

PCoIP Administrator's Guide

TER0606004

Issue 15



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
15	December 2, 2011	Updated for Firmware Release 3.5.0 <ul style="list-style-type: none"> • Proximity card based SSO with Imprivata OneSign server support • IEEE 802.1X network authentication • IPv6 support • DHCPv6 support • Self-help link added: Lets you configure an end-user link for access to self-help information • Limited USB 2.0 support for View 4.6 or later deployments (bulk only for devices directly connected to root ports) • Enhanced imaging controls • View Connection Server cache increased up to 25 entries • Audio Line-in Mode • Enhanced logging modes • Revamped User Interface: Improved the layout of the pages and screens: <ul style="list-style-type: none"> ◦ Home and Statistics pages: Added statistics, consolidated information ◦ Session page: consolidated information/pages for improved user experience ◦ Attached Devices page: expose the resolution, new onscreen legend to explain statistics • Certificate management (at this time, limited to 802.1X client certificate) • Monitor alignment support • Disconnect Message Filter field added: Lets you control the message that appears when a session disconnects • New hotkey to reset zero client to factory default configuration • New Session Connection Type field • New Pipeline Processing Rate field
14	September 16, 2011	Updated for Firmware Release 3.4.1 <ul style="list-style-type: none"> • Support for .Net cards
13	June 8, 2011	Updated for Firmware Release 3.4.0 <ul style="list-style-type: none"> • New banner at the top of the Administrative Web Interface page • RDP is no longer supported • Diagnostic enhancements: <ul style="list-style-type: none"> ◦ 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

Version	Date	Description
		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	<ul style="list-style-type: none"> Updated for Firmware Release 3.3. Incorporated information from Administrative notes (which documented features for Firmware Release 3.2.0).
10	Apr 06, 2010	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Updated for Firmware Release 2.3 Added notes about Host and Portal webpage banners Added description for SNMP enable feature
7	Jun 15, 2009	<ul style="list-style-type: none"> Updated for Firmware Release 2.2 Added description for enable display override Clarified Network Connection Lost overlay description (2 seconds of network inactivity)
6	May 14, 2009	<ul style="list-style-type: none"> 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

Version	Date	Description
		<ul style="list-style-type: none"> Updated description (removed Enable Audio Compression) for Audio webpage
5	Nov 25, 2008	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 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

Version	Date	Description
		<ul style="list-style-type: none"><li data-bbox="727 279 1146 302">• Updated for Firmware Release 0.20<li data-bbox="727 310 1057 333">• Added Bandwidth Statistics<li data-bbox="727 342 1182 365">• Updated RDP compatibility information
1	January 15, 2008	Initial release

Contents

Revision History.....	3
Table of Figures.....	11
Table of Tables.....	15
Definitions.....	17
1 Introduction.....	18
1.1 About this Document.....	18
1.2 Menu and Page Overview.....	19
2 Administrative Web Interface Overview.....	22
2.1 About the Page Layout.....	22
2.2 Supported Web Browsers.....	23
2.3 Administrative Web Interface IP Address.....	24
2.4 Administrative Interface Security.....	24
2.4.1 Installing the CA Root Certificate for Firefox.....	24
2.4.2 Installing the CA Root Certificate for Internet Explorer.....	24
2.5 Logging In.....	25
2.6 Viewing the Home Page.....	26
2.7 About the Administrative Interface Menus.....	28
2.7.1 Viewing the Configuration Menu.....	29
2.7.2 Viewing the Permissions Menu.....	29
2.7.3 About the Diagnostics Menu.....	29
2.7.4 About the Information Menu.....	30
2.7.5 About the Upload Menu.....	30
3 Working with the On Screen Display (OSD).....	31
3.1 About the Connect Window.....	31
3.1.1 Connect Button.....	32
3.2 About the OSD Options Menu.....	32
4 Configuring the Device.....	34
4.1 Initial Setup Page.....	34
4.2 Configuring the Network Settings.....	37
4.3 Configuring the IPv6 Settings for a Device.....	41
4.4 Adding Custom Information for the Device.....	44
4.5 Configuring the Discovery Mechanism.....	45
4.6 Configuring the SNMP Agent.....	47
4.7 Configuring the Session.....	47

4.7.1	Configuring a Direct Session.....	48
4.7.2	Configuring a Direct Session with SLP Host Discovery.....	52
4.7.3	Configuring a VMware View Connection.....	56
4.7.4	Configuring Kiosk Mode.....	63
4.7.5	Configuring a View Connection Server + Imprivata OneSign Connection.....	68
4.7.6	Enabling or Disabling Connection Management.....	72
4.8	Controlling the Bandwidth for PCoIP Sessions.....	76
4.9	Setting the User Interface Language.....	78
4.10	Configuring the OSD Screen-save Timeout.....	79
4.11	Adjusting the Image Quality.....	80
4.12	Enabling the Host Driver Function.....	83
4.13	Configuring the NTP Parameters.....	84
4.14	Updating the Password for a Device.....	85
4.15	Resetting the Parameters to Factory Default Values.....	87
4.16	Configuring the EDID Override Mode.....	88
4.17	Enabling Monitor Emulation.....	89
4.18	Enabling or Disabling the OSD Configuration Menus.....	90
4.19	Enabling or Disabling the Web Server.....	91
5	Setting up the User Permissions.....	92
5.1	Specifying USB Devices.....	92
5.2	Configuring the Audio Parameters.....	95
5.3	Setting up the Client's Power-off Permissions.....	96
6	Using the Diagnostic Tools.....	98
6.1	Viewing and Clearing Event Log Messages.....	98
6.1.1	Syslog Features.....	98
6.2	Controlling the Device Session.....	102
6.3	Viewing PCoIP Protocol Statistics.....	103
6.4	Working with the Host Information and Power State.....	106
6.5	Generating an Audio Test Tone from the Client.....	107
6.6	Viewing a Test Pattern on the Client's Display.....	107
6.7	Resetting the Device Processor.....	108
6.8	Determining if a Device is Reachable.....	110
7	Viewing Device Information.....	111
7.1	Viewing the Version Information.....	111
7.2	Viewing the Attached Devices.....	113
8	Uploading to the Device.....	115
8.1	Uploading Firmware to the Device.....	115

8.1.1 Firmware Upload Process Example:.....	115
8.2 Uploading a Logo to the Device.....	116
8.2.1 OSD Logo Upload Process Example.....	117
8.3 Uploading the Certificate.....	117
9 Configuring the User Settings.....	118
9.1 Configuring the Mouse Settings.....	118
9.2 Changing the Keyboard Repeat Settings.....	119
9.3 Adjusting the Image Quality from the OSD.....	120
9.4 Configuring the Display Topology.....	120
9.5 Configuring the Touch Screen.....	122
9.5.1 Installing the Touch Screen to the Zero Client.....	124
9.5.2 Setting up the Touch Screen as a Bridged Device.....	124
9.5.3 Configuring the Zero Client to Automatically Login to a VMware View Host.....	125
10 About the Overlay Windows.....	126
10.1 Network Connection Lost Overlay.....	126
10.2 USB Device Not Authorized Overlay.....	126
10.3 USB Over Current Notice Overlay.....	126
10.4 Half Duplex Overlay.....	127
10.5 Video Source Overlays.....	127
11 Using Smart Cards with PCoIP Zero Clients.....	128
11.1 Smart Card Requirements.....	128
11.1.1 Virtual Desktop Environment.....	128
11.1.2 Supported USB Card Readers.....	128
11.1.3 CAC Smart Card Properties.....	129
11.1.4 .Net Smart Card Properties.....	129
11.1.5 Communication Protocol.....	129
11.1.6 Card Certificate Requirements.....	129
11.1.7 Tested Smart Card Models.....	129
11.2 Using a Smart Card to Connect to a VMware View Brokered Session.....	130
Appendix A: Usage Examples Overview.....	133
A.1 Peer-to-Peer Direct Connection Example.....	133
A.1.1 Configuring the Client Peer-to-Peer Operation.....	133
A.1.2 Configuring the Host Peer-to-Peer Operation.....	134
A.1.3 Initiating the Peer-to-Peer Session.....	135
A.2 DHCP and Enable Host Discovery Example.....	136
A.2.1 Configuring the Client for DHCP and SLP Discovery.....	136
A.2.2 Configuring the Host for Host DHCP and SLP Discovery.....	138
A.2.3 Initiating an SLP Discovery Session.....	140
A.3 USB Permissions Example.....	140

A.3.1 Authorizing USB Device By Class.....	141
A.3.2 Authorizing USB Device By Vendor/Product ID.....	141
Appendix B: Client Language and Keyboard Support.....	143
B.1 Languages Supported by the Client.....	143
B.2 Keyboard Layouts Supported by the Client.....	143

Table of Figures

Figure 2-1: Administrative Web Interface Home Page (Host).....	23
Figure 2-2: Administrative Web Interface Log In Page.....	25
Figure 2-3: Administrative Web Interface Home Page (Host Card).....	26
Figure 2-4: Administrative Web Interface Menu Overview.....	29
Figure 3-1: OSD Connect Window.....	31
Figure 3-2: Network Not Ready (detail).....	31
Figure 3-3: Network Ready (detail).....	32
Figure 3-4: OSD Connect Screen (Connecting).....	32
Figure 3-5: OSD Options Menu.....	33
Figure 4-1: Initial Setup Page (Host).....	35
Figure 4-2: Initial Setup Page (Client).....	36
Figure 4-3: Administrator Web Interface Network Page.....	38
Figure 4-4: OSD Network Page.....	39
Figure 4-5: Administrative Web Interface IPv6 Page.....	42
Figure 4-6: OSD IPv6 Page.....	43
Figure 4-7: Administrative Web Interface Label Page.....	44
Figure 4-8: OSD Label Page.....	44
Figure 4-9: Administrative Web Interface Discovery Page.....	45
Figure 4-10: OSD Discovery Page.....	46
Figure 4-11: Administrative Web Interface SNMP Agent Page.....	47
Figure 4-12: AWI Session Connection Type Options (Host).....	48
Figure 4-13: AWI Session Connection Type Options (Client).....	48
Figure 4-14: AWI Session Connection Type – Direct from Client (Host).....	49
Figure 4-15: AWI Session Connection Type – Direct to Host (Client).....	49
Figure 4-16: OSD Session Connection Type – Direct to Host.....	50
Figure 4-17: OSD Session Connection Type – Direct to Host (Advanced Settings).....	50
Figure 4-18: AWI Session Connection Type – Direct from Host with SLP Host Discovery.....	53
Figure 4-19: OSD Session Connection Type – Direct to Host with SLP Host Discovery.....	53
Figure 4-20: OSD Session Connection Type – Direct to Host with SLP Host Discovery (Advanced Settings).....	54
Figure 4-21: AWI Session Connection Type – View Connection Server.....	57
Figure 4-22: OSD Session Connection Type – View Connection Server.....	58
Figure 4-23: OSD Session Connection Type – View Connection Server (Advanced Options).....	58

Figure 4-24: Enable Self Help Link Options.....	62
Figure 4-25: View Connection Server with Auto-Logon.....	63
Figure 4-26: AWI Session Connection Type View Connection Server + Kiosk.....	64
Figure 4-27: OSD View Connection Server + Kiosk Advanced Options.....	65
Figure 4-28: OSD View Connection Server + Kiosk (Advanced Settings).....	65
Figure 4-29: AWI Session Connection Type – View Connection Server + Imprivata OneSign...	69
Figure 4-30: OSD Session Connection Type – View Connection Server + Imprivata OneSign...	70
Figure 4-31: OSD View Connection Server + Imprivata OneSign (Advanced Settings).....	70
Figure 4-32: AWI Connection Type – Connection Management Interface.....	73
Figure 4-33: OSD Session Page – Connection Management Interface.....	74
Figure 4-34: OSD Session Page – Connection Management Interface (Advanced Options)....	74
Figure 4-35: Administrative Web Interface Bandwidth Page.....	76
Figure 4-36: Administrative Web Interface Language Page.....	78
Figure 4-37: OSD Language Page.....	78
Figure 4-38: Administrative Web Interface OSD Page.....	79
Figure 4-39: OSD-OSD Page.....	80
Figure 4-40: Administrative Web Interface Image Page (Host).....	81
Figure 4-41: Administrative Web Interface Image Page (Client).....	81
Figure 4-42: OSD Image Page.....	82
Figure 4-43: Administrative Web Interface Host Driver Function Page.....	84
Figure 4-44: Administrative Web Interface Time Page.....	85
Figure 4-45: Administrative Web Interface Change Password Page.....	86
Figure 4-46: OSD Change Password Page.....	86
Figure 4-47: Administrative Web Interface Reset Page (Client).....	87
Figure 4-48: OSD Reset Page.....	88
Figure 4-49: OSD Display Page.....	89
Figure 4-50: Administrative Web Interface Monitor Emulation Page.....	90
Figure 4-51: OSD Configuration – Hidden Menu Entries Option.....	91
Figure 4-52: Security Configuration – Enable Web Interface Option.....	91
Figure 5-1: Administrative Web Interface USB Page.....	93
Figure 5-2: Administrative Web Interface Audio Page (Host).....	95
Figure 5-3: Administrative Web Interface Power Page (Client).....	96
Figure 6-1: Administrative Web Interface Event Log Page.....	99
Figure 6-2: OSD Event Log Page.....	100
Figure 6-3: Administrative Web Interface Session Control Page.....	102

Figure 6-4: Administrative Web Interface Session Statistics Page (Host).....	103
Figure 6-5: OSD Session Statistics Page.....	104
Figure 6-6: Administrative Web Interface Host CPU Page.....	106
Figure 6-7: Administrative Web Interface Audio Diagnostics Page.....	107
Figure 6-8: Administrative Web Interface Display Page.....	108
Figure 6-9: Administrative Web Interface PCoIP Processor Page.....	109
Figure 6-10: OSD PCoIP Processor Page.....	109
Figure 6-11: OSD Ping Page.....	110
Figure 7-1: Administrative Web Interface Version Page.....	111
Figure 7-2: OSD Version Page.....	112
Figure 7-3: Administrative Web Interface Attached Devices Page (Host).....	113
Figure 7-4: Administrative Web Interface Attached Devices Page (Client).....	113
Figure 8-1: Administrative Web Interface Firmware Page.....	115
Figure 8-2: Administrative Web Interface OSD Logo Upload Page (Client).....	116
Figure 8-3: Administrative Web Interface Certificate Upload Page.....	117
Figure 9-1: OSD Mouse Page.....	118
Figure 9-2: OSD Keyboard Page.....	119
Figure 9-3: OSD Image Page.....	120
Figure 9-4: Display Topology Page.....	121
Figure 9-5: OSD Touch Screen Page.....	123
Figure 10-1: Network Connection Lost Overlay.....	126
Figure 10-2: USB Device Not Authorized Overlay.....	126
Figure 10-3: USB Over Current Notice Overlay.....	127
Figure 10-4: Half Duplex Overlay.....	127
Figure 10-5: No Source Signal Overlay.....	127
Figure 10-6: Source Signal on Other Port Overlay.....	127
Figure 11-1: Accessing the Smart Card Message.....	130
Figure 11-2: Select Certificate Prompt.....	131
Figure 11-3: Certificate Details Window.....	131
Figure 11-4: Smart Card Holder Verification Window.....	132
Figure 12-1: Peer-to-Peer Connect Screen.....	135
Figure 12-2: Client Network Page DHCP Configuration.....	138
Figure 12-3: Host Network Page DHCP Configuration.....	139
Figure 12-4: USB Permissions Example: Class Authorization.....	141
Figure 12-5: USB Permissions Example: Entering Vendor ID and Product ID.....	142

Figure 12-6: USB Permissions Example: Vendor ID and Product ID Authorization..... 142

Table of Tables

Table 1-1: Configuration Menu	20
Table 1-2: Permissions Menu	20
Table 1-3: Diagnostics Menu	20
Table 1-4: Info Menu	21
Table 1-5: Upload Menu	21
Table 1-6: User Settings Menu	21
Table 2-1: Home Page Statistics	27
Table 4-1: Audio Parameters	36
Table 4-2: Network Parameters	37
Table 4-3: Session Parameters (Host)	37
Table 4-4: Session Parameters (Client)	37
Table 4-5: Network Page Parameters	40
Table 4-6: IPv6 Page Parameters	43
Table 4-7: Label Page Parameters	45
Table 4-8: Discovery Page Parameters	46
Table 4-9: SNMP Agent Page Parameters	47
Table 4-10: Session Page Parameters	51
Table 4-11: Session Page Parameters	55
Table 4-12: VMware View Page Parameters	59
Table 4-13: View Connection Server + Auto-Logon Parameters	63
Table 4-14: View Connection Server + Kiosk Parameters	66
Table 4-15: VMware View Page Parameters	71
Table 4-16: Connection Management Page Parameters	75
Table 4-17: Bandwidth Page Parameters	77
Table 4-18: Language Page Parameters	78
Table 4-19: OSD Page Parameters	80
Table 4-20: Image Page Parameters	82
Table 4-21: Time Page Parameters	85
Table 4-22: Change Password Page Parameters	87
Table 4-23: Reset Parameters	88
Table 5-1: USB Page Parameters	94
Table 5-2: USB Device Authorized/Unauthorized Entry Types	95

Table 5-3: Audio Page Parameters.....	96
Table 5-4: Power Page Parameter.....	97
Table 6-1: Event Log Parameters.....	101
Table 6-2: Session Control Page Parameters.....	102
Table 6-3: Session Statistics Page Parameters.....	105
Table 6-4: Host CPU Page Parameters.....	107
Table 6-5: Display Page Parameters.....	108
Table 6-6: PCoIP Processor Page Statistics.....	109
Table 6-7: Ping Page Parameters.....	110
Table 7-1: OSD Version Page Parameters.....	112
Table 7-2: Attached Devices Page Statistics.....	114
Table 8-1: Firmware Page Parameters.....	115
Table 8-2: OSD Logo Page Parameters.....	116
Table 8-3: Administrative Web Interface Certificate Upload Page Parameters.....	117
Table 9-1: Mouse Page Parameters.....	118
Table 9-2: Keyboard Page Parameters.....	119
Table 9-3: Display Topology Page Parameters.....	122
Table 9-4: OSD Touch Screen Page Parameters.....	123

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 zero client 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
SLAAC	Stateless Address Autoconfiguration
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 (a 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 Web Interface (AWI), login details, and onscreen menus.	2
On Screen Display (OSD) Overview	This section describes the OSD, how to log in, and its menus.	3
Configuring the Device	This section describes the options available from the Configuration menu. It covers the available configuration parameters.	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. It also describes how to upload the certificate.	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 lets you see examples of things like setting up a peer-to-peer direct connection, configuring the device for DHCP, and enabling host discovery.	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 (AWI) and On Screen Display (OSD) have various menus and pages. The following table lists the pages according to their menus and if they are available in the AWI, OSD, or both.

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

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
IPv6	Both	Both	4.3
Label	Both	Both	4.4
Discovery	Both	Both	4.5
SNMP	AWI	Both	4.6
Session	Both	Both	4.7
Bandwidth	AWI	Both	4.8
Language	Both	Client	4.9
OSD	Both	Client	4.18
Image <i>Note: In the OSD, this page is available from the User Settings menu</i>	AWI	Both	4.11
Host Driver Function	AWI	Host	4.12
Time	AWI	Both	4.13
Display	OSD	Client	4.16
Password	AWI	Both	4.14
Reset Parameters	Both	Both	4.15
Monitor Emulation <i>Note: This page only appears for older host cards still using monitor emulation.</i>	AWI	Host	4.17

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
Certificate	AWI	Both	8.3

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	4.11
Display Topology	OSD	Client	9.4
Touch Screen	OSD	Client	9.5

2 Administrative Web Interface Overview

The PCoIP Administrative Web Interface (AWI) 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 is an example of an Administrative Web Interface page from a host. Each page (usually) has seven basic regions:

Log Out: Log out and end your Administrative Web Interface.

PCoIP endpoint: Displays PCoIP endpoint information:

- PCoIP® host card
- PCoIP® zero client

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

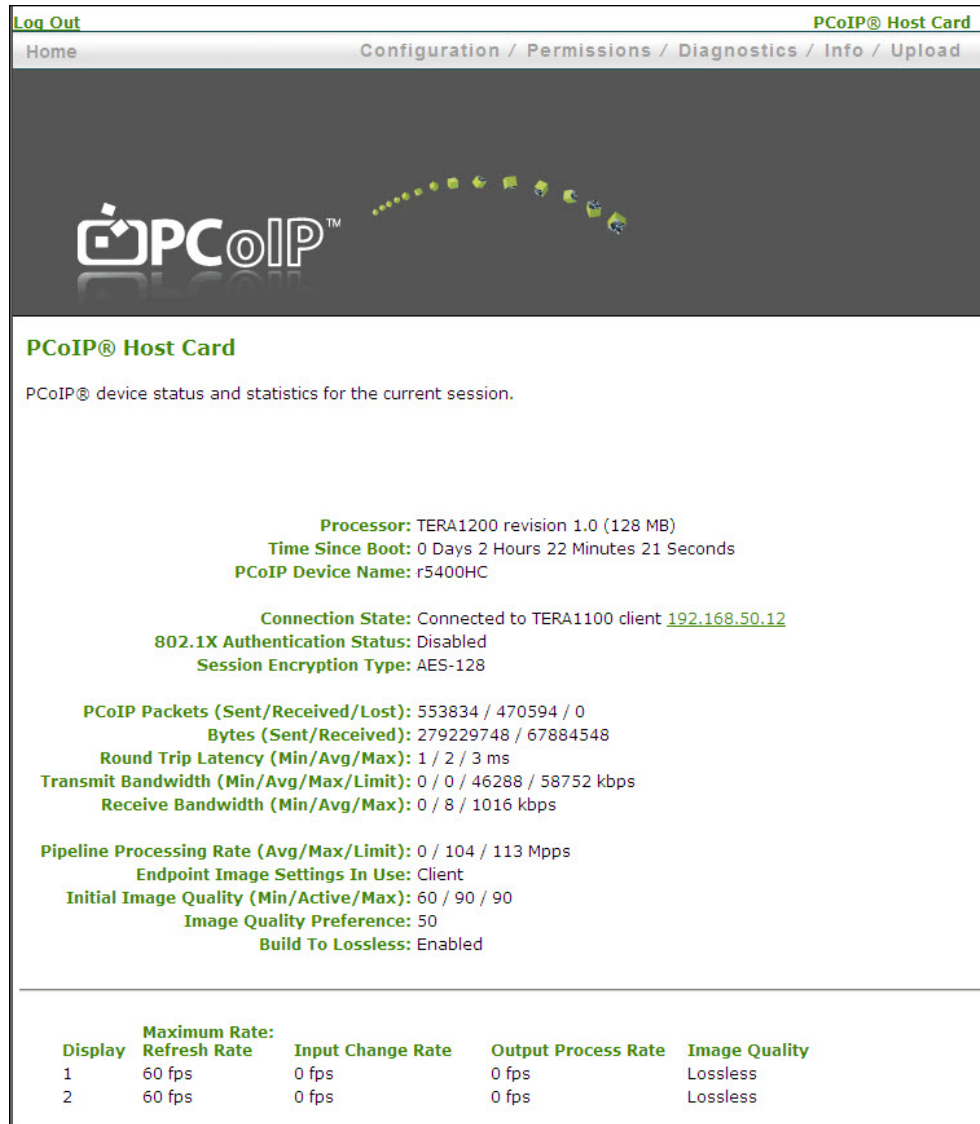
Drop-down menus: The toolbar at the top part of the page lets you easily find pages through its menus: Configuration, Permissions, Diagnostics, Info, and Upload.

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.



Log Out **PCoIP® Host Card**

Home Configuration / Permissions / Diagnostics / Info / Upload

PCoIP® Host Card

PCoIP® device status and statistics for the current session.

Processor: TERA1200 revision 1.0 (128 MB)
Time Since Boot: 0 Days 2 Hours 22 Minutes 21 Seconds
PCoIP Device Name: r5400HC

Connection State: Connected to TERA1100 client [192.168.50.12](#)
802.1X Authentication Status: Disabled
Session Encryption Type: AES-128

PCoIP Packets (Sent/Received/Lost): 553834 / 470594 / 0
Bytes (Sent/Received): 279229748 / 67884548
Round Trip Latency (Min/Avg/Max): 1 / 2 / 3 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 0 / 0 / 46288 / 58752 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 8 / 1016 kbps

Pipeline Processing Rate (Avg/Max/Limit): 0 / 104 / 113 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Active/Max): 60 / 90 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	0 fps	0 fps	Lossless
2	60 fps	0 fps	0 fps	Lossless

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

2.2 Supported Web Browsers

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

- Firefox 8.0 or earlier
- 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. From an Internet browser, enter the IP address of the host or client you want to configure. 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 earlier or later versions.

1. From the **Tools** menu, select **Options**.
2. Click 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". Enable 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., "").

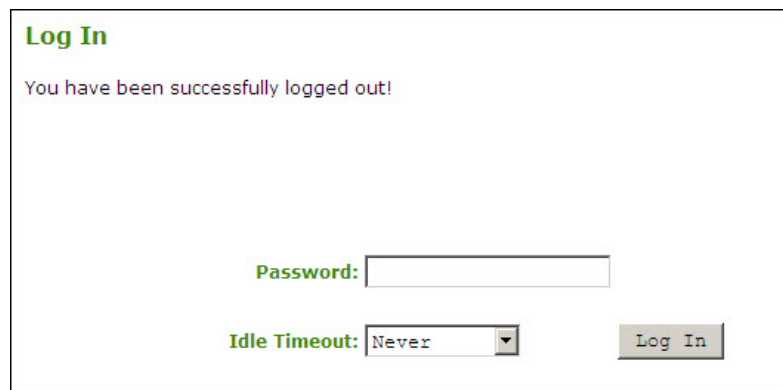


Figure 2-2: Administrative Web Interface Log In Page

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 appears the first time you log in.

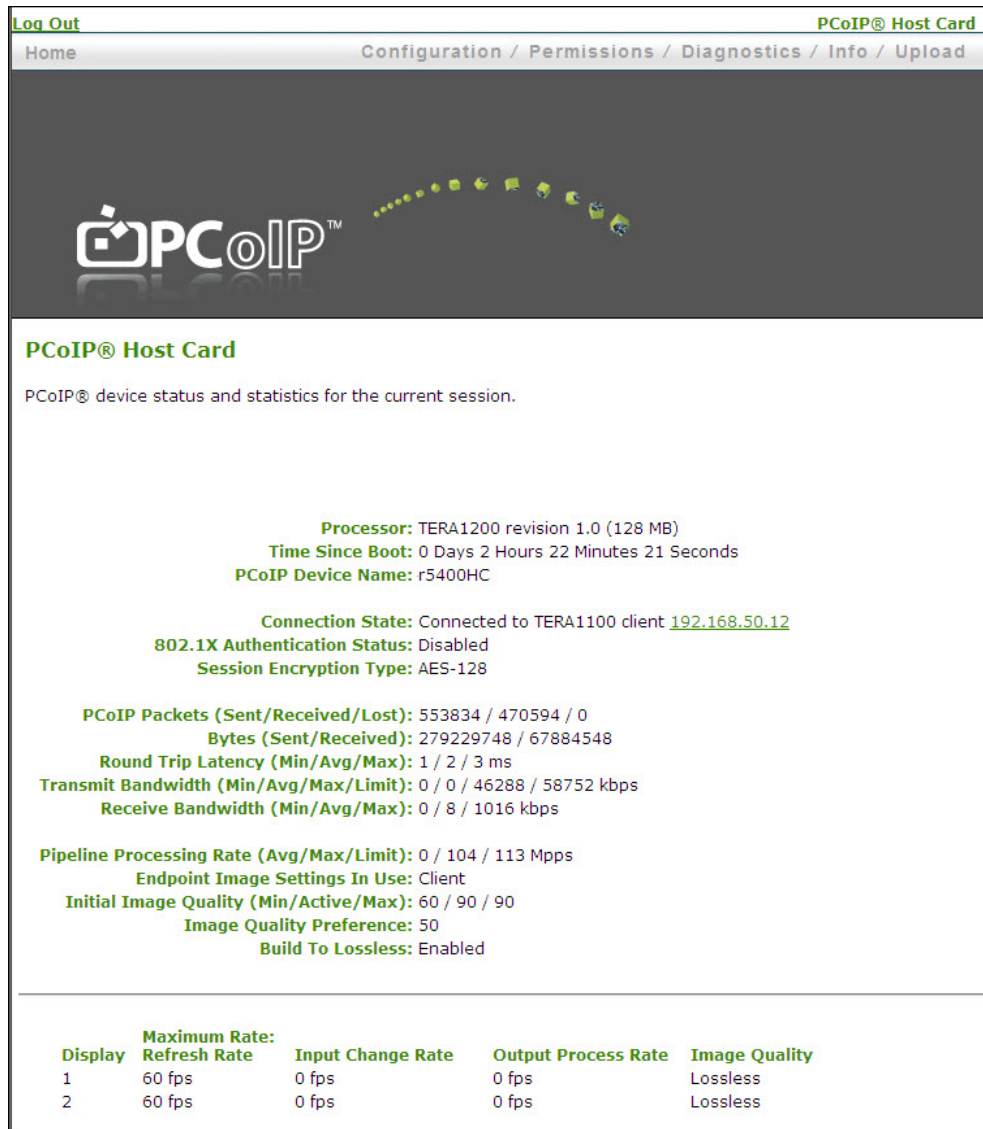
Note: Some PCoIP devices have password protection disabled by default. You do not need a password to login. You can enable or disable password protection for the **Log In** page using the PCoIP Management Console. For details, see the *PCoIP Management Console User Manual* (TER0812002).

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



The screenshot shows the PCoIP Administrative Web Interface. At the top, there is a navigation bar with 'Log Out' on the left and 'PCoIP® Host Card' on the right. Below this is a breadcrumb trail: 'Home Configuration / Permissions / Diagnostics / Info / Upload'. The main content area features the PCoIP logo and a 'PCoIP® Host Card' section. This section provides a summary of the device status and statistics for the current session, including processor information, boot time, device name, connection state, authentication status, encryption type, and various performance metrics like packets sent/received/lost, bandwidth, and processing rates. At the bottom, there is a table showing display settings for two different display configurations.

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	0 fps	0 fps	Lossless
2	60 fps	0 fps	0 fps	Lossless

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

Table 2-1: Home Page Statistics

Statistics	Description	For Further Details
Processor	PCoIP processor type, version, and RAM size	N/A
Time Since Boot	Length of time that the PCoIP processor has been running.	See section 6.3
PCoIP Device Name	The logical name for the device. This field is the name the host or client registers with the DNS server if: <ul style="list-style-type: none"> • DHCP is enabled • the system is configured to support registering the hostname with the DNS server 	See section 4.4
Connection State	Possible states: Disconnected, Connection Pending, Connected. Click the hyperlinked IP address to access the Administrative Web Interfaces for the peer of the host or client.	See section 6.3
802.1X Authentication Status	Identify if the 802.1X authentication is enabled or disabled on the device.	See section 4.2
Session Encryption Type	The type of encryption in use when a session is active: <ul style="list-style-type: none"> • AES-128-GCM • SALSA20-256-Round 12 	See section 4.7
PCoIP Packets	<ul style="list-style-type: none"> • Packets Sent • Packets Received • Packets Lost 	See section 6.3
Bytes	<ul style="list-style-type: none"> • Bytes Sent • Bytes Received 	See section 6.3
Round Trip Latency	Approximate network minimum, average, and maximum round trip latency (e.g., client to host and back to client).	See section 6.3
Transmit Bandwidth:	Minimum, average, and maximum and active limit for traffic transmitted.	See section 6.3
Receive Bandwidth	Minimum, average, and maximum traffic received.	See section 6.3
Pipeline Processing Rate	How much image data is currently being processed by the image engine (in megapixels per second).	N/A
Endpoint Image Settings In Use	Displays whether the image settings being used are configured within the client or within the host. This is based on how the Use Client Image Settings field is configured on the Image page for the host device.	See section 4.11
Initial Image Quality	The minimum and maximum quality setting is taken from the Image page for the device. The active setting is what's currently being used in the session and only appears on the host.	See section 4.11
Image Quality Preference	This setting is taken from the Image Quality	See section 4.11

Statistics	Description	For Further Details
	Preference field on the Image page. The value determines if the image is set to a smoother versus a sharper image.	
Build to Lossless	Options that may appear in this field include: Enabled: The Disable Build to Lossless field on the Image page is disabled. Disabled: The Disable Build to Lossless field is enabled.	See section 4.11
Display	The port number for the display.	N/A
Maximum Rate	This column shows the refresh rate of the attached display. If the Maximum Rate field on the Image page is set to: 0 (that is, there is no limit): The maximum rate is taken from the monitor's refresh rate. A value greater than 0: The refresh rate shows as "User Defined".	See section 4.11
Input Change Rate	The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video).	See section 4.11
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.	N/A
Image Quality	Shows the current lossless state of the attached display: <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless 	See section 4.11

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).

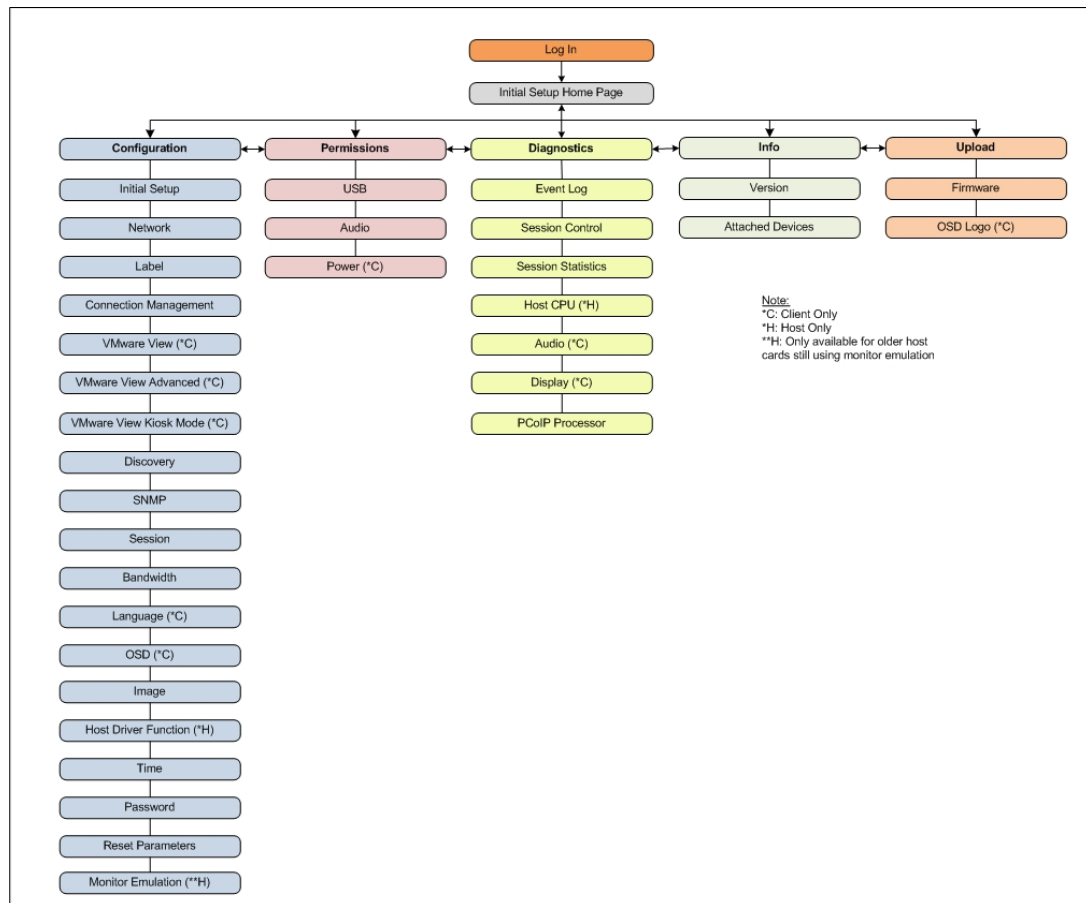


Figure 2-4: Administrative Web Interface Menu Overview

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. 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. 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. 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. 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. 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** window.

The **Connect** window 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** window.

3.1 About the Connect Window

The **Connect** window 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 **Upload** menu.



Figure 3-1: OSD Connect Window

The **Network** icon at the bottom right of the **Connect** window shows the status of the network connection.

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)

Users must wait until the **Network Ready** icon appears.

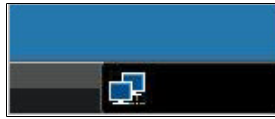


Figure 3-3: Network Ready (detail)

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 the session image appears.



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, see section [4](#).

Diagnostics: This option helps you troubleshoot the device. For details, see section [6](#).

Information: This option lets you view certain details about the device. For details, 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, see section [5](#).

Password: This option lets you update the administrative password for the device. For details, see section [4.14](#).

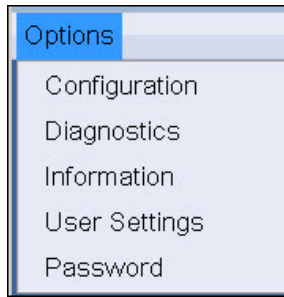


Figure 3-5: OSD Options Menu

4 Configuring the Device

The **Configuration** option on the Administrative Web Interface and OSD lets you configure various aspects for the device. This section describes the full set of configuration options available from the host and the client.

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 later lets you disable the OSD and Administrative Web Interface from the PCoIP Management Console. See sections [4.18](#) and [4.19](#) for more details.

4.1 Initial Setup Page

The **Initial Setup** page contains the configuration parameters that you must set before the client and host devices can be used. 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**.

Initial Setup (1:1 Manual Configuration)

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

Step 1: Audio

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

Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode: Important: If using Microsoft® Windows Vista® / Windows® 7 64-bit Edition, this feature must be enabled for audio to function correctly.

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

Step 2: Network

Enable DHCP:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:

Step 3: Session

Accept Any Client:

Client MAC Address:

Step 4: Apply Changes

Figure 4-1: Initial Setup Page (Host)

Initial Setup (1:1 Manual Configuration)

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

Step 1: Audio

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

Step 2: Network

Enable DHCP:

IP Address: ...

Subnet Mask: ...

Gateway: ...

Primary DNS Server: ...

Secondary DNS Server: ...

Step 3: Session

Identify Host by: IP address FQDN

Host IP Address: ...

Host MAC Address: -----

Step 4: Apply Changes

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	<p>Enables 64-bit mode on the host. This mode should only be used for Windows Vista 64-bit and Windows 7® 64-bit versions to ensure audio works correctly.</p> <p style="color: green;">Note: This option is only available on the host. It does not appear on the client.</p> <p style="color: green;">Note: Enabling 64-bit mode is not required for Linux or Windows XP (32-bit or 64-bit).</p>
Enable Audio Line In	<p>Enable: Use the line-in connector found on the client.</p> <p>Disable: Use the line-in connector as a microphone input. Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device.</p> <p style="color: green;">Note: This option is only available on the host. It does not appear on the client.</p>

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
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 [4.7](#).

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. <i>Note: You cannot set the client MAC address to 0-0-0-0-0.</i>

Table 4-4: Session Parameters (Client)

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 to ignore this field when a session starts.

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

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.

Network

Change the network settings for the device

Enable DHCP:

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

Primary DNS Server: . . .

Secondary DNS Server: . . .

Domain Name:

FQDN:

Ethernet Mode: ▼

Maximum MTU Size: bytes

Enable 802.1X Security:

Authentication: ▼

Identity:

Client Certificate:

Figure 4-3: Administrator Web Interface Network Page

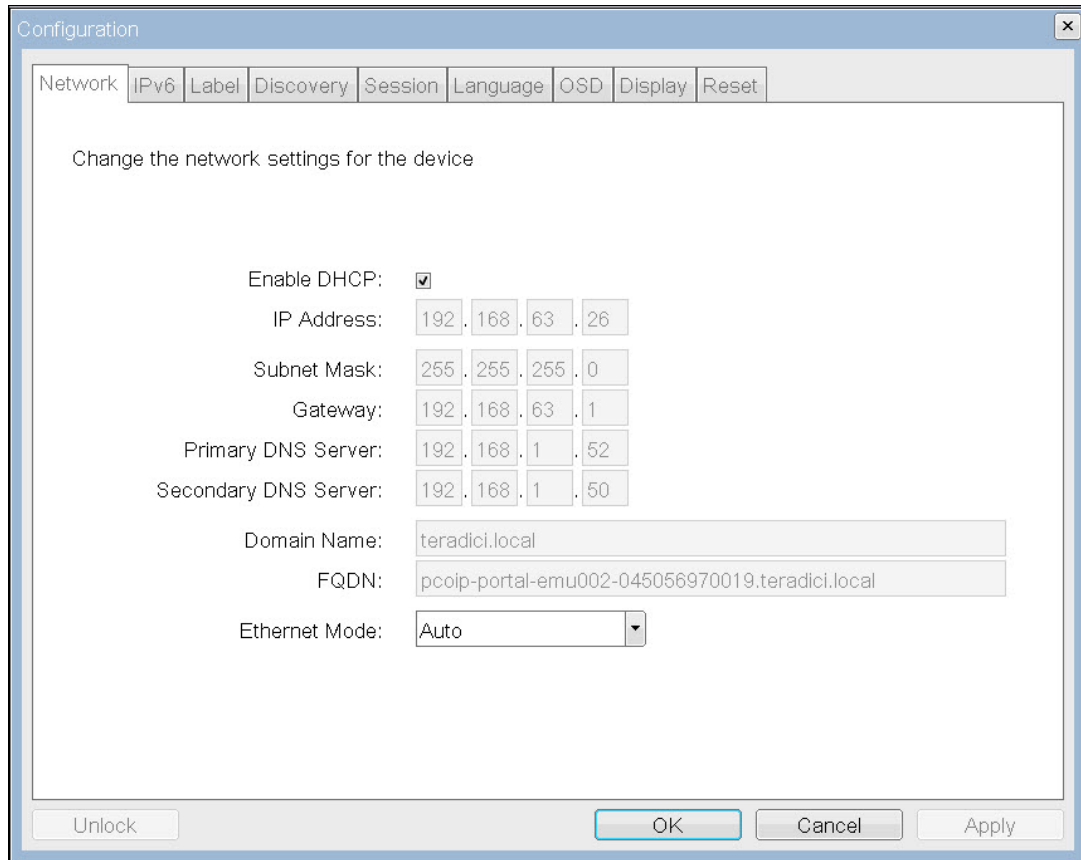


Figure 4-4: OSD Network Page

Table 4-5: Network Page Parameters

Parameter	Description
Enable DHCP	<p>When enabled: The device contacts a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers. The firmware requests a domain name (option 15), host name (option 12), and client FQDN (option 81).</p> <p>When disabled: You must set these parameters manually.</p>
IP Address	The device's IP address. If DHCP is disabled, you must set this field to a valid IP address. If DHCP is enabled, you cannot edit this field.
Subnet Mask	<p>The device's subnet mask. If DHCP is disabled, you must set this field to a valid subnet mask. If DHCP is enabled, you cannot edit this field.</p> <p>Warning: 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.</p>
Gateway	The device's gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, you cannot edit this field.
Primary DNS Server	The device's primary DNS IP address. This field is optional. If the DNS server IP address is configured when using a Connection Manager, the Connection Manager address may be set as an FQDN instead of an IP address.
Secondary DNS Server	The device's secondary DNS IP address. This field is optional. If the DNS server IP address is configured when using a connection manager, the connection manager address may be set as an FQDN instead of an IP address.
Domain Name	The domain named used (for example, 'domain.local'). This field is optional. This field specifies the host or client's domain.
FQDN	<p>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.</p> <p>Note: To use the FQDN feature, the DNS server with DHCP option 81 must be available and properly configured.</p>
Ethernet Mode	<p>Lets you configure the Ethernet mode of the host or client as:</p> <ul style="list-style-type: none"> • Auto • 10 Mbps • Full-Duplex • 100 Mbps Full-Duplex <p>When you choose 10 Mbps Full Duplex or 100 Mbps Full-Duplex and then click Apply, a warning message appears.</p> <p>"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?"</p> <p>Click OK to change the parameter.</p> <p>Note: You should always set the Ethernet Mode to Auto and only use 10 Mbps Full-Duplex or 100 Mbps Full-Duplex when the other network equipment (for example, switch) is also configured to operate at 10 Mbps full-duplex or 100 Mbps full-duplex. An improperly set Ethernet</p>

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	<p>Lets you configure the Maximum Transfer Unit packet size.</p> <p>A smaller MTU may be needed for situations such as VPN tunneling because PCoIP packets cannot be fragmented. Set the Maximum MTU Size to a value smaller than the network path MTU for the end-to-end connection between the host and client.</p> <p>The Maximum MTU Size range is 500 to 1500 bytes.</p> <p>Note: The default MTU is 1400 for sessions between PCoIP zero clients and PCoIP host cards.</p> <p>The default MTU is 1300 for sessions with PCoIP software (in the host or client) such as VMware View.</p>
Enable 802.1X Security	Enable this field for each of your hosts and zero clients if your network uses 802.1X security. If enabled, configure the Authentication , Identity , and Client Certificate fields.
Authentication	This field is set to TLS (Transport Layer Security) and is grayed-out. TLS is currently the only authentication protocol supported by the PCoIP protocol.
Identity	Enter the identity string used to identify your device to the network.
Client Certificate	<p>Click Choose to select the client certificate you want to use for your 802.1X devices. The list of certificates that appears includes the certificates uploaded from the Certificate Upload page. The certificate you choose from the Network page is linked to the read-only Client Certificate field on the Certificate Upload page.</p> <p>Note: PCoIP only supports one 802.1X client certificate. Ensure your security details are all contained within the one file.</p>

4.3 Configuring the IPv6 Settings for a Device

The IPv6 page lets you enable IPv6 for PCoIP devices connected to your IPv6 network.

Note: IPv6 is not currently supported by VMware View.

IPv6

Change the IPv6 network settings for the device

Enable IPv6:

Link Local Address:

Gateway:

Enable DHCPv6:

Primary DNS:

Secondary DNS:

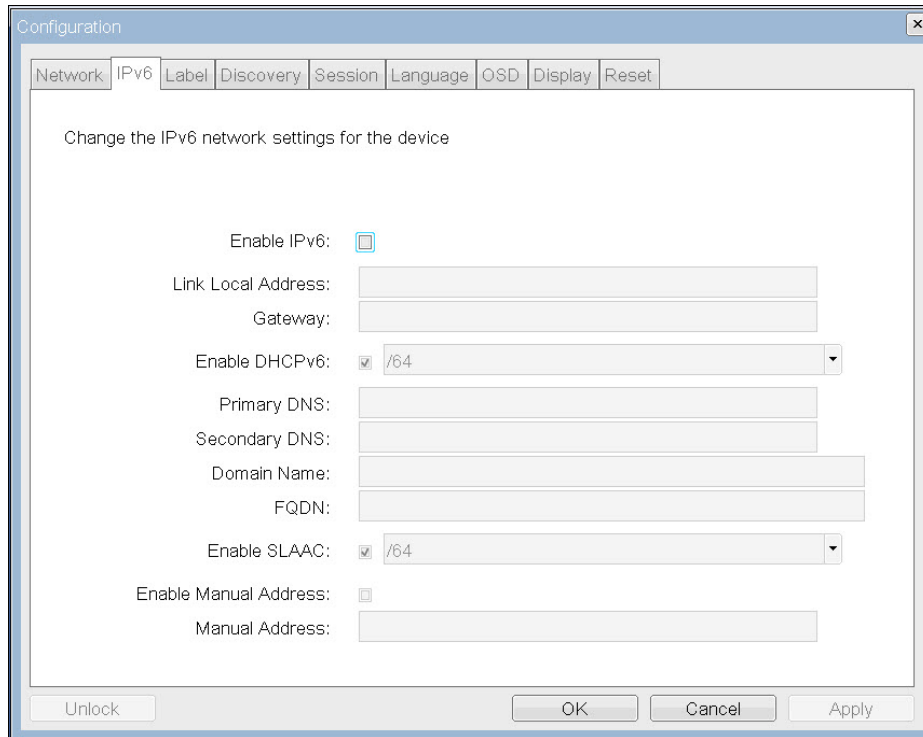
Domain Name:

FQDN:

Enable SLAAC:

Enable Manual Address:

Figure 4-5: Administrative Web Interface IPv6 Page


Figure 4-6: OSD IPv6 Page
Table 4-6: IPv6 Page Parameters

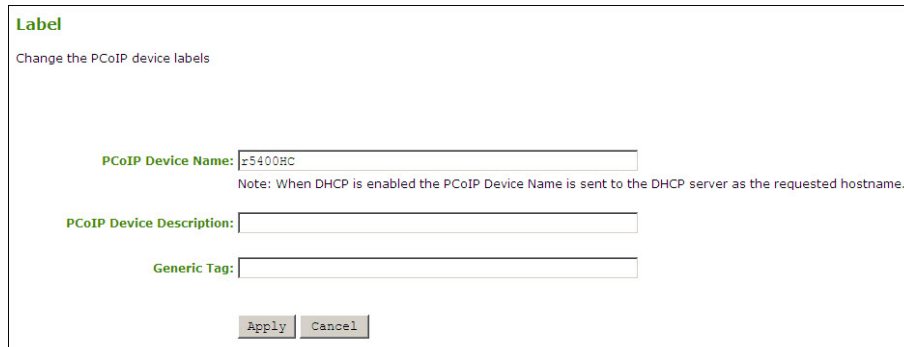
Note: When you make a change to one of the settings on this page, you must reboot your device for the change to take effect.

Parameter	Description
Enable IPv6	Enable this field to enable IPv6 for your PCoIP devices.
Link Local Address	This field is autopopulated.
Gateway	Enter the gateway address.
Enable DHCPv6	Enable this field to set up Dynamic Host Configuration Protocol version 6 (DHCPv6) for your device.
DHCPv6 Addresses	When DHCPv6 is enabled and the device is rebooted, the server autopopulates these fields with addresses for the device.
Primary DNS	The device's primary DNS IP address. If DHCPv6 is enabled, this field is autopopulated by the DHCPv6 server.
Secondary DNS	The device's secondary DNS IP address. If DHCPv6 is enabled, this field is autopopulated by the DHCPv6 server.
Domain Name	The domain name used (for example, 'domain.local') for the host or client. If DHCPv6 is enabled, this field is autopopulated by the DHCPv6 server.
FQDN	The fully qualified domain name for the host or client. If DHCPv6 is enabled, this field is autopopulated by the DHCPv6 server.
Enable SLAAC	Enable this field to set up stateless address auto-configuration (SLAAC) for your devices.
SLAAC Addresses	When SLAAC is enabled and the device is rebooted, these fields are autopopulated.

Parameter	Description
Enable Manual Address	Enable this field to set up a manual (static) address for the device.
Manual Address	Enter the IP address for the device.

4.4 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.



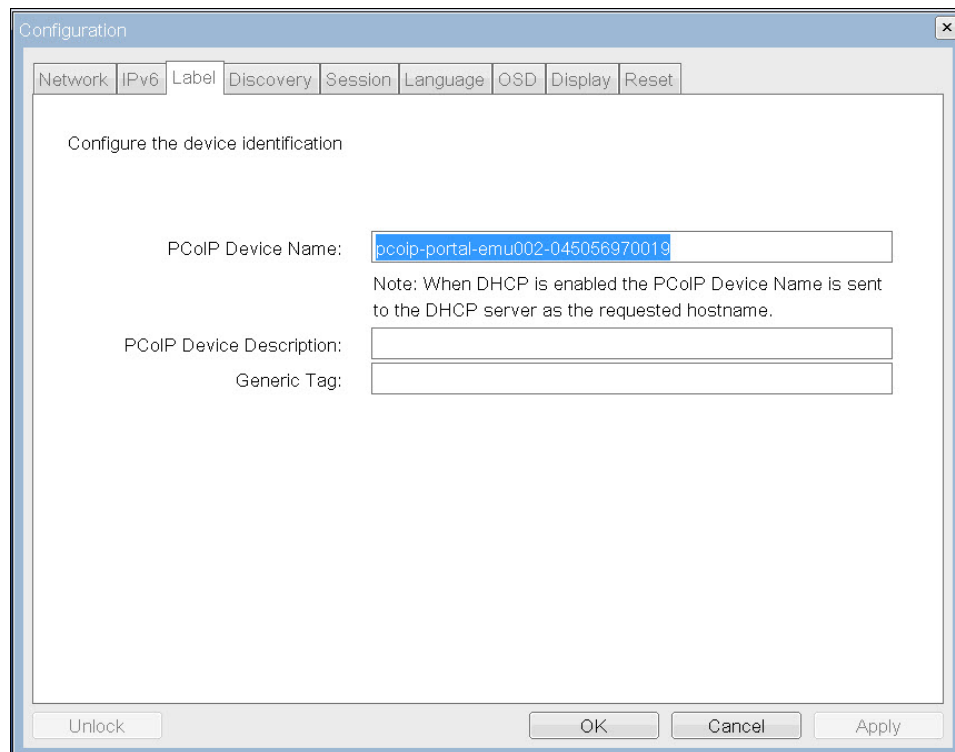
Label
Change the PCoIP device labels

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

PCoIP Device Description:

Generic Tag:

Figure 4-7: Administrative Web Interface Label Page



Configuration

Network | IPv6 | **Label** | Discovery | Session | Language | OSD | Display | Reset

Configure the device identification

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

PCoIP Device Description:

Generic Tag:

Figure 4-8: OSD Label Page

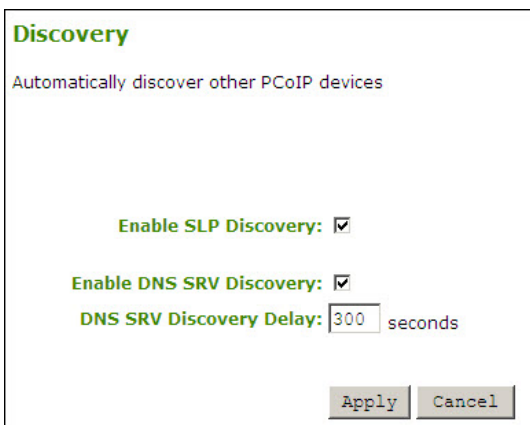
Table 4-7: Label Page Parameters

Parameter	Description
PCoIP Device Name	<p>Lets you give the host or client a logical name. The default is pcoip-host-<MAC> or pcoip-portal-<MAC> where <MAC> is the device's MAC address.</p> <p>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.</p> <p>It's important to ensure that the PCoIP Device Name is unique for each endpoint in the network and follows these naming conventions:</p> <ul style="list-style-type: none"> • The first and last character must be a letter (A-Z or a-z) or a digit (0-9) • The remaining characters must be letters, digits, or hyphens • The length must be 63 characters or less
PCoIP Device Description	A description or other information (such as the location of the endpoint) 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.

4.5 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 4-9: Administrative Web Interface Discovery Page

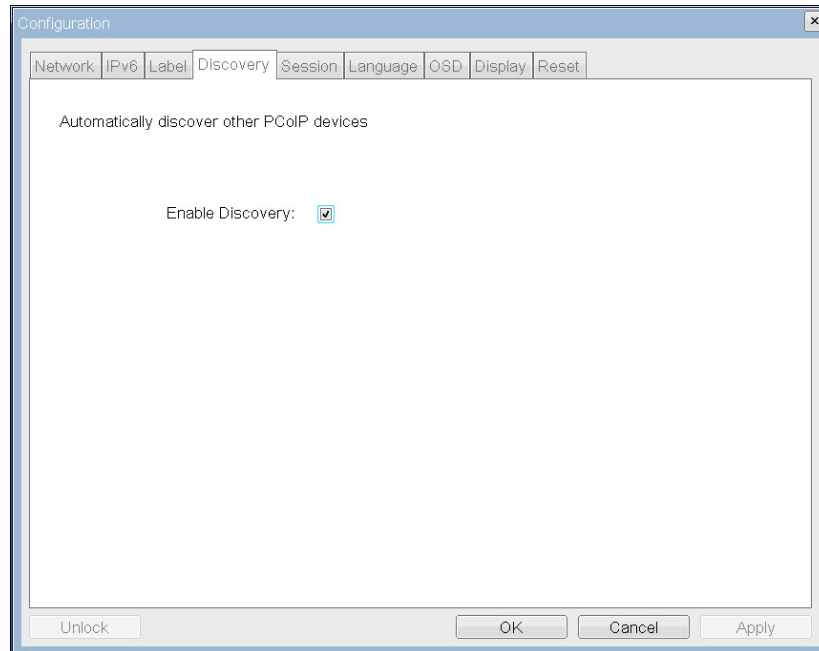


Figure 4-10: OSD Discovery Page

Table 4-8: 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 DNS SRV Discovery	<p>When enabled:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
DNS SRV Discovery Delay	<p>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.</p> <p>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.</p>

4.6 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 \(TER0805002\)](#).

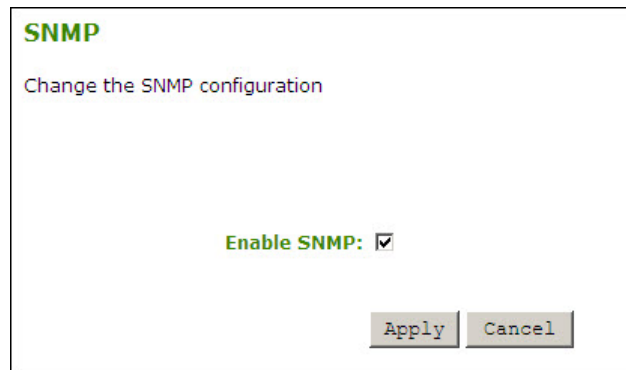


Figure 4-11: Administrative Web Interface SNMP Agent Page

Table 4-9: 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.

4.7 Configuring the Session

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

The **Advanced** configuration options available from the **Session** page depend on the option you select in the **Session Connection Type** field:

Session Connection Type Field Option	Available from Client/Host
Direct from Client	Host
Direct to Host	Client
Direct to Host + SLP Host Discovery	Client
View Connection Server	Client
View Connection Server + Auto-Logon	Client
View Connection Server + Kiosk	Client
View Connection Server + Imprivata OneSign	Client
Connection Management Interface	Host/Client

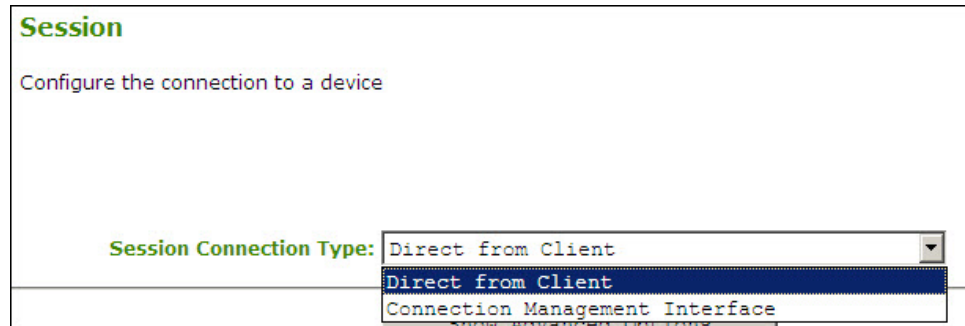


Figure 4-12: AWI Session Connection Type Options (Host)

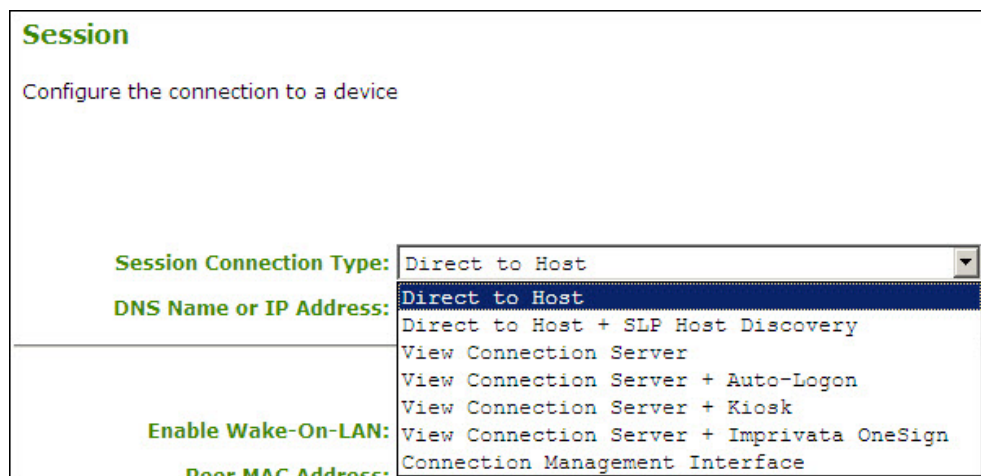


Figure 4-13: AWI Session Connection Type Options (Client)

4.7.1 Configuring a Direct Session

When you select a direct session connection type from the Session page, specific configuration options appear.

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, you must enter the peer (client) MAC address.

Session

Configure the connection to a device

Session Connection Type: Direct from Client

Hide Advanced Options

Accept Any Peer:

Peer MAC Address: 00 - 30 - 04 - 0D - 1A - 6C

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Apply Cancel

Figure 4-14: AWI Session Connection Type – Direct from Client (Host)

Session

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 192.168.42.76

Hide Advanced Options

Enable Wake-On-LAN:

Peer MAC Address: 00 - 0C - 87 - 00 - 8A - 53

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply Cancel

Figure 4-15: AWI Session Connection Type – Direct to Host (Client)

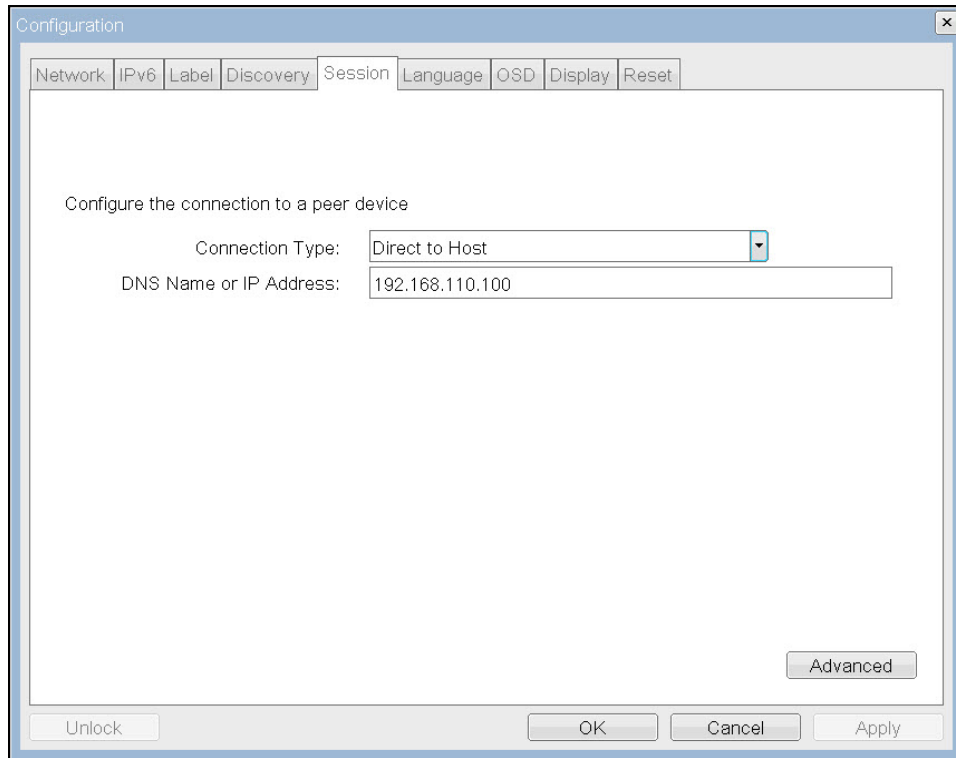


Figure 4-16: OSD Session Connection Type – Direct to Host

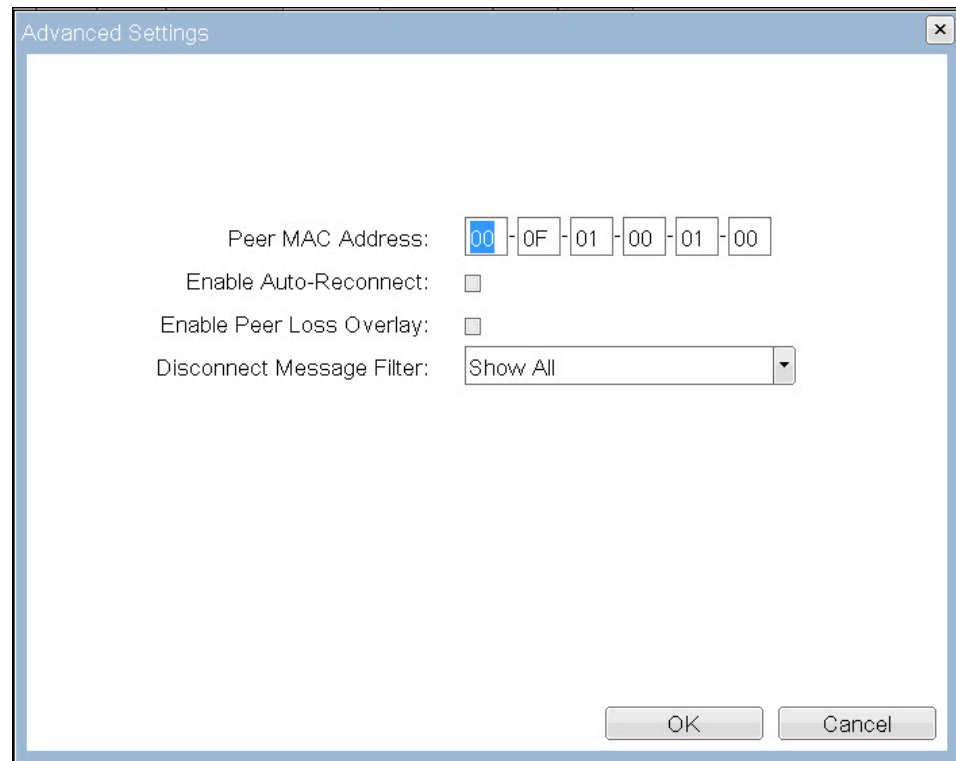


Figure 4-17: OSD Session Connection Type – Direct to Host (Advanced Settings)

Table 4-10: Session Page Parameters

Parameters	Description
DNS Name or IP Address	Enter the IP address or DNS name for the host. Note: This setting is only available on the client.
Accept Any Peer	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 setting is only available on a host.
Enable Wake-On-LAN	Enable this field to automatically turn on the host when the user presses the Remote Power button or clicks the Connect button on the Connect window. Note: <ul style="list-style-type: none"> The feature only works with hardware hosts. (It does not work with software hosts as they cannot be put into a low-power state.) The hardware host must be able to support waking from low power state (off/hibernate/sleep) when it receives a wake-on-LAN packet
Peer MAC Address	If you are configuring the host, enter the MAC address of the client that is allowed to connect to the host. If the Accept Any Peer option is enabled, these fields are not required and not editable on the host. If you are configuring the client and Enable Wake-On-LAN is enabled, enter the MAC address for the host. The "magic packet" sent from the zero client to "wake up" the host is made up of numerous repetitions of the host's MAC address.
Enable Auto-Reconnect	When enabled, it lets the client automatically reconnect with the last connected host when a session is lost. Note: This setting is only available for the client.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. 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 setting is only available on the client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.
Enable AES-128-GCM	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: <ul style="list-style-type: none"> Host to client: AES-128-GCM for the PCoIP session VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable SALSA20-256-Round 12	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 later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.)

Parameters	Description
	<p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User or administrator initiated actions affecting the session.</p> <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect <p>Warning: System-initiated, but expected actions affecting the session. This occurs when a session is closed remotely (the global timeout value is reached).</p> <p>Error: Unexpected system-initiated actions causing session to fail. The following are Error messages:</p> <ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages <p>Note: This setting is only available for the zero client.</p>

4.7.2 Configuring a Direct Session with SLP Host Discovery

If you are connecting a client to a host using SLP discovery, select the **Direct to Host + SLP Discovery** option in the **Session Connection Type** field on the **Session** page. Click the **Show Advanced Options** button, and then configure the **Advanced Options** for your session.

Note: This session connection type is only available on the client. It is not available on the host.

Session

Configure the connection to a device

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

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

Hide Advanced Options

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply Cancel

Figure 4-18: AWI Session Connection Type – Direct from Host with SLP Host Discovery

Configuration

Network IPv6 Label Discovery **Session** Language OSD Display Reset

Configure the connection to a peer device

Connection Type: Direct to Host + SLP Host Discovery

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

Advanced

Unlock OK Cancel Apply

Figure 4-19: OSD Session Connection Type – Direct to Host with SLP Host Discovery

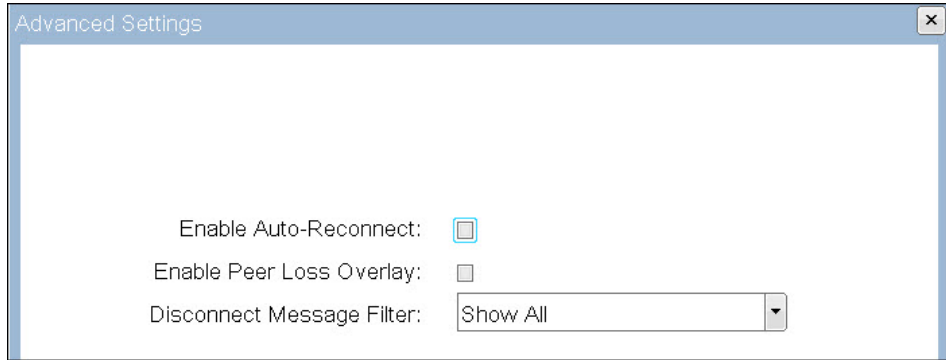


Figure 4-20: OSD Session Connection Type – Direct to Host with SLP Host Discovery (Advanced Settings)

Table 4-11: Session Page Parameters

Parameters	Description
Enable Auto-Reconnect	Lets the client automatically reconnect with the last connected host when a session is lost. Note: This setting is only available on a client.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. 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 setting is only available on a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.
Enable AES-128-GCM	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: <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable SALSA20-256-Round 12	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 later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.) 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: <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: Information: User or administrator initiated actions affecting the session. <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect Warning: System-initiated, but expected actions affecting the session. This occurs when a session is closed remotely (the global timeout value is reached). Error: Unexpected system-initiated actions causing session to fail. The following are Error messages:

Parameters	Description
	<ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages


4.7.3 Configuring a VMware View Connection

The **Session** page lets you configure your client for use with a VMware View Connection server. When you select **View Connection Server** as the **Session Connection Type**, specific configuration options appear.

Note: This session connection type is only available on the client. It is not available on the host.

Session

Configure the connection to a device



Session Connection Type: View Connection Server

DNS Name or IP Address: viewdesktop.teradici.com

Hide Advanced Options

Desktop Name to Select:

Port: (Leave blank for default)

SSL: Use secure connection (SSL)

Auto Connect: Always connect to this server at startup

Connection Server Cache Mode: Last servers used Clear cache entries

Enable Self Help Link:

Auto Launch If Only One Desktop:

Login Username Caching:

Use OSD Logo for View banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply
Cancel

Figure 4-21: AWI Session Connection Type – View Connection Server

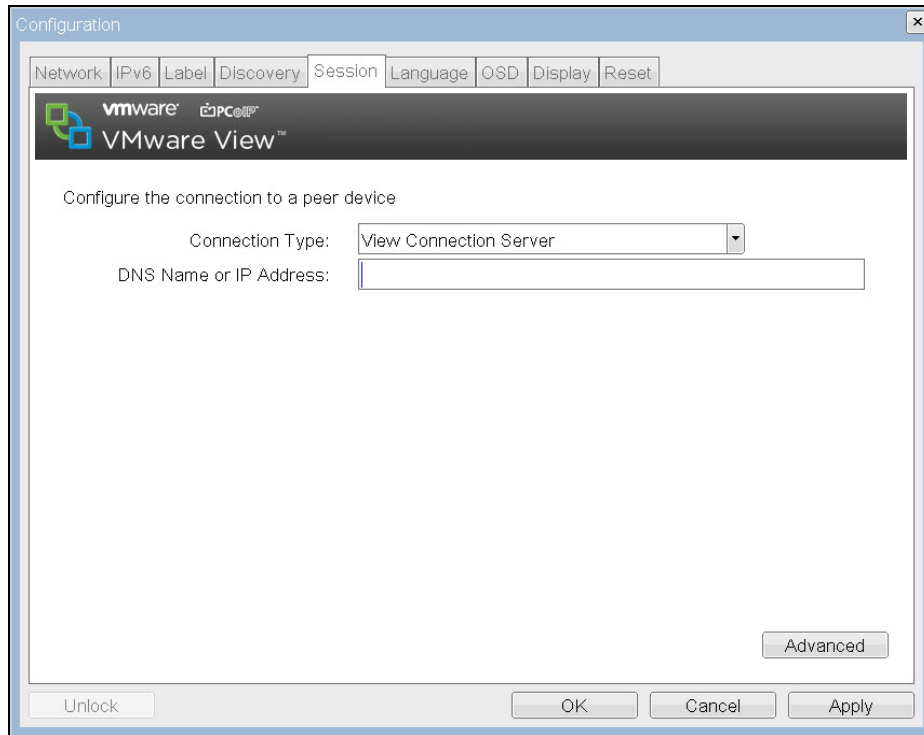


Figure 4-22: OSD Session Connection Type – View Connection Server

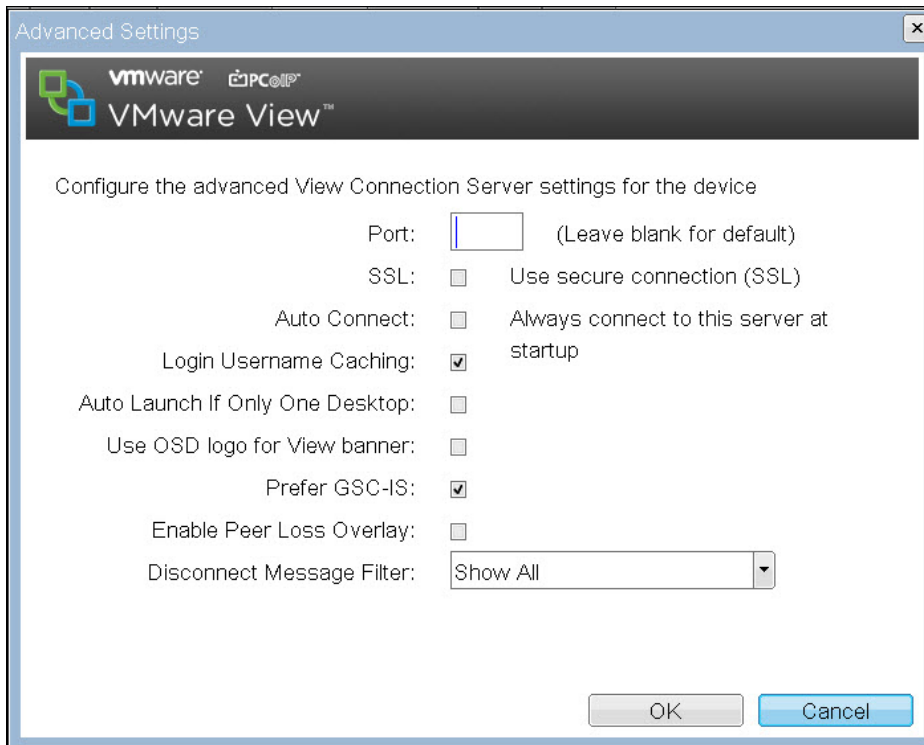


Figure 4-23: OSD Session Connection Type – View Connection Server (Advanced Options)

Table 4-12: VMware View Page Parameters

Parameter	Description															
DNS Name or IP Address	Enter the IP address or DNS name for the View Connection server.															
Desktop Name to Select	Enter the pool/desktop name used by a zero client when starting a session.															
Port	<p>Specify the port used to communicate to the VMware View Connection server. The Port field works with the SSL field setting.</p> <p>If SSL is enabled and the port number is blank, port 443 is used. By default, the Port field is blank.</p> <p>If SSL is disabled and the port number is blank, port 80 is used. By default, the Port field is blank.</p> <p>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.</p> <p>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.</p>															
SSL	<p>Specify if you want the client to communicate with the VMware View Connection server over a secure connection using SSL.</p> <p>You can configure the SSL setting in both the VMware View Connection server and from the Session page. 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 Session page appear in the following table.</p> <table border="1" data-bbox="647 1079 1406 1314"> <thead> <tr> <th colspan="2"></th> <th colspan="2">VMware View Connection Server</th> </tr> <tr> <th colspan="2"></th> <th>SSL disabled</th> <th>SSL enabled</th> </tr> </thead> <tbody> <tr> <th rowspan="2">Session Page</th> <th>SSL disabled</th> <td>SSL disabled</td> <td>SSL enabled</td> </tr> <tr> <th>SSL enabled</th> <td>View Connection server communication error</td> <td>SSL enabled</td> </tr> </tbody> </table> <p>For example, if SSL is enabled in the VMware View Connection server but is disabled from the Session page, the resulting SSL mode is enabled.</p> <p>By default, the SSL field is enabled.</p> <p>Note: For security, we recommend using Port 443 and enabling SSL from the Session 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.</p> <p>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 setting.</p>			VMware View Connection Server				SSL disabled	SSL enabled	Session Page	SSL disabled	SSL disabled	SSL enabled	SSL enabled	View Connection server communication error	SSL enabled
		VMware View Connection Server														
		SSL disabled	SSL enabled													
Session Page	SSL disabled	SSL disabled	SSL enabled													
	SSL enabled	View Connection server communication error	SSL enabled													
Auto Connect	<p>Specify if the client should always connect with the VMware View Connection server at startup.</p> <p>When Auto connect is enabled, the client automatically connects to the VMware View Connection server whenever the client powers up or</p>															

Parameter	Description
	<p>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</p> <p>After enabling auto connect, the client must be power-cycled for the change to take effect.</p>
Connection Server Cache Mode	<p>Set this field to:</p> <ul style="list-style-type: none"> Last 25 servers used: These appear on the Connection Server entry box on the OSD VMware View Connect page. Read-only <p>Note: You can use the PCoIP Management Console to pre-populate the list of available connection servers.</p>
Enable Self Help Link	See the following section for details.
Auto Launch If Only One Desktop	<p>When enabled, after user credentials are entered, users are automatically connected to their virtual desktop.</p> <p>Note: This feature only applies to users who are entitled to a single desktop. It does not apply to users entitled to multiple virtual desktops.</p>
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	<p>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.</p> <p>Prefer GSC-IS is selected by default.</p>
Enable Peer Loss Overlay	<p>When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. 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.</p> <p>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.</p>
Enable AES-128-GCM	<p>AES-128-GCM is an encryption method implemented in the TERA1x100 processor that allows best performance between hardware endpoints.</p> <p>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:</p> <ul style="list-style-type: none"> Host to client: AES-128-GCM for the PCoIP session VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable SALSA20-256-Round 12	<p>SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 or later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.)</p>

Parameter	Description
	<p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User or administrator initiated actions affecting the session.</p> <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect <p>Warning: System-initiated, but expected actions affecting the session. This occurs when a session is closed remotely (the global timeout value is reached).</p> <p>Error: Unexpected system-initiated actions causing session to fail. The following are Error messages:</p> <ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages.

Enabling the Self Help Link

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

Enable Self Help Link:

View Connection Server:

Port: (Leave blank for default)

SSL: Use secure connection (SSL)

Username:

Password:

Domain:

Desktop Name to Select:

Link Text:

Figure 4-24: Enable Self Help Link Options

When you enable this field, the following options appear:

Parameter	Description
View Connection Server	Enter the name of the View Connection Server hosting the self-help virtual machine.
Port	Specify the port used to communicate to the VMware View Connection server.
SSL	Specify if you want the client to communicate with the VMware View Connection server for the self-help link over a secure connection using SSL.
Username	To password protect the virtual machine for the self-help link, enter a username in this field.
Password	To password protect the virtual machine for the self-help link, enter a password in this field.
Domain	Enter the domain name used by the virtual machine for the self-help link.
Desktop Name to Select	Enter the pool/desktop name used by the virtual machine for the self-help link.
Link Text	Enter the text that you want to appear as hyperlinked text on the Connect window.

Configuring the VMware View Connection with Auto-Logon


You can set up the client so that the user does not need to enter a username or password to start a VMware View session (that is, the usual login details are automatically entered for the user). Select the **View Connection Server + Auto-Logon** option from **Session Connection Type** field on the **Session** page.

When you choose this connection type, the parameters are the same appear for the View Connection Server with the exception of those parameters highlighted in the following table.

Note: This session connection type is only available from the Administrative Web Interface. It is not available from the OSD.

Session

Configure the connection to a device



Session Connection Type: View Connection Server + Auto-Logon

DNS Name or IP Address:

Logon Username:

Logon Password:

Logon Domain Name:

Desktop Name to Select:

Port: (Leave blank for default)

SSL: Use secure connection (SSL)

Auto Connect: Always connect to this server at startup

Connection Server Cache Mode: Last servers used

Auto Launch If Only One Desktop:

Use OSD Logo for View banner:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Figure 4-25: View Connection Server with Auto-Logon

Table 4-13: View Connection Server + Auto-Logon Parameters

Parameter	Description
Logon Username	Enter the username for the client.
Logon Password	Enter the password.
Logon Domain Name	Enter the domain name.


4.7.4 Configuring Kiosk Mode

You can configure kiosk mode by selecting the **View Connection Server + Kiosk** option as the **Session Connection Type** on the **Session** page on 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.

Note: This session connection type is only available on the client. It is not available on the host.

Session

Configure the connection to a device



Session Connection Type: View Connection Server + Kiosk

DNS Name or IP Address: viewdesktop.teradici.com

Username Type: Zero Client MAC

Username: cm-00:30:04:0D:1A:6C

Password:

Hide Advanced Options

Port: (Leave blank for default)

SSL: Use secure connection (SSL)

Use OSD Logo for View banner:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply
Cancel

Figure 4-26: AWI Session Connection Type View Connection Server + Kiosk

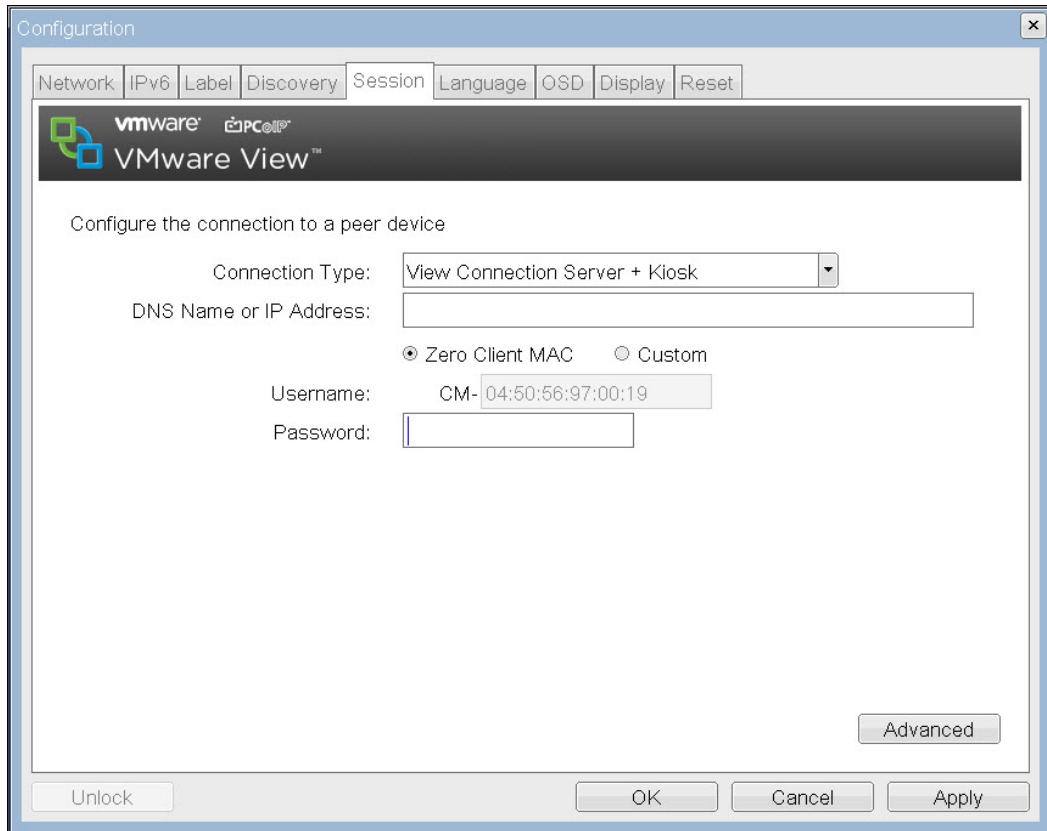


Figure 4-27: OSD View Connection Server + Kiosk Advanced Options

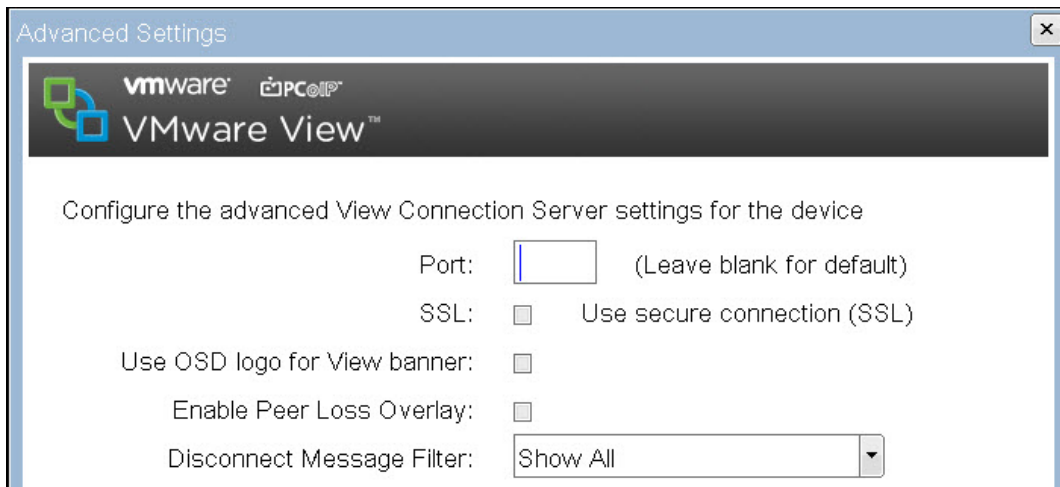


Figure 4-28: OSD View Connection Server + Kiosk (Advanced Settings)

Table 4-14: View Connection Server + Kiosk Parameters

Parameters	Description															
DNS Name or IP Address	Enter the IP address or DNS name for the kiosk's View Connection Server.															
Username Type	Select the type of username that matches the naming you use for the devices on the View Connection Server. <ul style="list-style-type: none"> Zero Client MAC: Select this option to autopopulate the Username field with the MAC address of the zero client. Custom: Enter the username for the zero client. This username has the prefix "Custom". 															
Password	To password protect the virtual machine for the kiosk, enter a password in this field. This password must match the one entered for the device in the View Connection Server.															
Port	Specify the port used to communicate to the VMware View Connection server. The Port field works with the SSL field setting. 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.															
SSL	Specify if you want the client to communicate with the VMware View Connection server over a secure connection using SSL. You can configure the SSL setting in both the VMware View Connection server and from the Session page. 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 Session page appear in the following table. <table border="1" data-bbox="646 1335 1403 1570"> <thead> <tr> <th colspan="2"></th> <th colspan="2">VMware View Connection Server</th> </tr> <tr> <th colspan="2"></th> <th>SSL disabled</th> <th>SSL enabled</th> </tr> </thead> <tbody> <tr> <th rowspan="2">Session Page</th> <th>SSL disabled</th> <td>SSL disabled</td> <td>SSL enabled</td> </tr> <tr> <th>SSL enabled</th> <td>View Connection server communication error</td> <td>SSL enabled</td> </tr> </tbody> </table> For example, if SSL is enabled in the VMware View Connection server but is disabled from the Session page, the resulting SSL mode is enabled. By default, the SSL field is enabled. Note: For security, we recommended using Port 443 and enabling SSL from the Session 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			VMware View Connection Server				SSL disabled	SSL enabled	Session Page	SSL disabled	SSL disabled	SSL enabled	SSL enabled	View Connection server communication error	SSL enabled
		VMware View Connection Server														
		SSL disabled	SSL enabled													
Session Page	SSL disabled	SSL disabled	SSL enabled													
	SSL enabled	View Connection server communication error	SSL enabled													

Parameters	Description
	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 setting.
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.
Enable Peer Loss Overlay	When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. It also appears in the case of a virtual desktop such as VMware View. Normal hypervisor scheduling delays can falsely trigger this message. This option is disabled by default. Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.
Enable AES-128-GCM	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: <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable Salsa20-256-Round12	SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 or later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.) 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: <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: Information: User or administrator initiated actions affecting the session. <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect Warning: System-initiated, but expected actions affecting the session. This occurs when a session is closed remotely (the global timeout value is reached). Error: Unexpected system-initiated actions causing session to fail.

Parameters	Description
	<p>The following are Error messages:</p> <ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages

4.7.5 Configuring a View Connection Server + Imprivata OneSign Connection

If you use the Imprivata OneSign system in your network, you need to configure the **View Connection Server + Imprivata OneSign** option as the **Session Connection Type** on the **Session** page.

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

Session

Configure the connection to a device

Session Connection Type: View Connection Server + Imprivata OneSign

Bootstrap URL:

Hide Advanced Options

Login Username Caching:

Use OSD Logo for View banner:

Prefer GSC-IS:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply
Cancel

Figure 4-29: AWI Session Connection Type – View Connection Server + Imprivata OneSign

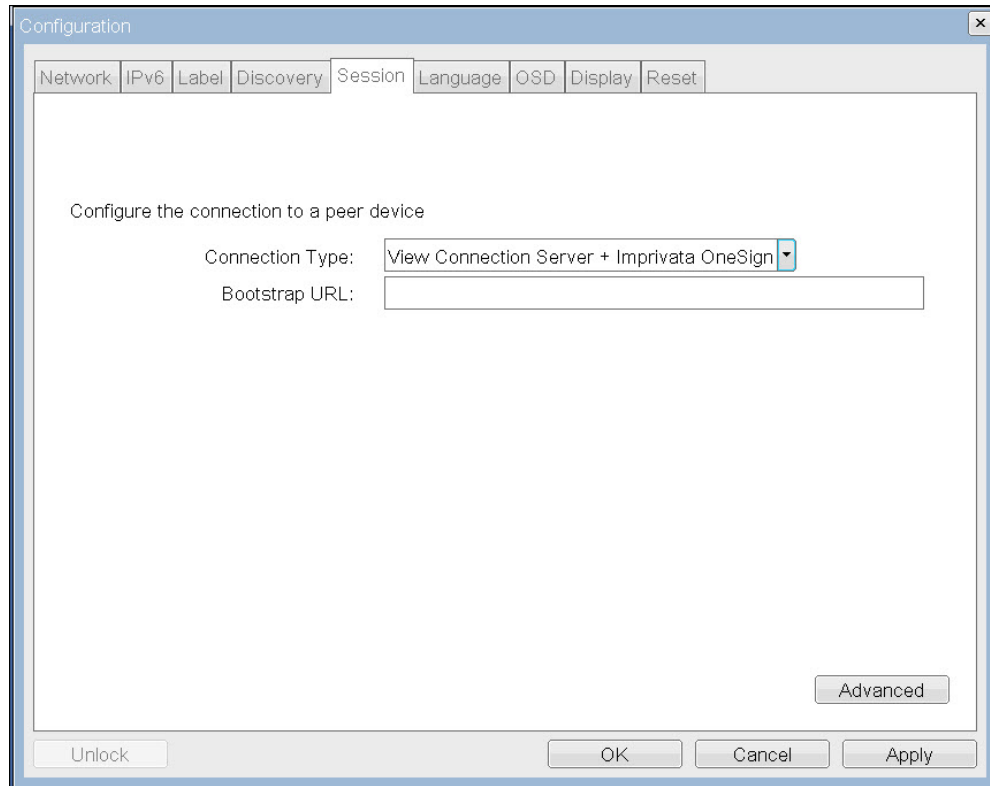


Figure 4-30: OSD Session Connection Type – View Connection Server + Imprivata OneSign

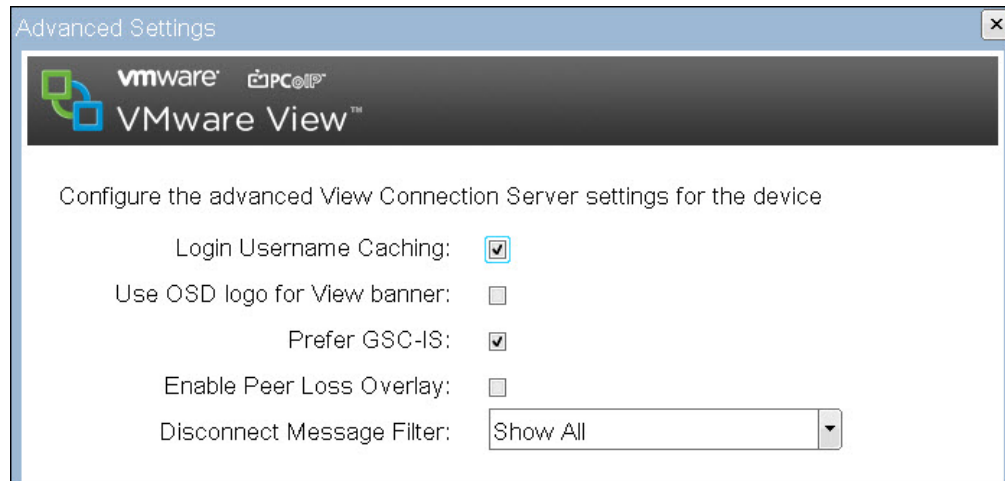


Figure 4-31: OSD View Connection Server + Imprivata OneSign (Advanced Settings)

Table 4-15: VMware View Page Parameters

Parameter	Description
Bootstrap URL	Enter the address of the OneSign Server.
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.
Enable Peer Loss Overlay	<p>When enabled, the "Network Connection Lost" overlay appears on the display(s) when a loss of network connectivity is detected. 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.</p> <p>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.</p>
Enable AES-128-GCM	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable SALSA20-256-Round 12	<p>Configure SALSA20-256-Round 12 encryption for the client. SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 or later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.)</p> <p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User or administrator initiated actions affecting the session.</p> <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect <p>Warning: System-initiated, but expected actions affecting the session.</p>

Parameter	Description
	<p>This occurs when a session is closed remotely (the global timeout value is reached).</p> <p>Error: Unexpected system-initiated actions causing session to fail. The following are Error messages:</p> <ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages

4.7.6 Enabling or Disabling Connection Management

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

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.

Session

Configure the connection to a device

Session Connection Type: Connection Management Interface

DNS Name or IP Address:

Hide Advanced Options

Enable Peer Loss Overlay:

Enable Event Log Notification:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply
Cancel

Figure 4-32: AWI Connection Type – Connection Management Interface

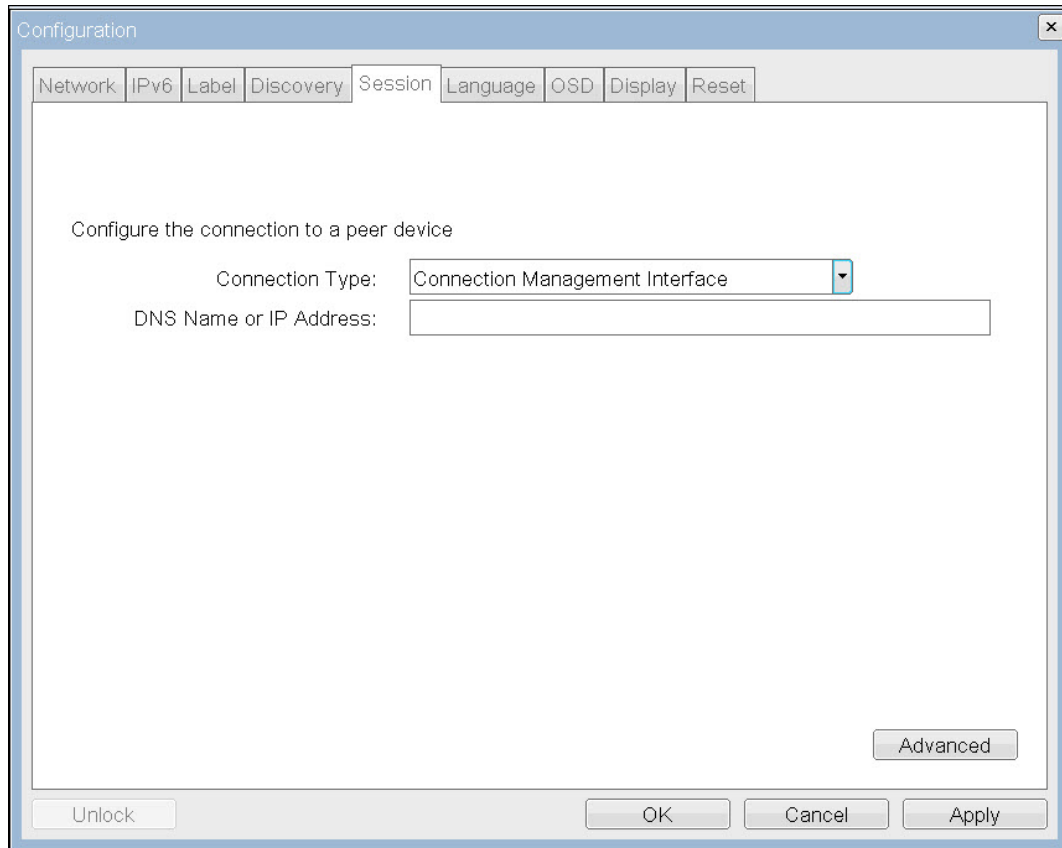


Figure 4-33: OSD Session Page – Connection Management Interface

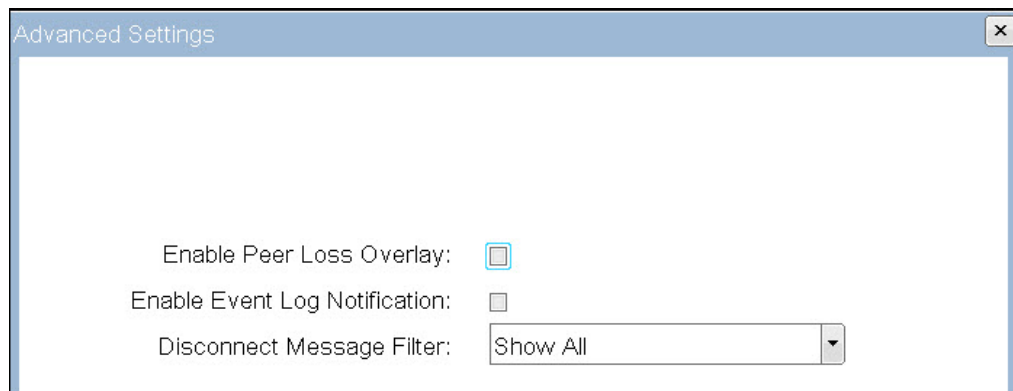


Figure 4-34: OSD Session Page – Connection Management Interface (Advanced Options)

Table 4-16: Connection Management Page Parameters

Parameter	Description
DNS Name or IP Address	Enter the DNS name or IP address of the connection manager.
Enable Peer Loss Overlay	<p>When enabled, the “Network Connection Lost” overlay appears on the display(s) when a loss of network connectivity is detected. 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.</p> <p>Note: This option is only available for a zero client. Desktop applications that require the peer loss notification should re-enable the feature through the OSD, Administrative Web Interface, or PCoIP Management Console.</p>
Enable Event Log Notification	Controls if the host and client devices send the contents of their event logs to the connection management server.
Enable AES-128-GCM	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and later to client: SALSA20-256-Round12 for the PCoIP session
Enable SALSA20-256-Round 12	<p>Configure SALSA20-256-Round 12 encryption for the client. SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 or later when there is more than about 7 Mbps available on the network. (See <i>TER0904005 Using PCoIP Zero Clients with VMware View</i> for more information.)</p> <p>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:</p> <ul style="list-style-type: none"> • Host to client: AES-128-GCM for the PCoIP session • VM 4.5 and above to client: SALSA20-256-Round12 for the PCoIP session
Disconnect Message Filter	<p>This field lets you control what type of messages appear when a session is disconnected. There are three categories:</p> <p>Information: User or administrator initiated actions affecting the session.</p> <ul style="list-style-type: none"> • Session closed remotely - closed by login at an alternate location or host shutdown/restart • Session closed remotely - user-initiated logout • Session closed remotely - disconnected by administrator • Session closed remotely - closed by login at an alternate location • Session closed remotely - host driver disconnect <p>Warning: System-initiated, but expected actions affecting the session. This occurs when a session is closed remotely (the global timeout value is reached).</p> <p>Error: Unexpected system-initiated actions causing session to fail. The following are Error messages:</p>

Parameter	Description
	<ul style="list-style-type: none"> • Session lost • Session refused • Session timeout • Session closed remotely - unknown cause • Session closed remotely - incompatible host driver version • Session closed remotely - disconnect because of an internal server error <p>You can choose to display:</p> <ol style="list-style-type: none"> 1. Show All messages – This option shows all disconnect messages including Info, Warning, and Error messages. 2. Show Error and Warnings Only – This option hides info messages and displays only error and warning messages. 3. Show Error Only – This option hides Info and Warning messages and displays only Error messages 4. Show None – Don't show any disconnect messages <p>Note: This setting only appears on the client.</p>

4.8 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.

Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: kbps (0 = no limit)

Device Bandwidth Target: kbps (0 = disabled)

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

Figure 4-35: Administrative Web Interface Bandwidth Page

Table 4-17: Bandwidth Page Parameters

Parameters	Description
Device Bandwidth Limit	<p>Defines the maximum bandwidth peak for the PCoIP system.</p> <p>The bandwidth setting defines the bandwidth based on which side is sending data:</p> <ul style="list-style-type: none"> • 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) <p>The usable range of the device bandwidth is 1000 to 220,000 kbps.</p> <p>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.</p> <p>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.</p> <p>We recommend setting this field to the limit of the network connected to the client and host.</p> <p>Note: The setting in this field is applied immediately after you click Apply.</p>
Device Bandwidth Target	<p>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.</p> <p>After the congestion is alleviated, the bandwidth used increases depending on the available network resources up to the Device Bandwidth Limit.</p> <p>You should have a good understanding of the network topology before setting this to a non-zero value.</p>
Device Bandwidth Floor	<p>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.</p> <p>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.</p> <p>Note: The firmware implements a Slow Start Algorithm that:</p> <ul style="list-style-type: none"> • 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) <p>After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.</p>

4.9 Setting the User Interface Language

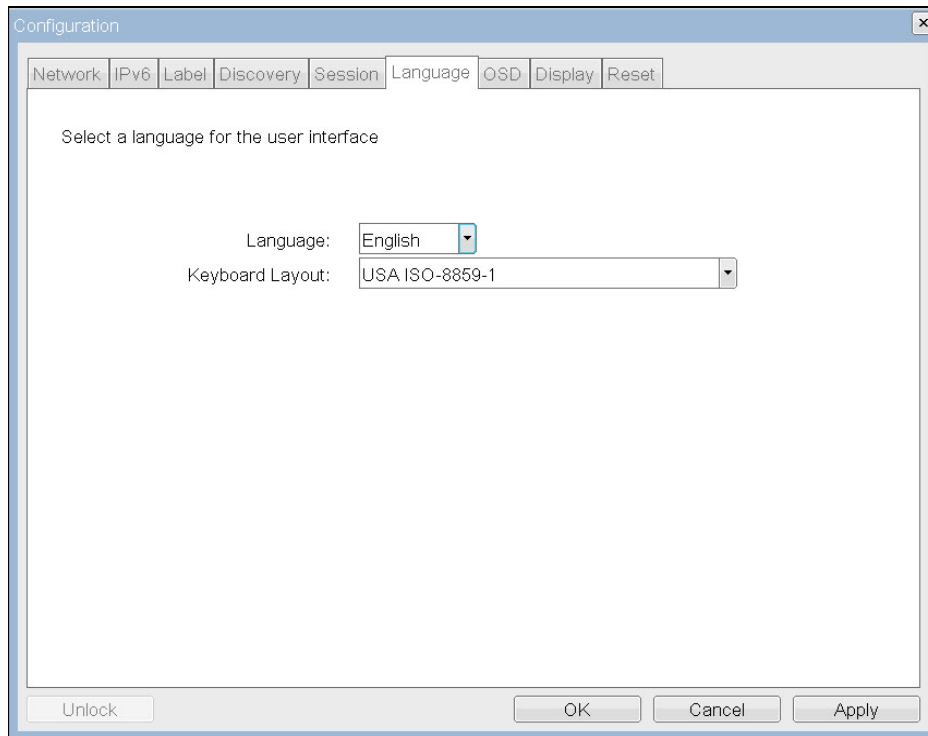
The **Language** page lets you change the user interface language.

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



The screenshot shows a web interface titled "Language". Below the title, it says "Select a language for the local GUI (client only)". There are two dropdown menus: "Language" set to "English" and "Keyboard Layout" set to "United States of America ISO-8859-1". At the bottom, there are "Apply" and "Cancel" buttons.

Figure 4-36: Administrative Web Interface Language Page



The screenshot shows a "Configuration" window with several tabs: "Network", "IPv6", "Label", "Discovery", "Session", "Language", "OSD", "Display", and "Reset". The "Language" tab is selected. The text "Select a language for the user interface" is displayed. There are two dropdown menus: "Language" set to "English" and "Keyboard Layout" set to "USA ISO-8859-1". At the bottom, there are "Unlock", "OK", "Cancel", and "Apply" buttons.

Figure 4-37: OSD Language Page

Table 4-18: 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.

4.10 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.

On Screen Display

Change the settings of the On Screen Display (client only)

Screen-Saver Timeout: Seconds (0 = disabled)

Figure 4-38: Administrative Web Interface OSD Page

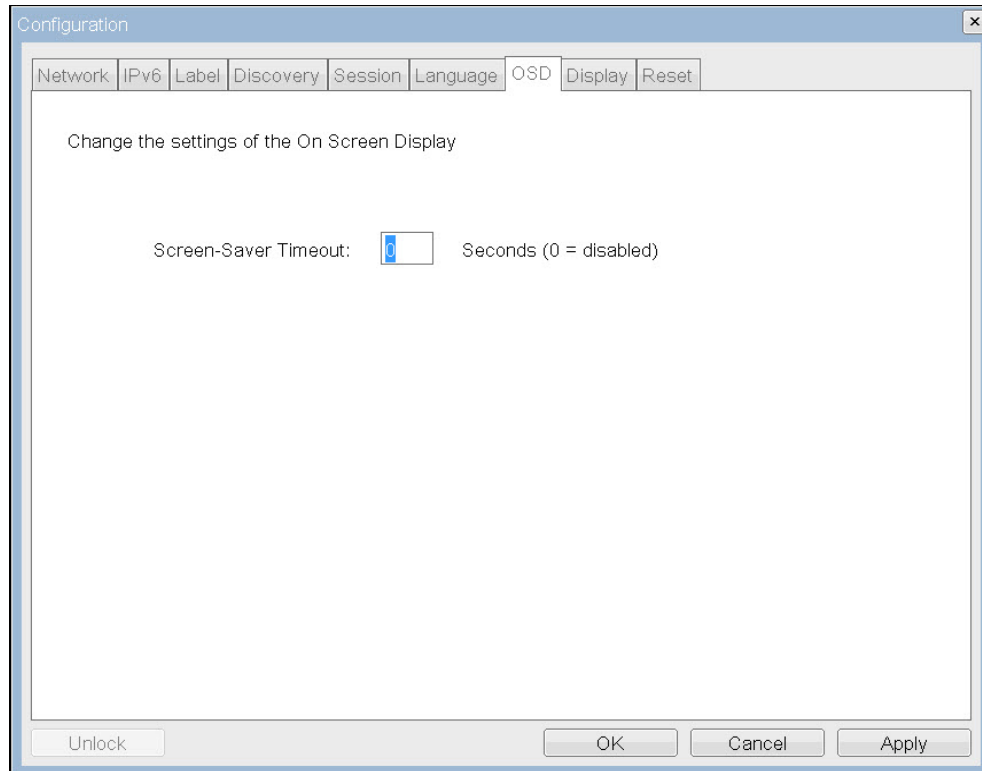


Figure 4-39: OSD-OSD Page

Table 4-19: 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.

4.11 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 for a VMware View virtual desktop, adjust the PCoIP session variables. See *VMware View 4 to PCoIP Client WAN Network Guidelines* for more information.

Image

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

Use Client Image Settings:

Minimum Image Quality:

Maximum Initial Image Quality:

Maximum Frame Rate: fps (0 = no limit)

Disable Build To Lossless:

Figure 4-40: Administrative Web Interface Image Page (Host)

Image

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

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

Minimum Image Quality: Reduced Perception-Free

Maximum Initial Image Quality: Reduced Perception-Free

Image Quality Preference: Smoother Motion Sharper Image

Maximum Frame Rate: fps (0 = no limit)

Disable Build To Lossless:

Figure 4-41: Administrative Web Interface Image Page (Client)

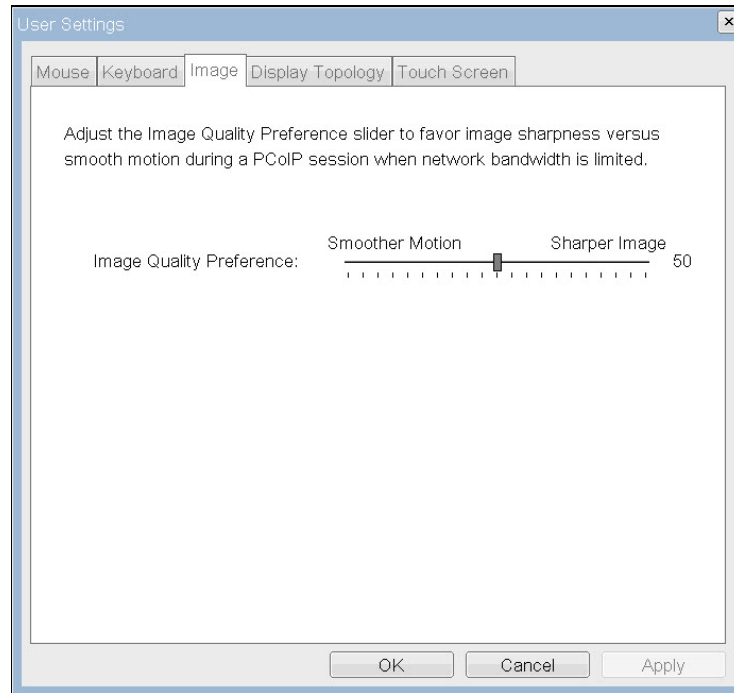


Figure 4-42: OSD Image Page

Table 4-20: Image Page Parameters

For more details about adjusting the image quality, see section [9.4](#).

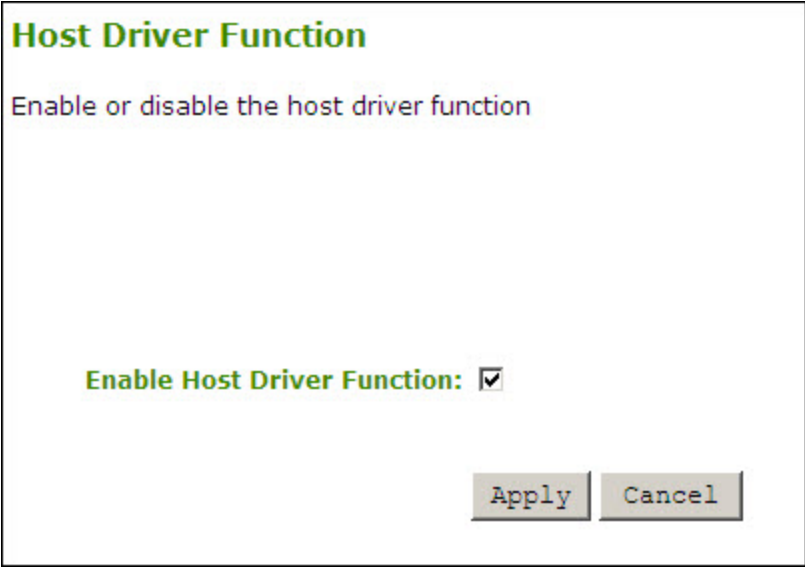
Parameter	Description
Use Client Image Settings	<p>This field is only available from the host. (It is not available on the client.)</p> <p>When enabled: The image settings on this page are not editable. The settings that appear (grayed out) are those stored for the host in flash.</p> <p>When disabled: The image settings are editable and are applied to any current sessions.</p>
Minimum Image Quality	<p>Lets you compromise between image quality and frame rate when network bandwidth is limited. Some use cases may require lower-quality images at a higher frame rate while others need higher-quality images at a lower frame rate.</p> <p>In environments where the network bandwidth is constrained, 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.</p> <p>Note: The Minimum Image Quality must be less than or equal to the Maximum Initial Image Quality. It does not have a corresponding parameter on the OSD as it is an administrator-only parameter</p>
Maximum Initial Image Quality	<p>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.</p>

Parameter	Description
	<p>Note: The Maximum Image Quality:</p> <ul style="list-style-type: none"> • must be greater than or equal to the Minimum Image Quality • does not have a corresponding parameter on the OSD as it is an administrator-only parameter
Image Quality Preference	<p>Use the slider to set if you want the image to favor image sharpness versus smooth motion during a PCoIP session when network bandwidth is limited.</p> <p>Note: This field is also accessible on the host if the PCoIP Host Software is installed. The slider appears in the host software's Image tab. This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier.</p>
Maximum Frame Rate	<p>The maximum frame rate helps you manage multiple PCoIP sessions over a single network link. This setting determines the limit that your users can reach. Set this field to 0 to set no frame limit. If you set a value, a single user is limited to that value. This helps to control the user experience for all your users.</p> <p>Note: The Maximum Frame Rate does not have a corresponding parameter on the OSD as it is an administrator-only parameter. This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier.</p>
Disable Build to Lossless	<p>Leave this field unchecked to retain build to lossless. In these cases, the images continue to be built to a lossless state. This is the default (recommended) setting.</p> <p>Warning: Activating the Disable build-to-lossless feature will degrade the image presented to the user by the zero client. Do not activate the Disable Build to Lossless feature unless it has been determined by the administrator of the zero client that users do not require optimal image quality to perform critical functions. It is the sole responsibility of the zero client administrator to make this determination.</p> <p>If you choose to disable build to lossless, PCoIP rapidly builds the client image to a high quality, but perceptually lossless image. If you enable build to lossless, if the image remains constant, PCoIP continues to refine the image in the background until it reaches a fully lossless state. Stopping the build process when the image reaches the "perceptually lossless" stage can deliver significant bandwidth savings. If you have any questions about this field setting, contact Teradici Support.</p> <p>Note: There is no Disable Build to Lossless setting on the OSD as it is an administrator-only parameter. This setting does not work in PCoIP sessions with VMware View virtual desktops running release 5.0 or earlier.</p>

4.12 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.



Host Driver Function

Enable or disable the host driver function

Enable Host Driver Function:

Apply Cancel

Figure 4-43: Administrative Web Interface Host Driver Function Page

When the **Enable Host Driver Function** checkbox is enabled, the PCoIP host driver function allows 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

4.13 Configuring the NTP Parameters

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

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

Time

Change the local time configuration

Current time: 11/18/2011 12:22:45

Enable NTP:

Identify NTP Host by: IP address FQDN

NTP Host DNS Name:

NTP Host Port:

NTP Query Interval: Day(s)

Time Zone:

Enable Daylight Saving Time:

Figure 4-44: Administrative Web Interface Time Page

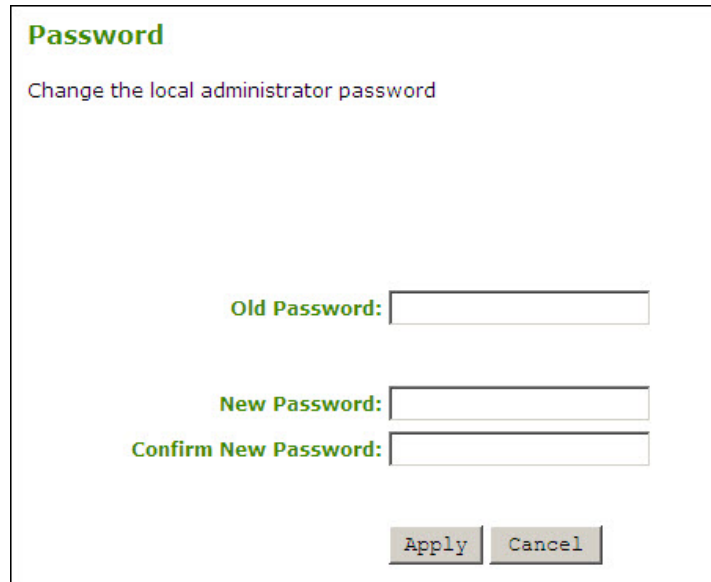
Table 4-21: Time Page Parameters

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: <ul style="list-style-type: none"> • IP Address: Shows the NTP Host IP address • FQDN: Shows the NTP Host DNS name
NTP Host Port	Configure the NTP port number.
NTP Query Interval	Configure the query interval. The first field is for the interval period and the second field is for the time unit in Minute(s), Hour(s), Day(s), and Week(s).
Time Zone	Select the local time zone.
Enable Daylight Savings Time	Enable or disable the automatic adjustment for daylight savings time.

4.14 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. You can enable password protection through the PCoIP Management Console for these devices.

Note: This parameter affects the Administrative 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.



Password

Change the local administrator password

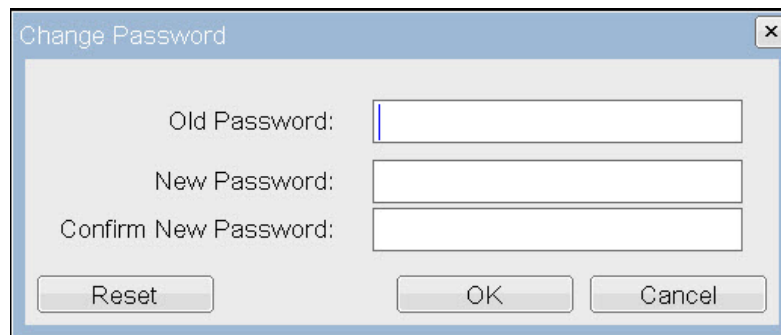
Old Password:

New Password:

Confirm New Password:

Apply Cancel

Figure 4-45: Administrative Web Interface Change Password Page



Change Password

Old Password:

New Password:

Confirm New Password:

Reset OK Cancel

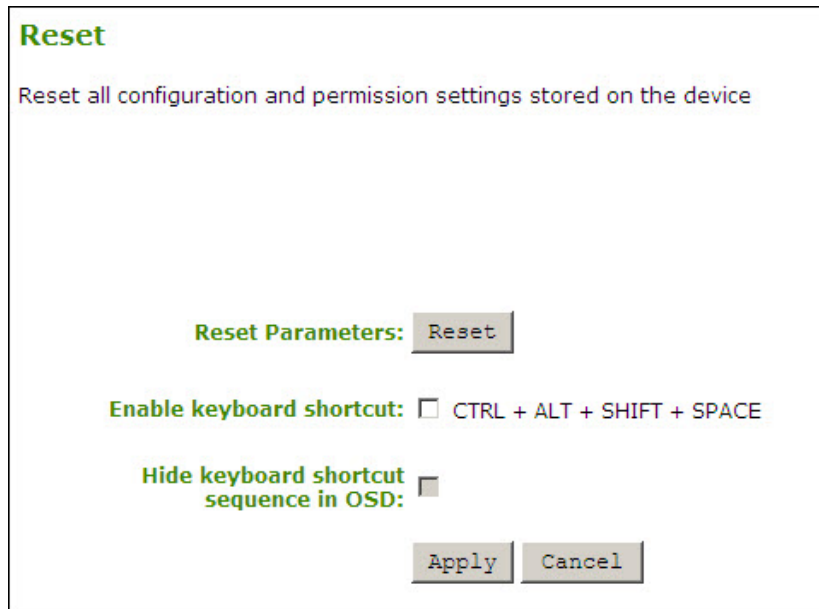
Figure 4-46: OSD Change Password Page

Table 4-22: 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	<p>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 is sent to the vendor. The vendor qualifies the request and returns a response code if authorized by Teradici. When the response code is correctly entered, the client's password is reset to an empty string. You must enter a new password.</p> <p><i>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.</i></p>

4.15 Resetting the Parameters to Factory Default Values

The **Reset Parameters** page lets you reset configuration and permissions to factory default values stored in flash.



Reset

Reset all configuration and permission settings stored on the device

Reset Parameters:

Enable keyboard shortcut: CTRL + ALT + SHIFT + SPACE

Hide keyboard shortcut sequence in OSD:

Figure 4-47: Administrative Web Interface Reset Page (Client)

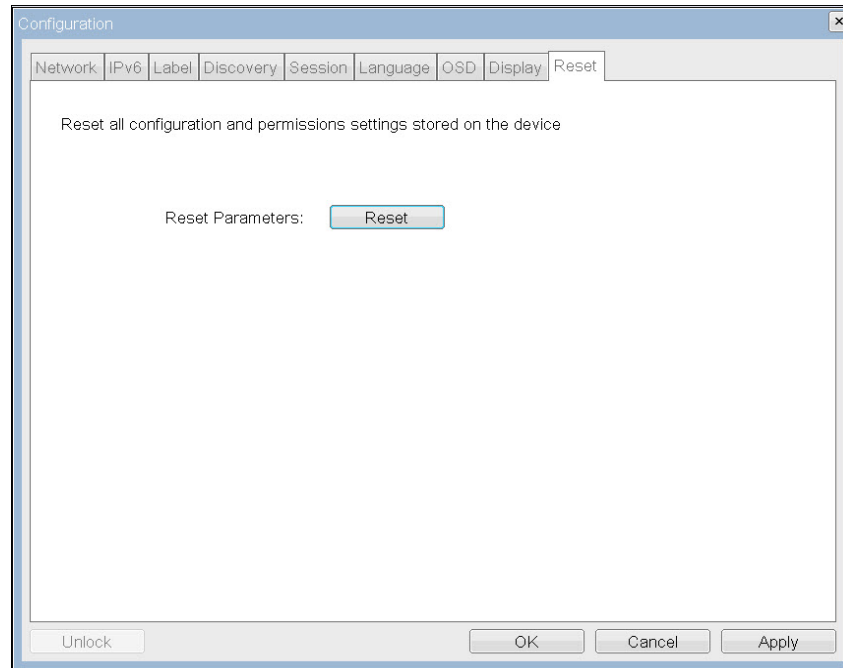


Figure 4-48: OSD Reset Page

Table 4-23: Reset Parameters

Parameter	Description
Reset Parameters	When you click this button, a prompt appears for confirmation. This is to prevent accidental resets.
Enable Keyboard Shortcut	When enabled, the user can press the combination of keys to automatically reset the parameters and permissions for the device. <i>Note: This field is only available from the zero client. It is not available from the host.</i>
Hide Keyboard Shortcut Sequence in OSD	When the Enable Keyboard Shortcut field is enabled, and this field is: Disabled: The keyboard sequence appears on the Reset Parameters page for the zero client. Enable this field: The keyboard sequence does not appear on the Reset Parameters page for the zero client. The user can still reset the parameters through the keyboard sequence.

4.16 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.

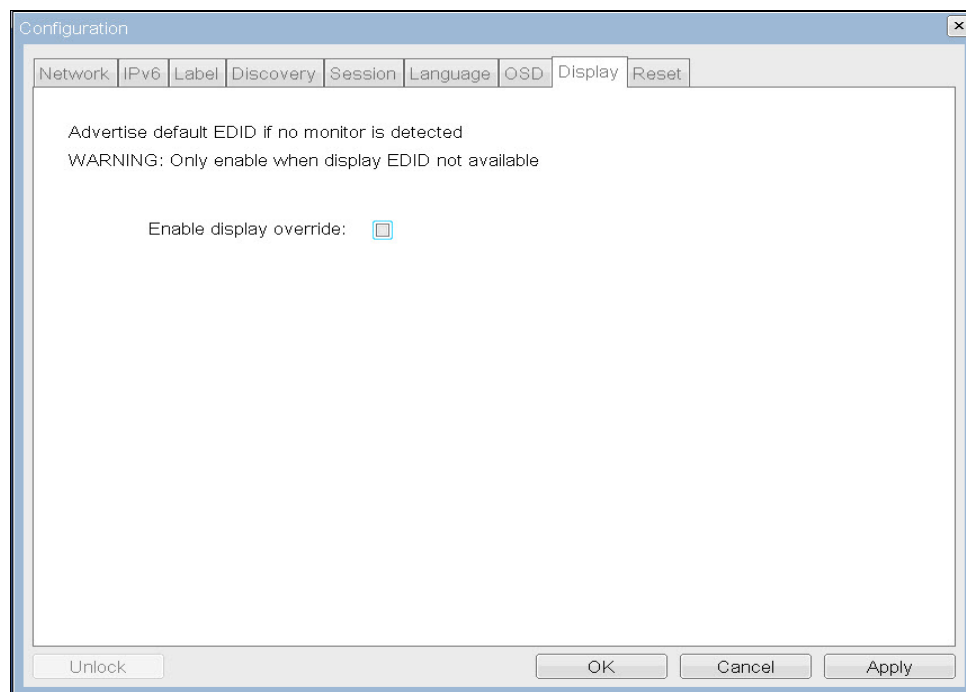


Figure 4-49: OSD Display Page

4.17 Enabling Monitor Emulation

The **Monitor Emulation** page lets you enable or disable the monitor emulation feature. The **Monitor Emulation** page is only available on host cards still using monitor emulation. It is disabled and non-editable on the client.

Some PCs and workstations do not boot if a display is not attached. Monitor emulation presents a generic display to ensure the boot process completes. When a session is connected, the client display information is sent to the host.

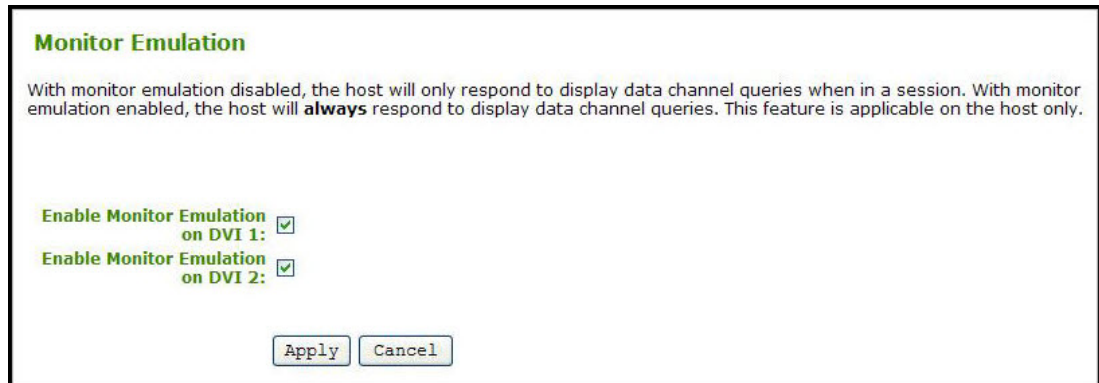


Figure 4-50: Administrative Web Interface Monitor Emulation Page

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 or not.

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

4.18 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.



Set in Profile			
<input type="checkbox"/>	OSD Screensaver Text	<input type="text"/>	This property configures the OSD screensaver text for devices running firmware older than 3.0. The text can be up to 240 characters long. The screensaver is a simple black screen with the screensaver text jumping randomly. Beginning with firmware 3.0 the screensaver was replaced with monitor sleep and this text is not used.
<input type="checkbox"/>	OSD Screensaver Timeout	<input type="text"/> s (0,10-9999)	This property configures the OSD screensaver/monitor sleep timeout. A setting of 0 seconds disables the screensaver/monitor sleep.
<input type="checkbox"/>	Hidden Menu Entries 	<input type="checkbox"/> Hide Options -> Configuration <input type="checkbox"/> Hide Options -> Diagnostics <input type="checkbox"/> Hide Options -> Information <input type="checkbox"/> Hide Options -> User Settings <input type="checkbox"/> Hide Options -> Password <input type="checkbox"/> Hide the Options menu <input type="checkbox"/> Hide all menus	This property controls which menu items or entire menus are hidden in the OSD. Hide a single menu item by selecting it. To hide an entire menu select the menu hide checkbox. To hide all of the menus select the hide all menu checkbox.
		<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
 indicates that the property requires a device restart after being changed			

Figure 4-51: OSD Configuration – Hidden Menu Entries Option

4.19 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.




Set in Profile			
<input type="checkbox"/>	Password	<input type="text"/>	This property configures the Host or Portal local administrative password. This password is required to access the web interface. It is also required to modify certain configuration settings accessible through the OSD. The password is a string of zero to 20 characters.
<input type="checkbox"/>	Enable Password Protection 	<input type="radio"/> True <input checked="" type="radio"/> False	This property enables the Host or Portal local administrative password. When it is false, the web interface and OSD are not password protected.
<input type="checkbox"/>	Additional Root Certificate	<input type="text"/> <input type="button" value="Browse..."/>	Installs an additional root certificate into the endpoint for use in the web UI and with VMware View Connection Servers.
<input type="checkbox"/>	Enable Web Interface 	<input type="radio"/> True <input checked="" type="radio"/> False	When this property is true the device's embedded web interface is enabled. When it is false the web interface is disabled.
		<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
 indicates that the property requires a device restart after being changed			

Figure 4-52: 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

USB

Configure the USB permissions table

Authorized Devices:

Any Device Class	Any Sub Class	Any Protocol	<input type="button" value="Remove"/>
<input type="button" value="Add new"/>			

Unauthorized Devices: *Table is empty*

Bridged Devices: *Table is empty*

Enable EHCI (root port only):

Figure 5-1: Administrative Web Interface USB Page

Table 5-1: USB Page Parameters

Parameter	Description
Authorized Devices	<p>Specify the authorized USB devices for the host and client. Two buttons let you customize this "white list":</p> <p>Add New: add a new device or device group to the list. This allows USB authorization by ID or Class:</p> <ul style="list-style-type: none"> • ID: The USB device is authorized by its Vendor ID and Product ID • Class: The USB device is authorized by Device Class, Sub Class, and Protocol <p>Remove: Delete a rule for a device or device group from the list.</p>
Unauthorized Devices	<p>Specify the unauthorized USB devices for the host or client.</p> <p>Add New: add a new device or device group to the list. This allows USB devices to be unauthorized by ID or Class:</p> <ul style="list-style-type: none"> • ID: The USB device is unauthorized by its Vendor ID and Product ID • Class: The USB device is unauthorized by Device Class, Sub Class, and Protocol <p>Remove: Delete a rule for a device or device group from the list.</p>
Bridged Devices	<p>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.</p> <p>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.</p> <p>Add New: Add a device or device group to the list. This lets you bridge USB devices by their Vendor ID and Product ID.</p> <p>Remove: Delete a rule for a device or device group from the list.</p>
Enable EHCI (root port only)	<p>Enable this field to configure EHCI (USB 2.0) for devices connected directly to the zero client USB ports for sessions with a soft host running VMware View 4.6 or later.</p> <p>Note: This feature cannot be enabled on zero clients with less than 128 MB of RAM. Devices with isochronous endpoints will not operate at USB 2.0 speeds.</p>

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	0-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; asterisk (*) indicates any protocol 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**.

Audio

Enable or disable high definition audio

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

Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode: Important: If using Microsoft® Windows Vista® / Windows® 7 64-bit Edition, this feature must be enabled for audio to function correctly.

Enable Audio Line In: This will select the Line In input. If using Microsoft® Windows Vista® / Windows® 7, please ensure you do the following for this feature to function correctly:

1. Run regedit.
2. Search the registry keys for 'PinConfigOverrideVerbs' and delete these registry entries.

Figure 5-2: Administrative Web Interface Audio Page (Host)

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 operating system to enumerate.
Enable Microsoft Windows Vista 64-bit Mode	<p>Note: This option is only available on the host. It is not available on the client.</p> <p>Enables 64-bit mode on host. Enable this option for Windows Vista 64-bit and Windows 7 64-bit versions. This ensures audio works correctly.</p> <p>This option is only available on a host. It does not appear on the client.</p> <p>Warning: Do NOT use this mode with Windows XP 64 or 32-bit operating systems.</p> <p>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.</p>
Enable Audio Line In	<p>Enable: Use the line-in connector found on the client.</p> <p>Disable: Use the line-in connector as a microphone input.</p> <p>Follow the onscreen instructions if you have Windows Vista or Windows 7 installed on the device.</p> <p>Note: This option is only available on the host. It does not appear on the client.</p>

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.

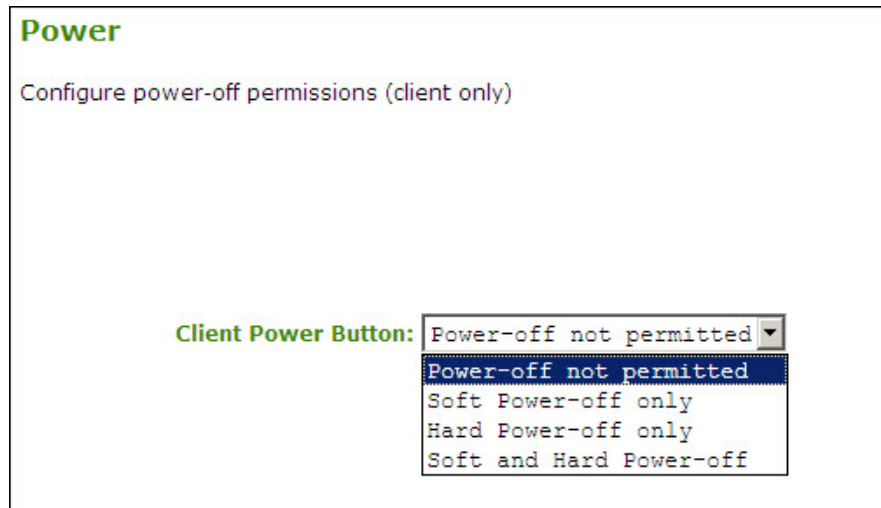

Figure 5-3: Administrative Web Interface Power Page (Client)

Table 5-4: Power Page Parameter

Parameter	Description
Client Power Button	<p>The drop-down menu lets you configure the client Power button functionality. Options include:</p> <ul style="list-style-type: none"> • 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 pages 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.

Event Log

Configure diagnostic logging options

Event Log Messages:

Event Log Filter Mode:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: ...

Syslog Host Port:

Syslog Facility:

Enhanced logging mode:

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

Figure 6-1: Administrative Web Interface Event Log Page

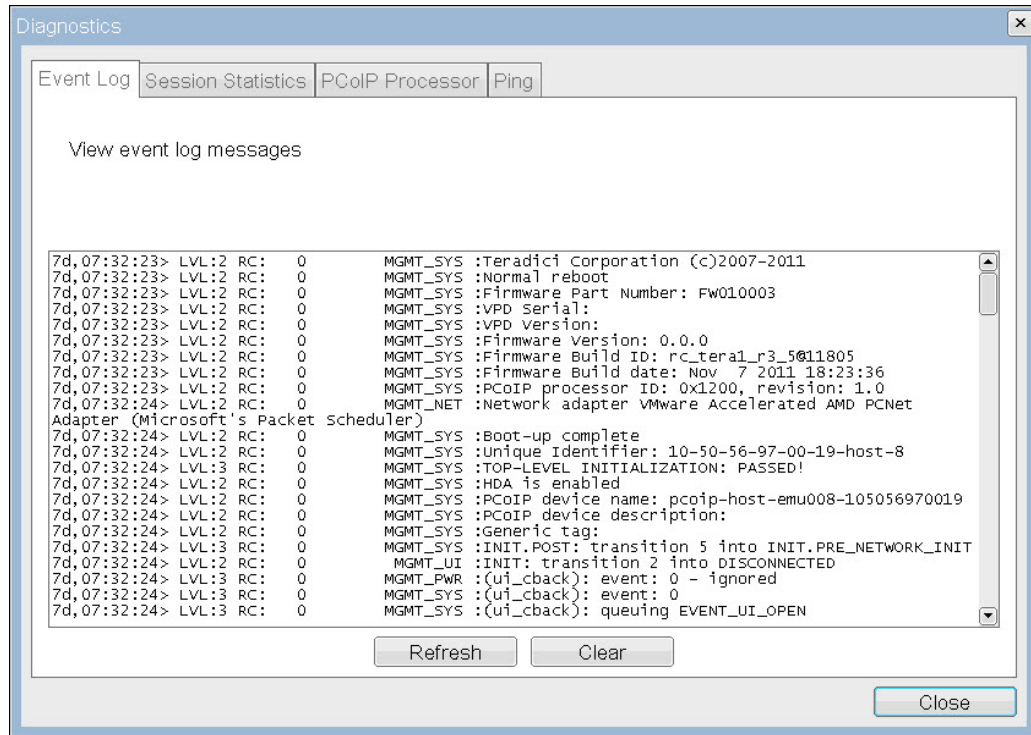


Figure 6-2: OSD Event Log Page

Table 6-1: Event Log Parameters

Parameter	Description
Event log Messages	<p>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.</p> <p>Clear: Click to delete all event log messages stored on the device.</p>
Event Log Filter Mode	<p>Click the pull-down menu to filter the event logs. Options include:</p> <ul style="list-style-type: none"> • Verbose (this is the default setting) • Terse
Enable Syslog	<p>Enable the syslog standard for your event logs. If syslog is enabled, you must configure the remaining fields (if disabled, they are non-editable).</p>
Identify Syslog Host By	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>If you set the Identify Syslog Host By field to:</p> <ul style="list-style-type: none"> • IP Address: Enter the IP address for the syslog host • FQDN: Enter the DNS name for the syslog host
Syslog Host Port	<p>Lets you configure the syslog port number.</p>
Syslog Facility	<p>The facility is a number attached to every syslog message used to categorize the source of the syslog messages. The facility is part of the standard syslog header and can be interpreted by all syslog servers. Enter a facility to suit your logging needs. For example, you could configure:</p> <ul style="list-style-type: none"> • zero clients to use facility 19 • Cisco routers to use facility 20 • VMware ESX hosts to use facility 21 <p>Note: The default facility is set to "19 – local use 3". Cisco routers default to "23 – local use 7".</p>
Enhanced logging mode	<p>This field lets you collect enhanced log messages for one of the following categories. Click Disable to turn off the enhanced logging mode.</p> <ul style="list-style-type: none"> • Audio • Management Console • Networking • Session Negotiation • Smart Card • System • USB • Video <p>Note: You can only enable enhanced logging for one of the above categories at one time.</p>

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

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.

Session Statistics

View statistics for the current session

Connection State: Connected to TERA1100 client [192.168.50.12](#)
802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 744042 / 630636 / 0
Bytes (Sent/Received): 372089028 / 92452440
Round Trip Latency (Min/Avg/Max): 1 / 1 / 3 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 0 / 0 / 46288 / 75104 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 8 / 1016 kbps

Pipeline Processing Rate (Avg/Max/Limit): 0 / 104 / 113 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Active/Max): 60 / 90 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	0 fps	0 fps	Lossless
2	60 fps	0 fps	0 fps	Lossless

Figure 6-4: Administrative Web Interface Session Statistics Page (Host)

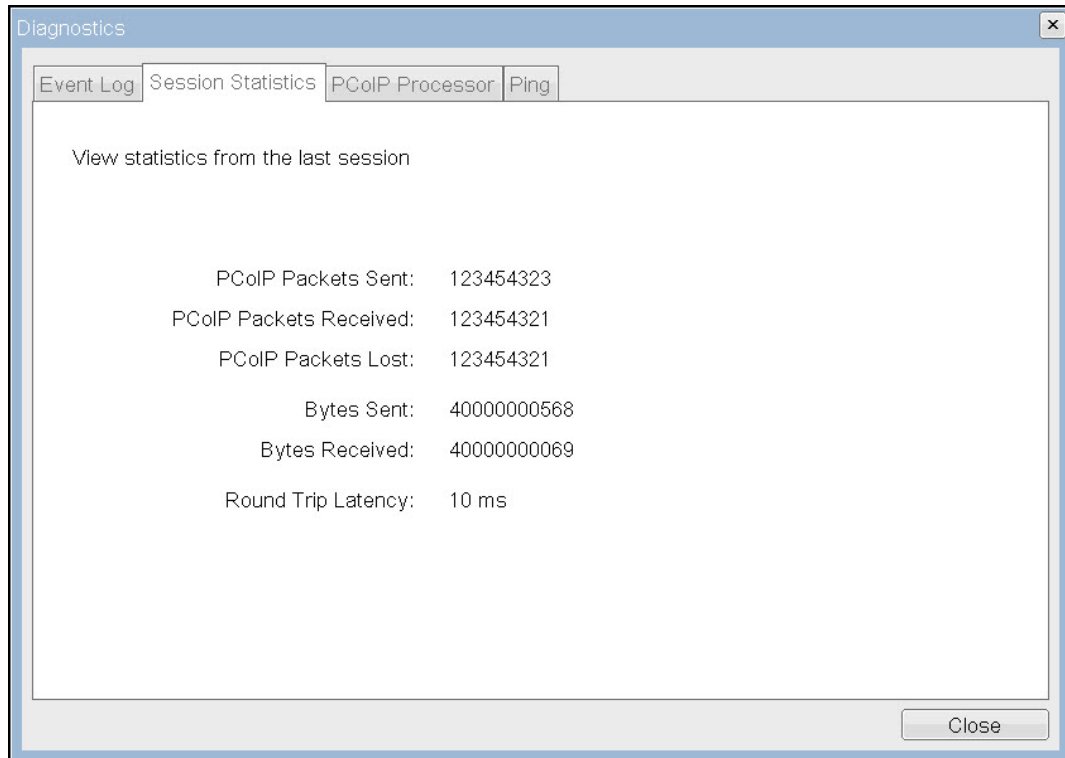


Figure 6-5: OSD Session Statistics Page

Table 6-3: Session Statistics Page Parameters

Parameters	Description
Connection State	The current (or last) state of the PCoIP session. Values include: <ul style="list-style-type: none"> • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	Identify if the 802.1X authentication is enabled or disabled on the device.
PCoIP Packets Statistics	<p>PCoIP Packets Sent: The total number of PCoIP packets sent in the current/last session.</p> <p>PCoIP Packets Received: The total number of PCoIP packets received in the current/last session.</p> <p>PCoIP Packets Lost: The total number of PCoIP packets lost in the current/last session.</p>
Bytes	<p>Bytes Sent: The total number of bytes sent in the current/last session.</p> <p>Bytes Received: The total number of bytes received in the current/last session.</p>
Round Trip Latency	The minimum, average, and maximum round-trip PCoIP system (for example, host to client and then back to host) and network latency in milliseconds (+/- 1 ms).
Bandwidth Statistics	<p>Transmit Bandwidth: The minimum, average, and maximum traffic transmitted by the Tera1x00 processor. The active bandwidth limit is 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.</p> <p>Receive Bandwidth: The minimum, average, and maximum traffic received by the Tera1x00 processor.</p>
Pipeline Processing Rate	How much image data is currently being processed by the image engine (in megapixels per second).
Endpoint Image Settings In Use	Displays if the image settings being used are configured within the client or within the host. This is based on how the Use Client Image Settings field is configured on the Image page for the host device. <p><i>Note: This field only appears on the host. It is not available on the client.</i></p>
Initial Image Quality	The minimum and maximum quality setting is taken from the Image page for the device. The active setting is what's currently being used in the session and only appears on the host.
Image Quality Preference	This setting is taken from the Image Quality Preference field on the Image page. The value determines if the image is set to a smoother versus a sharper image.
Build to Lossless	Options that may appear in this field include: <p>Enabled: The Disable Build to Lossless field on the Image page is unchecked.</p> <p>Disabled: The Disable Build to Lossless field is checked.</p>
Reset Statistics	Click this button to reset the statistic information on this page.

Parameters	Description
	Note: The Reset Statistics button also resets the statistics reported in the Home page.
Display	The port number for the display.
Maximum Rate	This column shows the refresh rate of the attached display. If the Maximum Rate field on the Image page is set to: 0 (that is, there is no limit) : The maximum rate is taken from the monitor's refresh rate. A value greater than 0 : The refresh rate shows as "User Defined".
Input Change Rate	The rate of content change from the GPU. This includes everything the user is doing (such as cursor movement, email editing, or streaming video).
Output Process Rate	The frame rate currently being sent from the image engine on the host to the client.
Image Quality	Shows the current lossless state of the attached display: <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless

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.

Host CPU

View identity, view and change power state (host only)

Host Identity:

Current Power State: S0 (On)

Change Power State: S5 (Soft Off)

Figure 6-6: Administrative Web Interface Host CPU Page

Table 6-4: Host CPU Page Parameters

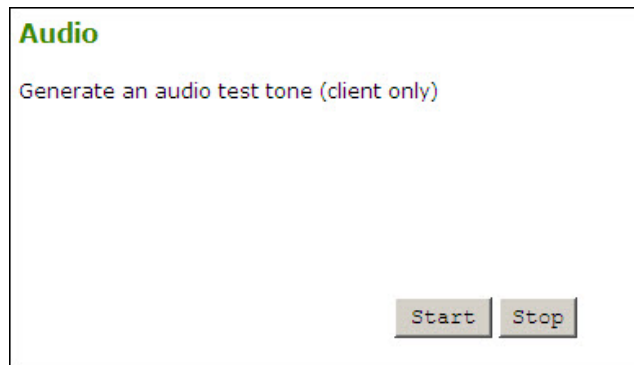
Parameters	Description
Host Identity	The identity string of the host computer (if data is available).
Current Power State	The current state of the power for the host (e.g., "on").
Change Power State	Power off the host as: <ul style="list-style-type: none"> • S5 (Soft Off) • S5 (Hard Off) Note: To use 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.

Display

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

Test mode:

Test resolution:

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: <ul style="list-style-type: none"> • Video Test Pattern Generator • Pseudo Random Bitstream
Test resolution	Set the test pattern resolution as: <ul style="list-style-type: none"> • 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.

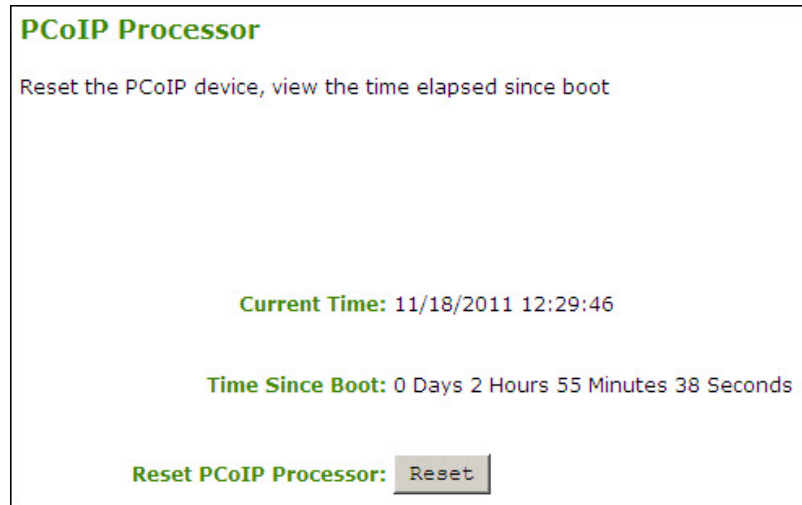


Figure 6-9: Administrative Web Interface PCoIP Processor Page

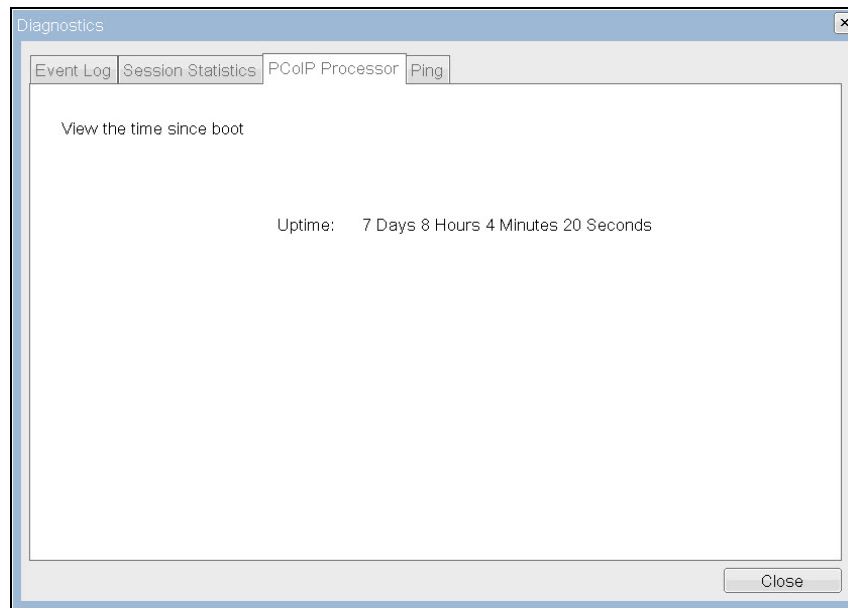


Figure 6-10: OSD PCoIP Processor Page

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 4.13.
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 later force the “do not fragment flag” in the ping command, you can also use this feature to determine the maximum MTU size.

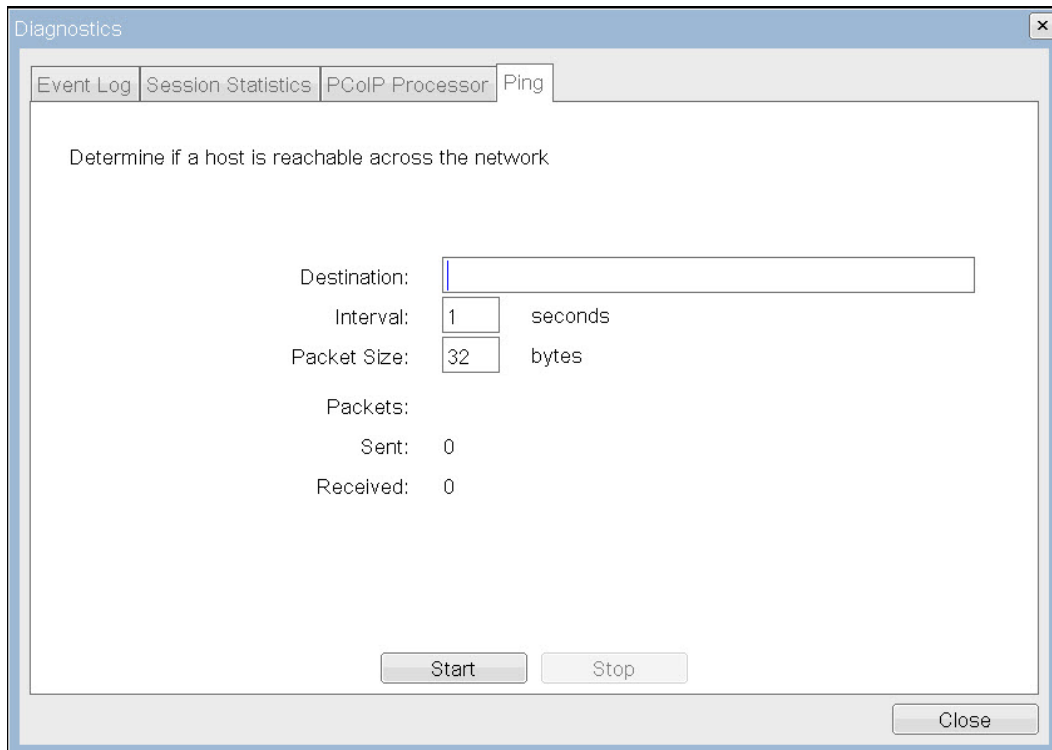


Figure 6-11: OSD Ping Page

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.

Version

View the hardware and firmware version information

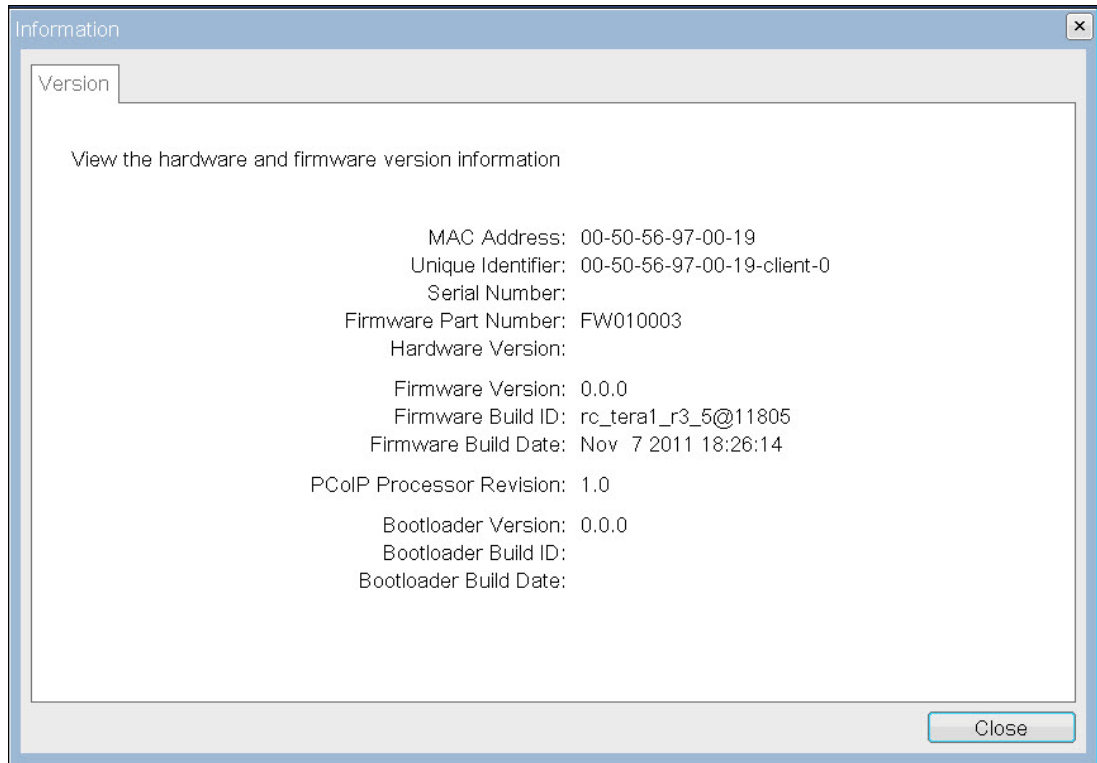
MAC Address: 00-0C-87-00-8A-53
Unique Identifier: 00-0C-87-00-8A-53
Serial Number: 21312-0039
Firmware Part Number: FW010040
Hardware Version: RG220_rev_C

Firmware Version: 0.0.0
Firmware Build ID: rc_tera1_r3_5@11829
Firmware Build Date: Nov 15 2011 14:09:35

PCoIP Processor Revision: 1.0

Bootloader Version: 2.2.0
Bootloader Build ID: v327
Bootloader Build Date: Apr 6 2011 19:28:23

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

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.

Attached Devices

View presently connected monitors

Displays:

Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date
1	SME2320	Connected	DVI	1920x1080 @ 60 Hz	HVDZB00113	SAM	682	47-2010
2	SME2320	Connected	DVI	1920x1080 @ 60 Hz	HVDZA00340	SAM	682	43-2010

Legend (Displays):

Status [potential failures]	Description
Connected [EDID read failure / EDID override]	The display is connected and the EDID has been bridged (host/client)
Disconnected	No display or cable has been detected
Not in Session [EDID read failure / EDID override]	The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)
Unknown	On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)
Potential Failures	Description
EDID read failure	There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.
EDID override	Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached

Figure 7-3: Administrative Web Interface Attached Devices Page (Host)

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

Attached Devices

View presently connected monitors and USB devices

Displays:

Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date
1	SME2320	Connected	DVI	1920x1080 @ 60 Hz	HVDZB00113	SAM	682	47-2010
2	SME2320	Connected	DVI	1920x1080 @ 60 Hz	HVDZA00340	SAM	682	43-2010

USB Devices:

Port	Model	Status	Device Class	Sub Class	Protocol	Serial	VID	PID
OHCI	USB Keyboard	Connected	00	00	00	-	046D	C31C
OHCI	USB Optical Mouse	Connected	00	00	00	-	046D	C05A

Legend (Displays):

Status [potential failures]	Description
Connected [EDID read failure / EDID override]	The display is connected and the EDID has been bridged (host/client)
Disconnected	No display or cable has been detected
Not in Session [EDID read failure / EDID override]	The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)
Unknown	On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)
Potential Failures	Description
EDID read failure	There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.
EDID override	Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached

Figure 7-4: Administrative Web Interface Attached Devices Page (Client)

Table 7-2: Attached Devices Page Statistics

Statistic	Description
Displays	<p>This section displays the model, status, mode, resolution, serial number, vendor identification (VID), product identification (PID), and date of the monitor attached to each port. The first line is for monitor 1. The second line is for monitor 2.</p> <p>Note: This option is available on a client and is available on the host when in a PCoIP session.</p>
USB Devices	<p>This section displays the port mode, model, status, device class, subclass, protocol, vendor identification (VID), and product identification (PID) of the USB device attached to the client.</p>
USB Device Status	<p>Status options include:</p> <ul style="list-style-type: none"> • Not Connected: No device is connected. • Not in Session: The device is detected outside of a PCoIP session. • Not Initialized: The device is detected in a PCoIP session but the host controller has not initialized the device. • Failed Authorization: The device is detected in a PCoIP session but is not authorized. (For more information, 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, an OSD logo to a device, or to manage your certificates. 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.

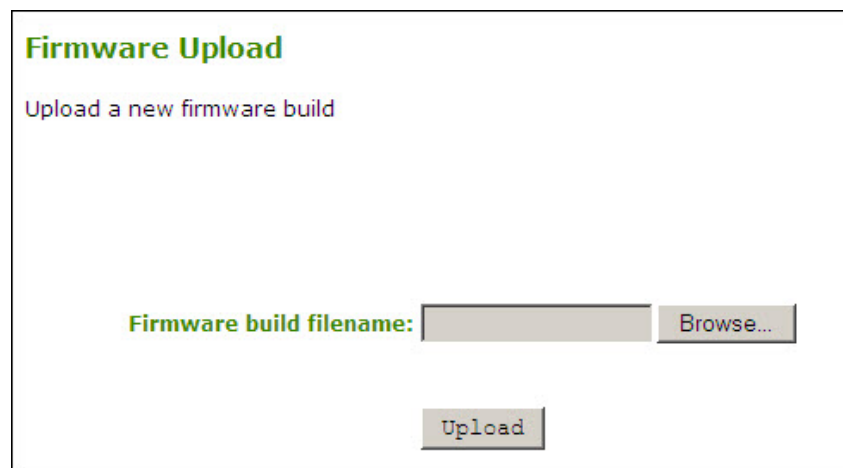


Figure 8-1: Administrative Web Interface Firmware Page

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_rell-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 1.

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

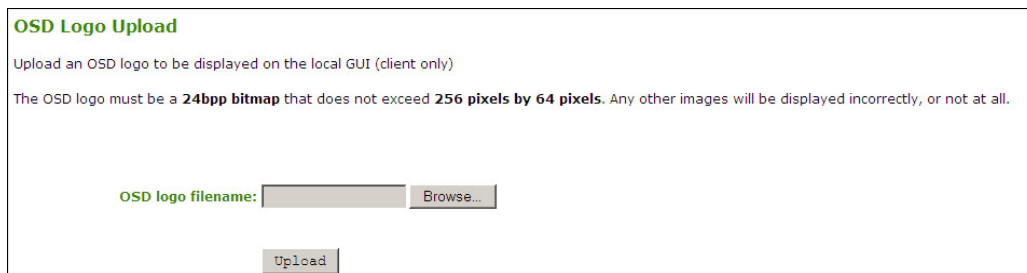


Figure 8-2: Administrative Web Interface OSD Logo Upload Page (Client)

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.

8.3 Uploading the Certificate

The **Certificate Upload** page lets you manage your root and client certificates. You can upload up to 16 certificates.

Note: In Firmware Release 3.5, the PCoIP protocol reads just one client certificate for 802.1X compliant networks. Make sure you include all the security information for your PCoIP devices in that 802.1X client certificate.

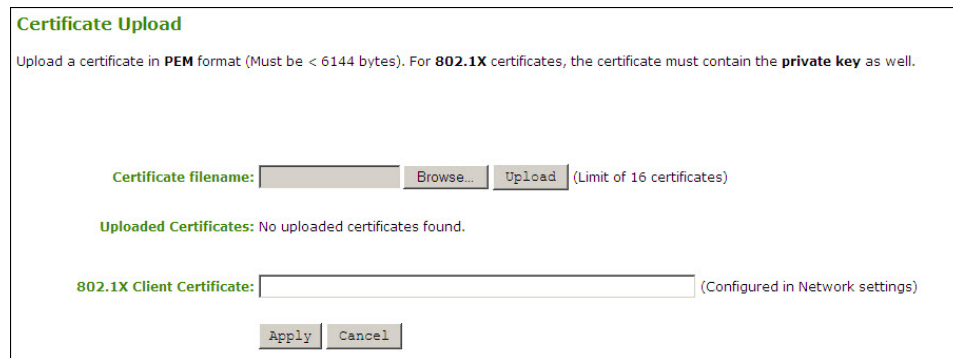


Figure 8-3: Administrative Web Interface Certificate Upload Page

Table 8-3: Administrative Web Interface Certificate Upload Page Parameters

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

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.

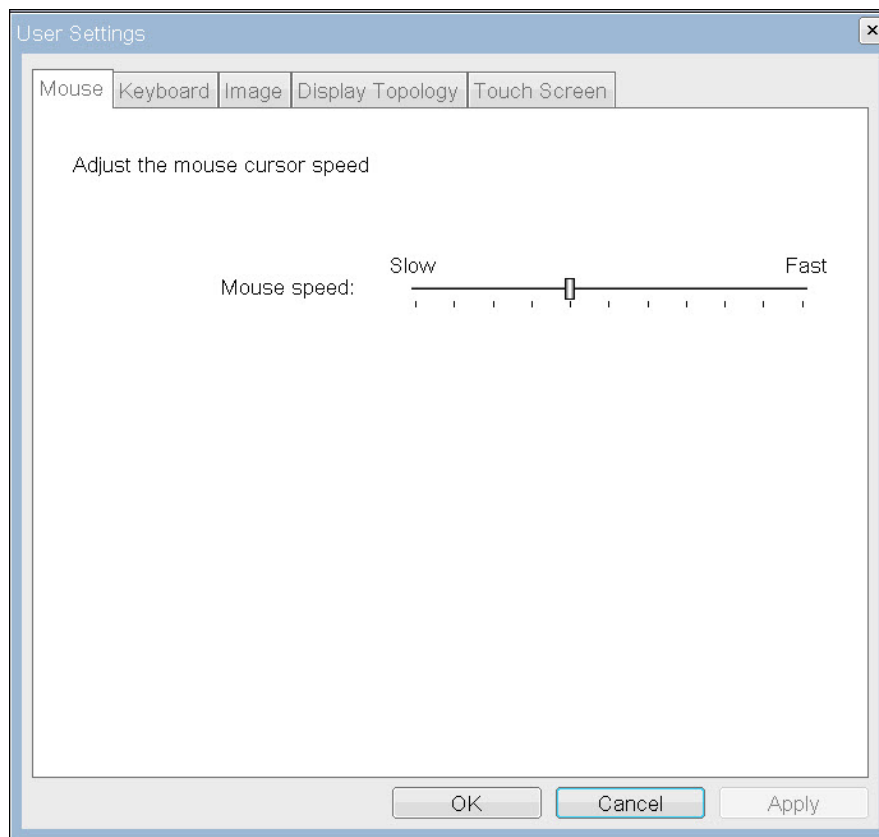


Figure 9-1: OSD Mouse Page

Table 9-1: Mouse Page Parameters

Parameter	Description
Mouse Speed	Configure the speed of the mouse cursor. <i>Note:</i> You can also configure the mouse speed through the PCoIP host software. See the <i>PCoIP Host Software for Windows User Guide</i> (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

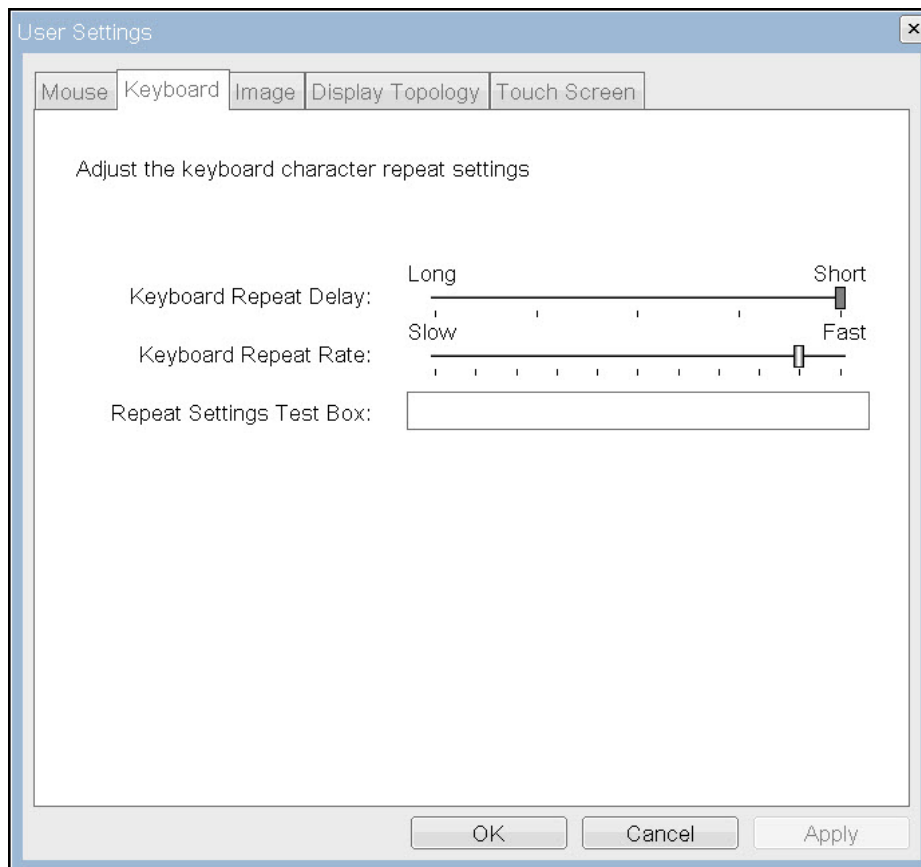


Figure 9-2: OSD Keyboard Page

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 [4.11](#).

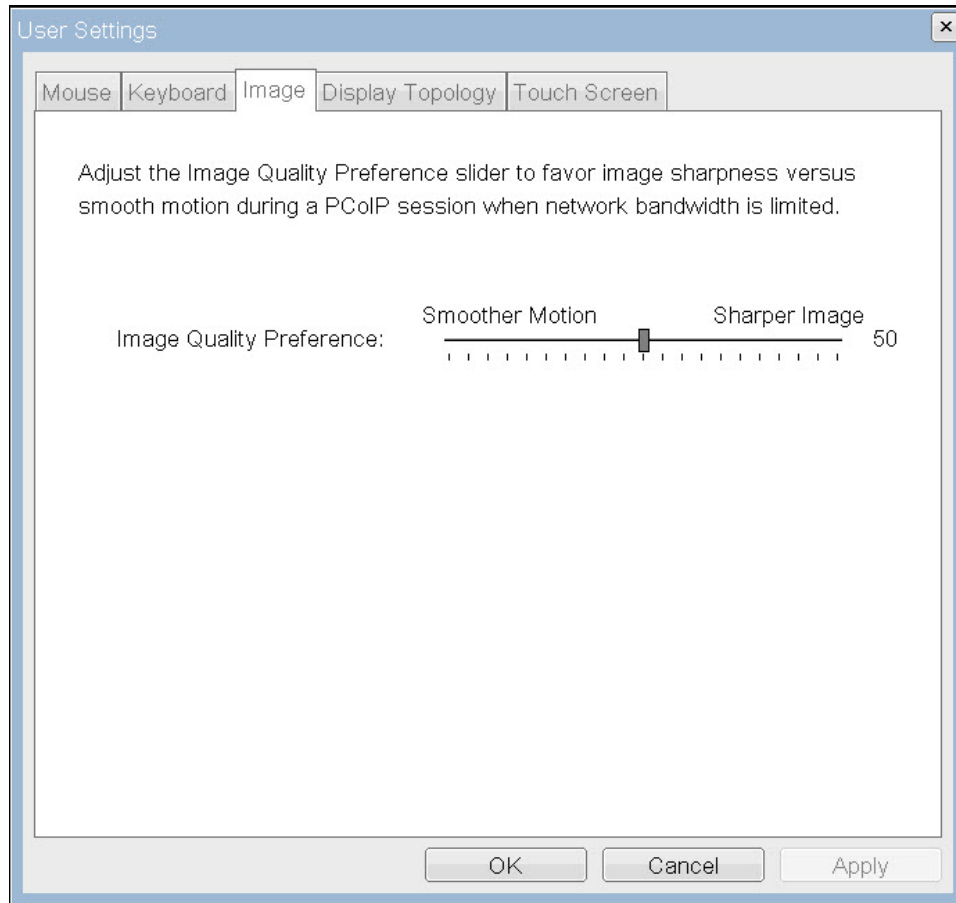


Figure 9-3: OSD Image Page

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.

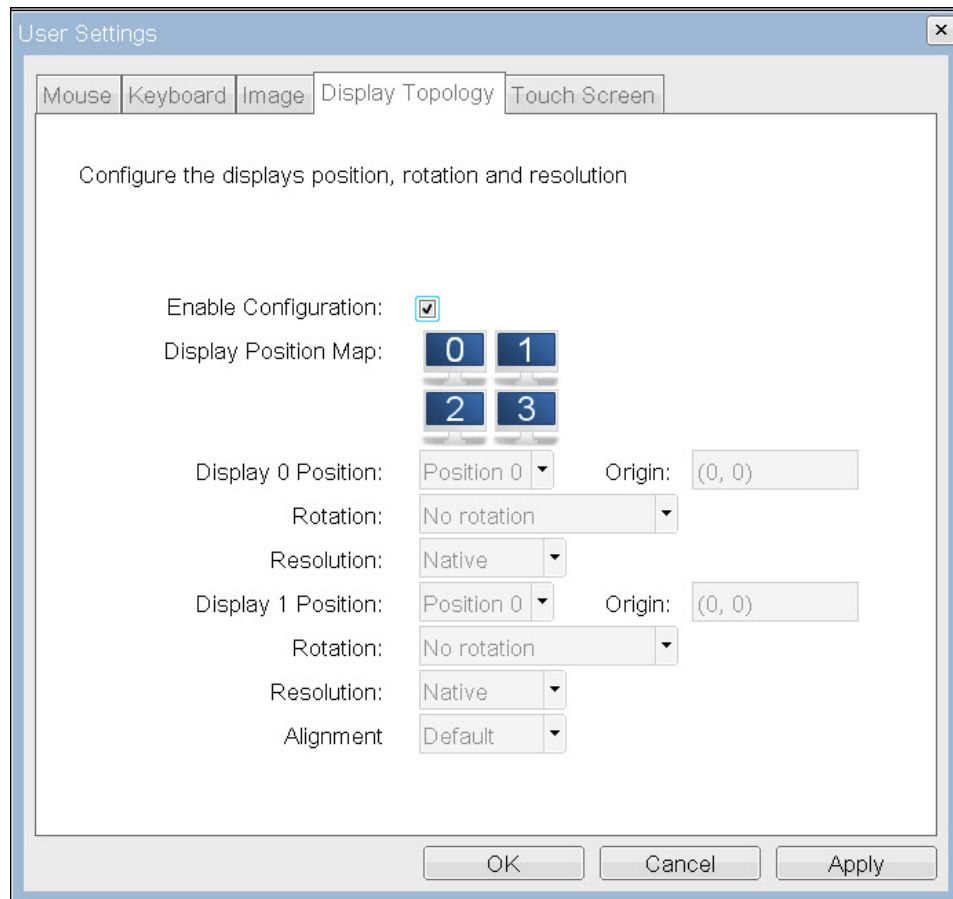


Figure 9-4: Display Topology Page

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
Alignment	Depending on the configuration of your monitors, you may want to set up the alignment. You can align your monitors horizontally or vertically, depending on their position.

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.

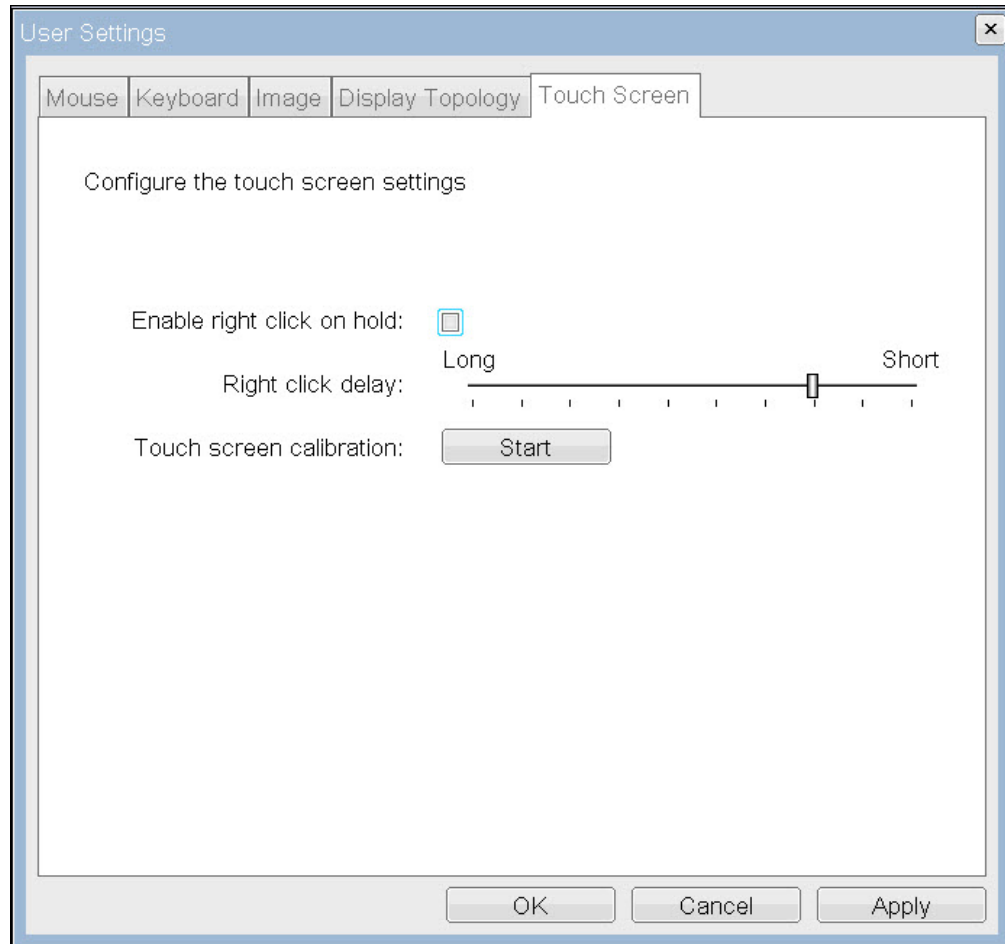


Figure 9-5: OSD Touch Screen Page

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

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 DVII, 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.

Attached Devices							
View presently connected monitors and USB devices							
Monitors:							
Name	Serial	VID	PID	Date	Status		
ET1515L	48954	ELO	1515	23-2010	Connected		
SME2320	HVRZA00941	SAM	6B2	42-2010	Connected		
USB Devices:							
Name	Serial	VID	PID	Device Class	Sub Class	Protocol	Status
USB Optical Mouse	-	046D	C05A	00	00	00	Locally Connected
USB Keyboard	-	046D	C31C	00	00	00	Locally Connected
Elo TouchSystems 2700 IntelliTouch(r) USB Touchmonitor Interface	20E38185	04E7	0020	00	00	00	Connected

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

USB

Configure the USB permissions table

The USB permissions table has been modified. Click 'Apply' to save your changes

Authorized Devices:

Any Device Class	Any Sub Class
------------------	---------------

Unauthorized Devices: *Table is empty*

Bridged Devices: *Table is empty*

Vendor ID:

Product ID:

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 4.7.

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".

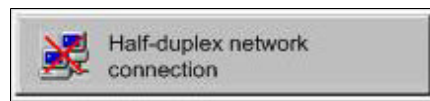


Figure 10-4: Half Duplex Overlay

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 later 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, the "PCoIP Smart Card Component" is enabled during View Agent 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 later 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 later
- VM Guest OS: Windows XP, Vista, Win7 with the View Agent PCoIP smart card component installed
- PCoIP zero client firmware 3.2.0 or later (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 later)
- PIV transitional cards (firmware 3.4.0 or later)
- PIV endpoint cards (firmware 3.4.0 or later)

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 later).

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 or later supports T=0. Firmware 3.4.0 and later 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 later)
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 later.

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.

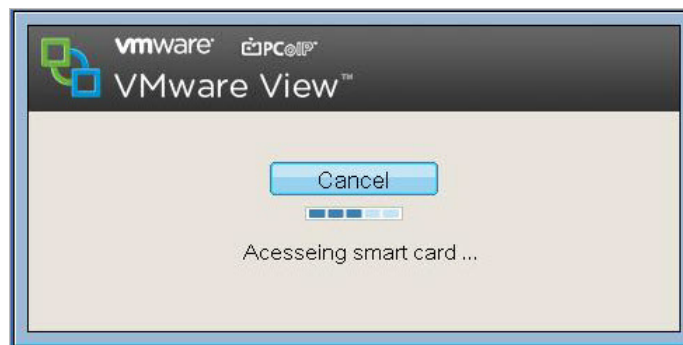


Figure 11-1: Accessing the Smart Card Message

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.

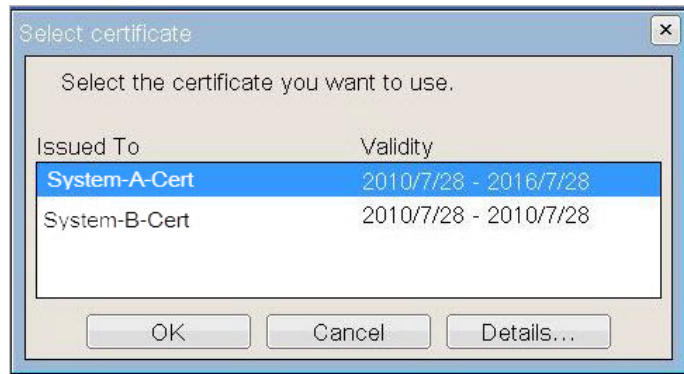


Figure 11-2: Select Certificate Prompt

2. Click **Details**.

The following window appears with the certificate details:

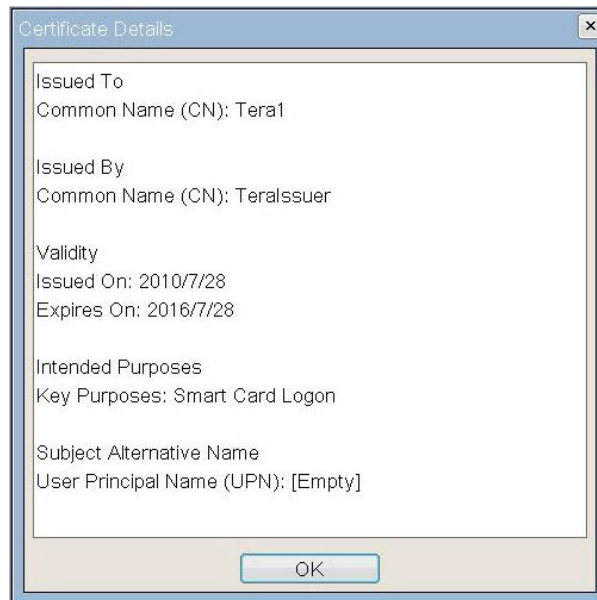


Figure 11-3: Certificate Details Window

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 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.

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

- **Client: IP Address:** 192.168.50.26, **MAC:** 00-30-04-0D-1A-6C
- **Host: IP Address:** 192.168.42.76, **MAC:** 00-1C-8A-03-00-CA

Note: For a peer-to-peer direct connection, you must know the IP address 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. From an Internet browser, enter the client's IP address, e.g., <https://192.168.50.26>.
2. Login to the client Administrative Web Interface (with password if enabled).
3. Select the **Session** page from the **Configuration** menu.
4. In the **Session Connection Type** field, select **Direct to Host**.

Session

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 192.168.42.76

Hide Advanced Options

Enable Wake-On-LAN:

Peer MAC Address: 00-0C-87-00-8A-53

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply Cancel

5. From the **DNS Name or IP Address** field, enter the IP address for the host. (For example, 192.168.42.76.)
6. Click **Apply** to accept the changes.

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

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

1. From an Internet browser, enter the host's IP address (for example, <https://192.168.42.76>).
2. Login to the host Administrative Web Interface (using a password if enabled).
3. From the **Configuration** menu, select the **Session** page.

Session

Configure the connection to a device

Session Connection Type: Direct from Client

Hide Advanced Options

Accept Any Peer:

Peer MAC Address: 00 - 30 - 04 - 0D - 1A - 6C

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Apply Cancel

4. From the **Session Connection Type** field, select **Direct from Client**.
5. Set the **Accept Any Peer** box:
 - Enable: Allow all zero clients to connect to the host
 - Disable: Allow only one zero client access to the host. Enter the client MAC address in the **Peer MAC Address** field.
6. 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 12-1: Peer-to-Peer Connect Screen

- 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

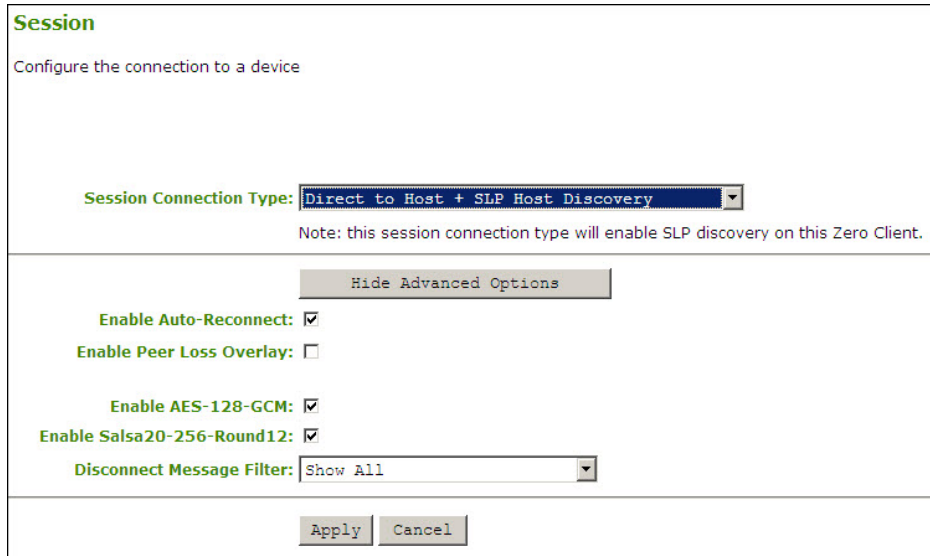
Note: To configure for DHCP and Host Discovery, you must know the IP address of the client and host, regardless of if it is set statically or dynamically.

A.2.1 Configuring the Client for 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 or PCoIP Management Console to configure the client.

To configure the client for DHCP and SLP discovery:

- From a browser, enter the IP address for the client, e.g., <https://192.168.0.111>.
- Login to the client Administrative Web Interface (with a password if enabled).
- From the **Configuration** menu, select **Session** to display the **Session** page.



Session

Configure the connection to a device

Session Connection Type: Direct to Host + SLP Host Discovery

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

Hide Advanced Options

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Disconnect Message Filter: Show All

Apply Cancel

- From the **Session Connection Type** field, select **Direct to Host + SLP Host Discovery**.
- Click **Apply**.
- Click **Continue** to complete the configuration.
- From the **Configuration** menu, select the **Discovery** page.

Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

8. Enable the **Enable SLP Discovery** box.
9. Click **Apply** to accept the changes.
10. Click **Continue** to complete the configuration.
11. From the **Configuration** menu, select the **Network** page.

Network

Change the network settings for the device

Enable DHCP:

IP Address: ...

Subnet Mask: ...

Gateway: ...

Primary DNS Server: ...

Secondary DNS Server: ...

Domain Name:

FQDN:

Ethernet Mode:

Maximum MTU Size: bytes

Enable 802.1X Security:

Authentication:

Identity:

Client Certificate:

Figure 12-2: Client Network Page DHCP Configuration

12. Enable the **Enable DHCP** box.
13. 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.

14. Click **Reset** to reset the PCoIP processor for the client.

A.2.2 Configuring the Host for Host DHCP and SLP Discovery

To configure the host for DHCP and SLP discovery:

1. From a browser, enter the host's 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 **Discovery** page.

Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

4. Enable the **Enable SLP Discovery** box.
5. Click **Apply** to accept the changes.
6. Click **Continue** to complete the configuration.
7. From the **Configuration** menu, select the **Network** page.

Network

Change the network settings for the device

Enable DHCP:

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

Primary DNS Server: . . .

Secondary DNS Server: . . .

Domain Name:

FQDN:

Ethernet Mode:

Maximum MTU Size: bytes

Enable 802.1X Security:

Authentication:

Identity:

Client Certificate:

Figure 12-3: Host Network Page DHCP Configuration

8. Select **Enable DHCP**.
9. 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.

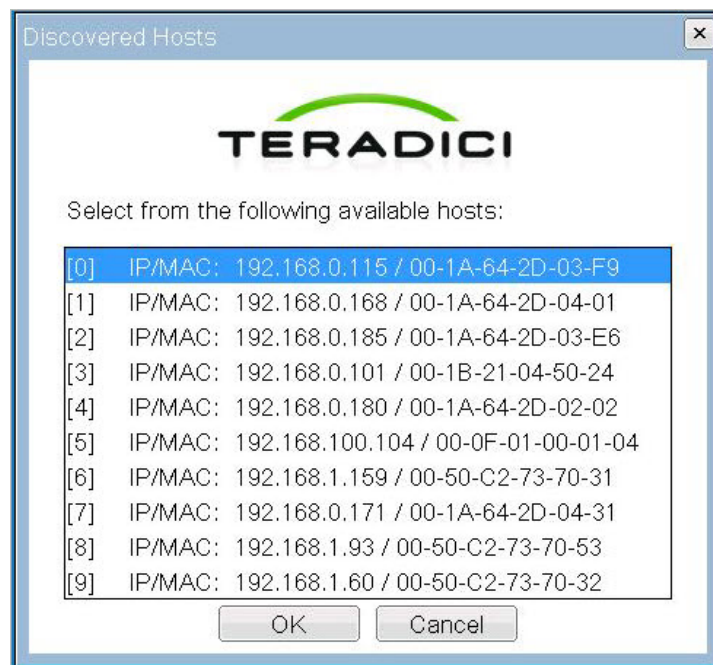
10. Click **Reset** to reset the PCoIP processor.

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 a PCoIP SLP discovery session:

1. From the OSD, click **Connect** to start discovering available hosts. The **Discovered Hosts** window appears and list of hosts that have the **Enable SLP** field enabled and are not currently in a session.
2. Select the desired host, and then click **OK**.



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

A.3 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.3.1 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**.
3. When the entry fields expand, select **Class** from the **Add New** drop-down menu to authorize a class of devices.
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.

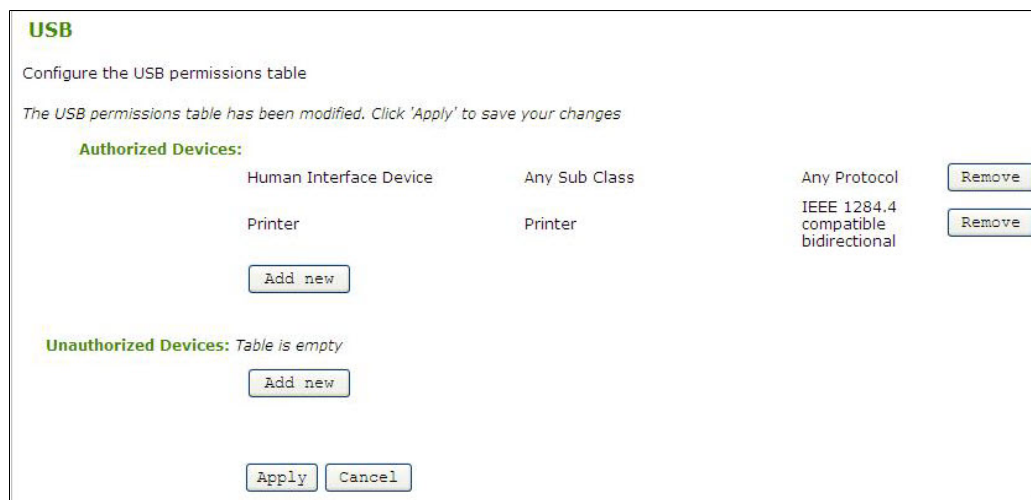


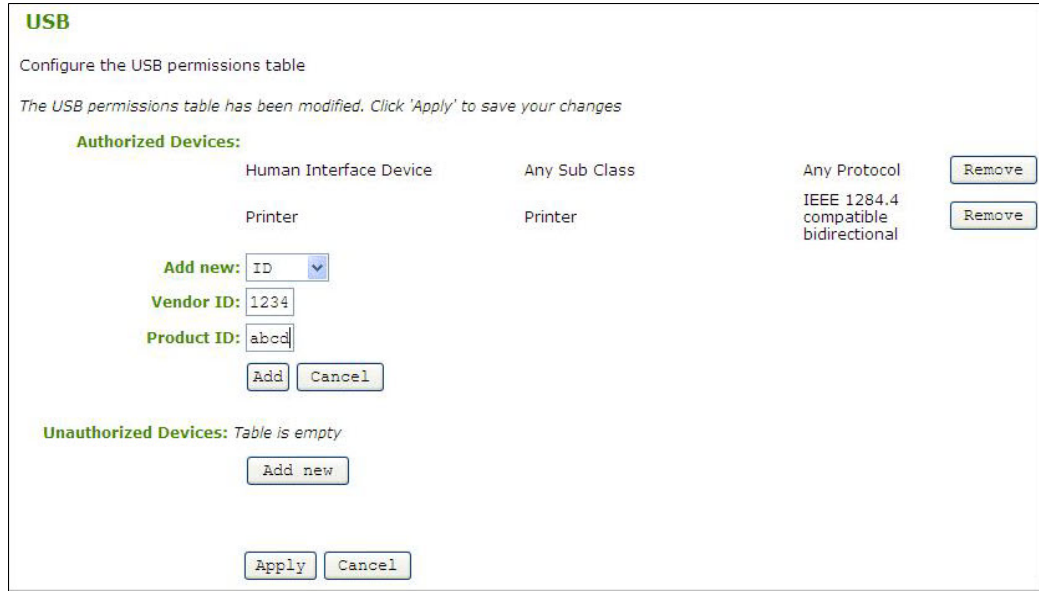
Figure 12-4: USB Permissions Example: Class Authorization

A.3.2 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**.
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.



USB

Configure the USB permissions table

The USB permissions table has been modified. Click 'Apply' to save your changes

Authorized Devices:

Human Interface Device	Any Sub Class	Any Protocol	<input type="button" value="Remove"/>
Printer	Printer	IEEE 1284.4 compatible bidirectional	<input type="button" value="Remove"/>

Add new: ID

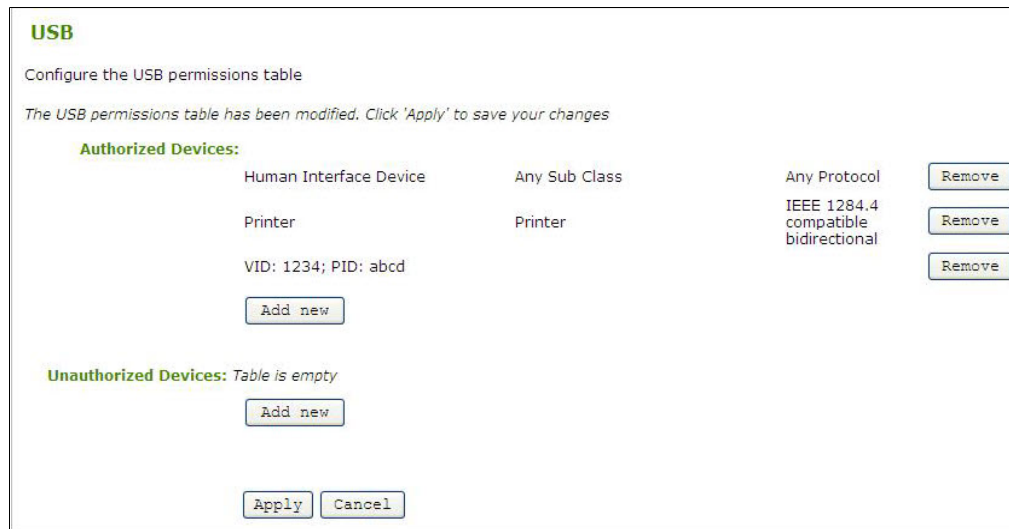
Vendor ID:

Product ID:

Unauthorized Devices: *Table is empty*

Figure 12-5: USB Permissions Example: Entering Vendor ID and Product ID

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



USB

Configure the USB permissions table

The USB permissions table has been modified. Click 'Apply' to save your changes

Authorized Devices:

Human Interface Device	Any Sub Class	Any Protocol	<input type="button" value="Remove"/>
Printer	Printer	IEEE 1284.4 compatible bidirectional	<input type="button" value="Remove"/>
VID: 1234; PID: abcd			<input type="button" value="Remove"/>

Unauthorized Devices: *Table is empty*

Figure 12-6: 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
- Finnish 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
- United Kingdom ISO-8859-1 (ctrl and caps swapped)
- United States of America Dvorak

- United States of America Dvorakx
- 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