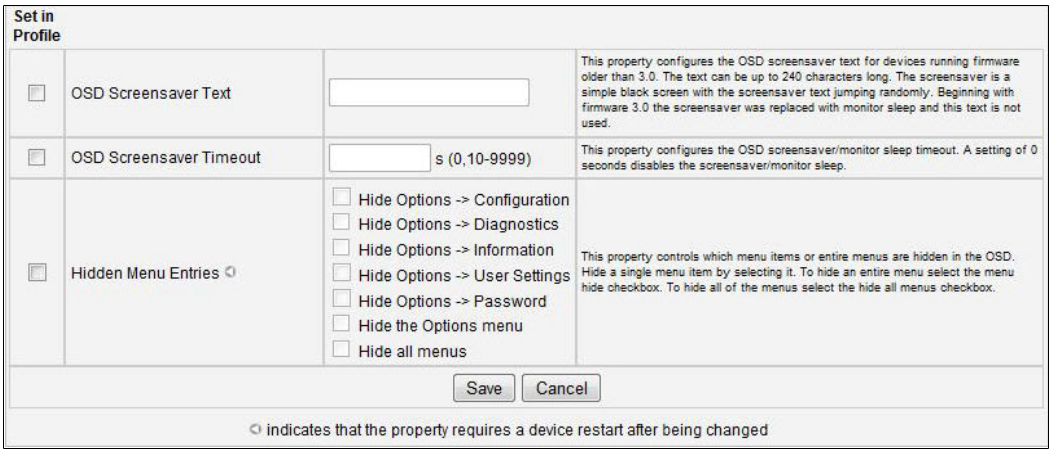


Figure 4-36: OSD Configuration – Hidden Menu Entries Option

4.22 Enabling or Disabling the Web Server

You can enable or disable the zero client and PCoIP host card web interfaces through the PCoIP Management Console (release 1.4.x or higher).

To enable or disable the zero client or host card web interfaces:

1. Log in to the PCoIP Management Console.
2. Edit the profile for the group or device.
3. Click **Security Configuration**, and then **Edit Properties**.
4. Check the **Set in Profile** option for **Enable Web Interface**.
5. Set the option to:
   - **True**: enable the web interface for the device or group of devices.
   - **False**: disable the web interface for the device or group of devices.
3. Click **Save**.
4. Apply the profile to the zero client or host.
5. For this option to take effect, restart the zero client or host.

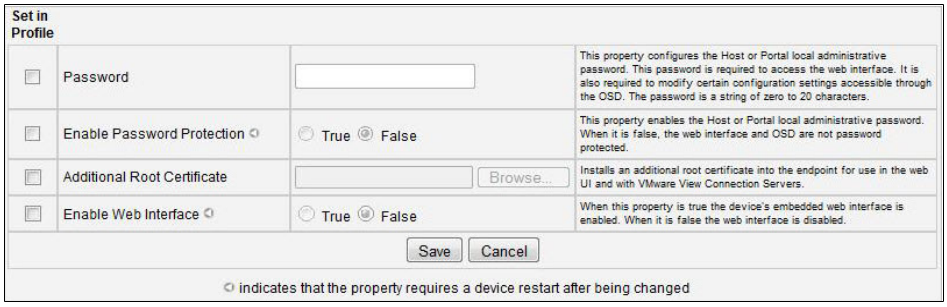


Figure 4-37: Security Configuration – Enable Web Interface Option

5 Setting up the User Permissions

The **Permissions** menu on the Administrative Web Interface has options that let you configure parameters for the USB, Audio, and Power for the device.

Note: There are no corresponding Permissions options for the OSD.

5.1 Specifying USB Devices

The **USB** page lets you specify authorized and unauthorized USB devices. It is divided into two sections: Authorized Devices ("white list") and Unauthorized Devices ("black list"). Devices are authorized or unauthorized 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.

- 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.

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

1. Unauthorized Vendor ID/Product ID
2. Authorized Vendor ID/Product ID
3. Unauthorized Device Class/Sub Class/Protocol
4. Authorized Device Class/Sub Class/Protocol

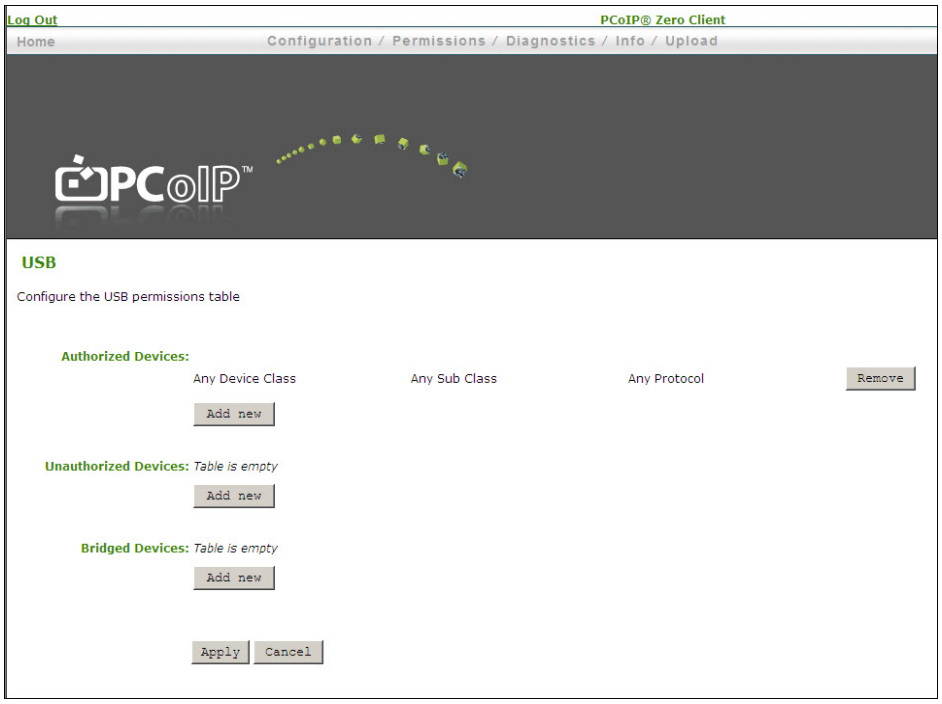


Figure 5-1: Administrative Web Interface USB Page

Table 5-1: USB Page Parameters

Parameter	Description
Authorized Devices	Specify the authorized USB devices for the host and client. Two buttons let you customize this "white list": **Add New:** add a new device or device group to the list. This allows USB authorization by ID or Class: • **ID**: The USB device is authorized by its Vendor ID and Product ID • **Class**: The USB device is authorized by Device Class, Sub Class, and Protocol **Remove:** Delete a rule for a device or device group from the list.
Unauthorized Devices	Specify the unauthorized USB devices for the host or client. **Add New:** add a new device or device group to the list. This allows USB devices to be unauthorized by ID or Class: • **ID**: The USB device is unauthorized by its Vendor ID and Product ID • **Class**: The USB device is unauthorized by Device Class, Sub Class, and Protocol **Remove:** Delete a rule for a device or device group from the list.
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. 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. **Add New:** Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID. **Remove:** Delete a rule for a device or device group from the list.

The following table summarizes the USB authorization entry type and the associated data fields. Two buttons let you customize this "white list":

Table 5-2: USB Device Authorized/Unauthorized Entry Types

Entry Type	Required Fields	Hexadecimal Value	Comments
ID	VID	O-FFFF	
	PID	0-FFFF	
Class	Device Class	0-FF; asterisk (*) indicates any device sub-classes	Drop-down menu provides human readable translations of the known device classes
	Sub Class	0-FF; asterisk (*) indicates any device sub-classes	Drop-down menu provides human readable translations of the known device sub-classes.
	Protocol	0-FF; askterisk (*) indicates any protocal authorized	Drop-down menu provides human readable translations of the known protocols.

5.2 Configuring the Audio Parameters

You can configure the audio parameters from the **Initial Setup** page when you start your first session. For subsequent sessions, use the **Audio** page 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**.

Table 5-3: Audio Page Parameters

Parameter	Description
Enable HD Audio	Enables audio support on host or client. If the **Enable HD Audio** option is disabled on the host, the audio hardware is not available for the OS to enumerate.
Enable Microsoft Windows Vista 64-bit Mode	Enables 64-bit mode on host. This mode should only be used for Windows Vista 64-bit and Windows 7 64-bit versions. This option is only available on a host. It does not appear on the client. Warning: Do NOT use this mode with Windows XP 64 or 32-bit operating systems. You do not have to enable the 64-bit mode for Linux 64-bit operating systems. Linux kernels should be compiled with the latest PCoIP audio CODEC support.

5.3 Setting up the Client's Power-off Permissions

The **Power** page lets you configure the power-off permissions of the client.

Note: The **Power** page is only available on the client. It is not available on the host.

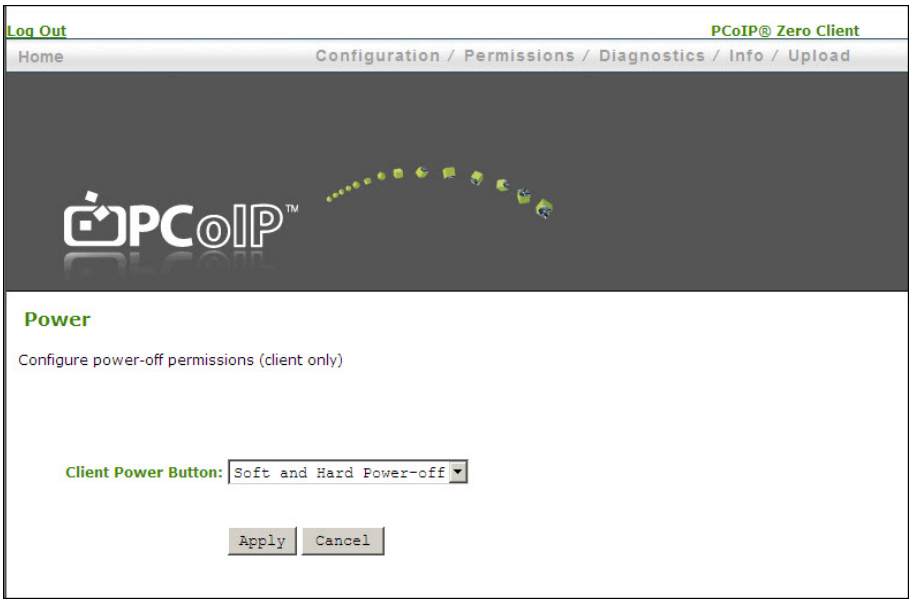


Figure 5-2: Administrative Web Interface Power Page

Table 5-4: Power Page Parameter

Parameter	Description
Client Power Button	The drop-down menu lets you configure the client **Power** button functionality. Options include: • Power-off not permitted • Soft power-off only soft limit • Hard power-off only • Soft and hard power-off

6 Using the Diagnostic Tools

The **Diagnostic** menu contains links to windows with run-time information and functions that may be useful for troubleshooting.

Note: The Diagnostic options in the OSD are a subset of those available through the Administrative Web Interface.

6.1 Viewing and Clearing Event Log Messages

The **Event Log** page lets you view and clear event log messages from the host or client. The web interface lets you change the log filter setting on the device, which controls which messages are put in the log. When you set the filter to “terse”, the device logs terse messages.

The **Event Log** page also lets you enable and define syslog as a way of collecting and reporting your events that meets the IETF standard for logging program messages.

6.1.1 Syslog Features

- allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.
- provides devices that would otherwise be unable to communicate a way to notify administrators of problems or performance.
- can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages.
- is supported by a wide variety of devices and receivers across multiple platforms.
- can be used to integrate log data from many different types of systems into a central repository.
- has messages that:
  - refer to a facility (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0, ... , local7) .
  - are assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug) by the sender of the message.
- lets you direct messages to various local devices (console), files (/var/log/) or remote syslog daemons.

  Note: Take care when you update the configuration as omitting or misdirecting message facilities or levels can cause important messages to be ignored by syslog or overlooked by the administrator.

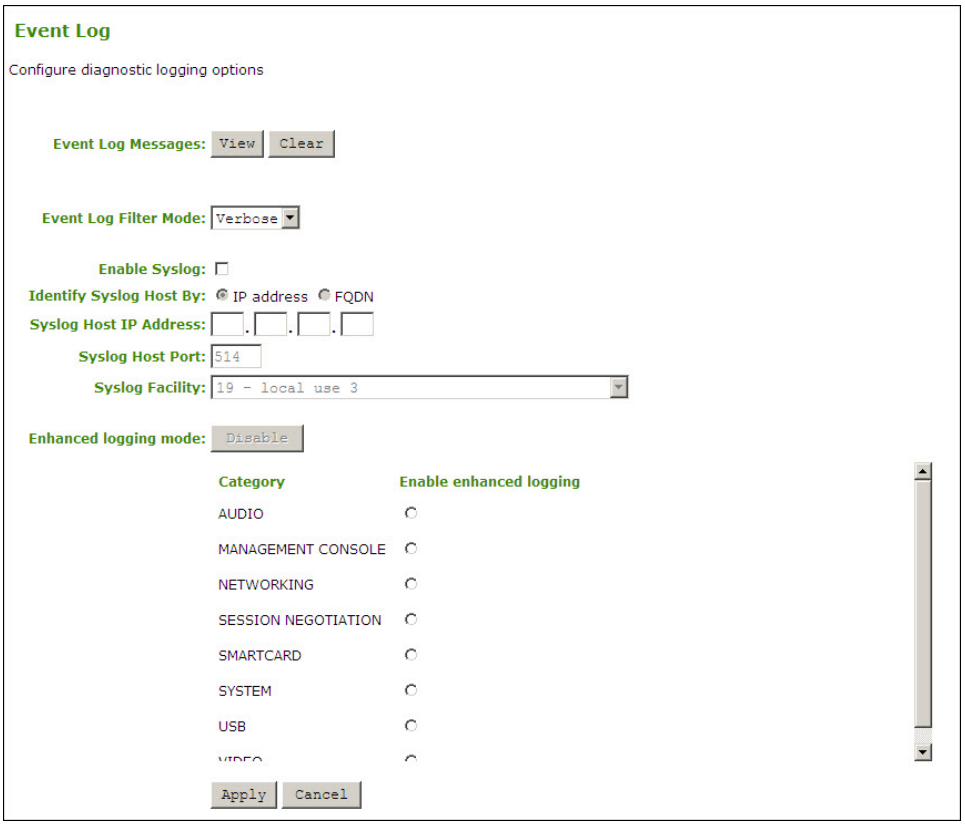


Figure 6-1: Administrative Web Interface Event Log Page

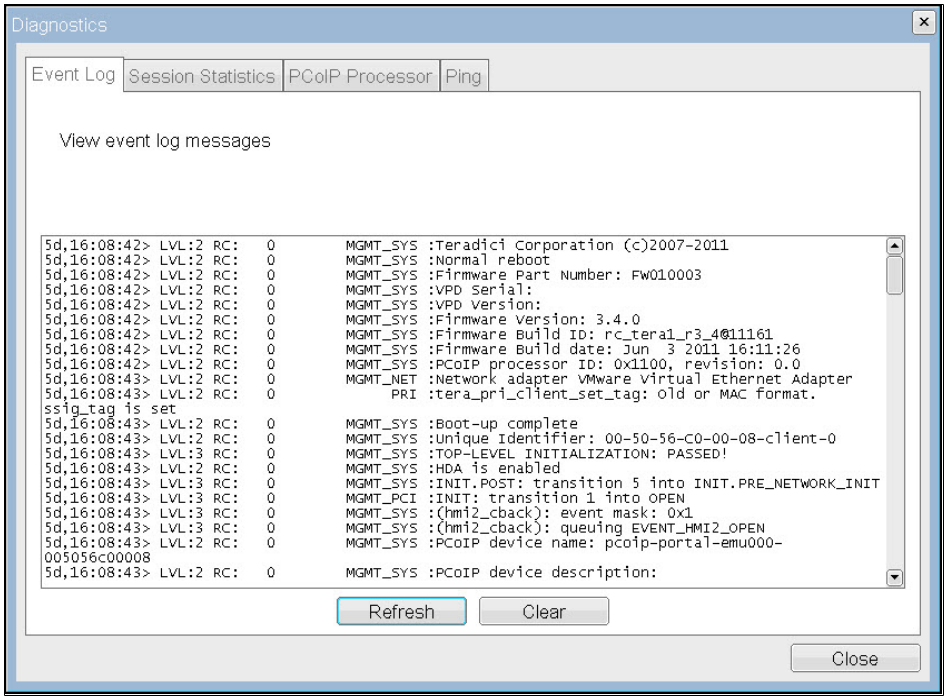


Figure 6-2: OSD Event Log Page

Table 6-1: Event Log 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. **Clear:** Click to delete all event log messages stored on the device.
Event Log Filter Mode	Click the pull-down menu to filter the event logs. Options include: • Verbose (this is the default setting) • Terse
Enable Syslog	Enable the syslog standard for your event logs. If syslog is enabled, you must configure the remaining fields (if disabled, they are non-editable).
Identify Syslog Host By	Choose if the syslog host is identified by IP address or by FQDN. If you enter an invalid IP address or DNS name, a message appears to prompt you to correct it. The parameter depends on which method you choose: • **IP Address:** The IP address for the syslog host • **FQDN:** The DNS name of the syslog host
Syslog Host IP Address / Syslog Host DNS name	If you set the **Identify Syslog Host By** field to: • **IP Address**: Enter the IP address for the syslog host • **FQDN:** Enter the DNS name for the syslog host
Syslog Host Port	Lets you configure the syslog port number.
Syslog Facility	The facility is a number attached to every syslog message used to categorize the source of the syslog messages. The facility is part of the standard syslog header and can be interpreted by all syslog servers. Enter a facility to suit your logging needs. For example, you could configure: • zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 Note: The default facility is set to “19 – local use 3”. Cisco routers default to “23 – local use 7”.
Enhanced logging mode	This field lets you collect enhanced log messages for one of the following categories. Click **Disable** to turn off the enhanced logging mode. • Audio • Management Console • Networking • Session Negotiation • Smart Card • System • USB • Video Note: You can only enable enhanced logging for one of the above categories at one time.

6.2 Controlling the Device Session

The **Session Control** page lets you view information about a device and can manually disconnect or connect a session.

Figure 6-3: Administrative Web Interface Session Control Page

Table 6-2: Session Control Page Parameters

Parameter	Description
Connection State	This field displays the current state for the session. Options include: • Disconnected • Connection Pending • Connected Two buttons appear below the **Connection State** field: • **Connect:** If the connection state is **Disconnected**, click this button to initiate a PCoIP session between the client and its peer device. If the connection state is **Connection Pending** or **Connected**, this button is disabled. Note: This option is only available on the client. It is disabled on the host. • **Disconnect:** If the connection state is **Connected** or **Connection Pending**, click this button to end the PCoIP session for the device. If the connection state is **Disconnected**, this button is disabled.
Peer IP/MAC Address	**Peer IP Address:** Displays the IP address for the peer device. When not in session, this field is blank. **Peer MAC Address:** Displays the MAC address of the peer device. When not in session, this field is blank.

6.3 Viewing PCoIP Protocol Statistics

The **Session Statistics** page lets you view current statistics when a session is active. If a session is not active, you can view the statistics from the last session.

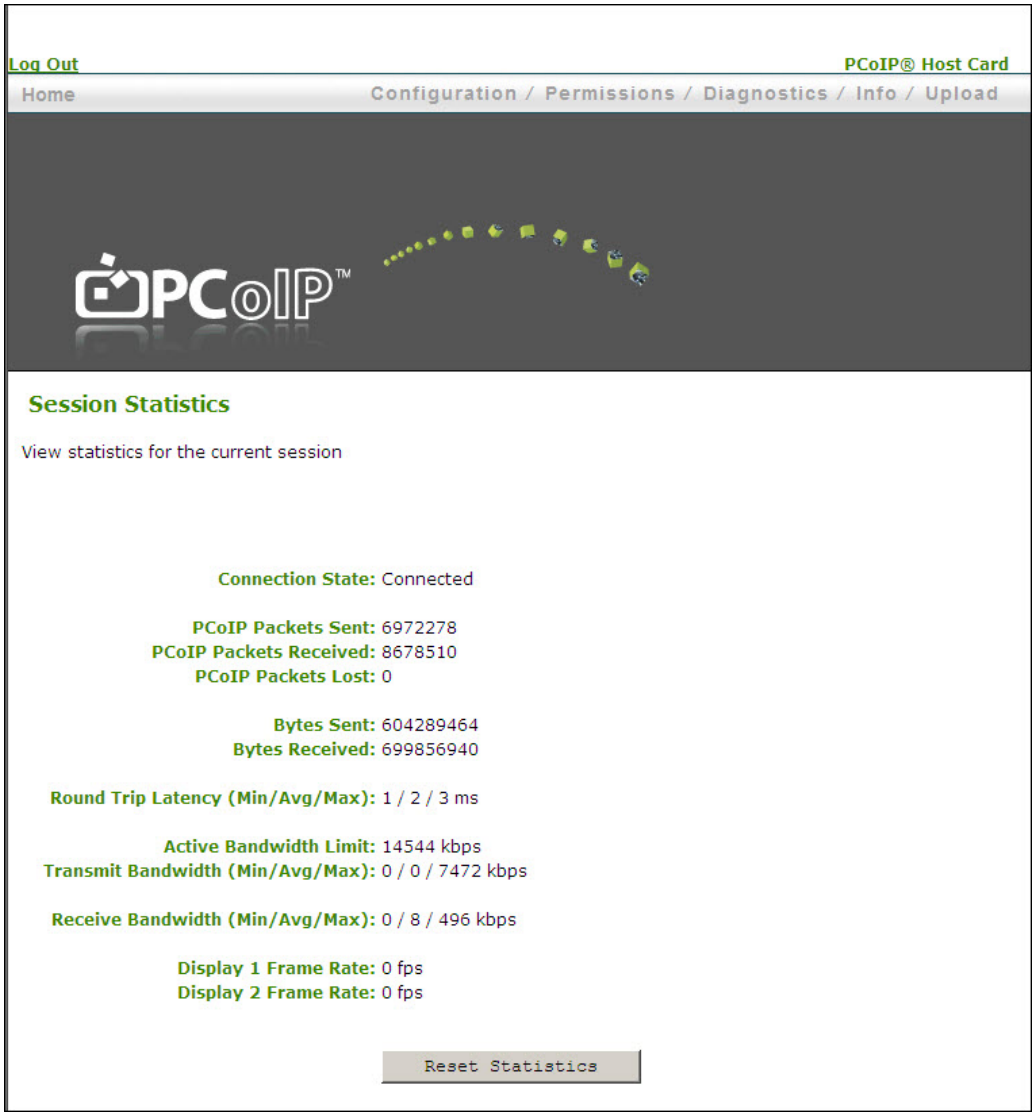


Figure 6-4: Administrative Web Interface Session Statistics Page

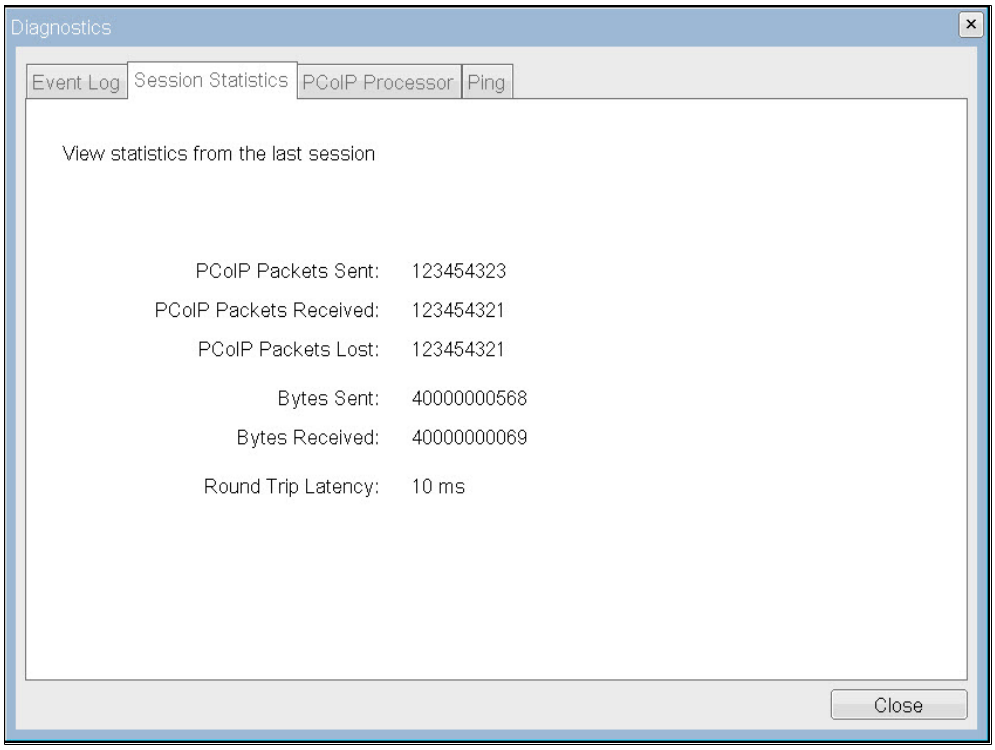


Figure 6-5: OSD Session Statistics Page

Table 6-3: Session Statistics Page Parameters

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Values include: • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
PCoIP Packets Statistics	**PCoIP Packets Sent:** The total number of PCoIP packets sent in the current/last session. **PCoIP Packets Received:** The total number of PCoIP packets received in the current/last session. **PCoIP Packets Lost:** The total number of PCoIP packets lost in the current/last session.
Bytes Statistics	**Bytes Sent:** The total number of bytes sent in the current/last session. **Bytes Received:** The total number of bytes received in the current/last session.
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system (for example, host to client and then back to host) and network latency in milliseconds (+/- 1 ms).
Bandwidth Statistics	**Active Bandwidth Limit:** The maximum amount of network traffic the Tera1x00 processor may currently generate. The value is derived from the configured bandwidth parameters and the current (or last) network congestion levels. **Transmit Bandwidth:** The minimum, average, and maximum traffic transmitted by the Tera1x00 processor. **Receive Bandwidth:** The minimum, average, and maximum traffic received by the Tera1x00 processor.
Display Frame Rate	**Display 1 Frame Rate:** The frame rate for Display 1, reported in frames per second (fps). **Display 2 Frame Rate:** The frame rate for Display 2, reported in frames per second (fps).
Reset Statistics	Click this button to reset the statistic information on this page. Note: The **Reset Statistics** button also resets the statistics reported in the **Home** page.

6.4 Working with the Host Information and Power State

The **Host CPU** page lets you view and modify the host information. You can view the current state of the power as well as power off the host.

Note: The **Host CPU** page is only available on a host. It is not available on the client.

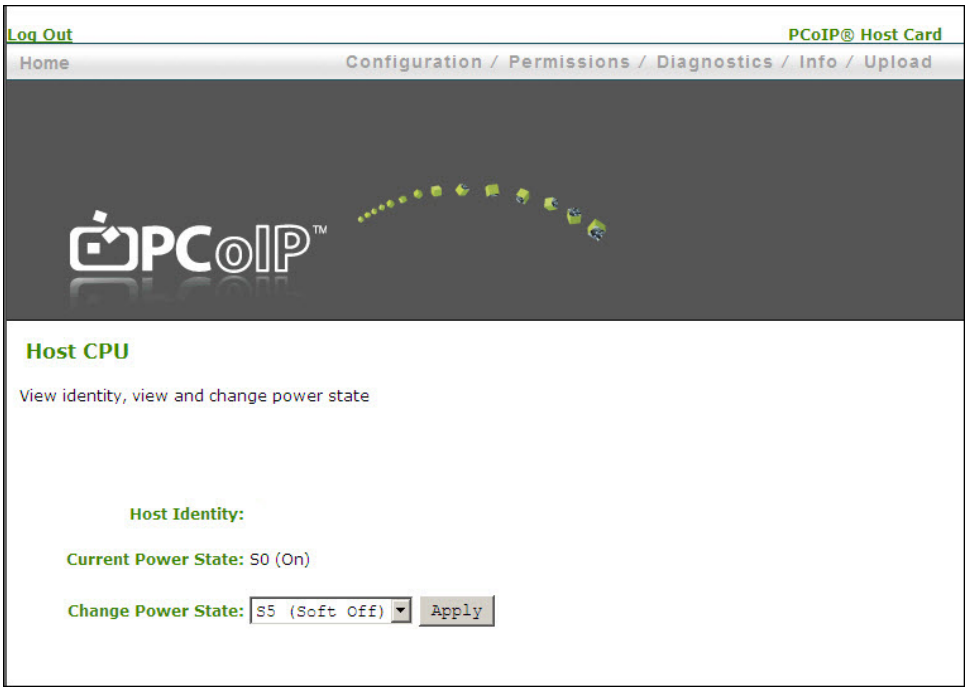


Figure 6-6: Administrative Web Interface Host CPU Page

Table 6-4: Host CPU Page Parameters

Parameters	Description
Host Identity	The identity string of the host computer (if data is available).
Current Power State	The current state of the power for the host (e.g., "on").
Change Power State	Power off the host as: • S5 (Soft Off) • S5 (Hard Off) Note: To use this feature, the host must have compatible hardware architecture.

6.5 Generating an Audio Test Tone from the Client

The **Audio** page lets you generate an audio test tone from the client.

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. It is unavailable on the host.

Figure 6-7: Administrative Web Interface Audio Diagnostics Page

6.6 Viewing a Test Pattern on the Client's Display

The **Display** page lets you initiate and view a test pattern on the client's display.

Note: The test pattern only appears on the **Display** page when the client is not in a PCoIP session. It is not available on the host. If you click **Start** when the client is in session, an error message appears.

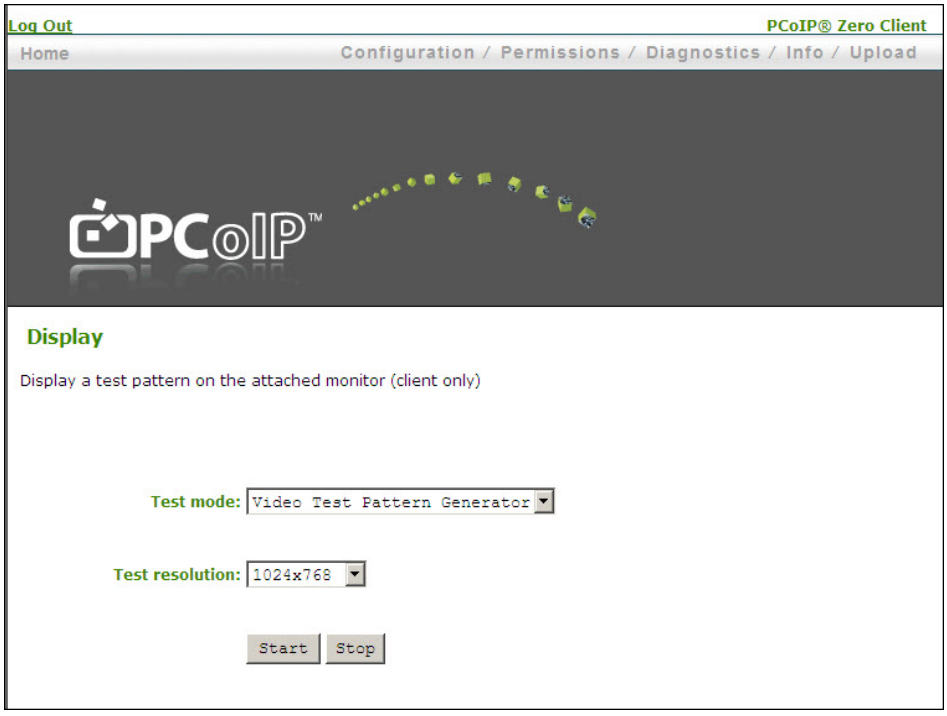


Figure 6-8: Administrative Web Interface Display Page

Table 6-5: Display Page Parameters

Parameters	Description
Test mode	Set the type of test pattern for the attached monitor(s) as: • Video Test Pattern Generator • Pseudo Random Bitstream
Test resolution	Set the test pattern resolution as: • 1024x768 • 1280x1024 • 1600x1200 • 1920x1200
Start/Stop	Click **Start** to begin the test pattern. Click **Stop** to stop the test.

6.7 Resetting the Device Processor

The **PCoIP Processor** page lets you reset the host or client and view the uptime of the client PCoIP processor since the last boot.

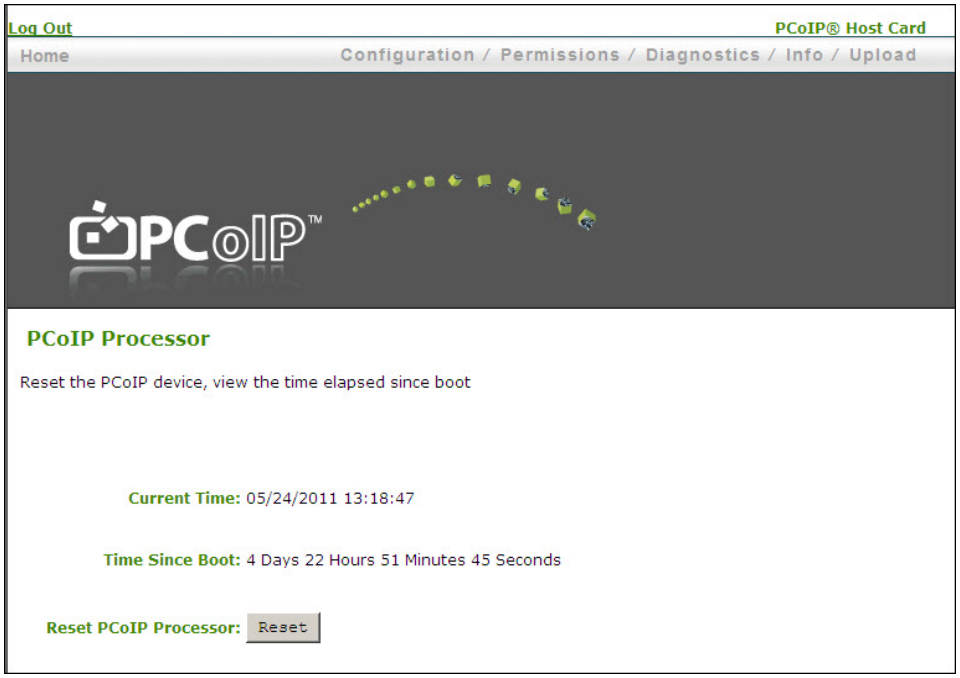


Figure 6-9: Administrative Web Interface PCoIP Processor Page

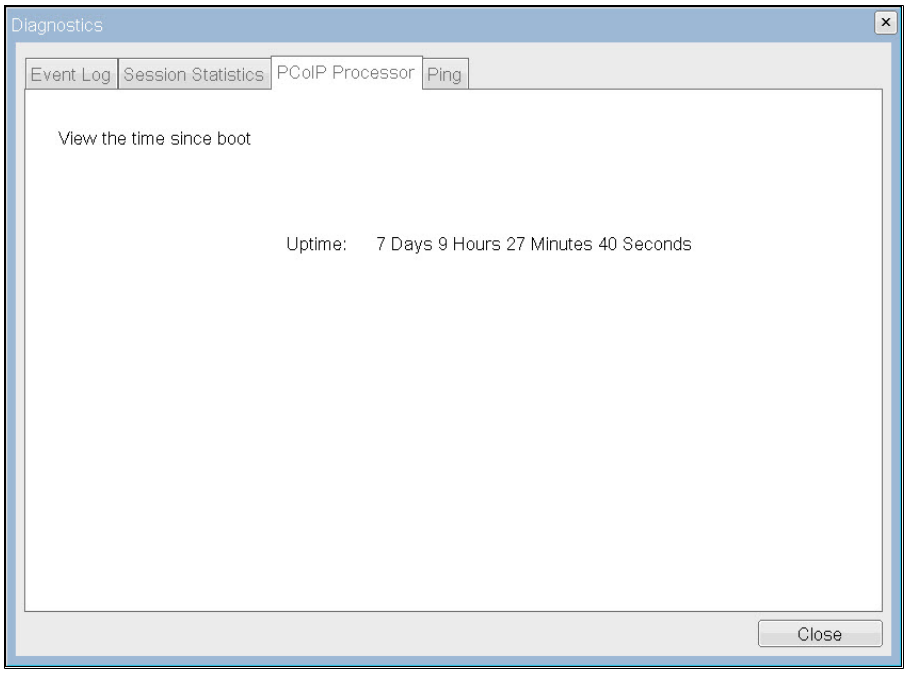


Figure 6-10: OSD PCoIP Processor Page

Table 6-6: PCoIP Processor Page Statistics

Statistics	Description
Current Time	The current time. This feature requires that NTP be enabled and configured. For details about configuring the NTP settings, see section 4.17.
Time Since Boot (Uptime)	View the uptime of the PCoIP processor since the last boot.
Reset PCoIP Processor	Click this button to reset the host or client.

6.8 Determining if a Device is Reachable

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 higher force the “do not fragment flag” in the ping command, you can also use this feature to determine the maximum MTU size.

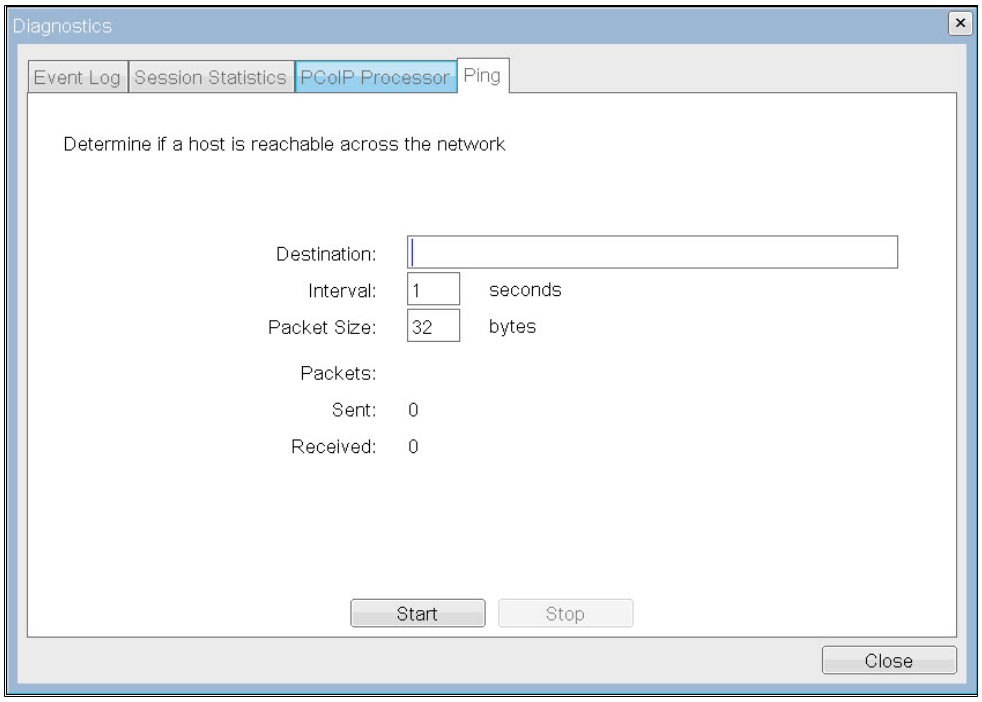


Figure 6-11: OSD Ping Page

Table 6-7: Ping Page Parameters

Parameter	Description
Destination	IP address or 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

7 Viewing Device Information

The **Information** page lets you see details about the device. The Administrative Web Interface shows version, VPD, and attached device information. The OSD lets you view the device version information.

7.1 Viewing the Version Information

The **Version** page lets you view the hardware and firmware version details for a device.

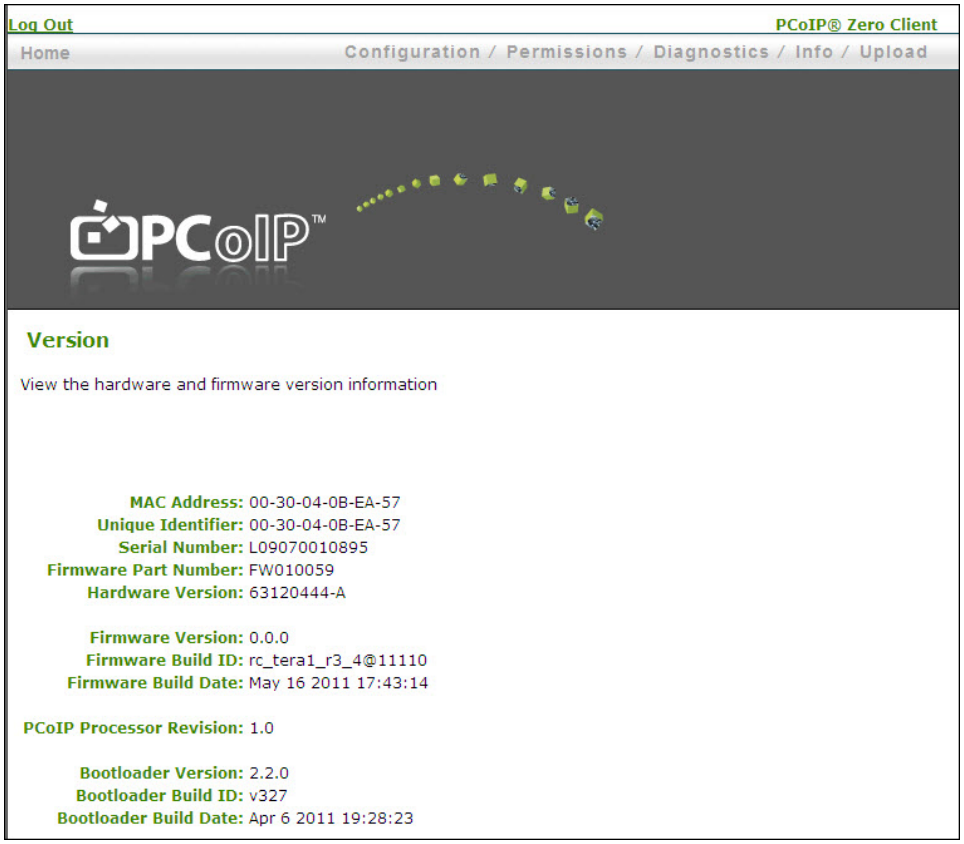


Figure 7-1: Administrative Web Interface Version Page

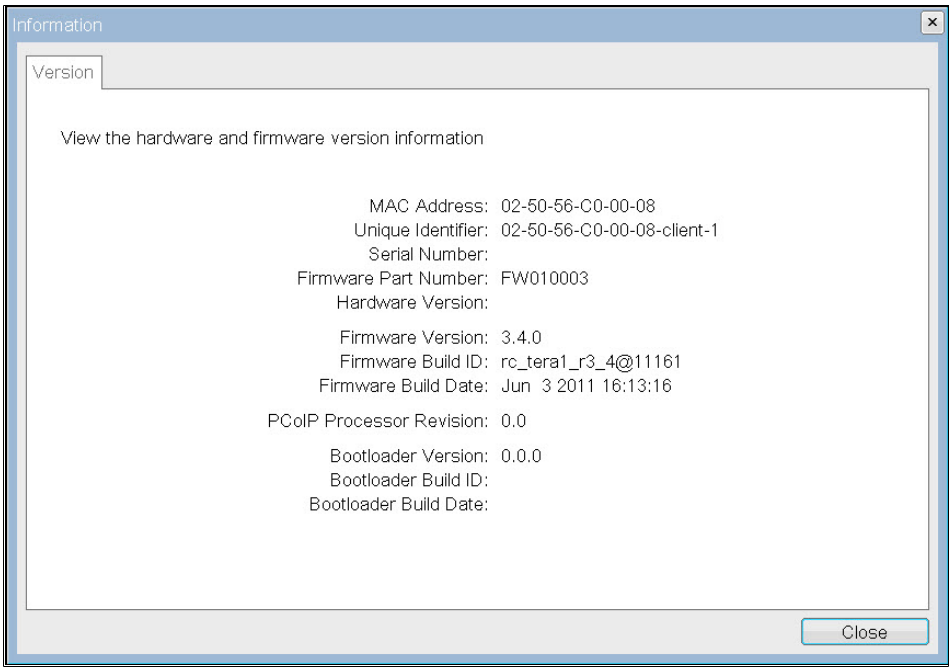


Figure 7-2: OSD Version Page

Table 7-1: OSD Version Page Parameters

Parameters	Description
VPD Information	**(Vital Product Data)**: Information provisioned by the factory to uniquely identify each host or client: • **MAC Address:** Host/client unique MAC address • **Unique Identifier:** Host/client unique identifier • **Serial Number:** Host/client unique serial number • **Firmware Part Number:** Part number of the current firmware • **Hardware Version:** Host/client hardware version number
Firmware Information	This information reflects the current firmware details: • **Firmware Version:** Version of the current firmware • **Firmware Build ID:** Revision code of the current firmware • **Firmware Build Date:** Build date for the current firmware
PCoIP Processor Revision	The silicon revision of the PCoIP processor. Revision B of the silicon is denoted by a 1.0.
Bootloader Information	This information reflects the current firmware bootloader details: • **Boatloader Version:** Version of the current bootloader • **Bootloader Build ID:** Revision code of the current bootloader • **Bootloader Build Date:** Build date of the current bootloader

7.2 Viewing the Attached Devices

The **Attached Devices** page lets you see the type and status of the monitor and USB hardware currently attached to the client.

Note: The attached USB device information is only available on a client. It is not available on a host.

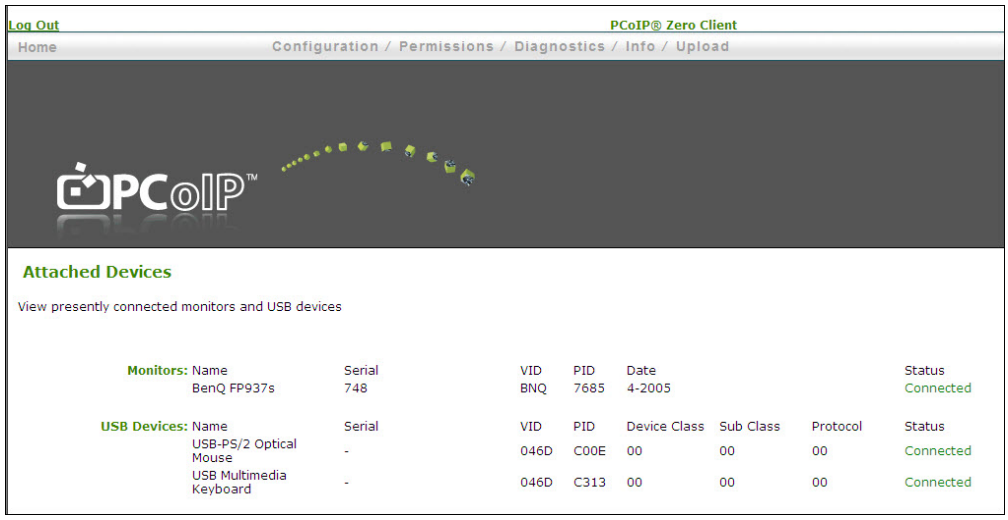


Figure 7-3: Administrative Web Interface Attached Devices Page

Table 7-2: Attached Devices Page Statistics

Statistic	Description
Monitors	This section displays the name, serial number, vendor identification (VID), product identification (PID), date, and status of the monitor attached to each port. The first line is for monitor 1. The second line is for monitor 2. Note: This option is available on a client and is available on the host when in a PCoIP session.
USB Devices	This section displays the name, serial number, vendor identification (VID), product identification (PID), device class, sub class, protocol, and status of the USB device attached to each port. The first line is for the first USB port. The second line is for the second port, and so on.
USB Device Status	Status options include: • **Not Connected**: No device is connected. • **Standalone**: The device is detected outside of a PCoIP session. • **Not Initialized**: The device is detected in a PCoIP session but the host controller has not initialized the device. • **Failed Authorized**: The device is detected in a PCoIP session but is not authorized. (For more information, see the Authorized section on the **USB Permissions** page in section 5.1). • **Locally Connected**: The device is detected and authorized but locally terminated in a PCoIP session (for example, a local cursor). • **Connected**: The device is detected and authorized in a PCoIP session.

8 Uploading to the Device

You can use the options in this menu to upload new firmware or an OSD logo to a device. These options are not available through the OSD.

8.1 Uploading Firmware to the Device

The **Firmware** page lets you upload a new firmware build to the host or client.

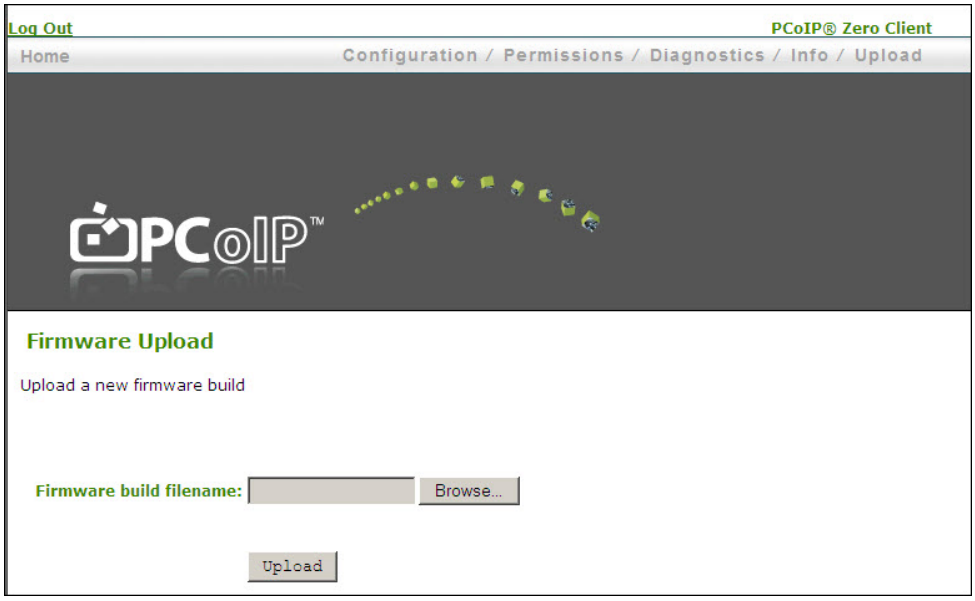


Figure 8-1: Administrative Web Interface Firmware Page

Table 8-1: Firmware 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 (that is, 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 web interface prompts you to confirm this action to avoid accidental uploads. Note: It's important to ensure that both the host and client have the same firmware release.

8.1.1 Firmware Upload Process Example:

1. Ensure the host PC or workstation is in an idle state (that is, all applications must be closed).
2. Log into the host Administrative Web Interface (with a password if enabled).

3. From the **Firmware Upload** page, browse to the firmware ".all" file (for example, "tera1x00_rel1-9-v175.all").
4. Click **Open**.
5. Click **Upload**.
6. Click **OK** to confirm that you want to proceed with the upload. When the firmware upload completes, the message "Success Flash successfully programmed! You must reset the device for the changes to take effect" appears.
7. Click **Reset**. The message "The PCoIP processor will reset on the next host system restart; your changes will take effect then. Are you sure you want to proceed?" appears.
8. Click **OK**.
9. Repeat steps 2 through 6 on the client but do not restart the client.
10. Restart the host PC or workstation.
11. Reset the client.
12. Start the PCoIP session as per usual.

8.2 Uploading a Logo to the Device

The **OSD Logo** page lets you upload an image to the device. This image appears on the **Connect** page of the local GUI On Screen Display (OSD).

The **VMware View Advanced** page includes an option "Use OSD Logo for View Banner," which lets you configure whether the OSD logo appears on the **View** login screen instead of the View banner. For more details, see section 4.6.

Note: This option is only available on the client. It is not available on the host.

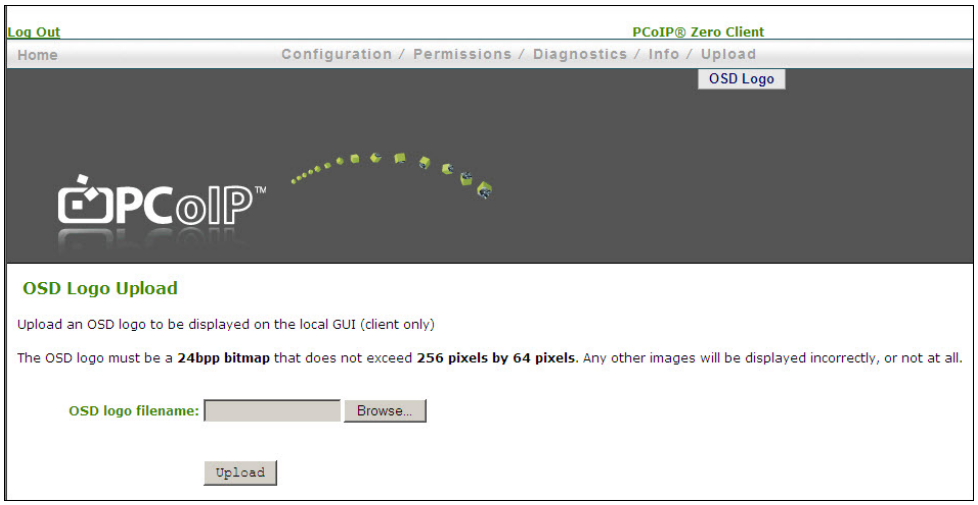


Figure 8-2: Administrative Web Interface OSD Logo Upload Page (Client)

Table 8-2: OSD Logo Page Parameters

Parameter	Description
OSD logo filename	Specify the filename of the logo image you want to upload. You can browse to the target file using the **Browse** button. The file must be accessible to the web browser (that is, on a local or accessible network drive). The 24-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.

8.2.1 OSD Logo Upload Process Example

1. From the **OSD Logo** webpage, click **Browse** to locate the target logo file.
2. Click **Open**.
3. Click **Upload**. The message "Are you sure? This will upload a new logo for the local GUI. This operation may take a few minutes." appears.
4. Click **OK**.
5. Wait for the OSD logo upload to finish. A message appears to advise if the upload was successful.
6. Reset the client.

9 Configuring the User Settings

The **User Settings** page lets you access tabs to define the mouse and keyboard settings, PCoIP protocol image quality, as well as the display topology.

9.1 Configuring the Mouse Settings

The **Mouse** page lets you change the mouse cursor speed settings for the OSD sessions.

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 for Windows User Guide* (TER0810001) for more details). This function is only available through the OSD. It is not available in the Administrative Web Interface.

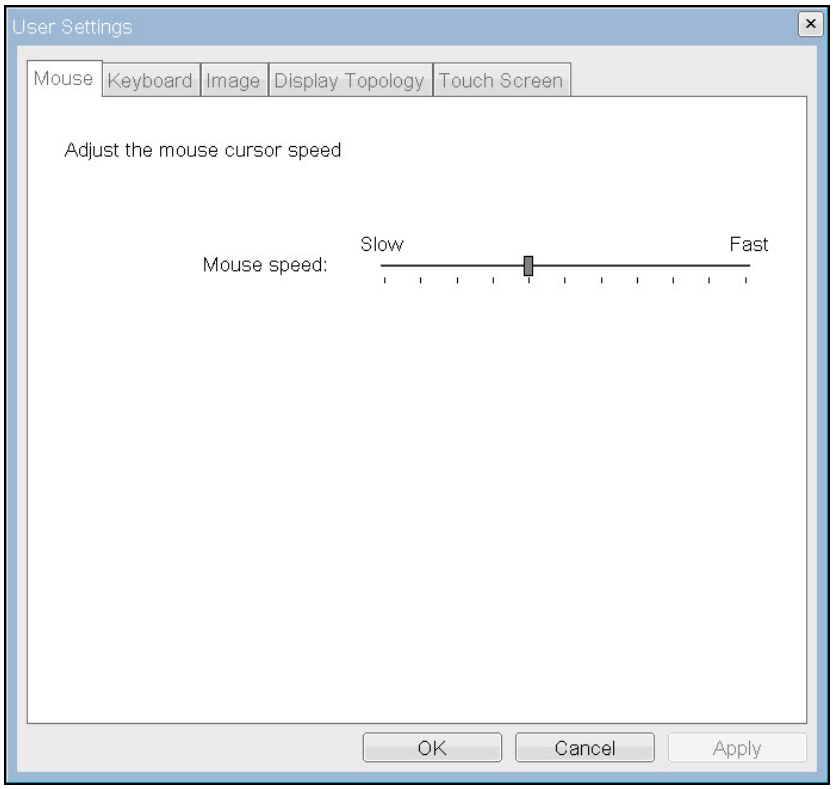


Figure 9-1: OSD Mouse Page

Table 9-1: Mouse Page Parameters

Parameter	Description
Mouse Speed	Configure the speed of the mouse cursor. Note: You can also configure the mouse speed through the PCoIP host software. See the *PCoIP Host Software for Windows User Guide* (TER0810001) for more details.

9.2 Changing the Keyboard Repeat Settings

The **Keyboard** page lets you change the keyboard repeat settings for the OSD session.

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 for Windows User Guide* (TER0810001) for more details). This setting is only available through the OSD. It does not appear on the Administration Web Interface.

You can also configure the keyboard repeat settings through the PCoIP host software. See the *PCoIP Host Software for Windows User Guide* (TER0810001) for more details

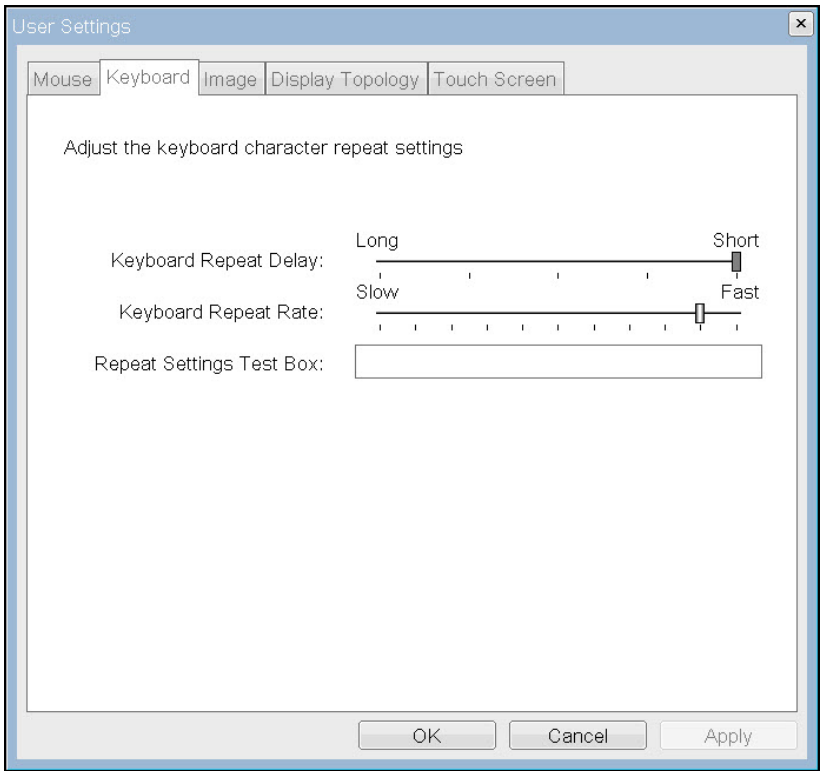


Figure 9-2: OSD Keyboard Page

Table 9-2: Keyboard Page Parameters

Parameter	Description
Keyboard Repeat Delay	Lets users configure the client keyboard repeat delay.
Keyboard Repeat Rate	Lets users configure the client keyboard repeat rate.
Repeat Settings Test Box	Lets users test the chosen keyboard settings.

9.3 Adjusting the Image Quality from the OSD

For more information about adjusting the image quality, see section 4.14.

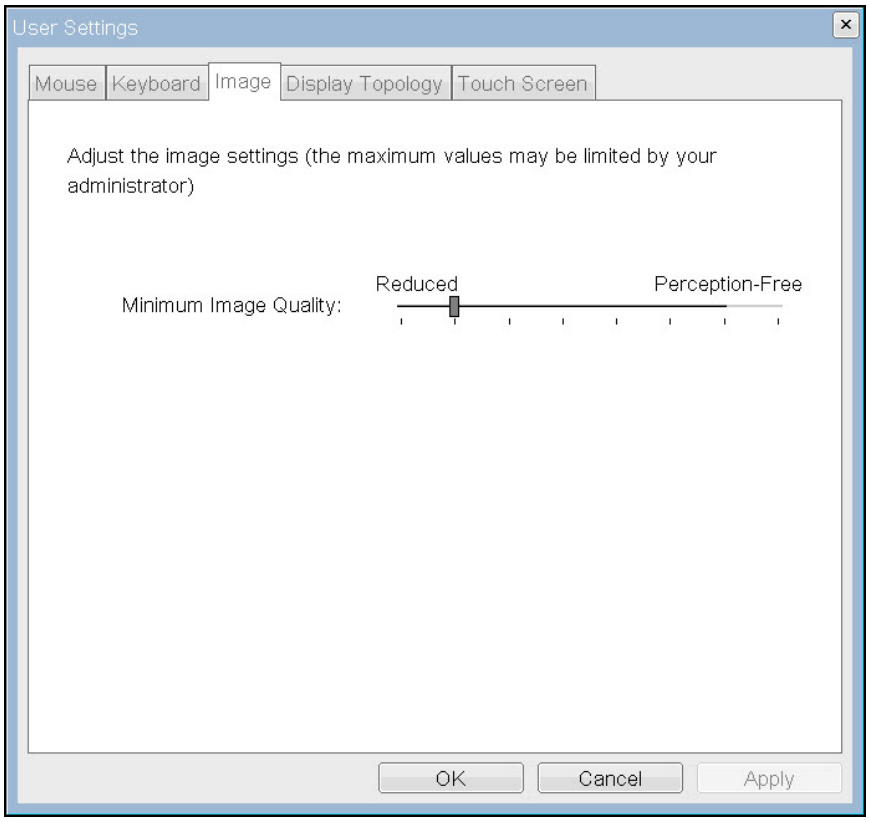


Figure 9-3: OSD Image Page

9.4 Configuring the Display Topology

The **Display Topology** page lets users change a display's position, rotation, and resolution for a PCoIP session. To apply the display topology feature to a PCoIP session between a zero client and a Virtual Machine (VM), you must have VMware View 4.5 or later.

To apply the display topology feature to a PCoIP session between a zero client and a PCoIP host, you must have the PCoIP host software installed on the host. See the *PCoIP Host Software for Windows User Guide* (TER0810001) for details.

Notes:

The **Display Topology** tab has no corresponding menu in the Administration Web Interface.

For details about the Display Topology feature for a PCoIP session between a host card and a zero client, see the *PCoIP Host Software for Windows User Guide* (TER0810001).

Always change the display topology settings using the **Display Topology** tab on the zero client OSD->Options->User Settings interface. Do not try to change these settings using the Windows Display Settings in a virtual machine when using VMware View.

To view the **Display Topology** page:

1. From the OSD, click **Options**, and then **User Settings**.
2. Click the **Display Topology** tab.

The **Display Topology** page appears.

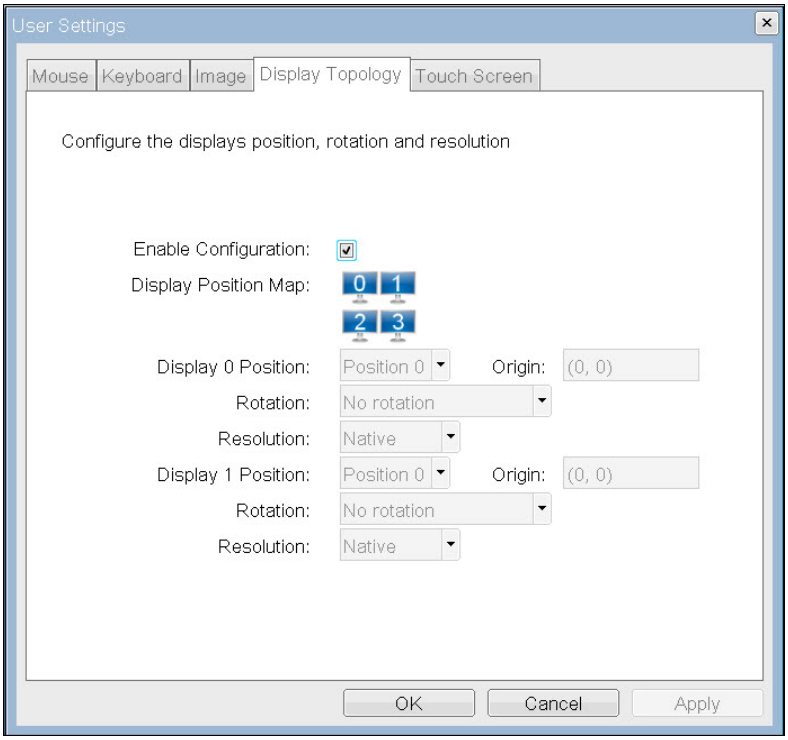


Figure 9-4: Display Topology Page

Table 9-3: Display Topology Page Parameters

Parameter	Description
Enable Configuration	When enabled, the device can be configured with display position, rotation and resolution settings. The settings are saved when you click **Apply** or **OK** and are applied when the device is reset.
Display Position Map	The display position map consists of four possible display positions. A maximum of two displays can be enabled at the same time.
Display Position	When two displays are connected to the zero client DVI-1 and DVI-2 connectors the user must configure how the monitors are arranged. The **Display Position** settings support this. Using these settings the user can arrange the displays horizontally or vertically. For example, to arrange the displays: • Horizontally with the monitor connected to DVI-1 on the left: Set Display 0 Position and Display 1 Position to Position 0 and 1, or Position 2 and 3, respectively. • Horizontally with the monitor connected to DVI-2 on the left: Set Display 0 Position and Display 1 Position to Position 1 and 0, or Position 3 and 2, respectively.
Origin	Origin is a read-only parameter that indicates the (x,y) position of the upper left-hand corner of a display.
Rotation	You can configure the orientation of a display to: • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	The display resolution can be configured for a PCoIP session between a virtual machine or host and a zero client. The zero client detects the supported display resolutions of the monitor and populates them to the drop-down menu. By default, the display's native resolution is used.

9.5 Configuring the Touch Screen

The **Touch Screen** page lets you configure and calibrate certain aspects for an attached Elo TouchSystems touch screen display.

Note: The **Touch Screen** page is only available through the OSD. It is not available from the Administrative Web Interface.

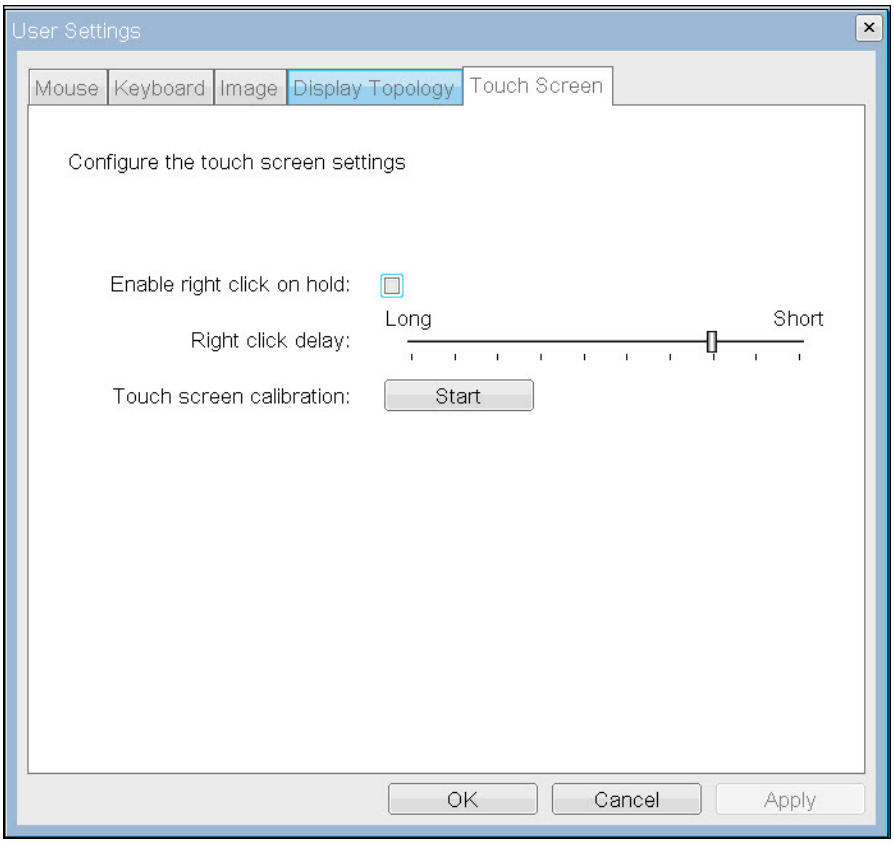


Figure 9-5: OSD Touch Screen Page

Table 9-4: 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. To test the calibration, run your finger along the monitor and ensure that the cursor follows it. If it is not successful, the calibration program automatically restarts. Once calibrated, the coordinates are stored in flash. To manually start the calibration program, from the OSD **Touch Screen** page, click **Start**. Follow the onscreen prompts.

9.5.1 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. You can manually recalibrate the screen as required through the OSD **Touch Screen** page.

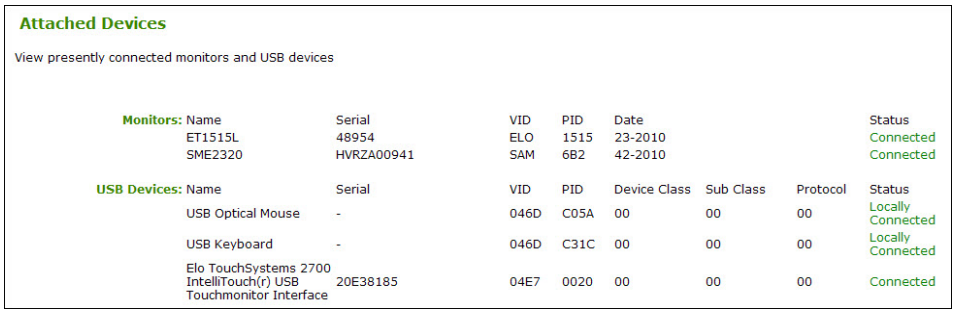
5. Follow the touch screen prompts. You can test the calibration with your finger (the cursor should move with your finger). If the screen is not properly calibrated, the system automatically restarts the calibration program.

9.5.2 Setting up the Touch Screen as a Bridged Device

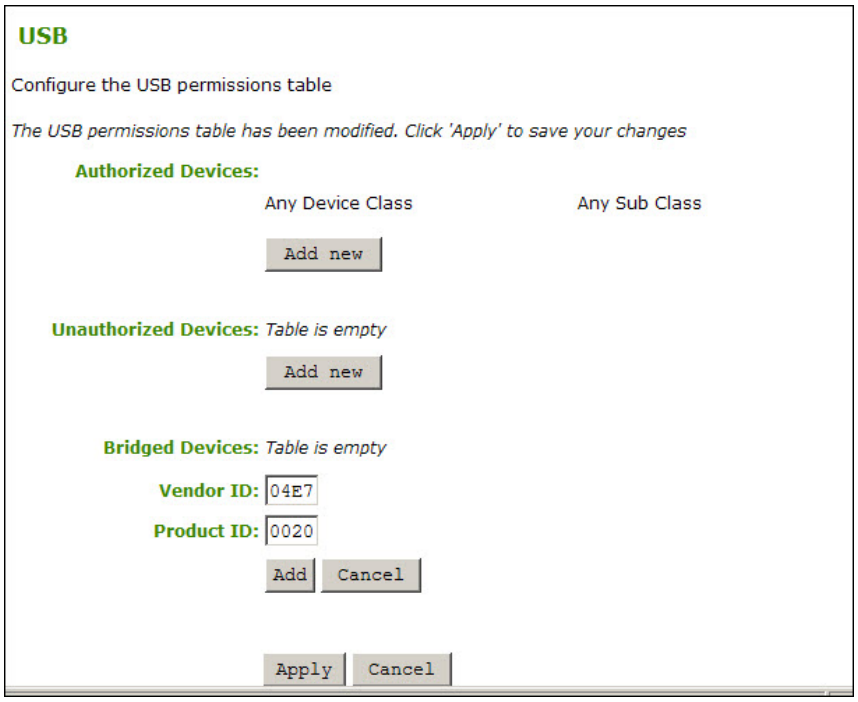
Note: This procedure is optional and only necessary if you want the touch screen to be set up as a bridged device.

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.



5. From the **Permissions** menu, click **USB** to display the **USB** page.
6. In the **Bridged Devices** area, click **Add New**.



7. Enter the Vendor ID and Product ID for the touch screen, and the 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.

9.5.3 Configuring the Zero Client to Automatically Login to 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. Login to the Administrative Web Interface.
2. From the **Configuration** menu, select **VMware Advanced** page.
3. Select the **Enable Auto-Logon** checkbox.
4. Fill out the user credentials, and then click **Apply**.

10 About the Overlay Windows

Overlay pages display pertinent information to users during a PCoIP session. These pages occasionally appear on top of the user's remote session.

Status overlay pages show network, USB device, and monitor statuses as icons and text. The overlays have simple animation and appear when the status changes (that is, the network connection is lost or an unauthorized USB device is plugged in).

10.1 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.

Figure 10-1: 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. For more information see the **Enable Peer Loss Overlay** setting described in section 4.10.

10.2 USB Device Not Authorized Overlay

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

Figure 10-2: USB Device Not Authorized Overlay

10.3 USB Over Current Notice Overlay

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

Figure 10-3: USB Over Current Notice Overlay

10.4 Half Duplex Overlay

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

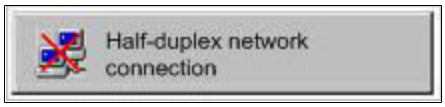


Figure 10-4: Half Duplex Overlay

10.5 Video Source Overlays

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

- When no video source is connected to the host, an 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.

Figure 10-5: No Source Signal Overlay

Note: This message can be triggered by the host going into display power save mode.

- When a video source to the host does not correspond to the video port used on the client, an 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."

Figure 10-6: Source Signal on Other Port Overlay

11 Using Smart Cards with PCoIP Zero Clients

Firmware 3.2.0 and higher provides pre-session and in-session smart-card support for PCoIP zero clients connecting to VMware View 4.5 or higher virtual desktops.

Note: Before using smart cards with PCoIP zero clients, be sure that the smart card infrastructure is properly deployed. For example, the **Smart Card Authentication** setting is properly configured in View Connection Server 4.5, the "PCoIP Smart Card Component" is enabled during View Agent 4.5 installation, and the Smart Card middle is deployed. For details about deploying a View infrastructure with smart card enabled, see *View Manager Administration Guide*.

11.1 Smart Card Requirements

When used with VMware View 4.5 or higher with smart card authentication enabled, the firmware securely transfers the attached smart-card information to the View Connection Server for authentication and Single Sign-On (SSO) of a user prior to session establishment.

11.1.1 Virtual Desktop Environment

- VMware View 4.5 or higher
- VM Guest OS: Windows XP, Vista, Win7 with VMware View Agent PCoIP smart card component installed
- PCoIP zero client firmware 3.2.0 or newer (where those smart cards supported in later firmware releases are indicated as such)

11.1.2 Supported USB Card Readers

- SCR331
- SCR3310
- SCR3310/v2.0
- SCR333
- SCR335
- Dell Smartcard USB keyboard SK3205
- Cherry SmartBoard keyboard
- OmniKey 3021
- Castle EZM110CU
- Peripheral Dynamics PT-3901
- GemPC Twin HWP108765C
- PC Twin HWP108760D
- Alcor AU9540-GBS (built into selected Samsung zero clients)
- HP KUS0133 Smart Card Keyboard
- Castles Technology EZM110PU (built into selected ClearCube zero clients)

- HID Omnikey 5321
- Gemalto PC USB-SW

11.1.3 CAC Smart Card Properties

For smart card authentication and SSO, the smart card must meet one of these specifications:

- GSC-IS v2.0 and v2.1 cards (firmware 3.2.0 or higher)
- PIV transitional cards (firmware 3.4.0 or higher)
- PIV endpoint cards (firmware 3.4.0 or higher)

11.1.4 .Net Smart Card Properties

For smart card authentication and SSO, the smart card must be a Gemalto .Net card (firmware 3.4.1 or higher).

11.1.5 Communication Protocol

The communication protocol between the smart card and the reader is referred to as T=X, where X is 0 or 1. Firmware 3.2.0 and higher supports T=0. Firmware 3.4.0 and higher supports T=1.

11.1.6 Card Certificate Requirements

A certificate on the smart card must have these properties:

- Key usage set to digital signature
- Subject Common Name and/or Subject Alternative Name (Other Name) is set
- Enhanced Key Usage includes Client Authentication and/or Smart Card Logon
- Key Length is no larger than 2048 bits

11.1.7 Tested Smart Card Models

Teradici has tested these specific smart card models:

Smart Card Model	Tested for Firmware Release (or higher)
Axalto Cryptoflex .NET	3.4.1
Gemalto Cyberflex Access 64K V2c	3.4.0
Gemalto TOP DL GX4 144K DI	3.4.0
Gemalto TOP DM GX4 72K (FIPS)	3.4.0
GnD SmartCafe Expert 144K DI v3.2	3.4.0
Oberthur CosmopolIC 64K V5.2	3.2.0
Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application	3.4.0
Oberthur ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3.2	3.4.0
Oberthur ID-One Cosmo v7.0 128K	3.4.0

Note: Other readers may be supported. For the most up-to-date list, see Knowledge Base item #15134-299 from the Teradici Support Site.

11.2 Using a Smart Card to Connect to a VMware View Brokered Session

In addition to configuring the **Prefer GSC-IS** setting (which only applies to PIV Transitional cards), the following steps describe how to connect a PCoIP session from a zero client with smart card to a virtual machine brokered by VMware View 4.5 or higher.

Note: For details about establishing a PCoIP session without using a Smart Card from a zero client to a Virtual Machine brokered by VMware View, see *Using PCoIP Zero Clients with VMware View 4 User Guide* (TER0904005).

To set up a connection between the smart card and the PCoIP zero client:

1. From the **VMware View Login** page, click **Connect**.

   This establishes a session from a PCoIP zero client with a smart card to a virtual machine brokered by VMware View.

   An "Accessing Smart Card" message appears followed by the "Connecting" message. If this message doesn't appear, the zero client did not detect the smart card reader.

Figure 11-1: Accessing the Smart Card Message

   If the smart card contains multiple certificates, the "Select Certificate" prompt appears. If the smart card contains only one certificate, this prompt does not appear and the certificate is automatically selected.

Figure 11-2: Select Certificate Prompt

2. Click **Details**.

   The following window appears with the certificate details:

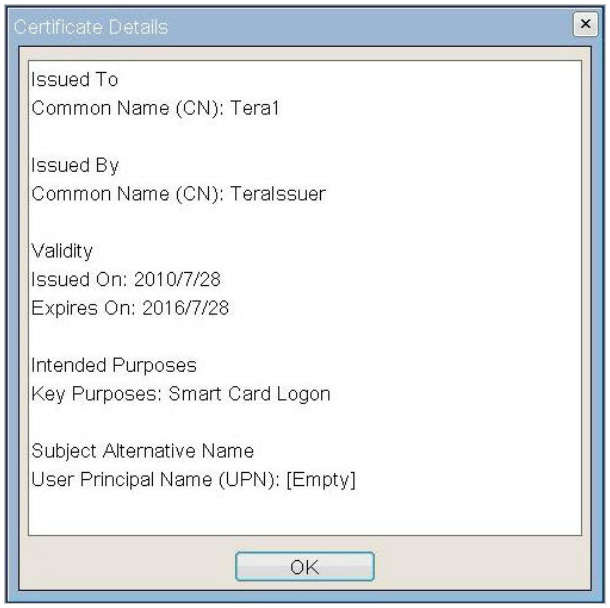


Figure 11-3: Certificate Details Window

3. After selecting a certificate from the dialog, enter the PIN information in the **Smart Card Holder Verification** window.

Figure 11-4: Smart Card Holder Verification Window

4. When the PIN is successfully authenticated, a window appears that lists VM(s) or VM pool(s) entitled to the user. Select the VM or VM pool to which you want to connect.

   A PCoIP session is established to the virtual machine, and the PIN is automatically transferred to Windows for SSO.

   .

Appendix A: Usage Examples Overview

This section provides detailed examples to help you determine how best to configure your own devices.

A.1 Peer-to-Peer Direct Connection Example

This example provides an overview of how to configure a client and host for a direct connection. That is, without the use of a Connection Management server or the **Enable Host Discovery** option.

The following IP and MAC addresses are used for this example:

- **Client: IP Address**: 192.168.42.149, MAC: 00-1C-59-00-05-0E
- **Host: IP Address**: 192.168.50.107, MAC: 00-1C-8A-03-00-CA

Note: For a peer-to-peer direct connection, you must know the IP and MAC addresses for the client and host.

A.1.1 Configuring the Client Peer-to-Peer Operation

Note: This example uses the Administrative Web Interface for configuring the client for peer-to-peer operation. You can also use the OSD to configure the client.

To configure the client for peer-to-peer direct connection:

1. Open the Administrative Web Interface by using an Internet browser to open the client IP address, e.g., https://192.168.42.149
2. Login to the client Administrative Web Interface (with password if enabled).
3. Select the **Discovery** page from the **Configuration** menu.
4. Ensure **Enable Host Discovery** is not enabled.

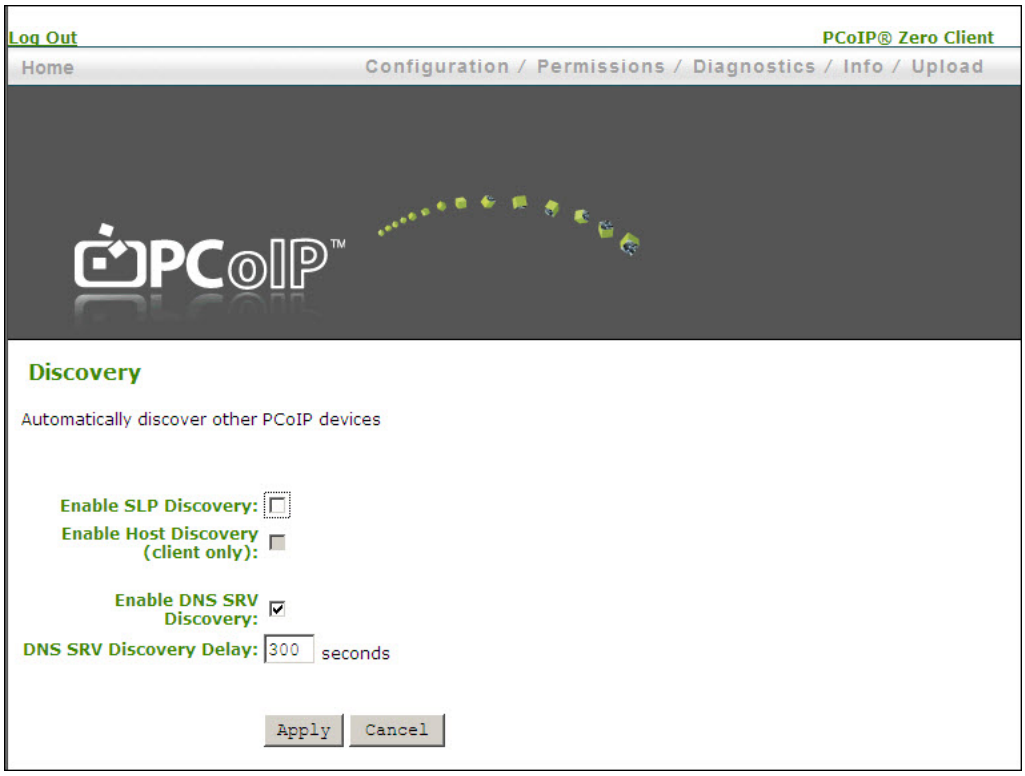


Figure 12-1: Client Discovery Configuration (Enable SLP Discovery disabled)

5. Select the **Connection Management** page from the **Configuration** menu.

Figure 12-2: Client Connection Management Peer-to-Peer Configuration

6. Ensure **Enable Connection Management** is not selected.
7. Select the **Session** page from the **Configuration** menu.

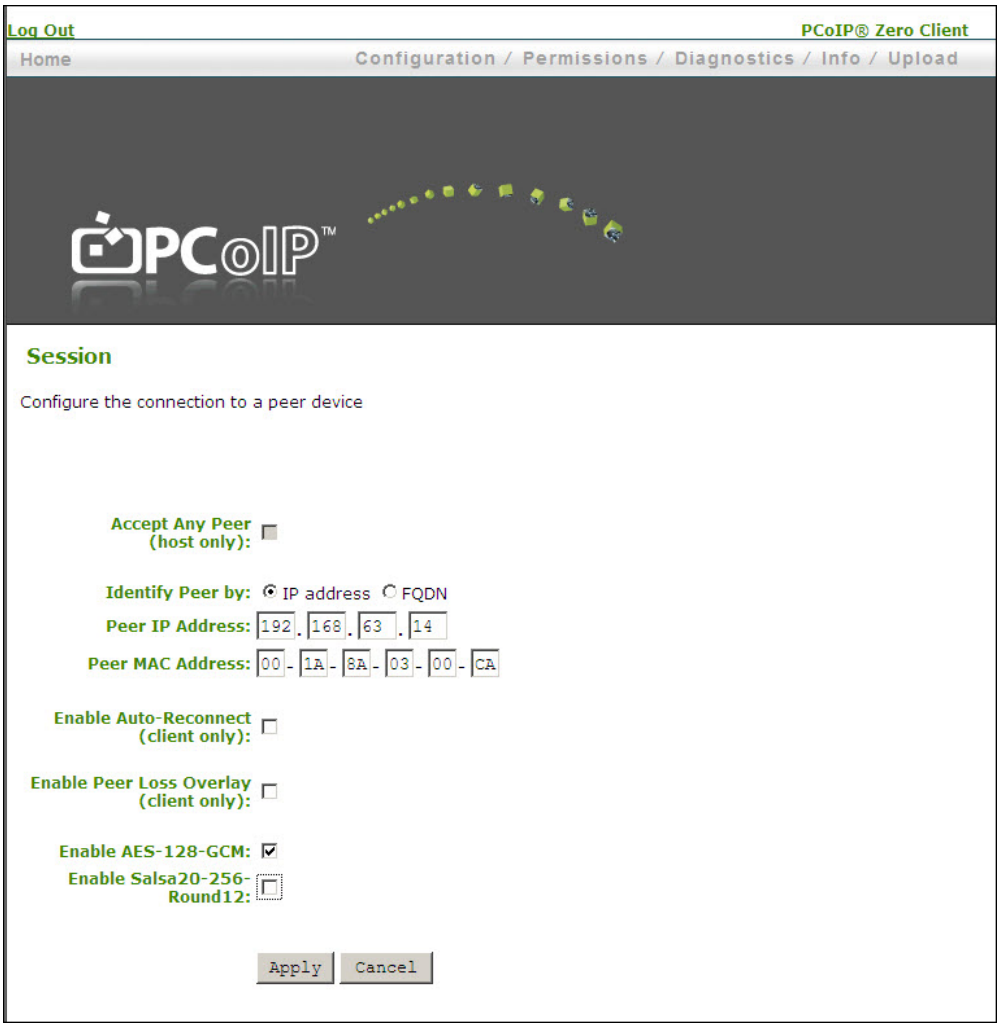


Figure 12-3: Client Session page Peer-to-Peer Configuration

8. In the **Identify Peer by** field, select the IP address.
9. Enter the host IP address in **Peer IP Address** field, e.g., 192.168.63.14.
10. Enter the host MAC address in **Peer MAC Address** field, e.g., 00-1A-8A-03-00-CA.

    Note: You can set the peer MAC address to 0-0-0-0-0-0 to ignore this field.
11. Click **Apply** to accept the changes.
12. From the **Diagnostics** menu, select the **PCoIP** page.
13. Click **Reset** to reset the PCoIP processor.

A.1.2 Configuring the Host Peer-to-Peer Operation

To configure the host for peer-to-peer connection:

1. Open the host Administrative Web Interface by using an Internet browser to open the host IP address, e.g., https://192.168.50.107.

2. Login to the host Administrative Web Interface (using a password if enabled).
3. From the **Configuration** menu, select the **Connection Management** page.

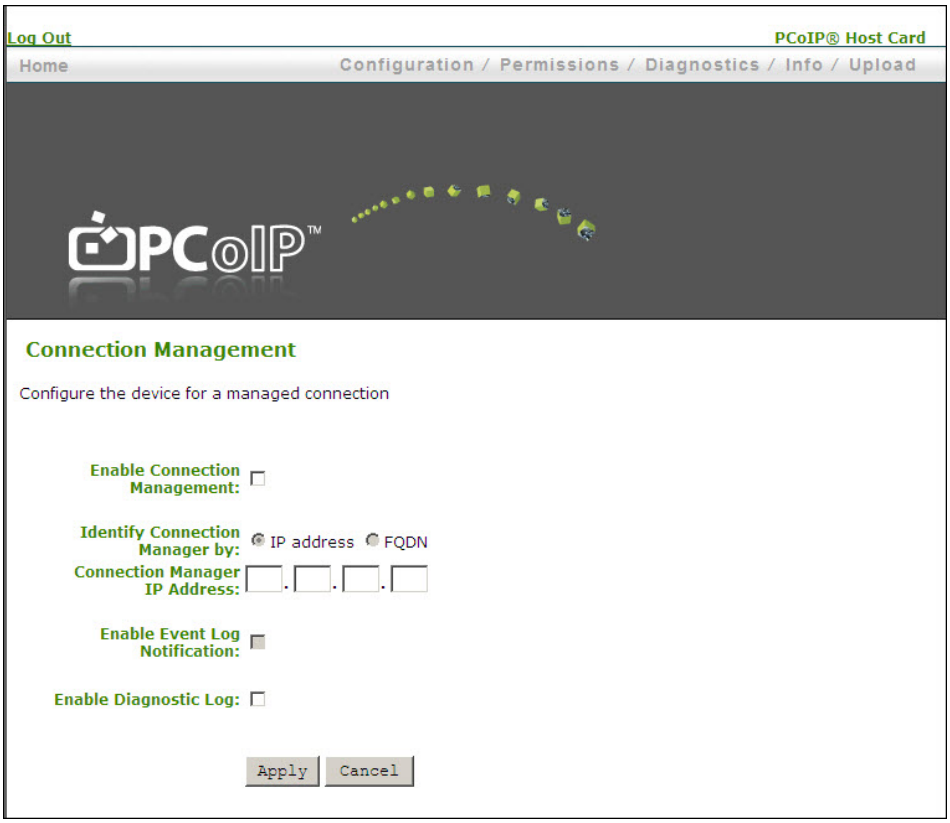


Figure 12-4: Host Connection Management Peer-to-Peer Configuration

4. Ensure the **Enable Connection Management** option is not selected.
5. From the **Configuration** menu, select the **Session** page.

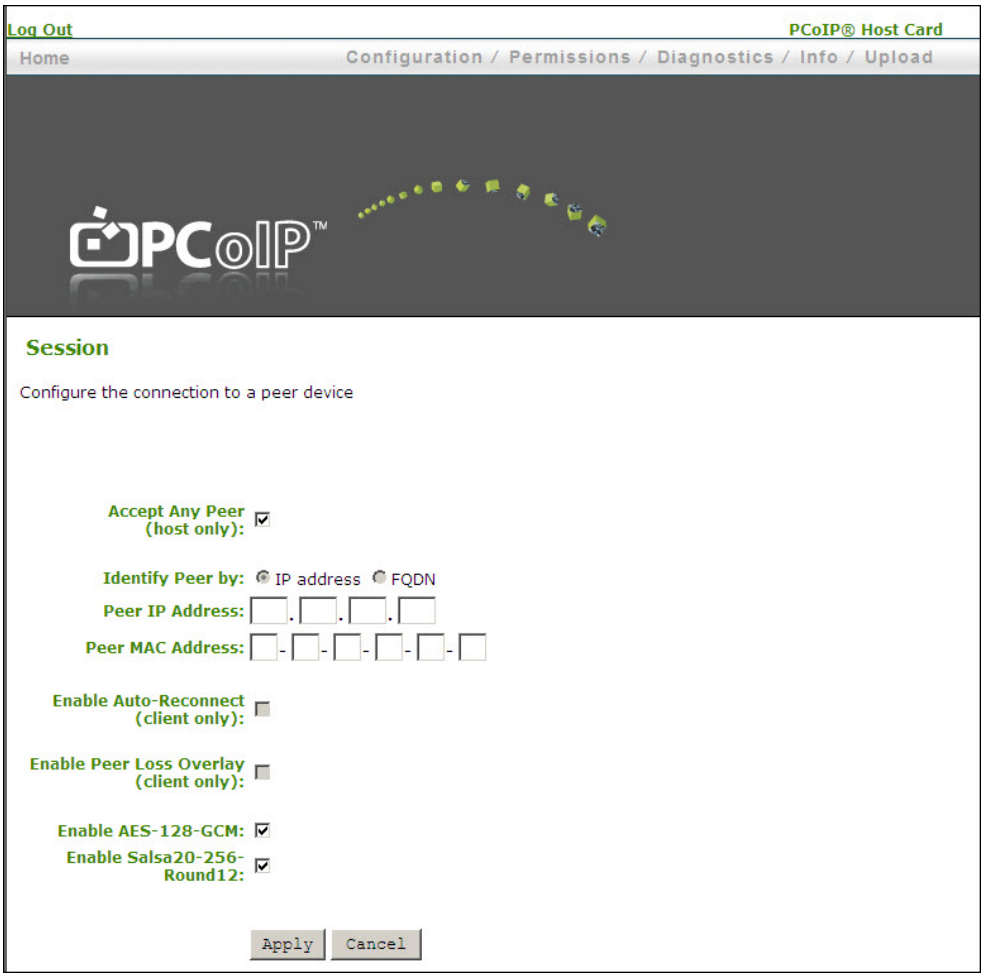


Figure 12-5: Session Page (Host)

6. Ensure **Accept any Peer** is not selected so that other clients cannot start a PCoIP session with the host.
7. Enter the client MAC address in the **Peer MAC Address** field, e.g., 00-1C-59-00-05-0E.
8. Click **Apply** to accept the changes.

A.1.3 Initiating the Peer-to-Peer Session

To start the peer-to-peer session:

1. From the OSD, click **Connect** to start the PCoIP session.

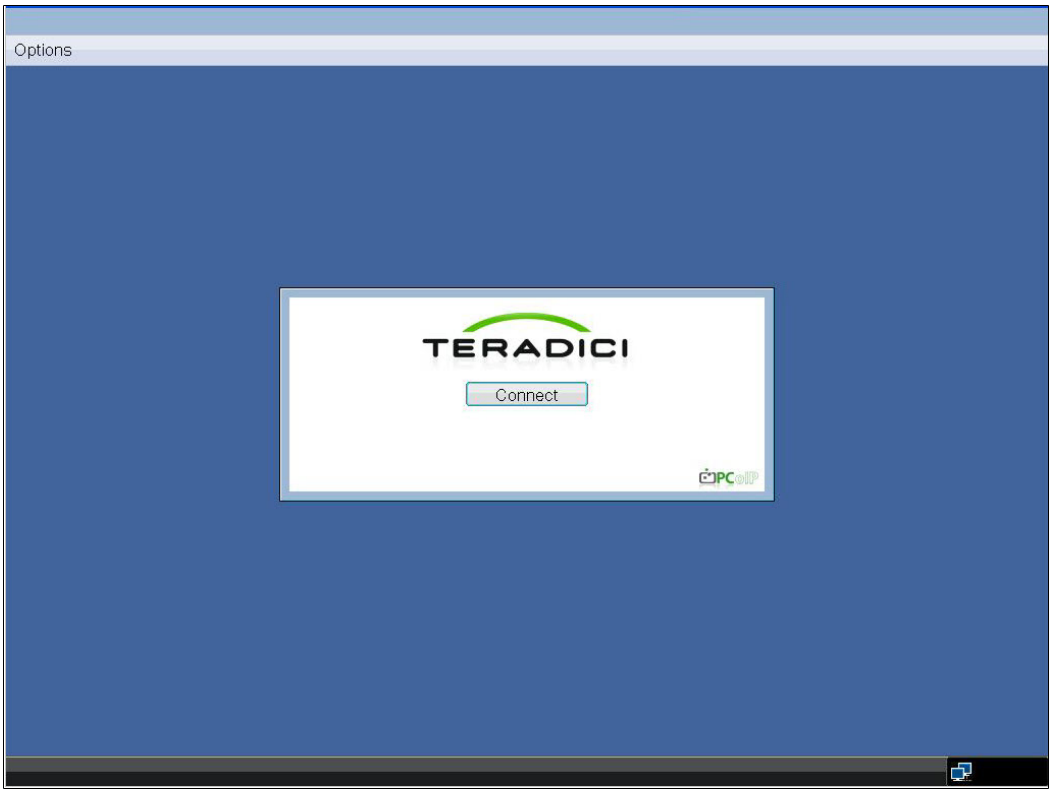


Figure 12-6: Peer-to-Peer Connect Screen

2. When connected, the host computer is ready to use over the PCoIP protocol.

A.2 DHCP and Enable Host Discovery Example

This example describes how to configure the client and host for use with a DHCP server and the Host Discovery feature without the use of a Connection Management Server.

The following starting IP addresses are used for this example:

- **Client**: IP Address: 192.168.0.111
- **Host:** IP Address: 192.168.1.222

Note: To configure for DHCP and Host Discovery, you must know the IP address of the client and host, regardless of whether it is set statically or dynamically.

A.2.1 Configuring Client DHCP and SLP Discovery

Note: Although this example uses the Administrative Web Interface for configuring the client for DHCP and Host Discovery operation, you can also use the OSD to configure the client.

To configure the client for DHCP and SLP Discovery:

1. Open the client Administrative Web Interface by using an Internet browser to open the client IP address, e.g., https//192.168.0.111.

2. Login to the client Administrative Web Interface (with a password if enabled).
3. From the **Configuration** menu, select the **Connection Management** page

Figure 12-7: Client Connection Management Configuration

4. Ensure **Enable Connection Management** is not selected.
5. From the **Configuration** menu, select the **Discovery** page.

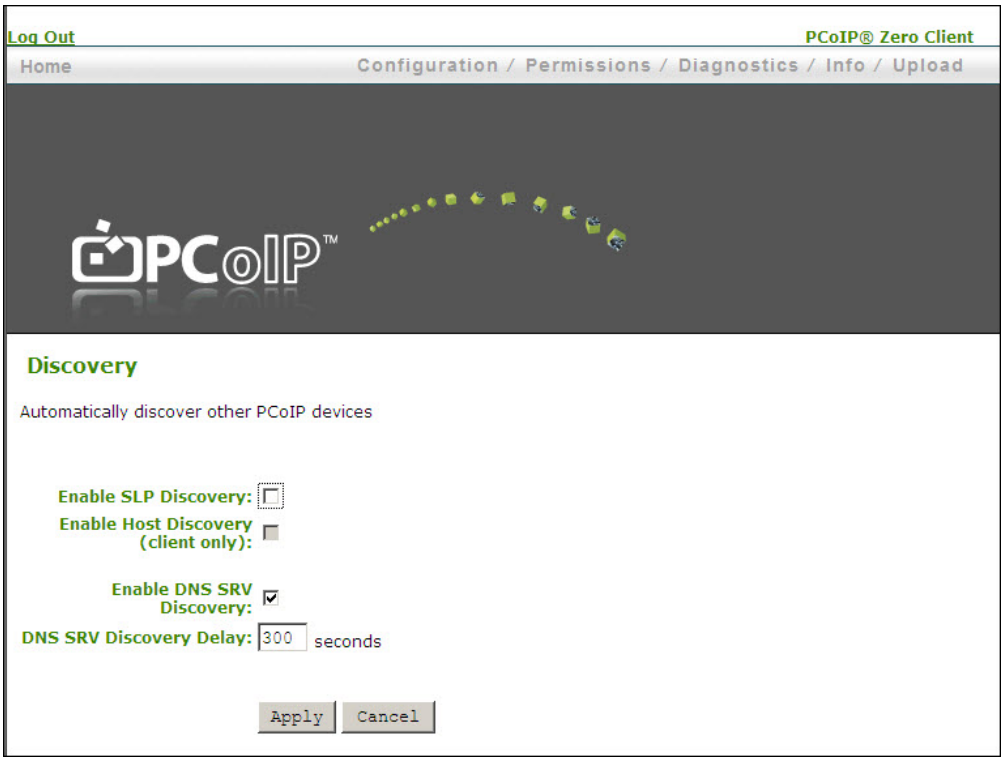


Figure 12-8: Client Discovery Page Enable SLP Discovery Configuration

6. Select **Enable SLP Discovery** and **Enable Host Discovery**.
7. Click **Apply** to accept the changes.
8. Click **Continue** to complete the configuration.
9. From the **Configuration** menu, select the **Network** page.

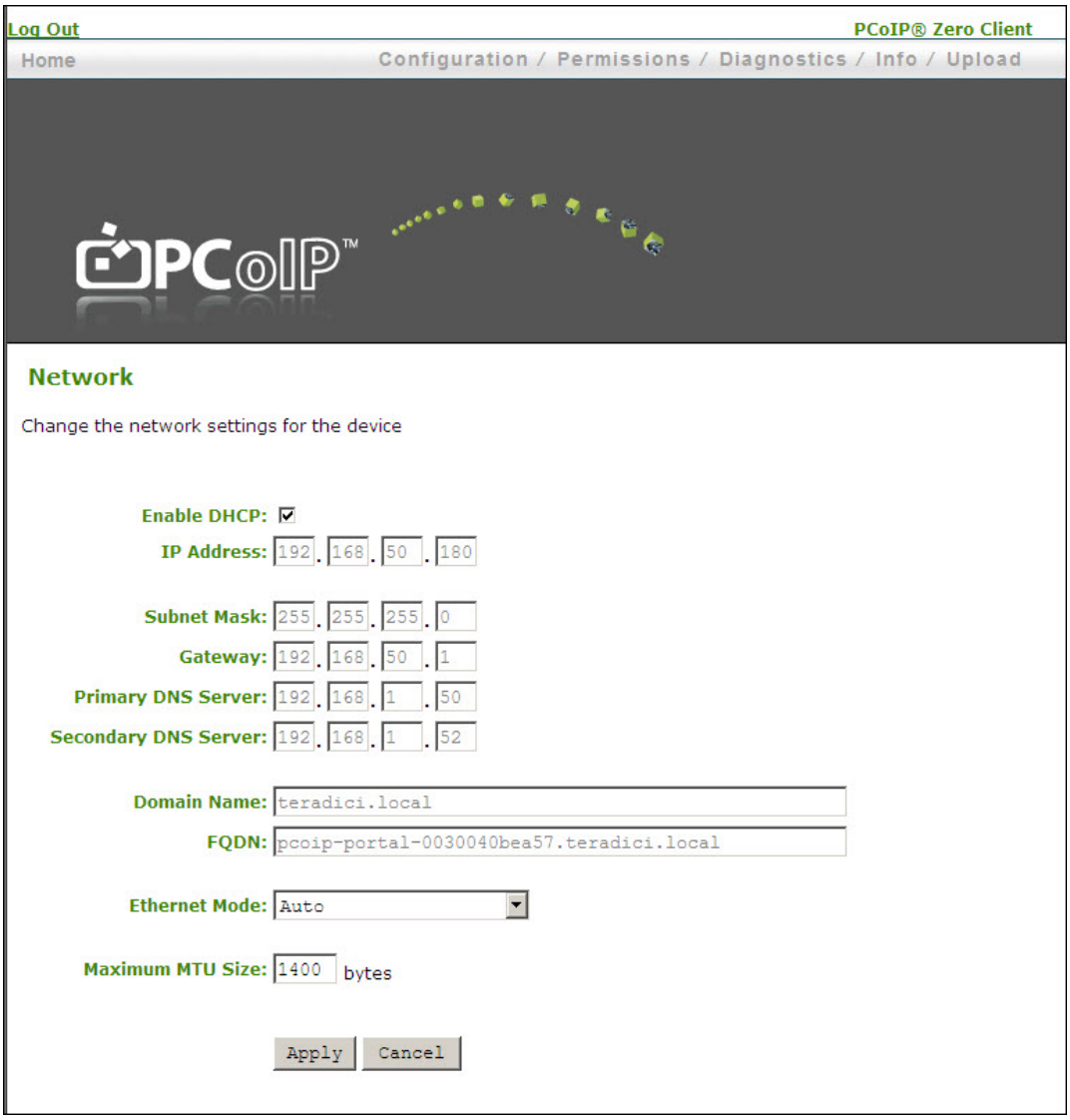


Figure 12-9: Client Network Page DHCP Configuration

10. Select **Enable DHCP**.
11. Click **Apply** to accept the changes.

    Note: Once configured for DHCP, the IP address is leased from the DHCP server. For future configuration, get the IP address from the DHCP server.

12. From the **Diagnostics** menu, select the **PCoIP Processor** page.
13. Click **Reset** to reset the PCoIP processor.

A.2.2 Configuring Host DHCP and SLP Discovery

To configure the host for DHCP and SLP Discovery:

1. From a browser, enter the host IP address. For example, https://192.168.1.222.
2. Login to the host Administrative Web Interface (with a password if enabled).

3. From the **Configuration** menu, select the **Connection Management** page.

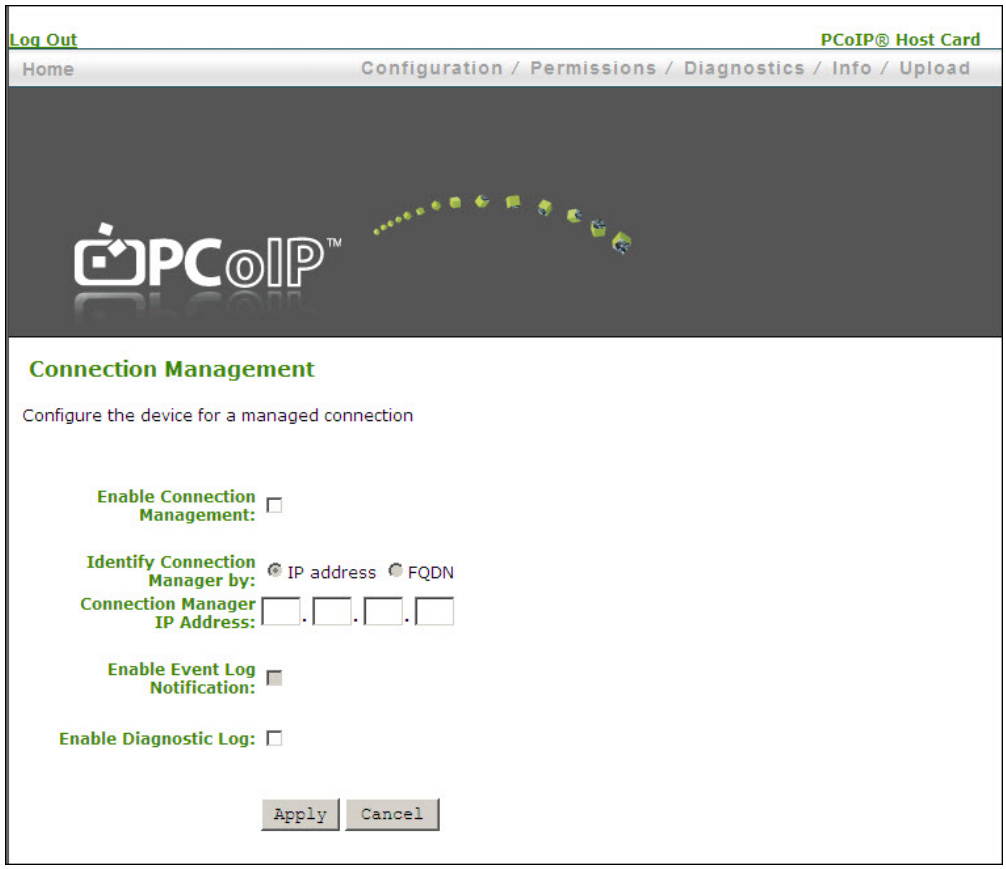


Figure 12-10: Host Connection Management Configuration

4. Ensure **Enable Connection Management** is not selected.
5. From the **Configuration** menu, select the **Discovery** page.

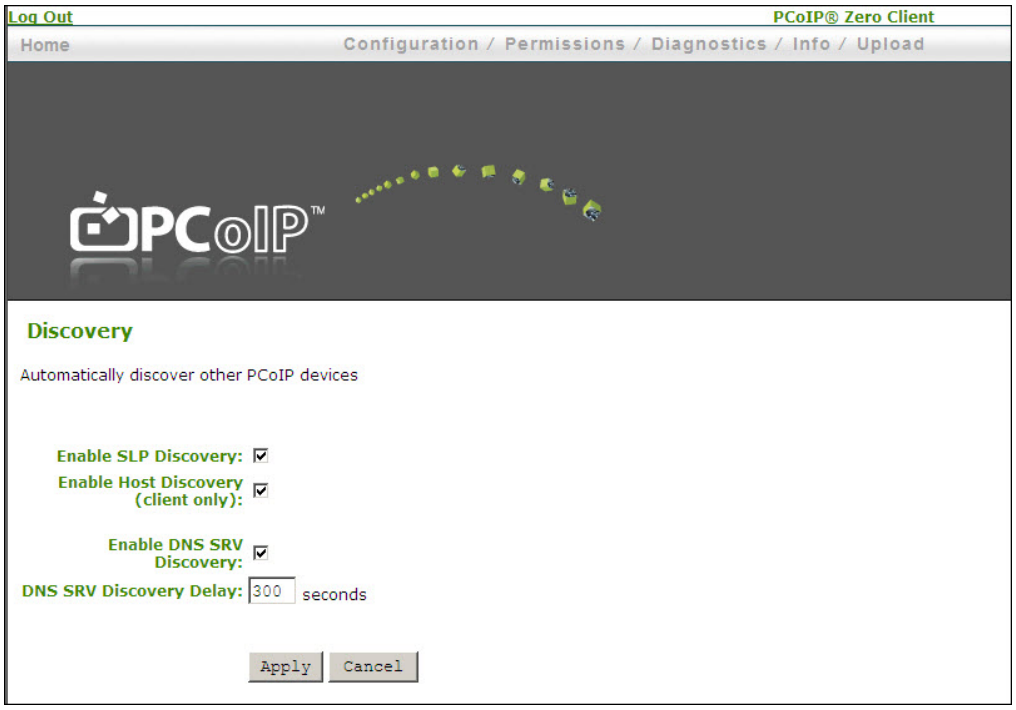


Figure 12-11: Host Discovery Page Enable SLP Discovery Configuration

6. Select **Enable SLP Discovery**.
7. Click **Apply** to accept the changes.
8. From the **Configuration** menu, select the **Network** page.

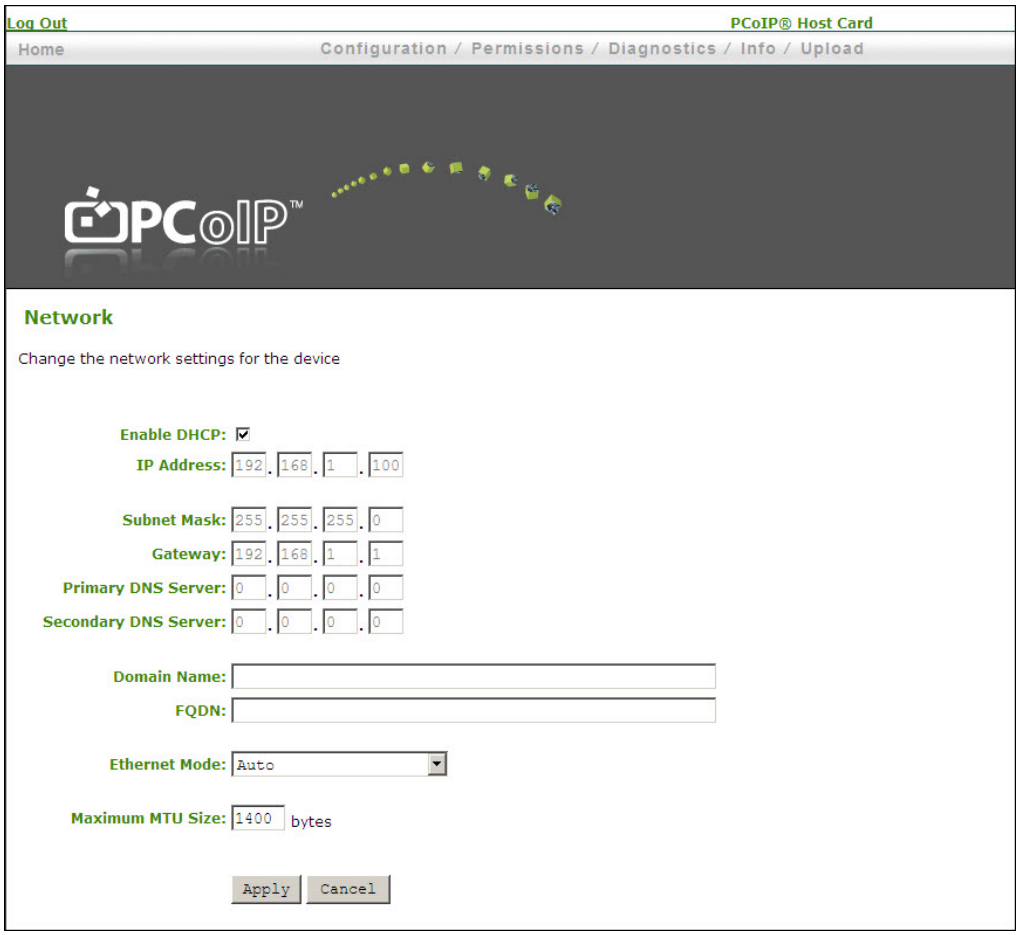


Figure 12-12: Host Network Page DHCP Configuration

9. Select **Enable DHCP**.
10. Click **Apply** to accept the changes.

    Note: Once configured for DHCP, the IP address is leased from the DHCP server. For future configuration, get the IP address from the DHCP server.

11. From the **Diagnostic** menu, select the **PCoIP Processor** page.
12. Click **Reset** to reset the PCoIP processor.

    Note: The host does not reset immediately. It waits until the host PC restarts, enters standby, hibernates, or powers off.

A.2.3 Initiating an SLP Discovery Session

To start the SLP discovery session:

1. From the OSD, click **Connect** to start discovering available hosts.
2. Select the desired host from the **Discovered Hosts** screen, and then click **OK**.

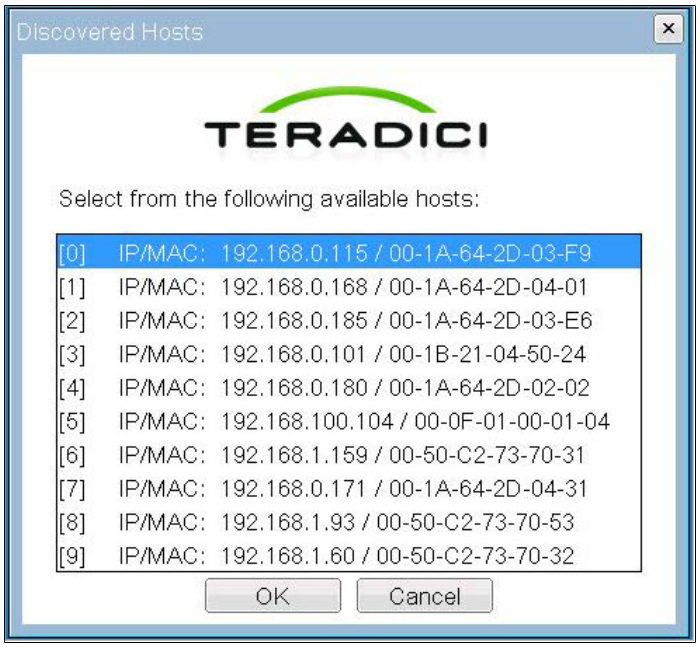


Figure 12-13: OSD Discovered Hosts Screen

3. When connected, the host PC is ready to use over the PCoIP protocol.

A.3 Bandwidth and Image Configuration Example

This example outlines the steps for optimizing user experiences in an environment where bandwidth is constrained. It is assumed that there are four task-based workers (web browsing, simple word processing, simple spreadsheet manipulation, and small video pages) that share one 100-Mbps switch.

Due to the nature of these tasks, the users do not require heavy graphics changes and each user would likely require peak network bandwidth at different times.

The following figure shows simplified bandwidth requirements for each user assuming they each had the full 100 Mbps available. The figure shows that network demand for each user peaks only for short periods (e.g., when opening/closing pages, scrolling a page, etc.).

Because the PCoIP system adapts quickly to available bandwidth, we recommend keeping the system defaults. However, the following examples show how to adapt the default settings if your configuration requires it.

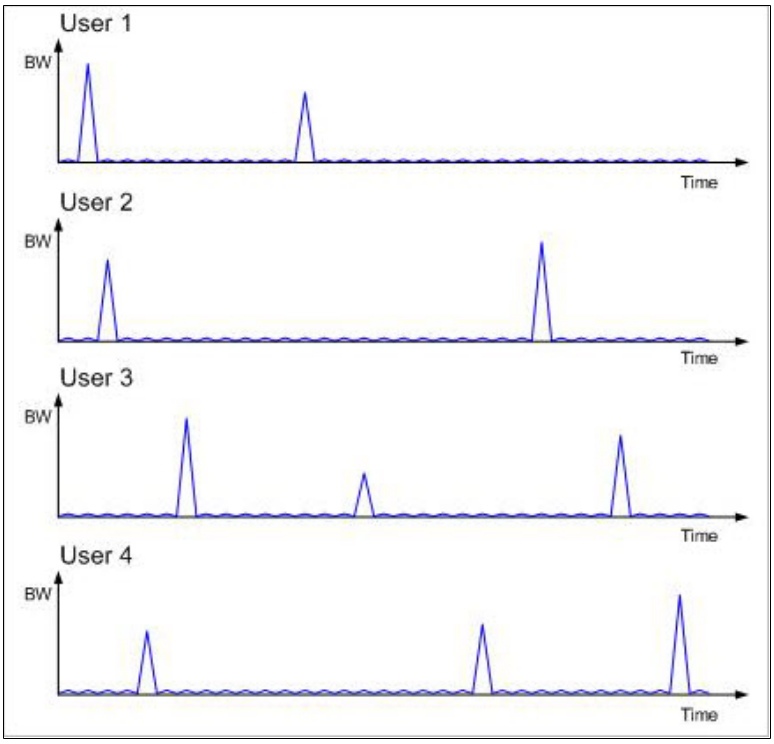


Figure 12-14: Simplified User Bandwidth Requirements (assuming 100 Mbps)

A.3.1 Configuring the Host Bandwidth Limit to 25 Mbps

In this example, the network is configured to minimize packet loss. Networks respond to congestion by dropping packets. The PCoIP processor responds to dropped (lost) packets by reducing the amount of bandwidth it generates. In most cases, the PCoIP processor conceals the packet loss to be imperceptible to the user. However, in some situations where bandwidth is low or network latency is high, it might be preferable to eliminate congestion-based packet loss by limiting the available bandwidth to each user. In this example, we limit each user's peak bandwidth to a hard limit of 25 Mbps (that is, the firmware does not use more than 25 Mbps).

We also set a target (soft limit) of 20 Mbps so that during periods of network congestion, the bandwidth is decreased rapidly to 20 Mbps and more slowly below 20 Mbps. This ensures that the available bandwidth is shared fairly if other network traffic further constrains the link.

Note: For example, it is assumed that very little data is required from the client back to the host (that is, USB keyboard and mouse data) and therefore only the host bandwidth is limited. To be complete, the client bandwidth limit could also be configured.

To set the bandwidth limit to 25 Mbps:

1. Open an Internet browser, and then open the Administrative Web Interface for the first user's host using the IP address for the host.
2. Log in using a password (if enabled).
3. From the **Configuration** menu, select the **Bandwidth** webpage.

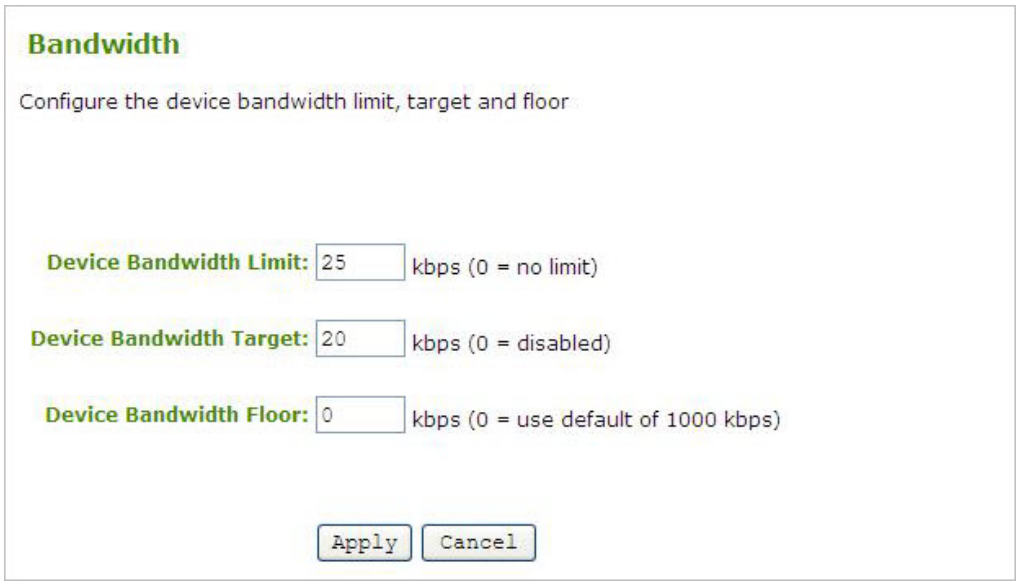


Figure 12-15: Host Bandwidth Limit Configuration (25 Mbps)

4. Enter *25* in the **Device Bandwidth Limited** field.
5. Enter *20* in the **Device Bandwidth Target** field.
6. Click **Apply** to accept the changes.
7. Repeat these steps for the other three users' hosts.

The bandwidth is now limited to 25 Mbps and targeted to 20 Mbps for each user.

The following figure shows simplified bandwidth usage with the limit for each user now configured for 25 Mbps. This figure shows that all users are limited to 25 Mbps and do not have access to more bandwidth when required. It also shows that even when the usage is totaled, the total switch bandwidth (100 Mbps) is never fully used.

Also note that since there is no congestion, there is no requirement to reduce the bandwidth to the targeted 20 Mbps or lower.

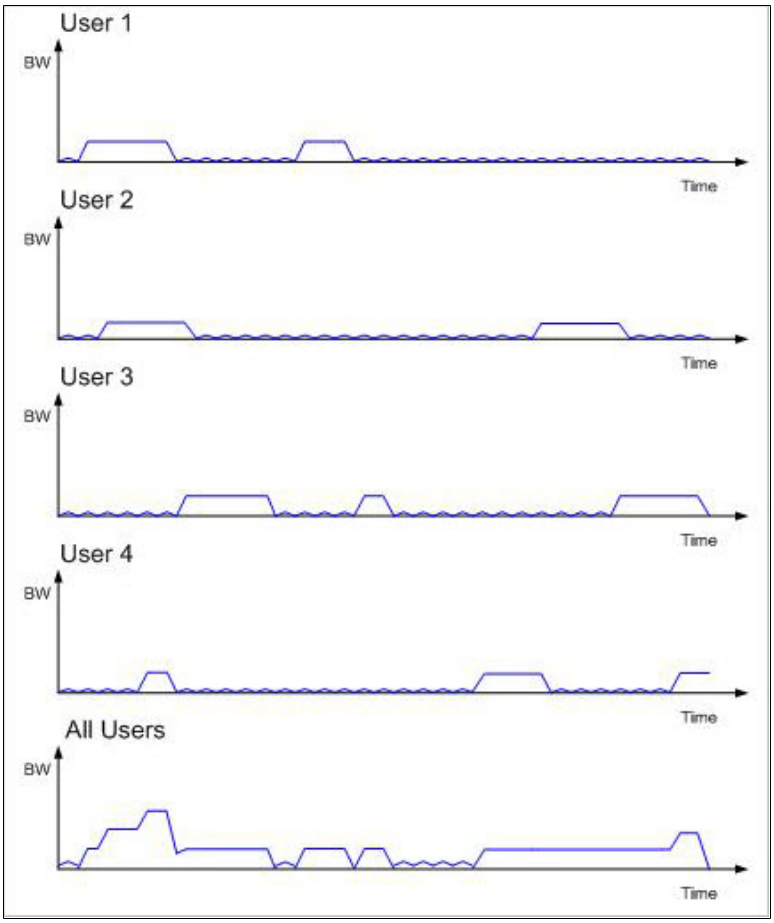


Figure 12-16: : Simplified User Bandwidth Requirements (25 Mbps)

A.3.2 Configuring Image Properties

In the example where the host bandwidth was set to 25 Mbps, it is possible that users may occasionally require more than that bandwidth limit to fully render their display information at maximum quality and full frame rate. The PCoIP system gives two controls over imaging quality that can optimize the user experience in environments where bandwidth is constrained.

For users who prefer higher image quality than what the PCoIP protocol balanced-quality/frame-rate algorithm provides, increasing the client **Minimum Image Quality** setting may be beneficial.

The **Maximum Initial Image Quality** setting can change the peak bandwidth required by any user. Decreasing the **Maximum Initial Image Quality** from the default setting of 90 can reduce the amount of bandwidth required per user while maintaining a minimum limit on the user experience.

Note: This example uses the Administration Web Interface for configuring the client for **Minimum Image Quality** and **Maximum Initial Image Quality**. Although you can also use the OSD to configure the client, the **Maximum Initial Image Quality** does not have a

corresponding parameter in the OSD as it is meant as an administrator-only parameter due to the potential impact on network traffic.

To configure the image properties:

1. From a browser, open the client Administrative Web Interface for the first user's client by using the client's IP address.
2. Login using a password (if enabled).
3. From the **Configuration** menu, select the **Image** webpage.

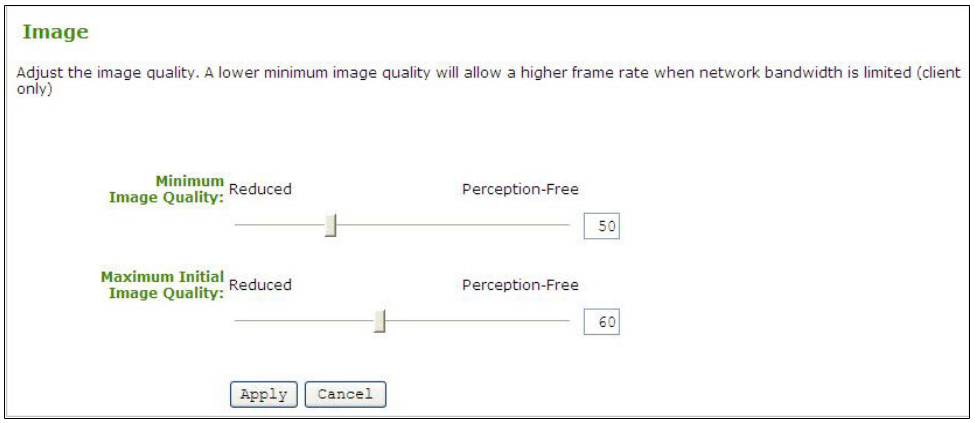


Figure 12-17: Client Minimum Image Quality Configuration

4. Slide the **Minimum Image Quality** slider to the right.
5. Slide the **Maximum Initial Image Quality** slider to the left.
6. Click **Apply** to accept the changes.
7. Repeat for the other three user clients.

The **Minimum Image Quality** is now configured towards **Perception-Free** to increase the minimum image quality the system reduces to under any condition. This effect is only noticeable in limited bandwidth cases. If bandwidth is not constrained, the system always maintains perception-free quality. The **Minimum Image Quality** feature does not alter the overall bandwidth requirements of the user.

The **Maximum Initial Image Quality** is now configured towards **Reduced** to limit the quality on the changed image (i.e., initial video frame). A lower **Maximum Initial Image Quality** setting requires less bandwidth as the lower-quality initial image requires less bandwidth to create. In this case, the administrator and the users determined that setting the **Maximum Initial Image Quality** to 60 was a preferable way of reducing bandwidth requirements than setting a hard limit on the **Device Bandwidth Limit**.

Regardless of the **Maximum Initial Image Quality** setting, the PCoIP system always builds unchanged regions of the display to a lossless image.

Note: The **Minimum Image Quality** setting must always be less than or equal to the **Maximum Initial Image Quality** setting.

A.3.3 Configuring the Host Bandwidth Limit to 0 Mbps (No Limit)

This example shows the PCoIP protocol default bandwidth and imaging settings being used to take advantage of the usage characteristics of the group. (The characteristics in this example are similar to many actual usage groups.) Here the device bandwidth limit and device bandwidth target are configured to 0 (no limit) to allow more effective bandwidth sharing. The firmware alleviates bandwidth congestion by implementing a bandwidth adaptation algorithm that strives for fairness on shared networks. The firmware uses the bandwidth as determined by the Ethernet physical-layer device.

Note: In this example, it is assumed that very little data is required from the client back to the host (i.e., USB keyboard and mouse data), and therefore only the host bandwidth is limited. To be complete, the client bandwidth limit could also be configured.

To configure the host bandwidth to no limit:

1. From a browser, enter the IP address of the first user's host.
2. Login to the Administrative Web Interface for the host (with a password if enabled).
3. From the **Configuration** menu, select the **Bandwidth** webpage.

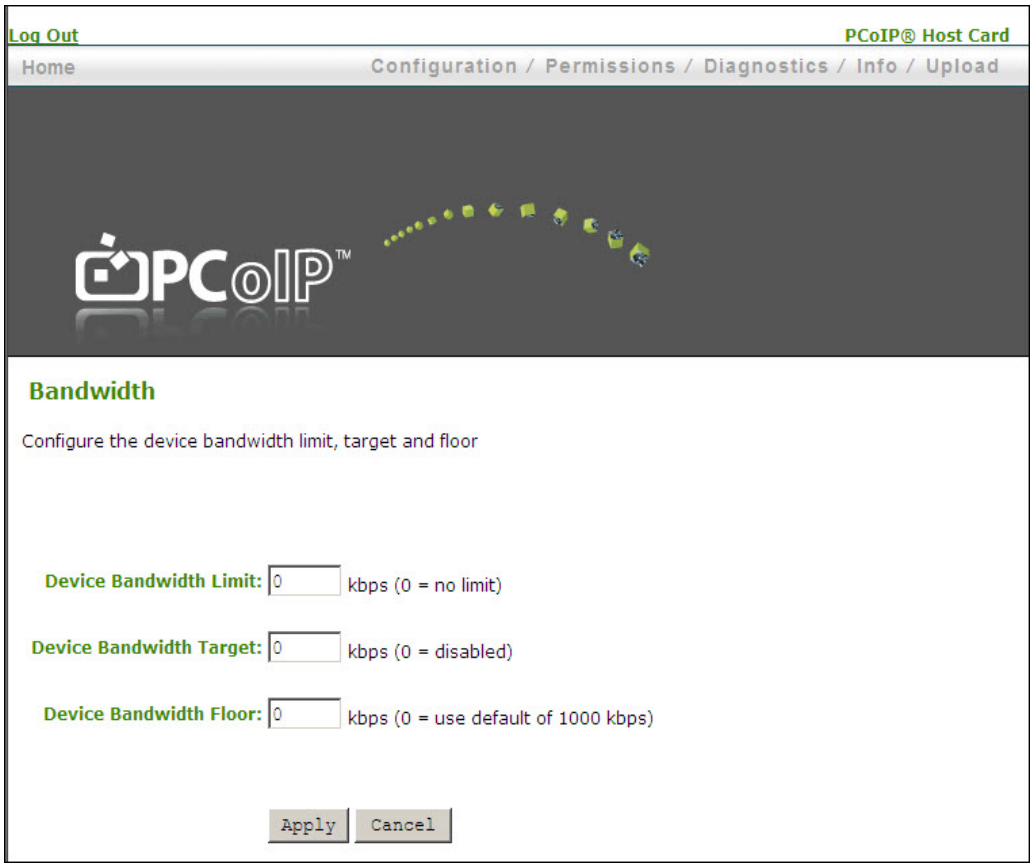


Figure 12-18: Host Bandwidth Limit Configuration (0 Mbps, no limit)

4. Enter *0* in the **Device Bandwidth Limit** field to enable no limit.
5. Enter *0* in the **Device Bandwidth Target** field to enable no limit.

6. Click **Apply** to accept the changes.
7. Repeat for the other three users' hosts.

The bandwidth limit and target are now set to 0 Mbps (no limit) for each user. Due to the nature of the users' tasks—light graphics changes and peak network demand at different times—little conflict is expected for the full 100-Mbps bandwidth. The users share the bandwidth more effectively and have fewer situations where their images would have to be compromised to meet a bandwidth limit.

When there is congestion, the firmware automatically reduces the bandwidth limit using a bandwidth adaptation algorithm that strives for fairness on shared networks. When the congestion clears, the firmware again opens the bandwidth limit.

The following figure shows the total simplified bandwidth usage with no limit for the four users in this example. This figure shows that the bandwidth is more efficiently shared, compared to the case of setting a low maximum bandwidth limit. In the unlimited case, each PCoIP session can use up to 100 Mbps. This provides the user with a more perception-free experience.

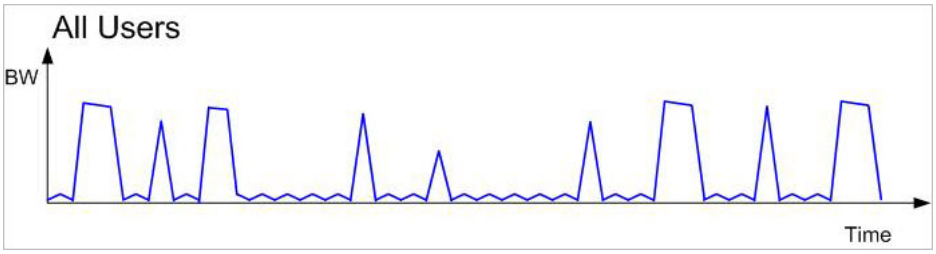


Figure 12-19: Simplified User Bandwidth Requirements (no limit)

A.4 USB Permissions Example

This example shows the use of the **USB Permissions** page. It shows how you can use the human-readable drop-down menus to authorize a specific class of IEEE-compatible bidirectional USB printers and a specific vendor/product ID.

This example outlines the steps to authorize a USB device by Class or by Device ID. The example assumes that the system already has Human Interface Devices (any Sub Class, Any Protocol) authorized.

Warning: As the host is the master for USB permissions, the USB permissions are applied with different priorities on the host vs. the client. Depending on the deployment, hardware PCoIP host vs. software PCoIP host, configuring the client USB permissions may or may not have advantages. See section 5.1 for more information on USB permission priorities.

.

A.4.1 Authorizing USB Device By Class

To authorize a USB device by class:

1. Open the **USB Permissions** page.
2. In the **Authorization** section, click **Add new**.

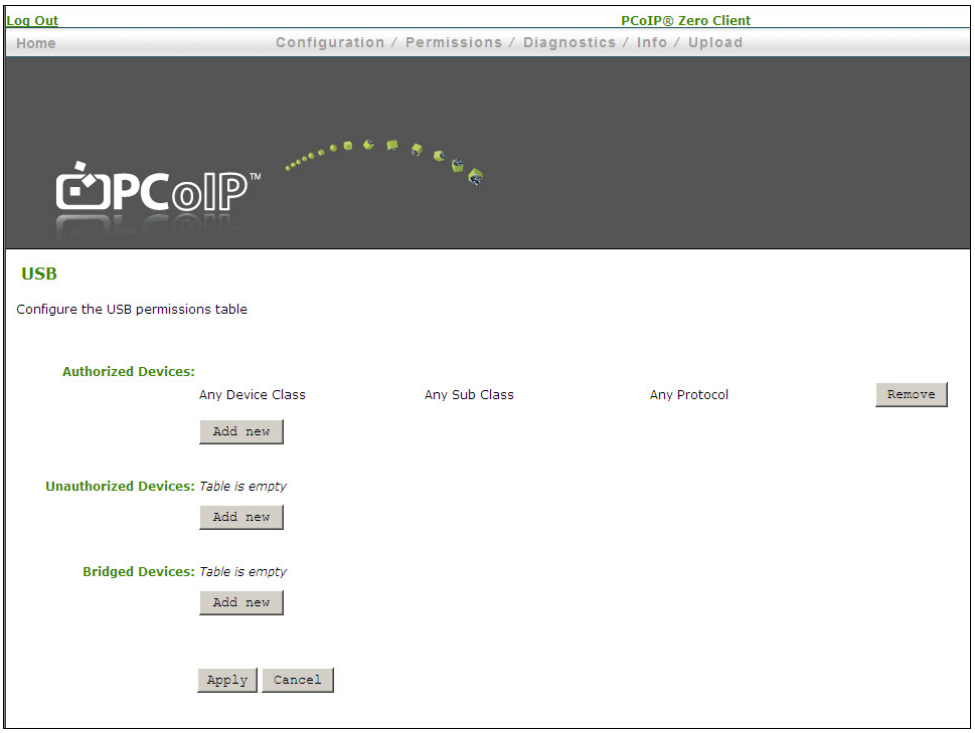


Figure 12-20: USB Permissions Example: Add new Button

3. When the entry fields expand, select **Class** from the **Add New** drop-down menu to authorize a class of devices.

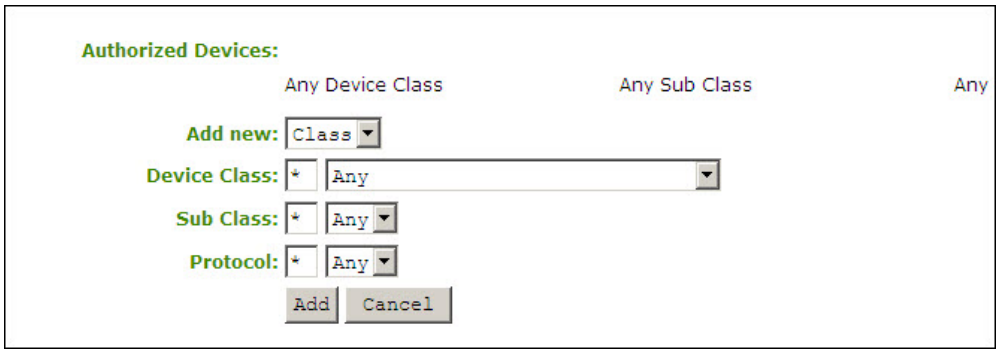


Figure 12-21: USB Permissions Example: Selecting the Class Entry Type

4. Select **Printer** from the **Device Class** drop-down menu to authorize a class of printers.
5. Select **Printer** from the **Sub Class** drop-down menu to authorize a specific class of printers (otherwise, the sub class and protocol could be left as "Any").
6. Select the desired IEEE 1284.4-compatible bidirectional protocol from the **Protocol** drop-down menu.
7. Click **Apply** to save the changes to flash and complete the configuration.

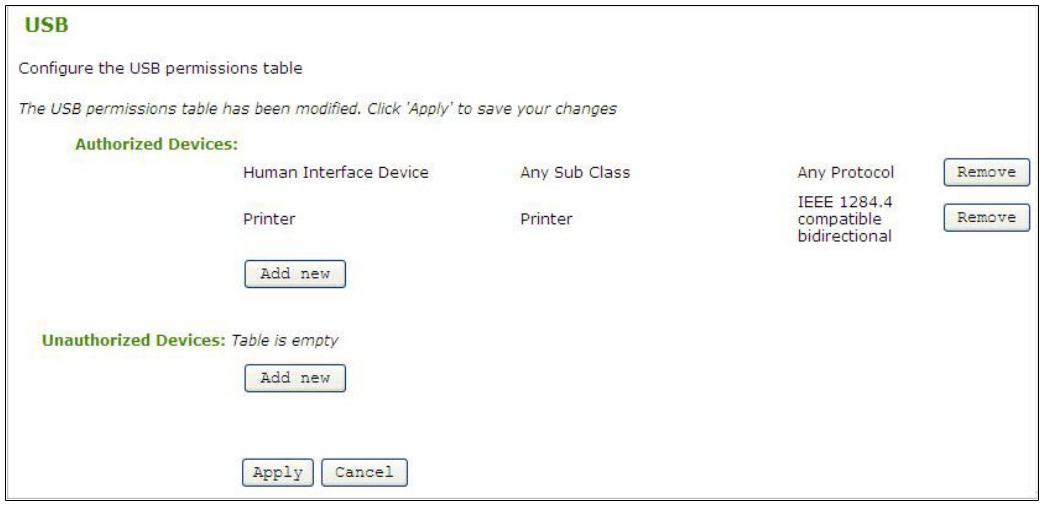


Figure 12-22: USB Permissions Example: Class Authorization

A.4.2 Authorizing USB Device By Vendor/Product ID

To authorize a USB device by its vendor or product ID:

1. In the **Authorization** section, click **Add new**.

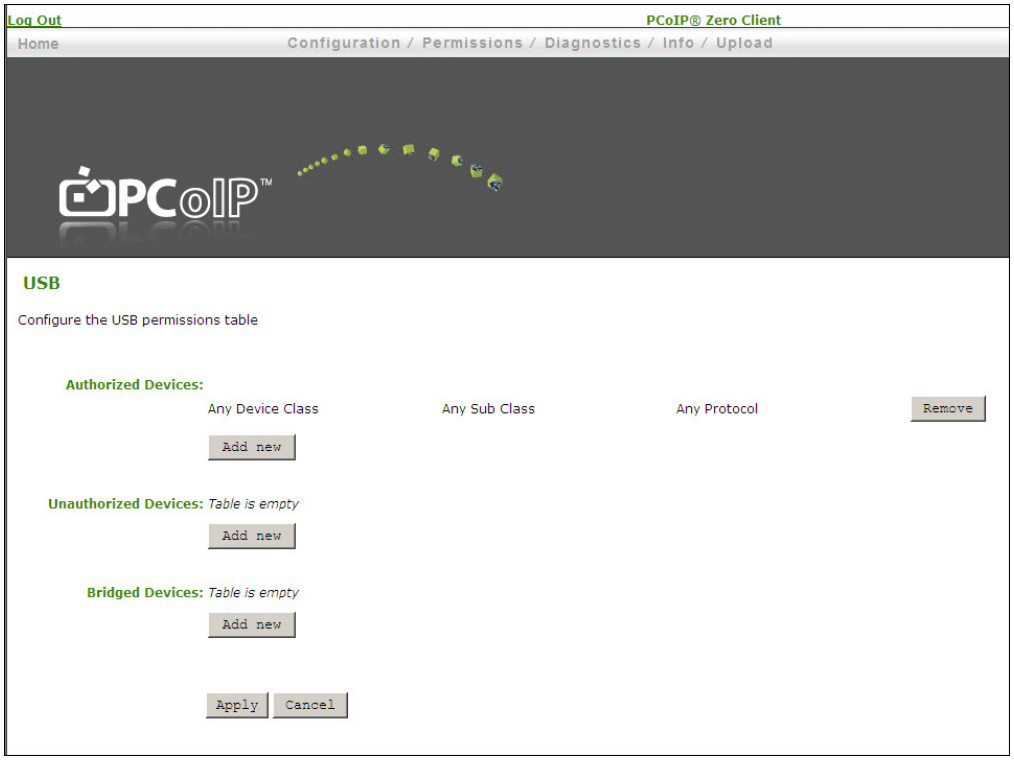


Figure 12-23: USB Permissions Example: Add new Button

2. When the entry fields expand, select **ID** from the **Add New** drop-down menu to authorize a device by its vendor/product ID.

3. Enter the USB device vendor ID and product ID into the corresponding fields.

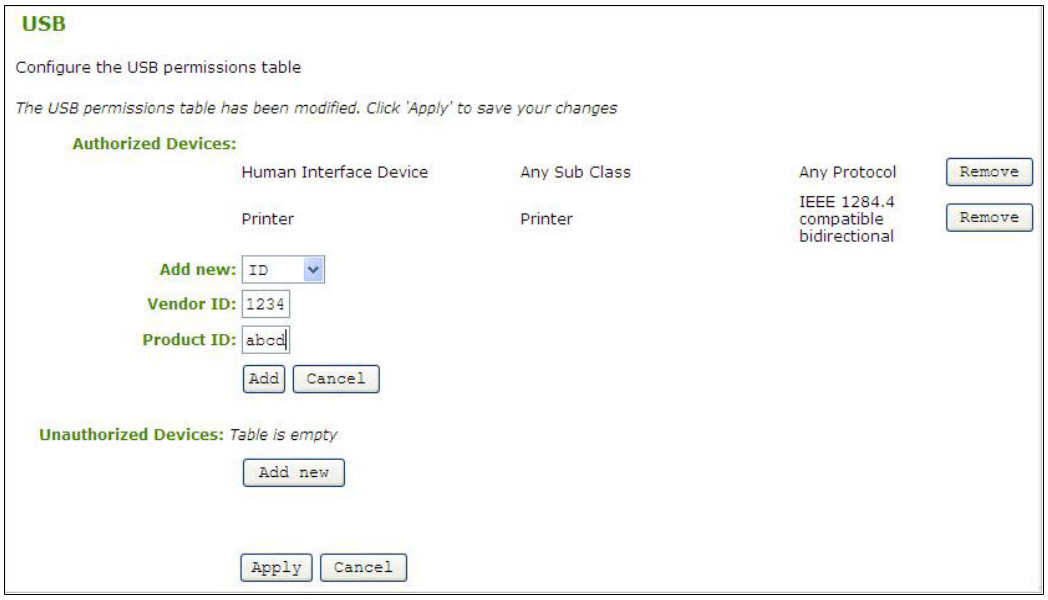


Figure 12-24: USB Permissions Example: Entering Vendor ID and Product ID

4. Click **Apply** to save the changes to flash and complete the configuration.

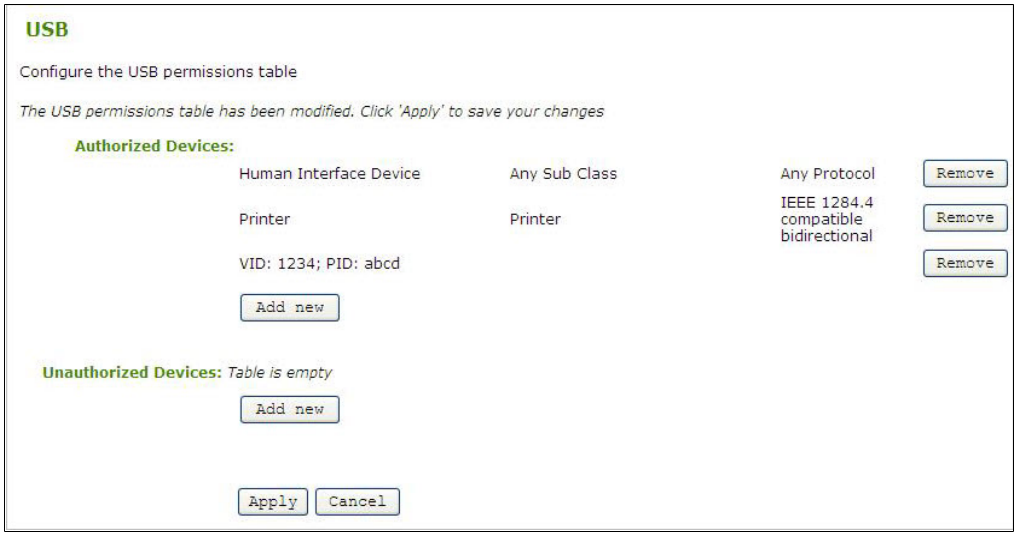


Figure 12-25: USB Permissions Example: Vendor ID and Product ID Authorization

Appendix B: Client Language and Keyboard Support

The client firmware can support various languages and keyboard layouts.

B.1 Languages Supported by the Client

- English (default)
- French
- German
- Greek
- Spanish
- Italian
- Portuguese
- Korean
- Japanese
- Traditional Chinese
- Simplified Chinese

B.2 Keyboard Layouts Supported by the Client

- Belgian ISO-8895-1
- Belgian ISO-8859-1 (accent keys)
- Czech
- Danish Codepage 865
- Danish ISO-8859-1
- Danish ISO-8859-1 (accent keys)
- Dutch ISO-8859-1 (accent keys)
- Estonian
- Finish Codepage 850
- Finnish ISO-8859-1
- Finnish ISO-8859-1 (accent keys)
- French Canadian ISO-8859-1 (accent keys)
- French Dvorak-like
- French Dvorak-like (accent keys)
- French ISO-8859-1
- French ISO-8859-1 (accent keys)
- German Codepage 850
- German ISO-8859-1
- German ISO-8859-1 (accent keys)

- Greek ISO-8859-7 (104 keys)
- Hungarian
- Italian ISO-8859-1
- Japanese 106/109
- Japanese 106x (ctrl and shift swapped)
- Korean Dubeolsik ISO-8859-1
- Latin American
- Latin American (accent keys)
- Latvian (QWERTY)
- Lithuanian
- Norwegian Dvorak
- Norwegian ISO-8859-1
- Norwegian ISO-8859-1 (accent keys)
- Polish ISO-8859-2 (Programmers)
- Portuguese ISO-8859-1
- Portuguese ISO-8859-1 (accent keys)
- Romanian
- Russian
- Serbian (Cyrillic)
- Serbian (Latin)
- Slovenian
- Spanish ISO-8859-1
- Spanish ISO-8859-1 (accent keys)
- Spanish ISO-8859-15 (accent keys)
- Swedish Codepage 850
- Swedish ISO-8859-1
- Swedish ISO-8859-1 (accent keys)
- Swiss-French Codepage 850
- Swiss-French ISO-8859-1
- Swiss-French ISO-8859-1 (accent keys)
- Swiss-German Codepage 850
- Swiss-German ISO-8859-1
- Swiss-German ISO-8859-1 (accent keys)
- Turkish Q ISO-8859-9
- Turkish Q ISO-8859-9 (accent keys)
- United Kingdom Codepage 850
- United Kingdom Codepage 850 (ctrl and caps swapped)
- United Kingdom ISO-8859-1 (ctrl and caps swapped)
- United States of America Dvorak
- United States of America Emacs optimized layout

- United States of America ISO-8859-1
- United States of America ISO-8859-1 (accent keys)
- United States of America ISO-8859-1 (ctrl and caps swapped)
- United States of America left-hand Dvorak
- United States of America right-hand Dvorak
- United States of America traditional Unix workstation