Release Notes

Wyse® P Class PCoIP® Firmware

Release 4.x

Products: P20, P25, P45

Issue: 100913 Rev. F
General Release

Copyright Notices

Trademarks

About this Guide

This guide is intended for administrators of Wyse P class zero clients. This document is updated periodically as more information becomes available.

Finding the Information You Need in this Guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

Wyse Technical Support

To access Wyse technical resources, visit http://www.wyse.com/support. If you still have questions, you can submit your questions using the Wyse Self-Service Center at http://support.wyse.com/selfservice.html or call Customer Support at 1-800-800-WYSE (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access international support, visit http://www.wyse.com/global.

Wyse Online Community

Wyse maintains an online community where users of our products can seek and exchange information on user forums. Visit the Wyse Online Community forums at: http://community.wyse.com/forum.

Contents

1 Introduction

Purpose

This document contains new feature information for Tera1 and Tera2. A brief summary describes the feature additions and issues resolved in each firmware release going back to release 4.0. The sections in this document are organized according to release date with the most recent releases listed first.

IMPORTANT: Wyse has leveraged Teradici release notes with permission by Teradici for the creation of release notes for Wyse P class zero clients (P20, P25, and P45). Any reference to *Host Cards* is not applicable to the Wyse P20, P25, or P45 zero client products.

Definitions

CAC	Common Access Card (smart card technology used in the U.S. Department of Defense)
CMI	Connection Management Interface - Interface provided by the zero client or host, used to communicate with an external connection management server
CMS	Connection Management Server (also referred to as Connection Broker)
EDID	Extended Display Identification Data - Information provided by a monitor that describes the capabilities of the monitor. This information is typically used by the graphics card in the host computer.
FW	Firmware
GSC-IS	Government Smart Card Interoperability Specification
HPDET	Hot Plug Detect - HDMI signal used to sense when a display is plugged in or unplugged
OCSP	Online Certificate Status Protocol - protocol used to determine the status of an X.509 digital certificate (defined in RFC 2560).
OID	Object identifier - a numerical value used to identify objects in a certificate.
OS	Operating System
OSD	On Screen Display on the PCoIP zero client
OTP	One-Time Password - security system that requires a new password every time a user is authenticated

PCoIP®	Personal Computer over Internet Protocol (PC-over-IP®)
PCoIP Host	Host side of PCoIP system
PCoIP MC	PCoIP Management Console - Tool provided by Teradici that gives IT personnel the ability to access and to manage all PCoIP Hosts and zero clients from a single location in a deployment
PCoIP Zero Client	User or client side of PCoIP system in the form of a standalone desktop device or integrated display based on a PCoIP processor
PIV	Personal Identity Verification
SCEP	Simple Certificate Enrollment Protocol - Protocol which supports issuing and revoking digital certificates
SSO	Single Sign-On - Authentication process that lets a user enter one username and password and grants access to multiple applications
Software Client	VMware View™ software application that can establish a PCoIP session with a PCoIP Host
Tera1 product	Wyse P20
Tera2 product	Wyse P25, Wyse P45
URI	Uniform Resource Identifier
USB	Universal Serial Bus
VCS	View Connection Server
WDM	Dell Wyse Device Manager software

2 Release 4.1.2 (Tera1/Tera2)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.1.2 versus release 4.1.0.

Compatibility Notes

Workstation and VDI

Deployments using the PCoIP Management Console (MC) to manage Tera2 PCoIP endpoints must use PCoIP MC version 1.8.1 or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage Tera1 PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

Note: This Tera1 firmware release can only be installed on Tera1 PCoIP processors running firmware release 1.4 or later. If the processor is loaded with a firmware release prior to version 1.4, first download one or more intermediate firmware releases. The following table lists the installation steps for each version of firmware that may be installed on a PCoIP processor. To view the firmware version, go to the device **Info > Version** web page.

Installed Firmware Version	Upgrade process
0.1 through 0.17	**1.** Install firmware release 0.18. **2.** Install a 1.x firmware release (1.4 or greater). **3.** Install the new firmware (4.1.2).
0.18 through 1.3	**1.** Install a 1.x firmware release (1.4 or greater). **2.** Install the new firmware (4.1.2).
1.4 through 4.1.1	Install the new firmware (4.1.2).

VDI Specific

This PCoIP firmware is compatible with the release of VMware Horizon View that was generally available when this firmware was released. It is also compatible with one major release of Horizon View prior to this. Other versions of Horizon View may also be compatible, but will need to be verified in your specific deployment environment.

The version of Horizon View available at the time of this firmware release was Horizon View 5.2.

VMware View 5.0 or later deployments using zero client devices to connect to View virtual desktops should install release 4.1.2 on the zero client devices.

Local image caching is supported in Tera2 zero clients when deployed with VMware Horizon View 5.2 or later. This enables considerable bandwidth savings when accessing image intensive content.

Workstation Specific

It is highly recommended that remote workstation deployments using zero clients with PCoIP host cards install release 4.1.2 on *both* the host card and zero client devices. While mixed firmware release operation is not tested, firmware release 4.1.2 is compatible with 4.1.1, 4.1.0, 4.0.x, 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.1.x is not interoperable with releases 3.0, 2.x, 1.x or 0.x. An **"Unable to connect (0x1002). Please contact your IT administrator."** error message appears on the display if trying to connect to a PCoIP host card running an incompatible release.

Deployments using Dell Wyse Device Manager (WDM) to manage PCoIP endpoints must use WDM 4.9.1 HF or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

New Features

Workstation and VDI

Display Suspend (for Tera2 zero clients): When users are in-session, the firmware now supports a display suspend feature after a specified keyboard and mouse inactivity timeout. *See Figure 1.*

VDI Specific

Changed the **Auto Connect** feature from a checkbox to a dropdown menu with the following options:

- **Disabled**: The client does not automatically connect to the configured View Connection Server or PCoIP Connection Manager. Disabled is equivalent to the previous "unchecked" setting.
- **Enabled**: The client attempts to connect to the configured View Connection Server or PCoIP Connection Manager. Enabled is equivalent to the previous "checked" setting.
- **Enabled with Retry on Error**: The client attempts to connect to the configured View Connection Server or PCoIP Connection Manager. If a connection error occurs, the client will wait and retry the connection periodically until a connection is successful, or the Cancel button is pressed.

The **Auto Connect** feature is an advanced option supported by the following **Session Connection Types** *(see Figure 2)*:

- **PCoIP Connection Manager** (Tera2 zero clients)
- **PCoIP Connection Manager + Auto-Logon** (Tera2 zero clients)
- **View Connection Server** (Tera1 and Tera2 zero clients)
- **View Connection Server + Auto-Logon** (Tera1 and Tera2 zero clients)

Continuous Desktop Retry (for Ter1 and Tera2 zero clients): After user authentication and desktop selection, if the View Connection Server or PCoIP Connection Manager reports that the selected desktop is not available, the client will retry connecting to that desktop every 5 seconds until the desktop becomes available, or the Cancel button is pressed.

Workstation Specific

None

Fixes

Workstation and VDI

None

VDI Specific

Out of range certificate expiry dates will be capped at the year 2225 (for Tera1 and Tera2 zero clients).

PIN verification failure with CardOS smart cards has been resolved (for Tera2 zero clients).

Workstation Specific

None

Known Issues

- See*Table 1 and Table 2* for the operating mode of USB devices connected to a zero client based on device type, session type, and device configuration.
- Audio gets distorted with live Webcam session. **Note**: Teradici supports one *isochronous* device per connection. [15134-9931]
- Incorrect Peer MAC Address on “Session Control Page. [15134-9748]
- Wyse Case 279334 - VMware Horizon View Client screen corrupted when moved to the left side. [15134-12998]
- Teradici combined Tera1 and Tera2 image DDC upgrade support on WDM. [TIR67646]
- P45 with SFP Ethernet Adapter Does Not Wake On LAN. [TIR74266]
- P45 with SFP Ethernet Adapter Does Not Shut Down from WDM. [TIR74267]

Additional Collateral

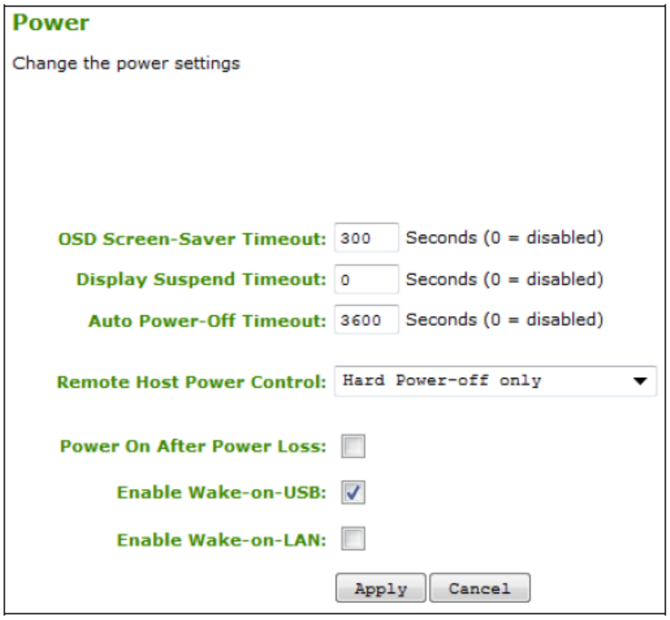
Additional Collateral	**Zero Client used with:**	
	VMware View	**Host card**
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	

Additional Collateral	Zero Client used with:	
	VMware View	Host card
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager™ (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

Supplemental Information

Configuration > Power Web Page

Figure 1 Configuration > Power Web Page



Power

Change the power settings

OSD Screen-Saver Timeout: 300 Seconds (0 = disabled)

Display Suspend Timeout: 0 Seconds (0 = disabled)

Auto Power-Off Timeout: 3600 Seconds (0 = disabled)

Remote Host Power Control: Hard Power-off only

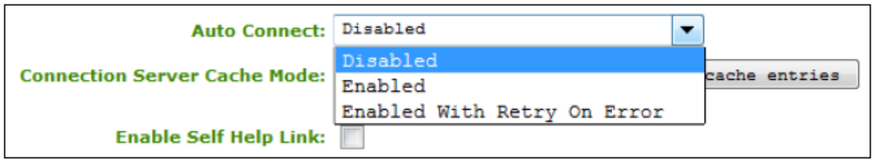
Power On After Power Loss: □

Enable Wake-on-USB: ☑

Enable Wake-on-LAN: □

VDI Auto Connect Options

Figure 2 VDI Auto Connect Options



Auto Connect: Disabled

Connection Server Cache Mode:

Enable Self Help Link: □

3 Release 4.1.0 (Tera1/Tera2)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.1.0.

Compatibility Notes

Workstation and VDI

Deployments using the PCoIP Management Console (MC) to manage Tera2 PCoIP endpoints must use PCoIP MC version 1.8.1 or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage Tera1 PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

Note: This firmware release can only be installed on Tera1 PCoIP processors running firmware release 1.4 or later. If the processor is loaded with a firmware release prior to version 1.4, first download one or more intermediate firmware releases. The following table lists the installation steps for each version of firmware that may be installed on a PCoIP processor. To view the firmware version, go to the device **Info > Version** web page.

Installed Firmware Version	Upgrade process
0.1 through 0.17	**1.** Install firmware release 0.18. **2.** Install a 1.x firmware release (1.4 or greater). **3.** Install the new firmware (4.0.0).
0.18 through 1.3	**1.** Install a 1.x firmware release (1.4 or greater). **2.** Install the new firmware (4.1.0).
1.4 through 4.0.x	Install the new firmware (4.1.0).

VDI Specific

VMware View 5.0 or later deployments using zero client devices to connect to View virtual desktops should install release 4.1.0 on the zero client devices.

Local image caching is supported in Tera2 zero clients when deployed with VMware Horizon View 5.2 or later. This enables considerable bandwidth savings when accessing image intensive content.

Workstation Specific

It is highly recommended that remote workstation deployments using zero clients with PCoIP host cards install release 4.1.0 on *both* the host card and zero client devices. While mixed firmware release operation is not tested, firmware release 4.1.0 is compatible with 4.0.3, 4.0.2, 4.0.1, 4.0.0, 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.1.0 is not interoperable with releases 3.0, 2.x, 1.x or 0.x. An **“Unable to connect (0x1002). Please contact your IT administrator.”** error message appears on the display if trying to connect to a PCoIP host card running an incompatible release.

Deployments using Dell Wyse Device Manager (WDM) to manage PCoIP endpoints must use WDM 4.9.1 HF or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

New Features

Workstation and VDI

Security features (for Tera1 and Tera2 endpoints):

- Following three failed attempts to access the Administrative Web Interface or the On Screen Display, each subsequent failed attempt will require additional time to complete.
- Added option to force the changing of the administrative password upon the nest access of the Administrative Web Interface or On-Screen-Display (selected password may be blank). *See Figures 1 and 2.*
- Logging of failed access attempts to the Administrative Web Interface, On Screen Display, or management interface (for example, PCoIP Management Console).
- Added options to disable the Administrative Web Interface and/or the management tool interface (for example, Tera1 and Tera2 endpoints can lock out access by the PCoIP Management Console). *See Figures 1 and 2.*

Added support for SCEP (Simple Certificate Enrollment Protocol): zero clients may be configured to submit a request for a certificate to a SCEP server (for Tera2 zero clients). *See Figures 3 and 4*.

Added Auto-Power-Off option, which powers off PCoIP zero clients after a configurable period of idle time when users are out of session (for Tera2 zero clients). The zero client **Permissions >Power** and **Configuration >OSD** web pages have been replaced by the **Configuration >Power** web page. *See Figure 5.*

Added option to configure PCoIP zero clients such that an image on a primary display can be reproduced on the secondary video port (for dual-display Tera2 zero clients). *See Figure 6.* **Note**: The resolution setting of the primary display will also be applied on the secondary display when this feature is enabled.

Added support for Brazilian ABNT2 keyboards (for Tera1 and Tera2 zero clients).

Added two new **Session Connection Types** (PCoIP Connection Manager and PCoIP Connection Manager + Auto-Logon) for Tera2 zero clients. The PCoIP Connection Manager can be used in the future to broker PCoIP sessions for Teradici solutions such as Arch Published Desktops. *See Figures 7 through 12.*

VDI Specific

Added support for SafeNet SC650 smart cards with SafeNet PKI applet and SHAC middleware (for Tera2 zero clients).

Added support for Atos CardOS smart cards (for Tera2 zero clients).

Added support for eToken 72k Pro USB user authentication devices (for Tera2 zero clients).

Added support for isochronous USB devices without a Video class interface connected behind a USB 2.0 hub. **Note**: A webcam is an example of an isochronous USB device with a Video class interface (for Tera2 zero clients).

Workstation Specific

Added support for local termination of keyboards and mice behind USB hubs provided all devices attached to the USB hub are HID keyboards and mice.

Added ability to configure the **Wake Host from Low Power State**, **Host Wake MAC Address** and **Host Wake IP Address** settings for Direct to Host sessions on the advanced session configuration dialog of the On-Screen Display. Previous releases support configuring these settings through the web interface or the PCoIP MC.
See Figure 13.

Fixes

Workstation and VDI

Resolved an issue where the Display Override feature in the OSD does not function (for Tera1 and Tera2 zero clients).

Resolved an issue where Greek keyboards do not function correctly in the OSD (for Tera1 and Tera2 zero clients).

Resolved two issues where keys were not mapped correctly on a Japanese keyboard (for Tera1 and Tera2 zero clients).

Resolved an issue where syslog would disable itself when it was unable to send a syslog message to the configured server because of a network error (for Tera1 and Tera2 zero clients).

USB port numbers are referred to as “logical” references in device logs to avoid confusion with physical labeling of USB ports (for Tera1 and Tera2 zero clients).

Resolved an issue where the Japanese 106 keyboard entered an incorrect character when the user presses the right-most character key in the upper row.

Edited supported language translations in the OSD.

VDI Specific

Resolved an issue where supported smart cards may not be able to successfully complete their login process (for Tera1 and Tera2 zero clients).

Resolved an issue where IronKey USB devices do not function with PCoIP zero clients (for Tera1 and Tera2 zero clients).

Resolved an issue where the BASYS2 breadboard device does not function correctly with PCoIP zero clients (Tera1 and Tera2).

Resolved an issue where the USB certify scanner device fails to connect to a virtual machine when used with PCoIP zero clients (for Tera1 and Tera2 zero clients).

Resolved an issue where the SeaI/O USB device may not function when the PCoIP zero client power is cycled off and back on while the device is connected (for Tera1 and Tera2 zero clients).

Resolved an issue where the microphone gain was being incorrectly set (for Tera1 and Tera2 zero clients).

Resolved an issue where a CAPS lock warning message was not being displayed if a user had previously failed a login attempt due to a bad username/password (for Tera1 and Tera2 zero clients).

When Imprivata OneSign is in lockdown mode, a message indicating the reason for the failed connection is presented to the user (for Tera1 and Tera2 zero clients).

The secure session state is now included in device logs (for Tera1 and Tera2 zero clients).

Workstation Specific

Resolved an issue where the workstation host card may reset when processing a malformed audio packet (for Tera1 and Tera2 host cards).

Resolved an issue where the incorrect bandwidth limit may be selected when connecting a Tera1 client to a Tera2 workstation host card. This issue only occurs when mixing both Tera1 and Tera2 clients to the same Tera2 workstation host card.

Known Issues

The following tables describe the operating mode of USB devices based on device type, session type, and device configuration when connected to a zero client.

Table 1 Tera1 USB Device Modes (Wyse P20)

EHCI Disabled (Devices operate in USB 1.1 mode only)			
	Root Port	**Behind USB 1.1 and 2.0 Hub**	
View Desktop	All devices operate in USB 1.1 mode.		
Tera1 and Tera2 PCoIP Host Card	All devices operate in USB 1.1 mode.		
EHCI Enabled (USB 2.0 support is enabled) - Default			
	Root Port	**Behind USB 1.1 Hub**	**Behind USB 2.0 Hub**
View Desktop	All devices operate in their native mode (USB 1.1 or USB 2.0) with the exception of USB 2.0 isochronous devices (i.e., audio devices, WebCams). USB 2.0 isochronous devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All non-isochronous devices operate in their native mode (USB 1.1 or USB 2.0) Isochronous devices are not supported (a warning overlay may appear).
Tera1 and Tera2 PCoIP Host Card	All devices operate in USB 1.1 mode.		

Table 2 Tera2 USB Device Modes (Wyse P25 and Wyse P45)

EHCI Disabled (Devices operate in USB 1.1 mode only)			
	Root Port	**Behind USB 1.1 and 2.0 Hub**	
View Desktop	All devices operate in USB 1.1 mode.		
Tera1 and Tera2 PCoIP Host Card	The EHCI disable flag does not apply to the PCoIP host card. See the following section for PCoIP host card behaviour.		
EHCI Enabled (USB 2.0 support is enabled) - Default			
	Root Port	**Behind USB 1.1 Hub**	**Behind USB 2.0 Hub**
View Desktop	All devices operate in their native mode (USB 1.1 or USB 2.0) with the exception of USB 2.0 isochronous devices (i.e., audio devices, WebCams). USB 2.0 isochronous devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All non-isochronous devices operate in their native mode (USB 1.1 or USB 2.0) Isochronous devices are not supported (a warning overlay may appear).
Tera1 PCoIP Host Card	All devices operate in USB 1.1 mode.		
Tera2 PPCoIP Host Card	All devices operate in their native mode (USB 1.1 or USB 2.0) with the exception of USB 2.0 isochronous devices (i.e., audio devices, WebCams). USB 2.0 isochronous devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All non-isochronous devices operate in their native mode (USB 1.1 or USB 2.0) Isochronous devices are not supported (a warning overlay may appear).

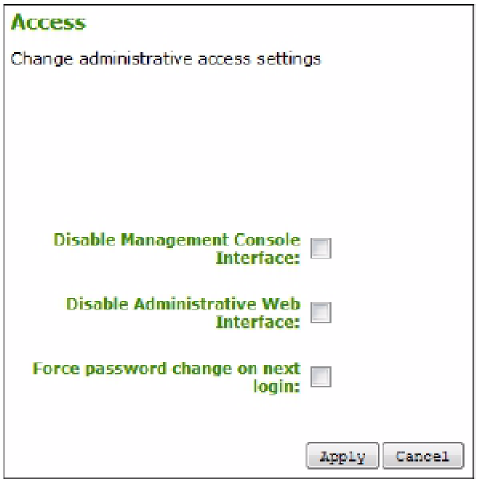
Additional Collateral

Additional Collateral	Zero Client used with:	
	VMware View	Host card
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager™ (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

Supplemental Information

Configuration > Access Web Page

Figure 1 Configuration > Access Web Page



Access

Change administrative access settings

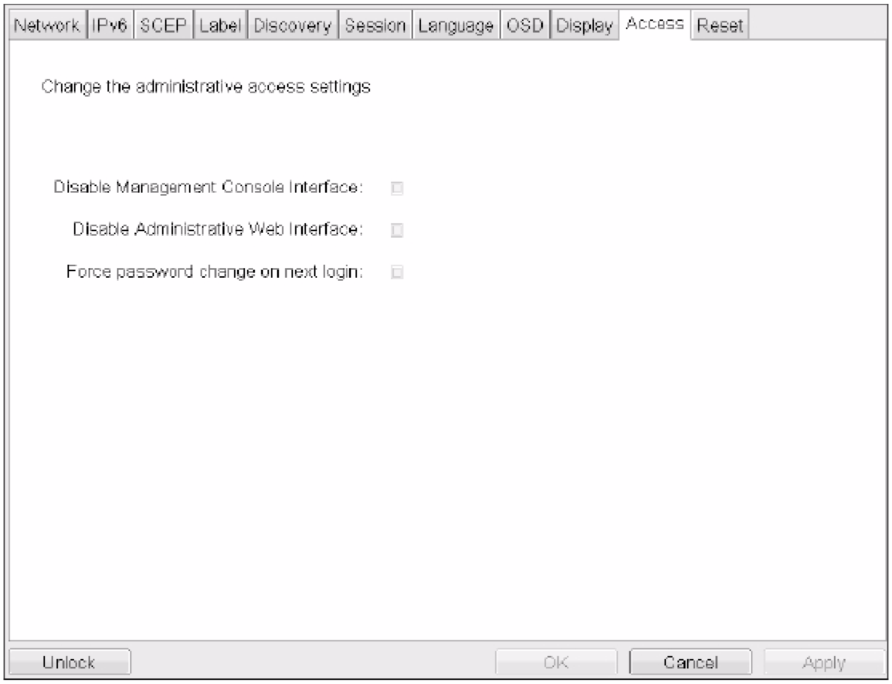
Disable Management Console Interface: □

Disable Administrative Web Interface: □

Force password change on next login: □

OSD Configuration > Access Options

Figure 2 OSD Configuration > Access Options



Change the administrative access settings

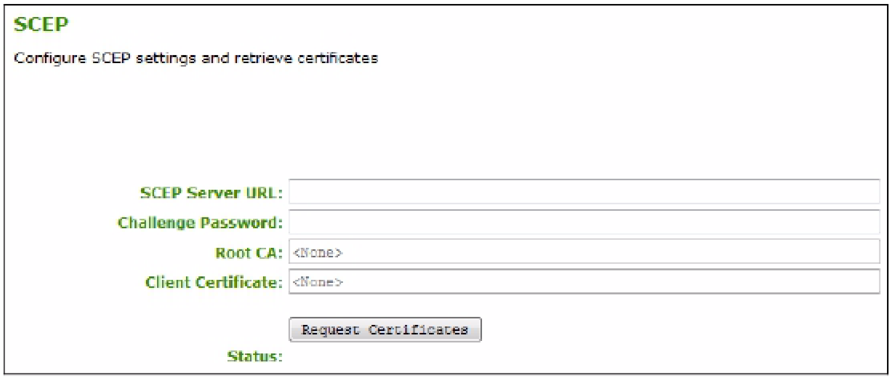
Disable Management Console Interface: □

Disable Administrative Web Interface: □

Force password change on next login: □

Configuration > SCEP Web Page (for Tera2)

Figure 3 Configuration > SCEP Web Page (for Tera2)



SCEP

Configure SCEP settings and retrieve certificates

SCEP Server URL:

Challenge Password:

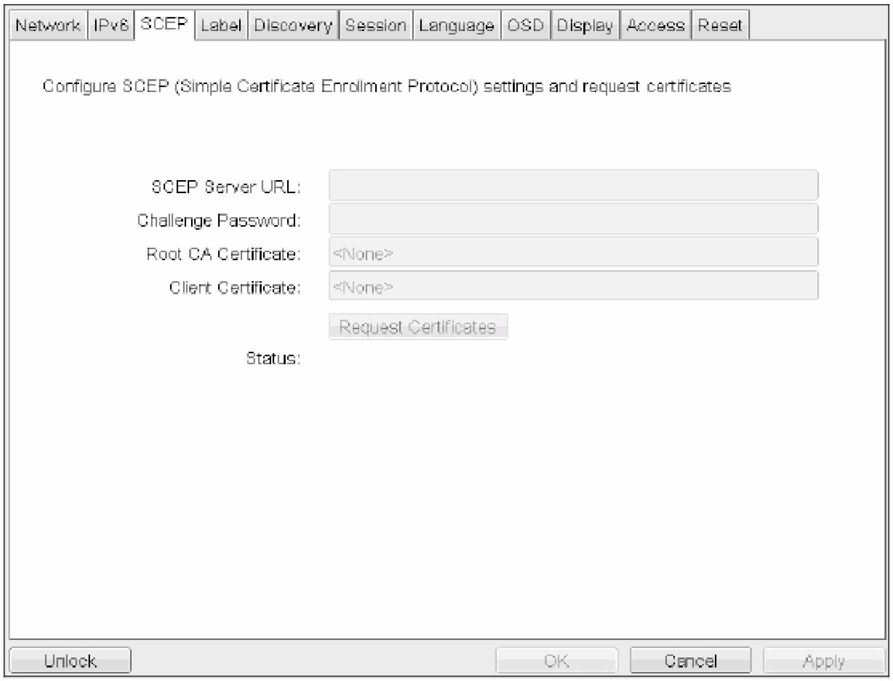
Root CA: <None>

Client Certificate: <None>

Status:

OSD Configuration > SCEP Options (for Tera2)

Figure 4 OSD Configuration > SCEP Options (for Tera2)

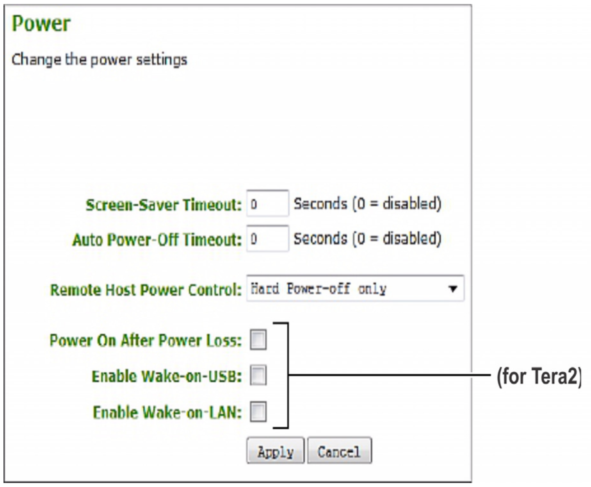


Configure SCEP (Simple Certificate Enrollment Protocol) settings and request certificates

SCEP Server URL:
Challenge Password:
Root CA Certificate: <None>
Client Certificate: <None>
Status:

Configuration > Power Web Page

Figure 5 Configuration > Power Web Page



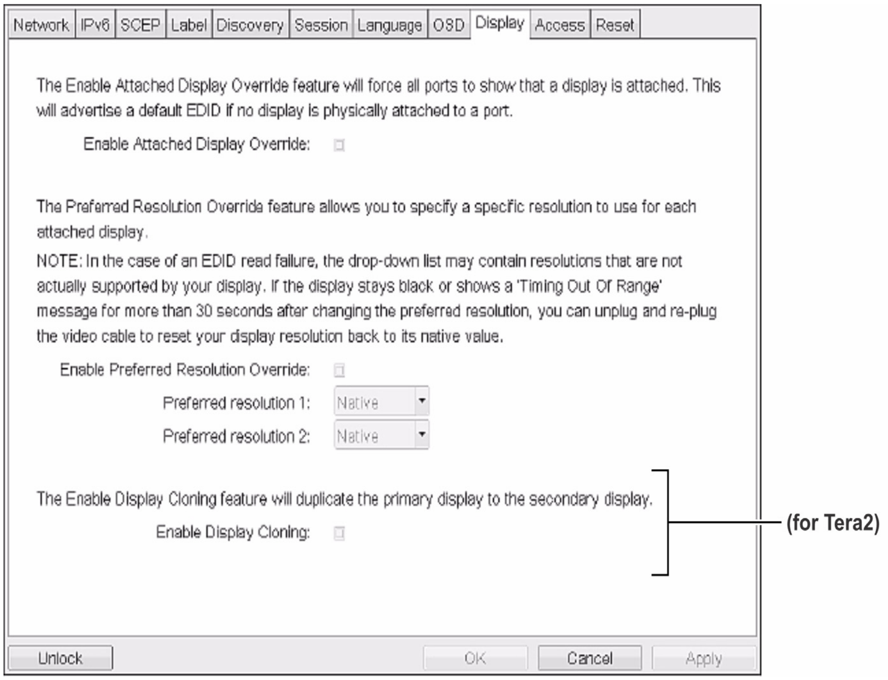
Power

Change the power settings

Screen-Saver Timeout: 0 Seconds (0 = disabled)
Auto Power-Off Timeout: 0 Seconds (0 = disabled)
Remote Host Power Control: Hard Power-off only ▼
Power On After Power Loss: □
Enable Wake-on-USB: □
Enable Wake-on-LAN: □

OSD Configuration > Display Options

Figure 6 OSD Configuration > Display Options



The Enable Attached Display Override feature will force all ports to show that a display is attached. This will advertise a default EDID if no display is physically attached to a port.

Enable Attached Display Override: □

The Preferred Resolution Override feature allows you to specify a specific resolution to use for each attached display.

NOTE: In the case of an EDID read failure, the drop-down list may contain resolutions that are not actually supported by your display. If the display stays black or shows a 'Timing Out Of Range' message for more than 30 seconds after changing the preferred resolution, you can unplug and re-plug the video cable to reset your display resolution back to its native value.

Enable Preferred Resolution Override: □

Preferred resolution 1: Native

Preferred resolution 2: Native

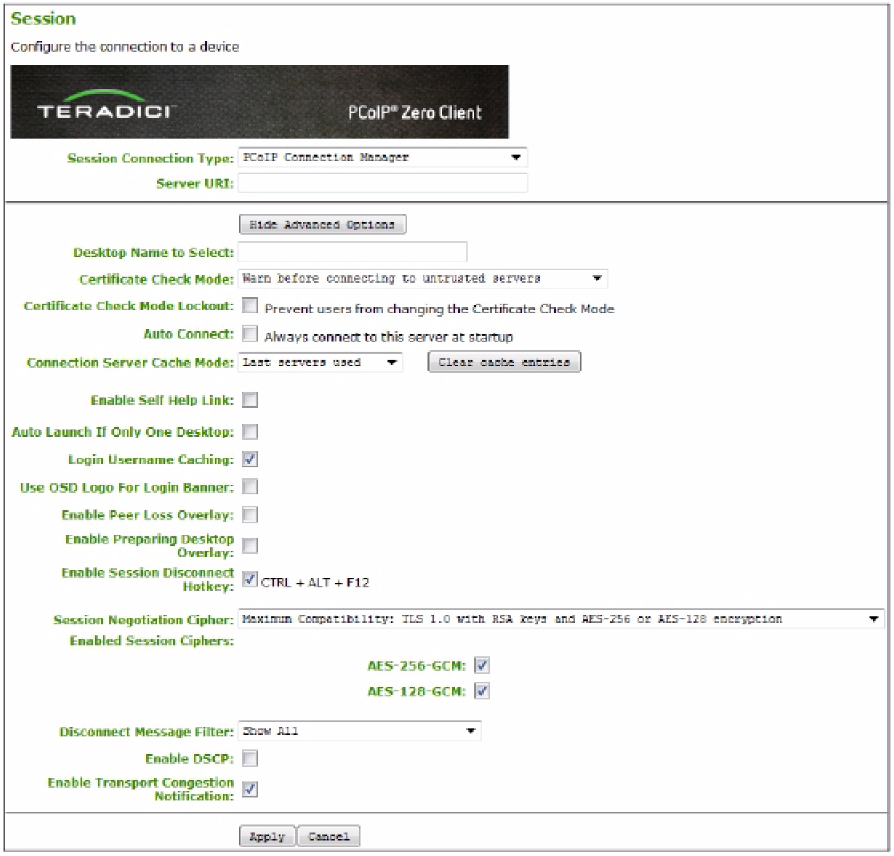
The Enable Display Cloning feature will duplicate the primary display to the secondary display.

Enable Display Cloning: □

(for Tera2)

OSD Configuration > Session PCoIP Connection Manager Web Page (forTera2)

Figure 7 OSD Configuration > Session PCoIP Connection Manager Web Page (for Tera2)



Session

Configure the connection to a device

Session Connection Type: PCoIP Connection Manager

Server URI:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers

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

Auto Connect: □ Always connect to this server at startup

Connection Server Cache Mode: Last servers used

Enable Self Help Link: □

Auto Launch If Only One Desktop: □

Login Username Caching: ☑

Use OSD Logo For Login Banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: ☑ CTRL + ALT + F12

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

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

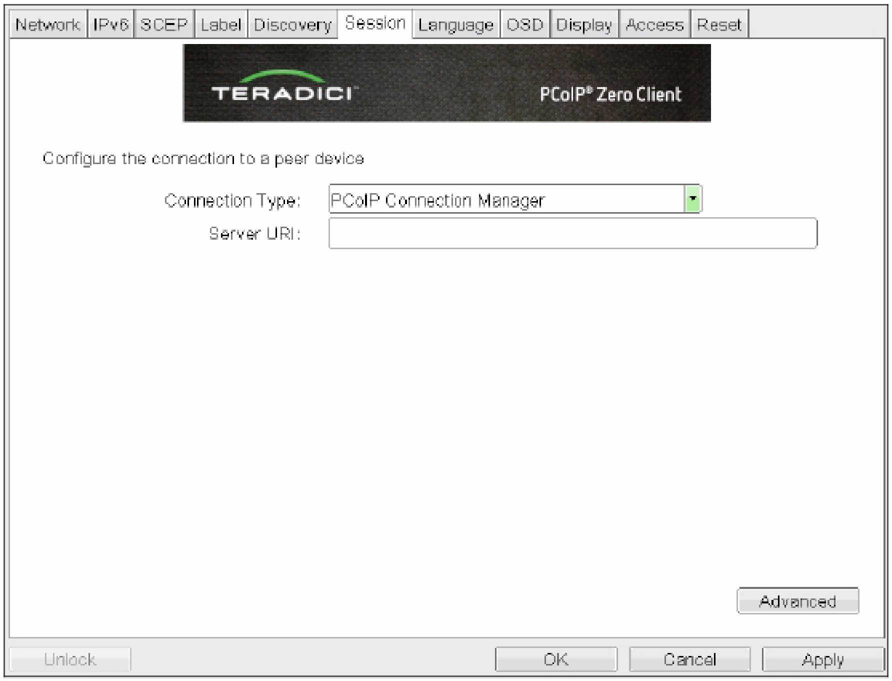
Disconnect Message Filter: Show All

Enable DSCP: □

Enable Transport Congestion Notification: ☑

OSD Configuration > Session PCoIP Conn Mgr Options (for Tera2)

Figure 8 OSD Configuration > Session PCoIP Conn Mgr Options (for Tera2)



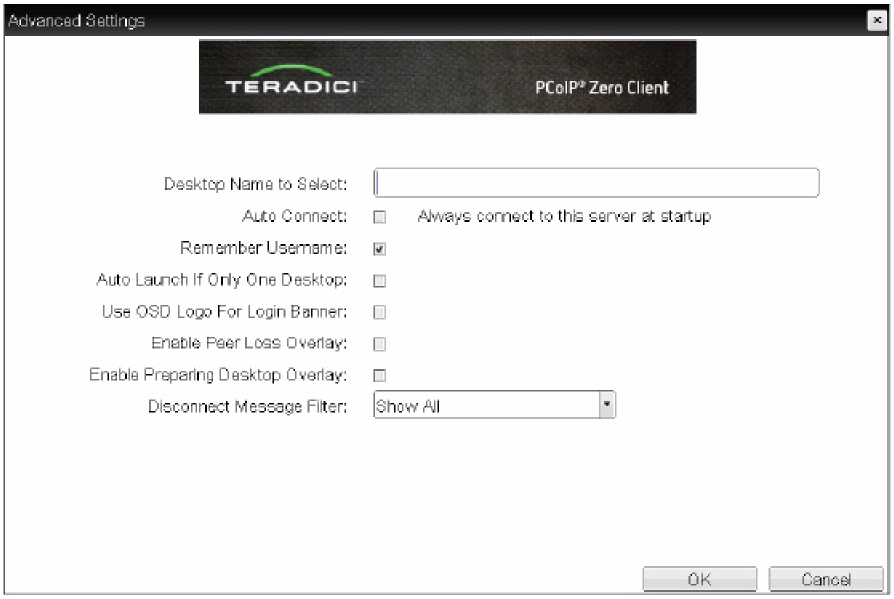
Configure the connection to a peer device

Connection Type: PCoIP Connection Manager

Server URI:

OSD Configuration > Session PCoIP Conn Mgr Advanced Options (for Tera2)

Figure 9 OSD Configuration > Session PCoIP Conn Mgr Advanced Options (for Tera2)



Desktop Name to Select:

Auto Connect: □ Always connect to this server at startup

Remember Username: ☑

Auto Launch If Only One Desktop: □

Use OSD Logo For Login Banner: □

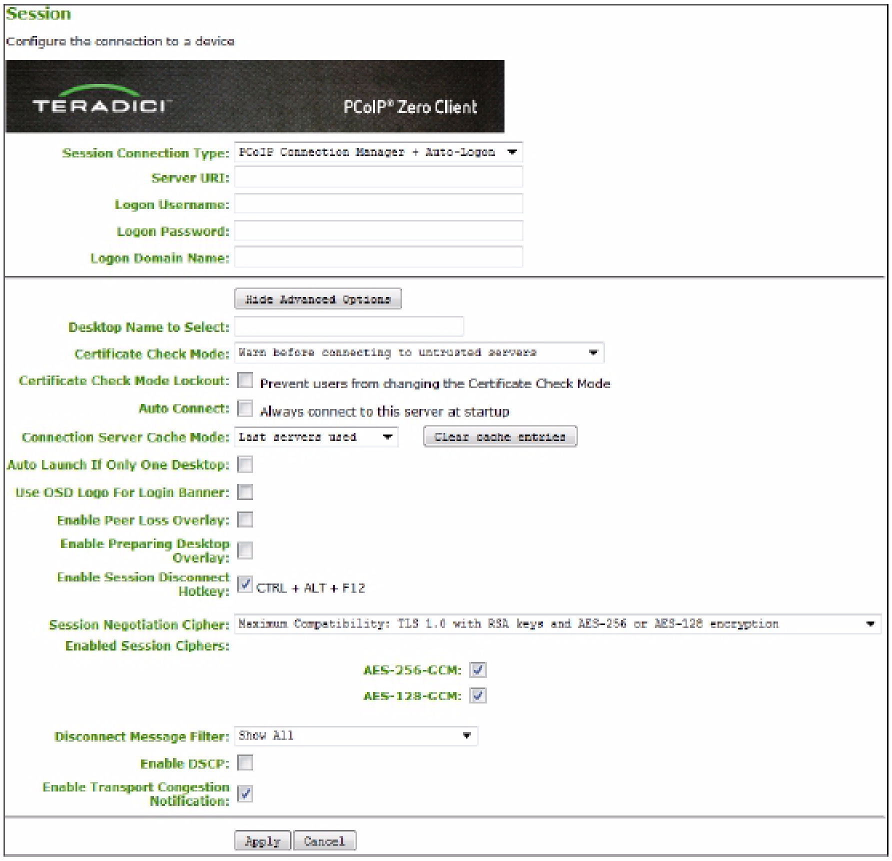
Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

Configuration > Session PCoIP Conn Mgr + Logon Web Page (for Tera2)

Figure 10 Configuration > Session PCoIP Conn Mgr + Logon Web Page (for Tera2)



Session

Configure the connection to a device

Session Connection Type: PCoIP Connection Manager + Auto-Logon

Server URI:

Logon Username:

Logon Password:

Logon Domain Name:

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers

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

Auto Connect: □ Always connect to this server at startup

Connection Server Cache Mode: Last servers used

Auto Launch If Only One Desktop: □

Use OSD Logo For Login Banner: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: ☑ CTRL + ALT + F12

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

Enabled Session Ciphers:

AES-256-GCM: ☑

AES-128-GCM: ☑

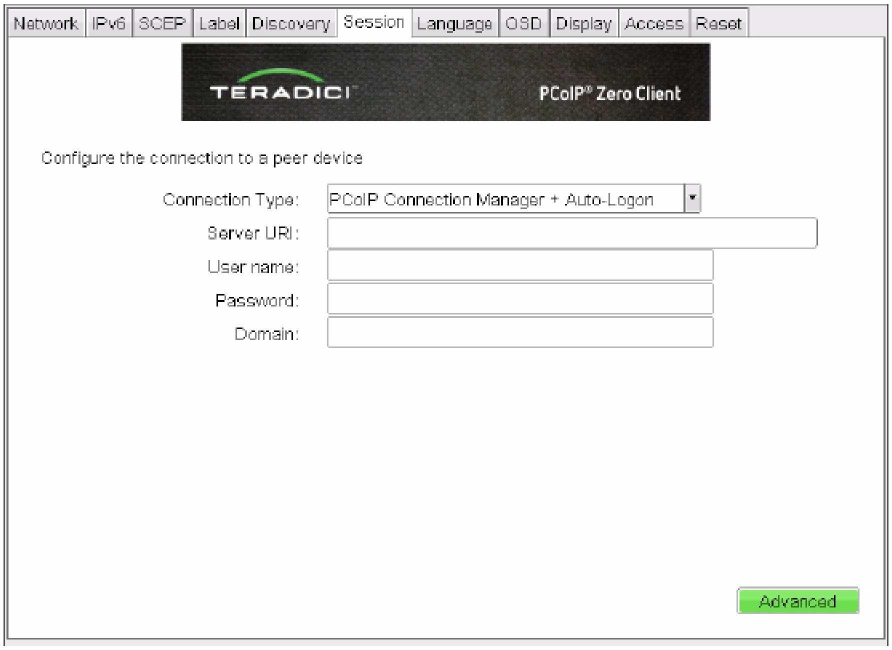
Disconnect Message Filter: Show All

Enable DSCP: □

Enable Transport Congestion Notification: ☑

OSD Configuration > Session PCoIP Conn Mgr + Logon Options (for Tera2)

Figure 11 OSD Configuration > Session PCoIP Conn Mgr + Logon Options (for Tera2)



Configure the connection to a peer device

Connection Type: PCoIP Connection Manager + Auto-Logon

Server URI:

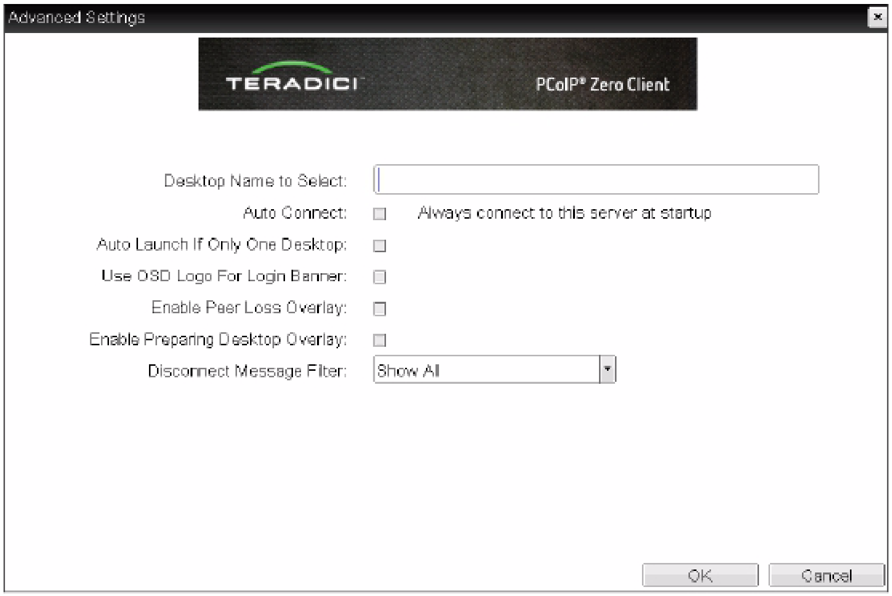
User name:

Password:

Domain:

OSD Configuration > Session PCoIP Conn Mgr + Logon Adv Options (for Tera2)

Figure 12 OSD Configuration > Session PCoIP Conn Mgr + Logon Adv Options (for Tera2)



Desktop Name to Select:

Auto Connect: □ Always connect to this server at startup

Auto Launch If Only One Desktop: □

Use OSD Logo For Login Banner: □

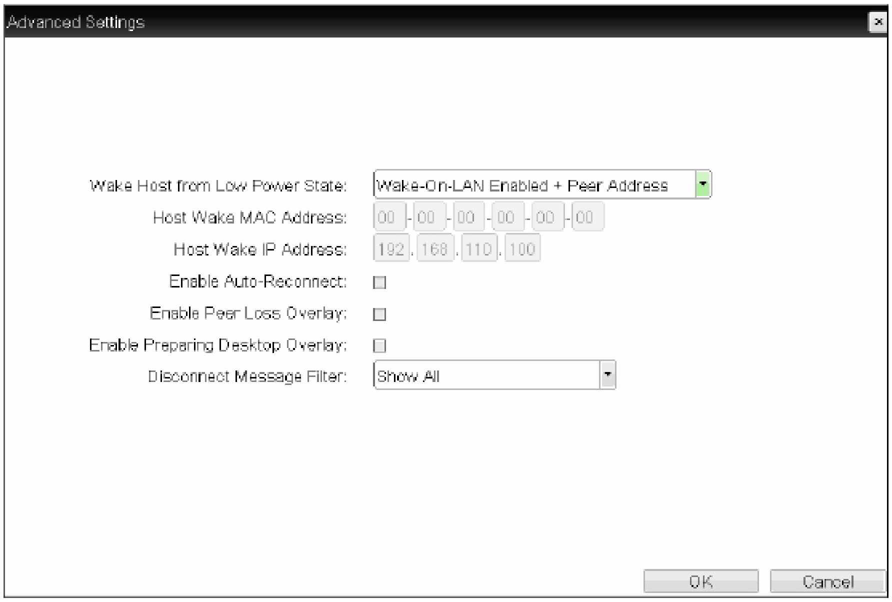
Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

OSD Configuration > Session Direct to Host Advanced Options

Figure 13 OSD Configuration > Session Direct to Host Advanced Options



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

Host Wake MAC Address: 00-00-00-00-00-00

Host Wake IP Address: 192.168.110.100

Enable Auto-Reconnect: □

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Disconnect Message Filter: Show All

This page intentionally blank.

4 Release 4.0.3 (Tera2)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.0.3 versus release 4.0.2.

NOTE: Release 4.0.3 is only applicable to Tera2 zero clients (Wyse P25 and Wyse P45) and host cards.

Compatibility

VMware View™ 5.0 or later deployments using TERA2xxx zero client devices to connect to View virtual desktops should install release 4.0.3 on the zero client devices.

It is highly recommended that remote workstation deployments using TERA2xxx zero clients with TERA2xxx PCoIP host cards install release 4.0.3 on *both* the host card and client devices. Deployments using a mix of TERA1x00 and TERA2xxx endpoints should install release 4.0.3 on TERA2xxx endpoints and release 4.0.2 on the TERA1x00 endpoints. While mixed firmware release operation, other than the previously mentioned configuration, is not tested, firmware release 4.0.3 is compatible with 4.0.2, 4.0.1, 4.0.0, 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.0.3 is not interoperable with releases 3.0, 2.x, 1.x or 0.x. An **"Unable to connect (0x1002). Please contact your IT administrator."** error message appears on the display if trying to connect to a PCoIP host card running an incompatible release.

Deployments using Dell Wyse Device Manager (WDM) to manage PCoIP endpoints must use WDM 4.9.1 HF04091034412 or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage PCoIP endpoints must use PCoIP MC version 1.8.1 or later with this firmware release.

NOTE: This firmware release can only be installed on TERA2xxx PCoIP processors.

New Features

None.

Fixes

Fixes	Zero Client used with:	
	VMware View	Host card
Resolved a flash memory issue that could cause a TERA2 device to become inoperative and unrecoverable while updating configuration settings using PCoIP MC version 1.8.0.	Tera2	Tera2
Resolved a potential memory corruption problem on TERA2xxx host cards, which could cause sessions to disconnect or workstations to crash..		Tera2
Set the minimum firmware version equal to 4.0.3 for TERA2 devices, preventing downgrades.	Tera2	Tera2
Resolved a communication error with the View Connection Server that prevented users from starting a session when Online Certificate Status Protocol (OSCP) server is unresponsive.	Tera2	
Resolved a "Source signal on other port" error on video port 2 that affected deployments using View 4.6 and Windows XP.	Tera2	

Known Issues

Known Issues	Zero Client used with:	
	VMware View	Host card
See the Knowledge Base on the Teradici support website (http://techsupport.teradici.com) for known issues.	✓	✓
Imprivata: Proximity card gives enroll error message for a configured card.	✓	
Session does not get logged off when Imprivata proximity card is tapped second time with dual monitor setup	✓	
Tera2: Webcam does not get detected under OSD attached devices	✓	
Tera2: Unit reports manufacturing date of 1/1/1900 to WDM	✓	
Tera2 P25: DVI port monitor is always set as monitor 2 under User Settings > Display Topology UI	✓	

See Table 1 and Table 2 for the operating mode of USB devices connected to a zero client based on device type, session type, and device configuration.

Additional Collateral

Additional Collateral	**Zero Client used with:**	
	VMware View	**Host card**
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager™ (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

This page intentionally blank.

5 Release 4.0.2 (Tera1/Tera2)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.0.2 versus release 4.0.1.

NOTE: The fixes and enhancements made to release 4.0.1 are also included in the 4.0.2 release.

Compatibility

VMware View™ 5.0 or later deployments using zero client devices to connect to View virtual desktops should install release 4.0.2 on the zero client devices.

It is highly recommended that remote workstation deployments using zero clients with PCoIP host cards install release 4.0.2 on *both* the host card and client devices. While mixed firmware release operation is not tested, firmware release 4.0.2 is compatible with 4.0.1, 4.0.0, 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.0.2 is not interoperable with releases 3.0, 2.x, 1.x or 0.x. An **"Unable to connect (0x1002). Please contact your IT administrator."** error message appears on the display if trying to connect to a PCoIP host card running an incompatible release.

Deployments using Dell Wyse Device Manager (WDM) to manage PCoIP endpoints must use WDM 4.9.1 hotfix (HF) or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

NOTE: Applicable to Tera1 only, this firmware release can only be installed on TERA1x00 PCoIP processors running firmware release 1.4 or later. If the processor is loaded with a firmware release prior to version 1.4, first download one or more intermediate firmware releases. The following table lists the installation steps for each version of firmware that may be installed on a PCoIP processor. To view the firmware version, go to the device **Info > Version** web page.

NOTE: Tera2 products are factory installed with firmware version 4.0.2.

Installed Firmware Version	Upgrade process for Tera1 (Wyse P20)
0.1 through 0.17	**1.** Install firmware release 0.18. **2.** Install a 1.x firmware release (1.4 or greater). **3.** Install the new firmware (4.0.2).
0.18 through 1.3	**1.** Install a 1.x firmware release (1.4 or greater). **2.** Install the new firmware (4.0.2).
1.4 through 4.0.1	Install the new firmware (4.0.2).

New Features

New Features	Zero Client used with:	
	VMware View	Host card
Added support for using the zero client in Imprivata OneSign Single Sign-On mode with the OMNIKEY 5427 proximity reader.	✓	
Added support for Wyse P25 and Wyse P45 zero clients.	✓	

Fixes

Fixes	Zero Client used with:	
	VMware View	Host card
Resolved an analog calibration issue with P25 zero clients.	✓	✓

Known Issues

Known Issues	Zero Client used with:	
	VMware View	Host card
See the Knowledge Base on the Teradici support website (http://techsupport.teradici.com) for known issues.	✓	✓
Audio gets distorted with live Webcam session. **NOTE**: Teradici supports one *isochronous* device per connection.	✓	
Incorrect Peer MAC Address on “Session Control” Page.	✓	
Display Resolution shows incorrect value under “Attached Device/ Current Resolution” field in the System Event log.	✓	
Alignment setting with dual monitors failing.	✓	
View5.1-Expired Certificate Connection failing Work In Progress 8/23/2012 3:43 PM PDT.	✓	
No connection and no feedback when Imprivata in lockdown mode.	✓	
Event Logs are not clearly depicting the secure session state.	✓	

See Table 1 and Table 2 for the operating mode of USB devices connected to a zero client based on device type, session type, and device configuration.

Additional Collateral

Additional Collateral	Zero Client used with:	
	VMware View	Host card
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager™ (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

This page intentionally blank.

6 Release 4.0.1 (not released)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.0.1 versus release 4.0.0.

IMPORTANT: Although it was not released to customers, Firmware 4.0.1 is included in this document. The 4.0.1 new features and fixes have been rolled into the Firmware Release 4.0.2.

New Features

New Features	Zero Client used with:	
	VMware View	**Host card**
Added support for using the zero client in Imprivata OneSign Single Sign-On mode with the OMNIKEY 5127 proximity reader.	✓	
Added hotkey to disconnect support (Ctrl+Alt+F12). This feature is enabled by default and is available in Workstation and View deployments. **NOTE**: Workstation deployments require that the PCoIP host software be installed with the **local cursor** feature enabled. The advanced options section of the session web page added a field to enable/disable the feature. *See Figure 1*.	✓	✓
Added pre-session support for the eToken 5205 Pro Anywhere and a eToken NG OTP.	✓	
Improved error indications in the View login flow. This change includes in-line error messages for bad username or password and a CAPS LOCK indicator.	✓	
Added support for configuring the SNMP community name. *See Figure 2.*	✓	✓
Removed network icon in the OSD and improved status indication in connect dialog.	✓	✓
Modified the View connection security text to match current View clients.	✓	
Event log is cleared when a reset to factory defaults is applied.	✓	✓
Added support for “Desktop Name to Select” configuration in “View Connection Server + Imprivata OneSign”. This field is available in the advanced options under session configuration. *See Figure 3.*	✓	

Fixes

Fixes	Zero Client used with:	
	VMware View	Host card
Zero client now trusts intermediate and leaf certificates.	✓	
Zero client does not require the View Connection Server certificate to have the Server Authentication Enhanced Key Usage if the certificate does not have any Enhanced Key Usage entries.	✓	
Certificate with RFC3280 GeneralizedTime four-digit years are now supported.	✓	
Zero client can now handle any OID appearing in a certificate's subject or issuer fields. For example, Go Daddy certificates.	✓	
Improved robustness when accessing smart card readers from applications on a virtual machine including RDP sessions.	✓	
Improved handling of certificates with Subject Alternative Name data.	✓	
Zero client now accepts certificates with a critical Certificate Policies extension.	✓	
Improved Online Certificate Status Protocol (OCSP) error handling.	✓	
Zero client no longer generates duplicate keystrokes when typing quickly. **NOTE**: For workstation deployments, this fix only applies to systems running the PCoIP host software with the **Local Cursor** feature enabled.	✓	✓
Zero client no longer loses the first character typed on bridged keyboards.	✓	
Zero client no longer asserts when connecting to a disabled View Connection Server.	✓	
Certificate store is now cleared when resetting to factory defaults through the OSD, Web, and CMI interfaces (instead of only the Web interface).	✓	✓

Known Issues

Known Issues	Zero Client used with:	
	VMware View	Host card
See the Knowledge Base on the Teradici support website (http://techsupport.teradici.com) for known issues.	✓	✓

See Table 1 and Table 2 for the operating mode of USB devices connected to a zero client based on device type, session type, and device configuration.

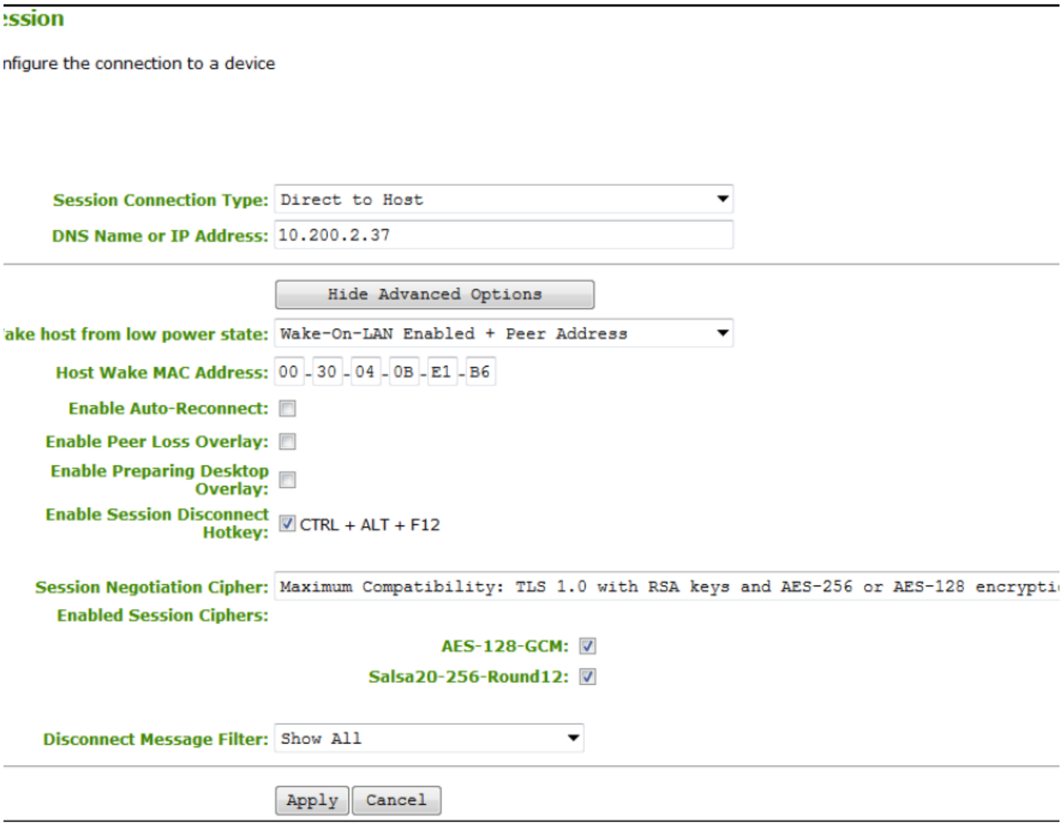
Additional Collateral

Additional Collateral	Zero Client used with:	
	VMware View	Host card
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager^{TM} (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

Supplemental Information

Configuration > Session Direct to Host Advanced Web Page

Figure 1 Configuration > Session Direct to Host Advanced Web Page



ssion

nfigure the connection to a device

Session Connection Type: Direct to Host ▾

DNS Name or IP Address: 10.200.2.37

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

Host Wake MAC Address: 00 - 30 - 04 - 0B - E1 - B6

Enable Auto-Reconnect: ☐

Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Enable Session Disconnect Hotkey: ☑ CTRL + ALT + F12

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

Enabled Session Ciphers:

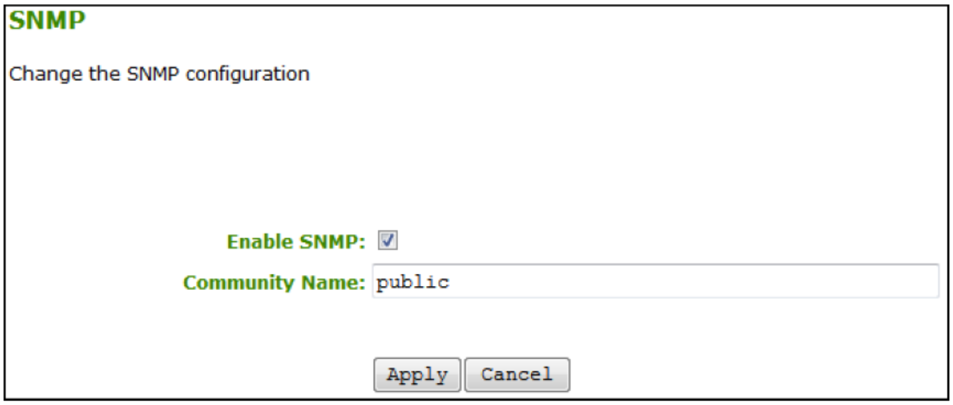
AES-128-GCM: ☑

Salsa20-256-Round12: ☑

Disconnect Message Filter: Show All ▾

Configuration > SNMP Web Page

Figure 2 Configuration > SNMP Web Page



SNMP

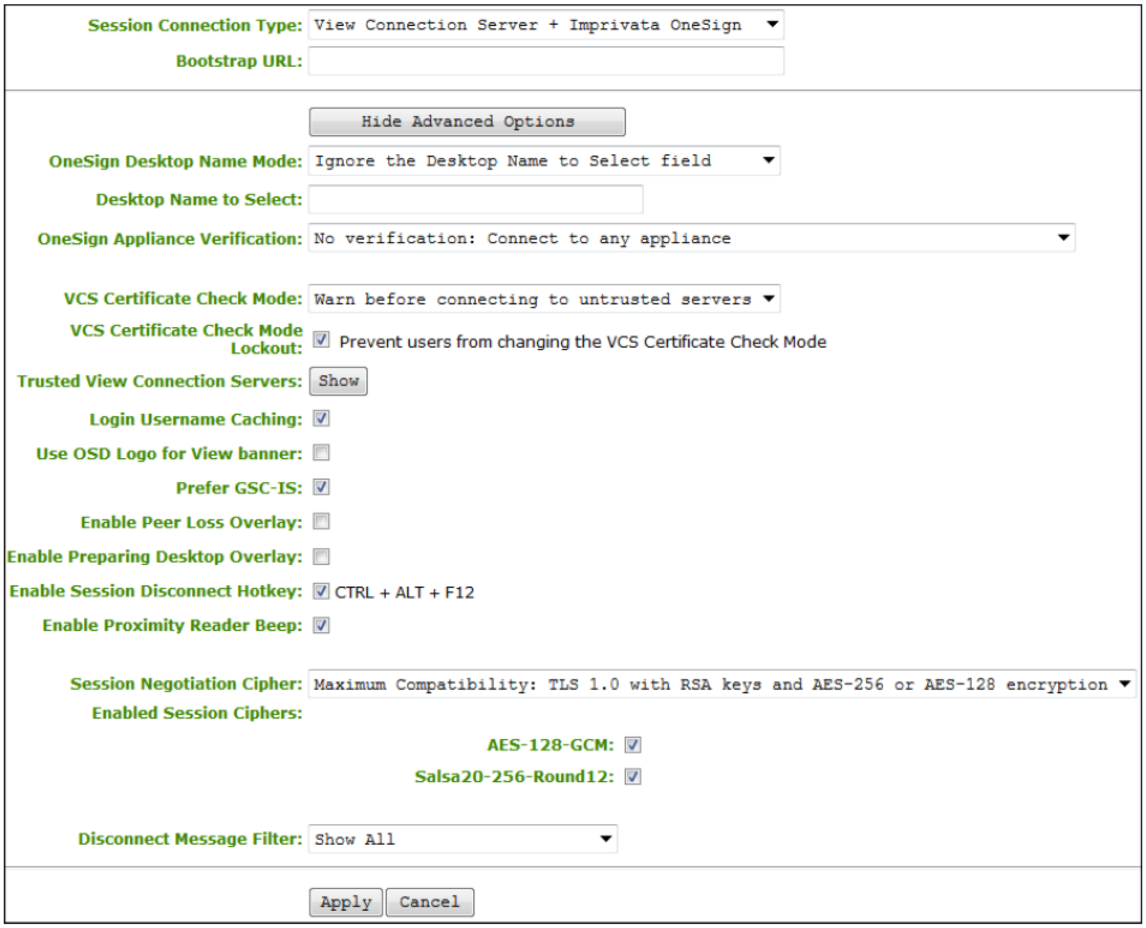
Change the SNMP configuration

Enable SNMP: ☑

Community Name: public

Configuration > Session VCS + Imprivata OneSign Advanced Web Page

Figure 3 Configuration > Session VCS + Imprivata OneSign Advanced Web Page



Session Connection Type: View Connection Server + Imprivata OneSign

Bootstrap URL:

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

Desktop Name to Select:

OneSign Appliance Verification: No verification: Connect to any appliance

VCS Certificate Check Mode: Warn before connecting to untrusted servers

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

Trusted View Connection Servers: Show

Login Username Caching: ☑

Use OSD Logo for View banner: □

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

Enable Session Disconnect Hotkey: ☑ CTRL + ALT + F12

Enable Proximity Reader Beep: ☑

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

Enabled Session Ciphers:

AES-128-GCM: ☑

Salsa20-256-Round12: ☑

Disconnect Message Filter: Show All

This page intentionally blank.

7 Release 4.0.0 (Tera1)

This chapter provides a brief summary of the feature additions and issues resolved in release 4.0.0 versus release 3.5.1.

NOTE: The 4.0.0 and prior releases are applicable to Tera1 only (Wyse P20).

Compatibility

VMware View™ 5.0 or later deployments using zero client devices to connect to View virtual desktops should install release 4.0.0 on the zero client devices.

It is highly recommended that remote workstation deployments using zero clients with PCoIP host cards install release 4.0.0 on *both* the host card and client devices. While mixed firmware release operation is not tested, firmware release 4.0.0 is compatible with 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.0.0 is not interoperable with releases 3.0, 2.x, 1.x or 0.x. An **“Unable to connect (0x1002). Please contact your IT administrator.”** error message appears on the display if trying to connect to a PCoIP host card running an incompatible release.

Deployments using Dell Wyse Device Manager (WDM) to manage PCoIP endpoints must use WDM 4.9.1 HF or later with this firmware release.

Deployments using the PCoIP Management Console (MC) to manage PCoIP endpoints must use PCoIP MC version 1.7.0 or later with this firmware release.

NOTE: This firmware release can only be installed on TERA1x00 PCoIP processors running firmware release 1.4 or later. If the processor is loaded with a firmware release prior to version 1.4, first download one or more intermediate firmware releases. The following table lists the installation steps for each version of firmware that may be installed on a PCoIP processor. To view the firmware version, go to the device **Info > Version** web page.

Installed Firmware Version	Upgrade process
0.1 through 0.17	**1.** Install firmware release 0.18. **2.** Install a 1.x firmware release (1.4 or greater). **3.** Install the new firmware (4.0.0).
0.18 through 1.3	**1.** Install a 1.x firmware release (1.4 or greater). **2.** Install the new firmware (4.0.0).
1.4 through 3.5.1	Install the new firmware (4.0.0).

New Features

New Features	Zero Client used with:	
	VMware View	Host card
Security enhancement: Add support for configuring the **VCS Certificate Check Mode** and **VCS Certificate Check Mode Lockout** settings on the **Configuration > Session** web page. *See Figures 1 and 5.* Three modes are supported. • Reject the unverifiable connection (Secure) - requires a trusted, valid certificate. • Warn if the connection may be insecure (Default) - warns when unsigned (View default), expired certificates or when the certificate is not self-signed and the zero client trust-store is empty. • Allow the unverifiable connection (Not Secure) - connects even if the connection may be compromised The **VMware View** tab on the **OSD Options > User Settings** screen lets users view and potentially modify the **VCS Certificate Check Mode**. Users cannot modify the mode when the **VCS Certificate Check Mode Lockout** setting is checked. *See Figure 4.*	✓	✓
Security enhancement: Add support for configuring the **Session Negotiation Cipher** setting on the **Configuration >Session** web page. This setting applies to all session connection types (Direct to Host, View Connection Server and Connection Management System). Two cipher settings are supported. *See Figure 3.* • Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption. • Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption (**NOTE**: At the time of writing this cipher setting is not supported by View 5.1 and earlier virtual desktops).	✓	✓
Updated the OSD look and feel: • Revised color scheme • Revised logo placement	✓	✓
OSD enhancement: Remove **Peer MAC Address** and add **Enable Preparing Desktop Overlay** settings on the **Advanced Session** settings for Direct to Host connections *See Figure 5*.		✓
OSD enhancement: Add support for configuring the **Desktop Name to Select** and **Enable Preparing Desktop Overlay** settings on the **Advanced Session** settings for VCS connections. *See Figure 6*.	✓	
OSD enhancement: Add support for setting **Session Connection Type** equal to **View Connection Server + Auto-Logon** using the OSD. Previous releases support configuring this connection type through the web interface or the PCoIP MC. *See Figures 7 and 8.*	✓	✓
OSD enhancement: Add support for configuring the native resolution of each display when the display override feature is enabled. *See Figure 9.*	✓	✓
OSD enhancement: Modified the display topology setting page (see Figure 10).	✓	✓
OSD enhancement: Removed requirement to reboot zero client after changing display topology **Rotation** setting. *See Figure 10*.	✓	✓

New Features	Zero Client used with:	
	VMware View	Host card
Add support for a newly defined Teradici SNMP MIB which adds an extensive set of read-only variables. See Knowledge Base #15134-203 on the Teradici support site for details on the new MIB.	✓	✓
Add support for configuring the PCoIP endpoint session timeout (from 5 to 60 seconds) using the CMI.	✓	✓
Changed default OSD screen saver timeout to 300 seconds. Previous releases disabled the OSD screen saver by default.	✓	✓
Updated the zero client Wake-On-LAN session configuration settings (see Figure 11). **NOTE**: This change affects deployments using PCoIP host cards configured to wake workstations from a low power state using Wake-On-LAN messages.		✓

Fixes

Fixes	Zero Client used with:	
	VMware View	Host card
Resolved an issue where disabling **Login Username Caching** has no effect when using Imprivata OneSign.	✓	
Resolved an issue where the PCoIP endpoint would reset if DHCP Options 60 and 43 are not configured to identify the PCoIP Management Console. See the latest *PCoIP Management Console User Manual* (TER0812002) for configuration information.	✓	✓
Resolved an issue where the Omnikey 5325CL proximity card reader would not work with a zero client.	✓	
Resolved an issue where the zero client resets when logging out of a session authenticated with a smart card reader that uses an ALCOR AU9540A51-GBS-GR device.	✓	✓
Resolved an issue where the incorrect keyboard layout is used after downgrading firmware to a release that does not support the currently configured keyboard layout.	✓	✓
Resolved issues when using smart cards in-session with applications and middleware that make use of the SCardListReaders and SCardControl API functions.	✓	✓

Known Issues

Known Issues	Zero Client used with:	
	VMware View	Host card
See the Knowledge Base on the Teradici support website (http://techsupport.teradici.com) for known issues when PCoIP zero clients are connected to VMware View virtual desktops.	✓	
Deployments using PCoIP MC releases earlier than 1.7.0 may experience a problem where the PCoIP MC daemon resets while communicating with a zero client running FW release 3.5.0 or later. This occurs if the zero client has more than five VCS entries. ***Workaround:*** Upgrade to PCoIP MC version 1.7.0 or later or limit the maximum number of VCS entries to five.	✓	✓
The desktop display resolution may change when a user resizes the software client window while a session is active with a PCoIP host card. This occurs if the client window becomes smaller than the current desktop or a larger resolution will fit within the client window. Sometimes when this change occurs, the graphics driver scales the image resulting in the desktop not fitting within the client window. ***Workaround:*** Resize the client window or configure the graphics driver to use the monitor's built in scaling feature.	✓	
The PCoIP MC cannot be used to configure the IPv6 Gateway Address field. ***Workaround:*** Enable and configure DHCPv6 or SLAAC to set this field or configure the field statically using the device web interface.	✓	✓
Zero clients always connect to port 443 of the Imprivata OneSign server. Users cannot override the port by configuring a port number in the **Bootstrap URL** field.	✓	✓
Zero clients may fail to establish Imprivata OneSign sessions when the **OneSign Appliance Verification** setting equals **no verification**. This happens when the zero client trust store contains a certificate issued by the OneSign server that does not match the certificate used by the OneSign server. ***Workaround:*** Ensure the zero client trust store does not contain certificates issued by the OneSign server or ensure certificates in the zero client trust store match the certificates used by the OneSign server.	✓	✓
Zero clients in session with View 5.1 desktops running XP-32 may experience brief audio outages while using USB speakers or headsets.	✓	
Customers connecting a zero client to both PCoIP host cards and View desktops may experience USB device connectivity problems when connected to the View desktop. ***Workaround:*** *A*fter ending a session with a PCoIP host card, reset the zero client before establishing a session with a View desktop.	✓	✓
Customers connecting a zero client to a View 5.0.1 (or earlier) desktop may experience USB device connectivity problems. ***Workaround:*** Unplug and re-plug the USB device.	✓	

The following table describes the operating mode of USB devices based on device type, session type, and device configuration.

Table 3 Operating Mode of USB Devices

EHCI Disabled (Devices operate in USB 1.1 mode only)		
	Root Port	**Behind USB 1.1 and 2.0 Hub**
View Desktop	All devices operate in USB 1.1 mode.	
PCoIP Host Card	All devices operate in USB 1.1 mode.	

EHCI Enabled (USB 2.0 support is enabled)			
	Root Port	**Behind USB 1.1 Hub**	**Behind USB 2.0 Hub**
View Desktop	All devices operate in their native mode (USB 1.1 or USB 2.0) with the exception of USB 2.0 isochronous devices (i.e., audio devices, WebCams). USB 2.0 isochronous devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All non-isochronous devices operate in their native mode (USB 1.1 or USB 2.0) Isochronous devices are not supported (a warning overlay may appear).
PCoIP Host Card	All devices operate in USB 1.1 mode.		

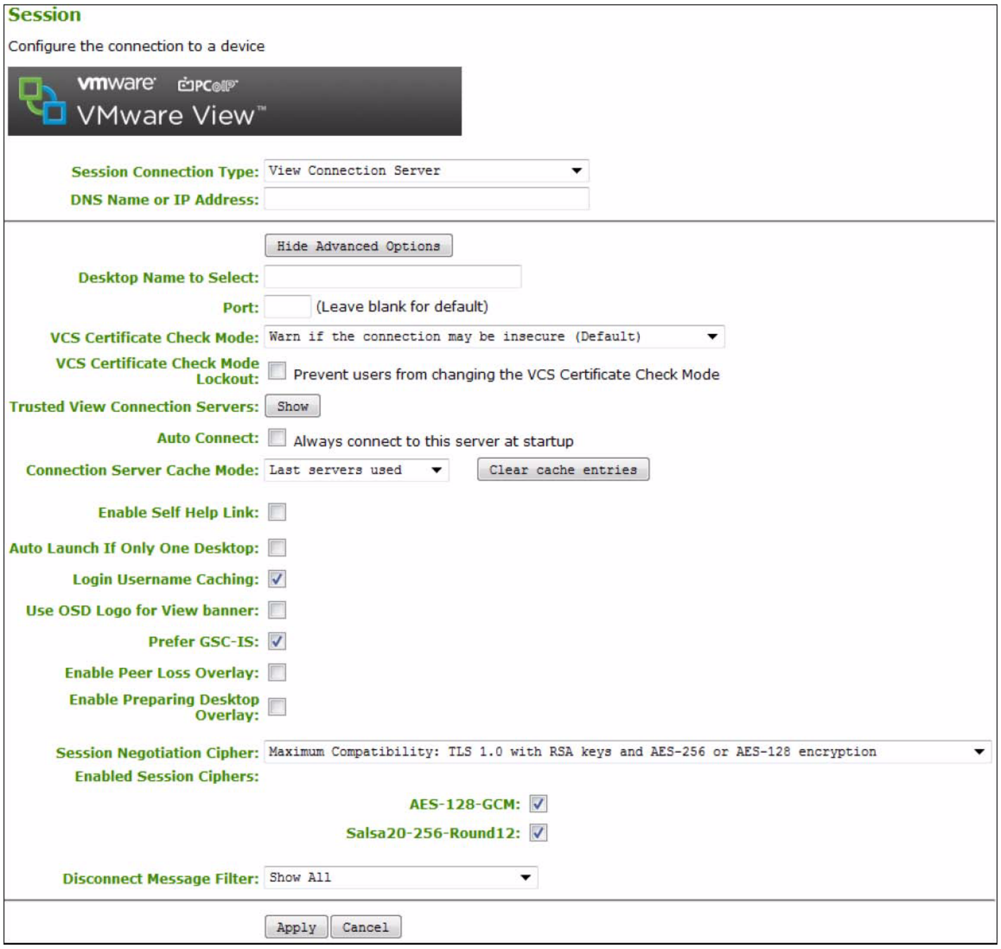
Additional Collateral

Additional Collateral	**Zero Client used with:**	
	VMware View	**Host card**
Refer to the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓	
Refer to the latest *VMware View to PCoIP Zero Client WAN Network Guidelines* (TER1007002) document for network optimization guidelines when connecting PCoIP zero clients to VMware View 4 virtual desktops over remote access WAN networks.	✓	
Refer to the Teradici support website (http://techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓
Refer to the Wyse website (http://www.wyse.com) for information on Wyse Device Manager™ (WDM) network management services for the PCoIP zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot rename, automatic check-in support, Wake-On-LAN, change device properties, and so on).	✓	

Supplemental Information

Configuration > Session VCS Advanced Web Page

Figure 1 Configuration > Session VCS Advanced Web Page



Session

Configure the connection to a device

Session Connection Type: View Connection Server

DNS Name or IP Address:

Desktop Name to Select:

Port: (Leave blank for default)

VCS Certificate Check Mode: Warn if the connection may be insecure (Default)

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

Trusted View Connection Servers:

Auto Connect: □ Always connect to this server at startup

Connection Server Cache Mode: Last servers used

Enable Self Help Link: □

Auto Launch If Only One Desktop: □

Login Username Caching: ☑

Use OSD Logo for View banner: □

Prefer GSC-IS: ☑

Enable Peer Loss Overlay: □

Enable Preparing Desktop Overlay: □

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

Enabled Session Ciphers:

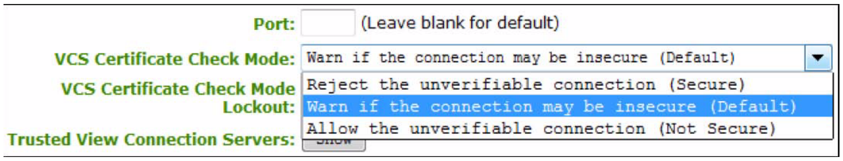
AES-128-GCM: ☑

Salsa20-256-Round12: ☑

Disconnect Message Filter: Show All

VCS Certificate Check Mode Options

Figure 2 VCS Certificate Check Mode Options



Port: (Leave blank for default)

VCS Certificate Check Mode: Warn if the connection may be insecure (Default)

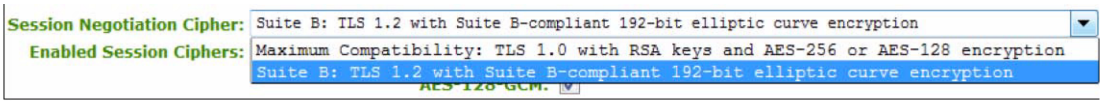
- Reject the unverifiable connection (Secure)
- Warn if the connection may be insecure (Default)
- Allow the unverifiable connection (Not Secure)

VCS Certificate Check Mode Lockout:

Trusted View Connection Servers:

Session Negotiation Cipher Options

Figure 3 Session Negotiation Cipher Options



Session Negotiation Cipher: Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption

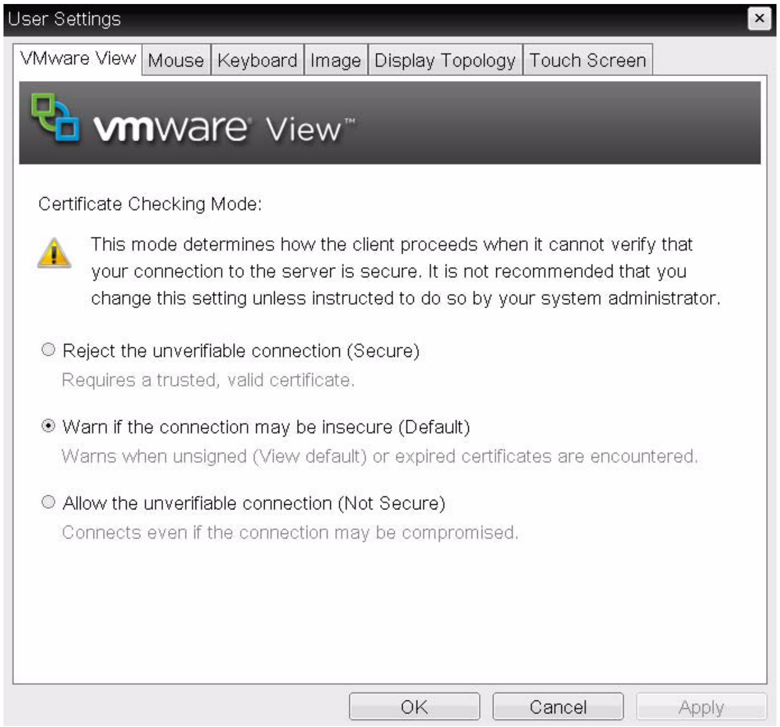
Enabled Session Ciphers:

- Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption
- Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption

AES-128-GCM: ☑

OSD User Settings > VMware View Options

Figure 4 OSD User Settings > VMware View Options



Certificate Checking Mode:

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

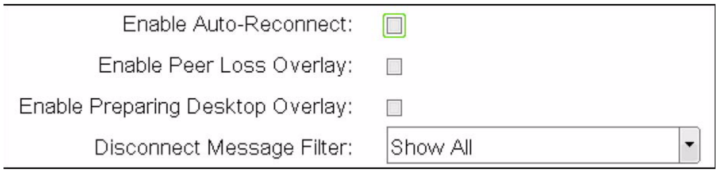
○ Reject the unverifiable connection (Secure)
Requires a trusted, valid certificate.

● Warn if the connection may be insecure (Default)
Warns when unsigned (View default) or expired certificates are encountered.

○ Allow the unverifiable connection (Not Secure)
Connects even if the connection may be compromised.

OSD Configuration > Session Direct to Host Advanced Options

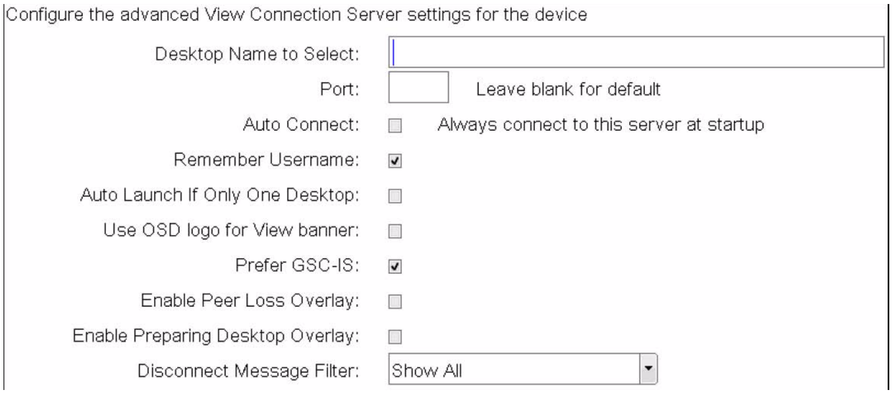
Figure 5 OSD Configuration > Session Direct to Host Advanced Options



Enable Auto-Reconnect:	□
Enable Peer Loss Overlay:	□
Enable Preparing Desktop Overlay:	□
Disconnect Message Filter:	Show All

OSD Configuration > Session VCS Advanced Options

Figure 6 OSD Configuration > Session VCS Advanced Options



Configure the advanced View Connection Server settings for the device

Desktop Name to Select:

Port: Leave blank for default

Auto Connect: ☐ Always connect to this server at startup

Remember Username: ☑

Auto Launch If Only One Desktop: ☐

Use OSD logo for View banner: ☐

Prefer GSC-IS: ☑

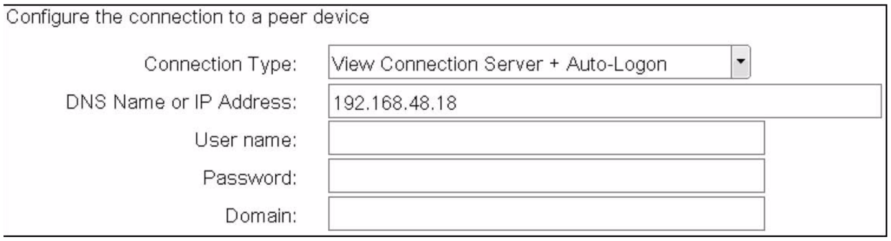
Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Disconnect Message Filter: Show All

OSD Configuration > Session VCS + Auto-Logon Options

Figure 7 OSD Configuration > Session VCS + Auto-Logon Options



Configure the connection to a peer device

Connection Type: View Connection Server + Auto-Logon

DNS Name or IP Address: 192.168.48.18

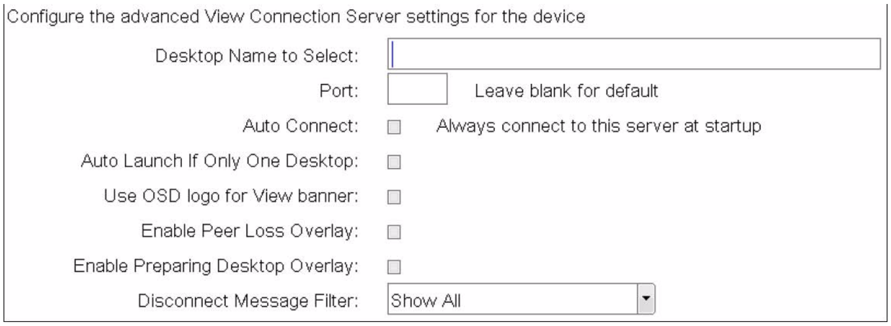
User name:

Password:

Domain:

OSD Configuration > Session VCS + Auto-Logon Advanced Options

Figure 8 OSD Configuration > Session VCS + Auto-Logon Advanced Options



Configure the advanced View Connection Server settings for the device

Desktop Name to Select:

Port: Leave blank for default

Auto Connect: ☐ Always connect to this server at startup

Auto Launch If Only One Desktop: ☐

Use OSD logo for View banner: ☐

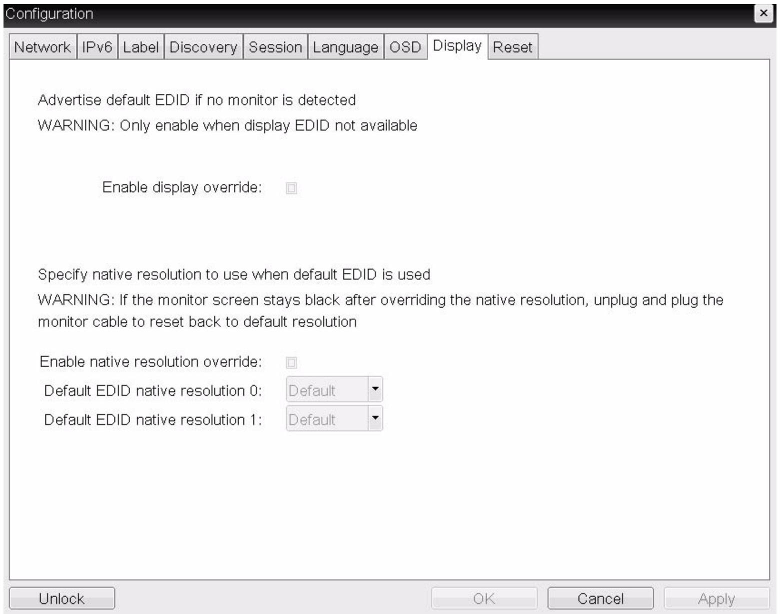
Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Disconnect Message Filter: Show All

OSD Configuration > Display Options

Figure 9 OSD Configuration > Display Options



Advertise default EDID if no monitor is detected

WARNING: Only enable when display EDID not available

Enable display override: □

Specify native resolution to use when default EDID is used

WARNING: If the monitor screen stays black after overriding the native resolution, unplug and plug the monitor cable to reset back to default resolution

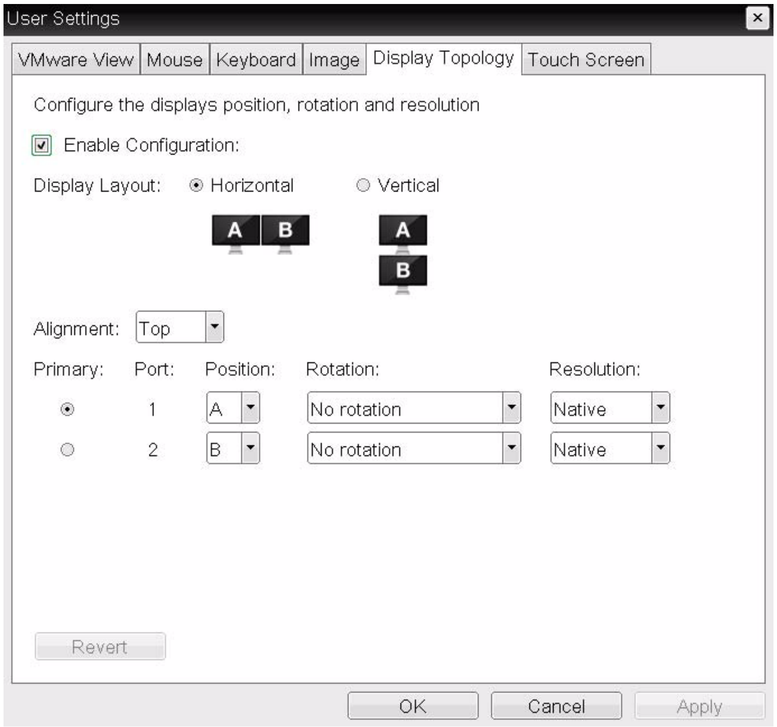
Enable native resolution override: □

Default EDID native resolution 0: Default

Default EDID native resolution 1: Default

OSD User Settings > Display Topology Options

Figure 10 OSD User Settings > Display Topology Options



Configure the displays position, rotation and resolution

☑ Enable Configuration:

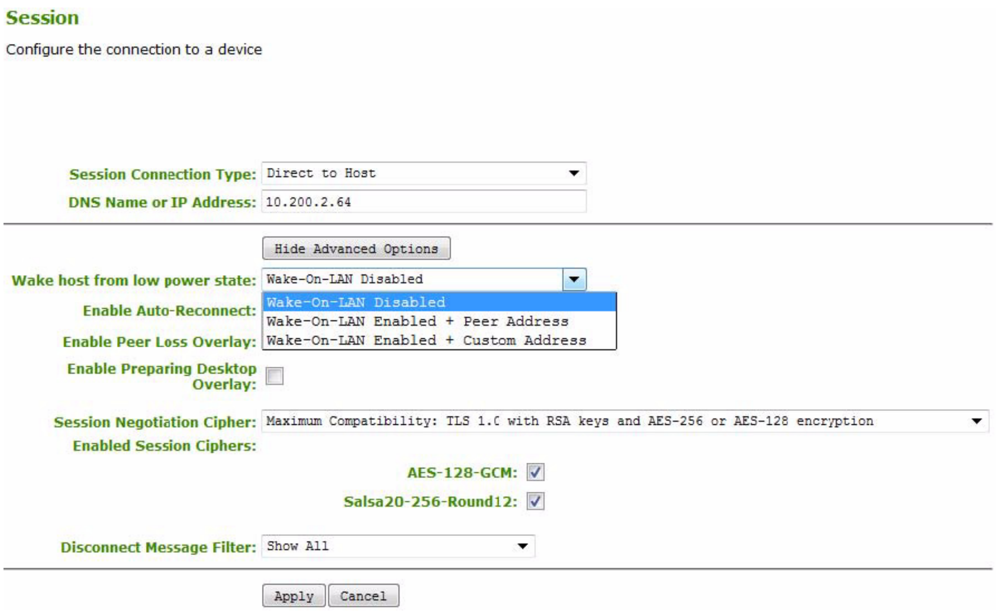
Display Layout: ● Horizontal ○ Vertical

Alignment: Top

Primary:	Port:	Position:	Rotation:	Resolution:
●	1	A	No rotation	Native
○	2	B	No rotation	Native

Configuration > Session Direct to Host Advanced Web Page

Figure 11 Configuration > Session Direct to Host Advanced Web Page



Session

Configure the connection to a device

Session Connection Type: Direct to Host

DNS Name or IP Address: 10.200.2.64

Wake host from low power state: Wake-On-LAN Disabled

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay: □

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

Enabled Session Ciphers:

AES-128-GCM: ☑

Salsa20-256-Round12: ☑

Disconnect Message Filter: Show All

Hide Advanced Options
Wake-On-LAN Disabled
Wake-On-LAN Enabled + Peer Address
Wake-On-LAN Enabled + Custom Address
Apply
Cancel

This page intentionally blank.

Release Notes

Wyse® PCoIP Firmware Release 4.x
Issue: 100913

Written and published by:
Wyse Technology LLC, October 2013

Created using FrameMaker® and Acrobat®