TERA Firmware Release Notes Version 4.x

TER1204003

Issue 2

PCoIP CONNECTED

TERADICI™

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

Revision History

Version	Date	Description
2	Aug 13, 2012	Updated for release 4.0.1
1	May 17, 2012	Initial release

Contents

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
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
POE	Power Over Ethernet
RDP	Remote Desktop Protocol
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
URI	Uniform Resource Identifier
USB	Universal Serial Bus
VCS	VMware View Connection Server

Preface

This application note provides a brief summary of the feature additions and issues resolved in each TERA1x00/TERA2xxx firmware release starting with release 4.0.0. The sections in this document are organized according to release date, with the most recent releases listed first.

1 Release 4.0.1

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

1.1 Compatibility

VMware View 5.0 or later deployments using zero client devices to connect to View virtual desktops should install release 4.0.1 on the zero client devices.

It is highly recommended that remote workstation deployments using zero clients with PCoIP host cards install release 4.0.1 on both the host card and client devices. While mixed firmware release operation is not tested, firmware release 4.0.1 is compatible with 4.0.0, 3.5.x, 3.4.x, 3.3.x, 3.2.x and 3.1.x releases. Firmware 4.0.1 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 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 later) 3) Install the new firmware (4.0.1)
0.18 through 1.3	1) Install a 1.x firmware release (1.4 or later) 2) Install the new firmware (4.0.1)
1.4 through 4.0.0	Install the new firmware (4.0.1)

1.2 Feature Additions

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Added support for the new TERA2240/2220/2140/2321 Processor based zero clients and host cards.	✓	✓	✓

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	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 section 1.6.1.	✓	✓	
Added pre-session support for the eToken 5205 Pro Anywhere and 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 section 1.6.2.	✓	✓	✓
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 section 1.6.3.	✓		

1.3 Important Bug Fixes

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Zero client now trusts intermediate and leaf certificates.	✓		

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
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.	✓		
Certificates 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).	✓	✓	✓

1.4 Known Issues

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

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

Tera 1			
	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) - 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, web cams). 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		

Tera 2		
	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	The EHCI disable flag does not apply to the PCoIP host card. See 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, web cams). 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 their native mode (USB 1.1 or USB 2.0) with the exception of USB 2.0 isochronous devices (i.e. audio devices, web cams). 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 will not appear).

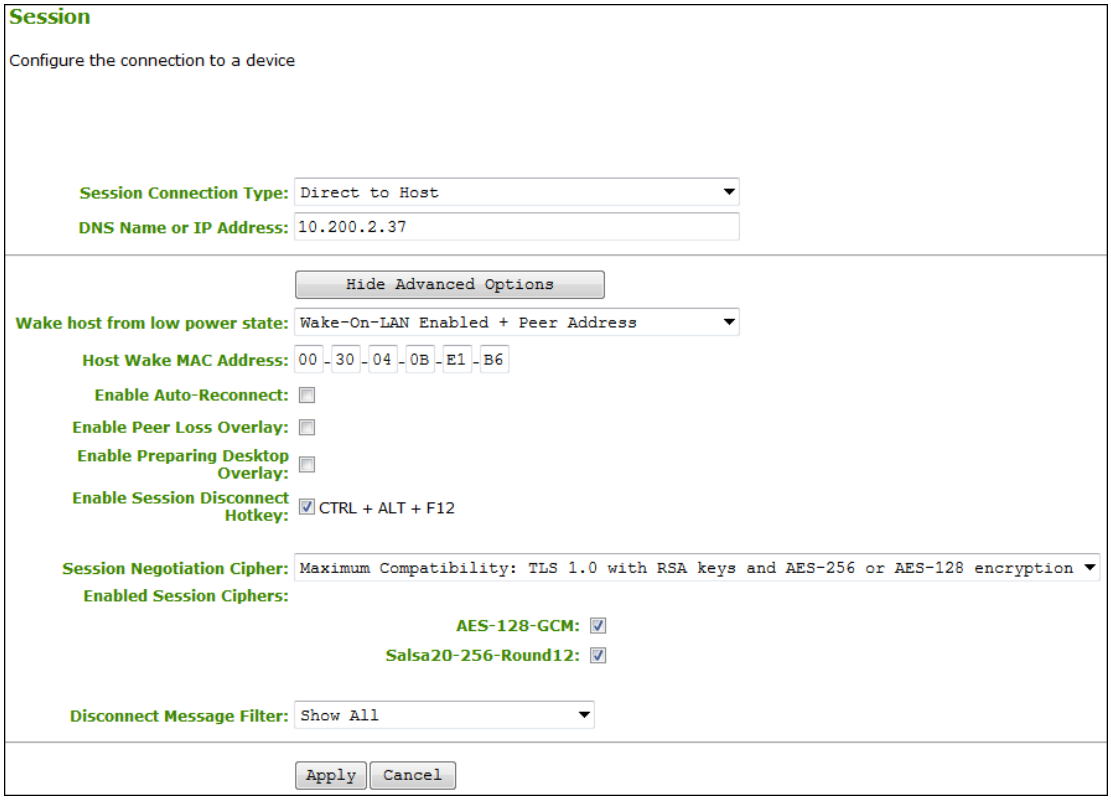
1.5 Additional Collateral

Description	**Zero Client (used with VMware View)**	**Zero Client (used with Host Card)**	**Host Card**
See 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.	✓		

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See 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.	✓		
See the Teradici support website (techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓	✓

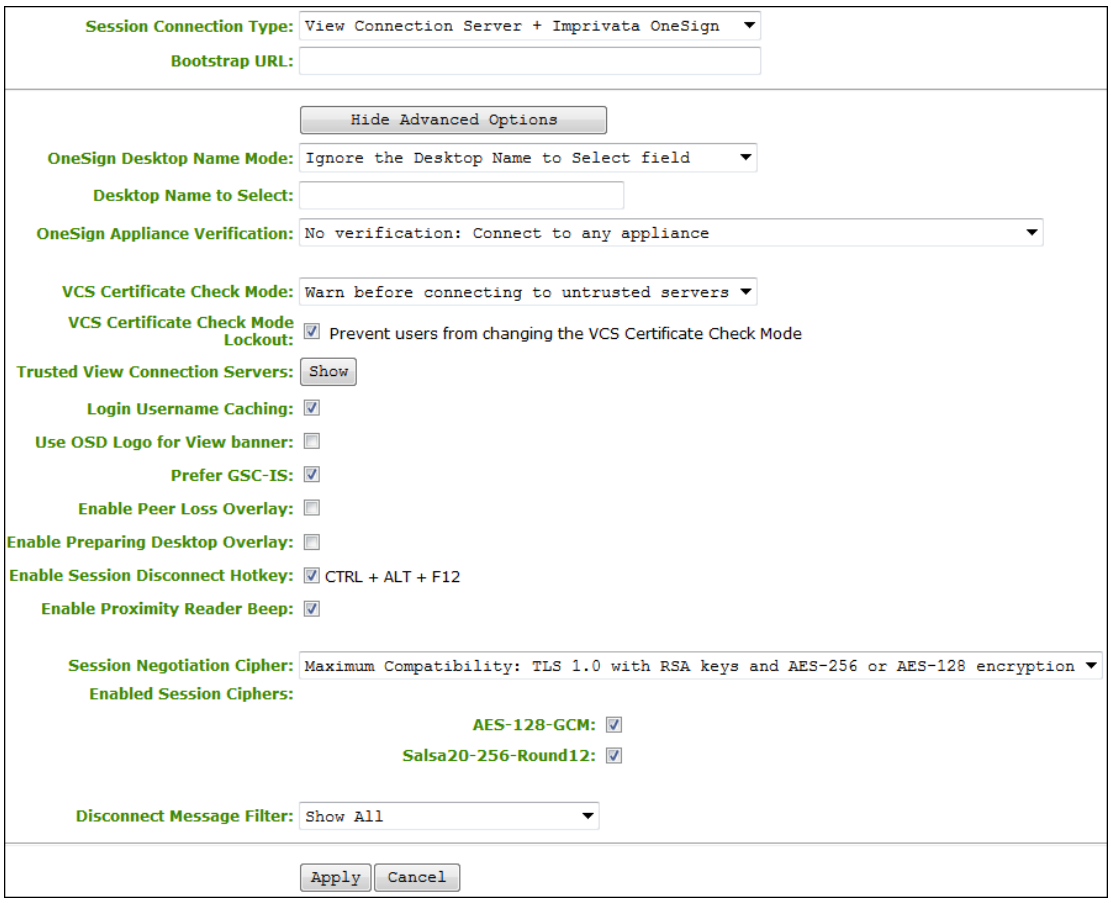
1.6 Supplemental Information

1.6.1 Configuration->Session Direct to Host Advanced Web Page



1.6.2 Configuration->SNMP Web Page

1.6.3 Configuration->Session VCS + Imprivata OneSign Advanced Web Page



2 Release 4.0.0

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

2.1 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 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 later) 3) Install the new firmware (4.0.0)
0.18 through 1.3	1) Install a 1.x firmware release (1.4 or later) 2) Install the new firmware (4.0.0)
1.4 through 3.5.1	Install the new firmware (4.0.0)

2.2 Feature Additions

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	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 sections 2.6 and 2.6.2. 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 section 2.6.4.	✓	✓	
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). See sections 2.6 and 2.6.3. Two cipher settings are supported. • 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 section 2.6.5.		✓	
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 section 2.6.6.	✓	✓	

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
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 sections 2.6.7 and 2.6.8.	✓	✓	
OSD enhancement: Add support for configuring the native resolution of each display when the display override feature is enabled. See section 2.6.9.	✓	✓	
OSD enhancement: Modified the display topology setting page. See section 2.6.10.	✓	✓	
OSD enhancement: Removed requirement to reboot zero client after changing display topology **Rotation** setting. See section 2.6.10.	✓	✓	
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 section 2.6.11. Note: This change affects deployments using PCoIP host cards configured to wake workstations from a low power state using Wake-On-LAN messages.		✓	

2.3 Important Bug Fixes

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Resolved an issue where disabling **Login Username Caching** has no effect when using Imprivata OneSign.	✓		

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
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.	✓	✓	

2.4 Known Issues

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	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.	✓	✓	

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
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:** After 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 mode USB devices operate in based on device type, session type, and device configuration.

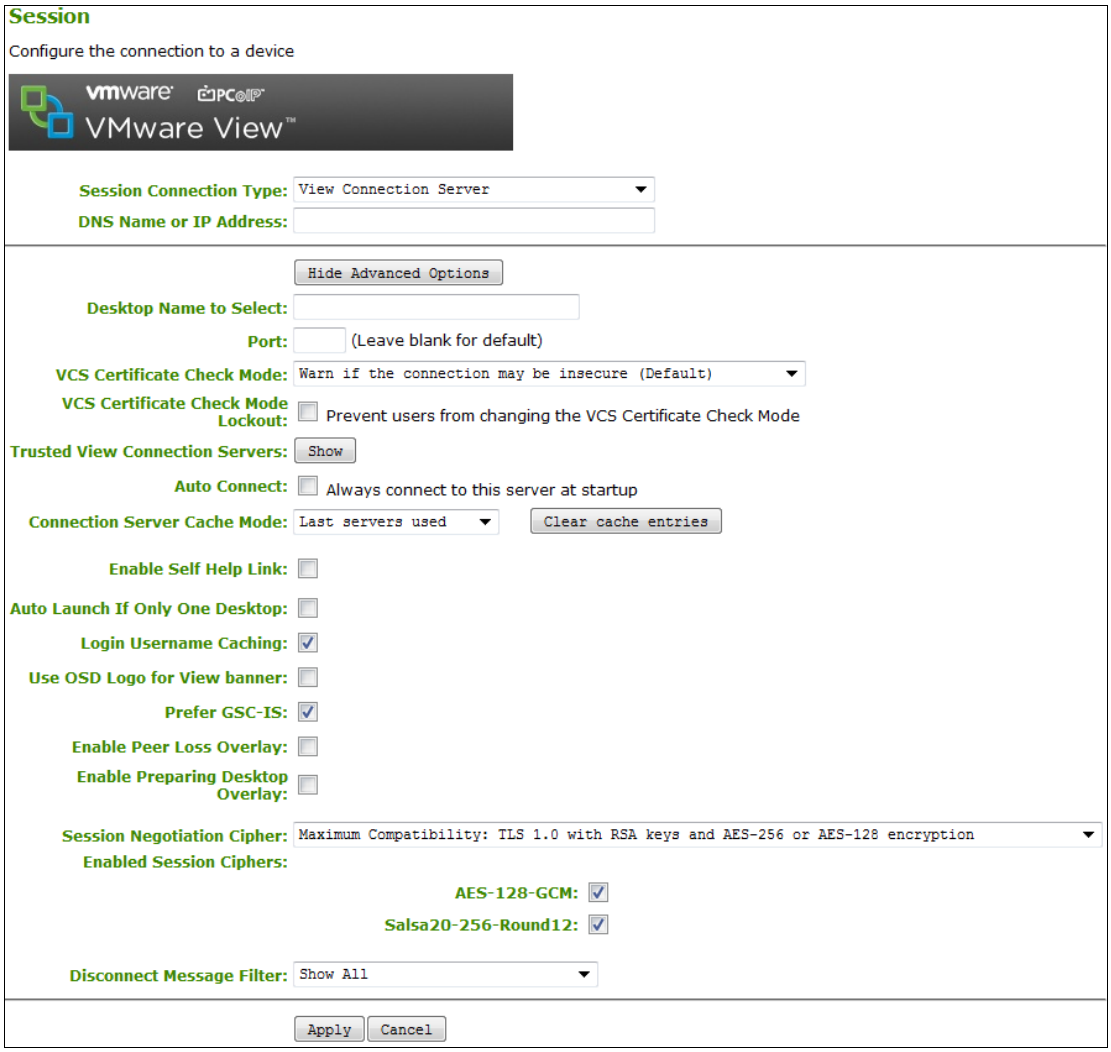
	EHCI Disabled (Devices operate in USB 1.1 mode only)		
	Root Port		**Behind USB 1.1 and 2.0 Hub**
View Desktop	All devices operate in USB 1.1 mode		
PCoIP Host Card	All devices operate in USB 1.1 mode		
	EHCI Enabled (USB 2.0 support is enabled)		
	Root Port	**Behind USB 1.1 Hub**	**Behind USB 2.0 Hub**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

2.5 Additional Collateral

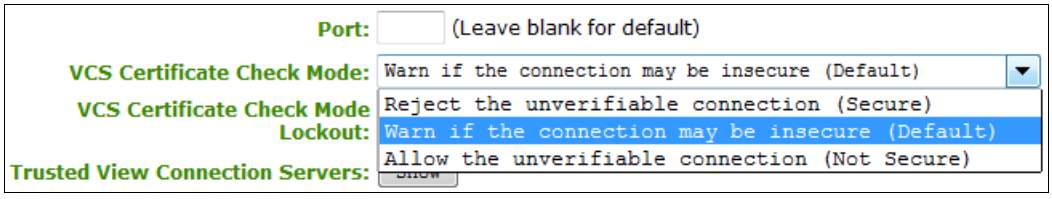
Description	**Zero Client (used with VMware View)**	**Zero Client (used with Host Card)**	**Host Card**
See the latest *VMware View to PCoIP Zero Client Optimization Guide* (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the 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.	✓		
See the Teradici support website (techsupport.teradici.com) for additional collateral for PCoIP zero client and PCoIP host card applications, implementation and management.	✓	✓	✓

2.6 Supplemental Information

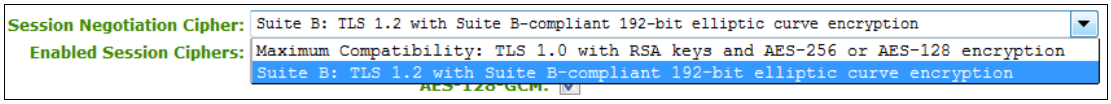
2.6.1 Configuration->Session VCS Advanced Web Page



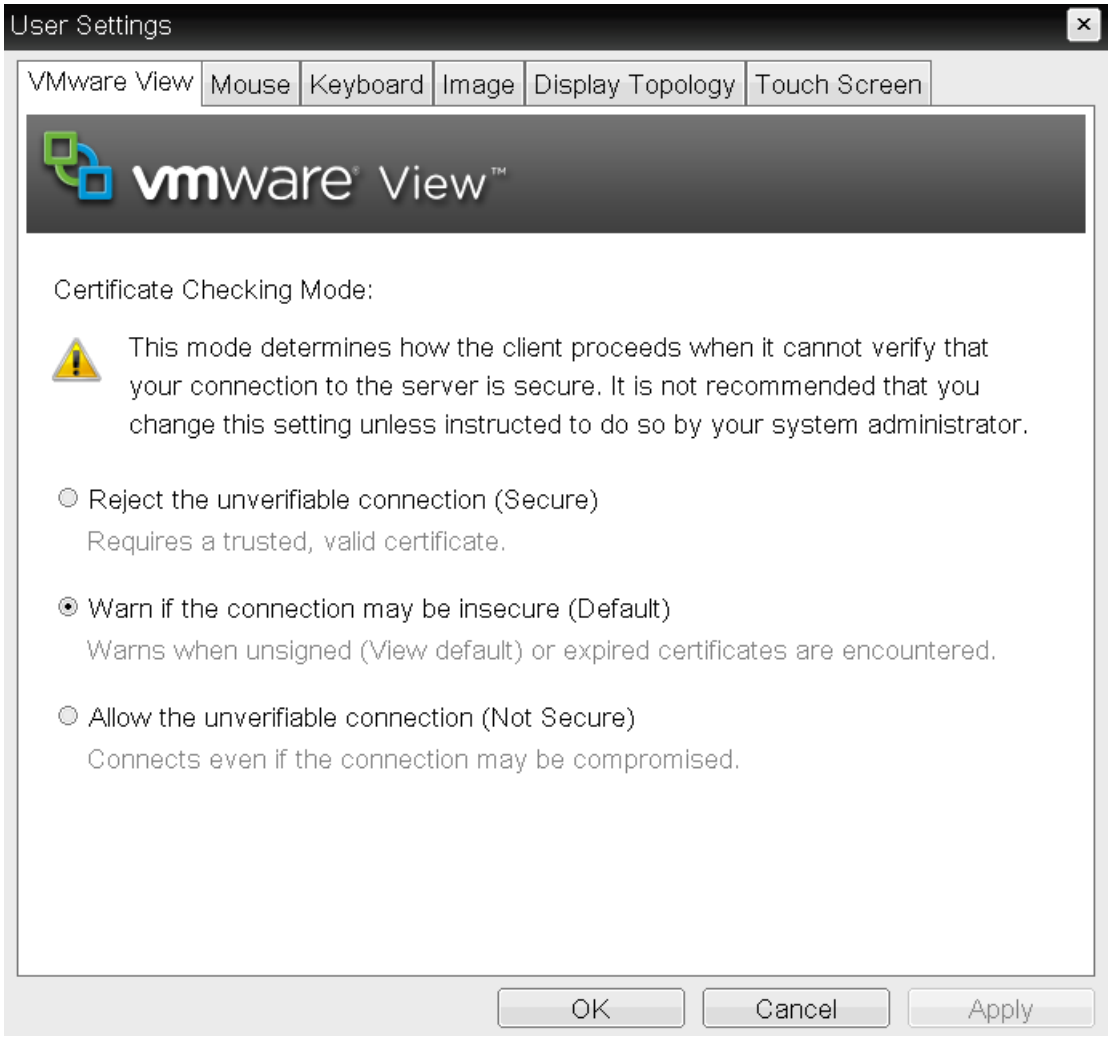
2.6.2 VCS Certificate Check Mode Options



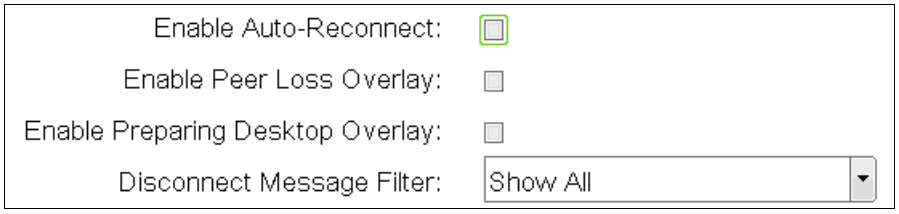
2.6.3 Session Negotiation Cipher Options



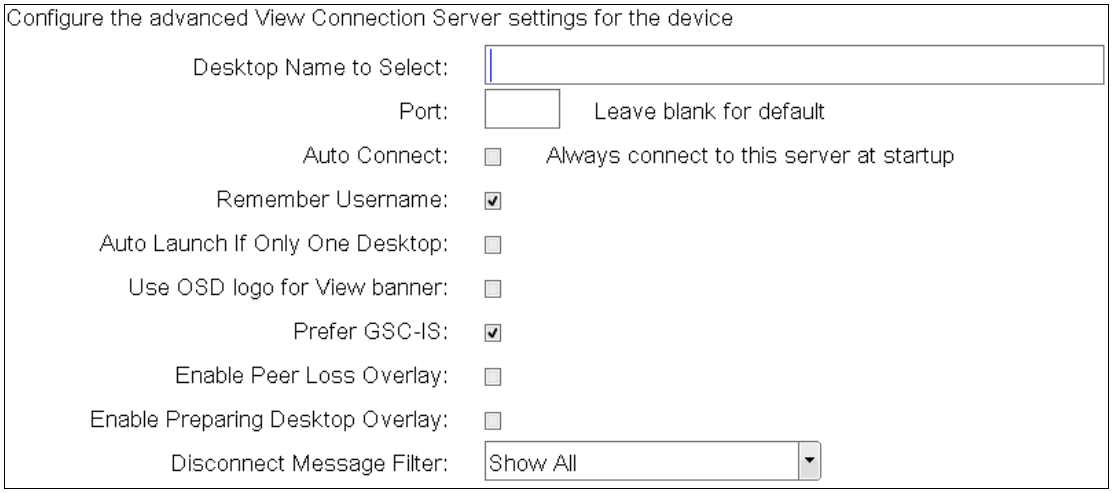
2.6.4 OSD User Settings->VMware View Options



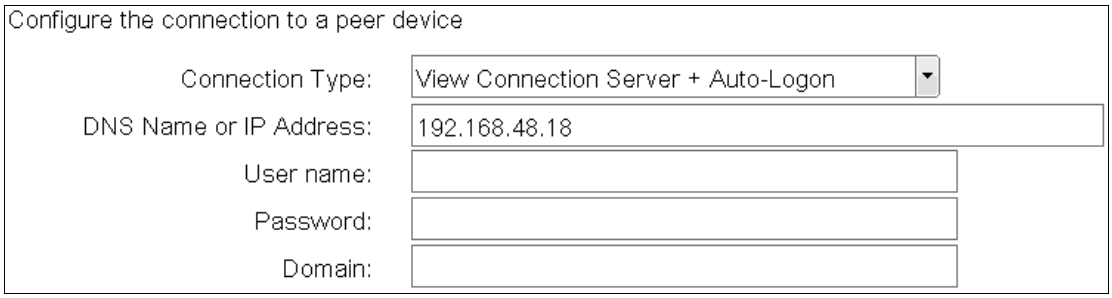
2.6.5 OSD Configuration->Session Direct to Host Advanced Options



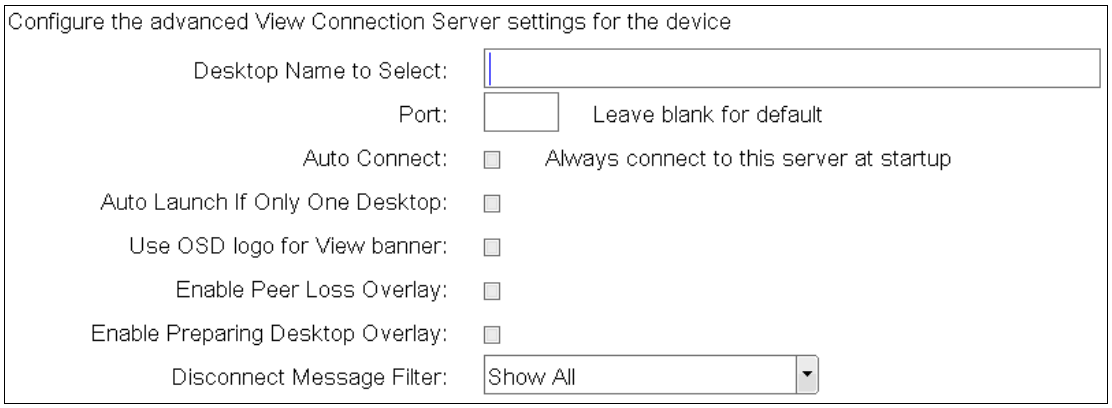
2.6.6 OSD Configuration->Session VCS Advanced Options



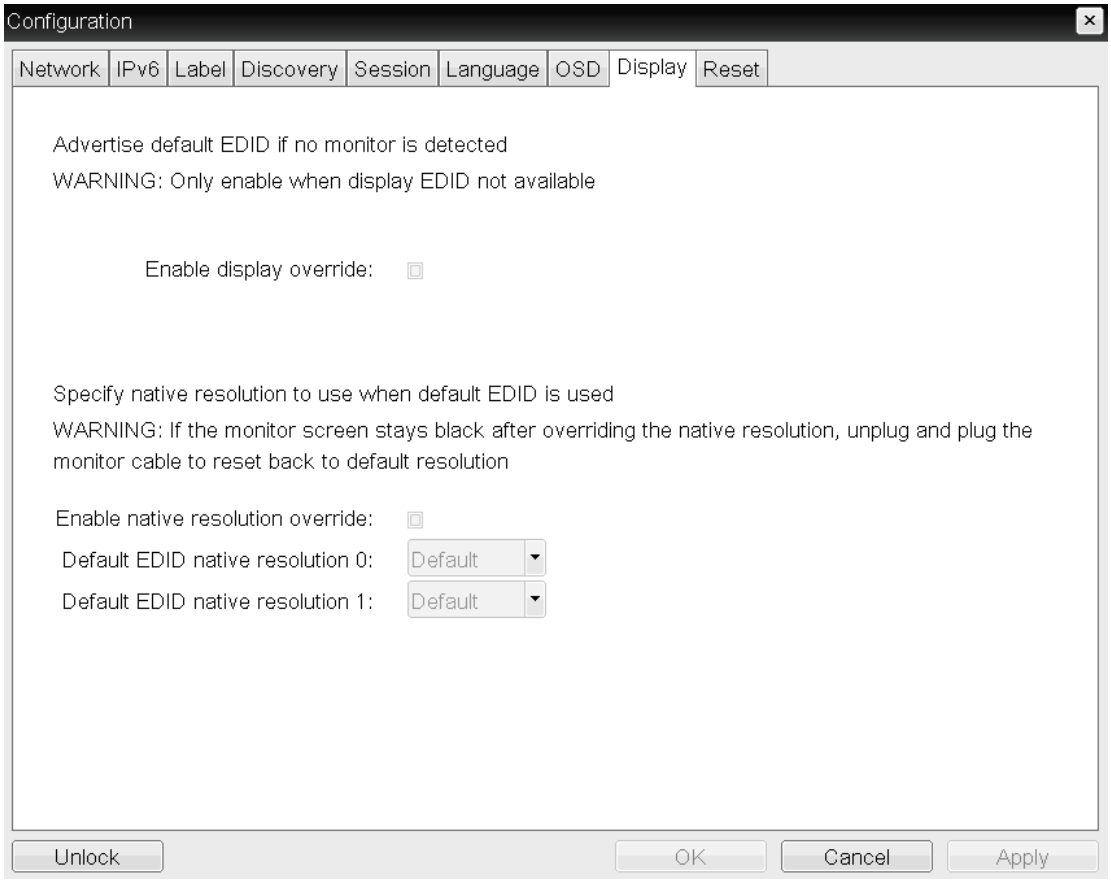
2.6.7 OSD Configuration->Session VCS + Auto-Logon Options



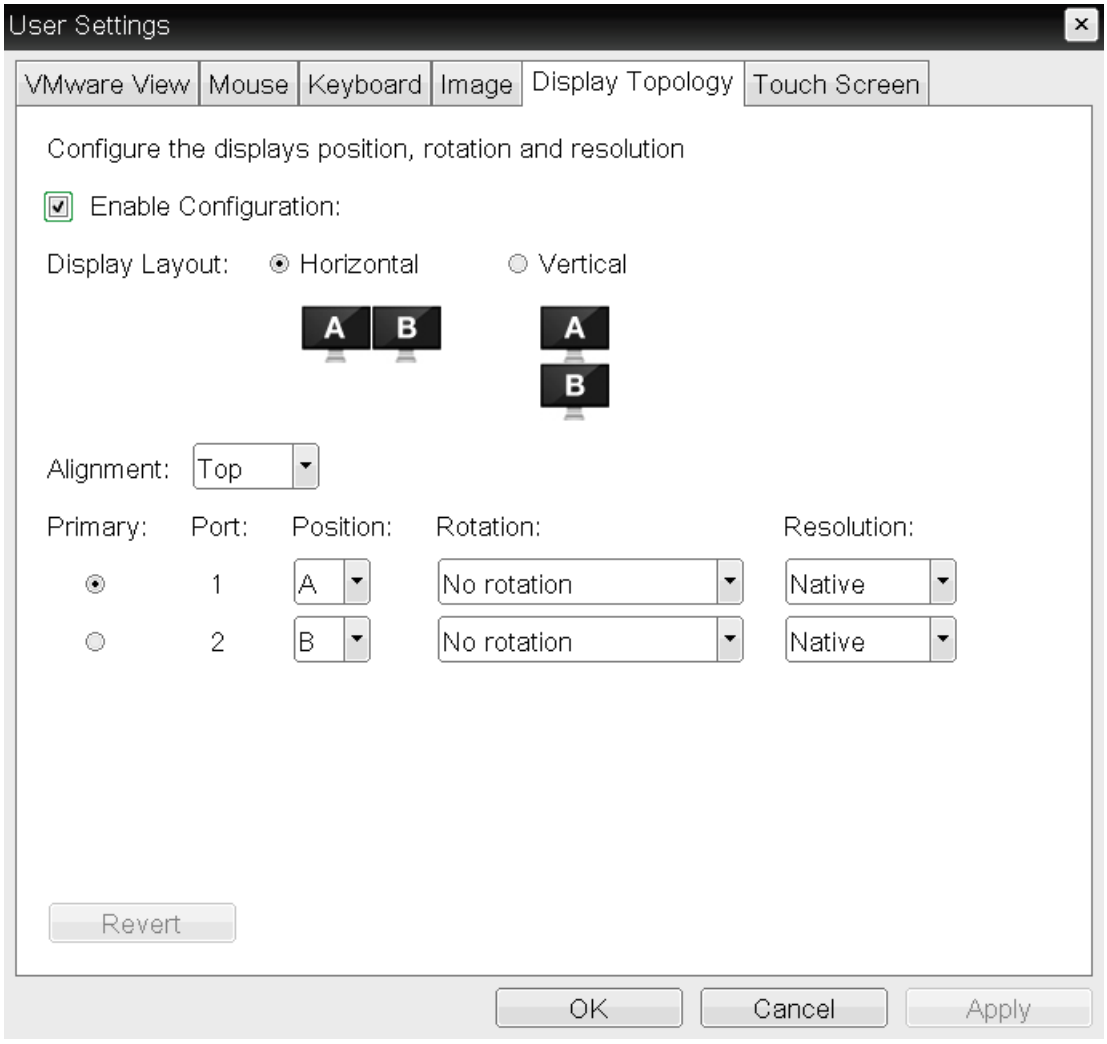
2.6.8 OSD Configuration->Session VCS + Auto-Logon Advanced Options



2.6.9 OSD Configuration->Display Options



2.6.10 OSD User Settings->Display Topology Options



2.6.11 Configuration->Session Direct to Host Advanced Web Page