Using VMware Horizon Client for Linux

VMware Horizon Client for Linux 4.0
VMware Horizon Client for Linux 3.5
VMware Horizon Client for Linux 3.4
VMware Horizon Client for Linux 3.2
VMware Horizon Client for Linux 3.1

vmware®

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

https://docs.vmware.com/

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 Client for Linux

This guide, *Using VMware Horizon Client for Linux*, provides information about installing and using VMware Horizon™ Client™ 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 Client for Linux.

This information is intended for administrators who need to set up a 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 mostly to the Horizon Client for Linux that VMware makes available. In addition, several VMware partners offer thin and zero client devices for View deployments. The features that are available for each thin or zero client device, and the operating systems supported, are determined by the vendor, the model, and the configuration that an enterprise chooses to use. For information about the vendors and models for these 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 Horizon Client is like installing most other applications.

- System Requirements for Linux Client Systems on page 8

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

- System Requirements for Real-Time Audio-Video on page 11

  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 View deployment must meet certain software and hardware requirements.

- Requirements for Using Flash URL Redirection on page 12

  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.

- Smart Card Authentication Requirements on page 13

  Client systems that use a smart card for user authentication must meet certain requirements.

- Supported Desktop Operating Systems on page 14

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

- Preparing Connection Server for Horizon Client on page 14

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

- Install or Upgrade Horizon Client for Linux from VMware Product Downloads on page 14

  With Horizon Client 3.2 and later, you can download and run a Horizon Client installer bundle from the VMware Downloads page. This installer contains modules for features such as USB redirection, virtual printing, Real-Time Audio-Video, smart card, and client drive redirection.

- Install Horizon Client for Linux from the Ubuntu Software Center on page 20

  If you have a Ubuntu system, you can install the client from the Ubuntu Software Center as an alternative to installing the version provided on the VMware Downloads Web site. If you use the Ubuntu Software Center, you install the client by using the Synaptic Package Manager.

- Configure VMware Blast Options on page 21

  In Horizon Client 4.0 and later, you can configure decoding and network protocol options for remote desktop and application sessions that use the VMware Blast display protocol.

- Horizon Client Data Collected by VMware on page 22

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

System Requirements for Linux Client Systems

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

Note These system requirements pertain to the Horizon Client for Linux that VMware makes available. In addition, several VMware partners offer thin and zero client devices for View deployments. The features that are available for each thin or zero 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 these client devices, see the VMware Compatibility Guide, available on the VMware Web site.

Note

- Starting with version 7.0, View Agent is renamed Horizon Agent.
- VMware Blast, the display protocol that is available starting with Horizon Client 4.0 and Horizon Agent 7.0, is also known as VMware Blast Extreme.

Architecture Intel-based, ARM

Memory At least 2GB of RAM

Operating systems

- Horizon Client 4.0 supports the following operating systems.

Operating System	Version
Ubuntu	12.04, 14.04
Ubuntu x64	12.04, 14.04
Red Hat Enterprise Linux (RHEL)	6.7, 7.2
SUSE Linux Enterprise Desktop (SLED)	11 SP4
CentOS	6.7

- Horizon Client 3.5 supports the following operating systems.

Operating System	Version
Ubuntu	12.04, 14.04
Ubuntu x64	12.04
Red Hat Enterprise Linux (RHEL)	6.6, 6.7
SUSE Linux Enterprise Desktop (SLED)	11 SP3
CentOS	6.6

Important Ubuntu 12.04 is the only 64-bit Linux distribution that is supported.

- Horizon Client 3.4 supports the following operating systems.

Operating System	Version
Ubuntu	12.04, 14.04
Red Hat Enterprise Linux (RHEL)	6.6
SUSE Linux Enterprise Desktop (SLED)	11 SP3
CentOS	6.6

Important Only 32-bit systems are supported.

- Horizon Client 3.2 supports the following operating systems.

Operating System	Version
Ubuntu	12.04, 14.04
Red Hat Enterprise Linux (RHEL)	6.5
SUSE Linux Enterprise Desktop (SLED)	11 SP3
CentOS	6.5

Important Only 32-bit systems are supported.

- Horizon Client 3.1 supports the following operating systems.

Operating System	Version
Ubuntu	12.04, 14.04

Important Only 32-bit systems are supported.

OpenSSL requirement

Horizon Client requires a specific version of OpenSSL. If you have Horizon Client 3.4 or later, the correct version is automatically downloaded and installed. If you have Horizon Client 3.2 or earlier, if you do not install the correct version of OpenSSL, the client might not start, might exit unexpectedly, or might not be able to connect to the server. The client might also be vulnerable to security bugs that exist in the older versions of libraries that are in use.

Table 1-1. Open SSL Requirements for Specific Versions of Horizon Client

Client Version	Requirement
Horizon Client 4.0	OpenSSL 1.0.2f or later. For your convenience, it you do not have the correct version of OpenSSL, the Horizon Client installer will download and install the required version of OpenSSL
Horizon Client 3.4 and 3.5	OpenSSL 1.0.1m or later. For your convenience, it you do not have the correct version of OpenSSL, the Horizon Client installer will download and install the required version of OpenSSL

Table 1-1. Open SSL Requirements for Specific Versions of Horizon Client (Continued)

Client Version	Requirement
Horizon Client 3.2	OpenSSL 1.0.1i or later. **Important** If you download the source code for OpenSSL 1.0.1i from the OpenSSL Web site or some other site, compile, and install it, you might get libraries with the extension 1.0.0 or 1.0.1i, but Horizon Client looks for libraries with the extension 1.0.1. Specifically, the client looks for files named `libssl.so.1.0.1` and `libcrypto.so.1.0.1` in system's library path. To work around this issue, you can create a symbolic link by linking `libssl.so.1.0.1` to `libssl.so.1.0.1i` or `libssl.so.1.0.0`, as appropriate, and linking `libcrypto.so.1.0.1` to `libcrypto.so.1.0.1i` or `libcrypto.so.1.0.0`.
Horizon Client 3.1	OpenSSL 1.0.1h

View Connection Server, Security Server, and View Agent

Latest maintenance release of View 5.3.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.

Remote (hosted) applications are available only on Horizon 6.0 (or later) View servers.

Display protocol

- VMware Blast (requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later)
- PCoIP
- RDP

Screen resolution on client system

Minimum: 1024 X 768 pixels

Hardware Requirements for VMware Blast and PCoIP

- x86- or x64-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- or x64-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.

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 42.

Other Software Requirements

Horizon Client also has certain other software requirements, depending on the Linux distribution you use. Be sure to allow the Horizon Client installation wizard to scan your system for library compatibilities and dependencies. The following list of requirements pertains only to Ubuntu distributions.

- To support idle session timeouts: `libXsso.so.1`.
- To support Flash URL redirection: `libexpat.so.1`. (The `libexpat.so.0` file is no longer required.)
- To support USB redirection and Real-Time Audio-Video: `libudev0`.

  NOTE By default, `libudev0` is not installed in Ubuntu 14.04.

- To improve performance when using multiple monitors, enable Xinerama.

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 View deployment must meet certain software and hardware requirements.

This feature is supported on the following versions of Horizon Client for Linux:

- Horizon Client 3.2 or a later release that is available from VMware.
- Horizon Client 2.2 or a later release that is available from third-party vendors.

View remote desktop

The desktops must have View Agent 5.3 or later, or Horizon Agent 7.0 or later, installed. For View Agent 5.3 desktops, 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 View 5.3 Feature Pack 1. See the *View Feature Pack Installation and Administration* document for View. If you have View Agent 6.0 or later, or Horizon Agent 7.0 or later, no feature pack is required. Real-Time Audio-Video is not supported in remote applications.

Horizon Client computer or client access device

- In Horizon Client 3.4 and earlier, Real-Time Audio-Video is supported on x86 devices only. In Horizon Client 3.5 and later, it is supported on x86 and x64 devices. This feature is not supported on ARM processors. The client system processor must have at least two cores.
- Horizon Client requires the following libraries:
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

The plug-in file (`/usr/lib/pcoip/vchan_plugins/libmmredir_plugin.so` in Horizon Client 3.5 and earlier, `/usr/lib/pcoip/vchan_plugins/libviewMMDevRedir.so` in Horizon Client 4.0) has the following dependencies.:

```
libuuid.so.1
libv4l2.so.0
libspeex.so.1
libudev0
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 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 the agent is installed.

Display protocol for View

- PCoIP
- VMware Blast (requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later)

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

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. Both multicast and unicast are supported.

This feature is available when used in conjunction with the correct version of the agent software. For View 5.3, this feature is included in the Remote Experience Agent, which is part of the View Feature Pack. For View 6.0 and later releases, this feature is included in View Agent or Horizon Agent.

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

- This feature is supported on the version of Horizon Client provided by partners or provided on the VMware download page, on x86 devices in Horizon Client 3.4 and earlier, on x86 and x64 devices in Horizon Client 3.5 and later, and for PCoIP only. 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.1` 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 remote 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 View documentation.

Smart Card Authentication Requirements

Client systems that use a smart card for user authentication must meet certain requirements.

Each client system that uses a smart card for user authentication must have the following software and hardware:

- Horizon Client
- A compatible smart card reader
- Product-specific application drivers

You must also install product-specific application drivers on the remote desktops or Microsoft RDS host.

Users that authenticate with smart cards must have a smart card, and each smart card must contain a user certificate.

In addition to meeting these requirements for Horizon Client systems, other View components must meet certain configuration requirements to support smart cards:

- For information about configuring Connection Server to support smart card use, see the topic "Configure Smart Card Authentication," in the *View Administration* document.

  All applicable CA (certificate authority) certificates for all trusted user certificates must be added to a server truststore file on the Connection Server host or security server host. These certificates include root certificates and must include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.
- For information about tasks you might need to perform in Active Directory to implement smart card authentication, see the topics about preparing Active Directory for smart card authentication, in the *View Installation* document.

Configure Horizon Client for Smart Card

In Horizon Client 3.5, to set up smart card authentication you must perform some configuration steps.

Prerequisites

Horizon Client is installed.

Procedure

1 Create the folder `/usr/lib/vmware/view/pkcs11`.

2 Create a symbol link to the pkcs11 library which is used for smart card authentication.

  For example, run the following command:

```
sudo ln –s /usr/lib/pkcs11/libgtop11dotnet.so
               /usr/lib/vmware/view/pkcs11
```

Supported Desktop Operating Systems

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

For a list of the supported Windows guest operating systems, see the "Supported Operating Systems for View Agent" topic in the View 5.x or 6.x installation documentation. See the "Supported Operating Systems for Horizon Agent" topic in the Horizon 7 installation documentation.

Some Linux guest operating systems are also supported if you have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, and Horizon Client 3.4 or later. For information about system requirements, configuring Linux virtual machines for use in Horizon 6 or Horizon 7, and a list of supported features, see *Setting Up Horizon 6 for Linux Desktops*, which is part of the Horizon 6, version 6.1 documentation, or see *Setting Up Horizon 7 for Linux Desktops*.

Preparing Connection Server for Horizon Client

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

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

- If you plan to use Access Point, which is available with Horizon 6 version 6.2 or later, configure Connection Server to work with Access Point. See *Deploying and Configuring Access Point*. Access Point appliances fulfill the same role that was previously played by only security servers.
- If you are using a security server, verify that you are using the latest maintenance releases of Connection Server 5.3.x and Security Server 5.3.x or later releases. See the *View Installation* document.
- 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 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 or application pool has been created and that the user account that you plan to use is entitled to access the pool. For Connection Server 5.3.x, see the topics about creating desktop pools in the *View Administration* document. For Connection Server 6.0 and later, see the topics about creating desktop and application pools in the *Setting Up Desktop and Application Pools in View* document.
- To use two-factor authentication with Horizon Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in the *View Administration* document.

Install or Upgrade Horizon Client for Linux from VMware Product Downloads

With Horizon Client 3.2 and later, you can download and run a Horizon Client installer bundle from the VMware Downloads page. This installer contains modules for features such as USB redirection, virtual printing, Real-Time Audio-Video, smart card, and client drive redirection.

Note On most Linux distributions, the Horizon Client installer bundle launches a GUI wizard. On SUSE Linux distributions, the bundle installer launches a command-line wizard. You can also run the installer with the `--console` option to launch the command-line wizard.

During the installation process, you are prompted to confirm whether to install various components. The default is to install all components except for Horizon Client 3.5, which does not, by default, install client drive redirection, a Tech Preview feature. The following table provides a brief summary of each optional component.

Table 1-2. Horizon Client for Linux Installation Options

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. USB redirection is supported on remote desktops that are deployed on single-user machines but is not supported on RDS host-based remote desktops. The component files are installed in `/usr/lib/vmware/view/usb/`. If you have Horizon Client 3.2, to enable the USB redirection feature, as a user with root access, run `vmware-usbarbitrator` and `vmware-view-usbd` under `/usr/lib/vmware/view/usb/` whenever you start or reboot your Linux system. If you have Horizon Client 3.4 or later, these services are started automatically if you allow the installer to register and start installed services after the installation. **Note** You can use group policy settings to disable USB redirection for specific users.
Real-Time Audio-Video	Redirects webcam and audio devices that are connected to the client system so that they can be used on the remote desktop. The component file is installed in `/usr/lib/pcoip/vchan_plugins/`.
Virtual Printing	Lets users print to any printer available on their client computers. Users do not have to install additional drivers on their remote desktops. The component files are installed in `/usr/lib/vmware/view/virtualPrinting/`. After you install the client, if you have Horizon Client 3.2, you must configure this feature to enable it, as described in "Enable the Virtual Printing Feature on a Linux Client," on page 19. If you have Horizon Client 3.4 or later, you do not need to manually configure this feature if you allow the installer to register and start installed services after the installation. In Horizon 6.0.2 and later, virtual printing is supported on the following remote desktops and applications: ■ Desktops that are deployed on single-user machines ■ Desktops that are deployed on RDS hosts, where the RDS hosts are virtual machines ■ Hosted (remote) applications, which are provided by RDS hosts ■ Remote applications that are launched from Horizon Client inside remote desktops
Smart Card	Lets users authenticate with smart cards when they use the VMware Blast or PCoIP display protocol. Although this option is selected in the client installer by default, this option is not selected by default when you run the View Agent installer in the remote desktop. Smart card is supported on remote desktops that are deployed on single-user machines. For smart card support on session-based desktops on RDS hosts, you must have .Horizon Client 3.4 or later and View Agent 6.1.1 or later. The component files are installed in `/usr/lib/pcoip/vchan_plugins/`.
Client Drive Redirection	Lets users share folders and drives on the client computer with remote desktops and applications. Drives can include mounted drives and USB storage devices. This is a Tech Preview feature in Horizon Client 3.5 and a fully supported feature in Horizon Client 4.0 and later. This feature is not selected by default when you install Horizon Client 3.5, but is selected by default when you install Horizon Client 4.0 or later. The component files are installed in `/usr/lib/vmware/view/vdpService/`.

Prerequisites

- Verify that the client system runs a supported operating system. See "System Requirements for Linux Client Systems," on page 8.
- For Horizon Client 3.2 and earlier, verify that OpenSSL 1.0.1i or later is installed on the client system. For Horizon Client 3.4 and later, if the correct OpenSSL library is not installed, the installer downloads and installs it for you. See the release notes for the OpenSSL library version.
- Verify that you have root access on the host system.
- Verify that VMware Workstation is not installed 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 for Linux Client Systems," on page 8.
- If you have an earlier version of the Horizon Client software installed on the Linux client system, uninstall that application before installing Horizon Client 3.2 or later. See "Uninstall Horizon Client for Linux," on page 70.
- If you plan to use the command-line installer, familiarize yourself with the Linux command-line installation options. See "Command-Line Installation Options for the Linux Client," on page 17.

As part of the installation process, the installer runs a scan of the system libraries to determine whether the system is compatible with Horizon Client, although you can select to skip the scan.

Procedure

1 On the Linux client system, download the Horizon Client installer file from the Horizon Client Product Downloads page at http://www.vmware.com/go/viewclients.

The name of the file is `VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`, where *x.x.x* is the version number, *yyyyyyy* is the build number, and *arch* is either `x86` or `x64`. `x64` is available in Horizon Client 3.5 and later.

2 Open a Terminal window, change directories to the directory that contains the installer file, and run the installer, using the appropriate command.

Option	Command
For the GUI wizard, if you have set executable permissions	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
For the GUI wizard, if you have not set executable permissions	`sudo sh ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
For the command-line installer	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console`

The installer wizard appears, prompting you to accept the end user license agreement.

3 Follow the prompts to finish the installation.

Important If you are installing Horizon Client 3.4 or later, you are prompted to allow the installer to register and start installed services after the installation. Allowing the installer to complete these tasks means that you will not need to manually start USB redirection services every time you reboot, and you will not need to manually enable the virtual printing feature.

4 After installation is complete, specify whether to perform the compatibility scan for libraries that various feature components are dependent on.

The system scan displays a result value for each library compatibility.

Result Value	Description
Success	All needed libraries were found.
Failed	The specified library was not found. **Important** With Horizon Client 3.4, the scan reports failure if the OpenSSL library is not installed (`libssl.so.1.0.1` and `libcrypto.so.1.0.1` files), but you can safely ignore this failure because the installer will automatically download and install the correct library. This scan failure does not occur with Horizon Client 3.5 or later.

Log information about the installation is recorded in `/tmp/vmware-root/vmware-installer-pid.log`.

What to do next

If you have Horizon Client 3.2, to use the USB redirection feature, run `vmware-usbarbitrator` and `vmware-view-usbd` under `/usr/lib/vmware/view/usb/`. If you have Horizon Client 3.4 or later, performing this procedure is not necessary if you specify that the installer should register and start installed services after the installation.

If you have Horizon Client 3.2, to use the virtual printing feature, perform the procedure described in "Enable the Virtual Printing Feature on a Linux Client," on page 19. If you have Horizon Client 3.4 or later, performing this procedure is not necessary if you specify that the installer should register and start installed services after the installation. When the user launches the client, a configuration file is automatically created and placed in the user's `home` directory.

Start Horizon Client and verify that you can log in to the correct virtual desktop. See "Connect to a Remote Desktop or Application," on page 47.

Command-Line Installation Options for the Linux Client

You can use command-line installation options to install Horizon Client on a Linux system.

Install Horizon Client silently by using the `--console` option along with other command-line options and environment variable settings. With silent installation, you can efficiently deploy View components in a large enterprise.

The following table lists the options you can use when you run the `VMware-Horizon-Client-`*`x.x.x-yyyyyyy.arch`*`.bundle` installer file.

Table 1-3. Linux Command-Line Installation Options

Option	Description
`--help`	Displays usage information.
`--console`	Enables you to use the command-line installer in a Terminal window.
`--custom`	Shows all installation questions, even if default answers have been scripted, such as, for example, by using the `--set-setting` options. The default is `--regular`, which means show only questions that do not have a default answer.
`--eulas-agreed`	Agrees to the end user license agreement.
`--gtk`	Opens the GUI-based VMware installer, which is the default option. If the GUI cannot be displayed or loaded for any reason, console mode is used.
`--ignore-errors` or `-I`	Allows the installation to continue even if there is an error in one of the installer scripts. Because the section that has an error does not complete, the component might not be properly configured.
`--regular`	Shows installation questions that have not been answered before or are required. This is the default option.
`--required`	Shows the license agreement prompt only and then proceeds to install the client. The default is `--regular`, which means show only questions that do not have a default answer.
`--set-setting vmware-horizon-smartcard smartcardEnable yes`	Installs the smart card component.
`--set-setting vmware-horizon-rtav rtavEnable yes`	Installs the Real-Time Audio-Video component.
`--set-setting vmware-horizon-usb usbEnable yes`	Installs the USB redirection feature.
`--set-setting vmware-horizon-virtual-printing tpEnable yes`	Installs the virtual printing feature.

Table 1-3. Linux Command-Line Installation Options (Continued)

Option	Description
`--set-setting vmware-horizon-tsdr tsdrEnable yes`	Installs the client drive redirection feature.
`--stop-services`	(For Horizon Client 3.4 and later) Do not register and start installed services.

In addition to the options listed in the table, you can set the following environment variables.

Table 1-4. Linux Environment Variable Installation Settings

Variable	Description
`TERM=dumb`	Displays a very basic text UI.
`VMWARE_EULAS_AGREED=yes`	Allows you to silently accept the product EULAs.
`VMWARE_KEEP_CONFIG=yes`	For Horizon Client 3.2 and earlier, retains the configuration if you uninstall the client software.
`VMIS_LOG_LEVEL=`*value*	Use one of the following values for *value*: ■ `NOTSET` ■ `DEBUG` ■ `INFO` ■ `WARNING` ■ `ERROR` ■ `CRITICAL` Log information is recorded in `/tmp/vmware-root/vmware-installer-`*pid*`.log`.

Example: Silent Installation Commands

Following is an example of how to install Horizon Client silently, and, for each component, the example specifies whether to install that component.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \

./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console \

--set-setting vmware-horizon-usb usbEnable no \

--set-setting vmware-horizon-virtual-printing tpEnable yes \

--set-setting vmware-horizon-smartcard smartcardEnable no\

--set-setting vmware-horizon-rtav rtavEnable yes \

--set-setting vmware-horizon-tsdr tsdrEnable yes
```

This next example shows how to perform a silent installation of Horizon Client using the default settings.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \
./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console --required
```

Enable the Virtual Printing Feature on a Linux Client

The installer bundle for Horizon Client 3.2 and later includes a virtual printing component. If you have Horizon Client 3.2, you must create a configuration file and set some environment variables to enable the 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.

Important Performing this procedure is usually not necessary if you have Horizon Client 3.4 or later because you can specify during client installation that the installer should register and start installed services after installation. When the user launches the client, a configuration file is automatically created and placed in the user's `home` directory

Prerequisites

You must use the installer bundle provided by VMware to install Horizon Client 3.2 or later. The virtual printing component is then installed by default.

Procedure

1 Open a Terminal window and enter a command to create a folder named `.thnuclnt` in the `home` directory.

```
$ mkdir ~/.thnuclnt/
```

Note Because this file is created in a specific user's home directory, the file needs to be created for each user who will be using the Linux client system.

2 Use a text editor to create a configuration file called `thnuclnt.conf` in the `~/.thnuclnt` folder, and add the following text to the file:

```
autoupdate = 15
automap = true
autoid = 0
updatecount = 1
editcount = 0

connector svc {
   protocol = listen
   interface = /home/user/.thnuclnt/svc
   setdefault = true
}
```

In this text, substitute the user name for *user*.

3 Save and close the file.

4 Enter a command to start the `thnuclnt` process.

```
$ thnuclnt –fg
```

5 Enter the commands to set the environment variables for the virtual printing components.

```
$ export TPCLIENTADDR=/home/user/.thnuclnt/svc
$ export THNURDPIMG=/usr/bin/thnurdp
```

6 To launch Horizon Client, start the `vmware–view` process.

The printers that normally appear in the client are now also redirected so that they appear in the Print dialog boxes in your remote desktop.

7 (Optional) If you ever want to disable the virtual printing feature, use the following steps:

a Enter a command to stop the `thnuclnt` process.

```
$ killall thnuclnt
```

b Disconnect from the remote desktop and reconnect to the desktop.

The printers will no longer be redirected.

Install Horizon Client for Linux from the Ubuntu Software Center

If you have a Ubuntu system, you can install the client from the Ubuntu Software Center as an alternative to installing the version provided on the VMware Downloads Web site. If you use the Ubuntu Software Center, you install the client by using the Synaptic Package Manager.

This topic provides instructions for obtaining the client software from the Ubuntu software Center. With Horizon Client 3.2 and later, you can also obtain the Horizon Client software from the VMware Product Downloads Web site, as described in "Install or Upgrade Horizon Client for Linux from VMware Product Downloads," on page 14.

Important Customers using Linux-based thin clients must contact their thin client vendor for Horizon 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 for Linux Client Systems," on page 8.
- Verify that you have the correct version of OpenSSL installed. See "System Requirements for Linux Client Systems," 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 for Linux Client Systems," on page 8.
- If you have a View Client 1.x or 2.x installed on the Linux client system, uninstall that application before installing Horizon Client 3.1 or later. See "Uninstall Horizon Client for Linux," on page 70.

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 If you have Ubuntu 12.04 or 14.04, download and install the package from the Ubuntu software Center, as follows.

a Open a Terminal window and enter the command to get new packages:

```
sudo apt-get update
```

New packages are downloaded, and you see a list of the packages in the Terminal window.

b Open the Update Manager, check for updates, and install updates.

c Open the Ubuntu Software Center app, and search on **vmware-view-client**.

d Install the vmware-view-client app.

If your operating system is Ubuntu 12.04 or 14.04, the latest version of Horizon Client is installed.

An application icon for **VMware Horizon Client** appears in the Application Launcher.

3 If you have Ubuntu 10.04, download and install 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 10.04, View Client for Linux 1.7 is installed.

e 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 Client and verify that you can log in to the correct virtual desktop. See "Connect to a Remote Desktop or Application," on page 47.

Configure VMware Blast Options

In Horizon Client 4.0 and later, you can configure decoding and network protocol options for remote desktop and application sessions that use the VMware Blast display protocol.

H.264 decoding has the following restrictions:

- Multiple monitors are not supported.
- The maximum resolution that is supported depends on the capability of the graphical processing unit (GPU) on the client. A GPU that can support 4K resolution for JPEG/PNG might not be able to support 4K resolution for H.264. If a resolution for H.264 is not supported, Horizon Client uses JPEG/PNG instead.

H.264 decoding is supported on AMD and Nvidia GPUs only. Also, H.264 decoding requires that the graphics library OpenGL 3.2 or later is installed.

Prerequisites

Verify that you have Horizon Client 4.0 or later. VMware Blast is not supported in earlier Horizon Client versions. This feature also requires Horizon Agent 7.0 or later.

Procedure

1 In the desktop and application selector window, select **Connection > Settings** or click the Settings icon in the upper-right portion of the window, and select **VMware Blast** in the left pane of the Settings window.

2 Configure the decoding and network protocol options.

Option	Description
H.264	Select this option to allow H.264 decoding in Horizon Client. When this option is selected (the default setting), Horizon Client uses H.264 decoding if the agent supports H.264 software encoding. If the agent does not support H.264 software encoding, Horizon Client uses JPG/PNG decoding. Deselect this option to always use JPG/PNG decoding.
UDP	Select this option to allow UDP networking in Horizon Client. When this option is selected (the default setting), Horizon Client uses UDP networking if UDP connectivity is available. If UDP networking is blocked, Horizon Client uses TCP networking. Deselect this option to always use TCP networking. **Note** UDP is disabled by default on a Horizon remote desktop. For UDP to work, it must be enabled on the desktop, the client, and the Blast Secure Gateway (BSG).

Your changes take effect the next time a user connects to a remote desktop or application and selects the VMware Blast display protocol. Your changes do not affect existing VMware Blast sessions.

Horizon Client Data Collected by VMware

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

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 Client information is sent first to Connection Server and then on to VMware, along with data from Connection Server instances, desktop pools, and remote desktops.

Although the information is encrypted while in transit to 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.

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

Table 1-5. Data Collected from Horizon Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous ?	Example Value
Company that produced the Horizon Client application	No	VMware
Product name	No	VMware Horizon 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

Table 1-5. Data Collected from Horizon Clients for the Customer Experience Improvement Program (Continued)

Description	Is This Field Made Anonymous ?	Example Value
Client build name	No	Examples include the following: ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-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 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
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
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)
Number of USB devices connected	No	2 (USB device redirection is supported only for Linux, Windows, and Mac OS X clients.)
Maximum concurrent USB device connections	No	2

Table 1-5. Data Collected from Horizon Clients for the Customer Experience Improvement Program (Continued)

Description	Is This Field Made Anonymous ?	Example Value
USB device vendor ID	No	Examples include the following: ■ Kingston ■ NEC ■ Nokia ■ Wacom
USB device product ID	No	Examples include the following: ■ DataTraveler ■ Gamepad ■ Storage Drive ■ Wireless Mouse
USB device family	No	Examples include the following: ■ Security ■ Human Interface Device ■ Imaging
USB device usage count	No	(Number of times the device was shared)

Configuring Horizon Client for End Users

2

Horizon 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 only some of the configuration settings that you can set in one or more ways.

Table 2-1. Common Configuration Settings

Setting	Mechanisms for Configuring
View Connection Server address	URI, Configuration File Property, Command Line
Active Directory user name	URI, Configuration File Property, Command Line
Domain name	URI, Configuration File Property, Command Line
Desktop display name	URI, Configuration File Property, Command Line
Window size	URI, Configuration File Property, Command Line
Display protocol	URI, Configuration File Property, Command Line
Configuring certificate checking	Configuration File Property
Configuring SSL protocols and cryptographic algorithms	Configuration File Property, Command Line

This chapter includes the following topics:

Using URIs to Configure Horizon Client

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

You can simplify the process of connecting to a remote desktop or application 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:

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

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

Note You can use URIs to launch Horizon 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 or application, and, optionally, a query to specify desktop or application actions or configuration options.

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 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. Note that underscores (_) are not supported in server names. 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 or application. Use the desktop display name or application display name. This name is the one specified in View Administrator when the desktop or application pool was created. 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 or application 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 Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the *Using VMware Horizon 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 and applications hosted on the specified server. You are not required to specify a desktop or application when using this action.
`start-session`	Launches the specified desktop or application. If no action query is provided and the desktop or application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified desktop or remote application. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC. In Horizon Client 3.0, if you specify an application, the action will be ignored. In Horizon Client 3.1, if you specify an application, the end user is prompted to confirm quitting all remote applications.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify an application, the action will be ignored or the end user will see the warning message "Invalid URI action."

appProtocol

For remote applications, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`appProtocol=PCOIP`**. This query is supported only in Horizon Client 4.0 and later releases. In earlier Horizon Client releases, remote applications always use PCoIP.

desktopLayout

Sets the size of the window that displays a 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 For remote desktops, valid values are **`RDP`**, **`PCOIP`**, and **`BLAST`**. For example, to specify PCoIP, use the syntax **`desktopProtocol=PCOIP`**. **`BLAST`** is supported only in Horizon Client 4.0 and later releases.

domainName The NETBIOS domain name associated with the user who is connecting to the remote desktop or application. For example, you would use `mycompany` rather than `mycompany.com`.

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 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 Horizon Client Command-Line Interface and Configuration Files," on page 29.

---

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 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 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://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client is launched and connects to the `view.mycompany.com` server. In the login box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the application whose display name is displayed as **Calculator**. The connection uses the VMware Blast display protocol.

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

Horizon 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.

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

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

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

Horizon 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 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.

8 `vmware-view://`

Horizon Client is launched, and the user is taken to the page for entering the address of a 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 Horizon Client Command-Line Interface and Configuration Files

You can configure Horizon 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 Horizon 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 Horizon 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 Horizon Client, any changed settings are saved in the `~/.vmware/view-preferences` file.

Properties That Prevent Users from Changing Defaults

For many properties, 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 of the server when they connect using Horizon 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 Horizon Client. You configure a proxy exception for the View Connection Server instance.

Horizon 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 are available only with the version of Horizon 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. Horizon 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 Horizon Client user interface in full screen mode on all monitors that are connected when the client is launched. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE".
`view.allowDefaultBroker`	`-l`, `--lockServer`	Using this command-line option, or setting the property to "FALSE", disables the **Server** field unless the client has never connected to any server, and no server address is provided in the command line or the preferences file. Example of using the command-line option: `--lockServer -s view.company.com`
`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.autoDisconnectEmptyAppSession`	None	When set to **"TRUE"** (the default), if the application session becomes empty because the user quits all applications, a message is displayed to the end user. This message prompts the user to choose between disconnecting the empty session or keeping the empty session running. If set to **"FALSE"**, the session is closed according to the timeout setting used in View Administrator, which by default would be to disconnect after one minute.
`view.defaultAppHeight`	None	Specifies the default height of the window for remote applications, in pixels. Use this property in conjunction with `view.defaultAppWidth` when specifying a custom desktop size (`view.defaultAppSize` property is set to "5"). Default is "480".

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

Configuration Key	Command-Line Option	Description
`view.defaultAppSize`	`--appSize=`	Sets the default size of the window for remote applications: ■ To use all monitors, specify **`"1"`**. ■ To use full screen mode on one monitor, specify **`"2"`**. ■ To use a large window, specify **`"3"`**. ■ To use a small window, specify **`"4"`**. ■ To set a custom size, specify **`"5"`**and then also set the `view.defaultAppWidth` and `view.defaultAppHeight` properties. Default is "1".
`view.defaultAppWidth`	None	Specifies the default width of the window for remote applications, in pixels. Use this property in conjunction with `view.defaultAppHeight` when specifying a custom desktop size (`view.defaultAppSize` property is set to "5"). Default is "640".

`view.defaultBroker`	`-s`, `--serverURL=`	Adds the name that you specify to the **Server** field in Horizon 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.
		Examples of using the command-line option:
		`--serverURL=https://view.company.com`
		`-s view.company.com`
		`--serverURL=view.company.com:1443`

`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. Use this property in conjunction with `view.defaultDesktopWidth` when specifying a custom desktop size (`view.defaultDesktopSize` property is set to "5").

`view.defaultDesktopSize`	`--desktopSize=`	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"`**.
		Examples of using the command-line option:
		`--desktopSize="1280x800"`
		`--desktopSize="all"`

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

Configuration Key	Command-Line Option	Description
`view.defaultDesktopWidth`	None	Specifies the default width of the window for the View desktop, in pixels. Use this property in conjunction with `view.defaultDesktopHeight` when specifying a custom desktop size (`view.defaultDesktopSize` property is set to "5").
`view.defaultDomain`	`-d, --domainName=`	Sets the domain name that Horizon Client uses for all connections and adds the domain name that you specify to the **Domain Name** field in the authentication dialog box.
`view.defaultLogLevel`	None	Sets the log level for Horizon Client logs. Set the property to one of the following values: ■ **`"0"`** means include all log events. ■ **`"1"`** means include trace-level events and events captured for settings 2 though 6. ■ **`"2"`** means include debug events and events captured for settings 3 through 6. ■ **`"3"`** (the default) means include info-level events and events captured for settings 4 through 6. ■ **`"4"`** means include warning, error, and fatal events. ■ **`"5"`** means include error and fatal events. ■ **`"6"`** means include fatal events. Default is "3".
`view.defaultPassword`	`-p "-", --password="-"`	For VMware Blast, PCoIP, and `rdesktop` connections, always specify **`"-"`** to read the password from `stdin`. Sets the password that Horizon Client uses for all connections and adds the password to the **Password** field in the 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.
`view.defaultUser`	`-u, --userName=`	Sets the user name that Horizon Client uses for all connections and adds the user name that you specify to the **User Name** field in the 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.disableMaximizedApp`	`--disableMaximizedApp`	If set to **`"FALSE"`** (the default), the application is launched in full screen mode.
`view.fullScreen`	`--fullscreen`	Hides the host operating system and opens the Horizon 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".

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

Configuration Key	Command-Line Option	Description

view.kbdLayout	-k, --kbdLayout=	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`
		Example of using the command-line option for rdesktop:
		`--kbdLayout="en-us"`
		`-k "fr"`
		Example of using the command-line option for freerdp:
		`-k "0x00010407"`

view.kioskLogin	--kioskLogin	Specifies that Horizon Client is going to authenticate using a kiosk mode account. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Default is "FALSE". For examples, see the kiosk mode example that follows this table.
view.mmrPath	-m, --mmrPath=	(Available only with distributions from third-party vendors) Specifies the path to the directory that contains the Wyse MMR (multimedia redirection) libraries. Example of using the command-line option: `--mmrPath="/usr/lib/altmmr"`
view.monitors	--monitors= *numbered list*	(Available with Horizon Client 3.2 and later) Allows you to specify which adjacent monitors to use for Horizon Client. Use --allmonitors (or view.allMonitors) to specify that you want to use full screen on all monitors, and use --monitors=*numbered list* to specify which subset of the monitors to use. Example of using the command-line option to specify the first and second monitors in a configuration where 3 monitors are set next to each other horizontally: `--allmonitors --monitors="1,2" ` `
view.nomenubar	--nomenubar	Suppresses the Horizon Client menu bar when the 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	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".
		Example of using the command-line option:
		`--nonInteractive`
		`--serverURL="https://view.company.com"`
		`--userName="user1" --password="-"`
		`--domainName="xyz"`
		`--desktopName="Windows 7"`

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

Configuration Key	Command-Line Option	Description
`view.once`	`--once`	Specifies that you do not want Horizon Client to retry connecting in the case of an error occurring. 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=`	(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. Example of using the command-line option: `--rdesktopOptions="-f -m"`
None	`-r`, `--redirect=`	(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. Example of using the command-line option: `--redirect="sound:off"`
`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 42.
None	`--save`	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.
`view.sendCtrlAltDelToLocal`	None	(Available if you use the VMware Blast or PCoIP display protocol) 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`. This option has the same priority as the setting in the `/etc/vmware/view-keycombos-config` file.
`view.sendCtrlAltDelToVM`	None	(Available if you use the VMware Blast or PCoIP display protocol) When set to **`"TRUE"`**, sends the key combination Ctrl+Alt+Del to the virtual desktop rather than opening a dialog box to prompt the user to disconnect from the View desktop. Default is "FALSE". This option has a higher priority than the setting in the `/etc/vmware/view-keycombos-config` file.

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

Configuration Key	Command-Line Option	Description
`view.sendCtrlAltInsToVM`	None	(Available if you use the VMware Blast or PCoIP display protocol) 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 *Setting Up Desktop and Application Pools in View* document. This option has a lower priority than the setting in the `/etc/vmware/view-keycombos-config` file.
`view.sslCipherString`	`--sslCipherString=`	Configures the cipher list to restrict the use of certain cryptographic algorithms before establishing an encrypted SSL connection. For a list of cipher strings, see http://www.openssl.org/docs/apps/ciphers.html . The default for Horizon Client 3.5 and later is "!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH". The default for Horizon Client 3.4 and earlier is "AES:!aNULL:@STRENGTH".
`view.sslProtocolString`	`--sslProtocolString=`	Configures the cipher list to restrict the use of certain cryptographic protocols before establishing an encrypted SSL connection. The supported protocols are SSLv3/SSLv3.0, TLSv1.0/TLSv1, TLSv1.1, and TLSv1.2. The cipher list consists of one or more protocol strings separated by colons. The strings are not case-sensitive. The default for Horizon Client 3.5 and later is "TLSv1.0:TLSv1.1:TLSv1.2". The default for Horizon Client 3.4 and earlier is "TLSv1.0:TLSv1.1".
`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 42.
None	`--enableNla`	(Applies if you are using FreeRDP for RDP connections) Enables network-level authentication (NLA). You must use this option in conjunction with the `--ignore-certificate` option. For more information, see "Using FreeRDP for RDP Connections," on page 41. 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 42. **Note** The `rdesktop` program does not support NLA.

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

Configuration Key	Command-Line Option	Description

None	`--printEnvironmentInfo`	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.
		Example of using the command-line option:
		`--printEnvironmentInfo`
		`-s view.company.com`

None	`--usb=`	(Available only with Horizon Client 3.2 or later, or with distributions from third-party vendors) Specifies which options to use for USB redirection. See Chapter 6, "Configuring USB Redirection on the Client," on page 71.
None	`--version`	Displays version information about Horizon 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 *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, Horizon 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 Horizon Client on a Linux client system and has the following characteristics:

- The user account name is based on the client's MAC address.
- Horizon Client runs in full screen mode without a Horizon 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 Horizon 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 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 Connection Server and Horizon 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 Client," on page 51.

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 "Horizon Client Configuration Settings and Command-Line Options," on page 31.

Configuring Advanced TLS/SSL Options

You can select the security protocols and cryptographic algorithms that are used to encrypt communications between Horizon Client and Horizon servers or between Horizon Client and the agent in the remote desktop.

These options are also used to encrypt the USB channel (communication between the USB service daemon and the agent).

With the default setting, cipher suites use 128- or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length.

- In Horizon Client 4.0 and later, by default, TLS v1.1 and TLS v1.2 are enabled. (TLS v1.0 is disabled. SSL v2.0 and v3.0 are removed.)

- In Horizon Client 3.5, by default, TLS v1.0, TLS v1.1, and TLS v1.2 are enabled. (SSL v2.0 and v3.0 are disabled.)
- In Horizon Client 3.3 and 3.4, by default, TLS v1.0 and TLS v1.1 are enabled. (SSL v2.0 and v3.0, and TLS v1.2 are disabled.)
- In Horizon Client 3.2 and earlier, by default, SSL v3.0 is also enabled. (SSL v2.0 and TLS v1.2 are disabled.)

Note In Horizon Client 3.1 to 3.5, the USB service daemon adds RC4 (:RC4-SHA: +RC4) to the end of the cipher control string when it connects to a remote desktop. Starting with Horizon Client 4.0, the USB service daemon no longer adds RC4 to the end of the cipher control string.

Note If TLS v1.0 and RC4 are disabled, USB redirection does not work when users are connected to Windows XP desktops. Be aware of the security risk if you choose to make this feature work by enabling TLS v1.0 and RC4.

You should change the security protocols in Horizon Client only if your View server does not support the current settings. If you configure a security protocol for Horizon Client that is not enabled on the View server to which the client connects, a TLS/SSL error occurs and the connection fails.

Important If the only protocol you enable on the client is TLS v1.1, you must verify that TLS v1.1 is also enabled on the remote desktop. Otherwise, USB devices cannot be redirected to the remote desktop.

On the client system, you can use either configuration file properties or command-line options for these settings:

- To use configuration file properties, use the `view.sslProtocolString` and `view.sslCipherString` properties.
- To use command-line configuration options, use the `--sslProtocolString` and `--sslCipherString` options.

For more information, see "Using the Horizon Client Command-Line Interface and Configuration Files," on page 29 and look up the property and option names in the table in "Horizon Client Configuration Settings and Command-Line Options," on page 31.

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

Starting with Horizon Client, if you use PCoIP, or, starting with Horizon Client 4.0, it you use VMware Blast or PCoIP, you can create a `view-keycombos-config` file to specify which individual keys and key combinations should not be forwarded to the remote desktop.

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. You can create a file located at `/etc/vmware/view-keycombos-config` and specify the key combinations and individual keys.

Place each key or key combination on a new line using the following format:

```
<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. 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

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. In addition to the key codes listed in that file, you can also use the following codes:

Table 2-5. Multimedia Keys

Key Name	Scan Code
PREVIOUS_TRACK	0x110
NEXT_TRACK	0x119
MUTE	0x120
CALCULATOR	0x121
PLAY_PAUSE	0x122
STOP	0x124
VOLUME_DOWN	0x12e
VOLUME_UP	0x130
BROWSER_HOME	0x132
BROWSER_SEARCH	0x165
BROWSER_FAVORITES	0x166
BROWSER_REFRESH	0x167
BROWSER_STOP	0x168
BROWSER_FORWARD	0x169
BROWSER_BACK	0x16A
MY_COMPUTER	0x16B
MAIL	0x16C
MEDIA_SELECT	0x16D

Table 2-6. Hangul and Hanja Keys

Key Name	Scan Code
HANGUL_EN	0x72
HANJA_EN	0x71
HANGUL_KO	0x172
HANJA_KO	0x171
HANGUL	0xF2
HANJA	0xF1

Table 2-7. System Sleep, Wake, and Power Keys

Key Name	Scan Code
SYSTEM_SLEEP	0x15F
SYSTEM_WAKE	0x163
SYSTEM_POWER	0x15e

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
```

Using FreeRDP for RDP Connections

If you plan to use RDP rather than VMware Blast or 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, Horizon Client can also run the `xfreerdp` executable if your Linux machine has the required version and patches for FreeRDP.

Important If you plan to connect to remote desktops or applications on a Microsoft RDS host, if that host is configured with the Per Device mode of licensing, you must use `xfreerdp` or else change the licensing mode to Per User mode. The reason is that Per Device licensing mode requires the RDP client to provide a client ID, and `rdesktop` does not provide that ID, whereas `xfreerdp` does.

You must have the correct version of FreeRDP installed, along with any applicable patches. For more information, see "Install and Configure FreeRDP," on page 42.

General Syntax

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 Horizon 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`

For more information about using the `vmware-view` command-line interface and configuration files, see "Using the Horizon Client Command-Line Interface and Configuration Files," on page 29.

Syntax for Network Level Authentication

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`

Also, you must add the `/cert-ignore` option so that the certificate verification process can succeed. Following is an example of the correct syntax:

`vmware-view --enableNla --rdpclient=xfreerdp --xfreerdpOptions="/p:`*`password`* `/cert-ignore /u:`*`user-name`* `/d:`*`domain-name`* `/v:`*`server`*`"`

If the password contains any special characters, escape the special characters (for example: **\$**).

Syntax Specific to Using FreeRDP with Horizon Client

Keep the following guidelines in mind:

- You must escape special characters that you might normally place in quotation marks. For example, the following command does not work because the special character $ in pa$$word is not escaped:

  (incorrect) `vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa$$word' /u:'crt\administrator'"`

  Instead, you must use:

  (correct) `vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa\$\$word' /u:'crt\administrator'"`

- If end users will use a session-in-session implementation of Horizon Client, you must use the `/rfx` option. An example of a session-in-session implementation is one in which an end user logs in to Horizon Client on a thin client, so that the Horizon Client interface is the only one the end user sees, and the end user then launches a nested version of Horizon Client in order to use a remote application provided by an RDS host. In cases like this, if you do not use the `/rfx` option, the end user will not be able to see the remote desktop and application icons in the desktop and application selector of the nested client.

Install and Configure FreeRDP

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

For Horizon Client 3.1 and later releases, you must have FreeRDP 1.1 installed.

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

Prerequisites

On your Linux client machine, download FreeRDP 1.1 from GitHub, at https://github.com/FreeRDP/FreeRDP.

Procedure

1 Patch with the file called `freerdp-1.1.0.patch`, using following patch commands:

```
cd /client-installation-directory/patches/FreeRDP-stable-1.1
patch -p1 < freerdp-1.1.0.patch
```

Here *client-installation-directory* is the path to `VMware-Horizon-View-Client-x.x.x-yyyyyy.i386`, where *x.x.x* is the version number and *yyyyyy* is the build number. For more information about the `freerdp-1.1.0.patch` file, see the `README.patches` file in the same *`client-installation-directory`*`/patches` directory.

2 Run the following command:

```
cmake -DWITH_SSE2=ON -DWITH_PULSEAUDIO=ON -DWITH_PCSC=ON -DWITH_CUPS=ON .
```

3 Run the following command:

```
make
```

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

```
sudo make install
```

5 (Optional) Verify that the virtual printing module can be loaded successfully.

a To verify that `tprdp.so` can be loaded by FreeRDP 1.1, run the following command:

```
sudo ln -s /usr/lib/vmware/rdpvcbridge/tprdp.so /usr/local/lib/i386-linux-
gnu/freerdp/tprdp-client.so
```

b To start Horizon Client with the virtual printing feature enabled, run the following command:

```
vmware-view --rdpclient=xfreerdp --xfreerdpOptions='/cert-ignore /vc:tprdp'
```

Note The virtual printing feature is available with Horizon Client 3.2 or later if you use PCoIP, or with Horizon Client 4.0 or later if you use VMware Blast or PCoIP.

Enabling FIPS Mode on Horizon Client 3.2 and Earlier

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. This mode is not supported on Horizon Client 3.4 or 3.5.

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.

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 Horizon 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.

Enabling FIPS Mode on Horizon Client 4.0

With Horizon client 4.0, you can enable FIPS (Federal Information Processing Standard) mode so that the client uses FIPS-compliant cryptographic algorithms when communicating with remote desktops.

Important If you enable FIPS mode in the client, the remote desktop must have FIPS mode enabled as well. Mixed mode, where only the client, or only the desktop, has FIPS mode enabled, is not supported.

To enable FIPS mode, make the following configuration changes:

1 Edit `/etc/vmware/config` and add the following lines:

```
usb.enableFIPSMode = "TRUE"
mks.enableFIPSMode = “TRUE”
```

2 Edit `/etc/vmware/view-mandatory-config` and add the following line:

```
View.fipsMode = ”TRUE”
```

3 Edit `/etc/teradici/pcoip_admin.conf` and add the following line:

```
pcoip.enable_fips_mode = 1
```

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.

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. 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 that is less than the amount of available memory divided by 2, the cache is set using one of the following formulas, but the minimum is still 50.

Version	Formula for Cache Size
Horizon Client 3.1 and 3.2	*customer-setting* - 10
Horizon Client 3.4 and later	*customer-setting* rounded to the nearest multiple of 10

With Horizon Client 3.0, if you specify a number larger than the maximum, the number is converted to 1024MB. With later versions, if you specify a number that is larger than the available memory divided by 2, the cache is set using one of the following formulas.

Version	Formula for Cache Size
Horizon Client 3.1 and 3.2	*available-memory* / 2 - 10
Horizon Client 3.4 and later	(*available-memory* / 2) rounded to the nearest multiple of 10

You can set this property in any of several files. When Horizon 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 Remote Desktop and Application Connections 3

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

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

- Connect to a Remote Desktop or Application on page 47

  After connecting to a View server, you can use the remote desktops and applications that you are authorized to use.

- Share Access to Local Folders and Drives on page 49

  You can configure Horizon Client to share folders and drives on your local system with remote desktops and applications. Drives can include mapped drives and USB storage devices. This feature is called client drive redirection.

- Certificate Checking Modes for Horizon Client on page 51

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

- Switch Desktops or Applications on page 53

  If you are connected to a remote desktop, you can switch to another desktop. You can also connect to remote applications while you are connected to a remote desktop.

- Log Off or Disconnect on page 53

  With some configurations, if you disconnect from a remote desktop without logging off, applications in the desktop can remain open. You can also disconnect from a server and leave remote applications running.

Connect to a Remote Desktop or Application

After connecting to a View server, you can use the remote desktops and applications that you are authorized to use.

Before you have end users access their remote desktops and applications, test that you can connect to a remote desktop or application from a client device. You must specify a server and supply credentials for your user account.

To use remote applications, you must connect to View Connection Server 6.0 or later.

Prerequisites

- Obtain the credentials you need to log in, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).
- Obtain the NETBIOS domain name for logging in. For example, you would use `mycompany` rather than `mycompany.com`.
- Perform the administrative tasks described in "Preparing Connection Server for Horizon Client," on page 14.
- 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 or application. Note that underscores (_) are not supported in server names. 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 agent group policy setting is enabled.

Procedure

1 Either open a terminal window and enter **`vmware-view`** or search the applications for **VMware Horizon Client**, and double-click the icon.

2 Double-click the **+ Add Server** button if no servers have yet been added, or click the **+ New Server** button in the menu bar, and enter the name of View Connection Server or a security server, and click **Connect**.

  Connections between Horizon Client and View Connection Server always use SSL. The default port for SSL connections is 443. If View Connection Server is not configured to use the default port, use the format shown in this example: **`view.company.com:1443`**.

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

  NOTE After a successful connection is made, an icon for this server is saved to the Horizon Client home screen. The next time you open Horizon Client to connect to this server, you can double-click the icon, or, if you use only this one server, you can right-click the icon for the server and select **Autoconnect to this Server** from the context menu.

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

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 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.

6 (Optional) To configure display settings for remote desktops, either right-click a desktop icon or select a desktop icon and click the **Settings** (gear-shaped) icon next to the server name in the upper portion of the screen.

Option	Description
Display protocol	If your administrator has allowed it, you can use the **Connect Via** list to choose between VMware Blast, PCoIP, and Microsoft RDP display protocols. VMware Blast (Blast Extreme) requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later.
Display layout	Use the **Display** list to select a window size or to use multiple monitors.

7 (Optional) To mark the remote desktop or application as a favorite, right-click the desktop or application icon and select **Mark as Favorite** from the context menu that appears.

A star icon appears in the upper-right corner of the desktop or application name. The next time you log in, you can click the **Show Favorites** button to quickly find this application or desktop.

8 Double-click a remote desktop or application to connect.

If you are connecting to a session-based remote desktop, which is hosted on a Microsoft RDS host, and if the desktop is already set to use a different display protocol, you will not be able to connect immediately. You will be prompted to either use the protocol that is currently set or have the system log you off of the remote operating system so that a connection can be made with the protocol you selected.

After you are connected, the client window appears.

If authentication to View Connection Server fails or if the client cannot connect to the remote desktop or application, perform the following tasks:

- Determine whether View Connection Server is configured not to use SSL. The client software 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. These are symptoms of additional connection problems caused by certificate problems.
- Verify that the tags set on the View Connection Server instance allow connections from this user. See the *View Administration* document.
- Verify that the user is entitled to access this desktop or application. See the *Setting Up Desktop and Application Pools in View* document.
- If you are using the RDP display protocol to connect to a remote desktop, verify that the remote operating system allows remote desktop connections.

Share Access to Local Folders and Drives

You can configure Horizon Client to share folders and drives on your local system with remote desktops and applications. Drives can include mapped drives and USB storage devices. This feature is called client drive redirection.

Client drive redirection is a Tech Preview feature in Horizon Client 3.5 . It is a fully supported feature in Horizon Client 4.0 and later.

In a Windows remote desktop, shared folders and drives appear in the **Devices and drives** section in the **This PC** folder, or in the **Other** section in the **Computer** folder. In a remote application, such as Notepad, you can browse to and open a file in a shared folder or drive. The folders and drives you select for sharing appear in the file system as network drives that use the naming format ***name* on *MACHINE-NAME***.

You do not need to be connected to a remote desktop or application to configure client drive redirection settings. The settings apply to all your remote desktops and applications. That is, you cannot configure the settings so that local client folders are shared with one remote desktop or application but not with other remote desktops or applications.

The client drive redirection feature requires that the following library files be installed. On some thin client machines, these library files might not be installed by default.

- `libsigc-2.0.so.0`
- `libglibmm-2.4.so.1`

By default, the USB redirection feature redirects USB storage to the remote desktop or application. If the USB storage can be mounted locally, you might get better performance by using client drive redirection instead of USB redirection to share USB storage. To prevent USB redirection from redirecting USB storage, set one of the following USB configuration properties and restart Horizon Client.

- `viewusb.ExcludeFamily` = "**`storage`**"
- `viewusb.ExcludeVidPid` = "**`Vid-xxxx_Pid-xxxx`**"

Configuring the browser on the client system to use a proxy server can cause poor client drive redirection performance if the secure tunnel is enabled on the Connection Server instance. For the best client drive redirection performance, configure the browser to not use a proxy server or to automatically detect LAN settings.

Prerequisites

To share folders and drives with a remote desktop or application, you must have Horizon Client 3.5 or later and you must enable the client drive redirection feature. This task includes installing View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, and enabling the agent **Client Drive Redirection** option. It can also include setting policies or registry settings to control client drive redirection behavior. For more information, see the *Setting Up Desktop and Application Pools in View* document.

Procedure

1 Open the Settings dialog box with the Sharing panel displayed.

Option	Description
From the desktop and application selection window	Right-click a desktop or application icon, select **Settings**, and click **Sharing**. Alternatively, select **Connection > Settings** from the menu bar and click **Sharing**.
From the Sharing dialog box when you connect to a desktop or application	Click **Allow** to share, or **Deny** to not share, your home directory.
From within a desktop OS	Select **Connection > Settings** from the menu bar and click **Sharing**.

2 Configure the client drive redirection settings.

Option	Action
Share a specific folder or drive with remote desktops and applications	Click the **Add** button, browse to and select the folder or drive to share, and click **OK**. **Note** You cannot share a folder on a USB device if the device is already connected to a remote desktop or application with the USB redirection feature.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the **Remove** button.

Option	Action
Allow remote desktops and applications access to files in your home directory	Select the **Share your home folder:** *home-directory* check box.
Do not show the Sharing dialog box when you connect to a remote desktop or application	Select the **Do not show dialog when connecting to a desktop or application** check box. If this check box is deselected, the Sharing dialog box appears the first time you connect to a desktop or application after you connect to a server. For example, if you log in to a server and connect to a desktop, you see the Sharing dialog box. If you then connect to another desktop or application, you do not see the dialog box again. To see the dialog box again, you must disconnect from the server and then log in again.

What to do next

Verify that you can see the shared folders from within the remote desktop or application:

- From within a Windows remote desktop, open File Explorer and look in the **Devices and drives** section in the **This PC** folder, or open Windows Explorer and look in the **Other** section in the **Computer** folder.
- From within a remote application, if applicable, select **File > Open** or **File > Save As** and navigate to the folder or drive, which appears in the file system as a network drive that uses the naming format ***folder-name* on *MACHINE-NAME***.

Share Folders by Editing a Configuration File

In addition to sharing folders through the Settings dialog box, you can also share folders by editing a configuration file.

Procedure

1 Create a configuration file named `config` if it does not exist in any of the following locations:

- `$HOME/.vmware/`
- `/usr/lib/vmware/`
- `/etc/vmware/`

2 Add the following line for each folder that you want to share:

`tsdr.share=`*`Folder Path`*

For example, to share folders `/` and `/home/user1`, create the file `/etc/vmware/config` and add the following lines:

```
tsdr.share=/
tsdr.share=/home/user1
```

Folders that are shared in a configuration file are not listed in the Sharing pane of the Settings dialog. You can edit the configuration file to stop sharing folders or share additional folders.

Certificate Checking Modes for Horizon 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 Connection Server and Horizon 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 Client to a server that has a certificate that does not match the host name entered in Horizon 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 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, Connection Server also sends a certificate thumbprint to Horizon Client. The thumbprint is a hash of the certificate public key and is used as an abbreviation of the public key. If Connection 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 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 server name you entered in Horizon Client.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

Switch Desktops or Applications

If you are connected to a remote desktop, you can switch to another desktop. You can also connect to remote applications while you are connected to a remote desktop.

Procedure

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

Option	Action
Choose a different desktop or application on the same server	Perform one of the following actions: ■ If you are logged in to a remote desktop and you want to switch to another remote desktop or application that is already running on your client, select the desktop or application from the **View** menu. ■ If you are logged in to a remote desktop or application and you want to switch to another desktop or application that is not running, select **File > Return to Desktop and Applications List** from the menu bar and then launch the desktop or application from the selector window. ■ From the desktop and application selector window, double-click the icon for the other desktop or application. That desktop or application opens in a new window so that you have multiple windows open, and you can switch between them.
Choose a different desktop or application on a different server	Perform either of the following actions: ■ If you want to keep the current desktop or application open and also connect to a remote desktop or application on another server, start a new instance of Horizon Client and connect to the other desktop or application. ■ If you want to close the current desktop and connect to a desktop on another server, go to the desktop selector window, click the **Disconnect** icon in the upper-left corner of the window, and confirm that you want to log off of the server. You will be disconnected from the current server and any open desktop or application sessions. You can then connect to a different server.

Log Off or Disconnect

With some configurations, if you disconnect from a remote desktop without logging off, applications in the desktop can remain open. You can also disconnect from a server and leave remote applications running.

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 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 remote 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.

Using a Microsoft Windows Desktop or Application on a Linux System

4

Horizon Client for Linux supports many features.

This chapter includes the following topics:

Feature Support Matrix for Linux

Some features are supported on one type of Horizon Client but not on another.

When planning which display protocol and features to make available to your end users, use the following information to determine which client operating systems support the feature.

NOTE Client drive redirection is a Tech Preview feature in Horizon Client 3.5 . It is a fully supported feature in Horizon Client 4.0 and later.

Table 4-1. Remote Desktop Features Supported Linux Clients

Feature	Windows XP Desktop (View Agent 6.0.2 and earlier)	Windows Vista Desktop (View Agent 6.0.2 and earlier)	Windows 7 Desktop	Windows 8.x Desktop	Windows 10 Desktop	Windows Server 2008 R2 Desktop	Windows Server 2012 R2 Desktop
USB redirection	Limited	Limited	X	X	X	X	X
Real-Time Audio-Video (RTAV)	Limited	Limited	X	X	X	X	X
Scanner redirection							
Serial port redirection							

Table 4-1. Remote Desktop Features Supported Linux Clients (Continued)

Feature	Windows XP Desktop (View Agent 6.0.2 and earlier)	Windows Vista Desktop (View Agent 6.0.2 and earlier)	Windows 7 Desktop	Windows 8.x Desktop	Windows 10 Desktop	Windows Server 2008 R2 Desktop	Windows Server 2012 R2 Desktop
RDP display protocol	Limited	Limited	X	X	X	X	X
PCoIP display protocol	Limited	Limited	X	X	X	X	X
VMware Blast display protocol			X	X	X	X	X
Persona Management							
Wyse MMR	Partner client systems only, and only with RDP	Partner client systems only, and only with RDP					
Windows Media MMR							
Location-based printing	Limited	Limited	X	X	X	X	X
Virtual printing	Limited	Limited	X	X	X	X	X
Smart cards	Limited	Limited	X	X	X	X	X
RSA SecurID or RADIUS	Limited	Limited	X	X	X	X	X
Single sign-on	Limited	Limited	X	X	X	X	X
Multiple monitors	Limited	Limited	X	X	X	X	X
Client Drive Redirection			X	X	X	X	X

Windows 10 desktops require View Agent 6.2 or later. Windows Server 2012 R2 desktops require View Agent 6.1 or later.

VMware Blast requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later.

Important View Agent 6.1 and later releases do not support Windows XP and Windows Vista desktops. View Agent 6.0.2 is the last View release that supports these guest operating systems. Customers who have an extended support agreement with Microsoft for Windows XP and Vista, and an extended support agreement with VMware for these guest operating systems, can deploy the View Agent 6.0.2 version of their Windows XP and Vista desktops with View Connection Server 6.1.

Feature Support for Session-Based Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and View Agent or Horizon Agent installed. Multiple users can have desktop sessions on an RDS host simultaneously. An RDS host can be either a physical machine or a virtual machine.

Note The following table contains rows only for the features that are supported. Where the text specifies a minimum version of View Agent, the text "and later" is meant to include Horizon Agent 7.0 and later.

Table 4-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0 or Later, Installed

Feature	Windows Server 2008 R2 RDS Host on a Physical Machine	Windows Server 2008 R2 RDS Host on a Virtual Machine	Windows Server 2012 RDS Host on a Physical Machine	Windows Server 2012 RDS Host on a Virtual Machine
RSA SecurID or RADIUS	X	X	X	X
Smart card	View Agent 6.1 and later	View Agent 6.1 and later	View Agent 6.1 and later	View Agent 6.1 and later
Single sign-on	X	X	X	X
RDP display protocol (for desktop clients)	X	X	X	X
PCoIP display protocol	X	X	X	X
VMware Blast display protocol	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later
HTML Access		View Agent 6.0.2 and later		View Agent 6.0.2 and later
Client drive redirection	View Agent 6.1.1 and later	View Agent 6.1.1 and later	View Agent 6.1.1 and later	View Agent 6.1.1 and later
Virtual printing (for desktop clients)		View Agent 6.0.1 and later		View Agent 6.0.1 and later
Location-based printing		View Agent 6.0.1 and later		View Agent 6.0.1 and later
Multiple monitors (for desktop clients)	X	X	X	X
Unity Touch (for mobile clients)	X	X	X	X

Note The smart card feature also requires Horizon Client 3.4 or later.

For information about which editions of each guest operating system are supported, or which service packs, see the "Supported Operating Systems for View Agent" topic in the View 5.x or 6.x installation documentation. See the "Supported Operating Systems for Horizon Agent" topic in the Horizon 7 installation documentation.

Limitations for Specific Features

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

Table 4-3. Requirements for Specific Features

Feature	Requirements
Real-Time Audio-Video	■ For Horizon Client provided by third-party vendors, the feature requires View 5.2 with Feature Pack 2 or later. ■ For client software available from VMware, you must have Horizon Client 3.2 and later and View Agent 6.0.2 and later. Requires the VMware Blast or PCoIP display protocol.
Virtual printing and location-based printing for Windows Server 2008 R2 desktops, RDS desktops (on virtual machine RDS hosts), and remote applications	■ For partner client software, Horizon Client 3.1 and later and Horizon 6.0.1 with View and later servers. ■ For client software available from VMware, Horizon Client 3.2 and later and View Agent 6.0.2 and later. Requires the VMware Blast or PCoIP display protocol.
USB redirection	■ For partner client software, and View 5.1 and later servers and desktops. ■ For client software available from VMware, Horizon Client 3.2 and later and View Agent 6.0.2 and later. Requires the VMware Blast or PCoIP display protocol.
Smart cards	For single-user virtual machine desktops, Horizon Client 3.2 or later and View Agent 6.0.2 and later. For session-based desktops on RDS hosts, Horizon Client 3.4 and later and View Agent 6.1 and later.
Client drive redirection	For single-user virtual machine desktops and session-based desktops on RDS hosts, Horizon Client 3.5 and later and View Agent 6.1.1 and later.

Note You can also use Horizon Client to securely access remote Windows-based applications, in addition to remote desktops. Selecting an application in Horizon Client opens a window for that application on the local client device, and the application looks and behaves as if it were locally installed.

You can use remote applications only if you are connected to Connection Server 6.0 or later. For information about which operating systems are supported for the RDS (Remote Desktop Sessions) host, which provides remote applications and session-based desktops, see "Supported Operating Systems for Horizon Agent" topic in the View 5.x or 6.x installation documentation. See the "Supported Operating Systems for Horizon Agent" topic in the Horizon 7 installation documentation.

Note 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.

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

Feature Support for Linux Desktops

Some Linux guest operating systems are supported if you have View Agent 6.1.1 or later and Horizon Client 3.4 or later. For a list of supported Linux operating systems and information about supported features, see *Setting Up Horizon 6 for Linux Desktops*, which is part of the Horizon 6, version 6.1 documentation.

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 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.
- Enable Xinerama. If you do not enable Xinerama, the primary display might be identified incorrectly.
- 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 Client uses the monitor configuration that is in use when Horizon 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 Client is running, you must restart Horizon Client in order to use the new monitor configuration.

Horizon 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 have a version of Horizon Client that is earlier than 4.0, and 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.
- If you specify that you want to use all monitors, and if you are using the VMware Blast or PCoIP display protocol, you can specify a subset of adjacent monitors to use by right-clicking the desktop in the desktop selector window, selecting **Full Screen - All Monitors** from the **Display** drop-down list, and clicking to select the monitors you want to use.

  Note If you have a Ubuntu client system, you must select the top-left-most monitor as one of the monitors. For example, if you have 4 monitors stacked 2 X 2, you must select either the 2 monitors on top or the 2 left-most 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 Horizon Client 3.4 or earlier and PCoIP, if you use 2 monitors, you can adjust the resolution for each monitor separately, with a resolution of up to 2560 x 1600 per display. If you use more than 2 monitors, the monitors must use the same screen resolution.
- With Horizon Client 3.5 and later and the PCoIP display protocol, and with Horizon Client 4.0 and later and the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Hardware Version	Windows Version	Number of 4K Displays Supported
10 (ESXi 5.5.x compatible)	7, 8, 8.x, 10	1
11 (ESXi 6.0 compatible)	7 (3D rendering feature disabled; Windows Aero disabled)	3
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1

  The remote desktop must have View Agent 6.2 or later, or Horizon Agent 7.0 or later, installed. For best performance, VMware recommends that the virtual machine have at least 2GB of RAM and 2 vCPUs. This feature might require good network conditions, such as a bandwidth of 1000Mbps with low network latency and a low package loss rate.

  Note When the remote desktop screen resolution is set to 3840 x 2160 (4K), items on the screen might appear smaller, and you might not be able to use the Screen Resolution dialog box in the remote desktop to make text and other items larger.

- 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 *Setting Up Desktop and Application Pools in View* 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. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications, and supports standard webcams, audio USB devices, and analog audio input.

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* document (for View 5.3.x desktops) or the *Setting Up Desktop and Application Pools in View* document (for Horizon 6.0 with View and later desktops). 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 Client for Linux provided by third-party vendors or with Horizon Client 3.2 or a later release that is available from the VMware Product Downloads Web site.

When You Can Use Your Webcam

If a View administrator has configured the Real-Time Audio-Video feature, and if you use the VMware Blast display protocol or 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, you can configure a preferred webcam to use on your remote desktop.

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 of 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 62.

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 VMware Blast display protocol or 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 VMware Blast display protocol or 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 Horizon 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-RTAV-<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 Mono"
   ```

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

5 Log off of the desktop session and start a new session.

Saving Documents in a Remote Application

With certain remote applications, such as Microsoft Word or WordPad, you can create and save documents. Where these documents are saved depends on your company's network environment. For example, your documents might be saved to a home share mounted on your local computer.

Administrators can use an ADMX template file to set a group policy that specifies where documents are saved. This policy is called "Set Remote Desktop Services User Home Directory." For more information, see the "RDS Profiles Settings" topic in the *Setting Up Desktop and Application Pools in View* document.

Set Printing Preferences for the Virtual Printer Feature on a Remote Desktop

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 Horizon Client 3.2 or a later release that is available from the VMware Product Downloads Web site, or with the version of Horizon Client for Linux that is provided by third-party vendors.

For the version of Horizon Client 3.2 or a later that is available from the VMware Web site, this feature also has the following requirements:

- The remote desktop must have View Agent 6.0.2 or later, or Horizon Agent 7.0 or later, installed.
- You must be using the VMware Blast or PCoIP display protocol.

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. For client software provided by third-party vendors, this feature also has the following requirements:

- The version of Horizon Client for Linux must be 2.1 or later.
- You must be using the VMware Blast, PCoIP, or FreeRDP display protocol. This feature does not work with rdesktop.

After a printer is added on the local computer, Horizon 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 Server 2008 and Windows Server 2012.

Prerequisites

Verify that the Virtual Printing component of the agent is installed on the remote desktop. In the remote desktop file system, verify that the following folder exists: `C:\Program Files\Common Files\ThinPrint`.

To use virtual printing, the View administrator must have enabled the virtual printing feature for the remote desktop. This task includes enabling the Virtual Printing setup option in the agent installer, and can include setting policies regarding virtual printing behavior. For more information, see the *View Administration* document if you are using Connection Server and View Agent 5.x or an earlier version. See *Setting Up Desktop and Application Pools in View* if you are using Horizon 6 or later.

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.

  Virtual printers appear as *<printer_name>* in single-user virtual machine desktops and as *<printer_name>(s<session_ID>)* in session-based desktops on RDS hosts if View Agent 6.2 or later, or Horizon Agent 7.0 or later, is installed. If View Agent 6.1 or earlier is installed 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

It is possible to copy text to and from remote desktops and applications. Your View administrator can set this feature so that copy and paste operations are allowed only from your client system to a remote desktop or application, or only from a remote desktop or application to your client system, or both, or neither.

This feature is available if you use the Blast Extreme display protocol or the PCoIP display protocol. Remote applications are supported with Horizon 6.0 or later.

Administrators configure the ability to copy and paste by using group policy objects (GPOs) that pertain to View Agent or Horizon Agent in remote desktops. For more information, see the topic about Blast Extreme or View PCoIP general session variables in *Setting Up Desktops and Applications in View*, in the chapter about configuring policies.

You can copy text from Horizon Client to a remote desktop or application, 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 remote desktop and the file system on your client computer.

Note The copy and paste feature is not supported on iOS Safari.

Troubleshooting Horizon Client 5

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

This chapter includes the following topics:

Problems with Keyboard Input

If, when you type in a remote desktop or application, none of the keystrokes seem to work, the issue might be with security software on your local client system.

Problem

While connected to a remote desktop or application, no characters appear when you type. Another symptom might be that a single key keeps repeating itself.

Cause

Some security software, such as Norton 360 Total Security, includes a feature that detects keylogger programs and blocks keystroke logging. This security feature is meant to protect the system against unwanted spyware that, for example, steals passwords and credit card numbers. Unfortunately, this security software might block Horizon Client from sending keystrokes to the remote desktop or application.

Solution

- On the client system, turn off the keylogger detection feature of your antivirus or security software.

Reset a Remote Desktop or Application

You might need to reset a desktop or application if the application or desktop operating system stops responding. Resetting a remote desktop shuts down and restarts the desktop. Resetting your remote applications quits the applications. 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.

Resetting applications is the equivalent of quitting all remote applications without saving any unsaved data. All open applications are closed, even if the applications come from different RDS server farms.

You can reset a remote desktop only if your administrator has enabled this feature.

Procedure

- Use the **Reset** command.

Option	Action
Reset a remote desktop from within the desktop	Select **Connection > Reset** from the menu bar.
Reset a remote desktop from the desktop and application selection window	Select the remote desktop and select **Connection > Reset** from the menu bar.
Reset remote applications from the desktop and application selection window	Click the **Settings** button (gear icon) in the upper right corner of the window, select **Applications** in the left pane, click **Reset**, and click **Continue**.

For a remote desktop, the operating system in the remote desktop is rebooted. The client disconnects from the desktop. For remote applications, the applications are quit.

What to do next

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

Uninstall Horizon Client for Linux

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

The method you use for uninstalling Horizon Client for Linux depends on the version and the method you used for installing the client software.

Prerequisites

Verify that you have root access on the Linux client system.

Procedure

- If you have Horizon Client 3.1 or earlier, or if you installed the client from the Ubuntu Software Center, select **Applications > Ubuntu Software Center**, and in the **Installed Software** section, select **vmware-view-client** and click **Remove.**
- If you have Horizon Client 3.2 or later, which you installed from the VMware Product Downloads Web site, open a Terminal window, change directories to the directory that contains the installer file, and run the installer command with the `–u` option.

  ```
  sudo env VMWARE_KEEP_CONFIG=yes \

  ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle –u vmware-horizon-client
  ```

  In the file name, *x.x.x* is the version number, *yyyyyyy* is the build number, and *arch* is either `x86` or `x64`. Using the `VMWARE_KEEP_CONFIG=yes` setting means retain the configuration settings when the client is uninstalled. If this environment variable is not set, you are prompted to specify whether to save the configuration settings.

What to do next

You can reinstall the client or install a new version. See "Install or Upgrade Horizon Client for Linux from VMware Product Downloads," on page 14.

Configuring USB Redirection on the Client

6

With Horizon Client, you can use a configuration file on the client system to specify which USB devices can be redirected to a View desktop.

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

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

System Requirements

The USB redirection feature is available only with certain versions of the client software. For the Horizon Client software provided by third-party vendors, this feature also has the following requirements:

- The version of View Agent and View Connection Server must be View 5.1 or later.
- 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, certain files must be installed in certain locations, and certain processes must be configured to start before Horizon Client is launched. These details are beyond the scope of this document.

If you have the version of Horizon Client 3.2 or a later that is available from the VMware Web site, this feature also has the following requirements:

- The remote desktop must have View Agent 6.0.2 or later installed.
- You must be using the VMware Blast or PCoIP display protocol.

If you use Horizon 6.0.1 and later, you can plug USB 3.0 devices into USB 3.0 ports. USB 3.0 devices are supported only with a single stream. Because multiple stream support is not yet implemented, USB device performance is not enhanced. Note that on the Linux client system, i386 processors are supported, whereas armel and armhf architectures are not. The Linux kernel version must be 2.6.35 or later.

USB-Specific Log Files

For troubleshooting purposes, you can increase the amount of information sent to USB-specific logs by using the following commands:

```
vmware-usbarbitrator --verbose
```

```
vmware-view-usbd -o log:trace
```

To get a list of usage information, use the following command:

```
vmware-usbarbitrator -h
```

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 Horizon 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 Horizon 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`	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`	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`	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`** because 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.
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 Horizon 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`** because 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
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 Horizon Client, the View Agent setting overrides the Horizon 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.
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 Horizon Client to allow mouse devices to be redirected to a View desktop. The second property overrides the first and tells Horizon 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 Horizon 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 *View Administration* document.

USB Device Families

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

Note Some devices do not report a device family.

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.

Table 6-2. USB Device Families (Continued)

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

Index