Using PCoIP® Zero Clients with VMware® View 4 User Guide

TER0904005

Issue 4

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
1	Jul 17, 2009	Initial Release
2	Oct 23, 2009	Update for VMware View 4
3	Dec 7, 2009	Update for PCoIP firmware release 3.0
4	Mar 12, 2010	Update for PCoIP firmware release 3.1.0 and View 4.0.1

Contents

Table of Figures

Definitions

Desktop	A physical or virtual desktop computer
FQDN	Fully Qualified Domain Name
OS	Operating System
OSD	On Screen Display on the PCoIP zero client
PC-over-IP®	Personal Computer over Internet Protocol
PCoIP Host	PCoIP PCIe add-in card for a PC or workstation
PCoIP zero client	PCoIP user side device, i.e. client.
PCoIP®	See PC-over-IP
Physical Desktop	A PC running Windows XP®, Windows Vista®, or Windows 7™
RDP	Microsoft® Remote Desktop Protocol
SSL	Secure Socket Layer (security protocol)
Virtual Desktop	A VM running Windows XP, Windows Vista, or Windows 7
VM	Virtual Machine

Introduction

This document describes the configuration and use of a PCoIP® zero client (or "client") e.g. PCoIP portal or PCoIP integrated display, with VMware View™. This document focuses on these clients with the firmware release 3.1.0 or newer installed. For a list of VMware Ready PCoIP zero clients, refer to:
`http://www.teradici.com/pcoip/pcoip-products/vmware-view-clients.php`

Detailed information on configuring VMware View or PCoIP Zero Clients can be found in the following documents:

- VMware View 4 Feature Support Matrix:
  `http://www.vmware.com/pdf/view401_architecture_planning.pdf`
- Getting Started with VMware View (EN-000276-00) available from
  `http://www.vmware.com/pdf/view40_quickstart.pdf`
- For additional VMware View documents see
  `http://www.vmware.com/support/pubs`

For a brief overview of using View 4 with PCoIP zero clients, refer to the VMware View 4 to PCoIP Zero Client Optimization Guide (TER1003001).

1 Overview

As a result of Teradici collaboration with VMware, VMware View 4 and newer incorporates PCoIP technology as the remote desktop protocol for virtual desktops, providing a significantly better user experience than is provided with other remoting protocols.

Packaged with VMware View 4 Agent installed in the virtual desktop, is a Teradici supplied PCoIP server executable which is launched and controlled by VMware View Agent under the direction of VMware View Manager. Packaged with the VMware View 4 Client is a Teradici supplied PCoIP client DLL which is launched by VMware View Client, and which establishes a PCoIP session with the PCoIP server running on the Virtual Machine guest.

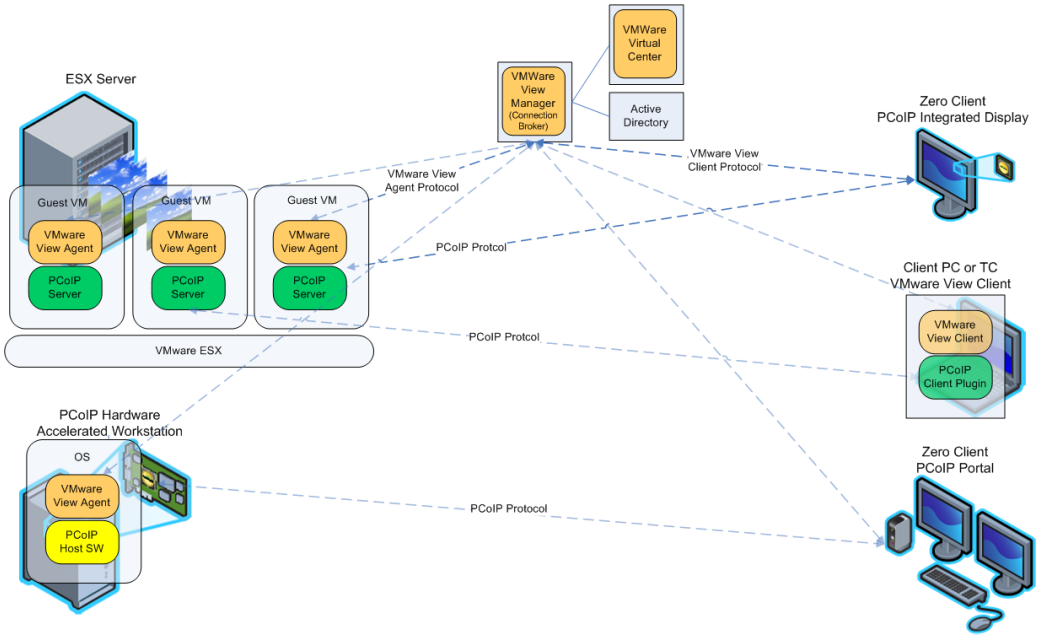
Coupled with the VMware View 4 release, Teradici provides firmware release 3.0 to enable interoperability of PCoIP zero clients with the PCoIP server installed with VMware View 4.

Administrators deploying VMware View 4 can now achieve all of the advantages of virtual desktop deployments with all of the advantages of the PCoIP protocol and with the manageability and performance advantages of PCoIP zero clients.

Additionally, VMware View managed PCoIP sessions can be established from PCoIP zero clients to workstations with PCoIP host add-in cards for full workstation class performance. While the client configuration steps are the same as described in this document, additional host side configuration steps are required and are not covered by this document.

The following diagram depicts the high level architecture of VMware View with PCoIP technology and PCoIP clients.

Figure 1-1: VMware View and PCoIP Technology Architecture



2 Prerequisites

This section describes the essential prerequisites required to use a PCoIP zero client with VMware View 4 and connect via PCoIP protocol to a virtual desktop.

1. VMware View 4.0.1
2. Firmware Release 3.1.0 for PCoIP zero clients

2.1 VMware View 4.0.1, or newer

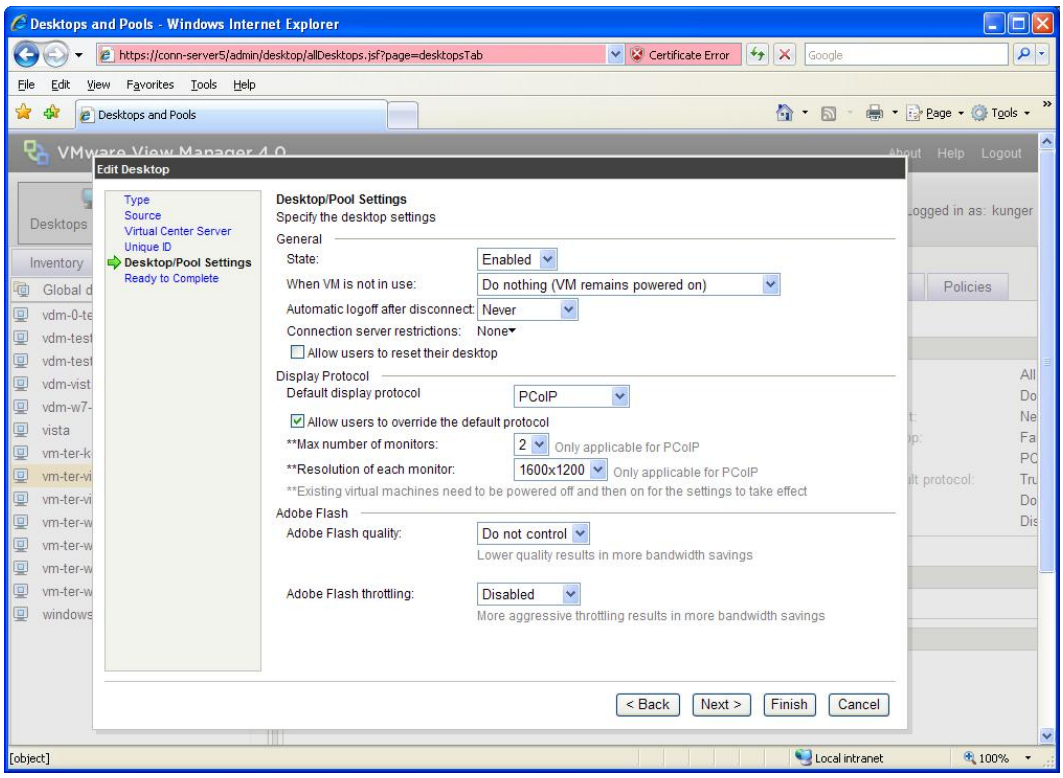
A VMware View 4 installation is required, consisting of the VMware View 4 Manager, and the VMware View 4 View Agent installed in the target virtual desktop (for more information, refer to VMware document *View Manager Administration Guide, View Manager 4.0*.

The PCoIP server is installed in the virtual desktop as part of the standard VMware View Agent install. PCoIP technology may be configured as the default remoting protocol, within the desktop settings in the VMware View Manager. The maximum display resolution and number of monitors should be also configured, as shown in Figure 2-1 below.

Note: When connecting, the client attempts to configure a resolution in the virtual desktop that matches the native resolution of the attached monitor(s), or failing that, a smaller valid resolution that the monitor supports. The PCoIP zero client supports only full-screen mode, as if your monitor were attached to the virtual desktop.

Note: When changing the number of monitors, or maximum resolution, the VM must be powered off in order for the modified settings to take effect.

Figure 2-1 Desktop Configuration in the VMware View Manager



2.2 Firmware Release 3.1.0

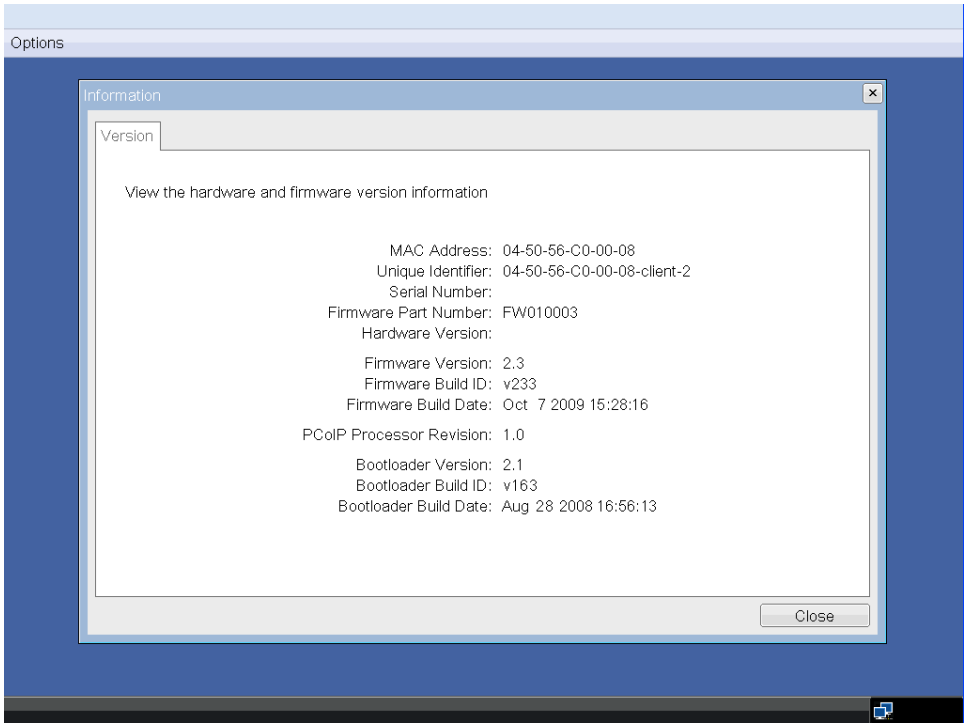
The functionality described in this document is available with firmware release 3.1.0 and later releases. Power on the client to verify the firmware release and be sure the client is using firmware release 3.1.0 or a later release. You can check the firmware version in the On Screen Display (OSD) or administrative web interface.

Checking Firmware Version Using the OSD

To check the firmware version In the OSD, click *Options* > *Information* > *Version*.

The example in Figure 2-2 shows the client is currently running firmware release 2.3, and the client will have to be updated to firmware release 3.1.0 or a later release.

Figure 2-2: OSD Version Tab

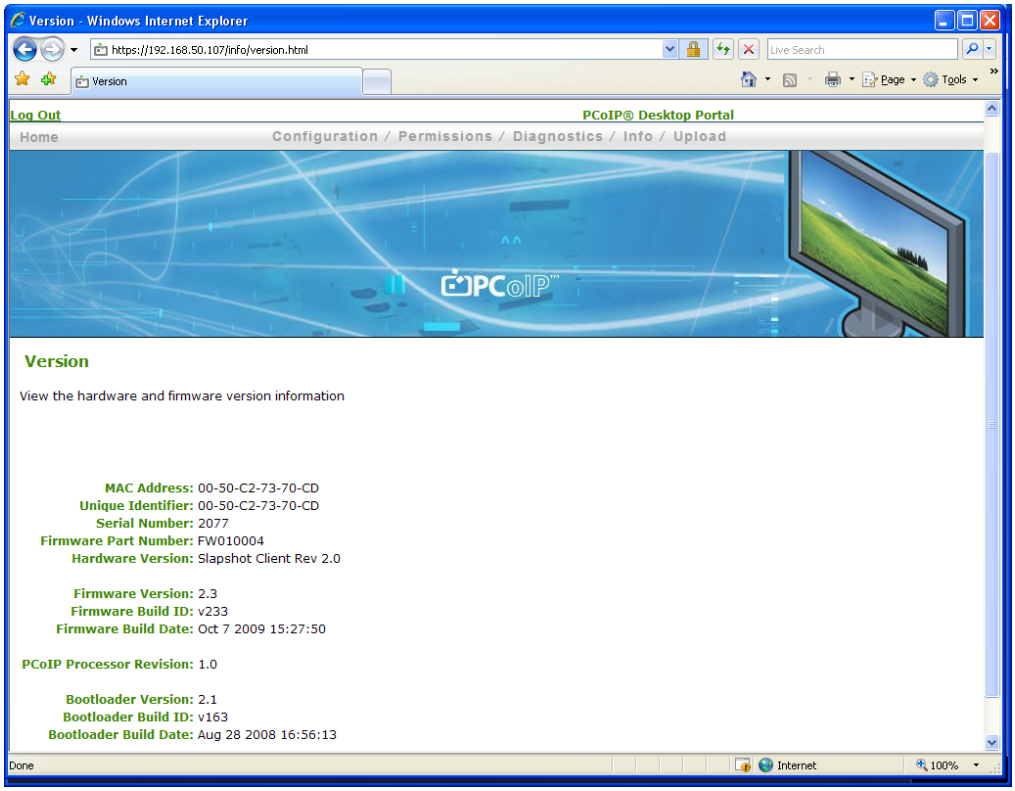


Checking Firmware Version Using the Administrative Web Interface

To check the firmware version in the Administrative Web Interface, enter the IP address of the client in a web browser and click *Info* > *Version* on the menu bar.

The example in Figure 2-3 also shows the client is currently running firmware release 2.3, and the client will have to be updated to firmware release 3.1.0 or a later release.

Figure 2-3: Administrative Web Interface Version Webpage



Updating PCoIP Firmware

Firmware can be updated via the client's Administrative Web Interface (see TER0606004 PCoIP Administrative Interface User Manual), the PCoIP Management Console (see TER0812002 PCoIP Management Console User Guide) or other tools such as connection brokers. If you do not have firmware release 3.1.0, contact your PCoIP zero client supplier.

Example Administrative Web Interface Firmware Upload Process:

1. Log into the zero client admin interface, e.g. 192.168.1.100 (accepting certificates and using password if enabled)
2. Select the *Firmware Upload* webpage Browse button to browse to the firmware ".all" file, e.g. tera1x00_rel3-1-0_v265.all
3. Select the File Upload window *Open* button
4. Select the webpage *Upload* button
5. Select the webpage *OK* button on the warning window that reads, *Are you sure? This will upload a new firmware image. This operation may take a few minutes.*
6. Wait for the firmware upload to complete. The following message appears when complete: *Success Flash successfully programmed! You must reset the device for the changes to take effect.*
7. Select the *Reset* button.
8. Select the *OK* button when the following message appears: *The PCoIP processor will reset immediately. Are you sure you want to proceed?*
9. Wait for zero client to restart

3 VMware View Configuration for PCoIP Zero Client

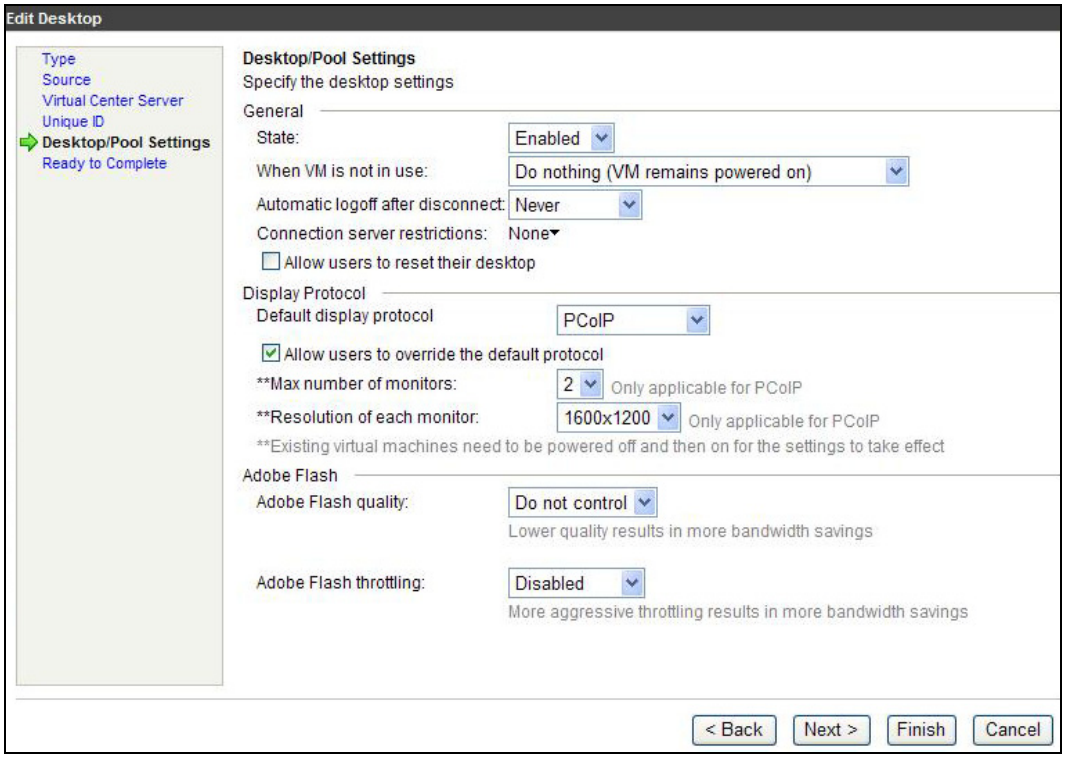
VMware View 4.0 enables use of the PCoIP protocol when connecting to virtual desktops. This section highlights VMware View configuration to use PCoIP zero clients.

3.1 Configuring Monitor Resolutions

When using the zero client, View must be configured for the maximum resolution for the attached monitors. In View Manager, configure the *Resolution of each monitor* parameter to reflect the attached displays. If this in incorrectly configured, the desktop may not be displayed.

Figure 3-1 below shows the *Resolution for each monitor* configured to 1600x1200.

Figure 3-1: VMware View Administrator: Edit Desktop - Display Configuration



3.2 vCPU Recommendation

The default setting for a VMware View virtual desktop is 1 vCPU. The virtual desktop should be configured to use 2 vCPUs for viewing videos greater than 480p (e.g. 720p or 1080p HD videos).

3.3 Adobe Flash Configuration

To optimize the user experience when using a zero client, it is recommended to ensure the following are configured under the Adobe Flash parameters (see Figure 3-1):

- Set *Adobe Flash quality* to *Do Not Control*
- Set the *Adobe Flash throttling* to *Disabled*

3.4 Uninstall Thin Print

Uninstall ThinPrint for the virtual desktop using the View Agent installer since ThinPrint uses CPU cycles even though the zero clients do not support this feature.

3.5 Disable MMR

Disable Multimedia Redirect (MMR) for the desktop policy (globally or per desktop) since MMR uses CPU cycles even though the zero clients do not support this feature.

4 PCoIP Zero Client Configuration for VMware View

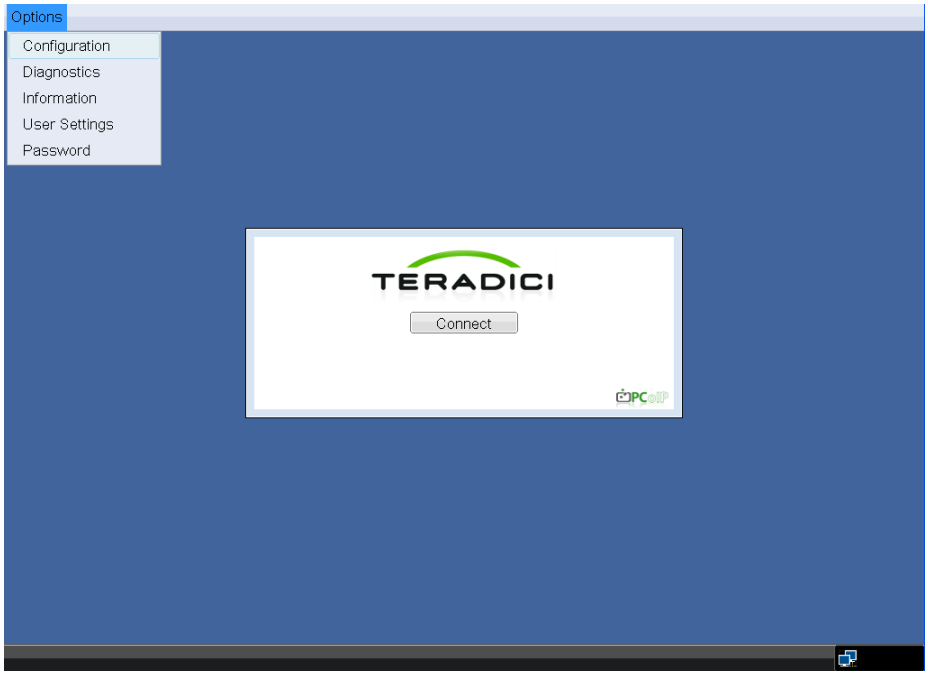
VMware View Client functionality is integrated into PCoIP zero client firmware. In firmware release 2.2 this functionality was restricted to the use of RDP when connecting to a virtual desktop. Beginning with firmware release 3.0, this functionality includes support for connecting via the PCoIP protocol to the PCoIP server controlled by the VMware View Agent in the desktop.

This feature is configured using the *VMware View* tab in the OSD of the client. When this feature is properly configured, users can connect to a VMware View Connection Server, which returns a list of available virtual desktops, or desktop pools, and the user can connect to desktop using the PCoIP protocol or RDP.

Note: The settings for VMware View with PCoIP technology can also be configured using the administrative web interface. For more information, please refer to the TER0606004 Administrative Web Interface User Manual.

This guide contains step-by-step instructions that describe how to configure the settings in the *VMware View* tab in the OSD and to establish a connection to a desktop. After powering on the client, the OSD appears on your monitor. To access the *VMware View* tab, click *Options* in the top left corner of the OSD and click *Configuration*, as shown in Figure 4-1.

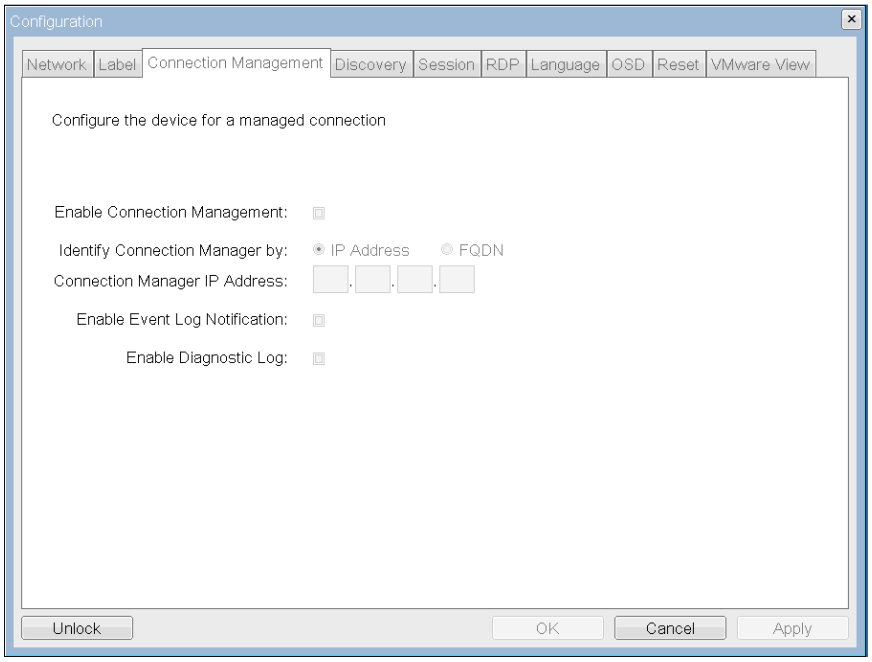
Figure 4-1 OSD on a PCoIP Zero Client



4.1 Disabling Connection Management

The settings in the *VMware View* tab, as shown in Figure 4-3, are not configurable if the *Enable Connection Management* option is enabled in the *Connection Management* tab, as shown in Figure 4-2. The Connection Management support is used by other connection brokers for non-VMware View deployments; hence is not compatible with VMware View. Click the *Connection Management* tab, and ensure that *Enable Connection Management* is disabled.

Figure 4-2 Disable Connection Management

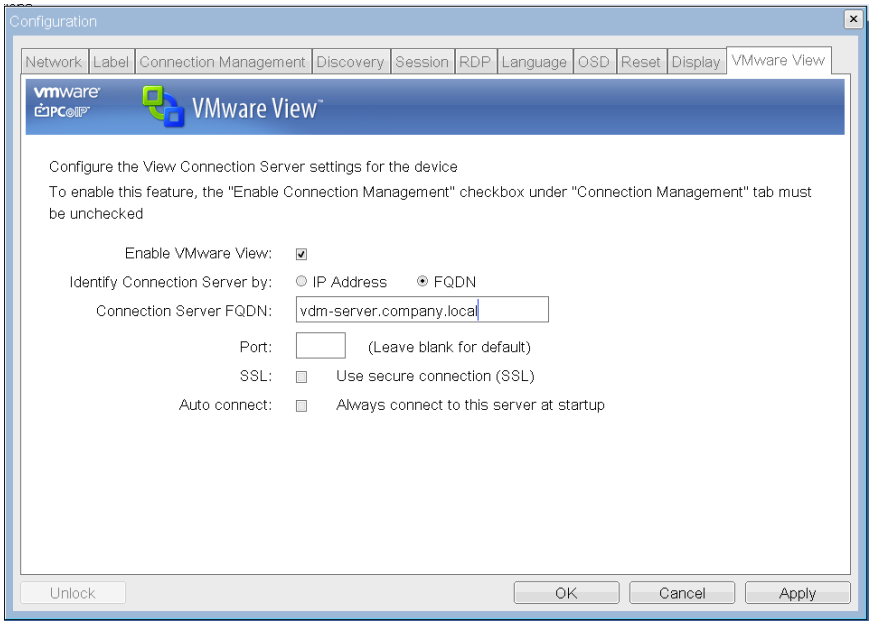


4.2 Configuring the VMware View Connection Server

Click the *VMware View* tab in the OSD Configuration Window to enter the settings required to connect to a VMware View Connection Server. If the client is password protected, click the *Unlock* button and enter the device's password. If the client is not password protected, *Unlock* button will not appear.

Details of the VMware View parameters are outlined below.

Figure 4-3 VMware View Tab



Enable VMware View

To connect the client to a VMware View Manager, enable the *Enable VMware View* option.

Connection Server IP Address/ Connection Server FQDN

Depending on which *Identify Connection Server by* option selected, enter the connection server IP address or the Fully Qualified Domain Name (FQDN). In this example, the *FQDN* option is selected and the FQDN of the View Connection Server, `vdm-server.company.local`, is entered into the *Connection Server FQDN* field.

Port

If *SSL* is enabled and the *Port* number is blank, port 443 will be used. By default, the *Port* field is blank.

If *SSL* is disabled and the *Port* number is blank, port 80 will be used. By default, the *Port* field is blank.

If *Port* number and SSL settings are not entered properly an error message may pop up and prevent you from connecting to a VMware View Connection Server.

Note: If the entered port number matches the default port number, the next time the *VMware View* tab is viewed the *Port* number field will be blank.

SSL

The SSL setting is configurable in both the VMware View Connection Server and in the client's *VMware View* tab. The SSL setting in the VMware View Connection Server is the master setting that overrides the local setting in the client. Based on how the SSL setting is configured in the VMware View Connection Server and in the *VMware View* tab, the resulting SSL mode that will be used is shown in Table 4-1. For example, if SSL is enabled in the VMware View Connection Server but is disabled in the *VMware View* tab, the resulting SSL mode is enabled.

By default, the *SSL* field is blank.

Note: For security it is highly recommended to use Port 443 and enable SSL in the *VMware View* tab and in View Connection Server, as the authentication password to the View Connection Server is not encrypted when the resulting SSL mode is disabled. With SSL disabled, the user's login password is not encrypted and can be captured using network protocol tools. When using SSL, it is suggested that the SSL setting be configured on the View Connection server (master) to ensure the SSL is used regardless of the client's *SSL* field configuration.

Table 4-1 SSL Mode Matrix

		VMware View Connection Server	
		SSL disabled	**SSL enabled**
***VMware View* tab**	**SSL disabled**	SSL disabled	SSL enabled
	SSL enabled	View Connection Server communication error	SSL enabled

Auto connect

When *Auto connect* is enabled, the client will automatically connect to the VMware View Connection Server whenever the client powers up or when a session with the virtual

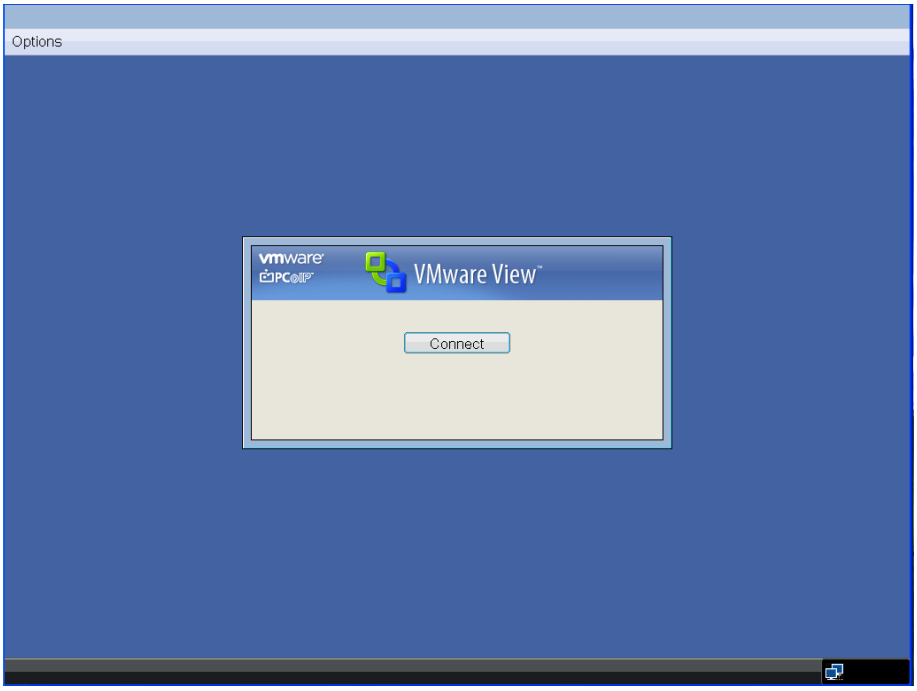
desktop is terminated, and the user sees the user credentials login dialog box on the OSD instead of the Connect dialog box

After enabling auto connect, the client must be power-cycled for the change to take effect.

Apply

Click *Apply* to accept the settings. The client connect dialog will now display the VMware View banner as shown in Figure 4-4 below.

Figure 4-4 PCoIP Zero Client OSD with VMware View Enabled



5 Connecting to a VMware View Managed Desktop

The following describes the step-by-step instructions to connect to a VMware View managed desktop.

1. Connecting to the VMware View Manager

When VMware View is enabled, the OSD switches to VMware View mode allowing connection to VMware View Manager and configured desktops. Click *Connect* to initiate a connection to VMware View Manager.

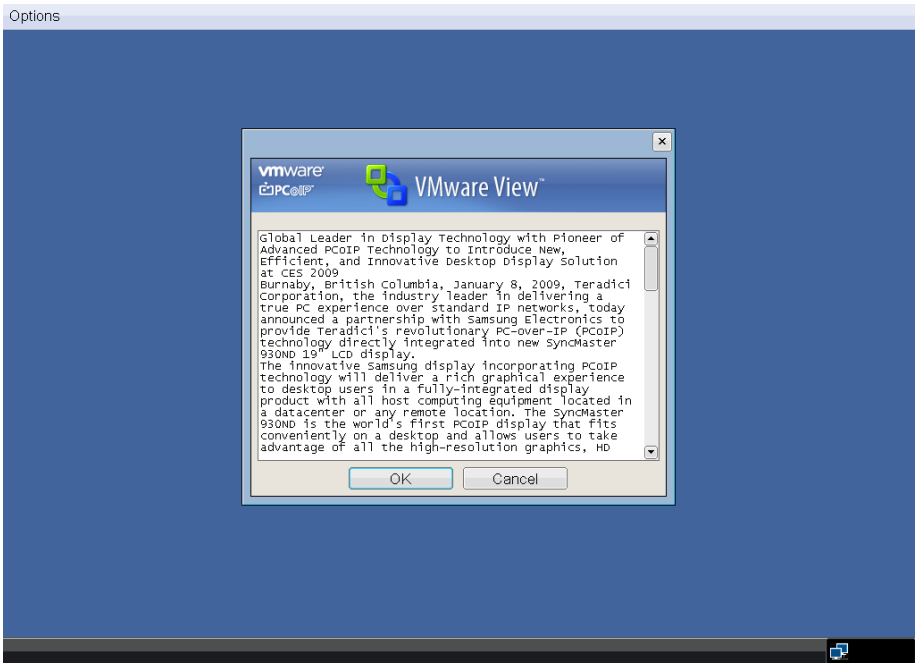
Note: When the *Auto connect* feature is enabled (see Section 4.2), the Connect screen shown in Figure 4-4 will not be used and clicking the *Connect* button is not available. Instead, the zero client auto connects with the View Connection Server and you see either a disclaimer or login dialog box.

2. Accepting the Disclaimer

Once connected to VMware View Manager, a disclaimer may appear, if configured in the VMware View Manager. After reviewing the disclaimer, click *OK* to accept.

Note: The disclaimer is optional and its content depends on what the administrator entered into the VMware View Manager.

Figure 5-1: Disclaimer



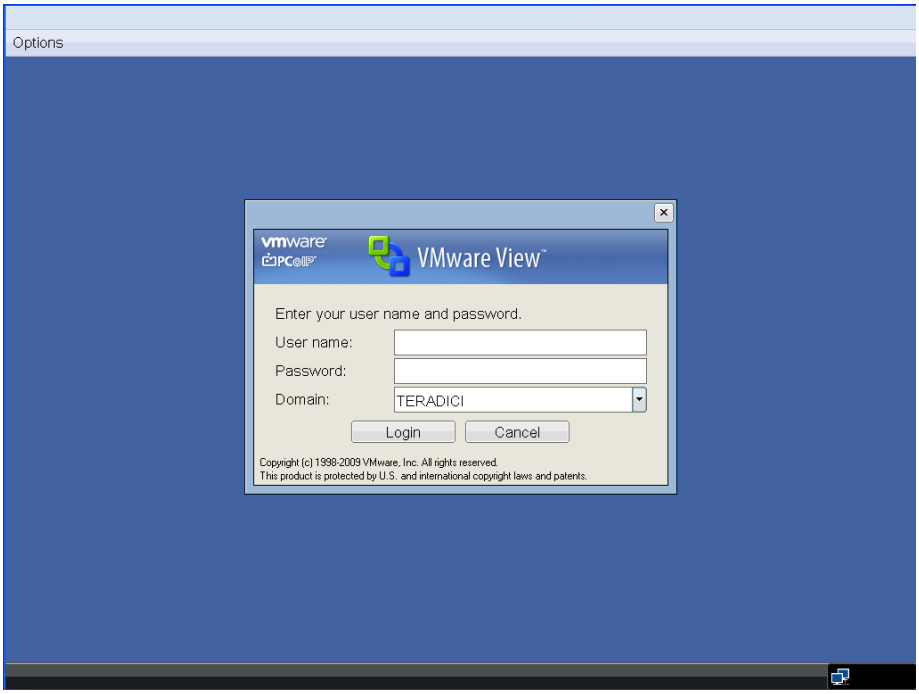
3. User Authentication

Enter user name and password, and select a domain from the drop down menu in the authentication window. Click *Login*.

Note: The last user name used during login will be shown as the default.

Note: The domains are detected automatically and up to 100 domains are shown. The last domain logged in will be shown as the default.

Figure 5-2 User Authentication



4. Desktop Selection

Once authentication is complete, the list of desktops or desktop pools configured by the VMware View Manager administrator appears. For each entry, the name of a desktop or a desktop pool shows on the left, and the status of a desktop or a desktop pool shows on the right. This window contains up to 10 desktops. The status field can be one of the following:

User Not In Session – User is not logged on to a desktop

User In Session – User is logged on to a desktop

Note: The session status on each listing reports only the log-on status for the user. However, it does not report whether other users are logged on to a desktop. For example, assume User A is using a desktop called “Desktop 3”. When another user, User B, logs on to the same domain and VMware View Connection Server, User B sees “Desktop 3” as “User Not In Session” because VMware View reports the log-on status for only User B even though user A is using “Desktop 3”.

This Desktop Selection window, allows following actions:

Connect – Connect to an available desktop or desktop pool / Resume the session to a desktop

Reset VM – Reset a VM (the Reset VM button is only active for the user logged on to that VM, otherwise it is grayed-out)

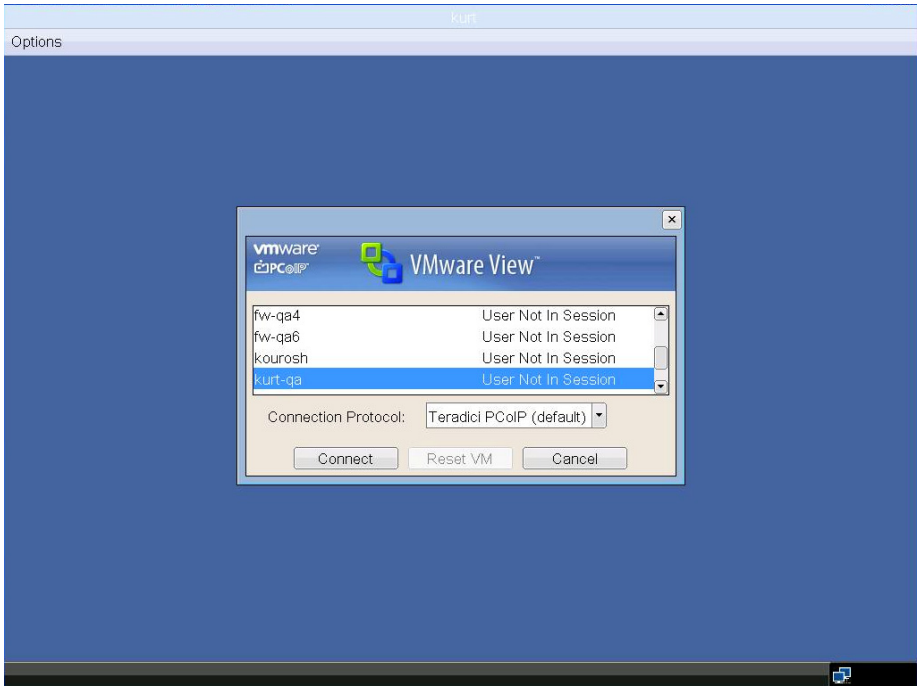
Cancel – Return to the Connect Screen as shown in Figure 4-4.

The protocol selection, provided below the list of desktops, allows the user to select either *PCoIP* protocol or *RDP* when connecting to the selected desktop. For best user experience, use PCoIP protocol.

To connect to a desktop, select it from the listing, select the protocol to use, and click *Connect*. The user can then connect to the desktop unless another user is currently logged on to it or it is unavailable.

Note: A PCoIP zero client only uses full-screen connections.

Figure 5-3 Desktop Selection



5. Disconnecting from a desktop

While the user is connected to a Windows® virtual desktop, the user can Log Off from Windows session. This will disconnect the PCoIP session and return to the client display OSD. Within VMware View, the status of the desktop becomes *User Not In Session.*

The user can also disconnect from the desktop using the client's disconnect button, which keeps the user logged in but locks the desktop. Within VMware View, the status of the virtual desktop the user disconnected from is *User In Session.* After disconnecting, the client displays the OSD. The user can resume the session to the desktop by selecting it and clicking *Connect*.

6 Firmware Release 3.1.0 Known Issues, Troubleshooting and FAQ

This section outlines known issues, troubleshooting and frequently asked questions relating to firmware release 3.1.0 when connecting to a View 4.0.1 virtual desktop.

Please also refer to the VMware View Manager 4.0.1 Release Notes for View 4.0.1 information:

http://www.vmware.com/support/view40/doc/releasenotes_viewmanager401.html

6.1 Known Issues

This section provides a brief summary of the current issues and limitations of PCoIP zero clients running firmware release 3.1.0 and connecting to a VMware View 4.0.1 virtual desktop using the PCoIP protocol.

6.1.1 Default Encryption Mode May Limit Desktop Performance

There are two encryption options when the client is connected to a View 4 virtual desktop, AES-128 and SALSA20-256. SALSA20-256 provides the best performance due to the lighter decryption load compared to the AES-128.

When using the default AES-128 bit encryption (and more than about 5 Mbps is available on the network) desktop experience may be reduced. To improve performance, SALSA20-256 may be optionally chosen.

To use SALSA20-256 with VMware View 4 General Release, SALSA20-256 must be enabled. This can be done using the client administrative web interface:

- Log into administrative web interface, e.g. https://192.168.1.100
- Menu option *Configuration* > *Session*
- Uncheck *Enable AES-128-GCM* (disable)
- Check *Enable Salsa20-256-Round12* (enable)
- Select *Apply*

6.1.2 No Isochronous USB Support

PCoIP firmware release 3.1.0 does not support isochronous USB when connected to a View 4 desktop.

Isochronous USB will be supported in a future firmware release. Alternatively for full isochronous support, the PCoIP zero client can be connected to a hardware accelerated PCoIP workstation host (blade PC, rack workstation, etc.).

6.1.3 No Support for Mouse Pointers that Require Background Inversion

Firmware release 3.1.0 does not support background inversion pointers.

6.1.4 No Audio Input

VMware View 4.0.1 does not support audio input. Audio input will be supported in a future release of View.

Alternatively, the PCoIP zero client can be connected to a hardware accelerated PCoIP workstation host (blade PC, rack workstation, etc.) for audio input support.

6.1.5 Dual Display Orientation

Dual display notes:

- In dual display mode, DVI#1 display must be to the left of DVI#2
- Only non-rotated landscape display orientation is currently supported (rotated displays will be supported in the future)

6.1.6 Experimental Smart Card Support

Firmware release 3.1.0 added experimental support for pre-session secure user authentication via Smart Card. Requirements:

- USB connected card readers including: SCR331, Omnikey 3121, Dell keyboard SK3205
- CAC cards
    - GSC-IS v2.0 and v2.1 java (virtual machine) cards
    - Registered data model of 2.
    - Digital signature certificate required (PIX=0100)
        - Key usage set to digital signature and key encipherment
        - Key length no larger that 2048 bits
- View 4.5 and above hosts

6.1.7 Issues with pointers greater than 220x218 pixels

Firmware release 3.1.0 improves handling of large pointers in View 4.0.1, but a future release of View is required to handle pointers greater than 220x218 pixels.

It is recommended users use pointers smaller than 220x218 in View 4.0.1.

6.2 Troubleshooting

Troubleshooting of PCoIP zero client to virtual desktop PCoIP connections is nearly identical to troubleshooting View Client connections. Users should first consult VMware View support documentation. Users should also consult Section **Error! Reference source not found.** and the release notes for firmware release 3.1.0 for known bugs and product limitations.

This section outlines some common issues and suggested solutions.

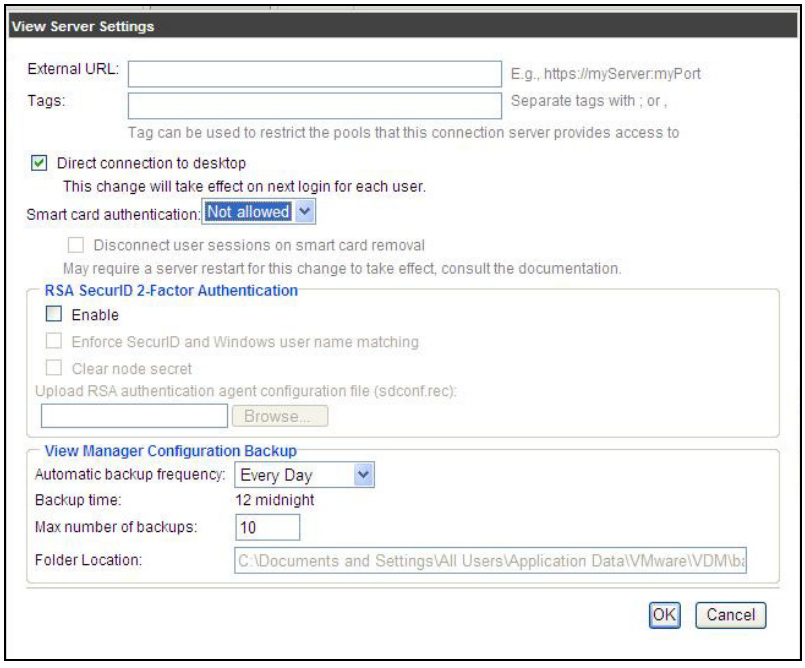
Table 6-1: Troubleshooting

Item	Description	Solution
1	Can not get monitor to display virtual desktop.	Check the desktop configuration in the View Manager, to ensure that PCoIP

		protocol is enabled. Ensure that the display resolution setting for the desktop is configured large enough to support at least one valid monitor configuration. It is suggested that the display resolution setting be configured large enough to support the native resolution of the monitor. Ensure that the VM has enough VRAM to support the display resolution. Note: When changing the desktop display resolution setting in the View Manager, the VM must be powered off for the changed settings to take effect.
2	Monitor does not display proper screen resolution on PCoIP session connect.	The following display resolutions are supported by firmware release 3.0 (assuming that the attached monitor supports). Setting arbitrary display resolutions in the Windows control panel can result in a failed connection. • 640 x 480 • 800 x 600 • 1024 x 768 • 1280 x 800 • 1280 x 1024 • 1440 x 900 • 1600 x 1200 • 1680 x 1050 • 1920 x 1080 • 1920 x 1200
3	Second monitor does not work.	Check the following: • When creating VM (template or Parent VM), disable Auto-detect video settings in the video card settings (refer to View 4 release notes) • VMware View configured for dual display • Both displays monitors attached properly to client
4	Audio not functioning after enabled in administrative web interface.	Changes made to the PCoIP audio enable in the administrative web interface are not recognized when the change is made while the PCoIP Portal is connected to a View 4 VM session. Ensure the client is not connected to a View 4 VM when making changes to the audio enable setting.
5	Changes made on session variables are not working.	The View 4 host supports multiple PCoIP session variables that affect how a PCoIP session operates (bandwidth, USB

		authorization, etc.). Ensure the client is not connected to a View 4 VM when making changes to the session variables.
6	Zero client can't connect to View Manager	A) Verify that the zero-client can ping the View Manager. In the OSD under Options->Diagnostics->Ping. A) In the View Manager, is the customer adding their own certificates? They do by adding a "locked.properties" file to the View Manager. • Ensure *Smart card authentication* not set to *Not allowed* (rather than *Optional*) • If using a certificate with extended validation and a 2048 bit key, then must use firmware release 3.1.0. Otherwise remove the use of the custom certificate in View Manager.

Figure 6-1: View Server Settings: Smart card authentication: Not allowed



6.3 Frequently Asked Questions

6.3.1 Which PCoIP zero clients work with VMware View?

The table below lists PCoIP zero clients compatible with VMware View.

Note: Refer to the VMware hardware compatibility list for an up-to-date list of PCoIP zero clients that are VMware Ready certified (www.vmware.com/go/hcl).

Manufacturer	Model(s)
Amulet Hotkey	DXR-iP Ultra-compact PC-over-IP Portal DXR2-iP Dual-head PC-over-IP Portal DXR4-iP Quad-head PC-over-IP Portal
ClearCube Technologies	I9420 I/Port
Dell	FX100 Remote Access Device
Devon IT	TC10 Desktop Access Device
ELSA Japan	VIXEL D200 Portal
EVGA	PD01 Desktop Portal
Fujitsu Technology Solutions	CELSIUS RemoteAccess Portal Device
Leadtek Research	WinFast® VP200 P Portal Device
IBM	CP20 Workstation Connection Device
Samsung	SyncMaster 930ND 19” integrated LCD Monitor SyncMaster NC190 19” integrated LCD Monitor SyncMaster NC240 24" integrated LCD Monitor
Verari Systems®	CNX0102 Connexxus™ Desktop Device
WYSE	P20 Zero Client

6.3.2 What are the minimum and maximum bandwidth requirements for PCoIP sessions within VMware View?

The expected bandwidth range is 100 kbps to 20 Mbps (peak) in a bandwidth unconstrained network environment. An idle session may generate as low as 10 kbps.

PCoIP technology adapts the peak bandwidth used in response to congestion detection, as indicated by packet loss. Higher peak bandwidth availability provides for improved user experience. Administrators may limit the peak bandwidth that the PCoIP server generates through GPO settings as described in VMware View documentation.

Be sure that there is sufficient bandwidth available on the network

- The bandwidth used between a View 4 virtual desktop and a PCoIP Zero Client depends on the activity on the users display (eg. Simple forms entry screens vs 720p video). A typical desktop using Microsoft Office applications can use an average of 100 - 200kbps.
- Provision the network with a minimum bandwidth of 512kbps per user. Note that the actual bandwidth used will depend on the activity on the user display and will be as low as 10kbps for a static user display.
- For more demanding desktop environments, consider increasing the minimum network bandwidth available.

6.3.3 What latency is supported?

Typically up to 250 ms of latency can be support by View 4 systems using the PCoIP protocol.

6.3.4 Can PCoIP technology be used to remote a desktop over the WAN?

Yes, the PCoIP protocol can be used over the WAN (Wide Area Network) or Internet. Typically, a VPN connection will be required to connect to the enterprise network. Over longer network latencies, the PCoIP protocol can provide for a significantly better user experience than is provided with RDP.

6.3.5 What is the maximum display resolution supported?

The maximum resolution supported is 1920x1200 per display.

6.3.6 What is the maximum number of displays supported?

PCoIP zero clients currently support up to 2 displays when connecting to a View 4.0.1 virtual desktop.

Note that some PCoIP zero clients can support up to 4 displays when connected to a dedicated remote workstation with hardware PCoIP protocol acceleration.

6.3.7 What USB devices are supported?

Firmware release 3.1.0 will support interrupt (e.g. HID devices) and bulk USB devices. Support for isochronous (e.g. web cams) for PCoIP zero clients will be introduced in later releases of VMware View and PCoIP firmware.

Users may come across some USB functionality issues in firmware release 3.1.0, including:

- Possible issues with programmable USB devices such as iPhones and Blackberry devices.

Note that VMware View 4.0.1 provides enhanced USB support which now includes support for multi-function keyboards such as Bloomberg keyboards

6.3.8 What audio inputs/outputs are supported?

The VMware audio driver included with View 4.0.1 supports audio output only. Audio input will be added in a future View release and associated PCoIP firmware update.

6.3.9 Can VMware View be used to connect PCoIP zero clients to dedicated remote workstations?

Yes, VMware View can be used to broker PCoIP zero clients to both Virtual Desktops and PCoIP enabled workstations and PCs with the PCoIP add-in card installed. See Figure 1-1. (Details are provided in separate documentation.)

6.3.10 What port numbers are used with the PCoIP protocol?

Port numbers used depend on the PCoIP endpoints used.

For PCoIP zero client to PCoIP host add-in cards connections, the PCoIP protocol uses the following ports:

Table 6-2: PCoIP Zero Clients to PCoIP Add-In Cards Port Numbers (not view brokered)

TCP	21, 80, 427, 443, 50000, 50001, 4172
UDP	9, 53, 67, 68, 427

For PCoIP zero clients and View Clients (software PCoIP protocol) to View connections, the PCoIP protocol uses the following ports (firmware release 3.1.0):

Table 6-3: PCoIP Zero Clients and View Clients to View Port Numbers

TCP	4172 or 5xxxx (as negotiated by View Connection Server)
UDP	4172 or 5xxxx (as negotiated by View Connection Server)

6.3.11 Are smart cards supported?

Firmware release 3.1.0 provides experimental smart card support.

Smart card will be supported in a future release. Alternatively, the client can be connected to a PCoIP hardware accelerated workstation host (blade PC, rack workstation etc) for post-session smart card support.

6.3.12 Does the zero client use Direct Connect mode in View?

By default the View Manager disables Direct Connect mode for RDP and PCoIP sessions. The PCoIP zero client firmware overrides the View Manager setting by enabling Direct Connect for RDP and PCoIP sessions. The PCoIP zero client establishes RDP and PCoIP sessions in Direct Connect mode and the tunnel is bypassed.

6.3.13 How do I change the screen resolution?

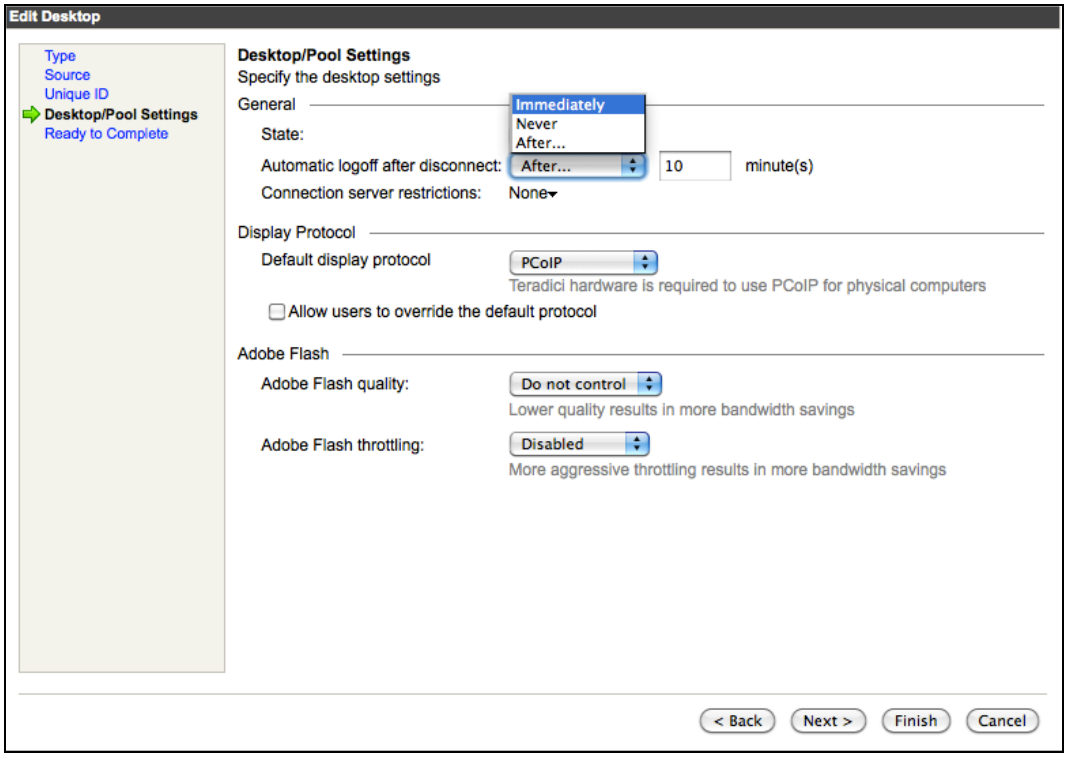
Windows Display Properties was disabled by View to minimize incorrect configuration. If desired, this can re-enabled by:

- Run: regedit
- Go to: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
- Find the REG_DWORD type: NoDispSettingsPage
- Set NoDispSettingsPage to 0.

6.3.14 Can a user be automatically logged off a VM after a session is disconnected?

Users can be automatically logged off a VM after a session is disconnected by configuring the *Automatic logoff after disconnect* in View Manager to *Immediately* or *After…*.

Figure 6-2: Edit Desktop - Automatically logoff after disconnect



6.3.15 What operation systems are supported?

Virtual desktops with Microsoft Windows XP or Vista installed. Support for Windows 7 in View 4.0.1 is experimental and requires replacing the WDDM driver with the VMware SVGA driver.

For a complete list of View 4 guest operating systems supported, please refer to the VMware View 4 Feature Support Matrix:
`http://www.vmware.com/pdf/view401_architecture_planning.pdf`

7 Appendix: PCoIP Protocol Group Policy Objects

This section outlines the PCoIP protocol General Policy Objects (GPOs) available with View 4.0.1. The View 4.0.1 pcoip.adm file is included in the View Connection Server install.

7.1 PCoIPMaxLinkRate_Policy

PCoIPMaxLinkRate_Policy configures the maximum PCoIP session bandwidth.

This policy constrains the peak bandwidth used by the PCoIP session. A value of 0 means no bandwidth constraints, otherwise the value is the maximum bandwidth in kilobits per second

7.2 PCoIPAudio_Policy

PCoIPAudio_Policy enables audio in the PCoIP session.

This policy controls whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. Set to *Enabled* to allow PCoIP audio or set to *Disabled* to prevent PCoIP audio. When this policy is not configured the default setting of audio enabled is used.

7.3 PCoIPEncryption_Policy

PCoIPEncryption_Policy configures PCoIP session encryption algorithms.

This policy controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation. At least one algorithm must be enabled. The endpoints negotiate the actual algorithm used."

7.4 PCoIPUsb_Policy

PCoIPUsb_Policy configure PCoIP USB allowed and unallowed device rules.

This policy sets USB device authorizations and unauthorizations for PCoIP sessions using a hardware portal. For a USB device to be used in a PCoIP session it must be included on the USB authorization list and not present on the USB unauthorization list.

7.5 PCoIPTcpServer_Policy

PCoIPTcpServer_Policy configures the TCP port the PCoIP host binds and listens to.

This policy sets the TCP server port bound to by software PCoIP hosts. The TCP port value sets the base TCP port that the server attempts to bind to. The TCP port range value determines how many additional ports should be tried if the base port is not available. The range spans from (base port) to (base port + port range).

7.6 PCoIPUdpServer_Policy

PCoIPUdpServer_Policy configures the Server PCoIP UDP port.

This policy sets the UDP server port bound to by software PCoIP hosts. The UDP port value sets the base UDP port to use. The UDP port range value determines how many additional ports should be tried if the base port is not available. The range spans from (base port) to (base port + port range). This setting has no effect on a client.

7.7 PCoIPVchan_Policy

PCoIPVchan_Policy configures PCoIP virtual channels.

This policy enables virtual channels and controls which virtual channels operate over PCoIP sessions. For a virtual channel to be used in a PCoIP session it must be included on the virtual channel authorization list and not present on the virtual channel unauthorization list.

7.8 PCoIPImaging_Policy

PCoIPImaging_Policy configures PCoIP image quality levels.

This policy enables control over how PCoIP renders images during periods of network congestion. There are two settings, which interoperate to allow fine control in network-bandwidth constrained environments: Minimum Image Quality and Maximum Initial Image Quality.

The Minimum Image Quality setting applies to the soft host only. The value ranges between 0 and 100 (a registry DWORD setting). The default value for this setting is 50. The Minimum Image Quality setting allows a balance between image quality and frame rate for limited bandwidth scenarios. With limited bandwidth, there must be a trade-off between image quality and frame rate - this setting allows the ability to configure which is preferred. The Minimum Image Quality setting ranges between 0 and 100. A lower value allows higher frame-rates (with a potentially lower quality display) and a higher value allows higher image quality (with potentially lower frame rates) when network bandwidth is constrained. When network bandwidth is not constrained, the PCoIP protocol will maintain maximum quality regardless of the setting. The value of the setting must be set to a value which is less than or equal to the Maximum Initial Image Quality setting.

The Maximum Initial Image Quality setting applies to the soft host only. The value ranges between 0 and 100 (a registry DWORD setting). The default value for this setting is 90. The Maximum Initial Image Quality setting can reduce the network bandwidth peaks required by the PCoIP protocol by limiting the initial quality of the changed regions of the display image. In a limited bandwidth scenario, this allows the configuration of which is preferred: a lower initial quality with more frequent updates or a higher image quality with less frequent updates. The Maximum Initial Image Quality setting ranges between 0 and 100. A lower value will reduce the image quality of content changes and decrease peak bandwidth requirements. A higher setting will increase the image quality of content changes and increase peak bandwidth requirements. Note that the unchanged regions of the image will progressively build to a lossless (perfect) quality regardless of setting. The value of the Maximum Initial Image Quality must be set to a value, which is greater than or equal to the Minimum Image Quality. The recommended Maximum Initial Image Quality setting value is 90 or lower to best utilize the available network bandwidth.

7.9 PCoIPDefaultInputLanguage_Policy

PCoIPDefaultInputLanguage_Policy enables PCoIP user default input language synchronization.

This policy controls whether the default input language for the user in the PCoIP session is synchronized with the default input language of the PCoIP client endpoint. Set to *Enabled* to allow the synchronization or set to *Disabled* to prevent the synchronization. When this policy is not configured the default setting of synchronization enabled is used.