

PC-over-IP[®] Administrative Interface

User Manual

(PCoIP Firmware Release 3.1.0)

TER0606004

Issue 10



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.

© 2010 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
1	January 15, 2008	Initial release
2	April 7, 2008	<p>Augmented definitions (see Definitions Section)</p> <p>Updated for Firmware Release 0.19</p> <ul style="list-style-type: none"> • Updated PCoIP Processor Information description (see Section 1/Figure 1-1) • Removed VLAN place holder from Network Configuration Webpage (see Section 1.6.1) • Added Maximum MTU Size in Network web configuration (see Section 1.6.2.10) • Added DNS SRV in Discovery web configuration (see Section 1.6.6.2) • Updated Session web configuration ordering (see Section 1.6.7) • Added Device Bandwidth Target to Bandwidth web configuration (see Section 1.6.9.2) • Updated RDP web configuration (see Section 1.6.9.3) • Added Maximum Initial Image Quality to Image web configuration (see Section 1.6.13.2) • Added Time web configuration (see Section 0) • Added Firmware Part Number in Version web information (see Section 1.9.1.1) • Updated Firmware Upload build filename web information (see Section 1.10.1.1) • Updated RDP OSD configuration (see Section 2.3.6) • Added Firmware Part Number in Version OSD information (see Section 2.5.1.1) • Clarified Bandwidth and Image Configuration Example (see Section 4.3) • Removed TERA1x00 Firmware Defaults appendix to enhance in separate Application Note <p>Updated for Firmware Release 0.20</p> <ul style="list-style-type: none"> • Added Bandwidth Statistics (see Section 1.8.3.5) <p>Updated RDP compatibility information (see Section 6)</p>
3	May 26, 2008	<p>Updated for Firmware Release 1.00</p> <ul style="list-style-type: none"> • Updated text and figure references to Portal • Added warning to Ethernet Mode section concerning PC-over-IP Half-Duplex in compatibility (Section 1.6.2.9) • Clarified when Device Bandwidth Limit and Device Bandwidth Target are applied (Section 1.6.9) • Updated USB Permissions documentation for USB

		<p>authorization/unauthorization functionality (Section 1.7.1)</p> <ul style="list-style-type: none"> • Added USB devices status descriptions in Attached Devices - USB Devices (Section 1.9.2.2)
4	Sep 12, 2008	<p>Updated for Firmware Release 1.4</p> <ul style="list-style-type: none"> • Added menu navigation overview (Figure 1-2: Administrative Web Interface Overview) • Added Initial Setup/Home webpage information (Section 1.5) • Added Initial Setup webpage details (Section 1.6.1) • Updated Enable Auto-Reconnect detail (Section 1.6.5.4) • Updated Ethernet Mode for Host (Section 1.6.1.7) • Added Enable Vista64 Mode (Section 1.7.2.3) • Added Half-Duplex Overlay (Section 3.3) <p>Added Video Source Overlays (Section 3.4)</p>
5	Nov 25, 2008	<p>Improved document wording and fixed errors</p> <p>Updated for Firmware Release 1.8</p> <p>Adjusted formatting; replaced bitmap graphics w/ GIFs to reduce file size</p>
6	May 14, 2009	<p>Updated for Firmware Release 2.1</p> <p>Modified to note some PCoIP devices have password webpage and password protection disabled by default</p> <p>Updated to note some webpages are only available for Host or Portal</p> <p>Added Domain Name and FQDN parameter details in Section 1.6.2</p> <p>Added description for Label webpage in Section 1.6.3</p> <p>Added description for VMware View webpage in Section 1.6.5</p> <p>Updated description (Device Bandwidth Floor) for Bandwidth webpage in Section 1.6.9</p> <p>Updated figure for Image webpage in Section 1.6.13</p> <p>Added description for Host Driver Function webpage in Section 1.6.15</p> <p>Updated description (removed Enable Audio Compression) for Audio webpage in Section 1.8.5</p> <p>Updated Section 2 OSD parameter descriptions to reflect changes described above</p> <p>Updated examples in Section 4 to reflect Firmware Release 2.0</p> <p>Updated webpage figures to reflect Release 2.x</p> <p>Added information for the Authorized Password Reset OSD feature in Section 2.7</p>

		Miscellaneous typo corrections and updates
7	Jun 15, 2009	<p>Updated for Firmware Release 2.2</p> <p>Added description for enable display override in Section 2.3.10</p> <p>Clarified Network Connection Lost overlay description (2 seconds of network inactivity) in Section 3.1</p>
8	Oct 22, 2009	<p>Updated for Firmware Release 2.3</p> <p>Added notes about Host and Portal webpage banners (Section 1)</p> <p>Added description for SNMP enable feature (see Section 1.6.7)</p>
9	Dec 08, 2009	<p>Updated for Firmware Release 3.0</p> <p>Simplified to endpoint terms “client” and “host card”</p> <p>Updated description for Home webpage (see Section 1.5.1)</p> <p>Added description for Enable AES-128-GCM (see Section 1.6.8.5) and Enable SALSA20-256-Round12 (see Section 1.6.8.6)</p> <p>Updated description to use kbps for Bandwidth (see Section 1.6.9)</p> <p>Updated description for OSD configuration (see Sections 1.6.12 and 2.3.8)</p> <p>Updated description for USB permission (see Section 1.7.1)</p> <p>Updated description for Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode (see Section 1.7.2.2) for Windows 7 64-bit</p> <p>Updated Session Statistics description for improved session stats (see Section 1.8.3)</p> <p>Added USB Over Current Notice Overlay description (see Section 3.3)</p> <p>Updated Appendix B: Client Language and Keyboard Support to include the Korean dubeolsik keyboard (see Section 5)</p>
10	Apr 06, 2010	<p>Updated for Firmware Release 3.1.0.</p> <p>Updated Section 2 On Screen Display (OSD) with appropriate references to Section 1 Administrative Web Interface.</p> <p>Updated Appendix B: Client Language and Keyboard Support to include Belgian, Danish, Finnish, Norwegian, Polish, Swedish and Turkish keyboards (see Section 5)</p>

Contents

REVISION HISTORY 2

CONTENTS 5

TABLE OF FIGURES 8

TABLES 11

DEFINITIONS 12

INTRODUCTION..... 13

1 ADMINISTRATIVE WEB INTERFACE 14

1.1 Supported Web Browsers.....16

1.2 Admin Interface IP Address16

1.3 Admin Interface Security17

 1.3.1 Installing the CA Root Certificate.....17

1.4 Log In.....18

 1.4.1 Warning18

 1.4.2 Password.....18

 1.4.3 Idle Timeout.....18

1.5 Home/Initial Setup Webpages.....19

 1.5.1 Home.....19

 1.5.2 Initial Setup.....20

1.6 Configuration Menu20

 1.6.1 Initial Setup.....21

 1.6.2 Network25

 1.6.3 Label28

 1.6.4 Connection Management29

 1.6.5 VMware View.....30

 1.6.6 Discovery.....32

 1.6.7 SNMP33

 1.6.8 Session33

 1.6.9 Bandwidth.....36

 1.6.10 RDP.....37

 1.6.11 Language.....38

 1.6.12 OSD39

 1.6.13 Image40

 1.6.14 Monitor Emulation.....41

 1.6.15 Host Driver Function41

 1.6.16 Time.....42

 1.6.17 Password.....43

 1.6.18 Reset Parameters.....44

- 1.7 Permissions Menu44**
 - 1.7.1 USB.....45
 - 1.7.2 Audio47
 - 1.7.3 Power48
- 1.8 Diagnostics Menu48**
 - 1.8.1 Event Log.....49
 - 1.8.2 Session Control.....49
 - 1.8.3 Session Statistics.....50
 - 1.8.4 Host CPU52
 - 1.8.5 Audio53
 - 1.8.6 Display54
 - 1.8.7 PCoIP Processor54
- 1.9 Info Menu55**
 - 1.9.1 Version.....55
 - 1.9.2 Attached Devices57
- 1.10 Upload Menu58**
 - 1.10.1 Firmware.....58
 - 1.10.2 OSD Logo59
- 2 ON SCREEN DISPLAY (OSD)..... 61**
 - 2.1 Connect Screen.....61**
 - 2.1.1 Connect Button62
 - 2.2 OSD Options Menu.....62**
 - 2.3 Configuration Window.....63**
 - 2.3.1 Network Tab64
 - 2.3.2 Label Tab65
 - 2.3.3 Connection Management Tab66
 - 2.3.4 Discovery Tab.....66
 - 2.3.5 Session Tab67
 - 2.3.6 RDP Tab68
 - 2.3.7 Language Tab69
 - 2.3.8 OSD Tab70
 - 2.3.9 Reset Tab71
 - 2.3.10 Display Tab.....71
 - 2.3.11 VMware View Tab72
 - 2.4 Diagnostics Window.....73**
 - 2.4.1 Event Log Tab74
 - 2.4.2 Session Statistics Tab.....74
 - 2.4.3 PCoIP Processor Tab75
 - 2.4.4 Ping Tab.....76
 - 2.5 Information Window77**
 - 2.6 User Settings Window.....78**
 - 2.6.1 Mouse Tab78
 - 2.6.2 Keyboard Tab79
 - 2.6.3 Image Tab79
 - 2.7 Password Window.....80**

3	OVERLAY WINDOWS	82
3.1	Network Connection Lost Overlay	82
3.2	USB Device Not Authorized Overlay	82
3.3	USB Over Current Notice Overlay.....	82
3.4	Half-Duplex Overlay.....	83
3.5	Video Source Overlays	83
4	APPENDIX A: USAGE EXAMPLES	84
4.1	Peer-to-Peer Direct Connection Example.....	84
4.1.1	Configuring the Client Peer-to-Peer Operation.....	84
4.1.2	Configuring the Host Peer-to-Peer Operation.....	86
4.1.3	Initiating the Peer-to-Peer Session.....	87
4.2	DHCP and Enable Host Discovery Example.....	88
4.2.1	Configuring Client DHCP and SLP Discovery.....	88
4.2.2	Configuring Host DHCP and SLP Discovery.....	90
4.2.3	Initiating SLP Discovery Session	92
4.3	Bandwidth and Image Configuration Example	93
4.3.1	Configuring the Host Bandwidth Limit to 25 Mbps	94
4.3.2	Configuring Image Properties	96
4.3.3	Configuring the Host Bandwidth Limit to 0 Mbps (No Limit).....	97
4.4	USB Permissions Example	99
4.4.1	Authorizing USB Device By Class.....	99
4.4.2	Authorizing USB Device By Vendor/Product ID.....	102
5	APPENDIX B: CLIENT LANGUAGE AND KEYBOARD SUPPORT	105
6	APPENDIX C: CLIENT RDP COMPATIBILITY	108

Table of Figures

Figure 1-1: Administrative Web Interface	15
Figure 1-2: Administrative Web Interface Overview	16
Figure 1-3: Log In Webpage	18
Figure 1-5: Home Page.....	19
Figure 1-6: Configuration Menu Navigation	21
Figure 1-6: Initial Setup Host Webpage	22
Figure 1-7: Initial Setup Client Webpage	23
Figure 1-9: Network Configuration Webpage	26
Figure 1-10: Label Configuration Webpage	28
Figure 1-11: Connection Management Configuration Webpage (IP Address)	29
Figure 1-12: Connection Management Configuration Webpage (FQDN).....	29
Figure 1-13: VMware View Configuration Webpage.....	31
Figure 1-14: Discovery Configuration Webpage	32
Figure 1-14: SNMP Configuration Webpage	33
Figure 1-16: Session Configuration Webpage	34
Figure 1-17: Session Configuration Webpage (RDP – client only).....	34
Figure 1-18: Bandwidth Configuration Webpage	36
Figure 1-19: RDP Configuration Webpage	37
Figure 1-20: Language Configuration Webpage.....	39
Figure 1-21: OSD Configuration Webpage	39
Figure 1-22: Image Configuration Webpage.....	40
Figure 1-23: Monitor Emulation Configuration Webpage.....	41
Figure 1-23: Host Driver Function Configuration Webpage.....	41
Figure 1-25: Time Configuration Webpage.....	42
Figure 1-26: Password Configuration Webpage	43
Figure 1-27: Reset Parameters Webpage	44
Figure 1-28: Permissions Menu Navigation	44
Figure 1-29: USB Permissions Webpage	45
Figure 1-30: Audio Permissions Webpage	47
Figure 1-31: Power Permissions Webpage	48
Figure 1-32: Diagnostics Menu Navigation	48
Figure 1-33: Event Log Webpage	49
Figure 1-34: Session Control Webpage.....	50
Figure 1-35: Session Statistics Webpage.....	51
Figure 1-36: Host CPU Webpage	53
Figure 1-37: Audio Diagnostics Webpage	53

Figure 1-38: Display Webpage	54
Figure 1-39: PColP Processor Webpage	55
Figure 1-40: Info Menu Navigation.....	55
Figure 1-41: Version Webpage	56
Figure 1-42: Attached Devices Webpage	57
Figure 1-43: Upload Menu Navigation	58
Figure 1-44: Firmware Upload Webpage.....	58
Figure 1-45: OSD Logo Upload Webpage.....	59
Figure 2-1: OSD Connect Screen	61
Figure 2-2: Network Not Ready (detail)	62
Figure 2-3: Network Ready (detail).....	62
Figure 2-4: OSD Connect Screen (Connecting)	62
Figure 2-8: OSD Options Menu	63
Figure 2-9: Network Configuration	64
Figure 2-10: Label Configuration	65
Figure 2-11: Connection Management Configuration.....	66
Figure 2-12: Discovery Configuration	67
Figure 2-13: Session Configuration	68
Figure 2-14: RDP Configuration.....	69
Figure 2-15: Language Configuration	70
Figure 2-16: OSD Configuration	70
Figure 2-17: Reset	71
Figure 2-18: Enable Display Override Configuration	72
Figure 2-19: VMware View Configuration	73
Figure 2-20: Event Log	74
Figure 2-21: Session Statistics	75
Figure 2-22: PColP Processor	76
Figure 2-23: Ping.....	76
Figure 2-24: Version.....	77
Figure 2-25: Mouse	78
Figure 2-26: Keyboard	79
Figure 2-27: Image.....	80
Figure 2-28: Change Password	80
Figure 2-29: Authorized Password Reset	81
Figure 3-1: Network Connection Lost Overlay.....	82
Figure 3-3: USB Device Not Authorized Overlay.....	82
Figure 3-5: USB Over Current Notice Overlay.....	82
Figure 3-7: Half-Duplex Overlay	83
Figure 3-9: No Source Signal Overlay	83

Figure 3-11: Source Signal on Other Port Overlay 83

Figure 4-1: Client Discover Configuration (Enable SLP Discovery disabled)..... 84

Figure 4-2: Client Connection Management Peer-to-Peer Configuration..... 85

Figure 4-3: Client Session Webpage Peer-to-Peer Configuration..... 85

Figure 4-4: Client PCoIP Processor Webpage Peer-to-Peer Configuration..... 86

Figure 4-5: Host Connection Management Peer-to-Peer Configuration..... 86

Figure 4-6: Host Session Webpage Peer-to-Peer Configuration..... 87

Figure 4-7: Peer-to-Peer Connect Screen 88

Figure 4-8: Client Connection Management Configuration 89

Figure 4-9: Client Discovery Webpage Enable SLP Discovery Configuration 89

Figure 4-10: Client Network Webpage DHCP Configuration..... 90

Figure 4-11: Client PCoIP Processor Webpage 90

Figure 4-12: Host Connection Management Configuration 91

Figure 4-13: Host Discovery Webpage Enable SLP Discovery Configuration 91

Figure 4-14: Host Network Webpage DHCP Configuration..... 92

Figure 4-15: Host PCoIP Processor Webpage 92

Figure 4-16: Connect Screen..... 93

Figure 4-17: Discovered Hosts Screen..... 93

Figure 4-18: Simplified User Bandwidth Requirements (Assuming 100 Mbps)..... 94

Figure 4-20: Host Bandwidth Limit Configuration (25 Mbps)..... 95

Figure 4-21: Simplified User Bandwidth Requirements (25 Mbps)..... 96

Figure 4-23: Client Minimum Image Quality Configuration..... 97

Figure 4-24: Host Bandwidth Limit Configuration (0 Mbps, no limit) 98

Figure 4-25: Simplified User Bandwidth Requirements (no limit) 98

Figure 4-27: USB Permissions Example: Add new Button 99

Figure 4-28: USB Permissions Example: Selecting the Class Entry Type 100

Figure 4-29: USB Permissions Example: Selecting the Device Class 100

Figure 4-30: USB Permissions Example: Selecting the Sub Class 101

Figure 4-31: USB Permissions Example: Selecting the Protocol 101

Figure 4-32: USB Permissions Example: Class Authorization 102

Figure 4-33: USB Permissions Example: Add new Button 102

Figure 4-34: USB Permissions Example: Selecting the Class Entry Type 103

Figure 4-35: USB Permissions Example: Entering Vendor ID and Product ID..... 103

Figure 4-36: USB Permissions Example: Vendor ID and Product ID Authorization..... 104

Tables

Table 1-1: Home Webpage Parameters	20
Table 1-2: Step 1: Audio Parameters.....	24
Table 1-3: Step 2: Network Parameters.....	24
Table 1-4: Step 3: Host Session Parameters	25
Table 1-5: Step 3: Client Session Parameters.....	25
Table 1-7: Connection Manager Method	30
Table 1-9: Peer Identify Methods.....	35
Table 1-8: NTP Host Method	43
Table 1-10: USB Device Authorization Entry Types	46
Table 1-12: USB Device Unauthorization Entry Types.....	47
Table 1-13: VPD Information	56
Table 1-14: Firmware Information.....	56
Table 1-15: VPD Information	57
Table 1-16: USB Device Status	57
Table 5-1: Languages Supported by the Client	105
Table 5-2: Keyboard Layouts Supported by the Client.....	105
Table 6-1: RDP Capabilities.....	108

Definitions

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 (3rd 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, i.e. client (e.g. PCoIP Portal or PCoIP Integrated Display)
PCoIP Host	Host side of PC-over-IP system
RDP	Remote Desktop Protocol
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

Introduction

Users and administrators can interact with PCoIP® Zero Clients and Host Cards (or “clients” and “hosts”) via an embedded HTTPS web interface. This Administrative Web Interface (or “admin interface”) allows configuration for hosts and clients.

The client can also be accessed via the local Graphical User Interface (GUI) On Screen Display (OSD). As well, messages are displayed overlaid on the user display when required.

Note: This document describes the admin interface for hardware PCoIP protocol devices. The administrative interface for the soft PCoIP protocol is not described in this document.

This document describes the client and host user interfaces for PCoIP Firmware Release 3.0 (or “firmware”). When a feature is only available for the host or client, this is explicitly stated.

This document has three main sections:

- Section 1 details the PCoIP Administrative Web Interface
- Section 2 reviews the On Screen Display (OSD) of the client
- Section 3 discusses the user message Overlay Windows

The Appendix contains:

- Appendix A: Usage Examples
- Appendix B: Client Language and Keyboard Support
- Appendix C: Client RDP Compatibility

This document is intended to give administrators and users a working understanding of a PCoIP system.

Note: The admin interface and OSD configuration features are also available via connection brokers and the PCoIP Management Console. However, connection brokers and the PCoIP Management Console details are outside the scope of this document. For more information on connection brokers contact connection broker vendors. For more information on the PCoIP Management Console (web based tool to manage multiple PCoIP endpoints) refer to the *PCoIP Management Console User Manual* (TER0812002).

1 Administrative Web Interface

The PColP Administrative Web Interface allows an administrator to interact with the device remotely using an Internet browser. The host and client webpages have unique banners to easily identify each (see Figure 1-1 for a host example and Figure 1-3 for a client example).

Users can connect or disconnect a session, view diagnostics, and configure user parameters. Administrators can view and change configuration settings and user permissions, upload data to the PColP device, view session diagnostics information, and view product information.

The interfaces are structured in a task-oriented fashion intended to maximize accessibility and minimize the learning curve. Additionally, the web interface and OSD are organized as similarly as possible, to reduce the total user learning curve.

Figure 1-1 shows an example of the host admin interface with seven regions highlighted:

- Log Out: Allows an administrator to log out of the admin interface
- PColP endpoint: Displays PColP endpoint information
 - PColP® Host Card
 - PColP® Zero Client
- Home: Allows an administrator to navigate to the Home webpage
- Drop-down menus: The five menus are Configuration, Permissions, Diagnostics, Info, and Upload
- Webpage information: Displays the title and summary of the current webpage
- Data field: Shows editable and/or displayed parameters that an administrator can configure from the current webpage (inline help is displayed when appropriate)
- Apply/Cancel: Every webpage with editable parameters has an Apply button and a Cancel button
 - Selecting Apply will store the edited parameters in flash
 - Selecting Cancel will reset the edited parameters to the values currently stored in flash.

Figure 1-1: Administrative Web Interface

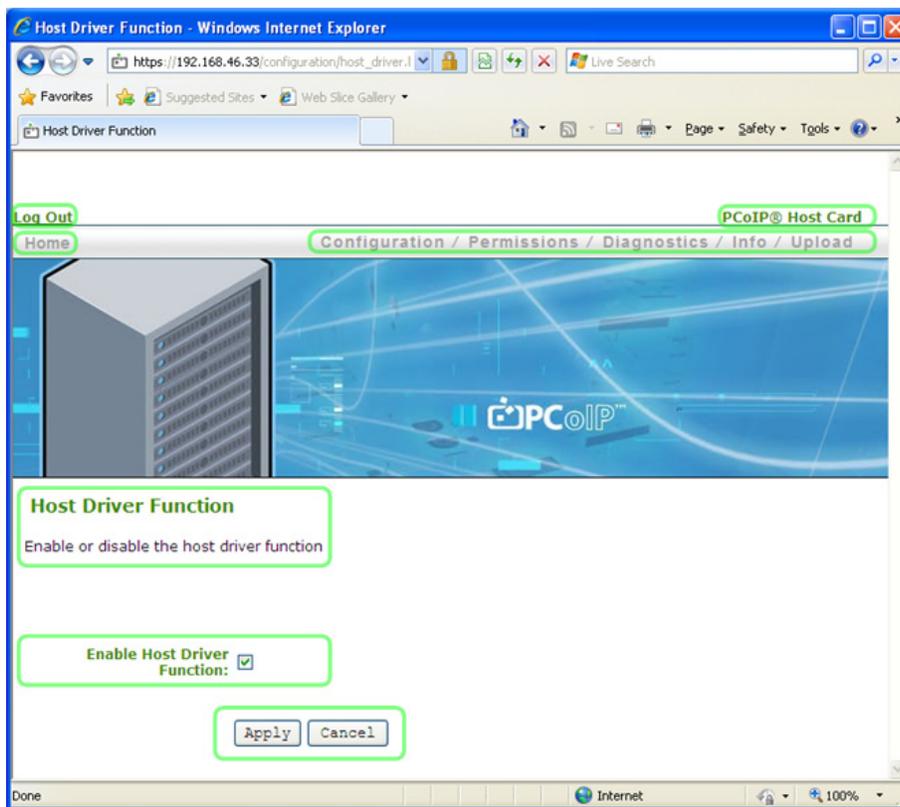
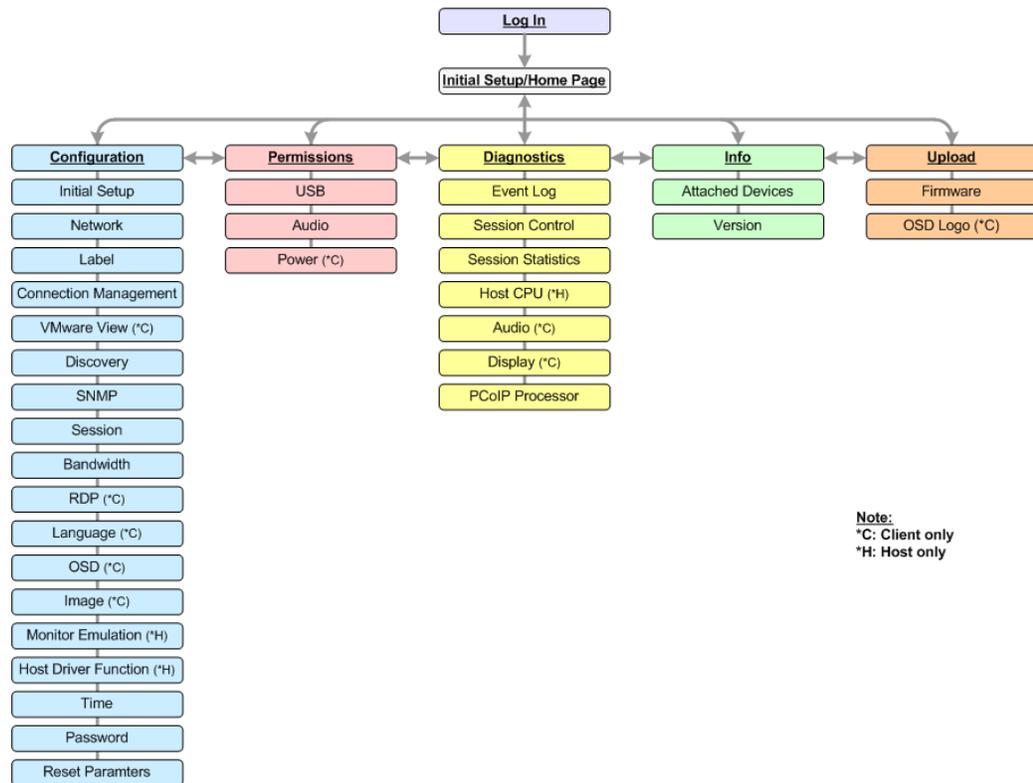


Figure 1-2 shows an overview of the configuration webpages available in the admin interface.

Figure 1-2: Administrative Web Interface Overview



Note:
 *C: Client only
 *H: Host only

1.1 Supported Web Browsers

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

- Firefox 1.5, 2.0 and 3.0
- Internet Explorer 6.0 and 7.0

Other browsers may also be compatible.

We strongly recommend you install the CA root certificate in the browser you use (see Section 1.3.1).

Note: A CA root certificate may be installed in the browser to avoid warning messages.

1.2 Admin Interface IP Address

To access the admin interface, the administrator must browse to the IP address of the host or client. The IP address used depends on how the IP addresses are determined within your IP network:

- Static IP Address: the IP address is hard-coded and must be known
- Dynamic IP Address: the IP address is dynamically assigned by the Dynamic Host Configuration Protocol (DHCP) server and can be obtained from the DHCP server

Once the administrator has determined the IP address, enter it into the browser to access the admin interface, e.g. <https://192.168.1.123>.

Note: Some networks using DHCP may be able to also access the admin interface using the *PCoIP Device Name*. See Section 1.6.3.1 for more information.

1.3 Admin Interface Security

The admin interface uses HTTP over an SSL socket (HTTPS), and cannot be accessed 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.

1.3.1 Installing the CA Root Certificate

The administrator can install a Certificate Authorities (CA) root certificate in the Internet browser to avoid the browser security warnings. Steps for installing the certificate on Internet Explorer 7 and Firefox are detailed below:

Internet Explorer 7

1. Open the *Tools* menu and select *Internet Options*
2. On the *Content* tab, and select *Certificates*
3. On the *Trusted Root Certification Authorities* tab, select *Import*
4. Follow the directions to import the certificate; ensure you use the *Trusted Root Certification Authorities* certificate store

Note: When browsing for the certificate, it may be necessary to change the file type to *all files*.

Firefox

1. Open the *Tools* menu and select *Options*
2. Select the icon labeled *Advanced* at the top of the window
3. On the *Encryption* tab, select *View Certificates*
4. On the *Authorities* tab, select *Import*
5. Follow the directions to import the certificate; ensure you check the option labeled *Trust this CA to identify web sites*

1.4 Log In

The *Log In* page allows the administrator to log into the admin interface webpages. Figure 1-3 shows the *Log In* page for the client.

Figure 1-3: Log In Webpage



Note: Some PCoIP devices have password protection disabled by default and do not require a password to login. Password protection for the *Log In* page can be enabled or disabled using the PCoIP Management Console; refer to the *PCoIP Management Console User Manual* (TER0812002) for more information.

1.4.1 Warning

The *Warning* displays pertinent information regarding the device the administrator is logging in to when there is an administrative session already in progress. Only one administrator is allowed per device. Logging into a session will terminate any other administrative session in progress.

1.4.2 Password

The *Password* field allows the administrator to enter the password to gain access to the admin interface webpage. The default value is blank, i.e. "".

See Section 1.6.17 for information on changing the password.

1.4.3 Idle Timeout

The *Idle Timeout* field sets the administration idle timeout. The options are:

- 1 minute
- 5 minutes
- 15 minutes
- 30 minutes
- Never

1.5 Home/Initial Setup Webpages

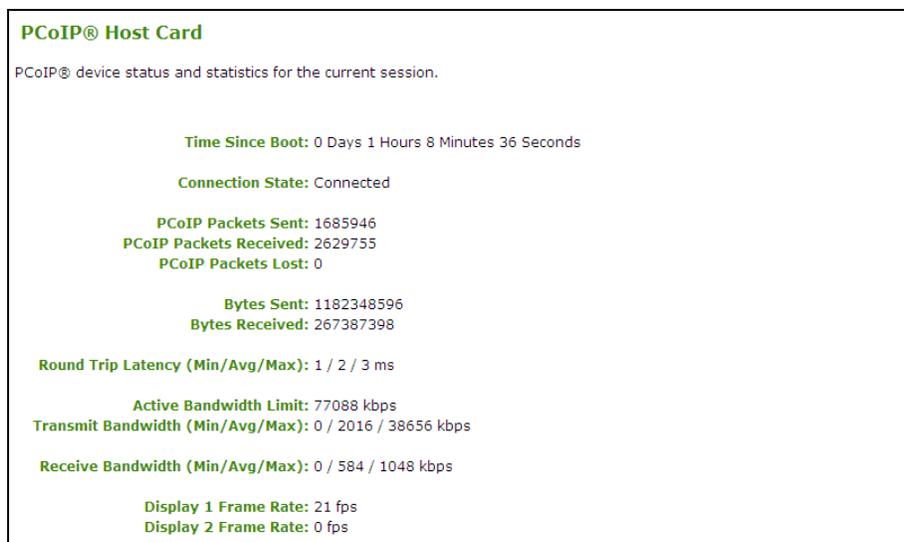
When an administrator logs in, the *Home* webpage is shown. The *Home* webpage provides an overview of the status.

If configured in the firmware defaults, the *Initial Setup* webpage is optionally used the first time an administrator logs in. Afterwards the *Home* page is shown unless the firmware parameters reset (see Section 1.6.18 Reset Parameters)

1.5.1 Home

The *Home* webpage provides a summary of the host or client. It can be accessed at any time using the *Home* link at the top left section of the menu bar.

Figure 1-4: Home Page



The information fields shown on the *Home* webpage are summarized in Table 1-1.

Note: The *Reset Statistics* button (see Section 1.8.3.7) also resets the statistics reported in the *Home* webpage.

Table 1-1: Home Webpage Parameters

Parameter	Comments
Time since boot	Length of time that the PColP processor has been running (refer to Section 1.8.7)
Connection State	Possible states: Disconnected, Connection Pending, Connected (refer to Section 1.8.3)
Packet Statistics	Packets sent (refer to Section 1.8.3)
	Packets received (refer to Section 1.8.3)
	Packets lost (refer to Section 1.8.3)
Byte Statistics	Bytes sent (refer to Section 1.8.3)
	Bytes received
Round Trip Latency	Approximate network min, average and max round trip latency, e.g. client to host and back to client (refer to Section 1.8.3)
Bandwidth Stats:	Active bandwidth Limit is bandwidth PColP processors may generate (refer to Section 1.8.3)
	Transmit Bandwidth is min, average and max traffic transmitted (refer to Section 1.8.3)
	Receive Bandwidth is min, average and max traffic received refer to Section 1.8.3)
Display Frame Rates	Display Rate for video content through PColP protocol; e.g. if nothing changing, Frame Rate is 0 fps (refer to Section 1.8.3)

1.5.2 Initial Setup

The *Initial Setup* webpage contains the configuration parameters that must be first set by the administrator when using the host and client devices. See Section 1.6.1 Initial Setup for more information.

1.6 Configuration Menu

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

- Initial Setup
- Network
- Label
- Connection Management
- VMware View (client only)
- Discovery
- SNMP
- Session

- Bandwidth
- RDP(client only)
- Language (client only)
- OSD (client only)
- Image (client only)
- Host Driver Function (host only)
- Time
- Password
- Reset Parameters

Figure 1-5: Configuration Menu Navigation



1.6.1 Initial Setup

The *Initial Setup* webpage contains the configuration parameters that the administrator must first set when using the client and host devices. The webpage simplifies the out-of-box experience and reduces the time for initial users to establish a 1-to-1 PCoIP session. More complex environments that use host discovery or connection management systems will require further configuration.

The client and host Initial Setup webpages are not identical and provide parameters applicable to the client and host, respectively.

Figure 1-6: Initial Setup Host Webpage

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.

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 1-7: Initial Setup Client Webpage

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

Session Type: ▼

Identify Host by: IP address FQDN

Host IP Address:

Host MAC Address:

Step 4: Apply Changes

1.6.1.1 Step 1: Audio

Step 1: Audio allows the administrator to configure the audio parameters. Table 1-2 summarizes the applicable parameters.

Table 1-2: Step 1: Audio Parameters

Parameter	Comments
Enable HD Audio	Enables audio support on host or client (refer to Section 1.7.2).
Enable Microsoft® Windows Vista® 64-bit Mode	<p>Enables 64-bit mode on host (refer to Section 1.7.2). This mode should only be used for Windows Vista 64-bit and Windows 7 64 bit versions.</p> <p>This option is only available on a host; on the client it is not shown.</p> <p>Note: Enabling 64-bit mode is not required for Linux or Windows XP (32-bit or 64-bit); refer to section 1.7.2.</p>

1.6.1.2 Step 2: Network

Step 2: Network allows the administrator to configure the network parameters. Table 1-3 summarizes the applicable parameters.

Table 1-3: Step 2: Network Parameters

Parameter	Comments
Enable DHCP	Enables DHCP vs. manual configuration (refer to Section 1.6.2).
IP Address	Device's IP address (refer to Section 1.6.2).
Subnet Mask	Device's subnet mask (refer to Section 1.6.2).
Gateway	Device's gateway IP address (refer to Section 1.6.2).
Primary DNS Server	Device's primary DNS IP address (refer to Section 1.6.2).
Secondary DNS Server	Device's secondary DNS IP address (refer to Section 1.6.2).

1.6.1.3 Step 3: Session

Step 3: Session allows the administrator to configure the session parameters. Table 1-4 summarizes the host parameters and Table 1-5 shows the client parameters.

Table 1-4: Step 3: Host Session Parameters

Parameter	Comments
Accept Any Client	Allows the host to accept any client for a PCoIP Session (refer to Section 1.6.7).
Client MAC Address	Allows the administrator to specify the client MAC address for a PCoIP Session (refer to Section 1.6.7).

Table 1-5: Step 3: Client Session Parameters

Parameter	Comments
Session Type	Specifies the PCoIP protocol or RDP (refer to Section 1.6.7).
Identify Host by	Specifies the host identify method (refer to Section 1.6.7).
Host IP Address	Specifies the host IP address (refer to Section 1.6.7).
Host MAC Address	Specifies the host MAC address (refer to Section 1.6.7).

Note: When Host Discovery or connection management is configured by default on the client, it is not possible to modify the client session parameters. A message will be displayed on the Initial Setup Client webpage instead of the session parameters.

1.6.1.4 Step 4: Apply Changes

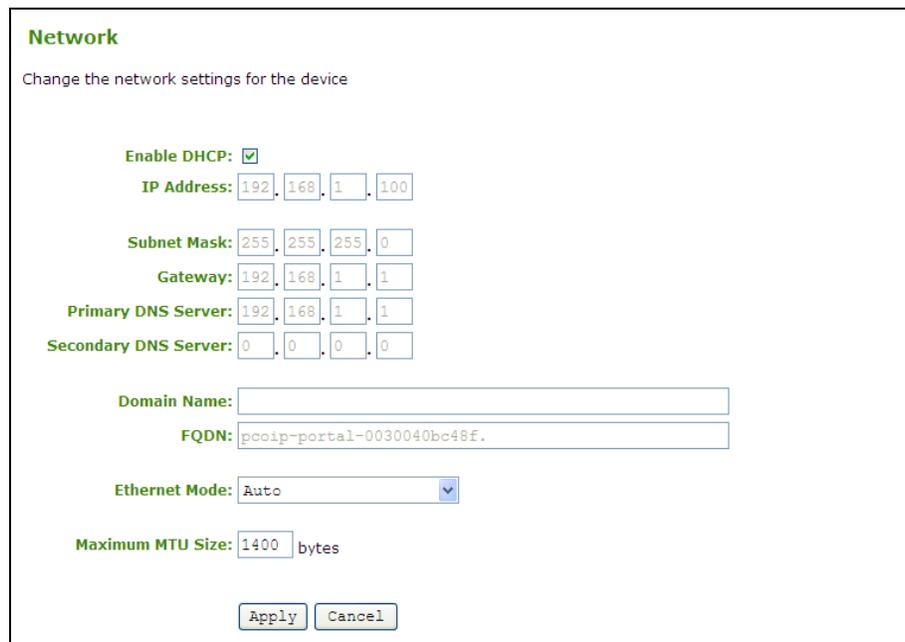
Step 4: Apply Changes allows the administrator to apply the parameter updates made in the steps above. Parameters will not be updated until *Apply* is selected.

1.6.2 Network

The *Network* webpage allows an administrator to set the client and host network parameters.

Note: The client Network parameters can also be configured using the OSD. See Section 2.3.1 Network.

Figure 1-8: Network Configuration Webpage



1.6.2.1 Enable DHCP

When *Enable DHCP* is enabled, the device will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address, and DNS servers. When *Enable DHCP* is disabled, these parameters must be set manually.

When *Enable DHCP* is enabled, the firmware requests domain name (option 15), host name (option 12) and Client FQDN (option 81).

1.6.2.2 IP Address

The *IP Address* is the device’s IP address. If DHCP is disabled, this field is required. If DHCP is enabled, this field is not editable. This field must be a valid IP address; if an invalid IP address is entered, the web interface will prompt the administrator to correct it.

1.6.2.3 Subnet Mask

The *Subnet Mask* is the device’s subnet mask. If DHCP is disabled, this field is required. If DHCP is enabled, this field is not editable. This field must be a valid subnet mask; if an invalid subnet mask is entered, the web interface will prompt the administrator to correct it.

Warning: It is possible to configure an illegal IP Address/Subnet Mask combination (e.g. invalid mask) that will leave the device unreachable. Care must be taken when setting the Subnet Mask.

1.6.2.4 Gateway

The *Gateway* is the device’s gateway IP address. If DHCP is disabled, this field is required. If DHCP is enabled, this field is not editable.

1.6.2.5 Primary DNS Server

The *Primary DNS Server* is 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 a FQDN instead of an IP address (see Section 1.6.4.2).

1.6.2.6 Secondary DNS Server

The *Secondary DNS Server* is 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 a FQDN instead of an IP address (see Section 1.6.4.2).

1.6.2.7 Domain Name

The *Domain Name* is the domain name used, e.g. 'domain.local'. This field is optional. This field specifies the domain that the host or client is on.

The *Domain Name* is obtained from the DHCP server when DHCP is enabled. If the *Domain Name* is used, it will also be appended to the FQDN as outlined below.

1.6.2.8 FQDN

The *FQDN* is 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* will be appended, e.g. `pcoip-host-<MAC>.domain.local`.

Note: To use the FQDN feature, a properly configured DNS server with DHCP option 81 must be available.

Note: *FQDN* field is read only on the *Network* webpage.

1.6.2.9 Ethernet Mode

The *Ethernet Mode* field configures the Ethernet mode of the host or client. The options are:

- Auto
- 10 Mbps Full-Duplex
- 100 Mbps Full-Duplex

When the administrator chooses *10 Mbps Full Duplex* or *100 Mbps Full-Duplex* and selects the *Apply* button, the following warning is displayed:

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 settings. Different settings may result in a loss of network connectivity. Are you sure you want to continue?

The administrator must select *OK* to change the parameter setting.

Note: Administrators should always set the *Ethernet Mode* to *Auto* and only use *10 Mbps Full-Duplex* or *100 Mbps Full-Duplex* when the other network equipment, e.g. switch, is also configured to operate at 10M Mbps Full-Duplex or 100M Mbps Full-Duplex. An improperly-set Ethernet Mode may result in the network operating at Half-Duplex. Half-Duplex is not supported by PCoIP protocol; the session will be severely degraded and eventually dropped.

1.6.2.10 Maximum MTU Size

The *Maximum MTU Size* option allows the administrator to configure the Maximum Transmission Unit (MTU) packet size. A smaller MTU may be required in situations such

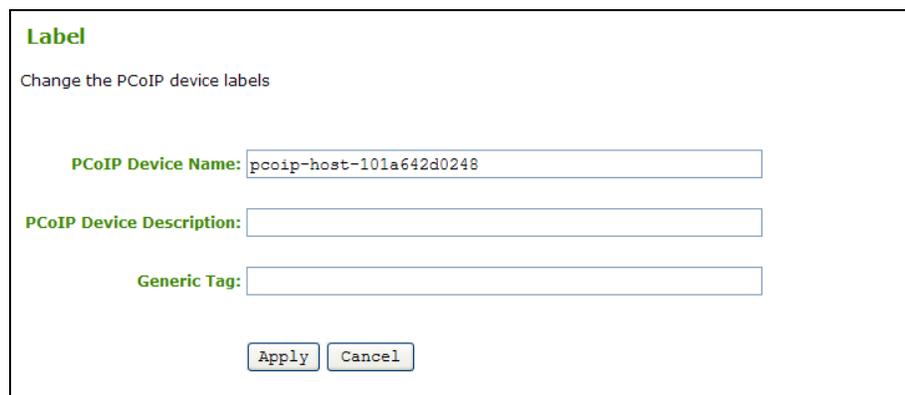
as VPN tunneling because PCoIP packets cannot be fragmented. The *Maximum MTU Size* should be set to a value smaller than the network path MTU for the end-to-end connection between the host and client. The *Maximum MTU Size* range is 500 to 1500 bytes.

1.6.3 Label

The *Label* webpage allows an administrator to add custom information for the host or client.

Note: The client *Label* parameters can also be configured using the OSD. See Section 2.3.2 *Label Tab*.

Figure 1-9: Label Configuration Webpage



Label
Change the PCoIP device labels

PCoIP Device Name:

PCoIP Device Description:

Generic Tag:

1.6.3.1 PCoIP Device Name

The *PCoIP Device Name* allows the administrator to give the host or client a logical name. The default is `pcoip-host-<MAC>` or `pcoip-portal-<MAC>` where `<MAC>` is the host or client's MAC address.

The *PCoIP Device Name* is the name the host or client will register with the DNS server if DHCP is enabled and the system is configured to support registering the hostname with the DNS server. Ensure the *PCoIP Device Name* is unique for each endpoint in the network.

1.6.3.2 PCoIP Device Description

The *PCoIP Device Description* allows the administrator to give the host or client a description or more information, e.g. location of endpoint, etc.

The *PCoIP Device Description* is not used by the Firmware and is provided strictly for administrator use.

1.6.3.3 Generic Tag

The *Generic Tag* allows the administrator to give the host or client generic tag information.

The *Generic Tag* is not used by the Firmware and is provided strictly for administrator use.

1.6.4 Connection Management

The *Connection Management* webpage allows an administrator to enable or disable connection management and to specify the IP address of the connection manager.

In a managed connection, an external Connection Manager Server communicates with and can remotely control and configure the device. Additionally, the connection manager can locate an appropriate peer for the device to connect to and initiate the connection. Connection management can greatly simplify the administration effort for a large, complex system.

Note: The client Connection Management parameters can also be configured using the OSD. See Section 2.3.3 Connection Management Tab.

Figure 1-10: Connection Management Configuration Webpage (IP Address)



The screenshot shows the 'Connection Management' configuration page. The title is 'Connection Management' in green. Below the title is the instruction 'Configure the device for a managed connection'. The page contains the following elements:

- 'Enable Connection Management:' with an unchecked checkbox.
- 'Identify Connection Manager by:' with two radio buttons: 'IP address' (selected) and 'FQDN'.
- 'Connection Manager IP Address:' with four input fields for IP address digits.
- 'Enable Event Log Notification:' with an unchecked checkbox.
- 'Enable Diagnostic Log:' with an unchecked checkbox.
- 'Apply' and 'Cancel' buttons at the bottom.

Figure 1-11: Connection Management Configuration Webpage (FQDN)



The screenshot shows the 'Connection Management' configuration page with 'FQDN' selected. The title is 'Connection Management' in green. Below the title is the instruction 'Configure the device for a managed connection'. The page contains the following elements:

- 'Enable Connection Management:' with a checked checkbox.
- 'Identify Connection Manager by:' with two radio buttons: 'IP address' and 'FQDN' (selected).
- 'Connection Manager DNS Name:' with a single text input field.
- 'Enable Event Log Notification:' with an unchecked checkbox.
- 'Enable Diagnostic Log:' with an unchecked checkbox.
- 'Apply' and 'Cancel' buttons at the bottom.

1.6.4.1 Enable Connection Management

If the *Enable Connection Management* option is enabled, the device can be configured and controlled by an external connection manager.

1.6.4.2 Identify Connection Manager By

The *Identify Connection Manager By* selector allows the administrator to choose whether the connection manager is identified by IP address or by Fully Qualified Domain Name (FQDN). If connection management is disabled, this field is not required and is not editable.

Table 1-6 shows the configuration parameters available when either method is chosen. If an invalid IP address or DNS name is entered, the web interface will prompt the administrator to correct it.

Table 1-6: Connection Manager Method

Method	Data Fields	Figure
IP address	Connection Manager IP Address	See Figure 1-10
FQDN	Connection Manager DNS name	See Figure 1-11

1.6.4.3 Enable Event Log Notification

The *Event Log Notification* field controls whether the host and client devices send the contents of their event logs to the connection management server

1.6.4.4 Enable Diagnostic Log

The *Enable Diagnostic Log* field controls whether connection management specific debug messages are written to the event log of the host and client devices.

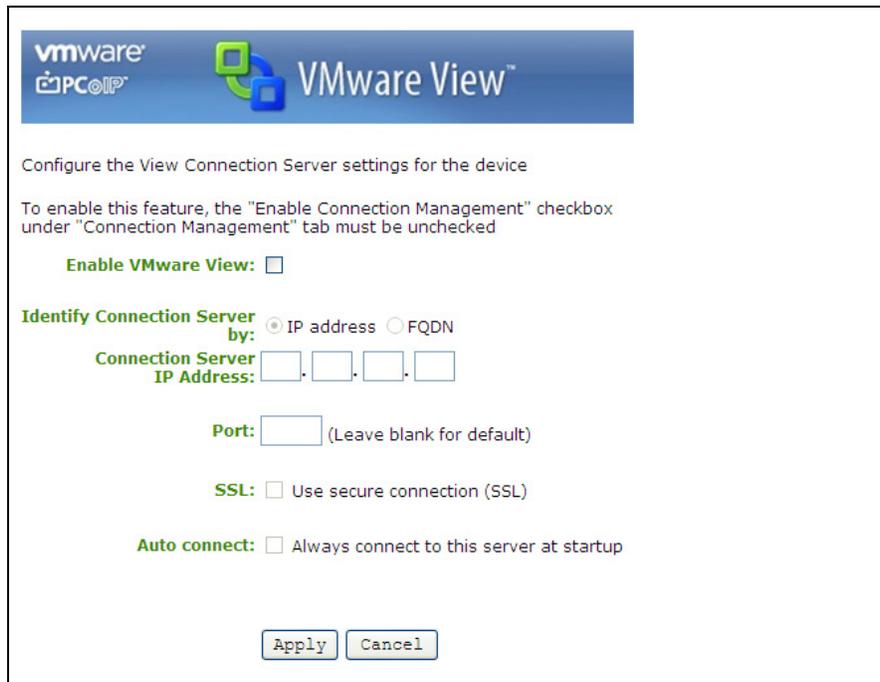
1.6.5 VMware View

The *VMware View* webpage allows configuration for use with a VMware View Connection Server.

Note: The VMware View webpage is only available on a client; on the host it is not available.

Note: The client VMware View parameters can also be configured using the OSD. See Section 2.3.11 VMware View Tab.

Figure 1-12: VMware View Configuration Webpage



1.6.5.1 Enable VMware View

When the *Enable VMware View* option is enabled, the client can be configured for use with a VMware View Connection Server.

Note: To enable the VMware View feature, the *Enable Connection Management* checkbox on the Connection Management webpage (see Section 1.6.4.1) must be unchecked.

1.6.5.2 Identify Connection Server by

The *Identify Connection Server By* selector allows the administrator to choose whether the connection manager is identified by IP address or by Fully Qualified Domain Name (FQDN). If VMware View is disabled, this field is not required and is not editable.

1.6.5.3 Port

The *Port* parameter allows the administrator to specify the port used to communicate to the VMware View Connection Server.

1.6.5.4 SSL

The *SSL* parameter allows the administrator to specify SSL to communicate with the VMware View Connection Server. The *SSL* parameter allows the administrator to specify whether or not the client communicates with the VMware View Connection Server over a secure connection using SSL.

1.6.5.5 Auto connect

The *Auto Connect* parameter allows the administrator to specify that the client automatically always connects with the VMware View Connection Server at startup.

1.6.6 Discovery

The *Discovery* configuration webpage allows the use of features that ease the discovery of hosts and clients in a PCoIP system.

Note: The client *Discovery* parameters can also be configured using the OSD. See Section 2.3.4 *Discovery*.

Figure 1-13: Discovery Configuration Webpage



Discovery
Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable Host Discovery (client only):

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

Apply Cancel

1.6.6.1 SLP Discovery

Enable SLP Discovery

When the *Enable SLP Discovery* option is enabled, the hosts and clients can be dynamically discovered by SLP management entities, without requiring prior knowledge of their locations in the network.

Using a discovery mechanism can dramatically reduce the configuration and maintenance effort for complex systems. This discovery mechanism is independent of DNS SRV discovery.

Note: SLP discovery requires routers configured to allow multicast, and therefore DNS-SRV Discovery is the recommended discovery mechanism.

Enable Host Discovery

The *Enable Host Discovery* feature allows the client to discover hosts that are not in a PCoIP session.

When enabled, the client is able to display up to 10 available hosts in the order that they were discovered. It is expected that the *Enable Host Discovery* feature will be used with small numbers of hosts.

Note: This option is only available on a client; on the host it is disabled and non-editable.

1.6.6.2 DNS SRV Discovery

Enable DNS SRV

When the *Enable DNS SRV* option is enabled, the hosts and clients can be dynamically discovered by a connection broker discovery method that uses DNS SRV Resource Records, without requiring prior knowledge of their locations in the network. When enabled, the host or client will attempt to download and use the DNS SRV record from the DNS server.

Using a discovery mechanism can dramatically reduce configuration and maintenance effort for complex systems. This discovery mechanism is independent of SLP Discovery.

Note: The *Enable DNS SRV* option configures the discovery for connection brokers, but does not effect the DNS SRV functionality for the PCoIP Management Console.

DNS SRV Discovery Delay

The *DNS SRV Discovery Delay* configures amount of delay time in seconds between DNS SRV Discovery attempts for connection brokers and the PCoIP Management Console. DNS SRV Discovery continues periodically until the device is successful in contacting a Connection Management Server.

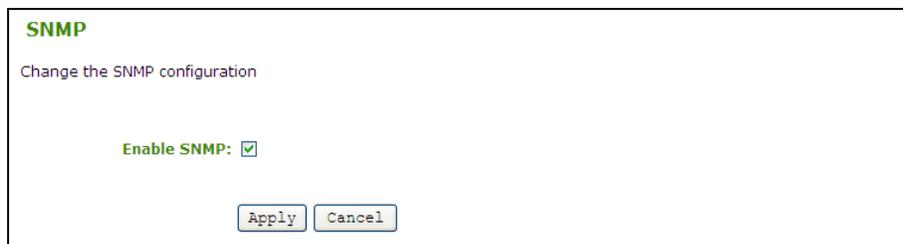
Note: Although the *Enable DNS SRV* option does not affect the DNS SRV functionality for the PCoIP Management Console, the *DNS SRV Discover Delay* is used for the PCoIP Management Console as well. If not installing DNS SRV records, it is recommended to set the delay to the maximum value, 9999, to minimize attempts by the host or client to contact the PCoIP Management Console.

1.6.7 SNMP

The *SNMP* webpage allows an administrator to enable or disable the host or client SNMP agent.

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

Figure 1-14: SNMP Configuration Webpage



1.6.7.1 Enable SNMP

If the *Enable SNMP* option is enabled, the host or client will enable the PCoIP SNMP agent. Disabling the SNMP agent ensures that the PCoIP SNMP MIB can not be accessed.

1.6.8 Session

The *Session* webpage allows an administrator to configure how the device connects to or accepts connections from peer devices.

Note: The client *Session* parameters can also be configured using the OSD. See Section 2.3.5 *Session*.

Figure 1-15: Session Configuration Webpage

Session

Configure the connection to a peer device

Accept Any Peer (host only):

Session Type (client only):

Identify Peer by: IP address FQDN

Peer IP Address: . . .

Peer MAC Address: - - - - -

Enable Auto-Reconnect (client only):

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

Figure 1-16: Session Configuration Webpage (RDP – client only)

Session

Configure the connection to a peer device

Accept Any Peer (host only):

Session Type (client only):

Identify Peer by: IP address FQDN

Peer IP Address: . . .

Peer MAC Address: - - - - -

Enable Auto-Reconnect (client only):

Enable AES-128-GCM:

Enable Salsa20-256-Round12:

1.6.8.1 Accept Any Peer

If the *Accept Any Peer* option is enabled, the host will accept connections from any client. If this option is disabled, the administrator must specify the peer MAC address.

Note: This option is only available on a host; on the client it is disabled and non-editable.

1.6.8.2 Session Type

The administrator can choose a PCoIP session or an RDP session.

For information on the RDP client, see Section 6 Appendix C: Client RDP Compatibility

Note: This option is only available on a client; on the host it is disabled and non-editable.

1.6.8.3 Identify Peer By

The *Identify Peer By* selector allows the administrator to choose whether the peer device is identified by IP and MAC address or by Fully Qualified Domain Name (FQDN). If Accept Any Peer is enabled, these fields are not required and are not editable.

Table 1-7 shows the peer identify parameters available when either method is chosen. If an invalid IP address or DNS name is entered, the web interface will prompt the administrator to correct it.

Table 1-7: Peer Identify Methods

Peer Identify Method	Data Fields	Comment
Peer IP/MAC	Peer IP Address	PCoIP client or RDP client
	Peer MAC Address	PCoIP client
Peer FQDN	Peer DNS Name	PCoIP client or RDP client
	Peer MAC Address	PCoIP client

1.6.8.4 Enable Auto-Reconnect

The *Enable Auto-Reconnect* option allows the client to automatically reconnect with the last connected host when a session is lost.

Note: This option is only available on a client; on the host it is disabled and non-editable.

1.6.8.5 Enable AES-128-GCM

The *Enable AES-128-GCM* option configures AES-128-GCM encryption for the host or client. AES-128-GCM is a encryption method implemented in the TERA1x00 processor that allows best performance between hardware endpoints.

Note: The enabled encryption must match on the host and client for a session to be established. If both modes are enabled, the firmware will select AES-128-GCM for the PCoIP session.

1.6.8.6 Enable SALSA20-256-Round12

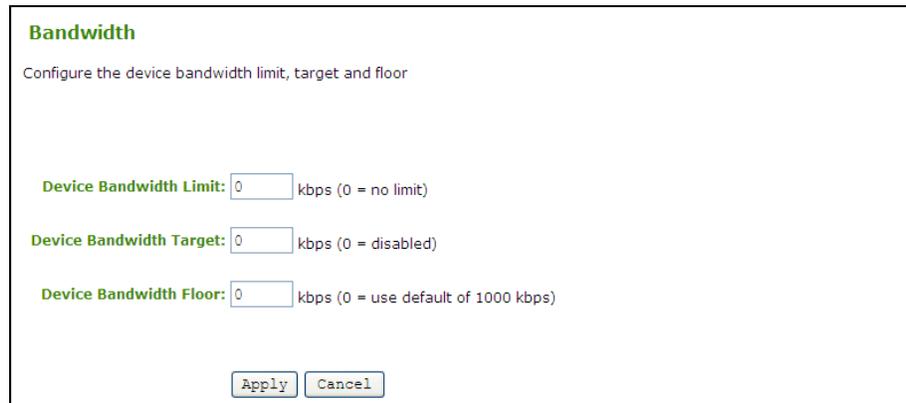
The *Enable SALSA20-256-Round12* option configures SALSA20-256-Round12 encryption for the host or client. SALSA20-256-Round12 is a lighter encryption method implemented in firmware that may offer improved performance when connecting to VMware View 4 when there is more than about 5 Mbps available on the network. (See TER0904005 Using PCoIP® Zero Clients with VMware® View 4 User Guide for more information.)

Note: The enabled encryption must match on the host and client for a session to be established. If both modes are enabled, the firmware will select AES-128-GCM for the PCoIP session.

1.6.9 Bandwidth

The *Bandwidth* webpage allows the device bandwidth to be controlled for PCoIP Sessions.

Figure 1-17: Bandwidth Configuration Webpage



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)

1.6.9.1 Device Bandwidth Limit

The *Device Bandwidth Limit* parameter defines the maximum bandwidth peak for the PCoIP system. The bandwidth setting on the host defines the bandwidth from the host to the client (e.g. graphics data), while the Bandwidth setting on the client side defines the bandwidth from the client to host (e.g. USB data). The usable range of the device bandwidth is 1 000 to 220 000 kbps.

The PCoIP processor will continue to use only the bandwidth required up to the *Device Bandwidth Limit* maximum. The PCoIP processor will dynamically adjust the bandwidth in response to network congestion.

Setting the *Device Bandwidth Limit* to 0 configures the PCoIP processor to adjust the bandwidth depending on network congestion. If there is no congestion, there will be no limit on bandwidth—i.e. the processor will use the maximum rate available.

We recommended setting the *Device Bandwidth Limit* to the limit of the network connected to the client and host.

See Section 4.3 Bandwidth and Image Configuration Example for an example on setting the *Device Bandwidth Limit*.

Note: The *Device Bandwidth Limit* is applied immediately after selecting *Apply*.

1.6.9.2 Device Bandwidth Target

The *Device Bandwidth Target* parameter defines the soft 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. Administrators should have a good understanding of the network topology before setting this to a non-zero value.

Note: The *Device Bandwidth Target* is applied immediately after selecting *Apply*.

1.6.9.3 Device Bandwidth Floor

The *Device Bandwidth Floor* parameter allows the administrator to configure the bandwidth floor the firmware will use when congestion is present and when bandwidth is required. This allows administrators to optimize performance for a network with understood congestion or packet loss. If the bandwidth is not required, the bandwidth used will drop below the floor.

A setting of 0 allows the firmware to reduce bandwidth to 1 000 kbps for these network impairments. Administrators should have a good understanding of the network topology before setting this to a non-zero value.

Note: The firmware implements a Slow Start Algorithm that increases the bandwidth used until the bandwidth required is reached, network congestion is detected or the *Device Bandwidth Limit* is reached. The Slow Start Algorithm begins at the lesser of the *Device Bandwidth Limit* and 8 000 kbps, and the algorithm increases the bandwidth used within seconds. The Slow Start Algorithm allows a graceful session start up for low bandwidth scenarios, e.g. WAN. After initiating a PCoIP session, users may temporarily notice low bandwidth video artifacts as the algorithm ramps up bandwidth use.

Note: The *Device Bandwidth Floor* is applied immediately after selecting *Apply*.

1.6.10 RDP

The *RDP* webpage allows the administrator to configure device settings specific to the Remote Desktop Protocol (RDP).

For information on the RDP client, see Section 6 Appendix C: Client RDP Compatibility.

Note: This RDP webpage is only available on a client; on the host it is not available.

Note: The RDP parameters can also be configured using the OSD. See Section 2.3.6 RDP.

Figure 1-18: RDP Configuration Webpage



RDP
Change the RDP-specific configuration (client only)

Resolution: Native Resolution ▾
Bitdepth: 16 ▾ bpp
Terminal Server Port: 3389
Audio Mode: Play on client ▾
Enable Wallpaper:
Enable Themes:

Apply Cancel

1.6.10.1 Resolution

The *Resolution* is the RDP screen resolution setting. Possible values are:

- Native Resolution

- 800x600
- 1024x768
- 1280x768
- 1280x1024
- 1440x900
- 1600x1200
- 1680x1050
- 1920x1080
- 1920x1200

1.6.10.2 Bit Depth

The *Bit Depth* is the RDP session colour bit depth. Possible values are:

- 8 bpp (bits per pixel)
- 16 bpp
- 24 bpp

1.6.10.3 Terminal Server Port

The *Terminal Server Port* sets the port number that the RDP client connects to.

1.6.10.4 Audio Mode

The *Audio Mode* field configures where the audio playback occurs for the RDP session. Possible options are:

- Do not play
- Play on client
- Play on host

1.6.10.5 Enable Wallpaper

The *Enable Wallpaper* field enables the use of wallpaper with the RDP session.

1.6.10.6 Enable Themes

The *Enable Themes* field enables the use of desktop themes with the RDP session.

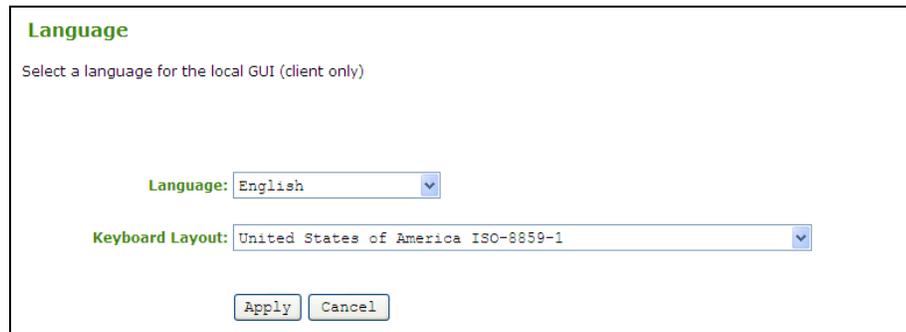
1.6.11 Language

The *Language* webpage allows the administrator to change the user interface language. Note that this will affect the local OSD GUI.

Note: This Language webpage is only available on a client; on the host it is unavailable.

Note: The client Language parameters can also be configured using the OSD. See Section 2.3.7 Language.

Figure 1-19: Language Configuration Webpage



1.6.11.1 Language

The *Language* field allows the administrator to configure the language of the OSD.

Refer to Section 5 Appendix B: Client Language and Keyboard Support for supported languages.

1.6.11.2 Keyboard Layout

The *Keyboard Layout* field allows the administrator to change the keyboard layout.

Refer to Table 5-2 in Section 5 Appendix B: Client Language and Keyboard Support for supported keyboard layouts.

1.6.12 OSD

The OSD webpage allows the administrator to modify the On Screen Display (OSD) parameters.

Note: This OSD webpage is only available on a client; on the host it is unavailable.

Note: The OSD parameters can also be configured using the OSD. See Section 2.3.8 OSD.

Figure 1-20: OSD Configuration Webpage



1.6.12.1 Screen-Saver Timeout

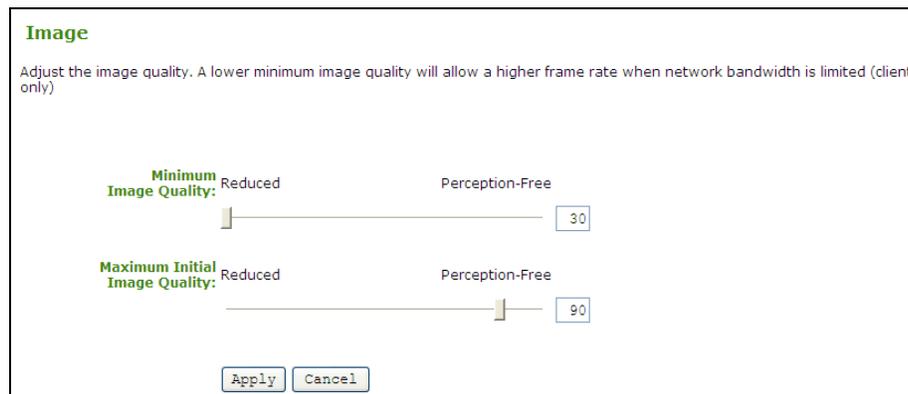
The *Screen-Saver Timeout* field allows the administrator to configure the screen-saver timeout before the client will put the attached displays into low power mode. The timeout can be configured in seconds, up to 9999 seconds. A setting of 0 seconds disables the screen-saver.

1.6.13 Image

The *Image* webpage allows the administrator to adjust the image (graphics) quality of the PCoIP session.

Note: This Image webpage is only available on a client; on the host it is unavailable.

Figure 1-21: Image Configuration Webpage



1.6.13.1 Minimum Image Quality

The *Minimum Image Quality* slider allows the administrator to make compromises 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 in other cases higher-quality images at a lower frame rate may be preferred.

In environments where the network bandwidth is constrained, moving the slider towards *Reduced* allows higher frame rates; moving the slider towards *Perception-Free* allows higher image quality. When network bandwidth is not constrained, the PCoIP system will maintain perception-free quality regardless of the *Minimum Image Quality* setting.

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

Note: The *Minimum Image Quality* can also be configured using the OSD. See Section 2.6.3 Image.

See Section 4.3 Bandwidth and Image Configuration Example for an example on setting the *Minimum Image Quality*.

1.6.13.2 Maximum Initial Image Quality

The *Maximum Initial Image Quality* slider can be used to reduce network bandwidth peaks caused by screen content changes. This setting limits the initial quality on the first video frame of a screen change. Unchanged regions of the image will build to a lossless state regardless of this setting.

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

Note: The *Maximum Initial Image Quality* does not have a corresponding parameter on the OSD, as it is intended as an administrator-only parameter.

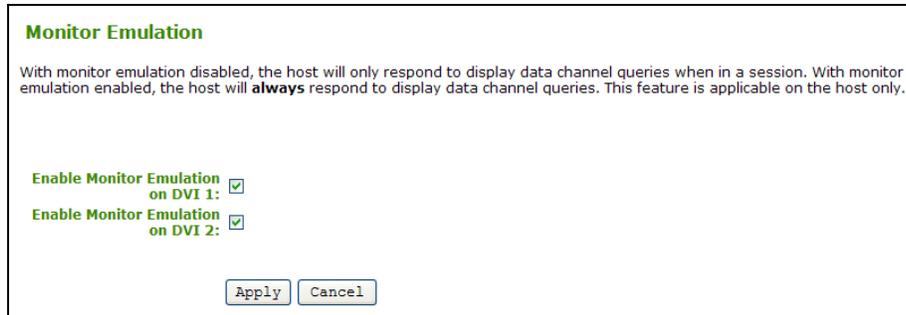
1.6.14 Monitor Emulation

The Monitor Emulation webpage allows the monitor emulation feature to be enabled and disabled.

This option is only available on a host; on the client it is disabled and non-editable.

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

Figure 1-22: Monitor Emulation Configuration Webpage



Monitor Emulation

With monitor emulation disabled, the host will only respond to display data channel queries when in a session. With monitor emulation enabled, the host will **always** respond to display data channel queries. This feature is applicable on the host only.

Enable Monitor Emulation on DVI 1:

Enable Monitor Emulation on DVI 2:

Apply Cancel

1.6.14.1 Enable Monitor Emulation

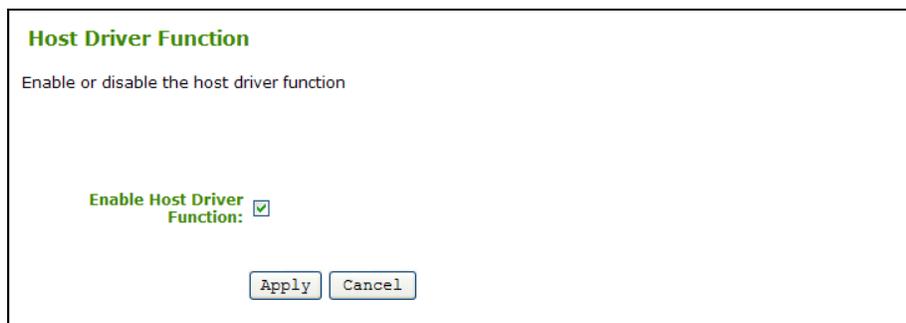
When Enable Monitor Emulation is disabled, the host will only respond to Display Data Channel (DDC) when in a PCoIP session. When Enable Monitor Emulation is enabled, the host will use emulated data for DDC queries regardless if in a PCoIP session or not. Independent Enable Monitor Emulation fields are available for both monitor ports, DVI1 and DVI2.

1.6.15 Host Driver Function

The *Host Driver Function* webpage allows the host driver function feature to be enabled and disabled.

Note: The *Host Driver Function* webpage is only available on a host; on the client it is unavailable.

Figure 1-23: Host Driver Function Configuration Webpage



Host Driver Function

Enable or disable the host driver function

Enable Host Driver Function:

Apply Cancel

1.6.15.1 Enable Host Driver Function

The *Enable Host Driver Function* check box enables a PCoIP Host Driver function to allow enhanced features including:

- Host PC lock when session is terminated
- Local cursor and keyboard
- Specify network interface for Wake on LAN function
- View host and client network parameters
- View session statistics

For more information on enabling, installing and using the PCoIP Host Software features, refer to the PCoIP Host Software User Guide.

1.6.16 Time

The *Time* webpage configures the Network Time Protocol (NTP) settings to allow the event logs (see Section 1.8.1 Event Log) of the host and client to be time-stamped based on NTP time.

Figure 1-24: Time Configuration Webpage



1.6.16.1 Current Time

The *Current time* field displays the time based on the NTP.

1.6.16.2 Enable NTP

The *Enable NTP* field allows the administrator to enable and disable the NTP feature.

1.6.16.3 Identify NTP Host By

The *Identify NTP Host by* selector allows the administrator to choose whether the NTP Host is identified by IP address or by Fully Qualified Domain Name (FQDN). If NTP is disabled, this field is not required and is not editable.

Table 1-8 shows the configuration parameters available when either method is chosen. If an invalid IP address or DNS name is entered, the web interface will prompt the administrator to correct it.

Table 1-8: NTP Host Method

Method	Data Fields
IP address	NTP Host IP Address
FQDN	NTP Host DNS name

1.6.16.4 NTP Host Port

The *NTP Host Port* field configures the NTP port number.

1.6.16.5 NTP Query Interval

The *NTP Query Interval* fields allow the administrator to configure the query interval. The first field denotes the interval period and the second field denotes the time unit in *Minute(s)*, *Hour(s)*, *Day(s)* and *Week(s)*.

1.6.16.6 Time Zone

The *Time Zone* field allows configuration for the local time zone.

1.6.16.7 Enable Daylight Savings Time

The *Enable Daylight Savings Time* field allows the administrator to enable and disable automatic adjustment for daylight savings time.

1.6.17 Password

The *Password* webpage allows the administrator to update the local administrative password for the device. Note that this will affect the web interface and the local GUI.

The password can be a maximum of 20 characters.

Note: Care must be taken when updating the client Password as the client may become unusable if the password is lost. (See Section 2.7 Password Window for information on resetting the client’s password.)

Note: The client Password can also be updated using the OSD. See Section 2.7 Password.

Note: Some PCoIP devices have password protection disabled by default and this *Password* webpage is not available on these devices. Password protection can be enabled through PCoIP Management Console for these devices.

Figure 1-25: Password Configuration Webpage



1.6.17.1 Old Password

The *Old Password* field must match the current administrative password for the update to take place.

1.6.17.2 New Password

The *New Password* field will be the new administrative password for both the web interface and the local OSD GUI.

Note: The host and client passwords are changed individually.

1.6.17.3 Confirm New Password

The *Confirm New Password* field must match the *New Password* field for the change to take place.

1.6.18 Reset Parameters

The *Reset* webpage allows the administrator to reset all the configurable parameters stored in flash.

Note: The client *Reset Parameters* can also be initiated using the OSD. See Section 2.3.9 *Reset*.

Figure 1-26: Reset Parameters Webpage



1.6.18.1 Reset Parameters

The *Reset Parameters* button resets all configuration and permissions to factory default values. When this button is selected, the web interface will prompt the administrator for confirmation to prevent accidental resets.

1.7 Permissions Menu

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

- USB
- Audio
- Power (client only)

Figure 1-27: Permissions Menu Navigation



1.7.1 USB

The *USB* webpage allows the administrator to specify authorized and unauthorized USB devices. The *USB* webpage is divided into two sections: *Authorized Devices* (“white list”) and *Unauthorized Devices* (“black list”). Entries can define an authorized or unauthorized device (or group of devices) based on ID or Class. Using wildcards (or specifying “any”) can reduce the number of entries needed to define all authorized or unauthorized devices. See Section 4.4 USB Permissions Example in Appendix A: Usage Examples for more details on USB configuration.

The *USB* webpage is available on the host and client, but the host USB permissions have higher priority and will update the client USB permissions:

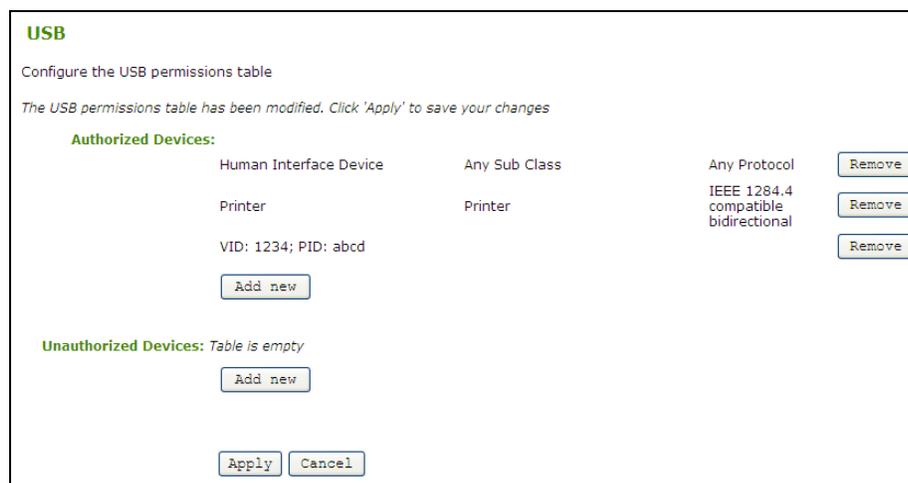
- If the host has any permissions programmed (authorized and/or unauthorized), then the permissions will be sent to the client. If the client has any unauthorized devices, they will be added to the host’s unauthorized devices and the consolidated list will be used.
- If the host does not have any permissions programmed, the clients permissions will be used.

The factory defaults have no USB permissions configured on the host. The factory defaults for the client USB permissions are *any, any, any*, i.e. all USB devices authorized. Depending on the host implementation, e.g. hardware PCoIP host or software PCoIP host, the administrator can configure the USB permissions as required on the client and/or host.

Warning: The host USB permissions are only updated on the start of a PCoIP session.

Note: It is strongly recommended to set the USB permissions on the host only.

Figure 1-28: USB Permissions Webpage



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	Remove
Printer	Printer	IEEE 1284.4 compatible bidirectional	Remove
VID: 1234; PID: abcd			Remove

Add new

Unauthorized Devices: Table is empty

Add new

Apply Cancel

1.7.1.1 Authorized Devices

The *Authorized Devices* section allows the administrator to specify the authorized USB devices for the host and client. Two buttons allow customization of this “white list.” The *Add new* button allows a new device or device group to be added to the list and the *Remove* button allows a device or device group to be removed from the list.

Selecting the *Add new* button allows USB authorization by *ID* or *Class*. If *ID* is selected, then this entry authorizes a USB device by *Vendor ID* and *Product ID*. If *Class* is selected, then this entry authorizes a USB device by *Device Class*, *Sub Class* and *Protocol*.

Note: USB authorizations are applied in the following priority order:

1. Unauthorized Vendor ID/Product ID (highest priority)
2. Authorized Vendor ID/Product ID
3. Unauthorized Device Class/Sub Class/Protocol
4. Authorized Device Class/Sub Class/Protocol (lowest priority)

Table 1-9 summarizes the USB authorization entry type and the associated data fields.

Table 1-9: USB Device Authorization 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 class	Drop-down menu provides human-readable translations of the known device classes
	Sub Class	0-FF; asterisk (*) indicates any device sub class	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

1.7.1.2 Unauthorized Devices

The *Unauthorized Devices* section allows the administrator to specify the unauthorized USB devices for the host or client. Two buttons allow customization of this “black list.” The *Add new* button allows a new device or device group to be added to the list and the *Remove* button allows a device or device group to be removed from the list.

Selecting the *Add new* button allows USB unauthorization by *Class* or *ID*. If *ID* is selected, then this entry unauthorizes a USB device by *Vendor ID* and *Product ID*. If *Class* is selected, then this entry unauthorizes a USB device by *Device Class*, *Sub Class* and *Protocol*.

Note: USB authorizations are applied in the following priority order:

1. Unauthorized Vendor ID/Product ID (highest priority)
2. Authorized Vendor ID/Product ID
3. Unauthorized Device Class/Sub Class/Protocol
4. Authorized Device Class/Sub Class/Protocol (lowest priority)

Table 1-9 summarizes the USB unauthorization entry types and the associated data fields.

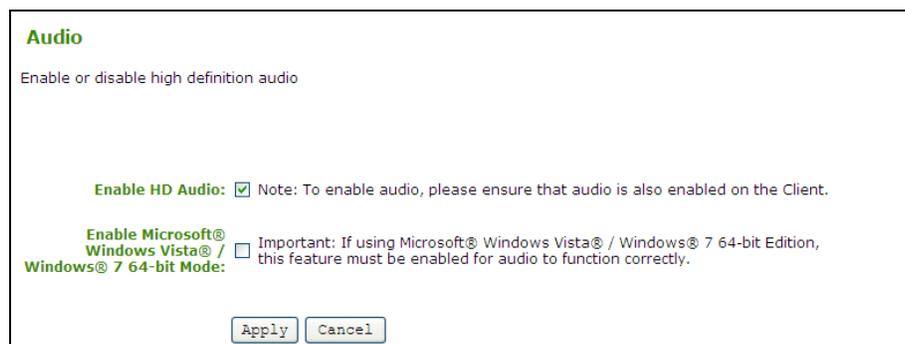
Table 1-10: USB Device Unauthorization Entry Types

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

1.7.2 Audio

The *Audio* webpage allows the administrator to configure the audio permissions of the device.

Figure 1-29: Audio Permissions Webpage



1.7.2.1 Enable HD Audio

The *Enable HD Audio* option enables and disables audio for the host and client. For audio to function, it must be enabled on both the host and client.

If the *Enable HD Audio* option is disabled on the host, the audio hardware will not be available for the OS to enumerate.

1.7.2.2 Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode

The *Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode* option enables the 64-bit work-around for Vista 64-bit or Windows 7 64-bit to avoid memory corruption when audio is enabled on host systems that are running 64-bit operating systems and that have more than 4 GB of RAM.

Note: This option is only available on a host.

Note: This mode is not to be used with Windows XP64 or 32-bit operating systems.

Note: Enabling the 64-bit mode is not required for Linux 64-bit operating systems, as Linux kernels should be compiled with latest PCoIP audio codec support.

1.7.3 Power

The *Power* webpage allows the administrator to configure the power-off permissions of the client.

Figure 1-30: Power Permissions Webpage



1.7.3.1 Client Power Button

The *Client Power Button* pull-down menu allows the client power button functionality to be configured. The options for the *Client Power Button* are:

- Power-off not permitted
- Soft Power-off only
- Hard Power-off only
- Soft and Hard Power-off

Note: The *Power* webpage is only available on a client; on the host it is unavailable.

1.8 Diagnostics Menu

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

- Event Log
- Session Control
- Session Statistics
- Host CPU (host only)
- Audio (client only)
- Display (client only)
- PCoIP Processor

Figure 1-31: Diagnostics Menu Navigation

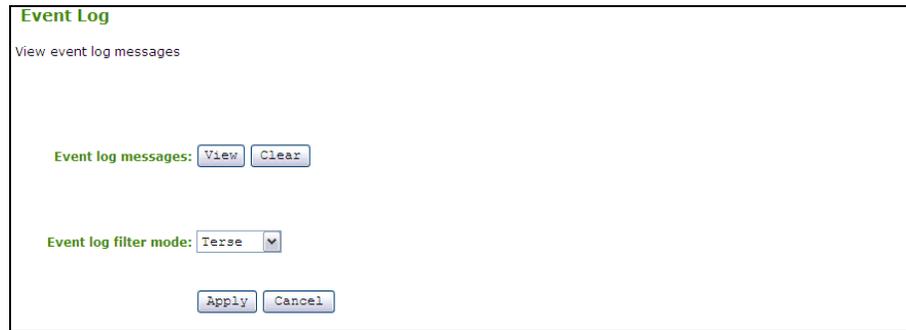


1.8.1 Event Log

The *Event Log* webpage allows the administrator to view and clear event log messages from the host or client.

Note: The client Event Log can also be viewed using the OSD. See Section 2.4.1 Event Log.

Figure 1-32: Event Log Webpage



1.8.1.1 Event log message

The *Event log messages* field allows the administrator to view and clear the message.

View

Selecting the *View* button opens a new browser window with the entire event log messages (with timestamp information) stored on the device.

Note: The F5 key can be used to refresh the browser window log information.

Clear

Selecting the *Clear* button deletes all of the stored event log messages.

1.8.1.2 Event log filter mode

The *Event log filter mode* pull-down menu allows the event log to be filtered. The options are:

- Verbose
- Terse

1.8.2 Session Control

The *Session Control* webpage allows control of the device session.

Figure 1-33: Session Control Webpage



1.8.2.1 Connection State

The *Connection State* field reports the current state of the session. Values are:

- Disconnected
- Connection Pending
- Connected

Below the *Connection State* field there are two buttons, *Connect* and *Disconnect*.

Connect

If the *Connection State* is *Disconnected*, selecting this button causes the client to initiate a PColP session with its peer device. If the *Connection State* is *Connection Pending* or *Connected*, this button is disabled.

Note: This option is only available on a client; on the host it is disabled.

Disconnect

If the *Connection State* is *Connected* or *Connection Pending*, selecting this button causes the device to end the PColP session. If the *Connection State* is *Disconnected*, this button is disabled.

1.8.2.2 Peer IP/MAC Address

Peer IP Address

The *Peer IP Address* reports the IP address of the peer device. When not in session, the field is blank.

Peer MAC Address

The *Peer MAC Address* displays the MAC address of the peer currently in session. When not in session, the field is blank.

1.8.3 Session Statistics

The *Session Statistics* webpage allows the administrator to view PColP protocol specific statistics.

Note: A subset of Session Statistics can also be viewed using the OSD. See Section 2.4.2 Session Statistics.

Figure 1-34: Session Statistics Webpage



1.8.3.1 Connection State

The *Connection State* field reports the current state of the PCoIP session. *Connection State* values are:

- Asleep
- Cancelling
- Connected
- Connection Pending
- Disconnected
- Waking

1.8.3.2 PCoIP Packets Statistics

PCoIP Packets Sent

PCoIP Packets Sent reports the total number of PCoIP packets sent in the current session.

PCoIP Packets Received

PCoIP Packets Received reports the total number of PCoIP packets received in the current session.

PCoIP Packets Lost

PCoIP Packets Lost reports the total number of PCoIP packets lost in the current session.

1.8.3.3 Bytes Statistics

Bytes Sent

Bytes Sent reports the total number of bytes sent in the current session.

Bytes Received

Bytes Received reports the total number of bytes received in the current session.

1.8.3.4 Round Trip Latency

The *Round Trip Latency* field reports the minimum, average and maximum round-trip PCoIP system (e.g. host to client, and back to host) and network latency in milliseconds (+/- 1 ms).

1.8.3.5 Bandwidth Statistics

Active Bandwidth Limit

Active Bandwidth Limit displays the maximum amount of network traffic the Tera1x00 processor may currently generate. The value is derived from the configured bandwidth settings (see Section 1.6.9 Bandwidth) and the current network congestion levels.

Transmit Bandwidth

Transmit Bandwidth reports the minimum, average and maximum traffic transmitted by the Tera1x00 processor.

Receive Bandwidth

Receive Bandwidth reports the minimum, average and maximum traffic received by the Tera1x00 processor.

1.8.3.6 Display Frame Rate

Display 1 Frame Rate

Display 1 Frame Rate reports the frame rate of Display 1. It is reported in frames per second (fps).

Display 2 Frame Rate

Display 2 Frame Rate reports the frame rate of Display 2. It is reported in frames per second (fps).

1.8.3.7 Reset Statistics

The *Reset Statistics* button resets the statistic information reported on the *Session Statistics* webpage.

Note: The *Reset Statistics* button also resets the statistics reported in the *Home* webpage.

1.8.4 Host CPU

The *Host CPU* webpage allows the administrator to view and modify the host information and state.

Note: The *Host CPU* webpage is only available on a host; on the client it is unavailable.

Figure 1-35: Host CPU Webpage



1.8.4.1 Host Identity

The *Host Identity* field displays the host computer identity string (if data is available).

1.8.4.2 Current Power State

The *Current Power State* field displays the current host power state.

1.8.4.3 Change Power State

The *Change Power State* pull-down menu allows the administrator to change the host power state. The options are:

- S5 (Soft Off)
- S5 (Hard Off)

Note: This requires compatible host hardware architecture.

1.8.4.4 Reset Host CPU

The *Reset Host CPU* button allows reset of the host CPU.

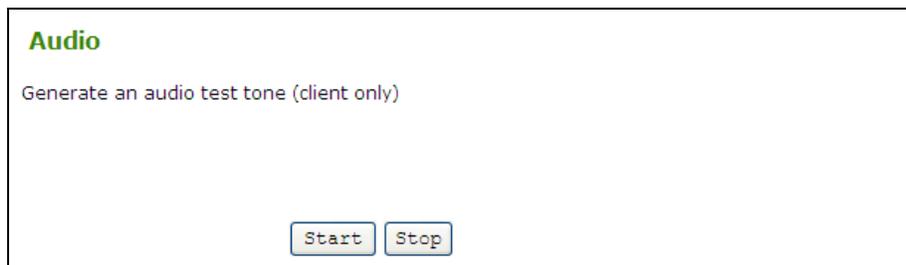
Note: This requires the host hardware to support remote resetting.

1.8.5 Audio

The *Audio* webpage allows the administrator to generate an audio test tone from the client.

Note: The *Audio* webpage functionality is only available on a client when not in a PCoIP session; on the host it is unavailable.

Figure 1-36: Audio Diagnostics Webpage



1.8.5.1 Generate an audio test tone (client only)

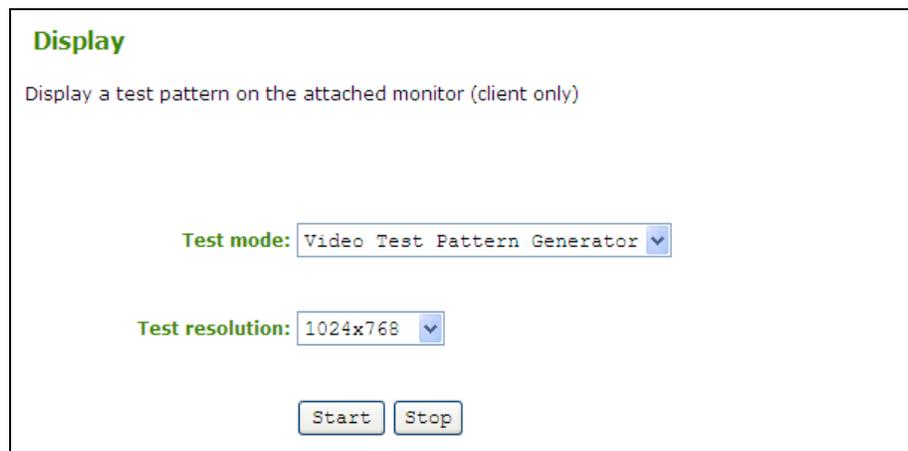
There are two buttons available: The *Start* button starts the test tone and the *Stop* button stops the test tone.

1.8.6 Display

The *Display* webpage allows the administrator to display a test pattern on the client displays.

Note: The *Display* webpage is only available on a client when not in a PCoIP session; on the host it is unavailable.

Figure 1-37: Display Webpage



The screenshot shows a web page titled "Display" with the subtitle "Display a test pattern on the attached monitor (client only)". Below the subtitle, there are two dropdown menus: "Test mode:" set to "Video Test Pattern Generator" and "Test resolution:" set to "1024x768". At the bottom of the form are two buttons labeled "Start" and "Stop".

1.8.6.1 Test mode

The *Test Mode* pull-down menu allows the administrator to enable a test pattern on the attached monitor(s). The test pattern options are

- Video Test Pattern Generator
- Pseudo Random Bitstream

1.8.6.2 Test resolution

The *Test resolution* pull-down menu sets the test pattern resolution. The options are:

- 1024x768
- 1280x1024
- 1600x1200
- 1920x1200

1.8.6.3 Start/Stop

The *Start* button starts the test pattern and the *Stop* button stops the test pattern.

1.8.7 PCoIP Processor

The *Reset PCoIP Processor Reset* button allows the administrator to reset the device processor.

Figure 1-38: PCoIP Processor Webpage



1.8.7.1 Current Time

The *Current Time* field displays the current time. This feature requires that the NTP be enabled and configured as described in Section 1.6.16 Time.

1.8.7.2 Time Since Boot

The *Time Since Boot* field allows a user to view the uptime of the PCoIP processor since last boot.

Note: The client uptime can also be viewed using the OSD. See Section 2.4.3 PCoIP Processor.

1.8.7.3 Reset PCoIP Processor

The *Reset PCoIP Processor* button allows the administrator to reset the host or client.

1.9 Info Menu

The *Info* menu contains links to pages that show information about the device. The webpages in the *Info* menu are:

- Version
- Attached Devices

Figure 1-39: Info Menu Navigation

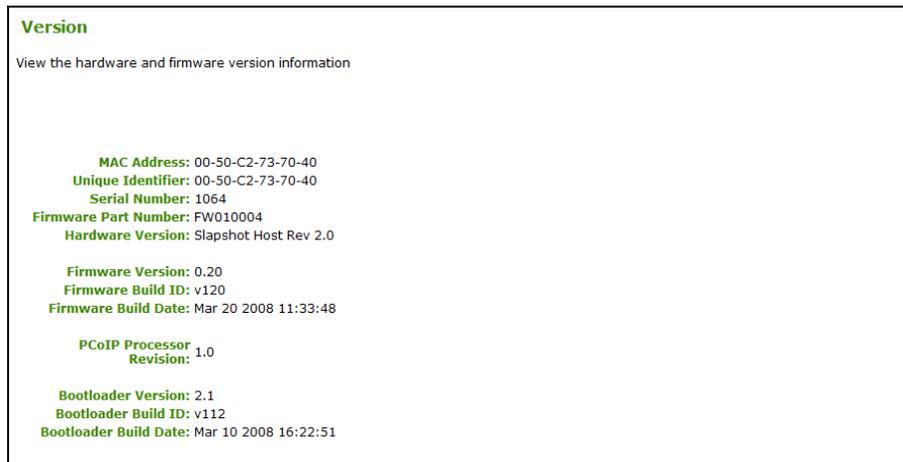


1.9.1 Version

The *Version* webpage allows the administrator to view hardware and firmware version information.

Note: The client Version information can also be viewed using the OSD. See Section 2.5 Information.

Figure 1-40: Version Webpage



1.9.1.1 VPD Information

Vital Product Data (VPD) is information provisioned by the factory to uniquely identify each host or client.

Note: The VPD information can also be viewed using the OSD. See Section 2.5.1.1 VPD Information.

Table 1-11: VPD Information

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

1.9.1.2 Firmware Information

The firmware information reflects the current firmware details.

Note: The Firmware information can also be viewed using the OSD. See Section 2.5.1.2 Firmware Information.

Table 1-12: Firmware Information

Firmware Version	Version of the current firmware
Firmware Build ID	Revision code of the current firmware
Firmware Build Date	Build date of the current firmware

1.9.1.3 PCoIP Processor Revision

The *PCoIP Processor Revision* code reports the silicon revision of the PCoIP processor. Revision B of the silicon is denoted by 1.0.

Note: The PCoIP Processor Revision information can also be viewed using the OSD. See Section 2.5.1.3 PCoIP Processor Revision.

1.9.1.4 Bootloader Information

The Bootloader information reflects the current firmware bootloader details.

Table 1-13: VPD Information

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

1.9.2 Attached Devices

The *Attached Devices* webpage reports the type and status of the Monitor and USB hardware currently attached to the client.

Figure 1-41: Attached Devices Webpage

The screenshot shows a webpage titled "Attached Devices" with the subtitle "View presently connected monitors and USB devices". It contains two tables:

Monitors:						Status
Name	Serial	VID	PID	Date		
SyncMaster	HCGPB03905	SAM	2B6	47-2007		Connected
VX922	PXU063334384	VSC	AD1C	33-2006		Connected

USB Devices:							Status
Name	Serial	VID	PID	Device Class	Sub Class	Protocol	
USB Multimedia	-	046D	C313	00	00	00	Connected
Keyboard	-	046D	C018	00	00	00	Connected
USB Optical Mouse	-	0000	0000	00	00	00	Not Connected
-	-	0000	0000	00	00	00	Not Connected
iPod	000A270015C400105AC	1209	08	06	06	50	Failed Authorization

1.9.2.1 Monitors

The *Monitors* section reports the *Name*, *Serial Number*, *Vendor Identification (VID)*, *Product Identification (PID)*, *Date*, and *Status* of the monitor attached to each port. The first line provides information for monitor 1 and the second line provides information for monitor 2.

Note: This option is available on a client and is available on the host when in a PCoIP session.

1.9.2.2 USB Devices

The *USB Devices* section reports the *Name*, *Serial Number*, *Vendor Identification (VID)*, *Product Identification (PID)*, *Device Class*, *Sub Class*, *Protocol*, and *Status* of the USB device attached to each port. The first line provides information for the first USB port, the second line provides information for the second port, etc.

Table 1-14 summarizes the possible *Status* descriptors for *USB Devices*.

Table 1-14: USB Device Status

Status	Description
Not Connected	No device connected
Standalone	Device detected outside of a PCoIP session

Not Initialized	Device detected in a PCoIP session, but host controller has not initialized the device
Failed Authorized	Device detected in a PCoIP session, but not authorized (see Section 1.7.1)
Locally Connected	Device detected and authorized, but locally terminated in a PCoIP session (e.g. local cursor)
Connected	Device detected and authorized in a PCoIP session

Note: The attached USB devices information is only available on a client; on the host it is not available.

1.10 Upload Menu

The *Upload* menu contains links to pages that can be used to upload files to the device. The webpages in the *Upload* menu are:

- Firmware
- OSD Logo (client only)

Figure 1-42: Upload Menu Navigation



1.10.1 Firmware

The *Firmware* webpage allows the administrator to upload a new firmware build to the host or client.

Figure 1-43: Firmware Upload Webpage



1.10.1.1 Firmware build filename

The *Firmware build filename* field specifies the filename of the firmware image to be uploaded. The administrator can browse to the file via the *Browse* button. The file must be accessible to the web browser (i.e. on a local or accessible network drive). The firmware image must be an “.all” file.

1.10.1.2 Upload

Selecting the *Upload* button will cause the specified file to be transferred to the device. The web interface will prompt the administrator for confirmation to avoid accidental uploads.

Note: Ensure that both the host and client have the same firmware release.

Example Firmware Upload Process:

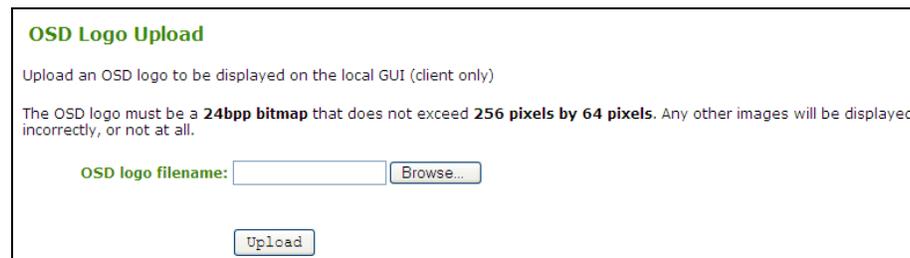
1. Ensure host PC or Workstation is in a idle state (all applications must be closed).
2. Log into the host admin interface (using password if enabled)
3. Select the *Firmware Upload* webpage *Browse* button to browse to the firmware “.all” file, e.g. *tera1x00_rel1-9_v175.all*
4. Select the File Upload window *Open* button
5. Select the webpage *Upload* button
6. Select the webpage *OK* button on the warning window that reads, “Are you sure? This will upload a new firmware image. This operation may take a few minutes.”
7. Wait for the firmware upload to complete. The following message appears when complete: “Success Flash successfully programmed! You must reset the device for the changes to take effect.”
8. Select the *Reset* button.
9. Select the *OK* button on the warning window that reads, "The PCoIP processor will reset on the next host system restart; your changes will take effect then. Are you sure you want to proceed?"
- 10.Repeat steps 2 through 7 on the client, but do not restart the client.
- 11.Restart the Host PC or Workstation
- 12.Reset the client
- 13.Start PCoIP Session

1.10.2 OSD Logo

The *OSD Logo* webpage allows an image to be uploaded to the device. This image is displayed on the connect window of the local GUI On Screen Display (OSD) logo.

Note: This option is only available on a client.

Figure 1-44: OSD Logo Upload Webpage



1.10.2.1 OSD logo filename

The *OSD logo filename* field specifies the filename of the logo image to be uploaded. The administrator can browse to the file via the *Browse* button. The file must be accessible to the web browser (i.e. 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, 64 pixels in height. If the file extension is incorrect, the web interface will display an error message.

1.10.2.2 Upload

Selecting the *Upload* button will cause the specified file to be transferred to the client. The web interface will prompt the administrator for confirmation to avoid accidental image uploads.

Example OSD Logo Upload Process:

1. Select the webpage *Browse* button to browse to the logo file
2. Select the File Upload window *Open* button
3. Select the webpage *Upload* button
4. Select the *OK* button on the warning window that reads, “Are you sure? This will upload a new logo for local GUI. This operation may take a few minutes.”
5. Wait for the OSD Logo upload to complete. The following message appears when complete: “Success Flash successfully programmed! You must reset the device for the changes to take effect.”
6. Reset the client

2 On Screen Display (OSD)

The On Screen Display (OSD) local GUI (client only) is displayed to the user when the device is powered on and a PCoIP session is not in progress. The OSD provides a mechanism to connect to a host device via the Connect Screen. The Connect Screen is presented to the user on startup.

The Connect Screen also allows access to the Options Window. The Options Window provides a subset of the functionality provided by the admin interface described in Section 1. The Options Window is accessible through the Options button on the Connect Screen. An administrative password is required to change client options.

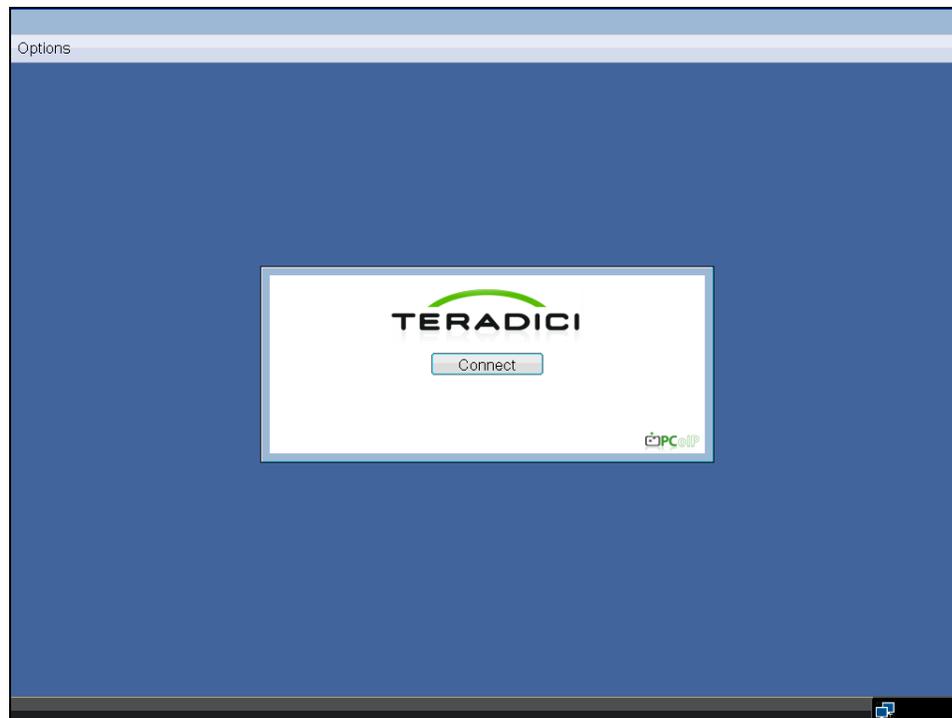
2.1 Connect Screen

The Connect Screen is shown on startup except when the client has been configured for a managed start-up or auto-reconnect.

The logo displayed above the *Connect* button can be changed by uploading a replacement image via the admin interface. Refer to 1.10.2 for information on updating the Connect Screen logo.

The network icon on the bottom right of the connect screen shows the status of the network connection. Users must wait until the network icon is as displayed below in Figure 2-1.

Figure 2-1: OSD Connect Screen



A red 'X' over the network icon indicates that the either the network is not properly connected or that the connection is still being initialized (i.e. during client boot up). Figure 2-2 shows the red 'X' over the network icon when the network isn't ready.

Figure 2-2: Network Not Ready (detail)



Figure 2-3 shows the network icon when ready.

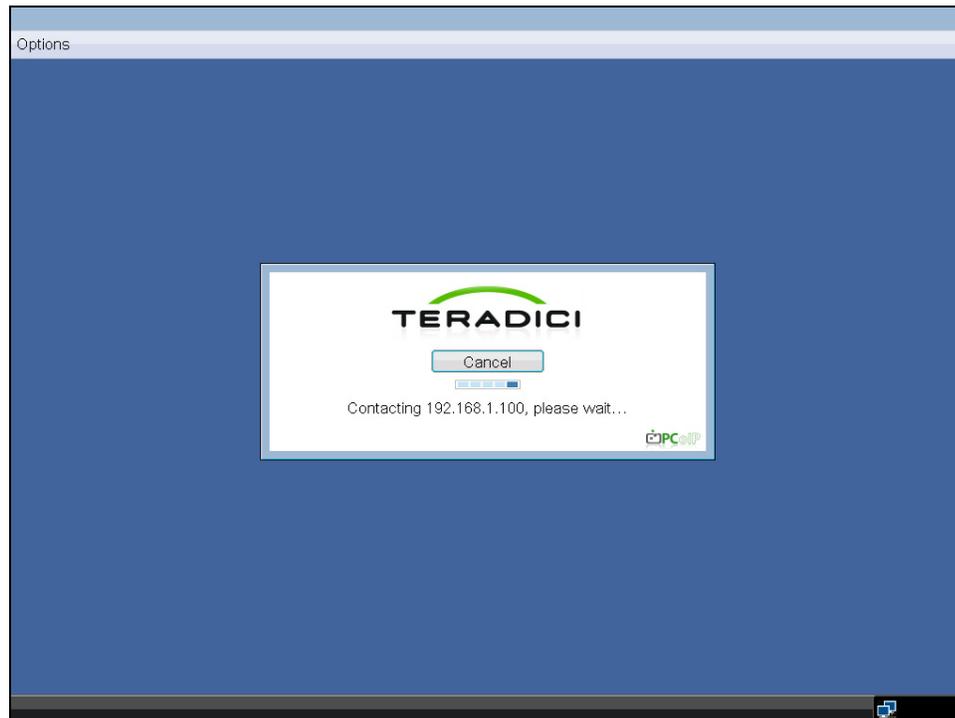
Figure 2-3: Network Ready (detail)



2.1.1 Connect Button

Selecting the *Connect* button initiates a PCoIP session or RDP session, depending on the session settings. While the PCoIP connection is pending, the OSD local GUI will display a “Connection Pending” message. When the connection is established, the OSD local GUI will disappear and be replaced with the session image.

Figure 2-4: OSD Connect Screen (Connecting)



2.2 OSD Options Menu

Selecting the *Options* menu will produce a list of selections. The OSD *Options* menu contains:

- Configuration

- Diagnostics
- Information
- User Settings
- Password

Selecting one of the selections will produce a settings window.

Figure 2-5: OSD Options Menu



2.3 Configuration Window

The *Configuration* window allows the administrator to access window tabs with settings that define how the client operates and interacts with its environment.

The tabs in the *Configuration* window are:

- Network
- Label
- Connection Management
- Discovery
- Session
- RDP
- Language
- OSD
- Reset
- Display
- VMware View

Each tab has *OK*, *Cancel*, and *Apply* buttons that allow the administrator to accept or cancel the setting changes made on the tab.

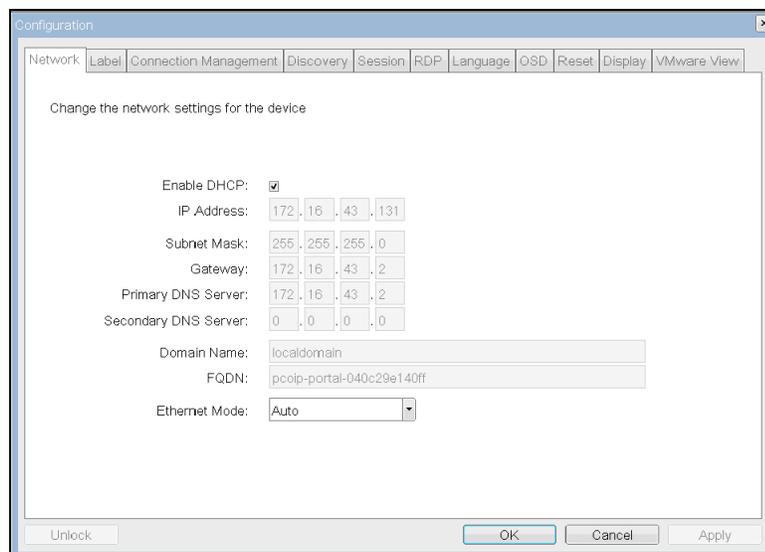
Note: Some PCoIP devices have password protection disabled and do not require a password to login into the administration webpages or access the OSD parameters. Password protection for the Log In page and OSD can be enabled through PCoIP Management Console.

2.3.1 Network Tab

The *Network* tab allows an administrator to set the client network parameters.

Note: The Network parameters can also be configured using the Webpage Administration Interface. See Section 1.6.2 Network.

Figure 2-6: Network Configuration



2.3.1.1 Enable DHCP

Refer to Section 1.6.2.1 Enable DHCP.

2.3.1.2 IP Address

Refer to Section 1.6.2.2 IP Address.

2.3.1.3 Subnet Mask

Refer to Section 1.6.2.3 Subnet Mask.

2.3.1.4 Gateway

Refer to Section 1.6.2.4 Gateway.

2.3.1.5 Primary DNS Server

Refer to Section 1.6.2.5 Primary DNS Server.

2.3.1.6 Secondary DNS Server

Refer to Section 1.6.2.6 Secondary DNS Server.

2.3.1.7 Domain Name

Refer to Section 1.6.2.7 Domain Name.

2.3.1.8 FQDN

Refer to Section 1.6.2.8 FQDN.

2.3.1.9 Ethernet Mode

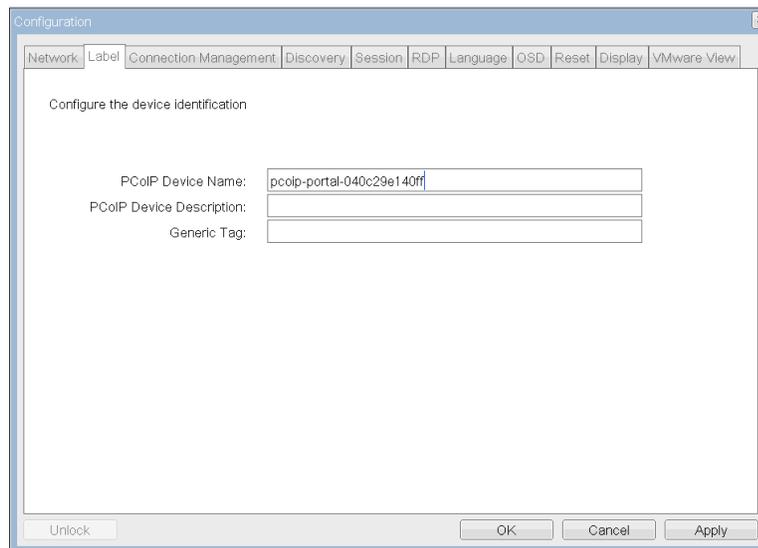
Refer to Section 1.6.2.9 Ethernet Mode

2.3.2 Label Tab

The *Label* tab allows an administrator to add custom information for the client.

Note: The client Label parameters can also be configured using the Webpage Administration Interface. See Section 1.6.3 Label.

Figure 2-7: Label Configuration



2.3.2.1 PCoIP Device Name

Refer to Section 1.6.3.1 PCoIP Device Name.

2.3.2.2 PCoIP Device Description

Refer to Section 1.6.3.2 PCoIP Device Description.

2.3.2.3 Generic Tag

Refer to Section 1.6.3.3 Generic Tag.

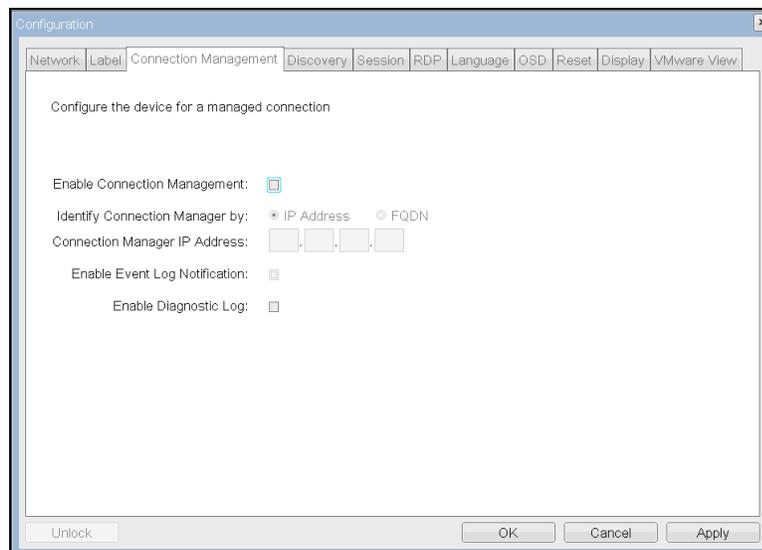
2.3.3 Connection Management Tab

The *Connection Management* tab allows the administrator to enable or disable connection management and to specify the IP address of the connection manager.

In a managed connection, an external Connection Manager Server communicates with and can remotely control and configure the device. Additionally, the connection manager can locate an appropriate peer for the device to connect to and initiate the connection. Connection management can greatly simplify the administration effort for a large, complex system.

Note: The Connection Management parameters can also be configured using the Webpage Administration Interface. See Section 1.6.4 Connection Management.

Figure 2-8: Connection Management Configuration



2.3.3.1 Enable Connection Management

Refer to Section 1.6.4.1 Enable Connection Management.

2.3.3.2 Identify Connection Manager By

Refer to Section 1.6.4.2 Identify Connection Manager By.

2.3.3.3 Enable Event Log Notification

Refer to Section 1.6.4.3 Enable Event Log Notification.

2.3.3.4 Enable Diagnostic Log

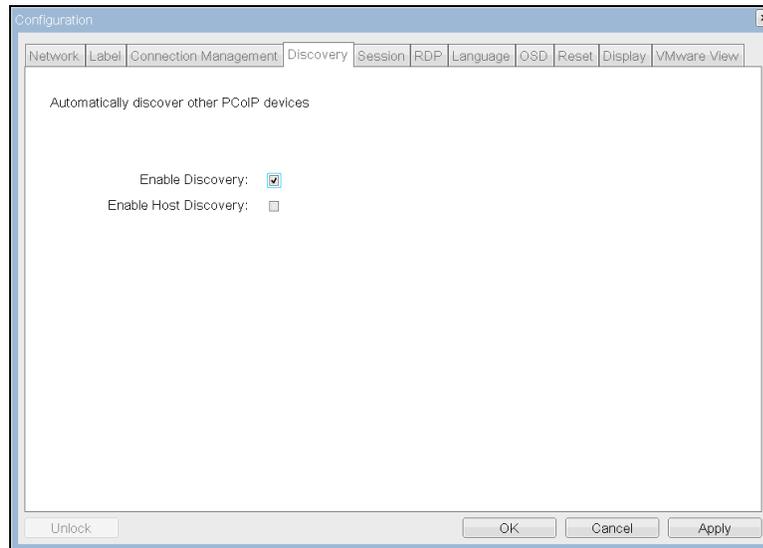
Refer to Section 1.6.4.4 Enable Diagnostic Log.

2.3.4 Discovery Tab

The *Discovery* configuration tab allows the use of features that ease the discovery of clients in a PCoIP system.

Note: The Discovery parameters can also be configured using the Webpage Administration Interface. See Section 1.6.6 Discovery.

Figure 2-9: Discovery Configuration



2.3.4.1 Enable Discovery

Refer to Section 1.6.6.1 SLP Discovery.

2.3.4.2 Enable Host Discovery

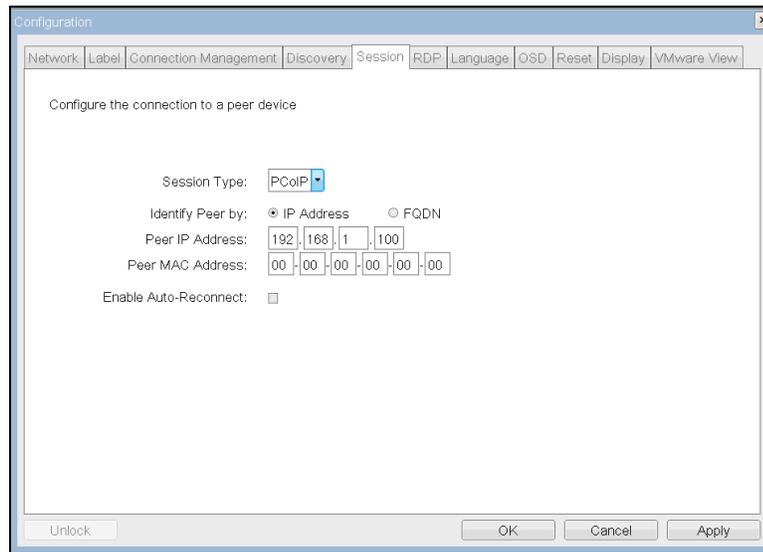
Refer to Section 1.6.6.1 SLP Discovery.

2.3.5 Session Tab

The *Session* tab allows an administrator to configure how the device connects to peer devices.

Note: The Session parameters can also be configured using the Webpage Administration Interface. See Section 1.6.8 Session.

Figure 2-10: Session Configuration



2.3.5.1 Session Type

Refer to Section 1.6.8.2 Session Type.

2.3.5.2 Identify Peer By

Refer to Section 1.6.8.3 Identify Peer By.

2.3.5.3 Enable Auto-Reconnect

Refer to Section 1.6.8.4 Enable Auto-Reconnect.

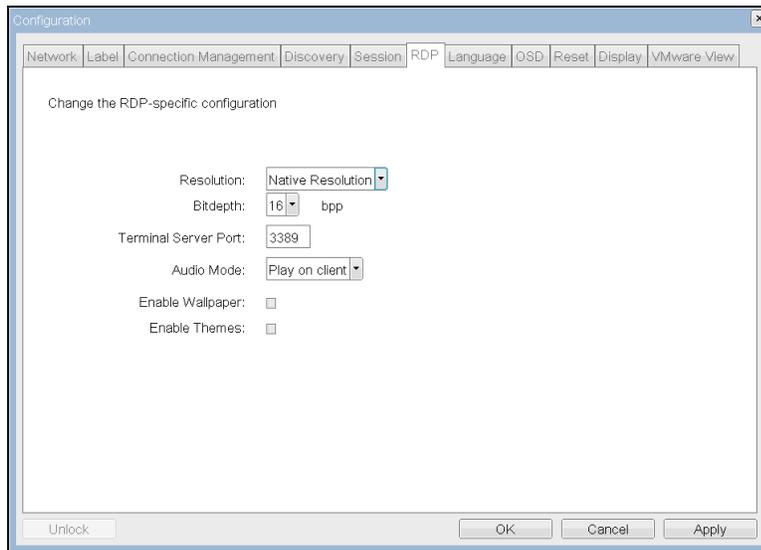
2.3.6 RDP Tab

The *RDP* tab allows the administrator to configure settings specific to the Remote Desktop Protocol (RDP).

For information on the RDP client, see Section 6 Appendix C: Client RDP Compatibility.

Note: The RDP parameters can also be configured using the Webpage Administration Interface. See Section 1.6.10 RDP.

Figure 2-11: RDP Configuration



2.3.6.1 Resolution

Refer to Section 1.6.10.1 Resolution.

2.3.6.2 Bit Depth

Refer to Section 1.6.10.2 Bit Depth.

2.3.6.3 Terminal Server Port

Refer to Section 1.6.10.3 Terminal Server Port.

2.3.6.4 Audio Mode

Refer to Section 1.6.10.4 Audio Mode.

2.3.6.5 Enable Wallpaper

Refer to Section 1.6.10.5 Enable Wallpaper.

2.3.6.6 Enable Themes

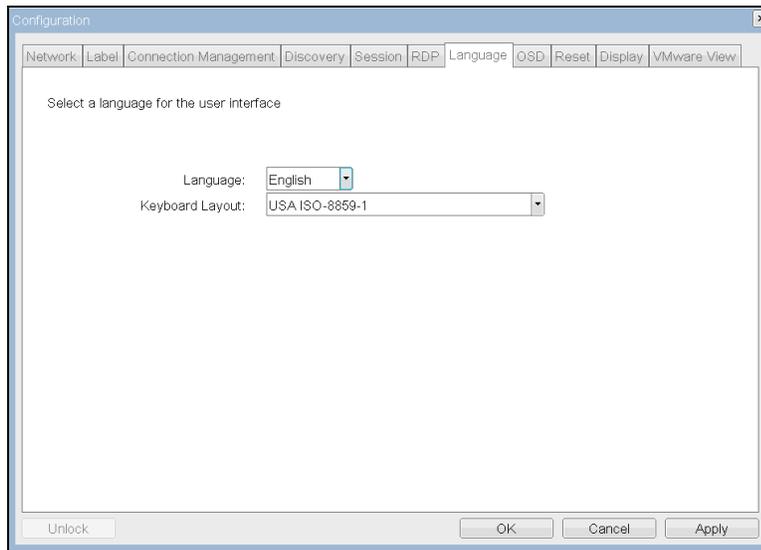
Refer to Section 1.6.10.6 Enable Themes.

2.3.7 Language Tab

The *Language* field allows the administrator to configure the language of the OSD.

Note: The Language parameters can also be configured using the Webpage Administration Interface. See Section 1.6.11 Language.

Figure 2-12: Language Configuration



2.3.7.1 Language

Refer to Section 1.6.11.1 Language.

2.3.7.2 Keyboard Layout

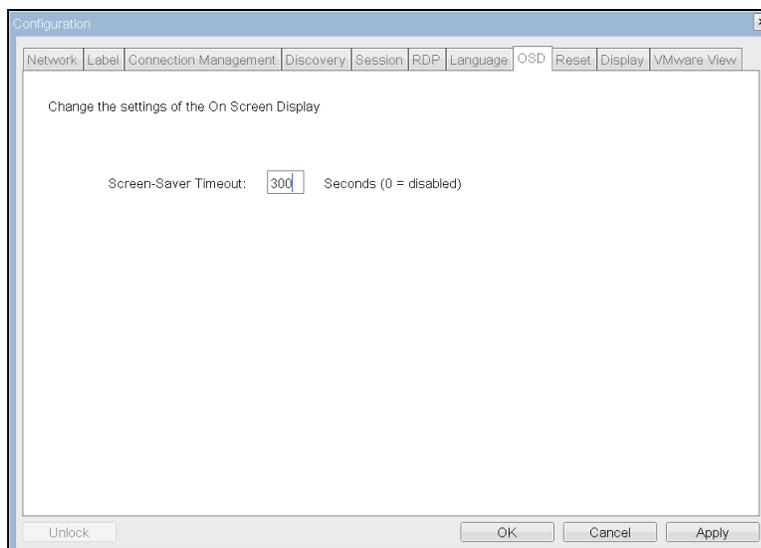
Refer to Section 1.6.11.2 Keyboard Layout.

2.3.8 OSD Tab

The *OSD* tab allows the administrator to modify the On Screen Display (OSD) parameters.

Note: The OSD parameters can also be configured using the Webpage Administration Interface. See Section 1.6.12 OSD.

Figure 2-13: OSD Configuration



2.3.8.1 Screen-Saver Timeout

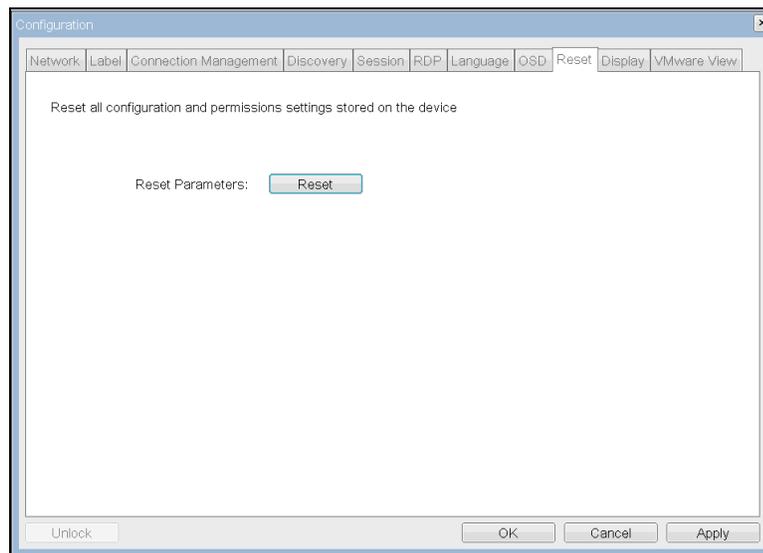
Refer to Section 1.6.12.1 Screen-Saver Timeout.

2.3.9 Reset Tab

The *Reset* tab allows the administrator to reset all the configurable parameters stored in flash.

Note: The Reset can also be initiated using the Webpage Administration Interface. See Section 1.6.18 Reset Parameters.

Figure 2-14: Reset



2.3.9.1 Reset Parameters

Refer to Section 1.6.18.1 Reset Parameters.

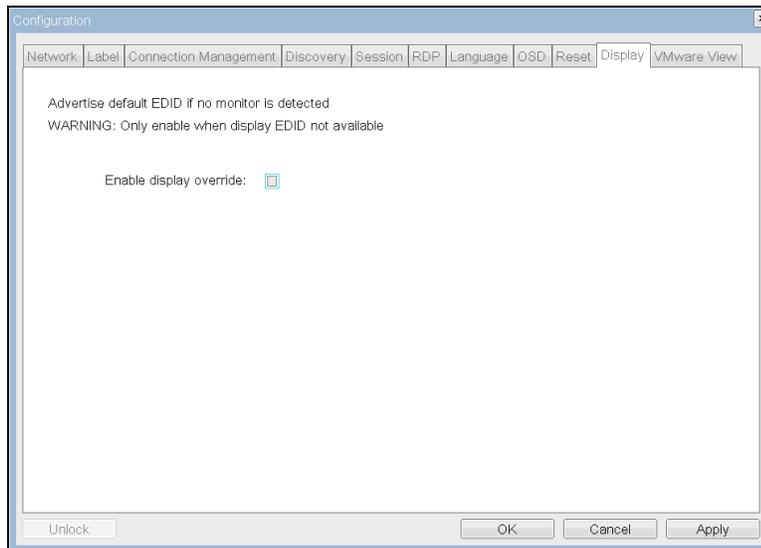
2.3.10 Display Tab

The *Display* tab allows enabling the EDID override mode.

Under normal operation the GPU in the host computer queries the monitor to determine the capabilities of the monitor. The capabilities of the monitor 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. In this situation the user should configure the client to report default EDID information to the GPU by enabling the display override mode.

Note: The EDID override mode can only be enabled from the OSD.

Figure 2-15: Enable Display Override Configuration



2.3.10.1 Enable Display Override

When the *Enable display override* option is enabled, the client will provide default EDID information to the attached display(s).

WARNING: Enabling display override will force default monitor display information that may not be compatible with the connected monitor and result in a blank monitor. Only enable display override when there is no valid EDID information and monitor display characteristics are understood.

When this feature is enabled the client provides EDID information to the host GPU that indicates the following resolutions are supported:

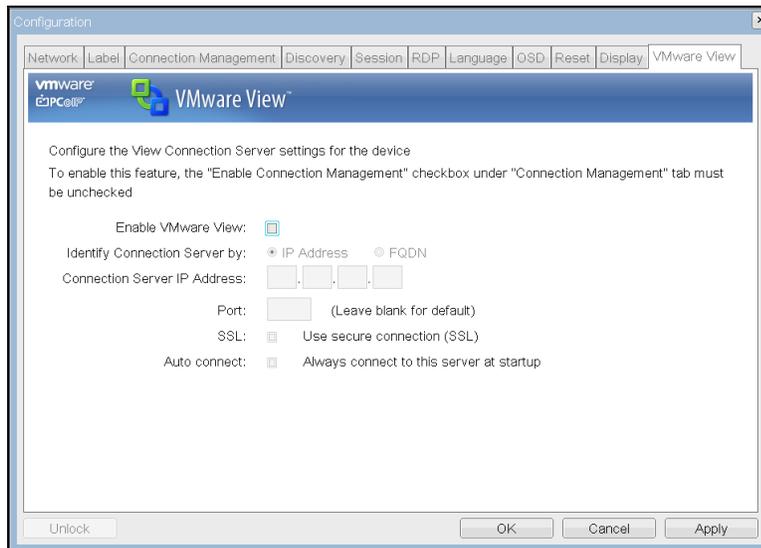
- 800x600 @60Hz
- 1280x800 @60Hz
- 1280x960 @60Hz
- 1280x1024 @60Hz (native resolution advertised)
- 1600x1200 @60Hz
- 1680x1050 @60Hz
- 1920x1080 @60Hz
- 1920x1200 @60Hz

2.3.11 VMware View Tab

The *VMWare View* tab allows configuration for use with a VMware View Connection Server.

Note: The *VMware View* parameters can also be configured using the *Webpage Administration Interface*. See Section 1.6.5 *VMware View*.

Figure 2-16: VMware View Configuration



2.3.11.1 Enable VMware View

Refer to Section 1.6.5.1 Enable VMware View.

2.3.11.2 Identify Connection Server by

Refer to Section 1.6.5.2 Identify Connection Server by.

2.3.11.3 Port

Refer to Section 1.6.5.3 Port.

2.3.11.4 SSL

Refer to Section 1.6.5.4 SSL.

2.3.11.5 Auto connect

Refer to Section 1.6.5.5 Auto connect.

2.4 Diagnostics Window

The *Diagnostics* window allows the administrator to access window tabs with diagnostics concerning the client. The tabs in the *Diagnostics* window are:

- Event Log
- Session Statistics
- PCoIP Processor
- Ping

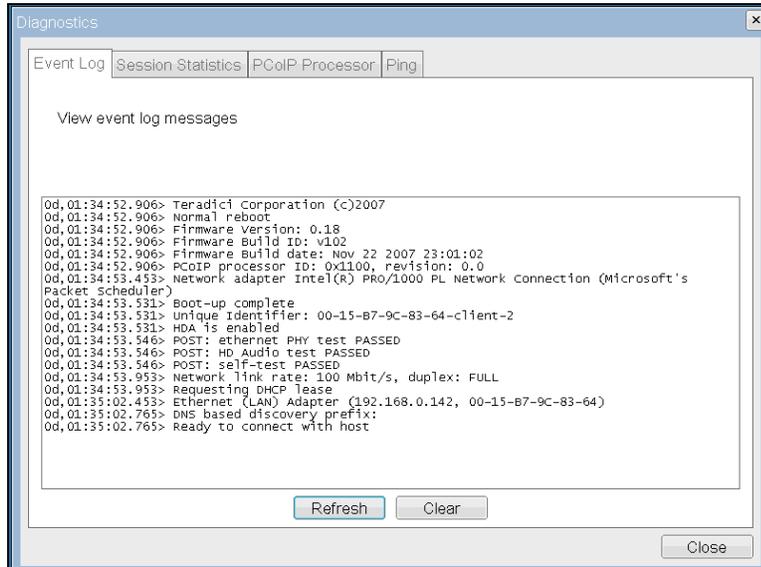
Each tab has a *Close* button to close the window.

2.4.1 Event Log Tab

The *Event Log* tab allows the administrator to view and clear event log messages from the client.

Note: The *Event Log* (terse or verbose) can also be initiated using the *Webpage Administration Interface*. See *Section 1.8.1 Event Log*.

Figure 2-17: Event Log



2.4.1.1 View event log message

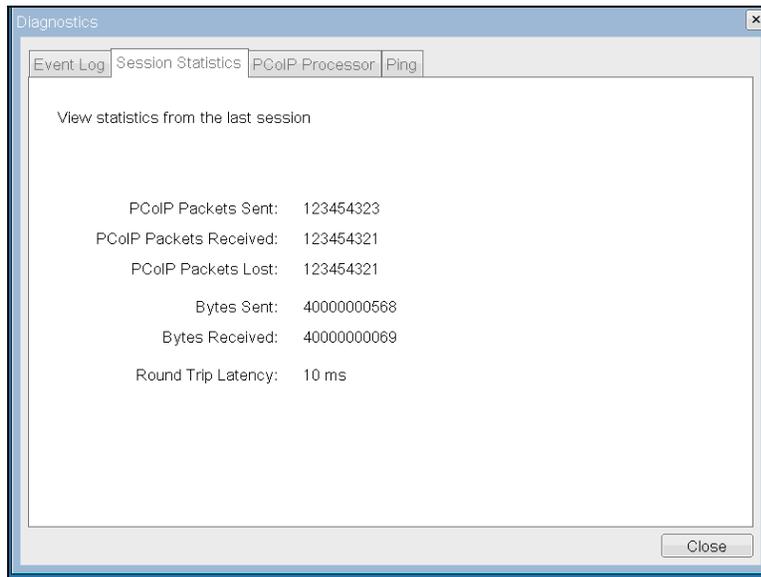
Refer to *Section 1.8.1.1 Event log message*.

2.4.2 Session Statistics Tab

The *Session Statistics* tab allows the administrator to view PCoIP protocol specific statistics for the last PCoIP session that was active on the client.

Note: *Session Statistics* can also be viewed using the *Webpage Administration Interface*. See *Section 1.8.3 Session Statistics*.

Figure 2-18: Session Statistics



2.4.2.1 PCoIP Packets Statistics

Refer to Section 1.8.3.2 PCoIP Packets Statistics.

2.4.2.2 Bytes Statistics

Refer to Section 1.8.3.3 Bytes Statistics.

2.4.2.3 Round Trip Latency

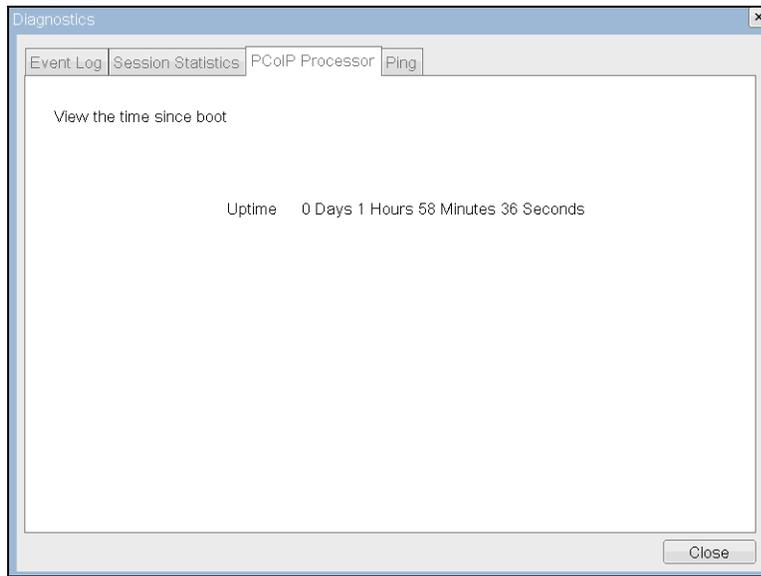
Refer to Section 1.8.3.4 Round Trip Latency.

2.4.3 PCoIP Processor Tab

The *PCoIP Processor* tab allows the administrator to view the uptime of the client PCoIP processor since last boot.

Note: The PCoIP Processor Uptime can also be viewed in the Webpage Administration Interface. See Section 1.8.7 PCoIP Processor.

Figure 2-19: PCoIP Processor



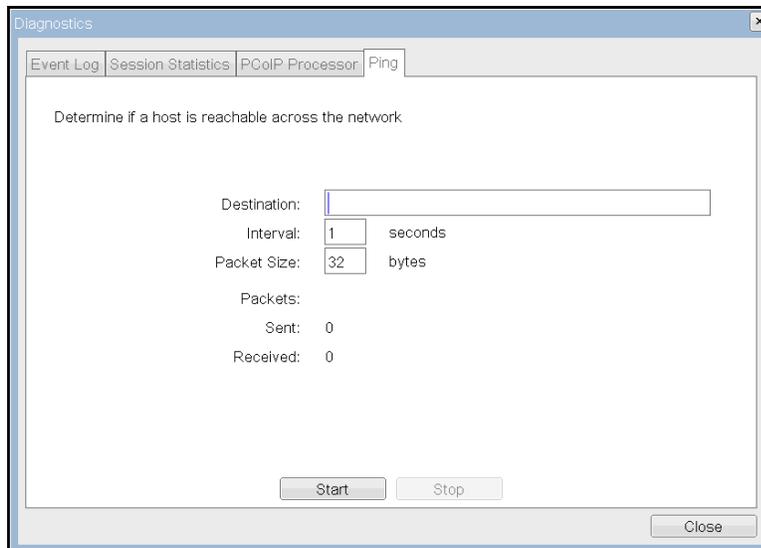
2.4.4 Ping Tab

The *Ping* tab allows the administrator to ping a device to see if it is reachable across an IP network. This may be useful for determining if a host is reachable.

Note: The OSD ping function does not force the “do not fragment” ping flag, and should not be used to determine MTU size for the network path.

Note: The Ping tab has no matching menu in the Webpage Administration Interface of Section 1.

Figure 2-20: Ping



2.4.4.1 Ping Settings

Destination	IP Address or FQDN to ping
Interval	Interval between ping packets
Packet Size	Size of ping packet

2.4.4.2 Packets

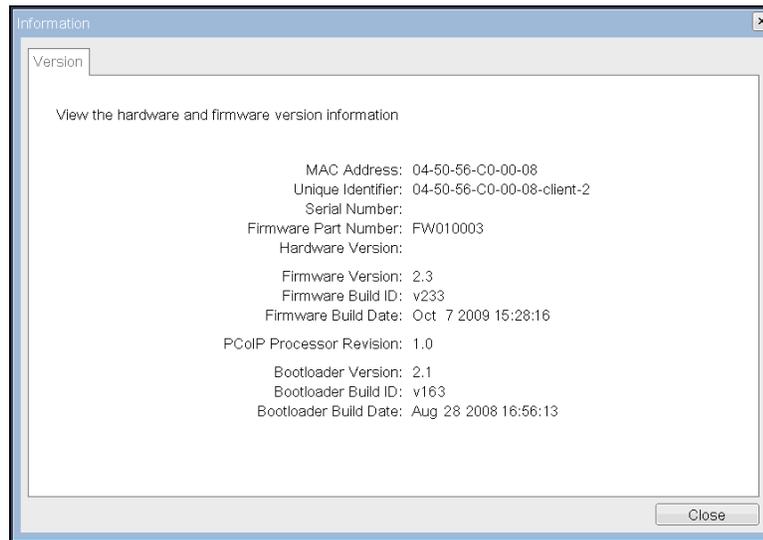
Sent	Number of ping packets sent
Received	Number of ping packets received

2.5 Information Window

The *Information* window allows an administrator to access the Version tab containing information about the device.

Note: The Version information can also be viewed using the Webpage Administration Interface. See Section 1.9.1 Version.

Figure 2-21: Version



2.5.1.1 VPD Information

Refer to Section 2.5.1.11.9.1.1 VPD Information.

2.5.1.2 Firmware Information

Refer to Section 1.9.1.2 Firmware Information.

2.5.1.3 PCoIP Processor Revision

Refer to Section 1.9.1.3 PCoIP Processor Revision.

2.5.1.4 Bootloader Information

Refer to Section 1.9.1.4 Bootloader Information.

2.6 User Settings Window

The *User Settings* window allows the user to access window tabs that define the mouse and keyboard settings and the PCoIP protocol image quality.

The tabs in the User Settings menu are:

- Mouse
- Keyboard
- Image

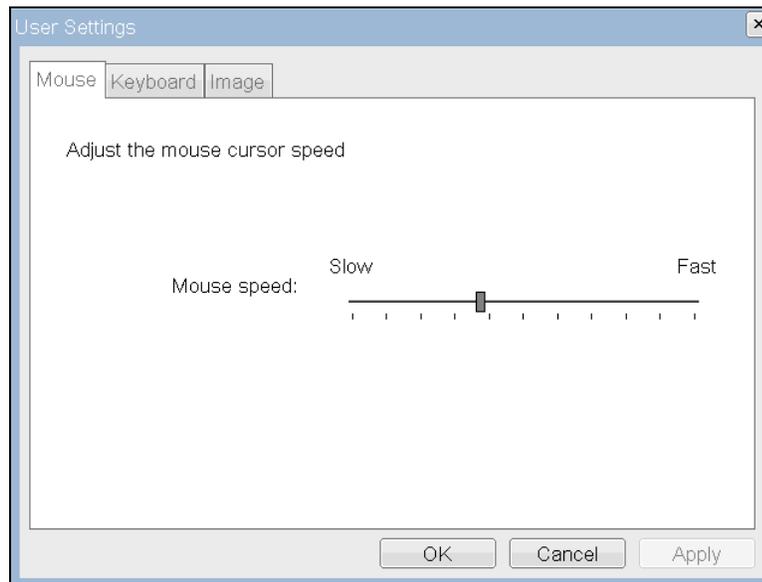
2.6.1 Mouse Tab

The *Mouse* tab allows a user to change the mouse cursor speed settings for the OSD and RDP 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 PCoIP Host Software User Guide for more information).

Note: The *Mouse* tab has no corresponding menu in the Webpage Administration Interface of Section 1.

Figure 2-22: Mouse



Mouse Speed

The *Mouse Speed* field allows the client mouse cursor speed to be configured.

Note: The *Mouse Speed* can also be configured via the PCoIP Host Software. For more information on using the PCoIP Host Software, refer to the PCoIP Host Software User Guide for more information.

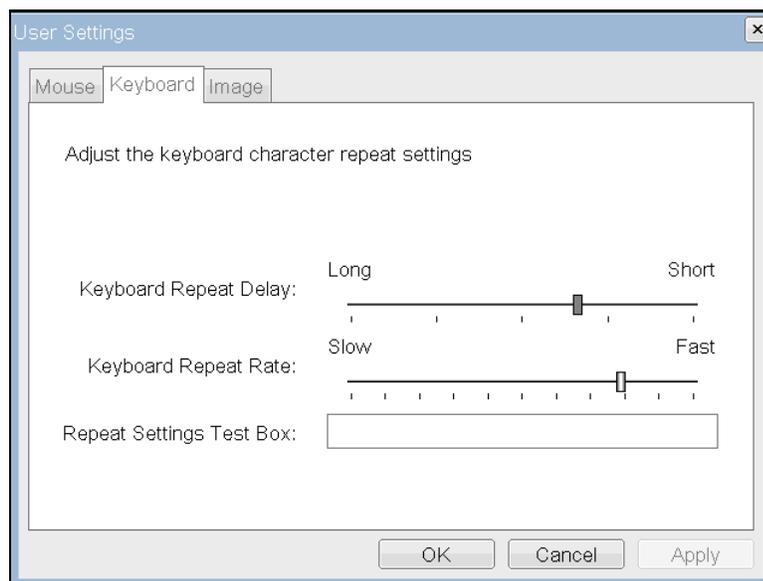
2.6.2 Keyboard Tab

The *Keyboard* tab allows a user to change the keyboard repeat settings for the OSD and RDP sessions.

Note: The keyboard settings do not affect the keyboard settings when a PCoIP session is active unless the Local Keyboard Host Driver function is being used (see PCoIP Host Software User Guide for more information).

Note: The *Keyboard* tab has no corresponding menu in the Webpage Administration Interface of Section 1.

Figure 2-23: Keyboard



Keyboard Repeat Delay

The *Keyboard Repeat Delay* field allows a user to configure the client keyboard repeat delay.

Keyboard Repeat Rate

The *Keyboard Repeat Rate* field allows a user to configure the client keyboard repeat rate.

Repeat Settings Test Box

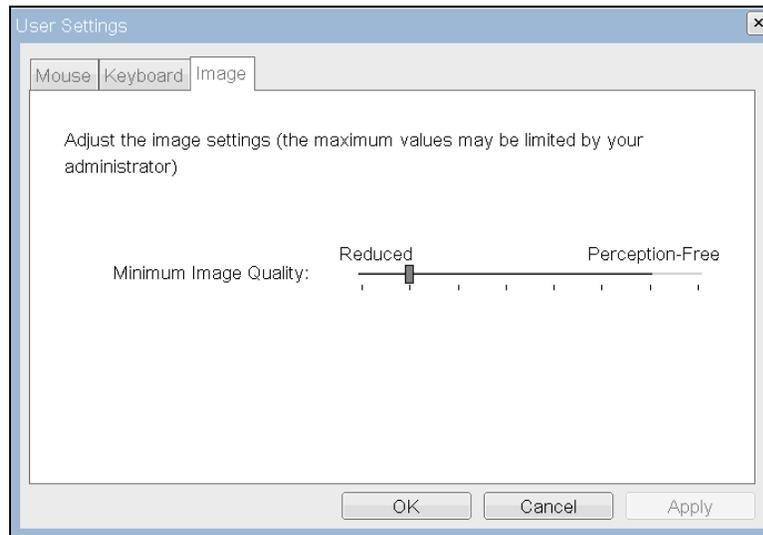
The *Repeat Settings Test Box* field allows a user to test the chosen keyboard settings.

2.6.3 Image Tab

The *Image* tab allows a user to change the image settings on the PCoIP system.

Note: The *Image* parameters can also be configured using the Webpage Administration Interface. See Section 1.6.13.1 Minimum Image Quality.

Figure 2-24: Image



Minimum Image Quality

Refer to Section 1.6.13.1 Minimum Image Quality.

2.7 Password Window

The *Password* window allows an administrator to update the administrative password for the device. Note that this will affect the web interface and the local OSD GUI.

Note: Care must be taken when updating the client password as the client may become unusable if the password is lost.

Note: The Password can also be updated using the Webpage Administration Interface. See Section 1.6.17 Password .

Note: Some PCoIP devices have password protection disabled by default and this *Password* window is not available. Password protection can be enabled through PCoIP Management Console for these devices.

Figure 2-25: Change Password



Old Password

The *Old Password* field must match the current administrative password for the change to take place.

New Password

The *New Password* field will be the new administrative password for both the web interface and the local OSD GUI.

Confirm New Password

The *Confirm New Password* field must match the *New Password* field for the change to take place.

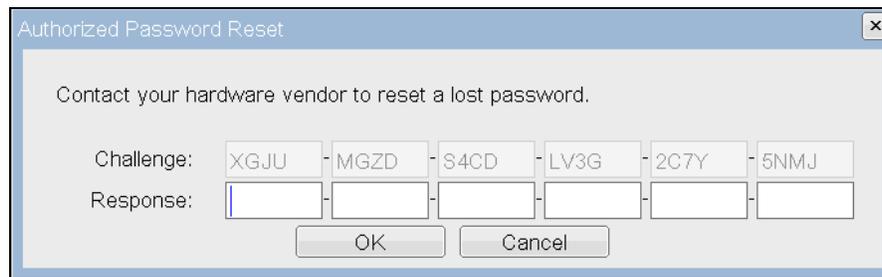
Reset

In the unlikely event that a client password is lost, the *Reset* button allows an administrator to request a *Response* code from their vendor. The *Challenge* code can be sent to the vendor. The vendor will qualify the request and return a *Response* code if authorized.

Once the *Response* code is correctly entered, the client's password is reset to an empty string and the administrator is prompted to enter a new password.

Note: Contact the client vendor for more information when an authorized password reset is required.

Figure 2-26: Authorized Password Reset



3 Overlay Windows

Overlay windows provide a mechanism for displaying information to the user while a PColP session is in progress. These windows are occasionally displayed on top of the user’s remote session.

Status overlay windows are used to show network, USB device status and monitor status in the form of icons and text. The overlays have simple animation and are displayed when the status changes (i.e., the network connection is lost or an unauthorized USB device is plugged in).

3.1 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 will be shown when the client network cable is disconnected or when no PColP protocol traffic is received by the client for more than two seconds. An example is shown in Figure 3-1.

Figure 3-1: Network Connection Lost Overlay

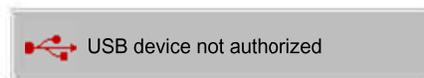


The lost network connection message will persist until the network is restored or the timeout expires (and the PColP session ends).

3.2 USB Device Not Authorized Overlay

If an unauthorized USB device is connected, an overlay with the message “USB device not authorized” is displayed. An example is shown in Figure 3-2.

Figure 3-2: USB Device Not Authorized Overlay



The overlay will be displayed for approximately 5 seconds.

3.3 USB Over Current Notice Overlay

If USD devices connected to the client are beyond the current handling for the USB ports, an overlay with the message “USB over current notice” is displayed. An example is shown in Figure 3-3.

Figure 3-3: USB Over Current Notice Overlay

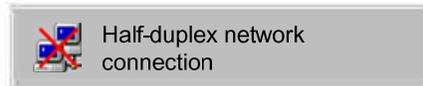


The overlay will be displayed until USB devices are removed to meet the current handling of the USB ports.

3.4 Half-Duplex Overlay

PCoIP Technology is not compatible with Half-Duplex network connections. When a half-duplex connection is detected, an overlay with the message “Half-duplex network connection” is displayed. An example is shown in Figure 3-4.

Figure 3-4: Half-Duplex Overlay



The overlay will be displayed for the first 30 seconds of the session. Refer to Section 1.6.2 for more information on network configuration.

3.5 Video Source Overlays

Improper connection of the host video source is denoted by two possible overlays.

When no video source is connected to the host, an overlay with the message “No source signal” is displayed. This helps the user debug a situation where the host does not have video source connected or the Host PC has stopped driving a video signal. This can be rectified by connecting the host PC video to the host. An example of the overlay is shown in Figure 3-5.

Figure 3-5: No Source Signal Overlay



When a video source to the host does not correspond to the video port used on the client, an overlay with the message “Source signal on other port” is displayed. This helps the user debug a situation where the video source is connected to the wrong port. This can be rectified by swapping the video port used either on the host or on the client. An example of the overlay is shown in Figure 3-6.

Figure 3-6: Source Signal on Other Port Overlay



The overlays will be displayed for approximately 5 minutes. The monitor will be put into sleep mode approximately 15 seconds later.

4 Appendix A: Usage Examples

4.1 Peer-to-Peer Direct Connection Example

This example provides an overview of configuring a client and host for a direct connection, i.e. without the use of a Connection Management Server or the Enable Host Discover option.

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

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

Note: For a Peer-to-Peer direct connection, the administrator must know the IP and MAC addresses of the client and host.

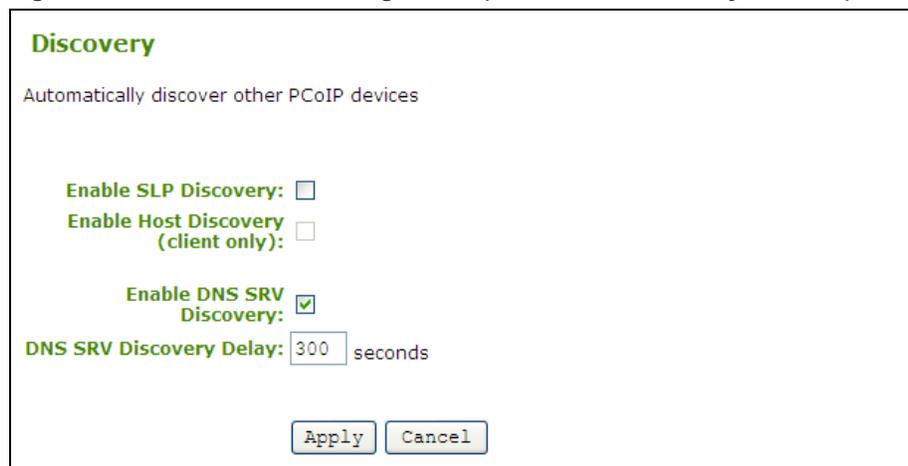
4.1.1 Configuring the Client Peer-to-Peer Operation

Note: This example uses the admin interface for configuring the client for peer-to-peer operation. The OSD could also be used to configure the client. See Section 2 On Screen Display (OSD) for the corresponding OSD functionality.

Configure the client for peer-to-peer direct connection:

1. Open the client admin interface by using an internet browser to open the client IP address, e.g. `https://192.168.42.149`
2. Log in to the client admin interface (with password if enabled)
3. Select the *Discovery* webpage from the *Configuration* menu
4. Ensure *Enable Host Discover* is not enable

Figure 4-1: Client Discover Configuration (Enable SLP Discovery disabled)



Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable Host Discovery (client only):

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

Apply Cancel

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

Figure 4-2: Client Connection Management Peer-to-Peer Configuration

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

Figure 4-3: Client Session Webpage Peer-to-Peer Configuration

8. In the Identify Peer by field, select IP address
9. Enter the host IP address in *Peer IP Address* field, e.g. 192.168.50.107
10. Enter the host MAC address in *Peer MAC Address* field, e.g. 00-1C-8A-03-00-CA
11. Select the *Apply* button to accept the changes
12. Select the *PCoIP Processor* webpage from the *Diagnostics* menu

Figure 4-4: Client PCoIP Processor Webpage Peer-to-Peer Configuration



13. Select the *Reset* button to reset the PCoIP processor

4.1.2 Configuring the Host Peer-to-Peer Operation

Configure the host for peer-to-peer direct connection:

1. Open the host admin interface by using an internet browser to open the host IP address, e.g. `https://192.168.50.107`
2. Log in to the host admin interface (using password if enabled)
3. Select the *Connection Management* webpage from the *Configuration* menu

Figure 4-5: Host Connection Management Peer-to-Peer Configuration



4. Ensure Enable Connection Management is not selected
5. Select the *Session* webpage from the *Configuration* menu

Figure 4-6: Host Session Webpage Peer-to-Peer Configuration

Session

Configure the connection to a peer device

Accept Any Peer (host only):

Session Type (client only):

Identify Peer by: IP address FQDN

Peer IP Address: . . .

Peer MAC Address: - - - - -

Enable Auto-Reconnect (client only):

Enable AES-128-GCM:

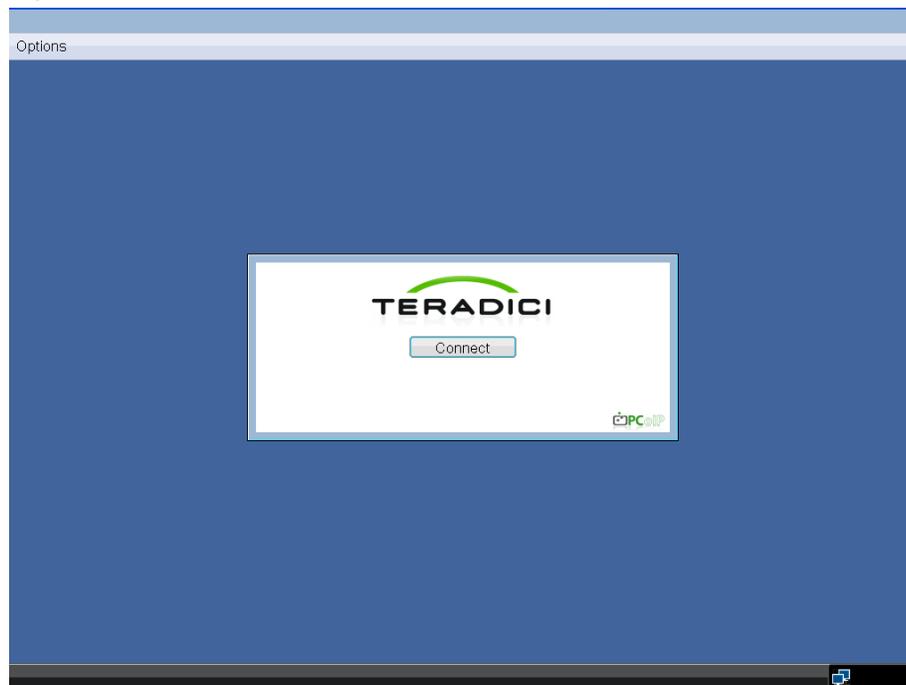
Enable Salsa20-256-Round12:

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

4.1.3 Initiating the Peer-to-Peer Session

Start the peer-to-peer session:

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

Figure 4-7: Peer-to-Peer Connect Screen


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

4.2 DHCP and Enable Host Discovery Example

This example covers configuring 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, the administrator must know the IP address of the client and host, regardless of whether it is set statically or dynamically.

4.2.1 Configuring Client DHCP and SLP Discovery

Note: Although this example uses the Administration Web Interface for configuring the client for DHCP and Host Discovery operation, the OSD may also be used to configure the client. See Section 2 On Screen Display (OSD) for the corresponding OSD functionality.

Configure the client for DHCP and SLP Discovery:

1. Open the client admin interface by using an internet browser to open the client IP address, e.g. <https://192.168.0.111>
2. Log in to the client admin interface (with password if enabled)
3. Select the *Connection Management* webpage from the *Configuration* menu

Figure 4-8: Client Connection Management Configuration



Connection Management
Configure the device for a managed connection

Enable Connection Management:

Identify Connection Manager by: IP address FQDN

Connection Manager IP Address: . . .

Enable Event Log Notification:

Enable Diagnostic Log:

Apply Cancel

4. Ensure Enable Connection Management is not selected
5. Select the *Discovery* webpage from the *Configuration* menu

Figure 4-9: Client Discovery Webpage Enable SLP Discovery Configuration



Discovery
Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable Host Discovery (client only):

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

Apply Cancel

6. Select Enable SLP Discovery and Enable Host Discovery
7. Select the *Apply* button to accept the changes
8. Select *Continue* to complete configuration
9. Select the *Network* webpage from the *Configuration* menu

Figure 4-10: Client Network Webpage DHCP Configuration

10. Select Enable DHCP

11. Select the *Apply* button to accept the changes

Note: Once configured for DHCP, the IP address will be leased from the DHCP server. For future configuration, obtain the IP address from the DHCP server.

12. Select the *PCoIP Processor* webpage from the *Diagnostics* menu

Figure 4-11: Client PCoIP Processor Webpage

13. Select the *Reset* button to reset the PCoIP processor

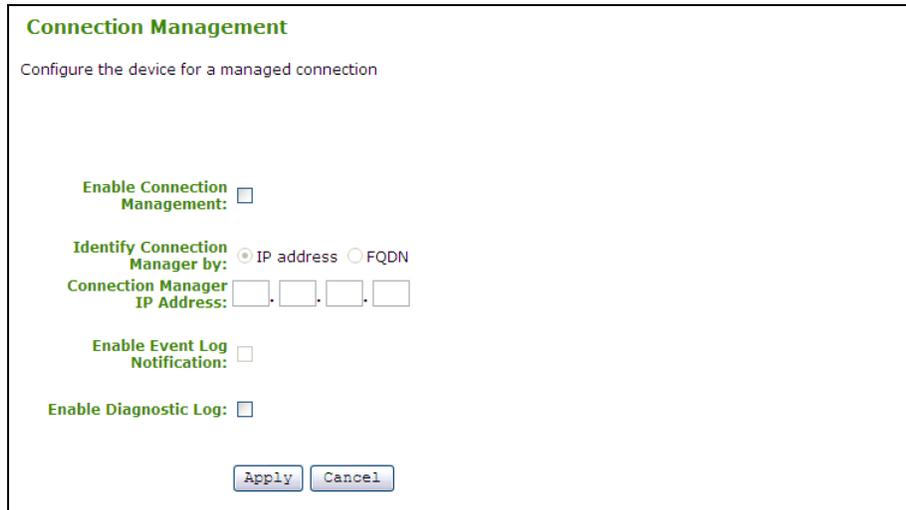
4.2.2 Configuring Host DHCP and SLP Discovery

Configure the host for DHCP and SLP Discovery:

1. Open the host admin interface by using an internet browser to open the host IP address, e.g. <https://192.168.1.222>

2. Log in to the host admin interface (using password if enabled)
3. Select the *Connection Management* webpage from the *Configuration* menu

Figure 4-12: Host Connection Management Configuration



Connection Management
Configure the device for a managed connection

Enable Connection Management:

Identify Connection Manager by: IP address FQDN

Connection Manager IP Address: . . .

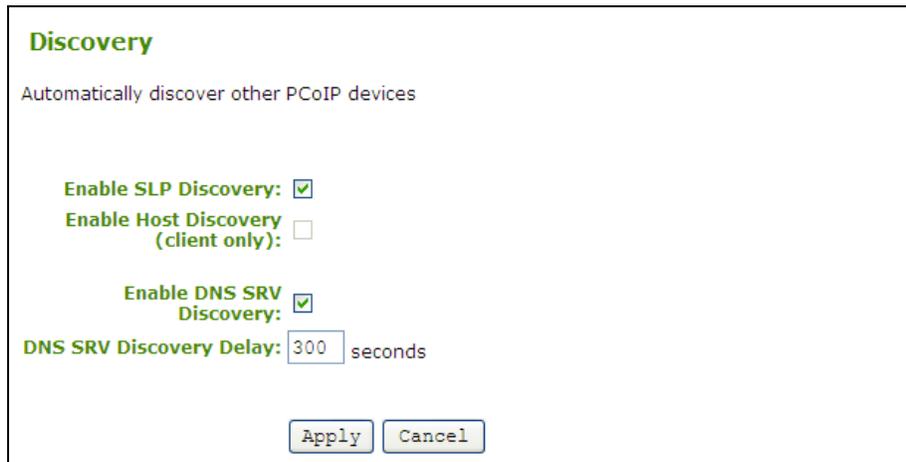
Enable Event Log Notification:

Enable Diagnostic Log:

Apply Cancel

4. Ensure Enable Connection Management is not selected
5. Select the *Discovery* webpage from the *Configuration* menu

Figure 4-13: Host Discovery Webpage Enable SLP Discovery Configuration



Discovery
Automatically discover other PCoIP devices

Enable SLP Discovery:

Enable Host Discovery (client only):

Enable DNS SRV Discovery:

DNS SRV Discovery Delay: seconds

Apply Cancel

6. Select Enable SLP Discovery
7. Select the *Apply* button to accept the changes
8. Select the *Network* webpage from the *Configuration* menu

Figure 4-14: Host Network Webpage DHCP Configuration

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 (client only):

Maximum MTU Size: bytes

9. Select Enable DHCP

10. Select the *Apply* button to accept the changes

Note: Once configured for DHCP, the IP address will be leased from the DHCP server. For future configuration, obtain the IP address from the DHCP server.

11. Select the *PCoIP Processor* webpage from the *Diagnostics* menu

Figure 4-15: Host PCoIP Processor Webpage

PCoIP Processor

Reset the PCoIP device, view the time elapsed since boot

Current Time:

Time Since Boot: 0 Days 1 Hours 17 Minutes 41 Seconds

Reset PCoIP Processor:

12. Select the *Reset* button to reset the PCoIP processor

Note: The host will not reset immediately. The reset will be deferred until the Host PC restarts, enters standby, hibernates or powers off.

4.2.3 Initiating SLP Discovery Session

Start the SLP discovery session:

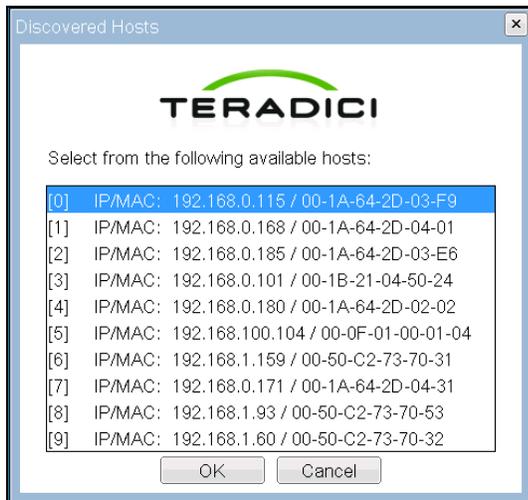
1. From the OSD, select the *Connect* button to start discovering available hosts

Figure 4-16: Connect Screen



2. Select the desired host from the *Discovered Hosts* screen and select *OK*

Figure 4-17: Discovered Hosts Screen



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

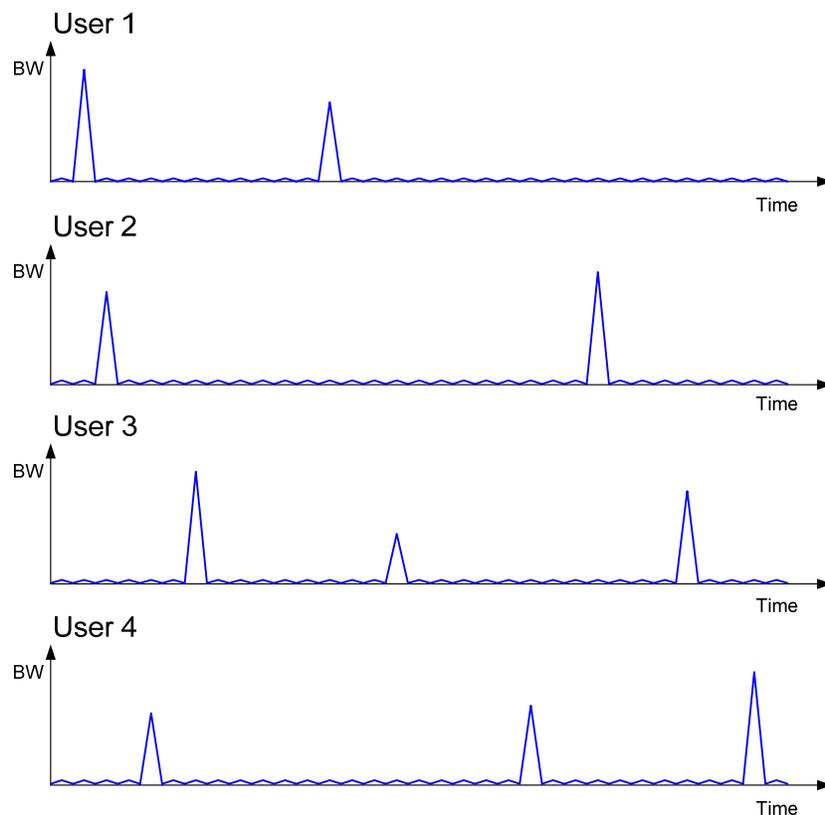
4.3 Bandwidth and Image Configuration Example

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

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

Figure 4-18 shows simplified bandwidth requirements for each user assuming they each had the full 100 Mbps available. The figure shows that network demand for each user peaks only for short periods (e.g. when opening/closing windows, scrolling a page, etc.).

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

Figure 4-18: Simplified User Bandwidth Requirements (Assuming 100 Mbps)


4.3.1 Configuring the Host Bandwidth Limit to 25 Mbps

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

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

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

1. Open the host admin interface for the first user's host by using an internet browser to open the host IP address
2. Log in to the host admin interface (using password if enabled)
3. Select the *Bandwidth* webpage from the *Configuration* menu

Figure 4-19: Host Bandwidth Limit Configuration (25 Mbps)

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)

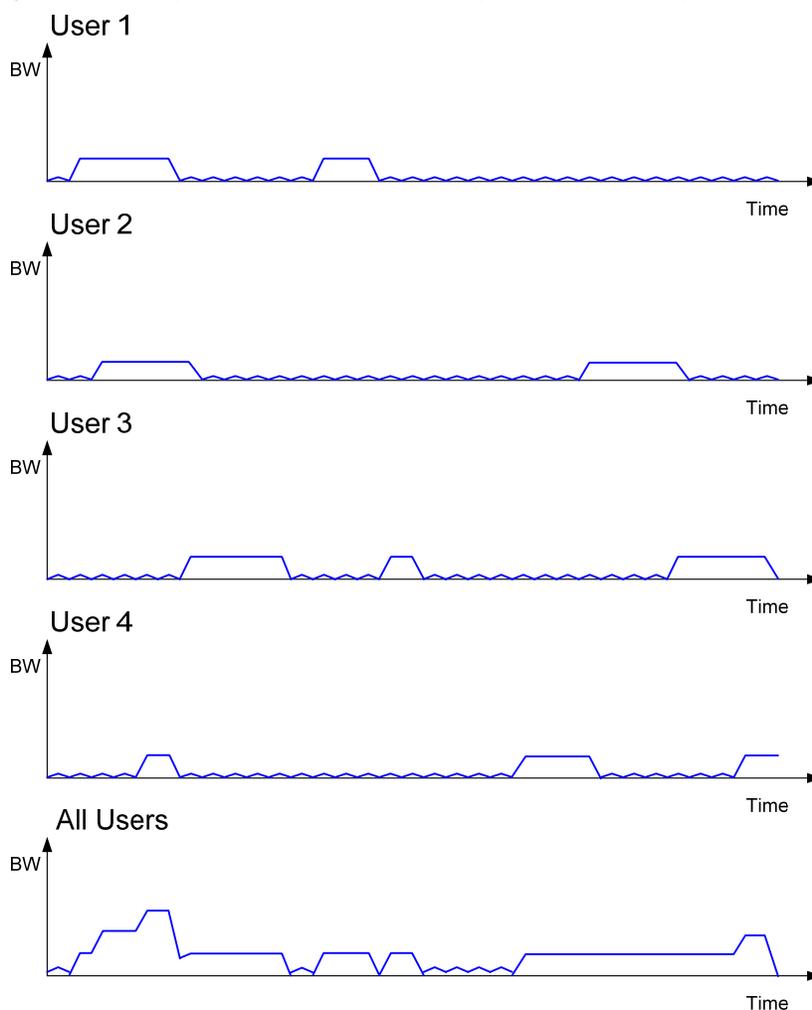
4. Enter 25 in the Device Bandwidth Limited field
5. Enter 20 in the Device Bandwidth Target field
6. Select the *Apply* button to accept the changes
7. Repeat for the other three users' hosts

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

Figure 4-20 shows simplified bandwidth usage with the limit for each user now configured for 25 Mbps. This figure shows that all users are limited to 25 Mbps and do not have access to more bandwidth when required. It also shows that even when the usage is totaled, the total switch bandwidth (100 Mbps) is never fully used.

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

Figure 4-20: Simplified User Bandwidth Requirements (25 Mbps)



4.3.2 Configuring Image Properties

In the above section, the bandwidth was limited to 25 Mbps with a bandwidth target of 20 Mbps. Depending on the usage, it is possible that users may occasionally require more than that bandwidth limit to fully render their display information at maximum quality and full frame rate. The PCoIP system gives two controls over imaging quality that can optimize the user experience in environments where bandwidth is constrained.

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

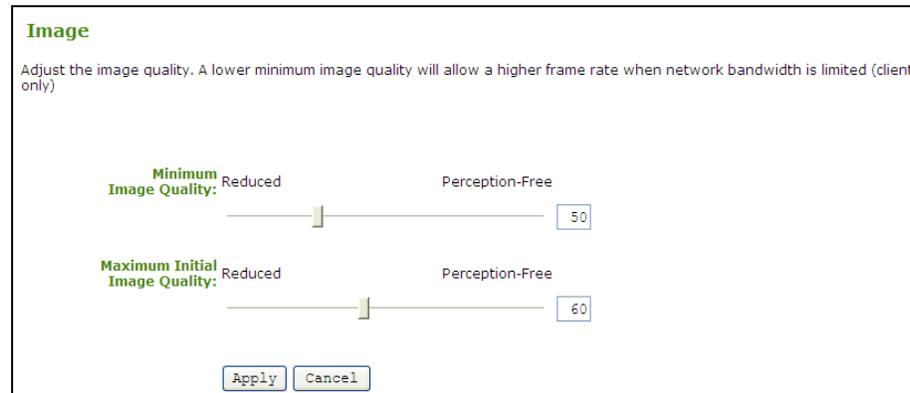
The *Maximum Initial Image Quality* setting can change the peak bandwidth required by any user. Decreasing the *Maximum Initial Image Quality* from the default setting of 90 can reduce the amount of bandwidth required per user while maintaining a minimum limit on the user experience.

Note: This example uses the Administration Web Interface for configuring the client for *Minimum Image Quality* and *Maximum Initial Image Quality*. The OSD may also be used to configure the client. See Section 2 On Screen Display (OSD) for the corresponding OSD functionality. The *Maximum Initial Image Quality* does not have a corresponding

parameter on the OSD; it is intended as an administrator-only parameter due to the impact on network traffic.

1. Open the client admin interface for the first user's client by using an internet browser to open the client IP address
2. Log in to the client admin interface (using password if enabled)
3. Select the *Image* webpage from the *Configuration* menu

Figure 4-21: Client Minimum Image Quality Configuration



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

The *Minimum Image Quality* is now configured towards *Perception-Free* to increase the minimum image quality the system will reduce to under any condition. This effect will only be noticed in limited-bandwidth cases; if bandwidth is not constrained the system will always maintain perception-free quality. The *Minimum Image Quality* feature does not alter the overall bandwidth requirements of the user.

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

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

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

4.3.3 Configuring the Host Bandwidth Limit to 0 Mbps (No Limit)

In Section 4.3.1, the bandwidth was limited to 25 Mbps with a bandwidth target of 20 Mbps. In this section, the PCoIP protocol default bandwidth and imaging settings are used to take advantage of the usage characteristics of the group. (The characteristics in this example are similar to many actual usage groups.) Here the *Device Bandwidth Limit* and *Device Bandwidth Target* are configured to 0 (no limit) to allow more effective bandwidth sharing. The firmware alleviates bandwidth congestion by implementing a

bandwidth adaptation algorithm that strives for fairness on shared networks. The firmware will use the bandwidth as determined by the Ethernet physical-layer device.

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

Open the host admin interface for the first user’s host by using an Internet browser to open the host IP address

1. Log in to the host admin interface (using password if enabled)
2. Select the *Bandwidth* webpage from the *Configuration* menu

Figure 4-22: Host Bandwidth Limit Configuration (0 Mbps, no limit)

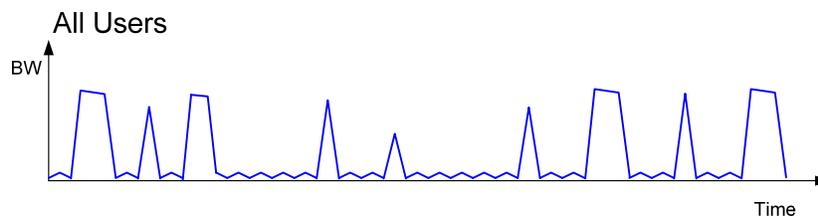
3. Enter 0 in the *Device Bandwidth Limited* field to enable no limit
4. Enter 0 in the *Device Bandwidth Target* field to enable no limit
5. Select the *Apply* button to accept the changes
6. Repeat for the other three users’ hosts

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

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

Figure 4-23 shows the total simplified bandwidth usage with no limit for the four users in this example. This figure shows that the bandwidth is more efficiently shared, compared to the case of setting a low maximum bandwidth limit as in Figure 4-20. In the unlimited case, each PColP session has the opportunity to use up to 100 Mbps. This provides the user with a more perception-free experience.

Figure 4-23: Simplified User Bandwidth Requirements (no limit)



4.4 USB Permissions Example

This example illustrates the use of the USB Permissions webpage. It shows how an administrator 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.

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

Warning: As the host is the master for USB permissions, the USB permissions are applied with different priorities on the host vs. client. Depending on the deployment, hardware PColP host vs. software PColP host, configuring the client USB permissions may or may not have advantages. Refer to Section 1.7.1 for more information on USB permission priorities.

4.4.1 Authorizing USB Device By Class

1. In the Authorization section, select *Add new* button

Figure 4-24: USB Permissions Example: Add new Button



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

Figure 4-25: USB Permissions Example: Selecting the Class Entry Type

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	Remove
------------------------	---------------	--------------	--------

Add new: Class

Device Class: Class

Sub Class: * Any

Protocol: * Any

Add Cancel

Unauthorized Devices: Table is empty

Add new

Apply Cancel

3. Select *Printer* from the *Device Class* drop-down menu to authorize a class of printers

Figure 4-26: USB Permissions Example: Selecting the Device Class

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	Remove
------------------------	---------------	--------------	--------

Add new: Class

Device Class: Printer

Sub Class: * Any

Protocol: * Any

Add Cancel

Unauthorized Devices: Table is empty

Add new

Apply Cancel

4. 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*)

Figure 4-27: USB Permissions Example: Selecting the Sub Class

The screenshot shows the 'USB' configuration page. At the top, it says 'Configure the USB permissions table' and 'The USB permissions table has been modified. Click 'Apply' to save your changes'. Under 'Authorized Devices', there is a table with columns: 'Human Interface Device', 'Any Sub Class', and 'Any Protocol'. A 'Remove' button is to the right. Below this, the 'Add new:' section has a 'Class' dropdown set to 'Printer'. The 'Device Class' is '07'. The 'Sub Class' dropdown is open, showing 'Any' selected. The 'Protocol' dropdown is also open, showing 'Printer' selected. There are 'Add' and 'Cancel' buttons below the dropdowns. At the bottom, there is an 'Add new' button for 'Unauthorized Devices' and 'Apply' and 'Cancel' buttons.

5. Select the desired IEEE 1284.4-compatible bidirectional protocol from the *Protocol* drop-down menu

Figure 4-28: USB Permissions Example: Selecting the Protocol

This screenshot is similar to Figure 4-27, but the 'Protocol' dropdown menu is open. The menu items are: 'Any', 'Reserved/Undefined', 'Unidirectional', 'Bidirectional', 'IEEE 1284.4 compatible bidirectional', and 'Vendor Specific'. The 'IEEE 1284.4 compatible bidirectional' option is highlighted. The 'Sub Class' dropdown is now set to 'Printer'. The 'Add' and 'Cancel' buttons are still visible below the dropdowns.

6. Select *Apply* to save the changes to flash and complete the configuration

Figure 4-29: USB Permissions Example: Class Authorization

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"/>

Unauthorized Devices: *Table is empty*

4.4.2 Authorizing USB Device By Vendor/Product ID

1. In the Authorization section, select the *Add new* button

Figure 4-30: USB Permissions Example: Add new Button

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"/>

Unauthorized Devices: *Table is empty*

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

Figure 4-31: USB Permissions Example: Selecting the Class Entry Type

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:

Device Class:

Sub Class: *

Protocol: *

Unauthorized Devices: *Table is empty*

3. Enter the USB device *Vendor ID* and *Product ID* into the corresponding fields

Figure 4-32: USB Permissions Example: Entering Vendor ID and Product ID

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:

Vendor ID:

Product ID:

Unauthorized Devices: *Table is empty*

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

Figure 4-33: USB Permissions Example: Vendor ID and Product ID Authorization

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	Remove
Printer	Printer	IEEE 1284.4 compatible bidirectional	Remove
VID: 1234; PID: abcd			Remove

Unauthorized Devices: *Table is empty*

5 Appendix B: Client Language and Keyboard Support

The client firmware can support various languages and keyboard layouts.

Information concerning configuring the language and keyboard layout can be found in Section 1.6.11 Language for the web interface and Section 2.3.7 Language for the OSD. Table 5-1 lists supported languages and Table 5-2 lists supported keyboards layouts (defaults are noted).

Table 5-1: Languages Supported by the Client

Supported Languages	English [default]
	French
	German
	Greek
	Spanish
	Italian
	Portuguese
	Korean
	Japanese
	Traditional Chinese
	Simplified Chinese

Table 5-2: Keyboard Layouts Supported by the Client

Supported Keyboards	Belgian ISO-8859-1
	Belgian ISO-8859-1 (accent keys)
	Danish Codepage 865
	Danish ISO-8859-1
	Danish ISO-8859-1 (accent keys)
	Dutch ISO-8859-1 (accent keys)
	Finnish Codepage 850
	Finnish ISO-8859-1
	Finnish ISO-8859-1 (accent keys)
	French Canadian ISO-8859-1 (accent keys)
	French ISO-8859-1
	French ISO-8859-1 (accent keys)

French Dvorak-like
French Dvorak-like (accent keys)
German ISO-8859-1
German ISO-8859-1 (accent keys)
German Codepage 850
Greek ISO-8859-7 (104)
Japanese 106
Japanese 106x
Korean Dubeolsik ISO-8859-1
Latin American
Latin American (accent keys)
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)
Italian ISO-8859-1
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 ISO-8859-1
Swiss-French ISO-8859-1 (accent keys)
Swiss-French Codepage 850
Swiss-German ISO-8859-1
Swiss-German ISO-8859-1 (accent keys)
Swiss-German Codepage 850
Turkish Q ISO-8859-1

	Turkish Q ISO-8859-1 (accent keys)
	United Kingdom ISO-8859-1
	United Kingdom ISO-8859-1 (ctrl and caps swapped)
	United Kingdom Codepage 850
	United Kingdom Codepage 850 (ctrl and caps swapped)
	United States of America Emacs optimized layout
	United States of America ISO-8859-1 [default]
	United States of America ISO-8859-1 (accent keys)
	United States of America ISO-8859-1 (ctrl and caps swapped)
	United States of America dvorak
	United States of America dvorakx
	United States of America left-hand dvorak
	United States of America right-hand dvorak United States of America dvorakx
	United States of America Emacs optimized layout
	United States of America Traditional Unix Workstation

6 Appendix C: Client RDP Compatibility

The PCoIP firmware also supports a Remote Desktop Protocol client. This can be enabled for a lower than PCoIP protocol experience. Table 6-1 below outlines the RDP client capability.

Table 6-1: RDP Capabilities

RDP Protocol	Version 5.2
Supported Terminal Servers	Windows XP, Vista, Server 2003, Server 2008, Linux XRDP
Display Resolution (single monitor)	800x600, 1024x768, 1280x768, 1280x1024, 1440x900, 1600x1200, 1680x1050, 1920x1200,
Color Depth	8, 16, 24 bits per pixel
RDP Port	Configurable (default 3389)
Audio	Two output channels (16 bit at 22.05 KHz)
Experience Options	Desktop Wallpaper enable/disable (via web/OSD & Connection broker) Display Window content while dragging (only via connection broker) Menu and window animation enable/disable (only via connection broker) Themes enable/disable (via web/OSD & Connection Broker) Bitmap caching is supported
Port Redirection	Port redirection not supported Clipboard redirection not supported
Logon	Connection broker can pass user ID and password to bypass the Windows logon screen when opening a session
Encryption (Windows Server 2003, Server 2008)	Security Layer: - RDP Security Layer => supported - Negotiate => supported Encryption Levels: - Low => supported - Client Compatible => supported - High => supported - FIPS Compliant => not supported
Network Level Authentication (Vista)	Not supported