Using VMware Horizon View Client for Linux

January 2014
Horizon View

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001162-03

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Using VMware Horizon View Client for Linux

This guide, *Using VMware Horizon View Client for Linux*, provides information about installing and using VMware® Horizon View™ software on a Linux client system to connect to a View desktop in the datacenter.

The information in this document includes system requirements and instructions for installing and using Horizon View Client for Linux.

This information is intended for administrators who need to set up a Horizon View deployment that includes Linux client systems. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

NOTE This document pertains to the Horizon View Client for Linux that VMware makes available on Ubuntu. In addition, several VMware partners offer thin client devices for Horizon View deployments. The features that are available for each thin client device, and the operating systems supported, are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the VMware Compatibility Guide, available on the VMware Web site.

System Requirements and Installation 1

Client systems must meet certain hardware and software requirements. The process of installing View Client is like installing most other applications.

- System Requirements on page 8

  The Linux PC or laptop on which you install Horizon View Client, and the peripherals it uses, must meet certain system requirements.

- System Requirements for Real-Time Audio-Video on page 9

  Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices, and with standard conferencing applications like Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your Horizon View deployment must meet certain software and hardware requirements.

- Supported Desktop Operating Systems on page 10

  Administrators create virtual machines with a guest operating system and install View Agent in the guest operating system. End users can log in to these virtual machines from a client device.

- Requirements for Using Flash URL Redirection on page 10

  Streaming Flash content directly from Adobe Media Server to client endpoints lowers the load on the datacenter ESXi host, removes the extra routing through the datacenter, and reduces the bandwidth required to simultaneously stream live video events to multiple client endpoints.

- Preparing View Connection Server for Horizon View Client on page 11

  Administrators must perform specific tasks to enable end users to connect to remote desktops.

- Install Horizon View Client for Linux on page 11

  End users open Horizon View Client to connect to remote desktops from a physical machine. Horizon View Client for Linux runs on Ubuntu 12.04 systems, and you install it by using the Synaptic Package Manager.

- Configure the View Client Download Links Displayed in View Portal on page 12

  By default, when you open a browser and enter the URL of a View Connection Server instance, the portal page that appears contains links to the VMware Download site for downloading Horizon View Client. You can change the default .

- Horizon View Client Data Collected by VMware on page 13

  If your company participates in the customer experience improvement program, VMware collects data from certain Horizon View Client fields. Fields containing sensitive information are made anonymous.

System Requirements

The Linux PC or laptop on which you install Horizon View Client, and the peripherals it uses, must meet certain system requirements.

NOTE These system requirements pertain to the Horizon View Client for Linux that VMware makes available on Ubuntu. In addition, several VMware partners offer thin client devices for Horizon View deployments. The features that are available for each thin client device, and the operating systems supported, are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the VMware Compatibility Guide, available on the VMware Web site.

Model	Intel-based desktop or laptop computer
Memory	At least 2GB of RAM
Operating systems	■ View Client 2.0 and later: 32-bit Ubuntu Linux 12.04 ■ View Client 1.6 and 1.7: 32-bit Ubuntu Linux 10.04 or 12.04 ■ View Client 1.5: 32-bit Ubuntu Linux 10.04 or 10.10
View Connection Server, Security Server, and View Agent	Latest maintenance release of VMware View 4.6.x and later releases If client systems connect from outside the corporate firewall, VMware recommends that you use a security server. With a security server, client systems will not require a VPN connection.
Display protocol for Horizon View	PCoIP or RDP **IMPORTANT** Although Horizon View Client for Linux supports the RDP display protocol, the particular RDP client that ships with your distribution of Ubuntu might not work with Horizon View Client.
Screen resolution on client system	Minimum: 1024 X 768 pixels

Hardware Requirements for PCoIP	■ x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
	■ Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide:
	`20MB + (24 * (# monitors) * (monitor width) * (monitor height))`
	As a rough guide, you can use the following calculations:
	`1 monitor: 1600 x 1200: 64MB`
	`2 monitors: 1600 x 1200: 128MB`
	`3 monitors: 1600 x 1200: 256MB`

Hardware Requirements for RDP	■ x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed. ■ 128MB RAM.
Software Requirements for Microsoft RDP	■ For Ubuntu 12.04, use rdesktop 1.7.0.

- For Ubuntu 10.04, use rdesktop 1.6.0.

Software Requirements for FreeRDP

If you plan to use an RDP connection to View desktops and you would prefer to use a FreeRDP client for the connection, you must install the correct version of FreeRDP and any applicable patches. See "Install and Configure FreeRDP," on page 32.

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices, and with standard conferencing applications like Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your Horizon View deployment must meet certain software and hardware requirements.

Horizon View remote desktop

The desktops must have View Agent 5.2 or later installed. The desktops must also have the corresponding Remote Experience Agent installed. For example, if View Agent 5.3 is installed, you must also install the Remote Experience Agent from Horizon View 5.3 Feature Pack 1. See the *VMware Horizon View Feature Pack Installation and Administration* document for VMware Horizon View

Horizon View Client software

Horizon View Client 2.2 for Linux or a later release. Note that this feature is available only with the version of Horizon View Client for Linux provided by third-party vendors.

Horizon View Client computer or client access device

- Real-Time Audio-Video is supported on x86 devices. This feature is not supported on ARM processors. The client system processor must have at least two cores.
- Horizon View Client requires the following libraries:
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

  The plug-in file `/usr/lib/pcoip/vchan_plugins/libmmredir_plugin.so` has the following dependencies.:

  ```
  libuuid.so.1
  libv4l2.so.0
  libspeex.so.1
  libudev.so.0
  libtheoradec.so.1
  libtheoraenc.so.1
  libv4lconvert.so.0
  libjpeg.so.8
  ```

  All of these files must be present on the client system or the Real-Time Audio-Video feature will not work. Note that these dependencies are in addition to the dependencies required for Horizon View Client itself.

- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. To support Real-Time Audio-Video, you do not have to install the device drivers on the desktop operating system where View Agent is installed.

Display protocol for Horizon View

PCoIP

Real-Time Audio-Video is not supported in RDP desktop sessions.

Supported Desktop Operating Systems

Administrators create virtual machines with a guest operating system and install View Agent in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported guest operating systems, see the "Supported Operating Systems for View Agent" topic in the Horizon View 4.6.x or 5.x installation documentation.

Requirements for Using Flash URL Redirection

Streaming Flash content directly from Adobe Media Server to client endpoints lowers the load on the datacenter ESXi host, removes the extra routing through the datacenter, and reduces the bandwidth required to simultaneously stream live video events to multiple client endpoints.

The Flash URL redirection feature uses a JavaScript that is embedded inside a Web page by the Web page administrator. Whenever a virtual desktop user clicks on the designated URL link from within a Web page, the JavaScript intercepts and redirects the ShockWave File (SWF) from the virtual desktop session to the client endpoint. The endpoint then opens a local VMware Flash Projector outside of the virtual desktop session and plays the media stream locally.

This feature is available when used in conjunction with the correct version of VMware Horizon View Feature Pack.

- Multicast support requires VMware Horizon View 5.2 Feature Pack 2 or later.
- Unicast support requires VMware Horizon View 5.3 Feature Pack 1 or later.

To use this feature, you must set up your Web page and your client devices. Client systems must meet certain software requirements:

- For multicast support, client systems must use Horizon View Client 2.1 or later. For unicast support, client systems must use Horizon View Client 2.2 or later.

  NOTE This feature is supported only on the version of Horizon View Client provided by partners and only on x86 thin client devices. This feature is not supported on ARM processors.

- Client systems must have IP connectivity to the Adobe Web server that hosts the ShockWave File (SWF) that initiates the multicast or unicast streaming. If needed, configure your firewall to open the appropriate ports to allow client devices to access this server.
- Client systems must have the appropriate Flash plug-in installed.

  a Install the `libexpat.so.0` file, or verify that this file is already installed.

  Ensure that the file is installed in the `/usr/lib` or `/usr/local/lib` directory.

  b Install the `libflashplayer.so` file, or verify that this file is already installed.

  Ensure that the file is installed in the appropriate Flash plug-in directory for your Linux operating system.

  c Install the `wget` program, or verify that the program file is already installed.

For a list of the View desktop requirements for Flash URL redirection, and for instructions about how to configure a Web page to provide a multicast or unicast stream, see the *VMware Horizon View Feature Pack Installation and Administration* document.

Preparing View Connection Server for Horizon View Client

Administrators must perform specific tasks to enable end users to connect to remote desktops.

Before end users can connect to View Connection Server or a security server and access a remote desktop, you must configure certain pool settings and security settings:

- If you are using a security server, as VMware recommends, verify that you are using the latest maintenance releases of View Connection Server 4.6.x and View Security Server 4.6.x or later releases. See the *VMware Horizon View Installation* documentation.
- If you plan to use a secure tunnel connection for client devices and if the secure connection is configured with a DNS host name for View Connection Server or a security server, verify that the client device can resolve this DNS name.

  To enable or disable the secure tunnel, in View Administrator, go to the Edit View Connection Server Settings dialog box and use the check box called **Use secure tunnel connection to desktop**.
- Verify that a desktop pool has been created and that the user account that you plan to use is entitled to access the remote desktop. See the topics about creating desktop pools in the *VMware Horizon View Administration* documentation.
- To use two-factor authentication with Horizon View Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on View Connection Server. RADIUS authentication is available with View 5.1 or later View Connection Server. For more information, see the topics about two-factor authentication in the *VMware Horizon View Administration* documentation.

Install Horizon View Client for Linux

End users open Horizon View Client to connect to remote desktops from a physical machine. Horizon View Client for Linux runs on Ubuntu 12.04 systems, and you install it by using the Synaptic Package Manager.

IMPORTANT Customers using Linux-based thin clients must contact their thin client vendor for Horizon View Client updates. Customers who have successfully built their own Linux-based endpoints and need an updated client must contact their VMware sales representative.

Prerequisites

- Verify that the client system uses a supported operating system. See "System Requirements," on page 8.
- Verify that you can log in as an administrator on the client system.
- If you plan to use the RDP display protocol to connect to a View desktop, verify that you have the appropriate RDP client installed. See "System Requirements," on page 8.

Procedure

1 On your Linux laptop or PC, enable Canonical Partners.

   a From the Ubuntu menu bar, select **System > Administration > Update Manager**.

   b Click the **Settings** button and supply the password for performing administrative tasks.

   c In the Software Sources dialog box, click the **Other Software** tab and select the **Canonical Partners** check box to select the archive for software that Canonical packages for their partners.

   d Click **Close** and follow the instructions to update the package list.

2 Download the package from the Ubuntu Software Center, as follows.

   a From the Ubuntu menu bar, select **System > Administration > Synaptic Package Manager**

   b Click **Search** and search for **vmware**.

   c In the list of packages returned, select the check box next to **vmware-view-client** and select **Mark for Installation**.

   d Click **Apply** in the toolbar.

   If your operating system is Ubuntu 12.04, the latest version of Horizon View Client is installed. If your operating system is Ubuntu 10.04, View Client for Linux 1.7 is installed.

3 To determine that installation succeeded, verify that the **VMware Horizon View** application icon appears in the **Applications > Internet** menu.

What to do next

Start Horizon View Client and verify that you can log in to the correct virtual desktop. See "Log In to a Remote Desktop for the First Time," on page 35.

Configure the View Client Download Links Displayed in View Portal

By default, when you open a browser and enter the URL of a View Connection Server instance, the portal page that appears contains links to the VMware Download site for downloading Horizon View Client. You can change the default .

The default Horizon View Client links on portal page ensure that you are directed to the latest compatible Horizon View Client installers. In some cases, however, you might want to have the links point to an internal Web server, or you might want to make specific client versions available on your own View Connection Server. You can reconfigure the page to point to a different URL.

When you make links for Mac OS X, Linux, and Windows client systems, the correct operating system specific link is shown on the portal page. For example, if you browse to the portal page from a Windows system, only the link or links for Windows installers appear. You can make separate links for 32-bit and 64-bit installers. You can also make links for iOS and Android systems, but these operating systems are not automatically detected, so that if you browse to the portal page from an iPad, for example, you see the links for both iOS and Android, if you created links for both.

IMPORTANT If you customize the portal page links, as described in this topic, and later install VMware Horizon View HTML Access on the server, your customized portal page is replaced by an HTML Access page. For information about customizing that page, see *Using VMware Horizon View HTML Access*.

Prerequisites

- Download the installer files for the Horizon View Client types that you want to use in your environment. The URL to the client download page is https://www.vmware.com/go/viewclients.
- Determine which HTTP server will host the installer files. The files can reside on a View Connection Server instance or on another HTTP server.

Procedure

1 On the HTTP server where the installer files will reside, create a folder for the installer files.

   For example, to place the files in a `downloads` folder on the View Connection Server host, in the default installation directory, use the following path:

   ```
   C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
   ```

The links to the files would then use URLs with the format `https://server-name/downloads/client-installer-file-name`. For example, a server with the name `view.mycompany.com` might use the following URL for View Client for Windows: `https://view.mycompany.com/downloads/VMware-Horizon-View-Client.exe`. In this example, the folder named `downloads` is located in the `webapps` root folder.

2 Copy the installer files into the folder.

If the folder resides on View Connection Server, you can replace any files in this folder without having to restart the VMware View Connection Server service.

3 On the View Connection Server machine, copy the `portal-links.properties` file and the `portal.properties` file located in *`install-path`*`\Server\Extras\PortalExamples`.

4 Create a `portal` folder the directory `C:\ProgramData\VMware\VDM`, and copy the `portal-links.properties` and `portal.properties` files into the `portal` folder.

5 Edit `C:\ProgramData\VMware\VDM\portal\portal-links.properties` file to point to the new location of the installer files.

You can edit the lines in this file and add to them if you need to create more links. You can also delete lines.

The following examples show properties for creating two links for View Client for Windows and two links for View Client for Linux:

```
link.win=https://server-name/downloads/VMware-Horizon-View-Client-x86_64-y.y.y-XXXX.exe#win
link.win.1=https://server-name/downloads/VMware-Horizon-View-Client-y.y.y-XXXX.exe#win
link.linux=https://server-name/downloads/VMware-Horizon-View-Client-x86_64-y.y.y-XXXX.rpm#linux
link.linux.1=https://server-name/downloads/VMware-Horizon-View-Client-y.y.y-XXXX.tar.gz#linux
```

In this example, *`y.y.y-XXXX`* indicates the version and build number. The `win` text at the end of the line indicates that this link should appear in the browser if the client has a Windows operating system. Use `win` for Windows, `linux` for Linux, and `mac` for Mac OS X. For other operating systems, use `unknown`.

6 Edit `C:\ProgramData\VMware\VDM\portal\portal.properties` file to specify the text to display for the links.

These lines appear in the section of the file called `# keys based on key names in portal-links.properties`.

The following example shows the text that corresponds to the links specified for `link.win` and `link.win.1`:

```
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
```

7 Restart the VMware View Connection Server service.

When end users enter the URL for View Connection Server, they see links with the text you specified. The links point to the locations you specified.

Horizon View Client Data Collected by VMware

If your company participates in the customer experience improvement program, VMware collects data from certain Horizon View Client fields. Fields containing sensitive information are made anonymous.

NOTE This feature is available only if your Horizon View deployment uses View Connection Server 5.1 or later. Client information is sent for View Client 1.7 and later clients.

VMware collects data on the clients to prioritize hardware and software compatibility. If your company's administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment in order to improve VMware's response to customer requirements. No data that identifies your organization is collected. Horizon View Client information is sent first to View Connection Server and then on to VMware, along with data from Horizon View servers, desktop pools, and remote desktops.

Although the information is encrypted while in transit to View Connection Server, the information on the client system is logged unencrypted in a user-specific directory. The logs do not contain any personally identifiable information.

To participate in the VMware customer experience improvement program, the administrator who installs View Connection Server can opt in while running the View Connection Server installation wizard, or an administrator can set an option in View Administrator after the installation.

Table 1-1. Data Collected from Horizon View Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous?	Example Value
Company that produced the Horizon View Client application	No	VMware
Product name	No	VMware Horizon View Client
Client product version	No	The format is *x.x.x-yyyyyy*, where *x.x.x* is the client version number and *yyyyyy* is the build number.
Client binary architecture	No	Examples include the following: ■ i386 ■ x86_64 ■ arm
Client build name	No	Examples include the following: ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-Client-WinStore
Host operating system	No	Examples include the following: ■ Windows 8.1 ■ Windows 7, 64-bit Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)
Host operating system kernel	No	Examples include the following: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unknown (for Windows Store)
Host operating system architecture	No	Examples include the following: ■ x86_64 ■ i386 ■ armv71 ■ ARM

Table 1-1. Data Collected from Horizon View Clients for the Customer Experience Improvement Program (Continued)

Description	Is This Field Made Anonymous?	Example Value
Host system model	No	Examples include the following: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Host system CPU	No	Examples include the following: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (for iPad)
Number of cores in the host system's processor	No	For example: 4
MB of memory on the host system	No	Examples include the following: ■ 4096 ■ unknown (for Windows Store)

Configuring Horizon View Client for End Users

2

Horizon View Client provides several configuration mechanisms to simplify the login and desktop selection experience for end users, and also to enforce security policies.

The following table shows some of the configuration settings that you can set in any of several ways. For many other configuration settings, you must use a particular mechanism. For example, to use the setting for Disable Toaster Notifications, you must use a Group Policy setting..

Table 2-1. Common Configuration Settings

Setting	Mechanisms for Configuring
View Connection Server address	URI, Group Policy, Command Line, Windows Registry
Active Directory user name	URI, Group Policy, Command Line, Windows Registry
Log in as current user	Group Policy, Command Line
Domain name	URI, Group Policy, Command Line, Windows Registry
Desktop display name	URI, Group Policy, Command Line
Window size	URI, Group Policy, Command Line
Display protocol	URI, Command Line
Options for redirecting USB devices	URI, Group Policy, Command Line
Configuring certificate checking	Group Policy, Windows Registry
Configuring SSL protocols and cryptographic algorithms	Group Policy, Windows Registry

This chapter includes the following topics:

Using URIs to Configure Horizon View Client

Using uniform resource identifiers (URIs), you can create a Web page or an email with links that end users click to launch Horizon View Client, connect to View Connection Server, and launch a specific desktop with specific configuration options.

You can simplify the process of logging in to a remote desktop by creating Web or email links for end users. You create these links by constructing URIs that provide some or all of the following information, so that your end users do not need to supply it:

- View Connection Server address
- Port number for View Connection Server
- Active Directory user name
- Domain name
- Desktop display name
- Window size
- Desktop actions, including reset, log off, and start session
- Display protocol

To construct a URI, you use the `vmware-view` URI scheme with Horizon View Client specific path and query parts.

NOTE You can use URIs to launch Horizon View Client only if the client software is already installed on end users' client computers.

Syntax for Creating vmware-view URIs

Syntax includes the `vmware-view` URI scheme, a path part to specify the desktop, and, optionally, a query to specify desktop actions or configuration options.

VMware Horizon View URI Specification

When you create a URI, you are essentially calling `vmware-view` with the full View URI string as an argument.

Use the following syntax to create URIs for launching Horizon View Client:

`vmware-view://[`*`authority-part`*`][/`*`path-part`*`][?`*`query-part`*`]`

The only required element is the URI scheme, `vmware-view`. For some versions of some client operating systems, the scheme name is case-sensitive. Therefore, use `vmware-view`.

IMPORTANT In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.utf8-chartable.de/.

authority-part Specifies the server address and, optionally, a user name, a non-default port number, or both. Server names must conform to DNS syntax.

To specify a user name, use the following syntax:

`user1@`*`server-address`*

Note that you cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax:

`server-address:port-number`

path-part Specifies the desktop. Use the desktop display name. If the display name has a space in it, use the **`%20`** encoding mechanism to represent the space.

query-part Specifies the configuration options to use or the desktop actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If queries conflict with each other, the last query in the list is used. Use the following syntax:

`query1=value1``[&`*`query2=value2...`*`]`

Supported Queries

This topic lists the queries that are supported for this type of Horizon View Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the *Using VMware Horizon View Client* guide for each type of client system.

action

Table 2-2. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available desktops hosted on the specified server. You are not required to specify a desktop when using this action.
`start-session`	Launches the specified desktop. If no action query is provided and the desktop name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified desktop. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC.
`logoff`	Logs the user out of the guest operating system in the remote desktop.
`rollback`	Discards changes made to the specified desktop while it was checked out for use in local mode on a Windows PC or laptop.

connectUSBOnInsert (The USB component is included only with the Horizon View Client available from third-party vendors.) Connects a USB device to the foreground desktop when you plug in the device. This query is implicitly set if you specify the `unattended` query. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`yes`** and **`no`**. An example of the syntax is **`connectUSBOnInsert=yes`**.

connectUSBOnStartup (The USB component is included only with the Horizon View Client available from third-party vendors.) Redirects all USB devices to the desktop that are currently connected to the client system. This query is implicitly set if you specify the `unattended` query. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`yes`** and **`no`**. An example of the syntax is **`connectUSBOnStartup=yes`**.

desktopLayout Sets the size of the window that displays the remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query.

Table 2-3. Valid Values for the desktopLayout Query

Value	Description
`fullscreen`	Full screen on one monitor. This is the default.
`multimonitor`	Full screen on all monitors.
`windowLarge`	Large window.
`windowSmall`	Small window.
*W*x*H*	Custom resolution, where you specify the width by height, in pixels. An example of the syntax is **`desktopLayout=1280x800`**.

desktopProtocol Valid values are **`RDP`** and **`PCoIP`**. For example, to specify PCoIP, use the syntax **`desktopProtocol=PCoIP`**.

domainName The domain associated with the user who is connecting to the remote desktop.

Examples of vmware-view URIs

You can create hypertext links or buttons with the `vmware-view` URI scheme and include these links in email or on a Web page. Your end users can click these links to, for example, launch a particular remote desktop with the startup options you specify.

URI Syntax Examples

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon View Client is launched and connects to the `view.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the desktop whose display name is displayed as **Primary Desktop**, and the user is logged in to the guest operating system.

NOTE The default display protocol and window size are used. The default display protocol is PCoIP. The default window size is full screen.

You can change the defaults. See "Using the View Client Command-Line Interface and Configuration Files," on page 21.

---

2 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for View Connection Server. (The default port is 443.) Because a desktop identifier is provided, the desktop is launched even though the `start-session` action is not included in the URI.

3 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCoIP`

Horizon View Client is launched and connects to the `view.mycompany.com` server. In the login box, the **User name** text box is populated with the name **fred**. The user must supply the domain name and password. After a successful login, the client connects to the desktop whose display name is displayed as **Finance Desktop**, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon View Client is launched and connects to the `view.mycompany.com` server. In the login box, the **User name** text box is populated with the name **fred**, and the **Domain** text box is populated with **mycompany**. The user must supply only a password. After a successful login, the client connects to the desktop whose display name is displayed as **Finance Desktop**, and the user is logged in to the guest operating system.

5 `vmware-view://view.mycompany.com/`

Horizon View Client is launched, and the user is taken to the login prompt for connecting to the `view.mycompany.com` server.

6 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon View Client is launched and connects to the `view.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, Horizon View Client displays a dialog box that prompts the user to confirm the reset operation for Primary Desktop. After the reset occurs, depending on the type of client, the user might see a message indicating whether the reset was successful.

NOTE This action is available only if the View administrator has enabled this feature for end users.

7 `vmware-view://`

Horizon View Client is launched, and the user is taken to the page for entering the address of a View Connection Server instance.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code a hypertext link that says, **Test Link**, and a button that says, **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Using the View Client Command-Line Interface and Configuration Files

You can configure View Client using command-line options or equivalent properties in a configuration file.

You can use the `vmware-view` command-line interface or set properties in configuration files to define default values your users see in View Client or to suppress some dialog boxes from prompting users for information. You can also specify settings that you do not want users to change.

Processing Order for Configuration Settings

When View Client starts up, configuration settings are processed from various locations in the following order:

1 `/etc/vmware/view-default-config`

2 `~/.vmware/view-preferences`

3 Command-line arguments

4 `/etc/vmware/view-mandatory-config`

If a setting is defined in multiple locations, the value that is used is the value from the last file or command-line option read. For example, to specify settings that override users' preferences, set properties in the `/etc/vmware/view-mandatory-config` file.

To set default values that users can change, use the `/etc/vmware/view-default-config` file. After users change a setting, when they exit View Client, any changed settings are saved in the `~/.vmware/view-preferences` file.

Properties That Prevent Users from Changing Defaults

For each property, you can set a corresponding `view.allow` property that controls whether users are allowed to change the setting. For example, if you set the `view.allowDefaultBroker` property to "FALSE" in the `/etc/vmware/view-mandatory-config` file, users will not be able to change the name in the **Server Name** field when they use View Client.

Syntax for Using the Command-Line Interface

Use the following form of the `vmware-view` command from a terminal window.

`vmware-view [`*`command-line-option`* `[`*`argument`*`]] ...`

By default, the `vmware-view` command is located in the `/usr/bin` directory.

You can use either the short form or the long form of the option name, although not all options have a short form. For example, to specify the domain you can use either `-d` (short form) or `--domainName=` (long form). You might choose to use the long form to make a script more human-readable.

You can use the `--help` option to get a list of command-line options and usage information.

IMPORTANT If you need to use a proxy, use the following syntax:

`http_proxy=`*`proxy_server_URL:port`* `https_proxy=`*`proxy_server_URL:port`* `vmware-view` *`options`*

This workaround is required because you must clear the environment variables that were previously set for the proxy. If you do not perform this action, the proxy exception setting does not take effect in View Client. You configure a proxy exception for the View Connection Server instance.

View Client Configuration Settings and Command-Line Options

For your convenience, almost all configuration settings have both a *key=value* property and a corresponding command-line option name. For a few settings, there is a command-line option but no corresponding property you can set in a configuration file. For a few other settings, you must set a property because no command-line option is available.

IMPORTANT Some command-line options and configuration keys, such as the ones for USB redirection and MMR, are available only with the version of View Client provided by third-party vendors. For more information about VMware thin-client and zero-client partners, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Table 2-4. View Client Command-Line Options and Configuration File Keys

Configuration Key	Command-Line Option	Description
`view.allMonitors`	`--allmonitors`	Hides the host operating system and opens the View Client user interface in full screen mode across all monitors that are connected when View Client is launched. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE".

`view.allowDefaultBroker`	`-l`, `--lockServer`
	Example:
	`--lockServer -s view.company.com`
		Using this command-line option, or setting the property to "FALSE", disables the **Server Name** field unless the client has never connected to any server, and no server address is provided in the command line or the preferences file.

`view.autoConnectBroker`	None	Automatically connects to the last View server used unless the `view.defaultBroker` configuration property is set or unless the `--serverURL=` command-line option is used. Specify **"TRUE"** or **"FALSE"**. Default is "FALSE". Setting this property and the `view.autoConnectDesktop` property to "TRUE" is the equivalent of setting the `view.nonInteractive` property to "TRUE".
`view.autoConnectDesktop`	None	Automatically connects to the last View desktop used unless the `view.defaultDesktop` configuration property is set or unless the `--desktopName=` command-line option is used. Specify **"TRUE"** or **"FALSE"**. Default is "FALSE". Setting this property and the `view.autoConnectBroker` property to "TRUE" is the equivalent of setting the `view.nonInteractive` property to "TRUE".

`view.defaultBroker`	`-s`, `--serverURL=`
	Examples:
	`--serverURL=https://view.company.com`
	`-s view.company.com`
	`--serverURL=view.company.com:1443`
		Adds the name that you specify to the **Server Name** field in View Client. Specify a fully qualified domain name. You can also specify a port number if you do not use the default 443.
		Default is the most recently used value.

`view.defaultDesktop`	`-n`, `--desktopName=`	Specifies which desktop to use when `autoConnectDesktop` is set to "TRUE" and the user has access to multiple desktops. This is the name you would see in the Select Desktop dialog box. The name is usually the pool name.
`view.defaultDesktopHeight`	None	Specifies the default height of the window for the View desktop, in pixels.

Table 2-4. View Client Command-Line Options and Configuration File Keys (Continued)

Configuration Key	Command-Line Option	Description

`view.defaultDesktopSize`	`--desktopSize=`
	Examples:
	`--desktopSize="1280x800"`
	`--desktopSize="all"`
		Sets the default size of the window for the View desktop:
		■ To use all monitors, set the property to **`"1"`** or use the command-line argument **`"all"`**.
		■ To use full screen mode on one monitor, set the property to **`"2"`** or use the command-line argument **`"full"`**.
		■ To use a large window, set the property to **`"3"`** or use the command-line argument **`"large"`**.
		■ To use a small window, set the property to **`"4"`** or use the command-line argument **`"small"`**.
		■ To set a custom size, set the property to **`"5"`**and then also set the `view.defaultDesktopWidth` and `view.defaultDesktopHeight` properties. Alternatively, specify the width by height, in pixels, at the command-line as **`"widthxheight"`**.

`view.defaultDesktopWidth`	None	Specifies the default width of the window for the View desktop, in pixels.
`view.defaultDomain`	`-d, --domainName=`	Sets the domain name that View Client uses for all connections and adds the domain name that you specify to the **Domain Name** field in View Client authentication dialog box.
`view.defaultPassword`	`-p "-", --password="-"`	For PCoIP and `rdesktop` connections, always specify **`"-"`** to read the password from `stdin`. Sets the password that View Client uses for all connections and adds the password to the **Password** field in View Client authentication dialog box if View Connection Server accepts password authentication. **NOTE** You cannot use a blank password. That is, you cannot specify --password=""
`view.defaultProtocol`	`--protocol=`	Specifies which display protocol to use. Specify **`"PCOIP"`** or **`"RDP"`**. These values are case-sensitive. For example, if you enter **`rdp`** the protocol used will be the default. Default is the setting specified in View Administrator, under pool settings for the pool. If you use RDP and you want to use FreeRDP rather than `rdesktop`, you must also use the `rdpClient` setting.

Table 2-4. View Client Command-Line Options and Configuration File Keys (Continued)

Configuration Key	Command-Line Option	Description
view.defaultUser	-u, --userName=	Sets the user name that View Client uses for all connections and adds the user name that you specify to the **User Name** field in View Client authentication dialog box. For kiosk mode, the account name can be based on the client's MAC address, or it can begin with a recognized prefix string, such as **custom-**.
view.fullScreen	--fullscreen	Hides the host operating system and opens the View Client user interface in full screen mode on one monitor. This option does not affect the screen mode of the desktop session. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE".
view.kbdLayout	-k, --kbdLayout= rdesktop examples: --kbdLayout="en-us" -k "fr" freerdp example: -k "0x00010407"	Specifies which locale to use for the keyboard layout. NOTE rdesktop uses locale codes, such as **"fr"** and **"de"**, whereas freerdp uses keyboard layout IDs. For a list of these IDs, use the following command: xfreerdp --kbd-list
view.kioskLogin	--kioskLogin Example: See the kiosk mode example that follows this table.	Specifies that View client is going to authenticate using a kiosk mode account. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE".
view.mmrPath	-m, --mmrPath= Example: --mmrPath="/usr/lib/altmmr"	(Available only with distributions from third-party vendors) Specifies the path to the directory that contains the Wyse MMR (multimedia redirection) libraries.
view.nomenubar	--nomenubar	Suppresses the View Client menu bar when View Client is in full screen mode, so that users cannot access menu options to log off of, reset, or disconnect from a View desktop. Use this option when configuring kiosk mode. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE".
view.nonInteractive	-q, --nonInteractive Example: --nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"	Hides unnecessary UI steps from end users by skipping the screens that are specified in the command line or configuration properties. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE". Setting this property to "TRUE" is the equivalent of setting the view.autoConnectBroker and view.autoConnectDesktop properties to "TRUE".

Table 2-4. View Client Command-Line Options and Configuration File Keys (Continued)

Configuration Key	Command-Line Option	Description
`view.once`	`--once`	Specifies that you do not want View Client to retry connecting in the case of an error occurring. Use `--once` if you want to obtain a similar workflow to the View 4.6 client. This option will force the View client to exit after the user disconnects or logs off from a desktop. You should usually specify this option if you use kiosk mode, and use the exit code to handle the error. Otherwise, you might find it difficult to kill the `vmware-view` process remotely. If you are setting the configuration key, specify **`"TRUE"`** or **`"FALSE"`**. Default is "FALSE".

`view.rdesktopOptions`	`--rdesktopOptions=`
	Example:
	`--rdesktopOptions="-f -m"`
		(Available if you use the Microsoft RDP display protocol) Specifies command-line options to forward to the rdesktop application. For information about rdesktop options, see the rdesktop documentation.

None	`-r, --redirect=`
	Example:
	`--redirect="sound:off"`
		(Available if you use the Microsoft RDP display protocol) Specifies a local device that you want rdesktop to redirect to the View desktop.
		Specify the device information that you want to pass to the `-r` option of rdesktop. You can set multiple device options in a single command.

`view.rdpClient`	`--rdpclient=`	(Available if you use the Microsoft RDP display protocol) Specifies which type of RDP client to use. The default is `rdesktop`. To use FreeRDP instead, specify `xfreerdp`. **NOTE** To use FreeRDP, you must have the correct version of FreeRDP installed, along with any applicable patches. For more information, see "Install and Configure FreeRDP," on page 32.
None	`--save`	(Available if you use View Client 2.2 or later) Saves the user name and domain name that were last used to successfully log in so that you do not need to enter the user name or domain name the next time you are prompted to supply login credentials.

Table 2-4. View Client Command-Line Options and Configuration File Keys (Continued)

Configuration Key	Command-Line Option	Description
`view.sendCtrlAltDelToLocal`	None	(Available if you use the PCoIP display protocol and View Client 2.1 or later) When set to **"TRUE"**, sends the key combination Ctrl+Alt+Del to the client system rather than opening a dialog box to prompt the user to disconnect from the View desktop. Default is "FALSE". **NOTE** If you use the Microsoft RDP display protocol, you can achieve this functionality by using the `–K` option; for example, `vmware–view –K`. You can also configure this key combination by using the `view–keycombos–config file`, as described in "Configuring Specific Keys and Key Combinations to Send to the Local System," on page 29.
`view.sendCtrlAltInsToVM`	None	(Available if you use the PCoIP display protocol and View Client 2.1 or later) When set to **"TRUE"**, sends the key combination Ctrl+Alt+Ins to the virtual desktop rather than sending Ctrl+Alt +Del. Default is "FALSE". **NOTE** To use this feature, you must also set the agent-side GPO policy called "Use alternate key for sending Secure Attention Sequence," available in the `pcoip.adm` template. See the topic called "View PCoIP Session Variables for the Keyboard" in the "Configuring Policies" chapter of the *VMware Horizon View Administration* document.
`view.sslVerificationMode`	None	Sets the server certificate verification mode. Specify **"1"** to reject connections when the certificate fails any of the verification checks, **"2"** to warn but allow connections that use a self-signed certificate, or **"3"** to allow unverifiable connections. If you specify **"3"** no verification checks are performed. Default is "2".
`view.xfreerdpOptions`	`––xfreerdpOptions=`	(Available if you use the Microsoft RDP display protocol) Specifies command-line options to forward to the `xfreerdp` program. For information about `xfreerdp` options, see the `xfreerdp` documentation. **NOTE** To use FreeRDP, you must have the correct version of FreeRDP installed, along with any applicable patches. For more information, see "Install and Configure FreeRDP," on page 32.

Table 2-4. View Client Command-Line Options and Configuration File Keys (Continued)

Configuration Key	Command-Line Option	Description
None	`--enableNla`	(Applies if you are using FreeRDP for RDP connections) Enables network-level authentication (NLA). NLA is turned off by default if you are using FreeRDP. You must have the correct version of FreeRDP installed, along with any applicable patches. For more information, see "Install and Configure FreeRDP," on page 32. NOTE The `rdesktop` program does not support NLA.

None	`--printEnvironmentInfo`
	Example:
	`--printEnvironmentInfo -s view.company.com`
		Displays information about the environment of a client device, including its IP address, MAC address, machine name, and domain name.
		For kiosk mode, you can create an account for the client based on the MAC address. To display the MAC address, you must use this option with the `-s` option.

None	`--usb=`	(Available only with distributions from third-party vendors and only for View Client 1.5) Specifies which options to use for USB redirection. See"Using the View Client 1.5 Command-Line Option to Redirect USB Devices," on page 56. To configure USB options with View Client 1.6 and later, see Chapter 6, "Configuring USB Redirection on the Client," on page 51.
None	`--version`	Displays version information about View Client.

Example: Kiosk Mode Example

Kiosk users might include customers at airline check-in stations, students in classrooms or libraries, medical personnel at medical data entry workstations, or customers at self-service points. Accounts are associated with client devices rather than users because users do not need to log in to use the client device or the View desktop. Users can still be required to provide authentication credentials for some applications.

To set up kiosk mode, you must use the `vdmadmin` command-line interface on the View Connection Server instance and perform several procedures documented in the chapter about kiosk mode in the *VMware Horizon View Administration* document. After you set up kiosk mode, you can use the `vmware-view` command on a Linux client to connect to a View desktop in kiosk mode.

To connect to View desktops from Linux clients in kiosk mode, you must, at a minimum, include the following configuration keys or command-line options.

Configuration Key	Equivalent Command-line Options
`view.kioskLogin`	`--kioskLogin`
`view.nonInteractive`	`-q`, `--nonInteractive`
`view.fullScreen`	`--fullscreen`
`view.nomenubar`	`--nomenubar`
`view.defaultBroker`	`-s`, `--serverURL=`

Omitting any of these configuration settings is not supported for kiosk mode. If View Connection Server is set up to require a non-default kiosk user name, you must also set the `view.defaultUser` property or use the `–u` or `––userName=` command-line option. If a non-default user name is not required and you do not specify a user name, View Client can derive and use the default kiosk user name.

NOTE If you set the `view.sslVerificationMode` configuration key, be sure to set it in the `/etc/vmware/view–mandatory–config` file. When the client runs in kiosk mode, the client does not look in the `view–preferences` file.

The command shown in this example runs View Client on a Linux client system and has the following characteristics:

- The user account name is based on the client's MAC address.
- View Client runs in full screen mode without a View Client menu bar.
- Users are automatically connected to the specified View Connection Server instance and View desktop and are not prompted for login credentials.
- If a connection error occurs, depending on the error code returned, a script might run or a kiosk monitoring program might handle the error. As a result, for example, the client system might display an out-of-order screen or might wait a certain amount of time before attempting to connect to View Connection Server again.

```
./vmware–view ––kioskLogin ––nonInteractive ––once ––fullscreen ––nomenubar
––serverURL="server.mycomany.com" ––userName="CM–00:11:22:33:44:55:66:77" ––password="mypassword"
```

IMPORTANT If a pre-login message has been configured to appear before allowing View Client to connect to a View desktop, the user must acknowledge the message before being allowed to access the desktop. To avoid this issue, use View Administrator to disable pre-login messages.

Configuring Specific Keys and Key Combinations to Send to the Local System

If you use the PCoIP display protocol and Horizon View Client 2.2 or later, you can create a `view–keycombos–config` file to specify which key combinations should not be forwarded to the remote desktop. If you use Horizon View Client 2.3, you can also specify individual keys.

You might prefer to have some keys or key combinations handled by your local client system when working in a remote desktop. For example, you might want to use a particular key combination to start the screen saver on your client computer. Beginning with Horizon View Client 2.2, you can create a file located at `/etc/vmware/view–keycombos–config` and specify the key combinations. If you have Horizon View Client 2.3 or later, you can also specify individual keys.

Place each key or key combination on a new line using the format shown in the following table.

Table 2-5. Format for Specifying Keys That Must Not Be Forwarded to Remote Desktops

Client Version	Format
Horizon View Client 2.2	*<modName>keyName* **IMPORTANT** This feature pertains to key combinations and not to single keys. For example, you cannot specify only *<modName>* or only *keyName*.
Horizon View Client 2.3 or later	*<modName>scanCode* *scanCode* The first example is for a key combination. The second example is for a single key. The *scanCode* value is the keyboard scan code, in hexadecimal.

In this example, *modName* is one of four modifier keys: `ctrl`, `alt`, `shift`, and `super`. The Super key is keyboard-specific. For example, the Super key is usually the Windows key on a Microsoft Windows keyboard but is the Command key on a Mac OS X keyboard. If you have Horizon View Client 2.3 or later, you can also use `<any>` as a wildcard for *modName*. For example, `<any>0x153` specifies all combinations of the Delete key, including the individual Delete key for the US keyboard. The value you use for *modName* is not case-sensitive.

Specifying the Scan Code for a Key in Horizon View Client 2.3 or Later

The *scanCode* value must be in hexadecimal format. To determine which code to use, open the appropriate language- and keyboard-specific file in the `lib/vmware/xkeymap` directory on your client system.

The following list shows the example contents of a `/etc/vmware/view-keycombos-config` file. Code comments are preceded by the # character.

```
<ctrl>0x152      #block ctrl-insert
<alt>15          #block alt-tab
<Ctrl><Alt>0x153 #block ctrl-alt-del
<any>0x137       #block any combinations of the Print key
0x010               #block the individual Q key in a US English keyboard
                 #or block the individual A key in a French keyboard
0x03b            #block the individual F1 key
0x04f            #block the individual 1 key in a numeric keypad
```

Specifying a Key Name in Horizon View Client 2.2

The *keyName* value is case-sensitive and can be any of the following: the numbers `0` through `9`, the function keys `F1` through `F12`, lowercase or uppercase letters `A` through `Z`, or any of the other keys in the list that follows.

NOTE In the list that follows, the keys prefixed with `KP`, such as in `KP_Enter`, mean keys in the numeric keypad.

BackSpace	Execute	KP_Page_Down	quotedbl	asciicircum
Tab	Insert	KP_End	numbersign	underscore
Linefeed	Undo	KP_Begin	dollar	grave
Clear	Redo	KP_Insert	percent	quoteleft
Return	Menu	KP_Delete	ampersand	braceleft
Pause	Find	KP_Equal	apostrophe	bar
Scroll_Lock	Cancel	KP_Multiply	quoteright	braceright
Sys_Req	Help	KP_Add	quoteleft	asciitilde
Escape	Break	KP_Separator	parenleft	
Delete	Num_Lock	KP_Subtract	parenright	
Multi_key	KP_Space	KP_Decimal	asterisk	
Codeinput	KP_Tab	KP-Divide	plus	
Home	KP_Enter	KP_0	comma	
Left	KP_F1	KP_1	minus	
Up	KP_F2	KP_2	period	
Right	KP_F3	KP_3	slash	
Down	KP_F4	KP_4	colon	
Prior	KP_Home	KP_5	less	

Page_Up	KP_Left	KP_6	equal
Next	KP_UP	KP_7	greater
Page_Down	KP_Right	KP_8	question
End	KP_Down	KP_9	at
Begin	KP_Prior	Caps_Lock	bracketleft
Select	KP_Page_Up	space	backslash
Print	KP_Next	exclam	bracketright

The following list shows the example contents of a `/etc/vmware/view-keycombos-config` file:

```
<ctrl><alt>Delete
<alt>Tab
<alt>1
<alt>h
<ctrl>1
<ctrl>S
<ctrl>h
<super>h
<shift>h
<ctrl>space
<Ctrl>KP_Enter
<Ctrl>Up
```

Configuring Certificate Checking for End Users

Administrators can configure the certificate verification mode so that, for example, full verification is always performed.

Certificate checking occurs for SSL connections between View Connection Server and Horizon View Client. Administrators can configure the verification mode to use one of the following strategies:

- End users are allowed to choose the verification mode. The rest of this list describes the three verification modes.
- (No verification) No certificate checks are performed.
- (Warn) End users are warned if a self-signed certificate is being presented by the server. Users can choose whether or not to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

For details about the types of verification checks performed, see "Certificate Checking Modes for Horizon View Client," on page 37.

Use the `view.sslVerificationMode` property to set the default verification mode:

- **`1`** implements `Full Verification`.
- **`2`** implements `Warn If the Connection May Be Insecure`.
- **`3`** implements `No Verification Performed`.

To configure the mode so that end users cannot change the mode, set the `view.allowSslVerificationMode` property to **`"False"`** in the `/etc/vmware/view-mandatory-config` file on the client system. See "View Client Configuration Settings and Command-Line Options," on page 22.

Using FreeRDP for RDP Connections

If you plan to use RDP rather than PCoIP for connections to View desktops, you can choose between using an `rdesktop` client or `xfreerdp`, the open-source implementation of the Remote Desktop Protocol (RDP), released under the Apache license.

Because the `rdesktop` program is no longer being actively developed, View Client 1.7 and later can also run the `xfreerdp` executable if your Linux machine has the required version and patches for FreeRDP.

You can use the `vmware-view` command-line interface or some properties in configuration files to specify options for `xfreerdp`, just as you can for `rdesktop`.

- To specify that View Client should run `xfreerdp` rather than `rdesktop`, use the appropriate command-line option or configuration key.

Command-line option:	`--rdpclient="xfreerdp"`
Configuration key:	`view.rdpClient="xfreerdp"`

- To specify options to forward to the `xfreerdp` program, use the appropriate command-line option or configuration key, and specify the FreeRDP options.

Command-line option:	`--xfreerdpOptions`
Configuration key:	`view.xfreerdpOptions`

Many configuration options for the `rdesktop` program are the same as for the `xfreerdp` program. One important difference is that `xfreerdp` supports network-level authentication (NLA). NLA is turned off by default. You must use the following command-line option to turn on network-level authentication:

```
--enableNla
```

For more information about using the `vmware-view` command-line interface and configuration files, see "Using the View Client Command-Line Interface and Configuration Files," on page 21.

You must have the correct version of FreeRDP installed, along with any applicable patches. For more information, see "Install and Configure FreeRDP," on page 32.

Install and Configure FreeRDP

To use a FreeRDP client for RDP connections to View desktops, your Linux machine must include the required version and patches for FreeRDP.

You must have FreeRDP 1.0.x installed and install the applicable patches so that the `--from-stdin` and `-X` options will work correctly.

For a list of the packages that `xfreerdp` depends on in Ubuntu, go to https://github.com/FreeRDP/FreeRDP/wiki/Compilation.

Procedure

1 On your Linux client machine, download FreeRDP 1.0.x from GitHub, at https://github.com/FreeRDP/FreeRDP.

2 If you install FreeRDP 1.0.1, patch with the file called `freerdp-1.0.1.patch`, using following patch command:

```
patch -p1 < freerdp-1.0.1.patch
```

3 To build and install FreeRDP, open a terminal window and run the following commands.

   a Run the following command:

   ```
   cmake –DWITH_SSE2=ON –DWITH_PULSEAUDIO=ON –DWITH_PCSC=ON .
   ```

   b Run the following command:

   ```
   make
   ```

   c Run the following command, which installs the built `xfreerdp` binary in a directory on the execution PATH so that View Client can run the program by executing `xfreerdp`:

   ```
   sudo make install
   ```

Enabling FIPS Mode on the Client

You can set a configuration property so that the client uses only FIPS (Federal Information Processing Standard) 140-2 approved cryptographic algorithms and protocols to establish a remote PCoIP connection.

NOTE View PCoIP FIPS mode does not support AES-256 encryption algorithms.

This setting applies to both server and client. You can configure either endpoint or both endpoints to operate in FIPS mode. Configuring a single endpoint to operate in FIPS mode limits the encryption algorithms that are available for session negotiation.

IMPORTANT If you enable FIPS mode on one endpoint but the other endpoint does not support cryptographic algorithms that are approved by FIPS 140-2, the connection will fail.

When this setting is disabled or not configured, FIPS mode is not used.

Setting the Configuration Property

To enable or disable FIPS mode, you can set the `pcoip.enable_fips_mode` property. Setting the property to **`1`** turns on FIPS mode, and setting the property to **`0`** turns off FIPS mode. For example, the following setting turns on FIPS mode:

```
pcoip.enable_fips_mode = 1
```

Use a space before and after the equals (=) sign.

You can set this property in any of several files. When View Client starts up, the setting is processed from various locations in the following order:

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

If a setting is defined in multiple locations, the value that is used is the value from the last file read.

Configuring the PCoIP Client-Side Image Cache

PCoIP client-side image caching stores image content on the client to avoid retransmission. This feature is enabled by default to reduce bandwidth usage.

IMPORTANT This feature is available only when the version of View Agent and View Connection Server is View 5.0 or later.

The PCoIP image cache captures spatial, as well as temporal, redundancy. For example, when you scroll down through a PDF document, new content appears from the bottom of the window and the oldest content disappears from the top of the window. All the other content remains constant and moves upward. The PCoIP image cache is capable of detecting this spatial and temporal redundancy.

Because during scrolling, the display information sent to the client device is primarily a sequence of cache indices, using the image cache saves a significant amount of bandwidth. This efficient scrolling has benefits both on the LAN and over the WAN.

- On the LAN, where bandwidth is relatively unconstrained, using client-side image caching delivers significant bandwidth savings.
- Over the WAN, to stay within the available bandwidth constraints, scrolling performance is often degraded unless client-side caching is used. In this situation, client-side caching can save bandwidth and ensure a smooth, highly responsive scrolling experience.

By default this feature is enabled, so that the client stores portions of the display that were previously transmitted. The default cache size is 250MB. You can configure the client image cache size, from a minimum of 50MB to a maximum of 1024MB for View Client 1.7 and later versions. The maximum size for earlier versions is 300MB. A larger cache size reduces bandwidth usage but requires more memory on the client. A smaller cache size requires more bandwidth usage. For example, a thin client with little memory requires a smaller cache size.

Setting the Configuration Property

To configure the cache size, you can set the `pcoip.image_cache_size_mb` property. For example, the following setting configures the cache size to be 50MB:

```
pcoip.image_cache_size_mb = 50
```

Use a space before and after the equals (=) sign. If you specify a number less than 50, the number is converted to 50. If you specify a number larger than the maximum, the number is converted to maximum.

You can set this property in any of several files. When View Client starts up, the setting is processed from various locations in the following order:

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

If a setting is defined in multiple locations, the value that is used is the value from the last file read.

NOTE You can set the following property to display a visual indication that the image cache is working:

```
pcoip.show_image_cache_hits = 1
```

With this configuration, for every tile (32 x 32 pixels) in an image that comes from the image cache, you can see a rectangle around the tile.

Managing Server Connections and Desktops 3

Use Horizon View Client to connect to View Connection Server or a security server and log in to or off of a remote desktop. For troubleshooting purposes, you can also reset a remote desktop assigned to you.

Depending on how the administrator configures policies for remote desktops, end users might be able to perform many operations on their desktops.

- Log In to a Remote Desktop for the First Time on page 35

  Before you have end users access their remote desktops, test that you can log in to a remote desktop from the client system.

- Certificate Checking Modes for Horizon View Client on page 37

  Administrators and sometimes end users can configure whether client connections are rejected if any or some server certificate checks fail.

- Switch Desktops on page 38

  If you are connected to a desktop, you can switch to another desktop.

- Log Off or Disconnect from a Desktop on page 38

  If you disconnect from a remote desktop without logging off, applications remain open.

- Roll Back a Desktop on page 39

  Rolling back discards changes made to a virtual desktop that you checked out for use in local mode on a Windows PC or laptop.

Log In to a Remote Desktop for the First Time

Before you have end users access their remote desktops, test that you can log in to a remote desktop from the client system.

Prerequisites

- Obtain the credentials that you need to log in, such as Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- Obtain the domain name for logging in.
- Perform the administrative tasks described in "Preparing View Connection Server for Horizon View Client," on page 11.
- If you are outside the corporate network and are not using a security server to access the remote desktop, verify that your client device is set up to use a VPN connection and turn that connection on.

IMPORTANT VMware recommends using a security server rather than a VPN.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop. You also need the port number if the port is not 443.
- If you plan to use the RDP display protocol to connect to a remote desktop, verify that the AllowDirectRDP View Agent group policy setting is enabled.
- If your administrator has allowed it, you can configure the certificate checking mode for the SSL certificate that the View server presents. See "Certificate Checking Modes for Horizon View Client," on page 37.

Procedure

1 Either open a terminal window and enter `vmware-view` or select **Applications > Internet > VMware Horizon View Client** from the Ubuntu menu bar.

2 Enter the server name and a port number if required, and click **Continue**.

An example using a nondefault port is `view.company.com:1443`.

3 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.

4 Enter your user name and password, select a domain, and click **OK**.

You might see a message that you must confirm before the login dialog box appears.

5 If the desktop security indicator turns red and a warning message appears, respond to the prompt.

Usually, this warning means that View Connection Server did not send a certificate thumbprint to the client. The thumbprint is a hash of the certificate public key and is used as an abbreviation of the public key. View Connection Server 4.6.1, 5.0.1, and later versions send thumbprint information, but earlier versions do not.

6 (Optional) Select the display protocol and window size to use.

Option	Description
Display protocol	The default is **PCoIP**. To use Microsoft RDP instead, click **PCoIP** under the desktop name to toggle and select **Microsoft RDP**.
Window size	The default is **Full Screen - All Monitors**. To choose another window size, click one of the other options under the desktop name, such as **Large Screen** or **Custom Size**.

7 Double-click a remote desktop shortcut to connect.

After you are connected, the client window appears. If Horizon View Client cannot connect to the desktop, perform the following tasks:

- Determine whether View Connection Server is configured not to use SSL. Horizon View Client requires SSL connections. Check whether the global setting in View Administrator for the **Use SSL for client connections** check box is deselected. If so, you must either select the check box, so that SSL is used, or set up your environment so that clients can connect to an HTTPS enabled load balancer or other intermediate device that is configured to make an HTTP connection to View Connection Server.
- Verify that the security certificate for View Connection Server is working properly. If it is not, in View Administrator, you might also see that the View Agent on desktops is unreachable.
- Verify that the tags set on the View Connection Server instance allow connections from this user. See the *VMware Horizon View Administration* document.
- Verify that the user is entitled to access this desktop. See the *VMware Horizon View Administration* document.

- If you are using the RDP display protocol to connect to a remote desktop, verify that the client computer allows remote desktop connections.

Certificate Checking Modes for Horizon View Client

Administrators and sometimes end users can configure whether client connections are rejected if any or some server certificate checks fail.

Certificate checking occurs for SSL connections between View Connection Server and Horizon View Client. Certificate verification includes the following checks:

- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon View Client to a server that has a certificate that does not match the host name entered in Horizon View Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

  To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

NOTE For instructions about distributing a self-signed root certificate that users can install on their Linux client systems, see the Ubuntu documentation.

Horizon View Client uses the PEM-formatted certificates stored in the `/etc/ssl/certs` directory on the client system. For instructions about importing a root certificate stored in this location, see the procedure called "Importing a Certificate into the System-Wide Certificate Authority Database" in the document at https://help.ubuntu.com/community/OpenSSL.

In addition to presenting a server certificate, View Connection Server 4.6.1, 5.0.1, and later versions also send a certificate thumbprint to Horizon View Client. The thumbprint is a hash of the certificate public key and is used as an abbreviation of the public key. If the View server does not send a thumbprint, you see a warning that the connection is untrusted.

If your administrator has allowed it, you can set the certificate checking mode. Select **File > Preferences** from the VMware Horizon View Client menu bar or the View desktop menu bar. You have three choices:

- **Never connect to untrusted servers**. If any of the certificate checks fails, the client cannot connect to the server. An error message lists the checks that failed.
- **Warn before connecting to untrusted servers**. If a certificate check fails because the server uses a self-signed certificate, you can click **Continue** to ignore the warning. For self-signed certificates, the certificate name is not required to match the View Connection Server name you entered in Horizon View Client.
- **Do not verify server identity certificates**. This setting means that View does not perform any certificate checking.

Switch Desktops

If you are connected to a desktop, you can switch to another desktop.

Procedure

- Select a remote desktop from the same server or a different server.

Option	Action
Choose a different remote desktop on the same server	Select **Desktop > Disconnect** from the menu bar.
Choose a remote desktop on a different server	Select **File > Disconnect from server** from the menu bar.

Log Off or Disconnect from a Desktop

If you disconnect from a remote desktop without logging off, applications remain open.

Even if you do not have a remote desktop open, you can log off of the remote desktop operating system. Using this feature has the same result as sending Ctrl+Alt+Del to the desktop and then clicking **Log Off**.

Procedure

- Disconnect without logging off.

Option	Action
Also quit Horizon View Client	Click the **Close** button in the corner of the window or select **File > Quit** from the menu bar.
Choose a different remote desktop on the same server	Select **Desktop > Disconnect** from the menu bar.
Choose a remote desktop on a different server	Select **File > Disconnect from server** from the menu bar.

NOTE Your View administrator can configure your desktop to automatically log off when disconnected. In that case, any open programs in your desktop are stopped.

- Log off and disconnect from a desktop.

Option	Action
From within the desktop OS	Use the Windows **Start** menu to log off.
From the menu bar	Select **Desktop > Disconnect and Log off**. If you use this procedure, files that are open on the remote desktop will be closed without being saved first.

- Log off when you do not have a remote desktop open.

  a From the Home screen with desktop shortcuts, select the desktop and select **Desktop > Log off** from the menu bar.

  b If prompted, supply credentials for accessing the remote desktop.

  If you use this procedure, files that are open on the remote desktop will be closed without being saved first.

Roll Back a Desktop

Rolling back discards changes made to a virtual desktop that you checked out for use in local mode on a Windows PC or laptop.

You can roll back a remote desktop only if your View administrator has enabled this feature and only if you checked out the desktop.

CAUTION If changes were made to the local mode desktop and those changes were not replicated back to the View server before rolling back, the changes are lost.

Prerequisites

- Obtain the credentials that you need to log in, such as Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- Back up the desktop to the server to preserve data or files.

  You can use View Administrator to replicate data to the server, or, if the policy is set to allow it, you can use View Client with Local Mode on the Windows client where the desktop is currently checked out.

Procedure

1. If the Horizon View Client Home screen displays the **View Connection Server** prompt, supply the server name and click **Continue.**
   a. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.
   b. Enter your user name and password in the login dialog box.
2. On the Horizon View Client Home screen that displays remote desktop shortcuts, select the desktop and select **Desktop > Rollback Desktop** from the menu bar.

After the remote desktop is rolled back, you can log in to it from the Linux client.

Using a Microsoft Windows Desktop on a Linux System

4

View Client for Linux supports some of the features included in View Client for Windows.

This chapter includes the following topics:

Feature Support Matrix for Linux

Some features are supported on one type of View Client but not on another. For example, local mode is supported only on View Client for Windows.

Table 4-1. Features Supported on Windows Desktops for Linux Clients

Feature	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008 R2 Desktop
RSA SecurID or RADIUS	X	X	X	X	X
Single sign-on	X	X	X	X	X
RDP display protocol	X	X	X	X	X
PCoIP display protocol	X	X	X	X	X
USB access	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only
Real-Time Audio-Video (RTAV)	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only
Wyse MMR			Partner client systems only, and only with RDP	Partner client systems only, and only with RDP	
Windows 7 MMR					
Virtual printing	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only	

Table 4-1. Features Supported on Windows Desktops for Linux Clients (Continued)

Feature	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008 R2 Desktop
Location-based printing	X	X	X	X	
Smart cards	Partner client systems only, and only with PCoIP	Partner client systems only	Partner client systems only	Partner client systems only	Partner client systems only
Multiple monitors	X	X	X	X	X
Local mode					

Features that are supported on Windows desktops for Linux View Client have the following restrictions.

- Windows 8.x desktops are supported only if you have Horizon View 5.2 or later servers and desktops.
- The real-time audio-video feature is supported only if you have Horizon View 5.2 with Feature Pack 2 or later.
- Windows Server 2008 R2 desktops are supported only if you have Horizon View 5.3 or later servers and desktops.

For descriptions of these features and their limitations, see the *VMware Horizon View Planning* document.

NOTE This feature support matrix applies to the View Client for Linux that VMware makes available on Ubuntu. In addition, several VMware partners offer thin client devices for Horizon View deployments. The features that are available for each thin client device are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Internationalization

The user interface and documentation are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, and Korean.

If you are using a Ubuntu 10.4 Linux client system and you want to display the View Client user interface in a language other than English, you must set the client system to use a locale that uses UTF-8 encoding.

Keyboards and Monitors

You can use multiple monitors and all types of keyboards with a remote desktop. Certain settings ensure the best possible user experience.

Best Practices for Using Multiple Monitors

Following are recommendations for successfully using multiple monitors with a remote desktop:

- Define the primary monitor as the bottom-left-most monitor.
- The menu bar will appear on the top-left-most monitor. For example, if you have two monitors side by side and the top of the left monitor is lower than the top of the right monitor, the menu bar will appear on the right monitor because the right monitor is still the top-left-most monitor.
- You can use up to 4 monitors if you have enough video RAM.

To use more than 2 monitors to display your remote desktop on a Ubuntu client system, you must configure the `kernel.shmmax` setting correctly. Use the following formula:

max horizontal resolution X *max vertical resolution* X *max number of monitors* X 4

For example, manually setting `kernel.shmmax` to 65536000 allows you to use four monitors with a screen resolution of 2560x1600.

- Horizon View Client uses the monitor configuration that is in use when Horizon View Client starts. If you change a monitor from landscape to portrait mode or if you plug an additional monitor in to the client system while Horizon View Client is running, you must restart Horizon View Client in order to use the new monitor configuration.

Horizon View Client supports the following monitor configurations:

- If you use 2 monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.
- If you use more than 2 monitors, the monitors must be in the same mode and have the same screen resolution. That is, if you use 3 monitors, all 3 monitors must be in either portrait mode or landscape mode and must use the same screen resolution.
- Monitors can be placed side by side, stacked 2 by 2, or vertically stacked only if you are using 2 monitors.

Screen Resolution

Consider the following guidelines when setting screen resolutions:

- If you open a remote desktop on a secondary monitor and then change the screen resolution on that monitor, the remote desktop moves to the primary monitor.
- With PCoIP, if you use 2 monitors, you can adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per display. If you use more than 2 monitors, the monitors must use the same screen resolution.
- With RDP, if you have multiple monitors, you cannot adjust the resolution for each monitor separately.

Keyboard Limitations

For the most part, keyboards work as well with a remote desktop as they do with a physical computer. Following is a list of the limitations you might encounter, depending on the type of peripherals and software on your client system:

- If you use the PCoIP display protocol and want the remote desktop to detect which keyboard map your client system uses, such as, for example, a Japanese keyboard or a German keyboard, you must set a GPO in the View agent. Use the **Turn on PCOIP user default input language synchronization** policy, available as part of the View PCoIP Session Variables ADM template file. For more information, see the *VMware Horizon View Administration* document.
- Some multimedia keys on a multimedia keyboard might not work. For example, the Music key and My Computer key might not work.
- If you connect to a desktop using RDP and if you have the Fluxbox window manager, if a screen saver is running in the remote desktop, after a period of inactivity, the keyboard might stop working.

  Regardless of which window manager you use, VMware recommends turning off the screen saver in a remote desktop and not specifying a sleep timer.

Using the Real-Time Audio-Video Feature for Webcams and Microphones

With the Real-Time Audio-Video feature, you can use your local computer's webcam or microphone on your remote desktop.

This feature is available when used in conjunction with VMware Horizon View 5.2 Feature Pack 2 or a later release. For information about setting up the Real-Time Audio-Video feature and configuring the frame rate and image resolution in a remote desktop, see the *VMware Horizon View Feature Pack Installation and Administration* guide. For information about configuring these settings on client systems, see the VMware knowledge base article *Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients*, at http://kb.vmware.com/kb/2053644.

To download a test application that verifies the correct installation and operation of the Real-Time Audio-Video functionality, go to http://labs.vmware.com/flings/real-time-audio-video-test-application. This test application is available as a VMware fling, and therefore no technical support is available for it.

NOTE This feature is available only with the version of Horizon View Client for Linux provided by third-party vendors.

When You Can Use Your Webcam

If your Horizon View administrator has configured the Real-Time Audio-Video feature, and if you use the PCoIP display protocol, a webcam that is built-in or connected to your local computer can be used on your desktop. You can use the webcam in conferencing applications such as Skype, Webex, or Google Hangouts.

During the setup of an application such as Skype, Webex, or Google Hangouts on your remote desktop, you can choose VMware Virtual Microphone and VMware Virtual Webcam as input devices and VMware Virtual Audio as output device from menus in the application. With many applications, however, this feature will just work, and selecting an input device will not be necessary.

If the webcam is currently being used by your local computer it cannot be used by the remote desktop simultaneously. Also, if the webcam is being used by the remote desktop it cannot be used by your local computer at the same time.

IMPORTANT If you are using a USB webcam, your administrator must not configure the client to automatically forward devices through USB redirection. If the webcam connects through USB redirection, the performance will be unusable for video chat.

If you have more than one webcam connected to your local computer, your administrator can configure a preferred webcam that will be used on your remote desktop. Consult with your Horizon View administrator if you are not sure which webcam is selected.

Select a Default Microphone on a Linux Client System

If you have multiple microphones on your client system, only one of them is used on your View desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

This procedure describes choosing a default microphone from the user interface of the client system. Administrators can also configure a preferred microphone by editing a configuration file. See "Select a Preferred Webcam or Microphone on a Linux Client System," on page 45.

Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your remote desktop.

Procedure

1 In the Ubuntu graphical user interface, select **System > Preferences > Sound**.

You can alternatively click the **Sound** icon on the right side of the toolbar at the top of the screen.

2 Click the **Input** tab in the Sound Preferences dialog box.

3 Select the preferred device and click **Close**.

Select a Preferred Webcam or Microphone on a Linux Client System

With the Real-Time Audio-Video feature, if you have multiple webcams and microphones on your client system, only one webcam and one microphone can be used on your View desktop. To specify which webcam and microphone are preferred, you can edit a configuration file.

The preferred webcam or microphone is used on the View desktop if it is available, and if not, another webcam or microphone is used.

With the Real-Time Audio-Video feature, webcams, audio input devices, and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

To set the properties in the `/etc/vmware/config` file and specify a preferred device, you must determine the device ID.

- For webcams, you set the `rtav.srcWCamId` property to the value of the webcam description found in the log file, as described in the procedure that follows.
- For audio devices, you set the `rtav.srcAudioInId` property to the value of the Pulse Audio `device.description` field.

  To find the value of this field you can search the log file, as described in the procedure that follows.

Prerequisites

Depending on whether you are configuring a preferred webcam, preferred microphone, or both, perform the appropriate prerequisite tasks:

- Verify that you have a USB webcam installed and operational on your client system.
- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your remote desktop.

Procedure

1 Launch the client, and start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the client log.

   a Attach the webcam or audio device you want to use.

   b Use the command `vmware-view` to start View Client.

   c Start a call and then stop the call.

   This process creates a log file.

2 Find log entries for the webcam or microphone.

a Open the debug log file with a text editor.

The log file with real-time audio-video log messages is located at `/tmp/vmware-<username>/vmware-mks-<pid>.log`. The client log is located at `/tmp/vmware-<username>/vmware-view-<pid>.log`.

b Search the log file to find the log file entries that reference the attached webcams and microphones.

The following example shows an extract of the webcam selection:

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=Microsoft®
LifeCam HD-6000 for Notebooks   UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

The following example shows an extract of the audio device selection, and the current audio level for each:

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering
enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of
Microsoft LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
```

Warnings are shown if any of the source audio levels for the selected device do not meet the PulseAudio criteria if the source is not set to 100% (0dB), or if the selected source device is muted, as follows:

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 Copy the description of the device and use it to set the appropriate property in the `/etc/vmware/config` file.

   For a webcam example, copy `Microsoft® LifeCam HD-6000 for Notebooks` to specify the Microsoft webcam as the preferred webcam and set the property as follows:

   ```
   rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
   ```

   For this example you could also set the property to `rtav.srcWCamId="Microsoft"`.

   For an audio device example, copy `Logitech USB Headset Analog Mono` to specify the Logitech headset as the preferred audio device and set the property as follows:

   ```
   rtav.srcAudioInId="Logitech USB Headset Analog Monoo"
   ```

4 Save your changes and close the `/etc/vmware/config` configuration file.

5 Start a new call.

Set Printing Preferences for the Virtual Printer Feature

The virtual printing feature lets end users use local or network printers from a remote desktop without requiring that additional print drivers be installed in the remote desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

IMPORTANT The virtual printing feature is available only with the version of Horizon View Client for Linux that is provided by third-party vendors. For more information about VMware thin-client and zero-client partners, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm. This feature also has the following requirements:

- The version of Horizon View Client for Linux must be 2.1 or later.
- The version of View Agent and View Connection Server must be Horizon View 5.2 or later.
- You must be using the PCoIP display protocol or FreeRDP. This feature does not work with rdesktop.

After a printer is added on the local computer, Horizon View Client adds that printer to the list of available printers on the remote desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the remote desktop without creating a conflict with the virtual printer component.

IMPORTANT This feature is not available for the following types of printers:

- USB printers that are using the USB redirection feature to connect to a virtual USB port in the remote desktop

  You must disconnect the USB printer from the remote desktop in order to use the virtual printing feature with it.

- The Windows feature for printing to a file

  Selecting the **Print to file** check box in a Print dialog box does not work. Using a printer driver that creates a file does work. For example, you can use a PDF writer to print to a PDF file.

This procedure is written for a remote desktop that has a Windows 7 or Windows 8.x (Desktop) operating system. The procedure is similar but not exactly the same for Windows XP and Windows Vista.

Prerequisites

Verify that the Virtual Printing component of View Agent is installed on the remote desktop. In the remote desktop file system, the drivers are located in `C:\Program Files\Common Files\VMware\Drivers\Virtual Printer`.

Installing View Agent is one of the tasks required for preparing a virtual machine to be used as a remote desktop. For more information, see the *VMware Horizon View Administration* document.

Procedure

1 In the Windows 7 or Windows 8.x remote desktop, click **Start > Devices and Printers**.

2 In the Devices and Printers window, right-click the default printer, select **Printer Properties** from the context menu, and select the printer.

In the remote desktop, virtual printers appear as <*printer_name*>#:<*number*>.

3 In the Printer Properties window, click the **Device Setup** tab and specify which settings to use.

4 On the **General** tab, click **Preferences** and specify which settings to use.

5 In the Printing Preferences dialog box, select the different tabs and specify which settings to use.

For the **Page Adjustment** advanced setting, VMware recommends that you retain the default settings.

6 Click **OK**.

Copying and Pasting Text

By default, you can copy and paste text from your client system to a remote View desktop. If your administrator enables the feature, you can also copy and paste text from a View desktop to your client system or between two View desktops. Some restrictions apply.

If you use the PCoIP display protocol and you are using a View 5.x or later View desktop, your View administrator can set this feature so that copy and paste operations are allowed only from your client system to a View desktop, or only from a View desktop to your client system, or both, or neither.

Administrators configure the ability to copy and paste by using group policy objects (GPOs) that pertain to View Agent in View desktops. For more information, see the topic about View PCoIP general session variables in the *VMware Horizon View Administration* document, in the chapter about configuring policies.

You can copy plain text or formatted text from View Client to a View desktop, or the reverse, but the pasted text is plain text.

You cannot copy and paste graphics. You also cannot copy and paste files between a View desktop and the file system on your client computer.

Troubleshooting Horizon View Client 5

You can solve most problems with Horizon View Client by resetting the desktop or by reinstalling the VMware Horizon View Client application.

This chapter includes the following topics:

Reset a Desktop

You might need to reset a desktop if the desktop operating system stops responding. Resetting shuts down and restarts the desktop. Unsaved data is lost.

Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop will be closed without being saved first.

You can reset the desktop only if your View administrator has enabled this feature.

Procedure

- Use the **Reset Desktop** command.

Option	Action
From within the desktop OS	Select **Desktop > Reset Desktop** from the menu bar.
From Home screen with desktop icons	Select the desktop and select **Desktop > Reset Desktop** from the menu bar.

The operating system in the remote desktop is rebooted. Horizon View Client disconnects from the desktop.

What to do next

Wait an appropriate amount of time for system startup before attempting to connect to the remote desktop.

Uninstalling Horizon View Client

You can sometimes resolve problems with Horizon View Client by uninstalling and reinstalling the Horizon View Client application.

You uninstall Horizon View Client by using the same method that you usually use to uninstall any other application.

For example, select **Applications > Ubuntu Software Center**, and in the **Installed Software** section, select **vmware-view-client** and click **Remove.**

After uninstalling is complete, you can reinstall the application.

See “Install Horizon View Client for Linux,” on page 11.

Configuring USB Redirection on the Client

6

With View Client 1.6, you can use a configuration file on the client system to specify which USB devices can be redirected to a View desktop. Note that the USB component is available only with the version of View Client for Linux provided by third-party vendors.

You can configure USB policies for both View Agent, on the remote desktop, and View Client, on the local system, to achieve the following goals:

- Restrict the types of USB devices that View Client makes available for redirection.
- Make View Agent prevent certain USB devices from being forwarded from a client computer.
- (View Client 1.7 and later) Specify whether View Client should split composite USB devices into separate components for redirection.

IMPORTANT The USB redirection feature is available only when the version of View Agent and View Connection Server is View 4.6.1 or later and only with the version of View Client provided by third-party vendors. The USB filtering features and device splitting features described in these topics are available with View Connection Server 5.1 and later. For more information about VMware thin-client and zero-client partners, see the VMware Compatibility Guide.

In order to use the USB components available for third-party vendors of View Client 1.6 and later, certain files must be installed in certain locations, and certain processes must be configured to start before View Client is launched. These details are beyond the scope of this document.

This chapter includes the following topics:

Setting USB Configuration Properties

You can set the USB properties in any one of several configuration files.

1. `/etc/vmware/config`. The `vmware-view-usbd` service first examines this file. If USB configuration properties are set in this file, those properties are used.
2. `/usr/lib/vmware/config`. If the USB properties are not found in `/etc/vmware/config`, the `/usr/lib/vmware/config` file is checked.
3. `~/.vmware/config`. If USB properties are not found in the other files, the `~/.vmware/config` file is checked.

Use the following syntax to set these properties in the configuration file.

```
viewusb.property1 = "value1"
```

NOTE With these properties, you can allow certain types of devices to be redirected or not. Filtering properties are also available so that you can exclude some types of devices and include others. For Linux clients version 1.7 and later, and for Windows clients, properties for splitting composite devices are also available.

Some values require the VID (vendor ID) and PID (product ID) for a USB device. To find the VID and PID, you can search on the Internet for the product name combined with `vid` and `pid`. Alternatively, you can look in the `/tmp/vmware-root/vmware-view-usbd-*.log` file after you plug in the USB device to the local system when View Client is running. To set the location of this file, use the `view-usbd.log.fileName` property in the `/etc/vmware/config` file; for example:

```
view-usbd.log.fileName = "/tmp/usbd.log"
```

IMPORTANT With regards to redirecting audio devices, make sure the kernel version of your Ubuntu system is 3.2.0-27.43 or later. Ubuntu 12.04 includes kernel version 3.2.0-27.43. If you cannot upgrade to this kernel version, you can alternatively disable host access to the audio device. For example, you can add the line "`blacklist snd-usb-audio`" at the end of the `/etc/modprobe.d/blacklist.conf` file. If your system does not meet either of these requirements, the client system might crash when View Client attempts to redirect the audio device. By default, audio devices are redirected.

Table 6-1. Configuration Properties for USB Redirection

Policy Name and Property	Description
Allow Auto Device Splitting Property: `viewusb.AllowAutoDeviceSplitting`	(View Client 1.7 and later) Allow the automatic splitting of composite USB devices. The default value is undefined, which equates to **`false`**.
Exclude Vid/Pid Device From Split Property: `viewusb.SplitExcludeVidPid`	(View Client 1.7 and later) Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is `vid-`*xxx1*`_pid-`*yyy1*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-55**`** The default value is undefined.
Split Vid/Pid Device Property: `viewusb.SplitVidPid`	(View Client 1.7 and later) Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` You can use the `exintf` keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **NOTE** If the composite device includes components that are automatically excluded, such as mouse and keyboard components, then View does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as `Include Vid/Pid Device` to include those components. The default value is undefined.
Allow Audio Input Devices Property: `viewusb.AllowAudioIn`	Allows audio input devices to be redirected. The default value is undefined, which equates to **`false`** in View Client 2.2 or later, but equates to **`true`** in View Client 2.1 and earlier. The default was changed because with View Client 2.2, the real-time audio-video feature is used for audio input and video devices, and USB redirection is not used for those devices by default.

Table 6-1. Configuration Properties for USB Redirection (Continued)

Policy Name and Property	Description
Allow Audio Output Devices Property: `viewusb.AllowAudioOut`	Allows audio output devices to be redirected. The default value is undefined, which equates to **`false`**.
Allow HID Property: `viewusb.AllowHID`	Allows input devices other than keyboards or mice to be redirected. The default value is undefined, which equates to **`true`**.
Allow HIDBootable Property: `viewusb.AllowHIDBootable`	Allows input devices other than keyboards or mice that are available at boot time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to **`true`**.
Allow Device Descriptor Failsafe Property: `viewusb.AllowDevDescFailsafe`	Allows devices to be redirected even if the View client fails to get the config/device descriptors. To allow a device even if it fails the config/desc, include it in the Include filters, such `IncludeVidPid` or `IncludePath`. The default value is undefined, which equates to **`false`**.
Allow Keyboard and Mouse Devices Property: `viewusb.AllowKeyboardMouse`	Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be redirected. The default value is undefined, which equates to **`false`**.
Allow Smart Cards Property: `viewusb.AllowSmartcard`	Allows smart-card devices to be redirected. The default value is undefined, which equates to **`false`**.
Allow Video Devices Property: `viewusb.AllowVideo`	Allows video devices to be redirected. The default value is undefined, which equates to **`false`** in View Client 2.2 or later, but equates to **`true`** in View Client 2.1 and earlier. The default was changed because with View Client 2.2, the real-time audio-video feature is used for audio input and video devices, and USB redirection is not used for those devices by default.
Disable Remote Configuration Download Property: `viewusb.DisableRemoteConfig`	Disables the use of View Agent settings when performing USB device filtering. The default value is undefined, which equates to **`false`**.
Exclude All Devices Property: `viewusb.ExcludeAllDevices`	Excludes all USB devices from being redirected. If set to **`true`**, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to **`false`**, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of `Exclude All Devices` to **`true`** on View Agent, and this setting is passed to View Client, the View Agent setting overrides the View Client setting. The default value is undefined, which equates to **`false`**.
Exclude Device Family Property: `viewusb.ExcludeFamily`	Excludes families of devices from being redirected. The format of the setting is *family_name_1*[`;`*family_name_2*]... For example: **`bluetooth;smart-card`** If you have enabled automatic device splitting, View examines the device family of each interface of a composite USB device to decide which interfaces should be excluded. If you have disabled automatic device splitting, View examines the device family of the whole composite USB device. The default value is undefined.
Exclude Vid/Pid Device Property: `viewusb.ExcludeVidPid`	Excludes devices with specified vendor and product IDs from being redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-****;vid-0561_pid-554c`** The default value is undefined.

Table 6-1. Configuration Properties for USB Redirection (Continued)

Policy Name and Property	Description
Exclude Path Property: `viewusb.ExcludePath`	Exclude devices at specified hub or port paths from being redirected. The format of the setting is `bus-`*x1*`[/`*y1*`]..._port-`*z1*`[;bus-`*x2*`[/`*y2*`]..._port-`*z2*`]...` You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** The default value is undefined.
Include Device Family Property: `viewusb.IncludeFamily`	Includes families of devices that can be redirected. The format of the setting is *family_name_1*`[;`*family_name_2*`]...` For example: **`storage`** The default value is undefined.
Include Path Property: `viewusb.IncludePath`	Include devices at a specified hub or port paths that can be redirected. The format of the setting is `bus-`*x1*`[/`*y1*`]..._port-`*z1*`[;bus-`*x2*`[/`*y2*`]..._port-`*z2*`]...` You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** The default value is undefined.
Include Vid/Pid Device Property: `viewusb.IncludeVidPid`	Includes devices with specified vendor and product IDs that can be redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0561_pid-554c`** The default value is undefined.

Additional Examples

Each example is followed by a description of the effect on USB redirection.

1 Include most devices within mouse device family:

```
viewusb.IncludeFamily = "mouse"
viewusb.ExcludeVidPid = "Vid-0461_Pid-0010;Vid-0461_Pid-4d20"
```

The first property in this example tells View Client to allow mouse devices to be redirected to a View desktop. The second property overrides the first and tells View Client to keep two specific mouse devices local and not redirect them.

2 Turn on automatic device splitting, but exclude one particular device from splitting. For another particular device, keep one of its components local and redirect the other components to the remote desktop:

```
viewusb.AllowAutoDeviceSplitting = "True"
viewusb.SplitExcludeVidPid = "Vid-03f0_Pid-2a12"
viewusb.SplitVidPid = "Vid-0911_Pid-149a(exintf:03)"
viewusb.IncludeVidPid = "Vid-0911_Pid-149a"
```

Composite USB devices consist of a combination of two or more devices, such as a video input device and a storage device. The first property in this example turns on automatic splitting of composite devices. The second property excludes the specified composite USB device (`Vid-03f0_Pid-2a12`) from splitting.

The third line tells View Client to treat the components of a different composite device (`Vid-0911_Pid-149a`) as separate devices but to exclude the following component from being redirected: the component whose interface number is 03. This component is kept local.

Because this composite device includes a component that is ordinarily excluded by default, such as a mouse or keyboard, the fourth line is necessary so that the other components of the composite device `Vid-0911_Pid-149a` can be redirected to the View desktop.

The first three properties are splitting properties. The last property is a filtering property. Filtering properties are processed before splitting properties.

IMPORTANT These client configuration properties might be merged with or overridden by corresponding policies set for View Agent on the remote desktop. For information about how USB splitting and filtering properties on the client work in conjunction with View Agent USB policies, see the topics about using policies to control USB redirection, in the *VMware Horizon View Administration* document.

USB Device Families

You can specify a family when you are creating USB filtering rules for Horizon View Client or View Agent.

Table 6-2. USB Device Families

Device Family Name	Description
`audio`	Any audio-input or audio-output device.
`audio-in`	Audio-input devices such as microphones.
`audio-out`	Audio-output devices such as loudspeakers and headphones.
`bluetooth`	Bluetooth-connected devices.
`comm`	Communications devices such as modems and wired networking adapters.
`hid`	Human interface devices excluding keyboards and pointing devices.
`hid-bootable`	Human interface devices that are available at boot time excluding keyboards and pointing devices.
`imaging`	Imaging devices such as scanners.
`keyboard`	Keyboard device.
`mouse`	Pointing device such as a mouse.
`other`	Family not specified.
`pda`	Personal digital assistants.
`physical`	Force feedback devices such as force feedback joysticks.
`printer`	Printing devices.
`security`	Security devices such as fingerprint readers.
`smart-card`	Smart-card devices.
`storage`	Mass storage devices such as flash drives and external hard disk drives.
`unknown`	Family not known.
`vendor`	Devices with vendor-specific functions.
`video`	Video-input devices.

Table 6-2. USB Device Families (Continued)

Device Family Name	Description
`wireless`	Wireless networking adapters.
`wusb`	Wireless USB devices.

NOTE In releases before View 5.1, View Client for Windows read the device family from the device driver that you installed on the client computer. In View 5.1, you do not need to install the device driver on a Windows client computer. View Client reads the device family from the device itself, and not from the device driver. The firmware on a USB device usually defines the family of the device that describes its intended functionality, although not all devices specify the correct value for the family.

Linux-based thin clients have always read the device family from the device itself.

Using the View Client 1.5 Command-Line Option to Redirect USB Devices

You can use the `--usb=` command-line option of the `vmware-view` command to configure which USB devices can be redirected to a View desktop. Note that the USB command-line option is available only with the version of View Client for Linux provided by third-party vendors and only for View Client 1.5.

IMPORTANT If you have View Client 1.6 or later, you must use a configuration file, rather than the `--usb=` command-line option, to configure USB redirection. See Chapter 6, "Configuring USB Redirection on the Client," on page 51.

The arguments to `--usb=` option are sent to the USB redirection command `vmware-view-usb`.

The following example turns on trace-level logging:

```
vmware-view --usb=log:trace
```

You can specify multiple instances of the `--usb` option for each `vmware-view-usb` option that you want to set. The following example turns on debug-level logging and excludes a device that is specified by its ID:

```
 vmware-view --usb=log:debug
--usb=exid:vid0012pid0034
```

The following table lists the arguments you can use with the `--usb` option .

Table 6-3. USB Redirection Options

Option	Description
`disable-boot-fwd`	Disables detection and filtering of the boot device by the View USB client. Specifying this option results in all USB devices being forwarded, including the one from which the client system booted.

`ex:`*device1*`[,`*device2*`]...`	Excludes a list of named devices from being forwarded. For example:
	`vmware-view`
	`--usb=ex:"flash 1"`

`exfa:`*device-family1*`[,`*device-family2*`]...`	Excludes a list of named device families from being forwarded. For example:
	`vmware-view`
	`--usb=exfa:storage`

`exid:`*device-ID1*`[,`*device-ID2*`]...`	Excludes a list of devices from being forwarded, where the devices are specified by the hexadecimal values of their vendor and product IDs using the format `vid`*xxxx*`pid`*xxxx* . For example:
	`vmware-view`
	`--usb=exid:vid1e2fpid5a1e`

Table 6-3. USB Redirection Options (Continued)

Option	Description
`expt:`*device-path1*`[,`*device-path2*`]...`	Excludes a list of devices from being forwarded where the devices are specified by the decimal values of their bus and port values using the format `bus`*n*`port`*n*. For example: `vmware-view --usb=expt:bus1port4,bus5port3`

`in:`*device1*`[,`*device2*`]...`	Includes a list of named devices to be forwarded. For example:
	`vmware-view`
	`--usb=in:"flash 1"`

`infa:`*device-family1*`[,`*device-family2*`]...`	Includes a list of named device families to be forwarded. For example:
	`vmware-view`
	`--usb=infa:storage`

`inid:`*device-ID1*`[,`*device-ID2*`]...`	Includes a list of devices to be forwarded, where the devices are specified by the hexadecimal values of their vendor and product IDs using the format `vid`*xxxx*`pid`*xxxx* . For example:
	`vmware-view`
	`--usb=inid:vid27f8pid2a1b`

`inpt:`*device-path1*`[,`*device-path2*`]...`	Includes a list of devices to be forwarded, where the devices are specified by the decimal values of their bus and port values using the format `bus`*n*`port`*n*. For example:
	`vmware-view`
	`--usb=inpt:bus3port1,bus4port2`

`log:{debug|error|info|trace}`	Specifies the logging level for `vmware-view-usb:trace`, `debug`, `info` (default), or `error` , in order of decreasing detail. The log file (`backendLog.txt`) is written to `/tmp/vmware-`*username*`/vmware-view-usb-`*pid*`.log`. For example:
	`vmware-view`
	`--usb=log:error`

The order of precedence for including or excluding devices is as follows, from highest to lowest precedence:

1 `expt` (excludes devices identified by bus and port)

2 `inpt` (includes devices identified by bus and port)

3 `ex` (excludes a list of named devices)

4 `in` (includes a list of named devices)

5 `exid` (excludes devices identified by vendor and product ID)

6 `inid` (includes devices identified by vendor and product ID)

7 `exfa` (excludes a list of named device families)

8 `infa` (includes a list of named device families)

The following example excludes all storage family devices apart from one device that is specified by its ID:

```
vmware-view --usb=exfa:storage
--usb=inid:vid1812pid1492
```

Following is a list of the USB device family classes you can use with the `infa` and `exfa` options.

`audio`	`printer`
`bluetooth`	`security`
`comm`	`smart-card`
`hid`	`storage`
`hid-bootable`	`unknown`

hub	vendor
imaging	video
other	wireless
pda	wusb
physical	

Index

V

W

X