

TERA Firmware Release Notes Version 4.x

TER1204003

Issue 6



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



The information contained in this document represents the current view of Teradici Corporation as of the date of publication. Because Teradici must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Teradici, and Teradici cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. TERADICI MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

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

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Visit <http://www.teradici.com/teradici/pat.php> for more information.

© 2013 Teradici Corporation. All rights reserved.

Teradici, PC-over-IP, and PCoIP are registered trademarks of Teradici Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision History

Version	Date	Description
6	Aug 23, 2013	Updated for release 4.1.2
5	Apr 26, 2013	Updated for release 4.1.0
4	Nov 09, 2012	Updated for release 4.0.3
3	Aug 23, 2012	Updated for release 4.0.2
2	Aug 13, 2012	Updated for release 4.0.1
1	May 17, 2012	Initial release

Contents

1	Release 4.1.2	11
1.1	Compatibility Notes	11
1.1.1	Workstation and VDI	11
1.1.2	VDI Specific	11
1.1.3	Workstation Specific	11
1.2	Feature Additions.....	12
1.2.1	Workstation and VDI	12
1.2.2	VDI Specific	12
1.2.3	Workstation Specific	12
1.3	Important Bug Fixes.....	12
1.3.1	Workstation and VDI	12
1.3.2	VDI Specific	13
1.3.3	Workstation Specific	13
1.4	Known Issues.....	13
1.5	Additional Collateral	13
1.6	Supplemental Information.....	14
1.6.1	Configuration->Power Web Page	14
1.6.2	VDI Auto Connect Options.....	14
2	Release 4.1.0	15
2.1	Compatibility Notes	15
2.1.1	Workstation and VDI	15
2.1.2	VDI Specific	15
2.1.3	Workstation Specific	15
2.2	Feature Additions.....	16
2.2.1	Workstation and VDI	16
2.2.2	VDI Specific	16
2.2.3	Workstation Specific	16
2.3	Important Bug Fixes.....	17
2.3.1	Workstation and VDI	17
2.3.2	VDI Specific	17
2.3.3	Workstation Specific	18
2.4	Known Issues.....	18
2.5	Additional Collateral	20
2.6	Supplemental Information.....	20
2.6.1	Configuration->Access Web Page.....	20
2.6.2	OSD Configuration->Access Options	21
2.6.3	Configuration->SCEP Web Page	21
2.6.4	OSD Configuration->SCEP Options.....	22

2.6.5	Configuration->Power Web Page	22
2.6.6	OSD Configuration->Display Options	23
2.6.7	Configuration->Session PColP Connection Manager Web Page	24
2.6.8	OSD Configuration->Session PColP Conn Mgr Options.....	25
2.6.9	OSD Configuration->Session PColP Conn Mgr Advanced Options	26
2.6.10	Configuration->Session PColP Conn Mgr + Logon Web Page.....	27
2.6.11	OSD Configuration->Session PColP Conn Mgr + Logon Options	28
2.6.12	OSD Configuration->Session PColP Conn Mgr + Logon Adv Options	29
2.6.13	OSD Configuration->Session Direct to Host Advanced Options.....	29
3	Release 4.0.3	30
3.1	Compatibility	30
3.2	Feature Additions.....	30
3.3	Important Bug Fixes.....	30
3.4	Known Issues.....	31
3.5	Additional Collateral.....	33
4	Release 4.0.2	34
4.1	Compatibility	34
4.2	Feature Additions.....	35
4.3	Important Bug Fixes.....	35
4.4	Known Issues.....	35
4.5	Additional Collateral.....	36
5	Release 4.0.1	37
5.1	Compatibility	37
5.2	Feature Additions.....	38
5.3	Important Bug Fixes.....	39
5.4	Known Issues.....	40
5.5	Additional Collateral.....	40
5.6	Supplemental Information.....	41
5.6.1	Configuration->Session Direct to Host Advanced Web Page	41
5.6.2	Configuration->SNMP Web Page.....	41
5.6.3	Configuration->Session VCS + Imprivata OneSign Advanced Web Page.....	42
6	Release 4.0.0	43
6.1	Compatibility	43
6.2	Feature Additions.....	44
6.3	Important Bug Fixes.....	45
6.4	Known Issues.....	46
6.5	Additional Collateral.....	48

6.6	Supplemental Information	49
6.6.1	Configuration->Session VCS Advanced Web Page	49
6.6.2	VCS Certificate Check Mode Options	49
6.6.3	Session Negotiation Cipher Options	49
6.6.4	OSD User Settings->VMware View Options	50
6.6.5	OSD Configuration->Session Direct to Host Advanced Options	50
6.6.6	OSD Configuration->Session VCS Advanced Options	51
6.6.7	OSD Configuration->Session VCS + Auto-Logon Options	51
6.6.8	OSD Configuration->Session VCS + Auto-Logon Advanced Options	51
6.6.9	OSD Configuration->Display Options	52
6.6.10	OSD User Settings->Display Topology Options	53
6.6.11	Configuration->Session Direct to Host Advanced Web Page	54

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
POE	Power Over Ethernet
RDP	Remote Desktop Protocol
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 Horizon View software application that can establish a PCoIP session with a PCoIP host
Tera1	First-generation family of Teradici processors for PCoIP zero clients and host cards.
Tera2	Second-generation family of Teradici processors for PCoIP zero clients and host cards.
TERA1100	First-generation Teradici processor supporting PCoIP zero client functionality. TERA1100 zero clients support up to two displays at a resolution of 1920x1200.

	The maximum resolution is dependent on the zero client memory size
TERA1202	First-generation Teradici processor supporting PCoIP host card functionality. TERA1202 host cards support two displays at a resolution of 1920x1200.
TERA2140	Second-generation Teradici processor supporting PCoIP zero client functionality. TERA2140 zero clients support two displays at a resolution of 2560x1600 or four displays at a resolution of 1920x1200.
TERA2220	Second-generation Teradici processor supporting PCoIP host card functionality. TERA2220 host cards support two displays at a resolution of 1920x1200 or one display at a resolution of 2560x1600.
TERA2240	Second-generation Teradici processor supporting PCoIP host card functionality. TERA2240 host cards support four displays at a resolution of 1920x1200 or two displays at a resolution of 2560x1600.
TERA2321	Second-generation Teradici processor supporting PCoIP zero client functionality. TERA2321 zero clients support two displays at a resolution of 1920x1200 or one display at a resolution of 2560x1600.
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 4.1.2

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

1.1 Compatibility Notes

1.1.1 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	<ol style="list-style-type: none"> 1) Install firmware release 0.18 2) Install a 1.x firmware release (1.4 or later) 3) Install the new firmware (4.1.2)
0.18 through 1.3	<ol style="list-style-type: none"> 1) Install a 1.x firmware release (1.4 or later) 2) Install the new firmware (4.1.2)
1.4 through 4.1.1	Install the new firmware (4.1.2)

1.1.2 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.

1.1.3 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.

1.2 Feature Additions

1.2.1 Workstation and VDI

Description
<p>Display Suspend (for Tera2 zero clients)</p> <p>When users are in-session, the firmware now supports a display suspend feature after a specified keyboard and mouse inactivity timeout. See section 1.6.1.</p>

1.2.2 VDI Specific

Description
<p>Changed the Auto Connect feature from a checkbox to a dropdown menu with the following options.</p> <ul style="list-style-type: none"> • 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. <p>The Auto Connect feature is an advanced option supported by the following Session Connection Types.</p> <ul style="list-style-type: none"> • 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) <p>See section 1.6.2.</p>
<p>Continuous Desktop Retry (for Tera1 and Tera2 zero clients)</p> <p>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.</p>

1.2.3 Workstation Specific

None

1.3 Important Bug Fixes

1.3.1 Workstation and VDI

None

1.3.2 VDI Specific

Description
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).

1.3.3 Workstation Specific

None

1.4 Known Issues

See the Knowledge Base on the Teradici support website (<http://techsupport.teradici.com>) for known issues.

Table 2-1 and Table 2-2 describe the mode USB devices connected to a zero client operate in based on device type, session type, and device configuration.

1.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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->Power Web Page

Power
 Change the power settings

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

Display Suspend Timeout: Seconds (0 = disabled)

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

Remote Host Power Control:

Power On After Power Loss: ☐

Enable Wake-on-USB: ☒

Enable Wake-on-LAN: ☐

1.6.2 VDI Auto Connect Options

Auto Connect:

Connection Server Cache Mode:

Enable Self Help Link: ☐

2 Release 4.1.0

This section provides a brief summary of the issues resolved in release 4.1.0.

2.1 Compatibility Notes

2.1.1 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 later) 3) Install the new firmware (4.1.0)
0.18 through 1.3	1) Install a 1.x firmware release (1.4 or later) 2) Install the new firmware (4.1.0)
1.4 through 4.0.x	Install the new firmware (4.1.0)

2.1.2 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.

2.1.3 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.

2.2 Feature Additions

2.2.1 Workstation and VDI

Description
<p>Security features (for Tera1 and Tera2 endpoints)</p> <ul style="list-style-type: none"> 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 next access of the Administrative Web Interface or On-Screen-Display (selected password may be blank). See sections 2.6.1 and 2.6.2. Logging of failed access attempts to the Administrative Web Interface, On Screen Display, or management interface (e.g. PCoIP Management Console). Added options to disable the Administrative Web Interface and/or the management tool interface (e.g. Tera1 and Tera2 endpoints can lock out access by the PCoIP Management Console). See sections 2.6.1 and 2.6.2.
<p>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 sections 2.6.3 and 2.6.4.</p>
<p>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 section 2.6.5.</p>
<p>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 section 2.6.6.</p> <p>Note: The resolution setting of the primary display will also be applied on the secondary display when this feature is enabled.</p>
<p>Added support for Brazilian ABNT2 keyboards (for Tera1 and Tera2 zero clients).</p>
<p>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 sections 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11 and 2.6.12.</p>

2.2.2 VDI Specific

Description
<p>Added support for SafeNet SC650 smart cards with SafeNet PKI applet and SHAC middleware (for Tera2 zero clients).</p>
<p>Added support for Atos CardOS smart cards.</p>
<p>Added support for eToken 72k Pro USB user authentication devices.</p>
<p>Added support for isochronous USB devices without a Video class interface connected behind a USB 2.0 hub.</p> <p>Note: A webcam is an example of an isochronous USB device with a Video class interface.</p>

2.2.3 Workstation Specific

Description
<p>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.</p>

Description
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 PColP MC. See section 2.6.13.

2.3 Important Bug Fixes

2.3.1 Workstation and VDI

Description
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.

2.3.2 VDI Specific

Description
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 PColP zero clients (for Tera1 and Tera2 zero clients).
Resolved an issue where the BASYS2 breadboard device does not function correctly with PColP zero clients (Tera1 and Tera2).
Resolved an issue where the USB certify scanner device fails to connect to a virtual machine when used with PColP zero clients (for Tera1 and Tera2 zero clients).
Resolved an issue where the Seal/O USB device may not function when the PColP 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).

2.3.3 Workstation Specific

Description
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.

2.4 Known Issues

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.

Table 2-1: Tera1 USB Device Modes

Tera1 Client			
	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 with a Video class interface (i.e. web cams); these devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All devices operate in their native mode (USB 1.1 or USB 2.0). Isochronous devices with a Video class interface are not supported (a warning overlay will appear).
Tera1 and Tera2 PCoIP Host Card	All devices operate in USB 1.1 mode		

Table 2-2: Tera2 USB Device Modes

Tera2 Client	
	EHCI Disabled (Devices operate in USB 1.1 mode only)

	<i>Root Port</i>	<i>Behind USB 1.1 and 2.0 Hub</i>	
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 following section for PCoIP host card behaviour.		
	EHCI Enabled (USB 2.0 support is enabled) - Default		
	<i>Root Port</i>	<i>Behind USB 1.1 Hub</i>	<i>Behind USB 2.0 Hub</i>
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 with a Video class interface (i.e. web cams); these devices operate in USB 1.1 mode.	All devices operate in USB 1.1 mode.	All devices operate in their native mode (USB 1.1 or USB 2.0). Isochronous devices with a Video class interface are not supported (a warning overlay will appear).
Tera1 PCoIP Host Card	All devices operate in USB 1.1 mode		
Tera2 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).

2.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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->Access Web Page

Access
Change administrative access settings

Disable Management Console Interface: ☐

Disable Administrative Web Interface: ☐

Force password change on next login: ☐

2.6.2 OSD Configuration->Access Options

Network	IPv6	SCEP	Label	Discovery	Session	Language	OSD	Display	Access	Reset
---------	------	------	-------	-----------	---------	----------	-----	---------	--------	-------

Change the administrative access settings

Disable Management Console Interface: ☐

Disable Administrative Web Interface: ☐

Force password change on next login: ☐

Unlock OK Cancel Apply

2.6.3 Configuration->SCEP Web Page

SCEP

Configure SCEP settings and retrieve certificates

SCEP Server URL:

Challenge Password:

Root CA:

Client Certificate:

Request Certificates

Status:

2.6.4 OSD Configuration->SCEP Options

Network	IPv6	SCEP	Label	Discovery	Session	Language	OSD	Display	Access	Reset
---------	------	------	-------	-----------	---------	----------	-----	---------	--------	-------

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

SCEP Server URL:

Challenge Password:

Root CA Certificate:

Client Certificate:

Status:

2.6.5 Configuration->Power Web Page

Power

Change the power settings

Screen-Saver Timeout: Seconds (0 = disabled)

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

Remote Host Power Control:

Power On After Power Loss: ☐

Enable Wake-on-USB: ☐

Enable Wake-on-LAN: ☐

2.6.6 OSD Configuration->Display Options

Network	IPv6	SCEP	Label	Discovery	Session	Language	OSD	Display	Access	Reset
---------	------	------	-------	-----------	---------	----------	-----	---------	--------	-------

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:

Preferred resolution 2:

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


Enable Display Cloning: ☐

Unlock OK Cancel Apply

2.6.7 Configuration->Session PCoIP Connection Manager Web Page

Note: The PCoIP Connection Manager can be used in the future to broker PCoIP sessions for Teradici solutions such as Arch Published Desktops.

Session
Configure the connection to a device


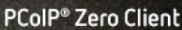


Session Connection Type: PCoIP Connection Manager
Server URI:

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: ☒

2.6.8 OSD Configuration->Session PColP Conn Mgr Options

Network	IPv6	SCEP	Label	Discovery	Session	Language	OSD	Display	Access	Reset
---------	------	------	-------	-----------	---------	----------	-----	---------	--------	-------

Configure the connection to a peer device

Connection Type:


Server URI:

Advanced

Unlock OK Cancel Apply

2.6.9 OSD Configuration->Session PColP Conn Mgr Advanced Options

Advanced Settings


PCoIP® Zero Client

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:

OK
Cancel

2.6.10 Configuration->Session PColP Conn Mgr + Logon Web Page

Session
Configure the connection to a device


PCoIP® Zero Client

Session Connection Type: PCoIP Connection Manager + Auto-Logon ▼
Server URI:
Logon Username:
Logon Password:
Logon Domain Name:


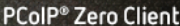
Desktop Name to Select:
Certificate Check Mode: Warn before connecting to untrusted servers ▼
Certificate Check Mode Lockout: ☐ Prevent users from changing the Certificate Check Mode
Auto Connect: ☐ Always connect to this server at startup
Connection Server Cache Mode: Last servers used ▼
Auto Launch 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: ☒

2.6.11 OSD Configuration->Session PColP Conn Mgr + Logon Options

Network	IPv6	SCEP	Label	Discovery	Session	Language	OSD	Display	Access	Reset
---------	------	------	-------	-----------	---------	----------	-----	---------	--------	-------

Configure the connection to a peer device

Connection Type:

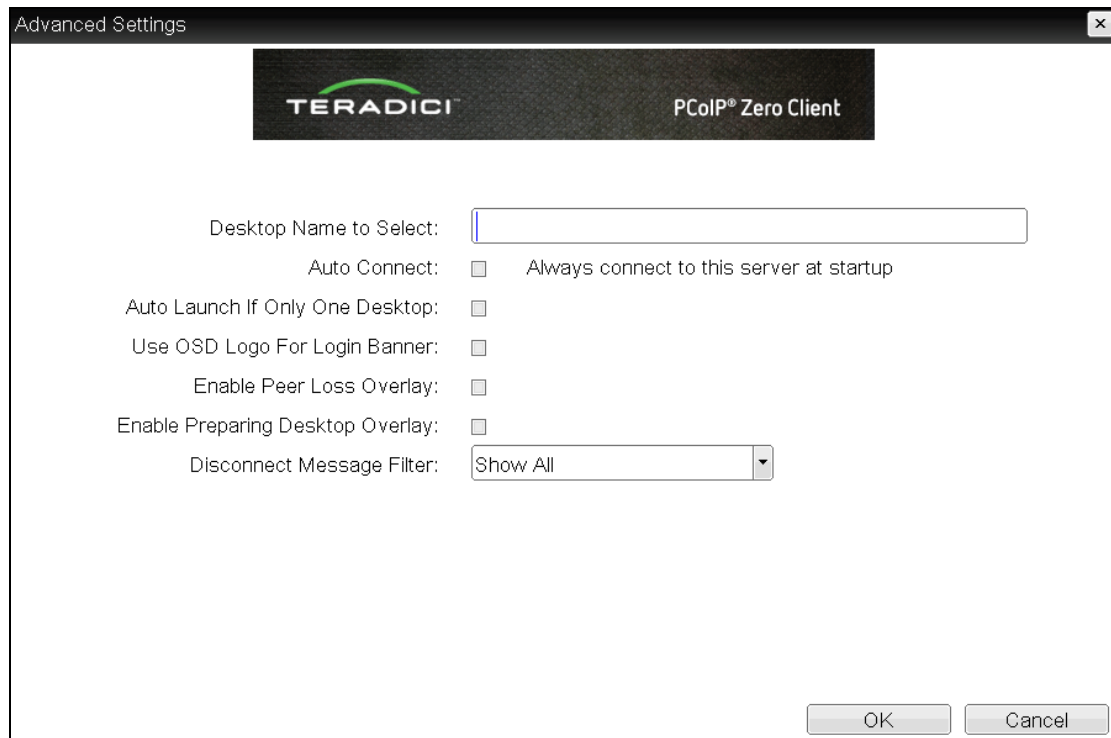
Server URI:

User name:

Password:

Domain:

2.6.12 OSD Configuration->Session PColP Conn Mgr + Logon Adv Options



Advanced Settings

TERADICI PColP® Zero Client

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: ☐

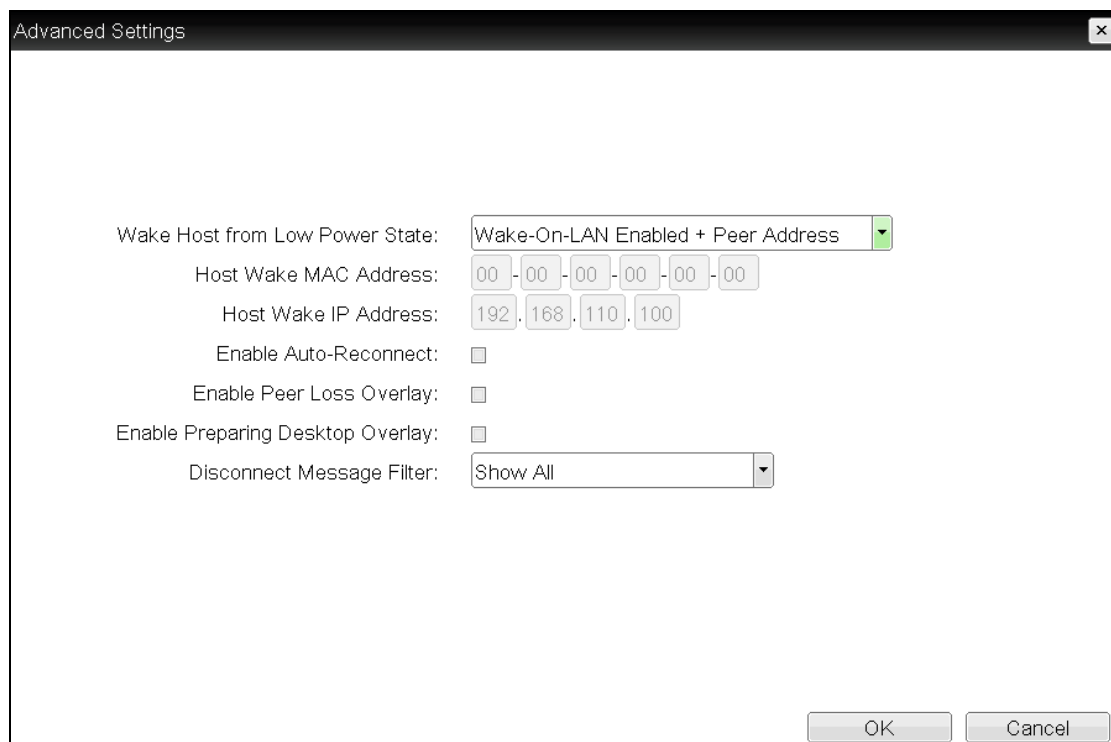
Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Disconnect Message Filter:

OK Cancel

2.6.13 OSD Configuration->Session Direct to Host Advanced Options



Advanced Settings

TERADICI Session Direct to Host

Wake Host from Low Power State:

Host Wake MAC Address:

Host Wake IP Address:

Enable Auto-Reconnect: ☐

Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Disconnect Message Filter:

OK Cancel

3 Release 4.0.3

This section provides a brief summary of the issues resolved in release 4.0.3 versus 4.0.2.

Note: Release 4.0.3 is only applicable to Tera2 zero clients and host cards.

3.1 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 host cards install release 4.0.3 on both the host card and zero client devices. Deployments using a mix of TERA1x00 and TERA2xxx endpoints should install release 4.0.3 on the 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 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.

3.2 Feature Additions

None

3.3 Important Bug Fixes

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Resolved a flash memory issue that could cause a TERA2xxx device to become inoperative and unrecoverable while updating configuration settings using PCoIP MC version 1.8.0.	Tera2	Tera2	Tera2
Resolved a potential memory corruption problem on TERA2xxx host cards, which could cause sessions to disconnect or workstations to crash.			Tera2

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Set the minimum firmware version equal to 4.0.3 for TERA2xxx devices, preventing downgrades.	Tera2	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		

3.4 Known Issues

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.

Table 3-1: Tera1 USB Device Modes

Tera1 Client			
	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, 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).

Tera1 and Tera2 PColP Host Card	All devices operate in USB 1.1 mode
--	-------------------------------------

Table 3-2: Tera2 USB Device Modes

Tera2 Client			
	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 PColP Host Card	The EHCI disable flag does not apply to the PColP host card. See following section for PColP 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).
Tera1 PColP Host Card	All devices operate in USB 1.1 mode		
Tera2 PColP 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).

3.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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.	✓	✓	✓

4 Release 4.0.2

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

Note: Tera2 endpoints with Release 4.0.2 must be upgraded to Release 4.0.3 or later in order to resolve a known issue where devices can potentially become non-functional and unrecoverable when managed by the PCoIP Management Console. Tera1 endpoints are not impacted. Please refer to section 3.3 Important Bug Fixes for additional details.

4.1 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 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 (4.0.2)
0.18 through 1.3	1) Install a 1.x firmware release (1.4 or later) 2) Install the new firmware (4.0.2)
1.4 through 4.0.1	Install the new firmware (4.0.2)

4.2 Feature Additions

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 5427 proximity reader.	✓		

4.3 Important Bug Fixes

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
Resolved an issue when using ATI FirePro RG220 and RG220A Remote Workstation Graphics (integrated GPU + PColP host card).			✓
Resolved an analog calibration issue with zero clients using the TERA2321 or TERA2140 with a DVI port (zero clients using only DisplayPort were not affected).	✓	✓	

4.4 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.	✓	✓	✓

Table 3-1 and Table 3-2 describe the mode USB devices connected to a zero client operate in based on device type, session type, and device configuration.

4.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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.	✓	✓	✓

5 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.

Note: Tera2 endpoints with Release 4.0.1 must be upgraded to Release 4.0.3 or later in order to resolve a known issue where devices can potentially become non-functional and unrecoverable when managed by the PCoIP Management Console. Tera1 endpoints are not impacted. Please refer to section 3.3 Important Bug Fixes for additional details.

5.1 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)

5.2 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.	✓	✓	✓
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 5.6.1.	✓	✓	
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 5.6.2.	✓	✓	✓
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 5.6.3.	✓		

5.3 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.	✓		
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).	✓	✓	✓

5.4 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.	✓	✓	✓

Table 3-1 and Table 3-2 describe the mode USB devices connected to a zero client operate in based on device type, session type, and device configuration.

5.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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.	✓	✓	✓

5.6 Supplemental Information

5.6.1 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: 10.200.2.37

Hide Advanced Options

Wake 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 encryption

Enabled Session Ciphers:

AES-128-GCM: ☒

Salsa20-256-Round12: ☒

Disconnect Message Filter: Show All

Apply Cancel

5.6.2 Configuration->SNMP Web Page

SNMP

Change the SNMP configuration

Enable SNMP: ☒

Community Name: public

Apply Cancel

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

Session Connection Type:	View Connection Server + Imprivata OneSign ▼
Bootstrap URL:	<input type="text"/>
<input type="button" value="Hide Advanced Options"/>	
OneSign Desktop Name Mode:	Ignore the Desktop Name to Select field ▼
Desktop Name to Select:	<input type="text"/>
OneSign Appliance Verification:	No verification: Connect to any appliance ▼
VCS Certificate Check Mode:	Warn before connecting to untrusted servers ▼
VCS Certificate Check Mode Lockout:	<input checked="" type="checkbox"/> Prevent users from changing the VCS Certificate Check Mode
Trusted View Connection Servers:	<input type="button" value="Show"/>
Login Username Caching:	<input checked="" type="checkbox"/>
Use OSD Logo for View banner:	<input type="checkbox"/>
Prefer GSC-IS:	<input checked="" type="checkbox"/>
Enable Peer Loss Overlay:	<input type="checkbox"/>
Enable Preparing Desktop Overlay:	<input type="checkbox"/>
Enable Session Disconnect Hotkey:	<input checked="" type="checkbox"/> CTRL + ALT + F12
Enable Proximity Reader Beep:	<input checked="" type="checkbox"/>
Session Negotiation Cipher:	Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption ▼
Enabled Session Ciphers:	<div>AES-128-GCM: <input checked="" type="checkbox"/></div> <div>Salsa20-256-Round12: <input checked="" type="checkbox"/></div>
Disconnect Message Filter:	Show All ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

6 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.

Note: Release 4.0.0 is only applicable to Tera1 zero clients and host cards.

6.1 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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)

6.2 Feature Additions

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
<p>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 6.6 and 6.6.2. Three modes are supported.</p> <ul style="list-style-type: none"> 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 <p>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 6.6.4.</p>	✓	✓	
<p>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 6.6 and 6.6.3. Two cipher settings are supported.</p> <ul style="list-style-type: none"> 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). 	✓	✓	✓
<p>Updated the OSD look and feel:</p> <ul style="list-style-type: none"> Revised color scheme Revised logo placement 	✓	✓	
<p>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 6.6.5.</p>		✓	
<p>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 6.6.6.</p>	✓	✓	

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 6.6.7 and 6.6.8.	✓	✓	
OSD enhancement: Add support for configuring the native resolution of each display when the display override feature is enabled. See section 6.6.9.	✓	✓	
OSD enhancement: Modified the display topology setting page. See section 6.6.10.	✓	✓	
OSD enhancement: Removed requirement to reboot zero client after changing display topology Rotation setting. See section 6.6.10.	✓	✓	
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 6.6.11. Note: This change affects deployments using PCoIP host cards configured to wake workstations from a low power state using Wake-On-LAN messages.		✓	

6.3 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 <i>PCoIP Management Console User Manual</i> (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.	✓	✓	

6.4 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		


6.5 Additional Collateral

Description	Zero Client (used with VMware View)	Zero Client (used with Host Card)	Host Card
See the latest <i>VMware View to PCoIP Zero Client Optimization Guide</i> (TER1003001) document for optimization guidelines for connecting PCoIP zero clients to VMware View virtual desktops.	✓		
See the latest <i>VMware View to PCoIP Zero Client WAN Network Guidelines</i> (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.	✓	✓	✓

6.6 Supplemental Information

6.6.1 Configuration->Session VCS Advanced Web Page

Session
Configure the connection to a device



Session Connection Type: View Connection Server
DNS Name or IP Address:

Hide Advanced Options

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: Show
Auto Connect: ☐ Always connect to this server at startup
Connection Server Cache Mode: Last servers used Clear cache entries

Enable Self Help Link: ☐
Auto Launch If Only One Desktop: ☐
Login Username Caching: ☒
Use OSD Logo for View banner: ☐
Prefer GSC-IS: ☒
Enable Peer Loss Overlay: ☐
Enable 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

Apply Cancel

6.6.2 VCS Certificate Check Mode Options

Port: (Leave blank for default)

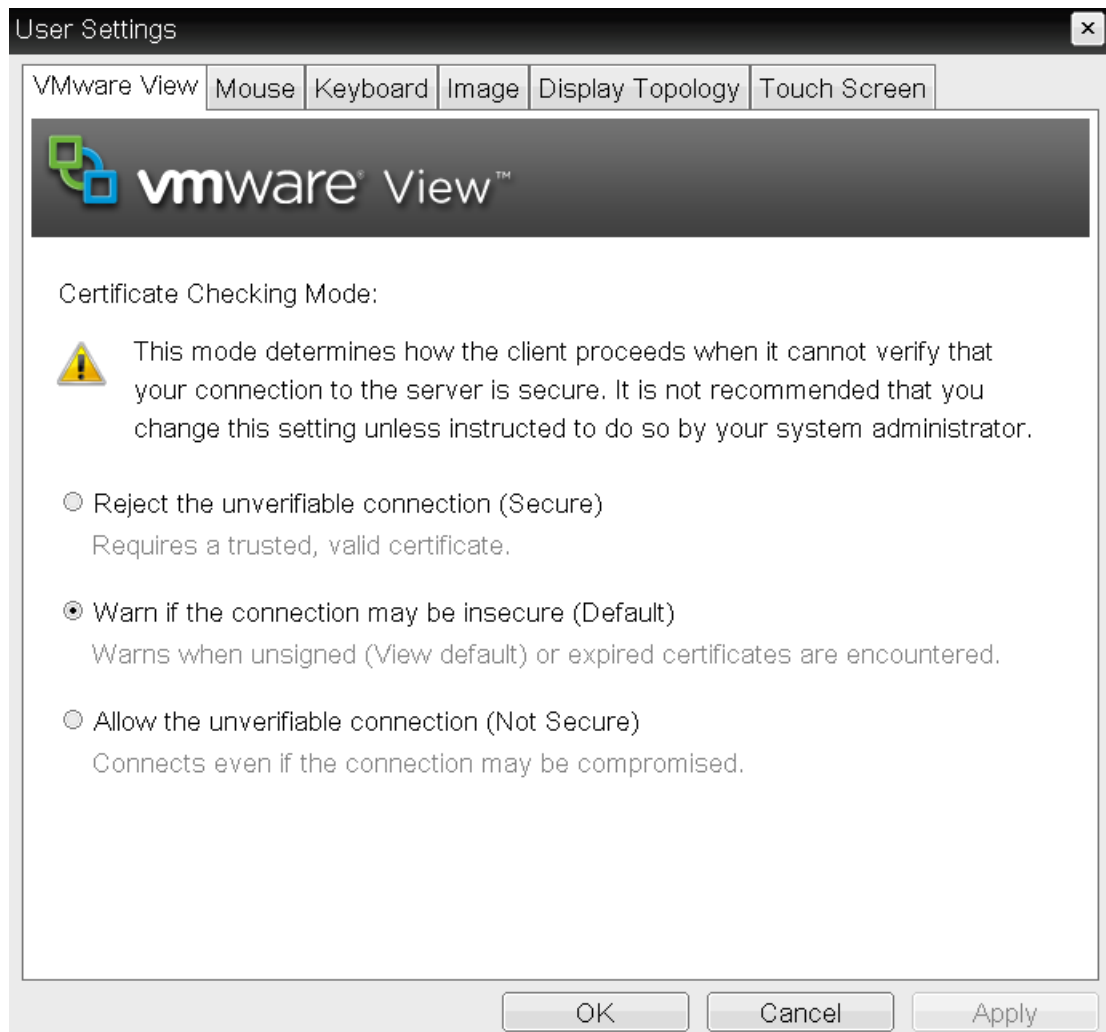
VCS Certificate Check Mode: Warn if the connection may be insecure (Default)
VCS Certificate Check Mode Lockout: Reject the unverifiable connection (Secure)
Warn if the connection may be insecure (Default)
Allow the unverifiable connection (Not Secure)

Trusted View Connection Servers: Show

6.6.3 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: ☒

6.6.4 OSD User Settings->VMware View Options



6.6.5 OSD Configuration->Session Direct to Host Advanced Options

Enable Auto-Reconnect:	<input checked="" type="checkbox"/>
Enable Peer Loss Overlay:	<input type="checkbox"/>
Enable Preparing Desktop Overlay:	<input type="checkbox"/>
Disconnect Message Filter:	Show All ▼

6.6.6 OSD Configuration->Session VCS Advanced Options

Configure the advanced View Connection Server settings for the device

Desktop Name to Select:	<input type="text"/>	
Port:	<input type="text"/>	Leave blank for default
Auto Connect:	<input type="checkbox"/>	Always connect to this server at startup
Remember Username:	<input checked="" type="checkbox"/>	
Auto Launch If Only One Desktop:	<input type="checkbox"/>	
Use OSD logo for View banner:	<input type="checkbox"/>	
Prefer GSC-IS:	<input checked="" type="checkbox"/>	
Enable Peer Loss Overlay:	<input type="checkbox"/>	
Enable Preparing Desktop Overlay:	<input type="checkbox"/>	
Disconnect Message Filter:	<input type="text" value="Show All"/>	

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

Configure the connection to a peer device

Connection Type:	<input type="text" value="View Connection Server + Auto-Logon"/>
DNS Name or IP Address:	<input type="text" value="192.168.48.18"/>
User name:	<input type="text"/>
Password:	<input type="password"/>
Domain:	<input type="text"/>

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

Configure the advanced View Connection Server settings for the device

Desktop Name to Select:	<input type="text"/>	
Port:	<input type="text"/>	Leave blank for default
Auto Connect:	<input type="checkbox"/>	Always connect to this server at startup
Auto Launch If Only One Desktop:	<input type="checkbox"/>	
Use OSD logo for View banner:	<input type="checkbox"/>	
Enable Peer Loss Overlay:	<input type="checkbox"/>	
Enable Preparing Desktop Overlay:	<input type="checkbox"/>	
Disconnect Message Filter:	<input type="text" value="Show All"/>	

6.6.9 OSD Configuration->Display Options

Configuration

Network

IPv6

Label

Discovery

Session

Language

OSD

Display

Reset

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

Unlock

OK

Cancel

Apply

6.6.10 OSD User Settings->Display Topology Options

User Settings

VMware View

Mouse

Keyboard

Image

Display Topology

Touch Screen

Configure the displays position, rotation and resolution

☒ Enable Configuration:

Display Layout: ☒ Horizontal ☐ Vertical

A

B

A

B

Alignment:

Top

Primary:	Port:	Position:	Rotation:	Resolution:
<input checked="" type="radio"/>	1	<div>A</div>	<div>No rotation</div>	<div>Native</div>
<input type="radio"/>	2	<div>B</div>	<div>No rotation</div>	<div>Native</div>

Revert

OK

Cancel

Apply

6.6.11 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

Hide Advanced Options

Wake host from low power state: Wake-On-LAN Disabled
Enable Auto-Reconnect: Wake-On-LAN Disabled
Enable Peer Loss Overlay: Wake-On-LAN Enabled + Peer Address
Enable Preparing Desktop Overlay: ☐ Wake-On-LAN Enabled + Custom Address

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

Apply Cancel